Use Umbrella Reporting API via Postman

Contents

Introduction

This document describes how to use the Cisco Umbrella Reporting API in Postman.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The Umbrella API was released in September 2022, providing a user-friendly and secure platform that enables users to build on, extend, and integrate with Umbrella.

The Umbrella API endpoints are hosted on api.umbrella.com, with grouped paths per use case. API keys can be managed both in the Umbrella dashboard, under **Admin > API keys**, and programmatically with the KeyAdmin API. Each key can be granularly configured with multiple scopes grouped under five primary use cases:

- Admin API endpoints enable you to provision and manage Umbrella API keys and users, view roles, and manage customers for providers and managed providers.
- Auth API endpoints enable you to authorize other services' integrations with the Umbrella platform.
- Deployments API endpoints enable you to provision, monitor and manage networks and other various entities, and secure them by configuring them in your existing Umbrella policies.
- Policies API endpoints enable you to provision and manage destination lists and the destinations per

list.
- Reports API endpoints enable you to read and audit real-time security information about your deployments. The Umbrella App Discovery API provides insights into your cloud-based applications.

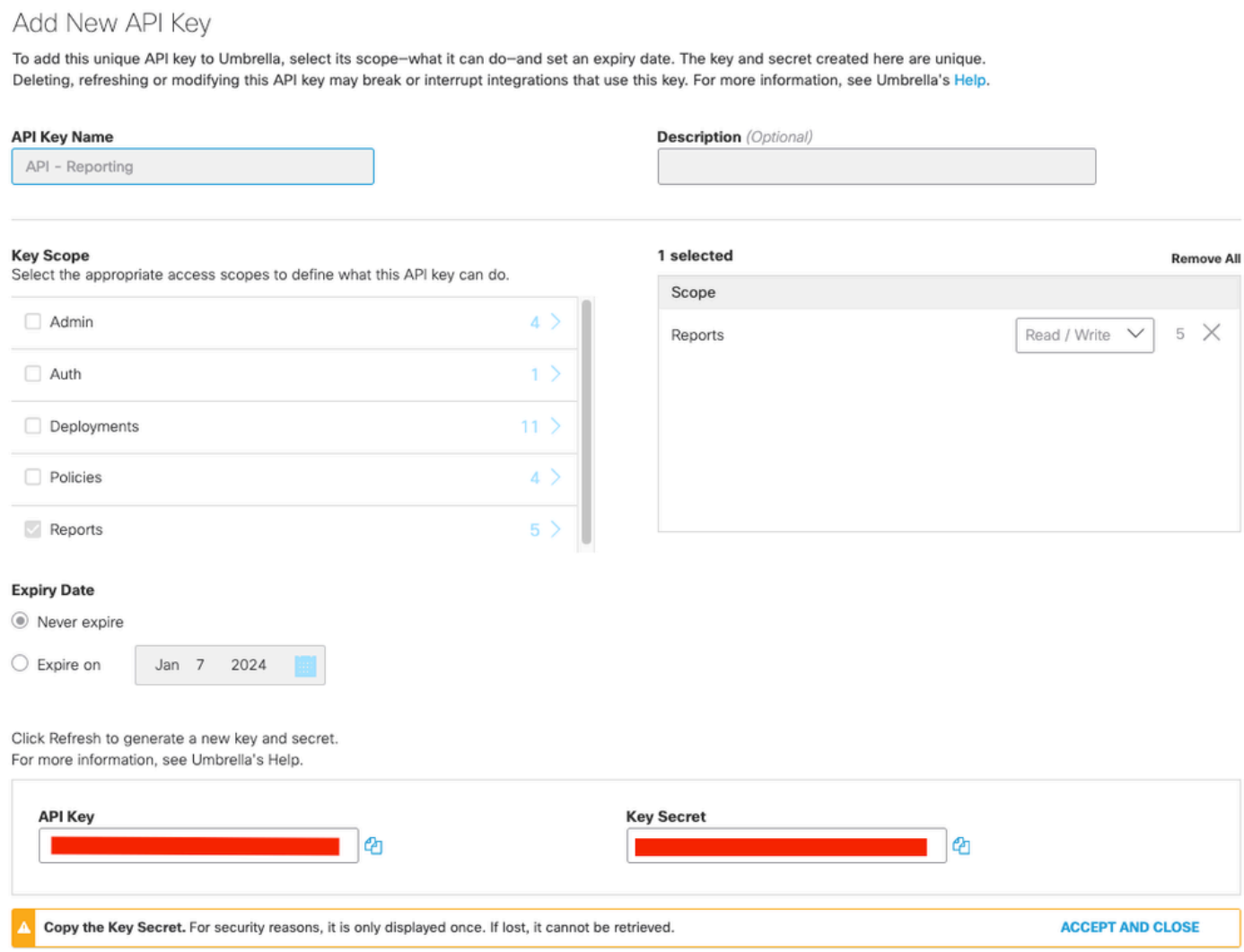
This article demonstrates how to collect activity search reports via API.

Umbrella Procedure

1. From the Umbrella dashboard, navigate to **Admin > API Keys**.

2. Select **API Keys > Add**.

3. Under **Key Scope**, select **Reports**, then **Create Key**.



21495050167956

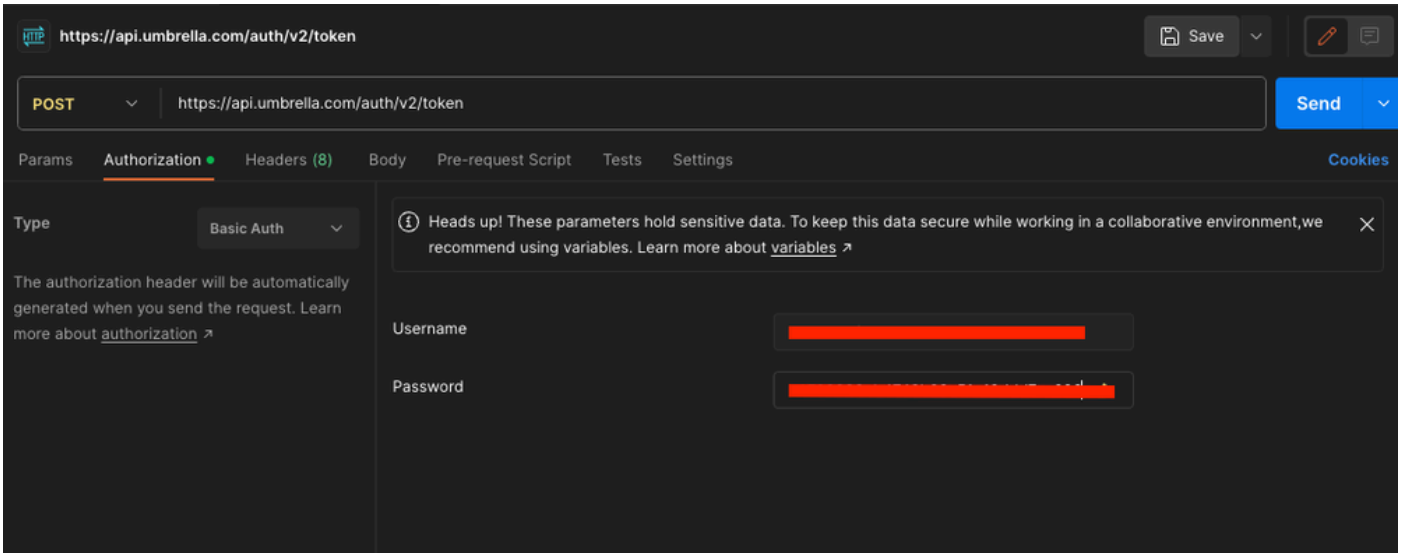
Admins can adjust the level of access per scope between Read / Write and Read-Only, depending on the intended use of each API key, while the API keys can be configured to expire on a pre-defined date. You are required to collect the API key/secret at this step, as they are currently visible, and they cannot show up afterwards.

The API credentials generate API access tokens which are valid for 60 minutes. This procedure supports the OAuth 2.0 client credentials flow. In Umbrella multi-org or service provider environments, parent-org API

credentials can be used to generate access tokens with the same scopes for a child org specified during the authorization process.

Postman Procedure

At the first, you are required to create an OAuth 2.0 access token. The Umbrella API auth paths begin with https://api.umbrella.com/auth/v2. Upon the submission of a POST query and user API key as username and API password as password, an Access Token is generated.

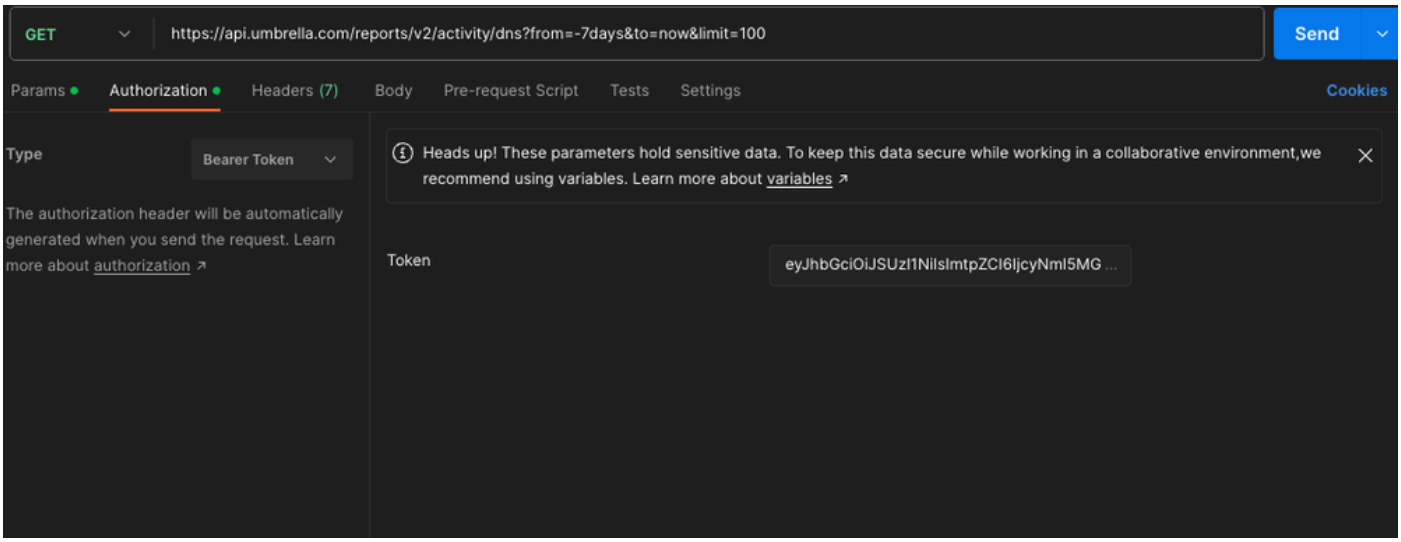


21606708808468

21607051456276

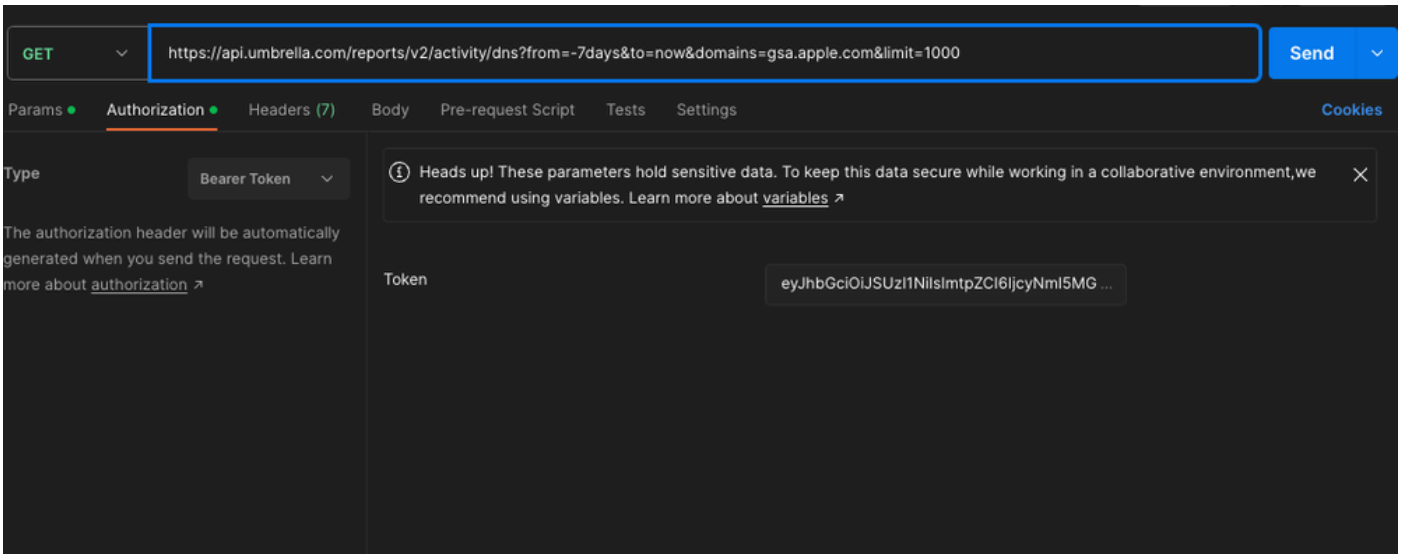
At this step, you are required to collect the Access Token. Now you can retrieve information with the Access Token.

You are required to select the GET method and enter both your API path (including the parameter you require) and Access Token. In this example, you can retrieve 100 reports from the activity search exclusively for DNS traffic for last 7 days.



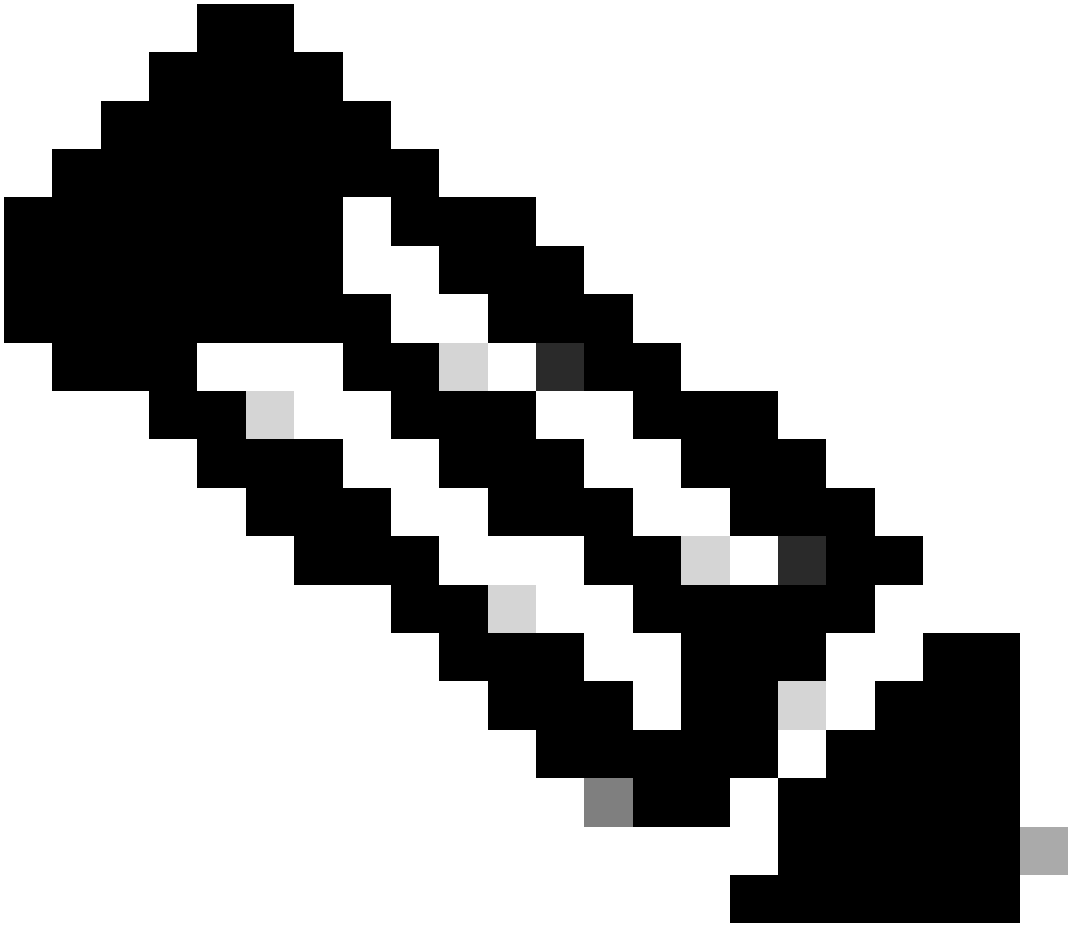
21607952074772

In another example, you can attempt to extract 1000 reports from activity search, exclusively for DNS traffic for last 7 days, specifically for the "gsa.apple.com" domain.



21607927544468

You can consult Request Query Parameters to discover additional parameters you can use in your API query.



Note: If an HTTP client request does not originate from the same continent as the location of the Umbrella data warehouse, the Umbrella server responds with 302 Found. To automatically redirect HTTP requests and preserve the HTTP Authorization header, you can set additional flags or enable a redirect setting.

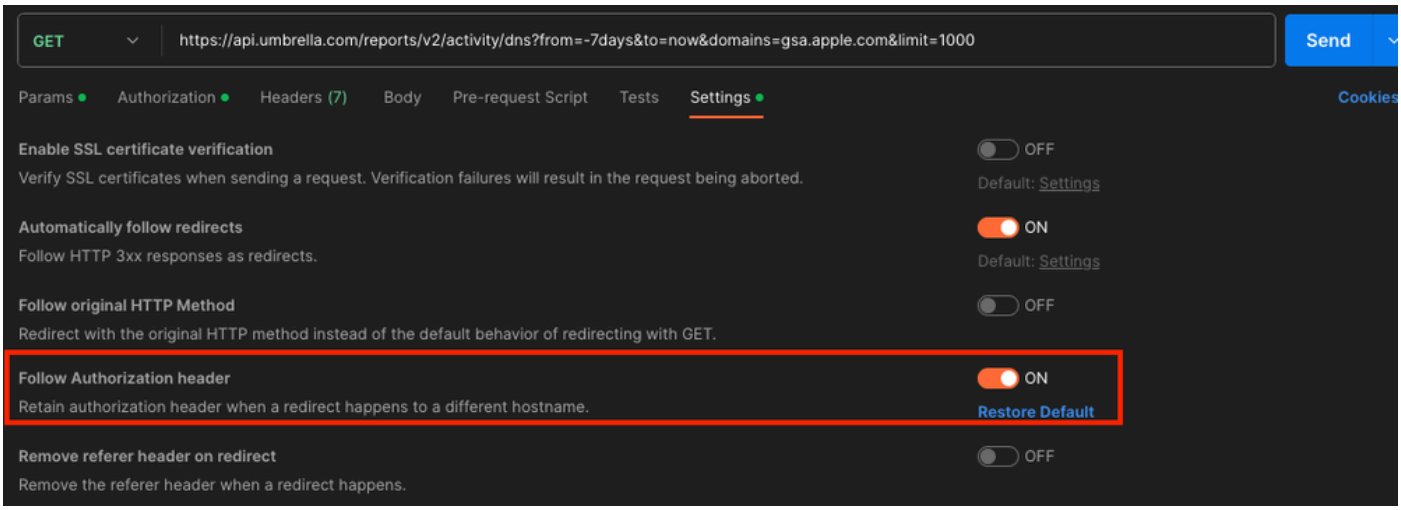
---

curl: You must pass the -L or --location, and --location-trusted flags to redirect the curl HTTP request and retain the Authorization header.

```
cURL
1 curl --location--trusted 'https://api.
      umbrella.com/reports/v2/activity/dns?
      from=-7days&to=now&domains=gsa.apple.
      com&limit=1000' \
```

21608126036628

Postman: Within the Postman environment, navigate to an API and select a GET method. Navigate to **Settings > Enable Follow Authorization header** to preserve the Authorization header for redirect requests.



21608126042388

Responses

After sending GET action to the URL you can receive various status codes:

- **Status:200**: The request successfully took the information you asked.
- **Status: 400**: Invalid request. It can be related to the URL you have sent to query. One or more parameters is not correct.
- **Status: 401**: Unauthorized. The authorization header is missing or the token is unauthorized.
- **Status:403**: Forbidden. The token is invalid.