Advanced Security Subscriber Portal User Guide

January 7, 2026

Contents

Chapter 1: Overview

The Advanced Security service enables you to customize the Internet browsing experiences for individual devices accessing your network. Use the Advanced Security service with the web filtering feature to filter and block specific content on your individual household devices. The Advanced Security service provides an easy-to-manage portal where you can see all household Internet activity in one place from any device.

The Advanced Security service empowers the following security measures:

- Provide DNS-based network security (protects all devices using your network) to household members and guests. The Advanced Security service analyzes data in real-time to detect threats so that you can provide protection against ransomware, phishing, and botnet attacks. The Advanced Security service identifies and reports malicious activity so that you can locate and mitigate (block) infected devices.
- Use the web filtering feature to apply web filtering that restricts web browsing on your household devices. With web filtering, you can perform the following tasks:
    - Restrict individual device access to explicit and inappropriate web content. You can differentiate content access permissions for the devices in your household. These permissions enable you to differentiate Internet usage, limiting access to specific types of content according to the age of the device user.
    - Apply content access settings to specific groups of devices at specific times. For example, restrict Internet usage and content access during a homework time period.
    - Pause internet access for specific groups of devices or specify hours during which internet access is disabled (Internet Off) at specific times.
    - Monitor DNS traffic volume generated by family members and guests.

  NOTE: Web filtering settings follow users as they traverse different (fixed and mobile) networks.
- If the security feature is enabled, you can protect devices from malware and phishing websites and data exfiltration. The Advanced Security home dashboard includes a live report which provides general data about the Internet usage in your household.
- Provide Network-based Google, Youtube, and Bing SafeSearch support to household and guest devices.

The Advanced Security service provides the following benefits:

- Because the Advanced Security service is a network based service, you do not need to install or update software on any devices. The service protects all internet connected devices regardless of browser or connection type.
- Prevent connected devices from accessing content restricted by either web-filter or security policies.
- You can access the Advanced Security service from any device, gaining visibility into threats against your network and your household Internet usage patterns.

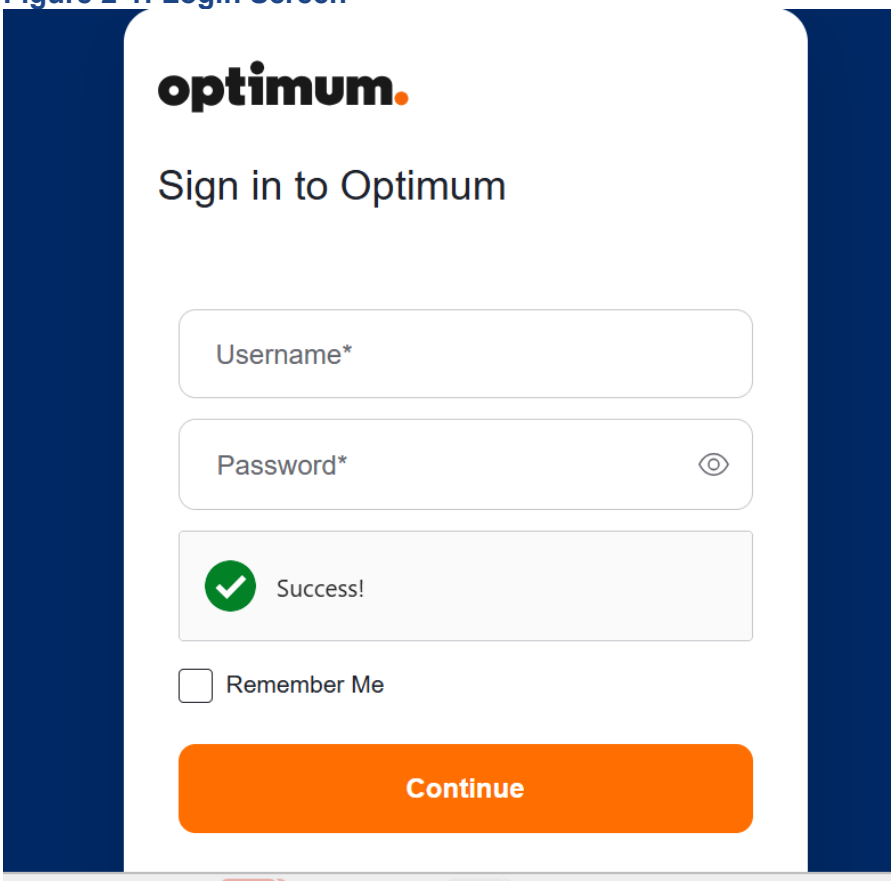
The Advanced Security service supports the following features:

- The security service—Proactively monitors and blocks outbound DNS requests to sites known to host malware, phishing or botnet command and control endpoints. The Advanced Security home dashboard includes a live report which provides general data related to your household Internet usage.
- Web filtering—With web filtering, you can control your household web browsing activity by creating profiles that dictate different levels of protection. By assigning devices to specific profiles, you can perform the following tasks:
    - Block a device's access to explicit and inappropriate web content at all times.
    - Restrict Internet usage during specific time periods.
    - Restrict and allow access to specific websites.

Chapter 2: Initial Configuration

Optimum customers will use a **single sign on (SSO)** to access the Advanced Security portal via their Optimum.net portal

Figure 2-1: Login Screen



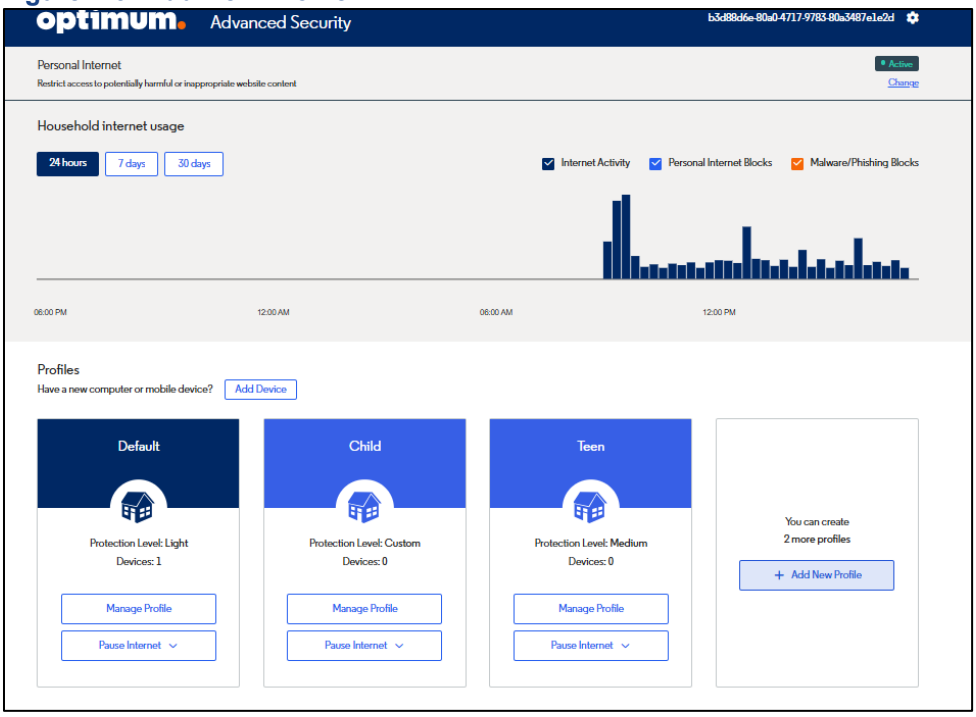
NOTE: If prior authorization tokens exist, you will not be prompted for login credentials.

Setting up a Multiple Profile Service

Use the following steps to set up multiple profiles:

1. For easy of use, three profiles are already created a) Default b) Child c) Teen
2. The application allows you to create two more profiles Figure 2-3; click the **Add New Profile** button to begin creating a new profile:

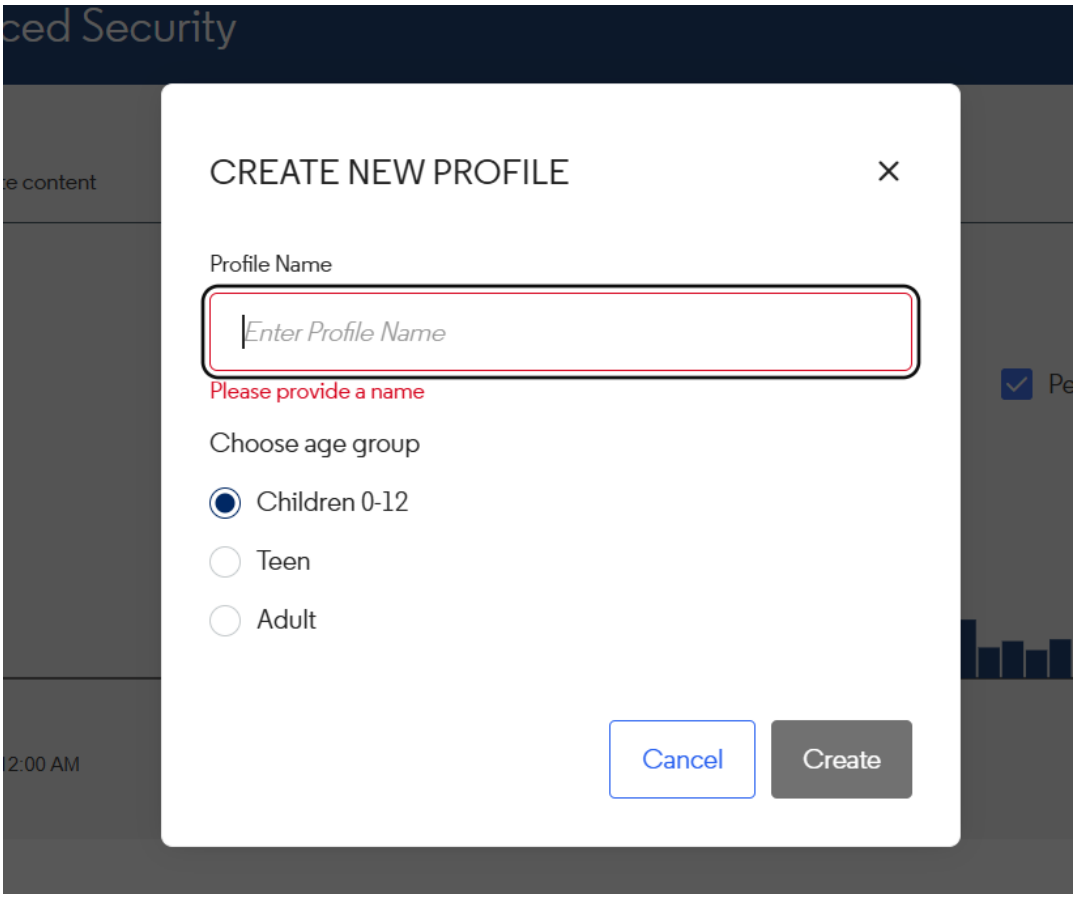
Figure 2-3: Add New Profile



3. When prompted, perform the following tasks:
    a. Assign an age range to the profile.
    b. Click the **Create** button to continue setting up the profile.

Figure 2-4 shows the “Create Profile” screen and demonstrates how to perform Step 2a and Step 2b.

Figure 2-4: Initial Configuration Screen - Choose Profile Age Range



4. When prompted, perform the following tasks:
    a. Enter a name for the profile.
    b. Select the age group you want to assign to the profile from the **Choose age group** drop-down menu.
    c. Click the **Create** button

Where to Go Next

Before assigning devices to your profiles, we recommend performing the following tasks to finish setting up your service:

- For an overview of the Advanced Security service menu options and how to navigate through the different pages in the application, see Chapter 3, “Navigating the Advanced Security Application.”
- To Customize the block pages the devices accessing your network can encounter, see Chapter 6, “Managing Block Pages.”

- If desired, you can configure your service to aggregate block statistics reports to be sent to yourself and to other interested parties. See Chapter 7, “Managing Statistics and Reporting” for more information.

Chapter 3: Navigating the Advanced Security service

This chapter describes how to navigate and manage the following Advanced Security features:

- The Advanced Security home dashboard
- Multiple profile support
- Device discovery
- Additional features

The Advanced Security Home Dashboard

After setting up your Advanced Security service as described in Chapter 2, "Initial Configuration," the Advanced Security home dashboard is the first screen you see when you open the Advanced Security service. The Advanced Security home dashboard is divided into two sections:

- The top half of the home dashboard comprises a live report which provides general data about the related to your household Internet usage.
- The bottom half of the home dashboard displays profile tile icons that represent the profiles that exist in your Advanced Security service.

Figure 3-1 shows an example of what the Advanced Security home dashboard looks like when you open an active Advanced Security service (after initial configuration). Figure 3-1 includes call-outs where each number corresponds to a component described in the Table 3-1.

Figure 3-1: Advanced Security Home Dashboard

Table 3-1: Advanced Security Home Dashboard Components

Callout	Component	Description
1	Services (gear) icon drop-down menu	Provides a drop-down menu that contains the following options: • **Account**—Accesses the "Account" page where you can manage your account settings. • **Block & Allow Lists** —Accesses the "Block & allow lists" page where you can manage your block and allow lists; this page provides controls for adding domains to and removing domains from block and allow lists. • **Block Page**—Accesses the "Block page" page where you can enable and disable malware and phishing protection and configure a Bypass PIN that enables users to bypass your block pages. • **Devices**—Access the "Devices" page where you can manage the devices in your Advanced Security service. • **Clear Data**—Clears the current statistical data in your Advanced Security service. • **Help Page**—Accesses online help documentation for the Advanced Security service. • **Log out**—Logs you out of the Advanced Security service.
2	New devices alert message	Appears on the home dashboard when the Advanced Security service detects new devices in your household. Click the **Take action** link to view and, if desired, manage the new devices in your Advanced Security service. Click the **X** icon to close the message.
3	"Malware & Phishing Protection" control	If your service supports the security feature, this field indicates whether the malware and phishing protection service is activated for your Advanced Security account. Clicking the **Change** link takes you to the "Block page" controls where you can enable and disable the security service. The malware and phishing protection service is disabled by default. **NOTE:** This field is available only if your service is licensed to support the security service. If your service does not include the security service, this field does not appear on your Advanced Security home dashboard. **Caution:** When the malware and phishing protection service is disabled, your devices are susceptible to phishing and downloading malware from malicious websites.

4	Web Filtering control	If your service supports web filtering, this field indicates whether web filtering is activated for your Advanced Security account. Clicking the **Change** link takes you to the “Block page” controls where you can enable and disable web filtering. **Caution!** When you disable web filtering, your profiles do not apply to the specified devices and all websites are accessible. **NOTE:** This field is available only if your service is licensed to support the security service. If your service does not include the security service, this field does not appear on your Advanced Security home dashboard.
5	Live Report time-period controller buttons	Dictates the time-period for which the live report graph displays data. Clicking any time period button changes the graph to display information for the selected time period. You can display Internet usage information for the last **24 hours**, **7 days**, or **30 days**. By default, the graph displays Internet usage information for the last **24 hours**.

6	Live report data selection checkboxes	Checkboxes which dictate the data represented in the live report for the specified time period. To include a specific data type in the graph, add a checkmark in the checkbox that appears next to the desired data type. The graph can include the following data types: • **Internet Activity**—Tracks household Internet usage during the specified time period; this data is represented by blue bars in the live report graph (see callout 7). • **Web Filtering Blocks**—Tracks the number of times a device tried to access a blocked or malicious website; this data is represented by yellow bars in the live report graph (see callout 7). • **Malware/Phishing Blocks**—Indicates whether a household user accessed a suspicious website that might have installed phishing or malware on a household device. When this data type is selected, the live report includes an orange alert under the Live Report graph when a household user accesses a suspicious website. Click the **See Details** button to see information pertaining to the affected devices and possible infections. By default, the graph includes **Internet Activity** and **Web Filtering Blocks** data. To exclude a specific data type in the live report, uncheck the box next to the data type you want to exclude. To include **Malware/Phishing Blocks** alerts in the live report, check the box next to the **Malware/Phishing Blocks** data type and ensure the malware and phishing protection service is **Active** in your Advanced Security service (see callout 3 for more information). Be aware you cannot add a checkmark to the **Malware/Phishing Blocks** check box unless Malware and Phishing protections are enabled in your system; see callout 3, "Malware & Phishing Protection" control, for information on enabling malware and phishing protections in your Advanced Security service.
7	Household Internet usage live report	Graphical representation of your household's Internet activity and the blocked request volume attributable to either malware & phishing or to parental control policies. You can dictate the data shown in the graph by selecting and deselecting specific data type checkboxes in the live report data selection section (described in callout 6). To see the date and time frame during which a particular set of blocks occurred, hover your cursor over the desired time-axis point.

8	**Add Device** button	Opens the “Devices” page, where you can add devices to and manage the device using your Advanced Security service.
9	Profile tiles	Represents the profiles that exist in your Advanced Security service. Each profile tile contains the following controls: ● A **Manage Profile** button that, when clicked, opens the “Profile details” page for the profile. See the “Managing Profile Settings” section for details ● A **Pause Internet** drop-down list of time-periods for which you can pause internet access on the devices the profile manages.

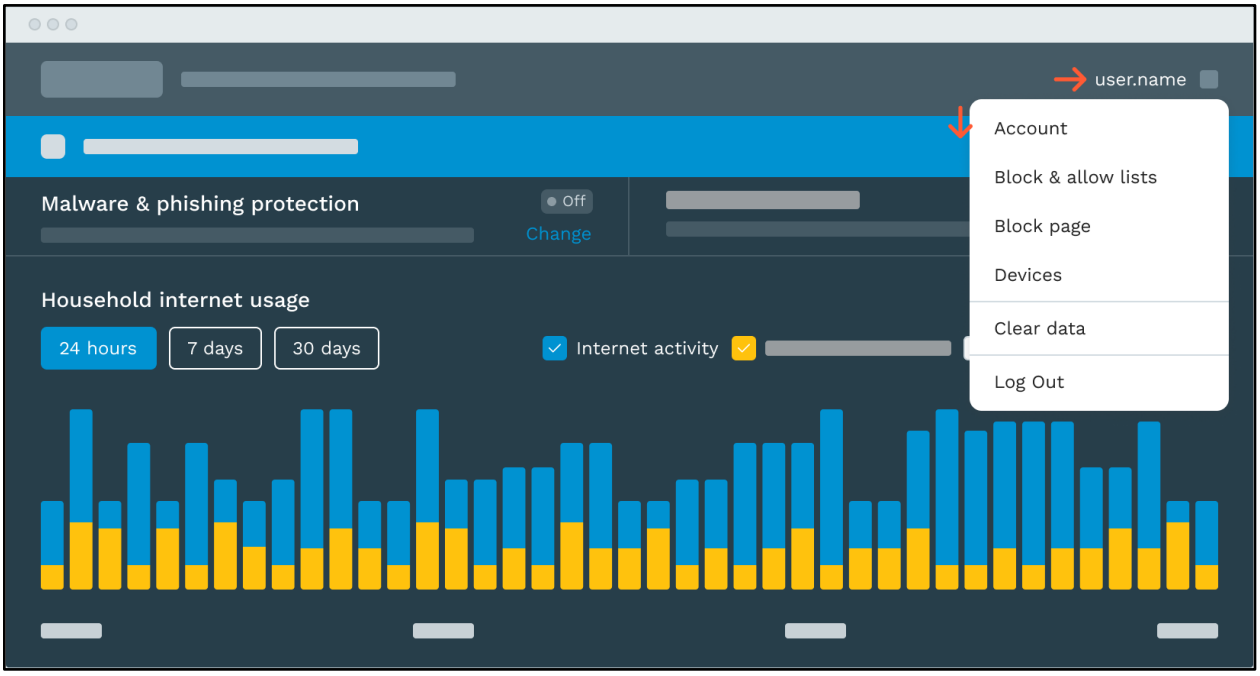
The Services Drop-down Menu

The Advanced Security drop-down menu provides the following options:

- **Account**—Accesses the “Account” page, where you can view and modify general Advanced Security service account settings. See the “Managing your Advanced Security account settings” section in this chapter for more information.
- **Block & Allow Lists** —Accesses the “Block & allow lists” page where you manage your block and allow lists. See the “Managing Block and Allow Lists” section in Chapter 4, “Managing Profile Settings” for details.
- **Block Page**—Accesses the “Block page” management page where you can manage your block pages and globally enable and disable web filtering and security services. See Chapter 6: “Managing Block Pages,” for details.
- **Devices**—Accesses the “Devices” page where you view and manage the devices in your Advanced Security Service. See Chapter 5, “Managing devices,” for details.
- **Clear Data**—Clears the data history in your Advanced Security service.
- **Log out**—Logs you out of the Advanced Security service.

Access the account settings options from the user account drop-down menu as demonstrated in Figure 3-2.

Figure 3-2: Advanced Security Services Drop-down Menu



Understanding Multiple Profile Support

The Advanced Security service supports the following modes of operation; this document describes how to use the Advanced Security service to manage multiple profiles:

- Multiple profiles—With multiple profiles, each profile has its own unique protection level and set of allowed content categories. The Advanced Security service supports the following profiles:
    - A preconfigured **Default** profile; this profile provides a preconfigured level of protection, but you can modify the protection level and content category restrictions enforced by the **Default** profile.

      NOTE: New and unregistered devices in your network are automatically assigned to the default profile. You can block such devices or you can assign those devices to another profile.
    - Any additional profiles that have a preconfigured or **Custom** level of protection assigned. You assign the level of protection when setting up the profile.

Device Discovery

The Advanced Security service alerts you upon detecting new and unregistered devices; you can perform the following actions on those devices:

- Assign the devices to a profile.
- Block the devices from accessing your network.

The Advanced Security service initially assigns all approved devices to the default profile until you manually assign those devices to the appropriate profile. The default profile needs to have protection preferences applicable to network guests whose network use is transitory.

Managing your Advanced Security Account Settings

You can modify the following account details on the “Account” page:

- The time zone for your Advanced Security service.
- The time format Advanced Security reports and schedules use.
- The language the Advanced Security service uses.

You can access the “Account” page from the following locations:

- The **services** drop-down menu (as demonstrated by callout 1 in Figure 3-3).
- The page selector that appears on all configuration pages in the Advanced Security service (as demonstrated by callout 2 in Figure 3-3).

Figure 3-3: How to Access the “Account” Page

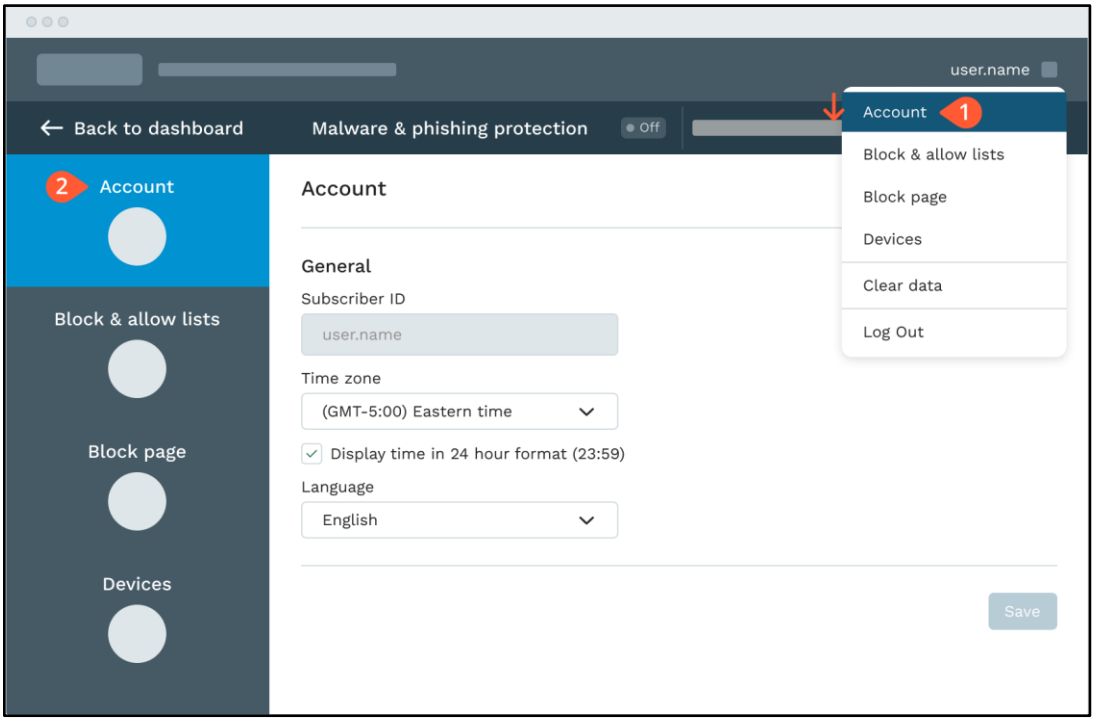


Figure 3-4 shows what the “Account” page looks like; the figure includes call-outs where each number corresponds to a component described in Table 3-2.

Figure 3-4: Account Page Settings

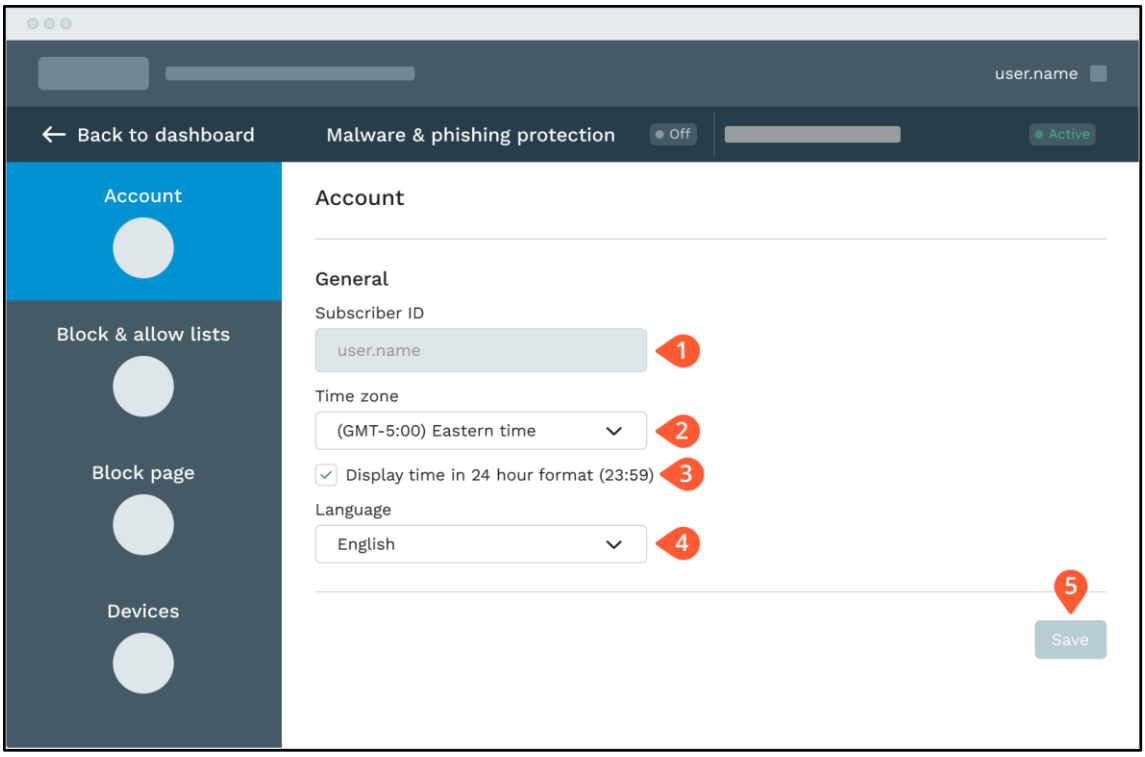


Table 3-2 describes the fields that appear on the “Accounts” page:

Table 3-2: “Account” Page Components

Callout	Component	Description
1	“Subscriber ID” field	Identifies the user that is currently logged into the Advanced Security service.
2	“Time Zone” drop-down list	Specifies the time zone for the application. To modify the time zone setting, select the desired time zone from the drop-down list.
3	“Display time in 24-Hour Format” checkbox	Indicates whether the Advanced Security service uses **24-hour** (military) or **12-hour** time notation. Add a checkmark to the checkbox to use **24-hour** time notation; clear the checkbox to use **12-hour** time notation. The Advanced Security service uses **12-hour** time notation by default.
4	“Language” drop-down menu	Specifies the language the Advanced Security service interface uses. Select the desired language from the drop-down menu.
5	**Save** button	When clicked, saves any changes you made to the Advanced Security account settings.

iCloud Private Relay Blocking

When you enable the iCloud Private Relay blocking feature in your service, devices that have iCloud Private Relay enabled receive a notification that indicates the local network is not compatible with the iCloud Private Relay service; the device owner needs to disable the iCloud Private Relay service if they want to use the network connection. See Appendix B, "Implementing the iCloud Private Relay Blocking Feature," for details.

Chapter 4: Managing Profile Settings

If your Advanced Security service includes web filtering, you can control web browsing activity in your network by specifying the types of content the devices can access.

With web filtering, you can perform the following tasks:

- Prevent devices from accessing explicit and inappropriate web content.
- Restrict Internet usage during specific time periods.
- Restrict and allow access to specific websites.

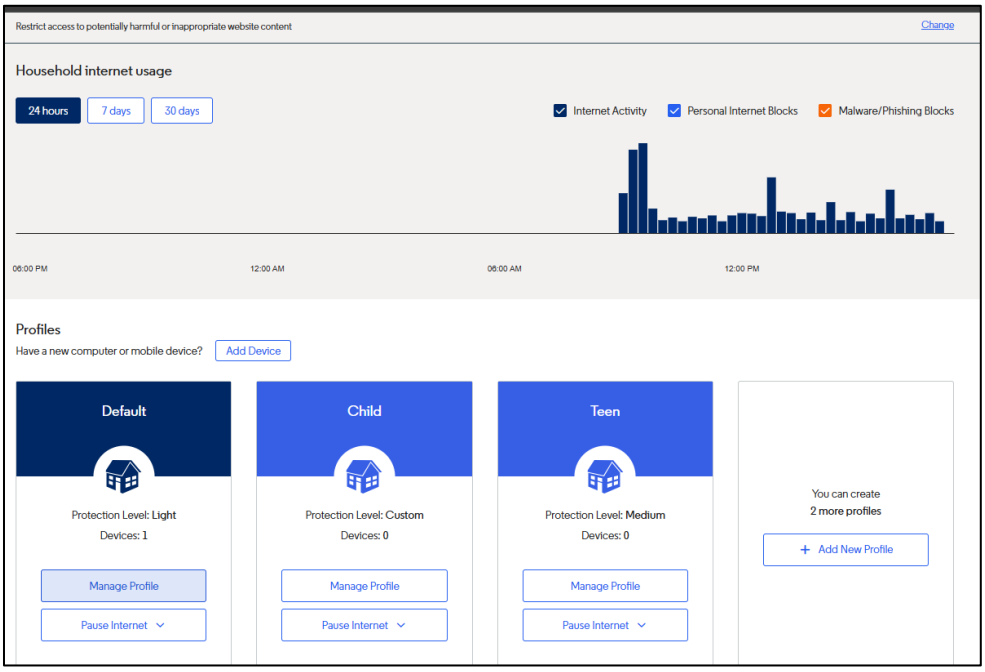
You manage web filtering settings on the following Advanced Security service pages:

- The "Profile details" page—The "Profile details" page contains controls for managing the following profile settings:
    - Which categories are allowed or restricted. See the "Managing Protection Levels and Content Categories" section for details about managing the content categories a profile allows and restricts.
    - The "Homework Time" schedule further restricts the content categories devices can access during a specific time period. See the "Set a 'Homework Time' Schedule" section for details about creating and managing Homework Time schedules.
    - The "Internet off" schedule disables internet access on devices during a specified time period. See the "Disable Internet Access for a Specified Time Period" section for details about creating and managing Internet off schedules.
    - Whether SafeSearch is enabled. See the "Managing Search Protection" section to enable or disable SafeSearch protection on the devices associated with a profile.
    - Which domains the profile blocks or allows (in addition to the domains in the global block and allow list). See the "Managing Profile-specific Block and Allow Lists" section for details about adding domains to and removing domains from profile-specific block and allow lists.

  In addition, the "Profile details" page shows the devices the profile is managing.

To access the “Profile details” page for a profile, click the **Manage Profile** button that is located on the desired profile tile (located on the Advanced Security home dashboard). Figure 4-1 shows where the **Manage Details** button is located on a profile tile.

Figure 4-1: How to Access the "Profile details" Page for a Profile



- The **"**Block & allow lists" page—Use the **"**Block & allow lists" page to add domains to your global block and allow lists. See the "Managing Block and Allow Lists" section for details. You can access the **"**Block & allow lists" page from the **services** drop-down menu or the page selector that appears on every configuration page (see Figure 4-2 for examples).

Figure 4-2: Access the "Block & allow lists" Page

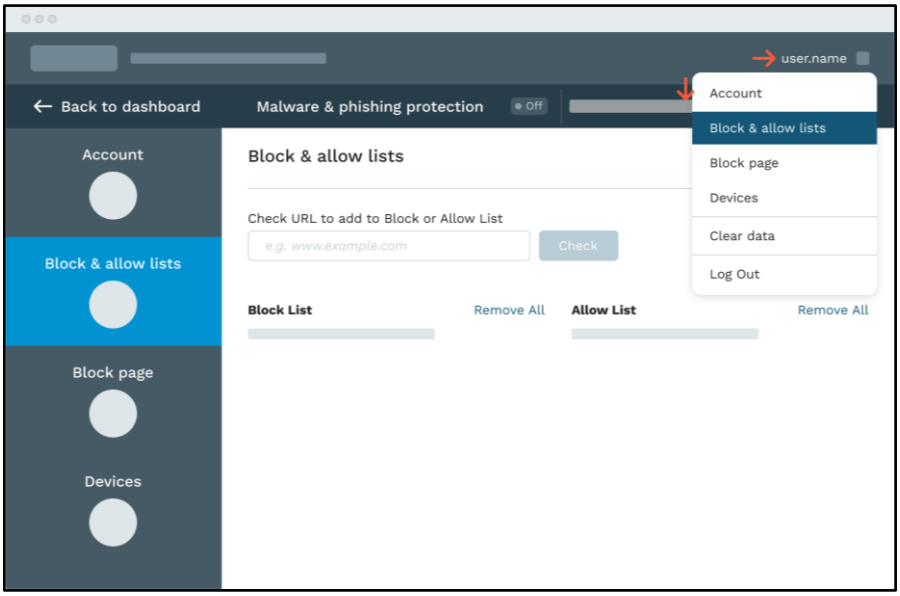


Figure 4-3 shows the "Profile details" page. This figure includes callouts where each number corresponds to a component described in Table 4-1.

Figure 4-3: Example "Profile details" Page

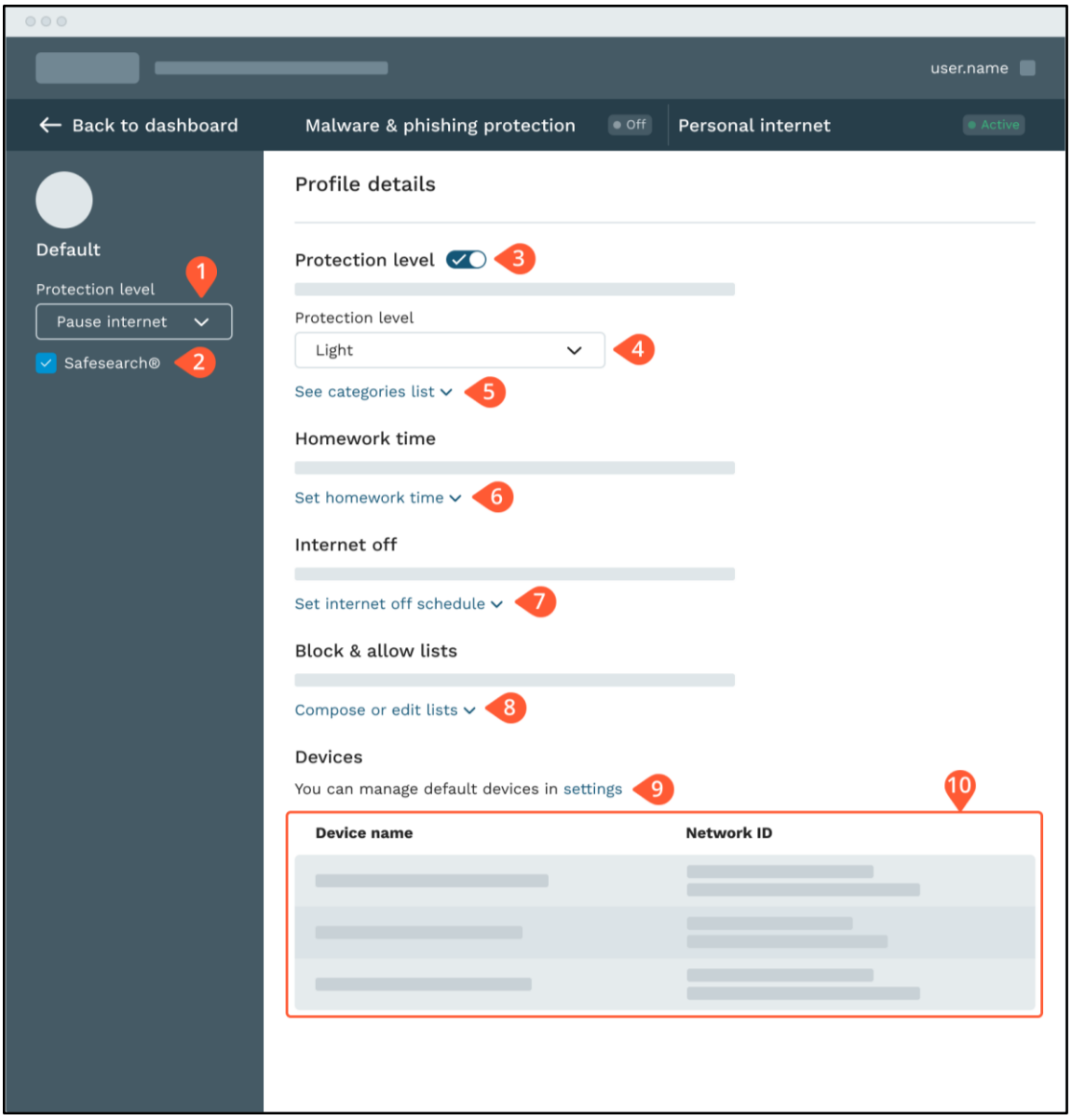

user.name
Back to dashboard
Malware & phishing protection
Off
Personal internet
Active
Default
Protection level
Pause internet
Safesearch®
1
2
Profile details
Protection level
3
Protection level
Light
4
See categories list
5
Homework time
Set homework time
6
Internet off
Set internet off schedule
7
Block & allow lists
Compose or edit lists
8
Devices
You can manage default devices in settings
9
10
Device name
Network ID

Table 4-1: "Profile details" Page Components

Callout	Component	Description
1	**Pause Internet** drop-down menu	Temporarily disables Internet access for a predetermined time period. Click the **Pause Internet** button to open a drop-down menu from which you can select on of the following time periods: ● **10 minutes** ● **1 hour** ● **3 hours** ● **24 hours** Internet access stops as soon as you select the time period from the **Pause Internet** drop-down menu.
2	SafeSearch checkbox	Indicates whether the Google, YouTube, and Bing SafeSearch features are enabled on devices attached to the selected profile. Clicking inside the checkbox changes the SafeSearch setting as follows: ● A checkmark indicates SafeSearch is enabled. When SafeSearch is enabled, the Advanced Security service hides explicit content from Google, YouTube, and Bing searches, making those search engines safer for children to use. ● A clear checkbox indicates SafeSearch is disabled. **NOTE:** Hover your cursor over the **question mark** (next to the checkbox) to see a pop-up description of what SafeSearch does when enabled. Clicking the **question mark** toggles the SafeSearch setting between enabled (the checkbox has a checkmark) and disabled (the checkbox is clear).
3	"Protection Level" toggle	Restricts and allows access to the websites blocked by the protection level assigned to the profile.

4	“Protection Level” drop-down selector	Specifies the protection level applied to the devices attached to the profile, where each level has a unique list of allowed and blocked content categories. Use the selector to apply a different protection level to the devices. You can apply the preset level of controls, or you can create your own **Custom** set of blocked and allowed categories. Changing the level automatically opens the Categories List for the level. To see the Categories Lists without changing the protection level, click the Set Categories List drop-down arrow described in callout 5. **NOTE:** The preset protection levels are preset; changing a preset category setting resets the profile's protection level to **Custom**. You can, however, further restrict the categories for a protection level. For example, you can set a “Homework Time” schedule that blocks social media websites during a specific time period only; when the “Homework Time” schedule is not being enforced, devices can access social media websites.
5	**Set Categories List** drop-down arrow	Toggle that hides and expands the Categories List settings for the selected protection level (described in callout 4). Expanding the Categories List displays a list of content categories, along with the status of each category (whether websites falling under the category are blocked or allowed). See the “Managing protection Levels and Content Categories” section for details.
6	**Set Homework Time** drop-down arrow	Toggle that hides and expands the controls for setting a “Homework Time” schedule for devices attached to the profile. A “Homework Time” schedule dictates whether devices can access websites that fall under the specified content categories during a specified timeframe. See the “Set a “Homework Time” schedule” section for details.
7	**Set Internet Off Schedule** drop-down arrow	Toggle that hides and expands the controls for setting an “Internet Off” schedule for devices attached to the profile. An “Internet Off” schedule dictates whether the associated devices can access the Internet during the specified timeframe. See the “Disable Internet Access for a Specified Time Period” section for details.
8	**Compose or Edit Lists** drop-down arrow	Toggle that hides and expands the controls for adding websites to the block and allow lists associated with the profile. See the “Managing Block and Allow Lists” section for details.
9	**Settings** link	Opens the “Devices” page when clicked. See Chapter 5, “Managing Devices” for details on managing the devices in your service.

10	“Devices” table	If the profile has devices attached, this section includes a table listing those devices along with general information about each device: ● The device name ● An icon indicating how the device is connected to your network (whether the device is roaming, using your WiFi, and so forth). ● The Network ID associated with the device. See Chapter 5, “Managing Devices” for details on devices and device management.

Managing Protection Levels and Content Categories

The “Profile details” page provides controls for restricting access to websites containing different types of content. This section describes content categories and provides instructions for restriction and allowing different content types.

Before applying protection levels and and setting content category status for the devices accessing your service, you need to understand the following information:

- The different types of web “content categories” you can restrict and allow.
- The different protection levels you can apply to the devices in your service.

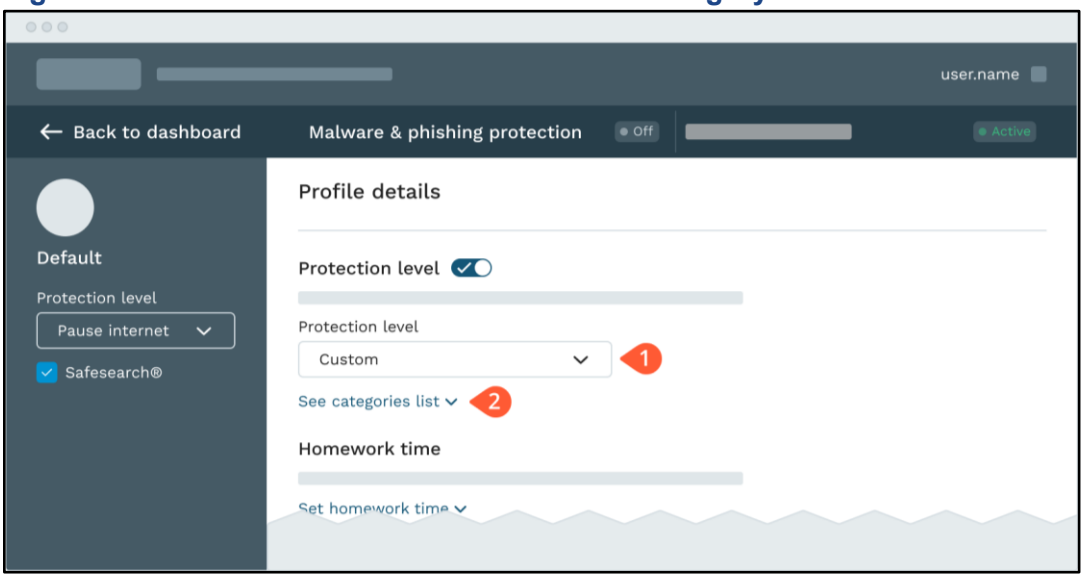
This information is provided in the sections that follow.

Understanding Web Filter Content Categories

You can control the types of content the devices in your service can access. Your service provider determines the content categories your service can block and allow, and you determine which devices can access websites falling under those content categories. To see the content categories you can allow or block, access the “Profile details” page for a profile (as demonstrated in Figure 4-1) and perform the following steps:

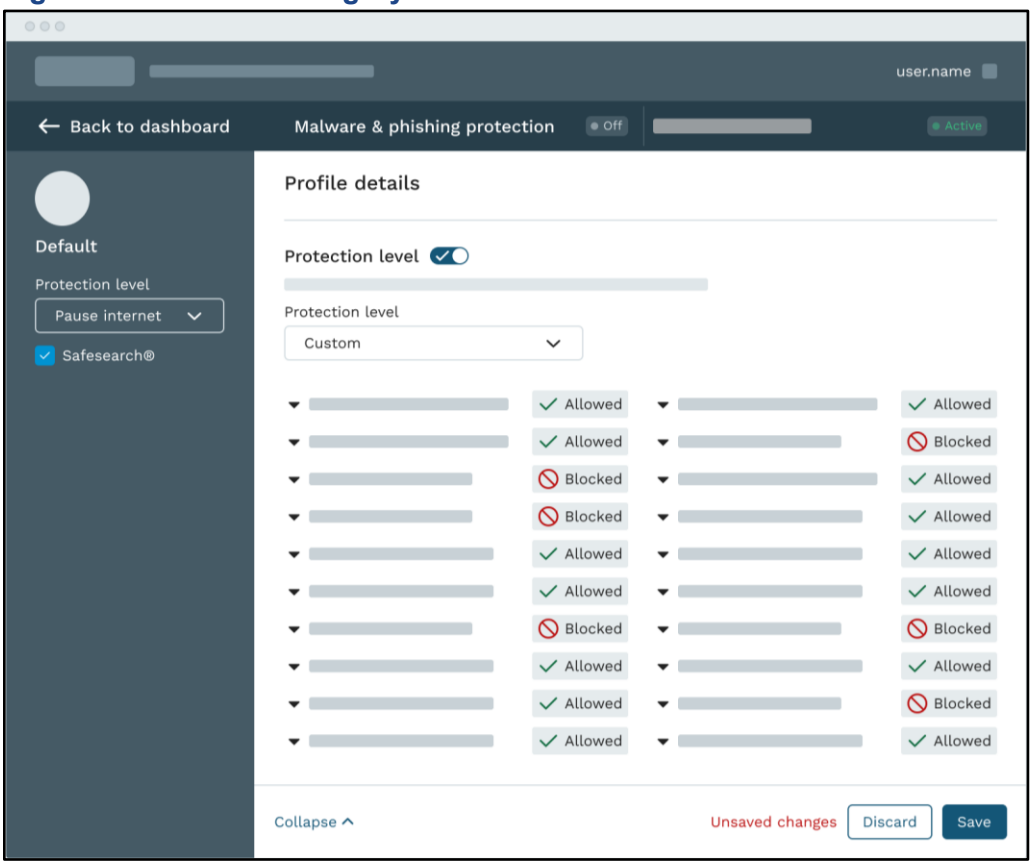
1. Select the **Custom** protection level from the “Protection level” drop-down list as demonstrated by callout 1 in Figure 4-4.
2. If the category list is hidden, click the **See categories list** toggle to example the categories list as demonstrated by callout 2 in Figure 4-4.

Figure 4-4: Access the Customizable Content Category List for a Profile



When the category list is expanded, you can see all content categories you can block and allow as demonstrated in Figure 4-5.

Figure 4-5: Custom Category List for a Profile



Understanding Protections Levels

When setting up a profile, you assign a level of protection to that profile. For example, your service might have a light level of protection that provides minimal protection, a moderate level of protection where the service restricts more content categories (in addition to the categories that are blocked for the light level of protection), and a strict level of protection, where most content categories are not allowed.

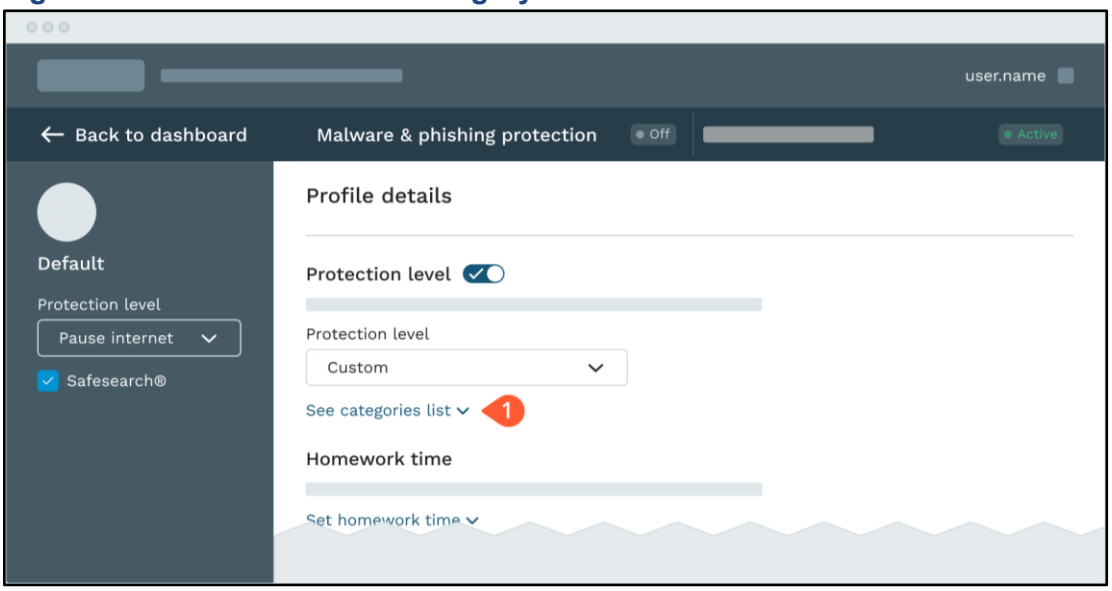
In addition to the preconfigured protection levels, your Advanced Security service offers a **Custom** level of protection for which you specify the types of content devices attached to the profile can access.

Setting Protection Level Content Restrictions

Use the following steps to set the protection level and content restrictions for devices in your service:

1. On the “Profile details” page, click the **Set Categories List** expansion toggle to expand the content category list. Figure 4-6 shows where the **Set Categories List** expansion toggle is located on the “Profile details” page:

Figure 4-6: View the Content Category List for a Profile



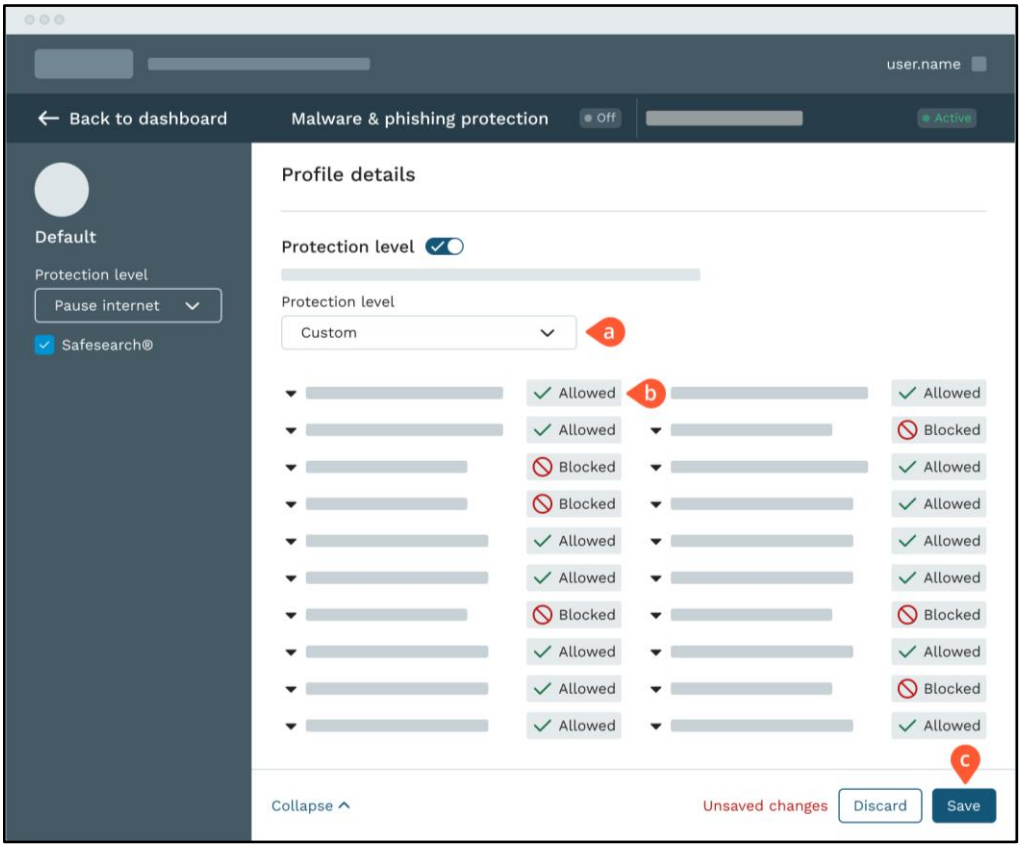
NOTE: Figure 4-1 demonstrates how to access the “Profile details” page for a profile.

2. You can perform the following tasks on the “Profile details” page:
    a. Review the content category statuses for each protection level by selecting a protection level from the “Protection Level” drop-down list. **Callout a** in Figure 4-7 shows where the “Protection Level” drop-down list is located on the “Profile details” page.
    b. Change the status level of any content category by clicking the **Allowed** or **Blocked** status toggle that appears next to that content category. A green checkmark indicates a content category is allowed, while a red prohibition icon indicates a category is blocked. In Figure 4-7, callout b points to a status toggle that is set to **Allowed**.
    c. Click the **Save** button to save any content category status changes made for the selected protection level. Callout c in Figure 4-7 shows where the **Save** button is located on the “Profile details” page.

NOTE: The **Custom** protection level initially allows all content categories until a user manually changes one or more content category settings.

Figure 4-7 demonstrates how to manage protection levels and content categories for your service.

Figure 4-7: Manage the Protection Levels and Content Categories for a Profile



NOTE: Changing the status of any content category in a preset protection level automatically changes the protection level to be **Custom**.

Caution! Be sure to save your configuration before navigating to another page in the Advanced Security service; the application does not save your protection level configuration until you click the **Save** button.

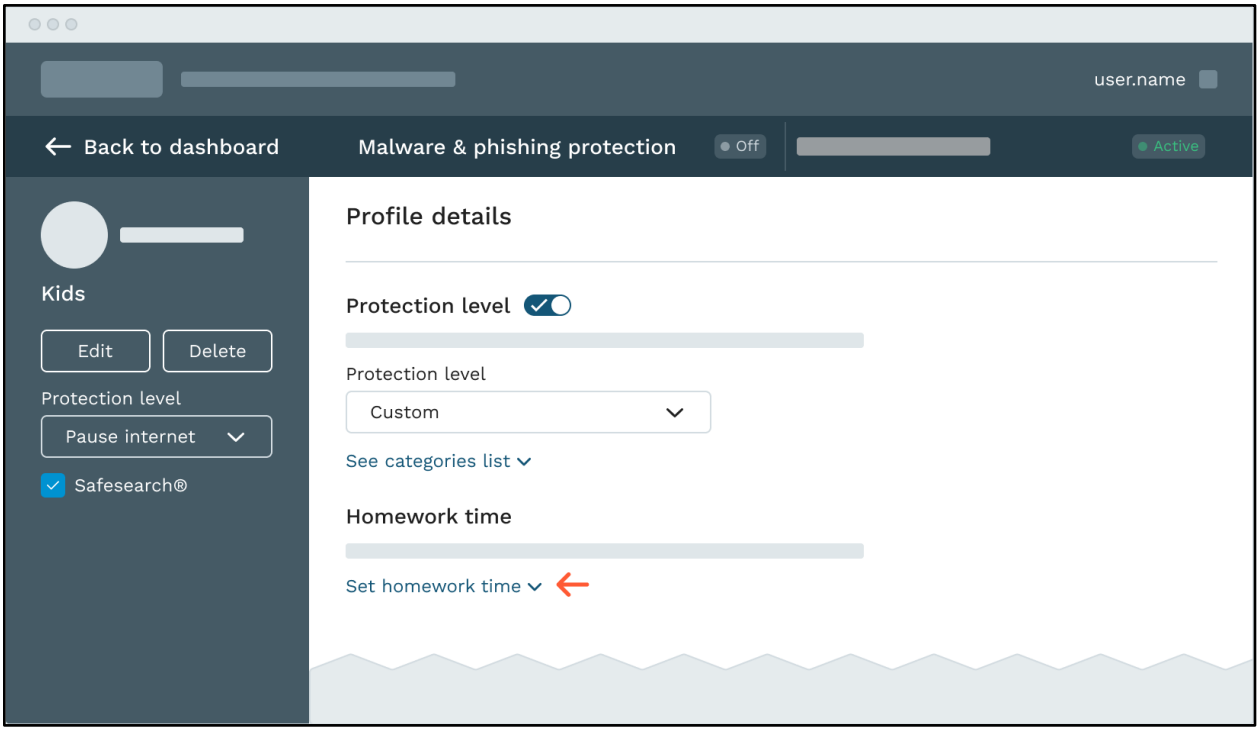
Set a “Homework Time” Schedule

If desired, you can set up a “Homework Time” schedule which further restricts the content categories devices can access during a specific time period. For example, you can create a “Homework Time” schedule that blocks social media websites during early after-school hours only. You create and manage “Homework time” schedules on the **“**Profile details” page for a specific profile; Figure 4-1 demonstrates how to access the “Profile details” page for a profile. After a schedule is set, the Advanced Security service enforces that schedule on all devices attached to the profile.

Use the following steps to set up a “Homework time” schedule:

1. On the **“**Profile details” page, locate the “Homework time” section. If the “Homework time” section is collapsed, click the **Set homework time** expansion toggle to expand the “Homework time” section as demonstrated in Figure 4-8:

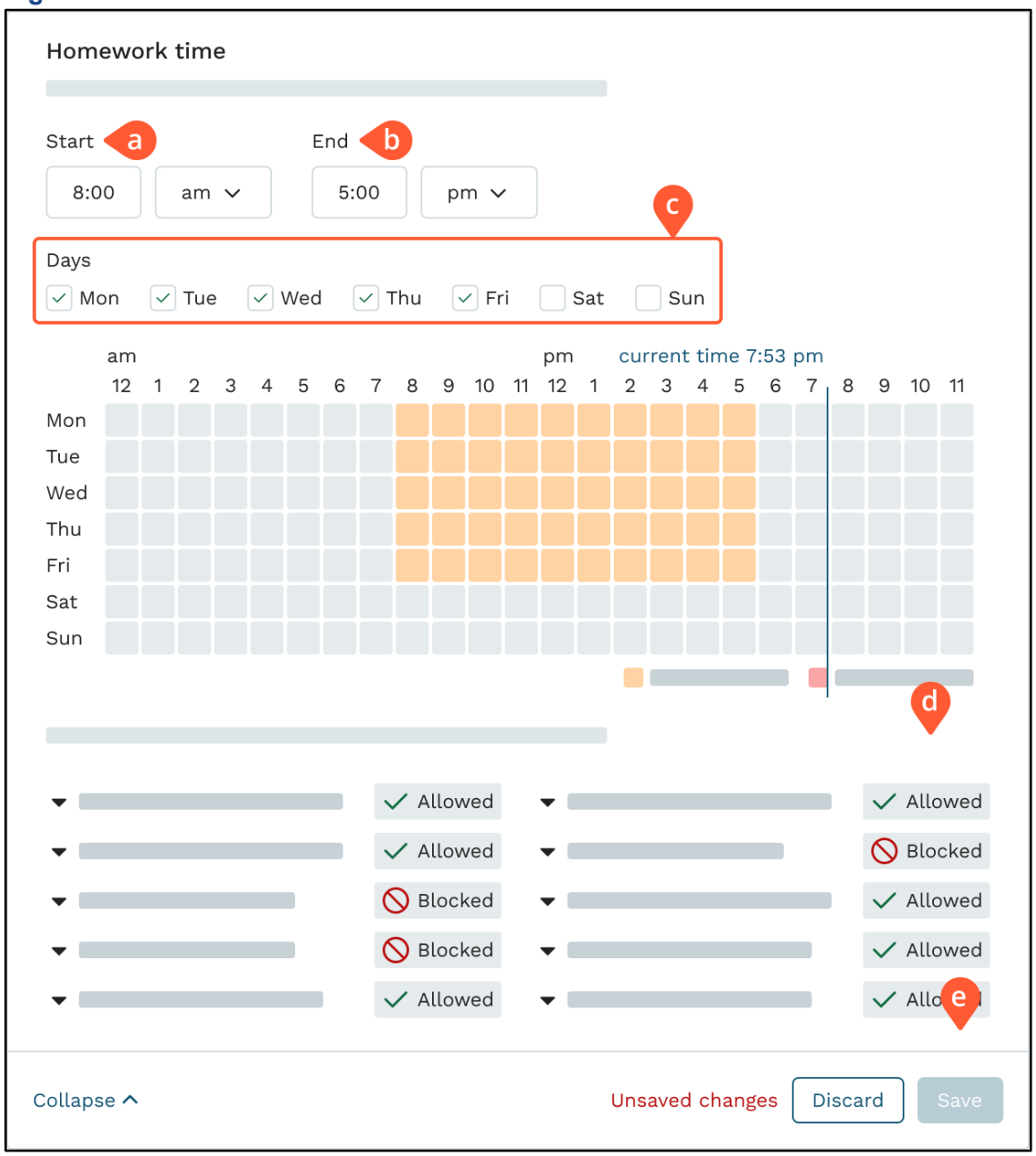
Figure 4-8: View the “Homework time” Schedule for a Profile



2. When the “Homework time” section is expanded, the “Homework time” schedule controls appear under the toggle as shown in Figure 4-9; perform the following tasks to create or modify a “Homework time” schedule:
    a. In the “Start” field, specify the time at which to start enforcing the “Homework Time” schedule (see callout a in Figure 4-9). Select **am** or **pm** from the drop-down list to indicate whether the start time occurs before or after noon.
    b. In the “End” field, specify the time at which to stop enforcing the “Homework Time” schedule (see callout b in Figure 4-9). Select **am** or **pm** from the drop-down list to indicate whether the end time occurs before or after noon.
    c. In the “Days” section, add checkmarks in the checkboxes that appear next to the days of the week on which to enforce the schedule (see callout c in Figure 4-9). The calendar located under the checkboxes reflects the time period you designate as “Homework Time.”

       NOTE: As you specify a “Start” time, “End” time, and days for the schedule, the calendar that is located under the “Days” checkboxes reflects your schedule settings.
    d. Select the categories you want to block (in addition to those categories which are already blocked as specified in the “Setting Protection Level Content Restrictions” section); see callout d in Figure 4-9. Click the **Blocked** or **Allowed** status toggle that appears next to any content category to change the status for that category. A green checkmark indicates a category is allowed, while a red prohibition icon indicates a category is blocked.
    e. Click the **Save** button to save and start enforcing the “Homework time” schedule (see callout e in Figure 4-9).

Figure 4-9: "Homework Time" Schedule Controls



NOTE: The Advanced Security service does not enforce your new "Homework Time" schedule until you click the **Save** button.

Disable Internet Access for a Specified Time Period

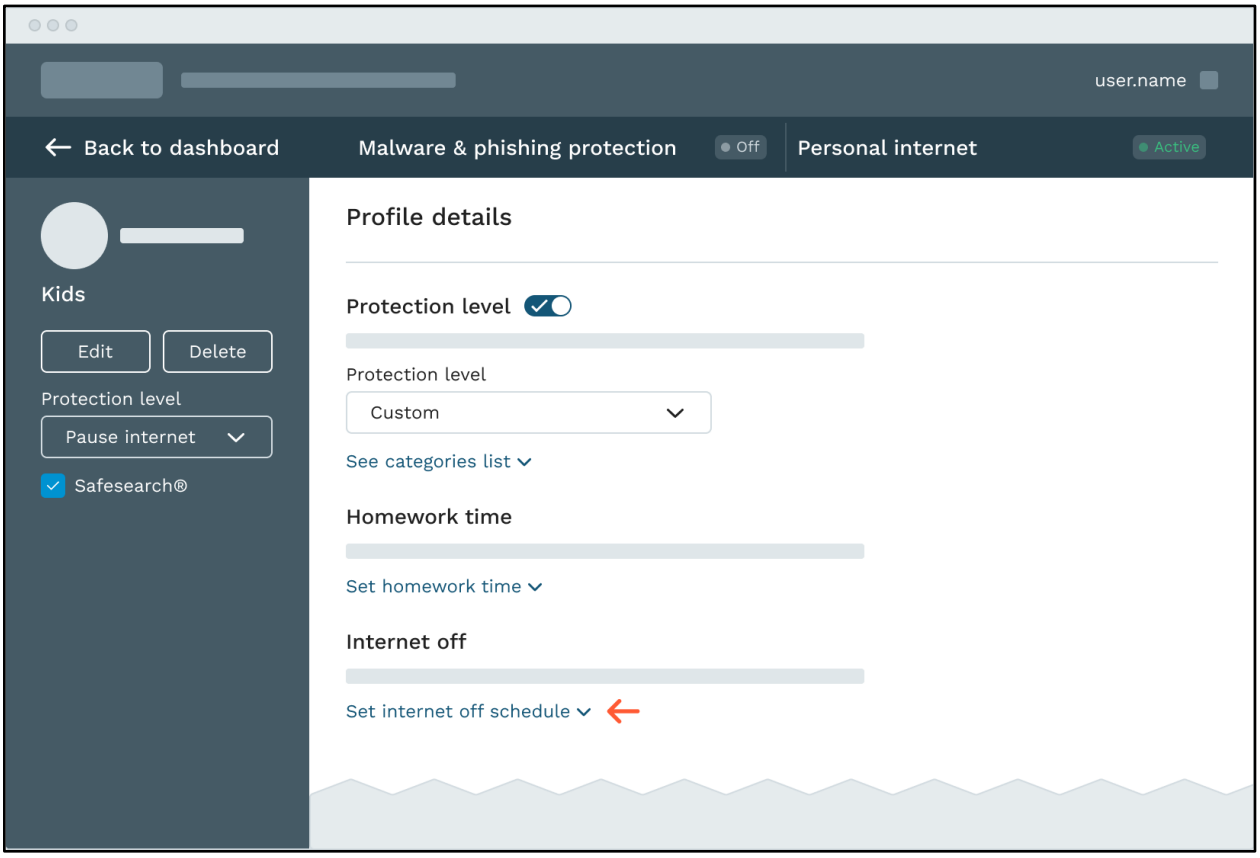
If desired, you can set up an “Internet off” schedule which prevents devices from accessing the Internet during a specified time period. For example, you can create an “Internet off” schedule that prevents the devices belonging to your children from accessing the Internet after 8:00 PM on school nights. After a schedule is set, the
Advanced Security service enforces that schedule on all devices attached to the profile.

You create and manage “Internet off” schedules on the **“**Profile details” page for a specific profile; Figure 4-1 demonstrates how to access the “Profile details” page for a profile.

Use the following steps to set up an “Internet off” schedule:.

1. On the **“**Profile details” page, locate the “Internet off” section. If the “Internet off” section is collapsed, click the **Set Internet off schedule** expansion toggle to expand the “Internet off” section as demonstrated in Figure 4-10.

Figure 4-10: View the “Internet off” Schedule for a Profile



2. When the “Internet off” section is expanded, the “Internet off” schedule controls appear under the toggle as shown in Figure 4-11; perform the following tasks to create or modify an “Internet off” schedule:

    a. In the “Start” field, specify the time at which to start enforcing the “Internet off” schedule (see callout a in Figure 4-11). Select **am** or **pm** from the drop-down list to indicate whether the start time occurs before or after noon.

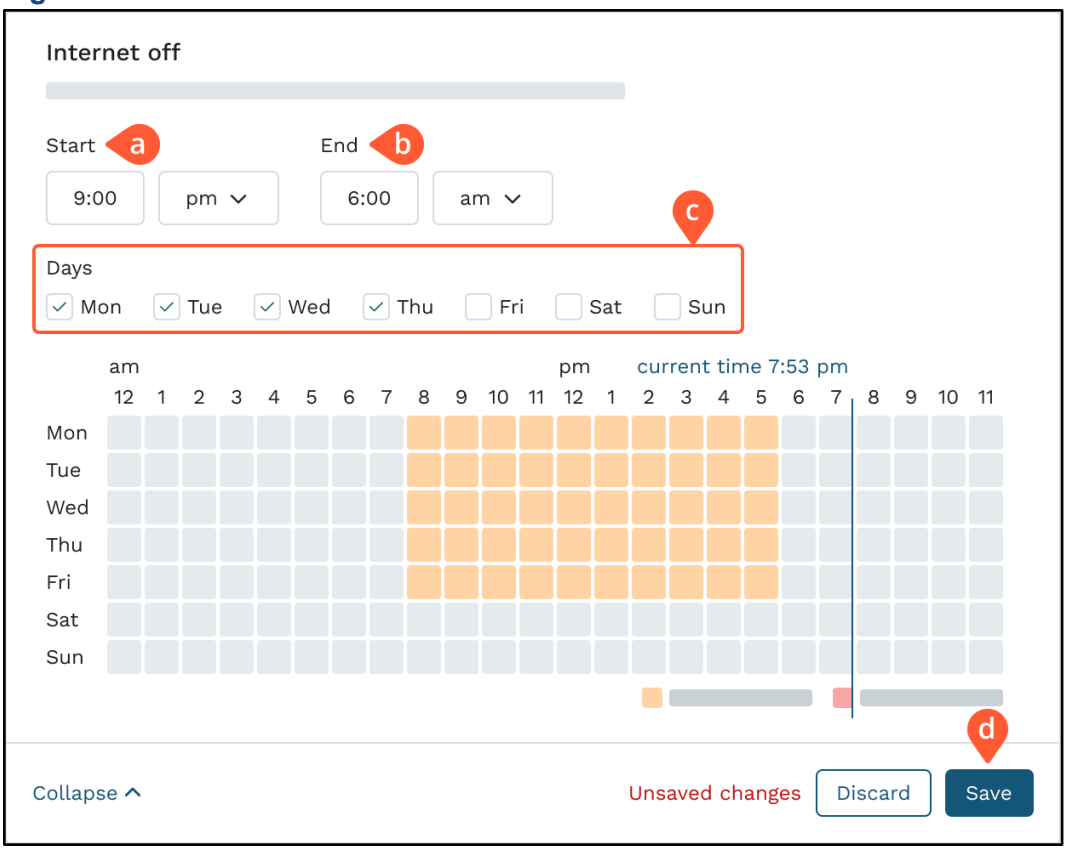
    b. In the “End” field, specify the time at which to stop enforcing the “Internet off” schedule (see callout b in Figure 4-11). Select **am** or **pm** from the drop-down list to indicate whether the end time occurs before or after noon.

    c. Add checkmarks in the checkboxes next to the days of the week on which to enforce the schedule (see callout c in Figure 4-11). The calendar that is located under the checkboxes reflects the time period you specified to disable Internet access on the selected days.

    d. Click the **Save** button to save and start enforcing the “Homework Time” schedule (see callout d in Figure 4-11).

    NOTE: The Advanced Security service does not enforce your new “Internet off” schedule until you click the **Save** button.

Figure 4-11: “Internet off” Schedule Controls



NOTE: The Advanced Security service does not enforce your new “Internet off” schedule until you click the **Save** button.

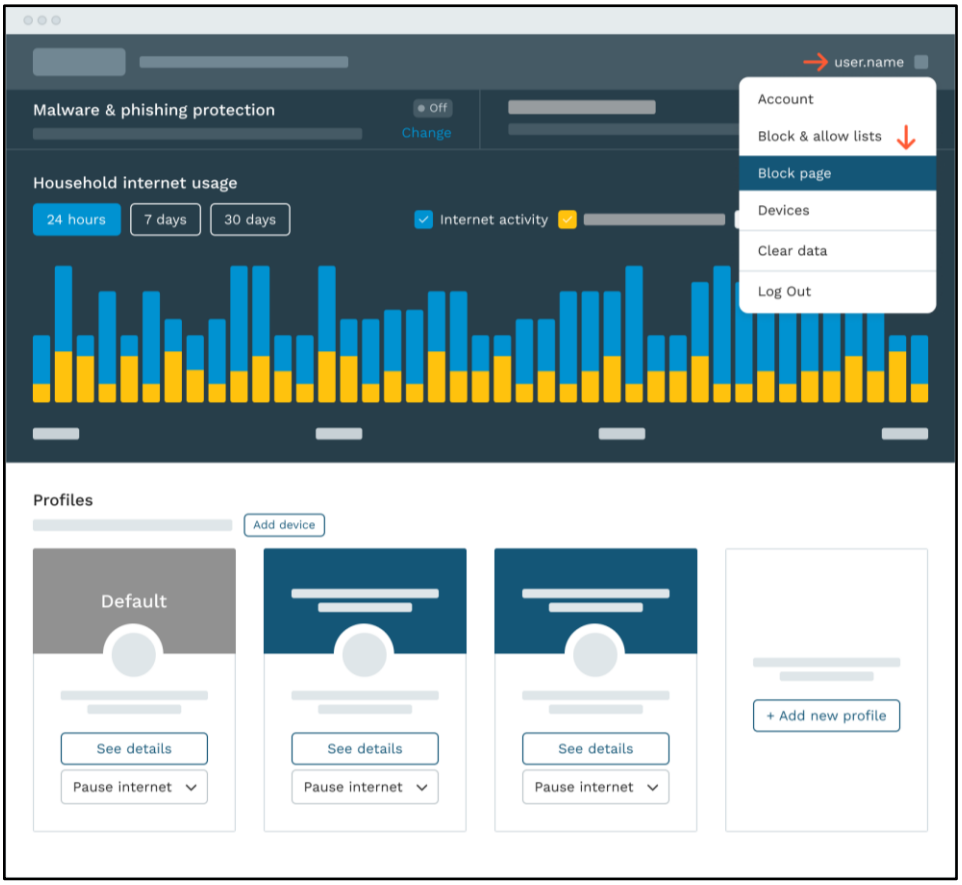
Manage Malware and Phishing Protections

Enabling malware and phishing protection protects the devices in your service from phishing attacks and accessing infected websites. When a device attempts to access an infected website, that device encounters a block page. Malware and phishing protection is enabled by default.

The “Block page” settings provide a toggle for enabling and disabling malware and phishing protection on the devices in a selected profile.:

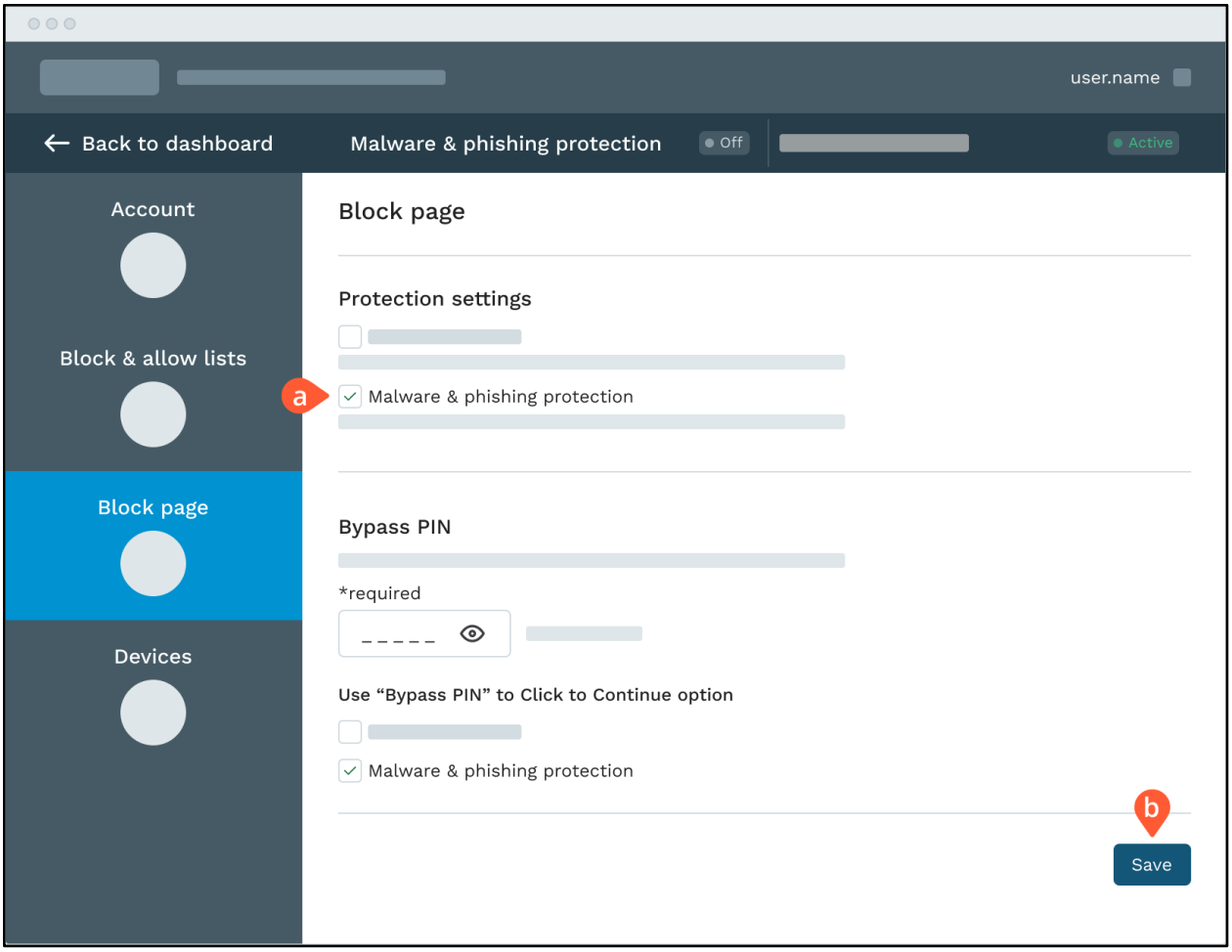
1. Access the **“**Block page” settings from the **services** drop-down list as demonstrated in Figure 4-12:

Figure 4-12: Access Block Page Settings



2. In the “Block page” settings, perform the following tasks:
    a. Click inside the “Malware & phishing protection” checkbox to enable or disable the malware and phishing protection service. A checkmark indicates malware and phishing protection is enabled on all devices in your service. Clear the checkbox to disable malware and phishing protection on all devices. Callout a in Figure 4-13 shows where the “Malware & phishing protection” checkbox is located on the “Block page” settings page.
    b. Click the **Save** button to save your changes. Callout b in Figure 4-13 shows where the **Save** button is located on the “Block page” settings page.

Figure 4-13: How to Enable and Disable Malware and Phishing Protection



NOTE: The Advanced Security service does not enforce your configuration until you click the **Save** button.

Managing Search Protection

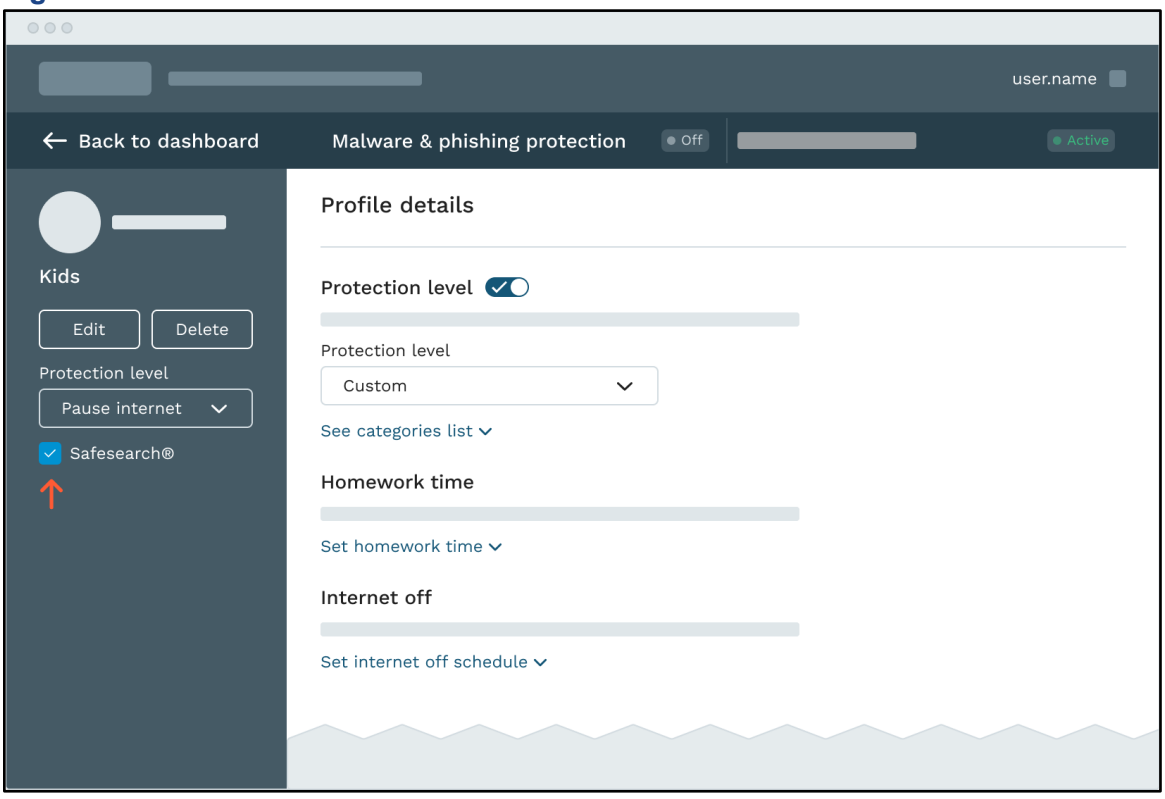
You can use the Advanced Security service to provide network-based search protection support to family and guests through Google SafeSearch, Youtube Restricted Mode, and Bing SafeSearch. All search protections are enabled by default, but you can disable (and re-enable) whether a particular profile enforces search protection. When SafeSearch protection is enabled, each search engine enforces SafeSearch results at the network level and individual users cannot disable SafeSearch protection protections on their devices.

NOTE: If your service has multiple profiles, you can enable and disable SafeSearch protection on a per-profile basis.

Use the following steps to enable or disable search protections on all devices attached to a specific profile:

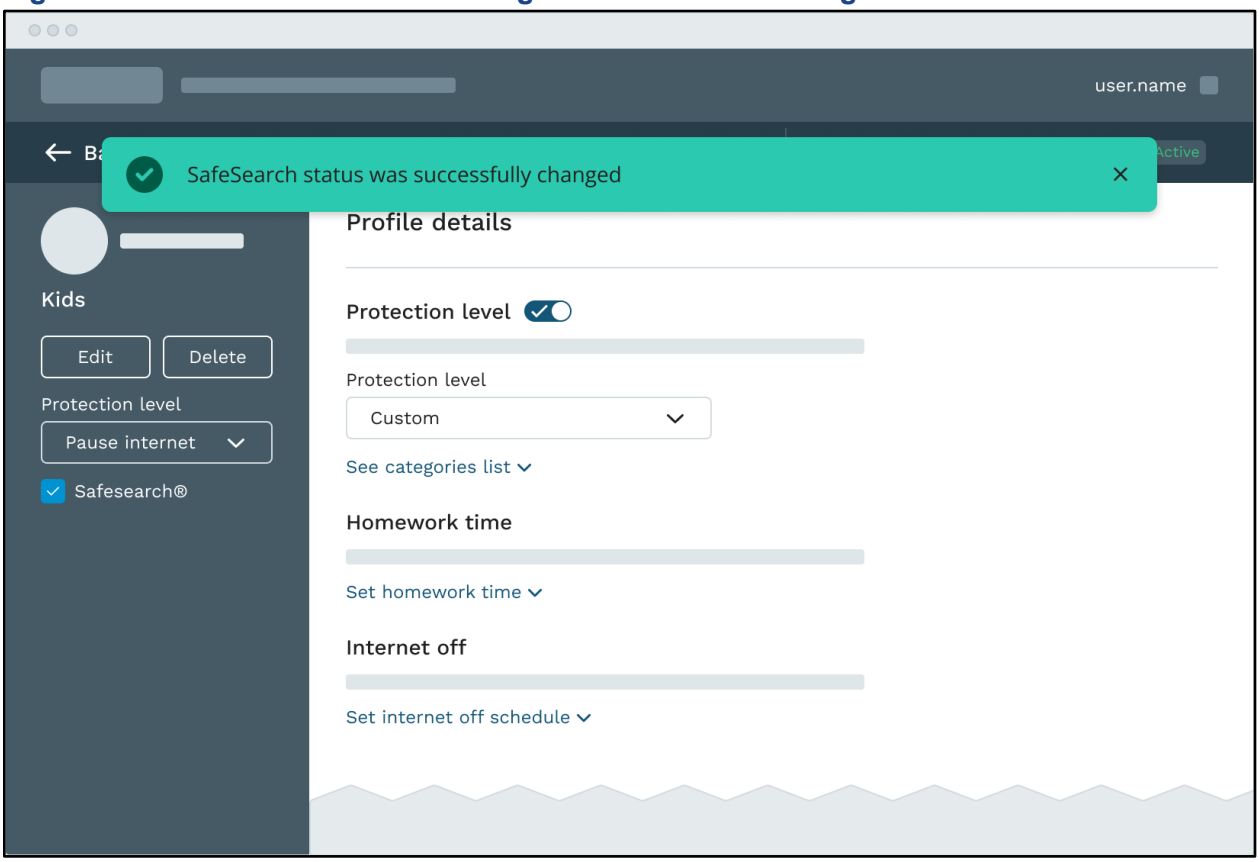
1. Access the **"**Profile details" page. Figure 4-1 demonstrates how to access the "Profile details" page for a profile.
2. On the **"**Profile details" page, locate the **SafeSearch checkbox** and click inside the checkbox to enable or disable SafeSearch protections as desired. A check mark indicates Safesearch protections are enabled; clear the check box to disable SafeSearch protections. Figure 4-14 shows where the **SafeSearch checkbox** is located on the "Profile details" page:

Figure 4-14: How to Enable and Disable SafeSearch Protections



3. A message appears on the “Profile details” page indicating your change is successful; Figure 4-15 shows an example of the message.

Figure 4-15: SafeSearch Status Change Confirmation Message



The Advanced Security service starts enforcing your SafeSearch setting immediately.

Managing Block and Allow Lists

The Advanced Security service supports block and allow lists that determine whether devices can access particular websites. An allow list contains the websites devices can always access, while a block list contains the websites devices cannot access. Block and allow lists make it easy to restrict websites that do not belong to any restricted content categories. In addition, users can ensure the devices using the Advanced Security service can always access certain websites that might otherwise fall under a restricted content category.

The Advanced Security service provides controls for performing the following tasks:

- Check whether a domain appears in a block or allow list.
- Add domains and URLs to global or per-profile block or allow lists.
- Remove domains and URLs from global or per-profile block or allow lists.

Keep the following in mind when configuring global and per-profile block and allow lists:

- Each individual profile has its own unique block or allow list. When you attach devices to a particular profile, those devices inherit the block and allow lists from the profile. There is also a global profile that has block and allow list entries that apply to all profiles. In other words, you can block and allow individual domains globally (for all devices in your Advanced Security service) or per-profile (for devices belonging to a particular profile only). With multiple profiles, the Advanced Security service applies block and allow lists in following order of priority:

    1. Per profile allow lists

       Per profile allow lists have the highest priority and take precedence over global allow lists and all block lists.

    2. Global allow lists

       Global allow lists take precedence over global and per-profile block lists.

    3. Per-profile block lists

       Per-profile block lists take precedence over global block lists; global block lists have the lowest priority.

    4. Global block lists

       Global block lists have the lowest priority.

- When you add a domain to a block or allow list, the Advanced Security service blocks or allows all subdomains of the core domain. For example, if you add the domain *www..com* to a block list, the service blocks access to *news..com* and so forth.
- Although you can specify a subdomain when updating a block or allow list, the Advanced Security service automatically adds the entire core domain to the list.
- You can block or allow device access to Top Level Domains (TLDs), where the Advanced Security blocks every domain under that TLD. An example of a TLD is “ru” (the TLD for the country Russia). The Advanced Security treats “public suffix” sites (for example, “co.uk”) as TLDs.
- When entering TLDs, do not use beginning or ending “dots” (for example, specify **com** instead of **.com** and so forth). The Advanced Security service rejects CSV files containing TLDs or wildcards (for example, **“*.com**).

  NOTE: You cannot add TLDs to an allow list or upload TLDs in CSV files.

- You can configure block and allow lists that apply consistently or during a scheduled “Homework time” period only. For example, you can set a “Homework time” schedule that blocks social media websites during a specific time period only. See the “Set a “Homework time” Schedule” section for details.
- You cannot add a specific URL to an allow list; when you specify a URL to be added to an allow list, the Advanced Security service allows access to the entire domain.

There are two ways to add domains to block and allow lists:

- Manually add an individual domain to a block or allow list as described in the following sections:
    - To manually add a domain to a global block or allow list, see the “Add Domains to Global Block or Allow Lists” section.
    - To manually add a domain to a per-profile block or allow list, see the “Managing Profile-specific Block and Allow Lists” section. Per-profile block and allow lists are supported in multiple-profile Advanced Security services only.
- Create a CSV file containing the domains you want to allow or block and upload the list into your system.

Managing Global Block and Allow Lists

Global block and allow lists apply to all devices in your Advanced Security service. This section describes how to perform the following tasks:

- Add domains to global block and allow lists.
- Remove domains from global block and allow lists.

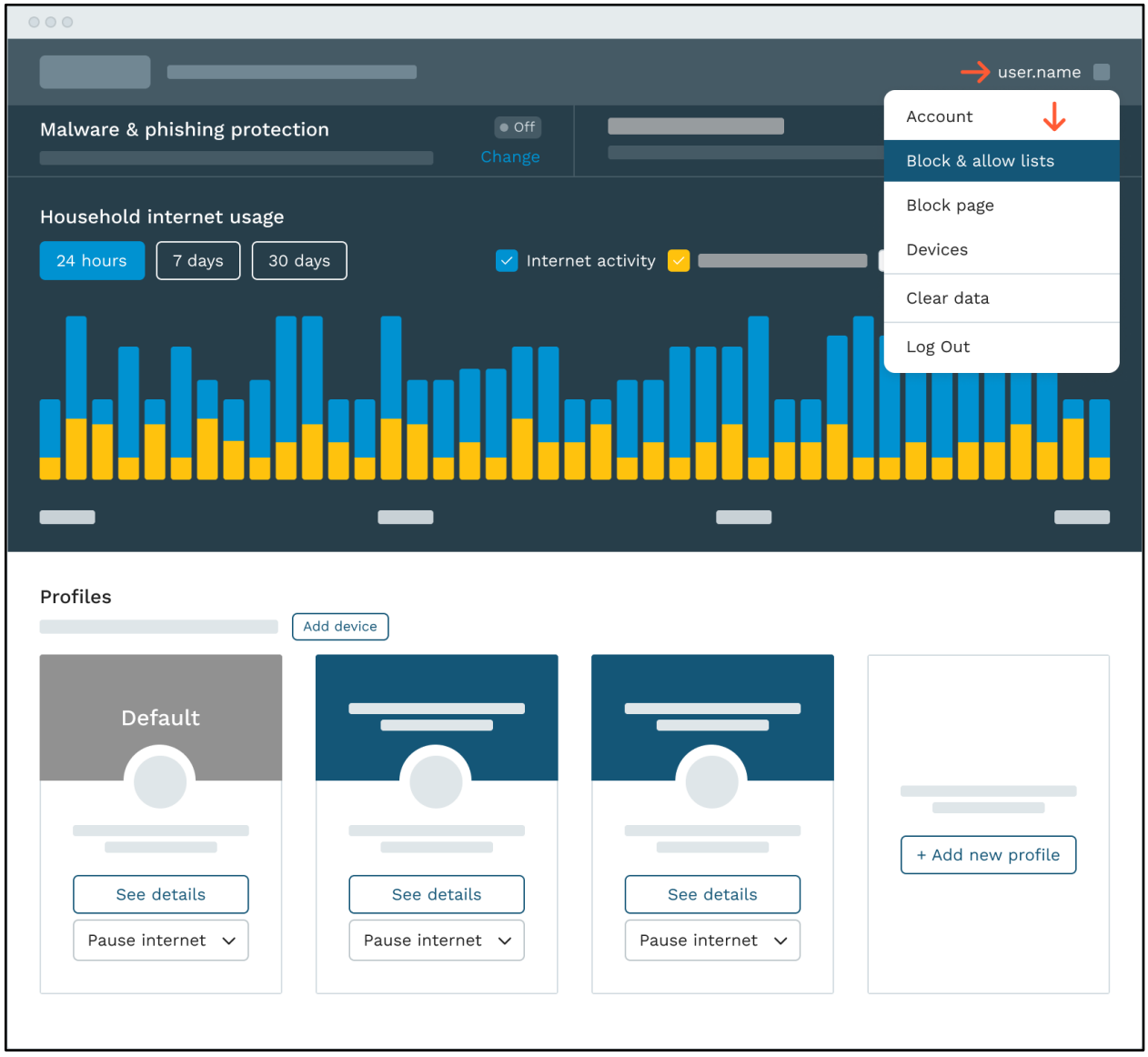
NOTE: This section describes how to configure and manage global block and allow lists only; to configure and manage profile-specific block and allow lists, see the "Managing Profile-specific Block and Allow Lists" section.

Add Domains to Global Block or Allow Lists

The steps that follow describe how to add domains to global block and allow lists; you can also use Step 1 through Step 2 to verify whether a website already appears in a block or allow list:

1. Select the **Block & allow lists** option from the **services** drop-down menu to access the "Block & allow lists" page. Figure 4-16 demonstrates how to access the "Block & allow lists" page:

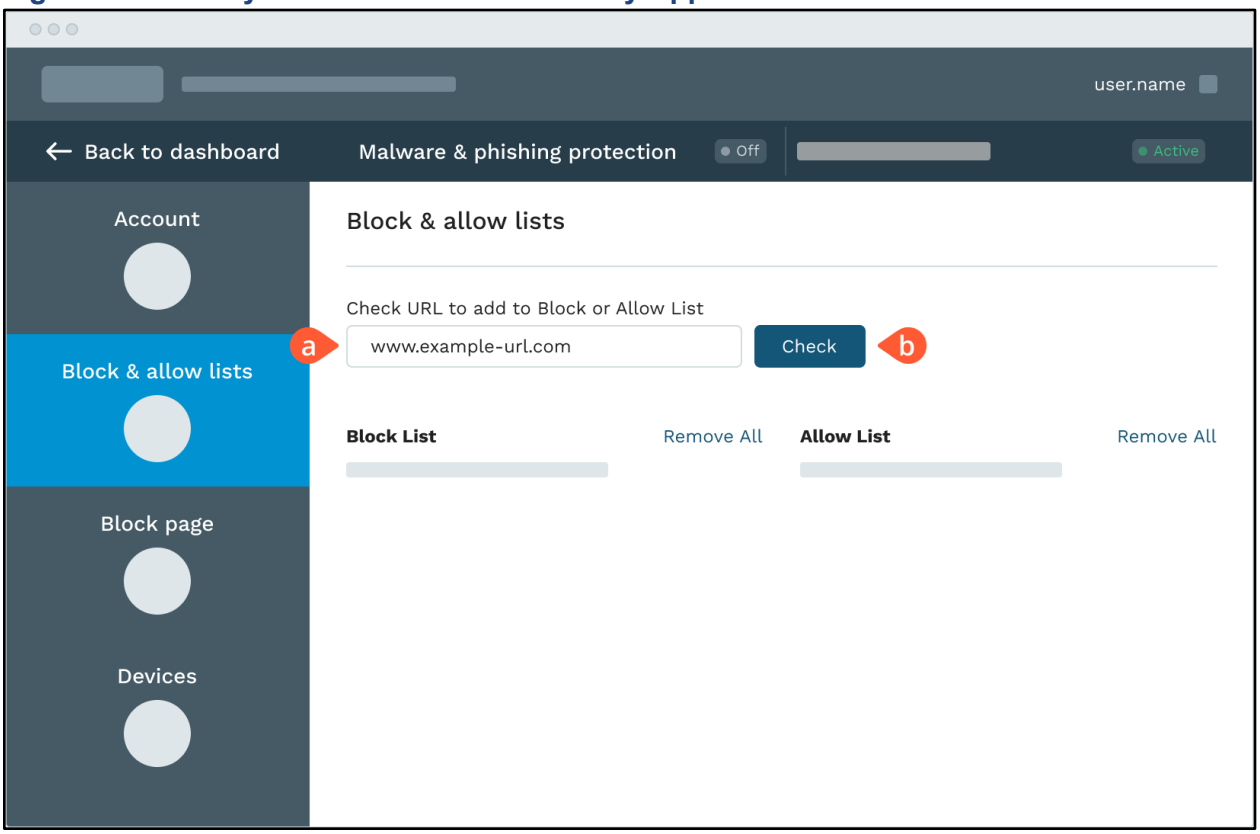
Figure 4-16: Access Block and Allow List Controls



2. In the “Block & allow lists” page, perform the following tasks to verify the desired domain does not already exist in your block or allow lists:
    a. In the “Check URL to add to Block or Allow List” field, type the domain you want to add to a block or allow list.
    b. Click the **Check** button to determine whether the domain already appears in a global block or allow list.

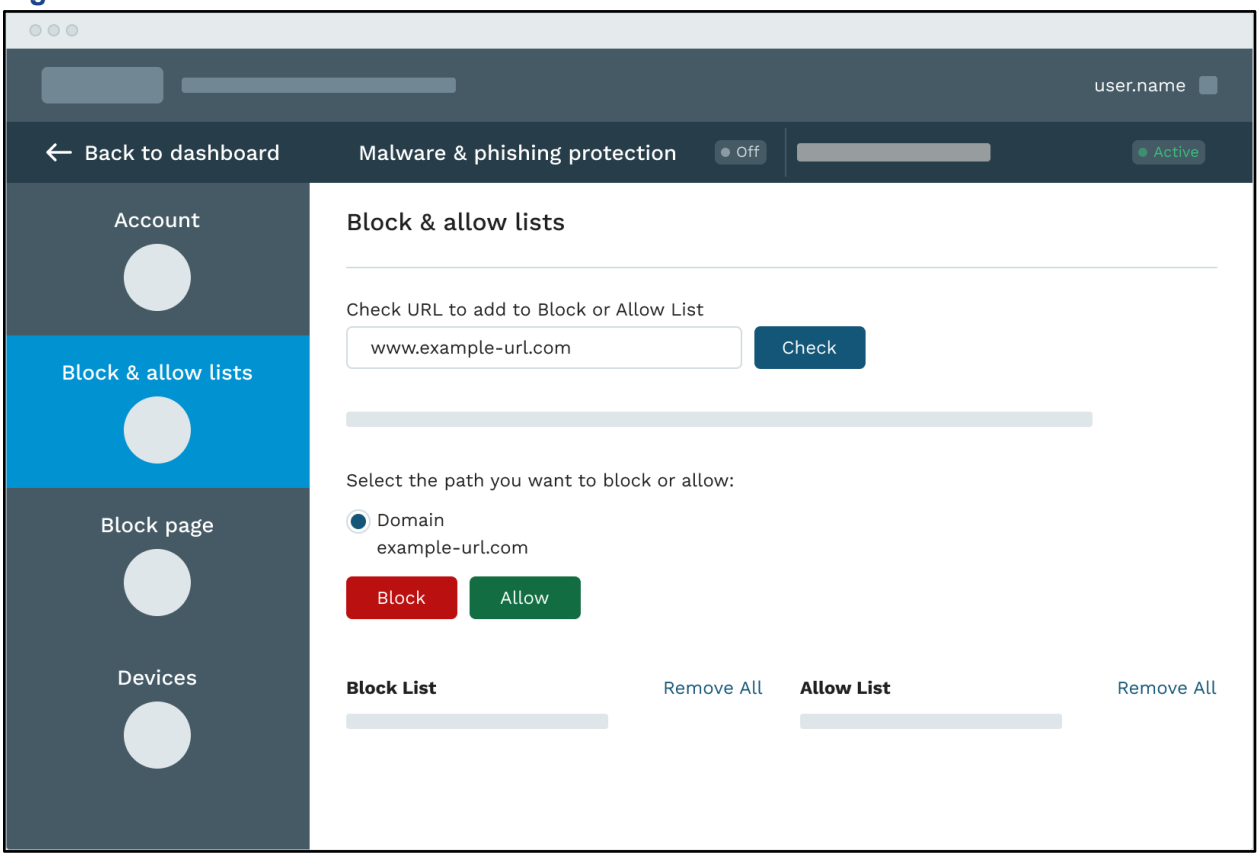
Figure 4-17 demonstrates how to perform Step a and Step b.

Figure 4-17: Verify Whether a Domain Already Appears in a Block or Allow List



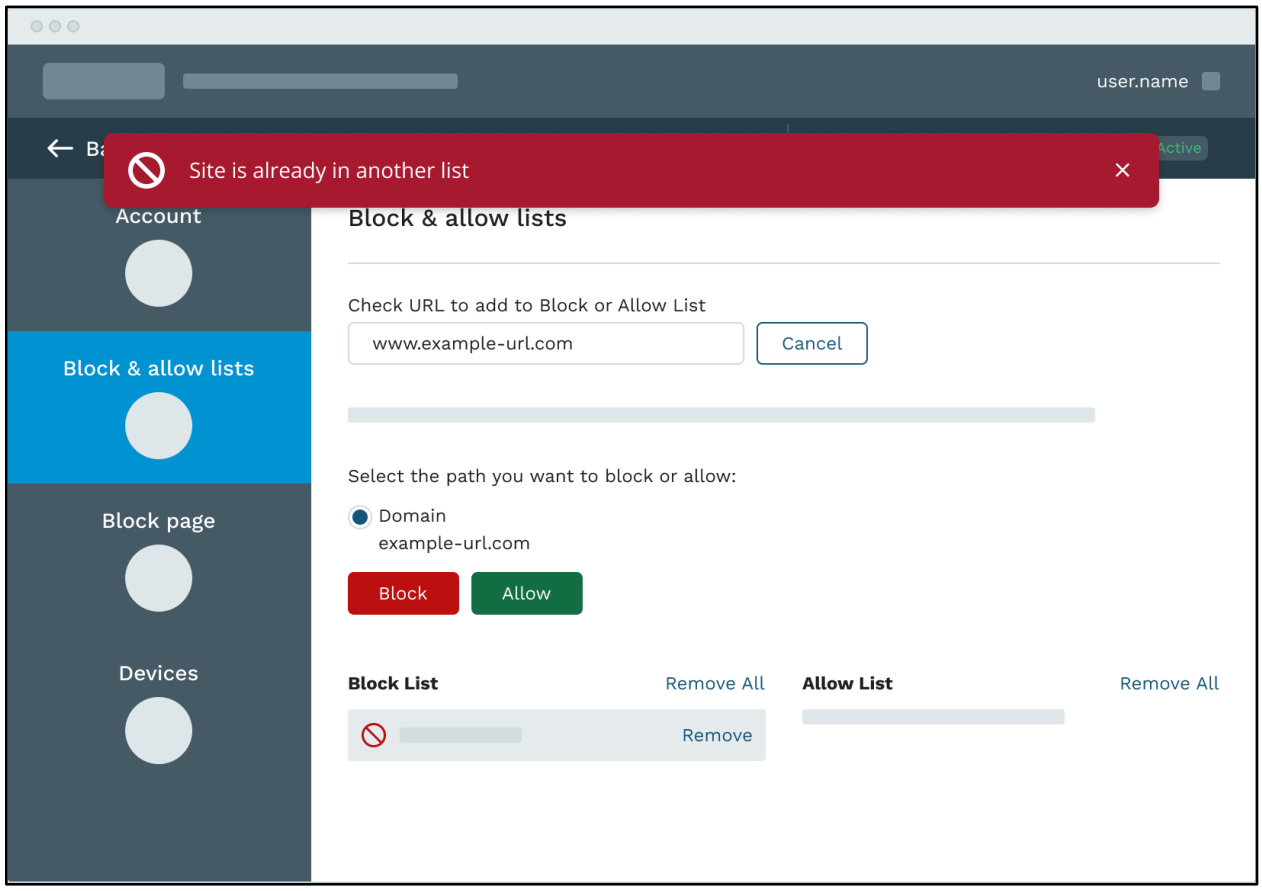
3. If the specified domain does not already exist in the global block or allow lists, the Advanced Security service prompts you to indicate whether to add the domain to the global block or allow list as demonstrated in Figure 4-18. Click the **Allow** button to add the domain to the global allow list; click the **Block** button to add the domain to the global block list:

Figure 4-18: Indicate Whether to Add a Domain to the Global Block or Allow List



If the domain already exists in a global block or allow list, an error message informs you that the domain already appears in a global block or allow list and the Advanced Security service does not add the domain to the selected list as demonstrated in Figure 4-19.

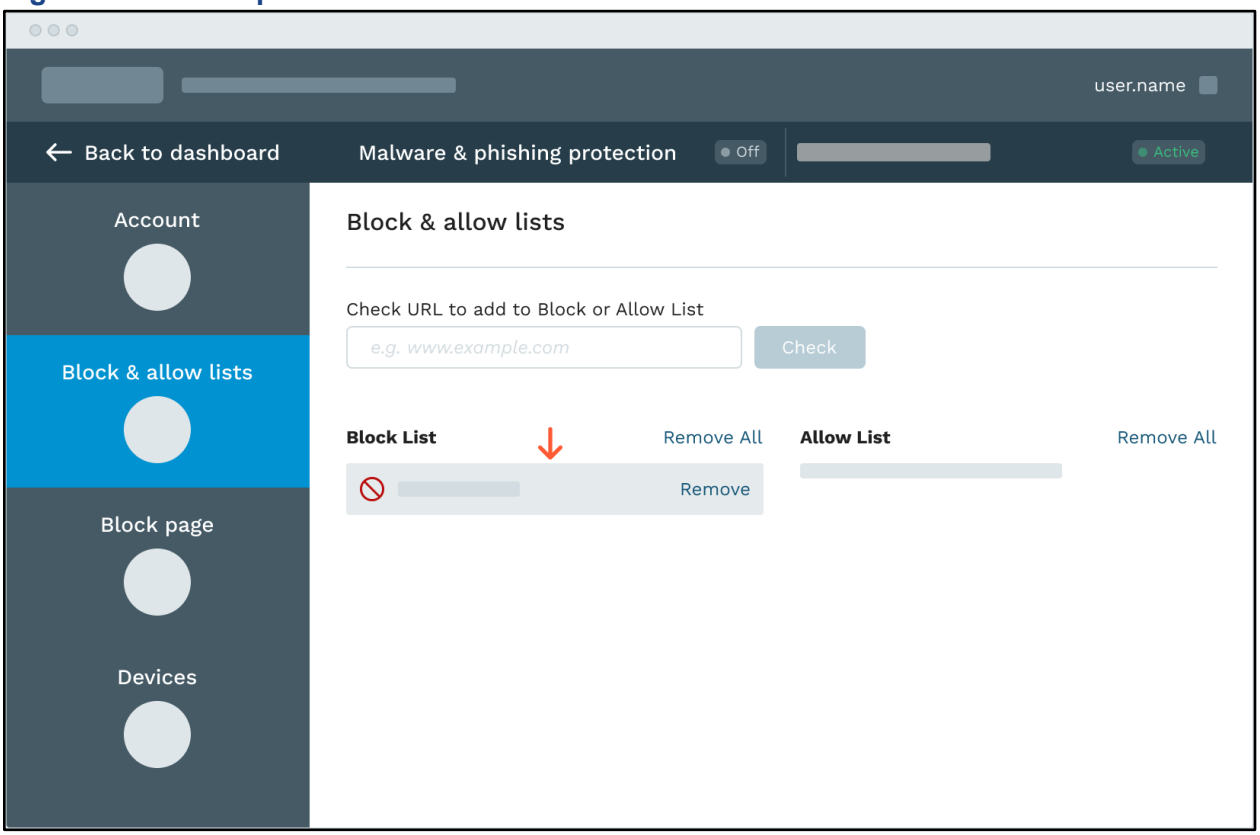
Figure 4-19: Error Message Indicating A Specified URL or Domain Already Exists in Another List



The error message remains on the page for a few seconds before disappearing; you can click the **X** icon that is located on the message to dismiss the message immediately.

4. After successfully adding a domain to a list, verify the domain appears in the correct list as demonstrated in Figure 4-20; in this example, a domain gets added to the global block list.

Figure 4-20: Example of a Successful Domain Addition



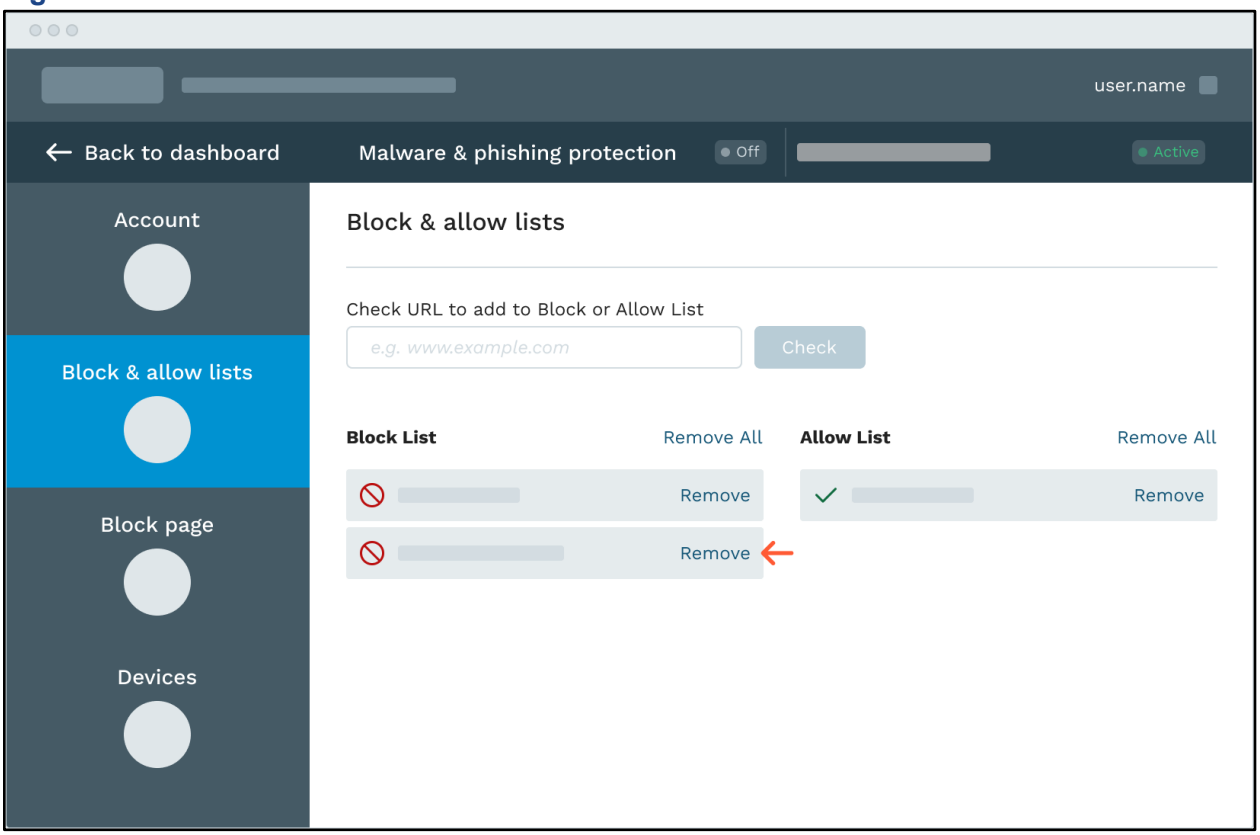
Remove Domains from a Global Block or Allow List

You can remove an individual domain from a global allow or block list, or you can remove all domains from a global allow or block list.

Use the following steps to remove a domain from a global block or allow list:

1. Access the “Block & allow lists” page.
2. In the block or allow list, locate the domain you want to remove and click the associated **Remove** option to immediately remove the domain from the list as demonstrated in Figure 4-21.

Figure 4-21: How to Remove a Domain from a Block or Allow List

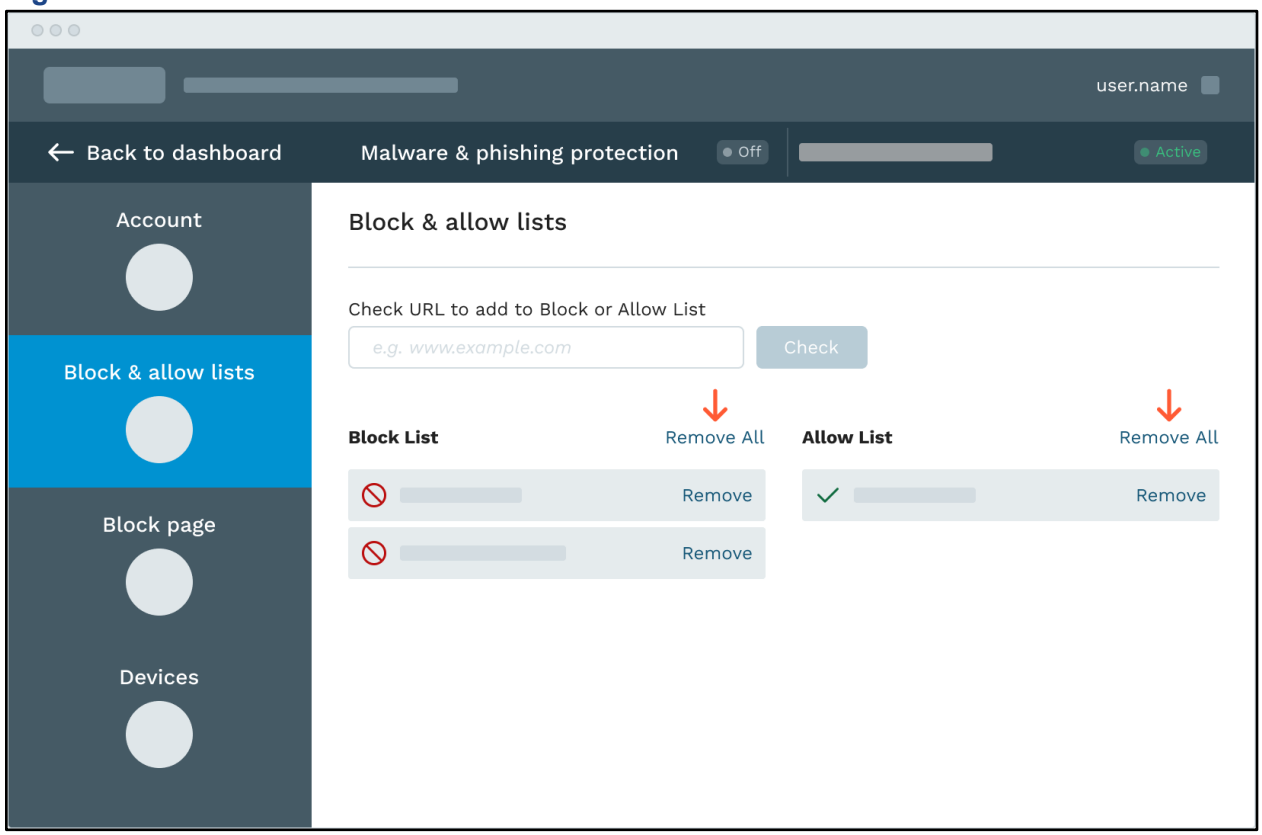


3. Verify the link no longer appears in the global block or allow list.

To remove all domains from a block or allow list, perform the following steps:

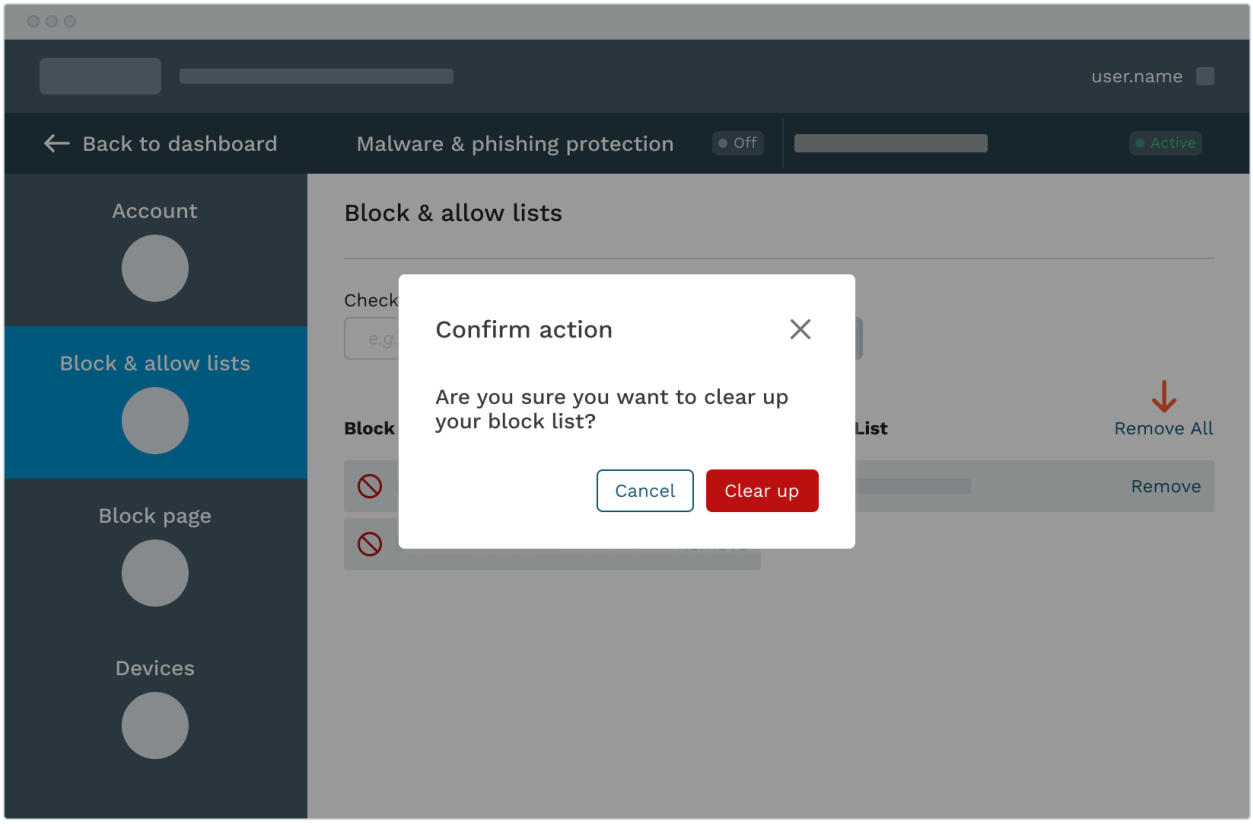
1. Access the “Block & allow lists” page.
2. Click the **Remove All** option that is associated with the list from which to remove all domains. Figure 4-22 shows where the **Remove All** options are located for the global Block and Allow lists.

Figure 4-22: How to Remove All Domains from a Global Block or Allow List



3. The application prompts you to confirm your request to remove all domains from the global block or allow list. Click the **Clear up** button to confirm your request and immediately remove all domains from the list. Figure 4-23 shows an example of the pop-up window that prompts you to confirm your request.

Figure 4-23: Confirm your Request to Remove All Domains From a Global Block or Allow List



4. Verify the link no longer appears in the global block or allow list.

Managing Profile-specific Block and Allow Lists

Profile-specific block and allow lists apply only to the devices attached to a particular profile. This section describes how to perform the following tasks:

- Add a domain to a profile-specific block or allow list.
- Remove a domain from a profile-specific block or allow list

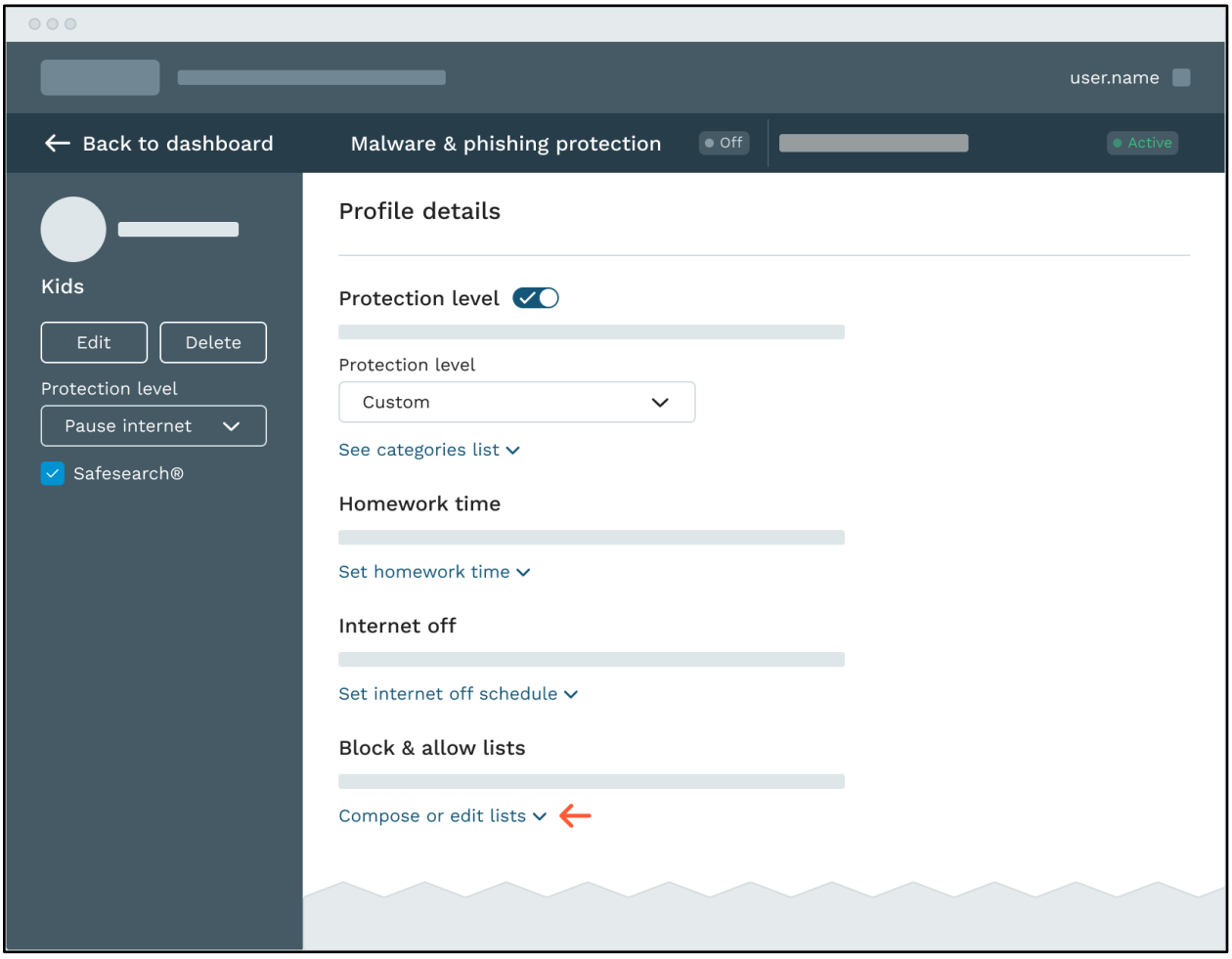
NOTE: This section describes how to configure and manage global block and allow lists only; to configure and manage profile-specific block and allow lists, see the "Add a Domain to a Profile-specific Block or Allow List" section.

Add a Domain to a Profile-specific Block or Allow List

The steps that follow describe how to add a domain to a profile-specific block and allow list:

1. Access the **“**Profile details” page for the desired profile. Figure 4-1 demonstrates how to access the **“**Profile details” page.
2. On the **“**Profile details” page, locate the “Block & allow lists” section. If the section is collapsed, click the **Compose or edit lists** expansion toggle to display block and allow list controls. Figure 4-24 shows where the **Compose or edit lists** expansion toggle is located on the “Profile details” page:

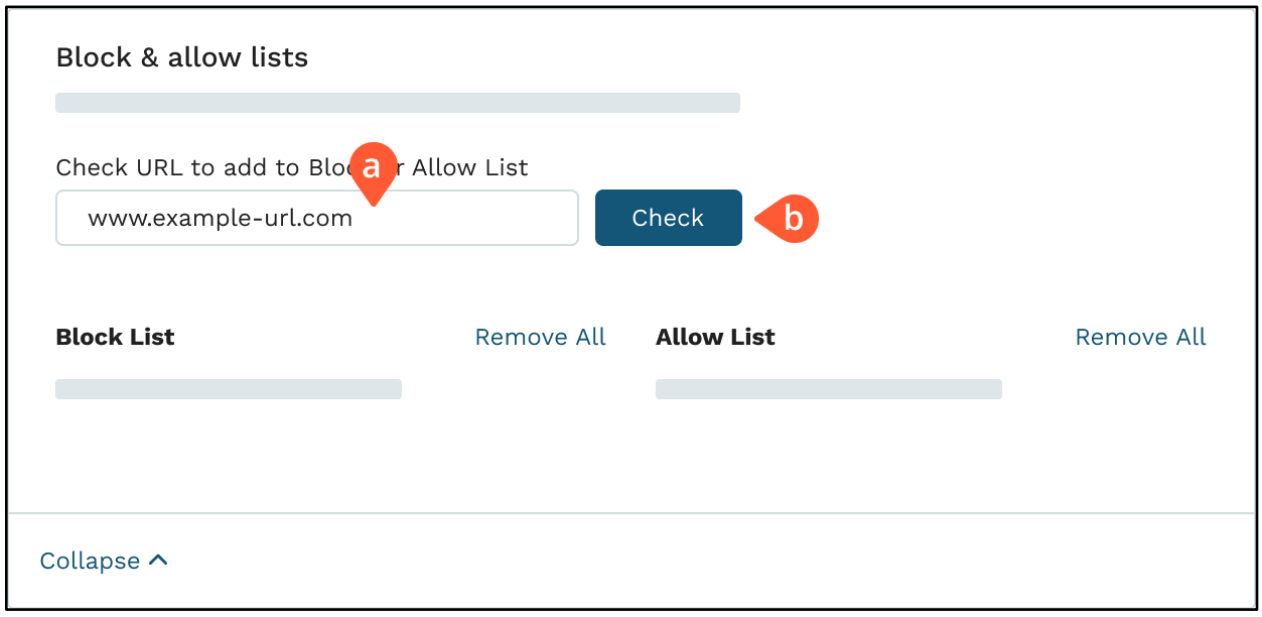
Figure 4-24: Display Profile-specific Block and Allow List Controls



3. Under the “Block & allow lists” section, perform the following tasks to verify whether a desired domain already exists in another block or allow list:
    a. In the “Check URL to add to Block or Allow List” search field, type the desired URL or domain name.
    b. Click the **Check** button to perform the search.

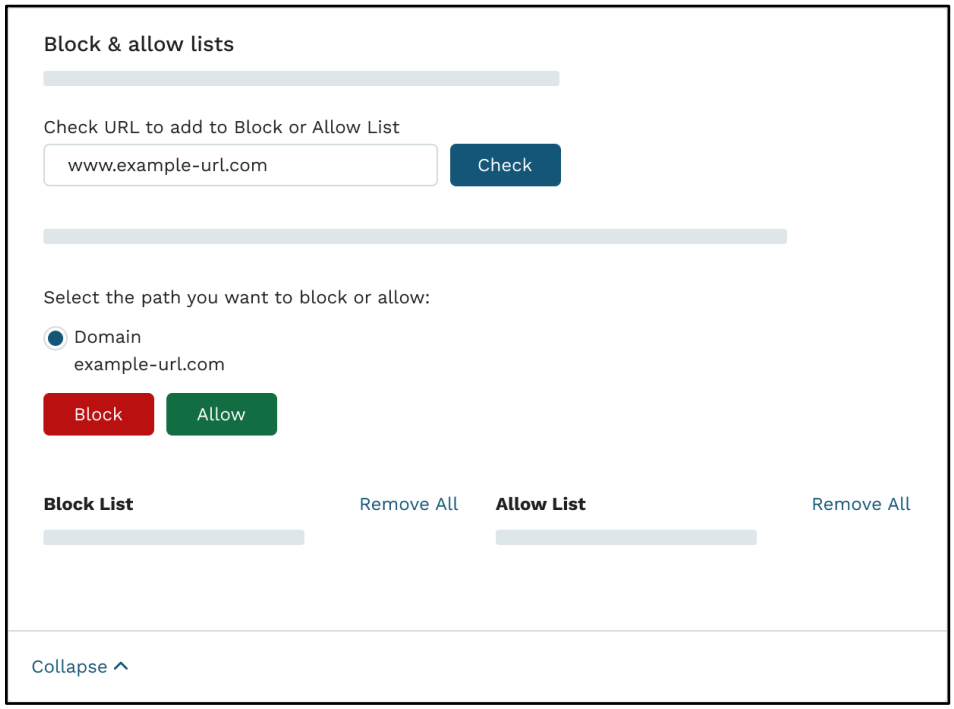
Figure 4-25 demonstrates how to perform Step a and Step b.

Figure 4-25: Verify Whether a Domain Already Appears in another Block or Allow List



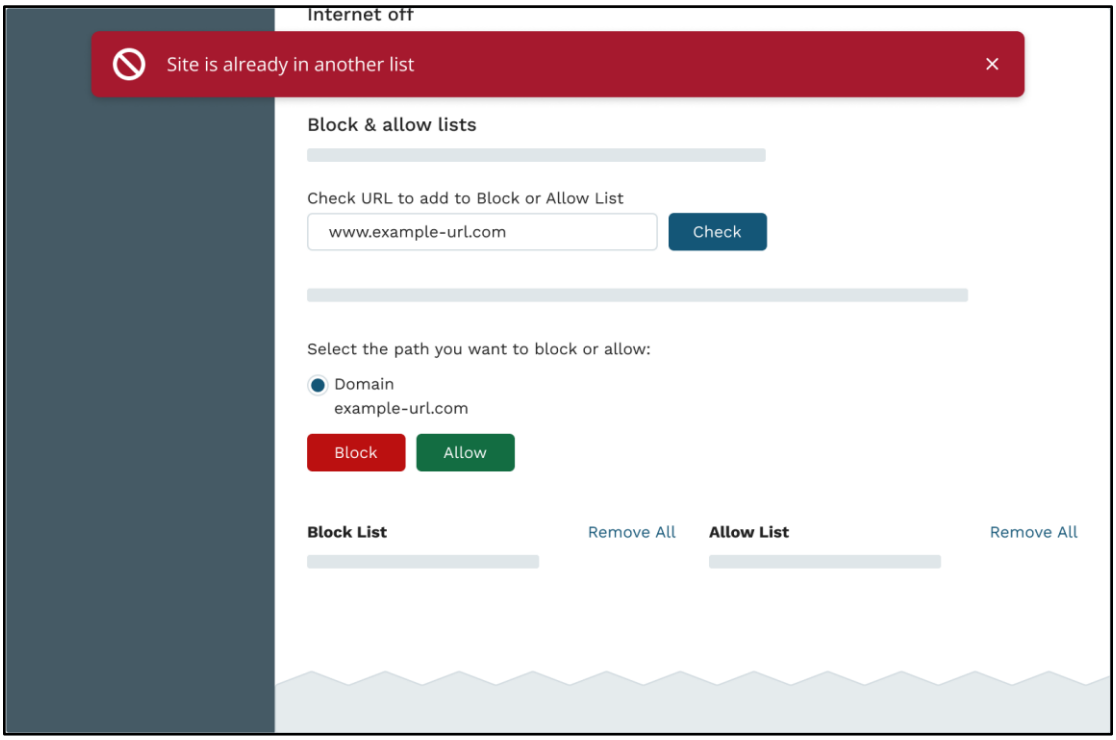
4. If the specified domain does not already exist in the profile block or allow lists, the Advanced Security service prompts you to indicate whether to add the domain to the global block or allow list as demonstrated in Figure 4-26. Click the **Block** button to add the domain to the block list; click the **Allow** button to add the domain to the allow list:

Figure 4-26: Indicate Whether to Add a Domain to a Profile-specific Block or Allow List



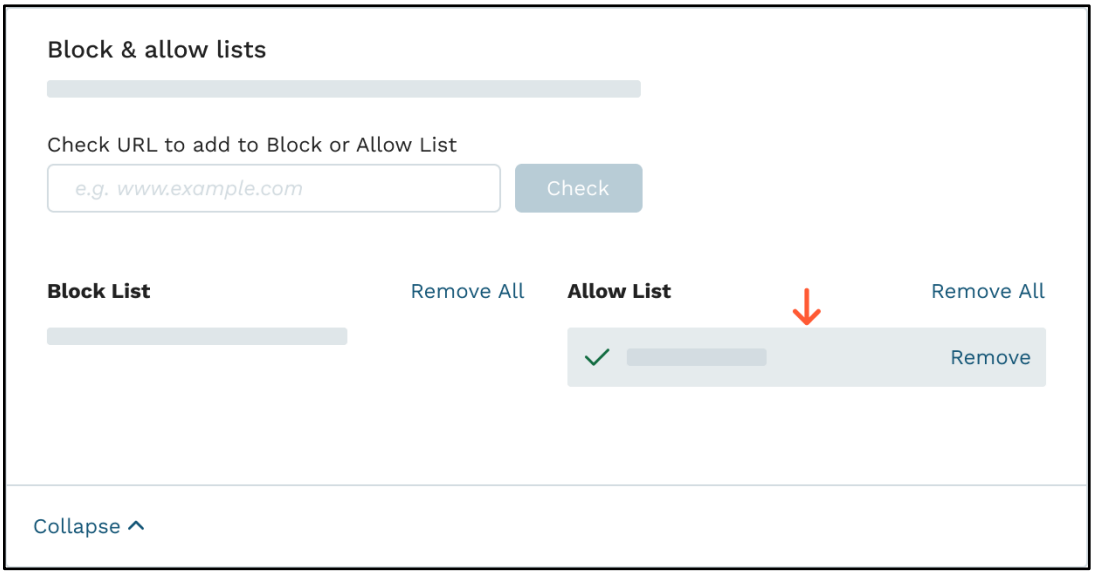
If the domain already exists in the profile block or allow list, an error message informs you that the domain already appears in a block or allow list and the Advanced Security service does not add the domain to the specified list demonstrated in Figure 4-27:

Figure 4-27: Error Message Indicating A Specified URL or Domain Already Exists in Another List



5. After successfully adding a domain to the a list, verify the domain appears in the correct list. Figure 4-28 shows what it looks like when a domain is successfully added to the allow list for a profile.

Figure 4-28: Example of a Successful Domain Addition



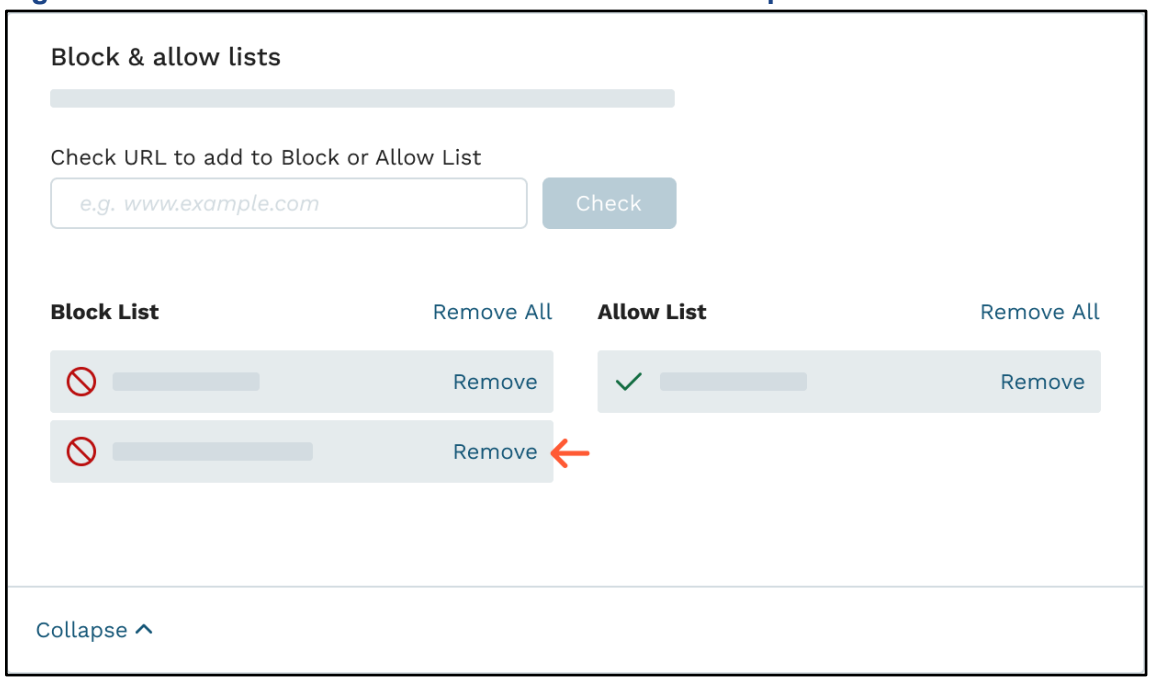
Remove Domains From a Profile-specific Block or Allow List

You can remove an individual domain from a profile-specific allow or block list, or you can remove all domains from a profile-specific allow or block list.

Use the following steps to remove a domain from a profile-specific block or allow list:

1. Access the "Profile details" page for the desired profile. Figure 4-1 demonstrates how to access the "Profile details" page.
2. In the block or allow list, locate the domain you want to remove and click the associated **Remove** option as demonstrated in Figure 4-29; the Advanced Security service immediately removes the domain from the list.

Figure 4-29: How to Remove a Domain from a Profile-Specific Block or Allow List

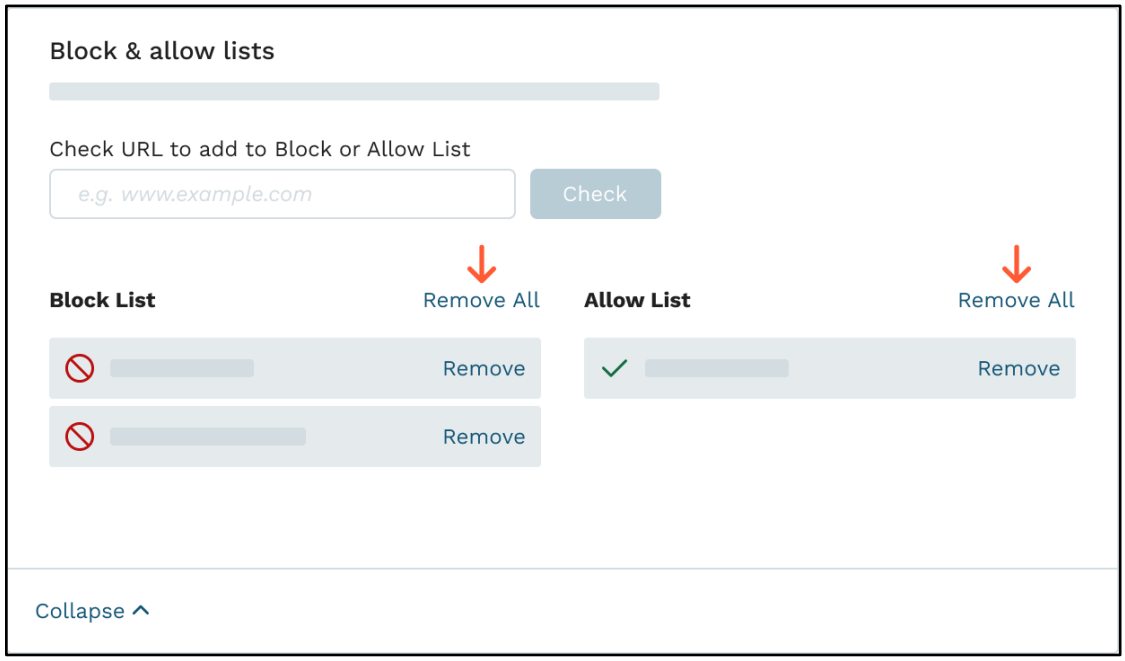


3. Verify the domain no longer appears in the profile-specific block or allow list.

To remove all domains from a profile-specific block or allow list, perform the following steps:

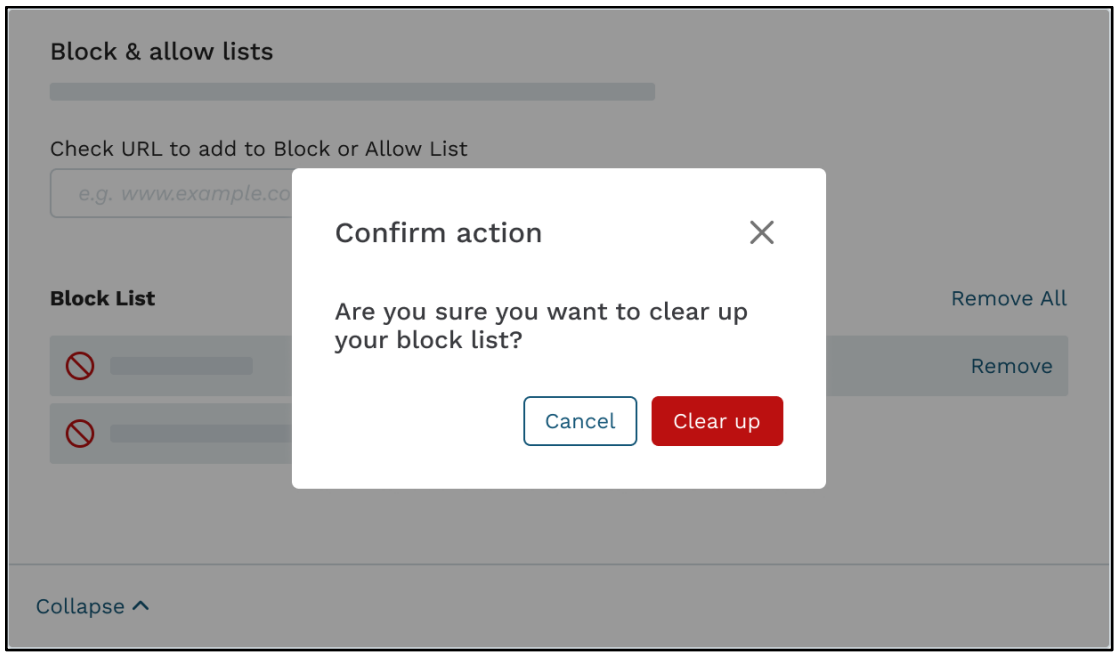
1. Access the "Profile details" page for the desired profile. Figure 4-1 demonstrates how to access the "Profile details" page.
2. Click the **Remove All** option that is associated with the list for which to remove all domains. Figure 4-30 shows where the **Remove All** options are located for profile-specific block and allow lists.

Figure 4-30: How to Remove All Domains from a Profile-specific Block or Allow List



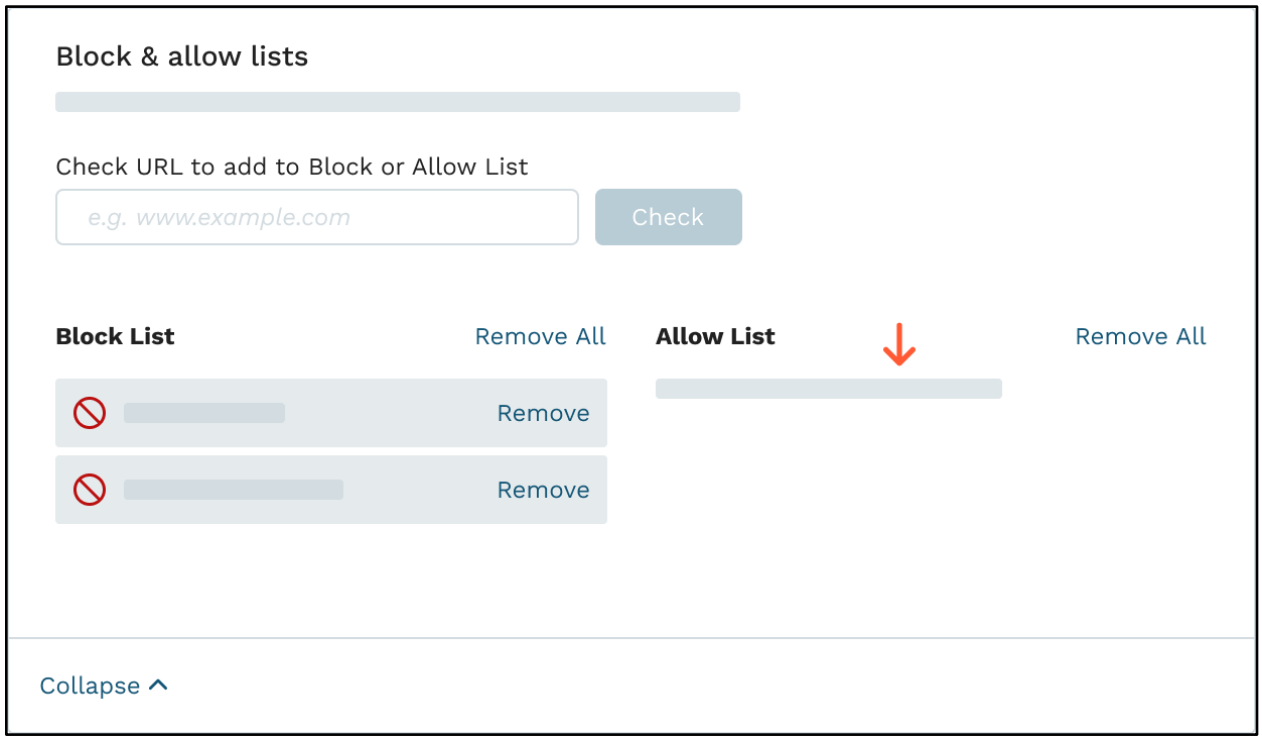
3. The application prompts you to confirm your request to remove all domains from the profile-specific block or allow list; click the **Clear up** button to immediately remove all domains from the list. Figure 4-31 shows what the “Confirm action” pop-up prompt looks like:

Figure 4-31: Confirm your Request to Remove All Domains From a Profile-specific Block or Allow List



4. Verify no domains appear in the profile-specific list you cleared in Step 3. Figure 4-32 shows what happens after you remove all domains from a profile-specific allow list; the allow list is now empty:

Figure 4-32: Verify All Domains are Removed From a Profile-specific Block or Allow List



Chapter 5: Managing Devices

If your Advanced Security service supports multiple profiles, you can group devices into individual profiles that have a unique set of rules and restrictions. You can instantly change protections and restrictions for devices accessing your network by assigning those devices to different profiles. When you add a device to a profile, that device inherits the protections and restrictions settings from the profile.

The Advanced Security service supports the following methods for adding devices to the service:

- Device detection—The Advanced Security detects new devices requesting access to your network. Each device is assigned a four-character code to be included in the access request; devices with a matching code are granted access to the network through the Advanced Security service.
- Manual addition of devices—An Advanced Security administrator can manually add devices to the service using the four-character code or unique MAC (Media Access Control) address associated with the device.

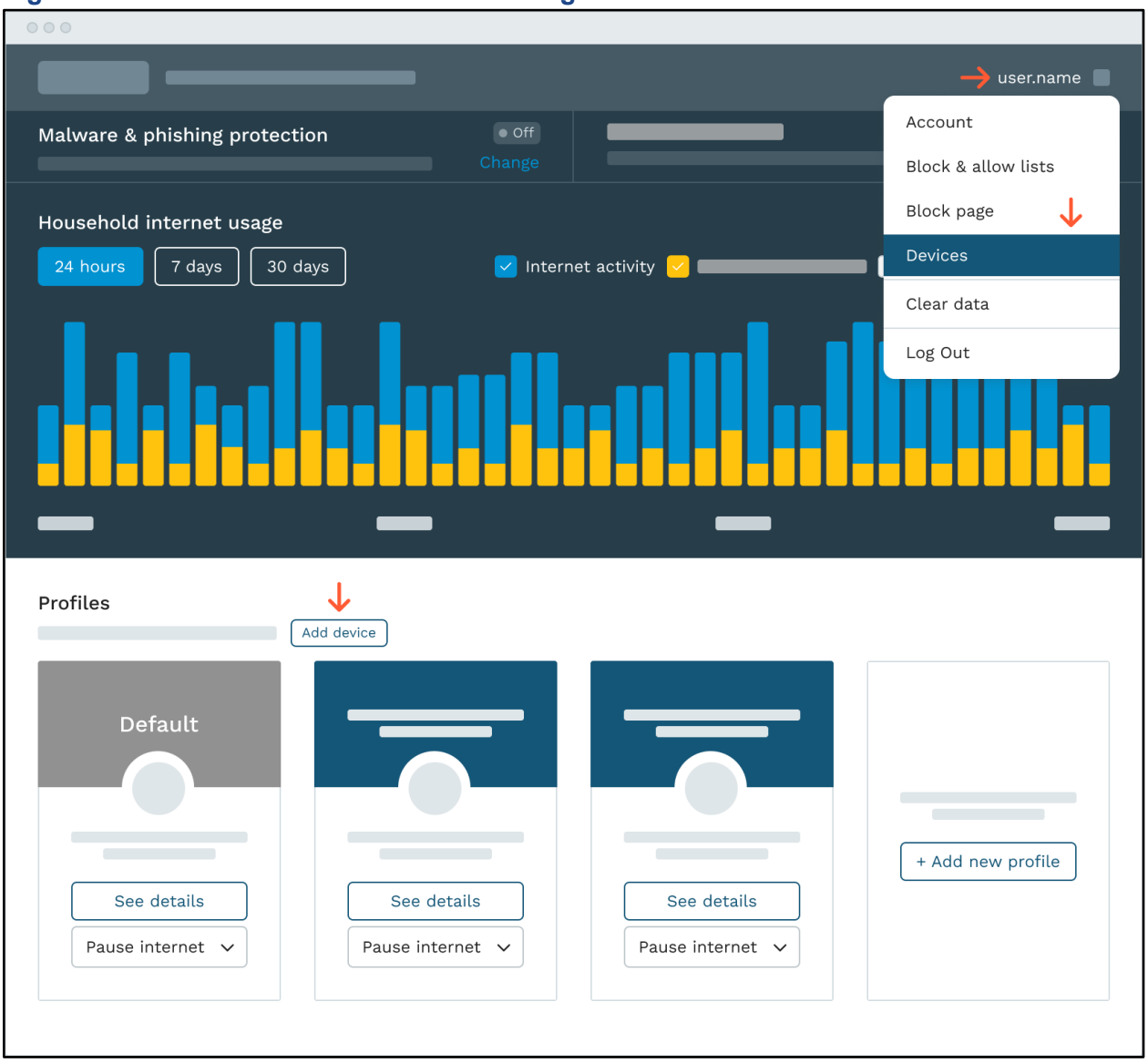
You manage devices on the “Devices” page (see the “Understanding the ‘Devices’ Page” section for instructions on how to access the “Devices” page).

Understanding the “Devices” Page

You manage devices on the “Devices” page. Use one of the following methods to access the “Devices” page:

- Select the **Devices** option from the **services** drop-down menu. Figure 5-1 shows where the Devices option is located in the **services** drop-down menu.
- On the Advanced Security home dashboard, click the **Add Device** button that is located above the profile tiles. Figure 5-1 shows where the **Add Device** button is located on the home dashboard.

Figure 5-1: How to Access the “Devices” Page



The “Devices” page comprises device tables which provide information about the devices in your Advanced Security service. Each profile has its own device table.

Figure 5-2 shows a sample “Devices” page that includes callouts, where each callout number corresponds to a component that is described in Table 5-1, “‘Devices’ Page Components.”

Figure 5-2: “Devices” Page Components

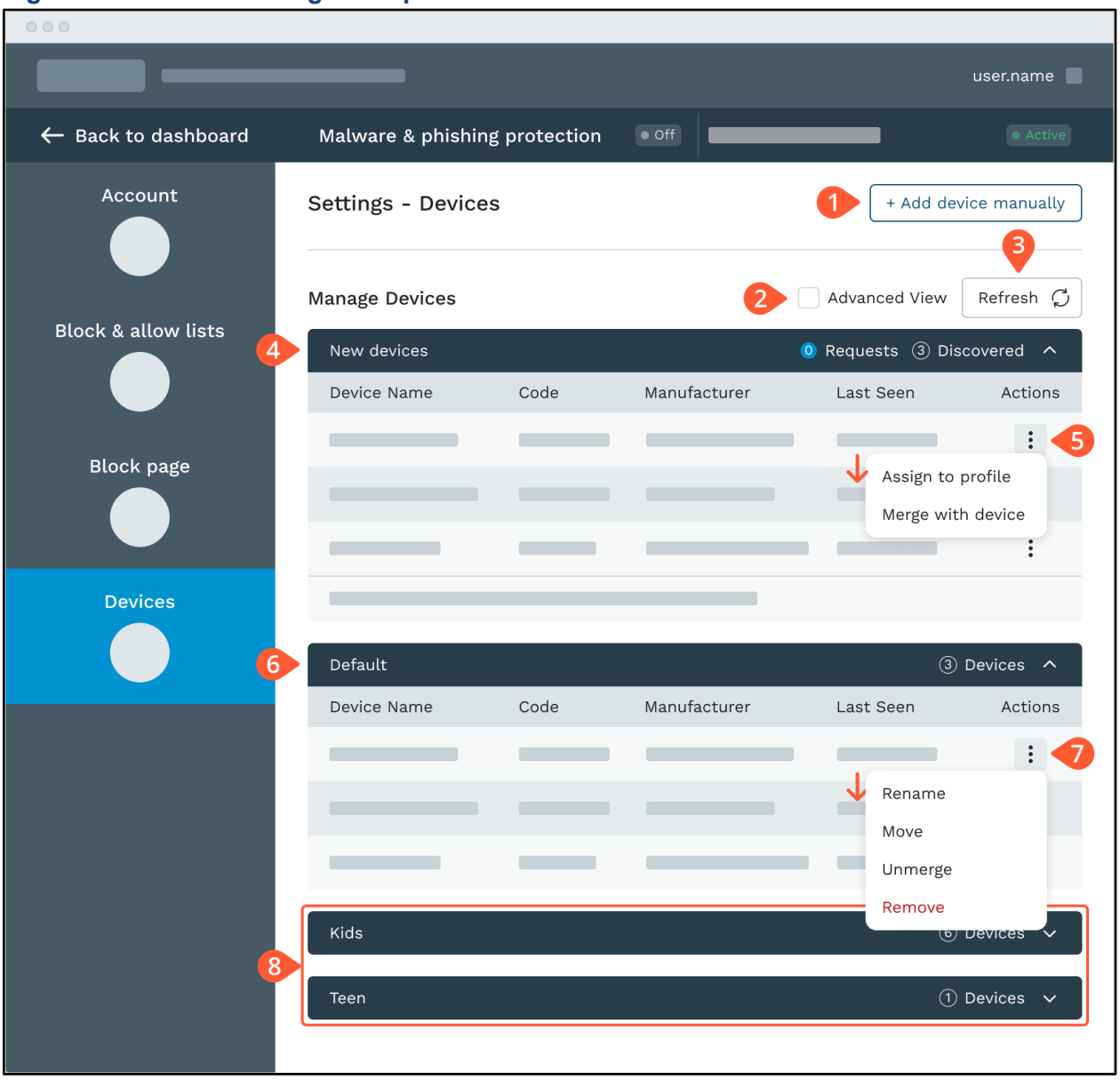


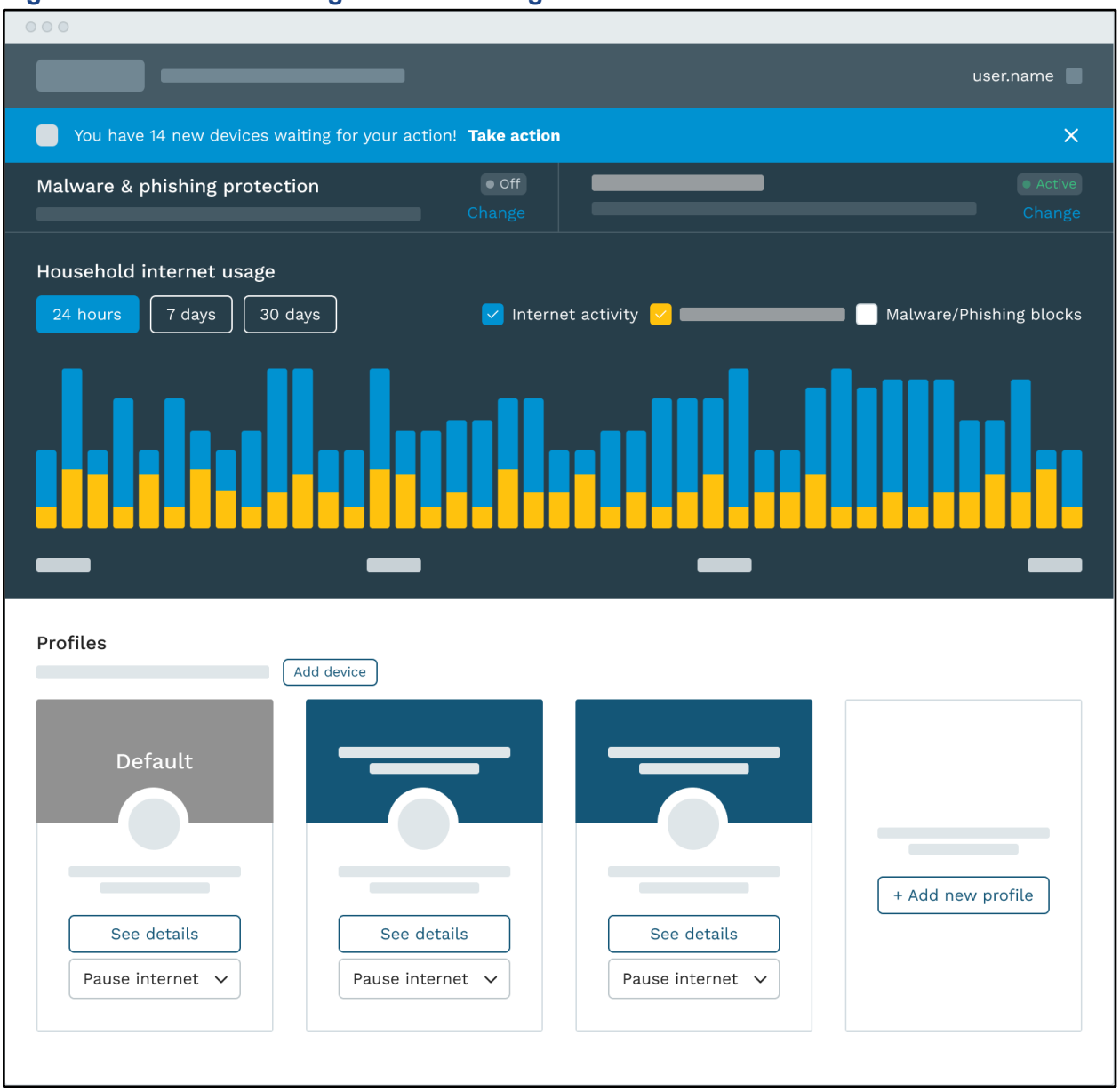
Table 5-1: “Devices” Page Components

Callout	Component	Description
1	**Add Device Manually** button	Opens the "Add device manually" pop-up window, in which you can specify the name and MAC address that is associated with the device you want to add to your Advanced Security service.
2	**Advanced View** checkbox toggle	Displays and hides the Network Identifier associated with each device in the device tables. Perform the following tasks to show and hide the network identifier in the device tables: ● Add a checkmark to the **Advanced View** checkbox to include the network identifier in the device tables. ● Clear the **Advanced View** checkbox to hide the network identifier.
3	**Refresh** button	Click the **Refresh** button to refresh the device tables and see all new devices in your network. Clicking the **Refresh** button updates the table to show recent changes.
4	“New Devices” table	Provides a list of devices requesting access to your Advanced Security service.
5	“New Devices” table “Actions” **ellipsis** icon drop-down menu	Opens a drop-down menu which provides the following options: ● **Assign to profile**—Assign the device to a particular profile.
6	“Default” profile device table	Provides a list of devices belonging to the “Default” profile. The “Default” table can contain many devices; click the **Last Seen** table heading to scroll through the devices in a profile.
7	Profile table “Actions” **ellipsis** icon drop-down menu	Opens a drop-down menu that provides the following options: ● **Rename**—Change the name of the associated device. ● **Move**—Assign the device to a different profile. ● **Remove**—Remove the device from the profile.
8	Additional profile device tables	Device tables for any additional profiles (if configured) in an Advanced Security service that supports multiple-profiles.

Device Detection

If there are new devices requesting access to your network through the Advanced Security, your home dashboard includes a message indicating the number of new devices requesting access as shown in the example Figure 5-3.

Figure 5-3: Devices Waiting Banner Message



The “Devices” page contains a “New Devices” table that lists all devices requesting access to your network, along with controls for managing those devices. Figure 5-4 shows an example of the “New Devices” table; this figure includes callouts next to each column heading in the “New Devices” table, where each callout number corresponds to a column that is described Table 5-2.

Figure 5-4: New Devices Table

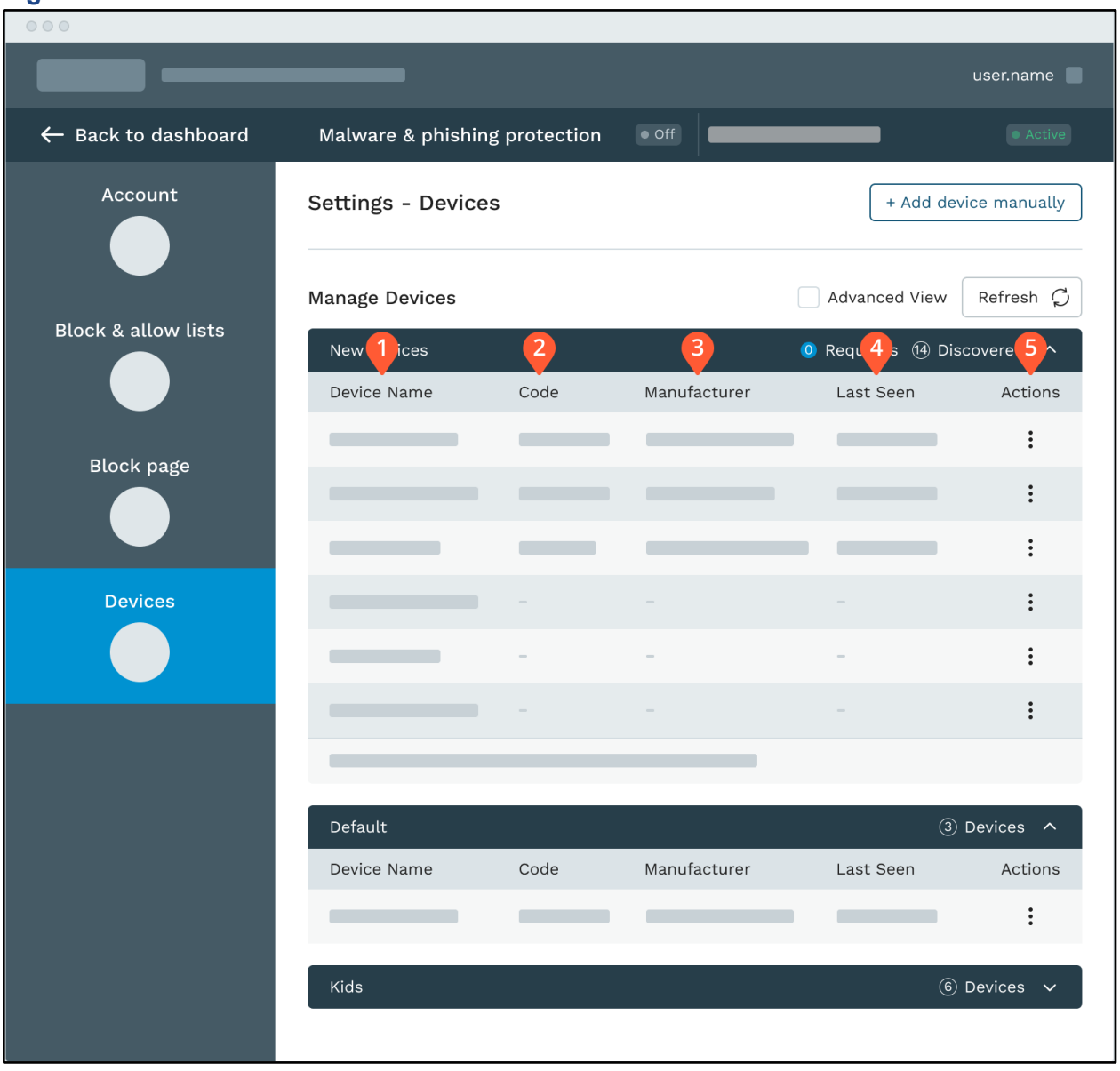


Table 5-2: "New Devices" Table Column Descriptions

Callout	Column Heading	Description
1	**Device Name**	Text string name that identifies the device requesting access to your network.
2	**Code**	Specifies a 4-character registration code associated with the device (if the device has a registration code).
3	**Manufacturer**	Identifies the manufacturer of the device.
4	**Last Seen**	Provides the date and time the specified device last accessed the network.
5	**Actions**	Provides an **ellipsis** drop-down menu which provides the following device management options. In the Actions column, click the **ellipsis** icon that is associated with the device you want to manage: • **Assign to Profile**—Assign the device to a particular profile. • **Merge with Device**—Merge the device with another eligible device in the service. Merging combines the changes made to different devices placed in different profiles or used by different users. The merge devices option is available only if there are other devices available for merging.

Assigning New Devices to a Profile

When you assign a device to a profile, that device inherits the rules and settings from the profile. You assign a recognized devices to a profile on the **Devices** page as described in the steps that follow:

1. On the "Devices" page, click inside the **Advanced View** checkbox to display the Network Identifier associated with each device in the device tables (see callout 1 in Figure 5-5).

   NOTE: A checkmark in the checkbox indicates the **Advanced View** is enabled and the device tables include the Network Identifiers that are associated with each device; clear the checkbox to hide the Network Identifiers that are associated with the devices.

2. In the "New Devices" table, locate the device you want to assign to a profile and select the **Assign to profile** option from the **vertical ellipses** drop-down menu that is associated with the device (see callout 2 in Figure 5-5). Clicking the **Assign to profile** option opens the "Assign to Profile" pop-up dialog shown in Figure 5-6.

   In the "Assign to profile" pop-up dialog, assign a name and a profile to the device and click the **Assign** button to close the dialog and return to the "Devices" page.

3. On the "Devices" page, click the **Assign Devices** button to immediately assign the devices to the profiles specified in Step 2. Verify the devices you assigned in Step 2 appear in the appropriate profile tables.

Figure 5-5 demonstrates how to perform Step 1 through Step 3.

Figure 5-5: Assign New Devices to a Profile

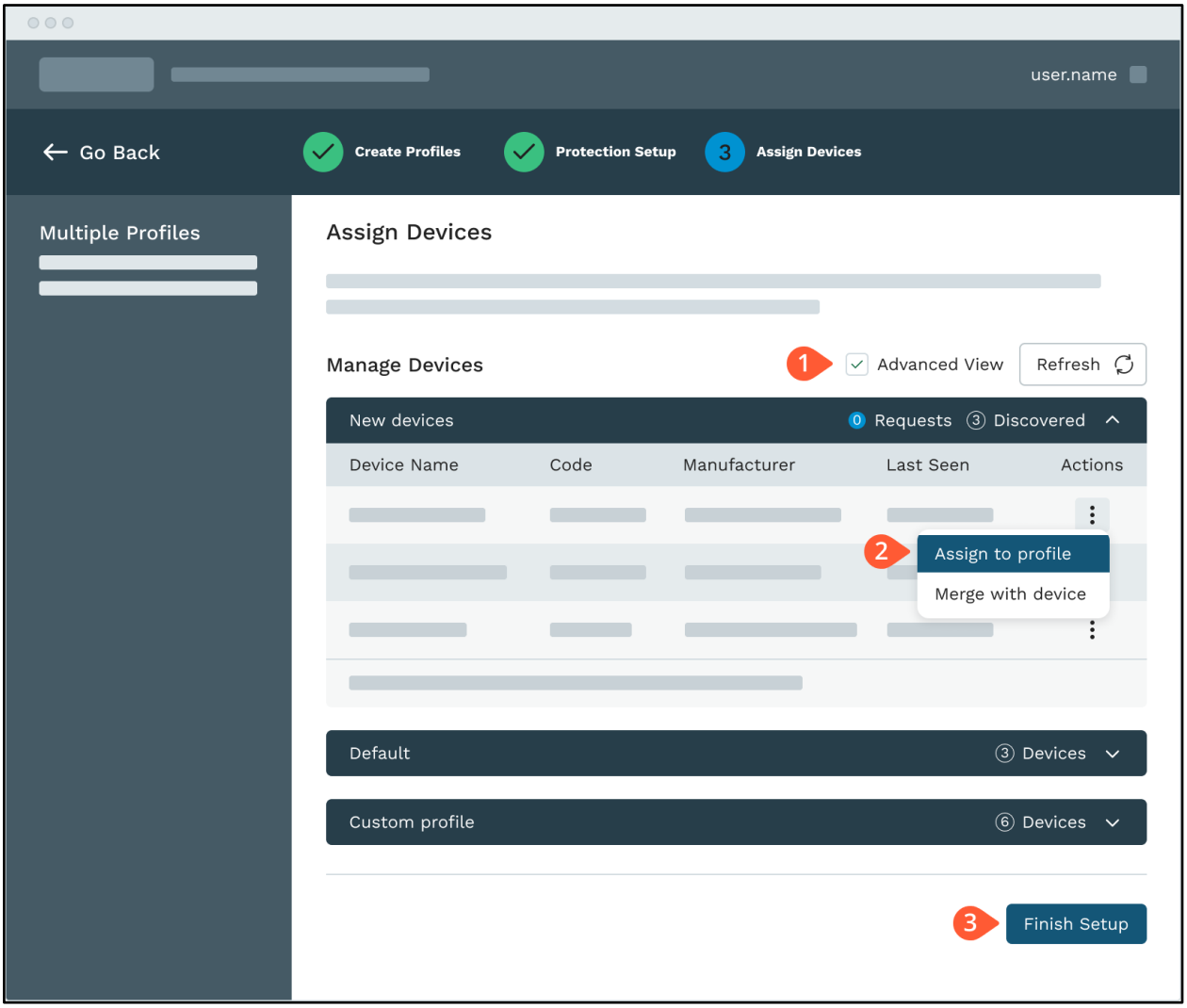
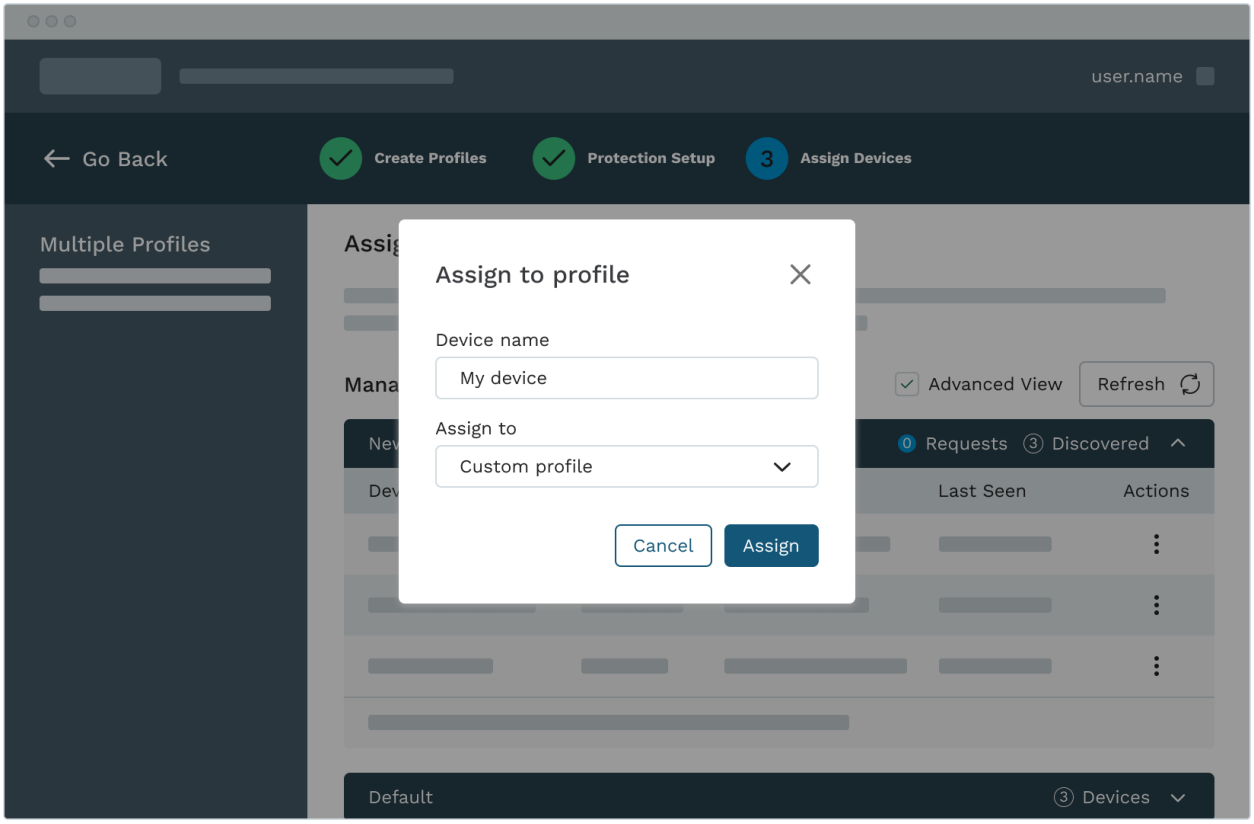


Figure 5-6 shows the “Assign to profile” popup dialog that appears when you click the **Assign to profile** option as described in Step 2:

Figure 5-6: “Assign to profile” Pop-up Dialog



Reassigning Devices to Another Profile

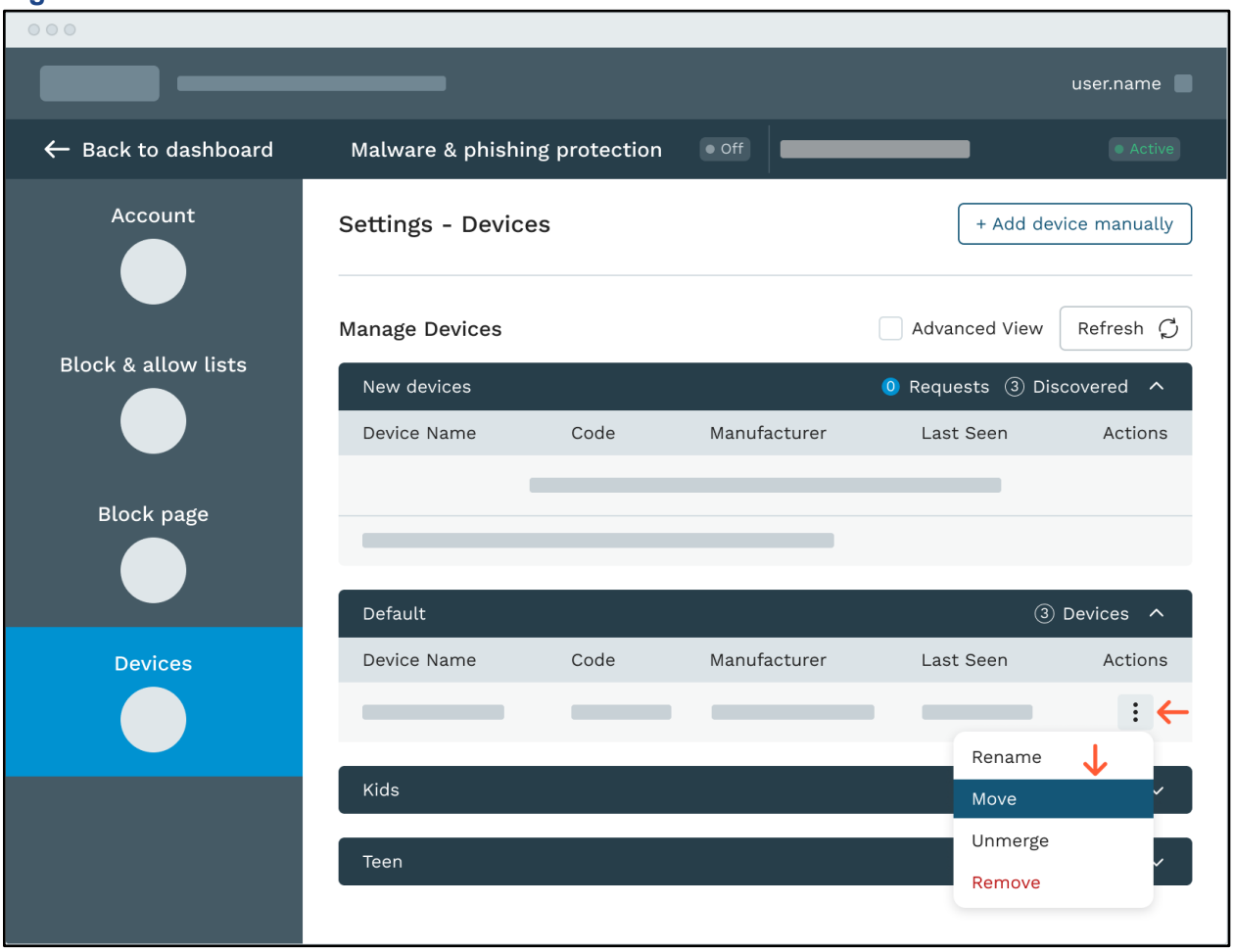
In addition to the “New Devices” device table, the “Devices” page includes profile-specific device tables, where each profile in your Advanced Security service has its own device table that provides general information about the devices in your service.

The profile-specific device tables provide general information about the devices that are attached to the specified profile, along with controls for managing those devices.

If desired, you can assign these devices to a different device profile as described in the following steps:

1. Navigate to the “Devices” page as described in the “Understanding the ‘Devices’ Page” section.
2. In a profile-specific device table, locate the device to reassign to a different profile and select the **Move** option from the **vertical ellipses** drop-down menu that is associated with the device. The **vertical ellipses** drop-down menu is located in the “Action” column as demonstrated in Figure 5-7.

Figure 5-7: How to Move a Device to Another Profile

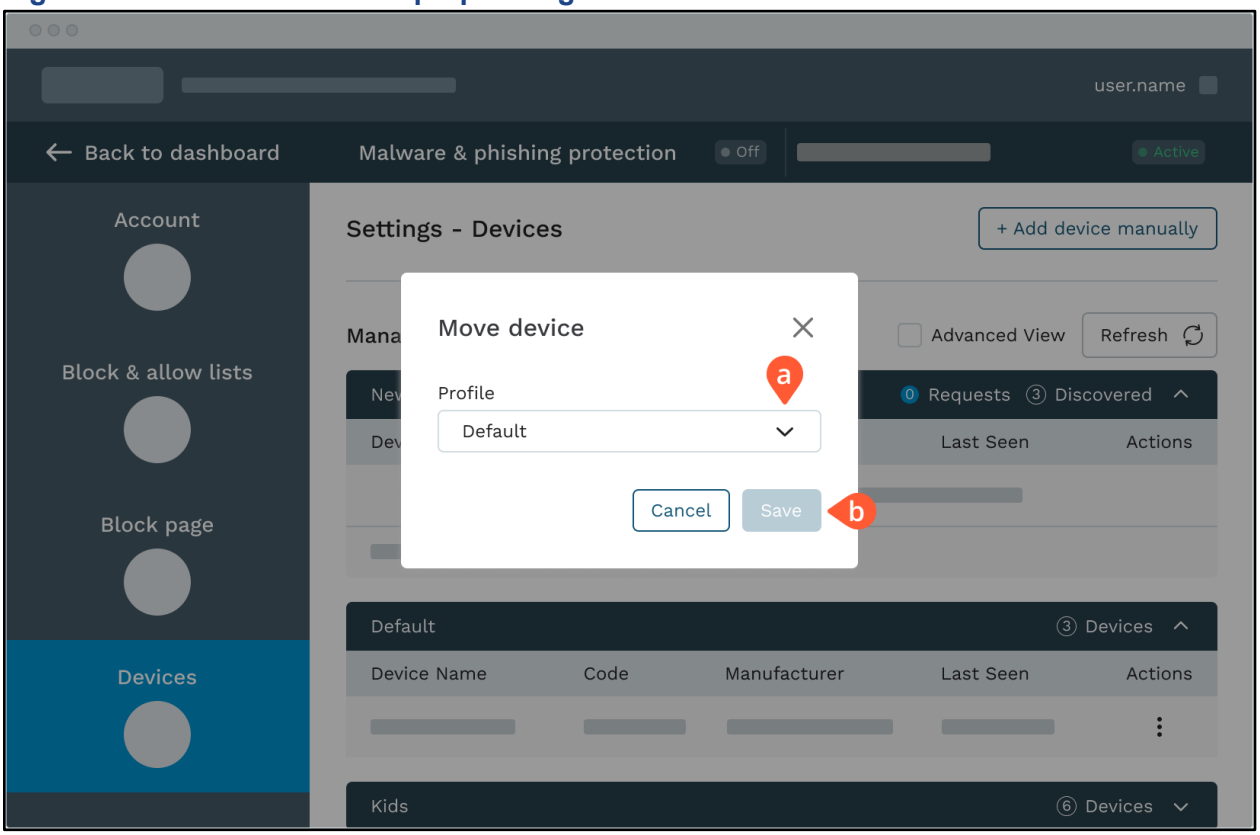


Selecting the **Move** option opens a “Move device” pop-up dialog shown in Figure 5-8.

3. In the “Move device” pop-up dialog, perform the following tasks:
    a. Use the “Profile” drop-down list to select the profile to assign the device to.
    b. Click the **Save** button to assign the device to the selected profile. The Advanced Security service immediately reassigns the device to the specified profile and returns to the “Devices” page.

Figure 5-8 shows the "Move device” pop-up dialog and demonstrates how to perform Step a and Step b.

Figure 5-8: “Move Device” Pop-up Dialog



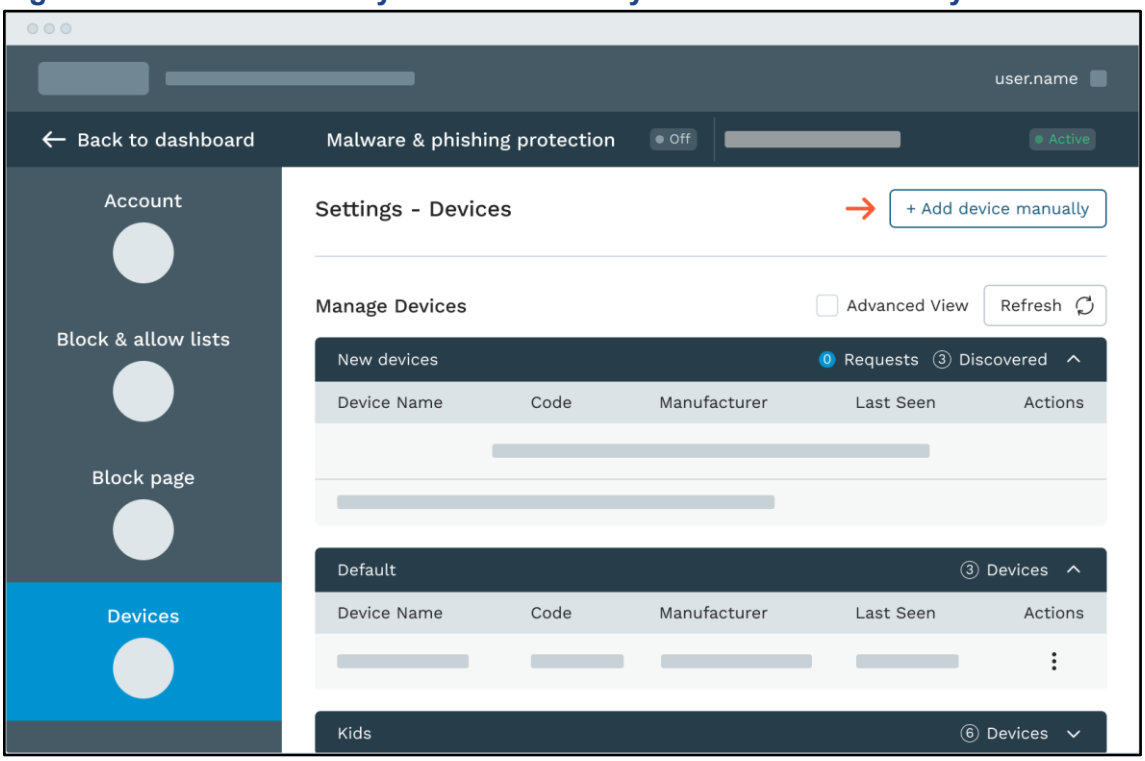
4. On the “Devices” page, verify the device appears in the appropriate profile.

Manually Add a New Device to the Advanced Security Service

Use the following steps to add a new device to your Advanced Security service:

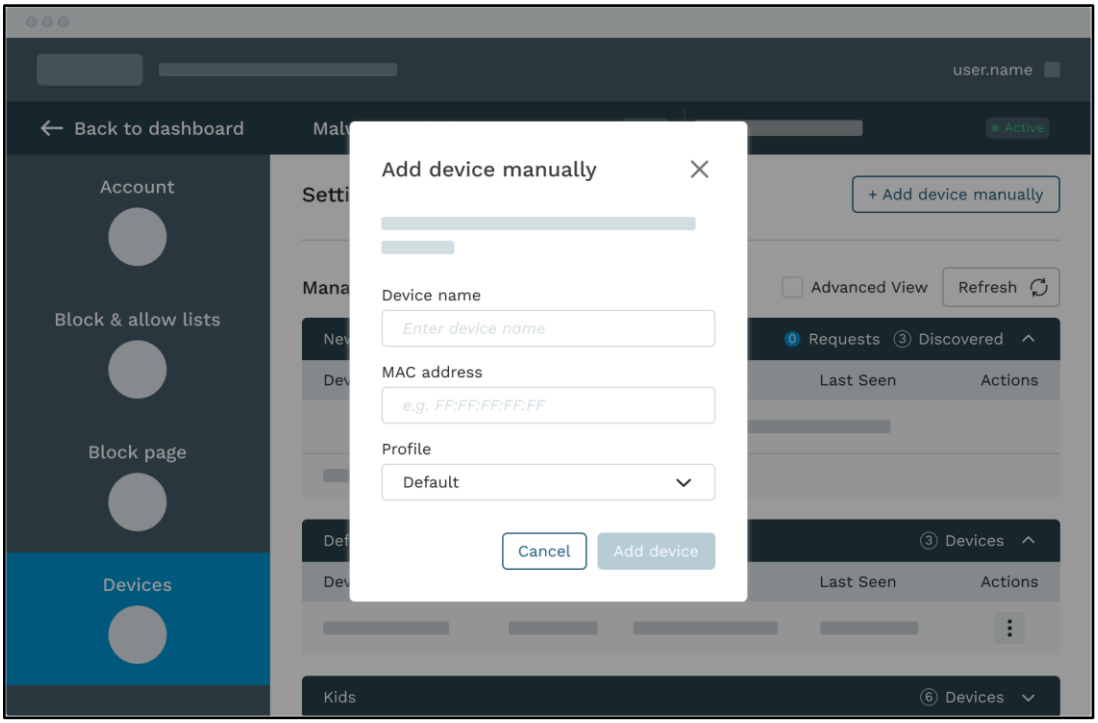
1. Navigate to the “Devices” page as described in the [”Understanding the ‘Devices’ Page](#)” section.
2. On the “Devices” page, click the **Add device manually** button to open the “Add device manually” pop-up dialog. [Figure 5-9](#) shows where the **Add device manually** button is located.

Figure 5-9: How to Manually Add a Device to your Advanced Security Service



3. In the “Add device manually” pop-up dialog, specify the requested information and click the **Add device** button to add the device to your service; Figure 5-10 shows the “Add device manually” pop-up dialog.

Figure 5-10: “Add Device Manually” Pop-up Dialog



The Advanced Security service immediately adds the device to the selected profile and displays a message confirming the device is successfully added.

For platform-specific details on how to find the MAC address for a device, see the document called *How to Find Any Device's IP Address, MAC Address, and Other Network Connection Details*.

4. Verify the device is added to the correct profile.

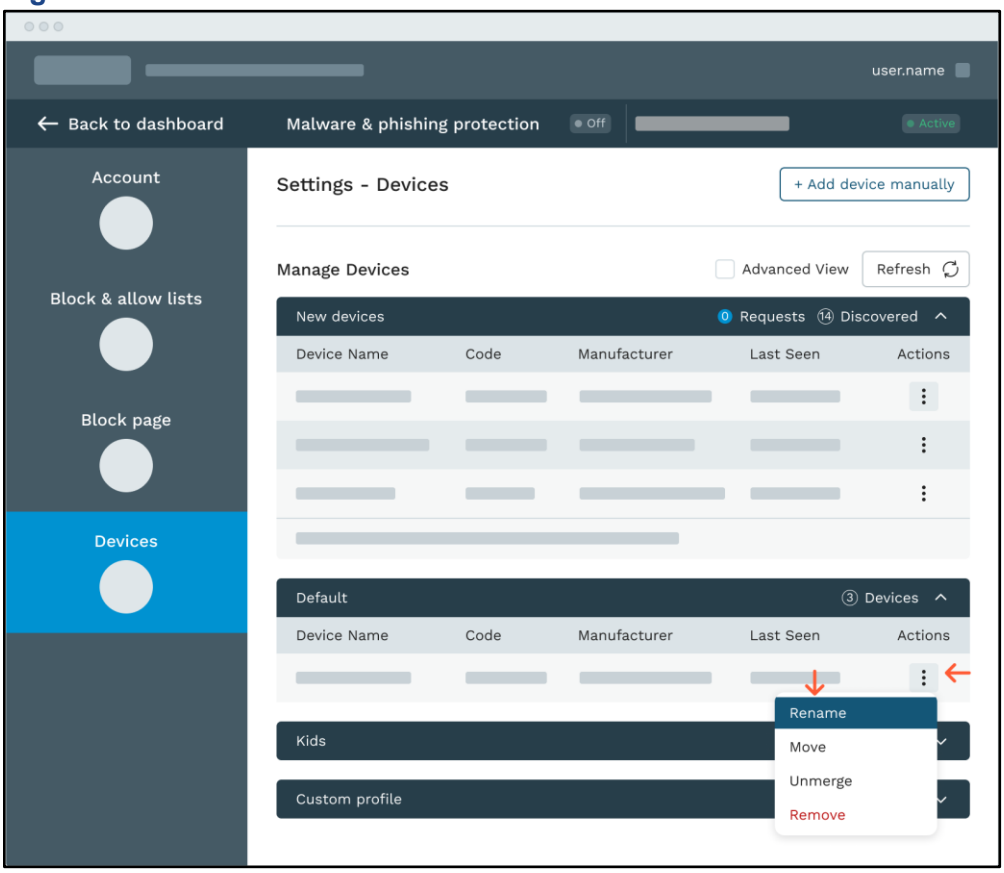
Rename Devices

If desired, you can rename any device in your Advanced Security service. To rename a device, use the following steps:

1. Navigate to the “Devices” page as described in the “Understanding the ‘Devices’ Page” section.
2. On the “Devices" page, locate the device you want to rename and select the **Rename** option from the associated **Actions** drop-down menu as shown in Figure 5-16 (in the “Actions” column, click the **Actions** ellipsis icon that is located in the same row as the device you want to rename).

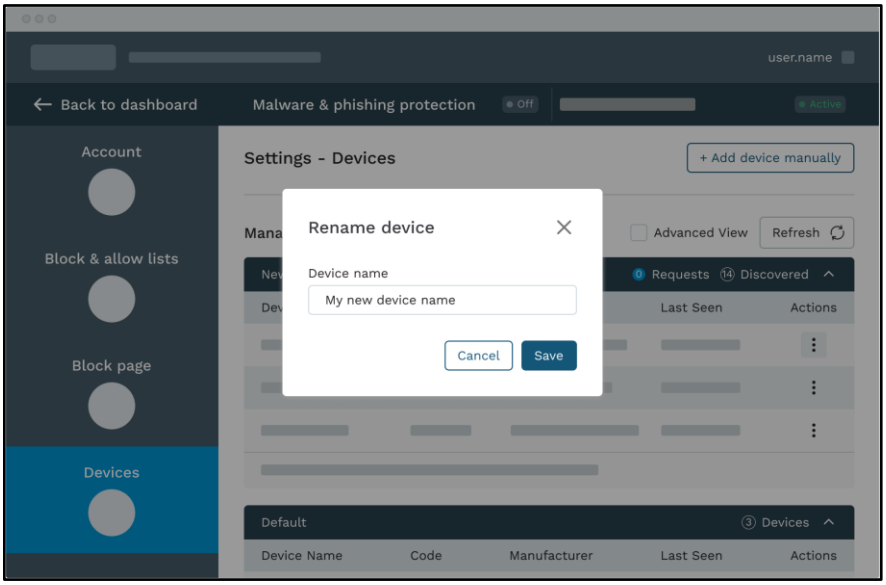
   Selecting the **Rename** option from the **Actions** drop-down menu opens the “Rename device” pop-up dialog shown in Figure 5-17.

Figure 5-16: How to Rename a Device



3. In the “Rename device” pop-up dialog, specify a new name for the device and click the **Save** button to rename the device. Figure 5-17 shows the “Rename device” pop-up dialog.

Figure 5-17: “Rename Device” Pop-up Dialog



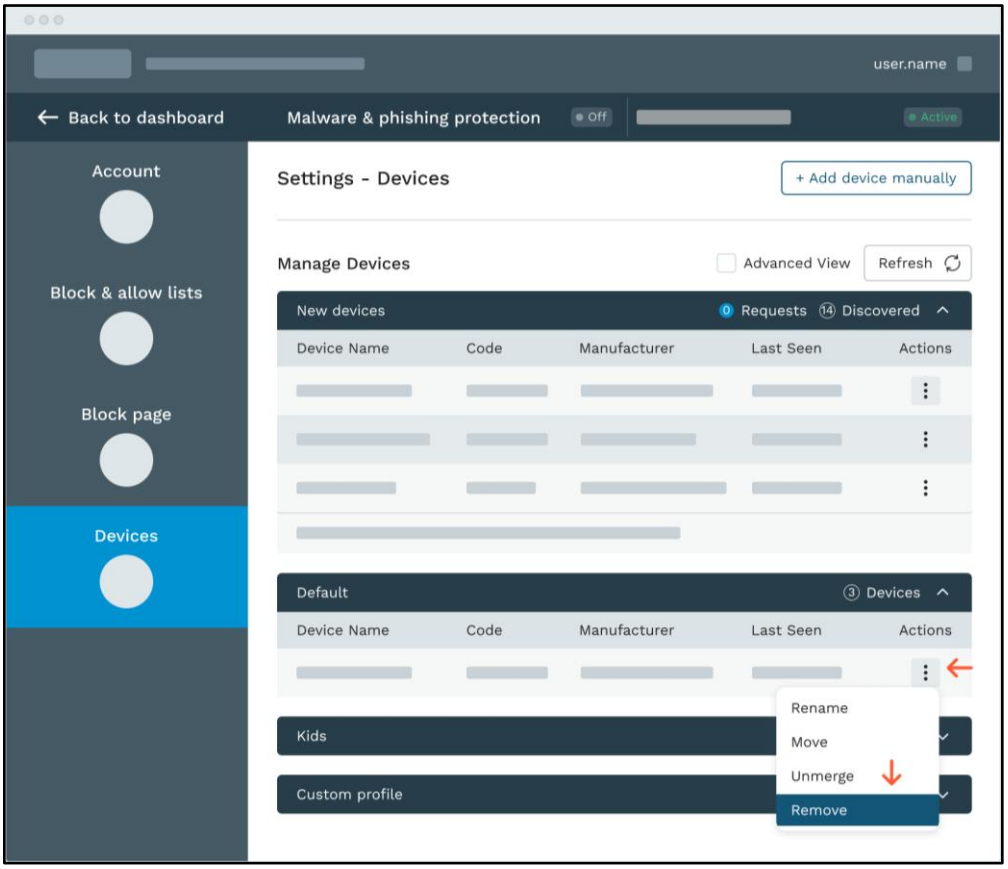
4. Verify the device you renamed appears as desired in the appropriate profile-specific device table.

Remove a Device from your Advanced Security Service

Use the following steps to remove a device from your Advanced Security service:

1. Navigate to the “Devices” page as described in the “Understanding the ‘Devices’ Page” section.
2. On the “Devices” page, locate the device you want to remove and select the **Remove** option from the associated **Actions** drop-down menu as shown in Figure 5-18 (in the “Actions” column, click the **Actions** ellipsis icon that is located in the same row as the device you want to remove):

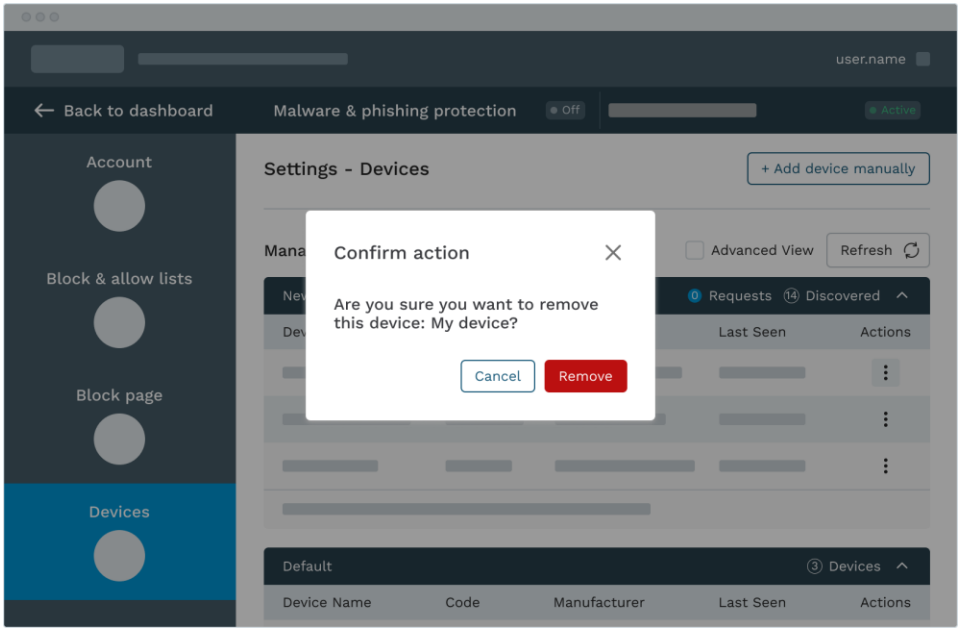
Figure 5-18: How to Remove a Device



Clicking the **Remove** option opens the “Confirm action” pop-up dialog shown in Figure 5-19, prompting you to confirm that you want to remove the specified device.

3. In the “Confirm action” pop-up dialog, verify the device ID and click the **Remove** button to remove the device from your Advanced Security service. Figure 5-19 shows the “Confirm action” pop-up dialog.

Figure 5-19: “CONFIRM ACTION” Pop-up Dialog



4. Verify the device you removed no longer appears in any device tables on the “Devices” page.

Chapter 6: Managing Block Pages

You can manage the block pages devices encounter when trying to access a domain that is blocked by your Advanced Security service. The Advanced Security service supports the following block pages:

- Malware and phishing
- Web filtering

You manage the block pages on the “Block page” management page; there are two ways to access this page:

- From any page in the Advanced Security service, select the **Block Page** option from the **services** drop-down menu. Figure 6-1 demonstrates how to select the **Block Page** option from the **services** drop-down menu.
- While on any settings page in the Advanced Security service, click the **Block Page** tab that is located on the settings page selector. Figure 6-1 shows where the **Block Page** tab is located on the page selector.

Figure 6-1: How to Access Block Page Settings

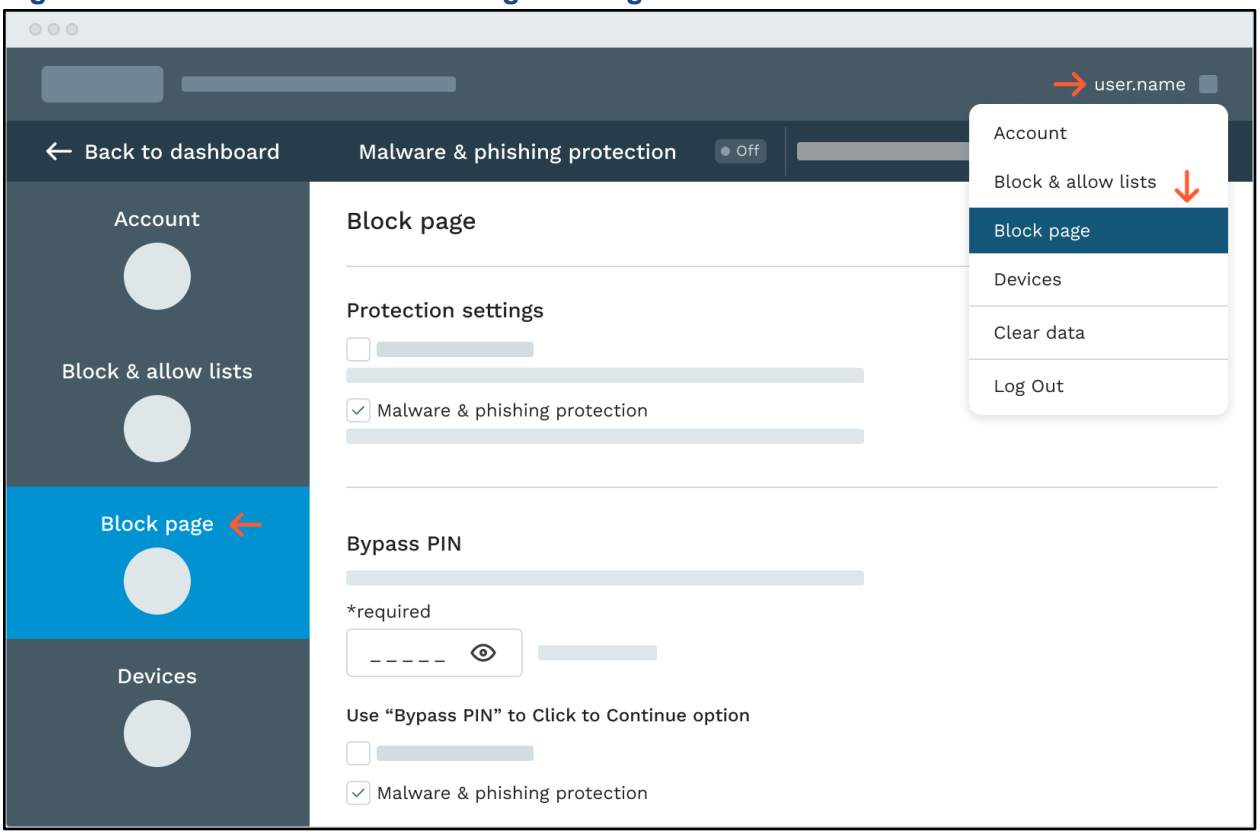


Figure 6-2 shows the “Block page” options and includes callouts, where each number corresponds to a component described in Table 6-1.

Figure 6-2: Block Page Settings

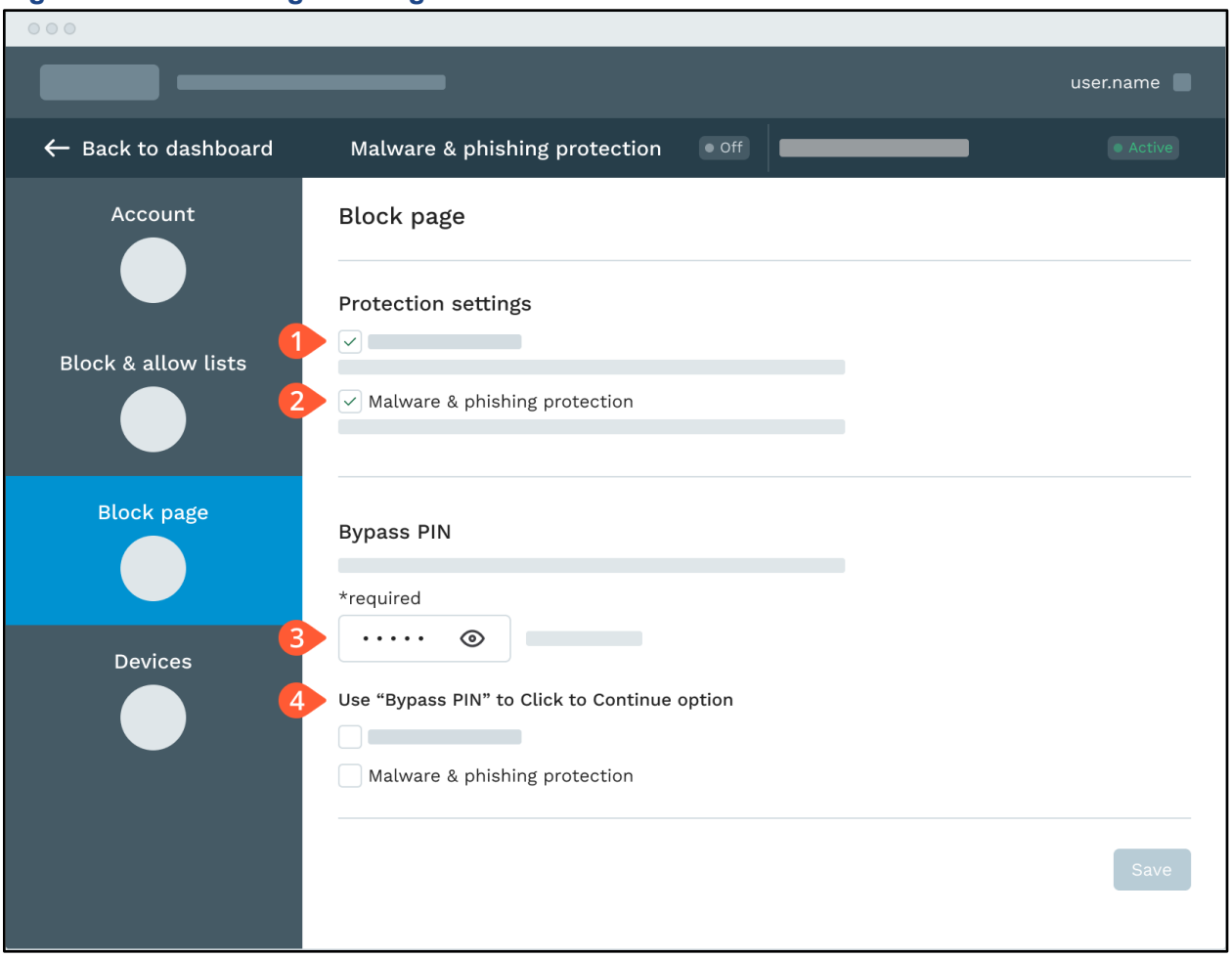


Table 6-1: "Block page" Component Descriptions

Callout	Field	Description
1	"Protection settings"—"Web Filtering" checkbox	Enables and disables web filtering on the devices your Advanced Security service manages. The check box acts as a toggle with the following settings: ● Add a checkmark to the check box to enable web filtering. When web filtering is enabled, your Advanced Security service restricts access to inappropriate websites. When a user attempts to access a blocked website, that user encounters a block page. This is the default setting. ● Clear the checkbox to disable web filtering When web filtering is disabled, your Advanced Security service does not apply web filtering.
2	"Protection settings"—"Malware & phishing protection" checkbox	Enables and disables security service protections on the devices your Advanced Security service manages. The checkbox acts as a toggle with the following settings: ● Add a checkmark to the check box to enable the security service. When the security service is enabled, your Advanced Security service prevents phishing attacks and blocks device access to websites that are infected with malware. When a device attempts to access an infected website, that user encounters a block page. ● Clear the checkbox to disable the security service When the security service is disabled, your Advanced Security service does not protect devices from phishing attacks or block access to infected websites. The security service is disabled by default.
3	Bypass PIN field	Specifies a five-digit device bypass pin that appears on your block pages if the User Bypass PIN Click to Continue option is enabled as described in callout 4. Click the **eye** icon to unhide the PIN. **NOTE:** This field appears only if the Bypass PIN option is enabled for the Advanced Security subscriber portal application.

4	Use “Bypass PIN” to Click to Continue option	Includes an option on a block page requesting the device user to confirm whether to access or leave a requested web page. When you include this option on a block page, the user has the following options: ● Click the **Click to Continue** option to continue accessing the requested web page. When clicked, this section expands to a section requiring the device user to specify the five-digit device Bypass PIN specified in the Bypass PIN field (see callout 3). ● Click the **Go Back** button to return to the previous web page. To add the expanded section to a block page, add a checkmark in the checkbox that is located next to the desired block page name. To remove the expanded section from a block page, clear the checkbox that is located next to the desired block page name. **NOTE:** This field appears only if the Bypass PIN option is enabled for the Advanced Security subscriber portal application.

The figures that follow show examples of the malware and phishing “INFECTED WEBSITE” block pages that include the Use “Bypass PIN” to Click to Continue option.

Figure 6-3 shows a sample Malware and phishing block page. In this example, the block page provides the subscriber with a **Continue to website anyway** option. What happens when the device user clicks on the **Continue to website anyway** depends on whether the “Bypass PIN Click to Continue” option is enabled in the Advanced Security service:

- If the “Bypass PIN Click to Continue” option is enabled in the Advanced Security service, clicking the **Continue to website anyway** option expands a section that prompts the device user to specify a five-digit device Bypass PIN (this is the PIN you set up in the Bypass PIN field when setting up your block pages). Figure 6-4 shows what the expansion prompt looks like. The device user needs to specify the correct PIN in order to access the requested URL.
- If the “Bypass PIN Click to Continue” option is disabled in your service, clicking the **Continue to website anyway** option takes the device user to the requested URL.

Clicking the **Go back** button returns the subscriber to the previous web page.

Figure 6-3: Malware and Phishing Initial Block Page Example

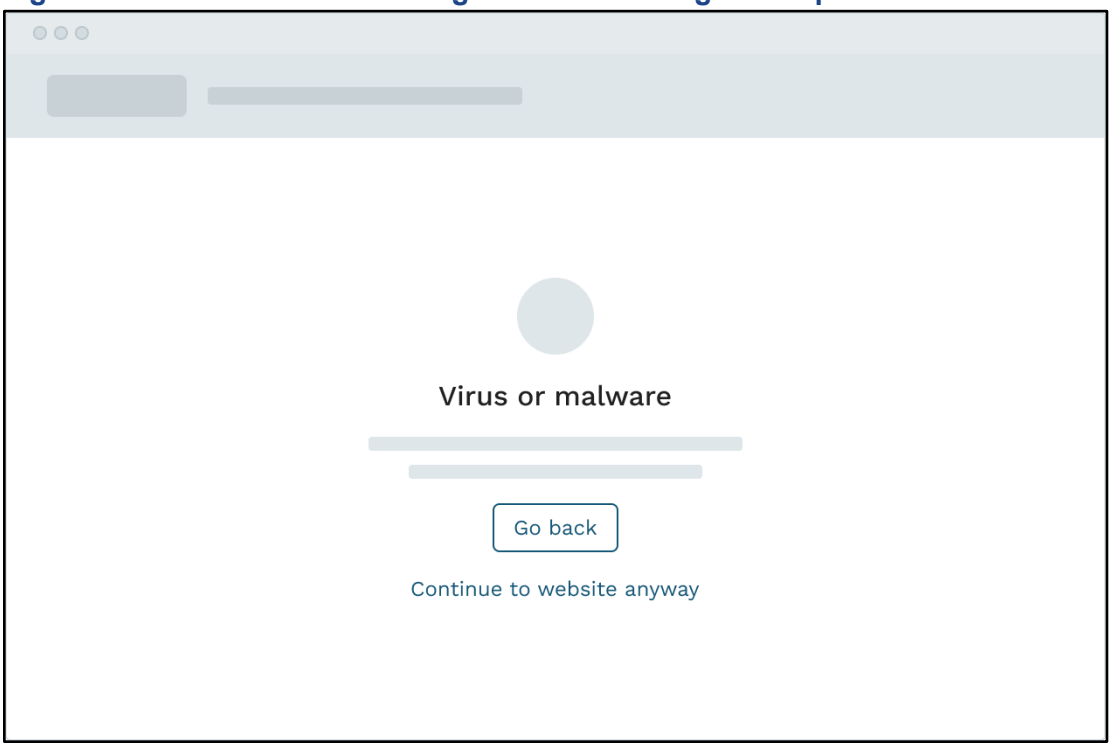


Figure 6-4: Malware and Phishing "INFECTED WEBSITE" Block Page Example with Bypass PIN Expansion

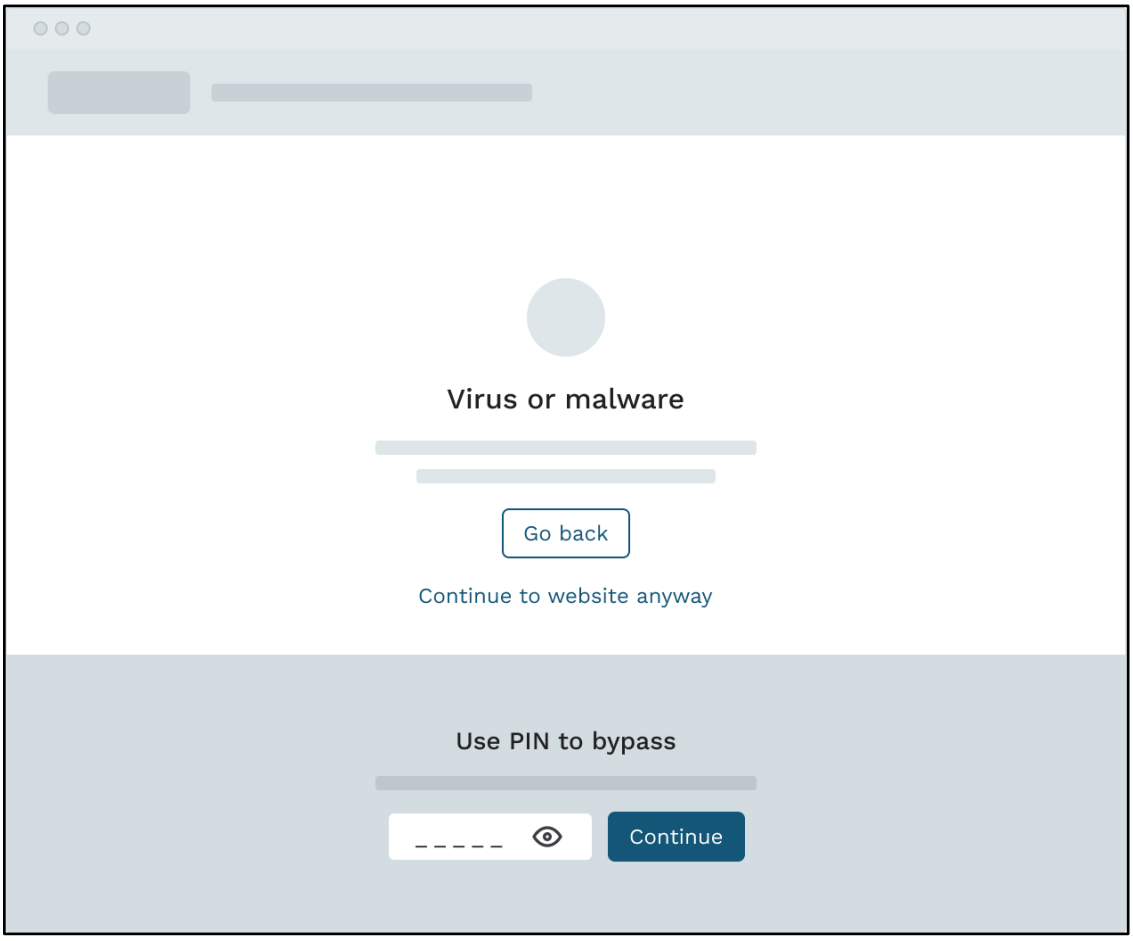


Figure 6-5 shows a sample web filtering block page that a device user encounters when attempting to access a website that falls under a content category that exists in the block list for that user. In this example, clicking the **Continue to website anyway** option expands the Bypass PIN request prompt, along with the following additional options (see Figure 6-6):

- The user can request permanent access to the blocked URL.
- The user can add the URL to their own allow list.

Figure 6-5: Security Service “WEBSITE BLOCKED” Initial Block Page Example

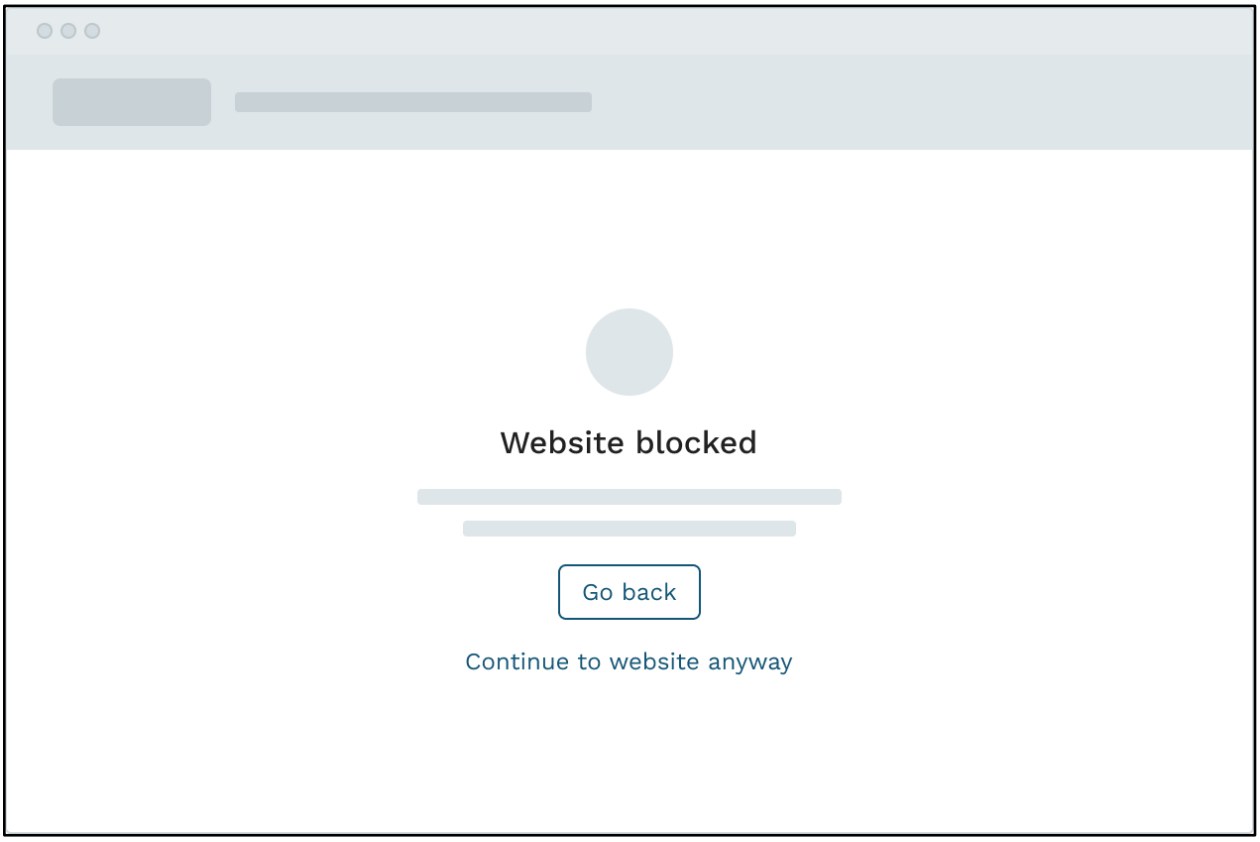
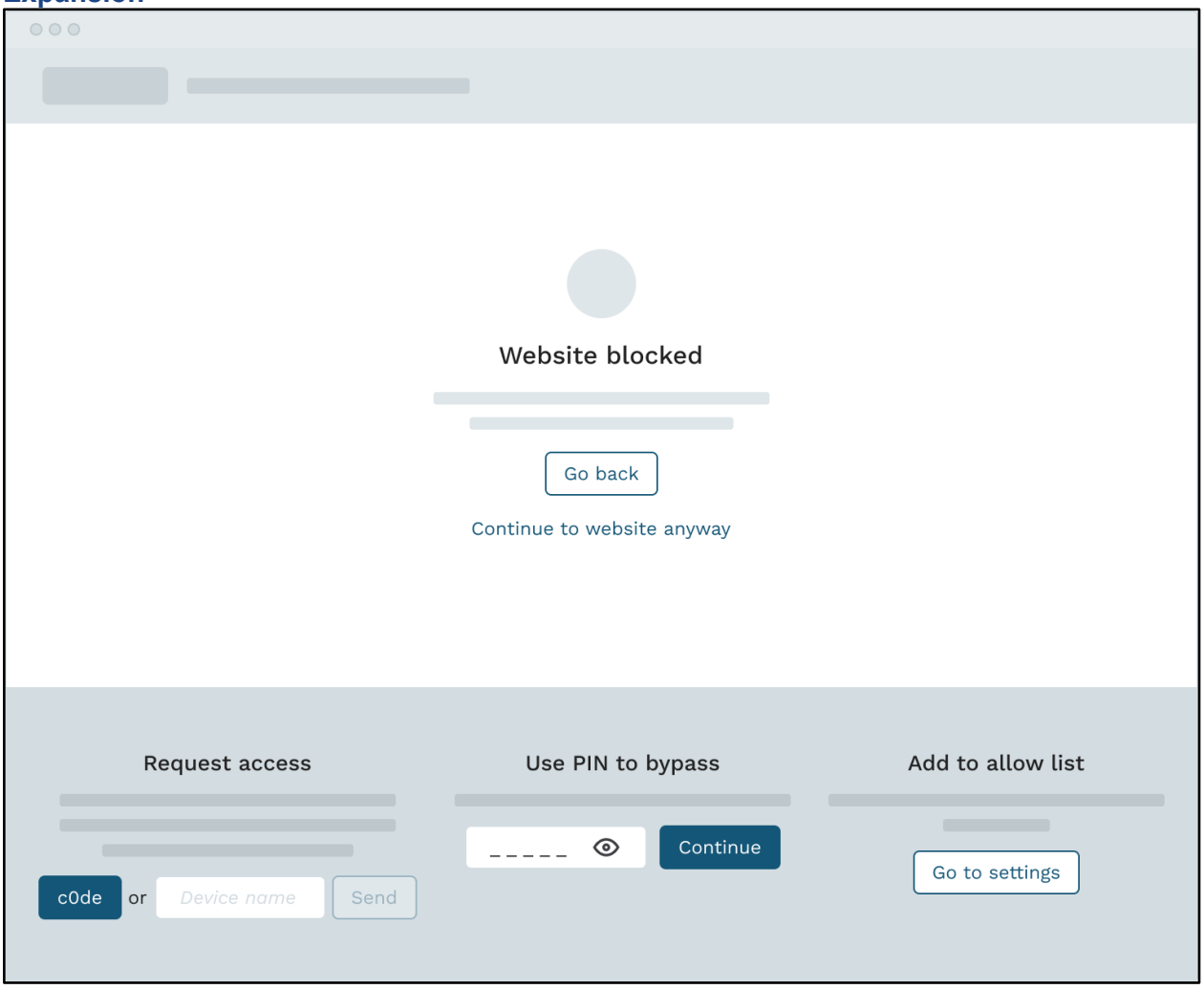


Figure 6-6: Security Service "WEBSITE BLOCKED" Block Page Example with Bypass PIN Expansion



Chapter 7: Managing Statistics and Reporting

The Advanced Security service home dashboard maintains a live report graph that tracks family member and guest Internet activity, along with the corresponding malware, phishing, and botnet block activity.

Figure 7-1 shows where to find the household Internet usage live report on your Advanced Security home dashboard; this example shows what a live report looks like when the Advanced Security service is actively protecting devices and tracking household device usage information. Figure 7-1 includes callouts where each number corresponds to a component described in Table 7-1.

Figure 7-1: Live Report Example

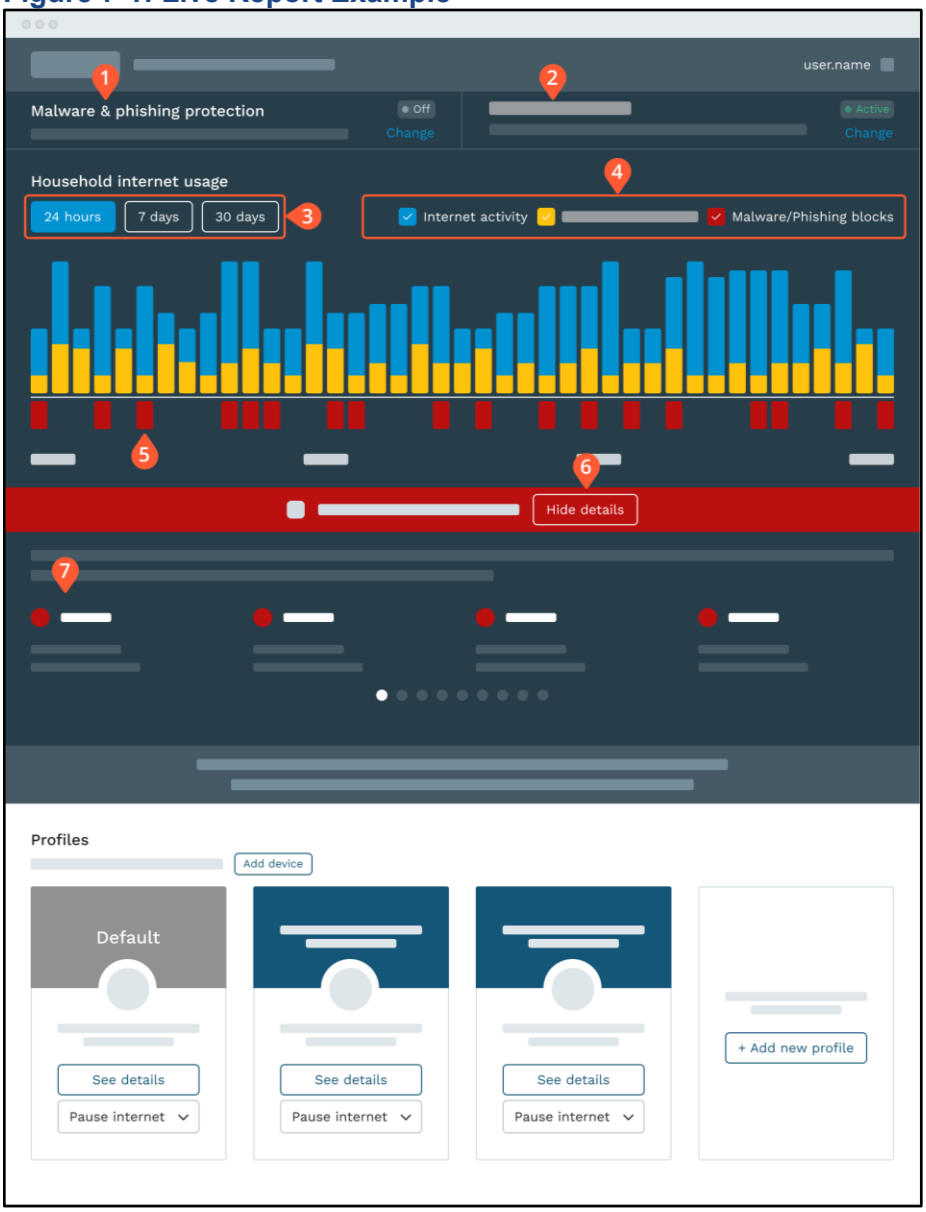


Table 7-1: Live Report Component Descriptions

Callout	Field	Description
1	“Malware & Phishing Protection” control	Indicates whether malware and phishing protection is activated for your Advanced Security account. Clicking the **Change** link takes you to the “Block page” controls, where you can enable and disable the security service. The malware and phishing protection service is disabled by default. **NOTE:** This field is available only if your service is licensed to support the security service. If your service does not include the security service, this field does not appear on your Advanced Security home dashboard. **Caution:** When the malware and phishing protection service is disabled, your devices are susceptible to phishing and downloading malware from malicious websites.
2	web filtering control	Indicates whether web filtering is activated for your Advanced Security account. Clicking the **Change** link takes you to the “Block page” controls where you can enable and disable web filtering. **Caution:** When you disable web filtering, your profiles do not apply to the specified devices and all websites are accessible. **NOTE:** This field is available only if your service is licensed to support the security service. If your service does not include the security service, this field does not appear on your Advanced Security home dashboard.
3	Live report time-period controller buttons	Dictates the time-period for which the live report graph (see callout 5) displays data. Clicking any time period button changes the graph to display information for the selected time period. You can display Internet usage information for the last **24 hours**, **7 days**, or **30 days**. By default, the graph displays Internet usage information for the last **24 hours**.

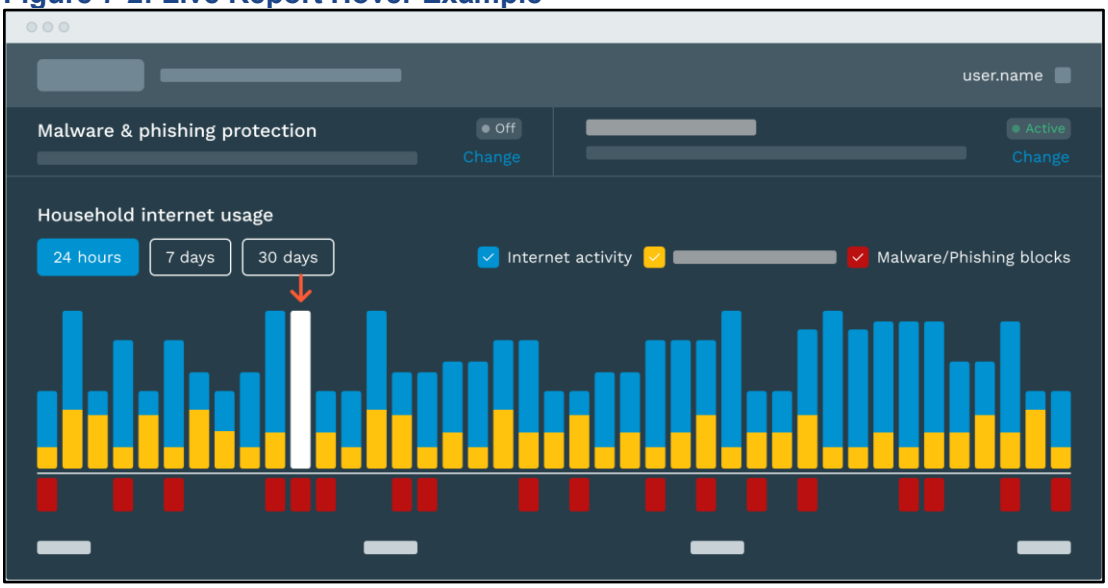
4	Live report data-type selectors	Controls which the data represented in the household Internet usage live report graph (see callout 5). The graph displays the data for the time period specified by the live report time-period control buttons (see callout 3). To include a particular data type in the graph, add a checkmark to the checkbox that appears next to the desired data type; the graph can include the following data types: • **Internet Activity**—Tracks household Internet usage during the specified time period; this data is represented by blue bars in the live report graph (see callout 5). • **Web Filtering Blocks**—Tracks the number of times a device tried to access a blocked or malicious website; this data is represented by yellow bars in the live report graph (see callout 5). • **Malware/Phishing Blocks**—Indicates whether a household user accessed a suspicious website that might have installed phishing or malware on a household device. When this data type is selected, the live report includes an orange alert under the Live Report graph when a household user accesses a suspicious website (see callout 6). Click the **Manage Profile** button to see information pertaining to the affected devices and possible infections. By default, the graph includes **Internet Activity** and **Web Filtering Blocks** data. To exclude a specific data type in the live report, clear the checkbox next to the data type you want to exclude. To include **Malware/Phishing Blocks** alerts in the live report, check the box next to the **Malware/Phishing Blocks** data type and ensure the malware and phishing protection service is **Active** in your Advanced Security service (see callout 1 for more information).

5	“Household Internet Usage” live report graph	Graphical representation of the Internet activity in your household and the number of times a device tried to access a blocked or malicious website. Use the data-type selectors (see callout 4) to control the types of data represented in the graph; use the time-period controller buttons (see callout 3) to direct whether the graph shows data for the last 24 hours, 7 days, or 30 days. To see the date and time frame during which a particular set of blocks occurred, hover your cursor over the desired time-axis point in the graph.
6	“Malware/Phishing Blocks” alerts	Indicates whether a household user accessed a suspicious phishing website or a site that might have installed malware on a household device. The alert contains a toggle button for showing and hiding details about the alerts; these details appear beneath the alert. ● If the malware and phishing block details are hidden, click the **See Details** button to display details about the affected devices and possible infections. ● If the malware and phishing block details display below the alert, click the **Hide Details** button to hide malware and phishing block details. The figure shows what the screen looks like after the user clicks the **See Details** button in the alert (the malware and phishing block details display below the alert).
7	Infected device notification	Provides details about devices that have attempted to access known command and control domains that indicate an active device infection. You can use this information to locate, quarantine, and mitigate infected devices.

To see the date and time frame during which a particular set of blocks occurred, hover your cursor over the desired time-axis point in the “Household Internet Usage” graph.

Figure 7-2 demonstrates what happens when you hover your cursor over a specific time-axis point in the “Internet & Activity Blocks” graph.

Figure 7-2: Live Report Hover Example



Appendix B: Understanding the iCloud Private Relay Blocking Feature

The iCloud Private Relay service is an opt-in feature for paid iCloud users that delivers DNS privacy enhancements. The <*SIA Consumer*> application supports an iCloud Private Relay blocking feature that, when enabled, blocks iCloud Private Relay on devices accessing the <*SIA Consumer*> service. Without the iCloud Private Relay blocking feature enabled in your system, devices that have iCloud Private Relay enabled can access websites your service typically restricts because it routes DNS around service protections.

In the <*SIA Consumer*> application, the “Account” page provides a control for enabling and disabling iCloud Private Relay blocking for a subscriber account. Use the following steps to view and change the iCloud Private Relay blocking setting for a subscriber account:

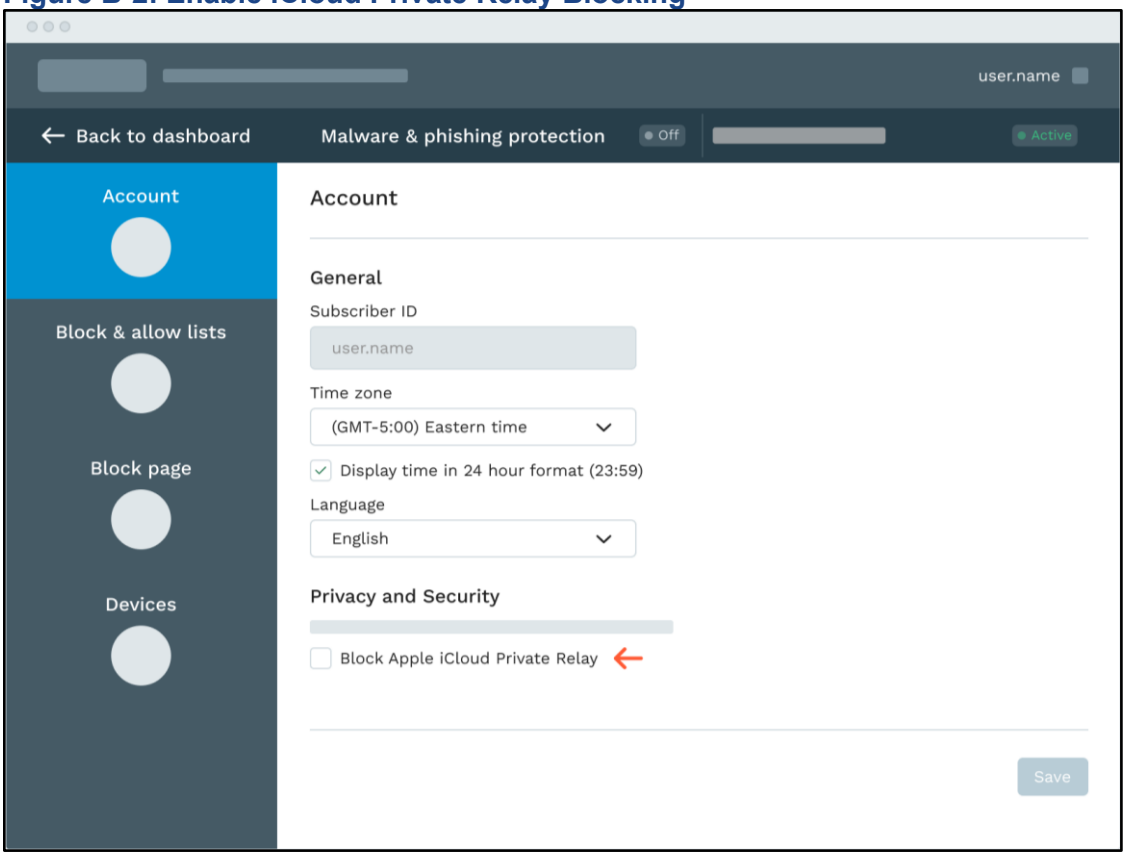
1. To access the “Account” page, select the **Account** option from the **services** drop-down menu as demonstrated in Figure B-1:

   Figure B-1: Access User Account Controls


user.name
Malware & phishing protection
Off
Change
Account
Block & allow lists
Block page
Devices
Clear data
Log Out
Household internet usage
24 hours
7 days
30 days
Internet activity
Profiles
Add device
Default

2. On the “Account” page, locate the “Block Apple iCloud Private Relay” checkbox and, if desired, enable or disable Apple iCloud Private Relay blocking for the subscriber account. Figure B-2 shows where the “Block Apple iCloud Private Relay” checkbox is located on the “Account” page. A checkmark indicates iCloud Private Relay blocking is enabled; clear the checkbox to disable iCloud Private Relay blocking:

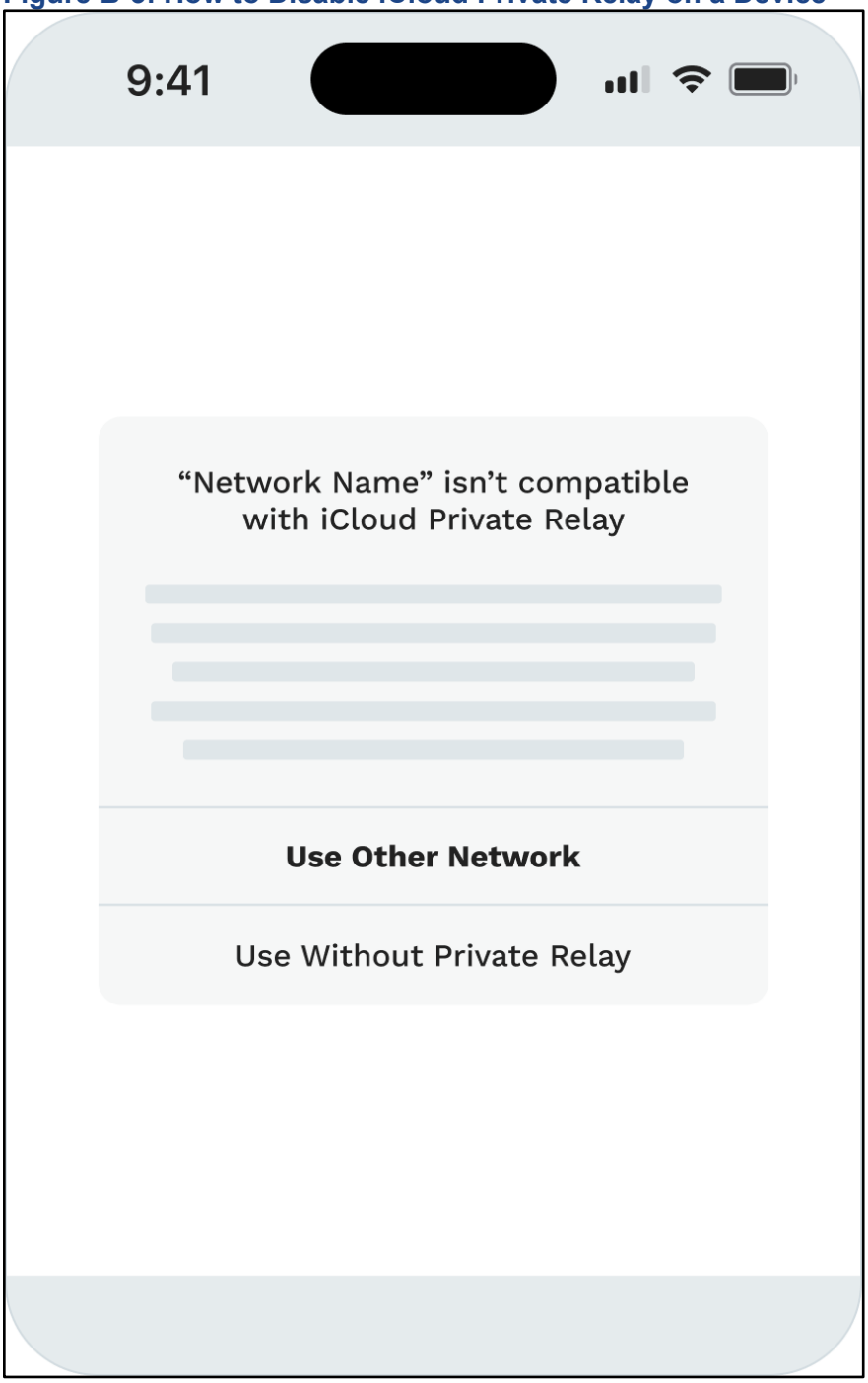
Figure B-2: Enable iCloud Private Relay Blocking



Caution! Be sure to click the **Save** button before navigating to another page in the <*SIA Consumer*> application; the application does not save changes made to your Account settings until you click the **Save** button.

When the iCloud Private Relay blocking feature is enabled in your <*SIA Consumer*> service, devices receive the following warning when trying to access your network, along with the option disable iCloud Private Relay and in order to access your network:

Figure B-3: How to Disable iCloud Private Relay on a Device



Device users can click the **Use Without Private Relay** option to disable iCloud Private Relate on the device.

If the device owner chooses the **Use Without Private Relay** option, iCloud Private Relay disables on the device and the device now has access to your network (along with your specific protections). Figure B-4 shows where iCloud Private Relay is disabled (and can be reenabled) on a device:

Figure B-4: How to Locate the iCloud Private Relay Toggle on a Device