# Integrating Cisco Umbrella

https://campus.barracuda.com/doc/96767812/

This document provides instructions on setting up Cisco Umbrella to Barracuda XDR monitoring: https://docs.umbrella.com/deployment-umbrella/docs/cisco-managed-s3-bucket

## Enable Logging to a Cisco-managed S3 Bucket

**Prerequisites**

- Full administrative access to Cisco Umbrella.

**To Enable Logging**

1. Navigate to **Admin** > **Log Management** and select **Use a Cisco-managed Amazon S3 bucket**.



2. Select a **Region** and a **Retention Duration**.

- **Select a Region**—Regional endpoints are important to minimize latency when downloading logs to your servers. The regions match those available in Amazon S3, however not all regions are available. Pick the region that's closest to you from the dropdown. If you wish to change your region in the future, you will need to delete your current settings and start over.
- **Select a Retention Duration**—Select 7, 14, or 30 days. Beyond the selected time period, all data will be purged and cannot be retrieved. We recommend a smaller time period if your ingestion cycle is regular. The retention duration can be changed at any time.

3. Click **Save** and then **Continue** to confirm your settings.



Umbrella activates its ability to export to an AWS S3 account. When activation is complete, the Amazon S3 Summary page appears.

4. Copy credentials from this page and store them in a safe place. This is the only time that the **Access** and **Secret** keys are made available to you. These keys are required to access your S3 bucket and download logs. If you lose these keys they must be regenerated.

   Save the information in this section and provide the **Data Path**, **Access Key**, and **Secret Key** to Barracuda XDR for log collection configuration.

5. Once keys are copied and safe, enable **Got it.**
6. Click **Continue**.

## Figures

1. 1.jpg
2. 2.jpg
3. ciscoumbrella3.jpg
4. ciscoumbrella4.jpg
5. ciscoumbrella5.jpg