Cisco Secure Cloud Analytics

Umbrella Integration Quick Start Guide

Table of Contents

Cisco Secure Cloud Analytics Integration with Umbrella

You can integrate Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) with the Umbrella Investigate REST API to provide additional information in the Secure Cloud Analytics web portal for external entity IP addresses. This information, generated by Umbrella, includes geolocation-related information, the domain name detected for the entity, and associated malicious domain names. From the Secure Cloud Analytics web portal, you can click through to open the Umbrella interface in a new window and view more information about the entity.

To add Umbrella integration to Secure Cloud Analytics, generate an Umbrella Investigate access token, then upload it to the Secure Cloud Analytics web portal. This integration requires a Secure Cloud Analytics deployment and an Umbrella Investigate REST API subscription. For more information, see https://umbrella.cisco.com/products/packages.

Generating an Umbrella Investigate Access Token

Generate an Umbrella Investigate access token to enable communications with the Umbrella Investigate REST API. For more information, see https://docs.umbrella.com/developer/investigate-api/about-the-api-authentication/.

Generate an Umbrella investigate access token:

Before You Begin

- Log in to the Umbrella Investigate UI as an administrator.

Procedure

1. Select **Settings icon > API Access**.
2. Click **create new token**.
3. Enter an access token **name**.
4. Click **Create**.

Uploading the Umbrella Access Token to Secure Cloud Analytics

After you generate the Umbrella Investigate access token, upload it to the Secure Cloud Analytics web portal to enable interaction with the Umbrella Investigate REST API, and receive DNS and other information from Umbrella.

Upload the Umbrella access token:

Before You Begin

- Log in to your Secure Cloud Analytics web portal as an administrator.

Procedure

1. Select **Settings > Integrations > Umbrella**.
2. Click **Edit Token** to expand the section.
3. Copy the Umbrella access token and paste it into the **New Access Token** field.
4. Select **Enabled.**
5. Click **Save**.

Verifying and Using Umbrella Integration

After you finish integrating Secure Cloud Analytics with Umbrella, you can view Umbrella DNS-related information for external IP addresses directly from the web portal by hovering over an external IP address. This information includes information about the hosting organization, geolocation data, and other malicious domain names associated with the detected organization.

You can also navigate directly to the Umbrella UI and view additional information about an IP address.

> ⓘ Wait up to ten minutes for Secure Cloud Analytics to start displaying Umbrella DNS-related information. If the system does not display this information, contact Cisco Support for assistance.

The following describes the possible field information displayed in the Secure Cloud Analytics web portal if you integrate Secure Cloud Analytics with Umbrella.

Umbrella Integration Fields

Field	Description	Format
ASN CIDR	The CIDR range associated with the organization to which this IP address belongs, as identified by Umbrella. This includes a link to Umbrella for additional information about the IP address.	A CIDR range.
ASN Description	The name of the organization to which this IP address belongs, as identified by Umbrella.	An organization's name.
ASN Region	The Regional Internet Registry where this IP address originated, as identified by Umbrella.	One of the following Regional Internet Registries: • `APNIC` – Asia-Pacific Network Information Centre • `RIPE NCC` - Réseaux IP Européens Network Coordination Centre • `AFRINIC` – African Network Information Centre • `ARIN` – American Registry for Internet Numbers • `LACNIC` - Latin America and Caribbean Network Information Centre
Country	The country where this IP address originated, as identified by Umbrella. This matches the	A country name.

	displayed geolocation flag icon.	
DNS Name	The domain name for this entity, as identified by Umbrella.	A domain name.
Umbrella	The number of malicious domains that this organization hosts or has hosted, as identified by Umbrella. This includes a link to Umbrella for additional information about the IP address.	The number of malicious domains.

View Umbrella information in the Secure Cloud Analytics Web Portal:

Before You Begin

- Log in to your Secure Cloud Analytics web portal as an administrator.

Procedure

- For an external IP address, hover your pointer over the geolocation icon.

Access IP address information through Umbrella directly:

Before You Begin

- Log in to your Secure Cloud Analytics web portal as an administrator.

Procedure

- You have the following options:
    - For an external IP address, hover your pointer over the geolocation icon, then click **details**.
    - For an external IP address, click the IP address, then click **Cisco Umbrella**.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html for a general overview
- https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html to sign up for a 60-day Free Trial
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html for documentation resources
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Change History

Revision	Revision Date	Description
1.0	16 January 2019	Initial version.
1.1	16 October 2020	Updated based on UI updates.
2.0	3 November 2021	Updated product branding.
2.1	4 August 2022	Added Contacting Support section.

Copyright Information