NOZOMI NETWORKS

Universal
Software Development Kit

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**

Chapter 2. OpenAPI **9**

Query endpoint 11

Vantage PATCH nodes 13

Glossary 15

Chapter 1. Introduction

*The **Universal SDK** provides a unified reference for working with Nozomi Networks software products through their application programming interfaces (APIs).*

The **Universal SDK** is designed to provide developers and integrators with a consistent and comprehensive guide to help you use the *application programming interface (API)s* across multiple Nozomi Networks software products.

This document serves as a centralized reference to:

- Help you understand the core principles of interacting with Nozomi Networks *APIs*
- Provide detailed examples for *API* usage applicable across various products
- Highlight best practices for *API* integration to ensure optimal performance and compatibility

Chapter 2. OpenAPI

Query endpoint

You can manipulate data sources through the use of queries, which are commands piped one after another.

See **Queries**, or go to `/#/query` in your Nozomi Networks solution Web *user interface (UI)* for examples.

Requirements and restrictions

- Users must have permission to execute *API* calls
- Results display the list of queried items
- We recommend that you use pagination, adding **page** and **count** params
- The **page** param is the page number to return, and **count** is the page dimension
- If count is not provided, the default value is **10,000**; if page is not provided, the default page number is **1**
- If the provided count value is higher than **10,000**, no more than **10,000** items are returned
- The maximum allowable page number is **1,000**. Requests for pages beyond this limit will result in an error response **Bad request**

Example: To see how many nodes are in the system, call the following *uniform resource locator (URL)*: `https://10.0.1.10/api/open/query/do?query=nodes | count`

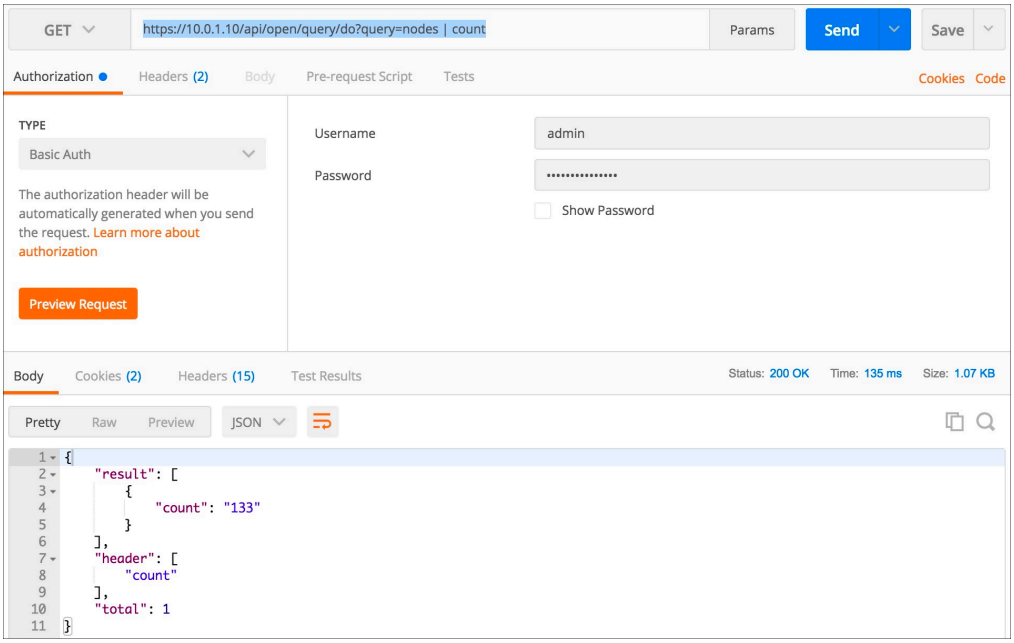

Figure 1. Example of a count query

A more complex example is: `https://10.0.1.10/api/open/query/do?query=nodes | where_link protocol == http | head 5`.

In the image we've used Postman's interface to collapse the results so you could clearly see it's five, as we wanted.

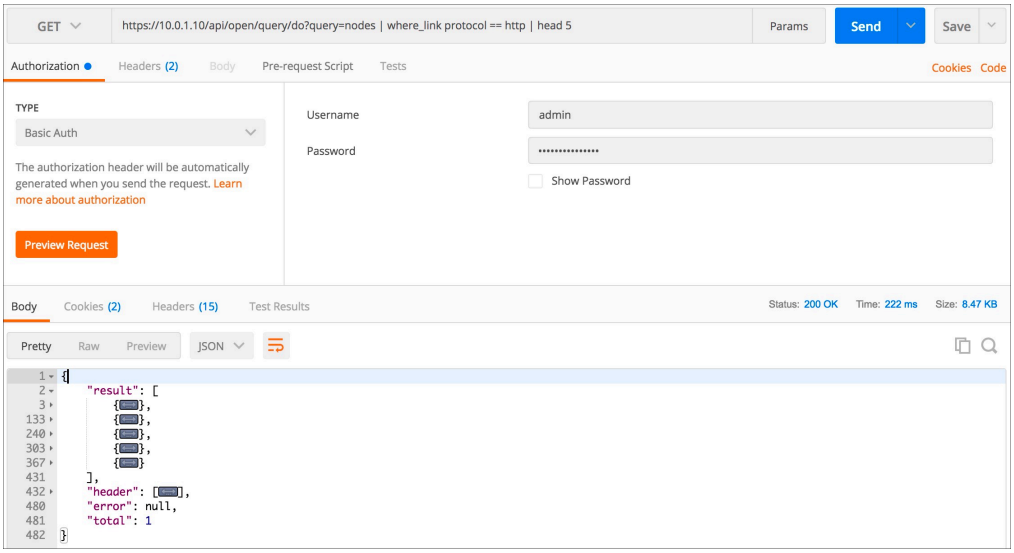

Figure 2. Filtering HTTP and taking the first five results

HTTP API Best Practices

Use time filter for ordering and filtering

When fetching items from the *API*, consider using a time filter, such as **record_created_at**, to sort the items and retrieve only those that are greater than the specified time value. This allows efficient fetching of recent data.

```
alerts | sort record_created_at asc | where record_created_at >
 1674828173887
```

Handling page 1000 number limit

The *API* supports pagination with a **page** parameter; it is advisable to set up a time field pivot when reaching page 1000 and start again from page 1.

```
/api/open/query/do?query=alerts | sort record_created_at asc | where
 record_created_at > 1674828173887&page=1&count=100
```

Select only relevant fields

When making *API* requests, specify the fields you are interested in. This will ensure that the *API* response contains only the data that is relevant to your use case, reducing the size of the response payload and minimizing unnecessary data transfer.

```
alerts | select id risk record_created_at description name
```

Limit items per page

To avoid heavy response payloads and potential performance issues, it is recommended to set a reasonable limit on the number of items per page. Generally, the number of items per page should be kept below 1000, unless there is a specific use case that necessitates a higher value.

Vantage PATCH nodes

A PATCH to `api/open/nodes/{id}` lets you to update the node's fields.

Requirements and restrictions

- The authenticated user must be in a group that has the admin role
- The fields to be updated and their value must be passed in the *JavaScript Object Notation (JSON)* body inside `attributes` key

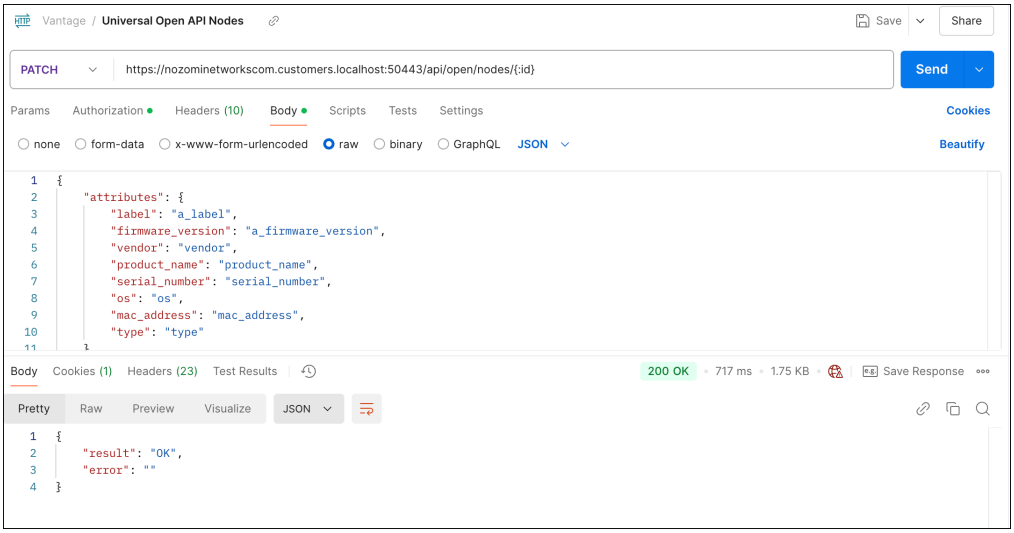

Figure 3. Example of a Vantage Open API nodes patch

Fields that can be updated are:

- `label`
- `firmware_version`
- `vendor`
- `product_name`
- `serial_number`
- `os`
- `mac_address`
- `type`

Glossary

Address Resolution Protocol

ARP is a communication protocol that is used to discover the link layer address, such as a *media access control (MAC)* address, that is associated with a given internet layer address. This is typically an IPv4 address.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

Asset Intelligence™

Asset Intelligence is a continuously expanding database of modeling asset behavior used by N2OS to enrich asset information, and improve overall visibility, asset management, and security, independent of monitored network data.

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.

Central Processing Unit

The main, or central, processor that executes instructions in a computer program.

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

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.

dmidecode

dmidecode is a Linux command-line tool that retrieves detailed hardware information from the system's DMI/SMBIOS tables, including BIOS, processor, memory, and motherboard details, requiring root access.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

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.

Identifier

A label that identifies the related item.

Industrial Control Systems

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

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

JavaScript Object Notation

JSON is an open standard file format for data interchange. It uses human-readable text to store and transmit data objects, which consist of attribute–value pairs and arrays.

Light-emitting Diode

An LED (Light Emitting Diode) is an electronic component that emits light when an electric current passes through it, offering energy-efficient, long-lasting illumination for displays, indicators, and lighting applications.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

Mobile Device Management

This is the administration of mobile devices, such as tablet computers, laptops, and smartphones. It is often implemented with a third-party product with features for specific vendors of mobile devices.

Nozomi Networks Operating System

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

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Executable

PE is a file format used by Windows operating systems (OS) for executable files, object code, and dynamic link libraries (DLLs). PE files contain the code and resources needed to run programs on Windows.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Random-access Memory

Computer memory that can be read and changed in any order. It is typically used to store machine code or working data.

Remote Terminal Unit

An RTU is a microprocessor-controlled electronic device that acts as an interface between a SCADA (supervisory control and data acquisition) system, or distributed control system, to a physical object. It transmits telemetry data to a master system, and uses messages from the master supervisory system to control connected objects.

Secure Digital

A type of flash memory storage card used in devices like cameras, smartphones, and embedded systems.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Structured Threat Information Expression

STIX™ is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Threat Intelligence™

Nozomi Networks **Threat Intelligence™** feature monitors ongoing OT and IoT threat and vulnerability intelligence to improve malware anomaly detection. This includes managing packet rules, YARA rules, STIX indicators, Sigma rules, and vulnerabilities. **Threat Intelligence™** allows new content to be added, edited, and deleted, and existing content to be enabled or disabled.

Transmission Control Protocol

One of the main protocols of the Internet protocol suite.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Datagram Protocol

UDP is a lightweight, connectionless communication protocol used for fast, time-sensitive data transmission, such as video streaming, online gaming, and VoIP. UDP prioritizes speed and low latency over guaranteed delivery or error correction.

User Interface

An interface that lets humans interact with machines.

Windows Remote Management

Is a Microsoft implementation of Web Services-Management in Windows which lets systems access or exchange management information across a common network. You can utilize the built-in command line tool, or scripting objects, WinRM can be used with remote computers that may have baseboard management controllers (BMCs) to acquire data.

Windows Server Update Services

WSUS is a Microsoft tool that enables centralized management and deployment of software updates and patches for Windows operating systems and other Microsoft products. It helps organizations enhance security by automating patch management, ensuring compliance, and reducing vulnerabilities.

YARA

YARA is a tool designed to help identify and classify malware samples by describing them in terms of textual or binary patterns. YARA rules are used to detect files, processes, or network traffic that match known malware signatures.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.