NOZOMI NETWORKS

Vantage for Government
User Guide

2026-09-02

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 **9**
- Vantage for Government overview 11
- Vantage and Vantage for Government comparison 13
- Architecture 15
- Data security in Vantage 16
- Compliance and certifications 17
- Graphical User Interface (GUI) 20
  - Homepage 20
  - Top navigation bar 21
  - Footer 24
- Get more from Vantage 26
  - Respond to the Get more from Vantage prompt 27

Chapter 2. Sensors **31**
- Overview 34
- Detailed list 36
- Details page 39
  - Summary tab 40
  - Synchronization tab 41
  - Settings tab 42
  - Health logs tab 42
  - Tags tab 44
  - Security control panel tab 47
  - Network interfaces tab 48
  - Support archives tab 49
  - Arc dependencies tab 51
- Summary drawer 58
- Table interactions 59
  - Actions menu 59
  - Open the details page 69
  - Open the summary drawer 69
- Connect a sensor 70
  - Identify and copy the sensor ID 70
  - Add a sensor 71
  - Configure a sensor 76
  - Arc sensor configuration 77
  - Complete the connection of a sensor 86
  - Verify the connection of a sensor 87
  - Reset a sensor token 88
- Troubleshooting 89

Sensor will not connect....89
Chapter 3. Alerts....91
Overview....94
Detailed list....96
Details page....98
Summary drawer....100
Table interactions....101
Chapter 4. Assets....113
Overview....116
Detailed list....118
Details page....120
Summary tab....122
Risk tab....124
Processes tab....126
Users tab....127
Hardware Components tab....128
Nodes tab....131
Links tab....132
Sessions tab....133
Variables tab....134
Vulnerabilities tab....135
CPEs tab....136
Software tab....137
Alerts tab....138
Tags tab....139
Sensors tab....142
Summary drawer....143
Table interactions....144
Actions menu....144
Open the details page....148
Open the summary drawer....148
Chapter 5. Wireless....149
Networks....153
Channels....154
Spectrum....155
Details page....156
Actions menu....157
Chapter 6. Queries....163
Editor....166
Saved Queries....168
Saved Assertions....169
Customize assertion name and description....170

Execute a query....172
Commands....173
Functions....181
Chapter 7. Vulnerabilities....187
Overview....190
Detailed list....192
Details page....194
Summary drawer....196
Table interactions....197
Workbooks....201
Chapter 8. Vantage IQ....203
Requirements....206
IQ assistant widget....207
Open the IQ assistant widget....209
Close the IQ assistant widget....210
Assistant....211
Start a new chat....213
Open a previous chat....214
Rename a chat....215
Delete a chat....216
Insights....217
Open insight details....219
Run an on-demand insights analysis....220
Dismiss an applied insight....221
Time Series....222
IQ summaries....223
Open the IQ summary drawer....225
Queries....228
Cluster....229
Compare....231
Correlation....232
Describe....233
Forecast....234
Pivot....235
Popular....236
Simplify....237
Timeline....238
Versus....239
Visualize....240
Chapter 9. Network....241
Nodes....244
Links....245
Sessions....246

Chapter 10. Graph **247**
Network graph 250
Physical graph 253
Graph customization 256
Chapter 11. Process **263**
Table interactions 266
Actions menu 266
Chapter 12. Dashboards **267**
Create a dashboard 270
Import a dashboard 271
Export a dashboard 272
Add a widget 273
Print a dashboard 274
Chapter 13. Reports **275**
Vantage 278
Create a report 279
Import a report 282
Print a report 283
From Sensors 284
Table interactions 285
Actions menu 285
Chapter 14. Sites **287**
Table interactions 290
Actions menu 290
Chapter 15. Workbooks **293**
Use a workbook to improve your network security 296
Chapter 16. Threat Intelligence **297**
Malware 301
Actors 303
Vulnerability 305
Chapter 17. Asset Risk **307**
Overview 310
Remediations 312
Details 313
Benchmarks 315
Chapter 18. Smart Polling **317**
Overview 320
Plan creation 322
Automatically add a plan 326
Manually add a plan 330

Centralized plan management....336
Actions menu....339
Smart Polling results....343
Activity Log....345
Chapter 19. Segmentation Advisor....347
Overview....350
Actions....352
Chapter 20. Integrations....353
Overview....356
Detailed list....358
Add a data importer....360
Add a data exporter....361
Static egress IP addresses for integrations....362
Chapter 21. Async operations....365
Chapter 22. What's new drawer....369
Chapter 23. Administration....373
Administration page....375
Chapter 24. Profile settings....377
Authentication....380
API Keys....381
Theme....383
Chapter 25. Organizations menu....385
Glossary....389

Chapter 1. Introduction

Vantage for Government overview

Vantage for Government is a Software as a Service (SaaS) product that lets you monitor and protect your networks. Vantage for Government lets you respond faster and more effectively to cyber threats, to ensure your operational resilience.

General

Vantage for Government (**Vantage™**) uses the power and simplicity of *Software as a Service (SaaS)* to deliver unmatched security and visibility across your *operational technology (OT)*, *Internet of Things (IoT)*, and *information technology (IT)* networks.

Vantage lets you:

- Centrally manage all sensor deployments from a single application
- Monitor an unlimited number of devices
- Protect an unlimited number of locations

Identify

Vantage lets you discover and identify your assets and visualize your networks. Its ability to automate processes to create asset inventories eliminates blind spots and increases awareness of your networks.

Dashboards let you generate macro views, as well as see detailed information on assets and connections in your networks. Vantage also shows extensive node information such as names, types, and firmware versions as well as asset behavior, roles, protocols, and data flows.

Assess

Vantage shows security alerts, missing patches and vulnerabilities to let you automatically assess vulnerabilities and monitor risks. It also correlates known vulnerabilities to *Common Vulnerabilities and Exposures (CVE)* reports to quickly research the root cause and potential impact. Vulnerability dashboards let you prioritize your efforts to focus on high-impact risk reductions first.

Vantage continuously monitors all supported protocols for the *OT*, *IoT*, and *IT* industries. It summarizes *OT* and *IT* risk information and highlights indicators of reliability issues, such as unusual process values.

Detect

Vantage gives you constantly updated threat detection to identify cybersecurity and process-reliability threats. It detects early and late stage advanced threats and cyber risks.

Vantage combines behavior-based anomaly detection with signature-based threat detection for comprehensive risk monitoring.

An optional subscription to **Threat Intelligence™** gives you up-to-date threat detection and vulnerability identification, which uses indicators that have been created and curated by Nozomi Networks Labs.

In addition, an optional subscription to **Asset Intelligence™** gives you breakthrough anomaly-detection accuracy for *OT* and *IoT* devices, which accelerates incident response times.

Act

Vantage accelerates your global incident response capabilities. It does this by focusing your attention on critical vulnerabilities, and letting you prioritize activities that maximize risk reduction.

Pre-defined playbooks guide users, and specific teams, in their efforts to counter the different types of threats. A centralized dashboard consolidates data to create high-priority alerts across a global network.

Clear explanations describe what has happened, the possible cause, and suggested solutions for every alert, which reduces the need for additional investigation.

Vantage lets you group alerts into incidents. This gives security and operations staff a simple, clear, and consolidated view of what's happening in your networks.

Scale

Vantage aggregates data from an unlimited number of globally-deployed sensors. It delivers customizable summaries of essential information which lets you drill down to individual sites or assets.

It streamlines security processes across *IT* and *OT* for a cohesive response.

Vantage lets you manage security risks centrally for all your global sites.

Related information

Architecture (on page 15)

Data security in Vantage (on page 16)

Vantage and Vantage for Government comparison

Vantage for Government is specifically designed to meet the unique requirements of U.S. government agencies and organizations that must comply with federal security and operational standards.

Overview

Vantage for Government provides the same core functionality as Vantage, with additional configurations and operational practices to support U.S. government deployment requirements. Both products deliver comprehensive security and visibility across *OT*, *IoT*, and *IT* networks.

Key differences

The following table summarizes the key differences between Vantage and Vantage for Government:

Table 1. Vantage and Vantage for Government comparison

Feature	Vantage	Vantage for Government
Target audience	Commercial enterprises	U.S. Government agencies and organizations with FedRAMP compliance requirements
Compliance framework	Industry standard security practices	*National Institute of Standards and Technology (NIST)* FedRAMP Moderate compliance standards
Data residency	Standard cloud infrastructure	FedRAMP-compliant data centers
Core features	Full feature set	No third-party integrations (they will be introduced in a future release)
User experience	Standard interface	Identical interface

Shared capabilities

Both Vantage and Vantage for Government include:

- Complete asset discovery and inventory management
- Real-time threat detection and alerting
- Vulnerability assessment and monitoring
- Network visualization and analysis
- Customizable dashboards and reports
- Integration with third-party security tools
- Centralized management of distributed sensors

- *Asset Intelligence (AI)*-driven security insights (when licensed)
- **Threat Intelligence™** integration (when licensed)

Choosing the right product

Select Vantage for Government if your organization:

- Is a U.S. government agency or contractor
- Must comply with federal security requirements
- Requires data residency in government-compliant facilities
- Needs audit trails that meet federal standards

Select standard Vantage for commercial deployments that do not require government-specific compliance frameworks.

Related information

Vantage for Government overview (on page 11)

Architecture

You can use Vantage, and the flexible architecture, to create a customized solution.

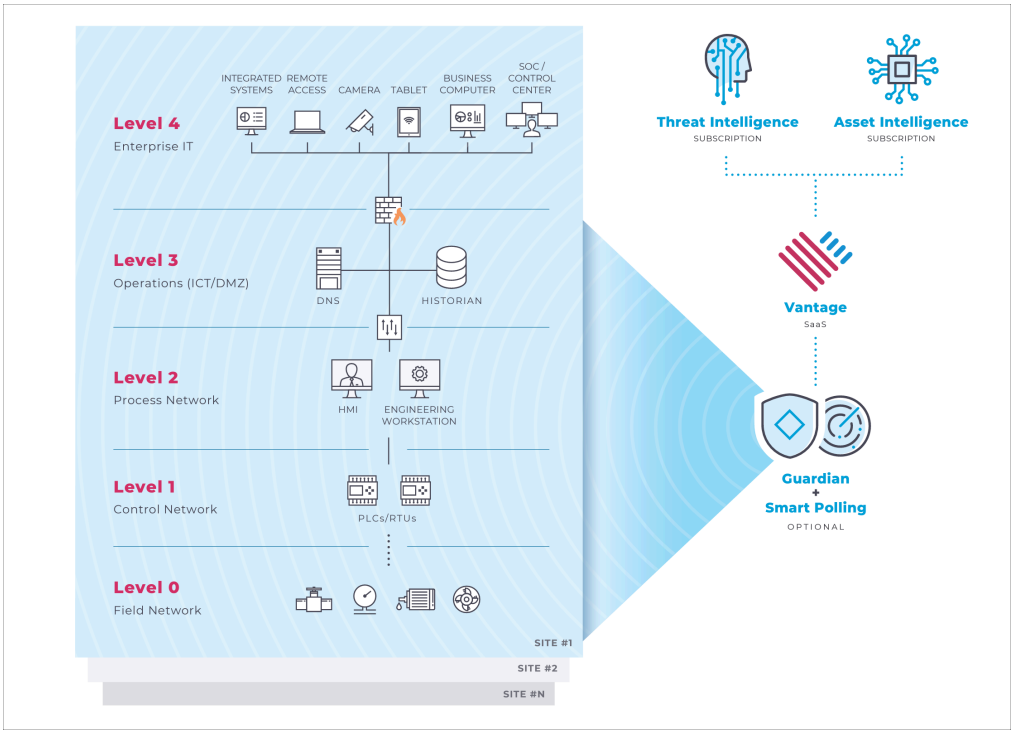


Figure 1. Vantage architecture

Data security in Vantage

It is important to understand how Vantage keeps your data secure.

Data privacy

For more details, see Nozomi Networks Vantage Data Privacy.

Data segregation and encryption

Data segregation is a key element of data security in Vantage. Every Vantage implementation has its own database. Access to an instance's database requires an encryption key that is only used for this instance.

FIPS support

The *NIST* develops *Federal Information Processing Standards (FIPS)*, which are publicly-announced standards for use in computer systems in-use with non-military United States government agencies and government contractors. The *FIPS* 140 series specifies requirements for cryptography modules within a security system protecting sensitive, but unclassified, data.

For implementations that adhere to *FIPS*, Nozomi Networks provides *FIPS*-compliant Vantage instances that use the FIPS-140-2 approved cryptography module.

While a *FIPS*-compliant sensor cannot connect to a standard, non-*FIPS* Vantage instance, an unlicensed sensor can connect to a *FIPS*-compliant Vantage instance. This allows Vantage to assign a license and enable *FIPS* mode on the sensor. Vantage now manages the sensor's license, and it can only connect to a *FIPS*-compliant Vantage instance.

To learn more about *FIPS*, contact Nozomi Networks.

FIPS-compliant Vantage and SAML configuration

When you use *security assertion markup language (SAML)* to configure Vantage for SSO, you must specify its *assertion consumer service (ACS) uniform resource locator (URL)*.

If your Vantage instance is *FIPS*-compliant, its *ACS URL* differs from the *ACS URL* of non-*FIPS* instances. For example:

- The *ACS URL* of a standard, non-*FIPS* Vantage instance is similar to:
  `https://customer1.customers.us1.vantage.nozominetworks.io`
- The *ACS URL* of a *FIPS*-compliant Vantage instance is similar to:
  `https://nozominetworkscom.customers.us1.vantage-govcloud.nozominetworks.io`

For more details about *ACS URL*s, see **IdP configuration for SAML integration**, in the **Administrator Guide**.

Compliance and certifications

Vantage for Government maintains compliance with U.S. federal security standards and requirements to ensure secure operations for government agencies and contractors.

Overview

Vantage for Government is designed and operated to meet the stringent security and compliance requirements of U.S. federal agencies. The platform undergoes regular assessments and maintains certifications that demonstrate adherence to federal standards.

FedRAMP authorization

This service is authorized under the *Federal Risk and Authorization Management Program (FedRAMP)* at the **Moderate** impact level. The authorization was issued by a U.S. federal authorizing agency following a comprehensive security assessment in accordance with *FedRAMP* requirements.

The *FedRAMP* Moderate *Authorization to Operate (ATO)* confirms that the service meets the security controls defined in *NIST* SP 800-53 for systems processing *Controlled Unclassified Information (CUI)*, where the potential impact of a security compromise could be serious to agency operations, assets, or individuals.

Any authorization conditions, limitations, or constraints applicable to this service are documented as part of the *FedRAMP* authorization package and are maintained in accordance with *FedRAMP* continuous monitoring requirements.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services used by U.S. federal agencies.

Vantage for Government

Vantage for Government Is authorized under *FedRAMP* at the Moderate impact level.

This authorization demonstrates compliance with federal security requirements defined in *NIST* Special Publication 800-53.

For more details, see FedRAMP authorization.

Compliance frameworks

Vantage for Government adheres to the following federal compliance frameworks:

FISMA compliance

: The *Federal Information Security Management Act (FISMA)* establishes requirements for federal information security programs. Vantage for Government implements security controls that support FISMA compliance.

NIST 800-53 security controls

: The platform implements security controls from *NIST* Special Publication 800-53, which provides a catalog of security and privacy controls for federal information systems and organizations.

FIPS 140-2 cryptography

All cryptographic operations use *FIPS* 140-2 validated modules to ensure data protection meets federal standards. For details, see Data security in Vantage (on page 16).

Department of Defense compliance

Vantage for Government aligns with applicable *Department of Defense (DoD)* cloud security requirements where required by customer deployment, including impact level considerations consistent with the *DoD* Cloud Computing *Security Requirements Guide (SRG)*.

Data residency and infrastructure

Vantage for Government operates within infrastructure that meets U.S. federal data residency and sovereignty requirements.

All customer data is stored and processed within **AWS GovCloud (US-East)** regions.

Data centers are located within **authorized U.S. government cloud regions**, with specific locations not publicly disclosed for security reasons.

No customer data is transmitted to or stored outside of authorized federal cloud infrastructure.

Personnel with access to customer data undergo background checks appropriate for government systems.

Audit and continuous monitoring

Vantage for Government maintains audit logs in accordance with *FedRAMP* Moderate requirements to support security monitoring, incident response, and compliance reporting.

Audit logs are retained for periods consistent with federal security control requirements and are protected against unauthorized access or modification. Authorized customers can export audit logs to approved government *security information and event management (SIEM)* or log aggregation systems using supported, secure mechanisms.

Compliance documentation

Organizations using Vantage for Government can access compliance documentation to support their own authorization and risk management processes.

The *FedRAMP* compliance artifacts below are made available to authorized government customers and partners upon request and are subject to applicable access controls and non-disclosure requirements:

- *System Security Plan (SSP)*
- *Security Assessment Report (SAR)*
- *Plan of Action and Milestones (POA&M)*
- Other related materials

Compliance updates

Federal security requirements and certifications are subject to change. Vantage for Government maintains current compliance through regular assessments and updates to security controls as requirements evolve.

Customers are notified of significant changes to compliance status or certifications through **direct communication from Nozomi Networks**, including email notifications and system announcements, as appropriate.

Related information

Vantage for Government overview (on page 11)

Vantage and Vantage for Government comparison (on page 13)

Graphical User Interface (GUI)

Homepage

*The **Overview** page is the default view in Vantage. It provides a high-level summary of your network's security health across key domains.*

When you sign into Vantage, the **Overview** page gives you a high-level view of your network's security health. The page is organized into sections by security domain, including assets, alerts, vulnerabilities, and traffic. Each section displays summary counts, trend charts, and breakdowns by the most relevant categories. Select **See more** in any section to open the corresponding dedicated page for deeper investigation.

Filters

Use the filters at the top of the page to control the scope of the data displayed. You can filter by the organizational scope and by time range. The filtered scope applies to all sections on the page.

Top navigation bar

The top navigation bar lets you navigate to the different areas of the software.

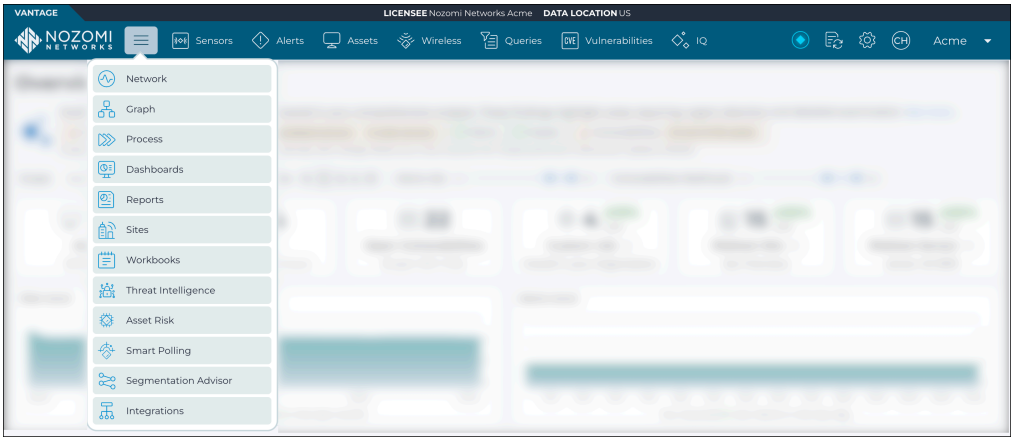


Figure 2. Top navigation bar

Hamburger menu

The ☰ icon opens a dropdown menu, which gives you access to buttons for these items:

- Network (on page 21)
- Graph (on page 21)
- Process (on page 21)
- Dashboards (on page 21)
- Reports (on page 22)
- Sites (on page 22)
- Workbooks (on page 22)
- Threat Intelligence (on page 22)
- Asset Risk (on page 22)
- Smart Polling (on page 22)
- Segmentation Advisor (on page 22)
- Integrations (on page 22)

Network

This button opens the **Network** page. For more details, see Network (on page 241).

Graph

This button opens the **Graph** page. For more details, see Graph (on page 247)

Process

This button opens the **Process** page. For more details, see Process (on page 263)

Dashboards

This button opens the **Dashboards** page. For more details, see Dashboards (on page 267).

Reports
This button opens the **Reports** page. For more details, see Reports (on page 275).

Sites
This button opens the **Sites** page. For more details, see Sites (on page 287).

Workbooks
This button opens the **Workbooks** page. For more details, see Workbooks (on page 201).

Threat Intelligence
This button opens the **Threat Intelligence** page. For more details, see Threat Intelligence (on page 297).

Asset Risk
This button opens the **Asset Risk** page. For more details, see Asset Risk (on page 307).

Smart Polling
This button opens the **Smart Polling** page. For more details, see Smart Polling (on page 317).

Segmentation Advisor
This button opens the **Segmentation Advisor** page. For more details, see Segmentation Advisor (on page 347).

Integrations
This button opens the **Data integrations** page. For more details, see Data integrations (on page 353).

Sensors
This button opens the **Sensors** page. For more details, see Sensors (on page 31).

Alerts
This button opens the **Alerts** page. For more details, see Alerts (on page 91).

Assets
This button opens the **Assets** page. For more details, see Assets (on page 113).

Wireless
This button opens the **Wireless** page. For more details, see Wireless (on page 149).

Queries
This button opens the **Queries** page. For more details, see Queries (on page 163).

Vulnerabilities
This button opens the **Vulnerabilities** page. For more details, see Vulnerabilities (on page 187).

(Vantage) IQ

This button opens the **Vantage IQ** page. For more details, see Vantage IQ (on page 203).

Async operations

This button opens the **Asynchronous operations** page. For more details, see Async operations (on page 365).

Administration

This button opens the **Administration** page. For more details, see the Vantage **Administrator Manual**.

Profile settings

This button opens the profile settings menu. For more details, see Profile settings (on page 377).

Organization

This button opens the profile **Organization** page. For more details, see Organizations menu (on page 385).

Footer

The footer lets you access support resources and page utilities from any page in Vantage.

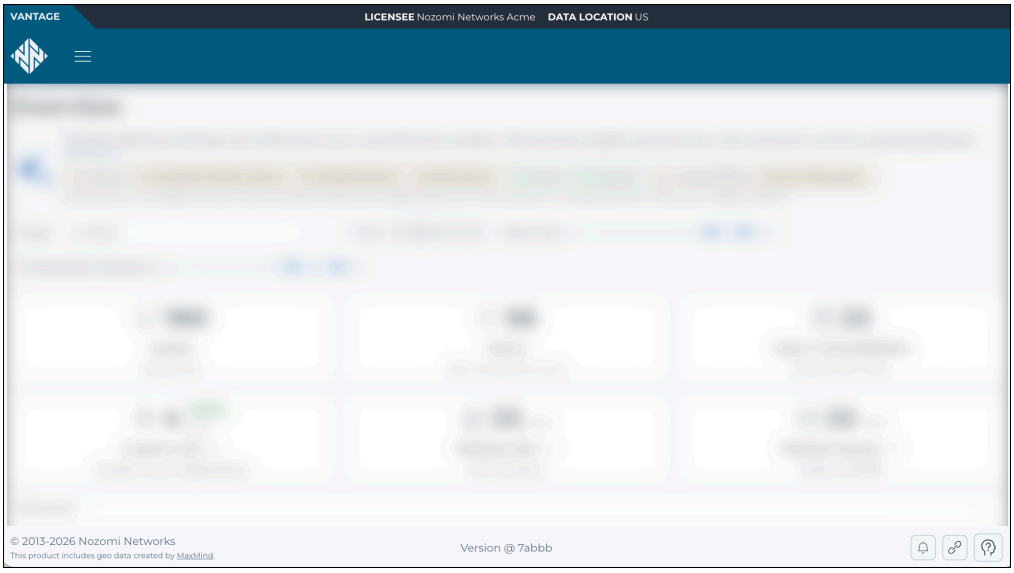


Figure 3. Footer position

Figure 4. Footer icons

What's new

Select to open the **What's new** drawer, which shows a list of new features, enhancements, and fixes. For more details, see What's new drawer (on page 369).

Copy current page URL

Select to copy the current page *URL* to your clipboard.

Documentation and support

Select to open a menu with links to these resources:

- **Open documentation**: Opens the Nozomi Networks technical documentation for Vantage.
- **Open support case**: Opens the Nozomi Networks support portal where you can open a support case.

- **Check Vantage status**: Opens the Vantage status page where you can check for service disruptions.
- **Developer API docs**: Opens the Vantage developer *application programming interface (API)* documentation.

Get more from Vantage

*The **Get more from Vantage** prompt helps root administrators optimize their environment by enabling Discovery and Smart Polling features. These capabilities improve asset visibility and support integration planning based on real usage data.*

Root administrators see the **Get more from Vantage** prompt after logging in. It collects details about software in the environment and offers the option to enable automatic Discovery and Smart Polling plans.

Completing the prompt is optional but recommended. Root administrators can choose to select:

- **Next** to continue with the setup
- **Assign to another user** to delegate the setup
- **Remind me later** to postpone the prompt

This proactive configuration helps Vantage deliver more relevant insights and accelerates time-to-value through intelligent automation.

Respond to the Get more from Vantage prompt

To help Vantage better understand their environment, root administrators see a guided setup dialog after logging in. This process collects preferences and offers the option to enable Discovery and Smart Polling. It improves asset visibility and supports tailored configuration recommendations.

About this task

After login, root administrators are prompted with a short setup dialog that helps identify the software in use and enables Discovery and Smart Polling features. Completing the prompt allows Vantage to automate data collection plans to enhance visibility and insights.

Procedure

1. Log in to Vantage as a root administrator.

   Result: A `Get more from Vantage` dialog shows.

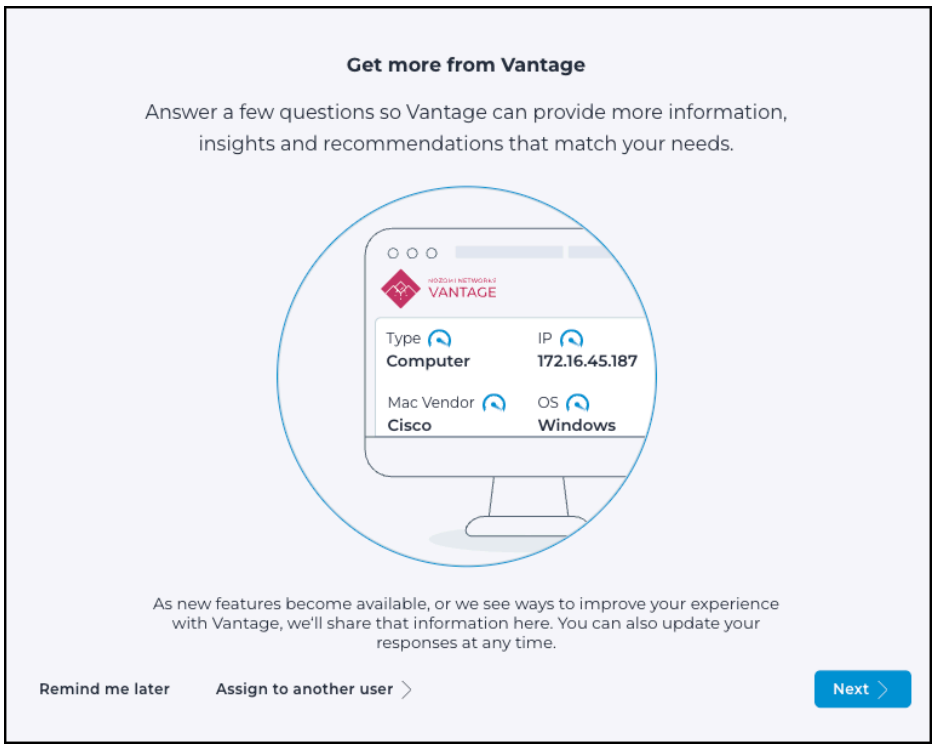


Figure 5. Get more from Vantage dialog

2. Select one of these options:

   Choose from:

   - **Remind me later**: The prompt will appear again the next time that you log in
   - **Assign to another user**: Transfer the task to a different user
   - **Next**: Complete the setup now

3. Select **Next**.

   Result: The **Asset Inventory** page opens.

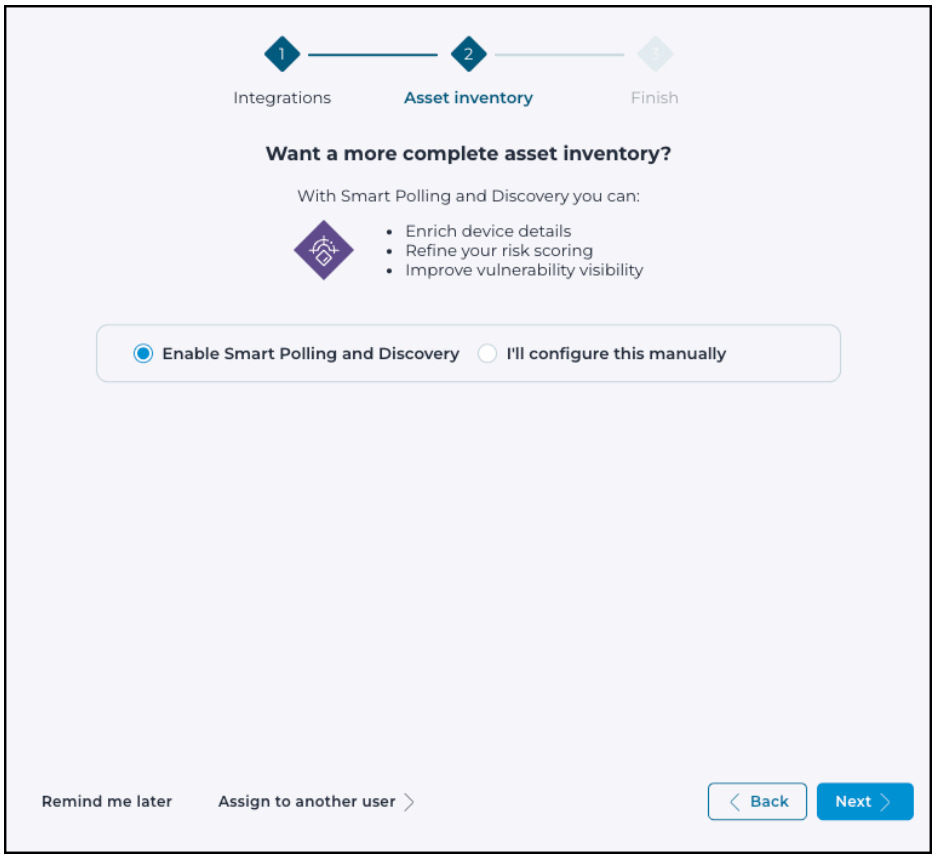


Figure 6. Asset Inventory page

4. On the **Asset Inventory** page:

   Choose from:

   - **Enable Smart Polling and Discovery** – Starts Discovery immediately and schedules Smart Polling plans automatically
   - **No, I'll configure this manually** – Skips automated configuration for now

5. Select **Next**.

   Result: The **Finish** page shows.

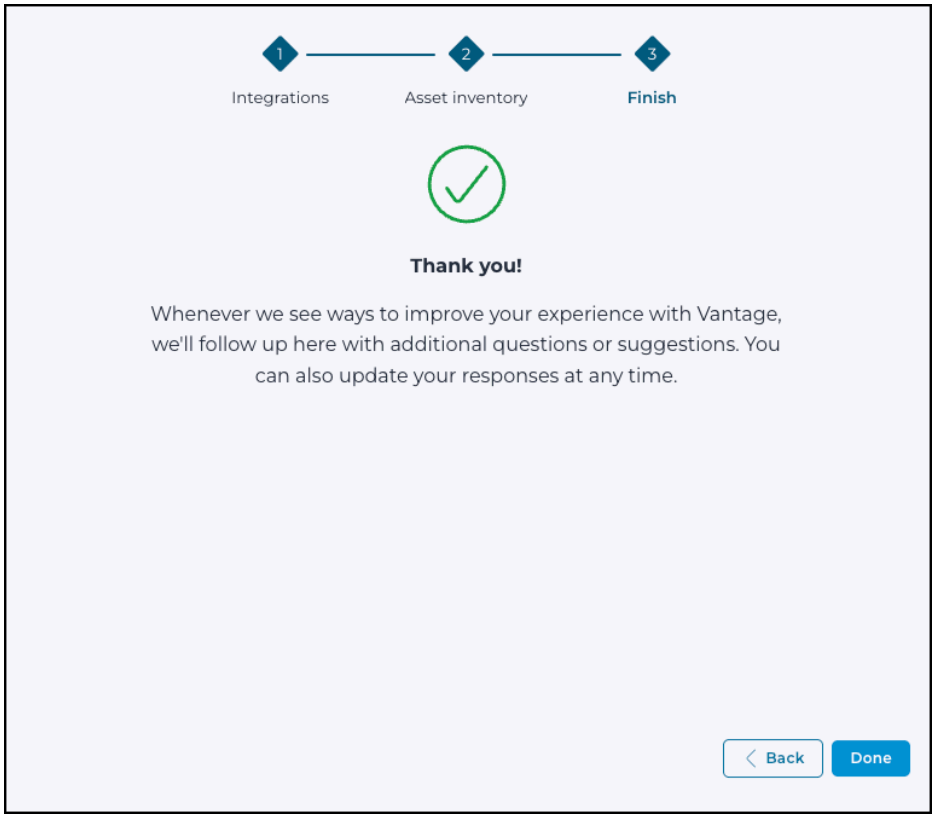


Figure 7. Finish page

Results

The setup is complete. Vantage uses this information to tailor support and improve asset visibility for your environment.

Chapter 2. Sensors

*The **Sensors** page shows all the sensors connected to your Vantage system.*

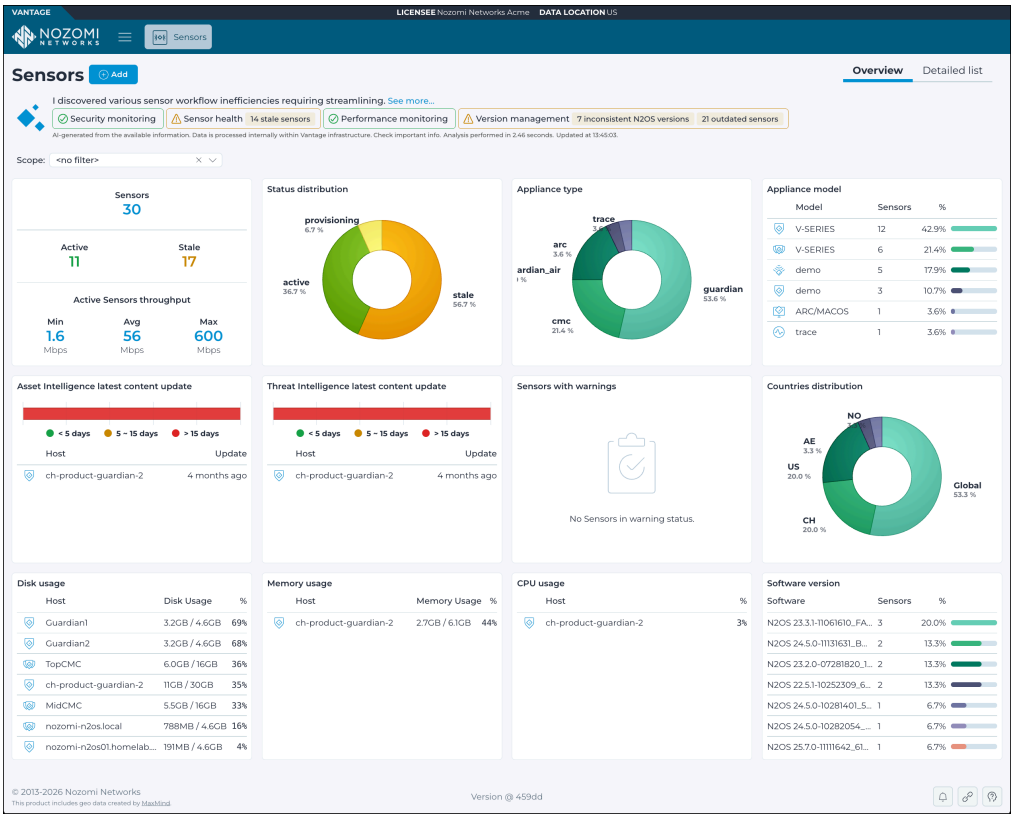


Figure 8. Sensors page

The **Sensors** page has these tabs:

- Overview (on page 34)
- Detailed list (on page 36)

Related information

Add a sensor (on page 71)

Configure a sensor (on page 76)

Verify the connection of a sensor (on page 87)

Reset a sensor token (on page 88)

Overview

*The **Overview** tab provides a high-level summary of your sensors, including their status, appliance types and models, resource usage, intelligence content update status, and geographic distribution.*

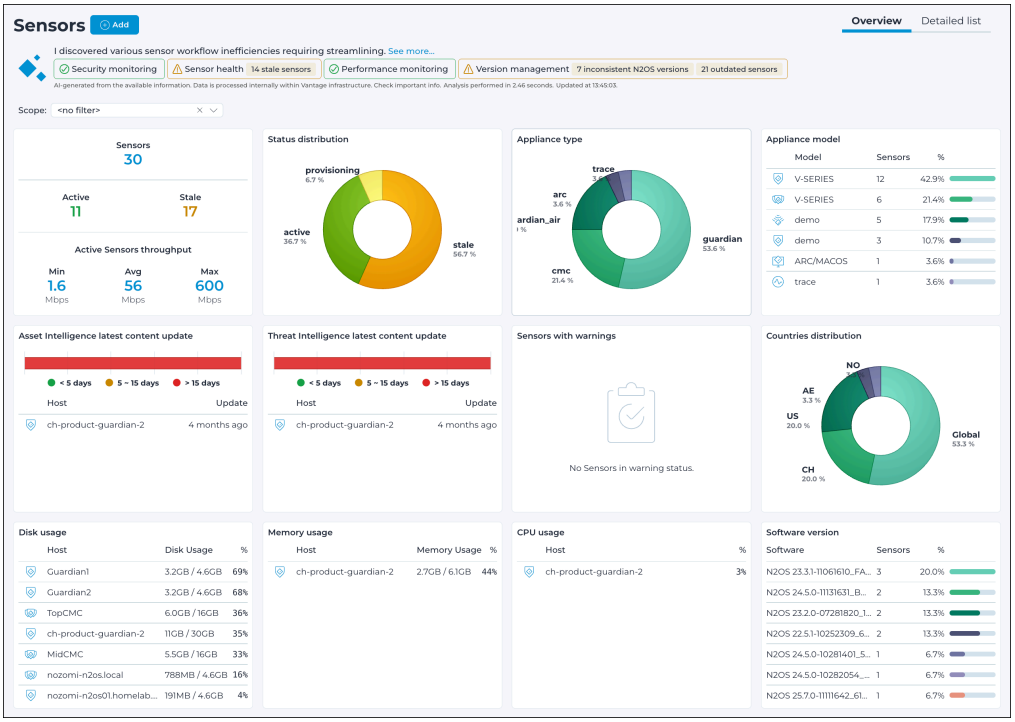


Figure 9. Overview tab

The **Overview** tab displays widgets that summarize the current state of your sensors. Use the **Scope** filter at the top of the page to limit the data shown to a specific site or network domain.

Sensors

This shows a count of all sensors in your system, broken down by status:

- **Active**: sensors that are connected and sending data.
- **Stale**: sensors that have not synced recently.

It also shows the throughput range across all active sensors, expressed as minimum, average, and maximum values in Mbps.

Status distribution

This shows a donut chart of sensors grouped by their current status: active, stale, and provisioning. Each segment is labeled with its percentage of the total.

Appliance type

This shows a donut chart of sensors grouped by appliance type, for example Guardian, *Central Management Console (CMC)*, Arc, Guardian Air, and Trace. Each segment is labeled with its percentage of the total.

Appliance model
This shows a table listing each appliance model alongside the number of sensors using that model and its percentage of the total. A bar indicator provides a visual representation of relative size.

Asset Intelligence latest content update
This shows the date of the most recent Asset Intelligence content update for each sensor host. A color-coded bar indicates how current the update is:

- **Green**: updated less than 5 days ago.
- **Orange**: updated 5–15 days ago.
- **Red**: updated more than 15 days ago.

Threat Intelligence latest content update
This shows the date of the most recent Threat Intelligence content update for each sensor host. The same color-coding applies as for the Asset Intelligence widget:

- **Green**: updated less than 5 days ago.
- **Orange**: updated 5–15 days ago.
- **Red**: updated more than 15 days ago.

Sensors with warnings
This shows a list of sensors that are currently in a warning state. If no sensors have warnings, the widget displays a message confirming that no sensors are in warning status.

Countries distribution
This shows a donut chart of sensors grouped by the country where they are located. Each segment is labeled with its percentage of the total.

Disk usage
This shows a table listing each sensor host with its current disk usage as a used/total value and a percentage. Hosts are sorted by percentage in descending order.

Memory usage
This shows a table listing each sensor host with its current memory usage as a used/total value and a percentage.

CPU usage
This shows a table listing each sensor host and its current *central processing unit (CPU)* usage as a percentage.

Software version
This shows a table listing the *Nozomi Networks Operating System (N2OS)* software versions in use across your sensors, alongside the number of sensors running each version and its percentage of the total. A bar indicator provides a visual representation of relative size.

Detailed list

*The **Detailed list** tab shows all the sensors connected to Vantage. Use this tab to view sensor status, manage sensors, and access individual sensor details.*

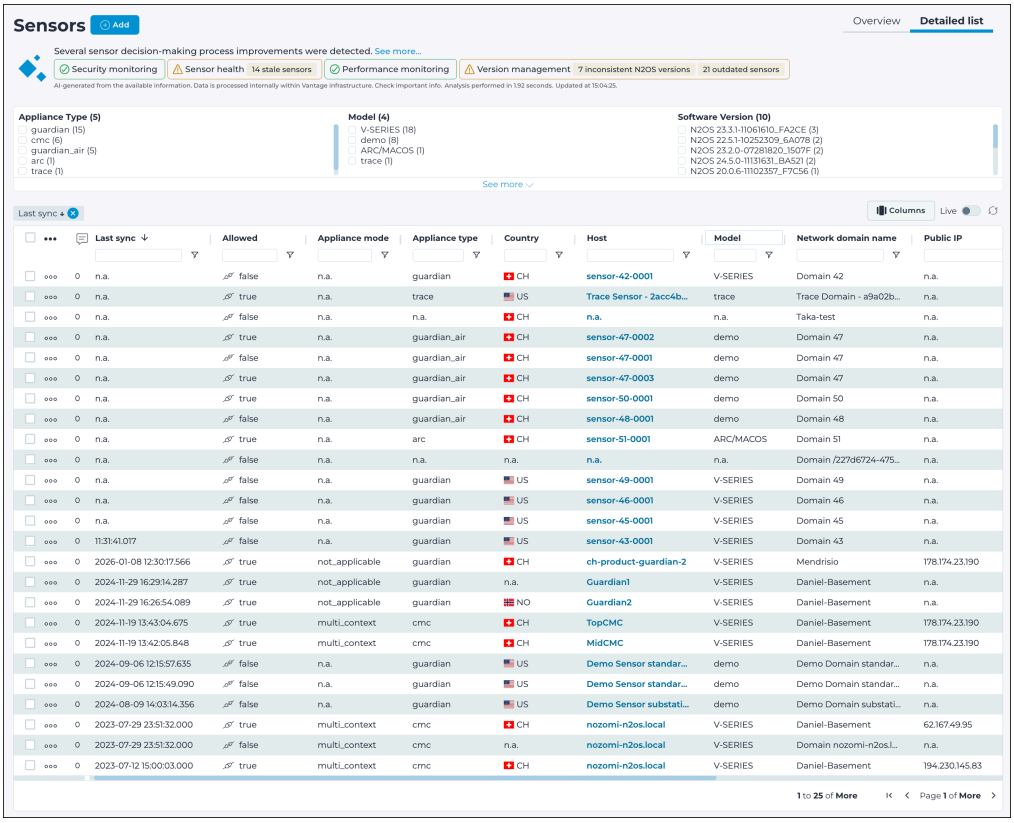


Figure 10. Detailed list tab

Appliance type

Filters the table by the type of appliance running the sensor, for example, Guardian or *CMC*.

Model

Filters the table by the model number of the sensor appliance.

Software version

Filters the table by the version of the sensor software currently installed.

Column descriptions

Column label	Description
Last sync	The last time this sensor sent data to Vantage. Displays **Never** for inactive sensors. If the sensor is not syncing, see Sensor will not connect (on page 89).

Column label	Description
Alerts count	The total number of alerts raised by this sensor.
Alerts count last 5m	The number of alerts raised by this sensor in the last 5 minutes.
Allowed	Indicates whether this sensor is authorized to connect to Vantage.
Appliance mode	The operating mode of the sensor appliance.
Appliance type	The type of appliance running this sensor, for example, **guardian** or **cmc**.
Country	The country where this sensor is located.
CPU percentage	The current *CPU* usage of the sensor as a percentage.
Description	A user-defined description of the sensor.
Disk usage percentage	The current disk usage of the sensor as a percentage.
Health	The overall health status of the sensor: **Good**, **Average**, **Poor**, or **Unknown**.
Host	The logical name of the computer hosting the sensor.
IP	The *internet protocol (IP)* address of the sensor.
Latitude	The latitude coordinate of the sensor's physical location.
Links count	The total number of network links detected by this sensor.
Location source	The method used to determine the sensor's geographic location.
Longitude	The longitude coordinate of the sensor's physical location.
Memory free	The amount of memory currently available on the sensor.
Total memory	The total memory capacity of the sensor.
Memory used	The amount of memory currently in use on the sensor.
Memory used percentage	The current memory usage of the sensor as a percentage.
Model	The model number of the sensor appliance, for example, **N1000R2** or **V_SERIES**.
N2OS version	The version of *N2OS* running on this sensor.

Column label	Description
Network domain name	The domain name of the network the sensor monitors.
Nodes count	The total number of nodes detected by this sensor.
Nozomi risk	The Nozomi-calculated risk score for this sensor.
Produces assets	Indicates whether this sensor is configured to generate asset data.
Public IP	The public-facing *IP* address of the sensor.
Risk	The current risk assessment of the sensor. Based on the alerts the sensor has raised, this is the maximum risk value reported in the last period.
Serial number	The unique serial number of the sensor hardware.
Site	The site text reported by the sensor appliance.
Site name	The name of the Vantage site this sensor is assigned to.
Software version	The version of the sensor software currently installed.
Status	The current connection status of the sensor.
Total Mbps	The total network throughput, in megabits per second, currently being monitored by this sensor.
Uptime	The duration the sensor has been continuously running since its last restart.
Variables count	The total number of variables detected by this sensor.

Details page

The details page shows a set of fields which are applicable to the related type of sensor.

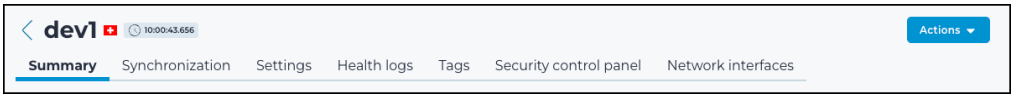


Figure 11. Details page

Actions dropdown

This dropdown gives you access to these actions:

- Delete (on page 59)
- Reset Token (on page 60)
- Renew Licenses (on page 61)
- Migrate Site (on page 62)
- Generate Support Archive (on page 67)

Summary

For more details, see Summary tab (on page 40).

Synchronization

For more details, see Synchronization tab (on page 41).

Settings

For more details, see Settings tab (on page 42).

Health logs

For more details, see Health logs tab (on page 42).

Tags

For more details, see Tags tab (on page 44).

Security control panel

For more details, see Security control panel tab (on page 47).

Network interfaces

For more details, see Network interfaces tab (on page 48).

Support archives

For more details, see Support archives tab (on page 49).

Arc dependencies

For more details, see Arc dependencies tab (on page 51).

Related information

Open the details page (on page 69)

Summary tab

*The **Summary** tab shows an overview of information for the related sensor.*

Figure 12. Summary tab

Sensor information

This section shows the asset information for the related sensor. shows information for:

- Appliance type
- Model
- Serial number
- Software
- Status
- IP
- Public IP
- GeoIP country
- GeoIP latitude
- GeoIP longitude

Throughput

This section shows the traffic throughput for the related sensor.

Summary

This section shows information for:

- Last sync
- Risk
- GeoIP - IP address

Health

This section shows metrics about the sensor. The section shows information for:

- CPU percentage
- Memory free
- Memory used
- Disk usage percentage

Comments

This section lets you write a comment for the sensor. It also shows comments that have been previously written.

Related information

Details page (on page 39)

Synchronization tab

*The **Synchronization** tab shows the settings that the related sensor inherits from its organization.*

Figure 13. Synchronization tab

You can select the **Click the Use organization settings** checkbox to make the settings editable and override the current values.

Changes made on this page affect the related sensor, but not the default settings for the organization it belongs to.

Settings tab

*The **Settings** tab shows sensor-specific settings that can be controlled in Vantage, including content updates, execution policies, and alert deduplication.*

Figure 14. Settings tab

An example of the settings that are shown in this tab are updates for:

- *AI*
- *Threat Intelligence (TI)*

Alerts deduplication

Alerts deduplication: Overrides the organization-level alert deduplication setting for this sensor. When enabled, the system groups repeated alerts of the same type that share identical deduplication key values, rather than creating a separate alert entry each time. You can select one of these options:

- **Enabled**: Alert deduplication is active for this sensor, regardless of the organization setting.
- **Disabled**: Alert deduplication is off for this sensor, regardless of the organization setting.
- **Organization default**: The sensor follows the deduplication setting configured at the organization level.

For more details, see the **Alert deduplication** topic in the Vantage User Guide under **Alerts**.

Health logs tab

*The **Health logs** tab shows the health logs that the related sensor has generated.*

Figure 15. Health logs tab

Delete a health log

The actions menu lets you delete a health log.

Procedure

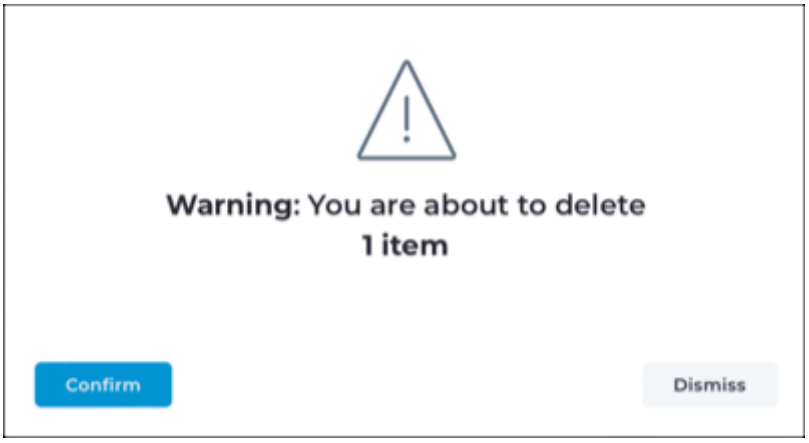
1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select **Health logs**.
4. Choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

5. Select **Delete**.



   Result: A confirmation dialog shows.

6. Select **Confirm**.

Results

The health log(s) has (have) been deleted.

Tags tab

The Tags tab lets you add tags to the related sensor.

Figure 16. Tags tab

The Tags tab shows a table of all the sensors that have had tags added to them.

Add

This button lets you add a new tag (on page 45) to the related sensor.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Related information

Add a tag to a sensor (on page 45)

Delete a tag from a sensor (on page 46)

Add a tag to a sensor

You can add tags to sensors. This lets you refine the permissions that you grant to users.

About this task

You can add one or more tags to the selected sensor.

Procedure

1. Open the details page (on page 69) for the applicable sensor.
2. Select the **Tags** tab.
3. Select **Add new**.

   Result: The **Tag** dropdown shows.
4. Open the dropdown and select the correct tag.

   Note:
   Only the tags that have been assigned for your organization show.
5. Select **Create**.

   Result: The tag has been added to the related sensor.

Related information

Tags tab (on page 44)

Delete a tag from a sensor (on page 46)

Delete a tag from a sensor

If a tag has been added to a sensor, you can delete it.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select **Tags**.
4. Double-click the applicable tag.

   Result: The summary drawer shows.

5. Select **Details**.

   Result: The details page for the related tag shows.

6. Select **Actions > Delete**.

Results

The tag has been deleted.

Related information

Tags tab (on page 44)

Add a tag to a sensor (on page 45)

Security control panel tab

*The **Security control panel** tab lets you add tags to the related sensor.*

Figure 17. Security control panel tab

The Security control panel tab lets you control which alerts are created on sensors. The dropdown lets you select from these options:

- Low
- Medium
- High
- Paranoid
- Organization default

Network interfaces tab

*The **Network interfaces** tab shows the network ports available on a Guardian sensor. Use this tab in Vantage to review interface details and filtering settings. Configuration changes can only be made on the Guardian sensor itself.*

Figure 18. Network interfaces tab

Support archives tab

*The **Support archives** tab shows the support archives that have been generated for the related sensor, and lets you download them.*

Figure 19. Support archives tab

The **Support archives** tab is only shown for Arc sensors. The table only shows support archives that have finished generating, with these columns:

- Name
- Sensor host
- Created at
- Site name

To generate a new support archive, see Generate a support archive (on page 67).

Related information

Generate a support archive (on page 67)

Download a support archive (on page 50)

Download a support archive

You can download a support archive that's been generated for an Arc sensor.

Procedure

1. Open the details page (on page 69) for the applicable sensor.
2. Select the **Support archives** tab.
3. Double-click the applicable support archive.

   Result: The summary drawer shows.

4. Select **Details**.

   Result: The details page for the related support archive shows, with a **Download** button.

5. Select **Download**.

Results

The support archive file starts to download in your browser.

Related information

Support archives tab (on page 49)

Generate a support archive (on page 67)

Arc dependencies tab

*The **Arc dependencies** tab shows the dependencies required by the related sensor, and lets you install, uninstall, update, enable, and disable them.*

Figure 20. Arc dependencies tab

The **Arc dependencies** tab is only shown for Arc sensors running Arc v2.8.0 or later that are connected directly to Vantage, or connected through a Guardian running *N2OS* v26.5 or later.

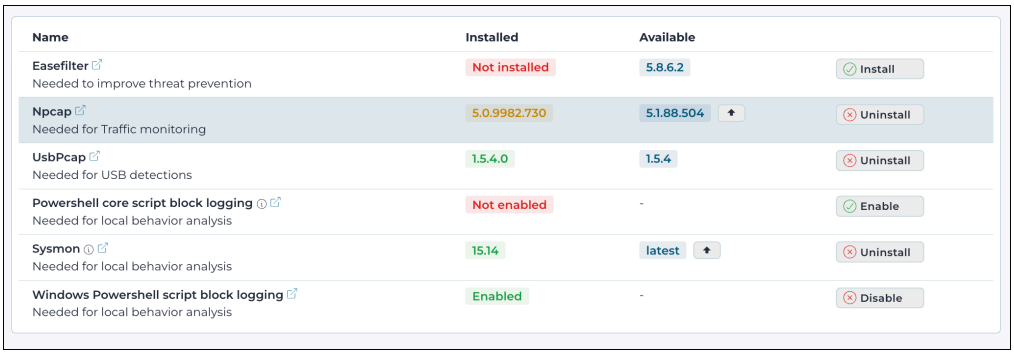


Figure 21. Arc dependencies list

The tab shows a table of the dependencies that are available for the sensor, with these columns:

- **Name**: The dependency's name, with a short description of why it's needed underneath. Some dependencies also show an information icon with more details, an external link to more information, or both
- **Installed** and **Available**: Each dependency is one of these types:
  - **Software** dependencies show the installed version (or **Not installed**) in the **Installed** column, and the available version in the **Available** column.
  - **Setting** dependencies show **Enabled** or **Not enabled** in the **Installed** column. The **Available** column doesn't apply.

Note:

If a dependency shows a **Reboot required** tag, its actions aren't available until the sensor is rebooted.

Note:
For sensors running Windows 7 or Windows Server 2008 R2, install the **Sysmon Legacy** dependency instead of **Sysmon**. Its bundle must first be uploaded from the organization's **Arc dependencies** page, using version **13.34** and a *ZIP* archive containing `Sysmon.exe` and `Sysmon64.exe`.

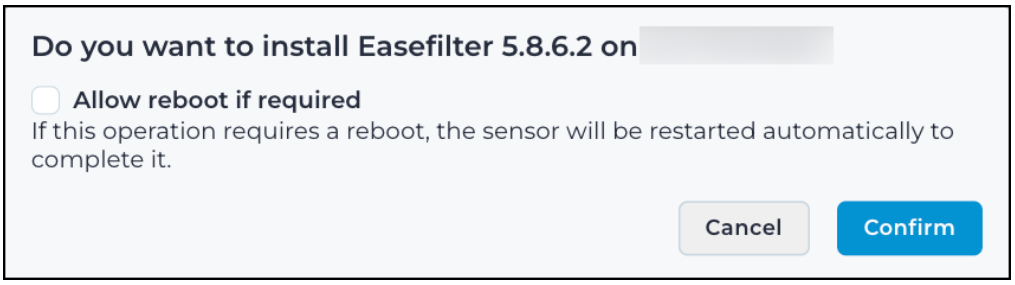


Figure 22. Confirmation dialog

Related information

Install an Arc dependency (on page 53)
Uninstall an Arc dependency (on page 54)
Update an Arc dependency (on page 55)
Enable an Arc dependency (on page 56)
Disable an Arc dependency (on page 57)

Install an Arc dependency

You can install a software dependency that isn't yet installed on an Arc sensor.

Before you begin

The sensor must be running Arc 2.9.0 or later.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select the **Arc dependencies** tab.
4. For the applicable dependency, select **Install**.

   Result: A confirmation dialog shows.

5. **Optional:** Select the **Allow reboot if required** checkbox.

   > **Note:**
   > If this operation requires a reboot, the sensor is restarted automatically to complete it.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The dependency is installed on the sensor.

Related information

Arc dependencies tab (on page 51)

Uninstall an Arc dependency (on page 54)

Update an Arc dependency (on page 55)

Uninstall an Arc dependency

You can uninstall a software dependency that's installed on an Arc sensor.

Before you begin

The sensor must be running Arc 2.9.0 or later.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select the **Arc dependencies** tab.
4. For the applicable dependency, select **Uninstall**.

   Result: A confirmation dialog shows.

5. **Optional:** Select the **Allow reboot if required** checkbox.

   > **Note:**
   > If this operation requires a reboot, the sensor is restarted automatically to complete it.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The dependency is uninstalled from the sensor.

Related information

Arc dependencies tab (on page 51)

Install an Arc dependency (on page 53)

Update an Arc dependency

If a newer version is available for an installed software dependency, you can update it.

Before you begin

The sensor must be running Arc 2.9.0 or later.

About this task

The **Update** action is only available for a dependency that's already installed and for which a newer version is available.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select the **Arc dependencies** tab.
4. For the applicable dependency, in the **Available** column, select the up-arrow icon.

   Result: A confirmation dialog shows.

5. **Optional:** Select the **Allow reboot if required** checkbox.

   > **Note:**
   > If this operation requires a reboot, the sensor is restarted automatically to complete it.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The dependency is updated to the available version on the sensor.

Related information

Arc dependencies tab (on page 51)

Install an Arc dependency (on page 53)

Enable an Arc dependency

You can enable a setting dependency that isn't yet enabled on an Arc sensor.

Before you begin

The sensor must be running Arc 2.9.0 or later.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select the **Arc dependencies** tab.
4. For the applicable dependency, select **Enable**.

   Result: A confirmation dialog shows.

5. **Optional:** Select the **Allow reboot if required** checkbox.

   > **Note:**
   > If this operation requires a reboot, the sensor is restarted automatically to complete it.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The dependency is enabled on the sensor.

Related information

Arc dependencies tab (on page 51)

Disable an Arc dependency (on page 57)

Disable an Arc dependency

You can disable a setting dependency that's enabled on an Arc sensor.

Before you begin

The sensor must be running Arc 2.9.0 or later.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69) for the applicable sensor.
3. Select the **Arc dependencies** tab.
4. For the applicable dependency, select **Disable**.

   Result: A confirmation dialog shows.

5. **Optional:** Select the **Allow reboot if required** checkbox.

   > **Note:**
   > If this operation requires a reboot, the sensor is restarted automatically to complete it.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The dependency is disabled on the sensor.

Related information

Arc dependencies tab (on page 51)

Enable an Arc dependency (on page 56)

Summary drawer

When you double-click a sensor in the table, the summary drawer shows. This lets you post a comment, or open the related details page.

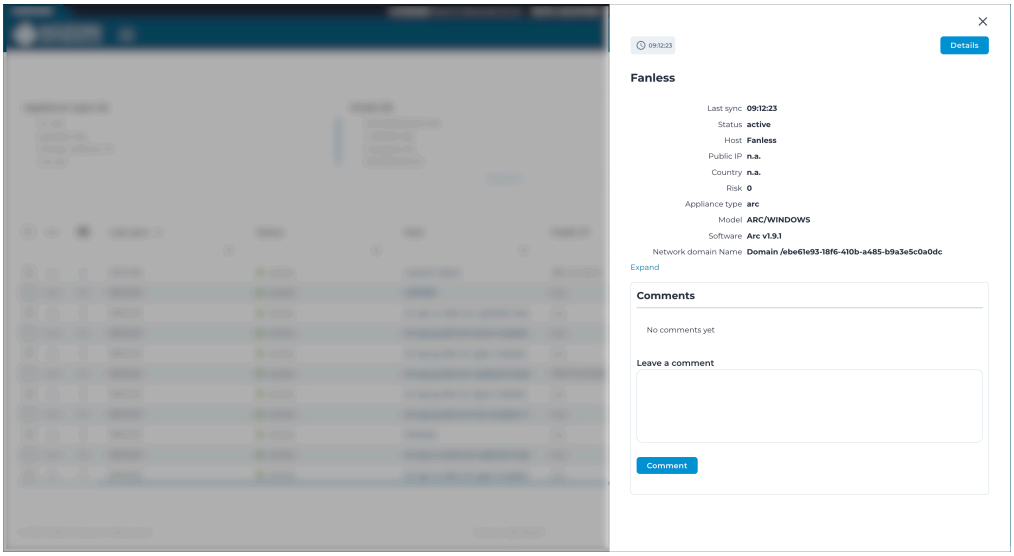


Figure 23. Summary drawer

Details button

You can select the **Details** button to open the details page for the related item.

Summary

The summary section shows a summary of applicable information for the related item.

Comments

This section lets you leave a comment, or read a comment that has been written, for the related item.

Table interactions

Actions menu

Delete a sensor

You can use the actions menu to delete a sensor.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Choose a method to open the actions menu.

   Choose from:

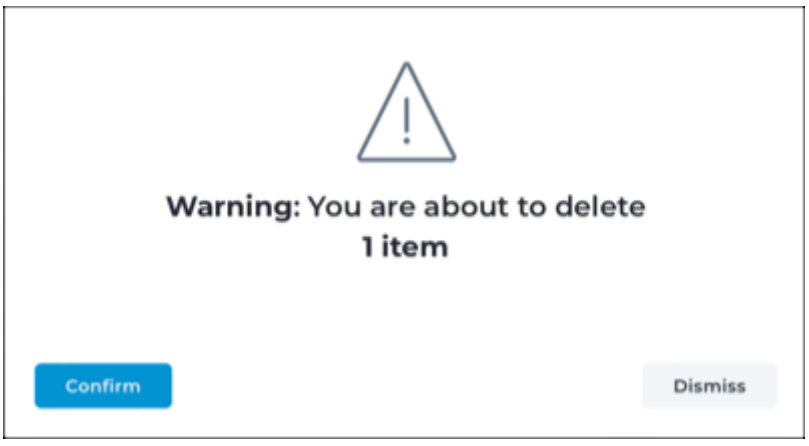
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Delete**.



   Result: A confirmation dialog shows.

Results

The sensor(s) has (have) been deleted.

Reset a sensor token

The Actions menu lets you reset a sensor token.

Procedure

1. In the table, select the applicable sensor.
2. Select **Actions > Reset Token**.

   Result: The message `When you confirm to Reset Token, you need to update the settings on your sensors or you will lose connectivity` shows.
3. Select **Confirm Reset Token**.

   Result: Vantage resets the token and displays its new value. Use this value to configure the connection (on page 76) again.

> **Note:**
> If Vantage loses contact with a sensor, resetting its token and reconnecting the sensor can sometimes restore communication.

> **Note:**
> If a sensor is correctly communicating with Vantage, resetting the token severs the connection. To reconnect the sensor, generate a new token and configure the sensor the sensor (on page 76) again.

Renew a sensor license

You can use the actions menu to renew the license for one or more sensors.

Procedure

1. In the top navigation bar, select **Sensors**.

   Note:
   If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

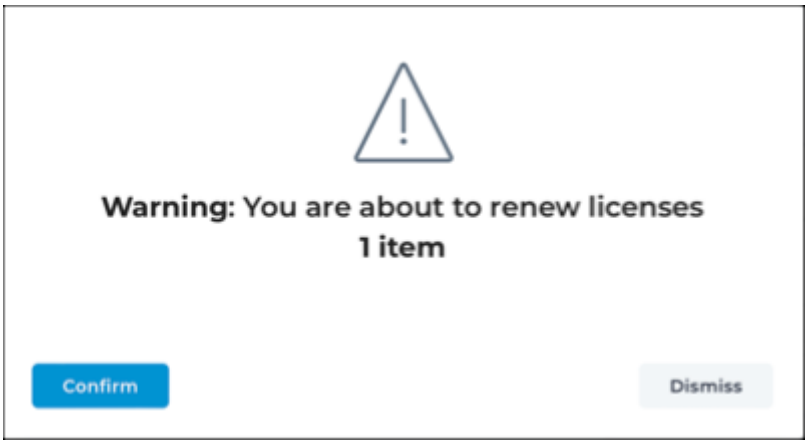
2. Choose a method to open the actions menu.

   Choose from:
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Renew Licenses**.



   Result: A confirmation dialog shows.

5. Select **Confirm**.

Results

The license(s) has (have) been renewed.

Migrate a sensor to a different site

It is possible to migrate a sensor from one site to a different, or new, site.

Procedure

1. In the top navigation bar, select **Sensors**.

   Note:
   If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Choose a method to open the actions menu.

   Choose from:
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

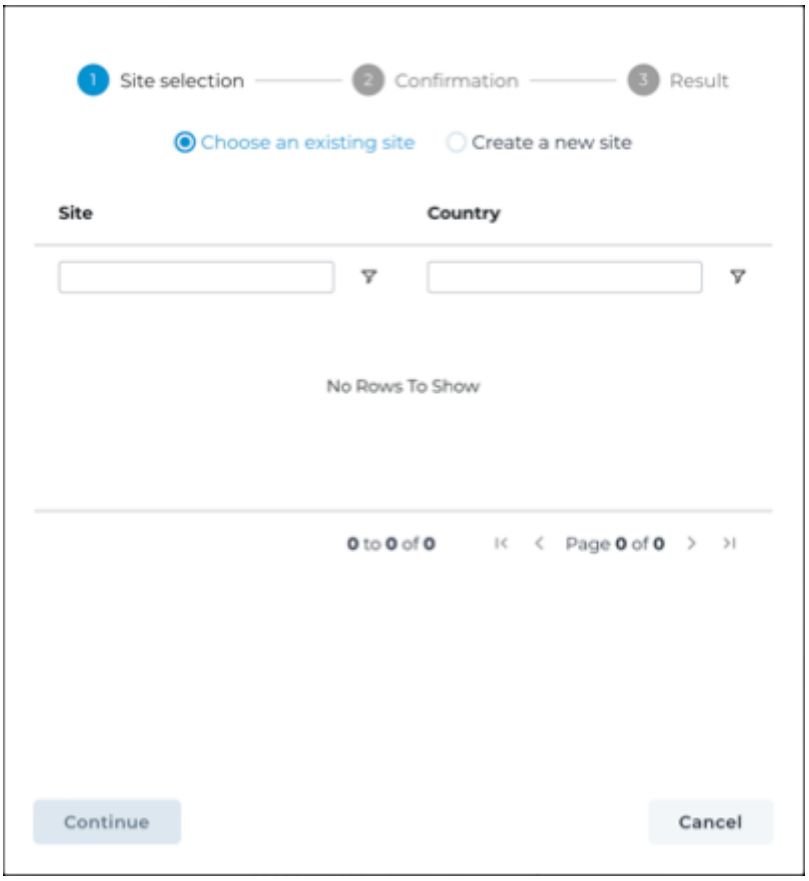
3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Migrate Site.**

   Result: A dialog shows.

5. Choose an option:

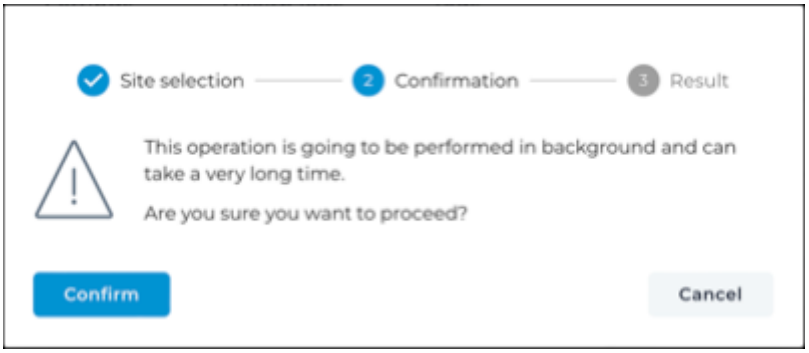


Choose from:

- **Choose an existing site**
- **Create a new site**

6. If you chose **Choose an existing site**, do the steps below:
   a. In the **Site** field, use the filter to select the site.
   b. In the **Country** field, use the filter to select the country.
   c. Select **Continue**.
   Result: A dialog shows.
   d. Go to step 8 (on page 64).

7. If you chose **Create a new site**, do the steps below:
   a. In the **City** field, enter the name of the city.
   b. In the **Country** dropdown, select a country.
   c. Select **Create and select new Site**.
   Result: A dialog shows.
8. Select **Confirm**.



Results

The site migration starts.

Change the context of a CMC

Change the context of a Central Management Console (CMC) from Multicontext to All-In-One or from All-In-One to Multicontext. This change affects how the CMC and its connected sensors operate within your network. Use the actions menu to initiate the change.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Choose a method to open the actions menu.

   Choose from:

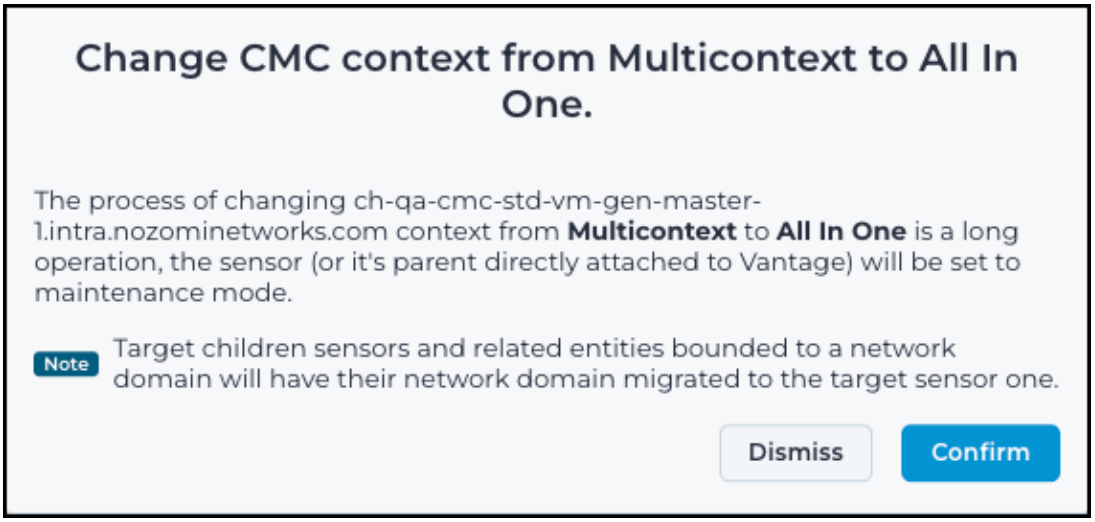
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Change CMC Context**.



Result: A confirmation dialog shows. (Multicontext to All-In-One version shown.)

Results

The context of the *CMC* has been changed.

Generate a support archive

You can use the actions menu to generate a support archive for an Arc sensor.

Procedure

1. In the top navigation bar, select **Sensors**.

   Note:
   If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Choose a method to open the actions menu.

   Choose from:
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Generate Support Archive**.

Result: A confirmation dialog shows.

5. **Optional:** Select the **Anonymize support archive** checkbox.

   Note:
   This option works only if the sensor is running Arc 2.5.0 or later.

6. Select **Confirm**.

   Result: The operation starts. You can monitor its progress on the Async operations (on page 365) page.

Results

The support archive is generated and shows in the Support archives tab (on page 49) of the sensor's details page.

Related information

Support archives tab (on page 49)

Open the details page

You can open a details page for individual sensors that are shown in the sensor page table. You can open the details page with two different methods.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Choose a method with which to open the details page. In the row for the applicable sensor:

   Choose from:

   - In the **Host** column of the table, select the hyperlink.
   - Double-click the row to open the summary drawer. In the top right section, select **Details**.

   Result: The details page (on page 39) opens.

Related information
Details page (on page 39)

Open the summary drawer

You can open a summary drawer for individual items that are shown in the related table.

Procedure

In the table, double-click the row for the applicable item.

Result: The summary drawer (on page 58) opens.

Related information
Summary drawer (on page 58)

Connect a sensor

Identify and copy the sensor ID

Before you can add a sensor to Vantage, you must first identify the sensor, and copy the ID for use in other the procedures that follow.

About this task

Note:
The *identifier (ID)* of a sensor is different from the machine *universally unique identifier (UUID)*. The machine *UUID* applies to the physical, or virtual, hardware running the system. The sensor *ID* applies to the sensor's software.

Note:
In N2OS versions before 23.x, the sensor *ID* was called Appliance *ID*.

Note:
If your N2OS version is earlier than 21.0.0, please update your N2OS installation. For more information, see the N2OS Release notes.

The sensor type and version will affect the steps that you need to do below.

Procedure

1. Determine the type of sensor that you want to connect:

   Choose from:

   - If your sensor uses N2OS, open the web UI and navigate to **Administration > Synchronization settings**.
   - If your sensor is Nozomi Arc, open the local configuration UI and go to the **Status** page.

2. Copy the applicable *ID*:

   Choose from:

   - If your sensor uses N2OS version 23.x, select Copy next to the **Sensor ID** field. Save the information to use in later steps.
   - If your sensor uses N2OS version 22.x, select Copy next to the **Appliance ID** field. Save the information to use in later steps.
   - If your sensor is Nozomi Arc, copy the value in the **Sensor ID** field. Save the information to use in later steps.

3. Add the sensor in Vantage. (on page 71)

Add a sensor

Before you can use a sensor in Vantage, you must add it.

Before you begin

Before you can add a sensor, you must first Identify and copy the sensor ID (on page 70).

About this task

Note:

You can only connect a sensor to one:

- Organization
- Site
- Network domain

Procedure

1. Log in to Vantage.
2. In the top navigation bar, select **Sensors**.

   Note:

   If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

3. Select the **Add new** button.

   Result: The **Make connections** page opens.

4. Select the product, and version, of the sensor that you want to connect to.

5. The options that show will depend on the sensor that you chose in the previous step.
6. Select an option:

   Choose from:

   - Select **N2OS** and do the Add an N2OS sensor (on page 72) procedure
   - Select **Arc** and do the Add an Arc sensor (on page 73) procedure
   - Select **Guardian Air** and do the Add a Guardian Air sensor (on page 75) procedure

Add an N2OS sensor

Before you can use an N2OS sensor in Vantage, you must add it.

Before you begin

Do the Add a sensor (on page 71) procedure and choose the **N2OS** option.

Procedure

1. Paste the *ID* that you previously retrieved into the **Sensor ID** field.

   > **Note:**
   > Vantage does not support N2OS versions before 23.0.0.

2. Select **Next**.

   > **Note:**
   > The sensor *ID* must be valid, and not be the same as one that was previously added in this Vantage console.

   Result: Vantage validates the *ID*.

3. Select the correct site:

   Choose from:

   - Select the correct site and network domain from the list.
   - To create a new site, enter the correct city and country for the sensor. Select **Continue**.

   Result: The host *ID* and sync token that Vantage will use to synchronize with the sensor show.

4. > **Important:**
   > Do not lose the *URL* or sync token. If you do, you will need to reset the token (on page 88).

   Copy the connection host *URL* and sync token, and paste them in a safe location.

5. Before you continue, you must configure the sensor (on page 76).

Add an Arc sensor

Before you can use an Arc sensor in Vantage, you must add it.

Before you begin

Do the Add a sensor (on page 71) procedure and choose the **Arc** option.

Procedure

1. Select **Configure Arc bundle**.

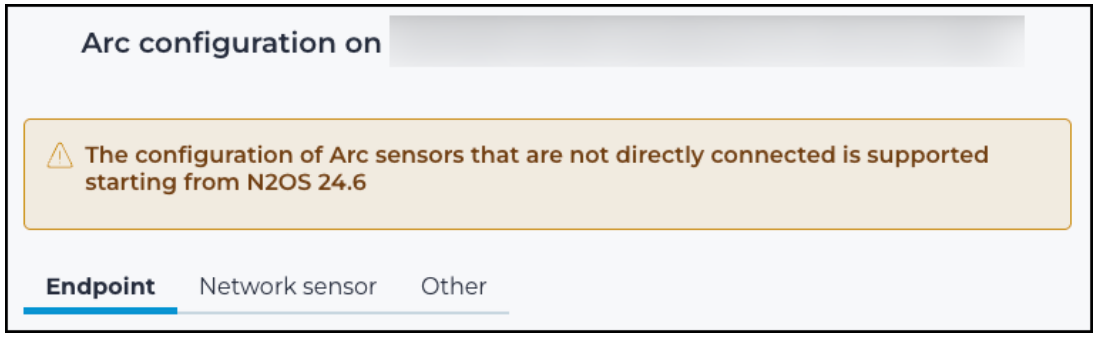
   Result: A dialog shows.

2. Do a check of the defaults settings.
3. Select an option:

   Choose from:

   - To accept the default settings, close the dialog and go to step 10 (on page 74)
   - Alternatively, to modify the settings, go to step 4 (on page 73)

4. In the **Execution time** section, enter a value in seconds.

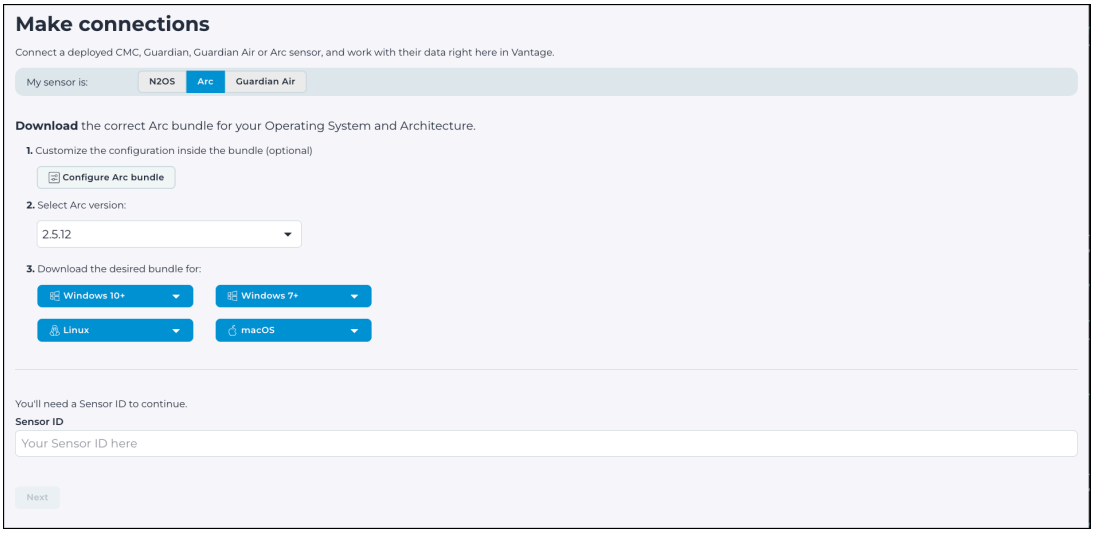


> **Note:**
> When this is set to 0, the execution time is interpreted as infinite.

5. Enable/disable from these options:
   - **Sigma rules** (Windows only)
   - **YARA rules** (Windows only)
   - **USB detections** (Windows only)
   - **Node points**
   - **Discovery**
   - **Smart Polling**
   - **Local ARP table**

6. From the **Log level** dropdown, select the verbosity level for the log files. Select from:
    - Debug
    - Info
    - Warning
    - Error
7. If necessary, in the **Traffic monitoring** section, select from:
    - **Enable**
    - **Enable continuous mode**

    a. In the **Monitoring time [s] per notification** field, enter a value in seconds.
    b. In the **Max packets per notification** field, enter a value.
    c. In the **Max used Memory [MB]** field, enter a value.
8. Select **Save**.
9. From the dropdown, select the correct Arc version.
10. Download the applicable bundle.



11. Before you continue, you must configure the sensor (on page 76).

Add a Guardian Air sensor

Before you can use a Guardian Air sensor in Vantage, you must add it.

Before you begin

Make sure that:

- The LED status indicator on the Guardian Air sensor is flashing green
- You have completed the Add a sensor (on page 71) procedure and you chose the **Guardian Air** option

Procedure

1. After you select **Guardian Air**, a **Use camera?** dialog shows.
2. Choose a method to connect the Guardian Air sensor (sensor).

   Choose from:

   - To scan the QR code, select **Allow** and go to step 3 (on page 75)
   - To enter the code manually, Select **Deny**, and go to step 4 (on page 75)

   > **Note:**
   > The exact labels can change depending on which browser you use.

3. Scan the QR code of the sensor.
4. In the **Serial Number** field, enter the serial number of the sensor.
   You will find the serial number in the Quick Start Guide, and on the bottom of the sensor.
5. Select **Next**.
6. Select **Site**.
7. Select **Next**.
8. Select **Network Domain**.
9. Select **Next**.
10. Wait for the sensor to be added.
    Once the sensor has been added, it will show on the **Sensors** page.
11. Before you continue, you must configure the sensor (on page 76).

Configure a sensor

After you have added a sensor, you must configure it before you can complete the connection of the sensor.

Before you begin

Before you configure the sensor, add the sensor in Vantage (on page 71).

About this task

Once you have added the sensor in Vantage (on page 71), you must configure it.

Procedure

1. Log in to the sensor that you want to connect to Vantage.
2. In the *user interface (UI)* of the sensor, go to the configuration page. If you want to connect a *CMC*, or Guardian, go to > **Synchronization settings**.
3. In **Upstream Connection**, select **On** to activate the connection.
4. In the **Host** field, paste the URL that you copied in Vantage.
5. In the **Sync token** field, paste the sync token that you copied in Vantage.
6. Optionally, enter a description of the Vantage connection and site.
7. If the sensor, is already connected in another system, replace the **Host** and **Sync token** values with those you copied from Vantage.
8. Select **Check connection**.
9. When a successful connection is confirmed, select **Save** in the top right corner of the page.

> **Note:**
> Consider the flow of data when you connect a *CMC* to Vantage. Depending on your implementation, there might be no advantage in doing this. It might be preferable to connect your Guardians directly to Vantage.

10. Complete the connection of the sensor (on page 86).

Arc sensor configuration

A description of the configuration settings for an Arc sensor.

Figure 24. Configuration settings

The Configuration page has these tabs:

- Endpoint (on page 78)
- Network sensor (on page 80)
- Other (on page 83)

Endpoint

Configure detection options for endpoint monitoring in Arc. Features include node point extraction, asset validation using ARP, and malware detection with customizable actions.

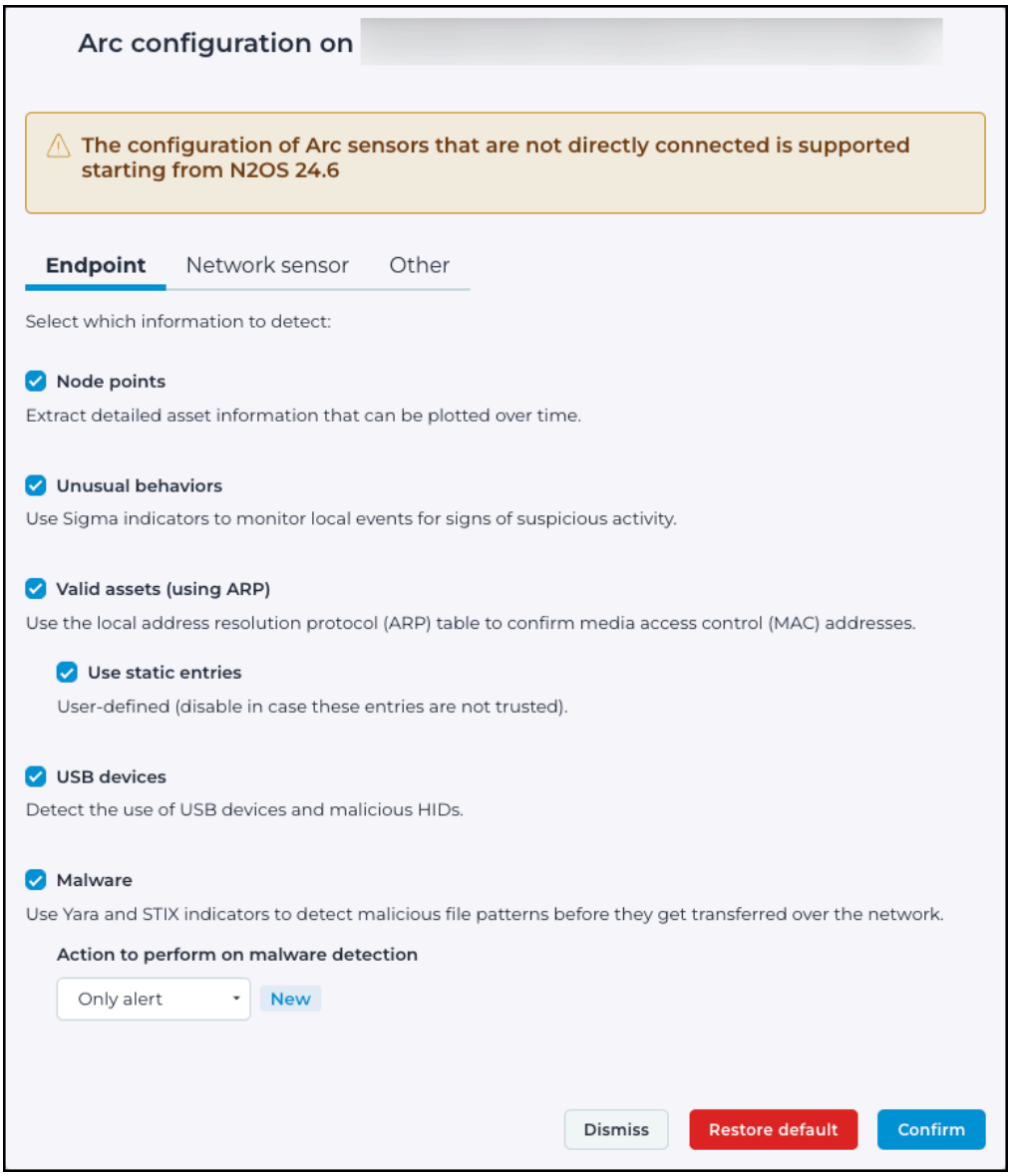


Figure 25. Configuration settings

Asset information

Enable **Asset information** to collect detailed information about the endpoint. Arc collects the following data:

- **CPU usage**: The current processor load of the endpoint.
- **RAM usage**: The amount of memory currently in use on the endpoint.
- **Disk usage**: The current disk space usage on the endpoint.
- **Logged-in users**: The users currently logged in to the endpoint.

- **Processes with network activity**: The running processes that have active network connections, including the local and remote addresses and ports.
- **Hotfixes**: The security patches and updates installed on the endpoint (Windows only).
- **User accounts**: The local user accounts configured on the endpoint.
- **DNS**: The *domain name server (DNS)* servers and configuration of the endpoint.
- **Installed software**: The software packages installed on the endpoint.

Unusual behaviors (Windows only)

This lets you enable/disable Sigma rules for local behavior analysis.

Valid assets (using ARP)

Enable this option to use the local *address resolution protocol (ARP)* table to confirm *media access control (MAC)* addresses for connected assets.

Enable **Use static entries** to include user-defined static *ARP* table entries in the validation. Only enable this if the static entries are trusted.

USB devices (Windows only)

This lets you enable/disable *universal serial bus (USB)* detections.

Malware (Windows only)

The **Malware** checkbox lets you enable protection mode and select from the **Action to perform on malware detection** dropdown. This lets you set the action that Arc will take when it finds a malicious file.

You can choose from these options:

- **Only alert**: Receive an alert with no further action
- **Quarantine**: Move the malicious file to the `quarantine` folder, which is located in the Arc installation folder
- **Delete**: Immediately delete the malicious file. Once deleted, the files cannot be recovered

You can also use the **Directory exclusions** feature to exclude specific directories from malware scanning. Select + to open a file browser and select a directory. You can add as many directories as needed. Arc skips the selected directories when scanning for malware.

Network sensor

Configure Arc network sensor features such as Discovery, Smart Polling, and traffic monitoring. These options help identify neighboring devices, enrich asset data, and analyze network traffic patterns.

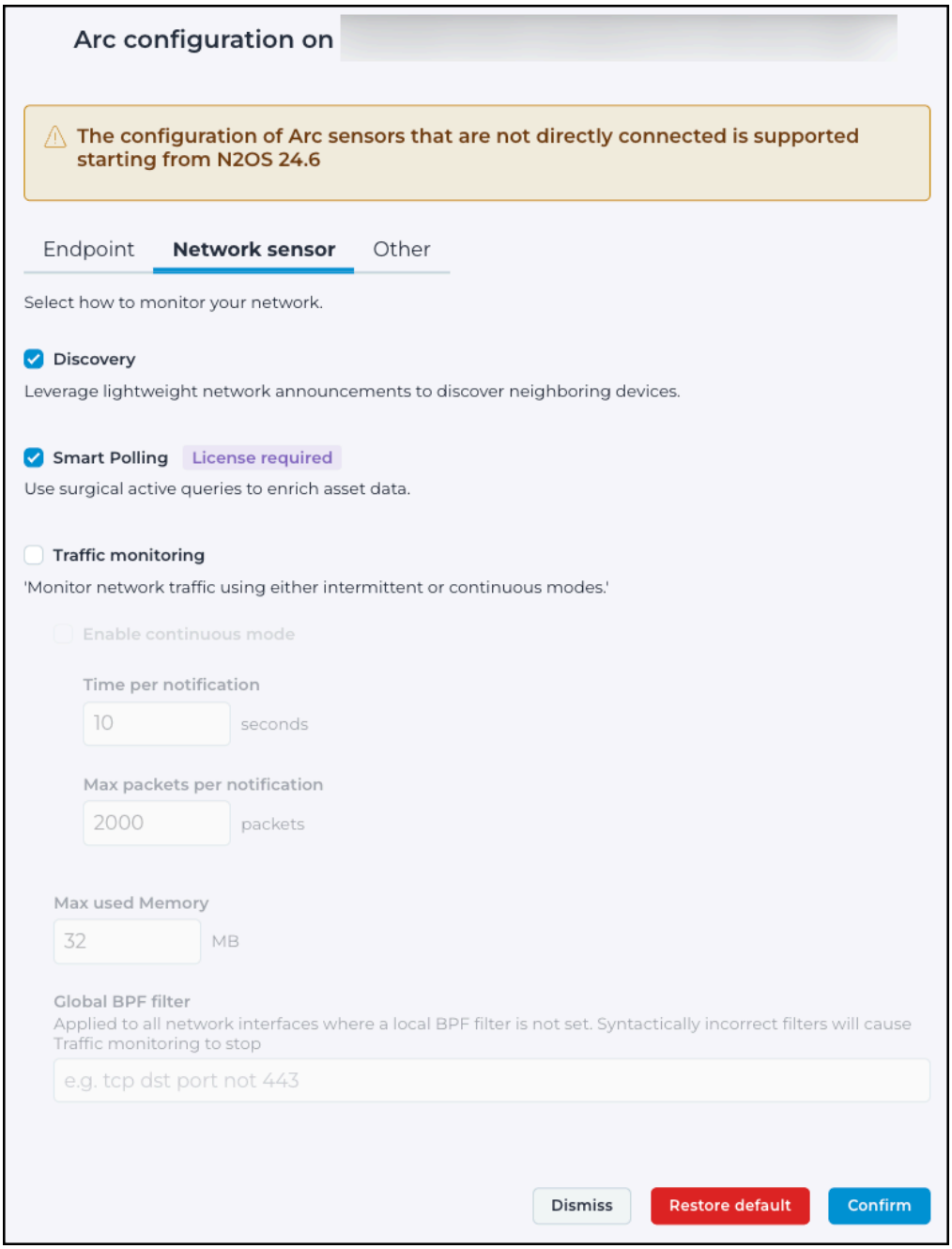


Figure 26. Configuration settings

Discovery

When enabled, this sends out unsolicited lightweight network announcements to discover neighboring nodes.

Discovery uses lightweight protocol-specific broadcast messages to identify network devices. These messages trigger a response from the devices, which includes identity information. The process is repeated at predefined intervals. At each interval, the sensor will identify the suitable network interfaces and send broadcast messages through them to discover devices on each subnetwork connected to the sensor.

Smart Polling

This lets you enable/disable the execution of Smart Polling strategies from Arc. When enabled, this sends out Smart Polling queries following remote requests coming from Guardian to poll assets that Arc can reach, or assets that have been identified with Discovery.

> **Note:**
> **Smart Polling** requires that a Smart Polling license is enabled upstream.

To force Smart Polling from a specific Arc sensor, even when Guardian was the first to monitor a node, you can use a *command-line interface (CLI)* command such as: `vi node 192.168.1.1 capture_device arc[1e6a174c]` In this example, `192.168.1.1` is an *IP* address of a node you want to poll from a specific Arc sensor. `1e6a174c` are the first eight characters of the Arc sensor *ID* that you want to poll the node with. To find that sensor *ID*, you can select the Arc sensor from the **Sensors** page of your Guardian and read the **ID** field in the right pane. To reset the behavior, you can set the `capture_device` back to the value of the Guardian interface.

Traffic monitoring

When enabled, this checkbox lets you enable/disable traffic monitoring.

Enable continuous mode

This checkbox lets you enable/disable continuous mode. For more details, see **Continuous mode**.

Arc uses two different methods for traffic monitoring:

- Intermittent mode
- Continuous mode

Intermittent mode: This is the default mode, the traffic is monitored, or sniffed, for a duration of 10 seconds at each notify. The purpose of this limitation is to preserve the resources of the host machine, which prevents excessive memory, or *CPU*, spikes. You can configure these options:

Continuous mode: This mode sniffs traffic continuously from the host's network interface controllers. Depending on the amount of sniffed traffic, continuous mode might utilize more *CPU* and memory on the host. As the traffic is processed upstream, the performance of the remote endpoint is also affected. You can configure:

- **Time [s] per notification**
- **Max packets per notification**
- **Max used Memory (MB)**: this value can be tuned to allow more or less traffic buffering in case the traffic to process exceeds the Arc and network capacity to send it out

Global BPF filter

This field lets you set a Global BPF filter to apply to all the network interfaces. Filters that are applied to single interfaces will take precedence over the global one.

Network interface

This dropdown lets you select a network interface to configure. Each network interface can then be enabled, and be tuned with a monitoring filter.

If you add, remove, or edit the network interfaces on the host, Arc does not automatically add it to the list of sniffing interfaces. For example, if you add a new network card, to enable Arc to use it, you should stop Arc, and then start it again.

Other

Set Arc log verbosity, data collection duration, and disk space usage limits for One-shot and Offline modes. These options help manage local resource usage and troubleshoot performance.

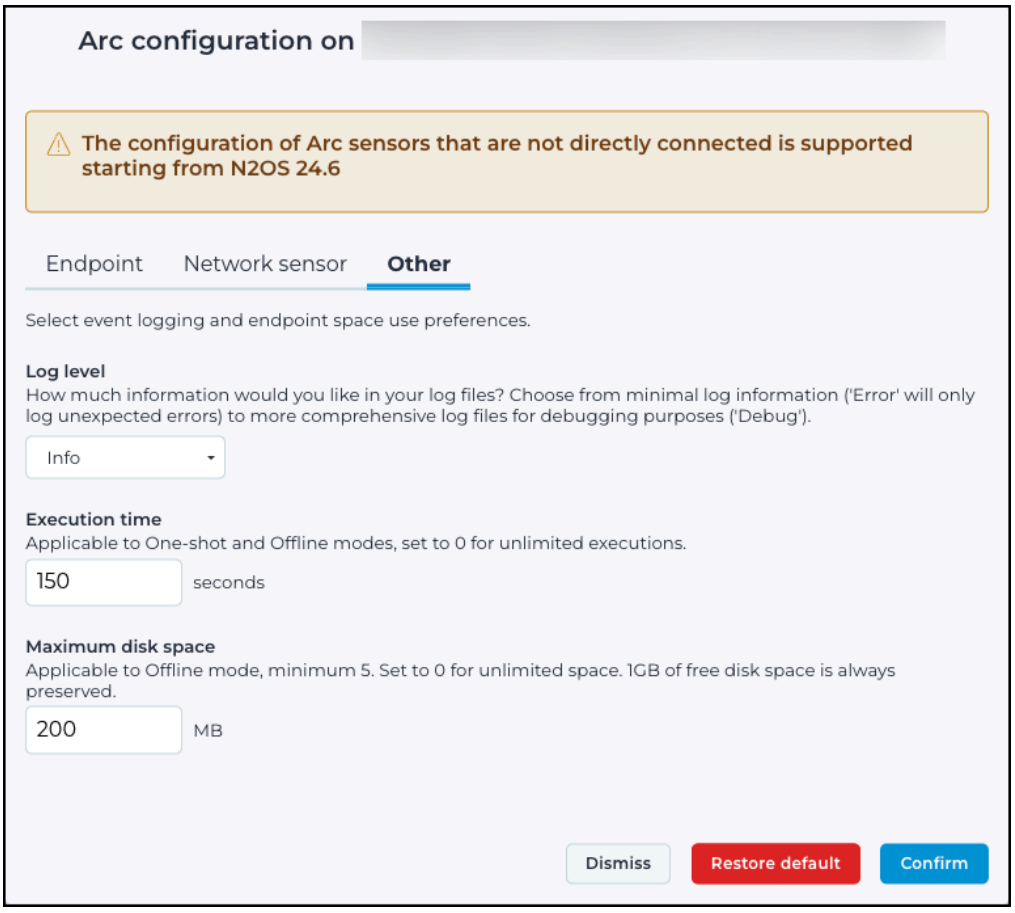


Figure 27. Configuration settings

Log level

This dropdown lets you select the verbosity level for the log files. The options are:

- Debug
- Info
- Warning
- Error

The logging system options have an increasing level of verbosity, from the least verbose to the most verbose. Error < Warning < Info < Debug.

- Error: Creates a minimalistic log, only unexpected errors are logged
- Warning: Creates extra errors that might show on some *operating system (OS)*s, but that are generally considered as acceptable
- Info: Logs relevant successful events, it shows the program's progress (recommended)
- Debug: Logs extra events that are normally useful for debugging purposes. Given its verbosity it is best to activate it only when debugging activities are involved

Note:
This setting applies to:

- `arc.log.txt`
- `arc_service.log.txt`
- `sp.log.txt`

It doesn't apply to `setup.log`, which covers Arc's initialization process, before the configuration has been loaded and applied.

For more details, see Log files (on page).

Execution time

This field lets you set the time that Arc will run to collect data. This is applicable for One-shot and Offline modes.

Note:
When this is set to 0, the execution time is interpreted as infinite.

Maximum disk space

This field lets you control the maximum amount of disk space in *megabyte (MB)* that will be used for Offline mode.

Configure an Arc sensor

*It is possible to configure an individual Arc sensor directly from the **Sensors** details page for the related sensor. Arc sensors in Service mode use these settings.*

Before you begin

Do the Add a sensor (on page 71) procedure and choose the **Arc** option.

About this task

This procedure shows you how to configure an individual Arc sensor. If you want to configure multiple Arc sensors at the same time, you can select multiple sensors in the table, and select the actions menu and **Configure Arc Sensor**.

Procedure

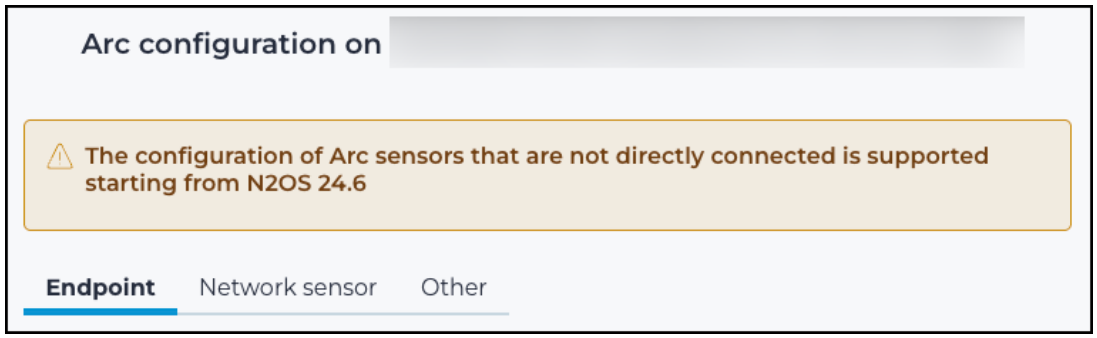
1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. Open the details page (on page 69).
3. In the top right section, select **Actions > Configure Arc Sensor**.

   Result: A dialog shows.

4. Choose the applicable options.



5. Select **Save**.

Results

The Arc sensor has been configured.

Complete the connection of a sensor

After you have configured a sensor, you must complete the connection of the sensor.

Before you begin

Before you complete the connection procedure to add a sensor (on page 71), make sure that you have configured the sensor (on page 76).

Procedure

1. In Vantage, go back to the **Make connections** page.
2. Select **Continue**.

   Result: Vantage shows a message with the *ID* of the sensor that you are connecting, and a timer shows as Vantage waits for traffic from the sensor.

   > **Note:**
   > When the message `Sensor attached successfully` shows, communication between the sensor and Vantage has been established.

3. If the **Continue** button does not show, the sensor might not be sending traffic. Reboot the sensor. If the **Continue** button still does not show, go to Sensor will not connect (on page 89).
4. Verify the connection of a sensor (on page 87).

Verify the connection of a sensor

After you have completed the connection of a sensor, you must verify the connection of the sensor.

Procedure

1. In the top navigation bar, select **Sensors**.

   Note:
   If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. In the table, find and select the applicable sensor.
3. Double-click the sensor to view its details.

   Note:
   Details such as the current risk score and the time of the last sync with Vantage will show. You can also leave a comment for other users.

   Note:
   If the applicable sensor does not show in the table, it might not have been successfully added. You can try to connect the sensor again. If Vantage shows an error message, it might be a display problem. Refreshing the browser might solve the problem.

   Note:
   When the connection to a sensor is incomplete, Vantage will show `n.a.` instead of the correct values.

4. If you continue to have problems, go to Sensor will not connect (on page 89).

Reset a sensor token

If you lose a sensor's token, it is possible to reset it.

About this task

Resetting a sensor's token lets you create a new token in cases where the sensor isn't sending traffic to Vantage. For example, if you are trying to complete a connection to a new sensor, and misplaced its token, you can reset the token and use the new value.

Procedure

1. In the top navigation bar, select **Sensors**.

   > **Note:**
   > If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. In the table, find the applicable sensor.
3. Select the sensor to view its details.
4. Select **Actions > Reset Token**.

   Result: The message `When you confirm to Reset Token, you need to update the settings on your sensors or you will lose connectivity` shows.

5. Select **Confirm Reset Token**.

   Result: Vantage resets the token and displays its new value. Use this value to configure the connection (on page 76) again.

   > **Note:**
   > If Vantage loses contact with a sensor, resetting its token and reconnecting the sensor can sometimes restore communication.

   > **Note:**
   > If a sensor is correctly communicating with Vantage, resetting the token severs the connection. To reconnect the sensor, generate a new token and configure the sensor the sensor (on page 76) again.

Troubleshooting

Sensor will not connect

Condition

Vantage does not receive traffic from a sensor.

Procedure

1. Log in to the sensor.
2. Reboot the sensor.

Procedure

1. Reset the token (on page 88).
2. Connect the sensor to Vantage.

> **Note:**
> When you reset the token, the connection between Vantage and the sensor is broken. You will need to connect the sensor again before it can send traffic to Vantage.

Procedure

1. Delete the sensor from Vantage (on page 59).
2. Add the sensor to Vantage again. (on page 71)

Chapter 3. Alerts

*The **Alerts** page shows all the alerts notifications that your sensors pass to Vantage related to security incidents in your network. This page lets you learn about the alerts, edit their values and post comments.*

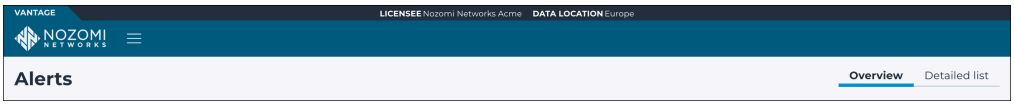


Figure 28. Alerts page

The Alerts page has these tabs:

- Overview (on page 94)
- Detailed list (on page 96)

Related information

Acknowledge an alert (on page 101)

Close an alert (on page 105)

Create an alert rule (on page 108)

Trace an alert (on page 110)

Overview

*The **Overview** page provides insights into security alerts, risk levels, and alert trends.*

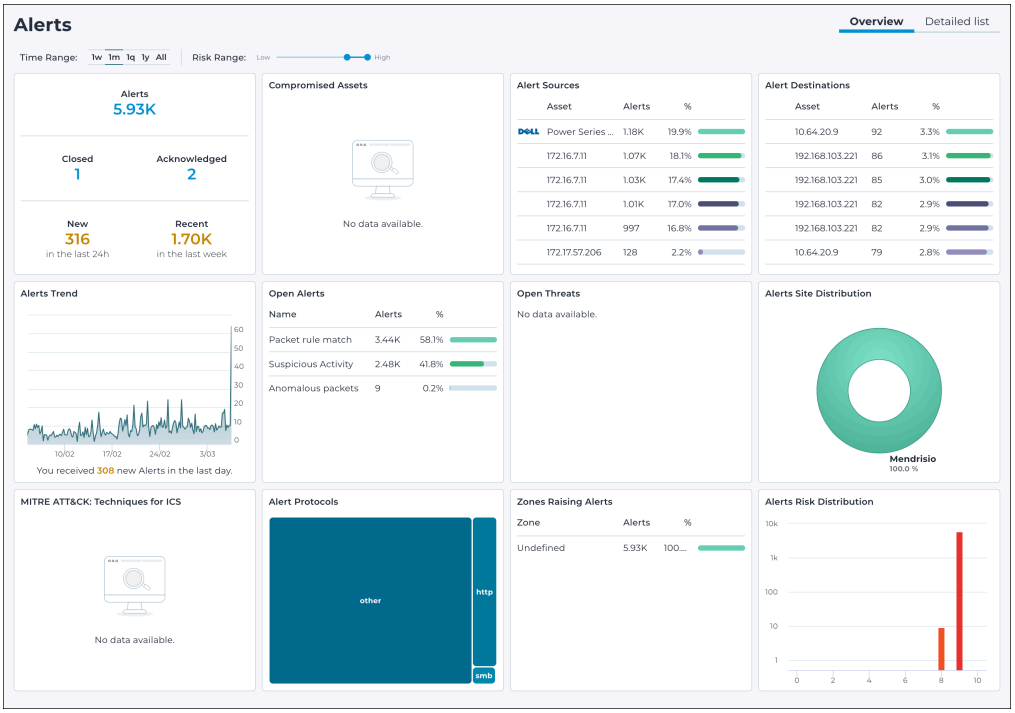


Figure 29. Overview page

Time Range

Allows users to filter alerts based on different time periods, such as:

- 1w (week)
- 1m (month)
- 1q (quarter)
- 1y (year)
- All

Risk Range

You can adjust the slider to filter alerts based on severity, from low to high.

Alerts

Shows the total number of security alerts, in these categories:

- Closed
- Acknowledged
- New
- Recent

Compromised Assets

Lists assets that have been flagged as compromised based on detected threats.

Alert Sources
Lists the origin of alerts, including affected devices and IP addresses.

Alert Protocols
Lists the types of network protocols associated with the detected alerts.

Alerts Trend
Shows a graphical representation of alerts over time, helping users analyze security trends.

Open Alerts
Lists a breakdown of open alerts by category.

Open Threats
Lists active security threats detected within the system.

Alerts Site Distribution
Shows the distribution of alerts by site or geographical region.

MITRE ATT&CK: Techniques for ICS
Provides security threat analysis using the MITRE ATT&CK framework, specifically for *industrial control systems (ICS)*.

Alert Protocols
Shows the network protocols associated with detected alerts.

Zones Raising Alerts
Shows which network zones are generating security alerts and their respective alert counts.

Alerts Risk Distribution
Shows the severity of alerts using a risk distribution graph.

Detailed list

*The **Detailed list** page shows all the alerts notifications that your sensors pass to Vantage related to security incidents in your network. This page lets you learn about the alerts, edit their values and post comments.*

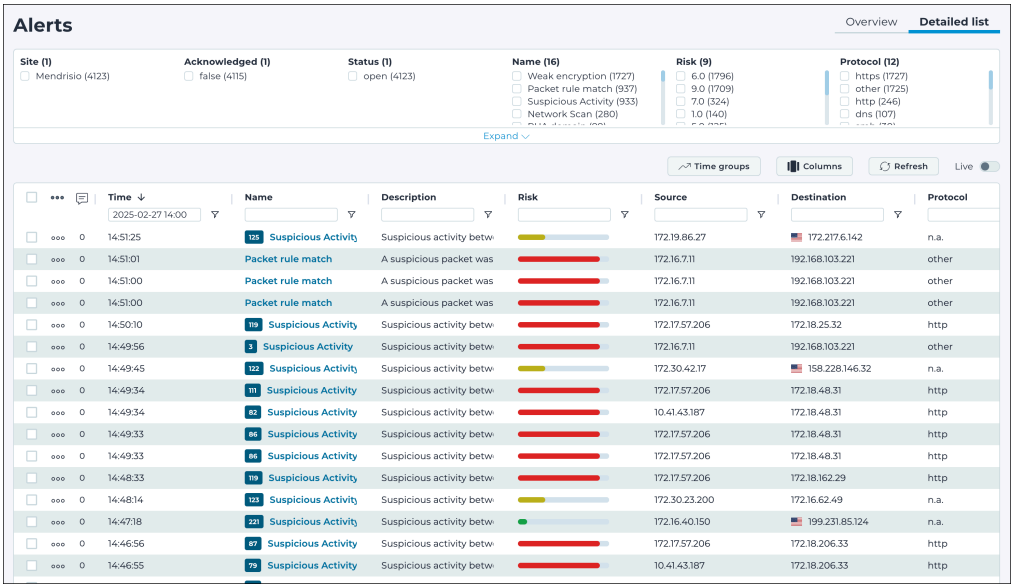


Figure 30. Detailed list page

Site

This shows a list of all the sites in the current table view.

Acknowledged

This shows a list of all the appliance types in the current table view.

Status

This shows a list of the different statuses that are applicable for the alerts in the current table view.

Name

This shows a list of the different names that are applicable for the alerts in the current table view.

Risk

This shows a list of the different risk levels that are applicable for the alerts in the current table view.

Protocol

This shows a list of the different protocols that are applicable for the alerts in the current table view.

Time groups

The **Time groups** button displays a throughput view of the data over a given time period.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Details page

The details page shows a set of fields which are applicable to the related type of alerts.

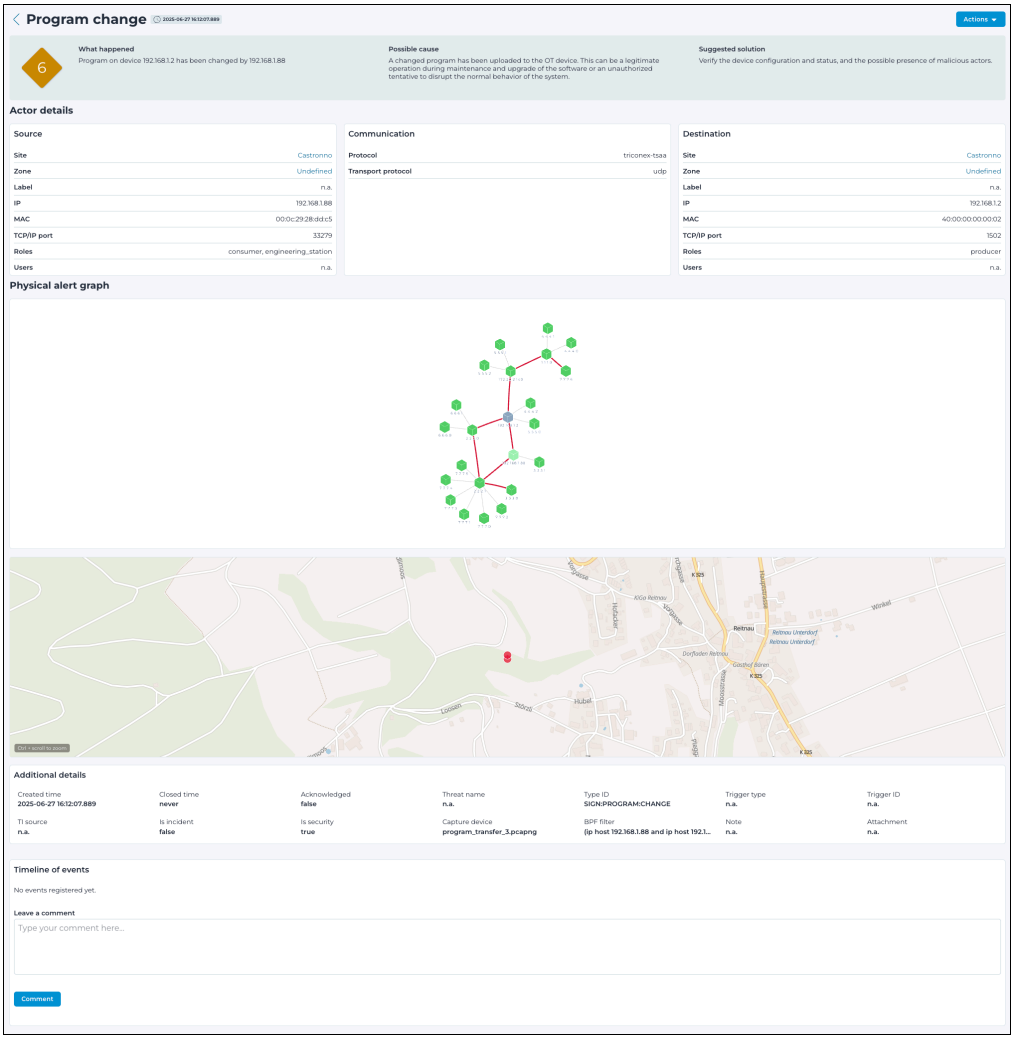


Figure 31. Details page

Actions dropdown

This dropdown gives you access to these actions:

- **Acknowledge**
- **Unacknowledge**
- **Close**
- **Create Alert Rule for this Alert**
- **Alert trace**

Summary
The summary section shows:

- What happened
- The possible cause of the alert
- The suggested solution for the alert

Actor details
The **Actor details** section shows information about the:

- **Source**: Details about where the activity was initiated
- **Communication**: The communication protocols detected
- **Destination**: Details about the targeted asset

Physical alert graph
The **Physical alert graph** view displays the physical connection path between source and destination devices involved in a triggered alert. Vantage shows this path at the cable level, including intermediate switches and any other devices connected along the route.

This view helps users assess the potential impact of response actions, such as disabling a specific switch port to isolate a device. By identifying additional assets that share the same physical infrastructure, operators can evaluate containment strategies and take targeted action directly from the alert interface.

Map
A map view that shows both the source and the destination of the alert to show it in a real-world context.

Playbook
If applicable, a playbook will be created from a template that has been defined by an administrator. The template guides you on how to best respond to the alert. You can edit an alert's playbook to collaborate with your colleagues and record the progress in resolving the alert.

Additional details
This section gives more context about the reported activity. Vantage displays the relevant details for this specific type of alert, and other fields are marked `n.a.`

MITRE ATT&CK for ICS Techniques Detection
This section shows when Vantage is able to provide information about the technique and attack tactics as defined in the MITRE ATT&CK Framework.

Timeline of events
This section shows all events that are related to this alert.

Comments
This section lets you add, or read, comments about this alert.

Related information

Open the details page (on page 112)

Summary drawer

When you double-click an alert in the table, the summary drawer shows. This lets you post a comment, or open the related details page.

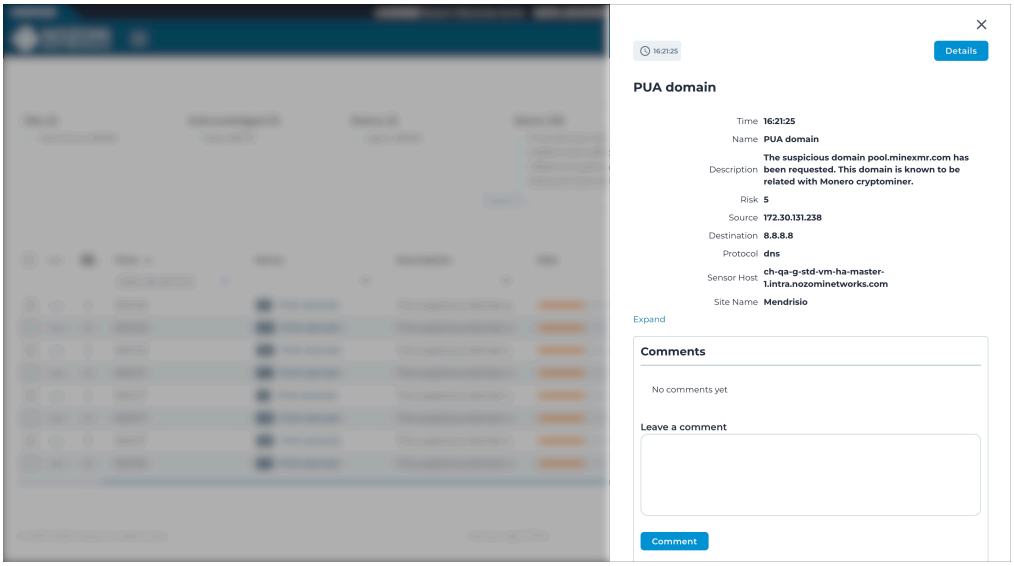


Figure 32. Summary drawer

Details button

You can select the **Details** button to open the details page for the related item.

Summary

The summary section shows a summary of applicable information for the related item.

Comments

This section lets you leave a comment, or read a comment that has been written, for the related item.

Related information

Open the summary drawer (on page 112)

Table interactions

Actions menu

Acknowledge an alert

The actions menu lets you acknowledge one or more alerts.

Procedure

1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

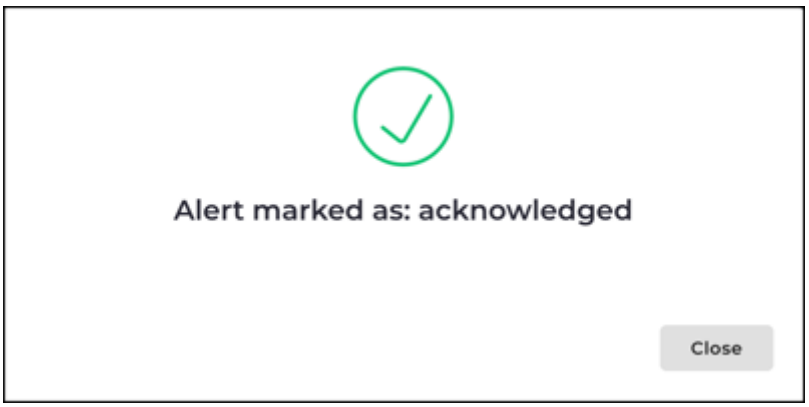
   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Acknowledge**.

   Result: A dialog shows.

5. Select **Confirm** to acknowledge the alert(s).

Result: A dialog shows.

6. Select **Close**.



Results

The alert has been acknowledged.

Unacknowledge an alert

The actions menu lets you unacknowledge an alert that has previously been acknowledged.

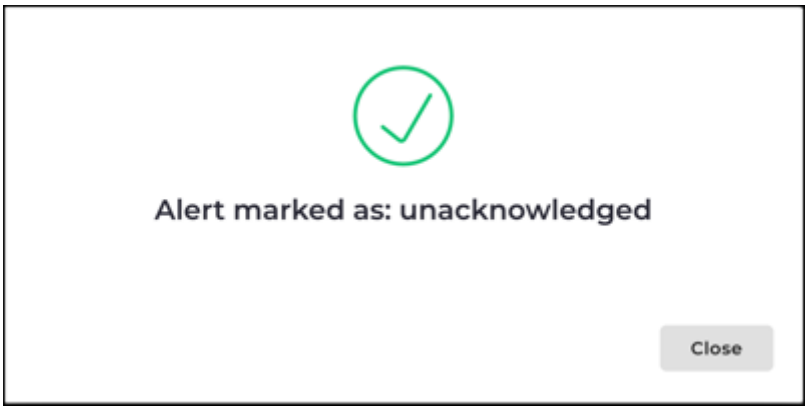
Procedure

1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Uncknowledge**.

   Result: A dialog shows.
5. Select **Confirm** to unacknowledge the alert(s).

   Result: A dialog shows.
6. Select **Close**.



Results

The alert has been unacknowledged.

Close an alert

The actions menu lets you close an alert.

Procedure

1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

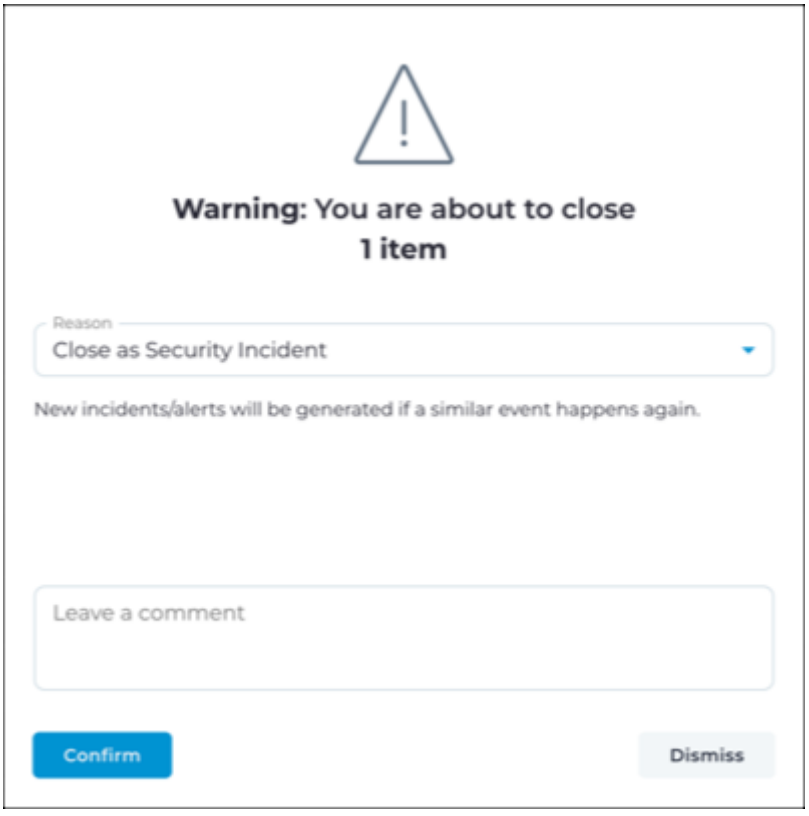
   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Close**.

   Result: A dialog shows.

5. Open the **Reason** dropdown, and select a reason.

6. Select **Confirm**.



Results

The alert(s) has (have) been closed.

Create an alert rule

The actions menu lets you create an alert rule from an alert. You can mute alerts permanently, or temporarily until a date that you specify.

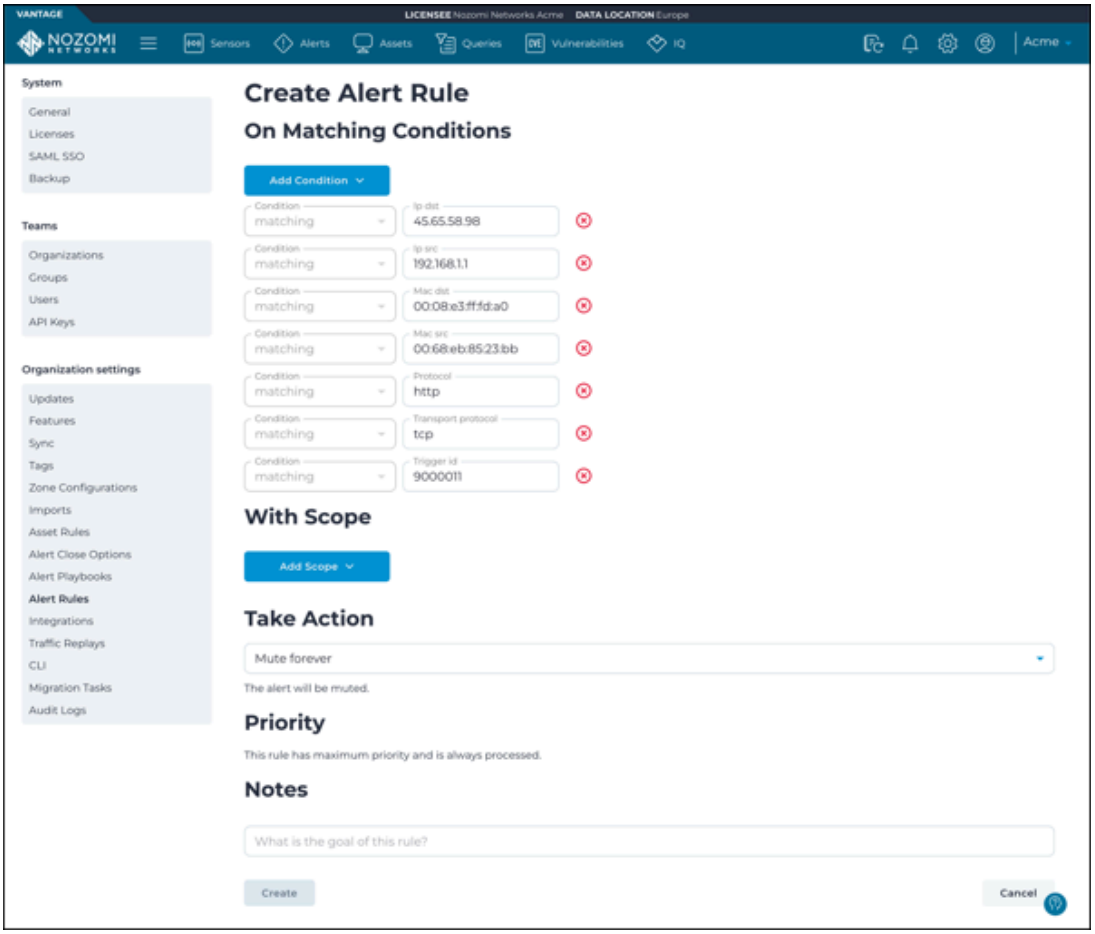
Procedure

1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Create Alert Rule From This Alert**.

   Result: The **Create Alert Rule** page opens.
5. Configure the alert rule as necessary.



6. Select **Create** to create the alert rule.

Results

The alert rule has been created.

Trace an alert

The action menu lets you download a trace file for a specific alert.

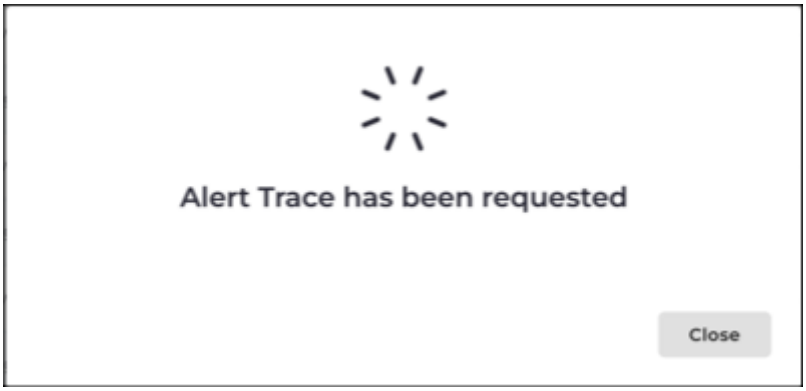
Procedure

1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Alert Trace**.

   Result: A dialog shows.
5. Select **Confirm** to create the alert rule.

   Result: A dialog shows.
6. Select **Close**.



Results

The alert trace has been requested.

Open the details page

You can open a details page for individual alerts that are shown in the alert page table. You can open the details page with two different methods.

Procedure

1. In the top navigation bar, select **Alerts**.
2. Choose a method with which to open the details page. In the row for the applicable alert:

   Choose from:

   - In the **Name** column of the table, select the hyperlink.
   - Double-click the row to open the summary drawer. In the top right section, select **Details**.

   Result: The details page (on page 98) opens.

Related information

Details page (on page 98)

Open the summary drawer

You can open a summary drawer for individual alerts that are shown in the alerts page table.

Procedure

1. In the top navigation bar, select **Alerts**.
2. In the table, double-click the row for the applicable alert.

   Result: The summary drawer (on page 100) opens.

Related information

Summary drawer (on page 100)

Chapter 4. Assets

*The **Assets** page shows all the physical components and systems that Vantage has detected through your sensors. Composed of one or more nodes, assets are the fundamental resources that Vantage protects.*

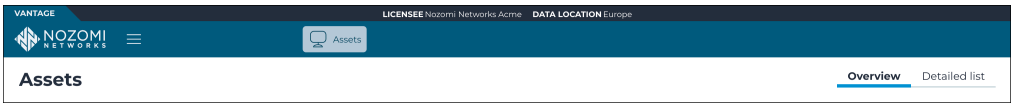


Figure 33. Assets page

The **Assets** page has these tabs:

- Overview (on page 116)
- Detailed list (on page 118)

Related information

Create an asset rule from an asset (on page 147)

Export an asset (on page 145)

Delete an asset (on page 144)

Overview

*The **Overview** page provides a high-level summary of assets that Vantage has detected. This information includes their types, vendors, operating systems, firmware versions, protocols, and risk levels, along with graphical insights into their distribution across zones, sites, and lifecycles.*

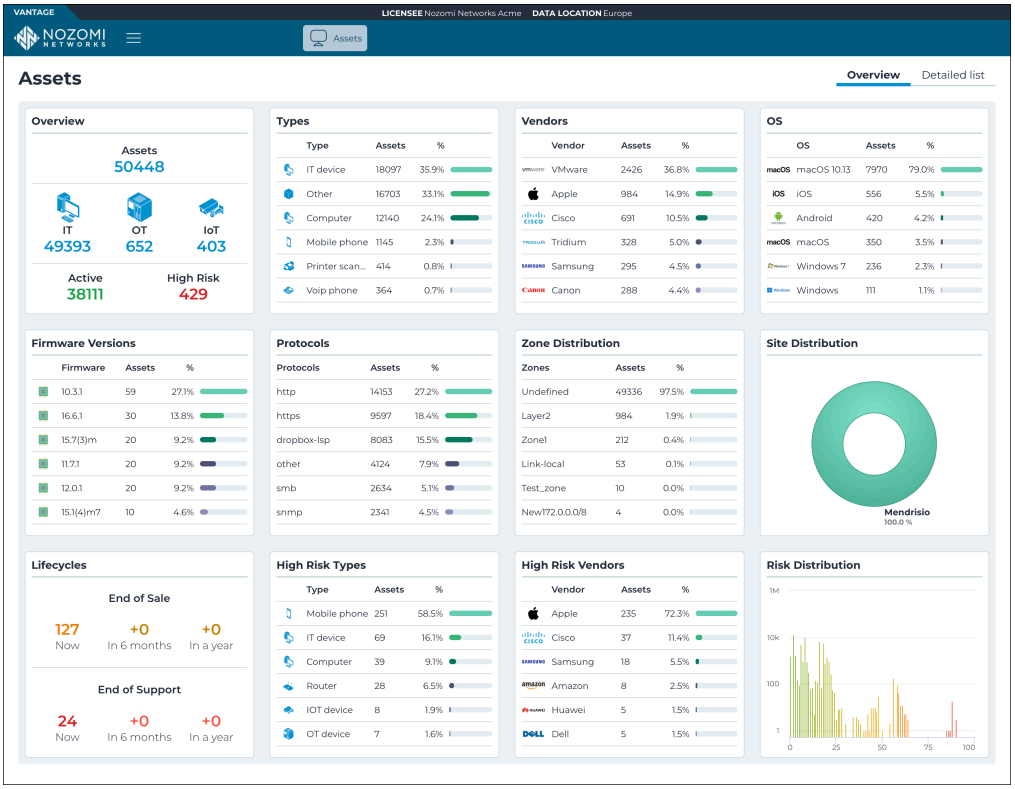


Figure 34. Overview page

The **Overview** page shows tiles that each show a different summarized view of different types of information. The tiles have hyperlinks that let you view the information in more detail. The tiles either show a graphical summary, or they show the:

- Related category
- Assets (the total number of assets that match the applicable category)
- % (this type of asset as a percentage of total assets)

Overview

This shows a high-level overview of all your assets. The tiles shows the:

- Total number of assets
- Type of asset
- Number of assets that are **Active**
- Number of assets that show as **High Risk**

Types

This shows a list of the type of assets, and the related information.

Vendors
This shows a list of the vendors of the assets, and the related information.

OS
This shows a list of the different *OS*s of the assets, and the related information.

Firmware Versions
This shows a list of the firmware versions for the assets, and the related information.

Protocols
This shows a list of the protocols that the assets use, and the related information.

Zone Distribution
This shows how the assets are distributed within zones, and the related information.

Site Distribution
This shows a donut chart that shows where the assets are distributed across sites.

Lifecycles
This shows lifecycle information about the assets.

High Risk Types
This shows a list of assets that are high risk types, in descending order, and the related information.

High Risk Vendors
This shows a list of assets that are from high risk vendors, in descending order, and the related information.

Risk Distribution
This shows a bar chart view of the risk as distributed across the different assets.

Detailed list

*The **Detailed list** page shows a comprehensive table view of all assets that Vantage has detected. This information includes details about their sites, types, vendors, operating systems, and firmware versions.*

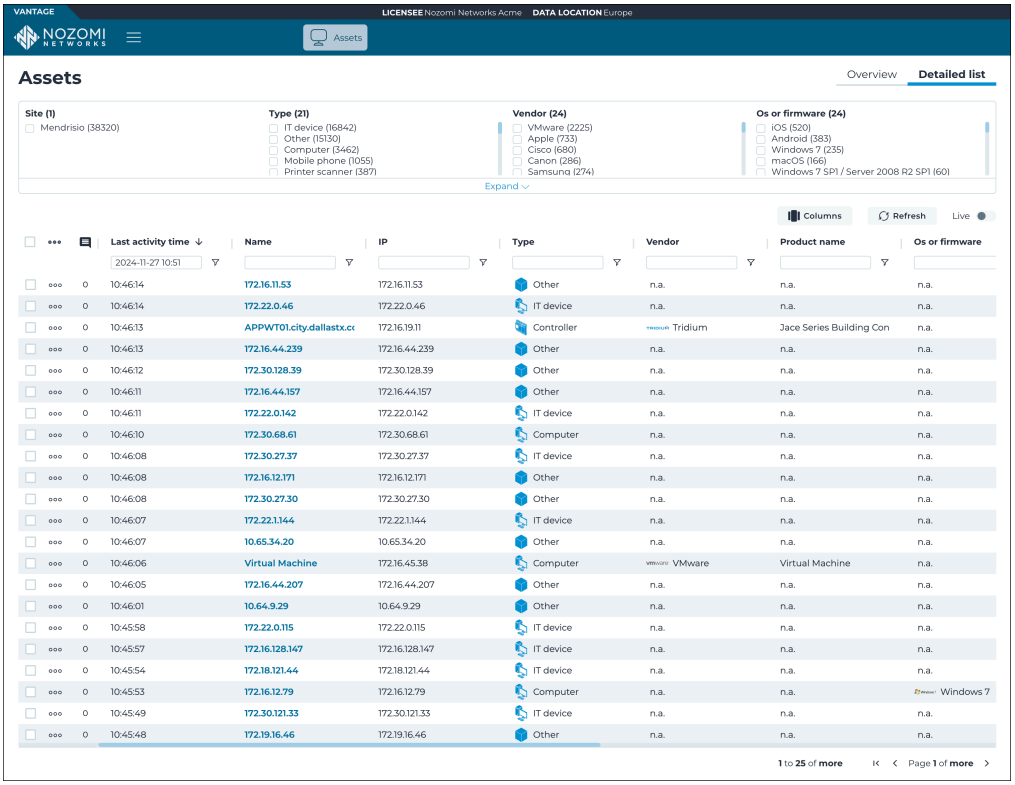


Figure 35. Detailed list page

Site

This shows a list of all the sites for the applicable assets in the current table view.

Type

This shows a list of all the types for all the assets in the current in the current table view.

Vendor

This shows a list of the different vendors that are applicable for the alerts in the current table view.

OS or firmware

This shows a list of the different *OS* or firmware that are applicable for the alerts in the current table view.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Details page

The details page shows a set of fields which are applicable to the related type of asset.

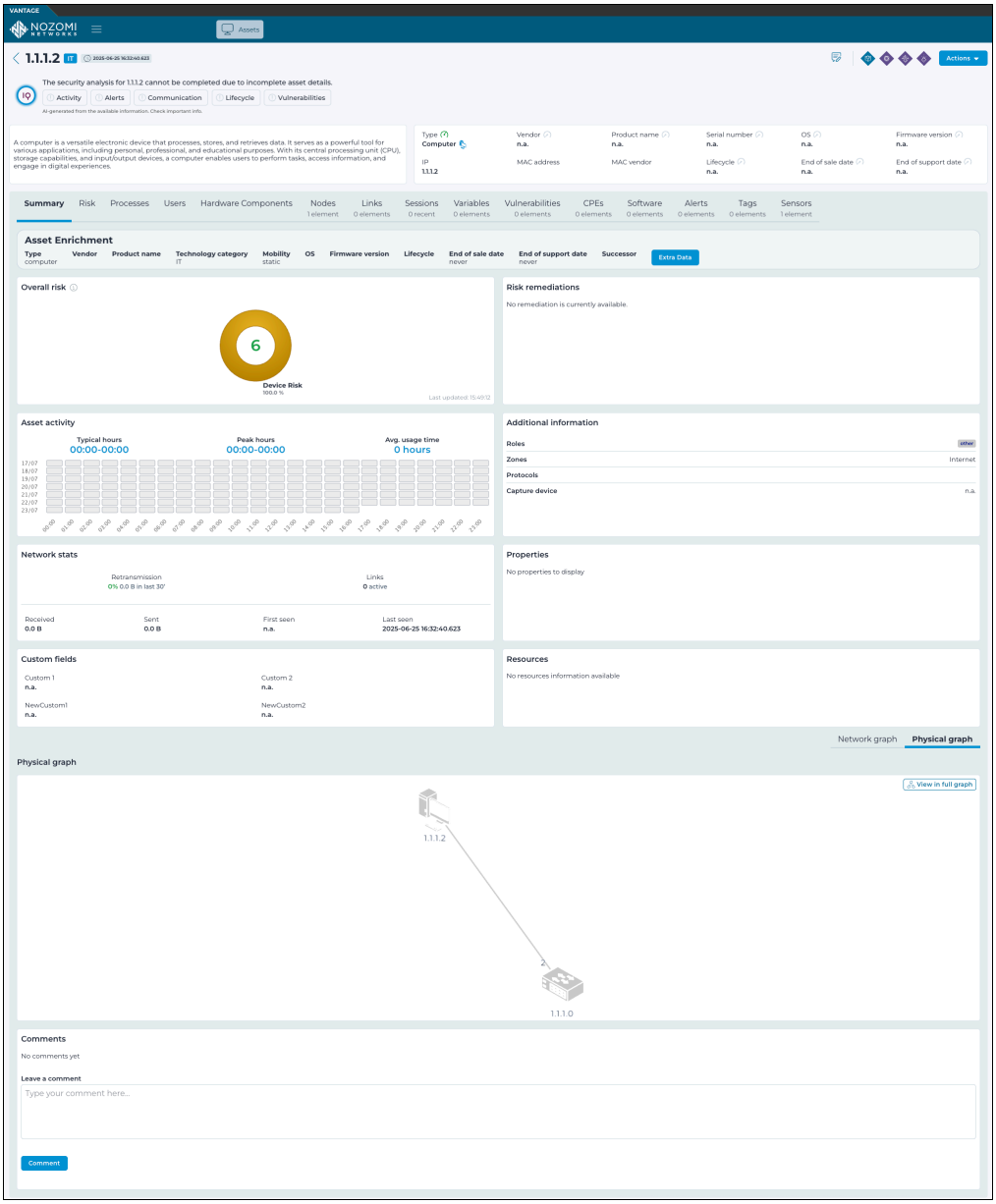


Figure 36. Details page

Actions dropdown

This dropdown gives you access to these actions:

- Delete (on page 144)
- Export (on page 145) (bulk option only)
- Create Asset Rule From This Asset (on page 147)

Tabs

The details page has these tabs:

- Summary tab (on page 122)
- Risk tab (on page 124)
- Processes tab (on page 126)
- Users tab (on page 127)
- Hardware Components tab (on page 128)
- Nodes tab (on page 131)
- Links tab (on page 132)
- Sessions tab (on page 133)
- Variables tab (on page 134)
- Vulnerabilities tab (on page 135)
- CPEs tab (on page 136)
- Software tab (on page 137)
- Alerts tab (on page 138)
- Tags tab (on page 139)
- Sensors tab (on page 142)

Related information

Open the details page (on page 148)

Summary tab

*The **Summary** tab shows an overview of the details for the asset.*

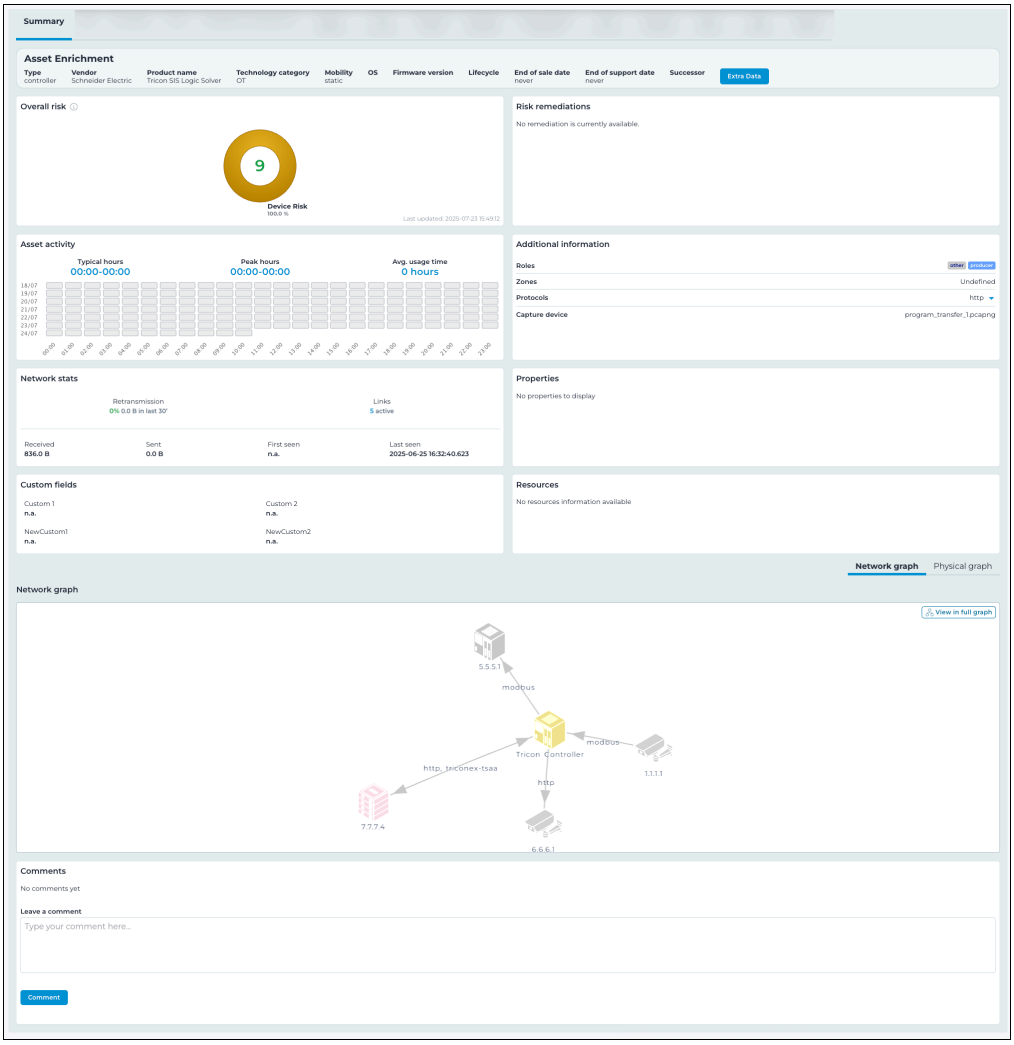


Figure 37. Summary tab

Network stats

This section shows different network statistics for the asset.

Properties

This section shows properties for the asset.

Hardware components

If applicable, Vantage shows a list of the asset's hardware components.

Network graph

This section shows these different views:

- Network graph (on page 250)
- Physical graph (on page 253)

Comments

This section lets you write a comment for the asset. It also shows comments that have been previously written.

Risk tab

*The **Risk** tab shows an overview of the risk assessment for the asset.*

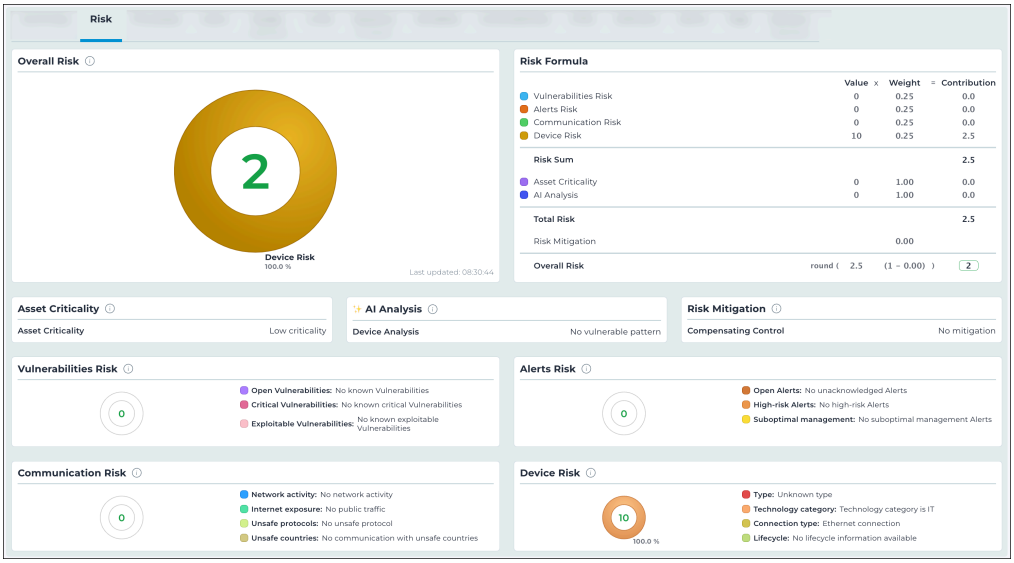


Figure 38. Risk tab

Overall Risk

This section displays the calculated overall risk score for the asset. It is visually represented with a risk level indicator.

Risk Formula

This section details the formula used to compute the overall risk score. It includes components such as:

- **Vulnerabilities Risk**: Risk derived from identified vulnerabilities.
- **Alerts Risk**: Risk due to unacknowledged or high-risk alerts.
- **Communication Risk**: Risk based on network activity and exposure.
- **Device Risk**: Risk based on the device's characteristics and lifecycle.

Asset Criticality

Indicates the criticality level of the asset in the network.

AI Analysis

Shows AI-driven insights into the risk posture of the asset.

Risk Mitigation

Displays all compensating controls applied to mitigate risk.

Vulnerabilities Risk

Summarizes detected vulnerabilities, categorized as:

- Open Vulnerabilities
- Critical Vulnerabilities
- Exploitable Vulnerabilities

Alerts Risk
Lists active security alerts impacting the asset.

Communication Risk
Analyzes network activity, including:

- Internet exposure
- Use of unsafe protocols
- Communication with unsafe countries

Device Risk
Assesses risk based on device attributes, such as:

- Technology category
- Connection type
- Lifecycle status

Processes tab

*The **Processes** tab shows all running processes detected on the asset with details like name, ID, and connection counts. It enables security teams to monitor activity and investigate potential threats and supports proactive management of asset performance and risk.*

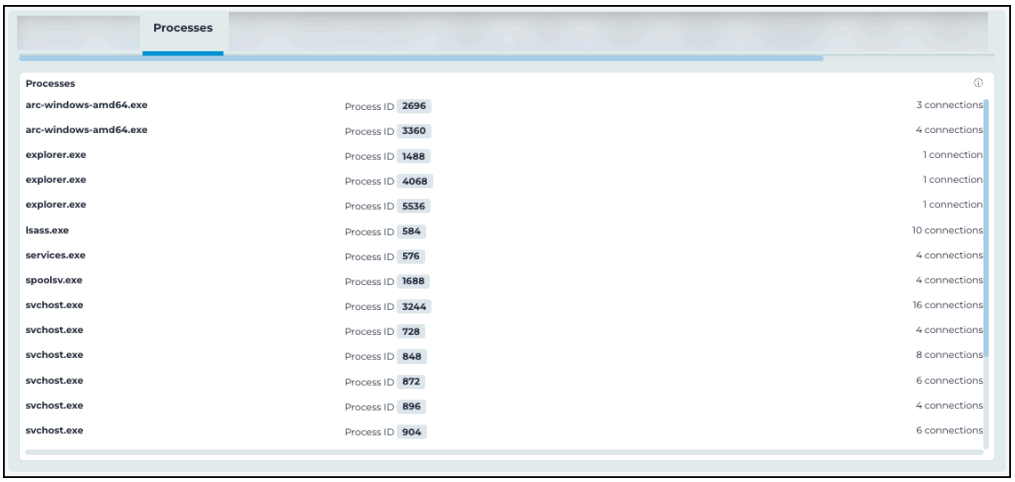


Figure 39. Processes tab

Users tab

*The **Users** tab shows all the users that Vantage has detected for this asset.*

Figure 40. Users tab

Lists all user accounts discovered on the asset, showing details such as username or the account type, such as:

- Username
- Account type
    - Guest
    - Administrator
- Status
- Domain membership

This helps security teams review local and domain accounts for risk assessment and user access auditing. It also supports the identification of inactive or misconfigured accounts that might present vulnerabilities.

Hardware Components tab

*The **Hardware Components** page shows a list of hardware modules installed on the same chassis as the selected controller, providing details on each component for better visibility and management of the device's physical configuration.*

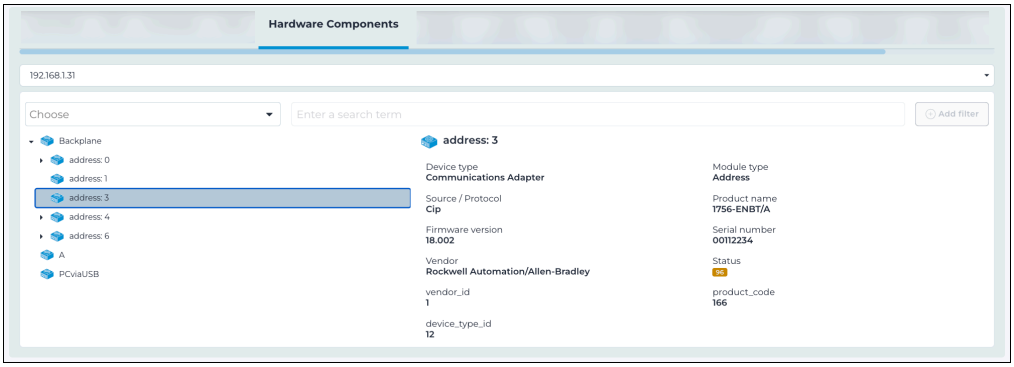


Figure 41. Hardware Components tab

Focus-on selector

This shows the *IP* address of the controller whose chassis information is shown below. When available, it lets you select other nodes related to the same controller.

Figure 42. Focus-on selector

Choose

This dropdown lets you select from a list of attributes.

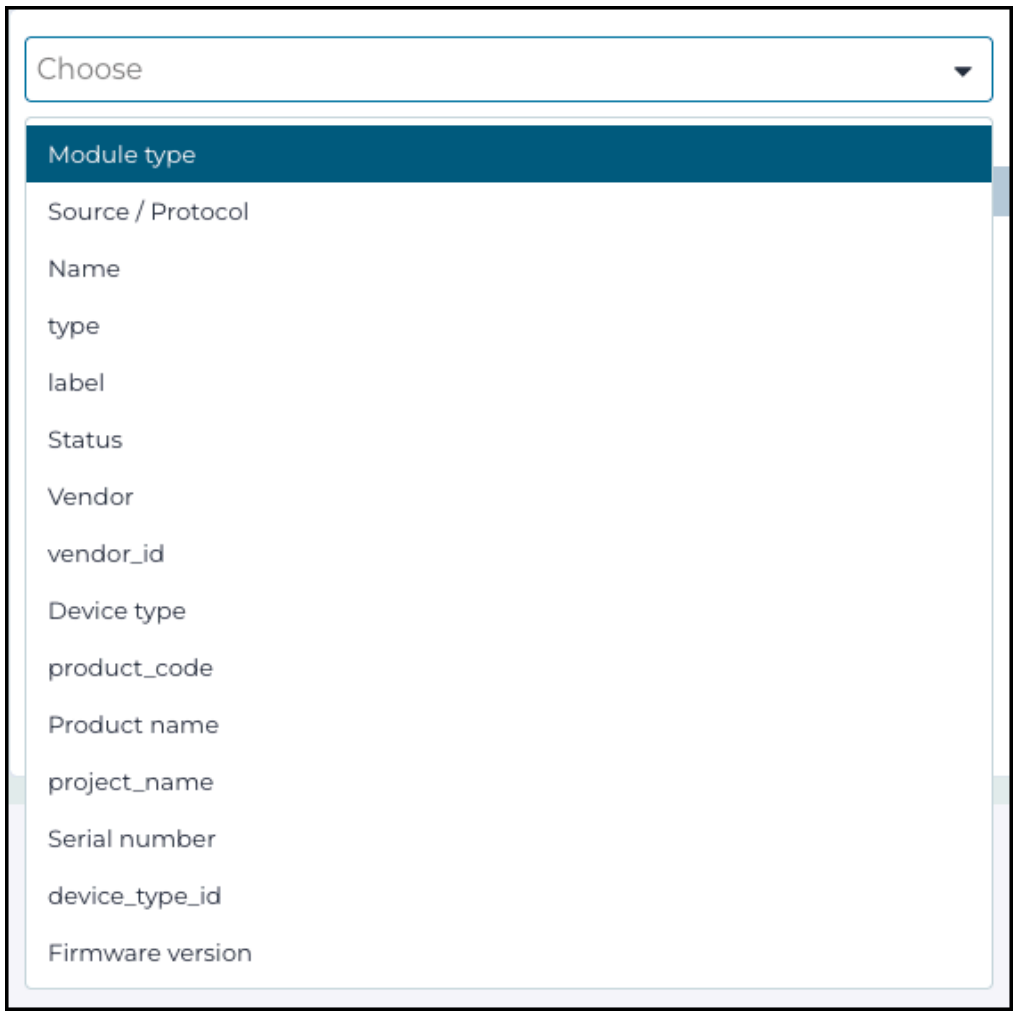


Figure 43. Choose dropdown

Search bar

The search bar lets you enter a term to filter the list.

Figure 44. Search bar

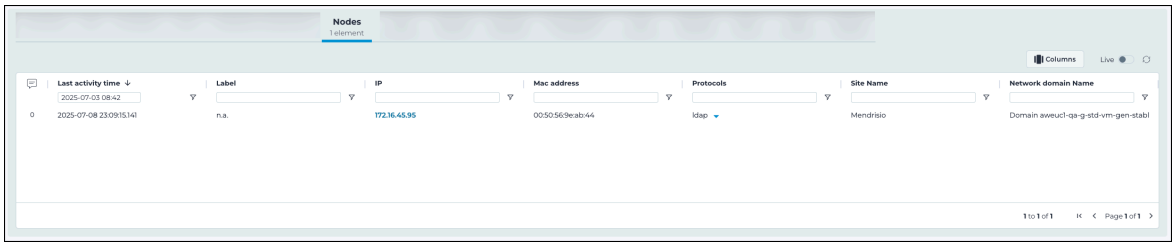
Add filter

Select this button to apply the filter in the search bar.

Figure 45. Add filter button

Nodes tab

*The **Nodes** tab shows all the nodes that Vantage has detected. Nodes are individual actors in the network communication. Assets have of one, or more, nodes. A node could be a device, such as a computer, a remote terminal unit (RTU), or a programmable logic controller (PLC). The protocols that a node uses can provide insights about its asset.*



Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Links tab

*The **Links** tab shows all the links that Vantage has detected. Links are the connections between the asset and other physical systems.*

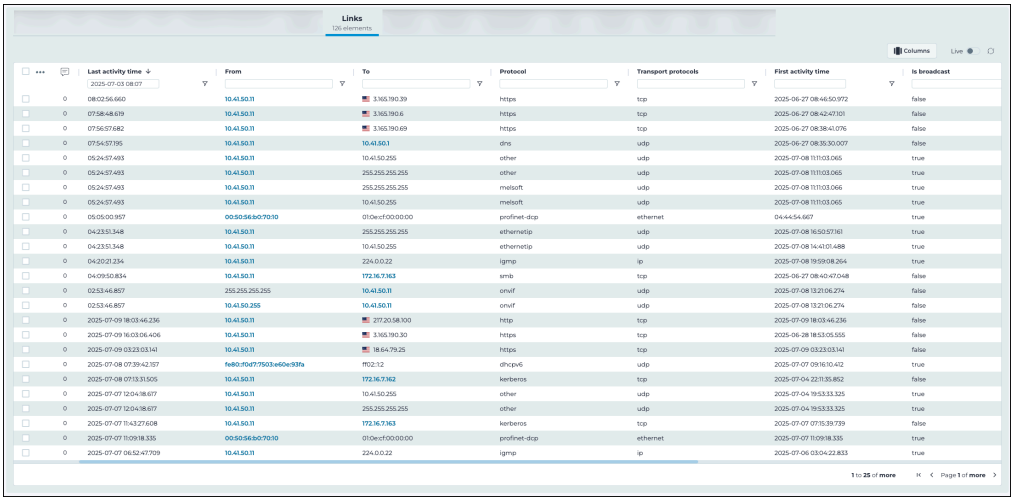


Figure 46. Links tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Sessions tab

*The **Sessions** tab shows all the sessions that Vantage has detected for this asset. Sessions are semi-permanent, interactive information exchanges between two or more communicating nodes.*

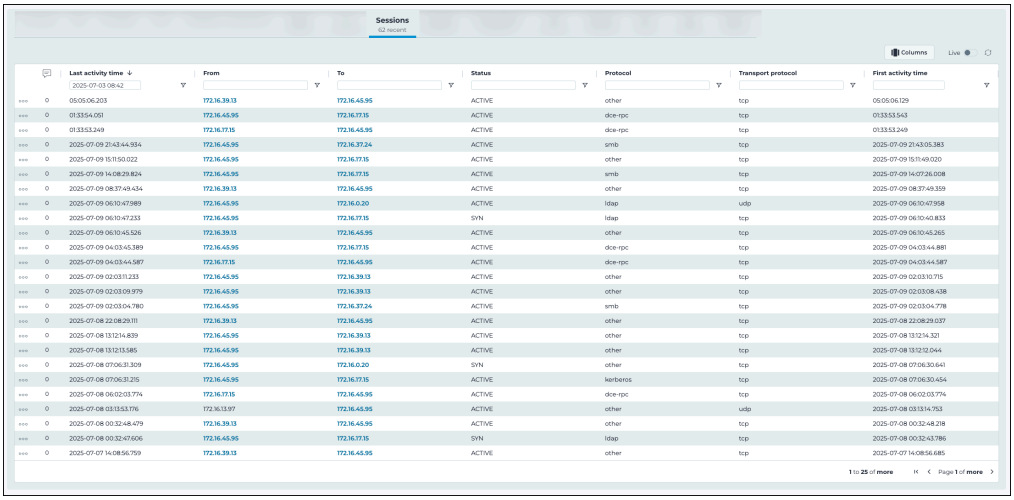


Figure 47. Sessions tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Variables tab

*The **Variables** tab shows all the variables that Vantage has detected for this asset. Variables are the numerical values that are related to an industrial process that your sensors monitor.*

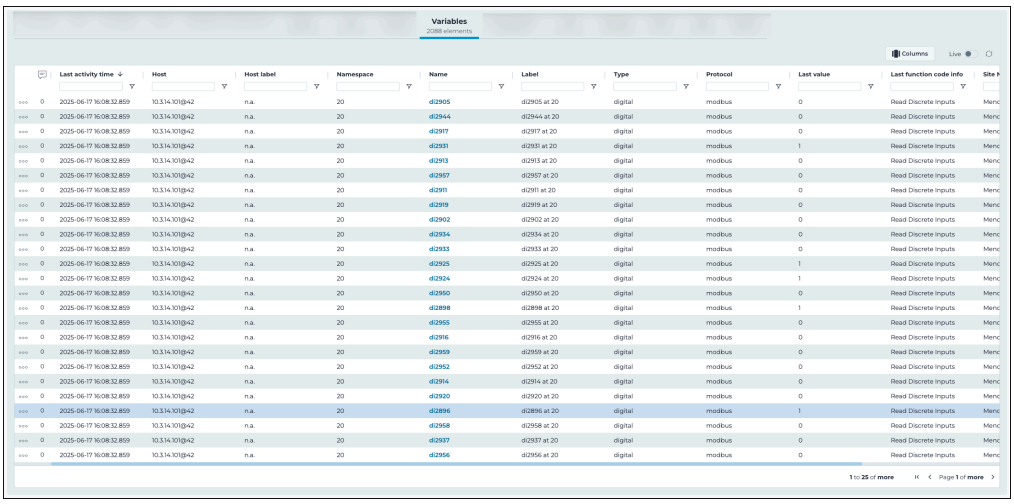


Figure 48. Variables tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Vulnerabilities tab

*The **Vulnerabilities** tab shows all the vulnerabilities that Vantage has detected for this asset. Vulnerabilities are weaknesses that reduce the security of your system and give threat actors an opportunity to exploit your system.*

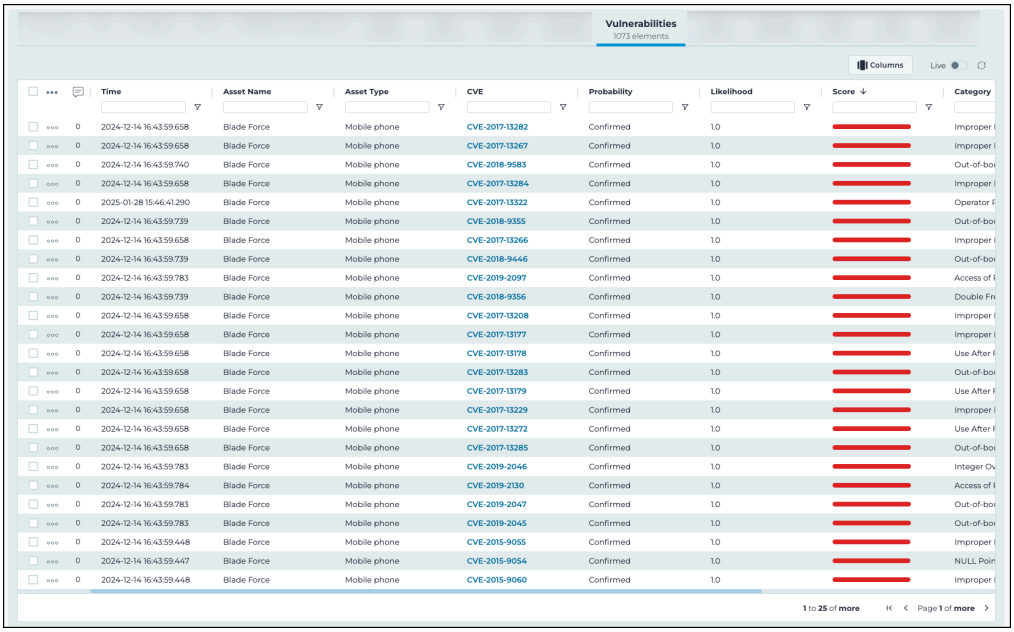


Figure 49. Vulnerabilities tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

CPEs tab

*The **CPEs** tab shows all the common platform enumerations (CPEs) that Vantage has detected for this asset.*

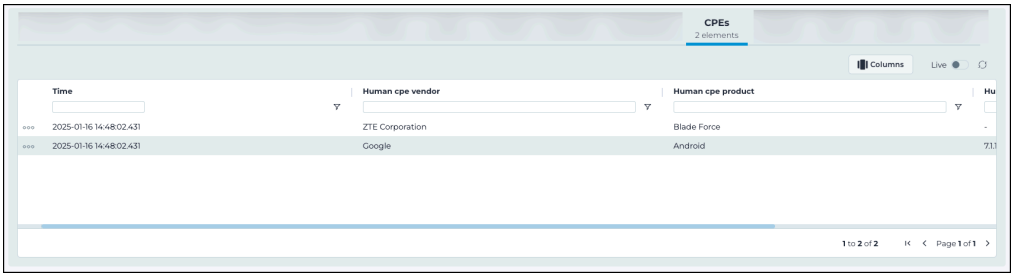


Figure 50. CPE tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Software tab

*The **Software list** tab shows all the software installations that Vantage has detected on this asset.*

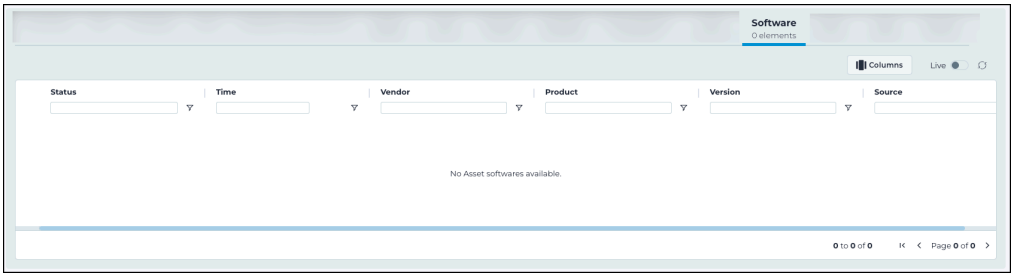


Figure 51. Software tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Alerts tab

*The **Alerts** tab shows all the alerts that Vantage has detected for this asset.*

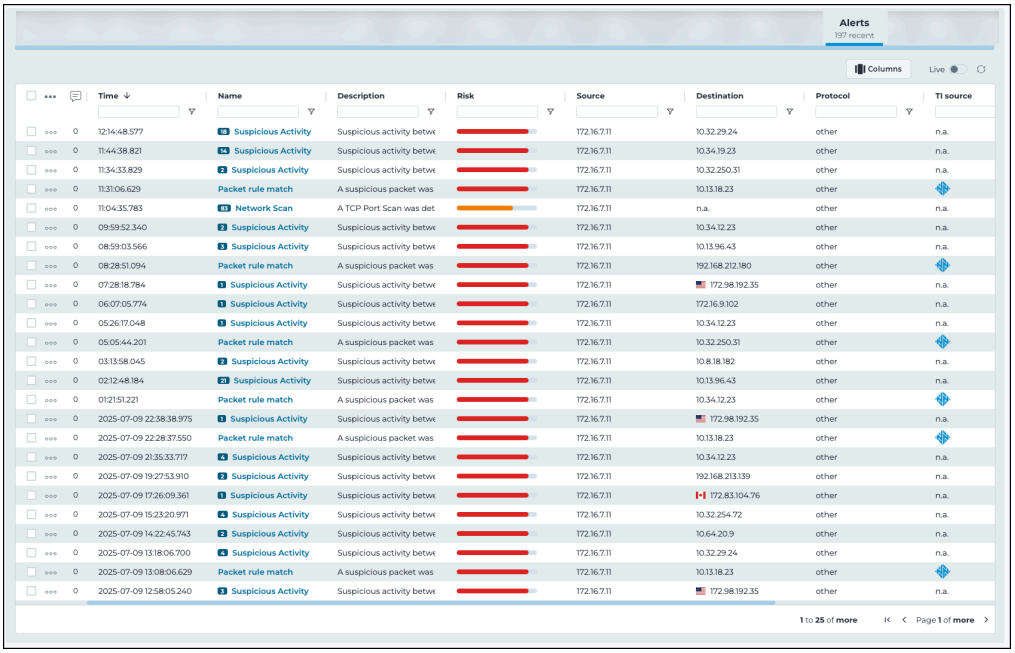


Figure 52. Alerts tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Tags tab

*The **Tags** tab shows all the tags for this asset. Tags are user-defined labels that have been assigned to this asset. Tags are associated with user roles to define access control.*

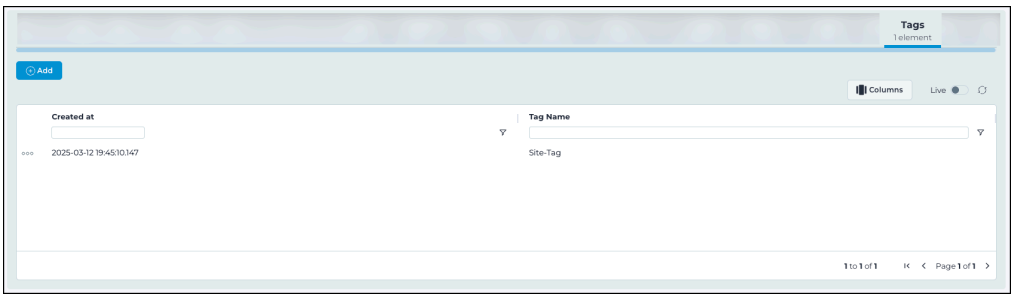


Figure 53. Tags tab

Add new

This button lets you add a new tag (on page 140) to the related asset.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Add a tag to an asset

You can add tags to assets. This lets you refine the permissions that you grant to users.

About this task

You can add one or more tags to the selected asset.

Procedure

1. Open the details page (on page 148) for the applicable asset.
2. Select the **Tags** tab.
3. Select **Add new**.

   Result: The **Tag** dropdown shows.
4. Open the dropdown and select the correct tag.

   Note:
   Only the tags that have been assigned for your organization show.
5. Select **Create**.

   Result: The tag has been added to the related asset.

Related information

Tags tab (on page 139)

Delete a tag from an asset (on page 141)

Delete a tag from an asset

If a tag has been added to a asset, you can delete it.

Procedure

1. Open the details page (on page 148) for the applicable asset.
2. Select the **Tags** tab.
3. Double-click the applicable tag.

   Result: The summary drawer shows.
4. Select **Details**.

   Result: The details page for the related tag shows.
5. Select **Actions > Delete**.

Results

The tag has been deleted.

Related information

Tags tab (on page 139)

Add a tag to an asset (on page 140)

Sensors tab

*The **Sensors** tab shows all the sensors that Vantage has detected for this asset.*

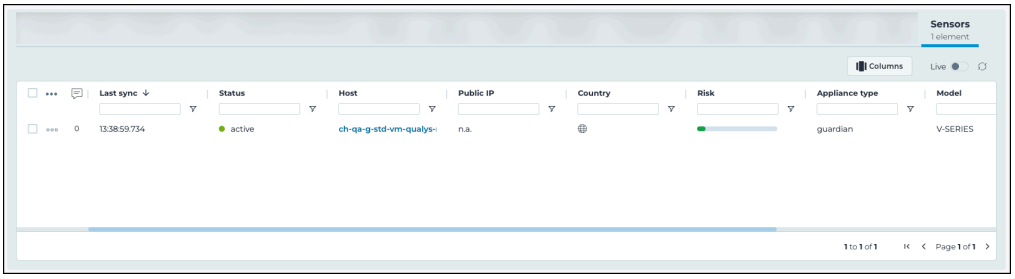


Figure 54. Sensors tab

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The refresh icon lets you immediately refresh the graph.

Summary drawer

When you double-click an asset in the table, the summary drawer shows. This lets you post a comment, or open the related details page.

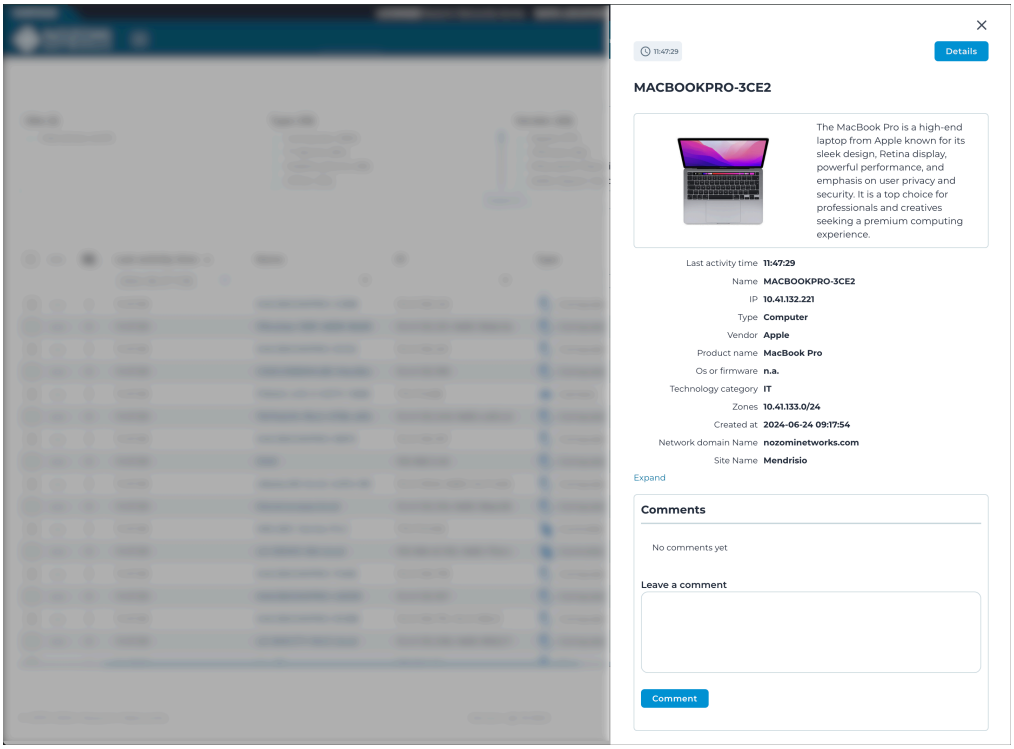


Figure 55. Summary drawer

Details button

You can select the **Details** button to open the details page for the related item.

Summary

The summary section shows a summary of applicable information for the related item.

Comments

This section lets you leave a comment, or read a comment that has been written, for the related item.

Related information

Open the summary drawer (on page 148)

Table interactions

Actions menu

Delete an asset

You can use the actions menu to delete an asset.

Procedure

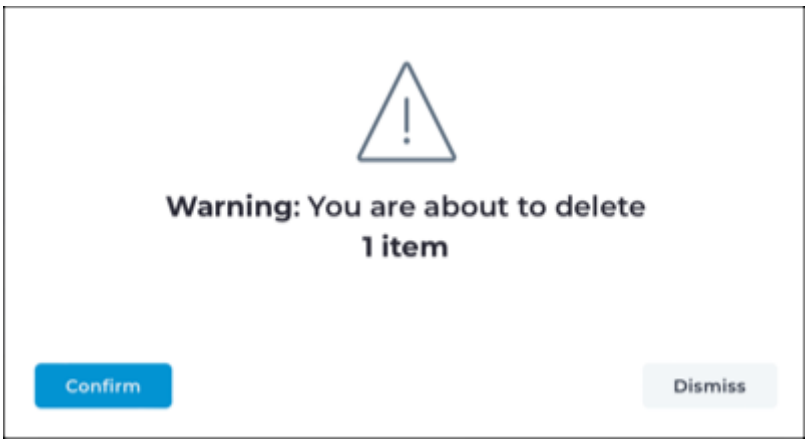
1. In the top navigation bar, select **Assets**.
2. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon
3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
4. Select **Delete**.



   Result: A confirmation dialog shows.

Results

The asset(s) has been deleted.

Export an asset

You can use the actions menu to export one or more assets to a spreadsheet.

Procedure

1. In the top navigation bar, select **Assets**.
2. Choose a method to open the actions menu.

   Choose from:

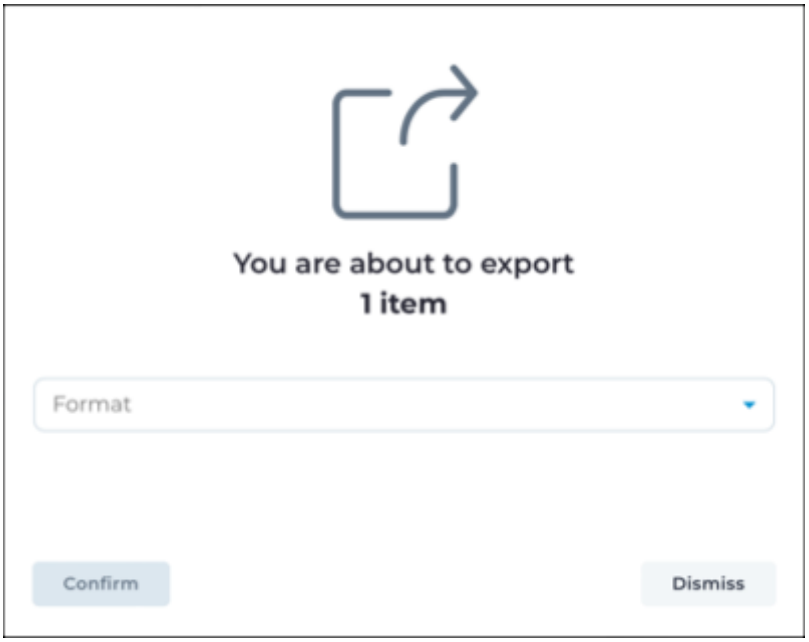
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Export**.

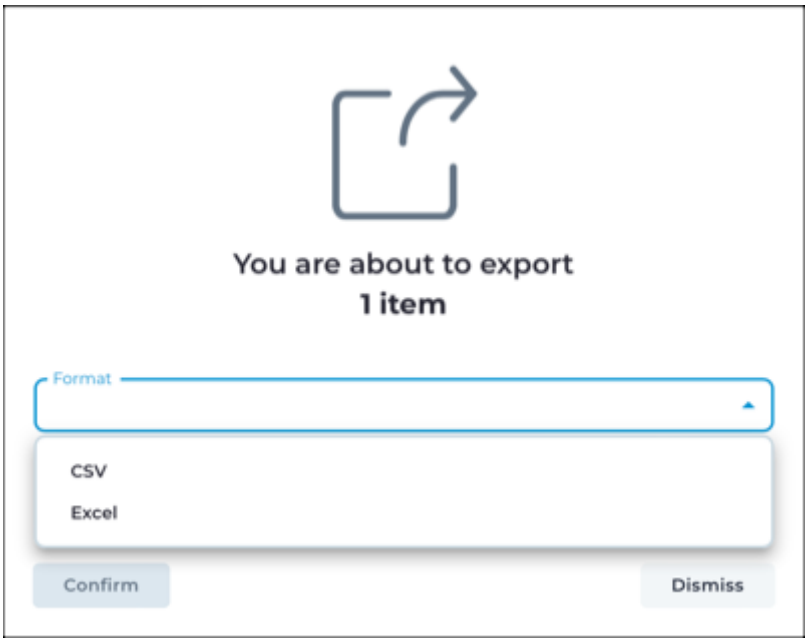


   Result: The export dialog shows.

5. Select the **Format** dropdown.

   Result: A dialog shows.

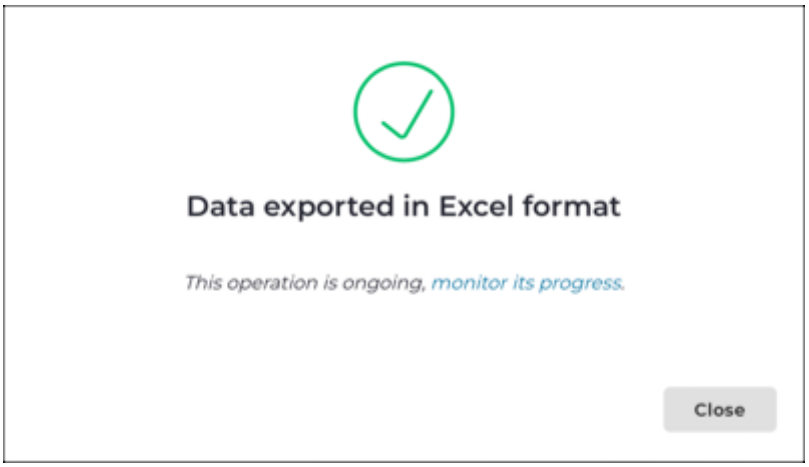
6. In the **Format** dropdown, select the format that you want to export.



7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.



Results

The asset(s) has been exported.

Create an asset rule from an asset

You can create an asset rule directly from one, or more, assets in the asset page table.

Procedure

1. In the top navigation bar, select **Assets**.
2. Choose a method to open the actions menu.

   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

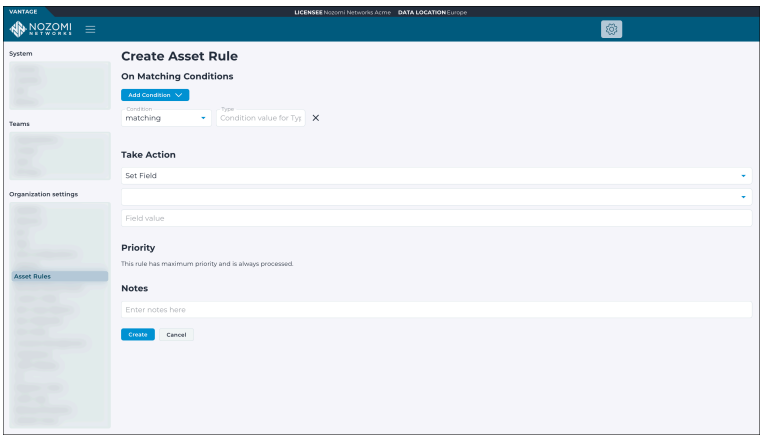
   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Create Asset Rule From This Asset**.

   Result: The **Create Asset Rule** page opens.

5. Configure the asset rule as necessary.



6. Select **Create**.

Results

The asset rule has been created.

Open the details page

You can open a details page for individual assets that are shown in the asset page table. You can open the details page with two different methods.

Procedure

1. In the top navigation bar, select **Assets**.
2. Choose a method with which to open the details page. In the row for the applicable asset:

   Choose from:

   - In the **Name** column of the table, select the hyperlink.
   - Double-click the row to open the summary drawer. In the top right section, select **Details**.

   Result: The details page (on page 120) opens.

Related information

Details page (on page 120)

Open the summary drawer

You can open a summary drawer for individual assets that are shown in the assets page table.

Procedure

1. In the top navigation bar, select **Assets**.
2. In the table, double-click the row for the applicable asset.

   Result: The summary drawer (on page 143) opens.

Related information

Summary drawer (on page 143)

Chapter 5. Wireless

*The **Wireless** page lets you buy and connect a Guardian Air sensor. Once you have connected one or more Guardian Air sensor, the **Wireless** page show the connected Guardian Air sensors.*

First use

If you open the Wireless page, but you have not previously connected a Guardian Air sensor, you will see a view similar to the one below.

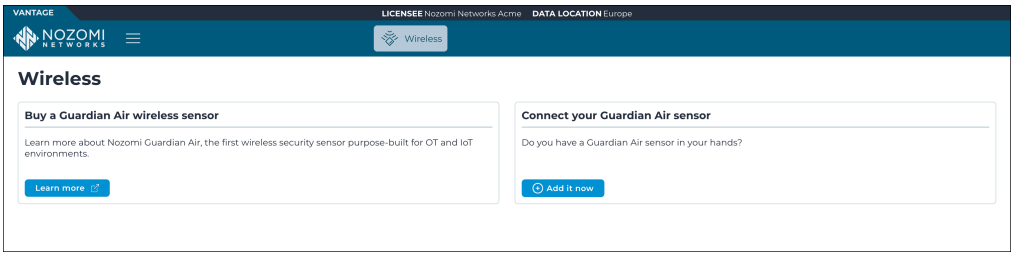


Figure 56. Wireless page (before a Guardian Air sensor has been added)

Buy a Guardian Air wireless sensor

This section lets you buy your first Guardian Air sensor, and learn more about Guardian Air.

Connect your Guardian Air sensor

Once you have purchased one or more Guardian Air sensors, this section lets you connect it.

After you have connected a Guardian Air sensor

Once you have connected one or more Guardian Air sensors, you will see a view similar to the one below.

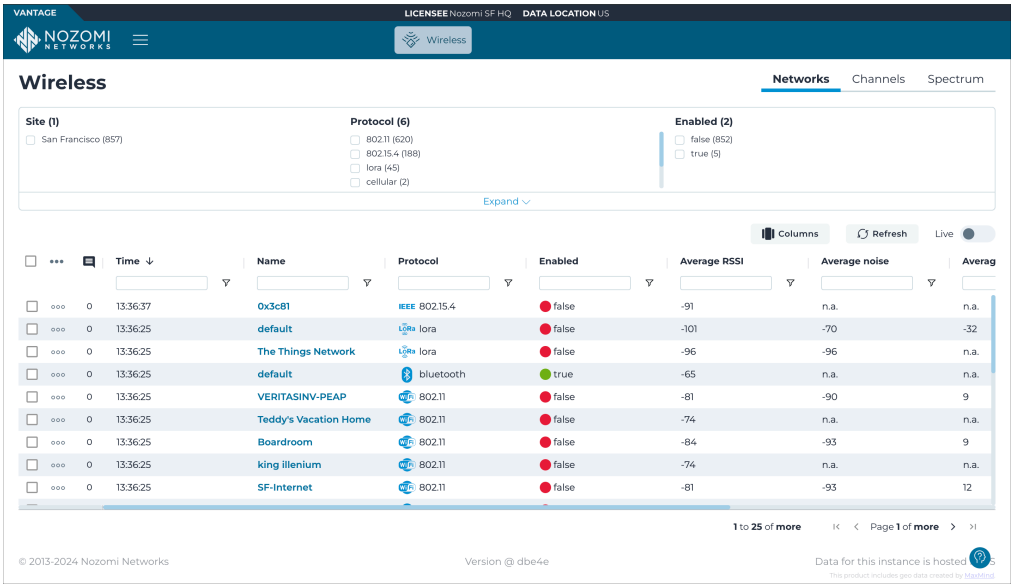


Figure 57. Wireless page (after a Guardian Air sensor has been added)

Related information

Enable a wireless network (on page 157)

Disable a wireless network (on page 158)

Delete a wireless network (on page 161)

Enable the inspection of devices with private MAC addresses (on page 159)

Disable the inspection of devices with private MAC addresses (on page 160)

Networks

*The **Networks** page shows an overview of network sites, protocols, and sensor activation statuses, and includes interactive sections for managing these elements effectively.*

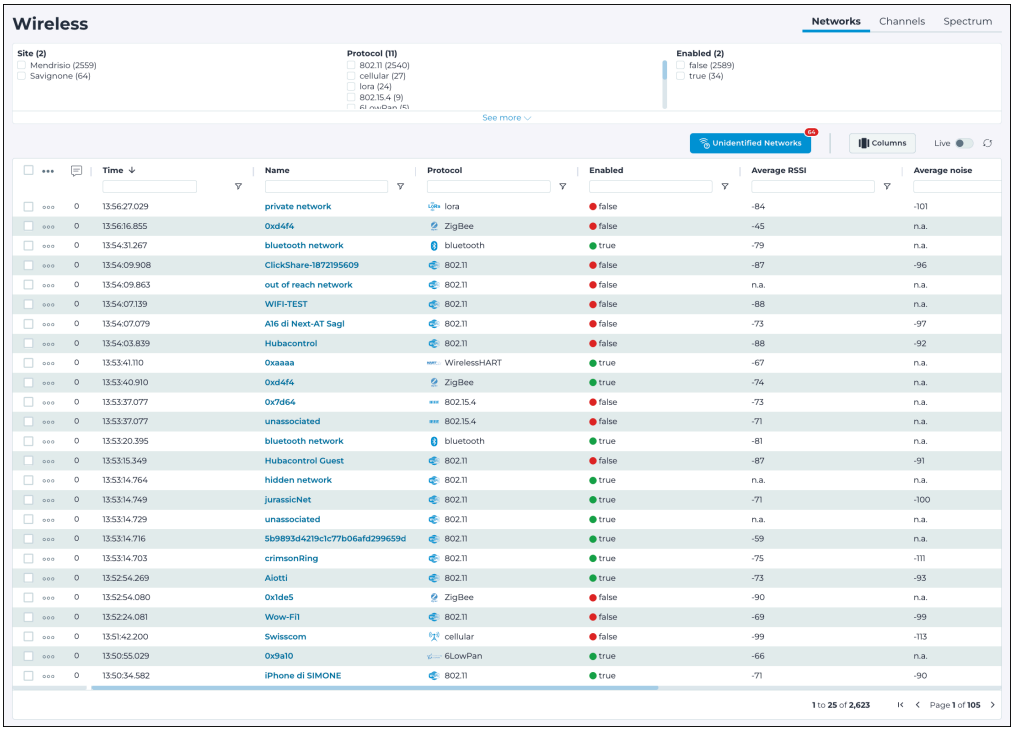


Figure 58. Networks page

Site

This section shows all sites that you have added to your environment, and lets you select the sensors related to a site.

Protocol

This column shows the protocol for the related sensor.

Enabled

This column shows whether the related sensor is enabled or not.

Live

The live toggle lets you immediately refresh the graph.

Refresh

The refresh icon lets you immediately refresh the graph.

Channels

*The **Channels** page gives a detailed view and management options for wireless channels.*

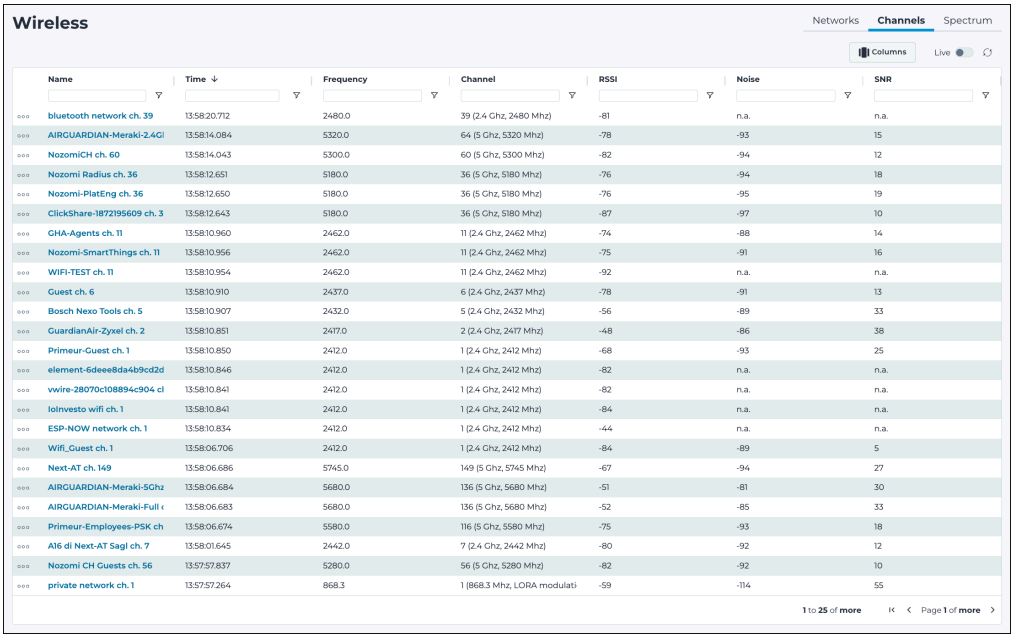


Figure 59. Channels page

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The live toggle lets you immediately refresh the graph.

Refresh

The refresh icon lets you immediately refresh the graph.

Spectrum

*The **Spectrum** page shows a comprehensive view of wireless signal metrics and customizable viewing options to analyze channels, signal strength, and noise across different timeframes.*

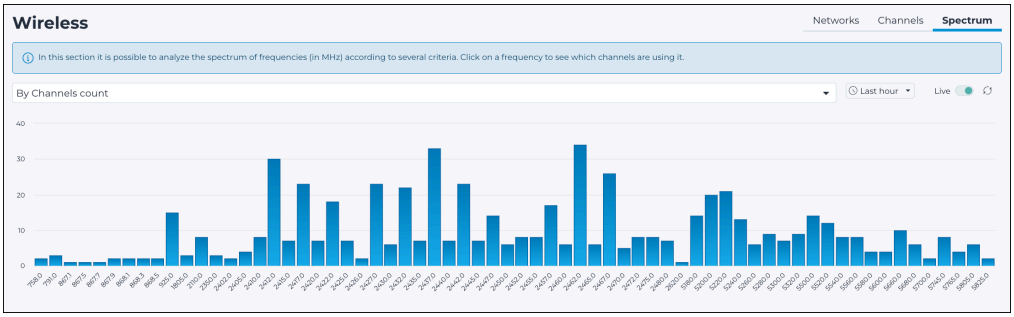


Figure 60. Spectrum page

Options dropdown

This lets you select different views. You can choose from:

- By Channels count
- By Average Signal to Noise Ratio
- By Average RSSI
- By Average Noise

Timeframe dropdown

This lets you select a timeframe for the chart view. You can choose from:

- Last hour
- Last day
- Last week

Live

The live toggle lets you immediately refresh the graph.

Refresh

The refresh icon lets you immediately refresh the graph.

Details page

The details page displays information about wireless networks, including its protocol, site, status, and signal metrics. It also provides tabs for viewing channels, assets, and alerts.

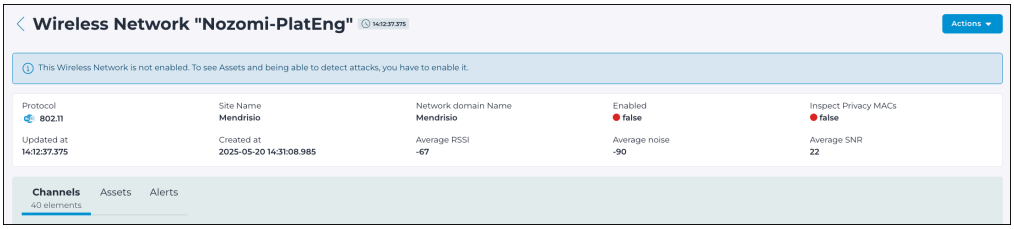


Figure 61. Details page

Actions dropdown

This dropdown gives you access to these actions:.

- Enable a wireless network (on page 157)
- Disable a wireless network (on page 158)
- Enable the inspection of devices with private MAC addresses (on page 159)
- Disable the inspection of devices with private MAC addresses (on page 160)
- Delete a wireless network (on page 161)

Actions menu

Enable a wireless network

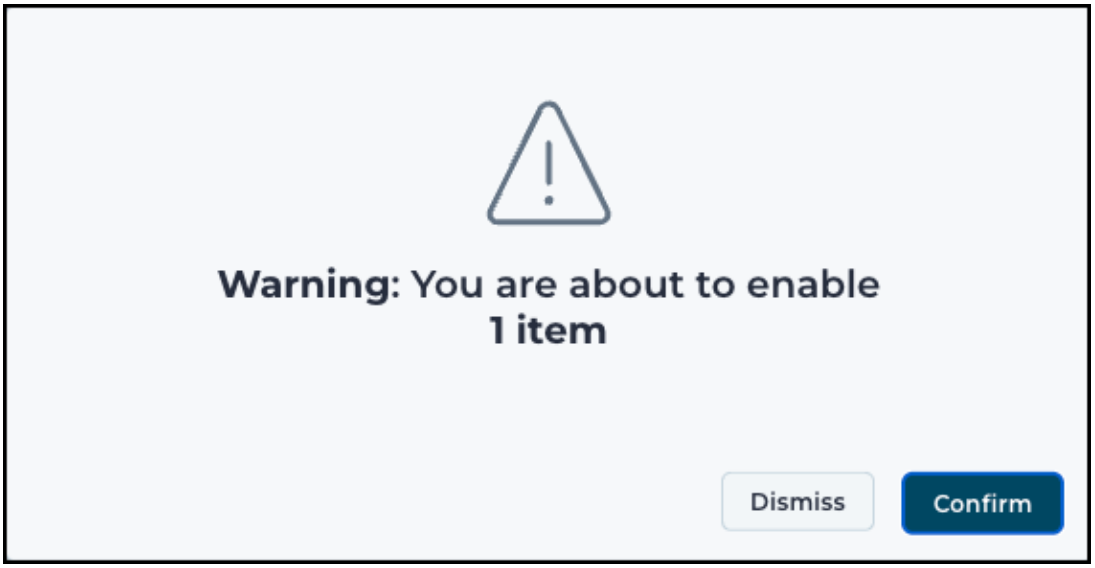
Do this procedure to enable a wireless network in Vantage to gather data such as: Assets, Alerts, Nodes, or Links.

Procedure

1. In the top navigation bar, select **Wireless**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Enable**.

   Result: A dialog shows.
5. Select **Confirm**.



6. Select **Close**.

Results

The wireless network(s) has (have) been enabled.

Disable a wireless network

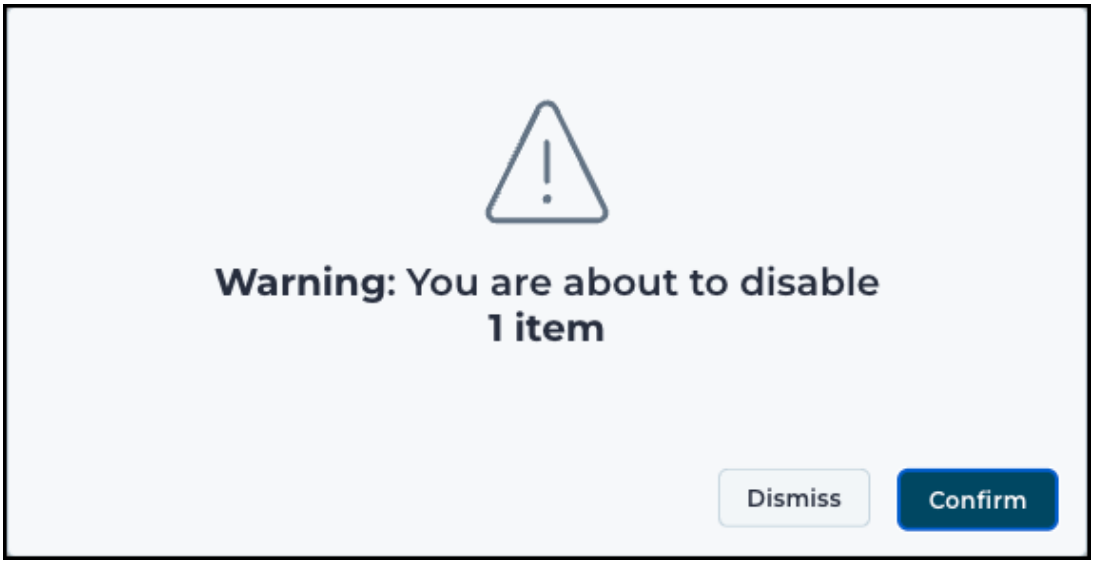
Disable a wireless network in Vantage to stop collecting data from selected assets, alerts, nodes, and links.

Procedure

1. In the top navigation bar, select **Wireless**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Disable**.

   Result: A dialog shows.
5. Select **Confirm**.



6. Select **Close**

Results

The wireless network(s) has (have) been disabled.

Enable the inspection of devices with private MAC addresses

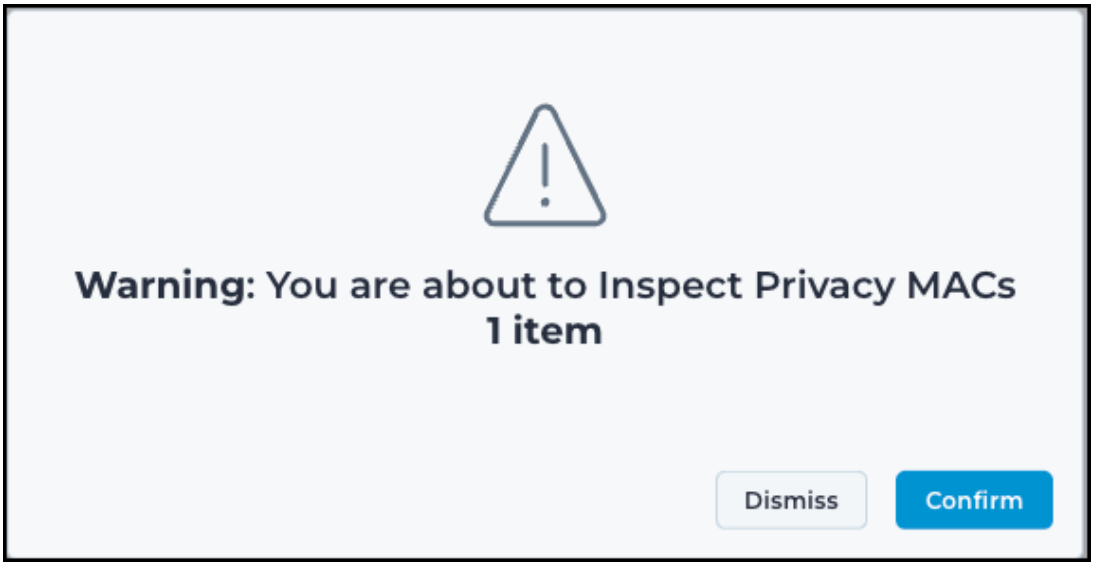
The **Inspect Privacy MACs** *function lets you also inspect devices with private MAC addresses.*

Procedure

1. In the top navigation bar, select **Wireless**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Inspect Privacy MACs**.

   Result: A dialog shows.
5. Select **Confirm**.



6. Select **Close**

Results

Private *MAC* addresses will now be inspected.

Disable the inspection of devices with private MAC addresses

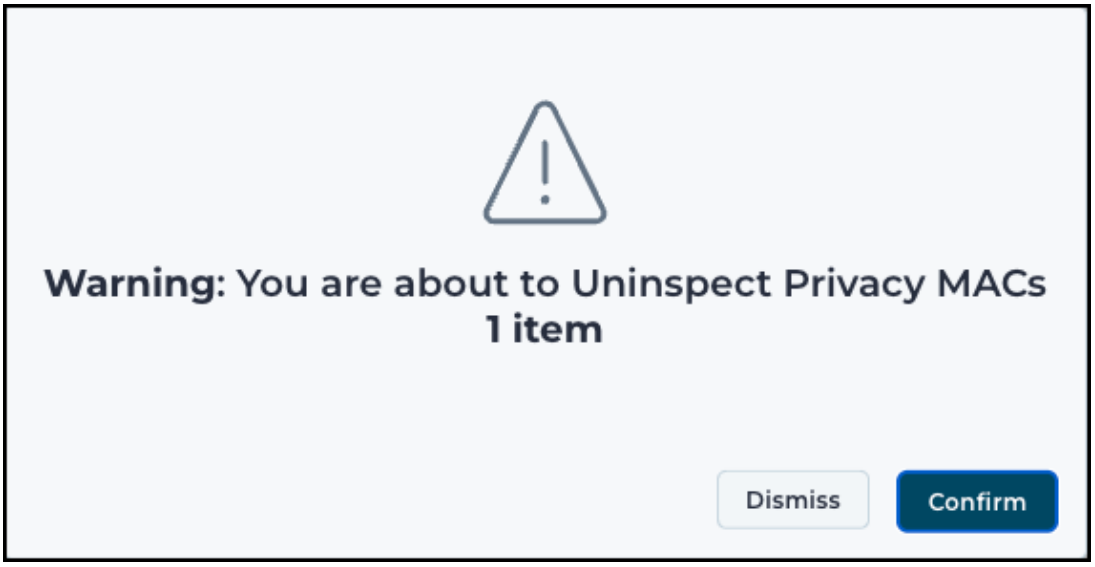
The **Uninspect Privacy MACs** *function disables the inspection of devices with private MAC addresses.*

Procedure

1. In the top navigation bar, select **Wireless**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Uninspect Privacy MACs**.

   Result: A dialog shows.
5. Select **Confirm**.



6. Select **Close**

Results

Private *MAC* addresses will no longer be inspected.

Delete a wireless network

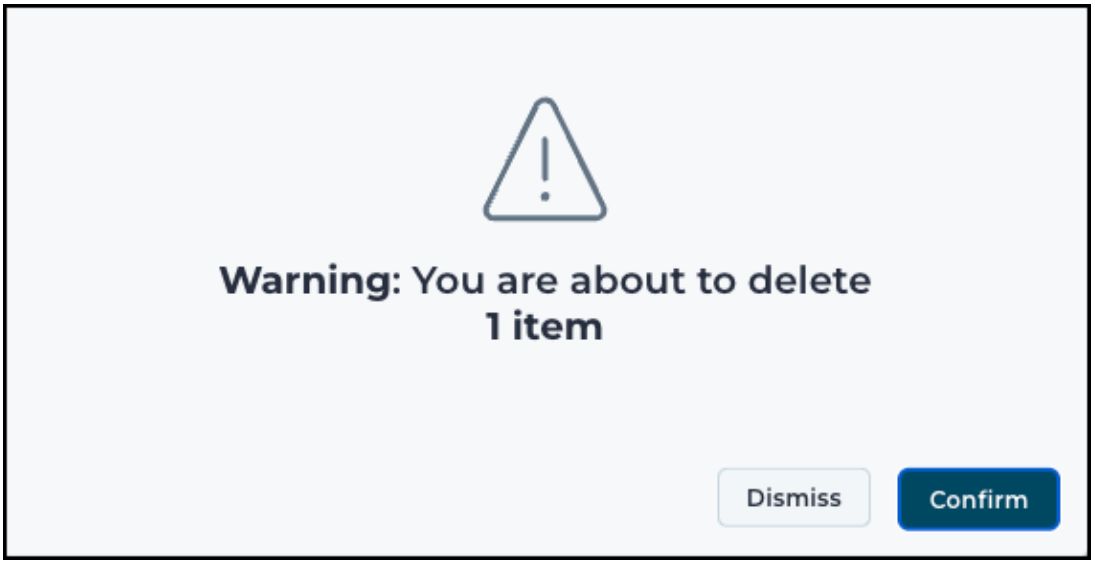
Delete a wireless network in Vantage to remove it from the system and stop all related data collection.

Procedure

1. In the top navigation bar, select **Wireless**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Delete**.

   Result: A dialog shows.
5. Select **Confirm** to delete the wireless network(s).



   Result: A dialog shows.
6. Select **Close**.

Results

The wireless network has been deleted.

Chapter 6. Queries

*The **Queries** page lets you write queries for your system. You can also save queries and assertions to be used again.*

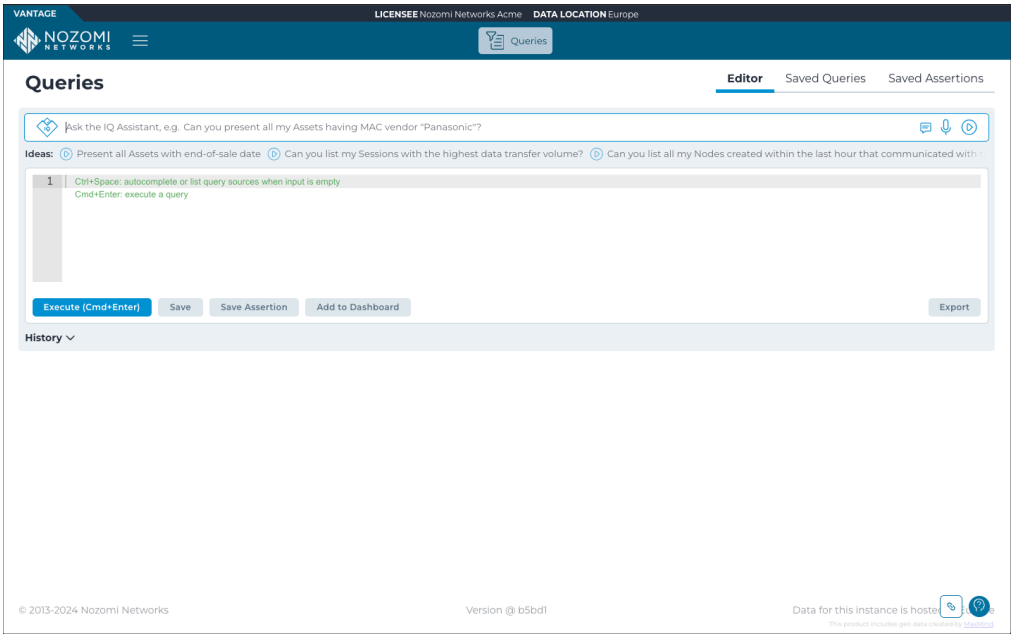


Figure 62. Queries page

The **Queries** page has these tabs:

- Editor (on page 166)
- Saved Queries (on page 168)
- Saved Assertions (on page 169)

Related information

Execute a query (on page 172)

Commands (on page 173)

Functions (on page 181)

Editor

*The **Editor** page lets you write queries for your system. When you query Vantage, the data it returns is based on the tables, fields, commands, and functions that you specify in the query text field.*

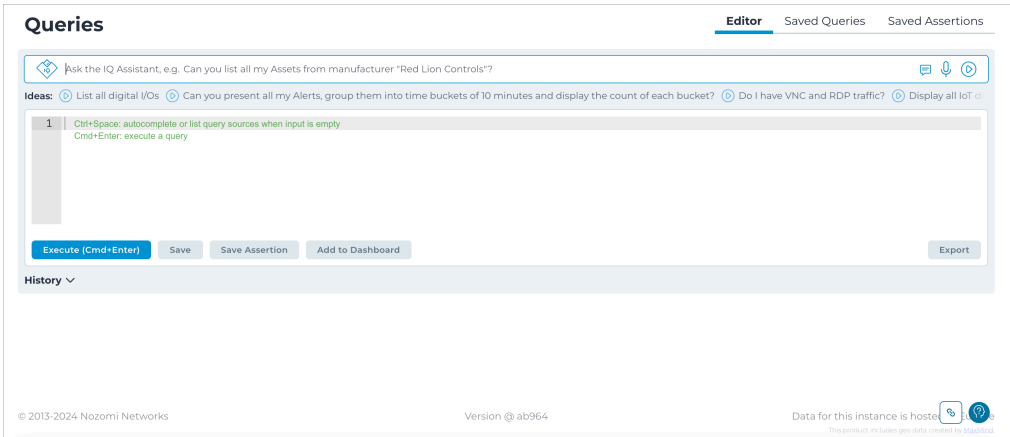


Figure 63. Editor page

This page lets you enter search queries and assertions and lets you save them for future use. You can also export them in Microsoft Excel or *comma-separated value (CSV)* format.

You can use the hashtag # symbol to enter a comment. For example:

```
asset_cpes # comment 1
| join assets asset_id id
# comment 2
| select cpe assets_name
| sort assets_name asc
```

Execute

This button lets you execute the query. Alternatively, you can use the keyboard shortcut `Cmd + Enter`.

Save

This button lets you save the current query.

Save Assertion

This button lets you save the current assertion. Once you have entered the details in the dialog and select **Save Assertion**, the assertion will show in the **Saved Assertions** page.

You can customize the assertion name and description using field values from your query. For more information, see Customize assertion name and description (on page 170).

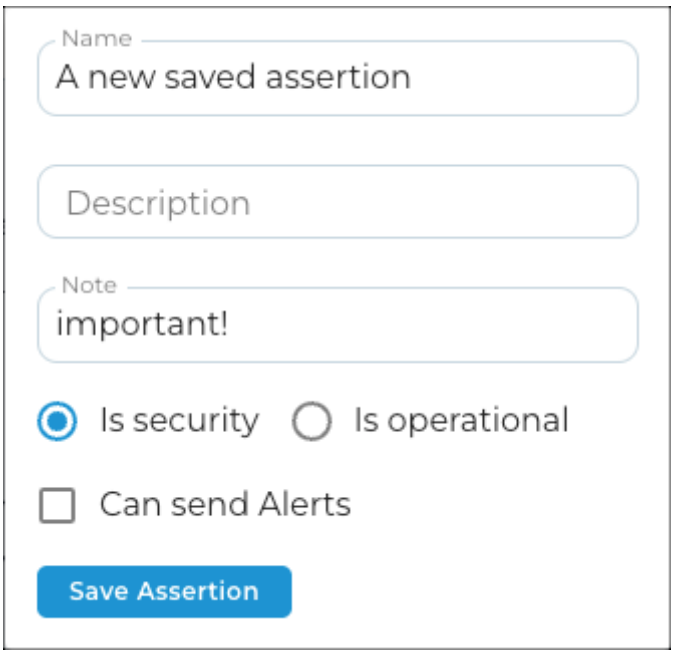


Figure 64. Save Assertion dialog

Add to Dashboard

This button lets you add a widget to a dashboard.

Export

This button lets you export the results in either *CSV* or Microsoft Excel format.

Saved Queries

*The **Saved Queries** page shows all the queries that have previously been saved.*

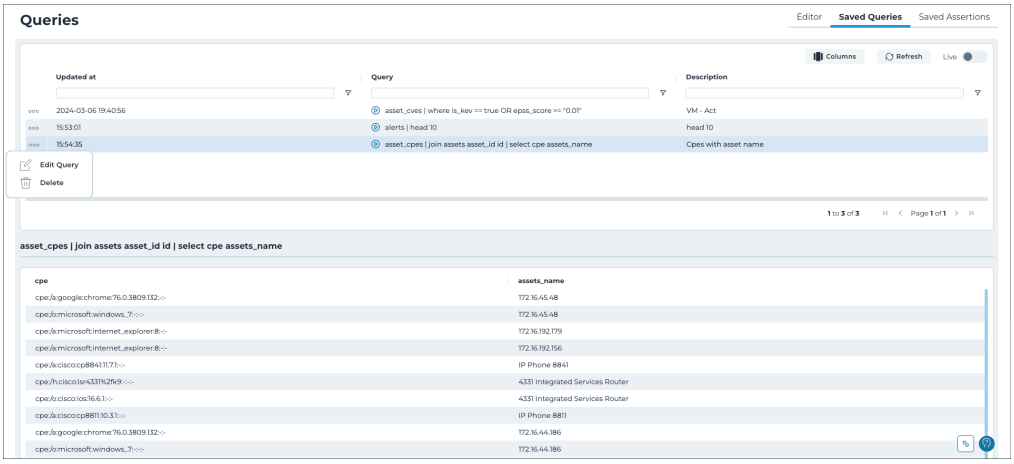


Figure 65. Saved Queries page

To run the applicable query, select the ▷ icon and the results will show in the pane below.

The actions menu has these options:

- **Edit Query**
- **Delete**

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Saved Assertions

*The **Saved Assertions** page shows all the assertions that have previously been saved.*

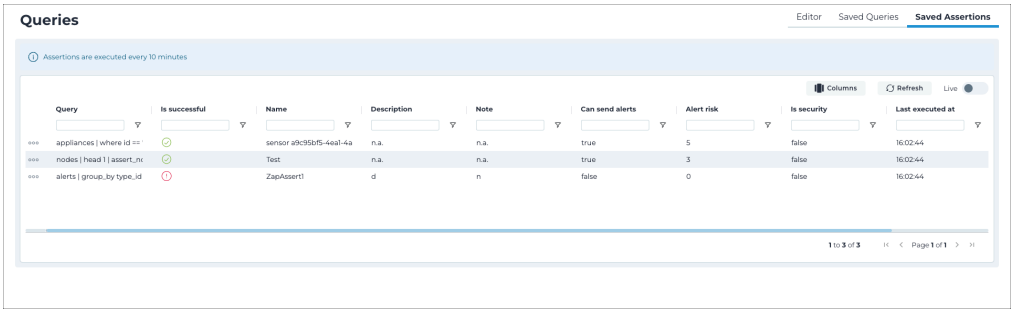


Figure 66. Saved Assertions page

The actions menu has these options:

- **Edit Query**
- **Delete**

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Customize assertion name and description

You can customize assertion names and descriptions with dynamic field values using string interpolation.

About this task

When saving an assertion, you can use field placeholders in the name and description fields. These placeholders are replaced with actual values from your query results when alerts are generated. This lets you create more descriptive and context-aware assertion names and alert descriptions.

Procedure

1. In the top navigation bar, select **Queries**.
2. Select **Editor**.
3. In the query field, enter your query.
4. Select **Execute** or press `Cmd + Enter`
5. Select **Save Assertion**.

   Result: The **Save Assertion** dialog opens.
6. In the **Name** field, enter a name for the assertion. To insert a field value from your query, select the plus icon button next to the field.

   Result: A placeholder `{{FIELD_NAME}}` is inserted into the field with `FIELD_NAME` highlighted. Replace it with the actual field name from your query.

   > **Tip:**
   > Field names must match the fields returned by your query. For example, if your query returns `host`, `name`, or `ip` fields, you can use `{{host}}`, `{{name}}`, or `{{ip}}`.
7. In the **Description** field, enter a description. You can also use field placeholders here by selecting the plus icon button.
   Example: `The sensor {{host}} with model {{model}} has been offline for more than 15 minutes`
8. Complete the remaining fields in the dialog.
9. Select **Save Assertion**.

Results

When the assertion generates an alert, the placeholders in the name and description are replaced with the actual values from the query results.

Example

If you save an assertion with the following configuration:

- Name: `Sensor offline: {{host}}`
- Description: `The sensor {{host}} with model {{model}} has not synchronized in the last 15 minutes`
- Query: `sensors | where minutes_ago(last_sync) > 15 | assert_empty`

When a sensor with `host` = `nozomi-guardian` and `model` = `V-SERIES` fails the assertion, the generated alert will display:

- Name: `Sensor offline: nozomi-guardian`
- Description: `The sensor nozomi-guardian with model V-SERIES has not synchronized in the last 15 minutes`

Execute a query

It is important to know how to execute a query correctly in Vantage.

About this task

Note:
Strings are always "quoted", otherwise they are interpreted as data fields. For example, you can write a query similar to `alerts | where closed_time > time` to compare two fields.

Note:
Use the `/` operator to navigate into *JavaScript Object Notation (JSON)* fields.

Note:
When you access a *JSON* sub field, occurrences of `/` are translated to `.` For example, `os:info/source` becomes `os:info.source` in the resulting dataset.

Procedure

1. In the top navigation bar, select **Queries**.
2. Choose a method to show the available data sources.

   Choose from:
   - In the Query text field, select **Ctrl+Space**.
   - In the Query text field, enter the first few letters of a data source.

   Result: A list of available data sources shows.
3. Enter your query.
4. Select **Execute (Cmd+Enter)**.

   Result: The results of your query show.
5. If necessary, select **Save** to save the query for future use.
6. If necessary, select **Save Assertion** to save the assertion for future use.
7. If necessary, select **Export** and choose **Excel** or **CSV** as an export format.

Commands

A list of example query commands.

assert_empty

Description: `assert_empty` will be rendered as a green or red bar and can be used to express conditions that need to be verified in the Vantage dataset.

Examples:

```
links | where protocol == "telnet" | assert_empty
```

assert_not_empty

Description: `assert_not_empty` will be rendered as a green or red bar and can be used to express conditions that need to be verified in the Vantage dataset.

Examples:

```
links | where protocol == "iec104" | where
 minutes_ago(last_activity_time) < 5 | assert_not_empty
```

bucket

Usage: `bucket <field> <range>`

Description: `bucket` will interpret `field` as a numeric value and will group the data in multiples of range.

Examples:

```
alerts | bucket risk 3
```

column

Usage: `column <value_field> <count_field> [option]`

Description: `column` will render a column chart with `value_field` on the X axis and `count_field` on the Y axis.

Examples:

```
assets | group_by type | sort count desc | column type count
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`colors`: Change the color of a single point in the chart that matches the provided label.

Arguments are a sequence of labels and colors in hex format all separated by a comma.

Example: -colors:dns,7bc043,modbus,f37736,iec104,ee4035

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

count

Description: `count` returns the number of records in the dataset

Examples:

```
links | count
```

exclude

Usage: `exclude <field1> ... <fieldN>`

Description: `exclude` removes the specified fields from each record of the dataset.

Examples:

```
assets | exclude name zones nodes
```

expand

Usage: `expand <array_field>`

Description: Expands a record into multiple records where the original `array_field` is replaced by each single value in it.

Examples:

```
nodes | expand roles
```

gauge

Usage: `gauge <field> [min] [max] [option]`

Description: Outputs a numeric field drawn as a gauge from the first dataset row.

Examples:

```
alerts
| where time > days_ago(7)
| reduce risk avg
| gauge round(risk_avg) -stops:3,7bc043,6,f37736,10,ee4035
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

grid

Usage: `grid <cols> <field1> ... <fieldN> [option]`

Description: Outputs a grid with `cols` columns with the specified fields in every cell.

Examples:

```
alerts | group_by type_id | grid 4 type_id count
```

```
sites | group_by country avg(risk) | grid 4 country avg_risk
 -stops:3,7bc043,7,f37736,10,ee4035
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`colors`: Change the color of a single point in the chart that matches the provided label.

Arguments are a sequence of labels and colors in hex format all separated by a comma.

Example: -colors:dns,7bc043,modbus,f37736,iec104,ee4035

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

group_by

Usage: `group_by <field1> [sum(<field2>)|avg(<field2>)]`

Description: Groups the dataset by a field and calculates the count of each bucket. Optionally sum and avg (average) can be calculated for some other numeric fields.

Examples:

```
alerts | group_by type_id avg(risk) avg(severity) sum(risk)
```

```
nodes | group_by type
```

head

Usage: `head [N]`

Description: Takes the first `N` records from the dataset, if `N` is not specified takes the first 10 records.

Examples:

```
assets | head
```

```
alerts | head 200
```

history

Usage: `history <value_field> <count_field> [option]`

Description: `history` will render a line chart with `value_field` on the X axis and `count_field` on the Y axis.

Examples:

```
alerts
| where time > days_ago(7)
| bucket time 3600000
| select bucket count
| sort bucket asc
| history bucket count
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`colors`: Change the color of a single point in the chart that matches the provided label.

Arguments are a sequence of labels and colors in hex format all separated by a comma.

Example: -colors:dns,7bc043,modbus,f37736,iec104,ee4035

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

join

Usage: `join <external_table> <inner_field> <external_field>`

Description: Joins two tables to create a new dataset where `inner_table.inner_field` is equal to `external_table.external_field`. The resulting dataset has all the fields from `external_table` prefixed with the `<external_table>_` string. For example, a table joined with `assets` will contain the `assets_name` field. Joining the same table multiple times will produce columns prefixed with the `<external_table>_` repeated the same time the table is joined. For example, the query `links | join nodes from id | join nodes to id` will contain `nodes_id` and `nodes_nodes_id` columns.

Examples:

```
vulnerabilities | join assets asset_id id
```

```
links | join nodes from id | join nodes to id
```

```
nodes | join assets name name | join links ip from
```

pie

Usage: `pie <value_field> <count_field> [option]`

Description: Renders a pie chart where the name of each slice is `value_field` and the slice is proportional to `count_field`.

Examples:

```
assets | group_by type | sort count desc | pie type count
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`colors`: Change the color of a single point in the chart that matches the provided label.

Arguments are a sequence of labels and colors in hex format all separated by a comma.

Example: -colors:dns,7bc043,modbus,f37736,iec104,ee4035

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

reduce

Usage: `reduce <field> [sum|avg]`

Description: `reduce` aggregates a numeric `field` by using the `sum` or `avg` functions and outputs a single number.

Examples:

```
alerts | reduce risk avg
```

select

Usage: `select <field1> ... <fieldN> [option]`

Description: `select` gives the possibility to restrict the fields in the dataset, to rename fields with the `->` operator or to apply functions to fields.

Examples:

```
nodes | select name properties/http.server_version
```

```
nodes | select name->my_name
```

```
nodes | select days_ago(last_activity_time)
```

```
assets | select name tags -fit:width
```

Options:

`fit`: Choose how the table will fit the content, this option accepts two values:

`width`: the table will adapt to the width of the container, cells width will be equally distributed

`content`: the table will expand to fully show the content of every cell

Note: This option only has an effect only when used in the context of Dashboard/Report widgets.

sort

Usage: `sort <field> [asc|desc]`

Description: Sorts the dataset by a `field`. `asc` or `desc` can be specified to define the sorting order, by default the order is ascending.

Examples:

```
assets | sort level
```

```
alerts | sort risk desc
```

to_entity

Usage: `to_entity <target_entity>`

Description: `to_entity` allows you to visualize query results as a specific entity type, making results interactive and navigable. Each row in the result set is treated as an instance of `target_entity`, giving it a link to its detail page in the Vantage interface.

Examples:

```
assets | select id name | to_entity assets
```

```
node_cves
| join assets asset_id id
| where likelihood >= "0.8"
| select id cve score cwe_name assets_name
| sort score desc
| to_entity vulnerabilities
```

uniq

Usage: `uniq <field1> ... <fieldN>`

Description: Reduce the dataset by returning only the unique records by one or more fields.

Examples:

```
alerts | uniq type_id risk
```

value

Usage: `value <field> [option]`

Description: Outputs a numeric field as a big graphical number by taking it from the first row of the dataset.

Examples:

```
alerts | reduce risk avg | value round(risk_avg)
 -stops:3,7bc043,6,f37736,10,ee4035
```

Options:

`color`: Change the color of the whole chart. The color must be provided in hex format.

Example: -color:7bc043

`stops`: Change the color of chart items based on their value.

Arguments are a sequence of values and colors in hex format all separated by a comma.

The respective color is applied when the value is <= to the actual value in the chart.

Example: -stops:3,7bc043,6,f37736,10,ee4035

where

Usage: `where <field1> [[==|!=|>=|>|<|<=|include?|!include?|exclude?|start_with?|!start_with?|end_with?|!end_with?|in_subnet?|in?|!in?|in_zones?] <field2>]`

Description: Filters the dataset by a specified criterion. `field1` and `field2` can be strings, fields, numbers, or function calls.

Some operators are specific to certain data types:

- `in_subnet?` requires a subnet in *classless inter-domain routing (CIDR)* notation as the right operand.
- `in?` and `!in?` work with *JSON* arrays as the right operand.
- `include?`, `!include?`, `exclude?`, `start_with?`, `!start_with?`, `end_with?`, and `!end_with?` work with both single values and arrays as the right operand.
- `in_zones?` works with tiered zones and requires a tiered zone name as the right operand.

Pattern-matching operators (`include?`, `start_with?`, `end_with?`, and their negated variants) cast values to text and use SQL `LIKE`/`NOT LIKE`. They can be expensive on large datasets, so use them with care.

Examples:

```
nodes
| select name properties/http.server_version
| where !is_empty(properties.http.server_version)
```

```
nodes | where is_public
```

```
nodes | where ip in_subnet? "192.168.1.0/24"
```

```
nodes | where type in? ["computer","historian"]
```

```
nodes | where type == "computer" OR days_ago(last_activity_time) < 5
```

```
sensors | where !is_empty(tags)
```

```
nodes | join assets name name | where assets_tags include? "tag1"
```

```
nodes | where subnet include? ".17.26."
```

```
nodes | where subnet include? ["172.17.26.0/24","172.17.42.0/24"]
```

```
assets | where name start_with? "HP"
```

```
assets | where name start_with? ["HP", "Control"]
```

```
assets | where name !end_with? "top"
```

```
assets | where name !end_with? ["top", "gix"]
```

```
alerts | where zone_src in_zones? "GlobalTieredZone"
```

Functions

A list of example query functions.

cast

Usage: `cast(<field>,<type>)`

Description: Casts a field to the given type. Allowed types: integer (4 bytes integer), bigint (8 bytes integer), real (4 bytes floating point number), boolean, text, json.

Examples:

```
alerts | select cast(risk,"integer")
```

```
alerts | select cast(severity,"text")->severity_as_text
```

coalesce

Usage: `coalesce(<field1>,<field2>,...)`

Description: Takes a list of fields and literals and returns the first non-empty value.

Examples:

```
nodes | select coalesce(label,name,"fallback")
```

concat

Usage: `concat(<field1>,<field2>,...)`

Description: Returns the concatenations of a list of fields and literals interpreted as strings.

Examples:

```
nodes | select concat(label,"/",name)
```

days_ago

Usage: `days_ago(<field|number>)`

Description: Returns the difference in days between the timestamp `field` and the time of execution of the query. In the `where` clause the `days_ago(number)` syntax gives the best query performance.

Examples:

```
alerts | select days_ago(time)
```

```
alerts | where days_ago(time) < 20
```

```
alerts | where time >= days_ago(20)
```

dist

Usage: `dist(<field1>,<field2>)`

Description: Returns the difference between `field1` and `field2`. The fields can also be literals.

Examples:

```
nodes | select dist(sent.bytes,received.bytes)
```

div

Usage: `div(<field1>,<field2>)`

Description: Returns the result of the arithmetic division of `field1` by `field2`. The fields can also be literals.

Examples:

```
nodes | select div(last_activity_time,"1000")
```

floor

Usage: `floor(<field>)`

Description: Returns the greatest integer less than or equal to the provided field.

Examples:

```
alerts | reduce risk avg | select floor(risk_avg)
```

```
assets | select div(risk, "10") | select floor(div)
```

format_time

Usage: `format_time(<time_field>, [format_string])`

Description: Returns a string representation of the time field formatted according to the format string or the default formatting string ('YYYY-MM-DD HH24:MI:SS') if none is specified. Accepted format patterns are:

- YYYY: year, 4 digits
- MM: month number, 2 digits
- DD: day of month, 2 digits
- HH12: hour of day, 01-12
- HH24: hour of day, 00-23
- MI: minute, 00-59
- SS: second, 00-59

Characters that can be used as separators are: -, :, whitespace

Examples:

```
sessions | select format_time(last_activity_time)
```

```
sessions | where last_activity_time > days_ago(7) | select
 format_time(last_activity_time, "YYYY-MM-DD") | group_by formatted
```

hours_ago

Usage: `hours_ago(<field|number>)`

Description: Returns the difference in seconds between the timestamp `field` and the time of execution of the query. In the `where` clause the `hours_ago(<number>)` syntax gives the best query performance.

Examples:

```
alerts | select hours_ago(time)
```

```
alerts | where hours_ago(time) < 20
```

```
alerts | where time >= hours_ago(20)
```

ipv4

Usage: `ipv4(<field>)`

Description: Returns a non-empty value if the field argument is an IPv4.

Examples:

```
nodes | select ipv4(ip)
```

```
nodes | where ipv4(ip) != ""
```

ipv6

Usage: `ipv6(<field>)`

Description: Returns a non-empty value if the field argument is an IPv6.

Examples:

```
nodes | select ipv6(ip)
```

```
nodes | where ipv6(ip) != ""
```

is_empty

Usage: `is_empty(<field>)`

Description: Returns true if the field is an empty string or array, false otherwise.

Examples:

```
nodes | where !is_empty(label)
```

```
nodes | select protocols is_empty(protocols)
```

is_recent

Usage: `is_recent(<field>)`

Description: Returns true if `field` represents a time in the last 30 minutes, false otherwise.

Examples:

```
alerts | where is_recent(time)
```

minutes_ago

Usage: `minutes_ago(<field|number>)`

Description: Returns the difference in minutes between the timestamp `field` and the time of execution of the query. In the `where` clause the `minutes_ago(<number>)` syntax gives the best query performance.

Examples:

```
alerts | select minutes_ago(time)
```

```
alerts | where minutes_ago(time) < 20
```

```
alerts | where time >= minutes_ago(20)
```

mult

Usage: `mult(<field1>,<field2>,...)`

Description: Multiplies the fields or literal values in the arguments list.

Examples:

```
alerts | select mult(risk,"10")
```

parse

Usage: `parse(<field>,<regex>)`

Description: Extracts a new field from an existing field by leveraging a POSIX regular expression. The new field will have the value of the portion of text that matches the regular expression, if the regular expression contains parentheses the return value will be the portion of text matching the regular expression inside the parentheses.

Examples:

```
assets | select
 parse(properties,".sysDescr\.0.:\s.([a-zA-Z0-9\-\.\s]+).")->sysDescr
```

```
assets | select parse(name, "\d+")->number
```

round

Usage: `round(<field>,[<decimal_places>])`

Description: Rounds a number at the given `decimal_places`. If `decimal_places` is not specified the number will be rounded to the closer integer.

Examples:

```
alerts | reduce risk avg | select round(risk_avg,3)
```

```
alerts | reduce risk avg | select round(risk_avg)
```

seconds_ago

Usage: `seconds_ago(<field|number>)`

Description: Returns the difference in seconds between the timestamp `field` and the time of execution of the query. In the `where` clause the `seconds_ago(<number>)` syntax gives the best query performance.

Examples:

```
alerts | select seconds_ago(time)
```

```
alerts | where seconds_ago(time) < 20
```

```
alerts | where time >= seconds_ago(20)
```

size

Usage: `size(<array_field>)`

Description: Returns the size of the `array_field`.

Examples:

```
nodes | where size(roles) > 1
```

split

Usage: `split(<field>,<splitter_string>,<index>)`

Description: Splits the value of `field` by `splitter_string` and returns the item at the `index` position, where `index` starts at 1.

Examples:

```
nodes | select split(mac_address,":",1)
```

to_epoch

Usage: `to_epoch(<timestamp_field>)`

Description: Converts a timestamp field into the numeric version suitable for queries.

Examples:

```
wireless_networks | bucket to_epoch(created_at) 3600000
```

to_time

Usage: `to_time(<field>|<ISO8601_datetime_string>)`

Description: Converts a time field, or an ISO-8601 datetime string, into the numeric timestamp (epoch milliseconds) used by time fields and other time-related functions. If the datetime string does not specify a UTC offset, it is assumed to be UTC.

Examples:

```
alerts | select to_time(time)
```

```
alerts | where time >= to_time("2024-01-15T10:30:00Z")
```

```
alerts | where time >= to_time("2024-01-15T10:30:00+02:00")
```

Chapter 7. Vulnerabilities

*The **Vulnerabilities** page shows a list of all the vulnerabilities that Vantage has detected in your system. Vulnerabilities are weaknesses that reduce the security of your system and give threat actors an opportunity to exploit your system.*

Figure 67. Vulnerabilities page

The Vulnerabilities page has these tabs:

- Overview (on page 190)
- Detailed list (on page 192)
- Workbooks (on page 201)

Related information

Resolve a vulnerability (on page 199)

Export a vulnerability (on page 197)

Overview

*The **Overview** page provides a comprehensive summary of the system's vulnerability landscape, helping you prioritize risk mitigation efforts.*

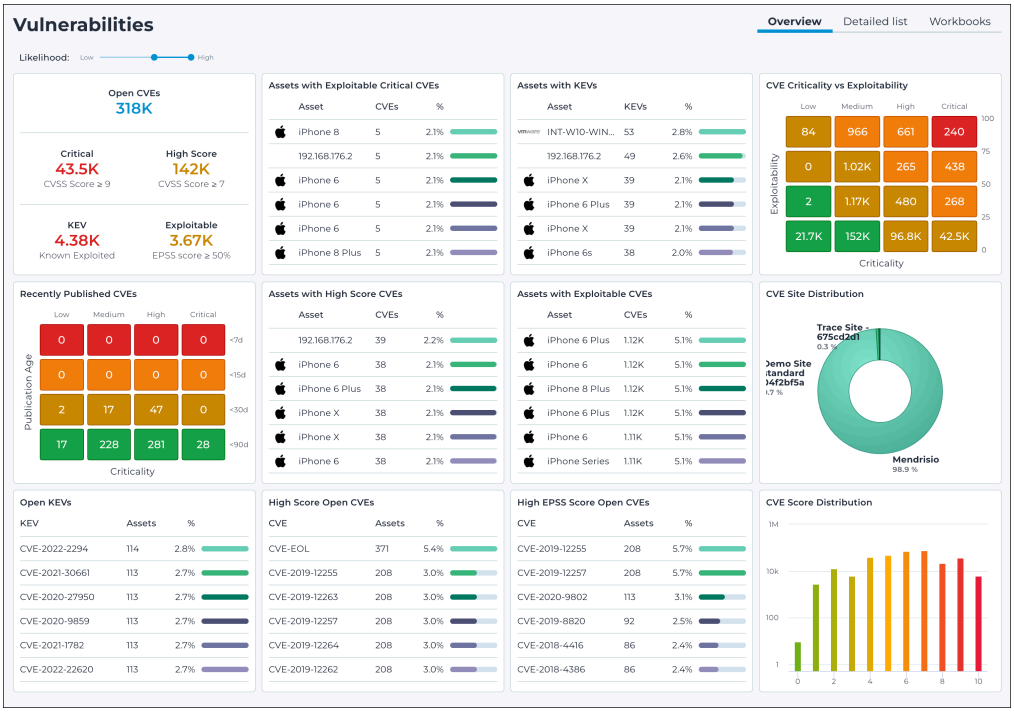


Figure 68. Overview page

Likelihood

The **Likelihood** slider allows you to adjust the risk threshold, helping you focus on vulnerabilities most likely to be exploited.

Open CVEs

See the total number of known *CVE* affecting assets in the system.

Assets with Exploitable Critical CVEs

Lists assets that have known *CVE*s with active exploits in the wild.

Assets with KEVs

Highlights assets impacted by *Known Exploited Vulnerabilities (KEV)*.

CVE Criticality vs Exploitability

Provides a visual representation of *CVE*s categorized by their severity and likelihood of exploitation.

Recently Published CVEs

Displays a grid of newly published *CVE*s categorized by severity and publication age.

Assets with High Score CVEs
Shows assets affected by *CVEs* with a high *Common Vulnerability Scoring System (CVSS)* score, indicating high risk.

Assets with Exploitable CVEs
Identifies assets with *CVEs* that have known exploitability indicators.

CVE Site Distribution
Displays how *CVEs* are distributed across different monitored sites.

Open KEVs
Lists vulnerabilities that have been publicly disclosed as *KEVs*.

High Score Open KEVs
Displays *KEVs* that have high severity scores.

High EPSS Score Open KEVs
Lists vulnerabilities with a high *Exploit Prediction Scoring System (EPSS)* scores, indicating a high probability of real-world exploitation.

CVE Score Distribution
Use the distribution graph to analyze *CVE* severity scores and assess overall risk exposure.

Detailed list

*The **Detailed list** page shows a list of all the vulnerabilities and their related details.*

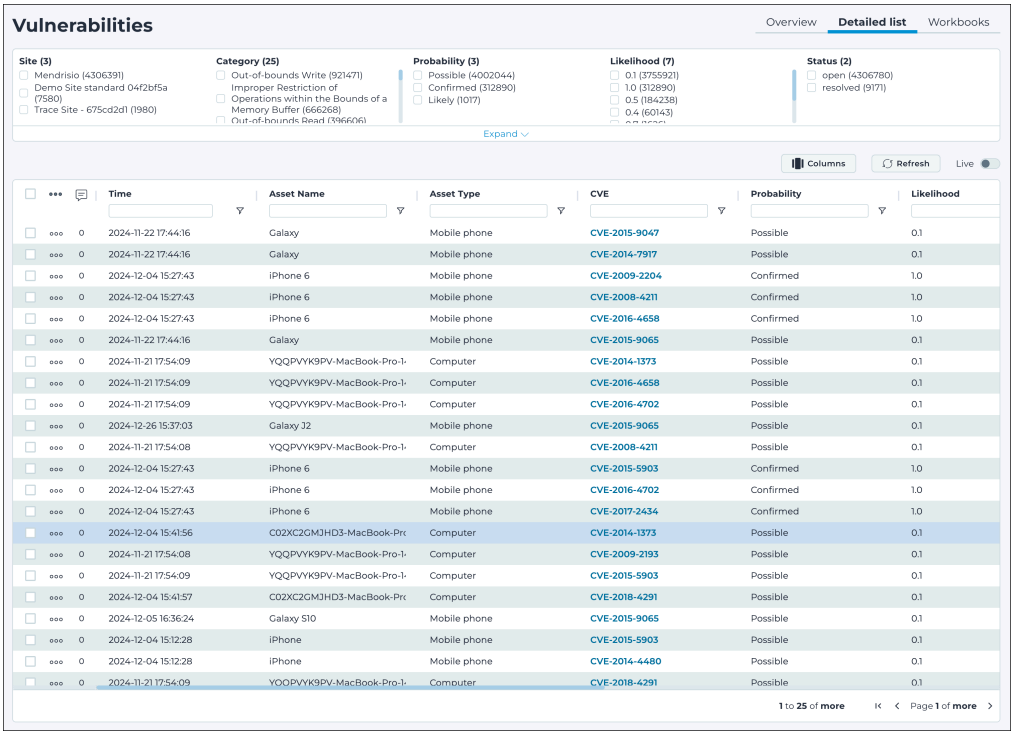


Figure 69. Detailed list page

Site

This shows a list of all the sites that are applicable for the vulnerabilities in the current table view.

Category

This shows a list of all the different categories that are applicable for the vulnerabilities in the current table view.

Probability

This shows a list of the different probabilities that have been confirmed for all the vulnerabilities in the current table view. When a vulnerability is not confirmed, it will show as **Possible**.

Likelihood

This shows a list of the different likelihoods that are applicable for the vulnerabilities in the current table view. This is a numerical assessment of the possibility that this vulnerability exists on an asset. It is measured on a scale from 0.1 to 1.0, where 1.0 is the most likely.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Details page

The details page shows a set of fields which are applicable to the related type of vulnerability.

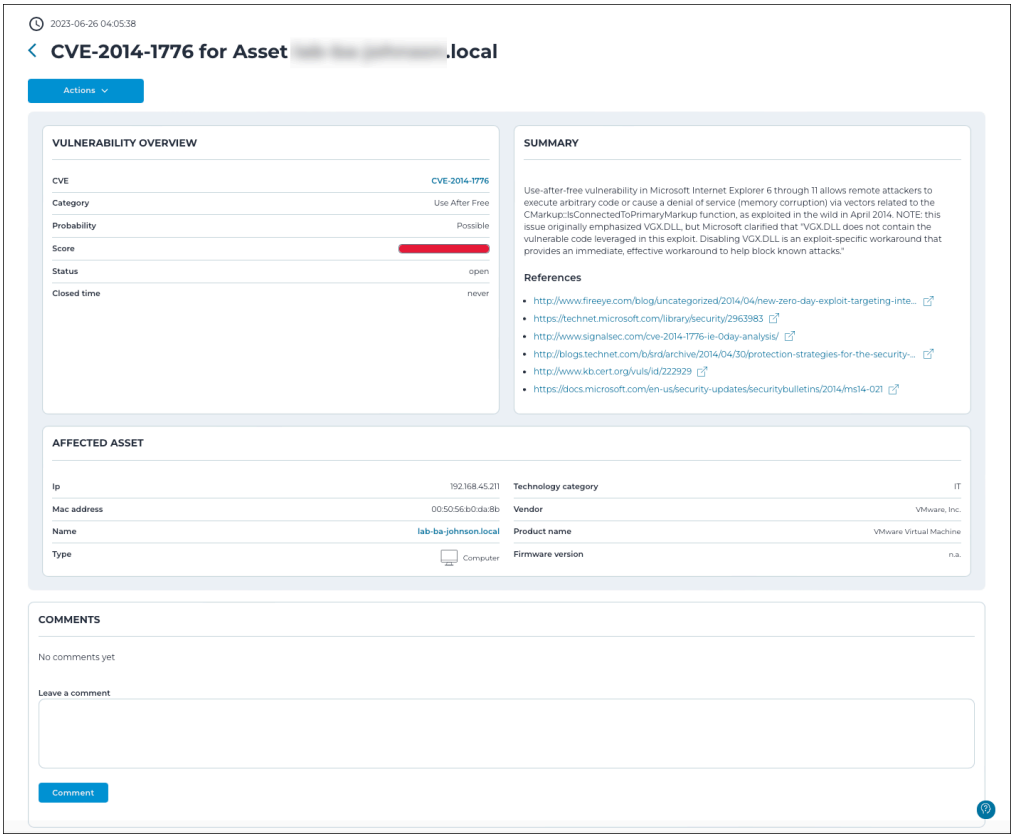


Figure 70. Details page

Actions dropdown

This dropdown gives you access to the action: Resolve Vulnerability (on page 199).

Vulnerability Overview

This section shows overview details for the related vulnerability.

Summary

This section shows a summary of information for the related vulnerability.

Affected Asset

This section shows this information for the affected asset:

- ip
- Mac address
- Name
- Type
- Technology category
- Vendor
- Product name
- Firmware version

Comments

This section lets you leave a comment, or read a comment that has been written, for the related vulnerability.

Summary drawer

When you double-click a sensor in the table, the summary drawer shows. This lets you post a comment, or open the related details page.

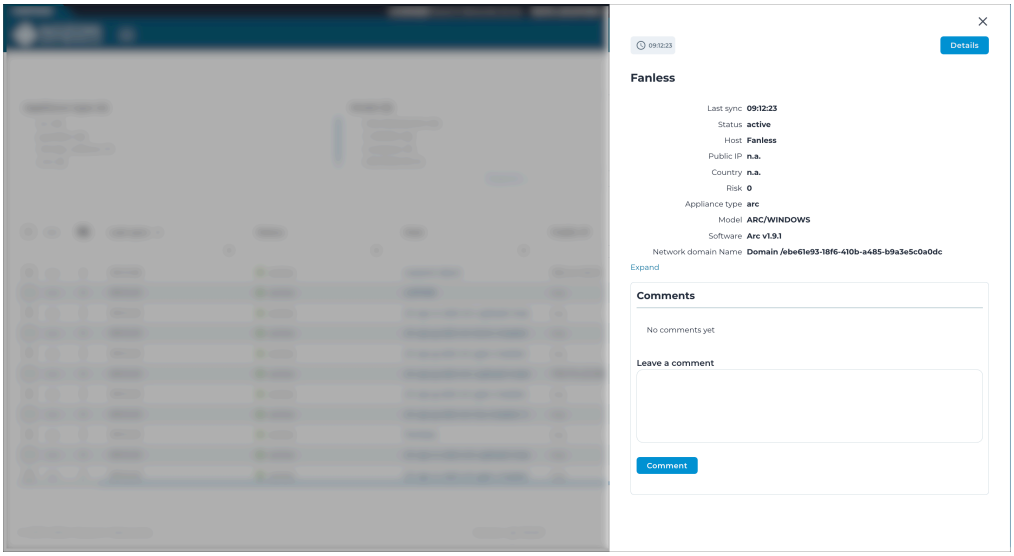


Figure 71. Summary drawer

Details button

You can select the **Details** button to open the details page for the related item.

Summary

The summary section shows a summary of applicable information for the related item.

Comments

This section lets you leave a comment, or read a comment that has been written, for the related item.

Table interactions

Actions menu

Export a vulnerability

You can use the actions menu to export one or more vulnerabilities to a spreadsheet.

Procedure

1. In the top navigation bar, select **Vulnerabilities**.
2. Choose a method to open the actions menu.

   Choose from:

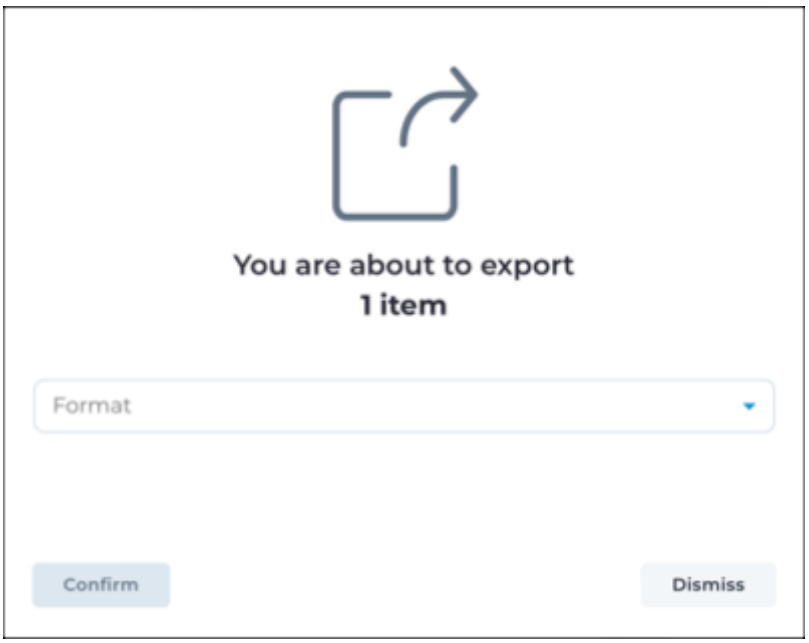
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Export**.

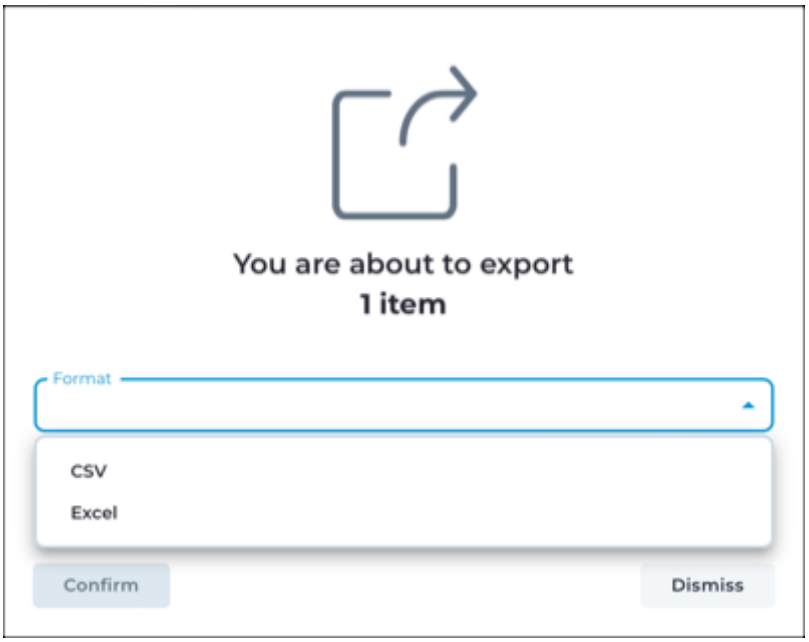


   Result: The export dialog shows.

5. Select the **Format** dropdown.

   Result: A dialog shows.

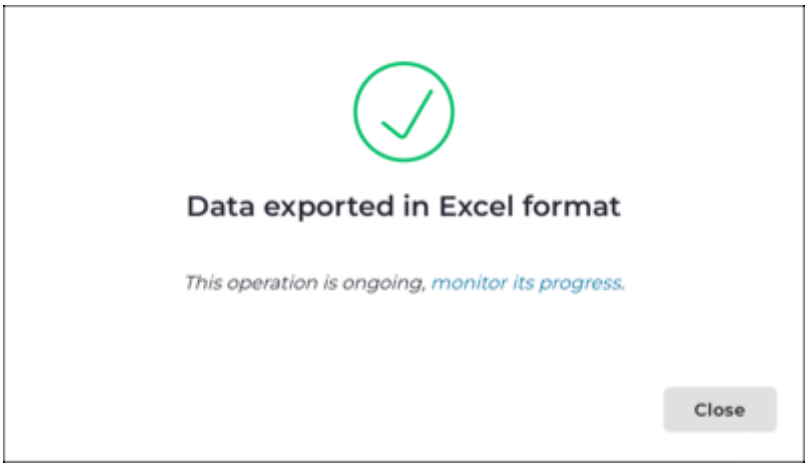
6. In the **Format** dropdown, select the format that you want to export.



7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.



Results

The vulnerability has been exported.

Resolve a vulnerability

You can use the actions menu to resolve one or more vulnerabilities.

Procedure

1. In the top navigation bar, select **Vulnerabilities**.
2. Choose a method to open the actions menu.

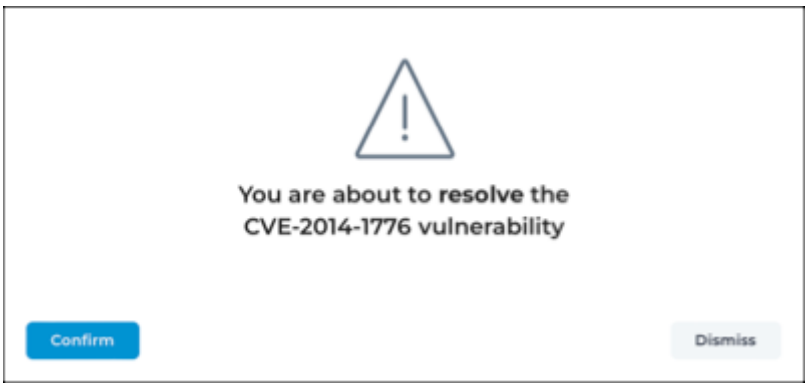
   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon
3. If you use the ••• icon in the table, choose a method to select one, or more, items.

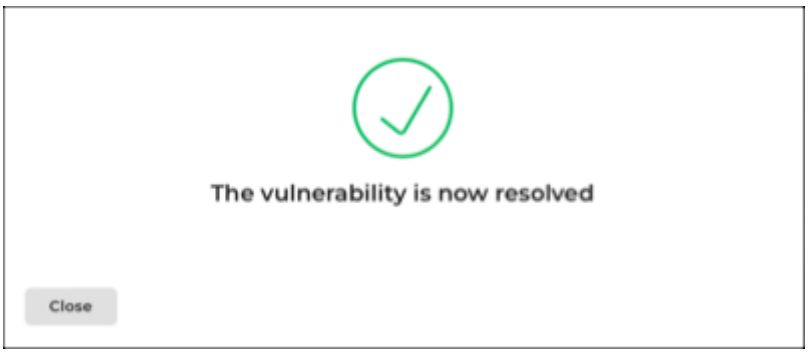
   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
4. Select **Resolve Vulnerability**.

   Result: A dialog shows.
5. Select **Confirm**.



   Result: A dialog shows.
6. Select **Close**.



Results

The vulnerability has been resolved.

Workbooks

*The **Workbooks** page shows recommended courses of action that can improve your network security. Generated through machine learning, workbooks highlight the vulnerabilities currently creating the highest risk exposure.*

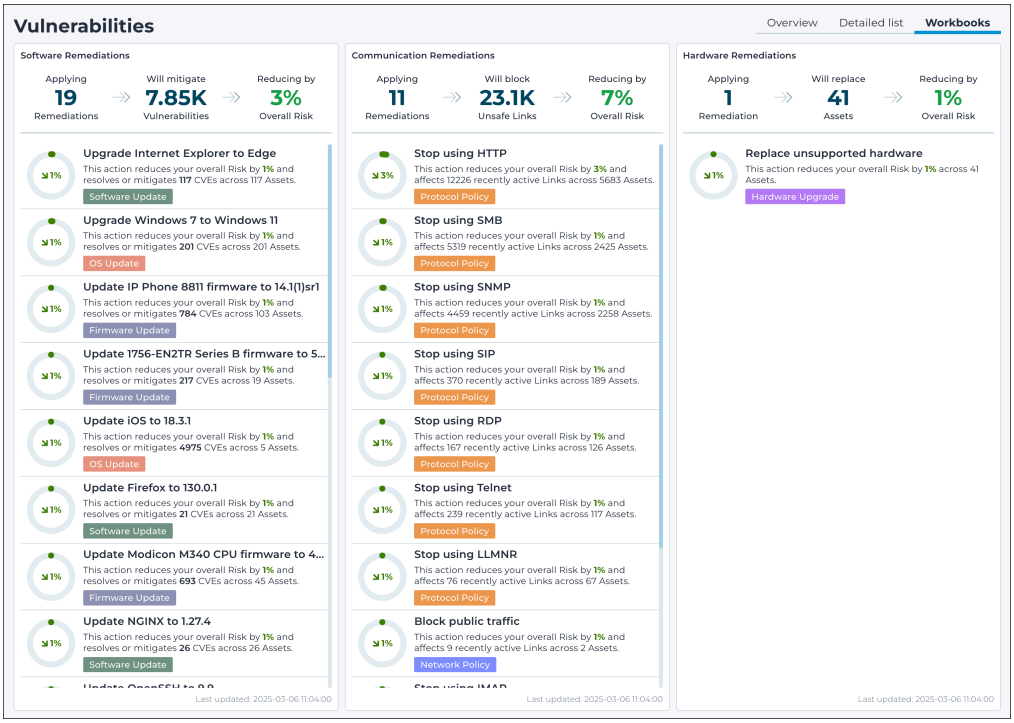


Figure 72. Workbooks page

Banner image

The banner image is a powerful visual report that uses bubble graphics to represent the relative impact of each workbook recommendation.

List

The list shows ranked recommendations, with the most effective actions at the top. For each workbook, Vantage shows:

- On the left, the highest risk score among all the vulnerabilities included in the workbook.
- A title that shows the recommended course of action.
- A description of the issue and the benefits of addressing it.
- In the top right corner of each workbook, Vantage shows:
  - An assessment of the risk reduction you will achieve if you follow the recommended steps. It is shown as a percentage.
  - The number of assets where the vulnerability was detected.
  - The number of *CVE* that you would address if you follow the recommended steps.

Related information

Use a workbook to improve your network security (on page 296)

Chapter 8. Vantage IQ

Vantage IQ helps you navigate and explore your network. You can use smart query commands to leverage advanced machine learning and data analytic algorithms to dive deeper into your data.

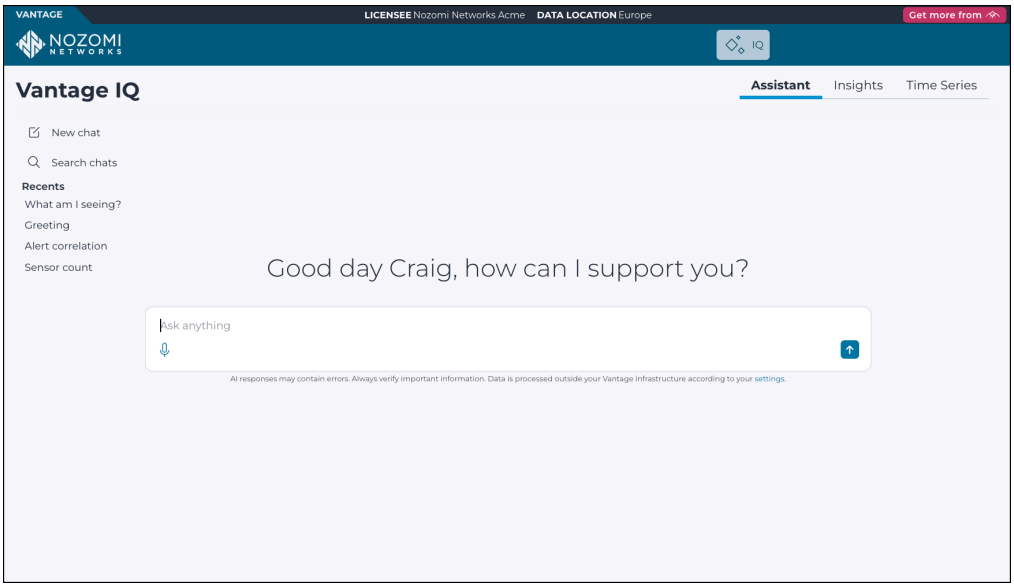


Figure 73. Vantage IQ page

Vantage IQ replicates the learned experiences of seasoned security analysts and automates tasks. Vantage IQ automatically:

- Reviews data
- Correlates data
- Prioritizes tasks

The dashboard shows the most recent insights. Vantage IQ uses the security level of each insight to prioritize them. When you select an individual insight, it shows the related details.

The **Vantage IQ** page has these tabs:

- Assistant (on page 211)
- Insights (on page 217)
- Time Series (on page 222)

You can also access the assistant from any page using the IQ assistant widget (on page 207). The widget appears as an animated icon in the top navigation bar and lets you query the assistant in context without navigating to the **IQ** page.

Requirements

Most Vantage IQ features require a Vantage IQ license; limited IQ summaries are available without a license.

Vantage IQ is a subscription service. Most Vantage IQ features require an active Vantage IQ license. If your organization does not have a Vantage IQ license, most **IQ** pages show the following message, while IQ summaries remain available with limited functionality:

Vantage IQ is a subscription service. Contact your account manager to enable it.

Contact your account manager to activate a Vantage IQ subscription for your organization.

IQ assistant widget

The IQ assistant widget gives you access to the Vantage IQ assistant from any page, without leaving your current view.

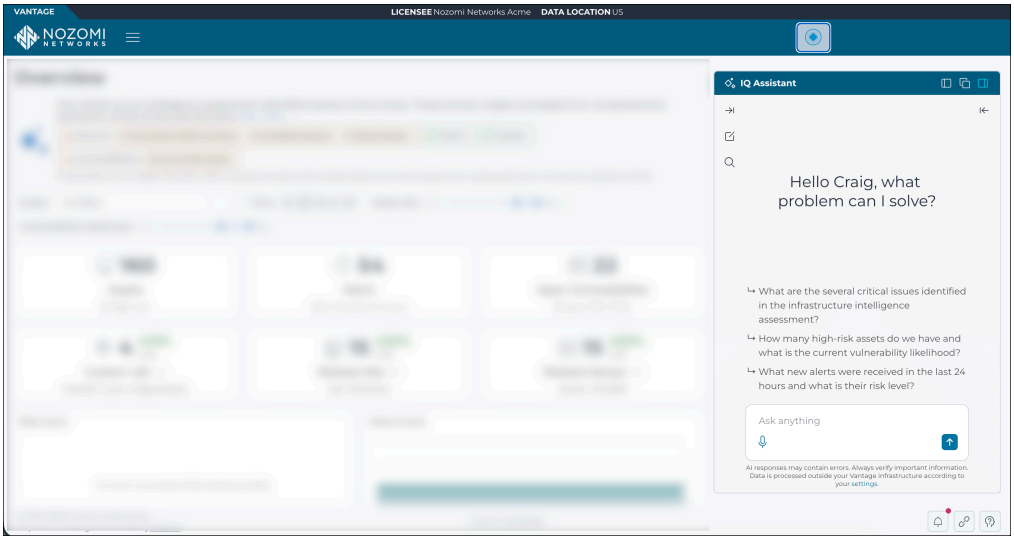


Figure 74. IQ assistant widget open and docked to the right

The IQ assistant widget appears as the icon in the top navigation bar. It is available on every page except the **IQ** page when you have a Vantage IQ license or are on a trial. The widget opens a panel where you can query the assistant and review results without navigating away from your current page.

> **Note:**
> The IQ assistant widget requires a Vantage IQ license or an active trial. If your organization does not have a license, the widget does not appear.

Sidebar

The widget panel has a collapsible sidebar on the left. Select the collapse arrow at the top of the sidebar to hide it and maximize the chat area. Select the expand arrow to show it again.

The sidebar contains these controls:

- **New chat**: Starts a new conversation with the assistant.
- **Search chats**: Opens a list of your previous chats so you can return to an earlier conversation.

To close the widget, select the icon again. The next time you open it, it returns to the same display mode and position.

Display modes

You can display the widget in three modes:

- **Docked right**: The panel attaches to the right side of the screen.
- **Docked left**: The panel attaches to the left side of the screen.
- **Detached**: The panel floats freely. You can move and resize it.

The widget remembers your last display mode and position when you close it and reopen it.

Page awareness

The widget is page-aware. When you open it, the assistant analyzes the data on your current page and suggests relevant questions. When you navigate to a different page, the assistant reanalyzes the data for that page and updates the suggested questions.

For example, if you open the widget on the **Assets** page, the assistant suggests questions about your assets. If you then navigate to the **Alerts** page, it suggests questions about your alerts. This lets you query data in context without copying identifiers or switching between tabs.

Behavior on the IQ page

The widget is not available on the **IQ** page because the full assistant is already present there. When you navigate to the **IQ** page, the widget automatically hides. When you navigate away from the **IQ** page, the widget reappears in its previous state.

Related information

Assistant (on page 211)

Open the IQ assistant widget (on page 209)

Open the IQ assistant widget

Open the IQ assistant widget to query the assistant from any page without leaving your current view.

Before you begin

Make sure that you have a Vantage IQ license or an active trial.

Procedure

1. In the top navigation bar, select the icon.

   Result:

   The IQ assistant widget panel opens. The assistant analyzes the current page and shows suggested questions.

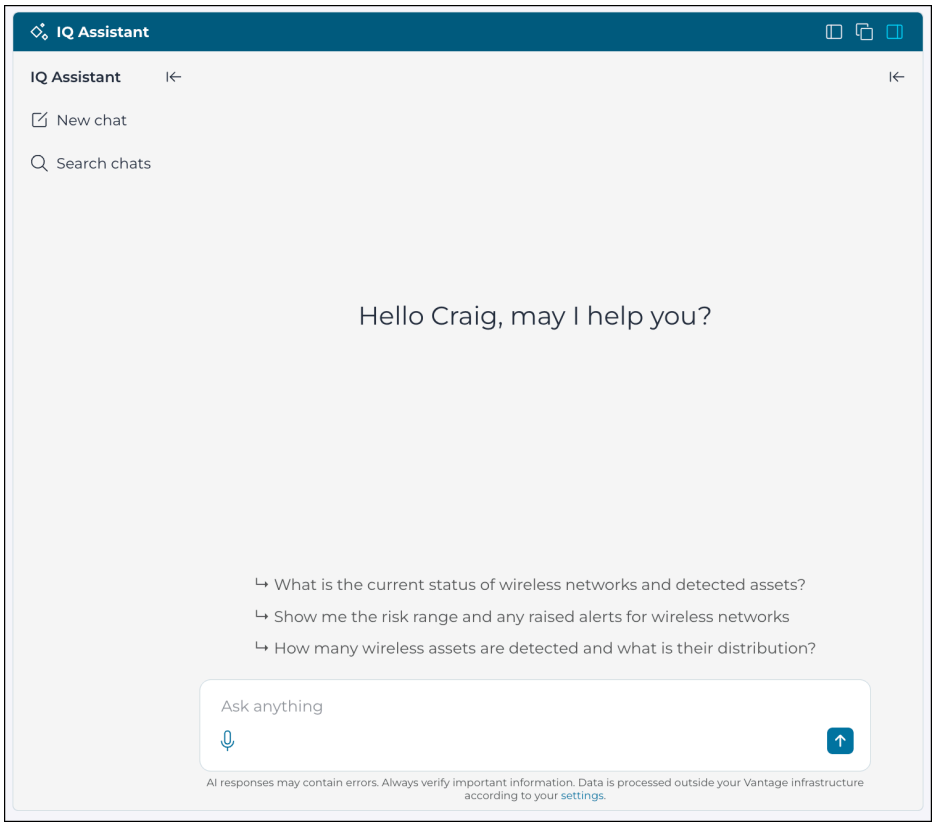


Figure 75. IQ assistant widget panel

2. **Optional:** To change the display mode, select the dock or detach icon in the widget panel header.

Related information

IQ assistant widget (on page 207)

Assistant (on page 211)

Close the IQ assistant widget

Close the IQ assistant widget to dismiss the panel by selecting its icon again. The widget reopens in the same display mode and position the next time you open it.

Procedure

In the top navigation bar, select the icon.

Result: The widget panel closes. Your display mode and position are saved for the next time you open the widget.

Related information

IQ assistant widget (on page 207)

Open the IQ assistant widget (on page 209)

Assistant

*The **Assistant** page lets you ask questions about your environment. The Vantage IQ assistant uses AI that is connected to your Vantage instance.*

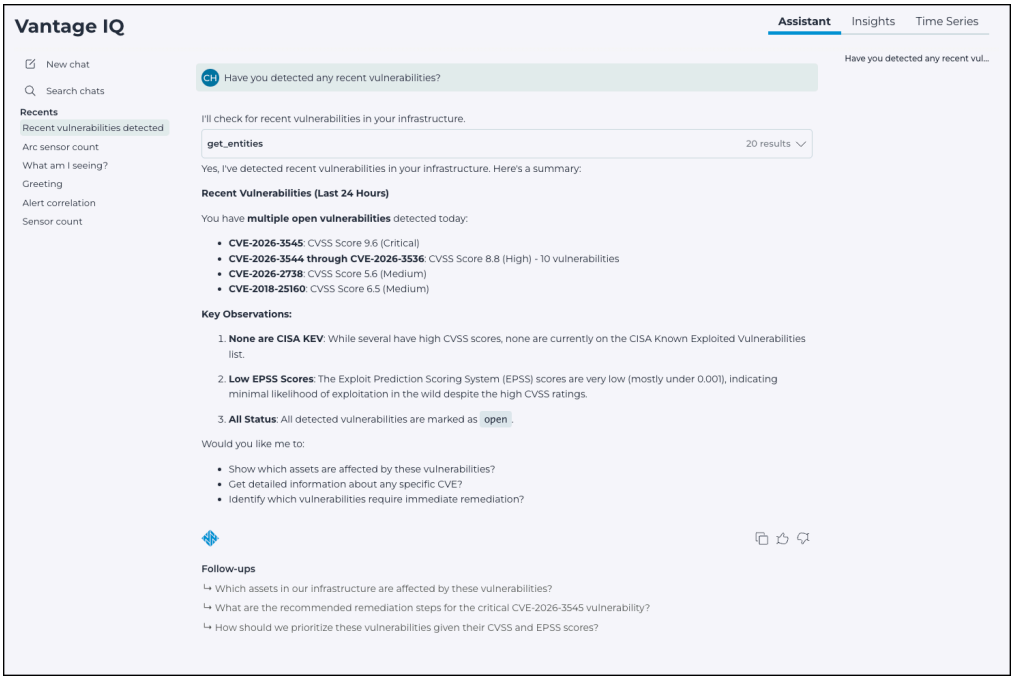


Figure 76. Assistant tab

The assistant lets you query your Vantage instance using natural language. It connects to your Vantage data in real time and returns results as tables, charts, or summaries depending on the query.

Chats

Each session in the assistant is a chat. The assistant saves chats automatically so you can return to them later. You can:

- Start a new chat from the assistant page
- View and reopen previous chats using **Search chats**
- Rename a chat to make it easier to find
- Delete a chat when it is no longer needed

The assistant generates chat titles automatically based on your first query. You can rename a chat at any time.

Response controls

Each assistant response includes three icons:

- copies the response text to the clipboard
- marks the response as useful
- marks the response as not useful

Use the thumbs up and thumbs down icons to rate responses and help improve result quality.

Follow-ups

When available, the assistant shows a set of suggested follow-up questions under **Follow-ups**. Select a suggested question to send it as your next query.

Data processing and privacy

Some assistant features rely on external processing of your prompts. You can disable external processing from the **Features** page. If you disable it, some assistant features will not be available.

When the assistant uses external processing:

- Nozomi Networks completely anonymizes your data before sending it for processing
- Nozomi Networks has a no-retention policy with its third-party processors. The third-party processor processes but never stores your data

Important:

Your data is never used to train any *AI* model, whether processing is internal or external. All models only perform processing of your data.

Start a new chat

*Start a new chat in the **Assistant** to ask questions about your environment without affecting your previous chats.*

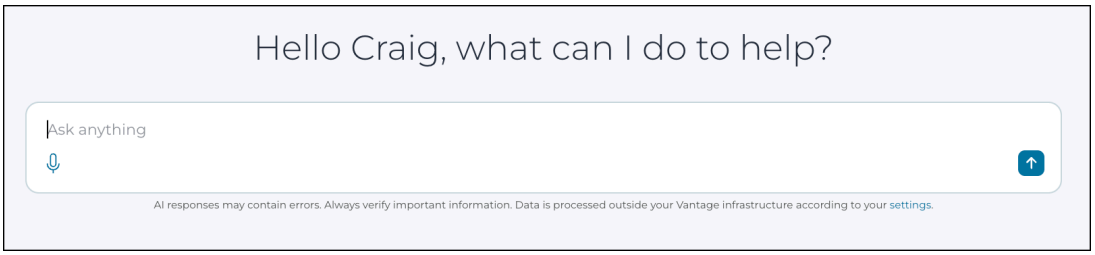
About this task

Each chat in the assistant is saved separately. Starting a new chat lets you ask questions in a fresh context, independent of any previous queries or results.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Assistant**.
3. Select **New chat**.

   Result: A new, empty chat opens. You can now type a query or question in the input field.



Open a previous chat

*Return to a previous chat in the **Assistant** to review earlier results or continue your investigation.*

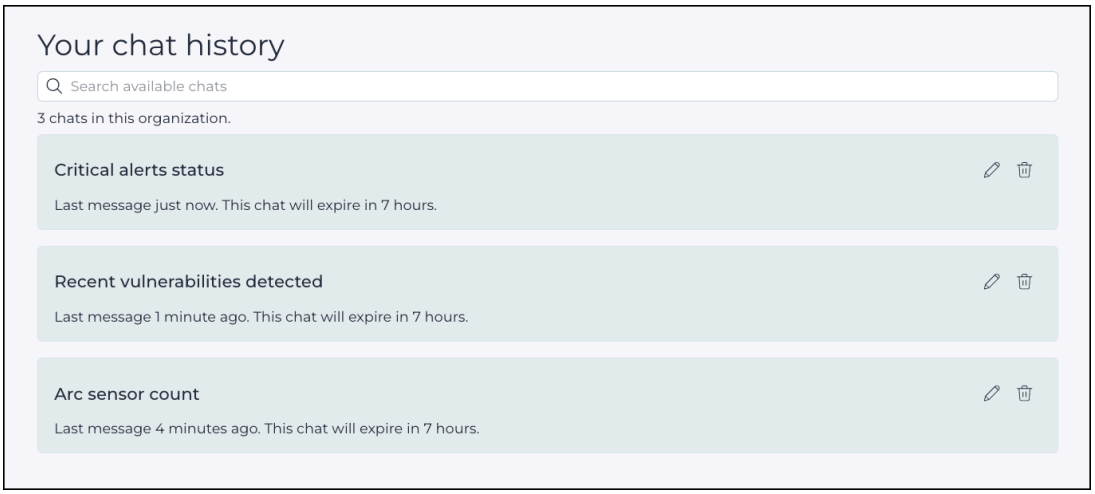
About this task

Chats are saved automatically and remain accessible using **Search chats**. You can reopen any previous chat to review results or run additional queries.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Assistant**.
3. Select **Search chats**.

   Result: Your chat history appears.



4. Select the chat you want to open.

   Result: The chat opens, showing your previous queries and results.

Rename a chat

*Rename a chat in the **Assistant** to make it easier to identify later.*

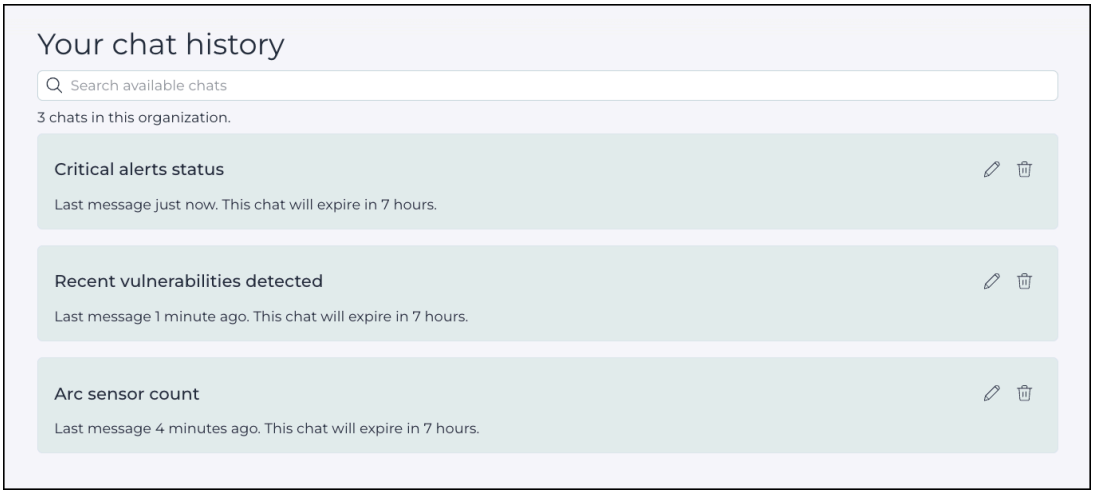
About this task

Chat titles are generated automatically from your first query. Rename a chat to give it a more meaningful name, especially if you plan to return to it later.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Assistant**.
3. Select **Search chats**.

   Result: Your chat history appears.



4. Select the edit icon next to the chat you want to rename.
5. Edit the chat name.
6. Select the save icon.

   Result: The chat is updated with the new name in the chat list.

Delete a chat

*Delete a chat from the **Assistant** history when it is no longer needed.*

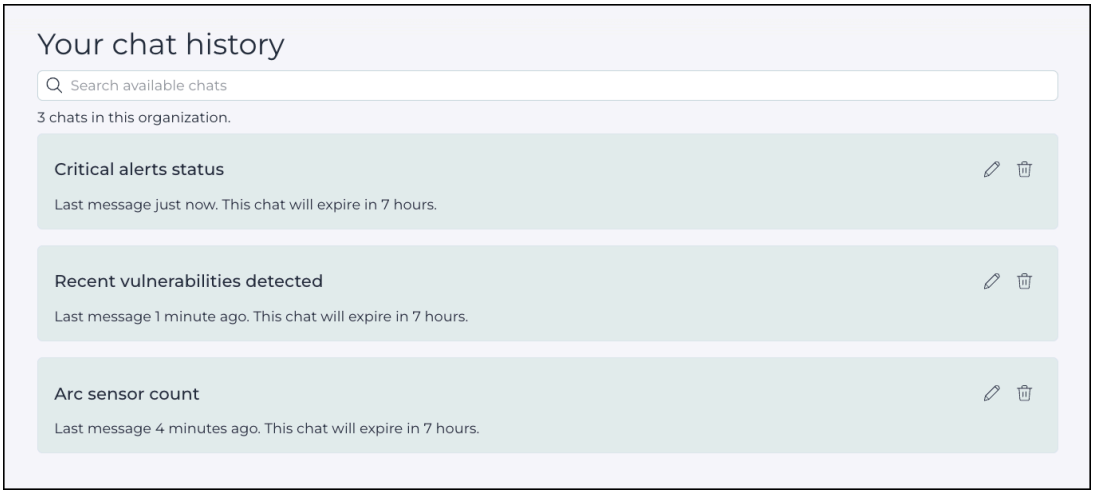
About this task

Deleting a chat removes it permanently from the chat history. You cannot recover a deleted chat.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Assistant**.
3. Select **Search chats**.

   Result: Your chat history appears.



4. Select the delete icon next to the chat you want to delete.

   Result: The icon turns red.

5. Select the delete icon again to confirm.

   Result: The chat is permanently removed from the chat list.

Insights

*The **Insights** page shows a dynamic summary of all the insights for your organization. The table shows a row for each insight, which relates to items within the environment that need to be addressed. Severity level and last trigger time determine the sort order.*

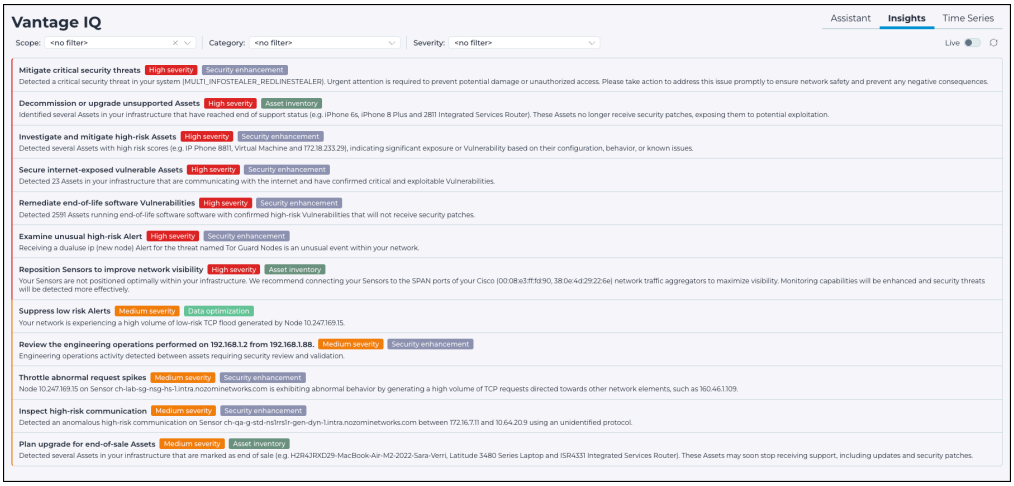


Figure 77. Insights tab

The **Insights** page shows correlated alerts and root-cause analysis. Vantage IQ uses deep neural networks to identify network activity patterns. Integrating data across Vantage makes it easier to:

- Analyze data forensically
- Tune settings
- Enhance security

A deeper understanding of security data and network traffic can help prioritize remediation efforts and close security gaps.

Filters

To filter the table view, there are these three dropdowns at the top of the page:

- **Scope**: This lets you use sites to limit the scope
- **Category**: This lets you use the insight category to filter the results
- **Severity**: This lets you use the insight severity level to filter the results

Severity levels

High severity

You should investigate this type of insight as soon as possible. The majority of critical insights relate to security issues.

Medium severity

This type of insight has security and operational concerns. The majority of warning insights are alerting improvements.

Low severity

This type of insight does not require immediate action. Informational insights help you understand your environment better.

The order the insights are shown in the list is:

- The most recent **High severity** insights show first, older **High severity** insights appear next
- The most recent **Medium severity** insights show next, older **Medium severity** insights appear next
- The most recent **Low severity** insights show next, older **Low severity** insights appear next

Table rows

You can select the table row of the insight to show a more detailed description of the insight. This lets you explore the insight further in the **Details list** of the related page.

Related information

IQ summaries (on page 223)

Open insight details

Select an insight from the Insights list to open its details. Explore related data, identify patterns, and act on findings immediately.

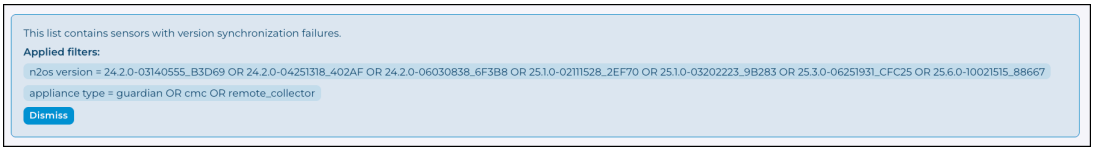
About this task

Open insight details to investigate the conditions or events associated with a specific insight. This step is typically part of a larger workflow where you assess and respond to detected anomalies, risks, or patterns in your environment. Understanding the detailed context behind each insight helps you prioritize actions and collaborate more effectively with your team.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.
3. Select anywhere in the insight row in the **Insights** table.

   Result: The applicable **Details list** opens, and displays context and related data for the selected insight.



Run an on-demand insights analysis

Run an on-demand insights analysis to get an up-to-date view of anomalies, risks, and patterns in your environment.

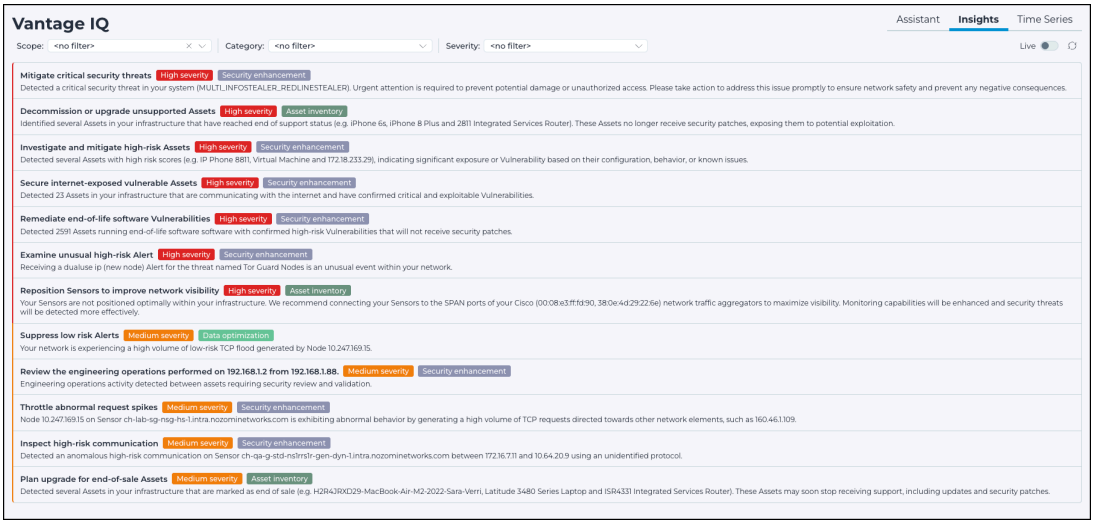
About this task

The **Insights** page runs a fresh analysis of your environment each time you open it. You can also trigger a new analysis at any time to reflect the latest state of your data.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.

   Result: Vantage IQ runs an on-demand analysis and updates the **Insights** table with the latest results.



3. **Optional:** If necessary, select the **Scope** dropdown and choose a site to limit the results to a specific scope.
4. **Optional:** If necessary, select the **Category** dropdown and choose a category to filter the results by insight type.
5. **Optional:** If necessary, select the **Severity** dropdown and choose a severity level to filter the results by priority.

Dismiss an applied insight

Dismiss an applied insight to clear the insight filter and return a page to its original unfiltered view.

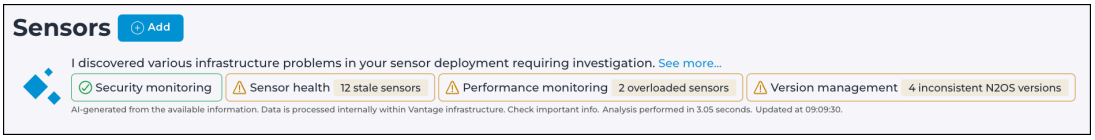
About this task

When you select an insight from the summary view on a related page, Vantage IQ applies a filter to that page to show only relevant data. If you then change the filters manually, the insight summary becomes unavailable. You can dismiss the applied insight to return the page to its original view without the insight filter.

Procedure

1. Navigate to a page that shows the Vantage IQ insight summary, such as the **Sensors** page.

   Result: The Vantage IQ insight summary bar appears at the top of the page.



2. Select an insight from the summary bar to apply its filter.
3. Select **Dismiss** in the insight summary bar.

   Result: The insight filter is cleared and the page returns to the original insights view.

What to do next

To restore the filtered view associated with an insight after making manual filter changes, select **Restore filters** instead of **Dismiss**.

Time Series

*The **Time Series** page uses machine learning to detect and forecast abnormal network activity across your sensors and numeric variables.*

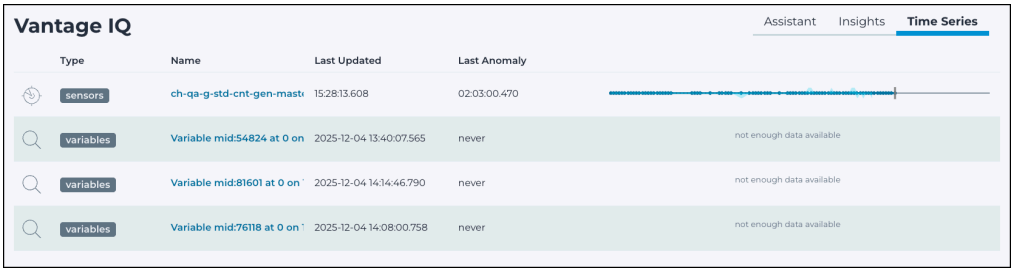


Figure 78. Time Series tab

With Time Series, you can predict and alert on abnormal activity from any sensor's or numeric variable's baseline using advanced machine learning techniques. Was the change expected or outside of the normal range of deviation for that period? Deep neural networks perform the forecasting and identify existing trends to predict forecast reliability using online signal analysis.

Setup

The **Time Series** page only shows items that have been individually enabled for IQ analysis. This includes sensors, and numeric variables for which variable history has been enabled. An item that has not been enabled does not appear in the **Time Series** list, even if your organization has a Vantage IQ license.

Time Series table

The table lists all sensors and numeric variables that have been enabled for Time Series monitoring. For each entry, the table shows:

- **Sensor name**: The name of the monitored sensor or variable
- **Last updated**: When the sensor's Time Series model was last updated
- **Last anomaly**: The timestamp of the most recent detected anomaly for that sensor
- **Activity**: A sparkline graph of recent network activity, showing observed values against the forecasted baseline

IQ summaries

IQ summaries appear as a summary bar at the top of multiple pages in Vantage, providing a quick overview of Vantage IQ insights relevant to that page.

IQ summaries and **Insights** are both computed using internal models that communicate only within your Vantage instance. An additional model specializes and reprocesses the insights for the context of each page. The summary bar appears at the top of multiple pages and summarizes the Vantage IQ data relevant to that page, helping you quickly recognize problems.

Important:

Your data is never used to train any model. All models are trained internally and only perform processing of your data.

Note:

The IQ summaries feature is the only Vantage IQ feature available to all customers, even without a Vantage IQ license (with restricted functionality). You can enable or disable it from the **Features** page.

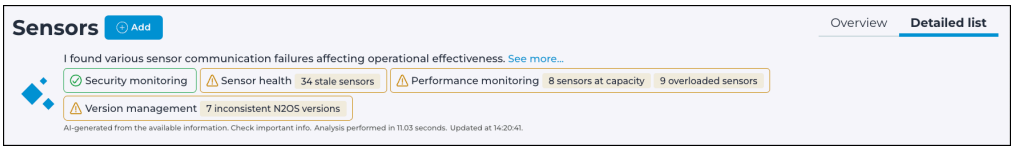


Figure 79. IQ summaries bar (Sensors page shown)

When the icon is animated, Vantage IQ is still processing the insights. Updates only take a few seconds.

If you select an insight in the summary bar, Vantage applies the applicable filter and the page or table updates. If you then make changes to the page, such as applying table filters, the summary bar becomes blurred to show it no longer applies. To restore the original filtered view, select **Restore filters** and the page resets. If you select **Dismiss**, the original insights view appears again.

Select **See more...** to open the summary drawer.

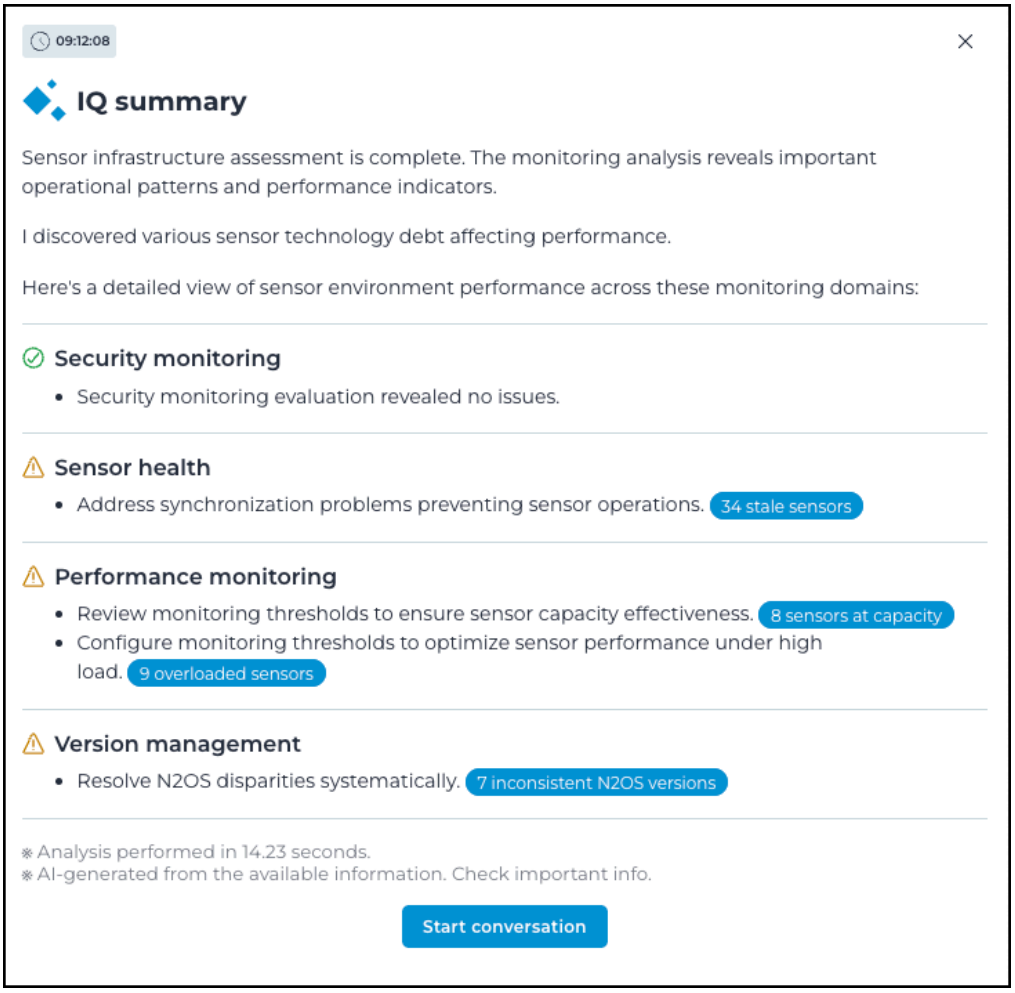


Figure 80. Summary drawer (Sensors page shown)

If you then select one of the blue buttons, the related table opens with the applicable filter active.

Related information

Open the IQ summary drawer (on page 225)

Dismiss an applied insight (on page 221)

Open the IQ summary drawer

Open the IQ summary drawer to see a detailed breakdown of all IQ summaries for the current page and start an assistant conversation in context.

About this task

The IQ summary bar at the top of the page shows a condensed view of available insights. Open the summary drawer to see a full breakdown and act on individual items.

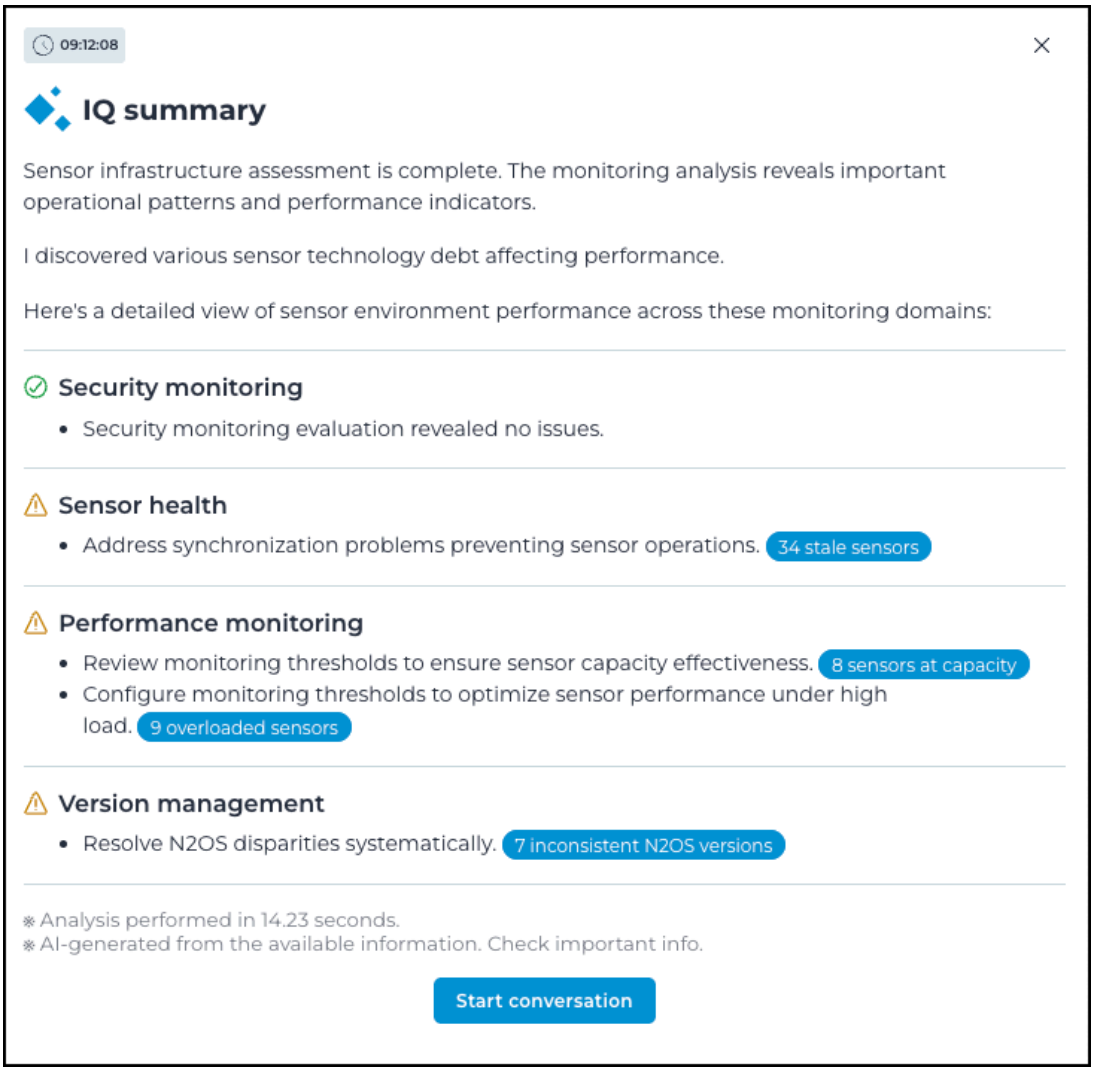
Procedure

1. Navigate to a page that shows the IQ summaries bar, such as the **Sensors** page.

   Result: The IQ summaries bar appears at the top of the page.

2. Select **See more...** in the IQ summaries bar.

   Result: The summary drawer opens and shows a detailed breakdown of the IQ summaries for the current page.



3. Select a blue button in the drawer to open the related table with the applicable filter active.

   Result: The summary drawer closes and the related table opens with the applicable filter active.

4. **Optional:** Select **Start conversation** in the drawer.

   Result: The **Assistant** page opens with a prefilled conversation thread based on the current page context.

Queries

With Vantage IQ, you can create charts, graphs, and AI calculations.

You can use these queries:

- Cluster (on page 229)
- Compare (on page 231)
- Correlation (on page 232)
- Describe (on page 233)
- Forecast (on page 234)
- Pivot (on page 235)
- Popular (on page 236)
- Simplify (on page 237)
- Timeline (on page 238)
- Versus (on page 239)
- Visualize (on page 240)

Cluster

*Use the **`cluster`** command to group rows by recognized patterns and identify outliers in your data.*

Usage: `<field> | cluster <number>`

Description: Group different rows in several clusters based on automatically recognized patterns within the data.

Example: `assets | cluster`

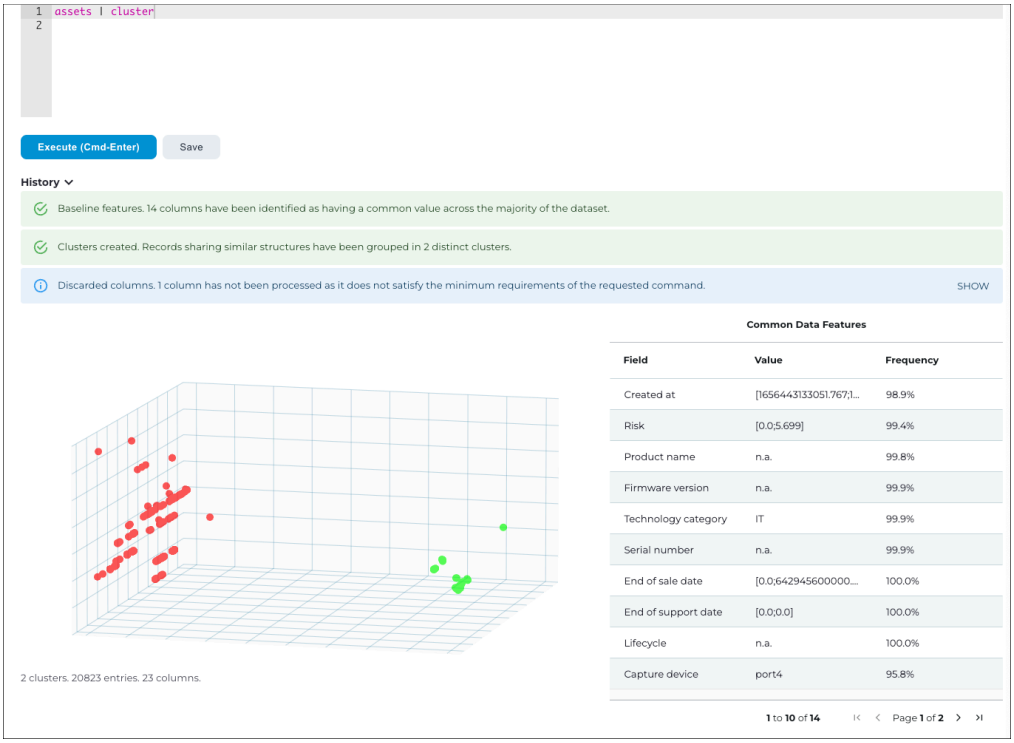


Figure 81. Query result: assets | cluster

Example: `assets | cluster 3`

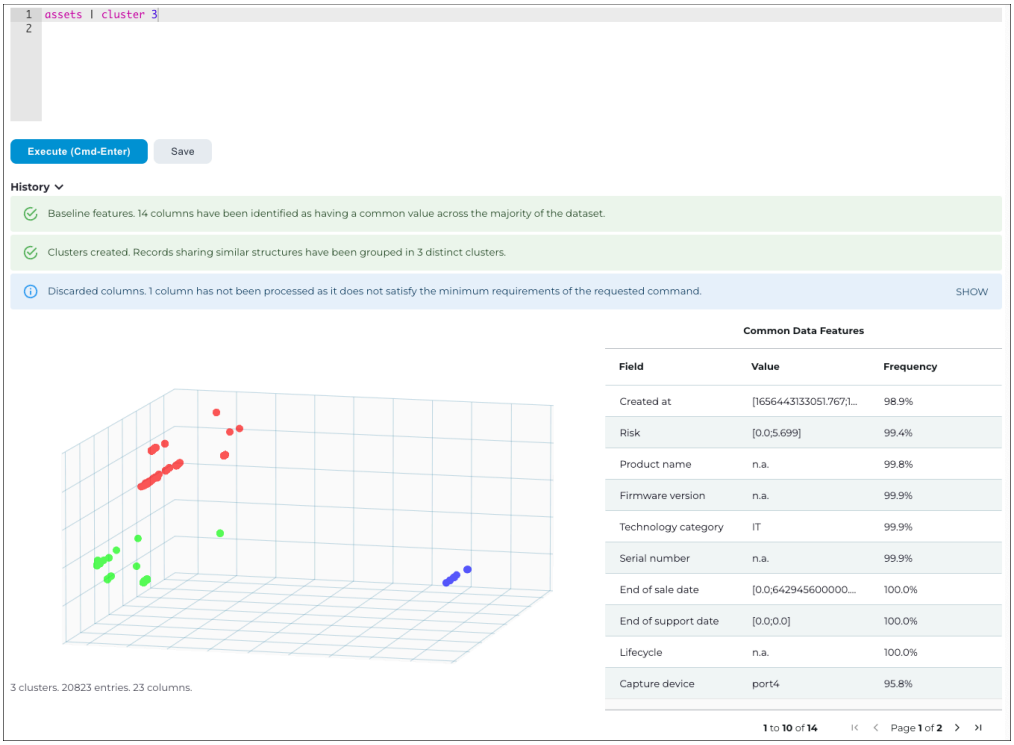


Figure 82. Query result: assets | cluster 3

Compare

*Use the **`compare`** command to evaluate differences between two datasets or time periods.*

Usage: `<field> | compare <field1> <field2>`

Description: Compute nonlinear value relationships between two categorical, interval, and ordinal columns.

Example: `alerts | compare risk protocol`

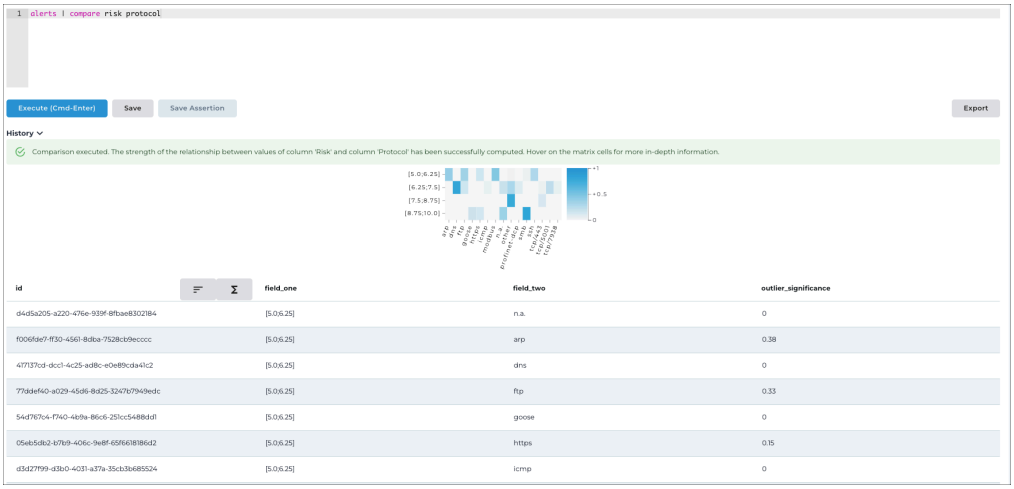


Figure 83. Query result: alerts | compare risk protocol

Example: `assets | compare os name`

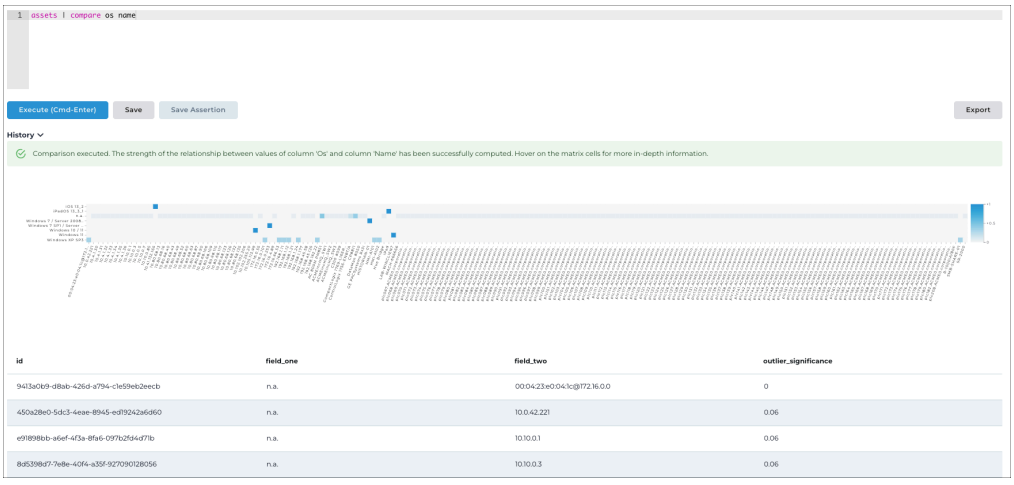


Figure 84. Query result: assets | compare os name

Correlation

Use the `correlation` command to discover relationships between fields or metrics in your data.

Usage: `<field> | correlation`

Description: Compute nonlinear correlations between categorical, interval, and ordinal columns.

Example: `alerts | correlation`

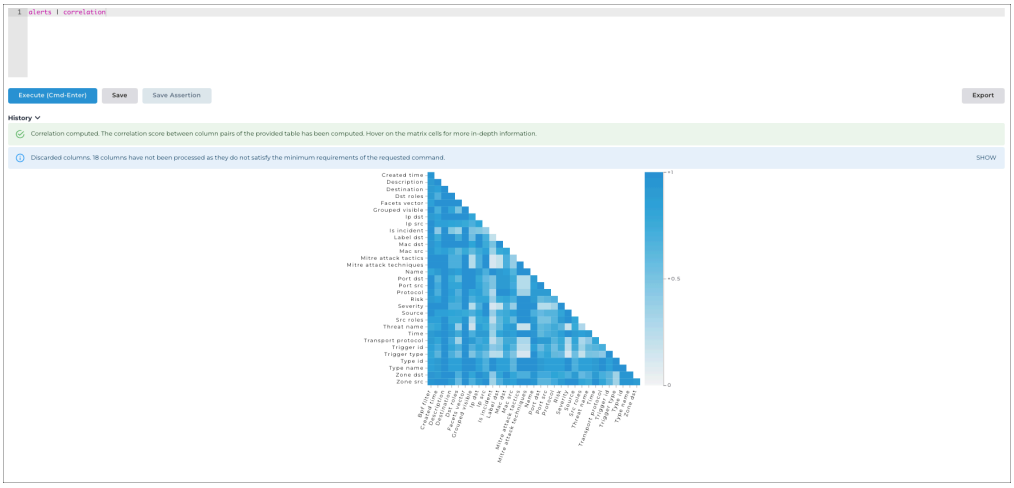


Figure 85. Query result: alerts | correlation

Example: `assets | correlation`

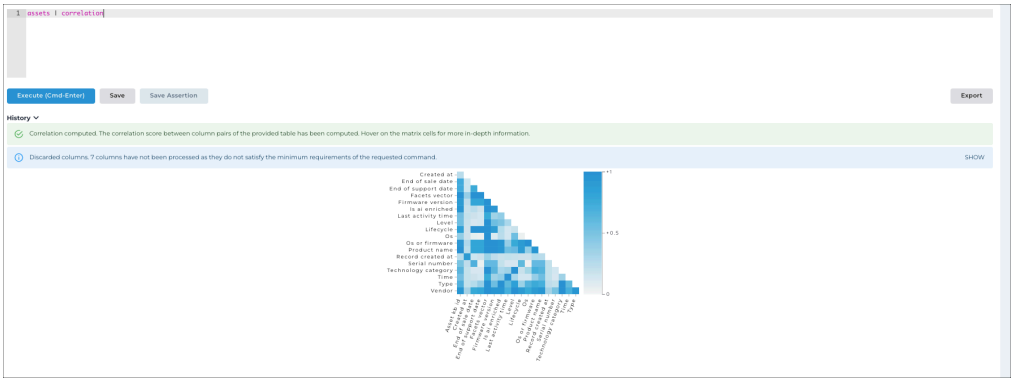


Figure 86. Query result: assets | correlation

Describe

*Use the **`describe`** command to generate a statistical summary of a dataset, including counts, ranges, and distributions.*

Usage: `<field> | describe`

Description: Compute several descriptive statistics of the passed content.

Example: `alerts | describe`

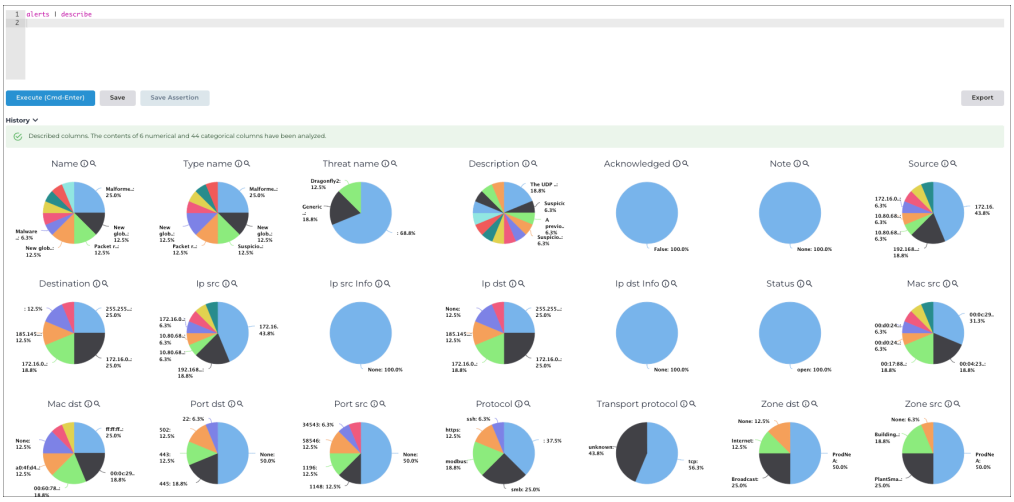


Figure 87. Query result: alerts | describe

Example: `assets | describe`

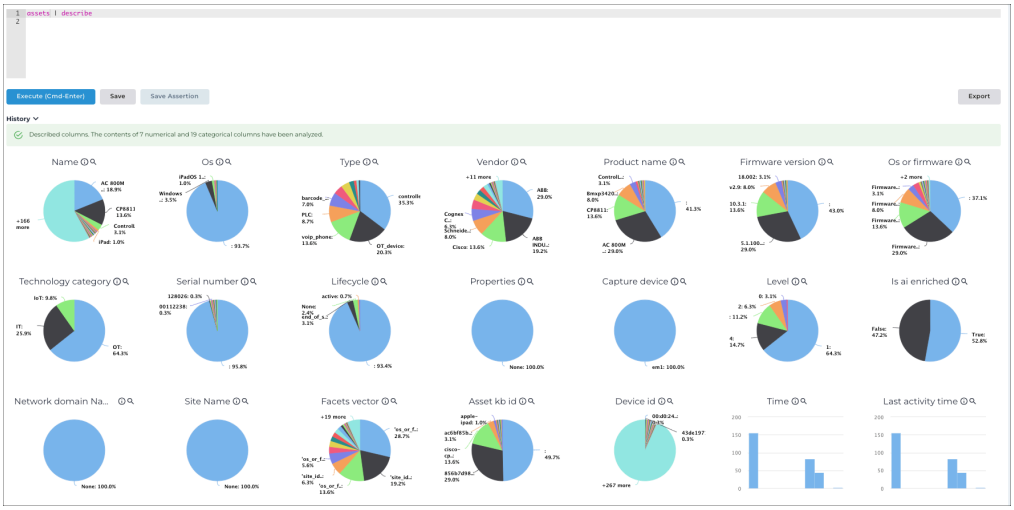


Figure 88. Query result: assets | describe

Forecast

Use the `forecast` command to predict future values based on historical trends in your data.

Usage: `<field> | forecast <number> <field1> <field2> <field3>`

Description: Forecast the values of a numeric time series.

Example: `alerts | forecast 10 time risk`

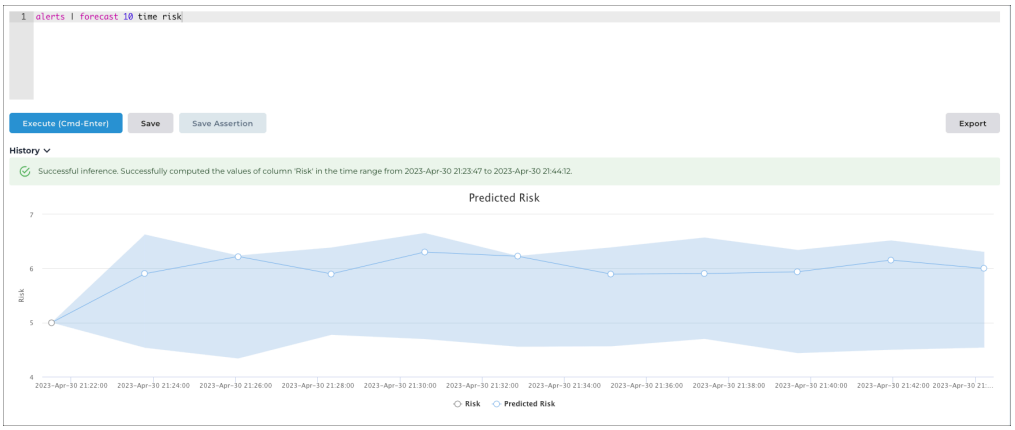


Figure 89. Query result: alerts | forecast 10 time risk

Example: `assets | forecast 3 created_at last_activity_time`

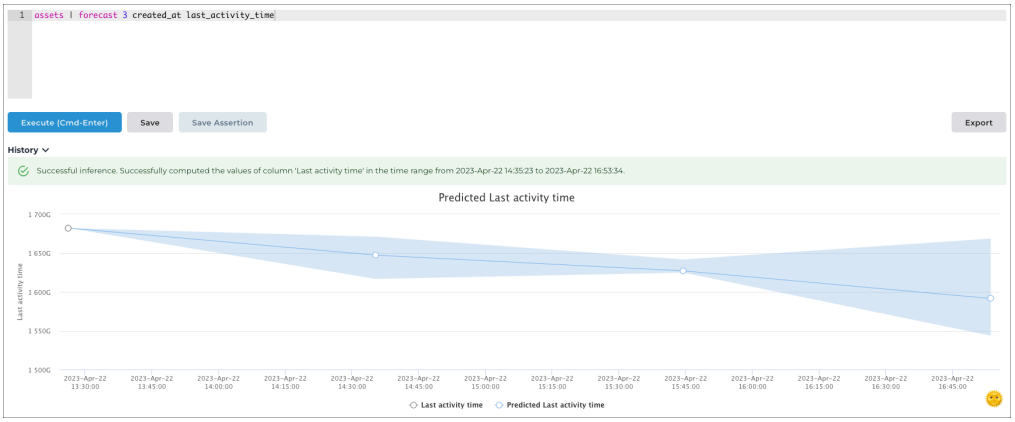


Figure 90. Query result: assets | forecast 3 created_at last_activity_time

Pivot

*Use the **`pivot`** command to reshape query results by rotating row values into columns for cross-tabulation.*

Usage: `<field> | pivot <field>`

Description: Splits the data using the unique values of a given column and analyzes the distributions of the other columns for each one of these values.

Example: `alerts | pivot protocol`

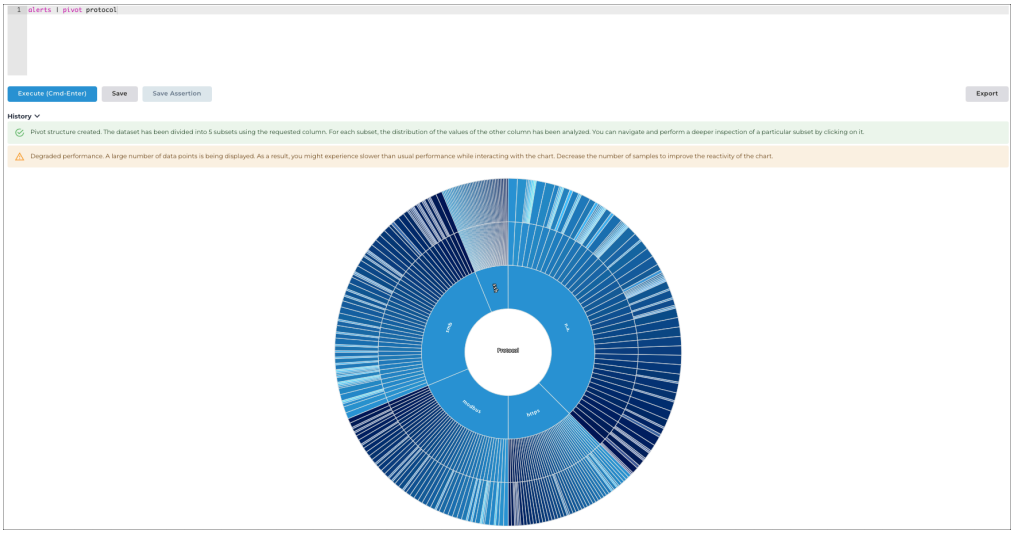


Figure 91. Query result: alerts | pivot protocol

Example: `assets | pivot type`

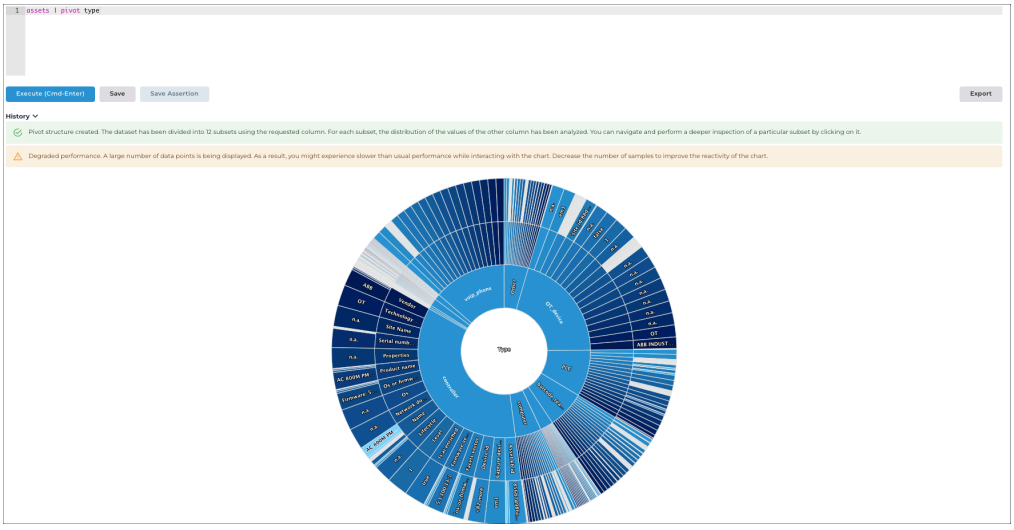


Figure 92. Query result: assets | pivot type

Popular

*Use the **`popular`** command to identify the most frequently occurring values in a dataset.*

Usage: `<field> | popular <field>`

Description: Find the most popular values in a table and visualize them.

Example: `alerts | popular`

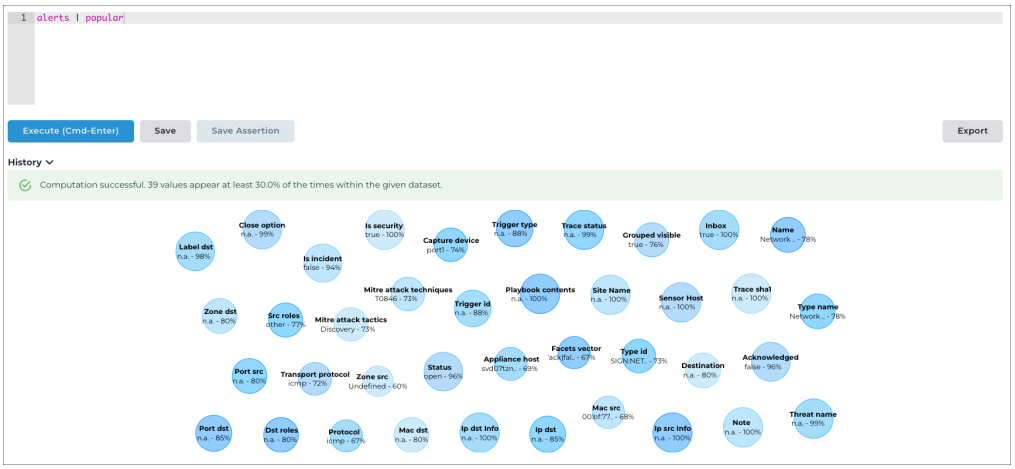


Figure 93. Query result: alerts | popular

Example: `alerts | popular 0.6`

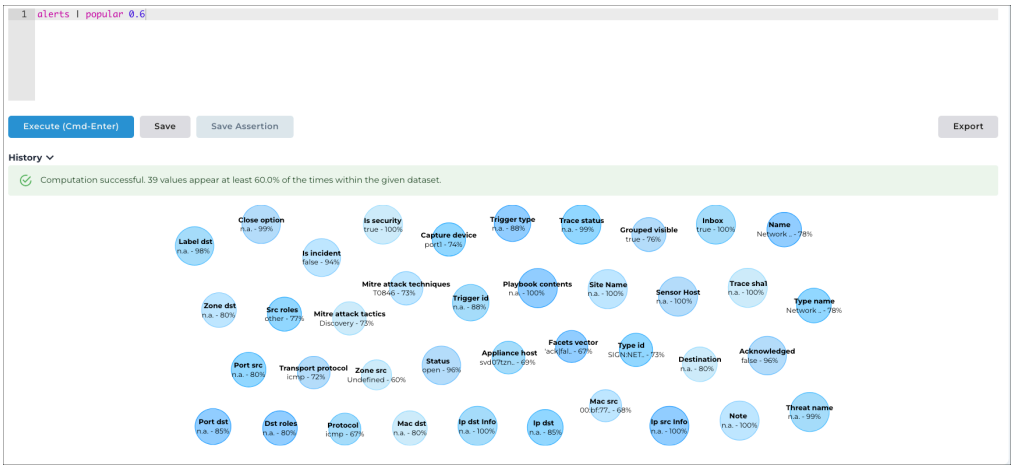


Figure 94. Query result: alerts | popular 0.6

Simplify

*Use the **`simplify`** command to reduce query output to its key patterns, making large result sets easier to interpret.*

Usage: `<field> | simplify <field> <rows> <number>`

Description: Identify the rows and columns carrying the highest information level.

Example: `alerts | simplify`

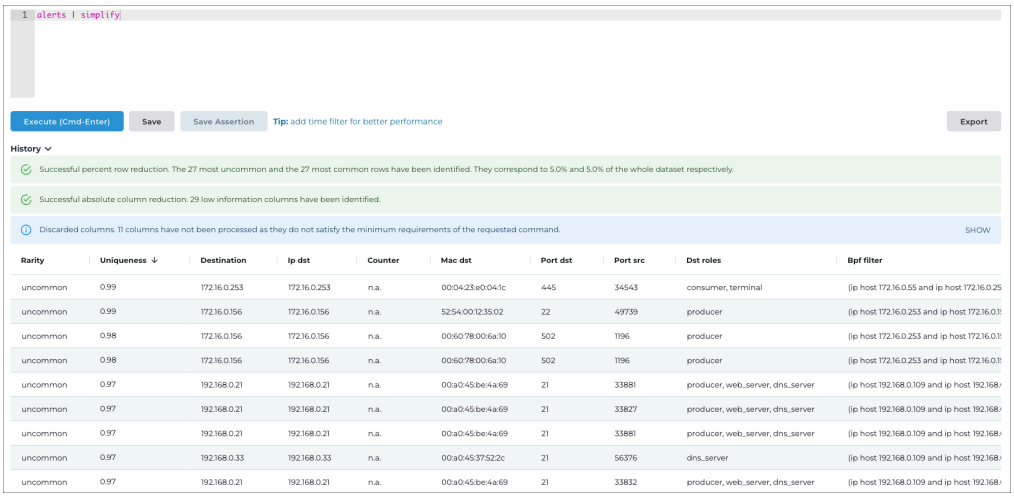


Figure 95. Query result: alerts | simplify

Example: `assets | simplify rows 10`

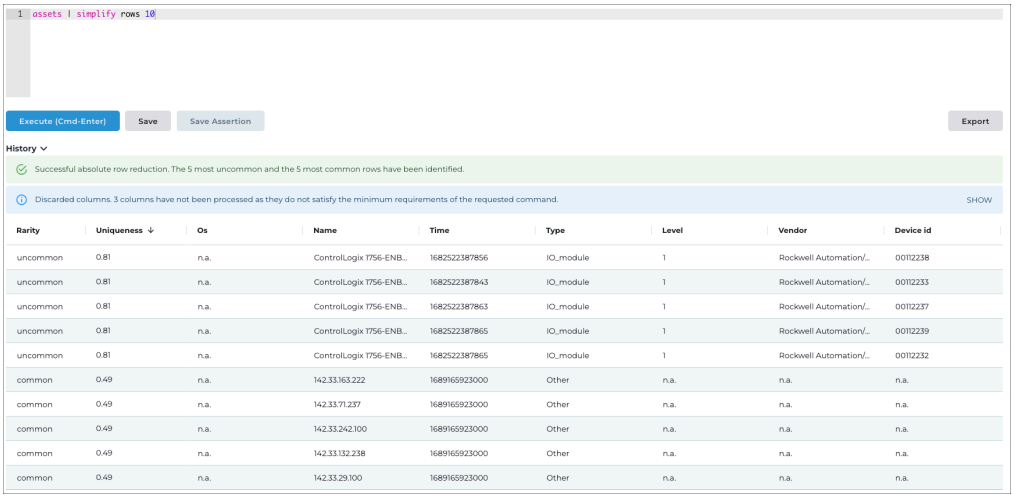


Figure 96. Query result: assets | simplify rows 10

Timeline

*Use the **`timeline`** command to display events or metrics in chronological order for time-based analysis.*

Usage: `<field> | timeline <field>`

Description: Displays the most significant events for the given dataset as time moves forward.

Example: `alerts | timeline time`

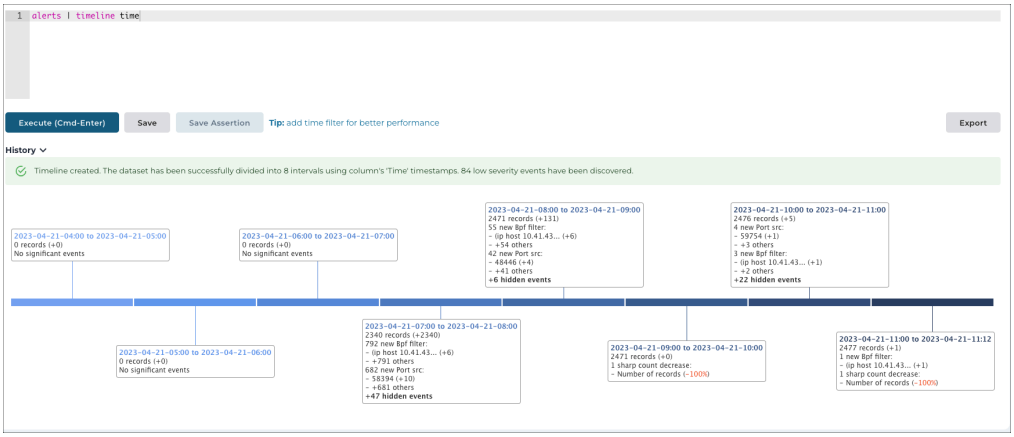


Figure 97. Query result: alerts | timeline time

Example: `assets | timeline created_at`

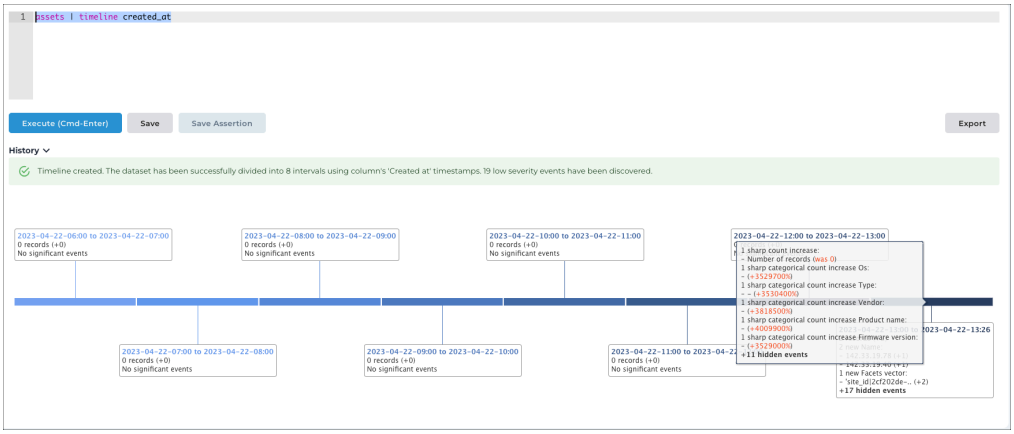


Figure 98. Query result: assets | timeline created_at

Versus

*Use the **versus** command to compare two specific entities or metrics side by side.*

Usage: `<field> | versus as <format> <field>`

Description: Given a boolean condition, it divides the dataset into two subsets and compares them to find columns where the behavior has significant changes.

Example: `alerts | versus as bars when risk >= 6`

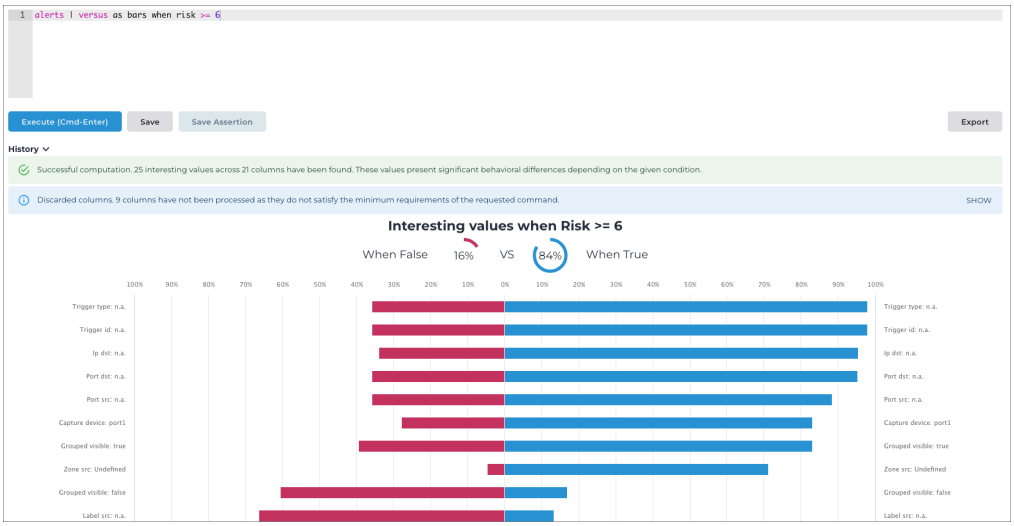


Figure 99. Query result: alerts | versus as bars when risk >= 6

Example: `alerts | versus as cards when risk >= 6`

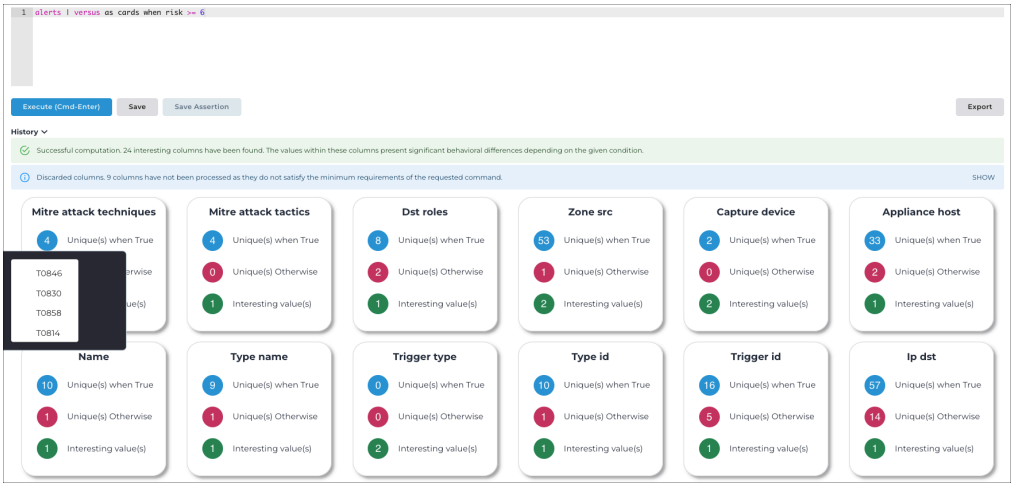


Figure 100. Query result: alerts | versus as cards when risk >= 6

Visualize

*Use the **`visualize`** command to render query results as a chart or graph for at-a-glance interpretation.*

Usage: `<field> | visualize`

Description: Provides a graphical visualization of the given rows.

Example: `alerts | visualize`

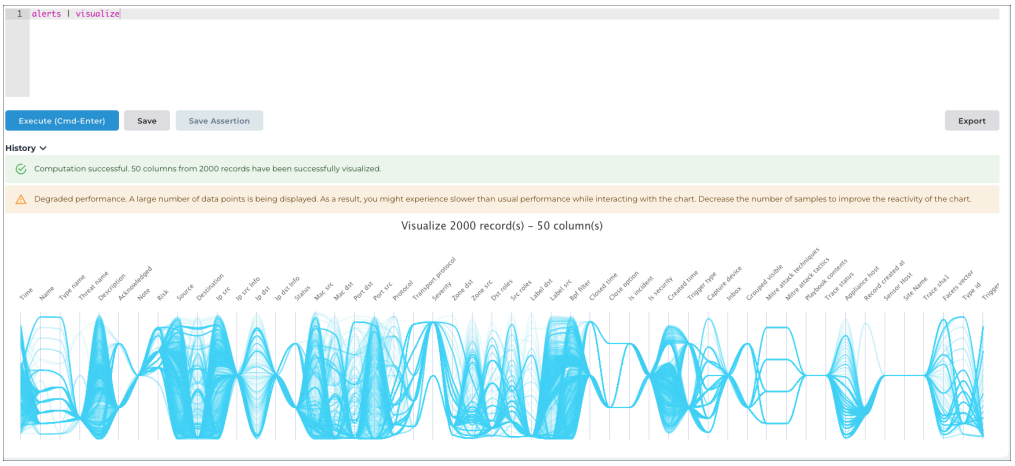


Figure 101. Query result: alerts | visualize

Example: `assets | visualize`

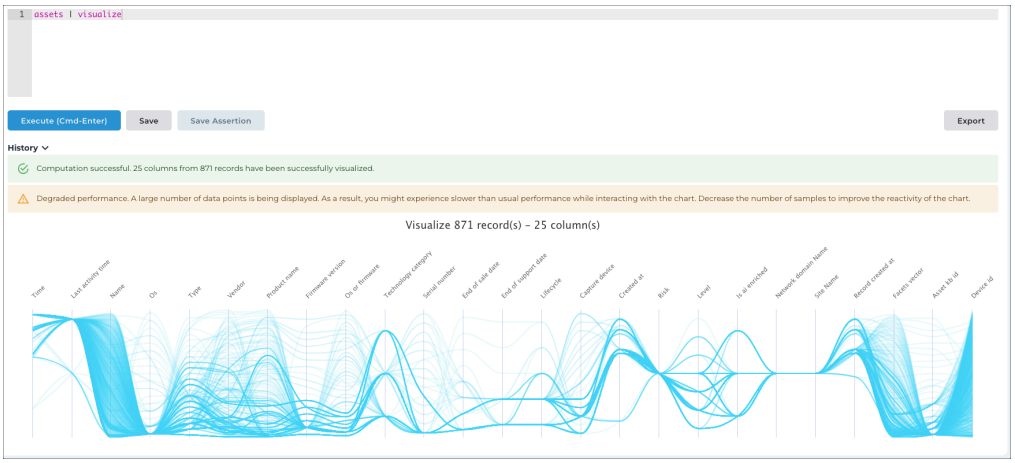


Figure 102. Query result: assets | visualize

Chapter 9. Network

*The **Network** page shows a visual representation of your network and all its assets.*

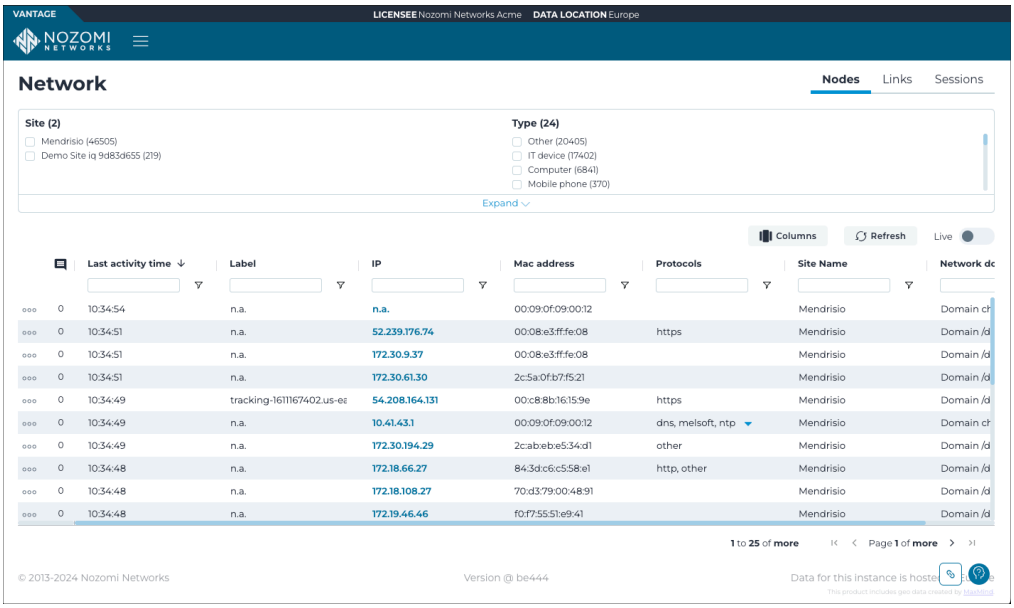


Figure 103. Network page

General

The **Network** page has these tabs:

- Nodes (on page 244)
- Links (on page 245)
- Sessions (on page 246)

Related information

Graph (on page 247)

Graph customization (on page 256)

Nodes

*The **Nodes** page shows a visual representation of your network and all its assets.*

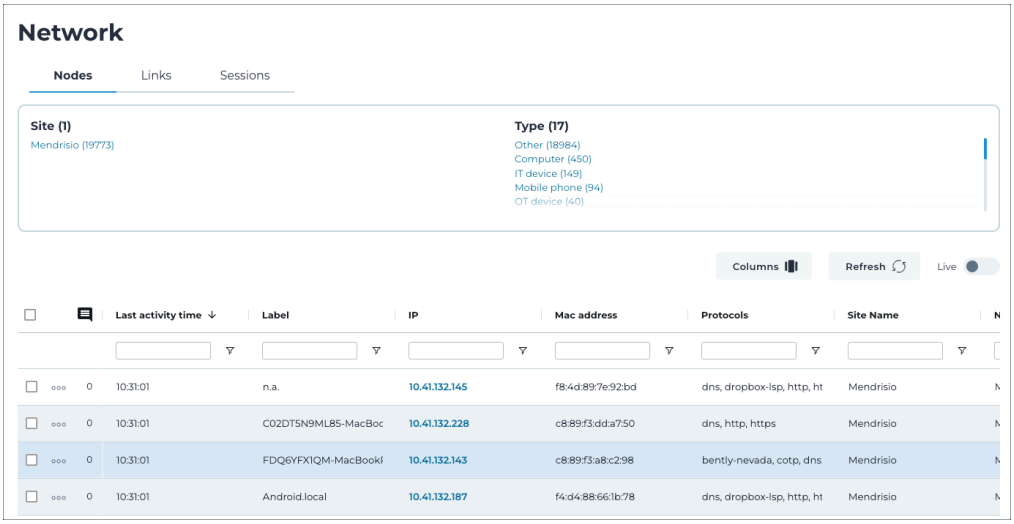


Figure 104. Nodes page

Site

This section shows a list of all the sites in your environment.

Type

This section shows a list of all the types of node in your environment.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Links

*The **Links** page shows a visual representation of your network and all its assets.*

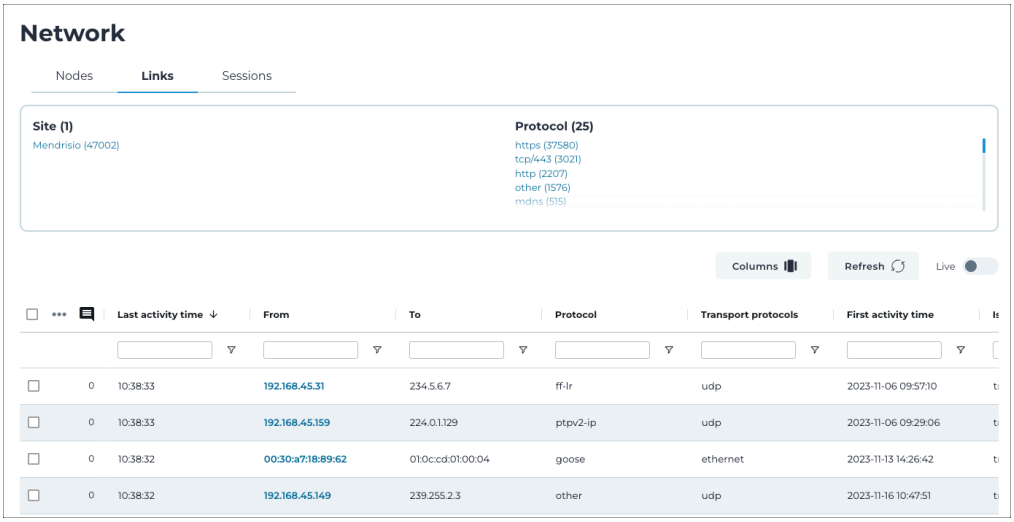


Figure 105. Links page

Site

This section shows a list of all the sites in your environment.

Protocol

This section shows a list of all the protocols in your environment.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Sessions

*The **Sessions** page shows a visual representation of your network and all its assets.*

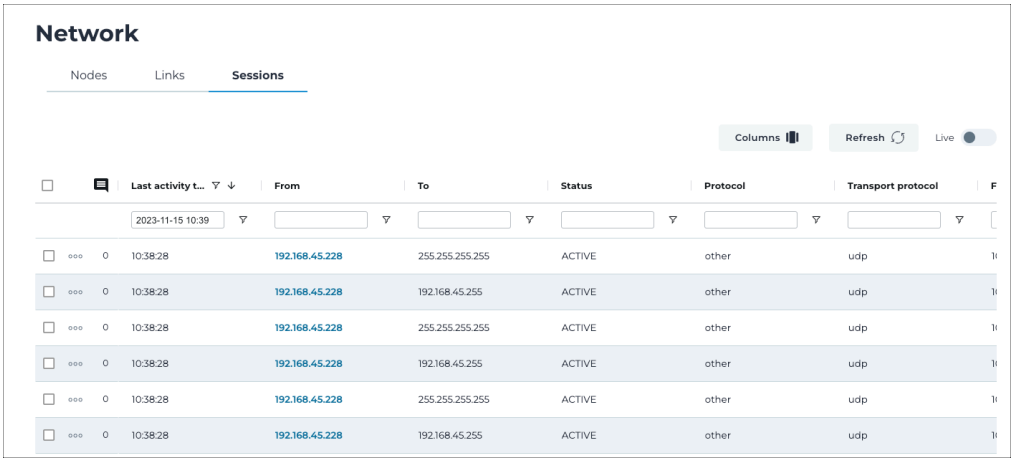


Figure 106. Sessions page

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Chapter 10. Graph

Displays a visual map of your network, highlighting asset connections and communication paths. Users can switch between network and physical views to explore infrastructure relationships.

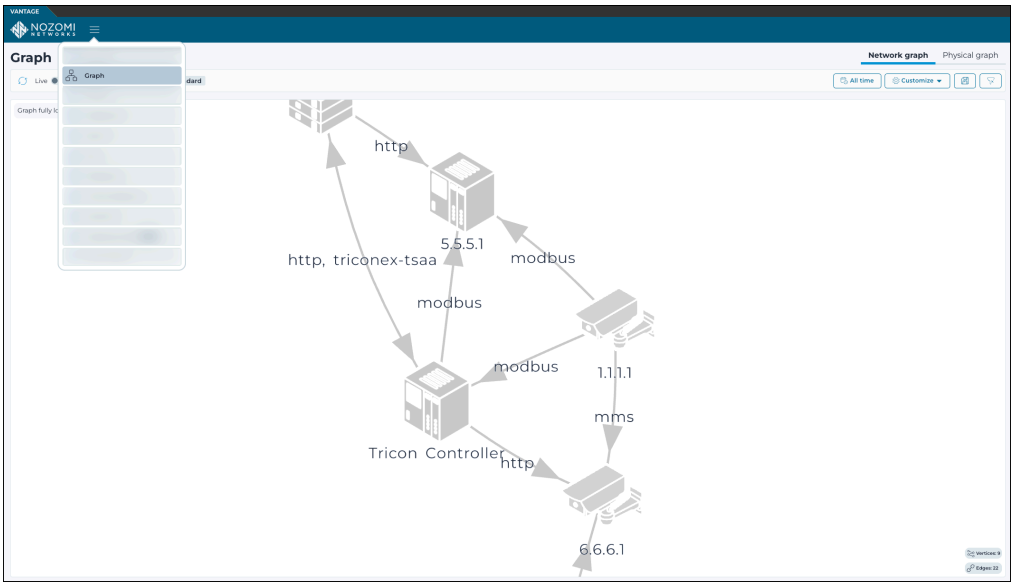


Figure 107. Graph page

The **Graph** page has these tabs:

- Network graph (on page 250)
- Physical graph (on page 253)

Related information

Network graph (on page 250)

Physical graph (on page 253)

Graph customization (on page 256)

Network graph

*The **Network graph** page shows a visual representation of your network and all its assets. The icons can represent both assets or nodes. If a node belongs to an asset, then only the asset will show. If several nodes belong to the same asset, they will not show, and only the asset will show. In the case that a node does not belong to an asset, the node itself will show.*

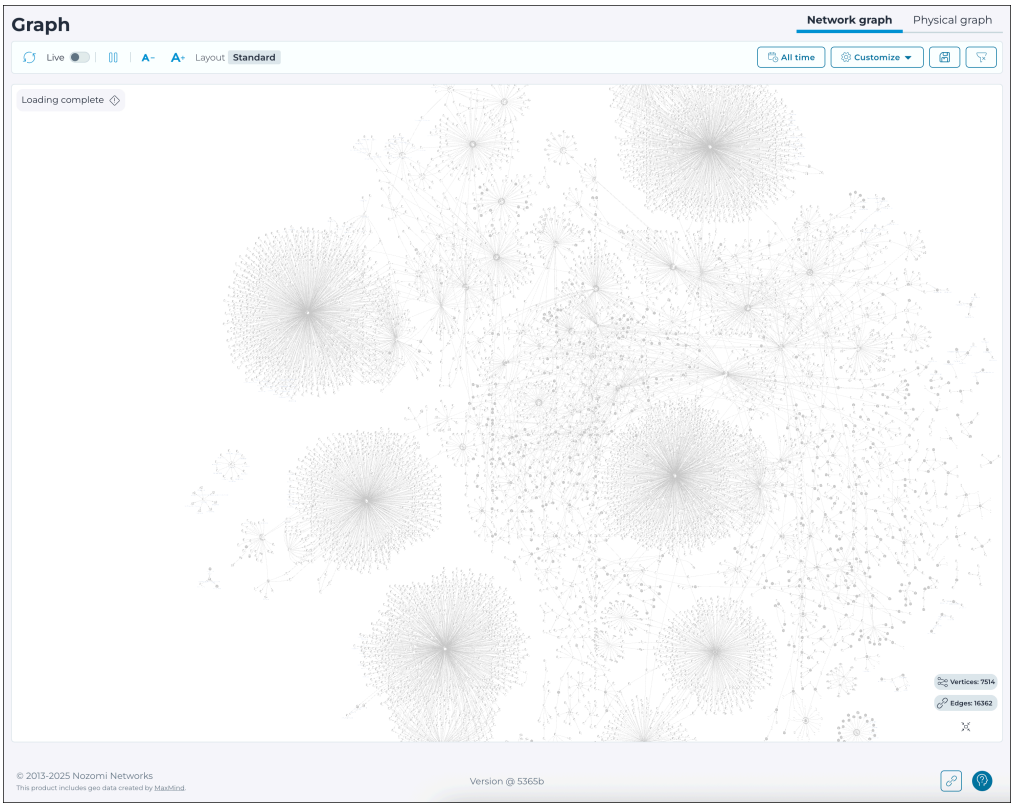


Figure 108. Network graph page

Icons

The top left and right corners have icons that you let interact with the graph.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Pause-play

The pause-play icon lets you pause, or restart the motion of the graph.

Layout
The Layout icon shows which layout is active in the graph. You can select from the available options in the **Customize** menu.

Icon size
These icons let you increase, or decrease the size of the icons.

Time selector
Choose a time period for the graph.

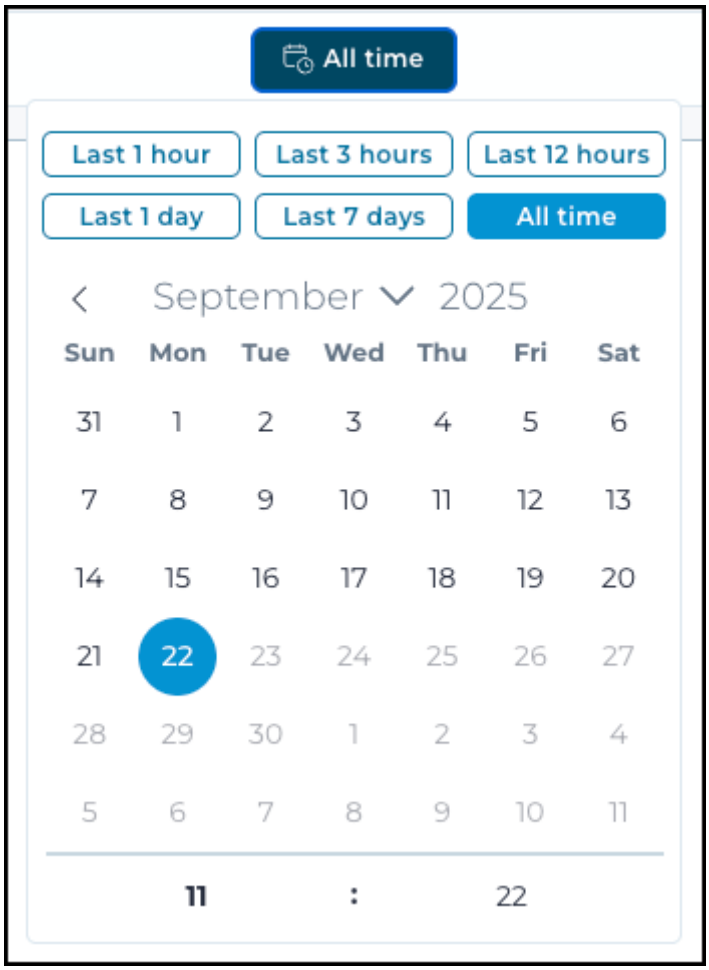


Figure 109. Time selector

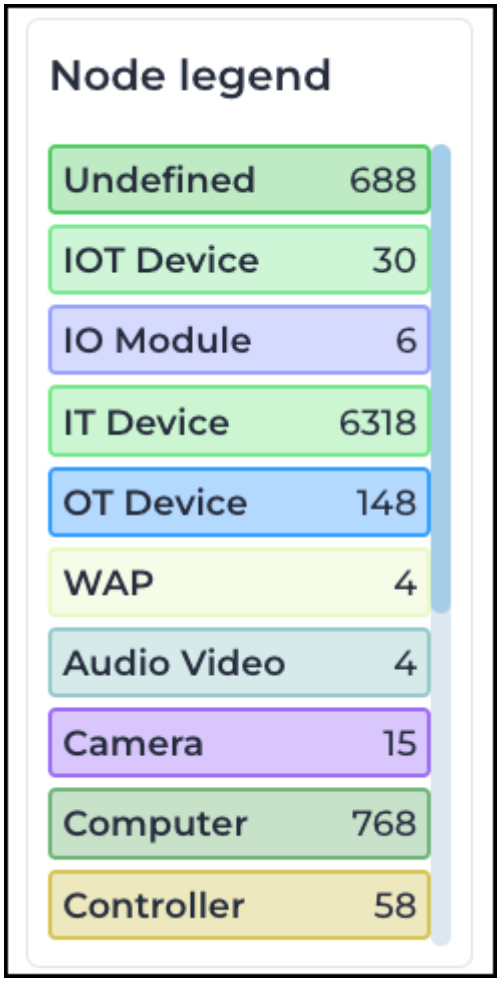
Customize
The **Customize** button opens a menu of settings that you can choose from. For more details, see Graph customization (on page 256).

Save
The save icon lets you save the current filter settings.

Clear filter
The clear filter icon lets you clear all the current filters.

Legend

The legend icon is in the bottom left corner of the graph. The legend will show when you click on the icon. To hide it, you need to click on it again.



Each type of node shows in a different color. The total number of the related type is also shown.

Reset and center zoom

The reset and center zoom icon resets the zoom level and centers the graph.

Graph navigation

To use the graph, you can:

- Use your cursor to zoom in and out
- Use your mouse to click-and-drag the graph and move it
- Select links (lines) and assets (icons) to view the related details in the right drawer
- In the drawer, you can select **Details** to open the related Vantage page

Physical graph

*The **Physical graph** page displays a real-time interactive map of all physical device connections in the network. Nodes are shown only if a physical link has been detected for them. The graph, shows how devices connect at the cable level. It is a live, visual way to understand your physical network layout down to the port.*

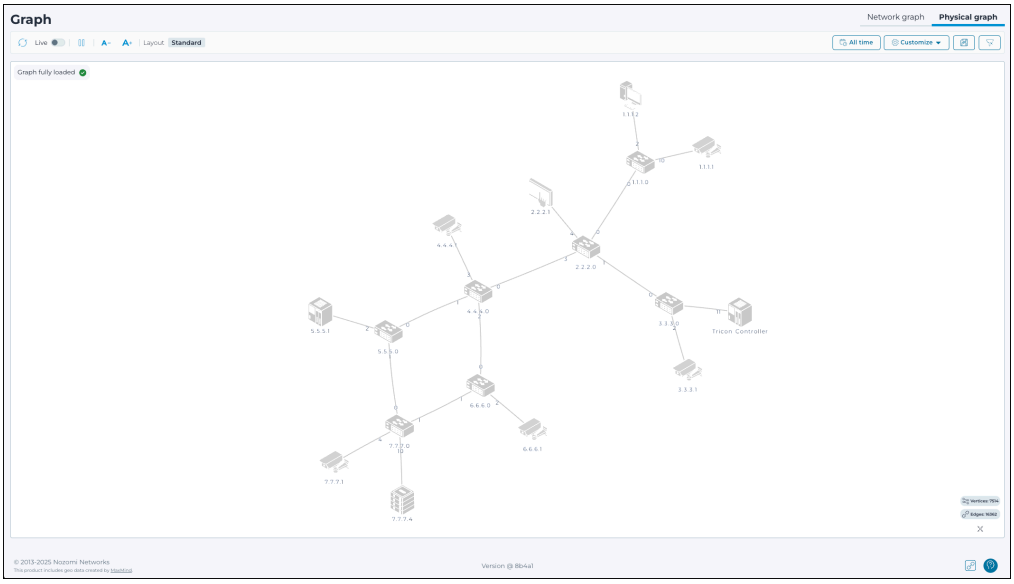


Figure 110. Physical graph page

Overview

The **Physical graph** view provides a visual representation of cable-level connections between devices in the network. It uses data collected through Smart Polling to display physical links in a dynamic topology graph that reflects actual hardware wiring, including switch port details.

This view supplements logical graphs by showing real-time or historical physical connectivity between assets. Devices are positioned based on link data, with visual indicators that show port assignments and device types. Use the **Physical graph** to examine network structure, trace physical paths, and identify connectivity changes.

Icons

The top left and right corners have icons that you let interact with the graph.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Pause-play

The pause-play icon lets you pause, or restart the motion of the graph.

Layout

The Layout icon shows which layout is active in the graph. You can select from the available options in the **Customize** menu.

Icon size

These icons let you increase, or decrease the size of the icons.

Time selector

Choose a time period for the graph.

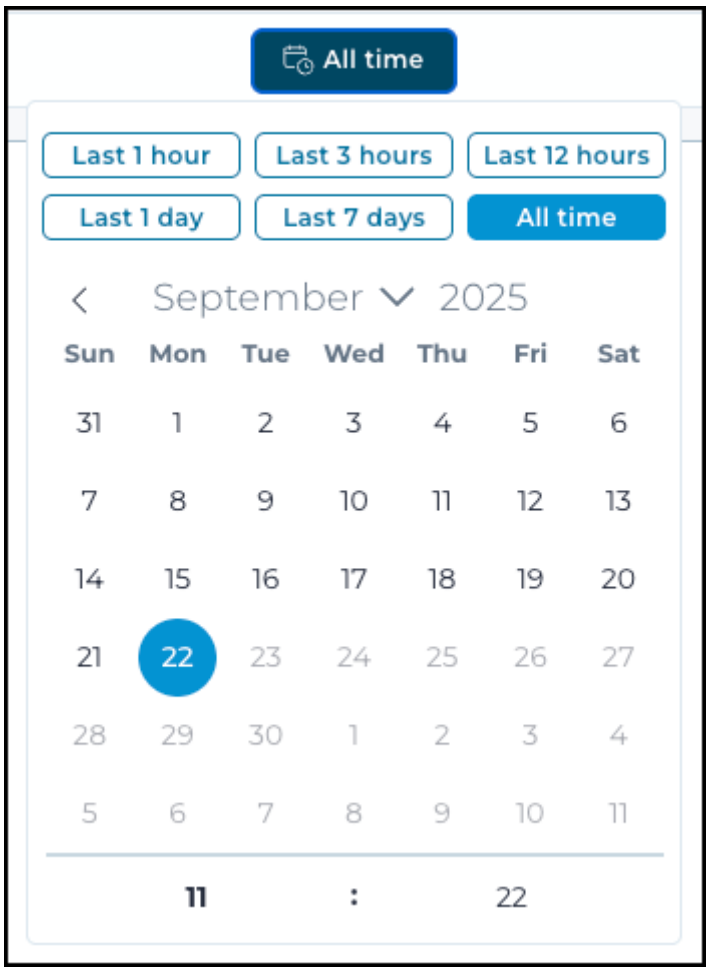


Figure 111. Time selector

Customize

The **Customize** button opens a menu of settings that you can choose from. For more details, see Graph customization (on page 256).

Save

The save icon lets you save the current filter settings.

Clear filter

The clear filter icon lets you clear all the current filters.

Reset and center zoom

The reset and center zoom icon resets the zoom level and centers the graph.

Graph navigation

To use the graph, you can:

- Use your cursor to zoom in and out
- Use your mouse to click-and-drag the graph and move it
- Select links (lines) and assets (icons) to view the related details in the right drawer
- In the drawer, you can select **Details** to open the related Vantage page

Graph customization

*The **Customize** button lets you customize the graph view.*

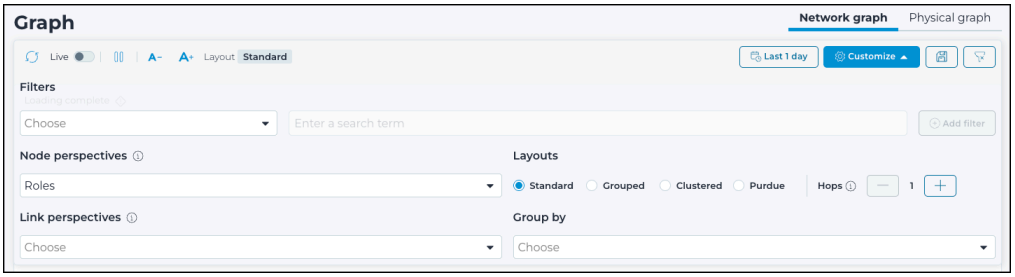


Figure 112. Customization settings (Network graph version shown)

The **Customize** button opens a menu of settings that you can choose from to change the graph view. These settings let you change the appearance and structure of the network graph for more effective data interpretation.

Filters

Use filters to restrict the visible assets and links based on selected criteria. This helps reduce visual clutter and focus on relevant areas of the network.

If several filters of different types are selected, a logical AND is applied.

If several filters of the same type are selected, a logical OR is applied.

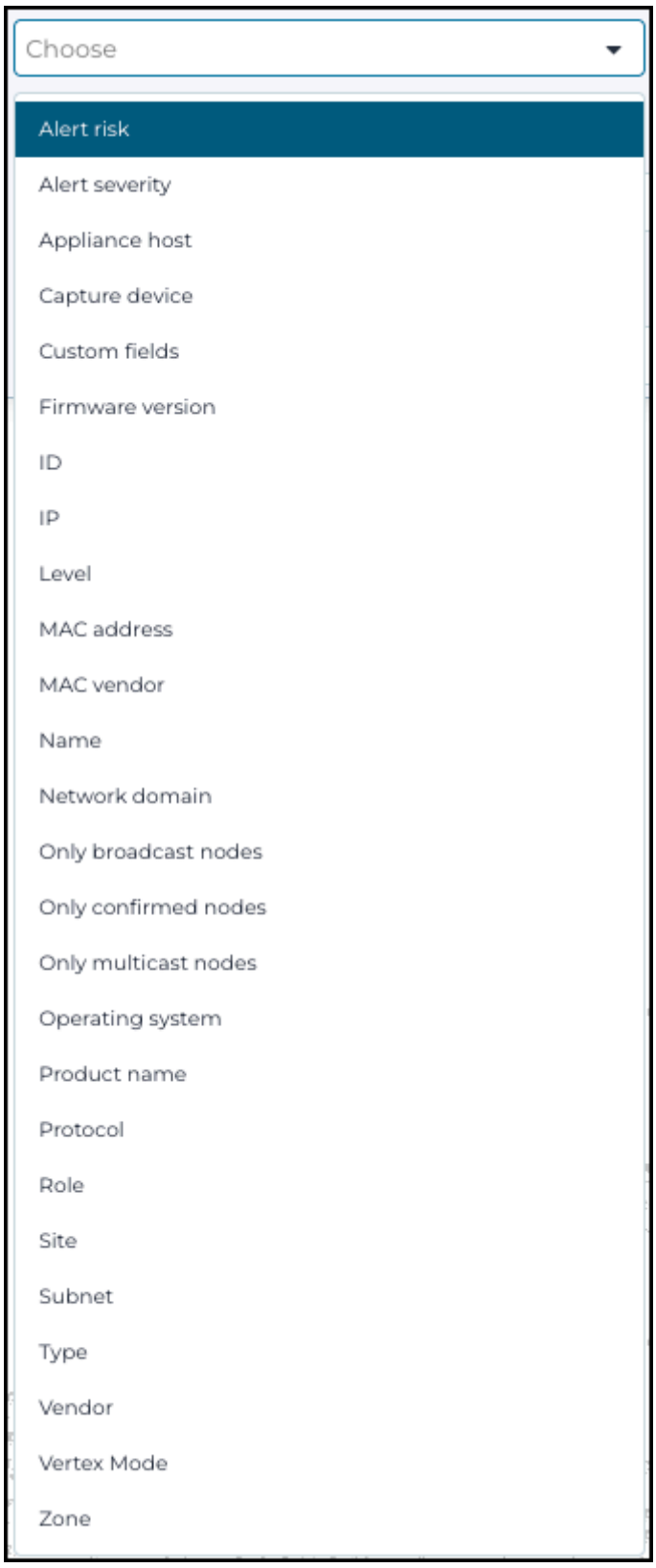


Figure 113. Filter dropdown

Once a filter is selected, one of these items will become active to the right:

- A dropdown that lets you make a further, related selection
- A text field that let's you enter and search for custom text

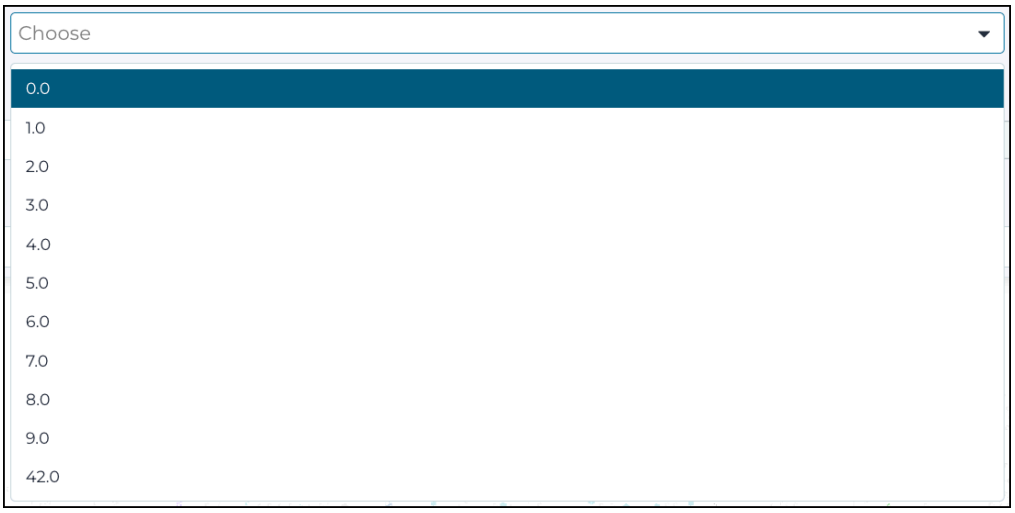


Figure 114. Choose dropdown/ text field

Node perspectives

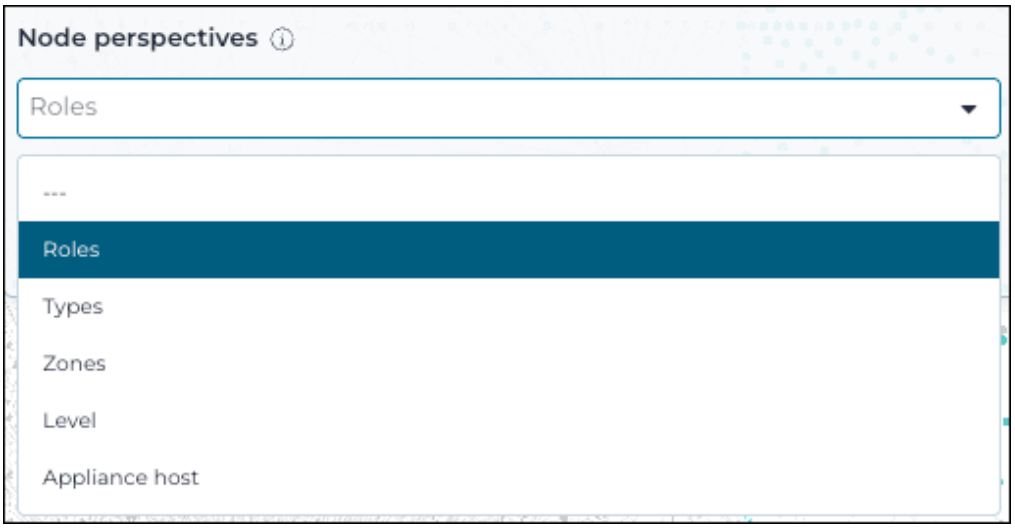


Figure 115. Nodes perspectives dropdown

Select the property that changes the color of the nodes in the graph. This setting controls the perspective from which nodes are visually and semantically organized. You can choose how the color of individual nodes show in the graph:

- **Roles** – Color nodes based on assigned roles, such as client, server, or gateway
- **Types** – Color nodes according to their device type (e.g., switch, sensor, workstation)
- **Zones** – Color nodes by logical zones, often reflecting segmentation policies or network architecture

- **Level** – Color nodes based on hierarchical levels, such as Purdue model layers
- **Appliance host** – Color nodes based on the monitoring appliance that discovered or manages them

Layouts

Select one of the available graph layout types to change how assets and links are visually arranged:

Standard: Default arrangement based on connectivity.

Grouped: Group nodes based on the **Group by** selection. Nodes will be grouped in different circles based on the value of the defined property. For example, if the property is **Zones**, nodes that belong to the same zone will be put in the same circle.

Clustered: The nodes are hierarchically grouped in clusters based on the topology. If a **Group by** is defined, this sets the first level of the hierarchy.

Purdue (Network graph only): Follows the Purdue model for industrial control system layers.

Hops

The **Hops** settings lets you adjust the number of connection hops shown in the graph in any filtered view. The settings let you start with a focused set of assets and progressively discover additional connections. This makes it easier to investigate relationships without losing context. The lowest setting is `1` and not `0`. This is because a graph with a single isolated node has no value. Therefore, by default you will see the node `1.1.1.1` with the first level of connected nodes. When you increase the setting to `2`, the nodes that are connected to all the first level nodes will also show.

From the start position, you not only see what you have filtered, but the first level of connected nodes. For example, if you filter with the *IP* address: `1.1.1.1`, you will not just see the single isolated node `1.1.1.1`, but also the first level of connected nodes.

Link perspectives (Network graph only)

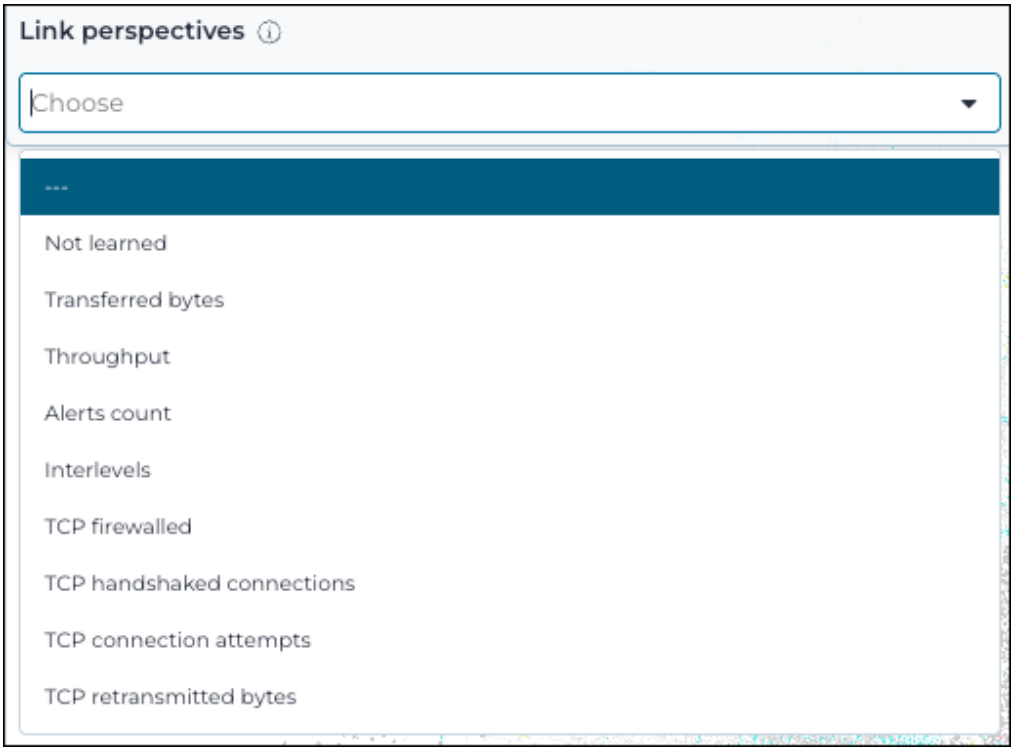


Figure 116. Link perspectives dropdown

Select the property that changes the color of the links in the graph. Link perspectives help illustrate different types of relationships or communication flows between devices. You can choose how the color of individual links show in the graph.

Group by

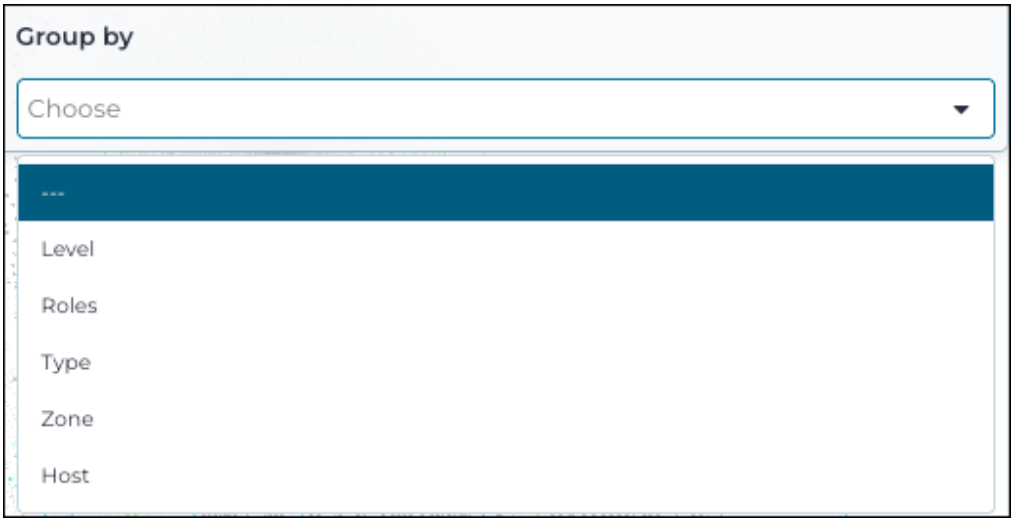


Figure 117. Group by dropdown

Dynamically group nodes in the graph by specified metadata such as device type or subnet. This feature enhances pattern visibility and makes it easier to detect anomalies or segment relationships.

When **Group by** is defined, the result will depend on the selected layout:

Standard: All nodes with the same **Group by** value will be condensed into a single node. For example, if the **Group by** is **Roles**, then all the nodes with the same role will be condensed into a single node.

Grouped: All nodes with the same **Group by** value will be put in the same circle. For example, if the **Group by** value is **Zone**, then all the nodes that belong to the same zone will be put in the same circle.

Clustered: All nodes with the same **Group by** value will be put in the same first level cluster of the cluster hierarchy.

Purdue: Nodes will show in different circles based on their level. Circles will show in a three dimensional view.

Chapter 11. Process

*The **Process** page shows a list of processes in your environment. Processes are a set of repeatable functions that a business does to deliver a core value.*

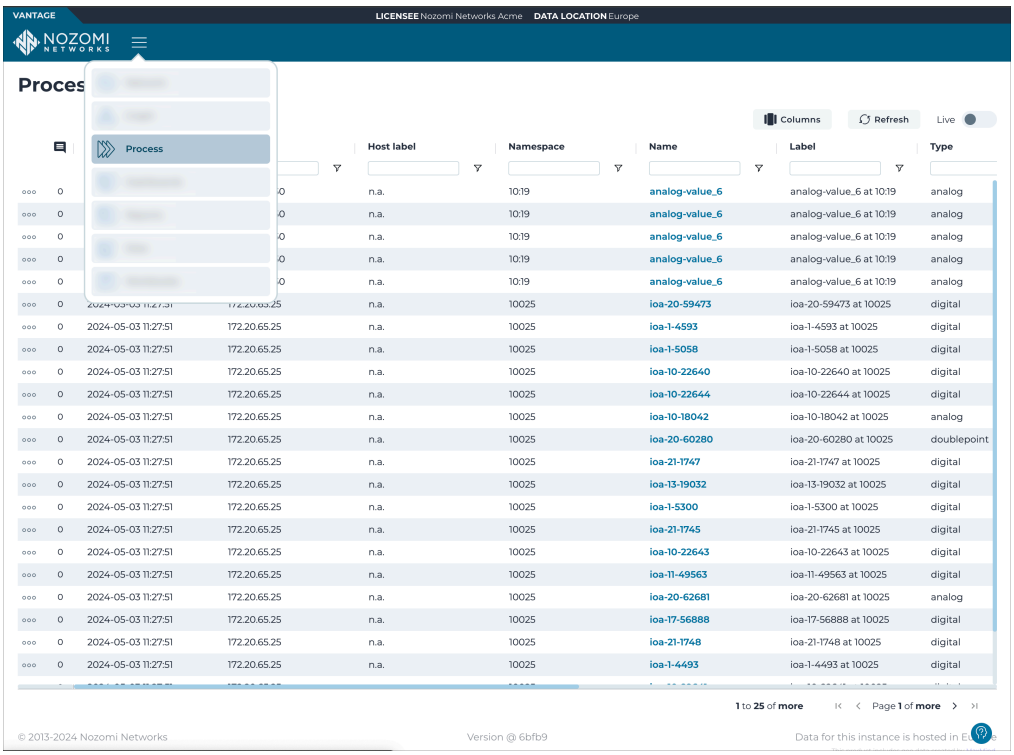


Figure 118. Process page

Process includes:

- Repeatable tasks
- Data collection
- Resource control in accordance with business policies

Variables model communication between operational devices as they participate in the industrial process.

Individual values within operational devices are represented as variables, and Vantage tracks them over time in **Process**.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Table interactions

Actions menu

Enable history

*The **Enable History** function lets you start to map historical values.*

Procedure

1. In the top navigation bar, select ☰ > **Process**.

   Result: The Process (on page 263) page opens.

2. Choose a method to open the actions menu.

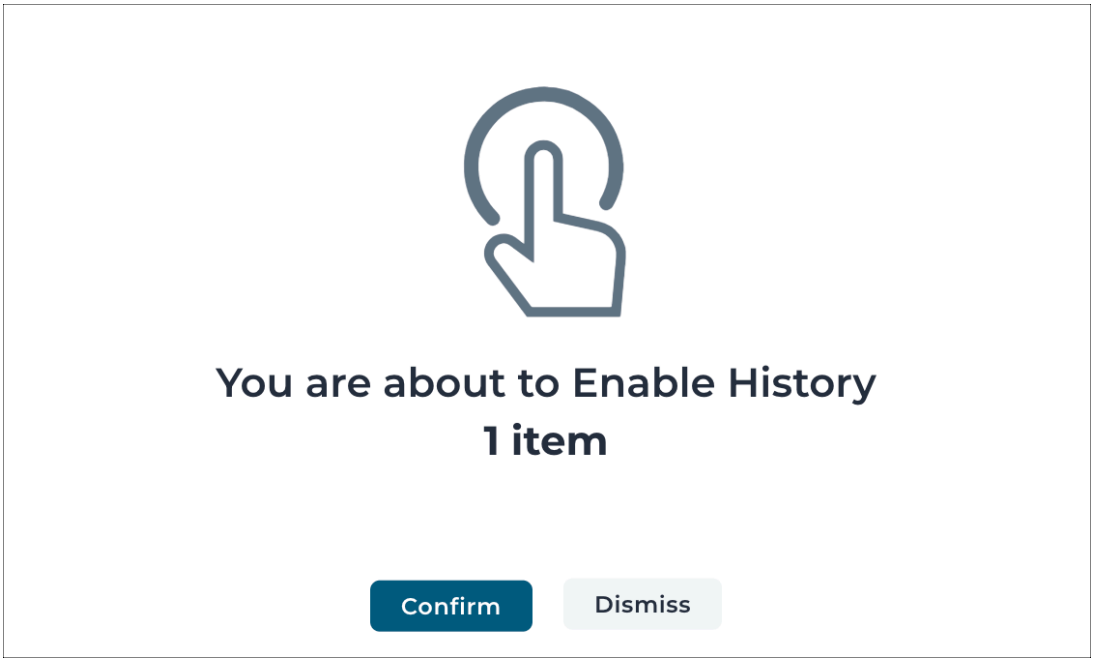
   Choose from:

   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. Select **Enable History**.

   Result: A dialog shows.

4. Select **Confirm**.



Results

History has been enabled.

Chapter 12. Dashboards

*The **Dashboards** page shows a list of all the dashboards that have been created.*

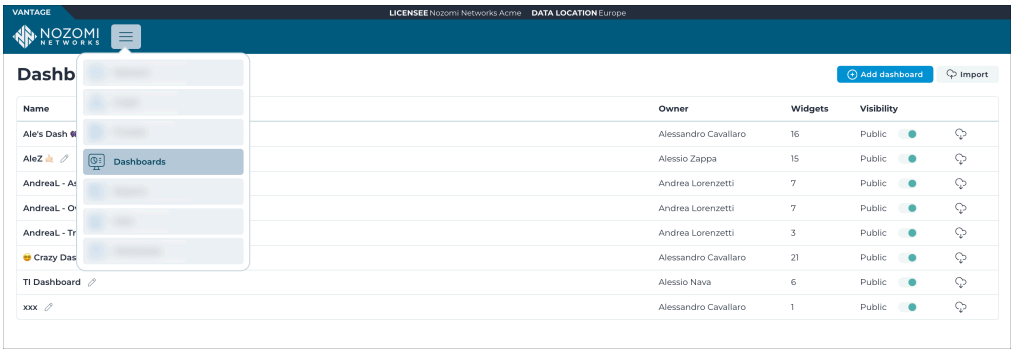


Figure 119. Dashboards page

Add dashboard

This button lets you Create a dashboard (on page 270).

Import

This button lets you Import a dashboard (on page 271).

Related information

Create a dashboard (on page 270)

Import a dashboard (on page 271)

Export a dashboard (on page 272)

Add a widget (on page 273)

Print a dashboard (on page 274)

Create a dashboard

This procedure explains how to create a dashboard, select a template, enter a name, and set visibility options.

Procedure

1. In the top navigation bar, select ☰ > **Dashboards**.

   Result: The Dashboards (on page 267) page opens.

2. From the **Choose a template** dropdown, select an option.

   You can choose from these options:

   - Empty
   - Alerts
   - Assets
   - Overview
   - Sensors
   - Traffic
   - Vulnerabilities

3. In the **Dashboard name** field, enter a name for your dashboard.
4. **Optional:** If you want the dashboard to be visible to everyone in your organization, select **is public?** to on.
5. Select **Create dashboard**.

Results

The dashboard has been created, and it is now visible in the **Dashboards** page.

Import a dashboard

It is possible to import a dashboard that has previously been exported in JSON format.

Procedure

1. In the top navigation bar, select ☰ > **Dashboards**.

   Result: The Dashboards (on page 267) page opens.

2. In the top right section, select **Import**.

   Result: The **Import a dashboard** page opens.

3. Select **Choose file** and select the *JSON* dashboard file.
4. Once the file has loaded, select **Confirm**.

Results

The dashboard has been imported, and it is now visible in the **Dashboards** page.

Export a dashboard

It is possible to export a dashboard in JSON format.

Procedure

1. In the top navigation bar, select ☰ > **Dashboards**.

   Result: The Dashboards (on page 267) page opens.

2. To the right of the applicable dashboard, select the icon.

Results

The dashboard downloads in *JSON* format.

Add a widget

Once you have a dashboard, you can add a widget to it.

Procedure

1. In the top navigation bar, select ☰ > **Dashboards**.

   Result: The Dashboards (on page 267) page opens.

2. Select the applicable dashboard.
3. In the top right section, select **Add widget**.

   Result: The **Edit widget** page opens.

4. From the **Widget** dropdown, select a widget type.
5. **Optional:** In the **Title** field, edit the title of the widget as necessary.
6. Select **Apply**.

Results

The widget has been added to the dashboard.

Print a dashboard

Print and save dashboards in PDF format using the built-in print-friendly option. Follow simple steps to generate a downloadable file for local storage or sharing.

Procedure

1. In the top navigation bar, select ☰ > **Dashboards**.

   Result: The Dashboards (on page 267) page opens.

2. Select the applicable dashboard.
3. In the top right section, select **Print mode**.

   Result: The page will show in a print-friendly format.

4. To save the file in *portable document format (PDF)* format, follow the standard procedure for your browser.

Results

The *PDF* file has been saved locally on your computer.

Chapter 13. Reports

*The **Reports** page shows all the reports that the sensors in your system have created.*

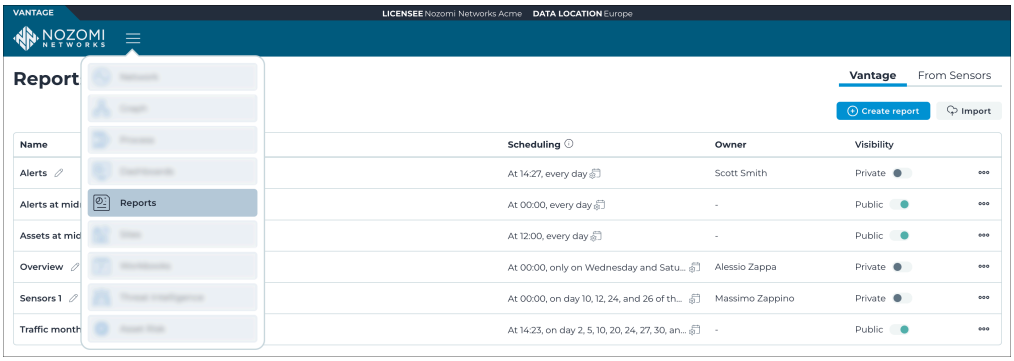


Figure 120. Reports page

The **Reports** page has these tabs:

- Vantage (on page 278)
- From Sensors (on page 284)

Related information

Create a report (on page 279)

Import a report (on page 282)

Export a report (on page 286)

Edit a report (on page 285)

Edit the settings of a report (on page 285)

Delete a report (on page 286)

Print a report (on page 283)

Vantage

*The **Vantage** page shows all the reports that have been created in Vantage.*

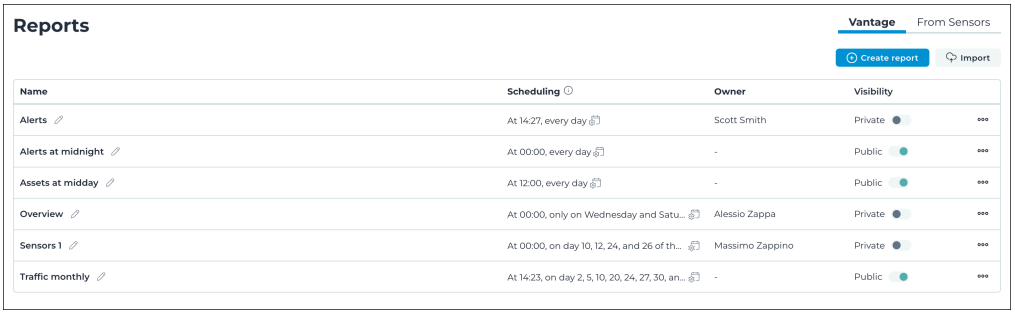


Figure 121. Vantage page

Create report

This lets you Create a report (on page 279).

Import

This lets you Import a report (on page 282).

Name

The name of the report. To modify the name, you can select the pencil icon, modify the name and select the tick icon.

Scheduling

The details of when the report is scheduled for creation.

Owner

The person that created the report.

Visibility

This toggle lets you choose whether the report is visible to a private or a public audience.

Actions menu

The actions menu gives you access to these options:

- Edit (on page 285)
- Settings (on page 285)
- Export (on page 286)
- Delete (on page 286)

Related information

From Sensors (on page 284)

Create a report

Learn how to create and schedule a custom report using predefined templates, recurrence settings, and visibility options in your organization.

About this task

The creation and scheduling of custom reports lets you streamline how critical information is shared within your organization. The use of predefined templates helps you quickly design reports tailored to specific needs, such as tracking vulnerabilities, monitoring traffic, or providing an overview of assets. The recurrence settings and visibility options make sure that the reports are generated on time and reach the correct audience, enhancing collaboration and decision-making across teams.

Procedure

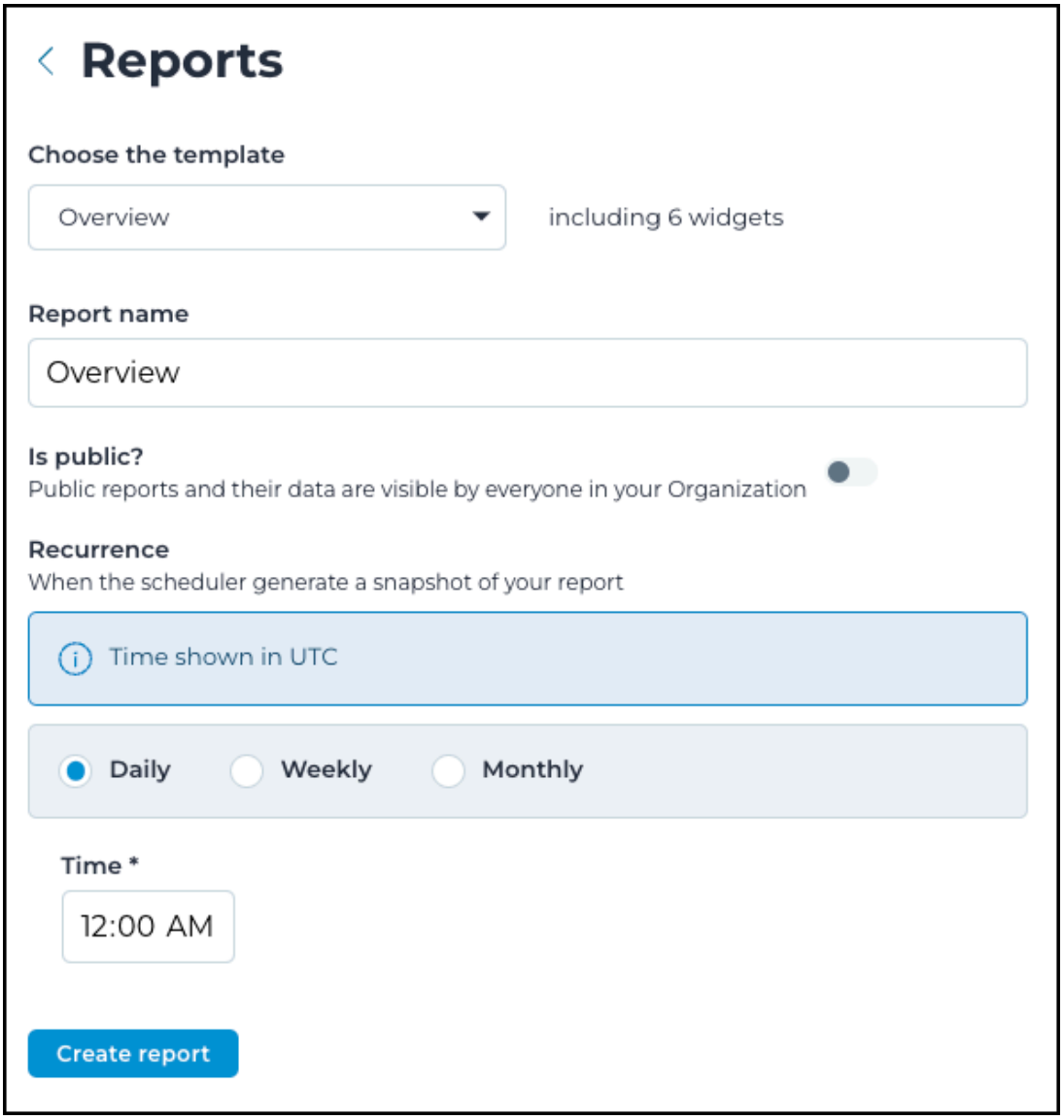
1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the top right corner, select **Create report**.

3. **Optional:**

   From the **Choose a template** dropdown, select an option.



   You can choose from these options;

   - Empty
   - Alerts
   - Assets
   - Overview
   - Sensors
   - Traffic
   - Vulnerabilities

4. In the **Report name** field, enter a name for the report.
5. **Optional:** To make the report visible to everyone in your organization, set the **Is public?** toggle to on.

6. In the **Recurrence** section, select one of these radio buttons:

   Choose from:

   - Daily
   - Weekly
   - Monthly

7. In the **Time** field, set the time that the report will be generated.
8. Select **Create report**.

Results

The report has been scheduled for creation.

Import a report

Learn how to import a report that was previously created in Vantage.

Procedure

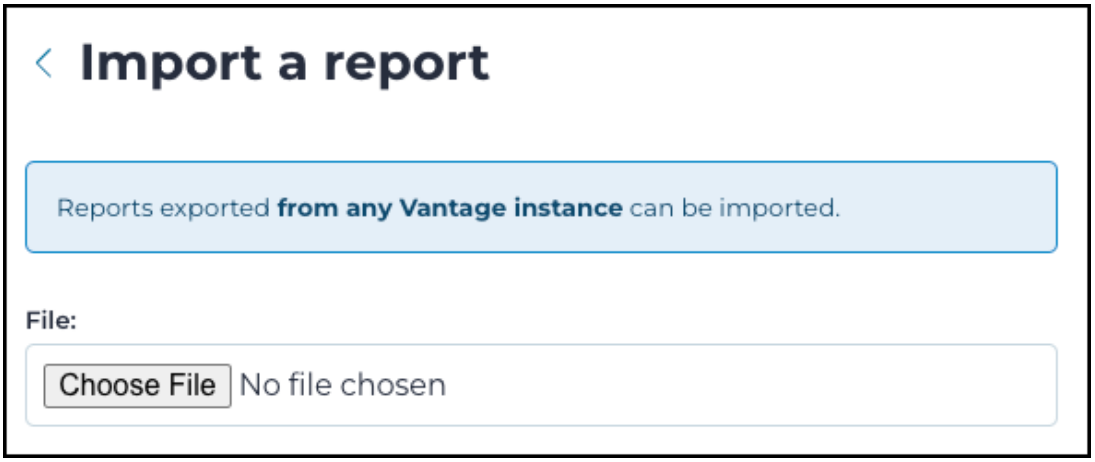
1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the top right corner, select **Import**.

   Result: The **Import a report** page opens.

3. Select **Choose File**.



4. Select the report file.

   The report will be in *JSON* format.

5. Select **Confirm**.

Print a report

Print and save reports in PDF format using the built-in print-friendly option. Follow simple steps to generate a downloadable file for local storage or sharing.

Procedure

1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. Select the applicable report.
3. In the top right section, select **Print mode**.

   Result: The page will show in a print-friendly format.

4. To save the file in *PDF* format, follow the standard procedure for your browser.

Results

The *PDF* file has been saved locally on your computer.

From Sensors

*The **From Sensors** page shows all the reports that have been created on sensors in your system.*

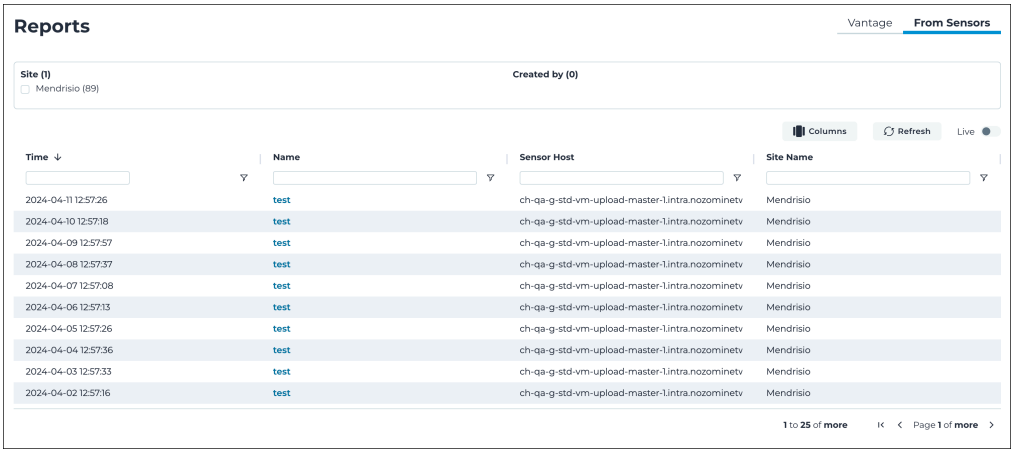


Figure 122. From Sensors page

Site

This shows the site location of the sensors that created the report.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Related information

Vantage (on page 278)

Table interactions

Actions menu

Edit a report

Learn how to use the actions menu to edit reports.

Procedure

1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the table, select the ••• icon.
3. Select **Edit**.

   Result: The report opens.

4. Edit the report as necessary.
5. Select **Apply**.

Results

The report has been edited.

Edit the settings of a report

Learn how to use the actions menu to edit the settings of a report.

Procedure

1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the table, select the ••• icon.
3. Select **Settings**.

   Result: The report opens.

4. Edit the report settings as necessary.
5. Select **Edit report**.

Results

The report has been edited.

Export a report

Learn how to use the actions menu to export reports.

Procedure

1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the table, select the ••• icon.
3. Select **Export**.

Results

The report downloads in *JSON* format.

Delete a report

You can use the actions menu to delete reports.

Procedure

1. In the top navigation bar, select ☰ > **Reports**.

   Result: The Reports (on page 275) page opens.

2. In the table, select the ••• icon.
3. Select **Delete**.

   Result: A dialog shows.

4. Select **OK**.

Results

The report has been deleted.

Chapter 14. Sites

*The **Sites** page shows all the geographical locations of the assets in your system. It lets you associate a site to one or more network domains. You can also add details such as the country or city of the site.*

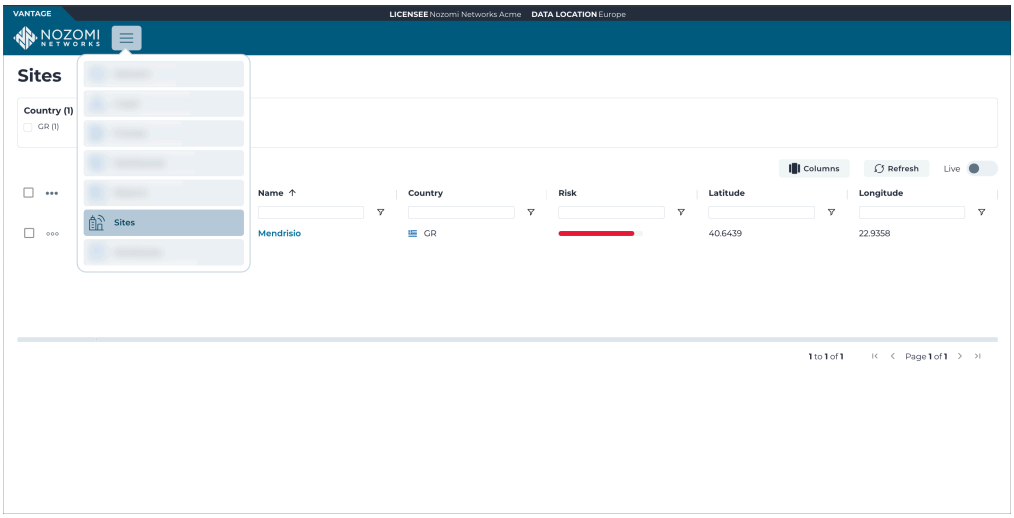


Figure 123. Sites page

Country

This shows a list of all the countries that are applicable for the sites in the current table view.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Table interactions

Actions menu

Export a site

You can use the actions menu to export sites.

Procedure

1. In the top navigation bar, select ☰ **> Sites**.

   Result: The Sites (on page 287) page opens.

2. Choose a method to open the actions menu.

   Choose from:

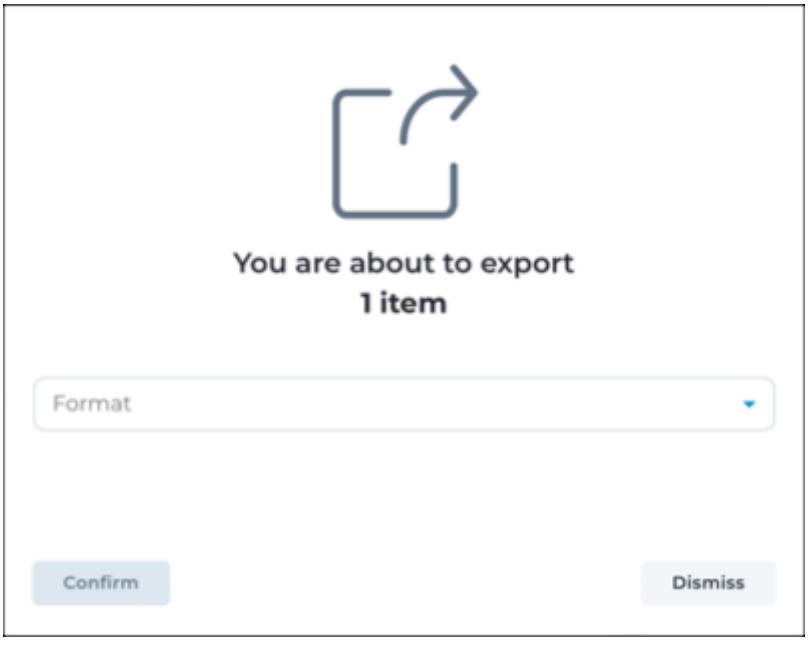
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

3. If you use the ••• icon in the table, choose a method to select one, or more, items.

   Choose from:

   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose

4. Select **Export**.

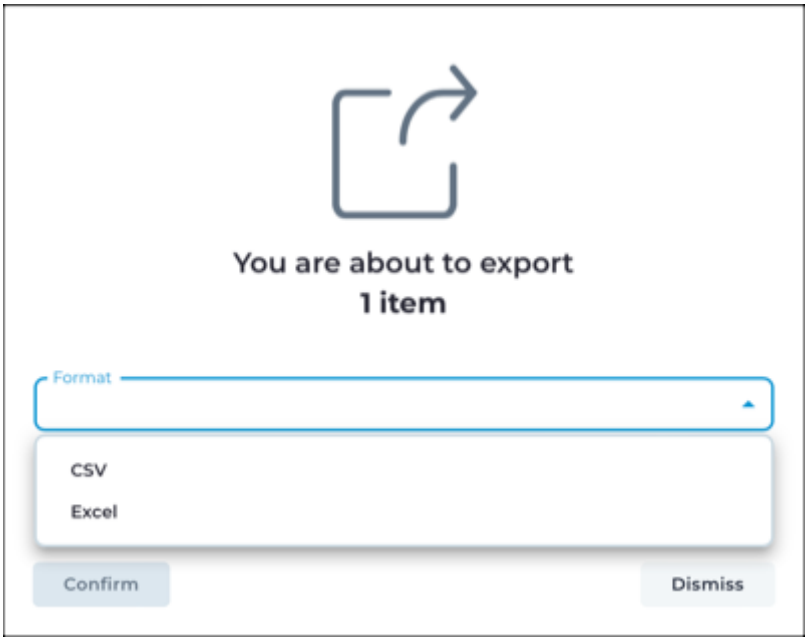


   Result: The export dialog shows.

5. Select the **Format** dropdown.

   Result: A dialog shows.

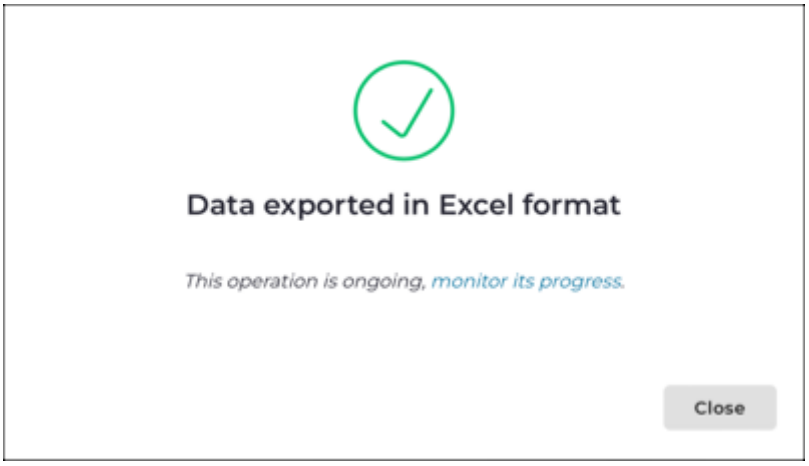
6. In the **Format** dropdown, select the format that you want to export.



7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.



Results

The site(s) has (have) been exported.

Chapter 15. Workbooks

*The **Workbooks** page shows recommended courses of action that can improve your network security. Generated through machine learning, workbooks highlight the vulnerabilities currently creating the highest risk exposure.*

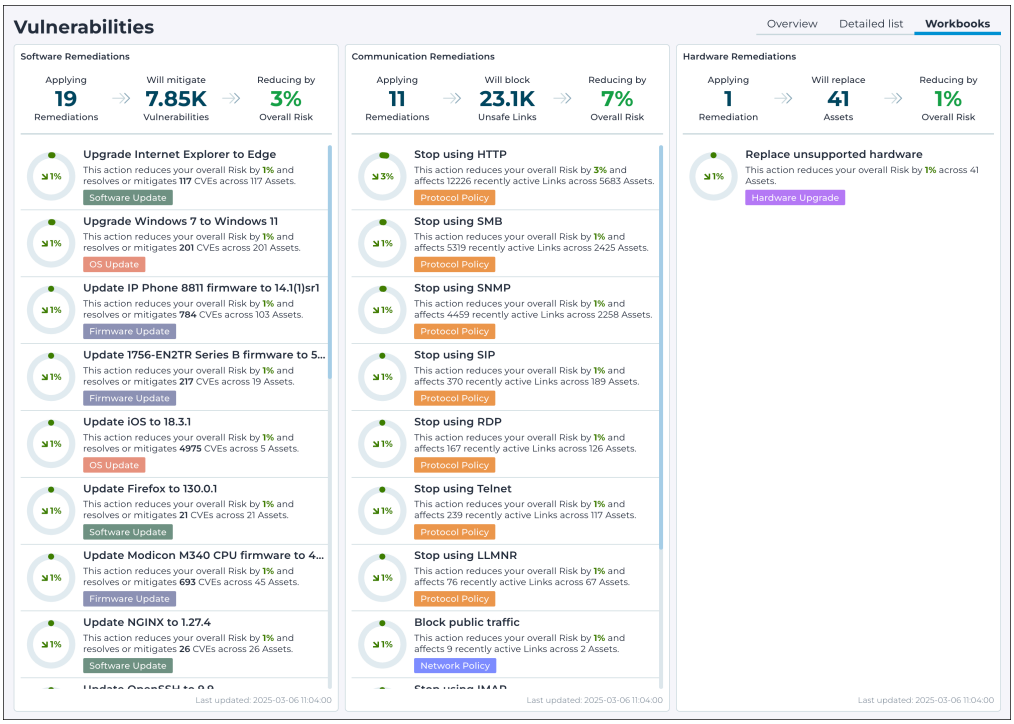


Figure 124. Workbooks page

Banner image

The banner image is a powerful visual report that uses bubble graphics to represent the relative impact of each workbook recommendation.

List

The list shows ranked recommendations, with the most effective actions at the top. For each workbook, Vantage shows:

- On the left, the highest risk score among all the vulnerabilities included in the workbook.
- A title that shows the recommended course of action.
- A description of the issue and the benefits of addressing it.
- In the top right corner of each workbook, Vantage shows:
  - An assessment of the risk reduction you will achieve if you follow the recommended steps. It is shown as a percentage.
  - The number of assets where the vulnerability was detected.
  - The number of *CVE* that you would address if you follow the recommended steps.

Related information

Use a workbook to improve your network security (on page 296)

Use a workbook to improve your network security

When workbooks make recommendations, you should use them to improve your network security.

Procedure

1. In the top navigation bar, select ☰ > **Workbooks**.

   Result: The Workbooks (on page 201) page opens.

2. Make a note of the description in the largest bubble in the banner image.

   > **Note:**
   > This workbook also shows at the top of the list of workbooks below.

3. Choose a method with which to open the list of vulnerabilities that you can address.

   Choose from:

   - In the banner image, select the largest bubble.
   - In the list, select **Review** to the right of a workbook.

4. Resolve the vulnerability (on page 199).

   > **Note:**
   > You should create a plan to take the recommended action. For example, a workbook might recommend that you upgrade all assets that run an old application version. In this case, you should create a maintenance schedule and take the necessary steps to update those applications to the latest, secure version.

Related information

Workbooks (on page 201)

Chapter 16. Threat Intelligence

*The **Threat Intelligence** page shows an overview of all of the available threat cards and categories. It also lets you filter the threat cards to show only malware, threat actors, or vulnerabilities*

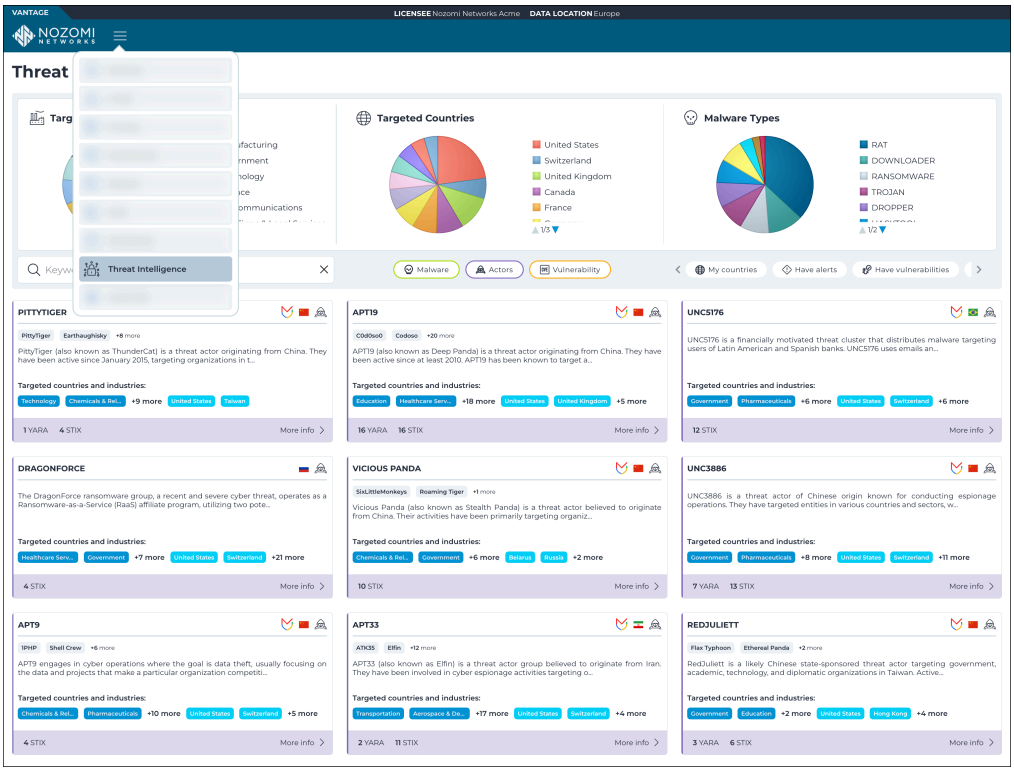


Figure 125. Threat Intelligence page

Targeted Industries

This section lets you filter cards based on any of the selected industries in the chart.

Targeted Countries

This section lets you filter cards on any of the selected countries.

Malware Types

This section lets you select which types of malware show.

Search bar

This lets you search the Threat Intelligence based on these attributes:

- Aliases
- Description
- Filenames
- Malware types
- Name
- Origin country
- *Structured Threat Information Expression (STIX)* domains
- *STIX IP* addresses
- *STIX URL*s

- Targeted country
- Targeted industry
- Trigger *IDs*
- *STIX* hashes

Malware
This button lets you filter malware cards based on any of the selected types. For more details, see Malware (on page 301).

Actors
This button lets you filter the content that shows below to only threat actors. For more details, see Actors (on page 303).

Vulnerability
This button lets you filter the content that shows below to only vulnerabilities. This section shows all known *CVEs*. For more details, see Vulnerability (on page 305).

My countries
This button lets you filter the threat cards to show only content that is relevant for the countries that your organization has sites in.

Have alerts
This button lets you filter the threat cards to show only content that have associated alerts.

Have vulnerabilities
This button lets you filter the threat cards to show only content that have associated vulnerabilities.

High risk
This button lets you filter the threat cards to show only content that have a high risk score.

Actively exploited
This button lets you filter the threat cards to show only vulnerabilities that are known to have been exploited.

Threat cards
For more details, see:

- Malware threat cards (on page 301)
- Actors threat cards (on page 303)
- Vulnerability threat cards (on page 305)

Malware

*Learn how the **Malware** page shows malware-specific attributes and associated threat cards.*

Malware filter

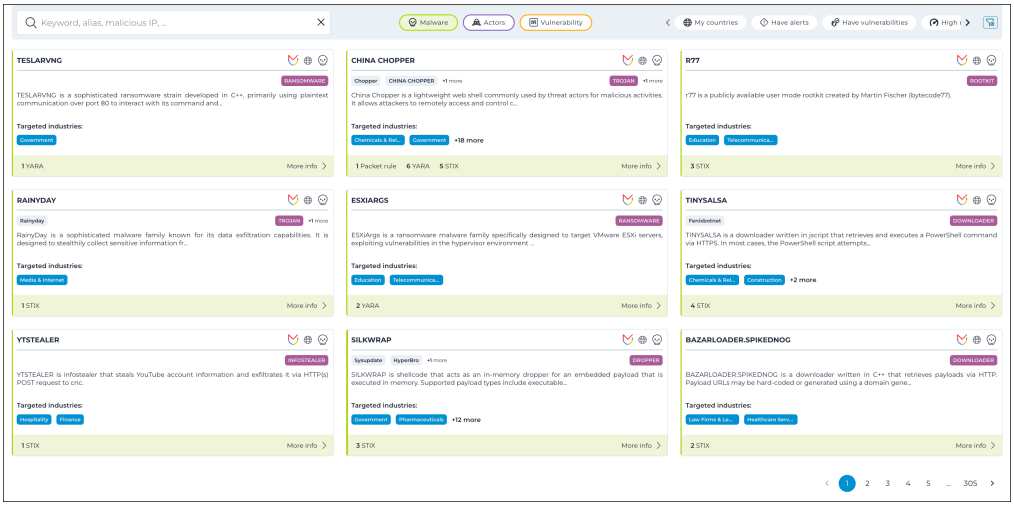


Figure 126. Malware filter applied

You can use the **Malware** button to show only malware-related threat cards.

Threat card

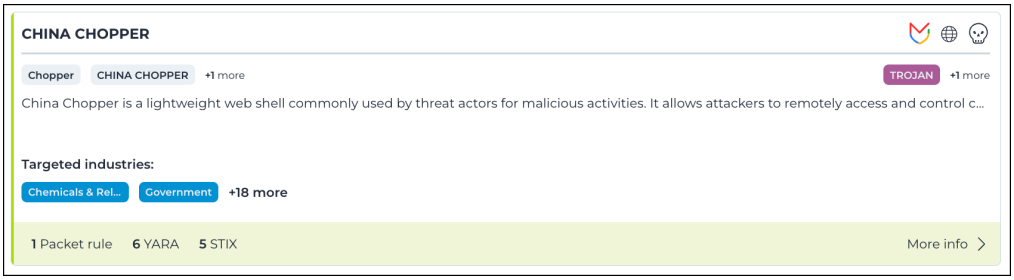


Figure 127. Malware threat card

A malware threat card can show all, or some, of these attributes:

- The name of the malware
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- This icon shows that the malware is global
- This icon shows the number of related alerts
- This icon indicates it is a malware-related threat card
- RANSOMWARE Shows the type of malware
- A description section

- The industries that the malware is known to have targeted
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page

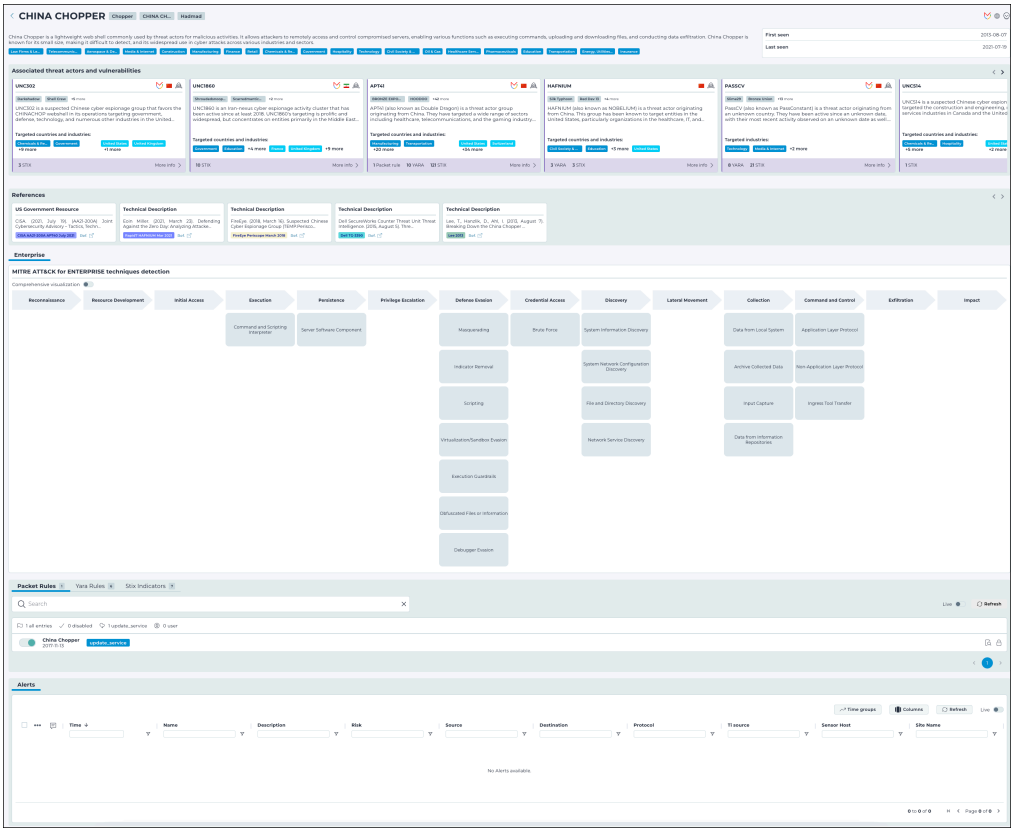


Figure 128. Details page

Actors

*Learn how the **Actors** page shows threat actor-specific attributes and associated threat cards.*

Actors filter

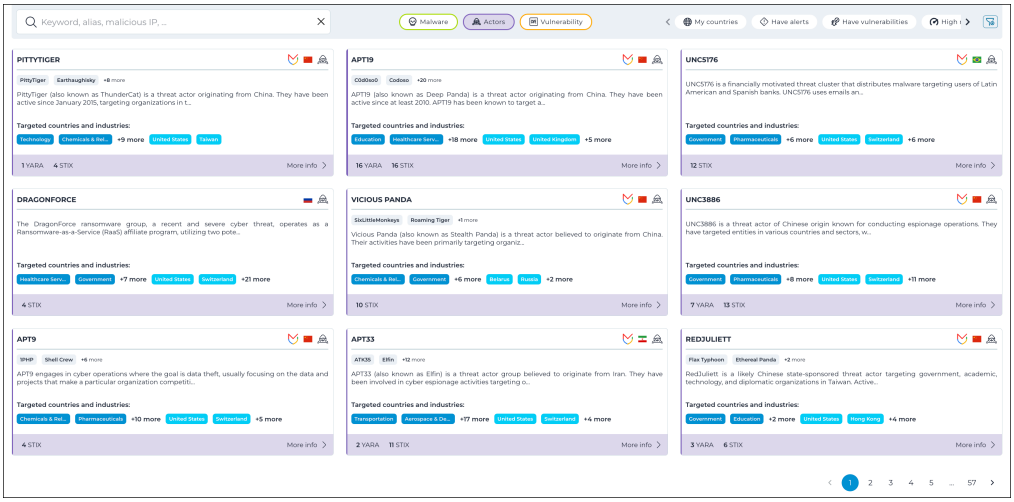


Figure 129. Actors filter applied

You can use the **Actors** button to show only actors-related threat cards.

Threat card

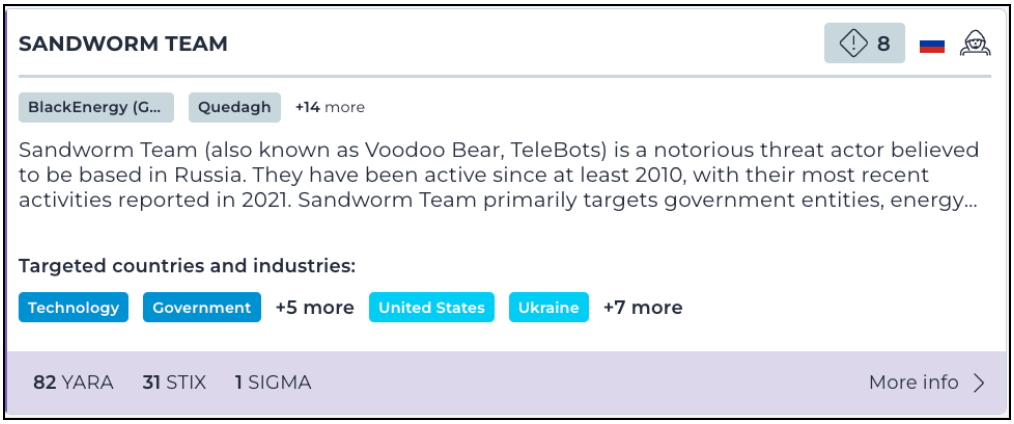


Figure 130. Actors threat card

An actor threat card show all, or some, of these attributes:

- The name of the threat actor
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- A flag will show the origin country
- This icon shows the number of related alerts

- Indicates it is a actor-related threat card
- RANSOMWARE Shows the type of malware
- A description section
- The countries and industries that the malware is known to have targeted
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page

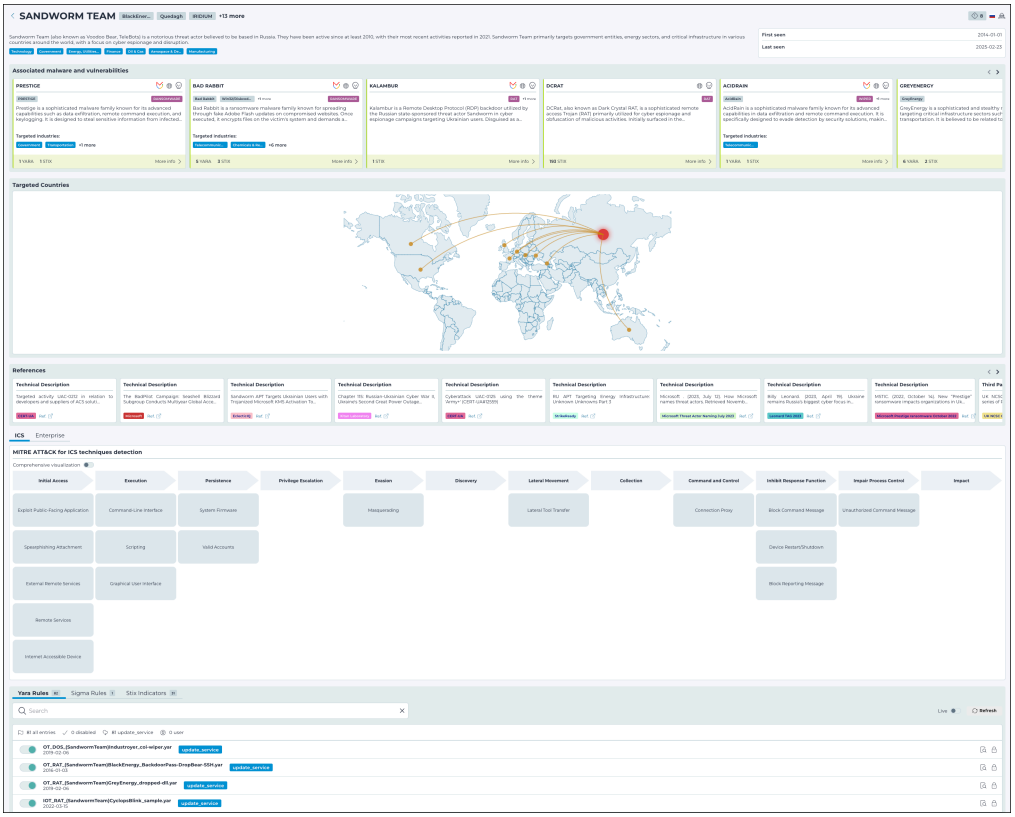


Figure 131. Details page

Vulnerability

*Learn how the **Vulnerability** page shows vulnerability-specific attributes and associated threat cards.*

Vulnerability filter

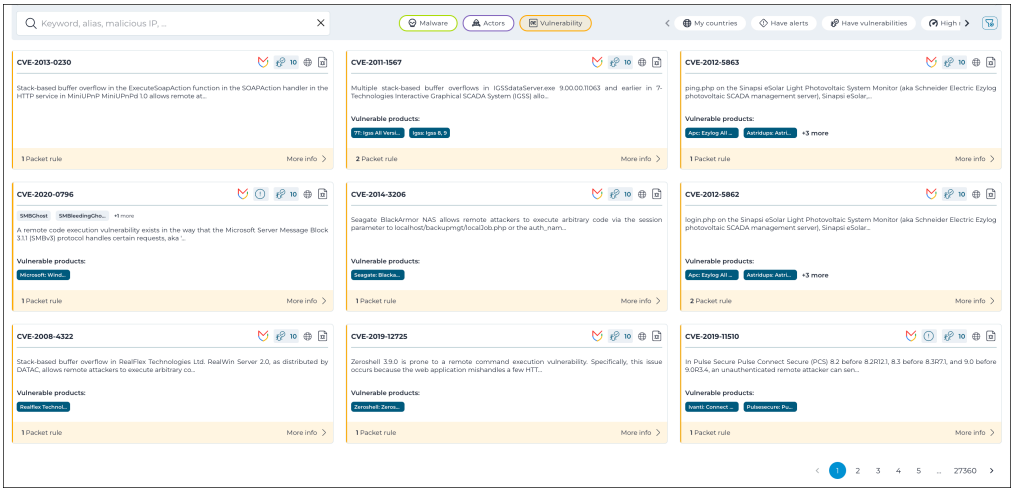


Figure 132. Vulnerability filter applied

You can use the **Vulnerability** button to show only vulnerability-related threat cards.

Threat card

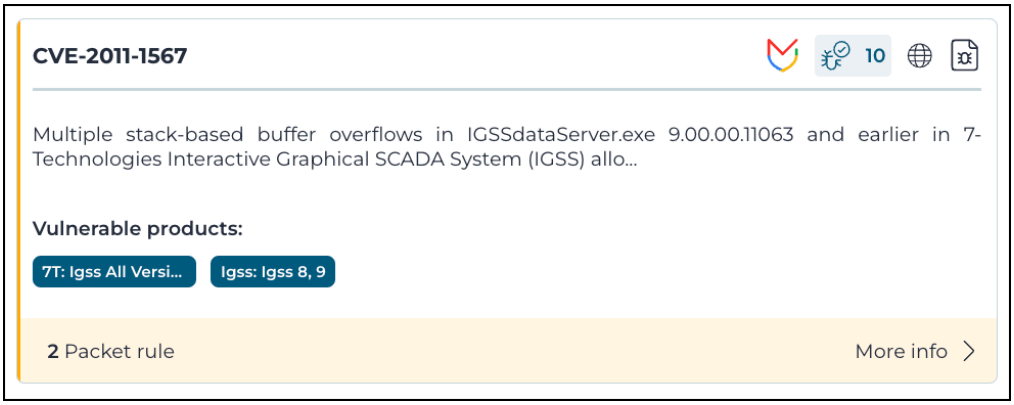


Figure 133. Vulnerability threat card

A vulnerability threat card show all, or some, of these attributes:

- The name of the vulnerability
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- This icon shows that the vulnerability is global
- This icon shows the *CVSS* score
- This icon indicates that it is a vulnerability-related threat card

- A description section
- The products that are vulnerable
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page

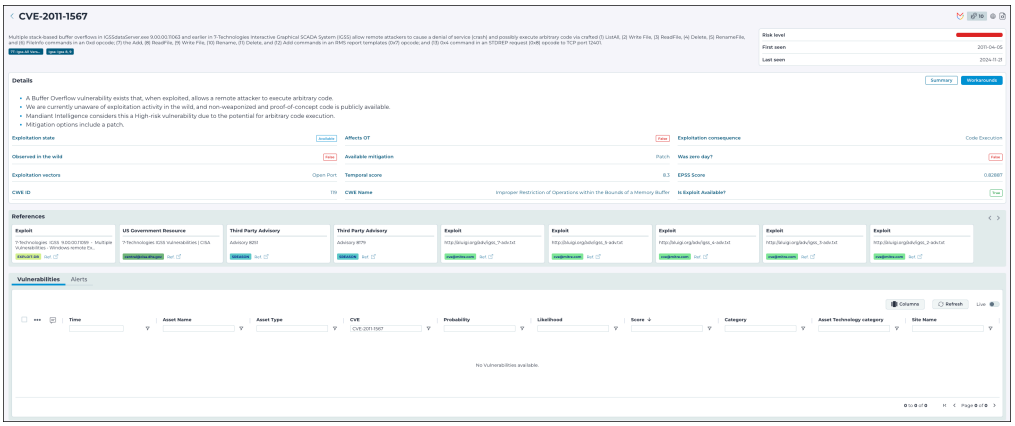


Figure 134. Details page

Chapter 17. Asset Risk

*The **Asset Risk** page provides an in-depth view of asset risk levels. This includes an overview, detailed analysis, and benchmark comparisons to help assess and manage risks effectively.*

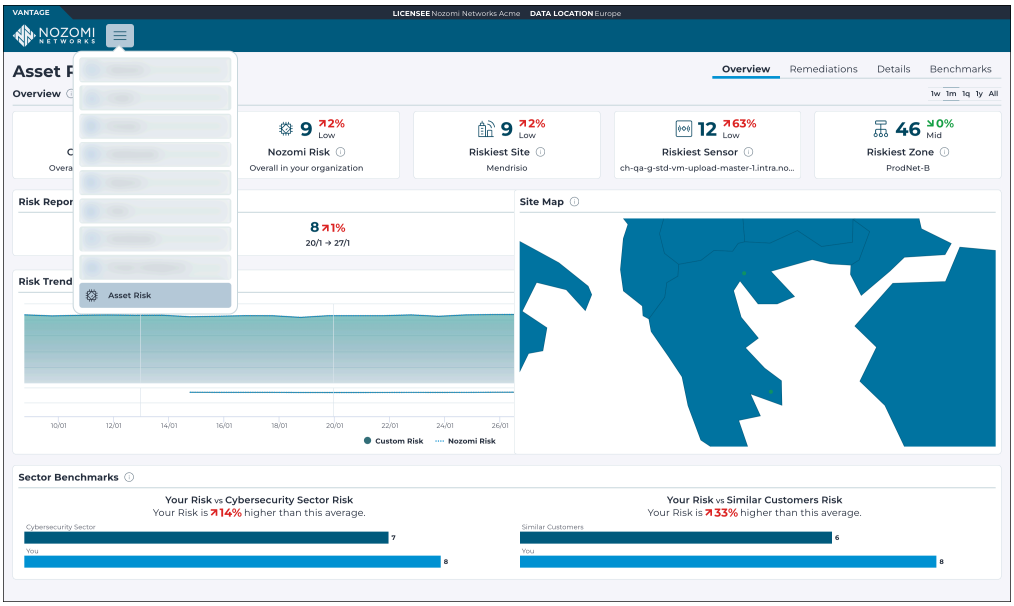


Figure 135. Asset Risk page

The **Asset Risk** page has these tabs:

- Overview (on page 310)
- Remediations (on page 312)
- Details (on page 313)
- Benchmarks (on page 315)

Overview

*The **Overview** page lets you analyze your risk position over time and compare it to the average risks of your industry and similar customers.*

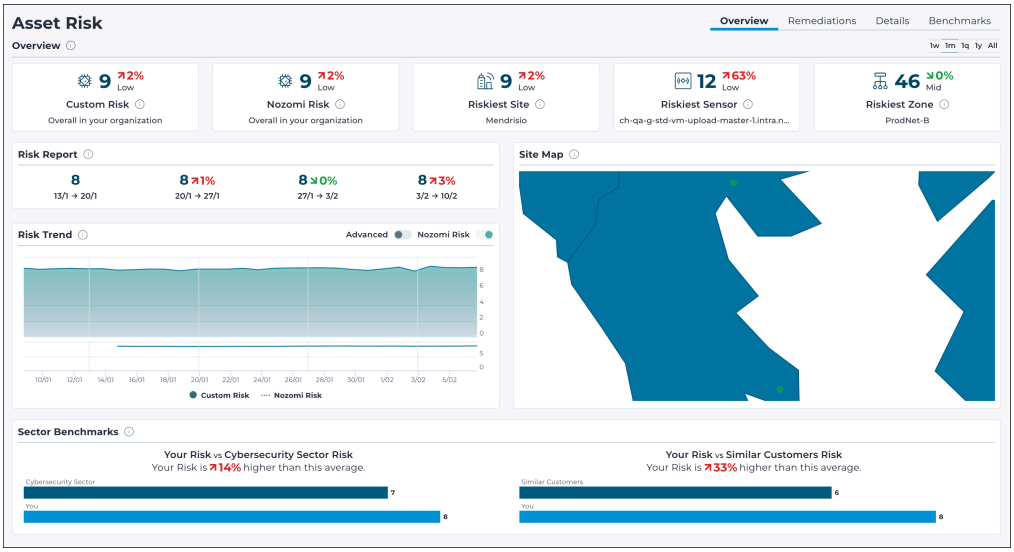


Figure 136. Overview page

Custom Risk
The overall risk, which is based on your specific risk formula.

Nozomi Risk
This is based on the standard Nozomi risk formula.

Riskiest Site
This shows the site in your organization that has the highest risk.

Riskiest Sensor
This shows the sensor that has the highest risk based on your specific risk formula.

Riskiest Zone
This shows the zone that has the highest risk based on your specific risk formula.

Risk Report
This shows the average risk values in the selected time frame.

Risk Trend
This lets you monitor the trends of both your overall risks, as well as Nozomi risks over time.

Site Map
This lets you evaluate the risk positions of your different sites.

Sector Benchmarks
This lets you compare your Nozomi risk industry sectors and similar customers.

Related information

Remediations (on page 312)
Details (on page 313)
Benchmarks (on page 315)

Remediations

*The **Remediations** tab provides an overview of the remediation actions you can take to reduce asset risks.*

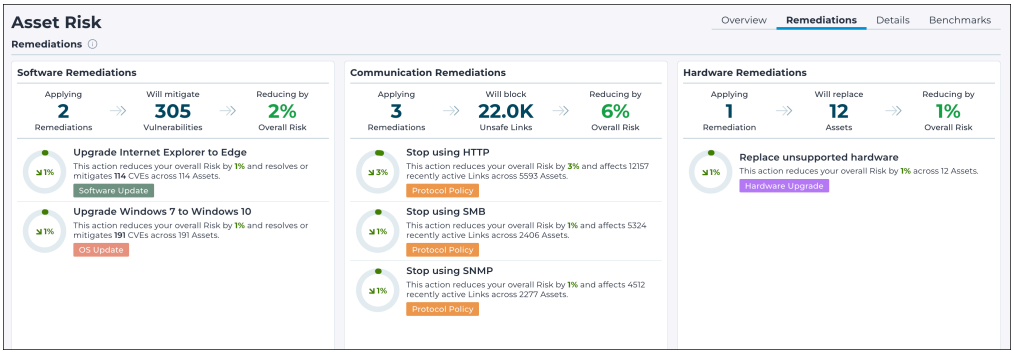


Figure 137. Remediations Overview

Software Remediations

These actions address software risks related to your assets.

Communication Remediations

These actions address network protocol risks related to your assets.

Hardware Remediations

These actions address hardware risks related to your assets.

Related information

Overview (on page 310)

Details (on page 313)

Benchmarks (on page 315)

Details

*The **Details** page provides an in-depth analysis of asset risks, highlighting the riskiest sites, sensors, and zones, along with detailed information about their associated assets.*

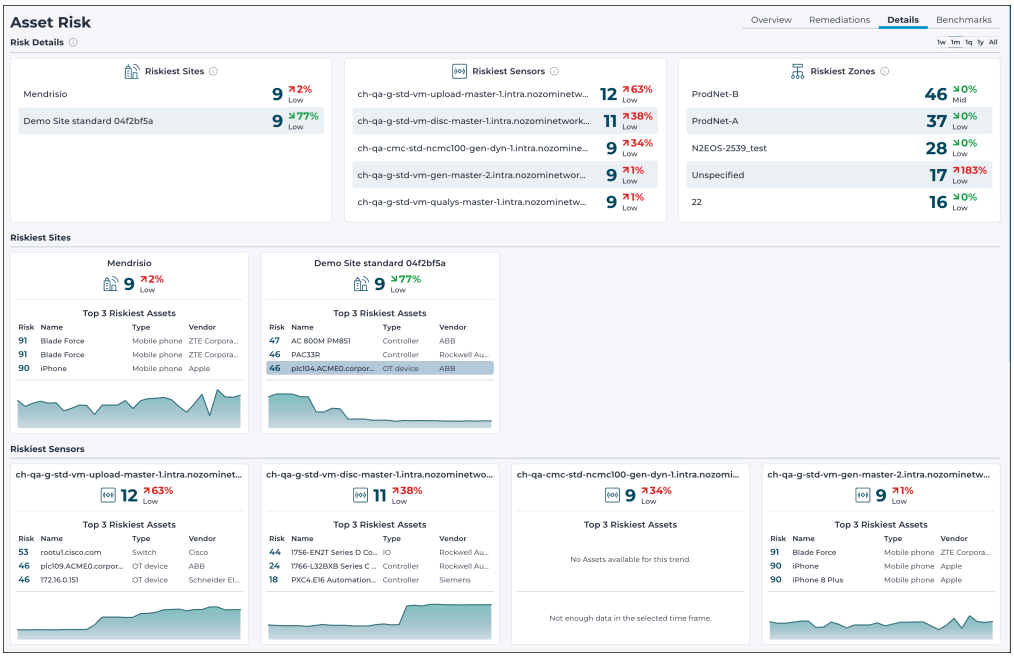


Figure 138. Details page

This pages shows a more in-depth view of data that is shown in the Overview (on page 310) page.

Risk Details

This shows a summary view for the categories below.

Riskiest Sites

This shows more details for the riskiest site, and the top three riskiest sensors in it. Each tile shows the:

- Risk
- Name
- Type
- Vendor

You can select an asset to open the related details page.

Riskiest Sensors

This shows the sensors that have the highest risk levels and the riskiest assets connected to the sensor. Each tile shows the:

- Risk
- Name

- Type
- Vendor

Riskiest Zones

This shows the zones that have the highest risk levels and the riskiest assets in the zone. Each tile shows the:

- Risk
- Name
- Type
- Vendor

Related information

Overview (on page 310)

Remediations (on page 312)

Benchmarks (on page 315)

Benchmarks

*The **Benchmarks** page lets you compare your organization's risk levels against industry sectors and similar customers to evaluate your security posture.*

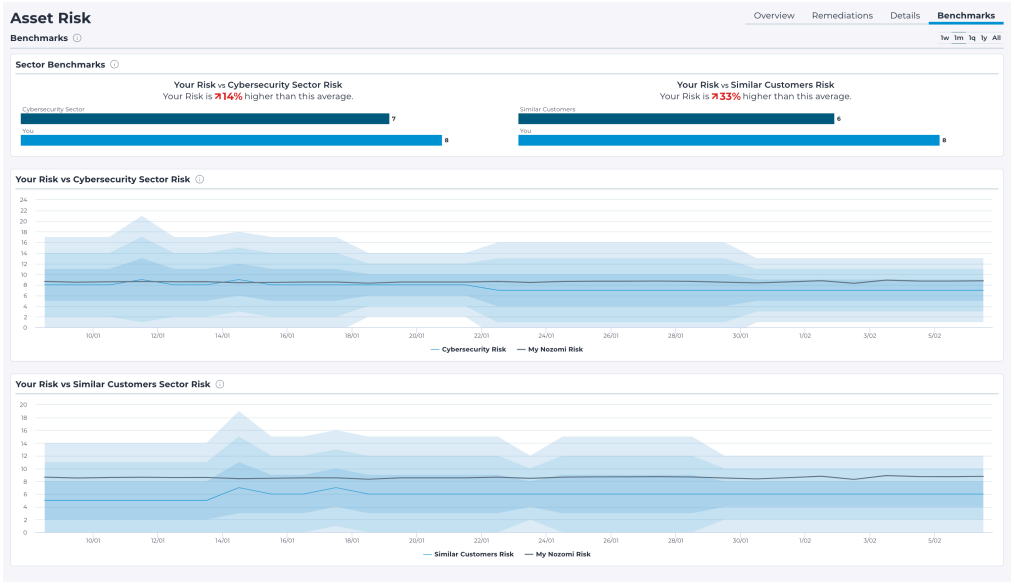


Figure 139. Benchmarks page

Related information

Overview (on page 310)

Remediations (on page 312)

Details (on page 313)

Chapter 18. Smart Polling

Smart Polling provides a centralized interface for creating, managing, and monitoring polling plans within your organization. It helps you streamline data collection and control monitoring activities from one location.

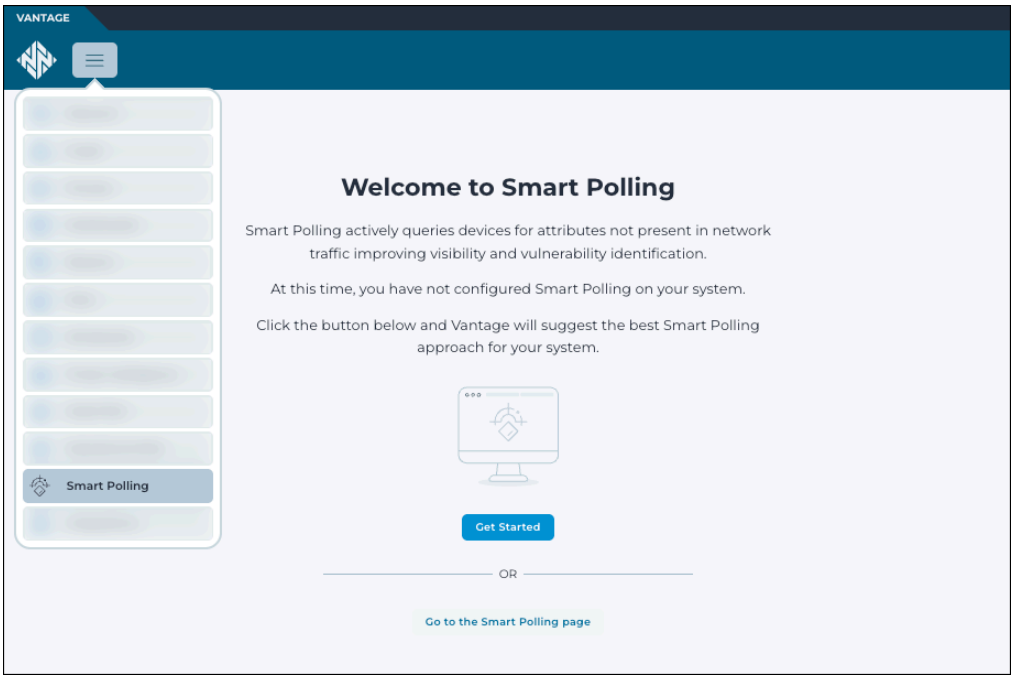


Figure 140. Smart Polling welcome page

The first time that you open the Smart Polling page, when no Smart Polling plans have been created for your organization, the welcome page shows.

The welcome page lets you choose from these two options:

- **Get Started** to Automatically add a Smart Polling plan from the onboarding page (on page 326)
- **Go to the Smart Polling page** to:
  - Add a Smart Polling plan that requires credentials (on page 330), or
  - Add a Smart Polling plan that does not require credentials (on page 333)

Once your organization has at least one Smart Polling plan, you no longer see the welcome page. Instead, the **Overview** page shows. Accept the suggestions in the plans list on this page to create progressive mode plans. For more details, see Overview (on page 320).

Vantage shows progressive plans from connected sensors and lets you merge duplicates into a single plan managed from Vantage. For more details, see Centralized plan management (on page 336).

Overview

Learn how Smart Polling plans are displayed, managed, and executed in the Vantage platform. This includes understanding plan statuses, how to add or search for plans, and how to interpret result data. Icons and table fields provide insight into device polling outcomes and plan performance. Plans can be defined in Vantage, but are executed in Guardian sensors, or Arc sensors that are connected to Guardian. Vantage receives the result of those executions via the usual synchronization process.

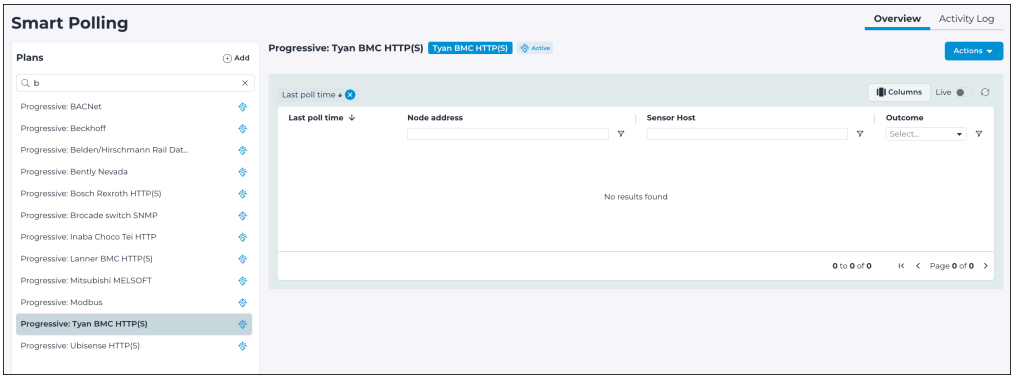


Figure 141. Populated Plans page

Plans

The **Plans** section shows a list of all the Smart Polling plans that have been added for your organization. The icons show the current status of the plan:

- : Active
- : Paused

Progressive plans from connected sensors are also shown here. You can merge duplicate progressive plans into a single plan managed from Vantage. For more details, see Centralized plan management (on page 336).

Add button

The **Add** icon lets you add a new Smart Polling plan.

Search field

The search field lets you easily find a specific Smart Polling plan.

Results

Once a Smart Polling plan has been executed, the results will show on the **Overview** page. When you select a specific plan, the table will show the:

- Status of the plan through the `ACTIVE` | `INACTIVE` indicator
- Result of the last polling of each node polled within the last two weeks

The table columns will show:

- **Node address**: The *IP* address of the node that was detected
- **Sensor Host**: The name of the sensor

- **Last poll time**: The time since the last execution of the plan for that node
- **Outcome**: The result of the last execution of the plan, which can be:
  - `Successful`: Smart Polling was able to poll the host and enrich the corresponding asset
  - `No connection`: Verify that the device is up, its services are running, that the sensor has a route to that host and no firewall is blocking the connection
  - `Missing credentials`: Add the credentials to the **Credentials Manager**
  - `Wrong credentials`: Update the credentials in the **Credentials Manager**
  - `Inconclusive`: This device is unsupported or only partly supported by Smart Polling
  - `Unsupported`: This strategy is not supported by the sensor that tried to poll the device
  - `Queued`: The sensor has not yet picked up the node for execution
  - `Denied`: The node lies in a subnet that Smart Polling does not have the permission to reach

For more details about the additional information that Smart Polling can provide, see Smart Polling results (on page 343).

Suggestions

Vantage regularly analyzes your organization and adds recommended Smart Polling plans to the **Suggestions** section based on the results. If there are no suggestions, this section will not show.

Plan creation

Learn how to create a Smart Polling plan by choosing a strategy, defining parameters, adding targets and credentials, and scheduling when data collection runs. Customize each step to control how and when your sensors gather information. Use recurrence or interval scheduling to automate plan execution.

Select the ⊕ **Add** icon to enter the plan creation wizard.

Strategy

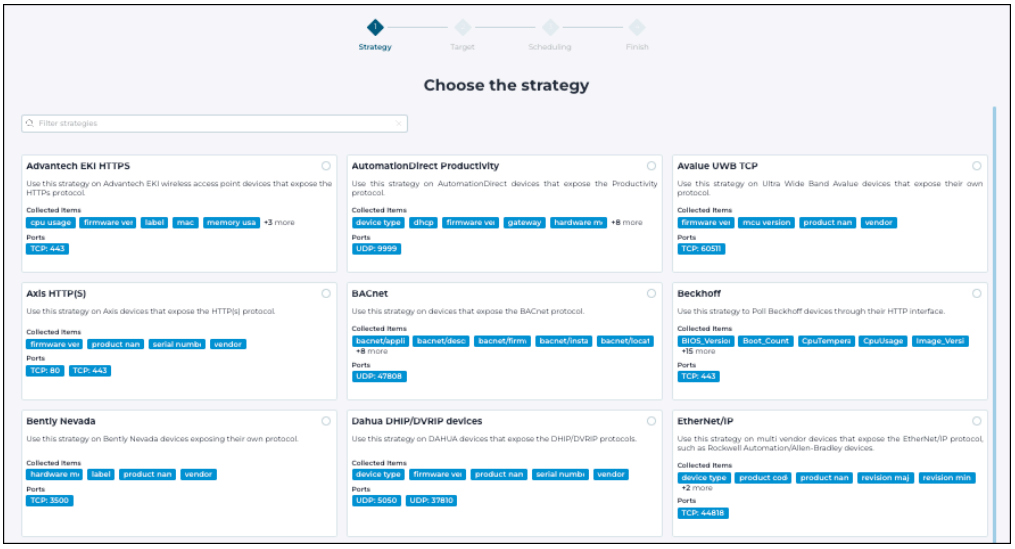


Figure 142. Choose the strategy page

Filter strategies: This field lets you enter text to easily find a specific strategy.

All available strategies show on the page with a summary. The summary section shows the:

- Name of the strategy
- A description of when it is useful to use the strategy
- The information that is collected
- Ports used

Parameters

Customize the plan with parameters used by the selected strategy, such as the port to use. Not all strategies accept parameters, in which case this step is skipped.

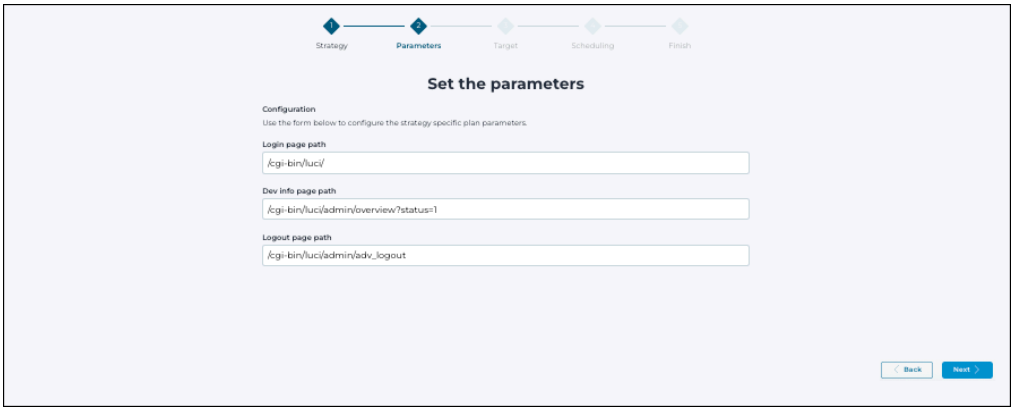


Figure 143. Parameters page

Target

Some of the strategies that are available require you to enter the related credentials. Therefore, there are two possible versions of the **Target** page that can show.

Figure 144. Target page (Query version shown)

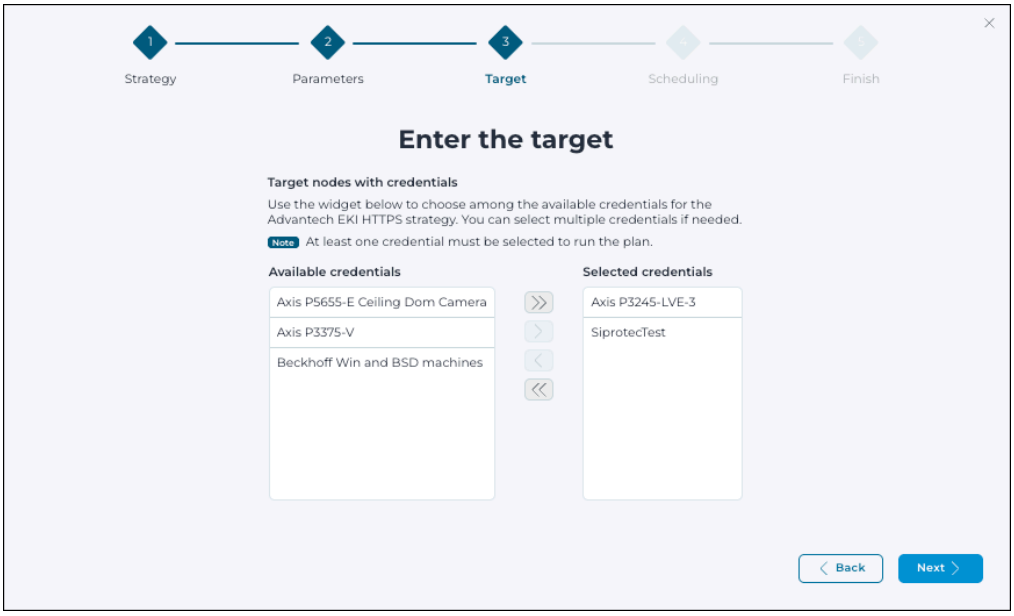


Figure 145. Target page (Credentials version shown)

For strategies that require credentials, you must select one, or more, of the available credentials that show in the panel on the left. To move the credentials to the panel on the right, you can use the:

- > icon to select one credential
- >> icon to select all credentials

Scheduling

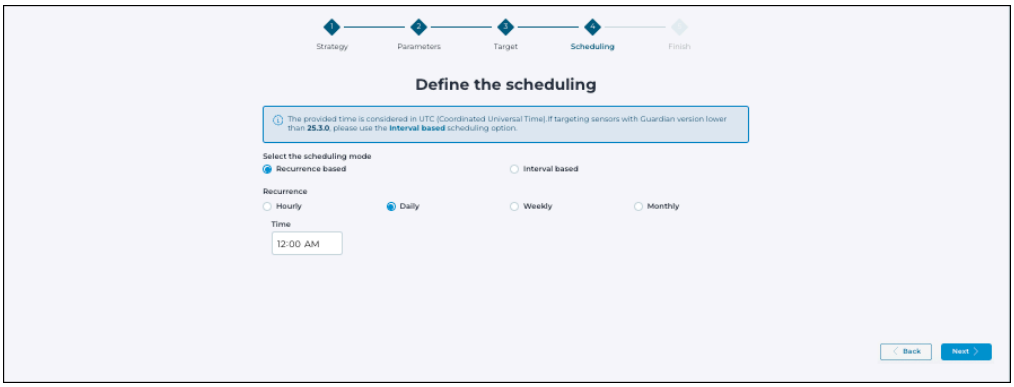


Figure 146. Scheduling page

Recurrence based: When this is selected, you can choose from these options:

- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**

Sensors that are *N2OS* v25.2.0 or lower do not fully support recurrence-based scheduling. However, if you have sensors with one of these older versions of *N2OS*, and you create a recurrence-based plan, there is a workaround. Under these circumstances, Vantage will still request that the sensor runs the plan at the desired frequency, but in a slightly different way. For example, if you choose the hourly-based scheduling, it will run the plan once an hour, but not necessarily at the minute that you specified. The same will happen if you selected the daily recurrence.

If you selected the weekly or monthly recurrence, the plan will be run once per week or month, regardless of whether you specified a single day or multiple days.

Time: You then must set the time that the Smart Polling plan will be executed. The time is set in *coordinated universal time (UTC)*.

Interval based: When this is selected, the sensors will run the plan immediately. Subsequently, it will run once at every interval. For example, if your interval is **Every 1 Day(s)**, and the current time is 10:15, then the plan will run immediately, and then every day at 10:15.

Finish

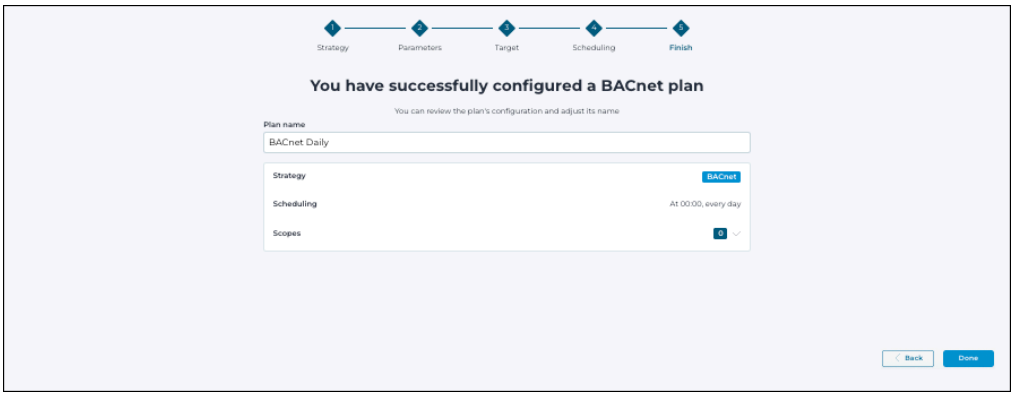


Figure 147. Finish page

On the **Finish** page, you can edit the **Plan name**, and configure **Scopes**.

If you select the arrow in the **Scopes** section, you can choose one of these options:

- Tag
- Site
- Sensor

Once you have made your selection, the number of item will show next to the arrow.

Automatically add a plan

Automatically add a Smart Polling plan from the onboarding page

*Use the **Get Started** button on the onboarding page to automatically create one or more Smart Polling plans.*

About this task

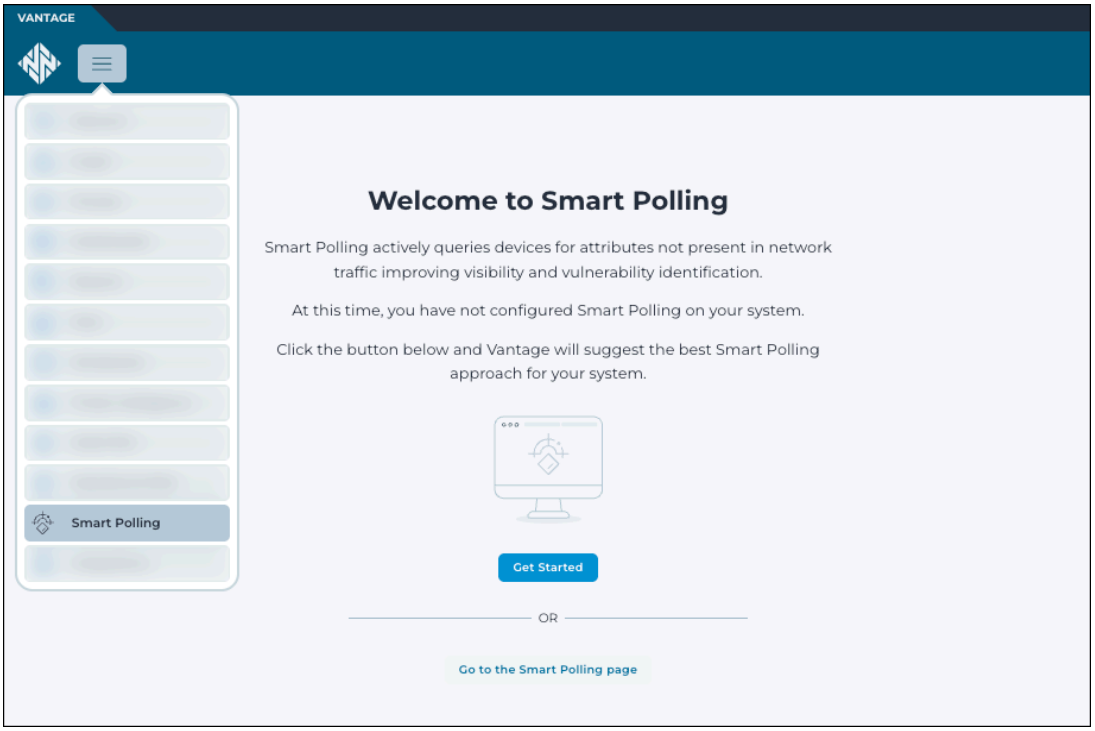
You will only see the onboarding page if no Smart Polling plans currently exist for your organization.

Procedure

1. In the top navigation bar, select ☰ **> Smart Polling**.

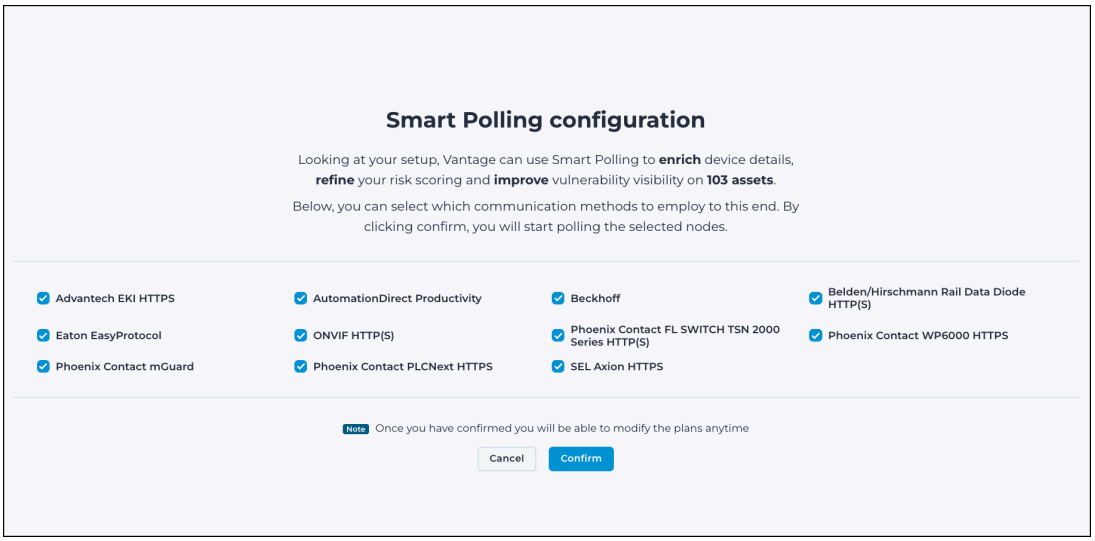
   Result: The **Smart Polling** page opens.

2. On the welcome page, select **Get Started**.



   Result: The **Smart Polling configuration** page opens. It will show a summary of what Vantage has detected in your environment, and the possible options that you can take.

3. Select one or more of the strategies that have been suggested.



4. Select **Confirm**.

Results

The Smart Polling plan(s) has (have) been added and they will run automatically.

Automatically add a Smart Polling plan from the suggestions section

*Use the **Suggestions** section on the **Smart Polling Plans** page to automatically create one or more Smart Polling plans.*

About this task

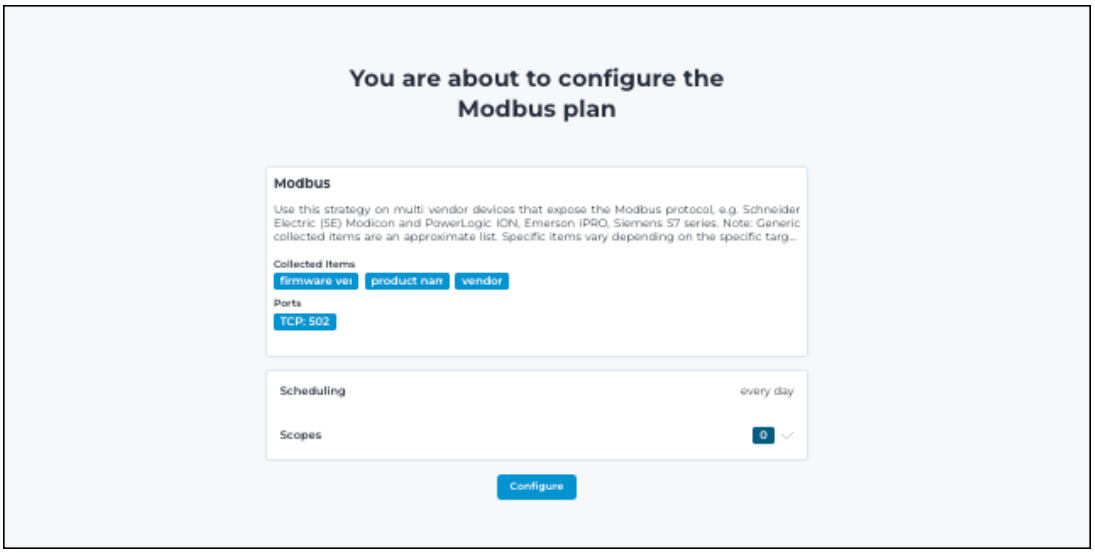
Use this process to create Smart Polling plans that automatically find the optimal target. This method allows for a single-click definition of plans that collect data from devices that the Nozomi Networks solution already recognizes in the environment.

Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. To select one of the strategies that have been suggested, in the bottom left corner, select the related ⚙ icon.



3. **Optional:** Expand the **Scopes** section and select **Add Scope**.
4. Select an option:

   Choose from:

   - Tag
   - Site
   - Sensor

   Result: A dialog shows.

5. Select one tag, site, or sensor.

   The option will depend on what you selected in the previous step.

6. Select **Configure**.

Results

The Smart Polling plan has been added and it will run automatically.

What to do next

If necessary, do the procedure above again for one or more of the other Smart Planning plans in the **Suggestions** section.

Manually add a plan

Add a Smart Polling plan that requires credentials

Create a Smart Polling plan that uses a strategy that requires credentials. Choose specific or all credentials, configure a schedule, and define the scope before completing the setup.

Before you begin

Make sure that the correct credentials for the Smart Polling plan you are about to add are in the **Credentials Manager**.

About this task

Use this process to create a Smart Polling plan that targets systems requiring authentication. This method allows the platform to access and collect data from sources that need credentials. You can configure the schedule and scope of the plan to suit your operational needs.

Procedure

1. In the top navigation bar, select ☰ **> Smart Polling**.

   Result: The **Smart Polling** page opens.

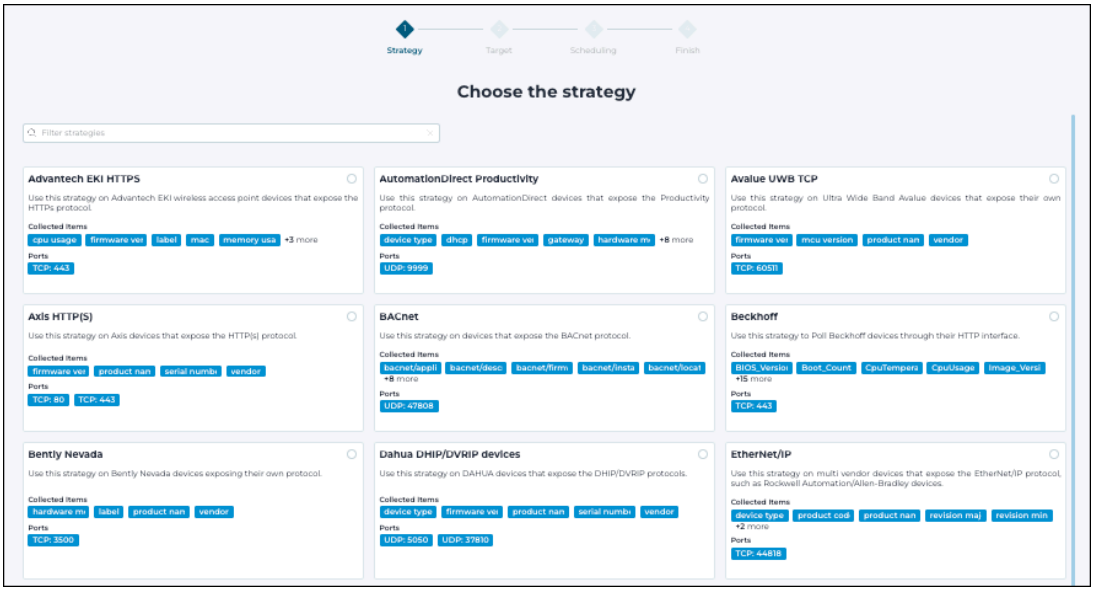
2. If the welcome page shows, select **Go to the Smart Polling page**.

3. On the **Smart Polling** page, select the ⊕ **Add** icon.

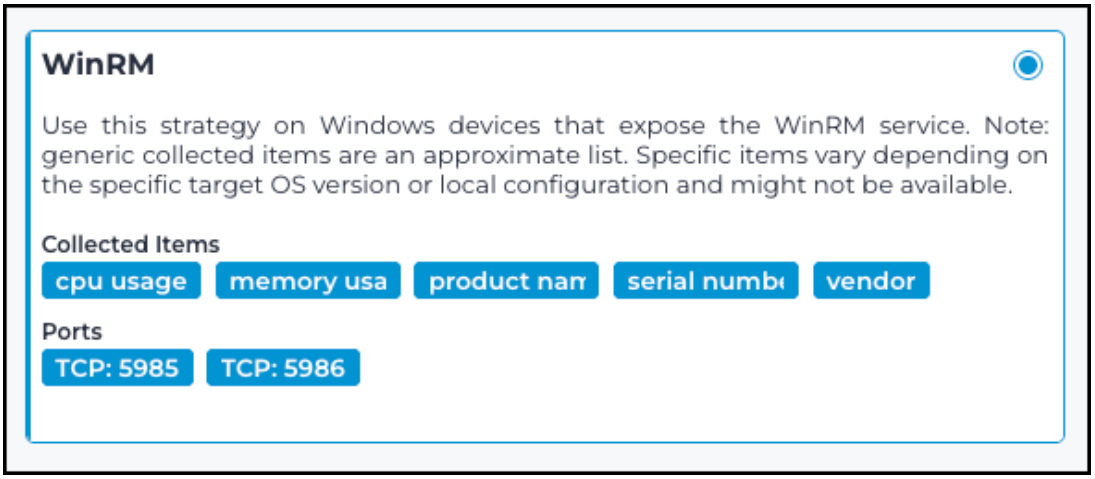
   Result: The **Choose the Strategy** page opens.

4. **Optional:**

   To find the correct strategy, enter text in the **Filter strategies** field.



5. In the top right corner of the relevant strategy, select the radio button.



6. Select **Next**.

   Result: Either the **Parameters** page or the **Target** page will show.

7. **Optional:** If the **Parameters** page shows, enter the necessary details.
8. Select **Next**.

   Result: The **Target** page will show.

9. From the **Available credentials** panel on the left, select the applicable credential.

10. Choose an option:

    Choose from:

    - To select one credential, select the > icon.
    - To select all the available credentials, select the >> icon.

11. Select **Next**.

    Result: The **Scheduling** page will show.

12. On the **Scheduling** page, select a scheduling type:

    > **Important:**
    > The **Recurrence based** option requires *N2OS* v25.3.0 or later. The **Interval based** option is available in all versions.

    Choose from:

    - Select **Interval based** to poll at a fixed interval
    - Select **Recurrence based** to poll at a specific frequency and time (requires *N2OS* v25.3.0 or later)

13. Configure the schedule:

    Choose from:

    - If you chose **Recurrence based**, set the frequency and the time
    - If you chose **Interval based**, set the interval

14. Select **Next**.

    Result: The **Finish** page will show.

15. **Optional:** In the **Plan name** field, edit the name of the plan.
16. **Optional:** Expand the **Scopes** section and select **Add Scope**.
17. Select an option:

    Choose from:

    - Tag
    - Site
    - Sensor

    Result: A dialog shows.

18. Select one tag, site, or sensor.

    The option will depend on what you selected in the previous step.

19. Select **Confirm**.
20. Select **Done**.

Results

The Smart Polling plan has been added.

Add a Smart Polling plan that does not require credentials

Create a Smart Polling plan for targets that do not require credentials. Define the query, configure the schedule, and set the scope to complete the setup.

About this task

Use this process to create a Smart Polling plan for devices or systems that do not require authentication. This method enables the platform to collect data from non-credentialed targets using a query-based selection. You can configure the schedule and scope of the plan to suit your operational needs.

Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

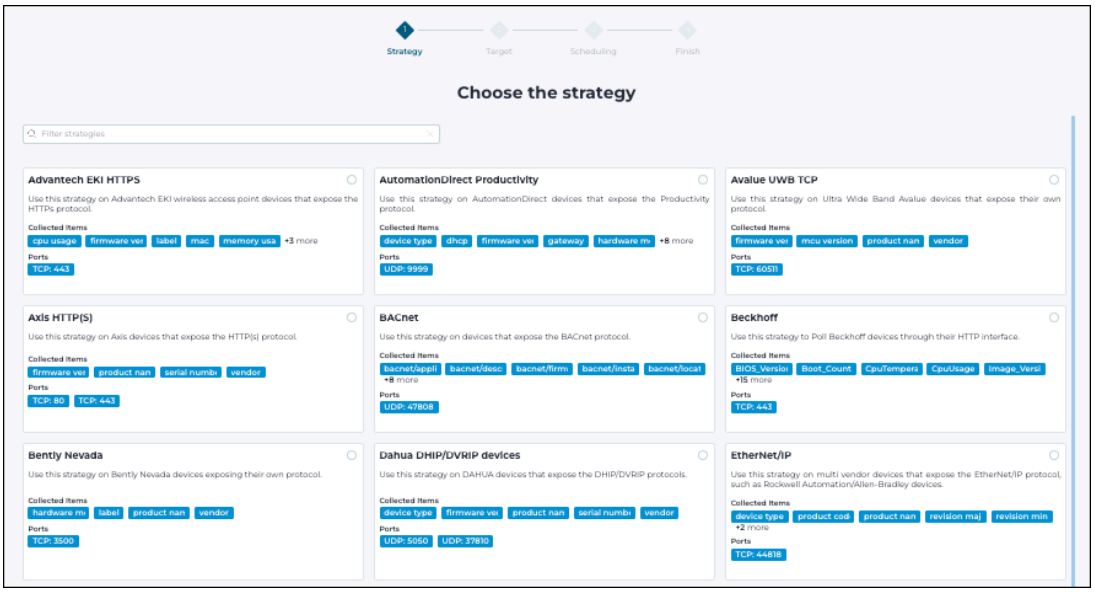
2. If the welcome page shows, select **Go to the Smart Polling page**.

3. On the **Smart Polling** page, select the ⊕ **Add** icon.

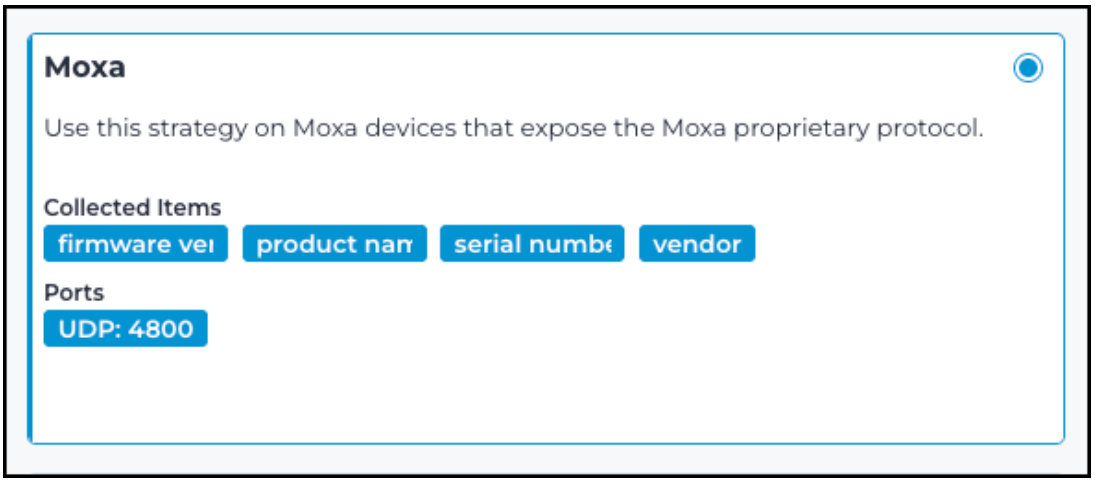
   Result: The **Choose the Strategy** page opens.

4. **Optional:**

   To find the correct strategy, enter text in the **Filter strategies** field.



5. In the top right corner of the relevant strategy, select the radio button.



6. Select **Next**.

   Result: Either the **Parameters** page or the **Target** page will show.

7. **Optional:** If the **Parameters** page shows, enter the necessary details.

> **Note:**
> Smart Polling proposes a safe default for each of these parameters. Unless you have specific requirements, we recommend that you use these parameters.

8. Select **Next**.

   Result: The **Target** page will show.

9. In the **Target nodes with a query** section, enter a query.
   For example, `nodes | where ip in_subnet? "192.168.45.0/24"`

10. Select **Test query**.
    If successful a `Success` indicator and the amount of nodes found will show and the **Next** button will be enabled.
11. Select **Next**.
    Result: The **Scheduling** page will show.
12. On the **Scheduling** page, select a scheduling type:

    > **Important:**
    > The **Recurrence based** option requires *N2OS* v25.3.0 or later. The **Interval based** option is available in all versions.

    Choose from:
    - Select **Interval based** to poll at a fixed interval
    - Select **Recurrence based** to poll at a specific frequency and time (requires *N2OS* v25.3.0 or later)
13. Configure the schedule:
    Choose from:
    - If you chose **Recurrence based**, set the frequency and the time
    - If you chose **Interval based**, set the interval
14. Select **Next**.
    Result: The **Finish** page will show.
15. **Optional:** In the **Plan name** field, edit the name of the plan.
16. **Optional:** Expand the **Scopes** section and select **Add Scope**.
17. Select an option:
    Choose from:
    - Tag
    - Site
    - Sensor

    Result: A dialog shows.
18. Select one tag, site, or sensor.
    The option will depend on what you selected in the previous step.
19. Select **Confirm**.
20. Select **Done**.

Results

The Smart Polling plan has been added.

Centralized plan management

Vantage displays progressive Smart Polling plans from connected sensors and lets you merge duplicates into a single centrally managed plan.

Progressive plans in Vantage

Progressive Smart Polling plans defined on connected sensors are shown on the Vantage **Smart Polling** page. These plans represent the progressive plans running on each connected Guardian.

Until the plans are consolidated, they do not yet contain historical data in Vantage.

Duplicate plan detection

When Vantage detects progressive plans defined on Guardian sensors, it shows a **Merge duplicates** message on the plan page. The message identifies how many duplicate plans exist and which sensors they come from.

You can merge the duplicates into a single plan and centralize its management in Vantage. After merging, the full polling history for the plan is immediately available in Vantage.

Effect of centralizing a plan

After you merge and centralize a progressive plan, Vantage manages the plan and propagates it to the connected sensors.

Important:

Once a progressive plan is centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Merge duplicate progressive plans

When multiple connected sensors have progressive plans for the same strategy, you can merge them into a single plan and manage it from Vantage.

About this task

When progressive mode is enabled on multiple connected sensors, each sensor may create its own progressive plan for the same strategy. Vantage detects these duplicates and lets you consolidate them into one plan. After merging, Vantage manages the plan and immediately shows the full polling history from all connected sensors.

Important:

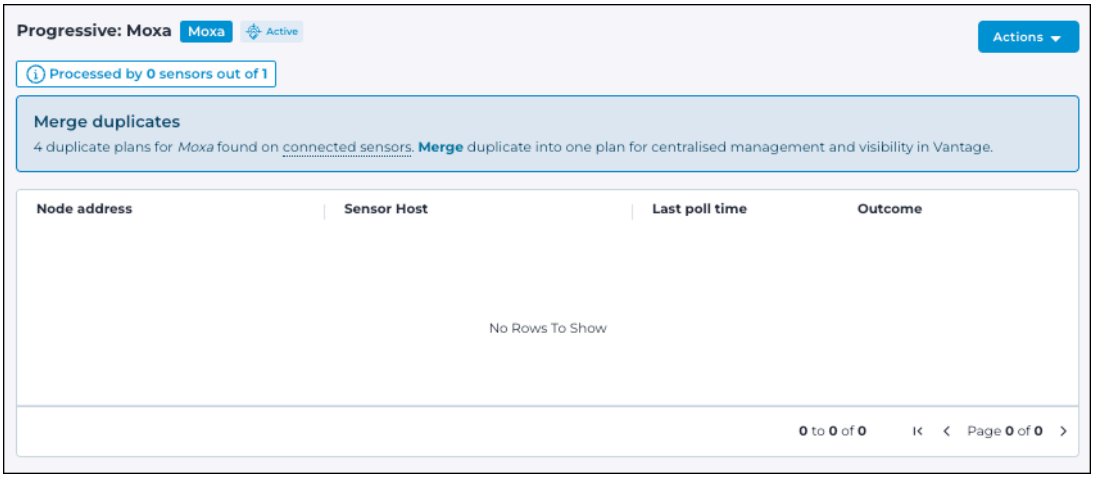
Once a plan is merged and centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

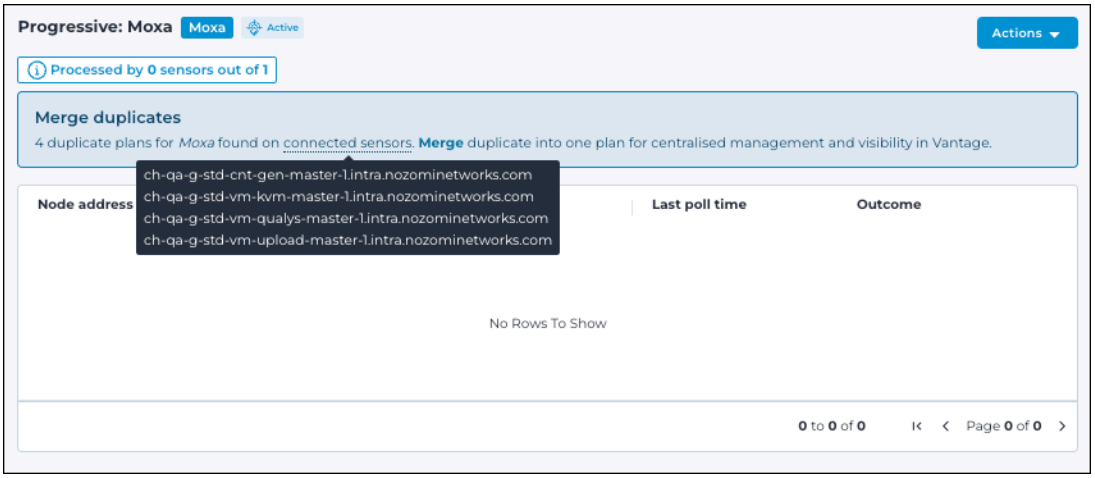
2. Select the progressive plan that shows a **Merge duplicates** message.



   Result: The plan page opens and shows the merge duplicates notification. The notification indicates how many duplicate plans exist across connected sensors.

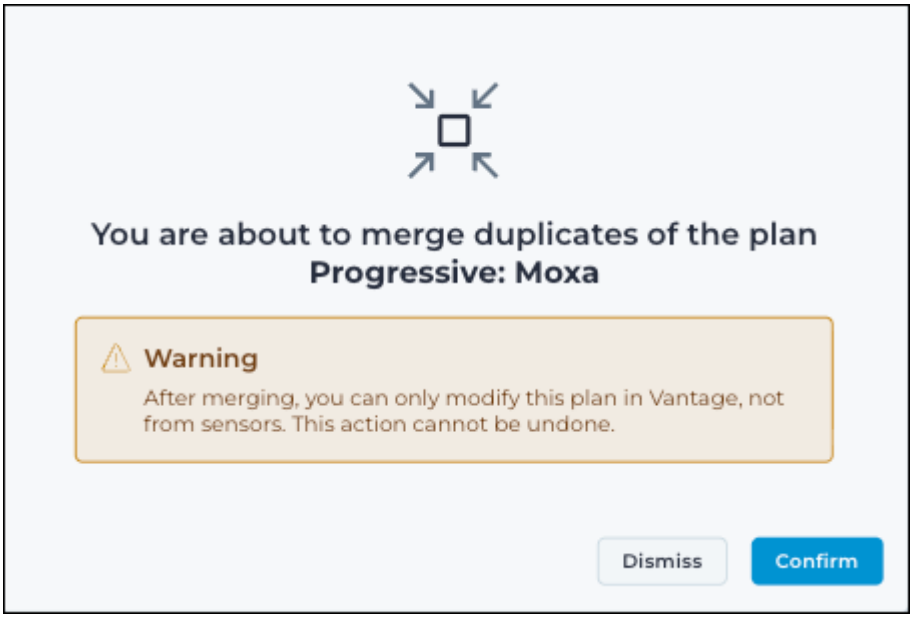
3. **Optional:**

   Hover over the **connected sensors** link in the notification to see which sensors have duplicate plans.



4. Select the option in the notification to merge the duplicates into this plan.

   Result: A confirmation dialog opens.



5. Select **Confirm**.

   Result: Vantage merges the duplicate plans and centralizes management of the plan. The polling history from all connected sensors is immediately available.

Actions menu

Pause a Smart Polling plan

Temporarily suspend a Smart Polling plan without deleting it. Use this option to stop polling activity while preserving the plan configuration. The plan can be resumed at any time.

About this task

When you pause a Smart Polling plan, it temporarily disables its polling activity without removing its configuration. This is useful when you want to stop monitoring for maintenance, troubleshooting, or scheduling reasons, but plan to resume later.

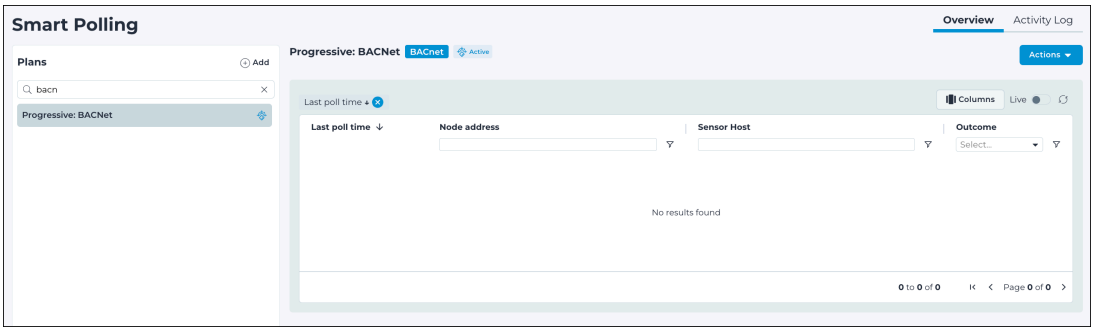
Procedure

1. In the top navigation bar, select ☰ **> Smart Polling**.

   Result: The **Smart Polling** page opens.

2. From the list of Smart Polling plans on the left, select the applicable plan.

3. In the top right corner, select **Actions**.



4. Select **Pause Plan**.

Results

The Smart Polling plan has been paused.

Resume a Smart Polling plan

Reactivate a previously paused Smart Polling plan to resume automated monitoring. This action restarts polling using the plan's saved configuration. Useful for restoring regular monitoring activity after a pause.

About this task

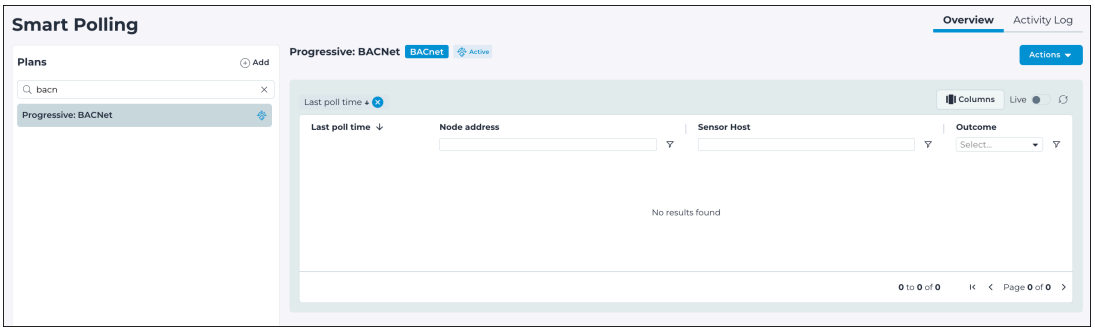
When you resume a Smart Polling plan, it restarts monitoring activity that was previously paused. This is useful after scheduled maintenance, issue resolution, or other intentional interruptions in polling. The plan resumes with its original configuration intact.

Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. From the list of Smart Polling plans on the left, select the applicable plan.
3. In the top right corner, select **Actions**.



4. Select **Resume Plan**.

Results

The Smart Polling plan has been resumed.

Edit a Smart Polling plan

Modify an existing Smart Polling plan to adjust its configuration or update associated settings. Editing a plan lets you fine-tune monitoring behavior. Ensure changes align with your system monitoring goals.

About this task

Editing a Smart Polling plan lets you change its targets, credentials, polling intervals, or other configurations. This is useful when your monitoring requirements change or you need to correct or refine existing settings.

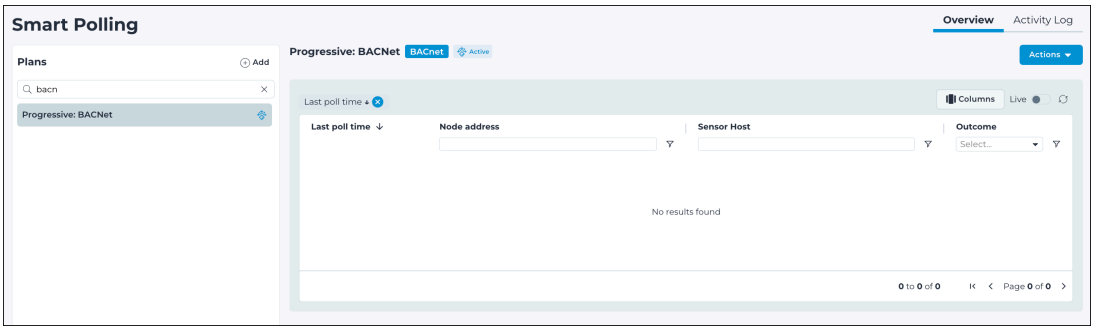
Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. From the list of Smart Polling plans on the left, select the applicable plan.

3. In the top right corner, select **Actions**.



4. Select **Edit Plan**.

   Result: The plan editing wizard opens in a modal window.

5. Use the applicable procedure to edit the plan:

   Choose from:

   - Add a Smart Polling plan that requires credentials (on page 330)
   - Add a Smart Polling plan that does not require credentials (on page 333)

   You can then confirm your edited details on the **Scheduling** and **Finish** pages.

Delete a Smart Polling plan

Delete an existing Smart Polling plan to remove obsolete or unneeded monitoring configurations. This action is permanent and cannot be undone. Use caution when confirming the deletion.

About this task

Deleting a Smart Polling plan permanently removes its configuration and stops all associated monitoring activity. Use this option when a plan is no longer relevant or needed. Be sure to confirm the deletion, as this action cannot be undone.

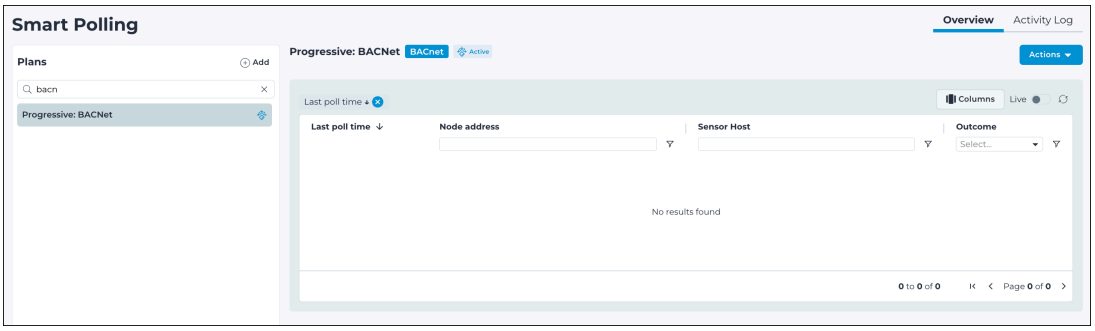
Procedure

1. In the top navigation bar, select ☰ > **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. From the list of Smart Polling plans on the left, select the applicable plan.

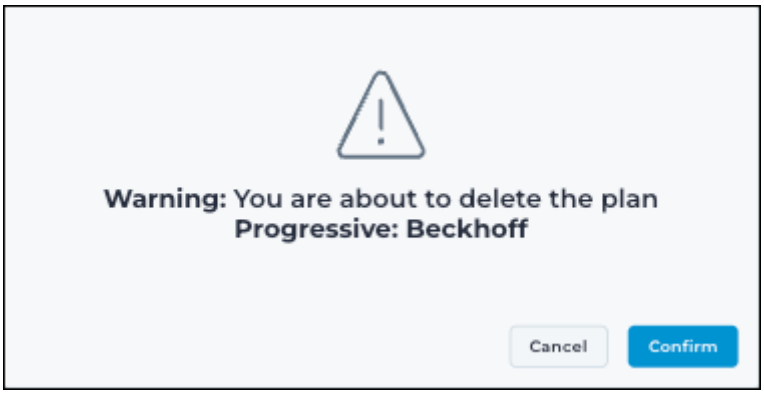
3. In the top right corner, select **Actions**.



4. Select **Delete Plan**.

   Result: A dialog shows

5. Select **Confirm**.



Results

The Smart Polling plan has been deleted.

Smart Polling results

*Smart Polling retrieves details from nodes to enrich asset data. This enriched information also enables other information to be enriched, such as hardware components, common platform enumeration (CPEs), and related vulnerabilities. When the Simple Network Management Protocol strategy (SNMP) strategy is used, it also populates the **Physical graph** in the **Graph** page.*

Once a Smart Polling plan has executed successfully, some or all of the information in sections of the Assets page should have been enriched.

Overview

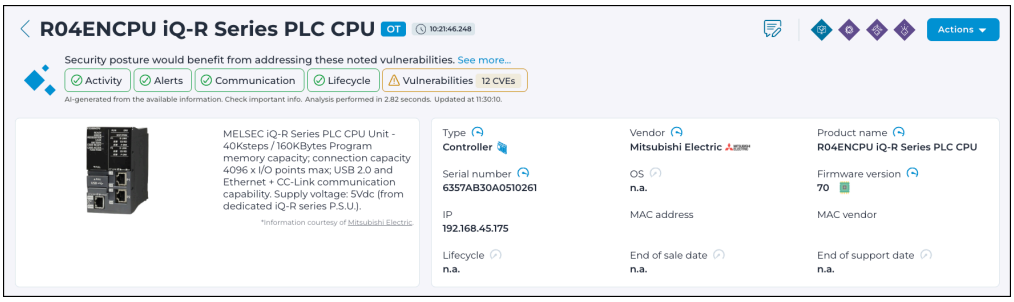


Figure 148. Assets page overview

Hardware Components tab

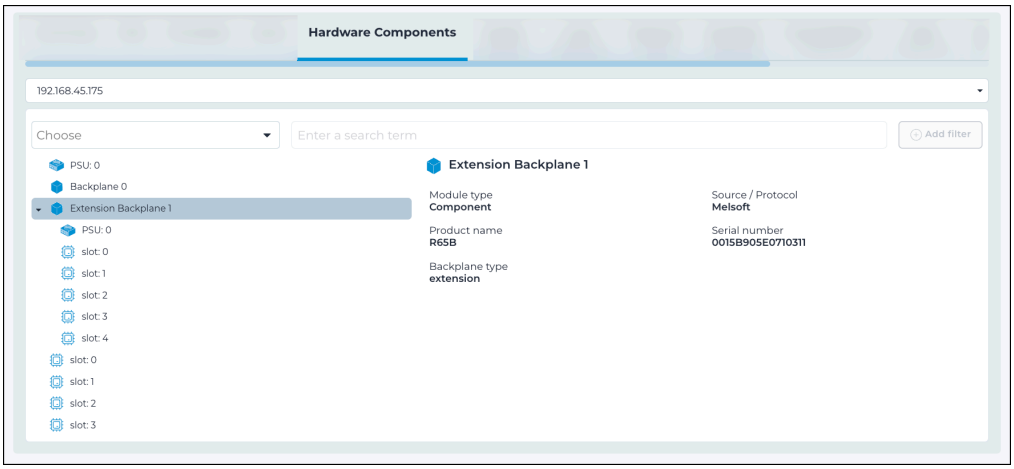


Figure 149. Assets page Hardware Components tab

CPEs tab

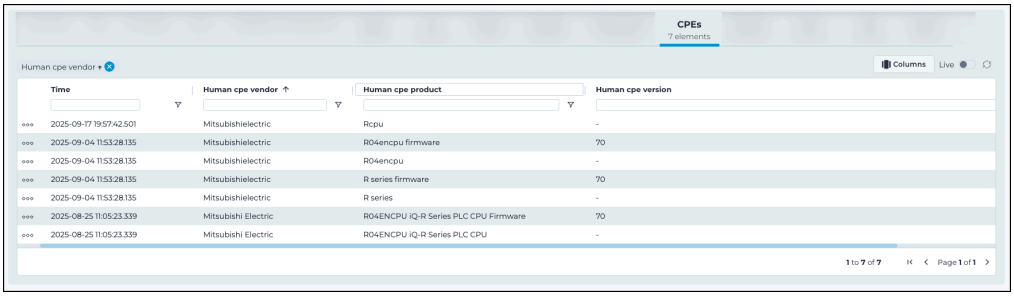


Figure 150. Assets page CPEs tab

Vulnerabilities tab

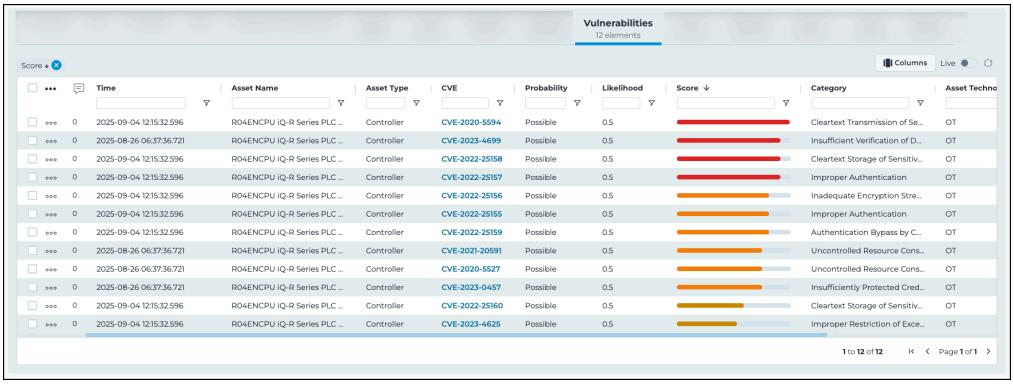


Figure 151. Assets page Vulnerabilities tab

Physical graph

In addition to the above sections, Smart Polling provides the necessary information to populate the **Physical graph**. To do this, you need to use the *simple network management protocol (SNMP)* strategy to poll network switches or routers.

Activity Log

*Use the **Activity Log** page in Vantage to inspect the history of Smart Polling activities. Each record in the table represents an execution of a Smart Polling plan on a specific node from a Nozomi Networks sensor.*

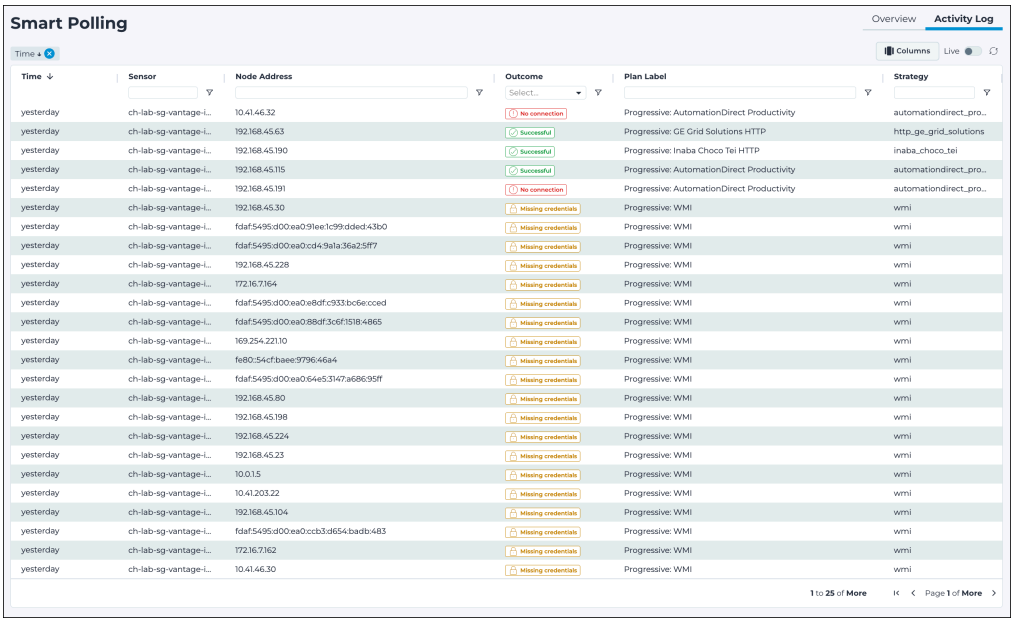


Figure 152. Activity Log page

Node executions

The **Activity Log** page shows the node executions. This is the individual executions of Smart Polling on a specific node with a configured plan. The table gives a view that you can filter and sort.

You can double-click a row in the table to open a sidebar with additional information. This includes a more granular report of the activity.

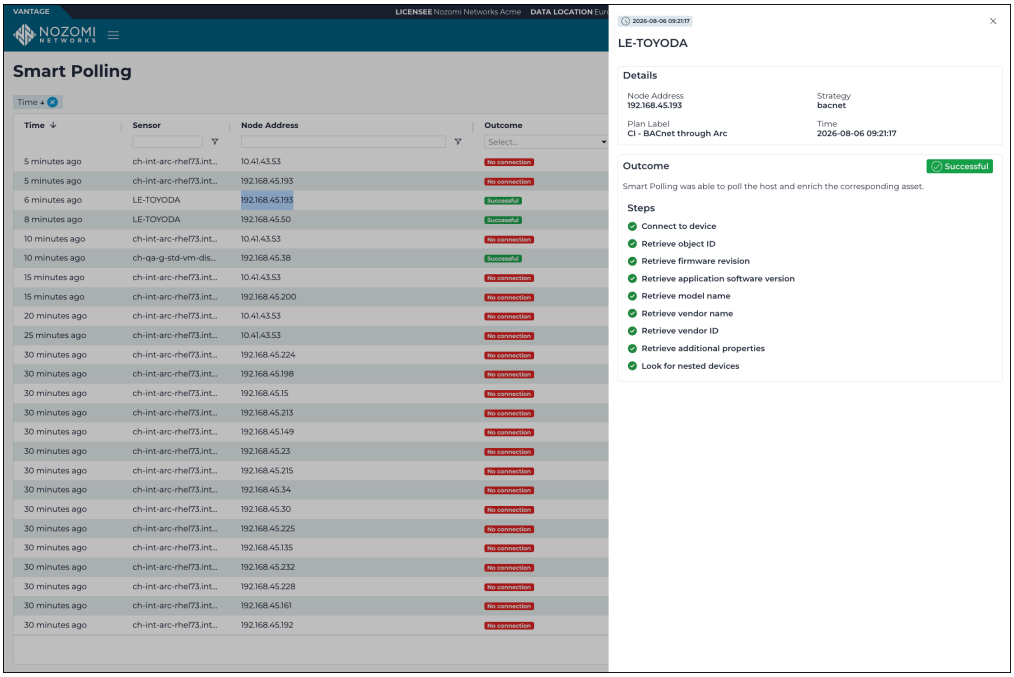


Figure 153. Activity Log sidebar

Column descriptions

Column label	Description
Time	The time this sensor connected to the monitored node.
Sensor	The hostname of the sensor performing the poll.
Node address	The address of the polled node.
Outcome	The result of the polling. For the list of possible outcomes, see Results (on page 320).
Plan label	The label of the executed plan.
Strategy	The strategy of the executed plan.

Chapter 19. Segmentation Advisor

*The **Segmentation Advisor** page helps you assess and improve your network segmentation by identifying risks and recommending actions.*

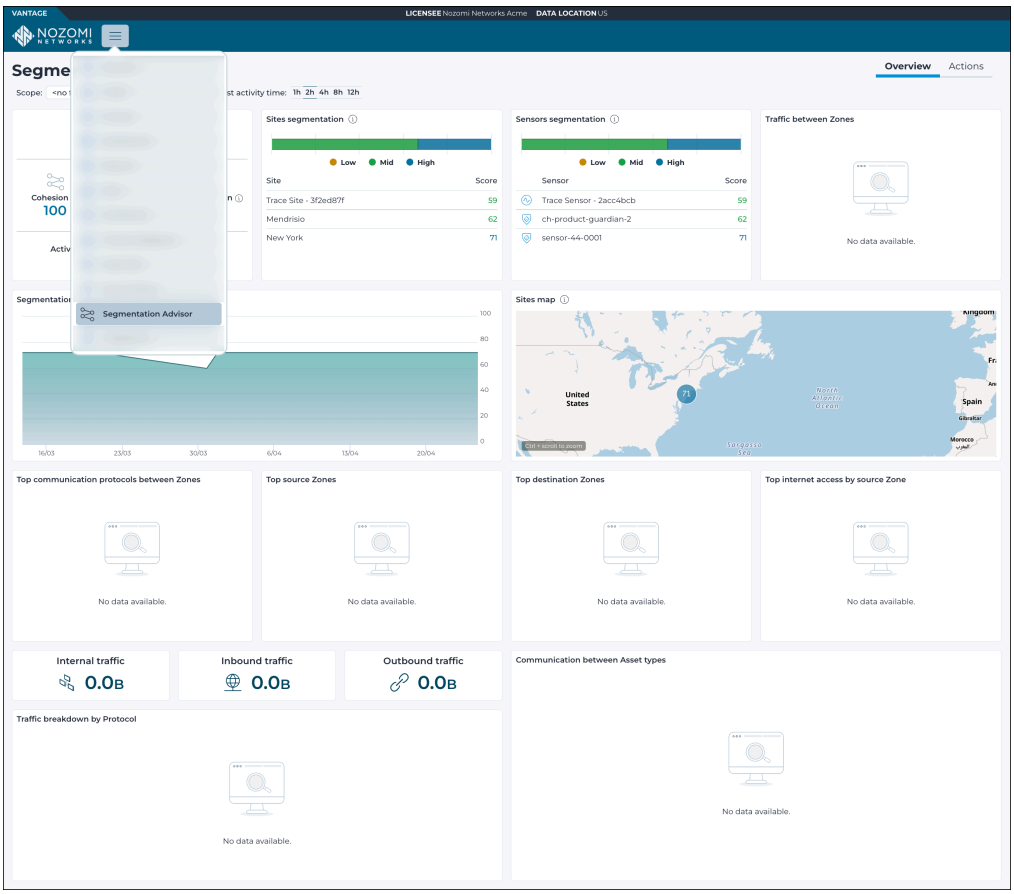


Figure 154. Segmentation Advisor page

The **Segmentation Advisor** page has these tabs:

- Overview (on page 350)
- Actions (on page 352)

Overview

*The **Overview** tab shows your overall network segmentation score and a breakdown of how your sites and sensors contribute to it.*

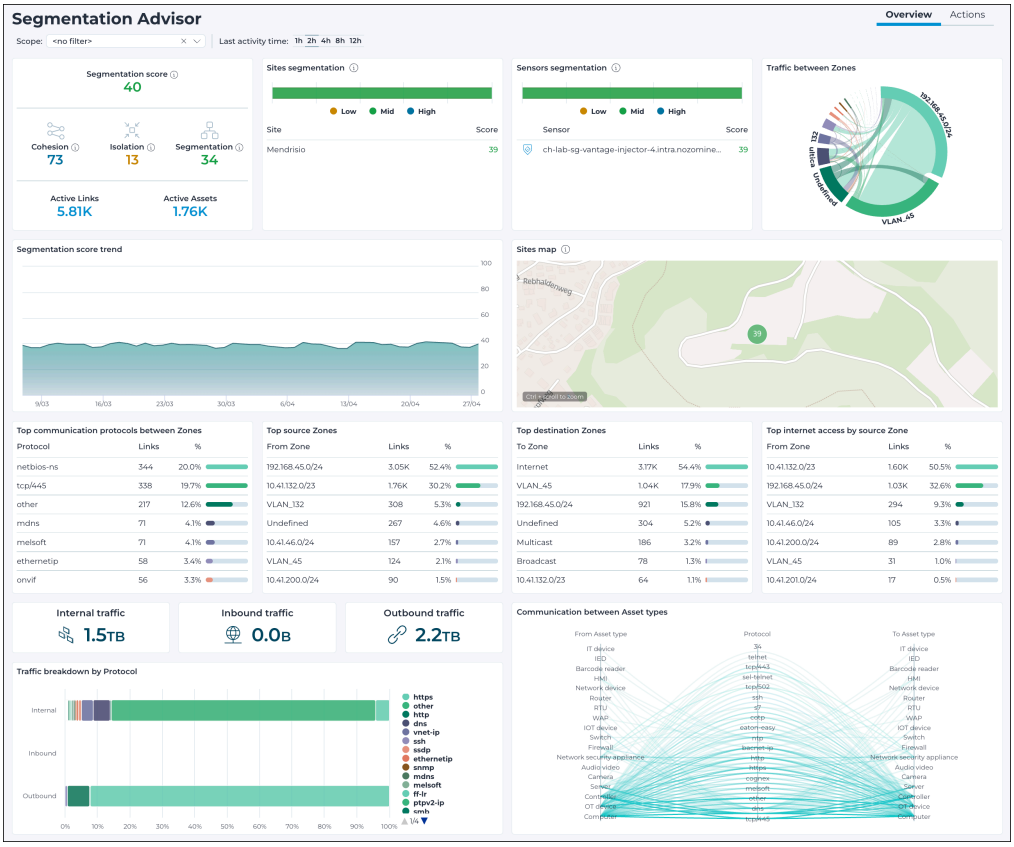


Figure 155. Overview tab

Use the **Scope** dropdown to filter the data to a specific site or sensor. Use the **Last activity time** buttons to set the time window for the data shown (1h, 2h, 4h, 8h, or 12h).

Segmentation score

The overall segmentation score (0–100) and its three component sub-scores:

- **Cohesion**: Measures how well assets within the same zone communicate with each other compared to across zones.
- **Isolation**: Measures how well zones are isolated from each other.
- **Segmentation**: The combined score derived from cohesion and isolation.

The panel also shows the counts of **Active Links** and **Active Assets** across your network.

Sites segmentation

Shows each site and its segmentation score in a table. A color-coded bar at the top of the panel indicates the overall distribution of scores across all sites: orange for Low, green for Mid, and blue for High.

Sensors segmentation
Shows each sensor and its segmentation score in a table. A color-coded bar at the top of the panel indicates the overall distribution of scores across all sensors: orange for Low, green for Mid, and blue for High.

Traffic between zones
A chord diagram showing the volume of traffic flowing between your network zones. Each arc segment represents a zone, and the ribbons between segments show the relative volume of traffic exchanged.

Segmentation score trend
An area chart showing how your segmentation score has changed over time.

Sites map
Shows the location of your sites on a map. Each site is represented by a bubble labeled with its segmentation score. Select **Ctrl + scroll** to zoom.

Top communication protocols between zones
A table showing the most frequently used protocols for communication between zones, with the link count and percentage of total traffic for each.

Top source zones
A table showing the zones that generate the most links, with the link count and percentage of total traffic for each.

Top destination zones
A table showing the zones that receive the most links, with the link count and percentage of total traffic for each.

Top internet access by source zone
A table showing which zones generate the most internet-bound links, with the link count and percentage of total internet traffic for each.

Internal traffic, inbound traffic, and outbound traffic
Three separate metric tiles showing the total volume of internal, inbound, and outbound traffic across your network.

Communication between asset types
A diagram showing traffic flows from source asset types, through the protocols used, to destination asset types. This helps you identify which asset type combinations communicate most and which protocols they use.

Traffic breakdown by protocol
A stacked horizontal bar chart showing how internal, inbound, and outbound traffic is distributed across protocols.

Actions

*The **Actions** tab guides you through your network segmentation journey with recommended actions across three phases.*

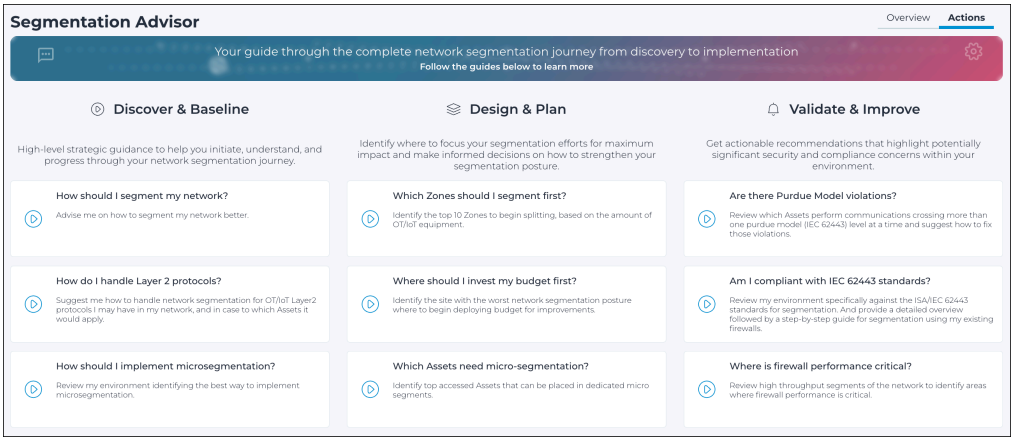


Figure 156. Actions tab

The **Actions** tab organizes recommendations into three phases of the segmentation journey:

Discover and baseline

Provides high-level strategic guidance to help you understand your current segmentation posture and establish a baseline for improvement.

Design and plan

Identifies where to focus your segmentation efforts for maximum impact and helps you make informed decisions on how to strengthen your segmentation posture.

Validate and improve

Provides actionable recommendations that highlight potentially significant security and compliance concerns in your environment.

Chapter 20. Data integrations

*The **Data integrations** page lets you connect Vantage to external systems by adding and managing data importers and exporters.*

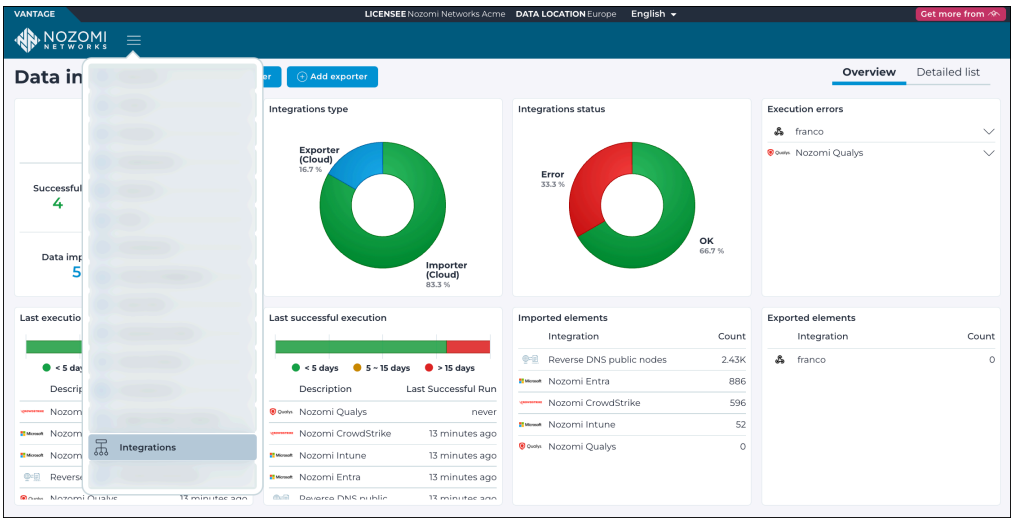


Figure 157. Data integrations page

The **Data integrations** page has these tabs:

- Overview (on page 356)
- Detailed list (on page 358)

Overview

*The **Overview** tab shows a summary of all data integrations configured for your organization, including their types, statuses, and execution history.*

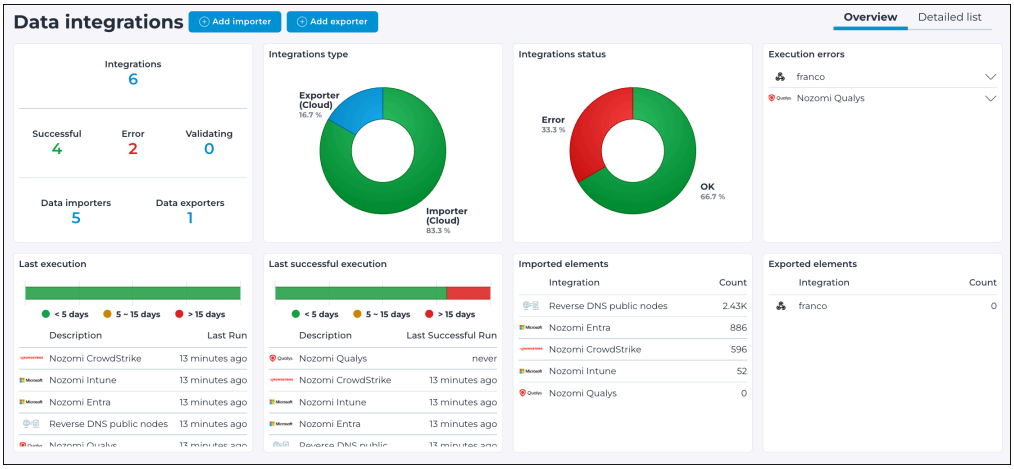


Figure 158. Overview tab

Add importer

The **Add importer** button opens the Configure data importer page, where you can select and configure a new data importer. Data importers bring external data into Vantage, for example asset and software information from third-party security tools.

Add exporter

The **Add exporter** button opens the Configure data exporter page, where you can select and configure a new data exporter. Data exporters send Vantage data to external systems, for example alerts and asset information to a SIEM or ticketing platform.

For the static *IP* addresses that Vantage uses to send this outbound traffic, see Static egress IP addresses for integrations (on page 362).

Integrations summary

The **Integrations summary** panel shows the total number of integrations and a breakdown by status:

- **Successful**: Integrations that ran without errors.
- **Error**: Integrations that encountered an error during their last run.
- **Validating**: Integrations currently being validated.

The panel also shows the total count of **Data importers** and **Data exporters**.

Integrations type

The **Integrations type** donut chart shows the proportion of integrations by type, for example Importer (Cloud) and Exporter (Cloud).

Integrations status

The **Integrations status** donut chart shows the proportion of integrations by their current status: OK (green) and Error (red).

Execution errors
A list of integrations that have encountered execution errors, with an expandable entry for each.

Last execution
A table showing when each integration last ran, color-coded by recency: green for less than 5 days ago, orange for 5–15 days ago, and red for more than 15 days ago.

Last successful execution
A table showing when each integration last ran successfully, using the same color-coded recency indicators as the Last execution panel.

Imported elements
A table showing the number of elements imported by each integration.

Exported elements
A table showing the number of elements exported by each integration.

Detailed list

*The **Detailed list** tab shows all configured integrations in a table with their type, description, propagation status, connectivity, and other configuration details.*

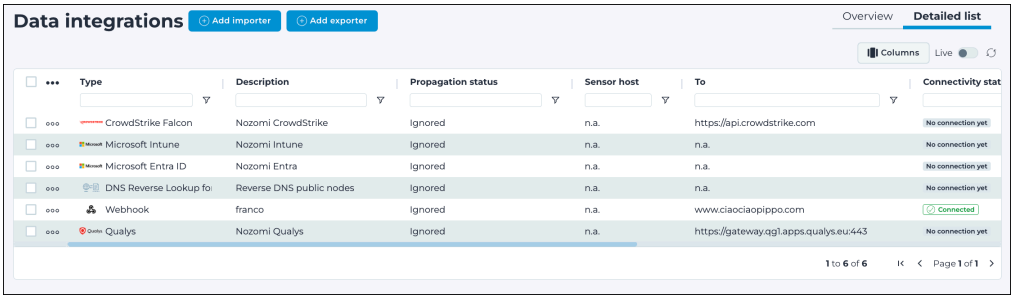


Figure 159. Detailed list tab

Add importer

The **Add importer** button opens the Configure data importer page, where you can select and configure a new data importer. Data importers bring external data into Vantage, for example asset and software information from third-party security tools.

Add exporter

The **Add exporter** button opens the Configure data exporter page, where you can select and configure a new data exporter. Data exporters send Vantage data to external systems, for example alerts and asset information to a SIEM or ticketing platform.

For the static *IP* addresses that Vantage uses to send this outbound traffic, see Static egress IP addresses for integrations (on page 362).

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The icon lets you immediately refresh the current view.

Table

Column	Description
Type	The integration type, for example `CrowdStrike EDR`, `ServiceNow`, or `Webhook`.
Description	The name given to the integration when it was configured.

Column	Description
Propagation status	Indicates whether the integration configuration has propagated to the relevant sensors. Possible values are `Pending`, `In progress`, `Done`, and `Ignored`. This column only appears for on-premise integrations that run on a sensor appliance.
Sensor host	The hostname or *IP* address of the sensor associated with the integration. This column only appears for on-premise integrations that run on a sensor appliance.
To	The destination *URL* or endpoint for the integration.
Connectivity status	Shows the connection state of the integration. Possible values are `Connected`, `No connection yet`, and `Connection error`. When there is a connection error, hover over the status to see the error details.
Status	Shows whether the last data transmission succeeded. Possible values are `OK`, `Not sent`, `Validating`, and `Error`. When there is an error, hover over the status to see the error details.
Last sent	The date and time when data was last successfully sent by the integration.
Processed items	The total number of items sent by the integration since it was configured.

Add a data importer

Add a data importer to bring external data into Vantage, for example asset and vulnerability information from third-party security tools.

Procedure

1. In the top navigation bar, select ☰ > **Integrations**.

   Result: The Data integrations (on page 353) page opens.

2. Select **Add importer**.

   Result: The **Configure data importer** page opens.

3. Select the integration type you want to configure.
4. Complete the configuration fields for the selected integration type, then select **Save**.

   Result: The new data importer appears in the **Data integrations** list.

Related information

Data integrations (on page 353)

Overview (on page 356)

Add a data exporter (on page 361)

Add a data exporter

Add a data exporter to send Vantage data to an external system, for example alerts and asset information to a security information and event management (SIEM) or ticketing platform.

Procedure

1. In the top navigation bar, select ☰ > **Integrations**.

   Result: The Data integrations (on page 353) page opens.

2. Select **Add exporter**.

   Result: The **Configure data exporter** page opens.

3. Select the integration type you want to configure.
4. Complete the configuration fields for the selected integration type, then select **Save**.

   Result: The new data exporter appears in the **Data integrations** list.

Related information

Data integrations (on page 353)

Overview (on page 356)

Add a data importer (on page 360)

Static egress IP addresses for integrations (on page 362)

Static egress IP addresses for integrations

Lists the static IP addresses that Vantage uses to send outbound integration traffic, organized by region, so you can allowlist them on your endpoints.

Vantage sends outbound integration traffic, for example *common event format (CEF)* or syslog forwarding to a *SIEM* platform such as Cribl, from a static *IP* address. Each region uses a dedicated set of three *IP* addresses that do not rotate.

Add all three *IP* addresses for your region to the allowlist on the receiving endpoint to ensure uninterrupted integration delivery.

Table 2. Static egress IP addresses by region

Region	IP addresses
AP1	3.105.117.255
	3.104.148.166
	54.253.222.8
EU1	18.156.141.195
	18.198.153.154
	18.198.127.144
EU2	18.102.13.150
	35.152.78.89
	35.152.33.240
ME1	51.112.74.197
	51.112.24.31
	51.112.87.34
US1	52.86.82.231
	23.22.197.94
	3.86.156.246

These *IP* addresses are intended to remain stable, but they may change in rare circumstances.

Important:

Before you configure an allowlist, read this topic to get the latest values.

Related information

Data integrations (on page 353)

Overview (on page 356)

Add a data exporter (on page 361)

Chapter 21. Async operations

*The **Async operations** page lets you keep track of tasks that are being executed in the background, and it shows their outcome once that they are completed.*

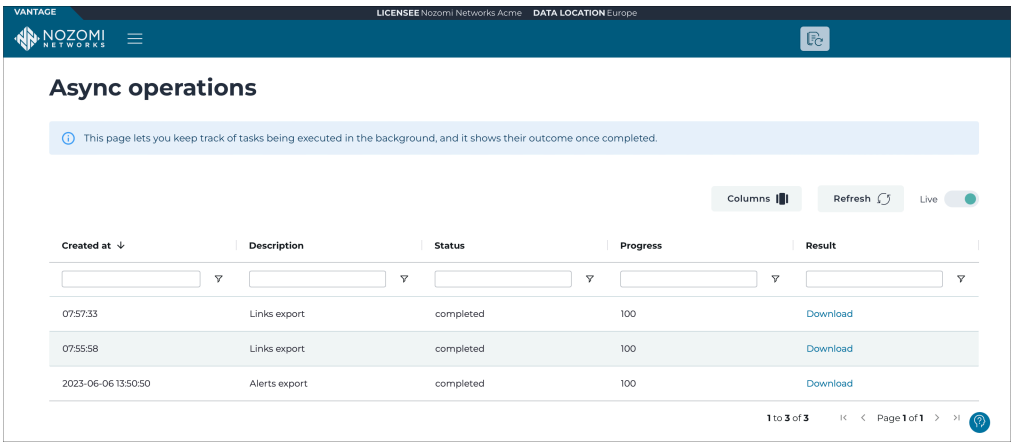


Figure 160. Async operations page

Chapter 22. What's new drawer

*The **What's new** drawer shows a list of new features, enhancements, and fixes for issues.*

Select in the footer to open the **What's new** drawer. When you open the drawer, the unread indicator on the footer icon disappears.

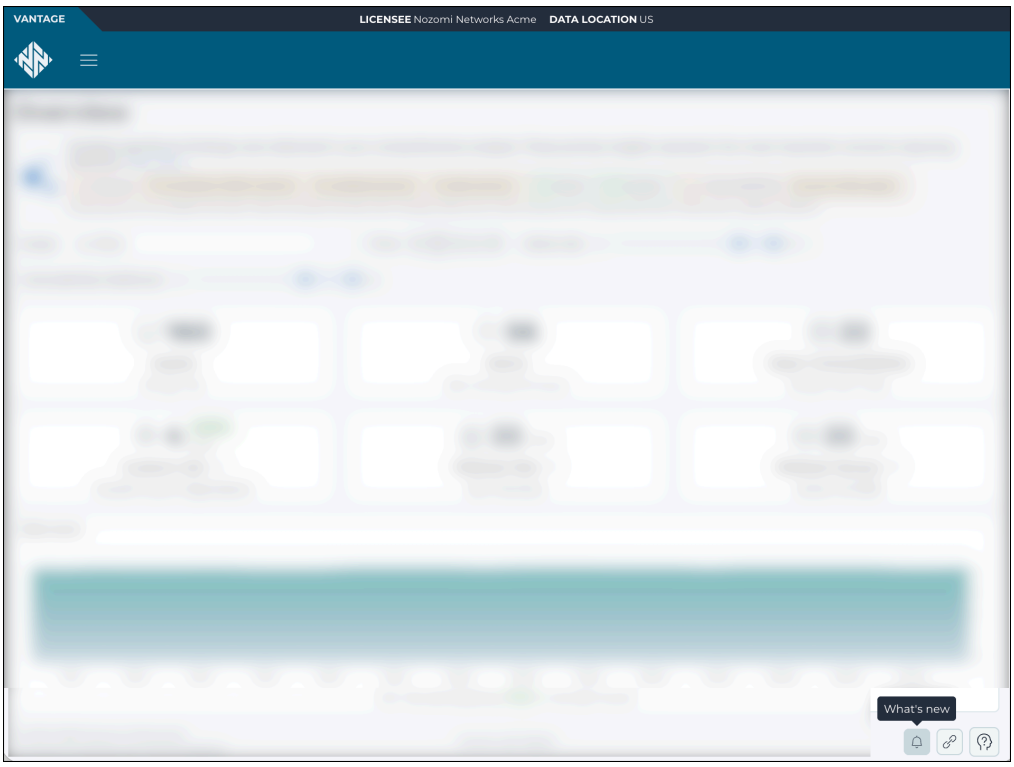


Figure 161. What's new icon

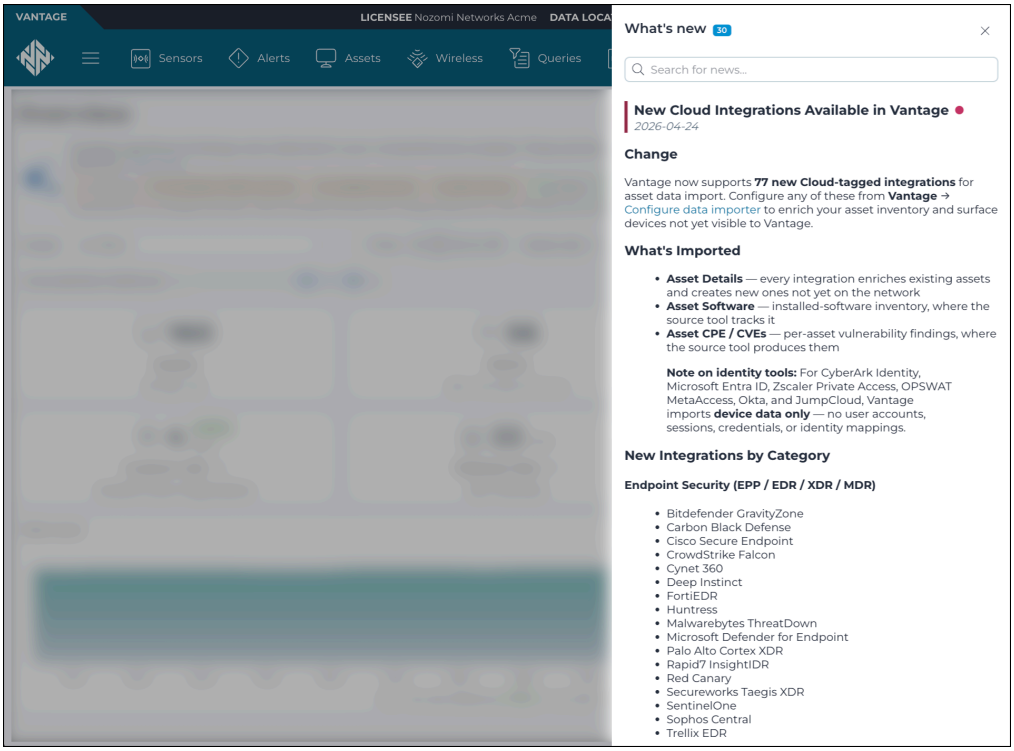


Figure 162. What's new drawer

Drawer elements

Count badge

The number next to the **What's new** heading shows the number of unread news items. The count stays visible while the drawer is open and resets to zero when you close it.

Search

Use the **Search for news** field to filter entries by keyword.

Unread indicator

A red dot on the footer icon indicates that there are unread news items. The dot clears as soon as you open the drawer, before you close it.

Entry structure

Each entry includes:

- A title and the date the entry was published.
- A **Change** section describing what was added or updated.

Chapter 23. Administration

Administration page

The administration page lets a user with administrator privileges configure settings and do other tasks.

For more details, see the Vantage **Administrator Guide**.

Chapter 24. Profile settings

The profile settings menu lets you edit your user settings and update your profile.

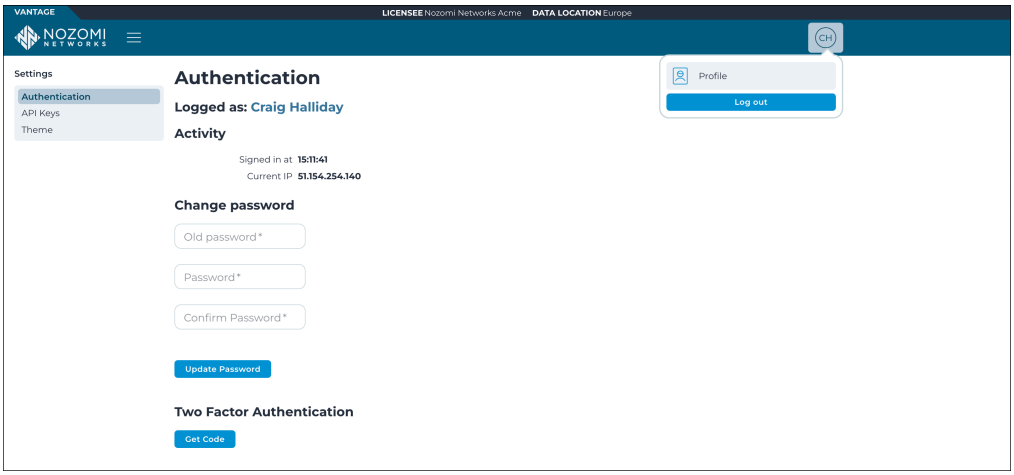


Figure 163. Profile settings menu

The **Profile** page has these tabs:

- Authentication (on page 380)
- API Keys (on page 381)
- Theme (on page 383)

Related information

Authentication (on page 380)

API Keys (on page 381)

Theme (on page 383)

Authentication

*The **Authentication** page shows user activity details, lets you change your password, and lets you create a two-factor authentication code.*

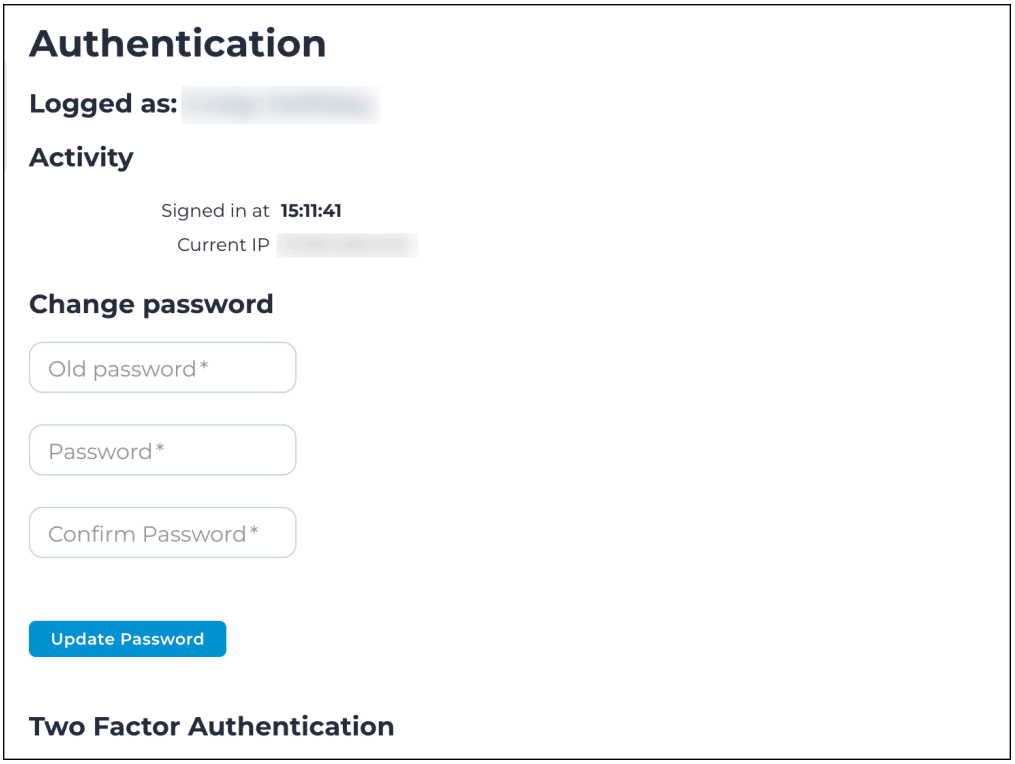


Figure 164. Authentication page

Activity

This section shows the last time the current user signed in and the *IP* address used.

Change password

This section lets you change your password.

Two Factor Authentication

The **Get Code** button lets you create a code that can be used for *two-factor authentication (2FA)* in third-party applications.

API Keys

*The **API Keys** pages lets you manage application programming interface (API) keys for the current user. Third-party applications that integrate with Vantage must use API keys to authenticate.*

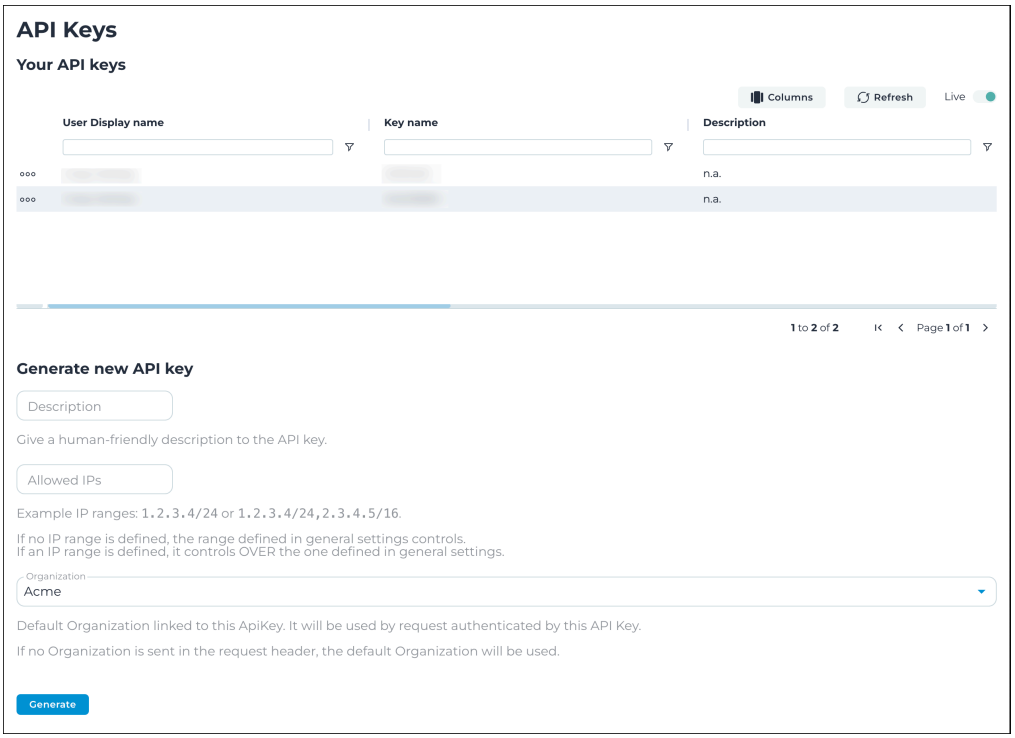


Figure 165. API Keys page

Each *API* key is associated with a Vantage user, who must have sufficient permissions in Vantage. This user should be the *SAML* account of the person responsible for the integration. Your third-party application must pass the *API* key name and token in order to authenticate with Vantage. An *API* key remains valid until it is revoked, or until its user is deleted.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Refresh

The **Refresh** icon lets you immediately refresh the current view.

Live

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Table

Created at	The date and time that the *API* key was created.
Updated at	The date and time that the *API* key was last updated.
Revoked at	The date and time that the *API* key was revoked.
User Display name	The display name of the user associated with the *API* key.
Key name	The name of the *API* key. Vantage generates this name when you create the *API* key.
Description	The user-defined description of the *API* key.
Last sign in at	The last date and time that the *API* key was used to sign in.
Last sign in ip	The originating *IP* address of the connection that last authenticated using the *API* key.
Allowed ips	The user-defined range of *IP* addresses from which connections are permitted.
Linked organization Name	The name of an organization that will serve as a default value when *API* calls using this key do not specify an organization.

Generate new API key

This section lets you:

- Create a description for the *API* key
- Set an allowed, or range of allowed, *IP* addresses for the *API* key
- Select an organization with which to associate the *API* key

Theme

*The **Theme** page lets you choose a theme for the user interface (UI).*

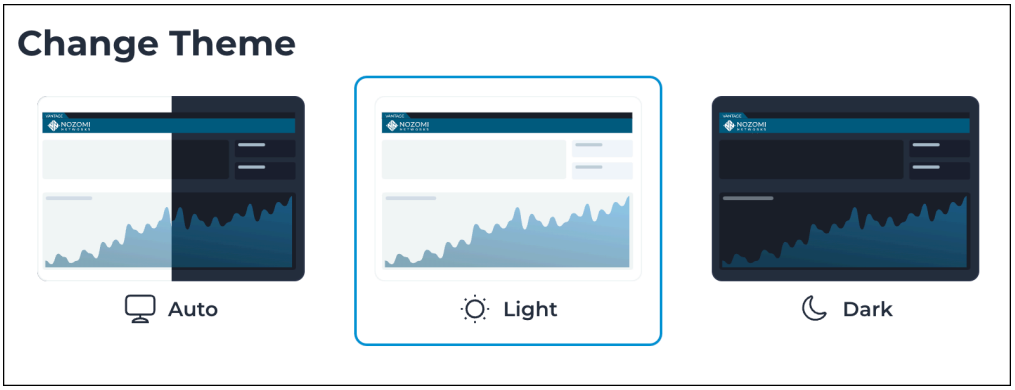


Figure 166. Theme page

The **Theme** page lets you customize the visual appearance of the *UI*. You can choose one of these themes:

- Auto: Automatically adjusts the theme based on system settings
- Light: Uses a bright interface for better visibility in well-lit environments
- Dark: Uses a dark interface for reduced eye strain in low-light environments

Chapter 25. Organizations menu

The organizations menu lets you search or show a list of all of your organizations, and lets you switch between them. Vantage provides a default organization, but administrators can add more organizations as necessary.

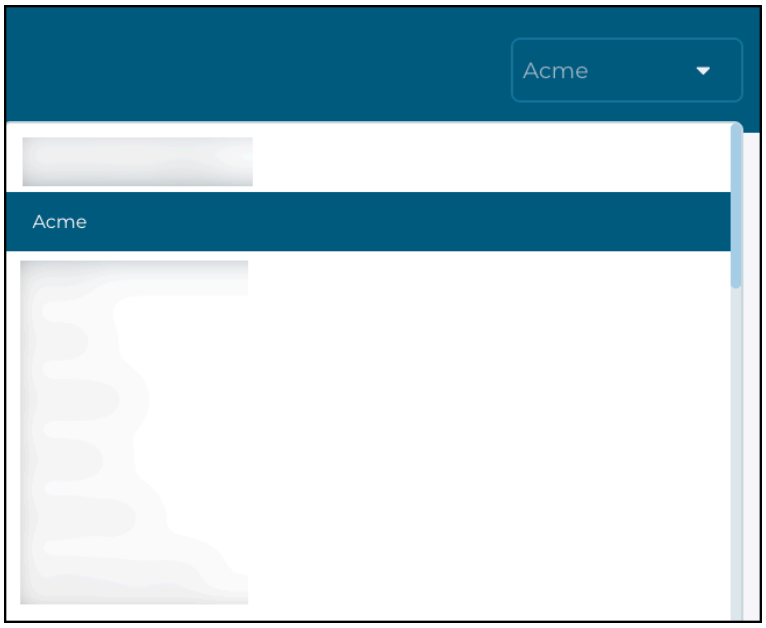


Figure 167. Organizations menu

An organization is a logical subdivision within your company. An organization is an isolated container that limits the access of your users. You can associate organizations with user groups and roles to define the type of changes that your users can make, and where they can make them.

The organizations menu lets you find one of your organizations. To do this you can either:

- Open the dropdown and select from the list
- Enter text to search the list

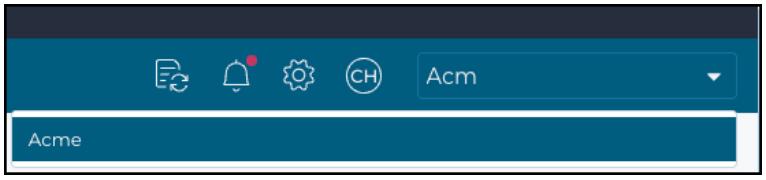


Figure 168. Search function

Glossary

Adaptive Learning

Adaptive Learning is when deviations are evaluated at a global level, rather than at the level of a single node. For example, using adaptive learning approach, the sensor doesn't raise an alert when it detects a device similar to those already installed in the network. This also applies for newly-detected communications that are similar to those previously detected. Adaptive learning is especially powerful and offers its best effect when combined with Asset Intelligence.

Address Resolution Protocol

ARP is a communication protocol that is used to discover the link layer address, such as a *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.

Artificial Intelligence

AI is computer intelligence, as opposed to human or animal intelligence. It is *artificial* because it is a digital computer that can perform tasks that are commonly associated with intelligent beings. *Intelligence* is the ability to learn and to reason.

Assertion Consumer Service

An ACS is a version of the SAML standard that is used to exchange authentication and authorization identities between security domains.

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.

Authorization to Operate

ATO is a formal declaration by a designated authorizing official that authorizes operation of an information system and explicitly accepts the risk to organizational operations, organizational assets, individuals, or other organizations based on the implementation of an agreed-upon set of security controls.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

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.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

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 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.

Common Vulnerability Scoring System

CVSS is a standardized framework used in cybersecurity to assess the severity of software vulnerabilities. It provides a numerical score to help prioritize risk management and response efforts.

Controlled Unclassified Information

CUI is information that requires safeguarding or dissemination controls pursuant to federal law, regulations, and government-wide policies, but is not classified under Executive Order 13526.

Coordinated Universal Time

Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. It is based on International Atomic Time (TAI) with leap seconds added to synchronize with Earth's rotation.

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.

Department of Defense

DoD is the executive branch department of the United States federal government responsible for coordinating and supervising all agencies and functions directly related to national security and the United States Armed Forces.

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.

Exploit Prediction Scoring System

EPSS is a cybersecurity risk assessment framework that predicts the likelihood of a software vulnerability being exploited in the wild. It uses data-driven models based on real-world exploit activity, vulnerability metadata, and other threat intelligence sources to help organizations prioritize patching efforts.

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

Federal Information Security Management Act

FISMA is a United States federal law that defines a framework of guidelines and security standards to protect government information and operations. It requires federal agencies to develop, document, and implement programs to provide information security for their data and information systems.

Federal Risk and Authorization Management Program

FedRAMP is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

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.

Identity Provider

An IdP is a system entity that creates, maintains, and manages identity information. It also provides authentication services to applications within a federation, or a distributed network.

Industrial Control Systems

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

Information Technology

IT is the use of computers to process, create, store, and exchange data and information.

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.

JSON web token

A JWT is an internet standard to create data with optional encryption and/or optional signature whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a private/public key.

Known Exploited Vulnerabilities

A list of software vulnerabilities that threat actors have actively exploited. Cybersecurity organizations track KEVs to help prioritize patching and mitigate security risks.

Link Layer Discovery Protocol

LLDP is a vendor-neutral link layer protocol used by network devices for advertising identity, capabilities, and neighbors on a local area network.

Management Information Base

An MIB is a collection of definitions that specify the properties of the managed resources within a network device (like routers or switches) and how they can be accessed using SNMP (Simple Network Management Protocol).

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.

National Institute of Standards and Technology

NIST is an agency of the United States Department of Commerce. NIST's mission is to promote American innovation and industrial competitiveness.

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Newline Delimited JSON

NDJSON is a data format where each line is a valid JSON value, used for streaming or storing structured records efficiently.

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.

Packet Capture

A pcap is an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Plan of Action and Milestones

POA&M is a document that identifies tasks that need to be accomplished to address security weaknesses or deficiencies. It details resources required, milestones for completion, and scheduled completion dates for each task. It is a key tool for tracking and managing remediation efforts in federal security compliance programs.

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.

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 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 Assertion Markup Language

SAML is an open standard, XML-based markup language for security assertions. It allows for the exchange of authentication and authorization data different parties such as a service provider and an identity provider.

Security Assessment Report

SAR is a comprehensive document that details the results of an independent security assessment of an information system. It includes findings, vulnerabilities, and recommendations from the assessment process and is a required component of the FedRAMP authorization.

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.

Security Requirements Guide

SRG is a Department of Defense publication that provides security requirements and controls for information systems and cloud computing services at various impact levels.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

Single Sign-on

SSO is an authentication method that lets users log in to one or more related, but independent, software systems.

Software as a Service

SaaS is a software licensing and delivery model. This type of software is hosted centrally and licensed on a subscription basis.

Strict (Learning)

Strict (Learning) is a mode which relies on a detailed anomaly-based approach. Each node is evaluated at the node level; when deviations from the baseline are detected, the sensor raises alerts. This approach is called strict because once a system is learned, it is expected to always behave as it did during the learning phase; maintaining systems with the Strict approach requires detailed knowledge of your system.

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.

System Security Plan

SSP is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned to meet those requirements. It is a key component of the FedRAMP authorization process.

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.

Two-factor authentication

2FA is a method that lets you add additional security to an account. The first factor is a standard password, the second factor is a code that is used on an app on a mobile device or computer that verifies the user.

Uniform Resource Identifier

A URI is a unique string of characters used to identify a logical or physical resource on the internet or local network.

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.

Virtual Local Area Network

A VLAN is a broadcast domain that is isolated and partitioned in a computer network at the data link layer (OSI layer 2).

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.

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.