Business Products - Endpoint Protection, DNS Protection, and Security Awareness Training

Administration Guide

Notices

Endpoint Protection, DNS Protection and Security Awareness Training Administration Guide revision Friday, April 11, 2025.

Information in this document is for the following products:

- Endpoint Protection
- DNS Protection
- Security Awareness Training
- Endpoint Detection and Response
- Managed Detection and Response

Contents

Overview

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

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

- **Endpoint Protection** is designed to help keep businesses and their customers safe from viruses, ransomware, phishing, malware, and other cyberattacks. You must install and configure Endpoint Protection before you can use either **DNS Protection** or **Security Awareness Training**.
- **Endpoint Detection and Response** offers advanced threat detection and rapid response by continuously monitoring endpoints to identify and neutralize threats in real time. This product is purchased separately and must be used in conjunction with **Endpoint Protection**. See *Endpoint Detection and Response* on page 94.
- **Managed Detection and Response** provides continuous endpoint and network protection with advanced threat intelligence and expert incident response, ensuring fast, reliable remediation of threats. This product is purchased separately and can work independently or in conjunction with **Endpoint Protection**. See *Managed Detection and Response* on page 96.
- **DNS Protection** provides a powerful and yet easy to use security solution that filters and manages DNS requests at the network and device level. This product is purchased separately and can work independently or in conjunction with **Endpoint Protection**. See *DNS Protection* on page 98.
- **Security Awareness Training** is a hosted program designed to increase understanding and practical implementation of security best practices. The program includes a phishing simulator, training courses, and other tools. This product is purchased separately and can work independently or in conjunction with **Endpoint Protection**. See *Security Awareness Training* on page 112.

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

This guide first walks you through installing and configuring Endpoint Protection and then provides instructions for **DNS Protection** and **Security Awareness Training**, which are included in separate chapters at the end.

Depending on your permissions, certain functionalities discussed within this guide might not be available to you.

Basic terms

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

Endpoint Protection terms:

- **Entities** are devices and Groups that you can manage using the Management Console.
    - **Devices** are the agent installations.
    - **Groups** are organizational units that allow you to manage devices together, for example to apply a specific Policy to a group of devices.
- A **Site** can represent a department, corporate region, or office location. For managed service providers (MSPs) or larger businesses, Sites are a way to summarize sets of endpoints and work with them by client.
- **Policies** configure the behavior of the agents. Default Policies for Endpoint Protection and DNS Protection cannot be edited. An Endpoint Protection unmanaged Policy allows you to select and manage your own settings.
- An **Agent** is a small piece of software that runs on your endpoint devices. The agent has a unique identity to the computer it is installed on and performs background security actions on behalf of the administrator.

Industry terms:

- **Malware** is short for malicious software, and refers to dangerous programs or code. Malware attacks are typically launched by clicking an infected attachment in an email and can include any of the following techniques:
    - A **virus** is a program that may replicate itself. It typically infects computer programs by inserting its own code.
    - **Spyware** is a program that spies on computer activity.
    - **Ransomware** is a program that blocks access to data or threatens to publish data unless a ransom is paid.
- **Social engineering** is a collective name for tricking users into revealing sensitive information. It may include attempts to get users to download a malicious attachment, phishing, baiting, email hacking, and other tactics.
    - **Phishing** is the practice of sending a fraudulent email that appears to be valid with the purpose of getting the recipient to make a purchase or reveal sensitive information. **Spear phishing** is a targeted version of phishing.
    - **Baiting** is the practice of using a false promise to attract a target's greed or curiosity. Typical strategies are to leave malware-infected flash drives in a conspicuous area, enticing online ads or promises that lead to malicious websites, or other tactics to encourage someone to download a malware infected file.
    - **Email hacking** is the unauthorized manipulation of an email account or message.
- **Security** best practices for general protection of endpoints include:

- **Password security** is a critical practice to ensure passwords are complex enough to survive hackers' brute force logins. Passwords should be updated regularly and after any potential security breach. Two factor authentication adds an extra layer of security. It is strongly recommended to adopt as many of these best practices as possible.
- **Endpoint/device security** are practices that ensure all endpoints are patched and up to date. It is strongly recommended that our users keep up to date with patches, in accordance with their own security standards.
- **WiFi security** ensures that wireless connectivity is limited to secure networks. It is strongly recommended that our users maintain as much WiFi security as possible.
- **Mobile device security** includes the practice of limiting the possibility of loss or theft of mobile devices and ensuring they are only used for company business on secure networks. It is strongly recommended that our users protect their mobile devices as much as possible.
- **Physical security** includes increased awareness of portable devices (laptops, tables, phones), as well as the importance of the physical office and its security. It is strongly recommended that our users follow physical security best practices as much as possible.
- **Travel security** includes all the security measures mentioned above when outside the office. It is strongly recommended that our users follow these best practices as much as possible.

Requirements

The products detailed in this section are managed through the **Management Console**, which supports the three most recent versions of the following browsers:

- Google Chrome
- Microsoft Edge
- Firefox
- Safari

Endpoint Protection supports most modern Windows and Mac computers. Windows servers and a mix of VMs are also protected. Review the detailed list if you have questions.

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

Note: To upgrade to SecureAnywhere 9.5.10 or later on Mac devices, you must be running macOS 11 (Big Sur®) or later versions. If you are running macOS 10.15 (Catalina®) or older versions of macOS, you will no longer receive any upgrades to the agent beyond version 9.5.8. Consider upgrading your operating system to macOS 11 (Big Sur®) or later to increase product functionality and feature availability.

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

Endpoint Detection and Response and **Managed Detection and Response** have the same requirements as Endpoint Protection.

Note: To use Detection and Response products on an M-Series Mac device, you must have Rosetta installed.

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

For specific firewall configuration settings, see the Knowledge Base.

Security Awareness Training requirements include:

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

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

Getting started

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

The Management Console is the foundation for Endpoint Protection, Endpoint Detection and Response, Managed Detection and Response,DNS Protection, and Security Awareness Training. Getting started with any of these products requires an initial setup.

Management Console:

- Step 1 – **Register** a trial or **purchase** your business product. You should have completed this step before receiving this guide.
    - See *Purchasing or registering for a trial* on page 12.
- Step 2 – Configure the Management Console by creating and activating your account, setting up two-factor authentication (if desired), and selecting your Management Console view.
    - See *Creating and activating your account* on page 13.
    - See *Setting up two-factor authentication (2FA)* on page 14.
    - See *Selecting your Management Console view* on page 13.
    - See *Creating a Site (MSPs only)* on page 15.

Endpoint Protection:

- Complete Steps 1 and 2 in the Management Console setup procedure to register and configure your console.
- Deploy the Endpoint Protection agents to devices.
- Install an agent on each computer that you want to protect. The agent then registers and reports endpoint activity through the Management Console.
    - See *Downloading and installing the agent* on page 19.

Endpoint Detection and Response

- Complete Steps 1 and 2 in the Management Console setup procedure to register and configure your console.
- Enable and install Endpoint Detection and Response.
    - See *Enabling Endpoint Detection and Response* on page 94 .
    - See *Installing the Endpoint Detection and Response agent* on page 94 .

Managed Detection and Response

- Complete Steps 1 and 2 in the Management Console setup procedure to register and configure your console.
- Enable and install Managed Detection and Response.

- See *Enabling Managed Detection and Response* on page 96.
- See *Installing the Managed Detection and Response agent* on page 96.

DNS Protection:

- Complete Steps 1 and 2 in the Management Console setup procedure to register and configure your console.
- Enable and install DNS Protection.
  - See *Enabling and configuring DNS Protection* on page 98.
- Install an agent on each computer that you want to protect. The agent then registers and reports DNS activity through the Management Console.
  - See *Installing network certificates and licenses* on page 110.

Security Awareness Training:

- Complete Steps 1 and 2 in the Management Console setup procedure to register and configure your console.
- Enable Security Awareness Training and target users.
  - See *Enabling Security Awareness Training* on page 112
  - See *Targeting users for training* on page 113.

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

Step 1: Register/Purchase

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

Purchasing or registering for a trial

1. Go to https://www.webroot.com/us/en/business. Confirm your location from the country list.
2. Under the **For Business** menu, find the **Products** section and click the product that you are interested in.
3. **Click How to Buy**.
   - To purchase **Endpoint Protection**, click **Buy Now** or **Try for Free** and follow the on-screen steps. To purchase large subscriptions or more than one product, contact Sales.
   - For DNS Protection and Security Awareness Training, you can **Try for Free** or **Request a Demo**. On the next page, complete the required information and click **Submit**.

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

Step 2: Setup

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

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

Creating and activating your account

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

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

Selecting your Management Console view

The Management Console has two configuration options:

- The **Managed Service Provider (MSP) view** can be used for businesses as well as organizations managing security for multiple companies.
- The **Business view** is designed for small organizations managing their own security on a single Site.

The Management Console view is established the first time you access it. Note that the **Business view** can be upgraded to the **MSP view** at a later time, if desired.

To select your Management Console view:

1. Log in to your Management Console at my.webrootanywhere.com.
2. If this is your first time accessing the console, you are prompted to select a view.
    - Selecting **Managed Service Provider** sets up a Management Console in which you can manage your products by Sites.
        - Sites can represent departments, office locations, clients, or other organizational units under your management.
        - Separate billing and keycodes are optionally available for each Site.
        - This view cannot be changed to **Business view**.
    - Selecting **Business** sets up a Management Console as a single Site, which focuses only on a smaller company's security.
        - All devices and billing use a single Site and keycode.
        - Separate billing and keycodes are available for each Site.
        - This view can be updated to the **Managed Service Provider view** later.
3. Click **Select** for your preferred view.
4. If you selected **Business**, fill out your company information.
    - **Site / Company Name** is a unique name for the Site or company.
    - **Number of Devices** is the number of devices to be managed.
    - **Company Industry** is the industry that the company works within.
    - **Company Size** is the range of numbers that represents the size of the company.
5. When done, click **Select**.

Note that if you selected **Business view**, you can upgrade it to the **Managed Service Provider view** at a later time. If you selected **Managed Service Provider view**, you cannot change it to **Business view**.

To change your console view from the Business view to the MSP view:

1. In the navigation pane, go to **Settings**.
2. Click the **Advanced Settings** tab.
3. Under **Convert to Managed Service Provider Console**, click **Convert**.

Setting up two-factor authentication (2FA)

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

Setting up 2FA is optional, but highly recommended.

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

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

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

If you selected the **Business view**, go to *Endpoint Protection* on page 18.

If you selected the **Managed Service Provider view**, go to *Creating a Site (MSPs only)* on page 15 next.

Creating a Site (MSPs only)

If you have selected the **Managed Service Provider view** in the Management Console, you need to create a Site to complete your initial configuration.

To create a Site:

1. Click **Sites List** and then click **Add Site**. The **Add Site** wizard opens.
2. Complete the Site **Details**.
   - **Site / Company Name** is a unique name for the Site or company.
   - **Site Type**
     - **External Company** is an external company that you maintain.
     - **Internal Site** is a Site within your own company, such as a location or office.

- **Company Size** (external companies only) is the range of numbers that represents the size of the company.
- **Company Industry** (external companies only) is the industry that the company works within.
- **Billing Cycle** (external companies only) is the billing cycle you define and use as needed for this Site. It is for your reference only and is not linked to your Webroot account.
- **Billing Date** (external companies only) is the month and date for billing, designed and used as needed for this Site. It is for your reference only and is not linked to your Webroot account.
- **Distribution List** is a comma-separated list of up to ten email addresses that can receive scheduled reports. When scheduling a new report, select **Send to distribution list of each site** so that all associated email addresses receive it.
- **Include Global Policies**
    - When enabled, all Global Policies are available for this Site. Once enabled, this option cannot be changed.
    - When disabled, separate Policies must be created for each Site.
- **Include Global Overrides**
    - When enabled, Global Overrides are applied to this Site. For example, if a Site has allowed a particular file and configured it to be a Global Override, all Sites with this option enabled will allow that file. Once enabled, this option cannot be changed.
    - When disabled, separate Overrides must be created for each Site.
- **Comments** (optional) are comments describing the Site or company.
- **Tags** (optional) are useful labels for filtering your searches. Adding custom tags to your Sites allows you to filter your **Sites List** by those tags. To apply a custom tag to your Site, type a tag name in the **Tags** box and press enter after each tag.

3. Click **Next** to continue.
4. In the **Admin Permissions** step, select the permissions to grant to this Site. By default, the account that created the Site is given full administrator permissions and is not shown in the list. All other accounts are listed and default to **No Access**.
    - **Admin** allows full access to the Site.
    - **View Only** allows the ability to only view the Site.
    - **No Access** denies access to the Site.
5. Click **Next** to continue.
6. In the third step, Endpoint Protection options are displayed, including Endpoint Detection and Response and Managed Detection and Response. To use Endpoint Detection and Response, you must have Endpoint Protection enabled. Managed Detection and Response can be used independently or in conjunction with Endpoint Protection.

- If **Endpoint Protection** is enabled, the following options are displayed:
  - **Keycode Type**
    - Full if you purchased the product.
    - Trial if you registered for a free 30-day trial.
  - **Site Seats** specifies the number of endpoints for the Site that you plan to configure. This setting will not set a limit to the number of seats that can be deployed and is not used for billing.
  - **Default Endpoint Policy** is used for all new devices installed for this Site unless the Policy is assigned using inheritance from the Group, Site, or Company. You can modify the Policy the device uses after installation. Creating a copy of the Default Endpoint Policy and modifying it according to Policy best practices and your specific needs is recommended. See *Endpoint Protection Policy best practices* on page 42.
    - **Recommended Defaults** is intended for desktops and laptops.
    - **Recommended DNS Enabled**, like **Recommended Defaults**, is intended for desktops and laptops. It will also automatically install the DNS Protection agent.
    - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit** allows for transparent use of Endpoint Protection. It reports on what is found, but does not remediate infections. It is designed to as a testing Policy to help minimize production impact. Webroot recommends using this Policy only for a short duration, such as during initial setup, to identify potential production false positives and conflicts, and to uncover unknown software.
    - The **Unmanaged** Policy designed to allow a user to edit their settings from the agent user interface. It inherits the previously applied Policy and its settings, but does not have any specific settings other than whether to show the user interface.
      - Intended for technical support, troubleshooting, and when no Policy management is needed.
      - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
      - Should not be used in production.
    - Policies with the prefix **Legacy** contain previously recommended Policy settings.
  - **Data Filter**
    - Use data filters to show or hide data displayed in the console.
    - For example, if you select **2 Months**, all devices that have not connected for two months are excluded from the data shown for this Site.

        - Data filtering may improve page loading performance but limits what you see.
        - When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.
        - **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under **Settings > Data Filter > Data Filter** drop-down.
    - If desired, enable **Endpoint Detection and Response** or **Managed Detection and Response**. The following options are displayed :
        - **Keycode Type**
            - Trial if you registered for a free 30-day trial.
        - **Data Centre**
            - When enabling Endpoint Detection and Response or Managed Detection and Response on a Site for the first time, you must select a **Data Centre**. Choose a data centre from the drop-down menu.
            - ***Note***: This selection applies to all future sites using Endpoint Detection and Response or Managed Detection and Response and cannot be changed.

7. Click **Next** to continue.
8. If desired, enable **DNS Protection**. See *DNS Protection* on page 98.
9. Click **Next** to continue.
10. If desired, enable **Security Awareness Training**. See *Security Awareness Training* on page 112.
11. Click **Save** to complete the Site configuration and to assign a keycode to the Site.

Endpoint Protection

The next step when setting up Endpoint Protection is to deploy the agent. This provides protection as well as feedback about potential problems on the devices. We recommend creating a custom Policy first so you can apply it easily to all devices going forward.

- Create a custom Policy
- Download and install the agent
- Learn how to find your keycode

Creating a custom Policy

Creating a custom Policy using best practices for securing your endpoints is recommended. By creating the Policy now, it can be easily applied to all endpoints in the future.

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

To create a custom Policy:

1. In the navigation pane, under **Manage**, click **Policies**.
    - To create a new custom Policy that is based on the Recommended Defaults Policy, click **Add Policy**.
    - To create a custom Policy that is based on an existing Policy, find the row for the Policy that you want to copy. Under **Actions**, click **Copy**.
2. The newly created Policy is based on the Recommended Defaults Policy, which is configured for most workstation use cases. Customize the Policy to apply best practices and configure specific requirements:
    - **Name** is the name of the Policy.
    - **Description** should be the intent or purpose of the Policy.
    - The following is a list of commonly changed settings:
        - **Basic Configuration**
            - **Show a system tray icon** (default: On).
        - **User Interface**
            - **GUI** (default: Show).
        - **Evasion Shield**
            - Set **Script Protection** to **Detect and Remediate** to allow immediate action when a threat is identified.
        - **USB Shield**
            - **Block USB Storage Devices** (default: Off).

Downloading and installing the agent

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

The Endpoint Protection agent is cloud-based. If you will be installing agents on a network that greatly restricts internet access, specific URLs should be allowed through the firewall for the agent to function correctly.

For a list of URLs that need to be allowed, see the Knowledge Base.

To download and install the agent:

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

a. Click **Sites List**.

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

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

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

2. Copy the **Keycode** for your company or for the Site for future reference. See *Finding your keycode* on page 20.

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

4. Install the agent.

   Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this knowledge base article for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.

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

Note that if you are using DNS Protection with Endpoint Protection, DNS Protection must be enabled in the Endpoint Policy. If the Site has DNS Protection enabled and the Endpoint Policy has DNS Protection turned to On, DNS filtering begins once the device is listed under **Entities**. For more information about DNS Protection, see *DNS Protection* on page 98.

Finding your keycode

A keycode is required when installing the agent. Each keycode is unique to a Site and must be referenced during install or specified by the command line. By default, the keycode is assigned as the filename for the installer for the .exe. This will be used if unchanged. However, if you are using the MSI or the filename has been changed, then the keycode must be specified through the command line or entered through the installer GUI. For more information about deploying the agent, see *Deploying agents* on page 77.

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

For Business view users:

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

For MSP users:

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

Starting to use Endpoint Protection

Congratulations! You have finished setting up Endpoint Protection.

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

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

Learn more

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

You can also see more information online:

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

Spotlight tours

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

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

Navigating your products

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

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

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

- The **Business view** enables you to use the Management Console as a single Site, focusing only on one company's cybersecurity.
  - All devices and billing use a single keycode.
  - You can use **Groups** to organize your devices.
  - This view can be changed to the **Managed Service Provider view** later.
- The **Managed Service Provider view** enables you to manage multiple Sites.
  - Sites can represent businesses, departments, regions, office locations, or other organizational units under your management.
  - Separate billing and keycodes are available for each Site.

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

Note that after 30 minutes of inactivity, you will automatically be signed out of the Management Console. To keep your session active before the session expires, perform any action within the Management Console. Once you have two minutes remaining in your session, you will receive a prompt to stay signed in. Click **Stay Signed In** or **Login** to renew your session.

Navigation

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

- The **console switcher** enables you to move between consoles. If you only have one console assigned to you, your console name will be statically displayed. If you work with multiple consoles, a selectable list of console names can be seen in a drop-down list. You can also rename a using the console switcher; any name change is seen by anyone who uses that console.
- The **Sites List** (**MSP view** only) shows all the Sites you can access. View and manage individual Sites from this page. See *Sites (MSPs only)* on page 26.
- The **Dashboard** tab provides high-level views of your protection. Because the **Business view** is designed for a single organization and the **MSP view** is for organizations managing multiple Sites, the **Dashboard** view is different for each console view. See *Dashboard* on page 24.
- The **Manage** tab contains three sub-tabs:

- The **Entities** page is where you can view, organize, and manage all your devices and Groups. See *Entities* on page 32.
  - **Devices** are the endpoints.
  - **Groups** are organizational units that allow you to manage devices together, for example to apply a specific Policy to a Group of devices.
- The **Policies** page is where you can create and manage your Policies. See *Policies* on page 42.
  - A Policy configures the behavior of the agent and includes setting for how the scan is performed, the frequency of the scan, and other instructions.
  - Default Policies for **Endpoint Protection** and **DNS Protection** cannot be edited.
  - An **Endpoint Protection** unmanaged Policy allows you to select and manage your own settings.
- **Overrides** allow you to identify files and URLs that should be allowed or blocked regardless of a Policy setting or how the products might define the file or URL. See *Overrides for Endpoint Protection* on page 64.

- **DNS Protection** (**Business view** only) shows whether you have **DNS Protection** enabled, and, if so, how it is configured. See *DNS Protection* on page 98.
  - In **MSP view**, **DNS Protection** is configured per Site. See *Sites (MSPs only)* on page 26.
- **Security Awareness Training** shows your campaigns, content, users, and settings (**Business view** only) for **Security Awareness Training**. See *Security Awareness Training* on page 112.
  - In **MSP view**, Security Awareness Training settings are available on the Site page.
- **Reports** provide in-depth information about **Endpoint Protection**, **DNS Protection**, and **Security Awareness Training**. You can create reports on demand or schedule them at recurring intervals. See *Reports* on page 67.
- **Alerts** are email notifications that notify you when a threat is detected or when the agent is installed on a device. An alert distribution list is a list of one or more email addresses that alerts are sent to. See *Alerts and alert distribution lists* on page 83.
- **Admins** shows the administrators, or accounts, that exist in your console. See *Administration tasks* on page 85.
- **Settings** contains configuration sections that vary depending on which view you are using. See *Settings* on page 88.

Commonly used functions

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

- The **Help** button provides links to help documentation and customer support, where you can open a new support ticket.
- Click your **Login Name** to log out of the console.

Dashboard

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

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

The **Business view** version of the **Dashboard** displays an assortment of statistical tiles and status charts.

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

- **Endpoint Protection** shows high-level statistics for the devices being scanned. Click **View Infected** to view infected devices.
- **DNS Protection** shows the status of the agents and networks covered by DNS Protection. If it is not enabled, click **Enable DNS Protection** to enable it.
- **Security Awareness Training** shows information about your target users and campaigns.

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

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

- Drill down within chart components by clicking on chart data.
- In some cases, you can drill down a second level within the displayed details.
- Click the **Edit** button to modify the chart.
- Click the **Remove** button to delete the chart.

The **MSP view** version of the **dashboard** displays Site summaries and status charts.

The **Dashboard Summary** shows high-level statistics for your Sites, seats, and devices.

- Hover over **Sites** to see a breakdown of the number.
- Click **Need Attention** or **Expiring Sites** to go to the **Sites List** page and view details on individual Sites.

Below the Dashboard Summary, various charts detail activity.

- Drill down within chart components by clicking on chart data.
- In some cases, you can drill down a second level within the displayed details.
- Click the **Edit** button to modify the chart.
- Click the **Remove** button to delete the chart.

From this dashboard you can also perform the following actions:

- Click **Add Chart** to create another chart. Select the options you require. Once the chart is defined, click **Add Chart**.

- Click **Site Filter** to set or clear the filter that determines which Sites are reported in the charts.
    - Choose **All** to display all Sites in the charts.
    - Choose **Select Sites** to select which Sites should be displayed in the charts.
- Click **Reset Dashboard** to reset the chart layout, display, and filter back to the default.
- The **Layout** buttons change the chart display to anywhere from one to four charts per row. You can also drag and drop charts to sort them in your desired view.

Sites (MSPs only)

A **Site** can represent a department, corporate region, or office location. For managed service providers (MSPs) or larger businesses, Sites are a way to summarize sets of endpoints and work with them by client.

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

To add a Site, see *Creating a Site (MSPs only)* on page 15.

Viewing all Sites (MSP view only)

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

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

- The **Sites List** table displays all products by default. Click the **View** drop-down menu to select a list of Products or your Custom view, which you can define by clicking the **Customize Columns** button .
- Enter text in the **Search** box to find only those rows that contain the search text.
    - The search checks the entire table, not just the visible rows.
    - Any applied filters will limit the search to only those rows displayed by the filter.
    - The search terms, filters, and sorting preferences that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.
- **Add Site** creates a new Site. See *Creating a Site (MSPs only)* on page 15.
- **Export** downloads the list of Sites as a comma-separated file (.csv), based on the currently applied search and filters.
- **Refresh** updates the list of Sites. Any search and filters you have specified continue to be applied.
- **Filters** opens the filter panel.
    - A green circle with a number on the **Filters** button indicates the number of filters currently being applied.
    - Within the filter panel, expand each section to see available filters.
    - Clicking the **exclude** link next to a filter excludes that filter and selects the rest of the filters in that group.
    - The filters that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.
    - Click **Reset** to manually clear any selections for a single filter group.
    - Click **Reset Filters** to clear all filters.

To customize the Sites List table view:

1. Click the **Customize Columns** button .
2. In the **Customize Columns** panel that opens, select the check box next to each data point to include or exclude it in the **Sites List** table.
3. Drag the double lines ═ icon next to each data point to rearrange the order of columns as they appear on the table.
4. Click **Apply** to save your changes.

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

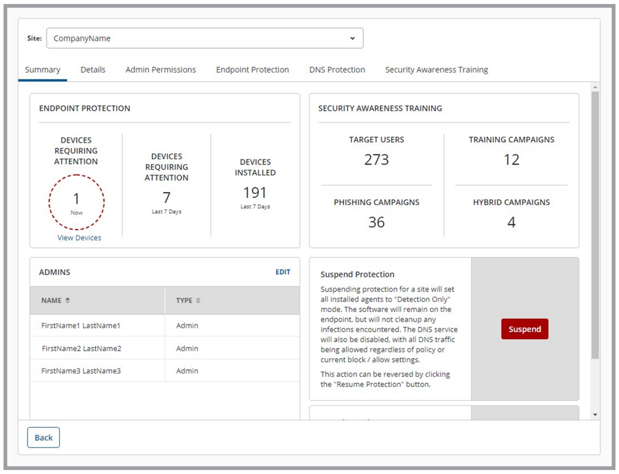
The **Sites List** table enables you to view and manage your Sites as follows:

- **Product subscription status** can be viewed by expanding the blue line. Click the blue arrow at the top of the line to expand and collapse the information.
  - **Active paid** subscriptions are denoted by a blue-filled circle with a white letter.
  - **Active trial** subscriptions are denoted by a white-filled circle with a blue letter.
  - **Expired trial** subscriptions are denoted by a white-filled circle with a blue letter and a blue slash.
  - **Expired paid** subscriptions are denoted by a red-filled circle with a white letter and a white slash.
  - **Inactive** subscriptions are denoted by a gray-filled circle with a black letter.
  - **Suspended** subscriptions are denoted by a black-filled circle with a white letter.
- Click the **Site Name** link to open that Site. Whether you can manage or view the site depends on your permissions.
- Click the **Key** button to see the keycode assigned to the Site. Click **Copy** to save the code to the clipboard.
- Click the **Actions** button to choose ways to manage the subscription:
  - The **Configure** button enables you to change the settings for the subscription.
  - **Start trial** appears as an option if the Site has never had a subscription enabled. Click to start a fully functional, free, 30-day trial.
  - **Upgrade** appears as an option if the subscription is a trial. Click to upgrade to a paid subscription.
  - **Buy** appears if the subscription has expired. Click to renew your subscription.
  - **Re-enable** appears if the subscription has been disabled. Click to re-enable the subscription.
  - The **Legacy Console** button appears for **Security Awareness Training** subscriptions that can access the legacy Security Awareness Training subconsole. Click to open the SAT subconsole. Once in the subconsole, click **Back To Console** to return to the Management Console. For more information on the SAT subconsole, see the Security Awareness Training Admin Guide.

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

Viewing a specific Site

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



- Once a Site is open, you can use the Site switcher at the top to move between Sites.
- The **Summary** tab provides a high-level overview of the devices, status, and administrators associated with this Site.
  - In the **Devices Requiring Attention** tile, the **View Devices** link is visible if you have at least one device that needs attention. Click the link to open the **Entities** page. See *Entities* on page 32.
  - In the **Admins** tile, click **Edit** to modify the administrators for the Site. See *Administration tasks* on page 85.
  - In the **Suspend Protection** tile, click **Suspend** to suspend all protection for the Site.
    - This action leaves the agent installed but will not resolve any infections.
    - If you are using the DNS Protection agent, the agent will stop filtering DNS requests and all DNS settings will revert to their original settings.
    - The DNS resolvers will stop responding to DNS requests from IP addresses registered under the Site.
    - Suspended Sites for Endpoint Protection will continue to be billed like active Sites unless the agents are uninstalled or deactivated. For DNS Protection, you will not continue to be billed.
  - In the **Suspend Protection** tile, click **Resume** to resume suspended protections.

        - Infections will begin resolving.
        - If you are using DNS Protection, filtering will resume, the agent will be enabled, the DNS servers will resolve requests from registered IP addresses, and DNS traffic will be handled according to Policy settings.
    - In the **Deactivate Site** tile, click **Deactivate Site** to deactivate the Site keycode.
        - This is a permanent action that cannot be reversed.
        - This action sends an uninstall command to all devices using that keycode.
        - Deactivated Sites will not be billed.
    - In the **Deactivate Site** tile, click **Delete Site** to delete a deactivated Site from the console.
        - This is a permanent action that cannot be reversed.
        - You will no longer be able to view any data for this Site.
- The **Details** tab shows the details of the Site as provided when you created the Site. Modify any of the settings as needed.
    - **Site / Company Name** is a unique name for the Site or company.
    - **Site Type**
        - **External Company** is an external company that you maintain.
        - **Internal Site** is a Site within your own company, such as a location or office.
    - **Company Size** (external companies only) is the range of numbers that represents the size of the company.
    - **Company Industry** (external companies only) is the industry that the company works within.
    - **Billing Cycle** (external companies only) is the billing cycle you define and use as needed for this Site. It is for your reference only and is not linked to your Webroot account.
    - **Billing Date** (external companies only) is the month and date for billing, designed and used as needed for this Site. It is for your reference only and is not linked to your Webroot account.
    - **Distribution List** is a comma-separated list of up to ten email addresses that can receive scheduled reports. When scheduling a new report, select **Send to distribution list of each site** so that all associated email addresses receive it.
    - **Include Global Policies**
        - When enabled, all Global Policies are available for this Site. Once enabled, this option cannot be changed.
        - When disabled, separate Policies must be created for each Site.
    - **Include Global Overrides**

    - When enabled, Global Overrides are applied to this Site. For example, if a Site has allowed a particular file and configured it to be a Global Override, all Sites with this option enabled will allow that file. Once enabled, this option cannot be changed.
    - When disabled, separate Overrides must be created for each Site.
  - **Comments** (optional) are comments describing the Site or company.
  - **Tags** (optional) are useful labels for filtering your searches. Adding custom tags to your Sites allows you to filter your **Sites List** by those tags. To apply a custom tag to your Site, type a tag name in the **Tags** box and press enter after each tag.
- The **Admin Permissions** tab identifies who has access to the Site.
  - The list of administrators shows who has been granted **Admin**, **View only**, or **No Access** to the Site.
  - Modify the permissions for each administrator as needed.
- The **Endpoint Protection** tab shows the subscription status and the default Site settings. It also contains download links for the agent installation files.
  - **Site Seats** are the number of endpoints for the Site you are configuring. This setting is not used for billing.
  - **Default Endpoint Policy** is used for all new Endpoint Protection devices installed for this Site unless the Policy is assigned using inheritance from the Group, Site, or company. You can modify the Policy that the device uses after installation. It is recommended that you create a copy of the Default Endpoint Policy and modify it according to Policy best practices and your specific needs. See *Endpoint Protection Policy best practices* on page 42.
    - **Recommended Defaults** is intended for desktops and laptops.
    - **Recommended DNS Enabled**, like **Recommended Defaults**, is intended for desktops and laptops. It will also automatically install the DNS Protection agent.
    - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit** allows for transparent use of Endpoint Protection. It reports on what is found, but does not remediate infections. It is designed to as a testing Policy to help minimize production impact. Webroot recommends using this Policy only for a short duration, such as during initial setup, to identify potential production false positives and conflicts, and to uncover unknown software.
    - The **Unmanaged** Policy designed to allow a user to edit their settings from the agent user interface. It inherits the previously applied Policy and its settings, but does not have any specific settings other than whether to show the user interface.
      - Intended for technical support, troubleshooting, and when no Policy management is needed.

        - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
        - Should not be used in production.
    - Policies with the prefix **Legacy** contain previously recommended Policy settings.
- **Data Filter**
    - Use data filters to show or hide data displayed in the console.
    - For example, if you select **2 Months**, all devices that have not connected for two months are excluded from the data shown for this Site.
    - Data filtering may improve page loading performance but limits what you see.
    - When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.
    - **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under **Settings > Data Filter > Data Filter** drop-down.
- **Endpoint Detection and Response** and **Managed Detection and Response** can be toggled on or off. Only one may be enabled for a site.
- The **Download Software** section contains links to the agent installation files for the Endpoint Protection products enabled for the site. These links and files are specific to the Site and keycode. See *Deploying agents* on page 77.

- The **DNS Protection** tab is where you enable or disable DNS Protection.
    - Once enabled, you can configure DNS Protection configuration for the Site. See *DNS Protection* on page 98.
- The **Security Awareness Training** tab is where you enable or disable Security Awareness Training.
    - Once enabled, you can target the users you want to include in training by identifying a domain that contains the email addresses you want to include.
    - You can use Azure Active Directory integration or a manual process to identify the domain. See *Security Awareness Training* on page 112.

Entities

Entities are devices and Groups that you can manage using the Management Console.

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

Viewing available Entities

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

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

- In **Business view** , the **Entities** table contains a list of Groups and devices within each Group.
- In **MSP view**, the **Entities** table contains a list of Sites. You can expand a Site and see the Groups and devices.

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

- You can quickly see if the device is protected.
- A device that has not checked in within the last seven days will be identified as not recently seen.
- Deactivated devices appear in a separate **Deactivated Devices** Group.
  - To reactivate a device and restore it to its former Group, select the check box next to the device name, then click **Reactivate**. Note that the agent must also be reinstalled.
- When looking at devices within a Group, the icon before the device **Name** identifies the type of device as follows:
  - **Windows** icon denotes a Windows desktop.
  - **Server** icon denotes a Windows server.
  - **Apple** icon denotes a macOS desktop.
  - **Location** icon denotes an IP address.
- The icon before the Policy name identifies the Policy assigned to the device. Hovering over this icon displays the full Policy name and assignment method.
  - **Monitor** icon signifies that the Policy is assigned directly to the device.
  - **Building** icon signifies that the Policy is assigned to the device using a Site Policy.
  - **Connected boxes** icon signifies that the Policy is assigned to the device using a Group Policy.
  - **Circle with letter I** icon signifies that there is more than one Policy assigned to the device.
- When you hover over a device name, a pencil icon appears.

- By default, the hostname of a device is displayed. Click **Edit** to change the assigned device name to one that is more intuitive or user-friendly.
- This changes the device name on the **Entities** page and all other locations that it appears within the console.

- The isolation status of a device is shown after its name.
  - **Isolated** is denoted by a lock icon .
  - **Pending Isolation** and **Pending Unisolation** are denoted by an hourglass icon .

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

- In **MSP view**, enter text in the **Search** box to find only those rows that contain the search text.
  - The search checks the entire table, not just the visible rows.
  - The search terms, filters, and sorting preferences that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.
- Click **Agent Commands** to perform specific functions on the selected device(s). Agent commands are executed based on the polling interval defined in the Policy assigned to the device.
  - Windows and Apple icons denote which commands apply to which operating systems.
  - The **Most Popular** commands for Endpoint Protection appear at the top of the list.
    - **Scan** starts a scan of the selected devices when the command is received.
    - **Clean Up** starts a scan of the device when the command is received and quarantines any malicious files. After the scan is complete, you can see the results in the **Scan History**.
    - **Uninstall** (Endpoint Protection and DNS Protection) removes the agent from the selected devices. If the device is using an Endpoint Protection Policy configured to install DNS Protection, DNS Protection will be installed the next time the device checks in.
    - **Deactivate Device** (Endpoint Protection and DNS Protection) uninstalls the agent from the selected devices. This option also moves the devices from the assigned Group to the **Deactivated Devices** Group.
    - **Change Keycode** changes the keycode on the selected devices to the keycode entered.
    - **Reverify All Files and Processes** verifies all files and processes on the selected devices when the next scan runs. This option is useful when creating manual Overrides and enforcing those changes to the selected devices.
    - **Restore File** restores a file that has been quarantined, for example, a false positive for a file that you want to allow.
    - **Run Customer Support Script** runs scripts provided by customer support to update devices or remove infections.

- **System Optimizer** starts the System Optimizer process when the command is received.
- **Restart Device** sends a reboot command to the selected devices. Once the device receives the command, the reboot happens immediately, without notification to the user.
- **Isolate Device** blocks all internal and external network traffic to the device except for communication with the Management Console. Use this command to disconnect a device that might be infected with malware from all networks and minimize the scope of the potential infection. For more information, see *Isolating and unisolating a device* on page 75.
    - Note that to send an **Isolate Device** command, the device must be running PC Agent 9.0.36.40 or later, or Mac Agent 9.6.4 or later.
- **Unisolate Device** unblocks all internal and external network traffic to the device.
    - Note that to send an **Unisolate Device** command, the device must be running PC Agent 9.0.36.40 or later, or Mac Agent 9.6.4 or later.

- Click **View All Commands** to see all possible commands. Use the **Search** box to find specific commands.
    - **Allow Application** allows an application to run on the selected devices.
    - **Allow Processes Blocked by Firewall** allows communication for all processes that are blocked by the Firewall Policy setting. See *Firewall* on page 57.
    - **Clear Log Files** erases current log files to free up space on the selected devices.
    - **Consider All Items as Good / Allow All Denied Applications** tags all detected files on the selected devices as safe and resets all applications that were previously blocked so that they can run.
    - **Customer Support Diagnostics** runs a utility to gather information about an infected device and sends the results to the support team.
    - **Deny Application** blocks an application from running on the selected devices.
    - **Disable Proxy Settings** disables any proxy settings that were enabled on the selected devices. The device will no longer be able to communicate with the internet if its only internet access is through the proxy server.
    - **Lock Endpoint** locks the selected devices by activating the login screen. The user must enter a user name and password to log back in.
    - **Log Off** ends the session and logs the user out of the current account.
    - **Protect an Application** adds an extra layer of security to a specified application running on the selected devices.
    - **Remove Password Protection** removes an uninstall password if one was configured during installation.
    - **Reset Desktop Wallpaper** resets the desktop wallpaper to its default settings. You must restart the device to apply these changes. This option is useful if the

device was recently infected with malware that changed the desktop wallpaper settings.

    - **Reset Screen Saver** resets the screen saver to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the screen saver settings.
    - **Restart in Safe Mode with Networking** restarts the selected devices in Safe Mode with Networking.
    - **Scan a Folder** scans a specified folder on the selected devices.
    - **Shutdown** shuts down the selected devices when they next report in.
    - **Stop Untrusted Processes** stops and terminates any processes that are not allowed. This option is useful if a regular scan did not completely remove all traces of suspected malware.
    - **Unprotect an Application** removes the extra security from a previously protected application.
  - The **Command Log** displays the history of the agent commands that have been run. You can export the command log to a CSV (comma-separated) file. In the Command Log, you can review information about recent and outstanding commands. The log includes data for:
    - **Device name** — The name of the endpoint that received the command.
    - **Command** — The command issued to the endpoint.
    - **Parameters** — Additional parameters for executing the command, such as the full path name.
    - **Date sent** — The date the command was sent from the Management Console.
    - **Status** — This can be one of the following:
      - **Cancelled** — An admin cancelled the command.
      - **Pending** — The agent has not received the command yet.
      - **Expired** — The command was unable to be delivered to the agent.
      - **Delivered** — The command was delivered to the agent.
    - **Actions** — You can perform either of the following actions:
      - **Cancel** — Cancels a command that is in Pending status.
      - **Retry** — Sends the same command again. This is only available for commands in Cancelled, Expired, or Completed statuses.
- **Move** moves selected devices to another Group.
  - If you are using the **MSP view**, the Groups must be within the same Site.
  - Specify if the devices are going to update to the Policy assigned to the Group that they are moving to or keep the Policy that they are currently using.
- **Change Policy** changes the Policy assigned to the selected devices.

- **Export** sends you an email with a link to download a .CSV report containing the current view of the **Entities** table so that you can work with the data locally.
- **Filters** opens the filter panel.
  - A green circle with a number on the **Filters** button indicates the number of filters that are currently applied.
  - Within the filter panel, expand each section to see available filters.
  - Clicking the **exclude** link to the right of a filter excludes that filter and selects the rest of the filters in that group.
  - The filters that you apply will persist as you navigate to other pages within the console until you manually reset them or log out of the console.
  - Click **Reset** to manually clear any selections for a single filter group.
  - Click **Reset Filters** at the bottom of the panel to clear all filters.
- The **Customize Columns** button allows you to customize the view of columns in the **Entities** table. See *Customizing the table view* on page 36 for more information.

Customizing the table view

The **Customize Columns** button allows you to customize the view of columns in the **Entities** table.

To customize the Entities table view:

1. Click the **Customize Columns** button .
2. In the **Customize Columns** panel that opens, select the check box next to each data point to include or exclude it in the **Entities** table.
3. Drag the double lines icon next to each data point to rearrange the order of columns as they appear on the table.
4. Click **Apply** to save your changes.

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

Viewing a specific Entity

1. Go to Manage > Entities.
   - In **MSP view**, select the Site that contains the device you want to manage.
   - In **Business view**, select the Group that contains the device you want to manage.
2. In the **Name** column, click a device. A tabbed page opens to the device **Summary** tab.

On the device **Summary** tab, you can view high-level information about the selected device and perform the following actions:

- By default, the hostname of a device is displayed. Click **Edit** after the device name to change the assigned device name to one that is more intuitive or user-friendly.
  - This changes the device name on the **Entities** page and all other locations that it appears within the console.
  - To change the device name back to its original name, click **Revert to original host name**.
  - The isolation status of a device is shown after its name.
    - **Isolated** is denoted by a lock icon.
    - **Pending Isolation** and **Pending Unisolation** are denoted by an hourglass icon.
- **Agent Commands** are executed based on the polling interval defined in the Policy assigned to the device.
  - Windows and Apple icons denote which commands apply to specific operating systems.
  - The **Most Popular** commands for Endpoint Protection appear at the top of the list.
    - **Scan** starts a scan of the selected devices when the command is received.
    - **Clean Up** starts a scan of the device when the command is received and quarantines any malicious files. After the scan is complete, you can see the results in the **Scan History**.
    - **Uninstall** (Endpoint Protection and DNS Protection) removes the agent from the selected devices.

      Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this knowledge base article for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.
    - **Deactivate Device** (Endpoint Protection and DNS Protection) uninstalls the agent from the selected devices. This option also moves the devices from the assigned Group to the **Deactivated Devices** Group.
    - **Change Keycode** changes the keycode on the selected devices to the keycode entered.
    - **Reverify All Files and Processes** verifies all files and processes on the selected devices when the next scan runs. This option is useful when creating manual Overrides and enforcing those changes to the selected devices.
    - **Restore File** restores a file that has been quarantined, for example, a false positive for a file that you want to allow.
    - **Run Customer Support Script** runs scripts provided by customer support to update devices or remove infections.

- **System Optimizer** starts the System Optimizer process when the command is received.
- **Restart Device** sends a reboot command to the selected devices. Once the device receives the command, the reboot happens immediately, without notification to the user.
- **Isolate Device** blocks all internal and external network traffic to the device except for communication with the Management Console. Use this command to disconnect a device that might be infected with malware from all networks and minimize the scope of the potential infection. For more information, see *Isolating and unisolating a device* on page 75.
    - Note that to send an **Isolate Device** command, the device must be running PC Agent 9.0.36.40 or later, or Mac Agent 9.6.4 or later.
- **Unisolate Device** unblocks all internal and external network traffic to the device.
    - Note that to send an **Unisolate Device** command, the device must be running PC Agent 9.0.36.40 or later, or Mac Agent 9.6.4 or later.

- Click **View All Commands** to see all possible commands. Use the search box to find specific commands.
    - **Allow Application** allows an application to run on the selected devices.
    - **Allow Processes Blocked by Firewall** allows communication for all processes that are blocked by the Firewall Policy setting. See *Firewall* on page 57.
    - **Clear Log Files** erases current log files to free up space on the selected devices.
    - **Consider All Items as Good / Allow All Denied Applications** tags all detected files on the selected devices as safe and resets all applications that were previously blocked so that they can run.
    - **Customer Support Diagnostics** runs a utility to gather information about an infected device and sends the results to the support team.
    - **Deny Application** blocks an application from running on the selected devices.
    - **Disable Proxy Settings** disables any proxy settings that were enabled on the selected devices. The device will no longer be able to communicate with the internet if its only internet access is through the proxy server.
    - **Lock Endpoint** locks the selected devices by activating the login screen. The user must enter a user name and password to log back in.
    - **Log Off** ends the session and logs the user out of the current account.
    - **Protect an Application** adds an extra layer of security to a specified application running on the selected devices.
    - **Remove Password Protection** removes an uninstall password if one was configured during installation.
    - **Reset Desktop Wallpaper** resets the desktop wallpaper to its default settings. You must restart the device to apply these changes. This option is useful if the

device was recently infected with malware that changed the desktop wallpaper settings.

        - **Reset Screen Saver** resets the screen saver to its default settings. You must restart the device to apply these changes. This option is useful if the device was recently infected with malware that changed the screen saver settings.
        - **Restart in Safe Mode with Networking** restarts the selected devices in Safe Mode with Networking.
        - **Scan a Folder** scans a specified folder on the selected devices.
        - **Shutdown** shuts down the selected devices when they next report in.
        - **Stop Untrusted Processes** stops and terminates any processes that are not allowed. This option is useful if a regular scan did not completely remove all traces of suspected malware.
        - **Unprotect an Application** removes the extra security from a previously protected application.
    - The **Command Log** displays the history of the agent commands that have been run. You can export the command log to a CSV (comma-separated) file. In the Command Log, you can review information about recent and outstanding commands. The log includes data for:
        - **Device name** — The name of the endpoint that received the command.
        - **Command** — The command issued to the endpoint.
        - **Parameters** — Additional parameters for executing the command, such as the full path name.
        - **Date sent** — The date the command was sent from the Management Console.
        - **Status** — This can be one of the following:
            - **Cancelled** — An admin cancelled the command.
            - **Pending** — The agent has not received the command yet.
            - **Expired** — The command was unable to be delivered to the agent.
            - **Delivered** — The command was delivered to the agent.
        - **Actions** — You can perform either of the following actions:
            - **Cancel** — Cancels a command that is in Pending status.
            - **Retry** — Sends the same command again. This is only available for commands in Cancelled, Expired, or Completed statuses.
- **Change Policy** changes the Policy assigned to the selected devices.

Click the other tabs to drill down to further details about the device.

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

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

Managing Groups

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

When an agent is deployed, all devices are automatically assigned to the **Default Group**. You can make customized Groups to manage separate devices in different ways.

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

- Click the **Create Group** button to create a new Group for the selected Site. In **MSP view**, you must select a Site to create a new Group.
- Click the **Delete Group** button to delete the selected Group. You must specify a new Group to move any devices that exist in the Group you are deleting.
- Click the **Edit Group** button to modify the name of the Group or the Policy assigned to the Group.
- Click the **Install Devices into this Group** button to deploy a new device directly into the selected Group (Endpoint Protection only). Follow the on-screen prompts to download and run the installer. The devices will automatically inherit the Policies assigned to the selected Group.

To move a device into a new Group:

1. In the navigate pane, click **Entities** .
2. On the **Entities** page, select one or more devices to move to a new Group.
3. Click **Move**.
    - If you are using the **MSP view**, the Groups must be within the same Site.
    - Specify if the devices are going to update to the Policy assigned to the Group they are moving to or keep the Policy they are currently using.

Policies

Policies configure the behavior of the agents. Default Policies for Endpoint Protection and DNS Protection cannot be edited. An Endpoint Protection unmanaged Policy allows you to select and manage your own settings.

- **Global** and **Site** Policies can be edited, copied, or deleted. The **Can Edit** icon beside the Policy **Name** indicates that a Policy can be edited.
- **System** Policies can be viewed or copied.

We recommend reviewing our suggested best practices when setting up Policies. See *Endpoint Protection Policy best practices* on page 42.

Endpoint Protection Policy best practices

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

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

- **Naming**. Make sure that your Policy names can be easily understood. When you have multiple Policies, use descriptive names that quickly identify the type of settings that are enabled in each Policy. You might want to also specify any applications or websites that are blocked.
- **Logical Groups and special circumstances**. What are your main logical Groups? Do some need to be broken down into smaller Groups? What functions require different Policy settings? Do you need to have different Policies for machines that you want to allow to be shut down versus those that cannot be shut down? Do you need to block applications or websites for some of your logical Groups?
- **People and computers**. You may need different Policies for executives and non-executives, workstations and servers, different departments, or even different roles within a department.

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

- **Workstations**. When creating a Policy for workstations, make a copy of the **Recommended Defaults** Policy and then modify each of the following settings:
    - **Scan Settings**
        - Turning **Automatically remove threats found on the learning scan** to **On** removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
- **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:

    - **Scan Settings**
        - Turning **Automatically remove threats found on the learning scan** to **On** removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
    - **Realtime Shield**
        - Turn the **Scan files when written or modified** option to **On**. This option prevents the injection of threats, especially back door threats, such as a malicious macro embedded in what appears to be a safe document file.
- **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**
        - Turn **Show SecureAnywhere in the Start Menu** to **Off**. Disabling this option provides more protection from Endpoint Protection being accessed from the **Start** menu. This is especially important if multiple people have access to the server.
        - Turn **Show SecureAnywhere in Add/Remove Programs** to **Off**. Disabling this option provides more protection from Endpoint Protection being uninstalled. This is especially important if multiple people have access to the server.
    - **Scan Settings**
        - Turn **Scan archived files** to **On**. This provides more thorough protection of the server.
        - Turning **Automatically remove threats found on the learning scan** to **On** removes found threats during the learning scan and creates a clean baseline. Once a machine is clean, Endpoint Protection can quickly check only the things that have changed.
    - **Realtime Shield**
        - Turn the **Scan files when written or modified** option to **On**. This option prevents the injection of threats, especially back door threats, such as a malicious macro embedded in what appears to be a safe document file.

Viewing available Policies

Go to **Manage > Policies** to work with Endpoint Protection and DNS Protection Policies.

If you are working in the **MSP view**, you can create Policies at either the **Global** or **Site** level.

- **Global** and **Site** Policies can be edited, copied, or deleted. The **Can Edit** icon beside the Policy **Name** indicates that a Policy can be edited.
- **System** Policies can be viewed or copied.

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

- Click the **Policies** drop-down menu to select the scope of results shown in the **Policies** table as follows:
    - Global Policies apply to all Sites that you have access to.
    - Under the **Sites** list, select a specific Site to view and manage Policies that are associated with it.
- To further narrow table results, use the **Search** box.
- Click **Add Policy** to create a new Policy. See *Adding a new Policy* on page 45.
- Click **Import Policy** to import an existing Policy from another Site or console. See *Importing an existing Policy from another site* on page 46.

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

- The **Endpoint Protection tab** displays the default Endpoint Protection system Policies and any global Policies that have been created:
    - **Recommended Defaults** is intended for desktops and laptops.
    - **Recommended DNS Enabled**, like **Recommended Defaults**, is intended for desktops and laptops. It will also automatically install the DNS Protection agent.
    - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit** allows for transparent use of Endpoint Protection. It reports on what is found, but does not remediate infections. It is designed to as a testing Policy to help minimize production impact. Webroot recommends using this Policy only for a short duration, such as during initial setup, to identify potential production false positives and conflicts, and to uncover unknown software.
    - The **Unmanaged** Policy designed to allow a user to edit their settings from the agent user interface. It inherits the previously applied Policy and its settings, but does not have any specific settings other than whether to show the user interface.
        - Intended for technical support, troubleshooting, and when no Policy management is needed.
        - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
        - Should not be used in production.
    - Policies with the prefix **Legacy** contain previously recommended Policy settings.
- The **DNS Protection tab** displays a switch to turn on DNS Protection, if it hasn't been enabled already. If DNS Protection has been enabled, it displays the default DNS Protection Policies and any Global Policies that have been created:
    - **DNS High Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - **DNS Medium Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - See *Managing DNS Protection Policies* on page 100.

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

- Click the Policy **Name** link to view or edit it. Only user-created Policies are editable.
- In the **Actions** column, you can manage the Policy as follows:
    - **View** enables you to review the Policy settings assigned to a default Policy.
    - **Copy** copies an existing Policy. See *Copying an existing Policy* on page 45.
    - **Edit** enables you to edit the Policy settings assigned to a Policy you created, copied, or imported. See *Editing a Policy* on page 46.
    - **Delete** deletes a user-created Policy. See *Deleting a Policy* on page 47.
- **Policy Usage** metrics are displayed at the bottom of the page.

Adding a new Policy

1. Open **Manage > Policies**.
2. From either the **Endpoint Protection** or **DNS Protection** tab, click **Add Policy**.
    - Provide a unique **Name** and a **Description**. Each field is limited to 50 alphanumeric characters.
    - Select the **Scope** to specify if the Policy can be applied to Sites that are configured to include **Global** Policies or just the selected **Site**. Note that once a **Scope** is set, it cannot be changed.
    - Click the caret to expand and contract the settings in each section.
    - Modify any of the default Policy settings as desired.
3. When done, click **Save**.

Copying an existing Policy

1. Open **Manage > Policies**.
2. From either the **Endpoint Protection** or **DNS Protection** tab, select the Policy you want to copy.
3. Under **Actions**, click **Copy**.
    - Provide a unique **Name** and a **Description**. Each field is limited to 50 alphanumeric characters.
    - Select the **Scope** to specify if the Policy can be applied to Sites that are configured to include **Global** Policies or just the selected **Site**. Note that once a **Scope** is set, it cannot be changed.
    - Click the caret to expand and contract the settings in each section.
    - The new Policy is based on the settings of the Policy that you copied.

- Modify the Policy settings as desired.

4. When done, click **Save**.

Renaming a Policy

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

Importing an existing Policy from another site

You can import an existing Endpoint Protection Policy from another Site or from another console.

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

Once the Policy has been imported, you can edit it as needed.

Editing a Policy

You can edit Policies that you created, copied, or imported. Default Policies cannot be edited.

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

Deleting a Policy

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

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

Endpoint Protection Policy settings

Review *Endpoint Protection Policy best practices* on page 42 when determining how best to set up your Policies.

To review or modify Endpoint Protection Policies:

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

Basic configuration

Basic configuration Policies control the behavior of the agent.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Show a SecureAnywhere shortcut on the desktop	An Endpoint Protection desktop shortcut is available on the desktop.	The Endpoint Protection shortcut is not available on the desktop.
Show a system tray icon	An Endpoint Protection icon is available in the system tray.	The Endpoint Protection icon is not in the system tray.
Show a splash screen on bootup	An Endpoint Protection screen displays during system boot.	The Endpoint Protection screen is not displayed during system boot.
Show SecureAnywhere in the Start Menu	Endpoint Protection is available in the **Start** menu.	Endpoint Protection is not available in the **Start** menu.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Show SecureAnywhere in Add/Remove Programs	Endpoint Protection is listed in **Add/Remove Programs** or **Programs and Features**, depending on your Windows version.	Endpoint Protection is not listed in **Add/Remove Programs** or **Programs and Features**.
Show SecureAnywhere in Windows Action Center	Endpoint Protection is listed in the **Action Center**, under Virus & threat protection.	Endpoint Protection is not listed in the **Action Center**.
Automatically download and apply updates*	The agent automatically downloads and applies updates without notifying the end-user.	The agent does not automatically download or apply updates.
Operate background functions using fewer CPU resources*	Non-scan functionality is run in the background to save CPU resources.	All Endpoint Protection functionality is run in the foreground.
Favor low disk usage over verbose logging	The Endpoint Protection log only maintains the last four log items.	The Endpoint Protection log maintains all log items.
Lower resource usage when intensive applications or games are detected*	Endpoint Protection functions are postponed while the end-user is gaming, watching videos, or using other intensive applications.	Endpoint Protection functions are not 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 is not available.
Force non-critical notifications into the background	Endpoint Protection only displays critical messages in the system tray. Information messages are hidden.	Both critical and information messages are displayed in the system tray.
Fade out warning messages automatically*	Endpoint Protection messages in the system tray automatically disappear after a few seconds.	The end-user must close Endpoint Protection messages in the system tray
Store Execution History details	Data is stored in the **Execution History** log.	No data is stored in the **Execution History** log.
Poll interval*	This specifies how often the agent will check for updates. The default setting is 1 hour. The recommended setting is 15 minutes.	

* applies to Apple devices as well.

Scan schedule

Scan schedule Policies control when scans occur.

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

* applies to Apple devices as well.

Scan Policies

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enable Realtime Master Boot Record (MBR) Scanning	The master boot record, which loads before the operating system, is scanned.	The master boot record is not scanned.
Enable Enhanced Rootkit Detection	Endpoint Protection scans for rootkits and other malicious software hidden on disk or in protected system areas. These are created by spyware developers to avoid detection and removal.	Endpoint Protection does not scan for rootkits and other malicious software.
Enable "right-click" scanning in Windows Explorer	A right-click menu is available in Windows Explorer to immediately scan a file.	The right-click menu is not available.
Update the currently scanned folder immediately as scanned	The Endpoint Protection display updates each time a file is scanned.	The Endpoint Protection display is updated periodically, showing all files scanned since the last update.
Favor low memory usage over fast scanning	Less memory is used to run a scan, but the scan might run slower.	More memory is used to run a scan, so the scan runs faster.
Favor low CPU usage over fast scanning	Less processor usage is used to run a scan, but the scan might run slower.	More processor usage is used to run a scan, so the scan runs faster.
Show the "Authenticating Files" popup when a new file is scanned on execution	A dialog box showing the scan appears when an end-user executes a file for the first time.	Nothing appears when an end-user executes a file for the first time, however, the file will still be scanned.
Save non-executable file details to scan logs	All file data is saved to the scan log, resulting in a larger log file.	Only executable file data is saved to the scan log, resulting in a smaller log file.
Scan archived files*	The file types .zip, .rar, .cab, and 7-zip are scanned.	The file types .zip, .rar, .cab, and 7-zip are not scanned.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Automatically reboot during cleanup without prompting	A reboot automatically occurs after a cleanup to remove malware.	The user is prompted to reboot after a cleanup to remove malware.
Never reboot during malware cleanup	The machine does not reboot during a cleanup to remove malware.	A reboot is not prevented during a cleanup to remove malware. The cleanup may be incomplete.
Automatically remove threats found during background scans	Threats found during background scans are automatically sent to quarantine.	Threats are sent to quarantine during scheduled scans.
Automatically remove threats found on the learning scan	Threats found during the first scan of the device are automatically sent to quarantine.	Threats are sent to quarantine during scheduled scans.
Enable Enhanced Support	Logs are sent to customer support.	No logs are sent to Webroot.
Show Infected Scan Results	Logs are sent to customer support.	No logs are sent to Webroot.
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) are blocked from installation or removed, if possible, from the machine. The default setting is **On**.	These applications are not blocked or removed.
Allow files to be submitted for threat research	Files are sent for threat research.	No files are sent to Webroot.

* applies to Apple devices as well.

Self protection

Self protection Policies control how the agent protects itself.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enable self-protection response cloaking	If another product is attempting to interfere with Endpoint Protection, Endpoint Protection attempts to protect itself by launching a protective scan.	Endpoint Protection does not attempt to protect itself.
Self-protection Level	This option specifies the self-protection detection level. • **Minimum** protects the Endpoint Protection settings. Use this level if you have other cybersecurity products installed. • **Medium** prevents other programs from disabling Endpoint Protection. Use this level for maximum compatibility with other cybersecurity products. • **Maximum** protects the Endpoint Protection processes. This is the recommended level if you have no other cybersecurity products.	

Heuristics

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

Realtime shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Realtime Shield Enabled*	Suspicious or known threats are immediately blocked.	Threats are not blocked, and the user is not notified. Protection is diminished when this setting is disabled.
Enable Predictive Offline Protection from the central SecureAnywhere database	A threat definition file is downloaded to the device and used for protection when the device is offline.	The threat definition file is not downloaded and the device is not protected when it is offline.
Remember actions on blocked files	Endpoint Protection remembers how an end-user responded to an alert (allow or block) and does not prompt the user again about the same file.	Endpoint Protection alerts every time for the same file.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Automatically quarantine previously blocked files*	Files that have been previously quarantined are quarantined automatically, for example if the file was downloaded a second time.	Files that have been previously quarantined are not quarantined during the next scheduled scan.
Automatically block files when detected on execution*	Suspicious or known threats are automatically blocked when executed.	Suspicious or known threats alert for the end-user to allow or block.
Scan files when written or modified*	New or modified files are scanned when they are saved or installed.	New or modified files are not scanned when they are saved or installed.
Block threats automatically if no user is logged in*	Suspicious or known threats are automatically blocked from execution when no user is logged in.	Files are not blocked from execution when no user is logged in.
Show realtime event warnings	An alert is displayed as soon as suspicious activity is detected.	No alerts are displayed.
Show realtime block modal alerts	An alert is 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**.	No alerts are displayed.
Show realtime block notifications	A tray notification alert is displayed as soon as malware is detected.	No tray notification alerts are displayed.

* applies to Apple devices as well.

Behavior shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Behavior Shield Enabled	The end-user is prompted for suspicious threats, and known threats are immediately blocked and quarantined.	Threats are not alerted or blocked.
Assess the intent of new programs before allowing them to execute	Endpoint Protection examines a program's activity before allowing it to run. If it appears safe, Endpoint Protection allows it to launch and continues to monitor its activity.	Programs are not examined.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enable advanced behavior interpretation to identify complex threats	Endpoint Protection examines a program to determine its intent. For example, malware may modify a registry entry and then send an email.	Programs are not examined.
Track the behavior of untrusted programs for advanced threat removal	Endpoint Protection examines only those programs that have not been classified as safe or a threat.	Programs are not examined.
Automatically perform the recommended action instead of showing warning messages	Endpoint Protection determines if a threat should be allowed or blocked.	The end-user is prompted to determine if a threat should be allowed or blocked.
Warn if untrusted programs attempt low-level system modifications when offline	Programs that are not classified alert if the program tries to make changes to a device when the device is offline.	Programs are not alerted if they try to make changes to a device when the device is offline.

* applies to Apple devices as well.

Core system shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Core System Shield Enabled	The end-user is prompted for suspicious threats, and known threats are immediately blocked and quarantined.	Threats are not alerted or blocked.
Assess system modifications before they are allowed to take place	Endpoint Protection intercepts any attempt to make system changes, for example a new service installation.	Endpoint Protection does not intercept any attempt to make system changes.
Detect and repair broken system components	Endpoint Protection detects and restores corrupted components or files.	Endpoint Protection does not detect or restore corrupted components or files.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Prevent untrusted programs from modifying kernel memory	Programs that are not classified are blocked from changing kernel memory.	Programs that are not classified are not blocked from changing kernel memory.
Prevent untrusted programs from modifying system processes	Programs that are not classified are blocked from changing system processes.	Programs that are not classified are not blocked from changing system processes.
Verify the integrity of the LSP chain and other system structures	Endpoint Protection monitors the Layered Service Provider (LSP) chain and other system structures for corruption.	Endpoint Protection does not monitor the Layered Service Provider (LSP) chain and other system structures for corruption.
Prevent any program from modifying the HOSTS file*	Endpoint Protection alerts when an attempt is made to modify the hosts file.	Endpoint Protection does not alert when an attempt is made to modify the hosts file.

* applies to Apple devices as well.

Web threat shield

Web threat shield Policies control browsing and search engine behavior.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enable Web Shield*	Endpoint Protection monitors internet browsing and alerts on suspicious sites. It also analyzes search engine result links.	There is no internet browsing monitoring or search engine analysis.
Activate browser extension	Users see icons when viewing web search results. They can hover over an icon to get a review of the site's reputation.	Users do not see reputation icons when viewing web search results.
Block malicious websites*	Endpoint Protection blocks known malicious websites.	No websites are blocked.
Enable real time antiphishing*	Endpoint Protection alerts on zero-day phishing sites, which are sites that have never been seen before and are not classified.	Zero-day phishing sites are not alerted.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Show safety ratings when using search engines*	Search engine result links are identified as trusted sites (green checkmark) or suspicious sites (red X).	Search engine results are not identified.
Enable web filtering driver	Additional protections against malicious connections, including when browser extensions are disabled, are used.	Additional protections against malicious connections are not used.
Suppress the user's ability to bypass blocked websites*	End-users are not able to bypass the block page presented when a known malicious website is detected.	A user can bypass the block page.
Suppress the user's ability to request website reviews*	End-users are not able to submit a website review request from the block page presented when a known malicious website is detected.	A user can request a website review from a block page.

* applies to Apple devices as well.

Identity shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Identity Shield Enabled*	Endpoint Protection monitors online transactions. On macOS, this option controls the **Secure Keyboard Entry Mode** setting.	Online transactions are not monitored.
Look for identity threats online	Endpoint Protection analyzes and alerts when it detects malicious content.	Content is not analyzed.
Verify websites when visited to determine legitimacy	Endpoint Protection analyzes and alerts when a website's IP address has been redirected or has been identified as a threat.	Website IP addresses are not analyzed.
Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks	Endpoint Protection analyzes and alerts when a website is redirected, such as a man-in-the-middle attack.	Website redirects are not analyzed.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Block websites from creating high risk tracking information	Endpoint Protection blocks third-party cookies if they originate from a malicious site.	Third-party cookies are not blocked.
Prevent programs from accessing protected credentials	Endpoint Protection blocks programs from accessing credentials, for example, when you enter your user name and password or choose to save credentials for a website.	Programs are not blocked from accessing credentials.
Warn before blocking untrusted programs from accessing protected data	Endpoint Protection alerts when programs attempt to access data.	Programs accessing data are not alerted.
Allow trusted screen capture programs access to protected screen contents	Trusted screen capture programs function, regardless of the content displayed on screen.	Screen capture programs are not able to access protected screen contents.
Enable Identity Shield compatibility mode	Certain applications that Identity Shield might normally block are allowed to run. For example, you may need to enable this option if devices have issues running applications. Even when enabled, the Identity Shield core functionality still protects the device.	Identity Shield continues to block all applications that it identifies as malicious.
Enable keylogging protection in non-Latin systems	Endpoint Protection protects devices using non-Latin languages, such as Japanese and Chinese, from keyloggers.	There is no protection from keyloggers.

* applies to Apple devices as well.

Firewall

The firewall Policies control the Endpoint Protection firewall.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enabled	The Endpoint Protection firewall monitors outgoing traffic and the Windows firewall monitors incoming traffic. The Endpoint Protection firewall looks for untrusted processes trying to connect to the internet and steal personal information. If the firewall detects suspicious traffic, the end-user is alerted.	Outgoing traffic is not monitored.
Firewall level	This option specifies the level of firewall protection. • **Default Allow** allows all processes to connect to the internet, unless explicitly blocked by the agent. • **Warn unknown and infected** looks for any new, untrusted processes connecting to the internet or if the device is infected. • **Warn unknown** looks for any new, untrusted process connecting to the internet. • **Default Block** looks for any process connecting to the internet, unless explicitly blocked by the agent.	
Show firewall management warnings	A warning is displayed when Windows firewall is off.	No warnings are displayed when Windows firewall is off.
Show firewall process warnings	Firewall level warnings are displayed.	No warnings are displayed and the process is allowed.

* applies to Apple devices as well.

User interface

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

- When set to **Show**, users can see and access Endpoint Protection on their device. They can perform a scan, but they cannot manage the agent or modify any settings.
- When set to **Hide**, users are prompted to contact their administrator if they attempt to access Endpoint Protection. On macOS, this option hides the system tray icon as well.

System optimizer

System optimizer Policies control general Windows cleanup tasks, such as removing unnecessary files and data.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Manage System Optimizer centrally	Displays the System Optimizer controls.	System Optimizer controls are not displayed.
Days of week	System Optimizer runs on the selected day of the week.	System Optimizer does not run on the selected day of the week.
Run at specific time of day - hour	This option specifies the hour of the day when you want the System Optimizer to run.	
Run at specific time of day - minute	This option specifies the minute of the selected hour when you want the System Optimizer to run.	
Run on bootup if the system was off at the scheduled time	System Optimizer runs at bootup if the machine was off at the scheduled run time.	System Optimizer only runs at the scheduled run time.
Enable Windows Explorer right click secure file erasing	Windows Explorer has a right-click menu option allowing a user to erase a file, without the file being sent to the Recycle Bin.	This option is not displayed in Windows Explorer.
Recycle Bin	All files in the Recycle Bin are deleted when System Optimizer runs.	Nothing is deleted from the Recycle Bin.
Recent document history	The history of recently opened files is deleted from the **Start** menu. Note that only the history is deleted, not the actual files.	Nothing is deleted from the **Start** menu.
Start Menu click history	The history of shortcuts to recently opened programs is deleted from the Start menu. Note that only the history is deleted, not the actual shortcuts.	No history is deleted.
Run history	The history of commands is deleted from the **Run** dialog box. A reboot may be needed to clear all commands.	No history is deleted.
Search history	The computer search history is deleted. Note that only the history is deleted, not any files or programs that were found during a search.	No history is deleted.
Start Menu order history	When a reboot occurs, any changes to the **Start** menu order is reverted, and the menu will be in the default alphabetical order.	The **Start** menu order is not reverted.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Clipboard contents	Content on the Clipboard is cleared.	No clipboard content is cleared.
Windows Temporary folder	All data in the Windows temporary folder, usually `C:\Windows\Temp\`, is deleted, unless the file is in use.	No data is deleted.
System Temporary folder	All data in the system temporary folder is deleted unless the file is in use. The location of this folder varies depending on the Windows version.	No data is deleted.
Windows Update Temporary folder	All data in the Windows Update temporary folder is deleted, unless the file is in use.	No data is deleted.
Windows Registry Streams	The Windows registry change history is deleted. Note that only the history is deleted, not any registry changes or keys.	No history is deleted.
Default logon user history	The registry key that stores the last user logged into the computer is deleted. Users have to enter their user name each time the computer is booted. This setting does not apply to computers using the default Welcome screen.	The registry key is not deleted.
Memory dump files	All memory dump files, which are automatically created for certain Windows errors, are deleted.	No dump files are deleted.
CD burning storage folder	All Windows project files, created when the Windows built-in function is used to copy files to a CD, are deleted unless the file is in use. The location of this folder varies depending on the Windows version.	No project files are deleted.
Flash Cookies	Adobe Flash data are deleted. Note that these are not actual cookies controlled by browser cookie privacy controls.	No data is deleted.
Address bar history	The history of visited websites is deleted from Internet Explorer.	No history is deleted.
Cookies	All cookies are deleted. Users must re-enter passwords, shopping cart items, and other entries stored in cookies.	No cookies are deleted.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Temporary internet Files	All temporary browser files are deleted.	No files are deleted.
URL history	The history pane in Internet Explorer is cleared.	No entries in the history pane are deleted.
Setup Log	Internet Explorer update log files are deleted.	No files are deleted.
Microsoft Download Folder	Files in the Internet Explorer download folder are deleted.	No files are deleted.
MediaPlayer Bar History	The list of audio and video files recently opened with the media player in Internet Explorer is deleted. Note that the files themselves are not deleted, just the list of recently opened files.	The list of recently opened files is not deleted.
Autocomplete form information	Internet Explorer AutoComplete data are deleted. Users must re-enter data on forms.	No data is deleted.
Clean index.dat	When a reboot occurs, the `index.dat` file that stores Windows information, such as web addresses, search queries, and recently opened files, is deleted.	The `index.dat` file is not deleted.
Control the level of security to apply when removing files	This option specifies how you want to handle deleted files. • **Normal**—Files are deleted, bypassing the Recycle Bin. A recovery utility may be able to restore these files. This option is the fastest cleanup process. • **Medium**—Files are deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten three times. A recovery utility has a harder time restoring these files. This cleanup process takes longer than a normal cleanup process. • **Maximum**—Files are deleted, bypassing the Recycle Bin, and the location where the data was stored will be overwritten seven times, including space around the data location. These files are the most difficult for a recovery utility to restore. This is the slowest cleanup process.	

DNS Protection Policy settings

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Install DNS Protection	DNS Protection is installed with the Endpoint Protection agent.	DNS Protection is not installed.

Evasion shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Script Protection	This setting specifies the level of script protection. • **Off** disables script protection. • **Detect and Report** detects and alerts when script threats are discovered. • **Detect and Remediate** detects, alerts, and quarantines script threats when discovered.	

EDR / MDR

The EDR / MDR Policy controls whether the Endpoint Detection and Response or Managed Detection and Response agent is installed with the Endpoint Protection agent.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Install EDR / MDR Agent	The EDR / MDR Agent is installed with the Endpoint Protection agent.	The EDR / MDR Agent is not installed.

Note: this policy is only available for Windows installation.

USB shield

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

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Enable USB Shield	Suspicious or known threats on a USB attached storage device are immediately blocked if executed.	Threats are not blocked in real-time. USB drives can still be scanned using the context menu option **Scan with Webroot**.

Policy Setting	When the Policy setting is enabled	When the Policy setting is disabled
Block USB Storage Devices	USB attached storage devices are blocked for all read, write, and execute access. End users receive a message when a USB storage device is inserted.	USB attached storage devices are fully accessible.

Overrides for Endpoint Protection

Overrides allow you to identify files and domains that should be allowed or blocked regardless of a Policy or the category of a domain.

In **MSP view**, Global file Overrides are applied to all Sites that have **Include Global Overrides** enabled in the Site **Details** tab (recommended).

Note that Site Overrides will always take precedence over Global Overrides.

Policy Overrides will always take precedence over Site Overrides.

Changes in Overrides replicate within 15 minutes of being applied.

To access DNS Overrides, go to **Manage > Overrides** and select the **Web Overrides** tab.

Allowing and blocking files

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

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

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

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

To add a file Override:

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

        - Select the **Include Sub-Folders** check box to include subfolders of the specified path.
        - Select the **Detect if Malicious** check box to detect and remediate the file according to the assigned Policy. Monitoring and journaling are disabled. When this option is disabled, the detect and remediate Policy settings do not apply to the file.
        - In the **Name** box, type a name for the override.
        - For **Scope**, click **Global** to specify that the rule should apply to all Sites that are configured to include Global settings, or click **Site** to include just the selected Site.
            - If you select **Site** , you can associate it with a Policy, which can be applied to individual Sites, Groups, or devices.
        - Select the **Associate with policy** check box to apply this override to a default or saved policy.
    - **MD5** hash
        - Files based on MD5 hash values can be allowed or blocked.
        - If selected, specify the 32-character hash value.
4. When you are finished, click **Save**.

To import defined Overrides from another console or Site:

1. Click **Import Overrides**.
2. Use the **Console / Site Source** drop-down menu to select the console/Site containing the Overrides you want to import from.
3. Use the **Console / Site Destination** drop-down menu to select the console/Site you want to import the Overrides to.
4. Select the check box next to any of the following options:
    - **Remove Redundant Overrides** removes redundant entries from the Override import list, keeping the Override that you already have in place. If not selected, redundant entries are not removed.
    - **Overwrite Existing Overrides** allows redundant entries that are not removed to overwrite existing entries. If not selected, redundant entries persist after the import.
    - **Include Policy Based Overrides** imports Overrides assigned to the Policy used by the Site that you are importing from. These Overrides will be converted to **Global** Overrides. If not selected, the Policy Overrides from the Site are not imported.
5. When you are finished, click **Import**.

To edit an Override:

1. Find the Override in the table and under the Actions column, click **Edit**.
2. Change any Override specifications. Note that you will receive a **Redundant Override** alert if the Cloud determination already matches the selected Allow/Block value.
3. Click **Save**.

To delete an Override:

1. In the **Override**s table, select the check box next to the name of the Override that you want to delete.
2. Click **Delete**.

Allowing and blocking websites

If you are only using Endpoint Protection, the allowed settings specified in the **Web Overrides** tab are related to the optional Web Threat Shield Policy settings.

If you are using DNS Protection, you can both allow and block domains in the **Web Overrides** tab.

To specify a domain that should be allowed or blocked:

1. Click **Add** to specify a domain that should be allowed or blocked.
    - In the **Domain(s)** box, enter a comma-separated list of domains you want to create a rule for. The protocol (such as https or www) is not needed. For example, you can specify domain.com. Wildcards are supported (*.domain.com).
    - Select **Scope** (**MSP view** only) to specify if the rule should apply to all Sites that are configured to include global settings or just the selected Site.
    - Select **Policy** (**MSP view** only) to associate this rule with a Policy and specify the Policy. If you do not specify a Policy, the Override will be associated with the Site.
    - Select **Block/Allow** to specify if the domain should be blocked or allowed.
    - When **Block Malicious URLs** (Web Threat Shield only) is selected, malicious URLs (such as domains with known malware) are still blocked by the Web Threat Shield Policy.
2. Click **Refresh** to update the table.

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

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

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

Reports

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

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

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

Report types

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

- **DNS Protection** reports are only available if you have DNS Protection enabled. See *DNS Protection reports* on page 111.
- **Security Awareness Training** reports are only available if you have Security Awareness Training enabled. See *Security Awareness Training reports* on page 124.

Device reports

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

File threat reports

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

Shield reports

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

Creating and running a report

You can see reports on-demand. You can also run existing, scheduled reports outside of their scheduled times.

1. Click **Reports** in the navigation pane. Ensure you are on the **On-demand** tab.
2. Select the **Site** to run the report against from the drop-down. You can also run reports against all Sites.
3. Select the **Report** you want to view.
4. When applicable, specify a time **Period** for the report data.

5. Click **Submit** to generate and display the report. Depending on the report type, you may have one or more of the following tasks and controls available for the report:
    - Click on chart data to show details for that subset of data. Some charts provide further levels to show more information.
    - In a table layout, click on a row to see details for that table row entry.
    - Click on file names to see more details.
    - Click **Export to CSV** to download the report data to a comma-separated file (.csv). Export to CSV is only available for the following reports:
        - All Threats Seen
        - All Undetermined Software Seen
        - Devices with Threats Seen on Last Scan
        - Devices with Undetermined Software on Last Scan
        - DNS: Active Hosts
        - Evasion Shield
        - Web Threat Shield Blocked URL History
        - Web Threat Shield Blocked URLs
    - Click **Actions** to access some of the following functions:
        - **Add this File to Allow list** specifies the file as an allowed file for the following reports:
            - All Threats Seen
            - All Undetermined Software Seen
            - Devices with Undetermined Software on Last Scan
            - Evasion Shield – Script Detections
            - Devices with Threats Seen on Last Scan
            - Threat Detection History reports
        - **Add this File to Block list** specifies the file as a blocked file for the following reports:
            - All Undetermined Software Seen
            - Devices with Undetermined Software on Last Scan
        - **Restore this File from Quarantine** removes the file from quarantine and restores it to its original location.
        - **Initiate Cleanup on this Device** starts a scan immediately and quarantines any malicious files.
        - **Create Override** creates an Override for the URL.

- In the **Domain(s)** box, enter a comma-separated list of domains you want to create a rule for. The protocol (such as https or www) is not needed. For example, you can specify domain.com. Wildcards are supported (*.domain.com). This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History
- Select **Scope** (**MSP view** only) to specify if the rule should apply to all Sites that are configured to include global settings or just the selected Site. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History
- Select **Policy** (**MSP view** only) to associate this rule with a Policy and specify the Policy. If you do not specify a Policy, the Override will be associated with the Site. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History
- Select **Block/Allow** to specify if the domain should be blocked or allowed. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History
- When **Block Malicious URLs** is selected, malicious URLs (such as domains with known malware) are blocked regardless of a rule. This applies to the following reports:
  - Web Threat Shield Blocked URLs
  - Web Threat Shield Blocked URL History

Scheduled reports

Scheduled reports allow you to get in-depth information on your Sites at recurring intervals. Links to scheduled reports provided in emails are only valid for 48 hours. If you need to see a report past that time frame, see *Viewing scheduled report history* on page 72.

All scheduled reports must be created from an existing report template. For more information on how to create a report template, see *Creating a scheduled report template* on page 70.

Creating a scheduled report template

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

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

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

- Click **Add** to add a new scheduled report template.
- Click **Copy** to make a copy of an existing scheduled report template. Select the new template to make modifications.
- Click **Delete** to delete a scheduled report template. If you delete a template, you need to assign a replacement template.

To create a scheduled report template:

1. Click **Reports** and select the **Scheduled Templates** tab.
2. Click **Add**. The **Create Template** dialog is displayed.
    - **Name** is a unique name for the template.
    - **Title Page Text** is used for the title of the report generated by this template.
    - **File Format** provides options between PDF or CSV.
3. Construct your report template by choosing and placing the types of data you want to be included.
    - Click **Add Page** to add report types to the template. Use the drop-down menu to select specific report types for each page.
    - **Data Field** shows the type of data that is displayed.
    - From the **Chart Type** drop-down, if applicable, select what type of chart to use for the data.
    - From the **Time Period** drop-down, if applicable, select the time frame for the data.
    - Click **Delete Page** to remove the selected row from the template.
    - Use the **Up/Down** arrows to reorder the rows.
4. When done, click **Create**.

Scheduling a report

You must have an existing scheduled report template before you can create a new report to be scheduled. See *Creating a scheduled report template* on page 70.

To view your existing scheduled reports:

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

    - Click **Resume** to resume a suspended report. The report is generated and emailed at the interval specified in the scheduled report settings.
2. Click **Run Report Now** to immediately generate and send a scheduled report. You can change the **Creation Method** and **Recipients** for an immediate run; changes are not applied to the scheduled report template.

To schedule a report:

1. Click **Reports** and select the **Scheduled Reports** tab.
2. Click **Add**. The **Create Report** dialog box opens.
    - **Report Name** is a unique name for the report.
    - Select **Delivery Schedule** to specify when you want the report to be generated. Specify the time zone in UTC.
    - Select from the **Creation Method** drop-down to specify whether to create one report per Site, or one report for all Sites.
    - The **Recipients** options vary depending on your creation method.
        - If you have selected one single report creating data for all selected Sites, enter a comma-separated list of up to 25 email addresses.
        - If you have selected one report per Site, select from the following:
            - Select **Send to distribution list of each site** to use the report distribution list associated with each site.
                - In **Business view**, this report distribution list is specified on the **Settings** tab.
                - In **MSP view**, go to the **Sites List** tab, click the Site **Name** link, and then go to the **Details** tab.
            - Select **Send to email addresses provided below** to enter a comma-separated list of up to 25 email addresses.
            - Select **Send to both** to use both options above.
        - Select **Template** to specify which template to use for the report.
    - Select the **Sites** you want to generate the report for.
    - Select **Languages** to specify the default text of the report to be generated in. One report per selected language will be created.
3. Once the report is configured, click **Create**.

Viewing scheduled report history

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

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

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

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

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

Process Log

Process logging capabilities for Endpoint Protection enhance endpoint visibility for MSPs by exposing more endpoint event data and allowing for near real-time threat response.

In **Reports**, go to the **Process Log** tab to view a table with high-level information about endpoint events that were logged within a given timeframe.

To customize the processes shown in the Process Log table, you can:

- Click the **Process Log** drop-down list to filter for processes that either occurred for a specific Site or for all Sites.
- Use the calendar drop-down list to filter for processes that occurred within a specific date range.
- Click **Filters** to open the filter panel.
    - Expand each section to see available filters within each filter group.
    - A green circle with a number on the **Filters** button indicates the number of filters that are currently applied.
    - Select a file **Determination**.
    - To filter results for a specific **Process Name**, **Process Path**, or **Username**, type a partial or full value in the respective fields.
    - To filter results for a specific **MD5** or **SHA256** hash, type the full value in the respective fields.
    - Click **Reset** to manually clear any selections for a single filter group.
    - Click **Reset Filters** to clear all filters.
    - The filters that you apply will persist as you navigate to other pages within the Management Console until you manually reset them or log out.

To download the data found within the Process Log table as a .csv file, click **Export**. The exported report will only include the applied date range and filters.

You can also view detailed information about a specific process and create an override for it using process tree view. See *Using process tree view* on page 73 for more information.

Using process tree view

In the **Process Log** tab, you can drill down to the process tree to see a visual representation and detailed information about a specific process and its related events. You can also isolate or unisolate a device and create an override for the file determination. See topics *Creating a process override* on page 75 for more information.

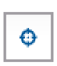
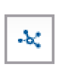
To view the specific details of a process:

- In the **Process Log** table, click a link in the **Process Name** column to drill down to the process tree view. The **Process Details** pane displays information about the process that you selected.

  Note: You can also click any related events within the process tree to view its details.

  - **Process Name** — The process name as identified by the device operating system.
  - **Determination** — The file determination value (Good, Undetermined, or Bad).
  - **Command args** — The command arguments passed to the process when it was executed.
  - **Elevation** — The elevation privilege of the running process (user, limited, admin, or system).
  - **MD5** — The MD5 hash of the file associated with the process.
  - **Normalized process path** — The normalized file path of the process.
  - **Parent process guid** — The unique GUID for the parent process data. This GUID tracks the process through its execution lifecycle.
  - **PID** — The ID assigned to the process by the device operating system upon execution.
  - **Process path** — The system path and filename of the file associated with the process.
  - **Timestamp** — The date and time associated with the receipt of the process execution event.
  - **Username** — The user or system account that executed the process.
  - **SHA256** — The SHA256 hash of the file associated with the process.

You can customize the process tree view in any of the following ways:

- Use your mouse or scroll wheel within the view area to drag, pan out, and zoom in.
- Choose any of the controls in the process tree navigation bar.
  - Click  to zoom in.
  - Click  to zoom out.
  - Click  to center the process tree within the view area.
  - Click  to reset the process tree to its default view.
  - Switch between different process tree views.
    - Horizontal view  aligns the process tree horizontally (default).
    - Vertical view  aligns the process tree vertically.
    - Polar view  displays all related processes stemming out from a central parent process.

Isolating and unisolating a device

Isolating a device blocks all internal and external network traffic to the device except for communication with the Management Console. This is useful when you want to disconnect a device that might be infected with malware from all networks and minimize the scope of the potential infection. You can also unisolate a device to restore it to all networks.

Note that to isolate or unisolate a device, it must be running PC Agent 9.0.36.40 or later, or Mac Agent 9.6.4 or later.

Best practices:

- To ensure that devices can be isolated and unisolated as quickly as possible, turn off the "Allow SecureAnywhere to be shut down manually" setting in your Policies. If Endpoint Protection is shut down on a device, the device cannot be isolated or unisolated until Endpoint Protection starts again.
- If you need to isolate a device, we recommend also disconnecting the device from any VPN. If a device might have malware, it should not be connected to a VPN.

To isolate a device:

1. In the process tree view, click **Isolate Device**.
2. The device will show that it is in **Pending Isolation** status, as denoted by a disabled button.
3. Once the Pending Isolation period is over, the device will show that it is **Isolated**.

To unisolate an isolated device:

1. In the process tree view, click **Unisolate Device**.
2. For a few moments, the device will show that it is in **Pending Unisolation** status.

Creating a process override

Overrides allow you to identify files and processes that should be allowed or blocked regardless of a Policy's rules.

To create an override for a file shown in the process tree:

1. In the process tree, click a process.
2. In the **Process Details** pane, click **Create Override**.
3. In the **Create Override** dialog box that opens, enter the following information:
    - Select one of the following **Allow/Block** options:
        - **Allow** - File Overrides allow a file to execute, regardless of the file's cloud classification.
        - **Block** - File Overrides block a file from executing, regardless of the file's cloud classification.
    - Select an Override **Type** to specify whether the file should be identified by its folder/file location or by its MD5 hash value.

- **Folder/File**
  - You cannot block based on folders/files; you can only allow folders/files.
  - In the **Folder** box, type an absolute file path or a file path using a system variable (such as %SystemDrive%) to be specified. Type % to see a list of supported variables.
  - In the **File** box, type a specific file name or a wildcard. If left blank, all files in the specified folder will be allowed.
  - Select the **Include Sub-Folders** check box to include subfolders of the specified path.
  - Select the **Detect if Malicious** check box to detect and remediate the file according to the assigned Policy. Monitoring and journaling are disabled. When this check box is cleared, the detect and remediate Policy settings do not apply to the file.

- In the **Name** box, type a name for the override.
- For **Scope**, click **Global** to specify that the rule should apply to all Sites that are configured to include Global settings, or click **Site** to include just the selected Site.
  - If you select **Site**, you can associate the override with a Policy, which can be applied to individual Sites, Groups, or devices.
- Select the **Associate with policy** check box to apply this override to a default or saved policy.

Deploying agents

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

The business products use two kinds of agents:

- **Endpoint Protection**
  - Cloud-based.
  - Once you install the agent you do not need to install or update any definition files.
  - When a new Endpoint Protection threat is identified, the agent is updated in the cloud for immediate protection of Endpoint Protection devices.
- **DNS Protection**
  - Only available when DNS Protection has been purchased.
  - The DNS Protection agent can be installed using the provided MSI or through an existing Endpoint Protection agent.
  - Can only be installed on Windows endpoints.
  - Mac endpoints can be protected through a DNS Protection protected network, either by using a VPN or on-site.
  - The DNS Protection agent will filter and manage DNS requests whenever access to the DNS Protection servers is available.
  - See *Installing the DNS Protection agent* on page 106.
- **Endpoint Detection and Response**
  - Only available when Endpoint Protection and Endpoint Detection and Response have been purchased.
  - See *Installing the Endpoint Detection and Response agent* on page 94.
- **Managed Detection and Response**
  - Only available when Managed Detection and Response has been purchased.
  - See *Installing the Managed Detection and Response agent* on page 96.

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

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

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

Installing Endpoint Protection on Windows or macOS using the installation wizard

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

1. Locate the agent installation download links in the Management Console.
   - If you are using **Business view**:
     a. Go to **Settings > Downloads** to see the installation file download links.
     b. Click the **Download** link under the operating system used by the target device.
   - If you are using **MSP view**:
     a. Click **Sites List**.
     b. Find your Site in the list and click the name.
     c. Open the **Endpoint Protection** tab.
     d. Click the **Download Windows .exe, Download Windows (.msi)**, or **Download Mac** link to download the appropriate file for the target device.
2. Copy the **Keycode** for your company or for the Site for future reference
3. Move the installation file to the device you are installing the agent on.
4. Install the agent.

   Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this knowledge base article for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.

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

If DNS Protection is enabled, the DNS Protection agent will install through the Endpoint Protection agent.

Installing Endpoint Protection on Windows or macOS from the command line

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

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

- If you are using **MSP view**:
    - Click **Sites List**.
    - Find your Site in the list and click the name.
    - Open the **Endpoint Protection** tab.

2. Select the Windows download link to download the file.
3. Install the agent using any of the command options that correspond to your device. Unless otherwise noted, these options are for Windows machines.
    - `/key=keycode` or `-keycode =` (mac) installs the agent software using the specified keycode, with or without hyphens.
    - `/silent` or `-silent` (mac) installs the agent in the background with no on-screen interaction.
    - `/nostart` installs the agent, but does not start it.
    - `/lockautouninstall=password` installs the agent without adding it to the Windows Control Panel programs list. You can silently uninstall later using the specified password. When you use `/lockautouninstall`, Endpoint Protection is not included in the **Add/Remove Programs** list in the Control Panel. Use the `/exeshowaddremove` command to include Endpoint Protection in **Add/Remove Programs**.
    - `/autouninstall=password` uninstalls the agent using the password specified with `/lockautouninstall`. By default, Endpoint Protection does not display in the **Add/Remove Programs** list in the Control Panel, which prevents the user from removing the software in unmanaged mode.
    - `-clone` enables you to assign a unique ID to the machine when the agent is installed on a device that does not have a unique host name due to cloning. The unique ID will be included in the host name to better identify this machine.
    - `-uniquedevice` enables you to assign a unique ID to the machine when the agent is installed on a device that does not have a unique machine ID, but does have a unique host name. The host name will be used to identify this machine.
    - `/exeshowaddremove` includes the agent software in the Windows Control Panel programs list. End-users will be able to uninstall the agent software when it is in unmanaged mode.
    - `/group=groupcode` assigns the device to the specified Group during the agent installation. The Group must already exist in the Management Console and the machine must not have had the agent software previously installed.
    - `/proxyhost=IPaddress` or `-proxy_host=` (mac) causes the specified proxy server to be used during the agent installation.

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

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

- `/proxyport=portnumber` or `-proxy_port=` (mac) causes the specified port number to be used for the proxy server.
- `/proxyuser=name` or `-proxy_user=` (mac) causes the specified user name to be used for the proxy server.
- `/proxypass=password` or `-proxy_pass=` (mac) causes the specified password to be used for the proxy server.
- `/proxyauth=authtype` or `-proxy_auth=` (mac) causes one of the following authentication types to be used for the proxy server:
  - `0`—Search through all authentication types. This option may take longer and may cause unnecessary errors on the proxy server.
  - `1`—Use basic authentication.
  - `2`—Use digest authentication.
  - `3`—Use negotiate authentication.
  - `4`—Use NTLM authentication.
- `/lang=languagecode` or `-language=` (mac) installs the agent using one of the following language codes.
  - `de`—German
  - `en`—English
  - `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

Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this knowledge base article for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.

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

If DNS Protection is enabled, the DNS Protection agent will install through the Endpoint Protection agent.

Installing Endpoint Protection on Windows using Msiexec

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

To install the Endpoint Protection agent on Windows using Msiexec:

1. Locate the agent installation download links in the Management Console.
   - If you are using **Business view**:
     a. Go to **Settings > Downloads** to see the installation file download links.
     b. Click the **Download** link under the operating system used by the target device.
   - If you are using **MSP view**:
     a. Click **Sites List**.
     b. Find your Site in the list and click the name.
     c. Open the **Endpoint Protection** tab.
2. Download the `.msi` file.
3. Use the following syntax to use Msiexec with Endpoint Protection. Substitute your keycode, with or without hyphens, for keycode in GUILIC.

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

   You can also specify `ARPNOREMOVE` in your command to prevent end-users from uninstalling Endpoint Protection.

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

If DNS Protection is enabled, the DNS Protection agent will install through the Endpoint Protection agent.

Installing Endpoint Protection on Windows using Group Policy

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

To install the Endpoint Protection agent on Windows using a Group Policy:

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

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

If DNS Protection is enabled, the DNS Protection agent will install through the Endpoint Protection agent.

Installing the Endpoint Protection agent using scripts

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

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

Alerts and alert distribution lists

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

Managing alerts and alert distribution lists

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

- Select a scope from the drop-down menu to view and manage results shown in the **Alerts** table as follows:
    - Global alerts apply to all Sites that you have access to.
    - Under the **Sites** list, select a specific Site to view and manage alerts that are associated with it.
- Click **Add** on either tab to add an alert or an alert distribution list.
- Click **Delete** on either tab to delete the selected alert or the alert distribution list.
    - If you delete a distribution list that has alerts assigned to it, you must replace it with a distribution list of the same scope.
- Click **Suspend** to suspend the selected alert. No emails are sent to the alert distribution list when the alert criteria is met.
- Click **Resume** to resume the selected alert. Emails are sent to the alert distribution list when the alert criteria is met.

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

Adding an alert

To add an alert:

1. Click **Alerts** and open the **Alert List** tab.
2. Click **Add**.
3. In the first step of the **Create Alert** wizard, configure the basic settings of the alert.
    - Click **Name** to specify a unique name for the alert.
    - Click **Alert type** to select the type of alert you want to create.
4. Click **Next** to continue.
5. In the second step of the **Create Alert** wizard, select the Sites that should use this alert.
    - Select scope
        - **Global** allows the alert to be created for multiple Sites.
        - **Site** allows the alert to be created for a specific Site.

- Select Sites
    - **All sites** configures all Sites for this alert.
    - **Selected sites** enables you to select specific Sites for this alert.

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

Adding an alert distribution list

To add an alert distribution list:

1. Click **Alerts** and open the **Distribution Lists** tab.
2. Click **Add**.
3. Select the scope.
    - **Global** allows the distribution list to be created for multiple Sites.
    - **Site** allows the distribution list to be created for a specific Site.
4. Configure the alert distribution list.
    - Click Name to specify a unique name for the alert.
    - In the **Email Addresses** box, specify a comma-separated list of up to 25 addresses to receive the alert notification email.
5. Click **Create** to create the alert distribution list.

Administration tasks

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

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

If you are using **MSP view**, you can also use user accounts to control access to Sites.

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

Viewing available administrators

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

- Super administrators and limited administrators are listed on the **Admins** tab.
- Site-only administrators (**MSP view** only) are listed on the **Site Only Admins** tab.
    - You can no longer add or edit administrators on the **Site Only Admins** tab. Instead, we recommend that you manage administrators using the **Admins** tab.

The following controls are available to manage administrators. You may not be able to perform some of these actions depending on the access granted to your user account or which tab you are on.

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

Adding an administrator

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

- **First Name** is the user’s first name.
- **Last Name** is the user's last name.
- **Email** is the user's email address. This is what the user will use to log in.
- **Phone** (optional) is the user's phone number.
- **Time Zone** is the user's time zone.
- **Account Type** determines the type of access you want to grant to this user for the Management Console.

Management Console Component	Super Admin	Limited Admin
Sites Lists (**MSP view** only)	Based on Site permissions	X
Dashboard	X	X
Entities	X	
Overrides	X	X
DNS Protection	X	
Security Awareness Training	X	
Reports	X	
Alerts	X	
Admins	X	View only
Settings	X	X

3. If you are in **Business view**, click **Save** to add the administrator.
4. If you are in **MSP view**, click **Next** to continue to assign site administrator permissions.
5. Select the Sites this administrator should have access to.
   - **Admin** has full access to the Site.
   - **View Only** has view-only access to the Site.
   - **No Access** denies access to the Site. The user cannot see the Site listed on the **Sites List** page.
6. Click **Save** to add the administrator.

Editing an administrator

To edit an administrator:

1. Go to the **Admins** page.
2. Click the admin **Name** link. The settings for the selected administrator are displayed.
3. Modify the settings on the **Details** or **Site Permissions** (**MSP view** only) tabs as needed.
4. When done, click **Save**.

Deleting an administrator

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

To delete an administrator:

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

Settings

The **Settings** tab contains various configuration sections. The available configurations vary if you are using the **Business view** or the **MSP view**.

Business view settings

The **Endpoint** tab includes general Site or company information.

- **Site / Company Name** is a unique name for the Site or company.
- **Keycode** is a read-only field that displays the keycode assigned to the Site or company. If the keycode is a trial, the number of days remaining in the trial period are also displayed. This is the keycode that is used in Endpoint Protection installations. This keycode is also on the **Downloads** tab.
- **Company Size** is a range that represents the size of the company.
- **Company Industry** should be the industry that best represents the company.
- **Comments** (optional) is any information that describes the Site or company.
- **Site Seats** are the number of endpoints for the Site you are configuring. This setting is not used for billing.
- **Default Endpoint Policy** is used for all new Endpoint Protection agents installed for this Site unless the Policy is assigned using inheritance from the Group, Site, or company. You can modify the Policy the device uses after installation. It is recommended that you create a copy of this Policy and modify it according to Policy best practices and your specific needs.
  -
    - **Recommended Defaults** is intended for desktops and laptops.
    - **Recommended DNS Enabled**, like **Recommended Defaults**, is intended for desktops and laptops. It will also automatically install the DNS Protection agent.
    - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit** allows for transparent use of Endpoint Protection. It reports on what is found, but does not remediate infections. It is designed to as a testing Policy to help minimize production impact. Webroot recommends using this Policy only for a short duration, such as during initial setup, to identify potential production false positives and conflicts, and to uncover unknown software.
    - The **Unmanaged** Policy designed to allow a user to edit their settings from the agent user interface. It inherits the previously applied Policy and its settings, but does not have any specific settings other than whether to show the user interface.
      - Intended for technical support, troubleshooting, and when no Policy management is needed.
      - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.

        - Should not be used in production.
    - Policies with the prefix **Legacy** contain previously recommended Policy settings.
- In the **Report Distribution** List, specify a comma-separated list of up to ten email addresses to receive the generated reports.

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

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

- The **Site / Company Name** is the company name used to define the console. Click **Rename** to edit the console name.
- The **Company Address** is specified for you when your account is created. If you need to modify the address, contact Webroot.
- **Contact Email** is the email of the primary account for the selected console. If you need to modify the email, contact Webroot.
- **Contact Phone** is specified for you when your account is created. If you need to modify the phone number, contact Webroot.
- **Parent Keycode** is the keycode assigned to the selected console. Do not use this keycode for installations. You should use the keycode assigned to the Site (found on the **Endpoint** tab) for installations. Click **Renew/Upgrade** to update your subscription.
- **View Usage** opens a separate console where you can view your usage for the previous year. Click **My Usage**, log in when prompted, and, if prompted, select a console. Once logged in, you will have tabs for usage and billing.
    - In the **My Usage** tab, the report shows a rolling 30 day total from the date selected on the **My Usage** page.
        - Export the usage data by clicking the **Download CSV** link.
        - Drill down to see Site usage by clicking the **Site Usage** button; you can also export the usage data for that Site.
- **Pay Invoices** opens a separate console where you can view your billing history. Click **My Billing**, log in when prompted, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.
    - In the **My Billing** tab, online payment features are available if you are paying Webroot directly. If you are paying a service provider or third party, the online payment features will not be available.
        - From the billing page, select an account. If needed, create an account following the on-screen instructions and then verify the email that you receive.
        - Review your invoices and if desired, you can make a payment.
        - You can also set up AutoPay to have your billing automatically paid using a saved credit card. Follow the on-screen instructions for saving the credit card information. If you want to discontinue AutoPay, contact wrAccountsReceivable@opentext.com or your sales representative.

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

The **Downloads** tab contains links for the Windows and macOS agent installations. It also contains a copy of the keycode that is built in and applied to the installation. Use these installation files to manually install on a device. See *Deploying agents* on page 77.

The **Web Block Page Settings** tab allows you to customize the notification page that is displayed when websites are blocked by DNS Protection or the Web Threat Shield.

- Drag and drop a logo to the dotted box if you want your own logo to appear on the notification page. You can also click the dotted box and select the logo.
  - The logo file name extensions must be either `.png`, `.gif`, or `.jpeg`.
  - The maximum height of the logo is 50 pixels.
  - The width will be adjusted automatically to maintain the aspect ratio of the logo.
  - The file size limit is 1 MB.
  - When a logo is added, the Webroot logo changes to “powered by Webroot.”
  - To remove a logo that you have uploaded, hover over the dotted box and click **Delete current image**. The powered by Webroot logo changes back to the standard Webroot logo.
- The **Website not allowed** text and graphics below the logo and above the formatting toolbar automatically appear on the notification page. The text and graphics cannot be modified or deleted.
- Enter **Additional information** into the free form field below the formatting bar.
  - You can modify or delete this text.
  - Enter a maximum of 500 characters.
- Click **Reset to Default Settings** to reset the logo and additional information back to the default settings.

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

- This is a REST API that you can use to automate access to Webroot services and information, such as billing, reporting, and so on.
- To get started, click **Create New Client Credential**. Follow the 3-step process, then acknowledge that you have made note of the client secret. You will need to use the client ID and client secret in order to authenticate with the API to access information or take action.
- You can also enable Notification API, which allows you to receive near real-time Unity API Notifications based on a set of events that you can subscribe to on different domain levels.
- You can create up to 20 unique client credentials. Once you have created at least one client credential, you can manage its Unity API settings from the Unity API Access table. From there, the following actions are available:
  - **New**—Opens the **Create New Client Credential** dialog box.
  - **Edit**—Opens the **Edit Client Credential** dialog box, which allows you to modify the selected client credential name, description, and purpose for using the Unity API. You can enable or disable API notifications in Step 2 by answering "Do you plan to use the

event notification API?" with either Yes or No.

  - **Delete—**Deletes the selected client credential record.
  - **Renew Secret**—Renews the client credential secret for the selected credential. This will expire the previously set secret and revoke any future requests attempted using this credential with the old secret.
  - **Suspend**—Temporarily revokes a client's API Access. To re-enable access for the selected client credential, click **Resume**.

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

- Click **Edit** to set or remove a filter, and to see the history of data filter changes. Data filters enable you to limit the data is that is displayed in the console. Narrowing your filters may improve page loading performance, depending on how much data is being loaded, but it will limit what you see. When you apply or clear filters, it may take a few minutes to update the data depending on the amount the deployment size and the amount of data to display.
- Click **Convert** if you want to change to **Managed Service Provider view**. This allows you to have multiple Sites, such as companies, business, organizational units, and so on, in the Management Console. Each Site will have separate keycodes and billing. Selecting the service provider option is not reversible.

Managed Service Provider view settings

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

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

- The **Site / Company Name** is the company name used to define the console. Click **Rename** to edit the console name.
- The **Company Address** is specified for you when your account is created. If you need to modify the address, contact Webroot.
- **Contact Email** is the email of the primary account for the selected console. If you need to modify the email, contact Webroot.
- **Contact Phone** is specified for you when your account is created. If you need to modify the phone number, contact Webroot.
- **Parent Keycode** is the keycode assigned to the selected console. Do not use this keycode for installations. You should use the keycode assigned to the Site (found on the **Endpoint** tab) for installations. Click **Renew/Upgrade** to update your subscription.
- **View Usage** opens a separate console where you can view your usage for the previous year. Click **My Usage**, log in when prompted, and, if prompted, select a console. Once logged in, you will have tabs for usage and billing.
  - In the **My Usage** tab, the report shows a rolling 30 day total from the date selected on the **My Usage** page.

    - Export the usage data by clicking the **Download CSV** link.
    - Drill down to see Site usage by clicking the **Site Usage** button; you can also export the usage data for that Site.
- **Pay Invoices** opens a separate console where you can view your billing history. Click **My Billing**, log in when prompted, and, if prompted, selected a console. Once logged in, you will have tabs for usage and billing.
  - In the **My Billing** tab, online payment features are available if you are paying Webroot directly. If you are paying a service provider or third party, the online payment features will not be available.
    - From the billing page, select an account. If needed, create an account following the on-screen instructions and then verify the email that you receive.
    - Review your invoices and if desired, you can make a payment.
    - You can also set up AutoPay to have your billing automatically paid using a saved credit card. Follow the on-screen instructions for saving the credit card information. If you want to discontinue AutoPay, contact wrAccountsReceivable@opentext.com or your sales representative.
- In the **Login Settings** section, you can change your **password**, change your **security questions**, **enable 2FA**, and change your **security code**.

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

The **Web Block Page Settings** tab allows you to customize the notification page that is displayed when websites are blocked by DNS Protection or the Web Threat Shield.

- Drag and drop a logo to the dotted box if you want your own logo to appear on the notification page. You can also click the dotted box and select the logo.
  - The logo file name extensions must be either `.png`, `.gif`, or `.jpeg`.
  - The maximum height of the logo is 50 pixels.
  - The width will be adjusted automatically to maintain the aspect ratio of the logo.
  - The file size limit is 1 MB.
  - When a logo is added, the Webroot logo changes to “powered by Webroot.”
  - To remove a logo that you have uploaded, hover over the dotted box and click **Delete current image**. The powered by Webroot logo changes back to the standard Webroot logo.
- The **Website not allowed** text and graphics below the logo and above the formatting toolbar automatically appear on the notification page. The text and graphics cannot be modified or deleted.
- Enter **Additional information** into the free form field below the formatting bar.
  - You can modify or delete this text.
  - Enter a maximum of 500 characters.

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

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

- This is a REST API that you can use to automate access to Webroot services and information, such as billing, reporting, and so on.
- To get started, click **Create New Client Credential**. Follow the 3-step process, then acknowledge that you have made note of the client secret. You will need to use the client ID and client secret in order to authenticate with the API to access information or take action.
- You can also enable Notification API, which allows you to receive near real-time Unity API Notifications based on a set of events that you can subscribe to on different domain levels.
- You can create up to 20 unique client credentials. Once you have created at least one client credential, you can manage its Unity API settings from the Unity API Access table. From there, the following actions are available:
    - **New**—Opens the **Create New Client Credential** dialog box.
    - **Edit**—Opens the **Edit Client Credential** dialog box, which allows you to modify the selected client credential name, description, and purpose for using the Unity API. You can enable or disable API notifications in Step 2 by answering "Do you plan to use the event notification API?" with either Yes or No.
    - **Delete—**Deletes the selected client credential record.
    - **Renew Secret—**Renews the client credential secret for the selected credential. This will expire the previously set secret and revoke any future requests attempted using this credential with the old secret.
    - **Suspend—**Temporarily revokes a client's API Access. To re-enable access for the selected client credential, click **Resume**.

Endpoint Detection and Response

Endpoint Detection and Response is a powerful security solution offering advanced threat detection and rapid response. It continuously monitors endpoints to identify and neutralize threats in real time, including zero-day and advanced attacks that evade traditional defences.

When Endpoint Detection and Response is enabled under **Settings**, select **Detection and Response** in the navigation pane to access all features.

Enabling Endpoint Detection and Response

Before enabling Endpoint Detection and Response, you must enable and configure Endpoint Protection. See *Getting started* on page 11.

To enable Endpoint Detection and Response:

1. In the navigation pane, click the **Settings** tab.
2. In the **Subscriptions** tab, activate a trial to Endpoint Detection and Response.
3. Enable Endpoint Detection and Response for the desired Site.
    - If you are using the **Managed Service Provider view**, in the navigation pane, click the **Sites List** tab. Then, select a Site that you want to enable Endpoint Detection and Response on, and click the **Endpoint Protection** tab.
4. Enable **Endpoint Detection and Response** using the slider control.
5. If required, select your keycode type.
    - **Trial** provides the full product, limited to a free, 30-day trial.
6. To deploy Endpoint Detection and Response, see *Installing the Endpoint Detection and Response agent* on page 94.

Installing the Endpoint Detection and Response agent

To deploy Endpoint Detection and Response on a device, the device must have Endpoint Protection installed and it must belong to a site with Endpoint Detection and Response enabled. By default, when Endpoint Detection and Response is enabled for a site, all devices on that site will have Endpoint Detection and Response installed when Endpoint Protection is installed.

Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this [knowledge base article]() for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.

Note: To use Detection and Response products on an M-Series Mac device, you must have Rosetta installed.

On Windows devices, if you have custom policies set that prevent automatic installation of Endpoint Detection and Response with Endpoint Protection, you can choose to enable Endpoint Detection and

Response by assigning an Endpoint Protection policy with the "Install EDR / MDR Agent" setting enabled.

To enable the "Install EDR / MDR Agent" setting:

Note: Currently, enabling or disabling Endpoint Detection and Responseusing an Endpoint Protection policy is only available for Windows devices.

1. In the navigation pane, go to Manage > Policies.
2. From the Endpoint Protection tab, select the Policy associated with devices that you want to install the EDR agent on. This Policy can be edited (excluding System Policies) to install the EDR agent.

   Note: System Policies (excluding the Unmanaged Policy) will have **Install EDR / MDR Agent** set to **On** by default.
3. Scroll down to **Policy Settings**. In the **EDR / MDR** section, select **On** beside **Install EDR / MDR Agent**.
4. In the **Policy Usage** section, you can identify which systems will be affected.
5. Click **Save**.

The next time Entities using this Policy check in, the Endpoint Detection and Response agent will be installed.

You can also choose to disable Endpoint Detection and Response for devices within a Site by assigning a custom policy to those devices with the "Install EDR / MDR Agent" setting disabled. Endpoint Detection and Response will remain enabled on any devices that do not have a custom policy disabling Endpoint Detection and Response.

Managed Detection and Response

Managed Detection and Response delivers automation-powered, continuous endpoint and network protection with advanced threat intelligence and expert incident response. The platform features real-time monitoring, integrated SIEM and SOAR capabilities, and seamless deployment, securing SMBs with 24/7/365 protection. OpenText MDR reduces false positives and ensures fast, reliable remediation of threats.

When Managed Detection and Response is enabled under **Settings**, select **Detection and Response** in the navigation pane to access all features.

Enabling Managed Detection and Response

To enable Managed Detection and Response:

1. In the navigation pane, click the **Settings** tab.
2. In the **Subscriptions** tab, activate a trial to Managed Detection and Response.
3. Enable Managed Detection and Response for the desired Site.
    - If you are using the **Managed Service Provider view**, in the navigation pane, click the **Sites List** tab. Then, select a Site that you want to enable Managed Detection and Response on, and click the **Endpoint Protection** tab.
4. Enable **Managed Detection and Response** using the slider control.
5. If required, select your keycode type.
    - **Trial** provides the full product, limited to a free, 30-day trial.
6. To deploy Managed Detection and Response, see *Installing the Managed Detection and Response agent* on page 96.

Installing the Managed Detection and Response agent

By default, when Managed Detection and Response is enabled for a site, all devices on that site will have Managed Detection and Response installed when Endpoint Protection is installed. If you intend to use Managed Detection and Response without an Endpoint Protection subscription, or if you have custom policies set that prevent automatic installation of Managed Detection and Response with Endpoint Protection, you can install it using one of two methods depending on your operating system.

Note: A system extension is installed with Mac Agent version 9.6.4 or later. This system extension is required for securely isolating a device from the network. See *Isolating and unisolating a device* on page 75. If you silently install the Mac Agent using mobile device management (MDM), see this knowledge base article for configuration file requirements that prevent content filter and system extension dialog boxes from appearing to your customers. If you silently uninstall the Mac Agent, the system extension remains on the device.

Note: To use Detection and Response products on an M-Series Mac device, you must have Rosetta installed.

To deploy Managed Detection and Response using Endpoint Protection:

Note: Currently, enabling or disabling Managed Detection and Response using an Endpoint Protection policy is only available for Windows devices.

1. In the navigation pane, go to Manage > Policies.
2. From the Endpoint Protection tab, select the Policy associated with devices that you want to install the MDR agent on. This Policy can be edited (excluding System Policies) to install the MDR agent.

   Note: System Policies (excluding the Unmanaged Policy) will have **Install EDR / MDR Agent** set to **On** by default.
3. Scroll down to **Policy Settings**. In the **EDR / MDR** section, select **On** beside **Install EDR / MDR Agent**.
4. In the **Policy Usage** section, you can identify which systems will be affected.
5. Click **Save**.

The next time Entities using this Policy check in with the console, Managed Detection and Response will be enabled.

You can also choose to disable Managed Detection and Response for devices within a Site by assigning a custom policy to those devices with the "Install EDR / MDR Agent" setting disabled. Managed Detection and Response will remain enabled on any devices that do not have a custom policy disabling Managed Detection and Response.

To deploy Managed Detection and Response without Endpoint Protection:

1. In MSP view, select the desired Site.
2. Go to the Endpoint Protection tab. Ensure Managed Detection and Response is enabled. For additional instructions, see *Enabling Managed Detection and Response* on page 96.
3. Follow the instructions shown within the console to install the Managed Detection and Response agent.

DNS Protection

DNS Protection is a DNS filtering service that can be used to protect an individual device through an agent, as well as a service that can protect all devices on the network by forwarding DNS requests to the DNS resolvers.

When DNS Protection is enabled under **Settings**, your Management Console will include some tabs and settings that are specific to DNS Protection and would otherwise not be displayed.

Getting started with DNS Protection

1. Register with the Management Console. See *Getting started* on page 11.
2. Enable and configure DNS Protection. See *Enabling and configuring DNS Protection* on page 98.
3. Ensure the endpoints are covered by **DNS Protection**.
    - Deploy the DNS Protection agent. See *Configuring the network* on page 109.
    - Protect the network. See *Configuring the network* on page 109

Enabling and configuring DNS Protection

Before you can deploy the DNS Protection agent, it must be enabled in the Management Console.

To enable and configure DNS Protection:

1. In the navigation pane, click the **Settings** tab.
2. In the **Subscriptions** tab, activate a trial or enable a subscription to DNS Protection.
3. Enable DNS Protection for the desired Site.
    - If you are using the **Managed Service Provider view**, in the navigation pane, click the **Sites List** tab. Then, select the Site that you want to enable DNS Protection on and click the **DNS Protection** tab.
    - If you are configured for the **Business view**, in the navigation pane, click the **DNS Protection** tab.
4. Enable **DNS Protection** using the slider control.
5. If required, select your keycode type.
    - **Full** provides the full product with no limitations. You will be billed for this service.
    - **Trial** provides the full product, limited to a free, 30-day trial.
6. Under **Agent Settings**, select a default DNS Site Policy. Whenever a new agent is installed, this Policy is assigned by default.
    - **DNS High Protection** is the recommended starting Policy. It blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - **DNS Medium Protection** provides the same security as **DNS High Protection**, but does not block Questionable/Legal content.

- Custom Policies are also easily created. See *Managing DNS Protection Policies* on page 100.

7. Under **Agent Settings**, the **Domain Bypass** setting is provided to domains that need to be looked up by the local DNS resolvers, such as Active Directory domains.
   - Domains entered in the list are resolved by the local DNS resolver and are not filtered.
   - To avoid any possible resolution issues, we recommend that you add any Active Directory domains in use.
   - Wildcards can be used to include any Subdomains, such as *.webroot.com.
   - The **Domain Bypass List** only applies to the DNS Protection agent.
8. Under **Network Settings**, you can enter details to protect all devices on the network, such as guest or IoT devices, even if no agent is installed.
   - **Static IP**: Identify the public IPv4 address used for internet access (WAN IP).
   - **Dynamic IP**: If a static IP address is not available, a domain associated with Dynamic DNS service can be entered. Once a domain is entered, the current corresponding IP address will be displayed beside the **Domain / IP Address** box.
   - Select a Policy to associate with the IP address. Any DNS requests received from this IP address are resolved based on this Policy.
   - Select **Add Network** to complete adding the IP address for this network. Note that this change will not take effect until you click **Save**.
   - If you need to add multiple networks or circuits, add the additional **Domains / IP Addresses**, then click **Add Network**.
9. Under **DNS Resolver Lookup**, use the Network Location menu to identify the best DNS resolvers for your region. Note that this is not a setting, but rather a mechanism to identify the most appropriate resolvers.
   - Select the correct Network Location for the Site on which you have enabled DNS Protection.
   - The best primary and secondary DNS servers are shown.
   - Once you have identified the best resolvers, these IP addresses can be used as your DNS Forwarders (AD) of the DNS servers in your router.
   - We strongly recommend testing DNS resolution to these servers before changing the configuration of your network. For example, nslookup can be used: `nslookup www.webroot.com 35.226.80.229`. If the server does not respond, verify the IP address entered in step 8 before updating your network configuration.
10. Under **Advanced Settings**, select whether the agent can be enabled on servers.
    - When checked, the DNS Protection agent will enable and try to filter on servers.
    - This is not typically recommended as the DNS Protection agent will conflict with Azure servers or with other services providing DNS resolution.
    - To protect DNS servers, we recommend that you use network filtering by registering the network and adding the resolvers as DNS Forwarders, as described in steps 8 and 9.

- If you selected the **Enable Agent on Servers** check box, the DNS Protection agent will enable and filter on RDS / Terminal Service servers, as well as other servers without the DNS role.

11. When done, click **Save**.

Managing DNS Protection Policies

To review or modify DNS Protection Policies:

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

   The **Policies** page is divided into several sections:

   - **Privacy Settings** control user privacy settings and the information that is logged.
     - **Hide User Information** improves privacy by replacing the user name and the domain requested with the word Hidden in the logs. If requests are made in the Security Risk category, the domain is still logged for visibility.
     - **Local Echo** echoes DNS requests made by the DNS Protection Agent to the local network's DNS resolver, providing visibility to these requests for your firewall or DNS server. To improve privacy, a DNS resolver can be specified, and requests will only be echoed when it is available.
     - **Fail Open** avoids a possible DNS interruption if the DNS resolvers are unavailable by deferring DNS resolution to the local resolver or returning without filtering.
   - **Leak Prevention** blocks alternate sources of DNS resolution, helping to ensure that all DNS requests are filtered and logged. This feature requires Agent version 4.2 or newer and is only supported on Windows 10 and newer.
     - **Standard DNS Requests** – When enabled, communication over port 53 TCP and UDP is blocked.
     - **DoH Requests** – When enabled, communication over port 443 TCP is blocked to known DoH providers.
     - **DoT Requests** – When enabled, communication over port 853 TCP is blocked.
     - **Exclusions** – Use this field to enter IP addresses of DNS servers to which communication should not be blocked. Any IP entered will not be blocked by DNS Leak Prevention for **Standard DNS Requests**, **DoH Requests**, and **DoT requests**.
   - **Security Settings** specify whether to block or allow certain domains.
     - **Keyloggers and Monitoring**: Domains that include downloads and discussions for software agents that track keystrokes or web surfing habits.
     - **Malware Sites**: Domains that are known to contain malicious content including executables, drive-by infection sites, malicious scripts, viruses, or Trojans.
     - **Phishing and Other Frauds**: Domains that are known to pose as reputable sites, usually to harvest personal information from a user. These sites are typically quite

short-lived, so examples don’t last long.

    - **Proxy Avoidance and Anonymizers**: Domains that use proxy servers or other methods to bypass filtering or monitoring.
    - **Spyware and Adware**: Domains that are known to contain spyware or adware that provides or promotes information gathering or tracking that is unknown to or without the explicit consent of the user. This Policy also includes sites that contain unsolicited advertising pop-ups and programs that may be installed on users' computers.
    - **Bot Nets**: Domains 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**: Domains contained in spam messages.
- **Content Settings** includes categories to control available content.
    - **Human Resources Protections**
        - **Abused Drugs**: Domains associated with illegal, illicit, or abused drugs, including legal highs, glue sniffing, misuse of prescription drugs, or abuse of other legal substances.
        - **Adult and Pornography**: Domains that contain sexually explicit material for the purpose of arousing sexual interest, including domains with adult products such as sex toys and videos. This category also includes online groups domains that are sexually explicit, sites with erotic stories or textual descriptions of sexual acts, sites for adult services such as video conferencing, escort services, and strip clubs, and sites with sexually explicit art.
        - **Dating**: Domains that focus on establishing personal relationships.
        - **Sex Education**: Domains that depict information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control and contraceptives, tips for better sex, and products used for sexual enhancement.
        - **Swimsuits & Intimate Apparel**: Domains that show swimsuits, intimate apparel, or other types of suggestive clothing.
        - **Gross**: Domains that show blood or bodily functions, such as vomit.
        - **Nudity**: Domains that contain nude or semi-nude depictions of the human body, that may not be sexual in intent but may include things like nudist or naturist sites, nude paintings, or photo galleries of artistic nature.
        - **Alcohol and Tobacco**: Domains that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.
    - **Questionable/Legal**

- **Cult and Occult**: Domains that provide methods, means of instruction, or other resources that attempt to affect or influence real events using astrology (including horoscopes), spells, curses, magic powers, or supernatural beings.
- **Gambling**: Domains that use real or virtual money; domains 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 domains that do not enable gambling on the domain are categorized as Lifestyle, Travel or General Information, Local information.
- **Marijuana**:Domains that depict marijuana use, cultivation, history, culture, or legal issues.
- **Hacking**: Domains that depict illegal or questionable access to or the use of communications equipment/software or domains for the development and distribution of programs that may compromise networks and systems, including domains that avoid licensing and feeds for computer programs and other systems.
- **Weapons**: Domains that provide sales reviews and descriptions of weapons such as guns, knives, or martial arts devices, including domains that provide information on accessories or other modifications.
- **Pay to Surf**: Domains that pay users in the form of cash or prizes for clicking on reading specific links in emails or webpages.
- **Questionable**: Domains that manipulate the browser user experience or client in some unusual, unexpected, or suspicious manner. Also includes get rich quick domains.
- **Hate and Racism**: Domains that support hate crime or racist content or language.
- **Violence**: Domains that advocate violence, violent depictions, or methods, including game/comic violence and suicide.
- **Cheating**: Domains that support cheating and contain materials such as free essays, exam copies, and plagiarism.
- **Illegal**: Domains that depict criminal activity including how not to get caught and copyright and intellectual property violations.
- **Abortion**: Domains that depict abortion, either pro-life or pro-choice.

- **Social Media/internet Communication**
  - **Social Networking**: Domains that have user communities where users interact, post messages, pictures, and otherwise communicate.
  - **Personal Sites and Blogs**: Domains that have posted content by individuals or groups, including blogs.
  - **Online Greeting Cards**: Domains that offer e-cards.

- **Search Engines**: Domains that use key words or phrases and return results that include text, websites, images, videos, and files.
- **Internet Portals**: Domains that aggregate a broader set of internet content and topics.
- **Web Advertisement**: Domains that contain advertisements, media content, and banners.
- **Web based email**: Domains offering web-based email and email clients.
- **Internet Communications**: Domains offering internet telephony, messaging, VoIP services, WiFi, and related businesses.
- **Dynamically Generated Content**: Domains that generate content dynamically based on arguments passed to the URL or other information, such as geo-location.
- **Parked Domains**: Domains that host limited content or click-through ads that may generate revenue for the hosting entity, but generally do not contain content useful to the user.
- **Private IP Addresses and URLs**: Domains that are assigned to a private domain and IP addresses reserved by organizations that distribute IP addresses for private networks.

- **Shopping**
  - **Auctions**: Domains that support the offering and purchasing of goods between individuals as their main purpose, excluding classified advertisements.
  - **Shopping**: Domains for department stores, retail stores, company catalogs and other entities that allow online consumer or business shopping and the purchase of goods and services.
  - **Shareware and Freeware**: Domains that enable downloading free software, open source code, or downloads that request a donation, including screen savers, icons, wallpapers, utilities, and ringtones.
- **Entertainment**
  - **Entertainment and Arts**: Domains 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**: Domains for sales, delivery, or streaming of audio or video content, including domains that provide downloads for such viewers.
  - **Peer to Peer**: Domains that provide peer-to-peer clients and access, including torrents and music download programs.
  - **Games**: Domains that are for game playing or downloading, video games, computer games, electronic games, tips and advice on games or how to

obtain cheat codes. Also includes domains dedicated to selling board games, journals and magazines dedicated to game playing, support or host online sweepstakes and giveaways, and fantasy sports domains that also host games or game playing.

  - **Music**: Domains that are for music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business.

- **Lifestyle**
  - **Travel**: Domains that are for airlines and flight booking agencies, travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
  - **Home and Garden**: Domains that are about home issues and products, such as maintenance, home safety, decor, cooking, gardening, home electronics, and design.
  - **Religion**: Domains that are about conventional or unconventional religious or quasi-religious subjects, including churches, synagogues, or other houses of worship.
  - **Hunting and Fishing**: Domains that are about sport hunting, gun clubs, and fishing.
  - **Society**: Domains that cover a variety of topics, groups, and associations relevant to the general populace, and broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups.
  - **Sports**: Domains that are team or conference websites, international, national, college, professional scores and schedules, sports-related online magazines or newsletters.
  - **Fashion and Beauty**: Domains that show fashion or glamor, magazines, beauty, clothes, cosmetics, and style.
  - **Recreation and Hobbies**: Domains with information, associations, forums, and publications on recreational pastimes such as collecting kit airplanes; outdoor activities such as hiking, camping, and climbing; specific arts, craft, or techniques; animal and pet related information, training, shows, techniques, and humane societies.

- **Business/Government/Services**
  - **Real Estate**: Domains 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**: Domains related to computer and internet security and security discussion groups.
  - **Financial Services**: Domains offering banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies, excluding domains that offer market information, brokerage or trading services.

    - **Business and Economy**: Domains for business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship.
    - **Computer and Internet Info**: Domains containing general computer and internet information, including technical information. Also includes software as a service (SaaS) domains and other domains that deliver internet services.
    - **Military**: Domains for the military branches, armed services, and military history.
    - **Individual Stock Advice and Tools**: Domains that promote or facilitate securities trading and management of investment assets, including market information on financial investment strategies, quotes, and news.
    - **Training and Tools**: Domains for distance education and trade schools, online courses, vocational training, software training, and skills training.
    - **Personal Storage** are sites that provide online storage and posting of files, music, pictures, and other data.
    - **Government**: Domains that are related to government (local, county, state, and national), government agencies, and government services such as taxation, public, and emergency services. Also includes domains that discuss or explain laws of various governmental entities.
    - **Content Delivery Networks**: Domains that are for the delivery of content and data for third parties, including ads, media, files, images, and videos.
    - **Motor Vehicles**: Domains that are 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**: Domains that offer free or paid hosting services for webpages and information concerning their development, publication, and promotion of websites.
- **General Information**
    - **Legal**: Domains related to legal topics and law firms as well as domains for discussions and analysis of legal issues.
    - **Local Information**: Domains for city guides and tourist information, including restaurants, area/regional information, and local points of interest.
    - **Job Search**: Domains that help find employment, tools for locating prospective employers, employers looking for employees, and career search and career placement from schools.
    - **Translation**: Domains that refer to language translation sites that allow users to see pages in other languages. These domains 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**: Domains for personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogs, genealogy, and scientific information.
        - **Philosophy and Political Advocacy**: Domains for politics, philosophy, discussions, promotion of a particular viewpoint or stance to further a cause.
        - **Educational Institutions**: Domains for pre-school, elementary, secondary, high school, college, university, and vocational school, and other educational content and information, including enrollment, tuition, and syllabus.
        - **Kids**: Domains that are designed specifically for children and teenagers.
        - **News and Media**: Domains with current events or contemporary issues of the day, including radio stations, magazines, newspapers, headline news domains, newswire services, personalized news services, and weather related domains.
        - **Health and Medicine**: Domains for general health, fitness, well-being, including traditional and non-traditional methods and topics. Also includes domains 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**: Domains that provide photo and image searches, online photo albums, digital photo exchange, and image hosting.
    - **Uncategorized Domains**: Domains that have not categorized in any of the above categories.
- **Additional filtering**. Many search engines provide the option to impose a filter that restricts explicit, adult, or inappropriate content. This can be done through DNS by returning the corresponding IP address associated with the filter.
    - When **Enable Google SafeSearch** is selected, DNS requests for www.google.com are resolved to forcesafesearch.google.com to filter explicit content from the search results.
    - When **Enable DuckDuckGo Safe Search** is selected, DNS requests for www.duckduckgo.com are resolved to safe.duckduckgo.com to filter adult content from the search results.
    - When **Enable Bing SafeSearch** is selected, DNS requests for www.bing.com are resolved to strict.bing.com to filter inappropriate content from the search results.
    - When **Enable YouTube Restricted Mode I Moderate Mode** is selected, DNS requests for www.youtube.com are resolved to restrictmoderate.youtube.com.
    - When **Strict Mode** is selected, DNS requests for www.youtube.com are resolved to restrict.youtube.com.

Installing the DNS Protection agent

There are two available options to install the DNS Protection agent:

- Download and install the MSI. This is used in the instance when the DNS Protection agent will be used without Endpoint Protection. The provided MSI will add an Entity to the Management Console, which you can then configure and manage. See *Installing the DNS Protection agent through the MSI* on page 107.
- Install through Endpoint Protection. Use this method when the DNS Protection agent will be used in conjunction with Endpoint Protection. See *Installing the DNS Protection agent through Endpoint Protection* on page 107.

Installing the DNS Protection agent through the MSI

To install the DNS Protection agent through the MSI:

1. In the Management Console, go to the **DNS Protection** tab.
   - Ensure that DNS Protection is enabled. See *Enabling and configuring DNS Protection* on page 98.
   - If you are using the **Managed Service Provider view**, in the navigation pane, click the **Sites List** tab. Then, select the Site that you want to enable DNS Protection on and click the **DNS Protection** tab.
   - If you are configured for the **Business view**, in the navigation pane, click the **DNS Protection** tab.
2. On the **DNS Protection** tab, in the **Installing the DNS Protection Agent** box, click the **Deploying the Agent with the MSI** link.
3. Run the MSI.
   - If the MSI is run directly on a system, you will be prompted for a keycode. Enter the keycode found in the **Installing the DNS Protection Agent** box, which corresponds to the Site that you want to install DNS Protection on.
   - The MSI can also be launched by command line, script, or through Active Directory. Use the keycode found in the **Installing the DNS Protection Agent** box. It must be written as follows, with `keycode=` for the agent to install successfully:

     ```
     Msiexec /i wrdnsp.msi /quiet keycode=xxxx-xxxx-xxxx-xxxx-xxxx
     ```

Due to restrictions with MSIs, it is not recommended to rename the MSI from `wrdnsp.msi`.

A restart is not required after installation.

Installing the DNS Protection agent through Endpoint Protection

In instances where both Endpoint Protection and DNS Protection will be used, the DNS Protection agent should be installed through Endpoint Protection. If the MSI is used on systems already running Endpoint Protection, or if Endpoint Protection is added to a system already running DNS Protection, Endpoint Protection will manage the DNS Protection agent per its configuration.

To deploy the DNS Protection agent using an Endpoint Protection Policy:

1. In the navigation pane, go to **Manage > Policies**.
2. From the **Endpoint Protection** tab, select the Policy that uses the Entities that you want to install the DNS Protection agent on.
    - We recommend that you make a copy of this Policy. Once editing is complete, this new Policy can be applied to the Entities that you want to install the DNS Protection agent on.
    - Alternatively, this Policy can be edited (excluding System Policies) to install the DNS Protection agent. In the **Policy Usage** section, you can identify which systems will be affected.
3. In the **DNS Protection** section, turn **Install DNS Protection** to **On**.
4. Click **Save**.

This new Policy can now be applied as default, to Groups, and individual Entities.

The next time Entities using this Policy check in, the DNS Protection agent is installed.

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

- The DNS Protection agent will validate the keycode as well as the associated DNS Protection license.
- The agent will automatically update to the most recent available version.
- A new service called “Webroot DNS Protection Agent” is created and started.
- When the service starts, the DNS settings for the active network adapter are identified for internal DNS resolution, such as Active Directory.
- The service then sets the network adapter DNS settings (both IPv4 and IPv6) to loopback addresses (127.0.0.1 and ::1), so that DNS requests are redirected to the agent.
- All external DNS requests are sent via DoH (DNS over HTTPS) to the DNS resolvers for fast, filtered resolution.
- All Active Directory and local DNS requests are resolved by the previously identified DNS resolvers for the active network adapter.
- While the DNS Protection agent service is running, any network adapter DNS changes are promptly reverted to loopback.
- If the service is stopped or the agent is uninstalled, the network adapter DNS settings are returned to their original settings.

DNS Protection agents will uninstall in the following situations:

- If you are using a trial of DNS Protection in conjunction with Endpoint Protection and it expires, the DNS Protection agent is automatically uninstalled the next time the device checks in.
- If the Endpoint Protection Policy is changed to no longer install DNS Protection, DNS Protection is automatically uninstalled the next time the device checks in.
- If an Uninstall Agent Command is sent to any device running DNS Protection.
- If the DNS Protection agent is uninstalled from **Add/Remove Programs**. Note that if the agent was installed by the Endpoint Protection agent, it will automatically be reinstalled.
- If a Site is deactivated, the DNS Protection agent will automatically uninstall.

DNS Protection agents will stop filtering and managing DNS requests if the DNS Protection agent was installed directly with the MSI (not through Endpoint Protection) and the license or trial expires. The DNS Protection agent will then return the DNS settings to their original values and will only resume filtering once the license is validated again. Note that the **Uninstall** Agent Command will remove the DNS Protection agent from the Entity.

Providing DNS Protection over a network

By registering the IP address or domain associated with the network and configuring your router and DNS forwarders, DNS Protection can protect all devices on the network, even those not running the DNS Protection agent. It allows you to control DNS on any network, including Wi-Fi and guest networks, while also providing protection for devices connecting through VPNs.

Configuring the network

To configure the network for DNS Protection:

1. In the Management Console, go to the **DNS Protection** tab.
    - If you are using the **Managed Service Provider view**, in the navigation pane, click the **Sites List** tab. Then, select the Site that you want to enable DNS Protection on and click the **DNS Protection** tab.
    - If you are configured for the **Business view**, in the navigation pane, click the **DNS Protection** tab.
2. In the **Network Settings** section, type the **Domain / IP Address** of a network that you want to protect.
    - **Static IP**: Type the public IPv4 address used for internet access (WAN IP).
    - **Dynamic IP**: If a static IP address is not available, you can type a domain associated with Dynamic DNS service. Once you type a domain, the current corresponding IP address appears in the **Domain / IP Address** box.
    - Select a Policy to associate with the IP address. Any DNS requests received from this IP address are resolved based on this Policy.
    - Click **Add Network** to complete adding the IP address for this network. Note that this change will not take effect until you click **Save**.
    - If you want to add multiple networks or circuits, type the additional **Domains / IP Addresses**, then click **Add Network**.
3. In the **DNS Resolver Lookup** section, select a network location from the **Network Location** list to identify the best DNS resolvers for your region. Note that this is not a setting, but rather a mechanism to identify the most appropriate resolvers.
    - Select the correct Network Location for the Site on which you have enabled DNS Protection. The best primary and secondary DNS servers are displayed.
    - Once you have identified the best resolvers, these IP addresses can be used as the DNS Forwarders (AD) of the DNS servers in your router.
    - We recommend testing DNS resolution to these servers before changing the configuration of your network. For example, you can use `nslookup`:

```
nslookup www.webroot.com 35.226.80.229
```

- If the server does not respond, verify your IP address before updating your router of DNS forwarders.

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

Installing network certificates and licenses

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

To correctly display the Block Page when a blocked domain is encountered, we recomend installing the Webroot certificates to the Trusted Root Authorities Certificate Store (typically `..\Certificates - Current User\Trusted Root Certification Authorities\Certificates`).

Note that this is not required when using the DNS Protection agent.

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

- Certificate Installer:

  https://download.webroot.com/DNS/certinstaller.exe

- Certificates:

  https://download.webroot.com/DNS/certificates/webroot-certificate.p7b

  https://download.webroot.com/DNS/certificates/webroot-certificate.pem

Overrides for DNS Protection

Overrides allow you to identify files and domains that should be allowed or blocked regardless of a Policy or the category of a domain.

In **MSP view**, Global file Overrides are applied to all Sites that have **Include Global Overrides** enabled in the Site **Details** tab (recommended).

Note that Site Overrides will always take precedence over Global Overrides.

Policy Overrides will always take precedence over Site Overrides.

Changes in Overrides replicate within 15 minutes of being applied.

To access DNS Overrides, go to **Manage > Overrides** and select the **Web Overrides** tab.

Allowing and blocking domains for DNS Protection

If you are not using **DNS Protection**, the **Web Overrides** will apply to the Endpoint Protection feature Web Threat Shield and only the allowed functionality will have an effect.

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

DNS Protection reports

In the navigation pane, click **Reports** to see all reporting options.

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

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

Security Awareness Training

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

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

Consider the following when designing and running campaigns:

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

Getting started with Security Awareness Training

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

To get started with Security Awareness Training:

1. Register and set up **Endpoint Protection**. You do not need to deploy agents to use **Security Awareness Training**. See *Getting started* on page 11.
2. Enable and configure **Security Awareness Training**. See *Enabling Security Awareness Training* on page 112.
3. Target users for training. See *Targeting users for training* on page 113.

Enabling Security Awareness Training

To enable Security Awareness Training:

1. Go to **Security Awareness Training**.
    - In **Business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
    - In **MSP view**, click **Sites List** in the navigation pane, open the Site, and then open the **Security Awareness Training** tab.
2. Turn on the **Security Awareness Training** switch.
3. If required, select your keycode type.
    - **Full** indicates a keycode that enables full use of the product with no limitations. You will be billed for this service.
    - **Trial** indicates a keycode that enables full use of the product, limited to a free, 30-day trial.
4. Click **Save**.

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

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

To configure Security Awareness Training settings:

- In **Business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
- In **MSP view**, click **Sites List** in the navigation pane, open the Site, and then open the **Security Awareness Training** tab.

Targeting users for training

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

To target users for training:

1. Go to the settings for Security Awareness Training.
    - In **Business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
    - In **MSP view**, click **Sites List** in the navigation pane, open the Site, and then open the **Security Awareness Training** tab.
2. Configure the domain to use to target your users.
    1. In **Business view**, use the options on the **Security Awareness Training > Settings** tab.
    2. In **MSP view**, click **Sites List** in the navigation pane, open the Site, then open the **Security Awareness Training** tab.

3. You can either configure the domain automatically, using Active Directory Integration, or manually, using Domain Verification.

    - **Active Directory Integration** synchronizes with Azure Active Directory to identify the domain. It also synchronizes a list of users in the domain that you can target for security training. See the Knowledge Base.

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

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

        - In the **Add New Domain** box, enter an email address.

            - If the email you enter is a **Domain Member**, campaigns can be created and run, but the breach report is not accessible.

            - If the email you enter is a system level **Domain Admin** (i.e., administrator, info, postmaster, root, system, or webmaster), campaigns can be created and run, and the breach report is accessible.

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

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

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

        - Select a Site (**MSP view** only)

        - Click **Add Users to Site**.

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

            - **Set up Active Directory** integration synchronizes using Azure Active Directory. See the Knowledge Base.

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

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

                - **LDIF** indicates an `.ldif` file exported from LDAP/Active Directory. The following fields will be used to add users for training:

                    - **givenname** (required) populates as the user's first name.

                    - **sn** (required) populates as the user's last name.

                    - **mail** (required) populates as the user's email address.

- **objectGUID** (optional) populates as the user's unique ID.
- **Ou** (optional) are organizational units that populate as tags.

Managing users

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

To manage users:

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

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

Creating and managing distribution lists

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

To create and manage a distribution list:

1. Click **Security Awareness Training** in the navigation pane and open the **Users** tab.
2. Click the Site you want to work with (**MSP view** only). This Site should already be enabled for Security Awareness Training and have at least one user assigned.
3. Click the **Create Distribution List** button to create a new Security Awareness Training distribution list.
    - **Distribution List Name** specifies a name for the Security Awareness Training distribution list.
    - The **Company** list displays the available users. Click a user in this list to move it to the **Distribution List Members** list.
    - Use the **Search** boxes to narrow either list to only those users that meet the search criteria. Click the x to clear the search criteria.
    - Click **Add All** to add all of the users in the company list to the **Distribution List Members** list. If you have applied a search filter, only the entries showing in the **Company** list will be added.
    - The **Distribution List Members** list displays all users to be included in the distribution list. The list being displayed shows all users in the list, regardless of any search filtering. To remove a user, click a user name and move it back to the company name list.
    - Click **Remove All** to remove all items from the **Distribution List Members** list and move them back to the company name list.
    - Click **Save** to save the new Security Awareness Training distribution list.

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

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

Creating a new campaign

Before you begin, make sure your email server does not block the phishing simulation and training emails sent to your users. In addition, you must have Admin permissions on at least one site to create campaigns.

1. Click **Security Awareness Training** on the navigation pane, and make sure the **Campaigns** tab is selected.
2. Click **New Campaign**. The New Campaign dialog is displayed.
3. Build the campaign in Section 1.
    - **Campaign Name** specifies a descriptive name for the campaign. This is only viewable by admins.
    - Select **Campaign Type** to specify the type of campaign to create.

    - **Training** is a campaign that will educate users using learning content and report on how many users completed the training. Selecting training provides a way to specify an optional title of the training campaign and an optional message on the landing page.

      Phishing is an email-based phishing simulation that will test and report on how many users clicked the phishing link. Users who click on the phishing link can be automatically enrolled in a previously configured Training Remediation Campaign.

    - **Training Remediation** is used to automatically enroll users into training if they fail phishing simulation campaigns. Training Remediation campaigns are maintained separately from Phishing campaigns so you can re-use them across phishing campaigns.

- For all campaign types, email templates can be customized. Click the **Customize Template** link to customize how the email will be delivered and displayed. Your intent for these fields will vary depending on if you are customizing an email for phishing or training. For example, for phishing you want the information to appear legitimate so that users are tested. For training, you want the information to appear legitimate so that users will not think it is phishing and delete the training invitation.
    - **Sender Name** is the name of the person, alias, group, or organization you want the email to be from.
    - **Sender Address** is the address that you want the email to be from.
    - **Email Subject** is the subject line of the email.
    - **Email Body** is the body of the email. You can customize any email template by editing the template image or linking to your own custom image.
        - In accordance with our terms and conditions, you must comply with all relevant copyright and usage terms to use custom images in your campaign. Consider the following when adding images into your customized email template:
            - The image address must be a valid URL hosted on the internet.
            - The URL must be publicly accessible in a web browser.
            - The image must not be hotlink-protected.
            - The image must be available to be embedded in third-party websites.
    - Click **Save As New** to create a new template based on your customizations
    - Click **Apply Edits** to modify the template you are customizing.
- For Phishing campaigns:
    - Select **Email Template** to specify a template for your emails. You can filter the thumbnails displayed by entering search text or selecting a category filter.
    - Click **Landing Page URL** to select a domain. This is the URL the user will be sent to from the phishing email. You can customize the URL with a subdomain to make it more relevant to the phishing email or your users.

- In the **Landing Page** section, select what you want to display when the **Landing Page URL** is clicked.
  - **Infographic** displays a web-based training page. It provides immediate education to users that they have clicked on a phishing simulation. This choice alerts users that a simulation is in progress.
    1. **Select Infographic Template** enables you to choose the infographic to be displayed.
    2. Click **Customize Template** if you want to modify the body of the infographic page.
  - **Broken Link** displays a 404 type of error page. This choice does not provide any immediate education. It tests users without alerting them that a simulation is in progress.
    1. **404 Type** enables you to choose the type of broken link error to be displayed.
  - **Lure Page** takes users to a web page and extends the simulation by testing to see if they will enter information. If users enter information, they will be redirected to a web-based training page. That page provides immediate education to users that they have clicked on a phishing simulation. If users make it this far, it alerts them that a simulation is in progress.
    1. Select **Lure Page Template** enables you to choose the lure page to be displayed.
    2. Click **Customize Template** to modify the body of the lure page.
    3. **Destination Upon Posting Data** enables you to select an infographic to be displayed if the user enters information on the lure page.
    4. Click **Customize Template** to modify the body of the infographic page.

- For Training and Training Remediation campaigns:
  - Specify **Landing Page Content** to control your end user experience when they click through on the training invite email which they will receive upon enrollment into the campaign.
  - **Select Email Template** provides thumbnails from which to select a training invitation email template. These templates are fully customizable.
  - **Select Training Courses** enables you to elect up to 10 courses per training campaign by scrolling through the thumbnails or filtering by course name using the **Search by name** box. You can also select a language for the training campaign and specify the display order on the landing page by dragging the courses to different positions in the selection list.

4. Select the Sites and Permissions for the campaign in Section 2. Click the heading to expand it.
   - Phishing and Training Campaign types require at least one site to be selected to be validated for launch. Unlike other campaign types, the Training Remediation campaign is

designed to be re-used across phishing campaigns as defined by its permission settings. A Training Remediation campaign can be set to Global or non-Global.

    - **Global Training Remediation Campaigns** will accept enrollments from phishing campaigns for all current and future sites on the console. *Note*: This option does not require specific site selection and is only available to Super Admin users.
    - **Non-Global Training Remediation Campaigns** require at least one site to be selected before they can be launched. Once launched, they will only accept enrollments from phishing campaigns for the selected sites.

- The **Select Sites** section lists the available Sites. It does not include expired Sites, Sites without any users, or Sites for which the current Administrator lacks sufficient permissions. Click a Site in this list to move it to the **Sites Selected** list. *Note*: If you are building a Global Training Remediation Campaign, this selector will not be visible as the campaign will accept enrollment from all sites.
    - Use the **Search** box to narrow either list to only those Sites that meet the search criteria. Click the x to clear the search criteria.
    - Clicking **Show Distribution Lists** shows all available Security Awareness Training distribution lists. A distribution list only sends the campaign to those users in list, rather than all users in a Site.
    - Click **Add All** to add all of the Sites and distribution lists currently displayed in the **Select Sites** list to the **Sites Selected** list. If you have applied a search filter or are not showing Security Awareness Training distribution lists, only the entries showing in the **Select Sites** list are added.
- The **Sites Selected** section lists all the Sites and Security Awareness Training distribution lists to 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.
- Click **Remove All** to remove all items from the **Sites Selected** list and move them back to the **Select Sites** list.
- The **Add Users to Training Remediation Campaign** setting is available when creating a Phishing Campaign. Selecting this option will display available Global and non-Global Training Remediation campaigns subject to the current user’s permission settings. Select a Training Remediation campaign for users to be enrolled into if they fail the phishing campaign simulation.

5. Schedule the campaign in the next section. Select the section to expand it.

   Note: Training Remediation campaigns do not require Auto-Enrollment, Launch Date, Duration, or Delivery Time.

   - Select **Auto-Enrollment** to automatically add new users to this campaign when they are added to the Site or distribution list selected for the campaign. If the campaign is still active, the new users will receive the campaign.
       - **Launch Date** specifies the date you want the campaign to start, If you are automatically enrolling users.
   - **Duration** is dependent on your Auto-Enrollment setting.

    - If you are automatically enrolling users, select the length of time enrolled users remain in the campaign. The campaign ends at 11:59 pm on the last day. If you select **Indefinitely**, the user remains enrolled in the campaign until the campaign is manually ended.
    - If you are not automatically enrolling users, select how long you want the campaign to run. If you do not set an end date, the campaign never expires, unless you manually end the campaign. If you set an end date, the campaign ends at 11:59pm on the last day.
  - **Delivery Time** is the time you want the campaign emails to be sent. Campaign scheduling times are specified according to the local computer time zone setting. For example, if your computer is using Eastern time and you select 10:00am, the time will automatically be adjusted to 7:00am when viewing on a computer using Pacific time.
    - **Deliver emails at time of launch** specifies that all the emails are sent as soon as the campaign starts.
    - **Deliver emails at custom time** sends all of the emails at the specified time.
    - **Spread email delivery out over period of days** spreads the delivery of the emails over the specified number of days.
  - Select **After the campaign ends, send Campaign Summary Report automatically** to automatically send a Campaign Summary report after the campaign has ended.
6. Review the campaign in the final section. Click the section to expand it. This section allows you to review the campaign configuration. Any campaign configuration settings that are incomplete are identified. In this section, you can also enter a single email address and click **Send Preview**. Repeat for multiple email addresses. Each email address receives a preview of what the campaign looks like and how it functions.
7. Click one of the following buttons.
  - **Cancel** exits the campaign creation without saving.
  - **Save & Close** exits the campaign and saves the campaign settings that you configured. The campaign remains in draft status and will not launch, even when the specified launch date is reached.
  - **Launch Campaign** exits the campaign, saves the campaign settings that you configured, and starts the campaign when the specified launch date is reached. If the launch date is immediate, the campaign launches immediately.

Enabling Autopilot

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

To enroll users in SAT Autopilot:

1. In the **Security Awareness Training** section of the Management Console, click the **Autopilot** tab.
2. To familiarize yourself with the program, click **View Autopilot Campaign Schedule**.
3. Turn on the **Autopilot** switch.

4. (Optional) Enter a single email address to automatically send the Campaign Summary Report to when each campaign ends. Note that the message will contain a link to a single zip file that includes individual reports for each Site enrolled in the campaign.
5. Select Sites or distribution lists that you want to enroll into Autopilot campaigns.
6. Click **Save**.

To disable Autopilot campaigns:

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

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

Viewing and managing available campaigns

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

You are not limited to viewing only your own campaigns. Depending on your Admin Account Type and Site Permissions, you can see, edit, and launch draft campaigns created by other administrators.

The following controls are available on the **Campaign Management** table:

- Enter text in the **Search** box to narrow the list to only those rows that contain the search text. The search checks the entire table, not just the visible rows.
- If you have Admin Site Permissions for at least one site, you can click **New Campaign** to create a new campaign. See *Creating a new campaign* on page 116.
- Click **Filters** to open and close the filter panel. Select one or more filters to apply.
- To **sort** a column, click the column heading.
- Click the campaign **Name** link of an active, scheduled, or completed campaign to view the summary report for that campaign.
- Click the **Site** name link to go to the legacy **Security Awareness Training** console. This is an older console that will be phased out in the future.
- Under **Actions**, you can perform the following functions based on your Admin Account Type and Site Permissions:
  - **End Campaign** immediately ends a campaign. Users who attempt to access a campaign after it has ended will see a diagnostic message.
  - **Send Reminder Now** immediately sends an email reminder to users who have not completed the training campaign.
  - **Edit Campaign** allows you to edit a campaign. This option is only available for draft campaigns.

- **Archive Campaign** keeps a campaign that is completed and no longer active. You can review archived campaigns.
- **Delete Campaign** deletes a draft campaign. You cannot review deleted campaigns.
- **Copy Campaign** creates a copy of a campaign. Your Site Permissions determine if a full or partial campaign copy is created.

- At the bottom of the **Campaign Management** table, rows and paging controls allow you to view more or less on a page and move between pages of the table.

Viewing available training courses

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

The available training courses are categorized by tabs. Within a tab, you see the courses for that category including the course name, description, and length. Click on a training course to see how the course is graded and who the course publisher is. From the detailed course view, you can click **Preview Course** to experience the course yourself. If you have Admin Site Permissions to at least one site, you can click **Add to Campaign** to create a new campaign with the selected training course.

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

Viewing a campaign summary report

If your campaign has not yet launched, its status will be **Scheduled**. While the campaign is in **Scheduled** status, no data is generated. However, you can click the campaign **Name** link to view the campaign settings.

Once your campaign has generated activity, you can view its campaign summary report. Go to the **Security Awareness Training** tab and click the campaign **Name** link to view its summary report. The report is divided into sections as follows:

- The top section contains high-level information about the campaign, including the launch, duration, and enrolled users.
- When Training Remediation campaign is in use, the top section will also display a linked campaign section to indicate remediation relationships and allow easy cross-referencing of results across the linked campaigns.
- For multi-site campaigns, the summary report will show a table containing a list of the sites included in the campaign along with key metrics. To view each site's individual report, click **Delivery Report**.
- The summary report view for individual sites displays **Results** in either **Sankey** or **Bar Graph** format, depending on which selection you choose. Below the chart are detailed results for each targeted user.
    - **Sankey** is the best option for evaluating more in-depth information about the campaign as the diagram shows all events logged for each user. The height of the dark vertical bar

for each bucket represents the total number of users that have logged that type of event. Only one instance of an event is logged for each user, even if that user clicks the link multiple times. For more information about campaign events, see *Interpreting campaign events* on page 123.

    - **Bar Graph** is the best option for providing a quick reference as the chart only displays the most recent priority event logged for each user.

- Below the data visualization graph, the Detailed Results table shows the most recent event and remediation status (if using Training Remediation) for active users in the campaign.
- On multi-site and single-site summary views, the content used by the campaign will be displayed in the final section.
    - **Email used** is the email used for the campaign.
    - **Landing page** (phishing campaigns only) displays any lure, infographic, or broken link specified for the campaign.
    - **Training courses** (training campaigns only) displays any courses specified for the campaign.
- Click **Export PDF** or **Export CSV** to download the summary report in that file format. The CSV file provides additional detailed activity data such as email delivery codes.

Interpreting campaign events

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

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

with a hybrid phishing campaign lure page (if enabled).

- **Campaign Complete –** The target user has successfully completed all activities assigned in a single campaign.

The remaining campaign events are mapped and tallied as follows:

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

Security Awareness Training reports

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

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

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