# Understand New Features in Umbrella Dashboard

## Contents



## Introduction

This document describes the file inspection and custom URL blocking via destination lists in the Umbrella Dashboard.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the Umbrella dashboard.

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.

## New Features

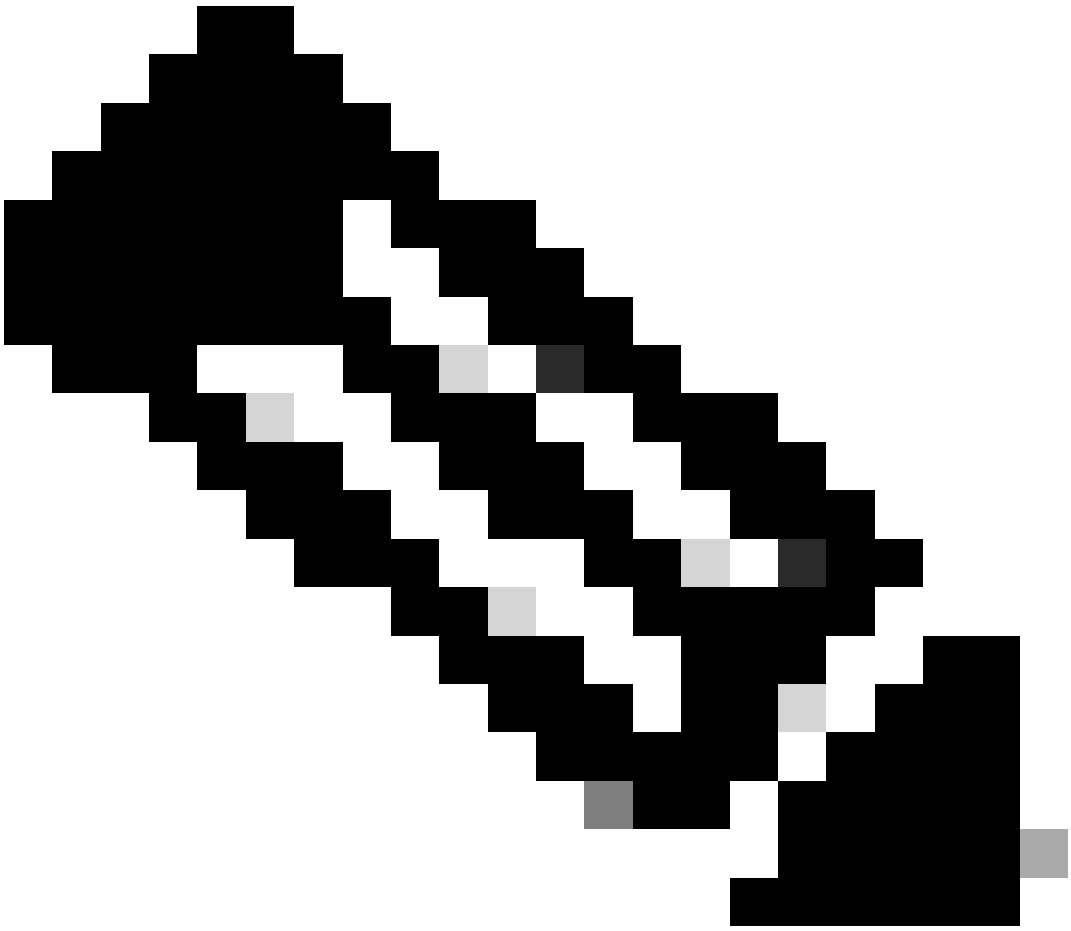
Umbrella is introducing a new set of features that improves your functionality. With this change, you can see two new features in your dashboard right now:

- File inspection scans the files that your identities download to see if they contain malicious code and block them if they do.
- Custom blocked URLs gives you the ability to block your own set of URLs in a destination list. This now gives you the flexibility to block specific pages without blocking entire domains.

To help you take advantage of this new feature, you can use the new and updated reports and a new policy creation experience..The file inspection feature is one of several  planned for future releases built around

advancing the Intelligent Proxy infrastructure to deliver even more cloud-based security for you.

---



> **Note**: These features are being rolled out in small increments to our customers and these updates are in limited availability as Umbrella progresses with this release. If you received an alert in your dashboard about these features, you have them. And if you would like to find out more about these features, contact umbrella-support@cisco.com.

---

The file inspection feature is only available for customers with the Umbrella Insights or Umbrella Platform packages. Read more about packages and contact your Cisco account representative with any questions.

## How to Take Advantage of these Features

Access to these new features is available in a couple of places: the policy wizard allows you to enable File Inspection from the summary page, and through destination lists you can add custom URLs to your blocked destination lists. Additionally, custom URL blocking can also be managed specifically from the **Destination Lists** management page.

On the reporting side, the reports navigation section of the Umbrella dashboard has been updated so you can easily find the new and updated reports. Read more in this article on how to enable these features and check out some reports.

## File Inspection

File inspection is a feature of the Intelligent Proxy that extends its scope and functionality by adding the ability to scan files for malicious content hosted on suspicious domains. A suspicious domain is neither trusted nor known to be malicious.

With the Umbrella policy wizard, file inspection is easy to implement. Navigate to **Policies > Policy List** and either expand a policy or select the **+ (Add)** icon to create a new policy. In the policy wizard, ensure **File Inspection** is enabled on the summary page, or from a new policy, select **Inspect Files** after you have enabled the Intelligent Proxy (under **Advanced Settings**). Read more in the full documentation for this feature.

## Testing File Inspection

From a device that is enrolled in a policy with File Inspection enabled:

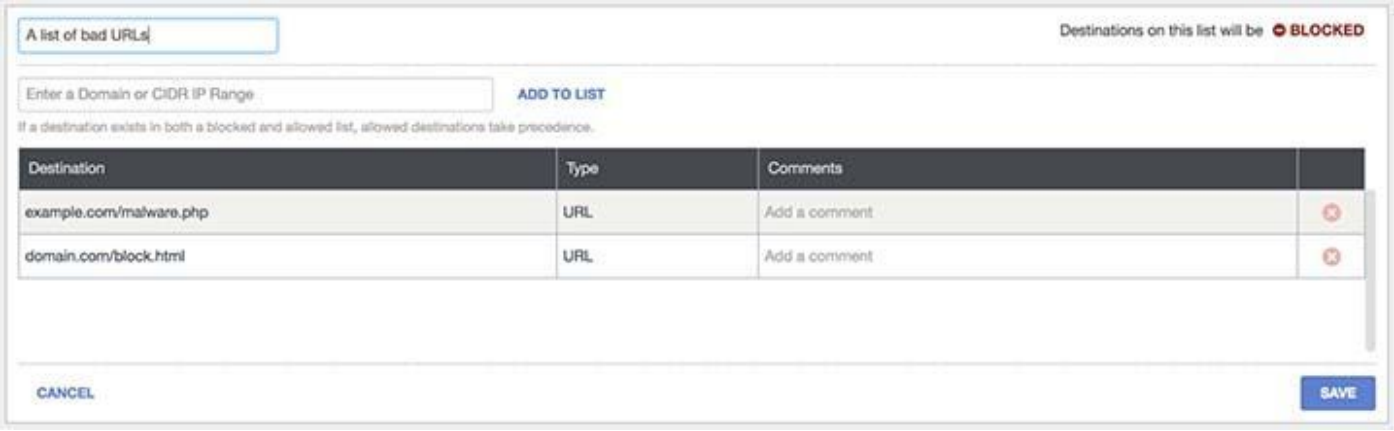
1. Browse to http://proxy.opendnstest.com/download/eicar.com.

2. A block page like this screenshot appears.


*Umbrella Blocked Page*

## Enable URLs to be Blocked in Your Destination Lists

To block a URL, simply enter it into a blocked destination list, or create a new blocked destination list just for URLs. To do this, navigate to **Policies > Destination Lists**, expand a **Destination list**, add a **URL**, and then select **Save**.




*Umbrella Blocked Destination List*

Read more in the full documentation for this feature.

In order for the Umbrella infrastructure to inspect a URL to determine if it matches the ones defined in your blocked destination list, you must have the following:

- The Intelligent Proxy and SSL Decryption must be enabled as a part of the policy. For more information, read the Umbrella docs.
- The Cisco Umbrella Root CA must be installed on the computer(s) using this policy—ensures https connections are filtered, too. For more information, read the Umbrella docs.

It is important to specify a URL correctly so that what is in your policy matches what the user is trying to access (and is subsequently blocked). For more information on what URLs you can or cannot use, please read Custom URL Destination List How-to.

# Reporting

Umbrella now has new and improved reports:

- The Security Overview Report: Gives you an easy to read snapshot of your network activity through charts and graphs. You can quickly see activity in your identities and their traffic, illustrating where problems can be occurring. Learn more about it in the Umbrella docs.
- The Security Activity Report: Highlights security events flagged, but not necessarily blocked, by Umbrella threat intelligence. This includes security events filtered through the Intelligent Proxy and file inspection. Learn more about it in the Umbrella docs.

- Activity Search report: Helps you find the result of every DNS, URL, and IP request from your various identities, ordered by descending date and time. This report can list all security related activity within Umbrella for the selected time period, and allows you to refine your search using filters to see only what you want to see. Learn more about it in the Umbrella docs.

These reports are easy to get as well.

# Sending Umbrella Feedback

Umbrella would love to hear what you think about these new features. Any questions or comments you have, Umbrella wants to hear from you! Send your feedback to umbrella-support@cisco.com and include as much detail as possible. For example, screenshots, the browser you are using, your OS and the scenario within which you are using these features.