Troubleshoot Block Page Bypass or Allow-Only Mode

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Problem

Solution

Introduction

This document describes how to troubleshoot websites not working in Block Page Bypass or Allow-Only Mode.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

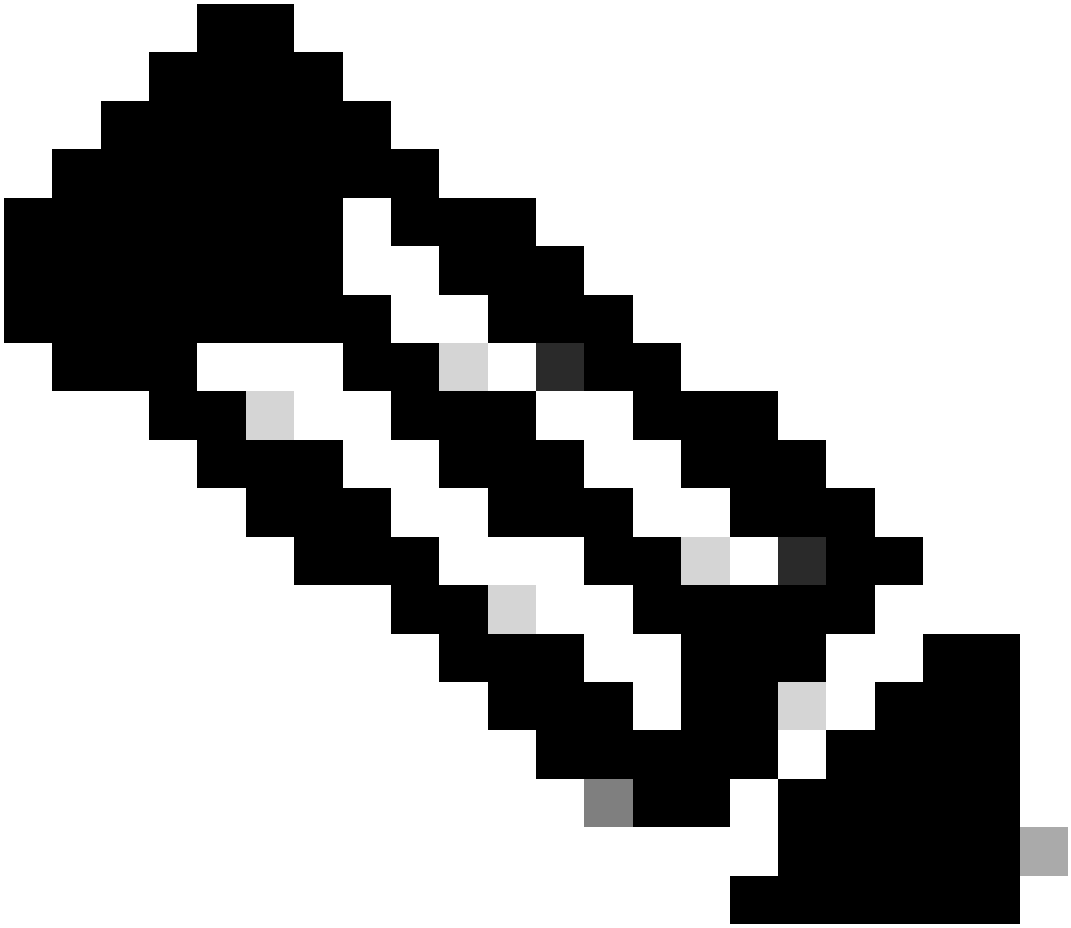
When using Block Page Bypass or Allow-Only Mode, you see a website that does not fully load all content, does not allow you to log in, or some video or audio is not streaming properly.

The issue becomes more common and noticeable when content filtering is set to "High" or "Custom" with many or most categories being blocked. The reason is that much of the aforementioned content (images, JavaScript, and so on) can load from domains which are tagged as "Business Services", "Research/Reference", "File Storage", "Ecommerce/Shopping", and so on.

This article outlines the causes for these problems as well as a list of additional domains for highly requested sites.

Solution

Since this is how Block Page Bypass works, Umbrella recommends adding additional domains to your **Destination** list.



> **Note**: This is different than the Block Page Bypass Allow List, which is what you use to add the top-level domain (for example, netflix.com).

Similarly, Allow-Only Mode can require other domains to be added to the allow list in order to fully utilize the website.

After a problem is detected and a domain is not loading properly, search against the identity that had trouble accessing a site to see blocks for additional domains beyond the one that was being accessed. These are the domains that you need to add to the allow list.

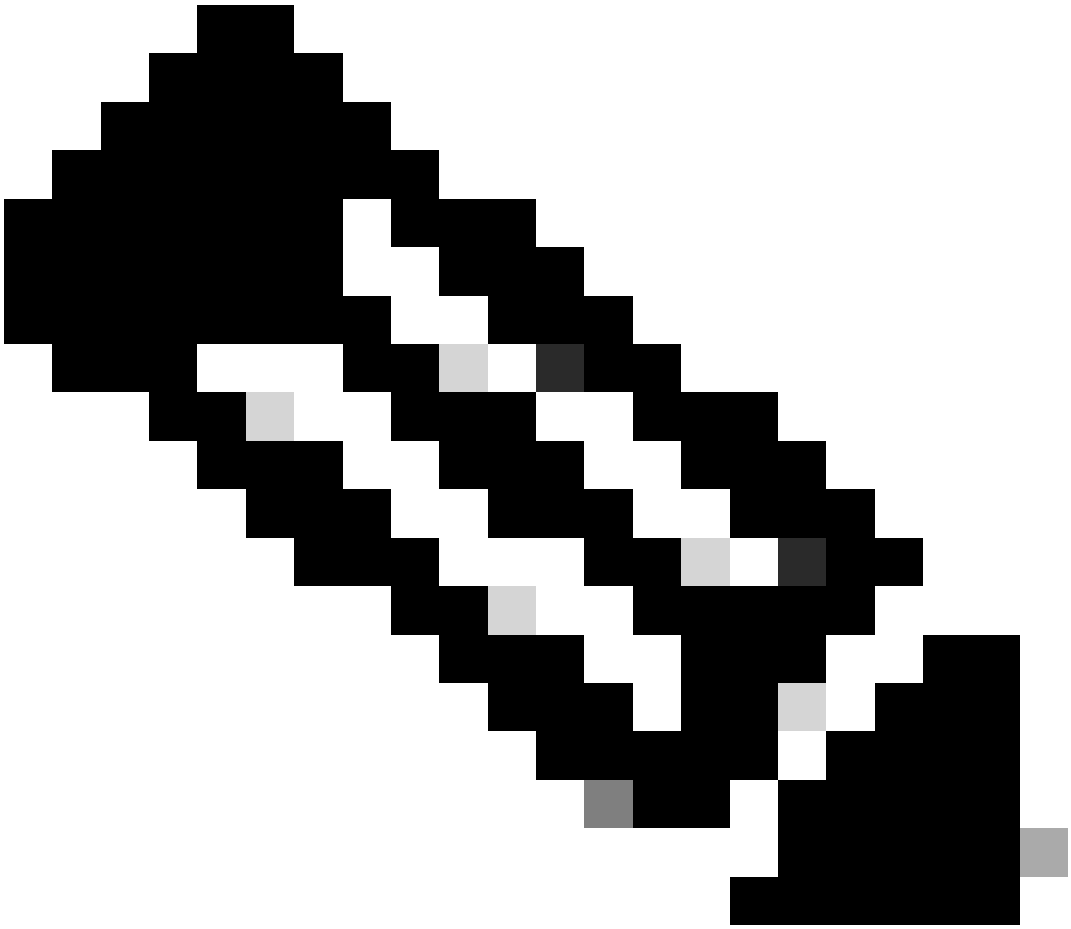
To run a report for this:

1. Navigate to **Reporting > Activity Search**.

2. Apply a filter for the identity you were testing with, as well as ensuring you are only showing "Blocked" results.

3. Select **Run Report**.

This gives you an idea of what you need to add to your Global Allow List, add domains to the Global Allow List, or to create a new allow list. For more information, refer to Umbrella documentation from earlier in this article.



Note: It takes a few minutes for the policy changes to take effect.

To see a list of our most frequently asked domain names with these issue, please read this Umbrella knowledge base article.