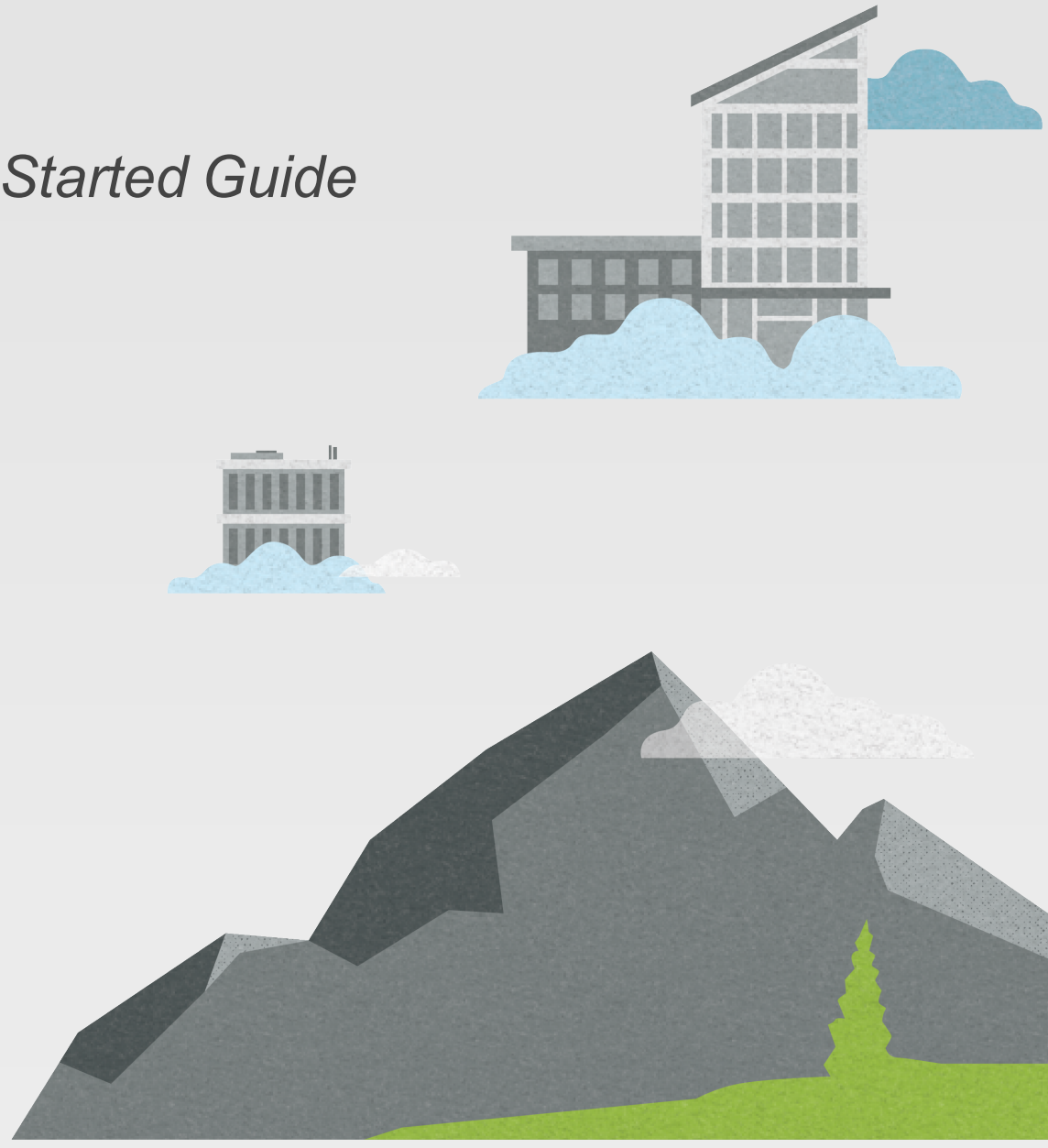
WEBROOT®
an opentext™ company

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

*Getting Started Guide*



## Notices

Webroot Business Products Getting Started Guide revision Friday, July 29, 2022

Information in this document is for the following products:

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

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

# Contents

# Overview

This Getting Started guide details how to get up and running with the Webroot Endpoint Protection, Webroot DNS Protection, and Webroot Security Awareness Training business products.

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

- **Webroot Endpoint Protection** is designed to help keep businesses and their customers safe from viruses, ransomware, phishing, malware, and other cyberattacks. You must install and configure Endpoint Protection before you can use either **DNS Protection** or **Security Awareness Training**.
- **Webroot DNS Protection** is a domain filtering service that uses DNS to provide internet usage restrictions both independently and across a network. This product works in conjunction with Webroot Endpoint Protection and is purchased separately. See DNS Protection in the Webroot Endpoint Protection Administration Guide.
- **Security Awareness Training** is a hosted program designed to increase understanding and practical implementation of security best practices. The program includes a phishing simulator, training courses, and other tools. This product works in conjunction with Webroot Endpoint Protection and is purchased separately. See Security Awareness Training in the Webroot Business Products Administration Guide.

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

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

For detailed information about Endpoint Protection and functionality common to all products, see the Webroot Business Products Administration Guide.

# Requirements

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

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

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

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

For specific firewall configuration settings, see the Knowledge Base.

**Security Awareness Training** requirements include:

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

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

# Getting started with Endpoint Protection

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

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

**Endpoint Protection:**

- Step 1 – **Register** a trial or **purchase** your Webroot business product. You should have completed this step before receiving this guide.
    - See *Purchasing or registering for a trial* on page 7 in the Webroot Business Products Administration Guide.
- Step 2 – Configure Endpoint Protection by creating and activating your Webroot account, setting up two-factor authentication (if desired), and selecting your Management Console view.
    - See *Creating and activating your account* on page 7 in the Webroot Business Products Administration Guide.
    - See *Setting up two-factor authentication (2FA)* on page 9 in the Webroot Business Products Administration Guide.
    - See *Selecting your Management Console view* on page 8 in the Webroot Business Products Administration Guide.
    - See *Creating a site (MSPs only)* on page 10 in the Webroot Business Products Administration Guide.
- Step 3 - Deploy the Endpoint Protection agents to devices. Install an agent on each computer you want protected; the agent then registers and reports endpoint activity through the Management Console. Managed service providers also need to set up at least one site.
    - *Deploying agents to devices* on page 14 in the Webroot Business Products Administration Guide.

**DNS Protection:**

- Complete Steps 1 – 3 above to register, configure, and deploy Endpoint Protection.
- Enable and install DNS Protection.
    - See *Enabling and configuring DNS Protection* on page 17 in the Webroot Business Products Administration Guide.
    - See *Installing network certificates and licenses* on page 20 in the Webroot Business Products Administration Guide.

**Security Awareness Training:**

- Complete Steps 1 – 2 above to register and configure Endpoint Protection.
- Enable Security Awareness Training and target users.

- See *Enabling Security Awareness Training* on page 27
- See *Targeting users for training* on page 28.

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

# Step 1: Register/Purchase

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

## Purchasing or registering for a trial

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

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

# Step 2: Setup

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

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

## Creating and activating your account

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

1. Open the email.
2. Click the registration link.
3. Use the temporary password from the email on the registration page.
4. Complete the remainder of the form.
    - Password
        - Case sensitive
        - Must contain 6 letters and 3 numbers

        - Special characters are allowed (except for < and >)
        - Cannot be longer than 32 characters
    - Security code
        - A word or number to be used as an extra security step after you enter your password
        - You are asked to enter two random characters from this code so something easy to remember is recommended
        - Case sensitive
        - Minimum of six characters
        - Cannot be sequential (i.e., 1 2 3 4 5 6)
        - Cannot be a common word

## Selecting your Management Console view

The Management Console has two configuration options:

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

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

**To select your Management Console view:**

1. Log in to your Management Console at https://my.webrootanywhere.com.
2. If this is your first time accessing the console, you are prompted to select a view.
    - Selecting **Business** sets up a Management Console as a single site, which focuses only on one company's security.
        - All devices and billing use a single keycode.
        - You can use **groups** to organize your devices.
        - This view can be changed to the managed **service provider view** later.
    - Selecting **Managed Service Provider** sets up a Management Console where you can manage multiple sites for the companies that pay you to provide their cybersecurity.
        - Sites can represent businesses, departments, regions, office locations, or other organizational units under your management.
        - Separate billing and keycodes are available for each site.
        - This view cannot be changed to **business view**.
3. Click **Select** for your preferred view.
4. If you selected **Business**, fill out your company information.

- **Site / Company Name** is a unique name for the site or company.
- **Number of Devices** is the number of devices to be managed.
- **Company Industry** is the industry that the company works within.
- **Company Size** is the range of numbers that represents the size of the company.

5. When done, click **Select**.

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

**To change your console view from business view to service provider view:**

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

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

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

Setting up 2FA is optional but highly recommended.

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

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

- If verification fails, enter a new code from your authenticator app. Codes are valid for 30 seconds.

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

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

If you are setting up a **business** console, go to *Step 3: Deploy* on page 13.

If you are a **managed service provider**, go to *Creating a site (MSPs only)* on page 10 next.

## Creating a site (MSPs only)

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

**To create a site:**

1. Click **Sites List** and then click **Add Site**. The **Add Site** wizard opens.
2. Complete the site **Details**.
    - **Site / Company Name** is a unique name for the site or company.
    - **Site Type**
        - **External Company** is an external company that purchases services from you.
        - **Internal Site** is a site within your own company, such as a location or office.
    - **Company Size** (external companies only) is the range of numbers that represents the size of the company.
    - **Company Industry** (external companies only) is the industry that the company works within.
    - **Billing Cycle** (external companies only) is the billing cycle you define and use as needed for this site (as opposed to the billing cycle associated with Webroot).
    - **Billing Date** (external companies only) is the month and date for billing, designed and used as needed for this site (as opposed to the billing date associated with Webroot).
    - **Distribution List** is a comma-separated list of up to ten email addresses that receive scheduled reports. When scheduling a new report, select **Send to distribution list of each site** so all associated email addresses receive it.
    - **Include Global Policies**
        - When enabled, all global policies are available for this site.
        - If a global policy is in use and changes, each device using the policy gets the change.
        - Once enabled, this option cannot be changed.
        - When disabled, global policies are not available, and site level policies are used.
    - **Include Global Overrides**

        - When enabled, global policy overrides are applied to this site. For example, if a site has blocked a particular file and configured it to be a global override, all sites with this option enabled use that override and block that file.
        - When this option is disabled, global overrides from other sites are not applied to this site, and all overrides for this site must be manually configured.
        - Once enabled, this option cannot be changed.
    - **Comments** (optional) are comments describing the site or company.
    - **Tags** (optional) are useful labels for filtering your searches.
3. Click **Next** to continue.
4. In the **Admin Permissions** step, select the permissions to grant to this site. By default, the account that created the site is given full administrator permissions and is not shown in the list. All other accounts are listed and default to **No Access**.
    - **Admin** allows full access to the site.
    - **View Only** allows the ability to only view the site.
    - **No Access** denies access to the site.
5. Click **Next** to continue.
6. In the third step of the **Add Site** wizard, configure Endpoint Protection.
    - **Keycode Type**
        - Full if you purchased the product.
        - Trial if you registered for a free 30-day trial.
    - **Site Seats** are the number of endpoints for the site you are configuring. This setting is not used for billing.
    - **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See Endpoint Protection policy best practices in the Webroot Business Products Administration Guide.
        - **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.
        - **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.
        - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
        - **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.

        - Use the undetermined threats reports to identify items to add to your block and allow overrides.
        - Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
        - Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.
    - **Unmanaged**
        - Intended for technical support, troubleshooting, and when no policy management is needed.
        - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
        - Should not be used in production.
- **Default Endpoint Policy** is used for all new devices installed for this site unless the policy is assigned using inheritance from the group, site, or company. You can modify the policy the device uses after installation. Webroot recommends that you create a copy of this default endpoint policy and modify it according to policy best practices and your specific needs. See Endpoint Protection policy best practices in the Webroot Business Products Administration Guide.
    - **Recommended Defaults** is intended for desktops and laptops. User interface and possibly unwanted applications (PUAs) are disabled. The setting to install DNS Protection is disabled in this policy.
    - **Recommended DNS Enabled** is the same as **Recommended Defaults**, except the setting to install DNS Protection is enabled.
    - **Recommended Server Defaults** is intended for server environments. It focuses on resource utilization and minimal impact on the server.
    - **Silent Audit** is based on the **Recommended Defaults** policy, except the remediation function is disabled to minimize production impact. It catches known threats, but not undetermined threats.
        - Use the undetermined threats reports to identify items to add to your block and allow overrides.
        - Use caution when using this policy as having the remediation function disabled can enable threats to stay on devices.
        - Webroot recommends only using this policy for a short duration, such as during initial setup, to identify potential production false positives, conflicts, and uncover unknown software.
    - **Unmanaged**
        - Intended for technical support, troubleshooting, and when no policy management is needed.

        - Turns the agent into a local, unmanaged application that can be controlled directly by the end-user.
        - Should not be used in production.
    - **Data Filter**
        - Use data filters to show or hide data displayed in the console.
        - For example, if you select **2 Months**, all devices that have not connected for two months are excluded from the data shown for this site.
        - Data filtering may improve page loading performance but limits what you see.
        - When applying or clearing filters, data may take a few minutes to update depending on the deployment size and the amount of data to display.
        - **Inherit Parent Setting** causes the filter set at the console level to be inherited. This is found under **Settings > Data Filter > Data Filter** drop-down.
7. Click **Next** to continue.
8. If desired, enable **DNS Protection**. See DNS Protection in the Webroot Business Products Administration Guide.
9. Click **Next** to continue.
10. If desired, enable **Security Awareness Training**. See Security Awareness Training in the Webroot Business Products Administration Guide.
11. Click **Save** to complete the site configuration and to assign a keycode to the site.

# Step 3: Deploy

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

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

## Creating a custom workstation policy

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

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

**To create a custom workstation policy:**

1. Make a copy of the Recommended Defaults policy:
    a. In the navigation pane, under **Manage**, click **Policies**.
    b. Find the row for **Recommended Defaults**.
    c. Under **Actions**, click **Copy**.
2. Create a custom policy to apply best practices and configure specific requirements:
    - **Name** is the name of the workstations.
    - **Description** should be the policy for workstations.
    - For each policy setting below, expand the section and make the recommended changes.
        - **Basic Configuration**
            - Change **Poll interval** to **1 Hour** (strongly recommended). This reduces the length of time that the agent checks for setting changes or commands. Changing this setting gets you up and running much faster.
        - **Scan Settings**
            - Set **Automatically remove threats found on the learning scan** to **ON** to eliminate threats and improve performance.
            - Set **Detect Possibly Unwanted Applications (PUAs) as malicious** to **ON** to identify more malicious code with a small chance of a false positive.
        - **Behavior Shield**
            - Set **Automatically perform the recommended action instead of showing warning messages** to **ON** to have Webroot immediately address an issue rather than delaying for a manual action.
        - **Core System Shield**
            - Set **Prevent any program from modifying the HOSTS file** to **ON** to limit malware's ability to tamper with the network configuration file.
        - **User Interface**
            - Set **GUI** to **Show** to have the user interface easily available for straightforward troubleshooting.
            - There are no security issues with exposing the user interface.
        - **Evasion Shield**
            - Set **Script Protection** to **Detect and Remediate** to allow immediate action when a threat is identified.

## Deploying agents to devices

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

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

- **Endpoint Protection** is cloud-based, so once you install the agent, you do not need to install or update any definition files. Any newly identified threats are updated in the cloud for immediate protection.
- **DNS Protection** filters DNS requests when the devices are on and off the network. It uses a different agent than Endpoint Protection, but the Endpoint Protection agent must be present for the DNS Protection agent to function properly.

Seethe Webroot Endpoint Protection Administration Guide and the Knowledge Base for more details.

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

**To download and install the agent:**

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

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

If DNS Protection is enabled, filtering begins immediately.

## Finding your keycode

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

**For business view users:**

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

**For MSP users:**

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

## Starting to use Endpoint Protection

Congratulations! You have finished setting up Endpoint Protection.

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

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

### Spotlight tours

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

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

To view the Spotlight Tour again in the future:

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

### Learn more

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

You can also see more information online:

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

# Getting started with DNS Protection

1. Register, set up, and deploy **Endpoint Protection**. See Getting Started with Endpoint Protection.
2. Enable and configure DNS Protection. See Enabling and Configuring DNS Protection.

3. Ensure the endpoints are covered by **DNS Protection**.
    - This can be done by deploying agents to the devices using policies. See Using policies to deploy the DNS Protection agent in the Webroot Business Products Administration Guide
    - You can also set up your network to cover all devices within the network, regardless of whether they have the DNS protection agent. See Configuring the network in the Webroot Business Products Administration Guide

For more information about configuring DNS Protection, refer to the Webroot Business Products Administration Guide.

# Enabling and configuring DNS Protection

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

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

**To enable and configure DNS Protection in business view:**

1. Click **DNS Protection** in the navigation pane.
2. Enable the **DNS Protection** setting using the slider control.
3. If required, select your keycode type.
    - **Full** provides the full product with no limitations. You will be billed for this service.
    - **Trial** provides the full product, limited to a free, 30-day trial.
4. Under **Agent Settings**, select a default DNS site policy for the roaming agent. This can be modified on the **Policies** page.
    - **DNS High Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - **DNS Medium Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - Custom policies may also be available.
5. Under **Agent Settings**, create a domain bypass list to have domains resolved locally.
    - The list only applies to the DNS Protection agent.
    - Entries in the list are passed to the local DNS resolver rather than being resolved by the DNS Protection Agent.
    - Wildcards can be used to include any Subdomains.
    - Include your internal domain in the bypass list.
6. Under **Network Settings** you can enter details to protect network connected devices that do not have the agent installed.

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

7. Under **Network Settings**, use the Network Location menu to identify the best Webroot DNS services for your region.
    - Select the correct Network Location for the site on which you have enabled DNS Protection.
    - The best primary and secondary Webroot DNS services are shown.
    - Once you have identified the best resolvers, update your DNS forwarders.
8. Under **Advanced Settings**, select whether the agent can be installed on servers.
    - When checked, the DNS Protection agent installs on servers.
    - This is not recommended on DNS servers as it can cause DNS resolution problems.
    - DNS servers should be protected by configuring the DNS forwarders.
    - Other servers, such as terminal services, can run DNS Protection if you selected the **Allow DNS Agent to run on Servers** check box.
9. When done, click **Save**.

**To enable and configure DNS protection in service provider view:**

1. Click **Sites List** and expand the columns using the slider.
2. For the site you are working with, in the **DNS Protection** column, check if DNS Protection is either **Active** or in a **Trial** period by hovering over the **DNS Protection** icon  .
    - **Blue background** indicates DNS is active.
    - **Grey background** indicates DNS is inactive. Click the **Start Trial** link to start a free 30-day trial of DNS Protection. You are prompted to take one of two actions. These actions are not required to get started.
        - **Download Software** enables you to download the agent software.
        - **Configure DNS Settings** enables you to customize your DNS network settings.

        - This step allows you to protect devices without the agent installed by registering the WAN IP address associated with the network.
        - You do not need to configure this setting to get started.
    - **White background** indicates DNS is in trial period. Click the **Upgrade** link to convert to a full version, which you will be billed for.
    - **Slash mark** indicates the trial period is expired. Click the **Upgrade** link to convert to a full version, which you will be billed for.
3. To configure the DNS Protection settings for this site, hover over the **DNS Protection** icon and click the **Configure** button .
4. Under **Agent Settings**, select a default DNS site policy for the roaming agent. This can be modified on the **Policies** page.
    - **DNS High Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - **DNS Medium Protection** blocks all security categories as well as Human Resource Protections and Questionable/Legal content.
    - Custom policies may also be available.
5. Under **Agent Settings**, create a domain bypass list to have domains resolved locally.
    - The list only applies to the DNS Protection agent.
    - Entries in the list are passed to the local DNS resolver rather than being resolved by the DNS Protection Agent.
    - Wildcards can be used to include any Subdomains.
    - Include your internal domain in the bypass list.
6. Under **Network Settings** you can enter details to protect network connected devices that do not have the agent installed.
    - Identify the public IPv4 address used for internet access (WAN IP).
    - To make use of a domain name within our service, you need to use a third party Dynamic DNS service to transmit a changing IP address to a static domain name. Endpoint Protection uses this service to determine what IP address we should use to accept DNS requests from.
    - If you have dynamic IP support, entering a domain name resolves to the IP address. Third party dynamic DNS services are needed for this to be able to transmit a changing IP address to a static domain name.
    - Select a policy for that network. Any DNS requests received from this WAN IP are resolved based on this filter.
    - Requests from unregistered IP addresses or from IP addresses under expired or disabled sites do not receive a response.
    - Select **Add Network** to add multiple networks.

7. Under **Network Settings**, use the Network Location menu to identify the best Webroot DNS services for your region.
    - Select the correct Network Location for the site on which you have enabled DNS Protection.
    - The best primary and secondary Webroot DNS services are shown.
    - Once you have identified the best resolvers, update your DNS forwarders.
8. Under **Advanced Settings**, select whether the agent can be installed on servers.
    - When checked, the DNS Protection agent installs on servers.
    - This is not recommended on DNS servers as it can cause DNS resolution problems.
    - DNS servers should be protected by configuring the DNS forwarders.
    - Other servers, such as terminal services, can run DNS Protection if you selected the **Allow DNS Agent to run on Servers** check box.
9. When done, click **Save**.

## Installing network certificates and licenses

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

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

Certificates are automatically installed with the DNS Protection agent.

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

- Certificate Installer:

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

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

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

## Managing DNS Protection policies

To review or modify DNS Protection Policies:

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

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

- **Privacy Settings** control user privacy settings and the information that is logged.
    - **Hide User Information** improves privacy by replacing the user name and the domain requested with the word Hidden in the logs. If requests are made in the Security Risk category, the domain is still logged for visibility.
    - **Local Echo** echoes DNS requests made by the DNS Protection Agent to the local network's DNS resolver, providing visibility to these requests for your firewall or DNS server. To improve privacy, a DNS resolver can be specified, and requests will only be echoed when it is available.
    - **Fail Open** avoids a possible DNS interruption if the Webroot DNS resolvers are unavailable by deferring DNS resolution to the local resolver or returning without filtering.
- **Security Settings** specify whether to block or allow certain sites.
    - **Keyloggers and Monitoring** are sites that include downloads and discussions for software agents that track keystrokes or web surfing habits.
    - **Malware Sites** are sites known to contain malicious content including executables, drive-by infection sites, malicious scripts, viruses, or Trojans.
    - **Phishing and Other Frauds** are sites known to pose as reputable sites, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples don't last long.
    - **Proxy Avoidance and Anonymizers** are sites that use proxy servers or other methods to bypass URL filtering or monitoring.
    - **Spyware and Adwares** are sites that are known to contain spyware or adware that provides or promotes information gathering or tracking that is unknown to or without the explicit consent of the user. This policy also includes sites that contain unsolicited advertising pop-ups and programs that may be installed on users' computers.
    - **Bot Nets** are URLs or IP addresses known to be part of a Bot network from which network attacks are launched. Attacks may include SPAM messages, denial of service (DOS) attacks, SQL injections, proxy jacking, and other unsolicited contact.
    - **SPAM URLs** are URLs contained in spam messages.
- **Content Settings** specify whether to block or allow content that is inappropriate, illegal, or sexually explicit in nature.
    - **Human Resources Protections**
        - **Abused Drugs** sites show illegal, illicit, or abused drugs, including legal highs, glue sniffing, misuse of prescription drugs, or abuse of other legal substances.
        - **Adult and Pornography** sites contain sexually explicit material for the purpose of arousing sexual interest, including sites with adult products such as sex toys and videos. This policy also includes online groups sites that are sexually explicit, sites with erotic stories or textual descriptions of sexual

acts, sites for adult services such as video conferencing, escort services, and strip clubs, and sites with sexually explicit art.

- **Dating** sites focus on establishing personal relationships.
- **Sex Education** sites depict information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control and contraceptives, tips for better sex, and products used for sexual enhancement.
- **Swimsuits & Intimate Apparel** sites show swimsuits, intimate apparel, or other types of suggestive clothing.
- **Gross** sites show blood or bodily functions, such as vomit.
- **Nudity** sites contain nude or semi-nude depictions of the human body, that may not be sexual in intent but may include things like nudist or naturist sites, nude paintings, or photo galleries of artistic nature.
- **Alcohol and Tobacco** sites provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.

- **Questionable/Legal**
  - **Cult and Occult** sites provide methods, means of instruction, or other resources that attempt to affect or influence real events using astrology (including horoscopes), spells, curses, magic powers, or supernatural beings.
  - **Gambling** or lottery sites include sites that use real or virtual money; sites that contain information or advice for placing wagers, participating in lotteries, gambling, or running numbers; virtual casinos and offshore gambling ventures; sports picks and betting pools; and virtual sports and fantasy leagues that offer large rewards or request significant wagers. Hotels and resort sites that do not enable gambling on the site are categorized as Lifestyle, Travel or General Information, Local information.
  - **Marijuana** sites depict marijuana use, cultivation, history, culture, or legal issues.
  - **Hacking** sites depict illegal or questionable access to or the use of communications equipment/software or sites for the development and distribution of programs that may compromise networks and systems, including sites that avoid licensing and feeds for computer programs and other systems.
  - **Weapons** sites provide sales reviews and descriptions of weapons such as guns, knives, or martial arts devices, including sites that provide information on accessories or other modifications.
  - **Pay to Surf** sites pay users in the form of cash or prizes for clicking on reading specific links in emails or webpages.

- **Questionable** sites manipulate the browser user experience or client in some unusual, unexpected, or suspicious manner. Also includes get rich quick sites.
- **Hate and Racism** sites support hate crime or racist content or language.
- **Violence** sites advocate violence, violent depictions, or methods, including game/comic violence and suicide.
- **Cheating** sites support cheating and contain materials such as free essays, exam copies, and plagiarism.
- **Illegal** sites depict criminal activity including how not to get caught and copyright and intellectual property violations.
- **Abortion** sites depicting abortion, either pro-life or pro-choice.

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

- **Shopping** sites are for department stores, retail stores, company catalogs and other entities that allow online consumer or business shopping and the purchase of goods and services.
- **Shareware and Freeware** sites enable downloading free software, open source code, or downloads that request a donation, including screen savers, icons, wallpapers, utilities, and ringtones.

- **Entertainment**
  - **Entertainment and Arts** include motion pictures, videos, television, music and programming guides, books, comics, movie theaters, galleries, artists or reviews on entertainment, performing arts (such as theater, vaudeville, opera, or symphonies), museums, galleries, libraries, and artist sites (such as sculpture or photography).
  - **Streaming Media** are sites for sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers.
  - **Peer to Peer** sites provide peer-to-peer clients and access, including torrents and music download programs.
  - **Games** sites are for game playing or downloading, video games, computer games, electronic games, tips and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games, journals and magazines dedicated to game playing, support or host online sweepstakes and giveaways, and fantasy sports sites that also host games or game playing.
  - **Music** sites are for music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business.
- **Lifestyle**
  - **Travel** sites are for airlines and flight booking agencies, travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
  - **Home and Garden** sites are about home issues and products, such as maintenance, home safety, decor, cooking, gardening, home electronics, and design.
  - **Religion** sites are about conventional or unconventional religious or quasi-religious subjects, including churches, synagogues, or other houses of worship.
  - **Hunting and Fishing** sites are about sport hunting, gun clubs, and fishing.
  - **Society** sites cover a variety of topics, groups, and associations relevant to the general populace, and broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups.
  - **Sports** sites are team or conference websites, international, national, college, professional scores and schedules, sports-related online magazines or newsletters.

- **Fashion and Beauty** sites show fashion or glamor, magazines, beauty, clothes, cosmetics, and style.
- **Recreation and Hobbies** are sites with information, associations, forums, and publications on recreational pastimes such as collecting kit airplanes; outdoor activities such as hiking, camping, and climbing; specific arts, craft, or techniques; animal and pet related information, training, shows, techniques, and humane societies.

- **Business/Government/Services**
  - **Real Estate** are sites for renting, buying or selling real estate or properties; tips on buying or selling a home; real estate agents; rental or relocation services and property improvement.
  - **Computer and internet Security** are sites related to computer and internet security and security discussion groups.
  - **Financial Services** are sites offering banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies, excluding sites that offer market information, brokerage or trading services.
  - **Business and Economy** are sites for business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship.
  - **Computer and Internet Info** are sites containing general computer and internet information, including technical information. Also includes software as a service (SaaS) sites and other sites that deliver internet services.
  - **Military** are sites for the military branches, armed services, and military history.
  - **Individual Stock Advice and Tools** are sites that promote or facilitate securities trading and management of investment assets, including market information on financial investment strategies, quotes, and news.
  - **Training and Tools** are sites for distance education and trade schools, online courses, vocational training, software training, and skills training.
  - **Personal Storage** are sites that provide online storage and posting of files, music, pictures, and other data.
  - **Government** are sites related to government (local, county, state, and national), government agencies, and government services such as taxation, public, and emergency services. Also includes sites that discuss or explain laws of various governmental entities.
  - **Content Delivery Networks** are sites for the delivery of content and data for third parties, including ads, media, files, images, and videos.
  - **Motor Vehicles** are sites for car reviews, vehicle purchasing, sales tips, parts catalogs, auto trading, photos, discussion of vehicles, motorcycles, boats, cars, trucks and RVs, and journals and magazines on vehicle

modifications.

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

- **General Information**
  - **Legal** are sites related to legal topics and law firms as well as sites for discussions and analysis of legal issues.
  - **Local Information** are sites for city guides and tourist information, including restaurants, area/regional information, and local points of interest.
  - **Job Search** are sites that help find employment, tools for locating prospective employers, employers looking for employees, and career search and career placement from schools.
  - **Translation** refers to language translation sites that allow users to see pages in other languages. These sites can allow users to circumvent filtering as the target page's content is presented within the context of the translator's URL.
  - **Reference and Research** are sites for personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogs, genealogy, and scientific information.
  - **Philosophy and Political Advocacy** are sites for politics, philosophy, discussions, promotion of a particular viewpoint or stance to further a cause.
  - **Educational Institutions** are sites for pre-school, elementary, secondary, high school, college, university, and vocational school, and other educational content and information, including enrollment, tuition, and syllabus.
  - **Kids** are sites designed specifically for children and teenagers.
  - **News and Media** are sites with current events or contemporary issues of the day, including radio stations, magazines, newspapers, headline news sites, newswire services, personalized news services, and weather sites.
  - **Health and Medicine** are sites for general health, fitness, well-being, including traditional and non-traditional methods and topics. Also includes sites with medical information on ailments, various conditions, dentistry, psychiatry, optometry, and other specialties, hospitals and doctor offices, medical insurance, and cosmetic surgery.
  - **Image and Video Search** are sites that provide photo and image searches, online photo albums, digital photo exchange, and image hosting.
- **Uncategorized Domains** are sites that Webroot has not categorized in any of the above categories.

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

- When **Enable Google SafeSearch** is selected, DNS requests for www.google.com are resolved to forcesafesearch.google.com to filter explicit content from the search results.
- When **Enable DuckDuckGo Safe Search** is selected, DNS requests for www.duckduckgo.com are resolved to safe.duckduckgo.com to filter adult content from the search results.
- When **Enable Bing SafeSearch** is selected, DNS requests for www.bing.com are resolved to strict.bing.com to filter inappropriate content from the search results.
- When **Enable YouTube Restricted Mode I Moderate Mode** is selected, DNS requests for www.youtube.com are resolved to restrictmoderate.youtube.com.
- When **Strict Mode** is selected, DNS requests for www.youtube.com are resolved to restrict.youtube.com.

# Getting started with Security Awareness Training

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

**To get started with Security Awareness Training:**

1. Register and set up **Endpoint Protection**. You do not need to deploy agents to use **Security Awareness Training**. See *Getting started with Endpoint Protection* on page 6.
2. Enable and configure **Security Awareness Training**. See *Enabling Security Awareness Training* on page 27.
3. Target users for training. See *Targeting users for training* on page 28.

For more information about configuring Security Awareness Training, refer to the Webroot Business Products Administration Guide.

## Enabling Security Awareness Training

**To enable Security Awareness Training:**

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

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

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

**To configure Security Awareness Training settings:**

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

## Targeting users for training

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

**To target users for training:**

1. Go to the settings for Security Awareness Training.
    - In **business view**, click **Security Awareness Training** in the navigation pane and then open the **Settings** tab.
    - In **service provider view**, click **Sites List** in the navigation pane, open the site, and then open the **Security Awareness Training** tab.
2. Configure the domain to use to target your users.
    1. In **business view**, use the options on the **Security Awareness Training > Settings** tab.
    2. In **service provider view**, click **Sites List** in the navigation pane, open the site, then open the **Security Awareness Training** tab.
3. You can either configure the domain automatically, using Active Directory Integration, or manually, using Domain Verification.
    - **Active Directory Integration** synchronizes with Azure Active Directory to identify the domain. It also synchronizes a list of users in the domain that you can target for security training. See the Knowledge Base.

      You can see the synchronization status on the **Security Awareness Training settings** page. If needed, you can also click **Disable** to stop synchronizing from Azure.
    - **Domain Verification** identifies the domain through a verification email, then enables users to be added. Email addresses on ISP or public domains (for example gmail.com) are restricted and cannot be used. Email addresses must be valid company or organization addresses.
        - In the **Add New Domain** box, enter an email address.
            - If the email you enter is a **Domain Member**, campaigns can be created and run, but the breach report is not accessible.

        - If the email you enter is a system level **Domain Admin** (i.e., administrator, info, postmaster, root, system, or webmaster), campaigns can be created and run, and the breach report is accessible.
    - Click **Send Verification Request** to send a verification email to the specified email address.
    - Once you get the email, click the verification link in the message to confirm access to that domain.
    - After access to the domain is confirmed, click **Security Awareness Training** on the navigation pane and open the **Users** tab.
    - Select a site (**service provider view** only)
    - Click **Add Users to Site**.
        - **Enter Users Manually** indicates you will manually specify the name and email for each user you want to target for training.
        - **Set up Active Directory** integration synchronizes using Azure Active Directory. See https://answers.webroot.com/Webroot/ukp.aspx?pid=4&app=vw&vw=1&login=1&solutionid=3883.
        - **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.