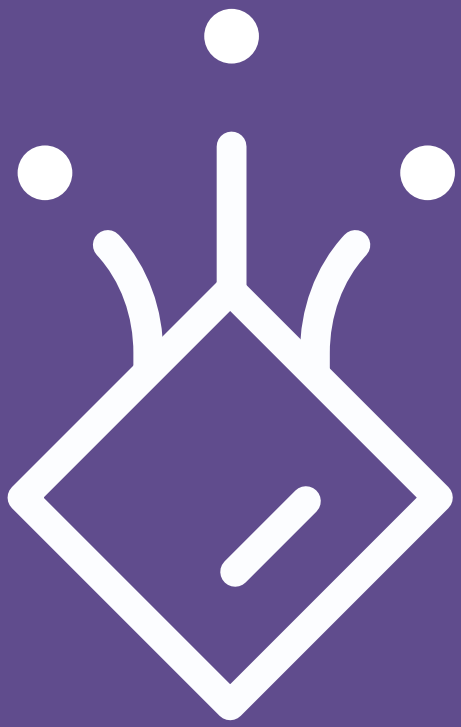
NOZOMI NETWORKS



Threat Intelligence
Administrator Guide

N2OS v26.5.0 — 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**
Threat Intelligence overview 7
License 9
Chapter 2. Requirements **11**
Resource requirements 13
Chapter 3. Configuration **15**
Configure a Threat Intelligence license 17
Enable automatic updates 18
Configure manual updates 20
Sensor-level contents management 21
Manage contents at sensor level 22
Chapter 4. Maintenance **23**
Check the version and status of Threat Intelligence 25
Glossary 27

Chapter 1. Introduction

Threat Intelligence overview

Threat Intelligence™ *(TI) is an add-on feature which enriches assets with additional information to improve detection of malware and anomalies.*

Threat Intelligence (TI) constantly monitors *operational technology (OT)* / *Internet of Things (IoT)* threat and vulnerability intelligence. This improves malware anomaly detection. This includes managing packet rules, YARA rules, *Structured Threat Information Expression (STIX)* indicators and vulnerabilities.

Threat Intelligence permits new content to be:

- Added
- Edited
- Deleted

It also lets you enable or disable existing content.
In order to identify malicious events, *TI* continuously analyzes network traffic and asset configuration details, and compares them with:

- Industry-standard packet rules
- YARA rules
- Indicators of compromise
- Vulnerability assessments
- Mapping content (*Common Platform Enumeration (CPE)*)

TI packages can be controlled at a modular level to:

- Disable or enable individual rules
- Manually add rules to investigate and deliver customer alerts

TI is a subscription service that is curated and proprietary. You can use it with Nozomi Networks products, or with 3rd party software. This subscription lets you receive an automatic, and continuous flow of updated threat intelligence information into Guardian sensors to detect the most up-to-date methods of attack. You can manage *TI* content from:

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

This makes it easy to propagate *TI* contents to an unlimited number of Nozomi Networks sensors.

You can set *TI* contents to update automatically, or you can upload a local file to manually update the Nozomi Networks sensors. This lets you operate the system in a fully air-gapped environment.

Management

To provide detailed threat information, the *TI* screen lets you manage:

- Packet rules
- YARA rules
- *STIX* indicators
- Vulnerabilities

Packet rules

Packet rules are executed on every packet. If a match is detected, they raise an alert of type **SIGN:PACKET-RULE**.

For more details on how to format packet rules, see the **Packet Rules Reference**.

YARA rules

Protocols like *hypertext transfer protocol (HTTP)* or *server message block (SMB)* execute YARA rules on every file transferred over the network. When a match is detected, an alert of type **SIGN:MALWARE-DETECTED** is raised. YARA rules conform to the specifications found at YARA Rules.

STIX indicators

The information that *STIX* indicators contain:

- Malicious *internet protocol (IP)* addresses
- *uniform resource locator (URL)s*
- Malware signatures, or
- Malicious *domain name server (DNS)* domains

This information enriches existing alerts, and raises new ones.

Vulnerabilities

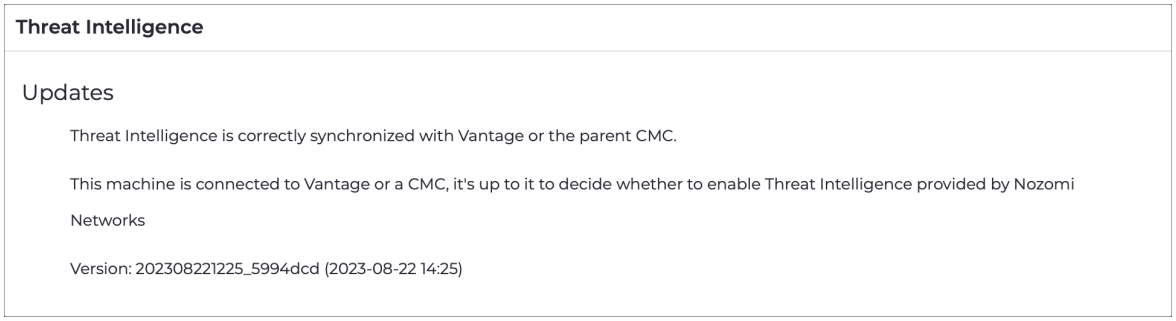
Vulnerabilities are assigned to each node, depending on the installed hardware and operating system, and the software identified in the traffic. The Nozomi Networks solution leverages *Common Vulnerabilities and Exposures (CVE)*, a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures.

License

You need a separate, additional license to use Threat Intelligence.

If you have a valid, up-to-date license for *TI*, it will show in Guardian here: **> System > Updates & License > Threat Intelligence**.

Figure 1. Guardian is connected to Vantage or a CMC



Updates section

The **Updates** section will show different details depending on how the Guardian is connected.

Update service configuration dialog

The **Update service configuration** dialog shows different options, depending on how Guardian receives Threat Intelligence information.

If Guardian is connected to a *CMC* or Vantage, it receives Threat Intelligence through that connection (see above).

If Guardian is not connected upstream, it receives Threat Intelligence through an S3 instance cloud service, which requires an internet connection. If a proxy is required for that connection, it might require authentication.

Chapter 2. Requirements

Resource requirements

The resource requirements for Threat Intelligence.

On top of the resource requirements for Guardian, you should regularly view the **Health** page to monitor the performance in these sections:

- **CPU percentage usage**
- **RAM MB usage**
- **Disk percentage usage**

Chapter 3. Configuration

Configure a Threat Intelligence license

Before you can use the Threat Intelligence, you must install a license.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. Choose a method to open the **Updates and licenses** page.

   Choose from:

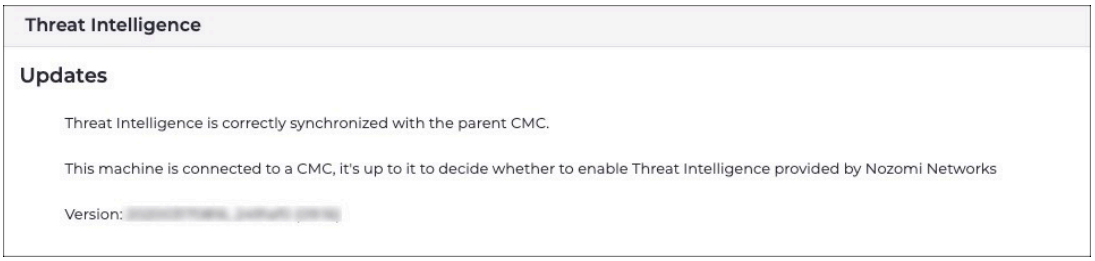
   - In the status bar, select the `TI` icon
   - In the top navigation bar, select ⚙ **> System > Updates and licenses**

   Result: The **Updates and licenses** page opens.

3. In the top right of the **Threat Intelligence** section, select **Set new license**.

   Result: The **Updates** dialog shows.

4. You can monitor the status of the update from this screen (in green font).



Results

The license has been configured.

Enable automatic updates

If you are connected to Vantage, or a Central Management Console (CMC), you can enable automatic Threat Intelligence updates.

Procedure

1. From your Guardian or *CMC*, make sure that you can reach `https://nozomi-contents.s3.amazonaws.com`

   > **Note:**
   > This is to make sure that you will be able to get the updates for Threat Intelligence.

2. Choose a method to open the **Updates and licenses** page.

   Choose from:

   - In the status bar, select the `TI` icon
   - In the top navigation bar, select ⚙ **> System > Updates and licenses**

   Result: The **Updates and licenses** page opens.

3. In the **Update service configuration** section, select **Nozomi Networks Update Service**.
4. Select the **Enable network connection to update service** checkbox.
5. Select **Check connection** to check the connection to Vantage or a *CMC*.

   Result: A message shows to confirm that the `Connection to endpoint is working`.

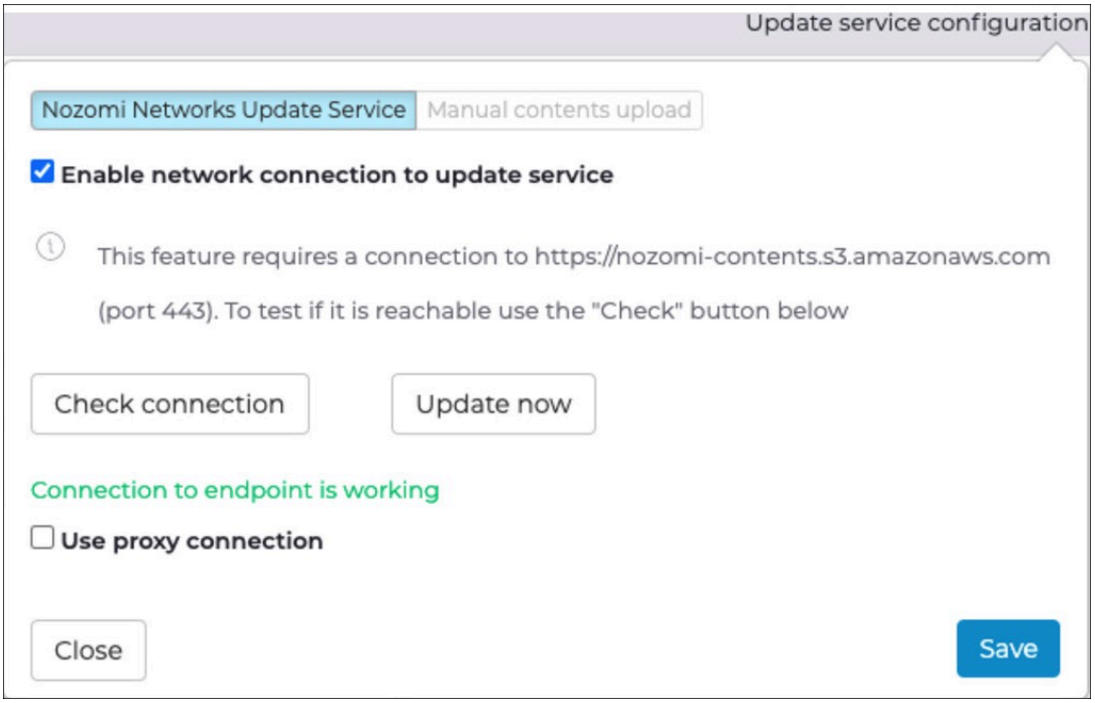
6. Select **Update now** to update the Threat Intelligence output immediately.

   > **Note:**
   > By default, the update will happen once an hour, or on reboot.

7. Select **Save**.

> **Note:**
> The **Update service configuration** dialog shows different options, depending on how Guardian receives Threat Intelligence information:
> - If Guardian is connected to a *CMC* or Vantage, it receives Threat Intelligence through that connection.
> - If Guardian is not connected upstream, it receives Threat Intelligence through an S3 instance cloud service, which requires an Internet connection. If a proxy is required for that connection, it may require authentication.

8. Select the **Use proxy connection** checkbox.



> **Note:**
> In the image above, a proxy server is being used to manage Threat Intelligence.

9. Select the **Enable Proxy Authentication** checkbox.

Results

Automatic updates have been enabled.

Configure manual updates

If your sensor, or Central Management Console (CMC), is not connected to the internet, you can update Threat Intelligence manually.

Before you begin

You have downloaded the applicable update package from the Customer Support portal.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

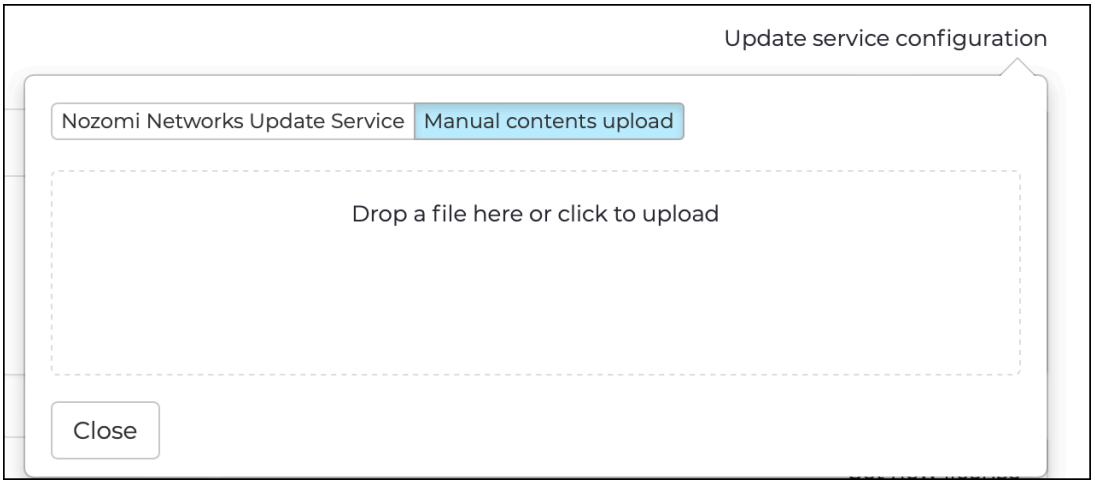
2. In the **System** section, select **Updates and licenses**.

   Result: The **Updates and licenses** page opens.

3. In the top, right corner, select **Update service configuration**.

   Result: A dialog opens.

4. Select the **Manual contents upload** button.



5. Drag and drop the update package, that you downloaded from the Customer Support portal, into the upload field.

   Result: A progress bar shows and the update is verified.

6. Select **Close**.

Results

Manual updates have been configured.

Sensor-level contents management

By default, Threat Intelligence contents can only be managed on the top-level sensor. However, this policy can be customized to allow any sensor in the solution to add, edit, enable or disable individual contents.

When the local management of *TI* contents is enabled, each sensor in the solution will allow the user to enable or disable any contents, and to define, edit and remove local contents. In this situation, any additions or changes performed on a *CMC* will not be propagated to the connected sensors.

When the local management of *TI* contents is disabled, each sensor in the solution will reflect exactly the contents defined on the top-level sensor. In this situation, any content added on the top sensor will be propagated to all connected sensors, and any content enabled or disabled will also be in the same state on all sensors. This also means that, when disabling the local management of contents, all custom contents created on the connected sensors will be erased.

Manage contents at sensor level

*You can change the status of the **Enable local contents** toggle to change how the Threat Intelligence contents are managed.*

Procedure

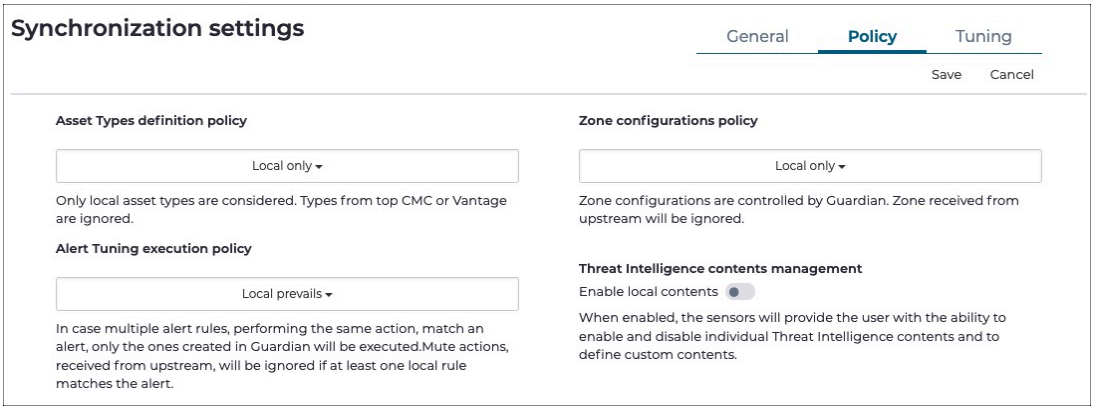
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **Settings** section, select **Synchronization settings**.

   Result: The **Synchronization settings** page opens.

3. Select the **Policy** tab.



4. In the **Threat Intelligence contents management** section, change the **Enable local contents** toggle to enable, or disable, the local management of the *TI* contents.

Chapter 4. Maintenance

Check the version and status of Threat Intelligence

*The **Updates & Licenses** page lets you check the version and status of Threat Intelligence (TI).*

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

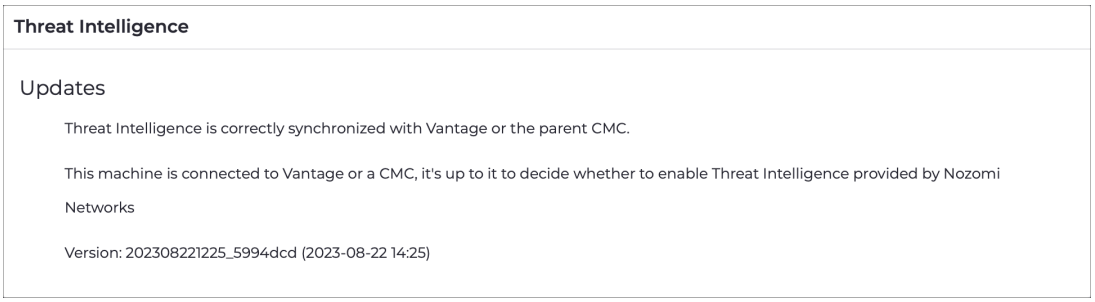
2. Choose a method to open the **Updates and licenses** page.

   Choose from:

   - In the status bar, select the `TI` icon
   - In the top navigation bar, select ⚙ **> System > Updates and licenses**

   Result: The **Updates and licenses** page opens.

3. Confirm that the *TI* contents are up-to-date.



4. **Optional:** View the **Version** number and the time stamp when this version was installed.

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.

Central Processing Unit

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

Common Platform Enumeration

CPE is a structured naming scheme for information technology (IT) systems, software, and packages. CPE is based on the generic syntax for Uniform Resource Identifiers (URI) and includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

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.

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.

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.

Operational Technology

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

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism.

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.

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.

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.