Integrate Cisco “Umbrella” OpenDNS
EventTracker v 9.x and above

Publication Date: May 20, 2019
Abstract

This guide provides instructions to configure/retrieve Cisco “Umbrella” OpenDNS Security Events and “All Traffic Events (Using Amazon S3)” related events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Cisco “Umbrella” OpenDNS.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise 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

Abstract .................................................................................................................................................. 1  
Scope .................................................................................................................................................. 1  
Audience .............................................................................................................................................. 1  
Overview ............................................................................................................................................ 4  
Prerequisites ....................................................................................................................................... 4  
Integrating OpenDNS Security Activities .......................................................................................... 4  
Integrating OpenDNS All Traffic Activity (Using Amazon S3) ......................................................... 4  
Configuring Cisco “Umbrella” OpenDNS to forward logs to EventTracker ....................................... 5  
OpenDNS Security Activities .............................................................................................................. 5  
  Collecting Open DNS “API Key” and “API Secret” and “Organization ID” ....................................... 5  
  Configuring EventTracker OpenDNS Integrator .............................................................................. 7  
OpenDNS All Traffic Activity (Using Amazon S3) ............................................................................... 8  
  Setting up your Amazon S3 bucket ................................................................................................. 8  
  Collecting OpenDNS Umbrella Insights logs into Amazon S3 ....................................................... 11  
  Ensuring logs are being uploaded into Amazon S3 ...................................................................... 14  
  Collecting Amazon S3 logs for OpenDNS into EventTracker system using AWS CLI ................ 15  
  Scheduling a Task to Generate OpenDNS Logs ........................................................................... 17  
  Forwarding OpenDNS logs into EventTracker Locally via Log file Monitor (LFM) ....................... 21  
Error Codes ........................................................................................................................................ 27  
EventTracker Knowledge Pack ........................................................................................................... 27  
  Flex Reports .................................................................................................................................. 27  
Alerts .................................................................................................................................................. 28  
Dashboards ........................................................................................................................................ 28  
Importing Cisco “Umbrella” OpenDNS knowledge pack into EventTracker ...................................... 30  
  Categories ...................................................................................................................................... 31  
  Alerts ............................................................................................................................................ 32  
  Knowledge Object ......................................................................................................................... 33  
  Flex Reports .................................................................................................................................. 34  
  Token Template ............................................................................................................................. 36  
  Dashboard ...................................................................................................................................... 37
Integrate Cisco “Umbrella” OpenDNS

Verifying Cisco “Umbrella” OpenDNS knowledge pack in EventTracker .......................................................... 39
Categories .......................................................................................................................................................... 39
Alerts .................................................................................................................................................................. 40
Token Value ......................................................................................................................................................... 40
Knowledge Objects ........................................................................................................................................... 41
Flex Reports ......................................................................................................................................................... 41
Dashboard ........................................................................................................................................................... 42
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 events related to general traffic, audit or security activities.

For the better convenience and ease of monitoring, EventTracker provides 2 different types of log monitoring:

1. **An Event specifically related to Security Activity** – This includes, security activities like malware, suspicious, phishing, botnet, drive-by download, etc.
2. **All Events (using Amazon S3)** – Includes security activity events along with DNS events, admin audit log.

Prerequisites

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.

Integrating OpenDNS All Traffic Activity (Using Amazon S3)

- Login to Amazon AWS service ([https://s3.console.aws.amazon.com](https://s3.console.aws.amazon.com)) and AWS CLI should be installed in the EventTracker machine.
- Amazon S3 should be turned on in your AWS account.
- A bucket configured in Amazon S3 to be used for storing logs.
- Full administrative access to the OpenDNS Umbrella dashboard.
- EventTracker v9.0 or later should be installed.
- Administrative access on the EventTracker machine.
Configuring Cisco “Umbrella” OpenDNS to forward logs to EventTracker

OpenDNS Security Activities

(NOTE: Follow the below configuration steps if only security activity is required)

The steps provided below will help to configure the EventTracker to receive specific events related to security activity from Cisco “Umbrella” OpenDNS.

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. Next, In the Umbrella dashboard for the organization, navigate to Admin > API Keys and click Add.

3. In the “What should this API do? “modal, select "Umbrella Network Devices", "Umbrella Reporting", or "Legacy Network Devices" as appropriate, then click Create.
4. Next, you'll see the key and secret. You must acknowledge that the secret can only be seen once by ticking the checkbox and clicking 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.

Configuring EventTracker OpenDNS Integrator

1. Contact the EventTracker support team and get the “OpenDNS Integrator” executable file.
2. Once the executable application is received, right click on the file and select “Run as Administrator”.
3. In the next dialog box, enter your Cisco Umbrella OpenDNS API key, Secret and the Organization ID (can be collected from OpenDNS GUI); and click on the “Validate” button to verify the credentials.

![Figure 4](image)

4. On successful verification, a pop window will appear with a message: “Credential Validated Successfully”.
5. Next, click on the “Submit” button to complete the integration process.

![Figure 5](image)
OpenDNS All Traffic Activity (Using Amazon S3)

(NOPE – Follow the below configuration steps if all activity logs are required including security activity)

The steps provided below will help to configure the EventTracker to receive events related to **All traffic activities (using Amazon S3)** from Cisco “Umbrella” OpenDNS.

But first, you must enable and configure logging on Amazon S3 for OpenDNS Umbrella Platform prior to configuring EventTracker.

**Setting up your Amazon S3 bucket**

Following are the step to create the Amazon S3 bucket:

1. Start by signing into the AWS Console, and selecting "S3 - Scalable Storage in the Cloud" from the list of options. It’s in the upper left, under Storage & Content Delivery.
2. Click Create **Bucket** tab.

![Create Bucket](image)

**Figure 8**

3. Start by entering a **Bucket Name**.

![Create a Bucket](image)

**Figure 9**

**NOTE**: Make sure that the bucket name is universally unique -- not just to your AWS or your Umbrella, but also to all of Amazon AWS. Using something personal, such as "**my-organization-name-log-bucket**" can help you bypass the requirement for a universally unique bucket name. The bucket name must only use lowercase letters and cannot contain spaces and must comply with DNS naming conventions.

4. After this is complete, select the **Region** that works best for your location.
5. Click **Create**.
6. Next, you will need to configure the bucket to accept uploads from the Umbrella Service. In S3, this is referred to as a **bucket policy**.
7. Click on the newly created bucket to open it.
8. Then, select Properties in the upper right-hand corner.
9. In the Properties drop-down menu, select and expand Permissions. Within the Permissions drop-down, click on Add bucket policy.

10. A modal window will appear, and at this point, you will have to upload the preconfigured bucket policy provided in this article.
Copy and paste the JSON string below, which contains the bucket policy, to a text editor or simply paste it into the window. Substitute your exact bucket name where `bucketname` is specified below:

**IMPORTANT:**

The bucket name must be exact or the service will not accept the bucket policy and you will receive an error reading "Policy has invalid resource - arn:aws:s3:::bucketname/**"

```json
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucketname/*"
    },
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::bucketname/*"
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::bucketname"
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::568526795995:user/logs"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::bucketname/*"
    }
  ]
}
```

Click Save to confirm this change:

**Collecting OpenDNS Umbrella Insights logs into Amazon S3**

Follow the steps for integrating OpenDNS Umbrella Insights and Platform with Amazon S3:
1. Go back to your Umbrella dashboard and navigate to **Log Management** under **System Settings > Log Management**.

![Figure 13](https://via.placeholder.com/150)

2. Click on "**Amazon S3**" as a Log Destination to expand the window.
3. In the field labeled **Bucket Name**: type or paste the exact bucket name that you have created in S3 and click **Verify**.
4. You should receive a confirmation message in your dashboard indicating that the bucket was successfully verified.

![Figure 14](https://via.placeholder.com/150)
5. If you receive an error indicating that your bucket could not be verified, recheck the syntax of the bucket name and review the configuration. If problems persist, open a case with the support department.

6. As a secondary precaution, to ensure that the correct bucket was specified, the dashboard will request you to enter a unique activation token.

7. The activation token can be obtained by revisiting your S3 bucket. As part of the verification process, a file named README_FROM_OPENDNS.txt will be uploaded from OpenDNS to your Amazon S3 bucket and the activation token will appear there.

8. Download the readme file by double-clicking on it and open the readme file in a text editor. Within the file, there will be a unique token tying your S3 bucket to your Umbrella dashboard.

**NOTE:** You may need to refresh your S3 bucket in the browser to see the README file after it has been uploaded.

9. Return to the Umbrella dashboard and paste the token into the field labeled "Enter your unique token" and click Save.

10. The configuration is complete. To review your configuration, just click on the Amazon S3 name in the Log Management section of the Umbrella dashboard.
Ensuring logs are being uploaded into Amazon S3

Logs are uploaded in 10-minute intervals from the OpenDNS log queue to the S3 buckets. Within the first 10 minutes after a completed configuration, you should receive your first log upload in your S3 bucket. To verify if everything is working, check whether the last sync time in the Umbrella dashboard is updated and logs appear in your S3 bucket.

The logs will appear in a GZIP format with the following file name format. The files will also be sorted into date-stamped folders:

dnslogs/<year>-<month>-<day>/<year>-<month>-<day>-<hour>-<minute>.csv.gz

If you do not see logs in your bucket within 10 minutes, contact support outlining the steps that you have taken as far.

Once logs do appear we recommend reviewing the data by unzipping the contents of the first few log uploads that are received to ensure the data is viewable in a text editor (or even Microsoft Excel, often the default for .CSV).
Collecting Amazon S3 logs for OpenDNS into EventTracker system using AWS CLI

2. Go to system properties and create an environment variable for AWSCLI as shown in below figure:

![Figure 18](image)


![Figure 19](image)

4. Access Key ID, Secret Access Key, and Region information given by the AWS console.
5. Export the logs from Amazon S3 to local machine using following command:

```bash
aws s3 sync s3://my-organization-name-log-bucket/dnslogs/2015-08-03/ s3logs
```

**Note:** Here “s3logs” specifies the path where you want to export your logs and `s3://my-organization-name-log-bucket/dnslogs/2015-08-03/` S3 log folder in Amazon S3. You can also schedule the command by saving it as a .bat file.

Below are the script contents which can be scheduled for every 10 min. Copy and save it as:

```bash
OpenDNSScript.bat
c:
cd %homepath%
mkdir opendnslogs
mkdir opendnslogs
```
mkdir s3logs
mkdir "final logs"
aws s3 sync s3://my-organisation-name-log-bucket/dnslogs/ s3logs
mkdir s3logsextracted
cd s3logs
for /r "." %a in (*) do (pushd %CD%
"C:\Program Files (x86)\7-Zip\7z.exe" x "%a" -o%homepath%opendnslogs\s3logsextracted\ -y popd ) Type "%homepath%opendnslogs\s3logsextracted\" > "%homepath%opendnslogs\final logs\file.csv"
echo "Timestamp","Most granular identity","Identities","InternalIP","ExternalIP","Action","Query type","ResponseCode","Domain","Category" > "%homepath%opendnslogs\final logs\header.txt"
type "%homepath%opendnslogs\final logs\header.txt" > "%homepath%opendnslogs\final logs\logs.csv"
copy "%homepath%opendnslogs\final logs\logs.csv" + "%homepath%opendnslogs\final logs\file.csv" "%homepath%opendnslogs\final logs\logs.csv"
del /F /Q "%homepath%opendnslogs\s3logsextracted\*.sorted"
exit

Note: In the example, my-organization-name-log-bucket is the S3 bucket name. Change it as per your bucket name.

Scheduling a Task to Generate OpenDNS Logs

1. To open Task Scheduler, click the Start >Administrative Tools> Task Scheduler. Task Scheduler window displays.
2. To schedule a task in task scheduler, select Create Task in Actions pane:

Create Task wizard window displays.
3. Enter the appropriate **Name** and **Description** for the task. Then click the **Triggers** button. Task Trigger pane displays.

4. Select the **New** button. The New Trigger window displays.
5. Select ‘Daily’ in the Setting option and then check the Repeat task every button and select 10 minutes.
6. Enter the date and time in Start and then click the OK button.
7. Click on the Actions tab, then click on the New button and select ‘Start a program’ from the dropdown list in Actions option.
8. Select ‘Start a program’ from the dropdown list in Actions option.
9. Click the Browse button and select the location of the OpenDNSScript.bat. Click the OK button.
10. Verify the task details and then click **OK** button.
11. The respective task is scheduled in Task Scheduler.
12. Double click on the respective task scheduled.
13. Click on the **General** tab.
14. In **Security options** pane, select **Run whether the user is logged on or not** and **Run with highest privileges** options and then click **OK** button.

**Forwarding OpenDNS logs into EventTracker Locally via Log file Monitor (LFM)**

Before LFM configuration, deploy the EventTracker agent on the AWS machine, refer the [EventTracker Agent installation guide](#). After installation of the agent follows below-mentioned steps to configure LFM.

1. Select the **Start** button, select **Prism Microsystems**, and then select the **EventTracker Control Panel**.
2. Select **EventTracker Agent Configuration**, select systems vCenter Single Sign-On machine name.
3. Select a **Logfile Monitor** option.
   EventTracker recommends adding the following log files for OpenDNS that you would like to monitor.
   %homepath%\opendnslogs\final logs\logs.csv

4. Click the **Add File Name** button.
   Enter **File Name** window displays.
5. Select **Get All Existing Log Files** option.
6. In select, **Log File Type** drop-down, select the **CSV** option.
7. Enter the path of the OpenDNS logs (%homepath%\opendnslogs\final logs\logs.csv).
8. Click the **OK** button.

9. Click the **Save** button.

10. As we are generating alerts for OpenDNS, we need to add Event ID ‘**3230**’ an exception.

11. Select the **Event Filters** Tab.
12. Select **Filter Exception** option, Filter Exception window will display

13. Click **New** Option,

14. Event **Details** window will display

15. Click on **New** button.
16. Enter the Event ID (3230) in the Event ID field and click the OK button.

17. Now, event id 3230 is added into exception and it is listed in the filter exception windows.
18. Close the Filter Exception window and **Save** the changes.
Error Codes

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

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Cisco “Umbrella” OpenDNS.

Flex Reports

- OpenDNS Security Activity – This report will generate all the security-related activities in a network. Activities captured by this report might include attempts to access sites hosting malware or phishing sites, botnet, drive-by download activity on infected machines on your local network, attempts to download malicious files—or more. (*Note – Available for both Security Activity and ALL Traffic Activity monitoring) – This will include both “Allowed” and “Blocked” traffic events.
Sample Logs:

```xml
```

**Alerts**

- **OpenDNS Security Activity** - This alert is generated when a “blocking” event is detected by EventTracker. (*Note – Available for both Security Activity and ALL Traffic Activity monitoring)*

**Dashboards**

- **OpenDNS Security Activity (By Category)**
• OpenDNS Security Activity (By Source IP)
Integrating Cisco “Umbrella” OpenDNS knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template
- Knowledge Objects
- Flex Reports
- Dashboard

1. Launch the EventTracker Control Panel.
2. Double click Export-Import Utility.

![Figure 42](image)

![Figure 43](image)
3. Click the **Import** tab.

### Categories

1. Click the **Category** option, and then click the browse button.

![Figure 44]

2. Navigate to the location having a file with the extension “.iscat” and then click on the “**Import**” button:

![Figure 45]
Integrate Cisco “Umbrella” OpenDNS

EventTracker displays a success message:

![Export Import Utility](image)

Figure 46

Alerts

1. Click **Alert** option, and then click the browse button

![Export Import Utility](image)

Figure 47

2. Navigate to the location having a file with the extension “.istoken” and then click on the “Import” button:
1. Click Knowledge objects under the Admin option in the EventTracker manager page.

2. Next, click on the “import object” icon:
3. A pop-up box will appear, click “Browse” in that and navigate to the file path with extension “.etko” button.

4. List of available knowledge object will appear. Select the relevant files and click on “Import” button:

**Flex Reports**

1. In EventTracker Control Panel, select “Export/ Import utility” and select the “Import tab”. Then, click Reports option, and Choose “New (*.etcrx)”: 
2. Once you have selected “**New (*.etcrx)**”, a new pop-up window will appear. Click on the “**Select File**” button and navigate to the file path with a file having the extension “*.etcrx*”.

3. Select all the relevant files and then click on the **Import** button.
4. EventTracker displays a success message:

![Success message](image)

**Token Template**

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Template**.
2. In the **Template** tab, click on the “import”, button:
3. In the new pop up window, click on **Browse**, and navigate to file path where the “.ettd” file is saved.

4. You will then see the token templates being loaded. Select the ones required and click on the “**Import**” button.

5. This will complete the “**Token Template**” import to **EventTracker**.

**Dashboard**

1. Login to **EventTracker Enterprise**.
2. Navigate to **Dashboard → My Dashboard**.
3. In “My Dashboard”, Click on **Import Button**:

![Image of Import Button](image1)

**Figure 59**

4. Select the **Browse** button and navigate to file path where dashboard file is saved:

![Image of Browse Button](image2)

**Figure 60**

5. Once completed, click on “**Upload**” Button.

6. Next, select all the relevant dashboards for **Cisco “Umbrella” OpenDNS** and click on the “**Import**” button:

![Image of Import Button](image3)

**Figure 61**
Integrate Cisco “Umbrella” OpenDNS

7. Next, click on “Customize dashlet” button as shown below:

![Customize dashlet button](image)

Figure 62

8. Now, put a text on the Search bar: “OpenDNS” and then select the MuleSoft Dashlets and then click on the “Add” button.

![Customize dashlets](image)

Figure 63

Verifying Cisco “Umbrella” OpenDNS knowledge pack in EventTracker

Categories

1. Login to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Cisco “Umbrella” OpenDNS group folder to view the imported categories
Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In search box enter “OpenDNS” and then click the Search button.
   EventTracker displays an alert of Cisco “Umbrella” OpenDNS – Security Activity.

Token Value

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Template.
2. In the Template tab, click on the “OpenDNS” group folder to view the imported Token Values.
Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand the “OpenDNS” group folder to view the imported Knowledge objects.

Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select the Report Configuration.
2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **OpenDNS** group folder to view the imported “**OpenDNS Security Activity**” reports.

**Dashboard**

1. In the EventTracker Enterprise web interface, Click on **Home Button** and select “**My Dashboard**”
2. In “OpenDNS” dashboard you should be now able to see something like this:

![My Dashboard](image)

**Figure 71**