Threater Portal Release Notes

Build 158 - March 8, 2024

New Feature: Unexpected Blocks

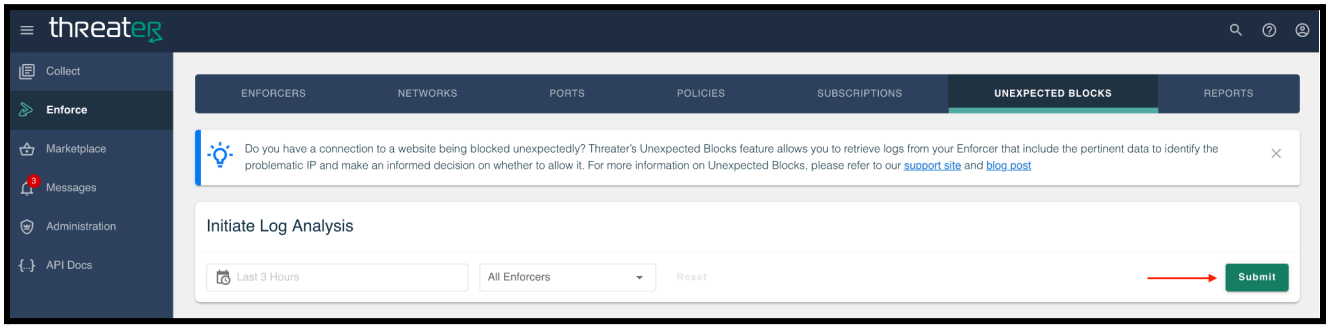
PREREQUISITE : Update all Enforcers to BUILD 240

After all of your Enforcers are successfully updated to the new build, we strongly recommend you log out and log back into the Threater portal.

Do you have a connection to a website being blocked unexpectedly? Threater's Unexpected Blocks feature allows you to retrieve outbound Port 80 and 443 traffic logs that your Enforcer(s) have blocked. These logs enable portal users to make an informed decision on whether to allow those IPs.

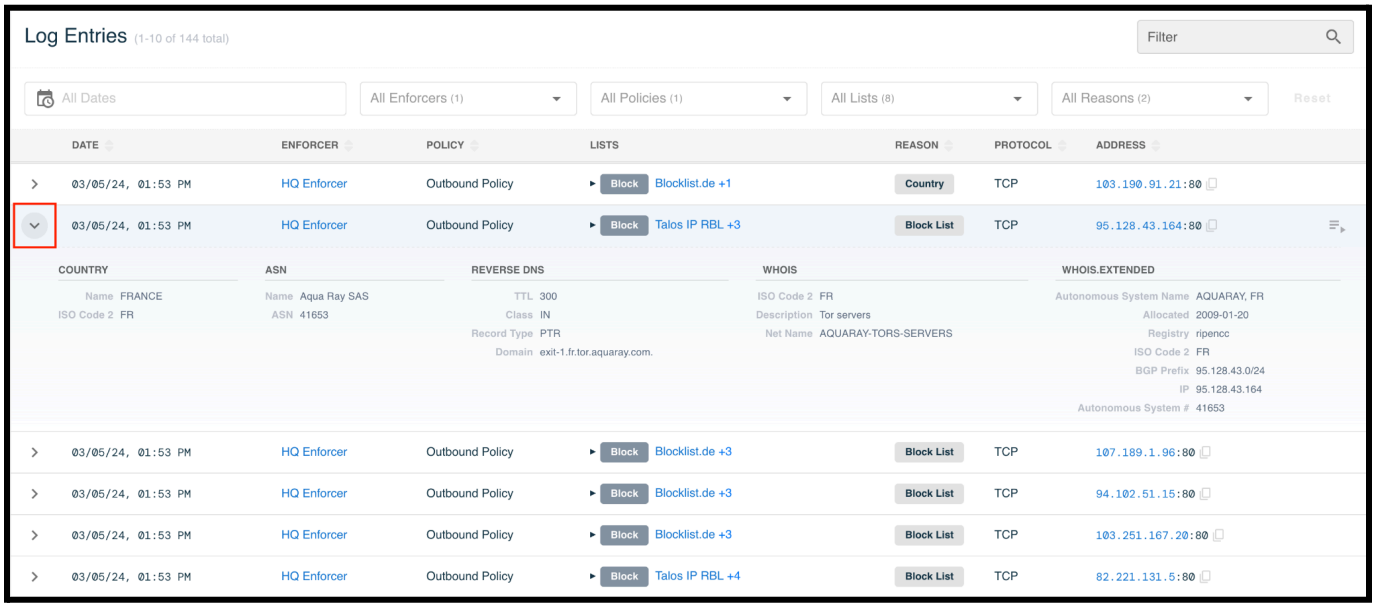
To perform an analysis:

1. Login to your Threater Portal account
2. Navigate to Enforce
3. Select the Unexpected Blocks tab
    - This tab will NOT appear until all Enforcers tied to your portal account have been updated to at least Build 240
4. Select a Date Range and the Enforcers you want to query logs on
    - Default selections are the last 3 hours and All Enforcers
5. Click Submit



Please note: The length of time associated with available results varies based on the parameters selected, your network activity/connection, and the resources (such as system RAM) of your Enforcers. The progress of your analysis is available on the Unexpected Blocks tab. You can navigate away and perform other functions within the application while your analysis is processing, but if you logout or close your browser your results will not complete.

Once your submitted query is complete, the log entries will display on the Unexpected Blocks tab. To view additional data in each entry, expand the row via the disclosure triangle in the far left column. The additional information can be very useful when determining whether or not an IP that is currently being blocked should be allowed.



Please note the following on the returned Log Entries:

- Reverse DNS and the basic WHOIS data may not be available for all entries
- It is common to find that some of the expanded data conflicts. For example, country and ASN information may differ across the various sources when expanded. These deltas can assist you when determining whether something is nefarious or not so that you can make a more informed decision about what you choose to allow.
- The “Existing Log Range”, available in the status card above the table, provides the date range of logs that were available for that individual Enforcer. This range can be within or outside the search

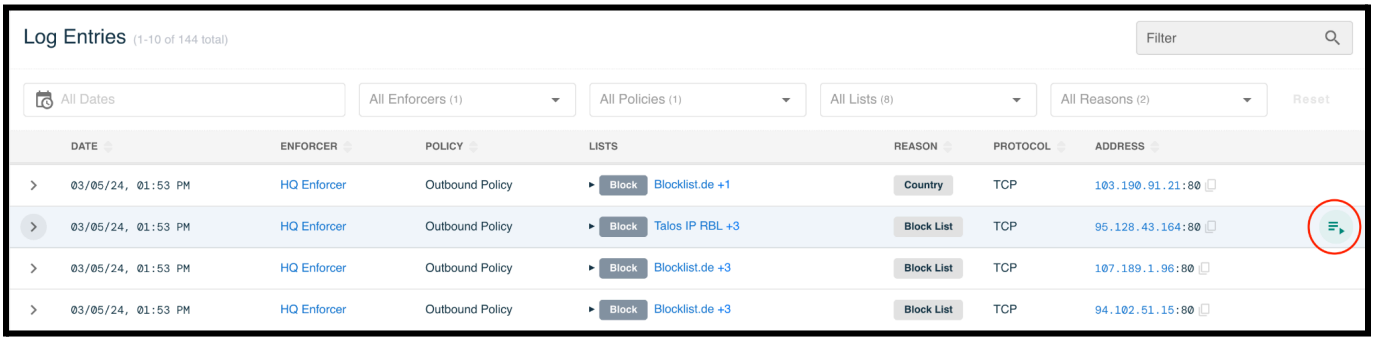
parameters. If the range available is outside the search parameters, the Log Entries table will still only display the results within the date range you originally searched for. You can use the "Existing Log Range" to determine if you may want to expand your search parameters.

  - Example: A log analysis is submitted for 03/07/24, 08:51 am to 03/07/24, 11:51 am. The "Existing Log Range" returned is 03/07/24, 03:00 am to 03/07/24, 11:51 am. The Log Entries table will only display Block IP entries on Ports 80 and 443 from 03/07/24, 08:51 am to 03/07/24, 11:51 am, if there are any that meet that criteria.

- A maximum of 1,000 entries per Enforcer will be returned.
- Threater Enforce software uses short-term RAM-based log storage to ensure the highest possible performance with no added latency to your network traffic while maintaining industry-leading security. Because of this and based on your network activity, your Enforce logs could wrap quickly and you may not be able to retrieve logs from within your specified time range.
  - For customers finding themselves constrained by these limitations, our strong recommendation is to leverage an external SIEM (such as Splunk, IBM Qradar, Gravwell, and others) to sink all logs using the Enforcer's built-in Syslog Export feature set, and then leverage the SIEM environment to perform unexpected blocks triage.

If an IP currently being blocked needs to be added to an Allow list:

1. Scroll over the row that contains the IP
2. Select the icon in the far-right column:



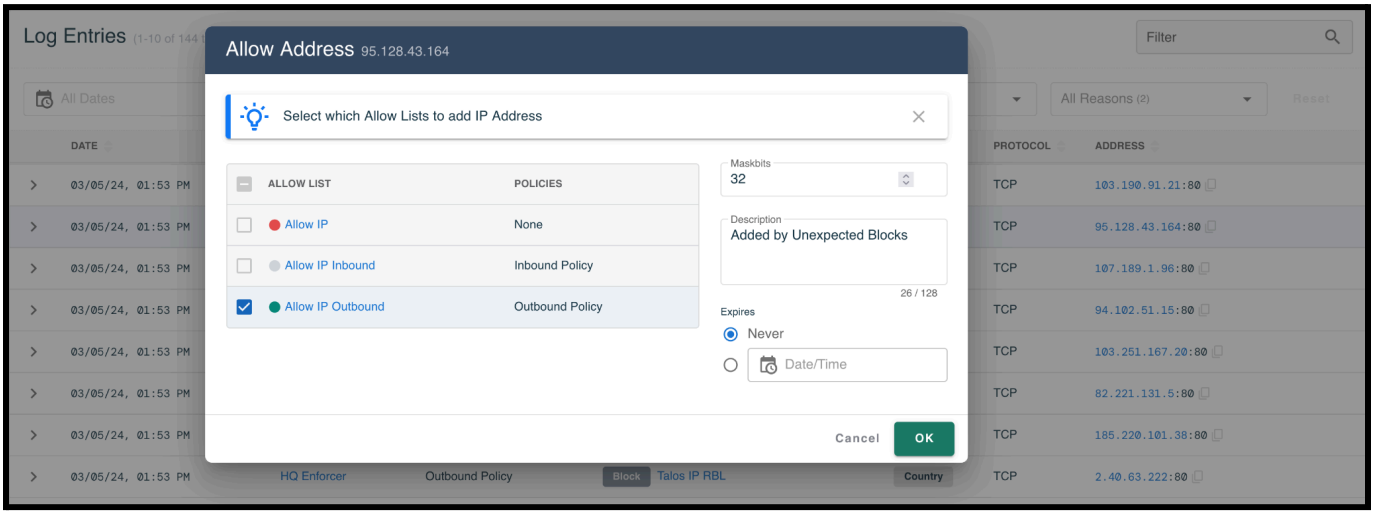
3. Select the Allow list(s) to add the IP to
   a. The colored pips next to the Allow list names indicate the following;

i. Green - The list is enforced by the policy that blocked the IP address. Adding the IP to this List will allow it through the Networks Enforced by this policy.

ii. Grey - The list is not Enforced by the policy that blocked the IP address. If the IP is added to this List, the IP will be allowed on the Networks Enforced by the Policy(s).

iii. Red - The list is not enforced by any of your policies. If the IP is added to this List, it will continue to be blocked until and unless the list is added to policies of interest.

4. Make any necessary edits to the IP entry:
   a. Maskbits - default is 32
   b. Description - default is "Added by Unexpected Blocks". We generally recommend that you update the description to be something meaningful such as tying it to a requesting end user, website, and/or discovery date.
   c. Expiration - default is "Never"; however, we generally recommend that you time-bound allowed-lists additions when feasible.
5. Click the "OK" Button



The IP is now added to the selected Allow list(s) and will be enforced by the policy(s) those lists are assigned to.