threatER Portal

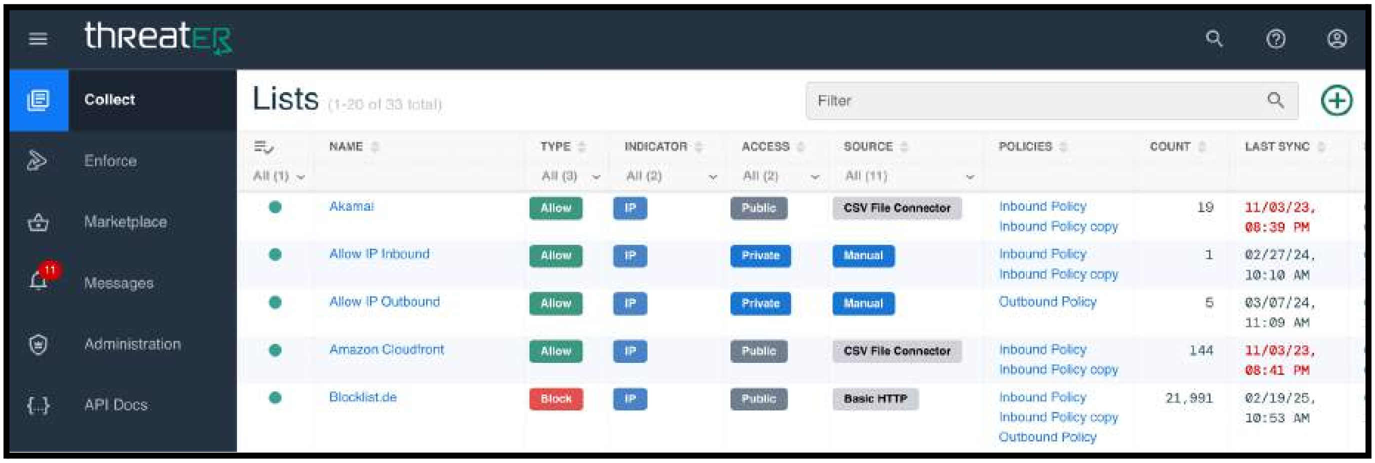
User Guide, April 2025

Collect

Collect is threatER's centralized SaaS solution to aggregate all of your threat intelligence. Collect provides customers access to best-in-class cyber intelligence feeds and threat lists, as well as the ability to create their own lists.

Lists

All List Types – Allow, Block, Threat – are consolidated into one table that is accessible by selecting Collect from the left-hand navigation.



Lists (1-20 of 33 total)

All (1)	NAME	TYPE All (3)	INDICATOR All (2)	ACCESS All (2)	SOURCE All (11)	POLICIES	COUNT	LAST SYNC
●	Akamai	Allow	IP	Public	CSV File Connector	Inbound Policy Inbound Policy copy	19	11/03/23, 08:39 PM
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM
●	Allow IP Outbound	Allow	IP	Private	Manual	Outbound Policy	5	03/07/24, 11:09 AM
●	Amazon Cloudfront	Allow	IP	Public	CSV File Connector	Inbound Policy Inbound Policy copy	144	11/03/23, 08:41 PM
●	Blocklist.de	Block	IP	Public	Basic HTTP	Inbound Policy Inbound Policy copy Outbound Policy	21,991	02/19/25, 10:53 AM

The table contains the following details on each List Type:

- List Name
- Type – Allow, Block, or Threat
- Health State (color of pip to the left of the List Name)
    - Green – the list is considered "healthy". It is actively syncing and pulling indicators
    - Red – the list "Needs Attention". When a list is in this state, the configuration of the list should be checked to ensure all settings are correct
    - Yellow – the list is syncing to the 3rd party platform it is meant to retrieve indicators from, but the list currently has 0 entries
- Indicator – will display the Indicators contained in the list (IP or Domain)
- Access –
    - Private – indicates the List was created by the end user. Private lists are editable and can be deleted by the end user

    - Public - indicates the List is not owned or managed by the end user and cannot be edited or deleted by the end user
- Source -
    - Manual will display for all Manual Lists that were created
    - For any plugin or integration, the Source Name or Type will display (ex. Basic HTTP, CSV File Connector, etc.)
- Policies - displays the names of the policies the list is enabled on
- Count - Indicates the number of entries (IPs or Domains) in the List
- Last Sync - This is the last time threatER connected to the 3rd party system to check for updates to the list. For Manual Lists, this will display the date the list was last edited
    - If a list has not synced for more than 48 hours, the timestamp will display in red
- Last Update - This is the last time the content of the list was modified

Users can filter down the results in the Lists table by utilizing the filter drop-downs and text filter above the table.

List Types

Allow Lists

Allow Lists can be used to ensure that trusted IPs and Domains are always allowed by Enforce, even in the case where your policies would otherwise block the connection due to country, ASN, threat list, or block list.

As Enforce can handle up to 150 million unique threat indicators with 10-30 million indicators provided out of the box, it is possible that users will run into outbound or inbound connections being blocked unexpectedly. Users can manage these blocked connections by configuring Allow Lists either utilizing manual lists or plugins. Unlike many other security controls on the market, there are no limits to the amount of entries you can include in your lists.

PLEASE NOTE: Both Allow IP and Domain lists are enabled on a **per-policy** basis.

Block Lists

Block Lists can be used to ensure that known-malicious IPs and Domains are blocked by Enforce.

PLEASE NOTE: Both Block IP and Domain lists are enabled on a **per-policy** basis.

Out-of-the-box partner block lists provided by threatER are refreshed at regular intervals. Depending on the rules enforced by the partner feed, the update interval can be anywhere from immediate, to every few minutes, to once per hour, and so on.

Threat Lists

Threat Lists are provided by our partners Webroot (included with your Enforce subscription) and Proofpoint (available in our Marketplace). These lists are composed of 3 pieces of information:

- IP Address - where an identified threat originates from
- Category - what type of threat has been identified
- Score - a confidence score ranging from 1 to 100 where 1 is least likely to be a threat, and 100 is most likely to be a threat

Threat Lists are used in Policy Risk Thresholds.

PLEASE NOTE: Threat lists are enabled on a **per-policy** basis.

Out-of-the-box Threat Lists are refreshed per terms of the partner feed, which is generally every few minutes.

List Creation

Creating IP Threat Lists

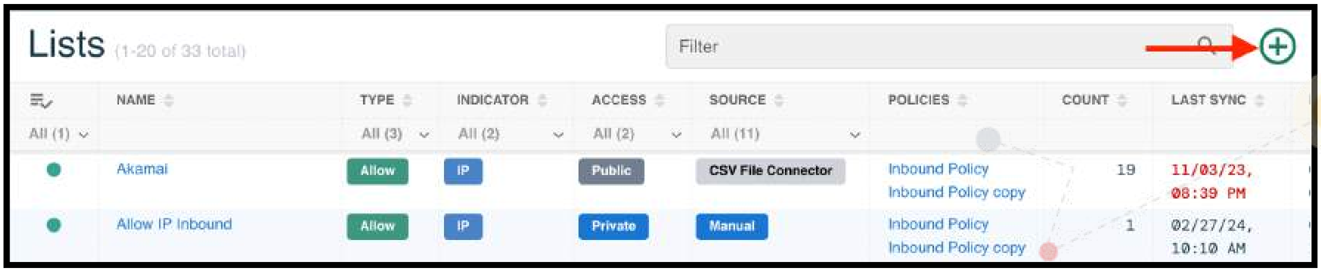
Currently, threatER does not support Manual Threat Lists, or Threat Domain lists. The application does support the following Threat IP Plugins:

- Threat IP CSV File Connector
- Anomali

Creating Manual IP Allow & Block Lists

To create a manual IP list:

- Navigate to Collect in the left-hand navigation menu
- Click on the "+" button in the top-right corner



Lists (1-20 of 33 total)

Filter

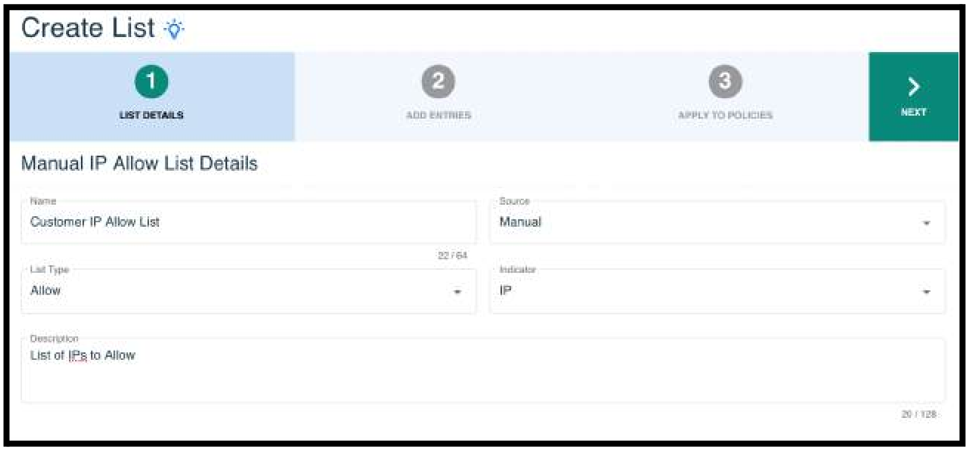
	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC
All (1)		All (3)	All (2)	All (2)	All (11)			
●	Akamai	Allow	IP	Public	CSV File Connector	Inbound Policy Inbound Policy copy	19	11/03/23, 08:39 PM
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM

List Details

Provide the following (* indicates required field):

- *Name (unique name required)
- *Source
  - Select Manual from the drop-down
- *List Type
  - Select Allow or Block from the drop-down
  - Note: Manual Threat Lists (IP & Domain) are not supported at this time
- *Indicator
  - Select IP from the drop-down
- Description

Once all required fields are complete, click the Next button to proceed to the Add Entries step.



Manual IP Allow List Details

Name: Customer IP Allow List (22 / 64)

Source: Manual

List Type: Allow

Indicator: IP

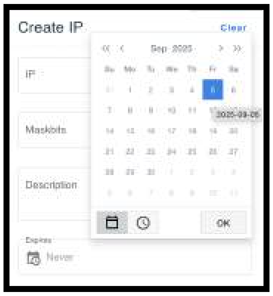
Description: List of IPs to Allow (20 / 128)

Add Entries

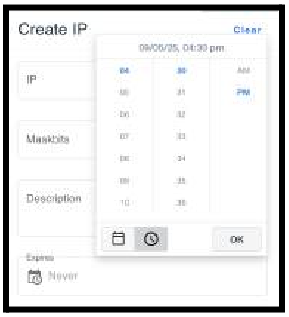
To add entries to the list, enter the following (* indicates required field):

- *IP address
- *Maskbits

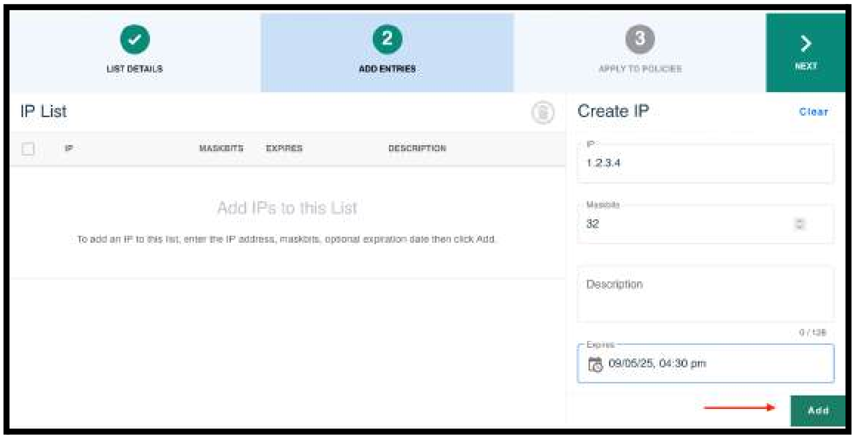
- Description (optional)
- Expiration
    - Default expiration is set to “Never”
    - To provide an expiration date and time:
        - Click within the Expires field
        - Select a date from the calendar



        - Click on the clock tab and choose the desired hour and minutes
        - Click OK



- Click the Add button to add the IP to the list



Add IPs to this List

To add an IP to this list, enter the IP address, maskbits, optional expiration date then click Add.

IP: 1.2.3.4

Maskbits: 32

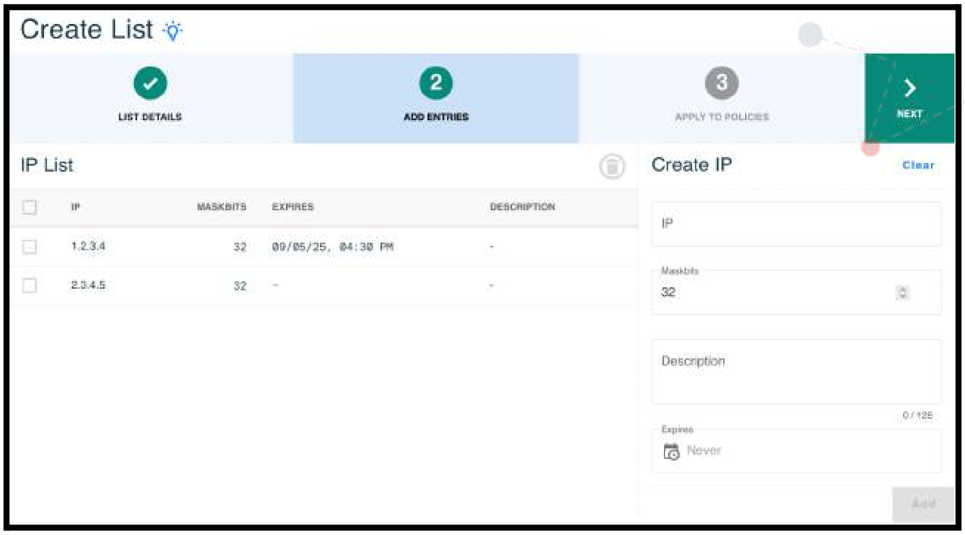
Description

0 / 128

Expires: 09/05/25, 04:30 pm

- Follow the steps above to add additional IPs to the list

Once all IPs are added, click the Next button to proceed to the Apply to Policies step.



□	IP	MASKBITS	EXPIRES	DESCRIPTION
□	1.2.3.4	32	09/05/25, 04:30 PM	-
□	2.3.4.5	32	-	-

IP

Maskbits: 32

Description

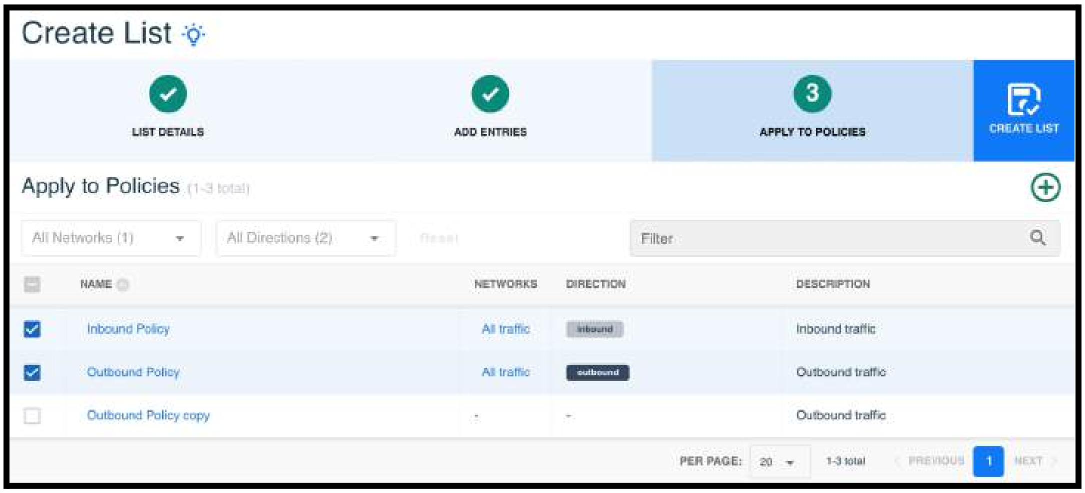
0 / 128

Expires: Never

NOTE: To remove an entry before moving to the next step, click the checkbox next to the entry and click the Remove button.

Apply to Policies

Entries within an IP list are not allowed or blocked until the List is applied to a Policy. To apply this new list to a policy, click the checkbox next to the applicable policies. Once all desired selections are made, click the Create List button to create the List.

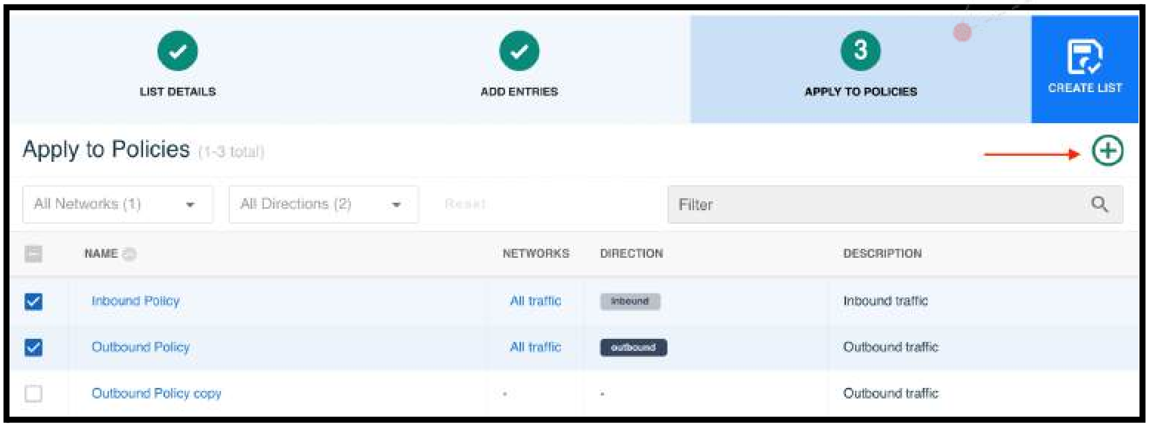


□	NAME	NETWORKS	DIRECTION	DESCRIPTION
☑	Inbound Policy	All traffic	inbound	Inbound traffic
☑	Outbound Policy	All traffic	outbound	Outbound traffic
□	Outbound Policy copy	-	-	Outbound traffic

PER PAGE: 20 1-3 total PREVIOUS 1 NEXT

Create New Policy During List Creation

If a policy does not exist that you want to apply your list to, you have the option to create a new policy within the Create List wizard. To do so, click the "+" button on the Apply to Policies step and then follow the steps to create a policy, outlined in the Policies section of this document.

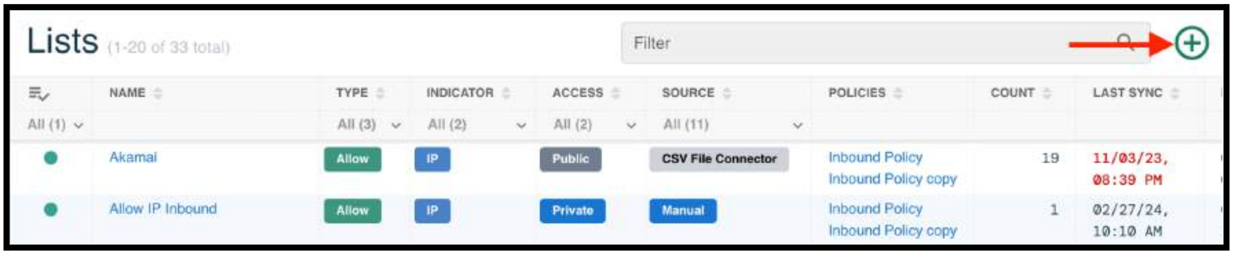


	NAME	NETWORKS	DIRECTION	DESCRIPTION
☑	Inbound Policy	All traffic	inbound	Inbound traffic
☑	Outbound Policy	All traffic	outbound	Outbound traffic
□	Outbound Policy copy	-	-	Outbound traffic

Creating Manual Domain Lists

To create a manual Domain list:

- Navigate to Collect in the left-hand navigation menu
- Click on the "+" button in the top-right corner



	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC
All (1)		All (3)	All (2)	All (2)	All (11)			
●	Akamai	Allow	IP	Public	CSV File Connector	Inbound Policy Inbound Policy copy	19	11/03/23, 08:39 PM
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM

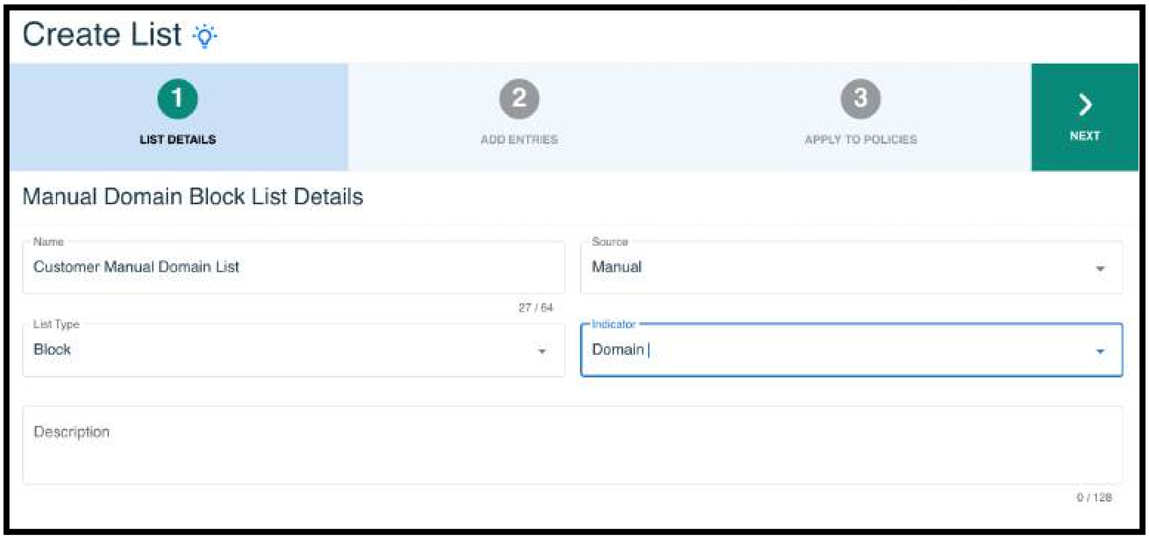
List Details

Provide the following (* indicates required field):

- *Name (unique name required)
- *Source
  - Select Manual from the drop-down
- *List Type
  - Select Allow or Block from the drop-down
  - Note: Manual Threat Lists (IP & Domain) are not supported at this time

- *Indicator
    - Select Domain from the drop-down
- Description

Once all required fields are complete, click the Next button to proceed to the Add Entries step.



Create List

Manual Domain Block List Details

Name: Customer Manual Domain List (27 / 64)

Source: Manual

List Type: Block

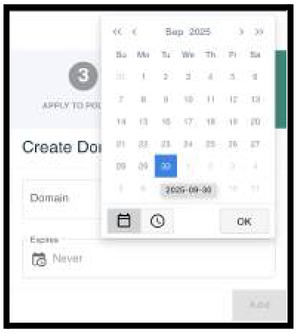
Indicator: Domain

Description (0 / 128)

Add Entries

To add entries to the list, enter the following:

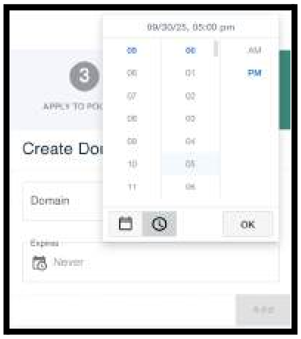
- Domain (required)
- Description
- Expiration
    - Default expiration is set to “Never”
    - To provide an expiration date and time:
        - Click within the Expires field
        - Select a date from the calendar



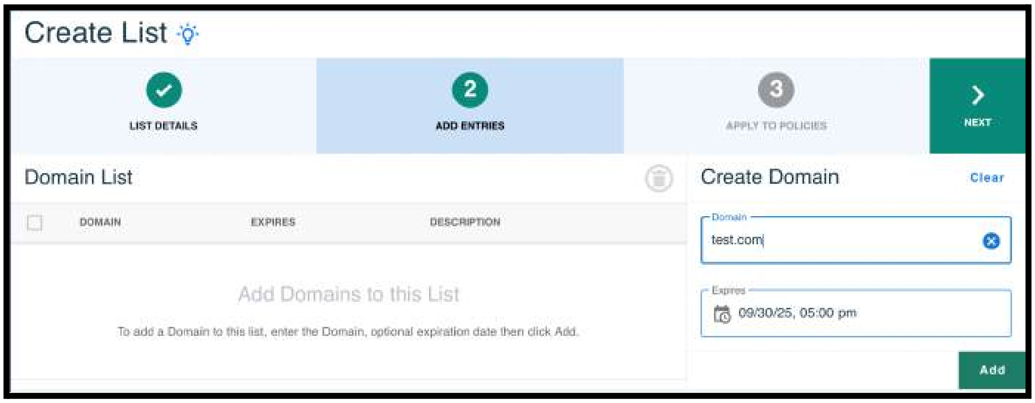
Domain

Expires: Never

  - Click on the clock tab and choose the desired hour and minutes
  - Click OK



- Click the Add button to add the Domain to the list



Create List

✓ LIST DETAILS | 2 ADD ENTRIES | 3 APPLY TO POLICIES | NEXT

Domain List

☐	DOMAIN	EXPIRES	DESCRIPTION

Add Domains to this List

To add a Domain to this list, enter the Domain, optional expiration date then click Add.

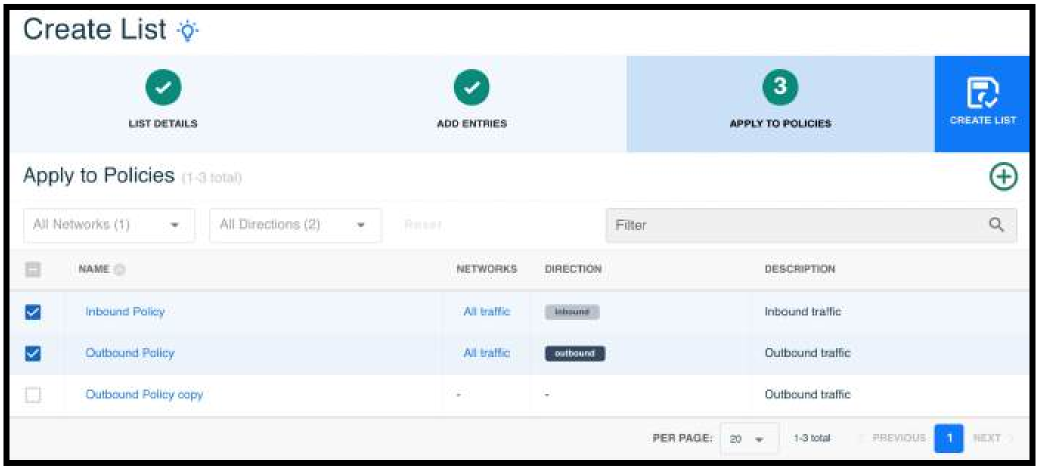
Create Domain — Clear

Domain: test.com

Expires: 09/30/25, 05:00 pm

Add

- Follow the steps above to add additional Domains to the list
- Once all domains are added, click the Next button
- Select the checkbox next to the policies you would like the list enabled on
- Click the Create List button to create the List



Create List

✓ LIST DETAILS | ✓ ADD ENTRIES | 3 APPLY TO POLICIES | CREATE LIST

Apply to Policies (1-3 total)

All Networks (1) | All Directions (2) | Reset | Filter

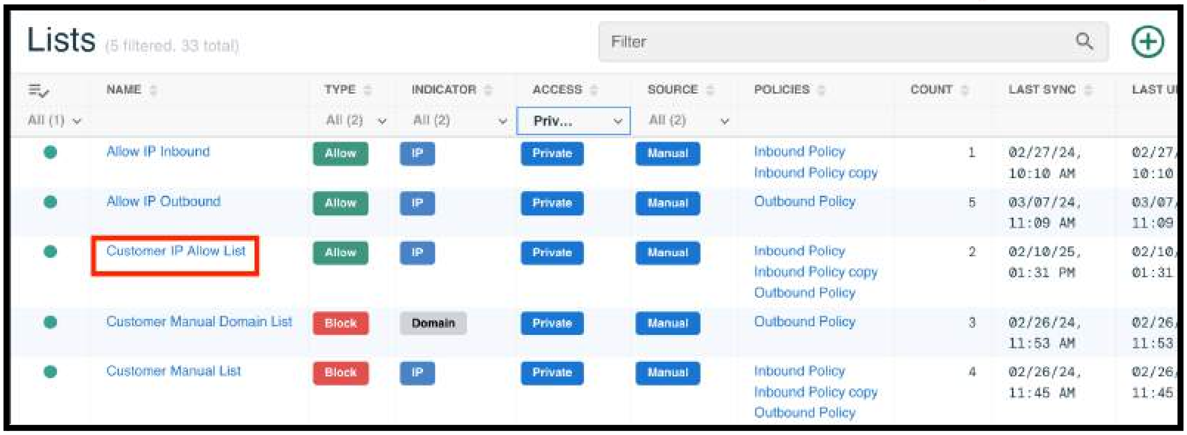
☐	NAME	NETWORKS	DIRECTION	DESCRIPTION
☑	Inbound Policy	All traffic	inbound	Inbound traffic
☑	Outbound Policy	All traffic	outbound	Outbound traffic
☐	Outbound Policy copy	-	-	Outbound traffic

PER PAGE: 20 | 1-3 total | PREVIOUS | 1 | NEXT

Adding & Removing Manual List Entries

To add entries to a Manual List:

- Find the list in the table (use the filter at the top of the table to narrow down the results) and click on the list name

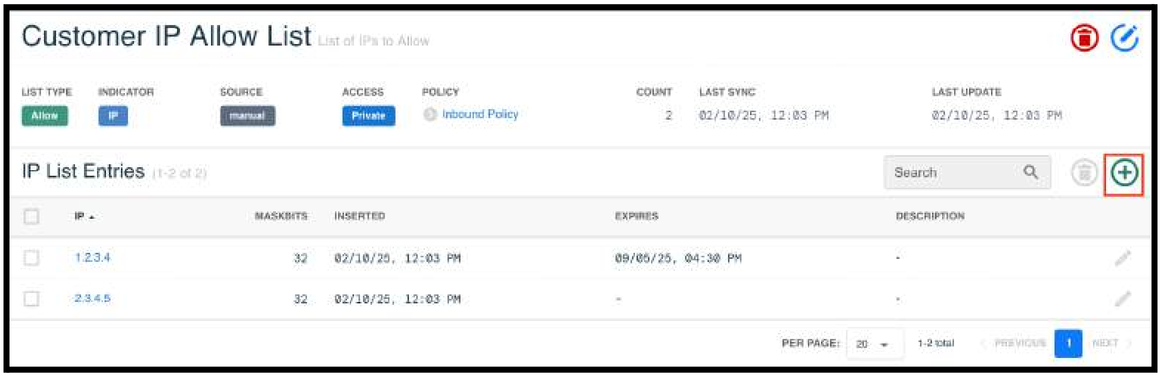


Lists (5 filtered, 33 total)

Filter

	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC	LAST U
All (1)		All (2)	All (2)	Priv...	All (2)				
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM	02/27 10:10
●	Allow IP Outbound	Allow	IP	Private	Manual	Outbound Policy	5	03/07/24, 11:09 AM	03/07 11:09
●	Customer IP Allow List	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy Outbound Policy	2	02/10/25, 01:31 PM	02/10 01:31
●	Customer Manual Domain List	Block	Domain	Private	Manual	Outbound Policy	3	02/26/24, 11:53 AM	02/26 11:53
●	Customer Manual List	Block	IP	Private	Manual	Inbound Policy Inbound Policy copy Outbound Policy	4	02/26/24, 11:45 AM	02/26 11:45

- Click on the "+" sign in the right hand corner



Customer IP Allow List List of IPs to Allow

LIST TYPE	INDICATOR	SOURCE	ACCESS	POLICY	COUNT	LAST SYNC	LAST UPDATE
Allow	IP	manual	Private	Inbound Policy	2	02/10/25, 12:03 PM	02/10/25, 12:03 PM

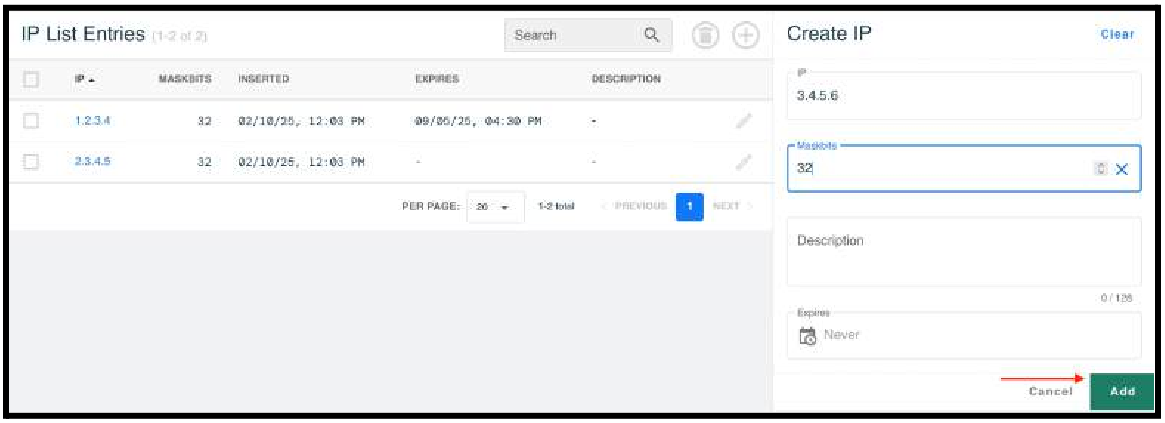
IP List Entries (1-2 of 2)

Search

☐	IP ▴	MASKBITS	INSERTED	EXPIRES	DESCRIPTION
☐	1.2.3.4	32	02/10/25, 12:03 PM	09/05/25, 04:30 PM	-
☐	2.3.4.5	32	02/10/25, 12:03 PM	-	-

PER PAGE: 20 1-2 total PREVIOUS 1 NEXT

- In the right-hand panel, enter the applicable data and click the "Add' button"



IP List Entries (1-2 of 2)

Search

☐	IP ▴	MASKBITS	INSERTED	EXPIRES	DESCRIPTION
☐	1.2.3.4	32	02/10/25, 12:03 PM	09/05/25, 04:30 PM	-
☐	2.3.4.5	32	02/10/25, 12:03 PM	-	-

PER PAGE: 20 1-2 total PREVIOUS 1 NEXT

Create IP Clear

IP: 3.4.5.6

Maskbits: 32

Description

0 / 128

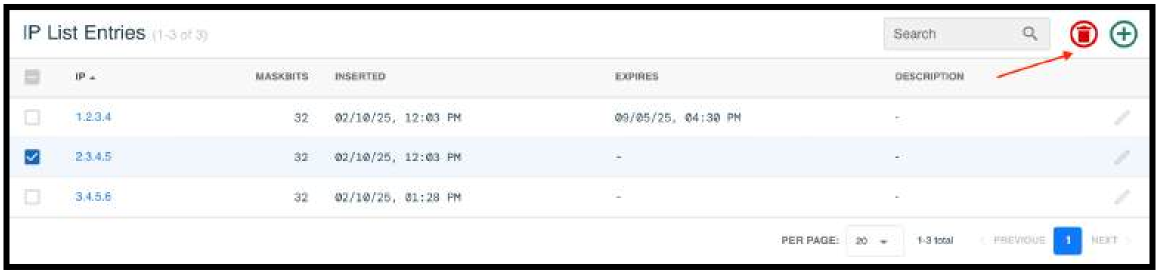
Expires: Never

Cancel Add

Follow the steps above to add additional entries to the list.

To remove entries from a Manual List:

- Find the list in the table and click on the list name
- Select the checkbox next to the entries to remove
- Click the Trash icon

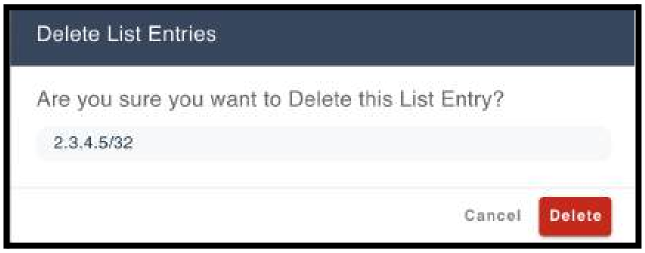


IP List Entries (1-3 of 3)

□	IP ▴	MASKBITS	INSERTED	EXPIRES	DESCRIPTION
□	1.2.3.4	32	02/10/25, 12:03 PM	09/05/25, 04:30 PM	-
☑	2.3.4.5	32	02/10/25, 12:03 PM	-	-
□	3.4.5.6	32	02/10/25, 01:28 PM	-	-

PER PAGE: 20 1-3 total

- On the confirmation modal, click the Delete button



Delete List Entries

Are you sure you want to Delete this List Entry?

2.3.4.5/32

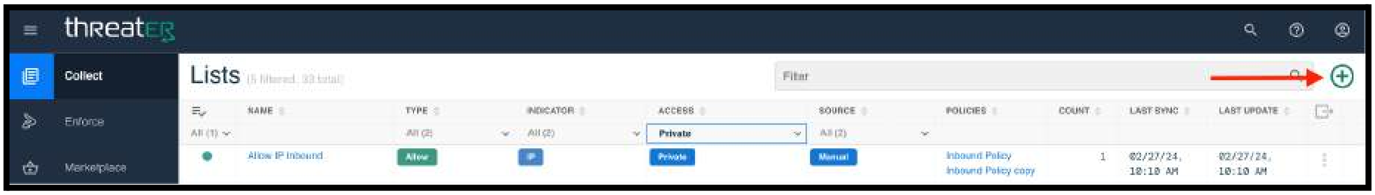
The entries are now deleted from the list.

Plugins

The threatER Portal has built-in data connectors, as well as integrations with 3rd party providers. Utilizing our plugin architecture and your membership credentials with these vendors, you can easily sync to external data sources or systems to retrieve threat intelligence to block or allow traffic.

To create a plugin:

- Navigate to Collect in the left-hand navigation menu
- Click on the “+” button in the top-right corner



Lists (5 filtered, 33 total)

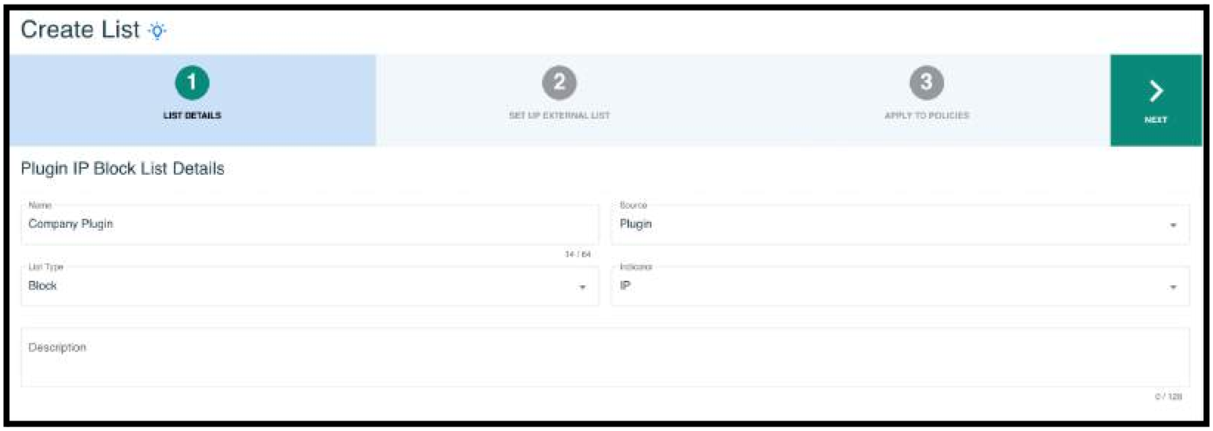
	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC	LAST UPDATE
All (1)		All (2)	All (2)	Private	All (2)				
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM	02/27/24, 10:10 AM

List Details

Provide the following (* indicates required field):

- *Name (unique name required)
- *Source
    - Select Plugin from the drop-down
- *List Type
    - Make a selection from the drop-down
- *Indicator
    - Make a selection from the drop-down
- Description

Once all required fields are complete, click the Next button to proceed to the Set Up External List step.



Create List

Plugin IP Block List Details

Name: Company Plugin (14 / 64)

Source: Plugin

List Type: Block

Indicator: IP

Description (0 / 128)

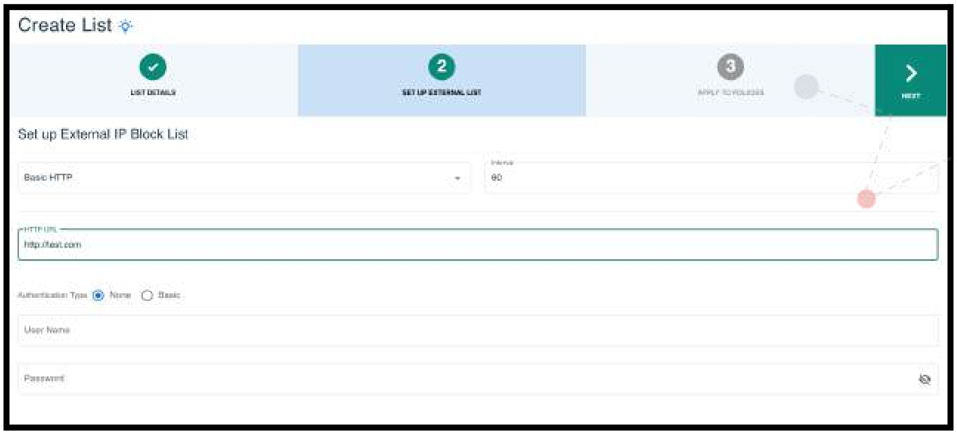
Set Up External List

- Select the plugin type from the drop-down
- Set the Interval
    - This is the time between each pull of data from the threatER platform to the 3rd party system
    - We generally recommend a value of 60
- Based on the plugin selected, you will need to enter additional fields

Please reference the following articles for details on each of our plugins:

- Available Data Integrations
- Available Data Connectors

Once all fields are provided, click the Next button to proceed to the Apply to Polices step.



Set up External IP Block List

Basic HTTP

Interval: 60

HTTP URL: http://test.com

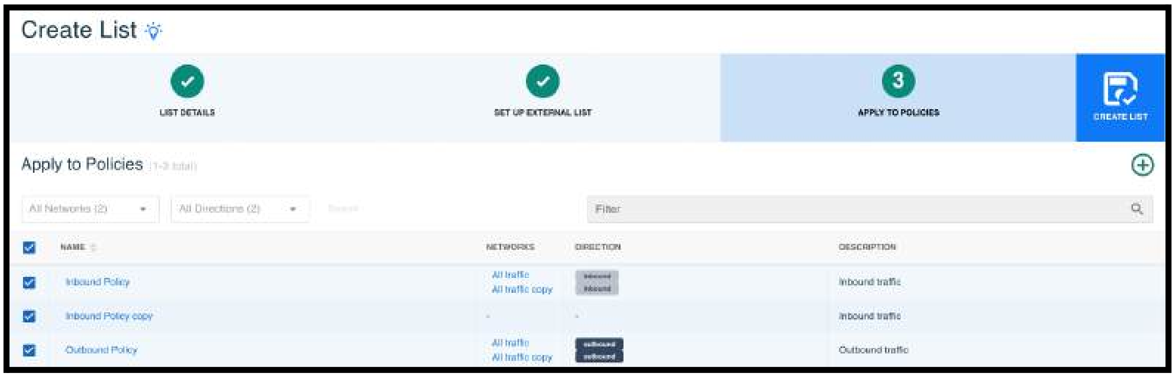
Authentication Type ● None ○ Basic

User Name

Password

Apply to Policies

Entries within a list are not allowed or blocked until the List is applied to a Policy. To apply this new list to a policy, click the checkbox next to the applicable policies. Once all desired selections are made, click the Create List button to create the List.



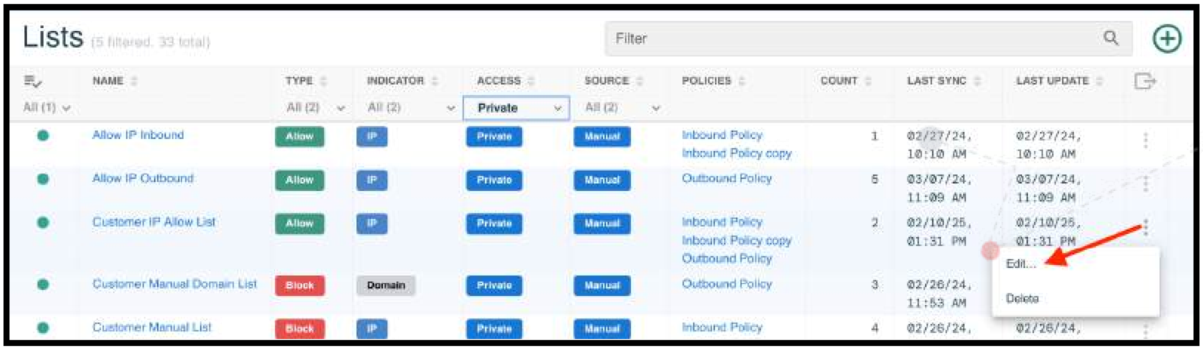
Apply to Policies (1-3 total)

☑	NAME	NETWORKS	DIRECTION	DESCRIPTION
☑	Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
☑	Inbound Policy copy	-	-	Inbound traffic
☑	Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

Editing all List Components

To edit all components (details, entries, policies) of a Manual list :

- Find the List in the table and select Edit from the the ellipsis menu



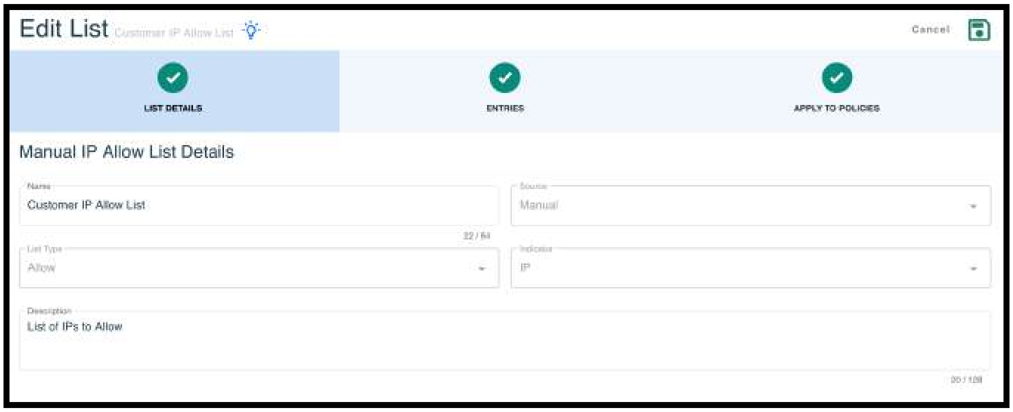
Lists (5 filtered, 33 total)

Filter

	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC	LAST UPDATE
All (1)		All (2)	All (2)	Private	All (2)				
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM	02/27/24, 10:10 AM
●	Allow IP Outbound	Allow	IP	Private	Manual	Outbound Policy	5	03/07/24, 11:09 AM	03/07/24, 11:09 AM
●	Customer IP Allow List	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy Outbound Policy	2	02/10/25, 01:31 PM	02/10/25, 01:31 PM
●	Customer Manual Domain List	Block	Domain	Private	Manual	Outbound Policy	3	02/26/24, 11:53 AM	
●	Customer Manual List	Block	IP	Private	Manual	Inbound Policy	4	02/26/24,	02/26/24,

NOTE: Lists that are tagged as "Public" Access cannot be edited by end users.

- ○ Edit List Details –
  - ■ This is the default view when editing a list. Make any necessary edits and then select another step that requires updates. If edits are only needed on this step, click the Save button in the top right corner



Edit List Customer IP Allow List

Manual IP Allow List Details

Name: Customer IP Allow List (22 / 64)

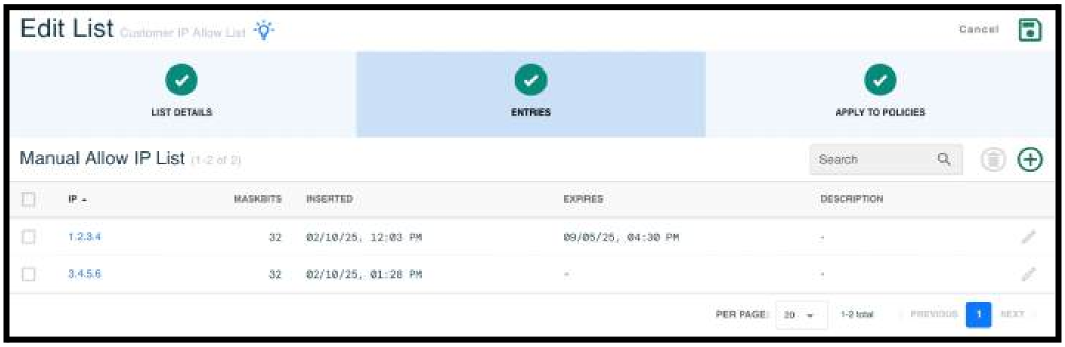
Source: Manual

List Type: Allow

Indicator: IP

Description: List of IPs to Allow (20 / 128)

- ○ Edit Entries (Manual Lists)–
  - ■ Select this step to add or remove entries
  - ■ Refer to the Adding & Removing Manual List Entries section for guidance on how to amend existing list entries
  - ■ If no other List edits are desired, click the Save button in the top right corner
  - ■ If additional List edits are needed, select the applicable step



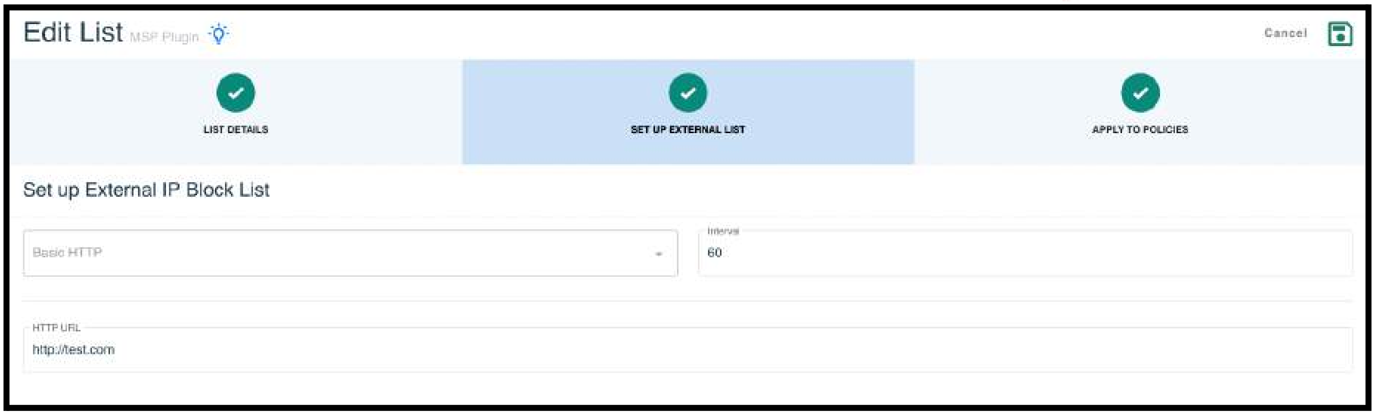
Edit List Customer IP Allow List

Manual Allow IP List (1-2 of 2)

☐	IP	MASKBITS	INSERTED	EXPIRES	DESCRIPTION
☐	1.2.3.4	32	02/10/25, 12:03 PM	09/05/25, 04:30 PM	-
☐	3.4.5.6	32	02/10/25, 01:28 PM	-	-

PER PAGE: 20 1-2 total PREVIOUS 1 NEXT

- Set Up External List (Plugins) –
  - Select this step update the configuration of a plugin
  - If no other List edits are desired, click the Save button in the top right corner
  - If additional List edits are needed, select the applicable step



Edit List MSP Plugin

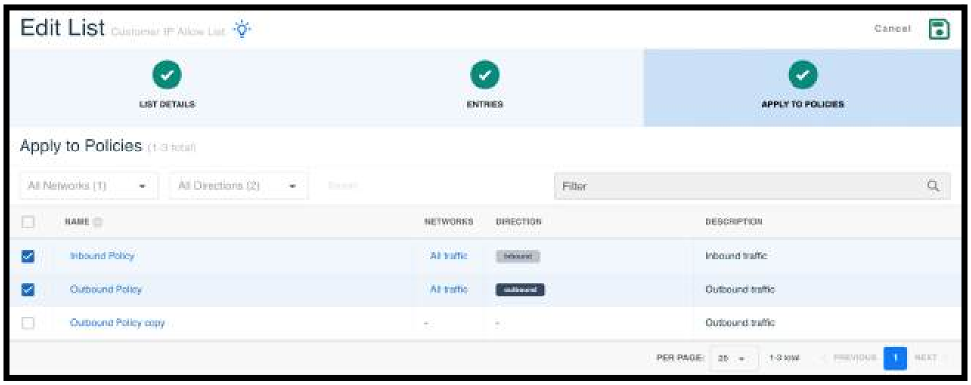
Set up External IP Block List

Basic HTTP

Interval: 60

HTTP URL: http://test.com

- Apply to Policies
  - Select this step to adjust the Policies the List should be enabled on
  - Refer to the Apply to Policies section above for guidance
  - If no other List edits are desired, click the Save button in the top right corner



Edit List Customer IP Allow List

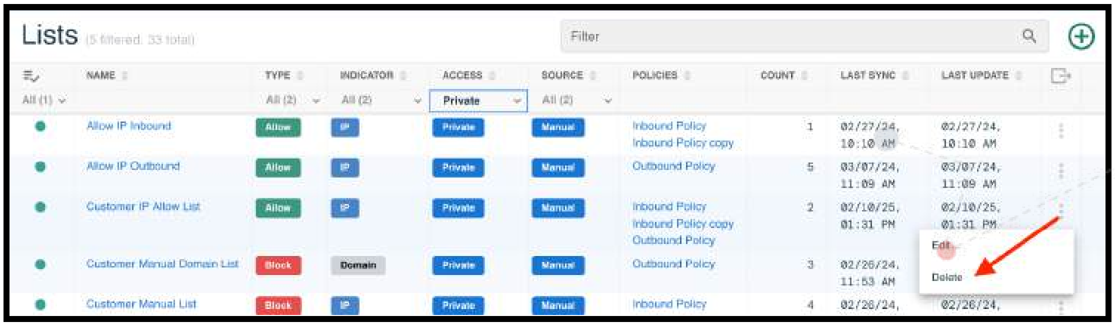
Apply to Policies (1-3 total)

☐	NAME	NETWORKS	DIRECTION	DESCRIPTION
☑	Inbound Policy	All traffic	inbound	Inbound traffic
☑	Outbound Policy	All traffic	outbound	Outbound traffic
☐	Outbound Policy copy	-	-	Outbound traffic

Deleting a List

To delete a List:

- Find the List in the table and from the the ellipsis menu, click Delete



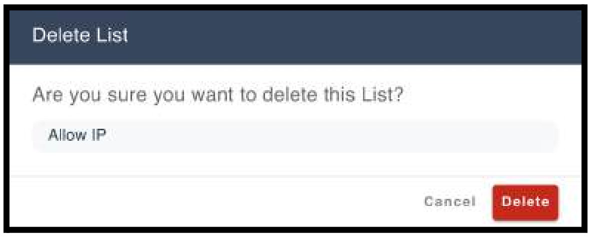
Lists (5 filtered, 33 total)

Filter

	NAME	TYPE	INDICATOR	ACCESS	SOURCE	POLICIES	COUNT	LAST SYNC	LAST UPDATE
All (1)		All (2)	All (2)	Private	All (2)				
●	Allow IP Inbound	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy	1	02/27/24, 10:10 AM	02/27/24, 10:10 AM
●	Allow IP Outbound	Allow	IP	Private	Manual	Outbound Policy	5	03/07/24, 11:09 AM	03/07/24, 11:09 AM
●	Customer IP Allow List	Allow	IP	Private	Manual	Inbound Policy Inbound Policy copy Outbound Policy	2	02/10/25, 01:31 PM	02/10/25, 01:31 PM
●	Customer Manual Domain List	Block	Domain	Private	Manual	Outbound Policy	3	02/26/24, 11:53 AM	
●	Customer Manual List	Block	IP	Private	Manual	Inbound Policy	4	02/26/24,	02/26/24,

NOTE: Lists that are tagged as “Public” Access cannot be deleted by end users

- On the confirmation modal, click Delete



Delete List

Are you sure you want to delete this List?

Allow IP

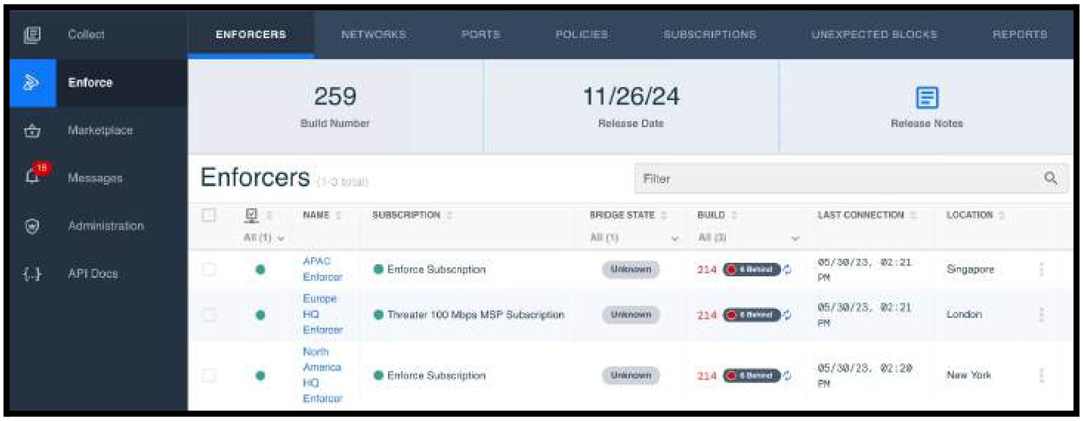
The list is now deleted.

Enforce

Enforce deploys and enforces data– in real time – at scale – across your entire network and blocks all known bad threat actors from ever entering your network. The Enforce menu options allow customers to view their Enforcers, and the pertinent data associated with each, install software builds, and configure their Networks and Ports.

Enforcers

The Enforcers tab displays all Enforcers that have been activated on your threatER account.



259
Build Number

11/26/24
Release Date

Enforcers (1-3 total)

	All (1)	NAME	SUBSCRIPTION	BRIDGE STATE All (1)	BUILD All (3)	LAST CONNECTION	LOCATION
□	●	APAC Enforcer	● Enforce Subscription	Unknown	214 6 Behind	05/30/23, 02:21 PM	Singapore
□	●	Europe HQ Enforcer	● Threater 100 Mbps MSP Subscription	Unknown	214 6 Behind	05/30/23, 02:21 PM	London
□	●	North America HQ Enforcer	● Enforce Subscription	Unknown	214 6 Behind	05/30/23, 02:20 PM	New York

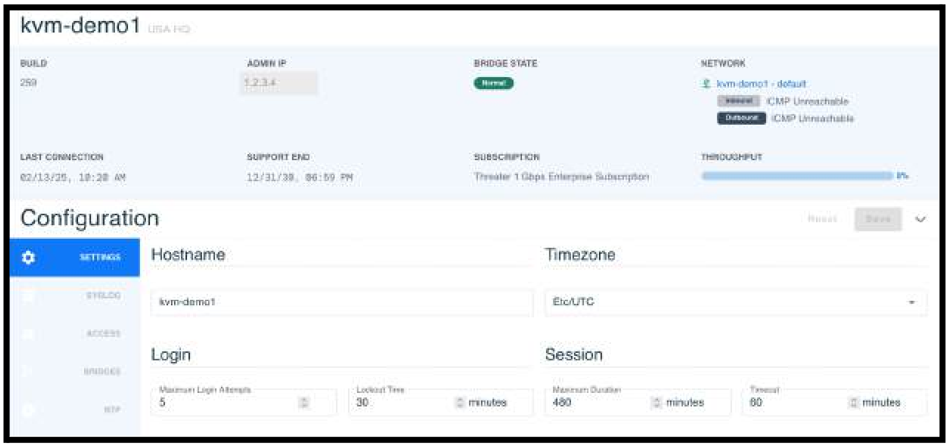
The following details display for each Enforcer:

- Enforcer Name - This is generally provided during activation time, but can be changed as needed (see below for instructions). If no such name is available, a unique identifier is displayed.
- Subscription - Enforce software subscription assigned to the Enforcer
    - See below more details on how to assign/unassign subscriptions
- Bridge State - displays one of the following:
    - Normal
    - Hardware Bypass - displays if the Enforcer is currently in hardware bypass mode
    - Unknown - displays for any Enforcer running legacy software, or if the Enforcer's current state is unknown
- Build – Displays the Enforce software build the Enforcer is currently running. If the Enforcer is not on the latest build, the build number will display in red and a label will display indicating the number of builds the instance is behind

    - Scheduled – displays the build schedule status. If there is no build status for the Enforcer, a "–" will display
- Last Connection – displays the date and time the Enforcer last connected to the threatER portal. Normally, this should be within a few minutes of the present time.
- Location – if a location has been provided by the user, it will display here. If no location has been provided, a "–" will display

To view additional details for an individual Enforcer click on the hyperlinked Enforcer name in the table. The following additional data will display:

- Admin IP of the Enforcer. This can be a great way for users to rediscover their administration IP if they've forgotten it and are in need of locally accessing Enforce, such as when working with our Customer Success team.
- Networks being managed by the Enforcer
- Support End Date
- Enforce Subscription assigned to the Enforcer
- Subscription Throughput – refer to the Subscription Throughput section below for more details
- Enforce Configuration Settings – see Enforce Configuration section below for more details



kvm-demo1 USA HQ

BUILD: 259
ADMIN IP: 1.2.3.4
BRIDGE STATE: Normal
NETWORK: kvm-demo1 - default
Inbound ICMP Unreachable
Outbound ICMP Unreachable

LAST CONNECTION: 02/13/25, 10:28 AM
SUPPORT END: 12/31/38, 06:59 PM
SUBSCRIPTION: Threater 1 Gbps Enterprise Subscription
THROUGHPUT: 0%

Configuration

Hostname: kvm-demo1
Timezone: Etc/UTC

Login
Maximum Login Attempts: 5
Lockout Time: 30 minutes

Session
Maximum Duration: 480 minutes
Timeout: 60 minutes

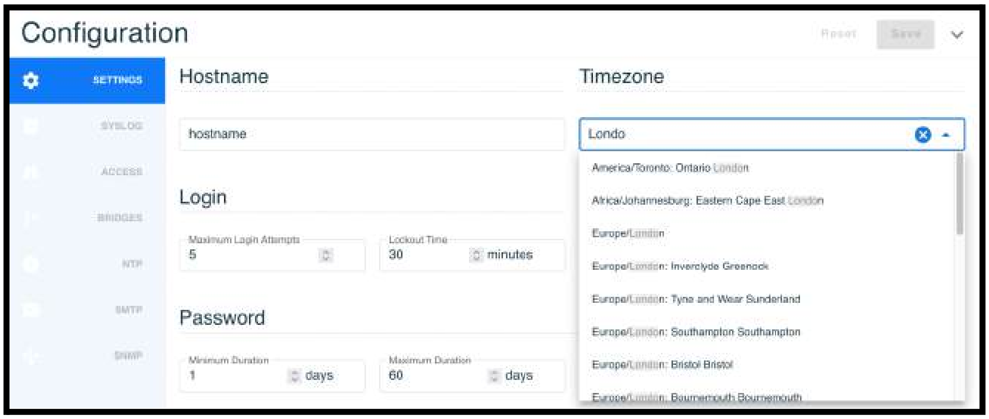
Enforce Configuration

This section outlines the Enforce configurations that can be managed in the threatER Portal. To manage configurations in the portal, an Enforcer needs to be on Build 247 or later. Once an Enforcer is updated to Build 247, these configurations will be read-only in the Enforce UI.

Settings

The following Settings are available for configuration in the portal:

- **Hostname**
  - This field allows you to provide a unique label for the Enforcer.
- **Timezone**
  - This sets the timezone for the Enforcer. The best way to set the timezone is to type a city in the field. Options, based on your entry, will display in the drop-down and one can be selected.



Configuration

Hostname

hostname

Timezone

Londo

America/Toronto: Ontario London
Africa/Johannesburg: Eastern Cape East London
Europe/London
Europe/London: Inverclyde Greenock
Europe/London: Tyne and Wear Sunderland
Europe/London: Southampton Southampton
Europe/London: Bristol Bristol
Europe/London: Bournemouth Bournemouth

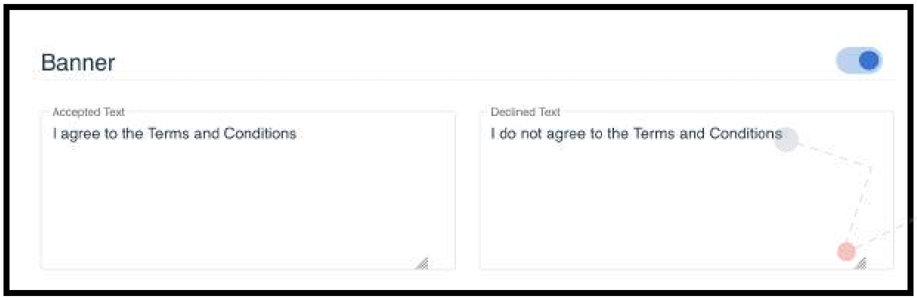
Login

Maximum Login Attempts: 5
Lockout Time: 30 minutes

Password

Minimum Duration: 1 days
Maximum Duration: 60 days

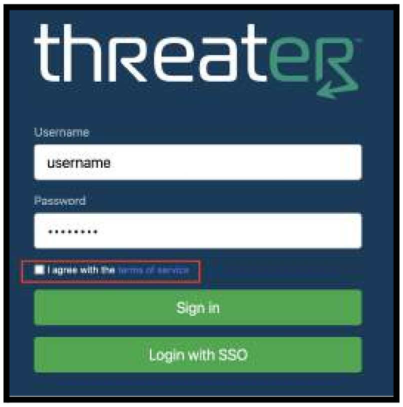
- **Login**
  - You can set the maximum number of login attempts a user can make before being locked out. If locked out, you can set how long the user will be locked out for before they can attempt to login again. These settings apply to the Enforce UI and NOT to the portal.
- **Session**
  - You can set how long a user's active session can last and when their session will be timed out if they are inactive. These settings apply to the Enforce UI and NOT to the portal.
- **Password**
  - You can set how long a password is valid for, the required character length, and the minimum number of password groups the password must contain (i.e. special characters, uppercase, lowercase, etc.) These password settings apply to the Enforce UI and NOT to the portal.
- **Banner**
  - Turning this setting on will enable a Terms of Service checkbox when a user attempts to login to the Enforce UI. If enabled, you can provide the text the user will see when accepting the Terms of Service, as well as what text will display if the user does not select the checkbox..



Banner

Accepted Text
I agree to the Terms and Conditions

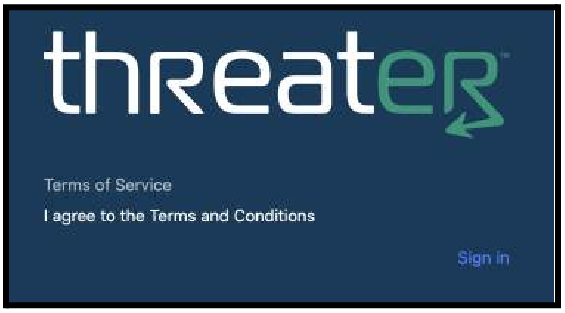
Declined Text
I do not agree to the Terms and Conditions



Username
username

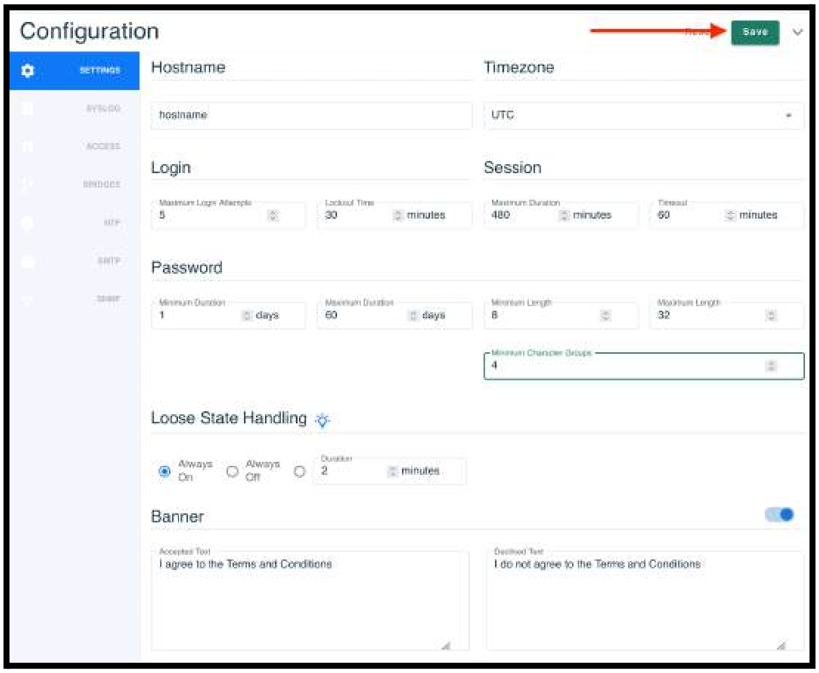
Password
••••••••

□ I agree with the terms of service



Terms of Service
I agree to the Terms and Conditions

After making any changes on the Settings tab, be sure to click on the Save button in the top right corner.



Hostname
hostname

Timezone
UTC

Login
Maximum Login Attempts: 5
Lockout Time: 30 minutes

Session
Maximum Duration: 480 minutes
Timeout: 60 minutes

Password
Minimum Duration: 1 days
Maximum Duration: 60 days
Minimum Length: 8
Maximum Length: 32
Minimum Character Groups: 4

Loose State Handling

● Always On ○ Always Off ○ Duration: 2 minutes

Banner

Accepted Text
I agree to the Terms and Conditions

Declined Text
I do not agree to the Terms and Conditions

Syslog

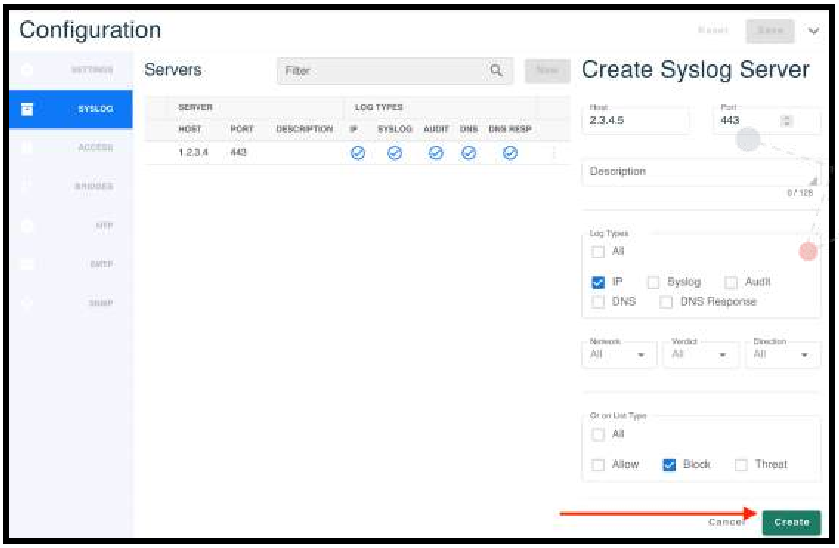
Syslog exports are an industry-standard way of exporting data in a concise, timely manner. Our syslog export format is compliant to RFC-5424 and ensures seamless integration alongside any number of external tools like:

- Security information and event management (SIEM) tools, such as Splunk and IBM QRadar
- Data analytics tools like Gravwell
- Full open-source tools like syslog-ng

Our Syslog export is not designed with any particular SIEM tool in mind. We focus on the comprehensive data contained in our syslog exports, enabling you to parse our logs by any tool that can ingest RFC-compliant syslog exports.

To setup a syslog server:

- Click on the “New” button in the top right corner of the table
- Enter the following required fields:
  - Host
  - Port
- Provide a description (optional)
- Choose the Log Types to export
  - “All” is the default selection
- Select the desired Network
  - “All is the default selection
- Select the desired Verdict
  - “All is the default selection
- Select the desired Direction
  - “All is the default selection
- Choose the List Types(s), if desired
- Click the “Create” button in the bottom right corner



SERVER			LOG TYPES				
HOST	PORT	DESCRIPTION	IP	SYSLOG	AUDIT	DNS	DNS RESP
1.2.3.4	443		✓	✓	✓	✓	✓

Create Syslog Server

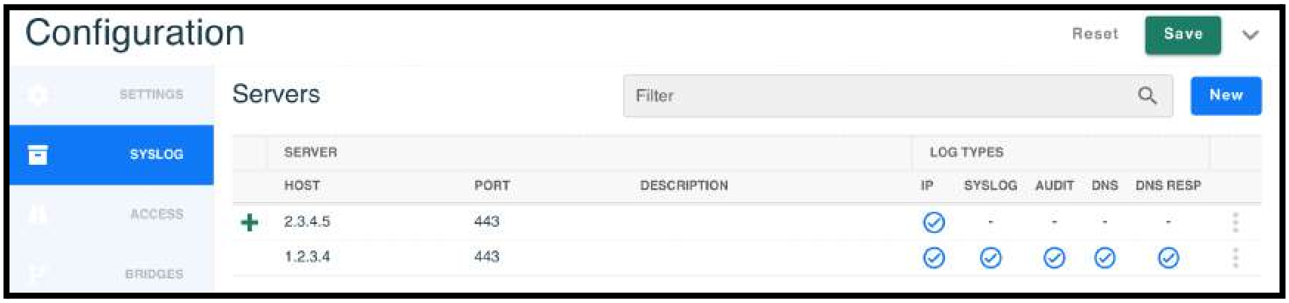
Host: 2.3.4.5
Port: 443
Description
0 / 128

Log Types
□ All
☑ IP □ Syslog □ Audit
□ DNS □ DNS Response

Network: All
Verdict: All
Direction: All

Or on List Type
□ All
□ Allow ☑ Block □ Threat

- Once all desired Syslog Servers have been added, click the Save button in the the top right corner



	SERVER			LOG TYPES				
	HOST	PORT	DESCRIPTION	IP	SYSLOG	AUDIT	DNS	DNS RESP
+	2.3.4.5	443		✓	-	-	-	-
	1.2.3.4	443		✓	✓	✓	✓	✓

Access

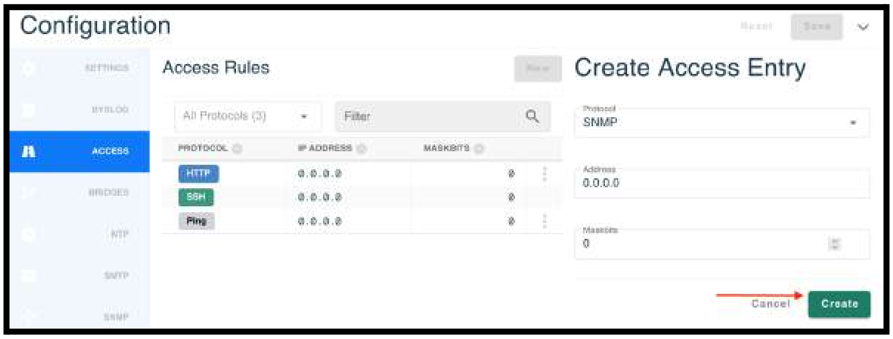
If your company has allowed Access rules to be managed in the threatER Portal (via a setting in the Enforce UI), the following protocols are available to add/edit:

- **HTTPS**- This setting allows you to add internal networks that are allowed access to the admin interface of the threatER Enforcer.
- **Ping** – The ping utility indicates if a particular internet address is accessible via the internet. This ping functionality can be abused by intruders, who may scan every internet address in a network, seeking out active targets. The Ping access setting allows you to block these intelligence-gathering scans by adding a list of trusted management networks. threatER Enforce will accept ping requests from these networks, and deny them from all others. By default, threatER Enforce will allow ping access from all IPv4 networks, as is indicated by the 0.0.0.0/0 address. After you allow access to your own local management networks, you can remove this "allow all" access by deleting it.

- **SNMP** – The SNMP access setting allows you to add a list of trusted management networks. threatER Enforce will accept SNMP requests from these networks, and deny them from all others.
- **SSH** – For any Enforcer in AWS, Azure, or Google Cloud, a default SSH access rule will be applied.

To add an Access rule:

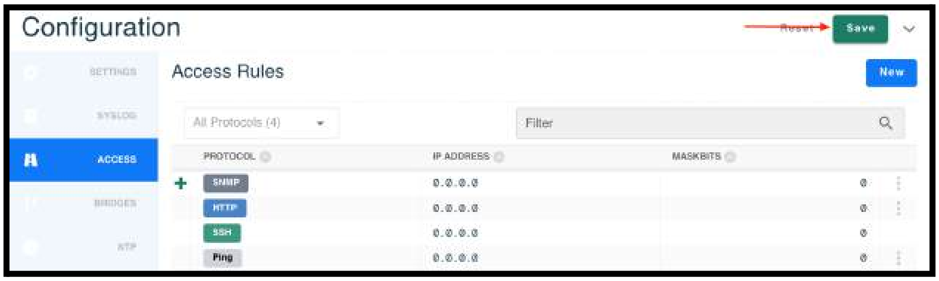
- Click the "New" button in the top-right corner of the table
- Select the desired Protocol
- Enter the applicable Address
- Enter the applicable Maskbits
- Click the Create button



PROTOCOL	IP ADDRESS	MASKBITS
HTTP	0.0.0.0	0
SSH	0.0.0.0	0
Ping	0.0.0.0	0

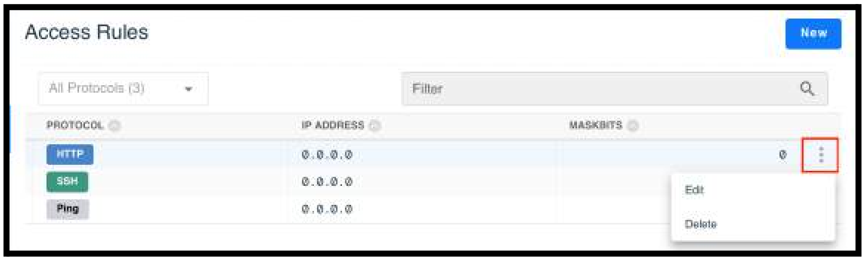
Protocol: SNMP
Address: 0.0.0.0
Maskbits: 0

- Once all desired Access Rules have been added, click the Save button in the top right corner



PROTOCOL	IP ADDRESS	MASKBITS
SNMP	0.0.0.0	0
HTTP	0.0.0.0	0
SSH	0.0.0.0	0
Ping	0.0.0.0	0

To edit or delete an Access Rule, click on the ellipsis in the right hand column of the table and select the desired option.



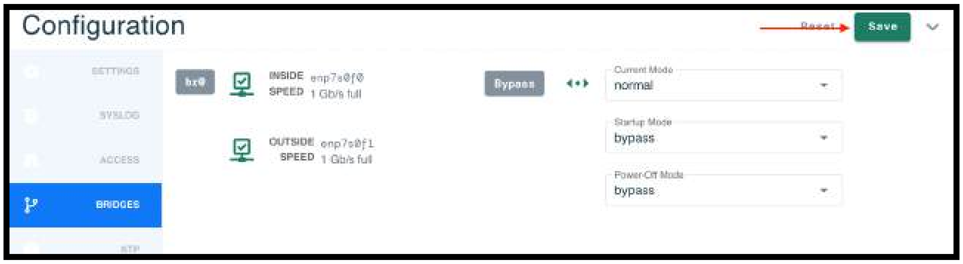
PROTOCOL	IP ADDRESS	MASKBITS
HTTP	0.0.0.0	0
SSH	0.0.0.0	
Ping	0.0.0.0	

Bridges

The Bridges tab displays the bandwidth or maximum rate of data transfer between the two bridge Ethernet ports. If Bypass is available, end users will be able to set the following modes:

- Bypass
- Startup
- Power-Off

If a Bypass Mode change is made, be sure to click the Save button in the top-right corner.



INSIDE enp7s0f0
SPEED 1 Gb/s full

OUTSIDE enp7s0f1
SPEED 1 Gb/s full

Current Mode: normal

Startup Mode: bypass

Power-Off Mode: bypass

NTP

The Network Time Protocol is a standard system for synchronizing the built-in clocks of network connected devices, to a very high degree of precision. Connecting threatER Enforce to the NTP network will ensure that the timestamps on its log files are accurate and coordinated with the computers in your organization.

threatER Enforce supports NTP version 3. Enter the IPv4 or IPv6 Internet address of your organization's NTP server, or if one isn't available, select a public server. Lists of time servers can be found at The NTP Public Services Project: http://support.ntp.org. NTPv3 has optional authentication. If required, click "Use Preshared Key" and enter the key information used by your selected time server.

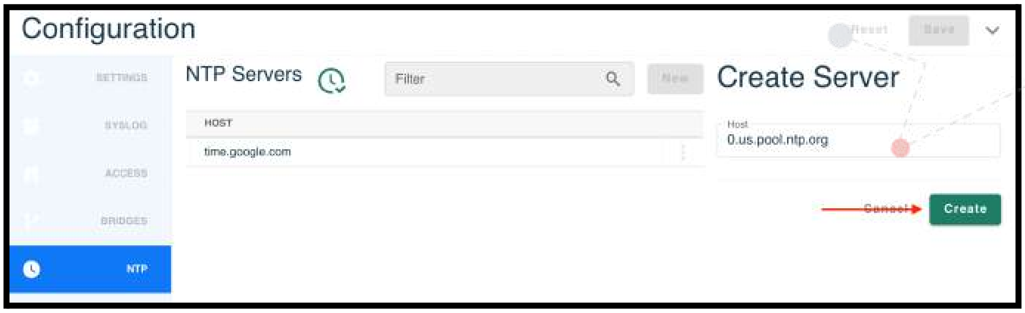
For more accurate time synchronization, and as a guard against network outages, configure more than one timeserver.

Configuring the Time Zone and Date/Time settings can be done either manually or using an NTP server. Note that manually set times will be overwritten by the NTP Server settings.

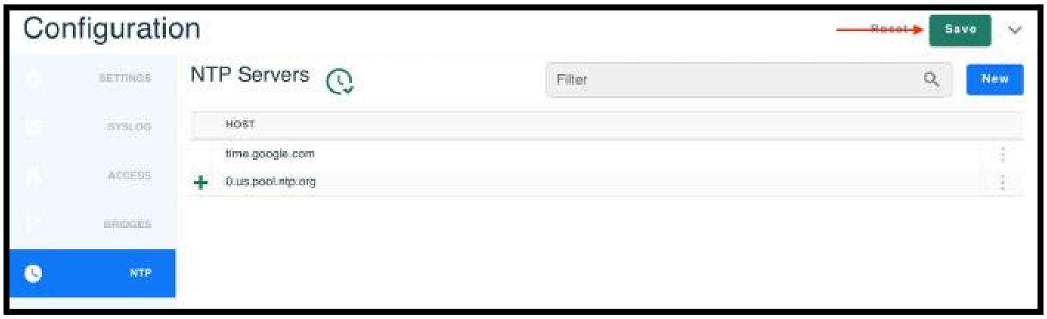
To create an NTP Server:

- Click on the “New” button in the top-right corner of the table

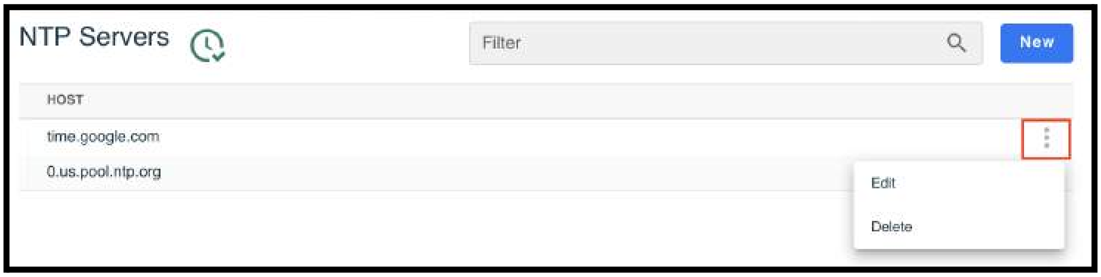
- Enter the Host
- Click the "Create" button



- Once all desired NTP Servers have been added, click the "Save" button in the top right corner.



To edit or delete a NTP Server, click on the ellipsis in the right hand column of the table and select the desired option.



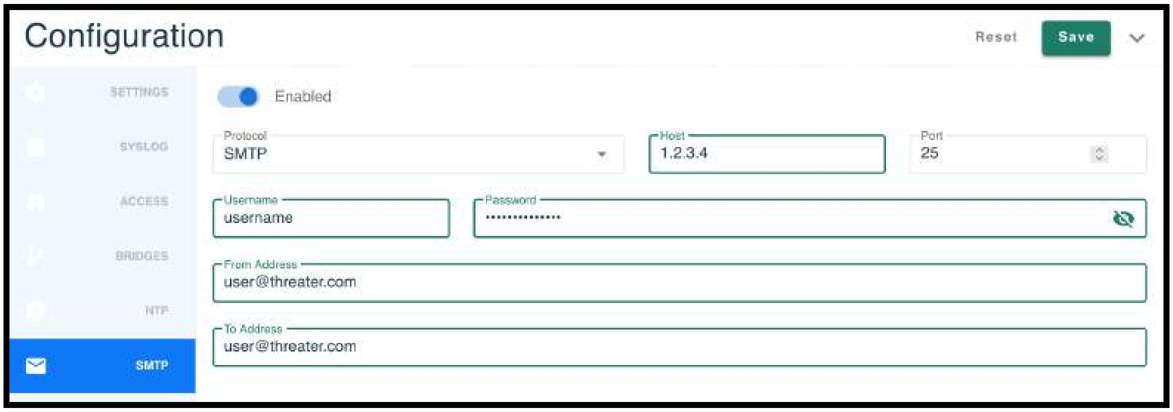
SMTP

SMTP messages can be sent when an alarm is raised (e.g. an update fails, entering bypass mode or an account gets locked out).

To enable SMTP alerts:

- Set the Enabled toggle to the right
- Select the desired Protocol

- Enter the Host
- Enter the Port
- If authentication is required, provide the Username and Password
- Enter the “From Address”
- Enter the “To Address”
- Click the Save button in the top right corner.



Configuration

Enabled

Protocol: SMTP

Host: 1.2.3.4

Port: 25

Username: username

Password: ••••••••••••••

From Address: user@threater.com

To Address: user@threater.com

SNMP

threatER Enforce supports the internet standard Simple Network Management Protocol (SNMP). Admins can remotely monitor Enforce by a network management system, such as IBM Tivoli Network Manager, CiscoWorks LAN Management Solution, and HP Network Node Manager.

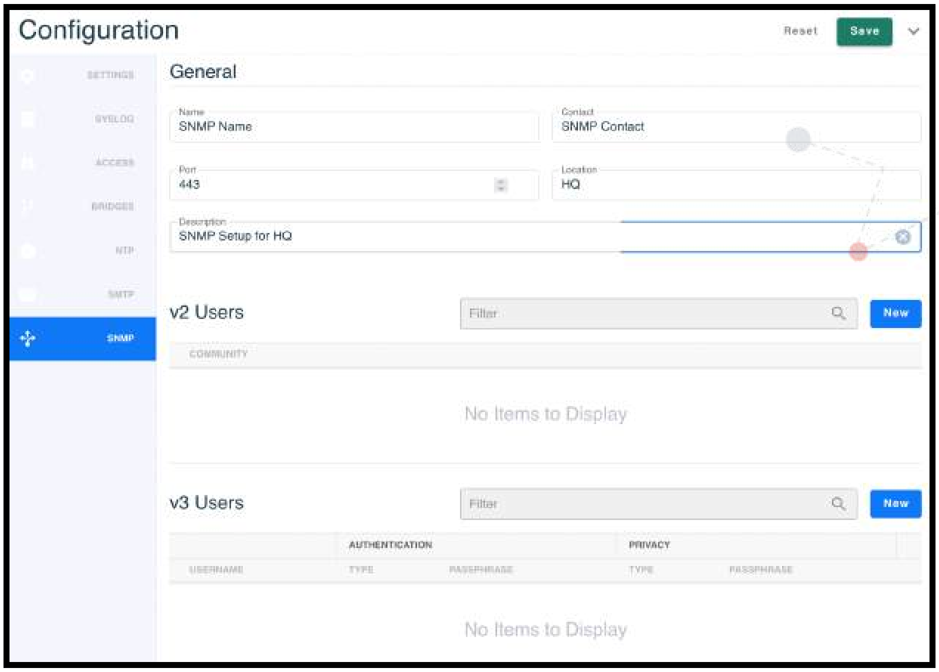
Admins will need to set up SNMP access first before making SNMP configurations.

To configure SNMP, enter the following:

- Name
- Contact
- Port
- Location
- Description

threatER supports two versions of SNMP:

- Community-based SNMPv2c
- SNMPv3



Configuration

General

Name: SNMP Name

Contact: SNMP Contact

Port: 443

Location: HQ

Description: SNMP Setup for HQ

v2 Users

COMMUNITY
No Items to Display

v3 Users

	AUTHENTICATION		PRIVACY	
USERNAME	TYPE	PASSPHRASE	TYPE	PASSPHRASE

No Items to Display

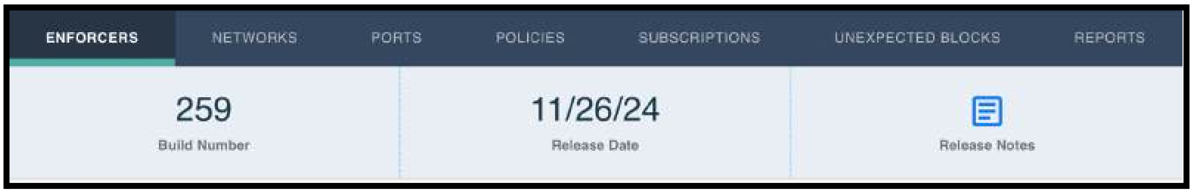
Click the "New" button next to the desired version and provide the necessary details. Once complete, click the "Save" button in the top right corner.

Enforce Software

From the Enforcers tab, customers can install the latest Enforce software build onto their Enforcers.

The following software information is displayed on this tab:

- Build Number
    - Critical Update – this will display if the build is critical in nature. Builds are flagged as critical if they include important security-related updates, critical bug fixes, or new features critical to the operation of the threatER platform. It is recommended to install critical updates as soon as possible.
- Release Date of the Build
- Release Notes – clicking this will open a PDF of the Build Release Notes in a separate browser tab



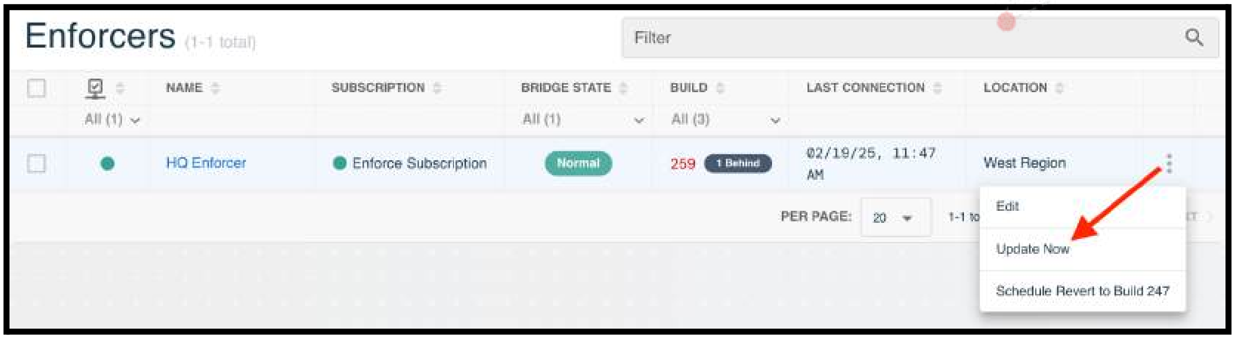
259	11/26/24	
Build Number	Release Date	Release Notes

Users have the option to perform an immediate update, or to schedule an update.

Update Now

To immediately install the latest build on an Enforcer:

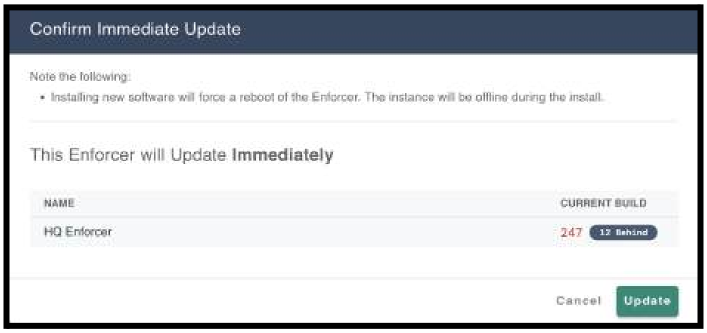
- In the row of the Enforcer, select Update Now from the ellipsis menu



Enforcers (1-1 total)

		NAME	SUBSCRIPTION	BRIDGE STATE	BUILD	LAST CONNECTION	LOCATION
	All (1)			All (1)	All (3)		
□	●	HQ Enforcer	● Enforce Subscription	Normal	259 1 Behind	02/19/25, 11:47 AM	West Region

- On the confirmation modal, click the Update button



Confirm Immediate Update

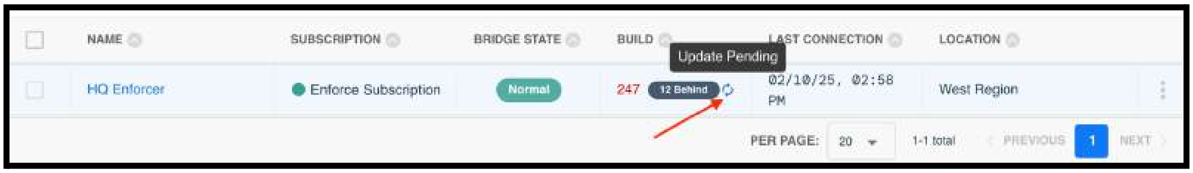
Note the following:

- Installing new software will force a reboot of the Enforcer. The instance will be offline during the install.

This Enforcer will Update **Immediately**

NAME	CURRENT BUILD
HQ Enforcer	247 12 Behind

The table will display an “Update Pending” icon for the Enforcer until the build installation is complete. The “Update Pending” will automatically clear as soon as the associated Enforcer has begun the process of the update. Upon completion, which can take several minutes, the new build number will appear in the status.

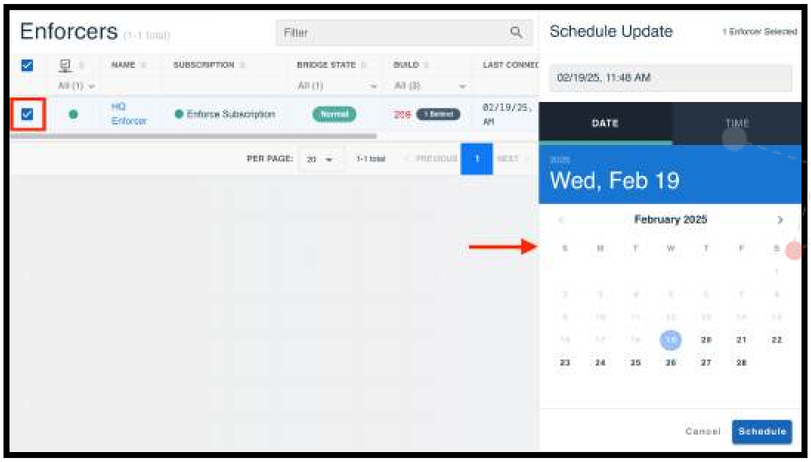


	NAME	SUBSCRIPTION	BRIDGE STATE	BUILD	LAST CONNECTION	LOCATION
□	HQ Enforcer	● Enforce Subscription	Normal	247 12 Behind	02/10/25, 02:58 PM	West Region

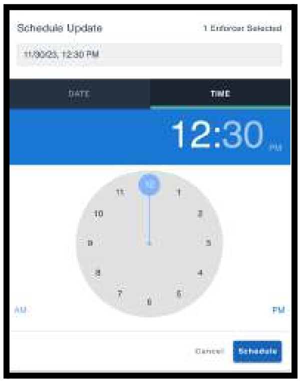
Schedule Update

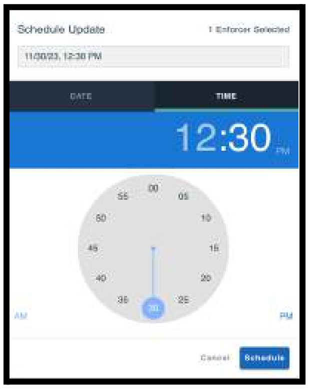
Updates can be scheduled for one or more Enforcers. To schedule a build installation:

- Select the Enforcer(s) in the table
- Select the desired date in the calendar



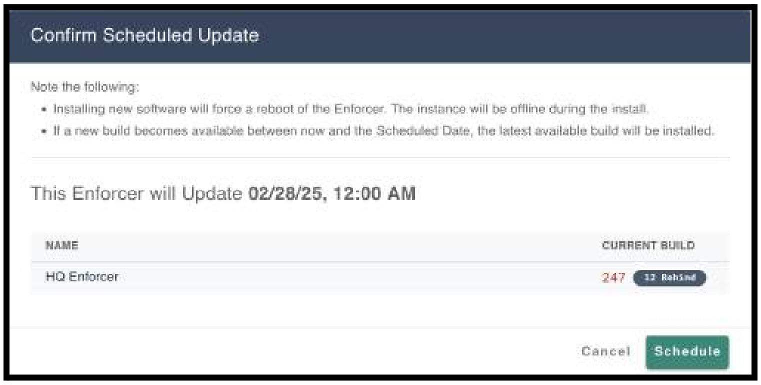
- Click the Time tab and choose the desired time (both hours and minutes)





PLEASE NOTE: The time selected is in the user's local timezone, but saved in the backend in UTC. For example, if the user is located in New York City (EST) and selects 6:00PM, but the Enforcer is located in San Francisco (PST), the installation will begin at 6:00PM EST / 3:00PM PST.

- Click the Schedule button
- On the Confirm Scheduled Updates modal, click Schedule



Confirm Scheduled Update

Note the following:

- Installing new software will force a reboot of the Enforcer. The instance will be offline during the install.
- If a new build becomes available between now and the Scheduled Date, the latest available build will be installed.

This Enforcer will Update **02/28/25, 12:00 AM**

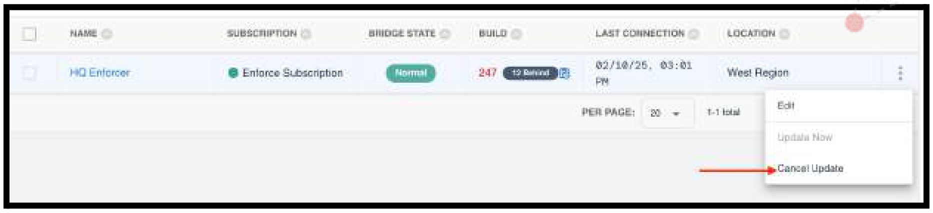
NAME	CURRENT BUILD
HQ Enforcer	247 13 Behind

The table will reflect the schedules.

Cancel a Scheduled Update

To cancel a scheduled update:

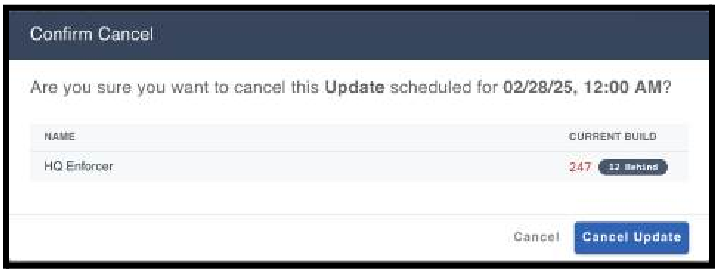
- In the row of the Enforcer, select Cancel Update from the ellipsis menu



☐	NAME	SUBSCRIPTION	BRIDGE STATE	BUILD	LAST CONNECTION	LOCATION
☐	HQ Enforcer	● Enforce Subscription	Normal	247 12 Behind	02/10/25, 03:01 PM	West Region

PER PAGE: 20 1-1 total

- On the Confirm Cancel modal, click the Cancel Update button



Confirm Cancel

Are you sure you want to cancel this **Update** scheduled for **02/28/25, 12:00 AM**?

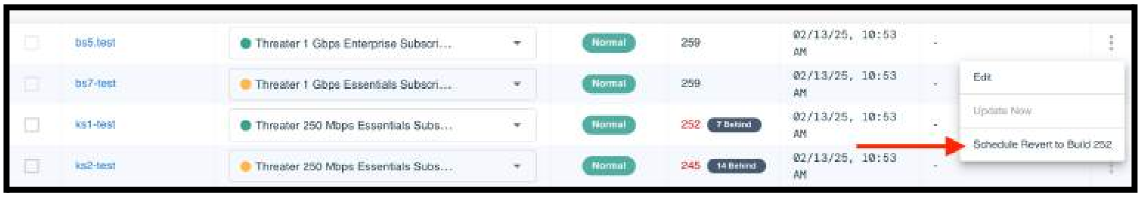
NAME	CURRENT BUILD
HQ Enforcer	247 12 Behind

The table will reflect the cancellation.

Revert to Previous Build

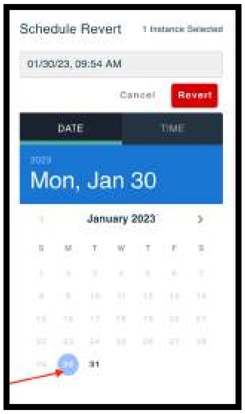
Users may have the ability to revert to the previous software build that was installed on an Enforcer, if both the previous and current versions, as a pair, are revertible. Reverts must be scheduled and can be done by completing the following steps:

- In the row of the Enforcer, select Schedule Revert to Build [#] from the ellipsis menu



☐	bs5.test	● Threater 1 Gbps Enterprise Subscri...	Normal	259	02/13/25, 10:53 AM	-
☐	bs7-test	● Threater 1 Gbps Essentials Subscri...	Normal	259	02/13/25, 10:53 AM	-
☐	ks1-test	● Threater 250 Mbps Essentials Subs...	Normal	252 7 Behind	02/13/25, 10:53 AM	-
☐	ks2-test	● Threater 250 Mbps Essentials Subs...	Normal	245 14 Behind	02/13/25, 10:53 AM	-

- Select a date from the calendar



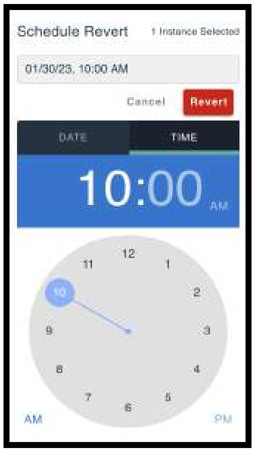
Schedule Revert

1 Instance Selected

01/30/23, 09:54 AM

- Click the Time tab and set the time (both hours and minutes)

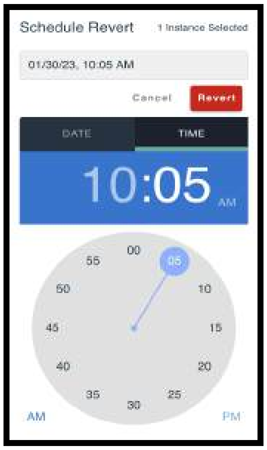
PLEASE NOTE: The time selected is in the user's local timezone, but saved in the backend in UTC. For example, if the user is located in New York City (EST) and selects 6:00PM, but the Enforcer is located in San Francisco (PST), the installation will begin at 6:00PM EST / 3:00PM PST.



Schedule Revert

1 Instance Selected

01/30/23, 10:00 AM

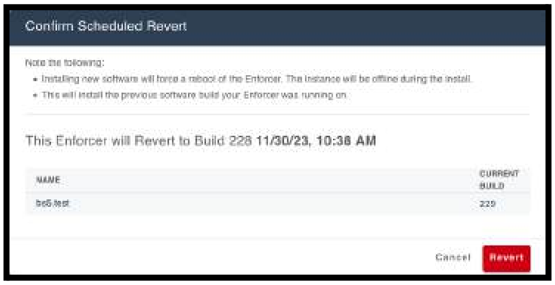


Schedule Revert

1 Instance Selected

01/30/23, 10:05 AM

- Click the Revert button
- On the Confirm Scheduled Revert modal, click Revert



Confirm Scheduled Revert

Note the following:

- Installing new software will force a reboot of the Enforcer. The instance will be offline during the install.
- This will install the previous software build your Enforcer was running on.

This Enforcer will Revert to Build 228 **11/30/23, 10:38 AM**

NAME	CURRENT BUILD
bs5.test	229

The table will reflect the scheduled revert.

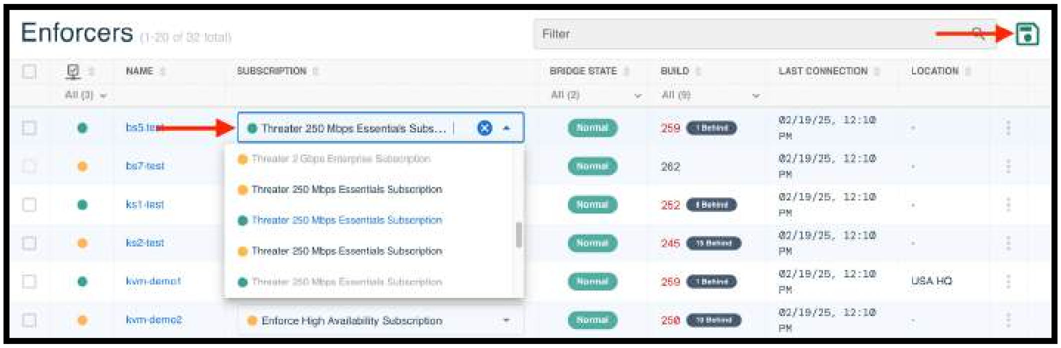
Manual Downloads

It is strongly recommended to utilize the automatic installation of Enforce software builds described in the above sections. Should a manual download of a build be required, please consult our [Customer Success team](#) for assistance. We do not recommend that you attempt Manual Downloads on your own without assistance. Use our automated mechanism as previously described unless instructed otherwise by our Customer Success team.

Subscription Management

To manage subscriptions from the Enforcers tab:

- Select (or remove) a subscription from the drop-down
- Make any additional necessary subscription updates to other Enforcers
- Click the Save Subscriptions button at the top of the table



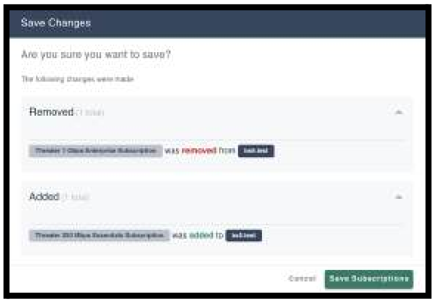
Enforcers (1-20 of 32 total)

Filter

□		NAME	SUBSCRIPTION	BRIDGE STATE	BUILD	LAST CONNECTION	LOCATION
	All (3)			All (2)	All (9)		
□	●	bs5.test	● Threater 250 Mbps Essentials Subs...	Normal	259 1 Behind	02/19/25, 12:10 PM	-
□	●	bs7-test		Normal	262	02/19/25, 12:10 PM	-
□	●	ks1-test		Normal	252 8 Behind	02/19/25, 12:10 PM	-
□	●	ks2-test		Normal	245 15 Behind	02/19/25, 12:10 PM	-
□	●	kvm-demo1		Normal	259 1 Behind	02/19/25, 12:10 PM	USA HQ
□	●	kvm-demo2	● Enforce High Availability Subscription	Normal	250 10 Behind	02/19/25, 12:10 PM	-

● Threater 2 Gbps Enterprise Subscription
● Threater 250 Mbps Essentials Subscription
● Threater 250 Mbps Essentials Subscription
● Threater 250 Mbps Essentials Subscription
● Threater 250 Mbps Essentials Subscription

- On the Save Changes modal, review the selected changes that were made and then click the Save Subscriptions button



Save Changes

Are you sure you want to save?

The following changes were made

Removed (1 total)

Threater 1 Gbps Enterprise Subscription was removed from bs5.test

Added (1 total)

Threater 250 Mbps Essentials Subscription was added to bs5.test

Subscription Status Indicators:

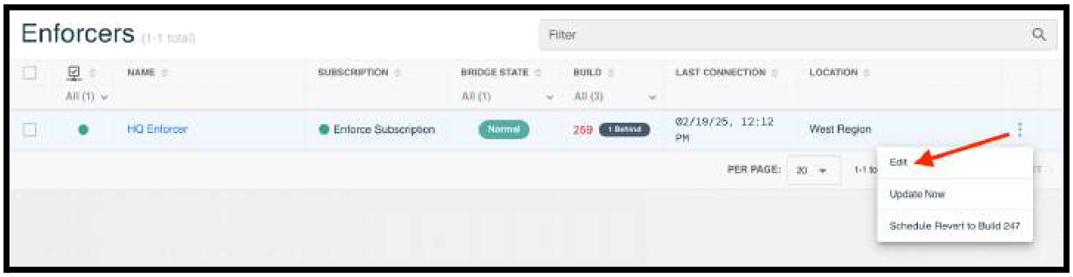
- Green - subscription is actively supported

- Yellow – support has lapsed; any Enforcer assigned a subscription in this state may not receive updated threat intelligence and as a result may be in an Allow-All state. You should contact our Customer Success team to review your subscription status.

Editing Enforcer Name and Location

To simplify your ability to identify your Enforcer according to your own network naming conventions, you can edit its Name and/or Location:

- Find the Enforcer in the table and from the ellipsis menu select Edit



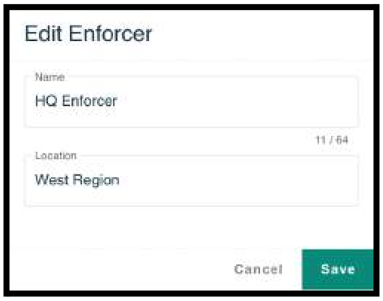
Enforcers (1-1 total)

Filter

□	All (1)	NAME	SUBSCRIPTION	BRIDGE STATE All (1)	BUILD All (3)	LAST CONNECTION	LOCATION
□	●	HQ Enforcer	● Enforce Subscription	Normal	259 1 Behind	02/19/25, 12:12 PM	West Region

PER PAGE: 20 1-1 to

- Enter the desired name and/or location
- Click Save



Edit Enforcer

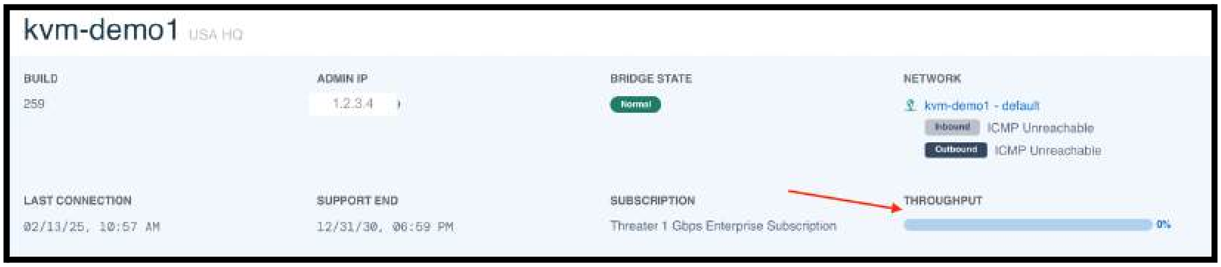
Name: HQ Enforcer

11 / 64

Location: West Region

Subscription Throughput

The Subscription Throughout chart provides the past 30 days of an Enforcer's inbound and outbound throughput. To access the Subscription Throughput chart, click on the hyperlinked name of an individual Enforcer and then select the Subscription Throughput bar.



kvm-demo1 USA HQ

BUILD: 259

ADMIN IP: 1.2.3.4

BRIDGE STATE: Normal

NETWORK: kvm-demo1 - default
Inbound ICMP Unreachable
Outbound ICMP Unreachable

LAST CONNECTION: 02/13/25, 10:57 AM

SUPPORT END: 12/31/30, 06:59 PM

SUBSCRIPTION: Threater 1 Gbps Enterprise Subscription

THROUGHPUT: 0%

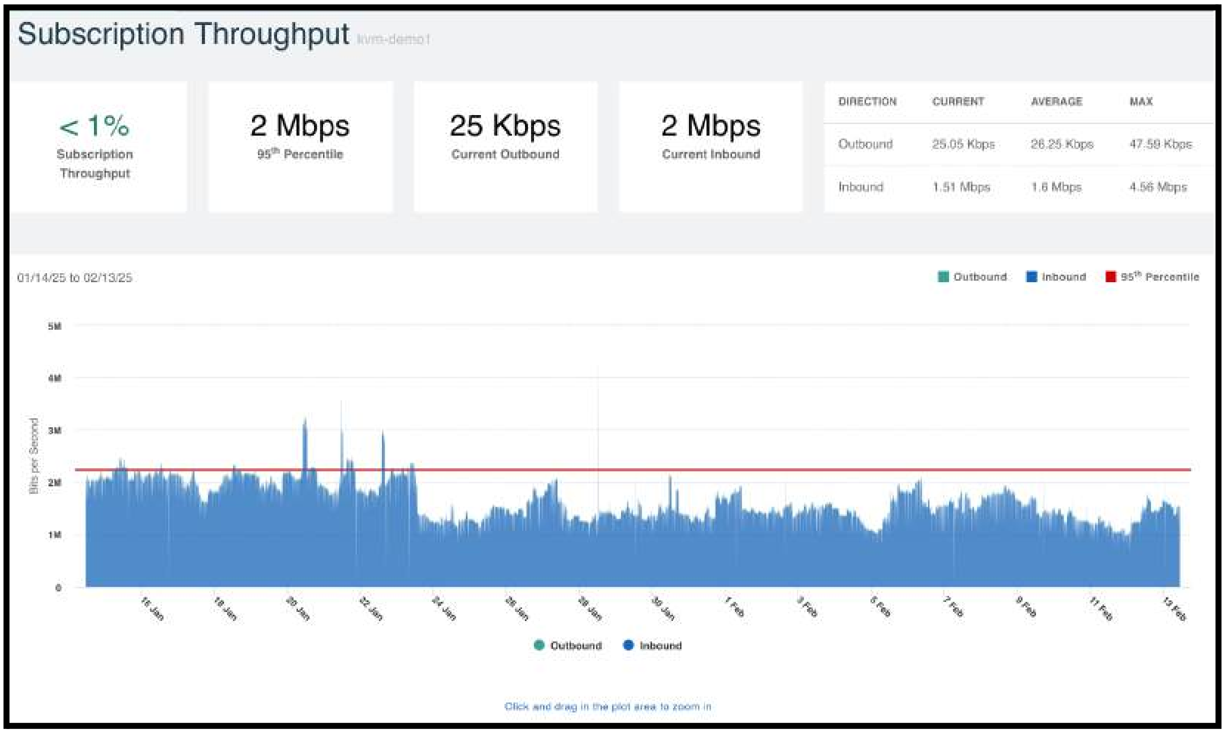
The following throughput details will display at the top:

- % Subscription Throughput utilized for the past 30 days
- 95th Percentile for the past 30 days, via industry standard 95/5 measurements
- Current Outbound throughput (in bits)
- Current Inbound throughput (in bits)

The table in the top right corner will display the following inbound and outbound data:

- Current throughput (in bits per second)
- Average throughput (in bits per second)
- Maximum throughput (in bits per second)

The chart displays a graphical representation of the inbound and outbound throughput and the 95th percentile for the past 30 days. You can click and drag within the plot area to zoom in to a specific date/time.



Subscription Throughput kvm-demo1

< 1%
Subscription Throughput

2 Mbps
95th Percentile

25 Kbps
Current Outbound

2 Mbps
Current Inbound

DIRECTION	CURRENT	AVERAGE	MAX
Outbound	25.05 Kbps	26.25 Kbps	47.59 Kbps
Inbound	1.51 Mbps	1.6 Mbps	4.56 Mbps

01/14/25 to 02/13/25

Click and drag in the plot area to zoom in

Networks

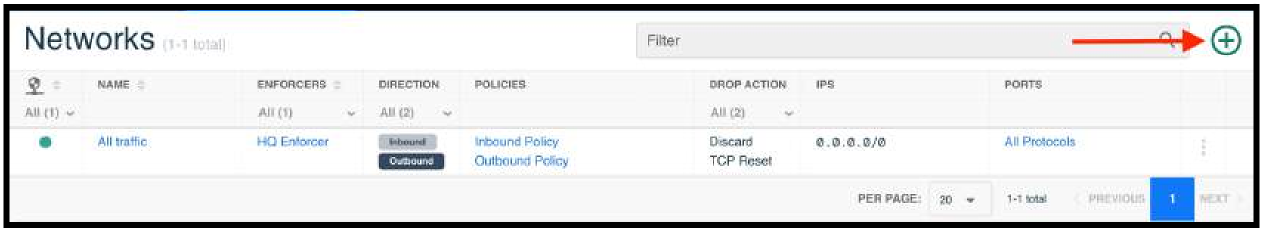
Enforce inspects Network traffic to determine which packets to block and which to allow. Policies attached to Networks determine the internet services allowed into your network, as well as those services your local users can access outside the network.

One or more network rules comprise a configured Network in threatER, and each network is identified as a device, asset, or subnet on your network. If the Enforcer receives traffic for the configured IP, then it will allow traffic according to the policy assigned to the Network. Each Network configuration includes a protocol and port, or range of ports, so that you may restrict specific policy activity to as granular a level as required.

Creating Networks

To create a Network:

- Navigate to Enforce in the left-hand navigation menu
- Click the Networks tab
- Click the "+" button in the top-right corner



Networks (1-1 total)

Filter

	NAME	ENFORCERS	DIRECTION	POLICIES	DROP ACTION	IPS	PORTS
All (1)		All (1)	All (2)		All (2)		
●	All traffic	HQ Enforcer	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols

PER PAGE: 20 1-1 total PREVIOUS 1 NEXT

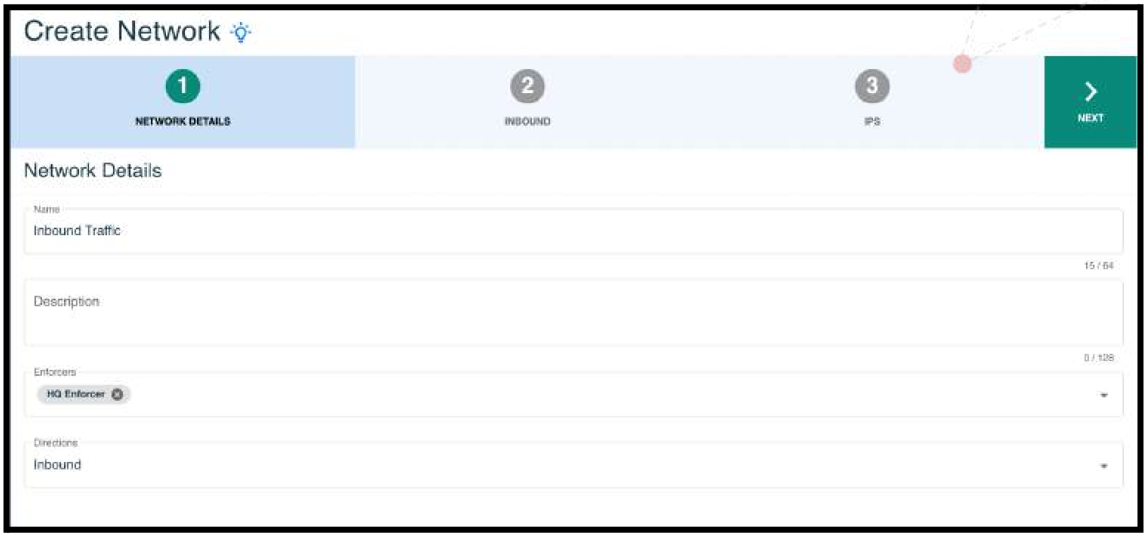
Network Details

Provide the following (* indicates required field):

- *Name (unique name required)
- Enter an optional description
- Enforcers
  - Select the desired Enforcer(s) from the drop-down
- *Direction
  - **Inbound** – determines the kind of internet traffic allowed into your network. Each inbound rule shows a particular computer and service that will be visible to the internet.

- ○ **Outbound** – determines how your local computers can access the internet. Each outbound rule shows which particular outside internet service a computer can access.

Once all required fields are complete, click the Next button to proceed to the next step.



Create Network

Network Details

Name
Inbound Traffic
15 / 64

Description
0 / 128

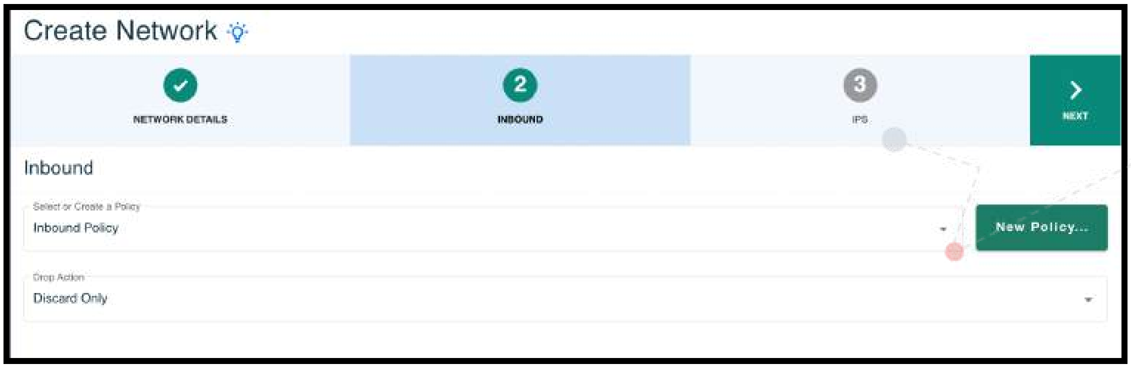
Enforcers
HQ Enforcer

Directions
Inbound

Inbound/Outbound

Provide the following for the Direction(s) selected in the previous step (* indicates required field):

- *Policy
- *Drop Action
    - ○ Discard – drops the packet and does not send any response (silently discards it). This is useful especially for inbound attempts, so that malicious attackers are not necessarily able to determine your presence
    - ○ ICMP Unreachable – drops the packet and sends an ICMP unreachable packet to the sender. This is generally recommended only for use with outbound policies.
    - ○ TCP Reset – drops the packet and sends a TCP Reset packet back to the sender. Recommended only if the firewall doesn't properly allow ICMP Unreachable messages. Additionally, this is generally recommended only for use with outbound policies.
- Click Next to proceed to the next step.



Create Network

Inbound

Select or Create a Policy: Inbound Policy

Drop Action: Discard Only

If “Both” was chosen as the Direction on the Details step, the next step will be the same as above, but for the Outbound direction.

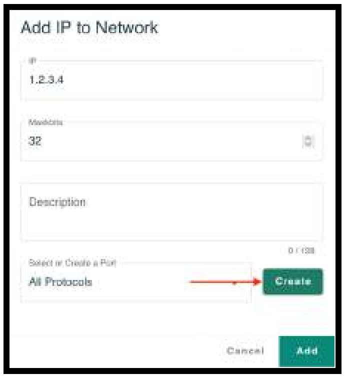
Create New Policy During Network Creation

If a policy does not exist that you want to apply your Network to, you have the option to create a new policy within the Network wizard. To do so, click the “New Policy” button on the Inbound and/or Outbound step and then follow the steps to create a policy, outlined above in the Policies section of this document.

IPs

To add IPs to your Network, provide the following (* indicates required field):

- *IP address
- *Maskbits
- Description
- *Port
    - All Protocols is the default selection
    - To choose a Port you have previously configured, click on the drop-down and select the desired option
    - To create a new Port:
        - Click on the Create button



Add IP to Network

IP: 1.2.3.4

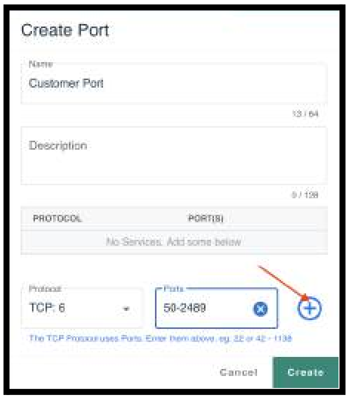
Maskbits: 32

Description

0 / 128

Select or Create a Port: All Protocols

- Provide the following (* indicates required field):
  - *Name
  - Description
  - *Protocol
    - "All: 256" is the default selection, but another protocol can be selected from the drop-down
      - You will be required to provide a Port or Port Range for some protocols, such as TCP and UDP
    - Click on the "+" button to add the Protocol
    - Add any additional Protocols, as necessary



Create Port

Name: Customer Port

13 / 64

Description

0 / 128

PROTOCOL	PORT(S)
No Services. Add some below	

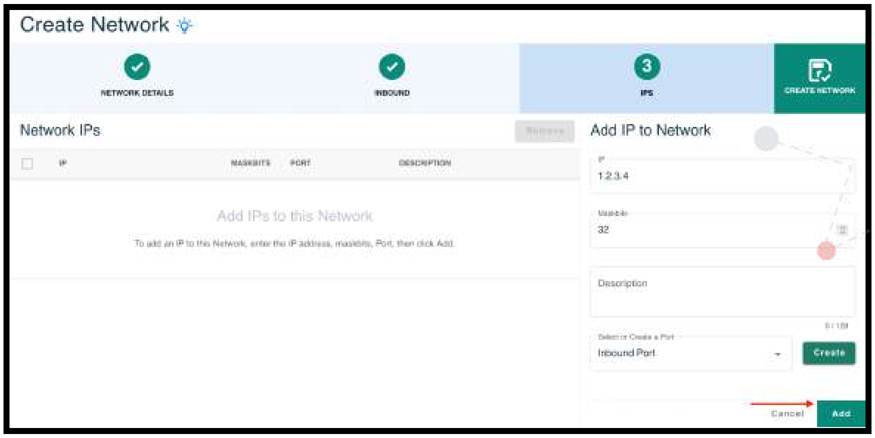
Protocol: TCP: 6

Ports: 50-2489

The TCP Protocol uses Ports. Enter them above, eg. 22 or 42 - 1138

    - Click the Create button to return to the Add IP Panel

- Click the Add button to add the IP to the Network



Create Network

NETWORK DETAILS — INBOUND — 3 IPS — CREATE NETWORK

Network IPs

□	IP	MASKBITS	PORT	DESCRIPTION

Add IPs to this Network

To add an IP to this Network, enter the IP address, maskbits, Port, then click Add.

Add IP to Network

IP: 1.2.3.4

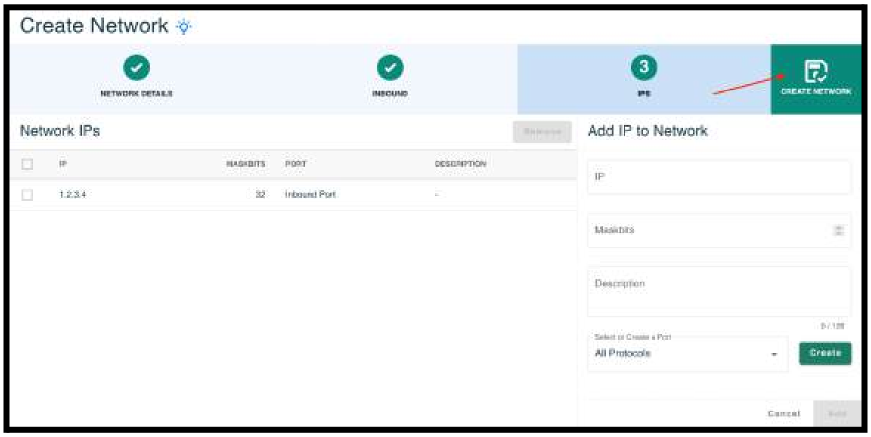
Maskbits: 32

Description

0 / 128

Select or Create a Port: Inbound Port

- Follow the steps above to add additional IPs
- Once all IPs are added, click the Create Network button to create the Network.



Create Network

NETWORK DETAILS — INBOUND — 3 IPS — CREATE NETWORK

Network IPs

□	IP	MASKBITS	PORT	DESCRIPTION
□	1.2.3.4	32	Inbound Port	-

Add IP to Network

IP

Maskbits

Description

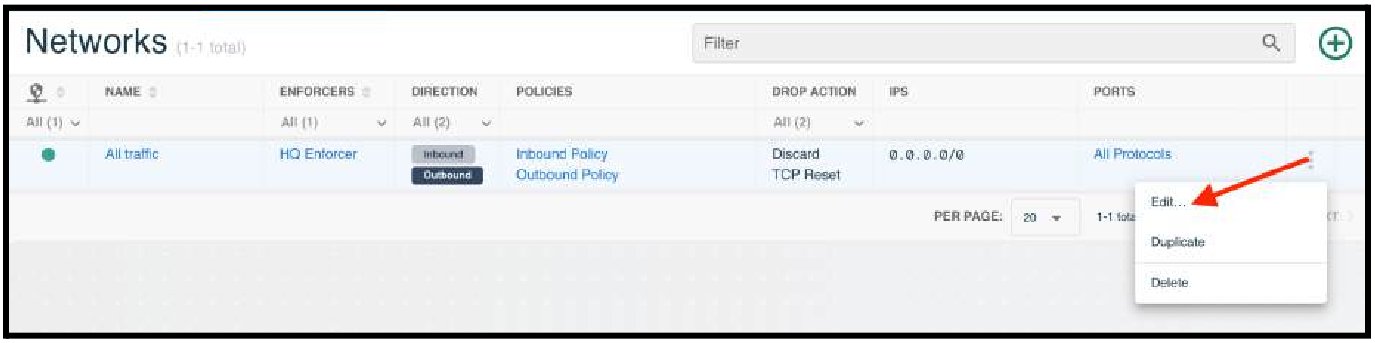
0 / 128

Select or Create a Port: All Protocols

Editing a Network

To Edit a Network:

- Find the Network in the table and from the ellipsis menu, select Edit



Networks (1-1 total)

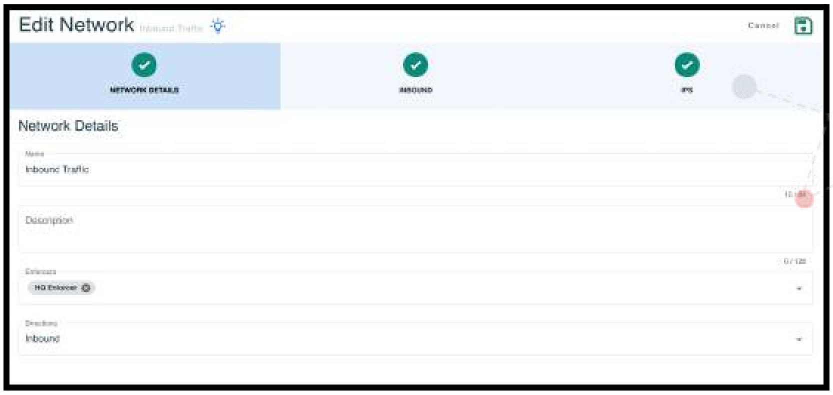
Filter

	NAME	ENFORCERS	DIRECTION	POLICIES	DROP ACTION	IPS	PORTS
All (1)		All (1)	All (2)		All (2)		
●	All traffic	HQ Enforcer	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols

PER PAGE: 20   1-1 tota

  - ○ Edit Network Details –
    - ■ This Is the default view when editing a Network. Make any necessary edits and then select another step that requires updates.

        - If edits are only needed on this step, click the Save button in the top right corner



Network Details

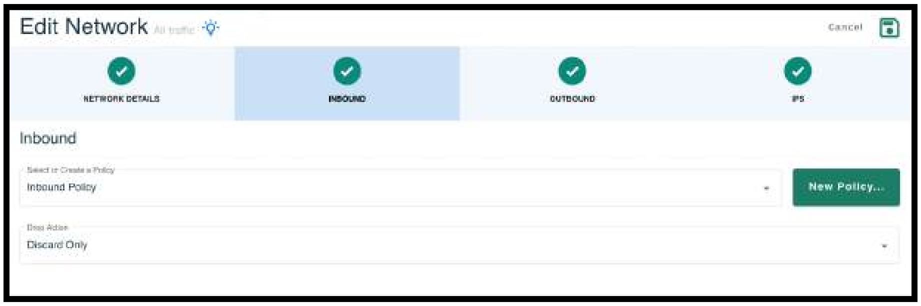
Name: Inbound Traffic

Description

Enforcers: HQ Enforcer

Directions: Inbound

    - Edit Direction (Inbound/Outbound) –
        - Select this step(s) to update the Policy and/or Drop Action
        - If no other Network edits are desired, click the Save button in the top right corner
        - If additional edits are needed, select the applicable step

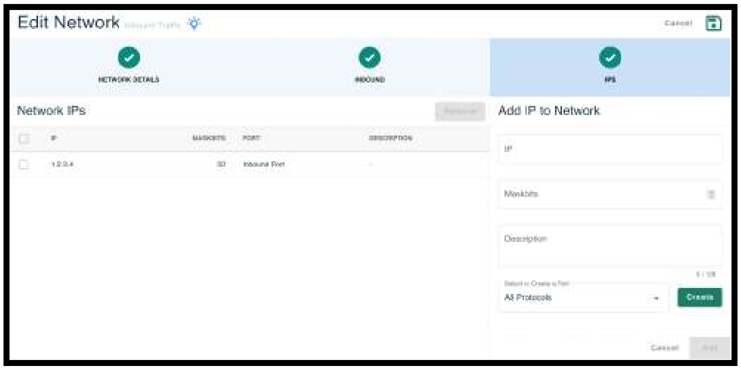


Inbound

Select or Create a Policy: Inbound Policy

Drop Action: Discard Only

    - IPs –
        - Select this step to add or remove IPs
        - Refer to the IPs section above for guidance
        - If no other Network edits are desired, click the Save button in the top right corner



Network IPs

IP	MASKBITS	PORT	DESCRIPTION
1.2.3.4	32	Inbound Port	-

Add IP to Network

IP

Maskbits

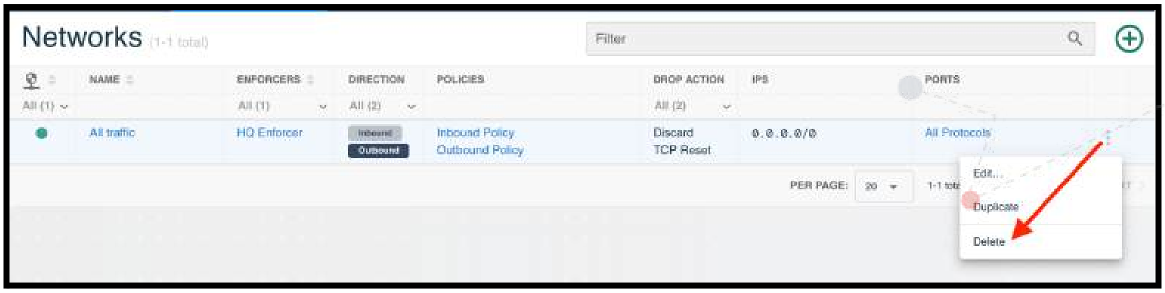
Description

Select or Create a Port: All Protocols

Deleting a Network

To delete a Network:

- Find the Network in the table and from the the ellipsis menu, select Delete



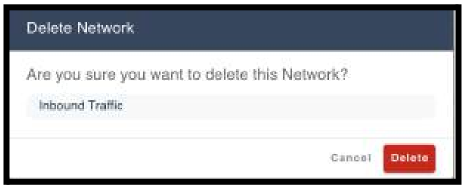
Networks (1-1 total)

Filter

	NAME	ENFORCERS	DIRECTION	POLICIES	DROP ACTION	IPS	PORTS
All (1)		All (1)	All (2)		All (2)		
●	All traffic	HQ Enforcer	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols

PER PAGE: 20 1-1 total

- On the confirmation modal, click Delete



Delete Network

Are you sure you want to delete this Network?

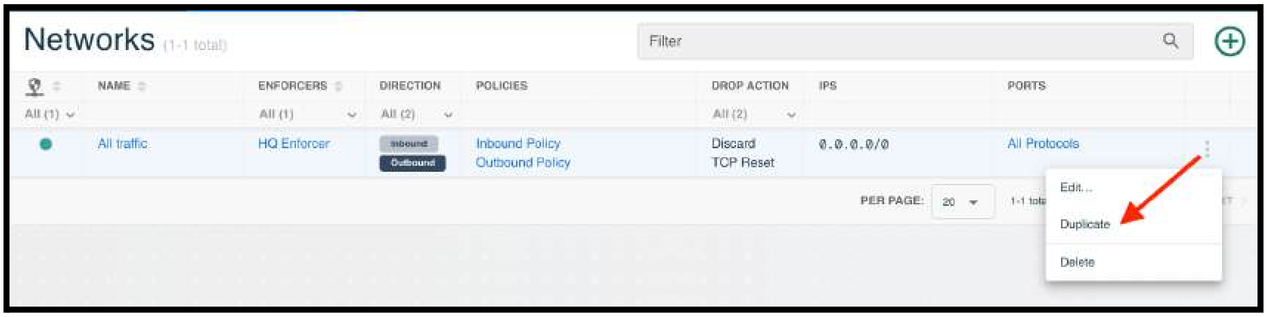
Inbound Traffic

The Network is now deleted.

Network Duplication

To create a new network, based on an existing one, you can utilize the network duplication feature. To duplicate a Network:

- From the ellipsis in the far-right corner of the table of the network you would like to duplicate, select Duplicate



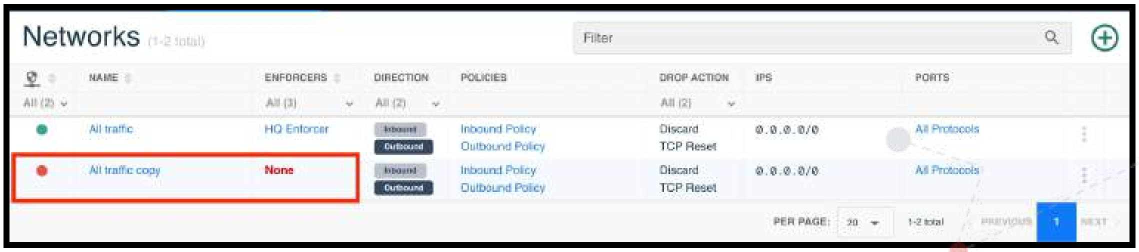
Networks (1-1 total)

Filter

	NAME	ENFORCERS	DIRECTION	POLICIES	DROP ACTION	IPS	PORTS
All (1)		All (1)	All (2)		All (2)		
●	All traffic	HQ Enforcer	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols

PER PAGE: 20 1-1 total

A copy of the network will be created with the word “copy” appended to the network name (this field can be edited to the desired network name). The network will not be assigned to any Enforcers until done so by editing the Network and manually applying the Enforcer(s) to the network.



Networks (1-2 total)

●	NAME	ENFORCERS	DIRECTION	POLICIES	DROP ACTION	IPS	PORTS
All (2)		All (3)	All (2)		All (2)		
●	All traffic	HQ Enforcer	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols
●	All traffic copy	None	Inbound Outbound	Inbound Policy Outbound Policy	Discard TCP Reset	0.0.0.0/0	All Protocols

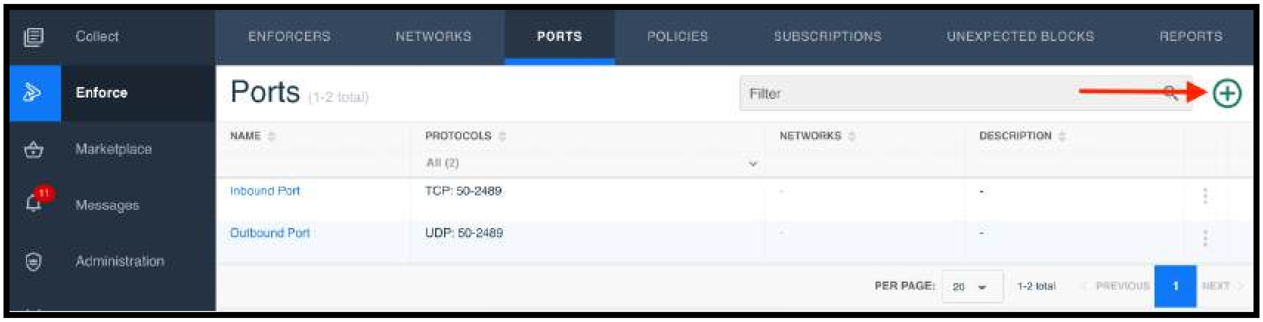
Ports

Ports define the protocols for a given Port and can be used across multiple Networks for allowing or blocking defined Ports.

Adding Ports

To add a Port:

- Navigate to Enforce in the left-hand navigation menu
- Click the Ports tab
- Click on the "+" button in the top right corner of the table

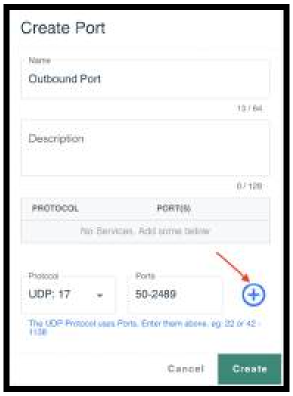


Ports (1-2 total)

NAME	PROTOCOLS All (2)	NETWORKS	DESCRIPTION
Inbound Port	TCP: 50-2489	-	-
Outbound Port	UDP: 50-2489	-	-

PER PAGE: 20   1-2 total   PREVIOUS 1 NEXT

- Provide the following (* indicates required field):
    - *Name
    - Description (optional)
    - *Protocol
        - "All: 256" is the default selection, but another protocol can be selected from the drop-down
            - You will be required to provide a Port or Port Range for some protocols, such as TCP and UDP
        - Click on the "+" button to add the Protocol to the Port



Create Port

Name: Outbound Port

13 / 64

Description

0 / 128

PROTOCOL	PORT(S)
No Services. Add some below	

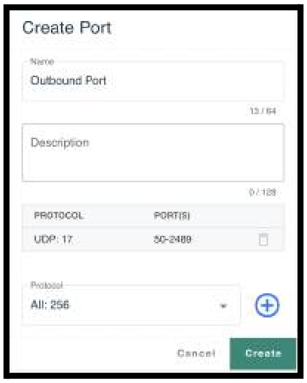
Protocol: UDP: 17

Ports: 50-2489

The UDP Protocol uses Ports. Enter them above. eg: 22 or 42 - 1138

        - Add any additional Protocols to the Port, as necessary

    - Click the Create button to create the Port



Create Port

Name: Outbound Port

13 / 64

Description

0 / 128

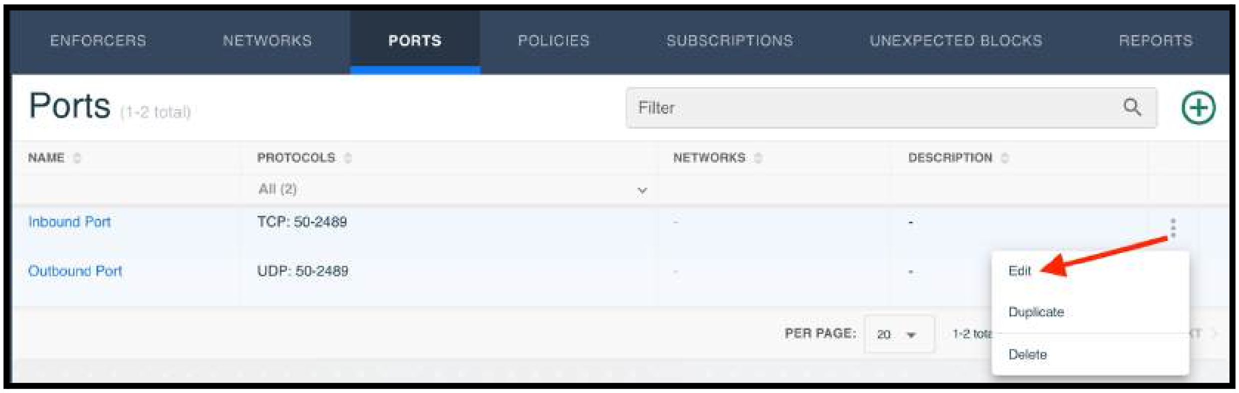
PROTOCOL	PORT(S)
UDP: 17	50-2489

Protocol: All: 256

Editing Ports

To edit a Port:

- Find the Port in the table and from the the ellipsis menu, select Edit

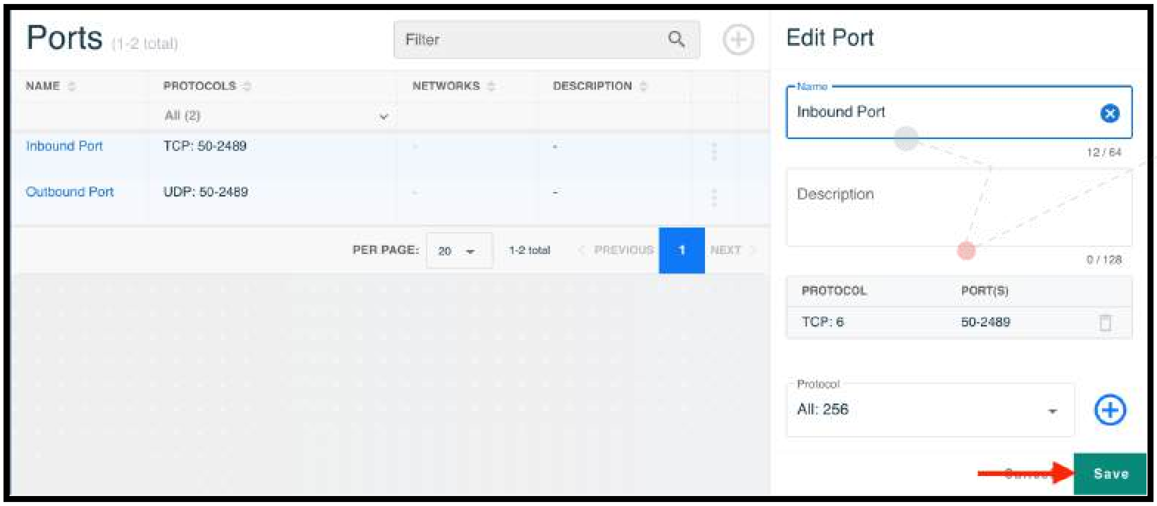


Ports (1-2 total)

NAME	PROTOCOLS	NETWORKS	DESCRIPTION
	All (2)		
Inbound Port	TCP: 50-2489	-	-
Outbound Port	UDP: 50-2489	-	-

PER PAGE: 20   1-2 total

- Make the necessary changes and click the Save button



Ports (1-2 total)

NAME	PROTOCOLS	NETWORKS	DESCRIPTION
	All (2)		
Inbound Port	TCP: 50-2489	-	-
Outbound Port	UDP: 50-2489	-	-

PER PAGE: 20 1-2 total

Edit Port

Name: Inbound Port 12 / 64

Description 0 / 128

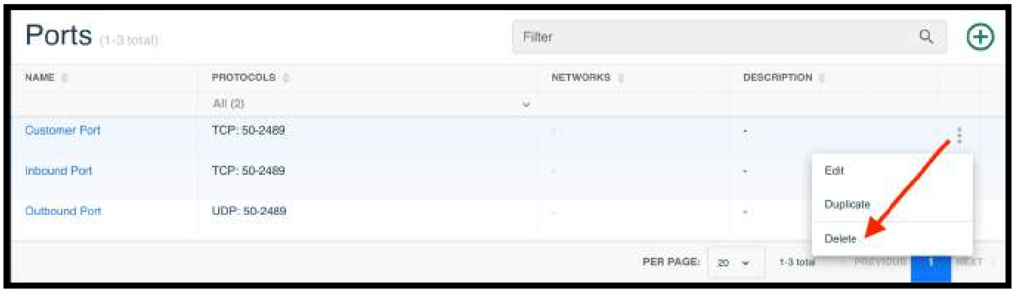
PROTOCOL	PORT(S)
TCP: 6	50-2489

Protocol: All: 256

Deleting Ports

To delete a Port:

- Find the Port in the table and from the the ellipsis menu, select Delete

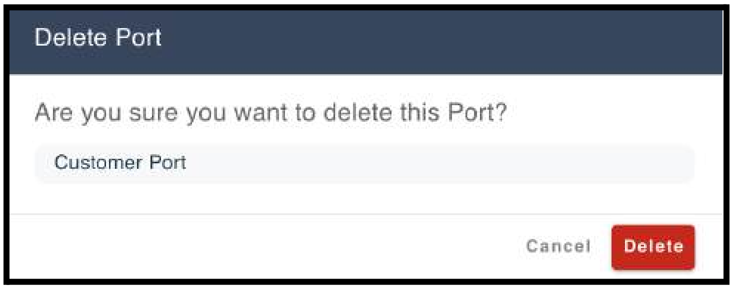


Ports (1-3 total)

NAME	PROTOCOLS	NETWORKS	DESCRIPTION
	All (2)		
Customer Port	TCP: 50-2489	-	-
Inbound Port	TCP: 50-2489	-	-
Outbound Port	UDP: 50-2489	-	-

PER PAGE: 20 1-3 total

- On the confirmation modal, click the Delete button



Delete Port

Are you sure you want to delete this Port?

Customer Port

The Port is now deleted.

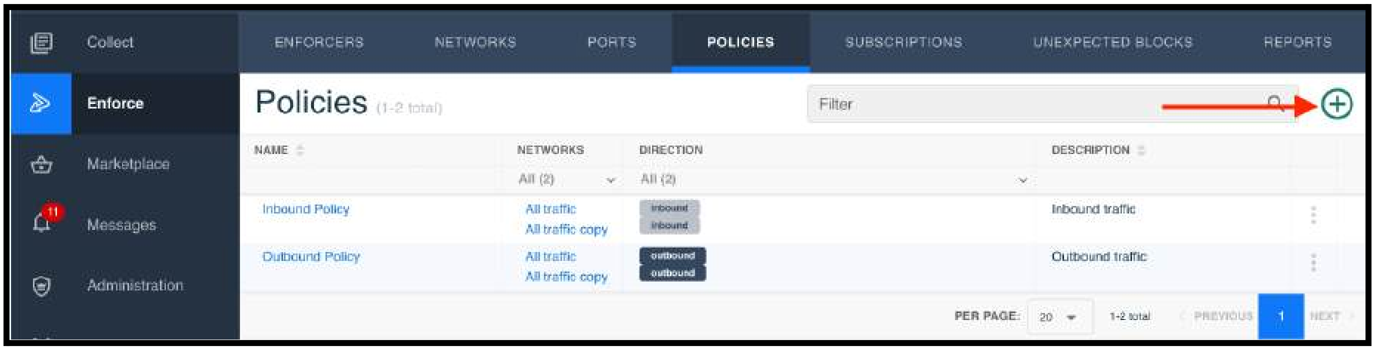
Policies

Policies allow users to determine what is or is not allowed through specific networks or network segments. As there are no limits to the number of policies that can be created, users can create as many or as few policies as they need to protect each of their networks as they deem necessary.

Create a Policy

To create a Policy:

- Navigate to Enforce in the left-hand navigation menu
- Click on the Policies tab
- Click the "+" button the top-right corner of the table



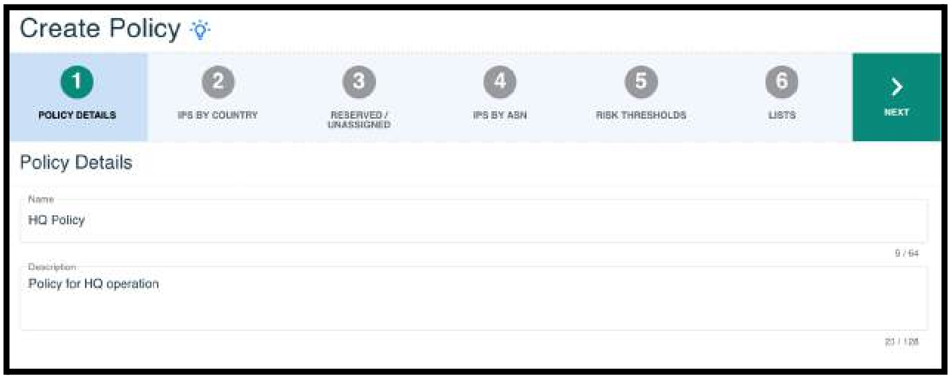
Policies (1-2 total)

NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

PER PAGE: 20 1-2 total PREVIOUS 1 NEXT

Policy Details

Enter a name (required) and optional description for the Policy, then click the Next button.



Policy Details

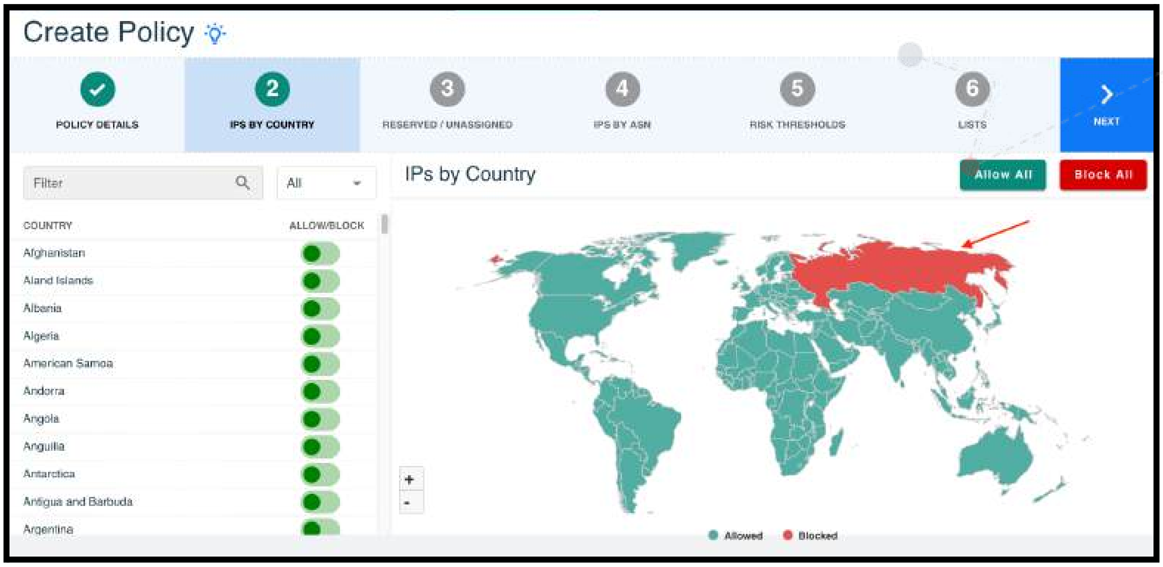
Name
HQ Policy
9 / 64

Description
Policy for HQ operation
23 / 128

IPs by Country

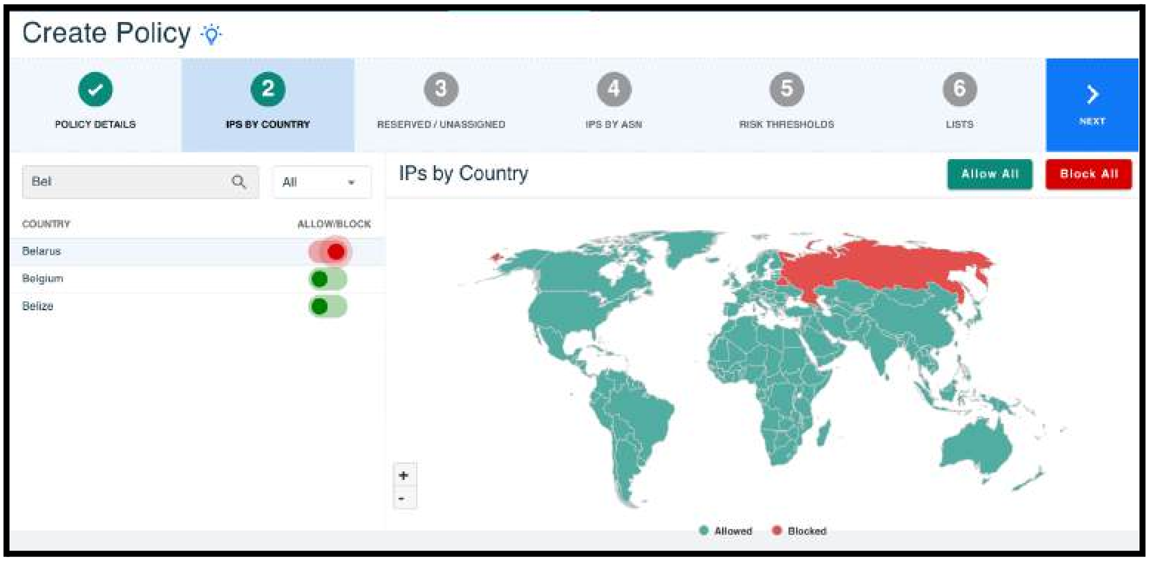
By default, IPs from all countries are allowed. Traffic can be blocked from specific countries one of two ways:

- Option 1 – Click on a country in the map to change it to the block setting (country will now be red)



COUNTRY	ALLOW/BLOCK
Afghanistan	🟢
Aland Islands	🟢
Albania	🟢
Algeria	🟢
American Samoa	🟢
Andorra	🟢
Angola	🟢
Anguilla	🟢
Antarctica	🟢
Antigua and Barbuda	🟢
Argentina	🟢

- Option 2 – Search for the country in the Filter box and then move the toggle to the Block state



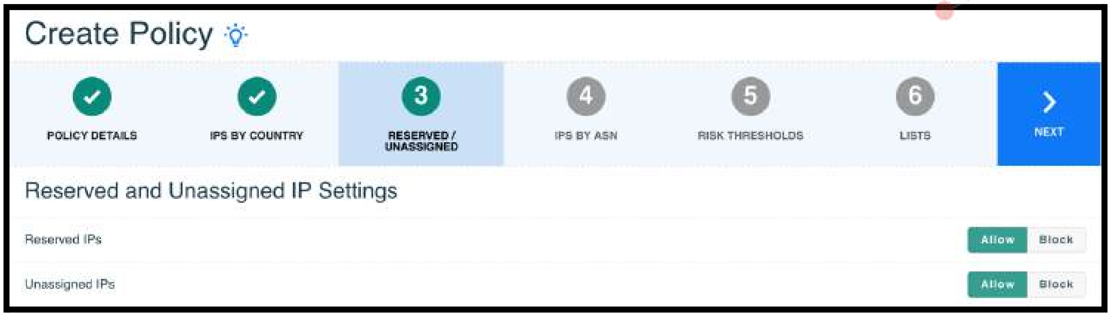
Bel

COUNTRY	ALLOW/BLOCK
Belarus	🔴
Belgium	🟢
Belize	🟢

- Alternatively, you could select ‘Block All’ and start selectively allowing individual countries. This can be a great way to geo-block most of the world except the areas in which you do business.
- Once all IPs by Country settings are complete, click the Next button

Reserved and Unassigned IPs

Reserved and Unassigned IPs are allowed, by default, to help prevent internal IPs from being blocked. To block either, select the Block button(s) and then click Next.



Reserved and Unassigned IP Settings

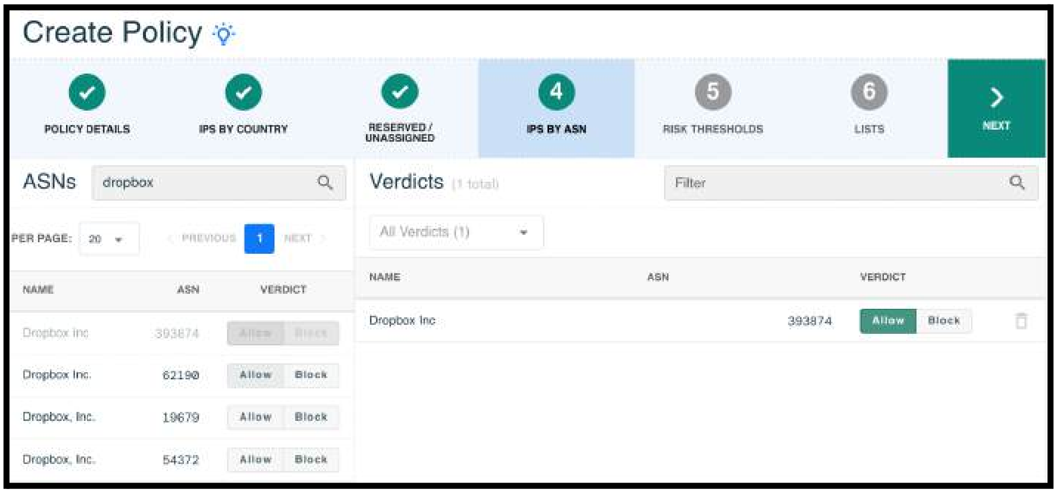
Reserved IPs	Allow Block
Unassigned IPs	Allow Block

IPS by ASN

Traffic can be allowed or blocked from a single autonomous system number (ASN). This can be a useful feature when you are relying on large-scale geo-blocking, but find the need to allow one or more ASNs in a given country while maintaining blocks on all other activity associated with that country. Similarly, it can be a great way to quickly block all activity to and from ASNs that have been compromised or are being heavily used by malicious actors.

To add an ASN to your policy:

- In the left-hand panel, search by ASN Name or ASN Number
- Click on the verdict you want to apply to that ASN (Allow or Block) to add it to the right-hand panel



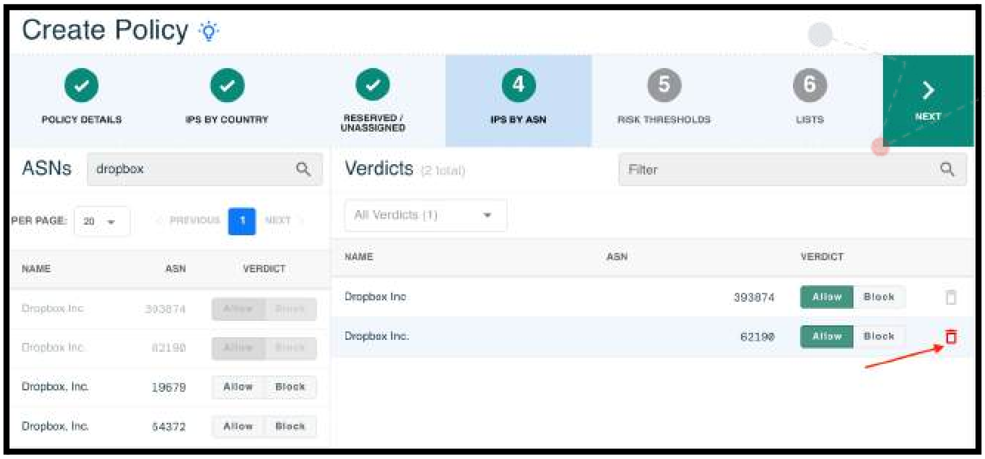
ASNs: dropbox

NAME	ASN	VERDICT
Dropbox Inc	393874	Allow Block
Dropbox Inc.	62190	Allow Block
Dropbox, Inc.	19679	Allow Block
Dropbox, Inc.	54372	Allow Block

NAME	ASN	VERDICT
Dropbox Inc	393874	Allow Block

- Repeat for any other ASNs you want to add

To remove an ASN click on the trash icon in the row of the ASN.



ASNs

NAME	ASN	VERDICT
Dropbox Inc	393874	Allow Block
Dropbox Inc	62190	Allow Block
Dropbox, Inc.	19679	Allow Block
Dropbox, Inc.	54372	Allow Block

Verdicts (2 total)

NAME	ASN	VERDICT
Dropbox Inc	393874	Allow Block
Dropbox Inc.	62190	Allow Block

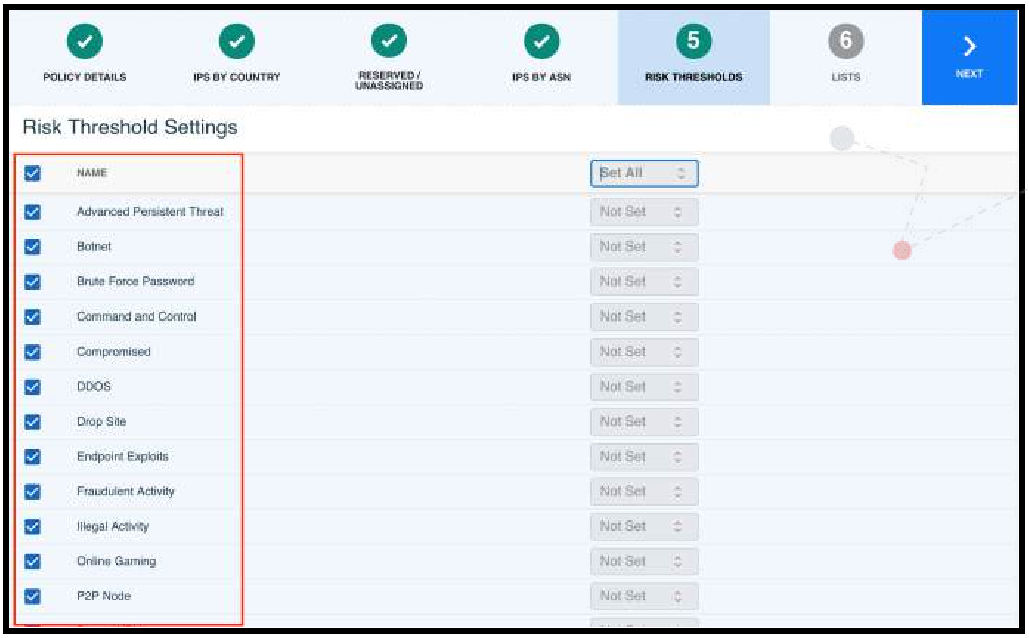
- Click the Next button when all desired IPs by ASNs verdicts are applied

Risk Thresholds

There are many threat categories that can be enabled. All IPs included in the threat lists are placed in one or more of these categories. Each IP in the threat intelligence also has an associated score that can range from 1 to 100, with a higher score representing a higher confidence of it being malicious, as rated by our feed partners. Enabling categories and setting Risk Thresholds allows you to control how strong of a policy you want to apply. Since the Risk Threshold setting indicates confidence in malicious activity, the lower this is set, more traffic will be blocked.

As an example, if the Command and Control category is enabled with a threshold of 90, any IP identified as a Command and Control with a score of 90 or above will be blocked. If the Command and Control category was not enabled, the connection would be allowed through by the threat list, but could still be blocked by other categories (since an IP or domain can appear in multiple categories), Block lists, IPs by Country policy, and so on.

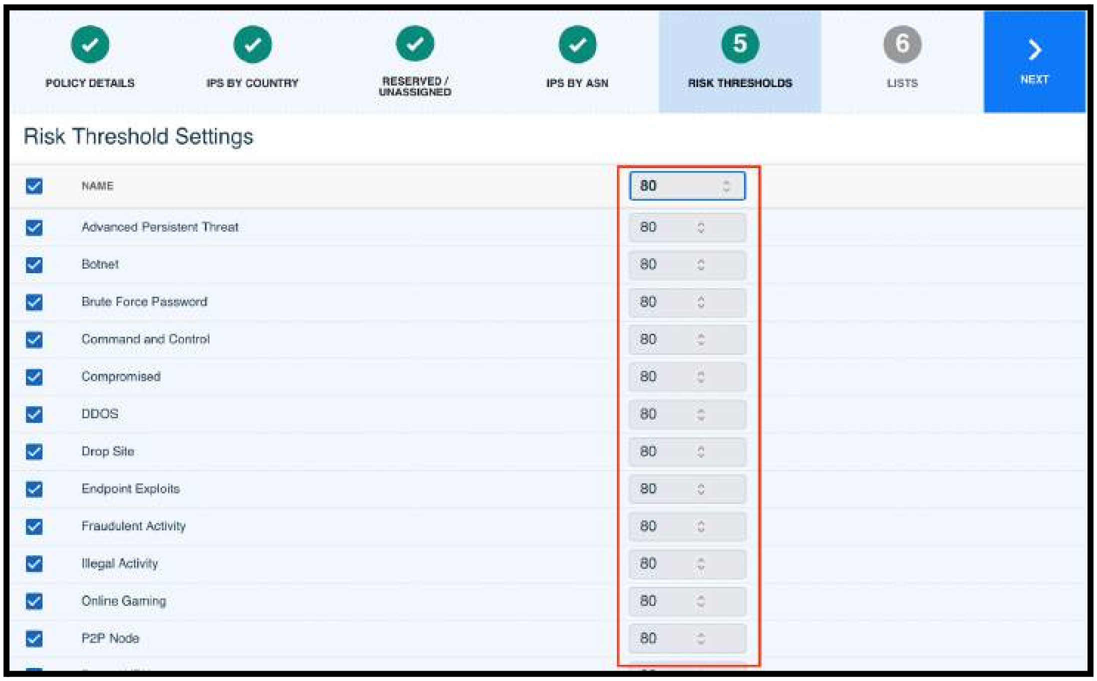
To enable a category, select the checkbox to the left of the desired category. To enable all categories, select the checkbox at the top of the column. As a matter of best-practice, we strongly recommend enabling all categories.



Risk Threshold Settings

☑ NAME	Set All
☑ Advanced Persistent Threat	Not Set
☑ Botnet	Not Set
☑ Brute Force Password	Not Set
☑ Command and Control	Not Set
☑ Compromised	Not Set
☑ DDOS	Not Set
☑ Drop Site	Not Set
☑ Endpoint Exploits	Not Set
☑ Fraudulent Activity	Not Set
☑ Illegal Activity	Not Set
☑ Online Gaming	Not Set
☑ P2P Node	Not Set

To set a Risk Threshold for a category, enter a value between 1 and 100 in the text field to the right of the category. To apply the same Risk Threshold to all categories, enter your value in the text field at the top of the column.



Risk Threshold Settings

☑ NAME	80
☑ Advanced Persistent Threat	80
☑ Botnet	80
☑ Brute Force Password	80
☑ Command and Control	80
☑ Compromised	80
☑ DDOS	80
☑ Drop Site	80
☑ Endpoint Exploits	80
☑ Fraudulent Activity	80
☑ Illegal Activity	80
☑ Online Gaming	80
☑ P2P Node	80

Once all settings have been applied, click the Next button.

Best Practice Recommendation for Risk Thresholds:

We recommend a value of 80 for customers who want to be aggressive (more will be blocked), and 90 for those who want to be more conservative (less will be blocked). If you need to block more IPs in a certain category, lower the score in that category. If you want to block fewer IPs in a certain category, raise the score in that category.

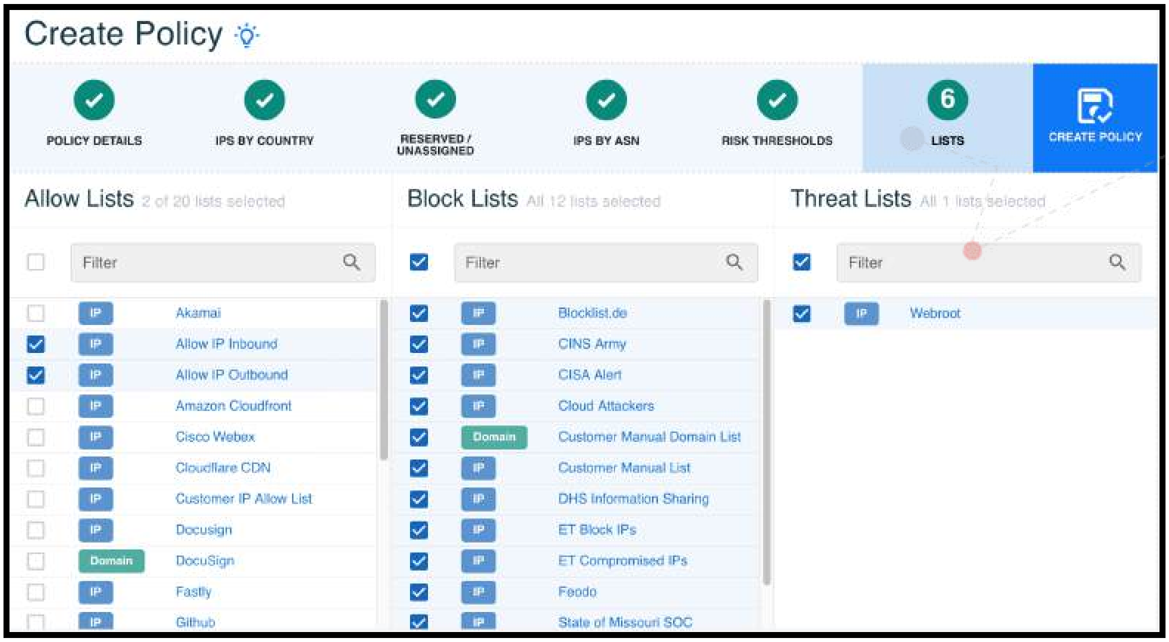
For example, if you're hearing that many legitimate sites or services are being blocked, and upon correlating with your logs find that they are being marked as spam with a score of 90-94, you can raise the threshold for the Spam category to 95. Now, you will see fewer unexpected blocks based on Spam.

On the other hand, if you are checking your logs and seeing many unidentifiable Endpoint Exploits are getting through with a score of 85-89, you can lower the score to 85. Now, you will see more blocks based on Endpoint Exploits.

Lists

Users can enable Allow, Block, and Threat Lists per policy, which specifies the IPs and/or domains that should be allowed or blocked on the policy. **Allowed, Blocked, and Threat Lists do not influence traffic until enabled on a Policy.**

To include a List as part of your policy, search for the List(s) (you can utilize the Filter at the top of each panel) and then select the checkbox next to each desired List.



Allow Lists 2 of 20 lists selected

□ Filter

□	IP	Akamai
☑	IP	Allow IP Inbound
☑	IP	Allow IP Outbound
□	IP	Amazon Cloudfront
□	IP	Cisco Webex
□	IP	Cloudflare CDN
□	IP	Customer IP Allow List
□	IP	Docusign
□	Domain	DocuSign
□	IP	Fastly
□	IP	Github

Block Lists All 12 lists selected

☑ Filter

☑	IP	Blocklist.de
☑	IP	CINS Army
☑	IP	CISA Alert
☑	IP	Cloud Attackers
☑	Domain	Customer Manual Domain List
☑	IP	Customer Manual List
☑	IP	DHS Information Sharing
☑	IP	ET Block IPs
☑	IP	ET Compromised IPs
☑	IP	Feodo
☑	IP	State of Missouri SOC

Threat Lists All 1 lists selected

☑ Filter

☑	IP	Webroot

Once all desired Lists have been selected, click the “Create Policy” button.

Best Practice Recommendation for Lists:

We recommend the following:

- Allow Lists – Enable only the lists/services you want allowed for the specific policy. Generally these would be services that your business is reliant on. **We strongly recommend that you always enable the threatER Curated DNS and threatER SaaS lists, especially for outbound policies, to ensure that your environment never loses connectivity to critical threatER resources.**
- Block Lists – Enable all Block Lists, except for Zoom, which can be enabled at your discretion.

Creating an Allow All Policy

Allow All policies can be used as a "break glass" policy in cases where a business critical site or service must be accessed, but is being blocked. By using an Allow All policy, all traffic is allowed through the Enforcer and continues to be logged for review. We recommend using this policy instead of putting the device into bypass mode if you don't know whether or not the threatER platform is blocking this traffic, so that logging is maintained. In bypass mode, no traffic is logged.

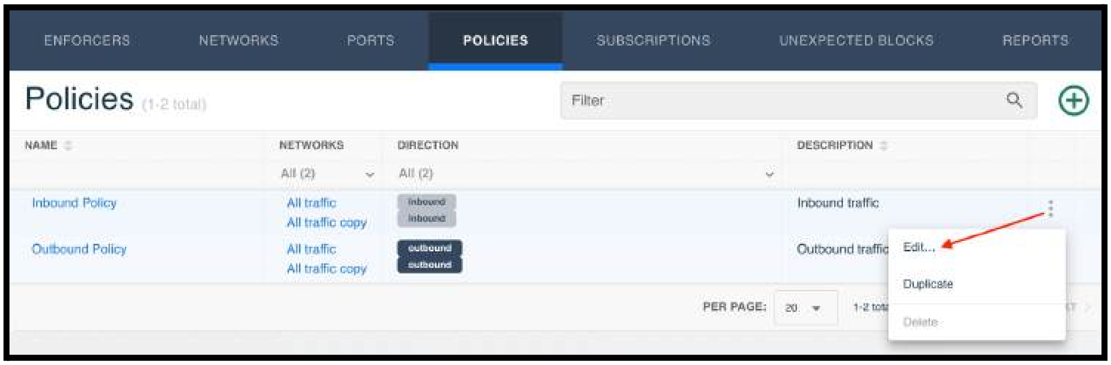
To create an Allow All policy, apply the following configurations on each step:

- **IP by Country:** Allow All
- **Reserved and Unassigned IPs:** Allow both
- **Risk Thresholds:** Disable (uncheck) all categories
- **Lists:** Disable (uncheck) all Block & Threat lists

Edit a Policy

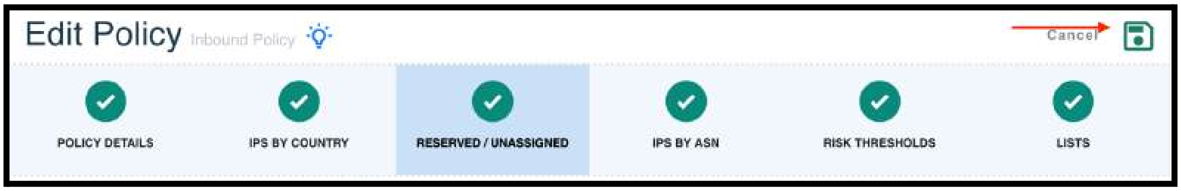
To edit configurations of an existing policy:

- Find the Policy that needs configuration edits in the table and from the ellipsis menu in the row of the policy, select Edit



NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

- Click on the Policy step that needs adjustments and make the necessary edits
- Click on any other steps that needs adjustments and make those edits
- After you have completed all desired edits, click the Save button to enact all policy edits. Your changes will temporarily save step to step within the wizard, but will be lost unless you click the Save button.



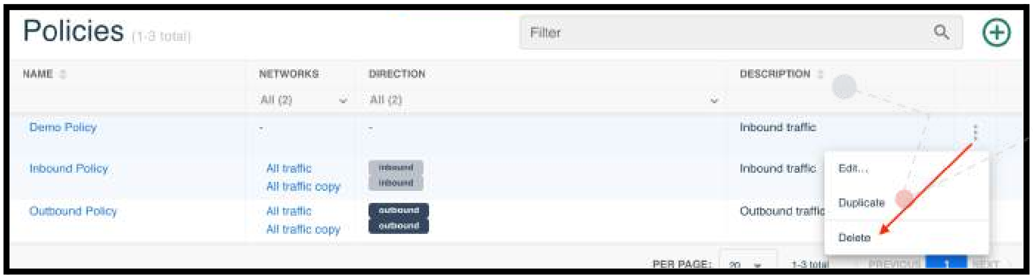
Delete a Policy

A Policy can only be deleted if there are no Networks utilizing that policy.

To delete a Policy with no Networks assigned to it:

- Find the Policy in the table

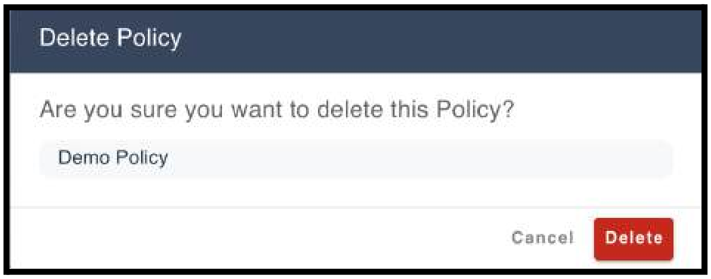
- From the ellipsis menu in the row of the policy, select Delete



Policies (1-3 total)

NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Demo Policy	-	-	Inbound traffic
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

- On the confirmation modal, click Delete



Delete Policy

Are you sure you want to delete this Policy?

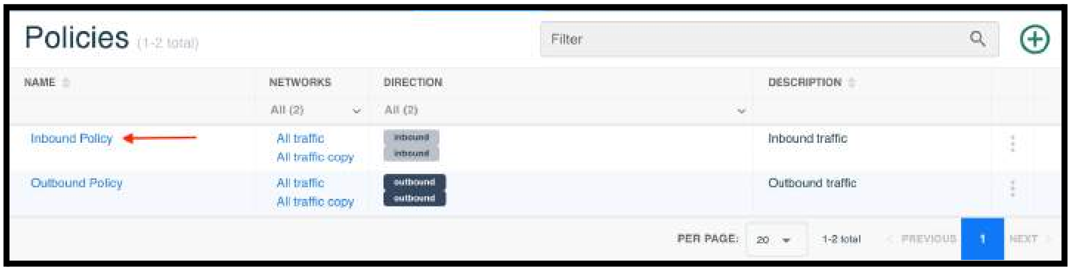
Demo Policy

To delete a policy that is being utilized by a Network, you will need to edit the Network the policy is assigned to and remove the policy from it.

Policy Overview

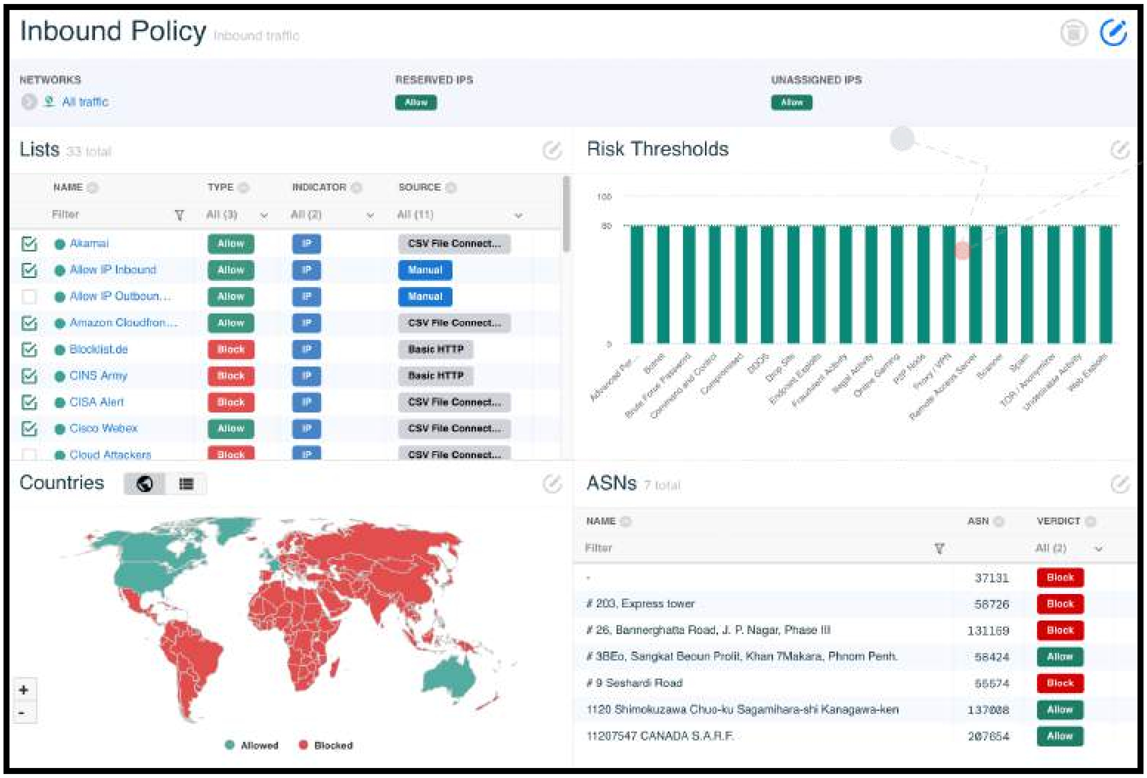
To view the details of a policy on one screen:

- Click on the hyperlink of a Policy Name



Policies (1-2 total)

NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic



Inbound Policy Inbound traffic

NETWORKS	RESERVED IPS	UNASSIGNED IPS
All traffic	Allow	Allow

Lists 33 total

	NAME	TYPE	INDICATOR	SOURCE
	Filter	All (3)	All (2)	All (11)
☑	Akamai	Allow	IP	CSV File Connect...
☑	Allow IP Inbound	Allow	IP	Manual
□	Allow IP Outboun...	Allow	IP	Manual
☑	Amazon Cloudfron...	Allow	IP	CSV File Connect...
☑	Blocklist.de	Block	IP	Basic HTTP
☑	CINS Army	Block	IP	Basic HTTP
☑	CISA Alert	Block	IP	CSV File Connect...
☑	Cisco Webex	Allow	IP	CSV File Connect...
□	Cloud Attackers	Block	IP	CSV File Connect...

Risk Thresholds

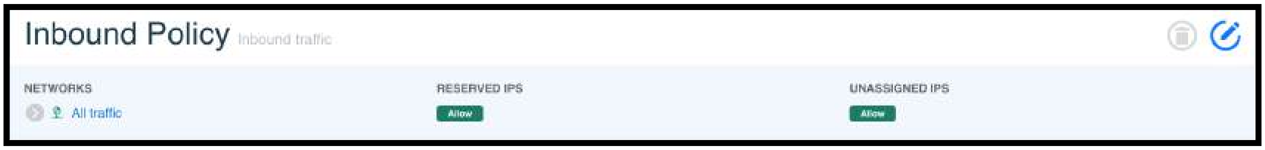
Countries

ASNs 7 total

NAME	ASN	VERDICT
Filter		All (2)
-	37131	Block
# 203, Express tower	58726	Block
# 26, Bannerghatta Road, J. P. Nagar, Phase III	131169	Block
# 3BEo, Sangkat Beoun Proll, Khan 7Makara, Phnom Penh.	58424	Allow
# 9 Seshardi Road	55574	Block
1120 Shimokuzawa Chuo-ku Sagamihara-shi Kanagawa-ken	137008	Allow
11207547 CANADA S.A.R.F.	207654	Allow

The top panel will display:

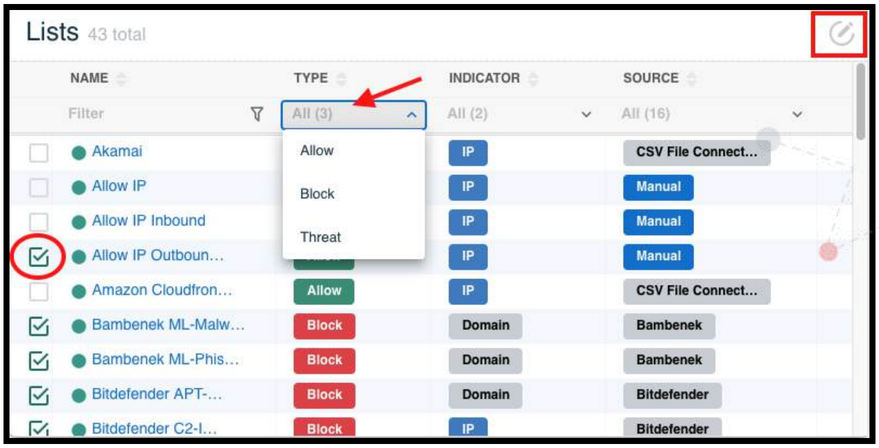
- Policy Name
- Network(s) the policy is assigned to
- Reserved and Unassigned IPs settings
- Policy Description



Inbound Policy Inbound traffic

NETWORKS	RESERVED IPS	UNASSIGNED IPS
All traffic	Allow	Allow

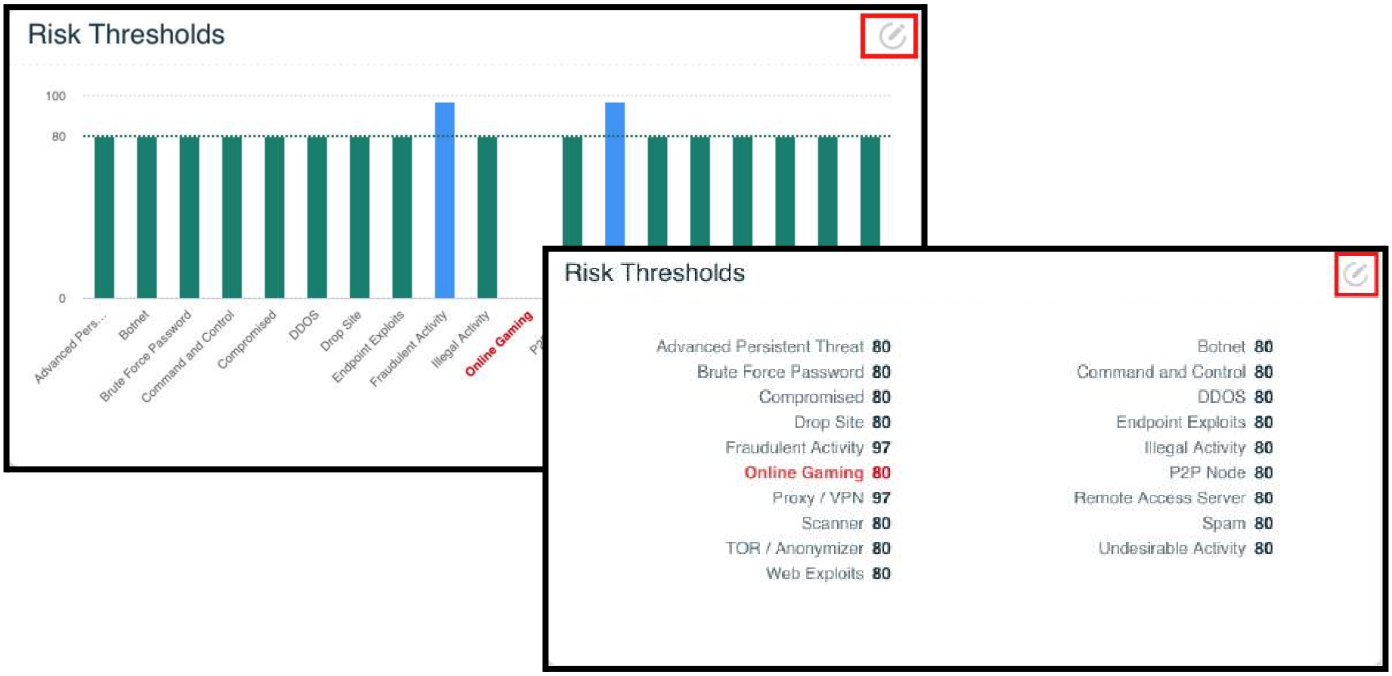
The Lists panel displays all lists available to your company. The left column will display a green checkbox if the list is enabled on the policy. You can narrow down the results via the filters available in each column. Clicking the Edit button in the top-right corner will allow you to add or remove Lists to/from the policy.



Lists 43 total

	NAME	TYPE	INDICATOR	SOURCE
	Filter	All (3)	All (2)	All (16)
☐	Akamai		IP	CSV File Connect...
☐	Allow IP		IP	Manual
☐	Allow IP Inbound		IP	Manual
☑	Allow IP Outboun...		IP	Manual
☐	Amazon Cloudfron...	Allow	IP	CSV File Connect...
☑	Bambenek ML-Malw...	Block	Domain	Bambenek
☑	Bambenek ML-Phis...	Block	Domain	Bambenek
☑	Bitdefender APT-...	Block	Domain	Bitdefender
☑	Bitdefender C2-I...	Block	IP	Bitdefender

The Risk Thresholds panel displays the current settings applied on the policy. Categories set to threatER's security best practice of "80" will display a green bar. Anything above or below that will display a blue bar. If a Category is NOT enabled on the policy, a bar will not display and the Category name will display in red. Click on the graph to view a list of the Category settings. If edits need to be made, click on the pencil icon in the top-right corner.

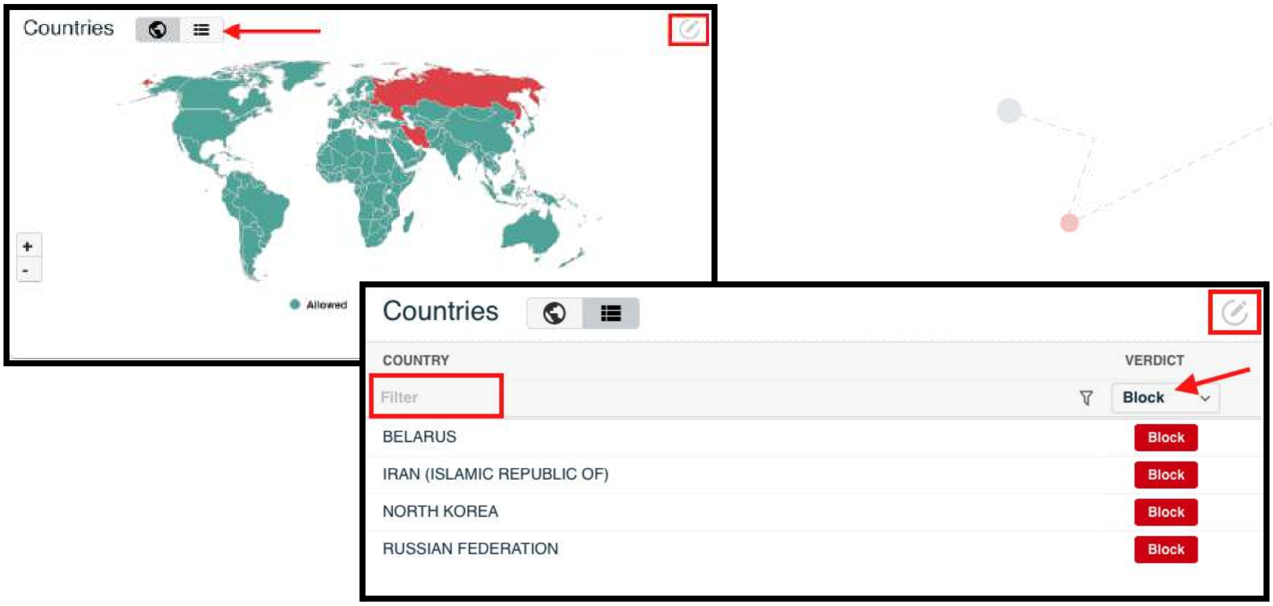


Risk Thresholds

Risk Thresholds

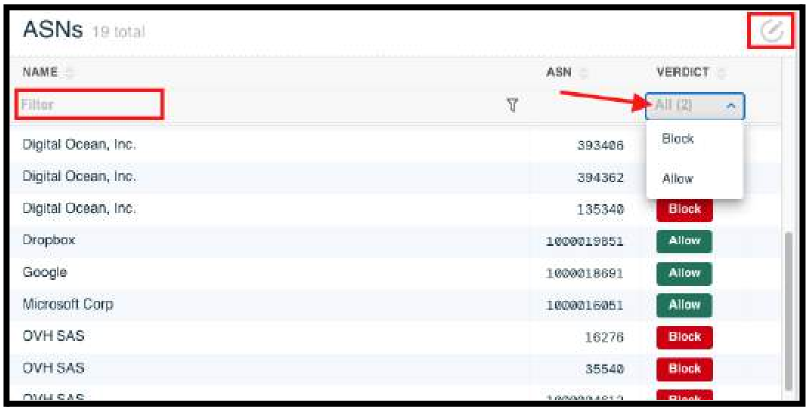
Advanced Persistent Threat	80	Botnet	80
Brute Force Password	80	Command and Control	80
Compromised	80	DDOS	80
Drop Site	80	Endpoint Exploits	80
Fraudulent Activity	97	Illegal Activity	80
Online Gaming	80	P2P Node	80
Proxy / VPN	97	Remote Access Server	80
Scanner	80	Spam	80
TOR / Anonymizer	80	Undesirable Activity	80
Web Exploits	80		

The Countries panel displays, by default, the map view of which countries are blocked and allowed. To view a list of the country settings, click on the list icon up top, or click on the map. To edit which countries you are blocking or allowed, click on the pencil icon in the top right corner.



COUNTRY	VERDICT
Filter	Block
BELARUS	Block
IRAN (ISLAMIC REPUBLIC OF)	Block
NORTH KOREA	Block
RUSSIAN FEDERATION	Block

The ASNs panel displays the ASNs explicitly blocked and allowed on the policy. You can filter down by ASN Name and Number, or by Verdict. To make any edits, click the pencil icon in the top right corner.

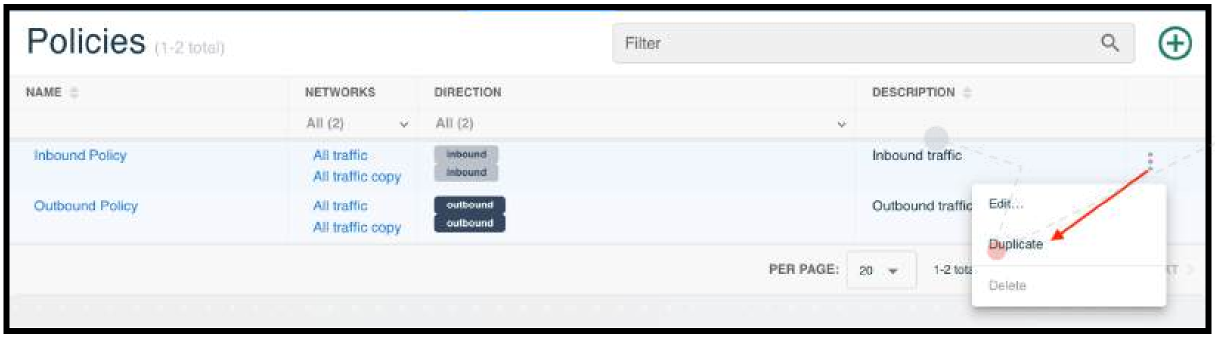

ASNs 19 total

NAME	ASN	VERDICT
Filter		All (2)
Digital Ocean, Inc.	393406	
Digital Ocean, Inc.	394362	
Digital Ocean, Inc.	135340	Block
Dropbox	1000019851	Allow
Google	1000018691	Allow
Microsoft Corp	1000016051	Allow
OVH SAS	16276	Block
OVH SAS	35540	Block

Policy Duplication

An existing policy can be duplicated by taking the following actions:

- From the ellipsis in the far-right corner of the table of the policy you would like to duplicate, select Duplicate



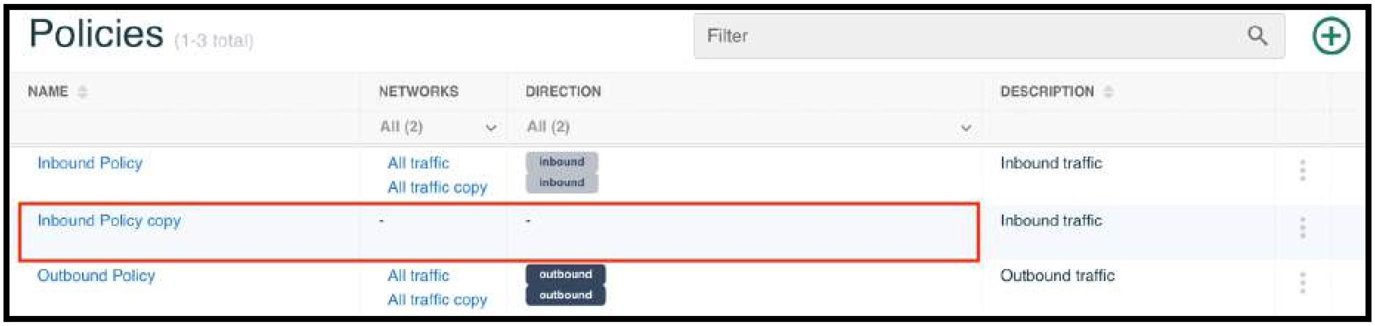
Policies (1-2 total)

Filter

NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

PER PAGE: 20 1-2 total

A copy of the policy will be created with the word “copy” appended to the policy name (this field can be edited to the desired policy name). The policy will not be assigned to any networks at the time of duplication. To assign a policy to a network, navigate to the networks tab and assign the policy to the desired network(s).



Policies (1-3 total)

Filter

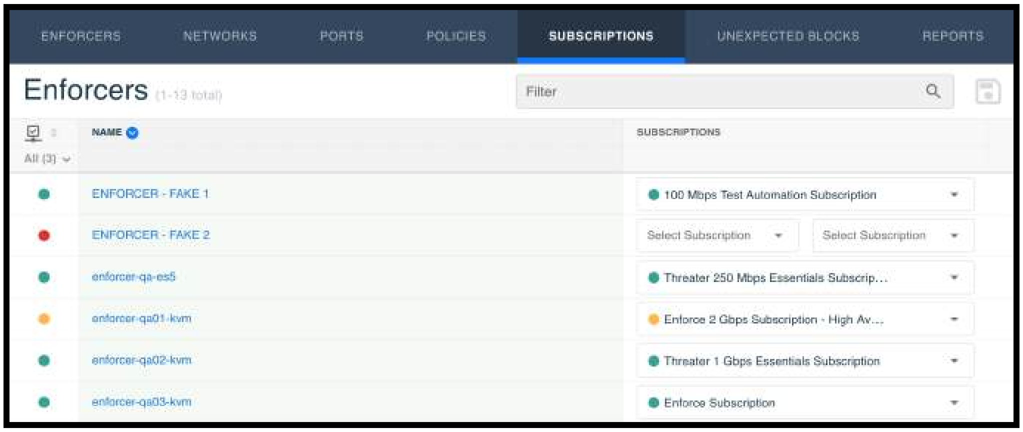
NAME	NETWORKS	DIRECTION	DESCRIPTION
	All (2)	All (2)	
Inbound Policy	All traffic All traffic copy	inbound inbound	Inbound traffic
Inbound Policy copy	-	-	Inbound traffic
Outbound Policy	All traffic All traffic copy	outbound outbound	Outbound traffic

Subscriptions

Enforcers log traffic, filter traffic, and receive updated threat intelligence with a supported subscription. Without a valid attached subscription, the Enforce software will blindly forward traffic in both directions with no filtering action and no logging. The Subscriptions tab can be used to assign subscriptions accordingly.

The following will display on this tab:

- Enforcers
    - Displayed in the left-hand column
    - Enforcer Statuses
        - Green – Enforcer is assigned an active subscription
        - Yellow – Enforcer is assigned a subscription that is no longer under active support; any Enforcer assigned a subscription in this state may not receive updated threat intelligence and as a result may be in an Allow-All state. You should contact our Customer Success team to review your subscription status.
        - Red – Enforcer does not have a subscription assigned to it; the Enforcer will not receive updated threat intelligence and will be in an Allow-All state
- Subscriptions
    - Displays the subscription assigned to the Enforcer

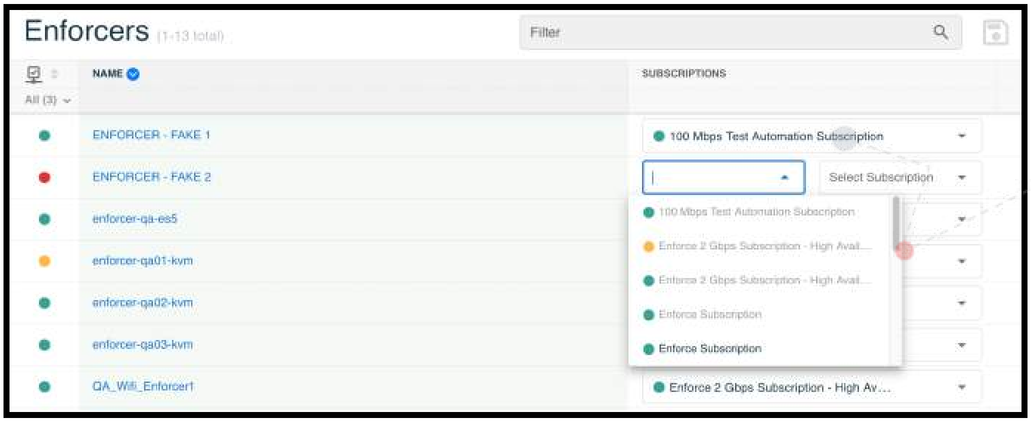


Enforcers (1-13 total)

All (3)	NAME	SUBSCRIPTIONS
🟢	ENFORCER - FAKE 1	🟢 100 Mbps Test Automation Subscription
🔴	ENFORCER - FAKE 2	Select Subscription Select Subscription
🟢	enforcer-qa-es5	🟢 Threater 250 Mbps Essentials Subscrip...
🟡	enforcer-qa01-kvm	🟡 Enforce 2 Gbps Subscription - High Av...
🟢	enforcer-qa02-kvm	🟢 Threater 1 Gbps Essentials Subscription
🟢	enforcer-qa03-kvm	🟢 Enforce Subscription

To assign a subscription to an Enforcer:

- Select the subscription from the drop-down

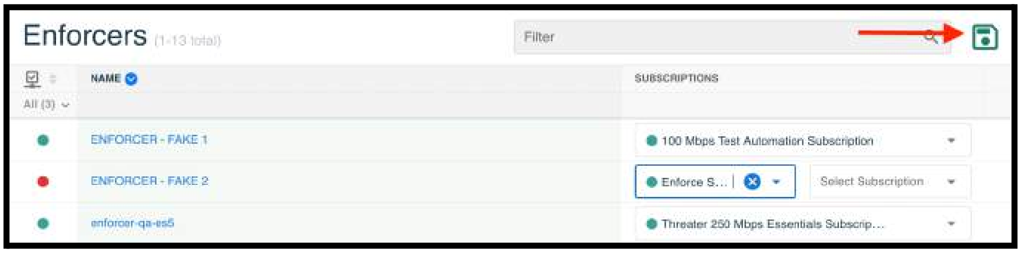


Enforcers (1-13 total)

NAME	SUBSCRIPTIONS
● ENFORCER - FAKE 1	● 100 Mbps Test Automation Subscription
● ENFORCER - FAKE 2	Select Subscription
● enforcer-qa-es5	
● enforcer-qa01-kvm	
● enforcer-qa02-kvm	
● enforcer-qa03-kvm	
● QA_Wifi_Enforcer1	● Enforce 2 Gbps Subscription - High Av…

- ● 100 Mbps Test Automation Subscription
- ● Enforce 2 Gbps Subscription - High Avail…
- ● Enforce 2 Gbps Subscription - High Avail…
- ● Enforce Subscription
- ● Enforce Subscription

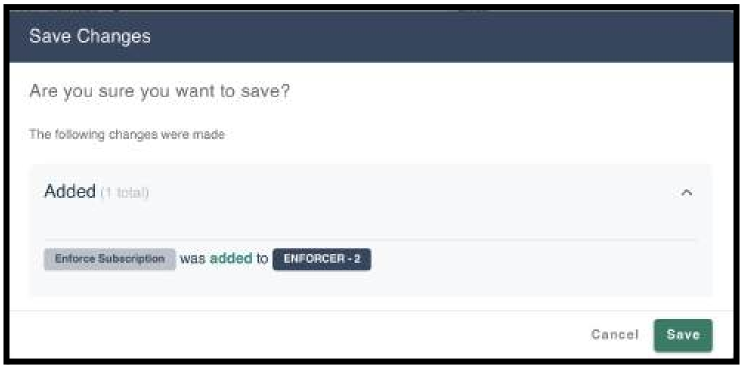
- Click the Save button



Enforcers (1-13 total)

NAME	SUBSCRIPTIONS
● ENFORCER - FAKE 1	● 100 Mbps Test Automation Subscription
● ENFORCER - FAKE 2	● Enforce S… ⊗ · Select Subscription
● enforcer-qa-es5	● Threater 250 Mbps Essentials Subscrip…

- On the Save Changes modal, review the selected changes that were made and then click the Save button



Save Changes

Are you sure you want to save?

The following changes were made

Added (1 total)

Enforce Subscription was added to ENFORCER - 2

Cancel Save

Unexpected Blocks

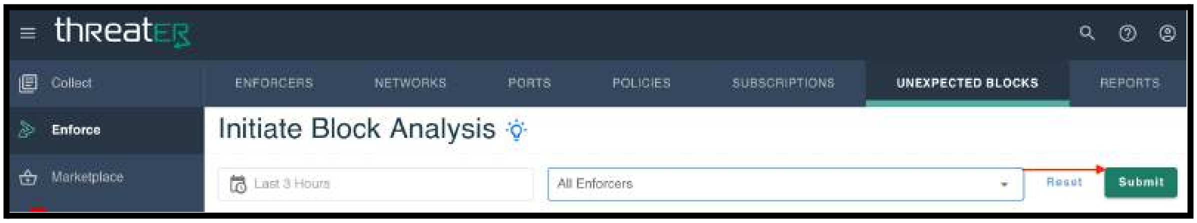
threatER's Unexpected Blocks feature allows you to retrieve outbound Port 80 and 443 traffic logs that your Enforcer(s) have blocked. These logs enable portal users to make an informed decision on whether to allow those IPs.

NOTE: *All Enforcers must be on Enforce Build 240 or greater to utilize the Unexpected Blocks feature, but it is recommended that you upgrade your Enforcers to Build 254 or greater for a more performant Unexpected Blocks experience.*

Block Events

To perform an analysis:

- Navigate to Enforce in the left-hand navigation menu
- Click 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
- Select a Date Range and the Enforcers you want to query logs on
  - Default selections are the last 3 hours and All Enforcers
- Click Submit

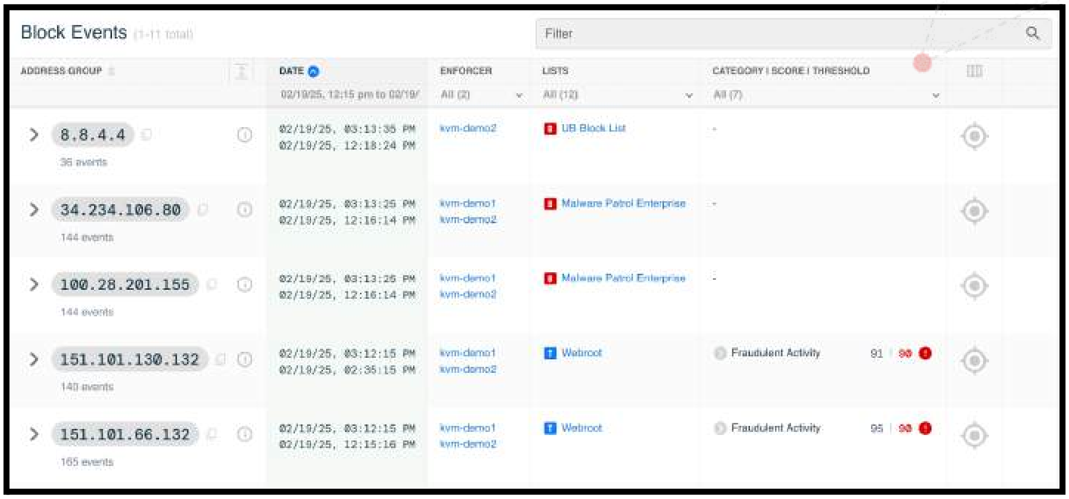


Last 3 Hours

All Enforcers

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. By default, duplicate IPs are consolidated into groups, and the resulting IP groups are listed in descending chronological order.



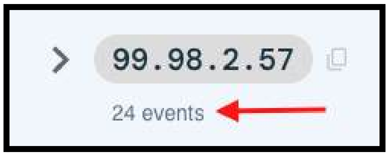
Block Events (1-11 total)

Filter

ADDRESS GROUP	DATE	ENFORCER	LISTS	CATEGORY | SCORE | THRESHOLD
	02/19/25, 12:15 pm to 02/19/	All (2)	All (12)	All (7)
8.8.4.4 36 events	02/19/25, 03:13:35 PM 02/19/25, 12:18:24 PM	kvm-demo2	UB Block List	-
34.234.106.80 144 events	02/19/25, 03:13:25 PM 02/19/25, 12:16:14 PM	kvm-demo1 kvm-demo2	Malware Patrol Enterprise	-
100.28.201.155 144 events	02/19/25, 03:13:25 PM 02/19/25, 12:16:14 PM	kvm-demo1 kvm-demo2	Malware Patrol Enterprise	-
151.101.130.132 140 events	02/19/25, 03:12:15 PM 02/19/25, 02:35:15 PM	kvm-demo1 kvm-demo2	Webroot	Fraudulent Activity 91 | 90
151.101.66.132 165 events	02/19/25, 03:12:15 PM 02/19/25, 12:15:16 PM	kvm-demo1 kvm-demo2	Webroot	Fraudulent Activity 95 | 90

The header row of the IP group will include:

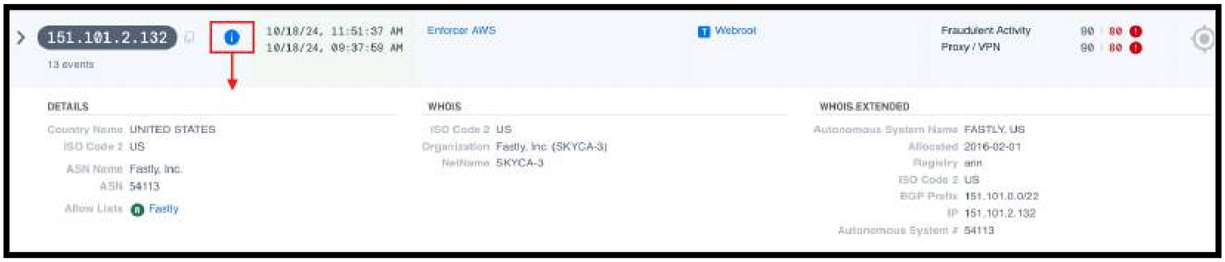
- Event count – The number of unique events returned for that IP in the log set



99.98.2.57

24 events

- Extended Info icon – Clicking on this icon will display any additional information that is available for the IP (i.e. Reverse DNS, WhoIS, County, ASN, etc.). Any Allow Lists the IP was found on that may be of interest when determining a proper mitigation strategy will also display. Note that although the allow lists may display, by virtue of appearing in the log, the corresponding set of IP events were indeed still blocked.



151.101.2.132
13 events

10/18/24, 11:51:37 AM
10/18/24, 09:37:59 AM

Enforcer AWS

Webroot

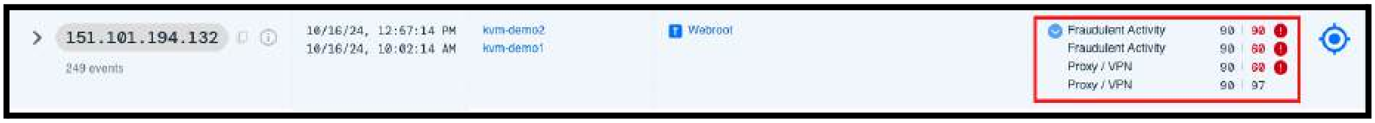
Fraudulent Activity 90 | 80
Proxy / VPN 90 | 80

DETAILS
Country Name UNITED STATES
ISO Code 2 US
ASN Name Fastly, Inc.
ASN 54113
Allow Lists Fastly

WHOIS
ISO Code 2 US
Organization Fastly, Inc. (SKYCA-3)
NetName SKYCA-3

WHOIS EXTENDED
Autonomous System Name FASTLY, US
Allocated 2016-02-01
Registry arin
ISO Code 2 US
BGP Prefix 151.101.0.0/22
IP 151.101.2.132
Autonomous System # 54113

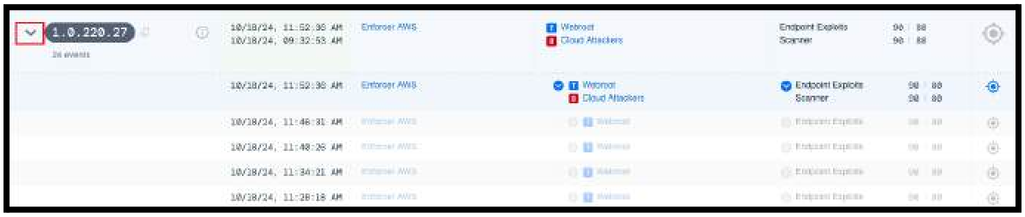
- Date range – the first and last logged timestamp for the IP in the queried range
- Enforcer(s) – a list of Enforcers that blocked the IP event set
- Lists – the Block and Threat Lists the IP was found on
- Category | Score | Threshold – If the IP was on a Threat List the following will display:
    - Threat Category(s) for the IP
    - Threat Score(s) for the IP
    - Threshold(s) set in the outbound blocking policy for that Threat Category
        - The header row will be a roll-up of all categories/scores/thresholds of the child events



151.101.194.132 249 events	10/16/24, 12:57:14 PM 10/16/24, 10:02:14 AM	kvm-demo2 kvm-demo1	Webroot	Fraudulent Activity Fraudulent Activity Proxy / VPN Proxy / VPN	90 90 90 90	90 60 60 97

Note: A warning icon will display next to Fraudulent Activity and Proxy/VPN if the threshold set on these categories is less than 97. Our threat intelligence has found that these 2 categories are the most likely source of unexpected blocks and setting these 2 categories to 97 can help alleviate issues you may be having with unexpected blocks.

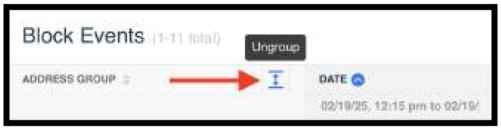
To view the IP's child events, click on the chevron to the left of the IP address:



1.0.220.27 26 events	10/18/24, 11:52:36 AM 10/18/24, 09:32:53 AM	Enforcer AWS	Webroot Cloud Attackers	Endpoint Exploits Scanner	90 90	88 88
	10/18/24, 11:52:36 AM	Enforcer AWS	Webroot Cloud Attackers	Endpoint Exploits Scanner	90 90	88 88
	10/18/24, 11:46:31 AM	Enforcer AWS	Webroot	Endpoint Exploits	[illegible]	[illegible]
	10/18/24, 11:40:26 AM	Enforcer AWS	Webroot	Endpoint Exploits	[illegible]	[illegible]
	10/18/24, 11:34:21 AM	Enforcer AWS	Webroot	Endpoint Exploits	[illegible]	[illegible]
	10/18/24, 11:28:18 AM	Enforcer AWS	Webroot	Endpoint Exploits	[illegible]	[illegible]

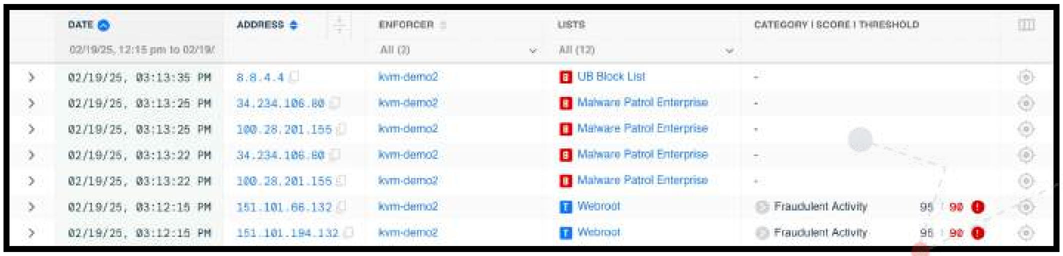
Each row will display the event-specific data for that individual timestamp.

If you prefer viewing all Block Events by timestamp, simply click on the Ungroup icon and the table will display all events in reverse chronological order.



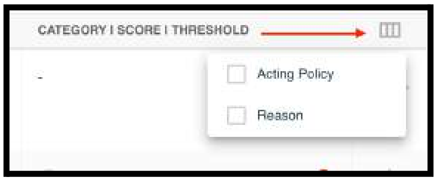
Block Events (1-11 total)

02/19/25, 12:15 pm to 02/19/



	DATE 02/19/25, 12:15 pm to 02/19/	ADDRESS	ENFORCER All (2)	LISTS All (12)	CATEGORY I SCORE I THRESHOLD
>	02/19/25, 03:13:35 PM	8.8.4.4	kvm-demo2	B UB Block List	-
>	02/19/25, 03:13:25 PM	34.234.106.80	kvm-demo2	B Malware Patrol Enterprise	-
>	02/19/25, 03:13:25 PM	100.28.201.155	kvm-demo2	B Malware Patrol Enterprise	-
>	02/19/25, 03:13:22 PM	34.234.106.80	kvm-demo2	B Malware Patrol Enterprise	-
>	02/19/25, 03:13:22 PM	100.28.201.155	kvm-demo2	B Malware Patrol Enterprise	-
>	02/19/25, 03:12:15 PM	151.101.66.132	kvm-demo2	T Webroot	Fraudulent Activity 95 | 90
>	02/19/25, 03:12:15 PM	151.101.194.132	kvm-demo2	T Webroot	Fraudulent Activity 95 | 90

In the Block Events table, you can add columns to view the Reason why the IP was blocked and the Policy that blocked the IP. To add (or remove) these columns, click on the column icon at the top of the far-right column and then select the column(s) you would like included in the Block Events table.

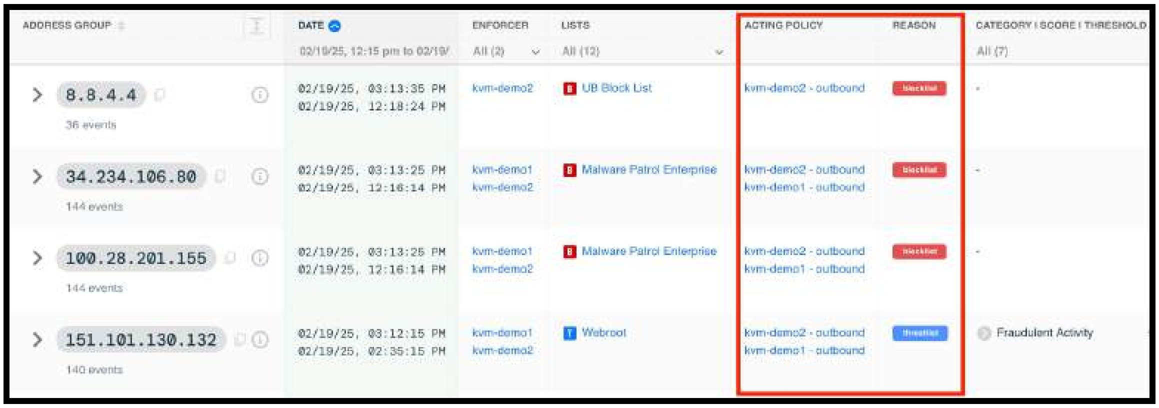


CATEGORY I SCORE I THRESHOLD

-

□ Acting Policy

□ Reason



ADDRESS GROUP	DATE 02/19/25, 12:15 pm to 02/19/	ENFORCER All (2)	LISTS All (12)	ACTING POLICY	REASON	CATEGORY I SCORE I THRESHOLD All (7)
> 8.8.4.4 36 events	02/19/25, 03:13:35 PM 02/19/25, 12:18:24 PM	kvm-demo2	B UB Block List	kvm-demo2 - outbound	blacklist	-
> 34.234.106.80 144 events	02/19/25, 03:13:25 PM 02/19/25, 12:16:14 PM	kvm-demo1 kvm-demo2	B Malware Patrol Enterprise	kvm-demo2 - outbound kvm-demo1 - outbound	blacklist	-
> 100.28.201.155 144 events	02/19/25, 03:13:25 PM 02/19/25, 12:16:14 PM	kvm-demo1 kvm-demo2	B Malware Patrol Enterprise	kvm-demo2 - outbound kvm-demo1 - outbound	blacklist	-
> 151.101.130.132 140 events	02/19/25, 03:12:15 PM 02/19/25, 02:35:15 PM	kvm-demo1 kvm-demo2	T Webroot	kvm-demo2 - outbound kvm-demo1 - outbound	threatlist	Fraudulent Activity

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

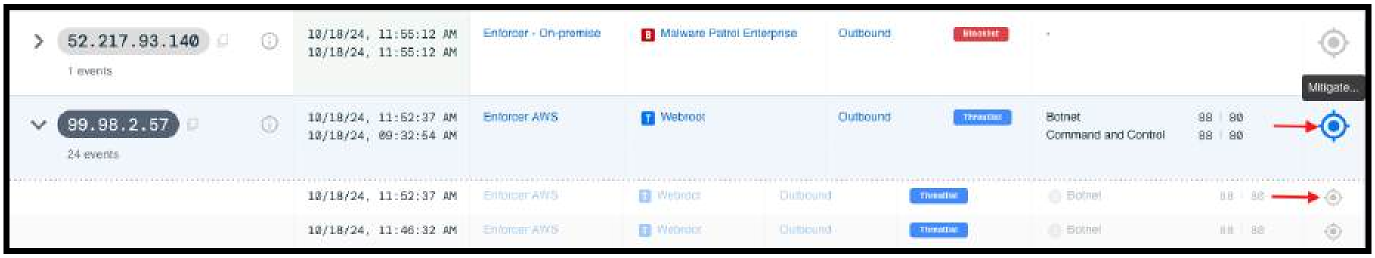
display the results within the date range you originally searched for. You can use the "Existing Log Range" to determine if you may want to expand your search parameters.

- 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.

Mitigation Strategies

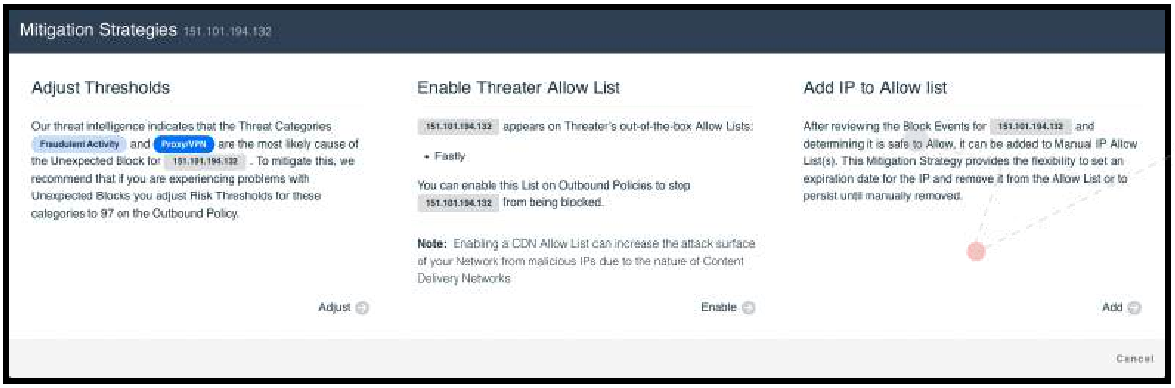
Once the IP that was being blocked is identified, you can click on the Mitigate button in the far-right column.



> 52.217.93.140 1 events	10/18/24, 11:55:12 AM 10/18/24, 11:55:12 AM	Enforcer - On-premise	B Malware Patrol Enterprise	Outbound	Blocklist	-		
⌄ 99.98.2.57 24 events	10/18/24, 11:52:37 AM 10/18/24, 09:32:54 AM	Enforcer AWS	T Webroot	Outbound	Throttled	Botnet Command and Control	88 | 80 88 | 80	Mitigate...
	10/18/24, 11:52:37 AM	Enforcer AWS	Webroot	Outbound	Throttled	Botnet	88 | 88	
	10/18/24, 11:46:32 AM	Enforcer AWS	Webroot	Outbound	Throttled	Botnet	88 | 88	

Note: Mitigation can happen at the roll-up level, or at the individual event level.

You will be presented with up to 3 mitigation options. Only mitigation strategies relevant to the particular event or event set will be displayed, so you may see less than 3.



Mitigation Strategies 151.101.194.132

Adjust Thresholds

Our threat intelligence indicates that the Threat Categories Fraudulent Activity and Proxy/VPN are the most likely cause of the Unexpected Block for 151.101.194.132 . To mitigate this, we recommend that if you are experiencing problems with Unexpected Blocks you adjust Risk Thresholds for these categories to 97 on the Outbound Policy.

Adjust

Enable Threater Allow List

151.101.194.132 appears on Threater's out-of-the-box Allow Lists:

- Fastly

You can enable this List on Outbound Policies to stop 151.101.194.132 from being blocked.

Note: Enabling a CDN Allow List can increase the attack surface of your Network from malicious IPs due to the nature of Content Delivery Networks

Enable

Add IP to Allow list

After reviewing the Block Events for 151.101.194.132 and determining it is safe to Allow, it can be added to Manual IP Allow List(s). This Mitigation Strategy provides the flexibility to set an expiration date for the IP and remove it from the Allow List or to persist until manually removed.

Add

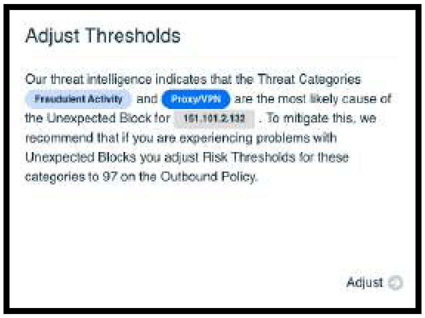
Cancel

Adjust Thresholds

The Adjust Thresholds option will be presented if the IP meets the following criteria:

- On a Threat list
- Categorized as Fraudulent Activity and/or Proxy VPN
- Thresholds on the outbound blocking policy for those either of these 2 categories is less than 97

If this is the desired mitigation strategy, click on Adjust.

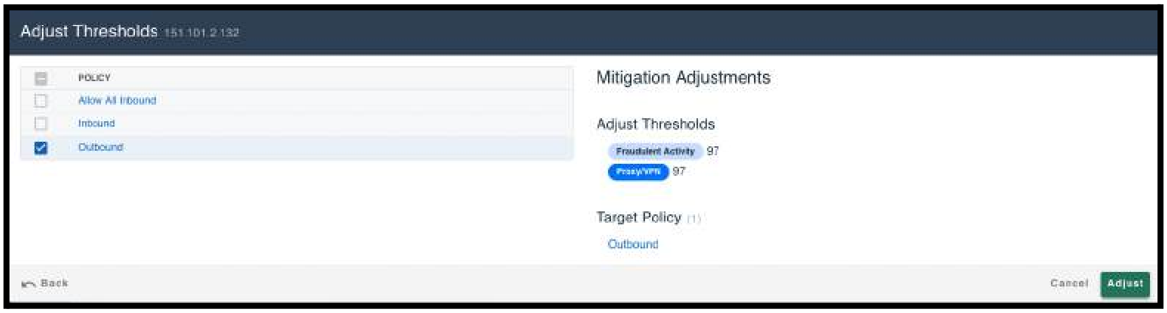


Adjust Thresholds

Our threat intelligence indicates that the Threat Categories Fraudulent Activity and Proxy/VPN are the most likely cause of the Unexpected Block for 151.101.2.132 . To mitigate this, we recommend that if you are experiencing problems with Unexpected Blocks you adjust Risk Thresholds for these categories to 97 on the Outbound Policy.

Adjust

The outbound policies that blocked the IP will be selected by default. All other policies are also available to select.



Adjust Thresholds 151.101.2.132

☐	POLICY
☐	Allow All Inbound
☐	Inbound
☑	Outbound

Mitigation Adjustments

Adjust Thresholds

Fraudulent Activity 97

Proxy/VPN 97

Target Policy (1)

Outbound

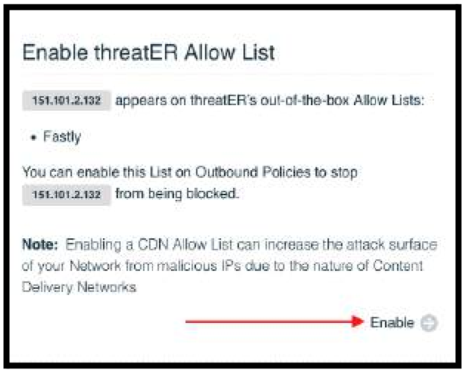
Once the desired policy selections are made, click on the Adjust button. A confirmation modal will then display.

The Fraudulent Activity and Proxy VPN category thresholds will now be set to 97 on the applicable policy(s) and enforced accordingly.

Enable threatER Allow List

If the IP is on any of threatER's out-of-the-box Allow lists, this option will be presented, as well as the names of the lists the IP was included on. An additional note will display if any of these lists are a CDN list.

If this is the desired mitigation strategy, click on Enable.



Enable threatER Allow List

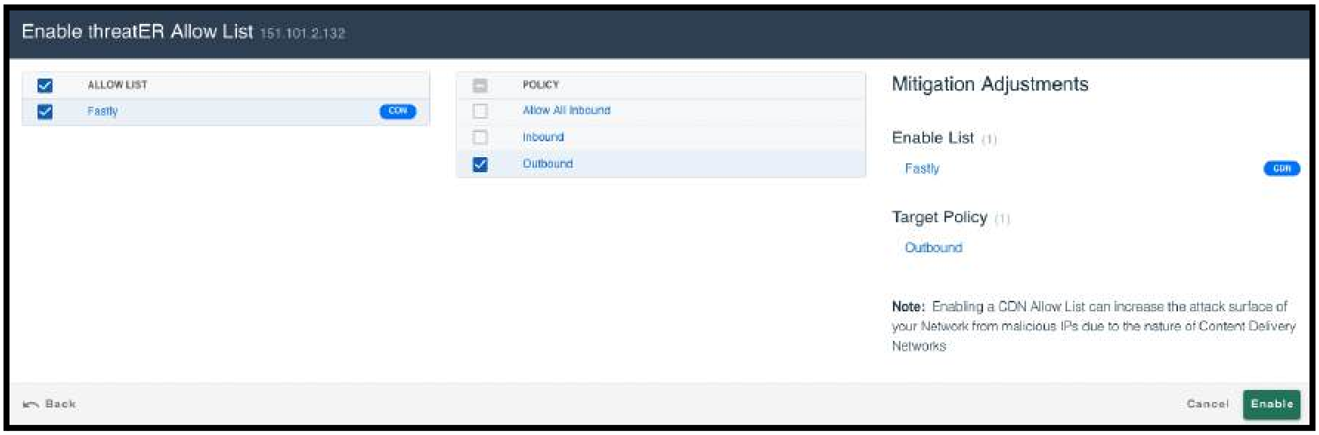
151.101.2.132 appears on threatER's out-of-the-box Allow Lists:

- Fastly

You can enable this List on Outbound Policies to stop 151.101.2.132 from being blocked.

Note: Enabling a CDN Allow List can increase the attack surface of your Network from malicious IPs due to the nature of Content Delivery Networks

Select the Allow List(s) you would like to enable. The outbound policies that blocked the IP will be selected by default. All other policies are also available to select.



Enable threatER Allow List 151.101.2.132

☑	ALLOW LIST	
☑	Fastly	CDN

▣	POLICY
□	Allow All Inbound
□	Inbound
☑	Outbound

Mitigation Adjustments

Enable List (1)

Fastly CDN

Target Policy (1)

Outbound

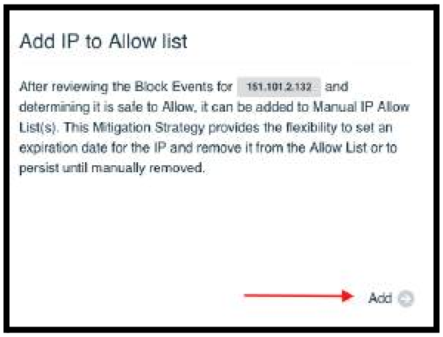
Note: Enabling a CDN Allow List can increase the attack surface of your Network from malicious IPs due to the nature of Content Delivery Networks

Once the desired policy selections are made, click on the Enable button. A confirmation modal will then display.The selected Allow list(s) are now enabled by the selected policy(s).

Add IP to (Manual) Allow List

This mitigation option will always be available as a selection. This option gives you the flexibility to set an expiration date or remove the IP from your manual allow list(s) at a later date.

If this is the desired mitigation strategy, click on Add.



Add IP to Allow list

After reviewing the Block Events for 151.101.2.132 and determining it is safe to Allow, it can be added to Manual IP Allow List(s). This Mitigation Strategy provides the flexibility to set an expiration date for the IP and remove it from the Allow List or to persist until manually removed.

Select the manual Allow list(s) to add the IP to.

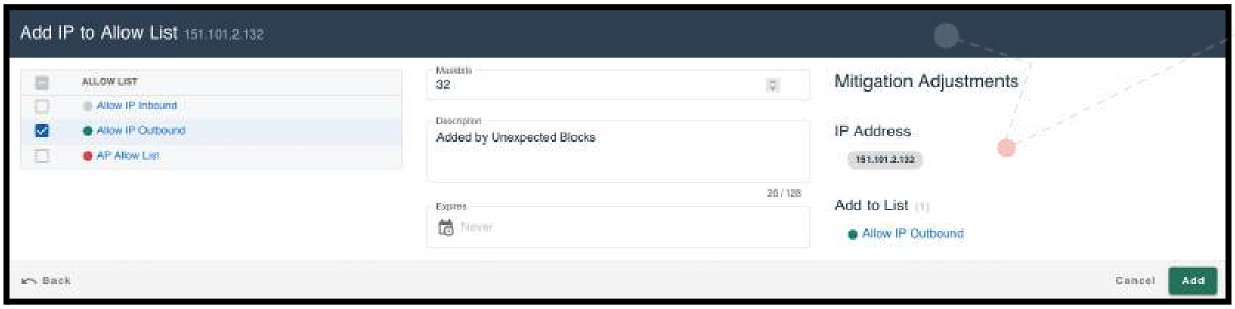
The colored pips next to the Allow list names indicate the following:

- 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.
- 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).
- 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.

Make any necessary edits to the IP entry:

- Maskbits – default is 32
- 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.

- Expiration – default is “Never”; however, we generally recommend that you time-bound allowed-lists additions when feasible.



Add IP to Allow List 151.101.2.132

□	ALLOW LIST
□	● Allow IP Inbound
☑	● Allow IP Outbound
□	● AP Allow List

Maskbits: 32

Description: Added by Unexpected Blocks

26 / 128

Expires: Never

Mitigation Adjustments

IP Address

151.101.2.132

Add to List (1)

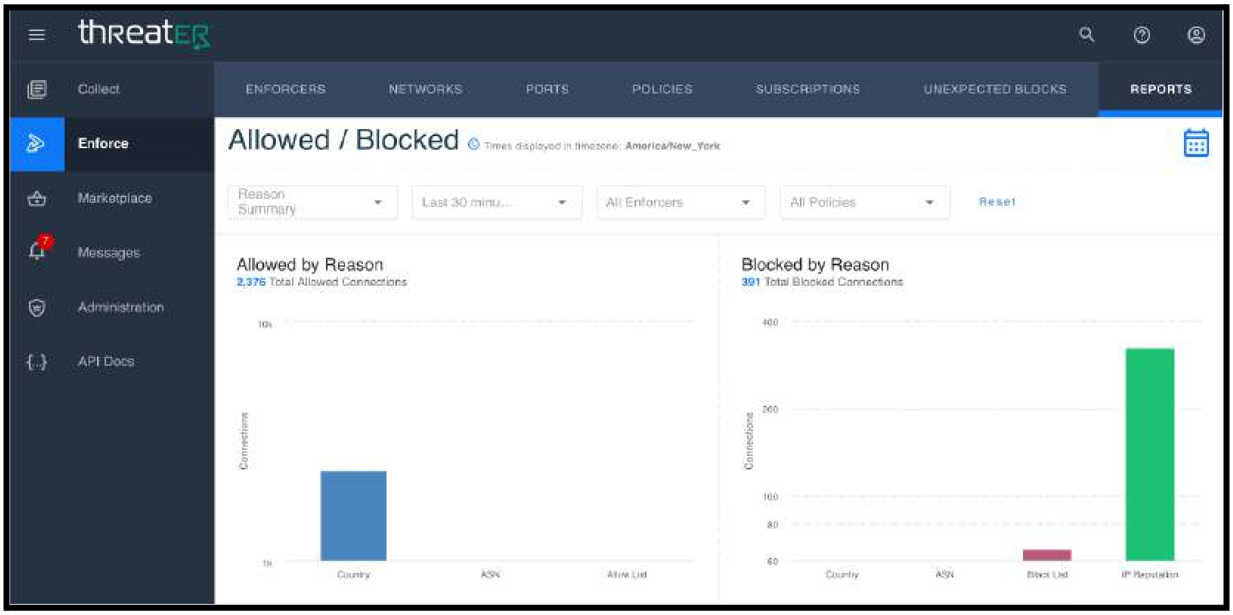
● Allow IP Outbound

Once the desired policy selections are made, click on the Add button. A confirmation modal will then display. The IP is now added to the selected Allow list(s) and will be enforced by the policy(s) those lists are assigned to.

Reports

Reports provide a quick, graphical look at your system summaries. They contain metadata summarized from the detailed logs stored in Enforce. As no specific data is contained within the threatER portal, there should be no compliance issues.

To access Reports, select Enforce from the left-hand navigation menu and then click the Reports tab. The “Allowed/Blocked: Reason Summary” report is the default view. All data in reports is displayed in your browser’s local time zone. There are 2 types of reports (Allowed/Blocked & Top 10) and each one has the functionality to schedule a report.



Allowed / Blocked Times displayed in timezone: America/New_York

Reason Summary | Last 30 minu... | All Enforcers | All Policies

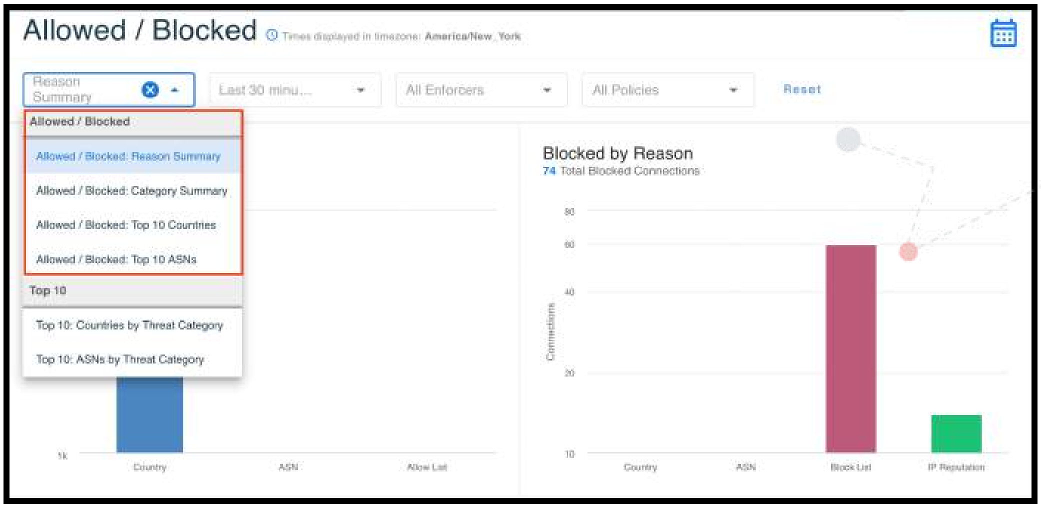
Allowed by Reason
2,376 Total Allowed Connections

Blocked by Reason
391 Total Blocked Connections

Allowed/Blocked

The Allowed/Blocked reports display the number of allowed or blocked connections for a given time frame, policy, and Enforcer. The default display for all Allowed/Blocked reports is all connections made in the last 30 minutes on all policies and Enforcers This data can be filtered based on a selection of preset timeframes, on a per policy basis, or on a per Enforcer basis.

This data is broken out into four separate reports, which are accessible via the drop-down at the top of the tab.


Allowed / Blocked
Times displayed in timezone: America/New_York
Reason Summary
Last 30 minu...
All Enforcers
All Policies
Reset
Allowed / Blocked
Allowed / Blocked: Reason Summary
Allowed / Blocked: Category Summary
Allowed / Blocked: Top 10 Countries
Allowed / Blocked: Top 10 ASNs
Top 10
Top 10: Countries by Threat Category
Top 10: ASNs by Threat Category
1k
Country
ASN
Allow List
Blocked by Reason
74 Total Blocked Connections
80
60
40
20
10
Connections
Country
ASN
Block List
IP Reputation

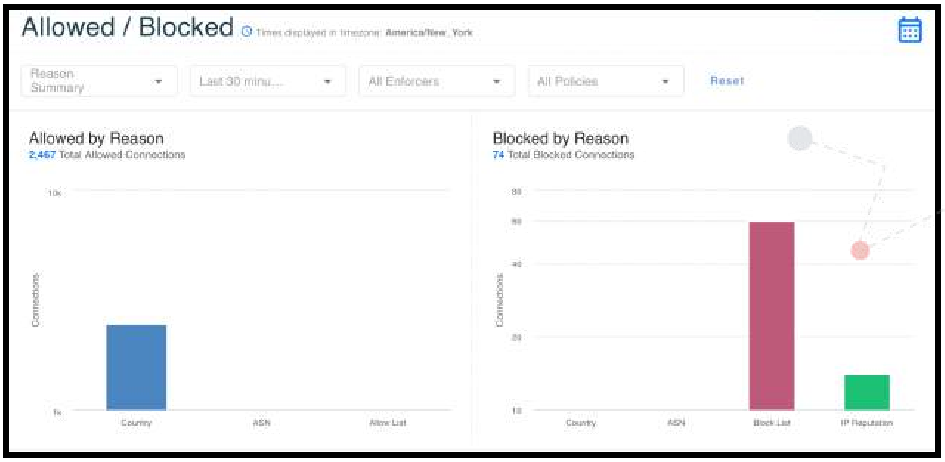
Reason Summary

The Allowed by Reason report displays connections that were allowed because of the following reasons (the below reasons are in the order the system processes enforcements):

- Allow List – connections allowed based on explicit Allow list content
- ASN – connections allowed by ASN adjustments
- Country – connections allowed by a policy that were not specifically allowed by an Allow List or an ASN adjustment

The Blocked by Reason report displays connections that were blocked because of the following reasons (the below reasons are in the order the system processes enforcements):

- Block List – connections blocked based on explicit Block list content
- IP Reputation – connections blocked based on explicit Threat list content
- ASN – connections blocked by ASN adjustments
- Country – connections blocked by a policy that were not specifically blocked by a Block List



Allowed / Blocked Times displayed in timezone: America/New_York

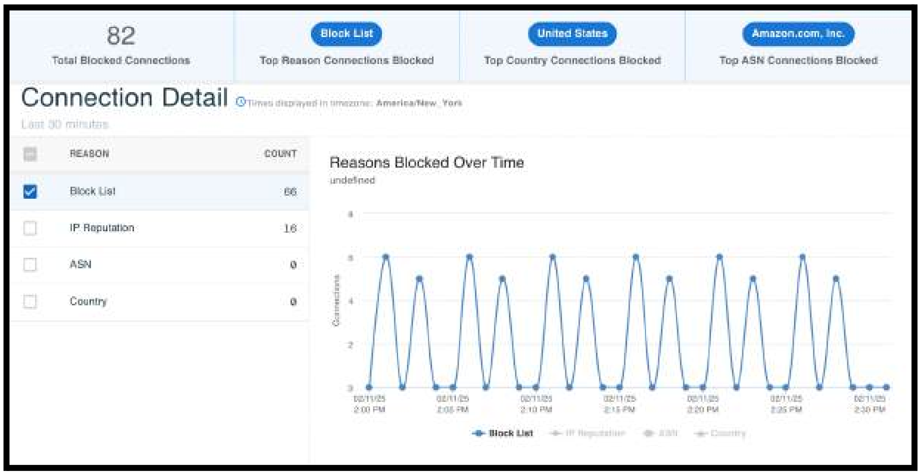
Reason Summary | Last 30 minu... | All Enforcers | All Policies | Reset

Allowed by Reason
2,467 Total Allowed Connections

Blocked by Reason
74 Total Blocked Connections

Clicking on a slice of data will open the Connection Detail for the report and display the following:

- Reasons and Count panel
  - Displays all reasons and the count for each
    - Default selection will be the reason selected on the previous graph
  - Selecting additional reasons will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connections Blocked or Allowed
- Top ASN Connections Blocked or Allowed



82	Block List	United States	Amazon.com, Inc.
Total Blocked Connections	Top Reason Connections Blocked	Top Country Connections Blocked	Top ASN Connections Blocked

Connection Detail Times displayed in timezone: America/New_York
Last 30 minutes

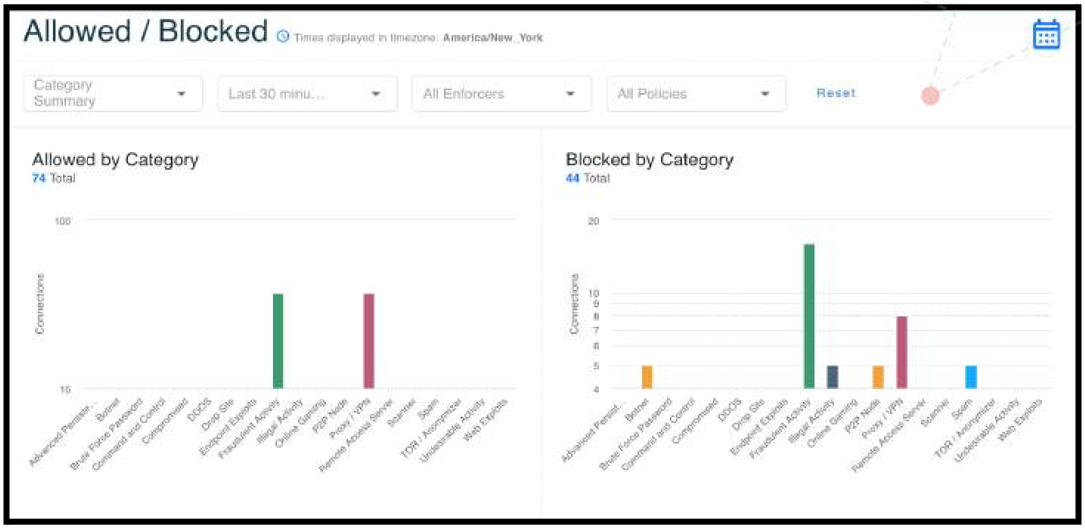
☐	REASON	COUNT
☑	Block List	66
☐	IP Reputation	16
☐	ASN	0
☐	Country	0

Reasons Blocked Over Time
undefined

Category Summary

The Allowed by Category report displays allowed connections that were indicated as part of a threat category, but fell below the configured thresholds for blocking at the time of connection.

The Blocked by Category report displays blocked connections that were found to be in a threat category at that time, regardless of why they were blocked and any blocking threshold.



Allowed / Blocked Times displayed in timezone: America/New_York

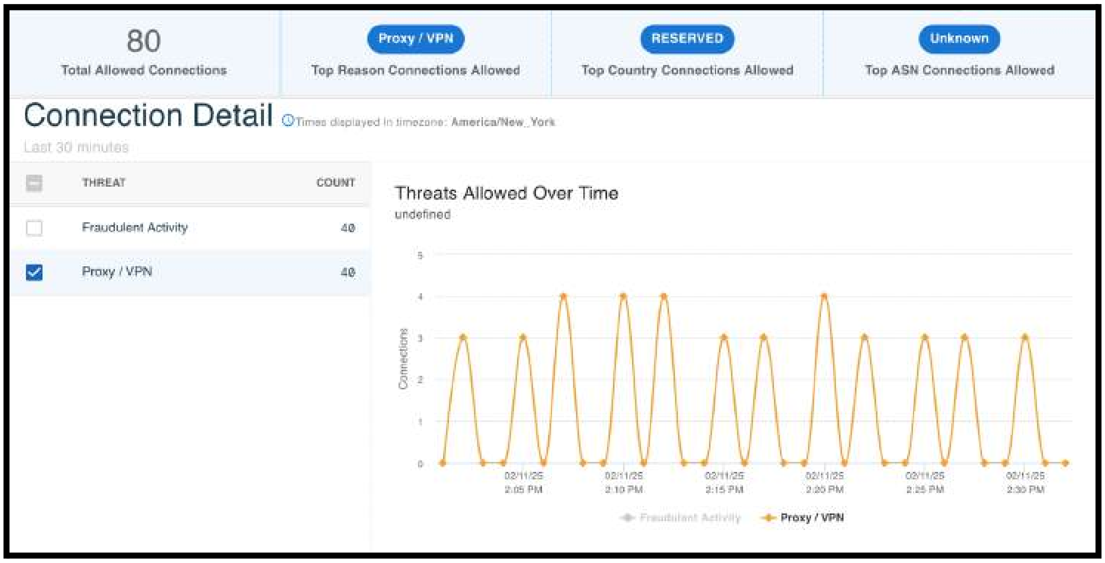
Category Summary | Last 30 minu... | All Enforcers | All Policies | Reset

Allowed by Category
74 Total

Blocked by Category
44 Total

Clicking on a slice of data will open the Connection Detail for the report and display the following:

- Threat category and Count panel
  - Displays the applicable threat categories and count for each
    - Default selection will be the category selected on the previous graph
  - Selecting additional categories will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed



80 Total Allowed Connections | Proxy / VPN Top Reason Connections Allowed | RESERVED Top Country Connections Allowed | Unknown Top ASN Connections Allowed

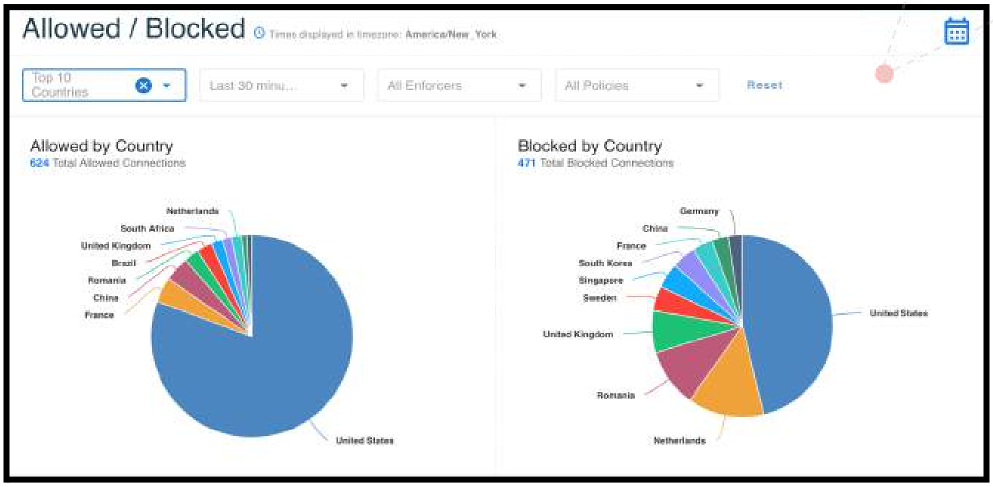
Connection Detail Times displayed in timezone: America/New_York
Last 30 minutes

□ THREAT	COUNT
□ Fraudulent Activity	40
☑ Proxy / VPN	40

Threats Allowed Over Time
undefined

Top 10 Countries

The Top 10 Countries report displays the countries the connections came from, based on what was allowed or blocked.



Allowed / Blocked Times displayed in timezone: America/New_York

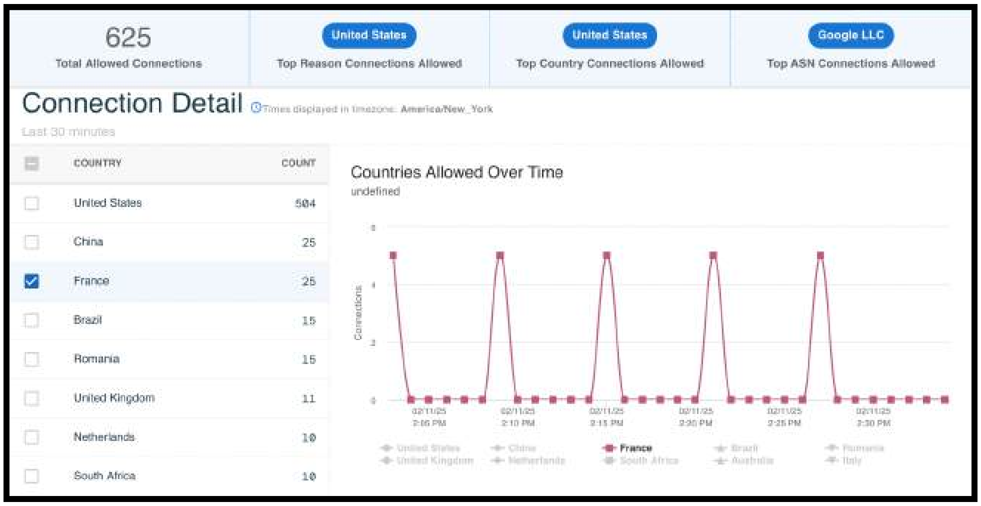
Top 10 Countries | Last 30 minu... | All Enforcers | All Policies | Reset

Allowed by Country
624 Total Allowed Connections

Blocked by Country
471 Total Blocked Connections

Clicking on a slice of data will open the Connection Detail for the dashboard and display the following:

- Country and Count panel
  - Displays the applicable countries and the count for each
    - Default selection will be the country selected on the previous graph
  - Selecting additional countries will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed



625 Total Allowed Connections | United States Top Reason Connections Allowed | United States Top Country Connections Allowed | Google LLC Top ASN Connections Allowed

Connection Detail Times displayed in timezone: America/New_York

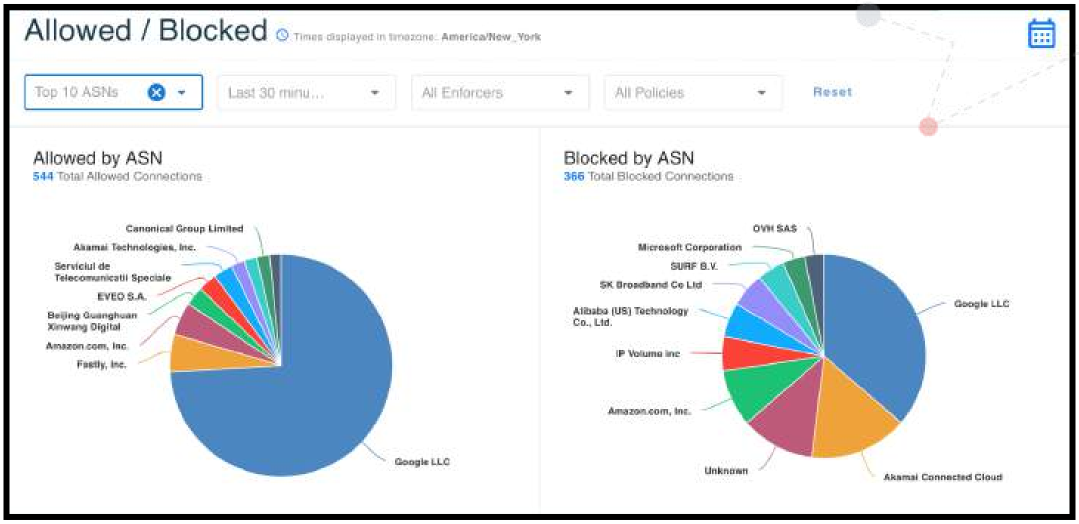
Last 30 minutes

▬	COUNTRY	COUNT
□	United States	504
□	China	25
☑	France	25
□	Brazil	15
□	Romania	15
□	United Kingdom	11
□	Netherlands	10
□	South Africa	10

Countries Allowed Over Time
undefined

Top 10 ASNs

The Top 10 ASN report displays the ASNs the connections came from, based on what was allowed or blocked.



Allowed / Blocked Times displayed in timezone: America/New_York

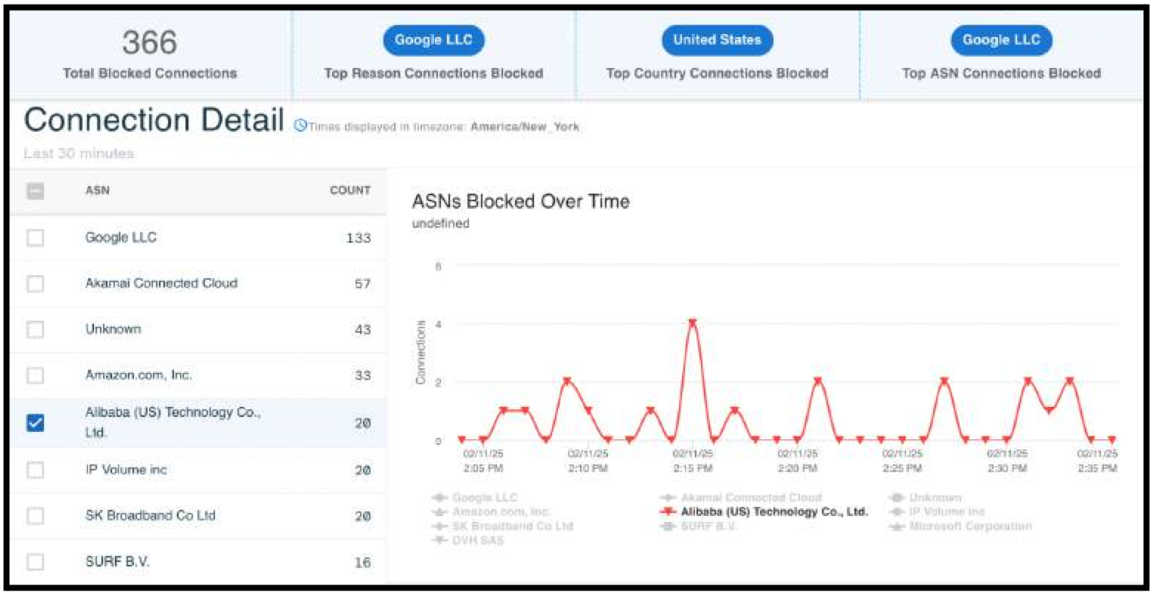
Top 10 ASNs | Last 30 minu... | All Enforcers | All Policies | Reset

Allowed by ASN
544 Total Allowed Connections

Blocked by ASN
366 Total Blocked Connections

Clicking on a slice of data will open the Connection Detail for the dashboard and display the following:

- ASN and Count panel
  - Displays the applicable ASNs and the count for each
    - Default selection will be the ASN selected on the previous graph
  - Selecting additional ASNs will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed
- Top Country Connection Blocked or Allowed
- Top ASN Connections Blocked or Allowed



366	Google LLC	United States	Google LLC
Total Blocked Connections	Top Reason Connections Blocked	Top Country Connections Blocked	Top ASN Connections Blocked

Connection Detail Times displayed in timezone: America/New_York
Last 30 minutes

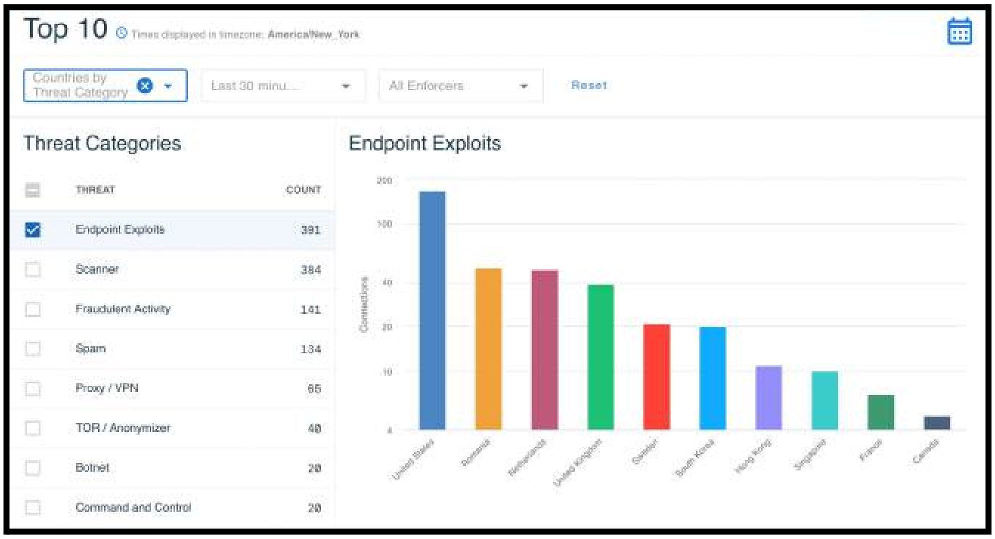
	ASN	COUNT
□	Google LLC	133
□	Akamai Connected Cloud	57
□	Unknown	43
□	Amazon.com, Inc.	33
☑	Alibaba (US) Technology Co., Ltd.	20
□	IP Volume inc	20
□	SK Broadband Co Ltd	20
□	SURF B.V.	16

ASNs Blocked Over Time
undefined

Top 10

Countries by Threat Category

The Top 10 Countries by Threat Category report displays graphs for the top 10 countries blocked due to specified threat category(s). These graphs can be accessed by selecting "Top 10: Countries by Threat Category" from the report drop-down.



Top 10 Times displayed in timezone: America/New_York

Countries by Threat Category | Last 30 minu... | All Enforcers | Reset

Threat Categories

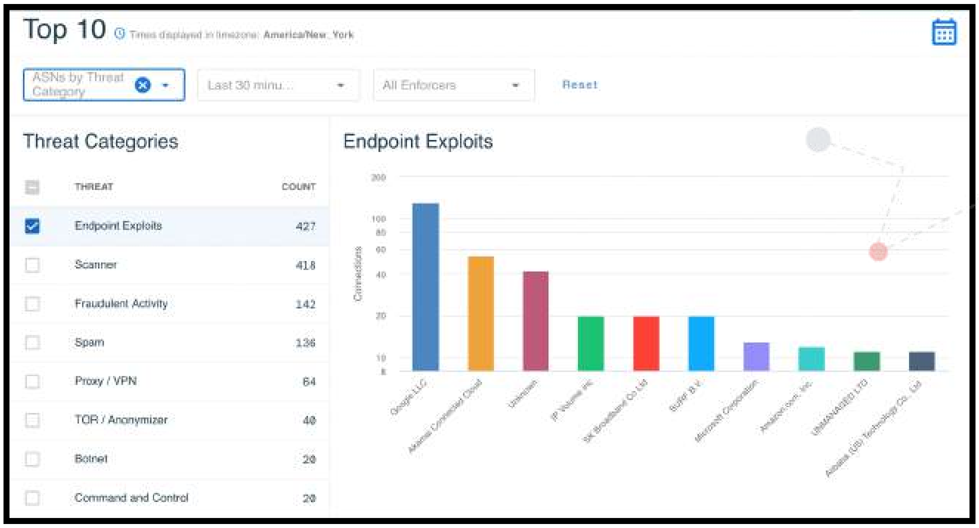
	THREAT	COUNT
☑	Endpoint Exploits	391
□	Scanner	384
□	Fraudulent Activity	141
□	Spam	134
□	Proxy / VPN	65
□	TOR / Anonymizer	40
□	Botnet	20
□	Command and Control	20

The Threat Category with the highest count will be selected by default and its graph will display in the right-hand panel. To view a graph for additional Threat Categories, select the desired category(s) in the left-hand panel.

Each threat category graph will display a bar for the top 10 countries with connections that have been flagged with that threat category. You can scroll over each bar to view the number of connections, based on the timeframe and Enforcer selected from the filters at the top of the screen.

ASNs by Threat Category

The Top 10 ASNs by Threat Category report displays graphs for the top 10 ASNs blocked due to specified threat category(s). These graphs can be accessed by selecting "Top 10: ASNs by Threat Category" from the report drop-down.



Top 10 Times displayed in timezone: America/New_York

ASNs by Threat Category | Last 30 minu... | All Enforcers | Reset

Threat Categories

	THREAT	COUNT
☑	Endpoint Exploits	427
□	Scanner	418
□	Fraudulent Activity	142
□	Spam	136
□	Proxy / VPN	64
□	TOR / Anonymizer	40
□	Botnet	20
□	Command and Control	20

The Threat Category with the highest count will be selected by default and its graph will display in the right-hand panel. To view a graph for additional Threat Categories, select the desired category(s) in the left-hand panel.

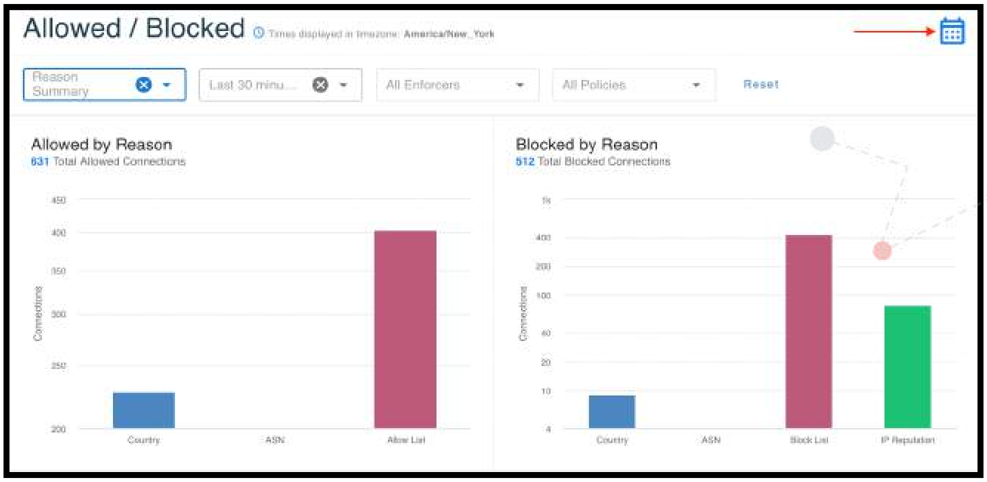
Each threat category graph will display a bar for the top 10 ASNs with connections that have been flagged with that threat category. You can scroll over each bar to view the number of connections, based on the timeframe and Enforcer selected from the filters at the top of the screen.

Scheduled Reports

Users can set a schedule for all reports. These reports will be emailed based on the schedule selected and the email will include a link to access the report by way of the threatER portal.

Reports can be scheduled by:

- Clicking the calendar icon in the top-right corner of a report



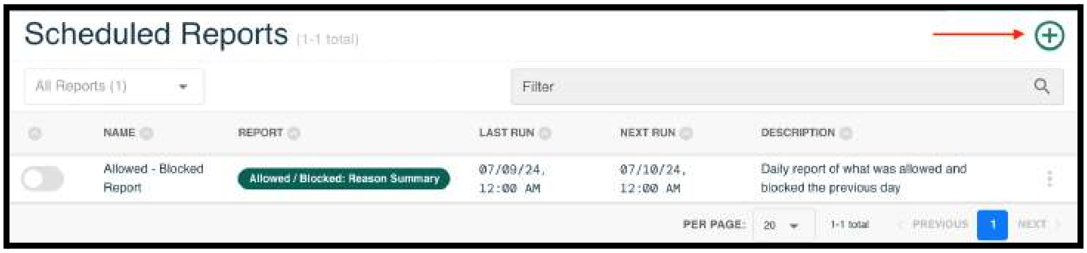
Allowed / Blocked Times displayed in timezone: America/New_York

Reason Summary | Last 30 minu... | All Enforcers | All Policies | Reset

Allowed by Reason
631 Total Allowed Connections

Blocked by Reason
512 Total Blocked Connections

- Click the “+” button in the top right corner



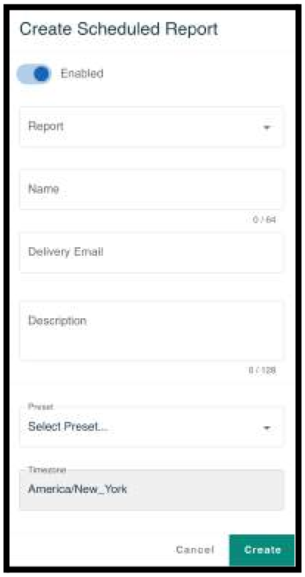
Scheduled Reports (1-1 total)

All Reports (1) | Filter

	NAME	REPORT	LAST RUN	NEXT RUN	DESCRIPTION
	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	07/09/24, 12:00 AM	07/10/24, 12:00 AM	Daily report of what was allowed and blocked the previous day

- Select the Report type
- Provide the following details (* indicates required field):
    - *Name
    - *Delivery Email
        - This is the email the link to the report will be sent to
    - Description
    - *Preset
        - Select one of the following from the drop-down:
            - **Yesterday** – report will run daily at midnight and includes data from the previous 24 hours
            - **Last Week** – report will run weekly at midnight on Sunday and includes data from the previous week
            - **Last Month** – report will run monthly at midnight on the 1st of each month and includes data from the previous month
            - **Last 7 days** – report will run daily at midnight and includes data from the previous 7 days

    - Policy (parameter only available for Allow/Blocked reports)
        - All Policies is the default selection
        - An individual policy can be selected from the drop-down
    - *Threat Categories (parameter only available for Top 10 reports)
        - From the drop-down, select the desired Threat Categories to include in the report
    - All Enforcers is the default selection
        - An individual Enforcer can be selected from the drop-down
- Click the Create button



Create Scheduled Report

Enabled

Report

Name

0 / 64

Delivery Email

Description

0 / 128

Preset

Select Preset...

Timezone

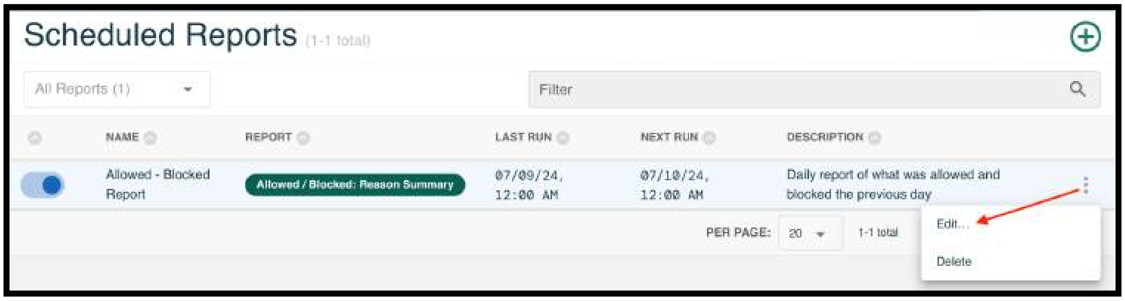
America/New_York

The report will be emailed to the address provided, based on the parameters selected.

Editing Scheduled Reports

To update the parameters of a scheduled report:

- On the Report tab, click the calendar icon
- Select Edit from the ellipsis menu in the row of the report you would like to edit

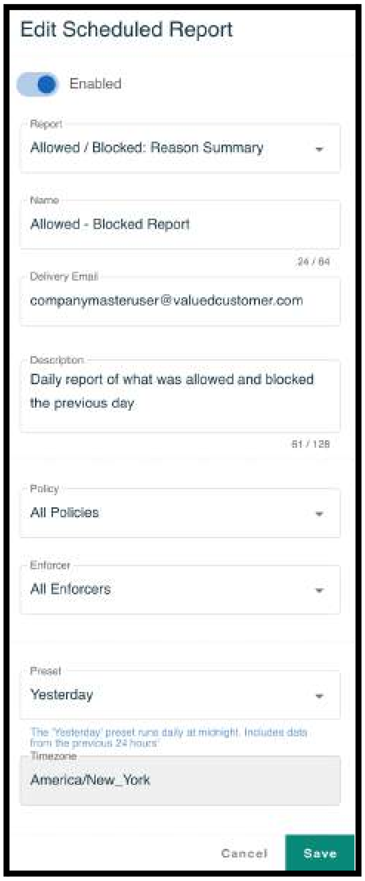


Scheduled Reports (1-1 total)

	NAME	REPORT	LAST RUN	NEXT RUN	DESCRIPTION
●	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	07/09/24, 12:00 AM	07/10/24, 12:00 AM	Daily report of what was allowed and blocked the previous day

PER PAGE: 20 1-1 total

- Make the desired updates and then click the Save button



Edit Scheduled Report

Enabled

Report: Allowed / Blocked: Reason Summary

Name: Allowed - Blocked Report

24 / 64

Delivery Email: companymasteruser@valuedcustomer.com

Description: Daily report of what was allowed and blocked the previous day

61 / 128

Policy: All Policies

Enforcer: All Enforcers

Preset: Yesterday

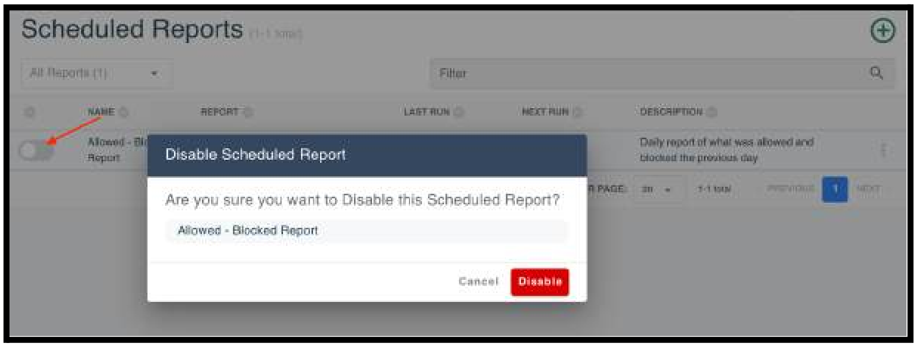
The 'Yesterday' preset runs daily at midnight. Includes data from the previous 24 hours'

Timezone: America/New_York

Disabling Scheduled Reports

To disable a scheduled report:

- In the row of the desired report, position the toggle to the left
- On the Disable Scheduled Report confirmation modal, click the Disable button



Scheduled Reports (1-1 total)

	NAME	REPORT	LAST RUN	NEXT RUN	DESCRIPTION
	Allowed - Bl… Report				Daily report of what was allowed and blocked the previous day

Disable Scheduled Report

Are you sure you want to Disable this Scheduled Report?

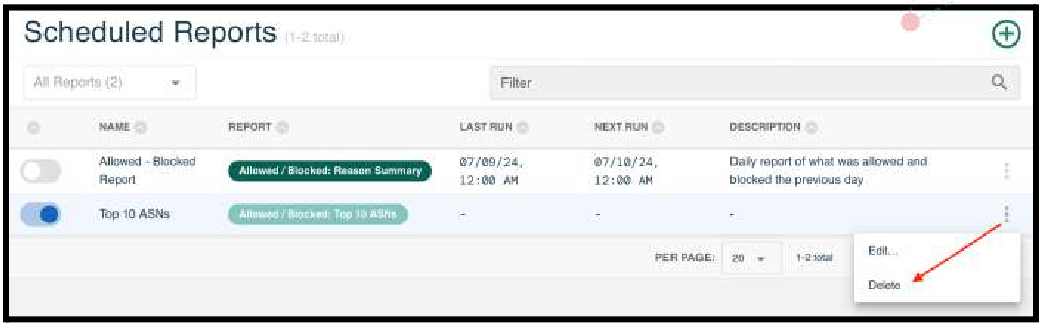
Allowed - Blocked Report

The report is now disabled and will no longer be emailed to the address that was provided. To enable the report at a later date, position the toggle to the right and confirm the action.

Deleting Scheduled Reports

To delete a scheduled report:

- On the Report tab, click the Scheduled button
- Select Delete from the ellipsis menu in the row of the report you would like to delete



Scheduled Reports (1-2 total)

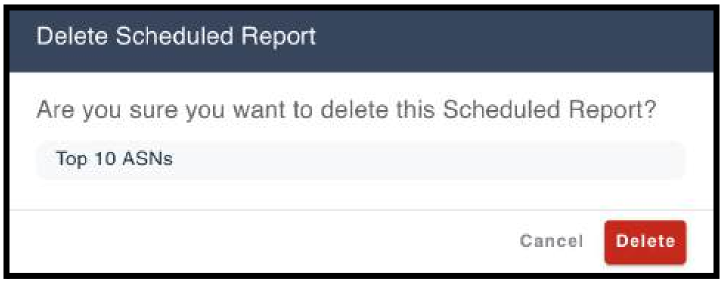
All Reports (2)

Filter

	NAME	REPORT	LAST RUN	NEXT RUN	DESCRIPTION	
○	Allowed - Blocked Report	Allowed / Blocked: Reason Summary	07/09/24, 12:00 AM	07/10/24, 12:00 AM	Daily report of what was allowed and blocked the previous day	⋮
●	Top 10 ASNs	Allowed / Blocked: Top 10 ASNs	-	-	-	⋮

PER PAGE: 20 1-2 total

- On the Delete Scheduled Report confirmation modal, click the Delete button



Delete Scheduled Report

Are you sure you want to delete this Scheduled Report?

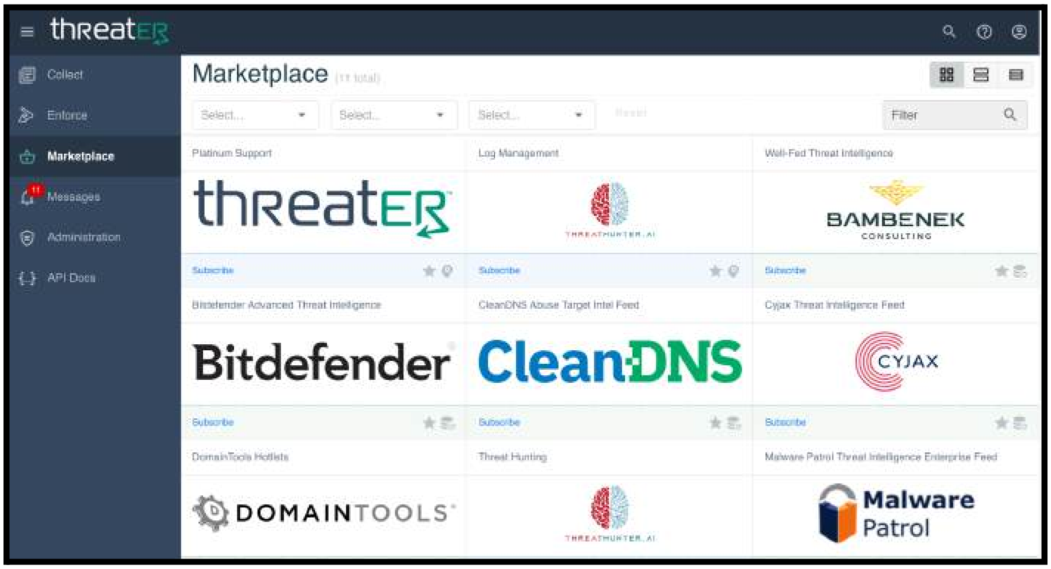
Top 10 ASNs

The report is now deleted, will not display in the Scheduled Reports table, and will no longer be emailed.

Marketplace

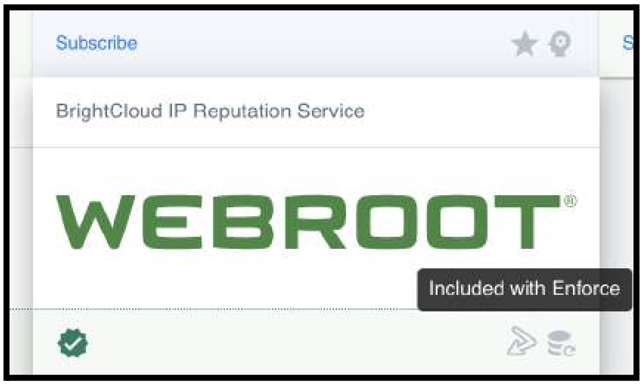
The Marketplace provides threatER customers access to high-value, multi-source cyber intelligence data from leading intelligence providers, as well as services to help manage and resolve threats in your network.

To access these offerings, select Marketplace from the left-hand navigation menu. All available products will display.



Included with Enforce Products

Some products, such as DomainTools and Webroot, are available to Enforce customers at no additional cost and display a “Included with Enforce” glyph on the card. There is no need to subscribe to these products and the feeds associated with these products are available to you and accessible via Collect.

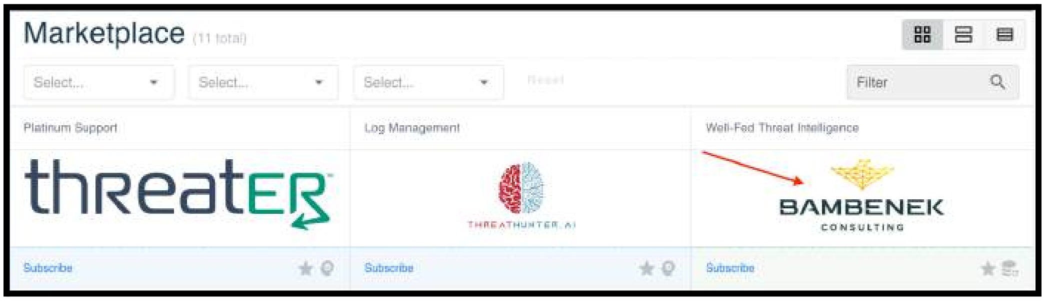


Premium Intelligence Products

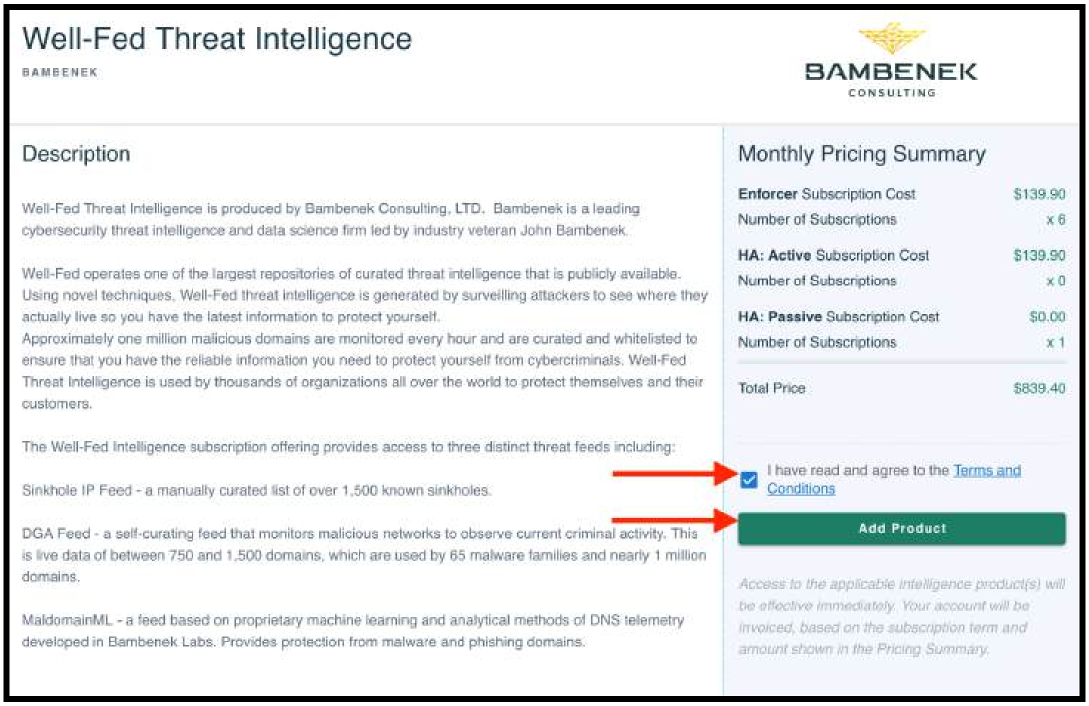
You may choose to purchase supplemental premium cyber intelligence feeds that are not included with your Enforce subscription. The pricing of these products is based on the total number of Enforcers on your account.

To purchase a product:

- Click on the product from the list



- Review the terms of the subscription provided on the next screen
- Click on the Terms and Conditions hyperlink (if applicable) to review in a separate tab
- Select the Terms and Conditions checkbox to enable the Add Product button
- Click the Add Product button



Well-Fed Threat Intelligence

BAMBENEK

Description

Well-Fed Threat Intelligence is produced by Bambenek Consulting, LTD. Bambenek is a leading cybersecurity threat intelligence and data science firm led by industry veteran John Bambenek.

Well-Fed operates one of the largest repositories of curated threat intelligence that is publicly available. Using novel techniques, Well-Fed threat intelligence is generated by surveilling attackers to see where they actually live so you have the latest information to protect yourself.
Approximately one million malicious domains are monitored every hour and are curated and whitelisted to ensure that you have the reliable information you need to protect yourself from cybercriminals. Well-Fed Threat Intelligence is used by thousands of organizations all over the world to protect themselves and their customers.

The Well-Fed Intelligence subscription offering provides access to three distinct threat feeds including:

Sinkhole IP Feed - a manually curated list of over 1,500 known sinkholes.

DGA Feed - a self-curating feed that monitors malicious networks to observe current criminal activity. This is live data of between 750 and 1,500 domains, which are used by 65 malware families and nearly 1 million domains.

MaldomainML - a feed based on proprietary machine learning and analytical methods of DNS telemetry developed in Bambenek Labs. Provides protection from malware and phishing domains.

Monthly Pricing Summary

Enforcer Subscription Cost	$139.90
Number of Subscriptions	x 6
HA: Active Subscription Cost	$139.90
Number of Subscriptions	x 0
HA: Passive Subscription Cost	$0.00
Number of Subscriptions	x 1
Total Price	$839.40

☑ I have read and agree to the Terms and Conditions

Access to the applicable intelligence product(s) will be effective immediately. Your account will be invoiced, based on the subscription term and amount shown in the Pricing Summary.

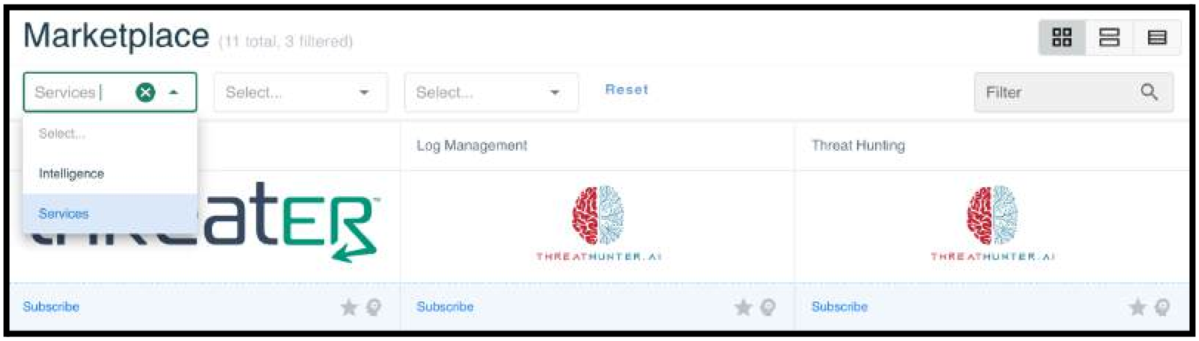
A modal will display providing further details about the subscription, to include the feeds you now have access to. Review these details and then click the OK button to close the modal. You will be redirected to the full list of Marketplace products. The product will now display as Subscribed.

Services

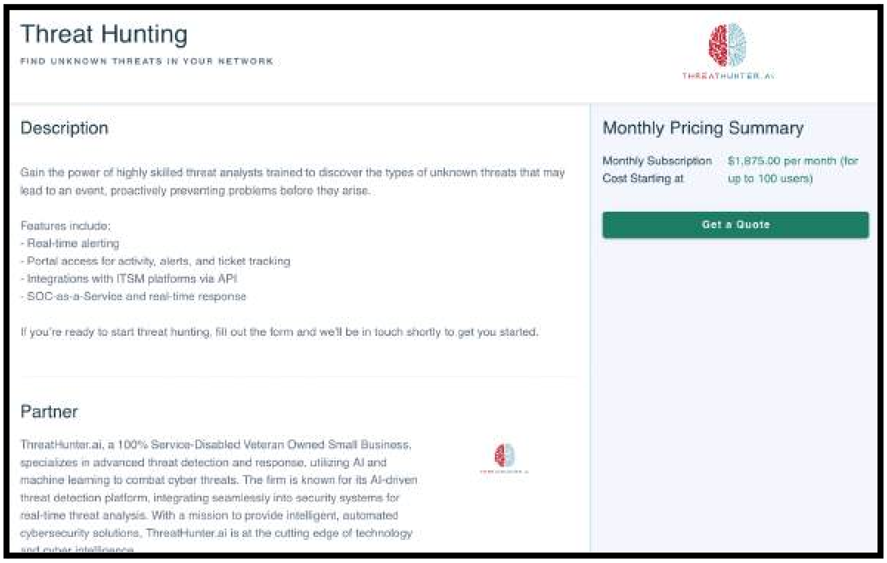
The threatER Marketplace included Services products that help manage and resolve threats in your network.

To request a quote on any of these services:

- Select "Services" from the Products drop-down
  - This will narrow down the available options to our Services products



- Click on a Service to view more information
- Click the "Get a Quote" button to submit your interest in this service



Threat Hunting

FIND UNKNOWN THREATS IN YOUR NETWORK

Description

Gain the power of highly skilled threat analysts trained to discover the types of unknown threats that may lead to an event, proactively preventing problems before they arise.

Features include:
- Real-time alerting
- Portal access for activity, alerts, and ticket tracking
- Integrations with ITSM platforms via API
- SOC-as-a-Service and real-time response

If you're ready to start threat hunting, fill out the form and we'll be in touch shortly to get you started.

Partner

ThreatHunter.ai, a 100% Service-Disabled Veteran Owned Small Business, specializes in advanced threat detection and response, utilizing AI and machine learning to combat cyber threats. The firm is known for its AI-driven threat detection platform, integrating seamlessly into security systems for real-time threat analysis. With a mission to provide intelligent, automated cybersecurity solutions, ThreatHunter.ai is at the cutting edge of technology and cyber intelligence

Monthly Pricing Summary

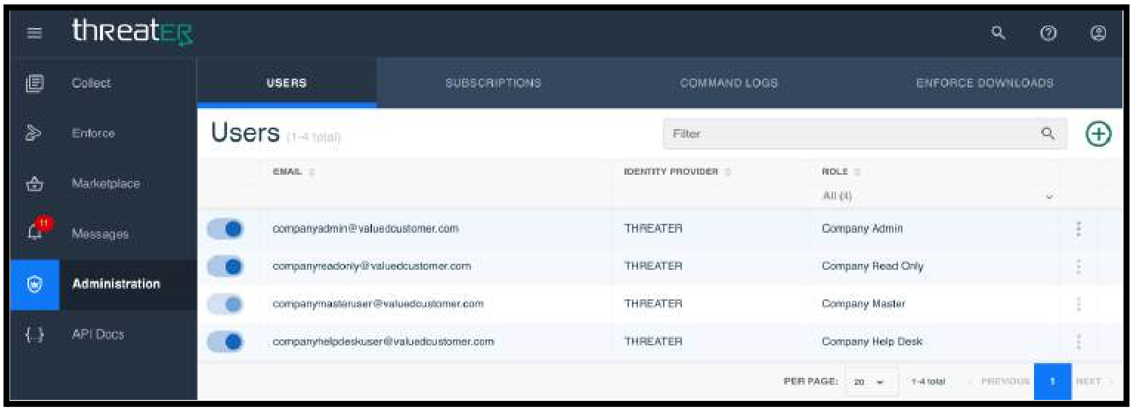
Monthly Subscription Cost Starting at	$1,875.00 per month (for up to 100 users)

After your request is submitted, someone from our team will contact you to discuss the necessary details and onboard the service to your account.

Administration

Users

The Users tab displays all users for your company and is where you can create new users, edit existing user accounts, enable/disable user accounts, and delete user accounts. To view your company's users, select Administration from the left-hand navigation menu and then click the User tab.



Users (1-4 total)

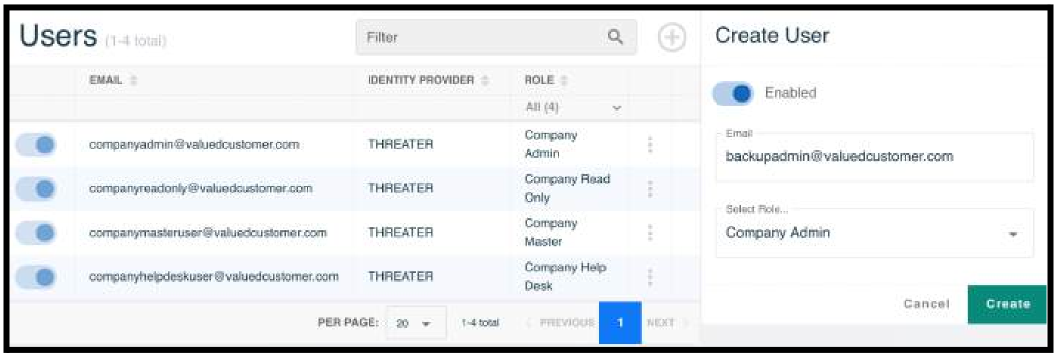
EMAIL	IDENTITY PROVIDER	ROLE
		All (4)
companyadmin@valuedcustomer.com	THREATER	Company Admin
companyreadonly@valuedcustomer.com	THREATER	Company Read Only
companymasteruser@valuedcustomer.com	THREATER	Company Master
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk

Please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

Create New User

Company Master users can create new users by completing the following steps:

- Click the "+" button in the top right corner of the Users table
- Enter the user's email address
- Select a Role from the drop-down
- Click the Create button



Users (1-4 total)

EMAIL	IDENTITY PROVIDER	ROLE
		All (4)
companyadmin@valuedcustomer.com	THREATER	Company Admin
companyreadonly@valuedcustomer.com	THREATER	Company Read Only
companymasteruser@valuedcustomer.com	THREATER	Company Master
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk

Create User

Enabled

Email: backupadmin@valuedcustomer.com

Select Role...: Company Admin

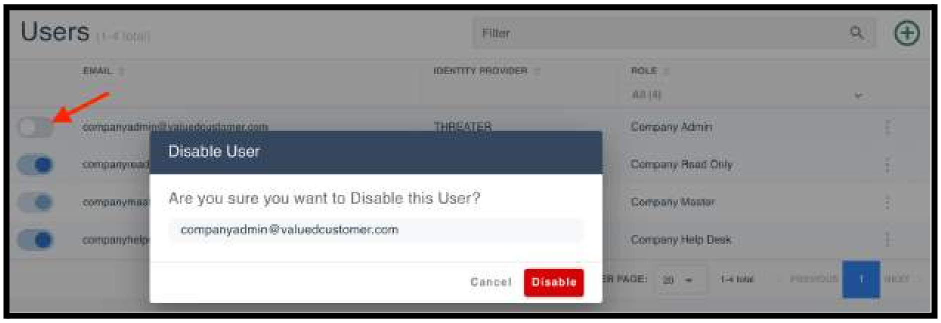
The new user will be created and an Account Activation email will be generated to the email provided. This email will contain the link for the user to complete the setup of their threatER account.

Edit User Accounts

Disable an Account

To disable an account:

- Search for the user account that needs to be disabled
- Position the Enable toggle to the left
- On the Disable User confirmation modal, click the Disable button



Disable User

Are you sure you want to Disable this User?

companyadmin@valuedcustomer.com

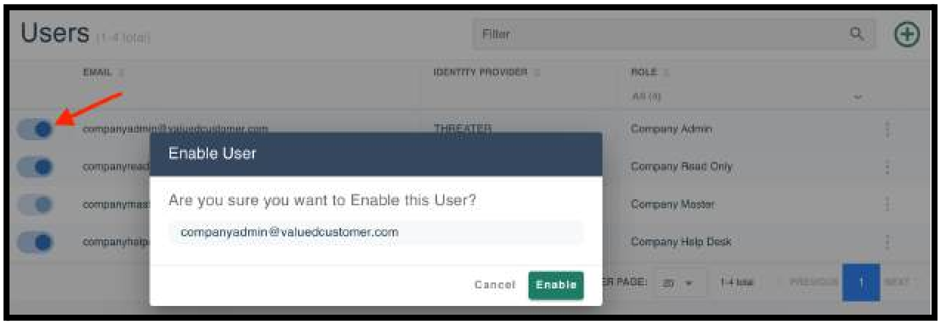
Cancel Disable

The user is now disabled and will not be able to log into the portal.

Enable an Account

To enable an account:

- Search for the user account that needs to be enabled
- Position the Enable toggle to the right
- On the Enable User confirmation modal, click the Enable button



Enable User

Are you sure you want to Enable this User?

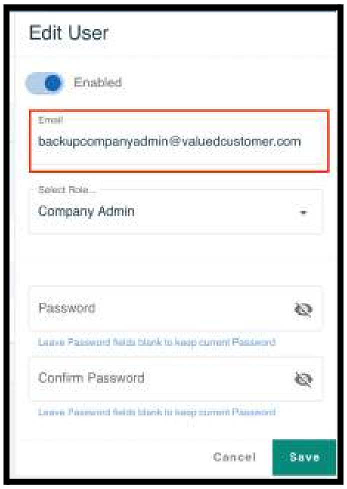
companyadmin@valuedcustomer.com

Cancel Enable

Update User Email

To update a user’s email address:

- Search for the user account
- From the ellipsis menu in the right-hand column of the row, select Edit
- Edit the Email field
- Click Save



Edit User

Enabled

Email: backupcompanyadmin@valuedcustomer.com

Select Role...: Company Admin

Password

Leave Password fields blank to keep current Password

Confirm Password

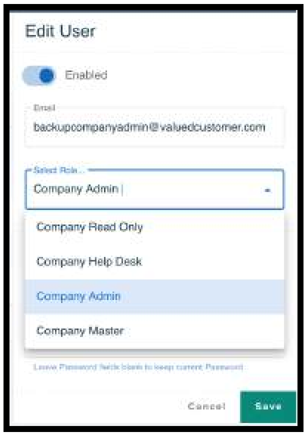
Leave Password fields blank to keep current Password

The user’s email address is now updated and this is the username the user needs to use when logging into the portal.

Update User Role

To update a user’s role:

- Search for the user account
- From the ellipsis menu in the right-hand column of the row, select Edit
- Select the desired role from the Role drop-down
- Click Save



Edit User

Enabled

Email: backupcompanyadmin@valuedcustomer.com

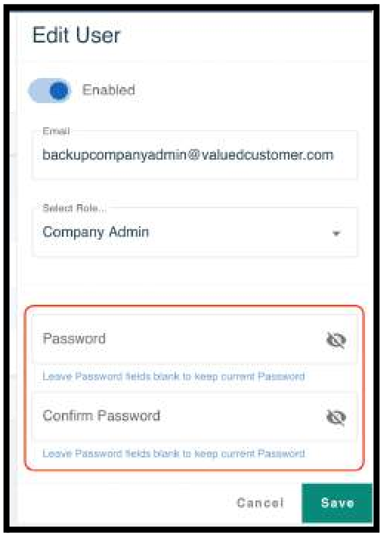
Select Role...: Company Admin

NOTE: please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

Update User Password

To update a user's password:

- Search for the user
- From the ellipsis menu in the right-hand column of the row, select Edit
- Enter the new password in both the Password and Confirm Password fields
- Click Save



Edit User

Enabled

Email: backupcompanyadmin@valuedcustomer.com

Select Role...: Company Admin

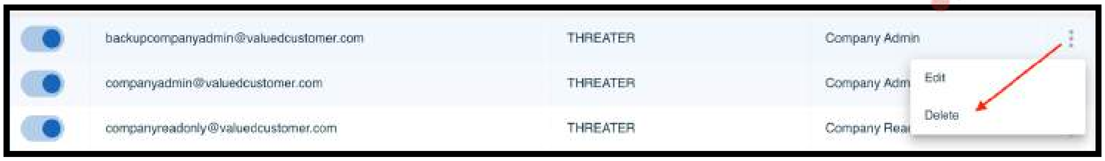
Password
Leave Password fields blank to keep current Password
Confirm Password
Leave Password fields blank to keep current Password
Cancel
Save

The user's password is now updated and this is the password the user will need to use when logging into the portal.

Delete Users

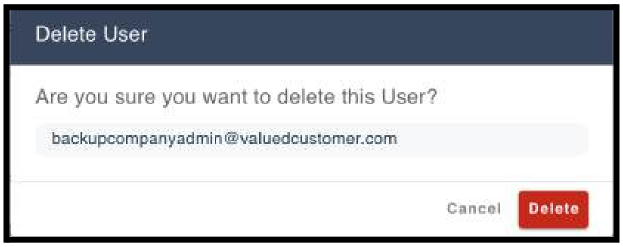
To delete a user:

- Search for the user
- From the ellipsis menu in the right-hand column of the row, select Delete



backupcompanyadmin@valuedcustomer.com	THREATER	Company Admin
companyadmin@valuedcustomer.com	THREATER	Company Adm
companyreadonly@valuedcustomer.com	THREATER	Company Rea

- On the Delete User confirmation modal, click the Delete button



Delete User

Are you sure you want to delete this User?

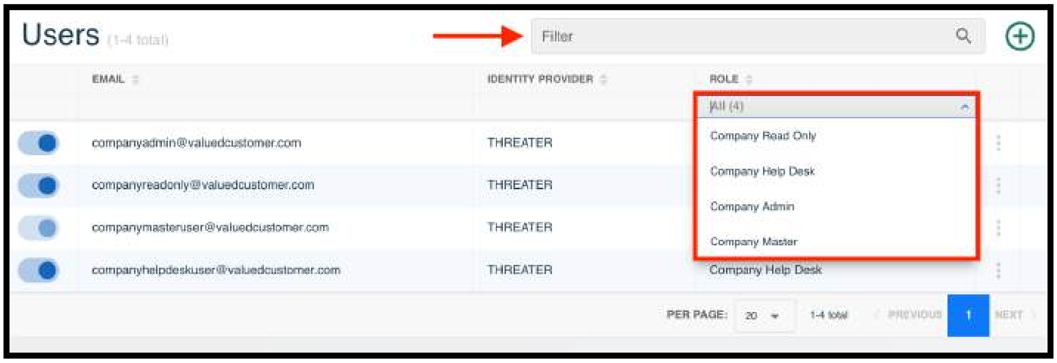
backupcompanyadmin@valuedcustomer.com

The user is now deleted and will not be able to access the admin console.

Users Filter

You can filter down to a user or set of users in the following ways:

- Roles - Selecting a user role from this drop-down will filter the table down to the users who are assigned the selected role.
- User Table Filter - Enter text in the Filter Table search bar in the top right corner of the screen and the table will update to display applicable results.

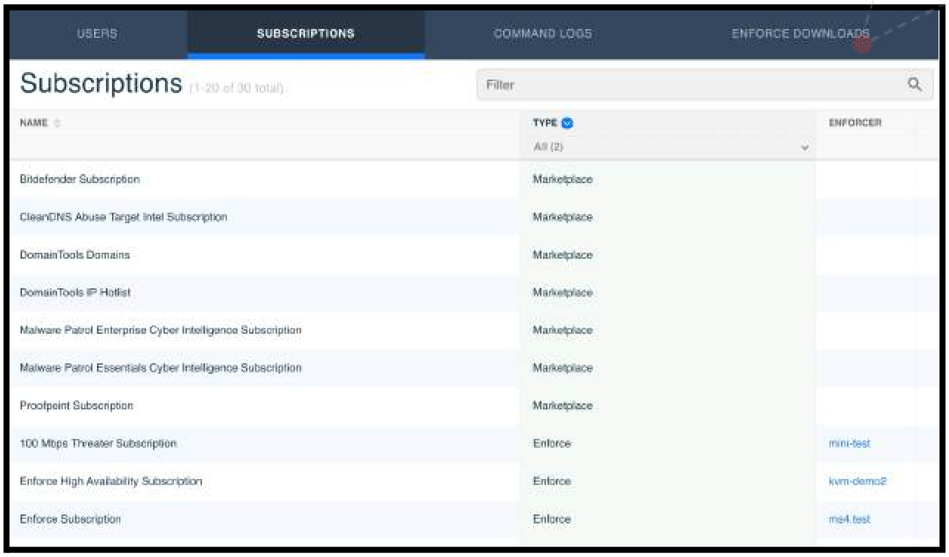


Users (1-4 total)

EMAIL	IDENTITY PROVIDER	ROLE
		All (4)
companyadmin@valuedcustomer.com	THREATER	
companyreadonly@valuedcustomer.com	THREATER	
companymasteruser@valuedcustomer.com	THREATER	
companyhelpdeskuser@valuedcustomer.com	THREATER	Company Help Desk

Subscriptions

The Subscriptions tab displays all threatER subscriptions that have been purchased. This includes Enforce and Marketplace subscriptions.



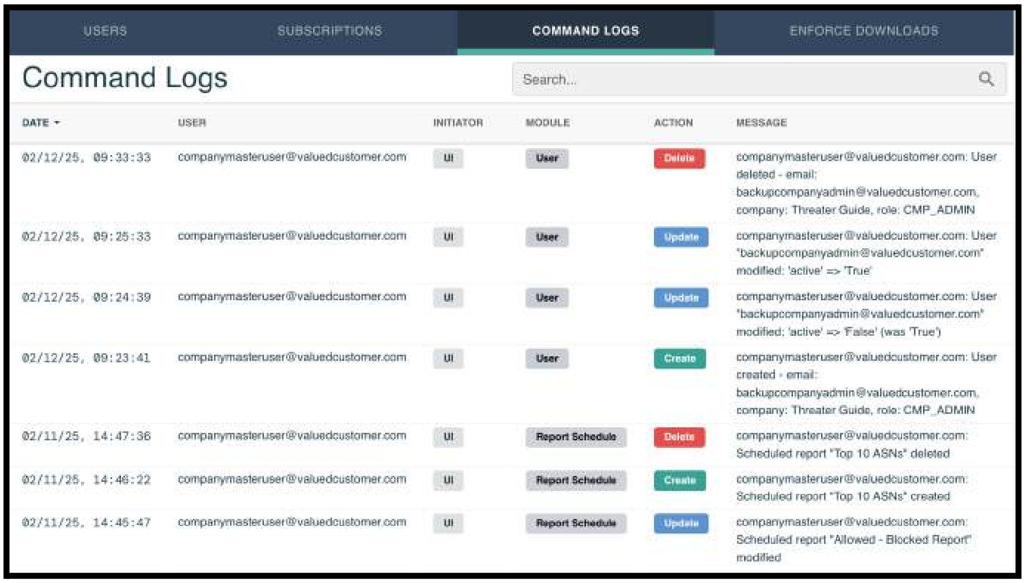
Subscriptions (1-20 of 30 total)

NAME	TYPE All (2)	ENFORCER
Bitdefender Subscription	Marketplace	
CleanDNS Abuse Target Intel Subscription	Marketplace	
DomainTools Domains	Marketplace	
DomainTools IP Hotlist	Marketplace	
Malware Patrol Enterprise Cyber Intelligence Subscription	Marketplace	
Malware Patrol Essentials Cyber Intelligence Subscription	Marketplace	
Proofpoint Subscription	Marketplace	
100 Mbps Threater Subscription	Enforce	mini-test
Enforce High Availability Subscription	Enforce	kvm-demo2
Enforce Subscription	Enforce	ms4.test

.

Command Logs

Command logs show a history of important actions taken by users of the system. These can be useful for auditing and troubleshooting any issues that arise.



Command Logs

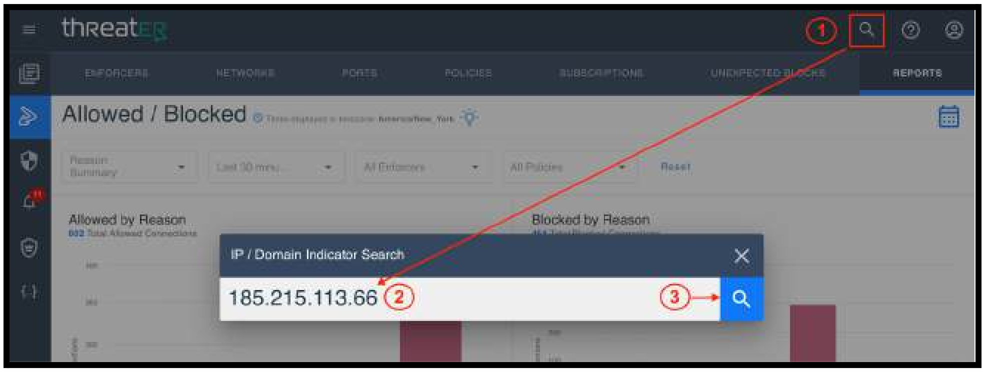
DATE	USER	INITIATOR	MODULE	ACTION	MESSAGE
02/12/25, 09:33:33	companymasteruser@valuedcustomer.com	UI	User	Delete	companymasteruser@valuedcustomer.com: User deleted - email: backupcompanyadmin@valuedcustomer.com, company: Threater Guide, role: CMP_ADMIN
02/12/25, 09:25:33	companymasteruser@valuedcustomer.com	UI	User	Update	companymasteruser@valuedcustomer.com: User "backupcompanyadmin@valuedcustomer.com" modified: 'active' => 'True'
02/12/25, 09:24:39	companymasteruser@valuedcustomer.com	UI	User	Update	companymasteruser@valuedcustomer.com: User "backupcompanyadmin@valuedcustomer.com" modified: 'active' => 'False' (was 'True')
02/12/25, 09:23:41	companymasteruser@valuedcustomer.com	UI	User	Create	companymasteruser@valuedcustomer.com: User created - email: backupcompanyadmin@valuedcustomer.com, company: Threater Guide, role: CMP_ADMIN
02/11/25, 14:47:36	companymasteruser@valuedcustomer.com	UI	Report Schedule	Delete	companymasteruser@valuedcustomer.com: Scheduled report "Top 10 ASNs" deleted
02/11/25, 14:46:22	companymasteruser@valuedcustomer.com	UI	Report Schedule	Create	companymasteruser@valuedcustomer.com: Scheduled report "Top 10 ASNs" created
02/11/25, 14:45:47	companymasteruser@valuedcustomer.com	UI	Report Schedule	Update	companymasteruser@valuedcustomer.com: Scheduled report "Allowed - Blocked Report" modified

IOC Search

The Indicator of Compromise (IOC) Search allows users to search any IP address or Domain to obtain valuable information about the indicator, such as whether it is included in available lists, as well as how it maps to policy decisions.

To perform a search:

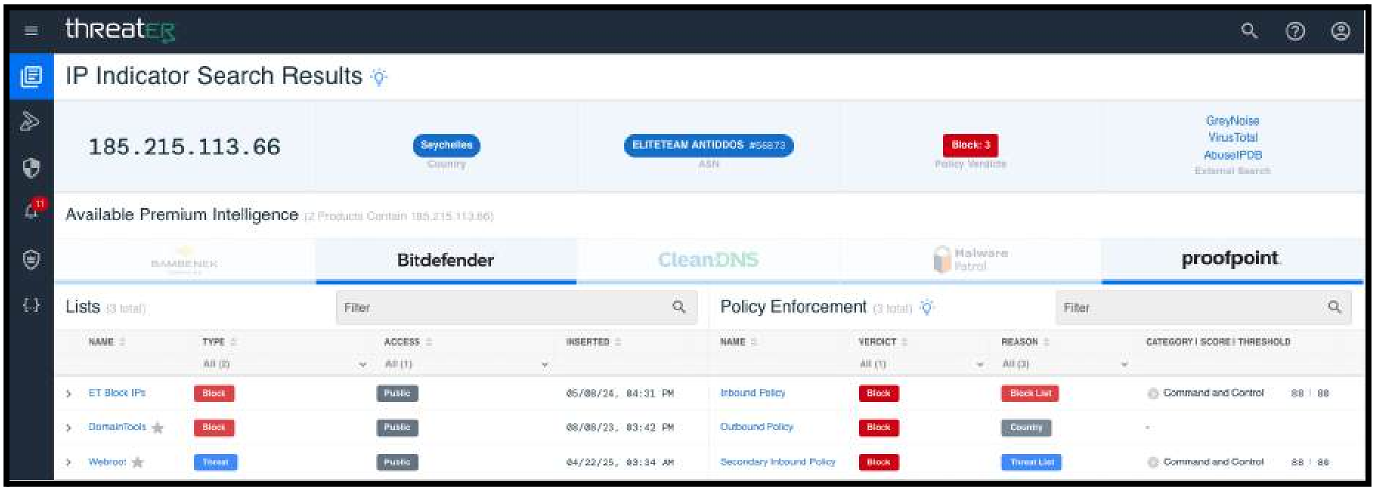
1. Click the spyglass icon in the top navigation bar
2. Enter an IP address or Domain
3. Click the search icon in the modal



IP / Domain Indicator Search

185.215.113.66

The IOC Search Results will display.



IP Indicator Search Results

185.215.113.66 | Seychelles (Country) | ELITETEAN ANTIDDOS #56873 (ASN) | Block: 3 (Policy Verdicts) | GreyNoise, VirusTotal, AbuseIPDB (External Search)

Available Premium Intelligence (2 Products Contain 185.215.113.66)

Lists (3 total)

NAME	TYPE	ACCESS	INSERTED
	All (2)	All (1)	
ET Block IPs	Block	Public	05/08/24, 04:31 PM
DomainTools	Block	Public	08/08/23, 03:42 PM
Webroot	Threat	Public	04/22/25, 03:34 AM

Policy Enforcement (3 total)

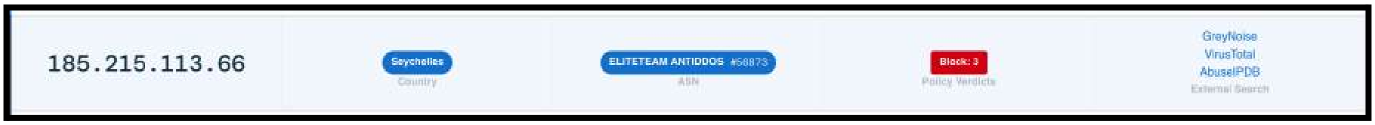
NAME	VERDICT	REASON	CATEGORY | SCORE | THRESHOLD
	All (1)	All (3)	
Inbound Policy	Block	Block List	Command and Control 88 | 88
Outbound Policy	Block	Country	-
Secondary Inbound Policy	Block	Threat List	Command and Control 88 | 88

IOC Results Header

The IOC Results Header will display the following:

- IOC
  - The IP or Domain that was entered in the search criteria
- Country
  - The country the IP originated from, if known
  - This will not display for domains
- ASN
  - The ASN the IP originated from, if known
  - This will not display for domains
- Policy Verdicts
  - A roll-up count of how your company's policies would enforce the IOC
- External Search URLs
  - Where applicable, the following URLs will display for you to conduct additional searches on the IOC via well-regarded third-party sources:
    - GreyNoise
    - VirusTotal
    - AbuseIPDB

IP Results Header Example:



185.215.113.66

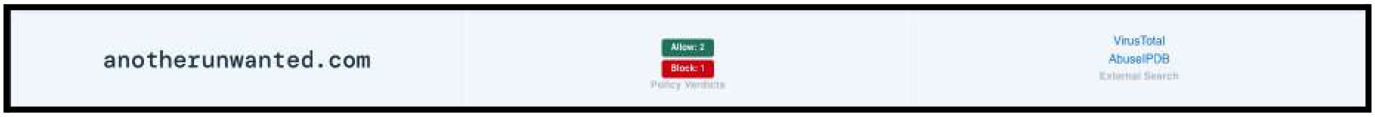
Seychelles
Country

ELITETEAM ANTIDDOS #58873
ASN

Block: 3
Policy Verdicts

GreyNoise
VirusTotal
AbuseIPDB
External Search

Domain Results Header Example:



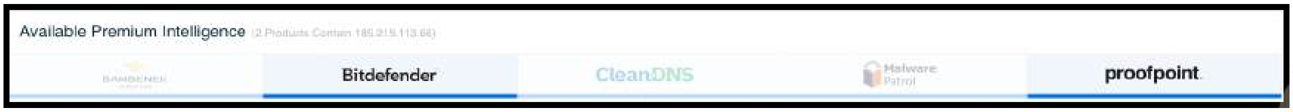
anotherunwanted.com

Allow: 2
Block: 1
Policy Verdicts

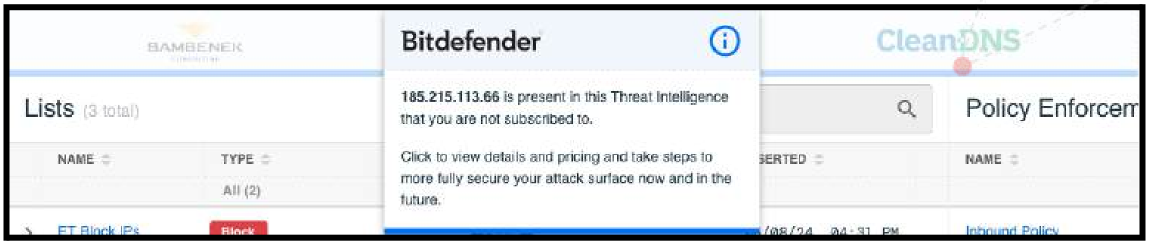
VirusTotal
AbuseIPDB
External Search

Available Premium Intelligence

Premium Intelligence products that your company is NOT subscribed to will display below the IOC Results Header. If the IOC was not found in a product's threat intelligence, it will be dimmed. If it was included the product will display in full color with a blue bar at the bottom. Scrolling over a product will provide that information to you, as well. You can click on any product to view more details and pricing and to take the necessary steps to purchase it in the threatER Marketplace.



Available Premium Intelligence (2 Products Contain 185.215.113.66)



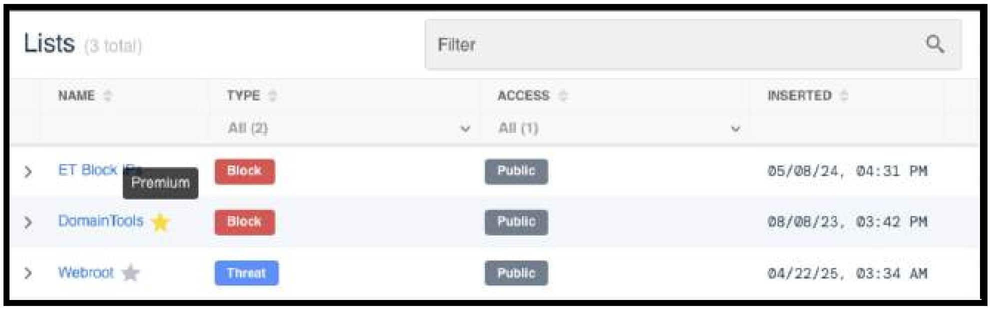
Bitdefender

185.215.113.66 is present in this Threat Intelligence that you are not subscribed to.

Click to view details and pricing and take steps to more fully secure your attack surface now and in the future.

Lists

The Lists panel will display all lists the IOC was found on at the time the search was performed. This includes all block, threat, and allow lists that are available to your company's account. The panel will include the list name, list type, and the timestamp the IOC was inserted on the list. For IPs found on Threat lists, the timestamp displayed is the earliest value for all associated entries. For domains, the timestamp displayed is the earliest value for the most specific match. A star next to a list name indicates it is a premium feed that is either included with your Enforce subscription, or was purchased by your company in the threatER Marketplace.

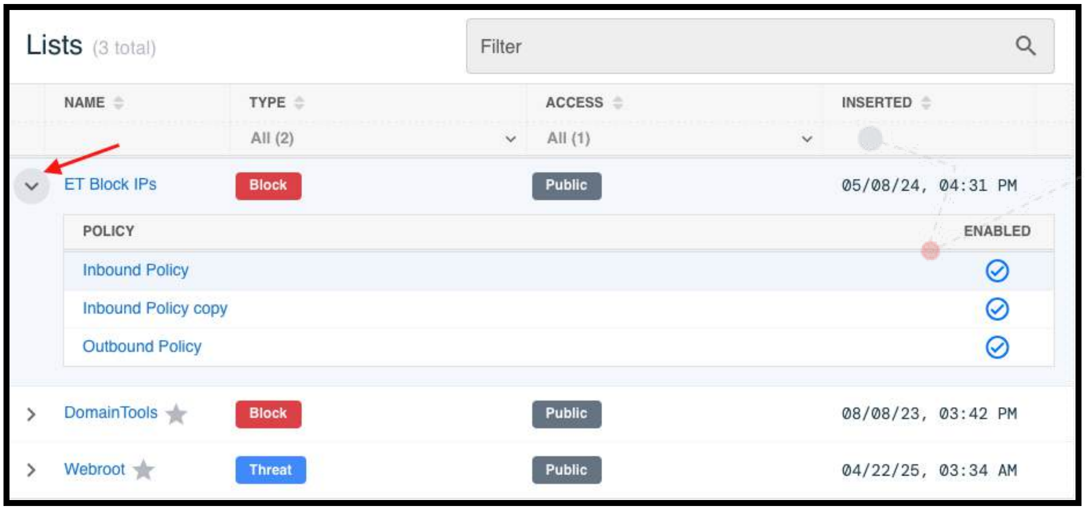


Lists (3 total)

Filter

NAME	TYPE	ACCESS	INSERTED
	All (2)	All (1)	
ET Block IPs ★	Block	Public	05/08/24, 04:31 PM
DomainTools ★	Block	Public	08/08/23, 03:42 PM
Webroot ★	Threat	Public	04/22/25, 03:34 AM

To view the list's enabled state on your company's policies, expand the chevron to the left of the list name. Every policy on your account will display and a check mark will display to the right of it if the list is enabled on that policy.



Lists (3 total)

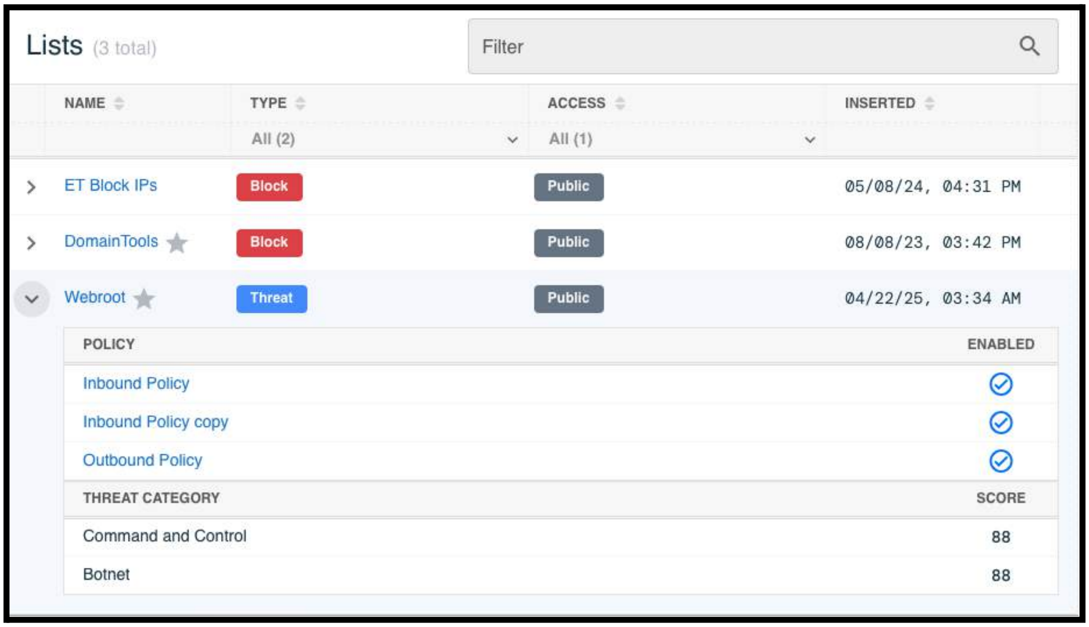
Filter

NAME	TYPE	ACCESS	INSERTED
	All (2)	All (1)	
ET Block IPs	Block	Public	05/08/24, 04:31 PM

POLICY	ENABLED
Inbound Policy	✓
Inbound Policy copy	✓
Outbound Policy	✓

NAME	TYPE	ACCESS	INSERTED
DomainTools ★	Block	Public	08/08/23, 03:42 PM
Webroot ★	Threat	Public	04/22/25, 03:34 AM

For threat lists, an additional table will display below the Policy table and include the Threat Category(s) and Score(s) of the IP.



Lists (3 total)

Filter

NAME	TYPE	ACCESS	INSERTED
	All (2)	All (1)	
ET Block IPs	Block	Public	05/08/24, 04:31 PM
DomainTools ★	Block	Public	08/08/23, 03:42 PM
Webroot ★	Threat	Public	04/22/25, 03:34 AM

POLICY	ENABLED
Inbound Policy	✓
Inbound Policy copy	✓
Outbound Policy	✓

THREAT CATEGORY	SCORE
Command and Control	88
Botnet	88

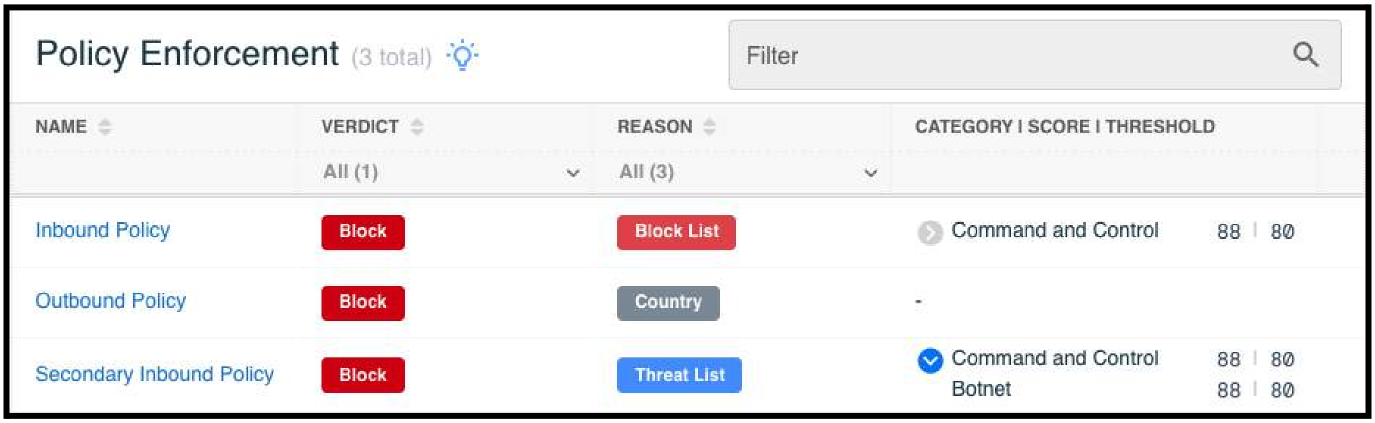
Policy Enforcement

The Policy Enforcement panel will display all policies on your account and how that policy would enforce the IOC. Each policy row will display the Policy Name, Verdict of the IOC on that policy (block or allow), and the Reason for the Verdict, which will be one of the following:

- Allow List – IOC is included on an Allow list that is enabled on the policy
- ASN – IOC is included in an ASN that is set to “allow” or “block” on the policy

- Block List – IOC is included on a Block list that is enabled on the policy
- Country – IOC originates from a Country that is blocked on the policy
- Threat list – IOC is included on a Threat list that is enabled on the policy
- Policy – IOC was allowed because it was not specifically allowed or blocked on the policy, based on the criteria outlined above in one of the 5 other reasons

If the IOC was included on a Threat list, the threat Category and Score will display, as well as the Threshold setting for that category on each policy. If the IOC was flagged as more than one Threat Category, a chevron will display next to the first Category name listed. You can expand the chevron to view the other Threat Categories, Scores, and Threshold settings.



Policy Enforcement (3 total)

Filter

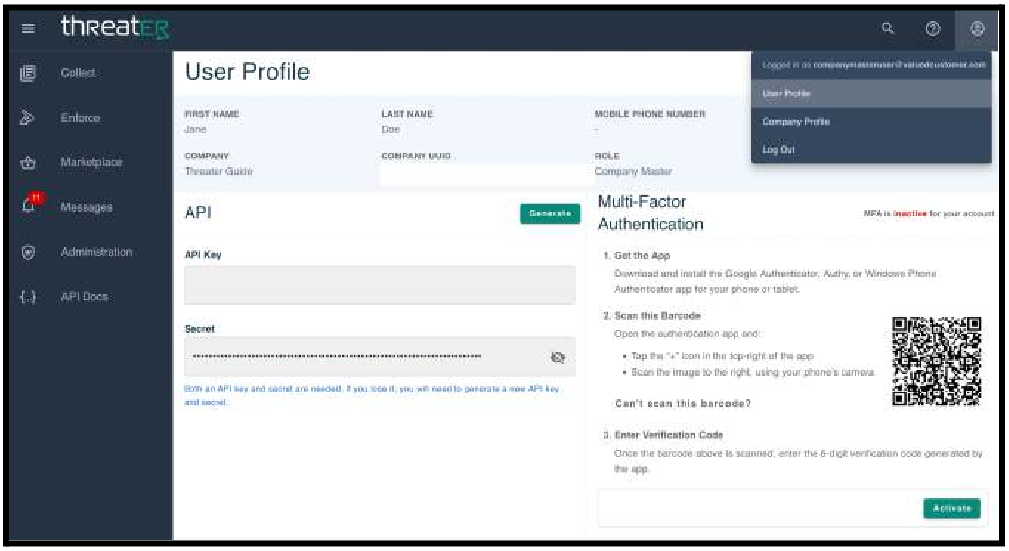
NAME	VERDICT	REASON	CATEGORY I SCORE I THRESHOLD
	All (1)	All (3)	
Inbound Policy	Block	Block List	Command and Control 88 I 80
Outbound Policy	Block	Country	-
Secondary Inbound Policy	Block	Threat List	Command and Control 88 I 80 Botnet 88 I 80

NOTE: Previous versions of the API endpoint for this feature have been deprecated. When directly using the API, please use our v6 endpoints:

- https://portal.threater.com/api/v6/search/ioc/domain/{domain}
- https://portal.threater.com/api/v6/ip{ip}

User Profile

The User Profile is where users can update their contact information, change their password, generate an API Key, and enable Multi-Factor Authentication. The User Profile is accessible by selecting the person icon in the top-right navigation bar and then selecting User Profile.



User Profile

FIRST NAME
Jane

LAST NAME
Doe

MOBILE PHONE NUMBER
-

COMPANY
Threater Guide

COMPANY UUID

ROLE
Company Master

API

API Key

Secret

Both an API key and secret are needed. If you lose it, you will need to generate a new API key and secret.

Multi-Factor Authentication

MFA is inactive for your account

1. Get the App

Download and install the Google Authenticator, Authy, or Windows Phone Authenticator app for your phone or tablet.

2. Scan this Barcode

Open the authentication app and:

- Tap the "+" icon in the top-right of the app
- Scan the image to the right, using your phone's camera

Can't scan this barcode?

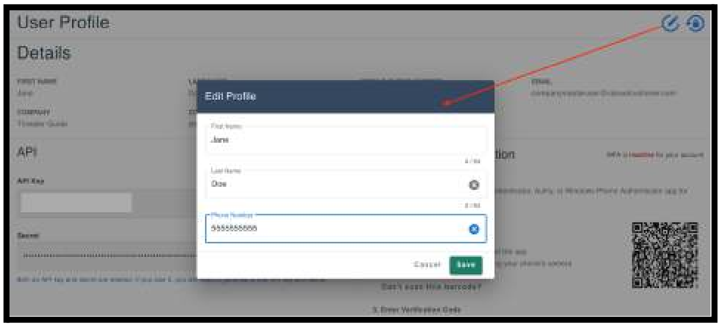
3. Enter Verification Code

Once the barcode above is scanned, enter the 6-digit verification code generated by the app.

User Details

The User Details section is where users can view and edit their profile details. To edit your profile:

- Click the pencil icon
- Enter the following optional information:
  - First Name
  - Last Name
  - Phone Number
- Click Save



First Name
Jane

Last Name
Doe

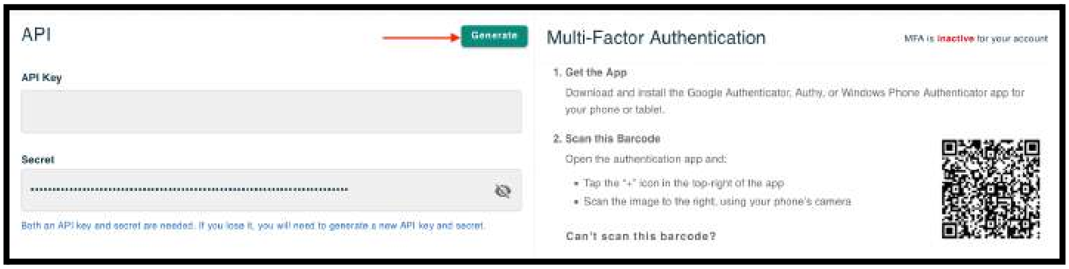
Phone Number
5555555555

Email and Role updates cannot be made on the User Profile. To update either of these, please contact your Company Master account.

API Key

If API Access is allowed for your company, you can generate an API Key for API endpoint authorization.

To generate an API Key, click the Generate button in the API Key section.



API

API Key

Secret

••

Both an API key and secret are needed. If you lose it, you will need to generate a new API key and secret.

Multi-Factor Authentication

MFA is inactive for your account

1. Get the App

Download and install the Google Authenticator, Authy, or Windows Phone Authenticator app for your phone or tablet.

2. Scan this Barcode

Open the authentication app and:

- Tap the "+" icon in the top-right of the app
- Scan the image to the right, using your phone's camera

Can't scan this barcode?

An API Key and Secret will be generated. Both are needed and should be maintained securely for API use. If the API Key and Secret are lost at any point, a new one will need to be generated. If API Access is not enabled for your company, this section will not display on the User Profile. If API Access is desired, please contact your Company Master account.

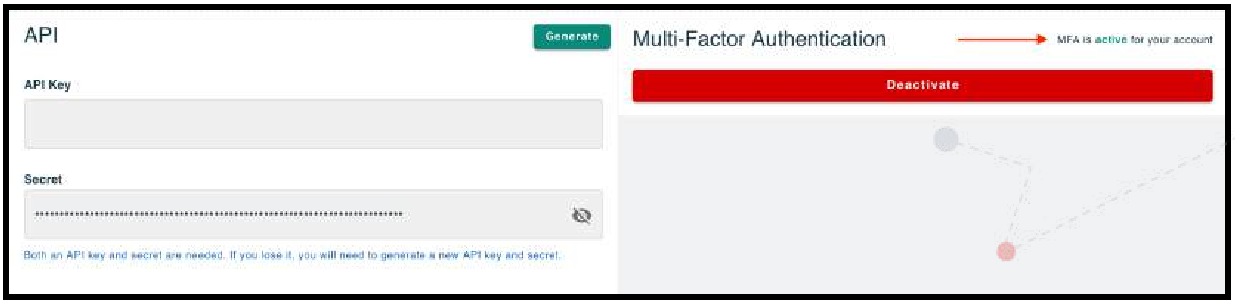
Multi-Factor Authentication (MFA)

MFA for Individual Account

MFA can be enabled for your individual account, if it is not required by your company by default. To enable MFA for your account:

- Download and install one of the following apps on your phone or tablet:
  - Google Authenticator
  - Twilio Authy
  - Windows Phone Authenticator
- Open the app of your choice and scan the barcode on the User Profile screen using the camera on your phone or tablet.
- Enter the Verification Code and click the Activate button

MFA is now active for your account and will be reflected as so on your User Profile. When logging in from this point forward, you will be prompted to enter a passcode after entering a valid username and password.



API

API Key

Secret

••

Both an API key and secret are needed. If you lose it, you will need to generate a new API key and secret.

Multi-Factor Authentication

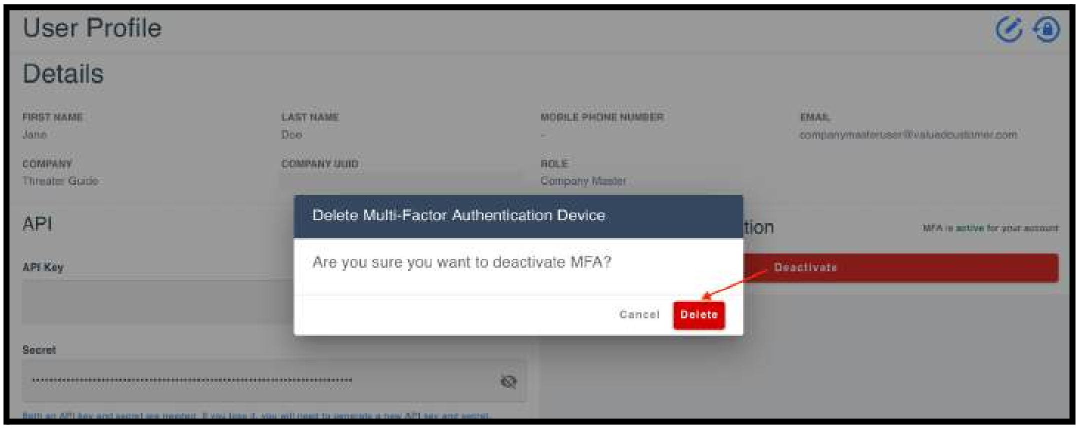
MFA is active for your account

When MFA is active, you will be prompted to provide a code from the authentication app you used to activate MFA each time you login to the portal.

Deactivate MFA

If MFA is not required by your company, you can deactivate it for your individual account. To deactivate MFA:

- Navigate to your User Profile
- Click the Deactivate button in the MFA panel
- On the Delete MFA confirmation modal, click the Delete button



User Profile

Details

FIRST NAME: Jane

LAST NAME: Doe

MOBILE PHONE NUMBER: -

EMAIL: companymasteruser@valuedcustomer.com

COMPANY: Threater Guide

COMPANY UUID

ROLE: Company Master

API

API Key

Secret

••

MFA is active for your account

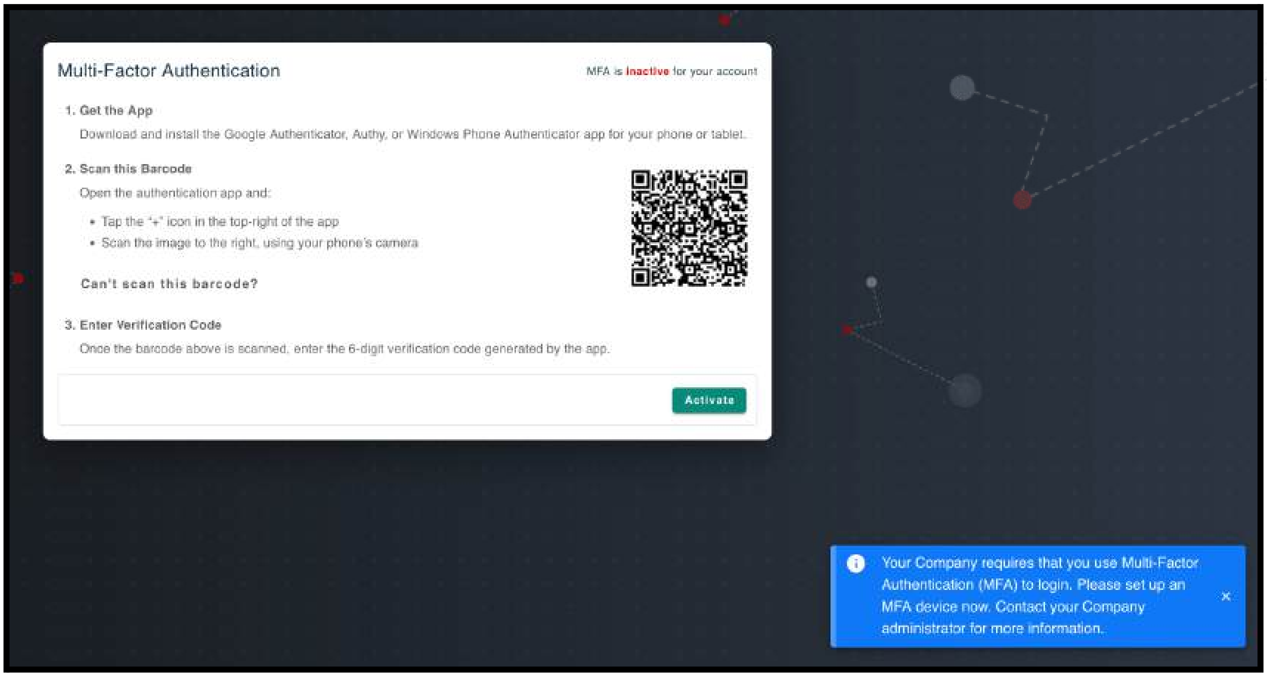
Delete Multi-Factor Authentication Device

Are you sure you want to deactivate MFA?

MFA is now inactive for your account. The next time you login to the portal you will not be prompted to enter a passcode.

MFA Required by Company

If MFA is required by your company, you will be required to set up MFA for your account. After entering your username and password and selecting Sign On on the login screen, you will be directed to set up MFA for your account.



Multi-Factor Authentication

MFA is Inactive for your account

1. Get the App

Download and install the Google Authenticator, Authy, or Windows Phone Authenticator app for your phone or tablet.

2. Scan this Barcode

Open the authentication app and:

- Tap the "+" icon in the top-right of the app
- Scan the image to the right, using your phone's camera

Can't scan this barcode?

3. Enter Verification Code

Once the barcode above is scanned, enter the 6-digit verification code generated by the app.

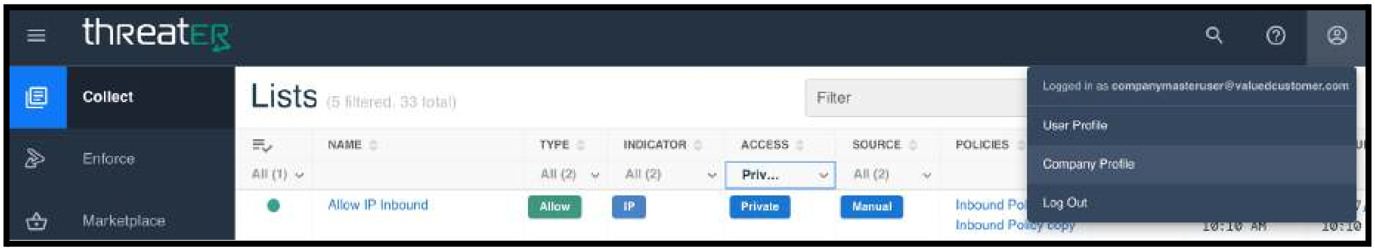
Your Company requires that you use Multi-Factor Authentication (MFA) to login. Please set up an MFA device now. Contact your Company administrator for more information.

- Download and install one of the following apps on your phone or tablet:
  - Google Authenticator
  - Twilio Authy
  - Windows Phone Authenticator
- Open the app of your choice and scan the barcode on the User Profile screen using the camera on your phone or tablet
- Enter the Verification Code and click the Activate button

MFA is now active for your account and will be reflected to the login screen. After entering a valid username and password, you will be prompted to enter a passcode from the authentication app. For every future login you will be prompted to enter a passcode after entering a valid username and password.

Company Profile

The Company Profile is only accessible to Company Master accounts and is where company-level settings can be made. The Company Profile is accessible by selecting the person icon in the top-right navigation bar and then selecting Company Profile.



Logged in as companymasteruser@valuedcustomer.com

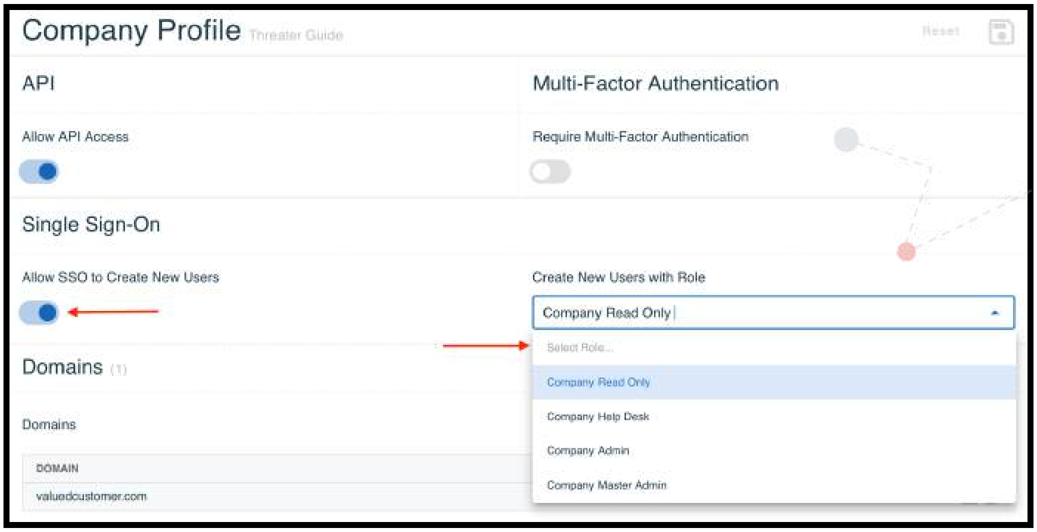
Single Sign-On (SSO)

If your company subscribes to Google Workspace and your company's domain is registered to Google Workspace, you can now log into the portal via SSO with Google. In addition to the standard SSO, Company Master accounts can configure your company to allow for new user creation via SSO. Properly configuring this setting allows new users to be created via SSO on the login screen when matched to one or more allowed domains.

Note that most customers will likely **not** want to enable this feature, since anyone with a valid domain credential would be able to log into the system, which is often undesirable for access to security controls such as threatER. However, it may be useful for some security organizations to allow employees to have the ability to create accounts quickly without having to bother a Company Master to do so.

To allow new users to be created via SSO, a Company Master should:

- Navigate to the Company Profile
- Toggle On the "Allow SSO to Create New Users" setting
- Select the User Role the new user will be created as
  - Read Only is **strongly** recommended
  - User permissions can be updated at a later time


Company Profile Threater Guide

API

Allow API Access: on

Multi-Factor Authentication

Require Multi-Factor Authentication: off

Single Sign-On

Allow SSO to Create New Users: on

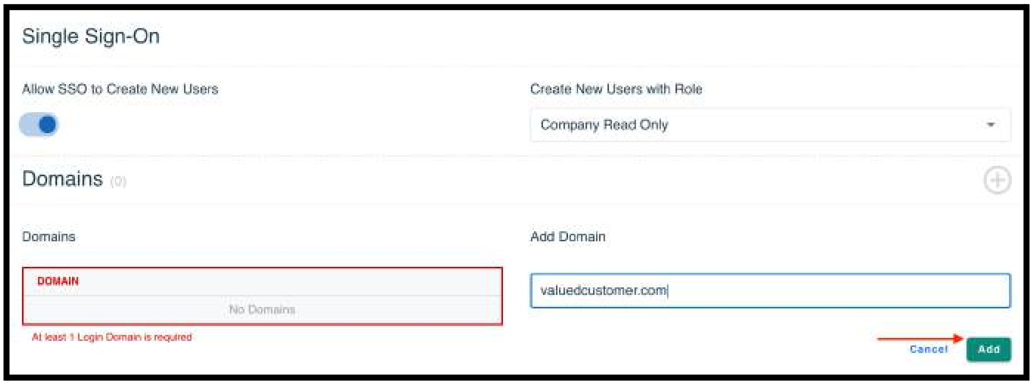
Create New Users with Role: Company Read Only

Domains (1)

Domains

DOMAIN
valuedcustomer.com

- Enter the applicable email domain(s). Anyone with a valid login to the specified domain as registered with the SSO provider (in this case, the associated Google Workspace domain) will be able to create an account on the system.
- Click the Add button


Single Sign-On

Allow SSO to Create New Users: on

Create New Users with Role: Company Read Only

Domains (0)

Domains

DOMAIN
No Domains

At least 1 Login Domain is required

Add Domain: valuedcustomer.com

- Click Save in the top right corner

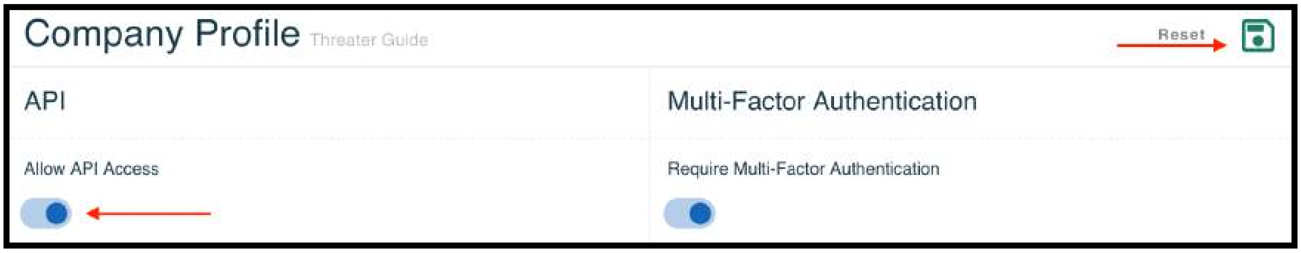
Once this setting is properly configured, the Company Master can direct their new users to:

- Navigate to the login screen
- Click "Sign On with Google"
- Follow the prompts

API

To allow users to use the portal API endpoints, Company Masters must turn on API access. To do this, a Company Master should:

- Navigate to the Company profile
- Toggle on "Allow API Access"
- Click the Save button in the top right corner



Company Profile Threater Guide

API

Allow API Access

Multi-Factor Authentication

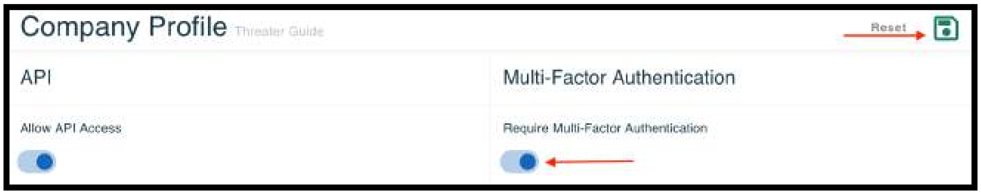
Require Multi-Factor Authentication

Each user will now have the ability to generate an API Key on their individual user profile. The generated API Key will give the user access to the API endpoints with the permissions their account is setup with (i.e. Company Help Desk).

Multi-Factor Authentication (MFA)

Company Masters can choose to require all users of their company to use MFA when logging in. To require MFA for your company, a Company Master should:

- Navigate to the Company Profile
- Toggle on "Require Multi-Factor Authentication"
- Click the Save button in the top right corner



Company Profile Threater Guide

API

Allow API Access

Multi-Factor Authentication

Require Multi-Factor Authentication

All users of your company will be required to set up MFA for their account. Please see the MFA Required by Company section for additional details.

Appendix

User Roles and Permissions

CMP Roles & Permissions				
	Read Only	Help Desk	Admin	Master
COLLECT				
LISTS				
View Lists	X	X	X	X
Create Lists			X	X
Edit Lists			X	X
Delete Lists			X	X
Export Lists			X	X
ENFORCE				
ENFORCERS				
View Enforcers	X	X	X	X
Edit Enforcer Name/Location			X	X
Manage Subscriptions			X	X
View Available Software	X	X	X	X
Update Software			X	X
Update Enforce Configurations			X	X
NETWORKS				
View Networks	X	X	X	X
Create Networks			X	X
Edit Networks			X	X
Delete Networks			X	X
PORTS				
View Ports	X	X	X	X

Create Ports			X	X
Edit Ports			X	X
Delete Ports			X	X
POLICIES				
View Policies	X	X	X	X
Create Policies			X	X
Edit Policy Settings			X	X
Delete Policies			X	X
Duplicate Policies			X	X
SUBSCRIPTIONS				
View Subscriptions	X	X	X	X
Manage Subscriptions			X	X
UNEXPECTED BLOCKS				
Submit and View Log Analysis	X	X	X	X
Add IP to Allow List(s)			X	X
REPORTS				
View Reports	X	X	X	X
View Scheduled Reports	X	X	X	X
Schedule Reports			X	X
Edit Scheduled Reports			X	X
Delete Scheduled Reports			X	X
MARKETPLACE				
View Products	X	X	X	X
View Product Details	X	X	X	X
Subscribe to a Product				X
MESSAGES				
View Messages	X	X	X	X
Delete Messages	X	X	X	X

ADMINISTRATION				
USERS (see User Management tabs for a more detailed breakdown)**				
View Users	X	X	X	X
Create User				X
Edit Users			X	X
Delete Users				X
SUBSCRIPTIONS				
View Subscriptions	X	X	X	X
COMMAND LOGS				
View Command Logs	X	X	X	X
ENFORCE DOWNLOADS				
Manual Downloads	X	X	X	X
COMPANY PROFILE				
Allow SSO to Create New Users				X
Allow API Access				X
Require MFA for Company				X

User Management

		View	Create	Edit	Delete
CMP Master	CMP Read Only	X	X	X	X
	CMP Help Desk	X	X	X	X
	CMP Admin	X	X	X	X
	CMP Master	X	X	X	X
CMP Admin	CMP Read Only	X		X	
	CMP Help Desk	X		X	
	CMP Admin	X		X	
	CMP Master	X			
CMP Help Desk	CMP Read Only	X			
	CMP Help Desk	X			

	CMP Admin	X			
	CMP Master	X			
CMP Read Only	CMP Read Only	X			
	CMP Help Desk	X			
	CMP Admin	X			
	CMP Master	X			