NOZOMI NETWORKS

Splunk Universal Add-on
Integration Guide

v1.0.7 — 2026-10-06

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Copyright © 2013-2026, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction **5**
Overview 7
Chapter 2. Requirements **9**
Requirements 11
Chapter 3. Installation **13**
Installation 15
Generate an API key in Vantage 16
Generate an API key 16
Generate an API key in Guardian or CMC 20
Generate an OpenAPI key 20
Chapter 4. Troubleshooting **23**
Troubleshooting 25
Glossary 27

Chapter 1. Introduction

Overview

*This documentation describes the **Splunk Universal Add-on** integration with the Nozomi Networks platform. This add-on is called the **Nozomi Networks Universal Add-on** in **splunkbase**.*

The **Splunk Universal Add-on** provides the capability to configure and retrieve information from these Nozomi Networks products:

- *Central Management Console (CMC)*
- Guardian
- Vantage

Chapter 2. Requirements

Requirements

*The requirements for the **Splunk Universal Add-on**.*

Splunk version

Splunk version 9.0 or higher.

Connectivity

The **Splunk Universal Add-on** can connect with an *Nozomi Networks Operating System (N2OS)* instance (*CMC* or Guardian) and/or Vantage.

The Splunk instance where the Add-on is installed must be able to send *hypertext transfer protocol (HTTP)* requests to the Nozomi Networks instances from which it retrieves data.

Dependencies

The only package dependency is the *common information model (CIM)*, which must be version 5.x or higher.

Chapter 3. Installation

Installation

*Instructions for installing and configuring the Nozomi Networks **Splunk Universal Add-on**. This topic covers logging into Splunkbase, downloading the add-on, setting up accounts, configuring inputs, and managing data retrieval parameters for seamless integration with Nozomi Networks.*

Procedure

1. Log in to the Splunkbase website.
2. In the search field, search for **Nozomi Networks**.

   Result: The **Nozomi Networks Universal Add-on** page shows.
3. Select **Download**.

   Result: The **Accept License Agreements** page shows.
4. Accept the terms and select **Agree to download**.

   Result: A dialog shows.
5. Select **Ok**.
6. For an overview of the **Splunk Universal Add-on**, select **Details**.
7. Select **Installation**.
8. In the configuration section, create an account. The account should include the username and password, which are the key name and key token of:
   - *CMC*
   - Guardian
   - Vantage
9. In the input section, configure the input to retrieve the following data from Nozomi Networks:
   - Alert
   - Asset
   - NodeCve
   - Node
   - Link
   - Variable
   - Session
10. Add the host without (*HTTP* or *hypertext transfer protocol secure (HTTPS)*).
11. Select the account that you just created.
12. To specify the data retrieval starting point, use the **from timestamp** filter.
13. To determine how many items are retrieved for every call, define the page size.
14. Select **Add**.

Generate an API key in Vantage

Generate an API key

Before you can use an API key, you must generate one. Once a key is created, it cannot be edited, it can only be revoked or rotated.

Before you begin

Before you do this procedure, make sure that you have:

- Created a user to associate with your third-party application
- Assigned the user a role that grants the necessary permissions and scope within Vantage

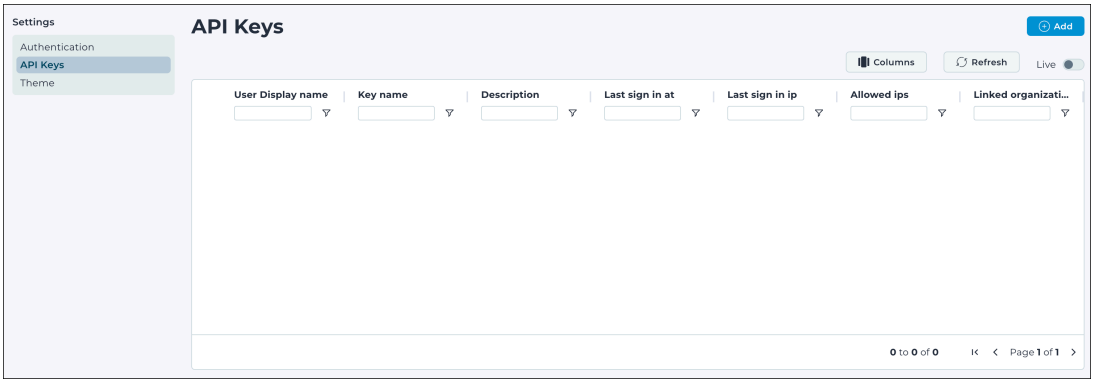
About this task

Once an key has been created, you cannot edit it. You can only revoke it.

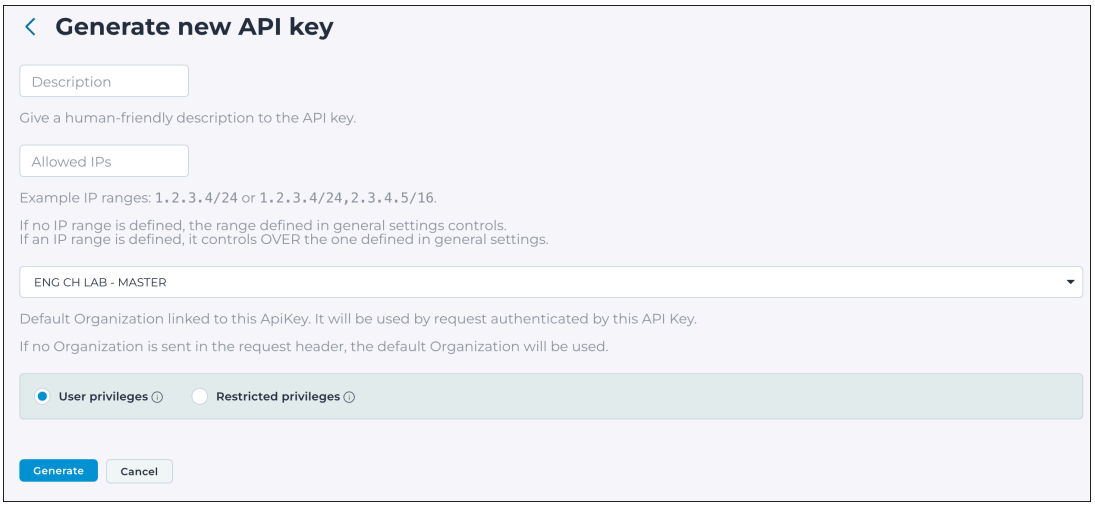
Procedure

1. Log into Vantage as the user who will own the key.
2. In the top navigation bar, select **> Profile**.
3. Select **API Keys**.

   Result: The **API Keys** page opens.
4. To generate a new key, select **Add**.



5. In the **Description** field, enter a description for the key.



> **Note:**
> Nozomi Networks recommends that the description includes the name of the application that will connect with the key.

6. **Optional:** Enter a range of allowed addresses in the **Allowed IPs** field. Only applications within this range will be permitted to connect with this key.

> **Note:**
> For these settings, you must use comma-delimited entries, in format. Values here will override the values in the **SECURITY** section on the **General** page.

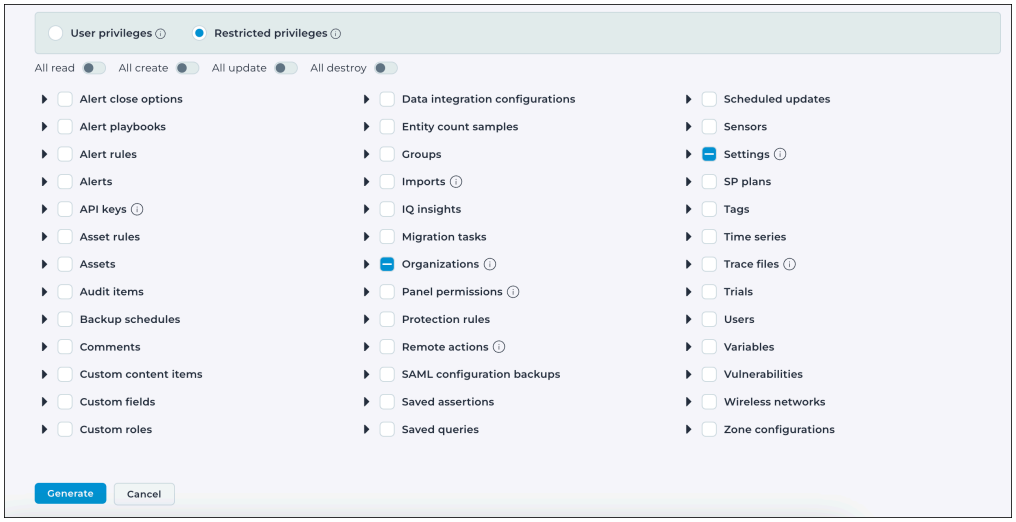
7. In the **Organization** field, select the organization that will be the default for this key.

> **Note:**
> If an request that uses this key doesn't include an organization, the default organization is used.

8. Select one of these options:

Choose from:

- **User privileges**
- **Restricted privileges**



User privileges applies the same permissions that the user has.
Restricted privileges allows you to define a set of permissions associated with the key.

Note:
During execution, the key's effective permissions are the permissions common to both the user and the key.

9. Select **Generate**.

   Result: Vantage generates a key and displays its:

   - Key name
   - Key token
   - Allowed ips
   - Linked organization

10. **Important:**
    You will need some of these values when you configure your third-party application. While the name is shown in the Vantage after this point, the token is not shown again. If you lose this data, you must generate a new key.

    Record these details:

    - Key name
    - Key token
    - Allowed ips

Generate an API key in Guardian or CMC

Generate an OpenAPI key

The profile settings menu lets you generate an OpenAPI key.

Procedure

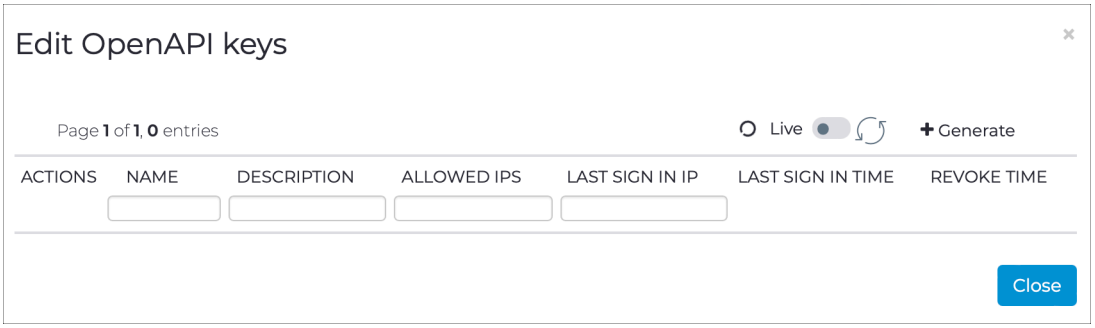
1. In the top navigation bar, select

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Edit OpenAPI keys**.

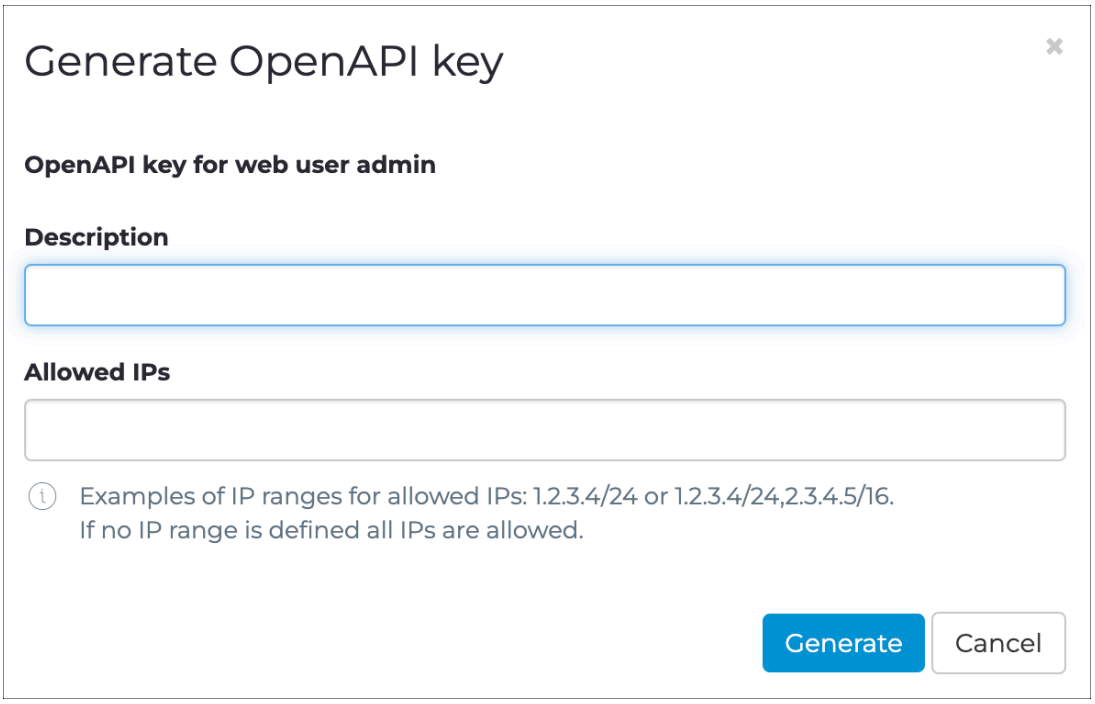
   Result: A dialog shows.

4. In the top right, select **+ Generate**.



Result: A dialog shows.

5. In the **Description** field, enter a description for the OpenAPI key.



6. In the **Allowed IPs** field, enter the details of the allowed addresses.
7. Select **Generate**.

Results

Your OpenAPI key has been generated.

Chapter 4. Troubleshooting

Troubleshooting

This section provides troubleshooting tips for secure sockets layer (SSL) verification issues in Splunk add-ons. It covers an alternate add-on version that bypasses SSL verification for users with untrusted certificates, available through support but not verified by Splunk.

If you encounter *secure sockets layer (SSL)* verification issues, there is a version of the **Splunk Universal Add-on** that allows skipping *SSL* verification. However, note that Splunk has not verified this version, and it is not available through the Splunk store. It is useful for customers with *CMC* or Guardian having untrusted certificates, *ask support for it*.

Glossary

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in a similar way as on the sensor.

Common Information Model

The CIM is a standardized data model used in the utility industry, particularly for smart grids, to ensure seamless data exchange and interoperability between systems and applications.

cURL

cURL is a command-line tool and library used to transfer data to or from a server. It supports many protocols, including HTTP, HTTPS, FTP, and more. In API contexts, curl is commonly used to test and interact with endpoints by sending requests and receiving responses.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Secure Sockets Layer

A secure sockets layer ensures secure communication between a client computer and a server.