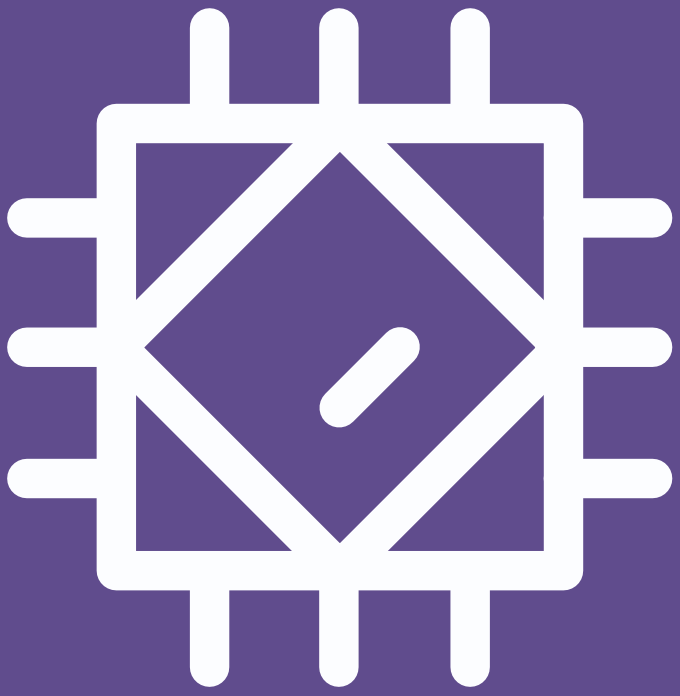
NOZOMI NETWORKS



Asset 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**
Asset Intelligence overview 7
Product availability 9
Enriched asset information 11
Enrichment feedback 13
Asset lifecycle management 14
CPE generation 16
Asset Intelligence and Asset Risk 17
License 19
Chapter 2. Requirements **21**
Resource requirements 23
Chapter 3. Configuration **25**
Install an Asset Intelligence license 27
Enable automatic updates 28
Configure manual updates 30
Enrichment modes 31
Chapter 4. Maintenance **33**
Check the version and status of Asset Intelligence 35
Chapter 5. Troubleshooting **37**
Troubleshoot Asset Intelligence 39
Glossary 41

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 11).

Not Active

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

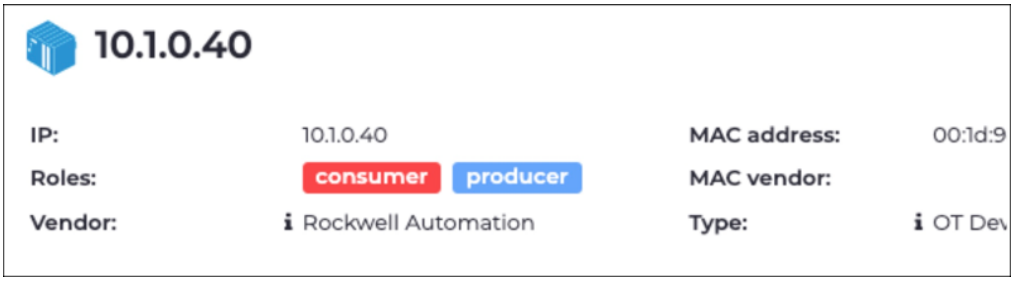


Figure 2. Not active asset

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**.

Product availability

Asset Intelligence capabilities vary depending on the Nozomi Networks product. Some features are available only in Vantage, while others extend to Guardian and CMC.

Deployment model

Asset Intelligence uses a cloud-centric architecture. The enrichment engine runs in Vantage and sends results to connected Guardian and *Central Management Console (CMC)* appliances. Enrichment processing requires a Vantage connection.

Guardian and *CMC* appliances receive enrichment results and display them in the local user interface. They also download Asset Intelligence content packs through the Update Service for local asset identification.

Feature availability matrix

The following table shows which Asset Intelligence capabilities are available on each product.

Table 1. Asset Intelligence feature availability by product

Capability	Vantage	Guardian	CMC
Enrichment orchestration and processing	✓	✗	✗
Enrichment mode configuration	✓	✗	✗
Display of enrichment results	✓	✓	✓
Content packs (Asset Knowledge Base)	N/A	✓	✓
Local *Common Platform Enumeration (CPE)* processing	✓	✓	✓
Asset Risk scoring and dashboards	✓	✗	✗
Risk trends and benchmarks	✓	✗	✗
Risk remediations	✓	✗	✗
Enrichment rollback	✓	✗	✗

Guardian

Guardian appliances include on-premises Asset Intelligence processing regardless of version. Appliances running version 23.1.0 or later also receive enrichment results propagated from Vantage, which provides more powerful enrichment than on-premises processing alone. The enrichment data updates local asset fields such as type, vendor, and product name.

Guardian also downloads Asset Intelligence content packs through the Update Service. These packs contain the Asset Knowledge Base, which supports local asset identification independently of the cloud enrichment.

The assets table in the Guardian user interface includes an **AI enriched** column. This column indicates whether each asset has been enriched by Asset Intelligence.

CMC

CMC appliances receive enrichment results through the same propagation mechanism as Guardian. In All-in-One deployments, Vantage uses a specialized workflow that groups assets by appliance host rather than by individual sensor.

For *CMC* All-in-One deployments, the highest-level *CMC* appliance is excluded from direct enrichment. This prevents duplicate processing of the same assets.

Vantage requirement

The following capabilities require an active connection to Vantage:

- Asset Risk scoring, trends, and remediation recommendations
- Configuration of enrichment modes
- Asset logos and detailed product information

Without a Vantage connection, Guardian and *CMC* appliances can still use locally installed Asset Intelligence content packs for basic asset identification.

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.

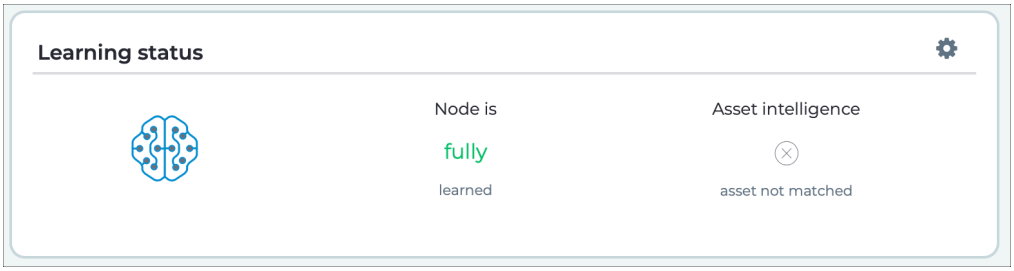


Figure 3. Learning status widget

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

Table 2. 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 3. 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 3. 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

AI uses all available fields of an asset to find the best match in the enrichment database. The more asset data is available, the higher the confidence of the enrichment result.

Enrichment feedback

Provide feedback on Asset Intelligence enrichments to improve the accuracy of future results.

Overview

AI includes a feedback mechanism that lets you confirm or report incorrect enrichment results. You can select the to open a dialog. The enrichment service receives this feedback and uses it to improve the accuracy of future enrichments.

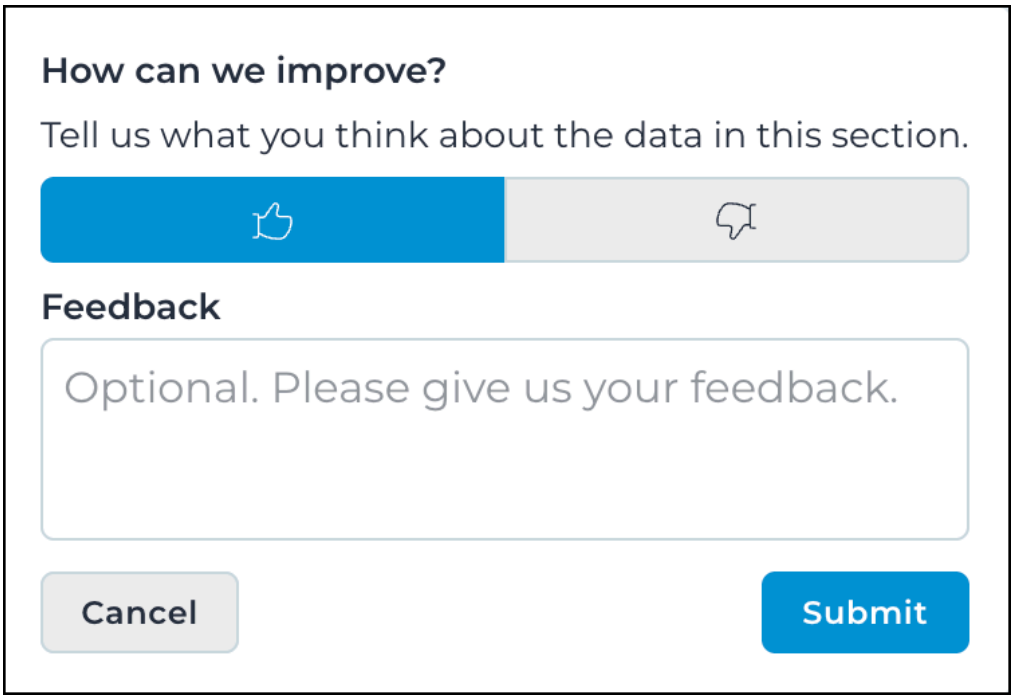


Figure 4. Enrichment feedback controls on an asset

How feedback works

When you review an enriched asset, you can submit feedback indicating whether the enrichment is correct or incorrect. The enrichment service uses this feedback to:

- Adjust confidence scores for similar assets
- Improve the machine learning model used for asset classification
- Reduce false positives in future enrichment cycles

When to provide feedback

Provide feedback in the following situations:

- **Positive feedback**: When the enrichment correctly identifies the asset vendor, product, type, or lifecycle information
- **Negative feedback**: When the enrichment assigns incorrect values to an asset. For example, the wrong vendor or product name.

Feedback is always recorded. Each submission is stored independently; new feedback does not replace or overwrite previous entries.

Asset lifecycle management

Asset Intelligence provides lifecycle information for enriched assets, including end of sale dates, end of support dates, and recommended successor products.

Overview

When *AI* enriches an asset, it includes lifecycle data from the enrichment database. This data helps you identify assets that are approaching or have passed end of life, and plan migrations to replacement products.

Lifecycle fields

AI provides the following lifecycle-related fields for enriched assets:

Lifecycle status

: The current lifecycle status of the product. This indicates whether the product is actively supported, approaching end of life, or no longer supported.

End of sale date

: The date when the vendor stops selling the product. After this date, new purchases of the product are no longer possible through official channels.

End of support date

: The date when the vendor stops providing support, updates, and security patches. Assets past this date present increased security risk.

Successor product

: The recommended replacement product identified by the vendor. When available, this field includes the product name and a link to the successor product information.

Use cases

Lifecycle data from *AI* supports the following activities:

- **Risk assessment**: Assets past their end of support date no longer receive security patches. Use this data to prioritize these assets for replacement or additional monitoring.
- **Migration planning**: Use successor product information to plan hardware and software replacements before support ends.
- **Budget planning**: Identify assets approaching end of sale to forecast replacement costs.
- **Compliance reporting**: Generate reports showing the lifecycle status of all assets in your environment.

Query enriched lifecycle data

You can use the *N2OS* query language to filter assets by lifecycle information. For example, use the `is_ai_enriched` field to find enriched assets and then filter by lifecycle-related fields in the enrichment data.

CPE generation

Asset Intelligence automatically generates Common Product Enumeration (CPE) entries for enriched assets, improving vulnerability matching accuracy.

Overview

As part of the enrichment process, *AI* generates Common Product Enumeration (*CPE*) entries for each enriched asset. *CPE*s are standardized identifiers that link assets to known products in vulnerability databases.

How CPE generation works

When *AI* enriches an asset, the enrichment service returns *CPE* data along with the enrichment results. The platform then:

1. Generates *CPE* strings in the standard *CPE* 2.3 format.
2. Calculates a likelihood score for each *CPE* match.
3. Removes any previously generated *CPE*s for the asset if the *CPE* signature has changed.
4. Inserts the new *CPE* records and links them to the asset.

CPE fields

Each generated *CPE* record contains the following fields:

- *CPE* **string**: The full *CPE* 2.3 identifier
- **Part**: The *CPE* part (hardware, operating system, or application)
- **Vendor**: The *CPE* vendor identifier
- **Product**: The *CPE* product identifier
- **Version**: The *CPE* version identifier
- **Edition and update**: Additional *CPE* classification data
- **Likelihood**: A score indicating the confidence of the *CPE* match
- **Human-readable names**: Readable versions of vendor, product, version, and edition

Impact on vulnerability matching

*CPE*s generated by *AI* are used for vulnerability matching. When the platform has an accurate *CPE* for an asset, it can match the asset against known vulnerabilities more precisely. This matching uses the *Common Vulnerabilities and Exposures (CVE)* database.

AI-generated *CPE*s are identified by the `asset-enrichment` translator tag. This distinguishes them from *CPE*s generated by other sources.

CPE updates

*CPE*s are automatically updated when the enrichment service provides new data. Each asset has a *CPE* signature hash that prevents unnecessary updates. When the signature changes, old *CPE*s are replaced with the updated versions.

Asset Intelligence and Asset Risk

Asset Intelligence powers the Asset Risk feature by providing enriched asset data that feeds into risk scoring and remediation recommendations.

Important:
Asset Risk scoring, dashboards, trends, and remediation recommendations are available only in Vantage. For a full list of capabilities by product, see Product availability (on page 9).

How Asset Intelligence feeds Asset Risk

AI and Asset Risk work together to provide comprehensive risk assessment for your assets. When *AI* enriches an asset, the system uses the enrichment results to calculate risk scores.

The data flow follows this sequence:

1. *AI* enriches the asset with vendor, product, type, and lifecycle data.
2. The enrichment results include risk assessment data.
3. Asset Risk calculates risk scores based on the enriched data and other factors.
4. The system generates risk remediation recommendations based on the analysis.

Figure 5. Data flow from Asset Intelligence to Asset Risk

Risk dimensions

Asset Risk evaluates assets across the following dimensions:

Global risk

The overall risk score that combines all individual risk dimensions into a single value.

Communication risk

Risk based on the asset's network communication patterns. Evaluates recent network links and communication behavior.

Vulnerabilities risk

Risk based on known vulnerabilities. Uses *CPE*s generated by *AI* to match assets against vulnerability databases.

Device risk

Risk based on the device type and characteristics. Enriched asset type and technology category data from *AI* improves the accuracy of this score.

Alerts risk

Risk based on active alerts associated with the asset.

Impact of enrichment on risk accuracy

Asset enrichment improves risk scoring accuracy in several ways:

- **Better vulnerability matching**: *CPE*s generated by *AI* provide more precise vulnerability matches
- **Lifecycle awareness**: End-of-life and end-of-support data affects the device risk score
- **Accurate classification**: Correct asset type and technology category improve the relevance of risk calculations

Risk remediations

Based on the risk analysis, the system generates remediation recommendations. Each remediation includes a unique identifier and a suggested action to reduce the asset's risk level.

Remediations are available through the Asset Risk widgets in the Vantage user interface and through the *application programming interface (API)*.

Risk trends

The platform tracks risk levels over time, providing trend data at multiple levels:

- Organization-level risk trends
- Site-level risk trends
- Sensor-level risk trends
- Zone-level risk trends

Risk benchmarks are available to compare your environment's risk levels against reference baselines.

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**.

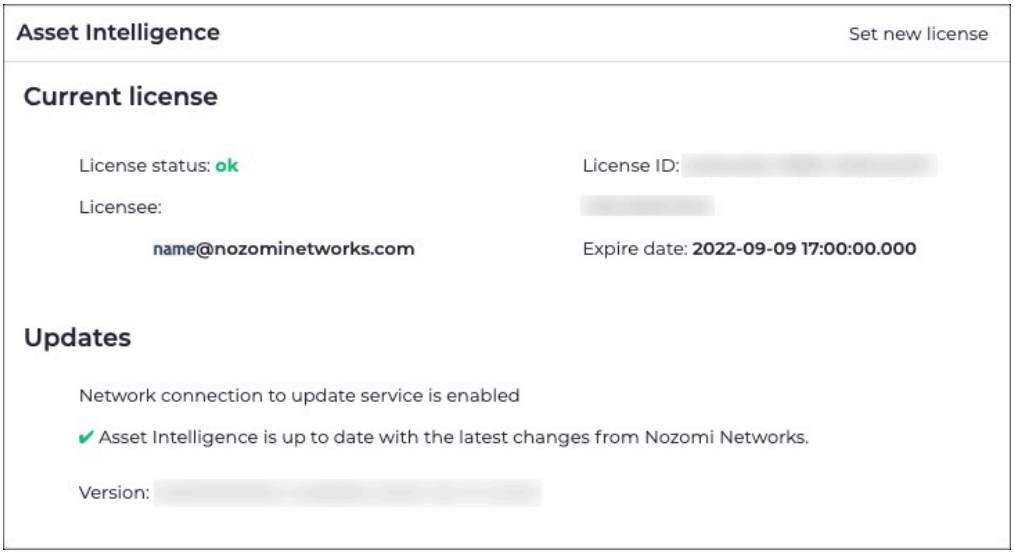


Figure 6. Asset Intelligence license

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

Figure 7. Utility navigation bar

Chapter 2. Requirements

Resource requirements

Asset Intelligence requires network connectivity and platform resources to enrich assets and calculate risk scores.

Important:
Asset Intelligence enrichment processing runs in Vantage. Guardian and *CMC* appliances receive enrichment results but cannot perform enrichment independently. For a full list of capabilities by product, see Product availability (on page 9).

License requirements

Asset Intelligence requires a valid license key. The license is installed and managed through the Vantage platform.

Network requirements

Asset Intelligence communicates with an external enrichment service. The following network connectivity is required:

- Outbound connectivity to the Nozomi Networks enrichment service
- If a proxy is configured, the proxy must support the required protocols
- Sensors that produce assets must be reachable from the platform

For air-gapped environments, manual content updates are available as an alternative. For more details, see Configure manual updates (on page 30).

Chapter 3. 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:

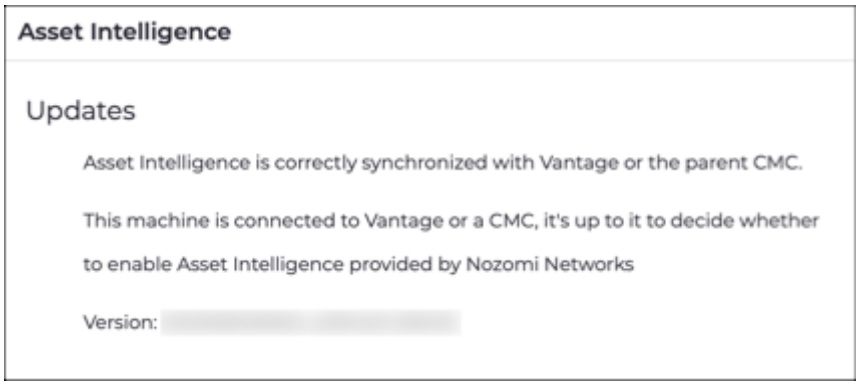
   - In the status bar, select the `AI` icon
   - In the top navigation bar, select ⚙ **> System > Updates and licenses**

   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 *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`.

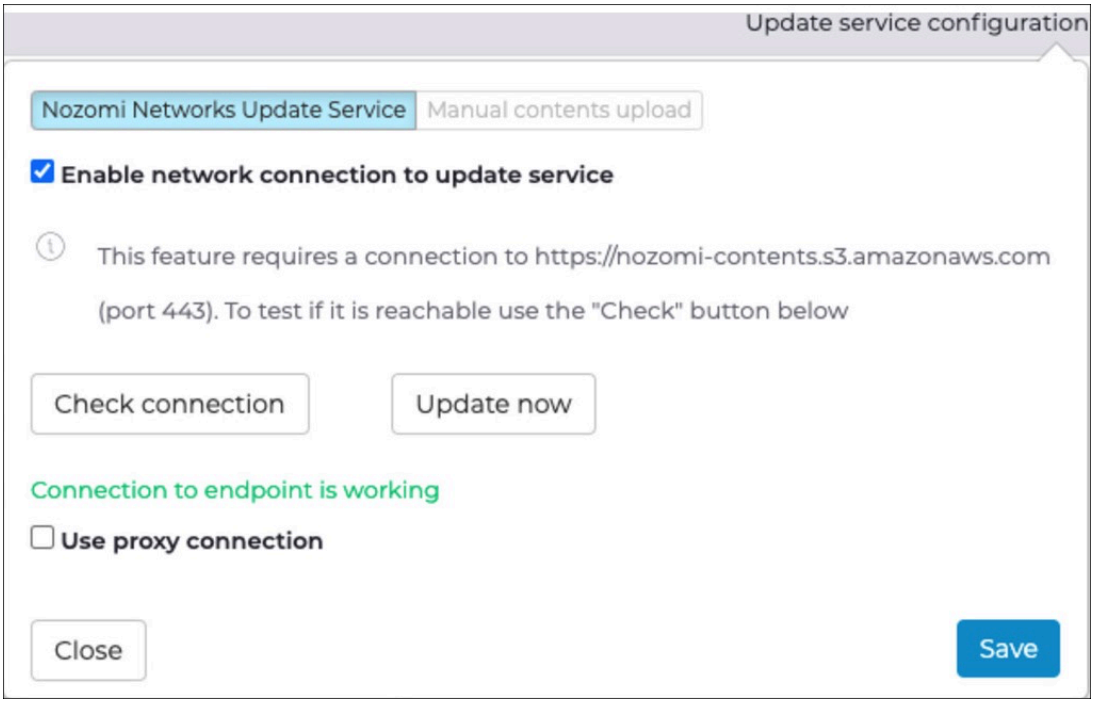
6. Select **Update now** to update the Asset Intelligence output immediately.

   > **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.

Enrichment modes

Asset Intelligence supports three enrichment modes that control the balance between enrichment coverage and accuracy.

Note:
Enrichment mode configuration is available only in Vantage. Guardian and CMC appliances use the mode configured in Vantage for their enrichment results. For more details, see Product availability (on page 9).

The enrichment mode determines how *AI* handles uncertain predictions. Configure the enrichment mode at the organization level.

Available modes

AI offers the following enrichment modes:

High confidence only

The most conservative mode. *AI* only applies enrichments with very high confidence scores. This mode minimizes false positives but results in lower enrichment coverage. Use this mode in environments where accuracy is critical.

Safe enrichment (default)

A balanced mode that discards uncertain predictions. This mode provides a good balance between accuracy and coverage. Safe enrichment is the recommended mode for most deployments.

Aggressive enrichment

The most permissive mode. *AI* maximizes enrichment coverage by including uncertain predictions. This mode has a higher false positive rate. Use this mode when broad asset discovery and classification is the priority.

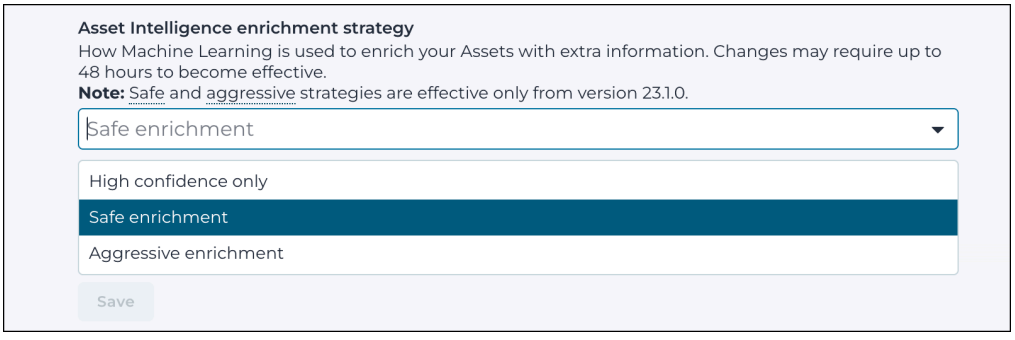


Figure 8. Enrichment mode configuration in Vantage

Choose the right mode

Consider the following factors when selecting an enrichment mode:

- **Environment sensitivity**: Critical infrastructure environments benefit from high confidence only mode to minimize incorrect enrichments
- **Asset visibility goals**: If broad coverage is the priority, aggressive enrichment provides the widest visibility
- **Feedback loop**: Use the enrichment feedback mechanism to report incorrect enrichments and improve future accuracy regardless of the mode

Impact of mode changes

Changing the enrichment mode affects only future enrichment requests. Existing enrichments are not retroactively modified. After changing the mode, new enrichment results reflect the updated confidence thresholds on the next enrichment cycle.

Chapter 4. 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.

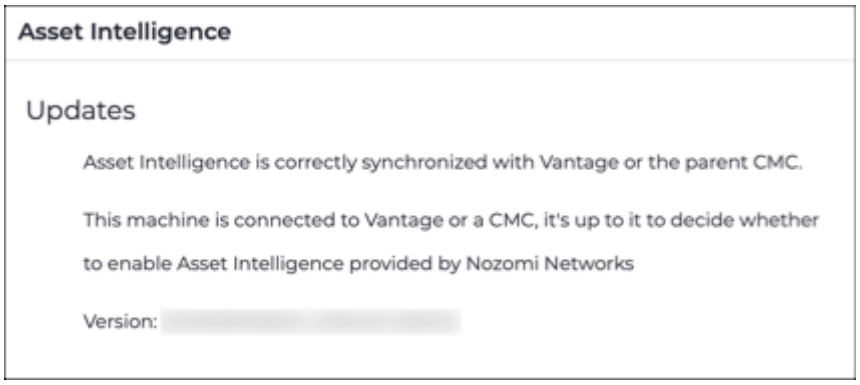
2. Choose a method to open the **Updates and licenses** page.

   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.

Chapter 5. Troubleshooting

Troubleshoot Asset Intelligence

Solutions for common Asset Intelligence issues, including enrichment failures, connectivity problems, and unexpected results.

Connectivity issues

AI requires outbound connectivity to the Nozomi Networks enrichment service. If enrichments are failing due to connectivity:

- Verify that outbound connections are permitted by your firewall rules
- If a proxy is configured, verify that the proxy settings are correct
- Check for network timeout errors in the platform logs

For air-gapped environments, use manual content updates instead of automatic updates. For more details, see Configure manual updates (on page 30).

Low confidence scores

If enrichments have low confidence scores:

- Verify that sensors have visibility to sufficient network traffic for the assets. *AI* uses all available asset fields to find the best match.
- Consider switching to the **aggressive enrichment** mode if broader coverage is acceptable. For more details, see Enrichment modes (on page 31).
- Use the enrichment feedback mechanism to report incorrect enrichments and improve future results

Incorrect enrichments

If an asset receives an incorrect enrichment:

- Submit negative feedback on the enrichment. This helps the enrichment service improve its accuracy for similar assets.
- If you are using aggressive enrichment mode, consider switching to safe enrichment mode to reduce false positives
- Verify that the asset's base data (vendor, product name) is correct in the asset inventory

Enrichments not propagating to sensors

If enrichments are visible on the platform but not propagating to sensors:

- Verify that the sensor supports enrichment propagation
- Check that the sensor is reachable from the platform
- Review the sensor logs for any enrichment command errors

Glossary

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.

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 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.

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.

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.

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.

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.

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.

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.

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.

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.