Integrate ZeroFOX with Umbrella

Contents

Introduction

This document describes how to integrate ZeroFOX Enterprise with Umbrella so that the security events can be applied to clients protected by Umbrella.

ZeroFOX Enterprise and Cisco Umbrella Integration Overview

By integrating ZeroFOX Enterprise with Cisco Umbrella, security officers and administrators can extend protection against today's social media-based threats to roaming laptops, tablets, or phones while also providing another layer of enforcement to a distributed corporate network.

Cisco Umbrella and ZeroFox Integration: How does it work?

ZeroFOX Enterprise pushes any threats it finds, such as social media-based cyber threats including targeted malware, phishing, social engineering, impersonations, and other fraudulent or malicious activity, to Cisco Umbrella for global enforcement.

Umbrella then validates the threat to ensure it can be added to a policy. If the information from ZeroFOX is confirmed to be a threat, the domain address is added to the ZeroFOX Destination List as part of a security setting that can be applied to any Umbrella policy. That policy is immediately applied to any requests made from devices assigned to that policy.

Going forward, Cisco Umbrella automatically parses ZeroFOX alerts and adds malicious sites to the

ZeroFOX Destination List—extending ZeroFOX intelligence to all remote users and devices and providing another layer of enforcement to your corporate network.

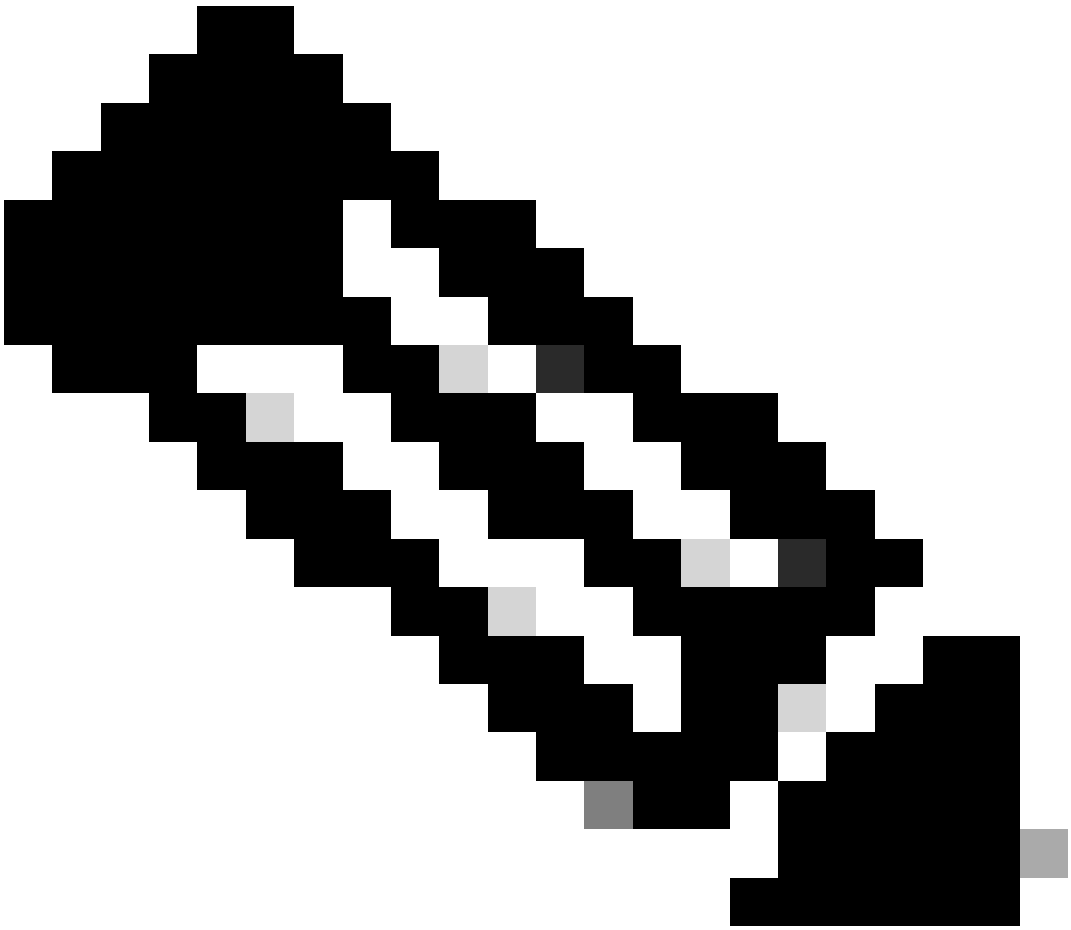
This is achieved through these simple setup steps:

1. Enable the integration in Umbrella to generate an API token.
2. Paste that API token into your ZeroFOX account.
3. Set ZeroFOX to block under security settings for your desired policy(s)

Prerequisites

- ZeroFOX Enterprise administrative rights
- Umbrella dashboard administrative rights
- The Umbrella dashboard must have the ZeroFOX integration enabled

---



Note: The ZeroFOX integration is only included in the Umbrella Platform package. If you do not have the Platform package and would like to have ZeroFOX integration, please contact your Cisco Umbrella representative. If you have the Platform package but do not see ZeroFOX as an integration for your dashboard, please contact Umbrella Support.

Important: While Umbrella tries its best to validate and allow domains that are known to be generally safe (for example, Google and Salesforce), to avoid any unwanted interruptions, we suggest adding any domains you do not want blocked to the Global Allow List or other destination lists as per your policy.

Examples include:

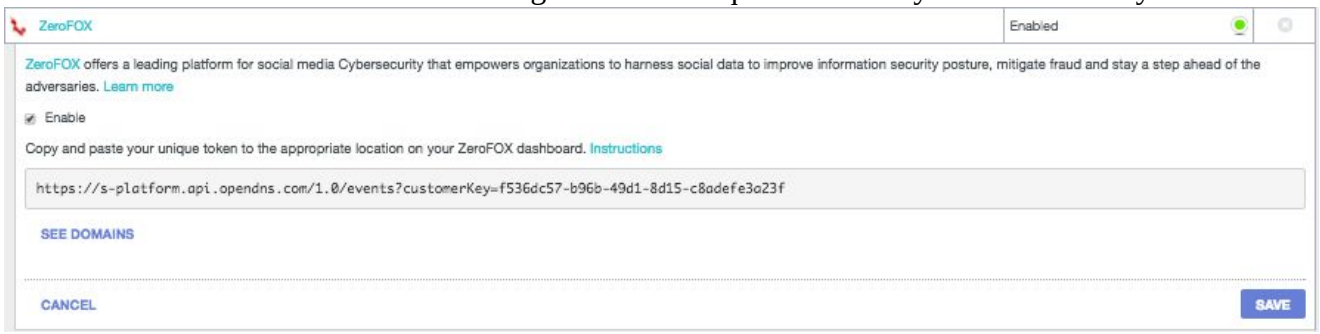
- The home page for your organization. For example, mydomain.com.
- Domains representing services you provide that can have both internal and external records. For example, mail.myservicedomain.com and portal.myotherservicedomain.com.
- Lesser-known cloud applications you depend on heavily that Umbrella can not be aware of or include in their automatic domain validation. For example, localcloudservice.com.

The Global Allow List is found at **Policies** > **Destination Lists** in Umbrella. See our documentation for more information: Manage Destination Lists

Step 1: Umbrella Script and API Token Generation

Begin by finding your unique URL in Umbrella for the ThreatQ appliance to communicate with.

1. Log in to your Umbrella dashboard as an Admin, navigate to **Settings > Integrations** and click "ZeroFOX" in the table to expand it.
2. Check **Enable** and then click **Save**. This generates a unique URL with your customer key.

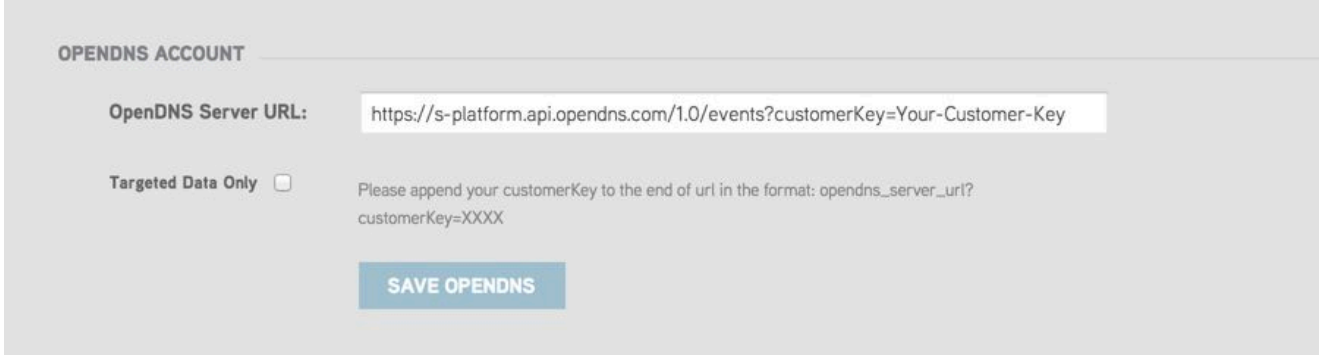


   You need the URL later when you are configuring ZeroFOX, so copy the URL and go to your ThreatQ dashboard.

Step 2: Setup Your ZeroFOX Enterprise Dashboard to Send Information to Umbrella

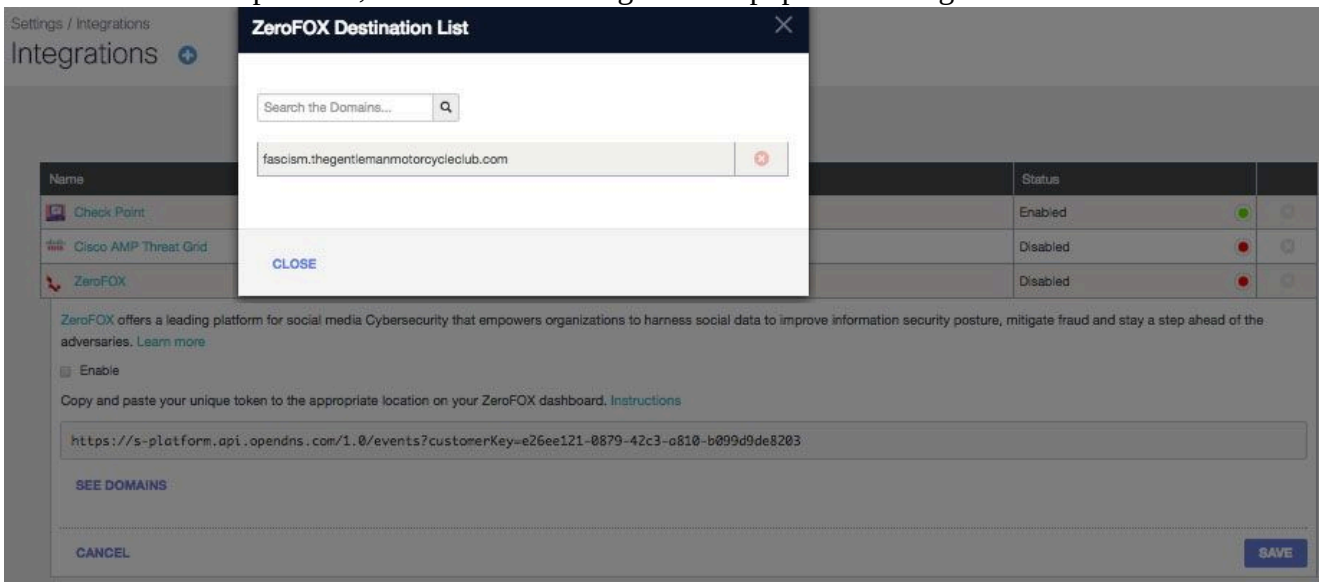
The next step is to add the URL you copied in step one to the ZeroFOX dashboard.

1. Click the gear icon in the Zerofox dashboard, then select **Account Settings**.
2. Scroll down the integration list until you see the OpenDNS Account information and paste the URL from Umbrella into the **OpenDNS Server URL** field.
3. Upon first enablement of the integration, we recommend that you check **Targeted Data Only**.



Step 3: Setup ZeroFOX Events to be Blocked Within Umbrella

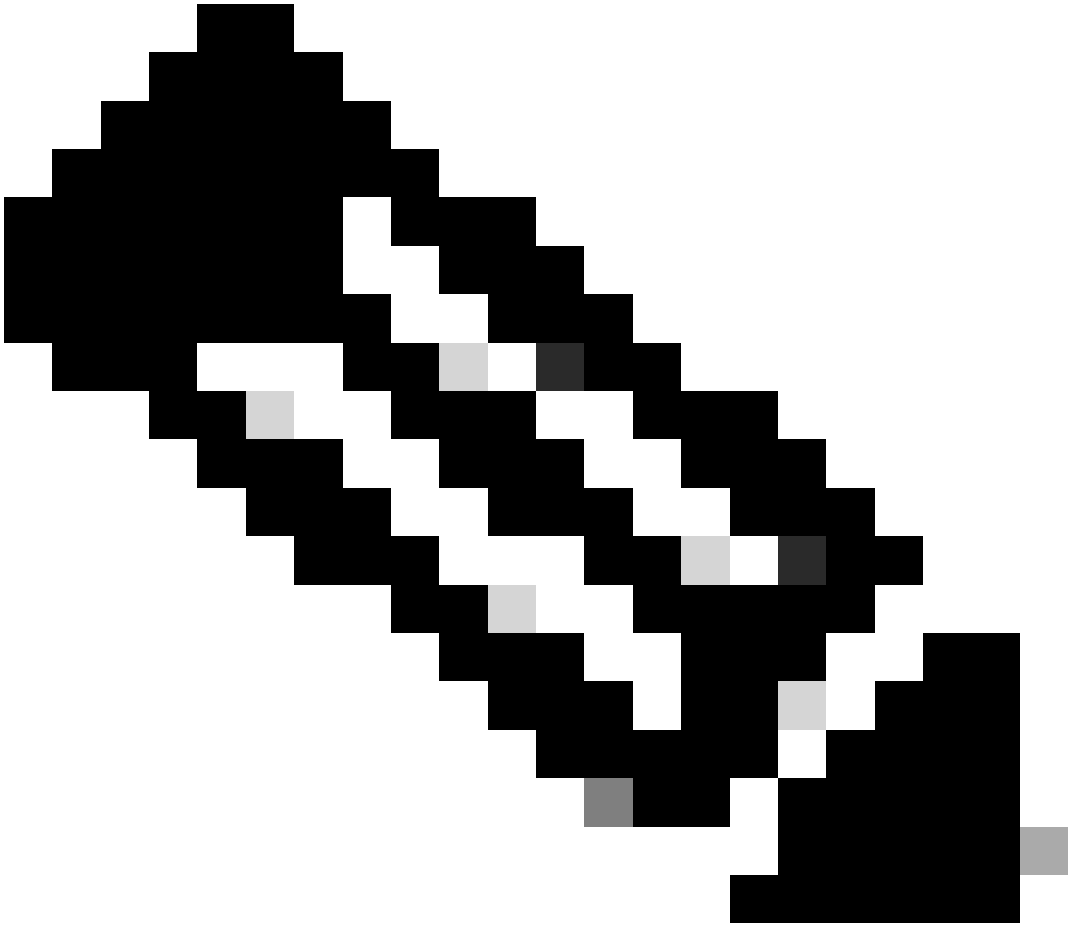
1. Log back in to your Umbrella dashboard as an Administrator.
2. Navigate to **Settings > Integrations** and click on "ZeroFOX" in the table to expand it.
3. Click **See Domains**.
   This expands a list of domains which includes the last few hours of events from your ZeroFOX account. From that point on, a searchable list begins to be populated and grow.



The next step is to observe and audit the events added to your new ZeroFOX Security Category.

Observing Events Added to the ZeroFOX Security Category in Audit Mode

The events from ZeroFOX Enterprise begin to populate a specific destination list that can be applied to policies as a ZeroFOX security category. By default, the destination list and the security category are in Audit mode and are not applied to any policies and do not result in any change to your existing Umbrella policies.



Note: Audit mode can be enabled for however long is necessary based on your deployment profile and network configuration.

Review Destination List

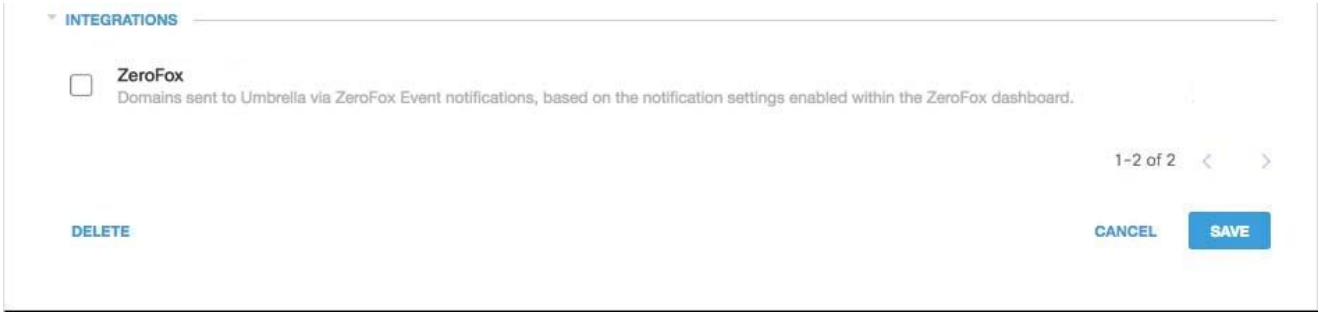
You can review the ZeroFox Destination List at any time.

1. Navigate to **Settings > Integrations**.
2. Expand "ZeroFOX" in the table and click **See Domains**.

Review Security Settings for a Policy

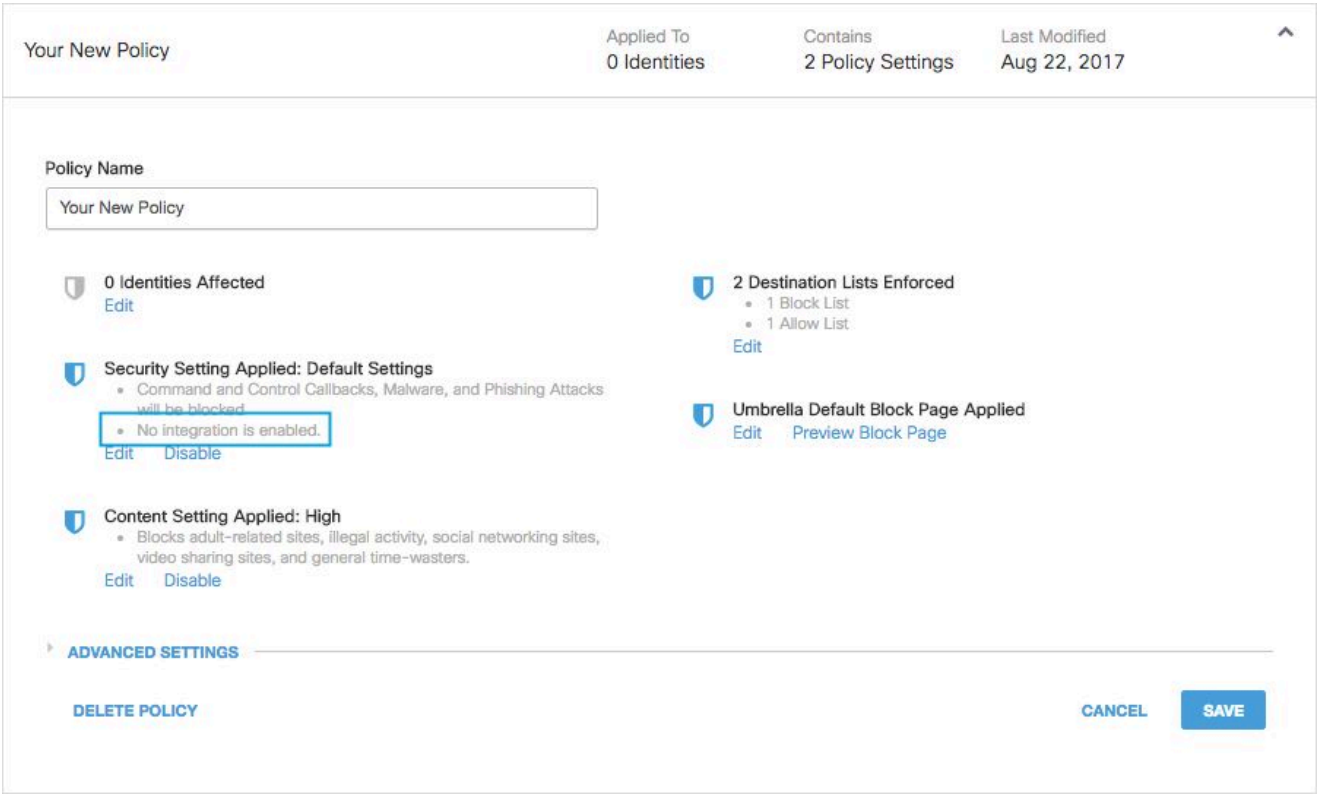
You can review the security setting that can be enabled for a policy at any time.

1. Navigate to **Policies > Security Settings**.
2. Click a security setting in the table to expand it and scroll to **Integrations** to locate the ZeroFOX setting.



115014041606

You can also review integration information through the **Security Settings Summary** page.

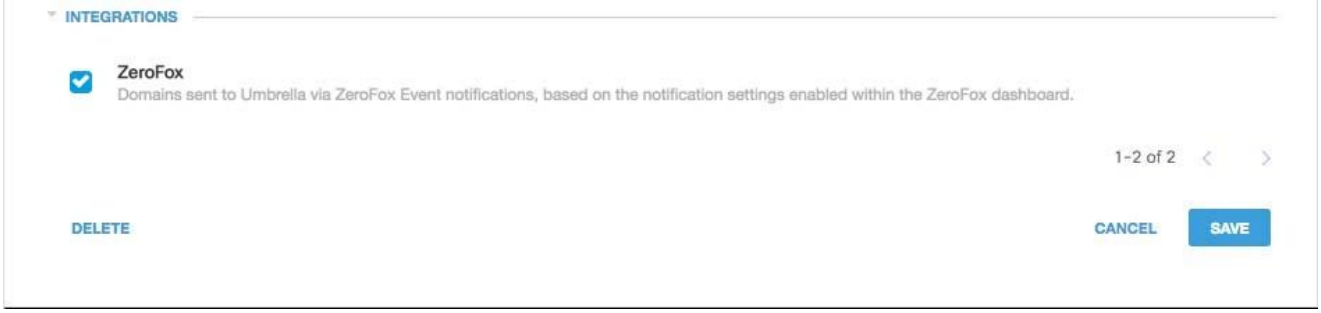


25464154913556

Applying the ZeroFOX Security Settings in Block Mode to a Policy for Managed Clients

Once you are ready to have these additional security threats enforced against by clients managed by Umbrella, simply change the security setting on an existing policy, or create a new policy that sits higher than your default policy to ensure it is enforced first.

1. Navigate to **Policies > Security Settings** and under Integrations, check **ZeroFOX** and click **Save**.



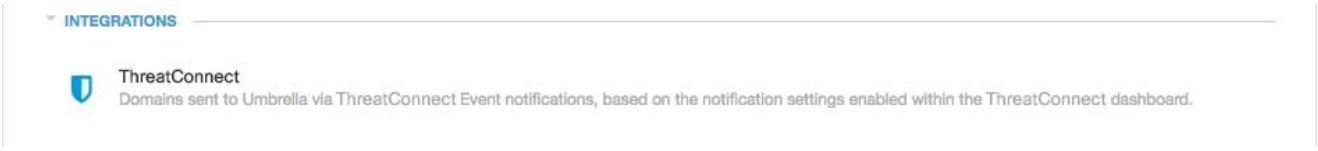
115014042806

Next, in the Policy wizard, add a security setting to the policy you are editing:

1. Navigate to **Policies > Policy List**.
2. Expand a policy and click **Edit** under Security Setting Applied.
3. In the **Security Settings** pull-down, select a security setting that includes the ThreatConnect setting.

25464147943700

The shield icon under **Integrations** updates to blue.



25464147957652

4. Click **Set & Return**.

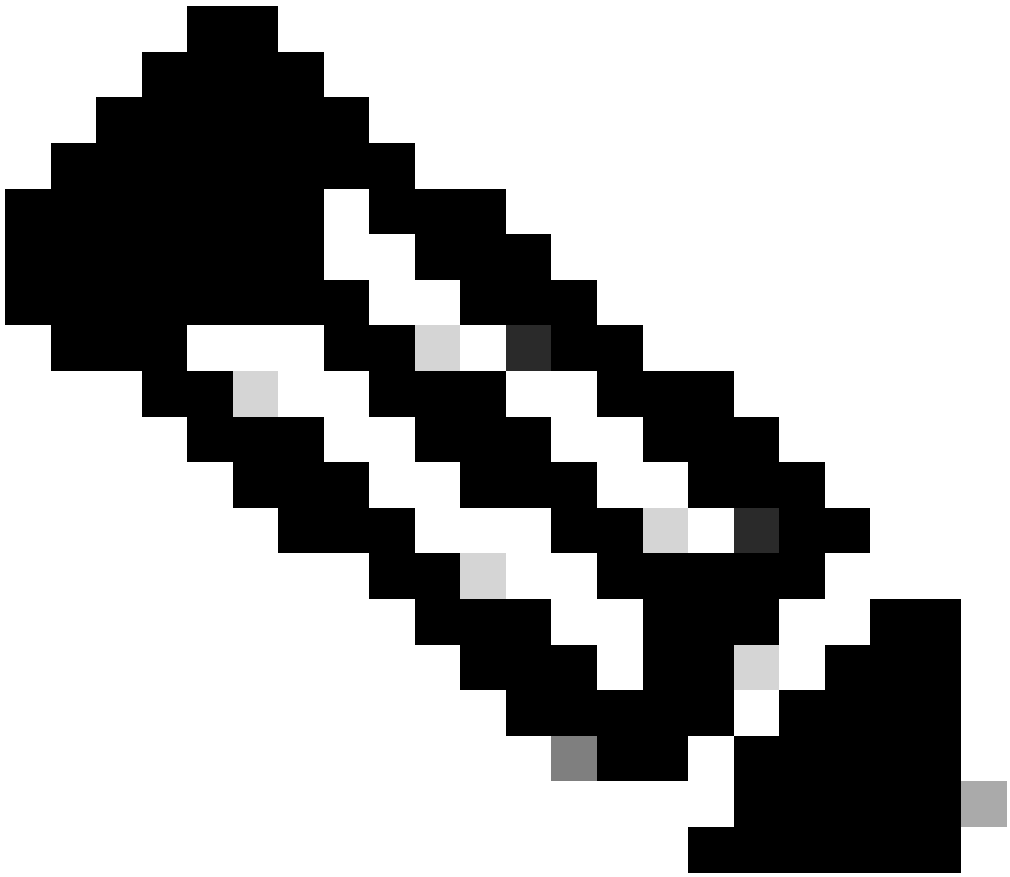
ZeroFOX domains contained within the security setting for ZeroFOX are blocked for those identities using that policy.

Reporting in Umbrella for ZeroFOX Events

Reporting on ZeroFOX Security Events

The ZeroFOX Destination List is one of the security categories lists you can report on. Most or all of the reports use the Security Categories as a filter. For instance, you can filter security categories to only show ZeroFOX related activity.

1. Navigate to **Reporting > Activity Search** and under **Security Categories** select **ZeroFOX** to filter the report to only show the security category for ZeroFOX.



Note: If ZeroFOX integration is disabled, it does not appear in the Security Categories filter.

115014043046

2. Click **Apply**.

Reporting When Domains Were Added to the ZeroFOX Destination List

The Umbrella Admin Audit log includes events from your ZeroFOX account as it adds domains to the destination list.

The Umbrella Admin Audit log can be found at Reporting > Admin Audit Log. In order to report on when a domain was added, filter to only include ZeroFOX changes by applying a filter to **Identities & Settings** for the ZeroFox Destination List.

Once you run the report, you see a list of the changes made when the ZeroFOX Destination List was added to from the integration.

Handling Unwanted Detections or False Positives

Managing an Allow List for Unwanted Detection

Although unlikely, it is possible that domains added automatically by ZeroFOX could trigger an unwanted block that would prevent users from accessing particular websites. In a situation like this, we recommend adding the domain(s) to an allow list, which takes precedence over all other types of block lists, including security settings. An allow list takes precedence over a block list when a domain is present in both.

There are two reasons that this approach is preferable. First, in case the ZeroFOX appliance was to re-add the domain again after it was removed, the allow list safeguards against this causing further issues. Secondly, the allow list shows a historical record of problematic domains that can be used for forensics or audit reports.

By default, there is a Global Allow List that is applied to all policies. Adding a domain to the Global Allow List results in the domain being allowed in all policies.

If the ZeroFOX security setting in block mode is only applied to a subset of your managed Umbrella identities (for instance, it is only applied to roaming computers and mobile devices), you can create a specific allow list for those identities or policies.

To create an allow list:

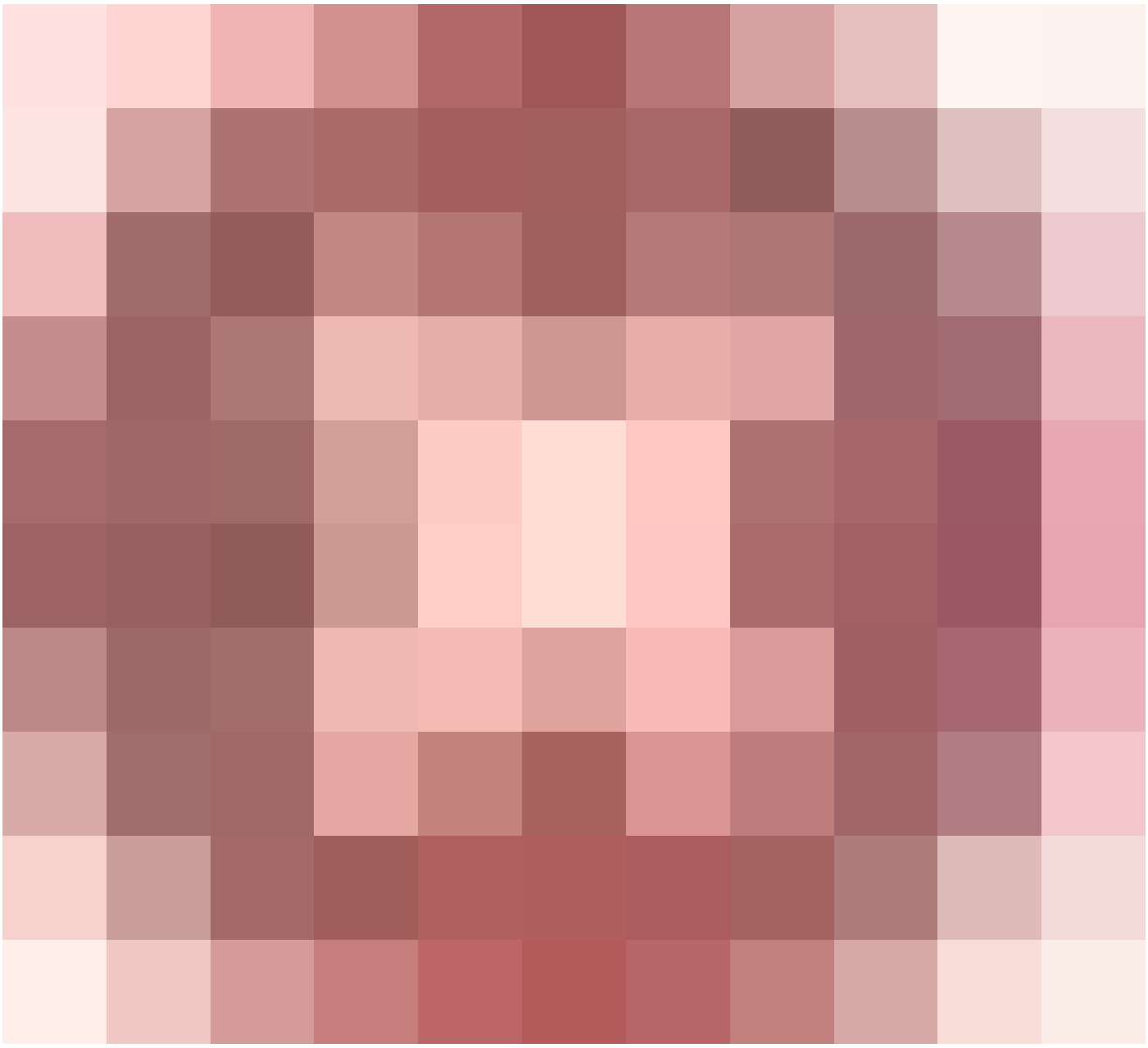
1. Navigate to **Policies > Destination Lists,** click the 

   Add icon.
2. Select **Allow**, and add your domain to the list.
3. Click **Save**.

Once the destination list has been saved, you can add it to an existing policy covering those clients that have been affected by the unwanted block.

Deleting Domains from the ZeroFOX Destination List

There is a



(**Delete**) icon next to each domain name in the ZeroFOX Destination List. Deleting domains lets you clean up the ZeroFOX Destination List in the event of an unwanted detection.

However, the delete *is not* permanent if ZeroFOX resends the domain to Umbrella.

To delete a domain:

1. Navigate to **Settings > Integrations**, then click "ZeroFOX" to expand it.
2. Click **See Domains**.
3. Search for the domain name you want to delete.
4. Click the **Delete** icon.

5. Click **Close**.
6. Click **Save**.

In the instance of an unwanted detection or false positive, we recommend creating an allow list in Umbrella immediately and then remediating the false positive within ZeroFOX. Later, you can remove the domain from the ZeroFOX Destination List.