Understand Umbrella LA Release of Block Password Protected File Upload DLP Feature

Contents

Introduction

This document describes the Limited Availability (LA) of the Block Password Protected File Upload DLP feature.

Background Information

Blocking password protected files uploads is an important measure for preventing data loss as password protected files cannot be inspected by DLP solutions.

How does Block Password Protected File Upload work?

Once the feature is enabled, the Block Password Protected File Upload applies to any destination that's configured with Realtime DLP (such as, inline) rules.

If you wish to prevent all password protected file uploads must have at least one Realtime DLP rule that has 'All Destinations' set in the Destination rule criteria.

Conversely, if you only wish to block password protected file uploads to specific destinations must make sure they do not have a Realtime DLP rule that has 'All Destinations' set in the Destination rule criteria.
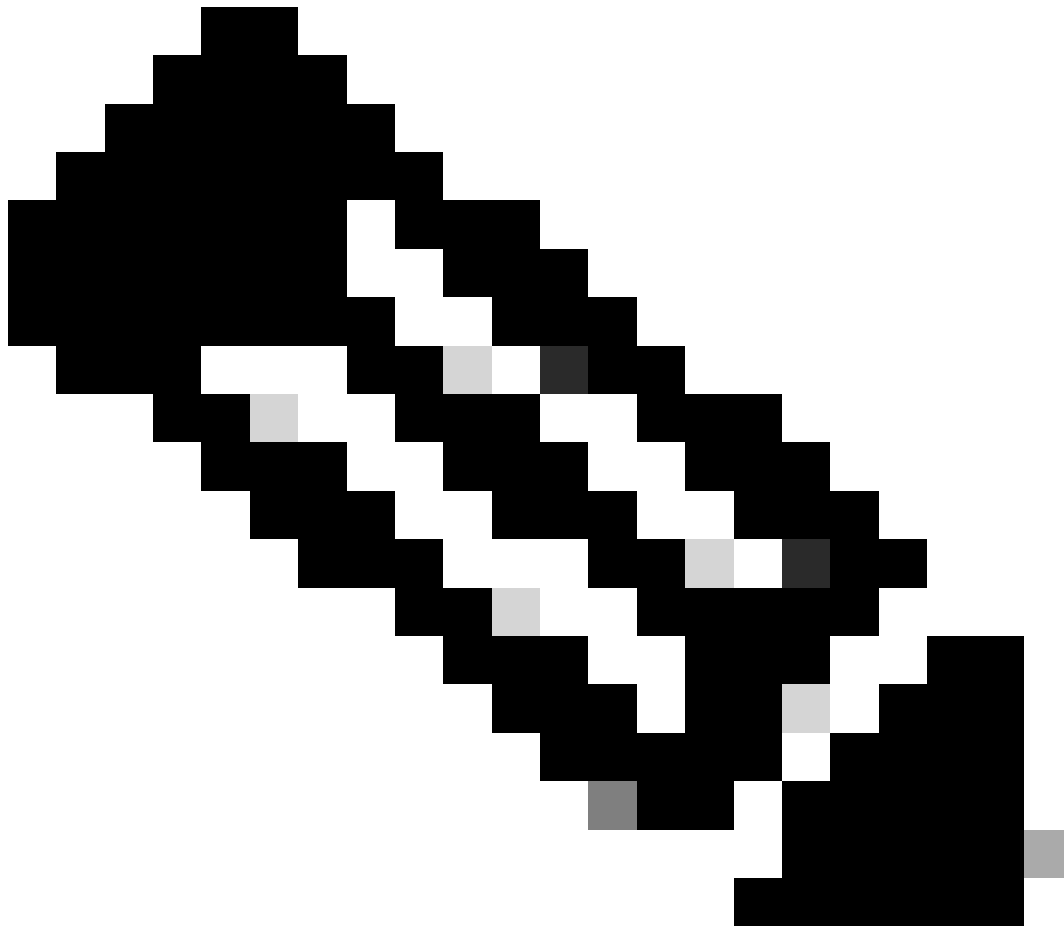
> **Note**: Destination exclusions in Realtime DLP rules do not apply to the Block Password Protected File Upload and still apply to all destinations.

How is the Block Password Protected File Upload Packaged?

This feature is available with all Umbrella packages that include DLP (i.e SIG-A and DLP-addon).

How Can I Access This Feature?

Please open a support ticket to be considered for enrollment into this limited availability feature.

Can I Enable or Disable This Feature in the Umbrella Dashboard?

Not at this moment. Once we enroll you into the LA program, we enable it on your behalf.

Where Can I Find the List of Supported File Types?

The list of file types that are supported by the Block Password Protected File Upload is available [here](#) and can be shared with LA customers.