NOZOMI NETWORKS

Vantage
User Guide

2025-07-03

Legal notices

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

Copyright

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction

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.*

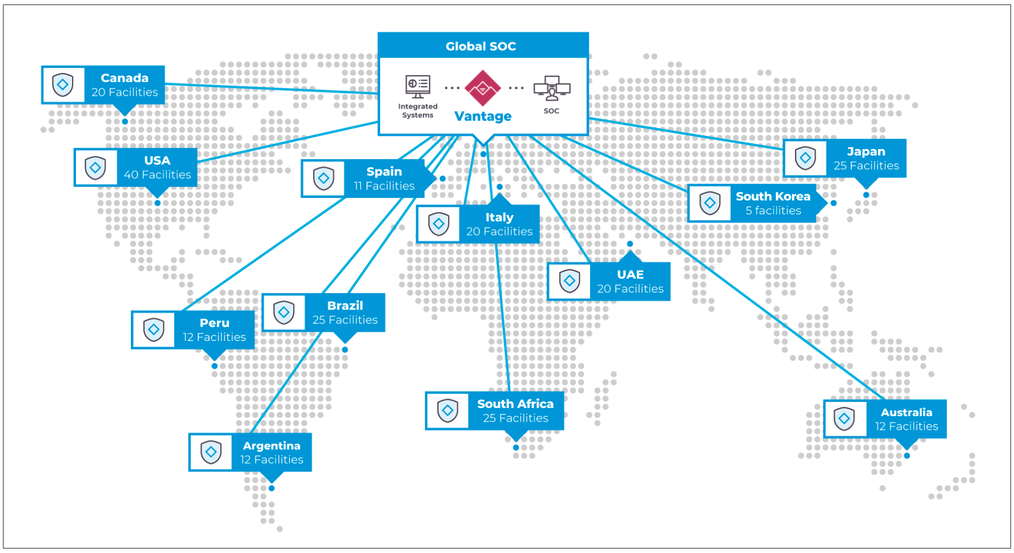


Figure 1. Vantage overview

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 from anywhere in the world
- Monitor an unlimited number of devices
- Protect an unlimited number of locations

Identify

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

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

Assess

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

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

Detect

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

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

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

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

Act

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

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

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

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

Scale

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

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

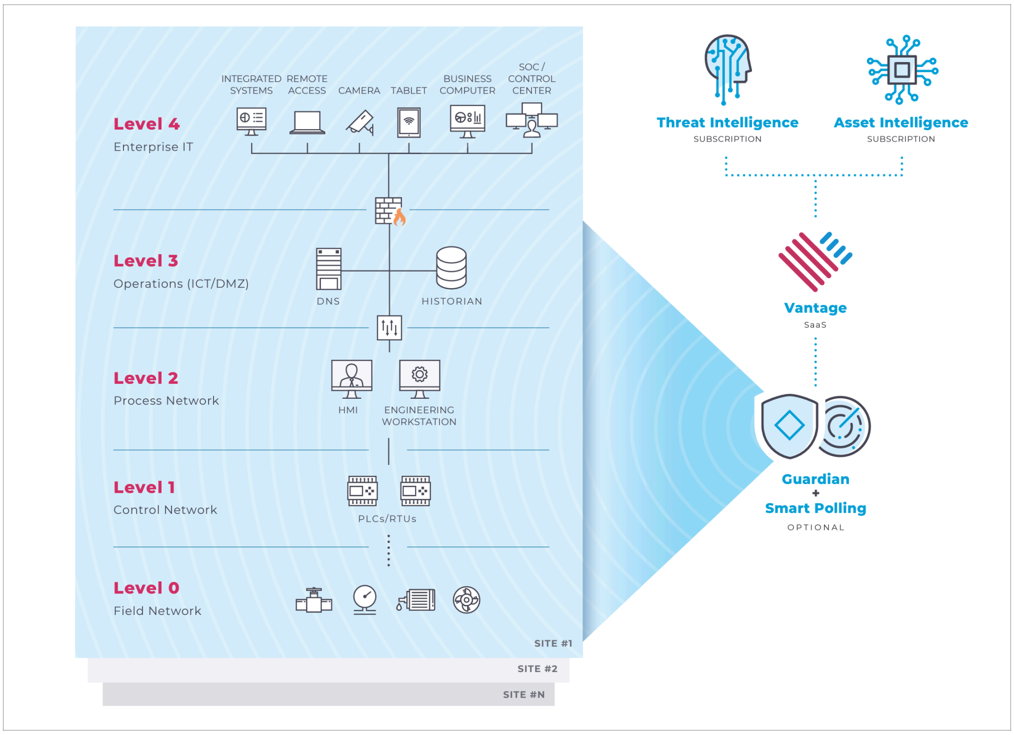


Figure 2. Vantage architecture

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:

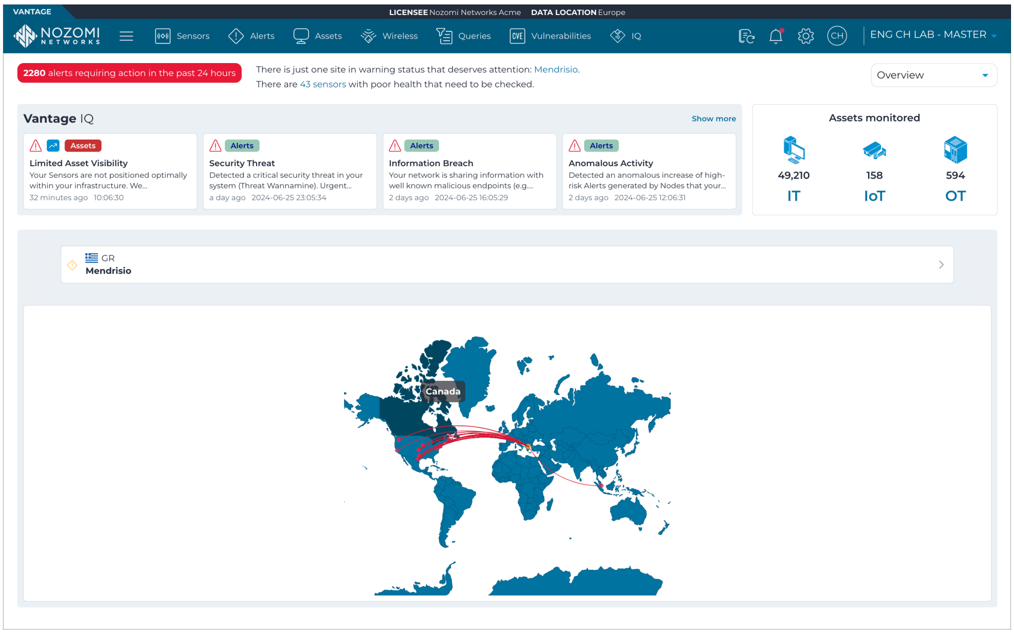
- The *ACS URL* of a standard, non-*FIPS* Vantage instance is similar to: `https://customer1.customers.us1.vantage.nozominetworks.io`
- The *ACS URL* of a *FIPS*-compliant Vantage instance is similar to: `https://nozominetworkscom.customers.us1.vantage-govcloud.nozominetworks.io`

For more details about *ACS URL*s, 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.



2280 alerts requiring action in the past 24 hours

There is just one site in warning status that deserves attention: Mendrisio.
There are 43 sensors with poor health that need to be checked.

Limited Asset Visibility
Your Sensors are not positioned optimally within your infrastructure. We...
32 minutes ago 10:06:30

Security Threat
Detected a critical security threat in your system (Threat Wannamine). Urgent...
a day ago 2024-06-25 23:05:34

Information Breach
Your network is sharing information with well known malicious endpoints (e.g....
2 days ago 2024-06-25 16:05:29

Anomalous Activity
Detected an anomalous increase of high-risk Alerts generated by Nodes that your...
2 days ago 2024-06-25 12:06:31

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 these 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 throughout 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

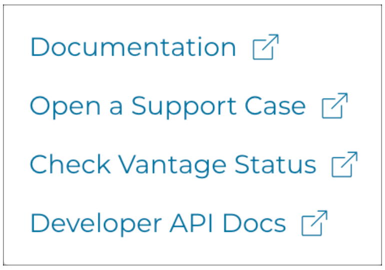
The **Refresh** icon lets you immediately refresh the current view.

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.



Top navigation bar

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

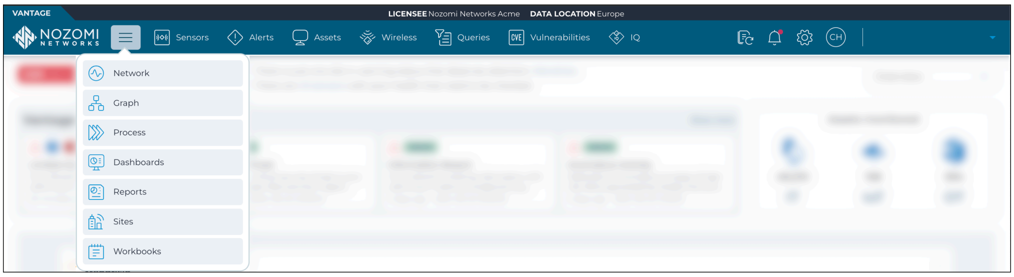


Figure 4. Top navigation bar

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 181).

Graph

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

Process

This button opens the **Process** page. For more details, see Process (on page 193)

Dashboards

This button opens the **Dashboards** page. For more details, see Dashboards (on page 197).

Reports

This button opens the **Reports** page. For more details, see Reports (on page 205).

Sites

This button opens the **Sites** page. For more details, see Sites (on page 217).

Workbooks

This button opens the **Workbooks** page. For more details, see Workbooks (on page 155).

Sensors

This button opens the **Sensors** page. For more details, see Sensors (on page 19).

Alerts

This button opens the **Alerts** page. For more details, see Alerts (on page 59).

Assets

This button opens the **Assets** page. For more details, see Assets (on page 81).

Wireless

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

Queries

This button opens the **Queries** page. For more details, see Queries (on page 121).

Vulnerabilities

This button opens the **Vulnerabilities** page. For more details, see Vulnerabilities (on page 141).

(Vantage) IQ

This button opens the **Vantage IQ** page. For more details, see Vantage IQ (on page 157).

Async operations

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

What's new

This button opens the **What's new** sidebar. For more details, see What's new drawer (on page 251).

Administration

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

Profile settings

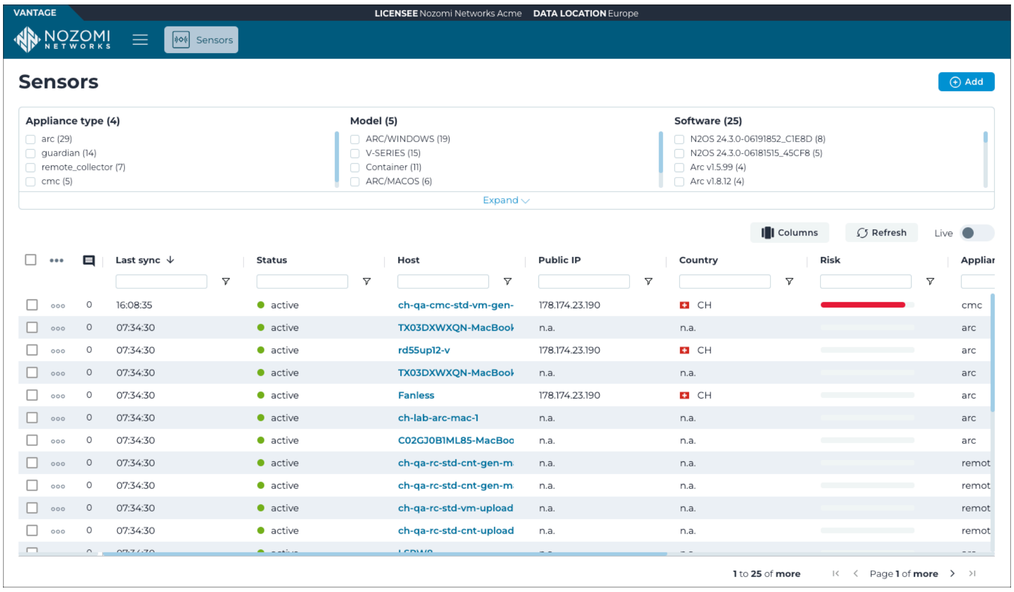
This button opens the profile settings menu. For more details, see Profile settings (on page 259).

Organization

This button opens the profile **Organization** page. For more details, see Organizations menu (on page 267).

Chapter 2. Sensors

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



Sensors

Appliance type (4)
- ☐ arc (29)
- ☐ guardian (14)
- ☐ remote_collector (7)
- ☐ cmc (5)

Model (5)
- ☐ ARC/WINDOWS (19)
- ☐ V-SERIES (15)
- ☐ Container (11)
- ☐ ARC/MACOS (6)

Software (25)
- ☐ N2OS 24.3.0-06191852_C1E8D (8)
- ☐ N2OS 24.3.0-06181515_45CF8 (5)
- ☐ Arc v1.5.99 (4)
- ☐ Arc v1.8.12 (4)

☐	•••		Last sync ↓	Status	Host	Public IP	Country	Risk	Appliar
☐	○○○	0	16:08:35	● active	ch-qa-cmc-std-vm-gen-	178.174.23.190	CH		cmc
☐	○○○	0	07:34:30	● active	TX03DXWXQN-MacBook	n.a.	n.a.		arc
☐	○○○	0	07:34:30	● active	rd55up12-v	178.174.23.190	CH		arc
☐	○○○	0	07:34:30	● active	TX03DXWXQN-MacBook	n.a.	n.a.		arc
☐	○○○	0	07:34:30	● active	Fanless	178.174.23.190	CH		arc
☐	○○○	0	07:34:30	● active	ch-lab-arc-mac-1	n.a.	n.a.		arc
☐	○○○	0	07:34:30	● active	C02GJ0B1ML85-MacBoo	n.a.	n.a.		arc
☐	○○○	0	07:34:30	● active	ch-qa-rc-std-cnt-gen-m	n.a.	n.a.		remot
☐	○○○	0	07:34:30	● active	ch-qa-rc-std-cnt-gen-m	n.a.	n.a.		remot
☐	○○○	0	07:34:30	● active	ch-qa-rc-std-vm-upload	n.a.	n.a.		remot
☐	○○○	0	07:34:30	● active	ch-qa-rc-std-cnt-upload	n.a.	n.a.		remot

1 to **25** of **more** Page **1** of **more**

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.

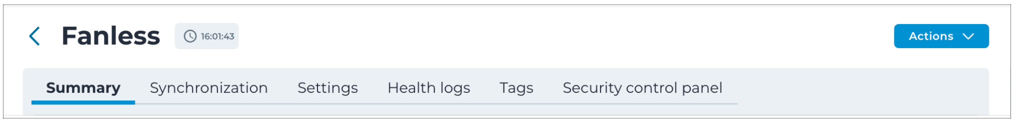


Figure 6. Details page

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

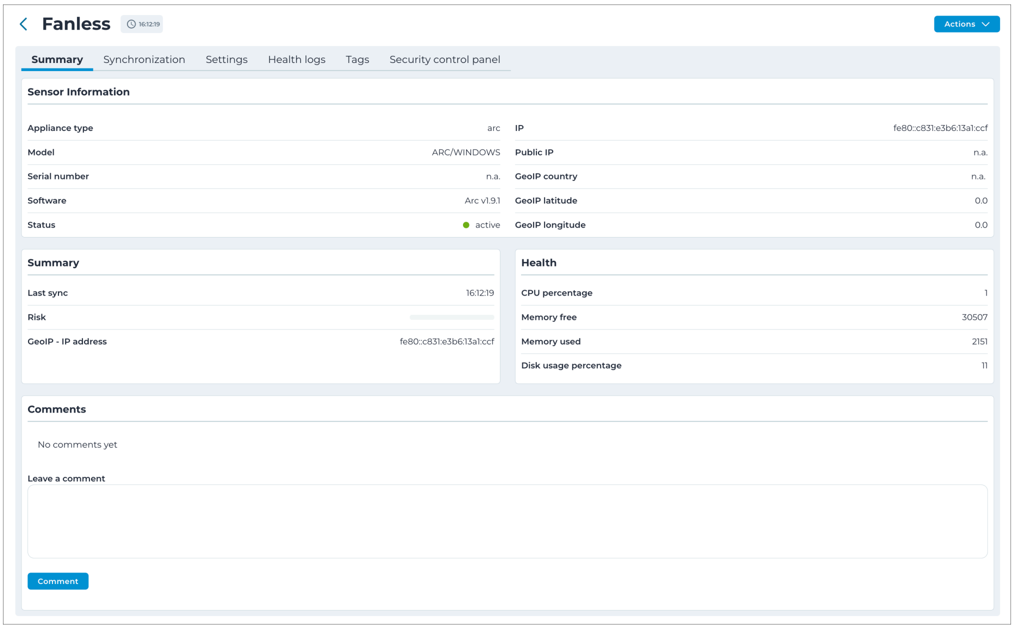
For more details, see Security control panel tab (on page 31).

Related information

Open the details page (on page 39)

Summary tab

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



Sensor Information

Appliance type	arc	IP	fe80::c831:e3b6:13a1:ccf
Model	ARC/WINDOWS	Public IP	n.a.
Serial number	n.a.	GeoIP country	n.a.
Software	Arc v1.9.1	GeoIP latitude	0.0
Status	● active	GeoIP longitude	0.0

Summary

Last sync	16:12:19
Risk	
GeoIP - IP address	fe80::c831:e3b6:13a1:ccf

Health

CPU percentage	1
Memory free	30507
Memory used	2151
Disk usage percentage	11

Comments

No comments yet

Leave a comment

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

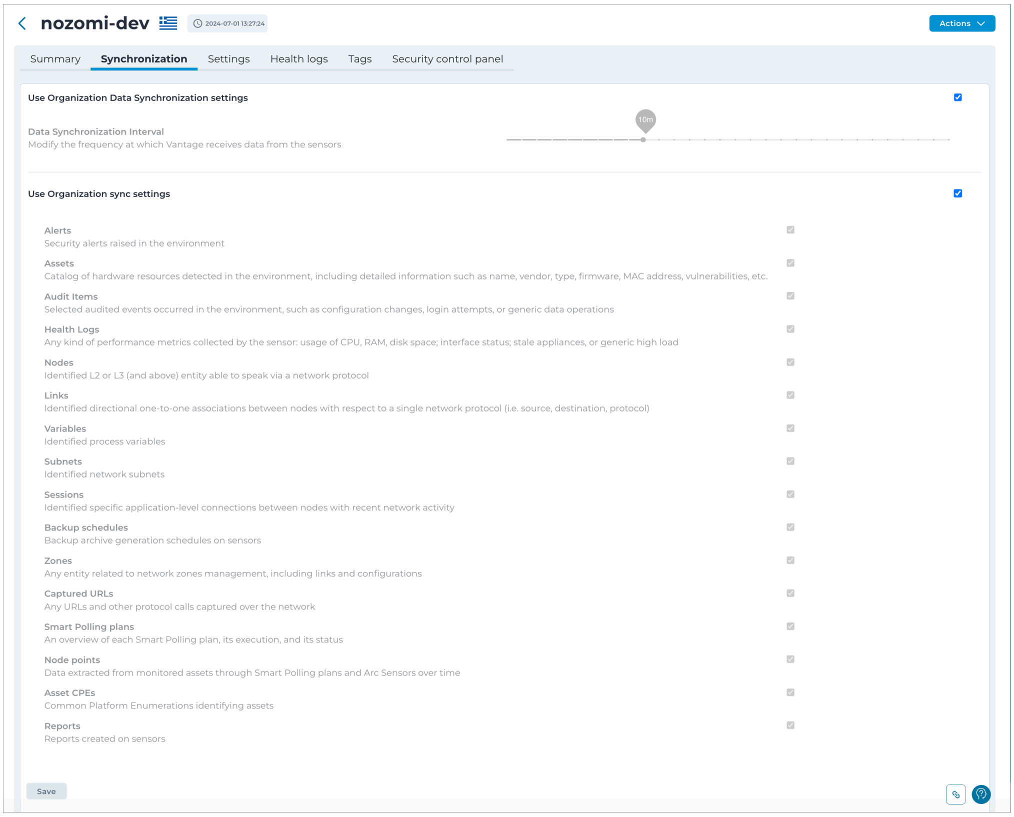
This section lets you write a comment for the sensor. It also shows comments that have been previously written.

Related information

Details page (on page 22)

Synchronization tab

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



Use Organization Data Synchronization settings ☑

Data Synchronization Interval: 10m
Modify the frequency at which Vantage receives data from the sensors

Use Organization sync settings ☑

- Alerts ☑
  Security alerts raised in the environment
- Assets ☑
  Catalog of hardware resources detected in the environment, including detailed information such as name, vendor, type, firmware, MAC address, vulnerabilities, etc.
- Audit Items ☑
  Selected audited events occurred in the environment, such as configuration changes, login attempts, or generic data operations
- Health Logs ☑
  Any kind of performance metrics collected by the sensor: usage of CPU, RAM, disk space; interface status; stale appliances, or generic high load
- Nodes ☑
  Identified L2 or L3 (and above) entity able to speak via a network protocol
- Links ☑
  Identified directional one-to-one associations between nodes with respect to a single network protocol (i.e. source, destination, protocol)
- Variables ☑
  Identified process variables
- Subnets ☑
  Identified network subnets
- Sessions ☑
  Identified specific application-level connections between nodes with recent network activity
- Backup schedules ☑
  Backup archive generation schedules on sensors
- Zones ☑
  Any entity related to network zones management, including links and configurations
- Captured URLs ☑
  Any URLs and other protocol calls captured over the network
- Smart Polling plans ☑
  An overview of each Smart Polling plan, its execution, and its status
- Node points ☑
  Data extracted from monitored assets through Smart Polling plans and Arc Sensors over time
- Asset CPEs ☑
  Common Platform Enumerations identifying assets
- Reports ☑
  Reports created on sensors

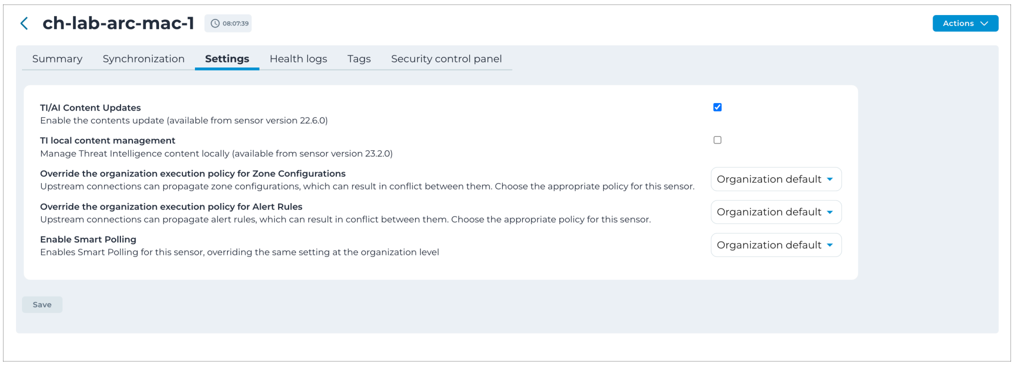
Figure 8. Synchronization tab

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.*



TI/AI Content Updates ☑
Enable the contents update (available from sensor version 22.6.0)

TI local content management □
Manage Threat Intelligence content locally (available from sensor version 23.2.0)

Override the organization execution policy for Zone Configurations Organization default
Upstream connections can propagate zone configurations, which can result in conflict between them. Choose the appropriate policy for this sensor.

Override the organization execution policy for Alert Rules Organization default
Upstream connections can propagate alert rules, which can result in conflict between them. Choose the appropriate policy for this sensor.

Enable Smart Polling Organization default
Enables Smart Polling for this sensor, overriding the same setting at the organization level

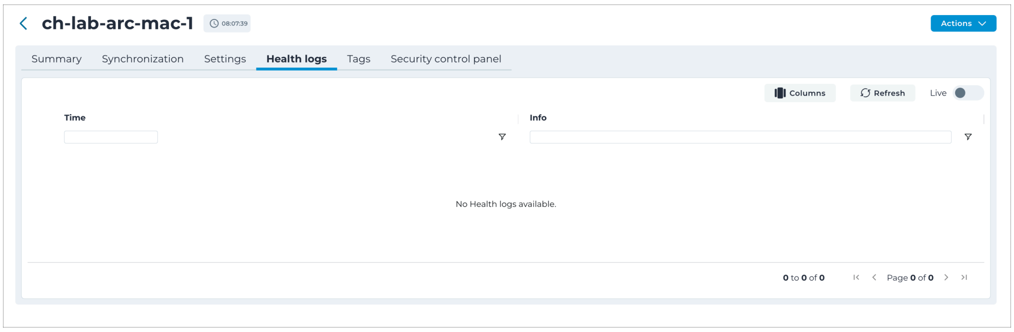
Figure 9. Settings tab

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.*



No Health logs available.

0 to 0 of 0

Page 0 of 0

Figure 10. Health logs tab

Delete a health log

The actions menu lets you delete a health log.

Procedure

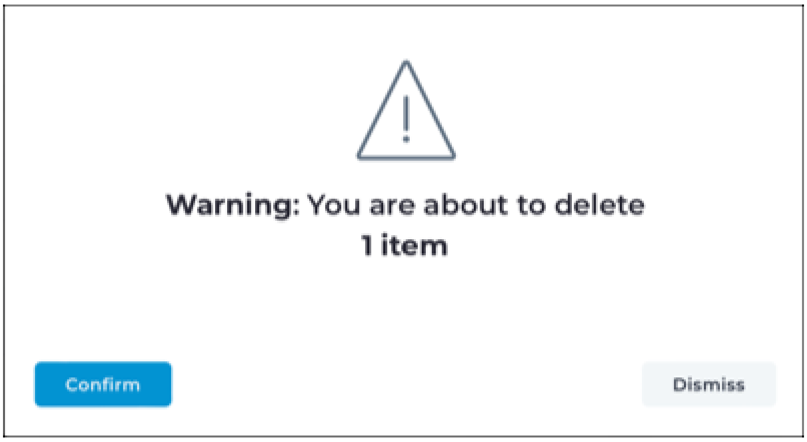
1. In the top navigation bar, select **Sensors**.

   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**.



Warning: You are about to delete 1 item

   Result: A confirmation dialog shows.

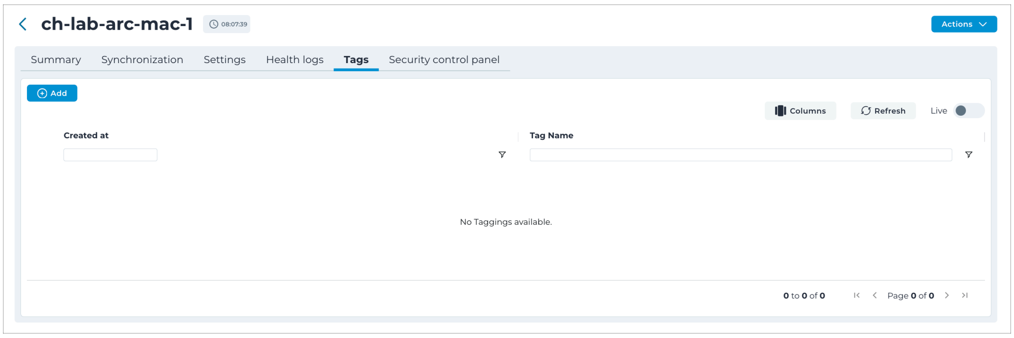
6. Select **Confirm**.

Results

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

Tags tab

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



No Taggings available.

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.

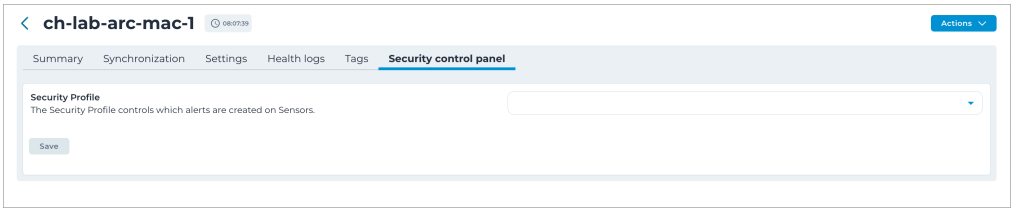
Related information

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.*



Security Profile

The Security Profile controls which alerts are created on Sensors.

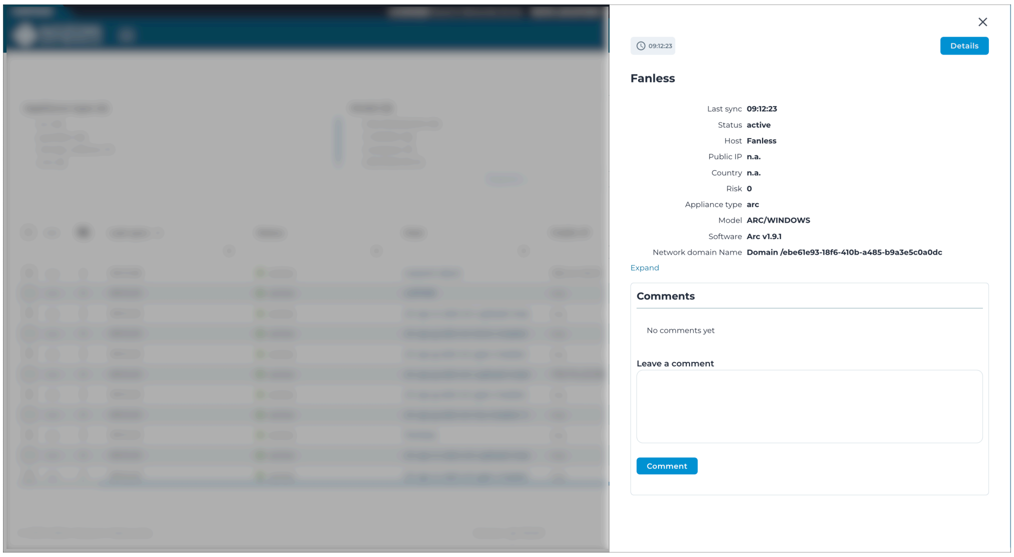
Figure 12. Security control panel tab

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.



Fanless

Last sync	09:12:23
Status	active
Host	Fanless
Public IP	n.a.
Country	n.a.
Risk	0
Appliance type	arc
Model	ARC/WINDOWS
Software	Arc v1.9.1
Network domain Name	Domain /ebe61e93-18f6-410b-a485-b9a3e5c0a0dc

Comments

No comments yet

Leave a comment

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.

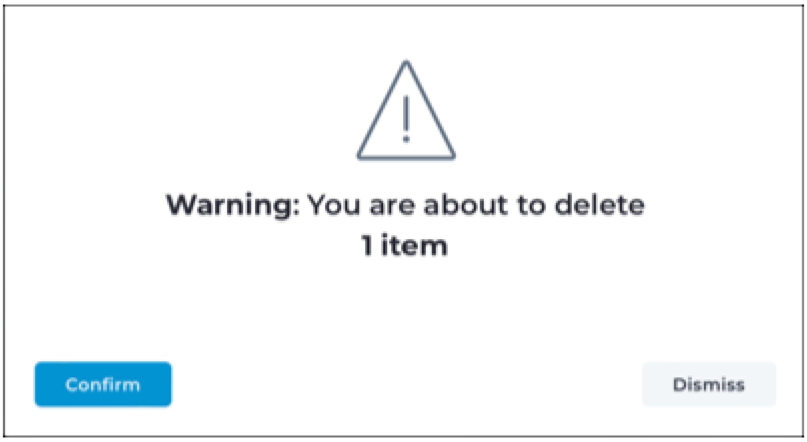
2. Choose a method to open the actions menu.

   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**.



Warning: You are about to delete 1 item

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:

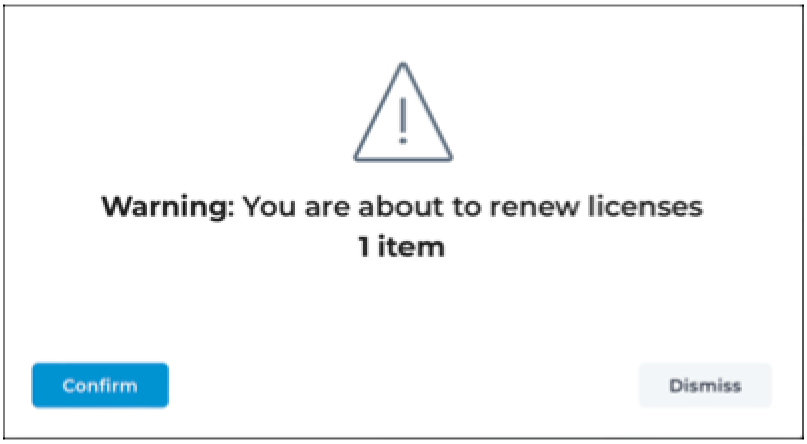
   - In the table, select the hyperlink to open the details page. Select **Actions**
   - In the table, select the ••• icon

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**.

   Warning: You are about to renew licenses
   1 item

   Result: A confirmation dialog shows.

5. Select **Confirm**.

Results

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

Migrate a sensor to a different site

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

Procedure

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

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

2. Choose a method to open the actions menu.

   Choose from:

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

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

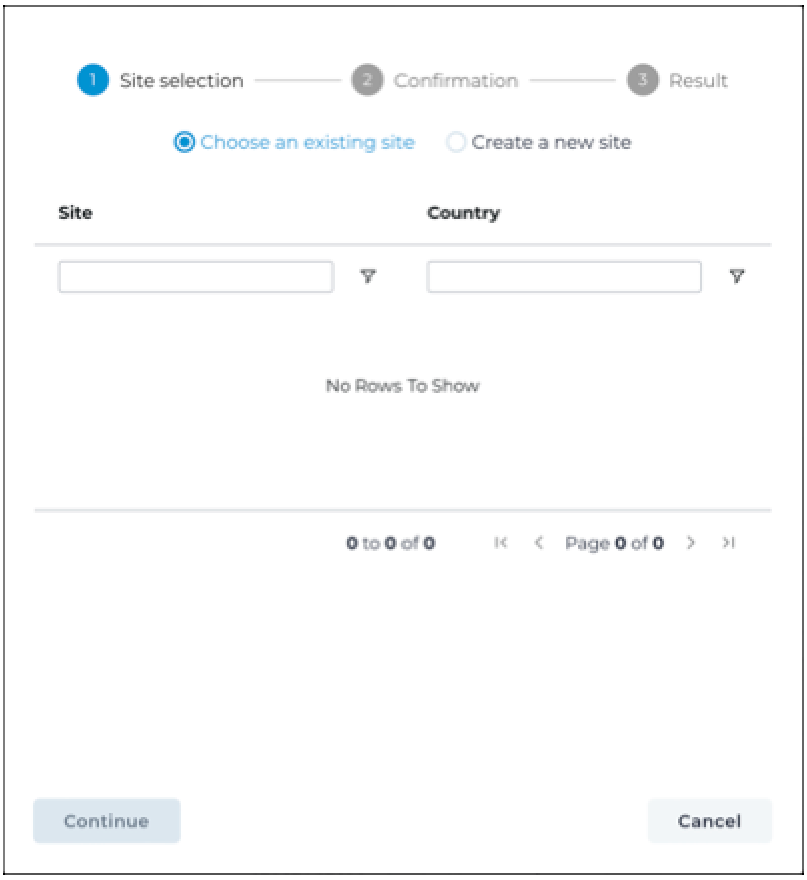
   Choose from:

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

4. Select **Migrate Site.**

   Result: A dialog shows.

5. Choose an option:



Choose from:

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

6. If you chose **Choose an existing site**, do the steps below:
   a. In the **Site** field, use the filter to select the site.

   b. In the **Country** field, use the filter to select the country.

   c. Select **Continue**.
   Result: A dialog shows.

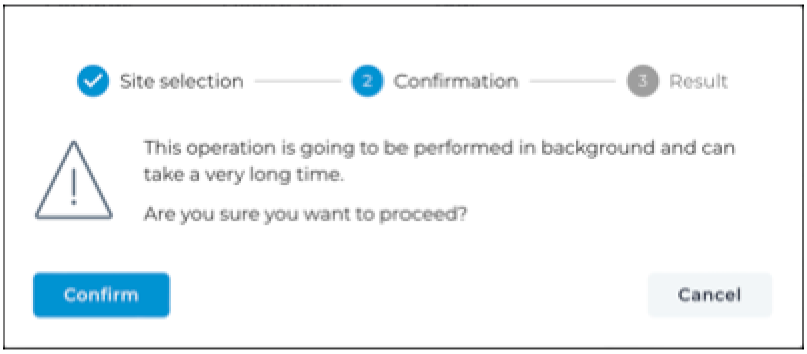
   d. Go to step 8 (on page 38).

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**.



This operation is going to be performed in background and can take a very long time.

Are you sure you want to proceed?

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**.

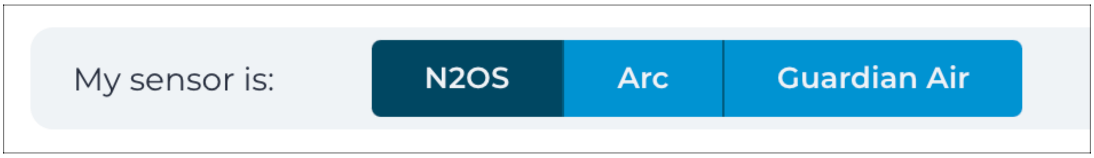
   Note:

   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.



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 56).

   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. Select **Configure Arc bundle**.

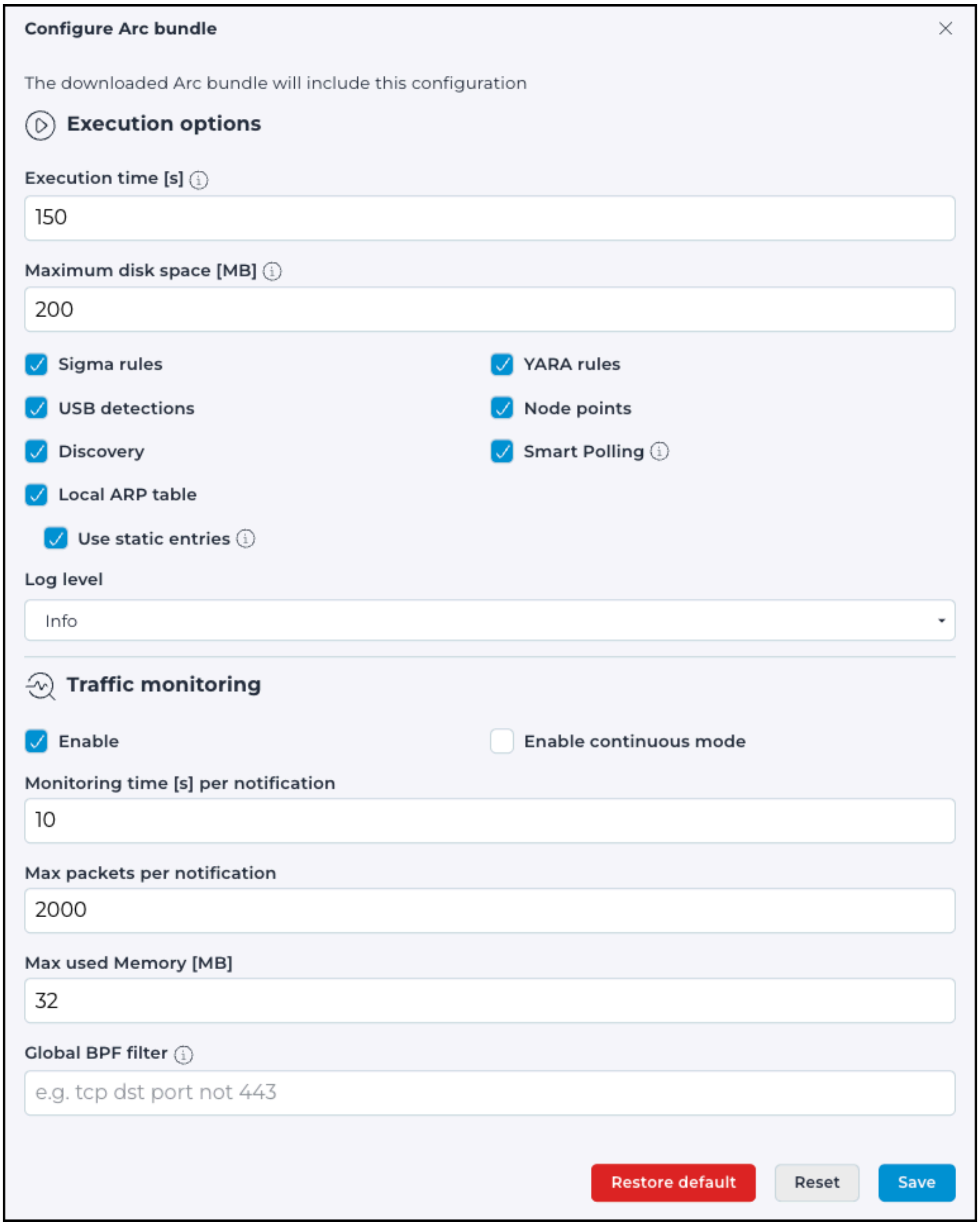
   Result: A dialog shows.

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] ⓘ

150

Maximum disk space [MB] ⓘ

200

☑ Sigma rules ☑ YARA rules

☑ USB detections ☑ Node points

☑ Discovery ☑ Smart Polling ⓘ

☑ Local ARP table

☑ Use static entries ⓘ

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

Global BPF filter ⓘ

e.g. tcp dst port not 443

Note:

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

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

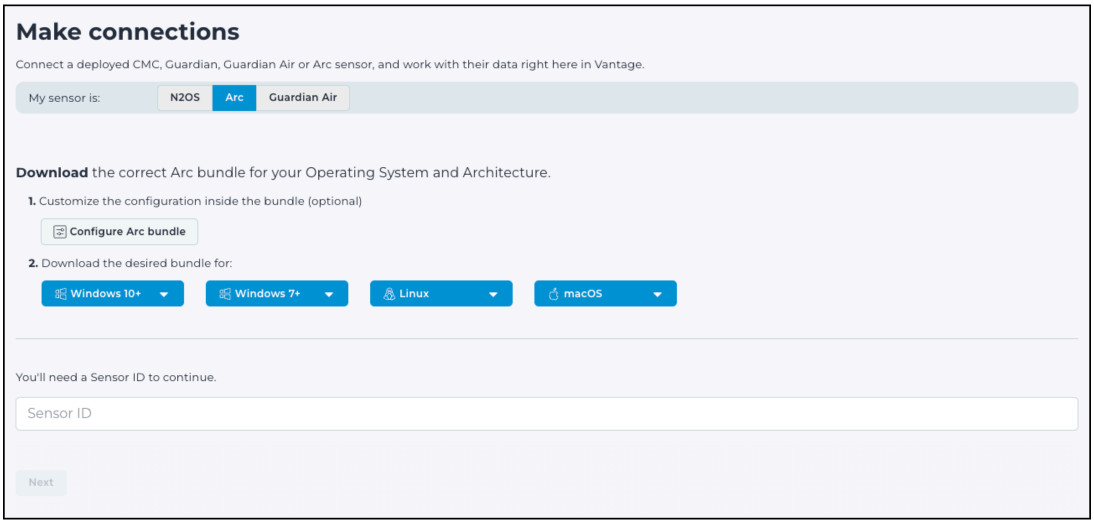
6. From the **Log level** dropdown, select the verbosity level for the log files. Select from:
    - Debug
    - Info
    - Warning
    - Error

7. If necessary, in the **Traffic monitoring** section, select from:
    - **Enable**
    - **Enable continuous mode**

    a. In the **Monitoring time [s] per notification** field, enter a value in seconds.
    b. In the **Max packets per notification** field, enter a value.
    c. In the **Max used Memory [MB]** field, enter a value.

8. Select **Save**.

9. Download the applicable bundle.



Make connections

Connect a deployed CMC, Guardian, Guardian Air or Arc sensor, and work with their data right here in Vantage.

My sensor is: N2OS [✓ Arc] Guardian Air

Download the correct Arc bundle for your Operating System and Architecture.

1. Customize the configuration inside the bundle (optional)

2. Download the desired bundle for:

You'll need a Sensor ID to continue.

Sensor ID

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

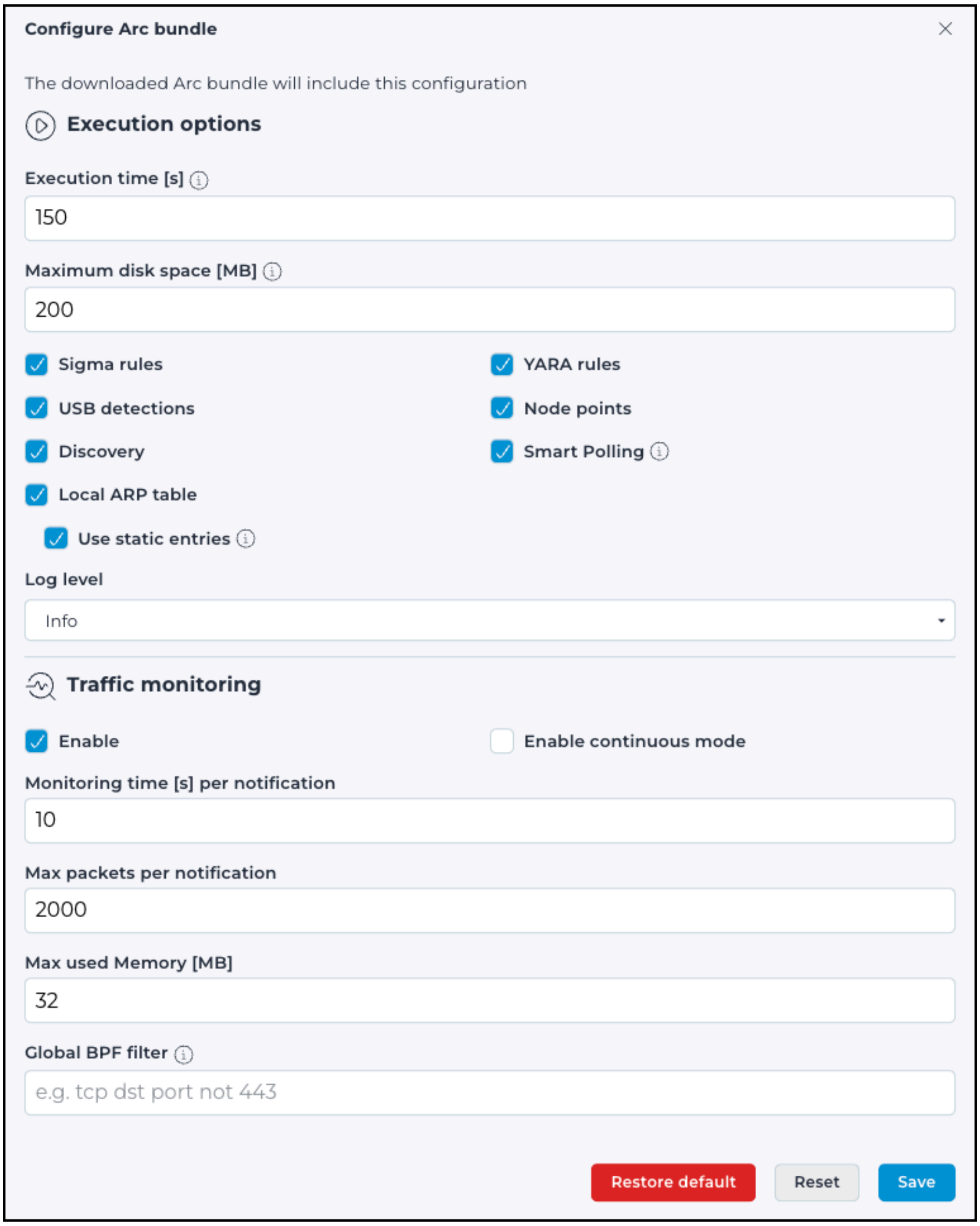
1. Log in to the sensor that you want to connect to Vantage.
2. In the *UI* of the sensor, go to the configuration page. If you want to connect a *Central Management Console (CMC)*, or Guardian, go to ⚙ **> Synchronization settings**.
3. In **Upstream Connection**, select **On** to activate the connection.
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 54).

Arc sensor configuration

A description of the configuration settings for an Arc sensor.



Configure Arc bundle

The downloaded Arc bundle will include this configuration

Execution options

Execution time [s]: 150

Maximum disk space [MB]: 200

☑ Sigma rules ☑ YARA rules

☑ USB detections ☑ Node points

☑ Discovery ☑ Smart Polling

☑ Local ARP table

☑ Use static entries

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

Global BPF filter: e.g. tcp dst port not 443

Figure 14. Configuration settings

Execution time

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

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

Maximum disk space

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

Sigma rules (Windows only)

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

YARA rules (Windows only)

This lets you enable/disable YARA rules. YARA rules are applied to every newly-detected non-signed on the host machine's file system.

USB detections (Windows only)

This lets you enable/disable detections.

Node points

This lets you enable/disable the production of node points.

Discovery

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

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

Smart Polling

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

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

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

Local ARP table

This lets you enable/disable the ability to use the local table to confirm *media access control (MAC)* addresses. The **Use static entries** checkbox lets you enable/disable the use of static entries in the table. Static entries are user-defined. You should only use them if they can be trusted.

Log level

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

- Debug
- Info
- Warning
- Error

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

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

Enable

This checkbox lets you enable/disable traffic monitoring.

Enable continuous mode

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

Arc uses two different methods for traffic monitoring:

- Intermittent mode
- Continuous mode

Intermittent mode

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

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

Continuous mode

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

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

Network interface

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

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

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

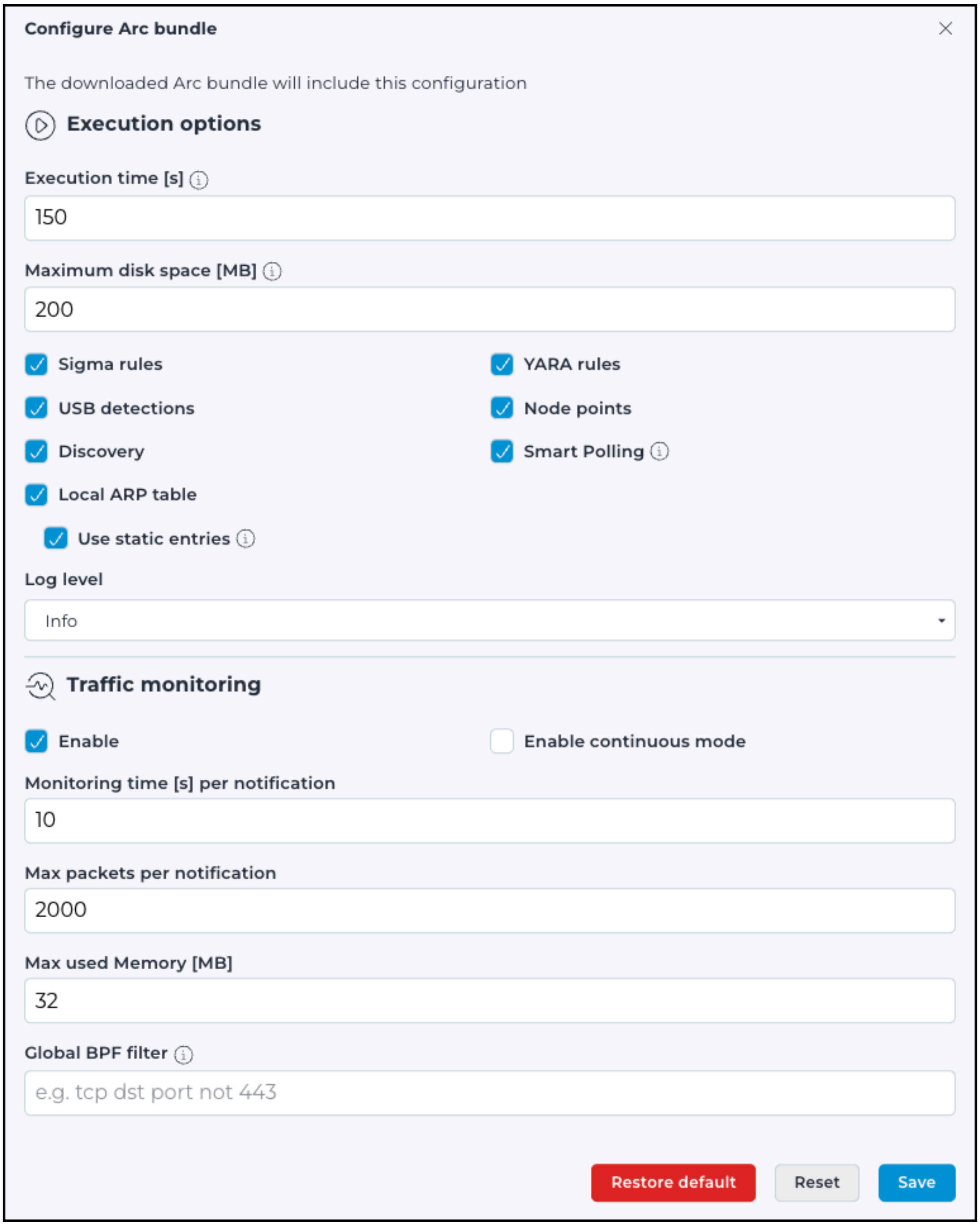
1. In the top navigation bar, select **Sensors**.

   > **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.



Configure Arc bundle

The downloaded Arc bundle will include this configuration

Execution options

Execution time [s]: 150

Maximum disk space [MB]: 200

☑ Sigma rules ☑ YARA rules

☑ USB detections ☑ Node points

☑ Discovery ☑ Smart Polling

☑ Local ARP table

☑ Use static entries

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

Global BPF filter: e.g. tcp dst port not 443

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 57).
4. Verify the connection of a sensor (on page 55).

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 57).

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 56).
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

*The **Alerts** page displays system-generated notifications about potential issues.*

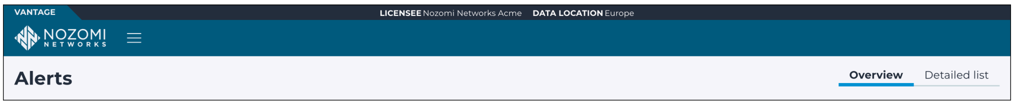


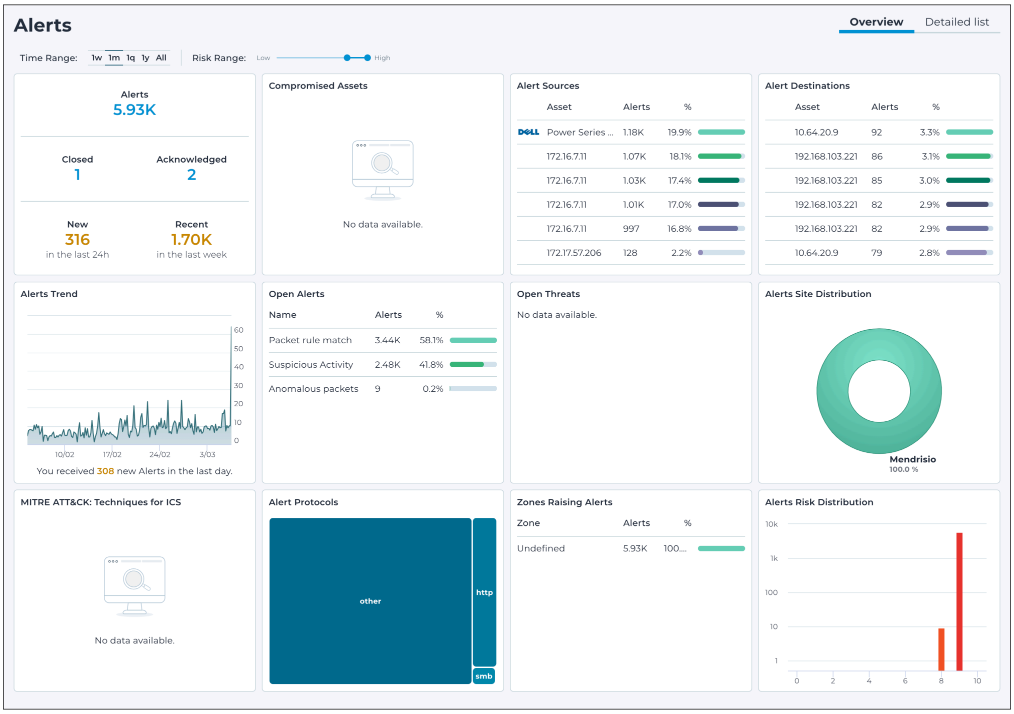
Figure 15. Alerts page

The Alerts page has these tabs:

- Overview (on page 62)
- Detailed list (on page 64)

Overview

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



Alerts
5.93K

Closed 1

Acknowledged 2

New 316 in the last 24h

Recent 1.70K in the last week

Compromised Assets

No data available.

Alert Sources

	Asset	Alerts	%
DELL	Power Series ...	1.18K	19.9%
	172.16.7.11	1.07K	18.1%
	172.16.7.11	1.03K	17.4%
	172.16.7.11	1.01K	17.0%
	172.16.7.11	997	16.8%
	172.17.57.206	128	2.2%

Alert Destinations

Asset	Alerts	%
10.64.20.9	92	3.3%
192.168.103.221	86	3.1%
192.168.103.221	85	3.0%
192.168.103.221	82	2.9%
192.168.103.221	82	2.9%
10.64.20.9	79	2.8%

Alerts Trend

You received 308 new Alerts in the last day.

Open Alerts

Name	Alerts	%
Packet rule match	3.44K	58.1%
Suspicious Activity	2.48K	41.8%
Anomalous packets	9	0.2%

Open Threats

No data available.

Alerts Site Distribution

MITRE ATT&CK: Techniques for ICS

No data available.

Alert Protocols

Zones Raising Alerts

Zone	Alerts	%
Undefined	5.93K	100....

Alerts Risk Distribution

Figure 16. Overview page

Time Range

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

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

Risk Range

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

Alerts

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

- Closed
- Acknowledged
- New
- Recent

Compromised Assets

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

Alert Sources

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

Alert Protocols

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

Alerts Trend

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

Open Alerts

Lists a breakdown of open alerts by category.

Open Threats

Lists active security threats detected within the system.

Alerts Site Distribution

Shows the distribution of alerts by site or geographical region.

MITRE ATT&CK: Techniques for ICS

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

Alert Protocols

Shows the network protocols associated with detected alerts.

Zones Raising Alerts

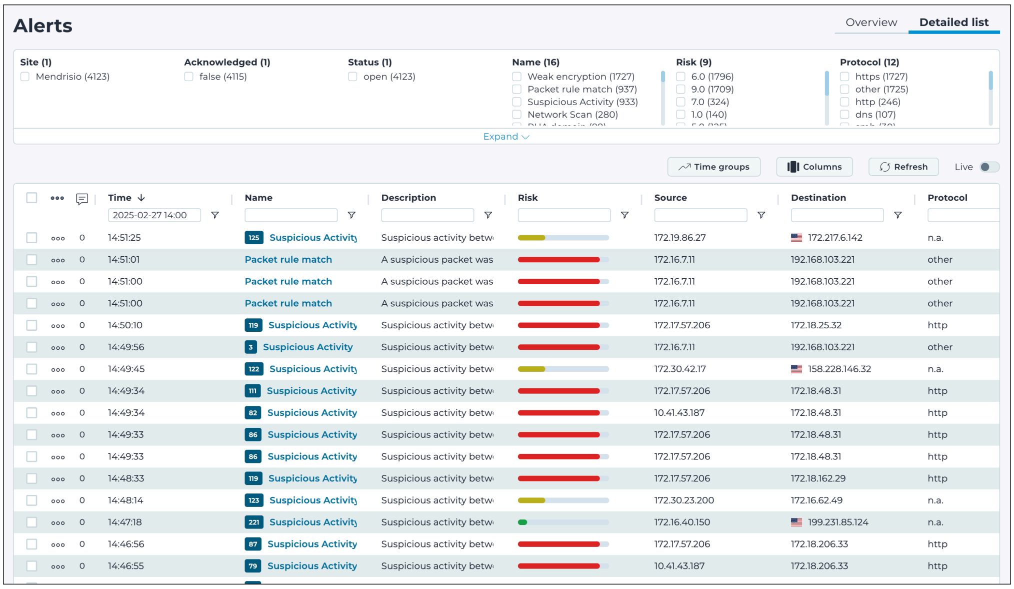
Shows which network zones are generating security alerts and their respective alert counts.

Alerts Risk Distribution

Shows the severity of alerts using a risk distribution graph.

Detailed list

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



Site (1)
□ Mendrisio (4123)

Acknowledged (1)
□ false (4115)

Status (1)
□ open (4123)

Name (16)
□ Weak encryption (1727)
□ Packet rule match (937)
□ Suspicious Activity (933)
□ Network Scan (280)

Risk (9)
□ 6.0 (1796)
□ 9.0 (1709)
□ 7.0 (324)
□ 1.0 (140)

Protocol (12)
□ https (1727)
□ other (1725)
□ http (246)
□ dns (107)

□	•••		Time ↓	Name	Description	Risk	Source	Destination	Protocol
			2025-02-27 14:00						
□	○○○	0	14:51:25	125 Suspicious Activity	Suspicious activity betw	🟨	172.19.86.27	172.217.6.142	n.a.
□	○○○	0	14:51:01	Packet rule match	A suspicious packet was	🟥	172.16.7.11	192.168.103.221	other
□	○○○	0	14:51:00	Packet rule match	A suspicious packet was	🟥	172.16.7.11	192.168.103.221	other
□	○○○	0	14:51:00	Packet rule match	A suspicious packet was	🟥	172.16.7.11	192.168.103.221	other
□	○○○	0	14:50:10	119 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.25.32	http
□	○○○	0	14:49:56	3 Suspicious Activity	Suspicious activity betw	🟥	172.16.7.11	192.168.103.221	other
□	○○○	0	14:49:45	122 Suspicious Activity	Suspicious activity betw	🟨	172.30.42.17	158.228.146.32	n.a.
□	○○○	0	14:49:34	111 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.48.31	http
□	○○○	0	14:49:34	82 Suspicious Activity	Suspicious activity betw	🟥	10.41.43.187	172.18.48.31	http
□	○○○	0	14:49:33	86 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.48.31	http
□	○○○	0	14:49:33	86 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.48.31	http
□	○○○	0	14:48:33	119 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.162.29	http
□	○○○	0	14:48:14	123 Suspicious Activity	Suspicious activity betw	🟨	172.30.23.200	172.16.62.49	n.a.
□	○○○	0	14:47:18	221 Suspicious Activity	Suspicious activity betw	🟩	172.16.40.150	199.231.85.124	n.a.
□	○○○	0	14:46:56	87 Suspicious Activity	Suspicious activity betw	🟥	172.17.57.206	172.18.206.33	http
□	○○○	0	14:46:55	79 Suspicious Activity	Suspicious activity betw	🟥	10.41.43.187	172.18.206.33	http

Figure 17. Detailed list page

Site

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

Acknowledged

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

Status

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

Name

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

Risk

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

Protocol

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

Time groups

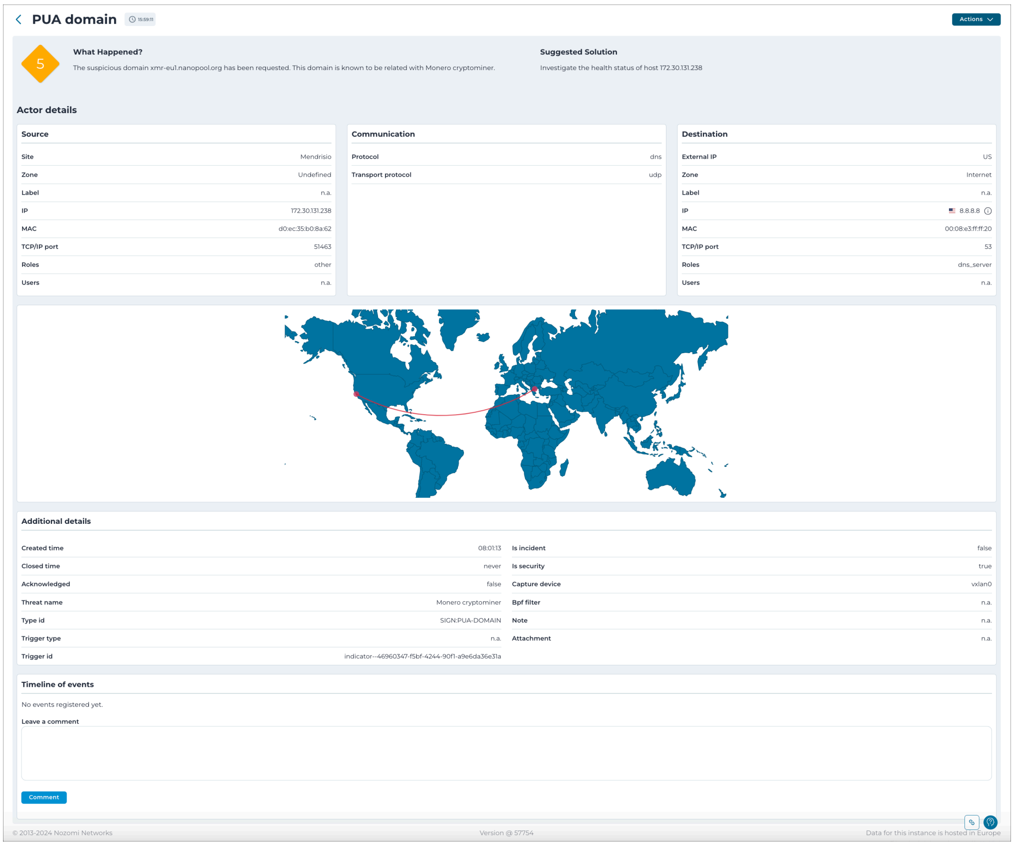
The **Time groups** button displays a throughput view of the data over a given time period.

Columns

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

Details page

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



What Happened?

The suspicious domain xmr-eu1.nanopool.org has been requested. This domain is known to be related with Monero cryptominer.

Suggested Solution

Investigate the health status of host 172.30.131.238

Actor details

Source	
Site	Mendrisio
Zone	Undefined
Label	n.a.
IP	172.30.131.238
MAC	d0:ec:35:b0:8a:62
TCP/IP port	51463
Roles	other
Users	n.a.

Communication	
Protocol	dns
Transport protocol	udp

Destination	
External IP	US
Zone	Internet
Label	n.a.
IP	8.8.8.8
MAC	00:08:e3:ff:ff:20
TCP/IP port	53
Roles	dns_server
Users	n.a.

Additional details

Created time	08:01:13	Is incident	false
Closed time	never	Is security	true
Acknowledged	false	Capture device	vxlan0
Threat name	Monero cryptominer	Bpf filter	n.a.
Type id	SIGN:PUA-DOMAIN	Note	n.a.
Trigger type	n.a.	Attachment	n.a.
Trigger id	indicator--46960347-f5bf-4244-90f1-a9e6da36e31a		

Timeline of events

No events registered yet.

Leave a comment

© 2013-2024 Nozomi Networks Version @ 57754 Data for this instance is hosted in Europe

Figure 18. Details page

Actions dropdown

This dropdown gives you access to these actions:

- **Acknowledge**
- **Unacknowledge**
- **Close**
- **Create Alert Rule For This Alert**
- **Alert Trace**

Summary

The summary section shows:

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

Actor details

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

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

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

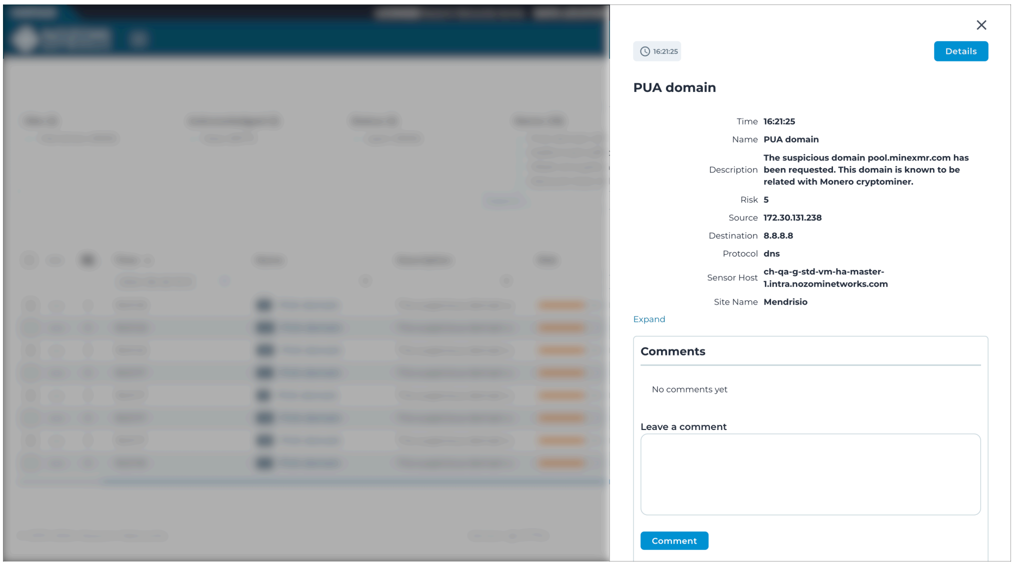
This section lets you add, or read, comments about this alert.

Related information

Open the details page (on page 80)

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.



PUA domain

Time	16:21:25
Name	PUA domain
Description	The suspicious domain pool.minexmr.com has been requested. This domain is known to be related with Monero cryptominer.
Risk	5
Source	172.30.131.238
Destination	8.8.8.8
Protocol	dns
Sensor Host	ch-qa-g-std-vm-ha-master-1.intra.nozominetworks.com
Site Name	Mendrisio

No comments yet

Figure 19. 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 80)

Table interactions

Actions menu

Acknowledge an alert

The actions menu lets you acknowledge one or more alerts.

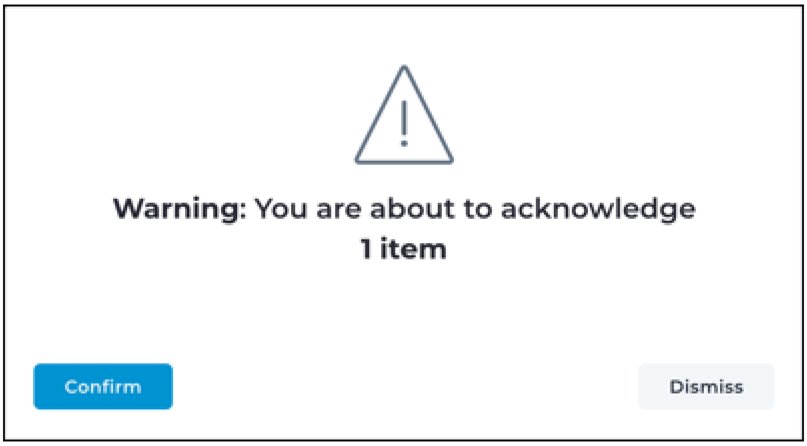
Procedure

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.

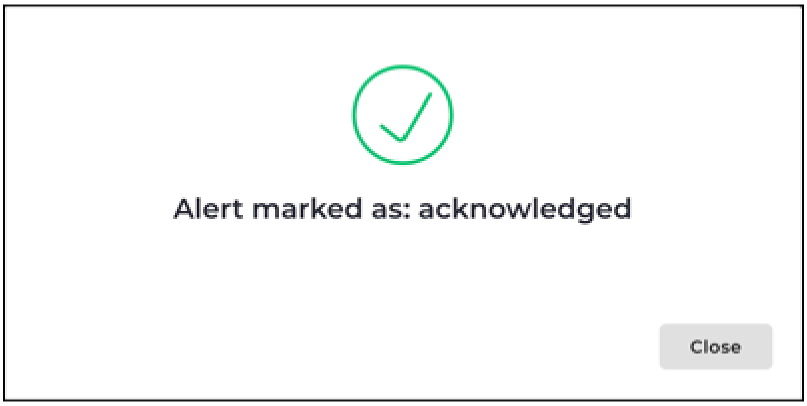
5. Select **Confirm** to acknowledge the alert(s).



Warning: You are about to acknowledge **1 item**

Result: A dialog shows.

6. Select **Close**.



Alert marked as: acknowledged

Results

The alert has been acknowledged.

Unacknowledge an alert

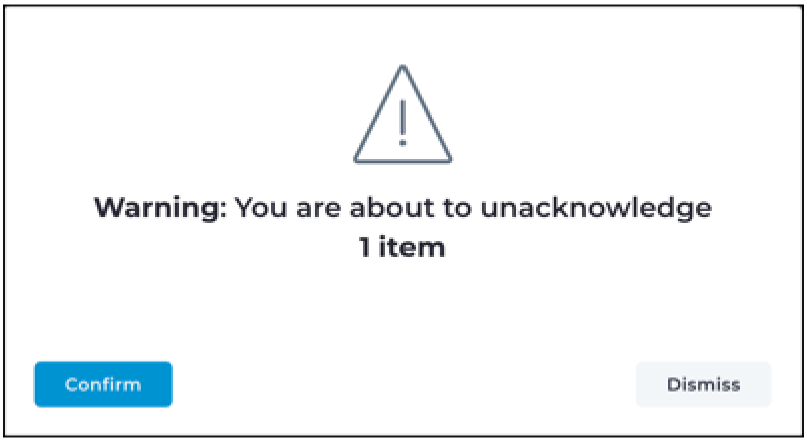
The actions menu lets you unacknowledge an alert that has previously been acknowledged.

Procedure

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

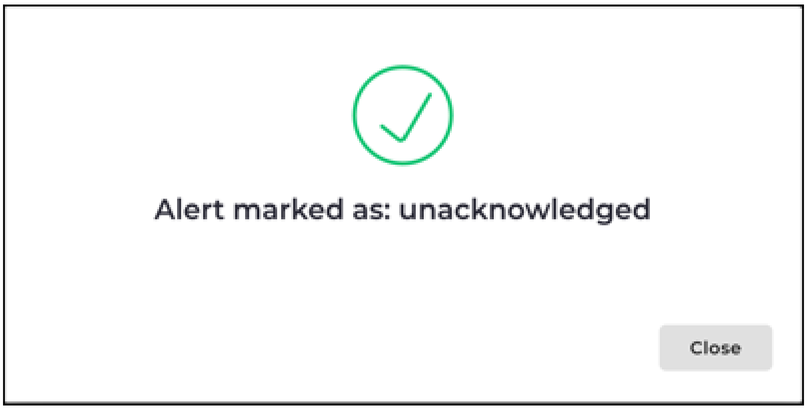
   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Uncknowledge**.

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



Warning: You are about to unacknowledge 1 item

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



Alert marked as: unacknowledged

Results

The alert has been unacknowledged.

Close an alert

The actions menu lets you close an alert.

Procedure

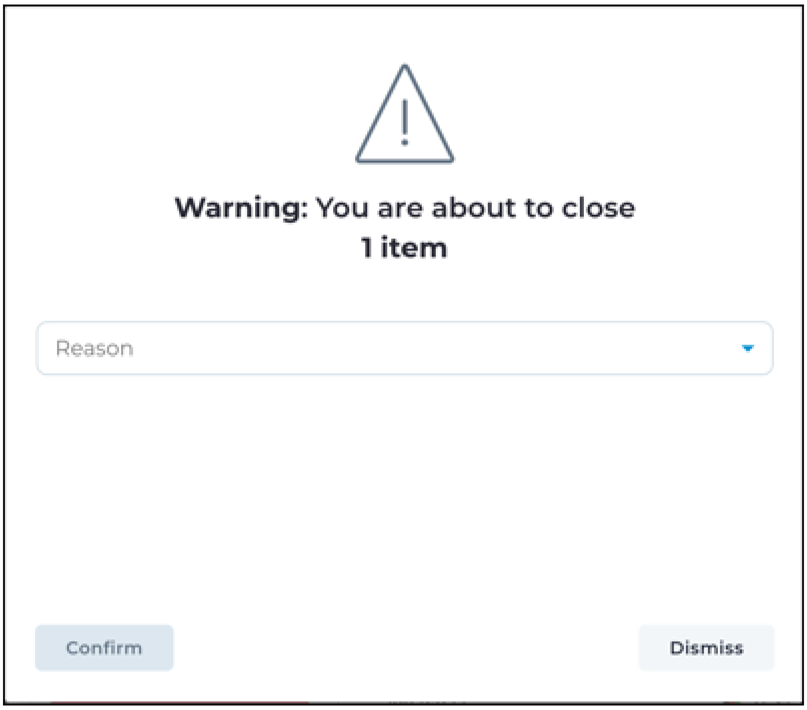
1. In the top navigation bar, select **Alerts**.
2. If you use the ••• icon in the table, choose a method to select one, or more, items.

   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**.

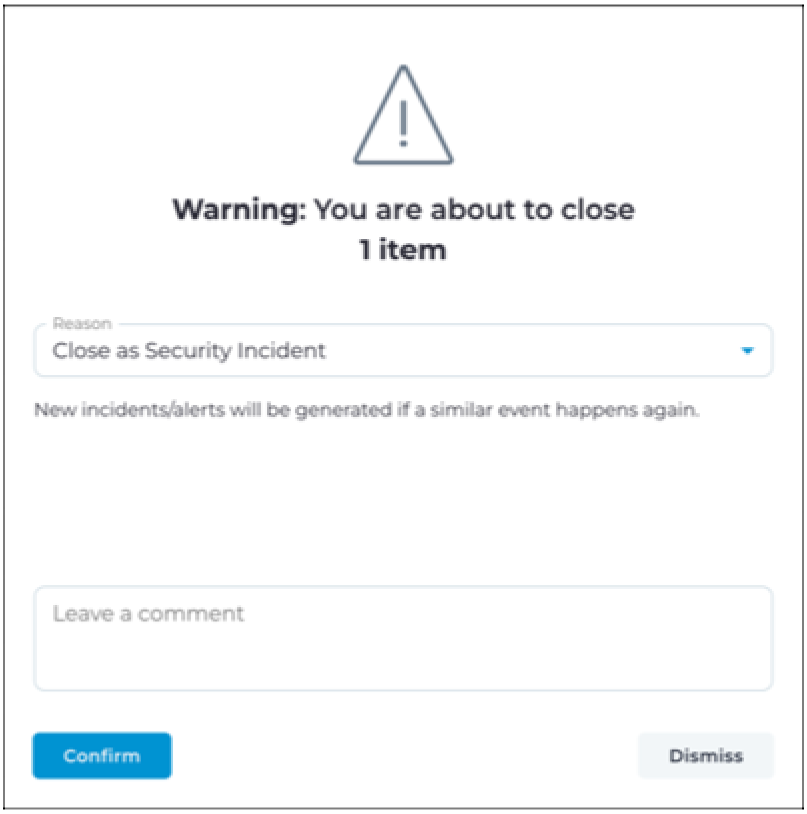
   Result: A dialog shows.

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



Warning: You are about to close
1 item

6. Select **Confirm**.



Warning: You are about to close
1 item

Reason: Close as Security Incident

New incidents/alerts will be generated if a similar event happens again.

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.

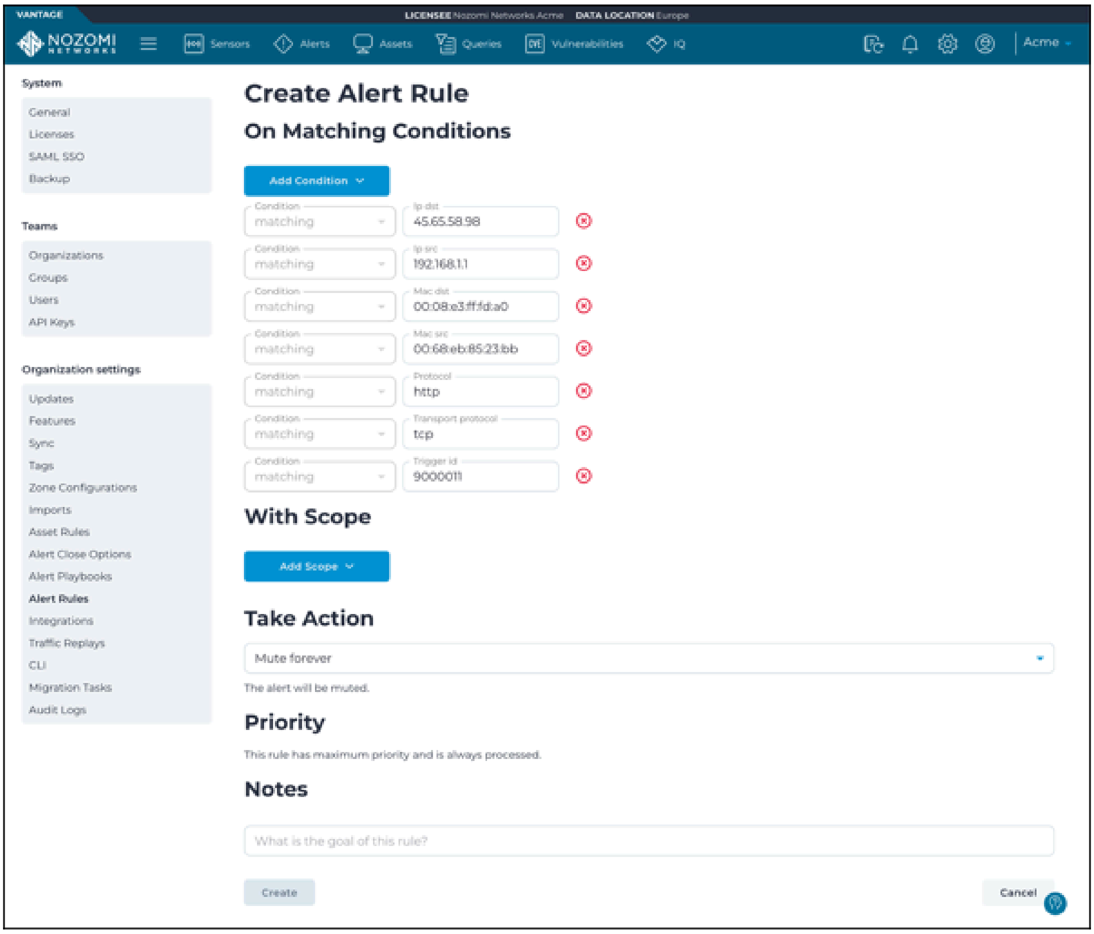
Procedure

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

Condition	Field	Value
matching	Ip dst	45.65.58.98
matching	Ip src	192.168.1.1
matching	Mac dst	00:08:e3:ff:fd:a0
matching	Mac src	00:68:eb:85:23:bb
matching	Protocol	http
matching	Transport protocol	tcp
matching	Trigger id	9000011

With 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?

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

Results

The alert rule has been created.

Trace an alert

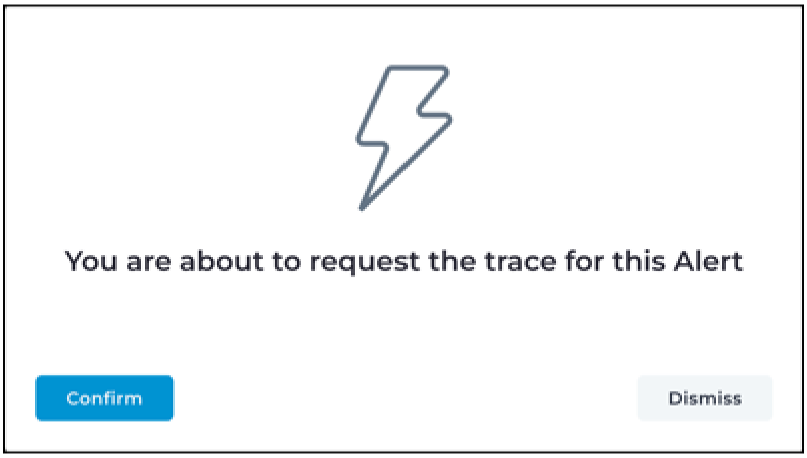
The action menu lets you download a trace file for a specific alert.

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.

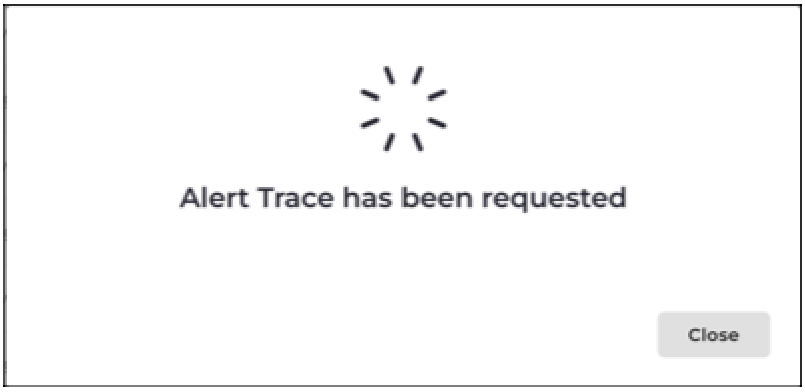
   Choose from:
   - Select the top checkbox to select all the items in the current table view
   - Select multiple checkboxes for the items that you want to choose
   - Select the checkbox for the item that you want to choose
3. Select the ••• icon to open the actions menu.
4. Select **Alert Trace**.

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



You are about to request the trace for this Alert

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



Alert Trace has been requested

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 66) opens.

Related information

Details page (on page 66)

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 68) opens.

Related information

Summary drawer (on page 68)

Chapter 4. Assets

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

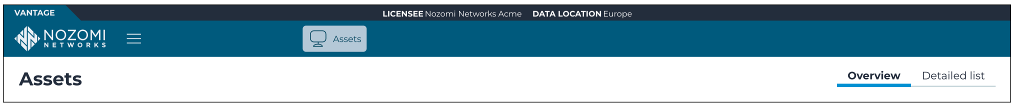


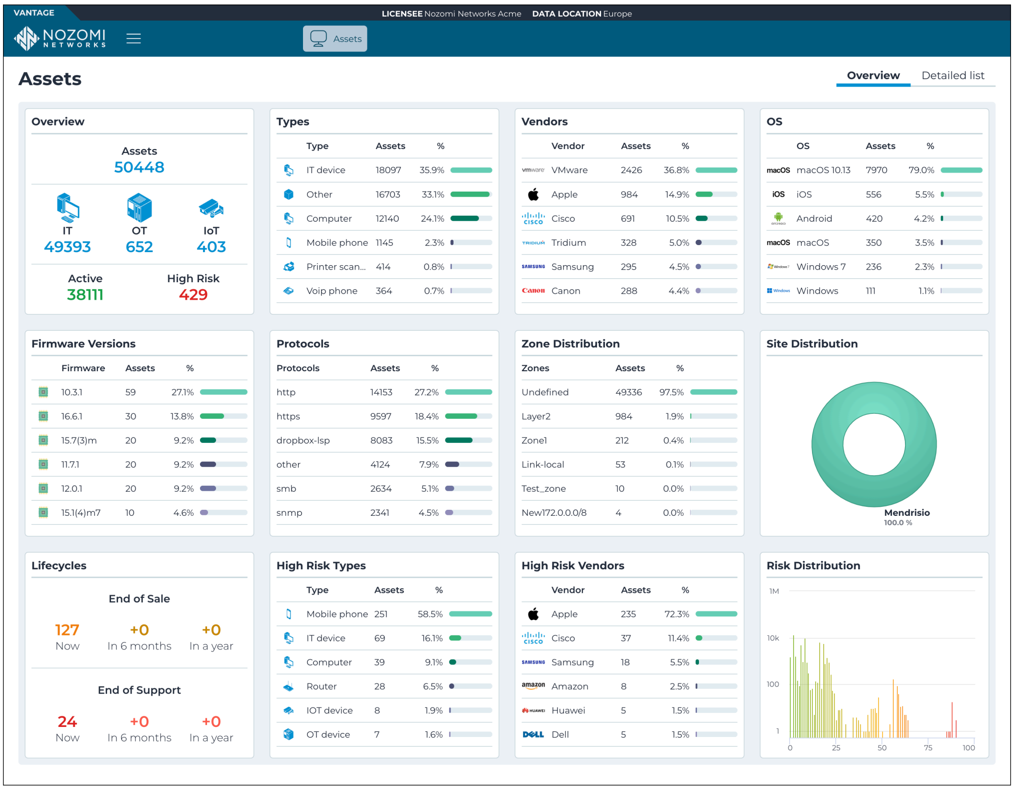
Figure 20. Assets page

The **Assets** page has these tabs:

- Overview (on page 84)
- Detailed list (on page 86)

Overview

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



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

Assets

Overview

Assets 50448

IT 49393 · OT 652 · IoT 403

Active 38111 · High Risk 429

Types

Type	Assets	%
IT device	18097	35.9%
Other	16703	33.1%
Computer	12140	24.1%
Mobile phone	1145	2.3%
Printer scan...	414	0.8%
Voip phone	364	0.7%

Vendors

Vendor	Assets	%
VMware	2426	36.8%
Apple	984	14.9%
Cisco	691	10.5%
Tridium	328	5.0%
Samsung	295	4.5%
Canon	288	4.4%

OS

OS	Assets	%
macOS 10.13	7970	79.0%
iOS	556	5.5%
Android	420	4.2%
macOS	350	3.5%
Windows 7	236	2.3%
Windows	111	1.1%

Firmware Versions

Firmware	Assets	%
10.3.1	59	27.1%
16.6.1	30	13.8%
15.7(3)m	20	9.2%
11.7.1	20	9.2%
12.0.1	20	9.2%
15.1(4)m7	10	4.6%

Protocols

Protocols	Assets	%
http	14153	27.2%
https	9597	18.4%
dropbox-lsp	8083	15.5%
other	4124	7.9%
smb	2634	5.1%
snmp	2341	4.5%

Zone Distribution

Zones	Assets	%
Undefined	49336	97.5%
Layer2	984	1.9%
Zone1	212	0.4%
Link-local	53	0.1%
Test_zone	10	0.0%
New172.0.0.0/8	4	0.0%

Lifecycles

End of Sale

Now	In 6 months	In a year
127	+0	+0

End of Support

Now	In 6 months	In a year
24	+0	+0

High Risk Types

Type	Assets	%
Mobile phone	251	58.5%
IT device	69	16.1%
Computer	39	9.1%
Router	28	6.5%
IOT device	8	1.9%
OT device	7	1.6%

High Risk Vendors

Vendor	Assets	%
Apple	235	72.3%
Cisco	37	11.4%
Samsung	18	5.5%
Amazon	8	2.5%
Huawei	5	1.5%
Dell	5	1.5%

Figure 21. Overview page

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

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

Overview

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

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

Types

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

Vendors

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

OS

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

Firmware Versions

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

Protocols

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

Zone Distribution

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

Site Distribution

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

Lifecycles

This shows lifecycle information about the assets.

High Risk Types

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

High Risk Vendors

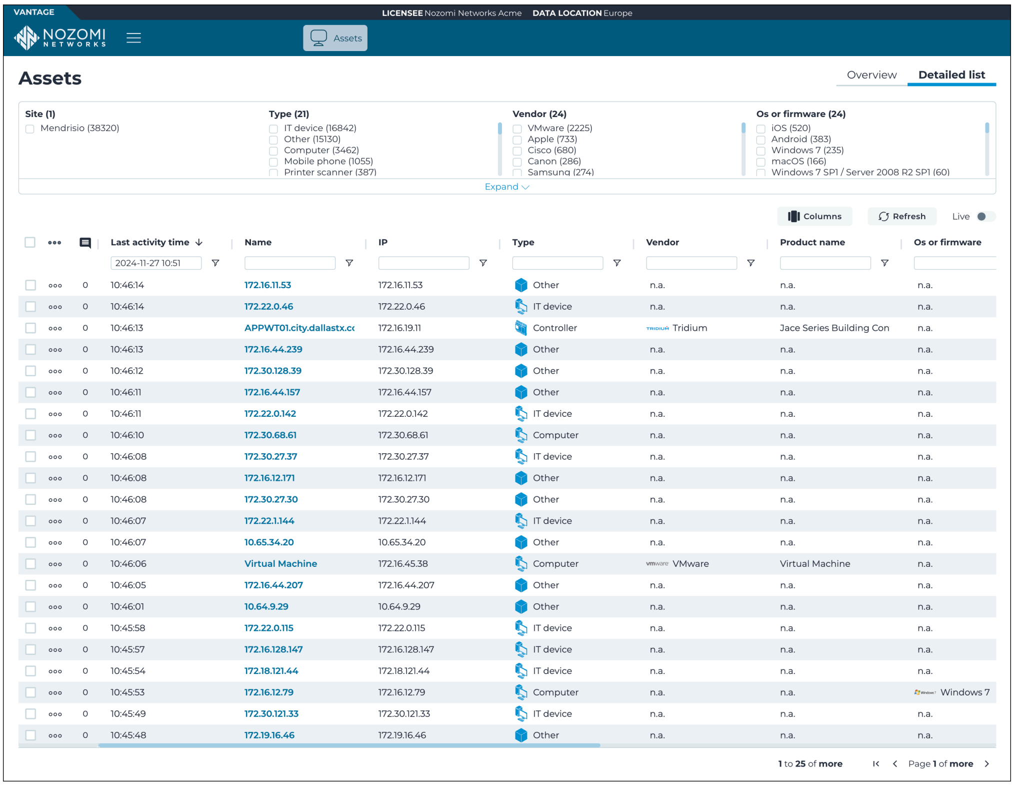
This shows a list of assets that are from high risk vendors, in descending order, and the related information.

Risk Distribution

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

Detailed list

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



LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Assets

Site (1)
□ Mendrisio (38320)

Type (21)
□ IT device (16842)
□ Other (15130)
□ Computer (3462)
□ Mobile phone (1055)
□ Printer scanner (387)

Vendor (24)
□ VMware (2225)
□ Apple (733)
□ Cisco (680)
□ Canon (286)
□ Samsung (274)

Os or firmware (24)
□ iOS (520)
□ Android (383)
□ Windows 7 (235)
□ macOS (166)
□ Windows 7 SP1 / Server 2008 R2 SP1 (60)

□	•••		Last activity time ↓	Name	IP	Type	Vendor	Product name	Os or firmware
			2024-11-27 10:51						
□	ooo	0	10:46:14	172.16.11.53	172.16.11.53	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:14	172.22.0.46	172.22.0.46	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:46:13	APPWT01.city.dallastx.co	172.16.19.11	Controller	Tridium	Jace Series Building Con	n.a.
□	ooo	0	10:46:13	172.16.44.239	172.16.44.239	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:12	172.30.128.39	172.30.128.39	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:11	172.16.44.157	172.16.44.157	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:11	172.22.0.142	172.22.0.142	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:46:10	172.30.68.61	172.30.68.61	Computer	n.a.	n.a.	n.a.
□	ooo	0	10:46:08	172.30.27.37	172.30.27.37	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:46:08	172.16.12.171	172.16.12.171	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:08	172.30.27.30	172.30.27.30	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:07	172.22.1.144	172.22.1.144	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:46:07	10.65.34.20	10.65.34.20	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:06	Virtual Machine	172.16.45.38	Computer	VMware	Virtual Machine	n.a.
□	ooo	0	10:46:05	172.16.44.207	172.16.44.207	Other	n.a.	n.a.	n.a.
□	ooo	0	10:46:01	10.64.9.29	10.64.9.29	Other	n.a.	n.a.	n.a.
□	ooo	0	10:45:58	172.22.0.115	172.22.0.115	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:45:57	172.16.128.147	172.16.128.147	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:45:54	172.18.121.44	172.18.121.44	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:45:53	172.16.12.79	172.16.12.79	Computer	n.a.	n.a.	Windows 7
□	ooo	0	10:45:49	172.30.121.33	172.30.121.33	IT device	n.a.	n.a.	n.a.
□	ooo	0	10:45:48	172.19.16.46	172.19.16.46	Other	n.a.	n.a.	n.a.

1 to **25** of **more** |< < Page **1** of **more** >

Figure 22. Detailed list page

Site

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

Type

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

Vendor

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

OS or firmware

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

Columns

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

Refresh

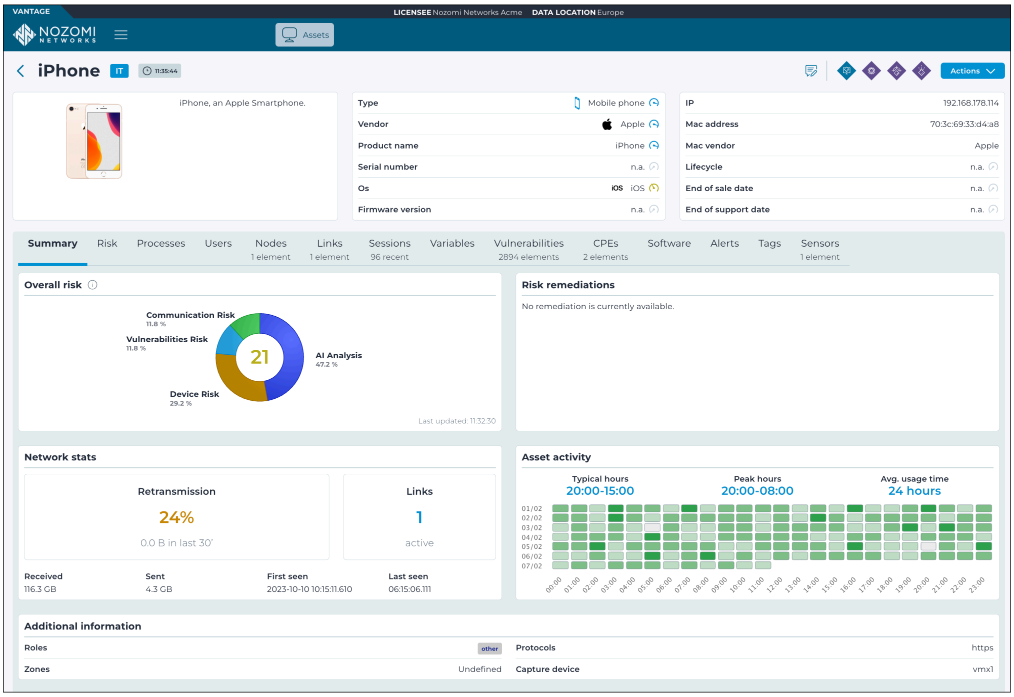
The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

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

Details page

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



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

iPhone IT 11:35:44

iPhone, an Apple Smartphone.

Type	Mobile phone
Vendor	Apple
Product name	iPhone
Serial number	n.a.
Os	iOS
Firmware version	n.a.

IP	192.168.178.114
Mac address	70:3c:69:33:d4:a8
Mac vendor	Apple
Lifecycle	n.a.
End of sale date	n.a.
End of support date	n.a.

Nodes 1 element · Links 1 element · Sessions 96 recent · Vulnerabilities 2894 elements · CPEs 2 elements · Sensors 1 element

Overall risk

Last updated: 11:32:30

Risk remediations

No remediation is currently available.

Network stats

Retransmission 24% 0.0 B in last 30'

Links 1 active

Received	Sent	First seen	Last seen
116.3 GB	4.3 GB	2023-10-10 10:15:11.610	06:15:06.111

Asset activity

Typical hours	Peak hours	Avg. usage time
20:00-15:00	20:00-08:00	24 hours

Additional information

Roles	other	Protocols	https
Zones	Undefined	Capture device	vmx1

Figure 23. Details page

Actions dropdown

This dropdown gives you access to these actions:

- Delete (on page 108)
- Export (on page 109) (bulk option only)
- Create Asset Rule From This Asset (on page 111)

Tabs

The details page has these tabs:

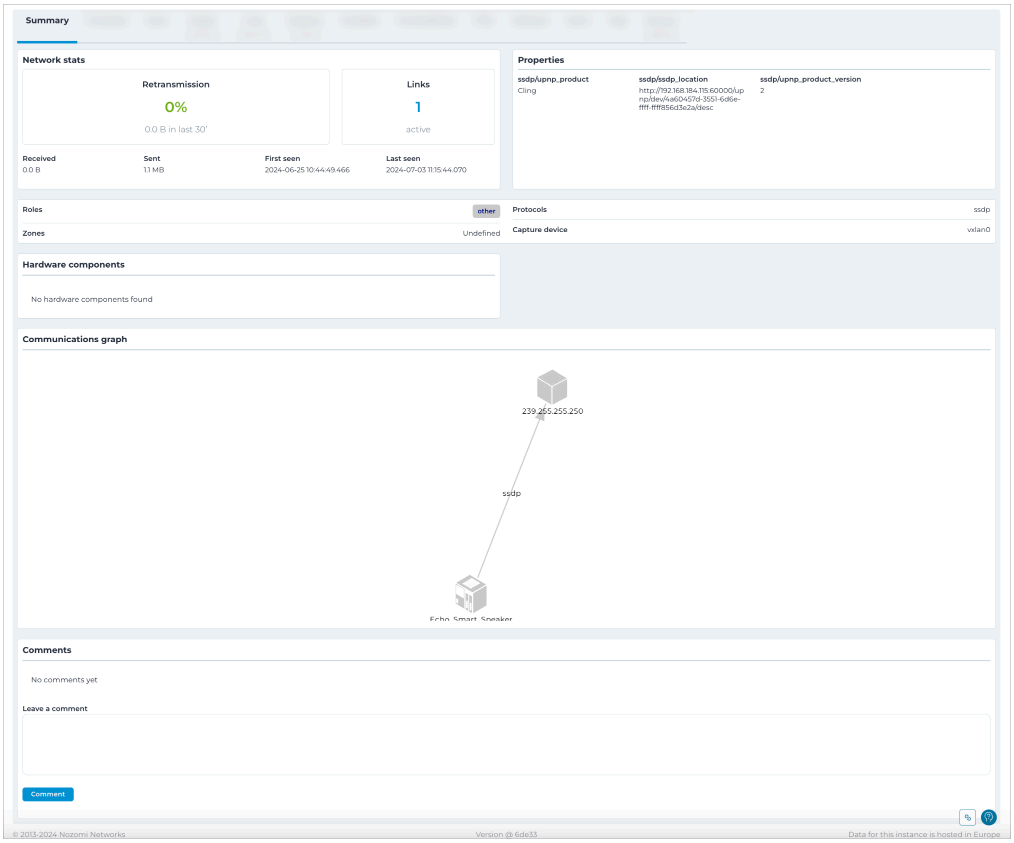
- Summary tab (on page 90)
- Risk tab (on page 91)
- Processes tab (on page 93)
- Users tab (on page 94)
- Nodes tab (on page 95)
- Links tab (on page 96)
- Sessions tab (on page 97)
- Variables tab (on page 98)
- Vulnerabilities tab (on page 99)
- CPEs tab (on page 100)
- Software tab (on page 101)
- Alerts tab (on page 102)
- Tags tab (on page 103)
- Sensors tab (on page 106)

Related information

Open the details page (on page 112)

Summary tab

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



Network stats

Retransmission
0%
0.0 B in last 30'

Links
1
active

Received	Sent	First seen	Last seen
0.0 B	1.1 MB	2024-06-25 10:44:49.466	2024-07-03 11:15:44.070

Properties

ssdp/upnp_product	ssdp/ssdp_location	ssdp/upnp_product_version
Cling	http://192.168.184.115:60000/upnp/dev/4a60457d-3551-6d6e-ffff-ffff856d3e2a/desc	2

Roles	other
Zones	Undefined
Protocols	ssdp
Capture device	vxlan0

Hardware components

No hardware components found

Communications graph

Comments

No comments yet

Leave a comment

© 2013-2024 Nozomi Networks Version @ 6de33 Data for this instance is hosted in Europe

Figure 24. 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

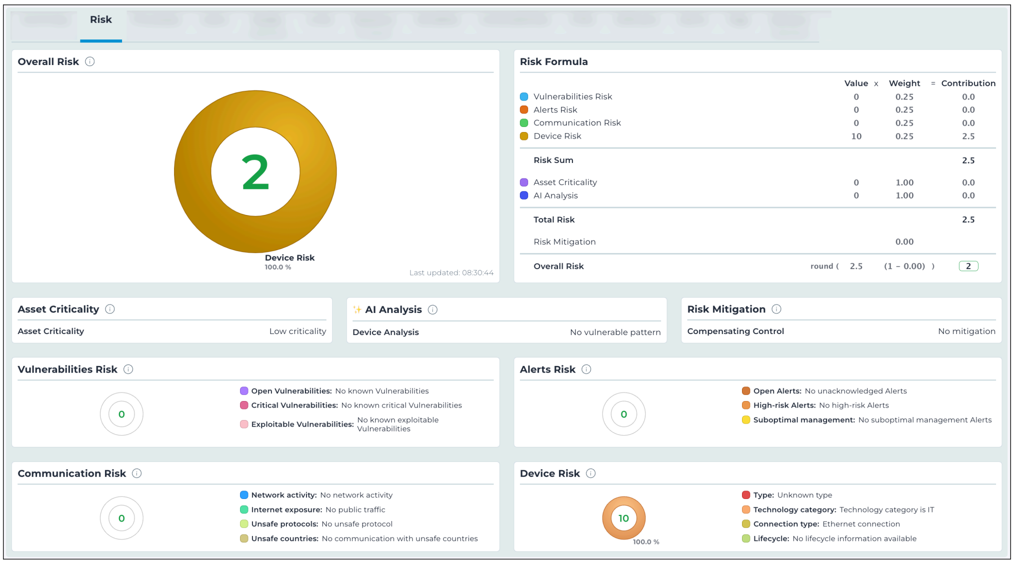
This section shows the same links as shown in the Links tab (on page 96) for this asset.

Comments

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

Risk tab

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



Overall Risk ⓘ

Last updated: 08:30:44

Risk Formula

	Value	x	Weight	=	Contribution
🟦 Vulnerabilities Risk	0		0.25		0.0
🟧 Alerts Risk	0		0.25		0.0
🟩 Communication Risk	0		0.25		0.0
🟨 Device Risk	10		0.25		2.5
Risk Sum					**2.5**
🟪 Asset Criticality	0		1.00		0.0
🟦 AI Analysis	0		1.00		0.0
Total Risk					**2.5**
Risk Mitigation			0.00		
Overall Risk	round (2.5		(1 − 0.00))		2

Asset Criticality ⓘ

Asset Criticality Low criticality

✨ **AI Analysis** ⓘ

Device Analysis No vulnerable pattern

Risk Mitigation ⓘ

Compensating Control No mitigation

Vulnerabilities Risk ⓘ

- **Open Vulnerabilities:** No known Vulnerabilities
- **Critical Vulnerabilities:** No known critical Vulnerabilities
- **Exploitable Vulnerabilities:** No known exploitable Vulnerabilities

Alerts Risk ⓘ

- **Open Alerts:** No unacknowledged Alerts
- **High-risk Alerts:** No high-risk Alerts
- **Suboptimal management:** No suboptimal management Alerts

Communication Risk ⓘ

- **Network activity:** No network activity
- **Internet exposure:** No public traffic
- **Unsafe protocols:** No unsafe protocol
- **Unsafe countries:** No communication with unsafe countries

Device Risk ⓘ

- **Type:** Unknown type
- **Technology category:** Technology category is IT
- **Connection type:** Ethernet connection
- **Lifecycle:** No lifecycle information available

Figure 25. Risk tab

Overall Risk

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

Risk Formula

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

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

Asset Criticality

Indicates the criticality level of the asset in the network.

AI Analysis

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

Risk Mitigation

Displays all compensating controls applied to mitigate risk.

Vulnerabilities Risk

Summarizes detected vulnerabilities, categorized as:

- Open Vulnerabilities
- Critical Vulnerabilities
- Exploitable Vulnerabilities

Alerts Risk

Lists active security alerts impacting the asset.

Communication Risk

Analyzes network activity, including:

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

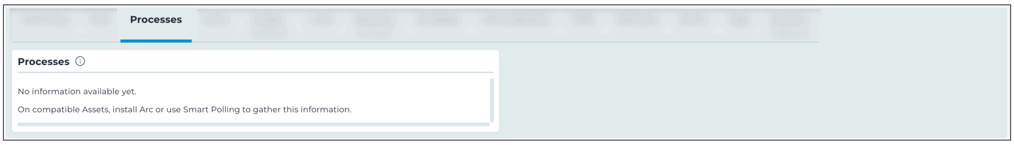
Device Risk

Assesses risk based on device attributes, such as:

- Technology category
- Connection type
- Lifecycle status

Processes tab

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



Processes ⓘ

No information available yet.

On compatible Assets, install Arc or use Smart Polling to gather this information.

Figure 26. Processes tab

Columns

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

Refresh

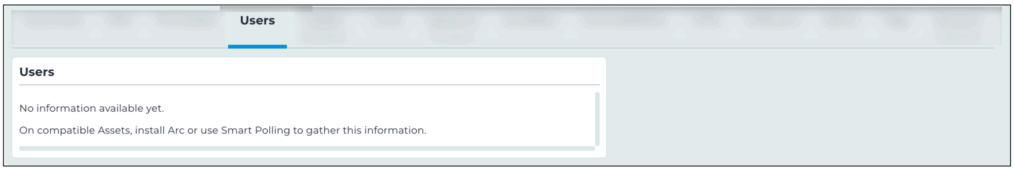
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



Users

No information available yet.

On compatible Assets, install Arc or use Smart Polling to gather this information.

Figure 27. Users tab

Columns

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

Refresh

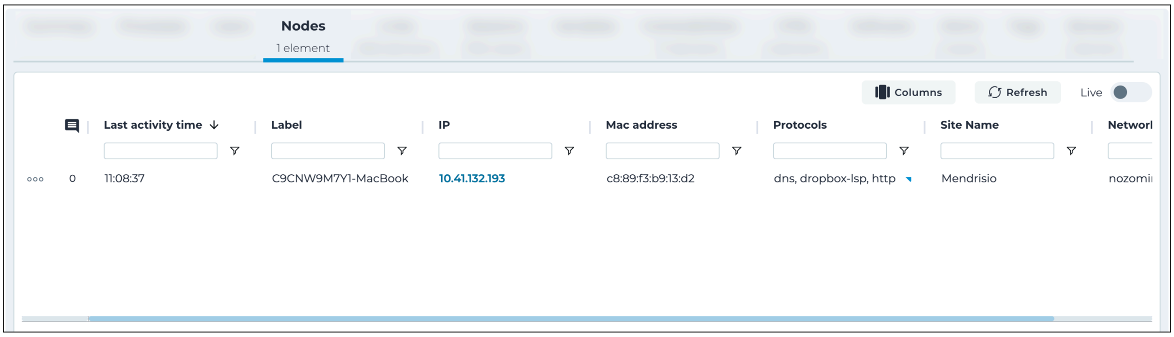
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



		Last activity time	Label	IP	Mac address	Protocols	Site Name	Networ
○○○	0	11:08:37	C9CNW9M7Y1-MacBook	10.41.132.193	c8:89:f3:b9:13:d2	dns, dropbox-lsp, http	Mendrisio	nozomi

Columns

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

Refresh

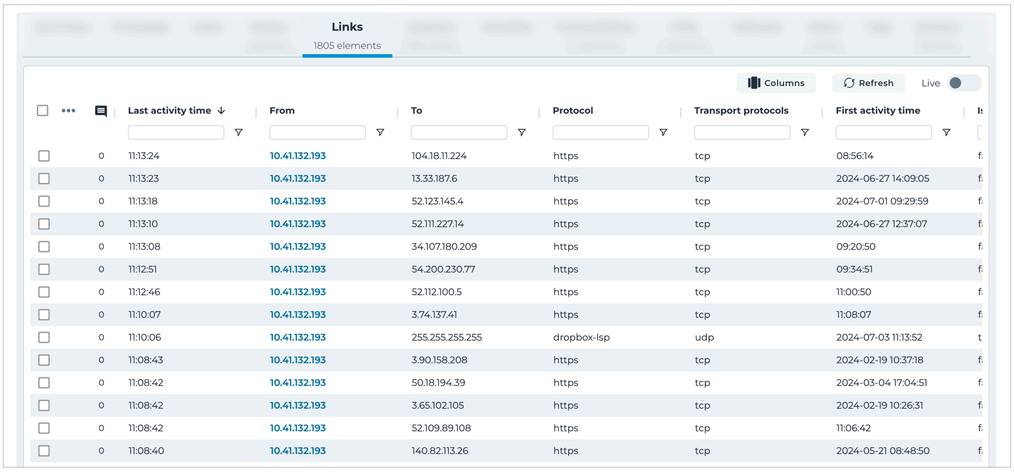
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



□	•••		Last activity time ↓	From	To	Protocol	Transport protocols	First activity time	I
□		0	11:13:24	10.41.132.193	104.18.11.224	https	tcp	08:56:14	f
□		0	11:13:23	10.41.132.193	13.33.187.6	https	tcp	2024-06-27 14:09:05	f
□		0	11:13:18	10.41.132.193	52.123.145.4	https	tcp	2024-07-01 09:29:59	f
□		0	11:13:10	10.41.132.193	52.111.227.14	https	tcp	2024-06-27 12:37:07	f
□		0	11:13:08	10.41.132.193	34.107.180.209	https	tcp	09:20:50	f
□		0	11:12:51	10.41.132.193	54.200.230.77	https	tcp	09:34:51	f
□		0	11:12:46	10.41.132.193	52.112.100.5	https	tcp	11:00:50	f
□		0	11:10:07	10.41.132.193	3.74.137.41	https	tcp	11:08:07	f
□		0	11:10:06	10.41.132.193	255.255.255.255	dropbox-lsp	udp	2024-07-03 11:13:52	t
□		0	11:08:43	10.41.132.193	3.90.158.208	https	tcp	2024-02-19 10:37:18	f
□		0	11:08:42	10.41.132.193	50.18.194.39	https	tcp	2024-03-04 17:04:51	f
□		0	11:08:42	10.41.132.193	3.65.102.105	https	tcp	2024-02-19 10:26:31	f
□		0	11:08:42	10.41.132.193	52.109.89.108	https	tcp	11:06:42	f
□		0	11:08:40	10.41.132.193	140.82.113.26	https	tcp	2024-05-21 08:48:50	f

Figure 28. Links tab

Columns

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

Refresh

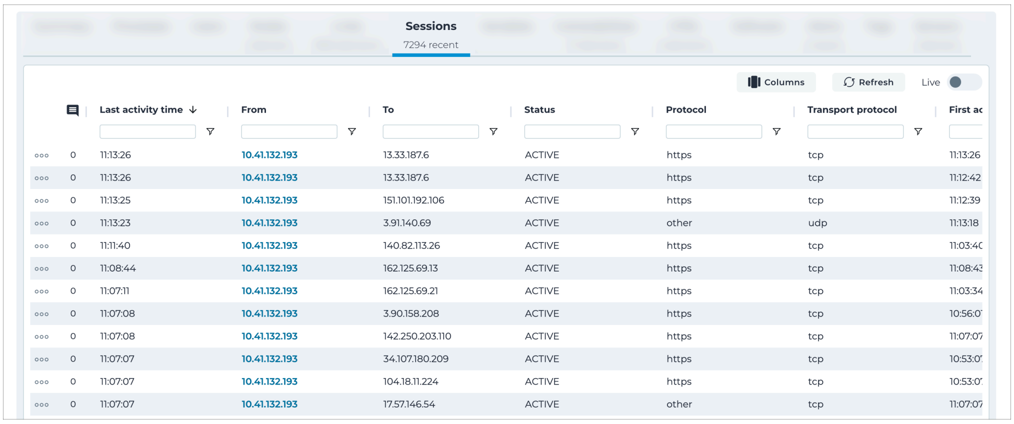
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



		Last activity time ↓	From	To	Status	Protocol	Transport protocol	First ac
ooo	0	11:13:26	10.41.132.193	13.33.187.6	ACTIVE	https	tcp	11:13:26
ooo	0	11:13:26	10.41.132.193	13.33.187.6	ACTIVE	https	tcp	11:12:42
ooo	0	11:13:25	10.41.132.193	151.101.192.106	ACTIVE	https	tcp	11:12:39
ooo	0	11:13:23	10.41.132.193	3.91.140.69	ACTIVE	other	udp	11:13:18
ooo	0	11:11:40	10.41.132.193	140.82.113.26	ACTIVE	https	tcp	11:03:4
ooo	0	11:08:44	10.41.132.193	162.125.69.13	ACTIVE	https	tcp	11:08:4
ooo	0	11:07:11	10.41.132.193	162.125.69.21	ACTIVE	https	tcp	11:03:34
ooo	0	11:07:08	10.41.132.193	3.90.158.208	ACTIVE	https	tcp	10:56:0
ooo	0	11:07:08	10.41.132.193	142.250.203.110	ACTIVE	https	tcp	11:07:07
ooo	0	11:07:07	10.41.132.193	34.107.180.209	ACTIVE	https	tcp	10:53:0
ooo	0	11:07:07	10.41.132.193	104.18.11.224	ACTIVE	https	tcp	10:53:0
ooo	0	11:07:07	10.41.132.193	17.57.146.54	ACTIVE	other	tcp	11:07:07

Figure 29. Sessions tab

Columns

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

Refresh

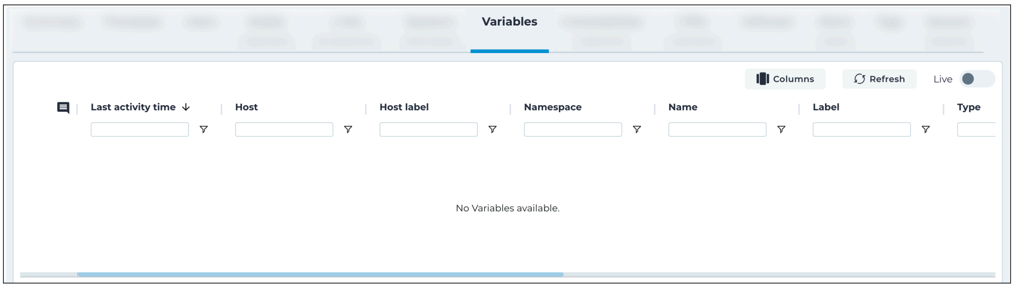
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



No Variables available.

Figure 30. Variables tab

Columns

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

Refresh

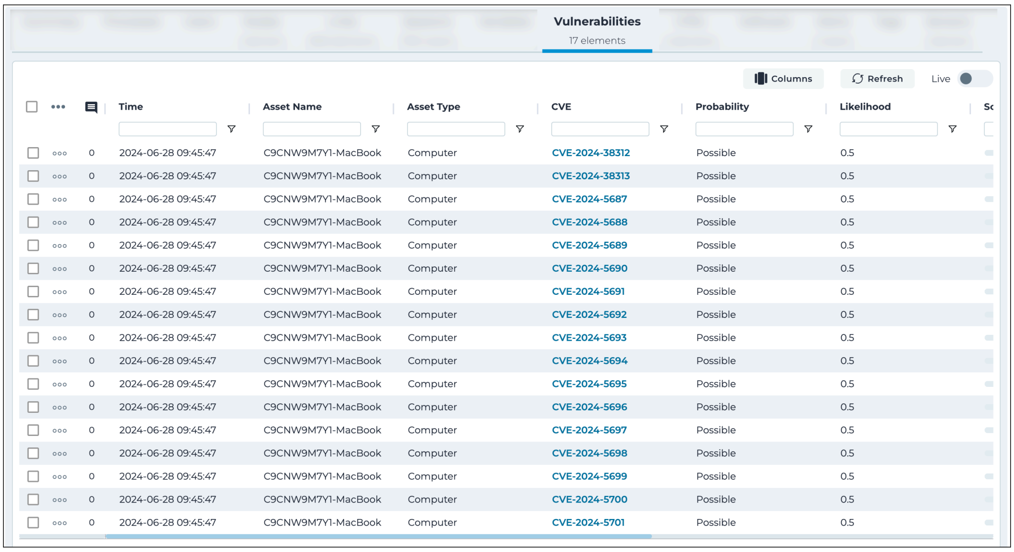
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



□	•••		Time	Asset Name	Asset Type	CVE	Probability	Likelihood	Sc
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-38312	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-38313	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5687	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5688	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5689	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5690	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5691	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5692	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5693	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5694	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5695	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5696	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5697	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5698	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5699	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5700	Possible	0.5	
□	○○○	0	2024-06-28 09:45:47	C9CNW9M7Y1-MacBook	Computer	CVE-2024-5701	Possible	0.5	

Figure 31. Vulnerabilities tab

Columns

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

Refresh

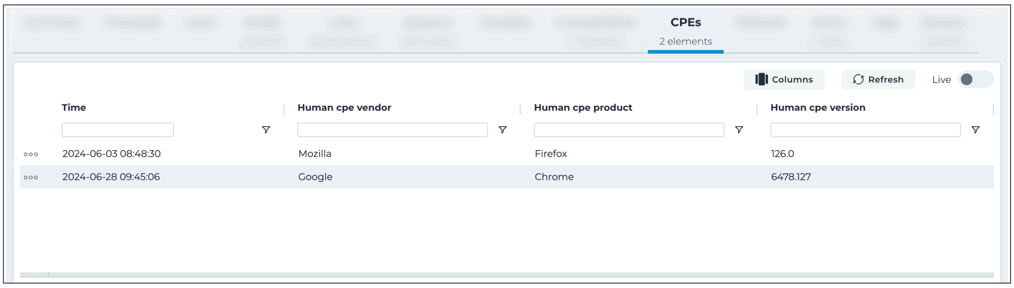
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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 32. CPE tab

Columns

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

Refresh

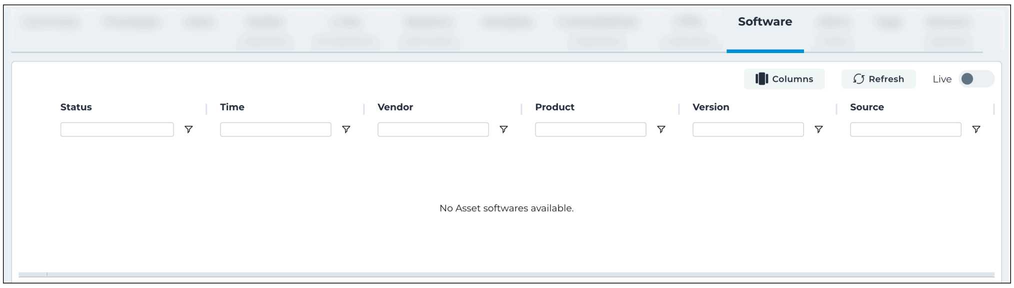
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



Status	Time	Vendor	Product	Version	Source

No Asset softwares available.

Figure 33. Software tab

Columns

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

Refresh

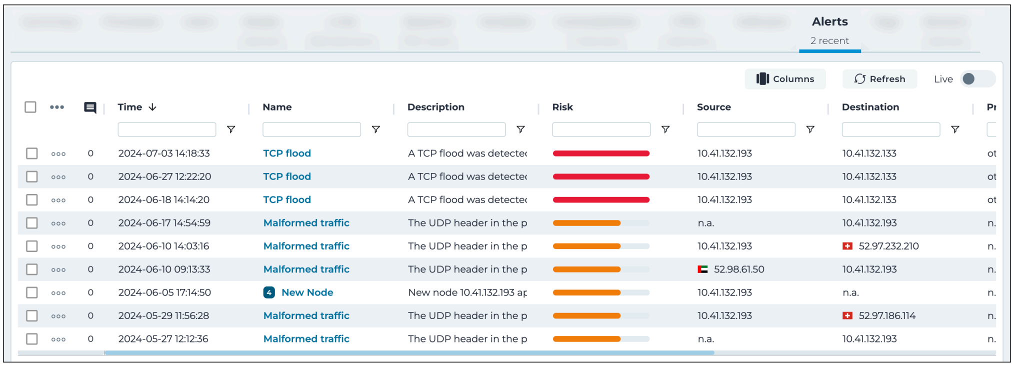
The **Refresh** icon lets you immediately refresh the current view.

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.*



☐	•••		Time ↓	Name	Description	Risk	Source	Destination	Pr
☐	○○○	0	2024-07-03 14:18:33	TCP flood	A TCP flood was detecte	🟥	10.41.132.193	10.41.132.133	ot
☐	○○○	0	2024-06-27 12:22:20	TCP flood	A TCP flood was detecte	🟥	10.41.132.193	10.41.132.133	ot
☐	○○○	0	2024-06-18 14:14:20	TCP flood	A TCP flood was detecte	🟥	10.41.132.193	10.41.132.133	ot
☐	○○○	0	2024-06-17 14:54:59	Malformed traffic	The UDP header in the p	🟧	n.a.	10.41.132.193	n.
☐	○○○	0	2024-06-10 14:03:16	Malformed traffic	The UDP header in the p	🟧	10.41.132.193	52.97.232.210	n.
☐	○○○	0	2024-06-10 09:13:33	Malformed traffic	The UDP header in the p	🟧	52.98.61.50	10.41.132.193	n.
☐	○○○	0	2024-06-05 17:14:50	4 New Node	New node 10.41.132.193 ap	🟧	10.41.132.193	n.a.	n.
☐	○○○	0	2024-05-29 11:56:28	Malformed traffic	The UDP header in the p	🟧	10.41.132.193	52.97.186.114	n.
☐	○○○	0	2024-05-27 12:12:36	Malformed traffic	The UDP header in the p	🟧	n.a.	10.41.132.193	n.

Figure 34. Alerts tab

Columns

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

Refresh

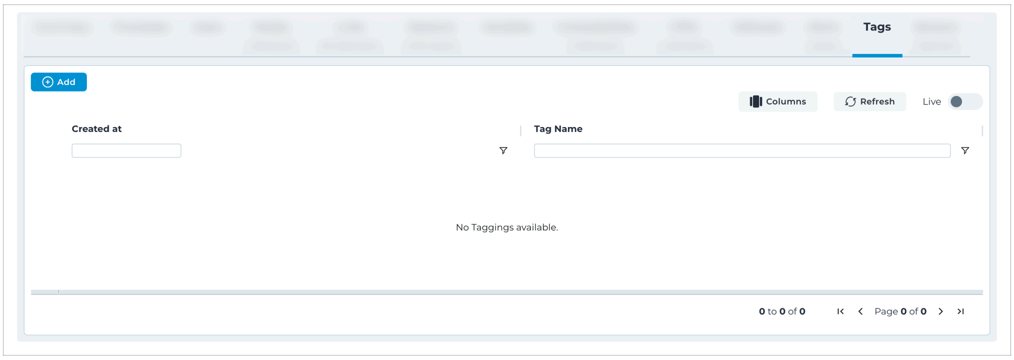
The **Refresh** ↻ icon lets you immediately refresh the current view.

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.*



No Taggings available.

0 to 0 of 0 Page 0 of 0

Figure 35. Tags tab

Add new

This button lets you add a new tag (on page 104) 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 112) 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 103)

Delete a tag from an asset (on page 105)

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 112) 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.

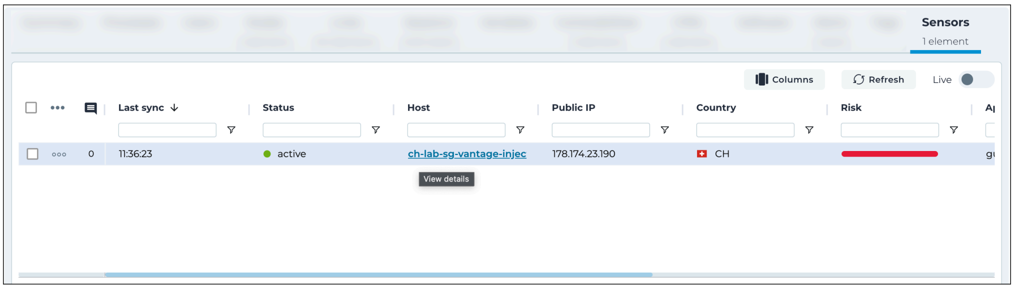
Related information

Tags tab (on page 103)

Add a tag to an asset (on page 104)

Sensors tab

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



□	•••		Last sync ↓	Status	Host	Public IP	Country	Risk	A
□	○○○	0	11:36:23	● active	ch-lab-sg-vantage-injec	178.174.23.190	CH		g

Figure 36. Sensors tab

Columns

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

Refresh

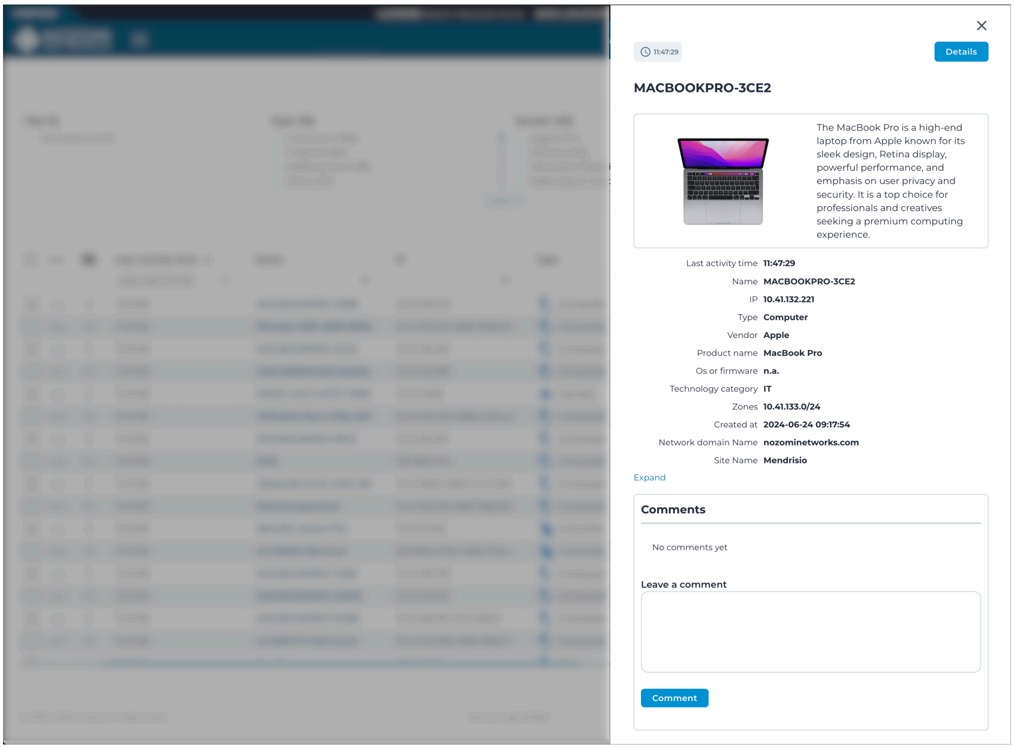
The **Refresh** icon lets you immediately refresh the current view.

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.



MACBOOKPRO-3CE2

The MacBook Pro is a high-end laptop from Apple known for its sleek design, Retina display, powerful performance, and emphasis on user privacy and security. It is a top choice for professionals and creatives seeking a premium computing experience.

Last activity time	**11:47:29**
Name	**MACBOOKPRO-3CE2**
IP	**10.41.132.221**
Type	**Computer**
Vendor	**Apple**
Product name	**MacBook Pro**
Os or firmware	**n.a.**
Technology category	**IT**
Zones	**10.41.133.0/24**
Created at	**2024-06-24 09:17:54**
Network domain Name	**nozominetworks.com**
Site Name	**Mendrisio**

Comments

No comments yet

Leave a comment

Figure 37. Summary drawer

Details button

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

Summary

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

Comments

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

Related information

Open the summary drawer (on page 112)

Table interactions

Actions menu

Delete an asset

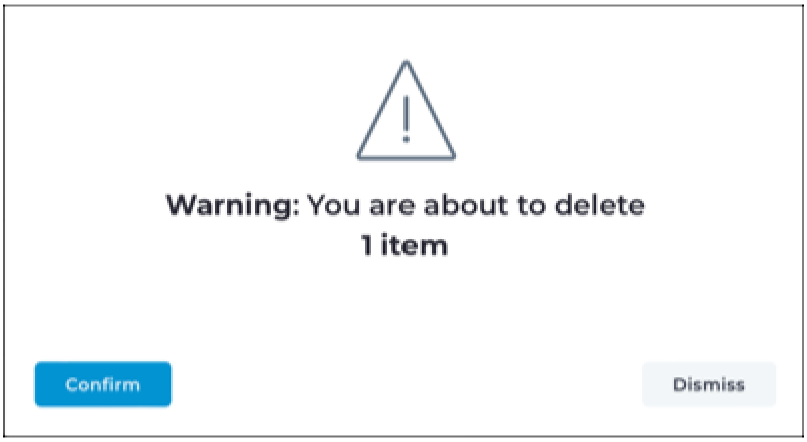
You can use the actions menu to delete an asset.

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**.



Warning: You are about to delete 1 item

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

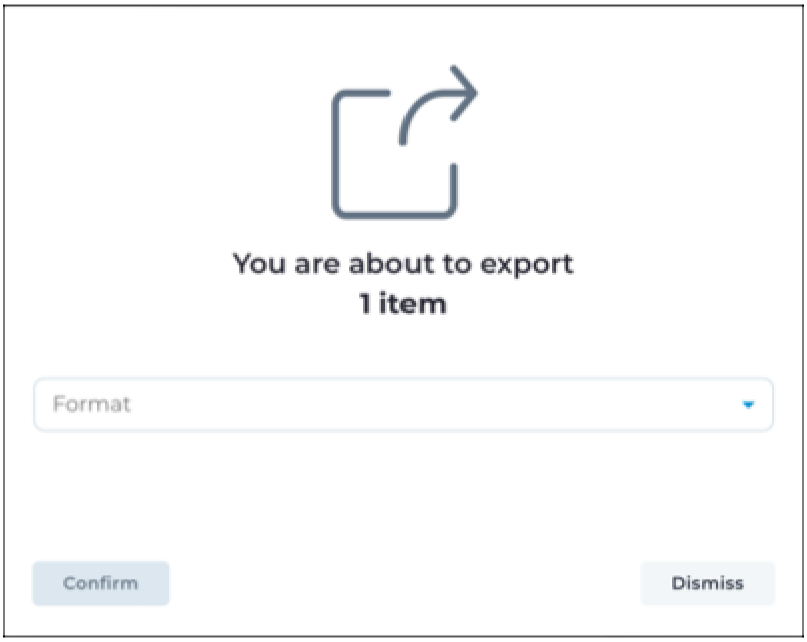
1. In the top navigation bar, select **Assets**.
2. Choose a method to open the actions menu.

   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**.

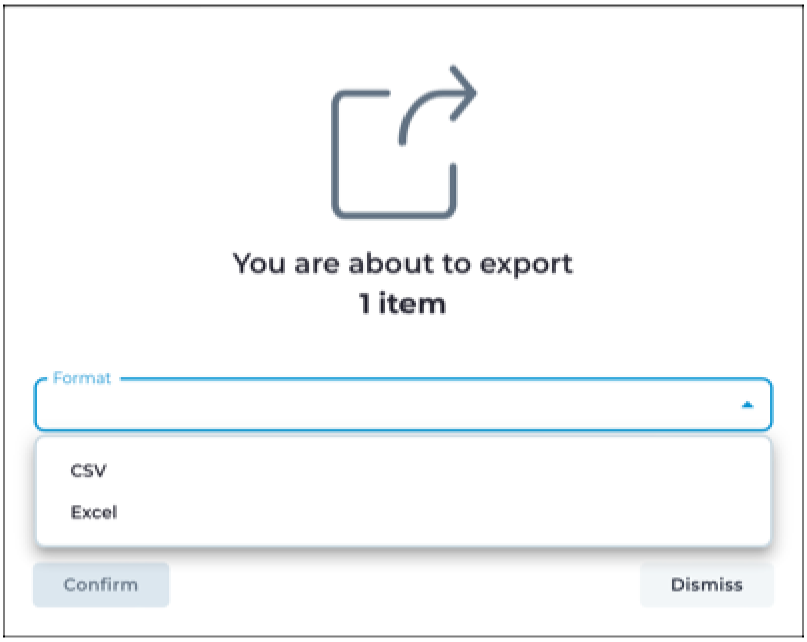
   

   You are about to export 1 item

   Result: The export dialog shows.
5. Select the **Format** dropdown.

   Result: A dialog shows.

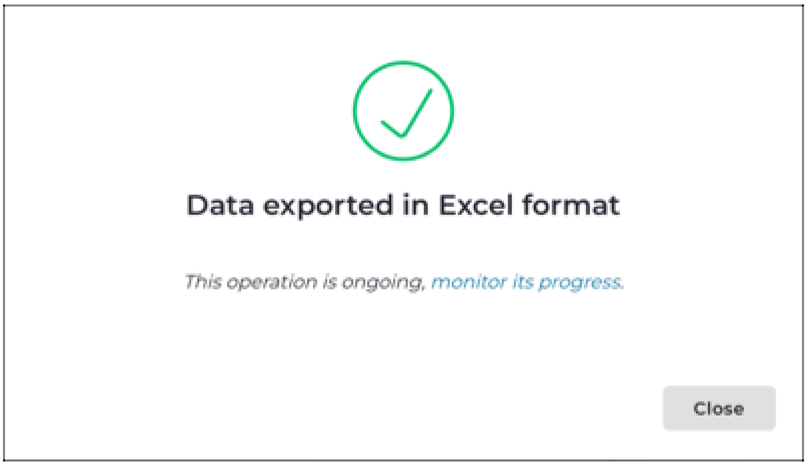
6. In the **Format** dropdown, select the format that you want to export.



7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.


Data exported in Excel format
This operation is ongoing, monitor its progress.
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.

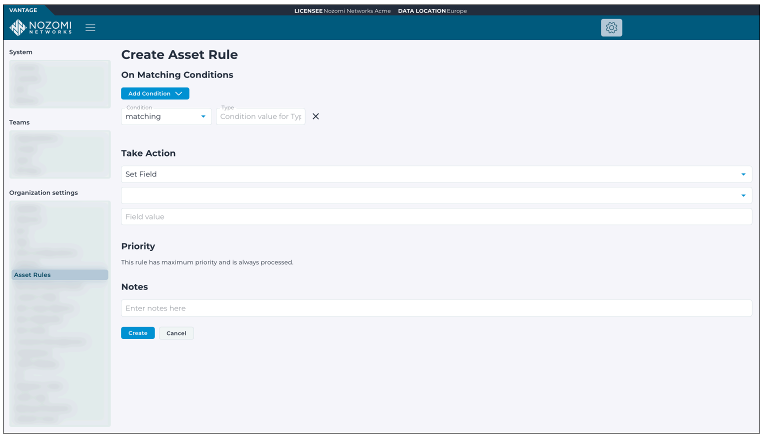
   Choose from:

   - 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.



Create Asset Rule

On Matching Conditions

Condition: matching

Type: Condition value for Typ

Take Action

Set Field

Field value

Priority

This rule has maximum priority and is always processed.

Notes

Enter notes here

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 88) opens.

Related information

Details page (on page 88)

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 107) opens.

Related information

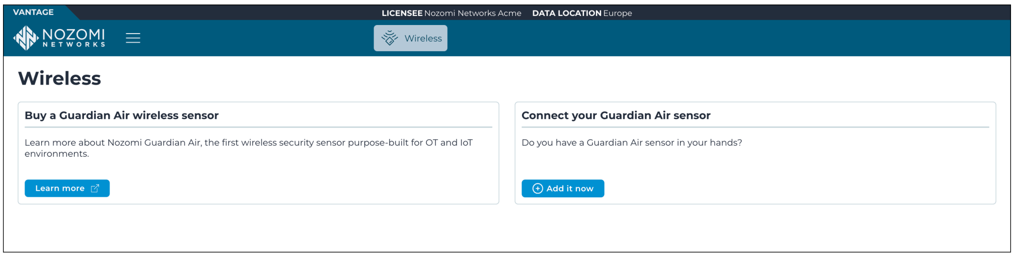
Summary drawer (on page 107)

Chapter 5. Wireless

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

First use

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



VANTAGE   **LICENSEE** Nozomi Networks Acme   **DATA LOCATION** Europe

Wireless

Buy a Guardian Air wireless sensor

Learn more about Nozomi Guardian Air, the first wireless security sensor purpose-built for OT and IoT environments.

Connect your Guardian Air sensor

Do you have a Guardian Air sensor in your hands?

Figure 38. Wireless page (before a Guardian Air sensor has been added)

Buy a Guardian Air wireless sensor

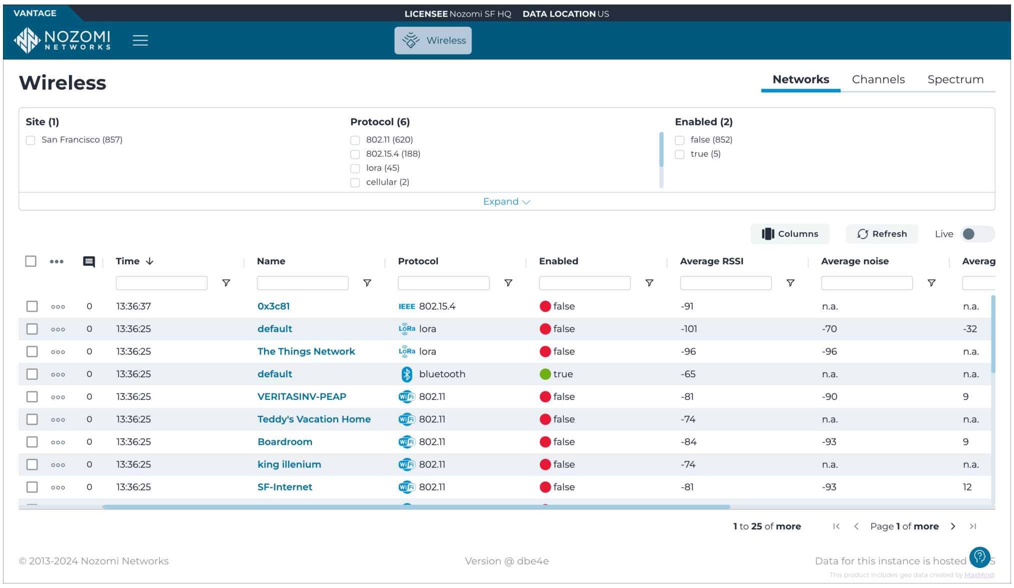
This section lets you buy your first Guardian Air sensor, and learn more about Guardian Air.

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.



VANTAGE   **LICENSEE** Nozomi SF HQ   **DATA LOCATION** US

Wireless

Site (1)
- □ San Francisco (857)

Protocol (6)
- □ 802.11 (620)
- □ 802.15.4 (188)
- □ lora (45)
- □ cellular (2)

Enabled (2)
- □ false (852)
- □ true (5)

□	•••		Time ↓	Name	Protocol	Enabled	Average RSSI	Average noise	Averag
□	○○○	0	13:36:37	0x3c81	IEEE 802.15.4	● false	-91	n.a.	n.a.
□	○○○	0	13:36:25	default	LoRa lora	● false	-101	-70	-32
□	○○○	0	13:36:25	The Things Network	LoRa lora	● false	-96	-96	n.a.
□	○○○	0	13:36:25	default	bluetooth	● true	-65	n.a.	n.a.
□	○○○	0	13:36:25	VERITASINV-PEAP	802.11	● false	-81	-90	9
□	○○○	0	13:36:25	Teddy's Vacation Home	802.11	● false	-74	n.a.	n.a.
□	○○○	0	13:36:25	Boardroom	802.11	● false	-84	-93	9
□	○○○	0	13:36:25	king illenium	802.11	● false	-74	n.a.	n.a.
□	○○○	0	13:36:25	SF-Internet	802.11	● false	-81	-93	12

1 to **25** of **more**   Page **1** of **more**

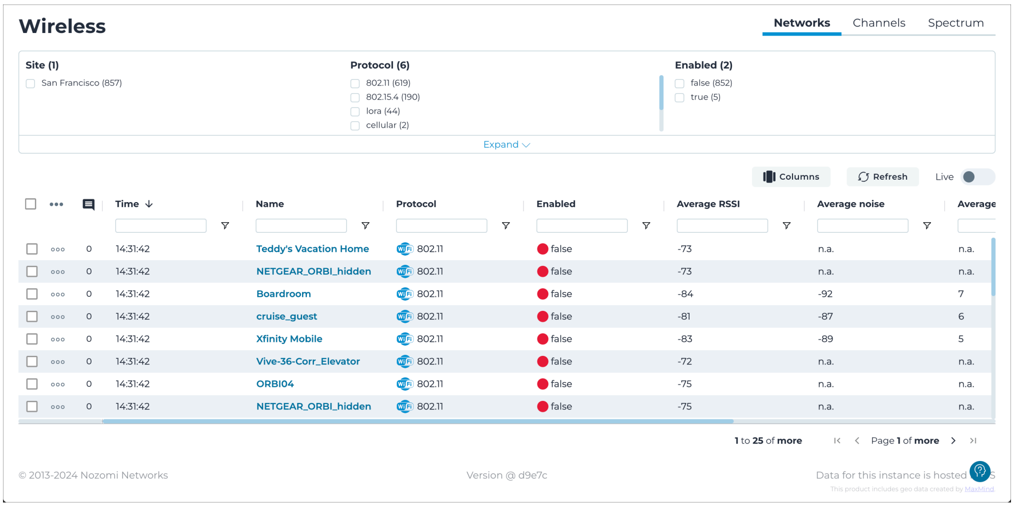
© 2013-2024 Nozomi Networks   Version @ dbe4e   Data for this instance is hosted S

This product includes geo data created by MaxMind.

Figure 39. 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.*



Site (1)
□ San Francisco (857)

Protocol (6)
□ 802.11 (619)
□ 802.15.4 (190)
□ lora (44)
□ cellular (2)

Enabled (2)
□ false (852)
□ true (5)

□	•••		Time ↓	Name	Protocol	Enabled	Average RSSI	Average noise	Average
□	∘∘∘	0	14:31:42	Teddy's Vacation Home	802.11	● false	-73	n.a.	n.a.
□	∘∘∘	0	14:31:42	NETGEAR_ORBI_hidden	802.11	● false	-73	n.a.	n.a.
□	∘∘∘	0	14:31:42	Boardroom	802.11	● false	-84	-92	7
□	∘∘∘	0	14:31:42	cruise_guest	802.11	● false	-81	-87	6
□	∘∘∘	0	14:31:42	Xfinity Mobile	802.11	● false	-83	-89	5
□	∘∘∘	0	14:31:42	Vive-36-Corr_Elevator	802.11	● false	-72	n.a.	n.a.
□	∘∘∘	0	14:31:42	ORBI04	802.11	● false	-75	n.a.	n.a.
□	∘∘∘	0	14:31:42	NETGEAR_ORBI_hidden	802.11	● false	-75	n.a.	n.a.

1 to **25** of **more** Page **1** of **more**

© 2013-2024 Nozomi Networks Version @ d9e7c Data for this instance is hosted S
This product includes geo data created by MaxMind.

Figure 40. 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.

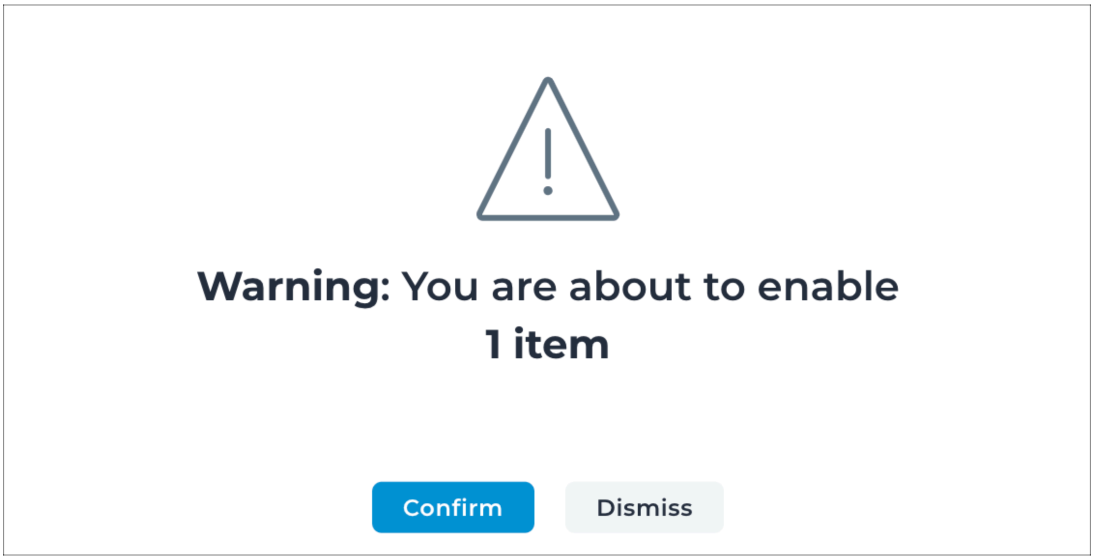
   Choose from:

   - 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**.



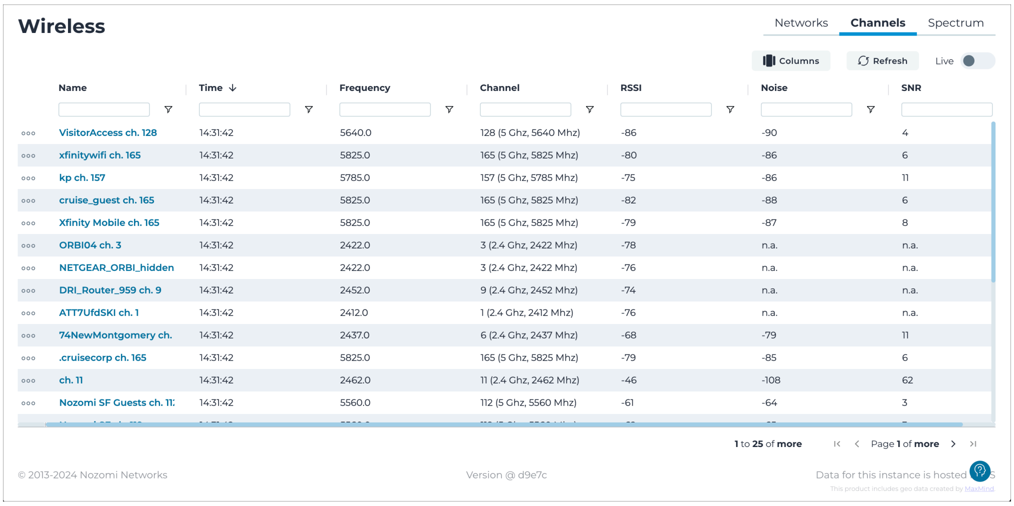
Warning: You are about to enable 1 item

Results

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

Channels

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



	Name	Time ↓	Frequency	Channel	RSSI	Noise	SNR
ooo	VisitorAccess ch. 128	14:31:42	5640.0	128 (5 Ghz, 5640 Mhz)	-86	-90	4
ooo	xfinitywifi ch. 165	14:31:42	5825.0	165 (5 Ghz, 5825 Mhz)	-80	-86	6
ooo	kp ch. 157	14:31:42	5785.0	157 (5 Ghz, 5785 Mhz)	-75	-86	11
ooo	cruise_guest ch. 165	14:31:42	5825.0	165 (5 Ghz, 5825 Mhz)	-82	-88	6
ooo	Xfinity Mobile ch. 165	14:31:42	5825.0	165 (5 Ghz, 5825 Mhz)	-79	-87	8
ooo	ORBI04 ch. 3	14:31:42	2422.0	3 (2.4 Ghz, 2422 Mhz)	-78	n.a.	n.a.
ooo	NETGEAR_ORBI_hidden	14:31:42	2422.0	3 (2.4 Ghz, 2422 Mhz)	-76	n.a.	n.a.
ooo	DRI_Router_959 ch. 9	14:31:42	2452.0	9 (2.4 Ghz, 2452 Mhz)	-74	n.a.	n.a.
ooo	ATT7UfdSKI ch. 1	14:31:42	2412.0	1 (2.4 Ghz, 2412 Mhz)	-76	n.a.	n.a.
ooo	74NewMontgomery ch.	14:31:42	2437.0	6 (2.4 Ghz, 2437 Mhz)	-68	-79	11
ooo	.cruisecorp ch. 165	14:31:42	5825.0	165 (5 Ghz, 5825 Mhz)	-79	-85	6
ooo	ch. 11	14:31:42	2462.0	11 (2.4 Ghz, 2462 Mhz)	-46	-108	62
ooo	Nozomi SF Guests ch. 11:	14:31:42	5560.0	112 (5 Ghz, 5560 Mhz)	-61	-64	3

1 to **25** of **more** Page **1** of **more**

© 2013-2024 Nozomi Networks Version @ d9e7c Data for this instance is hosted S

This product includes geo data created by MaxMind.

Figure 41. Channels page

Columns

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

Refresh

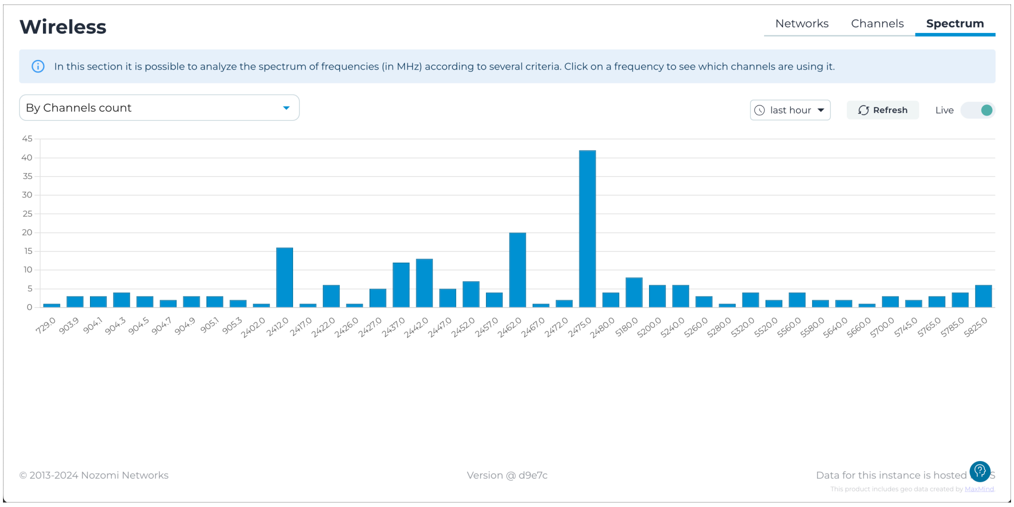
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



Wireless

In this section it is possible to analyze the spectrum of frequencies (in MHz) according to several criteria. Click on a frequency to see which channels are using it.

© 2013-2024 Nozomi Networks

Version @ d9e7c

Data for this instance is hosted

This product includes geo data created by MaxMind

Figure 42. 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

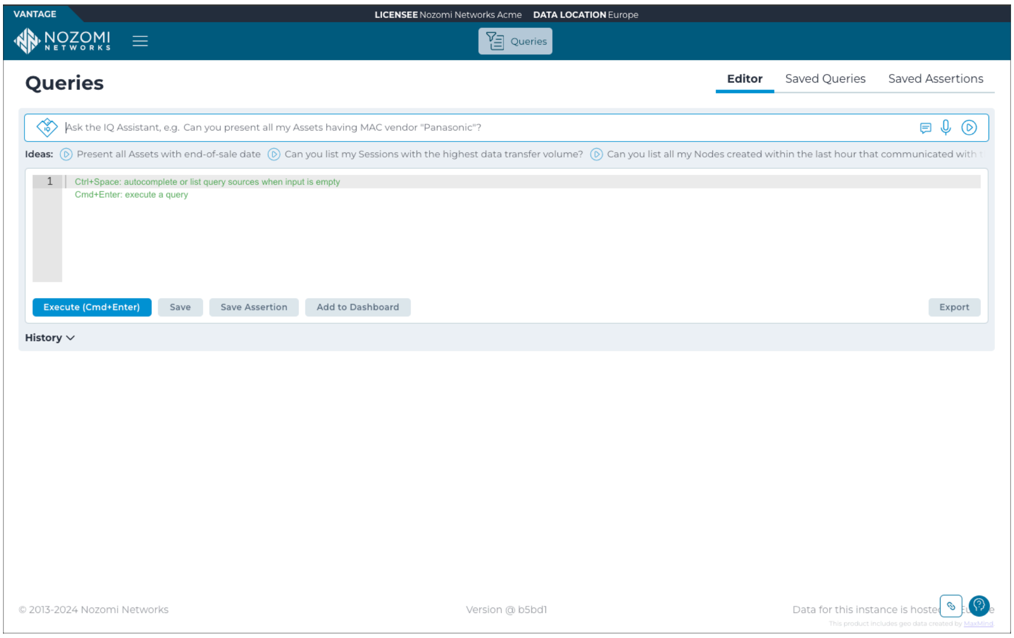
The **Refresh** icon lets you immediately refresh the current view.

Live

The live toggle lets you immediately refresh the graph.

Chapter 6. Queries

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


VANTAGE
LICENSEE Nozomi Networks Acme DATA LOCATION Europe
NOZOMI NETWORKS
Queries
Queries
Editor
Saved Queries
Saved Assertions
Ask the IQ Assistant, e.g. Can you present all my Assets having MAC vendor "Panasonic"?
Ideas:
Present all Assets with end-of-sale date
Can you list my Sessions with the highest data transfer volume?
Can you list all my Nodes created within the last hour that communicated with
Execute (Cmd+Enter)
Save
Save Assertion
Add to Dashboard
Export
History
© 2013-2024 Nozomi Networks
Version @ b5bd1
Data for this instance is hoste
This product includes geo data created by MaxMind

```
Ctrl+Space: autocomplete or list query sources when input is empty
Cmd+Enter: execute a query
```

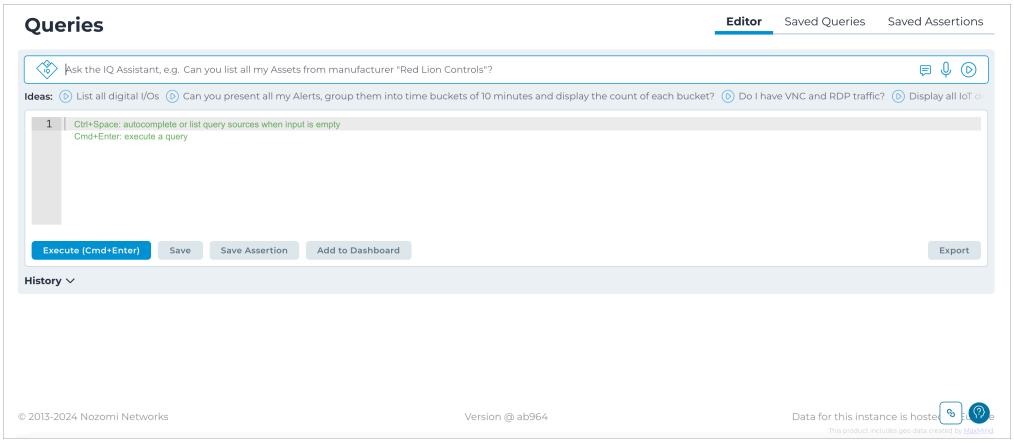
Figure 43. Queries page

The **Queries** page has these tabs:

- Editor (on page 124)
- Saved Queries (on page 126)
- Saved Assertions (on page 127)

Editor

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


Queries
Editor
Saved Queries
Saved Assertions
Ask the IQ Assistant, e.g. Can you list all my Assets from manufacturer "Red Lion Controls"?
Ideas:
List all digital I/Os
Can you present all my Alerts, group them into time buckets of 10 minutes and display the count of each bucket?
Do I have VNC and RDP traffic?
Display all IoT d
Execute (Cmd+Enter)
Save
Save Assertion
Add to Dashboard
Export
History
© 2013-2024 Nozomi Networks
Version @ ab964
Data for this instance is hoste
This product includes geo data created by MaxMind.

```
Ctrl+Space: autocomplete or list query sources when input is empty
Cmd+Enter: execute a query
```

Figure 44. Editor page

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

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

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

Execute

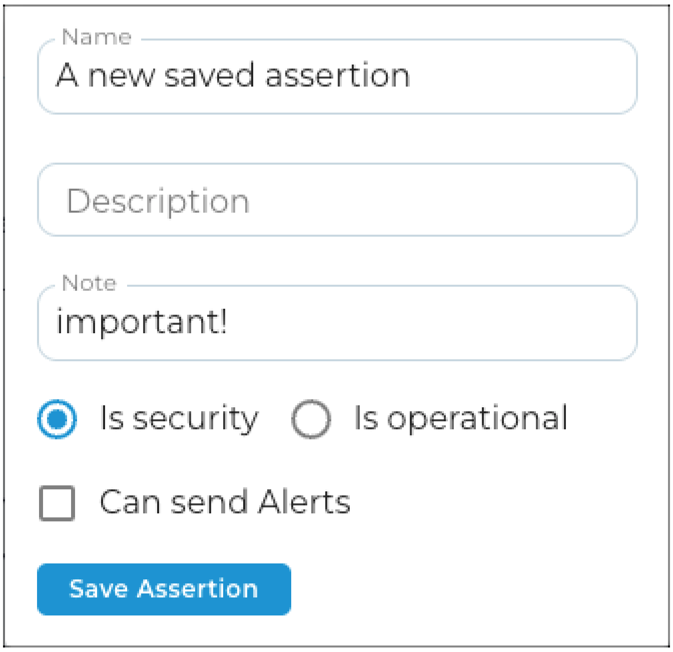
This button lets you execute the query. Alternatively, you can use the keyboard shortcut `Cmd + Enter`.

Save

This button lets you save the current query.

Save Assertion

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



Name
A new saved assertion

Description

Note
important!

● Is security ○ Is operational

□ Can send Alerts

Figure 45. Save Assertion dialog

Add to Dashboard

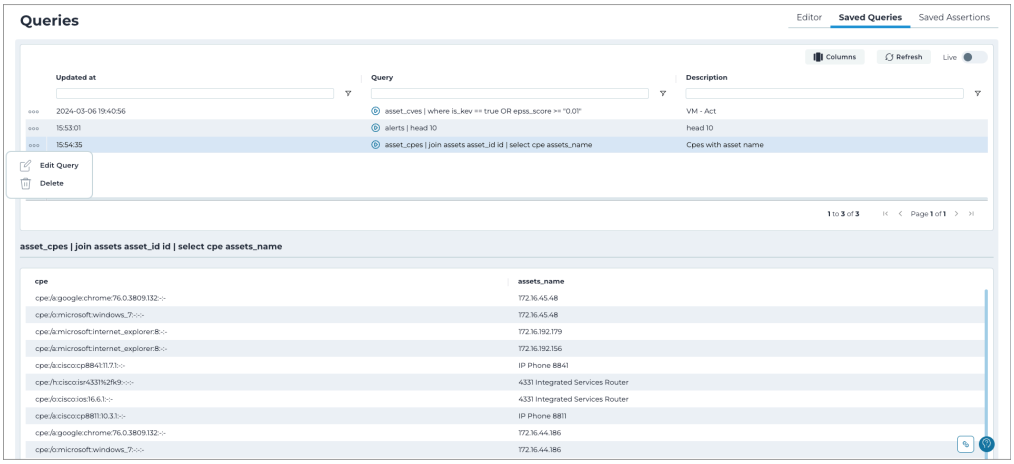
This button lets you add a widget to a dashboard.

Export

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

Saved Queries

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



Updated at	Query	Description
2024-03-06 19:40:56	asset_cves | where is_kev == true OR epss_score >= "0.01"	VM - Act
15:53:01	alerts | head 10	head 10
15:54:35	asset_cpes | join assets asset_id id | select cpe assets_name	Cpes with asset name

asset_cpes | join assets asset_id id | select cpe assets_name

cpe	assets_name
cpe:/a:google:chrome:76.0.3809.132:-:-	172.16.45.48
cpe:/o:microsoft:windows_7:-:-:-	172.16.45.48
cpe:/a:microsoft:internet_explorer:8:-:-	172.16.192.179
cpe:/a:microsoft:internet_explorer:8:-:-	172.16.192.156
cpe:/a:cisco:cp8841:11.7.1:-:-	IP Phone 8841
cpe:/h:cisco:isr4331%2fk9:-:-:-	4331 Integrated Services Router
cpe:/o:cisco:ios:16.6.1:-:-	4331 Integrated Services Router
cpe:/a:cisco:cp8811:10.3.1:-:-	IP Phone 8811
cpe:/a:google:chrome:76.0.3809.132:-:-	172.16.44.186
cpe:/o:microsoft:windows_7:-:-:-	172.16.44.186

Figure 46. Saved Queries page

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

The actions menu has these options:

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

Columns

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

Refresh

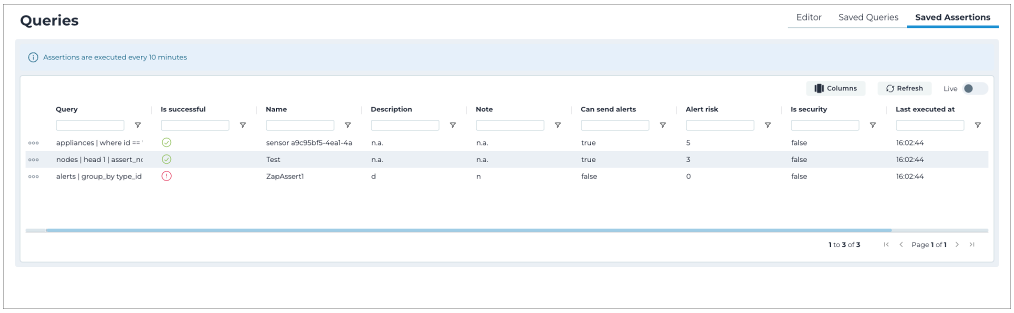
The **Refresh** ⟳ icon lets you immediately refresh the current view.

Live

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

Saved Assertions

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



Assertions are executed every 10 minutes

	Query	Is successful	Name	Description	Note	Can send alerts	Alert risk	Is security	Last executed at
ooo	appliances | where id == '	✓	sensor a9c95bf5-4ea1-4a	n.a.	n.a.	true	5	false	16:02:44
ooo	nodes | head 1 | assert_nc	✓	Test	n.a.	n.a.	true	3	false	16:02:44
ooo	alerts | group_by type_id	!	ZapAssert1	d	n	false	0	false	16:02:44

1 to 3 of 3 Page 1 of 1

Figure 47. Saved Assertions page

The actions menu has these options:

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

Columns

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

Refresh

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

Live

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

Execute a query

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

About this task

Note:

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

Note:

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

Note:

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

Procedure

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

   Choose from:

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

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

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

Commands

A list of example query commands.

assert_empty

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

Examples:

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

assert_not_empty

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

Examples:

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

bucket

Usage: `bucket <field> <range>`

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

Examples:

```
alerts | bucket risk 3
```

column

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

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

Examples:

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

Options:

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

Example: -color:7bc043

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

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

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

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

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

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

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

count

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

Examples:

```
links | count
```

exclude

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

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

Examples:

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

expand

Usage: `expand <array_field>`

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

Examples:

```
nodes | expand roles
```

gauge

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

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

Examples:

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

Options:

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

Example: -color:7bc043

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

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

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

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

grid

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

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

Examples:

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

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

Options:

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

Example: -color:7bc043

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

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

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

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

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

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

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

group_by

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

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

Examples:

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

```
nodes | group_by type
```

head

Usage: `head [N]`

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

Examples:

```
assets | head
```

```
alerts | head 200
```

history

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

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

Examples:

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

Options:

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

Example: -color:7bc043

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

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

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

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

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

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

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

join

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

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

Examples:

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

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

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

pie

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

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

Examples:

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

Options:

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

Example: -color:7bc043

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

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

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

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

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

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

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

reduce

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

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

Examples:

```
alerts | reduce risk avg
```

select

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

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

Examples:

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

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

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

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

Options:

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

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

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

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

sort

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

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

Examples:

```
assets | sort level
```

```
alerts | sort risk desc
```

uniq

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

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

Examples:

```
alerts | uniq type_id risk
```

value

Usage: `value <field> [option]`

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

Examples:

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

Options:

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

Example: -color:7bc043

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

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

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

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

where

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

Description: Filters the dataset by a specified criterion. `field1` and `field2` can be strings, fields, numbers or function calls. Some operators are specific to certain data types: * `in_subnet?` requires a subnet in CIDR notation as the right operand * `in?` and `!in?` works with JSON arrays as the right operand * `in_zones?` works with tiered zones and requires a tiered zone name as the right operand

Examples:

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

```
nodes | where is_public
```

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

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

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

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

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

```
alerts | where zone_src in_zones? "GlobalTieredZone"
```

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|number>)`

Description: Returns the difference in days between the timestamp `field` and the time of execution of the query. In the `where` clause the `days_ago(number)` syntax gives the best query performance.

Examples:

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

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

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

dist

Usage: `dist(<field1>,<field2>)`

Description: Returns the difference between `field1` and `field2`. The fields can also be literals.

Examples:

```
nodes | select dist(sent.bytes,received.bytes)
```

div

Usage: `div(<field1>,<field2>)`

Description: Returns the result of the arithmetic division of `field1` by `field2`. The fields can also be literals.

Examples:

```
nodes | select div(last_activity_time,"1000")
```

floor

Usage: `floor(<field>)`

Description: Returns the greatest integer less than or equal to the provided field.

Examples:

```
alerts | reduce risk avg | select floor(risk_avg)
```

```
assets | select div(risk, "10") | select floor(div)
```

format_time

Usage: `format_time(<time_field>, [format_string])`

Description: Returns a string representation of the time field formatted according to the format string or the default formatting string ('YYYY-MM-DD HH24:MI:SS') if none is specified. Accepted format patterns are:

- YYYY: year, 4 digits
- MM: month number, 2 digits
- DD: day of month, 2 digits
- HH12: hour of day, 01-12
- HH24: hour of day, 00-23
- MI: minute, 00-59
- SS: second, 00-59

Characters that can be used as separators are: -, :, whitespace

Examples:

```
sessions | select format_time(last_activity_time)
```

```
sessions | where last_activity_time > days_ago(7) | select
 format_time(last_activity_time, "YYYY-MM-DD") | group_by formatted
```

hours_ago

Usage: `hours_ago(<field|number>)`

Description: Returns the difference in seconds between the timestamp `field` and the time of execution of the query. In the `where` clause the `hours_ago(<number>)` syntax gives the best query performance.

Examples:

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

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

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

ipv4

Usage: `ipv4(<field>)`

Description: Returns a non-empty value if the field argument is an IPv4.

Examples:

```
nodes | select ipv4(ip)
```

```
nodes | where ipv4(ip) != ""
```

ipv6

Usage: `ipv6(<field>)`

Description: Returns a non-empty value if the field argument is an IPv6.

Examples:

```
nodes | select ipv6(ip)
```

```
nodes | where ipv6(ip) != ""
```

is_empty

Usage: `is_empty(<field>)`

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

Examples:

```
nodes | where !is_empty(label)
```

```
nodes | select protocols is_empty(protocols)
```

is_recent

Usage: `is_recent(<field>)`

Description: Returns true if `field` represents a time in the last 30 minutes, false otherwise.

Examples:

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

minutes_ago

Usage: `minutes_ago(<field|number>)`

Description: Returns the difference in minutes between the timestamp `field` and the time of execution of the query. In the `where` clause the `minutes_ago(<number>)` syntax gives the best query performance.

Examples:

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

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

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

mult

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

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

Examples:

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

parse

Usage: `parse(<field>,<regex>)`

Description: Extracts a new field from an existing field by leveraging a POSIX regular expression. The new field will have the value of the portion of text that matches the regular expression, if the regular expression contains parentheses the return value will be the portion of text matching the regular expression inside the parentheses.

Examples:

```
assets | select
 parse(properties,".sysDescr\.0.:\s.([a-zA-Z0-9\-\.\s]+).")->sysDescr
```

```
assets | select parse(name, "\d+")->number
```

round

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

Description: Rounds a number at the given `decimal_places`. If `decimal_places` is not specified the number will be rounded to the closer integer.

Examples:

```
alerts | reduce risk avg | select round(risk_avg,3)
```

```
alerts | reduce risk avg | select round(risk_avg)
```

seconds_ago

Usage: `seconds_ago(<field|number>)`

Description: Returns the difference in seconds between the timestamp `field` and the time of execution of the query. In the `where` clause the `seconds_ago(<number>)` syntax gives the best query performance.

Examples:

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

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

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

size

Usage: `size(<array_field>)`

Description: Returns the size of the `array_field`.

Examples:

```
nodes | where size(roles) > 1
```

split

Usage: `split(<field>,<splitter_string>,<index>)`

Description: Splits the value of `field` by `splitter_string` and returns the item at the `index` position, where `index` starts at 1.

Examples:

```
nodes | select split(mac_address,":",1)
```

to_epoch

Usage: `to_epoch(<timestamp_field>)`

Description: Converts a timestamp field into the numeric version suitable for queries.

Examples:

```
wireless_networks | bucket to_epoch(created_at) 3600000
```

Chapter 7. Vulnerabilities

*The **Vulnerabilities** page shows a list of all the vulnerabilities that Vantage has detected in your system. Vulnerabilities are weaknesses that reduce the security of your system and give threat actors an opportunity to exploit your system.*

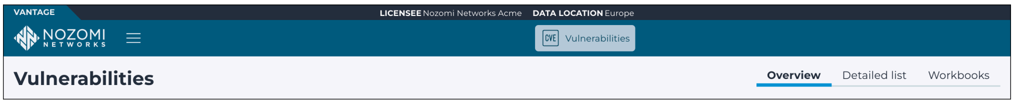


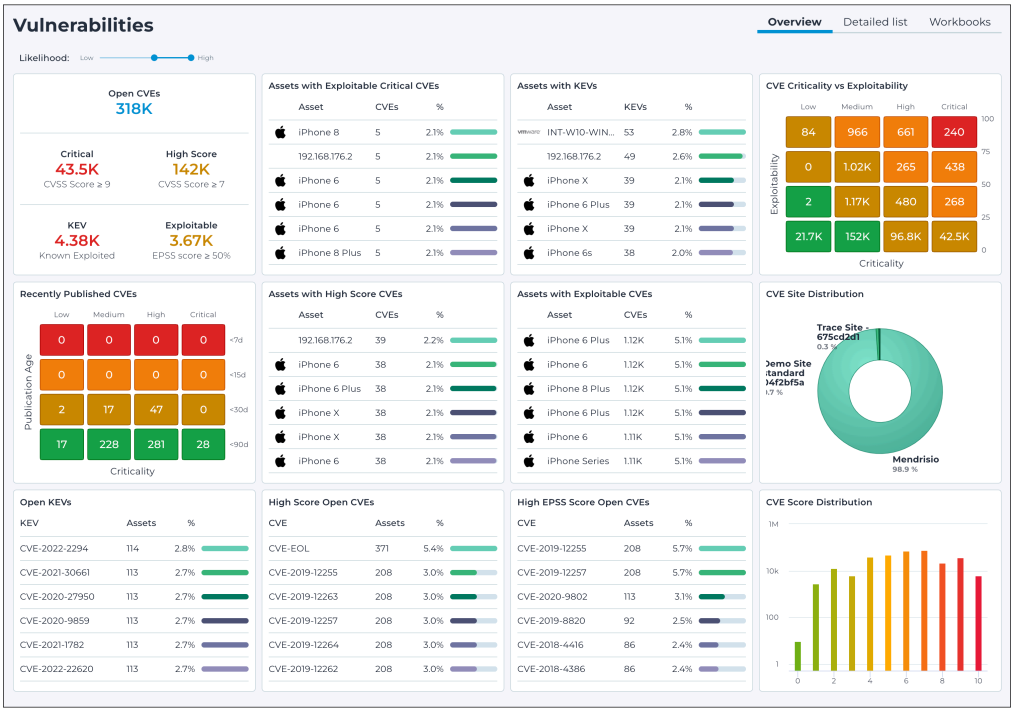
Figure 48. Vulnerabilities page

The Vulnerabilities page has these tabs:

- Overview (on page 144)
- Detailed list (on page 146)
- Workbooks (on page 155)

Overview

*The **Overview** page provides a comprehensive summary of the system's vulnerability landscape, helping you prioritize risk mitigation efforts.*



Vulnerabilities

Overview | Detailed list | Workbooks

Likelihood: Low High

Open CVEs 318K

Critical 43.5K CVSS Score ≥ 9

High Score 142K CVSS Score ≥ 7

KEV 4.38K Known Exploited

Exploitable 3.67K EPSS score ≥ 50%

Assets with Exploitable Critical CVEs

Asset	CVEs	%
iPhone 8	5	2.1%
192.168.176.2	5	2.1%
iPhone 6	5	2.1%
iPhone 6	5	2.1%
iPhone 6	5	2.1%
iPhone 8 Plus	5	2.1%

Assets with KEVs

Asset	KEVs	%
INT-W10-WIN...	53	2.8%
192.168.176.2	49	2.6%
iPhone X	39	2.1%
iPhone 6 Plus	39	2.1%
iPhone X	39	2.1%
iPhone 6s	38	2.0%

CVE Criticality vs Exploitability

Exploitability	Low	Medium	High	Critical
100	84	966	661	240
75	0	1.02K	265	438
50	2	1.17K	480	268
25	21.7K	152K	96.8K	42.5K
0				

Criticality

Recently Published CVEs

Publication Age	Low	Medium	High	Critical
<7d	0	0	0	0
<15d	0	0	0	0
<30d	2	17	47	0
<90d	17	228	281	28

Criticality

Assets with High Score CVEs

Asset	CVEs	%
192.168.176.2	39	2.2%
iPhone 6	38	2.1%
iPhone 6 Plus	38	2.1%
iPhone X	38	2.1%
iPhone X	38	2.1%
iPhone 6	38	2.1%

Assets with Exploitable CVEs

Asset	CVEs	%
iPhone 6 Plus	1.12K	5.1%
iPhone 6	1.12K	5.1%
iPhone 8 Plus	1.12K	5.1%
iPhone 6 Plus	1.12K	5.1%
iPhone 6	1.11K	5.1%
iPhone Series	1.11K	5.1%

CVE Site Distribution

Open KEVs

KEV	Assets	%
CVE-2022-2294	114	2.8%
CVE-2021-30661	113	2.7%
CVE-2020-27950	113	2.7%
CVE-2020-9859	113	2.7%
CVE-2021-1782	113	2.7%
CVE-2022-22620	113	2.7%

High Score Open CVEs

CVE	Assets	%
CVE-EOL	371	5.4%
CVE-2019-12255	208	3.0%
CVE-2019-12263	208	3.0%
CVE-2019-12257	208	3.0%
CVE-2019-12264	208	3.0%
CVE-2019-12262	208	3.0%

High EPSS Score Open CVEs

CVE	Assets	%
CVE-2019-12255	208	5.7%
CVE-2019-12257	208	5.7%
CVE-2020-9802	113	3.1%
CVE-2019-8820	92	2.5%
CVE-2018-4416	86	2.4%
CVE-2018-4386	86	2.4%

CVE Score Distribution

Figure 49. Overview page

Likelihood

The **Likelihood** slider allows you to adjust the risk threshold, helping you focus on vulnerabilities most likely to be exploited.

Open CVEs

See the total number of known *CVE* affecting assets in the system.

Assets with Exploitable Critical CVEs

Lists assets that have known *CVE*s with active exploits in the wild.

Assets with KEVs

Highlights assets impacted by *Known Exploited Vulnerabilities (KEV)*.

CVE Criticality vs Exploitability

Provides a visual representation of *CVE*s categorized by their severity and likelihood of exploitation.

Recently Published CVEs

Displays a grid of newly published *CVE*s categorized by severity and publication age.

Assets with High Score CVEs

Shows assets affected by *CVE*s with a high score, indicating high risk.

Assets with Exploitable CVEs

Identifies assets with *CVE*s that have known exploitability indicators.

CVE Site Distribution

Displays how *CVE*s are distributed across different monitored sites.

Open KEVs

Lists vulnerabilities that have been publicly disclosed as *KEV*s.

High Score Open KEVs

Displays *KEV*s that have high severity scores.

High EPSS Score Open KEVs

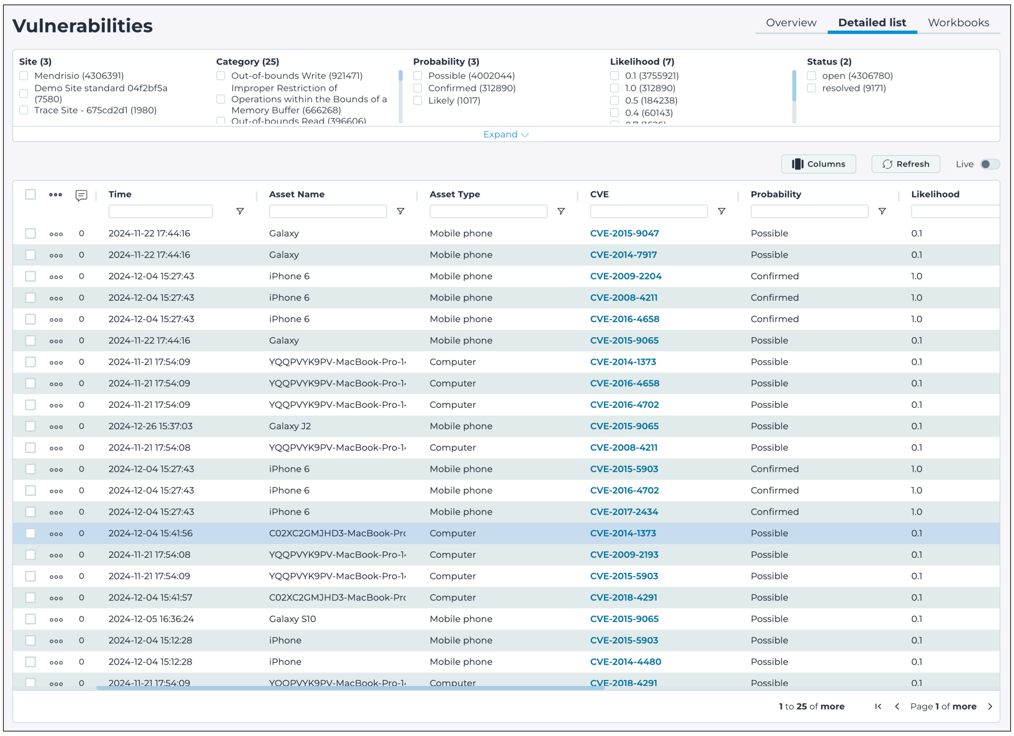
Lists vulnerabilities with a high *Exploit Prediction Scoring System (EPSS)* scores, indicating a high probability of real-world exploitation.

CVE Score Distribution

Use the distribution graph to analyze *CVE* severity scores and assess overall risk exposure.

Detailed list

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



Site (3)
- □ Mendrisio (4306391)
- □ Demo Site standard 04f2bf5a (7580)
- □ Trace Site - 675cd2d1 (1980)

Category (25)
- □ Out-of-bounds Write (921471)
- □ Improper Restriction of Operations within the Bounds of a Memory Buffer (666268)
- □ Out-of-bounds Read (396606)

Probability (3)
- □ Possible (4002044)
- □ Confirmed (312890)
- □ Likely (1017)

Likelihood (7)
- □ 0.1 (3755921)
- □ 1.0 (312890)
- □ 0.5 (184238)
- □ 0.4 (60143)

Status (2)
- □ open (4306780)
- □ resolved (9171)

□	•••		Time	Asset Name	Asset Type	CVE	Probability	Likelihood
□	∘∘∘	0	2024-11-22 17:44:16	Galaxy	Mobile phone	CVE-2015-9047	Possible	0.1
□	∘∘∘	0	2024-11-22 17:44:16	Galaxy	Mobile phone	CVE-2014-7917	Possible	0.1
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2009-2204	Confirmed	1.0
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2008-4211	Confirmed	1.0
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2016-4658	Confirmed	1.0
□	∘∘∘	0	2024-11-22 17:44:16	Galaxy	Mobile phone	CVE-2015-9065	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:09	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2014-1373	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:09	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2016-4658	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:09	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2016-4702	Possible	0.1
□	∘∘∘	0	2024-12-26 15:37:03	Galaxy J2	Mobile phone	CVE-2015-9065	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:08	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2008-4211	Possible	0.1
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2015-5903	Confirmed	1.0
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2016-4702	Confirmed	1.0
□	∘∘∘	0	2024-12-04 15:27:43	iPhone 6	Mobile phone	CVE-2017-2434	Confirmed	1.0
□	∘∘∘	0	2024-12-04 15:41:56	C02XC2GMJHD3-MacBook-Pr	Computer	CVE-2014-1373	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:08	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2009-2193	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:09	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2015-5903	Possible	0.1
□	∘∘∘	0	2024-12-04 15:41:57	C02XC2GMJHD3-MacBook-Pr	Computer	CVE-2018-4291	Possible	0.1
□	∘∘∘	0	2024-12-05 16:36:24	Galaxy S10	Mobile phone	CVE-2015-9065	Possible	0.1
□	∘∘∘	0	2024-12-04 15:12:28	iPhone	Mobile phone	CVE-2015-5903	Possible	0.1
□	∘∘∘	0	2024-12-04 15:12:28	iPhone	Mobile phone	CVE-2014-4480	Possible	0.1
□	∘∘∘	0	2024-11-21 17:54:09	YQQPVYK9PV-MacBook-Pro-1	Computer	CVE-2018-4291	Possible	0.1

1 to **25** of **more** Page **1** of **more**

Figure 50. Detailed list page

Site

This shows a list of all the sites that are applicable for the vulnerabilities in the current table view.

Category

This shows a list of all the different categories that are applicable for the vulnerabilities in the current table view.

Probability

This shows a list of the different probabilities that have been confirmed for all the vulnerabilities in the current table view. When a vulnerability is not confirmed, it will show as **Possible**.

Likelihood

This shows a list of the different likelihoods that are applicable for the vulnerabilities in the current table view. This is a numerical assessment of the possibility that this vulnerability exists on an asset. It is measured on a scale from 0.1 to 1.0, where 1.0 is the most likely.

Columns

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

Refresh

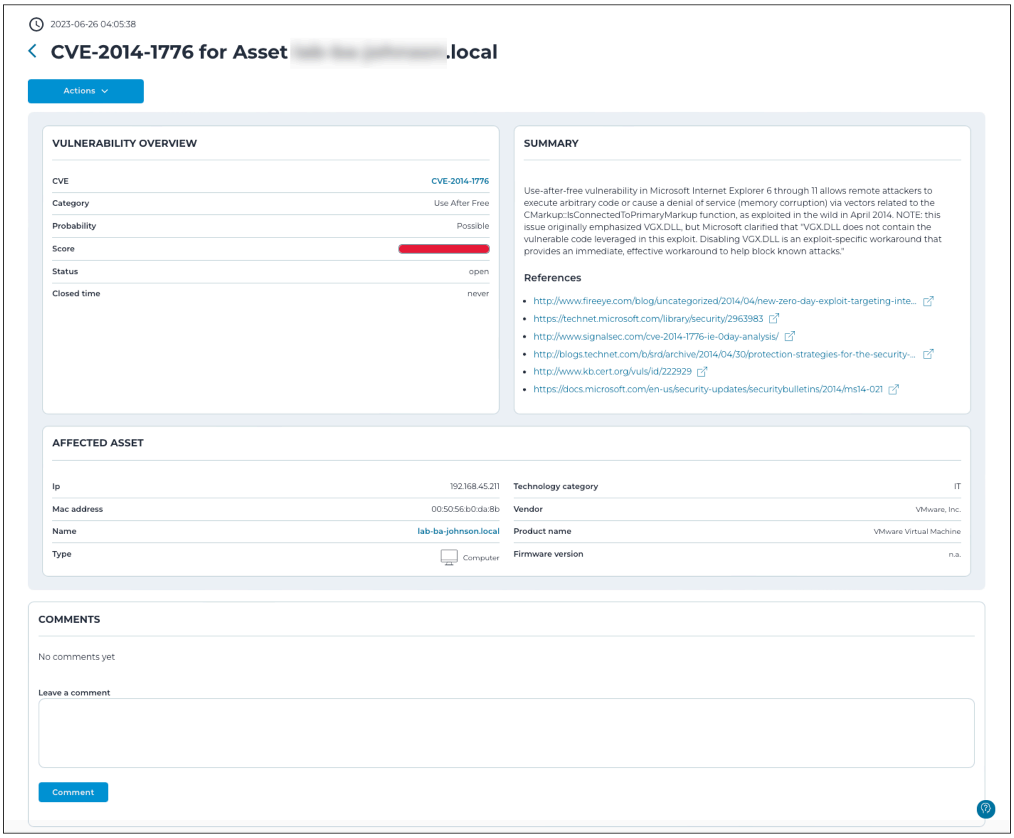
The **Refresh** ↻ icon lets you immediately refresh the current view.

Live

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

Details page

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



2023-06-26 04:05:38

CVE-2014-1776 for Asset [redacted].local

VULNERABILITY OVERVIEW

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

SUMMARY

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."

References

- http://www.fireeye.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

AFFECTED ASSET

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.

COMMENTS

No comments yet

Leave a comment

Figure 51. Details page

Actions dropdown

This dropdown gives you access to the action: Resolve Vulnerability (on page 153).

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:

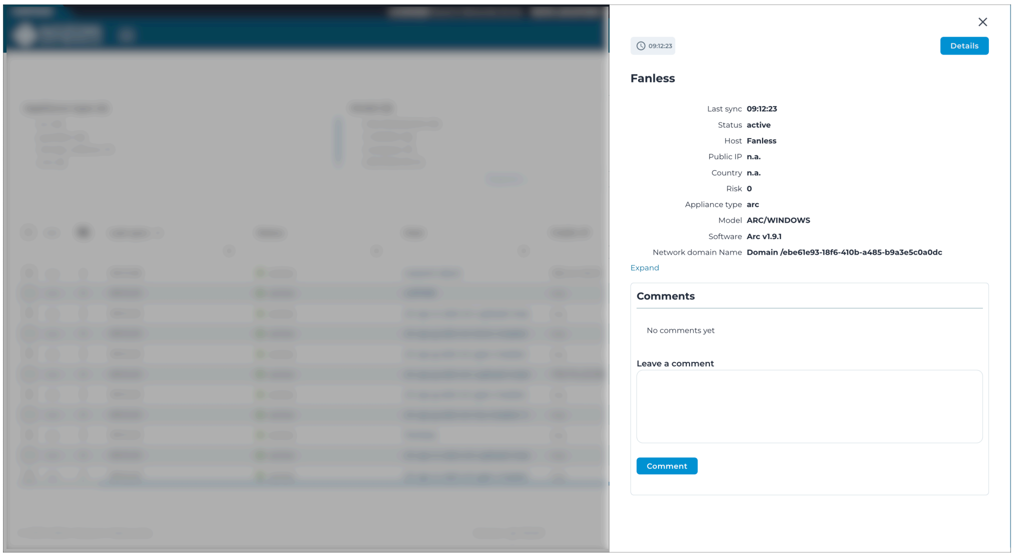
- ip
- Mac address
- Name
- Type
- Technology category
- Vendor
- Product name
- Firmware version

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.



Fanless

Last sync	**09:12:23**
Status	**active**
Host	**Fanless**
Public IP	**n.a.**
Country	**n.a.**
Risk	**0**
Appliance type	**arc**
Model	**ARC/WINDOWS**
Software	**Arc v1.9.1**
Network domain Name	**Domain /ebe61e93-18f6-410b-a485-b9a3e5c0a0dc**

Comments

No comments yet

Leave a comment

Figure 52. 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

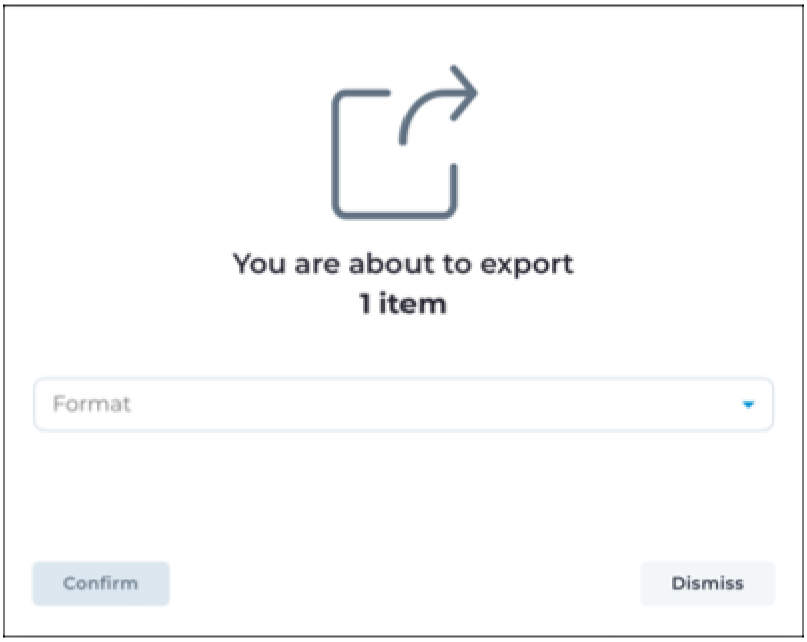
1. In the top navigation bar, select **Vulnerabilities**.
2. Choose a method to open the actions menu.

   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**.

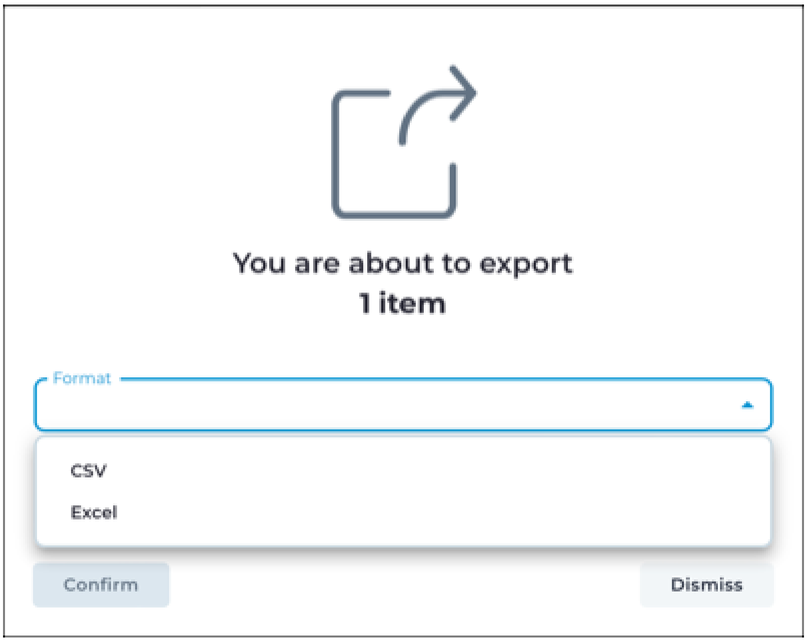
   

   You are about to export
   1 item

   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.

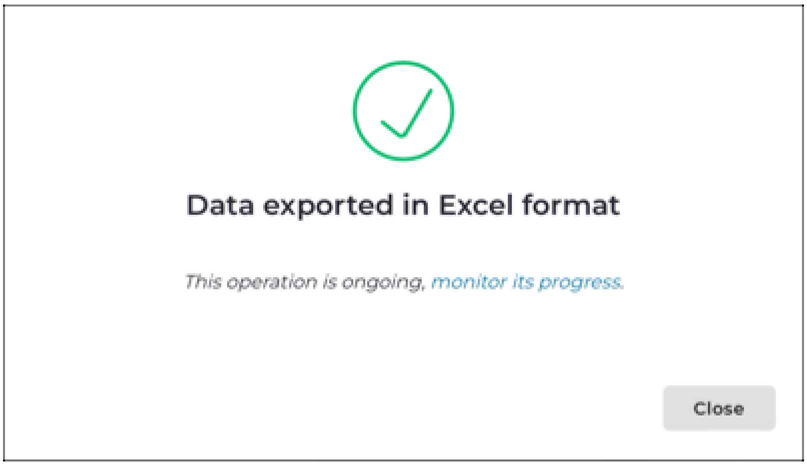


You are about to export
1 item

7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.



Data exported in Excel format

This operation is ongoing, monitor its progress.

Results

The vulnerability has been exported.

Resolve a vulnerability

You can use the actions menu to resolve one or more vulnerabilities.

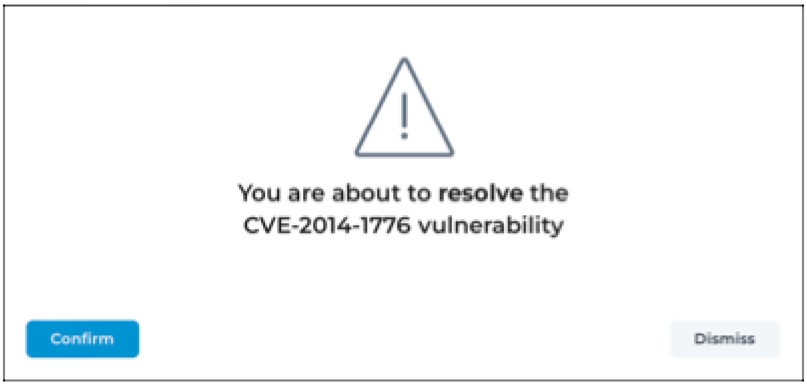
Procedure

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**.

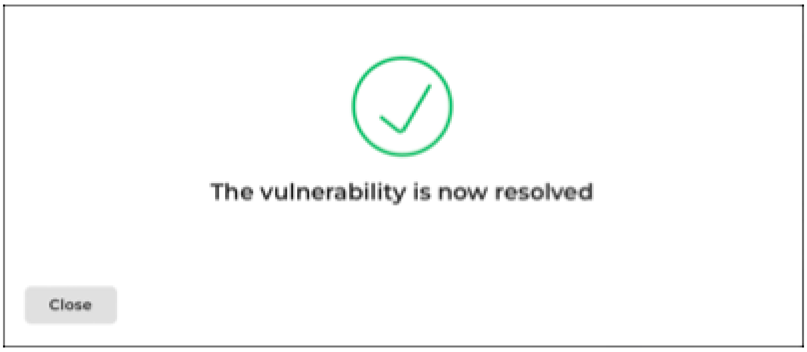
   Result: A dialog shows.
5. Select **Confirm**.



You are about to resolve the CVE-2014-1776 vulnerability

   Result: A dialog shows.

6. Select **Close**.



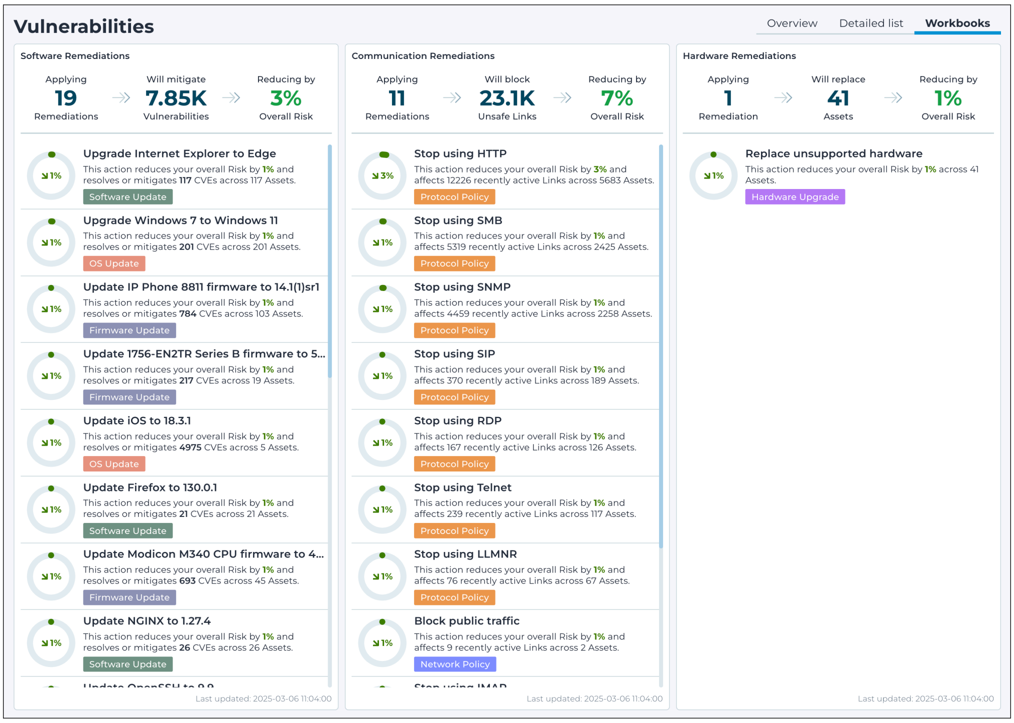
The vulnerability is now resolved

Results

The vulnerability has been resolved.

Workbooks

*The **Workbooks** page shows recommended courses of action that can improve your network security. Generated through machine learning, workbooks highlight the vulnerabilities currently creating the highest risk exposure.*



Vulnerabilities

Software Remediations

Applying 19 Remediations → Will mitigate 7.85K Vulnerabilities → Reducing by 3% Overall Risk

↘1% **Upgrade Internet Explorer to Edge**
This action reduces your overall Risk by **1%** and resolves or mitigates **117** CVEs across 117 Assets.
Software Update

↘1% **Upgrade Windows 7 to Windows 11**
This action reduces your overall Risk by **1%** and resolves or mitigates **201** CVEs across 201 Assets.
OS Update

↘1% **Update IP Phone 8811 firmware to 14.1(1)sr1**
This action reduces your overall Risk by **1%** and resolves or mitigates **784** CVEs across 103 Assets.
Firmware Update

↘1% **Update 1756-EN2TR Series B firmware to 5...**
This action reduces your overall Risk by **1%** and resolves or mitigates **217** CVEs across 19 Assets.
Firmware Update

↘1% **Update iOS to 18.3.1**
This action reduces your overall Risk by **1%** and resolves or mitigates **4975** CVEs across 5 Assets.
OS Update

↘1% **Update Firefox to 130.0.1**
This action reduces your overall Risk by **1%** and resolves or mitigates **21** CVEs across 21 Assets.
Software Update

↘1% **Update Modicon M340 CPU firmware to 4...**
This action reduces your overall Risk by **1%** and resolves or mitigates **693** CVEs across 45 Assets.
Firmware Update

↘1% **Update NGINX to 1.27.4**
This action reduces your overall Risk by **1%** and resolves or mitigates **26** CVEs across 26 Assets.
Software Update

Update OpenSSH to 9.9

Last updated: 2025-03-06 11:04:00

Communication Remediations

Applying 11 Remediations → Will block 23.1K Unsafe Links → Reducing by 7% Overall Risk

↘3% **Stop using HTTP**
This action reduces your overall Risk by **3%** and affects 12226 recently active Links across 5683 Assets.
Protocol Policy

↘1% **Stop using SMB**
This action reduces your overall Risk by **1%** and affects 5319 recently active Links across 2425 Assets.
Protocol Policy

↘1% **Stop using SNMP**
This action reduces your overall Risk by **1%** and affects 4459 recently active Links across 2258 Assets.
Protocol Policy

↘1% **Stop using SIP**
This action reduces your overall Risk by **1%** and affects 370 recently active Links across 189 Assets.
Protocol Policy

↘1% **Stop using RDP**
This action reduces your overall Risk by **1%** and affects 167 recently active Links across 126 Assets.
Protocol Policy

↘1% **Stop using Telnet**
This action reduces your overall Risk by **1%** and affects 239 recently active Links across 117 Assets.
Protocol Policy

↘1% **Stop using LLMNR**
This action reduces your overall Risk by **1%** and affects 76 recently active Links across 67 Assets.
Protocol Policy

↘1% **Block public traffic**
This action reduces your overall Risk by **1%** and affects 9 recently active Links across 2 Assets.
Network Policy

Stop using IMAP

Last updated: 2025-03-06 11:04:00

Hardware Remediations

Applying 1 Remediation → Will replace 41 Assets → Reducing by 1% Overall Risk

↘1% **Replace unsupported hardware**
This action reduces your overall Risk by **1%** across 41 Assets.
Hardware Upgrade

Last updated: 2025-03-06 11:04:00

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:

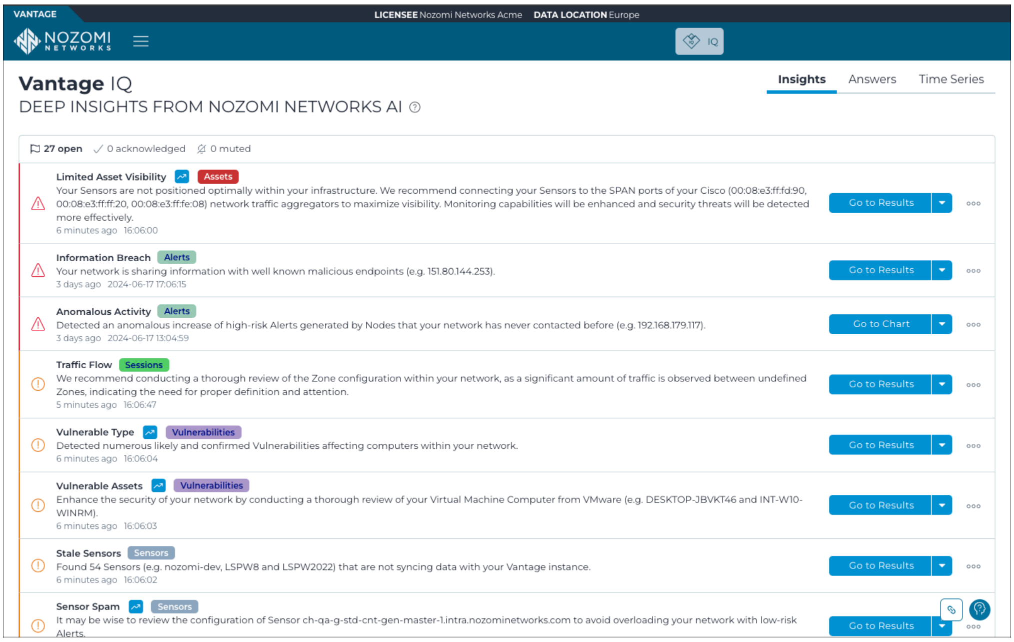
- On the left, the highest risk score among all the vulnerabilities included in the workbook.
- A title that shows the recommended course of action.
- A description of the issue and the benefits of addressing it.
- In the top right corner of each workbook, Vantage shows:
  - An assessment of the risk 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 226)

Chapter 8. Vantage IQ

Vantage IQ helps you navigate and explore your network. You can use smart query commands to leverage advanced machine learning and data analytic algorithms to dive deeper into your data.



LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Vantage IQ
DEEP INSIGHTS FROM NOZOMI NETWORKS AI

27 open ✓ 0 acknowledged 0 muted

Limited Asset Visibility Assets
Your Sensors are not positioned optimally within your infrastructure. We recommend connecting your Sensors to the SPAN ports of your Cisco (00:08:e3:ff:fd:90, 00:08:e3:ff:ff:20, 00:08:e3:ff:fe:08) network traffic aggregators to maximize visibility. Monitoring capabilities will be enhanced and security threats will be detected more effectively.
6 minutes ago 16:06:00

Information Breach Alerts
Your network is sharing information with well known malicious endpoints (e.g. 151.80.144.253).
3 days ago 2024-06-17 17:06:15

Anomalous Activity Alerts
Detected an anomalous increase of high-risk Alerts generated by Nodes that your network has never contacted before (e.g. 192.168.179.117).
3 days ago 2024-06-17 13:04:59

Traffic Flow Sessions
We recommend conducting a thorough review of the Zone configuration within your network, as a significant amount of traffic is observed between undefined Zones, indicating the need for proper definition and attention.
5 minutes ago 16:06:47

Vulnerable Type Vulnerabilities
Detected numerous likely and confirmed Vulnerabilities affecting computers within your network.
6 minutes ago 16:06:04

Vulnerable Assets Vulnerabilities
Enhance the security of your network by conducting a thorough review of your Virtual Machine Computer from VMware (e.g. DESKTOP-JBVKT46 and INT-W10-WINRM).
6 minutes ago 16:06:03

Stale Sensors Sensors
Found 54 Sensors (e.g. nozomi-dev, LSPW8 and LSPW2022) that are not syncing data with your Vantage instance.
6 minutes ago 16:06:02

Sensor Spam Sensors
It may be wise to review the configuration of Sensor ch-qa-g-std-cnt-gen-master-1.intra.nozominetworks.com to avoid overloading your network with low-risk Alerts.

Figure 54. 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 161).

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 166).

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 166).

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 161) 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 161) 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** page 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 121) 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 168)
- Compare (on page 170)
- Correlation (on page 171)
- Describe (on page 172)
- Forecast (on page 173)
- Pivot (on page 174)
- Popular (on page 175)
- Simplify (on page 176)
- Timeline (on page 177)
- Versus (on page 178)
- Visualize (on page 179)

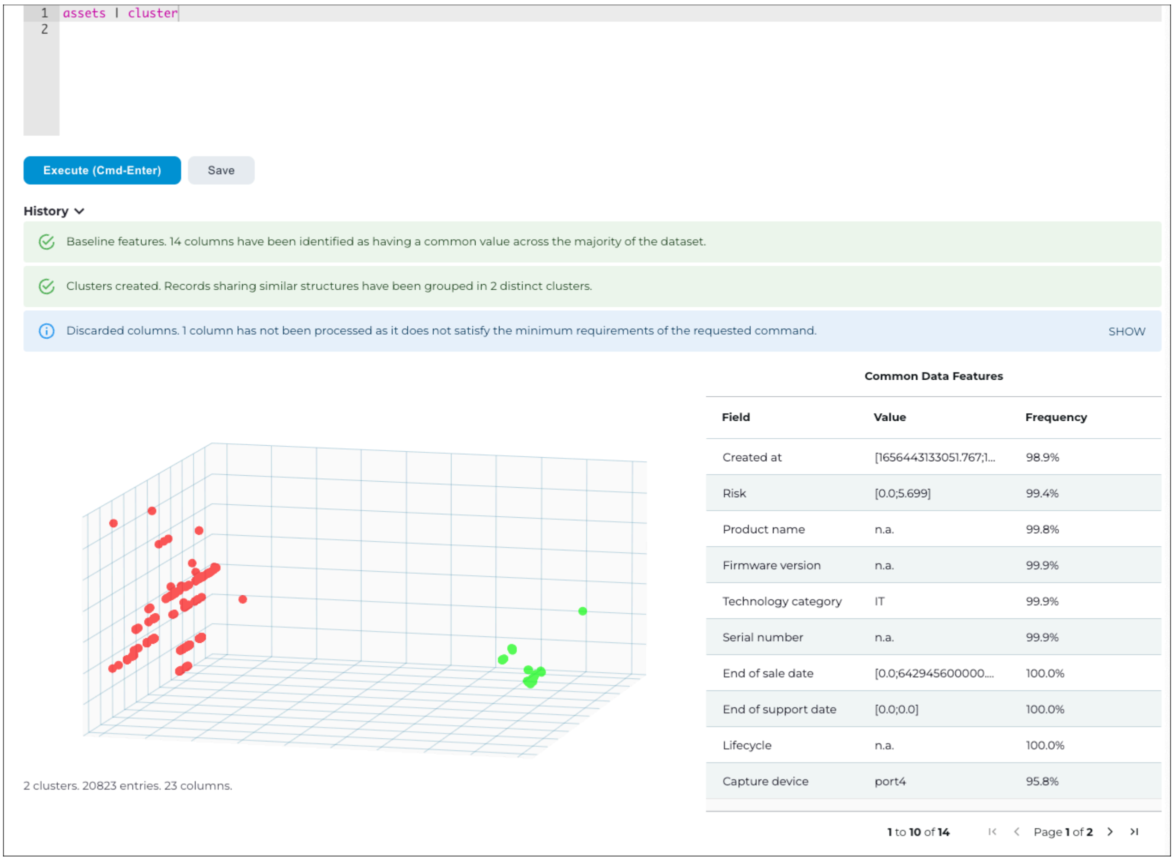
Cluster

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`



```
assets | cluster
```

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 2 distinct clusters.

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

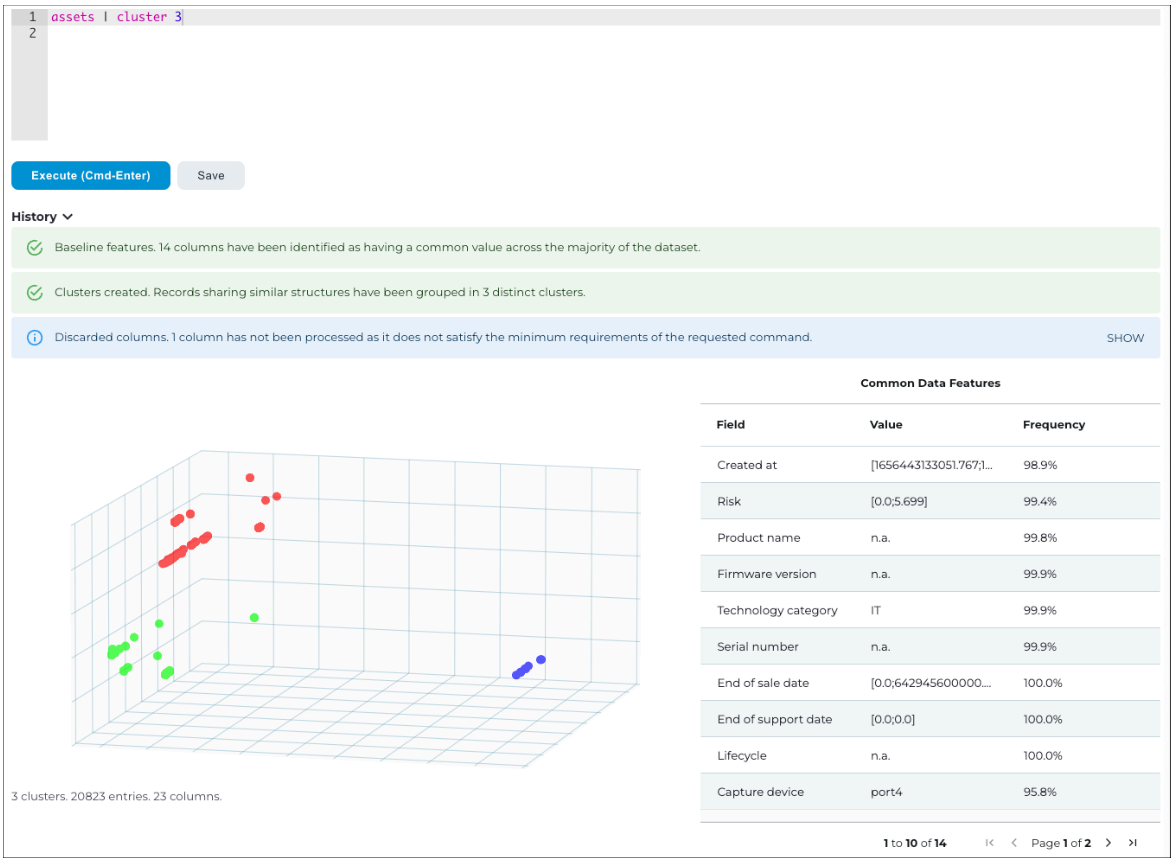
2 clusters. 20823 entries. 23 columns.

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

Example: `assets | cluster 3`



```
assets | cluster 3
```

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.

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%

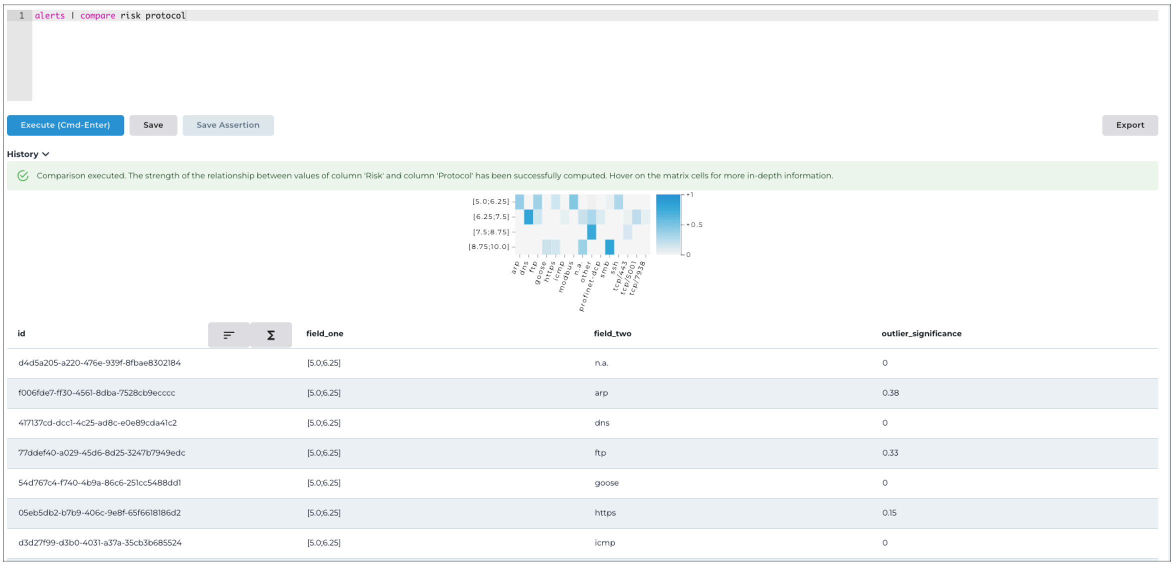
Compare

Vantage IQ query example: Compare.

Usage: <field> | compare <field1> <field2>

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

Example: `alerts | compare risk protocol`

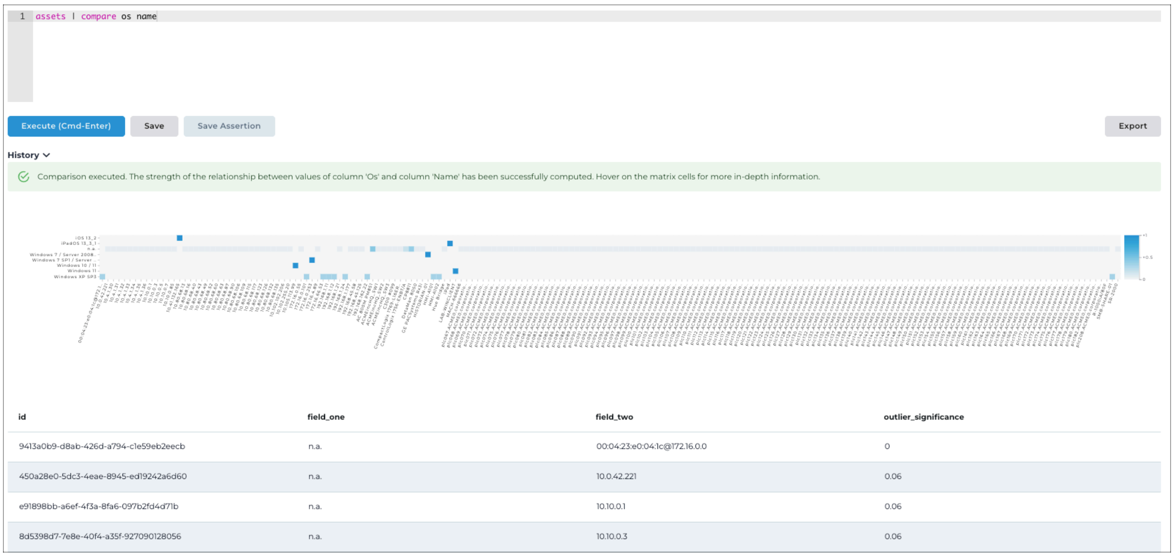


```
alerts | compare risk protocol
```

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-a220-476e-939f-8fbae8302184	[5.0;6.25]	n.a.	0
f006fde7-ff30-4561-8dba-7528cb9ecccc	[5.0;6.25]	arp	0.38
417137cd-dcc1-4c25-ad8c-e0e89cda41c2	[5.0;6.25]	dns	0
77ddef40-a029-45d6-8d25-3247b7949edc	[5.0;6.25]	ftp	0.33
54d767c4-f740-4b9a-86c6-251cc5488dd1	[5.0;6.25]	goose	0
05eb5db2-b7b9-406c-9e8f-65f6618186d2	[5.0;6.25]	https	0.15
d3d27f99-d3b0-4031-a37a-35cb3b685524	[5.0;6.25]	icmp	0

Example: `assets | compare os name`



```
assets | compare os name
```

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-c1e59eb2eecb	n.a.	00:04:23:e0:04:1c@172.16.0.0	0
450a28e0-5dc3-4eae-8945-ed19242a6d60	n.a.	10.0.42.221	0.06
e91898bb-a6ef-4f3a-8fa6-097b2fd4d71b	n.a.	10.10.0.1	0.06
8d5398d7-7e8e-40f4-a35f-927090128056	n.a.	10.10.0.3	0.06

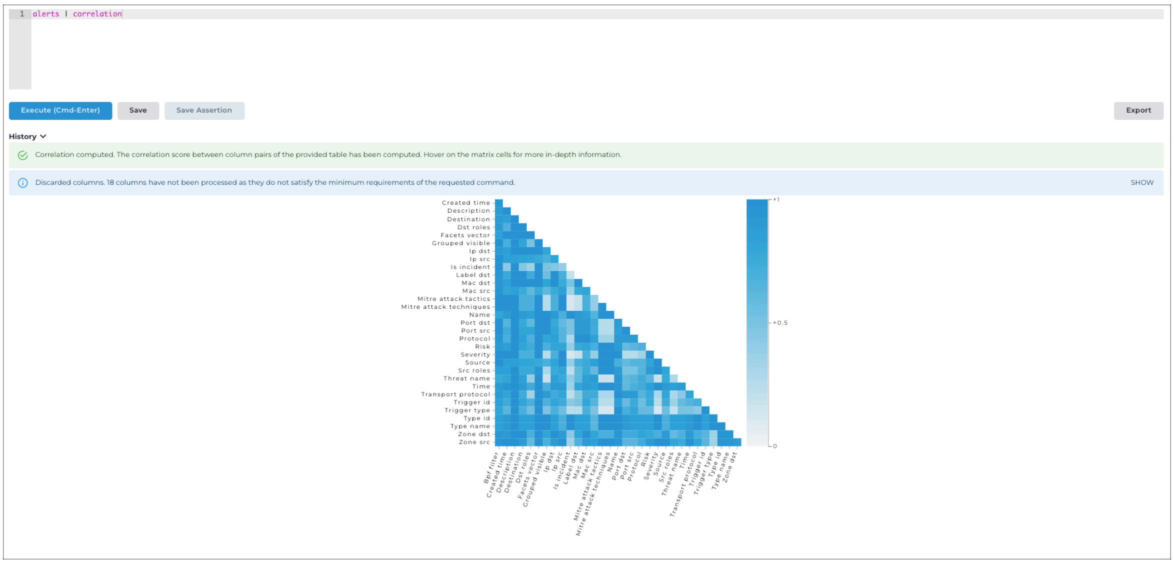
Correlation

Vantage IQ query example: Correlation.

Usage: <field> | correlation

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

Example: `alerts | correlation`

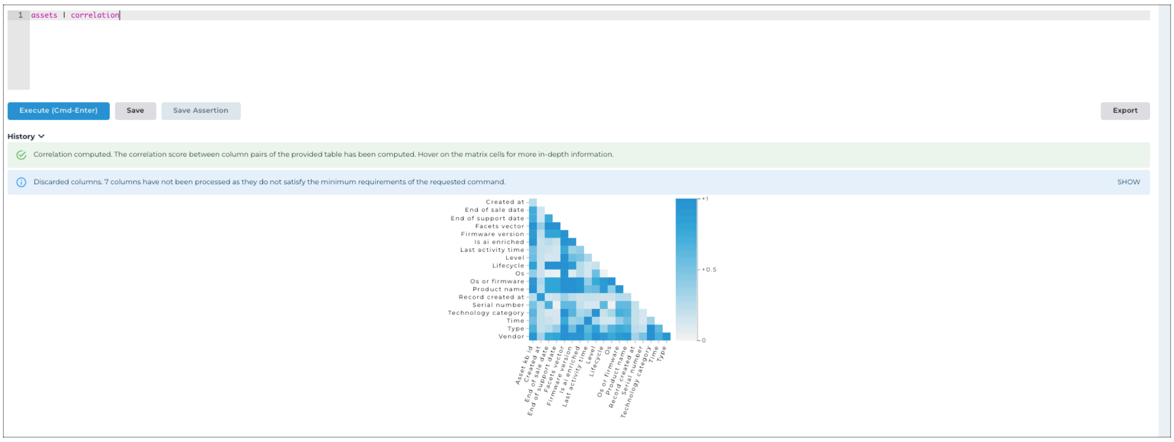


```
alerts | correlation
```

Correlation computed. The correlation score between column pairs of the provided table has been computed. Hover on the matrix cells for more in-depth information.

Discarded columns. 18 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

Example: `assets | correlation`



```
assets | correlation
```

Correlation computed. The correlation score between column pairs of the provided table has been computed. Hover on the matrix cells for more in-depth information.

Discarded columns. 7 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

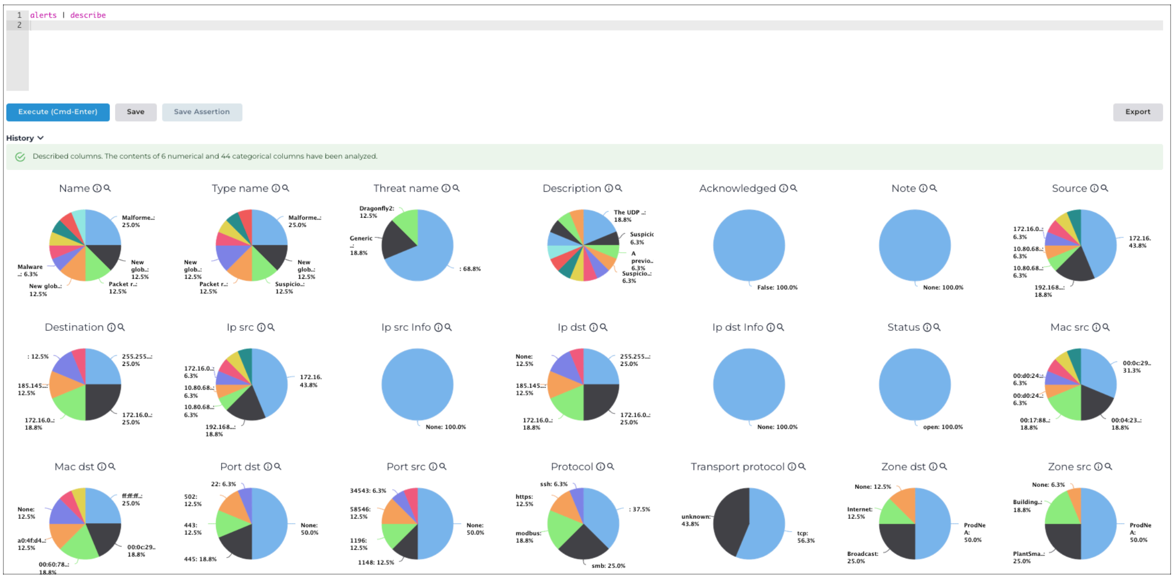
Describe

Vantage IQ query example: Describe.

Usage: <field> | describe

Description: Compute several descriptive statistics of the passed content.

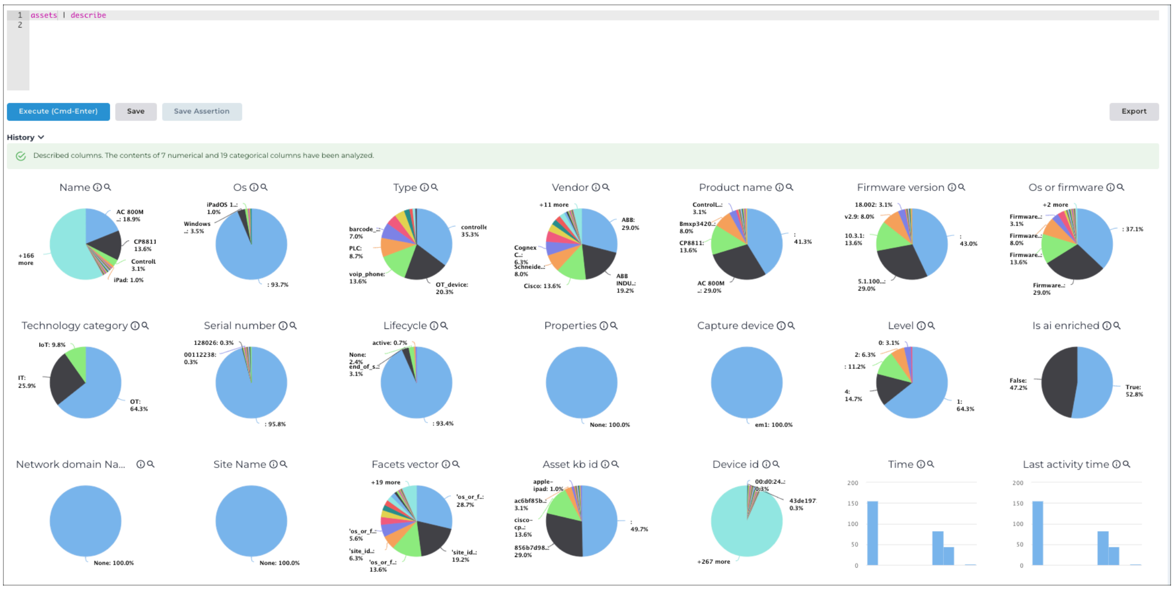
Example: `alerts | describe`



```
alerts | describe
```

Described columns. The contents of 6 numerical and 44 categorical columns have been analyzed.

Example: `assets | describe`



```
assets | describe
```

Described columns. The contents of 7 numerical and 19 categorical columns have been analyzed.

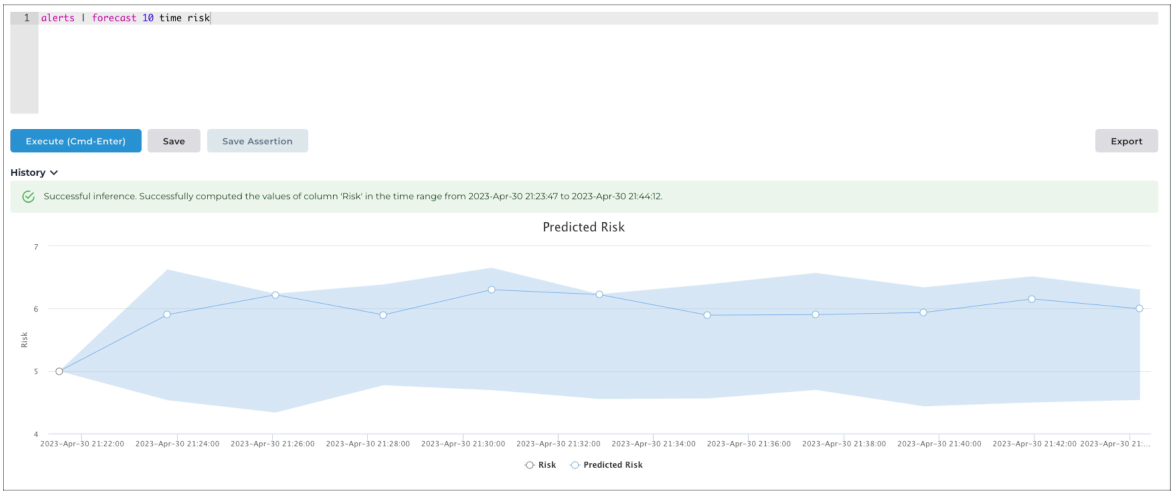
Forecast

Vantage IQ query example: Forecast.

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

Description: Forecast the values of a numeric time series.

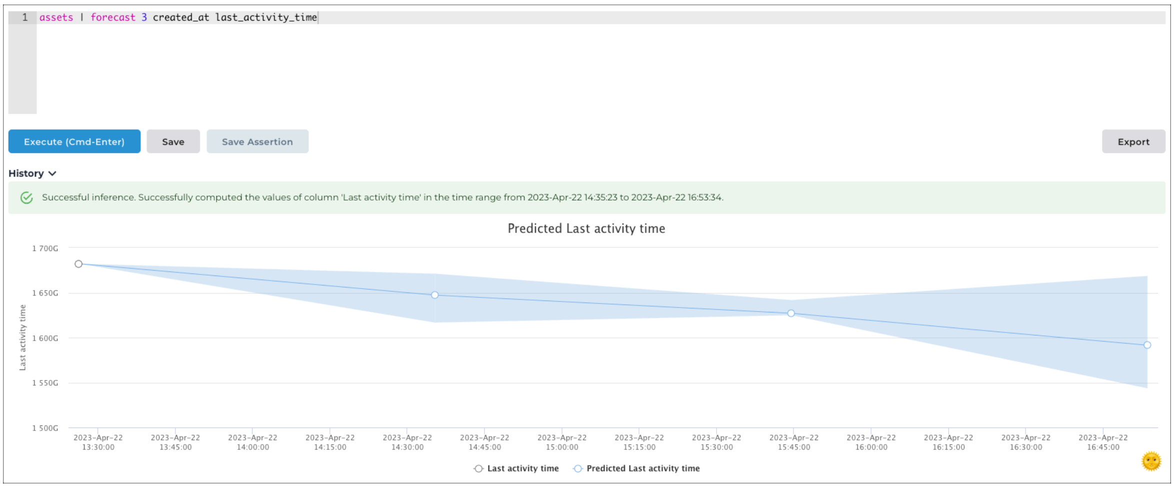
Example: `alerts | forecast 10 time risk`



```
alerts | forecast 10 time risk
```

Successful inference. Successfully computed the values of column 'Risk' in the time range from 2023-Apr-30 21:23:47 to 2023-Apr-30 21:44:12.

Example: `assets | forecast 3 created_at last_activity_time`



```
assets | forecast 3 created_at last_activity_time
```

Successful inference. Successfully computed the values of column 'Last activity time' in the time range from 2023-Apr-22 14:35:23 to 2023-Apr-22 16:53:34.

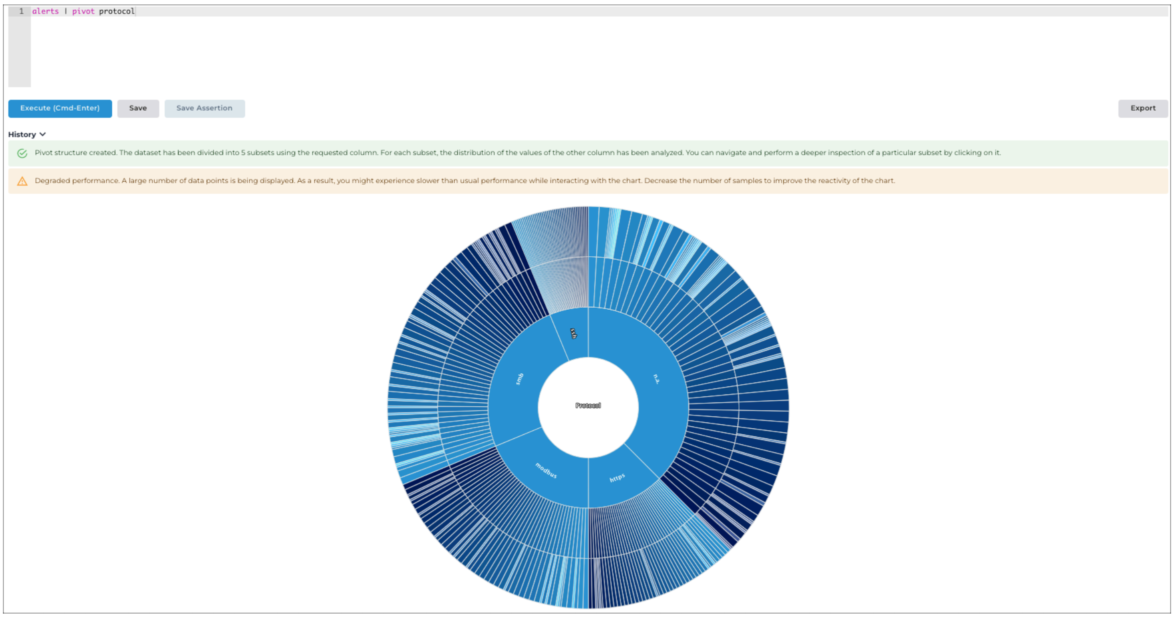
Pivot

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`

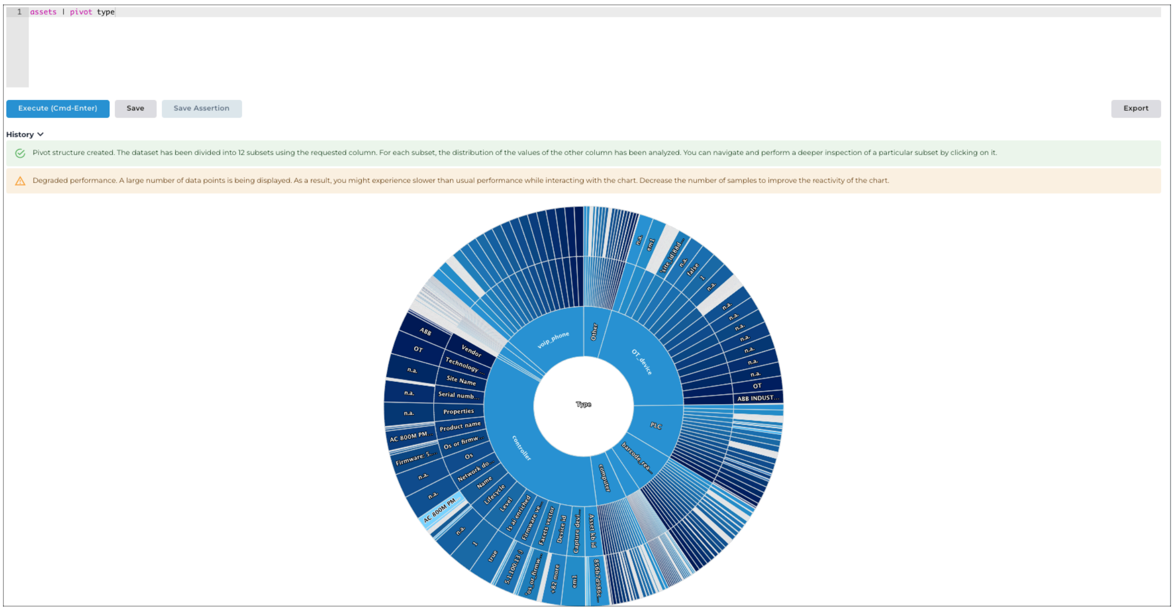


```
alerts | pivot protocol
```

Pivot structure created. The dataset has been divided into 5 subsets using the requested column. For each subset, the distribution of the values of the other column has been analyzed. You can navigate and perform a deeper inspection of a particular subset by clicking on it.

Degraded performance. A large number of data points is being displayed. As a result, you might experience slower than usual performance while interacting with the chart. Decrease the number of samples to improve the reactivity of the chart.

Example: `assets | pivot type`



```
assets | pivot type
```

Pivot structure created. The dataset has been divided into 12 subsets using the requested column. For each subset, the distribution of the values of the other column has been analyzed. You can navigate and perform a deeper inspection of a particular subset by clicking on it.

Degraded performance. A large number of data points is being displayed. As a result, you might experience slower than usual performance while interacting with the chart. Decrease the number of samples to improve the reactivity of the chart.

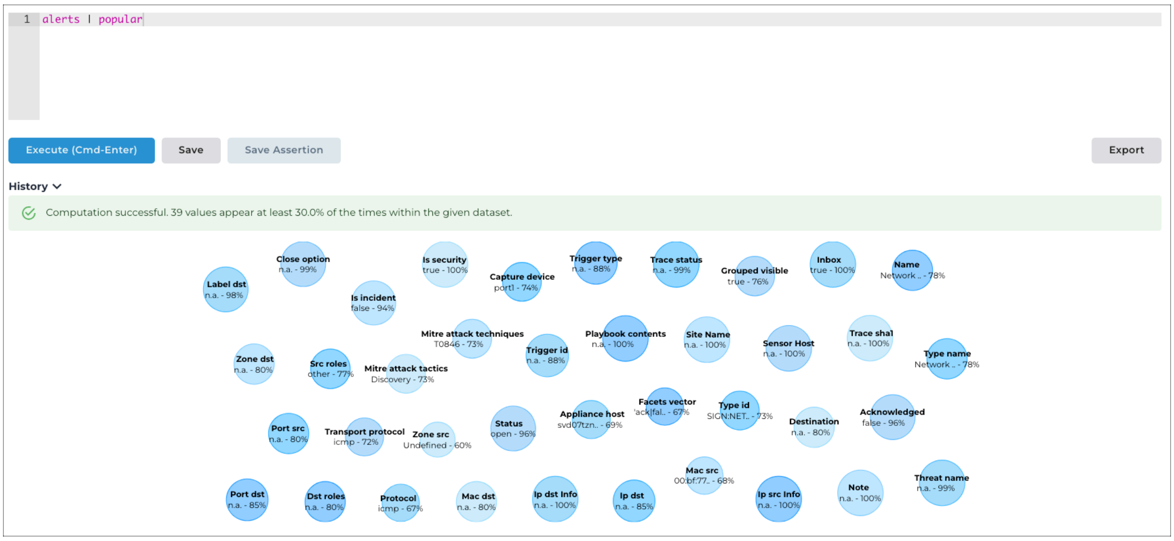
Popular

Vantage IQ query example: Popular.

Usage: <field> | popular <field>

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

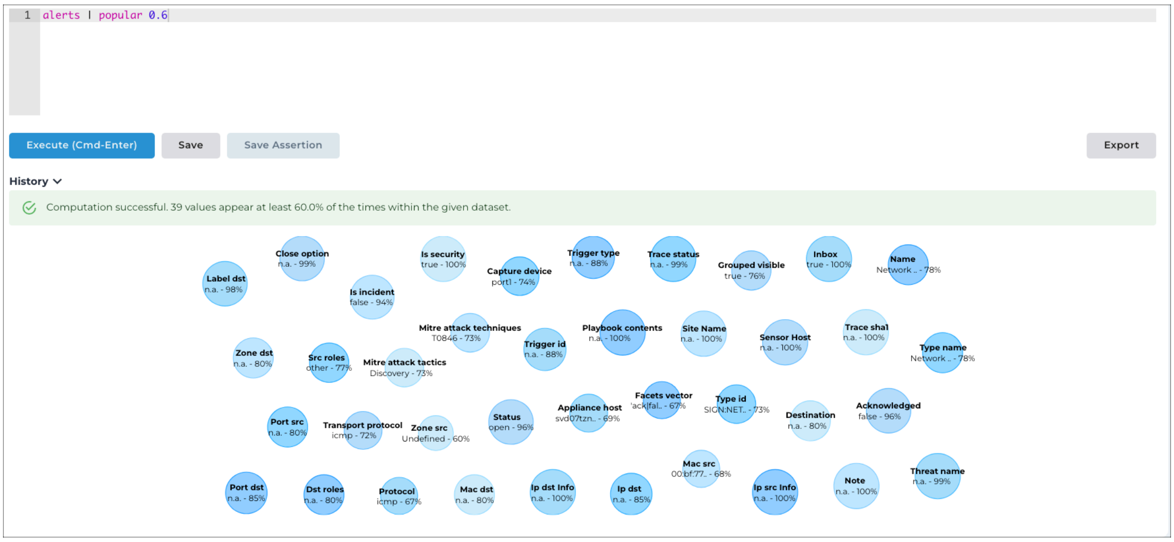
Example: `alerts | popular`



```
alerts | popular
```

Computation successful. 39 values appear at least 30.0% of the times within the given dataset.

Example: `alerts | popular 0.6`



```
alerts | popular 0.6
```

Computation successful. 39 values appear at least 60.0% of the times within the given dataset.

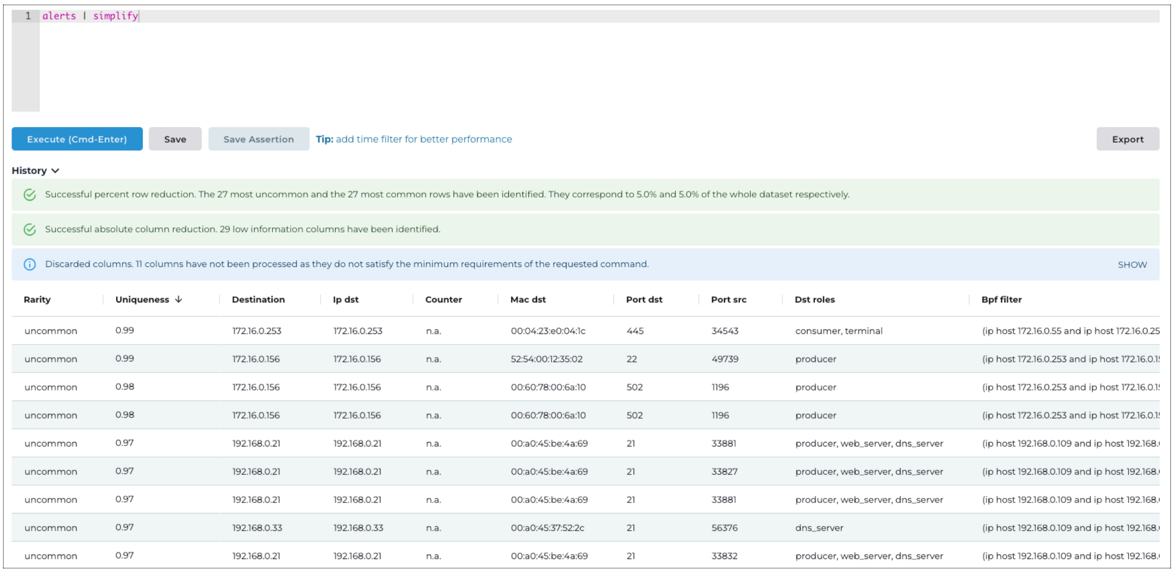
Simplify

Vantage IQ query example: Simplify.

Usage: <field> | simplify <field> <rows> <number>

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

Example: `alerts | simplify`



```
alerts | simplify
```

Tip: add time filter for better performance

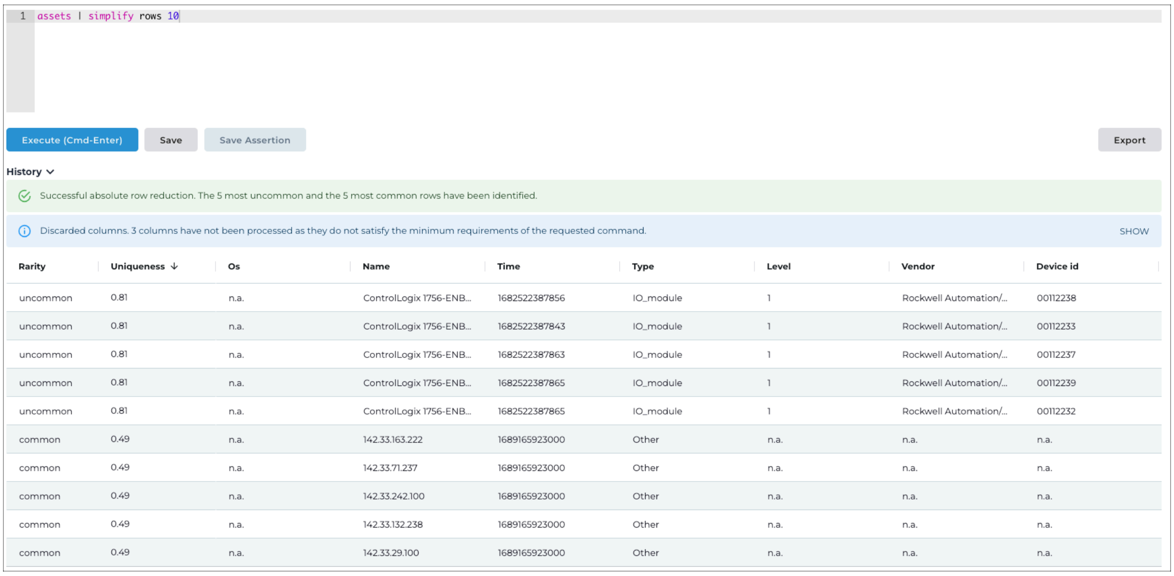
Successful percent row reduction. The 27 most uncommon and the 27 most common rows have been identified. They correspond to 5.0% and 5.0% of the whole dataset respectively.

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.
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.
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.
uncommon	0.97	192.168.0.33	192.168.0.33	n.a.	00:a0:45:37:52:2c	21	56376	dns_server	(ip host 192.168.0.109 and ip host 192.168.
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.

Example: `assets | simplify rows 10`



```
assets | simplify rows 10
```

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.

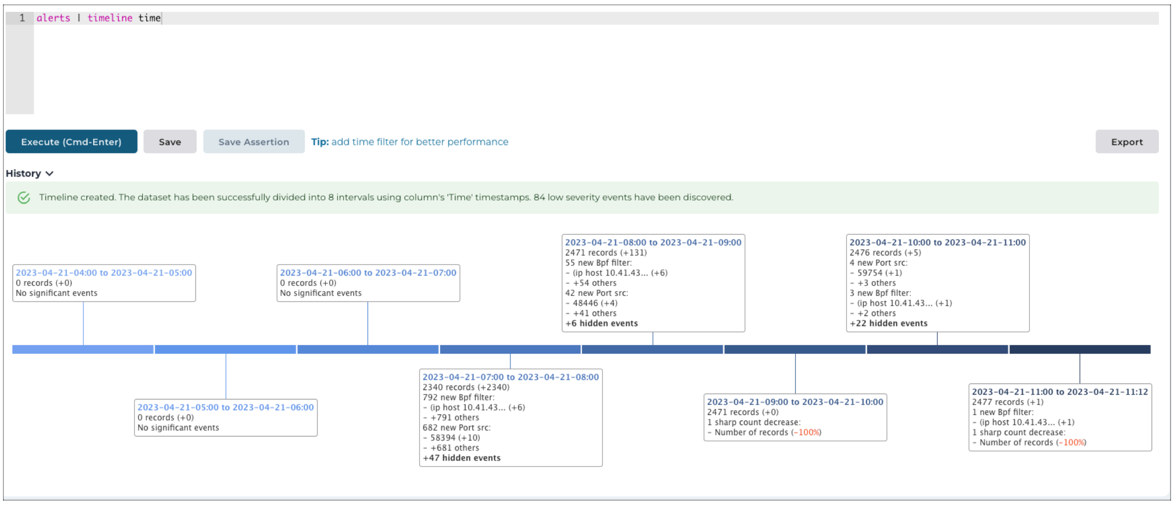
Timeline

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`

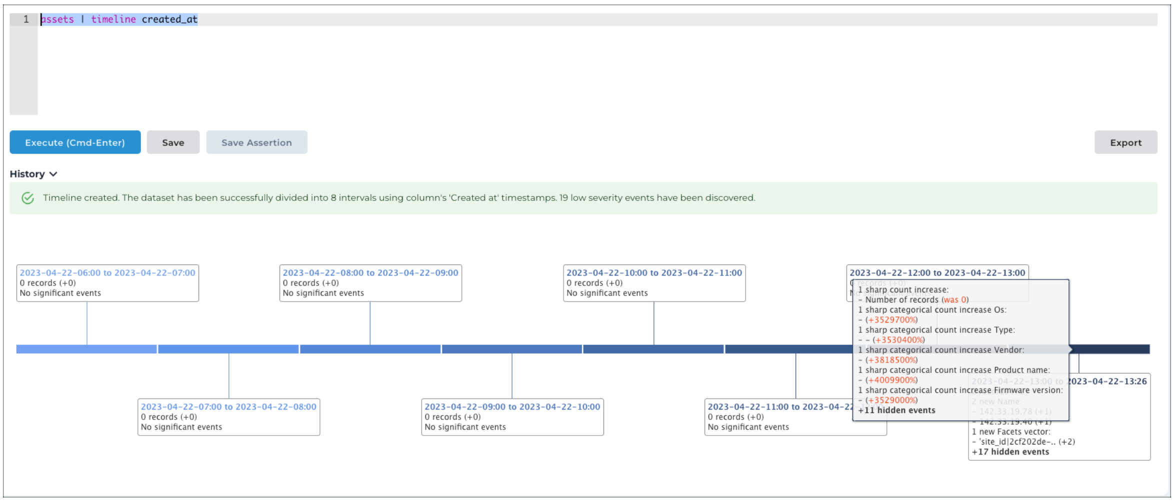


```
alerts | timeline time
```

Timeline created. The dataset has been successfully divided into 8 intervals using column's 'Time' timestamps. 84 low severity events have been discovered.

```
2023-04-21-04:00 to 2023-04-21-05:00
0 records (+0)
No significant events

2023-04-21-05:00 to 2023-04-21-06:00
0 records (+0)
No significant events

2023-04-21-06:00 to 2023-04-21-07:00
0 records (+0)
No significant events

2023-04-21-07:00 to 2023-04-21-08:00
2340 records (+2340)
792 new Bpf filter:
- (ip host 10.41.43... (+6)
- +791 others
682 new Port src:
- 58394 (+10)
- +681 others
+47 hidden events

2023-04-21-08:00 to 2023-04-21-09:00
2471 records (+131)
55 new Bpf filter:
- (ip host 10.41.43... (+6)
- +54 others
42 new Port src:
- 48446 (+4)
- +41 others
+6 hidden events

2023-04-21-09:00 to 2023-04-21-10:00
2471 records (+0)
1 sharp count decrease:
- Number of records (-100%)

2023-04-21-10:00 to 2023-04-21-11:00
2476 records (+5)
4 new Port src:
- 59754 (+1)
- +3 others
3 new Bpf filter:
- (ip host 10.41.43... (+1)
- +2 others
+22 hidden events

2023-04-21-11:00 to 2023-04-21-11:12
2477 records (+1)
1 new Bpf filter:
- (ip host 10.41.43... (+1)
1 sharp count decrease:
- Number of records (-100%)
```

Example: `assets | timeline created_at`



```
assets | timeline created_at
```

Timeline created. The dataset has been successfully divided into 8 intervals using column's 'Created at' timestamps. 19 low severity events have been discovered.

```
2023-04-22-06:00 to 2023-04-22-07:00
0 records (+0)
No significant events

2023-04-22-07:00 to 2023-04-22-08:00
0 records (+0)
No significant events

2023-04-22-08:00 to 2023-04-22-09:00
0 records (+0)
No significant events

2023-04-22-09:00 to 2023-04-22-10:00
0 records (+0)
No significant events

2023-04-22-10:00 to 2023-04-22-11:00
0 records (+0)
No significant events

2023-04-22-11:00 to 2023-04-22-12:00
0 records (+0)
No significant events

2023-04-22-12:00 to 2023-04-22-13:00
0 records (+0)
No significant events

1 sharp count increase:
- Number of records (was 0)
1 sharp categorical count increase Os:
- (+3529700%)
1 sharp categorical count increase Type:
- - (+3530400%)
1 sharp categorical count increase Vendor:
- (+3818500%)
1 sharp categorical count increase Product name:
- (+4009900%)
1 sharp categorical count increase Firmware version:
- (+3529000%)
+11 hidden events

2023-04-22-13:00 to 2023-04-22-13:26
2 new Name:
- 142.33.19.78 (+1)
- 142.33.19.40 (+1)
1 new Facets vector:
- 'site_id|2cf202de-.. (+2)
+17 hidden events
```

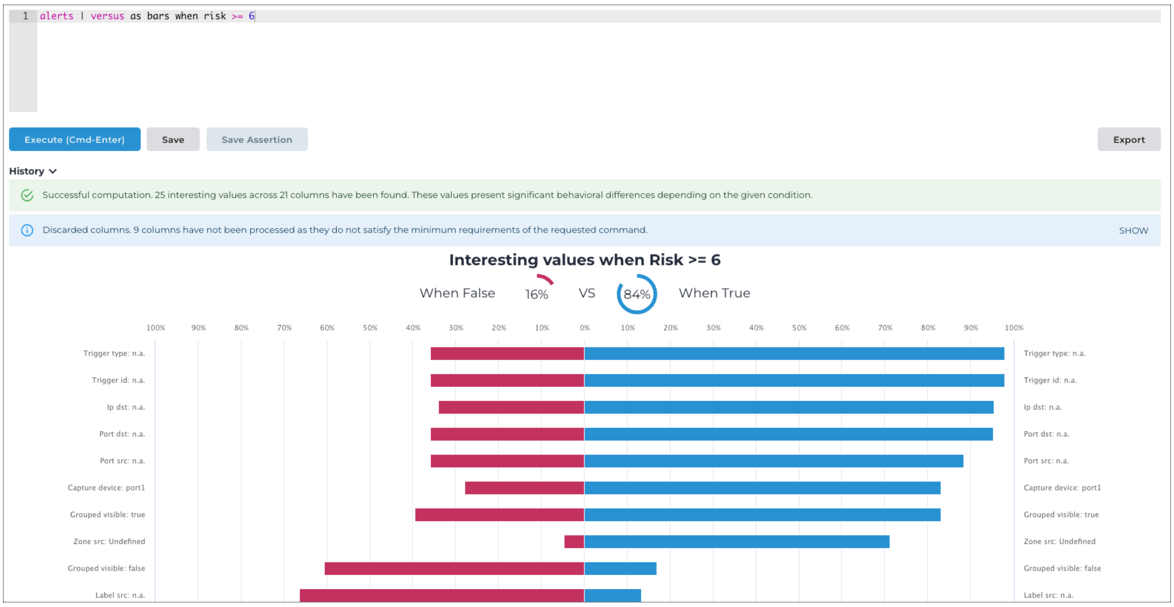
Versus

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`

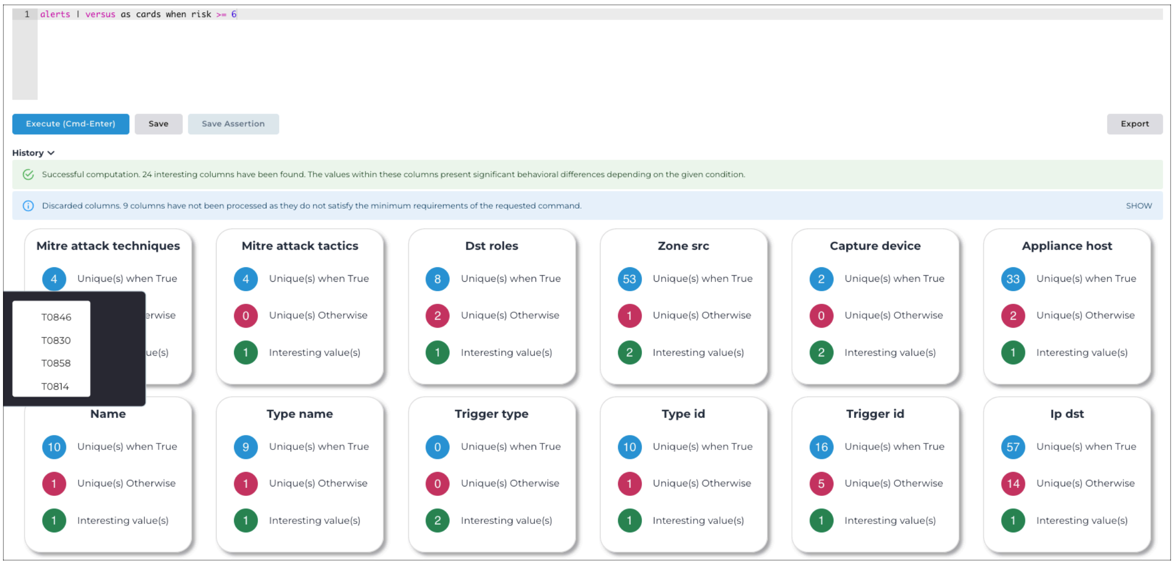


```
alerts | versus as bars when risk >= 6
```

Successful computation. 25 interesting values across 21 columns have been found. These values present significant behavioral differences depending on the given condition.

Discarded columns. 9 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

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



```
alerts | versus as cards when risk >= 6
```

Successful computation. 24 interesting columns have been found. The values within these columns present significant behavioral differences depending on the given condition.

Discarded columns. 9 columns have not been processed as they do not satisfy the minimum requirements of the requested command.

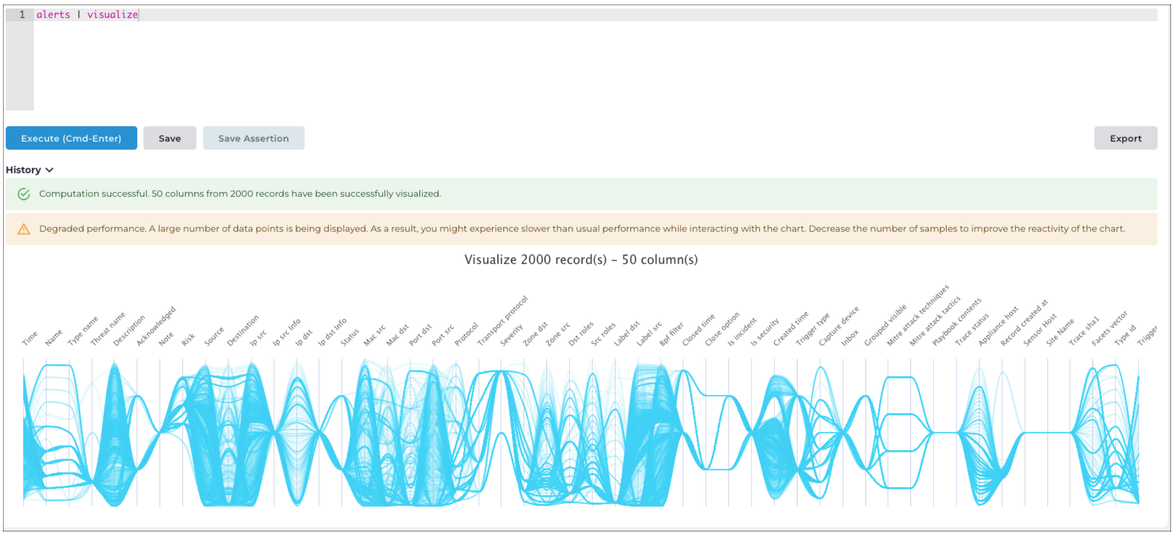
Visualize

Vantage IQ query example: Visualize.

Usage: <field> | visualize

Description: Provides a graphical visualization of the given rows.

Example: `alerts | visualize`



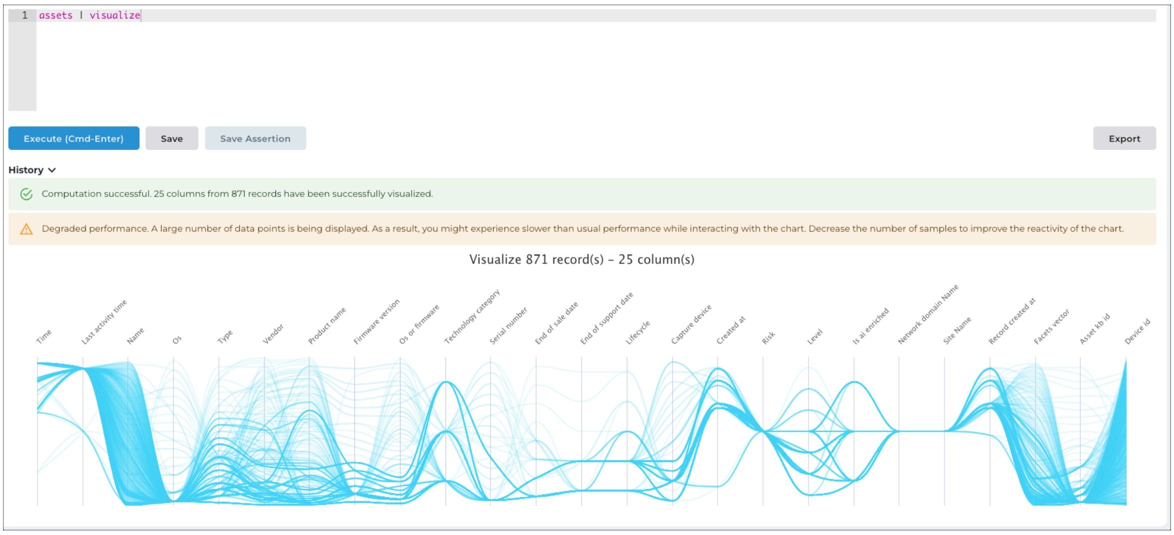
```
alerts | visualize
```

Computation successful. 50 columns from 2000 records have been successfully visualized.

Degraded performance. A large number of data points is being displayed. As a result, you might experience slower than usual performance while interacting with the chart. Decrease the number of samples to improve the reactivity of the chart.

Visualize 2000 record(s) – 50 column(s)

Example: `assets | visualize`



```
assets | visualize
```

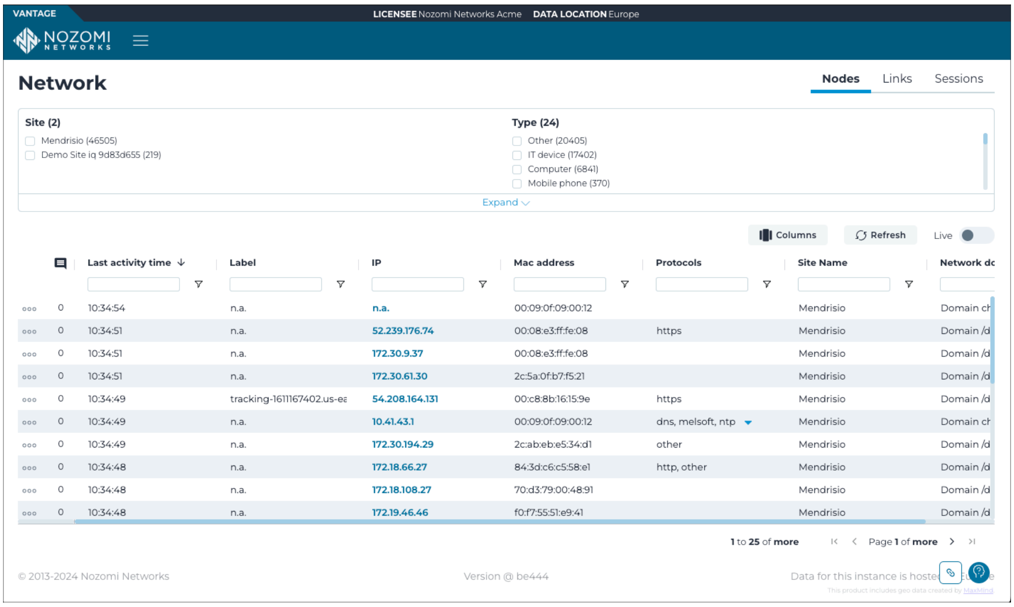
Computation successful. 25 columns from 871 records have been successfully visualized.

Degraded performance. A large number of data points is being displayed. As a result, you might experience slower than usual performance while interacting with the chart. Decrease the number of samples to improve the reactivity of the chart.

Visualize 871 record(s) – 25 column(s)

Chapter 9. Network

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



VANTAGE

LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

NOZOMI NETWORKS

Network

Site (2)

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

Type (24)

- □ Other (20405)
- □ IT device (17402)
- □ Computer (6841)
- □ Mobile phone (370)

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

This product includes geo data created by MaxMind

Figure 55. Network page

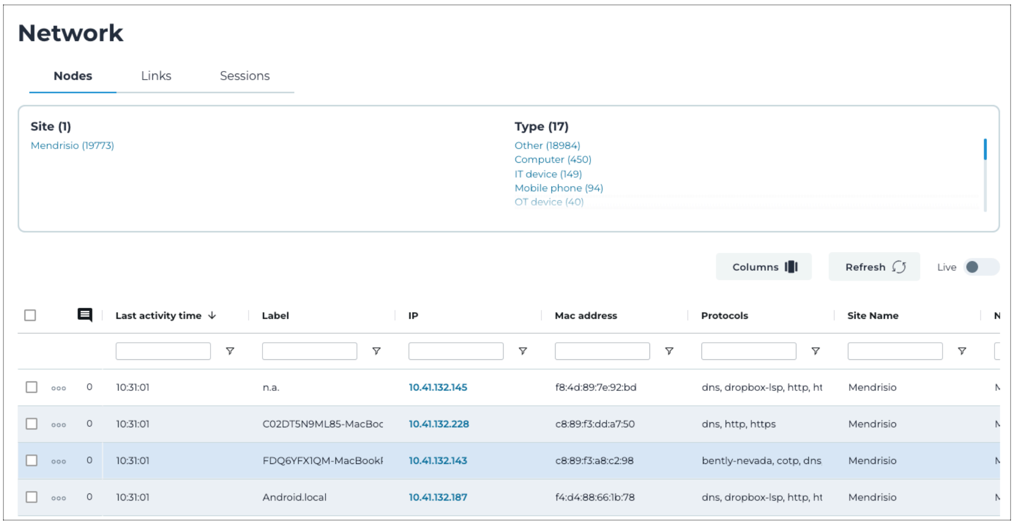
General

The **Network** page has these tabs:

- Nodes (on page 184)
- Links (on page 185)
- Sessions (on page 186)

Nodes

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



Site (1)
Mendrisio (19773)

Type (17)
Other (18984)
Computer (450)
IT device (149)
Mobile phone (94)
OT device (40)

□			Last activity time ↓	Label	IP	Mac address	Protocols	Site Name	N
□	○○○	0	10:31:01	n.a.	10.41.132.145	f8:4d:89:7e:92:bd	dns, dropbox-lsp, http, ht	Mendrisio	N
□	○○○	0	10:31:01	C02DT5N9ML85-MacBoc	10.41.132.228	c8:89:f3:dd:a7:50	dns, http, https	Mendrisio	N
□	○○○	0	10:31:01	FDQ6YFX1QM-MacBookI	10.41.132.143	c8:89:f3:a8:c2:98	bently-nevada, cotp, dns	Mendrisio	N
□	○○○	0	10:31:01	Android.local	10.41.132.187	f4:d4:88:66:1b:78	dns, dropbox-lsp, http, ht	Mendrisio	N

Figure 56. 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

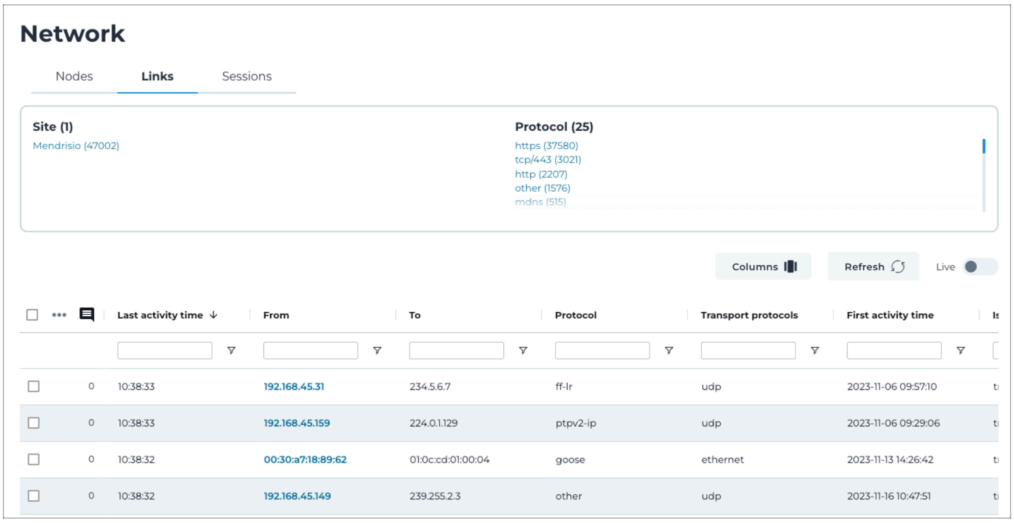
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



Network

Nodes Links Sessions

Site (1)

Mendrisio (47002)

Protocol (25)

https (37580)
tcp/443 (3021)
http (2207)
other (1576)
mdns (515)

☐		Last activity time ↓	From	To	Protocol	Transport protocols	First activity time	Is
☐	0	10:38:33	192.168.45.31	234.5.6.7	ff-lr	udp	2023-11-06 09:57:10	t
☐	0	10:38:33	192.168.45.159	224.0.1.129	ptpv2-ip	udp	2023-11-06 09:29:06	t
☐	0	10:38:32	00:30:a7:18:89:62	01:0c:cd:01:00:04	goose	ethernet	2023-11-13 14:26:42	t
☐	0	10:38:32	192.168.45.149	239.255.2.3	other	udp	2023-11-16 10:47:51	t

Figure 57. 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

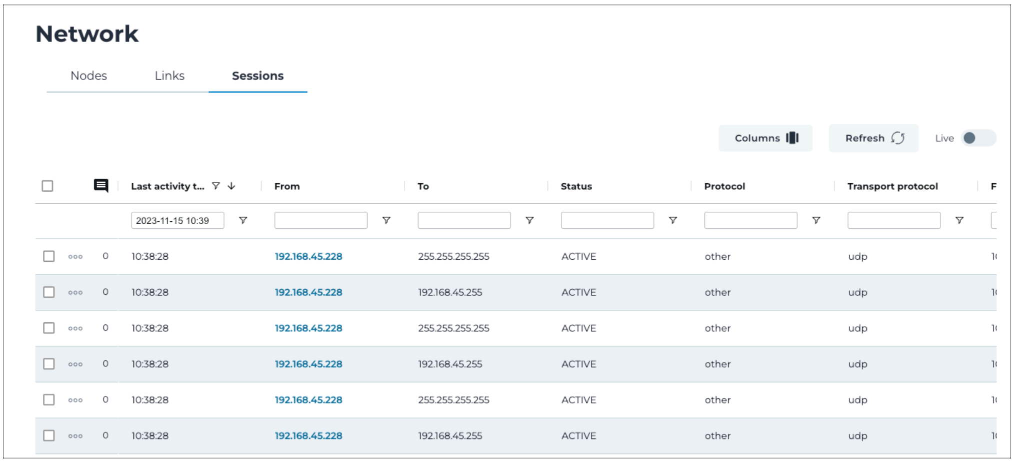
The **Refresh** ⟳ icon lets you immediately refresh the current view.

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.*



Network

□			Last activity t...	From	To	Status	Protocol	Transport protocol	F
			2023-11-15 10:39						
□	○○○	0	10:38:28	192.168.45.228	255.255.255.255	ACTIVE	other	udp	1
□	○○○	0	10:38:28	192.168.45.228	192.168.45.255	ACTIVE	other	udp	1
□	○○○	0	10:38:28	192.168.45.228	255.255.255.255	ACTIVE	other	udp	1
□	○○○	0	10:38:28	192.168.45.228	192.168.45.255	ACTIVE	other	udp	1
□	○○○	0	10:38:28	192.168.45.228	255.255.255.255	ACTIVE	other	udp	1
□	○○○	0	10:38:28	192.168.45.228	192.168.45.255	ACTIVE	other	udp	1

Figure 58. 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

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

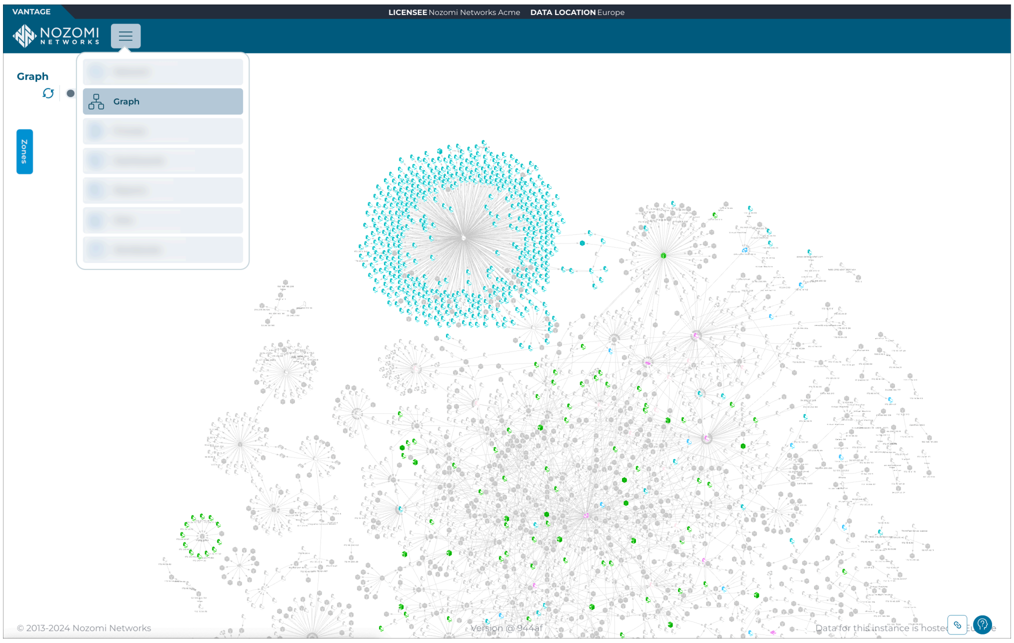
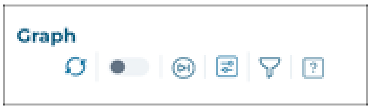

VANTAGE
LICENSEE Nozomi Networks Acme
DATA LOCATION Europe
NOZOMI NETWORKS
Graph
Graph
Zones
© 2013-2024 Nozomi Networks
Data for this instance is hosted

Figure 59. 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

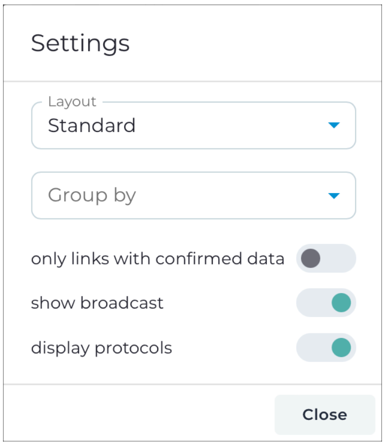
The **Live** ● toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

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

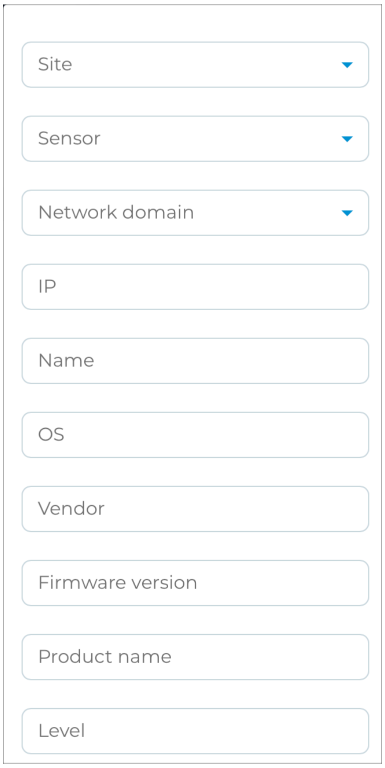
Layout
Standard

Group by

only links with confirmed data ○
show broadcast ●
display protocols ●

Filter

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



Site

Sensor

Network domain

IP

Name

OS

Vendor

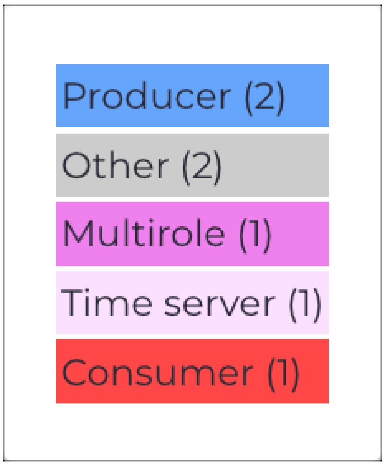
Firmware version

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.



Producer (2)

Other (2)

Multirole (1)

Time server (1)

Consumer (1)

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.

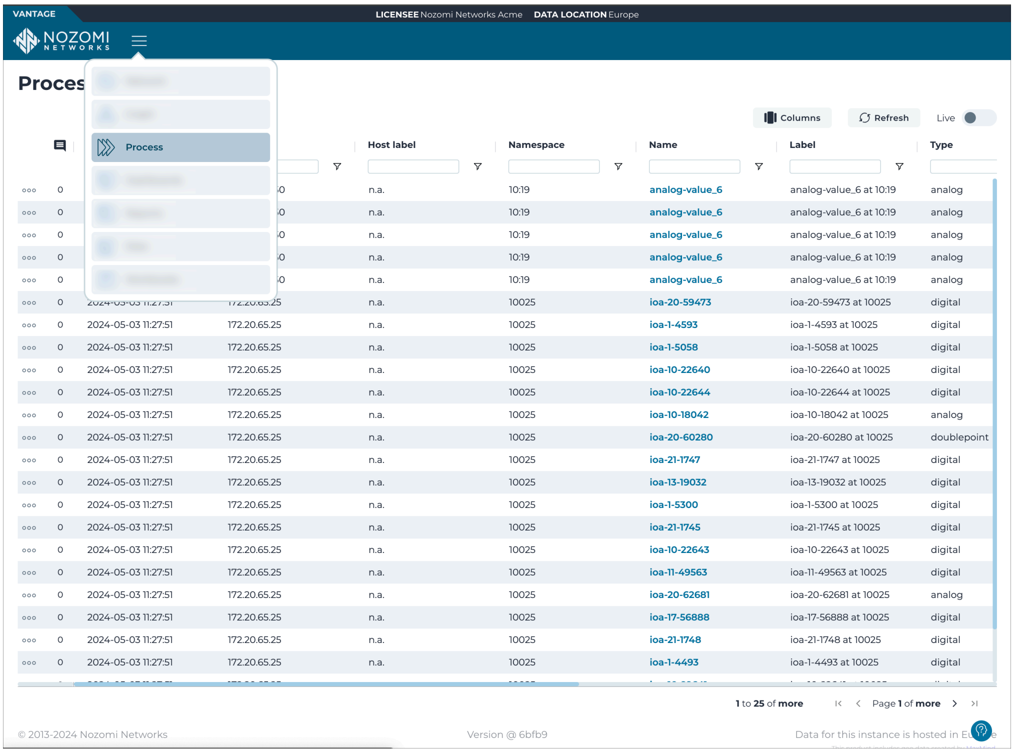
Graph navigation

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 191). An overview will show in the drawer in the left

Chapter 11. Process

*The **Process** page shows a list of processes in your environment. Processes are a set of repeatable functions that a business does to deliver a core value.*



VANTAGE LICENSEE Nozomi Networks Acme DATA LOCATION Europe

Proces

	🗨			Host label	Namespace	Name	Label	Type
○○○	0			n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
○○○	0			n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
○○○	0			n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
○○○	0			n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
○○○	0			n.a.	10:19	analog-value_6	analog-value_6 at 10:19	analog
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-20-59473	ioa-20-59473 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-1-4593	ioa-1-4593 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-1-5058	ioa-1-5058 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-10-22640	ioa-10-22640 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-10-22644	ioa-10-22644 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-10-18042	ioa-10-18042 at 10025	analog
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-20-60280	ioa-20-60280 at 10025	doublepoint
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-21-1747	ioa-21-1747 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-13-19032	ioa-13-19032 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-1-5300	ioa-1-5300 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-21-1745	ioa-21-1745 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-10-22643	ioa-10-22643 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-11-49563	ioa-11-49563 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-20-62681	ioa-20-62681 at 10025	analog
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-17-56888	ioa-17-56888 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-21-1748	ioa-21-1748 at 10025	digital
○○○	0	2024-05-03 11:27:51	172.20.65.25	n.a.	10025	ioa-1-4493	ioa-1-4493 at 10025	digital

1 to 25 of more Page 1 of more

© 2013-2024 Nozomi Networks Version @ 6bfb9 Data for this instance is hosted in Europe

Figure 60. 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 193) page opens.

2. Choose a method to open the actions menu.

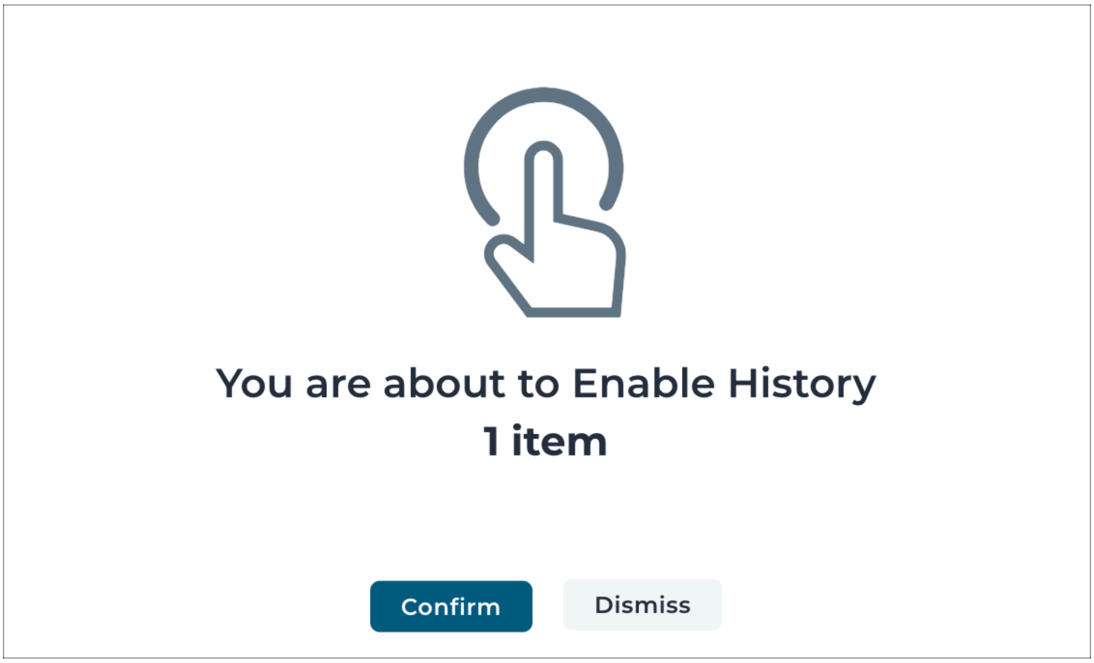
   Choose from:

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

3. Select **Enable History**.

   Result: A dialog shows.

4. Select **Confirm**.



You are about to Enable History

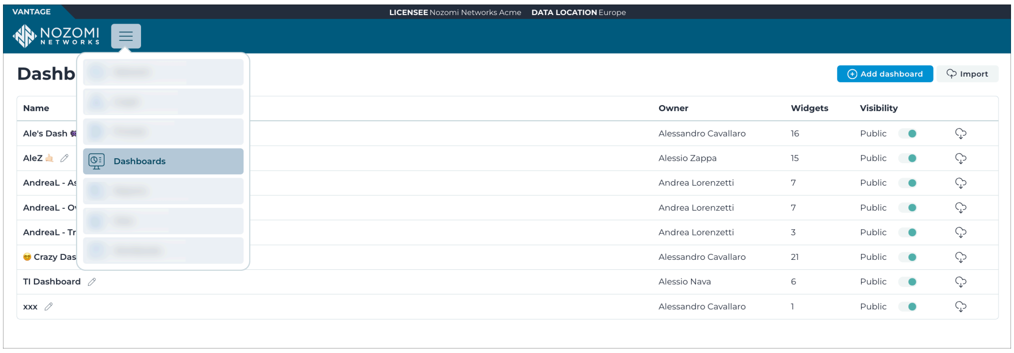
1 item

Results

History has been enabled.

Chapter 12. Dashboards

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



Dashb

Name	Owner	Widgets	Visibility
Ale's Dash	Alessandro Cavallaro	16	Public
AleZ	Alessio Zappa	15	Public
AndreaL - As	Andrea Lorenzetti	7	Public
AndreaL - O	Andrea Lorenzetti	7	Public
AndreaL - Tr	Andrea Lorenzetti	3	Public
Crazy Das	Alessandro Cavallaro	21	Public
TI Dashboard	Alessio Nava	6	Public
xxx	Alessandro Cavallaro	1	Public

Figure 61. Dashboards page

Add dashboard

This button lets you Create a dashboard (on page 200).

Import

This button lets you Import a dashboard (on page 201).

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 197) 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 197) 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 197) 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 197) page opens.

2. Select the applicable dashboard.
3. In the top right section, select **Add widget**.

   Result: The **Edit widget** page opens.

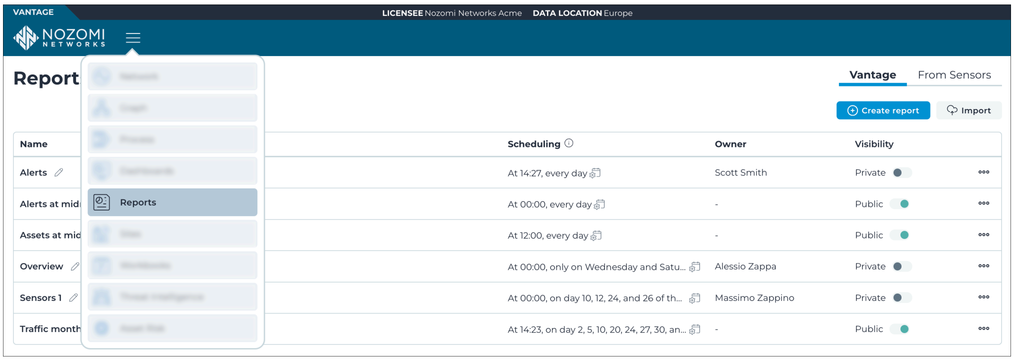
4. From the **Widget** dropdown, select a widget type.
5. **Optional:** In the **Title** field, edit the title of the widget as necessary.
6. Select **Apply**.

Results

The widget has been added to the dashboard.

Chapter 13. Reports

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



Report

Name	Scheduling	Owner	Visibility
Alerts	At 14:27, every day	Scott Smith	Private
Alerts at mid	At 00:00, every day	-	Public
Assets at mid	At 12:00, every day	-	Public
Overview	At 00:00, only on Wednesday and Satu...	Alessio Zappa	Private
Sensors 1	At 00:00, on day 10, 12, 24, and 26 of th...	Massimo Zappino	Private
Traffic month	At 14:23, on day 2, 5, 10, 20, 24, 27, 30, an...	-	Public

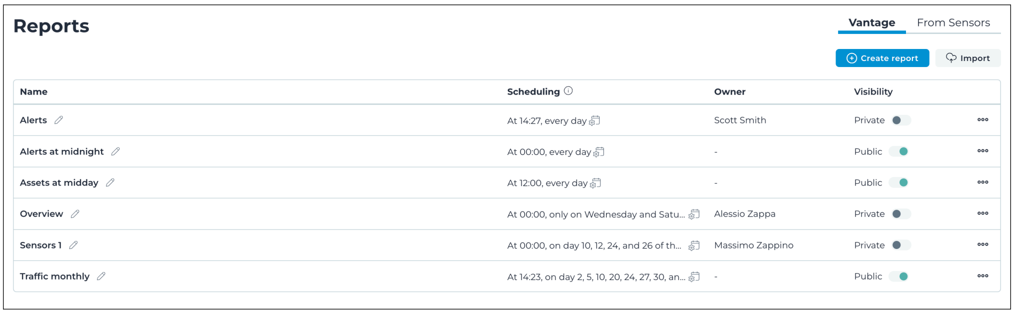
Figure 62. Reports page

The **Reports** page has these tabs:

- Vantage (on page 208)
- From Sensors (on page 213)

Vantage

*The **Vantage** page shows all the reports that have been created in Vantage.*



Reports

Name	Scheduling	Owner	Visibility	
Alerts	At 14:27, every day	Scott Smith	Private	•••
Alerts at midnight	At 00:00, every day	-	Public	•••
Assets at midday	At 12:00, every day	-	Public	•••
Overview	At 00:00, only on Wednesday and Satu...	Alessio Zappa	Private	•••
Sensors 1	At 00:00, on day 10, 12, 24, and 26 of th...	Massimo Zappino	Private	•••
Traffic monthly	At 14:23, on day 2, 5, 10, 20, 24, 27, 30, an...	-	Public	•••

Figure 63. Vantage page

Create report

This lets you Create a report (on page 209).

Import

This lets you Import a report (on page 212).

Name

The name of the report. To modify the name, you can select the pencil icon, modify the name and select the tick icon.

Scheduling

The details of when the report is scheduled for creation.

Owner

The person that created the report.

Visibility

This toggle lets you choose whether the report is visible to a private or a public audience.

Actions menu

The actions menu gives you access to these options:

- Edit (on page 214)
- Settings (on page 214)
- Export (on page 215)
- Delete (on page 215)

Related information

From Sensors (on page 213)

Create a report

Learn how to create and schedule a custom report using predefined templates, recurrence settings, and visibility options in your organization.

About this task

The creation and scheduling of custom reports lets you streamline how critical information is shared within your organization. The use of predefined templates helps you quickly design reports tailored to specific needs, such as tracking vulnerabilities, monitoring traffic, or providing an overview of assets. The recurrence settings and visibility options make sure that the reports are generated on time and reach the correct audience, enhancing collaboration and decision-making across teams.

Procedure

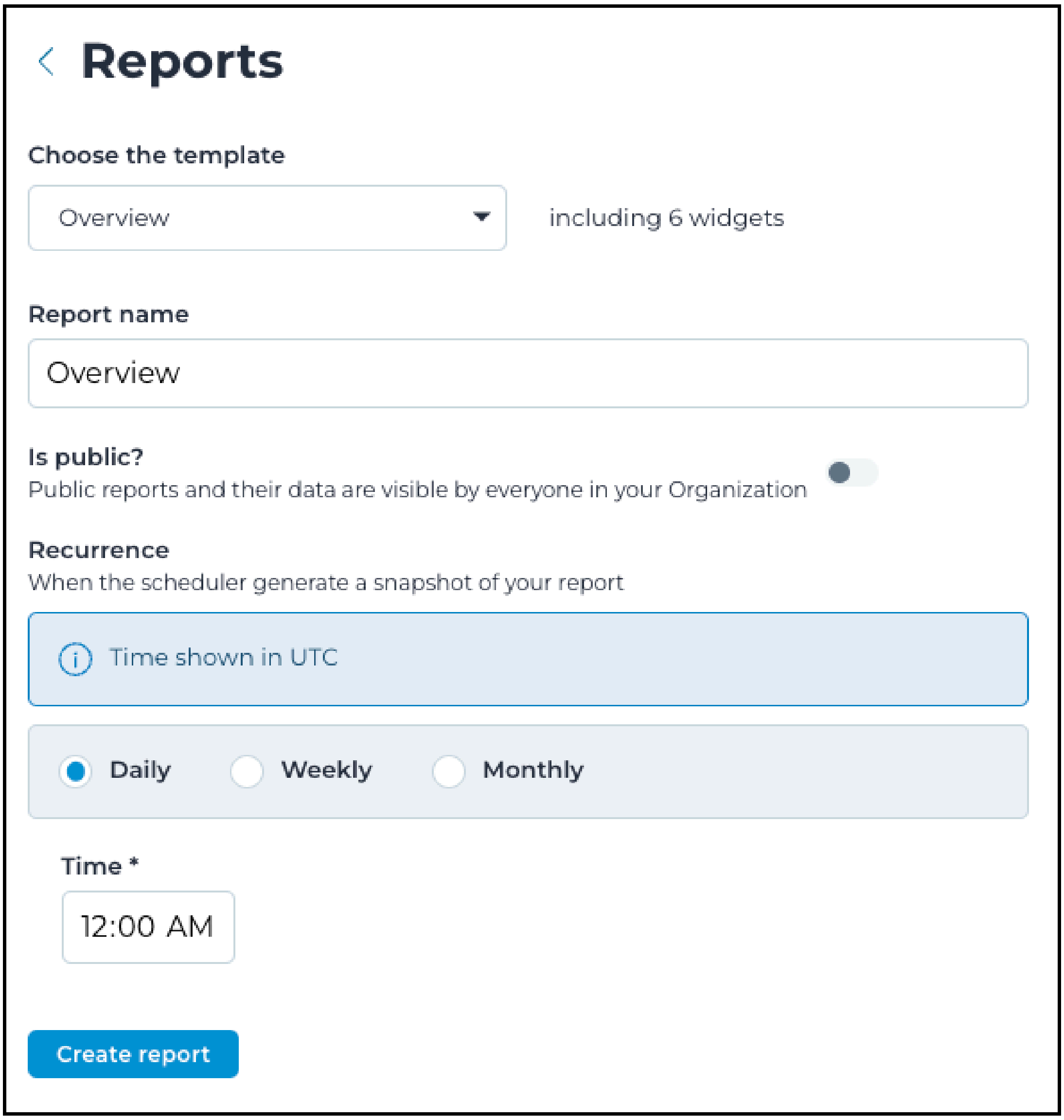
1. In the top navigation bar, select ☰ **> Reports**.

   Result: The Reports (on page 205) page opens.

2. In the top right corner, select **Create report**.

3. **Optional:**

   From the **Choose a template** dropdown, select an option.



Reports

Choose the template

Overview — including 6 widgets

Report name

Overview

Is public?

Public reports and their data are visible by everyone in your Organization

Recurrence

When the scheduler generate a snapshot of your report

Time shown in UTC

● Daily ○ Weekly ○ Monthly

Time *

12:00 AM

   You can choose from these options;

   - Empty
   - Alerts
   - Assets
   - Overview
   - Sensors
   - Traffic
   - Vulnerabilities

4. In the **Report name** field, enter a name for the report.
5. **Optional:** To make the report visible to everyone in your organization, set the **Is public?** toggle to on.

6. In the **Recurrence** section, select one of these radio buttons:

   Choose from:

   - Daily
   - Weekly
   - Monthly
7. In the **Time** field, set the time that the report will be generated.
8. Select **Create report**.

Results

The report has been scheduled for creation.

Import a report

Learn how to import a report that was previously created in Vantage.

Procedure

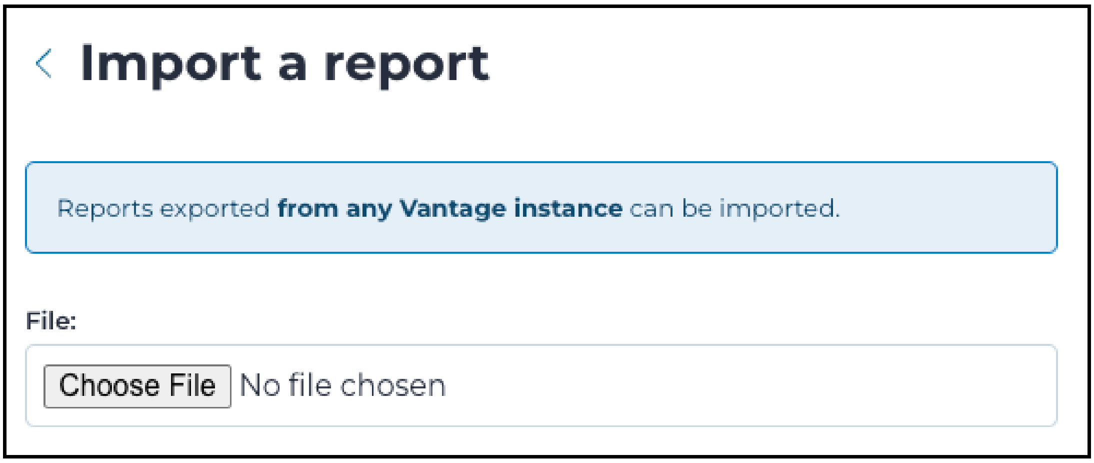
1. In the top navigation bar, select ☰ **> Reports**.

   Result: The Reports (on page 205) page opens.

2. In the top right corner, select **Import**.

   Result: The **Import a report** page opens.

3. Select **Choose File**.



Import a report

Reports exported **from any Vantage instance** can be imported.

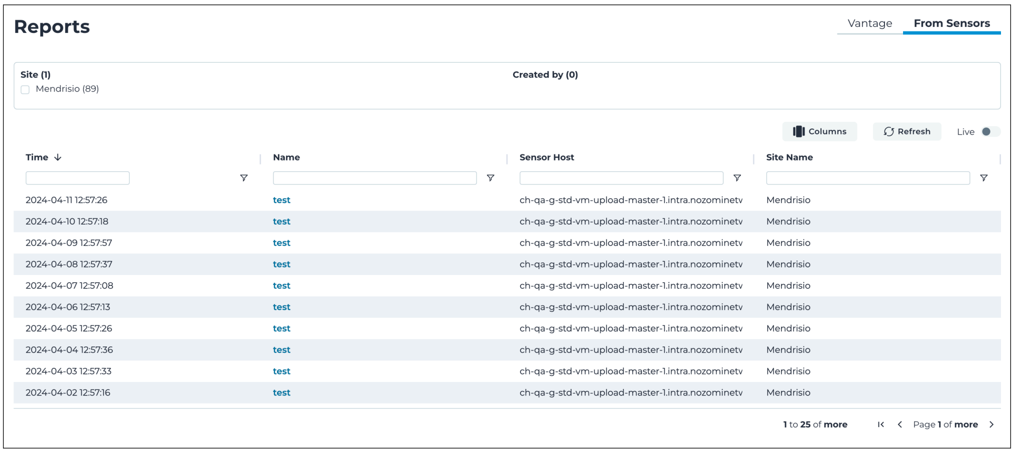
File:

4. Select the report file.
   The report will be in *JSON* format.

5. Select **Confirm**.

From Sensors

*The **From Sensors** page shows all the reports that have been created on sensors in your system.*



Time ↓	Name	Sensor Host	Site Name
2024-04-11 12:57:26	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-10 12:57:18	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-09 12:57:57	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-08 12:57:37	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-07 12:57:08	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-06 12:57:13	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-05 12:57:26	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-04 12:57:36	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-03 12:57:33	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio
2024-04-02 12:57:16	test	ch-qa-g-std-vm-upload-master-1.intra.nozominetv	Mendrisio

1 to 25 of more   Page 1 of more

Figure 64. From Sensors page

Site

This shows the site location of the sensors that created the report.

Columns

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

Refresh

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

Live

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

Related information

Vantage (on page 208)

Table interactions

Actions menu

Edit a report

Learn how to use the actions menu to edit reports.

Procedure

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

   Result: The Reports (on page 205) page opens.

2. In the table, select the ••• icon.
3. Select **Edit**.

   Result: The report opens.

4. Edit the report as necessary.
5. Select **Apply**.

Results

The report has been edited.

Edit the settings of a report

Learn how to use the actions menu to edit the settings of a report.

Procedure

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

   Result: The Reports (on page 205) page opens.

2. In the table, select the ••• icon.
3. Select **Settings**.

   Result: The report opens.

4. Edit the report settings as necessary.
5. Select **Edit report**.

Results

The report has been edited.

Export a report

Learn how to use the actions menu to export reports.

Procedure

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

   Result: The Reports (on page 205) page opens.

2. In the table, select the ••• icon.
3. Select **Export**.

Results

The report downloads in *JSON* format.

Delete a report

You can use the actions menu to delete reports.

Procedure

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

   Result: The Reports (on page 205) page opens.

2. In the table, select the ••• icon.
3. Select **Delete**.

   Result: A dialog shows.

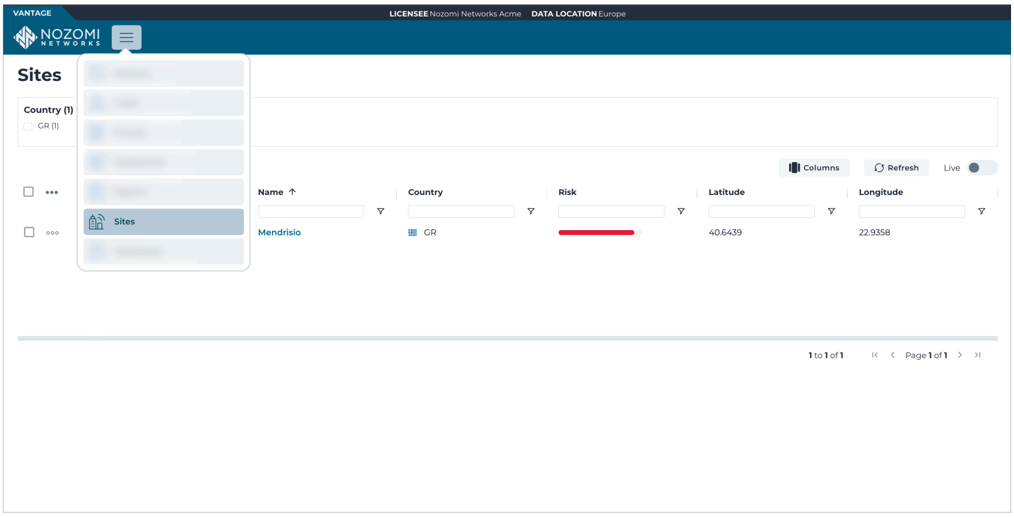
4. Select **OK**.

Results

The report has been deleted.

Chapter 14. Sites

*The **Sites** page shows all the geographical locations of the assets in your system. It lets you associate a site to one or more network domains. You can also add details such as the country or city of the site.*



Name	Country	Risk	Latitude	Longitude
Mendrisio	GR		40.6439	22.9358

1 to 1 of 1 Page 1 of 1

Figure 65. 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 217) page opens.

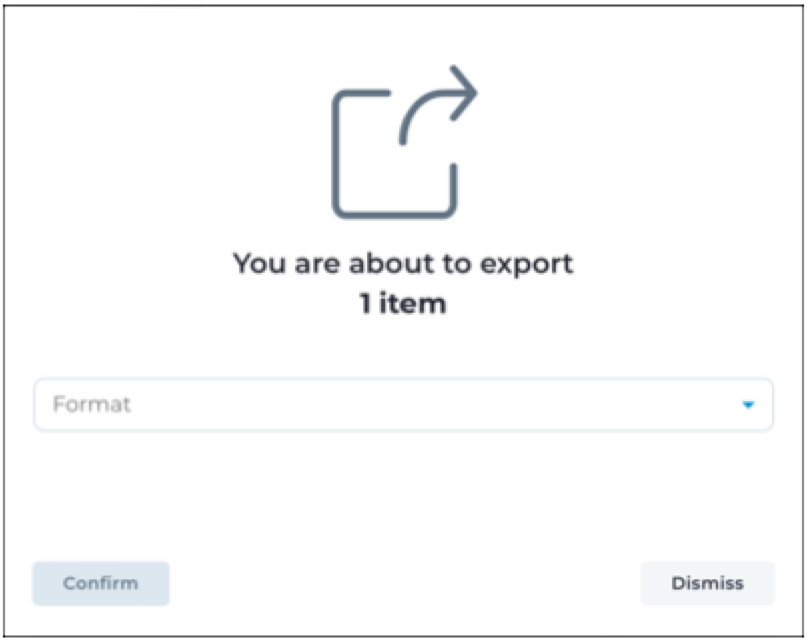
2. Choose a method to open the actions menu.

   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**.



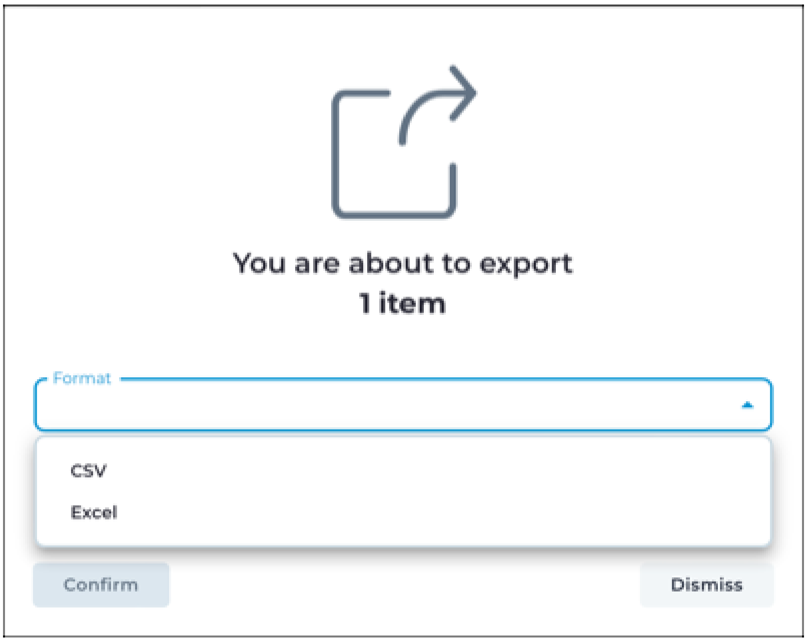
You are about to export
1 item

   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.

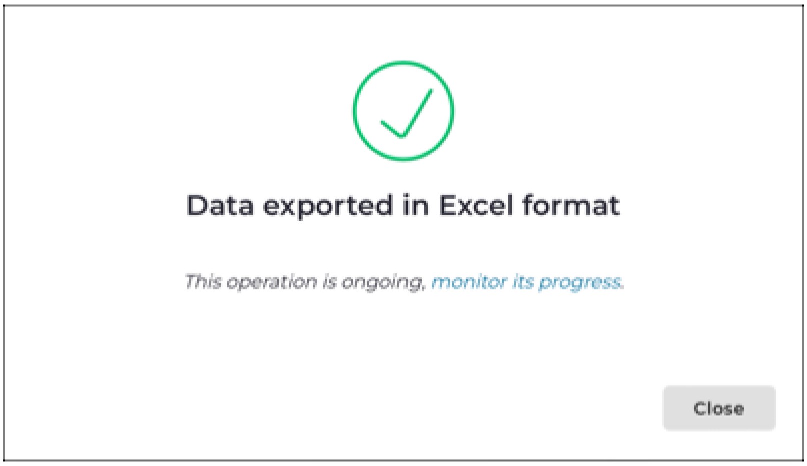


You are about to export
1 item

7. Select **Confirm**.

   Result: A confirmation dialog shows.

8. Select **Close**.



Data exported in Excel format

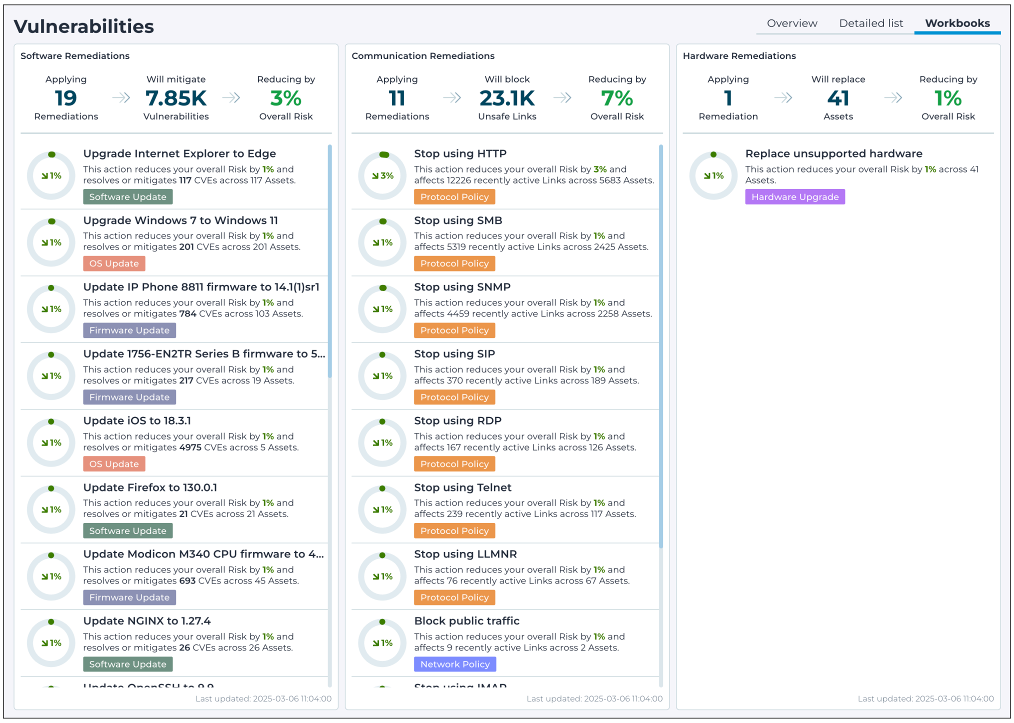
This operation is ongoing, monitor its progress.

Results

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

Chapter 15. Workbooks

*The **Workbooks** page shows recommended courses of action that can improve your network security. Generated through machine learning, workbooks highlight the vulnerabilities currently creating the highest risk exposure.*



Vulnerabilities

Software Remediations

Applying **19** Remediations → Will mitigate **7.85K** Vulnerabilities → Reducing by **3%** Overall Risk

- ↘1% **Upgrade Internet Explorer to Edge**
  This action reduces your overall Risk by **1%** and resolves or mitigates **117** CVEs across 117 Assets.
  Software Update
- ↘1% **Upgrade Windows 7 to Windows 11**
  This action reduces your overall Risk by **1%** and resolves or mitigates **201** CVEs across 201 Assets.
  OS Update
- ↘1% **Update IP Phone 8811 firmware to 14.1(1)sr1**
  This action reduces your overall Risk by **1%** and resolves or mitigates **784** CVEs across 103 Assets.
  Firmware Update
- ↘1% **Update 1756-EN2TR Series B firmware to 5...**
  This action reduces your overall Risk by **1%** and resolves or mitigates **217** CVEs across 19 Assets.
  Firmware Update
- ↘1% **Update iOS to 18.3.1**
  This action reduces your overall Risk by **1%** and resolves or mitigates **4975** CVEs across 5 Assets.
  OS Update
- ↘1% **Update Firefox to 130.0.1**
  This action reduces your overall Risk by **1%** and resolves or mitigates **21** CVEs across 21 Assets.
  Software Update
- ↘1% **Update Modicon M340 CPU firmware to 4...**
  This action reduces your overall Risk by **1%** and resolves or mitigates **693** CVEs across 45 Assets.
  Firmware Update
- ↘1% **Update NGINX to 1.27.4**
  This action reduces your overall Risk by **1%** and resolves or mitigates **26** CVEs across 26 Assets.
  Software Update
- **Update OpenSSH to 9.9**

Last updated: 2025-03-06 11:04:00

Communication Remediations

Applying **11** Remediations → Will block **23.1K** Unsafe Links → Reducing by **7%** Overall Risk

- ↘3% **Stop using HTTP**
  This action reduces your overall Risk by **3%** and affects 12226 recently active Links across 5683 Assets.
  Protocol Policy
- ↘1% **Stop using SMB**
  This action reduces your overall Risk by **1%** and affects 5319 recently active Links across 2425 Assets.
  Protocol Policy
- ↘1% **Stop using SNMP**
  This action reduces your overall Risk by **1%** and affects 4459 recently active Links across 2258 Assets.
  Protocol Policy
- ↘1% **Stop using SIP**
  This action reduces your overall Risk by **1%** and affects 370 recently active Links across 189 Assets.
  Protocol Policy
- ↘1% **Stop using RDP**
  This action reduces your overall Risk by **1%** and affects 167 recently active Links across 126 Assets.
  Protocol Policy
- ↘1% **Stop using Telnet**
  This action reduces your overall Risk by **1%** and affects 239 recently active Links across 117 Assets.
  Protocol Policy
- ↘1% **Stop using LLMNR**
  This action reduces your overall Risk by **1%** and affects 76 recently active Links across 67 Assets.
  Protocol Policy
- ↘1% **Block public traffic**
  This action reduces your overall Risk by **1%** and affects 9 recently active Links across 2 Assets.
  Network Policy
- **Stop using IMAP**

Last updated: 2025-03-06 11:04:00

Hardware Remediations

Applying **1** Remediation → Will replace **41** Assets → Reducing by **1%** Overall Risk

- ↘1% **Replace unsupported hardware**
  This action reduces your overall Risk by **1%** across 41 Assets.
  Hardware Upgrade

Last updated: 2025-03-06 11:04:00

Figure 66. 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 226)

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 155) 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 153).

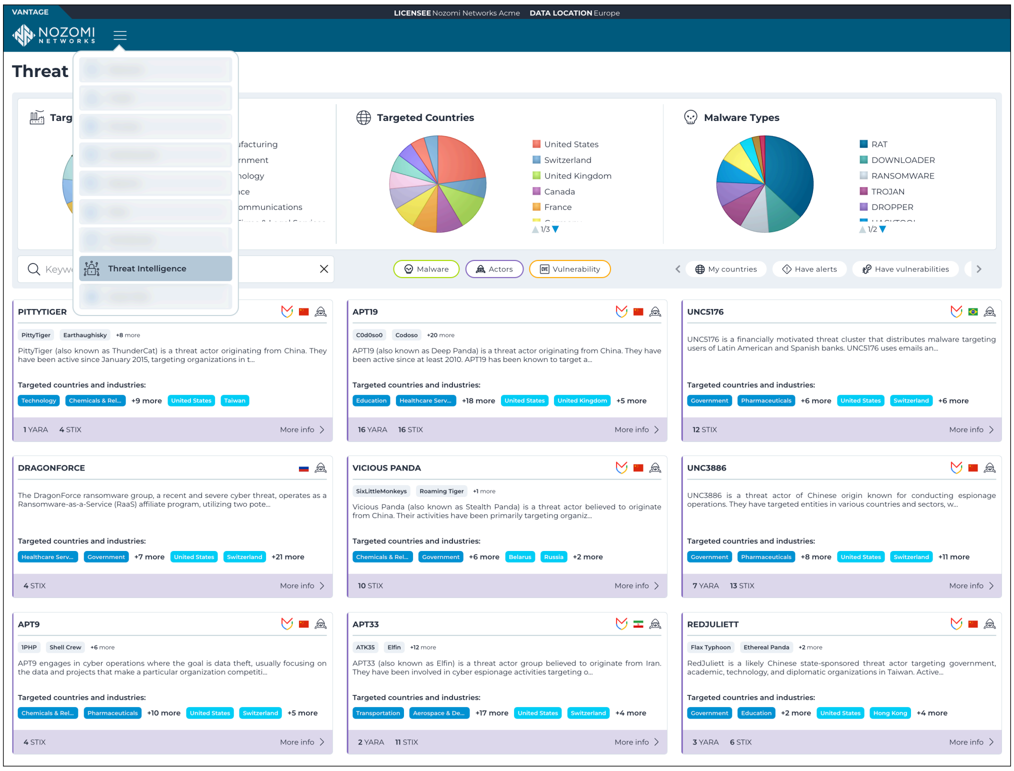
   > **Note:**
   > You should create a plan to take the recommended action. For example, a workbook might recommend that you upgrade all assets that run an old application version. In this case, you should create a maintenance schedule and take the necessary steps to update those applications to the latest, secure version.

Related information

Workbooks (on page 155)

Chapter 16. Threat Intelligence

*The **Threat Intelligence** page shows an overview of all of the available threat cards and categories. It also lets you filter the threat cards to show only malware, threat actors, or vulnerabilities*



PITTYTIGER

PittyTiger Earthaughisky +8 more

PittyTiger (also known as ThunderCat) is a threat actor originating from China. They have been active since January 2015, targeting organizations in t...

Targeted countries and industries:

Technology Chemicals & Rel... +9 more United States Taiwan

1 YARA 4 STIX More info

APT19

C0d0so0 Codoso +20 more

APT19 (also known as Deep Panda) is a threat actor originating from China. They have been active since at least 2010. APT19 has been known to target a...

Targeted countries and industries:

Education Healthcare Serv... +18 more United States United Kingdom +5 more

16 YARA 16 STIX More info

UNC5176

UNC5176 is a financially motivated threat cluster that distributes malware targeting users of Latin American and Spanish banks. UNC5176 uses emails an...

Targeted countries and industries:

Government Pharmaceuticals +6 more United States Switzerland +6 more

12 STIX More info

DRAGONFORCE

The DragonForce ransomware group, a recent and severe cyber threat, operates as a Ransomware-as-a-Service (RaaS) affiliate program, utilizing two pote...

Targeted countries and industries:

Healthcare Serv... Government +7 more United States Switzerland +21 more

4 STIX More info

VICIOUS PANDA

SixLittleMonkeys Roaming Tiger +1 more

Vicious Panda (also known as Stealth Panda) is a threat actor believed to originate from China. Their activities have been primarily targeting organiz...

Targeted countries and industries:

Chemicals & Rel... Government +6 more Belarus Russia +2 more

10 STIX More info

UNC3886

UNC3886 is a threat actor of Chinese origin known for conducting espionage operations. They have targeted entities in various countries and sectors, w...

Targeted countries and industries:

Government Pharmaceuticals +8 more United States Switzerland +11 more

7 YARA 13 STIX More info

APT9

1PHP Shell Crew +6 more

APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competiti...

Targeted countries and industries:

Chemicals & Rel... Pharmaceuticals +10 more United States Switzerland +5 more

4 STIX More info

APT33

ATK35 Elfin +12 more

APT33 (also known as Elfin) is a threat actor group believed to originate from Iran. They have been involved in cyber espionage activities targeting o...

Targeted countries and industries:

Transportation Aerospace & De... +17 more United States Switzerland +4 more

2 YARA 11 STIX More info

REDJULIETT

Flax Typhoon Ethereal Panda +2 more

RedJuliett is a likely Chinese state-sponsored threat actor targeting government, academic, technology, and diplomatic organizations in Taiwan. Active...

Targeted countries and industries:

Government Education +2 more United States Hong Kong +4 more

3 YARA 6 STIX More info

Figure 67. Threat Intelligence page

Targeted Industries

This section lets you filter cards based on any of the selected industries in the chart.

Targeted Countries

This section lets you filter cards on any of the selected countries.

Malware Types

This section lets you select which types of malware show.

Search bar

This lets you search the Threat Intelligence based on these attributes:

- Aliases
- Description
- Filenames
- Malware types
- Name
- Origin country
- *Structured Threat Information Expression (STIX)* domains
- *STIX IP* addresses
- *STIX URLs*

- Targeted country
- Targeted industry
- Trigger *IDs*
- *STIX* hashes

Malware

This button lets you filter malware cards based on any of the selected types. For more details, see Malware (on page 231).

Actors

This button lets you filter the content that shows below to only threat actors. For more details, see Actors (on page 233).

Vulnerability

This button lets you filter the content that shows below to only vulnerabilities. This section shows all known *CVEs*. For more details, see Vulnerability (on page 235).

My countries

This button lets you filter the threat cards to show only content that is relevant for the countries that your organization has sites in.

Have alerts

This button lets you filter the threat cards to show only content that have associated alerts.

Have vulnerabilities

This button lets you filter the threat cards to show only content that have associated vulnerabilities.

High risk

This button lets you filter the threat cards to show only content that have a high risk score.

Actively exploited

This button lets you filter the threat cards to show only vulnerabilities that are known to have been exploited.

Threat cards

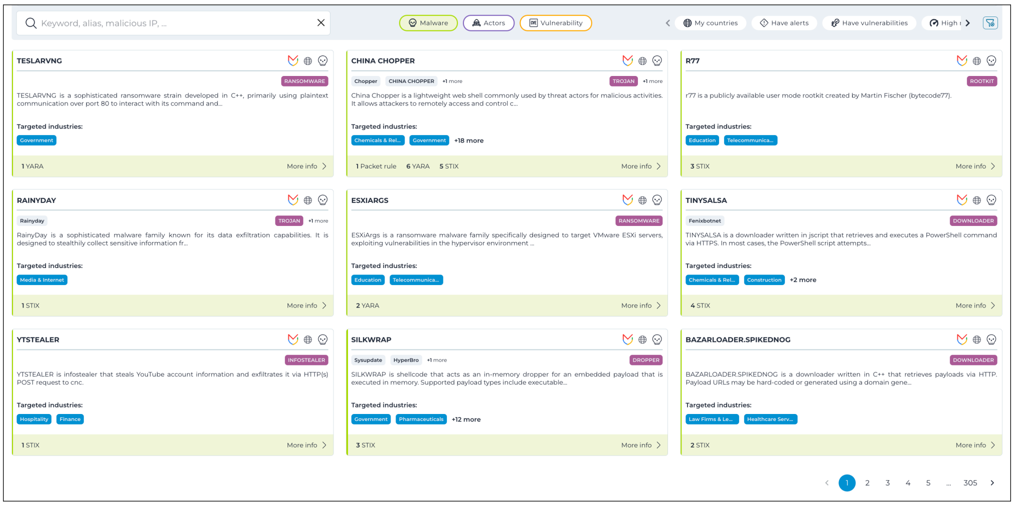
For more details, see:

- Malware threat cards (on page 231)
- Actors threat cards (on page 233)
- Vulnerability threat cards (on page 235)

Malware

*Learn how the **Malware** page shows malware-specific attributes and associated threat cards.*

Malware filter



TESLARVNG

RANSOMWARE

TESLARVNG is a sophisticated ransomware strain developed in C++, primarily using plaintext communication over port 80 to interact with its command and...

Targeted industries: Government

1 YARA More info

CHINA CHOPPER

Chopper CHINA CHOPPER +1 more TROJAN +1 more

China Chopper is a lightweight web shell commonly used by threat actors for malicious activities. It allows attackers to remotely access and control c...

Targeted industries: Chemicals & Rel... Government +18 more

1 Packet rule 6 YARA 5 STIX More info

R77

ROOTKIT

r77 is a publicly available user mode rootkit created by Martin Fischer (bytecode77).

Targeted industries: Education Telecommunica...

3 STIX More info

RAINYDAY

Rainyday TROJAN +1 more

RainyDay is a sophisticated malware family known for its data exfiltration capabilities. It is designed to stealthily collect sensitive information fr...

Targeted industries: Media & Internet

1 STIX More info

ESXIARGS

RANSOMWARE

ESXiArgs is a ransomware malware family specifically designed to target VMware ESXi servers, exploiting vulnerabilities in the hypervisor environment ...

Targeted industries: Education Telecommunica...

2 YARA More info

TINYSALSA

Fenixbotnet DOWNLOADER

TINYSALSA is a downloader written in jscript that retrieves and executes a PowerShell command via HTTPS. In most cases, the PowerShell script attempts...

Targeted industries: Chemicals & Rel... Construction +2 more

4 STIX More info

YTSTEALER

INFOSTEALER

YTSTEALER is infostealer that steals YouTube account information and exfiltrates it via HTTP(s) POST request to cnc.

Targeted industries: Hospitality Finance

1 STIX More info

SILKWRAP

Sysupdate HyperBro +1 more DROPPER

SILKWRAP is shellcode that acts as an in-memory dropper for an embedded payload that is executed in memory. Supported payload types include executable...

Targeted industries: Government Pharmaceuticals +12 more

3 STIX More info

BAZARLOADER.SPIKEDNOG

DOWNLOADER

BAZARLOADER.SPIKEDNOG is a downloader written in C++ that retrieves payloads via HTTP. Payload URLs may be hard-coded or generated using a domain gene...

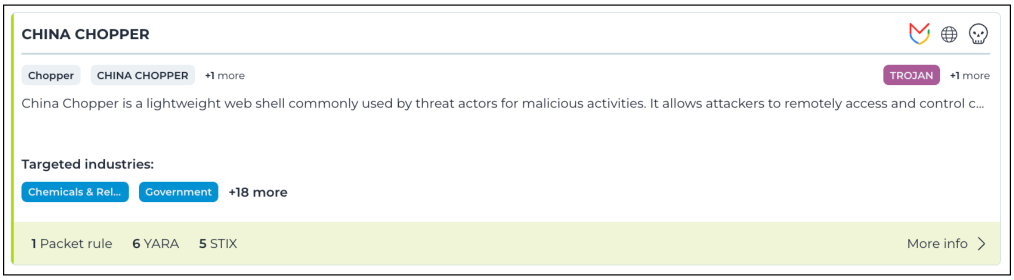
Targeted industries: Law Firms & Le... Healthcare Serv...

2 STIX More info

Figure 68. Malware filter applied

You can use the **Malware** button to show only malware-related threat cards.

Threat card



CHINA CHOPPER

Chopper CHINA CHOPPER +1 more TROJAN +1 more

China Chopper is a lightweight web shell commonly used by threat actors for malicious activities. It allows attackers to remotely access and control c...

Targeted industries:

Chemicals & Rel... Government +18 more

1 Packet rule 6 YARA 5 STIX More info

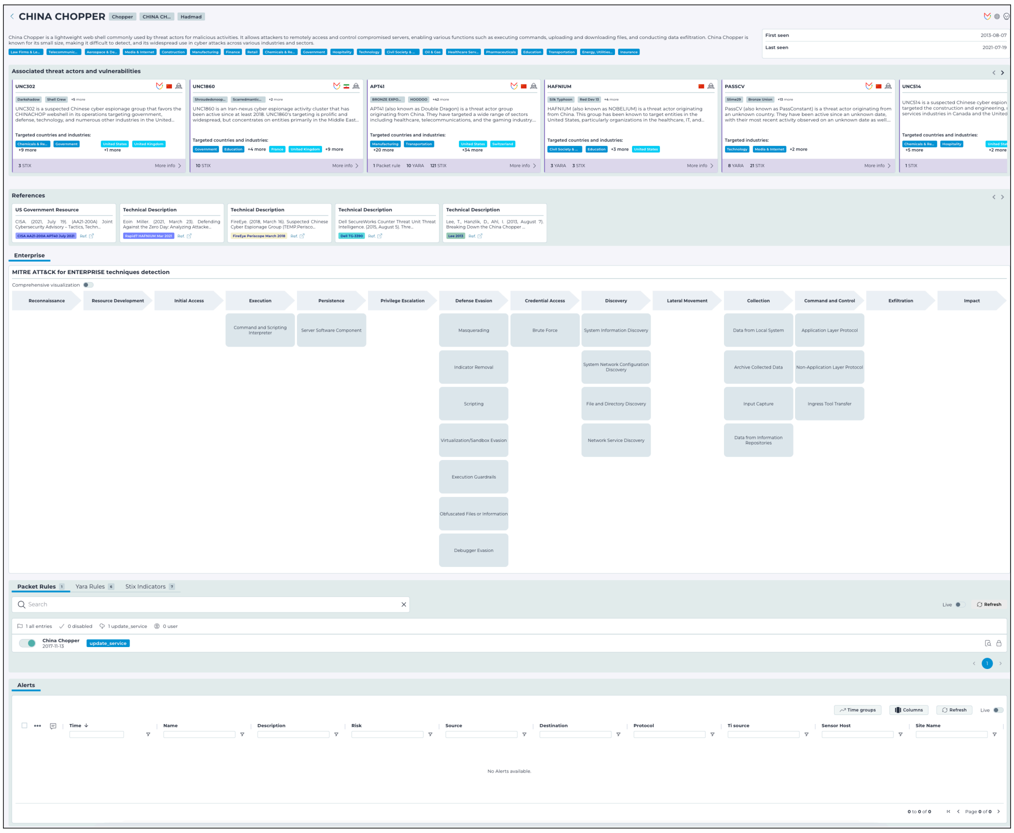
Figure 69. Malware threat card

A malware threat card can show all, or some, of these attributes:

- The name of the malware
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- This icon shows that the malware is global
- This icon shows the number of related alerts
- This icon indicates it is a malware-related threat card
- RANSOMWARE Shows the type of malware
- A description section

- The industries that the malware is known to have targeted
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page



CHINA CHOPPER Chopper CHINA CH... Hadmad

China Chopper is a lightweight web shell commonly used by threat actors for malicious activities. It allows attackers to remotely access and control compromised servers, enabling various functions such as executing commands, uploading and downloading files, and conducting data exfiltration. China Chopper is known for its small size, making it difficult to detect, and its widespread use in cyber attacks across various industries and sectors.

Law Firms & Le... Telecommunic... Aerospace & De... Media & Internet Construction Manufacturing Finance Retail Chemicals & Re... Government Hospitality Technology Civil Society & ... Oil & Gas Healthcare Serv... Pharmaceuticals Education Transportation Energy, Utilities... Insurance

First seen	2013-08-07
Last seen	2021-07-19

Associated threat actors and vulnerabilities

UNC302
Darkshadow Shell Crew +5 more
UNC302 is a suspected Chinese cyber espionage group that favors the CHINACHOP webshell in its operations targeting government, defense, technology, and numerous other industries in the United...
Targeted countries and industries:
Chemicals & Re... Government +9 more United States United Kingdom +1 more
3 STIX More info

UNC1860
Shroudedsnoop... Scarredmantic... +2 more
UNC1860 is an Iran-nexus cyber espionage activity cluster that has been active since at least 2018. UNC1860's targeting is prolific and widespread, but concentrates on entities primarily in the Middle East...
Targeted countries and industries:
Government Education +4 more France United Kingdom +9 more
10 STIX More info

APT41
BRONZE EXPO... HOODOO +42 more
APT41 (also known as Double Dragon) is a threat actor group originating from China. They have targeted a wide range of sectors including healthcare, telecommunications, and the gaming industry....
Targeted countries and industries:
Manufacturing Transportation +20 more United States Switzerland +34 more
1 Packet rule 10 YARA 121 STIX More info

HAFNIUM
Silk Typhoon Red Dev 13 +4 more
HAFNIUM (also known as NOBELIUM) is a threat actor originating from China. This group has been known to target entities in the United States, particularly organizations in the healthcare, IT, and...
Targeted countries and industries:
Civil Society & ... Education +3 more United States
3 YARA 3 STIX More info

PASSCV
Slime29 Bronze Union +13 more
PassCV (also known as PassConstant) is a threat actor originating from an unknown country. They have been active since an unknown date, with their most recent activity observed on an unknown date as well....
Targeted industries:
Technology Media & Internet +2 more
8 YARA 21 STIX More info

UNC514
UNC514 is a suspected Chinese cyber espion targeted the construction and engineering, services industries in Canada and the United
Targeted countries and industries:
Chemicals & Re... Hospitality +5 more United Stat +2 more
1 STIX

References

US Government Resource
CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Techn...
CISA AA21-200A APT40 July 2021 Ref.

Technical Description
Eoin Miller. (2021, March 23). Defending Against the Zero Day: Analyzing Attacke...
Rapid7 HAFNIUM Mar 2021 Ref.

Technical Description
FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Perisco...
FireEye Periscope March 2018 Ref.

Technical Description
Dell SecureWorks Counter Threat Unit Threat Intelligence. (2015, August 5). Thre...
Dell TG-3390 Ref.

Technical Description
Lee, T., Hanzlik, D., Ahl, I. (2013, August 7). Breaking Down the China Chopper ...
Lee 2013 Ref.

Enterprise

MITRE ATT&CK for ENTERPRISE techniques detection

Comprehensive visualization

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
			Command and Scripting Interpreter	Server Software Component		Masquerading	Brute Force	System Information Discovery		Data from Local System	Application Layer Protocol		
						Indicator Removal		System Network Configuration Discovery		Archive Collected Data	Non-Application Layer Protocol		
						Scripting		File and Directory Discovery		Input Capture	Ingress Tool Transfer		
						Virtualization/Sandbox Evasion		Network Service Discovery		Data from Information Repositories			
						Execution Guardrails							
						Obfuscated Files or Information							
						Debugger Evasion							

Packet Rules 1 Yara Rules 6 Stix Indicators 7

Search Live Refresh

1 all entries 0 disabled 1 update_service 0 user

China Chopper 2017-11-13 update_service

Alerts

Time groups Columns Refresh Live

Time	Name	Description	Risk	Source	Destination	Protocol	Ti source	Sensor Host	Site Name

No Alerts available.

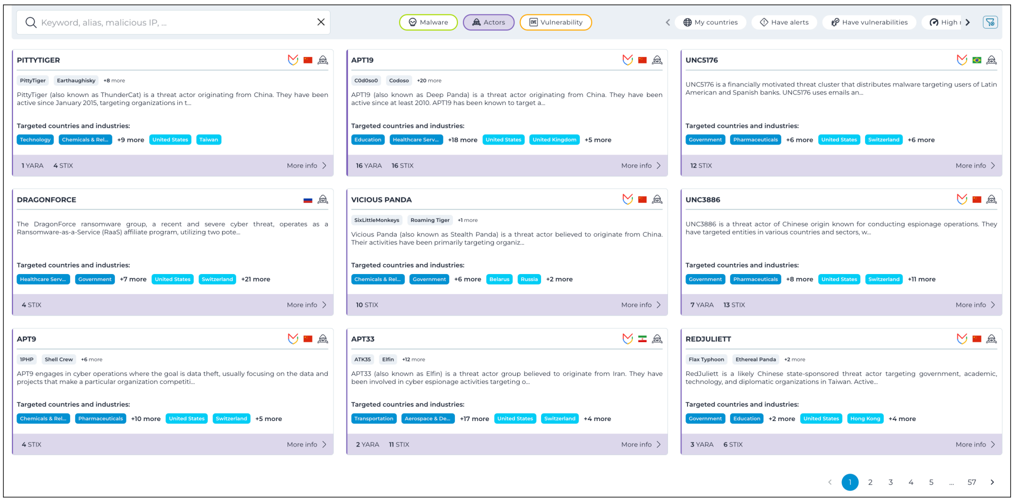
0 to 0 of 0 Page 0 of 0

Figure 70. Details page

Actors

*Learn how the **Actors** page shows threat actor-specific attributes and associated threat cards.*

Actors filter



PITTYTIGER

PittyTiger Earthaughisky +8 more

PittyTiger (also known as ThunderCat) is a threat actor originating from China. They have been active since January 2015, targeting organizations in t...

Targeted countries and industries:

Technology Chemicals & Rel... +9 more United States Taiwan

1 YARA 4 STIX More info

APT19

C0d0so0 Codoso +20 more

APT19 (also known as Deep Panda) is a threat actor originating from China. They have been active since at least 2010. APT19 has been known to target a...

Targeted countries and industries:

Education Healthcare Serv... +18 more United States United Kingdom +5 more

16 YARA 16 STIX More info

UNC5176

UNC5176 is a financially motivated threat cluster that distributes malware targeting users of Latin American and Spanish banks. UNC5176 uses emails an...

Targeted countries and industries:

Government Pharmaceuticals +6 more United States Switzerland +6 more

12 STIX More info

DRAGONFORCE

The DragonForce ransomware group, a recent and severe cyber threat, operates as a Ransomware-as-a-Service (RaaS) affiliate program, utilizing two pote...

Targeted countries and industries:

Healthcare Serv... Government +7 more United States Switzerland +21 more

4 STIX More info

VICIOUS PANDA

SixLittleMonkeys Roaming Tiger +1 more

Vicious Panda (also known as Stealth Panda) is a threat actor believed to originate from China. Their activities have been primarily targeting organiz...

Targeted countries and industries:

Chemicals & Rel... Government +6 more Belarus Russia +2 more

10 STIX More info

UNC3886

UNC3886 is a threat actor of Chinese origin known for conducting espionage operations. They have targeted entities in various countries and sectors, w...

Targeted countries and industries:

Government Pharmaceuticals +8 more United States Switzerland +11 more

7 YARA 13 STIX More info

APT9

1PHP Shell Crew +6 more

APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competiti...

Targeted countries and industries:

Chemicals & Rel... Pharmaceuticals +10 more United States Switzerland +5 more

4 STIX More info

APT33

ATK35 Elfin +12 more

APT33 (also known as Elfin) is a threat actor group believed to originate from Iran. They have been involved in cyber espionage activities targeting o...

Targeted countries and industries:

Transportation Aerospace & De... +17 more United States Switzerland +4 more

2 YARA 11 STIX More info

REDJULIETT

Flax Typhoon Ethereal Panda +2 more

RedJuliett is a likely Chinese state-sponsored threat actor targeting government, academic, technology, and diplomatic organizations in Taiwan. Active...

Targeted countries and industries:

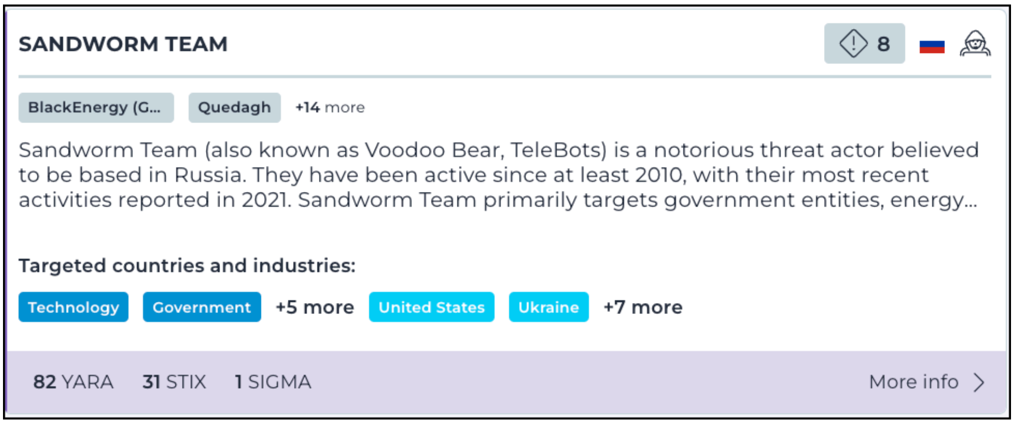
Government Education +2 more United States Hong Kong +4 more

3 YARA 6 STIX More info

Figure 71. Actors filter applied

You can use the **Actors** button to show only actors-related threat cards.

Threat card



SANDWORM TEAM

BlackEnergy (G... Quedagh +14 more

Sandworm Team (also known as Voodoo Bear, TeleBots) is a notorious threat actor believed to be based in Russia. They have been active since at least 2010, with their most recent activities reported in 2021. Sandworm Team primarily targets government entities, energy...

Targeted countries and industries:

Technology Government +5 more United States Ukraine +7 more

82 YARA 31 STIX 1 SIGMA More info

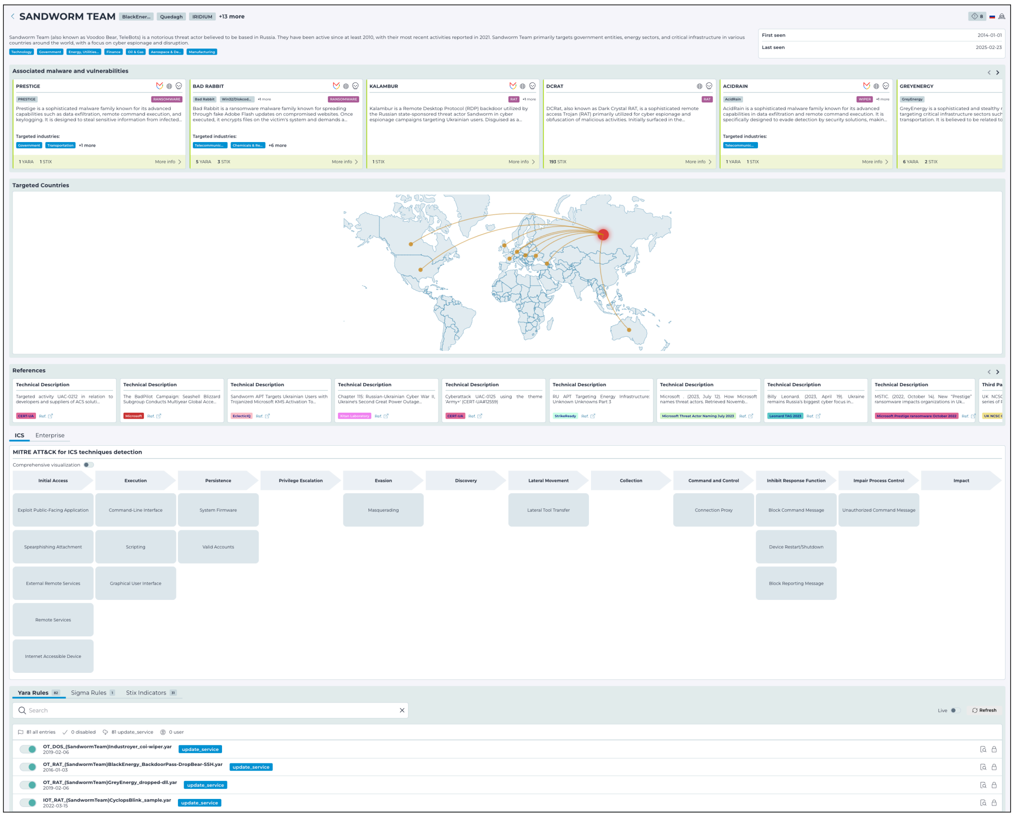
Figure 72. Actors threat card

An actor threat card show all, or some, of these attributes:

- The name of the threat actor
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- A flag will show the origin country
- This icon shows the number of related alerts

- 🕵 Indicates it is a actor-related threat card
- RANSOMWARE Shows the type of malware
- A description section
- The countries and industries that the malware is known to have targeted
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page



SANDWORM TEAM BlackEner... Quedagh IRIDIUM +13 more

Sandworm Team (also known as Voodoo Bear, TeleBots) is a notorious threat actor believed to be based in Russia. They have been active since at least 2010, with their most recent activities reported in 2021. Sandworm Team primarily targets government entities, energy sectors, and critical infrastructure in various countries around the world, with a focus on cyber espionage and disruption.

Technology Government Energy, Utilities... Finance Oil & Gas Aerospace & De... Manufacturing

First seen	2014-01-01
Last seen	2025-02-23

Associated malware and vulnerabilities

PRESTIGE — PRESTIGE — RANSOMWARE
Prestige is a sophisticated malware family known for its advanced capabilities such as data exfiltration, remote command execution, and keylogging. It is designed to steal sensitive information from infected...
Targeted industries: Government Transportation +1 more
1 YARA 1 STIX More info

BAD RABBIT — Bad Rabbit Win32/Diskcod... +1 more — RANSOMWARE
Bad Rabbit is a ransomware malware family known for spreading through fake Adobe Flash updates on compromised websites. Once executed, it encrypts files on the victim's system and demands a...
Targeted industries: Telecommunic... Chemicals & Re... +6 more
5 YARA 3 STIX More info

KALAMBUR — RAT +1 more
Kalambur is a Remote Desktop Protocol (RDP) backdoor utilized by the Russian state-sponsored threat actor Sandworm in cyber espionage campaigns targeting Ukrainian users. Disguised as a...
1 STIX More info

DCRAT — RAT
DCRat, also known as Dark Crystal RAT, is a sophisticated remote access Trojan (RAT) primarily utilized for cyber espionage and obfuscation of malicious activities. Initially surfaced in the...
193 STIX More info

ACIDRAIN — AcidRain — WIPER +1 more
AcidRain is a sophisticated malware family known for its advanced capabilities in data exfiltration and remote command execution. It is specifically designed to evade detection by security solutions, makin...
Targeted industries: Telecommunic...
1 YARA 1 STIX More info

GREYENERGY — GreyEnergy
GreyEnergy is a sophisticated and stealthy r
targeting critical infrastructure sectors such
transportation. It is believed to be related to
6 YARA 2 STIX

Targeted Countries

References

Technical Description — Targeted activity UAC-0212 in relation to developers and suppliers of ACS soluti... — CERT-UA Ref.

Technical Description — The BadPilot Campaign: Seashell Blizzard Subgroup Conducts Multiyear Global Acce... — Microsoft Ref.

Technical Description — Sandworm APT Targets Ukrainian Users with Trojanized Microsoft KMS Activation To... — EclecticIQ Ref.

Technical Description — Chapter 115: Russian-Ukrainian Cyber War II, Ukraine's Second Great Power Outage... — Xitan Laboratory Ref.

Technical Description — Cyberattack UAC-0125 using the theme 'Army+' (CERT-UA#12559) — CERT-UA Ref.

Technical Description — RU APT Targeting Energy Infrastructure: Unknown Unknowns Part 3 — StrikeReady Ref.

Technical Description — Microsoft . (2023, July 12). How Microsoft names threat actors. Retrieved Novemb... — Microsoft Threat Actor Naming July 2023 Ref.

Technical Description — Billy Leonard. (2023, April 19). Ukraine remains Russia's biggest cyber focus in... — Leonard TAG 2023 Ref.

Technical Description — MSTIC. (2022, October 14). New "Prestige" ransomware impacts organizations in Uk... — Microsoft Prestige ransomware October 2022 Ref.

Third Pa — UK NCSC series of F — UK NCSC

ICS Enterprise

MITRE ATT&CK for ICS techniques detection

Comprehensive visualization

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Exploit Public-Facing Application	Command-Line Interface	System Firmware		Masquerading		Lateral Tool Transfer		Connection Proxy	Block Command Message	Unauthorized Command Message	
Spearphishing Attachment	Scripting	Valid Accounts							Device Restart/Shutdown		
External Remote Services	Graphical User Interface								Block Reporting Message		
Remote Services											
Internet Accessible Device											

Yara Rules 82 Sigma Rules 1 Stix Indicators 31

Search Live Refresh

81 all entries ✓ 0 disabled 81 update_service 0 user

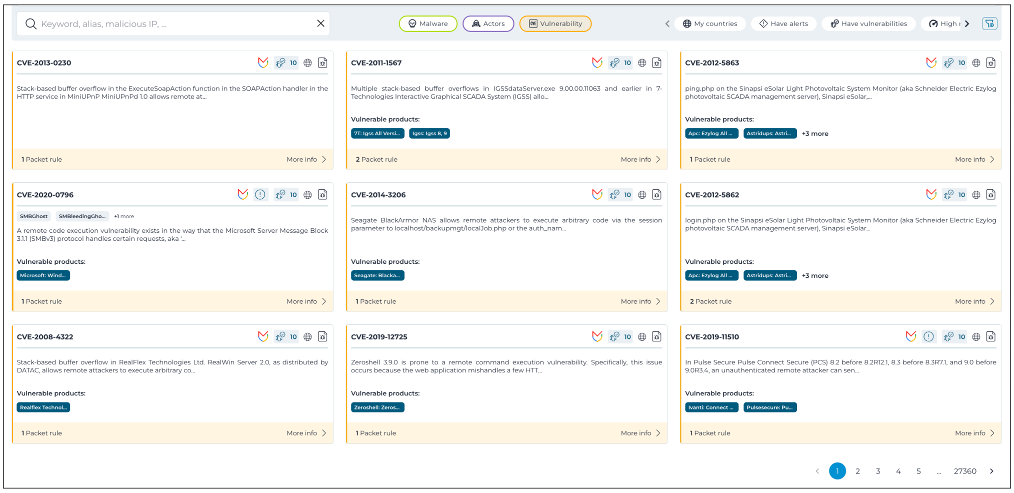
- OT_DOS_(SandwormTeam)Industroyer_coi-wiper.yar 2019-02-06 update_service
- OT_RAT_(SandwormTeam)BlackEnergy_BackdoorPass-DropBear-SSH.yar 2016-01-03 update_service
- OT_RAT_(SandwormTeam)GreyEnergy_dropped-dll.yar 2019-02-06 update_service
- IOT_RAT_(SandwormTeam)CyclopsBlink_sample.yar 2022-03-15 update_service

Figure 73. Details page

Vulnerability

*Learn how the **Vulnerability** page shows vulnerability-specific attributes and associated threat cards.*

Vulnerability filter



CVE-2013-0230 10

Stack-based buffer overflow in the ExecuteSoapAction function in the SOAPAction handler in the HTTP service in MiniUPnP MiniUPnPd 1.0 allows remote at...

1 Packet rule More info

CVE-2011-1567 10

Multiple stack-based buffer overflows in IGSSdataServer.exe 9.00.00.11063 and earlier in 7-Technologies Interactive Graphical SCADA System (IGSS) allo...

Vulnerable products:

7T: Igss All Versi... Igss: Igss 8, 9

2 Packet rule More info

CVE-2012-5863 10

ping.php on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar,...

Vulnerable products:

Apc: Ezylog All ... Astridups: Astri... +3 more

1 Packet rule More info

CVE-2020-0796 10

SMBGhost SMBleedingGho... +1 more

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka '...

Vulnerable products:

Microsoft: Wind...

1 Packet rule More info

CVE-2014-3206 10

Seagate BlackArmor NAS allows remote attackers to execute arbitrary code via the session parameter to localhost/backupmgt/localJob.php or the auth_nam...

Vulnerable products:

Seagate: Blacka...

1 Packet rule More info

CVE-2012-5862 10

login.php on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar...

Vulnerable products:

Apc: Ezylog All ... Astridups: Astri... +3 more

2 Packet rule More info

CVE-2008-4322 10

Stack-based buffer overflow in RealFlex Technologies Ltd. RealWin Server 2.0, as distributed by DATAC, allows remote attackers to execute arbitrary co...

Vulnerable products:

Realflex Technol...

1 Packet rule More info

CVE-2019-12725 10

Zeroshell 3.9.0 is prone to a remote command execution vulnerability. Specifically, this issue occurs because the web application mishandles a few HTT...

Vulnerable products:

Zeroshell: Zeros...

1 Packet rule More info

CVE-2019-11510 10

In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can sen...

Vulnerable products:

Ivanti: Connect ... Pulsesecure: Pu...

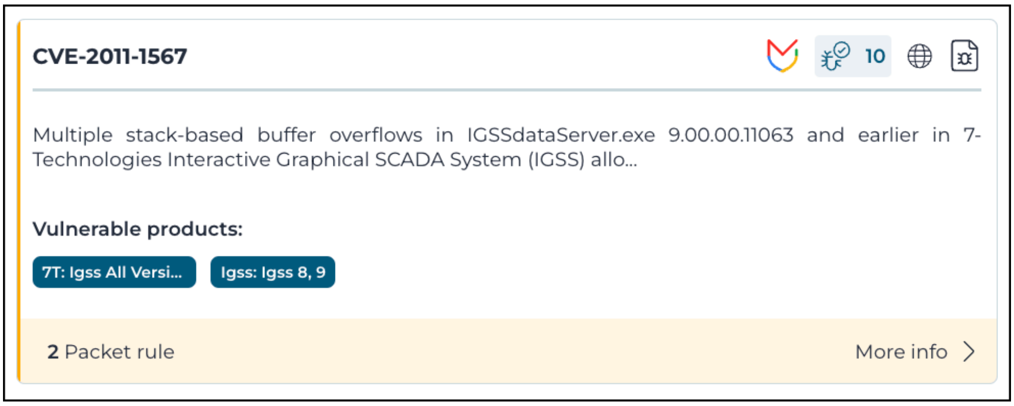
1 Packet rule More info

‹ 1 2 3 4 5 ... 27360 ›

Figure 74. Vulnerability filter applied

You can use the **Vulnerability** button to show only vulnerability-related threat cards.

Threat card



CVE-2011-1567 10

Multiple stack-based buffer overflows in IGSSdataServer.exe 9.00.00.11063 and earlier in 7-Technologies Interactive Graphical SCADA System (IGSS) allo...

Vulnerable products:

7T: Igss All Versi... Igss: Igss 8, 9

2 Packet rule More info

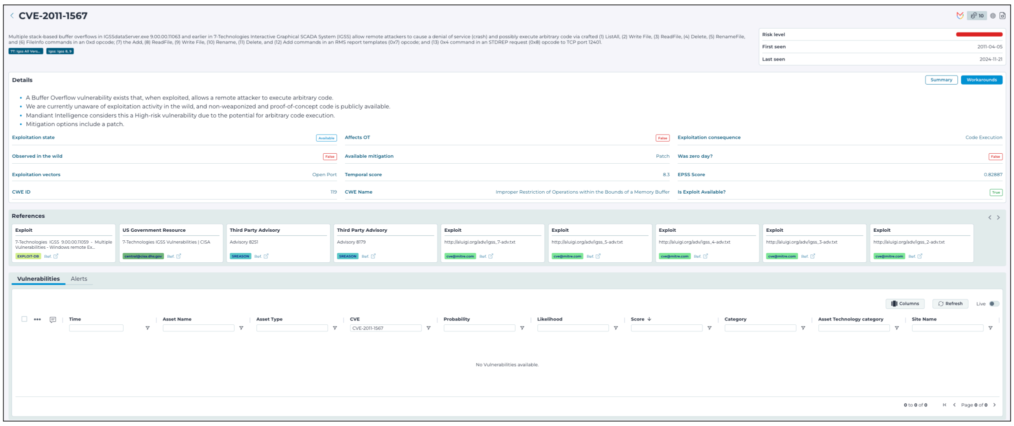
Figure 75. Vulnerability threat card

A vulnerability threat card show all, or some, of these attributes:

- The name of the vulnerability
- The Mandiant icon shows whenever a threat card is enriched with Mandiant data
- 🌐 This icon shows that the vulnerability is global
- This icon shows the score
- This icon indicates that it is a vulnerability-related threat card

- A description section
- The products that are vulnerable
- The rules, patterns, and indicators that are associated with the threat card content, the **More info** button lets you view more details in the details page

Details page



CVE-2011-1567

Multiple stack-based buffer overflows in IGSSdataServer.exe 9.00.00.11063 and earlier in 7-Technologies Interactive Graphical SCADA System (IGSS) allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted (1) ListAll, (2) Write File, (3) ReadFile, (4) Delete, (5) RenameFile, and (6) FileInfo commands in an 0xd opcode; (7) the Add, (8) ReadFile, (9) Write File, (10) Rename, (11) Delete, and (12) Add commands in an RMS report templates (0x7) opcode; and (13) 0x4 command in an STDREP request (0x8) opcode to TCP port 12401.

Risk level	
First seen	2011-04-05
Last seen	2024-11-21

Details

- A Buffer Overflow vulnerability exists that, when exploited, allows a remote attacker to execute arbitrary code.
- We are currently unaware of exploitation activity in the wild, and non-weaponized and proof-of-concept code is publicly available.
- Mandiant Intelligence considers this a High-risk vulnerability due to the potential for arbitrary code execution.
- Mitigation options include a patch.

Exploitation state	Available	Affects OT	False	Exploitation consequence	Code Execution
Observed in the wild	False	Available mitigation	Patch	Was zero day?	False
Exploitation vectors	Open Port	Temporal score	8.3	EPSS Score	0.82887
CWE ID	119	CWE Name	Improper Restriction of Operations within the Bounds of a Memory Buffer	Is Exploit Available?	True

References

Exploit	7-Technologies IGSS 9.00.00.11059 - Multiple Vulnerabilities - Windows remote Ex...	EXPLOIT-DB Ref.
US Government Resource	7-Technologies IGSS Vulnerabilities | CISA	central@cisa.dhs.gov Ref.
Third Party Advisory	Advisory 8251	SREASON Ref.
Third Party Advisory	Advisory 8179	SREASON Ref.
Exploit	http://aluigi.org/adv/igss_7-adv.txt	cve@mitre.com Ref.
Exploit	http://aluigi.org/adv/igss_5-adv.txt	cve@mitre.com Ref.
Exploit	http://aluigi.org/adv/igss_4-adv.txt	cve@mitre.com Ref.
Exploit	http://aluigi.org/adv/igss_3-adv.txt	cve@mitre.com Ref.
Exploit	http://aluigi.org/adv/igss_2-adv.txt	cve@mitre.com Ref.

Time	Asset Name	Asset Type	CVE	Probability	Likelihood	Score ↓	Category	Asset Technology category	Site Name
			CVE-2011-1567						

No Vulnerabilities available.

0 to 0 of 0 Page 0 of 0

Figure 76. Details page

Chapter 17. Asset Risk

*The **Asset Risk** page provides an in-depth view of asset risk levels. This includes an overview, detailed analysis, and benchmark comparisons to help assess and manage risks effectively.*

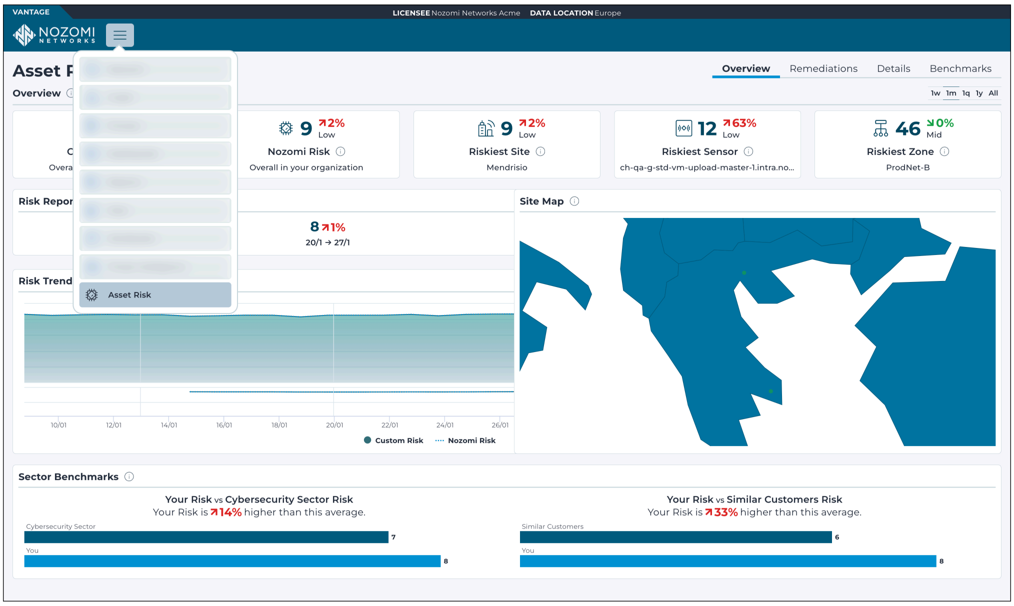


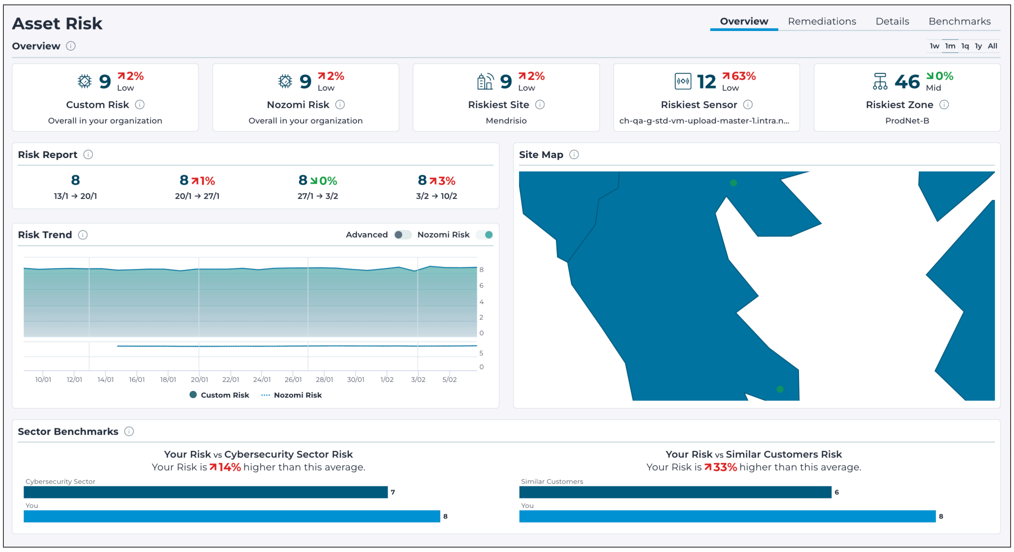
Figure 77. Asset Risk page

The **Asset Risk** page has these tabs:

- Overview (on page 240)
- Remediations (on page 242)
- Details (on page 243)
- Benchmarks (on page 245)

Overview

*The **Overview** page lets you analyze your risk position over time and compare it to the average risks of your industry and similar customers.*



Your Risk is ↗14% higher than this average.

Your Risk is ↗33% higher than this average.

Figure 78. Overview page

Custom Risk

The overall risk, which is based on your specific risk formula.

Nozomi Risk

This is based on the standard Nozomi risk formula.

Riskiest Site

This shows the site in your organization that has the highest risk.

Riskiest Sensor

This shows the sensor that has the highest risk based on your specific risk formula.

Riskiest Zone

This shows the zone that has the highest risk based on your specific risk formula.

Risk Report

This shows the average risk values in the selected time frame.

Risk Trend

This lets you monitor the trends of both your overall risks, as well as Nozomi risks over time.

Site Map

This lets you evaluate the risk positions of your different sites.

Sector Benchmarks

This lets you compare your Nozomi risk industry sectors and similar customers.

Related information

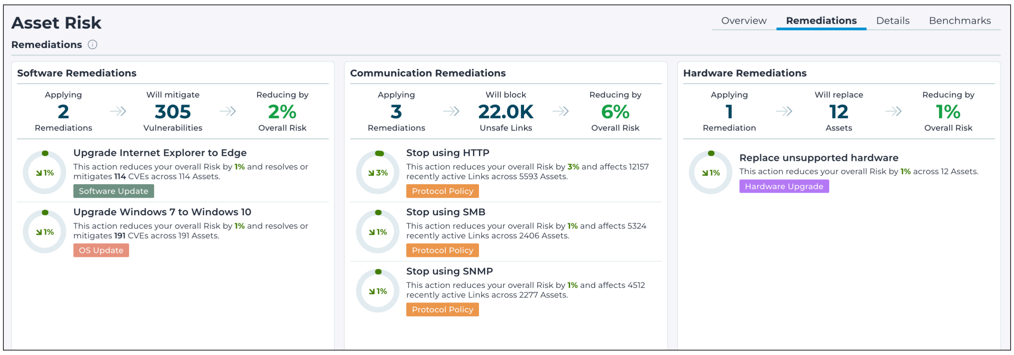
Remediations (on page 242)

Details (on page 243)

Benchmarks (on page 245)

Remediations

*The **Remediations** tab provides an overview of the remediation actions you can take to reduce asset risks.*



Software Remediations

Applying 2 Remediations → Will mitigate 305 Vulnerabilities → Reducing by 2% Overall Risk

1% Upgrade Internet Explorer to Edge
This action reduces your overall Risk by 1% and resolves or mitigates 114 CVEs across 114 Assets.
Software Update

1% Upgrade Windows 7 to Windows 10
This action reduces your overall Risk by 1% and resolves or mitigates 191 CVEs across 191 Assets.
OS Update

Communication Remediations

Applying 3 Remediations → Will block 22.0K Unsafe Links → Reducing by 6% Overall Risk

3% Stop using HTTP
This action reduces your overall Risk by 3% and affects 12157 recently active Links across 5593 Assets.
Protocol Policy

1% Stop using SMB
This action reduces your overall Risk by 1% and affects 5324 recently active Links across 2406 Assets.
Protocol Policy

1% Stop using SNMP
This action reduces your overall Risk by 1% and affects 4512 recently active Links across 2277 Assets.
Protocol Policy

Hardware Remediations

Applying 1 Remediation → Will replace 12 Assets → Reducing by 1% Overall Risk

1% Replace unsupported hardware
This action reduces your overall Risk by 1% across 12 Assets.
Hardware Upgrade

Figure 79. Remediations Overview

Software Remediations

These actions address software risks related to your assets.

Communication Remediations

These actions address network protocol risks related to your assets.

Hardware Remediations

These actions address hardware risks related to your assets.

Related information

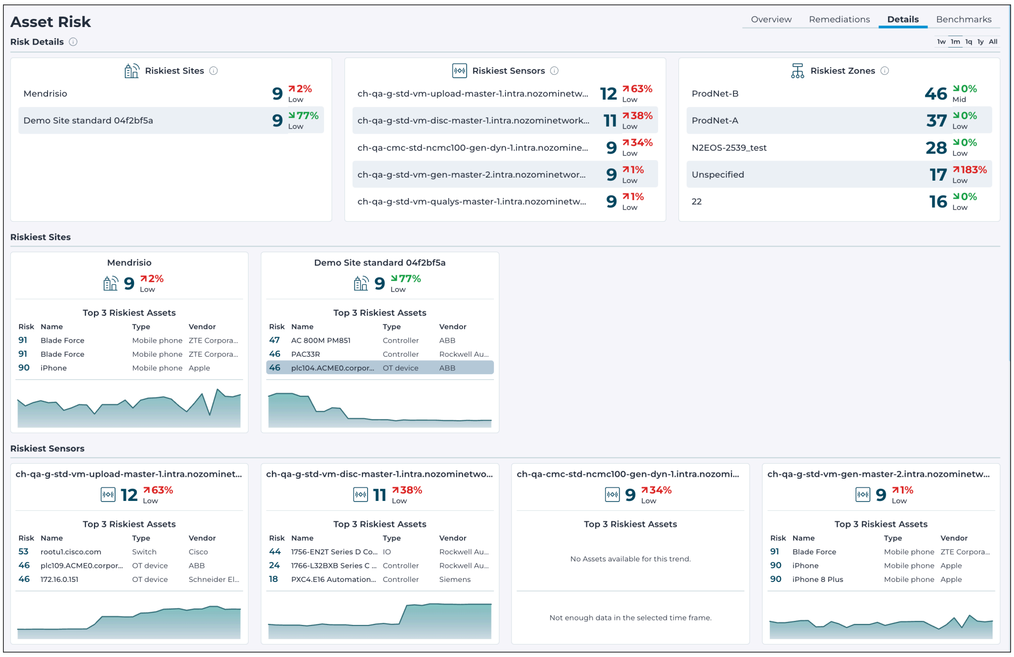
Overview (on page 240)

Details (on page 243)

Benchmarks (on page 245)

Details

*The **Details** page provides an in-depth analysis of asset risks, highlighting the riskiest sites, sensors, and zones, along with detailed information about their associated assets.*



Asset Risk

Risk Details

Riskiest Sites

Mendrisio	9	↗2% Low
Demo Site standard 04f2bf5a	9	↘77% Low

Riskiest Sensors

ch-qa-g-std-vm-upload-master-1.intra.nozominetw...	12	↗63% Low
ch-qa-g-std-vm-disc-master-1.intra.nozominetwork...	11	↗38% Low
ch-qa-cmc-std-ncmc100-gen-dyn-1.intra.nozomine...	9	↗34% Low
ch-qa-g-std-vm-gen-master-2.intra.nozominetwor...	9	↗1% Low
ch-qa-g-std-vm-qualys-master-1.intra.nozominetw...	9	↗1% Low

Riskiest Zones

ProdNet-B	46	↘0% Mid
ProdNet-A	37	↘0% Low
N2EOS-2539_test	28	↘0% Low
Unspecified	17	↗183% Low
22	16	↘0% Low

Riskiest Sites

Mendrisio

9 ↗2% Low

Top 3 Riskiest Assets

Risk	Name	Type	Vendor
91	Blade Force	Mobile phone	ZTE Corpora...
91	Blade Force	Mobile phone	ZTE Corpora...
90	iPhone	Mobile phone	Apple

Demo Site standard 04f2bf5a

9 ↘77% Low

Top 3 Riskiest Assets

Risk	Name	Type	Vendor
47	AC 800M PM851	Controller	ABB
46	PAC33R	Controller	Rockwell Au...
46	plc104.ACME0.corpor...	OT device	ABB

Riskiest Sensors

ch-qa-g-std-vm-upload-master-1.intra.nozominet...

12 ↗63% Low

Top 3 Riskiest Assets

Risk	Name	Type	Vendor
53	rootu1.cisco.com	Switch	Cisco
46	plc109.ACME0.corpor...	OT device	ABB
46	172.16.0.151	OT device	Schneider El...

ch-qa-g-std-vm-disc-master-1.intra.nozominetwo...

11 ↗38% Low

Top 3 Riskiest Assets

Risk	Name	Type	Vendor
44	1756-EN2T Series D Co...	IO	Rockwell Au...
24	1766-L32BXB Series C ...	Controller	Rockwell Au...
18	PXC4.E16 Automation...	Controller	Siemens

ch-qa-cmc-std-ncmc100-gen-dyn-1.intra.nozomi...

9 ↗34% Low

Top 3 Riskiest Assets

No Assets available for this trend.

Not enough data in the selected time frame.

ch-qa-g-std-vm-gen-master-2.intra.nozominetw...

9 ↗1% Low

Top 3 Riskiest Assets

Risk	Name	Type	Vendor
91	Blade Force	Mobile phone	ZTE Corpora...
90	iPhone	Mobile phone	Apple
90	iPhone 8 Plus	Mobile phone	Apple

Figure 80. Details page

This pages shows a more in-depth view of data that is shown in the Overview (on page 240) page.

Risk Details

This shows a summary view for the categories below.

Riskiest Sites

This shows more details for the riskiest site, and the top three riskiest sensors in it. Each tile shows the:

- Risk
- Name
- Type
- Vendor

You can select an asset to open the related details page.

Riskiest Sensors

This shows the sensors that have the highest risk levels and the riskiest assets connected to the sensor. Each tile shows the:

- Risk
- Name

- Type
- Vendor

Riskiest Zones

This shows the zones that have the highest risk levels and the riskiest assets in the zone. Each tile shows the:

- Risk
- Name
- Type
- Vendor

Related information

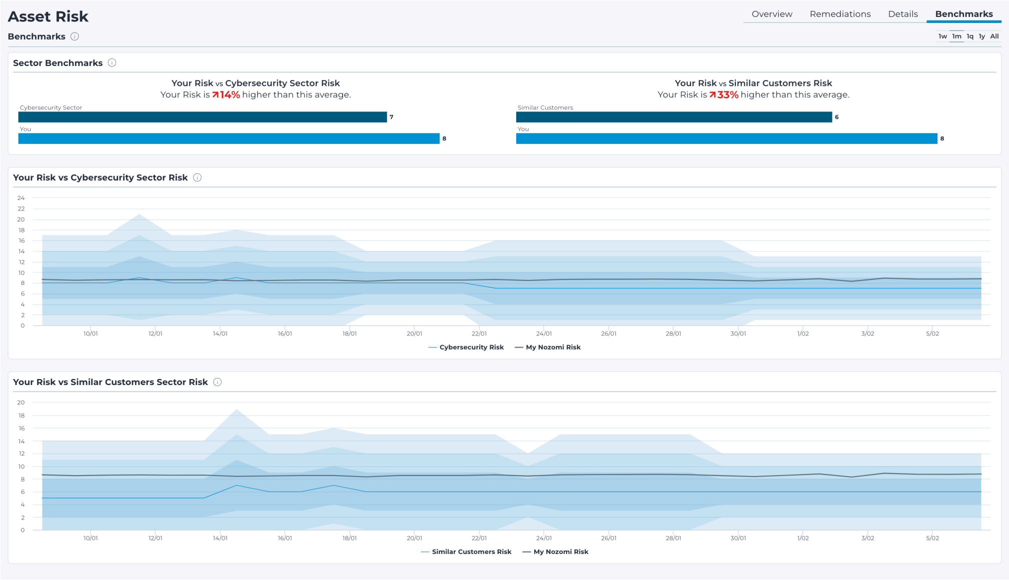
Overview (on page 240)

Remediations (on page 242)

Benchmarks (on page 245)

Benchmarks

*The **Benchmarks** page lets you compare your organization's risk levels against industry sectors and similar customers to evaluate your security posture.*



Your Risk vs Cybersecurity Sector Risk
Your Risk is ↗14% higher than this average.

Your Risk vs Similar Customers Risk
Your Risk is ↗33% higher than this average.

Figure 81. Benchmarks page

Related information

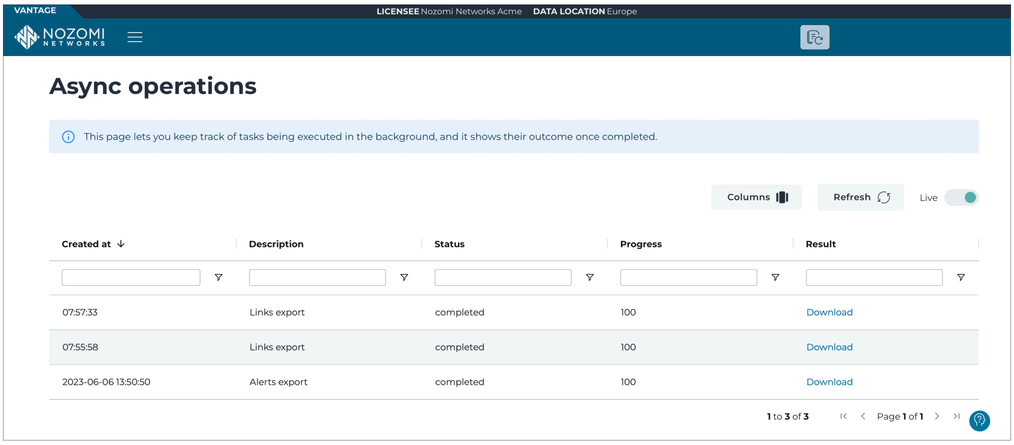
Overview (on page 240)

Remediations (on page 242)

Details (on page 243)

Chapter 18. Async operations

*The **Async operations** page lets you keep track of tasks that are being executed in the background, and it shows their outcome once that they are completed.*



Async operations

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

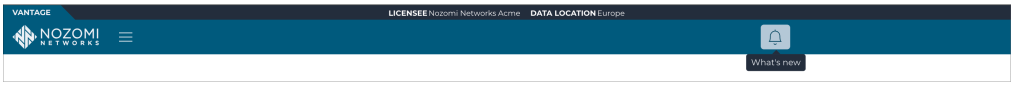
Created at	Description	Status	Progress	Result
07:57:33	Links export	completed	100	Download
07:55:58	Links export	completed	100	Download
2023-06-06 13:50:50	Alerts export	completed	100	Download

1 to 3 of 3 Page 1 of 1

Figure 82. Async operations page

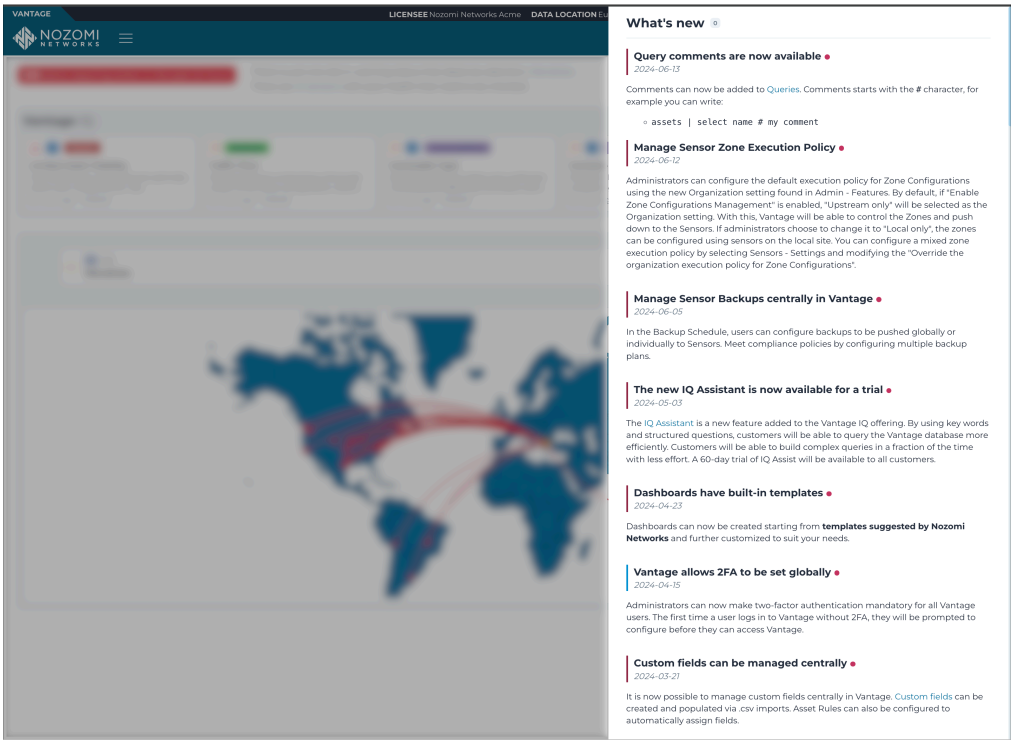
Chapter 19. What's new drawer

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



LICENSEE Nozomi Networks Acme **DATA LOCATION** Europe

Figure 83. What's new icon



LICENSEE Nozomi Networks Acme **DATA LOCATION** Eu

What's new 0

Query comments are now available
2024-06-13

Comments can now be added to Queries. Comments starts with the # character, for example you can write:

- `assets | select name # my comment`

Manage Sensor Zone Execution Policy
2024-06-12

Administrators can configure the default execution policy for Zone Configurations using the new Organization setting found in Admin - Features. By default, if "Enable Zone Configurations Management" is enabled, "Upstream only" will be selected as the Organization setting. With this, Vantage will be able to control the Zones and push down to the Sensors. If administrators choose to change it to "Local only", the zones can be configured using sensors on the local site. You can configure a mixed zone execution policy by selecting Sensors - Settings and modifying the "Override the organization execution policy for Zone Configurations".

Manage Sensor Backups centrally in Vantage
2024-06-05

In the Backup Schedule, users can configure backups to be pushed globally or individually to Sensors. Meet compliance policies by configuring multiple backup plans.

The new IQ Assistant is now available for a trial
2024-05-03

The IQ Assistant is a new feature added to the Vantage IQ offering. By using key words and structured questions, customers will be able to query the Vantage database more efficiently. Customers will be able to build complex queries in a fraction of the time with less effort. A 60-day trial of IQ Assist will be available to all customers.

Dashboards have built-in templates
2024-04-23

Dashboards can now be created starting from **templates suggested by Nozomi Networks** and further customized to suit your needs.

Vantage allows 2FA to be set globally
2024-04-15

Administrators can now make two-factor authentication mandatory for all Vantage users. The first time a user logs in to Vantage without 2FA, they will be prompted to configure before they can access Vantage.

Custom fields can be managed centrally
2024-03-21

It is now possible to manage custom fields centrally in Vantage. Custom fields can be created and populated via .csv imports. Asset Rules can also be configured to automatically assign fields.

Figure 84. What's new drawer

Chapter 20. Administration

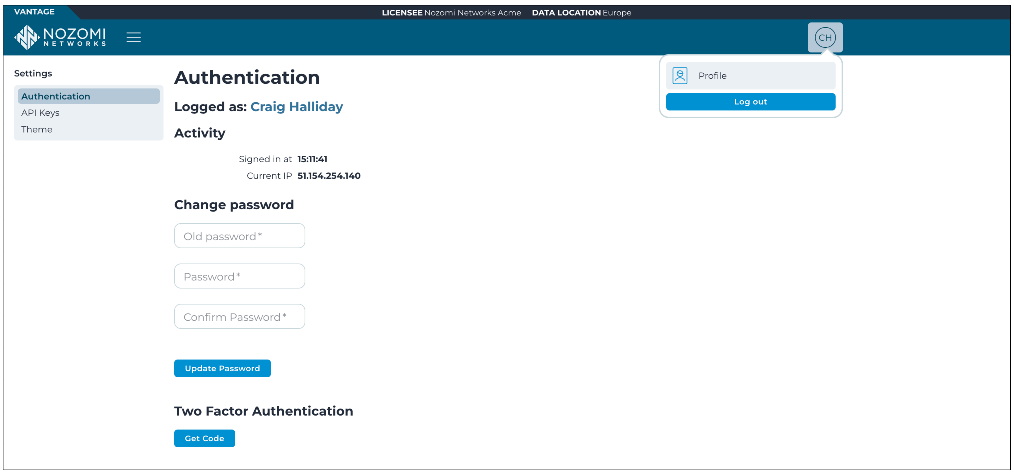
Administration page

The administration page lets a user with administrator privileges configure settings and do other tasks.

For more details, see the Vantage **Administrator Manual**.

Chapter 21. Profile settings

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



Authentication

Logged as: Craig Halliday

Activity

Signed in at 15:11:41
Current IP 51.154.254.140

Change password

Old password *

Password *

Confirm Password *

Two Factor Authentication

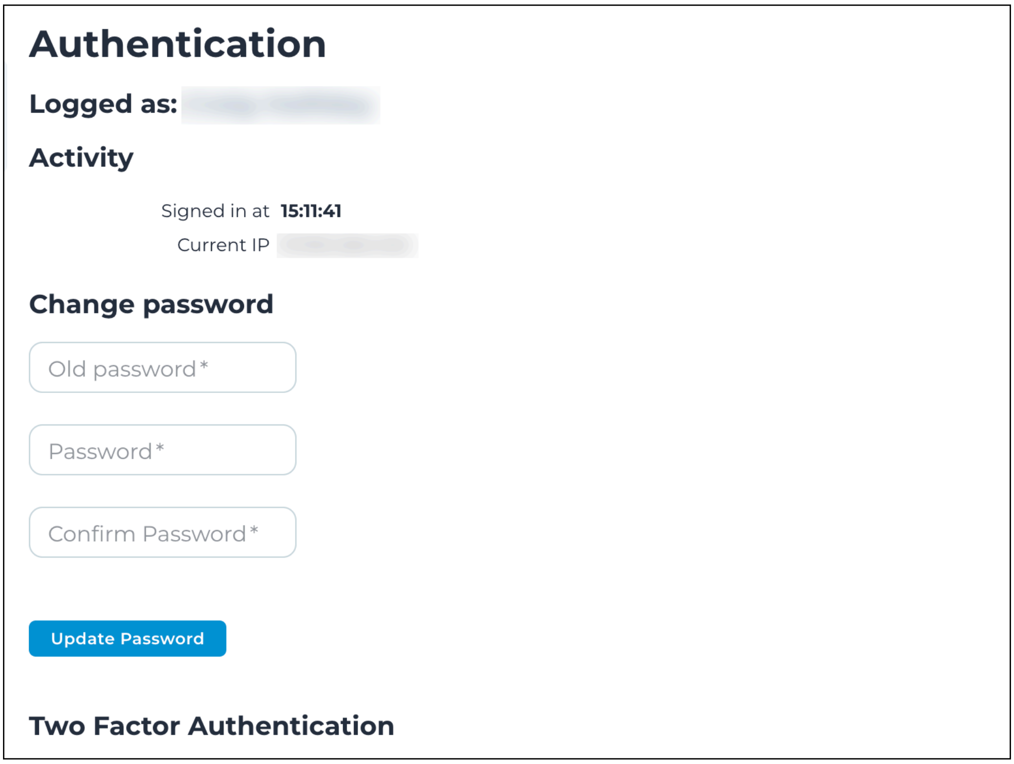
Figure 85. Profile settings menu

The **Profile** page has these tabs:

- Authentication (on page 262)
- API Keys (on page 263)
- Theme (on page 265)

Authentication

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



Authentication

Logged as: [redacted]

Activity

Signed in at **15:11:41**

Current IP [redacted]

Change password

Old password*

Password*

Confirm Password*

Two Factor Authentication

Figure 86. Authentication page

Activity

This section shows the last time the current user signed in and the *IP* address used.

Change password

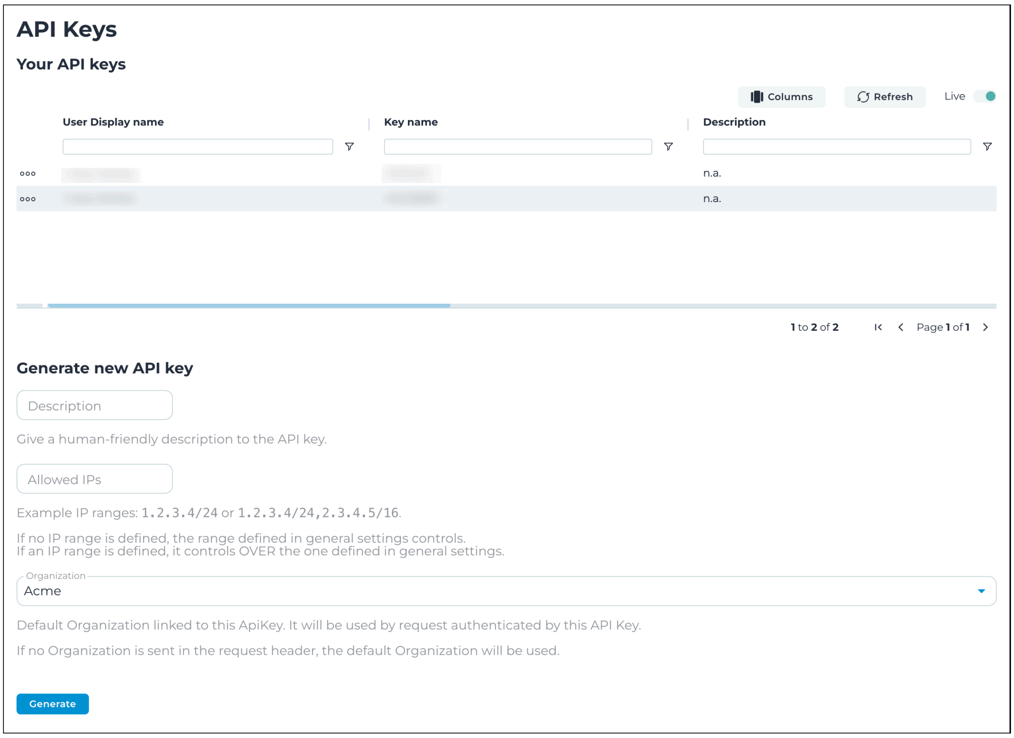
This section lets you change your password.

Two Factor Authentication

The **Get Code** button lets you create a code that can be used for *two-factor authentication (2FA)* in third-party applications.

API Keys

*The **API Keys** pages lets you manage application programming interface (API) keys for the current user. Third-party applications that integrate with Vantage must use API keys to authenticate.*



API Keys

Your API keys

	User Display name	Key name	Description
○○○	[redacted]	[redacted]	n.a.
○○○	[redacted]	[redacted]	n.a.

1 to **2** of **2** Page **1** of **1**

Generate new API key

Description

Give a human-friendly description to the API key.

Allowed IPs

Example IP ranges: `1.2.3.4/24` or `1.2.3.4/24,2.3.4.5/16`.

If no IP range is defined, the range defined in general settings controls.
If an IP range is defined, it controls OVER the one defined in general settings.

Organization: Acme

Default Organization linked to this ApiKey. It will be used by request authenticated by this API Key.

If no Organization is sent in the request header, the default Organization will be used.

Figure 87. 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 *API* key was created.
Updated at	The date and time that the *API* key was last updated.
Revoked at	The date and time that the *API* key was revoked.
User Display name	The display name of the user associated with the *API* key.
Key name	The name of the *API* key. Vantage generates this name when you create the *API* key.
Description	The user-defined description of the *API* key.
Last sign in at	The last date and time that the *API* key was used to sign in.
Last sign in ip	The originating *IP* address of the connection that last authenticated using the *API* key.
Allowed ips	The user-defined range of *IP* addresses from which connections are permitted.
Linked organization Name	The name of an organization that will serve as a default value when *API* calls using this key do not specify an organization.

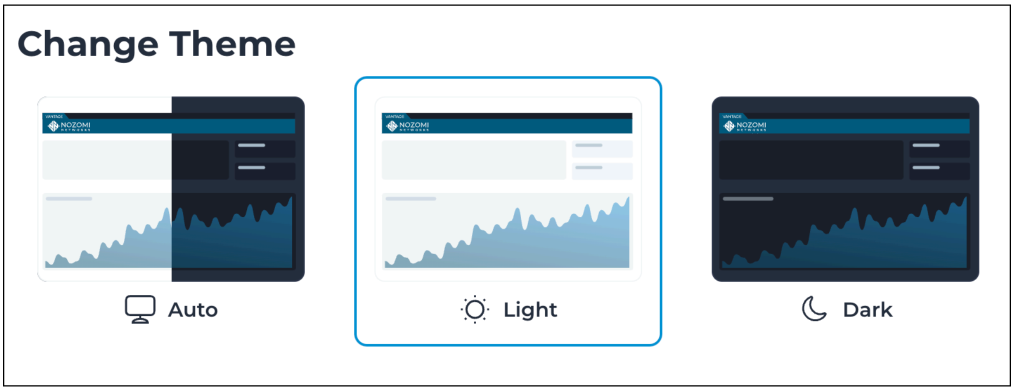
Generate new API key

This section lets you:

- Create a description for the *API* key
- Set an allowed, or range of allowed, *IP* addresses for the *API* key
- Select an organization with which to associate the *API* key

Theme

*The **Theme** page lets you choose a theme for the user interface (UI).*



Change Theme

Figure 88. Theme page

The **Theme** page lets you customize the visual appearance of the *UI*. You can choose one of these themes:

- Auto: Automatically adjusts the theme based on system settings
- Light: Uses a bright interface for better visibility in well-lit environments
- Dark: Uses a dark interface for reduced eye strain in low-light environments

Chapter 22. 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.

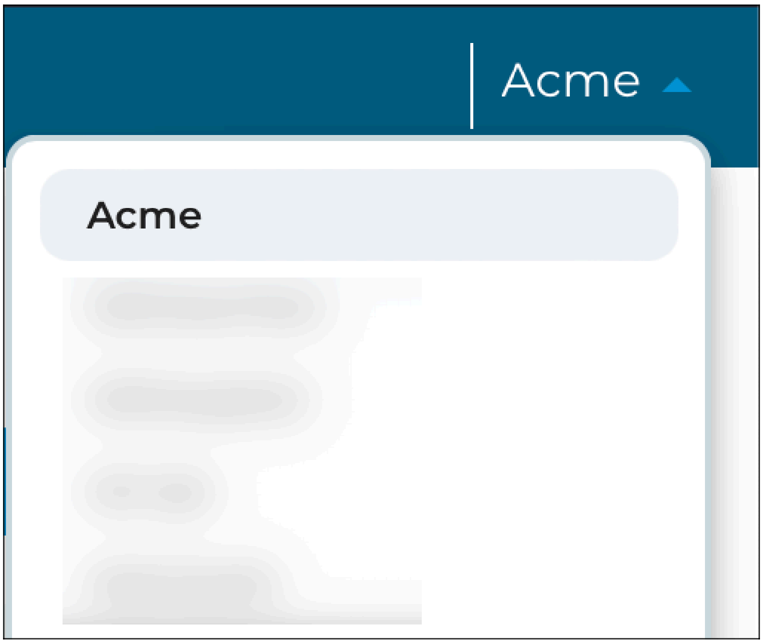


Figure 89. Organizations menu

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 a similar way as on 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.

Exploit Prediction Scoring System

EPSS is a cybersecurity risk assessment framework that predicts the likelihood of a software vulnerability being exploited in the wild. It uses data-driven models based on real-world exploit activity, vulnerability metadata, and other threat intelligence sources to help organizations prioritize patching efforts.

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

Identity Provider

An IdP is a system entity that creates, maintains, and manages identity information. It also provides authentication services to applications within a federation, or a distributed network.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.

Information Technology

IT is the use of computers to process, create, store, and exchange data and information.

Internet of Things

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

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

JavaScript Object Notation

JSON is an open standard file format for data interchange. It uses human-readable text to store and transmit data objects, which consist of attribute–value pairs and arrays.

JSON web token

A JWT is an internet standard to create data with optional encryption and/or optional signature whose payload holds JSON that asserts some number of claims. The tokens are signed either using a private secret or a private/ public key.

Known Exploited Vulnerabilities

A list of software vulnerabilities that threat actors have actively exploited. Cybersecurity organizations track KEVs to help prioritize patching and mitigate security risks.

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.

Packet Capture

A pcap is an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

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.

Structured Threat Information Expression

STIX™ is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Threat Intelligence™

Nozomi Networks **Threat Intelligence™** feature monitors ongoing OT and IoT threat and vulnerability intelligence to improve malware anomaly detection. This includes managing packet rules, YARA rules, STIX indicators, Sigma rules, and vulnerabilities. **Threat Intelligence™** allows new content to be added, edited, and deleted, and existing content to be enabled or disabled.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

Two-factor authentication

2FA is a method that lets you add additional security to an account. The first factor is a standard password, the second factor is a code that is used on an app on a mobile device or computer that verifies the user.

Uniform Resource Identifier

A URI is a unique string of characters used to identify a logical or physical resource on the internet or local network.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

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).