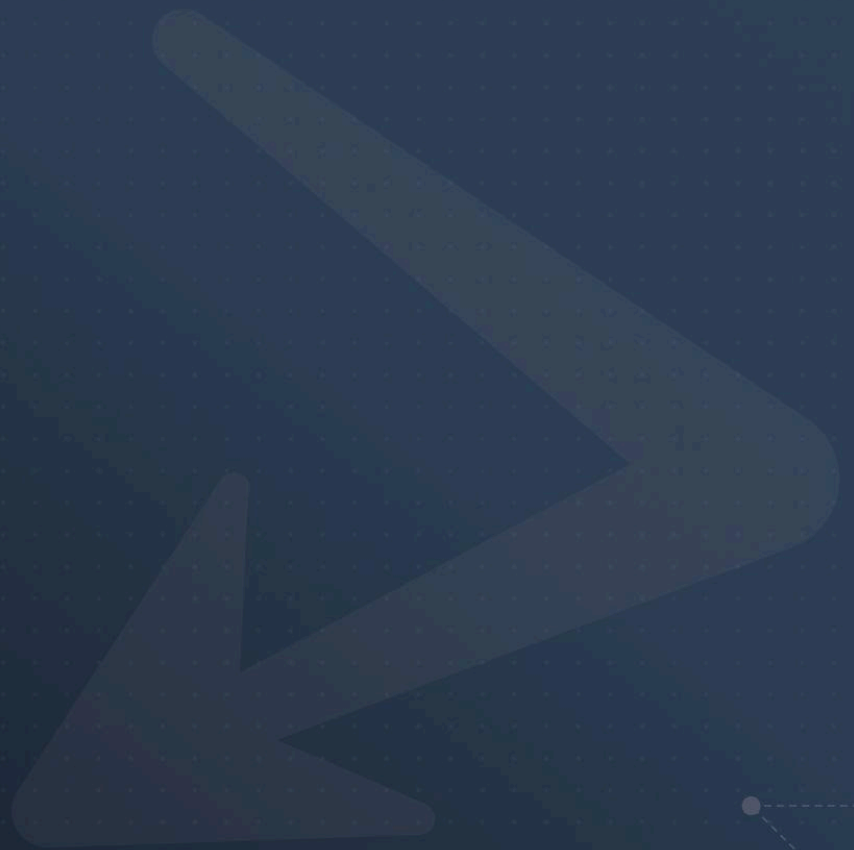




# threatER Portal

User Guide, June 2024



<b>Collect</b>	<b>4</b>
<b>Lists</b>	<b>4</b>
<b>List Types</b>	<b>5</b>
Allow Lists	5
Block Lists	6
Threat Lists	6
<b>List Creation</b>	<b>7</b>
Creating IP Threat Lists	7
Creating Manual IP Allow & Block Lists	7
List Details	7
Add Entries	8
Apply to Policies	11
Create New Policy During List Creation	11
Creating Manual Domain Lists	12
List Details	12
Add Entries	13
Adding & Removing Manual List Entries	15
Editing all List Components	18
Deleting a List	20
<b>Enforce</b>	<b>22</b>
<b>Enforcers</b>	<b>22</b>
<b>Enforce Configuration</b>	<b>24</b>
Settings	24
Syslog	26
Access	27
Bridges	29
NTP	29
<b>Enforce Software</b>	<b>33</b>
Update Now	34
Schedule Update	35
Cancel a Scheduled Update	36
Revert to Previous Build	37
Manual Downloads	39
<b>Subscription Management</b>	<b>39</b>
Editing Enforcer Name and Location	41
Subscription Throughput	41
<b>Networks</b>	<b>42</b>
Creating Networks	43
Network Details	43

Inbound/Outbound	44
Create New Policy During Network Creation	46
IPs	46
Editing a Network	48
Deleting a Network	50
Ports	51
Adding Ports	51
Editing Ports	53
Deleting Ports	53
<b>Policies</b>	<b>54</b>
Create a Policy	54
Policy Details	55
<b>IPs by Country</b>	<b>55</b>
Reserved and Unassigned IPs	57
<b>IPS by ASN</b>	<b>57</b>
Risk Thresholds	58
Best Practice Recommendation for Risk Thresholds:	60
Lists	61
Best Practice Recommendation for Lists:	61
Creating an Allow All Policy	62
Edit a Policy	62
Delete a Policy	63
<b>Subscriptions</b>	<b>64</b>
<b>Unexpected Blocks</b>	<b>66</b>
<b>Reports</b>	<b>69</b>
Allowed/Blocked	70
Reason Summary	71
Category Summary	73
Top 10 Countries	74
Top 10 ASNs	75
Top 10	77
Countries by Threat Category	77
ASNs by Threat Category	77
Scheduled Reports	78
Editing Scheduled Reports	80
Disabling Scheduled Reports	82
Deleting Scheduled Reports	82
<b>Marketplace</b>	<b>84</b>
Included with Enforce Products	84
Premium Intelligence Products	85



Services	86
<b>Administration</b>	<b>87</b>
Users	87
Create New User	87
Edit User Accounts	88
Disable an Account	88
Enable an Account	89
Update User Email	90
Update User Role	90
Update User Password	91
Delete Users	92
Users Filter	92
Subscriptions	93
<b>Command Logs</b>	<b>93</b>
<b>IOC Search</b>	<b>94</b>
<b>User Profile</b>	<b>95</b>
User Details	95
API Key	96
Multi-Factor Authentication (MFA)	96
MFA for Individual Account	96
Deactivate MFA	97
MFA Required by Company	98
<b>Company Profile</b>	<b>99</b>
Single Sign-On (SSO)	100
API	101
Multi-Factor Authentication (MFA)	102
<b>Appendix</b>	<b>103</b>
User Roles and Permissions	103
User Management	106



# 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.

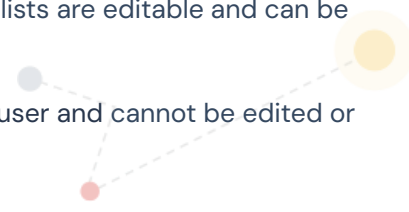
## Lists

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

NAME	TYPE	INDICATOR	SOURCE	ACCESS	POLICIES	COUNT	LAST SYNC	LAST UPDATE	DESCRIPTION
Akamai	Allow	IP	CSV File Connector	Public	None	19	10/25/23, 02:00 PM	02/13/23, 04:44 PM	Akamai curated by Greynoise
Amazon Cloudfront	Allow	IP	CSV File Connector	Public	None	144	10/25/23, 02:02 PM	07/10/23, 05:56 PM	Amazon Cloudfront curated by Greynoise
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	2,672	10/25/23, 02:14 PM	10/25/23, 02:14 PM	Machine Learning - Malware Domain feed
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,426	10/25/23, 01:29 PM	10/25/23, 01:29 PM	Machine Learning - Phishing Domain feed
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,042	10/25/23, 01:51 PM	10/25/23, 01:51 PM	Dec 20 2.23 pm
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	718	10/25/23, 02:00 PM	10/25/23, 02:00 PM	Bitdefender Command and Control (C2) IPs Feed
Bitdefender Malicious-do...	Block	Domain	Bitdefender	Public	None	401,593	10/25/23, 01:54 PM	10/25/23, 01:54 PM	Dec 20 2.23 pm

The table contains the following details on each List Type:

- List Name
- Health State
  - Healthy – if a list is in this state, a green pip will display to the left of the list name
  - Needs Attention – if a list needs attention, a red pip will display to the left of the list name. When a list is in this state, the configuration of the list should be checked to ensure all settings are correct.
- Indicator – will display the Indicators contained in the list (IP or Domain)
- 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.)

- 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
  - 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
  - Last Update – This is the last time the content of the list was modified
  - Description
- 

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.
  - If you are unable to enable domain lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists 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.
- If you are unable to enable domain lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists 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.
- If you are unable to enable threat lists per policy, please make sure your Enforcers all have the latest Enforce software installed. If any Enforcer is running a version previous to Enforce Build 214, please update immediately to enable domain lists 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

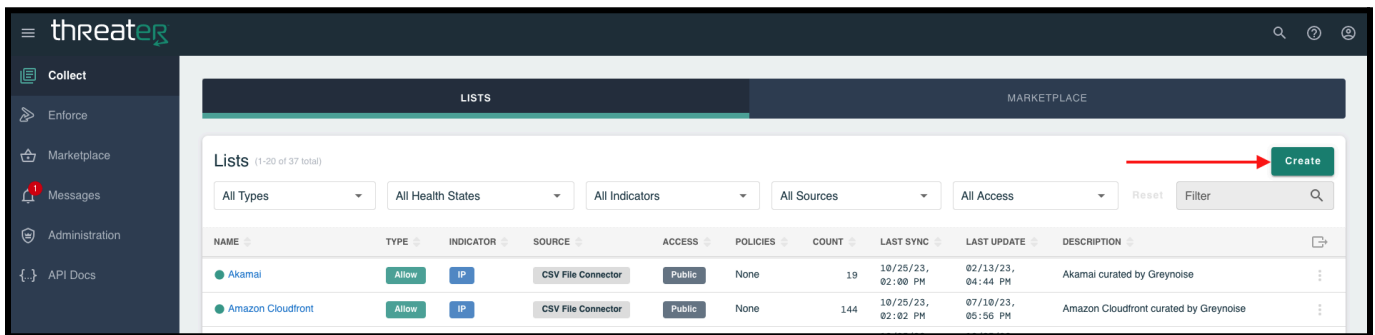
Currently, threatER does not support Manual Threat Lists, or Threat Domain lists. The application does support the following Threat IP Plugins:

- [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
- Select the Lists tab
- Select the “Create” button in the top-right corner



## 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, select the Next button to proceed to the Add Entries step.

### Create List

Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be blocked or allowed, depending on the list type, per the Policy it is assigned to.

1  
LIST DETAILS

2  
ADD ENTRIES

3  
APPLY TO POLICIES

#### Manual IP Allow List Details

Name  
Customer IP Allow List 22 / 64

Source  
Manual

List Type  
Allow

Indicator  
IP

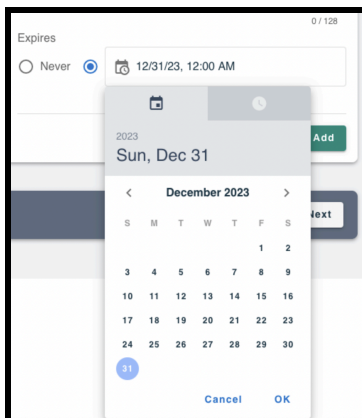
Description  
List of IPs to Allow 20 / 128

Next

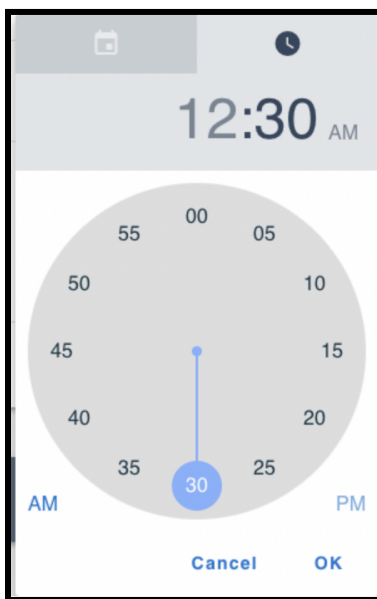
## Add Entries

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:
    - Select the radio button next to the timestamp field
    - Select a date from the calendar

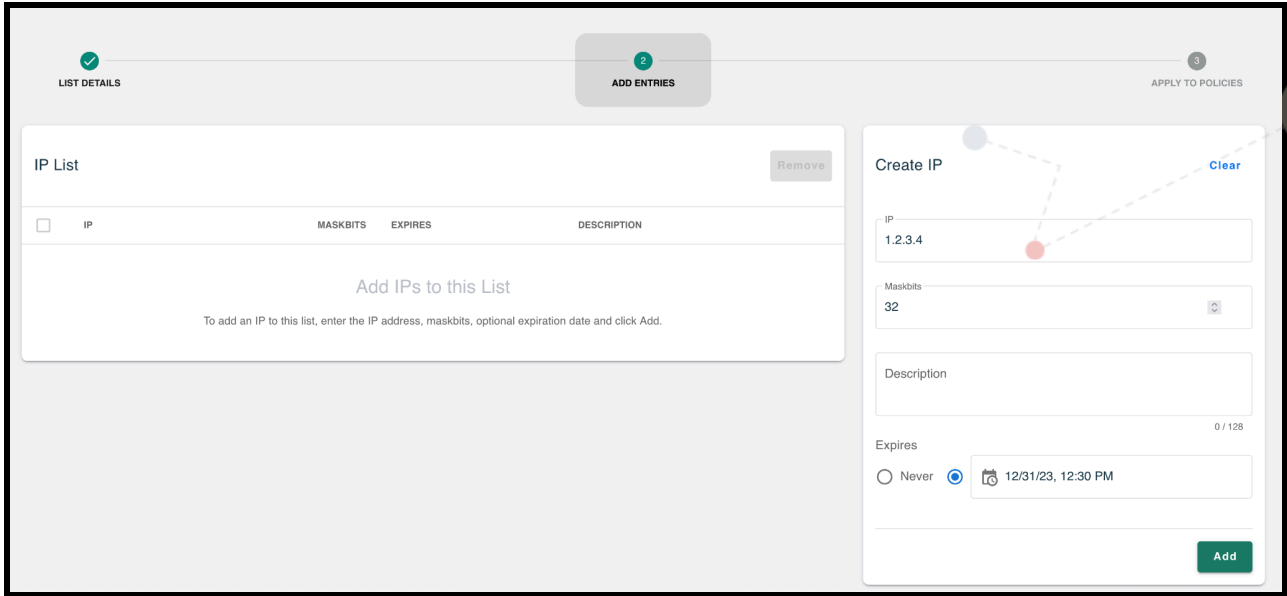


- Click on the clock tab and move the dial to the hours setting that is desired
- Move the dial to the minutes setting that is desired and click OK



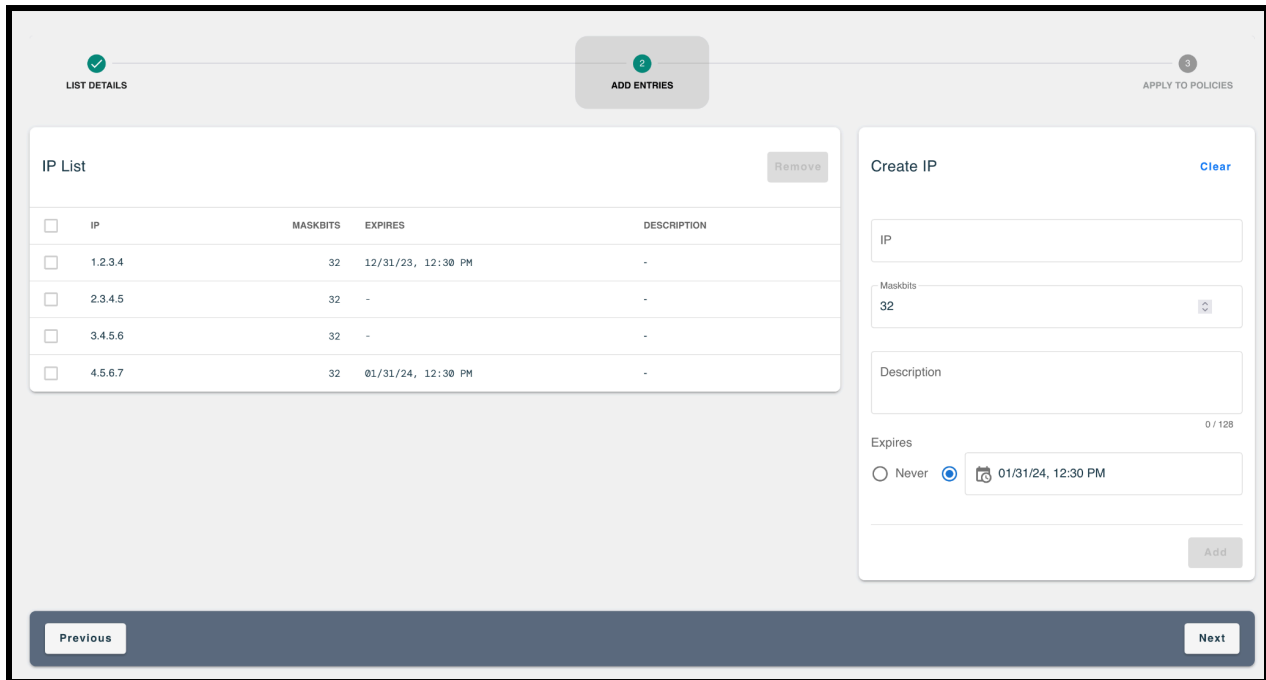
- Select the Add button to add the IP to the list





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

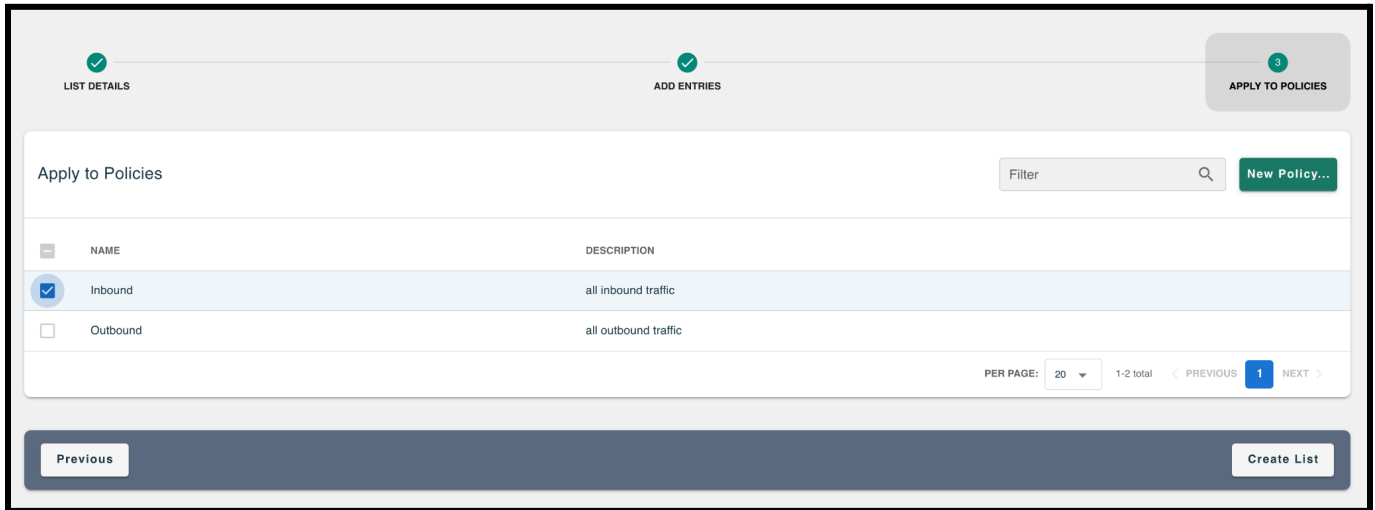
Once all IPs are added, select the Next button to proceed to the Apply to Policies step.



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

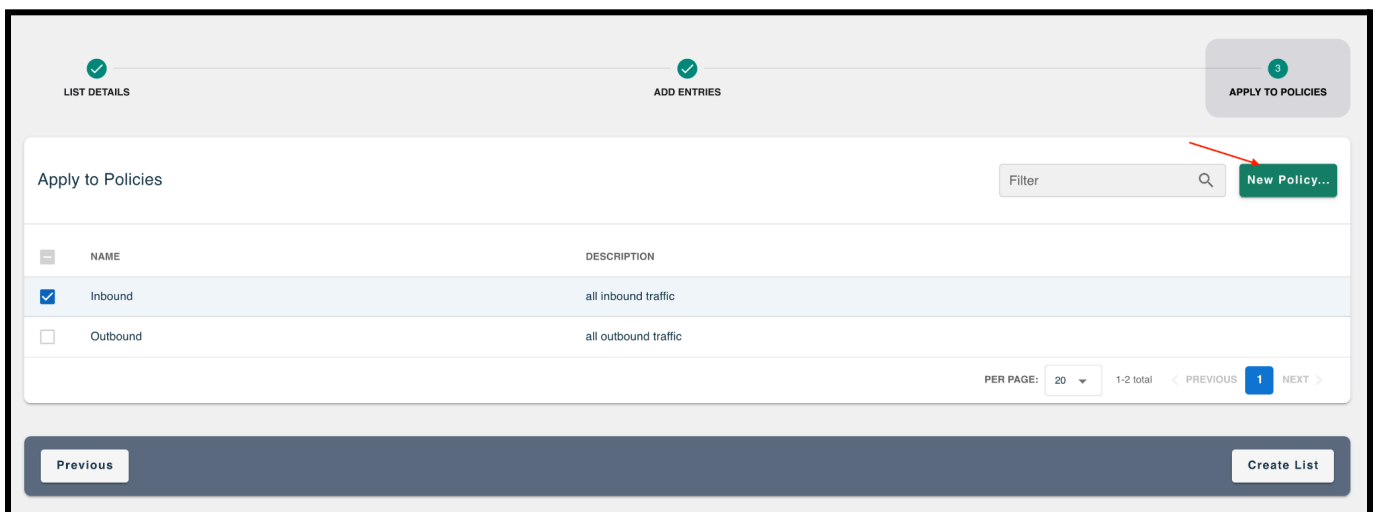
## Apply to Policies

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, select the applicable policies. Once all desired selections are made, select the Create List button to create the List.



## 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, select the "New Policy..." button on the Apply to Policies step and then follow the steps to create a policy, outlined above in the Policies section of this document.



## Creating Manual Domain Lists

To create a manual Domain list:

- Navigate to Collect in the left-hand navigation menu
- Select the Lists tab
- Select the “Create” button in the top-right corner



LISTS										MARKETPLACE
Lists (1-20 of 38 total)										Create
All Types	All Health States	All Indicators	All Sources	All Access	Reset	Filter	Filter	Filter	Filter	Filter
NAME	TYPE	INDICATOR	SOURCE	ACCESS	POLICIES	COUNT	LAST SYNC	LAST UPDATE	DESCRIPTION	
Akamai	Allow	IP	CSV File Connector	Public	Inbound	19	10/30/23, 02:59 PM	02/13/23, 04:44 PM	Akamai curated by Greynoise	
Amazon Cloudfront	Allow	IP	CSV File Connector	Public	Inbound	144	10/30/23, 03:01 PM	07/10/23, 05:56 PM	Amazon Cloudfront curated by Greynoise	
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	3,117	10/30/23, 03:13 PM	10/30/23, 03:13 PM	Machine Learning - Malware Domain feed	
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,245	10/30/23, 03:29 PM	10/30/23, 03:29 PM	Machine Learning - Phishing Domain feed	
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,106	10/30/23, 02:50 PM	10/30/23, 02:50 PM	Dec 20 2:23 pm	

### 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
- To Enable this list globally for all policies, position the Enabled toggle (above the Name field) to the right (the toggle will turn blue)

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

### Create List

Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be blocked or allowed, depending on the list type, per the Policy it is assigned to.

1 LIST DETAILS
2 ADD ENTRIES

#### Manual Domain Block List Details

Name  
Customer Manual Domain List 27 / 64

Source  
Manual

List Type  
Block

Indicator  
Domain

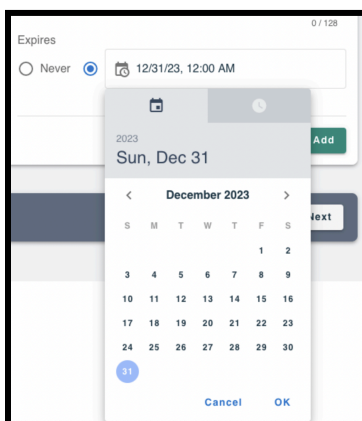
Description  
List of domains to block 24 / 128

Next

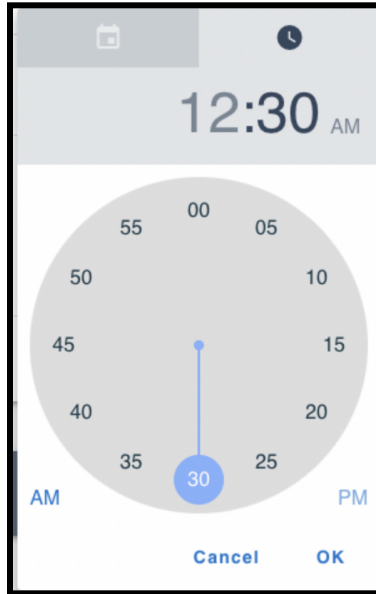
## Add Entries

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

- \*Domain
- Description (optional)
- \*Expiration
  - Default expiration is set to "Never"
  - To provide an expiration date and time:
    - Select the radio button next to the timestamp field
    - Select a date from the calendar



- Click on the clock tab and move the dial to the hours setting that is desired
- Move the dial to the minutes setting that is desired and click OK



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

### Create List

Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be blocked or allowed, depending on the list type, per the Policy it is assigned to.

**LIST DETAILS** **ADD ENTRIES**

#### Domain List

[Remove](#)

<input type="checkbox"/>	DOMAIN	EXPIRES	DESCRIPTION
Add Domains to this List			
<small>To add a Domain to this list, enter the Domain, optional expiration date and click Add.</small>			

#### Create Domain

[Clear](#)

Domain  
unwanted.com

Expires  
 Never

[Add](#)

[Previous](#) [Create List](#)

- Follow the steps above to add additional Domains to the list
- Once all domains are added, select the Next button
- Select the checkbox(es) next to the policy(s) you would like the list enabled on

**Create List**

Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be blocked or allowed, depending on the list type, per the Policy it is assigned to.

LIST DETAILS      ADD ENTRIES      **3** APPLY TO POLICIES

Apply to Policies Filter  New Policy...

NAME	DESCRIPTION
<input checked="" type="checkbox"/> Inbound	all inbound traffic
<input type="checkbox"/> Outbound	all outbound traffic

PER PAGE: 20 1-2 total < PREVIOUS 1 NEXT >

Previous Create List

Select the Create List button to create the List.

### Adding & Removing Manual List Entries

To add entries to a Manual List:

- Select the applicable List type (Allow or Block) from the filter at the top of the table
- Find the list in the table and click on the list name



Lists (1-20 of 21 filtered, 38 total)

Block All Health States All Indicators All Sources All Access Reset Filter

NAME	TYPE	INDICATOR	SOURCE	ACCESS	POLICIES	COUNT	LAST SYNC	LAST UPDATE	DESCRIPTION
Bambenek ML-Malware	Block	Domain	Bambenek	Public	None	3,117	10/30/23, 03:13 PM	10/30/23, 03:13 PM	Machine Learning - Malware Domain feed
Bambenek ML-Phishing	Block	Domain	Bambenek	Public	None	5,245	10/30/23, 03:29 PM	10/30/23, 03:29 PM	Machine Learning - Phishing Domain feed
Bitdefender APT-Domains	Block	Domain	Bitdefender	Public	None	11,109	10/30/23, 03:51 PM	10/30/23, 03:51 PM	Dec 20 2.23 pm
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	792	10/30/23, 02:59 PM	10/30/23, 02:59 PM	Bitdefender Command and Control (C2) IPs Feed
Bitdefender Malicious-do...	Block	Domain	Bitdefender	Public	None	398,279	10/30/23, 03:11 PM	10/30/23, 03:11 PM	Dec 20 2.23 pm
Bitdefender Phishing-dom...	Block	Domain	Bitdefender	Public	None	248,620	10/30/23, 02:57 PM	10/30/23, 02:57 PM	Dec 20 2.24 pm
Blocklist.de	Block	IP	Basic HTTP	Public	Inbound +1	23,130	10/30/23, 03:05 PM	10/30/23, 03:05 PM	-
CINS Army list	Block	IP	Basic HTTP	Public	Inbound +1	15,000	10/30/23, 03:05 PM	10/30/23, 03:05 PM	-
CISA Alert List	Block	IP	CSV File Connector	Public	Inbound +1	399	10/30/23, 03:05 PM	10/30/23, 03:05 PM	-
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,533	10/30/23, 03:19 PM	10/30/23, 03:19 PM	-
Customer Manual Domain L...	Block	Domain	Manual	Private	None	1	10/30/23, 03:52 PM	10/30/23, 03:52 PM	List of domains to block
Cyjax	Block	IP	Cyjax	Public	None	58	10/30/23, 03:18 PM	10/30/23, 11:14 AM	-
Cyjax	Block	Domain	Cyjax	Public	None	255	10/30/23, 03:11 PM	10/30/23, 11:07 AM	Cyjax Threat Intelligence Feed

- In the Search field, enter the IP or Domain to add
- If the entry does not already exist in the list, click the “+” sign in the right hand corner

List Customer Manual Domain List

List of domains to block

List Details

LIST TYPE	INDICATOR	SOURCE	ACCESS	POLICY	COUNT	LAST SYNC	LAST UPDATE
Block	Domain	Manual	Private	None	1	10/30/23, 03:52 PM	10/30/23, 03:52 PM

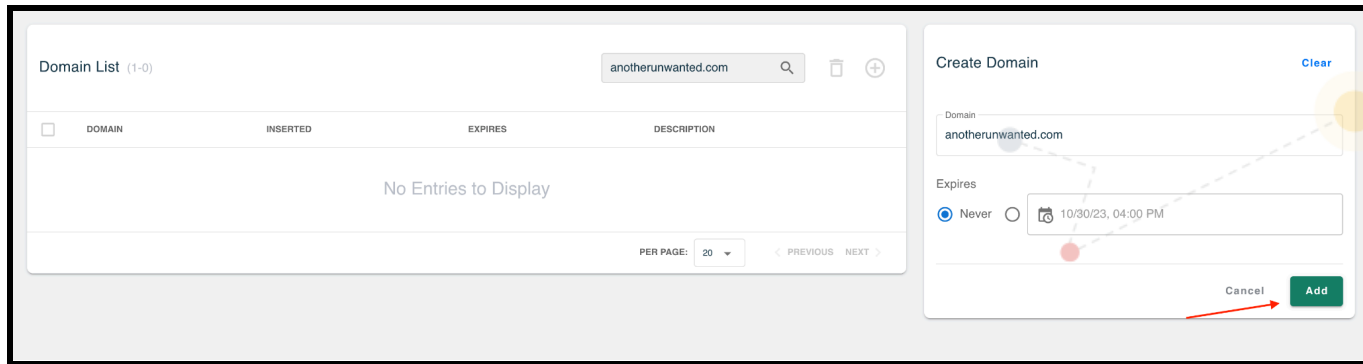
Domain List (1-0)

anotherunwanted.com [X] [Q] [Add]

DOMAIN	INSERTED	EXPIRES	DESCRIPTION
No Entries to Display			

PER PAGE: 20 [PREVIOUS] [NEXT]

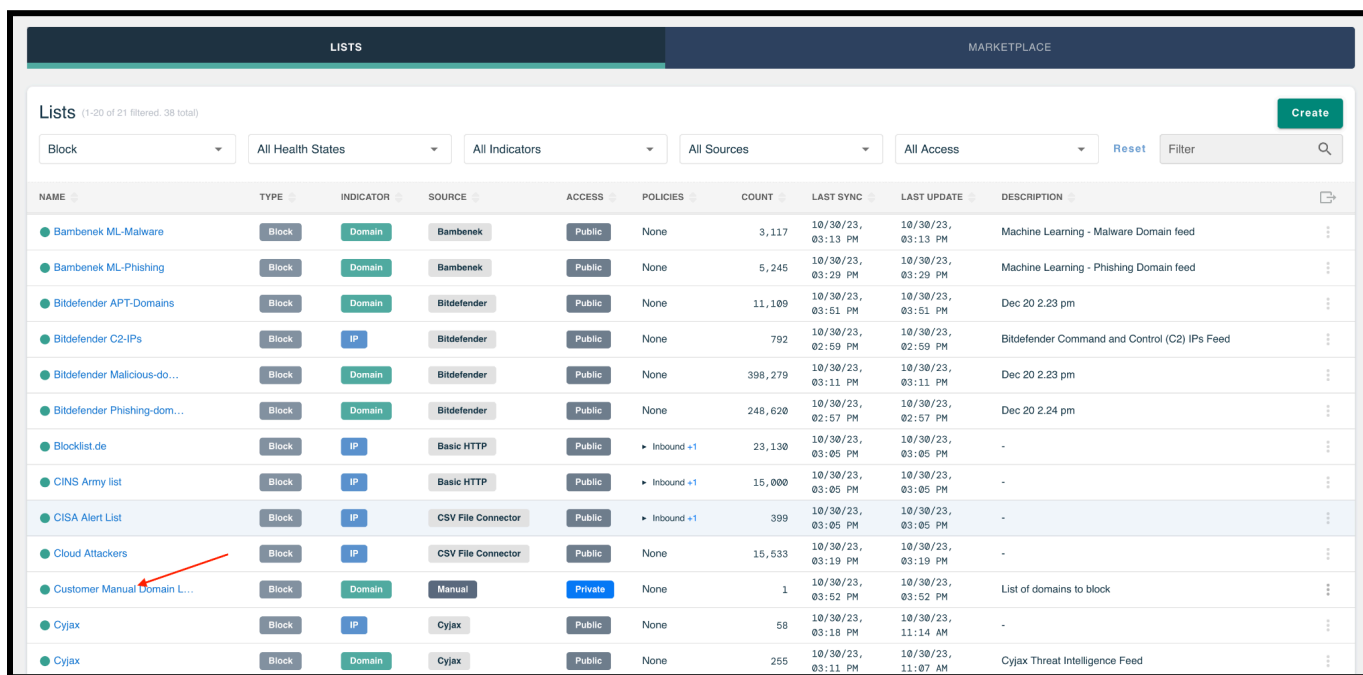
- In the right-hand panel, enter the applicable data and click the “Add’ button”



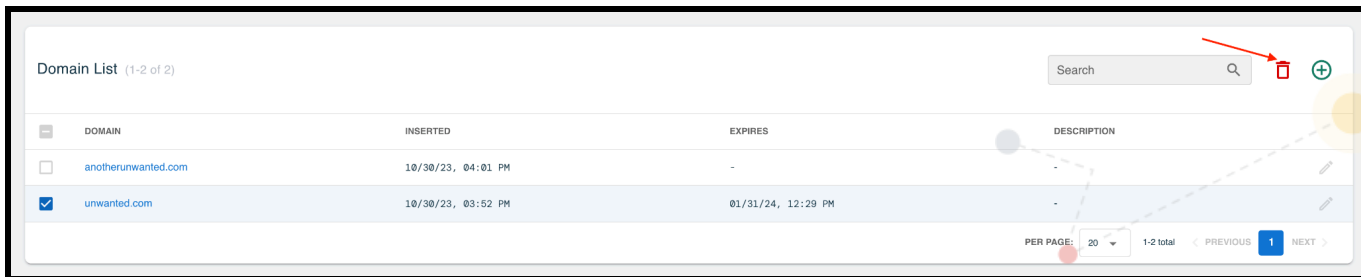
Follow the steps above to add additional entries to the list.

To remove entries from a Manual List:

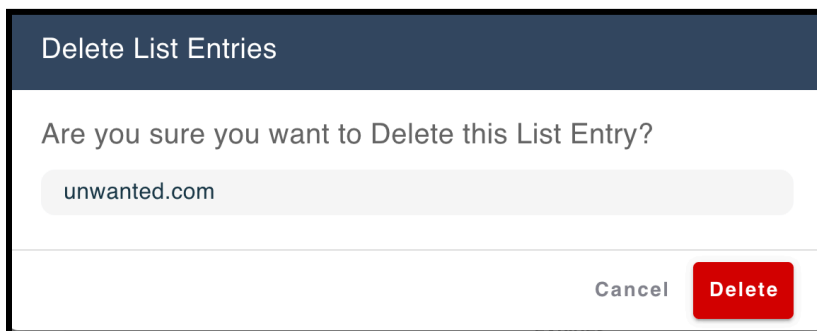
- Select the applicable List type (Allow or Block) from the filter at the top of the table
- Find the list in the table and click on the list name



- Select the checkbox(es) next to the entry(ies) that should be removed
- Select the Trash icon



- On the confirmation modal, select the Delete button

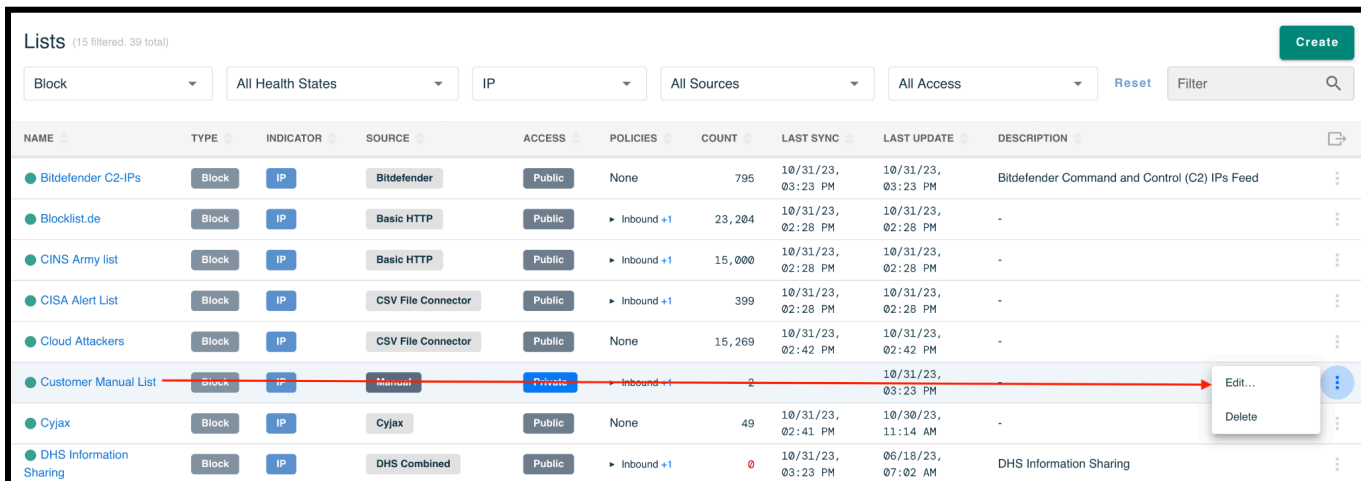


The entries are now deleted from the list.

## Editing all List Components

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

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



- 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, select the Save button in the top right corner

**Edit List** Customer Manual List Cancel Save

Lists can be used to allow or block IPs and Domains. The indicators contained in the list will be blocked or allowed, depending on the list type, per the Policy it is assigned to.

LIST DETAILS ENTRIES APPLY TO POLICIES

**Manual IP Block List Details**

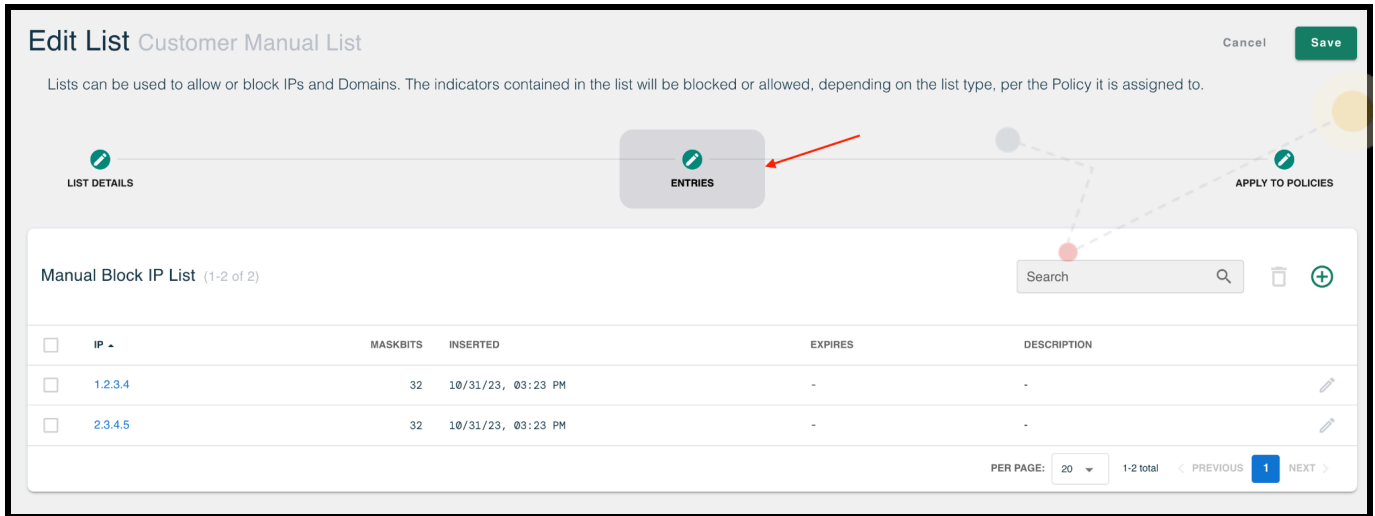
Name: Customer Manual List 20 / 64 Source: Manual

List Type: Block Indicator: IP

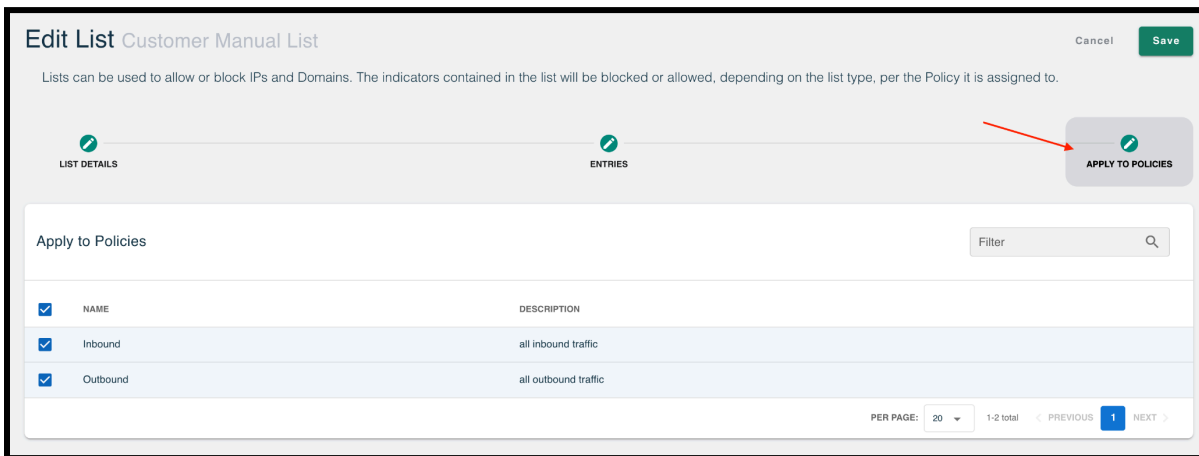
Description 0 / 128

- Edit Entries -

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



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



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

## Deleting a List

To delete a List:

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

Lists (15 filtered, 39 total) Create

Block All Health States IP All Sources All Access Reset Filter Q

NAME	TYPE	INDICATOR	SOURCE	ACCESS	POLICIES	COUNT	LAST SYNC	LAST UPDATE	DESCRIPTION
Bitdefender C2-IPs	Block	IP	Bitdefender	Public	None	795	10/31/23, 03:23 PM	10/31/23, 03:23 PM	Bitdefender Command and Control (C2) IPs Feed
Blocklist.de	Block	IP	Basic HTTP	Public	Inbound +1	23,204	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-
CINS Army list	Block	IP	Basic HTTP	Public	Inbound +1	15,000	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-
CISA Alert List	Block	IP	CSV File Connector	Public	Inbound +1	399	10/31/23, 02:28 PM	10/31/23, 02:28 PM	-
Cloud Attackers	Block	IP	CSV File Connector	Public	None	15,269	10/31/23, 02:42 PM	10/31/23, 02:42 PM	-
Customer Manual List	Block	IP	Manual	Private	Inbound +1	2	10/31/23, 03:23 PM	10/31/23, 03:23 PM	-
Cyjax	Block	IP	Cyjax	Public	None	49	10/31/23, 02:41 PM	10/30/23, 11:14 AM	-
DHS Information Sharing	Block	IP	DHS Combined	Public	Inbound +1	0	10/31/23, 03:23 PM	06/18/23, 07:02 AM	DHS Information Sharing
ET Block IPs	Block	IP	Basic HTTP	Public	Inbound +1	1,043	10/31/23, 03:23 PM	10/31/23, 03:23 PM	-

*Note: A red circle highlights the 'Customer Manual List' row, and a red arrow points from its 'More' menu to the 'Delete' option in the confirmation modal shown below.*

- On the confirmation modal, select Delete

**Delete List**

Are you sure you want to delete this List?

Customer Manual List

Cancel Delete

The list is now deleted.

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

# 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 to your threatER account.

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 additional data will display:

- Subscription Throughput – refer to the Subscription Throughput section below for more details
- 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.
- Enforce Configuration Settings – see Enforce Configuration section below for more details
- Networks being managed by the Enforcer

The screenshot displays the threatER web interface. At the top, there is a navigation bar with tabs for ENFORCERS, NETWORKS, PORTS, POLICIES, SUBSCRIPTIONS, and REPORTS. The 'ENFORCERS' tab is active.

**Enforcer Details** for 'Enforcer AWS' is shown with the following information:

<b>SUBSCRIPTION</b> Enforce Complimentary Subscription	<b>LAST CONNECTION</b> 11/09/23, 02:51 PM	<b>SUPPORT END</b> 12/31/2023	<b>BRIDGE STATE</b> Normal	<b>BUILD NUMBER</b> 229	<b>SUBSCRIPTION THROUGHPUT</b> 0%	<b>LOCATION</b> AWS us-east-1	<b>ADMIN IP</b> 1.2.3.4
---	--	----------------------------------	-------------------------------	----------------------------	--------------------------------------	----------------------------------	----------------------------

**Networks** (1-2 of 2 total) section includes filter options: All Configuration States, All Directions, All Drop Actions, and a Filter search box. Below is a table of networks:

NAME	DIRECTION	POLICY	DROP ACTION	IPS	PORTS	DESCRIPTION
Inbound ThreatBlockr AWS	Inbound	Inbound	Discard	10.0.1.0/24	All Protocols	(Legacy Import)
Outbound ThreatBlockr AWS	Outbound	Outbound	ICMP Unreachable	10.0.1.0/24	All Protocols	(Legacy Import)

At the bottom right, there is a pagination control: PER PAGE: All, 1-2 of 2 total, PREVIOUS, 1, NEXT.



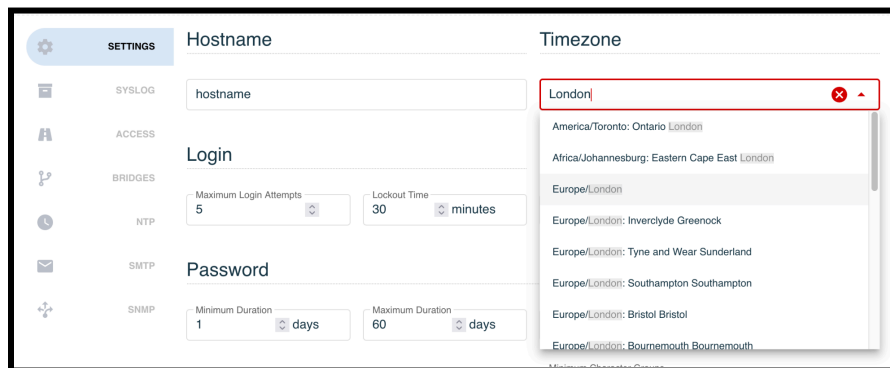
# Enforce Configuration

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.



- **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

threater

Username  
username

Password  
\*\*\*\*\*

I agree with the terms of service

Sign in

Login with SSO

threater

Terms of Service  
I agree to the Terms and Conditions

Sign in

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

Configuration

SETTINGS

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: 3

Banner:  Accepted Text: I agree to the Terms and Conditions Declined Text: I do not agree to the Terms and Conditions

Save

## Syslog

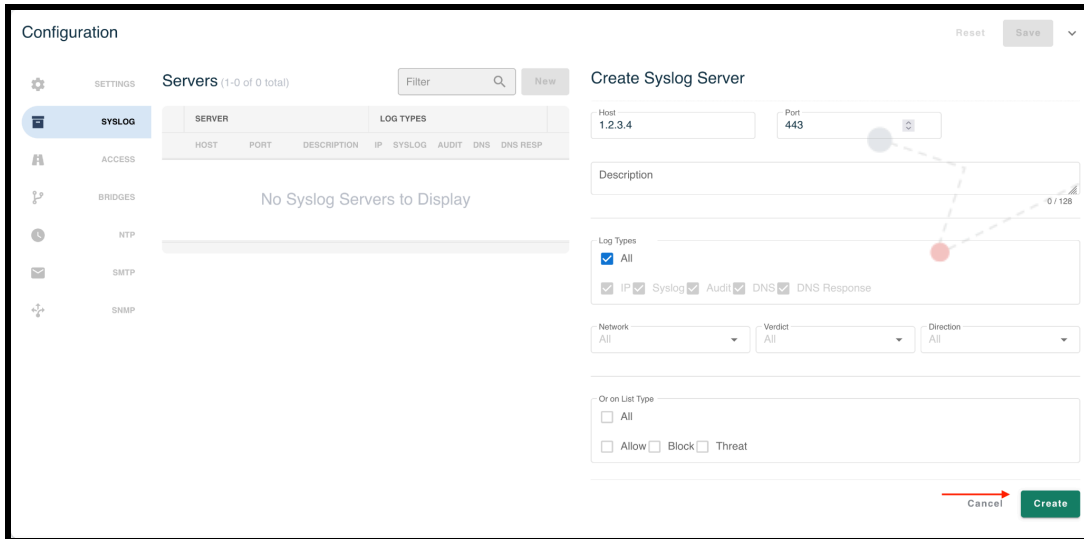
Syslog exports are an industry-standard way of exporting data in a concise, timely manner. Our syslog export format is compliant to RFC-5424 and ensures seamless integration alongside any number of external tools like:

- 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

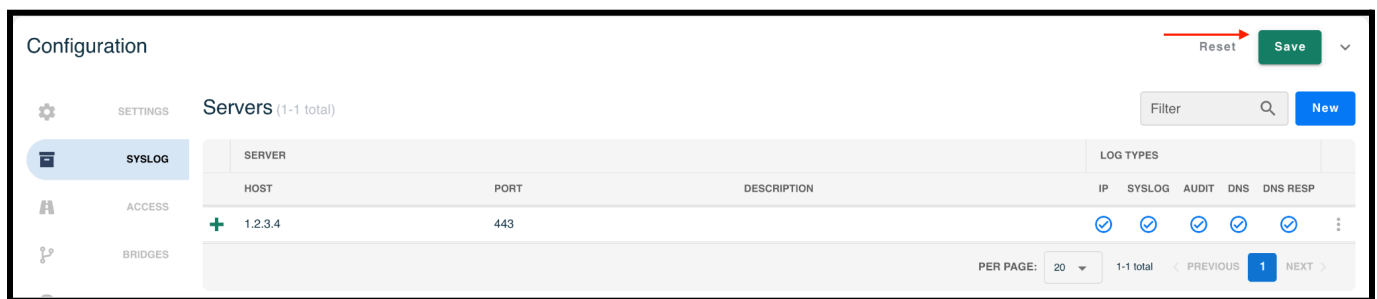
Our Syslog export is not designed with any particular SIEM tool in mind. We focus on the comprehensive data contained in our syslog exports, enabling you to parse our logs by any tool that can ingest RFC-compliant syslog exports.

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 Type(s), if desired
- Select the “Create” button in the bottom right corner



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



## Access

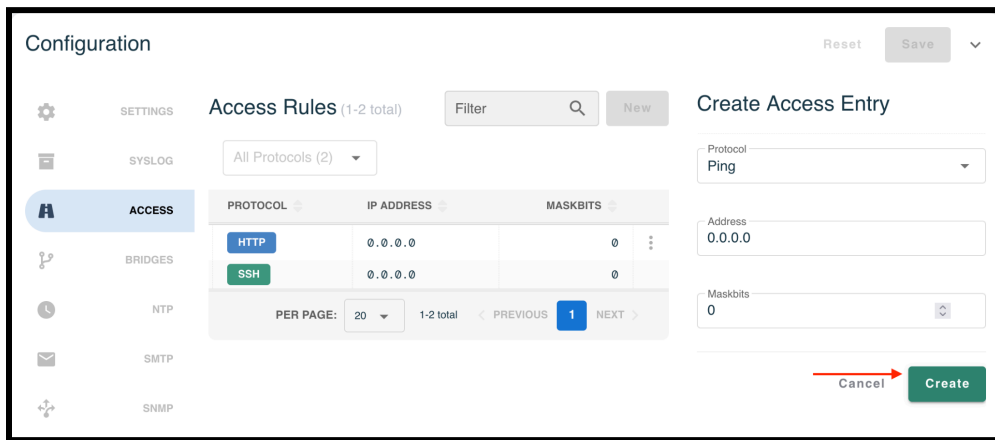
If your company has allowed Access rules to be managed in the threatER Portal (via a setting in the Enforce UI), the following protocols are available to add/edit:

- **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.

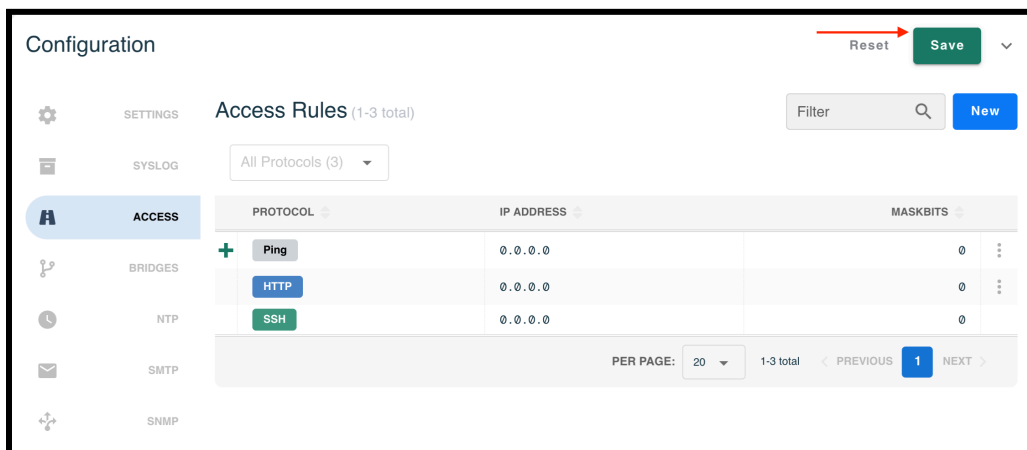
- **SNMP** – The SNMP access setting allows you to add a list of trusted management networks. threatER Enforce will accept SNMP requests from these networks, and deny them from all others.
- **SSH** – For any Enforcer in AWS, Azure, or Google Cloud, a default SSH access rule will be applied.

To add an Access rule:

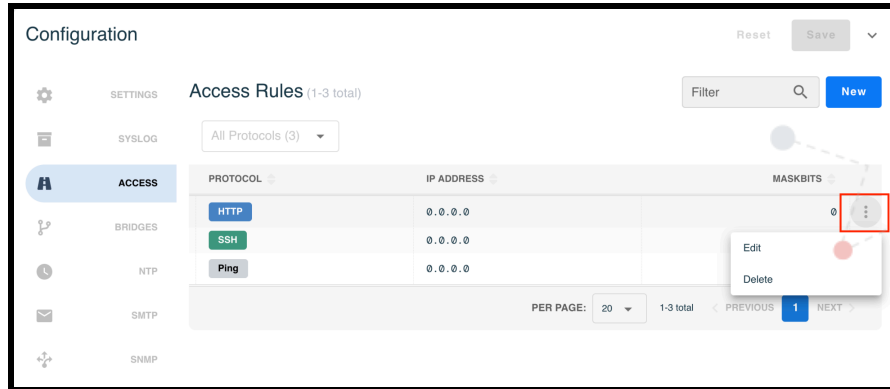
- Click the “New” button in the top-right corner of the table
- Select the desired Protocol
- Enter the applicable Address
- Enter the applicable Maskbits
- Click the Create button



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



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

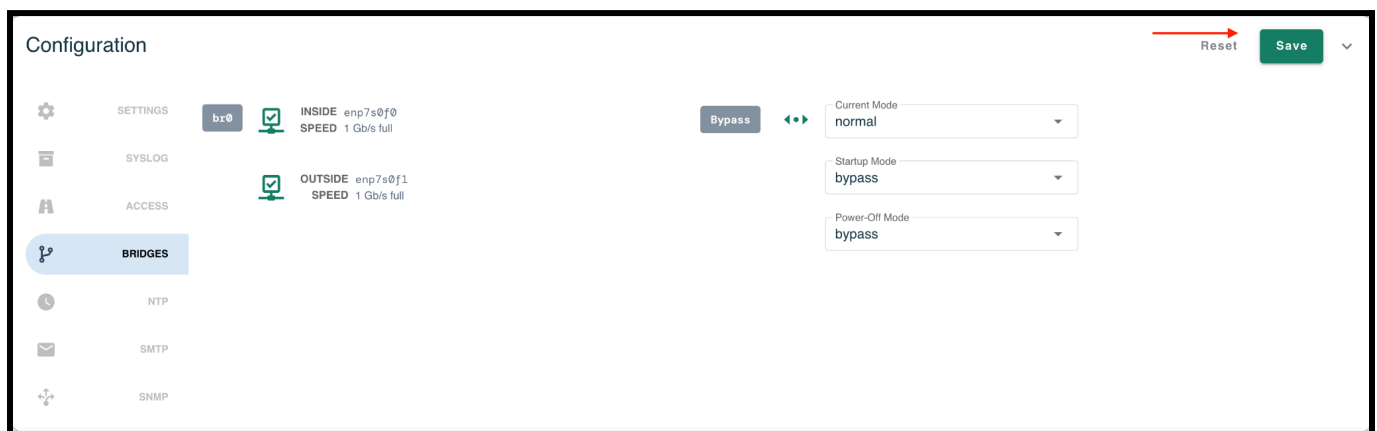


## Bridges

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.



## 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.

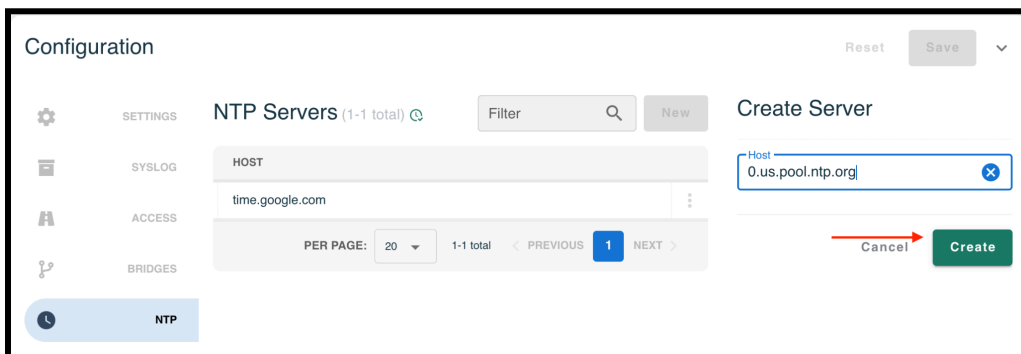
threatER Enforce supports NTP version 3. Enter the IPv4 or IPv6 Internet address of your organization's NTP server, or if one isn't available, select a public server. Lists of time servers can be found at The NTP Public Services Project: <http://support.ntp.org>. NTPv3 has optional authentication. If 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.

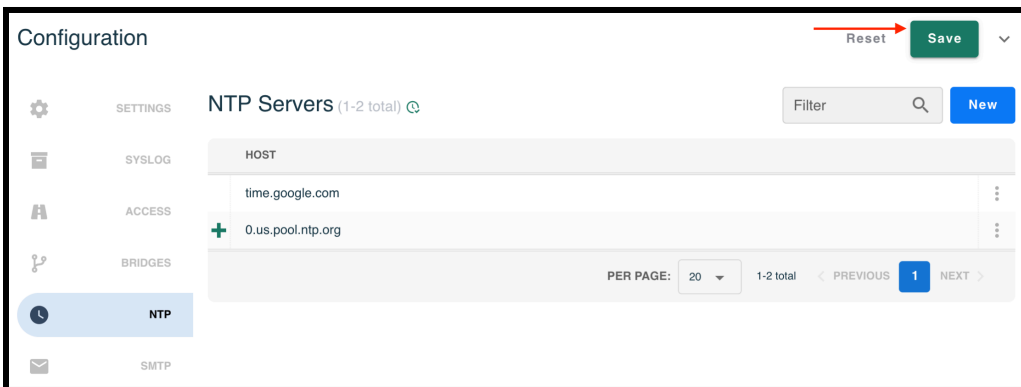
Configuring the Time Zone and Date/Time settings can be done either manually or using an NTP server. Note that manually set times will be overwritten by the NTP Server settings.

To create an NTP Server:

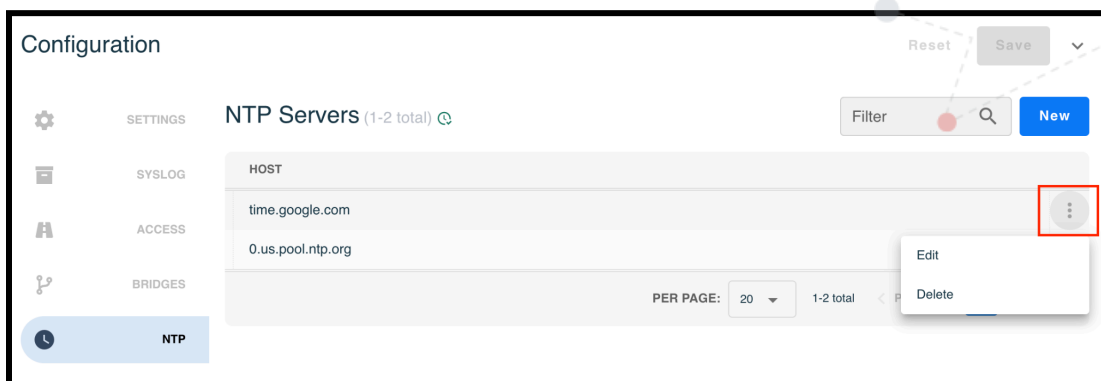
- Click on the "New" button in the top-right corner of the table
- Enter the Host
- Click the "Create" button



- 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

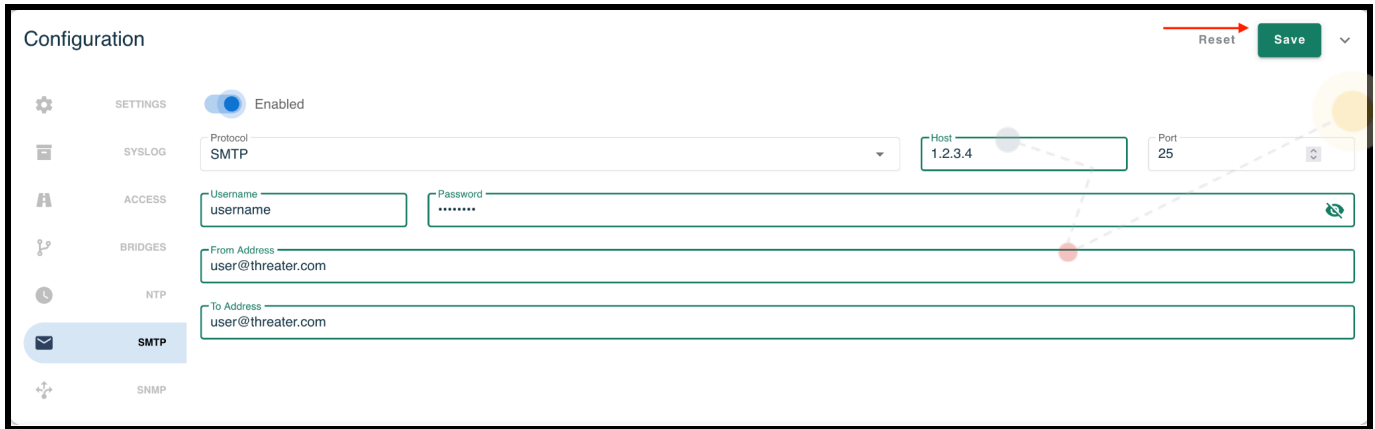
SMTP messages can be sent when an alarm is raised (e.g. an update fails, entering bypass mode or an account gets locked out).

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"

Once all fields have been provided, click the Save button in the top right corner.





## 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.

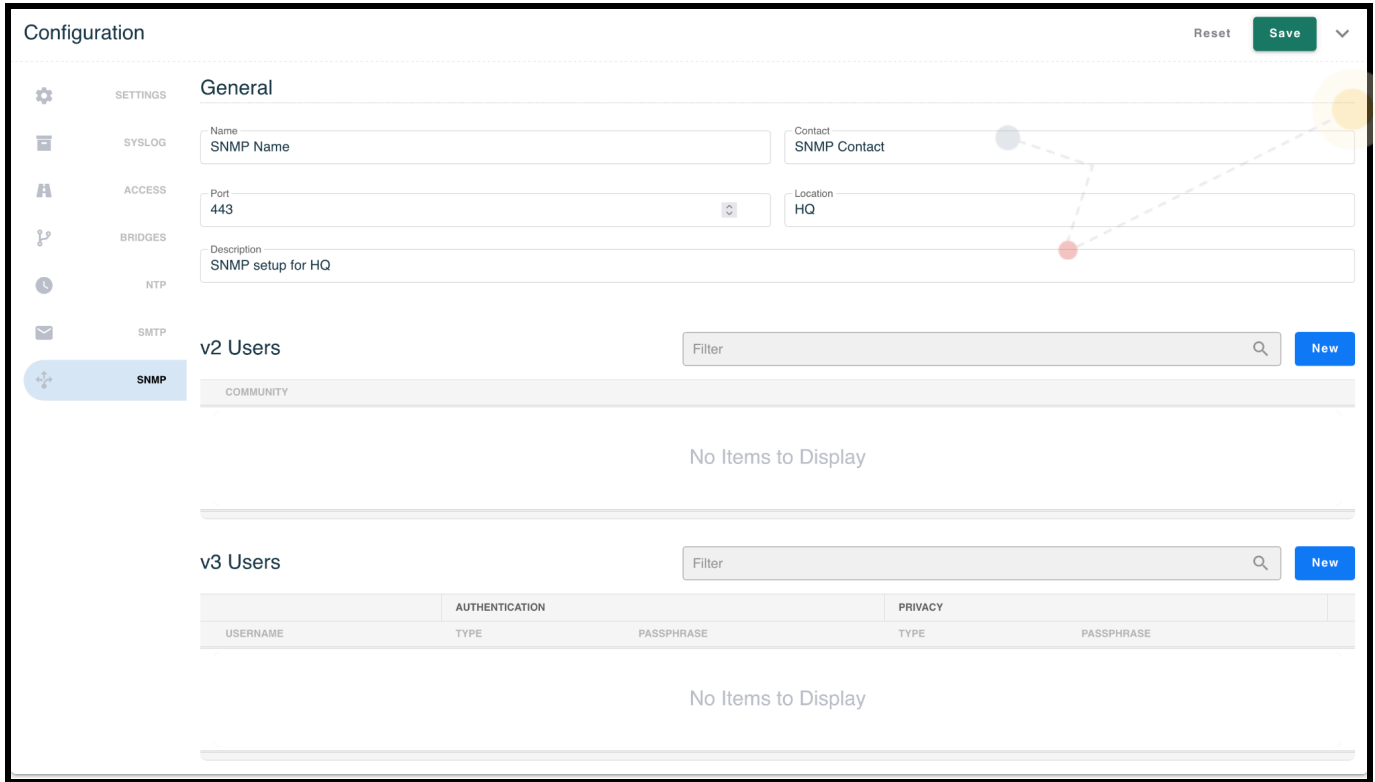
Admins will need to [set up SNMP access](#) first before making SNMP configurations.

To configure SNMP, enter the following:

- Name
- Contact
- Port
- Location
- Description

threatER supports two versions of SNMP:

- Community-based SNMPv2c
- SNMPv3



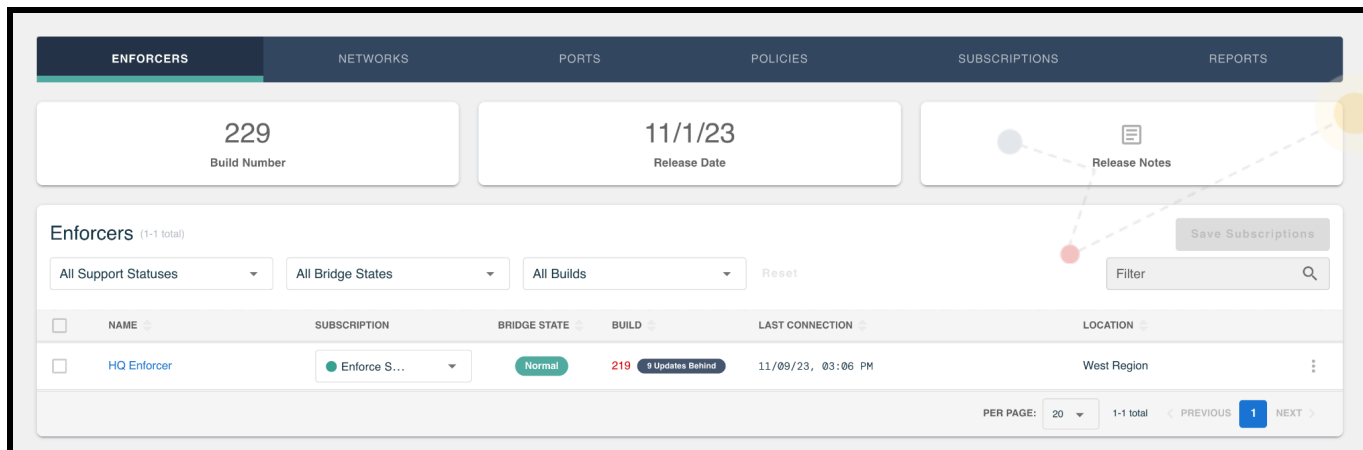
Click the “New” button next to the desired version and provide the necessary details. Once complete, click the “Save” button in the top right corner.

## Enforce Software

Customers can install the latest Enforce software build onto their Enforcers from the Enforcers tab.

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 – selecting this will open a PDF of the Build Release Notes in a separate browser tab

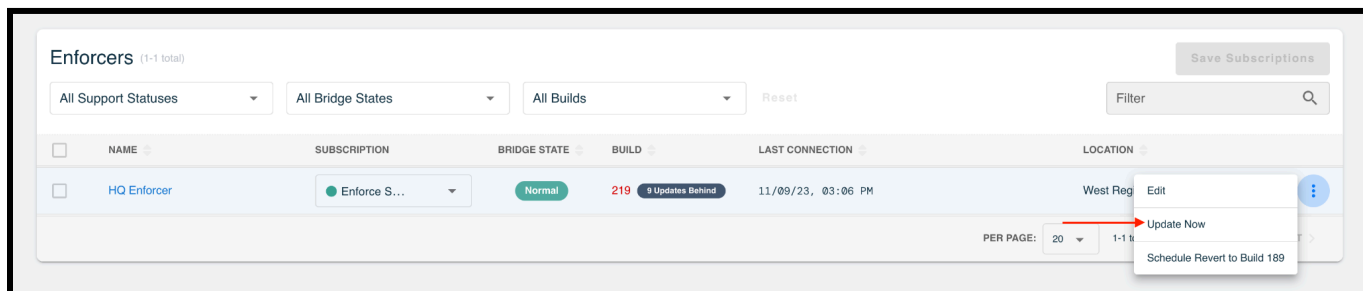


Users have the option to perform an immediate update, or to schedule an update.

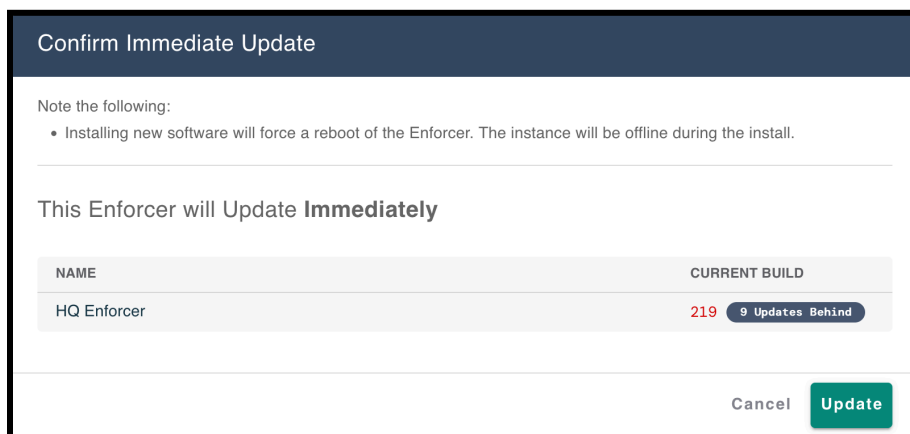
## Update Now

To immediately install the latest build on an Enforcer:

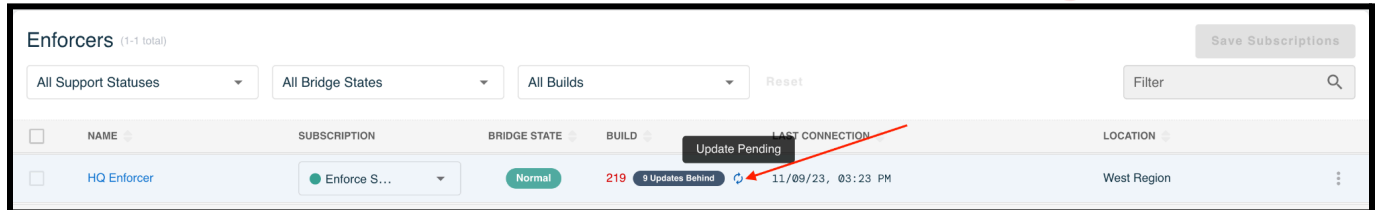
- In the row of the Enforcer, select Update Now from the ellipsis menu



- On the confirmation modal, select the Update button



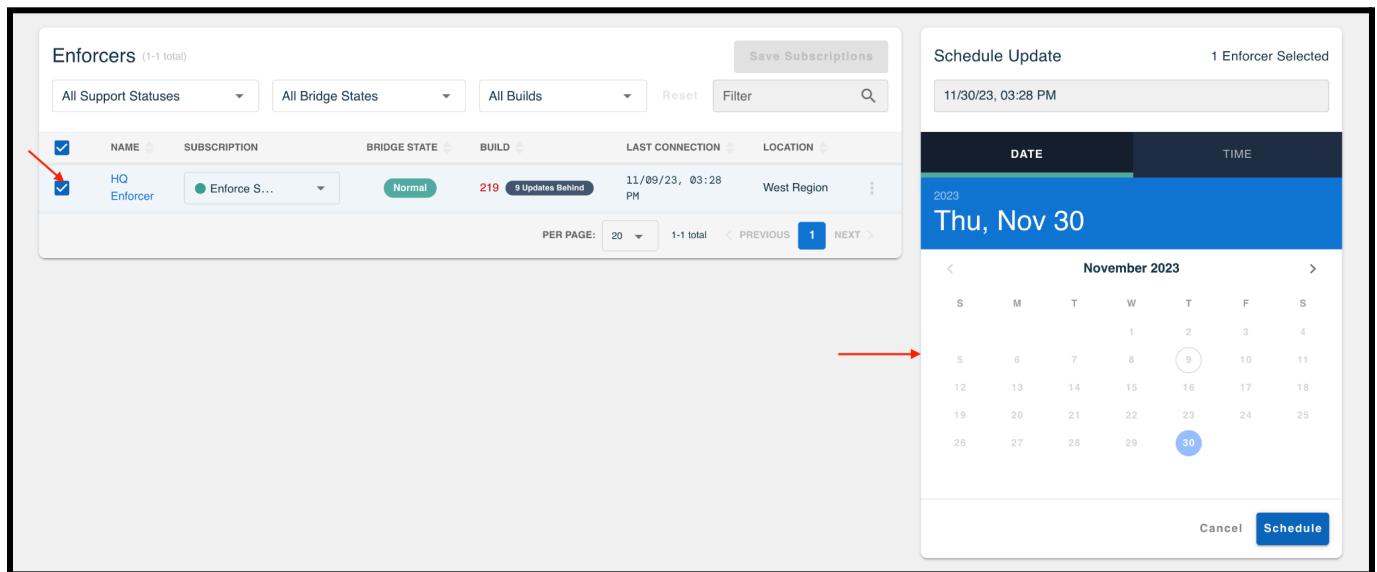
The table will display an "Update Pending" icon for the Enforcer until the build installation is complete. The "Update Pending" will automatically clear as soon as the associated Enforcer has begun the process of the update. Upon completion, which can take several minutes, the new build number will appear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



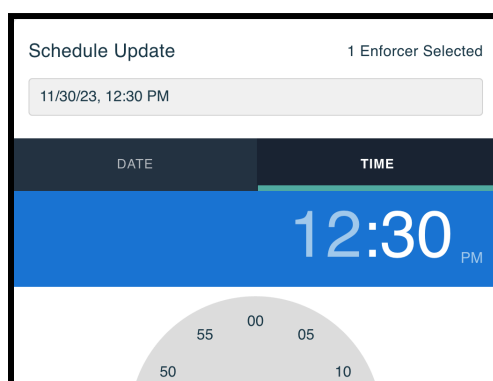
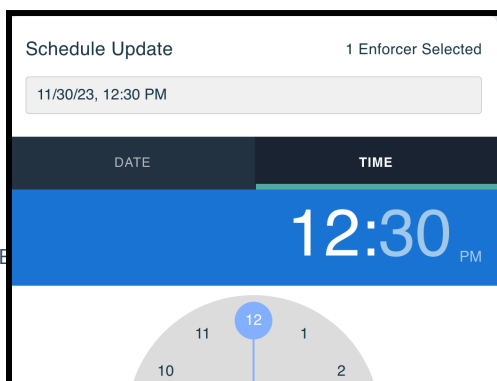
## Schedule Update

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

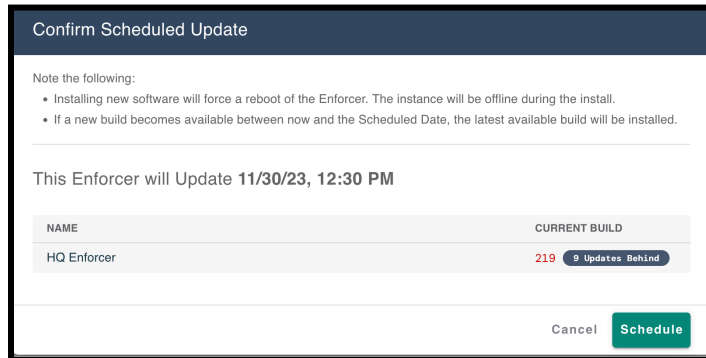


- Select the Time tab and choose the desired time (both hours and minutes)



**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.

- Select the Schedule button
- On the Confirm Scheduled Updates modal, select Schedule

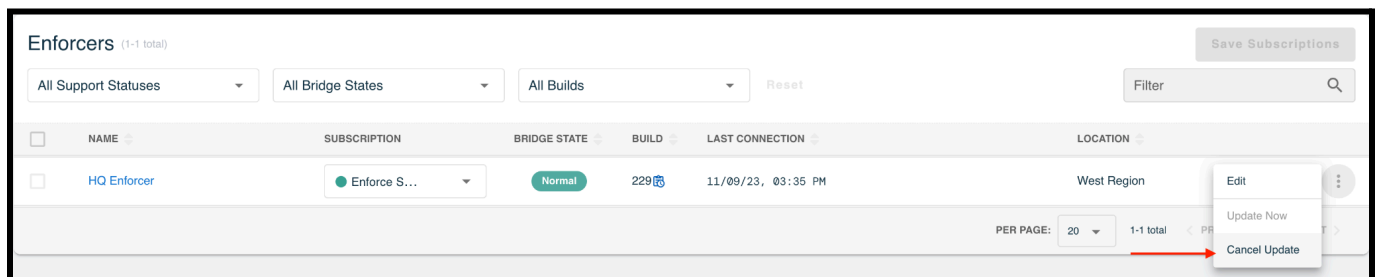


The table will reflect the schedules.

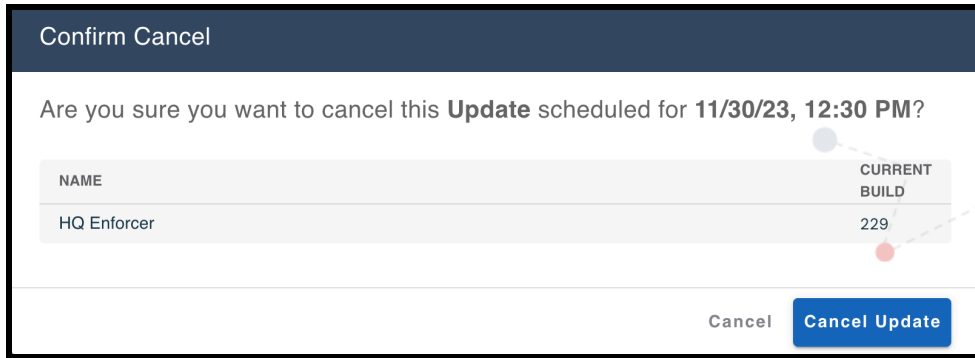
## Cancel a Scheduled Update

To cancel a scheduled update:

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



- On the Confirm Cancel modal, select the Cancel button

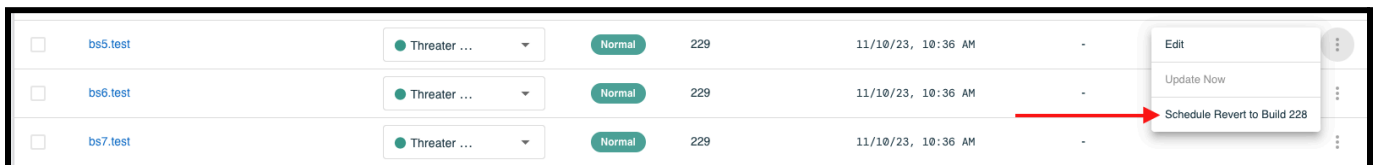


The table will reflect the cancellation.

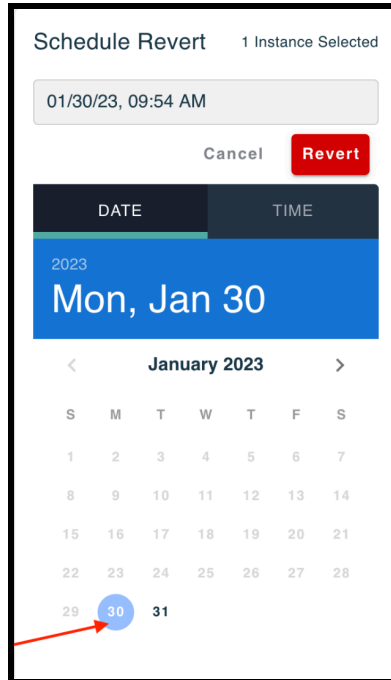
### Revert to Previous Build

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:

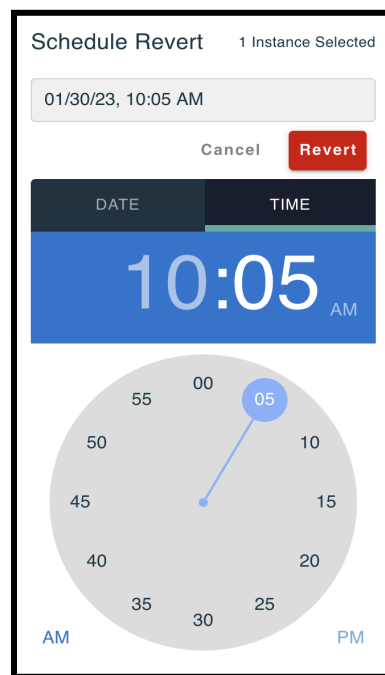
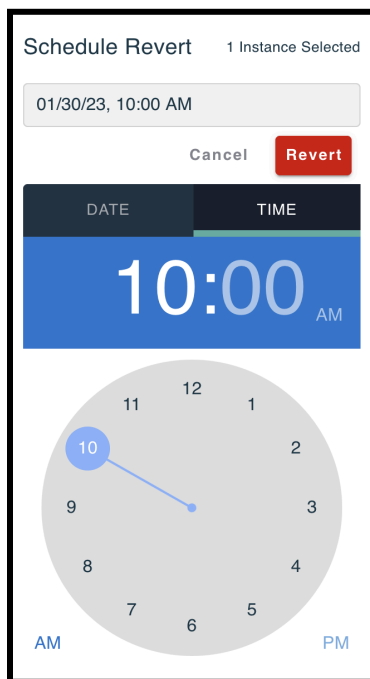
- In the row of the Enforcer, select Schedule Revert to Build [#] from the ellipsis menu



- Select a date from the calendar

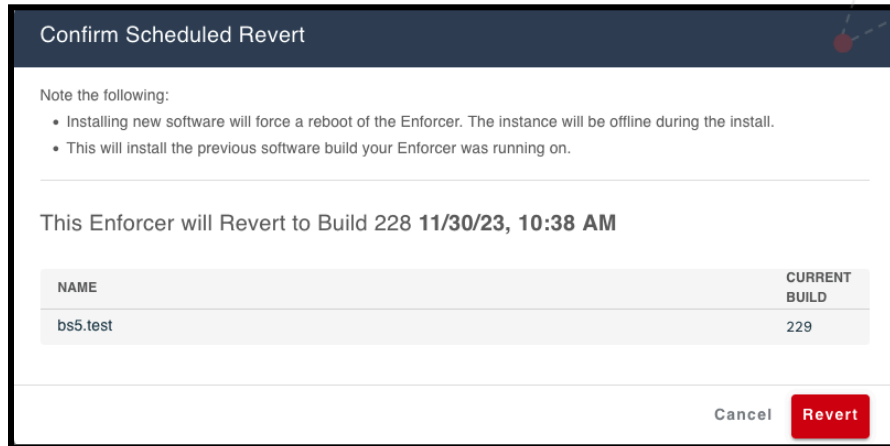


- Select the Time tab and set the time (both hours and minutes)



**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.

- Select the Revert button
- On the Confirm Scheduled Revert modal, select Revert



The table will reflect the scheduled revert.

## Manual Downloads

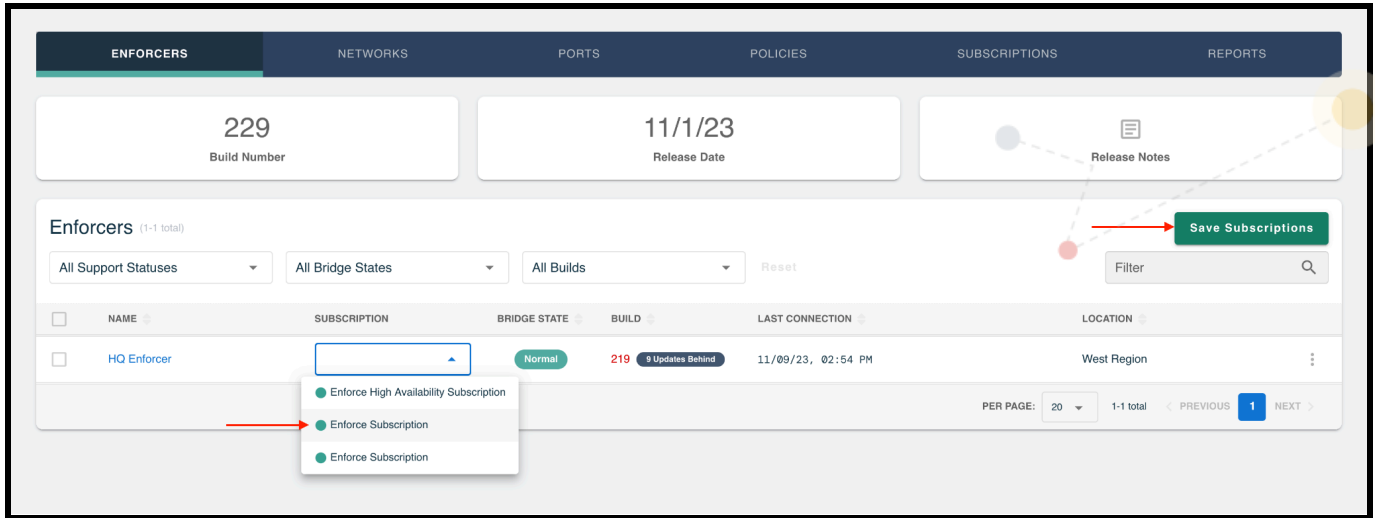
It is strongly recommended to utilize the automatic installation of Enforce software builds described in the above sections. Should a manual download of a build be required, please consult our [Customer Success team](#) for assistance. We do not recommend that you attempt Manual Downloads on your own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

## Subscription Management

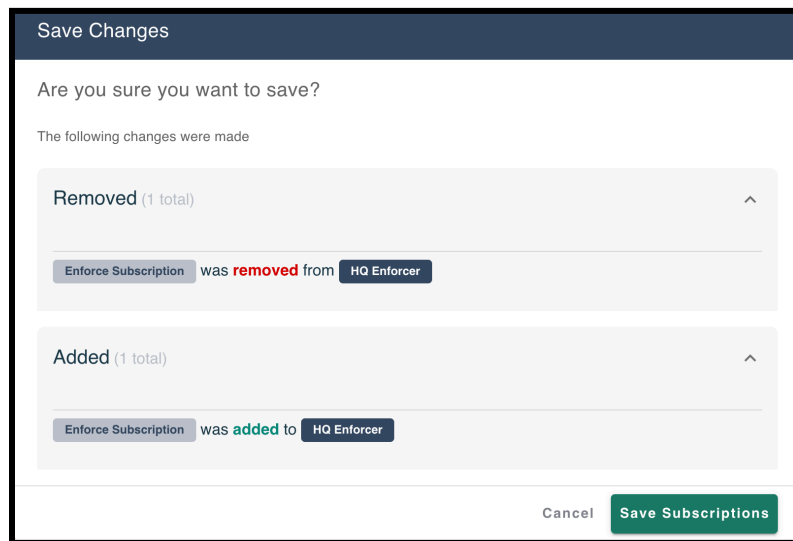
To manage subscriptions from the Enforcers tab:

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





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



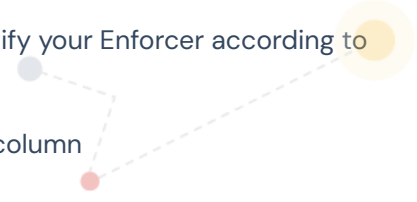
Subscription Status Indicators:

- Green – subscription is actively supported
- Yellow – support has lapsed; any Enforcee 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 edit the Name and/or Location of an Enforcer to simplify your ability to identify your Enforcer according to your own network naming conventions:

- Find the Enforcer in the table and select the pencil icon in the far right column
- Enter the desired name and/or location
- Select Save



## Subscription Throughput

The Subscription Throughput chart provides the past 30 days of an Enforcer’s inbound and outbound throughput.

To access the Subscription Throughput chart click on an individual Enforcer and then select the Subscription Throughput bar.

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)

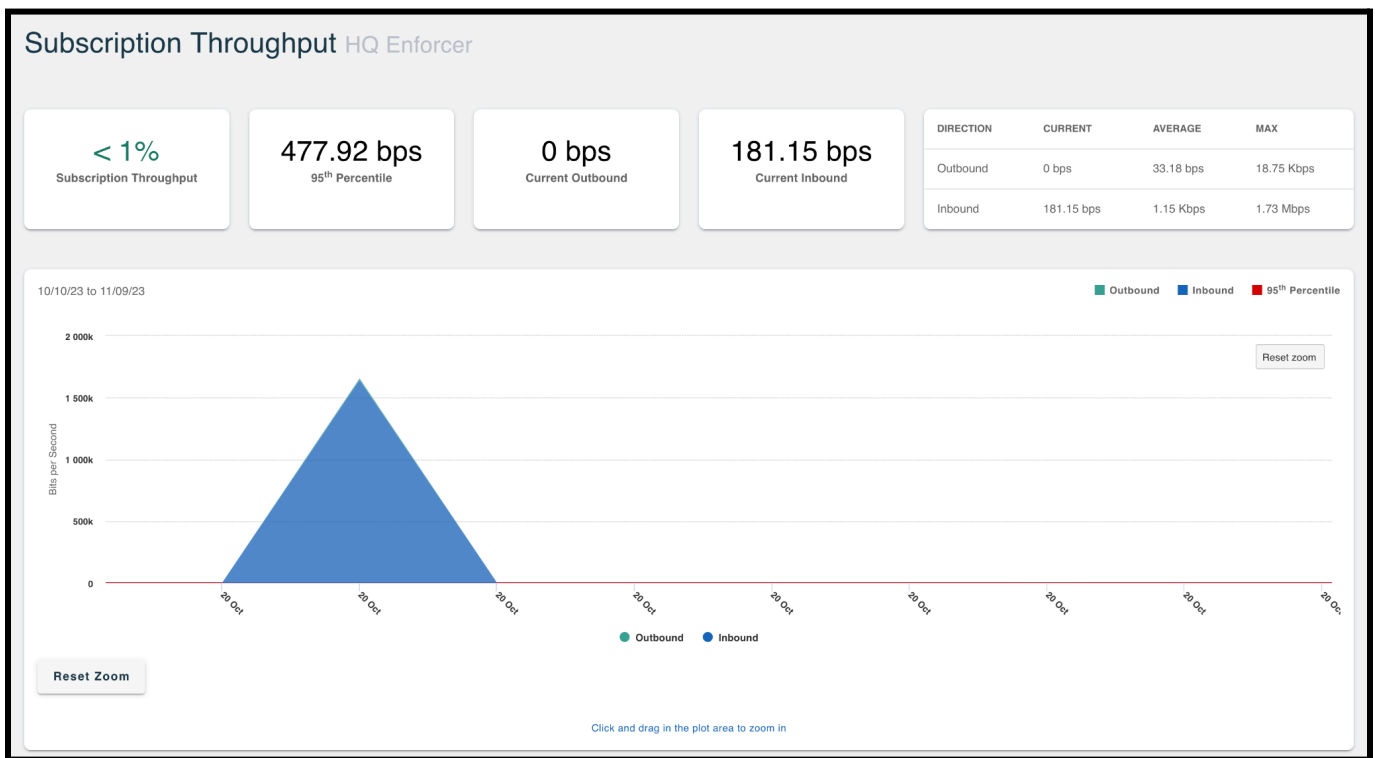
- Current Inbound throughput (in bits)

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.



## 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.

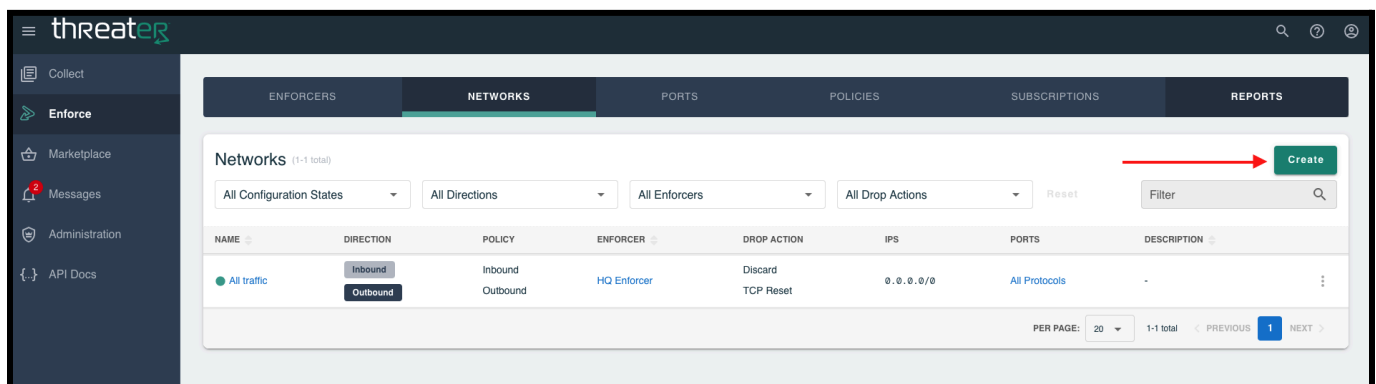
One or more network rules comprise a configured Network in threatER, and each network is identified as a device, asset, or subnet on your network. If the Enforcer receives traffic for the configured IP, then it will allow traffic according to the policy associated to the Network. Each Network configuration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

**NOTE:** An Enforcer must have an Enforce build greater than 180 installed to fully take advantage of this feature within the portal. As such, we strongly urge customers to update to the latest software to be able to use these powerful centralized control features. Customers who have not yet updated are not able to control these features centrally, and instead must leverage the legacy Enforce UI elements.

## Creating Networks

To create a Network:

- Navigate to Enforce in the left-hand navigation menu
- Select the Networks tab
- Select the “Create” button in the top-right corner



## 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
  - **NOTE:** Enforcers on Enforce Build 154 or prior build will not display in this 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, select the Next button to proceed to the next step.

### Create Network

Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet services allowed on your network, and those services your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, asset, or subnet on your network.

1 NETWORK DETAILS
2 INBOUND
3 OUTBOUND
4 IPS

**Network Details**

Name  
All traffic 11 / 64

Description 0 / 128

Enforcers  
HQ Enforcer

Directions  
Both

Next

## 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.

Select Next to proceed to the next step.

### Create Network

Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet services allowed on your network, and those services your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, asset, or subnet on your network.

1 NETWORK DETAILS    2 **INBOUND**    3 OUTBOUND    4 IPS

**Inbound**

Select or Create a Policy  
Inbound New Policy...

Drop Action  
Discard Only

Previous Next

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 Network

Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet services allowed on your network, and those services your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, asset, or subnet on your network.

1 NETWORK DETAILS    2 INBOUND    3 **OUTBOUND**    4 IPS

**Outbound**

Select or Create a Policy  
Outbound New Policy...

Drop Action  
ICMP Unreachable

Previous Next

## 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, select 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

- 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 +Add 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

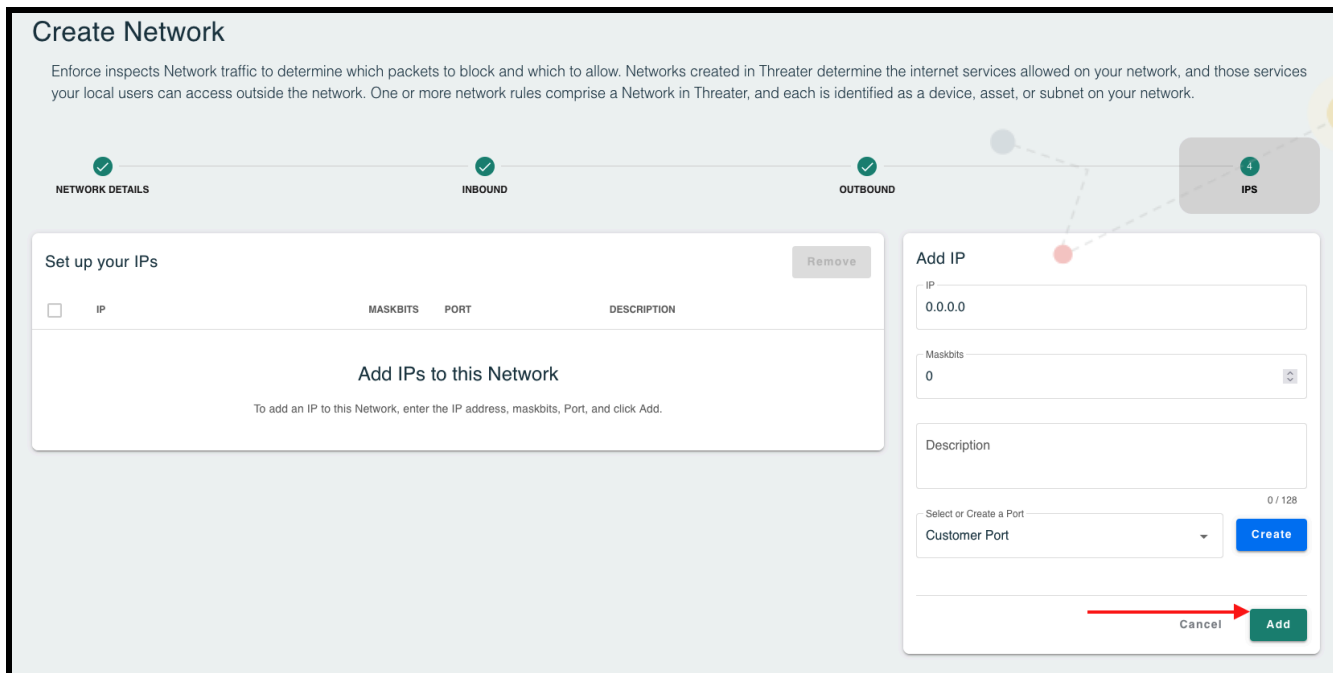
Ports: 50-2489 ✕ + Add

The TCP Protocol uses Ports. Enter them above. eg: 22 or 42-43-88

Cancel Create

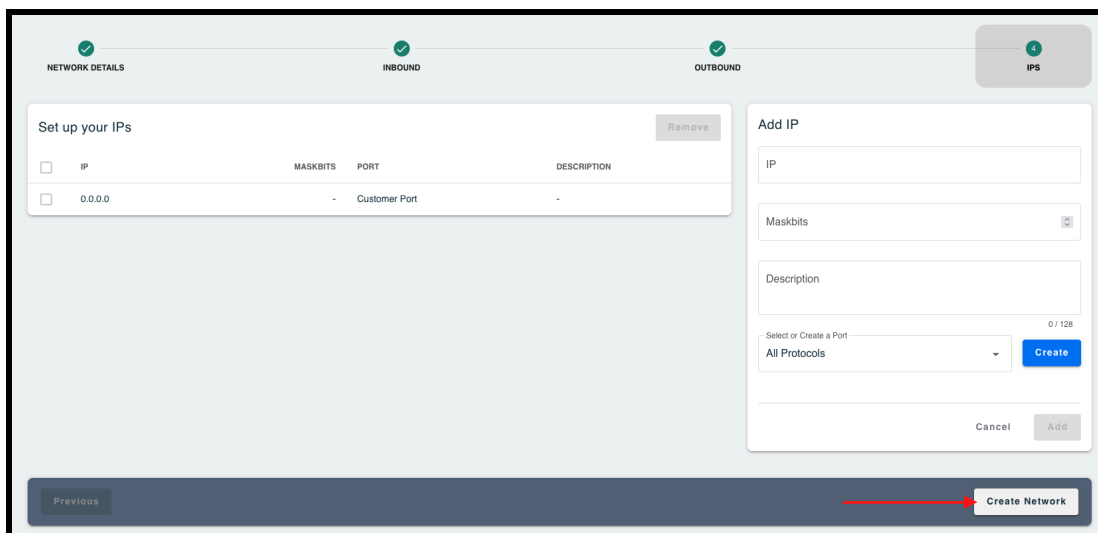
- Click the Create button to return to the Add IP Panel
- Select the Add button to add the IP to the Network





- Follow the steps above to add additional IPs

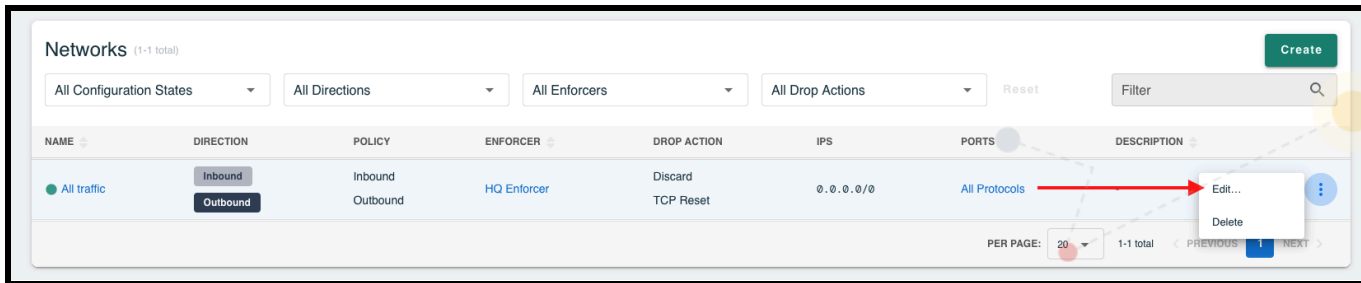
Once all IPs are added, select the Create Network button to create the Network.



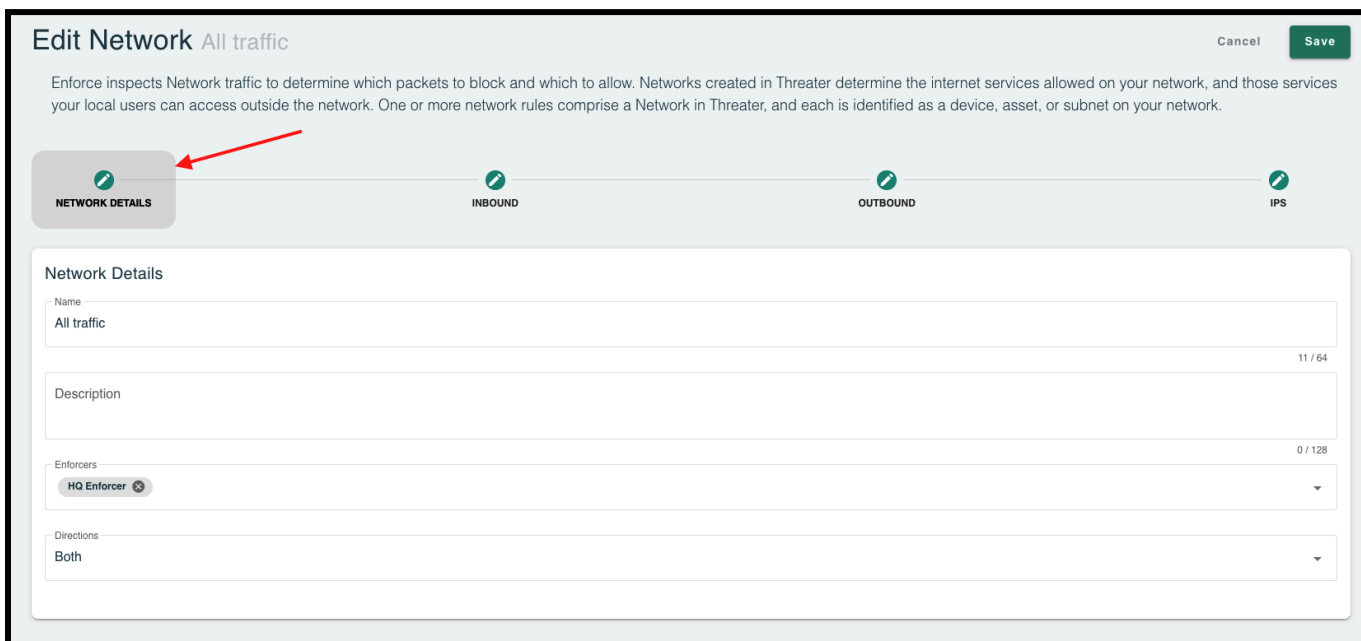
## Editing a Network

To Edit a Network:

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



- 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, select the Save button in the top right corner



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

**Edit Network** All traffic Cancel **Save**

Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet services allowed on your network, and those services your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, asset, or subnet on your network.

Progress bar: NETWORK DETAILS **INBOUND** OUTBOUND IPS

**Inbound**

Select or Create a Policy: Inbound **New 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, select the Save button in the top right corner

**Edit Network** All traffic Cancel **Save**

Enforce inspects Network traffic to determine which packets to block and which to allow. Networks created in Threater determine the internet services allowed on your network, and those services your local users can access outside the network. One or more network rules comprise a Network in Threater, and each is identified as a device, asset, or subnet on your network.

Progress bar: NETWORK DETAILS INBOUND OUTBOUND **IPS**

**Set up your IPs** Remove

<input type="checkbox"/>	IP	MASKBITS	PORT	DESCRIPTION
<input type="checkbox"/>	0.0.0.0	-	All Protocols	-

**Add IP**

IP:

Maskbits:

Description:

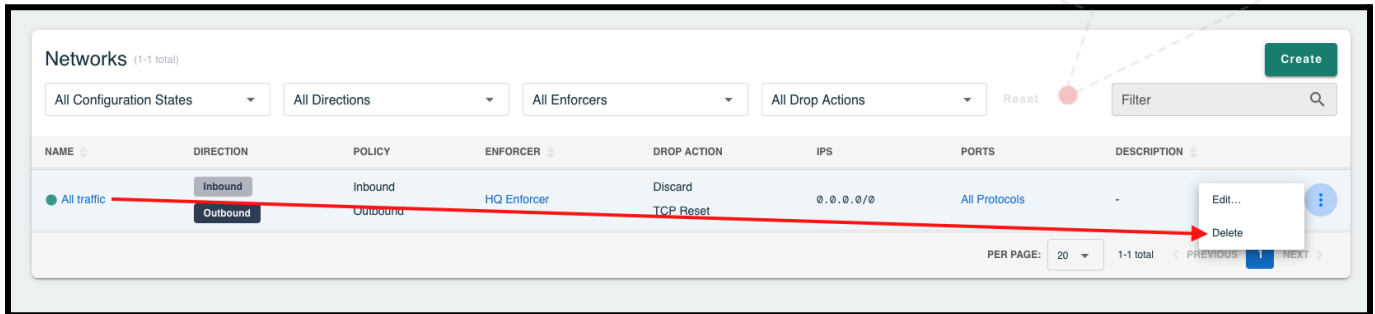
Select or Create a Port: All Protocols 0 / 128

**Create** Cancel Add

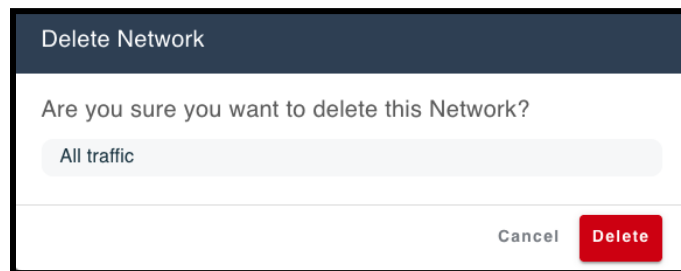
## Deleting a Network

To delete a Network:

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



- On the confirmation modal, select Delete



The Network is now deleted.

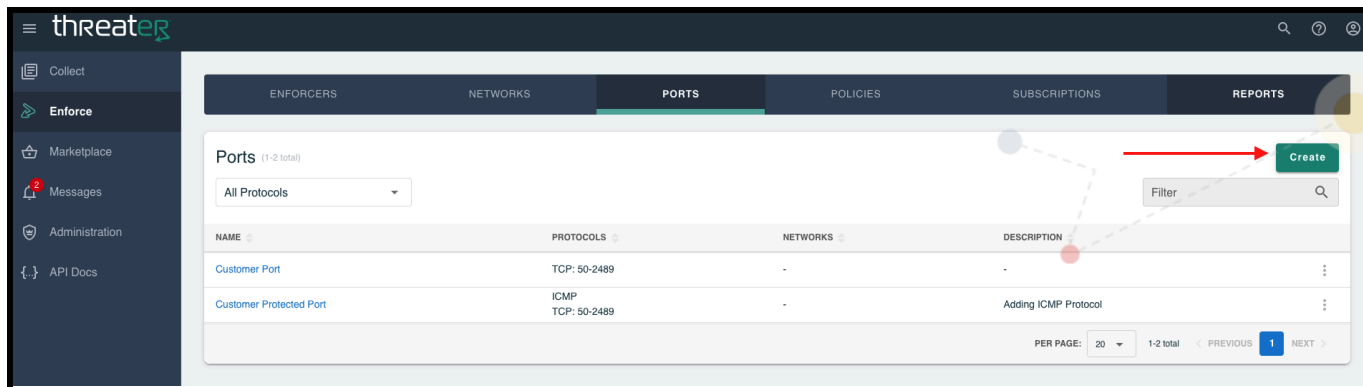
## Ports

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

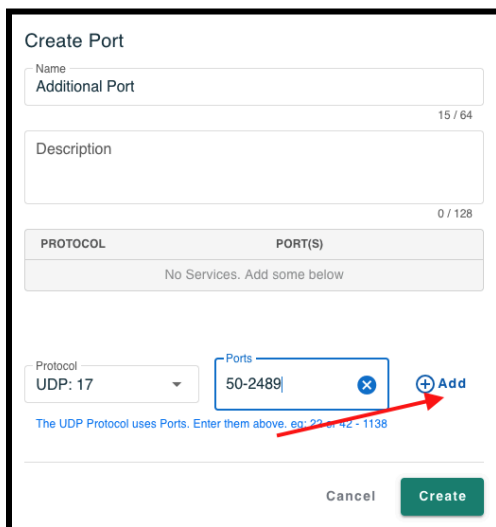
## Adding Ports

To add a Port:

- Navigate to Enforce in the left-hand navigation menu
- Select the Ports tab
- Click on the “Create” button in the top right corner of the table



- 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 +Add button to add the Protocol to the Port



- Add any additional Protocols to the Port, as necessary
  - Click the Create button to create the Port

## Editing Ports

To edit a Port:

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

The screenshot shows a table with three rows: 'Additional Port', 'Customer Port', and 'Customer Protected Port'. The 'Customer Port' row is highlighted in blue. A red arrow points from the ellipsis menu of this row to the 'Edit' button. The table has columns for NAME, PROTOCOLS, NETWORKS, and DESCRIPTION. A 'Create' button is in the top right, and a 'Filter' search box is below it. The bottom of the table shows pagination: 'PER PAGE: 20', '1-3 total', and navigation arrows.

- Make the necessary changes and click the Save button

The screenshot shows the 'Edit Port' form on the right side of the screen. The form has fields for 'Name' (Customer Port), 'Description', and 'PROTOCOL' (TCP: 6). The 'PORT(S)' field contains '50-2489'. At the bottom of the form, there is a 'Protocol' dropdown set to 'All: 256' and an '+ Add' button. A red arrow points to the 'Save' button. The left side of the screenshot shows the 'Ports' table with the 'Customer Port' row selected.

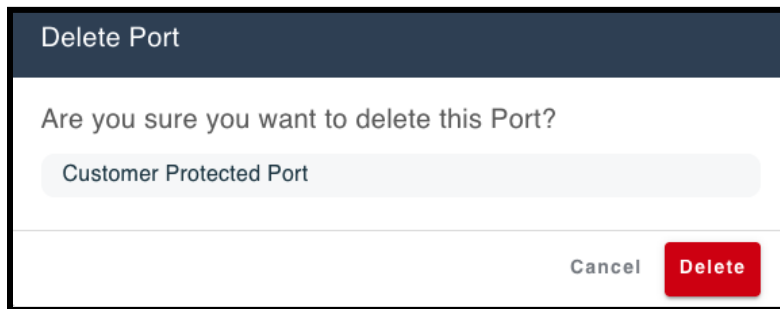
## Deleting Ports

To delete a Port:

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



- On the confirmation modal, select the Delete button



The Port is now deleted.

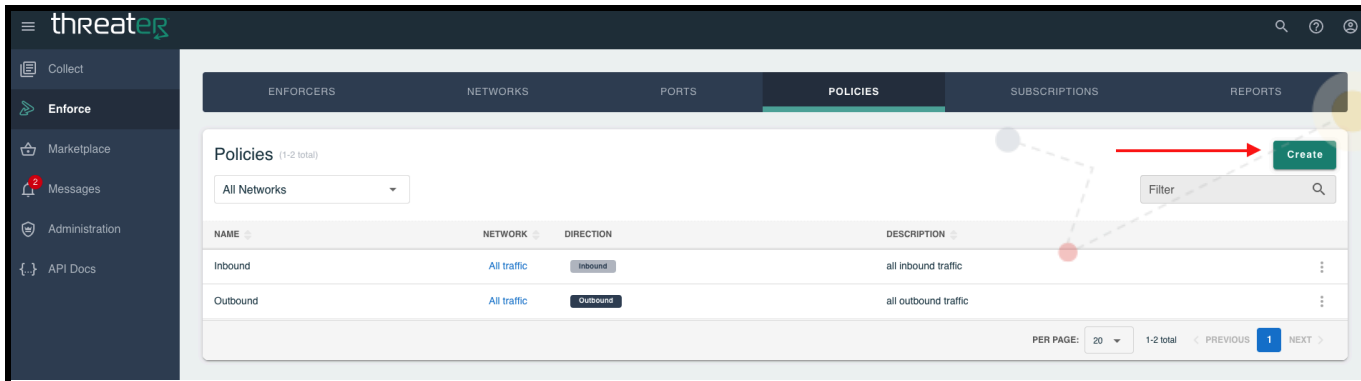
## Policies

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

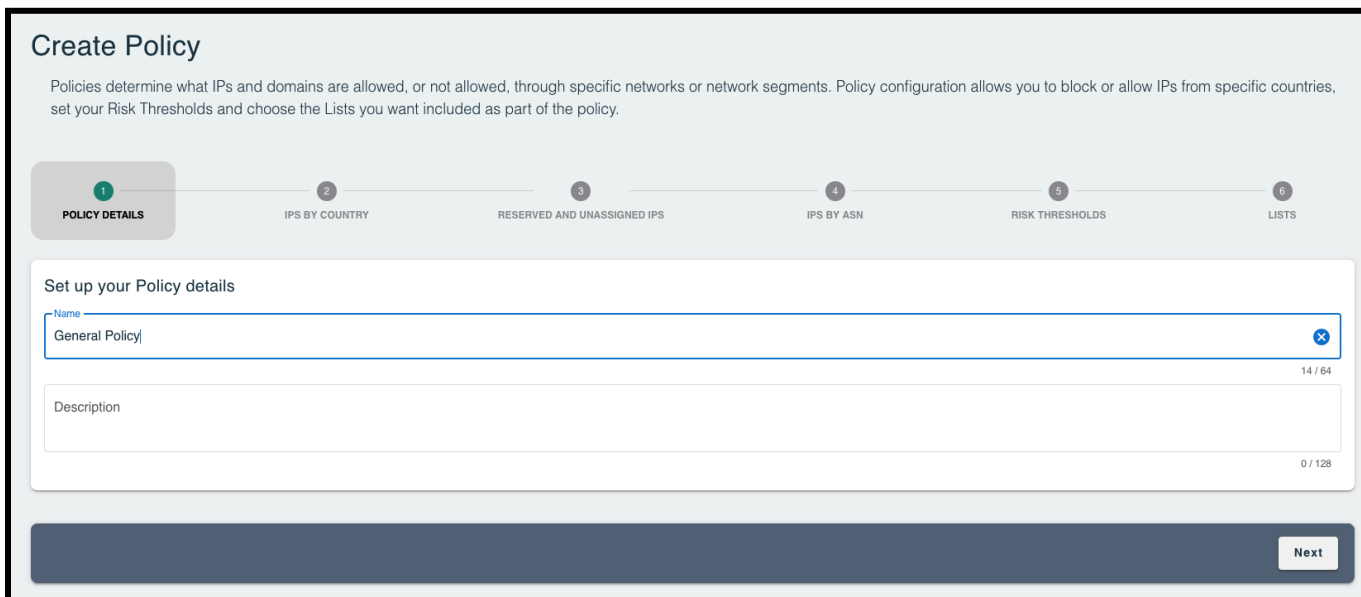
To create a Policy:

- Navigate to Enforce in the left-hand navigation menu
- Select the Policies tab
- Select the Create button the top-right corner of the table



## Policy Details

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



## 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)



### Create Policy

Policies determine what IPs and domains are allowed, or not allowed, through specific networks or network segments. Policy configuration allows you to block or allow IPs from specific countries, set your Risk Thresholds and choose the Lists you want included as part of the policy.

1 POLICY DETAILS    2 **IPS BY COUNTRY**    3 RESERVED AND UNASSIGNED IPS    4 IPS BY ASN    5 RISK THRESHOLDS    6 LISTS

Setup Your IPs by Country Allow All Block All

Filter  All

COUNTRY	ALLOW/BLOCK
AFGHANISTAN	<input checked="" type="checkbox"/>
ALAND ISLANDS	<input checked="" type="checkbox"/>
ALBANIA	<input checked="" type="checkbox"/>
ALGERIA	<input checked="" type="checkbox"/>
AMERICAN SAMOA	<input checked="" type="checkbox"/>
ANDORRA	<input checked="" type="checkbox"/>
ANGOLA	<input checked="" type="checkbox"/>
ANGUILLA	<input checked="" type="checkbox"/>
ANTARCTICA	<input checked="" type="checkbox"/>
ANTIGUA AND BARBUDA	<input checked="" type="checkbox"/>
ARGENTINA	<input checked="" type="checkbox"/>
ARMENIA	<input checked="" type="checkbox"/>
ARUBA	<input checked="" type="checkbox"/>
ASCENSION ISLAND	<input checked="" type="checkbox"/>

Legend: ● Allowed ● Blocked

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

### Create Policy

Policies determine what IPs and domains are allowed, or not allowed, through specific networks or network segments. Policy configuration allows you to block or allow IPs from specific countries, set your Risk Thresholds and choose the Lists you want included as part of the policy.

1 POLICY DETAILS    2 **IPS BY COUNTRY**    3 RESERVED AND UNASSIGNED IPS    4 IPS BY ASN    5 RISK THRESHOLDS    6 LISTS

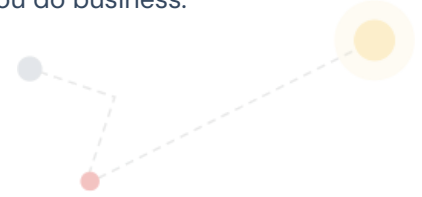
Setup Your IPs by Country Allow All Block All

Filter  All

COUNTRY	ALLOW/BLOCK
ROMANIA	<input checked="" type="checkbox"/>

Legend: ● Allowed ● Blocked

- 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, select 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 select Next.

ENFORCERS NETWORKS PORTS **POLICIES** SUBSCRIPTIONS REPORTS

### Create Policy

Policies determine what IPs and domains are allowed, or not allowed, through specific networks or network segments. Policy configuration allows you to block or allow IPs from specific countries, set your Risk Thresholds and choose the Lists you want included as part of the policy.

1 ✓ POLICY DETAILS    2 ✓ IPS BY COUNTRY    3 **RESERVED AND UNASSIGNED IPS**    4 IPS BY ASN    5 RISK THRESHOLDS    6 LISTS

Set up your Reserved and Unassigned IP Settings

Reserved IPs	Allow	Block
Unassigned IPs	Allow	Block

Previous Next

## 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 right-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 left-hand panel



### Create Policy

Policies determine what IPs and domains are allowed, or not allowed, through specific networks or network segments. Policy configuration allows you to block or allow IPs from specific countries, set your Risk Thresholds and choose the Lists you want included as part of the policy.

✓ POLICY DETAILS   
 ✓ IPS BY COUNTRY   
 ✓ RESERVED AND UNASSIGNED IPS   
 4 **IPS BY ASN**   
 5 RISK THRESHOLDS   
 6 LISTS

All Verdicts Filter

NAME	ASN	VERDICT
Dropbox	1000019851	<span>Allow</span> <span>Block</span>

dropbox Filter

PER PAGE: 20 < PREVIOUS 1 NEXT >

NAME	ASN	VERDICT
Dropbox	1000019851	<span>Allow</span> <span>Block</span>
Dropbox Inc	393874	<span>Allow</span> <span>Block</span>
Dropbox Inc.	62190	<span>Allow</span> <span>Block</span>
Dropbox Ireland Limited	1000021244	<span>Allow</span> <span>Block</span>
Dropbox, Inc.	19679	<span>Allow</span> <span>Block</span>
Dropbox, Inc.	54372	<span>Allow</span> <span>Block</span>

- Repeat for any other ASNs you want to add

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

✓ POLICY DETAILS   
 ✓ IPS BY COUNTRY   
 ✓ RESERVED AND UNASSIGNED IPS   
 ✓ **IPS BY ASN**   
 5 RISK THRESHOLDS   
 6 LISTS

All Verdicts Filter

NAME	ASN	VERDICT
Dropbox	1000019851	<span>Allow</span> <span>Block</span>
Digital Ocean	1000001621	<span>Allow</span> <span>Block</span> <span>Trash</span>
Microsoft Corp	1000016051	<span>Allow</span> <span>Block</span>

microsoft corp Filter

PER PAGE: 20 < PREVIOUS 1 NEXT >

NAME	ASN	VERDICT
Microsoft Corp	45139	<span>Allow</span> <span>Block</span>
Microsoft Corp	1000016051	<span>Allow</span> <span>Block</span>

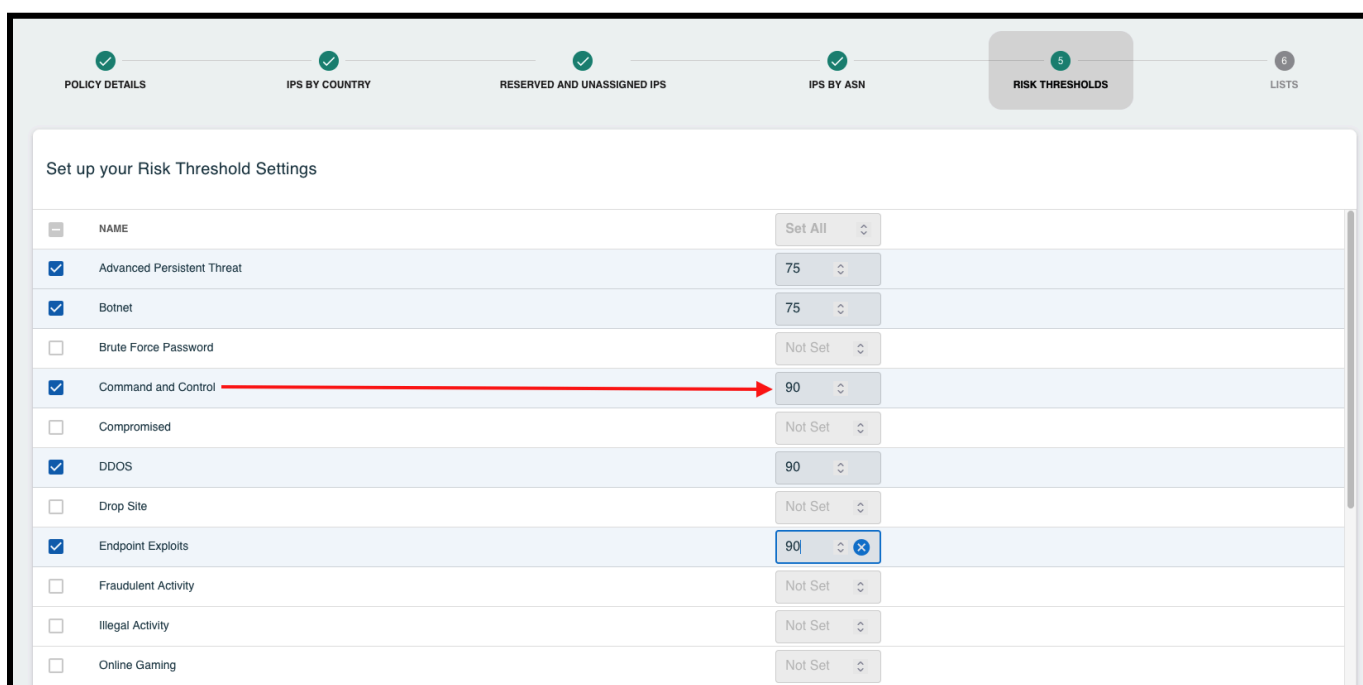
Click the Next button when all desired IPs by ASNs verdicts are applied.

## 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

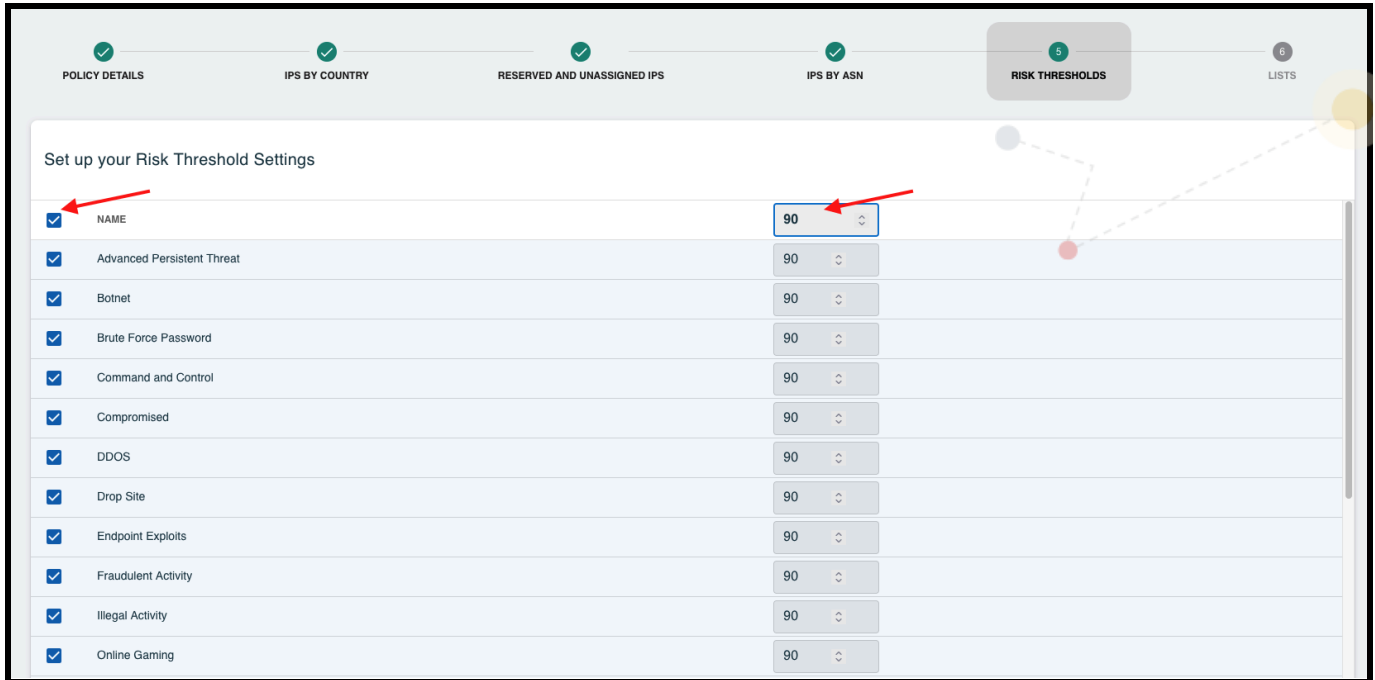
partners. Enabling categories and setting Risk Thresholds allows you to control how strong of a policy you want to apply. Since the Risk Threshold setting indicates confidence in malicious activity, the lower this is set, more traffic will be blocked.

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.

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.



Once all settings have been applied, select 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.

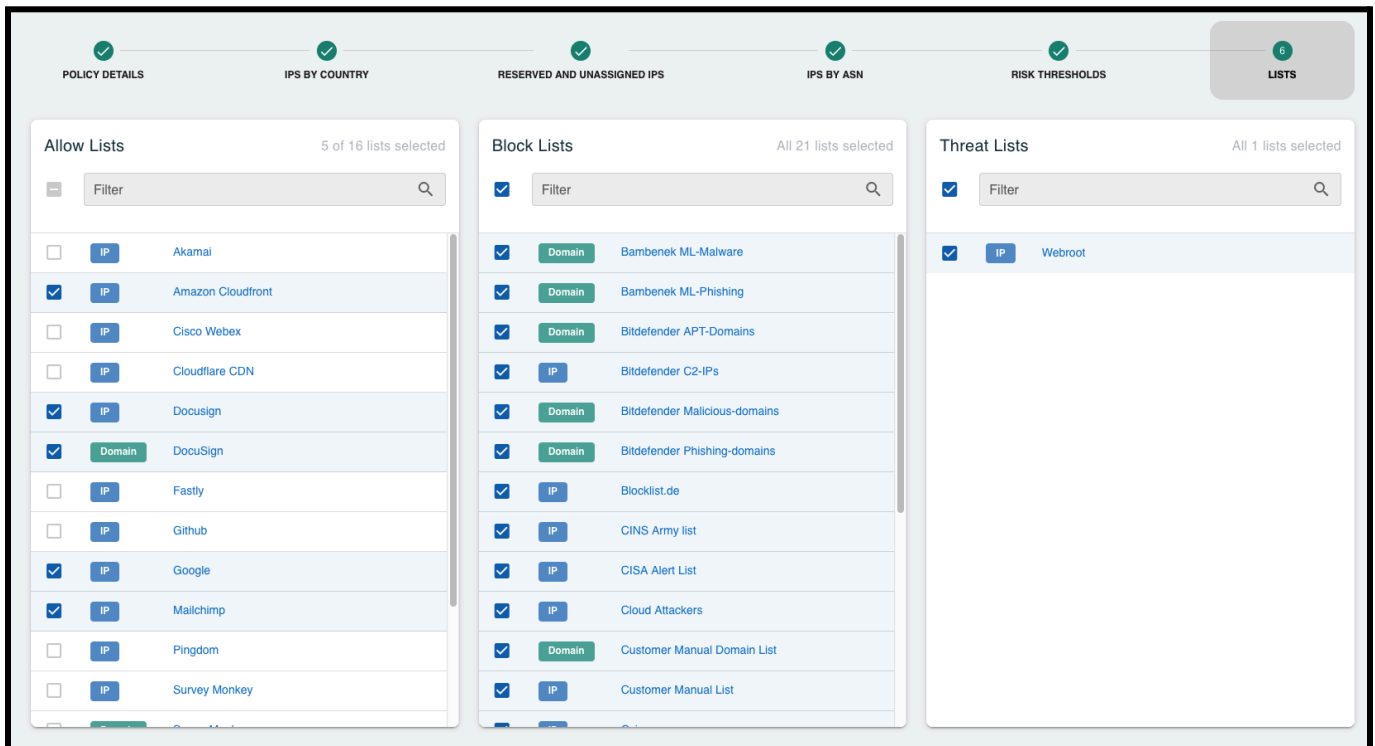
For example, if you're hearing that many legitimate sites or services are being blocked, and upon correlating with your logs find that they are being marked as spam with a score of 90–94, you can raise the threshold for the Spam category to 95. Now, you will see fewer unexpected blocks based on Spam.

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 and Blocked 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.



Once all desired Lists have been selected, select the "Create Policy" button. Your policy is now created.

### 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.

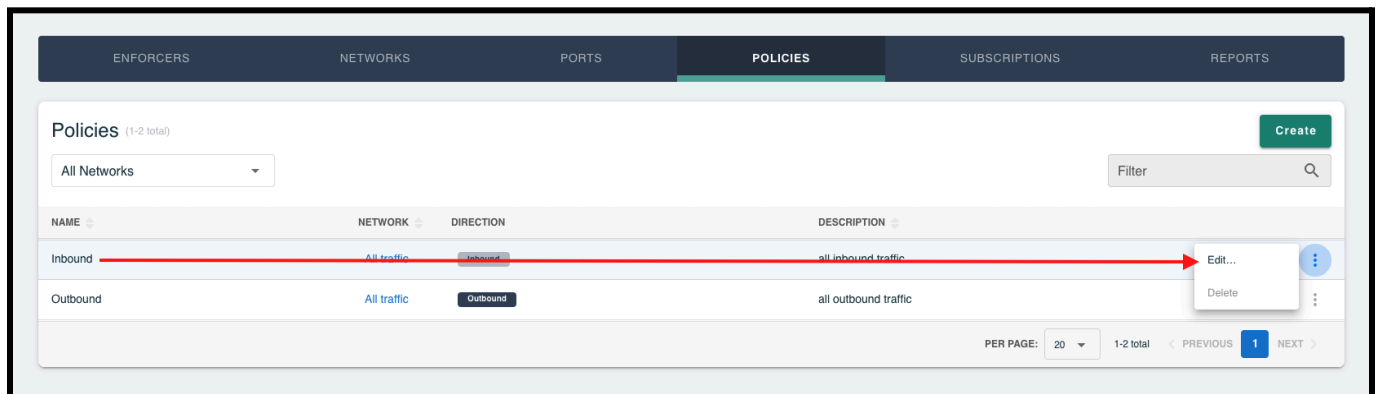
To create an Allow All policy, apply the following configurations on each step:

- **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

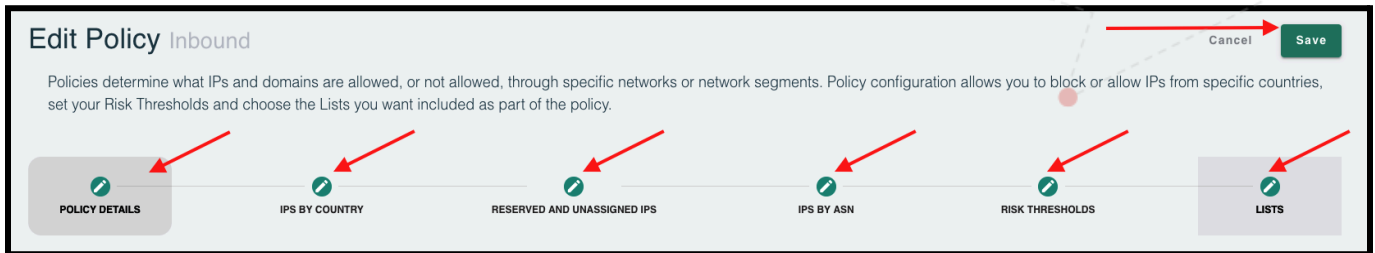
To edit configurations of an existing policy:

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



- 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 Save 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.

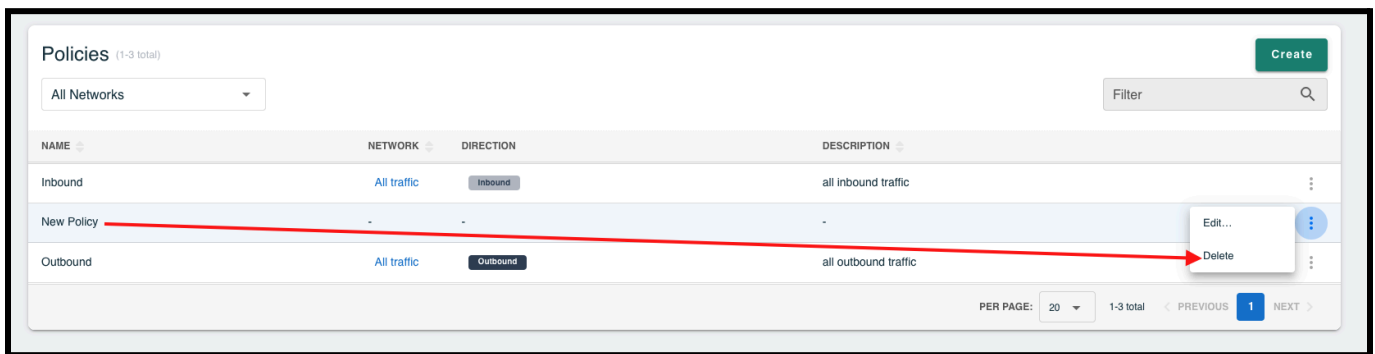


## Delete a Policy

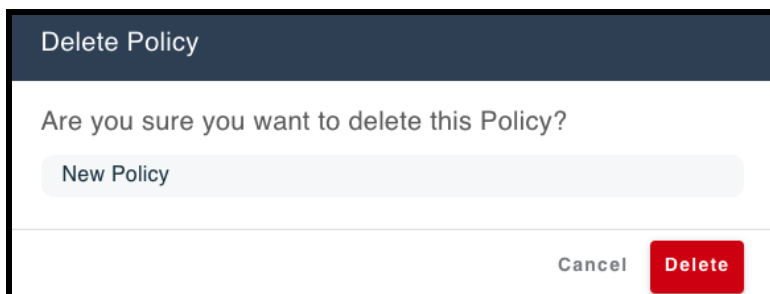
A Policy can only be deleted if there are no Networks utilizing that policy.

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



- On the confirmation modal, select Delete





To delete a policy that is being utilized by a Network, please refer to the steps to remove a policy from a Network first.

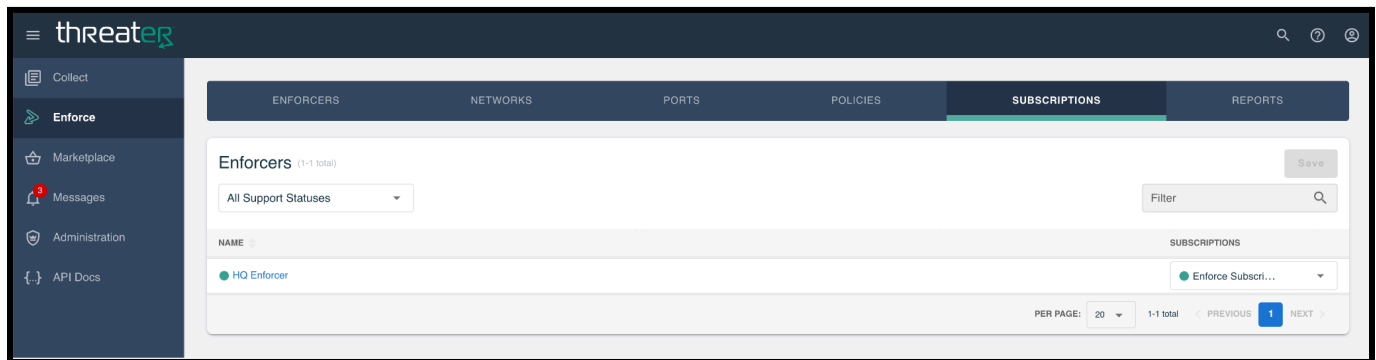


## Subscriptions

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.

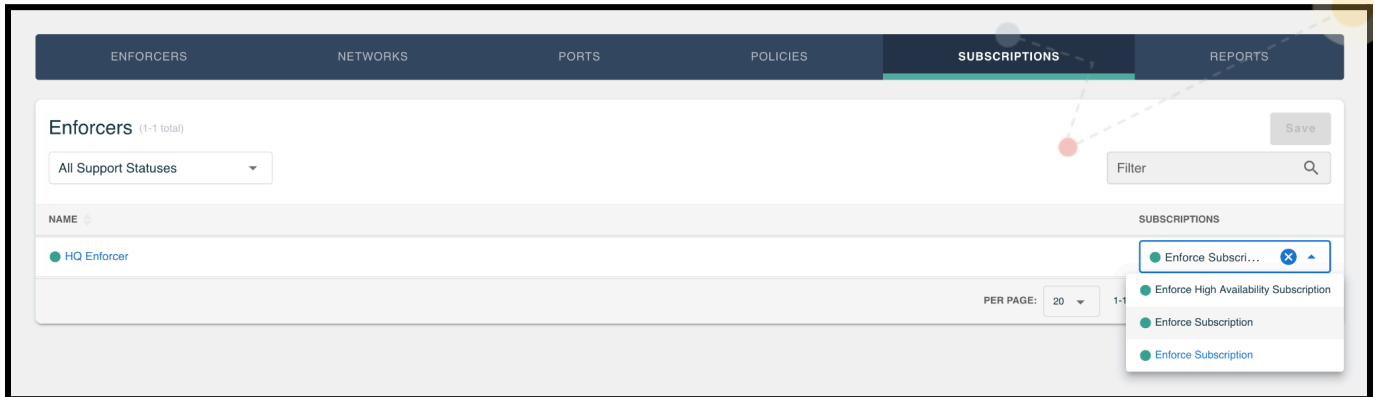
The following will display on this tab:

- 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

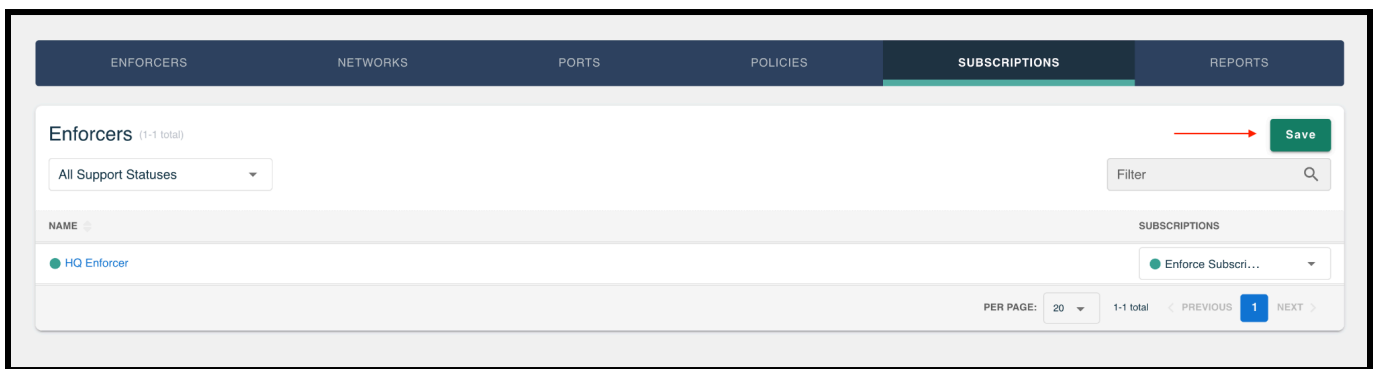


To assign a subscription to an Enforcer:

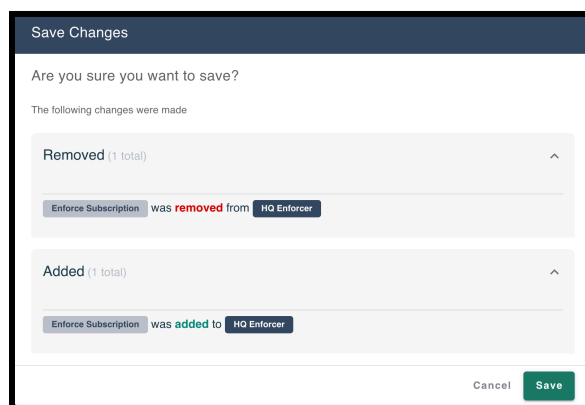
- Select the subscription from the drop-down



- Select the Save button



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



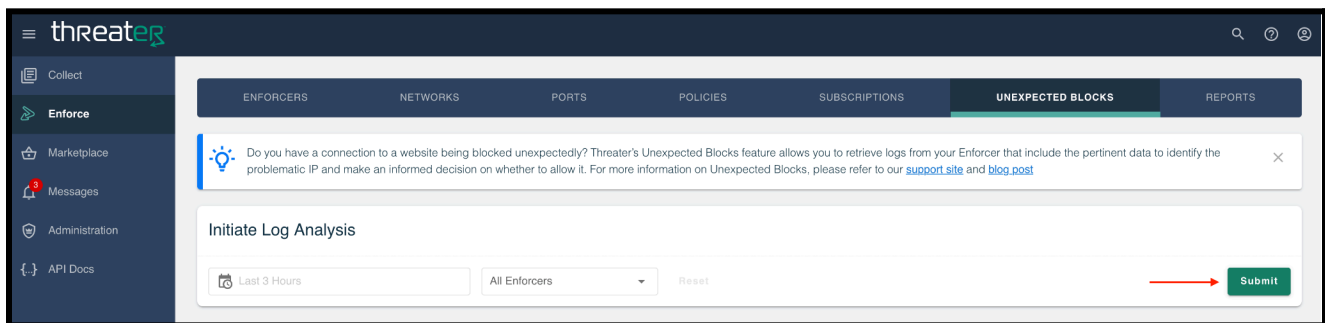
# Unexpected Blocks

**PREREQUISITE:** To access and utilize this feature, all Enforcers on your account need to be updated to BUILD 240 or later.

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

To perform an analysis:

- Navigate to Enforce in the left-hand navigation menu
- Select the Unexpected Blocks tab
  - This tab will NOT appear until all Enforcers tied to your portal account have been updated to at least Build 240
- 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



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

Once your submitted query is complete, the log entries will display on the Unexpected Blocks tab. To view additional data in each Log entry, expand the row via the disclosure triangle in the far left column. The additional

information can be very useful when determining whether or not an IP that is currently being blocked should be allowed.

**Log Entries** (1-10 of 144 total)

Filter

All Dates  All Enforcers (1)  All Policies (1)  All Lists (8)  All Reasons (2)

DATE	ENFORCER	POLICY	LISTS	REASON	PROTOCOL	ADDRESS										
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +1	Country	TCP	103.190.91.21:80										
▼ 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +3	Block List	TCP	95.128.43.164:80										
<table border="1"> <thead> <tr> <th>COUNTRY</th> <th>ASN</th> <th>REVERSE DNS</th> <th>WHOIS</th> <th>WHOIS.EXTENDED</th> </tr> </thead> <tbody> <tr> <td>Name: FRANCE ISO Code 2: FR</td> <td>Name: Aqua Ray SAS ASN: 41653</td> <td>TTL: 300 Class: IN Record Type: PTR Domain: exit-1.fr.tor.aquaray.com.</td> <td>ISO Code 2: FR Description: Tor servers Net Name: AQUARAY-TORS-SERVERS</td> <td>Autonomous System Name: AQUARAY, FR Allocated: 2009-01-20 Registry: ripenc ISO Code 2: FR BGP Prefix: 95.128.43.0/24 IP: 95.128.43.164 Autonomous System #: 41653</td> </tr> </tbody> </table>							COUNTRY	ASN	REVERSE DNS	WHOIS	WHOIS.EXTENDED	Name: FRANCE ISO Code 2: FR	Name: Aqua Ray SAS ASN: 41653	TTL: 300 Class: IN Record Type: PTR Domain: exit-1.fr.tor.aquaray.com.	ISO Code 2: FR Description: Tor servers Net Name: AQUARAY-TORS-SERVERS	Autonomous System Name: AQUARAY, FR Allocated: 2009-01-20 Registry: ripenc ISO Code 2: FR BGP Prefix: 95.128.43.0/24 IP: 95.128.43.164 Autonomous System #: 41653
COUNTRY	ASN	REVERSE DNS	WHOIS	WHOIS.EXTENDED												
Name: FRANCE ISO Code 2: FR	Name: Aqua Ray SAS ASN: 41653	TTL: 300 Class: IN Record Type: PTR Domain: exit-1.fr.tor.aquaray.com.	ISO Code 2: FR Description: Tor servers Net Name: AQUARAY-TORS-SERVERS	Autonomous System Name: AQUARAY, FR Allocated: 2009-01-20 Registry: ripenc ISO Code 2: FR BGP Prefix: 95.128.43.0/24 IP: 95.128.43.164 Autonomous System #: 41653												
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	107.189.1.96:80										
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	94.102.51.15:80										
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	103.251.167.20:80										
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +4	Block List	TCP	82.221.131.5:80										

**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, Graylog, and others) to sink all logs using the Enforcer’s built-in Syslog Export feature set, and then leverage the SIEM environment to perform unexpected blocks triage.

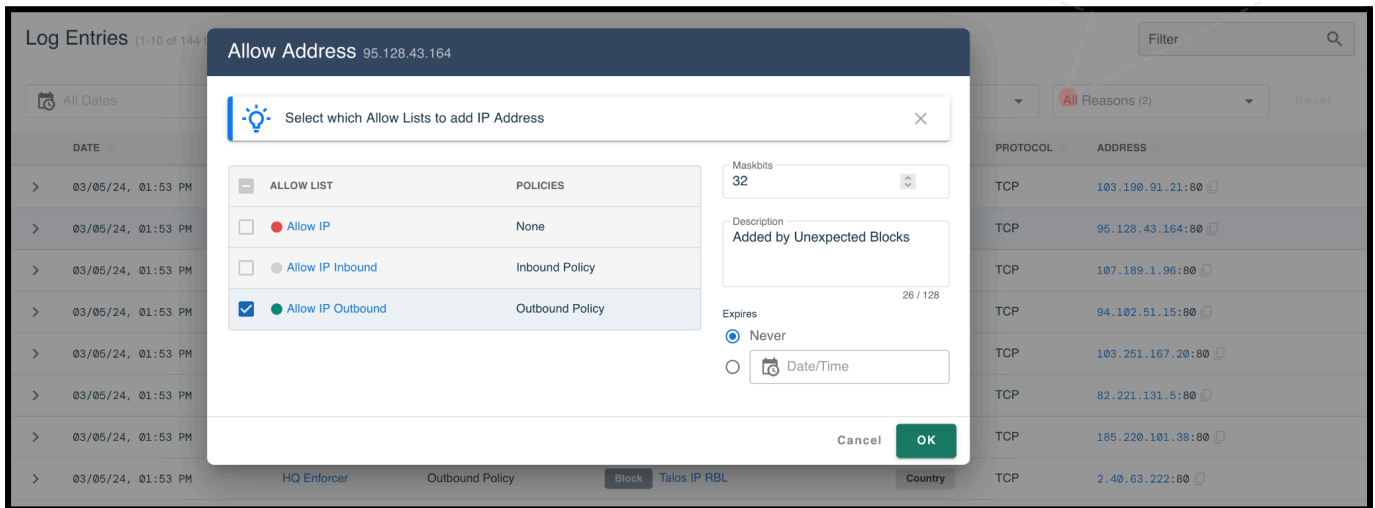
If an IP currently being blocked needs to be added to an Allow list:

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

DATE	ENFORCER	POLICY	LISTS	REASON	PROTOCOL	ADDRESS
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +1	Country	TCP	103.190.91.21:80
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Talos IP RBL +3	Block List	TCP	95.128.43.164:80
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	107.189.1.96:80
> 03/05/24, 01:53 PM	HQ Enforcer	Outbound Policy	Block Blocklist.de +3	Block List	TCP	94.102.51.15:80

- Select the 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.
- Click the “OK” Button

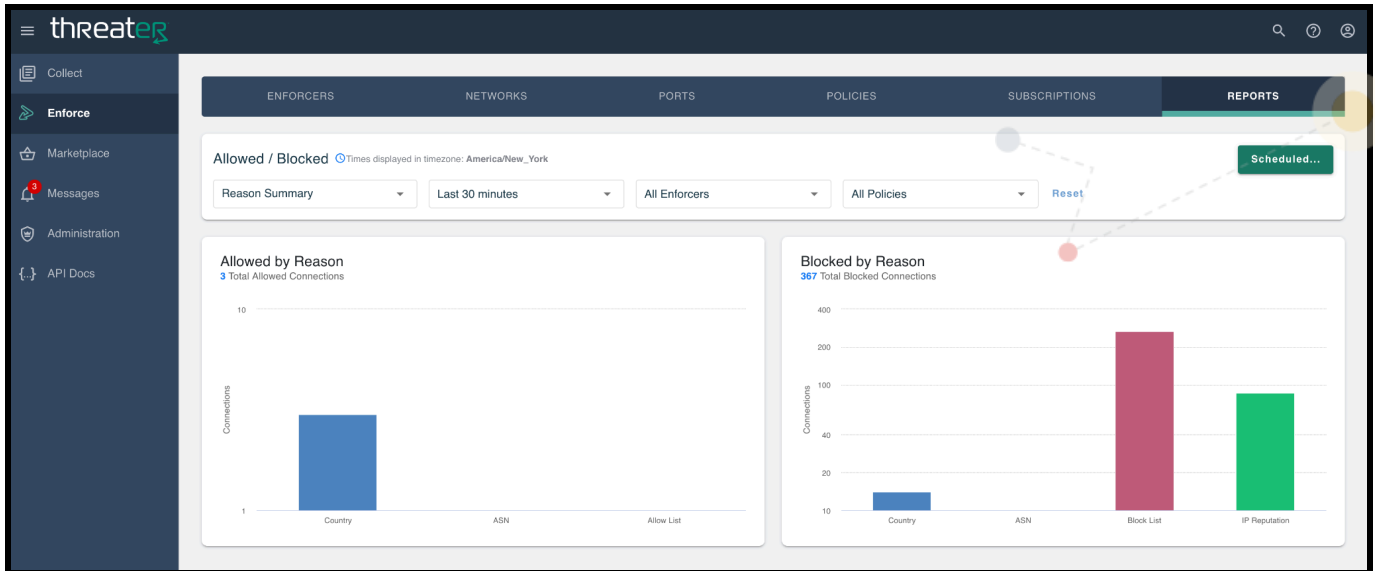


The IP is now added to the selected Allow list(s) and will be enforced by the policy(s) those lists are assigned to.

## 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.

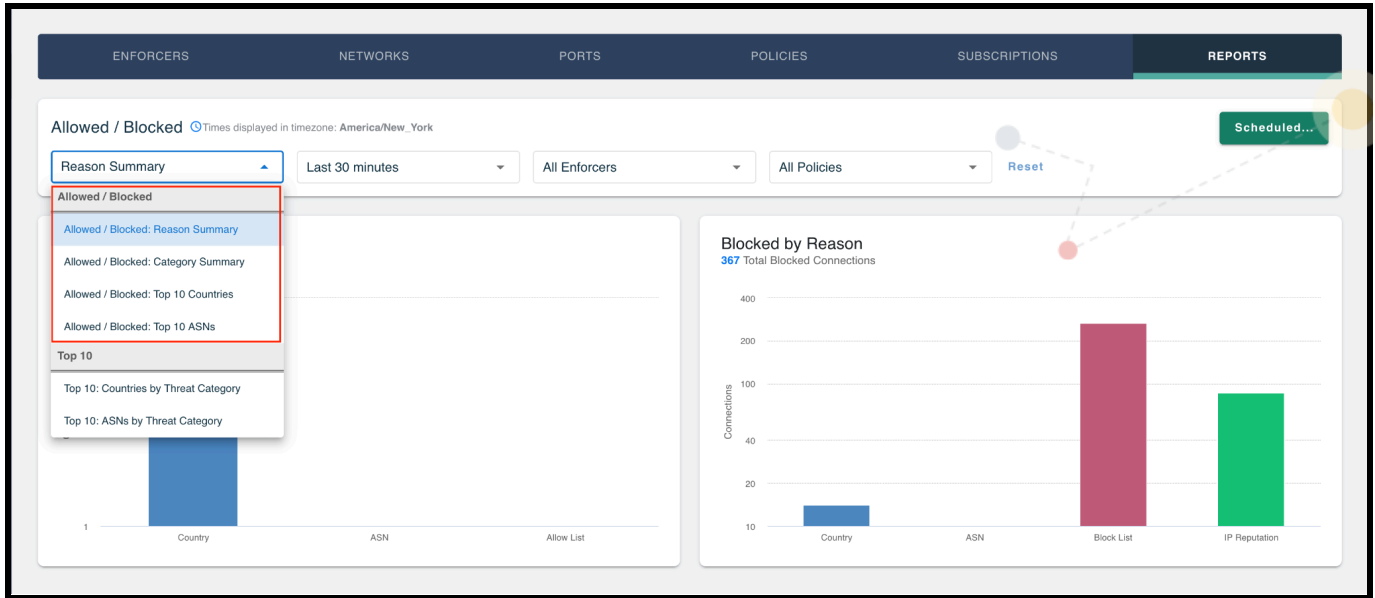
To access Reports, select Enforce from the left-hand navigation menu and then select the Reports tab. The “Allowed/Blocked: Reason Summary” report is the default view. All data in reports is displayed in your browser’s local time zone. There are 2 types of reports (Allowed/Blocked & Top 10) and each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



## Allowed/Blocked

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.



## Reason Summary

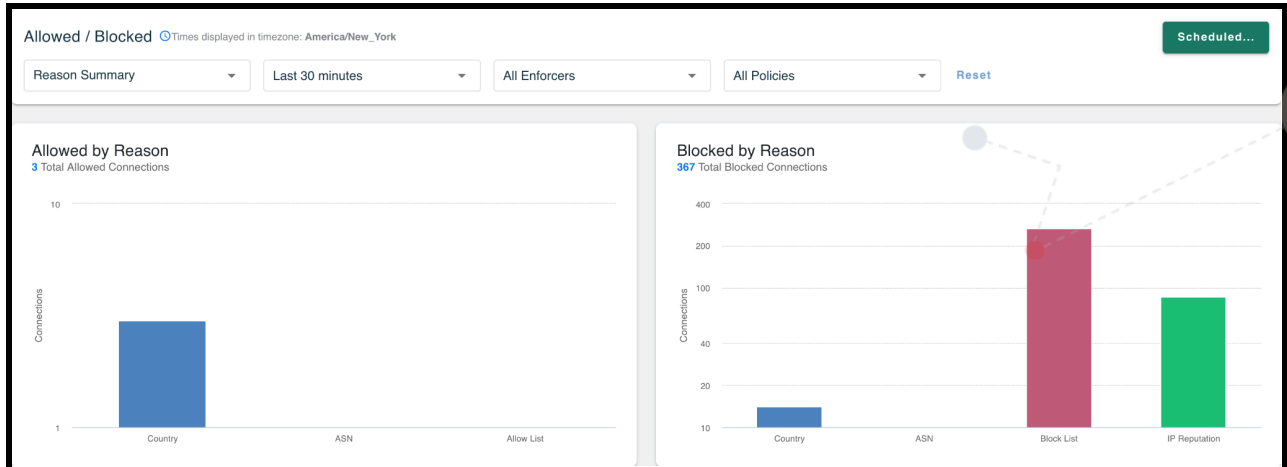
The Allowed by Reason report displays connections that were allowed because of the following reasons (the below reasons are in the order the system processes enforcements):

- 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):

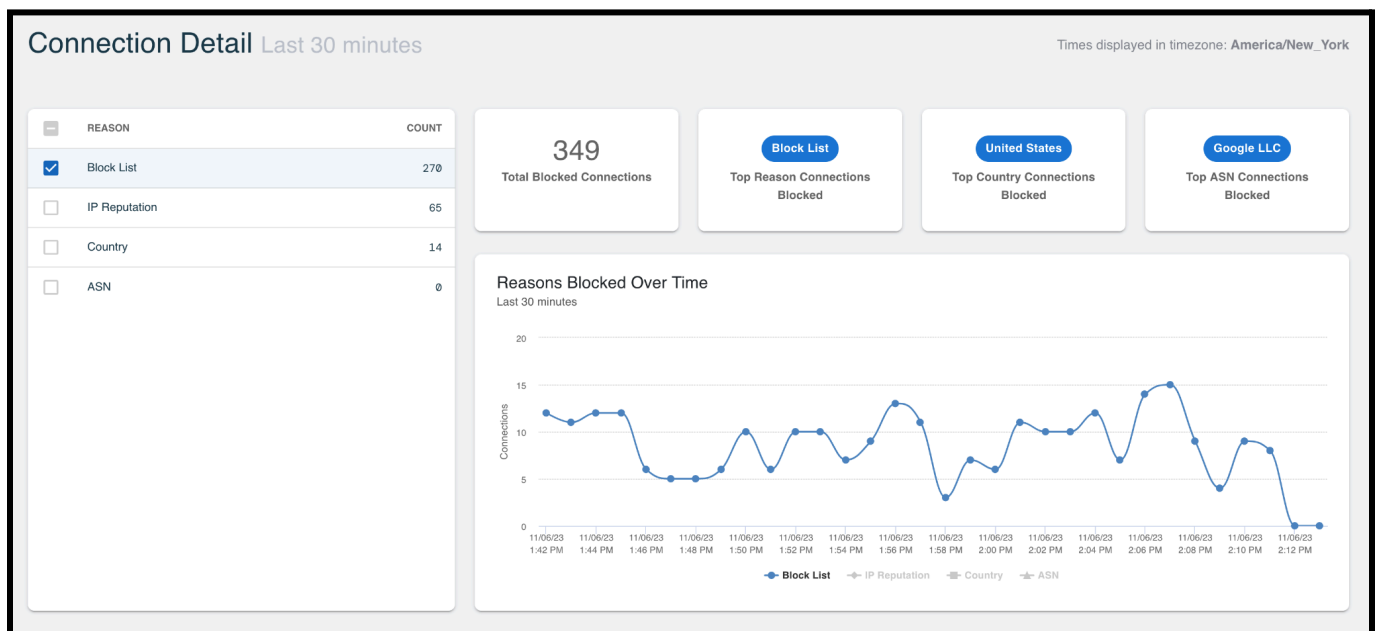
- Block List – connections blocked based on explicit Block list content
- IP Reputation – connections blocked based on explicit Threat list content
- ASN – connections blocked by ASN adjustments
- Country – connections blocked by a policy that were not specifically blocked by a Block List





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

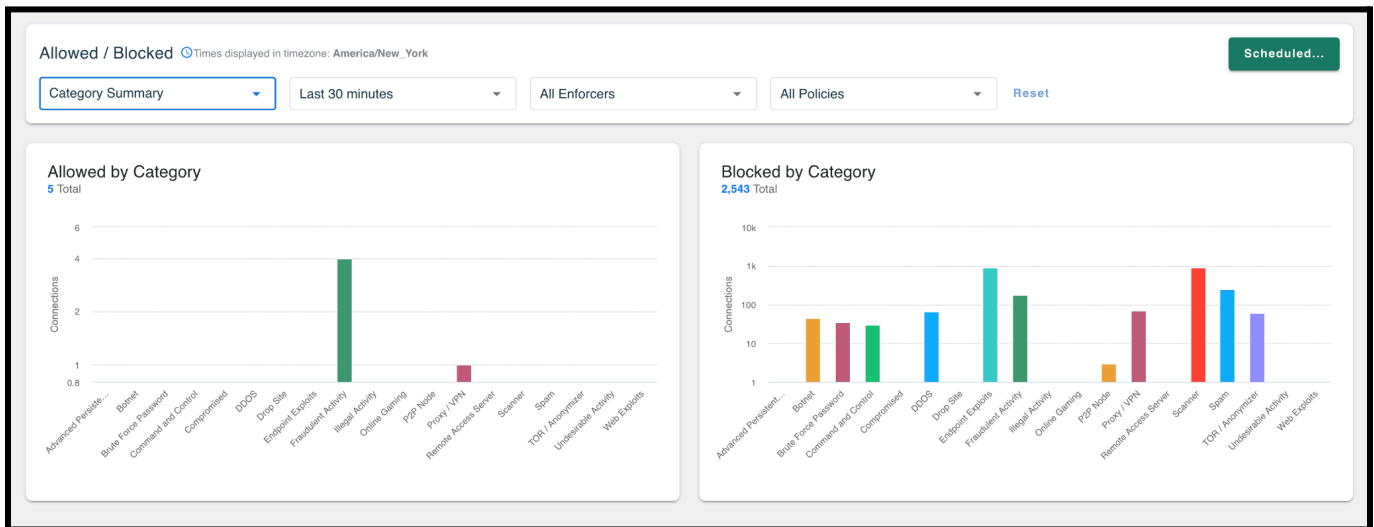
- Reasons and Count panel
  - Displays all reasons and the count for each
    - Default selection will be the reason selected on the previous graph
  - Selecting additional reasons will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or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



## Category Summary

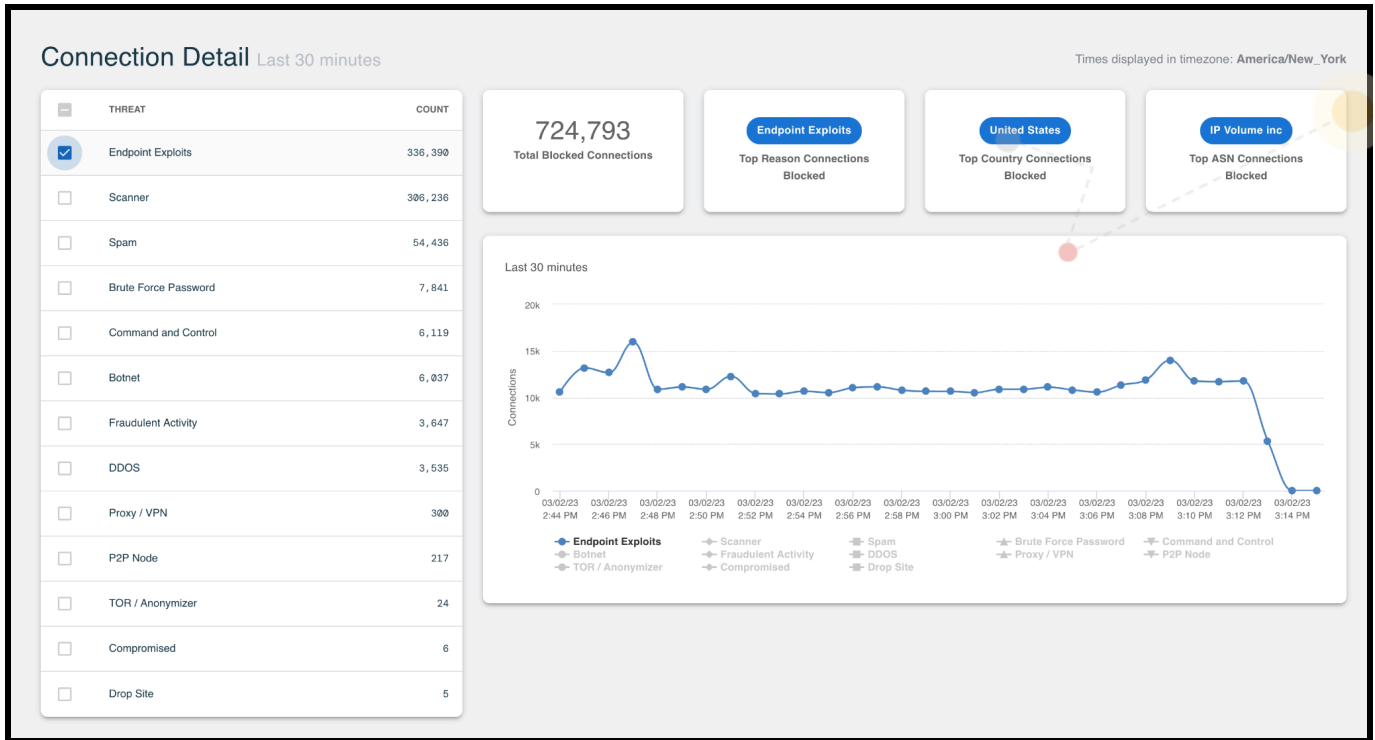
The Allowed by Category report displays allowed connections that were indicated as part of a threat category, but fell below the configured thresholds for blocking at the time of connection.

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.



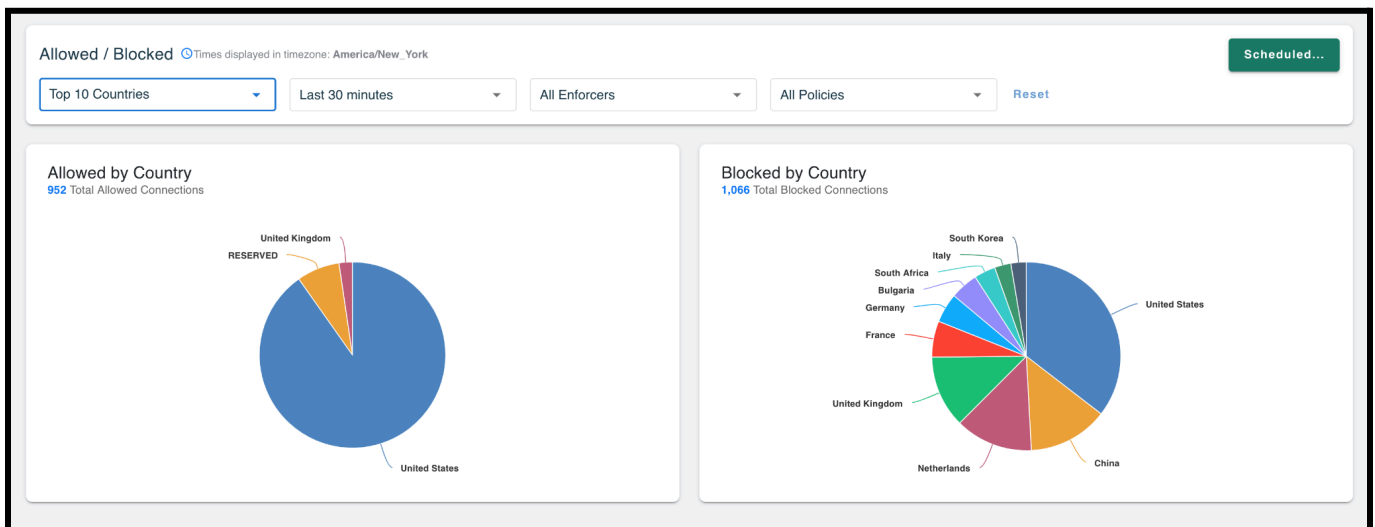
Clicking on a slice of data will open the Connection Detail for the report and display the following:

- 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



## Top 10 Countries

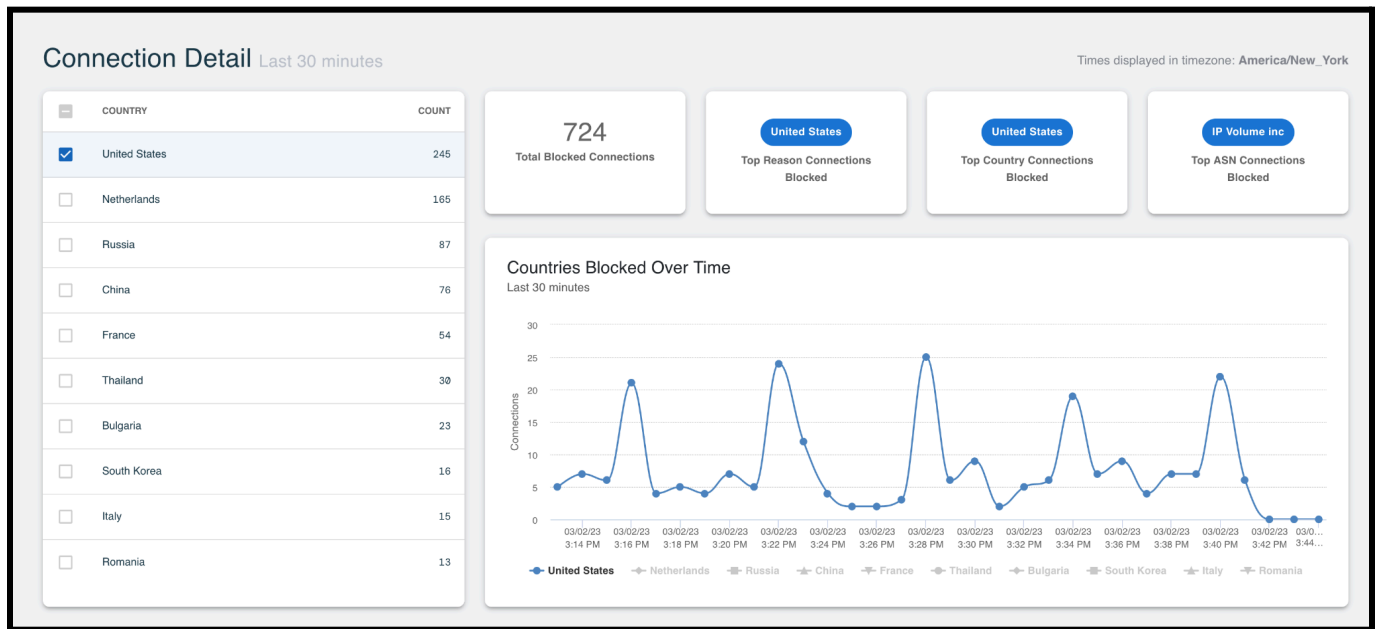
The Top 10 Countries report displays the countries the connections came from, based on what was allowed or blocked.



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

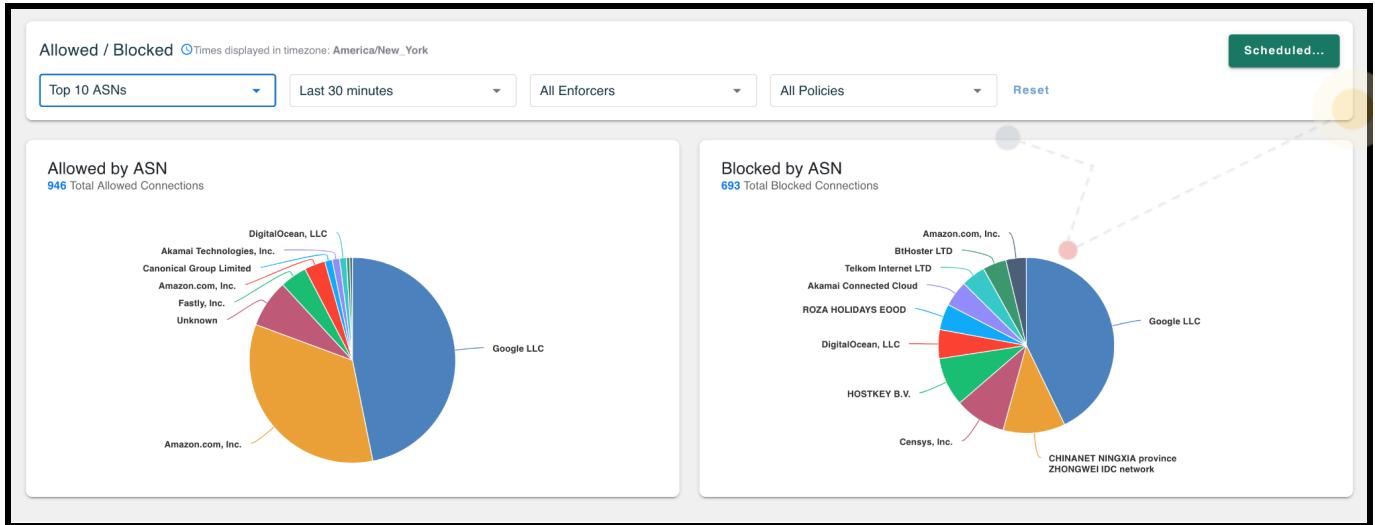
- Country and Count panel

- 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



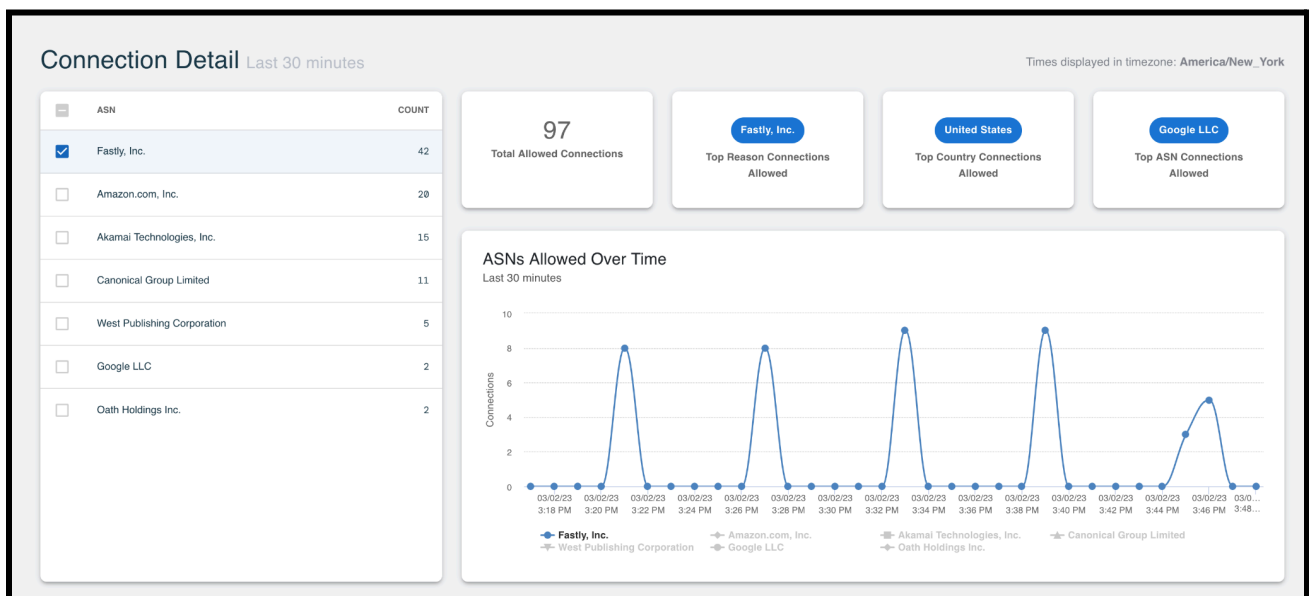
## Top 10 ASNs

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



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

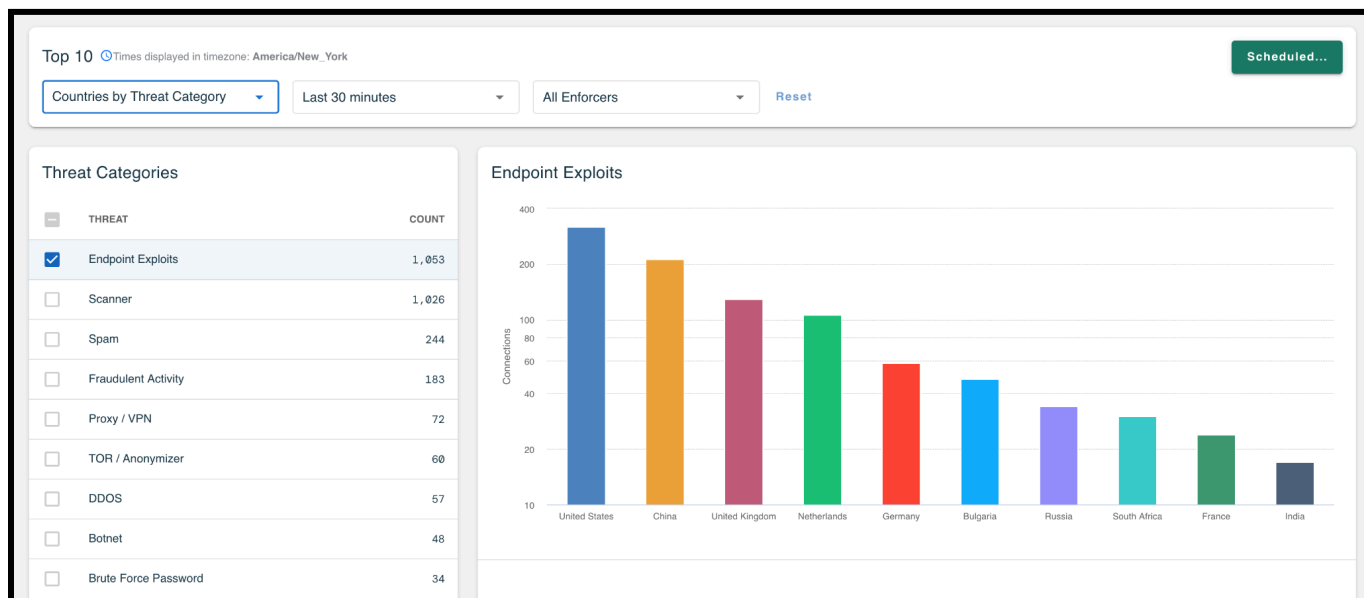
- ASN and Count panel
  - Displays the applicable ASNs and the count for each
    - Default selection will be the ASN selected on the previous graph
  - Selecting additional ASNs will add that data to the graph on the right
- Total Blocked or Allowed Connections
- Top Reason Connections Blocked or Allowed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



## 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.

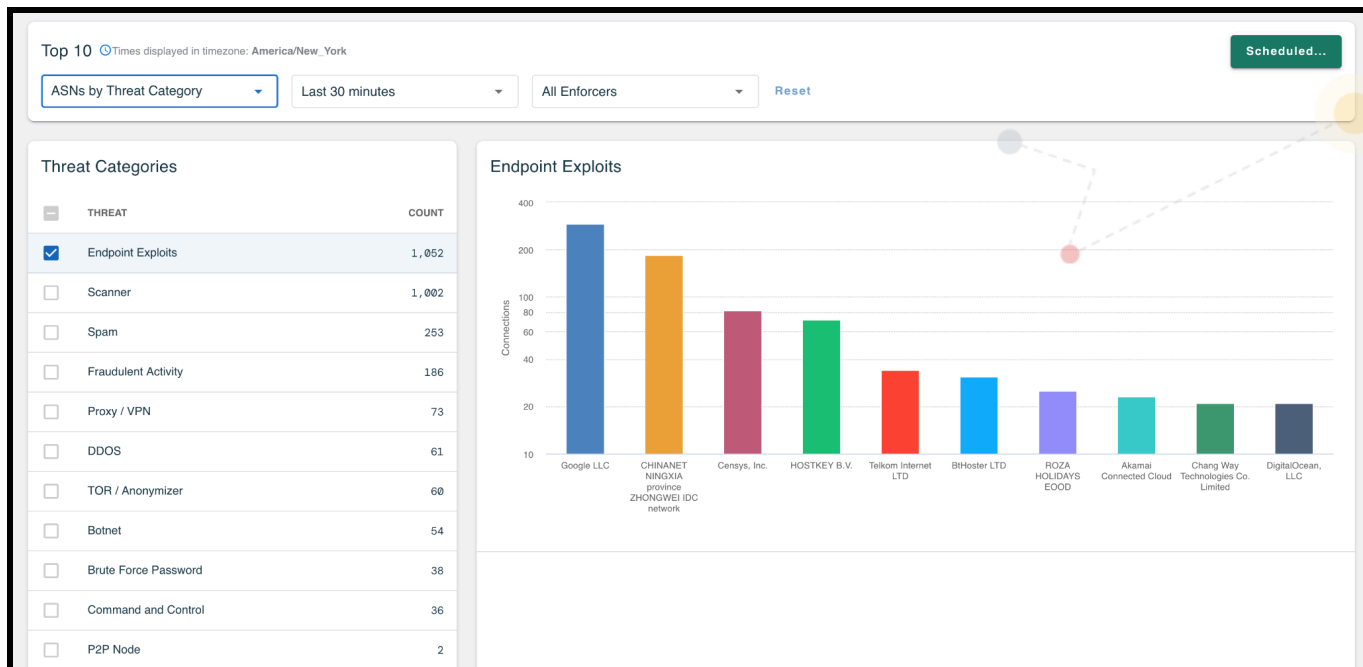


The Threat Category with the highest count will be selected by default and its graph will display in the right-hand panel. To view a graph for additional Threat Categories, select the desired category(s) in the left-hand panel.

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.



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.

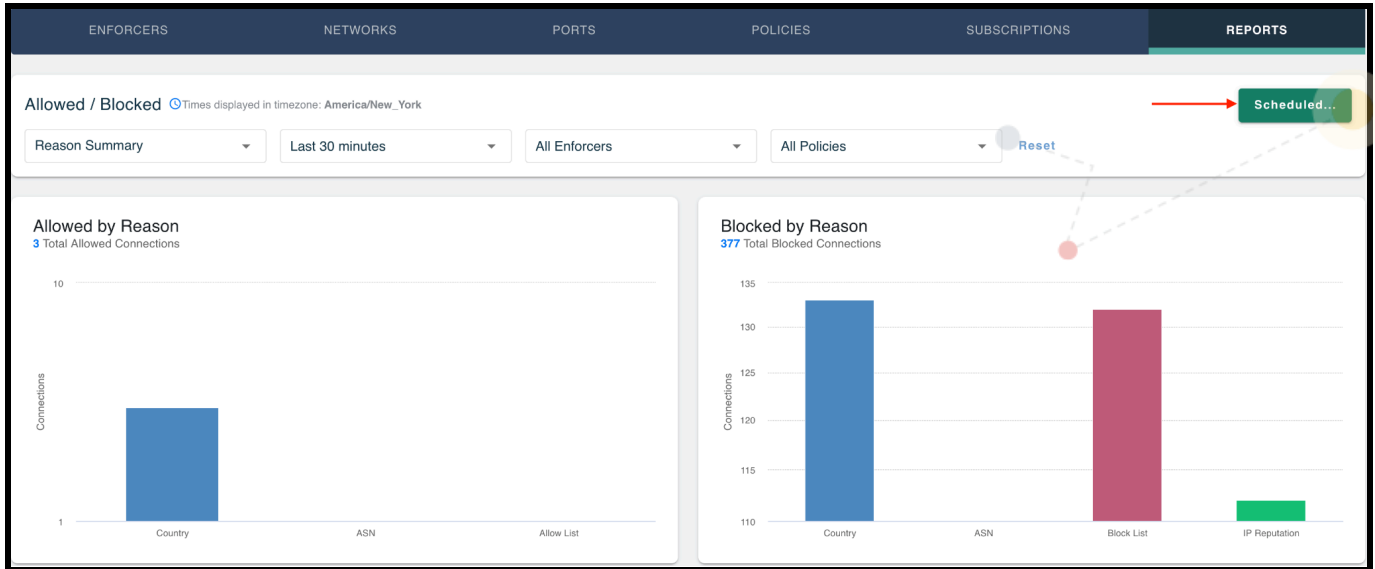
Each threat category graph will display a bar for the top 10 ASNs with connections that have been flagged with that threat category. You can scroll over each bar to view the number of connections, based on the timeframe and Enforcer selected from the filters at the top of the screen.

## 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:

- Selecting the "Scheduled" button in the top-right corner of a report



- Select the Create button in the top right corner

The screenshot shows the 'Scheduled Reports' section of the threatER interface. At the top, there are navigation tabs: ENFORCERS, NETWORKS, PORTS, POLICIES, SUBSCRIPTIONS, and REPORTS. Below the tabs, the main heading is 'Scheduled Reports (1-1 total)'. There is a dropdown menu for 'All Reports' and a 'Filter' search box. A red arrow points to a 'Create' button in the top right corner. Below the filters is a table with one report entry. At the bottom right, there is a 'PER PAGE: 20' dropdown and a pagination control showing '1-1 total' and '1' of 1 pages.

NAME	REPORT	LAST RUN	NEXT RUN	DESCRIPTION
Allowed - Blocked Report	Allowed / Blocked: Reason Summary	11/07/23, 12:00 AM	11/08/23, 12:00 AM	Daily report of what was allowed and blocked the previous day

- Selected 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
- Select the Create button



**Create Scheduled Report**

Enabled

Report ▼

Name 0 / 64

Delivery Email

Description 0 / 128

---

Preset ▼

Select Preset...

Timezone

America/New\_York

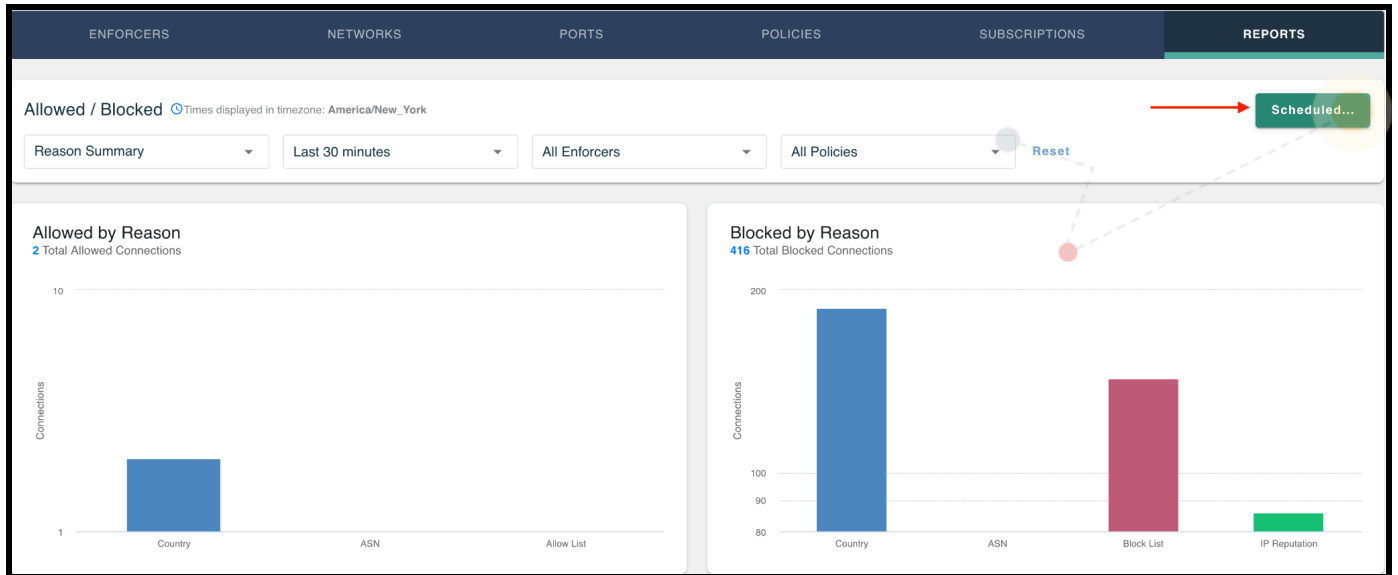
Cancel Create

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, select the Scheduled button



- Select Edit from the ellipsis menu in the row of the report you would like to edit

The screenshot shows the 'Scheduled Reports' section. It includes a 'Create' button, a filter input, and a table with columns: NAME, REPORT, LAST RUN, NEXT RUN, and DESCRIPTION. The table contains one row for 'Allowed - Blocked Report' with a report type of 'Allowed / Blocked: Reason Summary', last run on 11/07/23 at 12:00 AM, and next run on 11/08/23 at 12:00 AM. An ellipsis menu is open for this row, showing 'Edit...' and 'Delete' options, with a red arrow pointing to 'Edit...'. At the bottom right, there are pagination controls: 'PER PAGE: 20', '1-1 total', and navigation arrows.

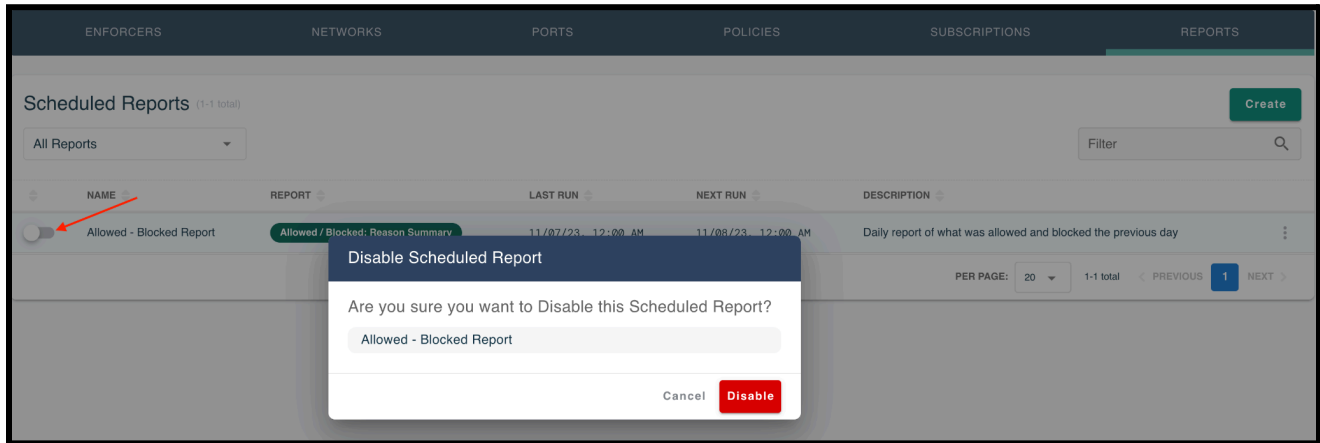
- Make the desired updates and then select the Save button

The screenshot shows the 'Edit Scheduled Report' form. It includes a toggle for 'Enabled' (checked), a 'Report' dropdown set to 'Allowed / Blocked: Reason Summary', a 'Name' field with 'Allowed - Blocked Report', a 'Delivery Email' field with 'companymasteruser@valuedcustomer.com', a 'Description' field with 'Daily report of what was allowed and blocked the previous day', a 'Policy' dropdown set to 'All Policies', an 'Enforcer' dropdown set to 'All Enforcers', a 'Preset' dropdown set to 'Yesterday', and a 'Timezone' field set to 'America/New\_York'. At the bottom, there are 'Cancel' and 'Save' buttons, with a red arrow pointing to 'Save'.

## Disabling Scheduled Reports

To disable a scheduled report:

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



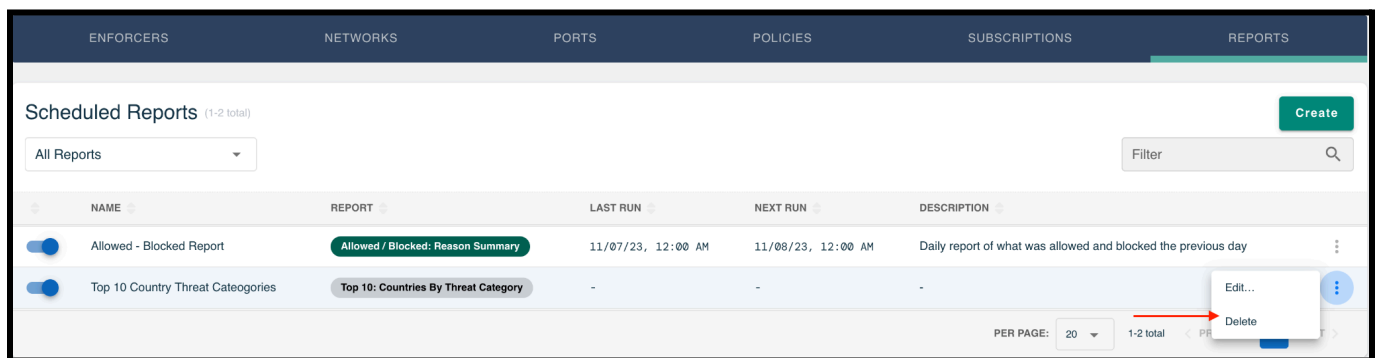
The report is now disabled and will no longer be emailed to the address that was provided.

To enable the report at a later date, position the toggle to the right and confirm the action.

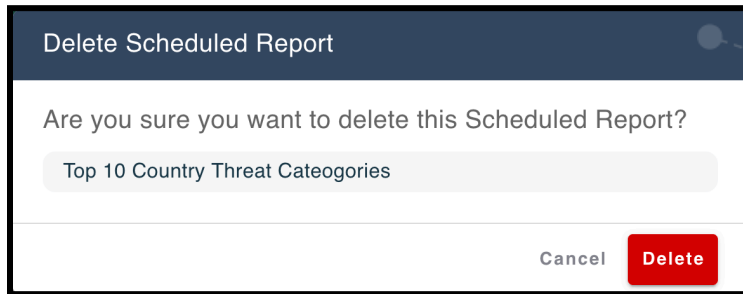
## Deleting Scheduled Reports

To delete a scheduled report:

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



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

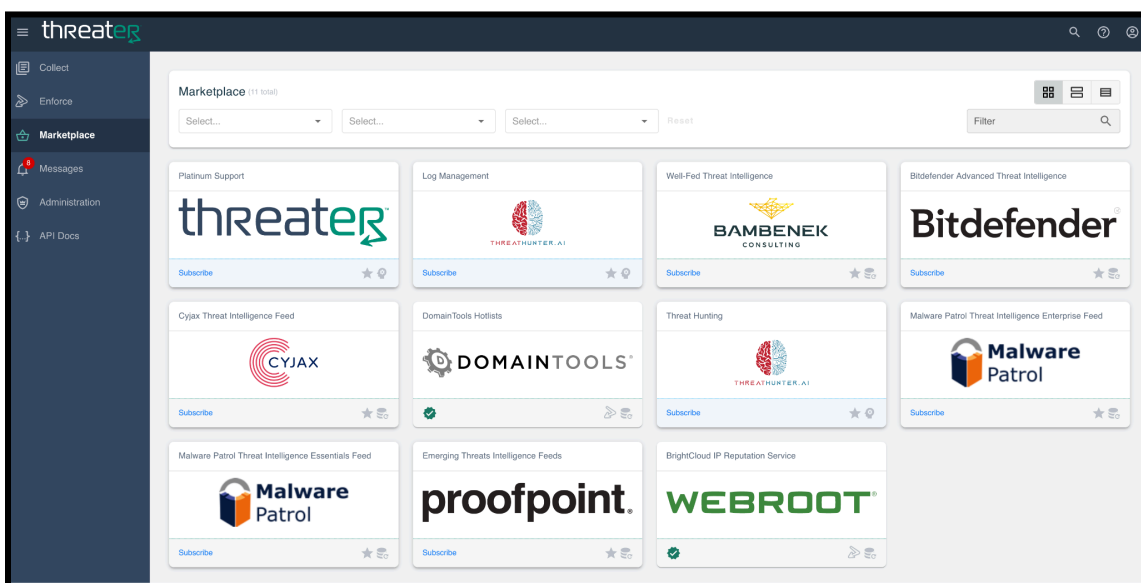


The report is now deleted, will not display in the Scheduled Reports table, and will no longer be emailed.

# Marketplace

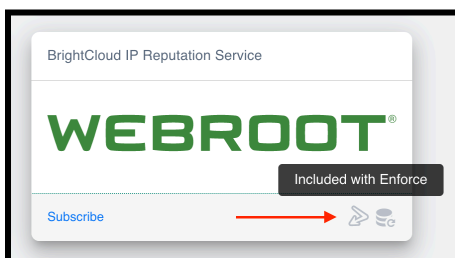
The Marketplace provides threatER customers access to high-value, multi-source cyber intelligence data from leading intelligence providers, as well as services to help manage and resolve threats in your network. Our Marketplace includes offerings from longtime partners, premium offerings from new partners, and an expanded partnership with DomainTools.

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.

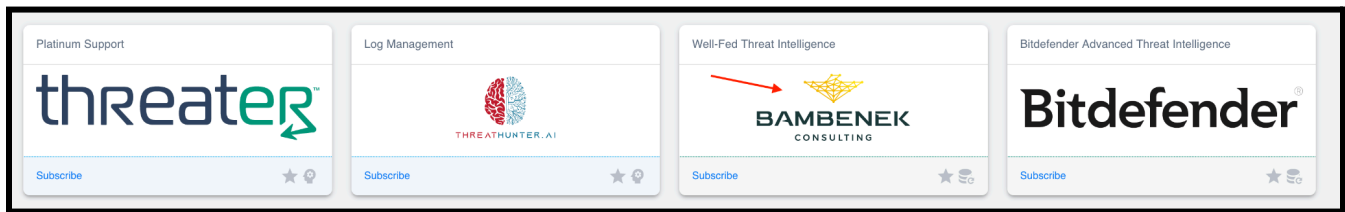


# Premium Intelligence Products

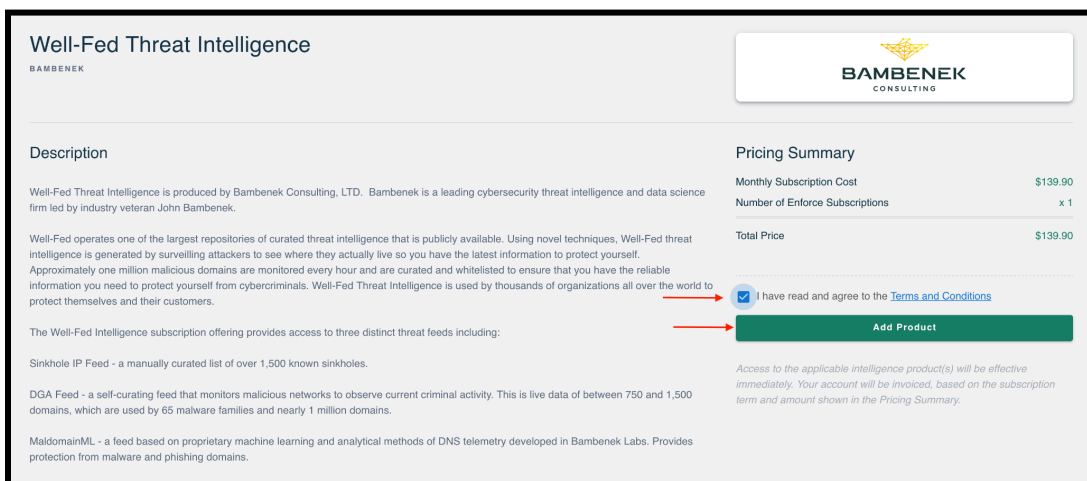
You may choose to purchase supplemental premium cyber intelligence feeds that are not included with your Enforce subscription. The pricing of these products is based on the total number of Enforcers on your account.

To purchase a product:

- Select the product from the list



- Review the terms of the subscription provided on the next screen
- Select 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
- Select the Add Product button



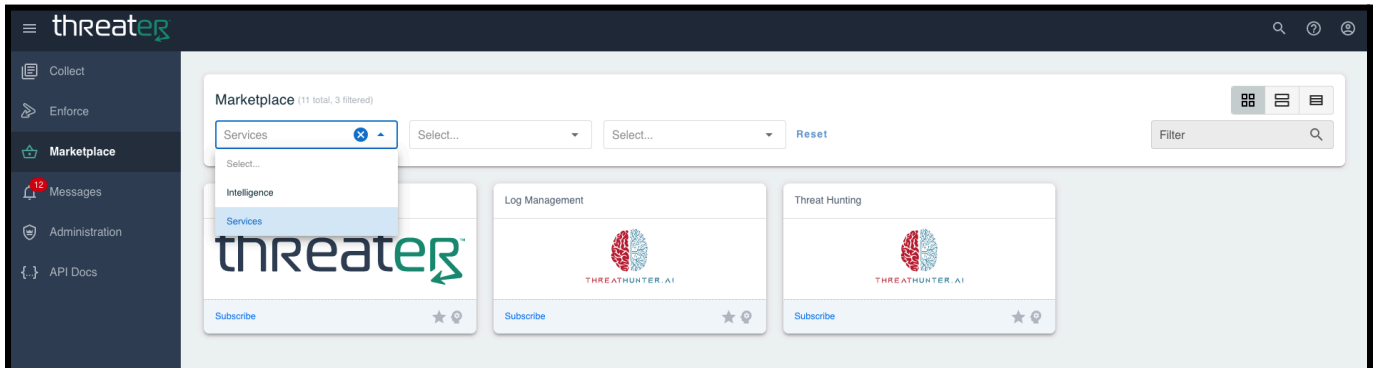
A modal will display providing further details about the subscription, to include the feeds you now have access to. Review these details and then select the OK button to close the modal. You will be redirected to the full list of Marketplace products. The product will now display as Subscribed.

# Services

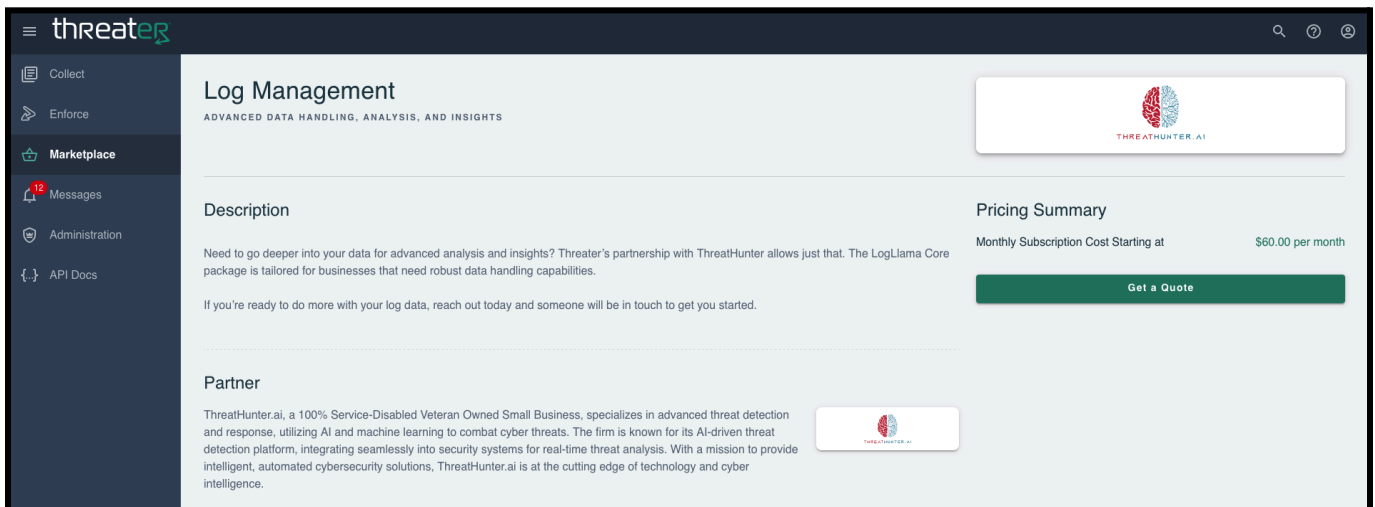
The threatER Marketplace included Services products that help manage and resolve threats in your network.

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

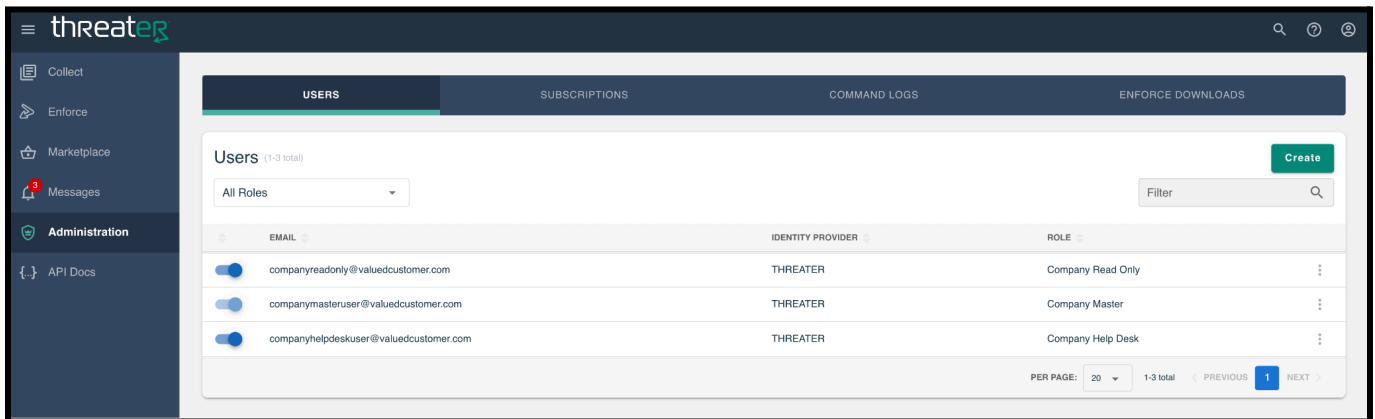


After your request is submitted, someone from our team will contact you to discuss the necessary details and onboard the service to your account.

# 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 select the User tab.



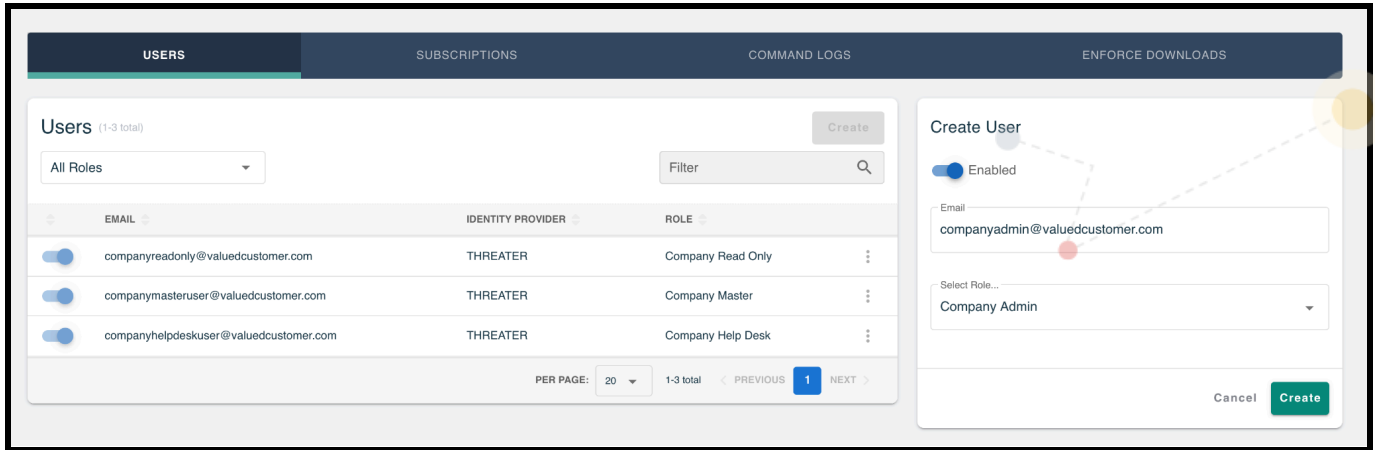
Please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

## Create New User

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

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





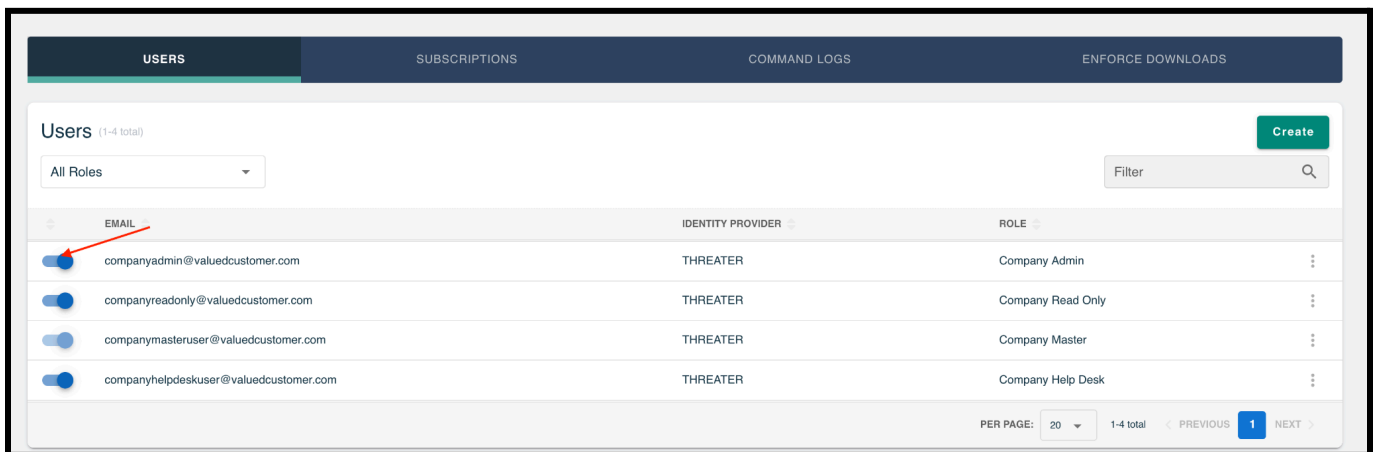
The new user will be created and an Account Activation email will be generated to the email provided. This email will contain the link for the user to complete the setup of their threatER account.

## Edit User Accounts

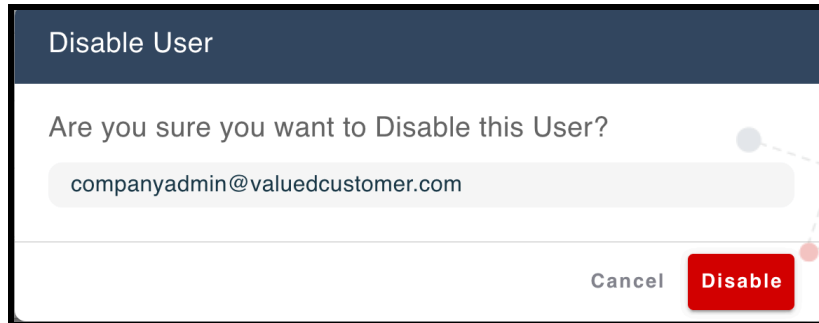
### Disable an Account

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, select the Disable button

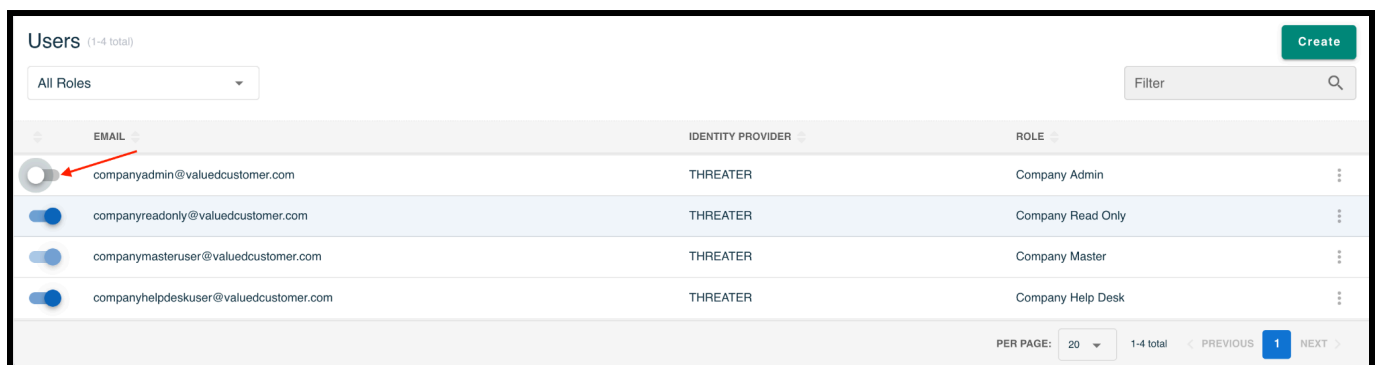


The user is now disabled and will not be able to log into the portal.

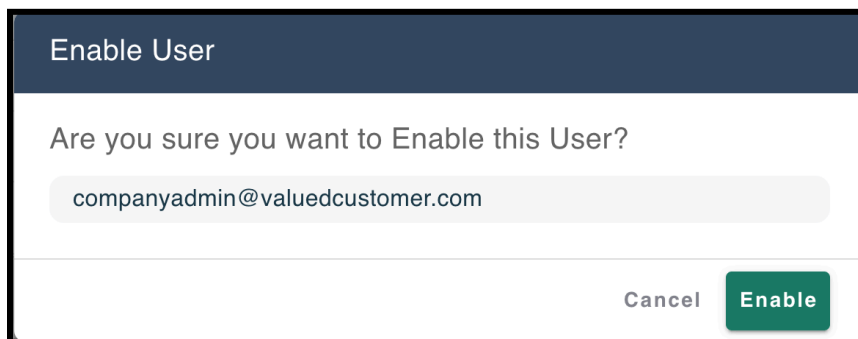
## Enable an Account

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, select the Enable button



## 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
- Select Save



The screenshot shows the 'Users' management interface. On the left, a table lists users with columns for EMAIL, IDENTITY PROVIDER, and ROLE. The first user is 'companyadmin@valuedcustomer.com' with the role 'Company Admin'. On the right, the 'Edit User' modal is open, showing the 'Email' field with the value 'companyadmin@valuedcustomer.com' and a red arrow pointing to it. Below the email field is a 'Select Role...' dropdown menu with 'Company Admin' selected. There are also 'Password' and 'Confirm Password' fields, each with a 'Leave Password fields blank to keep current Password' note. At the bottom right of the modal are 'Cancel' and 'Save' buttons.

EMAIL	IDENTITY PROVIDER	ROLE
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

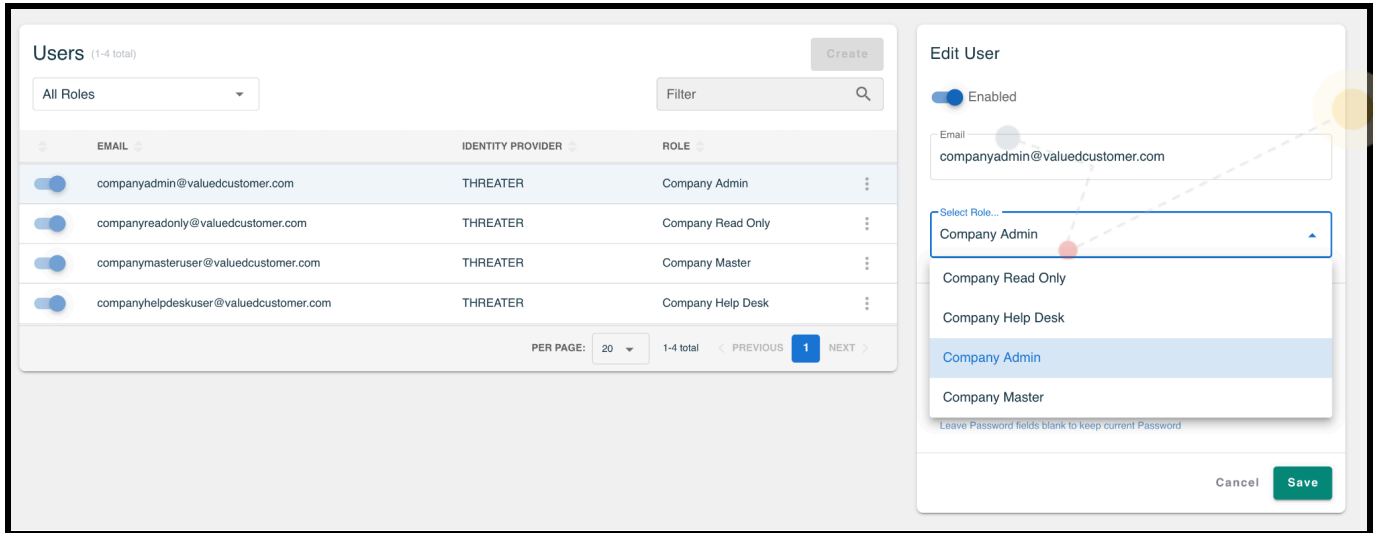
The user's email address is now updated and this is the username the user needs to use when logging into the portal.

## 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
- Select Save



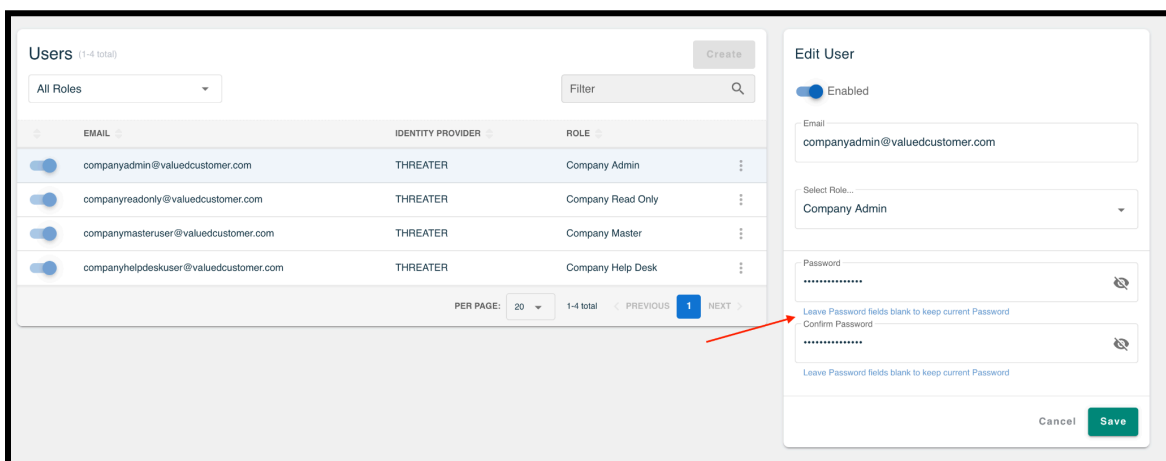


NOTE: please refer to the Appendix for an overview of what actions each user role can perform within the admin console.

## 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
- Select Save

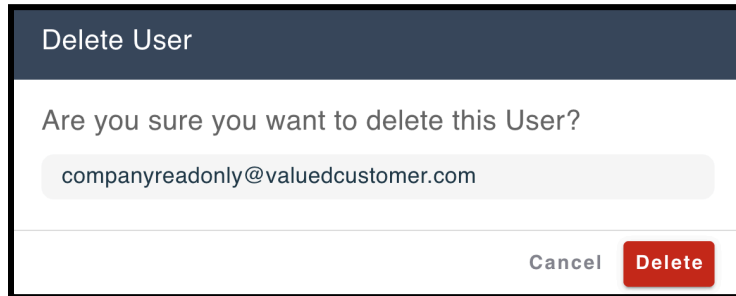


The user's password is now updated and this is the password the user will need to use when logging into the portal.

## Delete Users

To delete a user:

1. Search for the user
2. From the ellipsis menu in the right-hand column of the row, select Delete
3. On the Delete User confirmation modal, select the Delete button

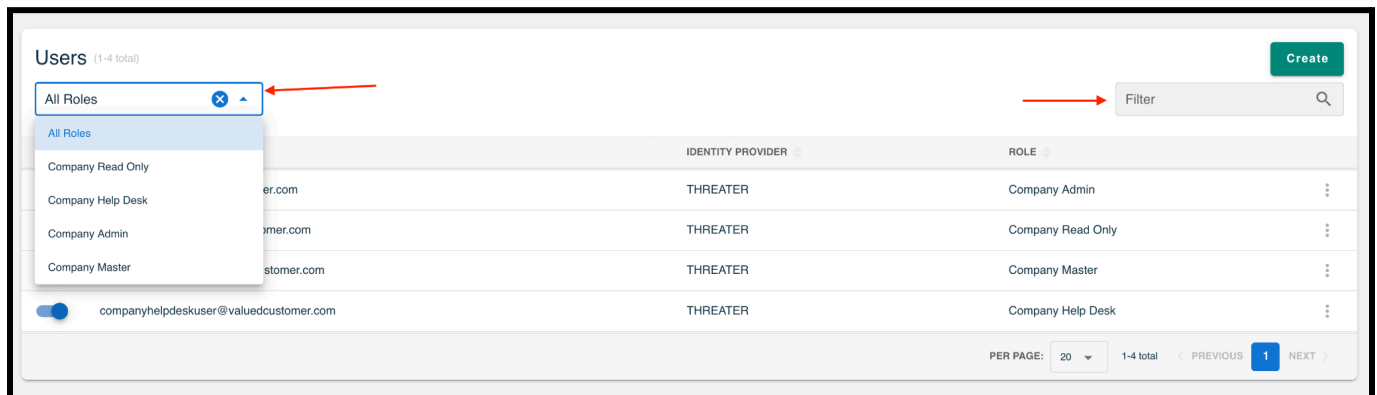


The user is now deleted and will not be able to access the admin console.

## Users Filter

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

- All 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.



# Subscriptions

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

NAME	TYPE	ENFORCER
Enforce Subscription	Enforce	HQ Enforcer
Enforce High Availability Subscription	Enforce	-
Enforce Subscription	Enforce	-
Bitdefender Intelligence Subscription 3Gb	Marketplace	-
Cyjax Intelligence Subscription	Marketplace	-
DomainTools IP Hotlist	Marketplace	-
Malware Patrol Enterprise Cyber Intelligence Subscription	Marketplace	-
WELL-FED Intelligence Subscription 3Gb	Marketplace	-

# 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.

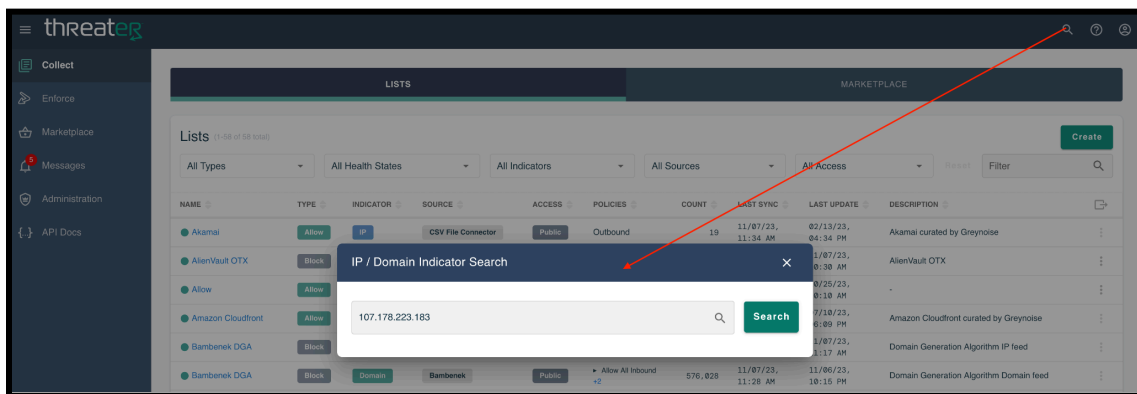
DATE	USER	INITIATOR	MODULE	ACTION	MESSAGE
11/07/23, 10:49:02	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companyadmin@valuedcustomer.com" modified: 'active' => 'True'
11/07/23, 10:47:49	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companyadmin@valuedcustomer.com" modified: 'active' => 'False' (was 'True')
11/07/23, 10:46:09	companymasteruser@valuedcustomer.com	User	User	Update	companymasteruser@valuedcustomer.com: User "companyadmin@valuedcustomer.com" modified: 'email' => 'companyadmin@valuedcustomer.com' (was 'marie.knight+userguideadmin@threat.com')
11/07/23, 10:45:53	companymasteruser@valuedcustomer.com	User	User	Delete	companymasteruser@valuedcustomer.com: User deleted - email: marie.knight+userguide@threatblockr.com, company: Threat Guide, role: CMP_READONLY
11/07/23, 10:45:48	companymasteruser@valuedcustomer.com	User	User	Delete	companymasteruser@valuedcustomer.com: User deleted - email: marie.knight@threat.com, company: Threat Guide, role: CMP_ADMIN
11/07/23, 10:36:37	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - email: marie.knight+userguide@threatblockr.com, company: Threat Guide, role: CMP_READONLY
11/07/23, 10:35:53	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - email: marie.knight@threat.com, company: Threat Guide, role: CMP_ADMIN
11/07/23, 10:34:56	companymasteruser@valuedcustomer.com	User	User	Create	companymasteruser@valuedcustomer.com: User created - email: marie.knight+userguideadmin@threat.com, company: Threat Guide, role: CMP_ADMIN
11/07/23, 10:24:38	companymasteruser@valuedcustomer.com	User	Report Schedule	Delete	companymasteruser@valuedcustomer.com: Scheduled report "Top 10 Country Threat Categories" deleted
11/07/23, 10:23:04	companymasteruser@valuedcustomer.com	User	Report Schedule	Create	companymasteruser@valuedcustomer.com: Scheduled report "Top 10 Country Threat Categories" created
11/07/23, 09:29:26	companymasteruser@valuedcustomer.com	User	Report Schedule	Delete	companymasteruser@valuedcustomer.com: Scheduled report "Country Top 10 Report" deleted
11/04/23, 11:01:40	companymasteruser@valuedcustomer.com	User	Policy	Delete	companymasteruser@valuedcustomer.com: Deleted policy "New Policy"

# IOC Search

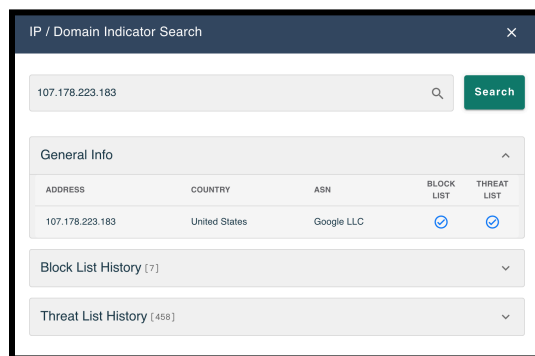
The Indicator of Compromise (IOC) Search allows users to search any IP address or domain to see if it is a malicious actor found in any of our threatER–provided Threat or Block feeds. Available information about the country and ASN, when available, are returned as well.

To perform a search:

- Select the spyglass icon in the top navigation bar
- Enter an IP address or domain
- Select the search icon in the modal



The results that display will provide general information on the IP or domain.



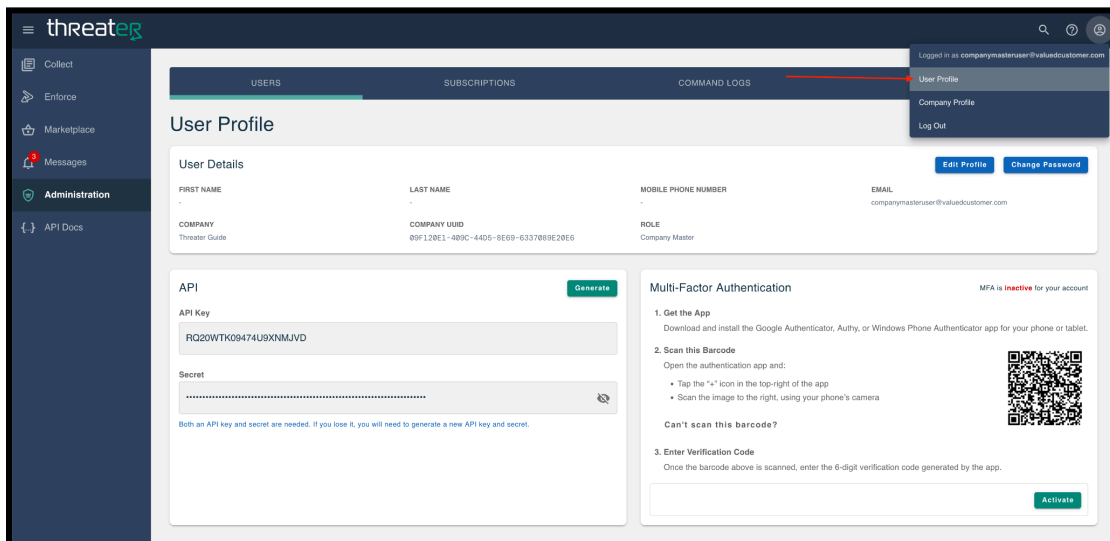
If the indicator has history on any Threat or Block feeds provided by threatER, this will be included and the section can be expanded to view those details.

Users can also perform the search by selecting the hyperlinked IP address or domain within a threatER–provided feed.

# 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.

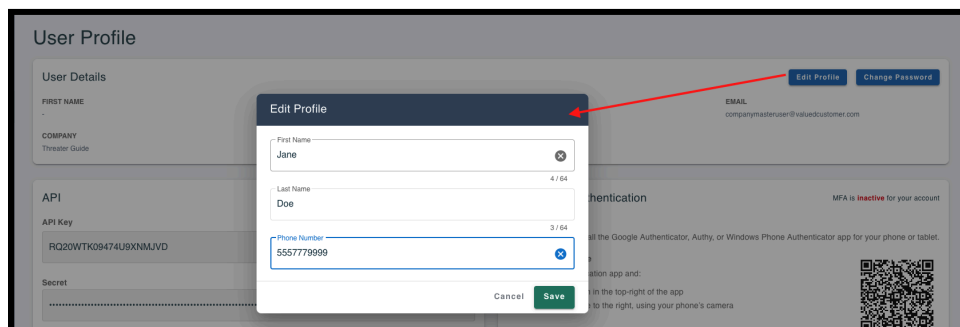
The User Profile is accessible by selecting the person icon in the top-right navigation bar and then selecting User Profile.



## User Details

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

- Select the Edit Profile button
- Enter the following optional information:
  - First Name
  - Last Name
  - Phone Number
- Select Save



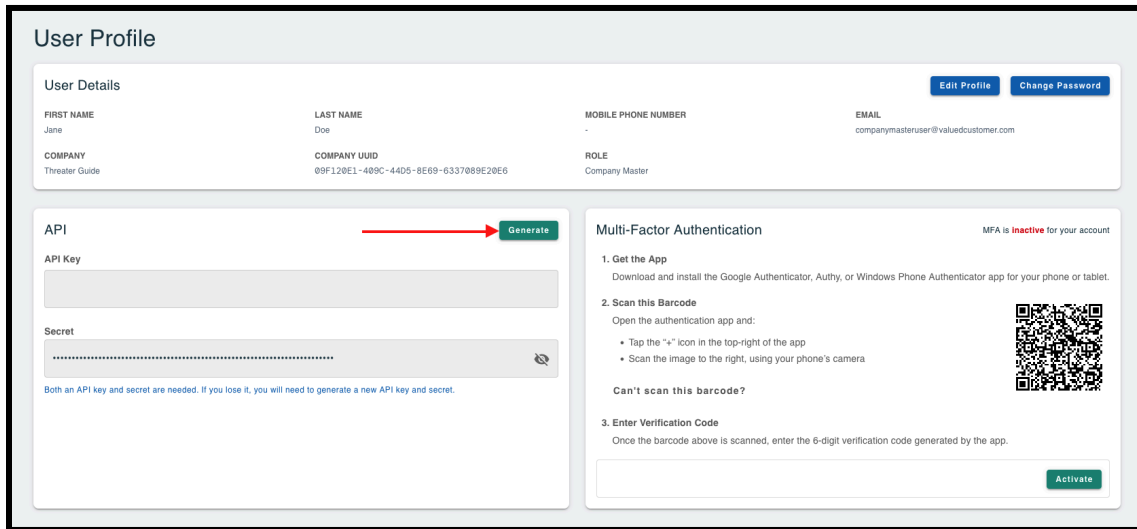


Email and Role updates cannot be made on the User Profile. To update either of these, please contact your Company Master account.

## 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, select the Generate button in the API Key section.



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

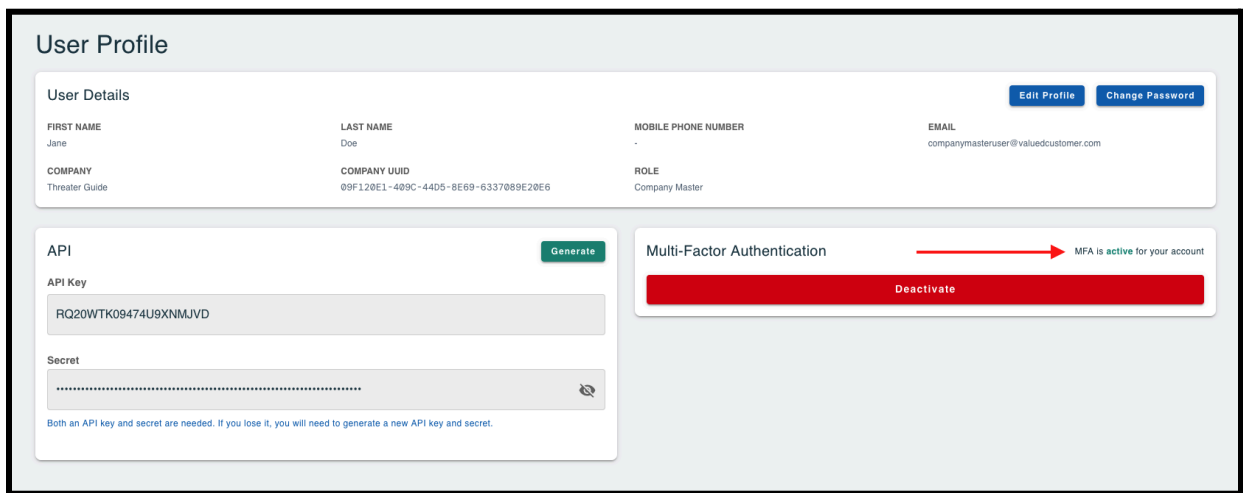
MFA can be enabled for your individual account, if it is not required by your company by default.

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 select 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.

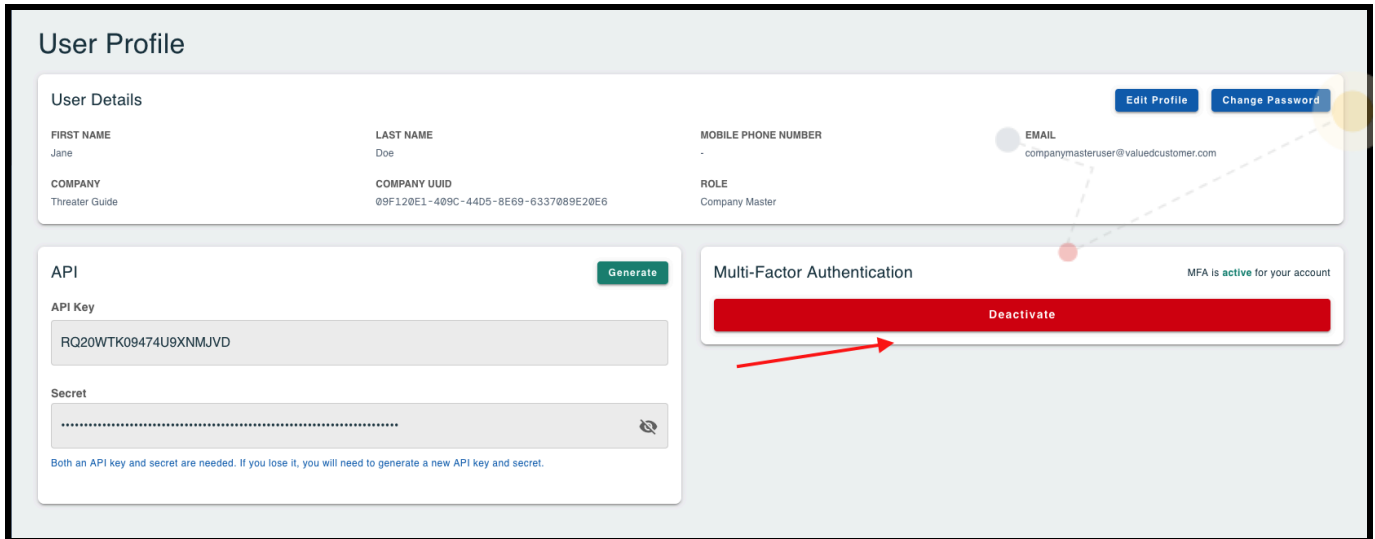


When MFA is active, you will be prompted to provide a code from the authentication app you used to activate MFA each time you login to the portal.

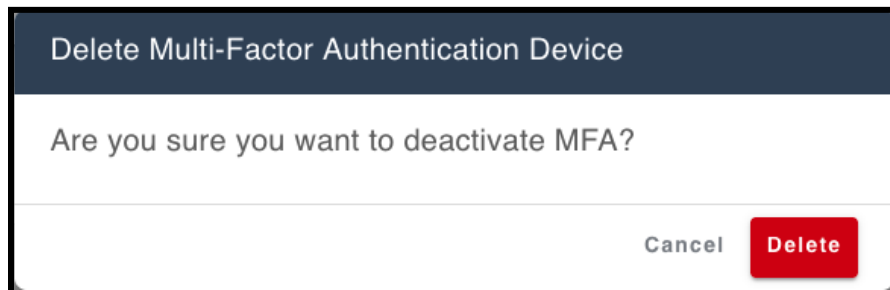
## Deactivate MFA

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

- Navigate to your User Profile
- Selecting the Deactivate button in the MFA panel



- On the Delete MFA confirmation modal, select the Delete button

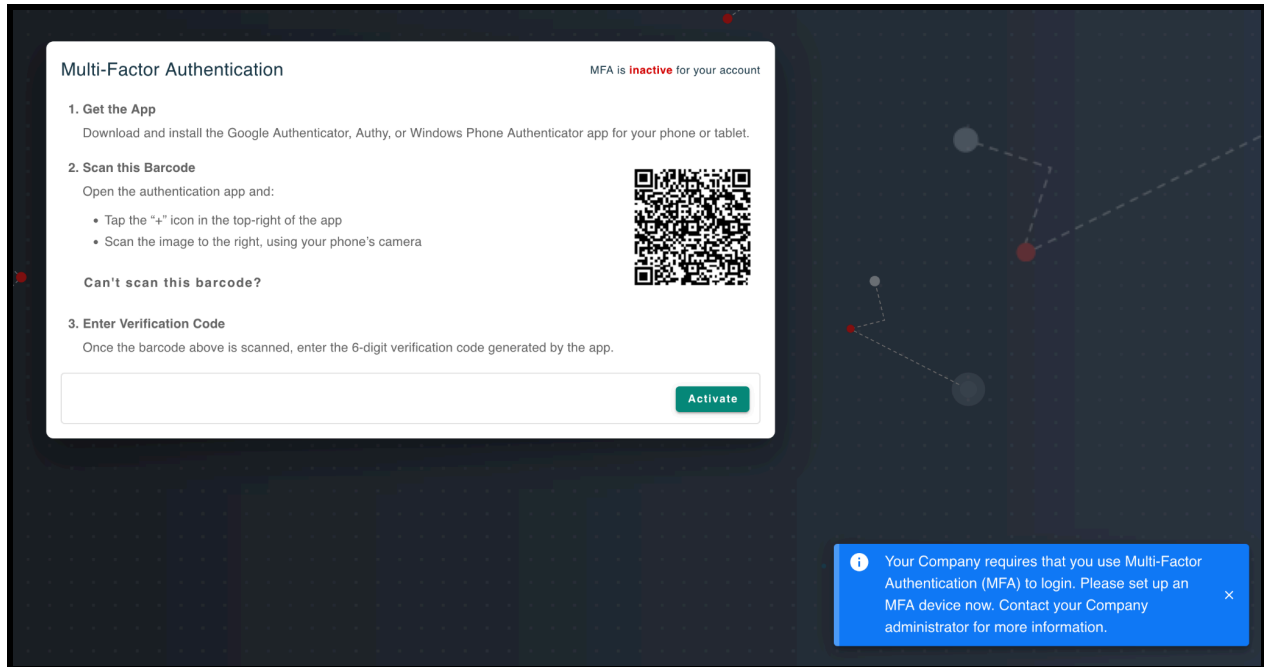


MFA is now inactive for your account. The next time you login to the portal you will not be prompted to enter a passcode.

## 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.



- 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 select 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.

# 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:

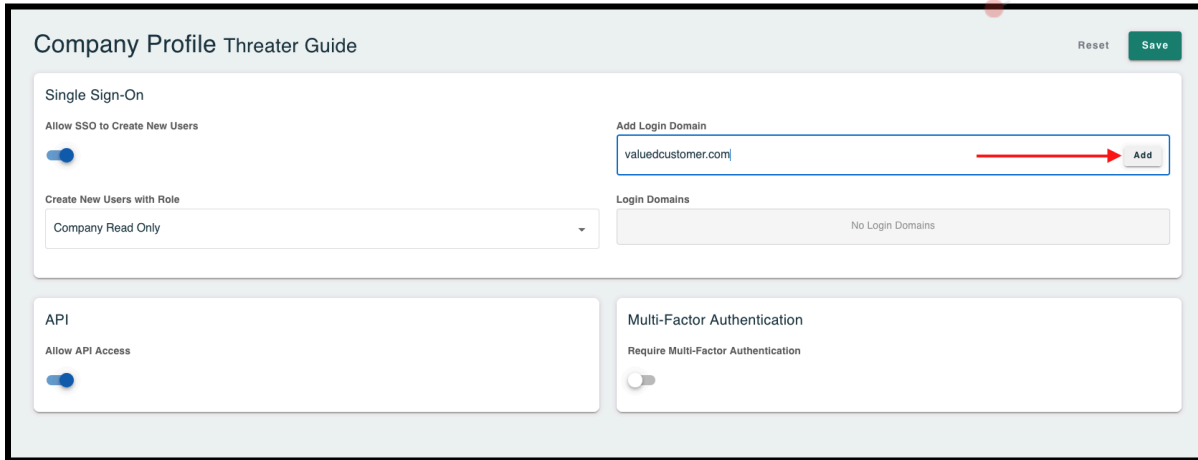
- Navigate to the Company Profile
- Toggle On the "Allow SSO to Create New Users" setting
- Select the User Role the new user will be created as
  - Read Only is **strongly** recommended
  - User permissions can be updated at a later time

The screenshot displays the 'Company Profile ThreatER Guide' interface. It features several configuration sections:

- Single Sign-On:**
  - Allow SSO to Create New Users:** A toggle switch is turned on (blue).
  - Create New Users with Role:** A dropdown menu is open, showing 'Company Read Only' as the selected role. A red arrow points to the 'Select Role...' text above the dropdown.
  - Other roles listed in the dropdown include: Company Help Desk, Company Admin, and Company Master Admin.
- Add Login Domain:** A text input field contains 'host.com' and an 'Add' button is visible.
- Login Domains:** A list of domains is shown, including 'valuedcustomer.com' with a trash icon for removal.
- Multi-Factor Authentication:** A section with a toggle switch for 'Require Multi-Factor Authentication', which is currently turned off.

At the top right of the interface, there are 'Reset' and 'Save' buttons.

- 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.
- Select the Add button



- Select Save

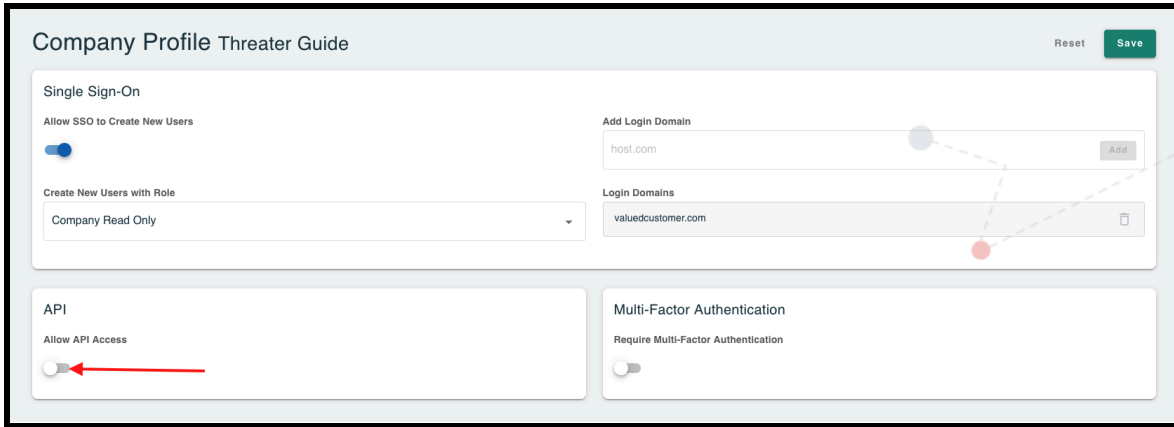
Once this setting is properly configured, the Company Master can direct their new users to:

- Navigate to the login screen
- Select "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"
- Select the Save button in the top right corner

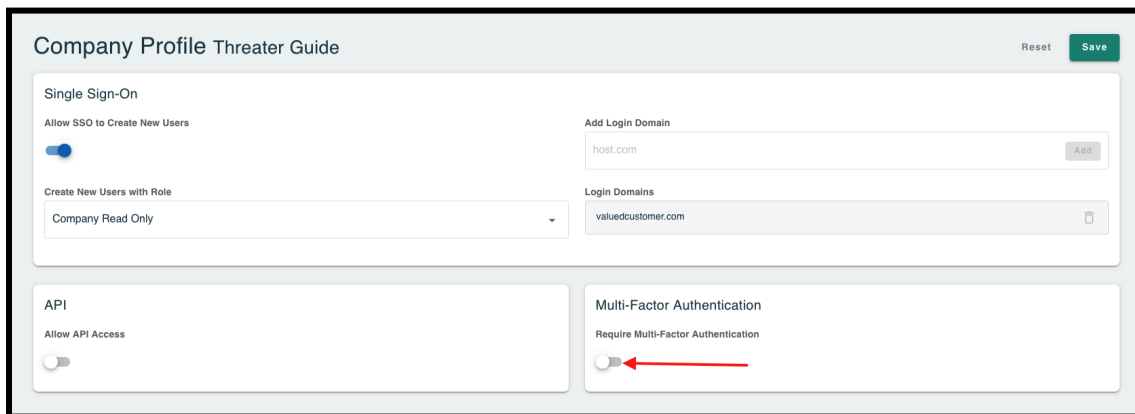


Each user will now have the ability to generate an API Key on their individual user profile. The generated API Key will give the user access to the API endpoints with the permissions their account is setup with (i.e. Company Help Desk).

## 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"
- Select the Save button in the top right corner



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
<b>COLLECT</b>				
<b>LISTS</b>				
View Lists	X	X	X	X
Create Lists			X	X
Edit Lists			X	X
Delete Lists			X	X
<b>MARKETPLACE</b>				
View Products	X	X	X	X
View Product Details	X	X	X	X
Subscribe to a Product				X
<b>ENFORCE</b>				
<b>ENFORCERS</b>				
View Enforcers	X	X	X	X
Edit Enforcer Name/Location			X	X
Manage Subscriptions			X	X
View Available Enforce Software	X	X	X	X
Update Enforce Software			X	X
<b>NETWORKS</b>				
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
SUBSCRIPTIONS				
View Subscriptions	X	X	X	X
Manage Subscriptions			X	X
UNEXPECTED BLOCKS				
Run Analysis	X	X	X	X
Add Entry to Allow List			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
<b>ADMINISTRATION</b>				
<b>USERS</b>				
View Users	X	X	X	X
Create User				X
Edit Users			X	X
Delete Users				X
<b>SUBSCRIPTIONS</b>				
View Subscriptions	X	X	X	X
<b>COMMAND LOGS</b>				
View Command Logs	X	X	X	X
<b>ENFORCE DOWNLOADS</b>				
Manual Downloads	X	X	X	X
<b>COMPANY PROFILE</b>				
Allow SSO to Create New Users				X
Allow API Access				X
Require MFA for Company				X
<b>IOC SEARCH</b>				
Search Indicators	X	X	X	X

# User Management

		View	Create	Edit	Delete
<b>CMP Master</b>	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
<b>CMP Admin</b>	CMP Read Only	X		X	
	CMP Help Desk	X		X	
	CMP Admin	X		X	
	CMP Master	X			
<b>CMP Help Desk</b>	CMP Read Only	X			
	CMP Help Desk	X			
	CMP Admin	X			
	CMP Master	X			
<b>CMP Read Only</b>	CMP Read Only	X			
	CMP Help Desk	X			
	CMP Admin	X			
	CMP Master	X			