Integration Guide

Integrate Cisco Meraki Cloud Management with Netsurion Open XDR

Publication Date

May 19, 2023

Abstract

This guide provides instructions to configure and integrate Cisco Meraki Cloud Management with Netsurion Open XDR to retrieve its logs and forward it 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 Meraki Cloud Management and Netsurion Open XDR 9.3 or later.

Audience

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

Table of Contents

1 Overview

Cisco Meraki cloud-based management provides centralized visibility and control over Meraki's wired & wireless networking hardware, without the complexity of wireless controllers or overlay management systems. Integrated with Meraki's entire product portfolio, cloud management provides feature rich, scalable, and intuitive centralized management for networks of any size.

Netsurion Open XDR manages logs from Cisco Meraki Cloud Management. The alerts, reports, dashboard, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities of Cisco Meraki Cloud Management.

2 Prerequisites

- PowerShell 5.0 must be installed on host system or server.
- User should have administrative privilege on the desired host system or server where the Integrator will be installed to run Powershell.
- Admin access to Meraki platform.
- The Data Source Integration package.

Note

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

- Existing legacy version of the Cisco Meraki integrator must be uninstalled.

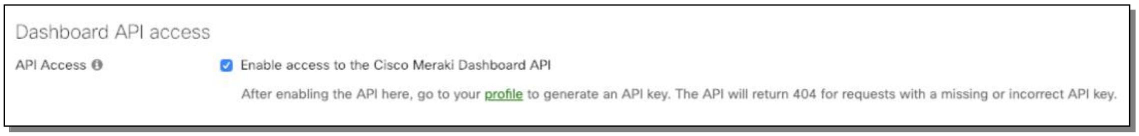
Note

Refer to the How to Uninstall guide to uninstall the Cisco Meraki Integrator.

3 Integrating Cisco Meraki Cloud Management with Netsurion Open XDR

3.1 Enabling the Dashboard API

1. Log in to the Cisco Meraki Cloud Management dashboard and navigate to **Organization** > **Configure** > **Settings.**
2. In **Dashboard API Access** section, select the **Enable access to the Cisco Meraki Dashboard API** check box to enable the Dashboard API access.



Dashboard API access

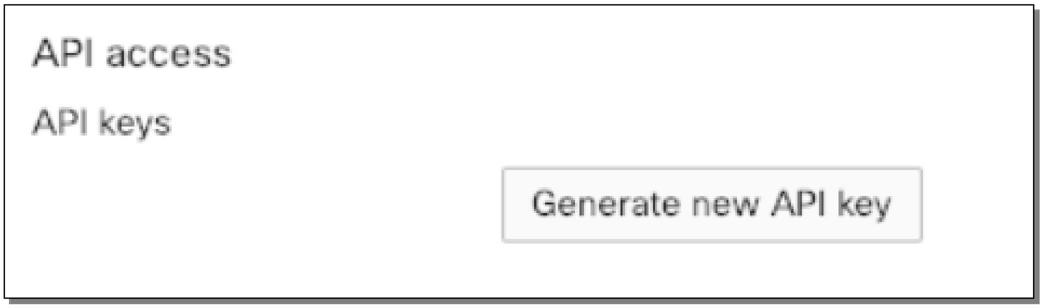
API Access ⓘ ☑ Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to your profile to generate an API key. The API will return 404 for requests with a missing or incorrect API key.

3.2 Generating API Key

In the Cisco Meraki Cloud Management interface, navigate to the user profile page to generate an API key.

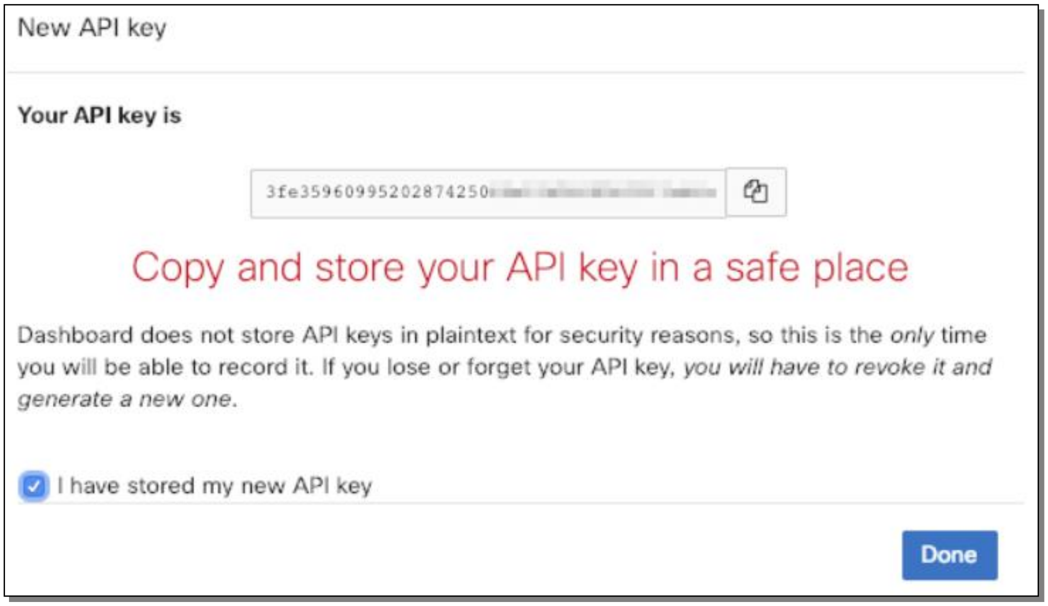
1. Click the username icon in the top right corner and select **My Profile.**
2. In the API access section, click **Generate new API key.**



API access

API keys

3. A window containing the unique API key for your individual user is displayed. Copy the key in a notepad (as this will be required in the later procedure).
4. Select the **I have stored my new API key** check box and click **Done**.



New API key

Your API key is

3fe35960995202874250[redacted]

Copy and store your API key in a safe place

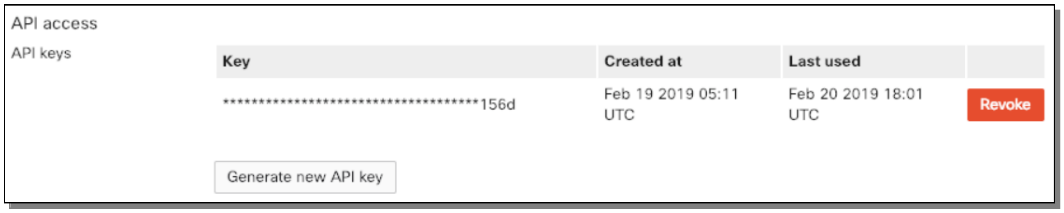
Dashboard does not store API keys in plaintext for security reasons, so this is the *only* time you will be able to record it. If you lose or forget your API key, *you will have to revoke it and generate a new one*.

☑ I have stored my new API key

5. The page refreshes and in the API access section, the newly generated API key will be displayed.

Note

Only the last 4 digits of the key will be displayed for security purpose.



API access

API keys

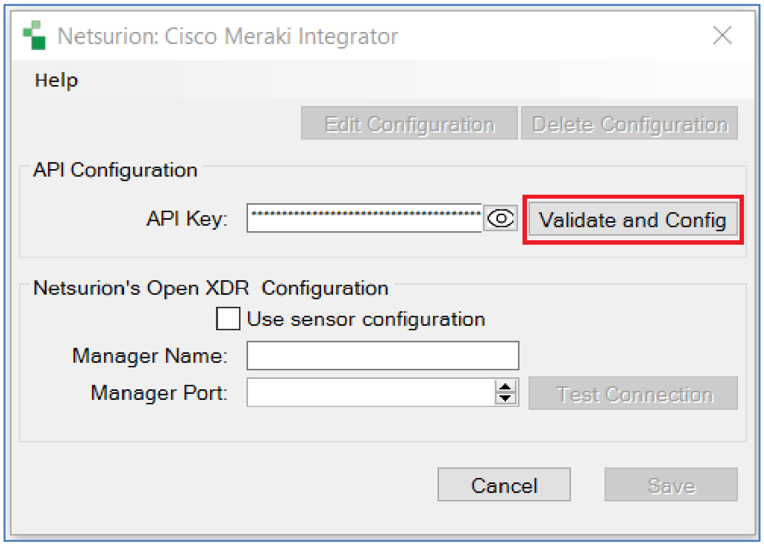
Key	Created at	Last used	
**************************************156d	Feb 19 2019 05:11 UTC	Feb 20 2019 18:01 UTC	Revoke

3.3 Configuring Netsurion Open XDR Cisco Meraki Cloud Management Integrator

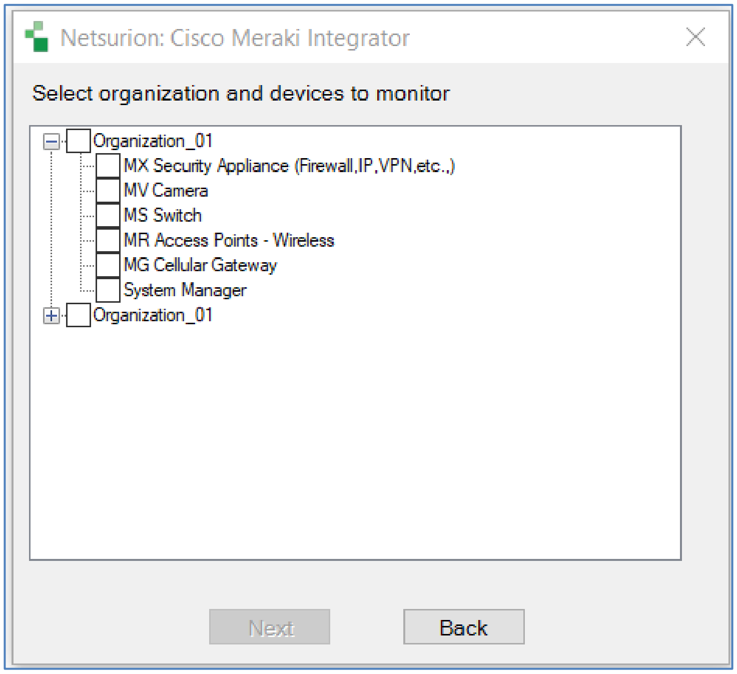
1. Run the **Netsurion: Cisco Meraki Integrator** package.

> **Note**
>
> To get the **Cisco Meraki Integrator** package, contact your Netsurion Account Manager.

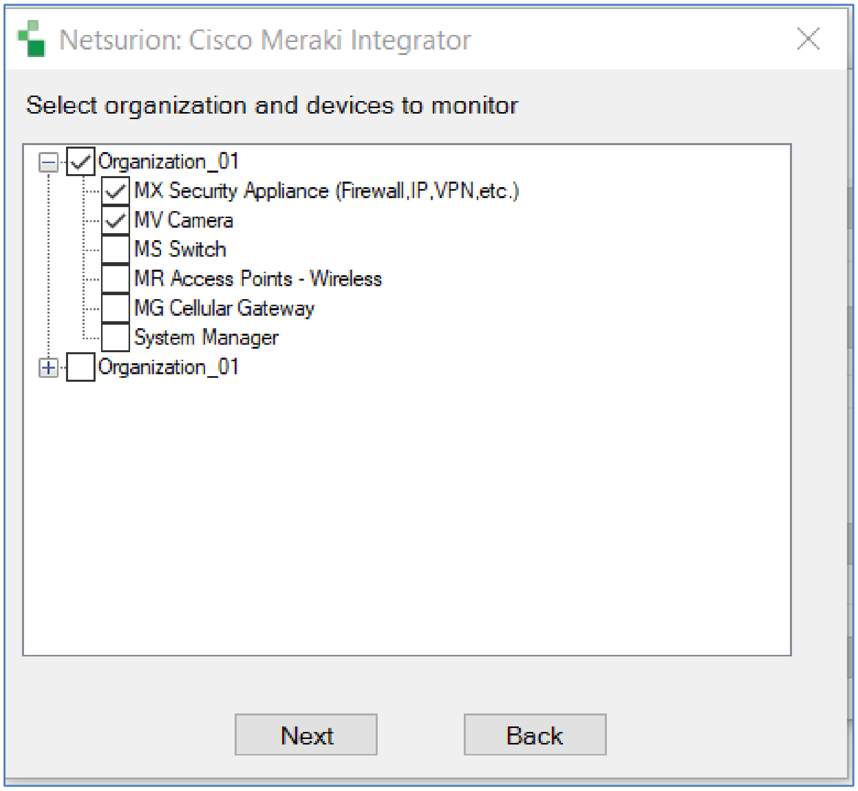
2. In the **Cisco Meraki Integrator** window > **API Configuration** section, enter the API key, that is, paste the API Key information which was copied earlier, and click **Validate and Config** to validate and configure the credentials.



If the configuration is validated successfully, another interface with the organization list will be displayed.


Netsurion: Cisco Meraki Integrator
Select organization and devices to monitor
□ Organization_01
□ MX Security Appliance (Firewall,IP,VPN,etc.,)
□ MV Camera
□ MS Switch
□ MR Access Points - Wireless
□ MG Cellular Gateway
□ System Manager
□ Organization_01
Next
Back

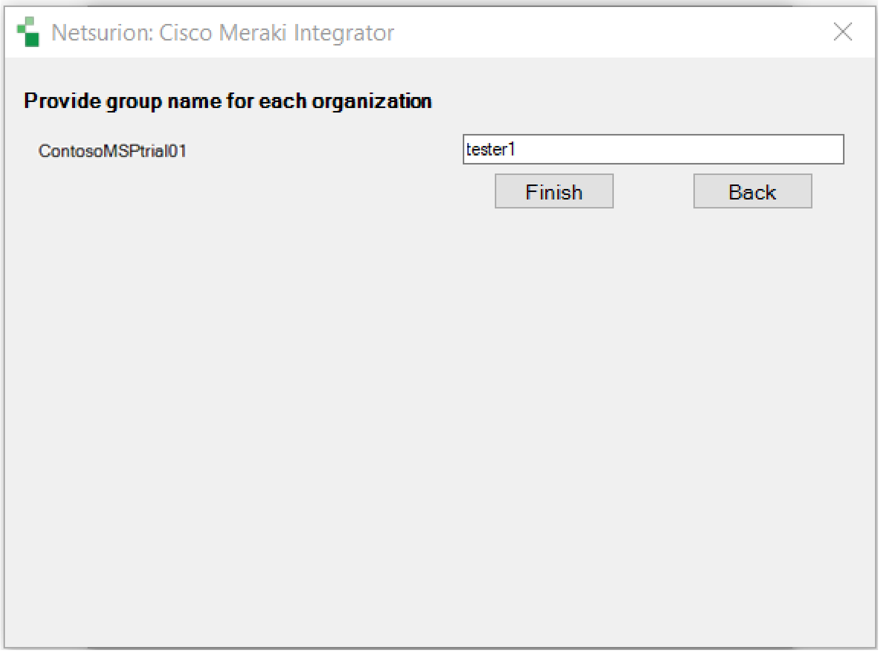
3. Select the organizations and the device types that require configuration.



Select organization and devices to monitor

- ☑ Organization_01
  - ☑ MX Security Appliance (Firewall,IP,VPN,etc.)
  - ☑ MV Camera
  - □ MS Switch
  - □ MR Access Points - Wireless
  - □ MG Cellular Gateway
  - □ System Manager
- □ Organization_01

4. Click **Next** and configure the **group name** for the selected organizations.



Provide group name for each organization

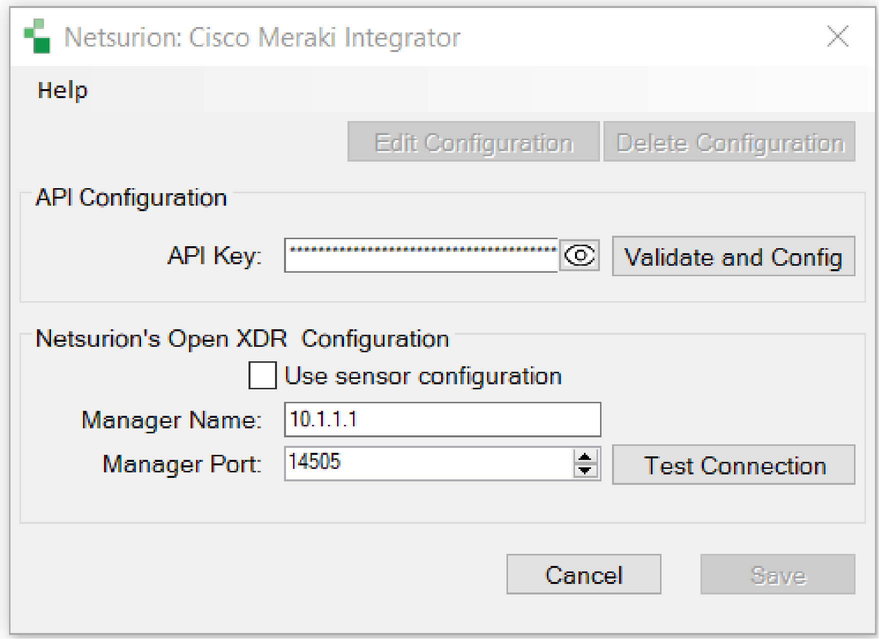
ContosoMSPtrial01 tester1

5. The information window pops-up displaying ***All the organizations have been successfully configured***.

6. In the **Cisco Meraki Integrator** > **Netsurion's 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 the details for **Manager Name**, **Manager Port**, and click **Test Connection** to validate the details.



Netsurion: Cisco Meraki Integrator

API Key: ••••••••••••••••••••••••••••••••••••••

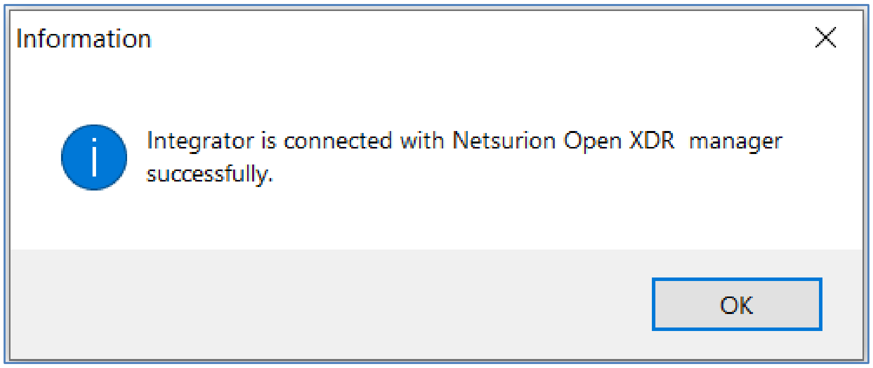
Netsurion's Open XDR Configuration

□ Use sensor configuration

Manager Name: 10.1.1.1

Manager Port: 14505

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

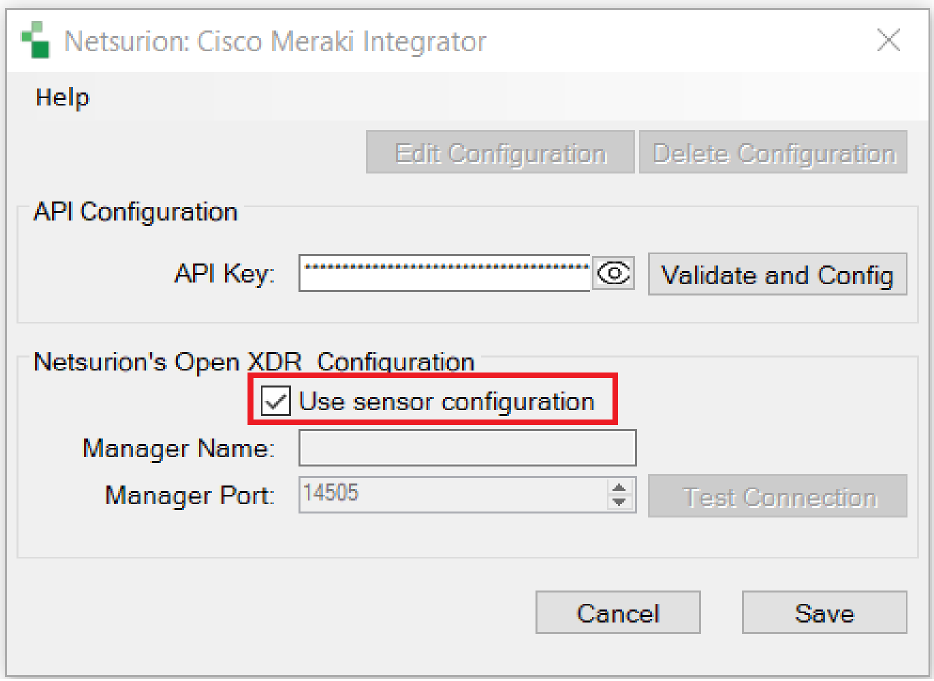


Information

Integrator is connected with Netsurion Open XDR manager successfully.

To use the Sensor configuration:

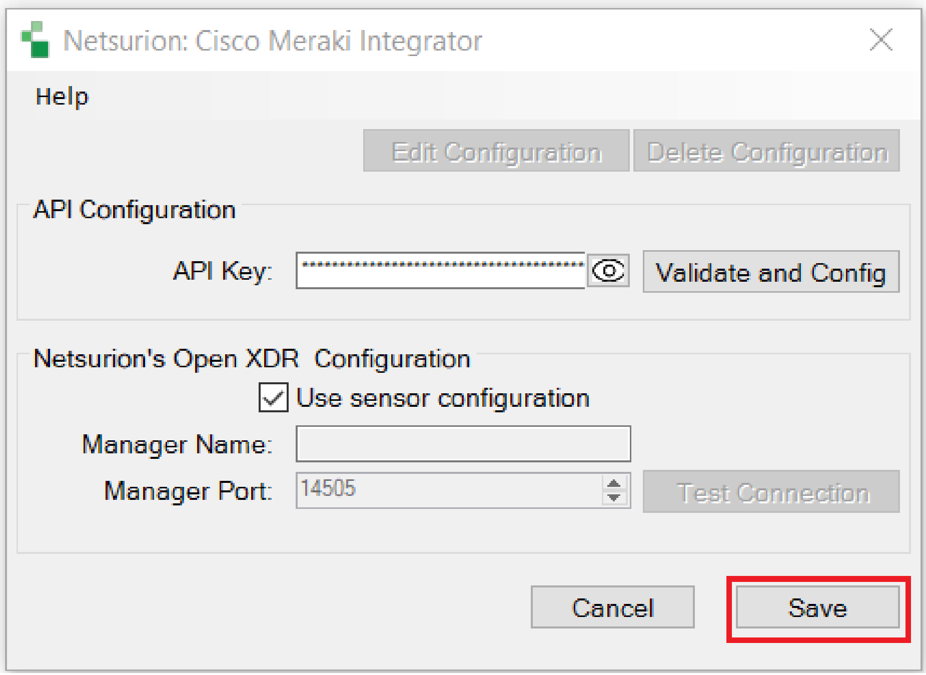
- Select the **Use sensor configuration** check box if you want to use the sensor configuration where the Netsurion Open XDR sensor is already installed in the system.



☑ Use sensor configuration

Manager Port: 14505

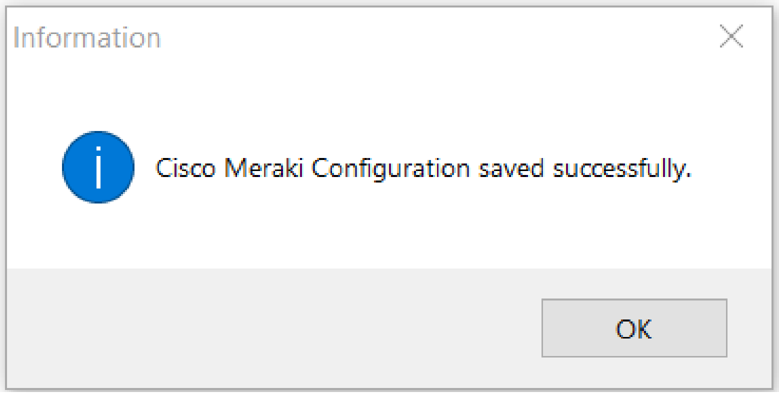
7. After providing the required details, click **Save**.



☑ Use sensor configuration

Manager Port: 14505

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



Cisco Meraki Configuration saved successfully.

4 Data Source Integrations (DSIs) in Netsurion Open XDR

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

The Data Source Integrations package contains the following files for the Cisco Meraki Cloud Management.

- Categories_Cisco Meraki CM.iscat
- Alerts_ Cisco Meraki CM.isalt
- Reports_ Cisco Meraki CM.etcrx
- KO_ Cisco Meraki CM.etko
- Dashboards_ Cisco Meraki CM.etwd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

Data Source Integrations Details

4.1 Alerts

Name	Description
Cisco Meraki CM: Authentication failure	Generated whenever a failure to connect to the AD server is detected in Meraki.
Cisco Meraki CM: Wireless attack detected	Generated whenever a suspicious wireless attack is detected in Meraki.
Cisco Meraki CM: Rogue DHCP detected	Generated whenever rogue DHCP is detected in Meraki.
Cisco Meraki CM: Switch loop detected	Generated whenever a loop on switch is detected in Meraki.
Cisco Meraki CM: Switch mac flap detected	Generated whenever a MAC flap on switch is detected in Meraki.
Cisco Meraki CM: Wireless packet flood detected	Generated whenever a packet flood on wireless is detected in Meraki.
Cisco Meraki CM: Wireless multiple DHCP servers detected	Generated whenever a multiple DHCP servers on wireless is detected in Meraki.

4.2 Reports

Name	Description
Cisco Meraki CM - Login failure activities	Provides information about all the authentication activities in Meraki.
Cisco Meraki CM - VPN connection activities	Provides information about all VPN connection activities.
Cisco Meraki CM - Port role change actions	Provides information about port role change.
Cisco Meraki CM - Successful login activities	Provides information about all the successful authentications.
Cisco Meraki CM - WiFi authentication activities	Provides information about all WPA authentications.
Cisco Meraki CM - DHCP activities	Provides information about all DHCP activities.

Cisco Meraki CM - Intrusion detection activities	Provides information about intrusion detection activities.
Cisco Meraki CM - Content filtering blocked URL	Provides information about blocked content filtering activities.
Cisco Meraki CM - Device activities	Provides information about the Meraki's Enterprise Mobility Management.

4.3 Dashboards

Name	Description
Cisco Meraki CM - Authentication activities	Displays the authentication activities.
Cisco Meraki CM - Content blocking by filter	Displays the device blocked by content filter.
Cisco Meraki CM - WiFi authorization actions	Displays the Wi-Fi authorization actions.
Cisco Meraki CM – 802.1x associated actions	Displays the associated actions.
Cisco Meraki CM - VPN Activities	Displays the VPN activities.
Cisco Meraki CM - Port role change activities by port number	Displays the port change activities.
Cisco Meraki CM - Events by device type	Displays the events by device type.

4.4 Saved Searches

Name	Description
Cisco Meraki CM - Authentication activities	Provides information about all the authentication failures detected in Meraki
Cisco Meraki CM - WiFi authentication activities	Provides information about all the WPA deauthentications detected in Meraki.
Cisco Meraki CM - VPN connection activities	Provides information about all VPN connection activities.
Cisco Meraki CM - Port role changes	Provides information about port role changes.
Cisco Meraki CM - WiFi association activities	Provides information about all WPA association and disassociation activities.

Cisco Meraki CM - DHCP activities	Provides information about all DHCP activities.
Cisco Meraki CM - Intrusion detection activities	Provides information about intrusion detection activities.
Cisco Meraki CM - Content blocked by filter	Provides information about blocked content filtering activities.
Cisco Meraki CM - Device activities	Provides information about the Meraki's Enterprise Mobility Management.

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-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support