Netskope Cloud Threat Exchange User Guide

Version 2.0.0

VERSION CONTROL

#	Document Version	Date	Author	Document Status	Comments
1	1.0.0	28th January 2020	Crest Data Systems	Initial Draft	

Installation

Getting started
- Default user
- Configure Proxy and Log Level
- Configure primary Netskope tenant
- Configure supported threat data sources
- Configure Sharing

Use Cases
- Dashboard
- CTE Plugins
- CTE Upload a new plugin
- CTE Configure a plugin
- CTE View configured Plugins
- CTE List IoCs and filtering capability
- CTO Plugins
- CTO Configure primary Netskope tenant
- CTO Create Business Rules
- CTO Perform actions on Business Rules
- CTO Add deduplication rules to Business Rules
- CTO List Alerts and filtering capability
- CTO Create Business Rules from filter of alerts
- CTO List Tickets and filtering capability
- CTO Forward alerts matching a business rule to Queue associated with configurations
- Settings
- General
- Manage Tags
- Proxy
- Logs
- API Tokens
- Users
- Account Settings
- Change Password
- Logout
- Help
- API Docs
- Audit logs
- Notifications

Operations
Reset Password
Logs cleanup
Update Plugin Configuration Checkpoint (Last Run time)
Troubleshooting & FAQs

1. Installation

This section describes how to install the Netskope CTE application.

Prerequisites

Docker is a prerequisite required to install the Netskope CTE application. Ensure that below mentioned commands are available.

- docker

  Execute the command mentioned below to verify if the command is available. If available, the command execution would output the path where docker command is available.

  ```
  $ which docker
  ```

- docker-compose

  Execute the command mentioned below to verify if the command is available.

```
$ which docker-compose
```

- HTTP Proxy Details

  In case your network expects the outgoing API to be routed via the proxy, make sure you have the details of HTTP Proxy

  - Proxy IP/Hostname
  - Proxy Port
  - Credentials

System Requirements

This section provides recommendation and guidance for selecting the server/VM/Instance on which Netskope CTE is going to be installed.

The deciding factors for system requirements are

- Total number of configured plugin sources.
- Total number of Indicators expected to be stored in the database. This factor defines the storage requirements.
- Netskope CTE has a worked based scheduling mechanism to cater to the data pull/push for multiple data sources. The number of workers determine how many data sources would be actively fetching data/sharing data concurrently. The total number of worker processes is equal to the number of cores. If the expectation is fetch data frequently with multiple data sources, consider increasing the number of cores.

The table below provides recommendation for standard deployments:

Workload Details	Memory Requirement(GBs)	# of cores	Storage(GBs)
Upto 2 configured plugins.	2	1	20GB
Upto 4 configured plugins. ~1 million IoCs	4	2	20GB
Upto 6 configured plugins. ~1 million IoCs	4	2-4	20GB
Upto 10 configured	6	4-6	40GB

plugins. ~2 million IoCs			

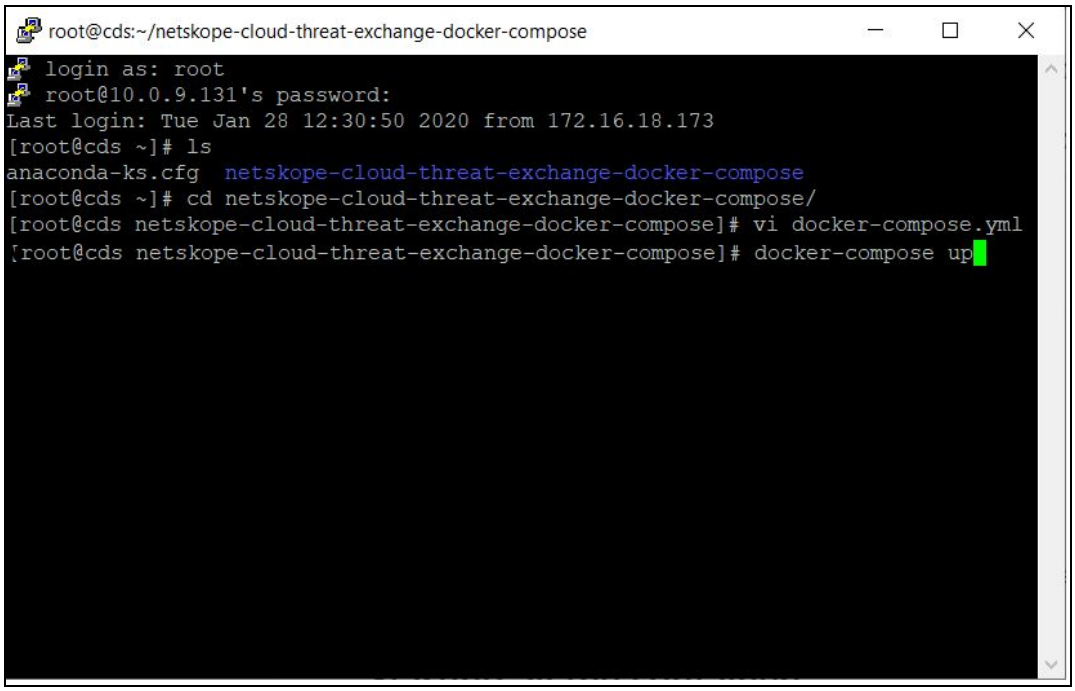
Installation Steps

1. SSH into the system(Linux) where Netskope CTE needs to be installed.
2. Download the deliverable to the system from Github.

```
$ git clone https://github.com/netskopeoss/ta_cloud_threat_exchange
```

3. Navigate under the directory available after downloading the directory. Locate docker-compose.yml
4. Update the value of "JWT_SECRET" in the docker-compose.yml file to a secure string. This will be used to encrypt the authentication tokens.
5. (*optional*) To replace the Netskope provided SSL certificate with a custom SSL certificate and key file:
    a. Replace the existing SSL certificate (cte_cert.crt) and key file (cte_cert_key.key) in the ssl_cert directory with custom certificate and key file using the same file names. Default location is ./data/ssl_certs which can be changed from the docker-compose.
6. (*optional*) Update the custom_plugins volume to store the user uploaded plugins in a different directory.
7. Execute the command `docker-compose up -d`.
8. UI is now accessible with the system's IP. (e.g. https://<ip>)

Note : The docker images are available on docker-hub. Make sure the connectivity to docker-hub before executing the docker-compose command. Ensure docker authentication prior to running the docker-compose command.



2. Getting started

This section describes the initial steps to getting started with Netskope CTE after installation is done.

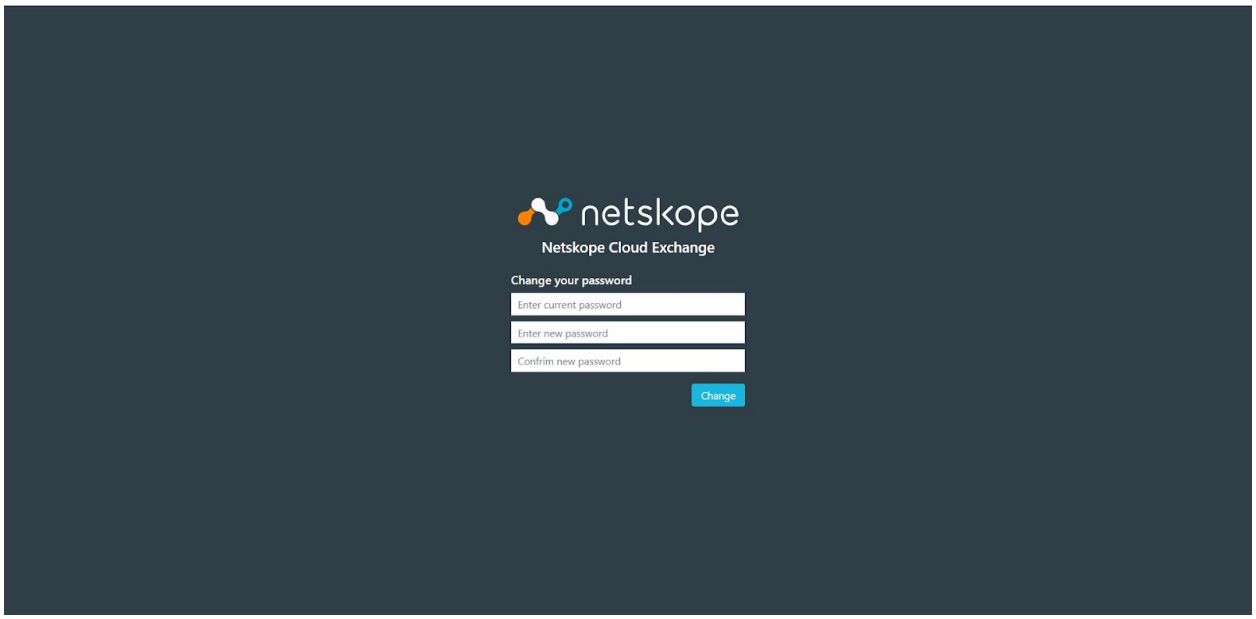
2.1. Default user

By default after successful installation one user will be created with default credentials.

1. Super admin user
   Username/Password: admin/admin
   Description:

This user will have Administrator level access to the application. This user will have the write access and will be able to create new users as well.

On the first login, the user will be forced to change their credentials. After that, the user can log in using new credentials.



2.2. Configure Proxy and Log Level

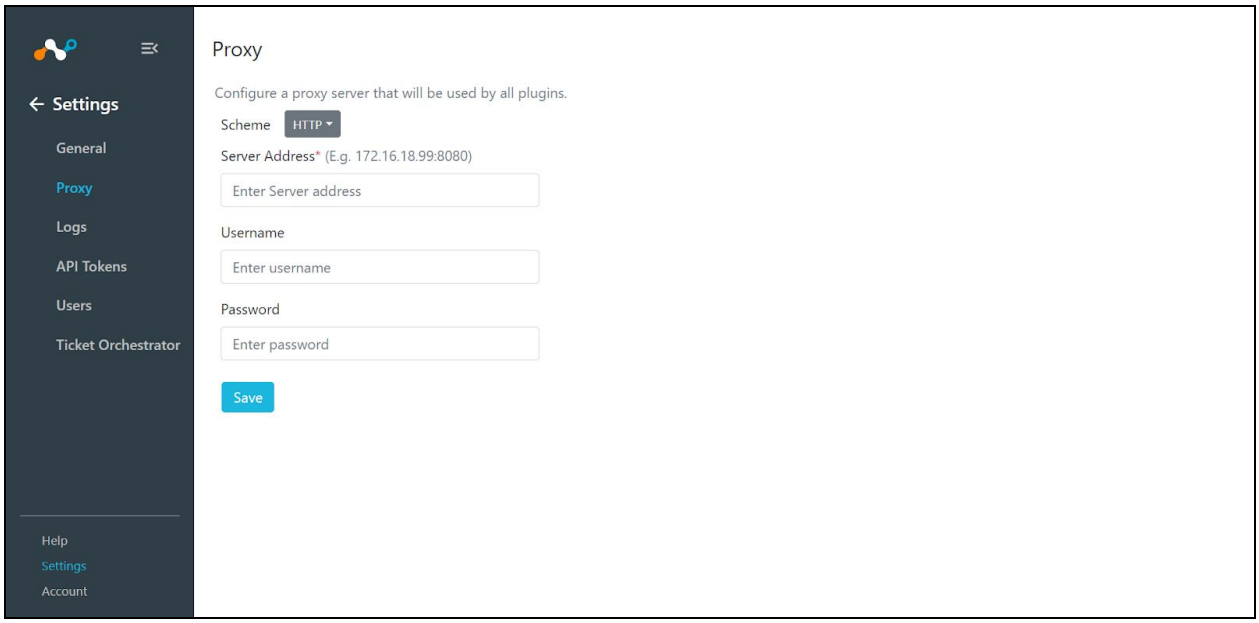
This section describes the settings options available for proxy and logs in the CTE. The changes to settings does not require CTE core restart.

Role required : admin

(1) Proxy

Admin can set global proxy settings that would be used for all outgoing API calls. Each plugin configuration has an option to use the system proxy.

1. Login to Netskope CTE.
2. On the Left hand navigation panel, there's an option 'Settings' available at the bottom part of the panel. Click on Settings.
3. Select Proxy option from sidebar.
4. The User has to provide Proxy Server Address and port(Do not provide http scheme). In case of authenticated proxy, make sure username and password are supplied.



(2) Log level

Users can set different log levels here, 3 different log level options are available.

1. Info
2. Warning
3. Error

1. Login to Netskope CTE.
2. On the Left hand navigation panel, there's an option 'Settings' available at the bottom part of the panel. Click on Settings.
3. Click on the Logs Option.
4. Set the Log level by selecting the value from the dropdown menu.

2.3. Use Cases

This section describes use-cases for the Netskope Cloud Exchange.

2.4. Dashboard

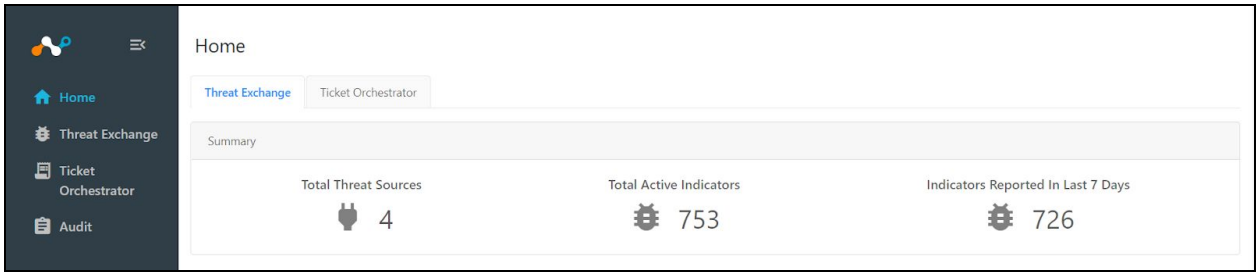
Dashboard provides a high level overview of both modules (CTE and CTO) and the purpose is to give a bird's eye view to the user.

Role Required : admin or read-only

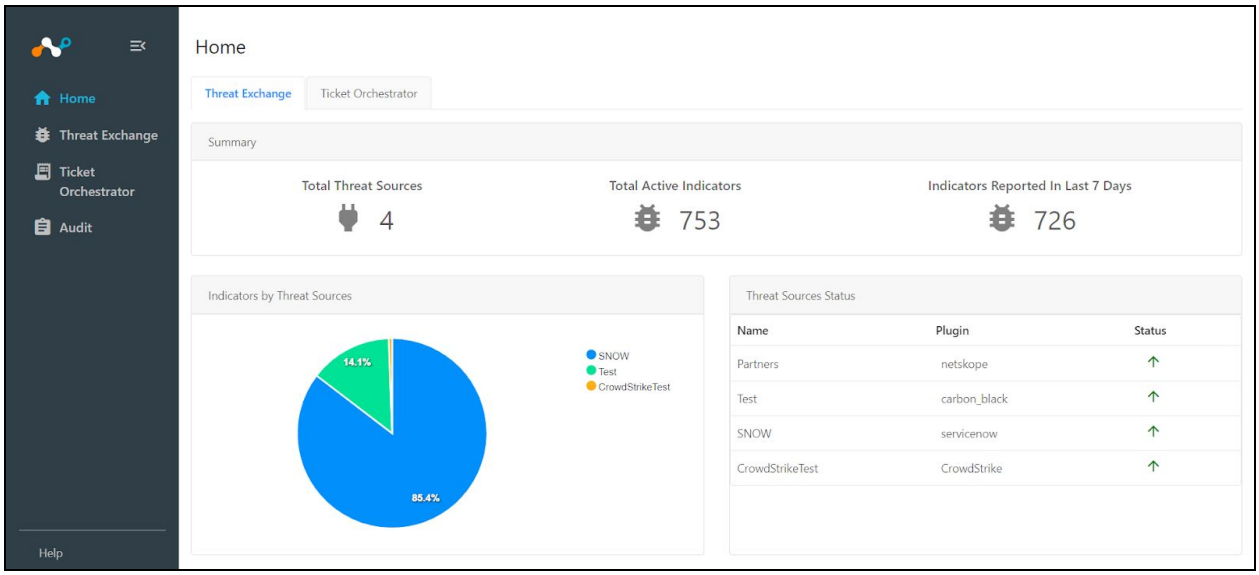
Below is the detail of each panel available within the Home Dashboard. After logging into the Netskope Cloud Exchange, the Dashboard appears by Default as the Home page.

2.4.1. CTE Dashboard

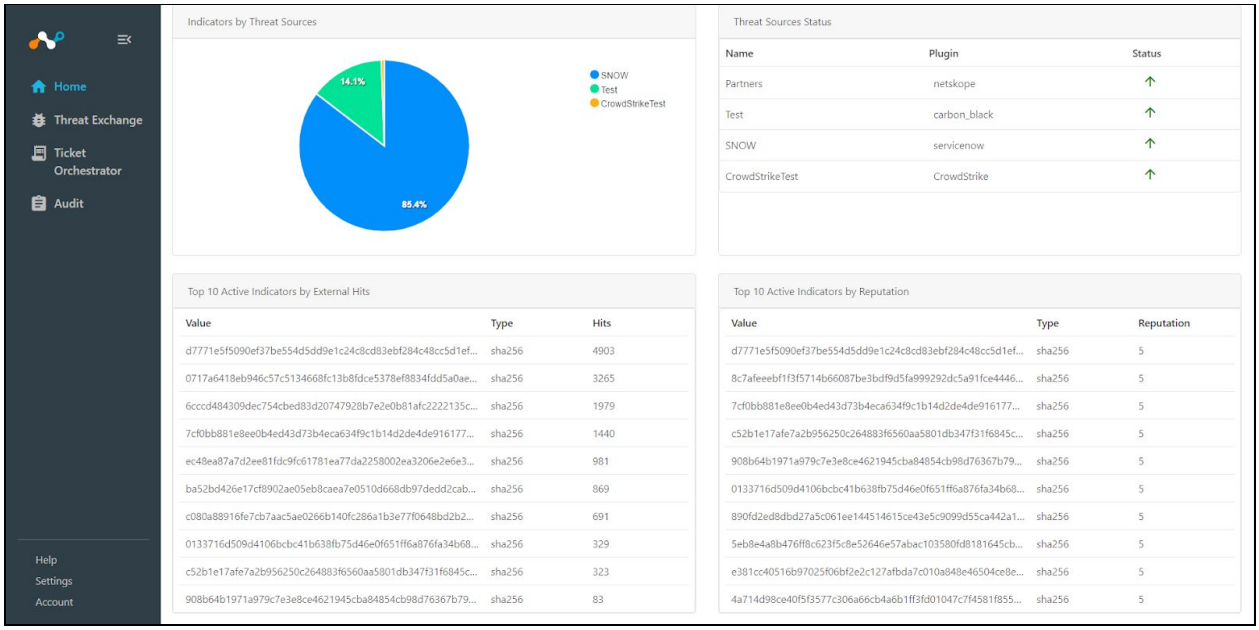
1. Total Threat Sources => Here the user will get the configured sources count.
2. Total Active Indicators => Total Active indicators count will be displayed in this option.
3. Indicators Reported In Last 7 Days => Active indicators count which are observed in last 7 days.
   Note: Although an indicator is fetched recently, if the event timestamp associated with the observable entry is earlier than 7 days, such indicators would not be considered in Last 7 Days count.



4. Indicators by Threat Sources => Here the user will get the Pie chart with indicators count.
5. Threat Sources Status => Current status of configured plugins.



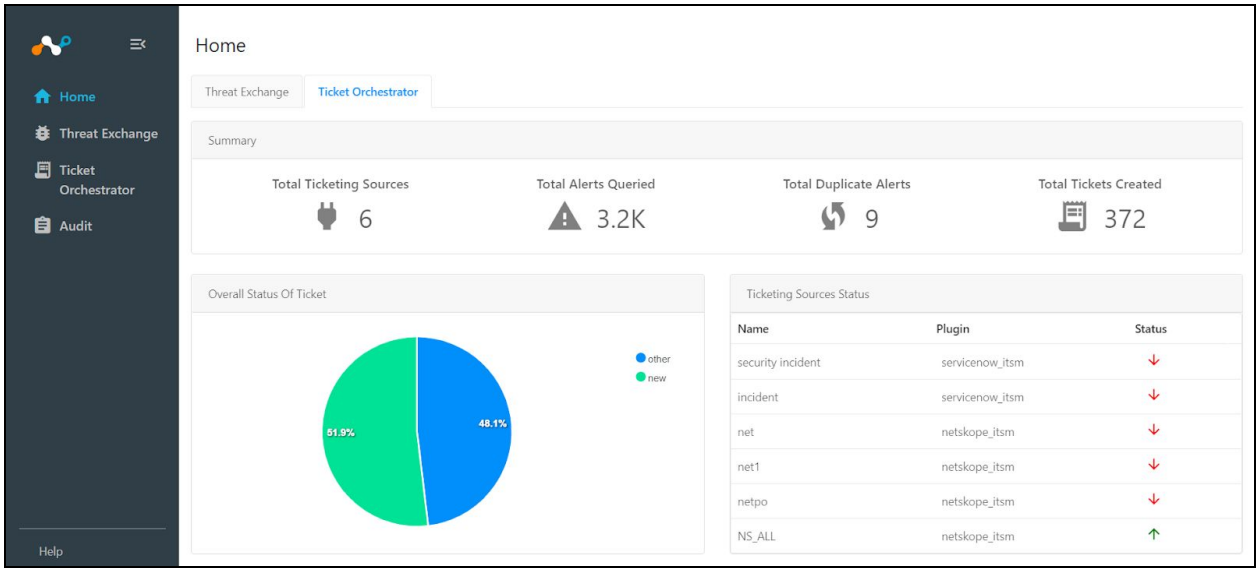
6. Top 10 Active Indicators by External Hits => List of top 10 active indicators by External hits are here.
7. Top 10 Active Indicators by Reputation => List of top 10 active indicators by reputation are displayed here.



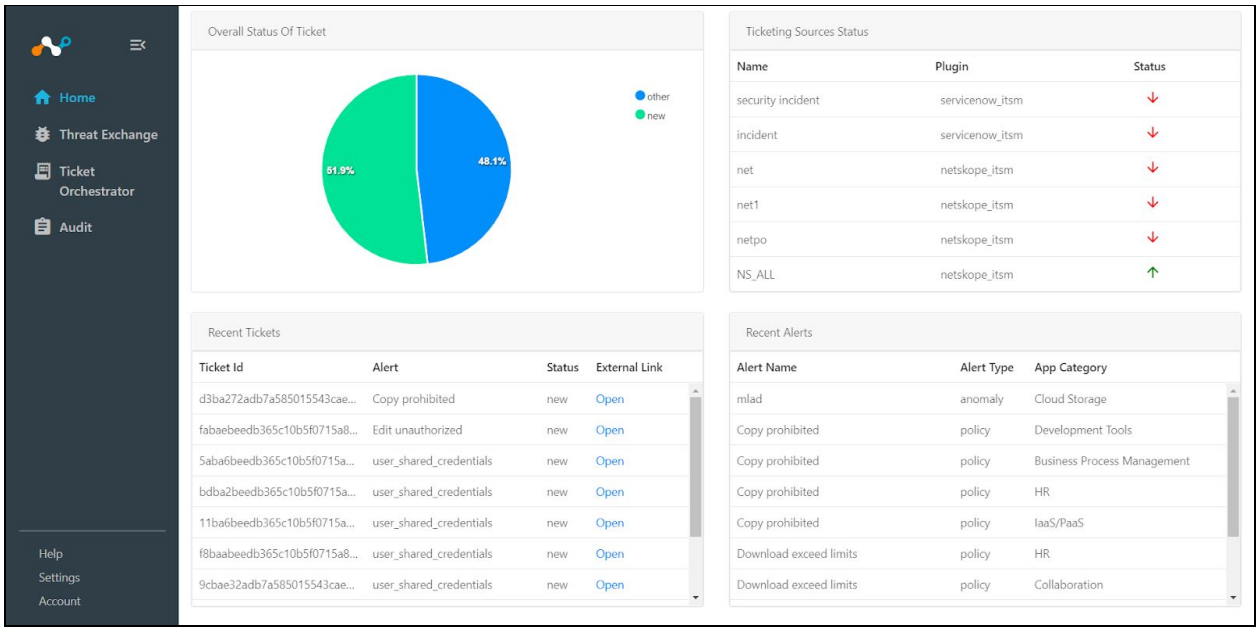
2.4.2. CTO Dashboard

1. Total Ticketing Sources => Here the user will get the configured ticketing sources count.
2. Total Alerts Queried => Total Active alerts count will be displayed in this option.
3. Total Duplicate Alerts => Duplicated alerts count will be displayed in this option.
4. Total Tickets Created => Total No. of alerts created will be displayed in this option.

5. Overall Status Of Ticket => Here the user will get the Pie chart with tickets count.
6. Ticketing Sources Status => Current status of configured plugins.



7. Recent Tickets => List of top 10 recent tickets are here.
8. Recent Alerts => List of top 10 recent alerts are here.



2.5. Threat Exchange(CTE)

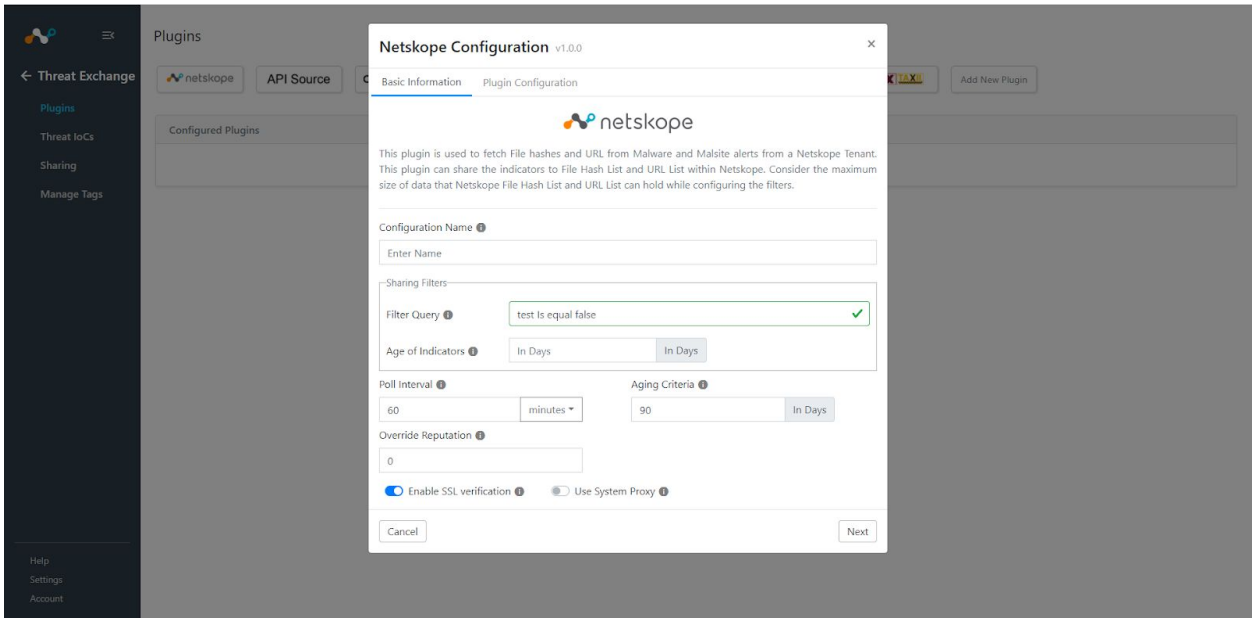
This section describes use-cases for the Netskope CTE.

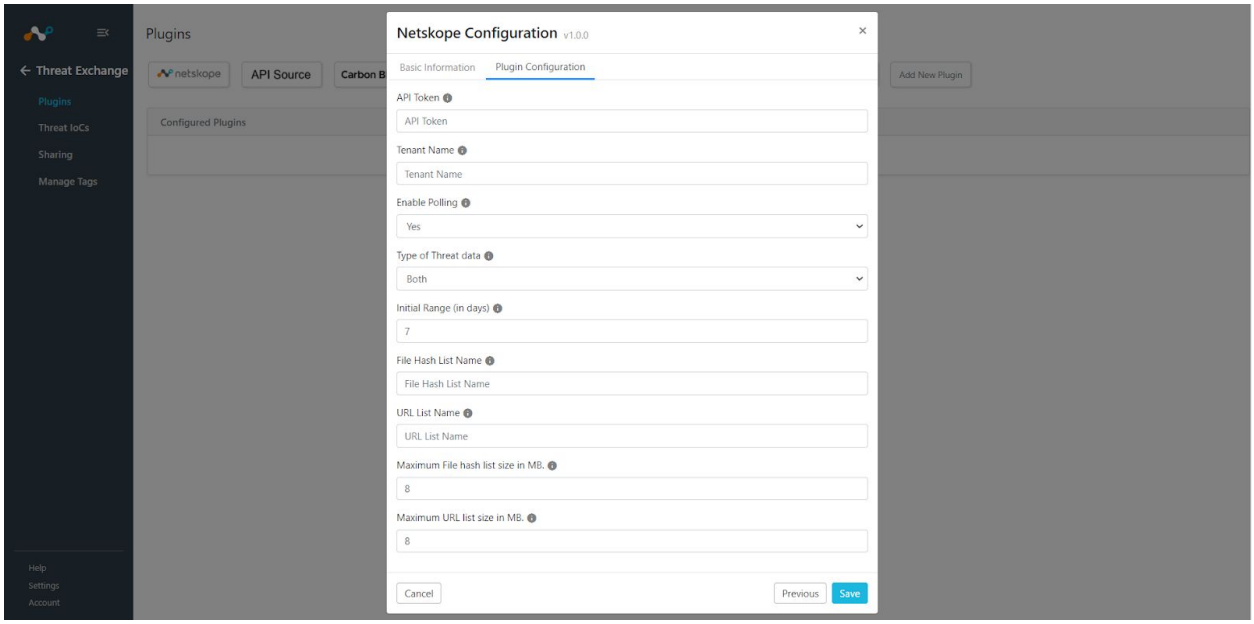
2.5.1. Configure primary Netskope tenant

This part section describes how to configure the primary Netskope tenant. This configuration would ensure that alerts data from the tenant is pulled regularly.

Role required : admin

1. Login to Netskope CTE.
2. Navigate to the Plugins. List of available Plugins is visible.
3. Click on the Netskope Plugin Card (+) to open a configuration form.
    a. First Page will have basic information about the configuration. More details about the parameters can be found here.
    b. The second page will have authentication parameters related to access to the tenant, File list and URL list.





Field	Description	Default Value
API Token	API token to authenticate Netskope Tenant.	
Tenant name	Netskope Tenant name e.g. <tenant-name>.goskope.com	
Enable Polling	Enable/Disable polling data from Netskope.	Yes
Type of the Threat data to pull	Type of Threat data to pull. Allowed values are Malware, URL(For Malsite data) and Both.	Both
Initial Range	Number of days to pull the data for the initial run.	7
File Hash List name	The name of File Hash List on Netskope where malware file hashes are pushed.	
URL List name	The name of the URL List on Netskope where malsites are stored.	

Maximum File hash list size	Size of allowed payload(In MBs) for File Hash List. Defaults to 8MB.	8
Maximum URL list size	Size of allowed payload(In MBs) for URL list. Defaults to 8MB.	8

2.5.2. Configure supported threat data sources

This section describes the certified plugins supported by Netskope.

Role required : admin

Other than Netskope plugin CTE is shipped with below plugins.

1. ServiceNow
2. Carbon Black
3. CrowdStrike
4. SentinelOne
5. STIX/TAXII
6. API Source (Allows for categorization of data delivered to CTE via API)

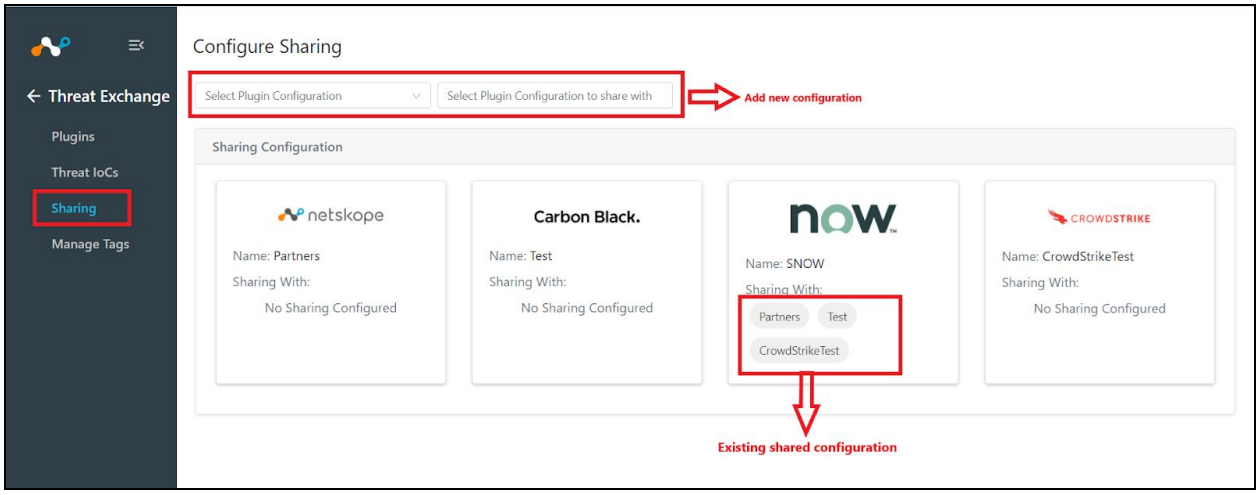
2.5.3. Configure Sharing

This section describes configuring sharing of IoCs between the plugin configurations. Make sure that you have identified the sharing amongst sources in advance. Consider the sharing filters available in the plugin configuration as this would define the traffic on the target configuration.

Role required : admin

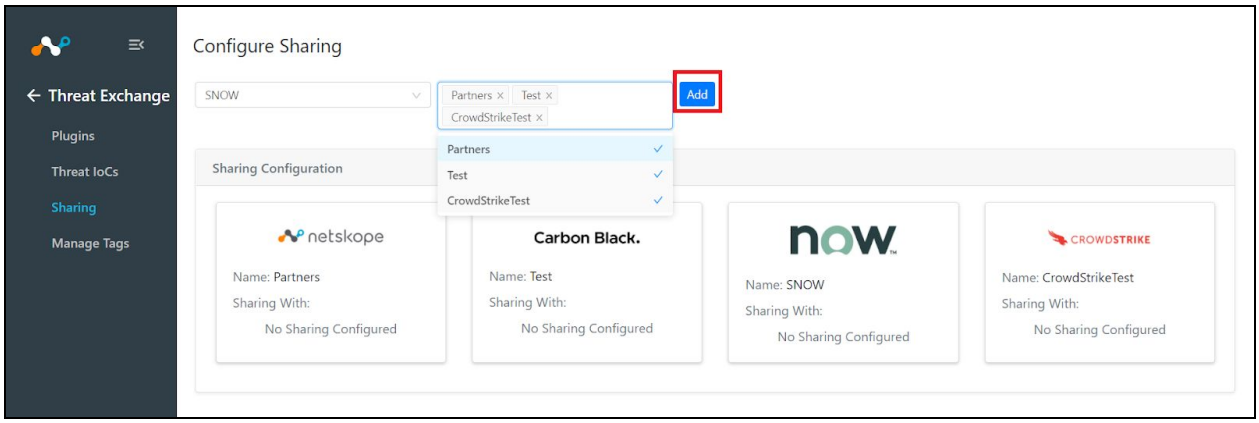
1. Login to Netskope CTE and navigate to the Sharing option. This page will display the existing sharing for each configuration in grid view. It also has inputs for configuring new sharing.
2. Adding a new sharing configuration will share the existing IoCs of the configuration to the destination configuration. Whenever a new sharing is configured, all the historical IoCs would also be considered for sharing.
3. The sharing configuration is unidirectional by default. To achieve bi-directional sharing, configure both directions of sharing separately.

Note- Plugins that do not have push support can not receive threat data. E.g API source.



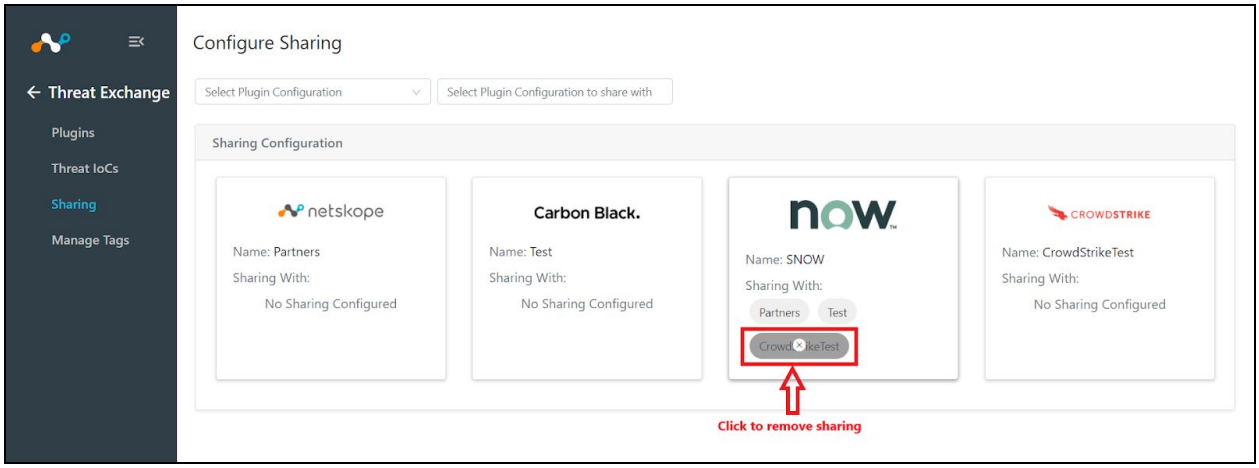
Steps for adding a sharing configuration

1. Select a configuration that will act as a source. IoCs of this configuration will be shared with other configurations.
2. Select a configuration that will receive the IoCs from the source selected in step-1. Users can select multiple destinations as well.



Deleting a sharing configuration.

1. To delete a plugin configuration click on the name of destination chip in the grid view. It will ask for a confirmation then the user can delete a configuration. Deleting a sharing configuration would stop the sharing of new IoCs.



2.5.4. Plugins

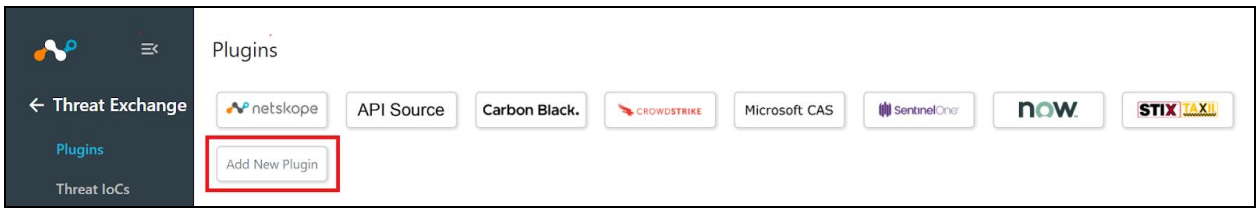
Netskope CTE comes with the library of supported plugins. In the case where the integration for desired product is not available, CTE allows adding new plugins. Referring to the plugin development guide, a new plugin can be easily developed.

Role Required : admin

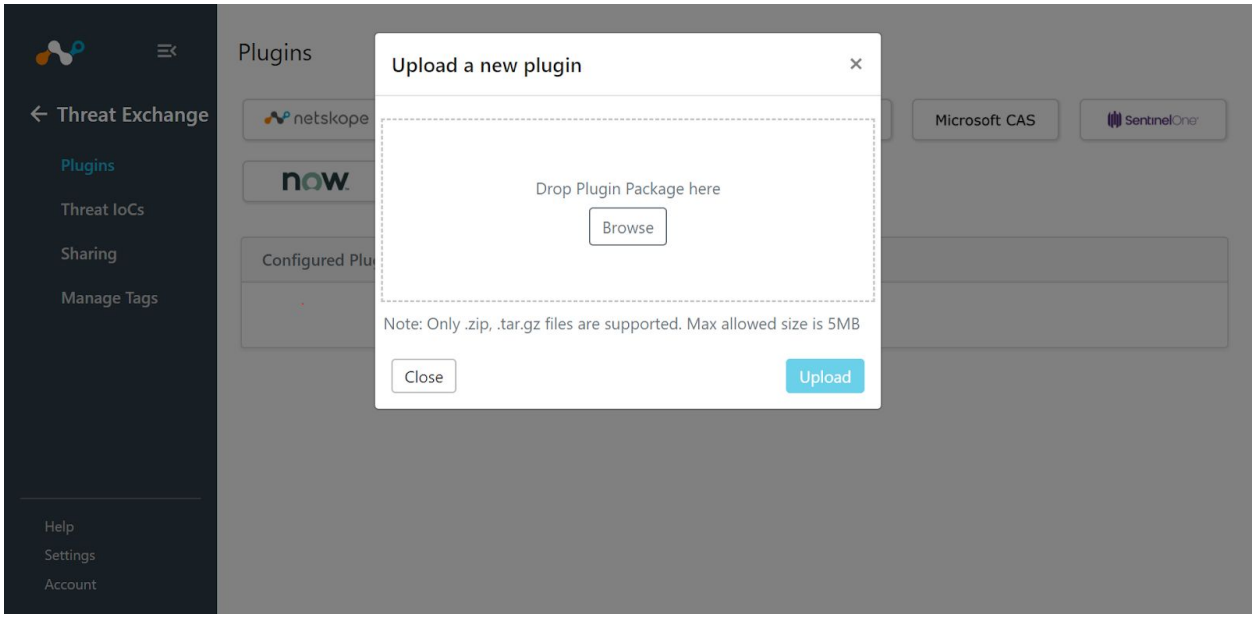
2.5.5. Upload a new plugin

Using this option the user can upload new plugins. Also the user can create configuration (source) for the same plugin. Here are the steps to upload a new plugin.

1. Login to Netskope CTE and navigate to Plugins.
2. On the plugin page there will be an “Add new Plugin” option.



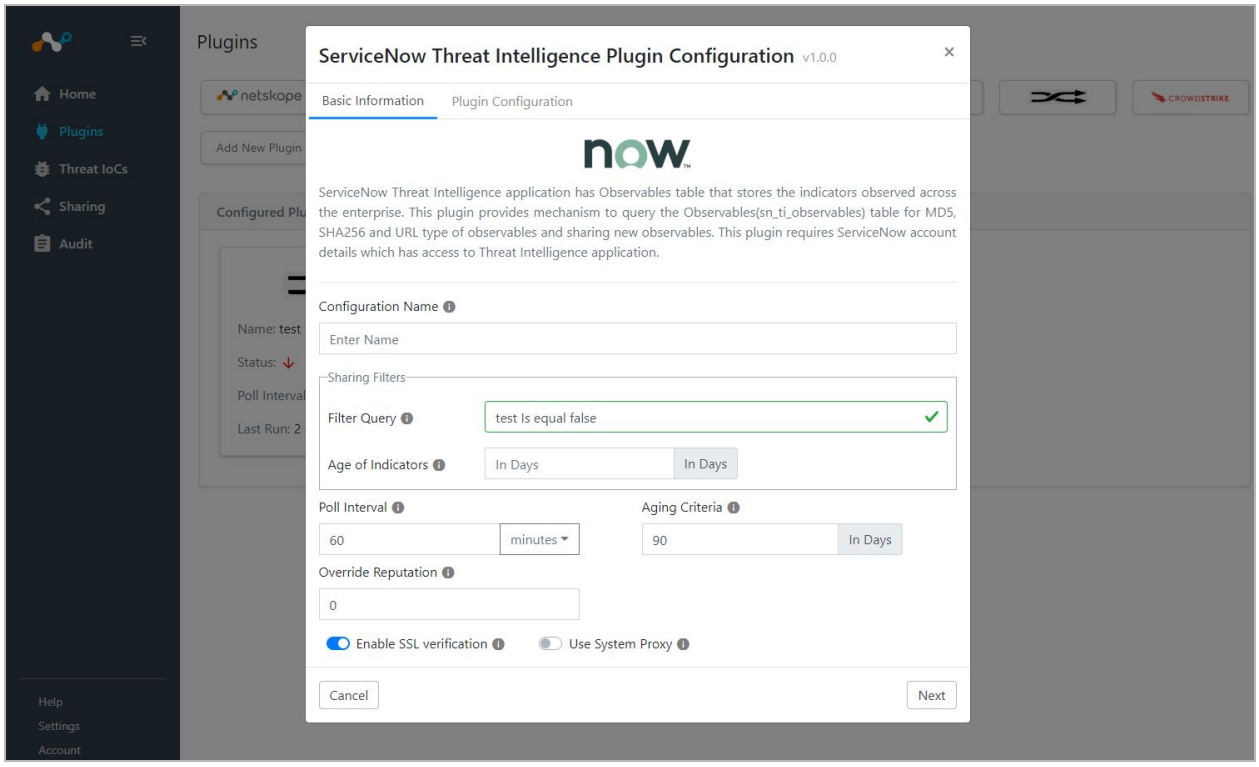
3. Click on the “Add new Plugin” and browse the ZIP or tar file and click on the upload button. After successful validation, the newly added plugin is available under the supported plugins list.
4. Uploaded plugins are stored in the host file system.
5. If the core docker container is upgraded or reset, all the user-uploaded plugins should still remain with all the configurations.



2.5.6. Configure a plugin

To integrate with the supported 3rd party product, user can configure the respective plugin and start fetching/sharing threat data.

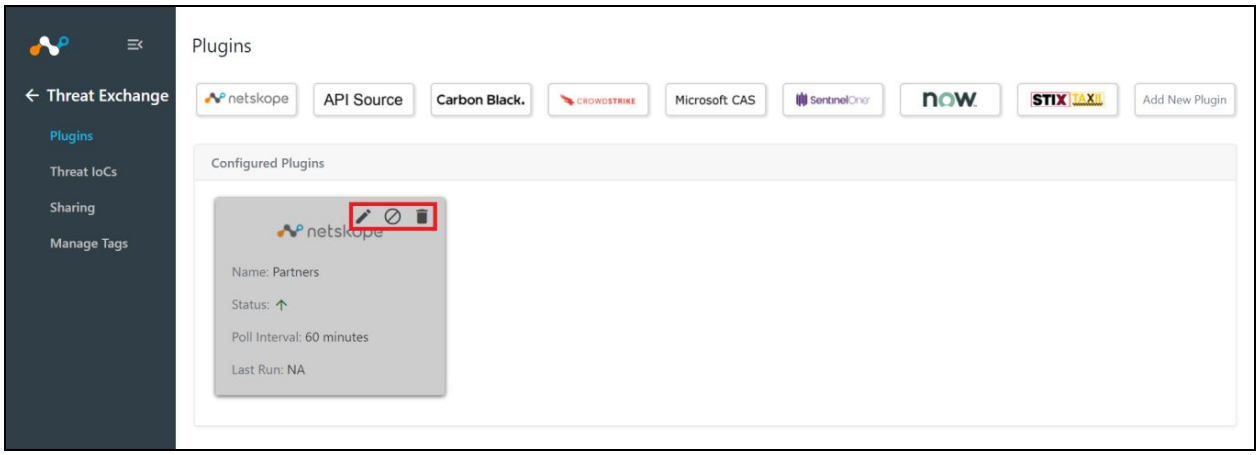
1. Click on that plugin for which you want to create the configuration.
2. The Configuration page will open with basic information fields like Configuration Name, Sharing Filters, Poll Interval, Aging Criteria, Enable SSL verification and Use System Proxy.
3. After adding all these details, click on save to create the configuration.
4. Details of the basic information fields.



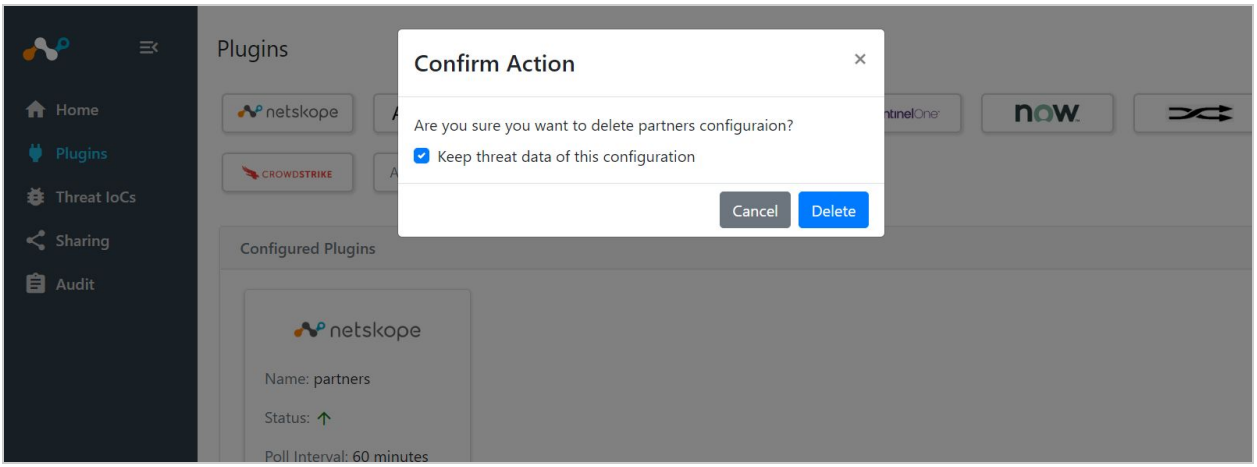
Field	Description	Required/ Default value
Configuration Name	Plugin configuration name by which it will be identified.	Required
Poll Interval	Interval to fetch data from source.	Required, Default- 60 minutes
Aging Criteria	Expire indicators after specific time.	Required, Default- 90 Days
Override Reputation	Set value to override reputation of indicators received from this configuration. Set 0 to keep default.	
Enable SSL Verification	Enable SSL certificate verification.	Required, Default- Yes
Use System Proxy	Use system proxy configured in Settings.	Required, Default- No
Last Run	Date-time indicating the last successful run. Modify this to fetch historical data.	

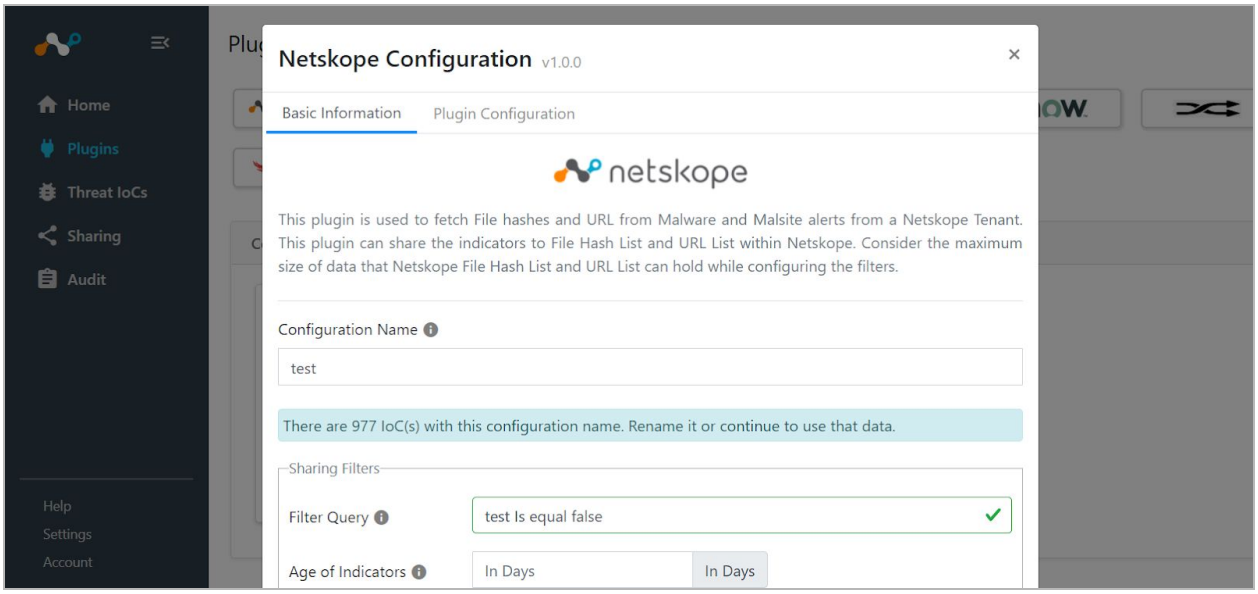
	Note: Only available on edit configuration.	
Sharing Filters (will be applied when indicators are pushed to this Configuration)		
Filter Query	Filter indicators while sharing with this plugin. Filter query can be generated from the Threat IoC page.	Optional
Age of Indicators	Set this filter to limit the indicators while sharing whose age(Last Seen) is within the age specified	Optional

5. The user can edit, disable/enable and delete the configuration using options available on created configuration.



6. When a user deletes the configuration, an option will be provided to keep the threat data of that configuration. If threat data exists for that configuration name, user will be displayed a info message when new configuration is being created.





2.5.7. View configured Plugins

The user can view the list of configured plugins and the status.

1. Login to Netskope CTE and navigate to Plugins from the left hand navigation menu.
2. The list of configured plugins are displayed under the section Configured Plugins. Each Plugin Configuration is displayed as a card. Details displayed under each card:
    a. Plugin logo.
    b. Name - The Plugin configuration name provided while configuring.
    c. Status - Enabled/Disabled. Status also provides information when the configuration is picked by the worker by a text “(running)” next to the status.
    d. Poll Interval - The configured poll interval.

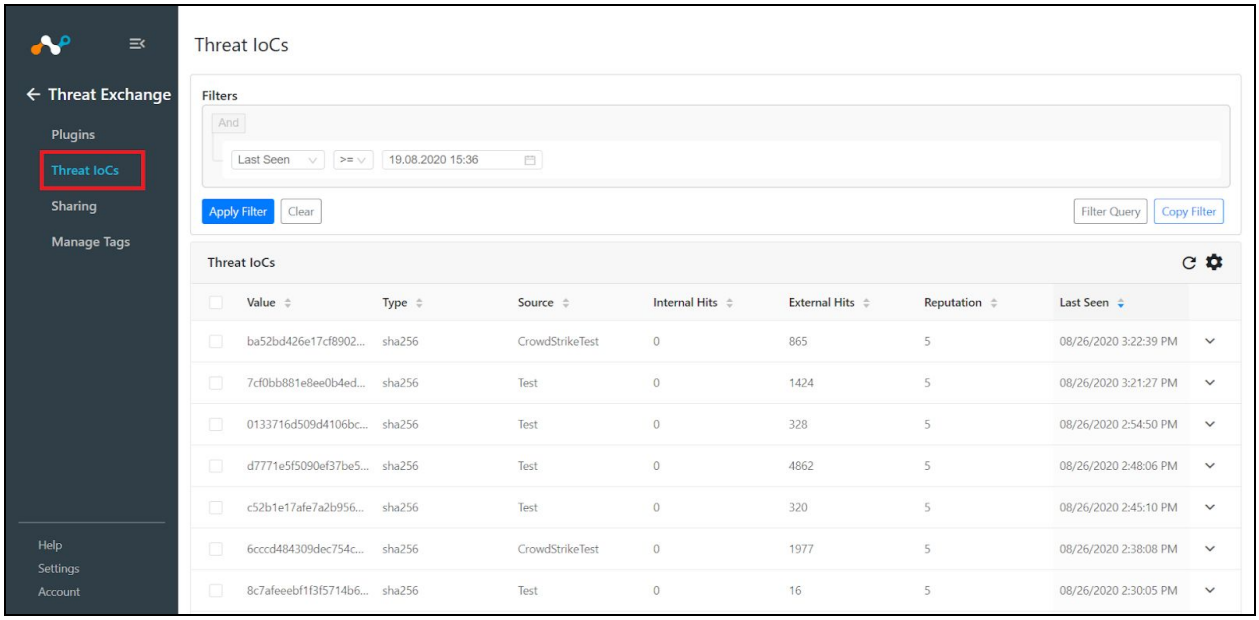
e. Last Run - The time when the plugin configuration was last executed. For the initial run, 'NA' is displayed.

2.5.8. List IoCs and filtering capability

Netskope CTE maintains the database of IoCs captured from multiple threat sources. Users are required to list the available IoCs, view the metadata and filter the IoCs.

Role Required : admin or read-only

1. Login to Netskope CTE and navigate to Threat IOCs.
2. The IoC list appears. By Default, IoCs updated in the last 7 days are fetched. The IoCs list is paginated with a default page size of 10. The records are sorted in descending order of Last Seen.



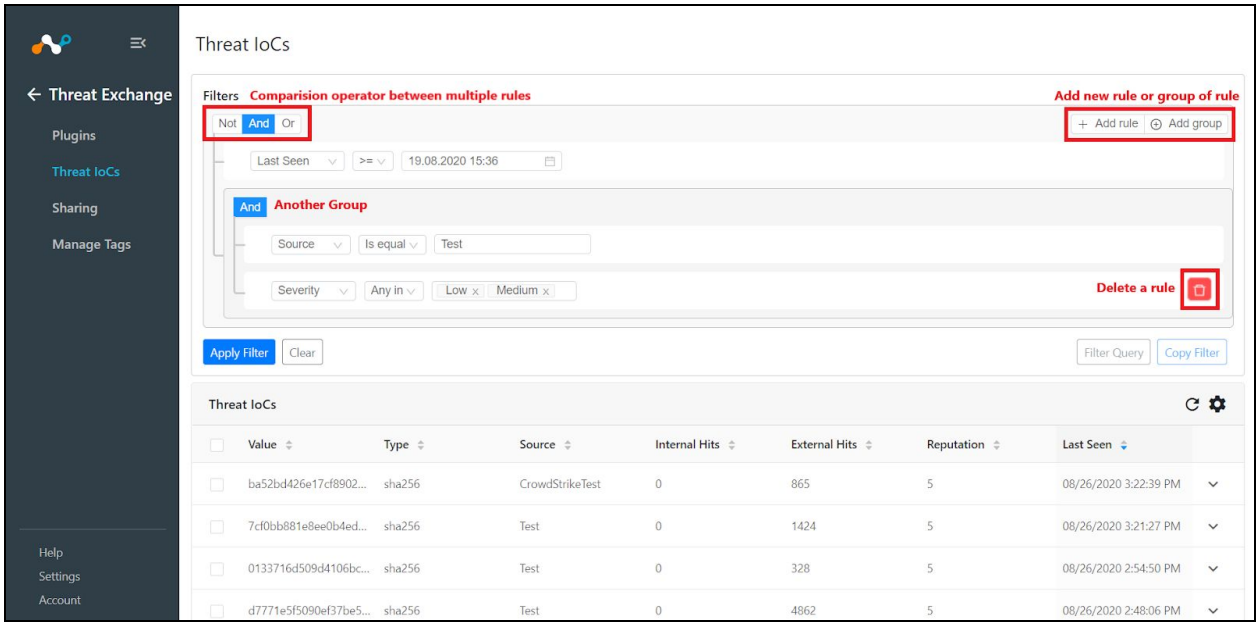
3. The User has different filter options available. The User can add one or more filters and also can add a group of filters. The detailed list of filter options is listed below.

Field	Filter String variable	Description	Filter operators
Value	value	Value of IoC can be the value of the MD5, SHA256 or URL.	Is equal and contains (Regex also supported).

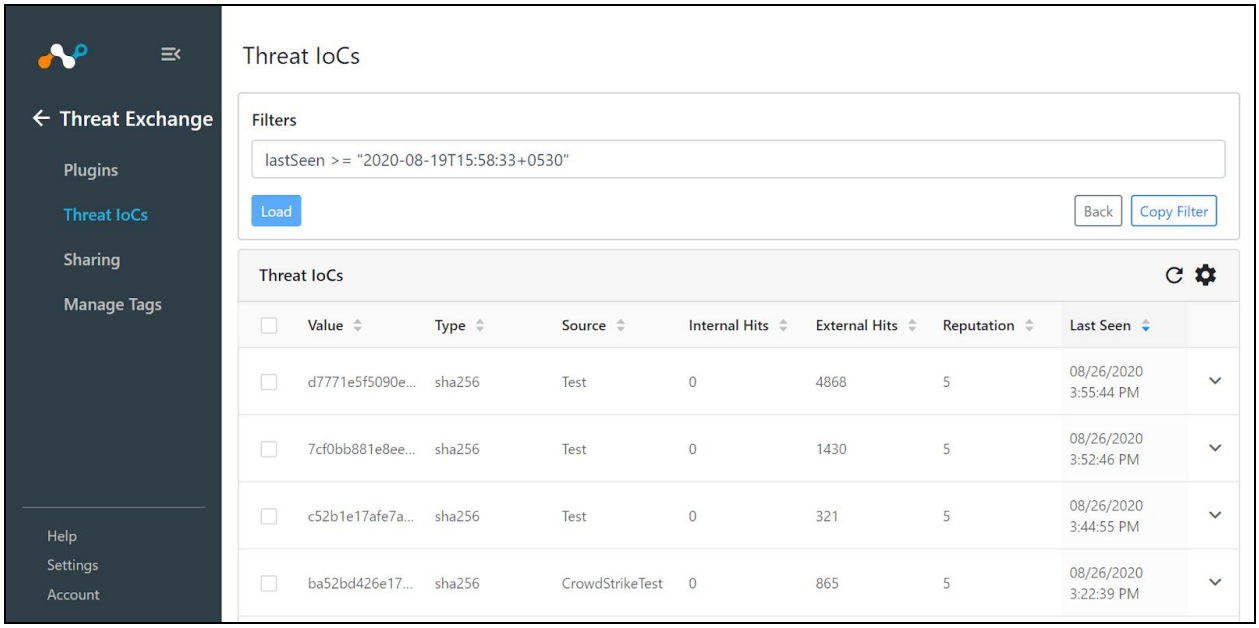
Source	source	Source plugin configuration of IoCs from where IoC is fethced.	Is equal and contains (Regex also supported).
Comments	comments	Comments provided for that IoC.	Is equal and contains (Regex also supported).
Type	type	Type of the IoC. MD5, SHA256, URL	any in, not in operator (Multiselect)
Reputation	reputation	Confidence of the information. Low 1 - High 10.	!=, <, <=, >, >=
Internal Hits	InternalHits	Number of times Netskope has seen this IoC.	!=, <, <=, >, >=
External Hits	ExternalHits	Number of times Third parties have seen this IoC.	!=, <, <=, >, >=
Test	test	Boolean value whether IoC is marked as Test from Netskope	Is equal, !=
Active	active	Boolean value whether IoC is expired or not.	Is equal, !=
Shared With	sharedWith	List of other configurations, with that IoC is shared.	any in, not in operator (Multiselect)
Severity	severity	Criticality of the information	any in, not in operator (Multiselect)
Tags	tags	Tags associated with the threat data	any in, not in operator (Multiselect)
Expires At	expiresAt	Expiry time of the IoC after that it will be active will be false.	!=, <, >, >=
First Seen	firstSeen	Time at which IoC was seen first in CTE.	!=, <, >, >=
Last Seen	lastSeen	Time at which IoC was seen last.	!=, <, >, >=

4. For more than one filter comparison operator AND , OR will be applied.

5. After selecting the desired filter, Click Apply Filter. The IoCs matching the filtering criteria would be listed.
6. To remove the custom filter, Click on Delete Filter option. This removes the applied filter and fallbacks to default filter. The IoCs matching the default filter would be listed.



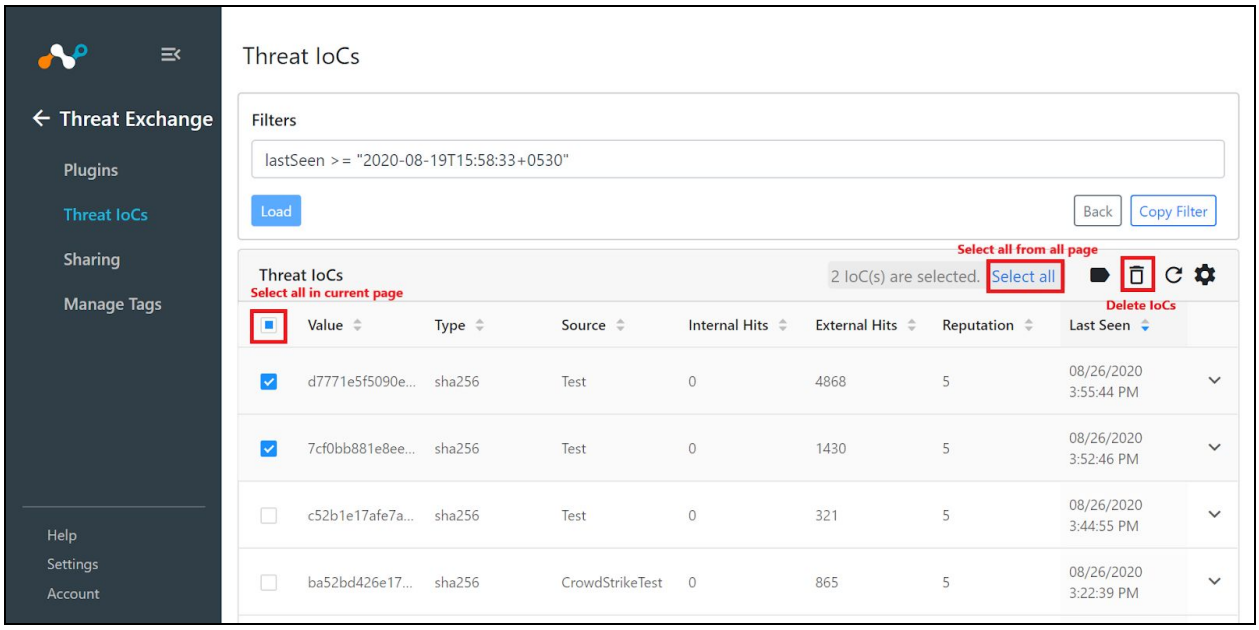
7. Users can copy the filter string that can be used as a filter query in the plugin configuration.
8. Also users can enter the filter query manually and can load the filters according to the query.



2.5.9. Delete threat IoCs

Role required: Admin

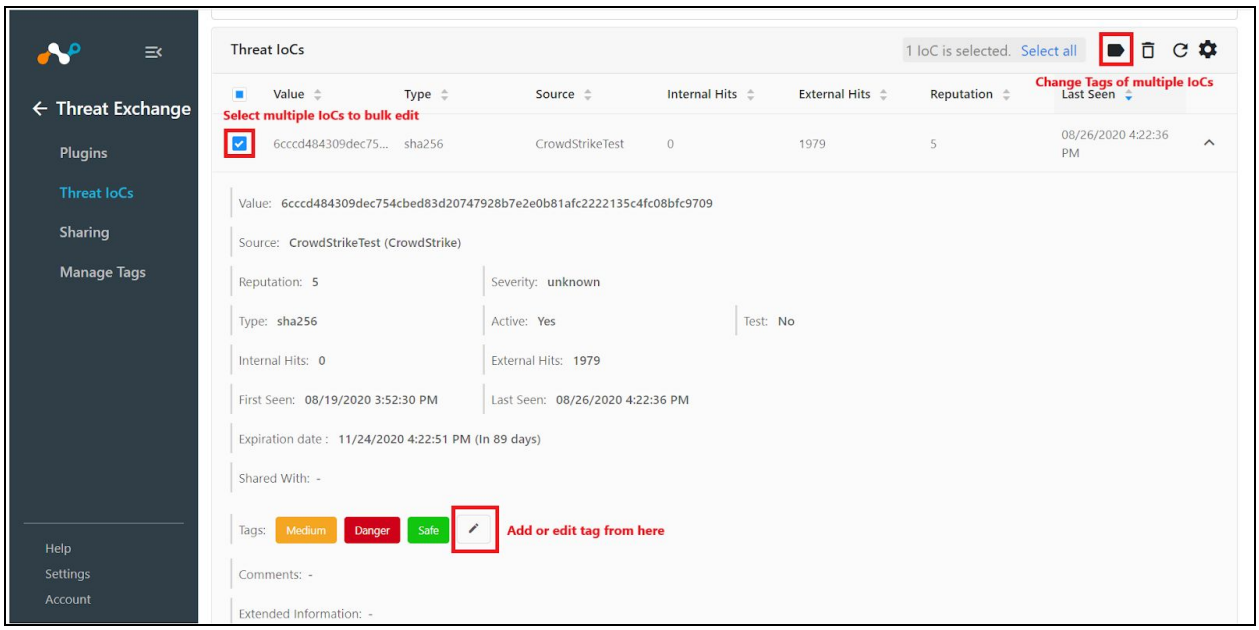
Users can select the threat IoCs or select all IoCs that match the current filter then the user can delete the selected IoCs by clicking the delete button on the right side.



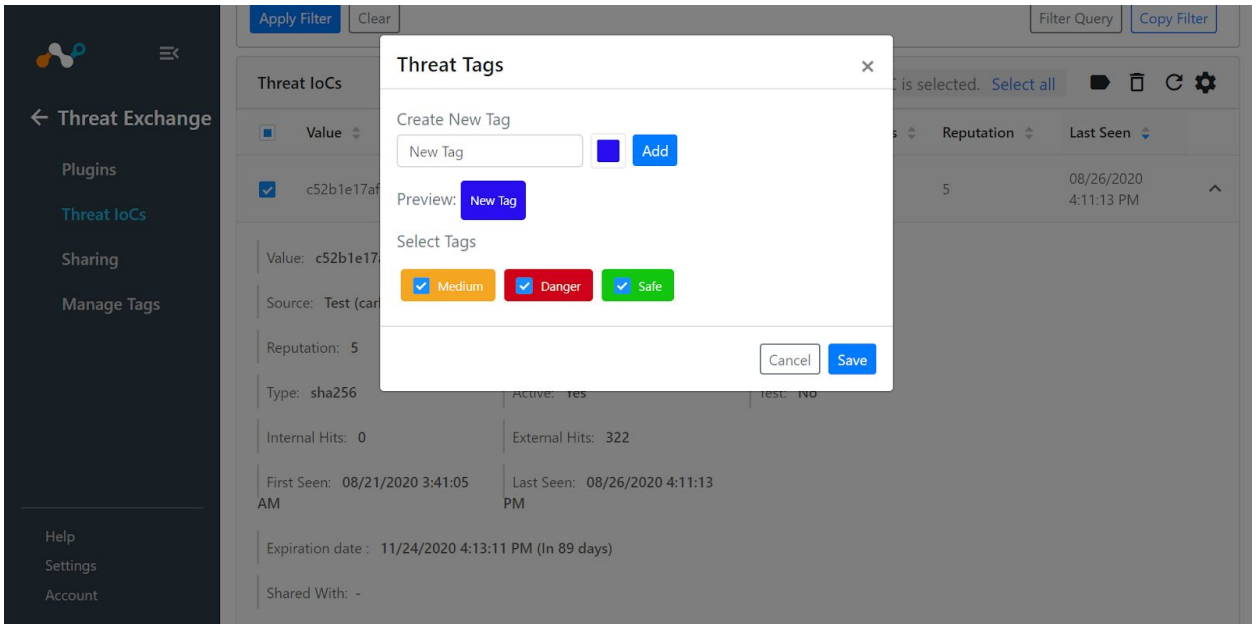
2.5.10. Select and modify tags

Role required: Admin

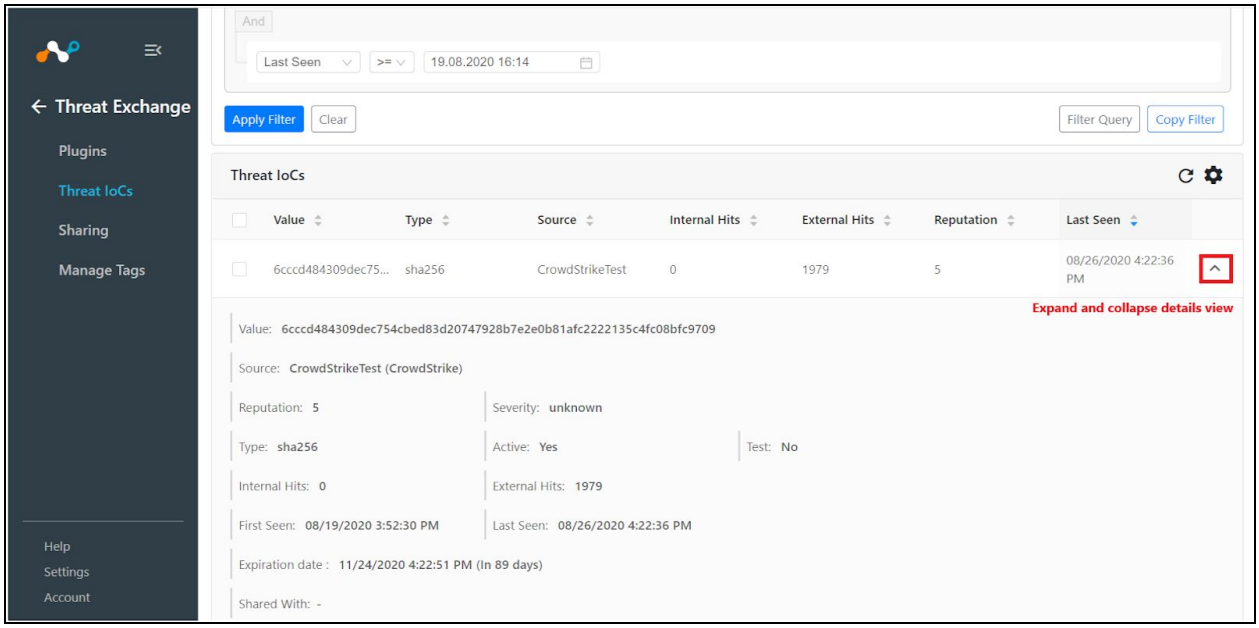
Tags are displayed in the detail view of the IoC. Users can add or edit the tags from there or user can select IoCs and click on the tags button to select tags.



Users can select or deselect the tags for selected iocs. Also user can create new Tags.



To view more details about a particular IoC user can click on the + icon and row will be expanded with details of the IoC.

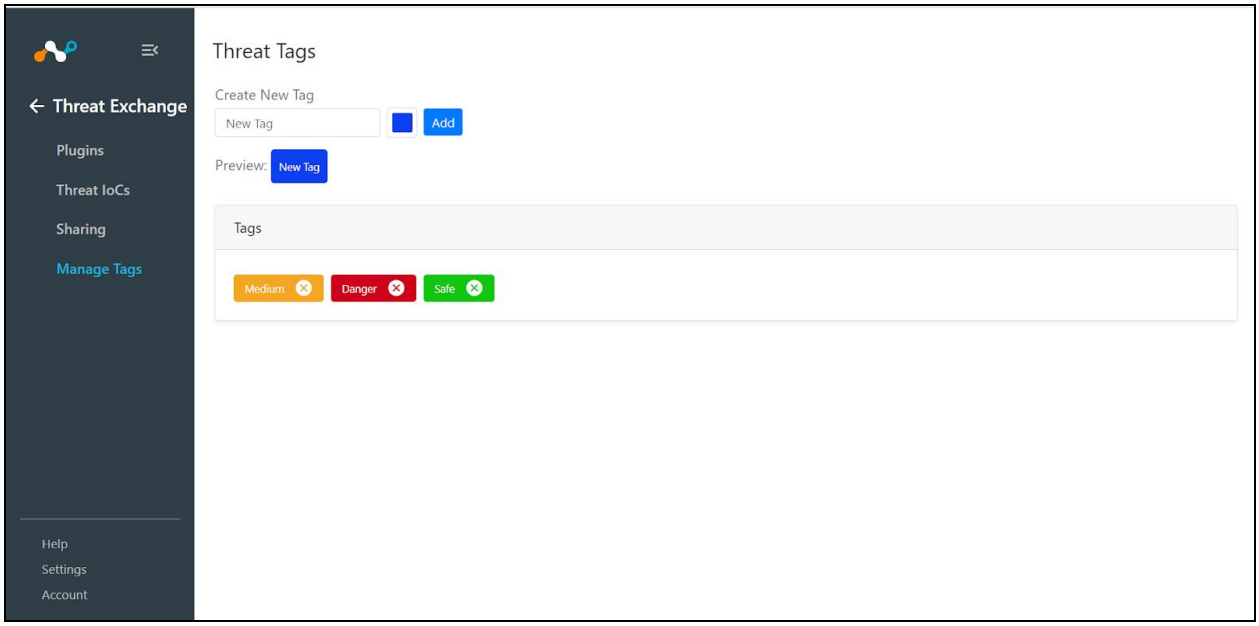


2.5.11. Manage Tags

Users can create new Threat tags or delete them in this settings menu.

Role required: Admin

1. Users can enter a name and select color then clicking on the add button will create the new tag.
2. Users can delete the tag by clicking on the cross icon in the tags list.



2.6. Ticket Orchestrator(CTO)

2.6.1. Plugins

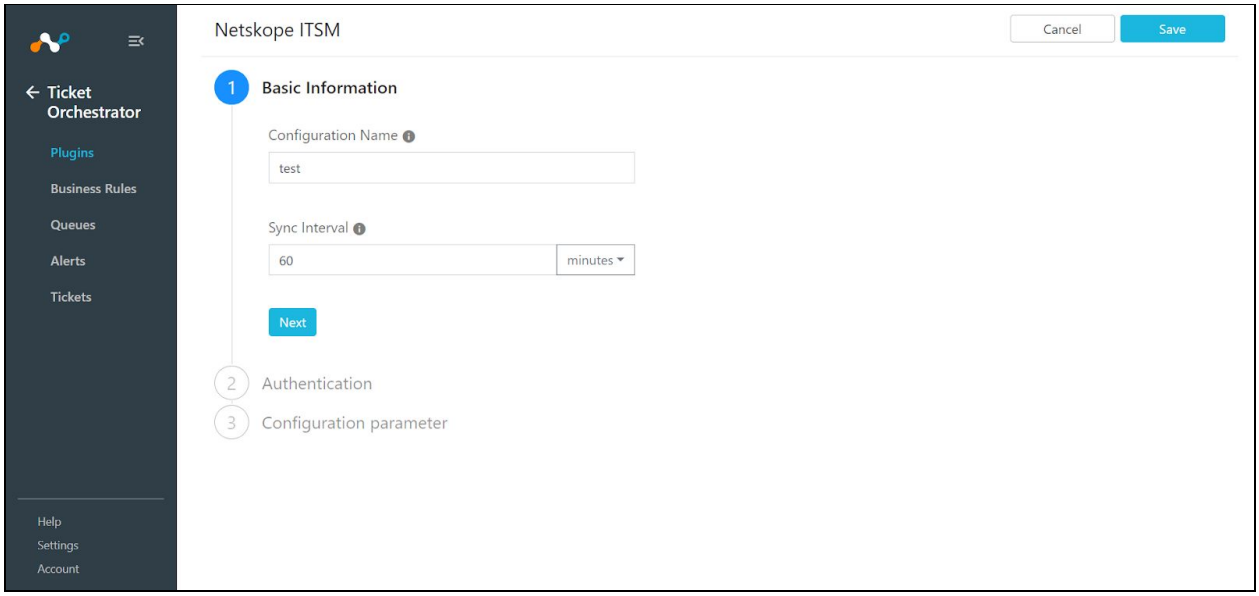
Netskope CTO comes with the library of supported plugins. Plugin can be easily configured for fetching alerts. Users can also disable/enable, delete the existing plugin configuration.

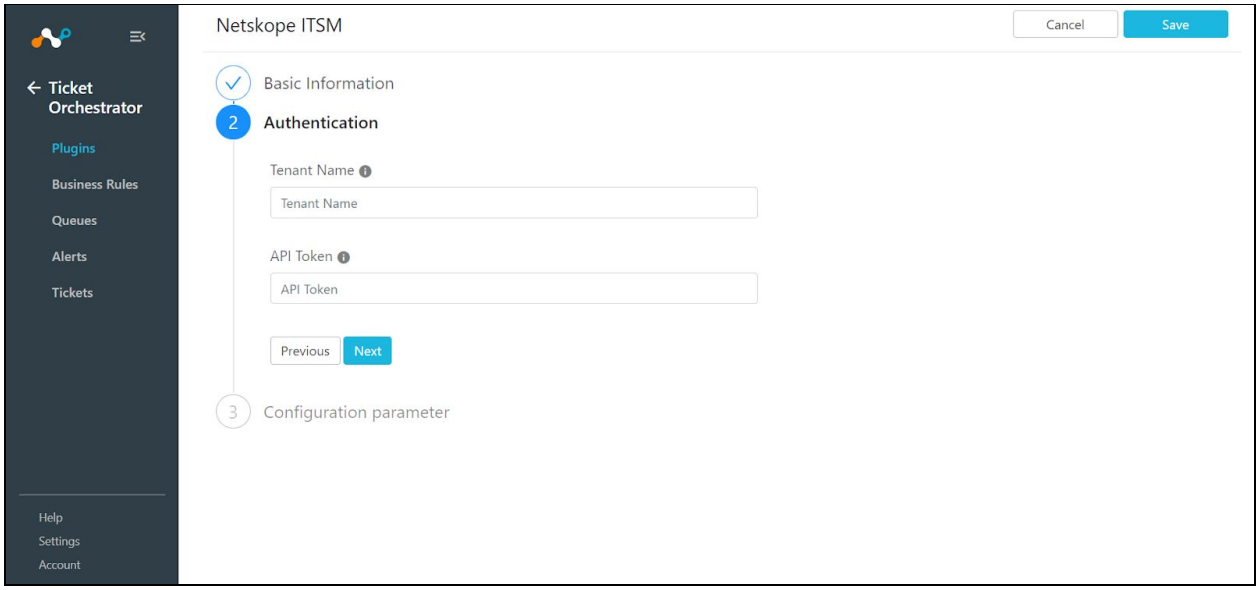
Role Required : admin

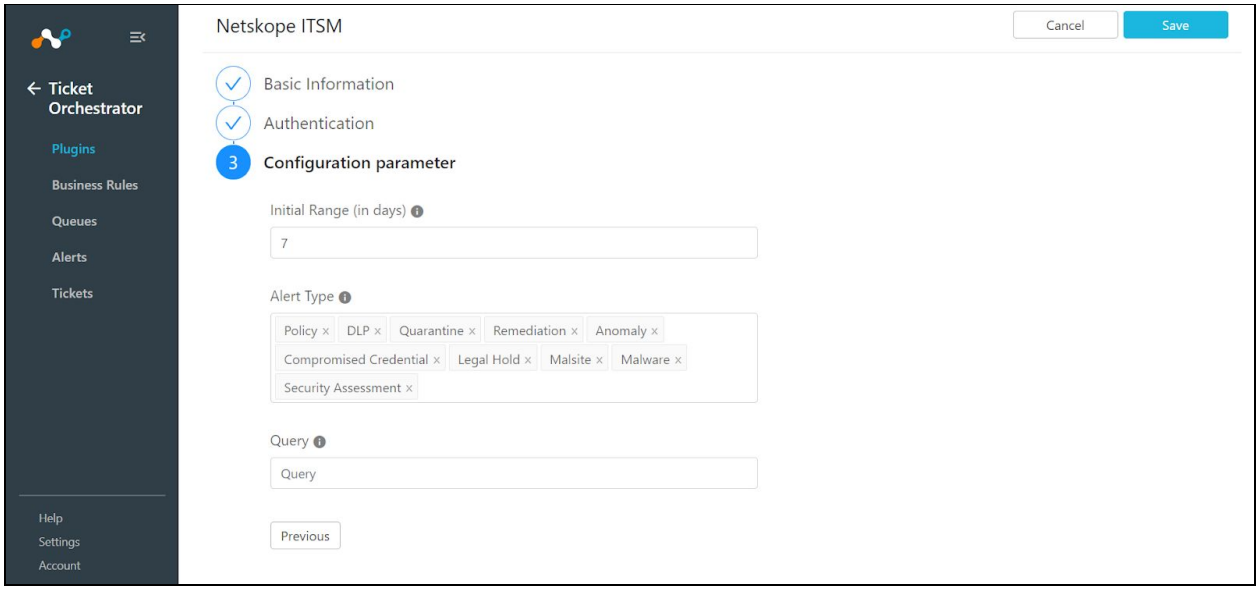
2.6.2. Configure primary Netskope tenant

This part section describes how to configure the primary Netskope tenant. This configuration would ensure that alerts data from the tenant is pulled regularly.

1. Login to Netskope and navigate to Ticket Orchestrator.
2. Navigate to Plugins.
3. Click on that plugin for which you want to create the configuration.
4. The Configuration page will open with some steps which includes basic information fields like Configuration Name, Sync Interval, Tenant name, API Token.
5. After adding valid credentials, the last step will include Initial range,Alert Type, Query for which alerts will be received from the platform.
6. Click on save to create the configuration.


Netskope ITSM
Cancel
Save
Ticket Orchestrator
Plugins
Business Rules
Queues
Alerts
Tickets
Help
Settings
Account
1 Basic Information
Configuration Name
test
Sync Interval
60
minutes
Next
2 Authentication
3 Configuration parameter


Netskope ITSM
Cancel
Save
Ticket Orchestrator
Plugins
Business Rules
Queues
Alerts
Tickets
Help
Settings
Account
Basic Information
2 Authentication
Tenant Name
Tenant Name
API Token
API Token
Previous
Next
3 Configuration parameter



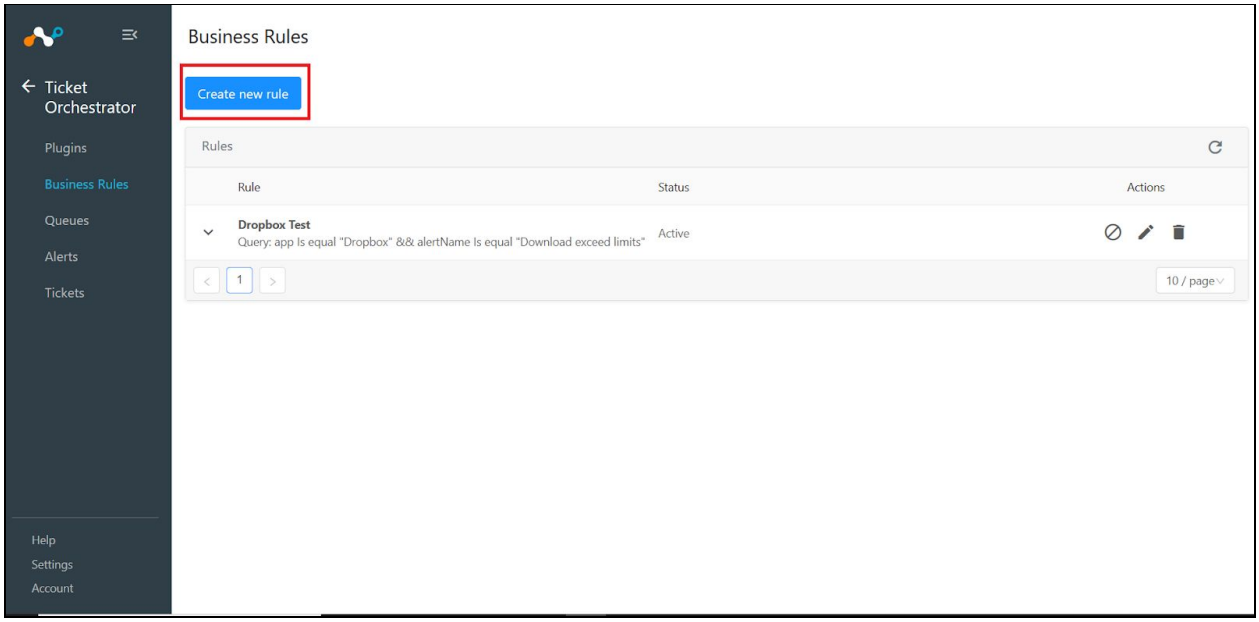
Field	Description	Default Value
Configuration Name	Plugin configuration name.	
Sync Interval	Interval to fetch data from source.	60 minutes
API Token	API token to authenticate Netskope Tenant.	
Tenant name	Netskope Tenant name e.g. <tenant-name>.goskope.com	
Initial Range	Number of days to pull the data from initial run	7 days
Alert Type	Types of alert to fetch	
Query	This acts as a filter for all the cloud app events in the events database.	

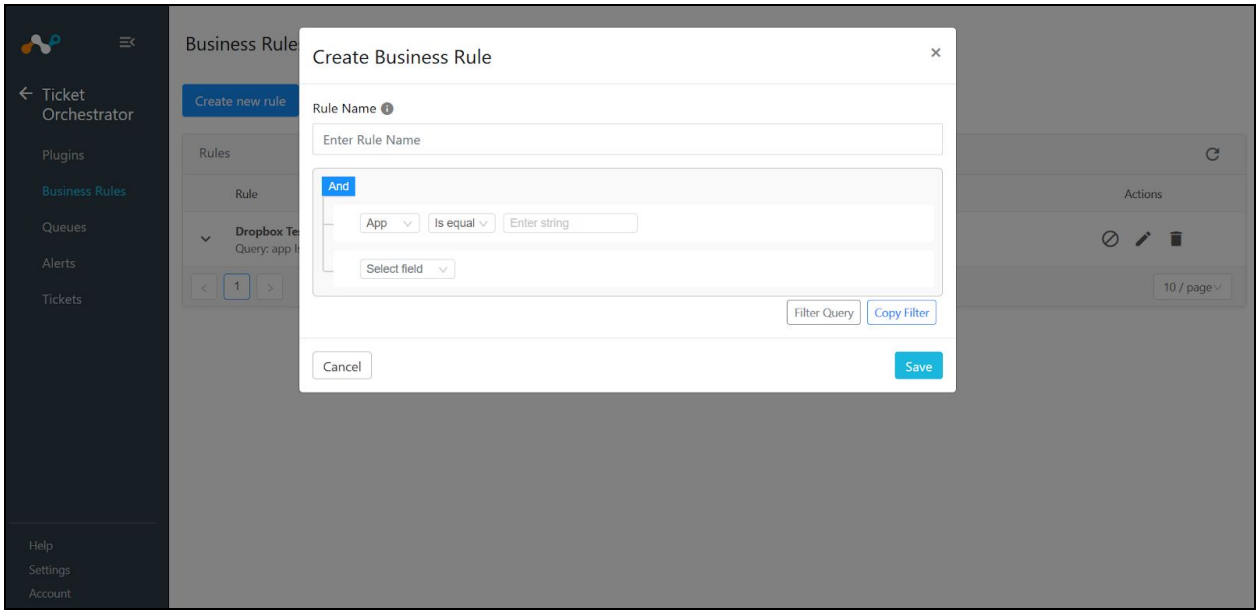
2.6.3. Create Business Rules

Users can configure queries as business rules, so users can specify what kind of alerts the user wants to be used for the CTO system for ticket creation. The alert matching a particular business rule will be converted into tickets.

Role Required : admin

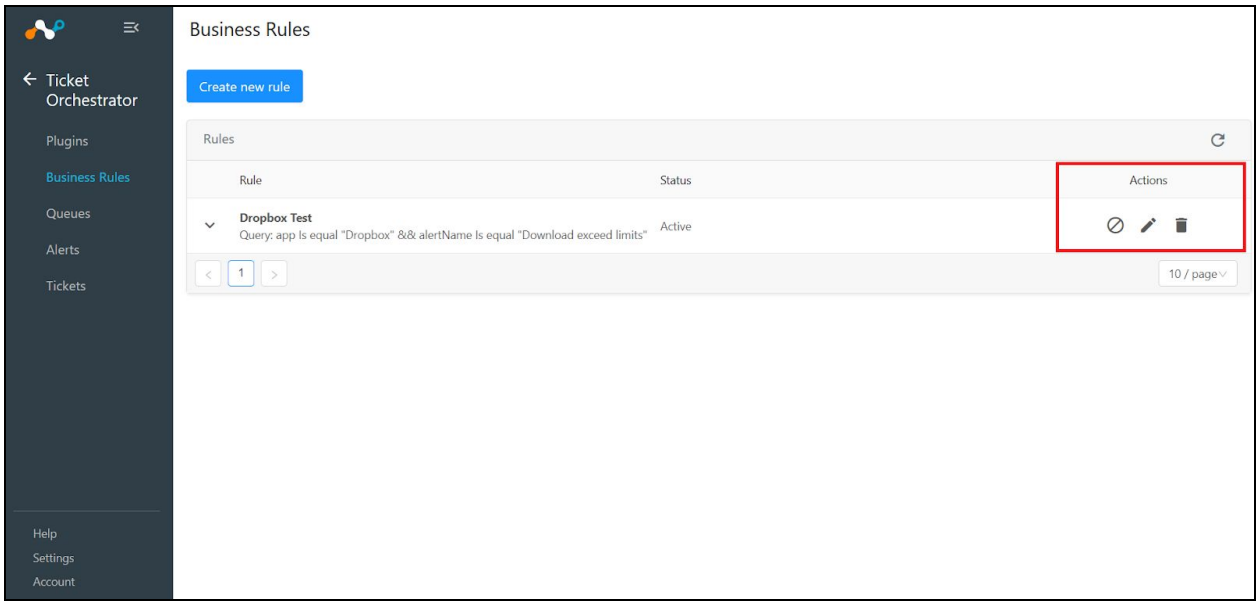
1. Login to Netskope and navigate to Ticket Orchestrator.
2. Navigate to Business Rules.
3. Click on the “Create new rule” button.
4. Enter Rule name select query from alert filter.
5. Click on the “Save” button.

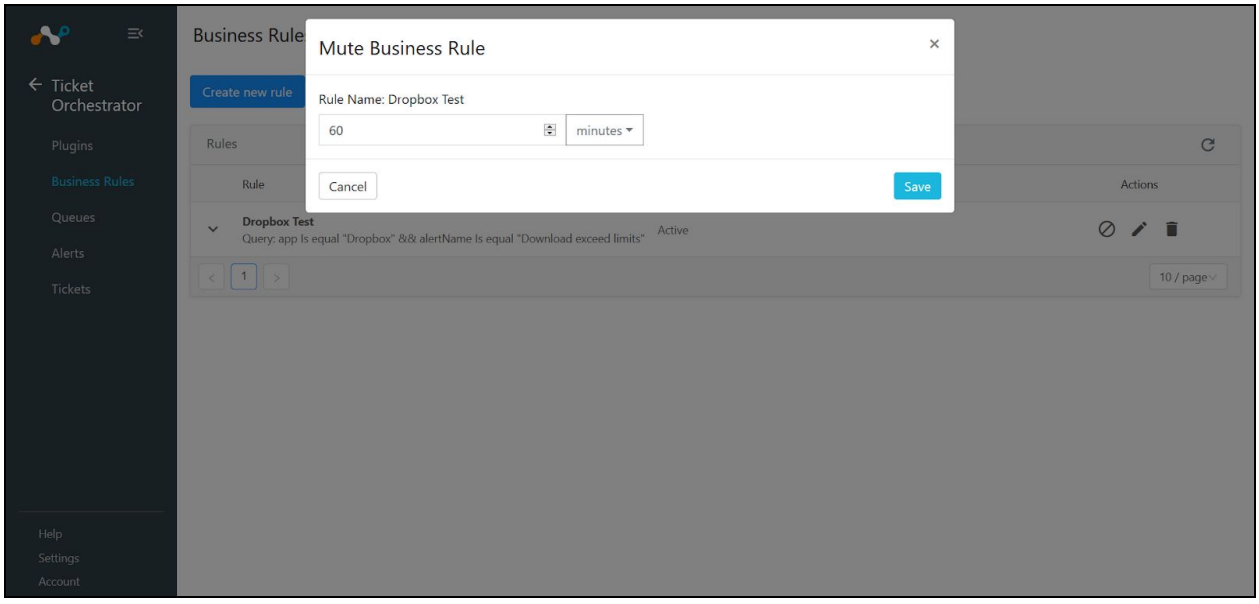


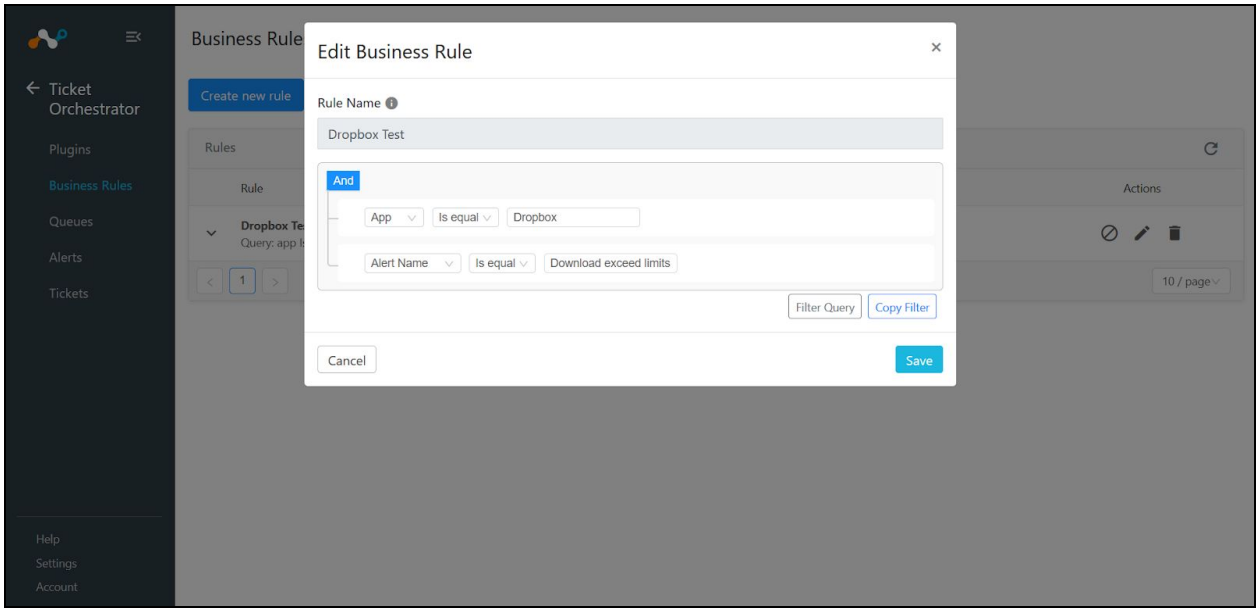


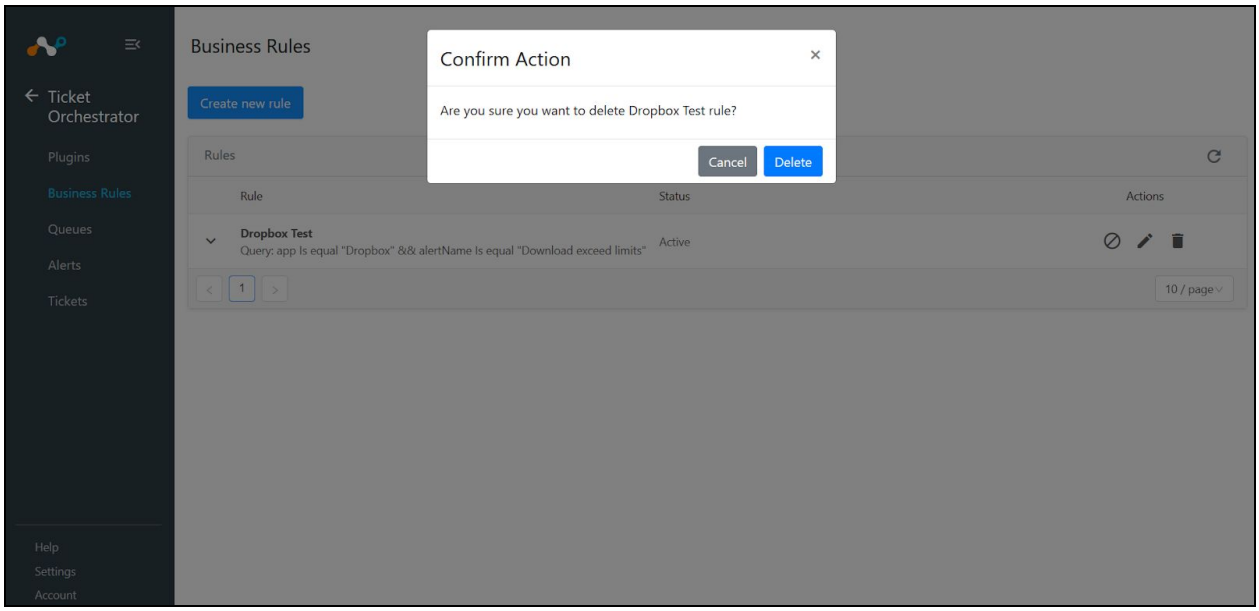
2.6.4. Perform Action on Business Rules

Users can manage all the business rules from a single place on the platform. User can mute one or multiple business rules, edit the query for business rules, delete the business rules.





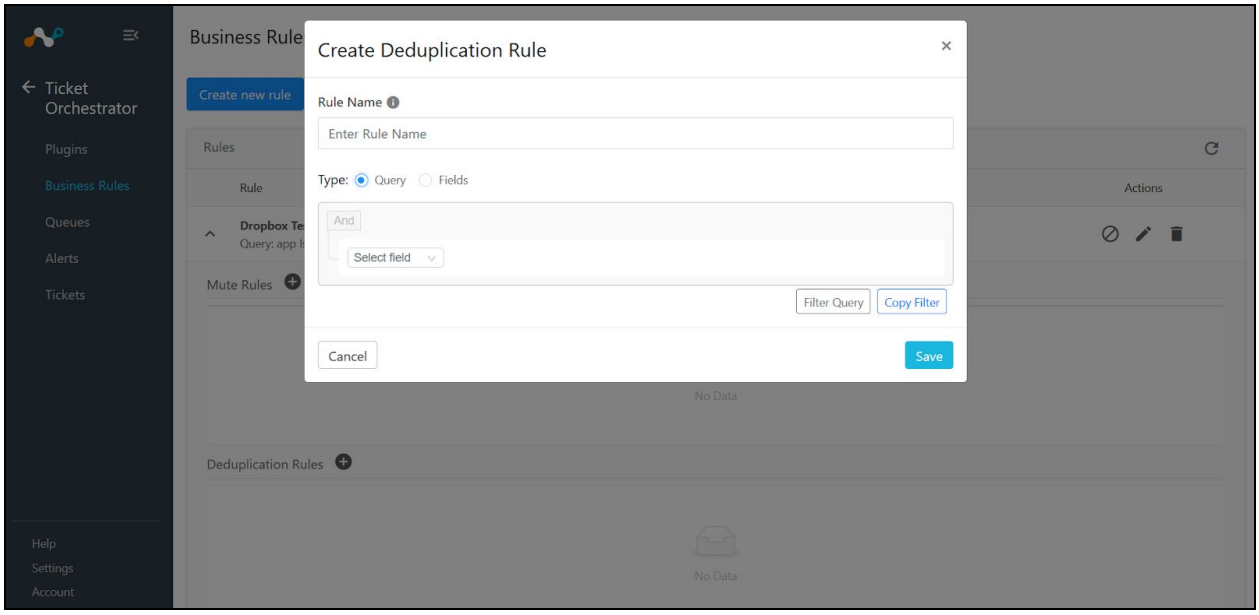




2.6.5. Add deduplication rules to Business Rules

Users can add deduplication rules or muted deduplication rules to the business rules to de-duplicate all the matching alerts into a single ticket on the target platform. For all the matching alerts, only a single ticket will be created and updated.

Role Required : admin

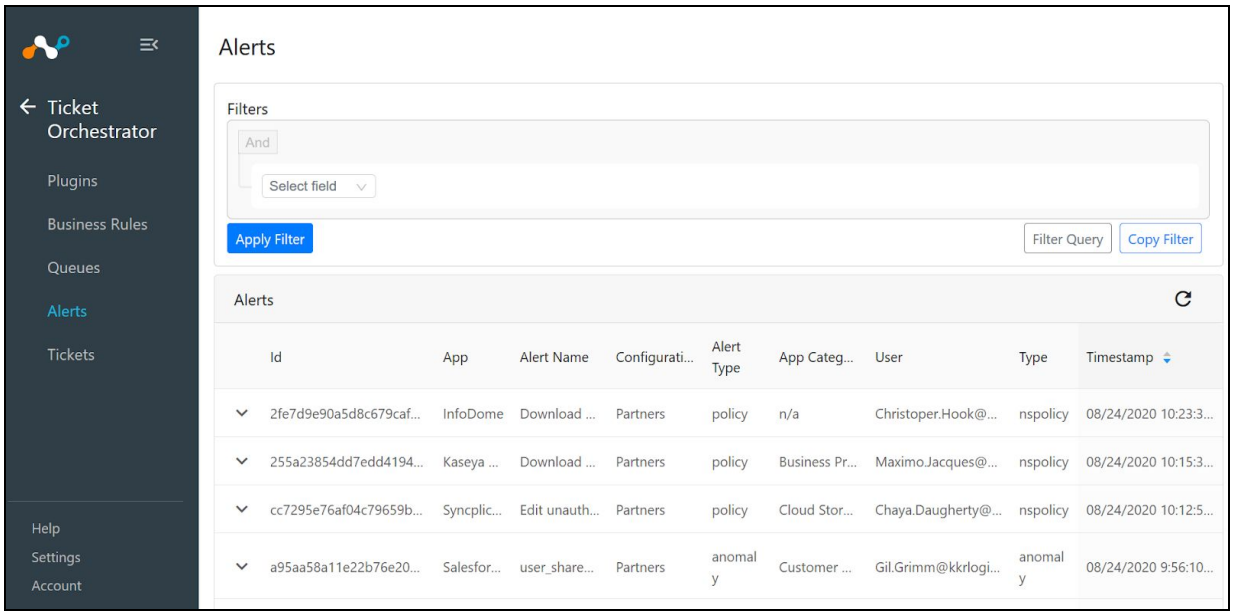


2.6.6. List Alerts and filtering capability

Netskope CTO maintains the database of Alerts captured from configured plugins. Users can list the available Alerts, view the metadata and filter the Alerts.

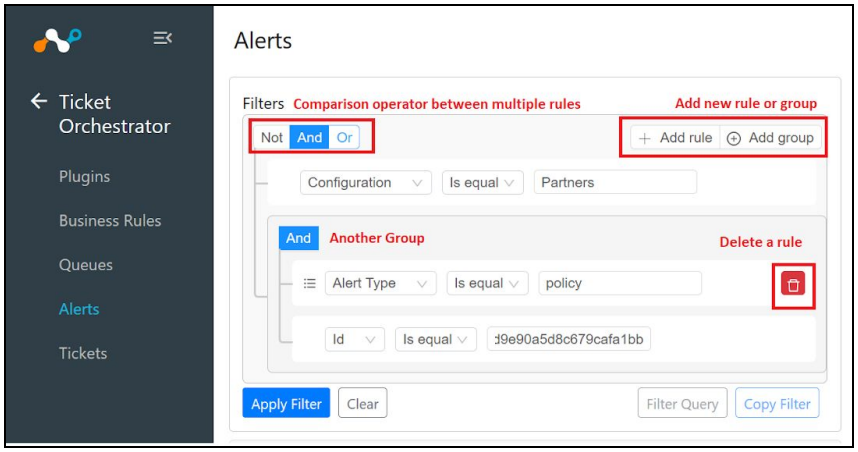
Role Required : admin or read-only

1. Login to Netskope and navigate to Ticket Orchestrator.
2. Navigate to Alerts. The Alerts list is paginated with a default page size of 10. The records are sorted in descending order of Time stamp.

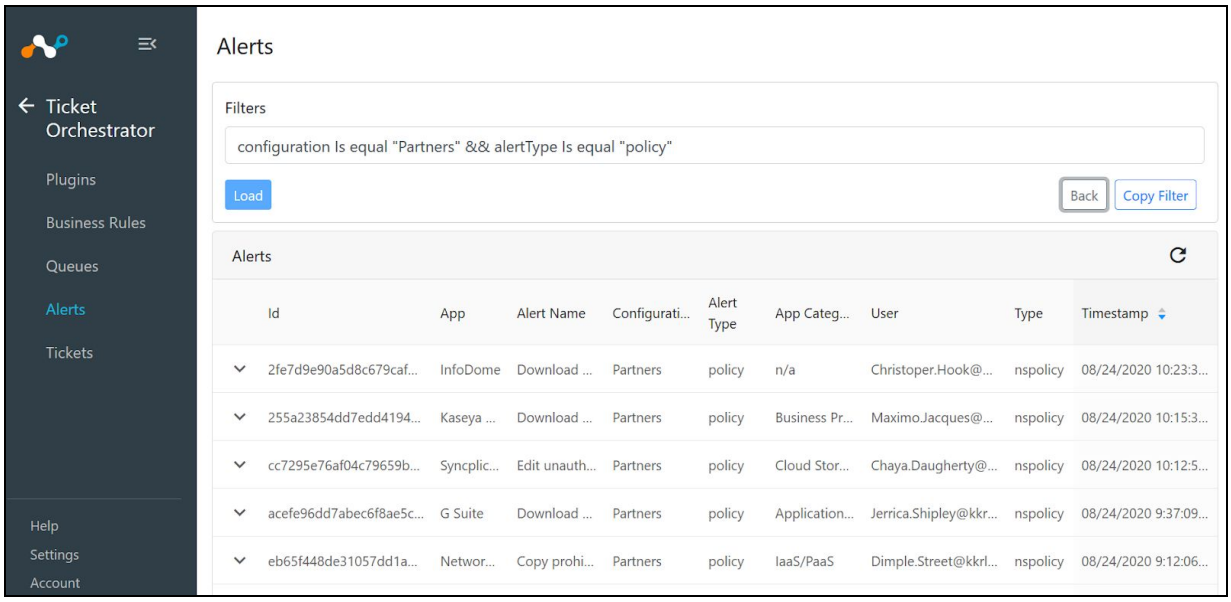


3. After selecting the desired filter, Click Apply Filter. The Alerts matching the filtering criteria would be listed.

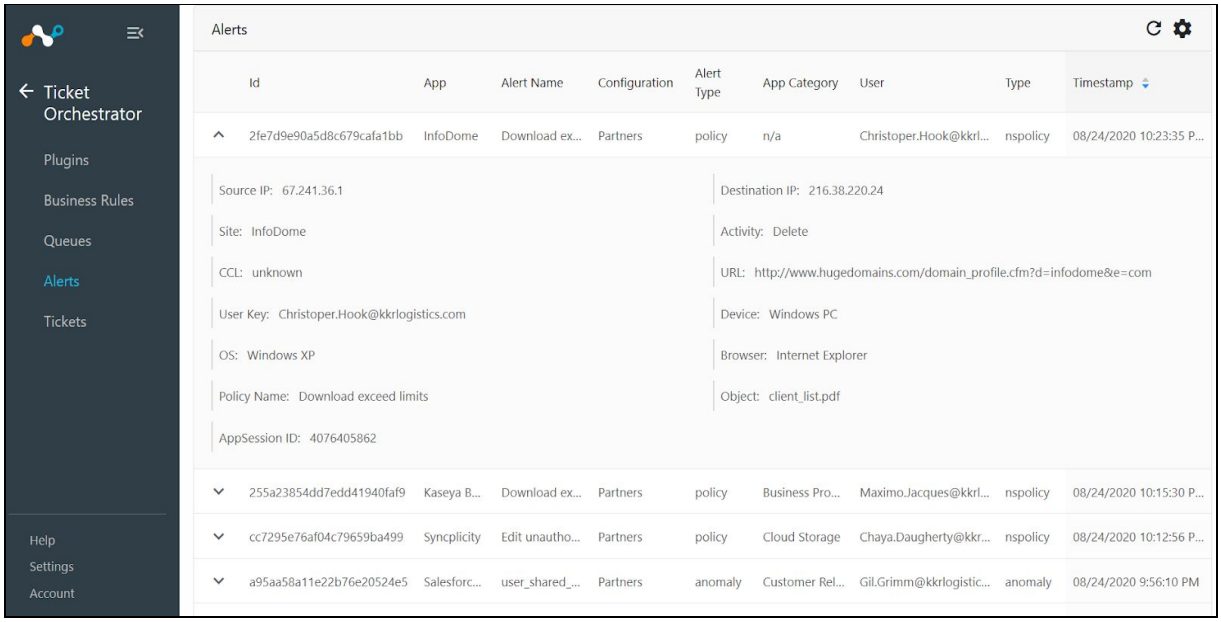
4. To remove the custom filter, Click on Delete Filter option. This removes the applied filter and fallbacks to default filter. The Alerts matching the default filter would be listed.



5. Users can copy the filter string that can be used as a filter query in the plugin configuration.
6. Also users can enter the filter query manually and can load the filters according to the query.



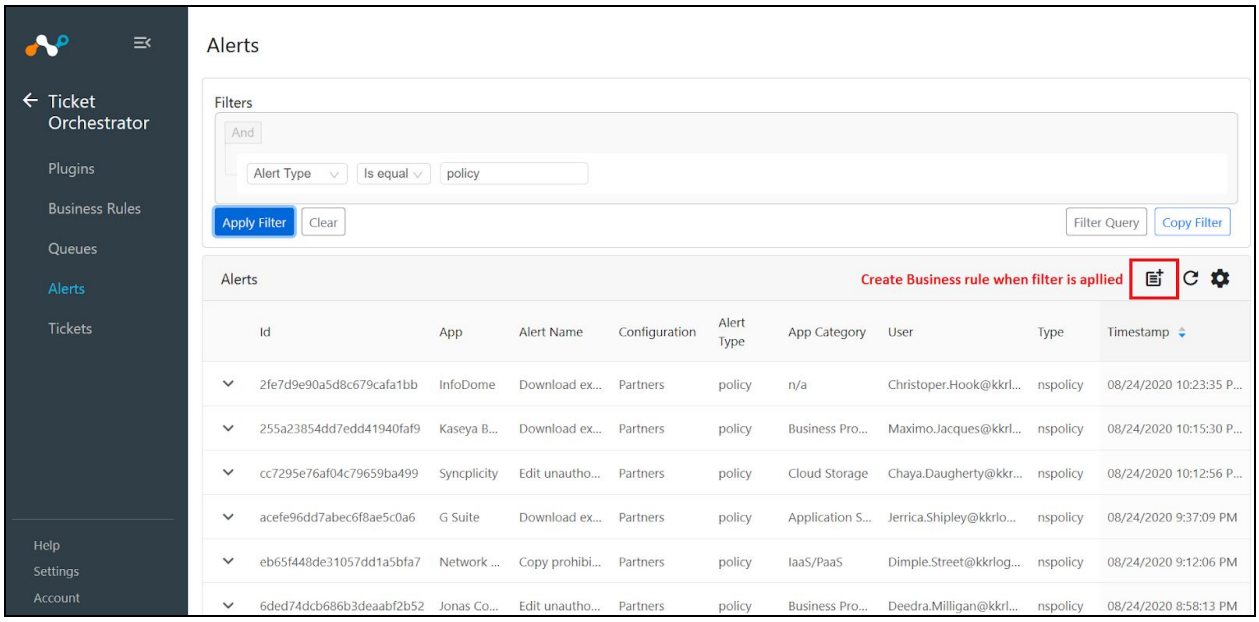
7. Expand row functionality in table.

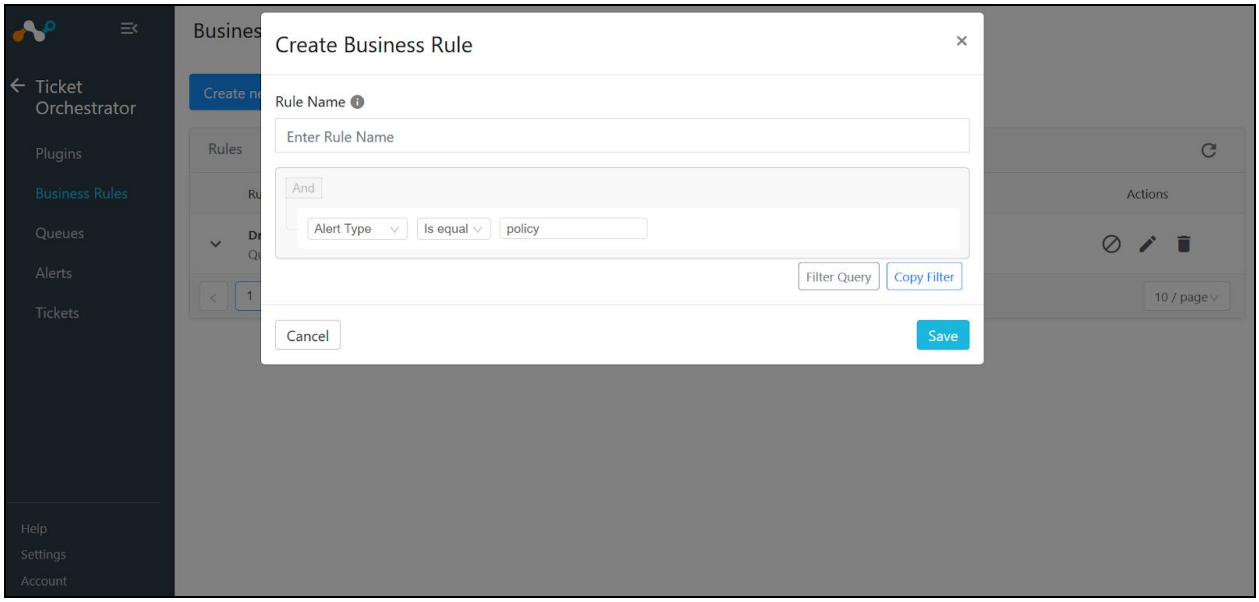


2.6.7. Create Business Rules from filter of alerts

Users can create business rules from the Alert page when the filter is applied. Query for that business rule will be generated based on the alert filter.

Role required : admin



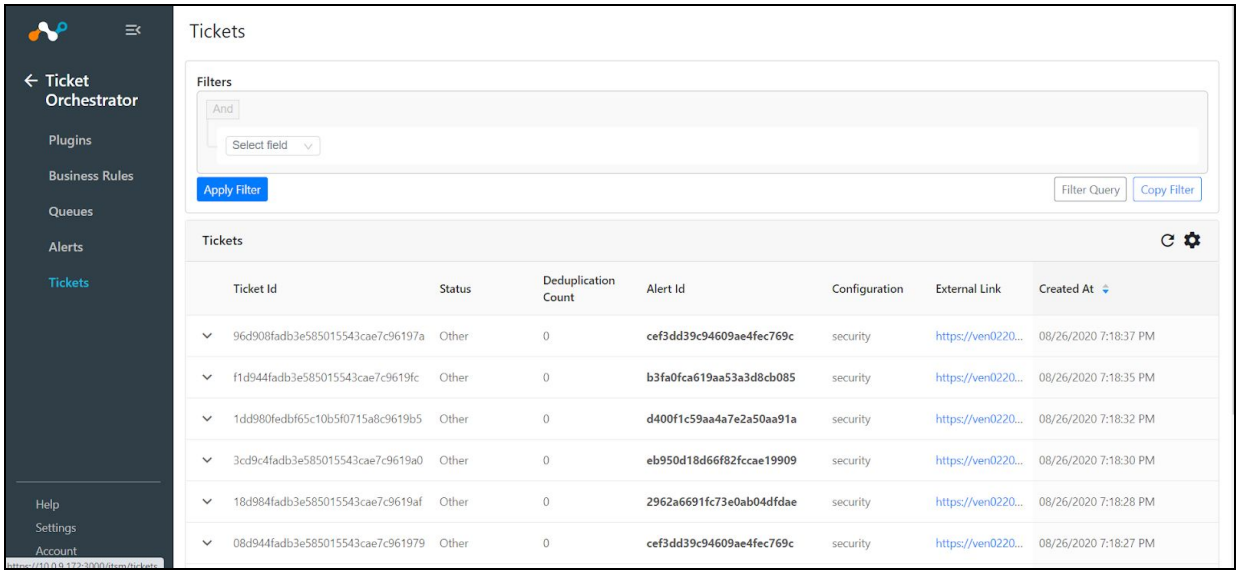


2.6.8. List Tickets and filtering capability

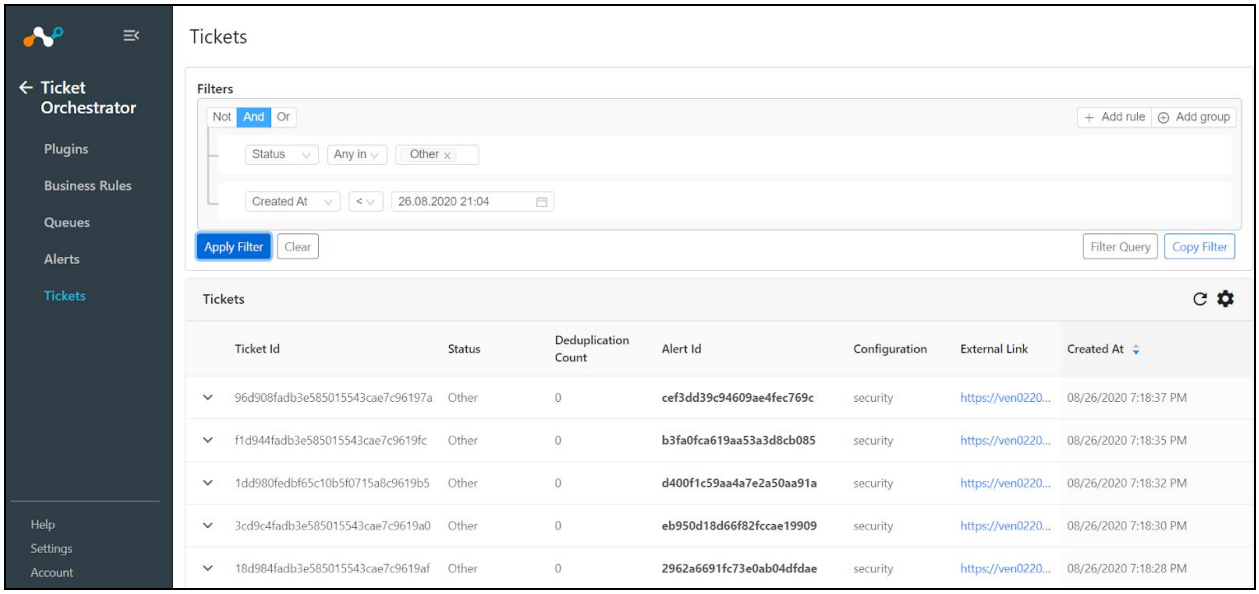
Netskope CTO maintains the database of Alerts captured from configured plugins. Users are required to list the available Alerts, view the metadata and filter the Alerts.

Role Required : admin or read-only

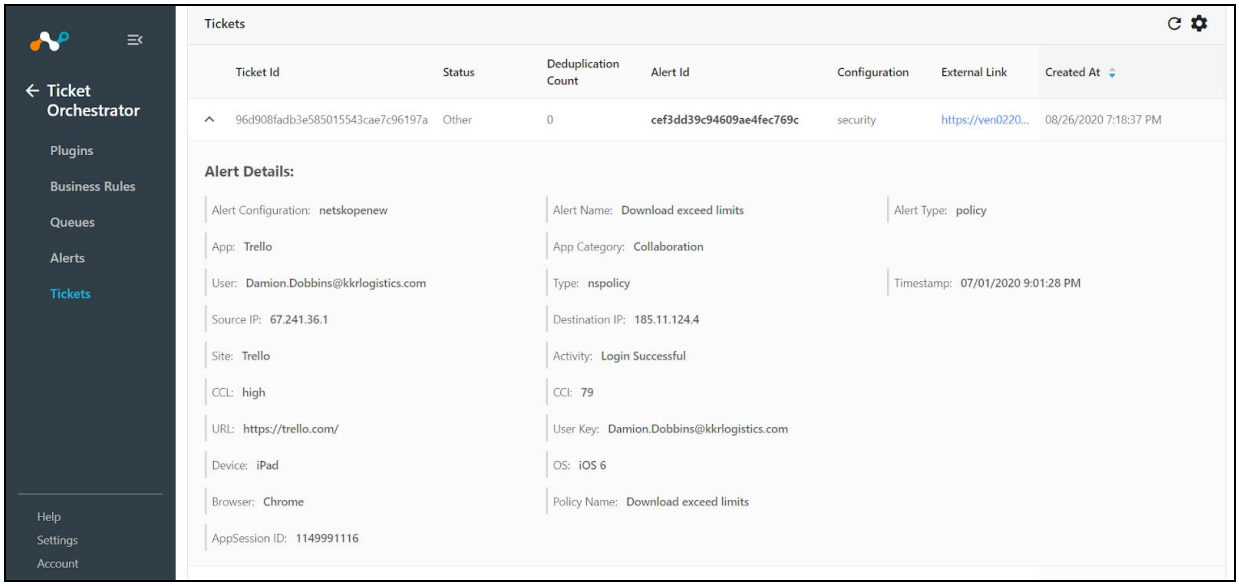
1. Login to Netskope and navigate to Ticket Orchestrator.
2. Navigate to Tickets.The Tickets list is paginated with a default page size of 10. The records are sorted in descending order of Created At.



3. After selecting the desired filter, Click Apply Filter. The Tickets matching the filtering criteria would be listed.



4. To remove the custom filter, Click on Delete Filter option. This removes the applied filter and fallbacks to default filter. The Tickets matching the default filter would be listed.
5. Users can copy the filter string that can be used as a filter query in the plugin configuration.
6. Also users can enter the filter query manually and can load the filters according to the query.
7. Expand row functionality in table.

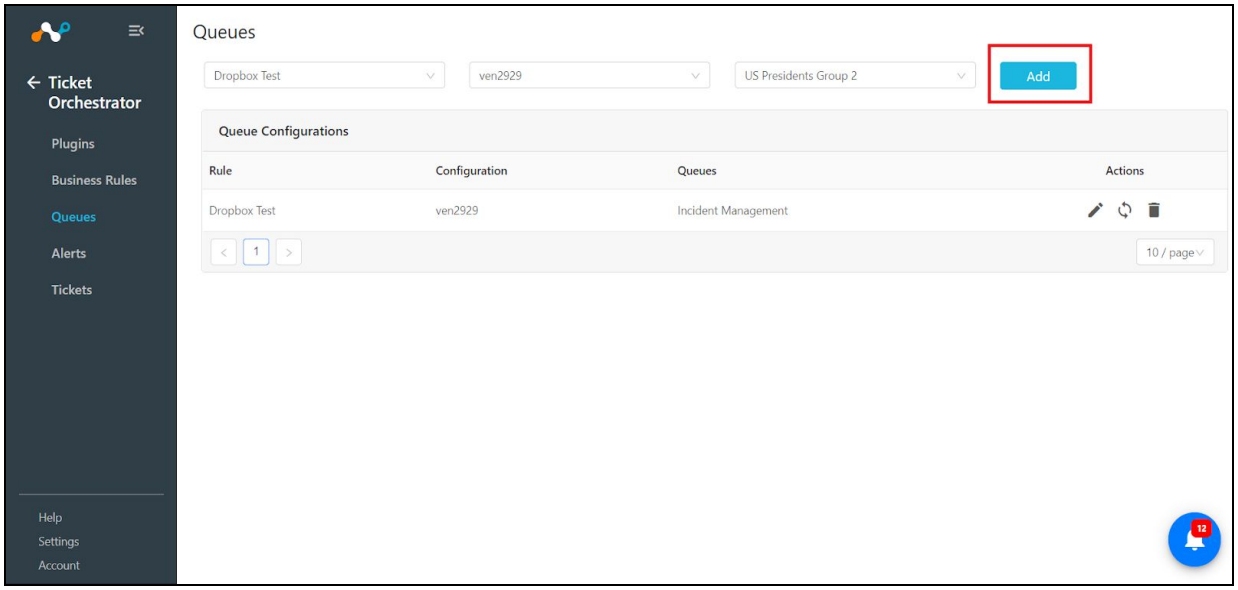


2.6.9. Forward alerts matching a business rule to Queue associated with configurations

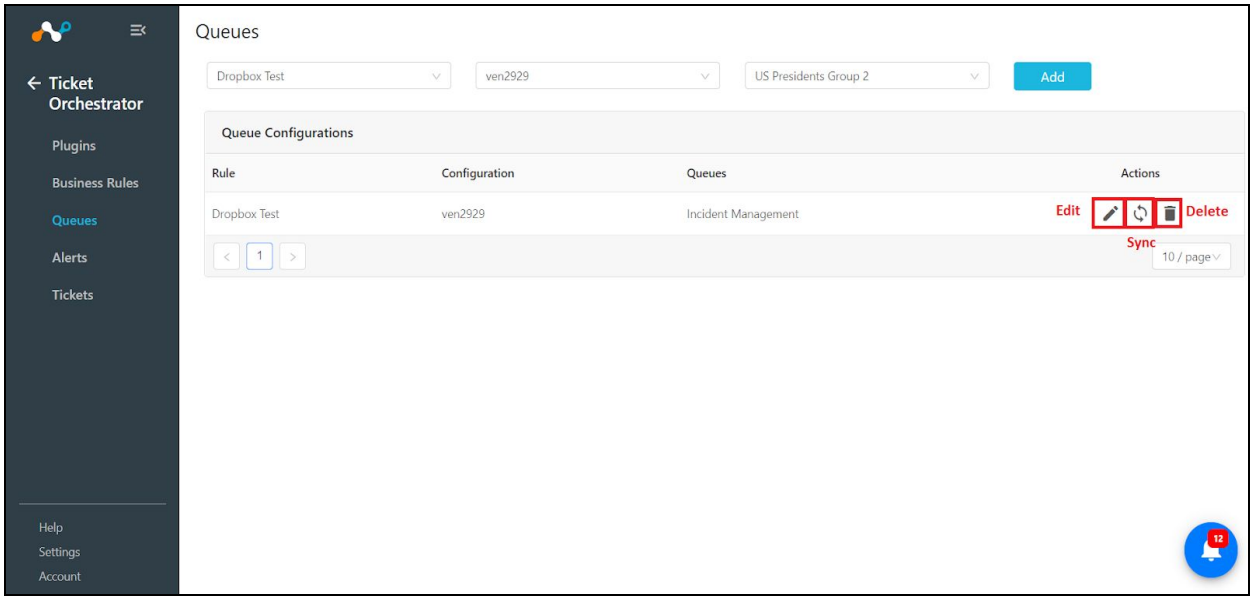
Users can link business rules to configuration queues such that users can receive tickets at different places on a single platform without making multiple configurations. Users can also perform actions on a list of queues.

Role required: admin

1. Login to Netskope and navigate to Ticket Orchestrator.
2. Navigate to Queues.The Queue configuration list is paginated with a default page size of 10.
3. Users can select business rules and configuration associated with the queue. Click on “Add” button to add queue configuration.



4. Users can perform action(Edit, Sync, Delete) on the queue.

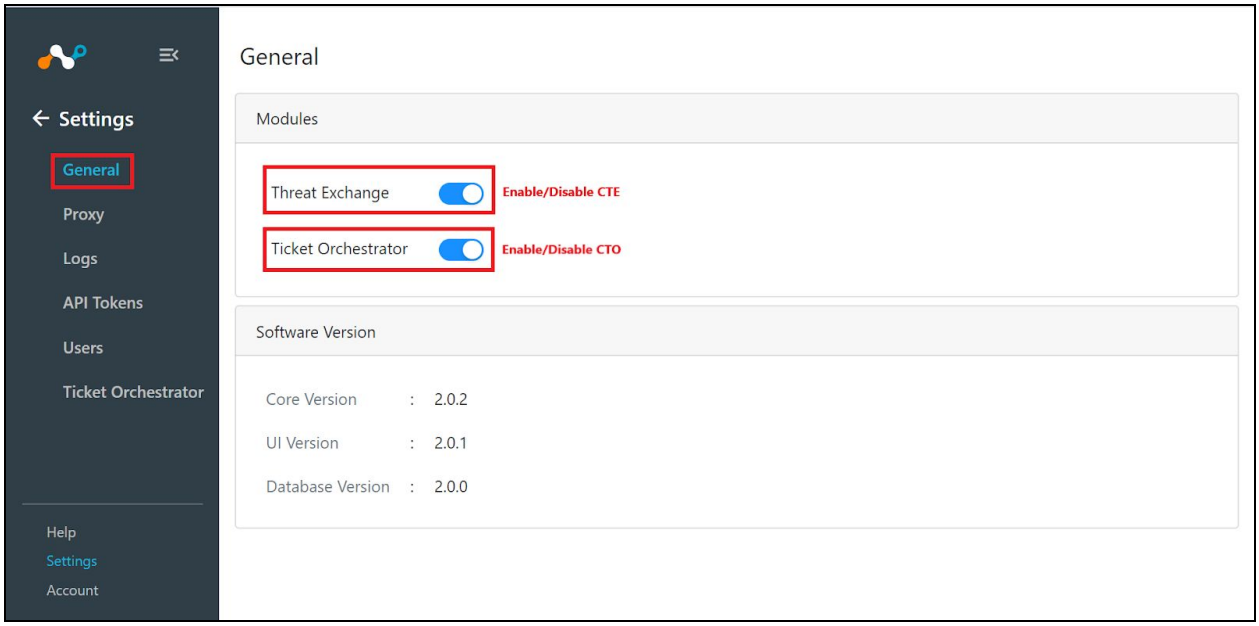


2.7. Settings

This section provides details about different settings that are available.

2.7.1. General

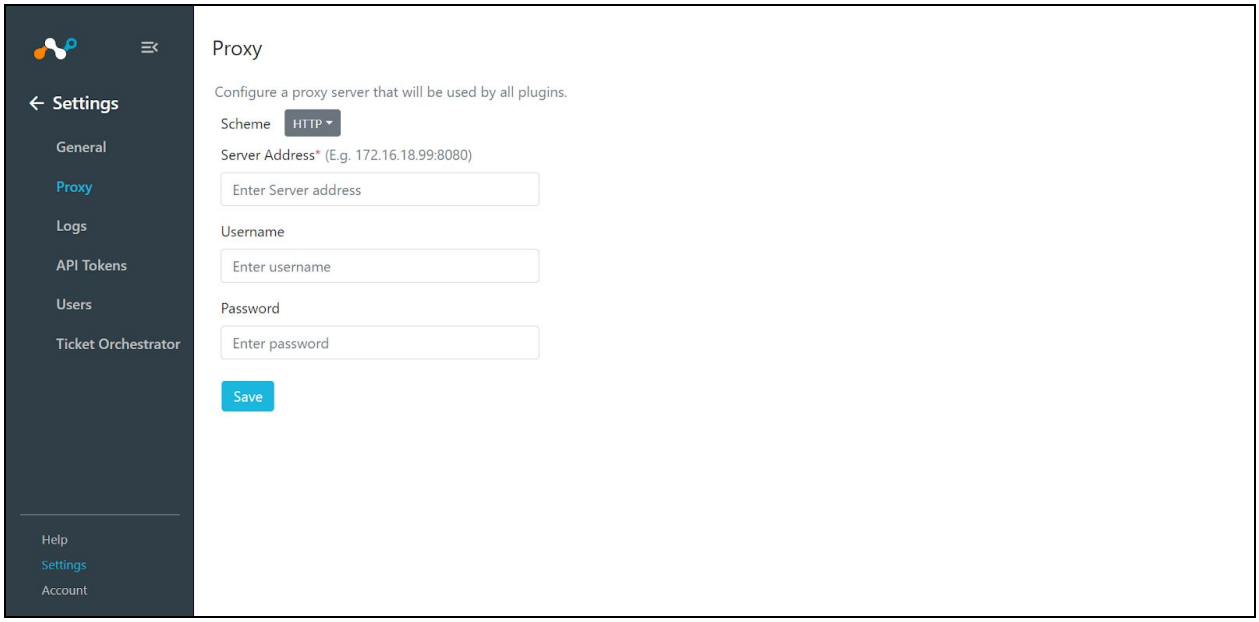
Super admin user will be able to enable/disable modules from here. Versions of the Core, UI and Database will be displayed here.



2.7.2. Proxy

Configure proxy settings on this page.

Role required: Admin



2.7.3. Logs

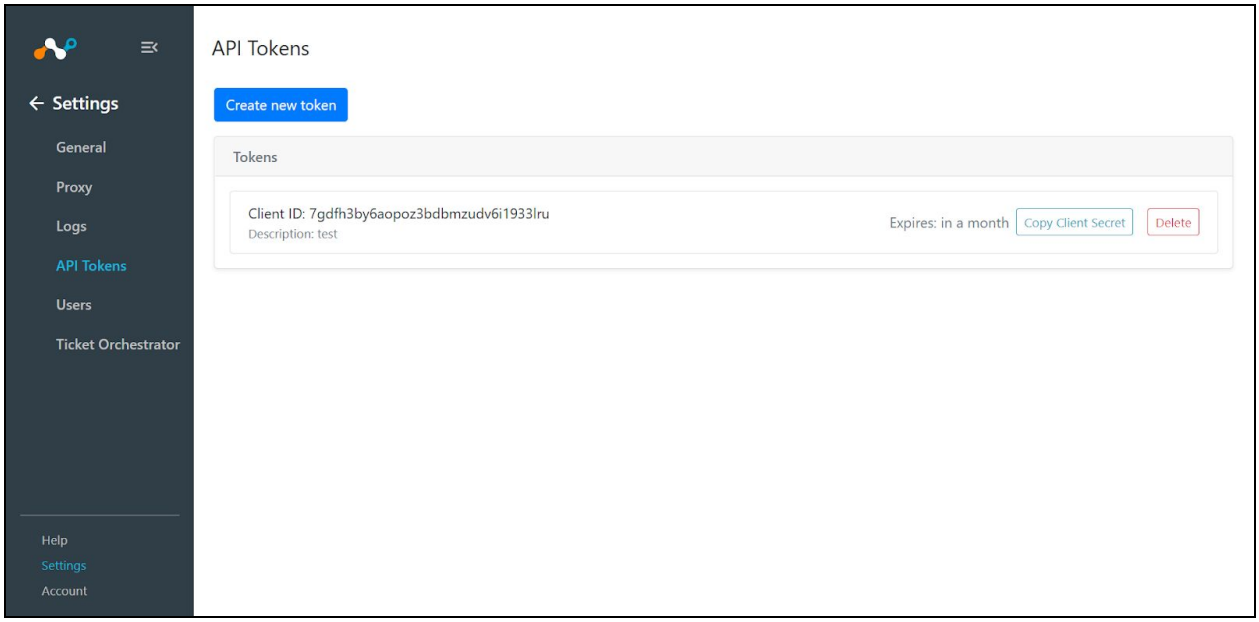
Set the default log level that will be used in application.

Role required: Admin

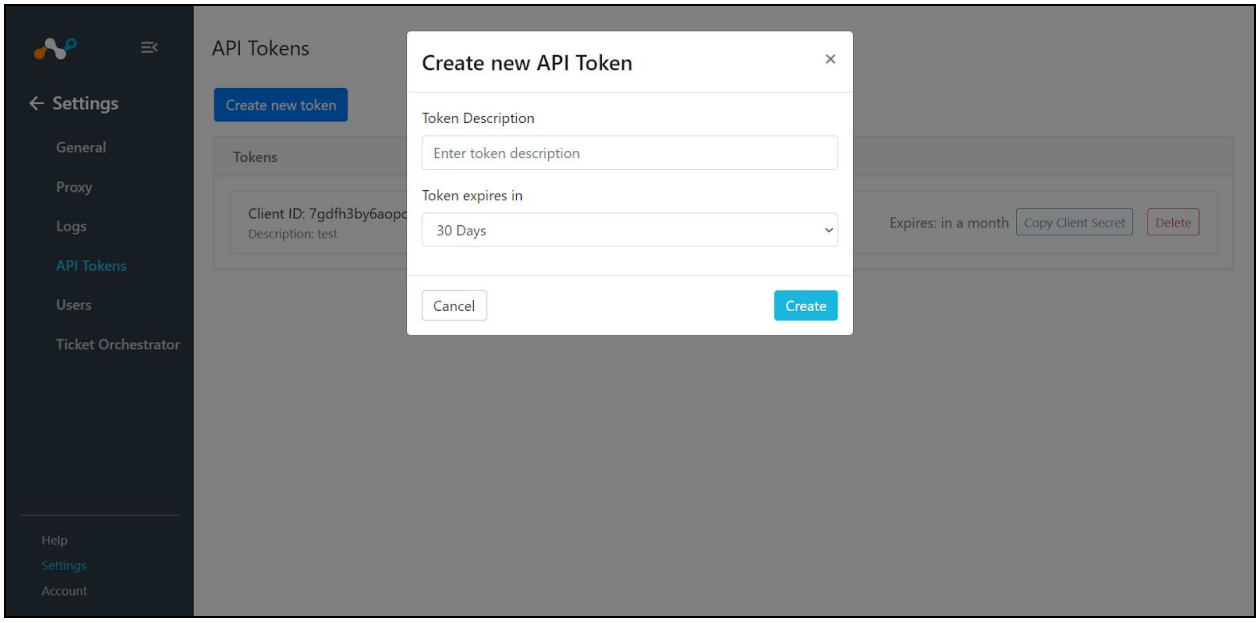
2.7.4. API Tokens

Netskope CTE exposes a REST API and each REST API call requires a valid credentials.
Users who are given API access will be able to create client id and client secret.
Users can create API tokens in these settings.

1. Users can create new API tokens by clicking create a new token button. This will open a form to create new tokens.
2. Users can copy Client secret using a copy button and client id and client secret can be used to access CTE APIs.



3. Users can fill description and expiry days of the token.

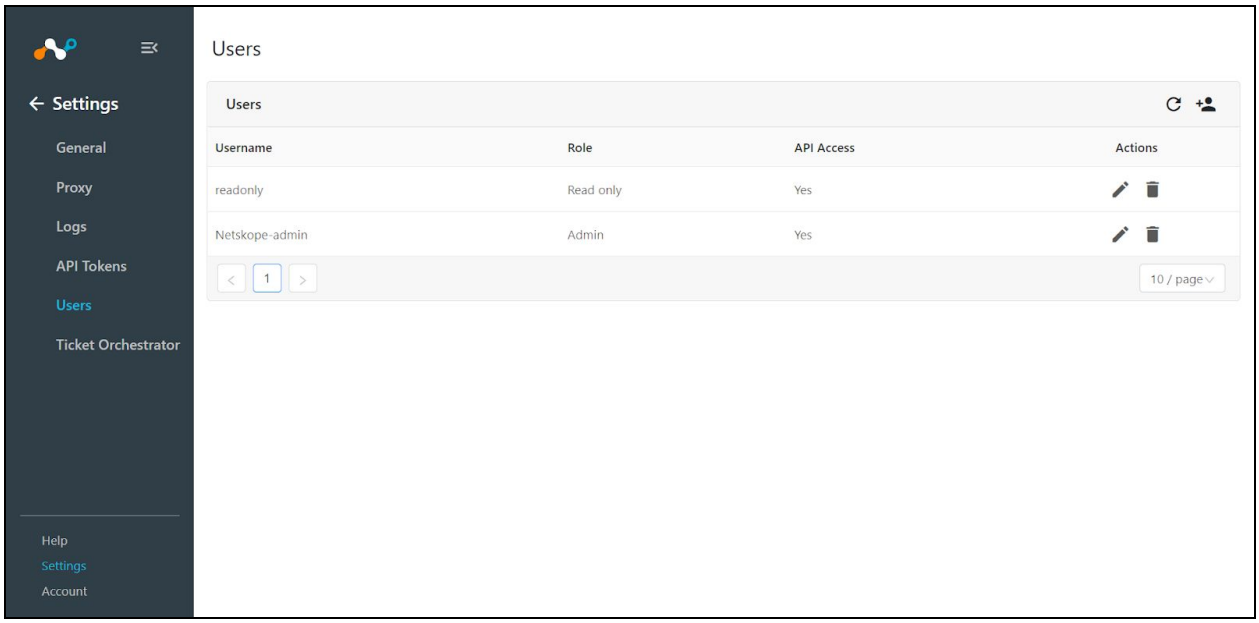


2.7.5. Users

New users can be added to the Netskope CTE with this setting.
Role required: Super admin
User Roles:

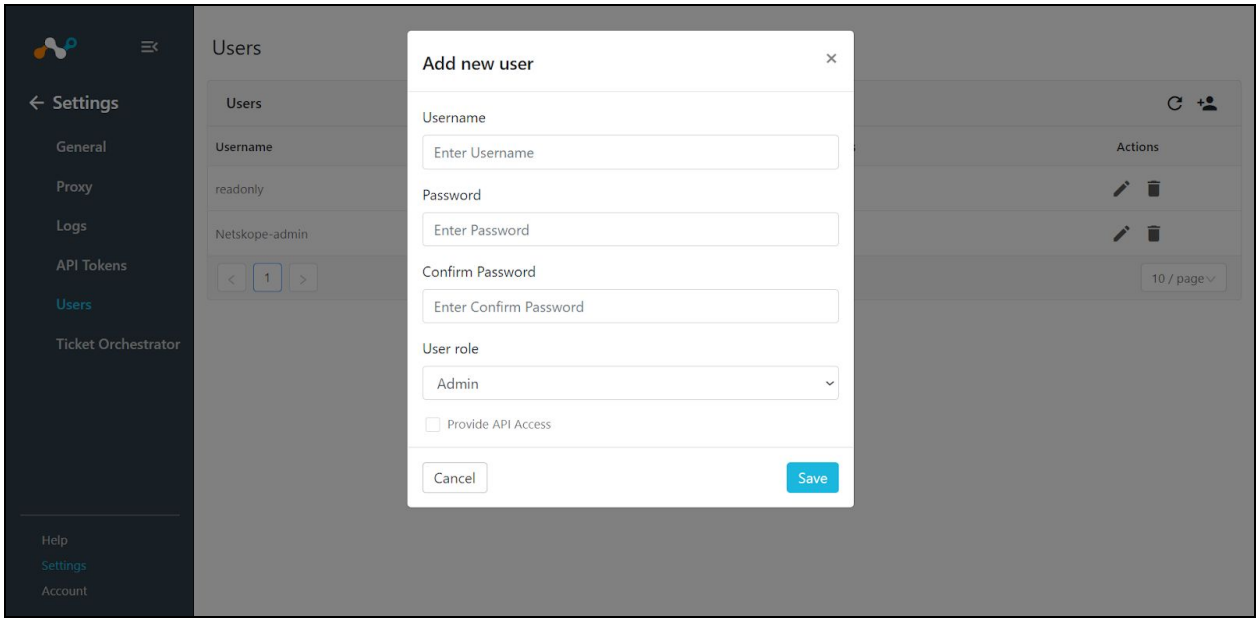
2. admin user
   Description:
   This user will have write level access to the application. Users will be able to create configurations, upload plugins, configure sharing and edit settings.
   Admin users will not be able to create new users.
3. Read only user
   Description:
   The read-only user will have limited access to the application. This user will not be able to perform any edit/update action on plugins and their configuration and settings.

Page will display all the current users in the table. Users can be edited or deleted from here.



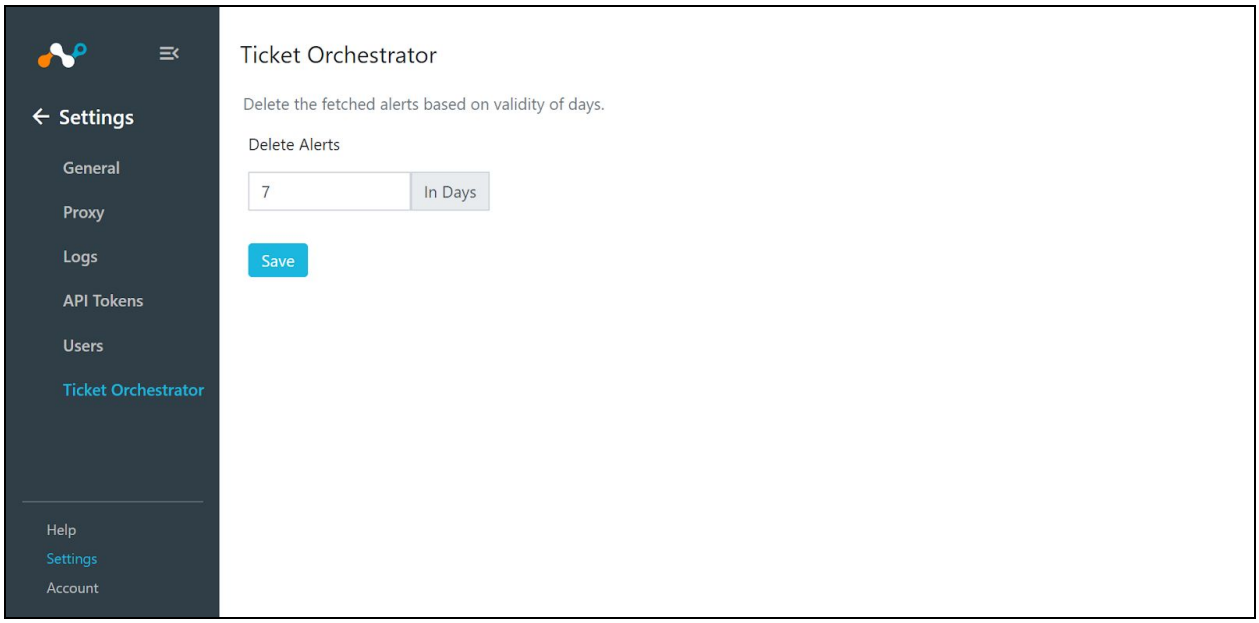
New users can be created by clicking the add user button. Form will be displayed to create a user.

Field	Description
Username	Username associated with this account.
Password	Initial password for the user. User will be prompted to change password after first login.
User Role	Two roles Admin and Read only can be assigned to the user.
API Access	Checkbox to give user API access and to generate API token.



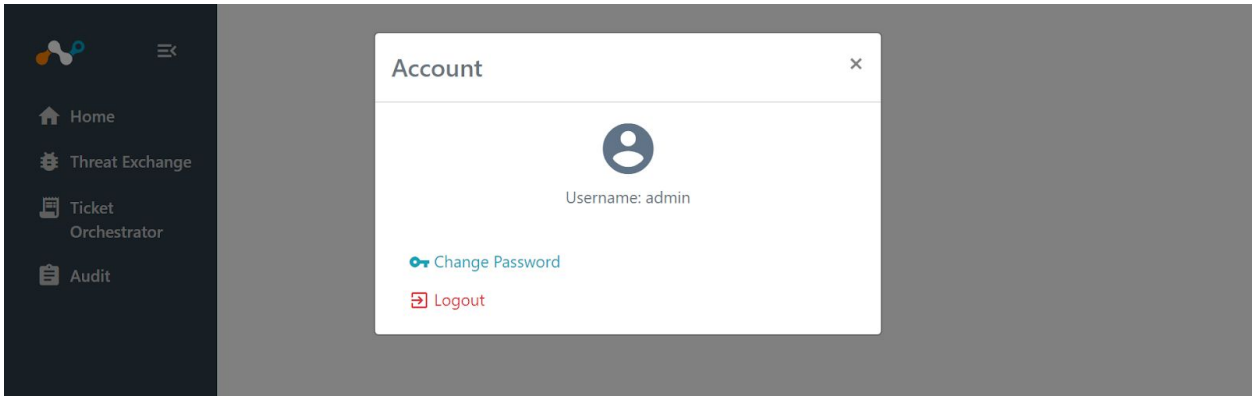
2.8. Ticket Orchestrator

This option is only available when the CTO module is enabled. User can configure periodic deletion of the fetched alerts' age in days.



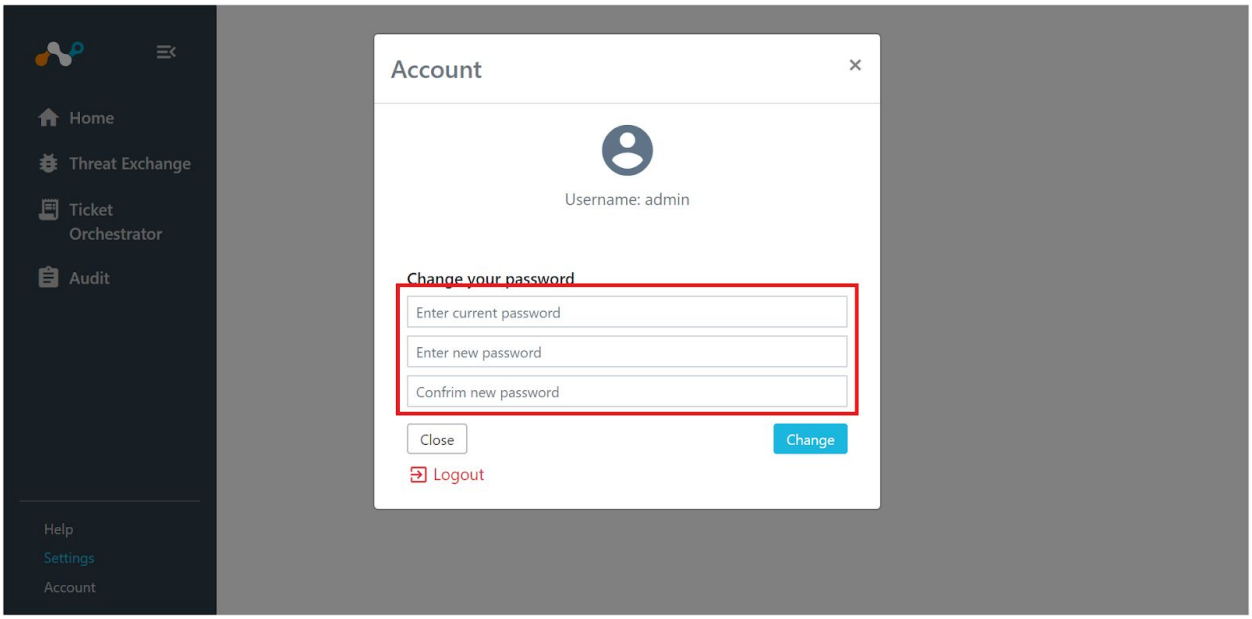
2.9. Account Settings

Users can change the password and logout from Account settings. Account Settings option is available on the bottom section of the Left hand navigation module.

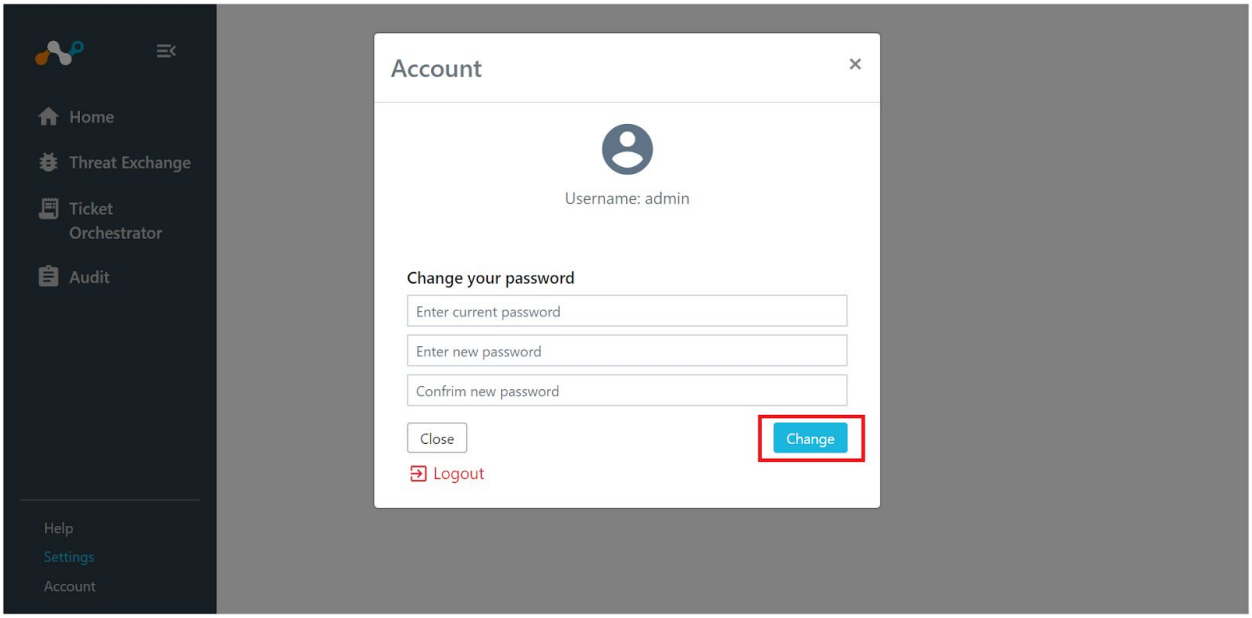


2.9.1. Change Password

1. Using this option the user can change the password of the account.
2. While the user clicks on the change password option, there will be three fields available current password, new password and confirm new password.

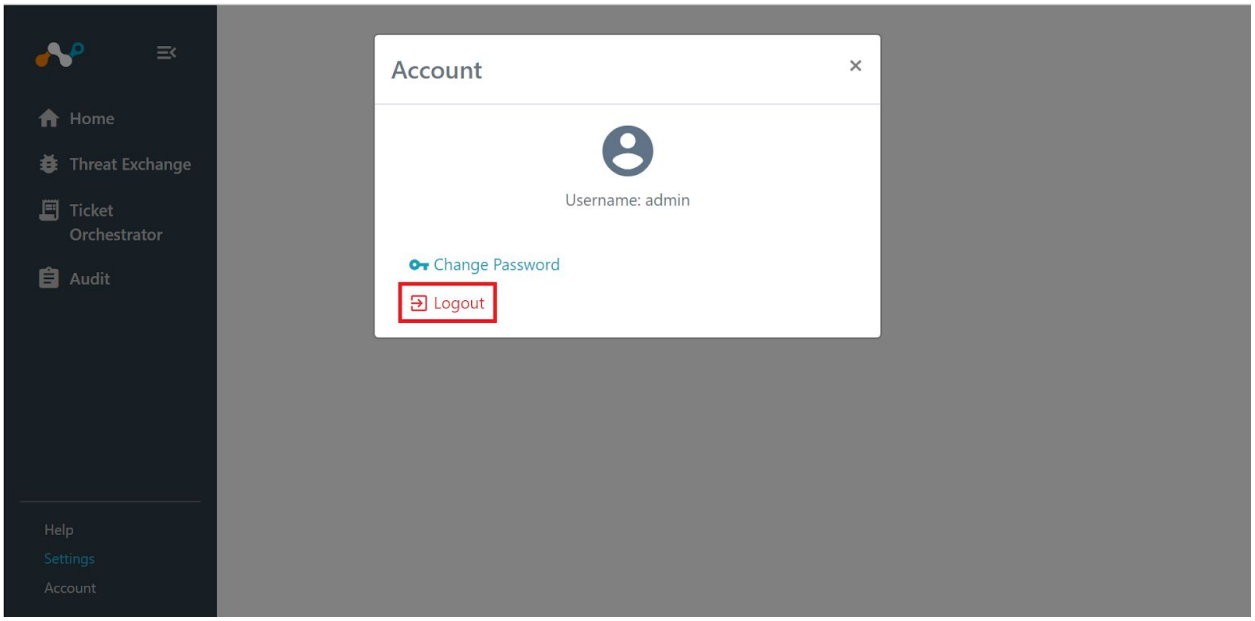


3. After the user adds all the details correctly and clicks on the Save, portal password will be changed and user will be logged out.



2.9.2. Logout

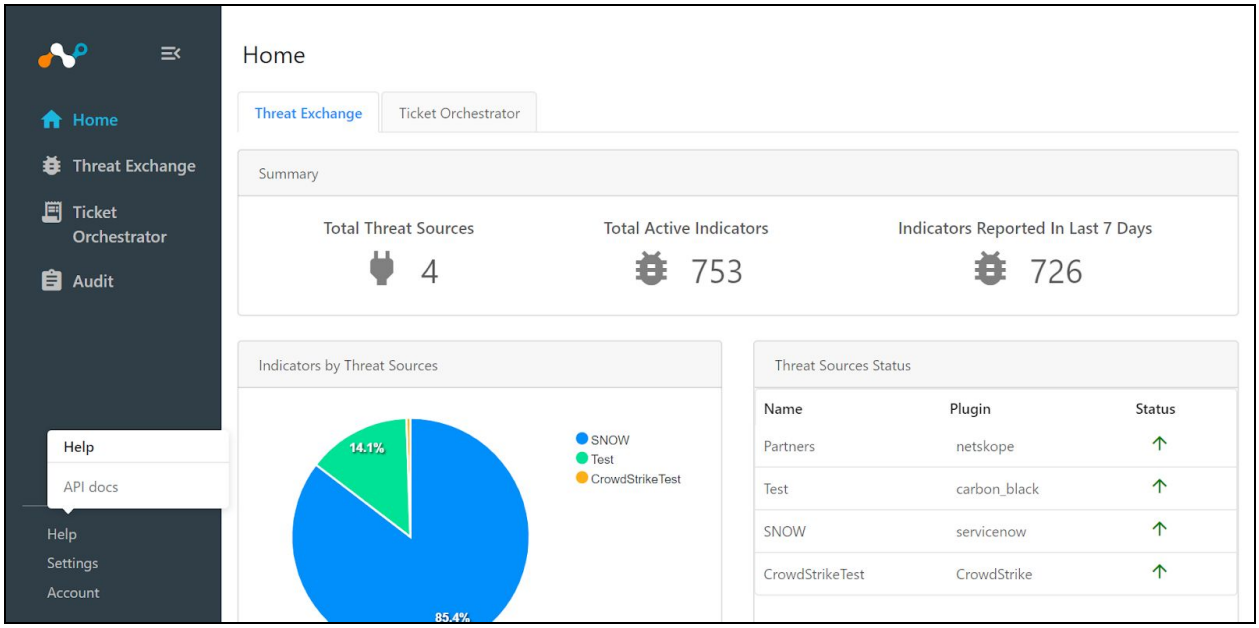
By clicking on this option the user can logout from the portal and login option will be available.

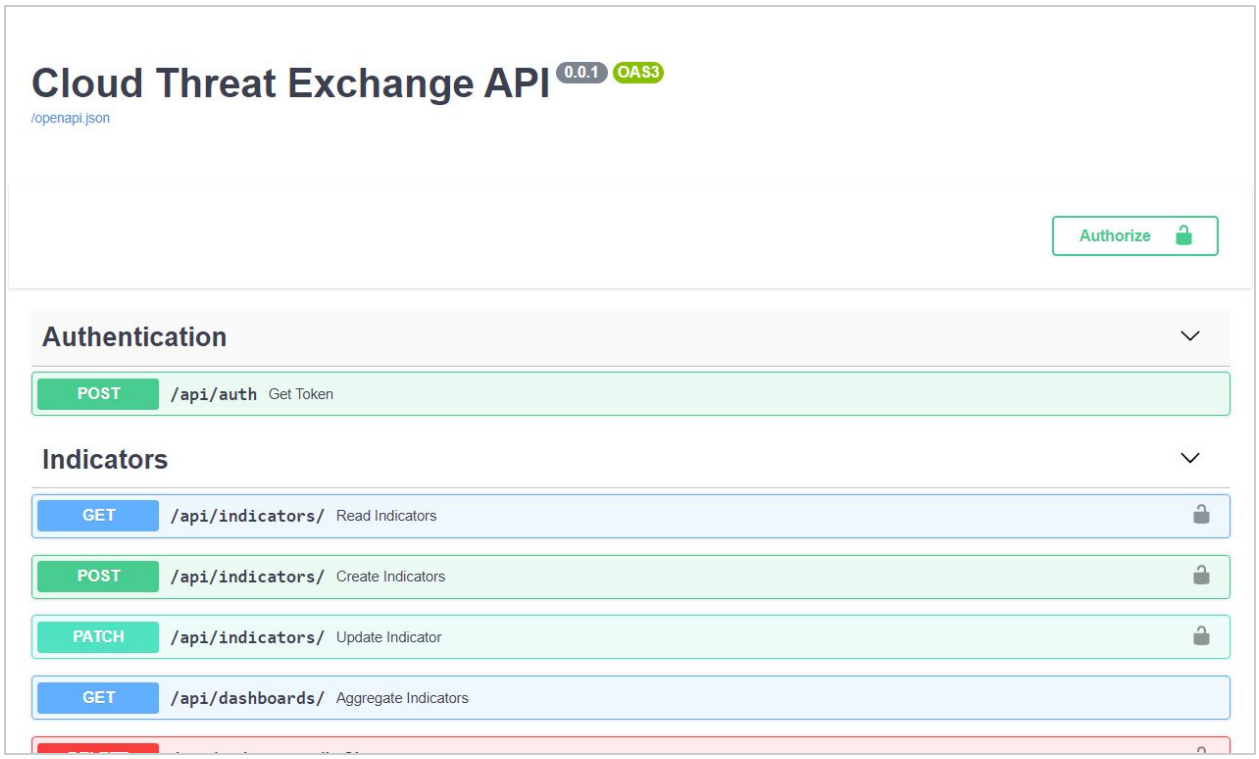


2.10. Help

2.10.1. API Docs

API documentation can be accessed from this link. Users who have API access will be able to see this link.



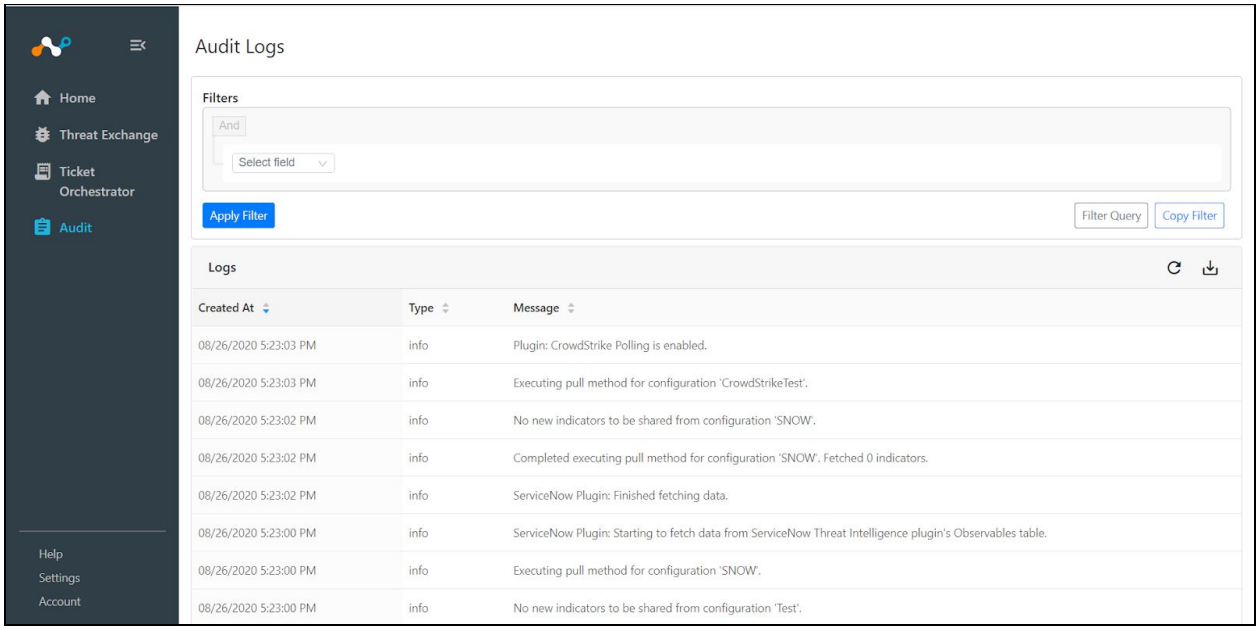


2.11. Audit logs

Audit log is journaling of significant events that occurred during the operations of Netskope CTE. Logs provide important information to troubleshoot any abnormal behavior of the system.
The audit logs can be searched through CTE UI and user can export the logs to the local system.

Role required : admin, read-only

1. Login to Netskope CTE and navigate to Audit Menu.
2. Logs entries are listed. By Default, log entries are sorted in descending order of occurrence.



3. Filters can be set to filter out specific log entries. The filter parameters are listed below:

Field	Description	Filter operators
Created At	Time at which log is created.	!=, <, >, >=
Type	Log type (info, warning, error).	any in, not in operator (Multiselect)
Message	Log message.	Is equal and contains (Regex also supported).

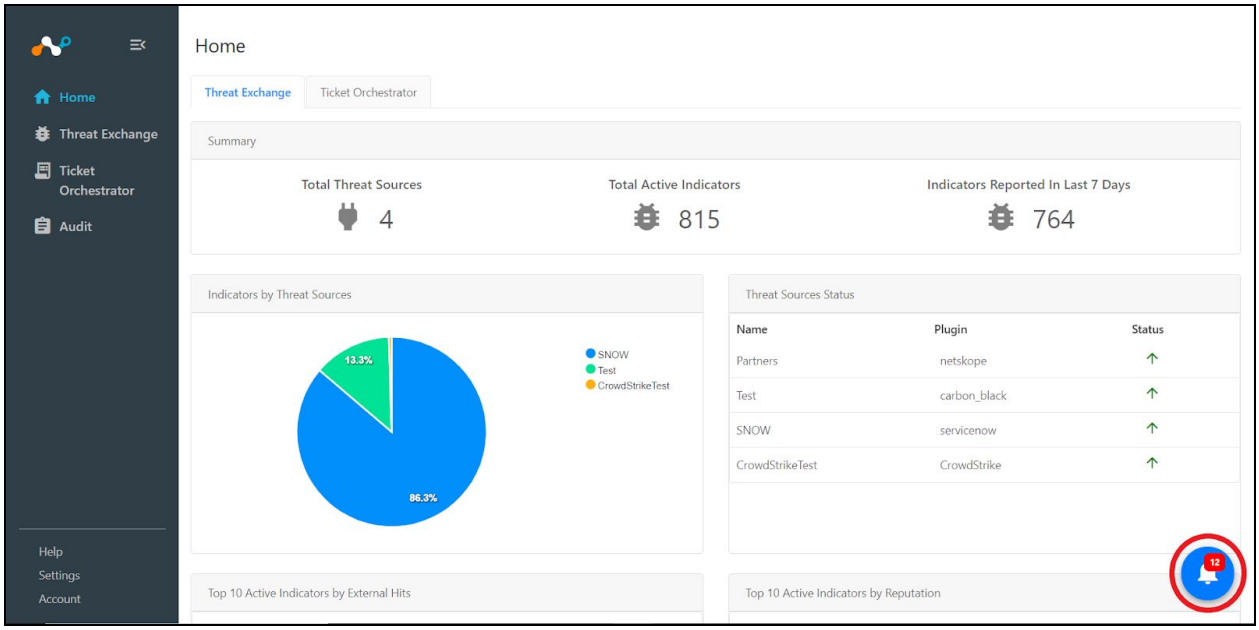
Users can also export the logs by clicking the Export button. Existing data (filtered and sorted) data will be exported to the cte.log file.

2.12. Notifications

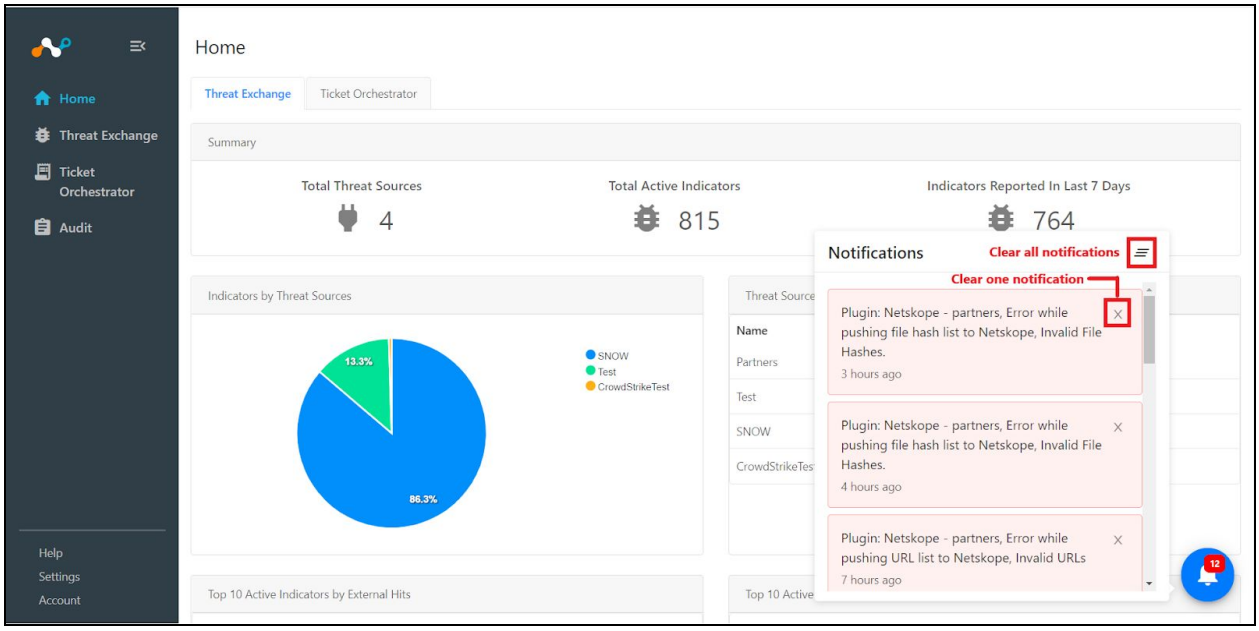
The Netskope CTE performs lot of tasks in background and the user need some mechanism to be alerted in case of anomalies.

Role required : admin (to clear notifications), read-only (to view notifications)

1. Whenever active notifications are available, a floating bell icon appears on all the UI pages. This bell icon appears in the bottom right part of the screen.
2. The bell icon also displays the count of open notifications. Maximum of 100 open notifications are displayed. To view the older notifications, clear the currently visible notifications.



3. Click on the bell icon and a pop-up appears with a list of notifications. There are 3 levels of notifications INFO, WARN and ERROR. These levels can be differentiated by color.
4. Admin user can clear a particular notification and clear all notifications as well. Clear All notifications would clear the currently displayed 100 notifications.



3. Operations

This section provides useful information for the administrator who is going to manage the CTE infrastructure.

Access required : System Administrator with SSH access to the server on which the CTE platform is installed.

3.1. Reset Password

To reset the admin password perform the steps shown below on the machine that is running the docker containers.

1. Enter the mongodb docker container.
   > docker exec -ti mongodb sh
2. Login to the mongodb client. Enter the value of the MONGO_PASSWORD environment variable (from docker-compose.yml) when prompted for a password.
   > mongo --username cteadmin
   > Enter password:
3. Switch to the cte database.
   > use cte
4. Type in the following line to reset admin password.
   > db.users.update({username: "admin"}, {$set: {password: "$2y12RBcV6xWFhHucm4a1YRmQXuEZHqz9NadpMuzIB6xEIXOhg.QzngiiO"}});
5. admin password should now be reset to default.
6. Login to the Netskope UI with default password and change the password of your choice.

3.2. Logs cleanup

To remove the log files perform the steps shown below on the machine that is running the docker containers.

1. Enter the core docker container.
   > docker exec -ti core sh
2. Remove log files.
   > rm -f /logs/celery /logs/celery-beat /logs/gunicorn /logs/rabbitmq
3. Restart the core container.
   > docker-compose restart core

To remove the logs from the database perform the steps shown below on the machine that is running the docker containers.

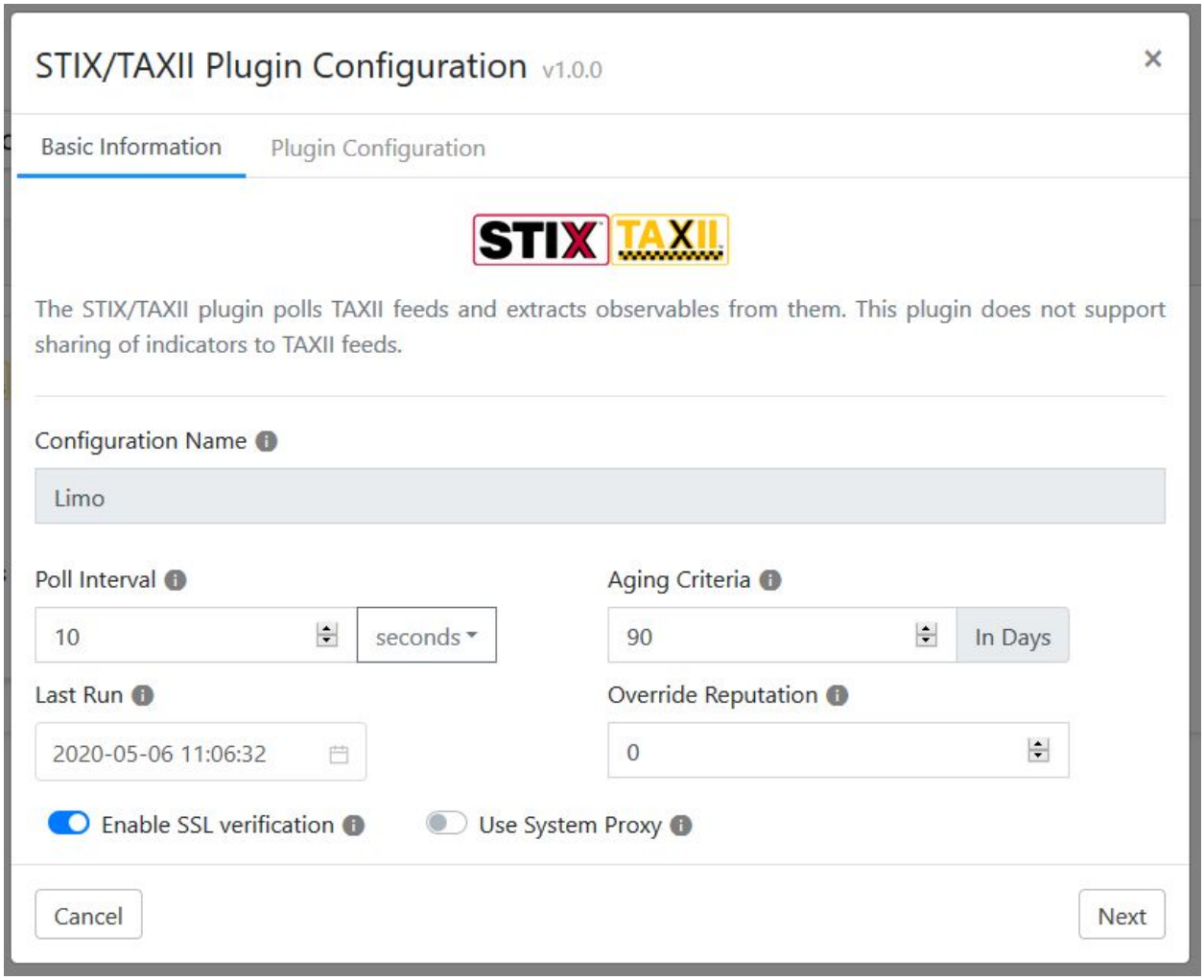
1. Enter the mongodb docker container.
   > docker exec -ti mongodb sh
2. Login to the mongodb client. Enter the value of the MONGO_PASSWORD environment variable (from docker-compose.yml) when prompted for a password.
   > mongo --username cteadmin
   > Enter password:
3. Switch to the cte database.
   > use cte
4. Remove the logs.
   > db.logs.remove({})

Note : Version 1 of the platform doesn't support auto log rotation. This feature will be addressed in future releases.

3.3. Update Plugin Configuration Checkpoint (Last Run time)

To fetch historical data for an existing configuration, the checkpoint has to be manually updated. Starting from version 2, you can do this from the UI.

To do this, goto Configurations and edit the configuration you want to modify the checkpoint of. Update the Last Run value to some historical date-time and save the configuration. The next time this configuration runs, data should be fetched from that particular date-time.



3.4. Migrating from Cloud Threat Exchange to Cloud Exchange

If you want to preserve your existing data (indicators, plugin configurations) while migrating from CTE to the latest Cloud Exchange Platform which includes both CTE and CTO then you need to follow the steps listed below.

1. Make sure you **do not remove the mongodb** container. To prevent accidentally deleting the mongodb container and only update ui and core containers, delete them by name.
   > docker-compose rm core ui
   > docker-compose pull core ui
2. To run the migration script, follow the following steps:
   a. Copy the script into the docker container.
      > docker cp migration.py core:/opt/netskope
   b. Execute the migration script inside the container.
      > docker exec python /opt/netskope/migration.py

Troubleshooting & FAQs

This section provides information about common problem statements and suggested solutions.

1. Although sharing is configured, the IoCs reported are not being shared with the threat source.

   While sharing the IoCs to a particular plugin, the sharing filters provided with the plugin's configuration are considered. Ensure that the sharing configuration matches with the IoCs you are expecting to be shared. If the sharing filter is incorrect, fix the sharing criteria. To fetch the historical data that you may have missed due to mis-configuration, consider removing the sharing configuration and re-adding it.

2. Can I create new users apart from the OOB users?

   See Users.

3. How can I configure SSL certificates to serve requests over HTTPS?

   Refer to the 5th point of the Installation Steps.

4. Where are all the uploaded plugins stored?

   By default, all the user uploaded plugins are stored inside the ./data/custom_plugins directory. However, this can be changed from the docker-compose by mounting a different directory.

5. How to reset the user password if the current password is forgotten?

   To reset the administrator password refer to the Reset Password mentioned in the Operations section. Make sure to change the password from Account Settings after the CTE administrator has reset the password.

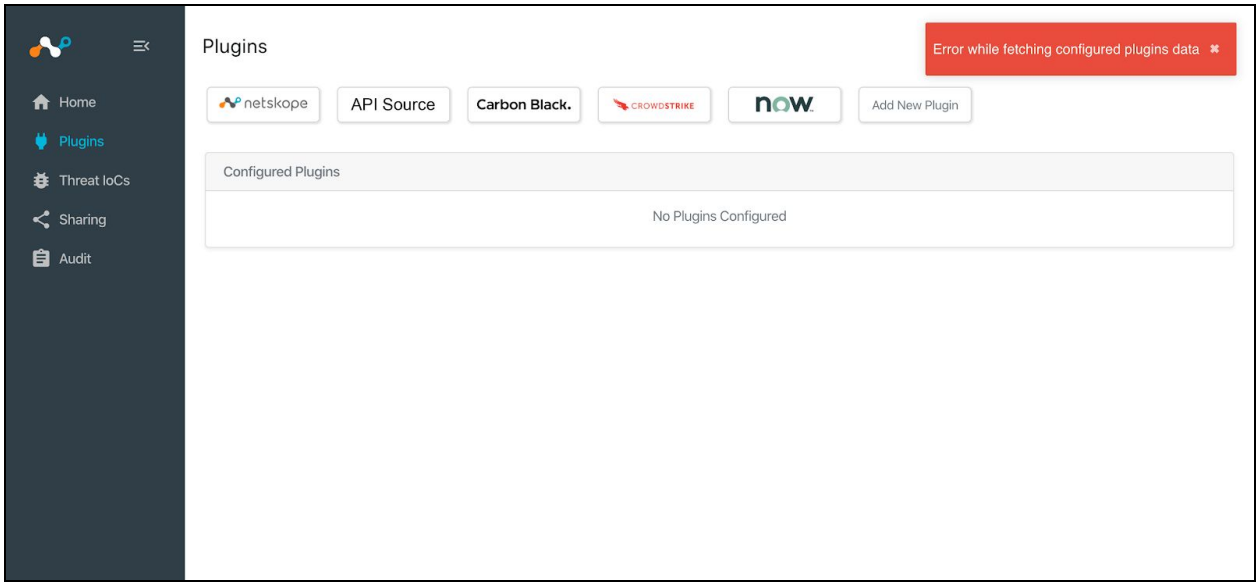
   To reset any other user's password, the "admin" user can update the user password from the Settings > Users section and click the Edit icon on right.

6. The IoCs search performance is slow. It takes more than 5 seconds to load results.

   The platform by default searches for the last 7 days of IoCs. If there are too many IoCs(more than 1 million) and no filter selected, the search performance would be slow.

   Proposed solution : Consider applying the filters and narrowing the search criteria. The performance is very good if the data set is ~100K records.

7. After upgrading/restarting the core and ui containers, the plugin configurations are not visible.



Verify if you uploaded a custom plugin with active configuration to Netskope CTE prior to upgrading the containers or restarting the containers. In such a case, upload the custom plugin(Refer Upload a new Plugin) after up. The configurations would be retained after uploading the custom plugin and normal operation is restored.

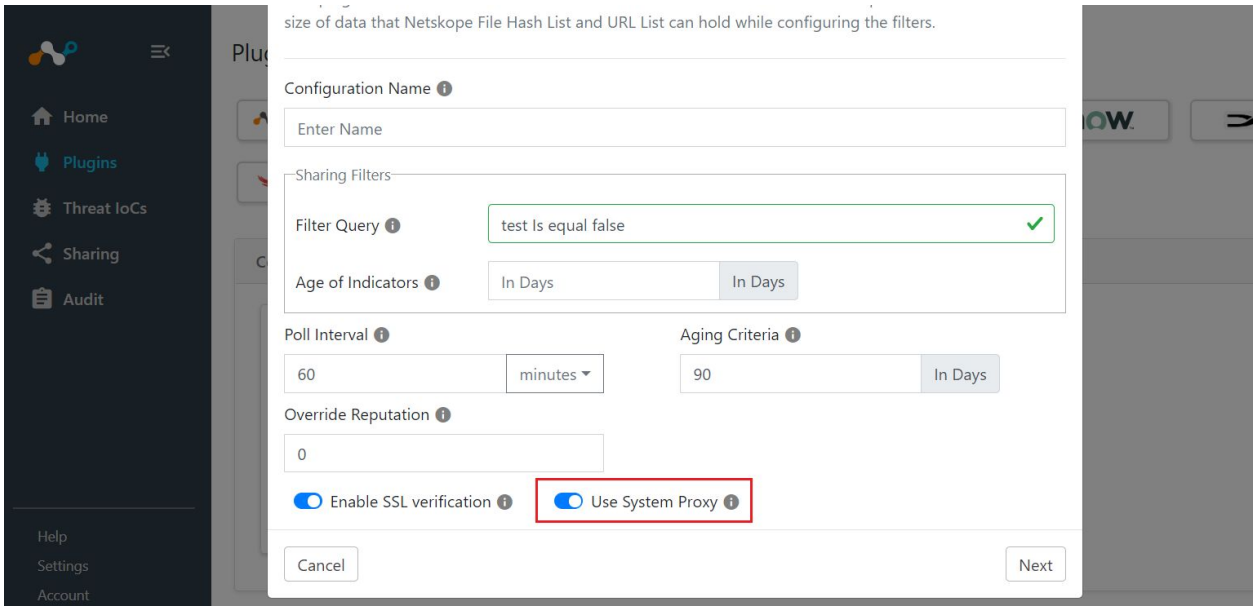
8. While configuring a new plugin, even after providing accurate credentials the configuration is not saved and error message is displayed.

Verify if the outgoing API calls require Proxy. If your network deployment expects proxy for HTTP

API calls and proxy is configured, the plugin operations would be impacted.

Proposed Solution:

- Configure the Proxy.
- Configure the Plugin with “Use System Proxy” setting enabled. Edit the existing configuration and enable “Use System Proxy” setting.

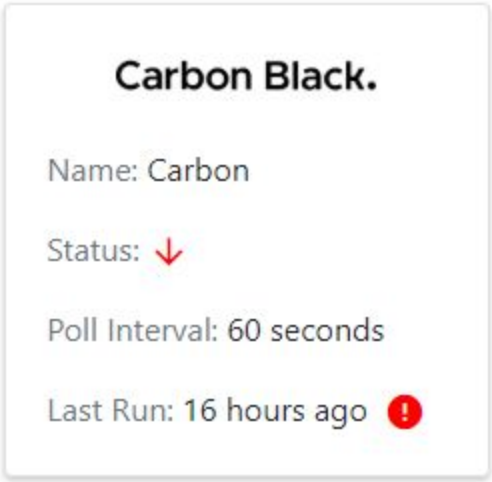


9. Although the Poll interval for a plugin is configured to poll every 5 minutes, the Last Run shows an interval which is more than 5 minutes ago.

   The Netskope CTE relies on an internal scheduling mechanism for the plugin's task. There are workers which execute the plugin tasks, by picking up a task from the queue one by one. The number of workers available in your system depends on the number of cores. If the available workers are busy serving plugin task, the already queued up task has to wait till the existing worker is available. This situation may usually occur during initial data ingestion, where there's more data to be processed.

   Proposed Solution : Consider increasing the cores of the system if number of configured plugins is more and the configured plugins are consistently lagging behind. For initial ingestion case, the system should pick up the backlog post initial ingestion and behave normally considering the incremental data is not large.

10. Plugin configuration shows a red alert icon similar to the image shown.

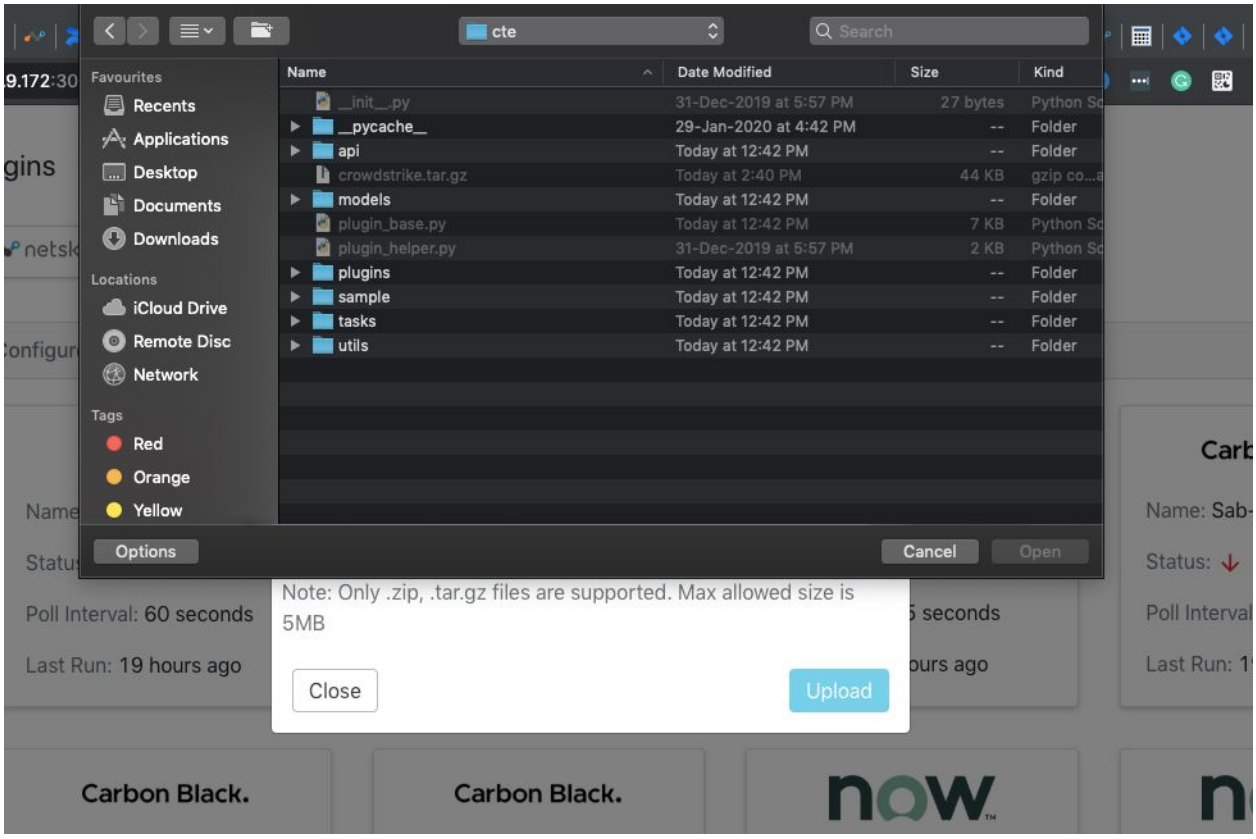


If there is a red alert icon on one of the configurations, it indicates that there was some problem while polling the data for that configuration. This could be related to API, proxy or SSL.

Proposed Solution:

- Make sure the Plugin Configuration has all the parameters like API and Secret key, URL etc correct.
- Make sure enable proxy is selected and proxy is configured if outbound network calls require a proxy connection.
- Check for the error logs made around the last run time displayed on the configuration from the Audit section.

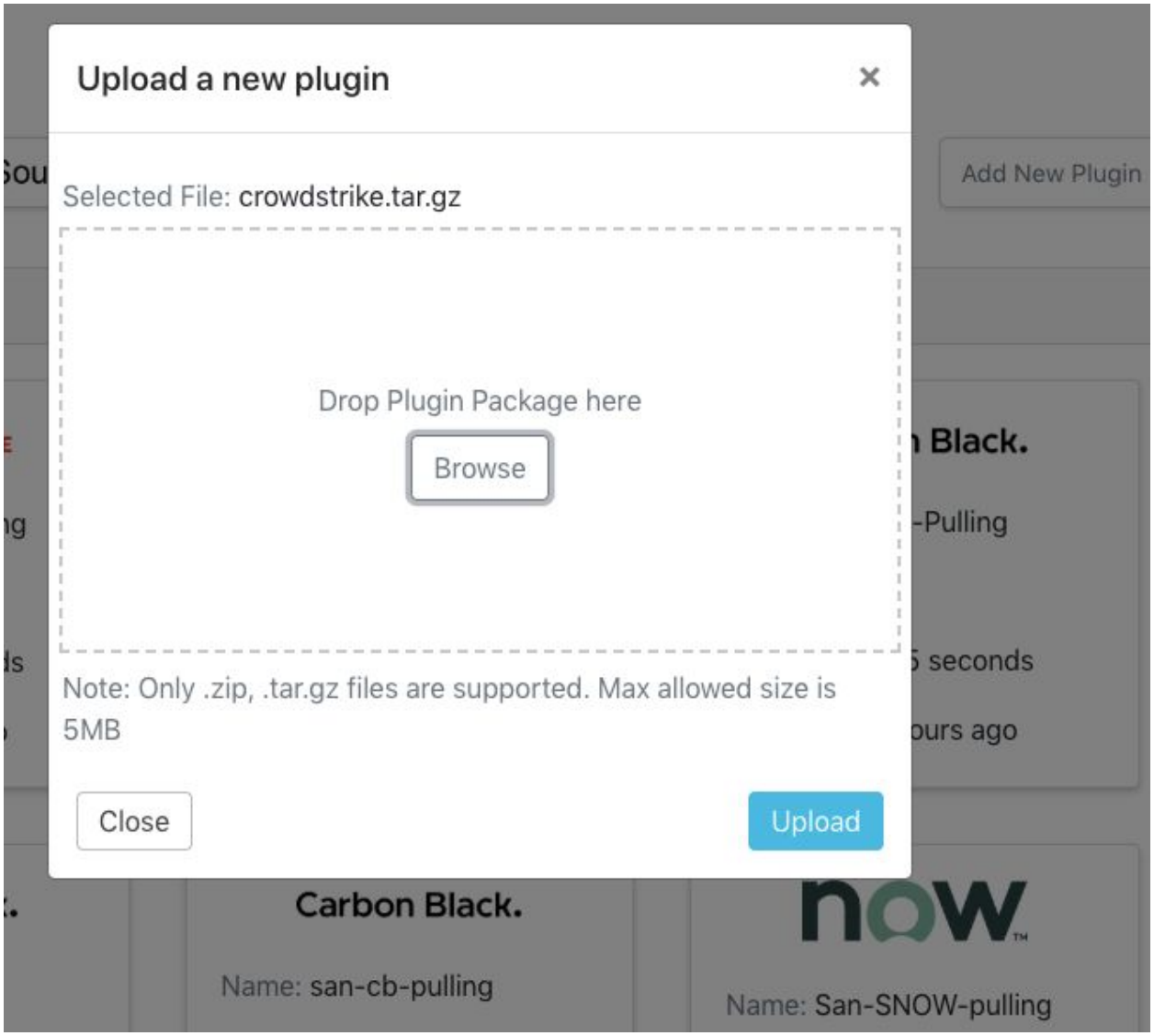
11. Mac OS users cannot select tar.gz while uploading a custom plugin.



When a user tries to upload a plugin with tar.gz package with browse button tar.gz files are not selectable by default.

Proposed Solution:

- Users can drag and drop plugin packages to the drop area of upload plugin UI.



12. How to update the last run time of a plugin configuration. This is to replay the indicators in case they are missed due to some issue.

    Open the plugin configuration and set the “Last Run” value to an older date-time and save the configuration. Make sure that the configuration is currently not running when you update the Last Run value.

13. What kind of indicators are extracted from STIX/TAXII sources?

    For STIX 1, the cybox observables of type URI, Domain, SHA256 and MD5 are extracted.
    For STIX 2, the same type of observables are extracted from the pattern string field of the indicators.