Illumio Plugin for Netskope CTE

User Guide v0.1.0

# Overview

This document explains how to install, configure, and use the Illumio plugin for Netskope Cloud Exchange.

The Illumio plugin retrieves workloads within a configured policy scope and creates Netskope Threat IoCs for all interfaces on each workload. The IoCs can then be used for granular access control to workloads that are not managed by Illumio policy.

# Prerequisites

To complete the plugin configuration, you’ll need:

* A Netskope Cloud Exchange instance with the [Threat Exchange module enabled](https://docs.netskope.com/en/configure-the-netskope-plugin-for-threat-exchange.html)
* An Illumio Policy Compute Engine (PCE) version 21.2 or higher
* Labelled PCE Workloads within the defined policy scope

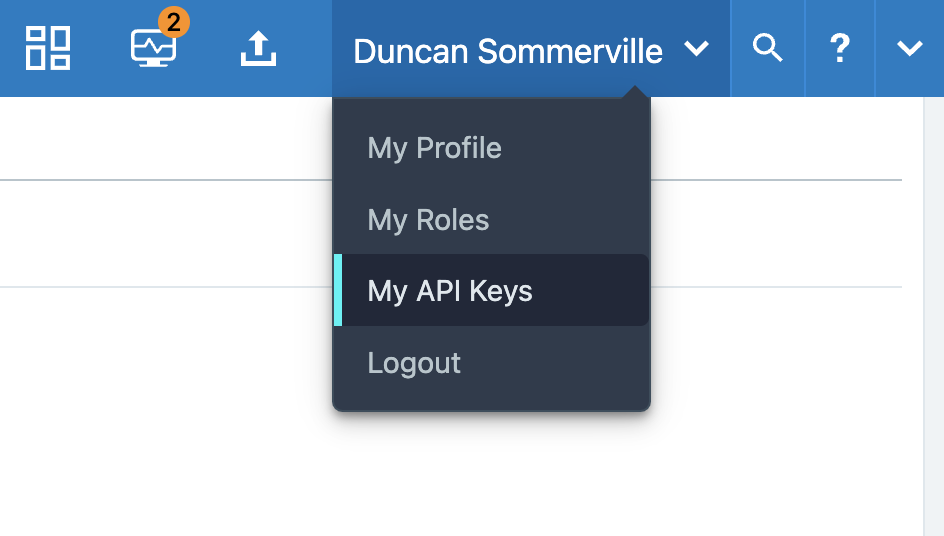
The Netskope CE server must be able to access the PCE over HTTP/S, optionally via proxy.

# Workflow

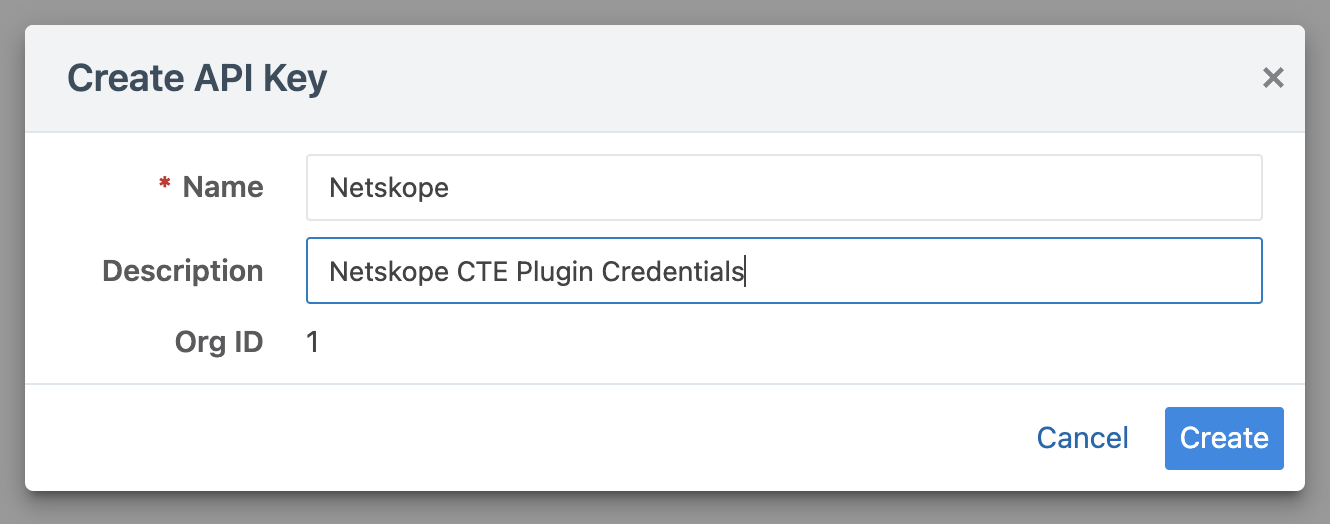
1. Create an API key on the PCE
2. Configure the Illumio plugin
3. Confirm the plugin is working

## Create an API Key on the PCE

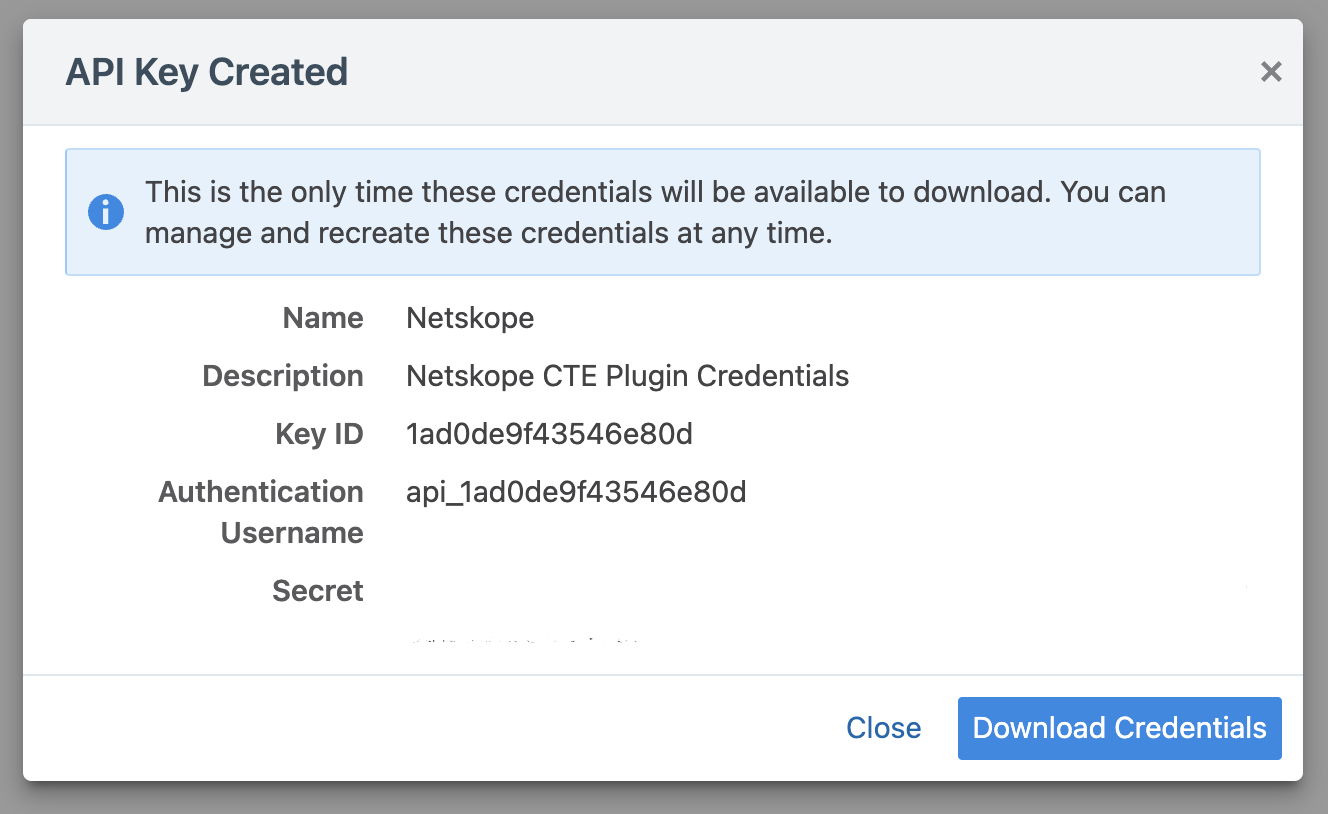
1. On the PCE, select My API Keys from the User dropdown in the top-right corner.



1. Click the **Add** buttonat the top-left of the page and enter a name and optional description for the API key. Note down the Org ID as you will need it when configuring the plugin.

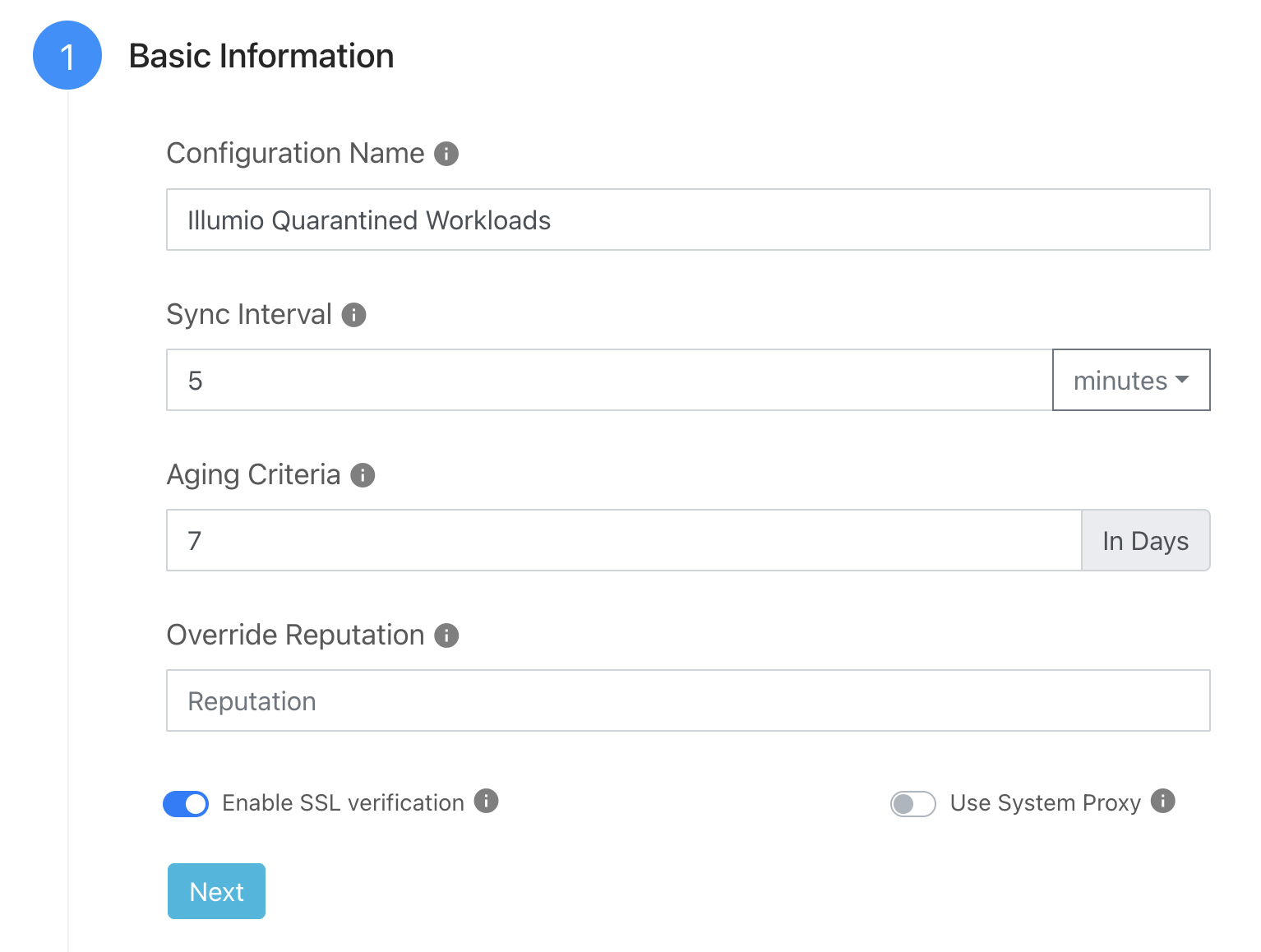


1. Click **Create** and note down the API key Username and Secret as these will be used by the plugin to authenticate to the PCE API. Optionally, download the credentials and store them in a secure location.

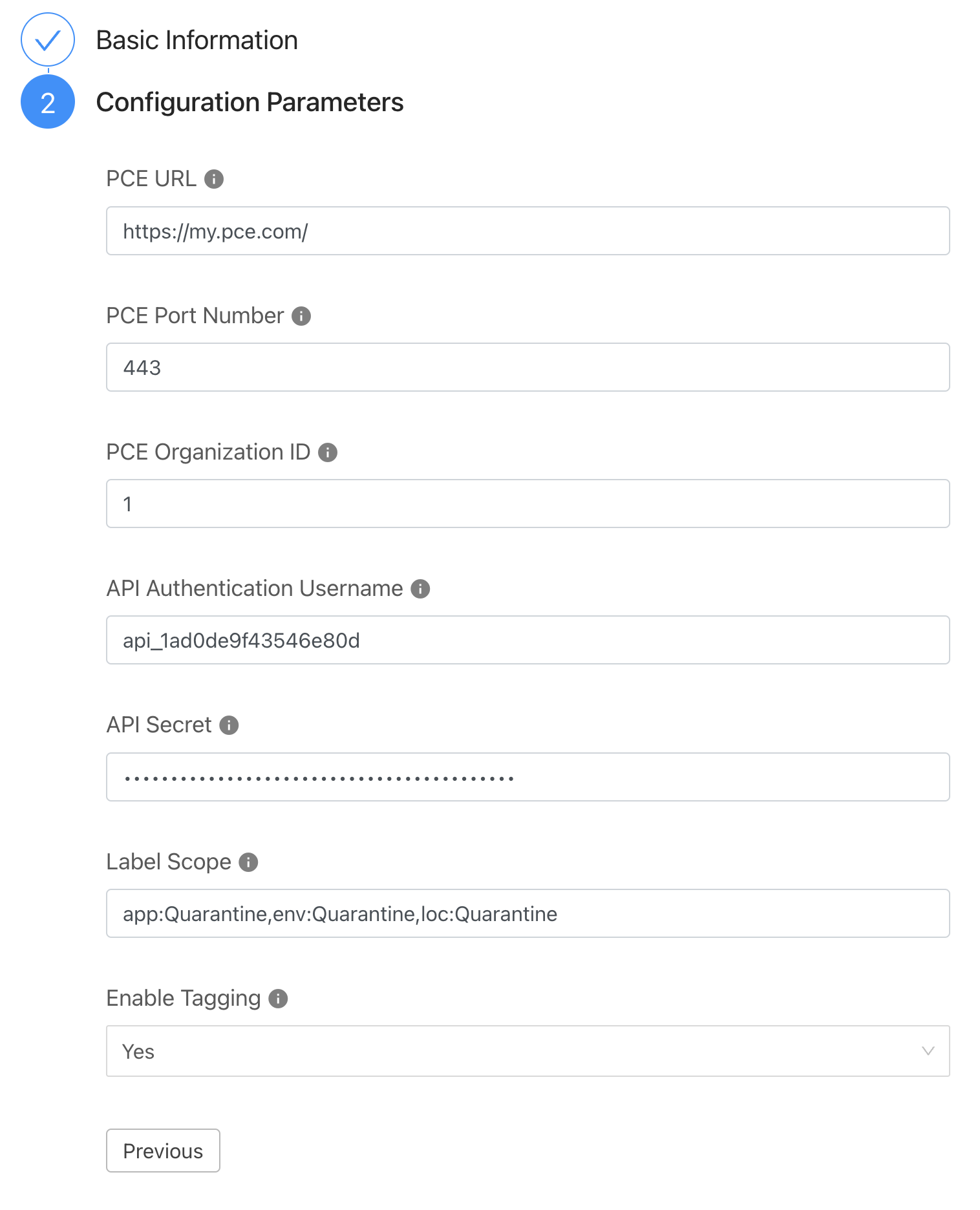


# Configure the Illumio Plugin

1. In Cloud Exchange, navigate to Settings > Plugins.
2. Find the Illumio plugin tile and select it to navigate to the plugin configuration page.
3. Fill out the basic information page for the instance:
   1. *Configuration Name:* Enter a valid name for the plugin instance (alphanumeric and spaces)
   2. *Sync Interval:* Adjust the resync interval for the instance.
   3. *Aging Criteria:* Adjust the expiration time for the Threat IoCs created by the plugin.
   4. *Override Reputation:* Optionally set the reputation values for Threat IoCs created by the plugin.
   5. *Enable SSL verification:* Toggle TLS certificate verification when connecting to the PCE.
   6. *Use System Proxy:* Toggle the use of the HTTP/S proxy configured in Netskope when connecting to the PCE.



1. Click **Next**.
2. Fill out the configuration parameters for the instance:
   1. *PCE URL:* Enter the PCE FQDN. You can optionally include the scheme.
   2. *PCE Port Number:* Enter the port number the PCE cluster is listening on. Defaults to 443.
   3. *PCE Organization ID:* Enter the Org ID shown when creating the API key.
   4. *API Authentication Username:* Enter the API Username for the key created above.
   5. *API Secret:* Enter the API Secret for the key created above.
   6. *Label Scope:* Enter a comma-separated list of label keys and values separated with colons. For example: *app:Quarantine, env:Quarantine, loc:Quarantine*
   7. *Enable Tagging:* Toggle whether Netskope tags will be created for labels on Workloads within the defined scope.



1. Click Save in the top-right corner of the page to create the instance. The configuration will be validated, and the plugin will test the connection to the PCE. The configured instance can now be viewed under **Threat Exchange > Plugins**.

# Confirm the Plugin is Working

1. Once the plugin runs, verify that Threat IoCs are being created for the Workloads within the defined scope.
2. On the PCE, navigate to the Workloads page and narrow the filter to the Label Scope configured for the plugin.

A screenshot of a computer

Description automatically generated with medium confidence

1. In Netskope CE, navigate to **Threat Exchange > Threat IoCs** and narrow the filter to just Illumio Workload entries. This can be done by searching for “Illumio” in the IoC Comments field, as shown below.

A screenshot of a computer

Description automatically generated with medium confidence

1. The Workloads within the configured scope should have IoCs created for their hostnames and interface addresses.