Configure File Inspector to Allow Password-Protected and Other Non-Malicious Files

Contents

Introduction

This document describes how to prevent a non-malicious file from being blocked by file inspection.

Issue

Enabling "File Inspection" in some cases this blocks non-malicious files. These types of files include:

- Password-protected files
- Potentially Unwanted Application (Corrupt) files

These files are blocked by Umbrella because they cannot be decompressed and scanned by our anti-virus tool. Password-protected files can appear blocked under the "Protected File" category. Corrupted files could include files that have encrypted content, have archived contents that cannot be extracted, have invalid compressed data or an invalid archive header, or is simply compressed or archived in an unsupported format. While these files can be non-malicious, Umbrella blocks them by default as a precaution as the files cannot be scanned.

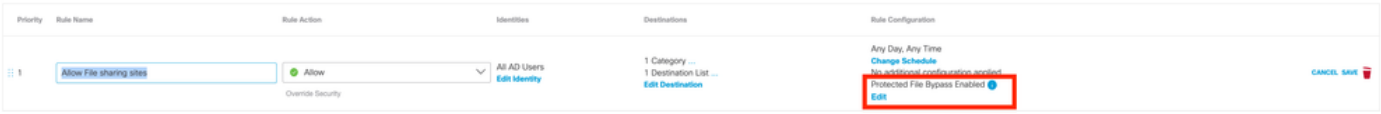
Solution

If you know of a non-malicious file that has been blocked because of one of the reasons above, you can work around this by allowing Protected Files. The behaviour of blocking protected files can now be changed at a Global level or in an individual web rule.

- **Rule (Recommended) -** Allow protected files for an identity and/or destination. Do this if you want to trust protected files from a particular destination or wish to override the behaviour for an individual user/group.
- **Global** - Allow protected files for all users in all rules/rulesets. Do this if you accept the risk of protected file downloads and prefer this option over the administrative burden of making more granular exceptions.

Rule

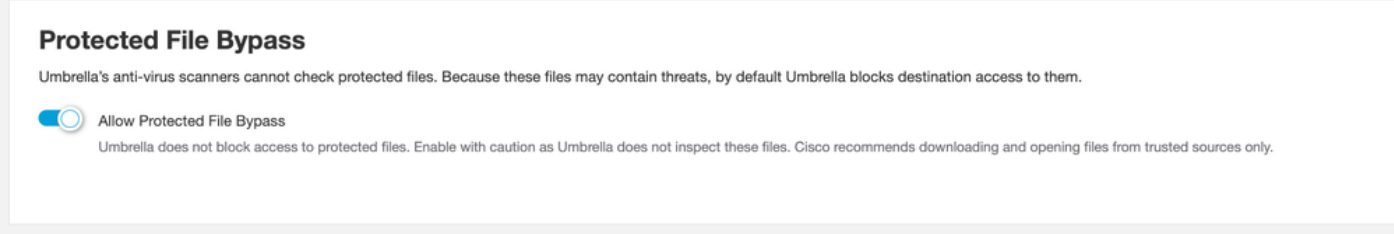
The functionality can be changed by editing a web rule on the **Policies** > **Web Policies** page.



10588971481748

Global

The functionality can be changed in **Policies** > **Web Policies** > **Global Settings**.

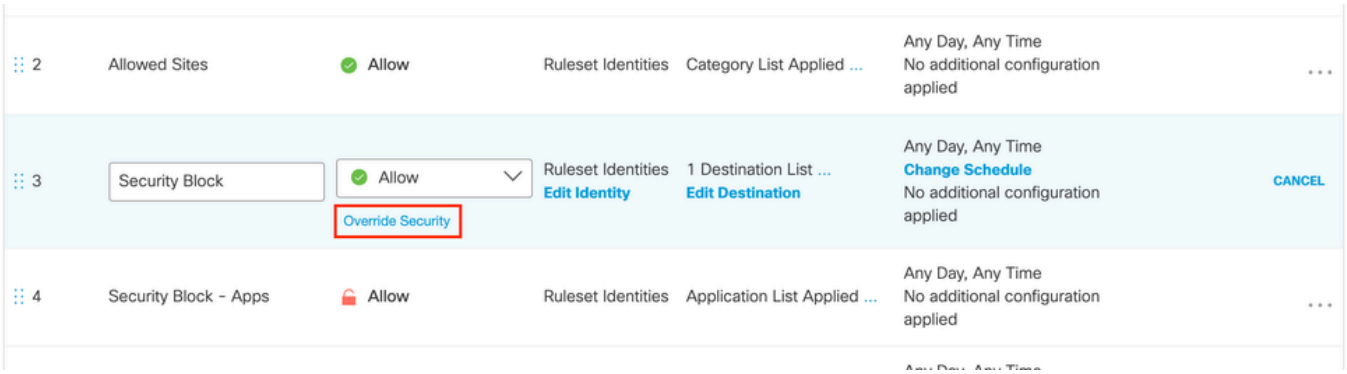


10589018672020

Alternative Solution

It is also possible to bypass problems with File Inspection using the **Override Security** option in any web policy. This option must be used with **caution** because it **disables all other security settings including blocking of malicious files**.

- For protected files, use one of the solutions described in this document instead.
- Use this only in circumstances where you trust the destination with absolute certainty and have no other option to workaround the problem.
- For Anti-Virus false positives, get confirmation that the file is clean from Cisco Talos before implementing any workarounds.



Screen_Shot_2021-10-07_at_2.59.04_PM.png