Cisco Umbrella

Last updated: Jun. 9, 2025

Overview

Enhance detections with data from Cisco Umbrella.

Requirements

Subscription: Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB.

CrowdStrike clouds: Available in US-1, US-2, EU-1, and US-GOV-1.

Other requirements:

- Your environment must include a functioning deployment of Cisco Umbrella.
- Access to an existing Amazon S3 bucket.
- Administrator access to the Falcon console for the respective CID.

Setup

> **Important:** Some of these steps are performed in third-party products. The CrowdStrike Falcon platform integrates the relevant settings as you configure them. However, CrowdStrike does not validate any third-party configurations. Perform the following steps with care, and validate your settings and values before finalizing configurations in Falcon.

Step 1. Company-managed S3 bucket: enable logging, and retrieve the access key and secret access key

If you enabled logging to your own S3 bucket, follow these steps. For more info, see
Enable Logging to Your Own S3 Bucket [https://docs.umbrella.com/deployment-umbrella/docs/setting-up-an-amazon-s3-bucket].

Enable logging

1. Log in to the Cisco Umbrella portal as an Administrator, and then go to **Admin > Log Management**.
2. Select **Use your company-managed Amazon S3 bucket**.
3. In the **Amazon S3 bucket** field, enter the precise bucket name that you created in Amazon S3 and click **Verify**.

   > **Note:** If an error message is displayed, see
   > Enable Logging to Your Own S3 Bucket [https://docs.umbrella.com/deployment-umbrella/docs/setting-up-an-amazon-s3-bucket].

4. Open the **README_FROM_UMBRELLA.txt** file in your Amazon S3 bucket.
   a. Copy the token listed in the readme file and paste it into the **Token Number** field in Cisco Umbrella.
   b. Click **Save**.
5. Optional. Enable **Admin Audit Log**.
6. Optional. Enable **Log Https Query** and review and agree to the terms and conditions. For more info, see
   HTTPS transactions [https://support.umbrella.com/hc/en-us/articles/215795814228 68-Log-query-string-parameters-for-HTTPS-transactions-to-s3-bucket-is-now-Generally-Available-GA]
   .

   > **Note:** We recommend that you upgrade your **Schema Version** to the most current version.

Retrieve the access key and secret access key

In AWS and Amazon S3, configure a policy, user group, and permissions in order to create the access key and secret access key.

Create an AWS policy for the Cisco Umbrella integration

1. Log in to AWS and go to **AWS > IAM > Access Management > Policies**.
2. Click **Create policy**.
3. On the **Specify permissions** page, click **JSON**.
4. Delete the contents of the **Policy editor** field and enter the following script. Replace both instances of `my-bucket` with your S3 bucket name.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "MyReadOnlyBucketPolicy"
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket",
                "arn:aws:s3:::my-bucket/*"
            ]
        }
    ]
}
```

5. Click **Next**.
6. Enter a **Policy Name** and **Description** (optional). Save the **Policy name** to enter later in the integration.
7. Click **Create policy**.

Create an AWS user group for the Cisco Umbrella integration

1. In AWS, go to **IAM > Access Management > User groups** and click **Create group**.
2. Enter a group name. Save the **Group name** to enter later in the integration.
3. In the **Attach permission policies - Optional** section, select the policy that you just created.
4. Click **Create group**.

Create an AWS user

1. In AWS, go to **IAM > Access Management > Users** and click **Create user**.
2. On the **Specify user details** page, enter a user name.

   > **Note:** This user account will only be used to send Cisco Umbrella data.

3. Do not enable **Provide user access to the AWS Management Console**.
4. Click **Next**.
5. On the **Set permissions** page, in the **Permissions options** section, select **Add user to group**.
6. Select the group you created earlier and click **Next**.
7. On the **Review and create** page, review the user details and click **Create user**.
8. On the **Users** page, click the user name of the user you created earlier.
9. In the Summary section, save the **ARN** value to enter later in the integration.

Create an access key and secret access key

1. In AWS, go to **Access Management > Users**.
2. On the **Users** page, click the user name of the user you created earlier.
3. In the **Security credentials** tab, in the **Access keys** section, click **Create access key**.
4. Select **Third-party service**.
5. Acknowledge the recommendation and click **Next**.
6. Optional. In the **Description tag value** field, enter a description, for example "This key is for read only access to *my-bucket* for the purpose of allowing the CrowdStrike platform to pull Cisco Umbrella data".
7. Click **Create access key**.
8. Save the **Access key** and **Secret access key** values to enter later in the integration.

   > **Important:** The **Access key** and **Secret access key** pose a security risk if compromised. We recommend deleting them after you enter them in a later step.

   > **Note:** You won't be able to access the **Access key** value again. If you lose this value, delete the existing Access key in the AWS and create a new one.

9. Click **Done**.

Update S3 bucket permissions

1. Log in to Amazon S3, and go to **Buckets**.
2. Click your S3 bucket.
3. On the **Permissions** tab, in the **Bucket policy** section, click **Edit**.
4. In the **Policy** editor, add the following script by adding a comma after the last existing statement Sid block {}, but within the Statement [] block.

   > **Important:** You must replace all instances of `my-arn` with the **ARN** value that you saved earlier and replace all instances of `my-bucket` with your S3 bucket name.

```
{
```

```
        "Sid": "allow-get",
        "Effect": "Allow",
        "Principal": {
            "AWS": "my-arn"
        },
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
        "Sid": "get-bucket-loc",
        "Effect": "Allow",
        "Principal": {
            "AWS": "my-arn"
        },
        "Action": "s3:GetBucketLocation",
        "Resource": "arn:aws:s3:::my-bucket"
    },
    {
        "Sid": "list-items",
        "Effect": "Allow",
        "Principal": {
            "AWS": "my-arn"
        },
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:::my-bucket"
    }
```

5. Click **Save changes**.

> **Note:** If there are any errors, ensure the JSON is in a valid format.

Step 1. Cisco-managed S3 bucket: enable logging, and retrieve the data path, access key and secret key

If you enabled logging to a Cisco-managed S3 bucket, follow these steps. For more info, see Enable Logging to a Cisco-managed S3 Bucket [https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket].

1. Log in to the Cisco Umbrella portal as an Administrator, and then go to **Admin > Log Management**.
2. Select **Use Cisco-managed Amazon S3 storage**.
3. Select a **Region** and **Retention Duration**.

> **Note:** The retention duration that you select does not affect the Falcon integration.

4. Click **Save**.
5. Confirm that your settings are correct and then click **Continue**.
6. Save the **Data Path**, **Access Key**, and **Secret Key** values to enter later in the integration.
7. Enable **Got It!** and click **Continue**.
8. Optional. Enable **Admin Audit Log**.
9. Optional. Enable **Log Https Query** and review and agree to the terms and conditions. For more info, see HTTPS transactions [https://support.umbrella.com/hc/en-us/articles/21579581422868-Log-query-string-parameters-for-HTTPS-transactions-to-s3-bucket-is-now-Generally-Available-GA]
.

> **Note:** We recommend that you upgrade your **Schema Version** to the most current version.

Step 2. Configure and activate the Cisco Umbrella Data Connector

For both types of AWS S3 bucket, in the Falcon console, configure the Cisco Umbrella data ingestion application.

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. Click **+ Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.
4. In the **New connection** dialog, review connector metadata, version, and description. Click **Configure**.

> **Note:** For connectors that are in a **Pre-production** state, a warning dialog appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.
6. Enter the following values:
    - **Name:** Enter a name for your configuration.
    - **Access Key ID:** Enter the **Access Key** value that you saved earlier.
    - **S3 Bucket Name:**
        - For company-managed S3 bucket: Enter your S3 bucket name.

- For Cisco-managed S3 bucket: Enter the name-region section of the **Data Path**. For example, from the data path `s3://cisco-us-west-1/1234567890`, enter cisco-us-west-1.

- **S3 object Prefix:** Enter the final character sequence from the path of your Cisco-managed S3 bucket. You must include the entire path listed after bucket name and region. For example, if your S3 bucket path is `s3://cisco-us-west-1/1234567890/group012345`, enter the entire folder path, `1234567890/group012345`, as the S3 object prefix. See S3 Bucket Data Path [https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket#s3-bucket-data-path] for more information on path fields.

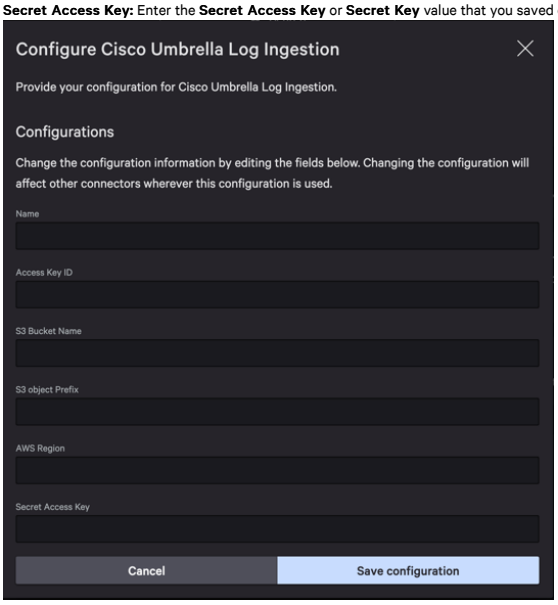
  > **Note:** Leave the **S3 object Prefix** field blank if you are using a company-managed S3 bucket.

- **AWS Region:**

  - For company-managed S3 bucket: Enter the region of your AWS S3 bucket. For example, us-west-1.

  - For Cisco-managed S3 bucket: Enter the region section of the **Data Path**. For example, from the data path `s3://cisco-us-west-1/1234567890`, enter us-west-1.

- **Secret Access Key:** Enter the **Secret Access Key** or **Secret Key** value that you saved earlier.



7. Click **Save Configuration**.
8. In the **Data connector configuration** field, select the configuration you just created.
9. Enter a name and an optional description to identify the connector.
10. Click the **Terms and Conditions** box, then click **Save**.

Step 3: Verify successful data ingestion

> **Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections [/data-connectors]**.
2. In the **Status** column, verify data connection status is **Active**.
3. In the **Actions** column, click **Open** menu ⋮ and select **Show events** to see all events related to this data connection in **Advanced Event Search**.
4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#Vendor=cisco | #event.module=umbrella
```

Data reference

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- Network:Allowed:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#d44jz11k]
- Network:Denied:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#o1co06s5]
- Network:Access:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#w0veajdl]
- Configuration:Change:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vkl]
- Configuration:Creation:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#n9xgygup]
- Configuration:Deletion:{failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#v267j0ck]

- Intrusion_detection:Allowed:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#p8u9kw22]
- Intrusion_detection:Denied:(failure,success,unknown) [/documentation/page/q1f14b54/next-gen-siem-data#x8zazrto]

For more information about Next-Gen SIEM events, see Next-Gen SIEM Data Reference [/documentation/page/q1f14b54/next-gen-siem-data] .

‹ Cisco Secure Network Analytics[/documentation/page/r96395b2/cisco-secure-netwo Citrix NetScaler › [/documentation/page/f608b9d4/citrix-netscaler]