



How-To Guide

Integrate Cisco Umbrella with Netsurion Open XDR

Publication Date

July 13, 2023

Abstract

This guide provides instructions to configure and integrate Cisco Umbrella with Netsurion Open XDR to retrieve its logs via API and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Cisco Umbrella and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Cisco Umbrella in Netsurion Open XDR.

Table of Contents

1	Overview	4
2	Prerequisites	4
3	Integrating Cisco Umbrella with Netsurion Open XDR	5
3.1	Integrating Cisco Umbrella for Single Organization	5
3.1.1	Collecting the Cisco Umbrella API Key and API Secret, and Organization ID	6
3.1.2	Verifying the API Region	8
3.1.3	Configuring the Integrator	8
3.2	Integrating Cisco Umbrella for MSP	12
3.2.1	Collecting MSP API Key and API Secret	12
3.2.2	Configuring Netsurion Open XDR Cisco Umbrella Integrator for MSP	13
3.3	Deleting the Configuration of Cisco Umbrella	19
4	Data Source Integration (DSI) in Netsurion Open XDR	20
4.1	Alerts	20
4.2	Reports	21
4.3	Dashboards	21
4.4	Saved Searches	21

1 Overview

Cisco Umbrella, formerly known as OpenDNS, is a cloud-based domain name resolution service. Netsurion Open XDR offers a solution for configuring and monitoring both events involving single organizations and Managed Service Providers (MSPs).

Netsurion Open XDR manages logs retrieved from Cisco Umbrella. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing any suspicious activities analyze the activity logs such as, DNS, proxy, firewall, or IP address.

2 Prerequisites

- PowerShell 5.0 must be installed on the host system or server.
- Users must have administrative privileges on the host system or server.
- Admin access to Cisco Umbrella platform.
- Uninstallation of the legacy version (below v2.0.0) of the Cisco Umbrella Integrator (if configured).

Note

Refer to [How To Uninstall OpenDNS Integrator guide](#) to uninstall any legacy version (below v2.0.0) of the OpenDNS integrator installed in the system. This process is mandatory before installing the new Cisco Umbrella integrator version 2.x.x.

- Upgradation of the existing version (v2.0.0) of Cisco Umbrella Integrator (if configured).

Note

Refer to [How-To-Upgrade-Cisco-Umbrella-Netsurion guide](#) to upgrade the Cisco Umbrella integrator from v2.0.0 to v2.1.0. There is no need to follow further instruction in this document when the integrator is being upgraded.

- The Data Source Integration package.

Note

To get the Data Source Integration package, contact your Netsurion Account Manager.

IMPORTANT

From integrator version 2.x.x onwards, the system name will be changed. Following is an example for the system name format.

<OrganizationName>-CiscoUmbrella@<ComputerName>~<GroupName>

By default, the following Cisco Umbrella Category logs are received by Netsurion Open XDR.

Adult, Adult Themes, Adware, Application Allow, Cannabis, Child Abuse Content, Command and Control, Command and Control, Cryptocurrency, Crypto mining, Drive-by Downloads/Exploits, Drugs, File Transfer Services, Filter Avoidance, Gambling, Hacking, Hate Speech, Hate/Discrimination, High Risk Sites and Locations, Illegal Activities, Illegal Downloads, Illegal Drugs, Infringing Intellectual Property, Malware, Malware, Mobile Threats, Non-sexual Nudity, Not Actionable, Nudity, Online Trading, Phishing, Pornography, Potentially Harmful, Proxy/Anonymizer, Sexuality, Terrorism, Terrorism and Violent Extremism, Weapons, Web Hosting, Web Spam

Note

Category IDs can be included or excluded in the **Fetch.csv** located in **\CiscoUmbrella\Data\Fetch.csv**. For further analysis, refer to the **CategoryList.txt** file available in same path.

3 Integrating Cisco Umbrella with Netsurion Open XDR

3.1 Integrating Cisco Umbrella for Single Organization

Perform the following procedure to configure Cisco Umbrella for Single Organization.

Note:

If trying to change the configuration from MSP to single, it is necessary to first delete the MSP configuration and then reconfigure.

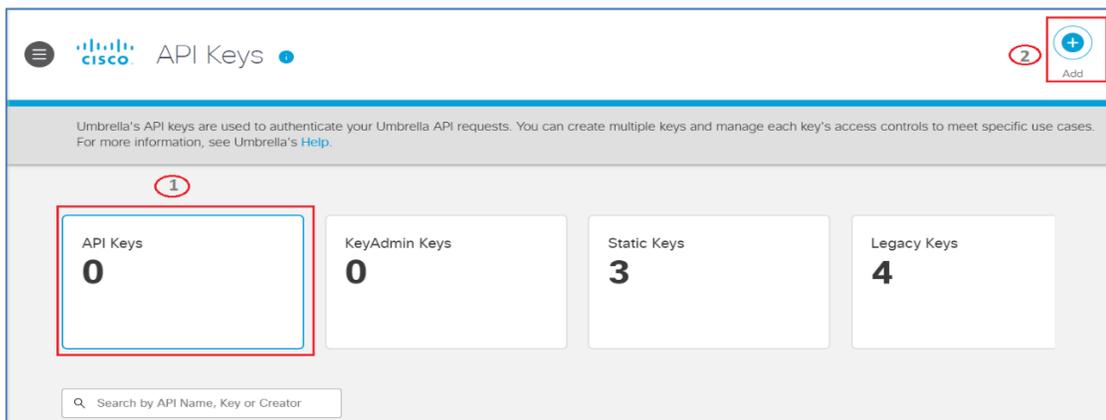
3.1.1 Collecting the Cisco Umbrella API Key and API Secret, and Organization ID

The organization Id can be obtained directly from the Umbrella dashboard after logging in to the organization, as it will be present in the URL.

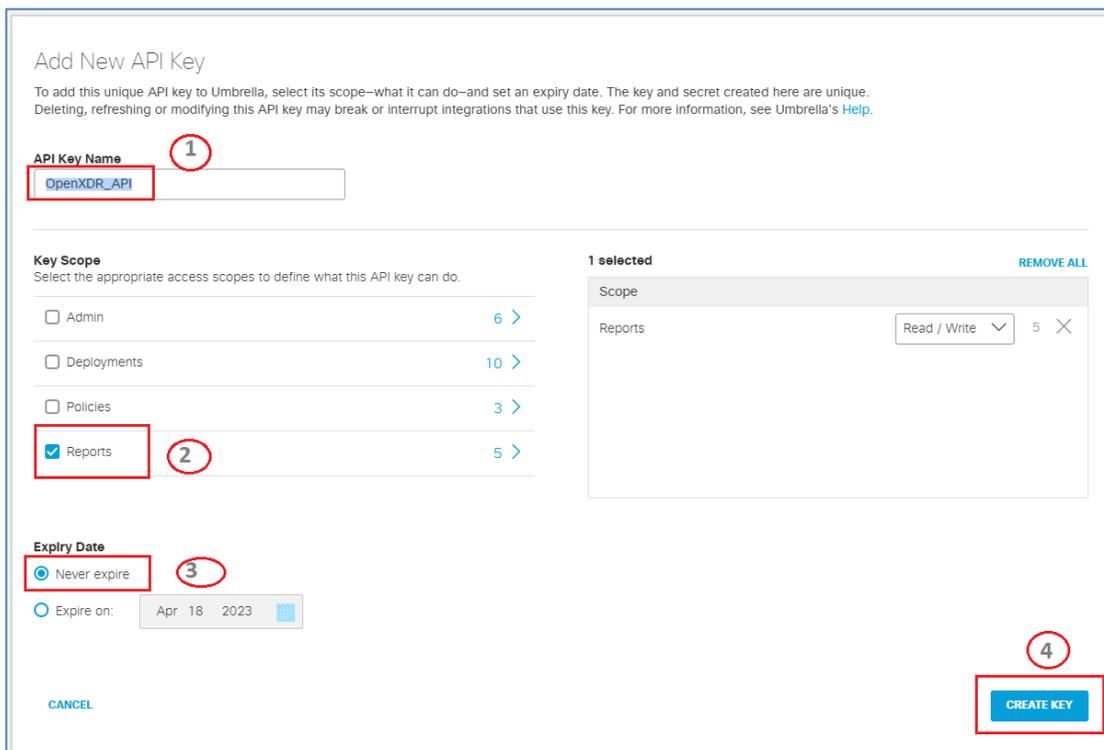
Note:

URL: <https://dashboard.umbrella.com/o/{organizationId}/#/overview>.

1. In the organization’s Umbrella dashboard, navigate to **Admin > API Keys**.
2. In the **API Keys** interface, click **API Keys** and then click **Add**.



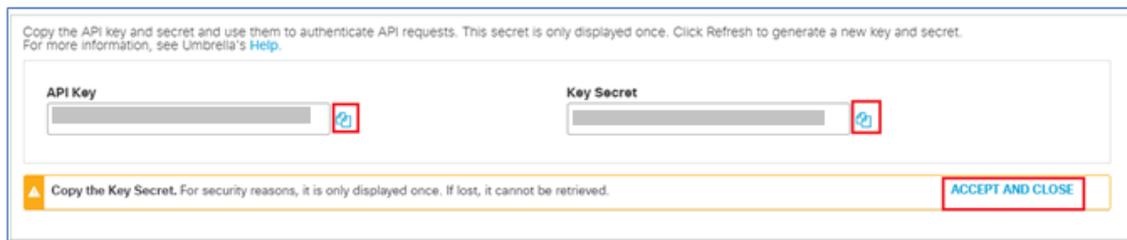
3. In the **Add New API Key** interface, specify the following details.



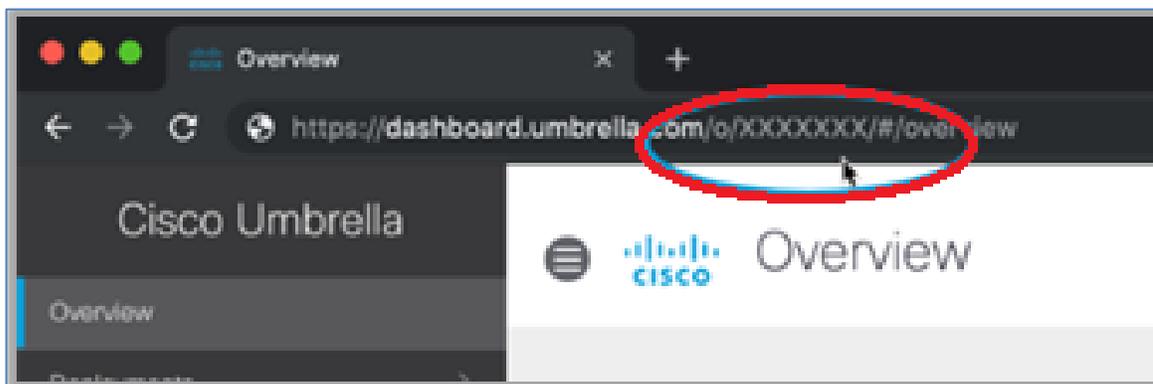
- a. Provide **API key Name** (for example, OpenXDR_API).
 - b. In the **Key Scope** section, select the **Reports** check box.
 - c. In the **Expiry Date** section, choose the **Never** option.
4. After providing the necessary details, click the **CREATE KEY** button to create the API KEY.
 5. Then, copy the **API key** and **Key Secret**, and then click **Accept** and **Close**.

Note:

Make a note of API key and Key secret which will be required while configuring the Integrator.



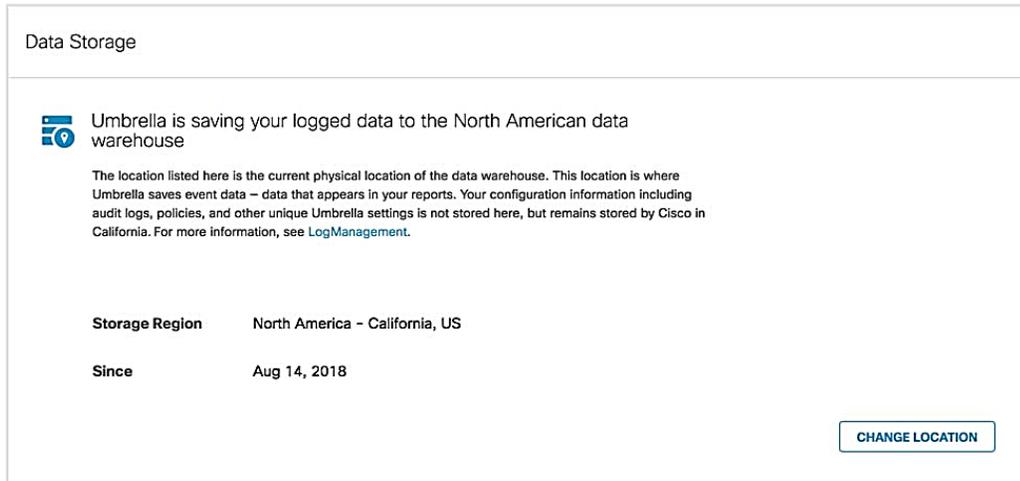
6. To generate a new **API Key** and **Key Secret**, you can either click the **Refresh** button on your existing **API Key** and **Key secret** or delete the existing **API Key** and **Key Secret** and then create a new **API Key** and **Key Secret**.
7. To collect the **Organization Id**, verify the URL in the address bar (after logging in to the appropriate organization) and the URL appears as shown in the following image.



3.1.2 Verifying the API Region

Cisco Umbrella's data warehouse is the virtual location where the instance of Umbrella stores its event data logs. By default, the Umbrella saves your event data logs to Cisco's California location.

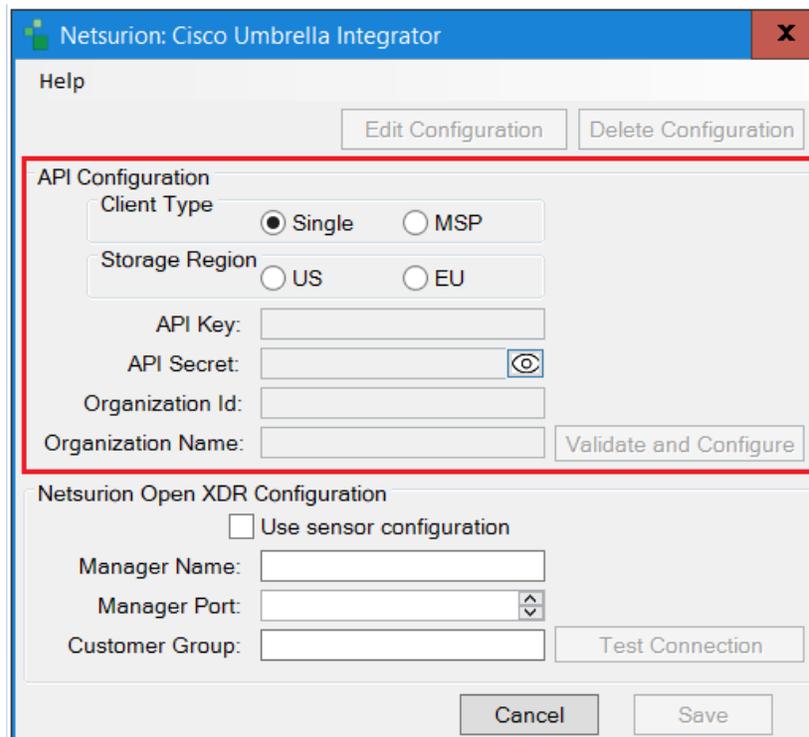
- In the **Umbrella** console, go to **Admin > Log Management > Data Storage** and look up for the **Storage region** to verify your Cisco Umbrella data warehouse location.



3.1.3 Configuring the Integrator

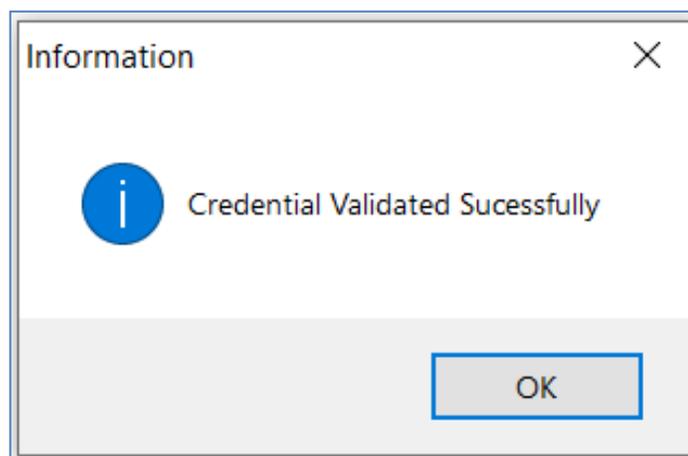
Perform the following procedure to configure the Cisco Umbrella Integrator. After completing the API and permission configurations, run the integrator package **Cisco_Umbrella_Integrator.exe**.

1. In the **Netsurion: Cisco Umbrella Integrator > API Configuration** section, provide the following details.



- a. **Client Type:** Choose the **Client Type** as **Single**
 - b. **Storage Region:** Choose the required **Storage Region**.
 - c. Specify the Cisco Umbrella **API Key**, **API Secret**, **Organization Id** (can be obtained from Cisco Umbrella GUI), **Organization Name**.
2. After providing the necessary details, click the **Validate and Configure** button to verify the credentials.

If the configuration is validated successfully, then an Information window pops-up stating ***Credential validated successfully***.



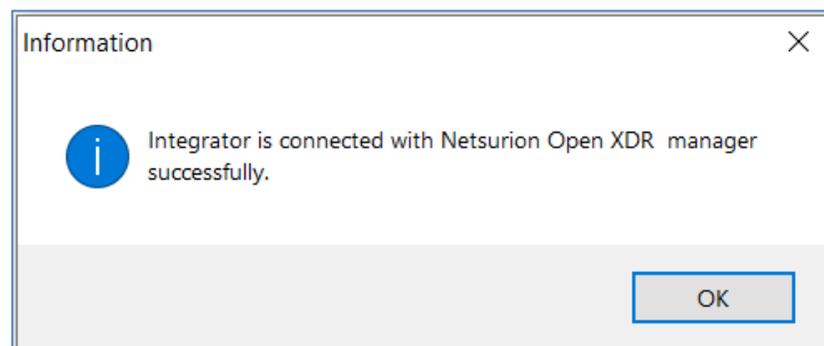
3. In the **Netsurion: Cisco Umbrella Integrator > Netsurion Open XDR Configuration** section, either provide the Manager details to send the logs to a particular Netsurion Open XDR or use the sensor configuration.

To provide the Manager details:

- Specify **Manager Name**, **Manager Port**, and **Customer Group**, and then click **Test Connection** to validate the details.

The screenshot shows a configuration window titled "Netsurion: Cisco Umbrella Integrator". It has a "Help" menu and buttons for "Edit Configuration" and "Delete Configuration". The "API Configuration" section includes radio buttons for "Client Type" (Single selected, MSP unselected) and "Storage Region" (US unselected, EU selected). Below are text boxes for "API Key", "API Secret" (masked with dots and a visibility icon), "Organization Id" (123456), and "Organization Name" (Contoso). A "Validate and Configure" button is next to the Organization Name field. The "Netsurion Open XDR Configuration" section, highlighted with a red box, contains a checkbox for "Use sensor configuration" (unchecked), and text boxes for "Manager Name" (masked), "Manager Port" (14505), and "Customer Group" (Test). A "Test Connection" button is located to the right of the Customer Group field. At the bottom of the window are "Cancel" and "Save" buttons.

If the connection is validated successfully, an Information window pops-up stating ***'Integrator is connected with Netsurion Open XDR manager successfully'***.



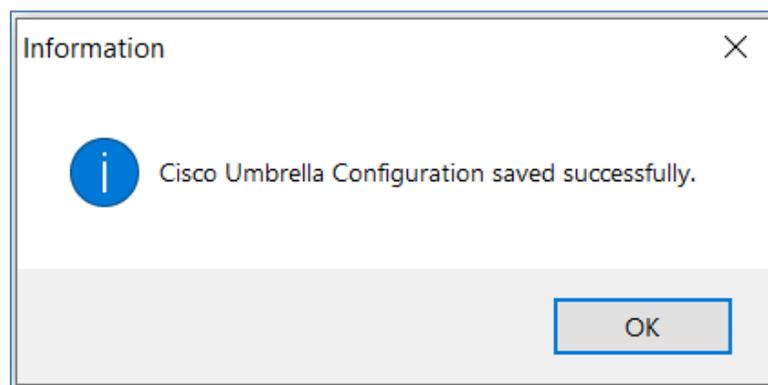
To use the Sensor configuration:

- Select the **Use sensor configuration** check box if you want to use the sensor configuration wherein the Netsurion Open XDR sensor is already installed in the system.

The screenshot shows the 'Netsurion: Cisco Umbrella Integrator' configuration window. It is divided into two main sections: 'API Configuration' and 'Netsurion Open XDR Configuration'. In the 'API Configuration' section, there are radio buttons for 'Client Type' (Single selected, MSP unselected) and 'Storage Region' (US unselected, EU selected). Below these are text fields for 'API Key', 'API Secret' (masked with dots), 'Organization Id' (123456), and 'Organization Name' (Contoso). A 'Validate and Configure' button is present. In the 'Netsurion Open XDR Configuration' section, the 'Use sensor configuration' checkbox is checked and highlighted with a red box. Below it are text fields for 'Manager Name', 'Manager Port', and 'Customer Group', along with a 'Test Connection' button. At the bottom of the window are 'Cancel' and 'Save' buttons.

4. After specifying the required details, click **Save** and the following information window pops-up stating **'Configuration saved successfully'**.

The integrator validates the details, retrieves the organization's information, and saves the configuration, resulting in the successful integration of Cisco Umbrella with Netsurion Open XDR.

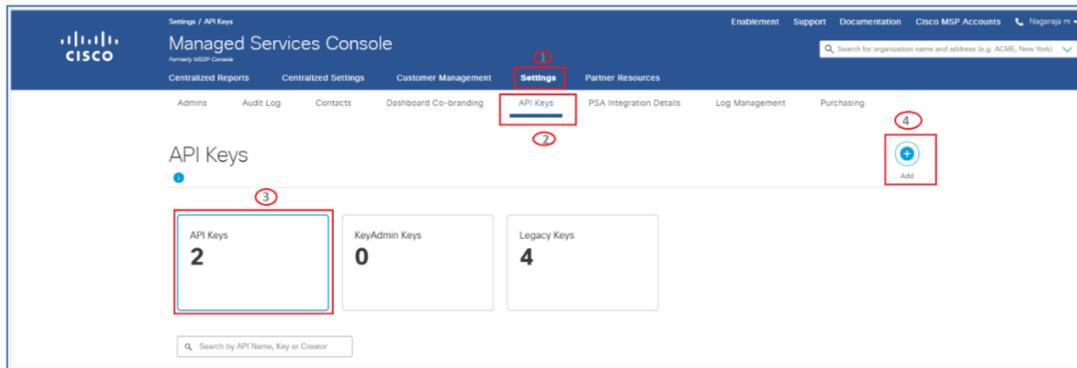


3.2 Integrating Cisco Umbrella for MSP

Perform the following procedures to configure Cisco Umbrella for MSP.

3.2.1 Collecting MSP API Key and API Secret

1. In the **Cisco Umbrella MSP** dashboard, go to **Settings > API Keys** and click **API Keys**, and then click **Add**.



2. In the **Add New API Key** interface, specify the following details.

Add New API Key

To add this unique API key to Umbrella, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key. For more information, see Umbrella's [Help](#).

API Key Name 1

Key Scope
Select the appropriate access scopes to define what this API key can do.

<input type="checkbox"/> Admin	6 >
<input type="checkbox"/> Deployments	10 >
<input type="checkbox"/> Policies	3 >
<input checked="" type="checkbox"/> Reports 2	5 >

1 selected REMOVE ALL

Scope

Reports Read / Write 5 X

Expiry Date

Never expire 3

Expire on:

4

CREATE KEY

[CANCEL](#)

- a. Provide **API Key Name** (for example, OpenXDR_API).
- b. In the **Key Scope** section, select the **Reports** check box.
- c. In the **Expiry Date** section, choose the **Never expire** option.

3. After providing the necessary details click the **CREATE KEY** button to create the API KEY.
4. Then, copy the **API key** and **Key Secret**, and then click **Accept** and **Close**.

Note:

Make a note of API Key and Key Secret which will be required while configuring the Integrator.

Copy the API key and secret and use them to authenticate API requests. This secret is only displayed once. Click Refresh to generate a new key and secret. For more information, see Umbrella's [Help](#).

API Key

Key Secret

Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

ACCEPT AND CLOSE

5. To generate a new **API Key** and **Key Secret**, you can either click the **Refresh** button on your existing **API Key** and **Key Secret** or delete the existing **API Key** and **Key Secret** and then create a new **API Key** and **Key Secret**.

3.2.2 Configuring Netsurion Open XDR Cisco Umbrella Integrator for MSP

After completing the API and permission configurations, run the integrator package **Cisco_Umbrella_Integrator.exe**.

1. In the **Netsurion: Cisco Umbrella Integrator > API Configuration** section, provide the following details.

Netsurion: Cisco Umbrella Integrator

Help

API Configuration

Client Type Single MSP

Storage Region US EU

API Key:

API Secret:

Organization Id:

Organization Name:

Netsurion Open XDR Configuration

Use sensor configuration

Manager Name:

Manager Port: 14505

Customer Group:

- a. **Client Type:** Choose the **Client Type** as **MSP**.
 - b. Specify the Cisco Umbrella **API Key, Key Secret**.
2. After providing the necessary details, click the **Validate and Configure** button to verify the credentials and configure the Organization.

If the credentials are successfully validated, a window appears displaying the list of organization.

3. Select the organizations based on the storage region that need to be configured.

Note:

The maximum number of organizations that can be selected is limited to 5.

Netsurion: Cisco Umbrella Integrator

Note: Maximum limit is 5 organizations.

Select organization in US storage region

<input checked="" type="checkbox"/>	Org_Name:	Org_ID:	
<input type="checkbox"/>	Org_Name:	Org_ID:	

Select organization in EU storage region

Back Next

4. Provide the **customer group** name for each organization and click **Finish**.

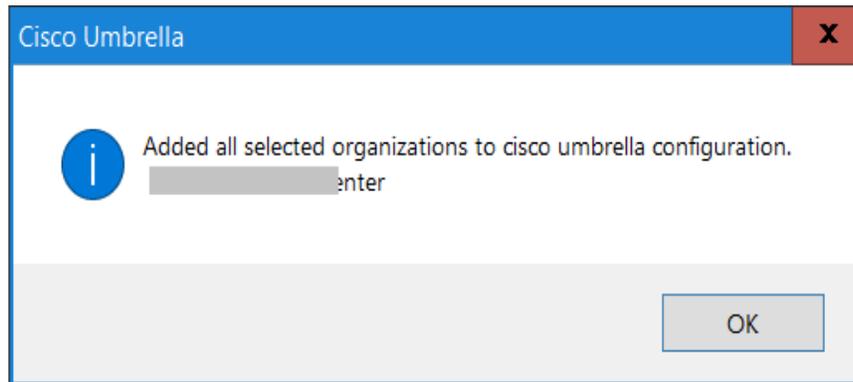
Netsurion: Cisco Umbrella Integrator

Provide group name for each organization

enter Test

Back Finish

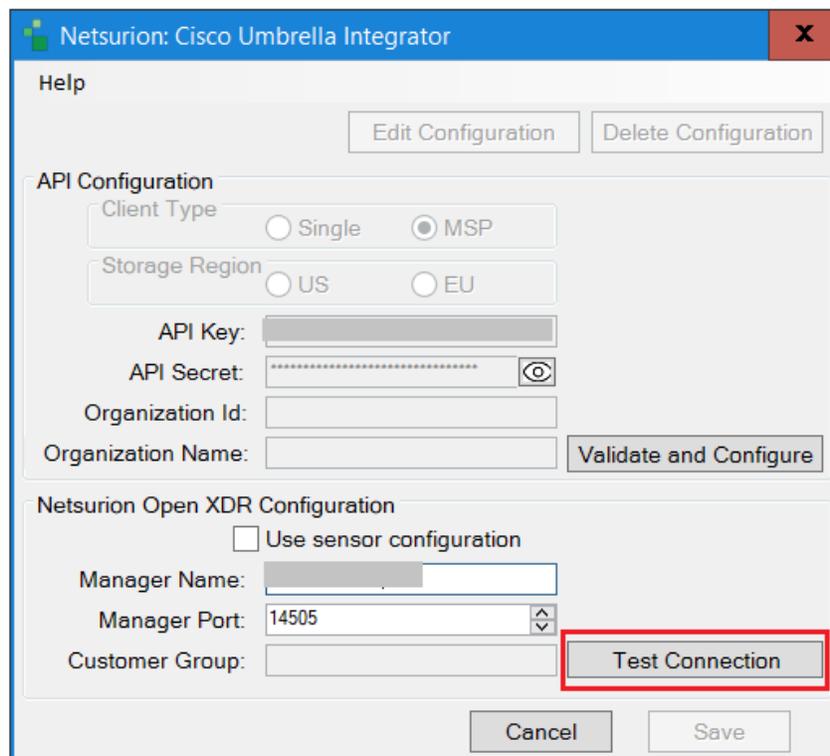
An Information window pops-up displaying *Added all selected organizations to cisco umbrella configuration.*



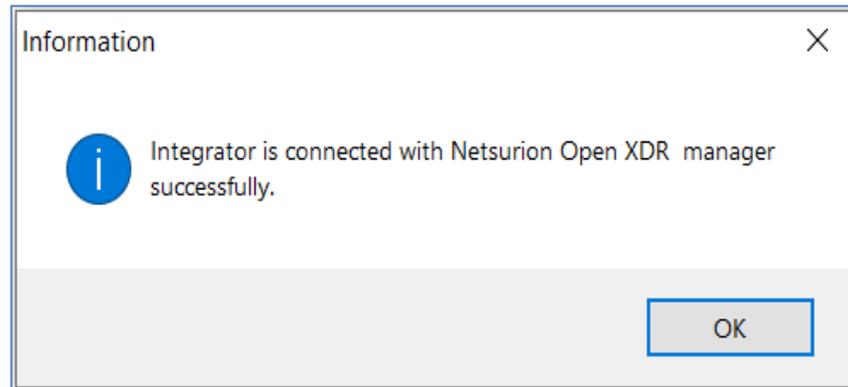
5. In the **Netsurion: Cisco Umbrella Integrator** > **Netsurion Open XDR Configuration** section, either provide the Manager details to send the logs to a particular Netsurion Open XDR or use the sensor configuration.

To provide the Manager details:

- Specify **Manager Name**, **Manager Port**, and **Customer Group**, and then click **Test Connection** to validate the details.

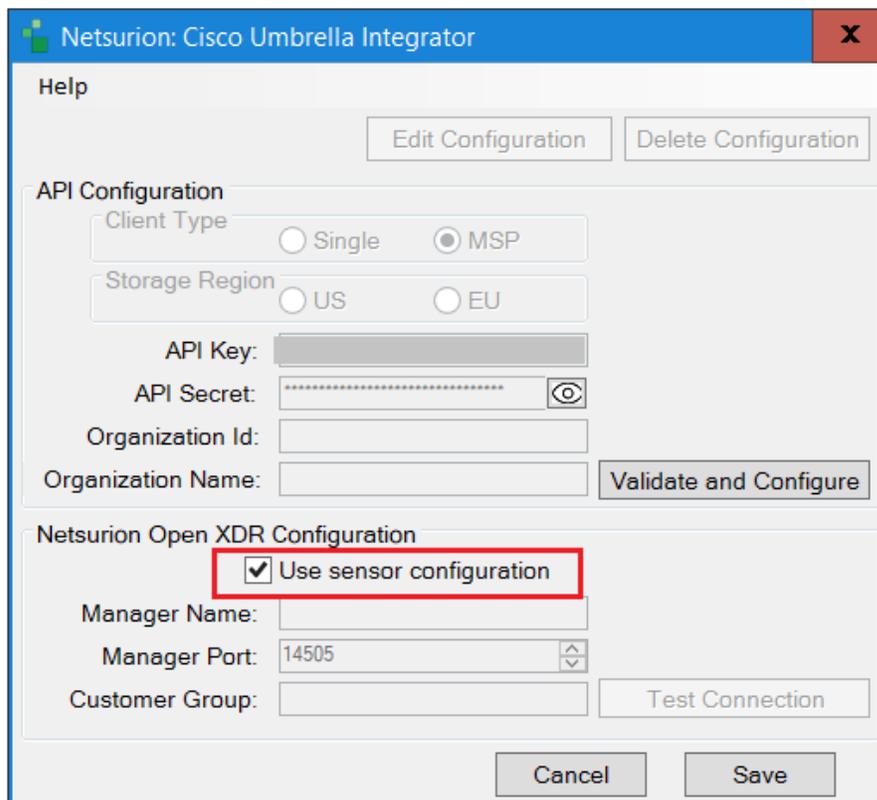


If the connection is validated successfully, an Information window pops-up stating *'Integrator is connected with Netsurion Open XDR manager successfully'*.



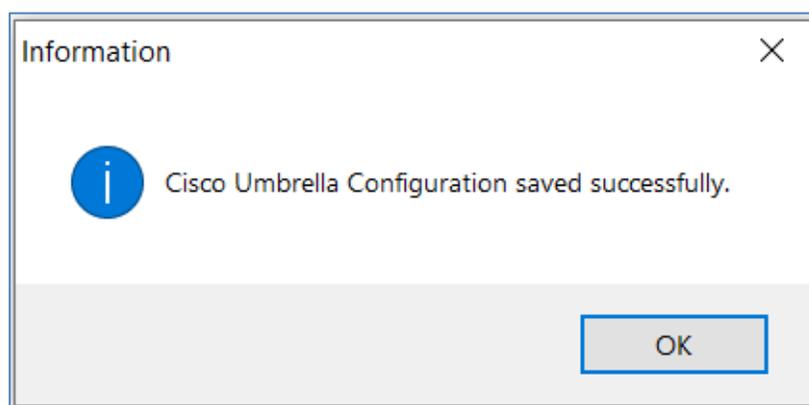
To use the Sensor configuration:

- Select the **Use sensor configuration** check box if you want to use the sensor configuration wherein the Netsurion Open XDR sensor is already installed in the system.



- After specifying the required details, click **Save** and the following information window pops-up stating '*Configuration saved successfully*'.

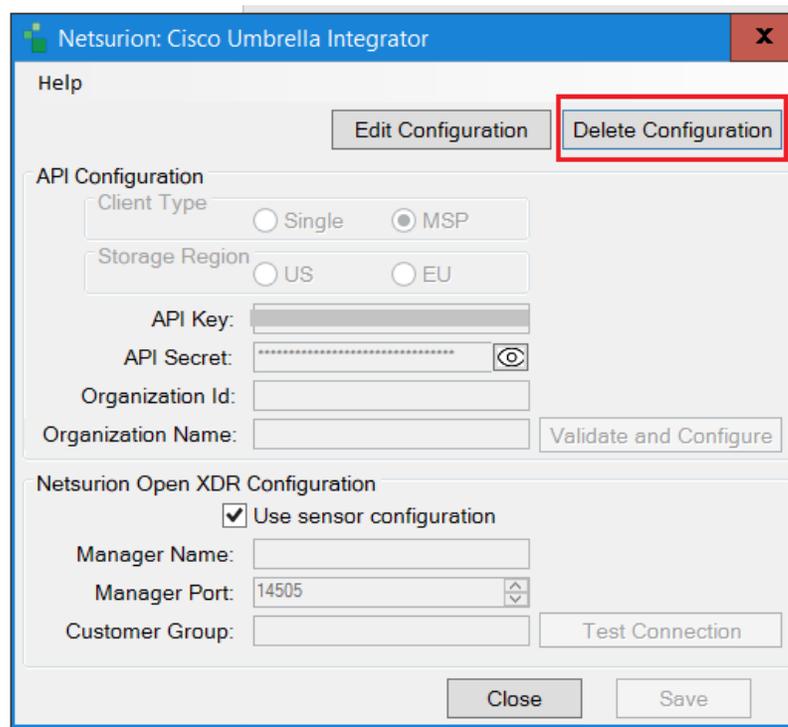
The integrator validates the details, retrieves the organization's information, and saves the configuration, resulting in the successful integration of Cisco Umbrella with Netsurion Open XDR.



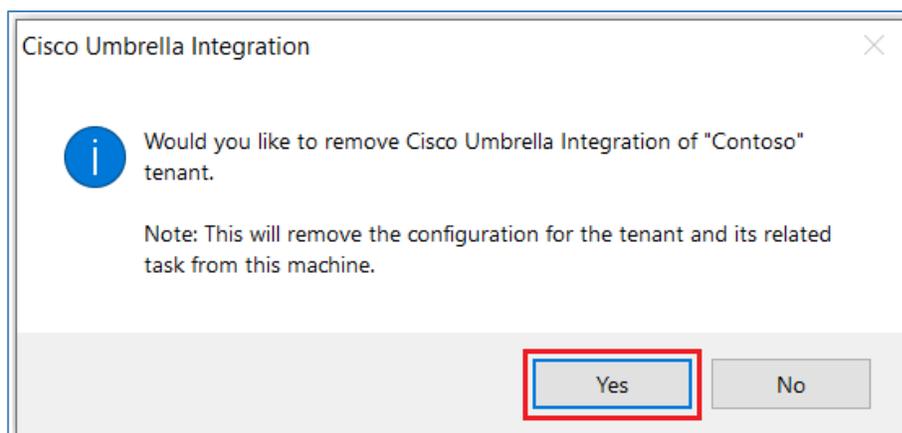
3.3 Deleting the Configuration of Cisco Umbrella

Perform the following steps in case you require to delete the existing configuration of the Cisco Umbrella integrator.

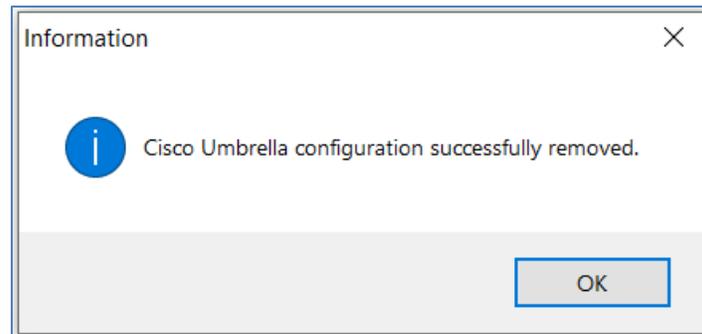
1. Run the Integrator to launch the configuration settings.
2. In the **Cisco Umbrella Integrator** window, click **Delete Configuration** to delete the existing configuration details.



3. An information window pops up to confirm the deletion of the existing configuration. Click **Yes** to proceed.



- An Information window pops-up confirming the successful deletion. Click **OK**.



4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integration in Netsurion Open XDR.

The Data Source Integration package contains the following files for **Cisco Umbrella**.

- Categories_Cisco Umbrella.iscat
- Alerts_Cisco Umbrella.isalt
- Reports_Cisco Umbrella.etcrx
- KO_Cisco Umbrella.etko
- Dashboards_Cisco Umbrella.etwd

Note

Refer the [How To Configure DSI](#) guide for the procedures to configure the above DSIs in Netsurion Open XDR.

4.1 Alerts

Name	Description
Cisco Umbrella: Threat has been blocked	Generated when an event, such as DNS, IP address, firewall, or proxy, is blocked by Cisco Umbrella.

4.2 Reports

Name	Description
Cisco Umbrella - Proxy activities	Provides a summary of all the proxy entries by Cisco Umbrella. It contains information such as the URL access by the user, URL category, threat name, timestamp of activity, threat score, action taken on the event, and more.
Cisco Umbrella - DNS activities	Provides a summary of all the DNS entries by Cisco Umbrella. It contains information such as the URL access by the user, URL category, timestamp of activity, action taken on the event, and more.
Cisco Umbrella - Firewall activities	Provides a summary of all the Firewall entries by Cisco Umbrella. It contains information such as the source IP address, destination IP address, source port, destination port, timestamp of activity, action taken on the event, and more.
Cisco Umbrella - IP activities	Provides a summary of all the IP address entries by Cisco Umbrella. It contains information such as the source IP address, destination IP address, source port, destination port, timestamp of activity, action taken on the event, and more.

4.3 Dashboards

Name	Description
Cisco Umbrella - Security activity by category	Displays the data about all security activities based on all different categories.
Cisco Umbrella - Security activity by source IP	Displays the data about all security activities based on source IP.

4.4 Saved Searches

Name	Description
Cisco Umbrella - Proxy activities	Provides a summary of all the proxy entries by Cisco Umbrella. It contains information such as the URL access by the user, URL category, threat name, timestamp of activity, threat score, action taken on the event, and more.
Cisco Umbrella - DNS activities	Provides a summary of all the DNS entries by Cisco Umbrella. It contains information such as the URL access by the user, URL category, timestamp of activity, action taken on the event, and

	more.
Cisco Umbrella - Firewall activities	<p>Provides a summary of all the Firewall entries by Cisco Umbrella.</p> <p>It contains information such as the source IP address, destination IP address, source port, destination port, timestamp of activity, action taken on the event, and more.</p>
Cisco Umbrella - IP activities	<p>Provides a summary of all the IP address entries by Cisco Umbrella.</p> <p>It contains information such as the source IP address, destination IP address, source port, destination port, timestamp of activity, action taken on the event, and more.</p>

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

<https://www.netsurion.com/support>