Netsurion®
Powering Secure and Agile Networks

How to - Guide

How to – Configure Cisco Umbrella OpenDNS to forward logs to EventTracker

EventTracker v9.x and above

Author: Marketing

April 5, 2021

Abstract

This guide provides instructions to configure/ retrieve Cisco Umbrella OpenDNS activity logs such as, DNS, proxy, firewall, or IP via REST API method.

Scope

The configurations detailed in this guide are consistent with EventTracker version v 9.x or above and Cisco Umbrella OpenDNS.

Audience

Administrators who are assigned the task to monitor Cisco Umbrella OpenDNS events using EventTracker.

Table of Contents

1. Overview

Cisco Umbrella OpenDNS service is a cloud-based domain name resolution service with added features like content filtering, anti-phishing, anti-malware, and anti-ransomware. This is designed to prevent any advance persistent threat from attacking a network with malicious content.

EventTracker helps to monitor events from Cisco Umbrella OpenDNS. EventTracker flex reports, alerts, and dashboards will help you to analyze the activity logs such as, DNS, proxy, firewall, or IP.

2. Prerequisites

2.1 Integrating OpenDNS Security Activities

- EventTracker agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run powershell.
- Admin access to OpenDNS platform.

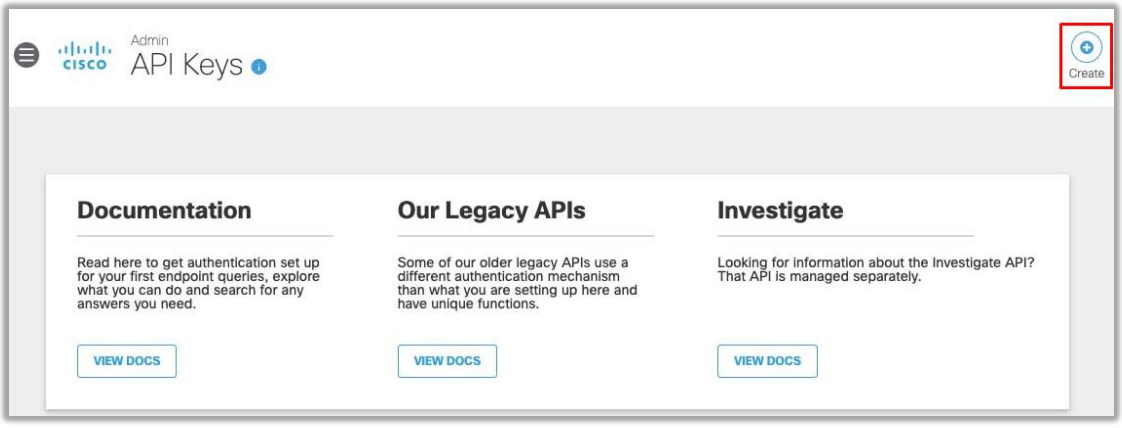
3. Configuring OpenDNS to forward logs to EventTracker

3.1 OpenDNS Security Activities

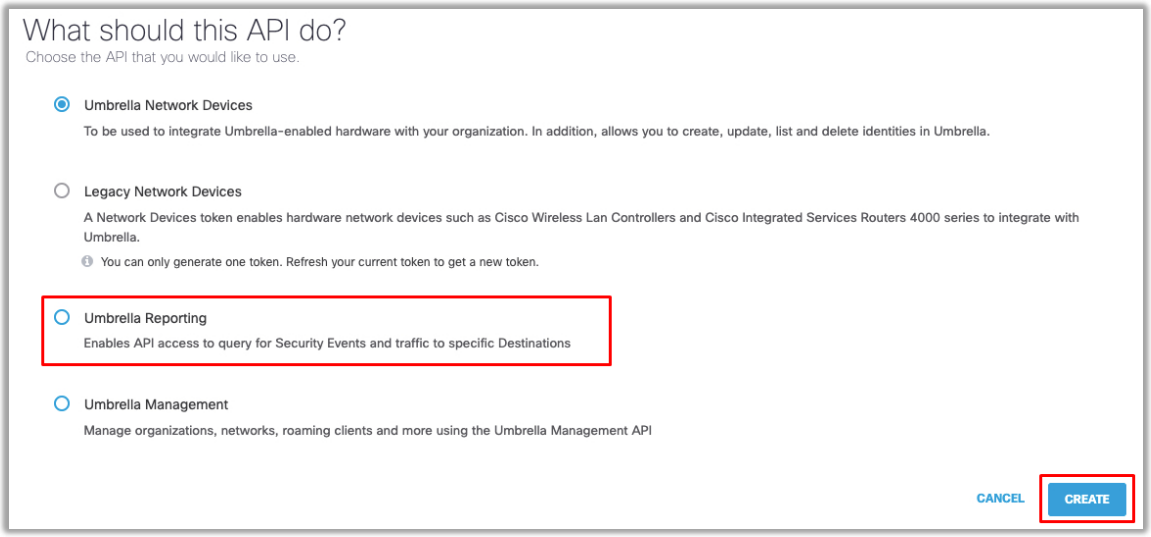
The steps provided below will help to configure the EventTracker to receive specific events related to DNS, proxy, firewall, or IP from Cisco Umbrella OpenDNS.

3.1.1 Collecting Open DNS, API Key and API Secret, and Organization ID

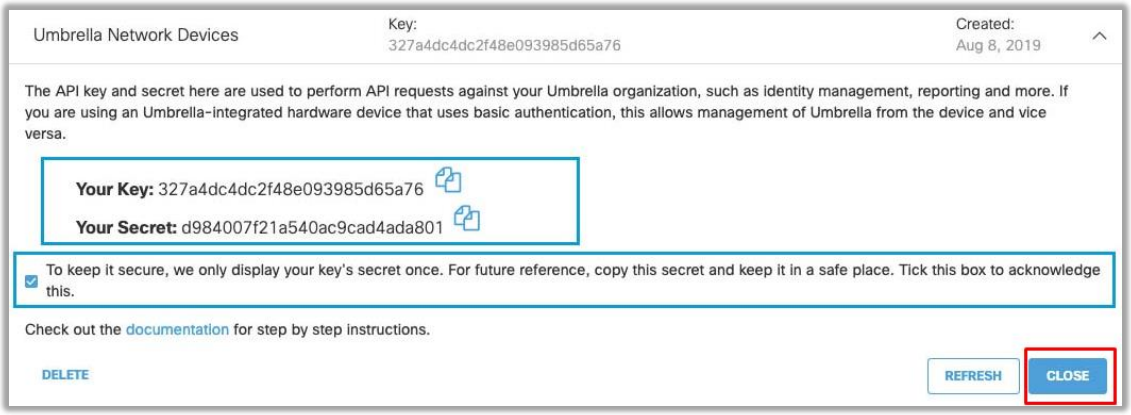
1. An organization ID can also be obtained directly from the Umbrella dashboard after you log in to that organization, as it will be in the URL of your browser: https://dashboard.umbrella.com/o/{organizationId}/#/overview
2. In the Umbrella dashboard for the organization, navigate to **Admin > API Keys** and click **Create**.



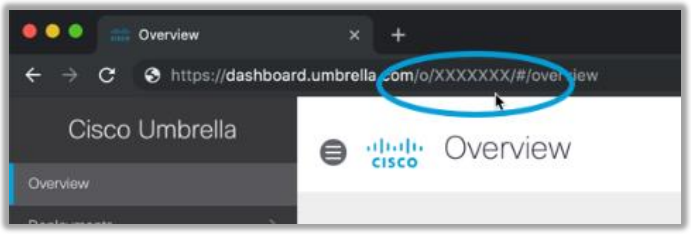
3. In the **What should this API do?** section, select **Umbrella Reporting**, and then click **Create**.



4. The **key** and **Secret display**. Enable the option to Acknowledge and click **Close**.



5. To generate a new key & secret, you can either click the refresh button on your existing key & secret or delete the existing key & secret and then create a new key & secret pair.
6. To Collect **Organization ID**, check the URL in the address bar (Once you are logged in to the correct org), the URL should be like:

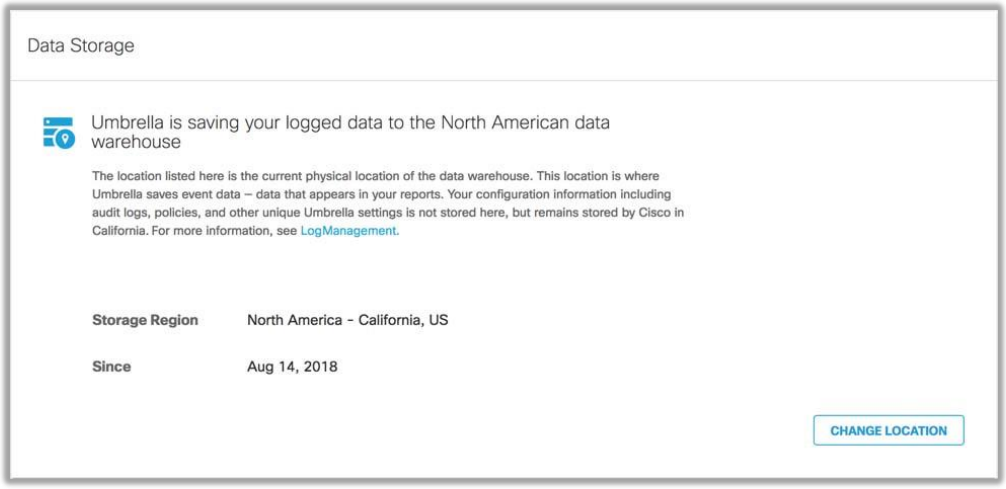


3.1.2 Verifying API region

Cisco Umbrella's data warehouse is the virtual location where your instance of Umbrella stores its event data logs. By default, Umbrella saves your event data logs to Cisco's California location.

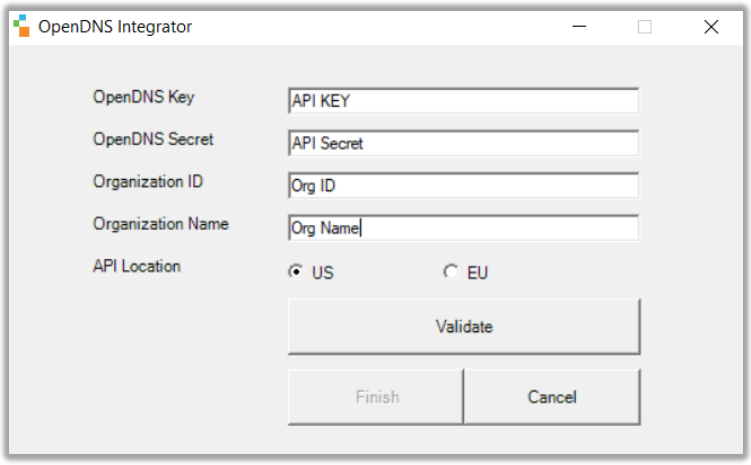
To verify you OpenDNS data warehouse's location, perform the below steps:

1. While you are still in Umbrella console, Navigate to **Admin > Log Management** > **Data Storage. Look for "Storage region":**



3.1.3 Configuring EventTracker OpenDNS Integrator

1. Get the **OpenDNS Integrator** executable file: https://downloads.eventtracker.com/kp-integrator/OpenDNSIntegrator.exe
2. Once the executable application is received, right click on the file, and select **Run as Administrator**.
3. In the dialog box, enter your Cisco Umbrella **OpenDNS API key, Secret, Organization ID** (can be collected from OpenDNS GUI), **Organization Name,** and the **API Location**; and click on the **Validate** button to verify the credentials.



4. On successful verification, a pop window will appear with a message: **Credential Validated Successfully**.
5. Click on the **Finish** button to complete the integration process.

3.2 Error Codes

HTTP Status Code	Error	Explanation
200	OK	Successful request
400	Validation error	Some field or property has not been filled out correctly
401	Unauthorized or Invalid authentication credentials	The authorization header is missing or the “key: secret“pair is invalid
403	Forbidden	Verify the endpoint
404	Resource Not Found	Verify the endpoint and any input field data
429	API rate limit exceeded	Wait before submitting another request
500	Error- This request could not be processed by the server	Try again later or contact support.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.
Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.
Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters
Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers
713-929-0200

https://www.netsurion.com/company/contact-us