Understand Blocked Requests in the App Discovery Report

Contents

Introduction

App Grid

App Details

Filtering by Date

More Information

FAQ

I have marked an App as "Not Approved", why is it not being blocked?

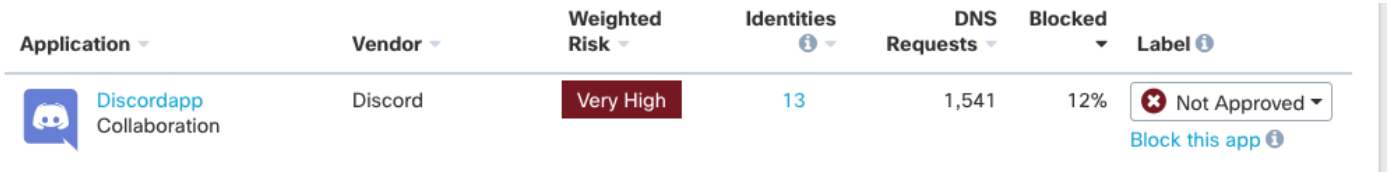
Is it possible to see a log of each individual blocked request?

Introduction

This document describes Blocked Requests in the App Discovery Report: App Grid (percentage of total) and App Details (count per identity).

App Grid

The Blocked % shows the percentage of DNS requests ***blocked for your Umbrella organization*** over the time period. The default time period is 90 days.



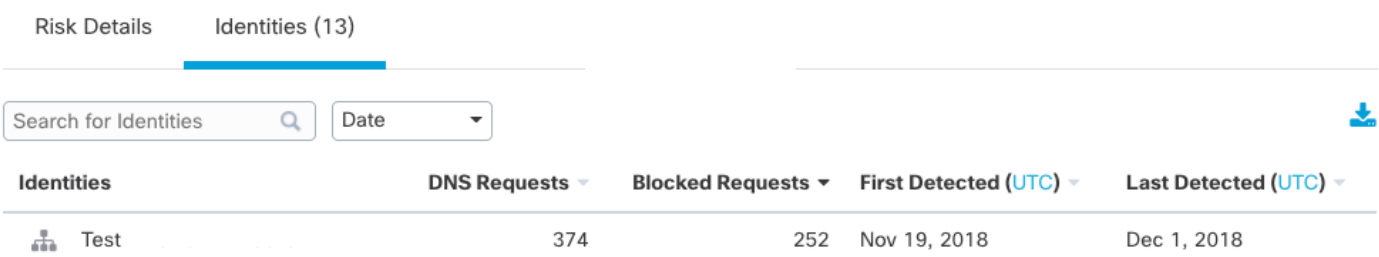
360015971991

App Details

The Blocked column shows a count of blocked DNS requests for each identity in your Umbrella organization (for this specific app). The default time period is 90 days.

This data can be accessed in two ways:

- Clicking on the count of Identities in the main App Grid report
- Clicking on an App name and then selecting the "Identities" tab

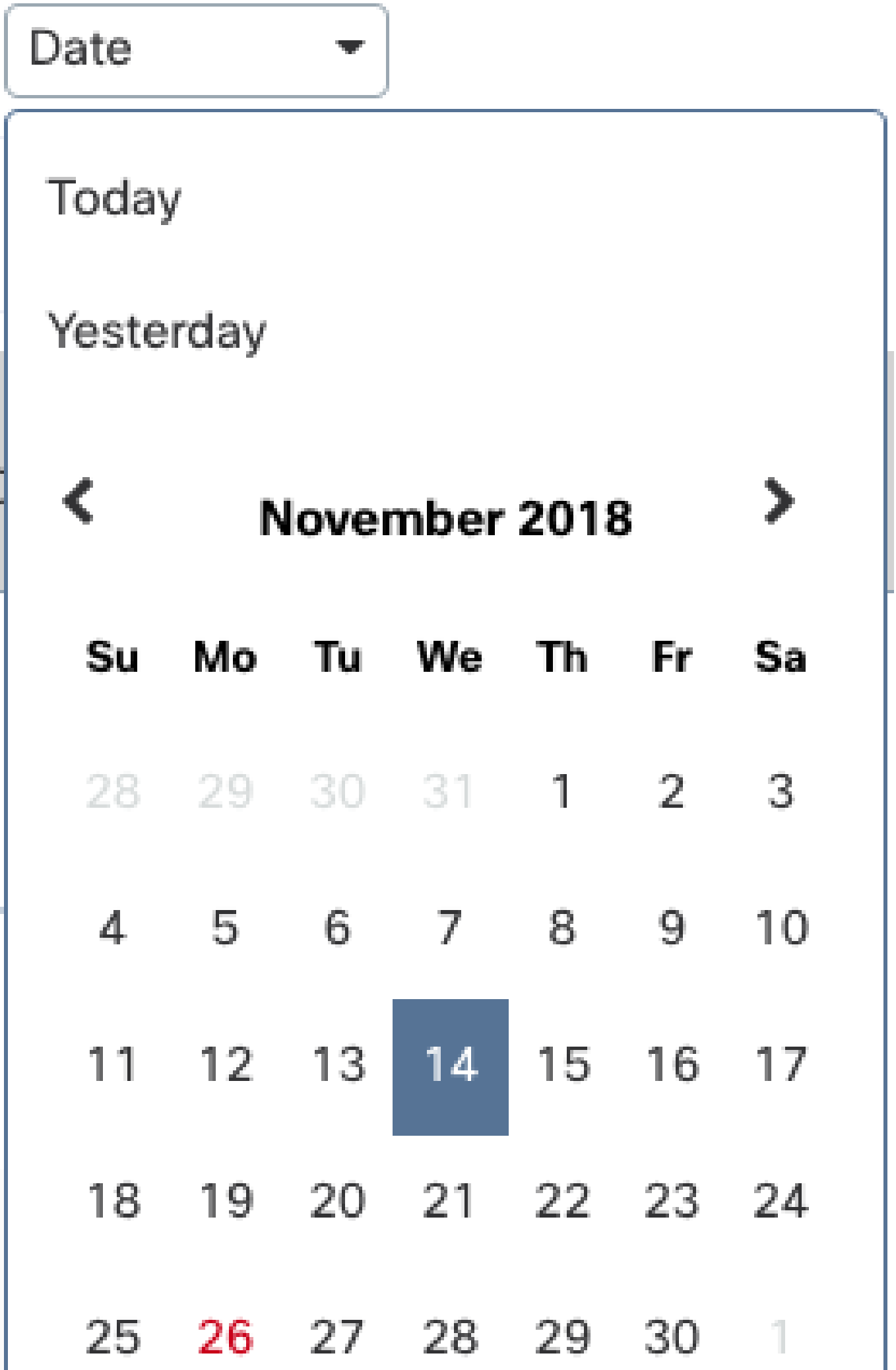


360018187812

Filtering by Date

To get more recent data on the % of blocked traffic, the report can be filtered by date. This gives a better insight as to the effect of recent policy changes. This filter is available in both the App Grid and App Details.

For example, the main Apps Grid can be filtered to show blocked requests from yesterday:


Date
Today
Yesterday
November 2018
Su Mo Tu We Th Fr Sa
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 1

: The default time period is 90 days but can be filtered to a single day. Other date ranges are not currently available but are on the product roadmap.

More Information

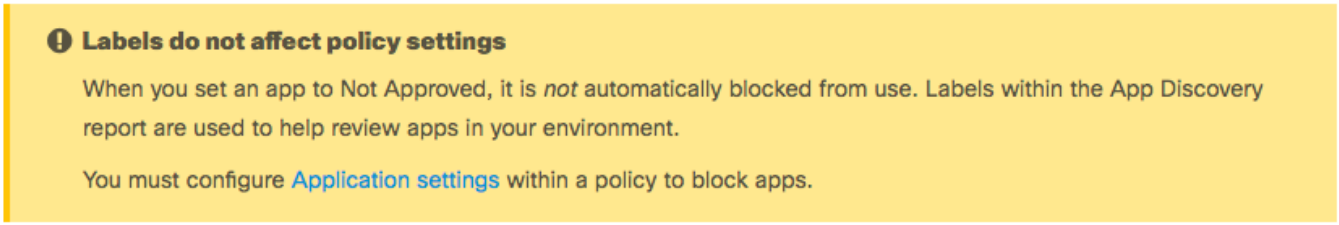
It is important to remember these:

- Each block represents an individual DNS request that was filtered by Umbrella.
- Some apps naturally generate more DNS requests than others. Some apps generate little DNS traffic even when in use, whereas others generate frequent requests even when idle. Umbrella counts the hits but is not aware of the intent of the user.
- All types of Umbrella DNS blocks are counted. This includes Security, Content, Destination List, Application and other blocks.
- Blocking an application is not expected to have any immediate impact on the App Discovery report...
  - App Discovery data is only aggregated once per day
  - The default view shows 90 days of data, so it can take some time to reflect 100% blocking.

FAQ

I have marked an App as "Not Approved", why is it not being blocked?

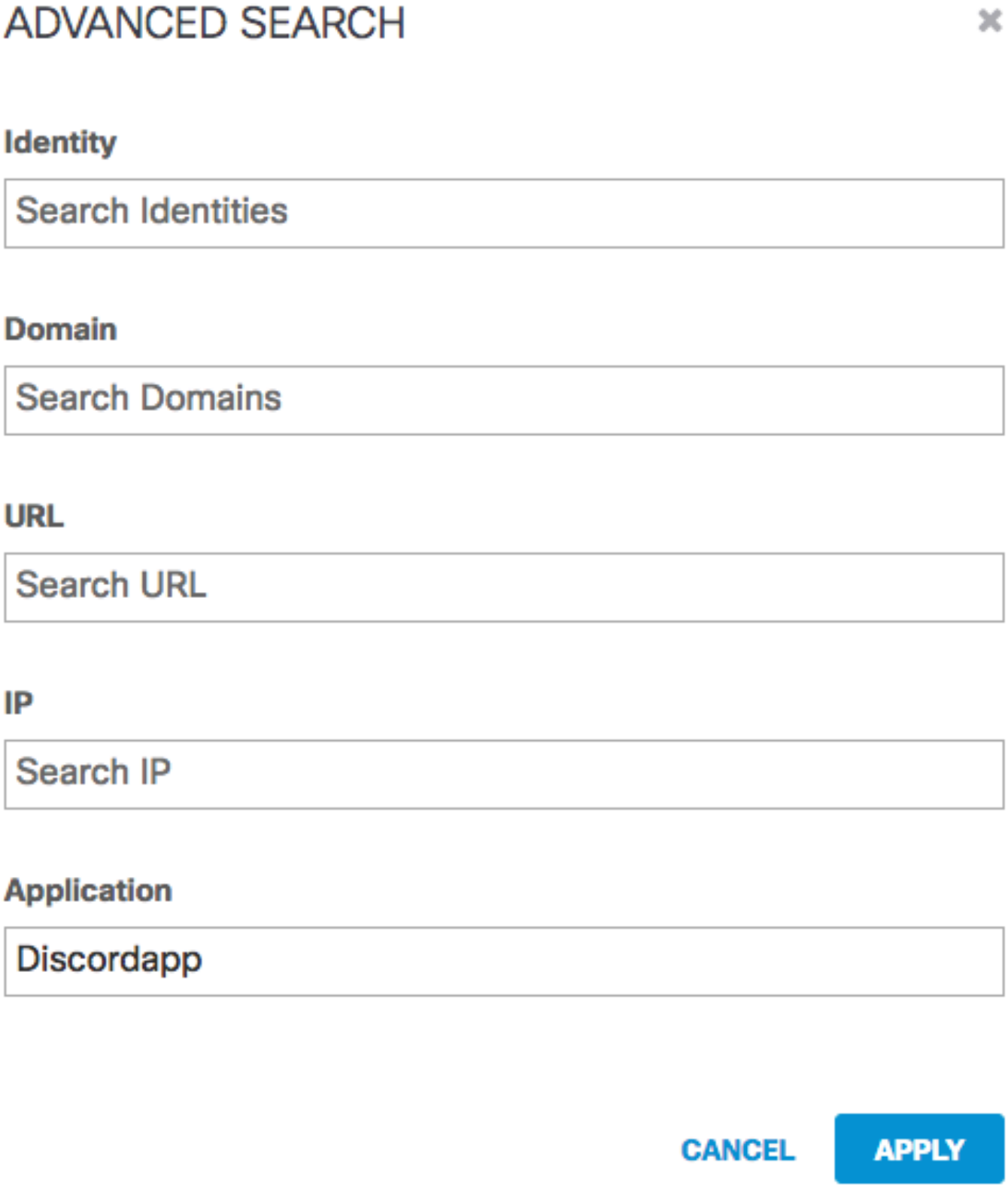
"Not Approved" is a label to help with your workflow but does not physically block the App. You must block the app via other means, such as the "Application Settings" page:



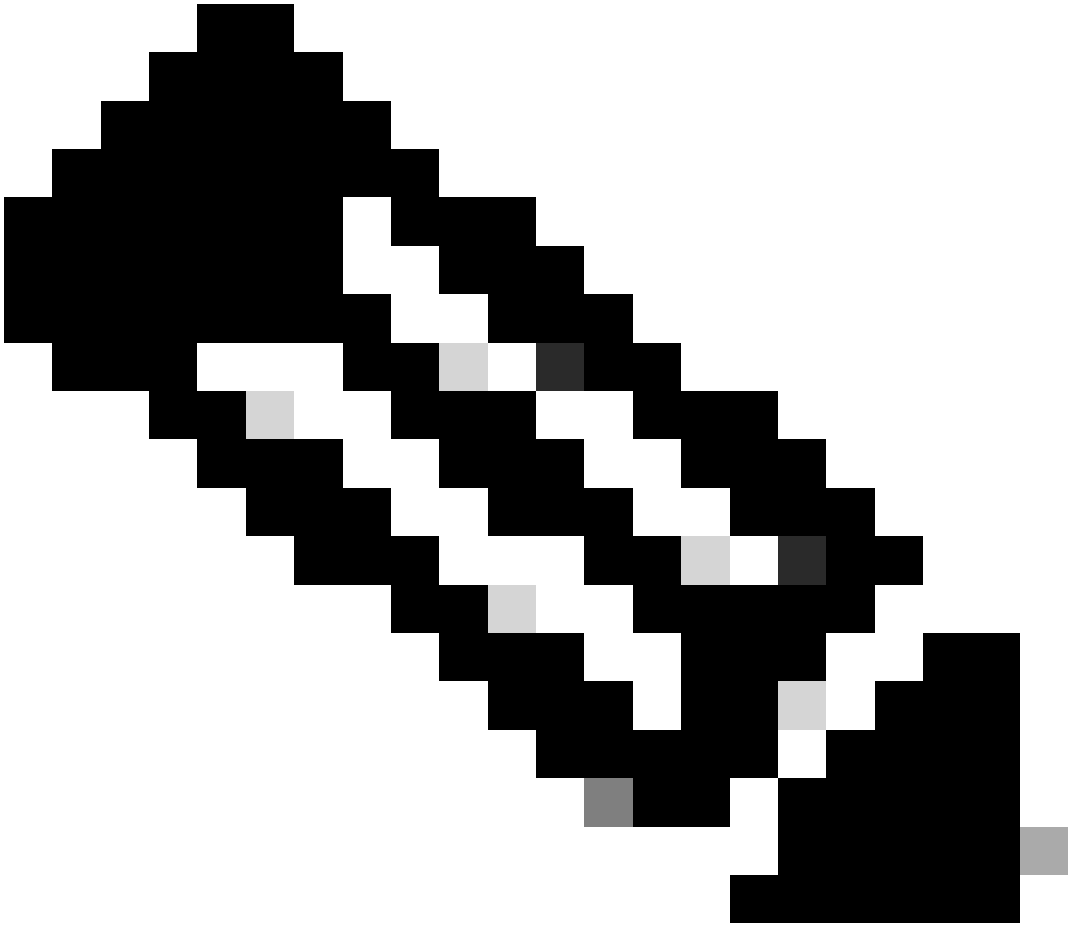
360022777211

Is it possible to see a log of each individual blocked request?

The App Discovery report is not able to perform this level of "forensic" investigation currently. However, you can search for blocked Applications using the Umbrella Activity Search. The Application filter is shown on the Advanced Search dialog.



360015931092



Note: Currently this functionality only works for Apps which are supported for blocking (those in Application Settings).