



Vantage **User Guide**

2024-09-13

Legal notices

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

Copyright

Copyright © 2013-2024, 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.....	7
Vantage overview.....	9
Architecture.....	11
Data security in Vantage.....	12
Graphical User Interface (GUI).....	13
Homepage.....	13
Top navigation bar.....	16
Chapter 2. Sensors.....	19
Sensors.....	21
Details page.....	22
Summary drawer.....	32
Table interactions.....	33
Connect a sensor.....	40
Troubleshooting.....	53
Chapter 3. Alerts.....	55
Alerts.....	57
Details page.....	59
Summary drawer.....	61
Table interactions.....	62
Chapter 4. Assets.....	75
Assets.....	77
Details page.....	79
Summary drawer.....	96
Table interactions.....	97
Chapter 5. Wireless.....	103
Wireless.....	105
Networks.....	107
Channels.....	109
Spectrum.....	110
Chapter 6. Queries.....	111
Queries.....	113
Execute a query.....	114
Commands.....	115
Functions.....	119
Chapter 7. Vulnerabilities.....	125
Vulnerabilities.....	127
Detailed list.....	128

Workbooks.....	130
Details page.....	131
Summary drawer.....	133
Table interactions.....	134
Chapter 8. Vantage IQ.....	139
Vantage IQ.....	141
Insights.....	143
Answers.....	147
Time Series.....	147
Queries.....	148
Chapter 9. Network.....	161
Network.....	163
Nodes.....	164
Links.....	165
Sessions.....	166
Chapter 10. Graph.....	167
Graph.....	169
Chapter 11. Process.....	173
Process.....	175
Table interactions.....	177
Actions menu.....	177
Chapter 12. Dashboards.....	179
Dashboards.....	181
Create a dashboard.....	182
Import a dashboard.....	183
Export a dashboard.....	184
Add a widget.....	185
Chapter 13. Reports.....	187
Reports.....	189
Table interactions.....	190
Actions menu.....	190
Chapter 14. Sites.....	191
Sites.....	193
Table interactions.....	194
Chapter 15. Workbooks.....	197
Workbooks.....	199
Use a workbook to improve your network security.....	200
Chapter 16. Async operations.....	201
Async operations.....	203

Chapter 17. What's new.....	205
What's new drawer.....	207
Chapter 18. Administration.....	209
Administration page.....	211
Chapter 19. Profile settings.....	213
Profile settings.....	215
Authentication.....	216
API keys.....	217
Chapter 20. Organizations menu.....	219
Organizations menu.....	221
Glossary.....	223



Chapter 1. Introduction



Vantage overview

Vantage™ is a *Software as a Service (SaaS)* product that lets you monitor and protect your networks from anywhere in the world. Vantage lets you respond faster and more effectively to cyber threats, to ensure your operational resilience.

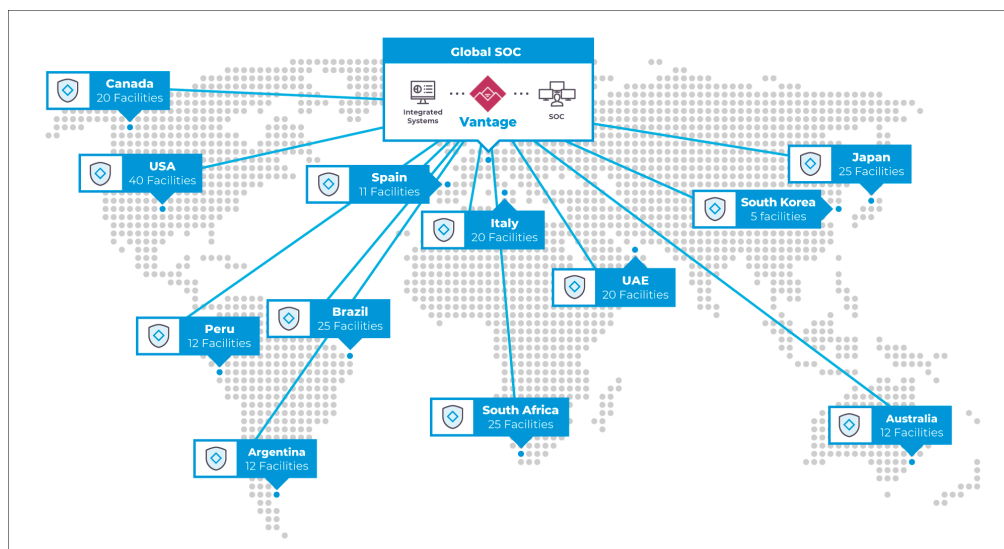


Figure 1. Vantage overview

General

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
- Centrally-manage all sensor deployments from anywhere in the world
- Monitor an unlimited amount of devices
- Protect an unlimited amount 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 threat. 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. It includes built-in integrations for asset, ticket and identity management systems, as well as for [security information and event management \(SIEM\)](#).

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

Architecture

You can use Vantage, and the flexible architecture and integrations with other systems, to create a customized solution.

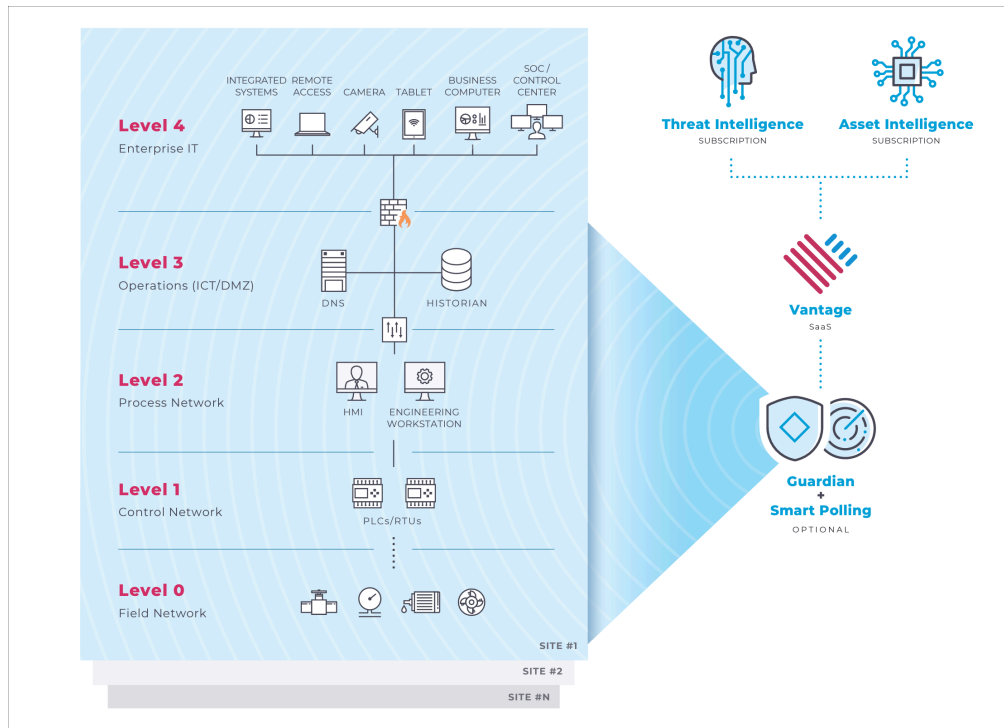


Figure 2. Vantage architecture

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 [National Institute of Standards and Technology \(NIST\)](#) 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.

Implementations that are [FIPS](#)-compliant are entirely separate from other Vantage instances and sensors:

- A [FIPS](#)-compliant Vantage instance only accepts connections from [FIPS](#) sensors
- A non-[FIPS](#) Vantage instance accepts only connections from non-[FIPS](#) sensors

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 URLs](#), see **IdP configuration for SAML integration**, in the **Administrator Guide**.

Graphical User Interface (GUI)

Homepage

This is the default view in Vantage, it offers the highest level view of the health of your network.

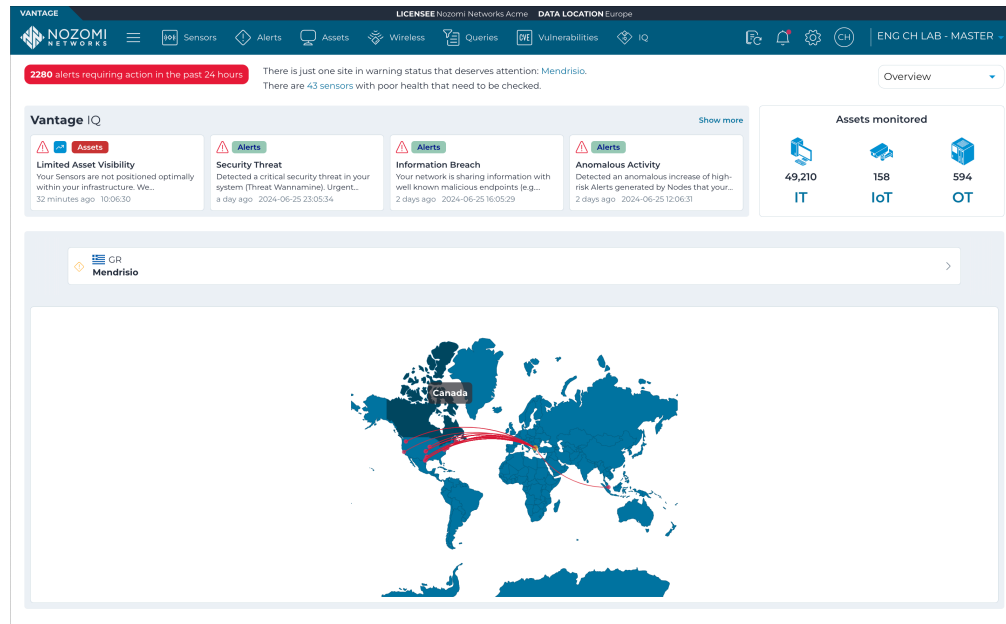


Figure 3. Overview page

When you sign into Vantage, the **Overview** page highlights the health of the assets and sites that you monitor, and shows alerts and incidents.

Top navigation bar

For more details, see [Top navigation bar \(on page 16\)](#).

Dropdown menu

The dropdown gives you access to theses different pages:

- **Overview:** The default view in Vantage, it offers the highest level view of your network's health.
- **Alerts:** Displays the total number of alerts across your entire network. The map shows the locations of the top alert types and protocols shown in the charts at the bottom of the page.
- **Assets:** Displays the total number of assets across your entire network. The map visualizes the locations of the top asset types, vendors, and operating systems shown in the charts at the bottom of the page.
- **Sensors:** Displays the total number of sensors connected to Vantage. The map visualizes the locations of the top sensor models shown in the chart at the bottom of the page.
- **Traffic:** Displays the total throughput in Mbps (megabits per second) and number of links across your entire network. The map visualizes the origin locations of links, while the list at the bottom of the page shows the top destination country.
- **Vulnerabilities:** Displays the total number of vulnerabilities detected in your network. The map visualizes the locations of the sites with the highest number of vulnerabilities, while the list at the bottom of the page shows the most common categories.



Note:

The totals displayed here are system-wide values. If you are only granted access to a subset of Vantage data, these values may not match results in the table or in query results.

Assets monitored

This panel shows a count of all of the organization's assets and classifies them into one of three categories:

- *IT*
- *IoT*
- *OT*

This value is based on the discovered details for the asset, such as:

- Mac address
- Vendor
- Protocol
- Type

Carousel

The carousel shows a quick view of your sites.

Map

The map helps you visualize your network and its health, and let you quickly understand where to focus your attention. Vantage draws lines across the map to depict the location of threat actors and the sites that their attacks target. You can select a site on the map to view it on the carousel. Use the **2D** and **3D** buttons to switch between flattened and spherical views of the Earth.

Elements

Common *user interface (UI)* elements are used in the different pages and sections.

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.

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.

Support

The support  icon opens a popup that gives you access to more items.

[Documentation](#) 
[Open a Support Case](#) 
[Check Vantage Status](#) 
[Developer API Docs](#) 

Top navigation bar

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

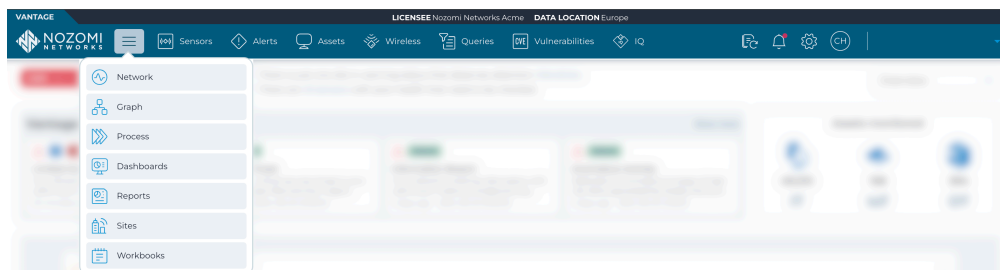



Figure 4. Top navigation bar

Hamburger menu

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

- [Network \(on page 16\)](#)
- [Graph \(on page 16\)](#)
- [Process \(on page 16\)](#)
- [Dashboards \(on page 16\)](#)
- [Reports \(on page 16\)](#)
- [Sites \(on page 16\)](#)
- [Workbooks \(on page 16\)](#)

Network

This button opens the **Network** page. For more details, see [Network \(on page 163\)](#).

Graph

This button opens the **Graph** page. For more details, see [Graph \(on page 169\)](#)

Process

This button opens the **Process** page. For more details, see [Process \(on page 175\)](#)

Dashboards

This button opens the **Dashboards** page. For more details, see [Dashboards \(on page 181\)](#).

Reports

This button opens the **Reports** page. For more details, see [Reports \(on page 189\)](#).

Sites

This button opens the **Sites** page. For more details, see [Sites \(on page 193\)](#).

Workbooks

This button opens the **Workbooks** page. For more details, see [Workbooks \(on page 130\)](#).

Sensors

This button opens the **Sensors** page. For more details, see [Sensors \(on page 21\)](#).

Alerts

This button opens the **Alerts** page. For more details, see [Alerts \(on page 57\)](#).

Assets

This button opens the **Assets** page. For more details, see [Assets \(on page 77\)](#).

Wireless

This button opens the **Wireless** page. For more details, see [Wireless \(on page 105\)](#).

Queries

This button opens the **Queries** page. For more details, see [Queries \(on page 113\)](#).

Vulnerabilities

This button opens the **Vulnerabilities** page. For more details, see [Vulnerabilities \(on page 127\)](#).

(Vantage) IQ

This button opens the **Vantage IQ** page. For more details, see [Vantage IQ \(on page 141\)](#).

Async operations

This button opens the **Asynchronous operations** page. For more details, see [Async operations \(on page 203\)](#).

What's new

This button opens the **What's new** sidebar. For more details, see [What's new drawer \(on page 207\)](#).

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 \(on page 215\)](#).

Organization

This button opens the profile **Organization** page. For more details, see [Organizations menu \(on page 221\)](#).



Chapter 2. Sensors



Sensors

The **Sensors** page lets you view all of the sensors that you have in your system.

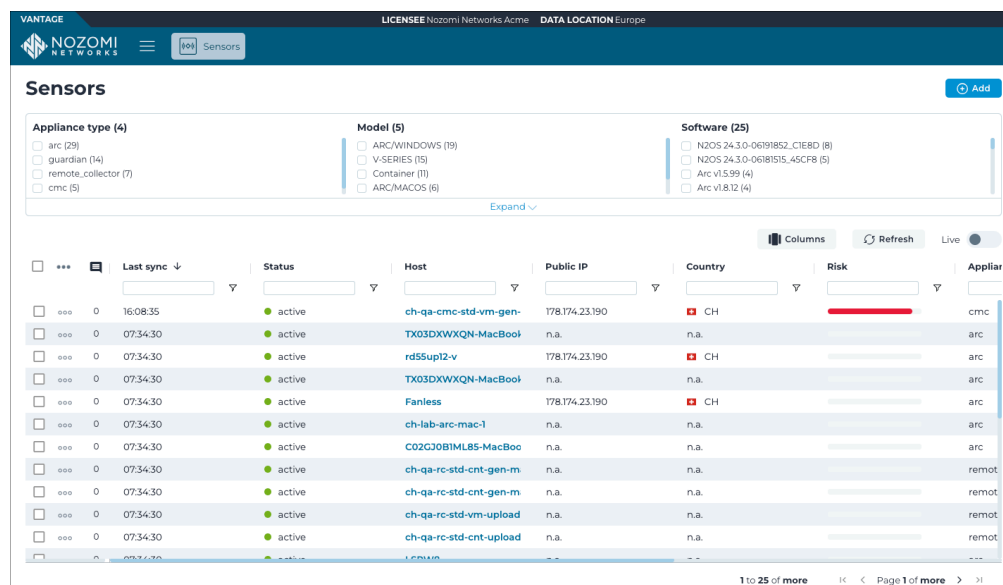


Figure 5. Sensors page

Add

This button lets you connect a new sensor.

Appliance type

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

Model

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

Software

This shows a list of all the software types 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 sensor.

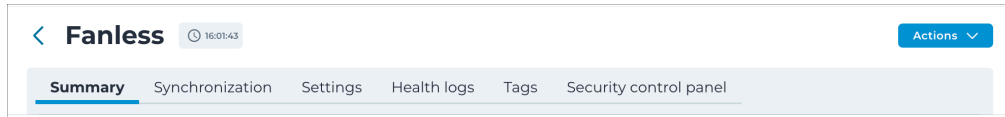


Figure 6. Details page

Actions dropdown

This dropdown gives you access to these actions:

- [Delete \(on page 33\)](#)
- [Reset Token \(on page 34\)](#)
- [Renew Licenses \(on page 35\)](#)
- [Migrate Site \(on page 36\)](#)

Summary

For more details, see [Summary tab \(on page 23\)](#).

Synchronization

For more details, see [Synchronization tab \(on page 25\)](#).

Settings

For more details, see [Settings tab \(on page 26\)](#).

Health logs

For more details, see [Health logs tab \(on page 26\)](#).

Tags

For more details, see [Tags tab \(on page 28\)](#).

Security control panel

For more details, see [Security control panel tab \(on page 31\)](#).

Related information

[Open the details page \(on page 39\)](#)

Summary tab

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

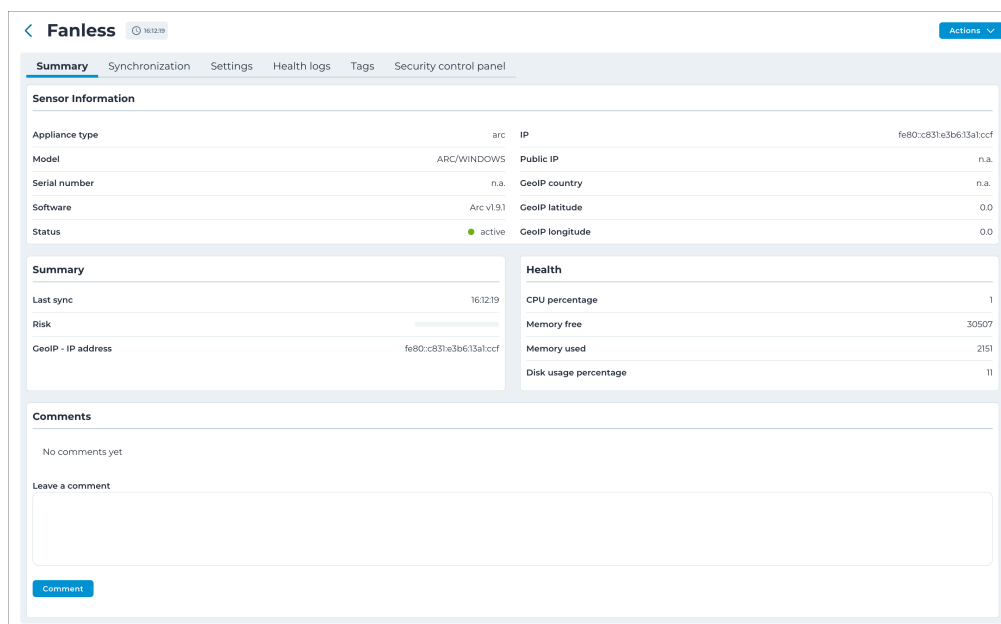


Figure 7. Summary tab

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 \(on page 22\)](#)

Synchronization tab

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

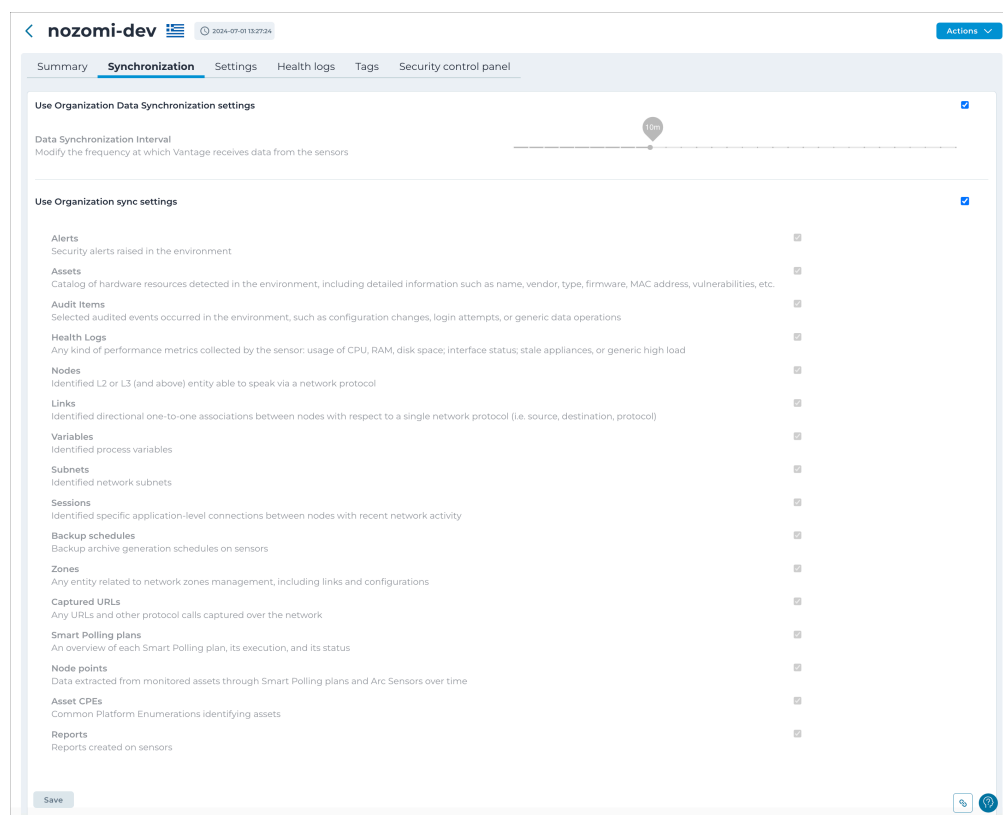


Figure 8. Synchronization tab

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.

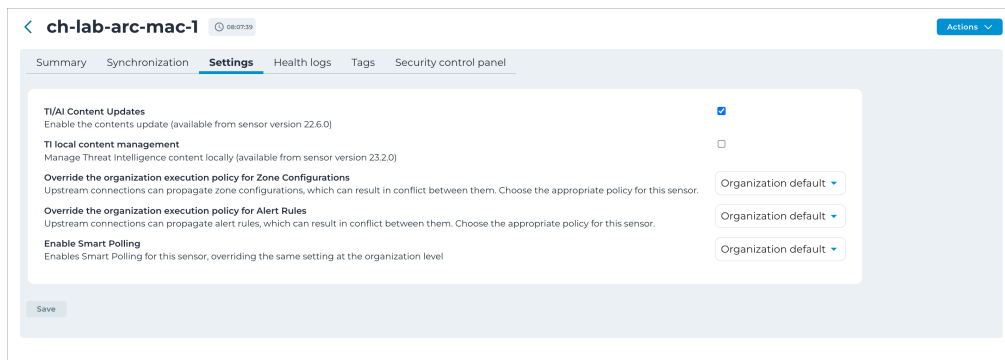


Figure 9. Settings tab

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

- [Asset Intelligence \(AI\)](#)
- [Threat Intelligence \(TI\)](#)

Health logs tab

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

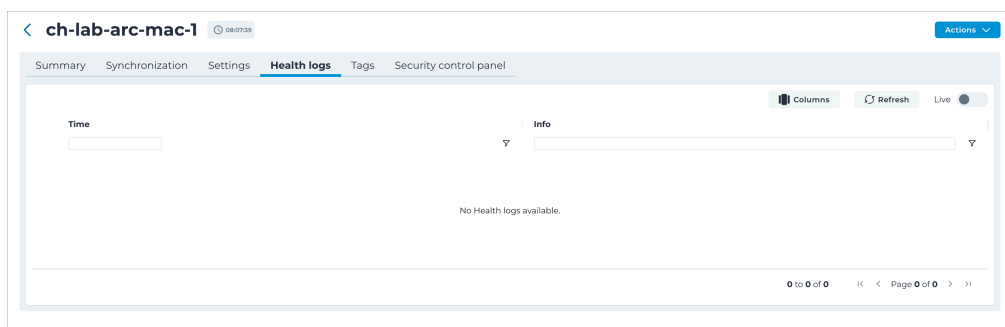


Figure 10. Health logs tab

Delete a health log

The actions menu lets you delete a health log.

Procedure

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

**Note:**

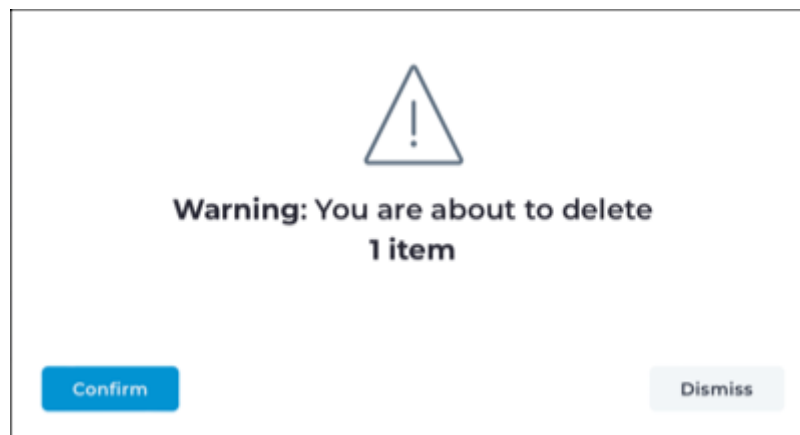
If you haven't added a sensor yet, Vantage opens the **Make connections** page where you can add one. If you have previously added a sensor, all the sensors that Vantage recognizes show.

2. [Open the details page \(on page 39\)](#) 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.

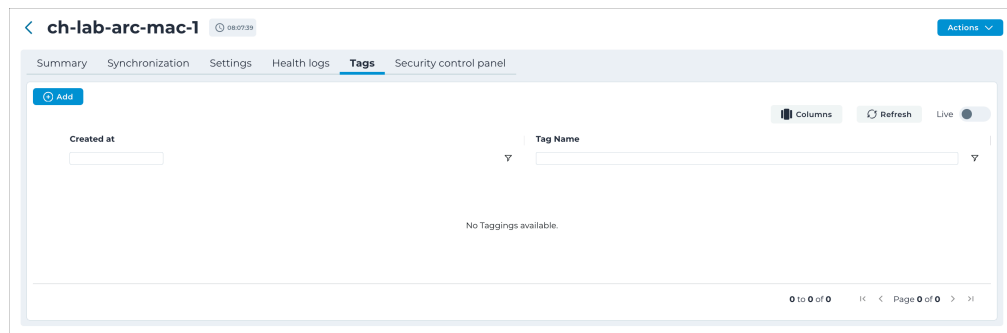


Figure 11. Tags tab

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 \(on page 29\)](#) 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 \(on page 29\)](#)

[Delete a tag from a sensor \(on page 30\)](#)

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 \(on page 39\)](#) 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 \(on page 28\)](#)

[Delete a tag from a sensor \(on page 30\)](#)

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 \(on page 39\)](#) 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 \(on page 28\)](#)

[Add a tag to a sensor \(on page 29\)](#)

Security control panel tab

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

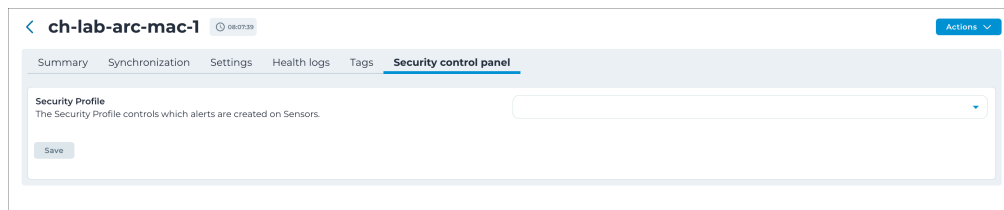


Figure 12. Security control panel tab

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

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.

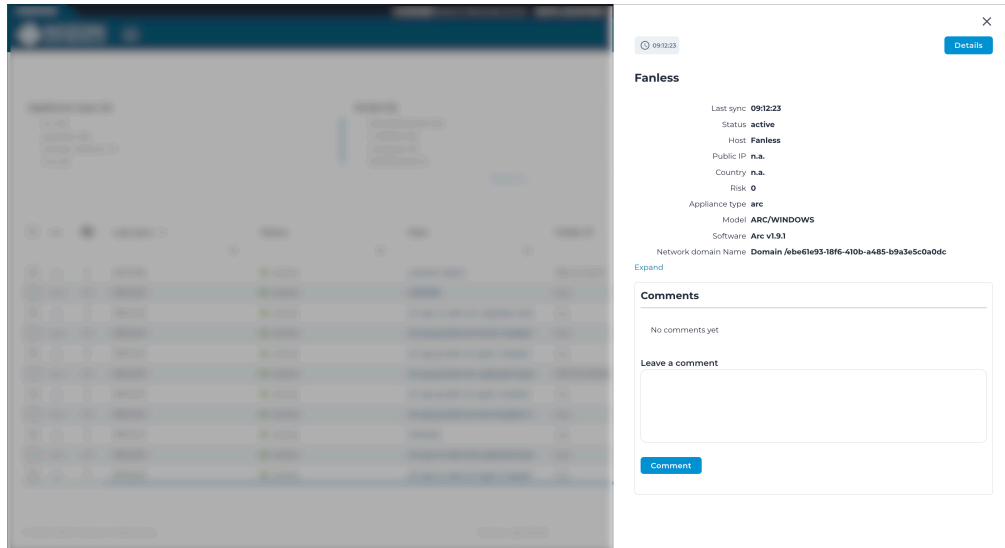


Figure 13. Summary drawer

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:

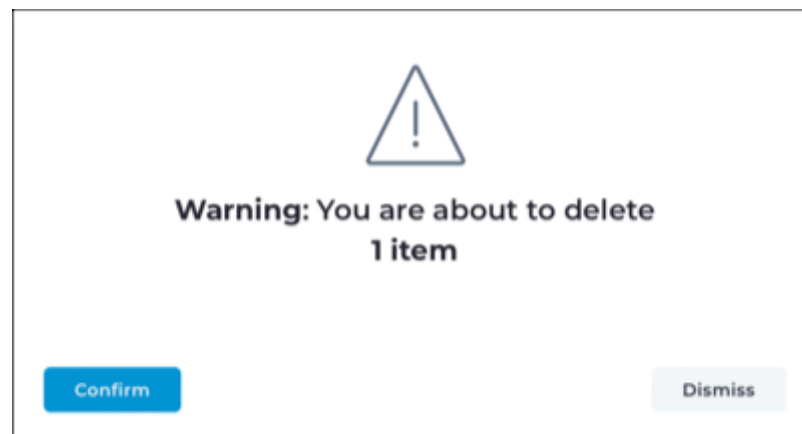
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **⋮** icon

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 \(on page 47\)](#) 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 \(on page 47\)](#) 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:

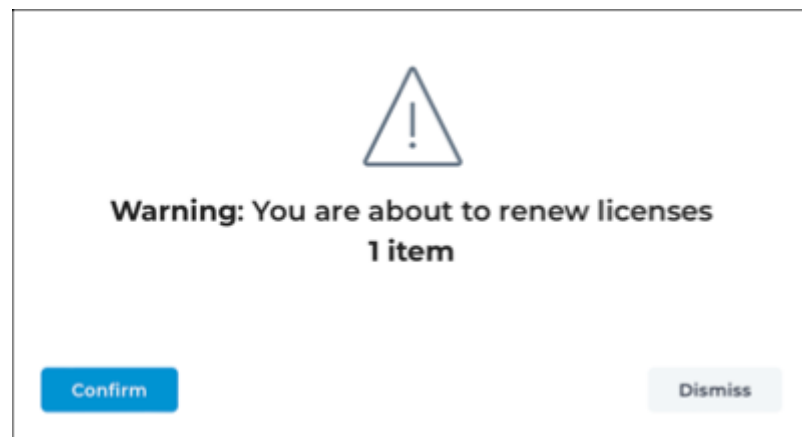
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **⋮** icon

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:

1 Site selection — 2 Confirmation — 3 Result

☒ Choose an existing site ☐ Create a new site

Site Country

▼ ▼

No Rows To Show

0 to 0 of 0 |< < Page 0 of 0 > >|

Continue Cancel

Choose from:

- Choose an existing site
- Create a new site

6. If you chose **Choose an existing site**, do the steps below:

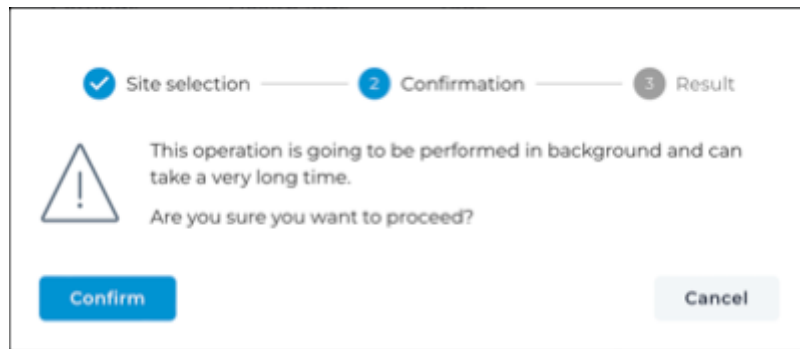
- In the **Site** field, use the filter to select the site.
- In the **Country** field, use the filter to select the country.
- Select **Continue**.
Result: A dialog shows.
- Go to step [8 \(on page 38\)](#).

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.

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 \(on page 22\)](#) opens.

Related information

[Details page \(on page 22\)](#)

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 \(on page 32\)](#) opens.

Related information

[Summary drawer \(on page 32\)](#)

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. \(on page 41\)](#)

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 \(on page 40\)](#).

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.

My sensor is:	N2OS	Arc	Guardian Air
---------------	------	-----	--------------

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 \(on page 42\)](#) procedure
- Select **Arc** and do the [Add an Arc sensor \(on page 43\)](#) procedure
- Select **Guardian Air** and do the [Add a Guardian Air sensor \(on page 46\)](#) 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 \(on page 41\)](#) 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 \(on page 52\)](#).

Copy the connection host [URL](#) and sync token, and paste them in a safe location.

5. Before you continue, you must [configure the sensor \(on page 47\)](#).

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 \(on page 41\)](#) procedure and choose the **Arc** option.

Procedure

1. From the section on the right, 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 [9 \(on page 45\)](#)
- Alternatively, to modify the settings, go to step [4 \(on page 44\)](#)

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

Configure Arc bundle

The downloaded Arc bundle will include this configuration

Execution Options

Execution time [s] (Applicable to One-shot and Offline modes, set to 0 for unlimited executions)

150

☒ Sigma rules

☒ USB detections

☒ Node points

☐ Smart Polling

☒ Local ARP table

Log level

Info

Traffic monitoring

☐ Enable

☐ Enable continuous mode

Monitoring time [s] per notification

10

Max packets per notification

2000

Max used Memory [MB]

32

Save

**Note:**

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

5. Enable/disable from these options:

- **Sigma rule** (Windows only)
- **Node points**
- **Local ARP table**
- **USB detections** (Windows only)
- **Smart Polling**

6. From the **Log level** dropdown, select the verbosity level for the log files. Select from:
 - Debug
 - Info
 - 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. In the section on the left, download the applicable package.
10. Before you continue, you must [configure the sensor \(on page 47\)](#).

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 \(on page 41\)](#) 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 \(on page 46\)](#)
- To enter the code manually, Select **Deny**, and go to step [4 \(on page 46\)](#)



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 \(on page 47\)](#).

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 \(on page 41\)](#).

About this task

Once you have [added the sensor in Vantage \(on page 41\)](#), you must configure it.

Procedure

1. Log in to the sensor that you want to connect to Vantage.
 2. In the [UI](#) of the sensor, go to the configuration page. If you want to connect a [Central Management Console \(CMC\)](#), 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 \(on page 50\)](#).

Configure an Arc sensor

*It is possible to configure an individual Arc sensor directly from the **Sensors** details page for the related sensor.*

Before you begin

Do the [Add a sensor \(on page 41\)](#) 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 \(on page 39\)](#).
3. In the top right section, select **Actions > Configure Arc Sensor**.

Result: A dialog shows.

4. Choose the applicable options.

Arc configuration on [redacted] -MacBook-Pro-14-inch-2021-
[redacted]

 **Only directly connected Arc sensors will be configured**

 **Execution Options**

Execution time [s] (Applicable to One-shot and Offline modes, set to 0 for unlimited executions)


150

☒ Sigma rules

☒ USB detections

☒ Node points


☒ Discovery

☒ Smart Polling 

☒ Local ARP table

Log level

Info ▼

 **Traffic monitoring**

☐ Enable

Save

Restore default

Dismiss

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 \(on page 41\)](#), make sure that you have [configured the sensor \(on page 47\)](#).

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 \(on page 53\)](#).
4. [Verify the connection of a sensor \(on page 51\)](#).

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 \(on page 53\)](#).

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 \(on page 47\)](#) 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 \(on page 47\)](#) 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 \(on page 52\)](#).
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 \(on page 33\)](#).
2. [Add the sensor to Vantage again. \(on page 41\)](#)



Chapter 3. Alerts



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.

The screenshot displays the Vantage Alerts interface. At the top, there's a header with the Vantage logo and navigation tabs. Below the header, a filter section allows users to refine alerts by Site (1), Acknowledged (1), Status (1), Name (19), Risk (10), and Protocol (25). The main area is a table with columns: Time, Name, Description, Risk, Source, Destination, and Protocol. The table lists several alerts, such as 'PUA domain' and 'Malformed traffic', each with a corresponding risk level and source/destination information. The bottom of the page includes pagination controls showing '1 to 25 of more' and 'Page 1 of more'.

Figure 14. Alerts 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.

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.

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

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 73)

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.

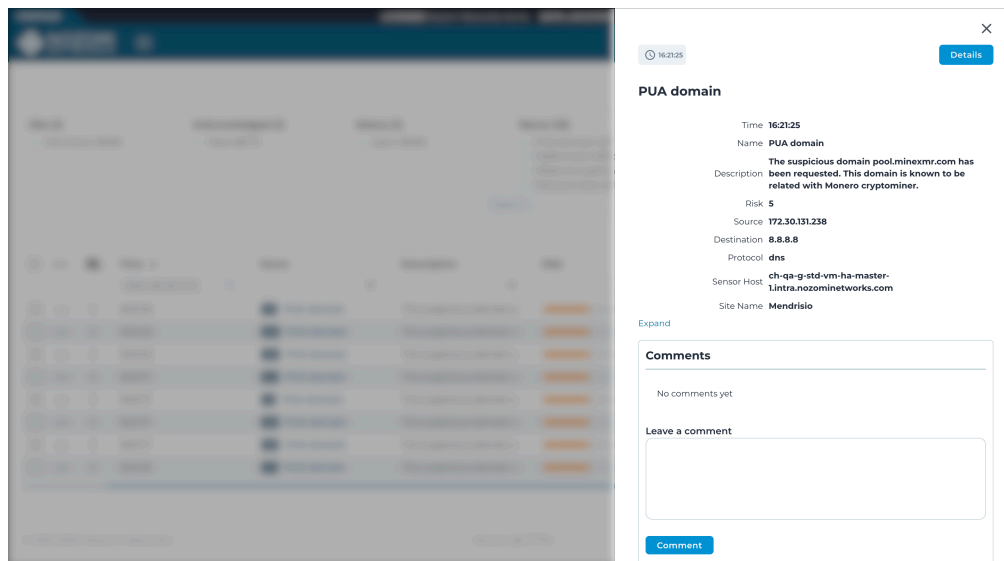


Figure 16. Summary drawer

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 73)

Table interactions

Actions menu

Acknowledge an alert

The actions menu lets you acknowledge one or more alerts.

Procedure

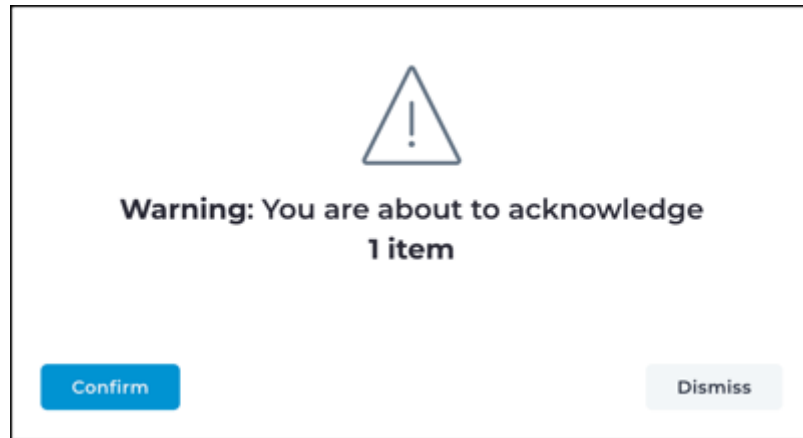
1. In the top navigation bar, select **Alerts**.
2. If you use the **☰** icon in the table, choose a method to select one, or more, items.

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**.

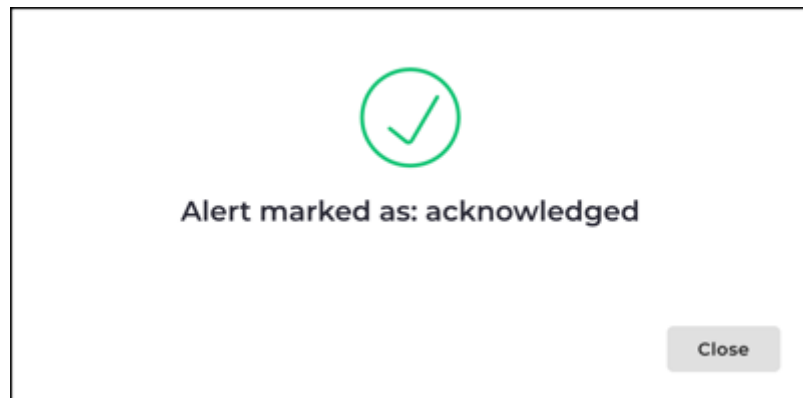
Result: A dialog shows.

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

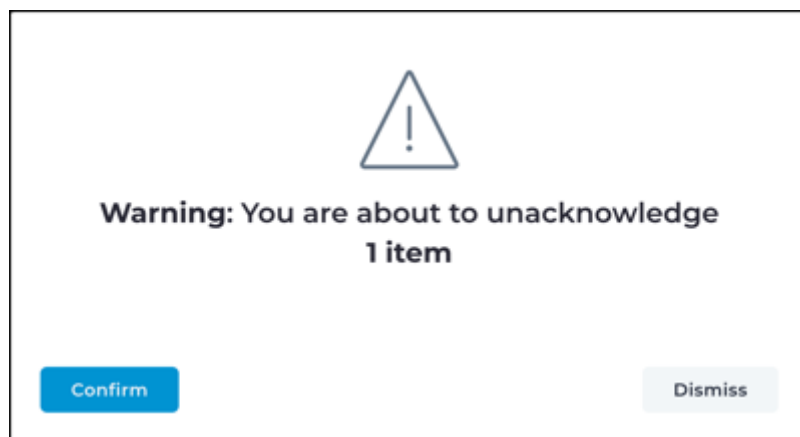
1. In the top navigation bar, select **Alerts**.
2. If you use the **☰** icon in the table, choose a method to select one, or more, items.

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 **Unacknowledge**.

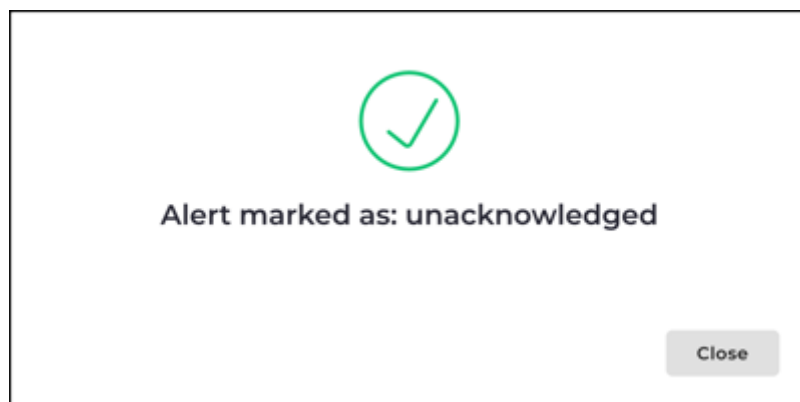
Result: A dialog shows.

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

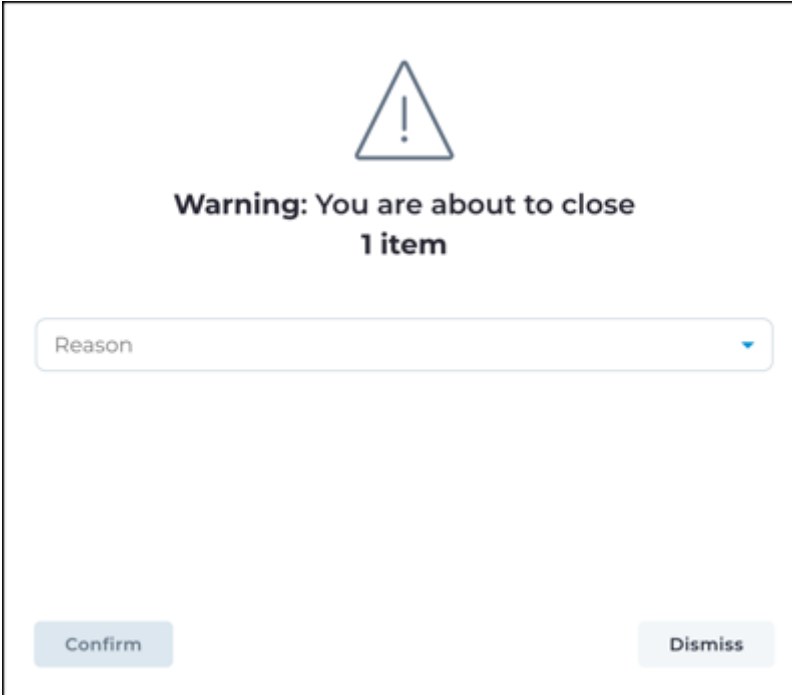
1. In the top navigation bar, select **Alerts**.
2. If you use the **☰** icon in the table, choose a method to select one, or more, items.

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**.

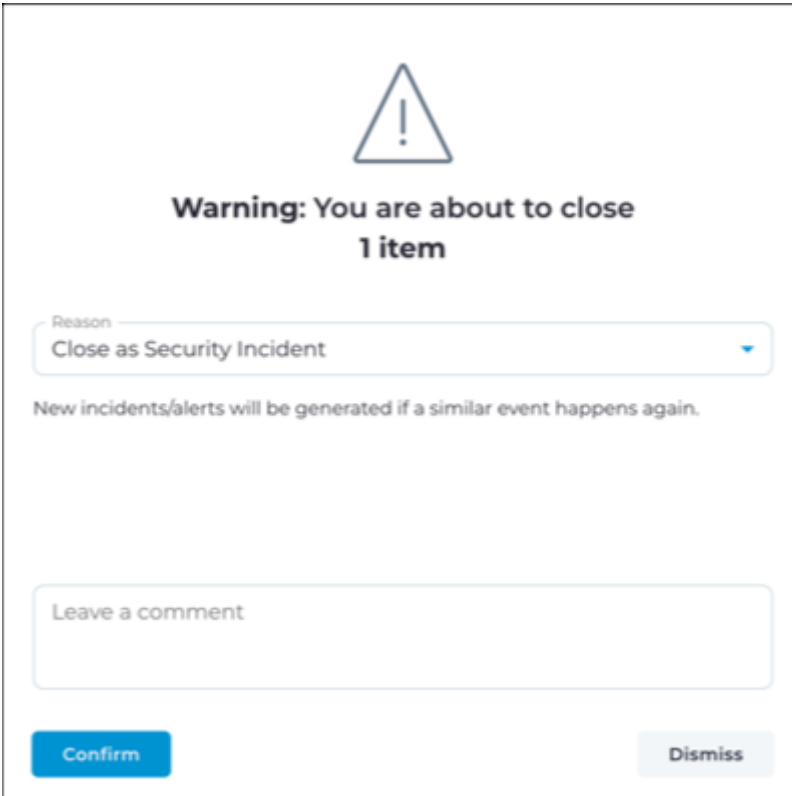
Result: A dialog shows.

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



A warning dialog box with a light gray background and a thin black border. At the top center is a warning icon: a triangle with an exclamation mark inside. Below the icon, the text "Warning: You are about to close 1 item" is centered in a bold, black font. Underneath this text is a dropdown menu with the word "Reason" and a small blue downward arrow on the right. At the bottom of the dialog, there are two buttons: "Confirm" on the left and "Dismiss" on the right, both with a light blue background and rounded corners.

6. Select **Confirm**.



The same warning dialog box as in the previous step, but with additional elements. The dropdown menu now shows "Close as Security Incident" as the selected option. Below the dropdown, the text "New incidents/alerts will be generated if a similar event happens again." is displayed in a smaller, gray font. Below this text is a text input field with the placeholder text "Leave a comment". At the bottom, the "Confirm" button is now highlighted with a solid blue background, while the "Dismiss" button remains light blue.

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.

Create Alert Rule
On Matching Conditions

Add Condition

Condition	matching	ip:dst	45.65.58.98	⊗
Condition	matching	ip:src	192.168.1.1	⊗
Condition	matching	Mac:dst	00:08:e3:ff:da:a0	⊗
Condition	matching	Mac:src	00:68:eb:85:23:bb	⊗
Condition	matching	Protocol	http	⊗
Condition	matching	Transport protocol	tcp	⊗
Condition	matching	Trigger id	9000011	⊗

Add Scope

Take Action

Mute forever

The alert will be muted.

Priority

This rule has maximum priority and is always processed.

Notes

What is the goal of this rule?

Create Cancel

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

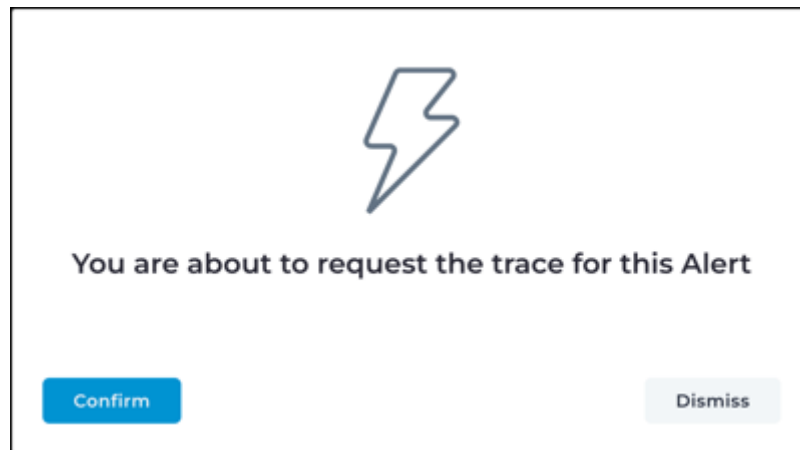
1. In the top navigation bar, select **Alerts**.
2. If you use the **☰** icon in the table, choose a method to select one, or more, items.

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**.

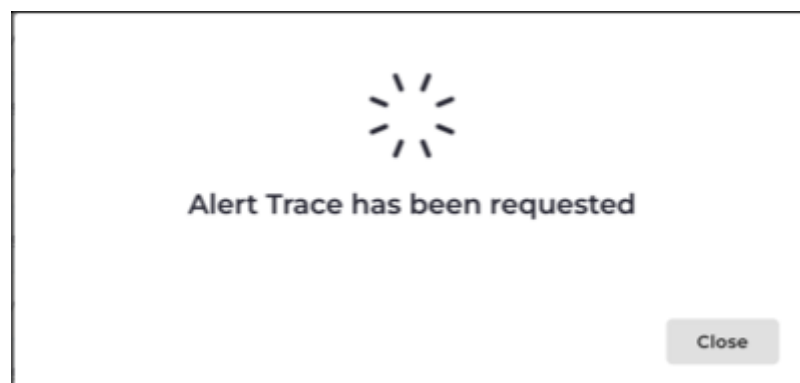
Result: A dialog shows.

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 \(on page 59\)](#) opens.

Related information

[Details page \(on page 59\)](#)

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 \(on page 61\)](#) opens.

Related information

[Summary drawer \(on page 61\)](#)



Chapter 4. Assets



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.

Site (1)	Type (21)	Vendor (25)	Os or firmware (25)
<input type="checkbox"/> Mendrisio (38229)	<input type="checkbox"/> IT device (17369)	<input type="checkbox"/> Cisco (687)	<input type="checkbox"/> macOS (332)
	<input type="checkbox"/> Other (12674)	<input type="checkbox"/> VMware (459)	<input type="checkbox"/> Windows 7 (235)
	<input type="checkbox"/> Computer (6615)	<input type="checkbox"/> Apple (429)	<input type="checkbox"/> Firmware: 10.31 (94)
	<input type="checkbox"/> Printer scanner (355)	<input type="checkbox"/> Canon (287)	<input type="checkbox"/> Android (84)

Site	Name	IP	Type	Vendor	Product name	Os or fi
07:32:28	172.16.37.129	172.16.37.129	IT device	n.a.	n.a.	n.a.
07:32:24	Virtual Machine	172.16.36.79	Computer	VMware	Virtual Machine	n.a.
07:32:23	172.18.66.56	172.18.66.56	Other	n.a.	n.a.	n.a.
07:32:19	172.16.152.31	172.16.152.31	Other	n.a.	n.a.	n.a.
07:32:18	172.30.23.32	172.30.23.32	Other	n.a.	n.a.	n.a.
07:32:18	172.19.25.46	172.19.25.46	IT device	n.a.	n.a.	n.a.
07:32:18	172.16.134.71	172.16.134.71	IT device	n.a.	n.a.	n.a.
07:32:18	172.31.18.35	172.31.18.35	Computer	n.a.	n.a.	n.a.
07:32:15	172.22.2.152	172.22.2.152	IT device	n.a.	n.a.	n.a.
07:32:15	172.31.36.39	172.31.36.39	Other	n.a.	n.a.	n.a.
07:32:15	172.17.209.23	172.17.209.23	IT device	n.a.	n.a.	n.a.

Figure 17. Assets 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 *operating system (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.

The screenshot displays the 'Details' page for an asset in the Nozomi Networks Vantage interface. The asset's IP address is 172.16.37.24. The page is organized into several sections:

- Header:** Includes the Nozomi Networks logo, a navigation menu, and a top bar with the asset's IP and an 'Actions' dropdown.
- Asset Description:** A text block explaining that a computer is a versatile electronic device that processes, stores, and retrieves data.
- Metadata Fields:** A table listing fields such as Type (Computer), Vendor (n.a.), Product name (n.a.), Serial number (n.a.), Os or firmware (Windows Server 2003 SP2), IP (172.16.37.24), Mac address (00:08:e3:ff:fe:08), Mac vendor (Cisco), End of sale date (n.a.), and End of support date (n.a.).
- Summary Tab:** The active tab, showing network statistics (Retransmission: 24%, 0.0 B in last 30'), links (38 active), and a table of received and sent data.
- Properties:** A section indicating 'No properties to display'.
- Roles and Zones:** A section showing 'other' roles and 'Undefined' zones.
- Hardware components:** A section indicating 'No hardware components found'.
- Communications graph:** A section with a message: 'The Graph is empty. This Asset has no Link data available.'
- Comments:** A section with 'No comments yet' and a 'Leave a comment' form.

The footer contains copyright information (© 2013-2024 Nozomi Networks), version information (Version @ 6de33), and a note about the data source (Data for this instance is hosted on the Nozomi Networks platform).

Figure 18. Details page

Actions dropdown

This dropdown gives you access to these actions:

- [Delete \(on page 97\)](#)
- [Export \(on page 98\)](#) (bulk option only)
- [Create Asset Rule From This Asset \(on page 100\)](#)

Tabs

The details page has these tabs:

- [Summary tab \(on page 81\)](#)
- [Processes tab \(on page 82\)](#)
- [Users tab \(on page 83\)](#)
- [Nodes tab \(on page 84\)](#)
- [Links tab \(on page 85\)](#)
- [Sessions tab \(on page 86\)](#)
- [Variables tab \(on page 87\)](#)
- [Vulnerabilities tab \(on page 88\)](#)
- [CPEs tab \(on page 89\)](#)
- [Software tab \(on page 90\)](#)
- [Alerts tab \(on page 91\)](#)
- [Tags tab \(on page 92\)](#)
- [Sensors tab \(on page 95\)](#)

Related information

[Open the details page \(on page 101\)](#)

Summary tab

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

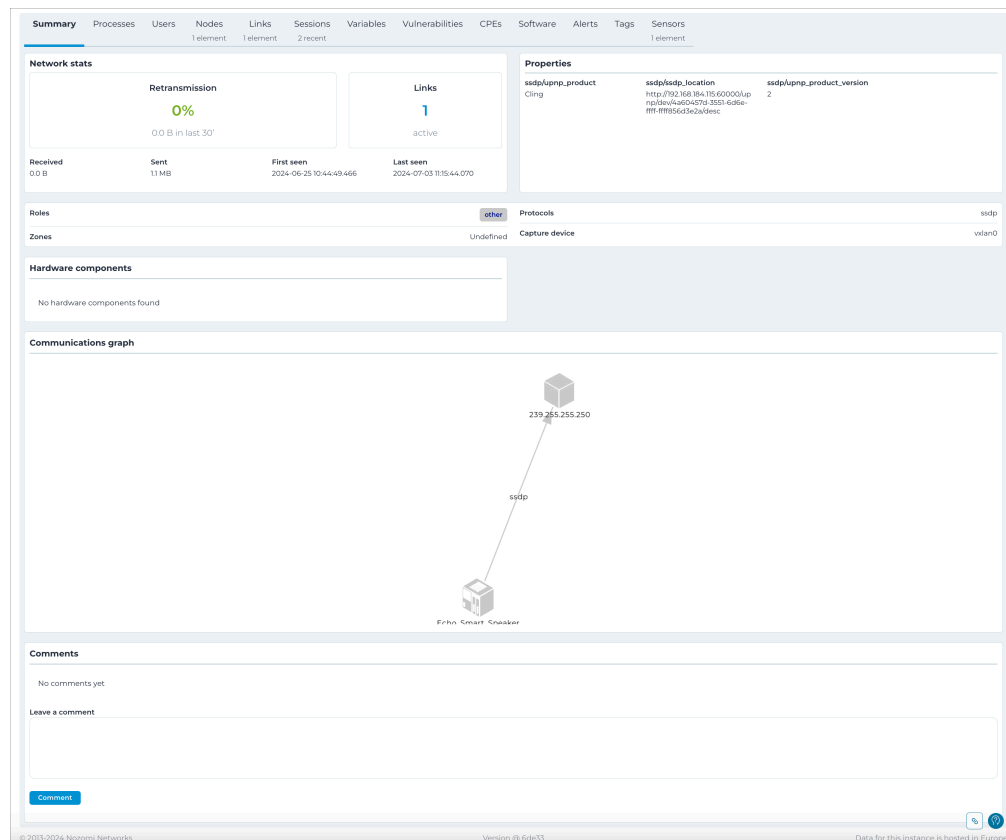


Figure 19. Summary tab

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.

Communications graph

This section shows the same links as shown in the [Links tab \(on page 85\)](#) for this asset.

Comments

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

Processes tab

The **Processes** tab shows all the processes that Vantage has detected for this asset.

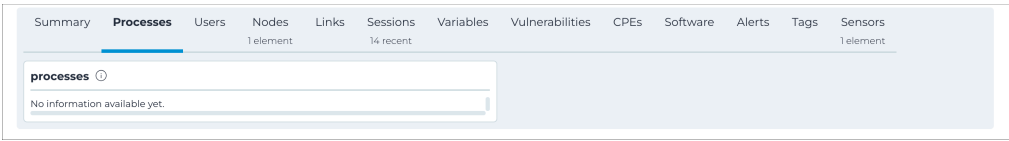


Figure 20. Processes tab

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.

Users tab

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

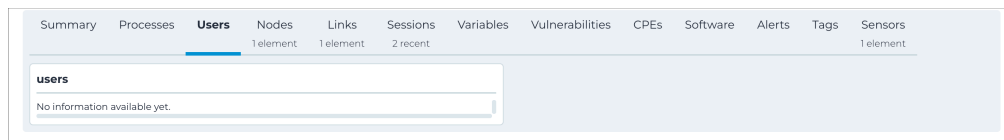


Figure 21. Users tab


Columns

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

Refresh

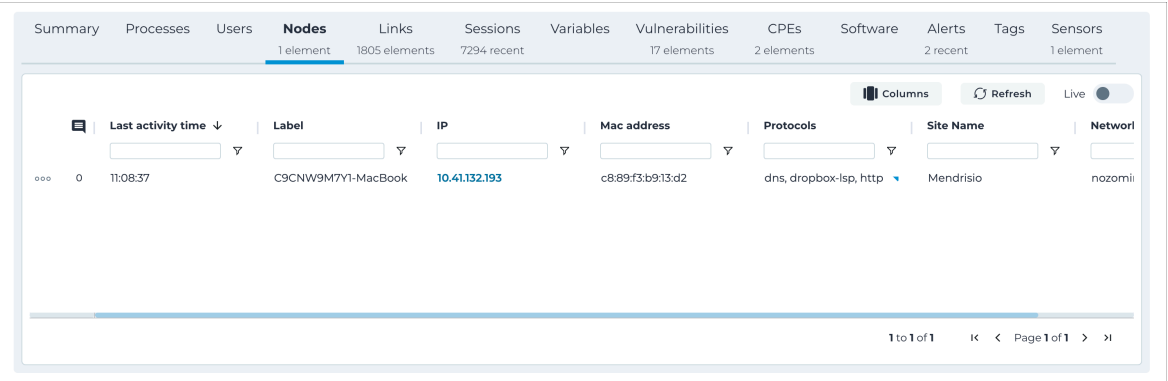
The **Refresh**  icon lets you immediately refresh the current view.

Live

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

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.

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 tab

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

Summary	Processes	Users	Nodes 1 element	Links 1805 elements	Sessions 7294 recent	Variables	Vulnerabilities 17 elements	CPEs 2 elements	Software	Alerts 2 recent	Tags	Sensors 1 element
<div>Columns Refresh Live</div>												
		Last activity time ↓	From	To	Protocol	Transport protocols	First activity time	It				
<input type="checkbox"/>	o	11:13:24	10.41.132.193	104.18.11.224	https	tcp	08:56:14	f				
<input type="checkbox"/>	o	11:13:23	10.41.132.193	13.33.187.6	https	tcp	2024-06-27 14:09:05	f				
<input type="checkbox"/>	o	11:13:18	10.41.132.193	52.123.145.4	https	tcp	2024-07-01 09:29:59	f				
<input type="checkbox"/>	o	11:13:10	10.41.132.193	52.111.227.14	https	tcp	2024-06-27 12:37:07	f				
<input type="checkbox"/>	o	11:13:08	10.41.132.193	34.107.180.209	https	tcp	09:20:50	f				
<input type="checkbox"/>	o	11:12:51	10.41.132.193	54.200.230.77	https	tcp	09:34:51	f				
<input type="checkbox"/>	o	11:12:46	10.41.132.193	52.112.100.5	https	tcp	11:00:50	f				
<input type="checkbox"/>	o	11:10:07	10.41.132.193	3.74.137.41	https	tcp	11:08:07	f				
<input type="checkbox"/>	o	11:10:06	10.41.132.193	255.255.255.255	dropbox-lsp	udp	2024-07-03 11:13:52	t				
<input type="checkbox"/>	o	11:08:43	10.41.132.193	3.90.158.208	https	tcp	2024-02-19 10:37:18	f				
<input type="checkbox"/>	o	11:08:42	10.41.132.193	50.18.194.39	https	tcp	2024-03-04 17:04:51	f				
<input type="checkbox"/>	o	11:08:42	10.41.132.193	3.65.102.105	https	tcp	2024-02-19 10:26:31	f				
<input type="checkbox"/>	o	11:08:42	10.41.132.193	52.109.89.108	https	tcp	11:06:42	f				
<input type="checkbox"/>	o	11:08:40	10.41.132.193	140.82.113.26	https	tcp	2024-05-21 08:48:50	f				

Figure 22. Links tab


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 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.

SummaryProcessesUsersNodes1 elementLinks1805 elementsSessions7294 recentVariablesVulnerabilities17 elementsCPEs2 elementsSoftwareAlerts2 recentTagsSensors1 element

ColumnsRefreshLive

	Last activity time	From	To	Status	Protocol	Transport protocol	First ac
...	0 11:13:26	10.41.132.193	13.33.187.6	ACTIVE	https	tcp	11:13:26
...	0 11:13:26	10.41.132.193	13.33.187.6	ACTIVE	https	tcp	11:12:42
...	0 11:13:25	10.41.132.193	151.101.192.106	ACTIVE	https	tcp	11:12:39
...	0 11:13:23	10.41.132.193	3.91.140.69	ACTIVE	other	udp	11:13:18
...	0 11:11:40	10.41.132.193	140.82.113.26	ACTIVE	https	tcp	11:03:40
...	0 11:08:44	10.41.132.193	162.125.69.13	ACTIVE	https	tcp	11:08:42
...	0 11:07:11	10.41.132.193	162.125.69.21	ACTIVE	https	tcp	11:03:34
...	0 11:07:08	10.41.132.193	3.90.158.208	ACTIVE	https	tcp	10:56:07
...	0 11:07:08	10.41.132.193	142.250.203.110	ACTIVE	https	tcp	11:07:07
...	0 11:07:07	10.41.132.193	34.107.180.209	ACTIVE	https	tcp	10:53:07
...	0 11:07:07	10.41.132.193	104.18.11.224	ACTIVE	https	tcp	10:53:07
...	0 11:07:07	10.41.132.193	175.7.146.54	ACTIVE	other	tcp	11:07:07

Figure 23. Sessions tab

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.

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.

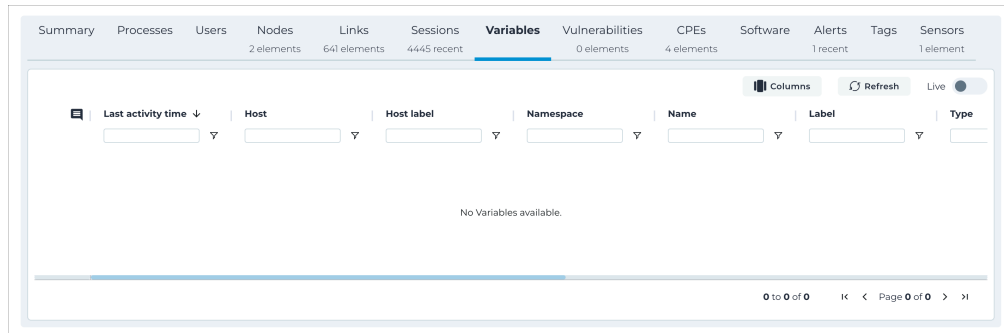


Figure 24. Variables tab


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.

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.

SummaryProcessesUsersNodes1 elementLinks1805 elementsSessions7294 recentVariablesVulnerabilities17 elementsCPEs2 elementsSoftwareAlerts2 recentTagsSensors1 element

ColumnsRefreshLive

<input type="checkbox"/>	***	<input type="checkbox"/>	Time	Asset Name	Asset Type	CVE	Probability	Likelihood	Sc
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-38312	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-38313	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5687	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5688	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5689	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5690	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5691	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5692	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5693	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5694	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5695	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5696	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5697	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5698	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5699	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5700	Possible	0.5	
<input type="checkbox"/>	ooo	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5701	Possible	0.5	

1 to 17 of 17<< < Page 1 of 1 > >>

Figure 25. Vulnerabilities tab


Columns

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

Refresh

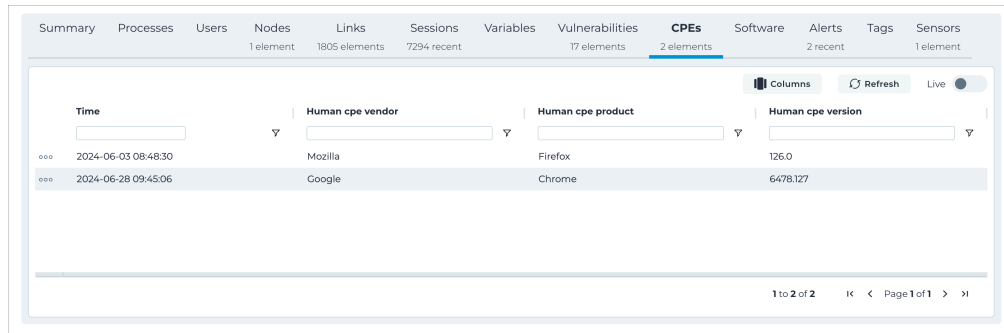
The **Refresh**  icon lets you immediately refresh the current view.

Live

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

CPEs tab

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



Time	Human cpe vendor	Human cpe product	Human cpe version
2024-06-03 08:48:30	Mozilla	Firefox	126.0
2024-06-28 09:45:06	Google	Chrome	6478.127

Figure 26. CPE tab


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.

Software tab

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

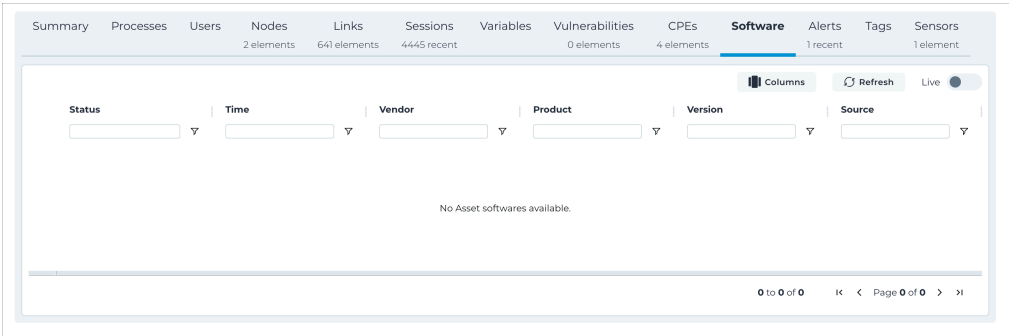


Figure 27. Software tab


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.

Alerts tab

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

Summary	Processes	Users	Nodes	Links	Sessions	Variables	Vulnerabilities	CPES	Software	Alerts	Tags	Sensors
			1 element	1805 elements	7294 recent		17 elements	2 elements		2 recent		1 element

	Time ↓	Name	Description	Risk	Source	Destination	Pr
<input type="checkbox"/>	2024-07-03 14:18:33	TCP flood	A TCP flood was detected	<div><div></div></div>	10.41.132.193	10.41.132.133	ot
<input type="checkbox"/>	2024-06-27 12:22:20	TCP flood	A TCP flood was detected	<div><div></div></div>	10.41.132.193	10.41.132.133	ot
<input type="checkbox"/>	2024-06-18 14:14:20	TCP flood	A TCP flood was detected	<div><div></div></div>	10.41.132.193	10.41.132.133	ot
<input type="checkbox"/>	2024-06-17 14:54:59	Malformed traffic	The UDP header in the p	<div><div></div></div>	n.a.	10.41.132.193	n.
<input type="checkbox"/>	2024-06-10 14:03:16	Malformed traffic	The UDP header in the p	<div><div></div></div>	52.98.61.50	10.41.132.193	n.
<input type="checkbox"/>	2024-06-05 17:14:50	New Node	New node 10.41.132.193 a	<div><div></div></div>	10.41.132.193	n.a.	n.
<input type="checkbox"/>	2024-05-29 11:56:28	Malformed traffic	The UDP header in the p	<div><div></div></div>	10.41.132.193	52.97.186.114	n.
<input type="checkbox"/>	2024-05-27 12:12:36	Malformed traffic	The UDP header in the p	<div><div></div></div>	n.a.	10.41.132.193	n.

1 to 9 of 9 < Page 1 of 1 >

Figure 28. Alerts tab


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.

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.

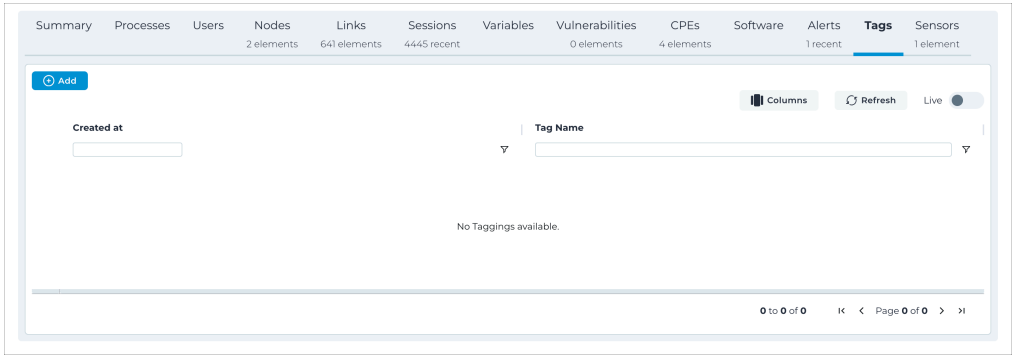


Figure 29. Tags tab

Add new

This button lets you [add a new tag \(on page 93\)](#) to the related asset.


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.

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 \(on page 101\)](#) 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 \(on page 92\)](#)

[Delete a tag from an asset \(on page 94\)](#)

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 \(on page 101\)](#) 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 \(on page 92\)](#)

[Add a tag to an asset \(on page 93\)](#)

Sensors tab

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

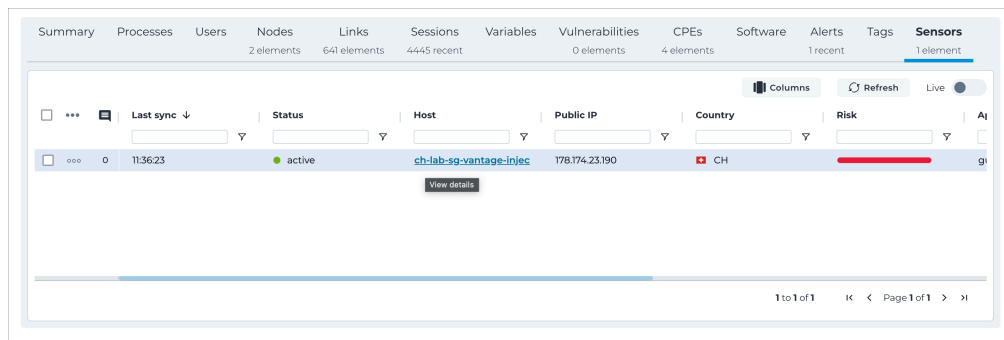


Figure 30. Sensors tab


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.

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.

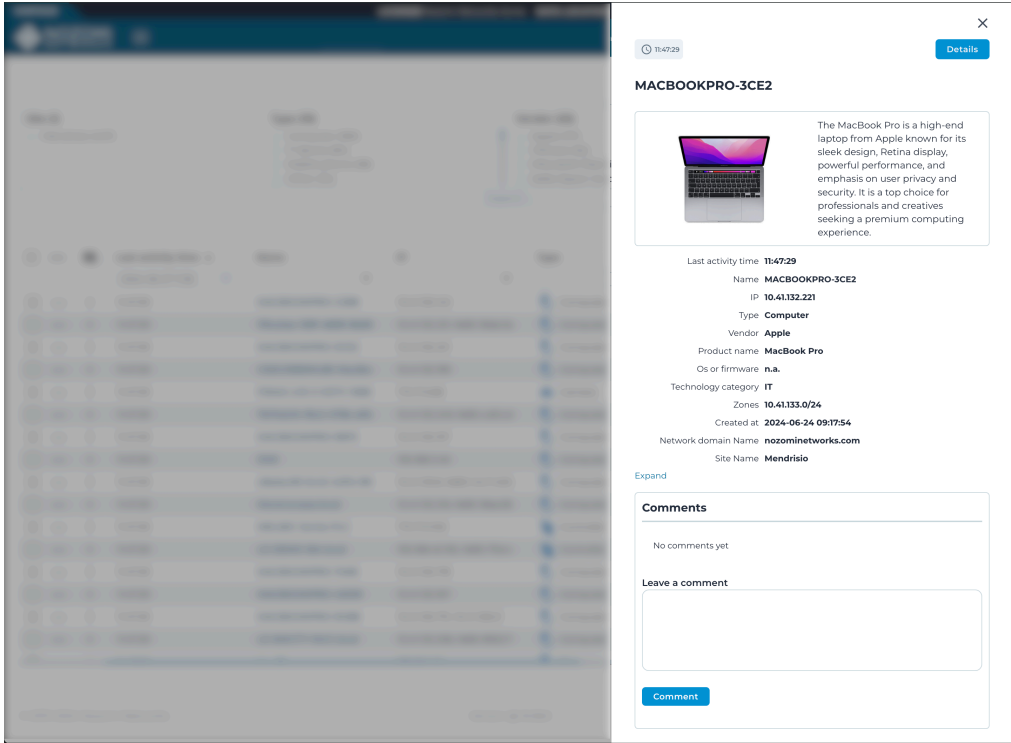


Figure 31. Summary drawer

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 101)

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:

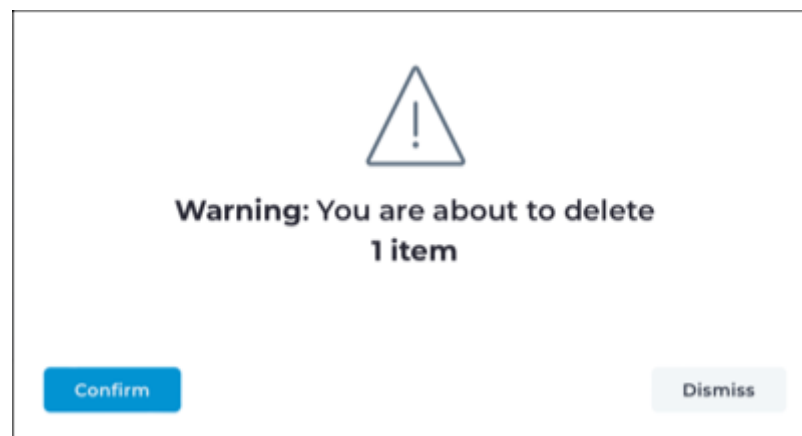
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the **⋮** icon

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

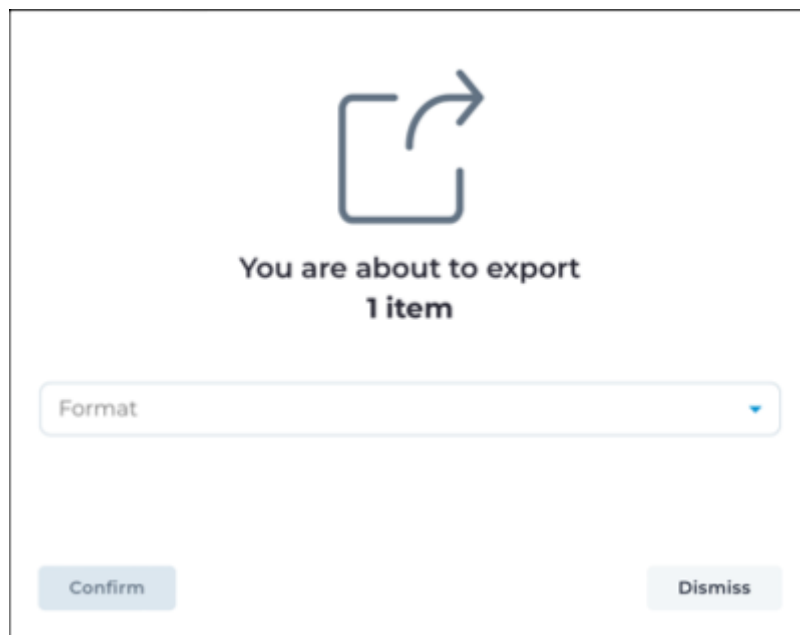
1. In the top navigation bar, select **Assets**.
2. Choose a method to open the actions menu.

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**.

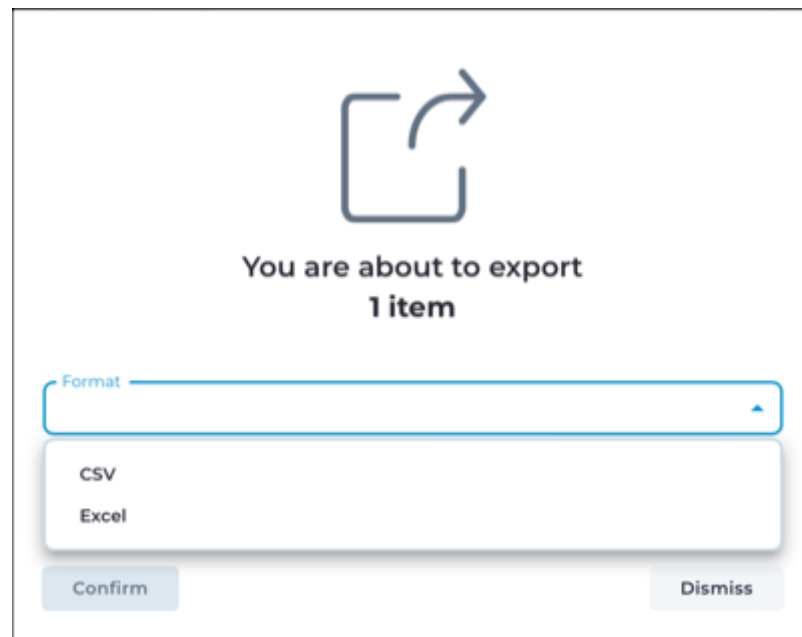


Result: The export dialog shows.

5. Select the **Format** dropdown.

Result: A dialog shows.

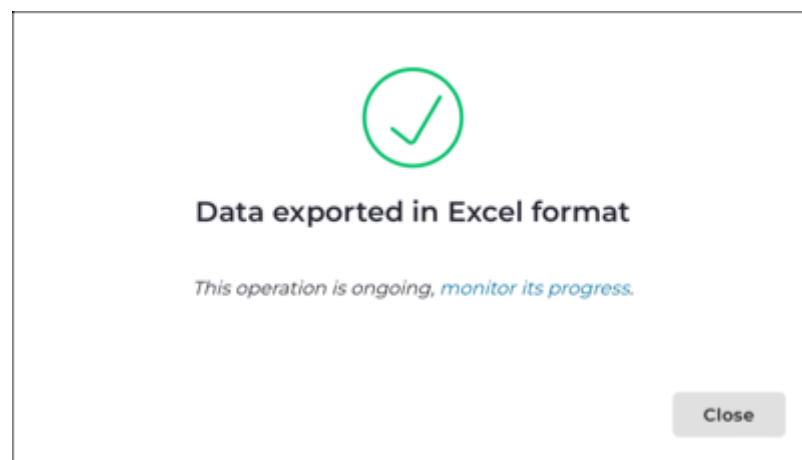
6. In the **Format** dropdown, select the format that you want to export.



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 \(on page 79\)](#) opens.

Related information

[Details page \(on page 79\)](#)

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 \(on page 96\)](#) opens.

Related information

[Summary drawer \(on page 96\)](#)



Chapter 5. Wireless



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.

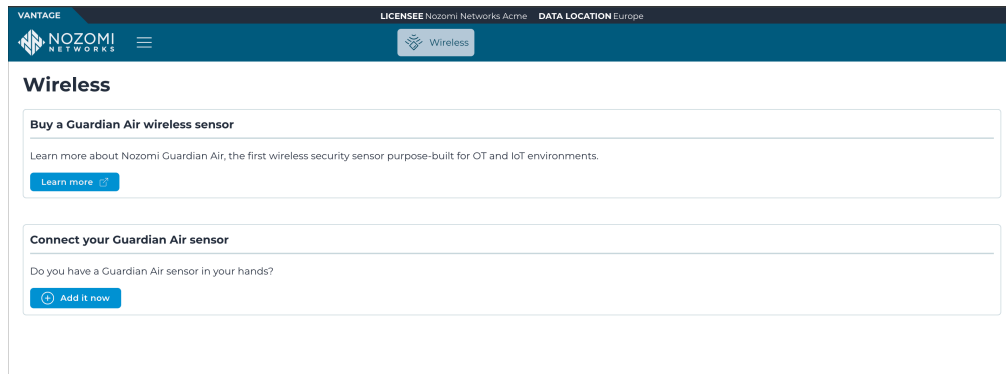


Figure 32. Wireless page (before a Guardian Air sensor has been added)

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.

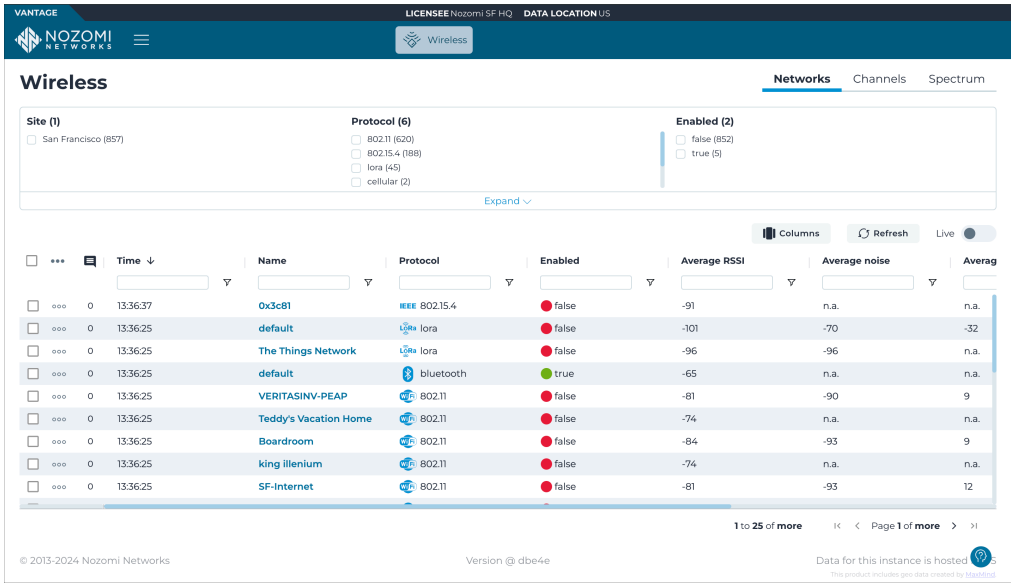


Figure 33. Wireless page (after a Guardian Air sensor has been added)

Networks

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

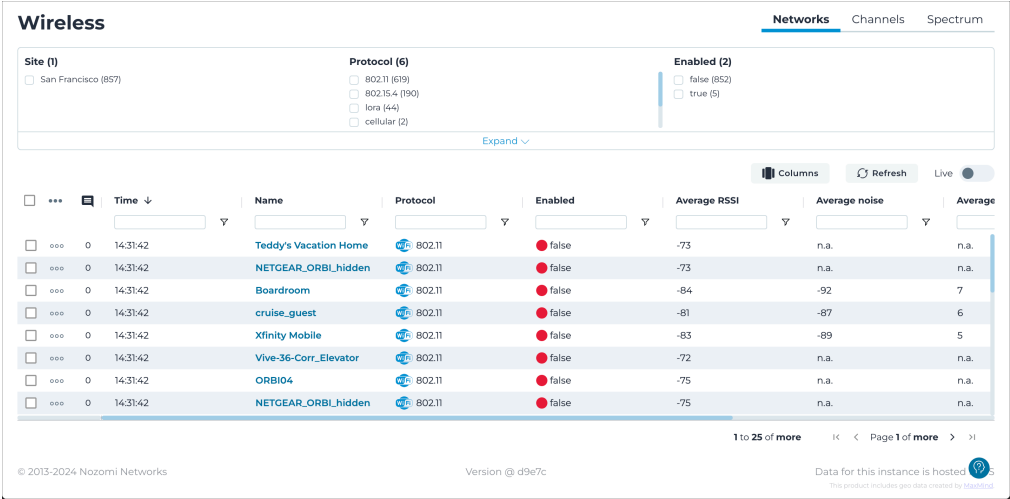


Figure 34. Networks page

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.

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 immediately refresh the graph.

Enable a network

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

Procedure

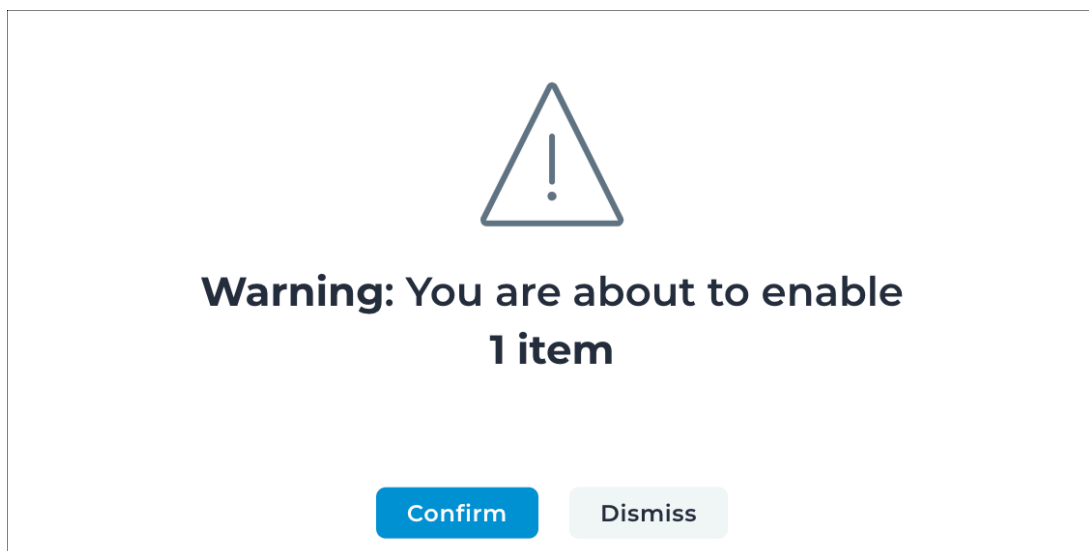
1. In the top navigation bar, select **Wireless**.
2. If you use the **☰** icon in the table, choose a method to select one, or more, items.

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**.



Results

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

Channels

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

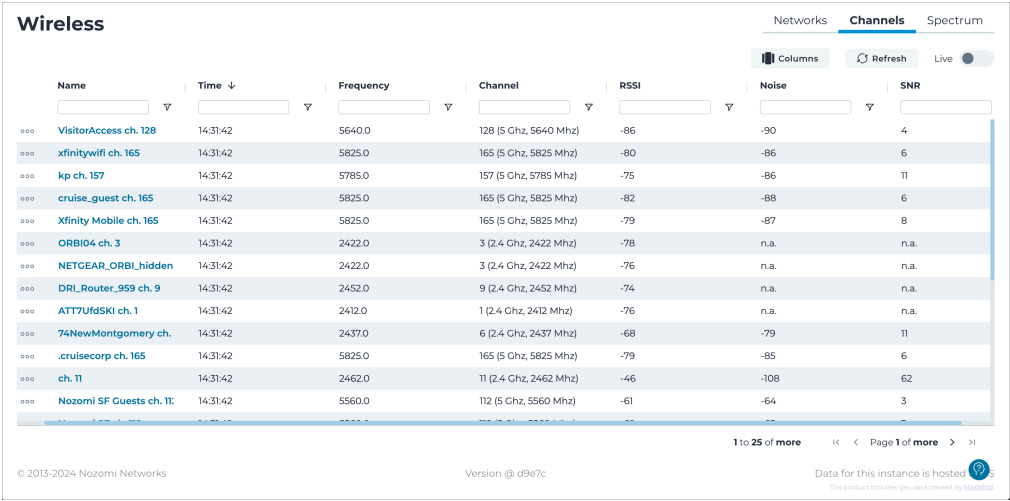


Figure 35. Channels page


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 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.

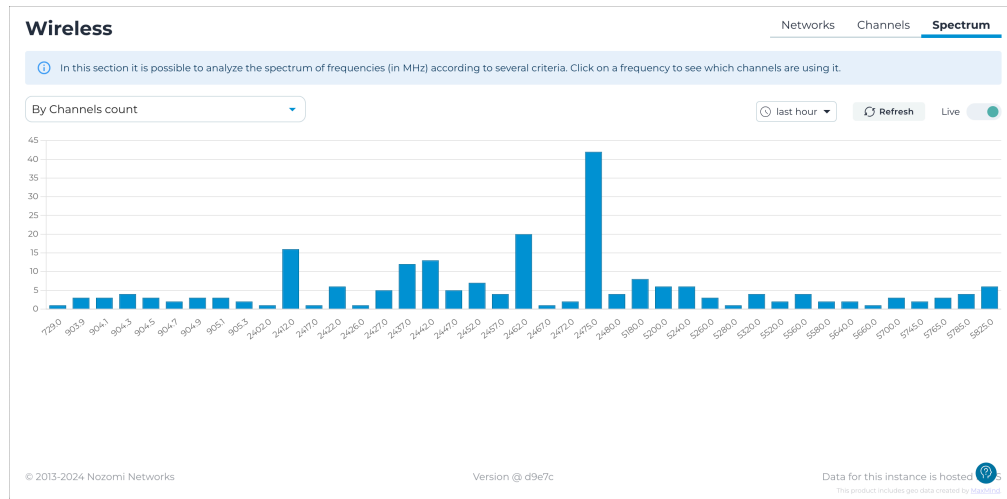


Figure 36. Spectrum page

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

Refresh

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

Live

The live  toggle lets you immediately refresh the graph.

Chapter 6. Queries



Queries

The **Queries** 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.

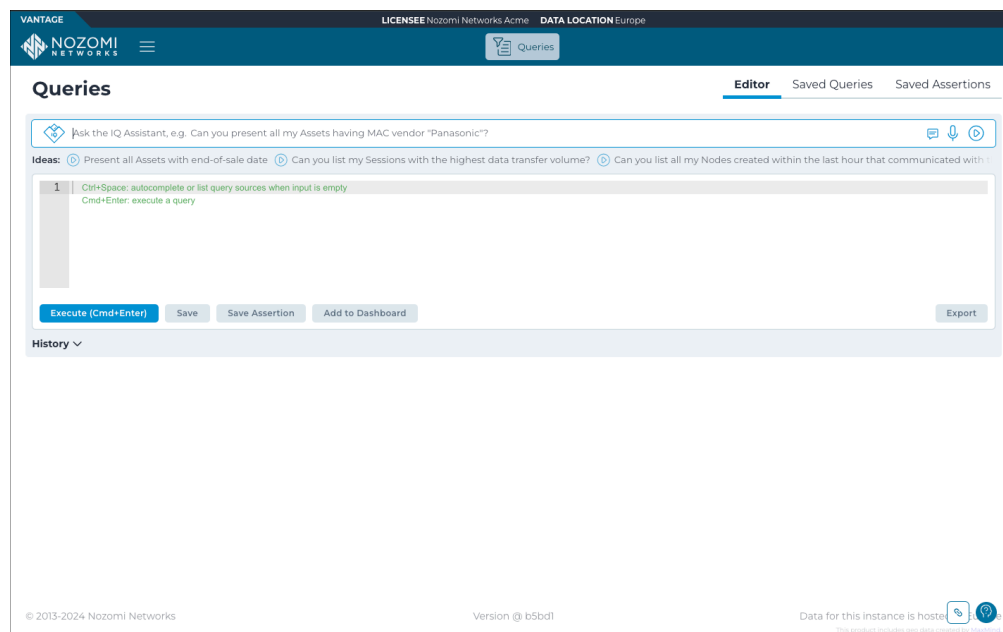


Figure 37. Queries page

Editor

This tab 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
```

Saved Queries

This section shows all your saved queries.

Saved Assertions

This section shows all your saved assertions.

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

Usage: When `assert_empty` is appended to a query, Vantage returns true if the dataset doesn't contain records. If the dataset contains records, it returns or false.

Description: `assert_empty` is rendered as a green or red bar; use it to express conditions you want to verify in the Vantage dataset.

Examples:

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

assert_not_empty

Usage: When `assert_not_empty` is appended to a query, Vantage returns true if the dataset contains records. If the dataset doesn't contain records, it returns or false.

Description: `assert_not_empty` is rendered as a green or red bar; use it to express conditions you want to verify in the Vantage dataset.

Examples:

```
links | where protocol == "iecl04" | where  
minutes_ago(last_activity_time) < 5 | assert_not_empty
```

bucket

Usage: `bucket <field> <range>`

Description: `bucket` interprets field as a numeric value and groups the data in multiples of range.

Examples:

```
alerts | bucket risk 3
```

count

Usage: When `count` is appended to a query, Vantage returns the number of records in the dataset.

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

Examples:

```
links | count
```

column

Usage: `column <value_field> <count_field>`

Description: `column` renders 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
```

exclude

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

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

Examples:

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

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
```

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 the `nodes_id` and the `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>`

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
```

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>

Description: select lets you 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)
```

sort

Usage: sort <field> [asc|desc]

Description: Arranges the dataset by the specified field. Specify asc (ascending) or desc (descending) to define the sort order; the default order is ascending.

Examples:

```
assets | sort level
```

```
alerts | sort risk desc
```

uniq

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

Description: Reduce the dataset by returning only those records that have a unique value in the specified field.

Examples:

```
alerts | uniq type_id risk
```

value

Usage: value <field>

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)
```

where

Usage:

```
where <field1>

[|=|!=|>|=|>|<|<=|
include?!include?|start_with?!start_with?|end_with?!end_with?|in_subnet?|in?!in?] <field2>]
```

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

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
```

The following operators are specific to these data types:

- `in_subnet?` requires a subnet in [classless inter-domain routing \(CIDR\)](#) notation as its right operand.
- `in?` and `!in?` use [JSON](#) arrays as their right operand.

Functions

A list of example query functions.

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>)`

Description: Returns the number of days between the timestamp field and the time that the query is executed.

Examples:

```
alerts | select days_ago(time)
```

```
alerts | where days_ago(time) < 20
```

```
alerts | where time >= days_ago(20)
```



Note:

This is the syntax that gives the best query performance

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")
```

gauge

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

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)
```

hours_ago

Usage: hours_ago(<field>)

Description: Returns the number of seconds between the timestamp field and the time the query was executed.

Examples:

```
alerts | select hours_ago(time)
```

```
alerts | where hours_ago(time) < 20
```

```
alerts | where time >= hours_ago(20)
```



Note:

This is the syntax that gives the best query performance

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) != ""
```

```
assets | expand ip | select ipv4(expanded_ip)
```

**Note:**

`assets.ip` is an array, you need to expand it with the `expand` operator to use the `ipv4` function.

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) != ""
```

```
assets | expand ip | select ipv6(expanded_ip)
```

**Note:**

`assets.ip` is an array, you need to expand it with the `expand` operator to use the `ipv6` function.

is_empty

Usage: `is_empty(<field>)`

Description: Returns true if the field is an empty string or array; otherwise, returns false.

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; otherwise, returns false.

Examples:

```
alerts | where is_recent(time)
```

minutes_ago

Usage: `minutes_ago(<field>)`

Description: Returns the number of minutes between the timestamp field and the time the query was executed.

Examples:

```
alerts | select minutes_ago(time)
```

```
alerts | where minutes_ago(time) < 20
```

```
alerts | where time >= minutes_ago(20)
```

**Note:**

This is the syntax that gives the best query performance

mult

Usage: `mult(<field1>,<field2>,...)`

Description: Multiplies the fields or literal values in the arguments list.

Examples:

```
alerts | select mult(risk,"10")
```

round

Usage: `round(<field>,[<decimal_places>])`

Description: Round a number at the given decimal_places. If decimal_places is not specified, the number is rounded to the closest 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>)`

Description: Returns the number of seconds between the timestamp field and the time the query was executed.

Examples:

```
alerts | select seconds_ago(time)
```

```
alerts | where seconds_ago(time) < 20
```

```
alerts | where time >= seconds_ago(20)
```

**Note:**

This is the syntax that gives the best query performance

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
```



Chapter 7. Vulnerabilities



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.

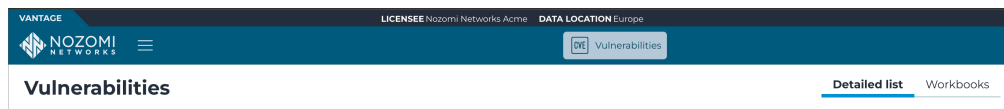


Figure 38. Vulnerabilities page

The Vulnerabilities page has these tabs:

- [Detailed list \(on page 128\)](#)
- [Workbooks \(on page 130\)](#)

Detailed list

The **Detailed list** page shows a list of all the vulnerabilities and their related details.

Vulnerabilities

Detailed list

Workbooks

Site (1)

☐

Mendrisio (9206)

Category (25)

☐ Out-of-bounds Write (29714)

☐ Use After Free (19225)

☐ Improper Input Validation (10894)

☐ Out-of-bounds Read (6546)

Probability (3)

☐ Possible (91925)

☐ Likely (89)

☐ Confirmed (47)

Likelihood (5)

☐ 0.5 (46980)

☐ 0.4 (44622)

☐ 0.8 (323)

☐ 0.9 (89)

Expand

Columns

Refresh

Live

<input type="checkbox"/>	***	Time	Asset Name	Asset Type	CVE	Probability	Likelihood	Score
<input type="checkbox"/>	0	2024-05-29 11:19:00	HIS0164	Paperino	CVE-2023-40455	Possible	0.4	
<input type="checkbox"/>	0	2024-05-29 11:19:00	HIS0164	Paperino	CVE-2023-38586	Possible	0.4	
<input type="checkbox"/>	0	2024-05-29 11:19:00	HIS0164	Paperino	CVE-2022-32845	Possible	0.4	
<input type="checkbox"/>	0	2024-03-20 12:47:24	HIS0164	Paperino	CVE-EOL	Confirmed	1.0	
<input type="checkbox"/>	0	2024-07-02 12:49:53	Apple Mac	Computer	CVE-2023-40455	Possible	0.4	
<input type="checkbox"/>	0	2024-07-02 12:49:53	Apple Mac	Computer	CVE-2023-38586	Possible	0.4	
<input type="checkbox"/>	0	2024-07-02 12:49:53	Apple Mac	Computer	CVE-2022-32845	Possible	0.4	
<input type="checkbox"/>	0	2023-11-09 02:03:48	BMXP342020 Modicon	Controller	CVE-2011-4859	Possible	0.8	
<input type="checkbox"/>	0	2024-07-03 11:13:37	MACBOOKPRO-3B36	Computer	CVE-EOL	Confirmed	1.0	
<input type="checkbox"/>	0	2024-07-01 15:09:11	10.41.200.38	Computer	CVE-EOL	Confirmed	1.0	
<input type="checkbox"/>	0	2024-07-01 08:33:54	d6817b3b-dd21-4c5a-87e	Computer	CVE-2023-40455	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 08:33:54	d6817b3b-dd21-4c5a-87e	Computer	CVE-2023-38586	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 08:33:54	d6817b3b-dd21-4c5a-87e	Computer	CVE-2022-32845	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 07:58:51	MacBook Pro	Computer	CVE-2023-40455	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 07:58:51	MacBook Pro	Computer	CVE-2023-38586	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 07:58:51	MacBook Pro	Computer	CVE-2022-32845	Possible	0.4	
<input type="checkbox"/>	0	2024-07-03 09:34:12	bec71896-df6f-4c69-8be	Computer	CVE-2023-40455	Possible	0.4	
<input type="checkbox"/>	0	2024-07-03 09:34:12	bec71896-df6f-4c69-8be	Computer	CVE-2023-38586	Possible	0.4	
<input type="checkbox"/>	0	2024-07-03 09:34:12	bec71896-df6f-4c69-8be	Computer	CVE-2022-32845	Possible	0.4	
<input type="checkbox"/>	0	2024-07-01 09:09:29	MacBook Pro	Computer	CVE-EOL	Confirmed	1.0	
<input type="checkbox"/>	0	2024-07-01 09:08:17	7b742cf4-f5c2-473b-af2e	Computer	CVE-EOL	Confirmed	1.0	
<input type="checkbox"/>	0	2024-07-01 05:19:55	CO2ZDIYGennaro	Computer	CVE-EOL	Confirmed	1.0	

1 to 25 of more

Figure 39. 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.

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.

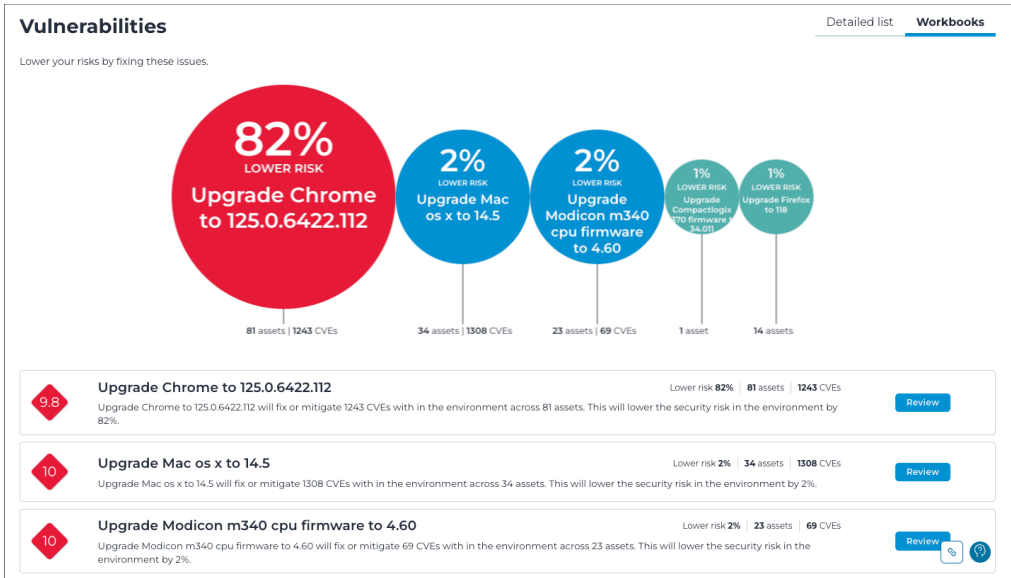


Figure 40. Workbooks page

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 200)

Details page

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

The screenshot displays the Vantage interface for a vulnerability details page. The top navigation bar includes 'VANTAGE', 'NOZOMI NETWORKS', and various icons for Sensors, Alerts, Assets, Queries, Vulnerabilities, and IQ. The main header shows the date '2023-06-26 04:05:38' and the title 'CVE-2014-1776 for Asset lab-ba-johnson.local'. Below the title is an 'Actions' dropdown menu.

The 'VULNERABILITY OVERVIEW' section contains the following details:

CVE	CVE-2014-1776
Category	Use After Free
Probability	Possible
Score	10.0
Status	open
Closed time	never

The 'SUMMARY' section provides a description of the vulnerability: 'Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks."'

The 'References' section lists several links to external resources:

- <http://www.freeeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-inte...>
- <https://technet.microsoft.com/library/security/2963983>
- <http://www.signalsec.com/cve-2014-1776-ie-0day-analysis/>
- <http://blogs.technet.com/b/srd/archive/2014/04/30/protection-strategies-for-the-security-...>
- <http://www.kb.cert.org/vuls/id/222929>
- <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-021>

The 'AFFECTED ASSET' section displays the following information:

Ip	192.168.45.211	Technology category	IT
Mac address	00:50:56:b0:da:8b	Vendor	VMware, Inc.
Name	lab-ba-johnson.local	Product name	VMware Virtual Machine
Type	Computer	Firmware version	n/a

The 'COMMENTS' section shows 'No comments yet' and a 'Leave a comment' form with a 'Comment' button.

Figure 41. Details page

Actions dropdown

This dropdown gives you access to the action: [Resolve Vulnerability \(on page 136\)](#).

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.

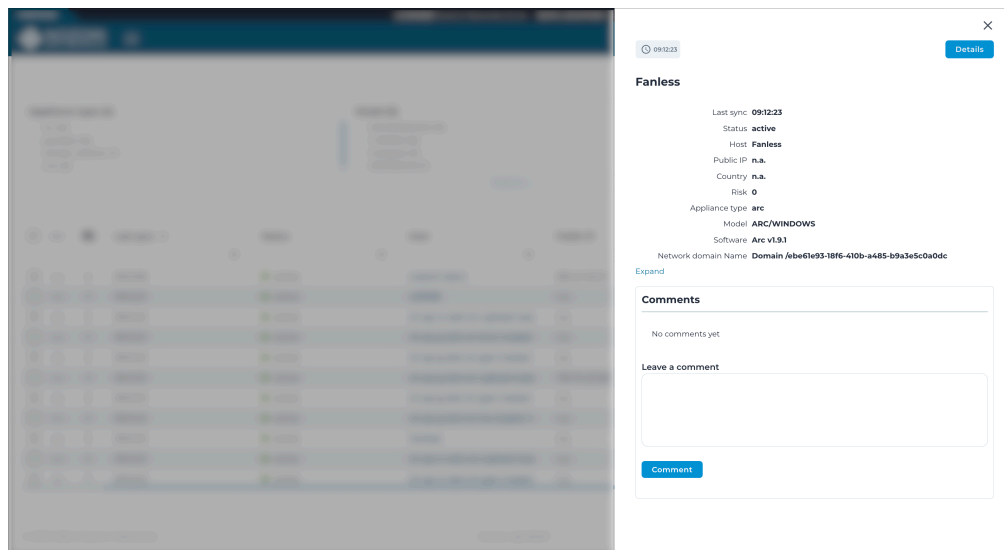


Figure 42. Summary drawer

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

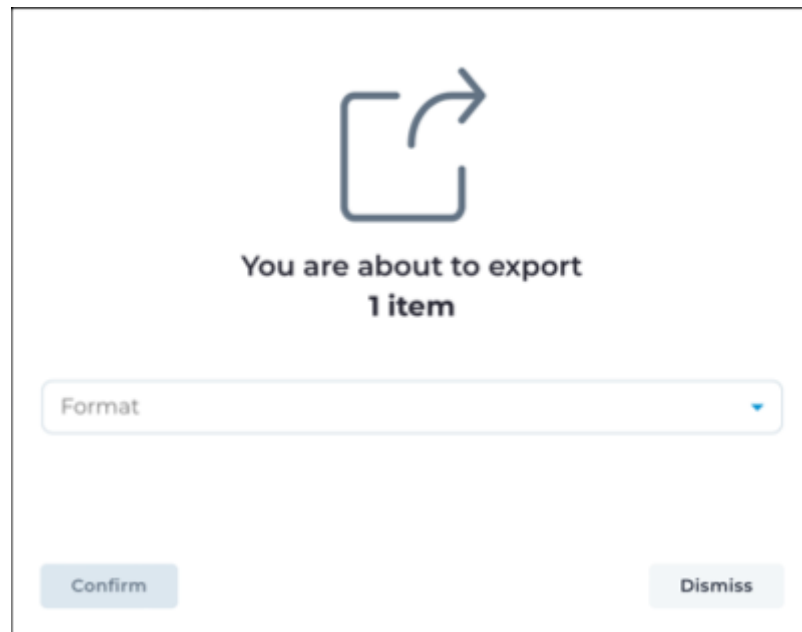
You can use the actions menu to export one or more vulnerabilities to a spreadsheet.

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**.

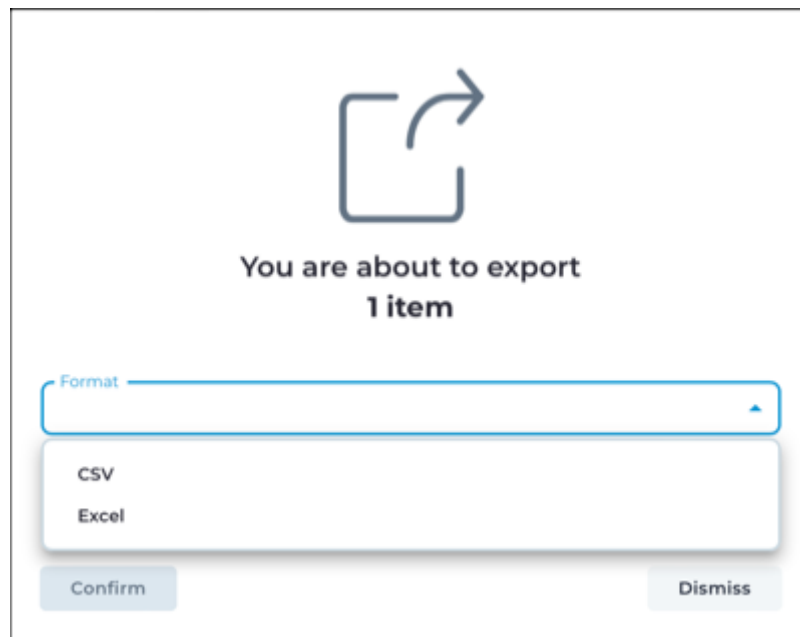


Result: The export dialog shows.

5. Select the **Format** dropdown.

Result: A dialog shows.

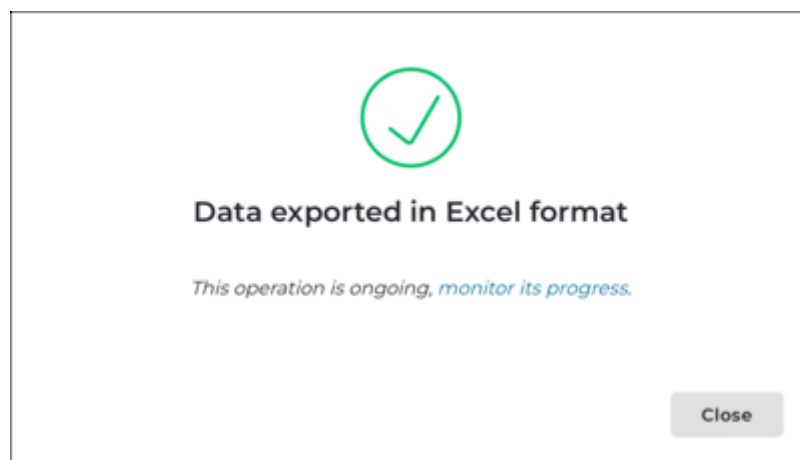
6. In the **Format** dropdown, select the format that you want to export.



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.

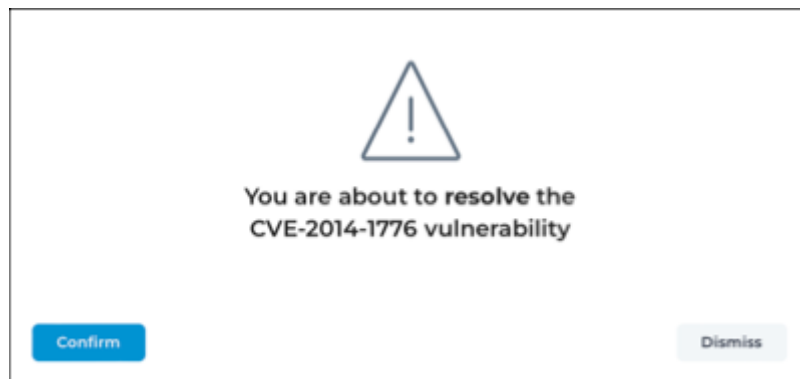
Choose from:

- 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**.

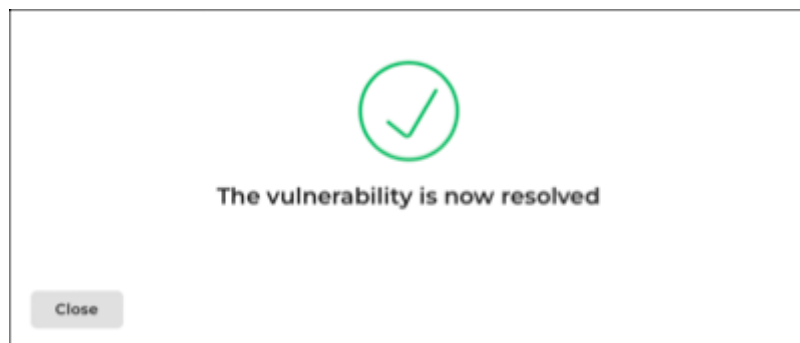
Result: A dialog shows.

5. Select **Confirm**.



Result: A dialog shows.

6. Select **Close**.



Results

The vulnerability has been resolved.



Chapter 8. Vantage IQ



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.

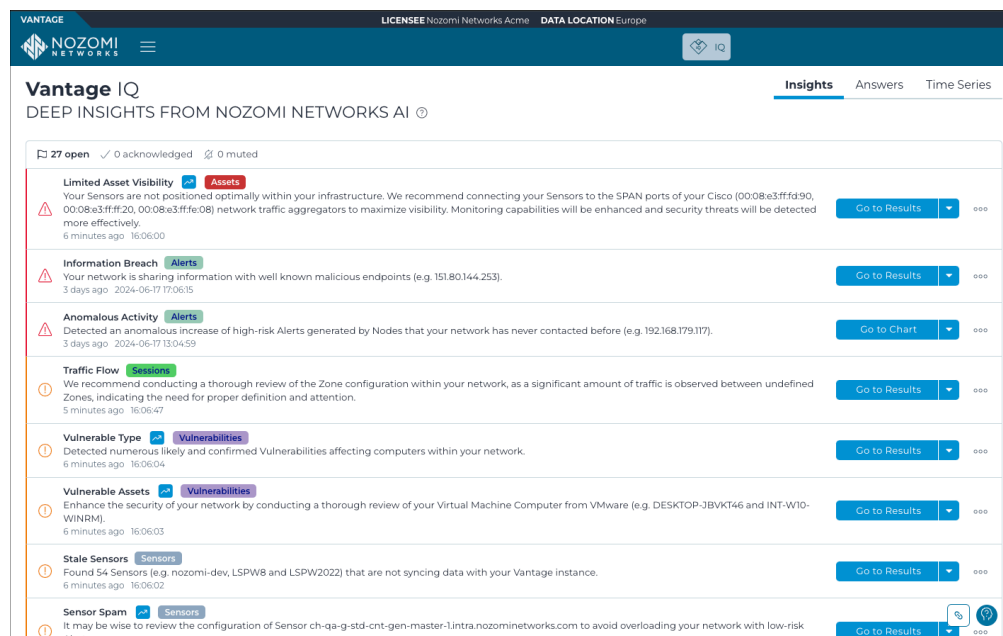


Figure 43. Vantage IQ page

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 click an individual insight, it will show the related details.

Insights

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.

For more details, see [Insights \(on page 143\)](#).

Answers

You can use powerful customizable queries to answer common questions and gain a deeper understanding of their environment. The preparation of semi-supervised, custom queries can aid users to identify anomalies more effectively.

For more details, see [Answers \(on page 147\)](#).

Time Series

With Time Series, you can predict and alert on abnormal bandwidth from any sensor's baseline network activity using advanced machine learning techniques. Was the change expected or outside of the normal range of deviation for that period? Forecasting is done via deep neural networks. It is possible to find existing trends and predict forecast reliability using online signal analysis.

For more details, see [Time Series \(on page 147\)](#).

Insights

The **Insights** page shows all the insights that Vantage IQ has collected throughout the day. The dashboard shows insights which relate to items within the environment that need to be addressed. The severity and the last trigger time of the insights are used to sort them.

Status bar

This bar shows:

- The number of **open** insights
- The number of **acknowledged** insights
- The number of **muted** insights

Insight types

Critical

You should investigate this type of insight as soon as possible. The majority of critical insights relate to security issues.




Warning

This type of insight has security and operational concerns. The majority of warning insights are alerting improvements.

Informational

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  critical insights will show first, older critical insights will be next
- The most recent  warning insights show next, older warning insights will be next
- The most recent  informational insights will show next, older informational insights will be next

Title

You can select the title of the insight to show a more detailed description of the insight. From this view, you can explore the insight further.

Go to Results

You can select this button to show a filtered tables page that highlights the data that created the insight.

Go to Chart

Vantage IQ will generate a chart to illustrate the insight. To modify and explore the insight further, you can modify the chart query from the queries page.

Go to Query

You can select this button to show the query page. The query for the insight is populated with the specific query for the insight. To explore the data further, you can modify the query.

Acknowledge

When you acknowledge an insight:

- The acknowledged insights will be hidden from the main **Insights** page.



Note:

You can select **acknowledged** in the [status bar \(on page 143\)](#) to view acknowledged insights.

- You can unacknowledge an insight to show it again
- The insight will be acknowledged for five days



Note:

After five days, if the insight is still triggered, it will show as reactivated on the main insights page.

- Insights generated by alerts will also be acknowledged if they are associated with the insight



Note:

If the insight is unacknowledged all the associated alerts will also be unacknowledged.

Mute

When you mute an insight:

- The insight will be hidden from the main **Insights** page



Note:

You can select **muted** in the [status bar \(on page 143\)](#) to view muted insights.

- You can unmute an insight to show it again



Note:

When insights with associated alerts are muted, a pop-up window shows that lets you generate mute rules that can be pushed down to sensors.

For more details on mute rules, see the **Alert Rules** section of the **Administrator Manual**.

Cycle time

Insights are only visible for five days, so when a new insight is triggered, it will remain on the **Insights** page for five days. If the insight is triggered again, the five day counter will start again.

Acknowledge an insight

The actions menu lets you acknowledge an insight.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.
3. Choose a method to open the actions menu.

Choose from:

- At the right end of the row, select the **⋮** icon
 - In the table, select the applicable insight to open the details page, to the right end of the row select the **⋮** icon
4. Select **Acknowledge**.

Results

The insight(s) has (have) been acknowledged.

Unacknowledge an insight

The actions menu lets you unacknowledge an insight.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.
3. In the top left, select **acknowledged**.

Result: A list of all the acknowledged insights shows.

4. Choose a method to open the actions menu.

Choose from:

- At the right end of the row, select the **⋮** icon
 - In the table, select the applicable insight to open the details page, to the right end of the row select the **⋮** icon
5. Select **Unacknowledge**.

Results

The insight(s) has (have) been unacknowledged.

Mute an insight

The actions menu lets you mute an insight.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.
3. Choose a method to open the actions menu.

Choose from:

- At the right end of the row, select the **⋮** icon
 - In the table, select the applicable insight to open the details page, to the right end of the row select the **⋮** icon
4. Select **Mute**.

Results

The insight(s) has (have) been muted.

Unmute an insight

The actions menu lets you unmute an insight.

Procedure

1. In the top navigation bar, select **IQ**.
2. Select **Insights**.
3. In the top left, select **muted**.

Result: A list of all the muted insights shows.

4. Choose a method to open the actions menu.

Choose from:

- At the right end of the row, select the **⋮** icon
 - In the table, select the applicable insight to open the details page, to the right end of the row select the **⋮** icon
5. Select **Unmute**.

Results

The insight(s) has (have) been unmuted.

Answers

The **Answers** page lets you use pre-configured queries that use artificial intelligence (AI) to quickly explore your environment. You can select a question you would like to explore and you will be redirected to the next page with the answer to your question.

Sections

The **Answers** pages is divided into these sections:

- Sensors
- Alerts
- Assets
- Vulnerabilities
- Links

Each section shows the related answers. You can select an answer to see more details. When you select an answer, the data is processed and after a few seconds, the data will show.

See and edit the Query behind

You can select this button to modify and explore the environment further. To learn more about the related environment, you can start a new query. When you select this button, the [Queries \(on page 113\)](#) page opens.

Time Series

Each sensor must be enabled for time series.

Once you select the Actions button on the Sensors Details page, followed by Enable IQ Analysis, Vantage IQ will begin to baseline the network traffic.

Queries

With Vantage IQ, you can create charts, graphs, and AI calculations.

You can use these queries:

- [Cluster \(on page 149\)](#)
- [Compare \(on page 151\)](#)
- [Correlation \(on page 152\)](#)
- [Describe \(on page 153\)](#)
- [Forecast \(on page 154\)](#)
- [Pivot \(on page 155\)](#)
- [Popular \(on page 156\)](#)
- [Simplify \(on page 157\)](#)
- [Timeline \(on page 158\)](#)
- [Versus \(on page 159\)](#)
- [Visualize \(on page 160\)](#)

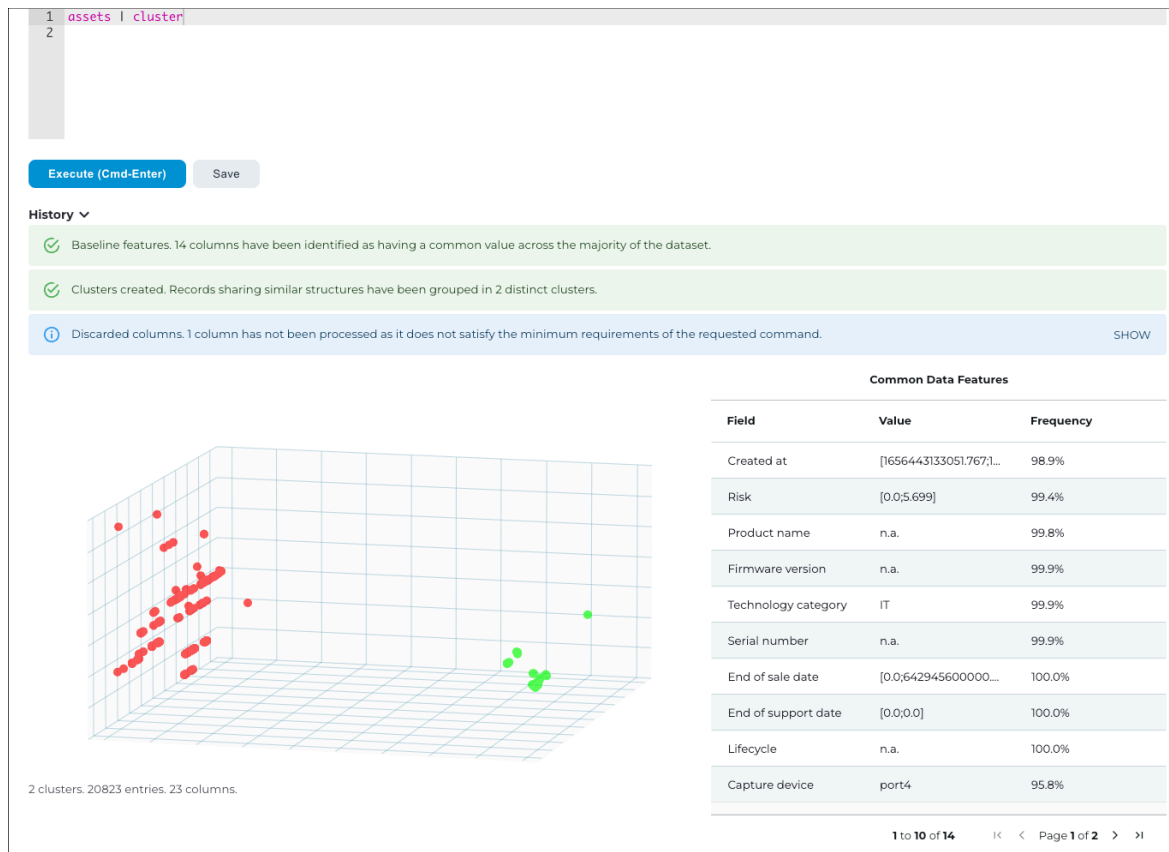
Cluster

Vantage IQ query example: *Cluster*.

Usage: <field> | cluster <number>

Description: Group different rows in several clusters based on automatically recognized patterns within the data.

Example: `assets | cluster`



Example: `assets | cluster 3`

1 assets | cluster 3

2

Execute (Cmd-Enter)

Save

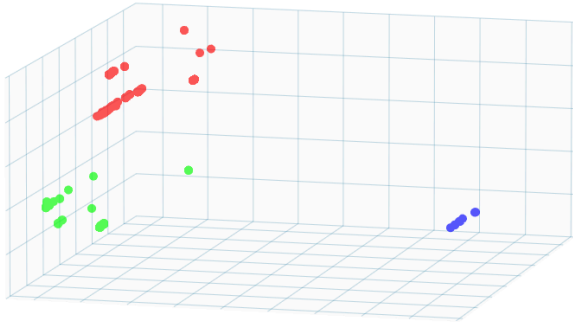
History

✓ Baseline features. 14 columns have been identified as having a common value across the majority of the dataset.

✓ Clusters created. Records sharing similar structures have been grouped in 3 distinct clusters.

ⓘ Discarded columns. 1 column has not been processed as it does not satisfy the minimum requirements of the requested command.

SHOW



3 clusters. 20823 entries. 23 columns.

Common Data Features

Field	Value	Frequency
Created at	[1656443133051,767;1...	98.9%
Risk	[0.0;5.699]	99.4%
Product name	n.a.	99.8%
Firmware version	n.a.	99.9%
Technology category	IT	99.9%
Serial number	n.a.	99.9%
End of sale date	[0.0;642945600000...	100.0%
End of support date	[0.0;0.0]	100.0%
Lifecycle	n.a.	100.0%
Capture device	port4	95.8%

1 to 10 of 14 < > Page 1 of 2 > >>

Vantage IQ query example: Compare.

Description: Compute nonlinear value relationships between two categorical, interval, and ordinal columns.

1

alerts | compare risk protocol

Execute [Cmd-Enter]

Save

Save Assertion

Export

History

✓

Comparison executed. The strength of the relationship between values of column 'Risk' and column 'Protocol' has been successfully computed. Hover on the matrix cells for more in-depth information.

id	field_one	field_two	outlier_significance
d4d5a205-a206-476e-939f-8fbae8302184	[5.0;6.25]	n.a.	0
f006fd67-f30-4561-8dba-7528cb9ecccc	[5.0;6.25]	arp	0.38
477373cd-dc1c-4c25-ad8c-e0e89cd41c2	[5.0;6.25]	dns	0
77d6ef40-a029-45d6-8d25-3247b79349edc	[5.0;6.25]	ftp	0.33
54d767c4-7f40-4b9a-86c6-251cc5488dd1	[5.0;6.25]	goose	0
05eb5db2-b7b9-406c-9e8f-69f6618186d2	[5.0;6.25]	https	0.15
d3d27f99-d3b0-4031-a37a-35cb3a6b85524	[5.0;6.25]	icmp	0

1 assets | compare os name

Execute (Cmd+Enter) Save Save Assertion Export

History ▾

✔ Comparison executed. The strength of the relationship between values of column 'Os' and column 'Name' has been successfully computed. Hover on the matrix cells for more in-depth information.

id	field_one	field_two	outlier_significance
9413a0b9-d8ab-426d-a794-c1e59eb2eebc	n.a.	0004231e0e041c@172.16.0.0	0
450a28e0-5dc3-4eae-8945-ed19242a6d60	n.a.	10.0.42.221	0.06
e9f898bb-a5ef-4f3a-8fa6-097b2fd4d71b	n.a.	10.10.0.1	0.06
8d5398d7-7e8e-40f4-a35f-927090128056	n.a.	10.10.0.3	0.06

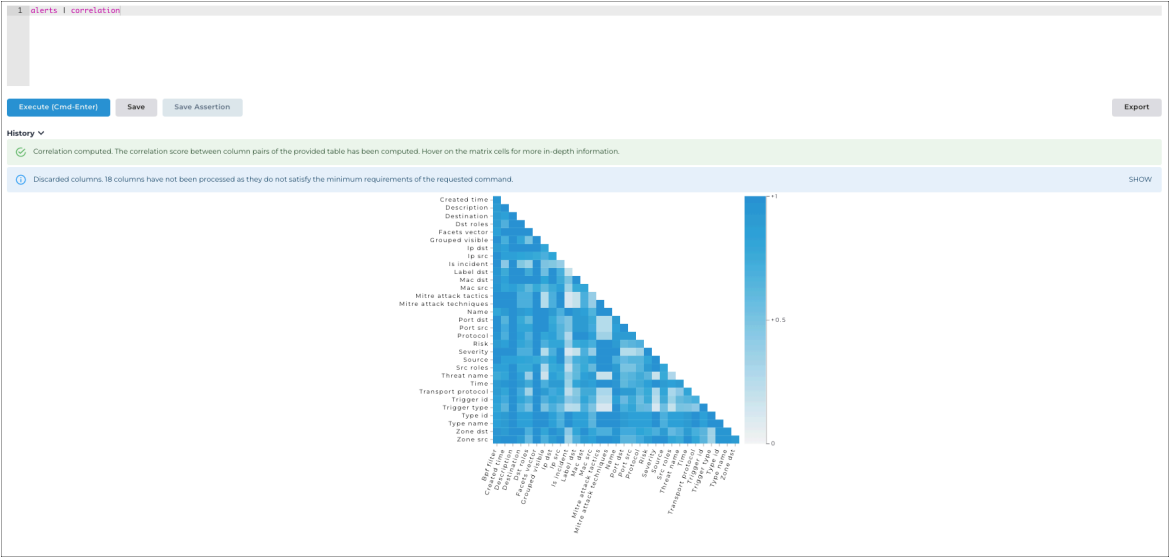
Correlation

Vantage IQ query example: Correlation.

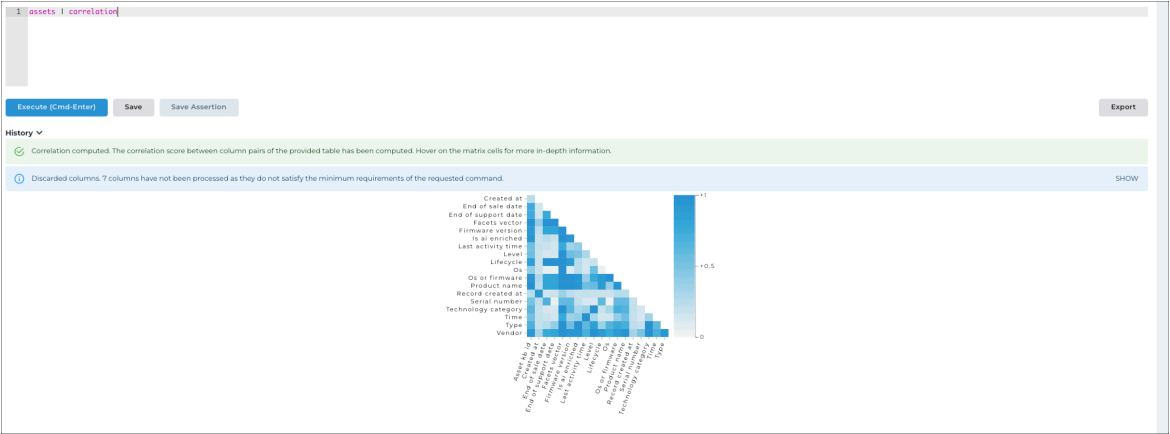
Usage: <field> | correlation

Description: Compute nonlinear correlations between categorical, interval, and ordinal columns.

Example: alerts | correlation



Example: assets | correlation



Describe

Vantage IQ query example: *Describe*.

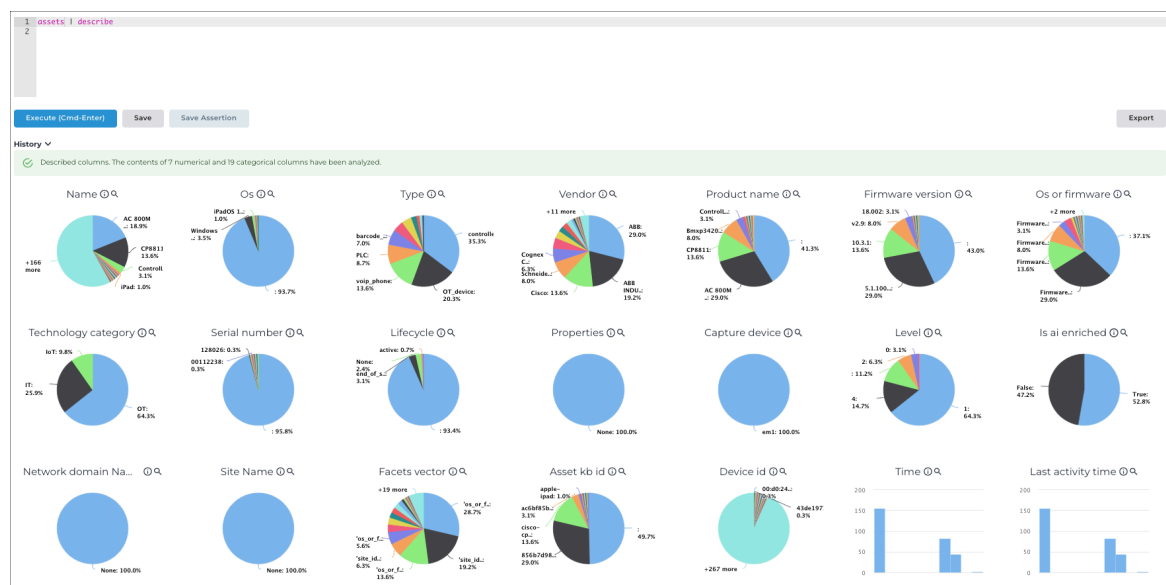
Usage: <field> | describe

Description: Compute several descriptive statistics of the passed content.

Example: `alerts | describe`



Example: `assets | describe`



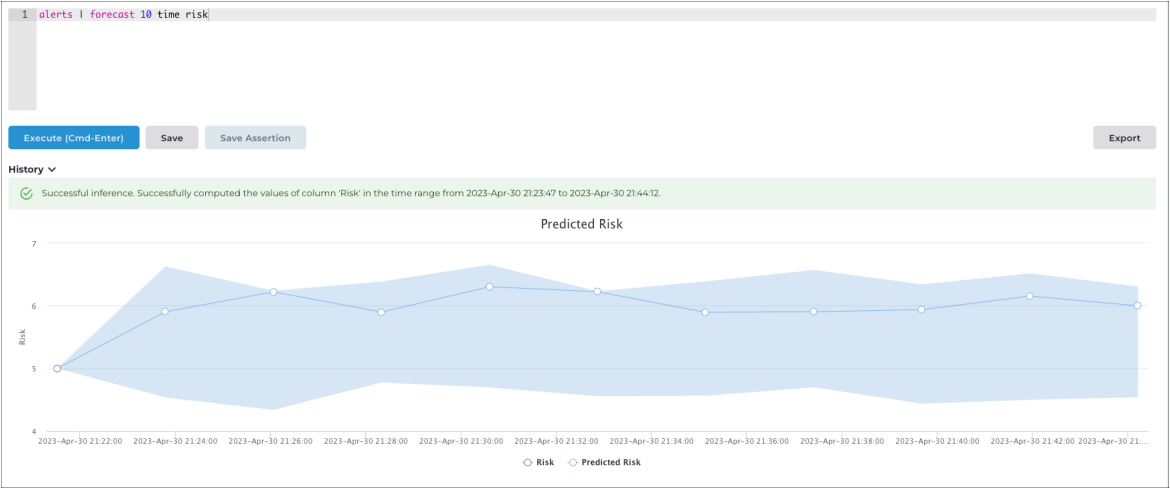
Forecast

Vantage IQ query example: Forecast.

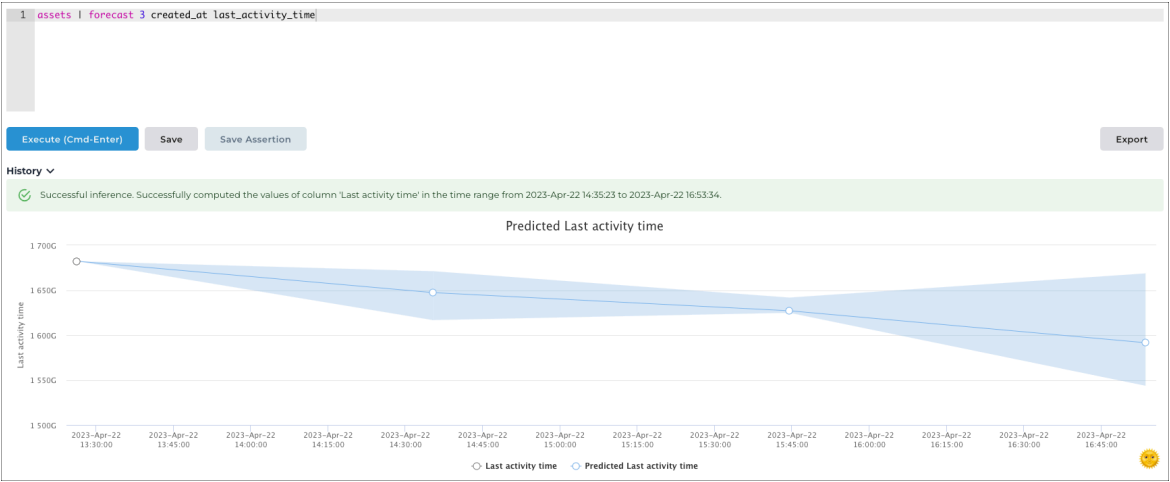
Usage: <field> | forecast <number> <field1> <field2> <field3>

Description: Forecast the values of a numeric time series.

Example: alerts | forecast 10 time risk



Example: assets | forecast 3 created_at last_activity_time



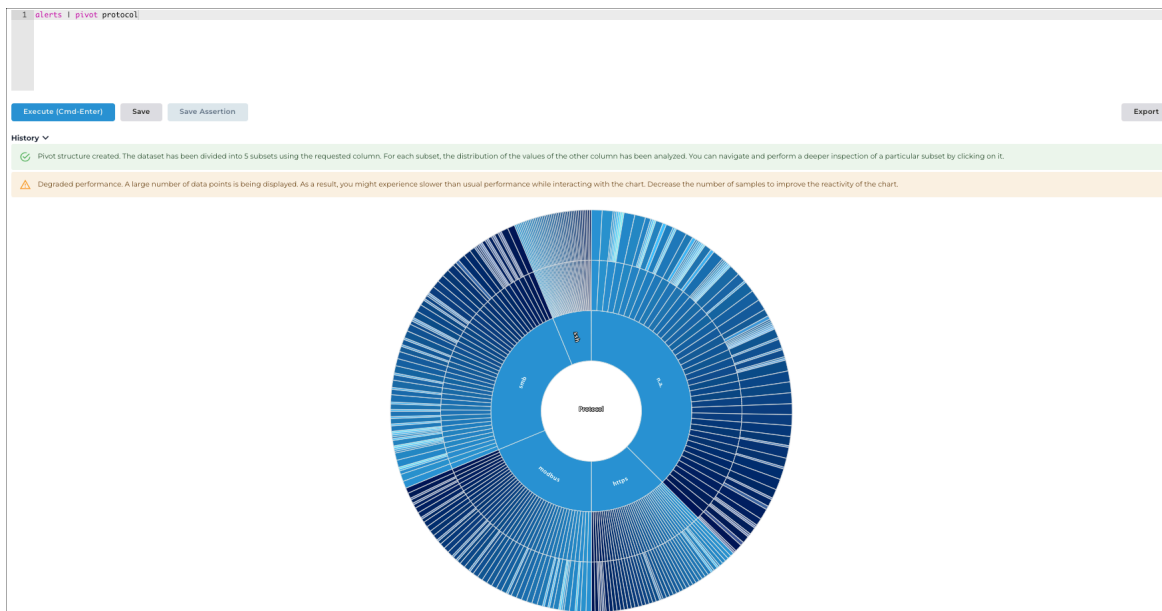
Pivot

Vantage IQ query example: *Pivot*.

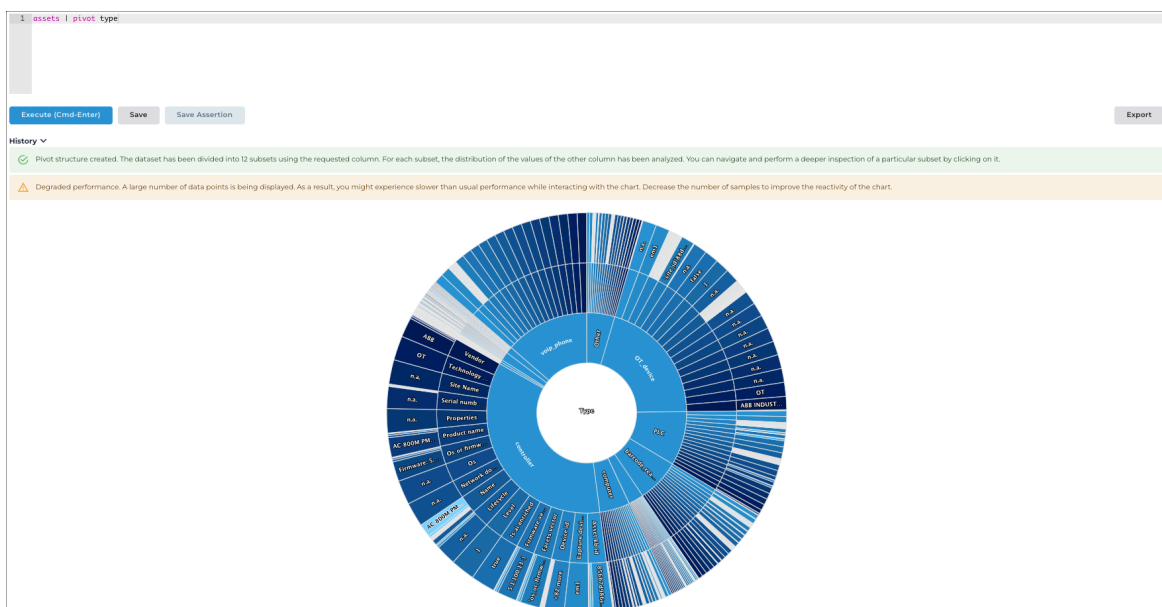
Usage: `<field> | pivot <field>`

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`



Example: `assets | pivot type`



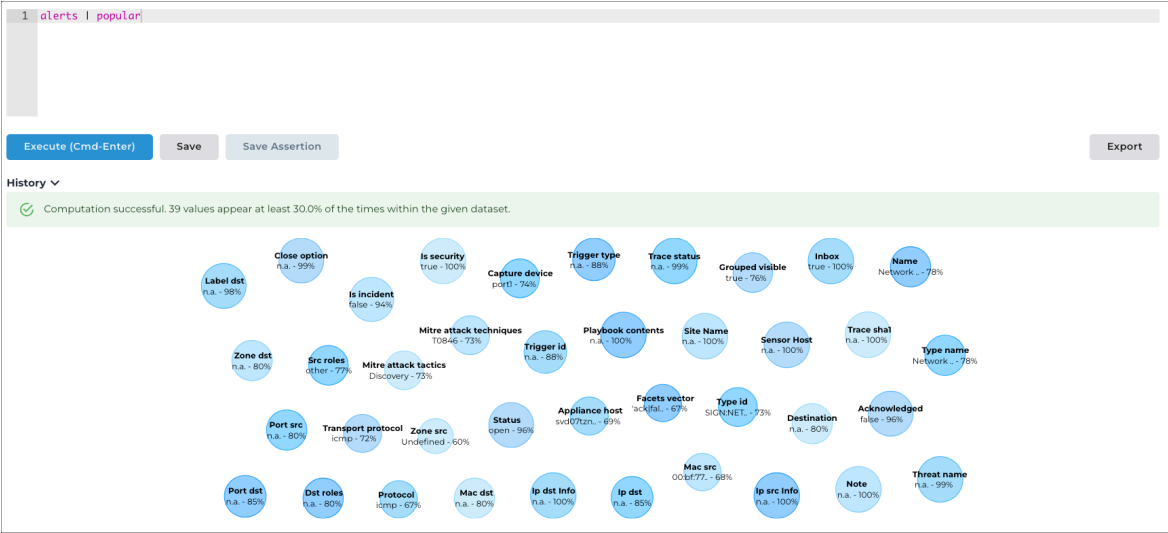
Popular

Vantage IQ query example: Popular.

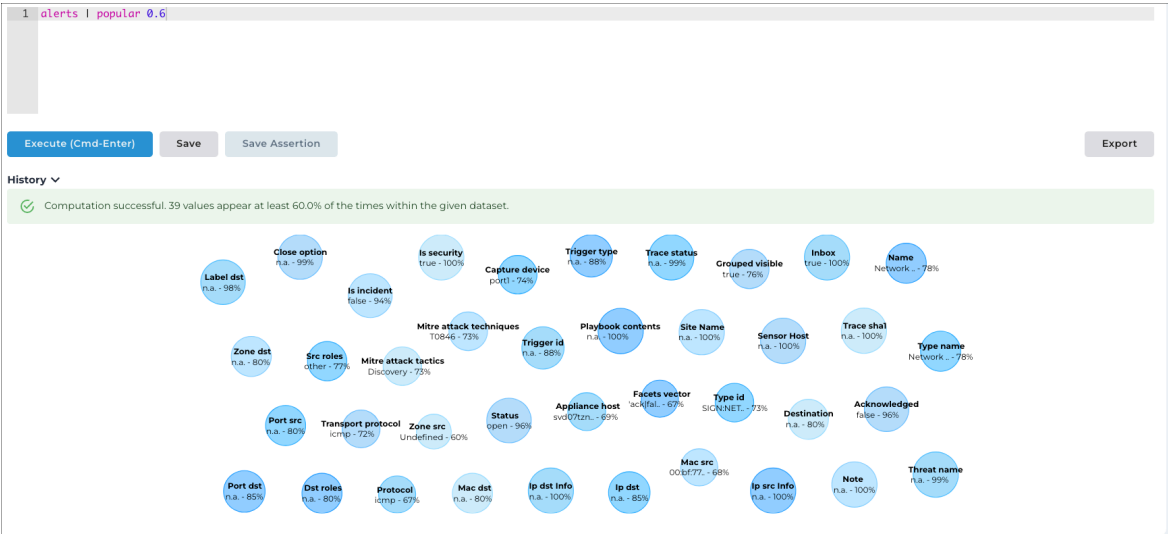
Usage: <field> | popular <field>

Description: Find the most popular values in a table and visualize them.

Example: alerts | popular



Example: alerts | popular 0.6



Vantage IQ query example: Simplify.

Description: Identify the rows and columns carrying the highest information level.

1 alerts | simplify

Execute (Cmd-Enter)

Save

Save Assertion

Tip: add time filter for better performance

Export

History

✓

Successful percent row reduction. The 27 most uncommon and the 27 most common rows have been identified. They correspond to 5.0% and 5.0% of the whole dataset respectively.

✓

Successful absolute column reduction. 29 low information columns have been identified.

ⓘ

Discarded columns. 11 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

SHOW

Rarity	Uniqueness ↓	Destination	Ip dst	Counter	Mac dst	Port dst	Port src	Dst roles	Bpf filter
uncommon	0.99	172.16.0.253	172.16.0.253	n.a.	00:04:23:e0:04:1c	445	34543	consumer, terminal	(ip host 172.16.0.55 and ip host 172.16.0.25)
uncommon	0.99	172.16.0.156	172.16.0.156	n.a.	52:54:00:12:35:02	22	49739	producer	(ip host 172.16.0.253 and ip host 172.16.0.1)
uncommon	0.98	172.16.0.156	172.16.0.156	n.a.	00:60:78:00:6a:10	502	1196	producer	(ip host 172.16.0.253 and ip host 172.16.0.1)
uncommon	0.98	172.16.0.156	172.16.0.156	n.a.	00:60:78:00:6a:10	502	1196	producer	(ip host 172.16.0.253 and ip host 172.16.0.1)
uncommon	0.97	192.168.0.21	192.168.0.21	n.a.	00:a0:45:be:4a:69	21	33881	producer, web_server, dns_server	(ip host 192.168.0.109 and ip host 192.168.0.1)
uncommon	0.97	192.168.0.21	192.168.0.21	n.a.	00:a0:45:be:4a:69	21	33827	producer, web_server, dns_server	(ip host 192.168.0.109 and ip host 192.168.0.1)
uncommon	0.97	192.168.0.21	192.168.0.21	n.a.	00:a0:45:be:4a:69	21	33881	producer, web_server, dns_server	(ip host 192.168.0.109 and ip host 192.168.0.1)
uncommon	0.97	192.168.0.33	192.168.0.33	n.a.	00:a0:45:37:52:c	21	56376	dns_server	(ip host 192.168.0.109 and ip host 192.168.0.1)
uncommon	0.97	192.168.0.21	192.168.0.21	n.a.	00:a0:45:be:4a:69	21	33832	producer, web_server, dns_server	(ip host 192.168.0.109 and ip host 192.168.0.1)

1

assets | simplify rows 10

Execute (Cmd-Enter)

Save

Save Assertion

Export

History

Successful absolute row reduction. The 5 most uncommon and the 5 most common rows have been identified.

Discarded columns. 3 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

SHOW

Rarity	Uniqueness ↓	Os	Name	Time	Type	Level	Vendor	Device id
uncommon	0.81	n.a.	ControlLogix 1756-ENB...	1682522387856	IO_module	1	Rockwell Automation/...	00112238
uncommon	0.81	n.a.	ControlLogix 1756-ENB...	1682522387843	IO_module	1	Rockwell Automation/...	00112233
uncommon	0.81	n.a.	ControlLogix 1756-ENB...	1682522387863	IO_module	1	Rockwell Automation/...	00112237
uncommon	0.81	n.a.	ControlLogix 1756-ENB...	1682522387865	IO_module	1	Rockwell Automation/...	00112239
uncommon	0.81	n.a.	ControlLogix 1756-ENB...	1682522387865	IO_module	1	Rockwell Automation/...	00112232
common	0.49	n.a.	142.33.163.222	1689165923000	Other	n.a.	n.a.	n.a.
common	0.49	n.a.	142.33.71.237	1689165923000	Other	n.a.	n.a.	n.a.
common	0.49	n.a.	142.33.242.100	1689165923000	Other	n.a.	n.a.	n.a.
common	0.49	n.a.	142.33.132.238	1689165923000	Other	n.a.	n.a.	n.a.
common	0.49	n.a.	142.33.29.100	1689165923000	Other	n.a.	n.a.	n.a.

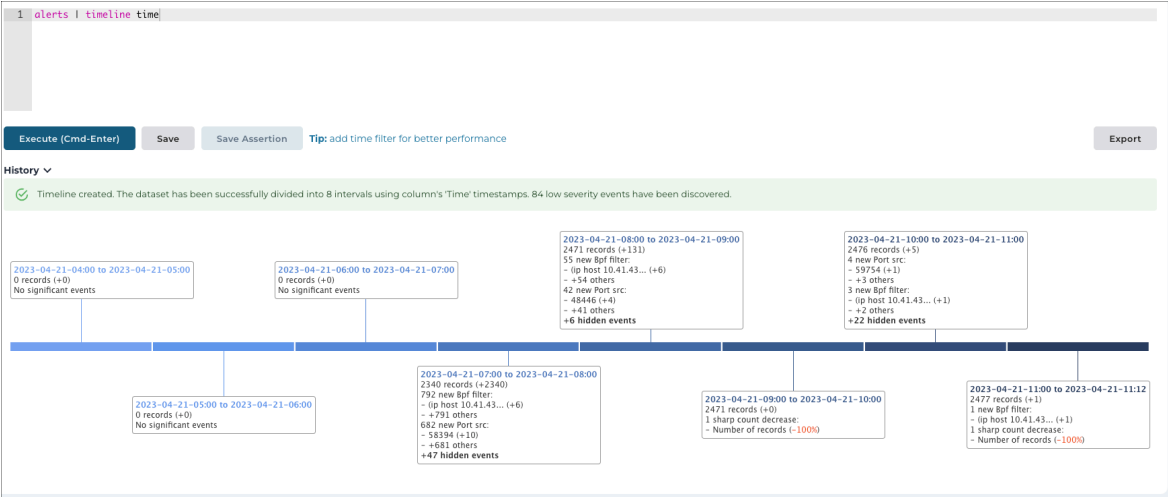
Timeline

Vantage IQ query example: Timeline.

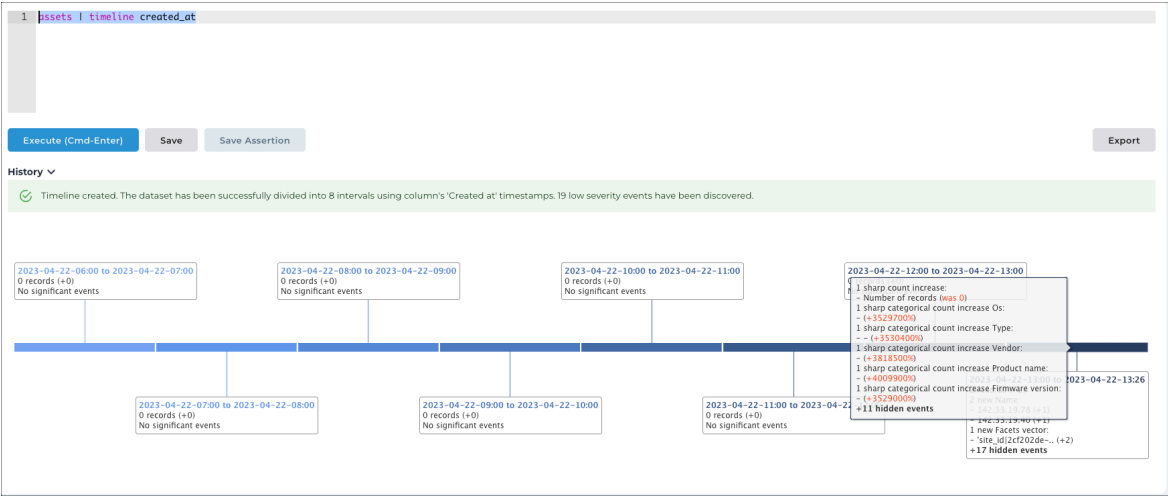
Usage: <field> | timeline <field>

Description: Displays the most significant events for the given dataset as time moves forward.

Example: alerts | timeline time



Example: assets | timeline created_at



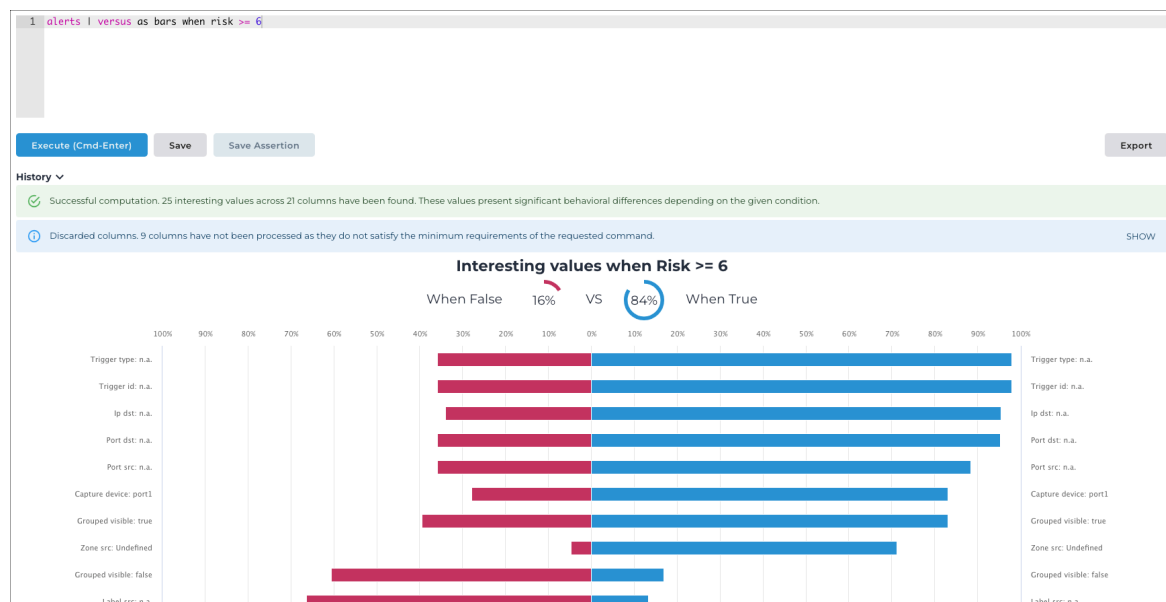
Versus

Vantage IQ query example: Versus.

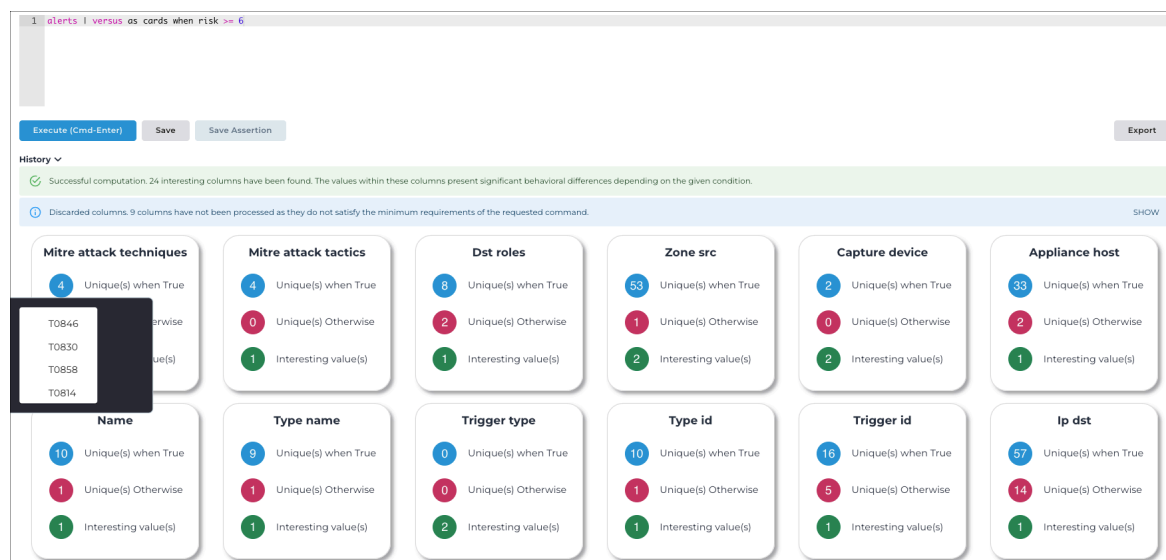
Usage: <field> | versus as <format> <field>

Description: Given a boolean condition, it divides the dataset into two subsets and compares them in order to find column where the behavior has significant changes.

Example: alerts | versus as bars when risk >= 6



Example: alerts | versus as cards when risk >= 6



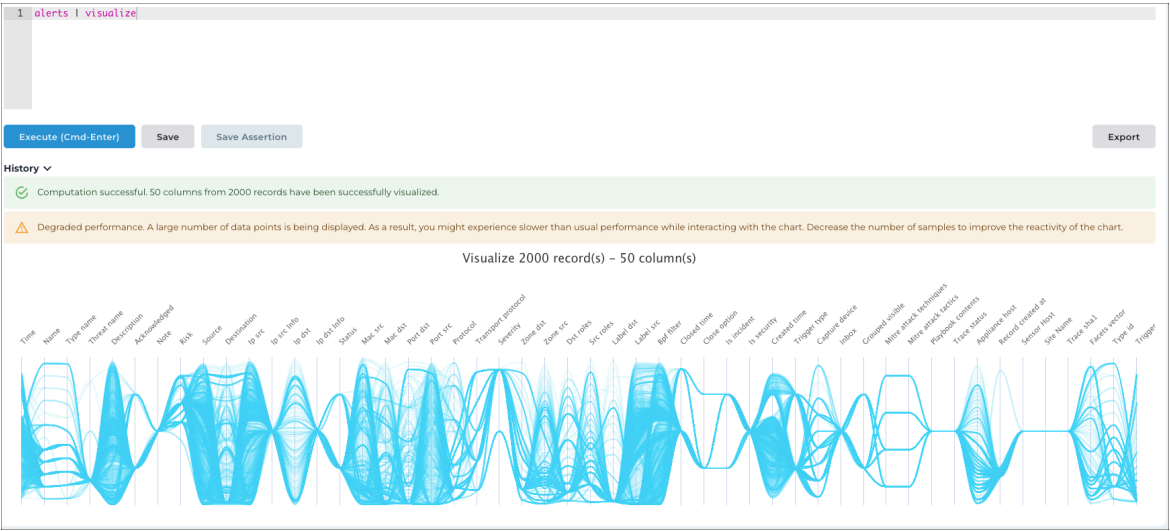
Visualize

Vantage IQ query example: Visualize.

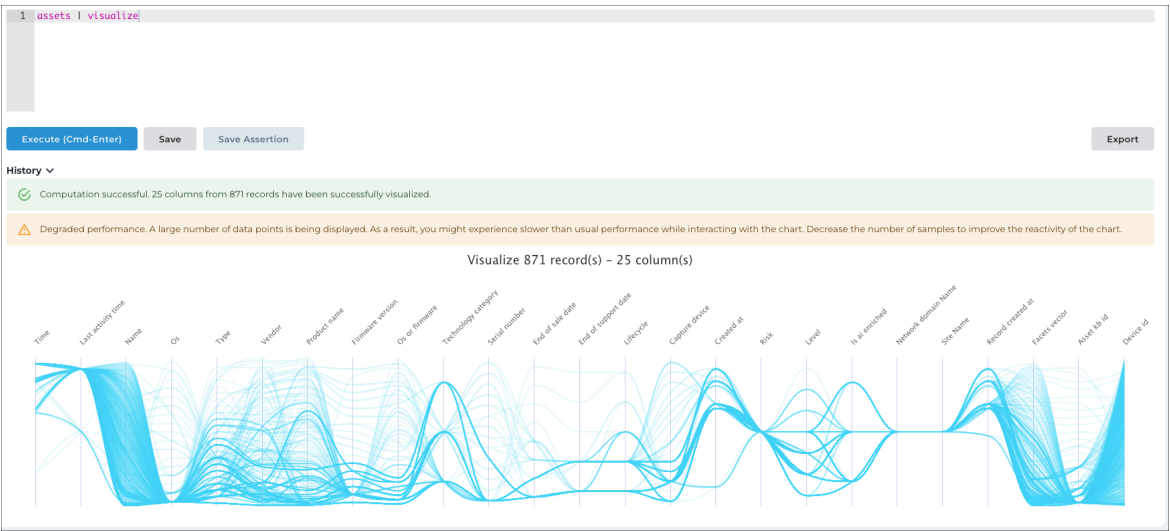
Usage: <field> | visualize

Description: Provides a graphical visualization of the given rows.

Example: alerts | visualize



Example: assets | visualize



Chapter 9. Network



Network

The **Network** page shows a visual representation of your network and all its assets.

VANTAGE LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Network Nodes Links Sessions

Site (2)

- ☐ Mendrisio (46505)
- ☐ Demo Site iq 9d83d655 (219)

Type (24)

- ☐ Other (20405)
- ☐ IT device (77402)
- ☐ Computer (6841)
- ☐ Mobile phone (370)

Expand

Columns Refresh Live

	Last activity time	Label	IP	Mac address	Protocols	Site Name	Network dc
0	10:34:54	n.a.	n.a.	00:09:0f:09:00:12		Mendrisio	Domain cr
0	10:34:51	n.a.	52.239.176.74	00:08:e3:ff:fe:08	https	Mendrisio	Domain /d
0	10:34:51	n.a.	172.30.9.37	00:08:e3:ff:fe:08		Mendrisio	Domain /d
0	10:34:51	n.a.	172.30.61.30	2c:5a:0f:b7:f5:21		Mendrisio	Domain /d
0	10:34:49	tracking-1611167402.us-ei	54.208.164.131	00:c8:8b:16:15:9e	https	Mendrisio	Domain /d
0	10:34:49	n.a.	10.41.43.1	00:09:0f:09:00:12	dns, melsoft, ntp	Mendrisio	Domain cr
0	10:34:49	n.a.	172.30.194.29	2c:ab:eb:e5:34:d1	other	Mendrisio	Domain /d
0	10:34:48	n.a.	172.18.66.27	84:3d:c6:c5:58:e1	http, other	Mendrisio	Domain /d
0	10:34:48	n.a.	172.18.108.27	70:d3:79:00:48:91		Mendrisio	Domain /d
0	10:34:48	n.a.	172.19.46.46	f0:f7:55:51:e9:41		Mendrisio	Domain /d

1 to 25 of more Page 1 of more

© 2013-2024 Nozomi Networks Version @ be444 Data for this instance is hosted by

Figure 44. Network page

General

The **Network** page has these tabs:

- [Nodes](#) (on page 164)
- [Links](#) (on page 165)
- [Sessions](#) (on page 166)

Nodes

The **Nodes** page shows a visual representation of your network and all its assets.

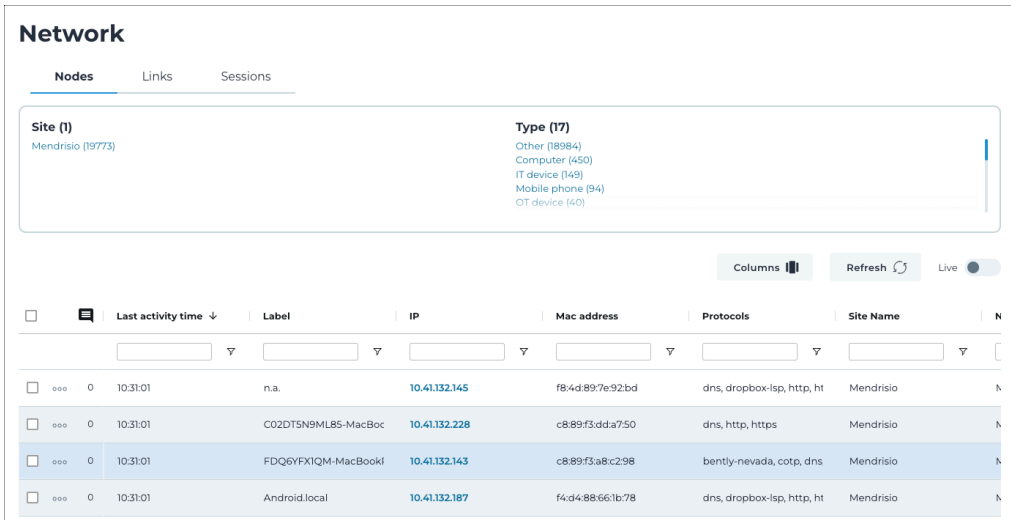


Figure 45. Nodes page

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.

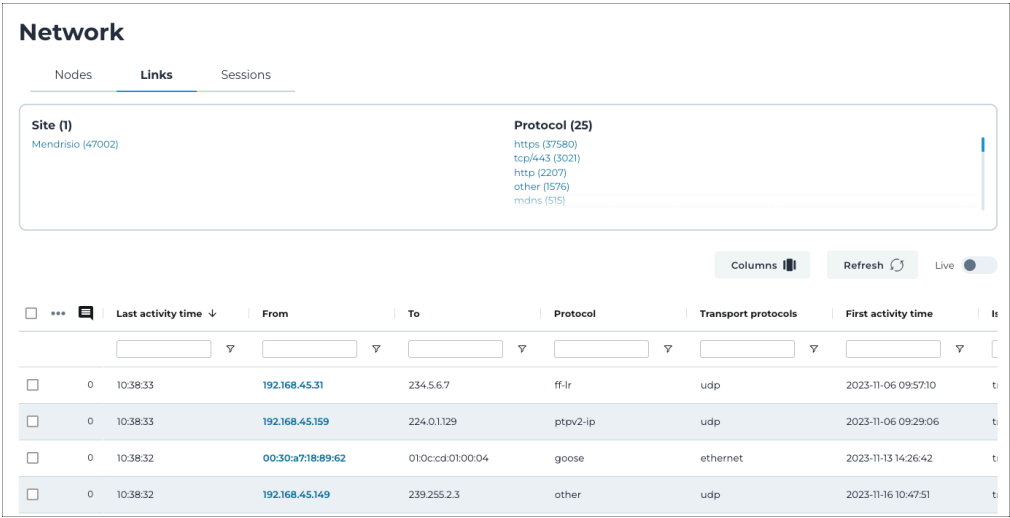


Figure 46. Links page

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.

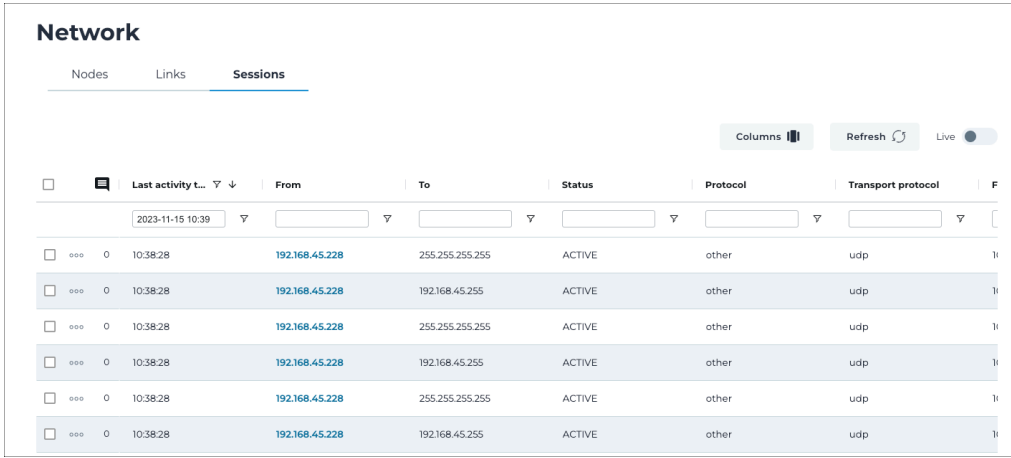


Figure 47. Sessions page


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



Graph

The **Graph** page shows a visual representation of your network and all its assets.

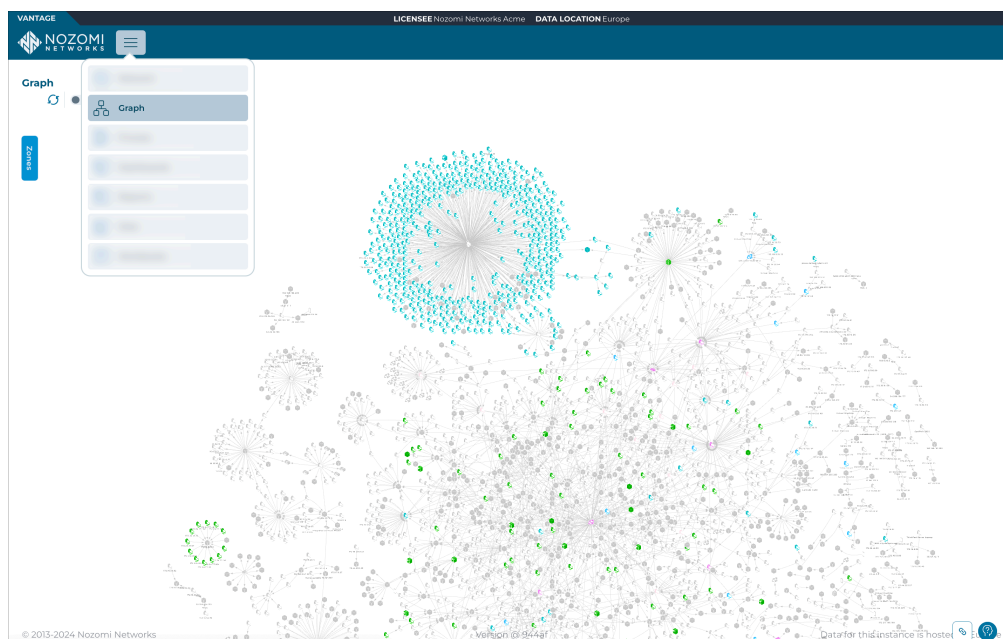


Figure 48. Graph page

Icons


The top left corner shows 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.

Play-pause

The play-pause  icon lets you pause, or restart the motion of the graph.

Settings

The settings  icon lets you configure the settings of the graph.

Settings

Layout

Standard

Group by

only links with confirmed data

show broadcast

display protocols

Close

Filter

The filter  icon lets you filter the elements in the graph.

Site

Sensor

Network domain

IP

Name

OS


Vendor

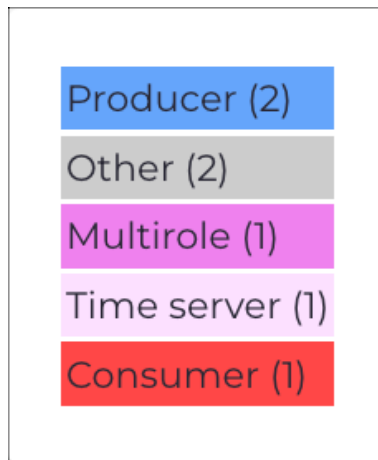
Firmware version

Product name

Level

Legend

The legend  icon lets you view the legend that shows the meaning of each color used in the graph. The legend only shows the roles related to nodes that are currently shown in the graph.



Zones

The **Zones** drawer shows your network in terms of the zones you have defined. Each zone and its links show in the drawer on the right.

Graph navigation

To use the graph, you can:

- Use your cursor zoom in and out; drag the graph to move it
- Select links (lines) and nodes (icons) to view the related details in the right drawer
- In the drawer, you can select **Details** to open the related Vantage page
- Select **Zones** to show your network in [zones \(on page 171\)](#). An overview will show in the drawer in the left



Chapter 11. Process



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.

Process	Host label	Namespace	Name	Label	Type
analog-value_6	n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
analog-value_6	n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
analog-value_6	n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
analog-value_6	n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
analog-value_6	n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
ioa-20-59473	n.a.	10025	ioa-20-59473	ioa-20-59473 at 10025	digital
ioa-1-4593	n.a.	10025	ioa-1-4593	ioa-1-4593 at 10025	digital
ioa-1-5058	n.a.	10025	ioa-1-5058	ioa-1-5058 at 10025	digital
ioa-10-22640	n.a.	10025	ioa-10-22640	ioa-10-22640 at 10025	digital
ioa-10-22644	n.a.	10025	ioa-10-22644	ioa-10-22644 at 10025	digital
ioa-10-18042	n.a.	10025	ioa-10-18042	ioa-10-18042 at 10025	analog
ioa-20-60280	n.a.	10025	ioa-20-60280	ioa-20-60280 at 10025	doublepoint
ioa-21-1747	n.a.	10025	ioa-21-1747	ioa-21-1747 at 10025	digital
ioa-13-19032	n.a.	10025	ioa-13-19032	ioa-13-19032 at 10025	digital
ioa-1-5300	n.a.	10025	ioa-1-5300	ioa-1-5300 at 10025	digital
ioa-21-1745	n.a.	10025	ioa-21-1745	ioa-21-1745 at 10025	digital
ioa-10-22643	n.a.	10025	ioa-10-22643	ioa-10-22643 at 10025	digital
ioa-11-49563	n.a.	10025	ioa-11-49563	ioa-11-49563 at 10025	digital
ioa-20-62681	n.a.	10025	ioa-20-62681	ioa-20-62681 at 10025	analog
ioa-17-56888	n.a.	10025	ioa-17-56888	ioa-17-56888 at 10025	digital
ioa-21-1748	n.a.	10025	ioa-21-1748	ioa-21-1748 at 10025	digital
ioa-1-4493	n.a.	10025	ioa-1-4493	ioa-1-4493 at 10025	digital

Figure 49. 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 \(on page 175\)](#) page opens.

2. Choose a method to open the actions menu.

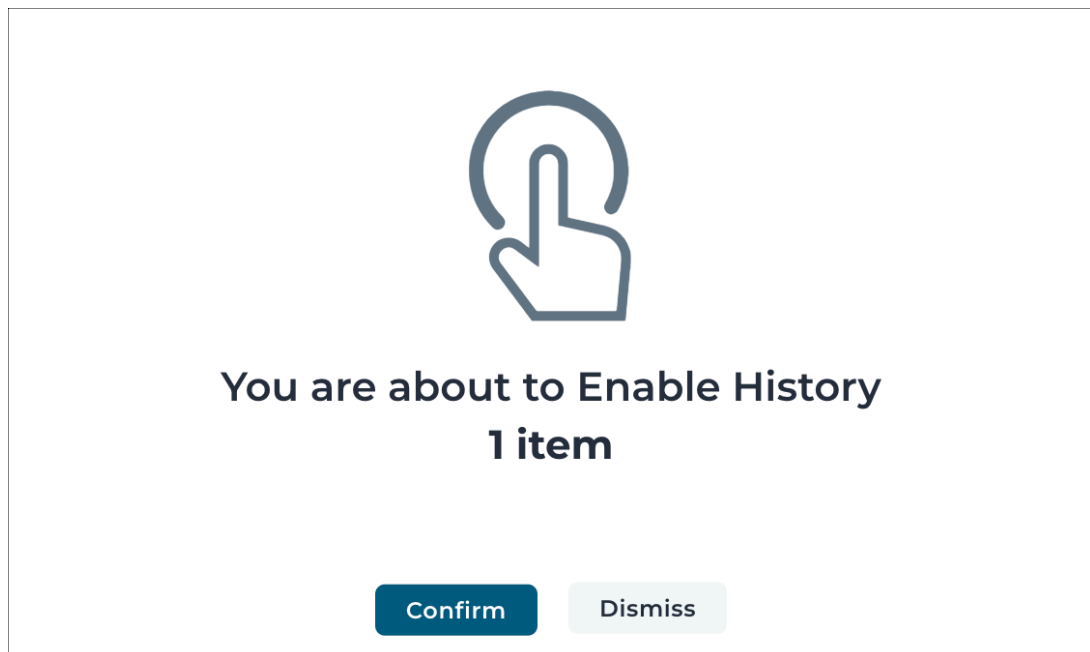
Choose from:

- 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



Dashboards

The **Dashboards** page shows a list of all the dashboards that have been created.

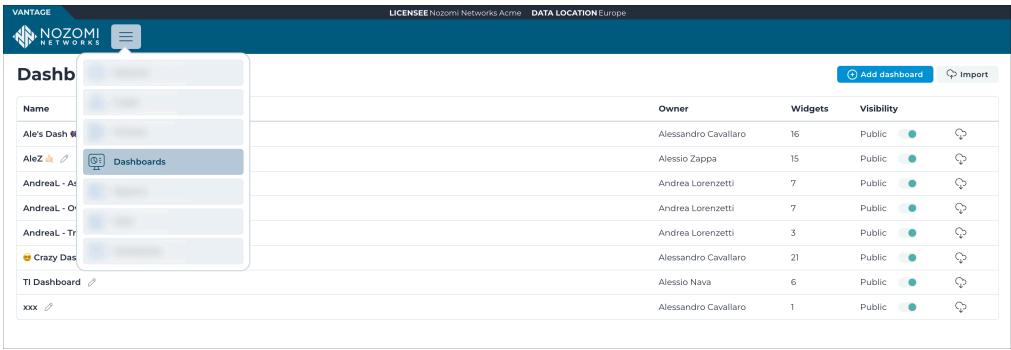


Figure 50. Dashboards page

Add dashboard

This button lets you [Create a dashboard \(on page 182\)](#).


Import

This button lets you [Import a dashboard \(on page 183\)](#).

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 \(on page 181\)](#) 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 \(on page 181\)](#) 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 \(on page 181\)](#) 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 \(on page 181\)](#) 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.



Chapter 13. Reports



Reports

The **Reports** page shows all the reports that the sensors in your system have created.

Time	Name	Sensor Host	Site Name
2024-04-10 12:57:16	vulns_andreal	ch-qa-cmc-std-vm-gen-master-1.intra.nozominetw	Mendrisio
2024-04-09 12:57:57	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-08 12:57:37	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-07 12:57:08	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-06 12:57:13	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-05 12:57:26	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-04 12:57:36	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-03 12:57:33	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-02 12:57:16	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-04-01 12:57:18	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-03-31 12:57:35	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-03-30 11:57:46	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-03-29 11:57:44	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio
2024-03-28 11:57:22	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetw	Mendrisio

Figure 51. Reports 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.

Table interactions

Actions menu

Delete a report

You can use the actions menu to delete reports.


Procedure

1. In the top navigation bar, select  > **Reports**.

Result: The [Reports \(on page 189\)](#) 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 **Delete**.

Results

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

Chapter 14. Sites



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.

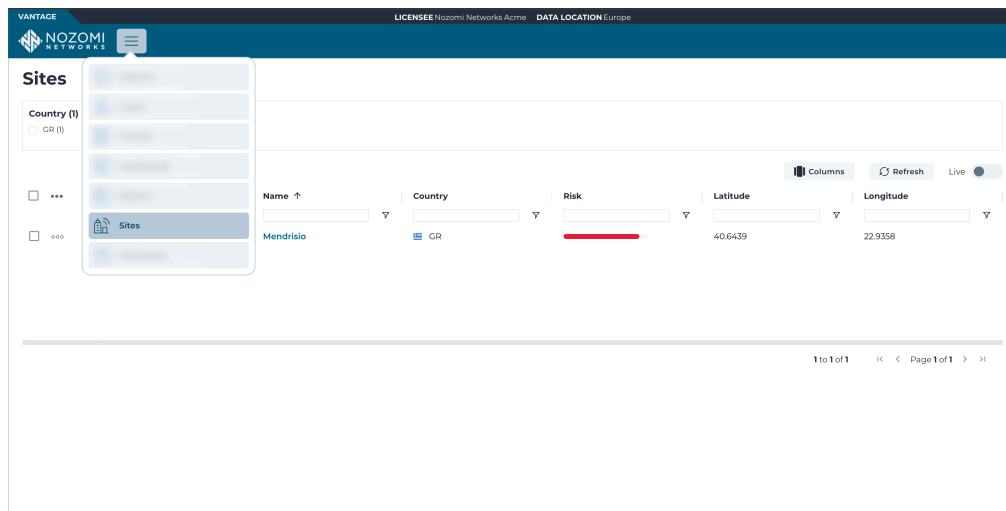


Figure 52. Sites page

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 \(on page 193\)](#) page opens.

2. Choose a method to open the actions menu.

Choose from:

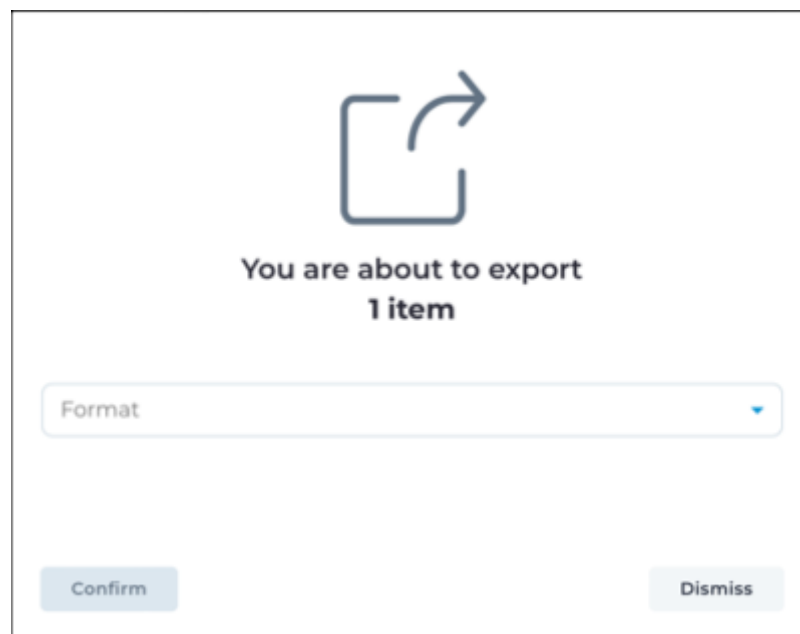
- In the table, select the hyperlink to open the details page. Select **Actions**
- In the table, select the  icon

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**.

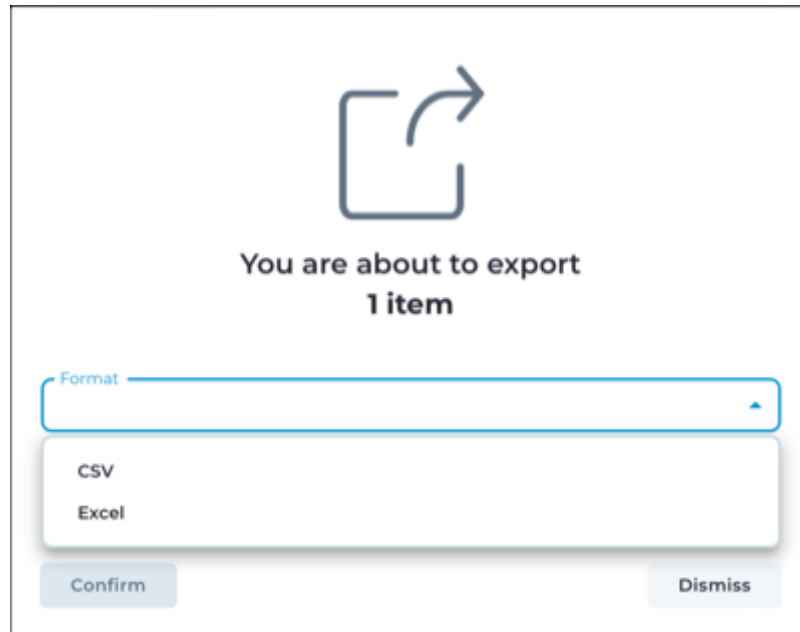


Result: The export dialog shows.

5. Select the **Format** dropdown.

Result: A dialog shows.

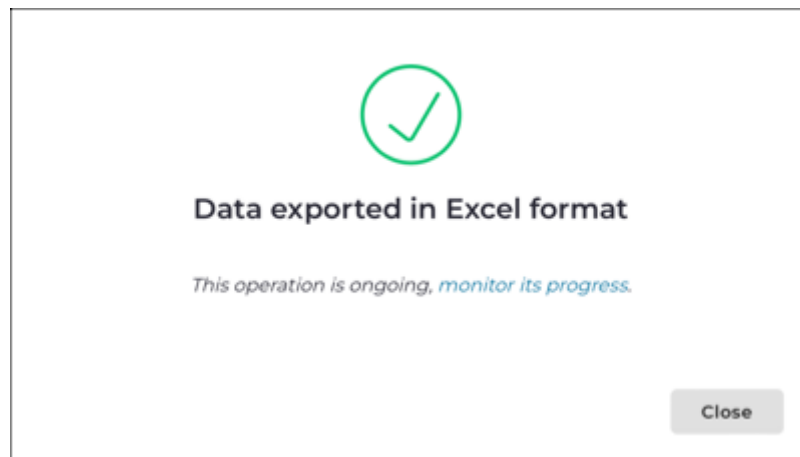
6. In the **Format** dropdown, select the format that you want to export.



7. Select **Confirm**.

Result: A confirmation dialog shows.

8. Select **Close**.



Results

The site(s) has (have) been exported.



Chapter 15. Workbooks



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.

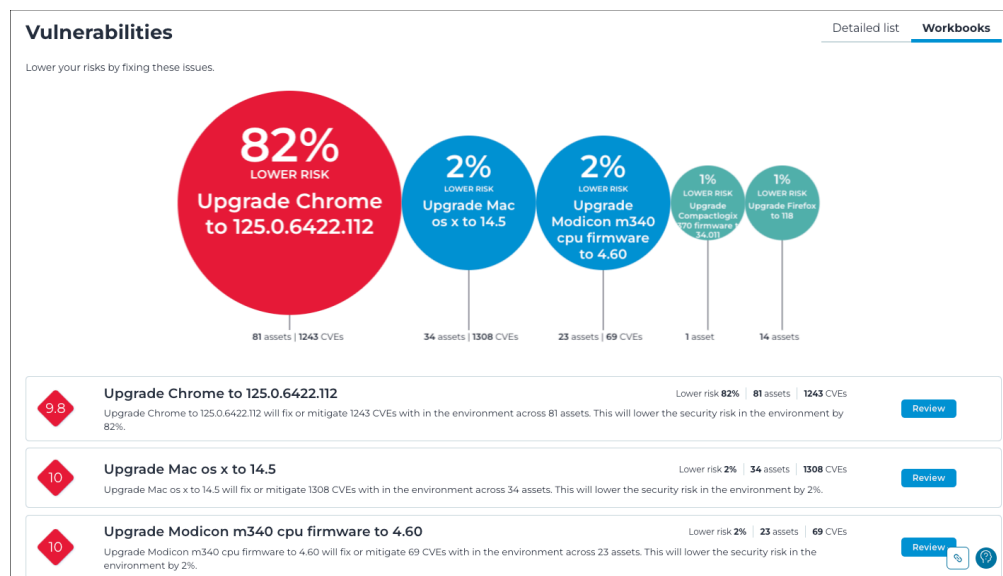


Figure 53. Workbooks page

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 200)

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 \(on page 130\)](#) 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 \(on page 136\)](#).



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

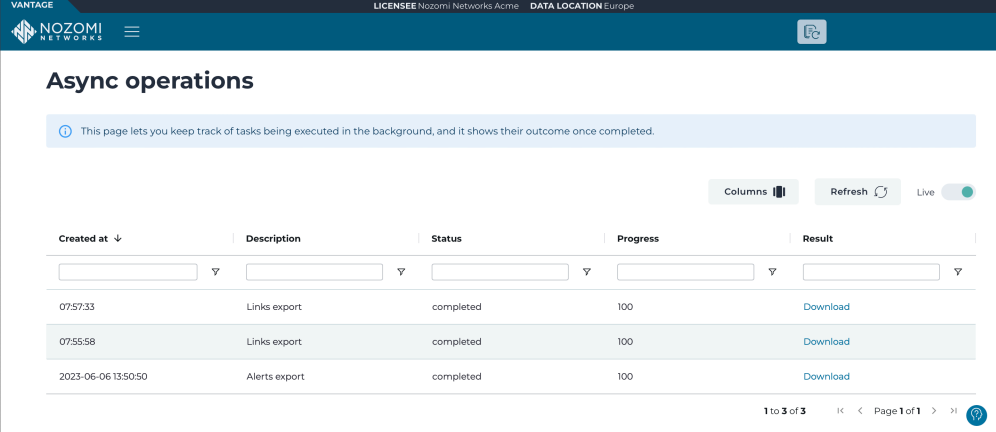
[Workbooks \(on page 130\)](#)

Chapter 16. Async operations



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 they are completed.



Async operations

This page lets you keep track of tasks being executed in the background, and it shows their outcome once completed.

Columns Refresh Live

Created at	Description	Status	Progress	Result
07:57:33	Links export	completed	100	Download
07:55:58	Links export	completed	100	Download
2023-06-06 13:50:50	Alerts export	completed	100	Download

1 to 3 of 3 Page 1 of 1

Figure 54. Async operations page



Chapter 17. What's new



What's new drawer

The **What's new** drawer shows a list of new features, enhancements, and fixes for issues.

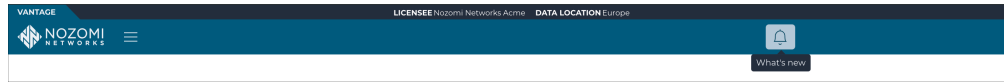


Figure 55. What's new icon

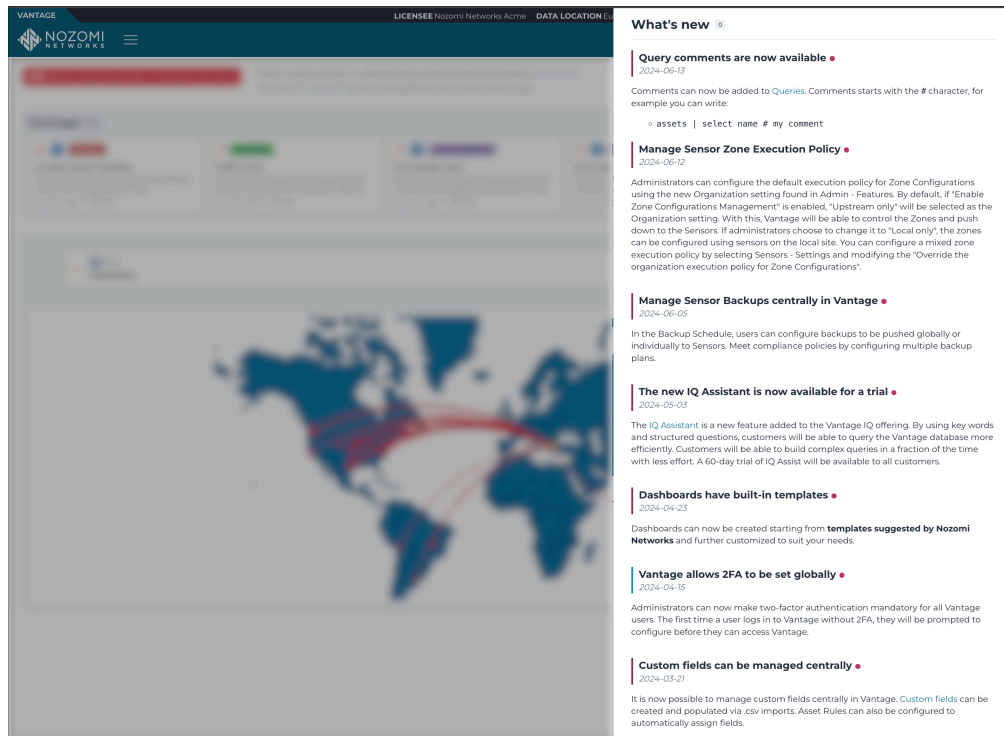


Figure 56. What's new drawer



Chapter 18. 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 Manual**.



Chapter 19. Profile settings



Profile settings

The profile settings menu lets you edit your user settings and update your profile.



Figure 57. Profile settings menu

The **Profile** page has these tabs:

- Authentication
- API keys

Authentication

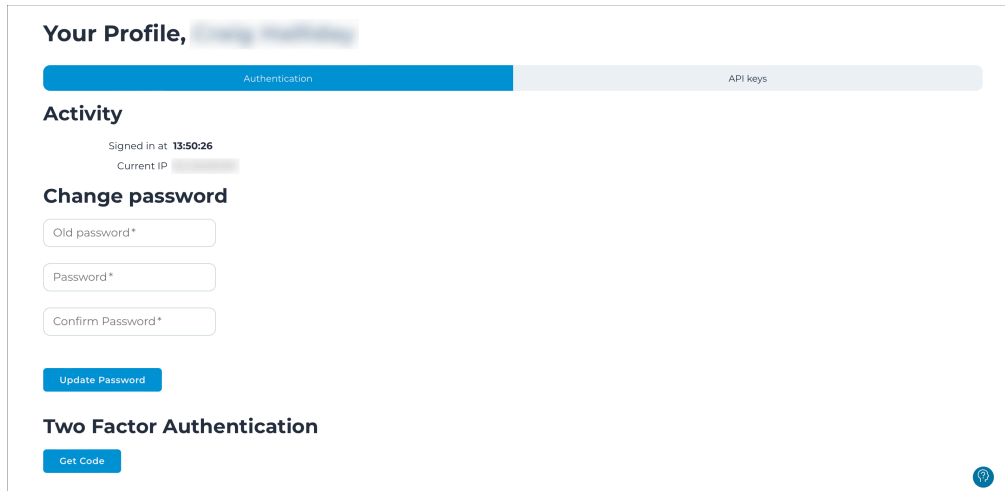
For more details, see [Authentication \(on page 216\)](#).

API keys

For more details, see [API keys \(on page 217\)](#).

Authentication

The **Authentication** page shows user activity details, lets you change your password, and lets you create a two-factor authentication code.



The screenshot shows a user profile page titled "Your Profile, [redacted]". It features a horizontal navigation bar with "Authentication" (active) and "API keys". The "Authentication" section includes:

- Activity**: Shows "Signed in at 13:50:26" and "Current IP" with a redacted address.
- Change password**: Contains three input fields labeled "Old password*", "Password*", and "Confirm Password*", followed by an "Update Password" button.
- Two Factor Authentication**: Contains a "Get Code" button.

A help icon is visible in the bottom right corner of the page.

Figure 58. Authentication page

Activity

This section shows the last time the current user signed in and the *internet protocol (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 API keys for the current user. Third-party applications that integrate with Vantage must use API keys to authenticate.

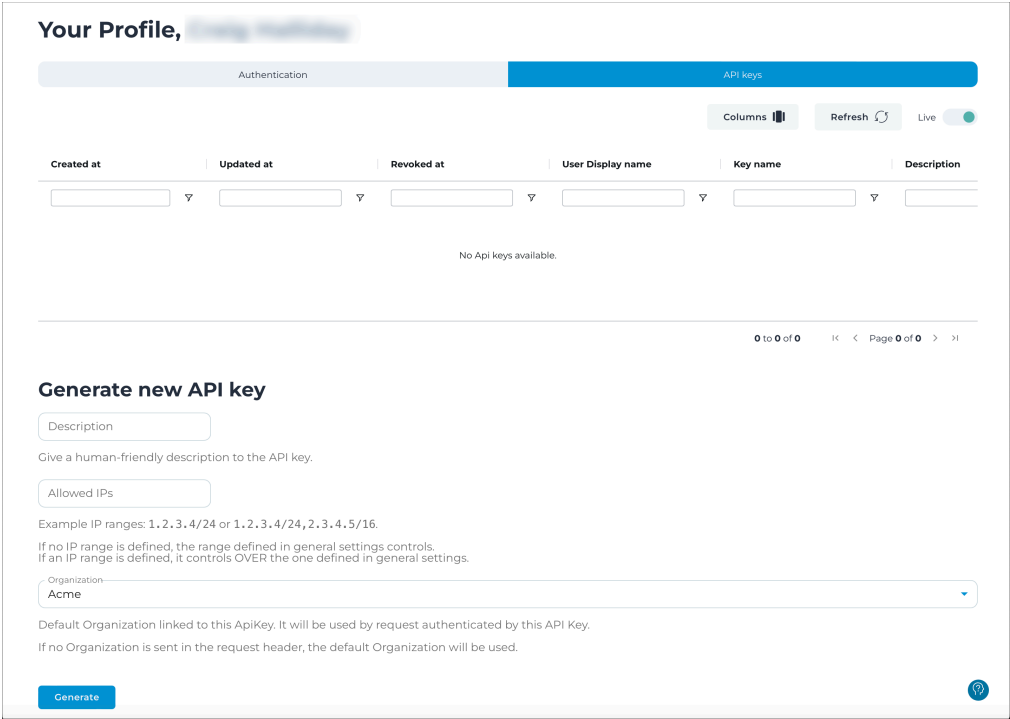


Figure 59. API Keys page

Each *application programming interface (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 <i>API</i> 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

Chapter 20. Organizations menu



Organizations menu

The organizations menu shows 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 60. 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.



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.

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.

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in the similar method to the sensor.

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 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.

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.

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.

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.

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.

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.

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.

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.

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 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.

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.

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 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.

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).

