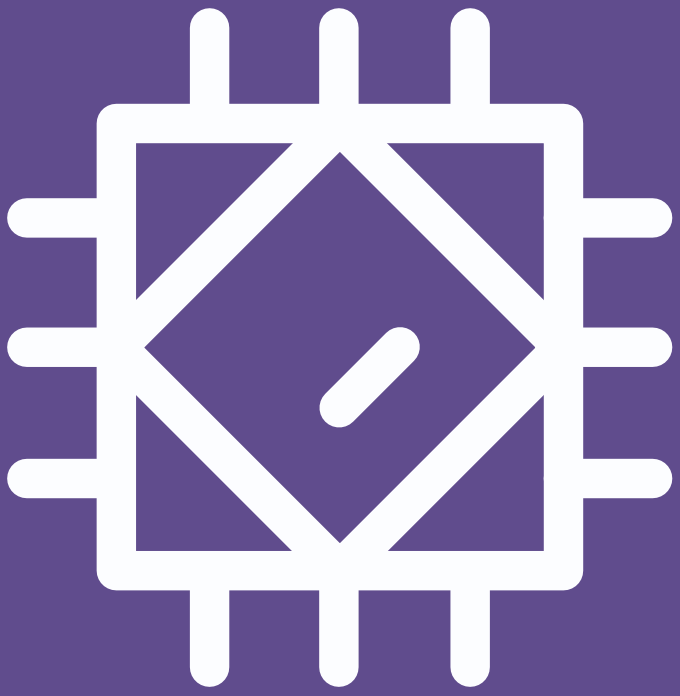
NOZOMI NETWORKS



Asset Intelligence
Administrator Guide

N2OS v25.0.0 — 2025-03-18

Legal notices

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

Copyright

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**
Asset Intelligence overview 7
Enriched asset information 9
License 11
Chapter 2. Configuration **13**
Install an Asset Intelligence license 15
Enable automatic updates 16
Configure manual updates 18
Chapter 3. Maintenance **19**
Check the version and status of Asset Intelligence 21
Glossary 23

Chapter 1. Introduction

Asset Intelligence overview

Asset Intelligence™ *(AI) is an add-on feature which enhances device profiles. This enables administrators to make better informed decisions with regards to the maintenance and security of their operational technology (OT) / Internet of Things (IoT) environments.*

Once the *Nozomi Networks Operating System (N2OS)* recognizes an asset, it is stored in the inventory of the *Asset Intelligence (AI)* database. The *AI* feed models expected behavior to enrich this information. This improves:

- Overall visibility
- Asset management
- Security

This strengthens the learned behavior from the baseline independently from the monitored network data.

Enriched asset

An enriched asset is one that has been confirmed against the *AI* database, matched to a known entity, and all additional database information has been applied to the asset.

Figure 1. Enriched asset

When an asset is **Enriched**, all asset information is visible, including the **End of sale** and **Product lifecycle status**. With this additional information, more specific vulnerabilities for the individual asset are visible.

For more details, see Enriched asset information (on page 9).

Not Active

The asset is not confirmed against the database and additional information is not applied.

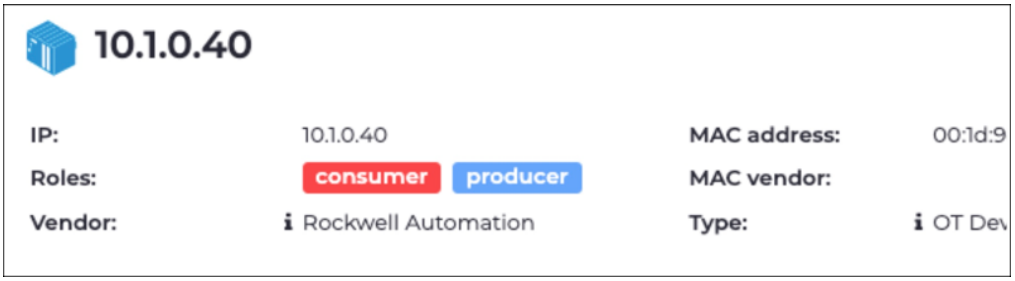


Figure 2. Not active asset

An asset might be Not Active for several reasons, but typically it is because traffic with the asset's full protocol is not visible to the sensor, which could be the result of sensor placement. For example, if the sensor only sees traffic for the *domain name server (DNS)* of the asset, it is unable to see enough information to match against the *AI* database, and the asset is tagged as **Not Active**.

Enriched asset information

Asset Intelligence enriches assets and delivers regular profile updates for anomaly detection. An active Asset Intelligence license is required for this feature.

If you select the details for a specific asset in the **Assets** page, the **Learning status** section has a widget that shows the effect of *AI* on assets.

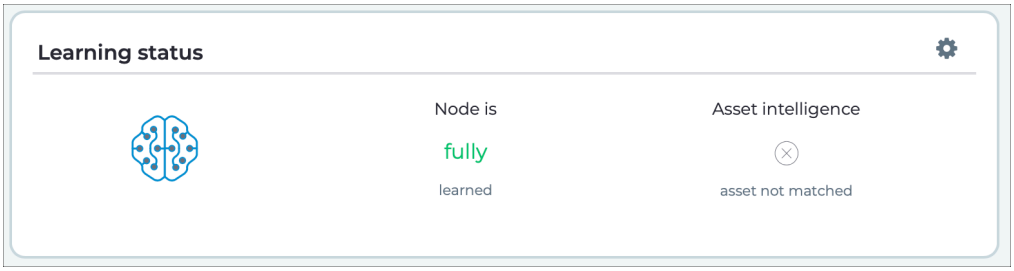


Figure 3. Learning status widget

The Assets table also shows an attribute such as: `is_ai_enriched`

Table 1. Asset states

Asset state	Description
Enriched asset	A match was found, and the asset is enriched
Asset not matched	A match was not found, and the asset is not enriched
Inactive → Not active	No content was found. This can be due to a missing license, or content not yet imported

The table below shows details about enriched assets. However, the specific enriched fields will vary with different types of asset.

Table 2. Asset details

Asset detail	Description
Type (asset type)	Users have the ability to overwrite an existing value for more precision, such as updating an *operational technology (OT)* device to an *intelligent electronic device (IED)*.
End of Sale	The date when the hardware is officially no longer for sale.
End of Support	The date when the hardware is officially no longer supported.

Table 2. Asset details (continued)

Asset detail	Description
Lifecycle status	Depending on the **End of Sale** and **End of Support** values, this value is set to **Active**, **End of Sale**, **End of Support**. This generic indication applies when precise dates for other fields are not specified, such as 'I know it's Active, but I'm not sure when it will go End of Sale'.
Protocols	A list of expected protocols for the asset on the *N2OS* learning engine, leading to alert creation when behavior deviates from the profile.
Function Codes	A list of expected function codes for the asset on the *N2OS* learning engine, leading to alert creation when behavior deviates from the profile.
Image (Vantage only)	Asset picture.
Description (Vantage only)	A description of the asset.

Input data requirements

For *AI* to be able to enrich an asset, it must find a match, and find one, or more, of these data types:

- Vendor
- Product Name
- URL

This data can change depending on the asset model.

License

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

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

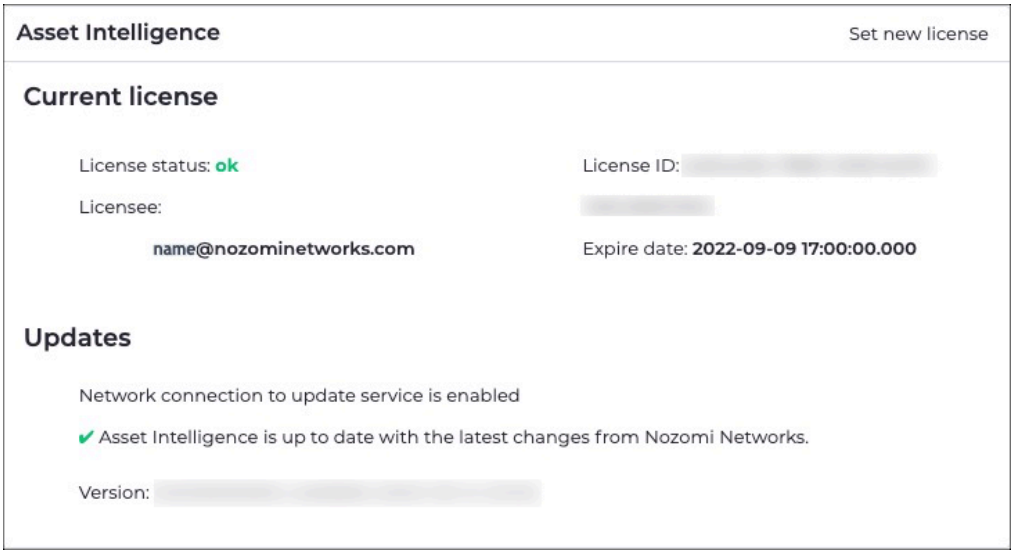


Figure 4. Asset Intelligence license

It will also show as a green tick mark next to the initials `AI` in the utility navigation bar.

Figure 5. Utility navigation bar

Chapter 2. Configuration

Install an Asset Intelligence license

Before you can use the Asset 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:

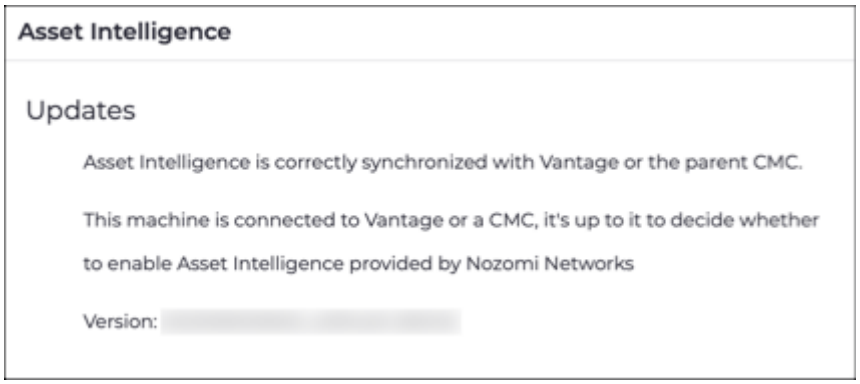
   - In the status bar, select the `AI` icon
   - In the top navigation bar, select ⚙ **> System > Updates and licenses**

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

3. In the top right of the **Asset 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 installed.

Enable automatic updates

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

Procedure

1. From your Guardian or *Central Management Console (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 Asset Intelligence.

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

   Choose from:

   - In the status bar, select the `AI` 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`.

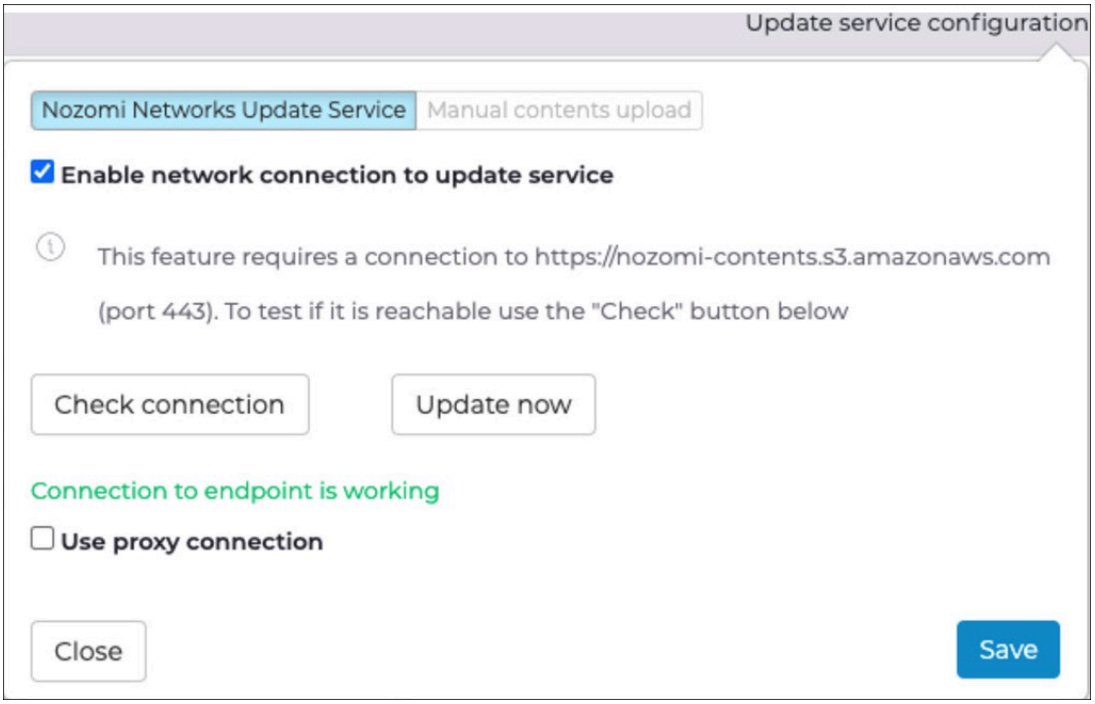
6. Select **Update now** to update the Asset Intelligence output immediately.

   > **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 Asset Intelligence information:
> - If Guardian is connected to a *CMC* or Vantage, it receives Asset Intelligence through that connection.
> - If Guardian is not connected upstream, it receives Asset 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 Asset 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 Asset Intelligence manually.

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 `AI` 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 **Manual contents upload**.
4. Contact Support for the manual update package and drop it in the area shown in the image above, or click to upload the update package.

   Result: After the update, new contents are propagated to the downstream sensors.

5. Select **Close** to save your settings.

Results

Manual updates have been configured.

Chapter 3. Maintenance

Check the version and status of Asset Intelligence

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

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

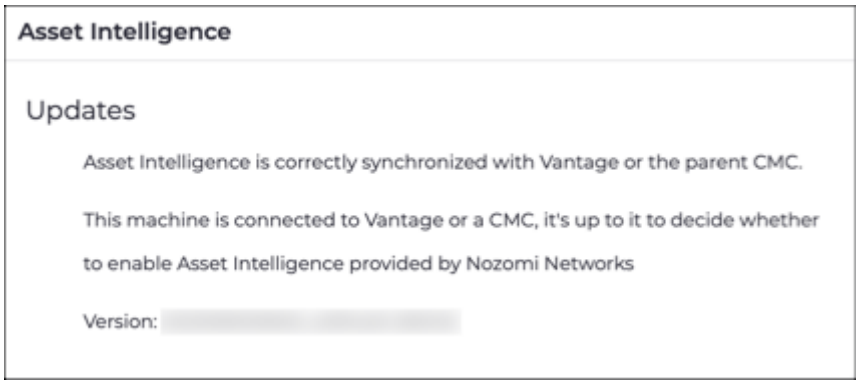
2. Choose a method to open the **Updates and licenses** page.

   Choose from:

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

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

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



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

Glossary

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 the similar method to the sensor.

Central Processing Unit

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

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.

Intelligent Electronic Device

An IED is an integrated microprocessor-based controller of power system equipment, such as capacitor banks, transformers, and circuit breakers. IEDs receive data from sensors and power equipment and can issue control commands. They can trip circuit breakers if they detect an anomaly in voltage, current, or frequency, or raise/lower tap positions in order to maintain the desired voltage level.

Internet of Things

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

Nozomi Networks Operating System

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

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.