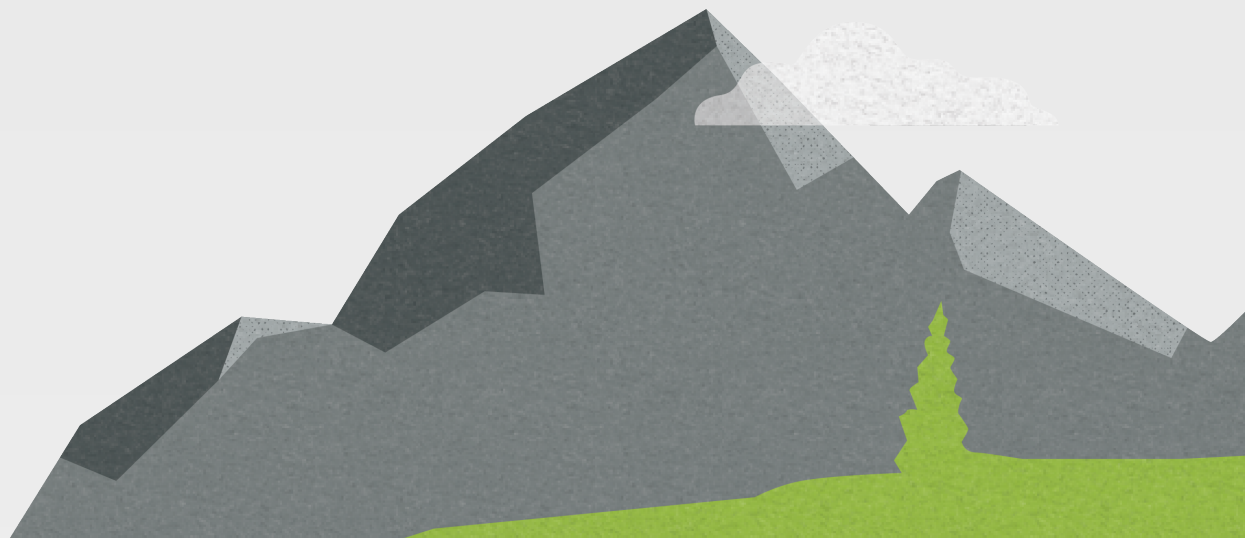


# Business Products - Endpoint Protection, Detection and Response, DNS Protection, and Security Awareness Training

## *Getting Started Guide*



# Notices

Endpoint Protection, Detection and Response, DNS Protection, and Security Awareness Training Getting Started Guide revision Wednesday, March 18, 2026.

Information in this document is for the following products:

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

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

© 2026 Open Text. One or more patents may cover these products. For more information, please visit <https://www.opentext.com/patents>.

# Contents

---

- Notices** ..... 2
- Contents** ..... 3
- Overview** ..... 4
- Requirements** ..... 6
- Getting started with Endpoint Protection** ..... 8
  - Step 1: Register/Purchase ..... 9
    - Purchasing or registering for a trial ..... 9
  - Step 2: Setup ..... 10
    - Creating and activating your account ..... 10
    - Selecting your Management Console view ..... 11
    - Setting up two-factor authentication (2FA) ..... 12
    - Creating a Site (MSPs only) ..... 13
  - Endpoint Protection ..... 16
    - Creating a custom Policy ..... 16
    - Downloading and installing the agent ..... 16
    - Finding your keycode ..... 17
    - Starting to use Endpoint Protection ..... 18
    - Learn more ..... 18
    - Spotlight tours ..... 18
- Getting started with Detection and Response** ..... 19
  - Enabling Detection and Response ..... 19
  - Installing the Detection and Response agent ..... 20
  - Integrations ..... 21
    - Integration categories ..... 21
    - Setting up an integration ..... 22
    - Setting up the Webroot integration ..... 22
- Getting started with DNS Protection** ..... 23
  - Enabling and configuring DNS Protection ..... 24
  - Managing DNS Protection Policies ..... 25
- Getting started with Security Awareness Training** ..... 32
  - Enabling Security Awareness Training ..... 33
  - Targeting users for training ..... 33
- Getting started with Server Backup - Public Cloud** ..... 35

# Overview

This Getting Started guide details how to get up and running with the Endpoint Protection, Detection and Response, DNS Protection, and Security Awareness Training business products. This guide also contains references to Server Backup - Public Cloud.

These business products are 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 Detection and Response in the Endpoint Protection Administration Guide
- **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 Detection and Response in the Endpoint Protection Administration Guide.
- **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 in the 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 is purchased separately and can work independently or in conjunction with **Endpoint Protection**. See Security Awareness Training in the Business Products Administration Guide.
- **Server Backup - Public Cloud** lets you quickly and securely back up your servers to cloud storage and recover files, volumes and servers when you need them. All backup data is encrypted in transit and at rest, and only you know the password required to restore it. In the event of a threat such as ransomware, hardware failure, or a natural disaster, you can recover exactly what you need— specific files and folders, selected volumes, or entire servers. For detailed information on Server Backup - Public Cloud, see the [Server Backup - Public Cloud 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 business products.

This guide first walks you through installing and configuring Endpoint Protection and then provides instructions for **Endpoint Detection and Response**, **Managed Detection and Response**, **DNS Protection**, **Security Awareness Training**, and **Server Backup - Public Cloud**, which are included in separate chapters at the end.

For detailed information about Endpoint Protection and functionality common to all products, see the [Business Products Administration Guide](#). Depending on your permissions, certain functionalities discussed within this guide might not be available to you.

# 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 Security Awareness Training email in Microsoft Exchange and Office 365](#)
  - [How to allow Security Awareness Training email in G Suite Gmail](#)
  - [How to allow 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, Security Awareness Training, Endpoint Detection and Response, and Managed Detection and Response. 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, DNS Protection, Security Awareness Training, Endpoint Detection and Response, and Managed Detection and Response. 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 9 in the Business Products Administration Guide.
- 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 10 in the Business Products Administration Guide.
  - See *Setting up two-factor authentication (2FA)* on page 12 in the Business Products Administration Guide.
  - See *Selecting your Management Console view* on page 11 in the Business Products Administration Guide.
  - See *Creating a Site (MSPs only)* on page 13 in the Business Products Administration Guide.

## 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 16 in the Business Products Administration Guide.

## Endpoint Detection and Response and Managed 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 or Managed Detection and Response.
  - See *Enabling Detection and Response* on page 19 in the Business Products Administration Guide.

- See *Installing the Detection and Response agent* on page 20 in the Business Products Administration Guide.

### 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 24 in the Business Products Administration Guide.
- 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* in the Business Products Administration Guide.

### 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 33
  - See *Targeting users for training* on page 33.

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

#### Purchase an Endpoint Protection subscription:

1. Go to <https://cybersecurity.opentext.com/products/threat-detection/endpoint-protection/>.
2. Click **Buy Now - Webroot.com**.
3. Enter the number of required seats for each product. To include additional products in your order, click the **Add Now** buttons and enter the number of required seats. To remove a product, click the **X** icon.
4. Enter all required billing information and click **Pay** to place your order. You will receive an email confirmation and next steps.

**Note:** 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.

#### Start a trial:

1. Go to <https://cybersecurity.opentext.com/products/threat-detection/endpoint-protection/free-trial/>.
2. Enter all required information in the appropriate fields.
3. Click **Get My Free Trial**. You will receive an email confirmation and next steps to start the trial and install the product. Follow the instructions in your browser to activate your account and install Endpoint Protection.

## 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 each time you sign in, 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. 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](https://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:** 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 16.

If you selected the **Managed Service Provider view**, go to *Creating a Site (MSPs only)* on page 13 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 in the Business Products Administration Guide.
      - **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**.
- If desired, enable **Endpoint Detection and Response** or **Managed Detection and Response**. The following options are displayed :
  - **Keycode Type**
    - Full if you purchased the product.
    - 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 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 in the Business Products Administration Guide.
9. Click **Next** to continue.
10. If desired, enable **Security Awareness Training**. See Security Awareness Training in the Business Products Administration Guide.
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.

This section of the guide includes instructions on how to:

- 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.

For more information on policies, see Policies.

### 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 17.
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*. 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:** 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 in the Business Products Administration Guide.

## 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* in the Business Products Administration Guide.

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

To view announcements, access online help and videos, or contact support, go to the **OpenText Resource Center** by clicking the bell icon  in the global navigation bar.

You can also see more information online:

- For how-to articles, go to the [OpenText Core Support Knowledge Base](#).
- Check out various product forums and ask questions on the [OpenText Cybersecurity 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

# Getting started with Detection and Response

This guide explains how to set up and use Detection and Response products through the Management Console.

## To get started with Detection and Response:

1. Enable **Endpoint Detection and Response** or **Managed Detection and Response**. See *Enabling Detection and Response* on page 19.

**Note:** To use **Endpoint Detection and Response** you must have **Endpoint Protection** enabled. To register and set up Endpoint Protection, see *Getting started with Endpoint Protection* on page 8 in the Business Products Administration Guide.

2. Install the Detection and Response agent. See *Installing the Detection and Response agent* on page 20.

For more information about Detection and Response, refer to the Business Products Administration Guide.

## Enabling Detection and Response

### To enable a Detection and Response product in the Management Console:

1. In the navigation pane, click the **Settings** tab.
2. In the **Subscriptions** tab, activate a trial to Endpoint Detection and Response or Managed Detection and Response.
3. Enable the Detection and Response product 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 the Detection and Response product on, and click the **Endpoint Protection** tab.
4. Enable **Endpoint Detection and Response** or **Managed Detection and Response** using the slider control.

**Note:** To use **Endpoint Detection and Response** you must have **Endpoint Protection** enabled. To register and set up Endpoint Protection, see *Getting started with Endpoint Protection* on page 8 in the Business Products Administration Guide.

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. To deploy Endpoint Detection and Response or Managed Detection and Response, see *Installing the Detection and Response agent* on page 20.

Once a Detection and Response product is enabled, you can access all features by selecting **Detection and Response** in the navigation pane.

# Installing the Detection and Response agent

There is a single, unified installer for Endpoint Detection and Response, Managed Detection and Response, and Endpoint Protection. When the installer is downloaded from a Site in the Management Console, it automatically deploys only the agents and components required for the Endpoint Protection and Detection and Response products enabled for that Site.

**Note:** If you already have Endpoint Protection enabled and installed, no additional steps or downloads are required to install a Detection and Response product once it is enabled in the Management Console. The existing agent will automatically install the newly enabled product the next time it checks in to the console.

## To install products with the unified installer:

1. In the Management Console, go to the **Sites List** and choose a Site where you want to install the agent.
2. Go to the **Endpoint Protection** tab. Ensure the appropriate Detection and Response product is enabled. For more information, see *Enabling Detection and Response* on page 19.
3. Follow the on-screen instructions to download the installer and run it on your devices.

Once installation is complete, no additional steps are required.

**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*. 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.

With Endpoint Protection enabled, you can disable Detection and Response for devices within a Site by assigning a custom Endpoint Protection policy to those devices with the "Install EDR / MDR Agent" setting disabled. For devices with existing EDR or MDR installations, setting this policy to **Off** will remove all EDR and MDR components from the device.

## Disable the "Install EDR / MDR Agent" setting:

1. In the navigation pane, go to **Manage > Policies**.
2. From the Endpoint Protection tab, select the Policy associated with devices that you do not want to install the EDR or MDR agent on.

**Note:** By default, System Policies (excluding the Unmanaged Policy) will have **Install EDR / MDR Agent** set to **On** and cannot be edited.


3. Scroll down to **Policy Settings**. In the **EDR / MDR** section, select **Off** beside **Install EDR / MDR Agent**.

4. In the **Policy Usage** section, identify which systems will be affected.
5. Click **Save**.



## Integrations

On the **Integrations** page, you can view and manage active integrations or set up new ones. To set up a new integration, see *Setting up an integration* on page 22.

The **Installed** tab shows all active integrations, including active integrations currently experiencing errors.

- Use the search bar to find a specific integration, or use filters to find integrations with a specific category or status. For more information on categories and the integrations in them, see *Integration categories* on page 21.
- To view details and modify an integration, click the pencil icon .
- To remove an integration, click the **X** icon.

To see all available integrations, click the **Browse Integrations** tab.

- Use the search bar to find a specific integration. Use filters to find integrations with a specific category or status. Each integration includes a short description explaining what it does.
- To begin configuring a new integration, click the pencil icon . See *Setting up an integration* on page 22.
- If available, click the booklet icon  to see the Knowledge Base article for setting up the integration.

**Note:** Integrations with a **Deprecated** label should not be used. Instead, click the pencil icon beside the deprecated integration and use the indicated replacement.

## Integration categories



Integrations are sorted into categories based on their function. Categories include:

- **Authentication Logs** - Collect and process login attempts, access patterns, and identity verification data to help detect suspicious behavior.
- **Application Security** - Protect applications from vulnerabilities and threats using tools that monitor, detect, and remediate risks within software applications
- **Automation Auditing** - Help with oversight of automated processes and workflows.
- **AWS** - Monitor and manage security for Amazon Web Services environments.
- **Azure EventHub** - Relates to Microsoft Azure's EventHub. Integrations help capture and process event data for analytics and security monitoring.

- **Cloud Security** - Integrations in this category help with threat and vulnerability detection and remediation across various cloud environments.
- **DNS and URL Monitoring** - Track domain name system activity and web traffic to detect potential threats and block malicious domains.
- **Endpoint Security** - Protect devices such as laptops and servers by detecting potential threats and vulnerabilities.
- **Google Cloud** - Ingest logs from Google Cloud Platform environments.
- **Messaging Security** - Solutions for secure communication channels such as email and messaging platforms, including spam filtering, phishing detection, and advanced email security.
- **Mobile Endpoint Security** - Protect mobile devices from various threats.
- **Multi Factor Authentication** - Implement and manage MFA across applications and systems.
- **Network Monitoring** - Monitor network traffic to detect unusual behavior, identify intrusions, and ensure network health.
- **Service Desk** - Connect and send alerts to third-party ticketing systems.
- **Syslog** - Ingest data from network devices like firewalls.

## Setting up an integration

To set up a new integration in the **Detection and Response console**:

1. In the navigation pane, click **Integrations**. Go to the **Browse Integrations** tab.
2. To find a specific integration in the list, use the search bar or filter by category or status. To begin configuring the integration, click the pencil icon  .
  - When available, you can click the booklet icon  to access the step-by-step Knowledge Base article on an integration.
3. Under **Connection Settings**, enter all required information for the integration.
4. Where applicable, click **Validate** to finish setting up the integration.

**Note:** Some integrations do not follow this process. For more information on a specific integration, click the booklet icon to review the appropriate Knowledge Base article.

## Setting up the Webroot integration

In the Detection and Response console, you can integrate with Webroot to allow for scanning of endpoints using Endpoint Protection.


This integration requires steps in the Management Console and the Detection and Response console. You will need to set up the Unity API in Secure Cloud before following the below processes. For more information on using APIs with Secure Cloud, see [Secure Cloud Help: Generate and manage API credentials](#) and the [Secure Cloud API reference](#).

### Setting up in the Management Console:

1. In the navigation pane, click **Settings**. Go to the **Account Information** tab.
2. Make note of the **Parent Keycode**. This is the GSM key and is required for use with the integration in the Detection and Response console.
3. Next, go to the **Unity API Access** tab and click the **New** button.
4. In the **Create New Client Credential** dialog box, enter a **Name** and **Description** for the credential, then click **Next**.
5. Enable the option to use the event notification API. Choose either "Integration with SIEM provider" or "Other use or enhancement" from the list. If you chose SIEM provider, enter "OpenText MDR". If you chose "Other use or enhancement", provide details.
6. The console displays a dialog box with both the **Client ID** and the **Client Secret**. Make note of both of these values. The Client Secret cannot be retrieved later, although it can be regenerated. Once you have made note of these values, click **I have made note of the client secret**.

**Note:** If you lose the client secret, you can regenerate one by selecting the credential in the **Unity API Access** tab and clicking the **Renew Secret** button. This will generate a new secret, and the previous one will expire. Any future requests made using the credential with the old secret will be revoked.

### Setting up in the Detection and Response Console:

1. In the Management Console navigation pane, click **Detection and Response** to log in to the Detection and Response console.
2. In the navigation pane, click **Integrations**.
3. Click **Browse Integrations**, then search for the **Webroot** integration. Click the pencil icon .
4. In the **Connection Settings** section, paste in the copied client ID and secret, the username and password of the super admin in the console, and the GSM key. Click **Save**. To add another host, click **Add Host**.
5. In the **Customer Mappings** section, specify which customer corresponds to which site in the Management Console. If a customer is not mapped, the integration will not work for that customer. Click **Auto Match Names** to automatically map customers to sites with the same name in the Management console.

Once enabled, the integration is immediately available for use.

## Getting started with DNS Protection

1. Register with the Management Console. See *Getting started with Endpoint Protection* on page 8.
2. Enable and configure DNS Protection. See *Enabling and configuring DNS Protection* on page 24.
3. Ensure the endpoints are covered by **DNS Protection**.

- Deploy the DNS Protection agent. See Configuring the network in the Business Products Administration Guide in the Business Products Administration Guide.
- Protect the network. See Configuring the network in the Business Products Administration Guide

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

## 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 25.
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 \*.opentext.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. 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 | 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 8.
2. Enable and configure **Security Awareness Training**. See *Enabling Security Awareness Training* on page 33.
3. Target users for training. See *Targeting users for training* on page 33.

For more information about configuring Security Awareness Training, refer to the 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 **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 Entra 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 Entra.

- **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 Entra 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.

## Getting started with Server Backup - Public Cloud

With OpenText Server Backup - Public Cloud, you can quickly and securely back up your servers to cloud storage, and recover files, volumes and servers when you need them. All backup data is encrypted in transit and at rest, and only you know the password required to restore it. In the event of a threat such as ransomware, hardware failure, or a natural disaster, you can recover exactly what you need— specific files and folders, selected volumes, or entire servers.

Once enabled, you can manage Server Backup within the Management Console.

To start a trial, order a subscription, and set up Server Backup in the Management Console, see the [Server Backup Guide](#).