



## Integration Guide

# Integrate Lacework With Netsurion Open XDR

### Publication Date

May 08, 2023

## Abstract

This guide provides instructions to configure and integrate Lacework with Netsurion Open XDR to retrieve its logs via API integration 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 Lacework and Netsurion Open XDR 9.3 or later.

## Audience

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

# Table of Contents

- 1 Overview .....4
- 2 Prerequisites .....4
- 3 Integrating Lacework with Netsurion Open XDR.....4
  - 3.1 Generate API Keys ..... 4
  - 3.2 Configuring Netsurion Open XDR Lacework Integrator..... 5
- 4 Data Source Integrations (DSIs) In Netsurion Open XDR .....9
  - 4.1 Alerts..... 9
  - 4.2 Reports..... 10
  - 4.3 Dashboards ..... 10
  - 4.4 Saved Search ..... 10

## 1 Overview

Lacework is a cloud security platform that offers a range of features and capabilities to help organizations secure their cloud workloads across platforms like Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and multicloud and hybrid environments. It includes misconfiguration alerts and compliance monitoring along with corresponding details per application. Lacework delivers end-to-end visibility into what's happening across your cloud environment, including detecting threats, vulnerabilities, misconfigurations, and unusual activity. Logs can be forwarded to Netsurion Open XDR using the Lacework API integration.

Netsurion Open XDR manages logs from Lacework. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities of Lacework cloud security.

## 2 Prerequisites

- Lacework CLI (Command Line Interface).
- PowerShell version 5.0 and above must be installed.
- Admin privilege in the Lacework console.
- API Key for the Lacework account administrators.

**Note:**

API Keys can be created by Lacework account administrators via the Lacework console.

- The Data Source Integrator package.

**Note:**

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

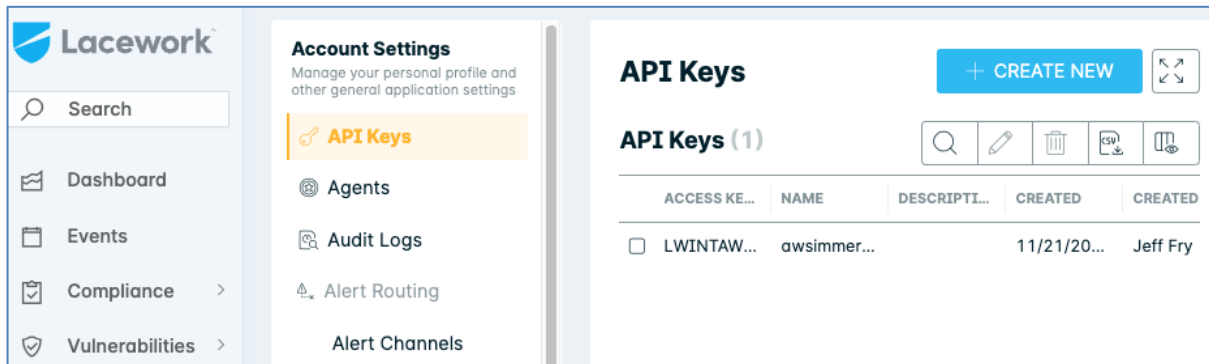
## 3 Integrating Lacework with Netsurion Open XDR

### 3.1 Generate API Keys

Perform the following procedure to generate the Lacework API keys in the Lacework console:

1. Log in to your Lacework account at Lacework Security.
2. Go to **Settings > Configuration > API keys** and click **Add New**.
3. In the new API key creation interface, enter the API key name and an optional description, and then click **Save**.

- Click the ellipsis icon and download the generated API key file.

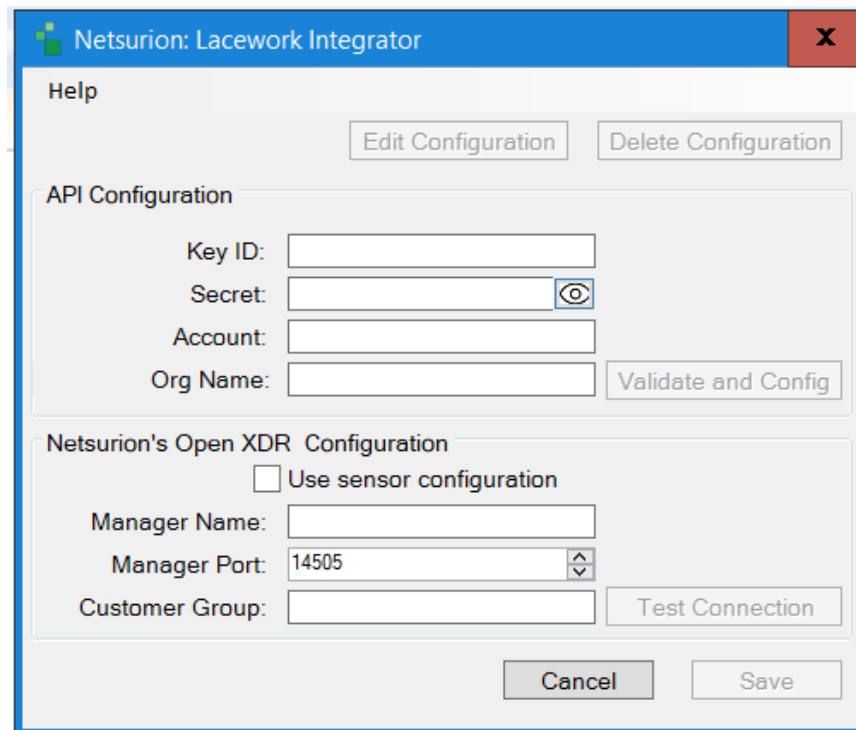


## 3.2 Configuring Netsurion Open XDR Lacework Integrator

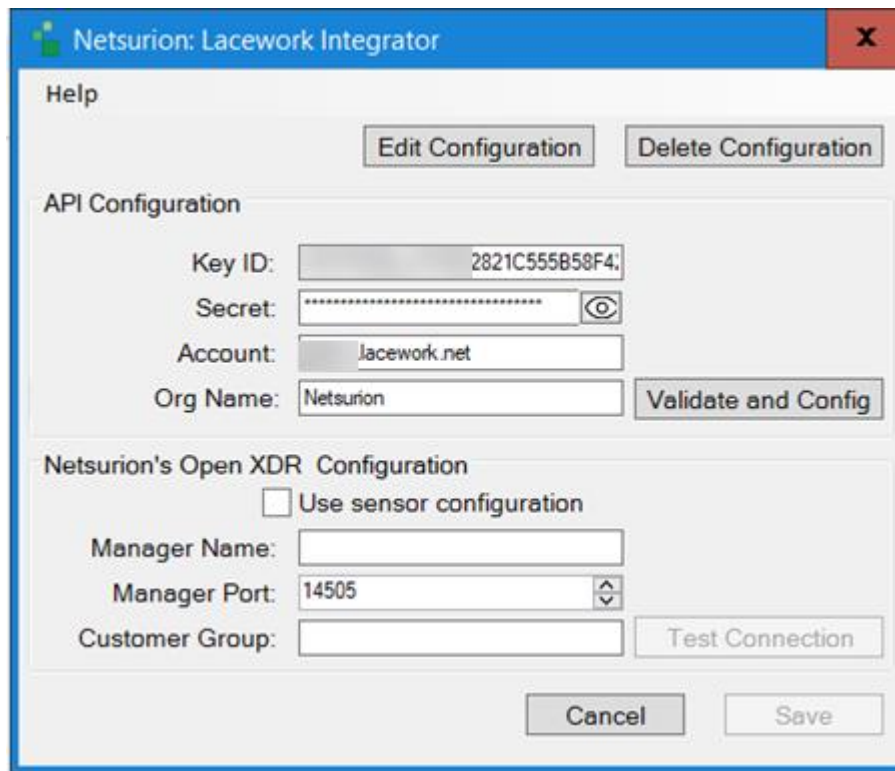
- Run the **Netsurion: Lacework Integrator** package.

### Note:

To get the Lacework Integrator package, contact your Netsurion Account Manager



2. In the **Netsurion: Lacework Integrator** window > **API Configuration** section, enter the details for **Key ID**, **Secret**, **Account**, **Org Name**, and then click **Validate and Config** to validate and configure the details.



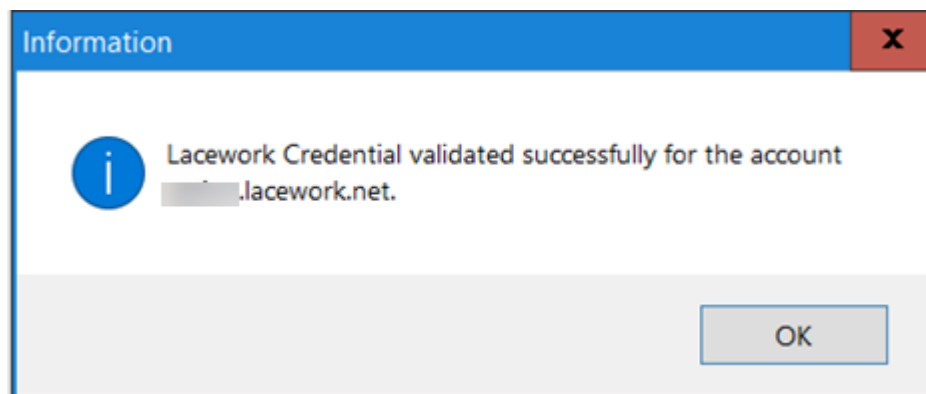
The screenshot shows the 'Netsurion: Lacework Integrator' window. The 'API Configuration' section contains the following fields and buttons:

- Key ID:** 2821C555B58F4;
- Secret:** [Redacted] (with an eye icon to toggle visibility)
- Account:** lacework.net
- Org Name:** Netsurion
- Buttons:** Edit Configuration, Delete Configuration, Validate and Config

The 'Netsurion's Open XDR Configuration' section contains the following fields and buttons:

- ☐ Use sensor configuration
- Manager Name:** [Empty field]
- Manager Port:** 14505
- Customer Group:** [Empty field]
- Buttons:** Test Connection, Cancel, Save

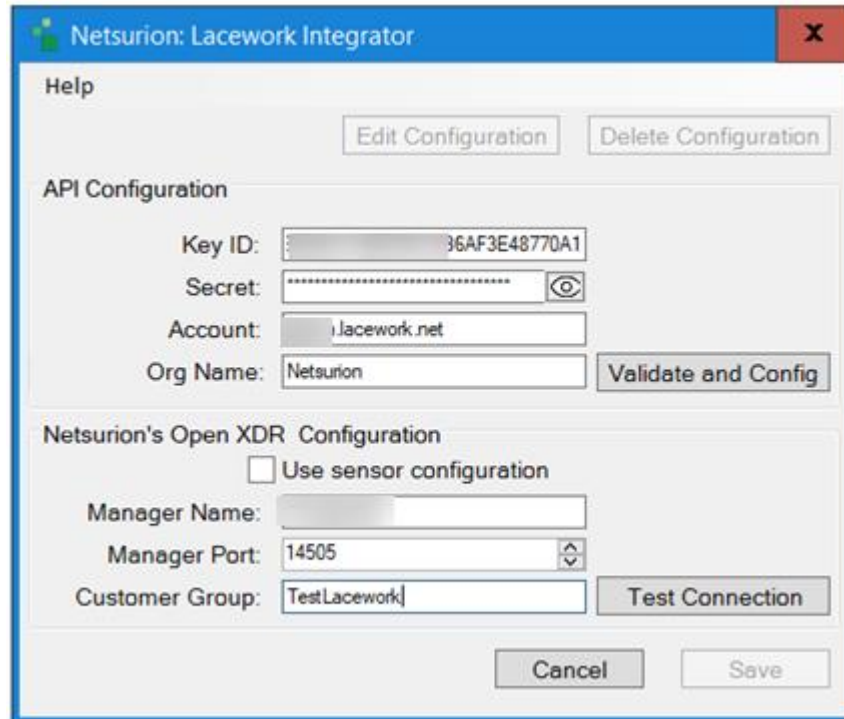
If the configuration is validated successfully, then an Information window pops-up stating '**Lacework Credential validated successfully for the account <Account Name>**'.



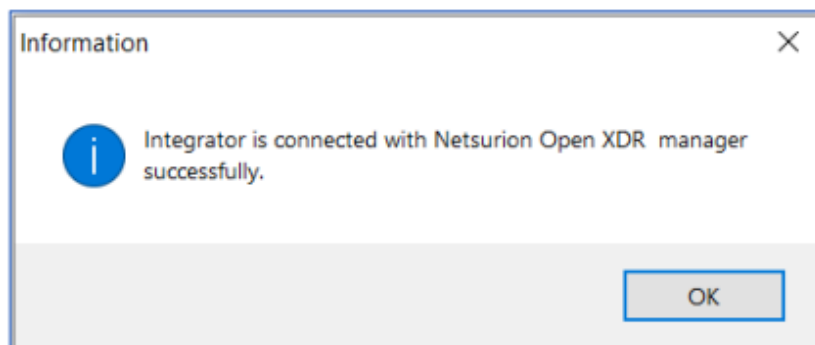
3. In the **Netsurion: Lacework Integrator > Netsurion's Open XDR Configuration** section, either provide the Manager details to send the logs to a particular Netsurion's Open XDR or use the sensor configuration.

**To provide the Manager details:**

- Specify the **Manager Name**, **Manager Port**, and **Manager group** fields, and then click **Test Connection** to validate the info.

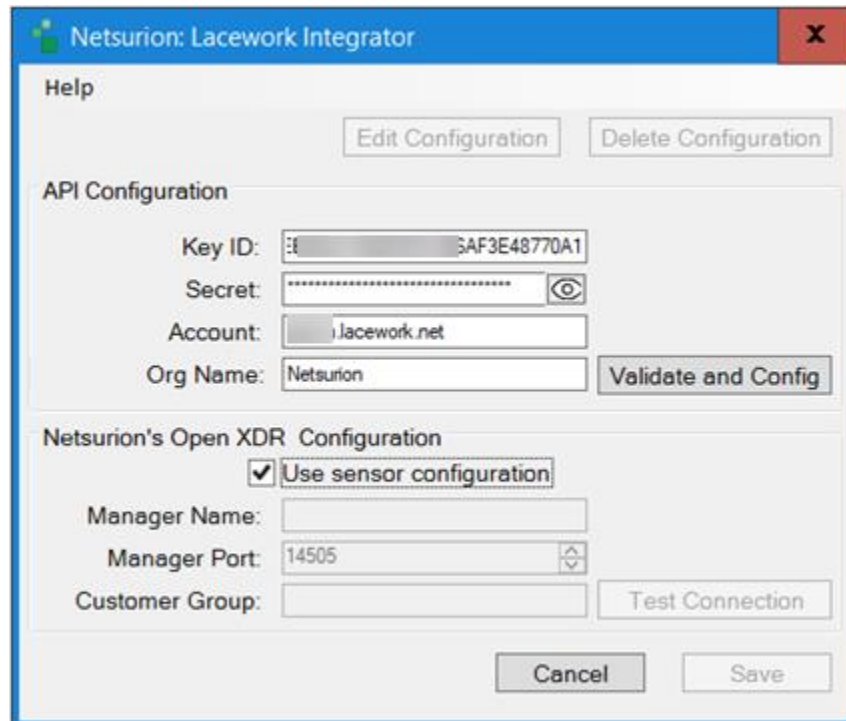


If the connection is validated successfully, an Information window pops-up stating '**Integrator is connected with Netsurion's Open XDR manager successfully**'.

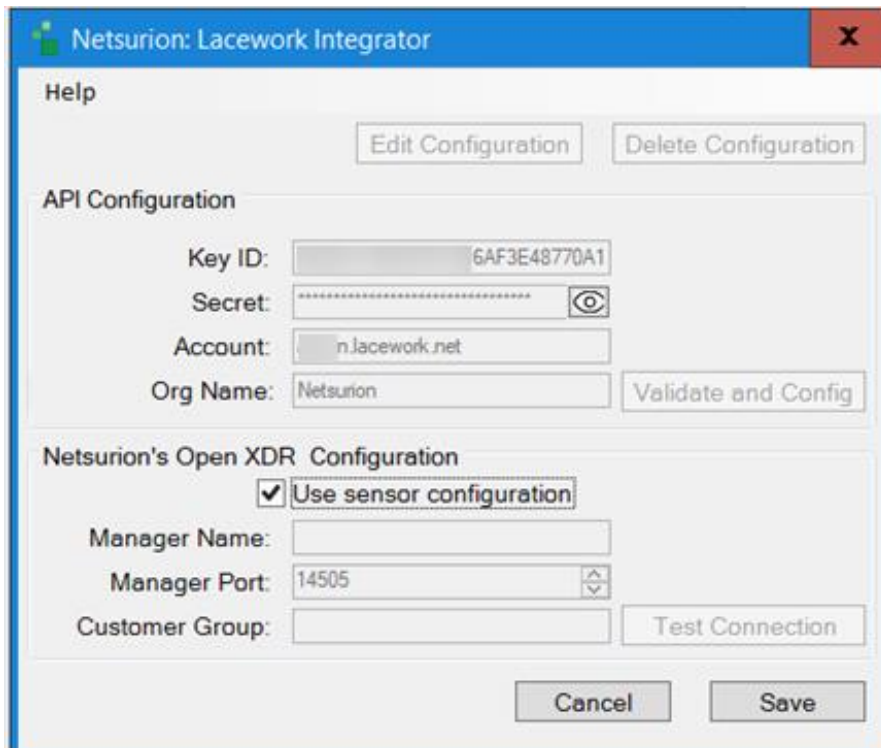


#### To use the Sensor configuration:

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

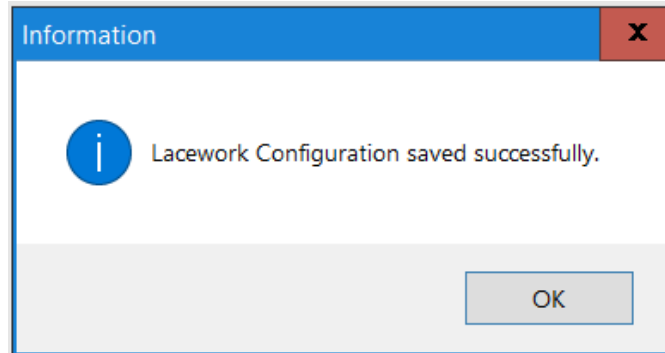


4. After specifying the required details, click **Save** and the following information window pops-up stating '**Configuration saved successfully**'.





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



## 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 Lacework.

- Categories\_Lacework.iscat
- Alerts\_Lacework.isalt
- Reports\_Lacework.etcx
- KO\_Lacework.etko
- Dashboards\_Lacework.etwd

### Note

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

## Data Source Integrations Details

### 4.1 Alerts

Name	Description
Lacework: Vulnerability detected	Generated whenever the Lacework detects the critical or high severity vulnerability.
Lacework: Policy violation detected	Generated whenever the Lacework detects the critical or high severity policy violation.
Lacework: Potential intrusion detected	Generated whenever the Lacework detects the critical or high severity potential intrusion.

## 4.2 Reports

Name	Description
Lacework – Audit activities	Provides details of all user management activities performed in the Lacework console.
Lacework – Alerts overview	Provides the details of all alerts generated by Lacework and its related content.

## 4.3 Dashboards

Name	Description
Lacework - User management activities by username	Displays the data about user management activities.
Lacework - Critical cloud activities	Displays all the cloud related critical activities.
Lacework - Alert status by severity	Displays the count of all the open status alerts.
Lacework - Alert types by policy	Displays the data about various alert types by policies.

## 4.4 Saved Search

Name	Description
Lacework – Audit activities	Provides details of all user management activities performed in Lacework console.
Lacework – Alerts overview	Provides the details of all alerts generated by Lacework and its related content.

## 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](https://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	<a href="mailto:SOC@Netsurion.com">SOC@Netsurion.com</a>
Managed XDR Enterprise MSPs	<a href="mailto:SOC-MSP@Netsurion.com">SOC-MSP@Netsurion.com</a>
Managed XDR Essentials	<a href="mailto:Essentials-Support@Netsurion.com">Essentials-Support@Netsurion.com</a>
Software-Only Customers	<a href="mailto:Software-Support@Netsurion.com">Software-Support@Netsurion.com</a>

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