Guardian
User Guide

N2OS v24.3.1 — 2024-09-09

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

Guardian overview

Guardian is the main Nozomi Networks sensor.

Asset discovery

Guardian gives you the ability to automatically track your *industrial control systems (ICS)*, *operational technology (OT)* and *Internet of Things (IoT)*/*Industrial Internet of Things (IIoT)* assets.

- Highly accurate asset inventory of all communicating devices
- Extensive node information including name, type, serial number, firmware version and components
- Actionable risk assessment insights including security and reliability alerts, missing patches and vulnerabilities

Network visualization

Guardian gives you instant visibility of your entire network. This lets you:

- Have instant awareness of your *OT*/*IoT* networks and normal activity patterns
- Access key data such as traffic throughput, *transmission control protocol (TCP)* connections, and protocols
- Use intuitive dashboards and reports with macro and micro views, plus filtering and grouping

Automated vulnerability assessment

Guardian lets you quickly identify which *ICS*, *OT* and *IoT* devices are vulnerable. This provides:

- Efficient prioritization and remediation
- A faster response with vulnerability dashboards, drill-downs and reports
- Based on the U.S. government's *National Vulnerability Database (NVD)* for standardized naming, description and scoring

Continuously monitor your networks and automation systems. Guardian gives you:

- The ability to continuously monitor all your assets, network communications and supported protocols
- Easy access to summarized *ICS*, *OT* and *IoT* risk information
- The ability to highlight potential reliability issues, such as unusual process values

Anomaly-based detection

Guardian builds a baseline of your environment and uses that knowledge to detect threats such as transferred malware, suspicious communications, unwanted operations, or changes to the network.

Chapter 2. Sensors

Sensors

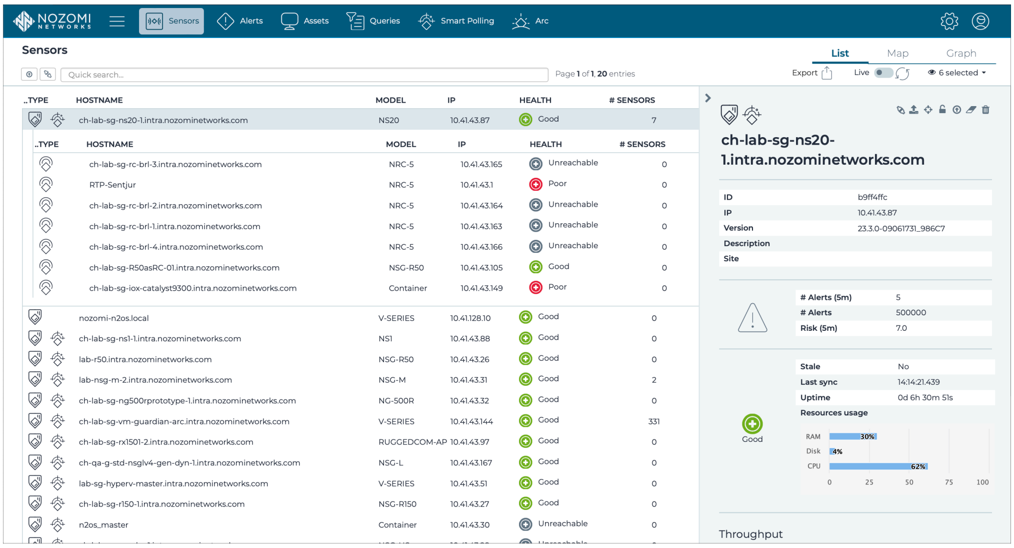
*The **Sensors** page lets you view all of the sensors that you have in your system.*

The **Sensors** page has these three tabs:

- List
- Map
- Graph

List

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



Sensors

Page 1 of 1, 20 entries

..TYPE	HOSTNAME	MODEL	IP	HEALTH	# SENSORS
	ch-lab-sg-ns20-1.intra.nozominetworks.com	NS20	10.41.43.87	Good	7

..TYPE	HOSTNAME	MODEL	IP	HEALTH	# SENSORS
	ch-lab-sg-rc-brl-3.intra.nozominetworks.com	NRC-5	10.41.43.165	Unreachable	0
	RTP-Sentjur	NRC-5	10.41.43.1	Poor	0
	ch-lab-sg-rc-brl-2.intra.nozominetworks.com	NRC-5	10.41.43.164	Unreachable	0
	ch-lab-sg-rc-brl-1.intra.nozominetworks.com	NRC-5	10.41.43.163	Unreachable	0
	ch-lab-sg-rc-brl-4.intra.nozominetworks.com	NRC-5	10.41.43.166	Unreachable	0
	ch-lab-sg-R50asRC-01.intra.nozominetworks.com	NSG-R50	10.41.43.105	Good	0
	ch-lab-sg-iox-catalyst9300.intra.nozominetworks.com	Container	10.41.43.149	Poor	0

..TYPE	HOSTNAME	MODEL	IP	HEALTH	# SENSORS
	nozomi-n2os.local	V-SERIES	10.41.128.10	Good	0
	ch-lab-sg-ns1-1.intra.nozominetworks.com	NS1	10.41.43.88	Good	0
	lab-r50.intra.nozominetworks.com	NSG-R50	10.41.43.26	Good	0
	lab-nsg-m-2.intra.nozominetworks.com	NSG-M	10.41.43.31	Good	2
	ch-lab-sg-ng500rprototype-1.intra.nozominetworks.com	NG-500R	10.41.43.32	Good	0
	ch-lab-sg-vm-guardian-arc.intra.nozominetworks.com	V-SERIES	10.41.43.144	Good	331
	ch-lab-sg-rx1501-2.intra.nozominetworks.com	RUGGEDCOM-AP	10.41.43.97	Good	0
	ch-qa-g-std-nsglv4-gen-dyn-1.intra.nozominetworks.com	NSG-L	10.41.43.167	Good	0
	lab-sg-hyperv-master.intra.nozominetworks.com	V-SERIES	10.41.43.51	Good	0
	ch-lab-sg-r150-1.intra.nozominetworks.com	NSG-R150	10.41.43.27	Good	0
	n2os_master	Container	10.41.43.30	Unreachable	0

ch-lab-sg-ns20-1.intra.nozominetworks.com

ID	b9ff4ffc
IP	10.41.43.87
Version	23.3.0-09061731_986C7
Description	
Site	

# Alerts (5m)	5
# Alerts	500000
Risk (5m)	7.0

Good

Stale	No
Last sync	14:14:21.439
Uptime	0d 6h 30m 51s

Resources usage

Throughput

Figure 1. Sensors list

Force update

The force update ⊕ icon lets you do a force update on the selected sensors.

Allow/disallow

The allow/disallow ⛓ icon lets you allow or disallow sensors.

Quick search

The quick search field lets you easily do a search on the current page.

Export

The **Export** ⇪ icon lets you export the current list in either *comma-separated value (CSV)* or Microsoft Excel format.

Download Arc

The **Download Arc** dropdown lets you select, and download, the applicable Arc package for your *operating system (OS)* and architecture.

Live

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

Refresh

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

Column selection

The columns selection icon lets you choose which columns to show or hide.

Information pane

The information pane to the right of the list of sensors shows additional information for the selected sensor.

It also lets you do these actions shown below.

Table 1. Sensors list actions

Allow/Disallow sensor	After allowing a sensor, this icon shows: Synchronized data coming from the sensor become part of the Environment of the *Central Management Console (CMC)*. Alerts coming from the sensor can be seen in the **Alerts** section.
Focus on sensor	Allows to filter out only the sensor chosen data, such as Alerts and Environment.
Go to sensor	Connect to a remote sensor directly from the *CMC*. Select this to open a new browser tab to the sensor selected login page. The action is hidden if the *CMC* isn't configured to allow this type of communication between sensors and *CMC*.
Place in map	This action is used to place the sensor on the map.
Toggle version lock	When locked, the sensor will not automatically update its software.
Force update	Even if it is locked, the sensor will automatically update its software, with the version installed on the *CMC*.
Clear sensor data on this machine	Clear all synchronized data at the *CMC* received from the selected sensor. Use this in combination with the clearing of the data on the sensor, and you will be able to restart the synchronization between the sensor and the *CMC* from an empty state
Delete sensor	Clear all data received from the selected sensor and delete it from the list. If the sensor tries to sync with the *CMC* again, it shows as disallowed in the list.

Map

*You can use the **Map** page to upload, and view, a map of the sensors in your environment.*

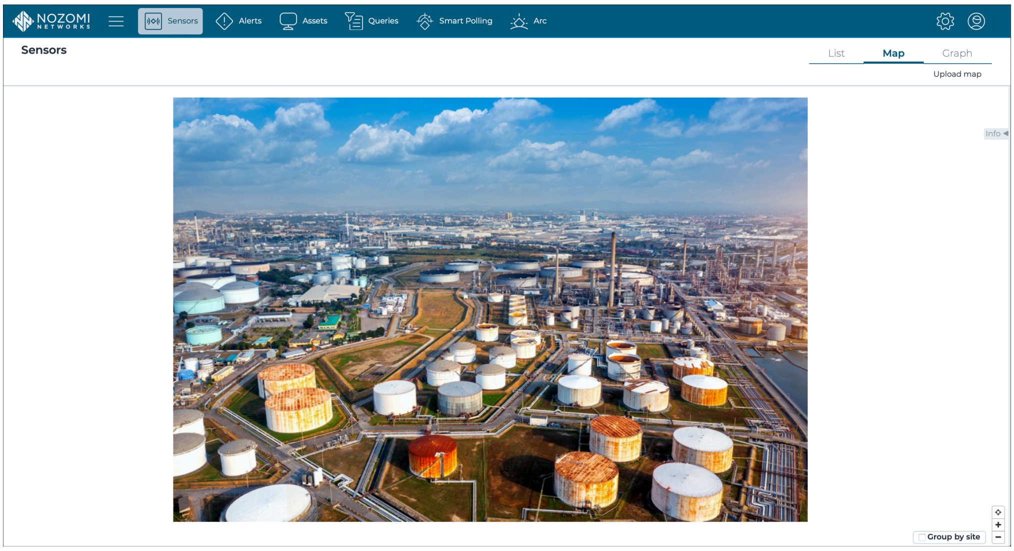
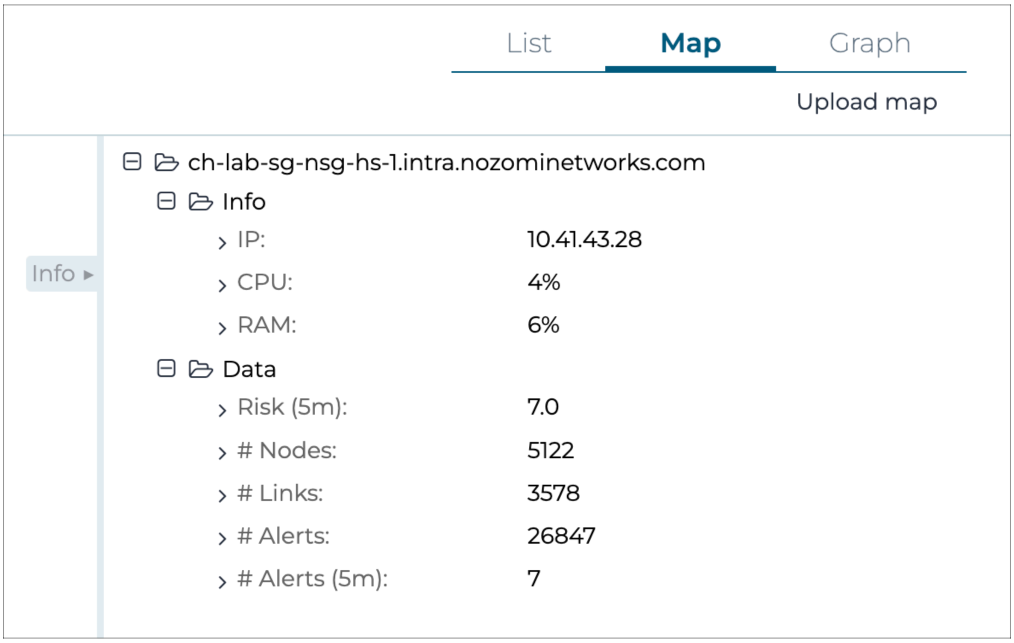


Figure 2. Sensors map

Info(rmation) pane



ch-lab-sg-nsg-hs-1.intra.nozominetworks.com

Info

› IP:	10.41.43.28
› CPU:	4%
› RAM:	6%

Data

› Risk (5m):	7.0
› # Nodes:	5122
› # Links:	3578
› # Alerts:	26847
› # Alerts (5m):	7

Figure 3. Info(rmation) pane

The **Info** pane lets you view information for the related sensor. The *identifier (ID)* of each sensor is used in the map to help you identify it. The marker color of the sensor relates to the risk of its alerts.

In the map view, a red indicator to the right of the sensor's *ID* shows the number of the alerts in the last five minutes. This indicator only shows if there are some alerts for the sensor. If the alerts in last 5 minutes increase, the sensor marker will blink for one minute.

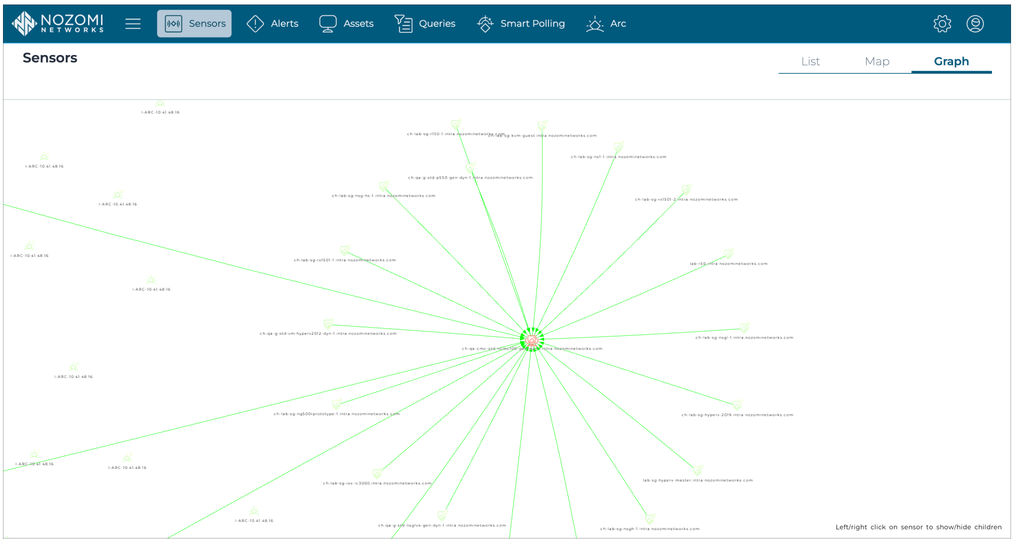
If the site of the sensor has been specified in ⚙ **> System > General**, it is possible to enable the **Group by site** option, in the bottom right corner of the map view. The sensors with the same site will be grouped to deliver a simpler view of a complex installation.

Note:

The sensors map is also available as a widget.

Graph

*The **Graph** page shows a graphical view of all the sensors in you environment.*


NOZOMI NETWORKS
Sensors
Alerts
Assets
Queries
Smart Polling
Arc
Sensors
List
Map
Graph
I-ARC-10.41.48.16
ch-lab-sg-r150-1.intra.nozominetworks.com
ch-lab-sg-kvm-guest.intra.nozominetworks.com
ch-lab-sg-ns1-1.intra.nozominetworks.com
ch-qa-g-std-p550-gen-dyn-1.intra.nozominetworks.com
ch-lab-sg-nsg-hs-1.intra.nozominetworks.com
ch-lab-sg-rx1501-2.intra.nozominetworks.com
ch-lab-sg-rx1501-1.intra.nozominetworks.com
lab-r50.intra.nozominetworks.com
ch-qa-g-std-vm-hyperv2012-dyn-1.intra.nozominetworks.com
ch-lab-sg-nsgl-1.intra.nozominetworks.com
ch-qa-cmc-std-ncmc100-ge[illegible].intra.nozominetworks.com
ch-lab-sg-ng500rprototype-1.intra.nozominetworks.com
ch-lab-sg-hyperv-2019.intra.nozominetworks.com
lab-sg-hyperv-master.intra.nozominetworks.com
ch-lab-sg-iox-ic3000.intra.nozominetworks.com
ch-qa-g-std-nsglv4-gen-dyn-1.intra.nozominetworks.com
ch-lab-sg-nsgh-1.intra.nozominetworks.com

Left/right click on sensor to show/hide children

Figure 4. Sensors graph

Do a force update on sensors

If you have disabled auto updates, you can use the force update icon to do a manual update.

Procedure

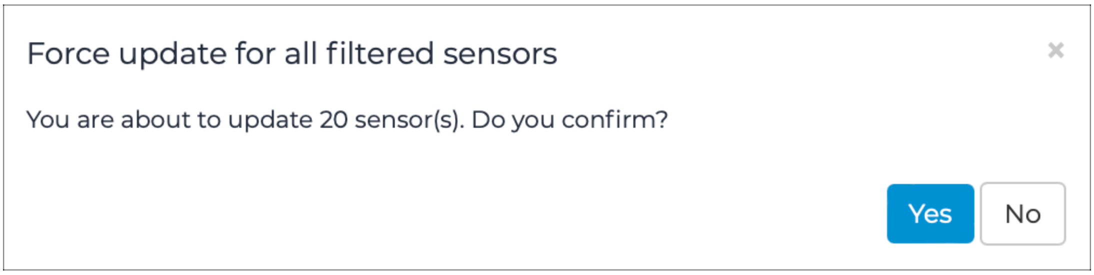
1. In the top navigation bar, select **Sensors**.

   Result: The **Sensors** page opens.

2. In the top left section, select ⬆.

   Result: A dialog shows.

3. To confirm, select **Yes**.



Force update for all filtered sensors

You are about to update 20 sensor(s). Do you confirm?

Allow a sensor

The allow icon lets you give permission for a new sensor to connect to Central Management Console (CMC).

Procedure

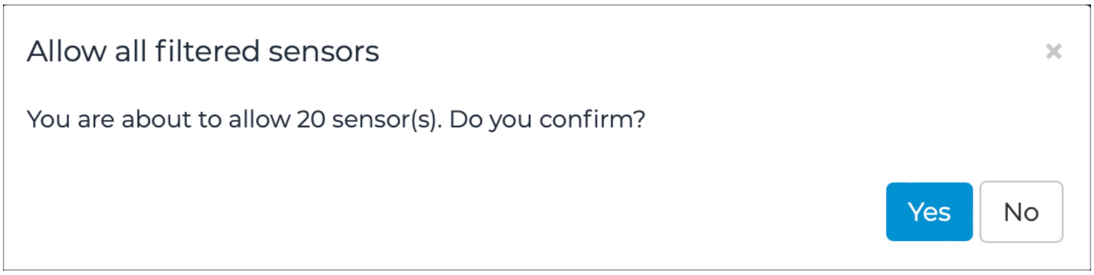
1. In the top navigation bar, select **Sensors**.

   Result: The **Sensors** page opens.

2. In the top left section, select the 🔌 icon.

   Result: A dialog shows.

3. To confirm, select **Yes**.



Allow all filtered sensors

You are about to allow 20 sensor(s). Do you confirm?

Export a list of sensors

You can export a list of the sensors from the current view.

Procedure

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

   Result: The **Sensors** page opens.

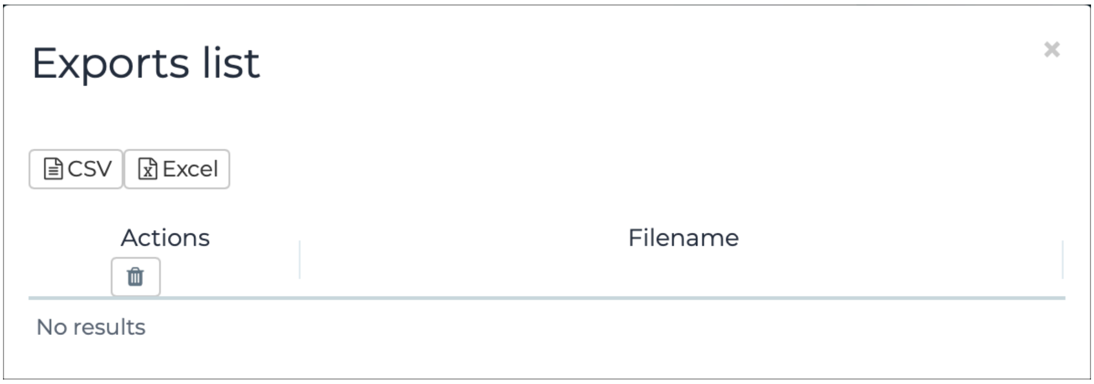
2. In the top right section, select **Export**.

   Result: A dialog shows.

3. Choose an export format:

   Choose from:

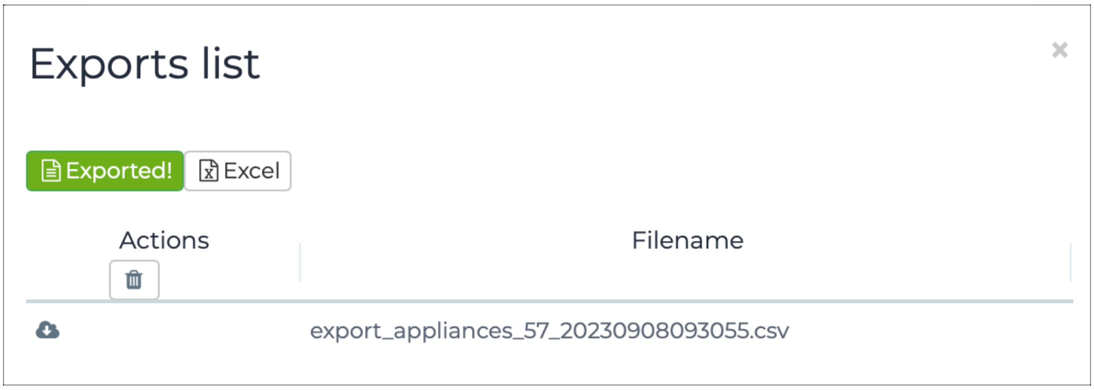
   - Select **CSV** to create a *CSV* file
   - Select **Excel** to create a Microsoft Excel file



Actions	Filename
🗑	
No results	

   Result: The file is created and a `Exported` message shows.

4. To download the file, in the bottom-left of the dialog, select ☁



Actions	Filename
🗑	
☁	export_appliances_57_20230908093055.csv

Results

The exported file has been downloaded.

Upload a map

*The **Map** page lets you upload a map of your sensors in your environment.*

Procedure

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

   Result: The **Sensors** page opens.

2. In the top right section, select **Map**.

   Result: The **Map** page opens.

3. In the top right section, select **Upload map.**
4. Select the image file that you want to upload.

Results

The map is uploaded.

Configure an Arc sensor

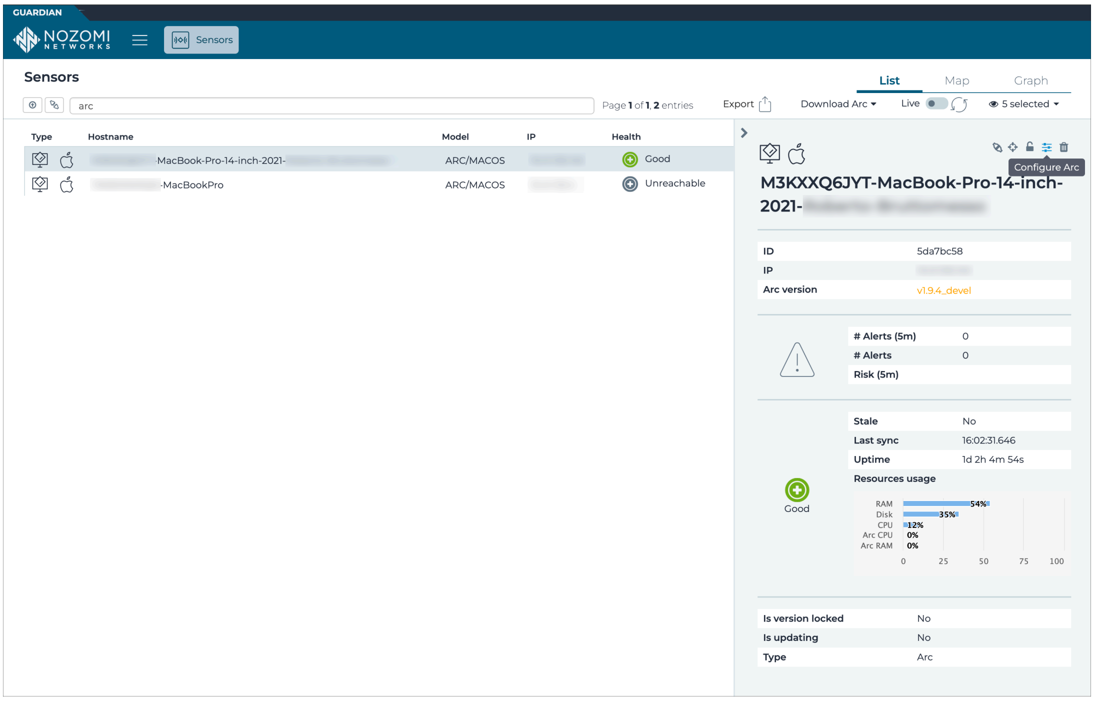
*It is possible to configure an individual Arc sensor directly from the **Sensors** details page for the related sensor.*

Procedure

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

   Result: The **Sensors** page opens.

2. From the list, select the applicable Arc sensor.



Sensors

arc

Page 1 of 1, 2 entries

Type	Hostname	Model	IP	Health
	[redacted]-MacBook-Pro-14-inch-2021-[redacted]	ARC/MACOS	[redacted]	Good
	[redacted]-MacBookPro	ARC/MACOS	[redacted]	Unreachable

M3KXXQ6JYT-MacBook-Pro-14-inch-2021-[redacted]

ID	5da7bc58
IP	[redacted]
Arc version	v1.9.4_devel

# Alerts (5m)	0
# Alerts	0
Risk (5m)	

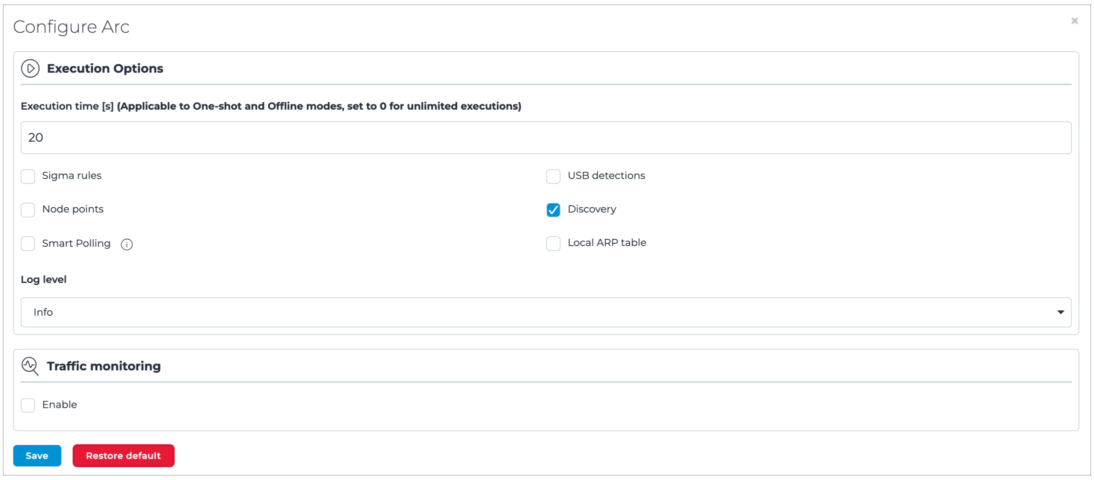
Stale	No
Last sync	16:02:31.646
Uptime	1d 2h 4m 54s
Resources usage	

Is version locked	No
Is updating	No
Type	Arc

3. In the top right section, select the ☰ icon.

   Result: A dialog shows.

4. Choose the applicable options.



Configure Arc

Execution Options

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

20

□ Sigma rules	□ USB detections
□ Node points	☑ Discovery
□ Smart Polling	□ Local ARP table

Log level

Info

Traffic monitoring

□ Enable

5. Select **Save**.

Results

The Arc sensor has been configured.

Chapter 3. Alerts

Alerts

*The **Alerts** page shows all the latest alerts in the system. It lets you view the alerts in different modes, and carry out actions on the alerts.*

Important:
To perform actions on alerts, the user must belong to a group with admin permissions. Non-admin users can access alerts only if at least one of the groups that they belong to has alerts permission enabled.

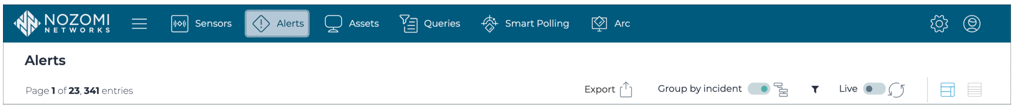


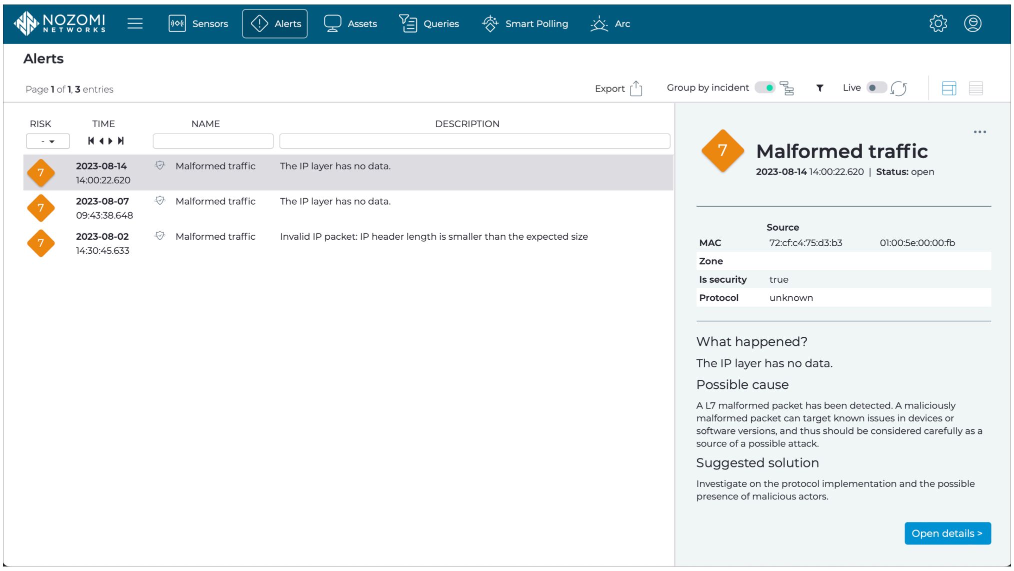
Figure 5. Alerts page menu

The top right section of the **Alerts** page has two icons that let you change between these two options:

- Standard mode (on page 28)
- Expert mode (on page 29)

Standard mode

You can view alerts in standard mode to give you an overview of the latest anomalies.



Alerts

Page **1** of **1**, **3** entries

RISK	TIME	NAME	DESCRIPTION
7	**2023-08-14** 14:00:22.620	Malformed traffic	The IP layer has no data.
7	**2023-08-07** 09:43:38.648	Malformed traffic	The IP layer has no data.
7	**2023-08-02** 14:30:45.633	Malformed traffic	Invalid IP packet: IP header length is smaller than the expected size

7 **Malformed traffic**

2023-08-14 14:00:22.620 | **Status:** open

	Source	
MAC	72:cf:c4:75:d3:b3	01:00:5e:00:00:fb
Zone		
Is security	true	
Protocol	unknown	

What happened?

The IP layer has no data.

Possible cause

A L7 malformed packet has been detected. A maliciously malformed packet can target known issues in devices or software versions, and thus should be considered carefully as a source of a possible attack.

Suggested solution

Investigate on the protocol implementation and the possible presence of malicious actors.

Figure 6. Standard mode

Risk

This shows the risk associated to each alert or incident.

Time

The time related to each event.

Name

The name category of the event.

Description

This shows a detailed description of the related event.

Analysis

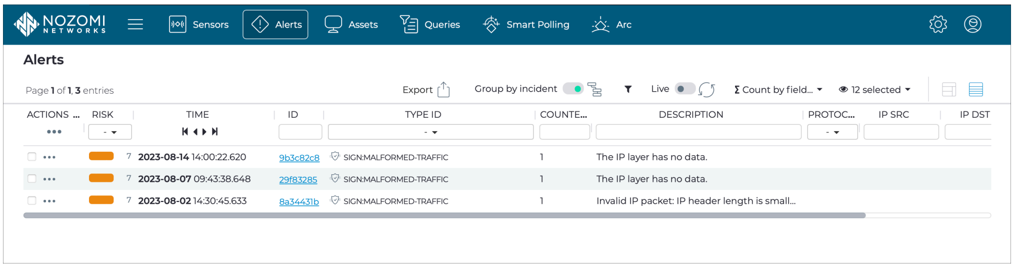
If you can select a row, this pane will show a more detailed analysis of the alert.

Expert mode

You can view alerts in expert mode to give you a detailed view of the alerts in the system. This lets you filter, sort, and analyze the information in detail.

Expert mode shows a comprehensive table layout, with details on the alerts and incidents listed, which include:

- Addresses
- Labels
- The roles of the involved nodes, zones, protocol, and ports used in the involved transactions, and more



Alerts

Page 1 of 1, 3 entries

ACTIONS ...	RISK		TIME	ID	TYPE ID	COUNTE...	DESCRIPTION	PROTOC...	IP SRC	IP DST
□ •••	🟧	7	**2023-08-14** 14:00:22.620	9b3c82c8	SIGN:MALFORMED-TRAFFIC	1	The IP layer has no data.			
□ •••	🟧	7	**2023-08-07** 09:43:38.648	29f83285	SIGN:MALFORMED-TRAFFIC	1	The IP layer has no data.			
□ •••	🟧	7	**2023-08-02** 14:30:45.633	8a34431b	SIGN:MALFORMED-TRAFFIC	1	Invalid IP packet: IP header length is small...			

Figure 7. Expert mode

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Group by incident

The **Group by incident** icon lets you group alerts by incident. This will show incidents, and hide all the alerts that belong to it.

Filter

The filter icon opens a list of items that you let you filter the results.

Live

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

Refresh

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

Count by field

The **∑ Count by field** dropdown lets you select a data field on which to group and count the alerts.

Column selection

The columns selection icon lets you choose which columns to show or hide.

View alerts in standard mode

You can view alerts in standard mode to give you an overview of the latest anomalies.

Procedure

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

   Result: The **Alerts** page opens.

2. In the top right corner, select the standard mode icon.

   Result: The Standard mode (on page 28) view opens.

View alerts in expert mode

You can view alerts in expert mode to give you a detailed view of the alerts in the system. This lets you filter, sort, and analyze the information in detail.

Procedure

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

   Result: The **Alerts** page opens.

2. In the top right corner, select the expert mode icon.

   Result: The Expert mode (on page 29) view opens.

Closing alerts

When you close an alert, or incident, a dialog lets you select a reason, and specify the learning process.

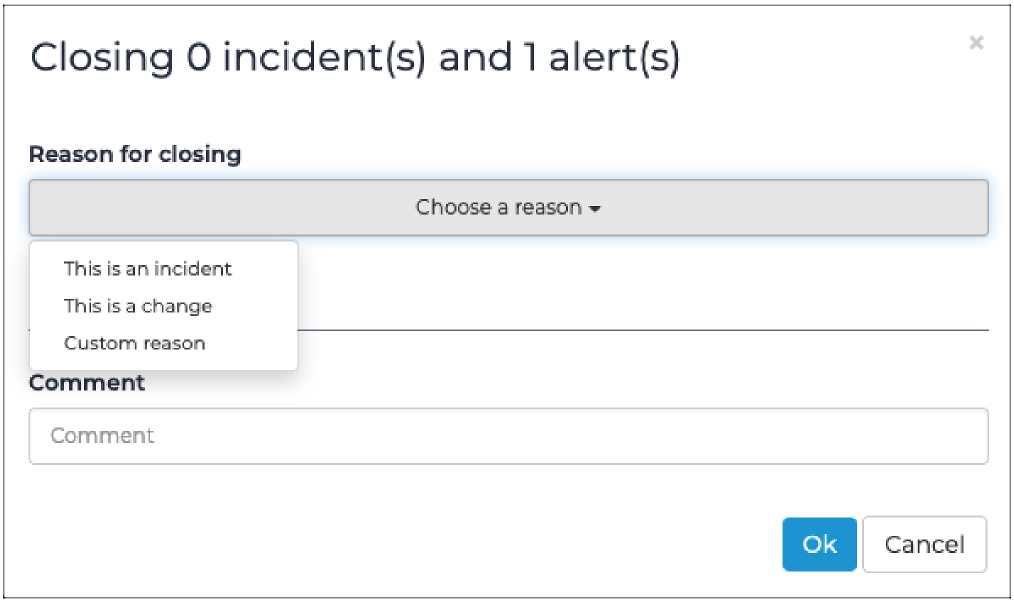


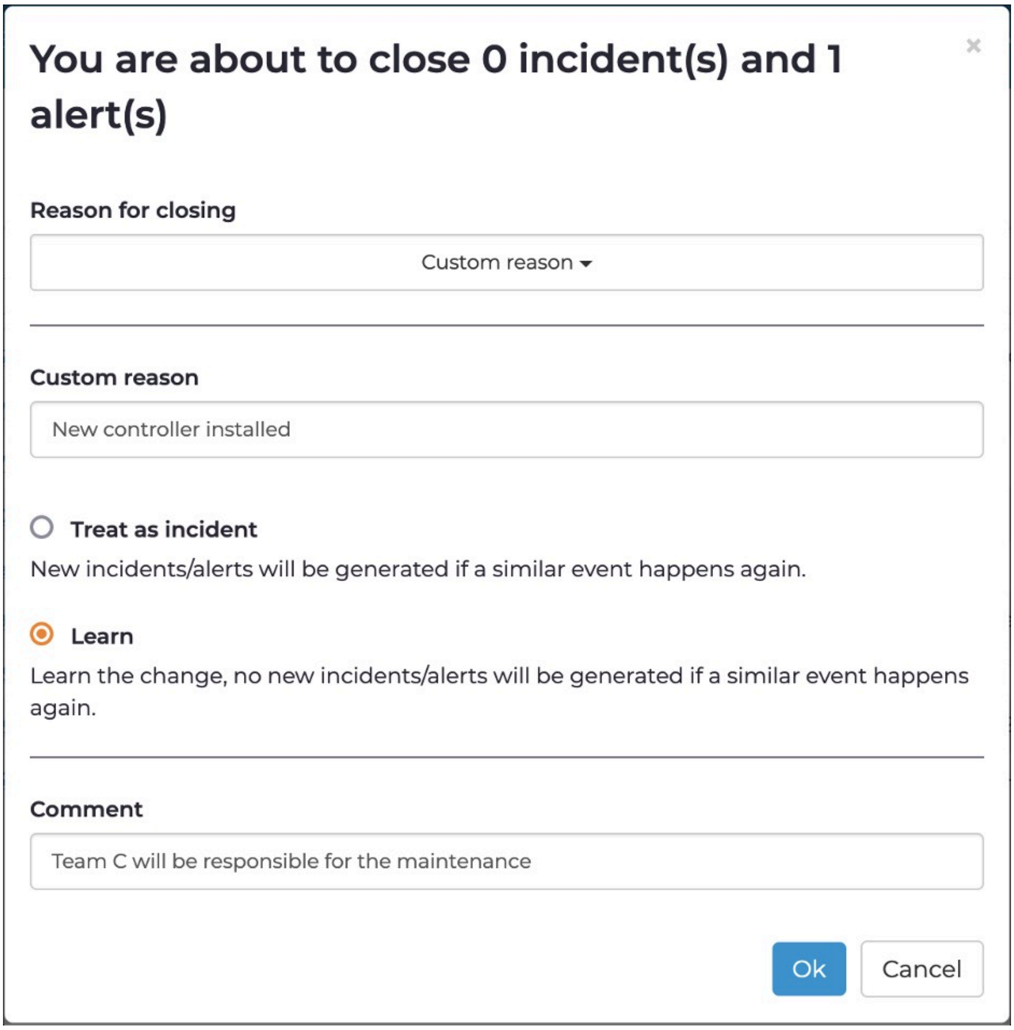
Figure 8. Alerts closing dialog

The **Reason for closing** dropdown has these options:

- **This is a change**: If the cause of the alert is an intended change to the network, such as:
    - A new computer being attached
    - New communication between two nodes that were not previously communicating

  Guardian can learn the change that has been detected as part of the environment baseline. When you close an alert in this way, the *intrusion detection system (IDS)* is instructed to learn the related objects. For example, when a `VI:NEW-NODE` alert is closed as a change, Guardian registers that the corresponding node is part of the environment and will not raise subsequent `VI:NEW-NODE` alerts about the same node.
- **This is a change**: If the cause of the alert is an intended change to the network, such as a new computer being attached, or a new communication between two nodes that were not talking before, the change detected by Guardian can be learned as part of the environment baseline. When closing an alert in this way, the IDS is instructed to learn the corresponding objects. For example, when a VI:NEW-NODE alert is closed as a change, Guardian registers that the corresponding node is part of the environment and will not raise subsequent VI:NEW-NODE alerts about the same node.

- **This is an incident**: If the cause of the alert is a configuration error, an attack, a malfunctioning device, or other security incident, the change is not learned as part of the environment baseline. When closing an alert in this way, the IDS is instructed to delete the corresponding objects. For example, a new node entering the network for the first time causes a VI:NEW-NODE alert. If an alert closes as an incident, reference to the new node is deleted. The VI:NEW-NODE alert is raised again in subsequent communication involving the same node.
- **Custom reason**: This lets you write a custom reason for closing an alert. You can enter a text string as the closing reason, with a request to apply one of the two described behaviors.



You are about to close 0 incident(s) and 1 alert(s)

Reason for closing: Custom reason ▾

Custom reason: New controller installed

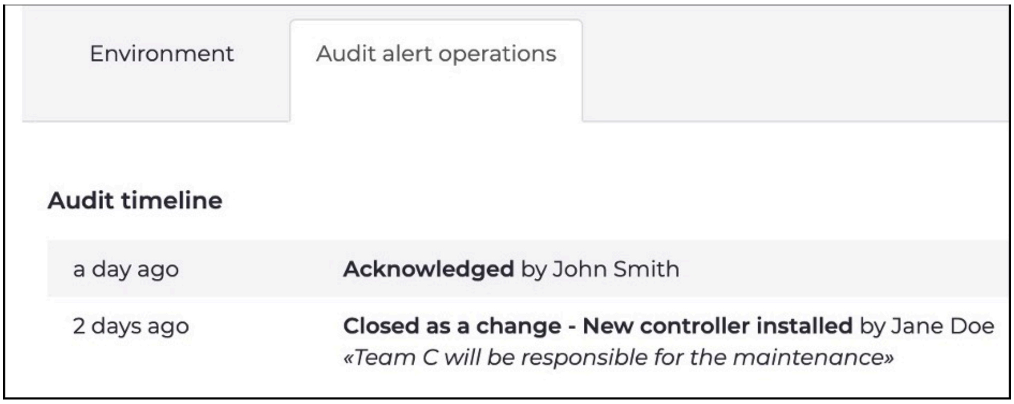
○ Treat as incident
New incidents/alerts will be generated if a similar event happens again.

● Learn
Learn the change, no new incidents/alerts will be generated if a similar event happens again.

Comment: Team C will be responsible for the maintenance

Figure 9. Closing alert for custom reason with comment

You can add a comment so that it shows in the **alert audit** log.



Audit timeline

a day ago	**Acknowledged** by John Smith
2 days ago	**Closed as a change - New controller installed** by Jane Doe *«Team C will be responsible for the maintenance»*

Figure 10. Audit alert operations

Actions menu

*The **Actions** menu gives you access to all the actions that you can do for the related alert.*

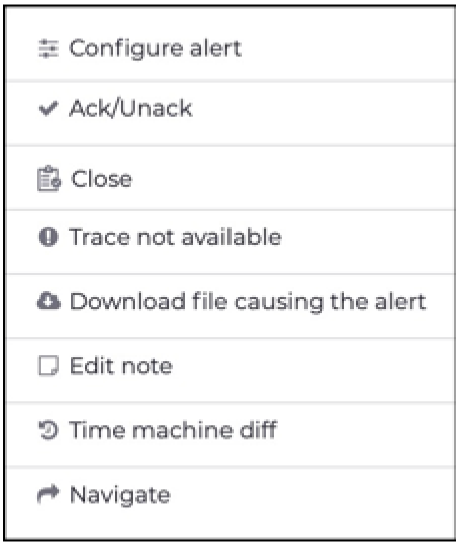


Figure 11. Actions menu

Note:
The options available in the **Actions** menu can change. The options will depend on:

- The type of alert
- The state of the sensor
- Whether the sensor is a Guardian or a *CMC*

Configure alert

You can use the **Configure alert** option to create a new alert rule for future events that are similar to the current one.

Ack/Unack

Once an alert or incident shows, you can mark it as acknowledged. You can also change the status back to unacknowledged again.

Close

Once an alert or incident has been addressed, you can mark it as closed, and choose the type of learning operation to perform.

Download trace

If a trace is available, you can choose to download it. The trace contains the packet that triggered the alert, along with an extract of the same session before and after that packet. Traces might be unavailable if the appliance is under stress. For detections that require multiple packets, such as **Multiple login failures**, the trace might not contain enough traffic to reproduce the alert. Incidents do not have an associated trace.

Download file causing the alert

Once a sensor has detected a malicious file, it is possible to download it for analysis. After you select this option, a dialog shows to warn the user that the file has been identified as malicious, or unwanted. To download the file, the user must acknowledge that they will do so at their own risk. In a *CMC*, this option is only available after the applicable file has been requested, (see below).

Edit note

Once an alert or incident shows, you can write a note for it, or edit an existing one.

Time machine diff

It is possible to open a time machine diff which corresponds to the time of the alert, or incident.

Navigate

Alerts and incidents have related nodes, links, vulnerabilities, or sessions. The **Actions** menu lets you navigate to these links.

Open the Actions menu in standard mode

*You can open the **Actions** menu to give you access to additional operations. When you are in standard mode, there are two different options available to open the menu.*

Procedure

1. View alerts in standard mode (on page 30).
2. Choose a method to open the **Actions** menu.

   Choose from:

   - Select the applicable alert, go to the top right corner and select the ••• icon
   - Select the **Open details** button. In the detailed view window, go to the top left corner and select the ••• icon

   Result: The **Actions** menu opens.

Open the Actions menu in expert mode

*You can open the **Actions** menu to give you access to additional operations.*

Procedure

1. View alerts in expert mode (on page 30).
2. Choose a method to open the **Actions** menu.

   Choose from:

   - To the left of the applicable alert, select the ••• icon
   - Select the link in the **ID** column. In the detailed view window, go to the top left corner and select the ••• icon

   Result: The **Actions** menu opens.

Configure an alert

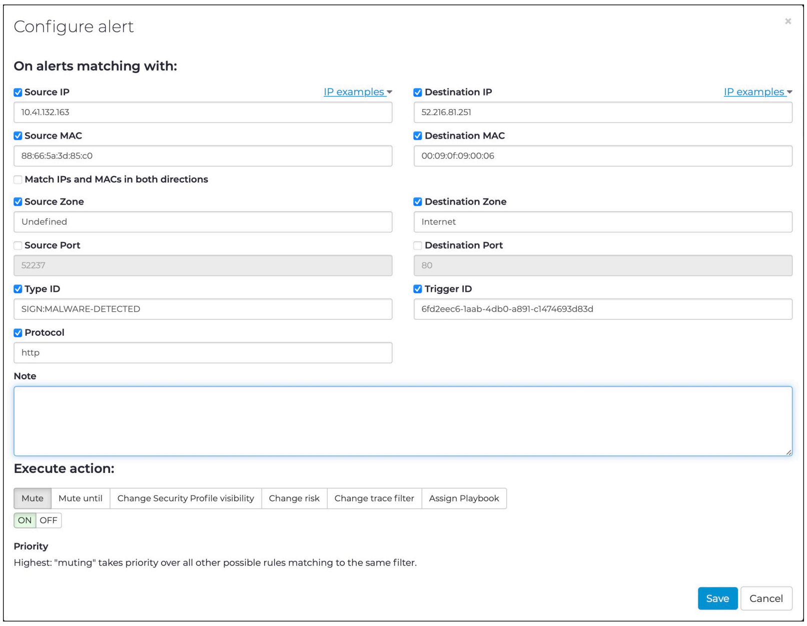
*You can use the **Configure alert** option to create a new alert rule for future events that are similar to the current one.*

Procedure

1. Open the **Actions** menu for the selected alert(s) with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)

2. Select **Configure alert**.

   Result: A dialog shows.



Configure alert

On alerts matching with:

☑ Source IP: 10.41.132.163

☑ Destination IP: 52.216.81.251

☑ Source MAC: 88:66:5a:3d:85:c0

☑ Destination MAC: 00:09:0f:09:00:06

☐ Match IPs and MACs in both directions

☑ Source Zone: Undefined

☑ Destination Zone: Internet

☐ Source Port: 52237

☐ Destination Port: 80

☑ Type ID: SIGN:MALWARE-DETECTED

☑ Trigger ID: 6fd2eec6-1aab-4db0-a891-c1474693d83d

☑ Protocol: http

Note

Execute action:

Mute: ON

Priority

Highest: "muting" takes priority over all other possible rules matching to the same filter.

3. In each of the fields, enter the necessary details.
4. Select **Save**.

Results

The alert has been configured.

Acknowledge an alert

Once an alert or incident shows, you can mark it as acknowledged. You can also change the status back to unacknowledged again.

Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)
2. Select **Ack/Unack**.

   Result: After a few seconds, the tick symbol changes from grey to green.
3. If necessary, click the **Ack/Unack** option again to cancel the acknowledgment.

   Result: After a few seconds, the tick symbol changes from green to grey.

Close an alert

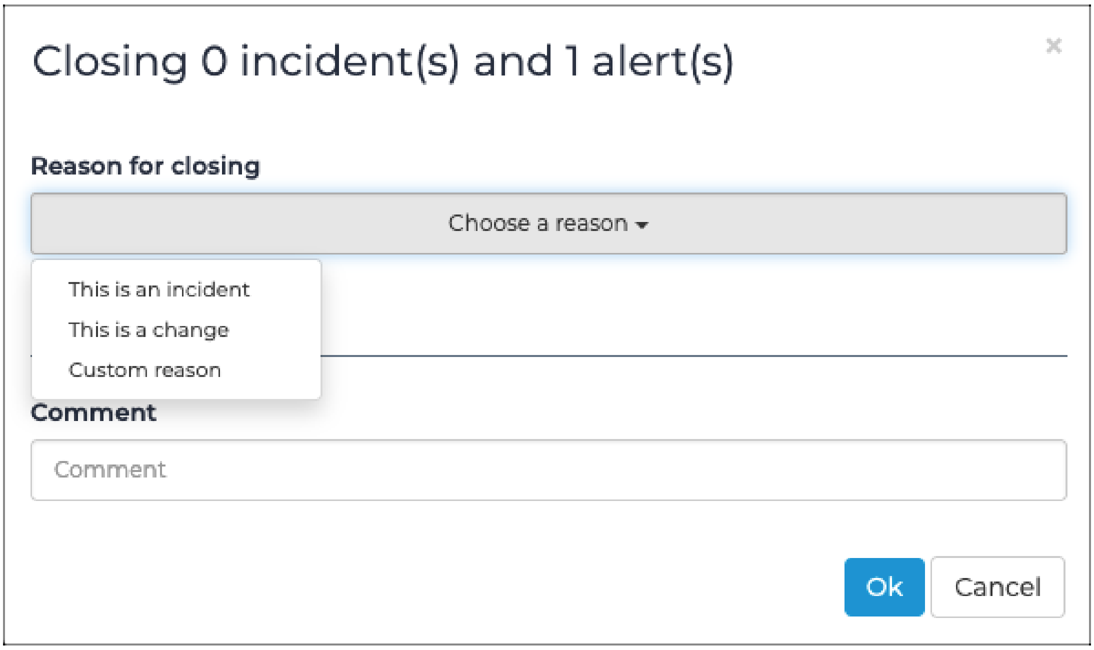
Once an alert or incident shows, you can mark it as closed, and choose the type of learning operation to perform.

Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)

2. Select **Close**.

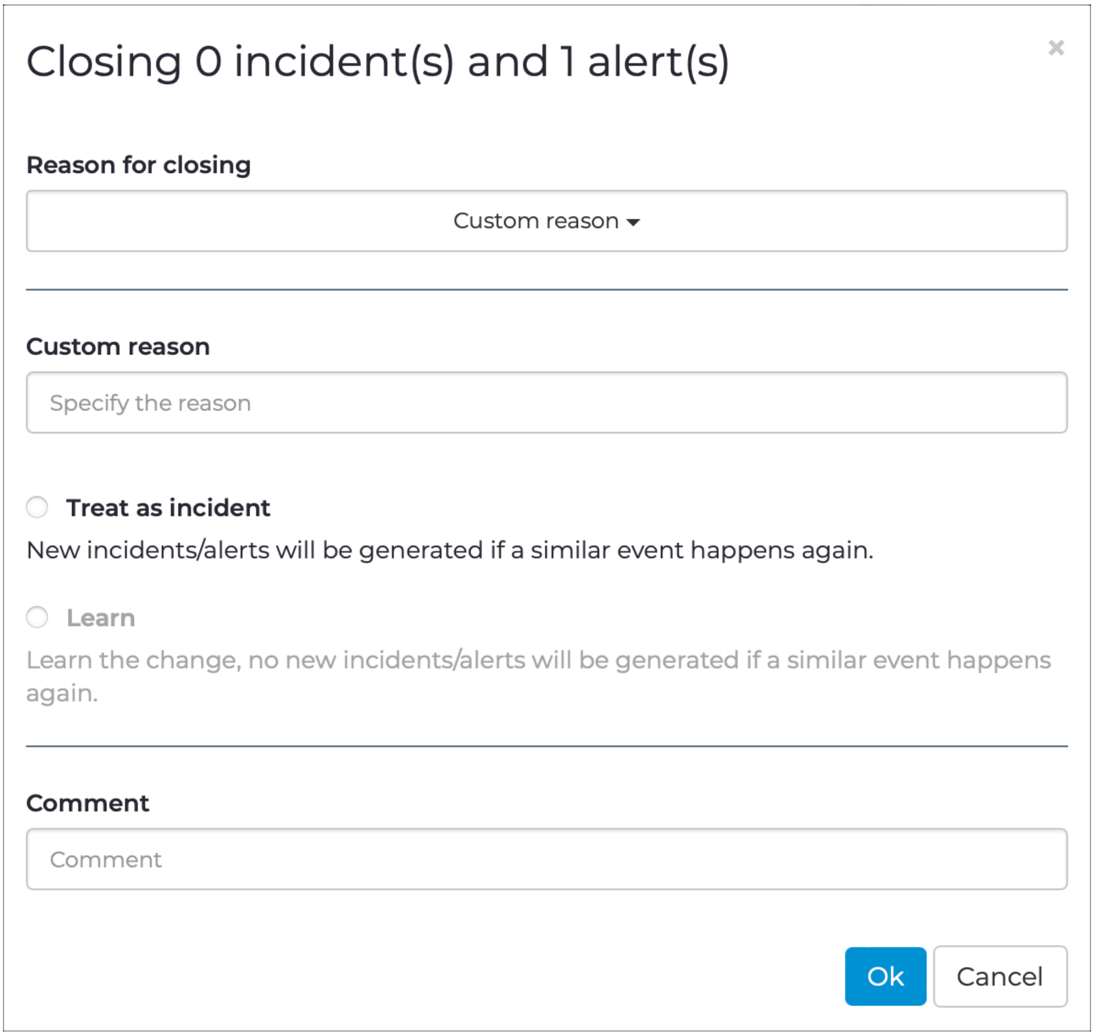
   Result: A dialog shows.



3. In the **Reason for closing** dropdown, choose one of these options:

   Choose from:
   - **This is a security incident**
   - **Custom reason**

4. If you chose **Custom reason**, the dialog will extend to show more options.



Closing 0 incident(s) and 1 alert(s)

Reason for closing

Custom reason

Custom reason

Specify the reason

○ **Treat as incident**

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

○ **Learn**

Learn the change, no new incidents/alerts will be generated if a similar event happens again.

Comment

Comment

5. If you chose **Custom reason**, do the steps that follow.
   a. In the **Custom reason** field, enter the details as necessary.
   b. Choose from one of these options:
      - **Treat as incident**
      - **Learn**
6. If necessary, enter a comment in the **Comment** field.
7. Select **Ok**.

Download a trace

If a trace is available, you can choose to download it. The trace contains the packet that triggered the alert, along with an extract of the same session before and after that packet. Traces might be unavailable if the appliance is under stress.

Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)
2. Select **Download trace**.

   Result: The file downloads to your downloads folder.

Download a malicious file

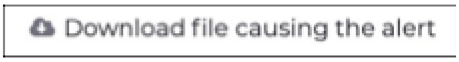
Once a sensor has detected a malicious file, it is possible to download it for analysis.

About this task

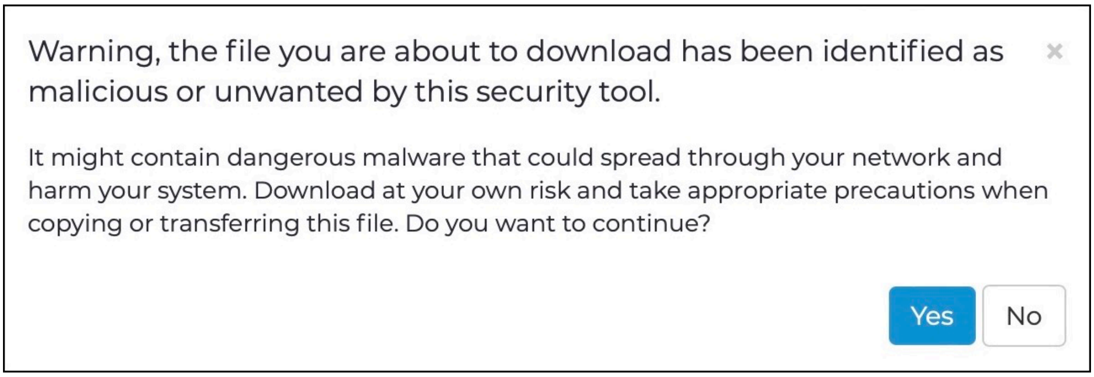
Only qualified personnel should download malicious files. Before you do this procedure, make sure that you have the correct permissions.

Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)
2. Select **Download file causing the alert**.

   Result: A dialog shows.

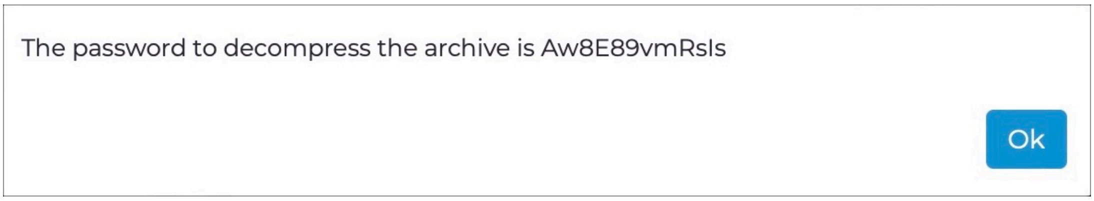
   Warning, the file you are about to download has been identified as malicious or unwanted by this security tool.

   It might contain dangerous malware that could spread through your network and harm your system. Download at your own risk and take appropriate precautions when copying or transferring this file. Do you want to continue?

3. If you want to proceed, select **Yes**.

   Important:
   Nozomi Networks recommends that only qualified personnel download malicious, or unwanted, files. Download these files at your own risk.

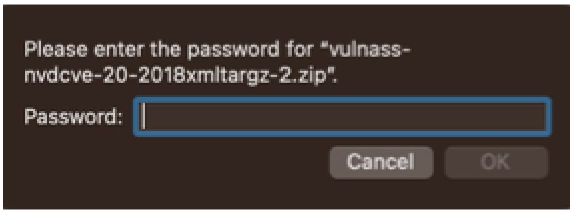
   Result: The file downloads to your downloads folder and a password dialog that contains a randomized, single-use password shows.



The password to decompress the archive is Aw8E89vmRsls

4. Copy the password, and select **Ok**.
5. Go to the folder where the file was downloaded to.
6. Double-click the *ZIP* file to open it.

   Result: A dialog that prompts you to enter a password shows.



Please enter the password for "vulnass-nvdcve-20-2018xmltargz-2.zip".

Password:

7. Paste the password into the password field and select **OK**.

   Result: You can now access the file.

Edit a note for an alert

Once an alert or incident shows, you can write a note for it, or edit an existing one.

Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:
   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)
2. Select **Edit note**.

   Result: A note is opened with the identification of the related alert, or incident.

3. In the text field, write a note.

> **Note:**
>
> There is a character limit of 1000 characters.

4. Select **Save**.

Results

The note has been edited.

View a diff from an alert

This automatic feature will use the previous and subsequent snapshots according to the time of the alert.

Procedure

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

   Result: The **Alerts** 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 **Time machine diff**.

   Result: The time diff shows.

4. To see more details on the right side of the graph, select the applicable node or link.

Navigate from an alert

Alerts and incidents have related nodes, links, vulnerabilities, or sessions. The actions menu lets you navigate to these links.

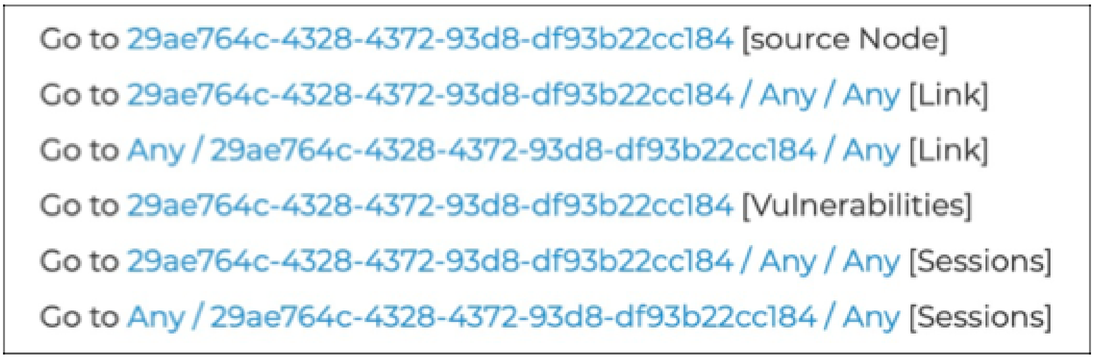
Procedure

1. Open the **Actions** menu for the applicable file with one of the these options:

   - Open the Actions menu in standard mode (on page 36)
   - Open the Actions menu in expert mode (on page 36)

2. Click the **Navigate** option.

   Result: A dialog shows.



Go to 29ae764c-4328-4372-93d8-df93b22cc184 [source Node]

Go to 29ae764c-4328-4372-93d8-df93b22cc184 / Any / Any [Link]

Go to Any / 29ae764c-4328-4372-93d8-df93b22cc184 / Any [Link]

Go to 29ae764c-4328-4372-93d8-df93b22cc184 [Vulnerabilities]

Go to 29ae764c-4328-4372-93d8-df93b22cc184 / Any / Any [Sessions]

Go to Any / 29ae764c-4328-4372-93d8-df93b22cc184 / Any [Sessions]

3. Select the desired link.

Edit a playbook associated with an alert

A playbook associated with an alert can be modified. A change you make on the playbook only affects the playbook related to that specific alert.

About this task

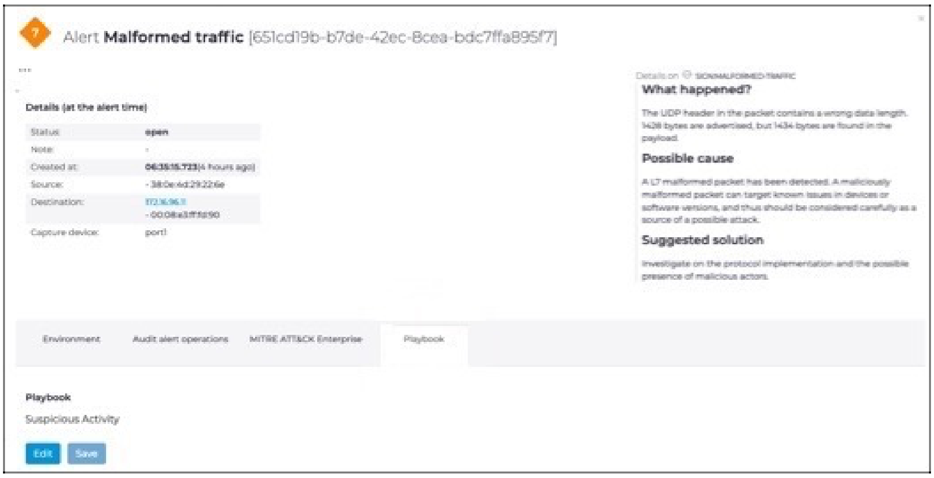
You can edit a playbook associated with an alert from the **Playbook** tab in the **Alerts** page.

Procedure

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

   Result: The **Alerts** page opens.

2. Find the alert on which to edit the assigned playbook.
3. Select the alert, then select **Playbook** at the bottom of the screen.
4. To edit the playbook, select **Edit**.



Alert **Malformed traffic** [651cd19b-b7de-42ec-8cea-bdc7ffa895f7]

Details (at the alert time)

Status:	open
Note:	-
Created at:	06:35:15.723 (4 hours ago)
Source:	- 38:0e:4d:29:22:6e
Destination:	172.16.96.1 - 00:08:a3:ff:fd:90
Capture device:	port1

Details on SIGN:MALFORMED-TRAFFIC

What happened?

The UDP header in the packet contains a wrong data length. 1428 bytes are advertised, but 1434 bytes are found in the payload.

Possible cause

A L7 malformed packet has been detected. A maliciously malformed packet can target known issues in devices or software versions, and thus should be considered carefully as a source of a possible attack.

Suggested solution

Investigate on the protocol implementation and the possible presence of malicious actors.

Playbook

Suspicious Activity

Figure 12. Playbook tab

5. Edit the playbook as necessary.
6. Select **Save**.

> **Note:**
> The playbook template from which the alert playbook was generated remains unchanged, as do all other alert playbooks generated from the same playbook template.

Chapter 4. Assets

Assets

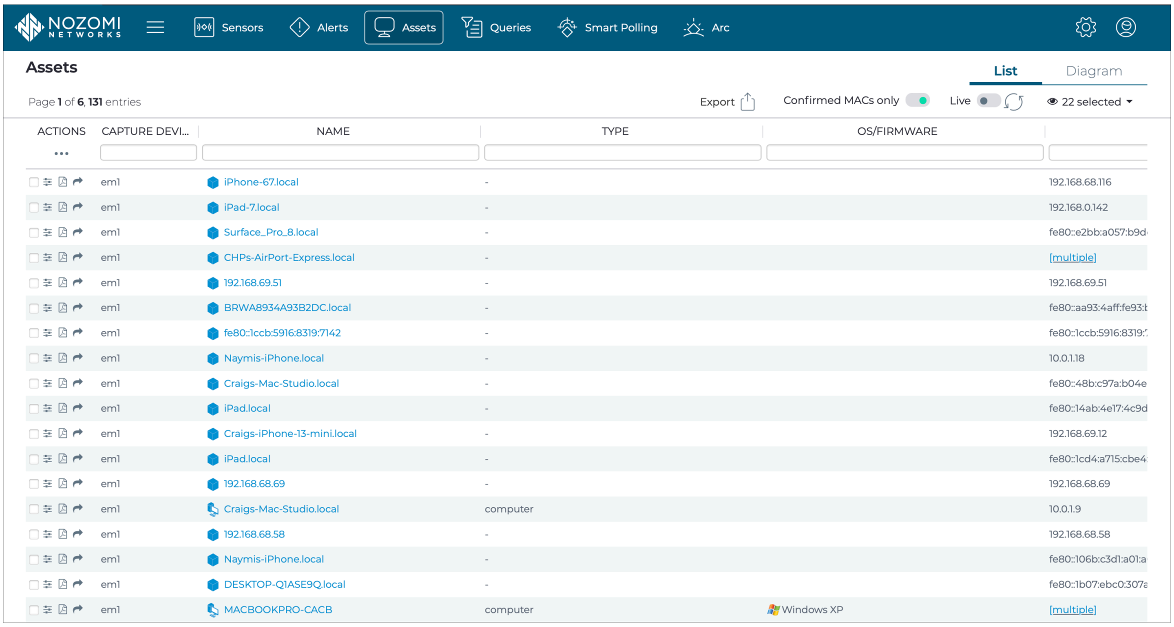
*The **Assets** page shows all the physical components and systems in the local network environment and their associated details. It also lets you perform actions on those assets. Depending on the nodes and components involved, assets can range from a simple personal computer to an operational technology (OT) device.*

The top right section of the **Assets** page has these two tabs:

- List (on page 49)
- Diagram (on page 51)

List

*The **List** page shows all the assets in table format.*



Assets

Page 1 of 6, 131 entries

ACTIONS	CAPTURE DEVI...	NAME	TYPE	OS/FIRMWARE	
☐	em1	iPhone-67.local	-		192.168.68.116
☐	em1	iPad-7.local	-		192.168.0.142
☐	em1	Surface_Pro_8.local	-		fe80::e2bb:a057:b9d
☐	em1	CHPs-AirPort-Express.local	-		[multiple]
☐	em1	192.168.69.51	-		192.168.69.51
☐	em1	BRWA8934A93B2DC.local	-		fe80::aa93:4aff:fe93:
☐	em1	fe80::1ccb:5916:8319:7142	-		fe80::1ccb:5916:8319:
☐	em1	Naymis-iPhone.local	-		10.0.1.18
☐	em1	Craigs-Mac-Studio.local	-		fe80::48b:c97a:b04e
☐	em1	iPad.local	-		fe80::14ab:4e17:4c9d
☐	em1	Craigs-iPhone-13-mini.local	-		192.168.69.12
☐	em1	iPad.local	-		fe80::1cd4:a715:cbe4
☐	em1	192.168.68.69	-		192.168.68.69
☐	em1	Craigs-Mac-Studio.local	computer		10.0.1.9
☐	em1	192.168.68.58	-		192.168.68.58
☐	em1	Naymis-iPhone.local	-		fe80::106b:c3d1:a01:a
☐	em1	DESKTOP-Q1ASE9Q.local	-		fe80::1b07:ebc0:307a
☐	em1	MACBOOKPRO-CACB	computer	Windows XP	[multiple]

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Confirmed MACs only

The **Confirmed MACs only** toggle lets you select only assets that have a confirmed *media access control (MAC)* address.

Live

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

Refresh

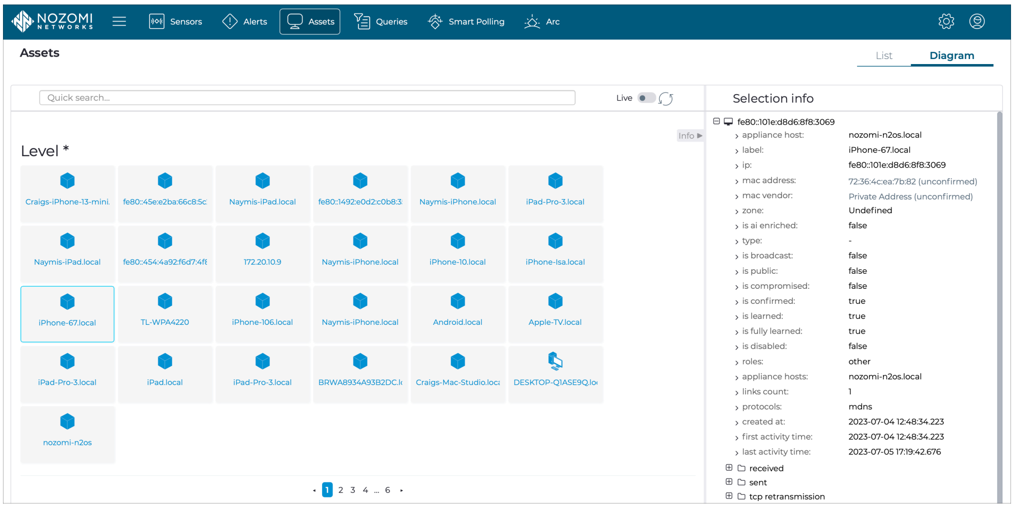
The **Refresh** icon lets you immediately refresh the current view.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Diagram

*The **Diagram** page uses the Purdue model format to display the assets. Assets are shown in separate rows, according to their level.*



Level *

Craigs-iPhone-13-mini.	fe80::45e:e2ba:66c8:5c	Naymis-iPad.local	fe80::1492:e0d2:c0b8:3	Naymis-iPhone.local	iPad-Pro-3.local
Naymis-iPad.local	fe80::454:4a92:f6d7:4f	172.20.10.9	Naymis-iPhone.local	iPhone-10.local	iPhone-Isa.local
iPhone-67.local	TL-WPA4220	iPhone-106.local	Naymis-iPhone.local	Android.local	Apple-TV.local
iPad-Pro-3.local	iPad.local	iPad-Pro-3.local	BRWA8934A93B2DC.l	Craigs-Mac-Studio.loc	DESKTOP-Q1ASE9Q.lo
nozomi-n2os					

Selection info

⊟ fe80::101e:d8d6:8f8:3069

› appliance host:	nozomi-n2os.local
› label:	iPhone-67.local
› ip:	fe80::101e:d8d6:8f8:3069
› mac address:	72:36:4c:ea:7b:82 (unconfirmed)
› mac vendor:	Private Address (unconfirmed)
› zone:	Undefined
› is ai enriched:	false
› type:	-
› is broadcast:	false
› is public:	false
› is compromised:	false
› is confirmed:	true
› is learned:	true
› is fully learned:	true
› is disabled:	false
› roles:	other
› appliance hosts:	nozomi-n2os.local
› links count:	1
› protocols:	mdns
› created at:	2023-07-04 12:48:34.223
› first activity time:	2023-07-04 12:48:34.223
› last activity time:	2023-07-05 17:19:42.676

⊞ received

⊞ sent

⊞ tcp retransmission

Figure 13. Diagram page

Search bar

The search bar lets you search for a specific item.

Live

The live ○ toggle lets you immediately refresh the graph.

Refresh

The refresh ↻ icon lets you immediately refresh the graph.

Levels section

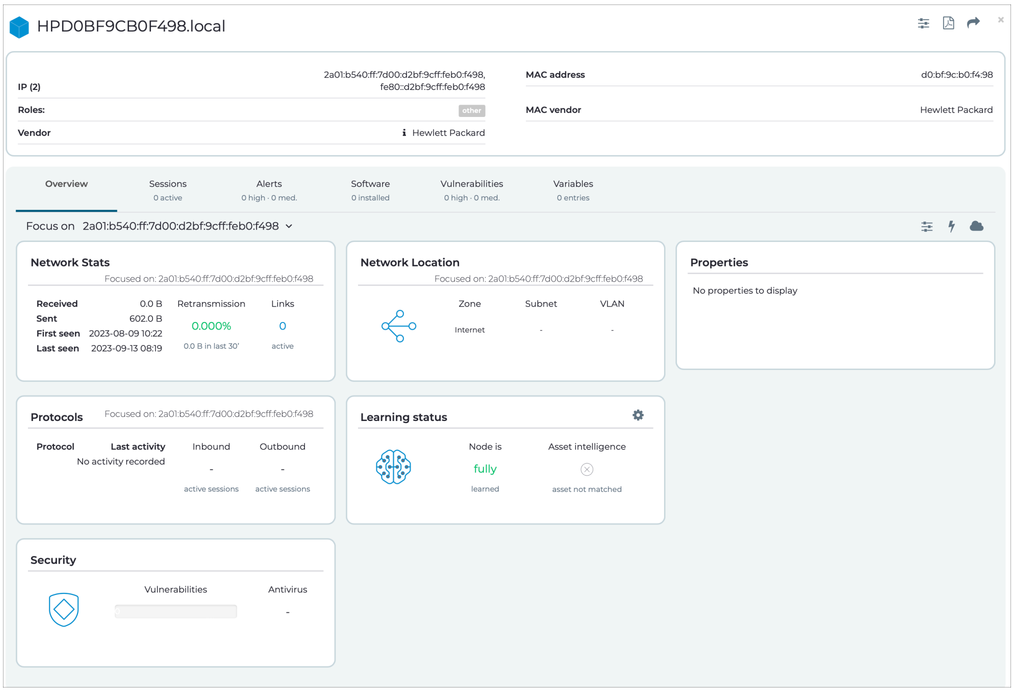
The levels section shows an icon for each asset, and shows on which level of the Purdue model it is.

Selection info

When you select the link below an asset's icon, the **Selection info** pane shows more details for the selected asset.

Details window

The details window lets you view more detailed information for an assets.



HPD0BF9CB0F498.local

IP (2)	2a01:b540:ff:7d00:d2bf:9cff:feb0:f498, fe80::d2bf:9cff:feb0:f498	MAC address	d0:bf:9c:b0:f4:98
Roles:	other	MAC vendor	Hewlett Packard
Vendor	ℹ Hewlett Packard		

Focus on 2a01:b540:ff:7d00:d2bf:9cff:feb0:f498

Network Stats

Focused on: 2a01:b540:ff:7d00:d2bf:9cff:feb0:f498

		Retransmission	Links
Received	0.0 B	0.000%	0
Sent	602.0 B		
First seen	2023-08-09 10:22	0.0 B in last 30'	active
Last seen	2023-09-13 08:19		

Network Location

Focused on: 2a01:b540:ff:7d00:d2bf:9cff:feb0:f498

Zone	Subnet	VLAN
Internet	-	-

Properties

No properties to display

Protocols Focused on: 2a01:b540:ff:7d00:d2bf:9cff:feb0:f498

Protocol	Last activity	Inbound	Outbound
	No activity recorded	-	-
		active sessions	active sessions

Learning status

Node is	Asset intelligence
fully	⊗
learned	asset not matched

Security

Vulnerabilities	Antivirus
	-

Figure 14. Asset details window

This details window shows more details for an asset.

The top section of the screen contains generic data. You can hover your mouse over the information ℹ icon to display the source, granularity and confidence of the corresponding piece of data. Data includes:

- *internet protocol (IP)* (address)
- Roles
- Vendor
- *MAC* address
- *MAC* vendor

The details window has these tabs:

- Overview (on page 58)
- Sessions (on page 59)
- Alerts (on page 60)
- Software (on page 61)
- Vulnerabilities (on page 64)
- Variables (on page 65)

Information icon

When you hover over the i icon, you can see information for:

- Source
- Granularity
- Confidence

Source

Information source	Description
manual	Information that is manually added from the configuration
imported data	Imported information
passive detection	Information from deep packet inspection
asset-kb	Information from Asset Intelligence
smart-polling	Information from Smart Polling

Granularity

Level of detailed information	Description
manual-or-import	Information manually added or imported
complete	Detailed information that has been extracted
partial	Detailed, but not complete information
generic	A family/generic value is found, but it is not detailed
unknown	Unknown

Confidence

Level of confidence in information	Description
manual-or-import	Information manually added or imported, with the highest level of confidence at this level
high	High level of confidence
good	Good level of confidence
low	Low level of confidence
unknown	Unknown confidence

Configure an asset

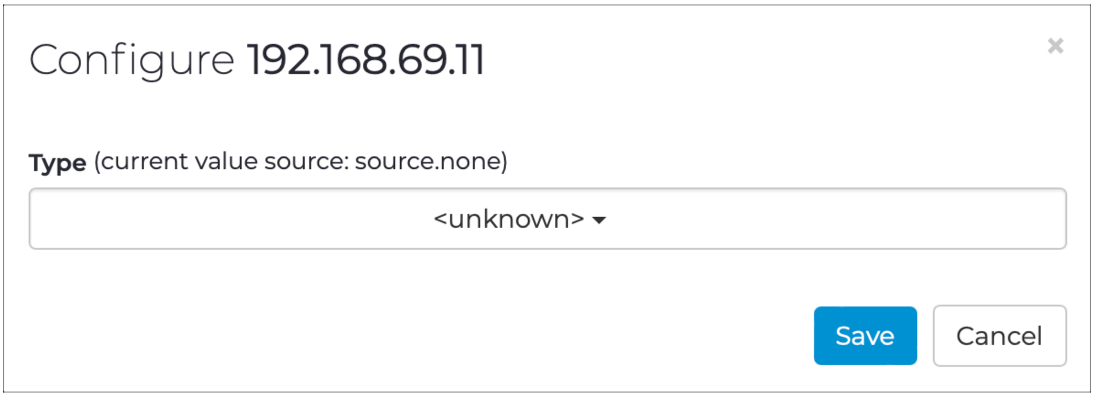
*The **Lists** page lets you configure assets.*

Procedure

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

   Result: The **Assets** page opens.

2. In the Actions column, to the left of the applicable asset, select the ☰ icon.



Configure **192.168.69.11**

Type (current value source: source.none)

<unknown> ▾

3. From the dropdown, select the applicable type.
4. Select **Save**.

Results

The asset has been configured.

Generate a PDF report of an asset

*The **Lists** page lets you generate a report in portable document format (PDF).*

Procedure

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

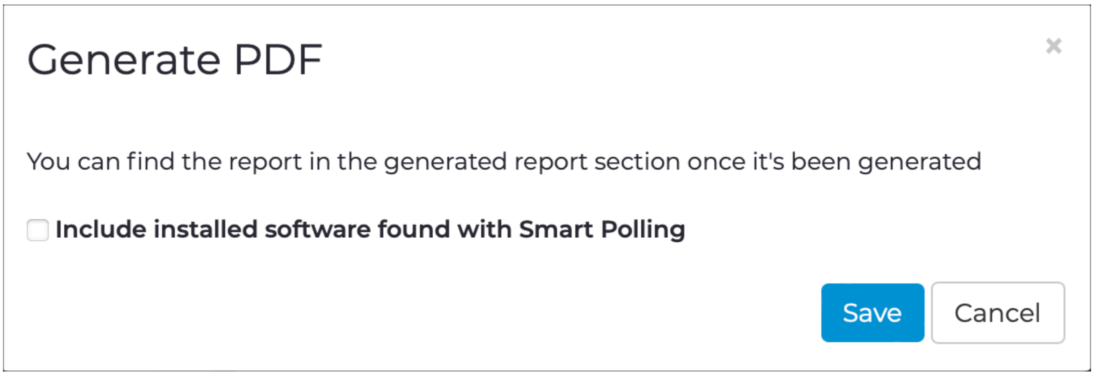
   Result: The **Assets** page opens.

2. In the Actions column, to the left of the applicable asset, select the 📄 icon.

   Result: A dialog shows.

3. **Optional:**

   If necessary, select the **Include installed software found with Smart Polling** checkbox.

   Generate PDF

   You can find the report in the generated report section once it's been generated

   □ **Include installed software found with Smart Polling**

4. Select **Save**.

   Result: The *portable document format (PDF)* file generates in the background.

   When it is ready, you can view it on the **Reports** page.

5. To view the report, go to **Reports > Generated**.

Navigate from an asset

*The **Lists** page lets you use hyperlinks to navigate to entities that are related to an asset.*

Procedure

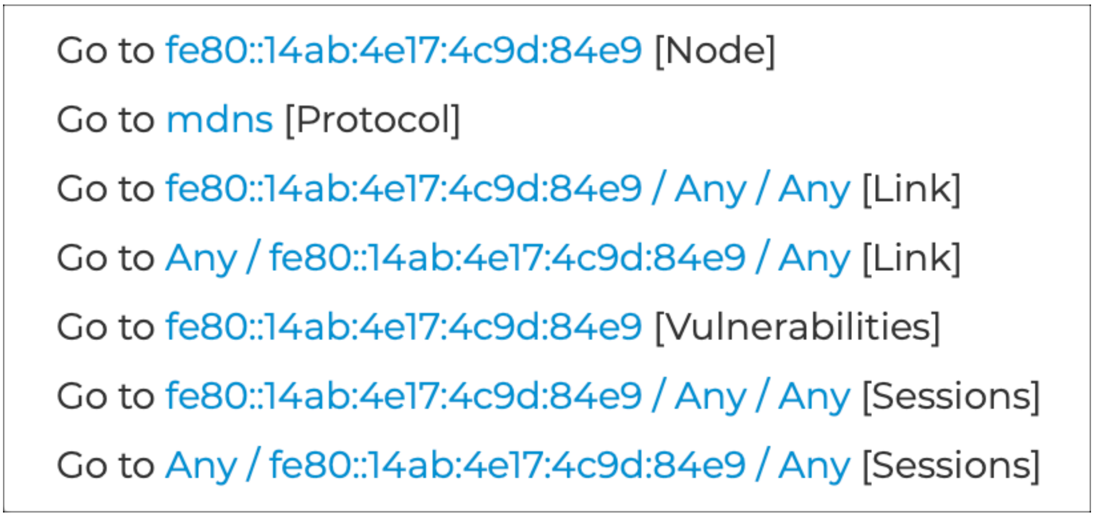
1. In the top navigation bar, select **Assets**.

   Result: The **Assets** page opens.

2. In the Actions column, to the left of the applicable asset, select the ➦ icon.

   Result: A list of related entities shows.

3. Select the hyperlink that you want to navigate to.



Go to fe80::14ab:4e17:4c9d:84e9 [Node]

Go to mdns [Protocol]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Link]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Link]

Go to fe80::14ab:4e17:4c9d:84e9 [Vulnerabilities]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Sessions]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Sessions]

Results

The entity shows in the applicable page.

View more details for an asset

*Both the **Lists** and **Diagrams** pages lets you view more details for a specific asset.*

Procedure

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

   Result: The **Assets** page opens.

2. In the top right section, select either **List** or **Diagram**
3. Choose a method to view more details for an asset:

   Choose from:

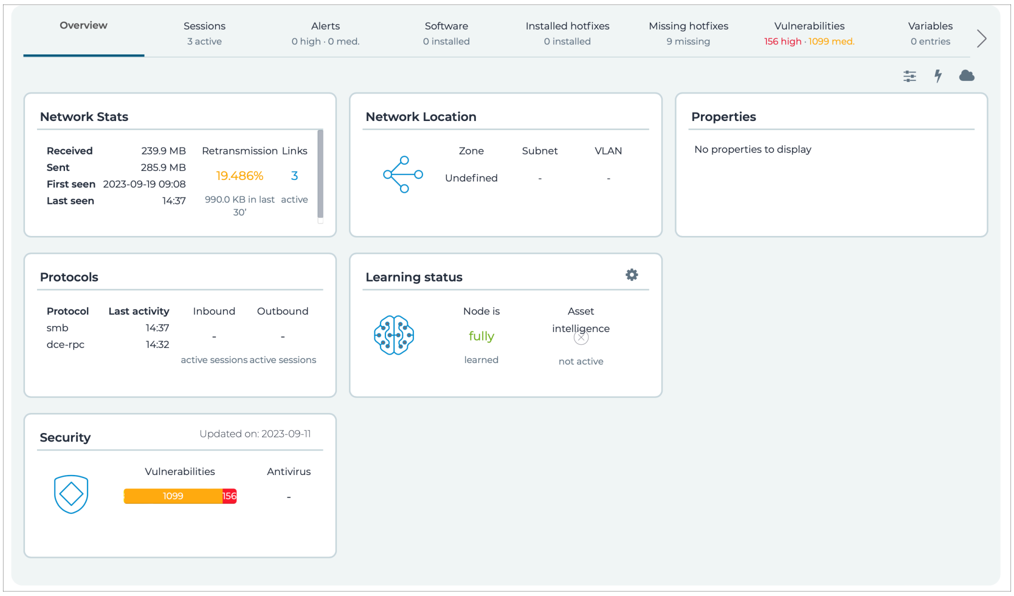
   - If you chose the **List** page, in the **NAME** column for the applicable asset, select the hyperlink
   - If you chose the **Diagram** page, below the applicable asset, select the hyperlink

Results

The Details window (on page 52) for the asset shows.

Overview

*The **Overview** page shows a general overview of information for items such as network statistics and location, protocols, and learning status for the related assets.*



Network Stats

		Retransmission	Links
Received	239.9 MB	19.486%	3
Sent	285.9 MB	990.0 KB in last 30'	active
First seen	2023-09-19 09:08		
Last seen	14:37		

Network Location

Zone	Subnet	VLAN
Undefined	-	-

Properties

No properties to display

Protocols

Protocol	Last activity	Inbound	Outbound
smb	14:37	-	-
dce-rpc	14:32	active sessions	active sessions

Learning status

Node is	Asset intelligence
fully	
learned	not active

Security Updated on: 2023-09-11

Vulnerabilities	Antivirus
1099 156	-

Figure 15. Overview tab

Network Stats

This shows useful statistics for the network activity for the related device.

Network Location

This shows information for the location for the related device on the network.

Properties

This shows additional information for the related device.

Protocols

This shows information for the different protocols that the related device uses.

Learning status

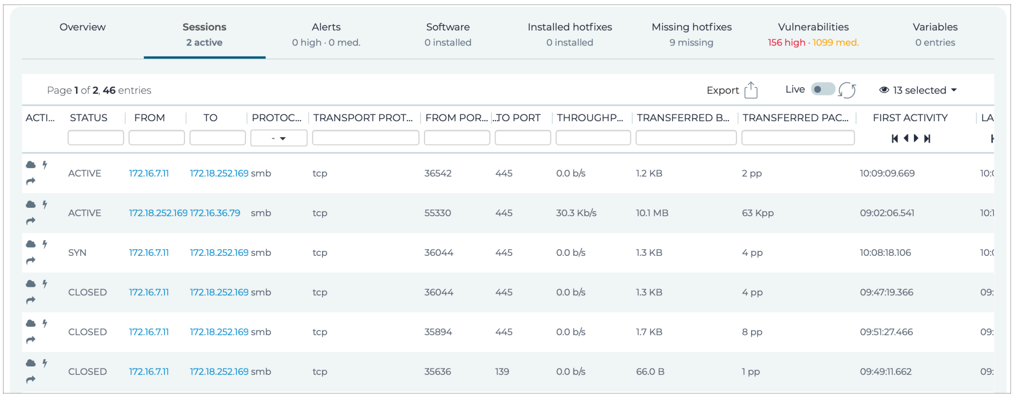
This shows the learning status of the related asset.

Security

This shows the security status of the related asset.

Sessions

*The **Sessions** page shows detailed information for communication sessions between devices.*



Page **1** of **2**, **46** entries

ACTI...	STATUS	FROM	TO	PROTOC...	TRANSPORT PROT...	FROM POR...	...TO PORT	THROUGHP...	TRANSFERRED B...	TRANSFERRED PAC...	FIRST ACTIVITY	LA
	ACTIVE	172.16.7.11	172.18.252.169	smb	tcp	36542	445	0.0 b/s	1.2 KB	2 pp	10:09:09.669	10:(
	ACTIVE	172.18.252.169	172.16.36.79	smb	tcp	55330	445	30.3 Kb/s	10.1 MB	63 Kpp	09:02:06.541	10:1
	SYN	172.16.7.11	172.18.252.169	smb	tcp	36044	445	0.0 b/s	1.3 KB	4 pp	10:08:18.106	10:(
	CLOSED	172.16.7.11	172.18.252.169	smb	tcp	36044	445	0.0 b/s	1.3 KB	4 pp	09:47:19.366	09:
	CLOSED	172.16.7.11	172.18.252.169	smb	tcp	35894	445	0.0 b/s	1.7 KB	8 pp	09:51:27.466	09:
	CLOSED	172.16.7.11	172.18.252.169	smb	tcp	35636	139	0.0 b/s	66.0 B	1 pp	09:49:11.662	09:

Figure 16. Sessions tab

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

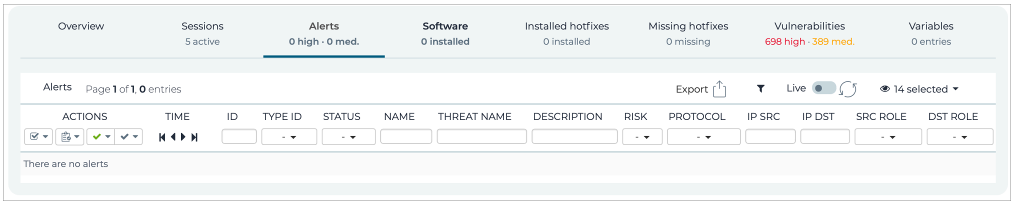
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Alerts

*The **Alerts** page shows detailed information for all the alerts that have been raised for the related assets.*



Alerts Page **1** of **1**, **0** entries

ACTIONS	TIME	ID	TYPE ID	STATUS	NAME	THREAT NAME	DESCRIPTION	RISK	PROTOCOL	IP SRC	IP DST	SRC ROLE	DST ROLE
			-	-				-	-			-	-

There are no alerts

Figure 17. Alerts tab

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

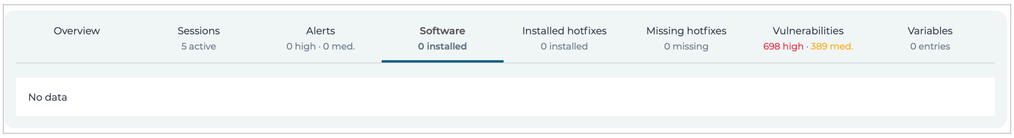
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Software

*The **Software** page shows a list of software applications that are installed on the related assets.*

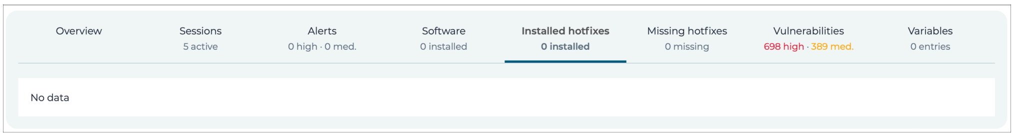


No data

Figure 18. Software tab

Installed hotfixes

*The **Installed hotfixes** page shows a list of hotfixes that are installed on the related assets.*

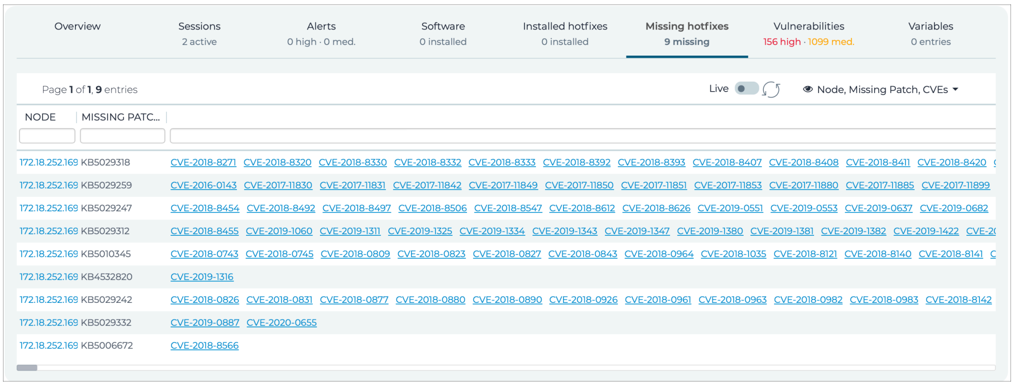


No data

Figure 19. Installed hotfixes tab

Missing hotfixes

*The **Missing hotfixes** page shows a list of hotfixes that could be installed on the related assets to resolve the related vulnerabilities.*



Page **1** of **1**, **9** entries

NODE	MISSING PATC...	
172.18.252.169	KB5029318	CVE-2018-8271 CVE-2018-8320 CVE-2018-8330 CVE-2018-8332 CVE-2018-8333 CVE-2018-8392 CVE-2018-8393 CVE-2018-8407 CVE-2018-8408 CVE-2018-8411 CVE-2018-8420
172.18.252.169	KB5029259	CVE-2016-0143 CVE-2017-11830 CVE-2017-11831 CVE-2017-11842 CVE-2017-11849 CVE-2017-11850 CVE-2017-11851 CVE-2017-11853 CVE-2017-11880 CVE-2017-11885 CVE-2017-11899
172.18.252.169	KB5029247	CVE-2018-8454 CVE-2018-8492 CVE-2018-8497 CVE-2018-8506 CVE-2018-8547 CVE-2018-8612 CVE-2018-8626 CVE-2019-0551 CVE-2019-0553 CVE-2019-0637 CVE-2019-0682
172.18.252.169	KB5029312	CVE-2018-8455 CVE-2019-1060 CVE-2019-1311 CVE-2019-1325 CVE-2019-1334 CVE-2019-1343 CVE-2019-1347 CVE-2019-1380 CVE-2019-1381 CVE-2019-1382 CVE-2019-1422 CVE-2
172.18.252.169	KB5010345	CVE-2018-0743 CVE-2018-0745 CVE-2018-0809 CVE-2018-0823 CVE-2018-0827 CVE-2018-0843 CVE-2018-0964 CVE-2018-1035 CVE-2018-8121 CVE-2018-8140 CVE-2018-8141 C
172.18.252.169	KB4532820	CVE-2019-1316
172.18.252.169	KB5029242	CVE-2018-0826 CVE-2018-0831 CVE-2018-0877 CVE-2018-0880 CVE-2018-0890 CVE-2018-0926 CVE-2018-0961 CVE-2018-0963 CVE-2018-0982 CVE-2018-0983 CVE-2018-8142
172.18.252.169	KB5029332	CVE-2019-0887 CVE-2020-0655
172.18.252.169	KB5006672	CVE-2018-8566

Figure 20. Missing hotfixes tab

Live / refresh

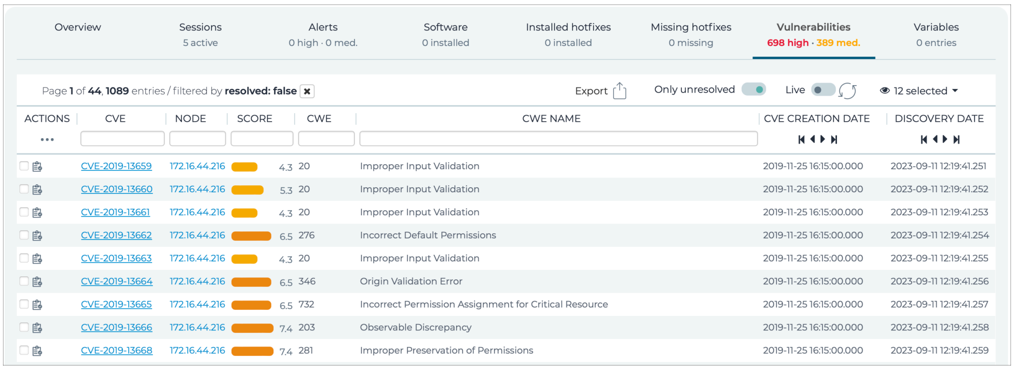
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Vulnerabilities

*The **Vulnerabilities** page shows a list of vulnerabilities that are present on the related asset.*



Page **1** of **44**, **1089** entries / filtered by **resolved: false** ✖

ACTIONS	CVE	NODE	SCORE	CWE	CWE NAME	CVE CREATION DATE	DISCOVERY DATE
□	CVE-2019-13659	172.16.44.216	4.3	20	Improper Input Validation	2019-11-25 16:15:00.000	2023-09-11 12:19:41.251
□	CVE-2019-13660	172.16.44.216	5.3	20	Improper Input Validation	2019-11-25 16:15:00.000	2023-09-11 12:19:41.252
□	CVE-2019-13661	172.16.44.216	4.3	20	Improper Input Validation	2019-11-25 16:15:00.000	2023-09-11 12:19:41.253
□	CVE-2019-13662	172.16.44.216	6.5	276	Incorrect Default Permissions	2019-11-25 16:15:00.000	2023-09-11 12:19:41.254
□	CVE-2019-13663	172.16.44.216	4.3	20	Improper Input Validation	2019-11-25 16:15:00.000	2023-09-11 12:19:41.255
□	CVE-2019-13664	172.16.44.216	6.5	346	Origin Validation Error	2019-11-25 16:15:00.000	2023-09-11 12:19:41.256
□	CVE-2019-13665	172.16.44.216	6.5	732	Incorrect Permission Assignment for Critical Resource	2019-11-25 16:15:00.000	2023-09-11 12:19:41.257
□	CVE-2019-13666	172.16.44.216	7.4	203	Observable Discrepancy	2019-11-25 16:15:00.000	2023-09-11 12:19:41.258
□	CVE-2019-13668	172.16.44.216	7.4	281	Improper Preservation of Permissions	2019-11-25 16:15:00.000	2023-09-11 12:19:41.259

Figure 21. Vulnerabilities tab

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Only unresolved

The **Only unresolved** toggle lets you filter the column to only show unresolved vulnerabilities.

Live / refresh

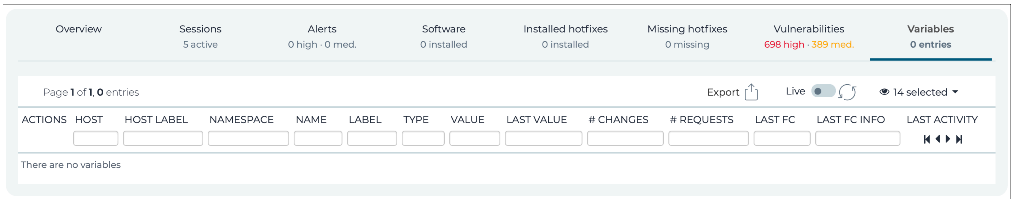
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Variables

*The **Variables** page shows detailed information for the variables hosted by the related asset.*



Page **1** of **1**, **0** entries

ACTIONS	HOST	HOST LABEL	NAMESPACE	NAME	LABEL	TYPE	VALUE	LAST VALUE	# CHANGES	# REQUESTS	LAST FC	LAST FC INFO	LAST ACTIVITY

There are no variables

Figure 22. Variables tab

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Chapter 5. Queries

Queries

You can use the Nozomi Networks Query Language (N2QL) syntax to create complex data processes to obtain, filter, and analyze lists of information from the Nozomi Networks software.

In *Nozomi Networks Query Language (N2QL)*, queries consist of:

- Data sources (on page 71)
- Commands (on page 76)
- Functions (on page 84)

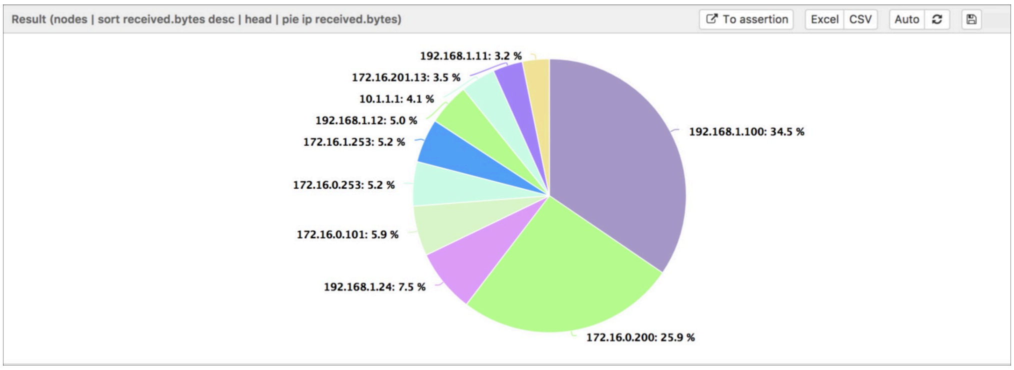
Data sources

Queries start by calling a data source. For example:

```
nodes | sort received.bytes desc | head
```

This query will show, in table format, the first 10 nodes that received the most bytes. If you add the `pie` command at the end of the query, the results will show in a pie chart format, where each slice has `node id` as the label and the `received.bytes` field as data.
For example:

```
nodes | sort received.bytes desc | head | pie ip received.bytes
```



Result (nodes | sort received.bytes desc | head | pie ip received.bytes)

Figure 23. Queries example

Functions

You might not achieved your desired result just using queries. Consequently, query syntax supports functions. With functions, you can apply calculations to the fields and use the results as a new temporary field. For example, the query:

```
nodes | sort sum(sent.bytes,received.bytes) desc | column ip
 sum(sent.bytes,received.bytes)
```

uses the `sum` function to `sort` on the aggregated parameters, which produces a chart with the columns representing the sum of the `sent` and `received` bytes.

Prefix

The `$` is a prefix that changes the interpretation of the right hand side (rhs) of a `where` clause. By default, the rhs is interpreted as a string. With the `$` prefix, the interpretation of the rhs changes to a field name.

For example, in a query such as:

```
nodes | where id == 17.179.252.2
```

the right side of the `==` is expected to be a constant. If you create a query such as:

```
nodes | where id == id
```

the query tries to match all of the nodes having `id` equal to the string `id`.
If, however, you use the `$`, the second field is interpreted as a field, not a constant:

```
nodes | where id == $id
```

and returns the full list of records.

Data sources

These are the available data sources with which you can start a query.

alerts	Raised events
appliances	Downstream connected sensors synchronizing data to this, local one
assertions	Assertions saved by the users. An assertion represents an automatic check against other query sources
assets	Identified assets. Assets represent a local (private), physical system to care about, and can be composed of one or more Nodes. Broadcast nodes, grouped nodes, internet nodes, and similar cannot be Assets accordingly
audit_log	System's log for important operational events, e.g., login, backup creation, etc.
captured_files	Files reconstructed for analysis
captured_logs	Logs captured passively over the network
captured_urls	URLs and other protocol calls captured over the network. Access to files, requests to DNS, requested URLs and other are available in this query source
cpe_items	CPE maps definitions
cve_files	CVE definitions
dhcp_leases	IP to Mac bindings due to the presence of DHCP
function_codes	Protocols' function codes used in the environment
health_log	System's Health-related events, e.g. high resource utilization or hardware-related issues or events
link_events	Events that can occur on a Link, like it being available or not
links	Identified links, defined as directional one-to-one associations with a single protocol (i.e. source, destination, protocol)
microsoft_hotfixes	Microsoft hotfix information

node_cpe_changes	Common Platform Enumeration changes identified over known nodes. On the event of update of a CPE (on hardware, operating system and software versions), an entry in this query source is created to keep track of software updates or better detection of software
node_cpes	Common Platform Enumeration identified on nodes (hardware, operating system and software versions)
node_cves	Common Vulnerability Exposures: vulnerabilities associated to identified nodes' CPEs
node_points	Data points extracted over time, via Smart Polling or via Arc, from monitored Nodes
node_points_last	node_points last samples per each included data point
nodes	Identified nodes, where a node is an L2 or L3 (and above) entity able to speak some protocol
packet_rules	Packet rules definitions
protocol_connections	Identified protocol handhsakes/connections needed to decode process variables
report_files	Generated report files available for consultation
report_folders	Generated report folders
sessions	Sessions with recent network actvity. A Session is a specific application-level connection between nodes. A Link can hold one or more Session at a given time
sessions_history	Archived sessions
sigma_rules	Sigma rules definitions
sp_executions	Executions of Smart Polling plans
sp_node_executions	Results of Smart Polling plans executions per node
stix_indicators	STIX definitions
subnets	Identified network subnets
threat_models	Threat Modeling definitions
trace_requests	Trace requests in processing

variable_history	Process variables' history of values
variables	Identified process variables
yara_rules	Yara rules definitions
zone_links	A list of protocols exchanged by the defined zones
zones	Defined network zones

Basic operators

Operator	| (pipe, AND logical operator)
Description	Add a where clause with a logical AND, append it using the pipe character (`|`). For example, the query below returns links that are from 192.168.254.0/24 `AND` going to 172.217.168.0/24.
Example	**links | where from in_subnet? 192.168.254.0/24 | where to in_subnet? 172.217.168.0/24**

Operator	`OR`
Description	To add a where clause with a logical OR, append it using the OR operator. For example, the query below returns links with either the http `OR` the https protocols.
Example	**links | where protocol == http OR protocol == https**

Operator	`!` (exclamation point, NOT logical operator)
Description	Put an exclamation point (`!`) before a term to negate it. For example, the query below returns links that do NOT (`!`) belong to 192.168.254.0/24.
Example	**nodes | where ip !in_subnet? 192.168.254.0/24 | count**

Operator	`->`
Description	To change a column name, select it and use the `->` operator followed by the new name. It is worth noting that specific suffixes are parsed and used to visualize the column content differently. For example: • `_time` data is shown in a timestamp format (1647590986549 becomes 2022-03-18 09:09:46.549) • `_bytes` adds KB or MB, as applicable (50 becomes 50.0 B) • `_percent` adds a percentage sign (50 becomes 50%) • `_speed` adds a throughput speed in Mb/s (189915 becomes 1.8 Mb/s) • `_date` converts numbers into a date format (2022-06-22 15:43:31.297 becomes 2022-06-2214:24:09.280 becomes 2022-06-24 (current day)) • `_packets` adds pp after the number of packets (50 becomes 50 pp)
Example 1	`nodes | select created_at created_at->my_integer | where my_integer > 946684800000`
Example 2	`nodes | select created_at->my_creation_time`

Example 3	`nodes | select tcp_retransmission.bytes->my_retrans_bytes`

Operators	==, =, <, >, <=, and >=
Description	Queries support the mathematical operators listed above.

Operator	`"` (Quotation marks)
Description	Use quotation marks (`"`) to specify an empty string. Consider these two cases where this technique is useful: • Finding non-empty values. Example 1 below returns assets where the `os` field is not blank. • Specifying that a value in the query is a string (if its type is ambiguous). Example 2 below tells concat to treat the `"--"` parameter as a fixed string to use rather than as a field from the **alerts** table.
Example 1	`assets | where os != ""`
Example 2	`alerts | select concat(id_src,"--",id_dst)`

Operator	`in?`
Description	`in?` is only used with arrays; the field `type` must be an array. The query looks for the text strings you specify using `in?` and returns arrays that match one of them. The example below uses `in?` to find any node having `computer` or `printer` as elements in the array.
Example	`assets | where type in? ["computer","printer_scanner"]`

Operator	`include?`
Description	The query looks for the text string you specify using `include?` and returns strings that match it. The example below uses `include?` to find assets where the **os** field contains the string **Win**.
Example	`assets | where os include? Win`

Commands

Syntax	`select <field1> <field2> ... <fieldN>`
Parameters	• the list of field(s) to output
Description	The select command takes all the input items and outputs them with only the selected fields

Syntax	`exclude <field1> <field2> ... <fieldN>`
Parameters	• the list of field(s) to remove from the output
Description	The exclude command takes all the input items and outputs them without the specified field(s)

Syntax	**where <field> <==|!=|<|>|<=|>=|in?|include?|start_with?|end_with?|in_subnet?> <value>**
Parameters	• field: the name of the field to which the operator will be applied • operator • value: the value used for the comparison. It can be a number, a string, or other data type. Advanced operators can use other data types, such as: ◦ a list (using JSON syntax) when using the in? operator, for example: `nodes | where ip in? ["172.18.41.44"]` ◦ another property when using the '$' symbol, for example: `nodes | where ip != $id`
Description	The where command will send to the output only the items which fulfill the specified criterion, many clauses can be concatenated using the boolean **OR** operator
Example	• `nodes | where roles include? consumer OR zone == office` • `nodes | where ip in_subnet? 192.168.1.0/24` • `<value>` can also be another `<field>`, as in: `links | where from_zone == $to_zone | select from_zone to_zone`

Syntax	`sort <field> [asc|desc]`
Parameters	• field: the field used for sorting • asc|desc: the sorting direction

Description	The sort command will sort all the items according to the field and the direction specified, it automatically understands if the field is a number or a string

Syntax	`group_by <field> [ [avg|sum] [field2] ]`
Parameters	• field: the field used for grouping • avg|sum: if specified, the relative operation will be applied on field2
Description	The group_by command will output a grouping of the items using the field value. By default the output will be the count of the occurrences of distinct values. If an operator and a **field2** are specified, the output will be the average or the sum of the **field2** values

Syntax	`head [count]`
Parameters	• count: the number of items to output
Description	The head command will take the first **count** items, if **count** is not specified the default is 10

Syntax	`uniq [<field1> <field2> ... <fieldN>]`
Parameters	• an optional list of fields on which to calculate the uniqueness
Description	The uniq command will remove from the output the duplicated items

Syntax	`expand <field>`
Parameters	• field: the field containing the list of values to be expanded
Description	The expand command will take the list of values contained in **field** and for each of them it will duplicate the original item substituting the original **field** value with the current value of the iteration

Syntax	`expand_recursive <field>`
Parameters	• field: the field to be recursively expanded

Description	The expand_recursive command will recursively parse the content of **field**, expanding each array or json structure until a scalar value is found. It generates a new row for each array element or json field. For each new row, it duplicates the original item substituting the original **field** value with the current value of the iteration and adding a new field that represents the current iteration path from the root

Syntax	`sub <field>`
Parameters	• field: the field containing the list of objects
Description	The sub command will output the items contained in **field**

Syntax	`count`
Parameters	
Description	The count command outputs the number of items

Syntax	`pie <label_field> <value_field>`
Parameters	• label_field: the field used for each slice label • value_field: the field used for the value of the slice, must be a numeric field
Description	The pie command will output a pie chart according to the specified parameters

Syntax	`column <label_field> <value_field ...>`
Parameters	• label_field: the field used for each column label • value_field: one or more field used for the values of the columns
Description	The column command will output a histogram; for each label a group of columns is displayed with the value from the specified value_field(s). The variant `column_colored_by_label` returns bars of different colors depending on their labels.

Syntax	`history <count_field> <time_field>`
Parameters	• count_field: the field used to draw the Y value • time_field: the field used to draw the X points of the time series

Description	The history command will draw a chart representing an historic series of values

Syntax	`distance <id_field> <distance_field>`
Parameters	• id_field: the field used to tag the resulting distances. • distance_field: the field on which distances are computed among entries.
Description	The distance command calculates a series of distances (that is, differences) from the original series of `distance_field`. Each distance value is calculated as the difference between a value and its subsequent occurrence, and tagged using the **id_field**. For example, assuming we're working with an **id** and a **time** field, entering **alerts | distance id time** returns a table where each distance entry is characterised by the **from_id**, **to_id**, and **time_distance** fields that represent time differences between the selected alerts.

Syntax	`bucket <field> <range>`
Parameters	• field: the field on which the buckets are calculated • range: the range of tolerance in which values are grouped
Description	The bucket command will group data in different buckets, different records will be put in the same bucket when the values fall in the same multiple of <range>

Syntax	`join <other_source> <field> <other_source_field>`
Parameters	• other_source: the name of the other data source • field: the field of the original source used to match the object to join • other_source_field: the field of the other data source used to match the object to join
Description	The join command will take two records and will join them in one record when <field> and <other_source_field> have the same value

Syntax	`gauge <field> [min] [max]`
Parameters	• field: the value to draw • min: the minimum value to put on the gauge scale • max: the maximum value to put on the gauge scale

Description	The gauge command will take a value and represent it in a graphical way

Syntax	`value <field>`
Parameters	• field: the value to draw
Description	The value command will take a value and represent it in a textual way

Syntax	`reduce <field> [sum|avg]`
Parameters	• field: the field on which the reduction will be performed • sum or avg: the reduce operation to perform, it is sum if not specified
Description	The reduce command will take a series of values and calculate a single value

Syntax	size()
Parameters	• field: the field to calculate the size of
Description	If the field is an array, then the size function returns the number of entries in the array. If the field contains a string, then the size function returns the number of characters in the string. **Note**: The size function may only be used on the following data sources: alerts, assets, captured_files, links, nodes, packet_rules, sessions, stix_indicators, subnets, variables, yara_rules, zones, and zone_links.
Example:	`assets | where size(ip) > 1`

Nodes-specific commands reference

Syntax	`where_node <field> < ==|!=|<|>|<=|>=|in?|include?|exclude?|start_with?|end_with? > <value>`
Parameters	• field: the name of the field to which the operator will be applied • operator • value: the value used for the comparison. It can be a number, a string or a list (using JSON syntax), the query engine will understand the semantics.
Description	The where_node command will send to the output only the items which fulfill the specified criterion, many clauses can be concatenated using the boolean **OR** operator. The where_node command is similar to the where command, but the output will also include all the nodes that are communicating directly with the result of the search. **Note**: This command is only applicable to the nodes table.

Syntax	`where_link <field> < ==|!=|<|>|<=|>=|in?|include?|exclude?|start_with?|end_with? > <value>`
Parameters	• field: the name of the links table's field to which the operator will be applied. • operator • value: the value used for the comparison. It can be a number, a string or a list (using JSON syntax) the query engine will understand the semantics.
Description	The where_link command will send to the output only the nodes which are connected by a link fulfilling the specified criterion. Many clauses can be concatenated using the boolean **OR** operator. **Note**: This command is only applicable to the nodes table.

Syntax	`graph [node_label:<node_field>]`
	`[node_perspective:<perspective_name>]`
	`[link_perspective:<perspective_name>]`

Parameters	• node_label: add a label to the node, the label will be the content of the specified node field • node_perspective: apply the specified node perspective to the resulting graph. Valid node perspective values are: ◦ roles ◦ zones ◦ transferred_bytes ◦ not_learned ◦ public_nodes ◦ reputation ◦ appliance_host • link_perspective: apply the specified link perspective to the resulting graph. Valid link perspectives are: ◦ transferred_bytes ◦ tcp_firewalled ◦ tcp_handshaked_connections ◦ tcp_connection_attempts ◦ tcp_retransmitted_bytes ◦ throughput ◦ interzones ◦ not_learned
Description	The graph command renders a network graph by taking some nodes as input.

Link-events-specific commands reference

Syntax	`availability`
Parameters	
Description	The availability command computes the percentage of time a link is UP. The computation is based on the link events UP and DOWN that are seen for the link.

Syntax	`availability_history <range>`
Parameters	• range: the temporal window in milliseconds to use to group the link events
Description	The availability_history command computes the percentage of time a link is UP by grouping the link events into many buckets. Each bucket will include the events of the temporal window specified by the range parameter.

Syntax	`availability_history_month <months_back> <range>`
Parameters	• months_back: number of months to go back in regards to the current month to group the link events • range: the temporal window in seconds to use to group the link events
Description	The availability_history command computes the percentage of time a link is UP by grouping the link events into many buckets. Each bucket will include the events of the temporal window specified by the range and months parameters.

Functions

Functions are always used in conjunction with other commands, such as `select`. In the following examples, functions are shown in **bold**:

- Combining functions with `select`: `nodes | select id type` **`color`**`(type)`
- Combining functions with `where`: `nodes | where` **`size`**`(label) > 10`
- Combining functions with `group_by`: `nodes | group_by` **`size`**`(protocols)`

Here is the complete list of functions:

Syntax	`abs(<field>)`
Parameters	• the field on which to calculate the absolute value
Description	The abs function returns the absolute value of the field

Syntax	`bitwise_and(<numeric_field>,<mask>)`
Parameters	• numeric_field: the numeric field on which apply the mask • mask: a number that will be interpreted as a bit mask
Description	The bitwise_and function calculates the bitwise & operator between the numeric_field and the mask entered by the user

Syntax	`coalesce(<field1>,<field2>,...)`
Parameters	• a list of fields or string literals in the format "<chars>"
Description	The coalesce function will output the first value that is not null

Syntax	`color(<field>)`
Parameters	• field: the field on which to calculate the color
Description	The color function generates a color in the rgb hex format from a value
Note	Only available for nodes, links, variables and function_codes

Syntax	`concat(<field1>,<field2>,...)`
Parameters	• a list of fields or string literals in the format "<chars>"

Description	The concat function will output the concatenation of the input fields or values

Syntax	`date(<time>)`
Parameters	• time defined as unix epoch
Description	The date function returns a date from a raw time

Syntax	`day_hour(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The day_hour function returns the hour of the day plus the sensor's local time offset from UTC, i.e. a value in the range 0 through 23. Be careful when accounting for daylight saving time. Use **day_hour_utc** when absolute precision is desired

Syntax	`day_hour_utc(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The **day_hour_utc** function returns the hour of the day expressed in UTC for the current time field, i.e. a value in the range 0 through 23

Syntax	`days_ago(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The days_ago function returns the amount of days passed between the current time and the time field value

Syntax	`dist(<field1>,<field2>)`
Parameters	• the two fields to compute the distance on
Description	The dist function returns the distance between field1 and field2, which is the absolute value of their difference

Syntax	`div(<field1>,<field2>)`

Parameters	• field1 and field2: the two field to divide
Description	The div function will calculate the division field1/field2

Syntax	`hours_ago(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The hours_ago function returns the amount of hours passed between the current time and the time field value

Syntax	`is_empty(field) == true | false`
Parameters	• field: the field to check to evaluate whether it is empty or not
Description	The is_empty command takes a field as input and returns only the entries that are either empty / not empty.
Example	**nodes | where is_empty(label) == false**

Syntax	`is_recent(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The is_recent function takes a time field and returns true if the time is not farther than 30 minutes

Syntax	`minutes_ago(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The minutes_ago function returns the amount of minutes passed between the current time and the time field value

Syntax	`mult(<field1>,<field2>,...)`
Parameters	• a list of fields to multiply
Description	The mult function returns the product of the fields passed as arguments

Syntax	`round(<field>,[precision])`

Parameters	• field: the numeric field to round • precision: the number of decimal places
Description	The round function takes a number and outputs the rounded value

Syntax	`seconds_ago(<time_field>)`
Parameters	• time_field: the field representing a time
Description	The seconds_ago function returns the amount of seconds passed between the current time and the time field value

Syntax	`split(<field>,<splitter>,<index>)`
Parameters	• field: the field to split • splitter: the character used to separate the string and produce the tokens • index: the 0 based index of the token to output
Description	The split function takes a string, separates it and outputs the token at the <index> position

Syntax	`sum(<field>,...)`
Parameters	• a list of fields to sum
Description	The sum function returns the sum of the fields passed as arguments

Examples

Pie chart

An example on how to create a pie chart to understand the media access control (MAC) vendor distribution in a network.

We choose nodes as our query source and we start to group the nodes by mac_vendor:

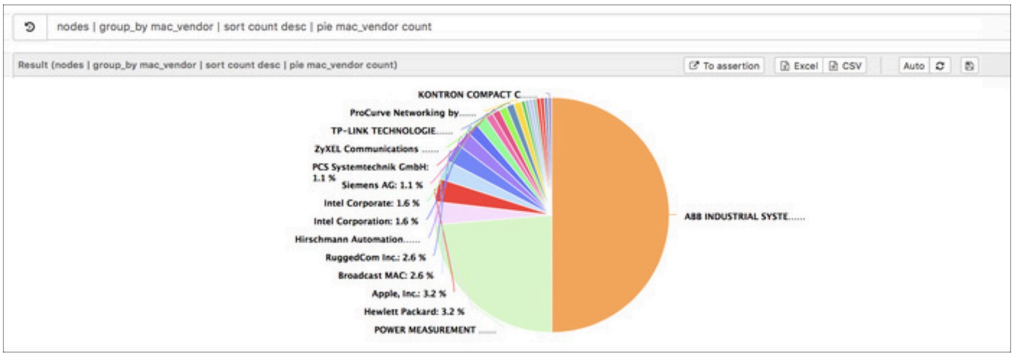
```
nodes | group_by mac_vendor
```

We can see the list of the vendors in our network associated with the occurrences count. To better understand our data we can use the sort command, so the query becomes:

```
nodes | group_by mac_vendor | sort count desc
```

In the last step we use the pie command to draw the chart with the mac_vendor as a label and the count as the value.

```
nodes | group_by mac_vendor | sort count desc | pie mac_vendor count
```



```
nodes | group_by mac_vendor | sort count desc | pie mac_vendor count
```

Result (nodes | group_by mac_vendor | sort count desc | pie mac_vendor count)

Figure 24. Pie chart example

Column chart

An example on how to create a column chart with the top nodes by traffic.

To start, you need to get the nodes and select the:

- `id`
- `sent.bytes`
- `received.bytes`
- `sent.bytes`
- `received.bytes`

To calculate the sum , you need to use the `sum` function. The query is:

```
nodes | select id sent.bytes received.bytes
 sum(sent.bytes,received.bytes)
```

When you execute this query, the sum field has a very long name. You can rename it to be more comfortable with these commands:

```
nodes | select id sent.bytes received.bytes
 sum(sent.bytes,received.bytes)->sum
```

To obtain the top nodes by traffic, you can sort and take the first 10:

```
nodes | select id sent.bytes received.bytes
 sum(sent.bytes,received.bytes)->sum | sort sum desc | head 10
```

Finally, to display the data in a graphical way, you can use the `column` command:

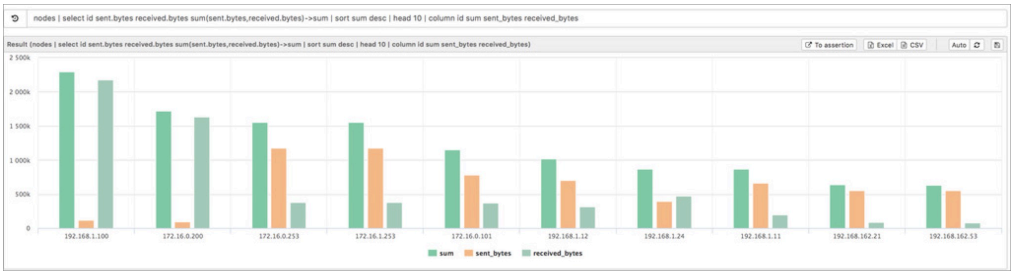
```
nodes | select id sent.bytes received.bytes
 sum(sent.bytes,received.bytes)->sum | sort sum desc | head 10 | column
 id sum sent_bytes received_bytes
```

Note:

You can access an inner field of a complex type with the dot syntax, in the example the dot syntax is used on the fields `sent` and `received` to access their bytes sub field.

Note:

After accessing a field with the dot syntax, it will gain a new name to avoid ambiguity; the dot is replaced by an underscore. In the example `sent.bytes` become `sent_bytes`



nodes | select id sent.bytes received.bytes sum(sent.bytes,received.bytes)->sum | sort sum desc | head 10 | column id sum sent_bytes received_bytes

Result (nodes | select id sent.bytes received.bytes sum(sent.bytes,received.bytes)->sum | sort sum desc | head 10 | column id sum sent_bytes received_bytes)

Figure 25. Column chart example

Where with multiple conditions in OR

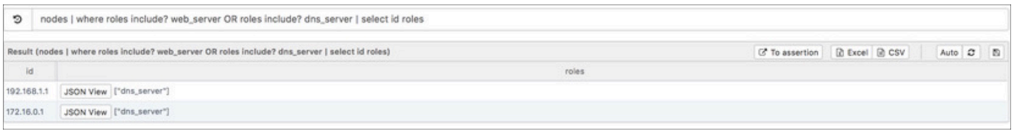
An example of a query to get all the nodes with a specific role, in particular all the nodes which are web or domain name server (DNS) servers.

With the `where` command, you can separate many conditions with `OR`

Note:

Because the roles field contains a list of values, you can use the `include?` operator to check if a value was contained in the list.

```
nodes | where roles include? web_server OR roles include? dns_server |
 select id roles
```



nodes | where roles include? web_server OR roles include? dns_server | select id roles

Result (nodes | where roles include? web_server OR roles include? dns_server | select id roles)

id	roles
192.168.1.1	JSON View ["dns_server"]
172.16.0.1	JSON View ["dns_server"]

Figure 26. Where with multiple conditions in OR example

Bucket and history

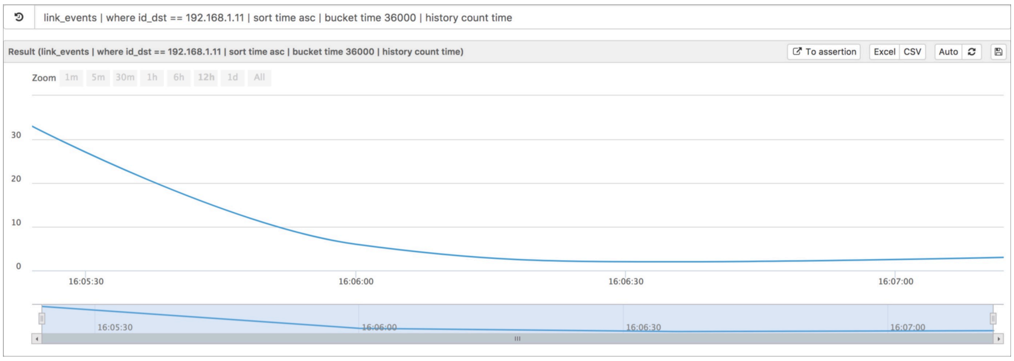
An example of a query to calculate the distribution of link events towards an internet protocol (IP) address.

You can filter all the `link_events` with `id_dst` equal to `192.168.1.11` After this you can sort by time, this is a very important step because bucket and history depend on how the data are sorted.

Then you can use `bucket` to group the data by time. The final step is to use the `history` command to draw a chart, we pass `count` as a value for the Y axis and `time` for the X axis.

The `history` command is particularly suited for displaying a big amount of data, in the image below we can see that there are many hours of data to analyze.

```
link_events | where id_dst == 192.168.1.11 | sort time asc | bucket time
 36000 | history count time
```



link_events | where id_dst == 192.168.1.11 | sort time asc | bucket time 36000 | history count time

Result (link_events | where id_dst == 192.168.1.11 | sort time asc | bucket time 36000 | history count time)

Figure 27. Bucket and history example

Join

An example query to join two data sources to obtain a new data source with more information. In particular, how to list the links with the labels for the source and destination nodes.

You can match the `from` field of the links with the `id` field of the nodes to ask for the links, and join them with the nodes:

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

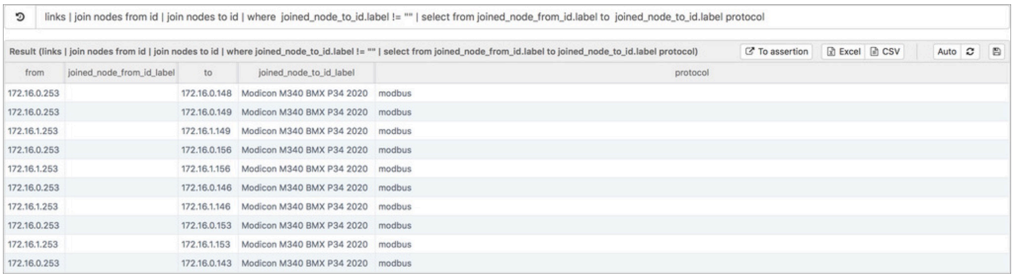
After executing the query above you will get all the links fields, plus a new field called `joined_node_from_id`, it contains the node which satisfies the `link.from == node.id` condition. You can use the dot syntax to access the sub fields of `joined_node_from_id`

Because we also want to get the labels for the `to` field of the `links` you add another `join` and exclude the empty labels of the node referred by `to` to get more interesting data:

```
links | join nodes from id | join nodes to id | where
 joined_node_to_id.label != ""
```

This will obtain a huge amount of data, which is difficult to understand. To only get the relevant information, you can use a `select`:

```
links | join nodes from id | join nodes to id | where
 joined_node_to_id.label != "" | select from joined_node_from_id.label to
 joined_node_to_id.label protocol
```



```
links | join nodes from id | join nodes to id | where  joined_node_to_id.label != "" | select from joined_node_from_id.label to  joined_node_to_id.label protocol
```

Result (links | join nodes from id | join nodes to id | where joined_node_to_id.label != "" | select from joined_node_from_id.label to joined_node_to_id.label protocol)

from	joined_node_from_id_label	to	joined_node_to_id_label	protocol
172.16.0.253		172.16.0.148	Modicon M340 BMX P34 2020	modbus
172.16.0.253		172.16.0.149	Modicon M340 BMX P34 2020	modbus
172.16.1.253		172.16.1.149	Modicon M340 BMX P34 2020	modbus
172.16.0.253		172.16.0.156	Modicon M340 BMX P34 2020	modbus
172.16.1.253		172.16.1.156	Modicon M340 BMX P34 2020	modbus
172.16.0.253		172.16.0.146	Modicon M340 BMX P34 2020	modbus
172.16.1.253		172.16.1.146	Modicon M340 BMX P34 2020	modbus
172.16.0.253		172.16.0.153	Modicon M340 BMX P34 2020	modbus
172.16.1.253		172.16.1.153	Modicon M340 BMX P34 2020	modbus
172.16.0.253		172.16.0.143	Modicon M340 BMX P34 2020	modbus

Figure 28. Join example

Compute the availability history

An example query to compute the availability history for a link.

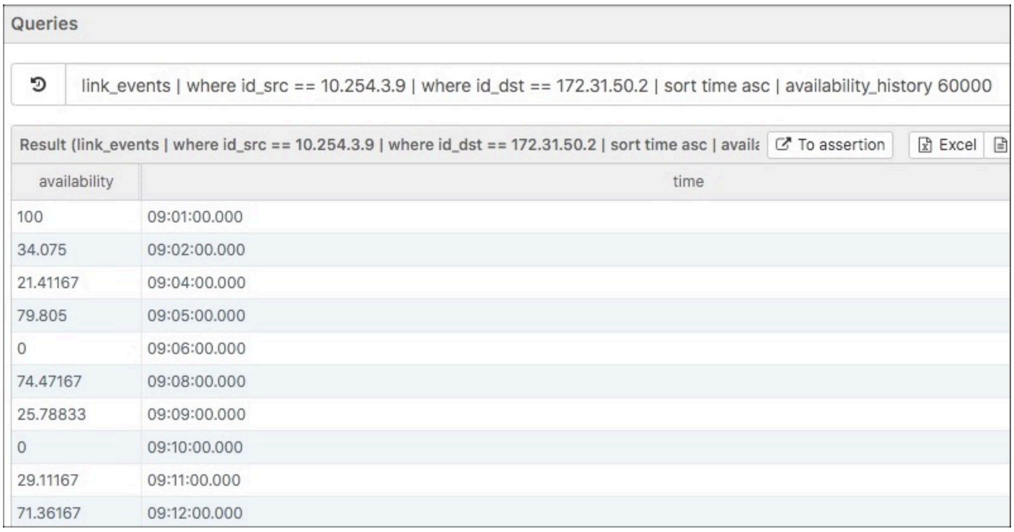
In order to achieve a reliable availability, it is recommended to enable the **Track availability** feature on the desired link.

Start from the `link_events` data source, filtered by source and destination ip in order to precisely identify the target link. Consider also filtering by protocol to achieve a higher degree of precision.

```
link_events | where id_src == 10.254.3.9 | where id_dst == 172.31.50.2
```

The next step is to sort the events by ascending time of creation. Without this step the `availability_history` might produce meaningless results, such as negative values. Then, to compute the `availability_history` with a bucket of 1 minute (60000 milliseconds), you can complete query is as follows:

```
link_events | where id_src == 10.254.3.9 | where id_dst == 172.31.50.2 |
 sort time asc | availability_history 60000
```



```
link_events | where id_src == 10.254.3.9 | where id_dst == 172.31.50.2 | sort time asc | availability_history 60000
```

Result (link_events | where id_src == 10.254.3.9 | where id_dst == 172.31.50.2 | sort time asc | availa

availability	time
100	09:01:00.000
34.075	09:02:00.000
21.41167	09:04:00.000
79.805	09:05:00.000
0	09:06:00.000
74.47167	09:08:00.000
25.78833	09:09:00.000
0	09:10:00.000
29.11167	09:11:00.000
71.36167	09:12:00.000

Figure 29. Availability history example

Note:
By default, `link_events` generation is disabled. To enable it, you can use the configuration rule described in **Configure links**.

Complex field types

Single scalar values

To query single scalar values, apply the commands that are explained in this section.

Objects

Objects show in braces: {object}

```
{
"source": "ARP",
"likelihood": 1,
"likelihood_level": "confirmed"
}
```

An example on how to query only `confirmed` *MAC* addresses.

> **Note:**
> Possible values are:
>
> - `confirmed`
> - `likely`
> - `not confirmed`

Since `mac_address:info` is an object, you can access subfields like `mac_address:info.likelihood_level` to apply the `where` condition:

```
nodes | select mac_address:info mac_address:info.likelihood_level | where
 mac_address:info.likelihood_level == confirmed
```

Since N2OS 24.1 is possible to access complex objects with a different syntax that is compatible with Vantage, using the `/` operator, the query specified above becomes:

```
nodes | select mac_address:info/likelihood_level | where
 mac_address:info.likelihood_level == "confirmed"
```

Note that also the `"confirmed"` literal can now be quoted and the query can be executed in Vantage without any change.

Arrays

> **Note:**
>
> For example, a `parent` in the alerts table.

Arrays show in braces: {array}

```
[
"5b867836-2b41-4c15-ab6f-4ae5f0251e30"
]
```

An example on how to only query alerts that have a parent incident, with a known incident id with the value: `d36d0`

Since the `parents` field is an array, you can use `expand` first to get an entry for each parent, then apply your condition:

```
alerts | expand parents | where expanded_parents include? d36d0
```

Object arrays

> **Note:**
>
> For example, `function_codes` in the links table.

Object arrays are a combination of the above examples. Therefore, they show an object included in a [{..},{..},..] :

```
[
{
"name": "M-SEARCH",
"is_learned": true,
"is_fully_learned": true
}
]
```

An example on how to query learned function codes.

Since `function_codes` is an object array, you can use `expand` first, to get an entry for each function code, then use the `.` operator (`function_code.is_learned`) to apply your `where` condition:

```
links | select from to protocol function_codes | expand function_codes |
 where expanded_function_codes.is_learned == true
```

Chapter 6. Smart Polling

Smart Polling in Guardian

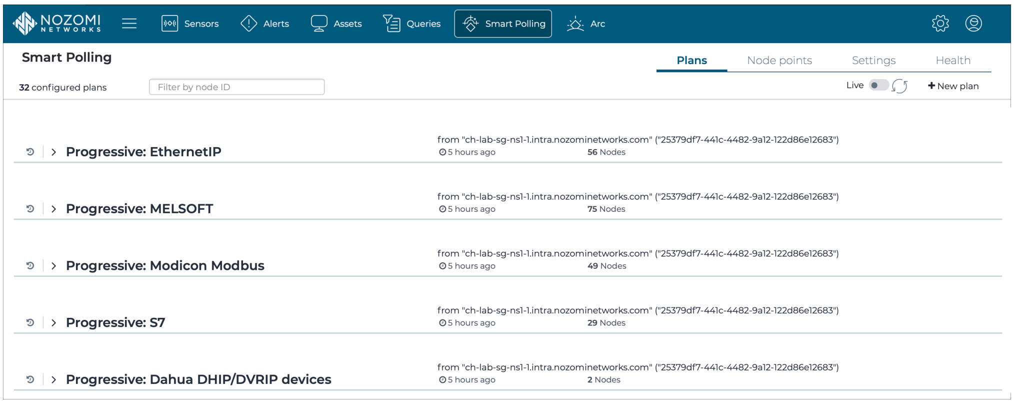
*The **Smart Polling** page lets you view and manage Smart Polling.*

Smart Polling has these tabs:

- Plans (on page 98)
- Node points (on page 99)
- Settings (on page 100)
- Health (on page 101)

Plans

*The **Plans** page shows a list of Smart Polling plans and lets you manage plans and add new ones.*



Smart Polling

32 configured plans

Filter by node ID

Progressive: EthernetIP
from "ch-lab-sg-ns1-1.intra.nozominetworks.com" ("25379df7-441c-4482-9a12-122d86e12683")
5 hours ago 56 Nodes

Progressive: MELSOFT
from "ch-lab-sg-ns1-1.intra.nozominetworks.com" ("25379df7-441c-4482-9a12-122d86e12683")
5 hours ago 75 Nodes

Progressive: Modicon Modbus
from "ch-lab-sg-ns1-1.intra.nozominetworks.com" ("25379df7-441c-4482-9a12-122d86e12683")
5 hours ago 49 Nodes

Progressive: S7
from "ch-lab-sg-ns1-1.intra.nozominetworks.com" ("25379df7-441c-4482-9a12-122d86e12683")
5 hours ago 29 Nodes

Progressive: Dahua DHIP/DVRIP devices
from "ch-lab-sg-ns1-1.intra.nozominetworks.com" ("25379df7-441c-4482-9a12-122d86e12683")
5 hours ago 2 Nodes

Figure 30. Plans page

Filter by node ID

The Filter by node ID field lets you use the node *ID* to filter the results.

Live / refresh

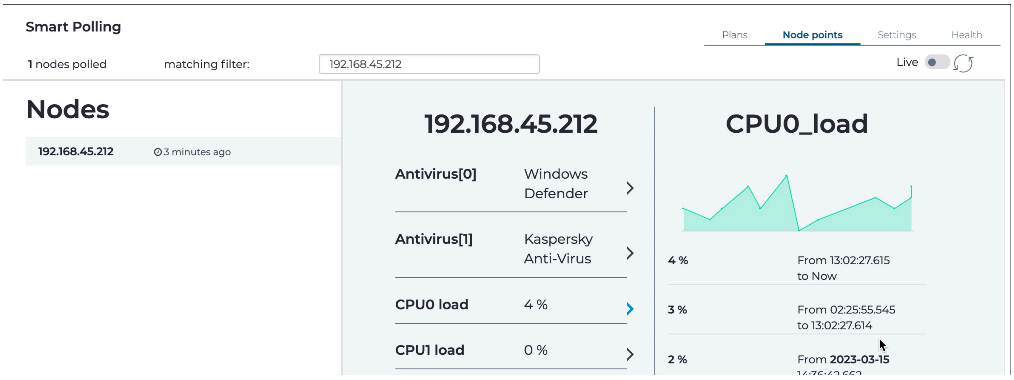
The **Live** ○ ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

New plan

The ✚ **New plan** icon lets you add a new plan.

Node points

*The **Node points** page shows all of the node points.*



1 nodes polled matching filter: 192.168.45.212

Nodes

192.168.45.212 3 minutes ago

192.168.45.212

Antivirus[0]	Windows Defender
Antivirus[1]	Kaspersky Anti-Virus
CPU0 load	4 %
CPU1 load	0 %

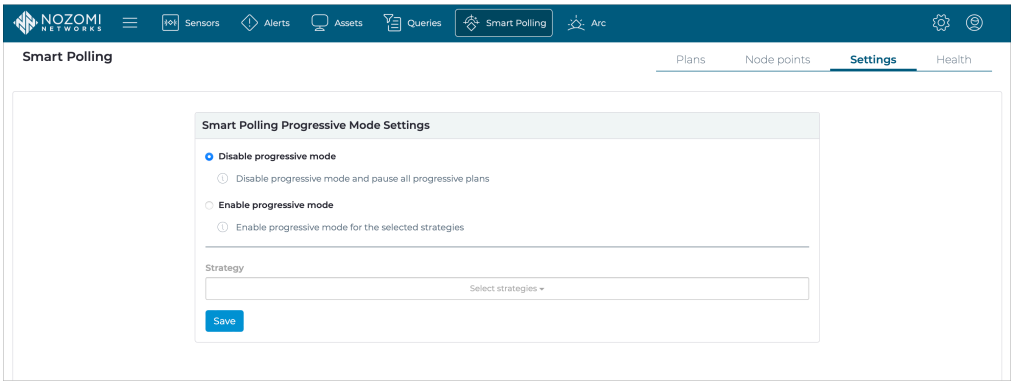
CPU0_load

4 %	From 13:02:27.615 to Now
3 %	From 02:25:55.545 to 13:02:27.614
2 %	From **2023-03-15** 14:36:42.662

Figure 31. Node points page

Settings

*The **Settings** page lets you configure the Smart Polling settings.*



Smart Polling Progressive Mode Settings

● Disable progressive mode

Disable progressive mode and pause all progressive plans

○ Enable progressive mode

Enable progressive mode for the selected strategies

Strategy

Select strategies ▾

Figure 32. Settings page

Disable progressive mode

You can select this to disable all progressive mode and pause all progressive plans.

Enable progressive mode

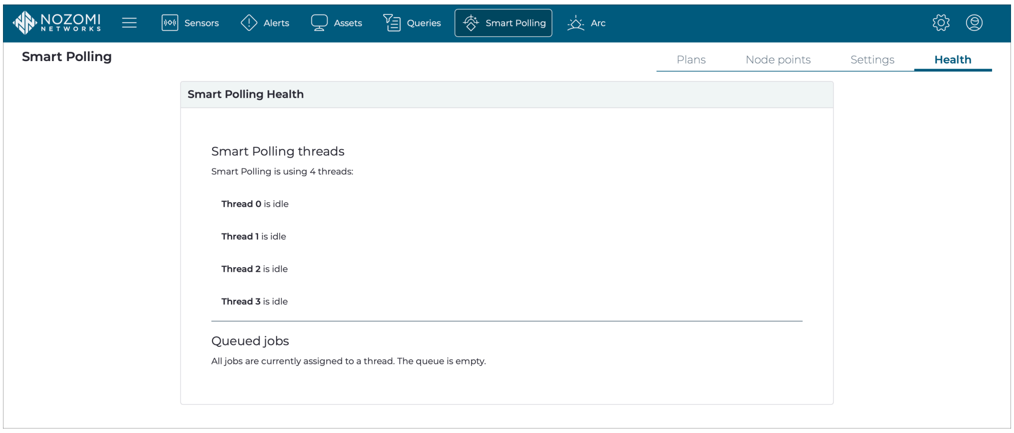
You can select this to enable progressive mode for selected strategies.

Strategy

This dropdown is only enabled when the Enable progressive mode checkbox is selected. The dropdown lets you select from a list of strategies.

Health

*The **Health** page lets you monitor the status of the CPU threads that Smart Polling is using, as well as queued jobs.*



Smart Polling Health

Smart Polling threads

Smart Polling is using 4 threads:

Thread 0 is idle

Thread 1 is idle

Thread 2 is idle

Thread 3 is idle

Queued jobs

All jobs are currently assigned to a thread. The queue is empty.

Figure 33. Health page

Create a Smart Polling plan

*The **Plans** page lets you create a new Smart Polling plan.*

About this task

Some of the options that follow depend on which strategy that you choose. Not all options apply to all strategies.

Procedure

1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

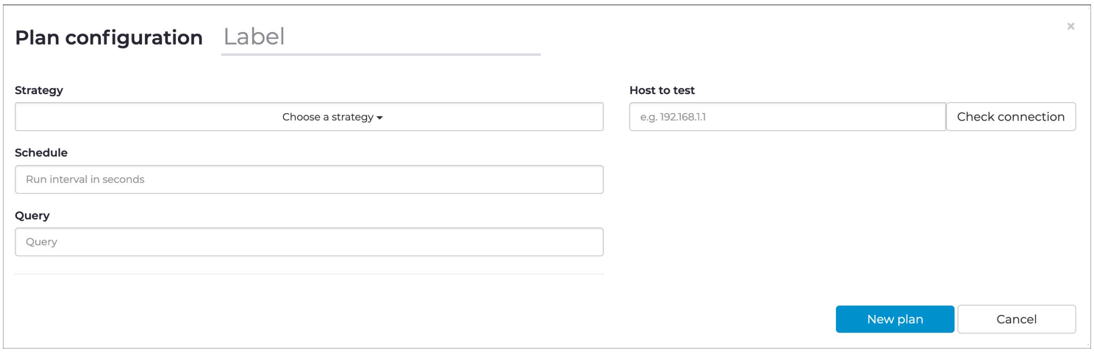
2. In the top right, select **Plans**.

   Result: The **Plans** page opens.

3. In the top right, select **New plan**.

   Result: A dialog shows.

4. In the **Label** field, enter a name for the plan.



5. In the **Strategy** dropdown, select a strategy.

> **Note:**
> You can use the **Credentials manager** to add credentials to the nodes that the plan targets.

6. In the **Schedule** field, enter a value (seconds) for the run interval.

7. If applicable, in the **Target** section, select an option:

   Choose from:

   - **Use identities**
   - **Use query**

   a. **Optional:** If you chose **Use identities**, choose the applicable credentials. To do this, select them from the list on the left and add them to the list on the right.
   b. **Optional:** If you chose **Use query**, the result of the query determines the list of node points. If necessary, use the **Credentials manager** to add credentials to the nodes targeted by the plan.
8. If applicable, from the **Data to be collected** dropdown, select the specific items to collect for the selected strategy.

   Note:
   The items shown are a generic list. The options available will vary depending on the specific target *OS* version, or the local configuration.

9. Verify that Smart Polling can connect correctly to a given node.
   a. In the **Host to test** field, enter an *IP* address of the node that you want to check.
   b. Select **Check connection**.

   Result: If the connection check is successful, a green tick will show.

10. View the results to determine if the Smart Polling plan is correct. You can also troubleshoot potential problems, such as incorrect credentials, or Guardian being unable to reach plan nodes.

Edit a Smart Polling plan

It is possible to edit a Smart Polling plan that already exists.

Procedure

1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. In the top right, select **Plans**.

   Result: The **Plans** page opens.

3. To the left of the name of the applicable plan, select the ☰ icon.

   Result: A dialog shows.

4. In the **Strategy** field, note the existing strategy.

   > **Note:**
   > When you edit a plan, you cannot change its strategy. For strategies that require credentials, you will need to use the **Credentials manager** to add credentials to the set of nodes to be polled when using a query.

5. In the **Schedule** field, enter a value in seconds.
6. In the **Target** section, select an option:

   Choose from:

   - **Use identities**
   - **Use query**

7. **Optional:** If you chose **Use identities**, choose the identities corresponding to the targeted nodes from the list on the left.
8. **Optional:** If you chose **Use query**, the result of the query determines the list of node points. Use the **Credentials manager** to add credentials to the nodes targeted by the plan.
9. Select **Edit plan**.

Add a network node to a Smart Polling plan

After you have created a plan, you can add a node, or multiple nodes, to it.

Procedure

1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. In the top right, select **Plans**.

   Result: The **Plans** page opens.

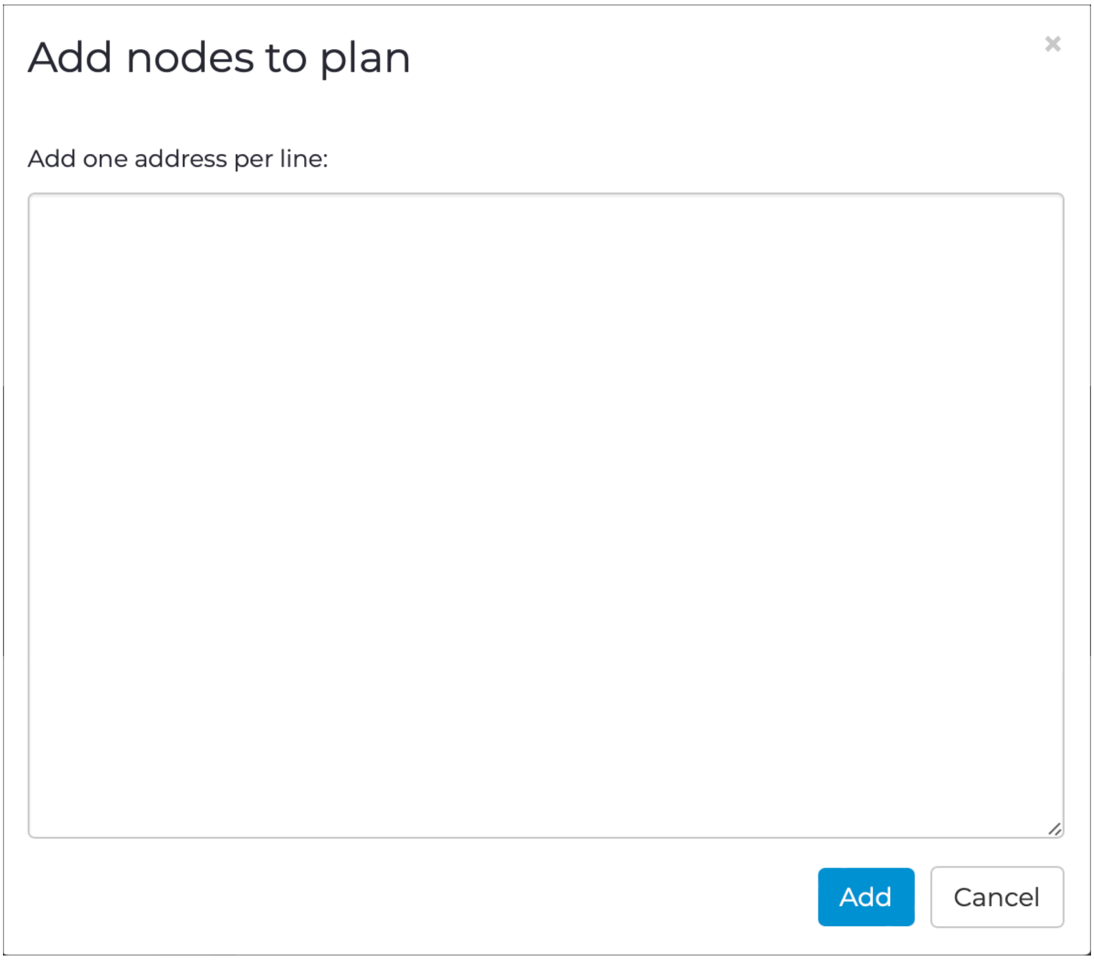
3. To the left of the name of the applicable plan, select the **>** icon.

   Result: The details for the plan show.

4. Select **+** **Add nodes to plan**.

   Result: A dialog shows.

5. In the dialog, enter an *IP* address. If you want to add more than one *IP* address, enter each one on a new line.



Add nodes to plan

Add one address per line:

6. Select **Add**.

Results

The node(s) has (have) been added to the Smart Polling plan.

Add a node from the Network page

Once you have created a Smart Polling plan, you can add arbitrary nodes to the target from the Network page. The Smart Polling plan will poll these nodes even if the plan's query does not return them.

Procedure

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

   Result: The **Network** page opens.

2. In the top right, select **Nodes**.

   Result: The **Nodes** page opens.

3. To the left of the name of the applicable plan, select the ◈ icon.

   Result: A dialog shows.

4. From the **Select an existing plan to add the node to** dropdown, select the plan you want to add the selected node to.

   Note:
   Fields that are not modified in this dialog are automatically populated with the plan-configured values.

   Result: A dialog shows.

5. Edit the field(s) as necessary to change the parameter(s) of the existing plan.
6. Select **Add**.

Results

The node(s) has (have) been added to the Smart Polling plan.

Edit the run interval of a progressive Smart Polling plan

You can manually adjust some aspects of Progressive mode plans. By default, each plan runs every 24 hours, but you can manually adjust this interval.

Procedure

1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. In the top right, select **Plans**.

   Result: The **Plans** page opens.

3. To the left of the title of the plan that you would like to edit, select the ☰ icon.

   Result: A dialog opens.

4. In the **Schedule** field, edit the value (seconds) as necessary.

   Note:
   The default value is 86400 (seconds) or 24 hours.

5. To save your changes, select **Edit plan**.

Progressive enablement

You can enable progressive mode to increase visibility.

Progressive mode is a Smart Polling option that increases visibility. To do this it automates plan creation and execution, and polls the correct nodes with the correct parameters based on asset information that has been detected passively.

Smart Polling automatically identifies the optimal target for polling. For example, only nodes that the query in the related strategy identifies will be polled.

You can select the Smart Polling strategies that you want to create a Progressive Smart Polling plan. Enabled Progressive Smart Polling plans show in the **Plans** tab.

Enable progressive mode

You can enable Progressive mode to increase visibility.

Procedure

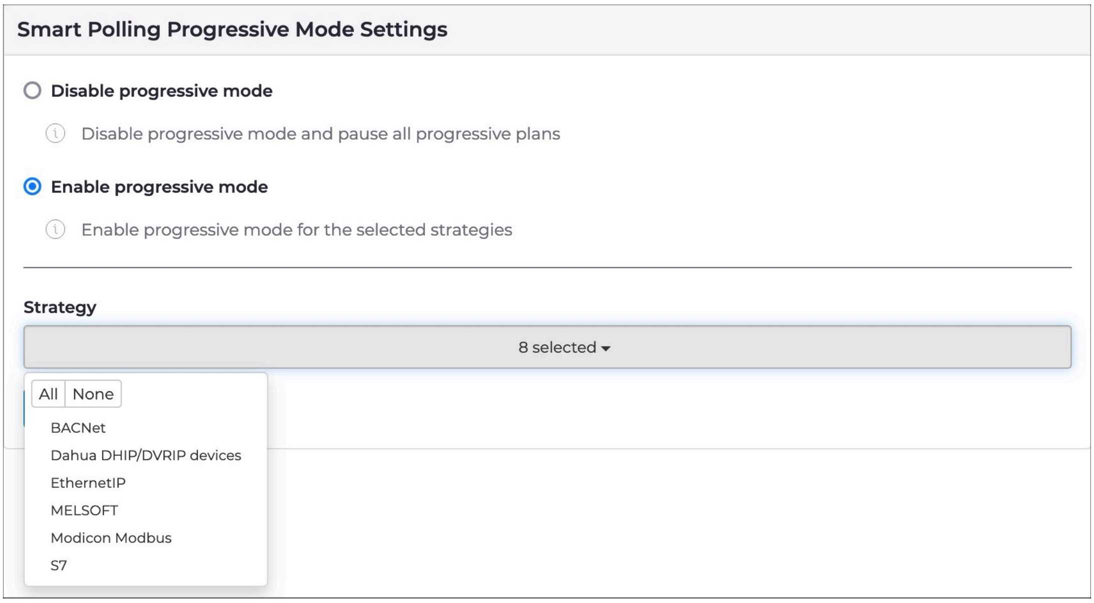
1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. In the top right, select **Settings**.

   Result: The **Settings** page opens.

3. In the **Smart Polling Progressive Mode Settings** section, select **Enable progressive mode**.



Smart Polling Progressive Mode Settings

○ Disable progressive mode

Disable progressive mode and pause all progressive plans

● Enable progressive mode

Enable progressive mode for the selected strategies

Strategy: 8 selected

Note:
If you select **Disable progressive mode** the progressive mode Smart Polling plans that have been newly created, will stop executing. Also, they will be, grayed-out in the **Plans** tab.

Results

Progressive mode has been enabled.

Log level customization

Smart Polling logs self-diagnostic information about its operations and activities during execution.

When Smart Polling logs self-diagnostic information, the logs are collected in the `/data/log/n2os/ n2ossp.log` file.

To change the level of detail in the logs, you can add these lines to the configuration file:

```
/data/cfg/n2os.conf.user:
```

```
sp log_level <LEVEL>
```

where `<LEVEL>` is one of the following values (in increasing order of verbosity):

- FATAL
- ERROR
- WARN
- INFO
- DEBUG

Note:
The default value is INFO.

After you have changed and saved the file, you can restart Smart Polling with the command:

```
service n2ossp stop
```

Note:

The service automatically restarts after the execution of this command.

To configure the file to see only ERROR and FATAL messages, in the `/data/cfg/ n2os.conf.user` file, you can add this rule:

```
sp log_level ERROR
```

then restart the process with the command:

```
service n2ossp stop
```

Note:

The configured level is the minimum to be printed, so ERROR will print log lines for both ERROR and FATAL messages, whereas FATAL will print log lines only for FATAL messages.

View the enriched information history for a node

*The **Node points** page lets you view the enriched information history for a node.*

Procedure

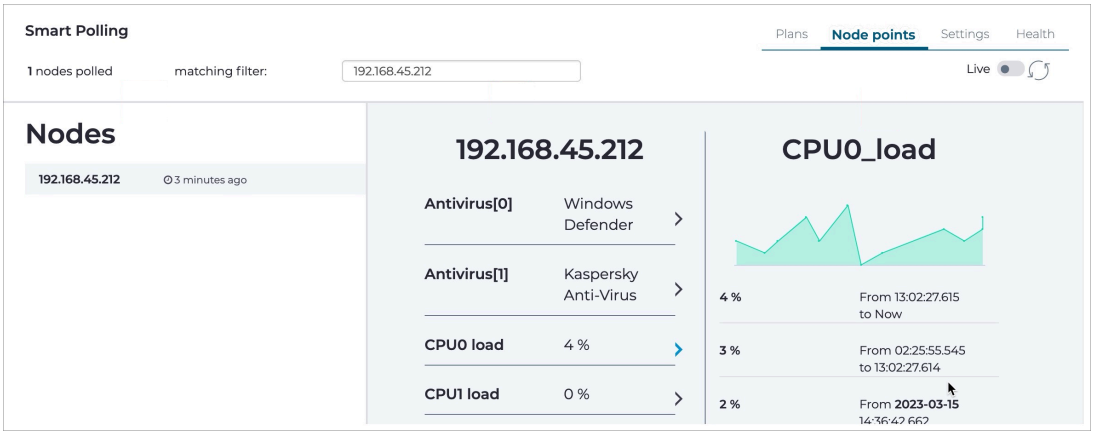
1. In the top navigation bar, select **Smart Polling**.

   Result: The **Smart Polling** page opens.

2. In the top right, select **Node points**.

   Result: The **Node points** page opens.

3. In the left column, select a node point.

   Smart Polling

   1 nodes polled matching filter: 192.168.45.212

   Nodes

   192.168.45.212 3 minutes ago

   192.168.45.212

Antivirus[0]	Windows Defender
Antivirus[1]	Kaspersky Anti-Virus
CPU0 load	4 %
CPU1 load	0 %

   CPU0_load

4 %	From 13:02:27.615 to Now
3 %	From 02:25:55.545 to 13:02:27.614
2 %	From 2023-03-15 14:36:42.662

   Result: The second and third columns show an increased level of detail for the extracted information for that node point

Chapter 7. Arc

Arc overview

Arc™ *is a host-based sensor that detects and defends against malicious or compromised endpoints, and insider attacks. You can use Arc sensors to aggregate data for analysis and reports, either on-premises, or in the Vantage cloud.*

General

When detecting cyberthreats, identifying vulnerabilities, or analyzing anomalies in your processes, it is critical to have as much detailed network and system information as possible. More accurate and timely access to data leads to better diagnostics and a faster time to repair.

Arc gives you enhanced endpoint data collection and asset visibility for your networks. This enhanced visibility gives you more:

- Vulnerability assessment capabilities
- Endpoint protection
- Traffic analysis capabilities
- Accurate diagnostics of in-progress threats and anomalies

Arc lets you easily identify compromised hosts that have:

- Malware
- Rogue applications
- Unauthorized *universal serial bus (USB)* devices
- Suspicious user activity

Arc sensors are endpoint executables that run on hosts on these operating systems:

- Microsoft Windows
- Linux
- Apple macOS
- Embedded devices (that run one of the above *OS*s). For more information, see

The data that is collected can be sent to either Guardian or Vantage.

Use cases and deployment scenarios

Arc lets you:

- Incorporate air-gapped devices into the analysis and reporting system
- Gain deeper intelligence or insight on critical endpoint devices
- Continuously monitor endpoints
- Automatically deploy sensors across thousands of devices
- Use a low-impact process to scan air-gapped networks
- Deploy with solutions

Continuous monitoring

Because the Arc sensor is on the host, it can monitor traffic continuously, even when the device is not sending or receiving traffic.

User-specific activity monitoring

With more access to endpoint data, Arc lets you connect network traffic and anomalies with specific users. This helps to identify potential insider threats and makes corrective actions both easier and quicker.

Local behavioral analysis (Sigma rules)

Sigma is a common open-source standard that lets you analyze log files to identify malicious events. They are not necessarily related to network artifacts, and as such, would not be detected without residing on a machine. Nozomi Networks Labs curates all the Sigma rules that are loaded into Arc. A *Threat Intelligence (TI)* active license is needed to receive curated rules from the upstream Nozomi endpoint.

Temporary deployment

It is not necessary to keep the Arc executable on a host after you have collected information. This means that you can remove it after data has been collected to conserve host resources, and maintain a clean host environment.

Architecture

It is important to understand the different architecture possibilities that are available with Arc.

You can connect Arc:

- To Guardian
- To Vantage

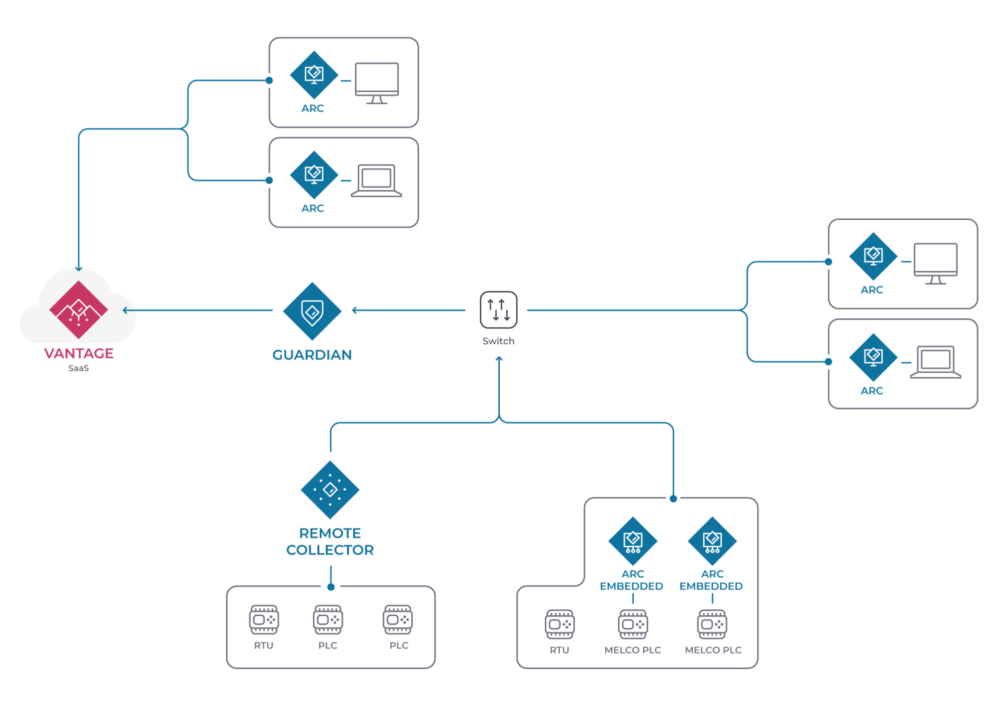


Figure 34. Arc architecture example

Arc in Guardian

*The **Arc** button in the Guardian Web UI lets you access the different pages for Arc.*

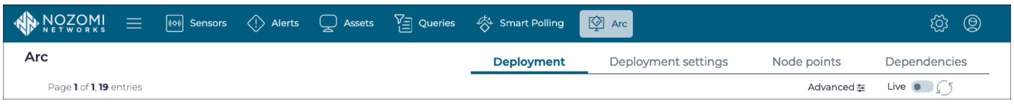


Figure 35. Arc button in Guardian Web UI

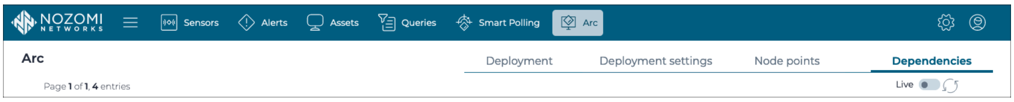
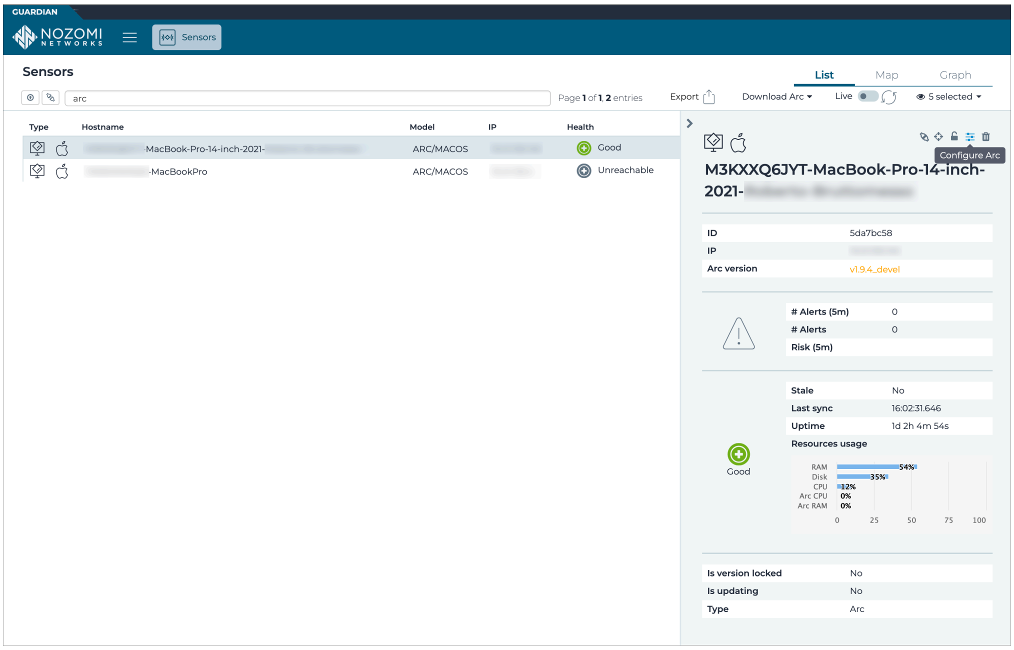


Figure 36. Arc button in Guardian Web UI (not connected to Vantage)

When you select **Arc** in the Guardian Web *user interface (UI)*, you get access to these pages:

- **Deployment**
- **Deployment settings**
- **Node points**
- **Dependencies** (only for Guardians that are not connected to Vantage)

Configure an Arc sensor



Type	Hostname	Model	IP	Health
	[redacted]-MacBook-Pro-14-inch-2021-[redacted]	ARC/MACOS	[redacted]	Good
	[redacted]-MacBookPro	ARC/MACOS	[redacted]	Unreachable

M3KXXQ6JYT-MacBook-Pro-14-inch-2021-[redacted]

ID	5da7bc58
IP	[redacted]
Arc version	v1.9.4_devel

# Alerts (5m)	0
# Alerts	0
Risk (5m)	

Stale	No
Last sync	16:02:31.646
Uptime	1d 2h 4m 54s

Is version locked	No
Is updating	No
Type	Arc

Figure 37. Configure an Arc sensor

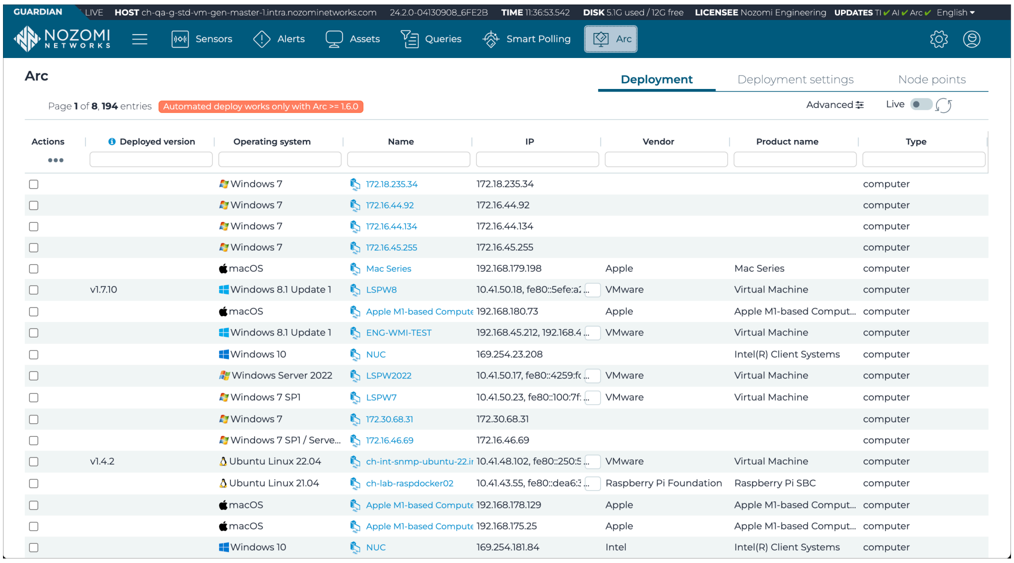
You can configure an individual Arc sensor directly from Guardian. To do this, you can select the applicable Arc sensor from the **Sensors** list, and select the ☰ icon.

Deployment

*The **Deployment** page shows a table of all the devices available for Arc deployment.*

The table only shows machines which have an *OS* that matches one that Arc supports.

As Guardian detects the installed *OS*, the correct Arc package will be automatically deployed.



HOST ch-qa-g-std-vm-gen-master-1.intra.nozominetworks.com 24.2.0-04130908_6FE2B **TIME** 11:36:53.542 **DISK** 5.1G used / 12G free **LICENSEE** Nozomi Engineering **UPDATES** TI ✓ AI ✓ Arc ✓ English

Arc

Page **1** of **8**, **194** entries Automated deploy works only with Arc >= 1.6.0

Actions	Deployed version	Operating system	Name	IP	Vendor	Product name	Type
•••							
□		Windows 7	172.18.235.34	172.18.235.34			computer
□		Windows 7	172.16.44.92	172.16.44.92			computer
□		Windows 7	172.16.44.134	172.16.44.134			computer
□		Windows 7	172.16.45.255	172.16.45.255			computer
□		macOS	Mac Series	192.168.179.198	Apple	Mac Series	computer
□	v1.7.10	Windows 8.1 Update 1	LSPW8	10.41.50.18, fe80::5efe:a ...	VMware	Virtual Machine	computer
□		macOS	Apple M1-based Compute	192.168.180.73	Apple	Apple M1-based Comput...	computer
□		Windows 8.1 Update 1	ENG-WMI-TEST	192.168.45.212, 192.168.4 ...	VMware	Virtual Machine	computer
□		Windows 10	NUC	169.254.23.208		Intel(R) Client Systems	computer
□		Windows Server 2022	LSPW2022	10.41.50.17, fe80::4259:f ...	VMware	Virtual Machine	computer
□		Windows 7 SP1	LSPW7	10.41.50.23, fe80::100:7f: ...	VMware	Virtual Machine	computer
□		Windows 7	172.30.68.31	172.30.68.31			computer
□		Windows 7 SP1 / Serve...	172.16.46.69	172.16.46.69			computer
□	v1.4.2	Ubuntu Linux 22.04	ch-int-snmp-ubuntu-22.i	10.41.48.102, fe80::250:5 ...	VMware	Virtual Machine	computer
□		Ubuntu Linux 21.04	ch-lab-raspdocker02	10.41.43.55, fe80::dea6:3 ...	Raspberry Pi Foundation	Raspberry Pi SBC	computer
□		macOS	Apple M1-based Compute	192.168.178.129	Apple	Apple M1-based Comput...	computer
□		macOS	Apple M1-based Compute	192.168.175.25	Apple	Apple M1-based Comput...	computer
□		Windows 10	NUC	169.254.181.84	Intel	Intel(R) Client Systems	computer

Figure 38. Deployment page

Advanced

The **Advanced** button lets you access the **Advanced** page. For more details, see Advanced (on page 119).

Execution details

The **Execution details** lets you access the **Activity Log**. For more details, see Execution details (on page 121).

Live toggle

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

Refresh

The ↻ icon lets you immediately refresh the current view.

Actions

The **ACTIONS** column has a checkbox for each row in the table. This lets you select multiple nodes before you then apply an action to them.

The **ACTIONS** menu icon ••• gives you access to these options:

- Select all in current page
- Select none in current page
- Invert selection in current page
- Deploy Service mode: this installs Arc in Service mode for the selected devices
- Remove Service mode: this removes the Arc previously installed in Service mode for the selected devices
- Execute One-shot: this executes a One-shot run for the selected devices, which are left clean after an execution. Arc self destroys after its execution

Operating System

The **OPERATING SYSTEM** column shows the *OS* for each of the Arc sensors in the table. The field at the top of the column lets you use the *OS* to filter the table.

IP

The **IP** column shows the *IP* for each of the Arc sensors in the table. The field at the top of the column lets you use the *IP* to filter the table.

Vendor

The **VENDOR** column shows the vendor name for each of the Arc sensors in the table. The field at the top of the column lets you use the vendor name to filter the table.

Product name

The **PRODUCT NAME** column shows the product name for each of the Arc sensors in the table. The field at the top of the column lets you use the product name to filter the table.

Type

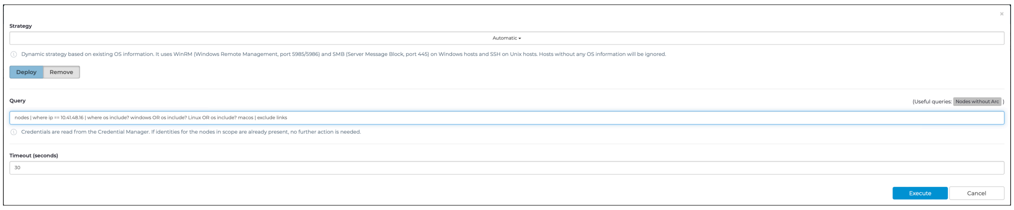
The **TYPE** column shows the device type for each of the Arc sensors in the table. The field at the top of the column lets you use the device type to filter the table.

Advanced

The ***Advanced*** *page lets you interact with nodes that have no operating system (OS) detected, or do not show on the same page in the table.*

The default table view only shows nodes that have had their *OS* detected. Also, if you select multiple nodes, actions will only be applied to a single page of nodes. To overcome these limitations, you can use the **Advanced** button to go to the **Advanced** page. This will let you interact with a:

- Set of nodes that cannot be shown on a single page
- Set of nodes that have no *OS* detected



Strategy

Automatic

Dynamic strategy based on existing OS information. It uses WinRM (Windows Remote Management, port 5985/5986) and SMB (Server Message Block, port 445) on Windows hosts and SSH on Unix hosts. Hosts without any OS information will be ignored.

Query

nodes | where ip == 10.41.48.16 | where os include? windows OR os include? Linux OR os include? macos | exclude links

Credentials are read from the Credential Manager. If identities for the nodes in scope are already present, no further action is needed.

Timeout (seconds)

30

Figure 39. Advanced page

Strategy

Automatic: This selection will use the *OS* that has been detected on the node to automatically choose a deployment strategy. You can select multiple nodes that have a different *OS*. This strategy will ignore a host if it has no *OS*.

WinRM: This selection will force the strategy, regardless of the *OS*, and deploy the correct Arc package for Windows.

SSH (Windows): This selection will force the *secure shell (SSH)* strategy, regardless of the *OS*, and deploy the correct Arc package for Windows.

SSH (Linux): This selection will force the *SSH* strategy, regardless of the *OS*, and deploy the correct Arc package for Linux.

SSH (macOS): This selection will force the *SSH* strategy, regardless of the *OS*, and deploy the correct Arc package for macOS.

Query

This field lets you create and execute queries on the nodes. This lets you filter and selectively install packages.

Timeout (seconds)

The **Timeout** dropdown lets you set the amount of time that Arc will try to communicate with a host machine before it skips it and goes to the next one.

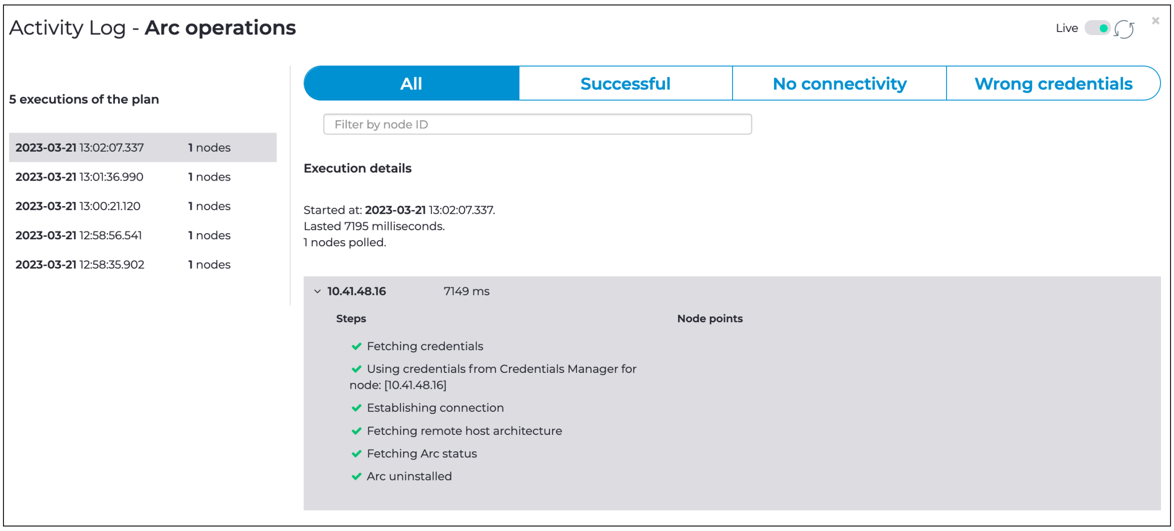
Execution details

*The **Execution details** button gives you access to the **Activity Log**.*

The **Activity Log** lets you troubleshoot the results of the executed deployments. When you select an execution on the left side of the page, you can analyze the selection.

You can use the **Filter by node ID** to focus on a single issue, such as:

- Credential missing, or
- Wrong credentials



Activity Log - **Arc operations**

5 executions of the plan

2023-03-21 13:02:07.337	**1** nodes
2023-03-21 13:01:36.990	**1** nodes
2023-03-21 13:00:21.120	**1** nodes
2023-03-21 12:58:56.541	**1** nodes
2023-03-21 12:58:35.902	**1** nodes

Execution details

Started at: **2023-03-21** 13:02:07.337.
Lasted 7195 milliseconds.
1 nodes polled.

10.41.48.16 7149 ms

Steps **Node points**

- ✓ Fetching credentials
- ✓ Using credentials from Credentials Manager for node: [10.41.48.16]
- ✓ Establishing connection
- ✓ Fetching remote host architecture
- ✓ Fetching Arc status
- ✓ Arc uninstalled

Live toggle

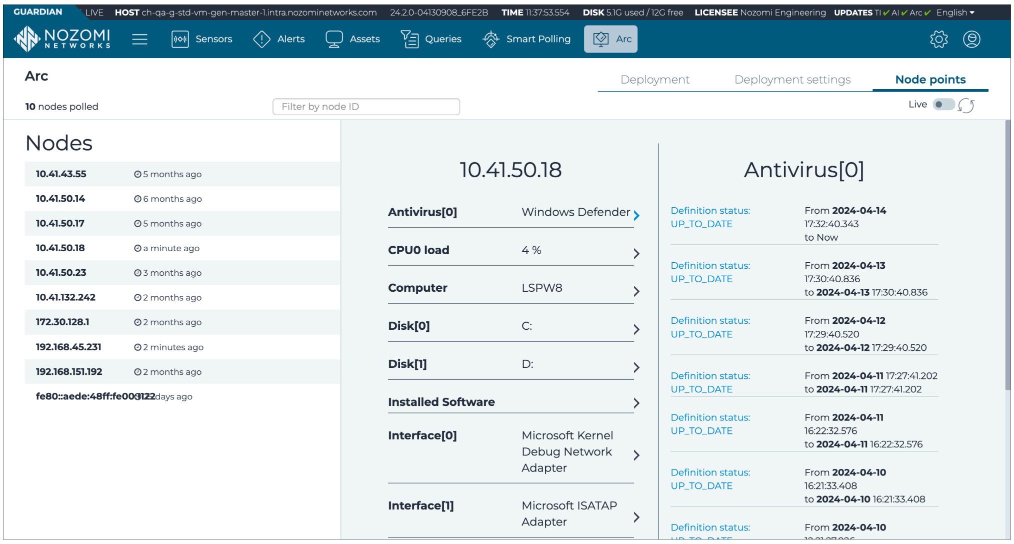
The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The ↻ icon lets you immediately refresh the current view.

Node points

*The **Node points** page shows data points that are collected over time, and represent the state of the target machine.*



Arc

10 nodes polled

Nodes

10.41.43.55	5 months ago
10.41.50.14	6 months ago
10.41.50.17	5 months ago
10.41.50.18	a minute ago
10.41.50.23	3 months ago
10.41.132.242	2 months ago
172.30.128.1	2 months ago
192.168.45.231	2 minutes ago
192.168.151.192	2 months ago
fe80::aede:48ff:fe006122	days ago

10.41.50.18

Antivirus[0]	Windows Defender
CPU0 load	4 %
Computer	LSPW8
Disk[0]	C:
Disk[1]	D:
Installed Software	
Interface[0]	Microsoft Kernel Debug Network Adapter
Interface[1]	Microsoft ISATAP Adapter

Antivirus[0]

Definition status: UP_TO_DATE	From **2024-04-14** 17:32:40.343 to Now
Definition status: UP_TO_DATE	From **2024-04-13** 17:30:40.836 to **2024-04-13** 17:30:40.836
Definition status: UP_TO_DATE	From **2024-04-12** 17:29:40.520 to **2024-04-12** 17:29:40.520
Definition status: UP_TO_DATE	From **2024-04-11** 17:27:41.202 to **2024-04-11** 17:27:41.202
Definition status: UP_TO_DATE	From **2024-04-11** 16:22:32.576 to **2024-04-11** 16:22:32.576
Definition status: UP_TO_DATE	From **2024-04-10** 16:21:33.408 to **2024-04-10** 16:21:33.408
Definition status:	From **2024-04-10**

Figure 40. Node points page in Guardian

Node points count

This shows the number of the nodes polled.

Filter by node ID

This field lets you use the node *ID* to filter the nodes.

Live toggle

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

Refresh

The ⟳ icon lets you immediately refresh the current view.

Nodes

The list of nodes that show at least one node point.

Chapter 8. Network

Network

The ***Network*** *page gives you access to multiple pages that show nodes, links, sessions in tabular format and graphs and traffic in a graphical format.*

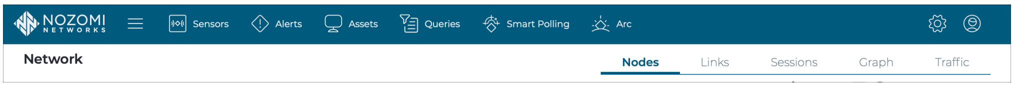


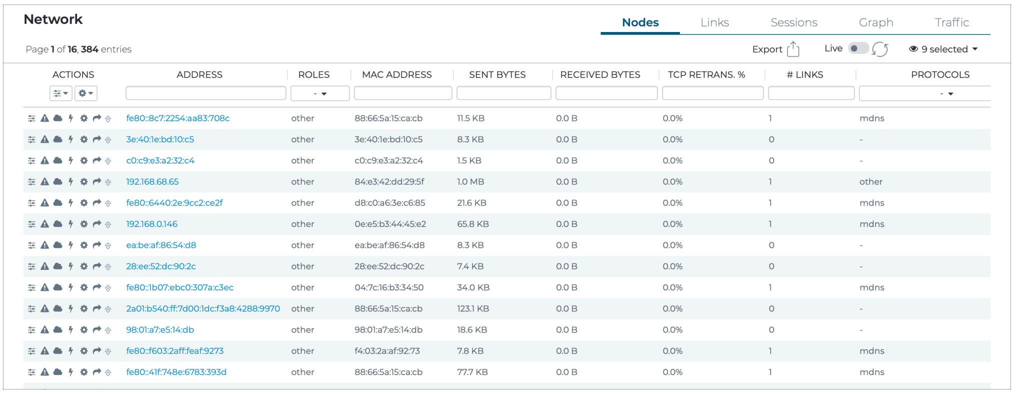
Figure 41. Network page

The **Network** page has these tabs:

- Nodes (on page 126)
- Links (on page 136)
- Sessions (on page 145)
- Graph (on page 149)
- Traffic (on page 158)

Nodes

*The **Nodes** page lets you view all the network nodes in your environment and perform actions on them.*



Page **1** of **16**, **384** entries

ACTIONS	ADDRESS	ROLES	MAC ADDRESS	SENT BYTES	RECEIVED BYTES	TCP RETRANS. %	# LINKS	PROTOCOLS
		-						-
	fe80::8c7:2254:aa83:708c	other	88:66:5a:15:ca:cb	11.5 KB	0.0 B	0.0%	1	mdns
	3e:40:1e:bd:10:c5	other	3e:40:1e:bd:10:c5	8.3 KB	0.0 B	0.0%	0	-
	c0:c9:e3:a2:32:c4	other	c0:c9:e3:a2:32:c4	1.5 KB	0.0 B	0.0%	0	-
	192.168.68.65	other	84:e3:42:dd:29:5f	1.0 MB	0.0 B	0.0%	1	other
	fe80::6440:2e:9cc2:ce2f	other	d8:c0:a6:3e:c6:85	21.6 KB	0.0 B	0.0%	1	mdns
	192.168.0.146	other	0e:e5:b3:44:45:e2	65.8 KB	0.0 B	0.0%	1	mdns
	ea:be:af:86:54:d8	other	ea:be:af:86:54:d8	8.3 KB	0.0 B	0.0%	0	-
	28:ee:52:dc:90:2c	other	28:ee:52:dc:90:2c	7.4 KB	0.0 B	0.0%	0	-
	fe80::1b07:ebc0:307a:c3ec	other	04:7c:16:b3:34:50	34.0 KB	0.0 B	0.0%	1	mdns
	2a01:b540:ff:7d00:1dc:f3a8:4288:9970	other	88:66:5a:15:ca:cb	123.1 KB	0.0 B	0.0%	0	-
	98:01:a7:e5:14:db	other	98:01:a7:e5:14:db	18.6 KB	0.0 B	0.0%	0	-
	fe80::f603:2aff:feaf:9273	other	f4:03:2a:af:92:73	7.8 KB	0.0 B	0.0%	1	mdns
	fe80::41f:748e:6783:393d	other	88:66:5a:15:ca:cb	77.7 KB	0.0 B	0.0%	1	mdns

Figure 42. Nodes page

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Configure a node

*The **Nodes** page lets you configure nodes.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Nodes**.

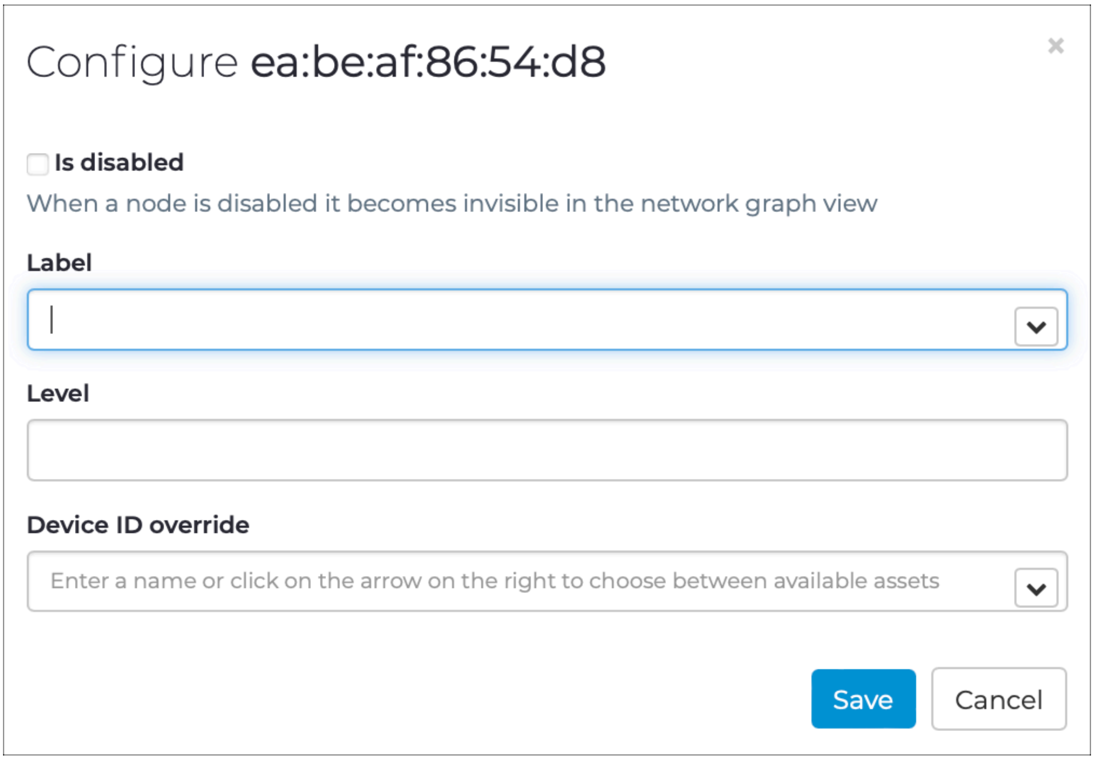
   Result: The **Nodes** page opens.

3. To the left of the applicable node, select the configure ☰ icon.

   Result: A dialog shows.

4. **Optional:**

   To make the node(s) invisible in network graph view, select **Is disabled**.



Configure **ea:be:af:86:54:d8** ×

□ **Is disabled**

When a node is disabled it becomes invisible in the network graph view

Label

Level

Device ID override

Enter a name or click on the arrow on the right to choose between available assets

5. From the **Label** dropdown, select an asset and assign the node to it.
6. In the **Level** field, enter a level in accordance with the Purdue model classification.
7. From the **Device ID override** dropdown, remove or re-assign Device ID to overwrite the automatically assigned **Device ID**.
8. Select **Save**.

Results

The node has been configured.

Show alerts for a node

*The **Nodes** page lets you show alerts for a selected node.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Nodes**.

   Result: The **Nodes** page opens.

3. To the left of the applicable node, select the ⚠ icon.

   Result: A list of all the requested traces for the node shows.

Show requested traces for a node

*The **Nodes** page lets you show requested traces for a selected node.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Nodes**.

   Result: The **Nodes** page opens.

3. To the left of the applicable node, select the ☁ icon.

   Result: A list of all the requested traces for the node shows.

Request a trace for a node

*The **Nodes** page lets you request a trace for a selected node.*

Procedure

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

   Result: The **Network** page opens.

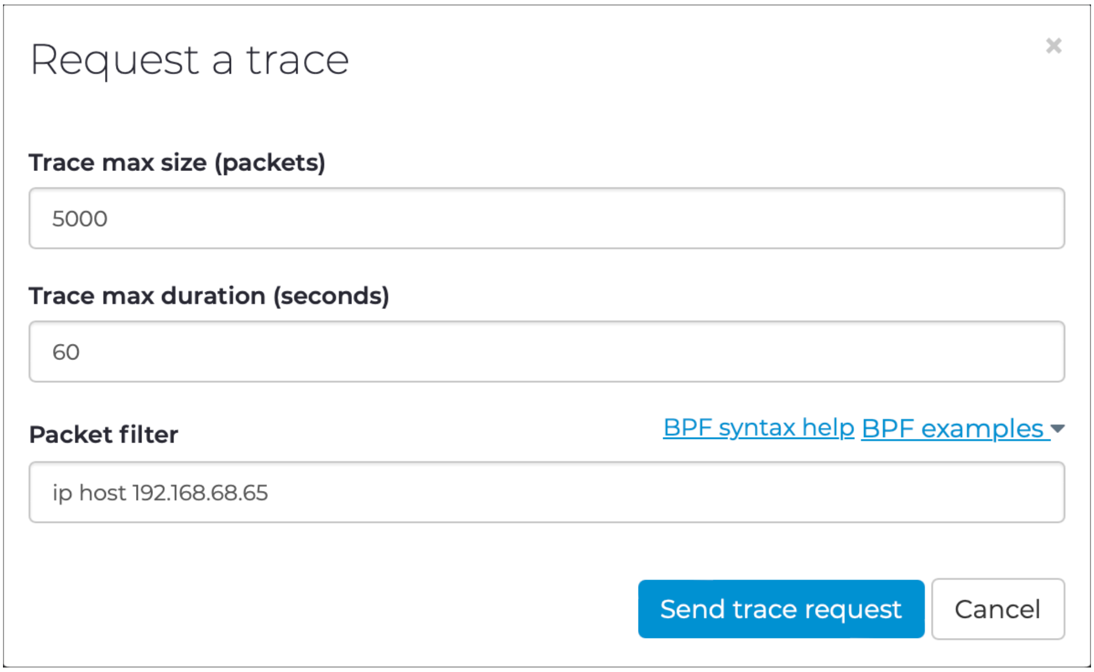
2. Select **Nodes**.

   Result: The **Nodes** page opens.

3. To the left of the applicable node, select the ϟ icon.

   Result: A dialog shows.

4. To set the maximum packet size, in the **Trace max size (packets)** field, enter a value.



Request a trace

Trace max size (packets)

5000

Trace max duration (seconds)

60

Packet filter

ip host 192.168.68.65

> **Note:**
> The default size is 5000 packets.

5. To set the maximum duration of the trace, in the **Trace max duration (seconds)** field, enter a value.

> **Note:**
> The default value is 60 seconds.

6. **Note:**
   The **Packet filter** field is automatically populated with a *Berkeley Packet Filter (BPF)* that captures the packets to/from the selected node, but you can customize this.

   If necessary, customize this field.

   Note:
   You can select **BPF syntax help** to show more information on *BPF* syntax.

   Note:
   You can select **BPF examples** to see some examples.

7. Select **Send trace request**.

Results

The trace has been requested.

Manage learning for a node

*The **Nodes** page lets you manage the learning for a selected node.*

About this task

The **Manage Learning** dialog lets you learn and delete the entire node and its individual details, such as *IP* or *MAC* address.

> **Note:**
>
> The icon adjacent to the node shows its status. When the node details are:
>
> - A green icon shows when the node details have been entirely learned
> - An orange icon shows when the node details are only partially learned
> - A red icon shows when the node details have not been learned
>
> Individual details have either a green or red icon, depending on whether they are learned or not. When you learn, or delete a node, all of its details are affected in the same way. When you learn, or delete, an individual detail, only that detail's learning status changes.

Procedure

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

   Result: The **Network** page opens.

2. Select **Nodes**.

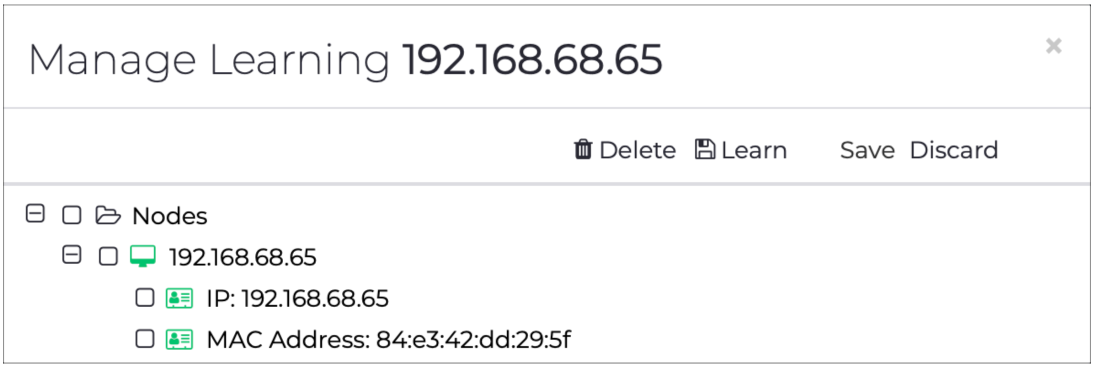
   Result: The **Nodes** page opens.

3. To the left of the applicable node, select the ⚙ icon.

   Result: A dialog shows.

4. **Optional:**

   Select an item(s) to delete.



Manage Learning **192.168.68.65**

   Choose from:

   - To delete the *IP* address, select the checkbox to the left.
   - To delete the *MAC* address, select the checkbox to the left.
   - To delete the node, and both the *IP* and *MAC* addresses, select the checkbox to the left.

   a. Select 🗑 **Delete** to delete the selected item(s).

5. **Optional:** Select an item(s) to learn.

   Choose from:

   - To learn the *IP* address, select the checkbox to the left.
   - To learn the *MAC* address, select the checkbox to the left.
   - To learn the node, and both the *IP* and *MAC* addresses, select the checkbox to the left.

   a. Select 💾 **Learn** to learn the selected item(s).

6. Select **Save**.

Navigate from a node

*The **Nodes** page lets you navigate to related entities from a selected node.*

Procedure

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

   Result: The **Network** page opens.

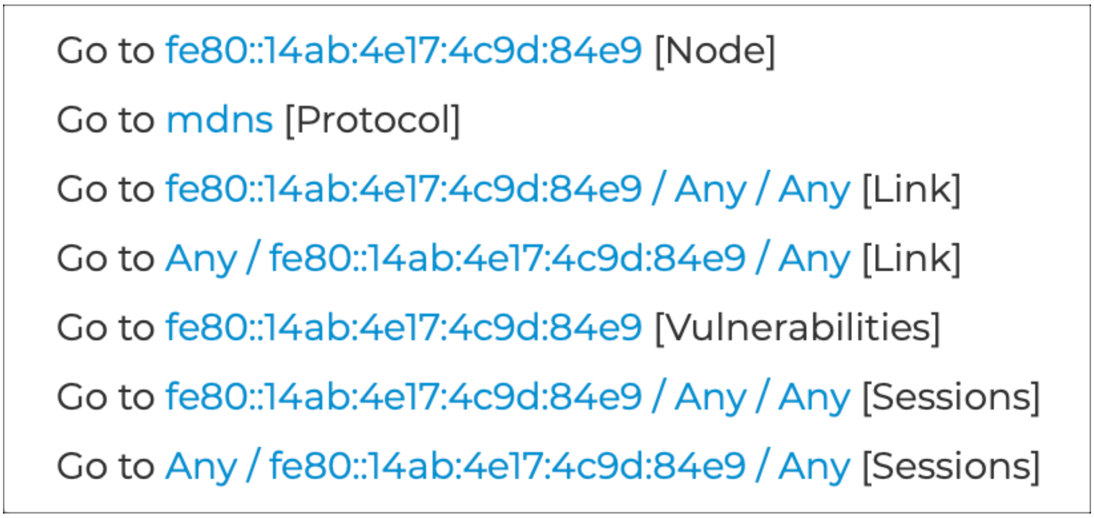
2. Select **Nodes**.

   Result: The **Nodes** page opens.

3. In the Actions column, to the left of the applicable node, select the ➦ icon.

   Result: A list of related entities shows.

4. Select the hyperlink that you want to navigate to.



Go to fe80::14ab:4e17:4c9d:84e9 [Node]

Go to mdns [Protocol]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Link]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Link]

Go to fe80::14ab:4e17:4c9d:84e9 [Vulnerabilities]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Sessions]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Sessions]

Results

The entity shows in the applicable page.

Add a node to a Smart Polling plan

*The **Nodes** page lets you add a node to an existing Smart Polling plan.*

About this task

The Smart Polling icon only shows if Smart Polling is present.

Procedure

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

   Result: The **Network** page opens.

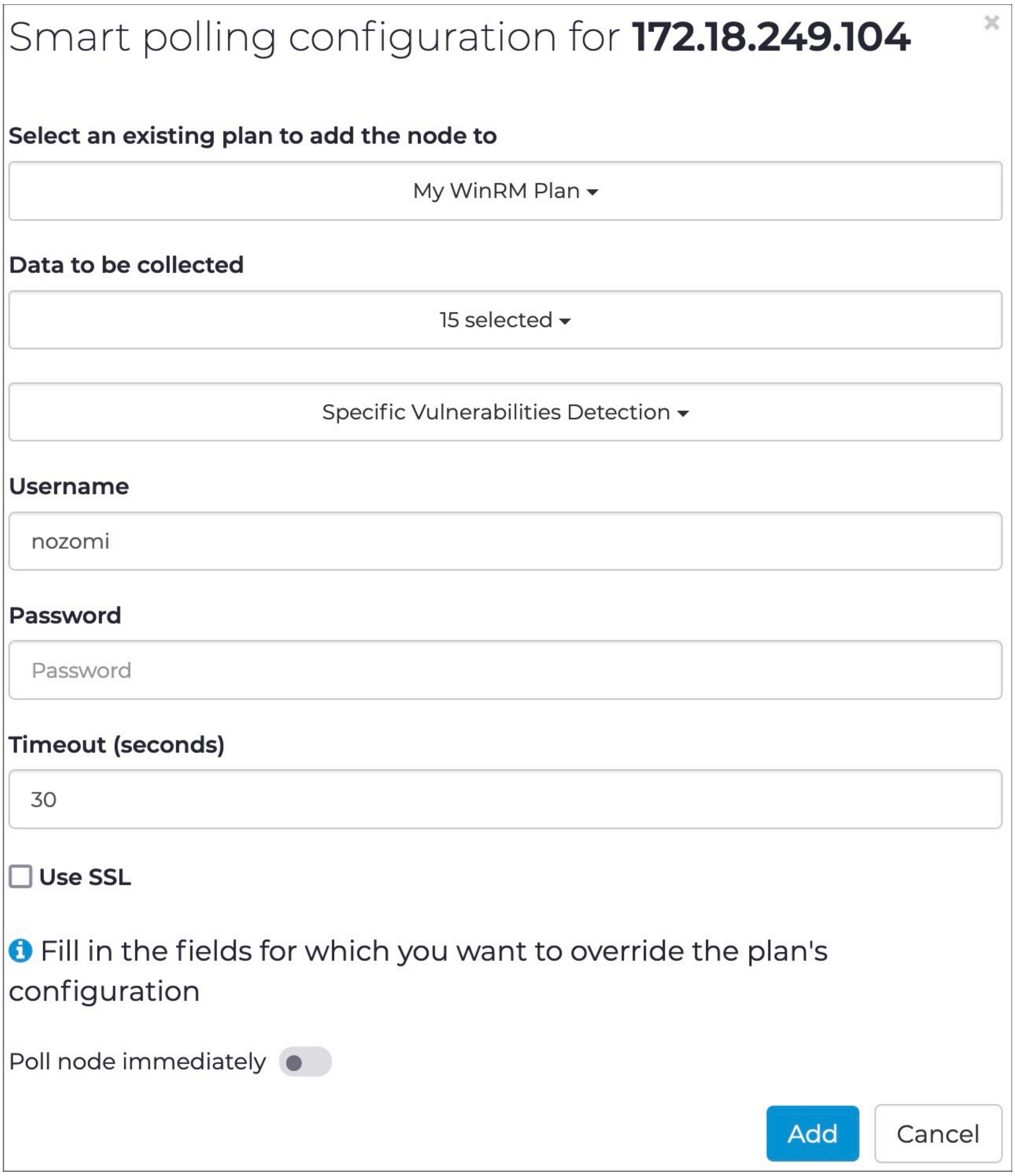
2. Select **Nodes**.

   Result: The **Nodes** page opens.

3. To add a node to a plan with an optionally different configuration from the plan's original one, in the Actions column, to the left of the applicable node, select the ◈ icon.

   Result: A dialog shows.

4. From the **Select an existing plan to add the node to** dropdown, select an existing plan to that you would like to add the node to.



Smart polling configuration for **172.18.249.104**

Select an existing plan to add the node to

My WinRM Plan

Data to be collected

15 selected

Specific Vulnerabilities Detection

Username

nozomi

Password

Password

Timeout (seconds)

30

☐ **Use SSL**

Fill in the fields for which you want to override the plan's configuration

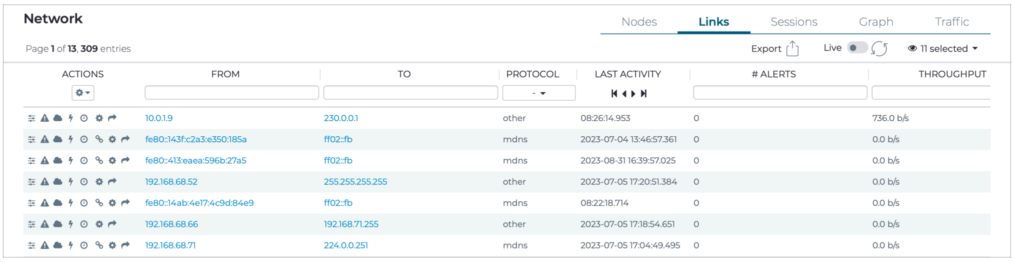
Poll node immediately

5. **Optional:** In the **Timeout (seconds)** field, enter a value to override the value in the current plan.
6. **Optional:** To poll the node immediately, set the **Poll node immediately** toggle to on.

> **Note:**
> If you do not set the **Poll node immediately** toggle to on, the node will be polled at the next execution of the selected plan.

Links

*The **Links** page shows all the links in your environment.*



Network

Page 1 of 13, 309 entries

ACTIONS	FROM	TO	PROTOCOL	LAST ACTIVITY	# ALERTS	THROUGHPUT
	10.0.1.9	230.0.0.1	other	08:26:14.953	0	736.0 b/s
	fe80::143f:c2a3:e350:185a	ff02::fb	mdns	2023-07-04 13:46:57.361	0	0.0 b/s
	fe80::413:eaea:596b:27a5	ff02::fb	mdns	2023-08-31 16:39:57.025	0	0.0 b/s
	192.168.68.52	255.255.255.255	other	2023-07-05 17:20:51.384	0	0.0 b/s
	fe80::14ab:4e17:4c9d:84e9	ff02::fb	mdns	08:22:18.714	0	0.0 b/s
	192.168.68.66	192.168.71.255	other	2023-07-05 17:18:54.651	0	0.0 b/s
	192.168.68.71	224.0.0.251	mdns	2023-07-05 17:04:49.495	0	0.0 b/s

Figure 43. Links page

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

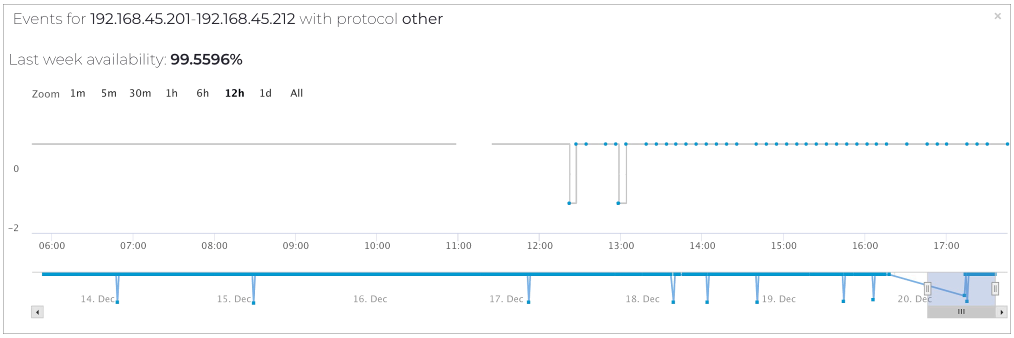
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Link events

Link events are shown in a graphical format.



Events for 192.168.45.201-192.168.45.212 with protocol other

Last week availability: 99.5596%

Figure 44. Link events

Availability

Link availability is based on UP and DOWN events.

Time span

You can use the time span control to view only the events in the specified time range. The available options are:

- Zoom
- 1m(inute)
- 5m
- 30m
- 1h(our)
- 6h
- 12h
- 1d(ay)
- All

Graphical history

A point with a value of 1 represents an UP event, a value -1 represents a DOWN event.

Link availability

A history of events is stored for each link.

Two events are of particular interest for computing availability:

- UP - This occurs when an activity is detected on an inactive link
- DOWN - This occurs when an active link stops its activity

Each event has a timestamp to track the precise moment of its occurrence.

Guardian computes the total downtime of a link by taking into consideration the history of events within a finite time window. Then, it sums the time spans of all events starting with a DOWN event and ending with an UP event. All links are considered active by default. Therefore, the availability of the link is 100% minus the percentage of the total downtime.

Track availability

The **Track availability** feature allows an accurate computation of availability. It enables the monitoring of activity on a link at regular intervals, generating extra UP and DOWN events, depending on the detected activity on both sides of the link during the last interval.

We recommend that you select a value greater than the expected link polling time to avoid checks that are too frequent and are likely to produce spurious DOWN events.

link_events generation is disabled by default. To enable it, see the configuration rule shown in **Configuration**.

Configure a link

The ***Links*** *page lets you configure links.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

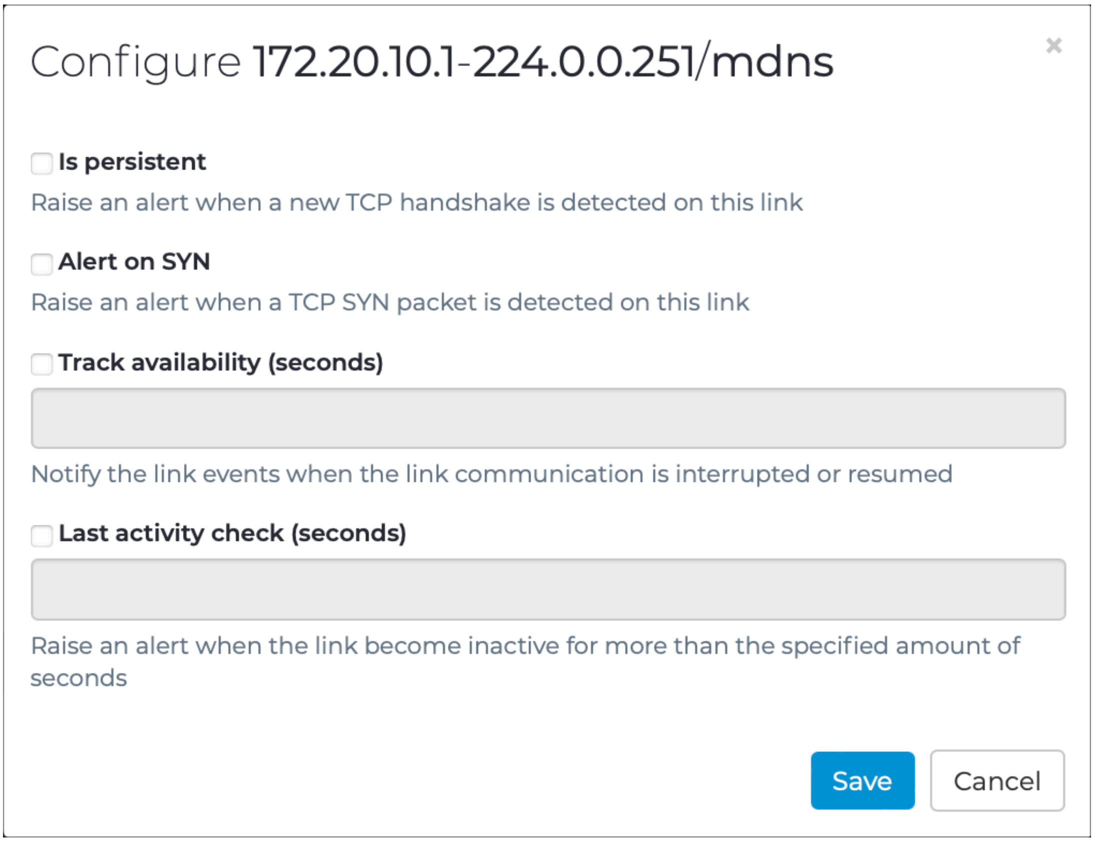
   Result: The **Links** page opens.

3. To the left of the applicable link, select the configure ☰ icon.

   Result: A dialog shows.

4. **Optional:**

   To raise an alert when a new *TCP* handshake is detected on the link, select **Is persistent**.



Configure **172.20.10.1-224.0.0.251/mdns**

□ **Is persistent**
Raise an alert when a new TCP handshake is detected on this link

□ **Alert on SYN**
Raise an alert when a TCP SYN packet is detected on this link

□ **Track availability (seconds)**
Notify the link events when the link communication is interrupted or resumed

□ **Last activity check (seconds)**
Raise an alert when the link become inactive for more than the specified amount of seconds

5. **Optional:** To raise an alert when a *TCP* SYN packet is detected on the link, select **Alert on SYN**.
6. **Optional:** To notify the link events when the link communication is interrupted or resumed., select **Track availability (seconds)** and enter a value.

7. **Optional:** To raise an alert when the link becomes inactive for more than the specified number of seconds, select **Last activity check (seconds)** and enter a value.
8. Select **Save**.

Results

The link has been configured.

Show alerts for a link

*The **Links** page lets you show alerts for a selected link.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

   Result: The **Links** page opens.

3. To the left of the applicable link, select the ⚠ icon.

   Result: A list of all the requested traces for the link shows.

Show requested traces for a link

*The **Links** page lets you show requested traces for a selected link.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

   Result: The **Links** page opens.

3. To the left of the applicable link, select the ☁ icon.

   Result: A list of all the requested traces for the link shows.

Request a trace for a link

*The **Links** page lets you request a trace for a selected link.*

Procedure

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

   Result: The **Network** page opens.

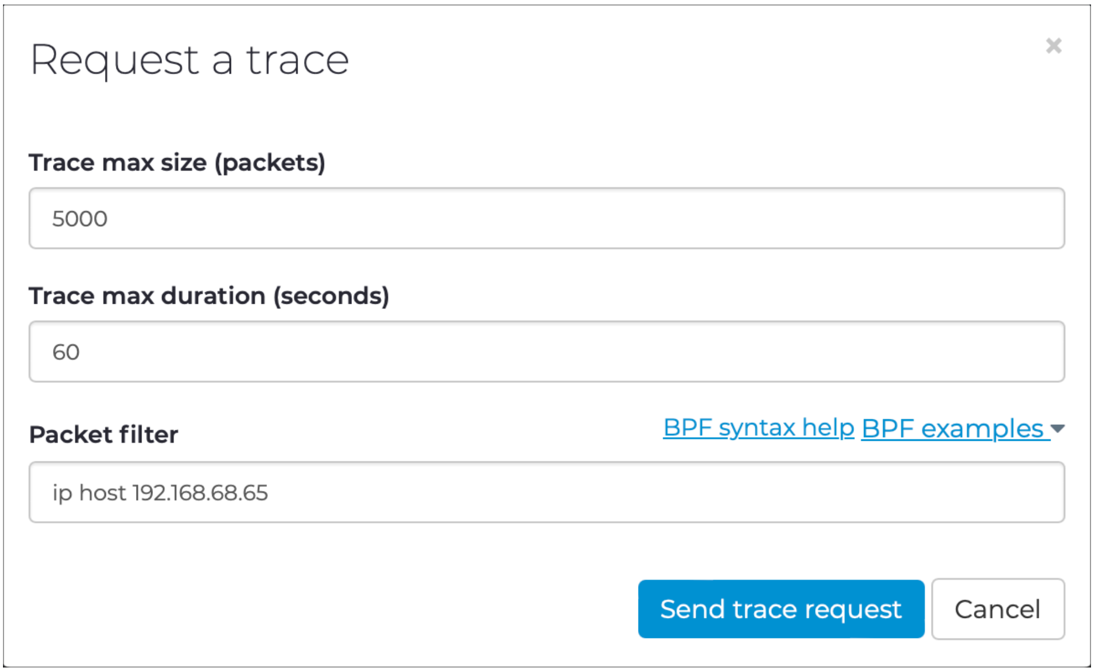
2. Select **Links**.

   Result: The **Links** page opens.

3. To the left of the applicable link, select the ⚡ icon.

   Result: A dialog shows.

4. To set the maximum packet size, in the **Trace max size (packets)** field, enter a value.

   Request a trace

   Trace max size (packets)

   5000

   Trace max duration (seconds)

   60

   Packet filter

   ip host 192.168.68.65

   Note:
   The default size is 5000 packets.

5. To set the maximum duration of the trace, in the **Trace max duration (seconds)** field, enter a value.

   Note:
   The default value is 60 seconds.

6. **Note:**
   The **Packet filter** field is automatically populated with a *BPF* that captures the packets to/from the selected link, but you can customize this.

   If necessary, customize this field.

   Note:
   You can select **BPF syntax help** to show more information on *BPF* syntax.

   Note:
   You can select **BPF examples** to see some examples.

7. Select **Send trace request**.

Results

The trace has been requested.

Show events for a link

*The **Links** page lets you show requested traces for a selected link.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

   Result: The **Links** page opens.

3. To the left of the applicable link, select the 🕘 icon.

   Result: A list of all the events for the link shows.

Show captured URLs for a link

*The **Links** page lets you show captured URLs for a selected link.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

   Result: The **Links** page opens.

3. To the left of the applicable link, select the 🔗 icon.

   Result: A list of all the captured *uniform resource locator (URL)*s from the analyzed traffic for the link shows.

Manage learning for a link

*The **Links** page lets you manage the learning for a selected node.*

About this task

The **Manage Learning** dialog lets you learn and delete the entire node and its individual details, such as *IP* or *MAC* address.

> **Note:**
>
> The icon adjacent to the node shows its status. When the node details are:
>
> - A green icon shows when the node details have been entirely learned
> - An orange icon shows when the node details are only partially learned
> - A red icon shows when the node details have not been learned
>
> Individual details have either a green or red icon, depending on whether they are learned or not. When you learn, or delete a node, all of its details are affected in the same way. When you learn, or delete, an individual detail, only that detail's learning status changes.

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

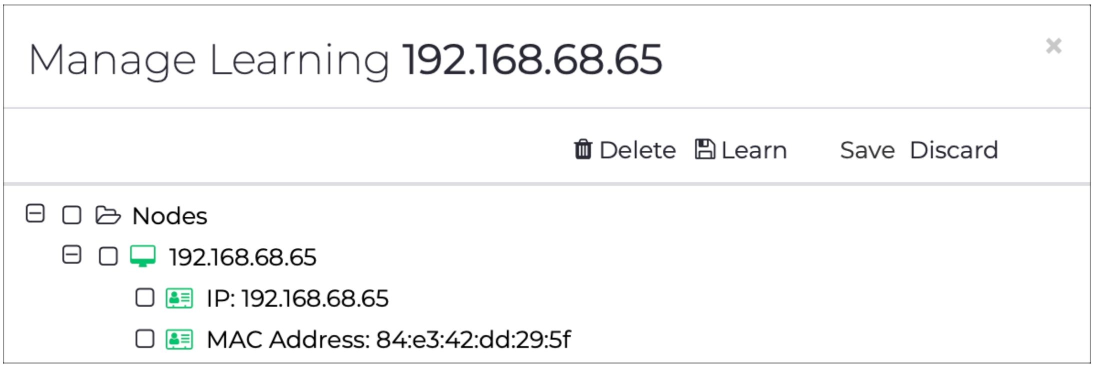
   Result: The **Links** page opens.

3. To the left of the applicable node, select the ⚙ icon.

   Result: A dialog shows.

4. **Optional:**

   If necessary, select one, or more, items and select 🗑 **Delete**.



Manage Learning **192.168.68.65**

⊟ □ Nodes

⊟ □ 192.168.68.65

□ IP: 192.168.68.65

□ MAC Address: 84:e3:42:dd:29:5f

5. **Optional:** If necessary, select one, or more, items and select **Learn**.
6. Select **Save**.

Navigate from a link

*The **Links** page lets you navigate to related entities from a selected node.*

Procedure

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

   Result: The **Network** page opens.

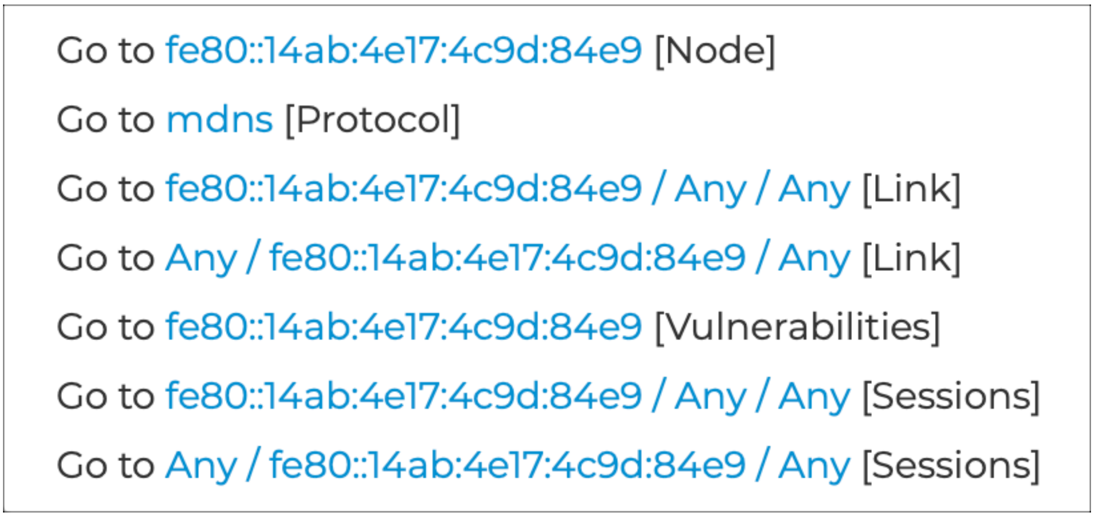
2. Select **Links**.

   Result: The **Links** page opens.

3. In the Actions column, to the left of the applicable node, select the ↪ icon.

   Result: A list of related entities shows.

4. Select the hyperlink that you want to navigate to.



Go to fe80::14ab:4e17:4c9d:84e9 [Node]

Go to mdns [Protocol]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Link]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Link]

Go to fe80::14ab:4e17:4c9d:84e9 [Vulnerabilities]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Sessions]

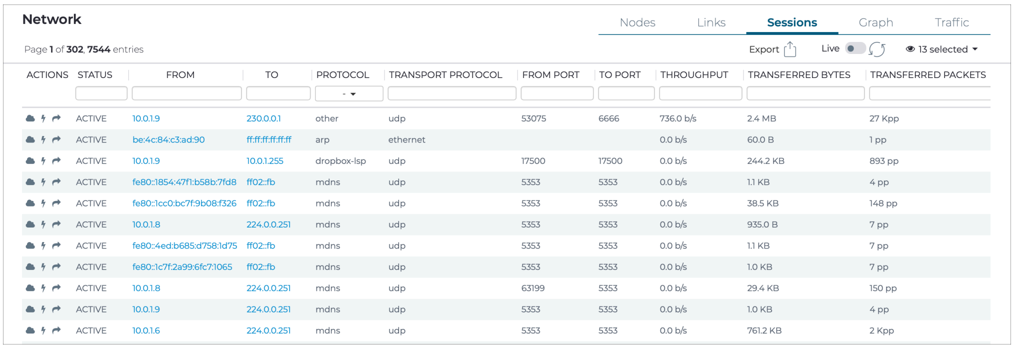
Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Sessions]

Results

The entity shows in the applicable page.

Sessions

A session is established at a certain point in time, and later turned down. An established communication session might involve more than one message in each direction.



Page **1** of **302**, **7544** entries

ACTIONS	STATUS	FROM	TO	PROTOCOL	TRANSPORT PROTOCOL	FROM PORT	TO PORT	THROUGHPUT	TRANSFERRED BYTES	TRANSFERRED PACKETS
☁ ϟ ↪	ACTIVE	10.0.1.9	230.0.0.1	other	udp	53075	6666	736.0 b/s	2.4 MB	27 Kpp
☁ ϟ ↪	ACTIVE	be:4c:84:c3:ad:90	ff:ff:ff:ff:ff:ff	arp	ethernet			0.0 b/s	60.0 B	1 pp
☁ ϟ ↪	ACTIVE	10.0.1.9	10.0.1.255	dropbox-lsp	udp	17500	17500	0.0 b/s	244.2 KB	893 pp
☁ ϟ ↪	ACTIVE	fe80::1854:47f1:b58b:7fd8	ff02::fb	mdns	udp	5353	5353	0.0 b/s	1.1 KB	4 pp
☁ ϟ ↪	ACTIVE	fe80::1cc0:bc7f:9b08:f326	ff02::fb	mdns	udp	5353	5353	0.0 b/s	38.5 KB	148 pp
☁ ϟ ↪	ACTIVE	10.0.1.8	224.0.0.251	mdns	udp	5353	5353	0.0 b/s	935.0 B	7 pp
☁ ϟ ↪	ACTIVE	fe80::4ed:b685:d758:1d75	ff02::fb	mdns	udp	5353	5353	0.0 b/s	1.1 KB	7 pp
☁ ϟ ↪	ACTIVE	fe80::1c7f:2a99:6fc7:1065	ff02::fb	mdns	udp	5353	5353	0.0 b/s	1.0 KB	7 pp
☁ ϟ ↪	ACTIVE	10.0.1.8	224.0.0.251	mdns	udp	63199	5353	0.0 b/s	29.4 KB	150 pp
☁ ϟ ↪	ACTIVE	10.0.1.9	224.0.0.251	mdns	udp	5353	5353	0.0 b/s	1.0 KB	4 pp
☁ ϟ ↪	ACTIVE	10.0.1.6	224.0.0.251	mdns	udp	5353	5353	0.0 b/s	761.2 KB	2 Kpp

Figure 45. Sessions page

Export

The **Export** ⇪ icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

The **Live** ◐ ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Show requested traces for a session

*The **Sessions** page lets you show requested traces for a selected node.*

Procedure

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

   Result: The **Network** page opens.

2. Select **Sessions**.

   Result: The **Sessions** page opens.

3. To the left of the applicable node, select the ☁ icon.

   Result: A list of all the requested traces for the session shows.

Request a trace for a session

*The **Sessions** page lets you request a trace for a selected node.*

Procedure

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

   Result: The **Network** page opens.

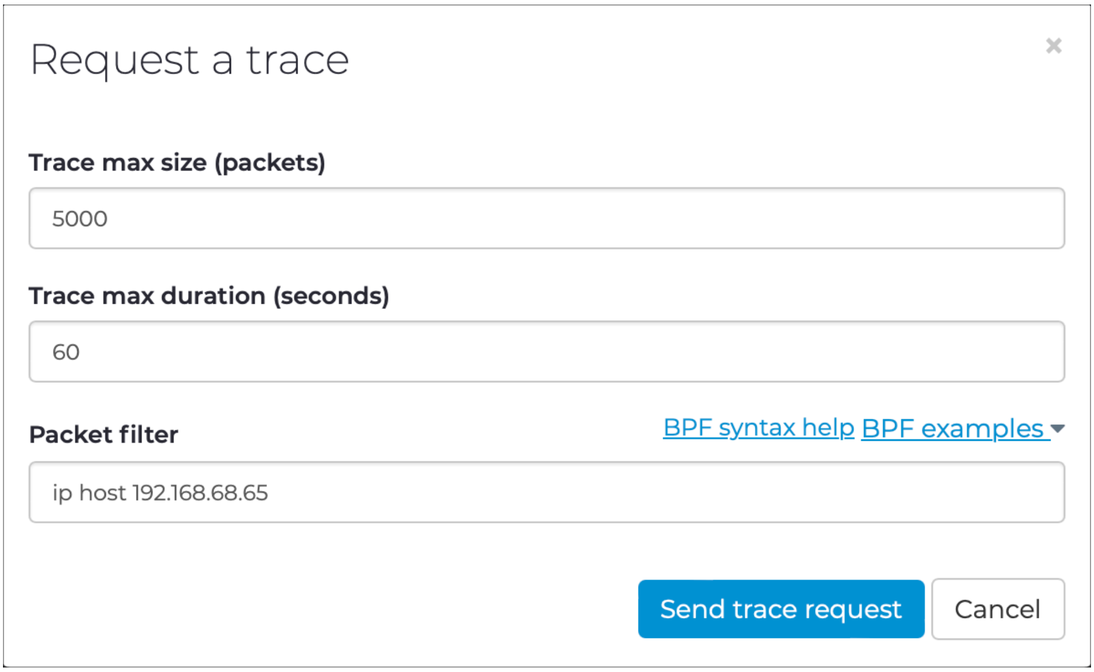
2. Select **Sessions**.

   Result: The **Sessions** page opens.

3. To the left of the applicable node, select the ⚡ icon.

   Result: A dialog shows.

4. To set the maximum packet size, in the **Trace max size (packets)** field, enter a value.



Request a trace

Trace max size (packets)

5000

Trace max duration (seconds)

60

Packet filter

ip host 192.168.68.65

> **Note:**
> The default size is 5000 packets.

5. To set the maximum duration of the trace, in the **Trace max duration (seconds)** field, enter a value.

> **Note:**
> The default value is 60 seconds.

6. **Note:**
   The **Packet filter** field is automatically populated with a *BPF* that captures the packets to/from the selected node, but you can customize this.

   If necessary, customize this field.

   Note:
   You can select **BPF syntax help** to show more information on *BPF* syntax.

   Note:
   You can select **BPF examples** to see some examples.

7. Select **Send trace request**.

Results

The trace has been requested.

Navigate from a session

*The **Sessions** page lets you navigate to related entities from a selected node.*

Procedure

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

   Result: The **Network** page opens.

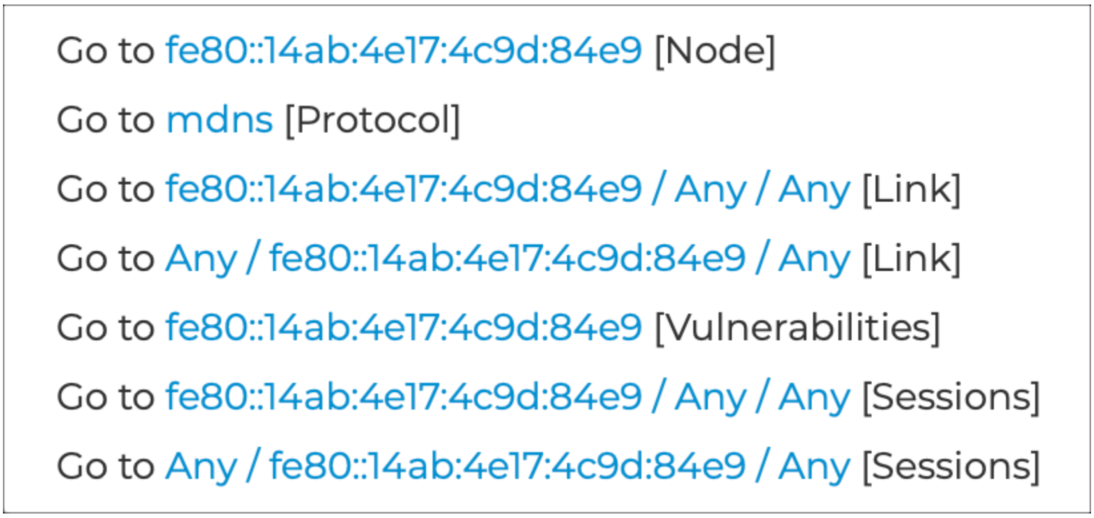
2. Select **Sessions**.

   Result: The **Sessions** page opens.

3. In the Actions column, to the left of the applicable node, select the ↪ icon.

   Result: A list of related entities shows.

4. Select the hyperlink that you want to navigate to.



Go to fe80::14ab:4e17:4c9d:84e9 [Node]

Go to mdns [Protocol]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Link]

Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Link]

Go to fe80::14ab:4e17:4c9d:84e9 [Vulnerabilities]

Go to fe80::14ab:4e17:4c9d:84e9 / Any / Any [Sessions]

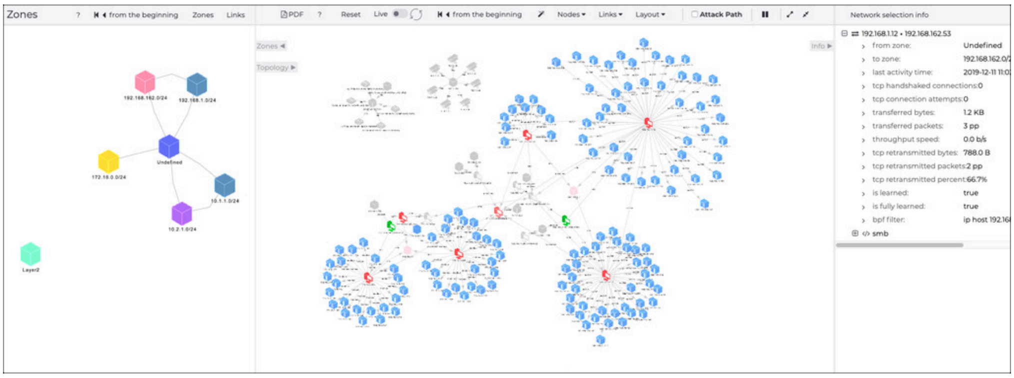
Go to Any / fe80::14ab:4e17:4c9d:84e9 / Any [Sessions]

Results

The entity shows in the applicable page.

Graph

*The **Graph** pages gives a graphical representation of the nodes in the environment.*



Network selection info

192.168.1.12 • 192.168.162.53
- from zone: Undefined
- to zone: 192.168.162.0/
- last activity time: 2019-12-11 11:0
- tcp handshaked connections:0
- tcp connection attempts:0
- transferred bytes: 1.2 KB
- transferred packets: 3 pp
- throughput speed: 0.0 b/s
- tcp retransmitted bytes: 788.0 B
- tcp retransmitted packets:2 pp
- tcp retransmitted percent:66.7%
- is learned: true
- is fully learned: true
- bpf filter: ip host 192.16

smb

Figure 46. Graph page

Each vertex represents a single network node or an ensemble of nodes, while every edge represents one or more links between nodes or node ensembles. Edges and vertices are annotated to provide node identification information, protocols used to communicate between two nodes, and more.

A specific layout format, or a dynamic automatic adjustment algorithm, control the position of the node in the graph. The algorithm ensures minimal overlap and the best readability of the items.

The graph layout menu controls the format of the data represented in the graph. From the menu, you can select the graph type and the node format in the graph.

The Graph page has these main elements:

- Zones/Topology graph (on page 156)
- Main network graph (on page 150)
- Information pane (on page 149)

Information pane

Contains additional information about the node or link selected in the network graph.

Main network graph

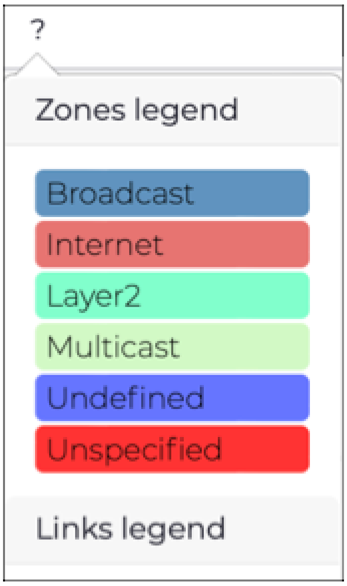
The main network graph shows a graphical representation of the nodes in your environment.

PDF

This icon lets you export a *PDF* report which contains the graph, as it is currently shown on the page.

?

This icon opens the legend for link and nodes based on the selected perspective.



?

Zones legend

Broadcast

Internet

Layer2

Multicast

Undefined

Unspecified

Links legend

Figure 47. Legend

Filters

This indicates active graph filtering, when present. Filters can be from the filter bar (see R and S below), or activated from the zone/topology graph when you select a link/node in the zone/topology graphs. Once a filter is enabled with a value, the graph is automatically updated. If more than one filter is enabled, then a logical and criteria is applied. Only nodes that satisfy all of the specified filters are shown.

> **Note:**
>
> If a node passes the filters, then all of the directly connected nodes are shown in the graph. For example if a specific *IP* filter is used, then the specified node is shown along with all the nodes connected to it.

Reset

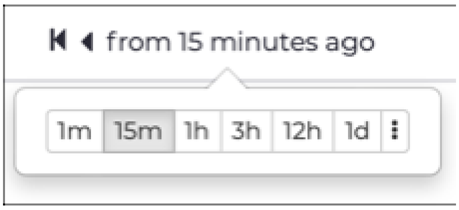
This resets customizations and reloads the data.

Live / refresh

The **Live** ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Time

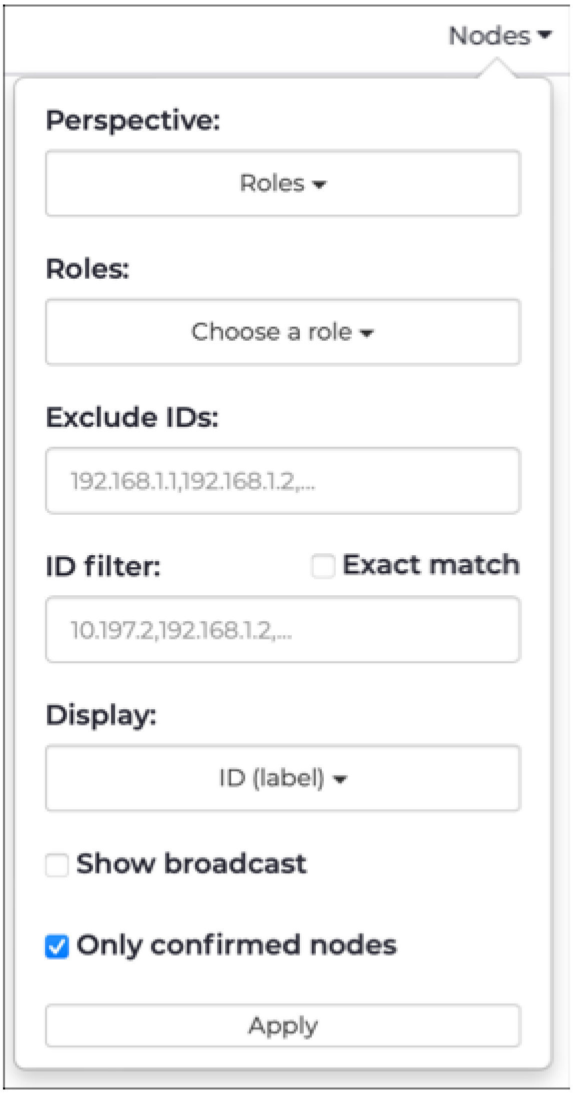
These icons let you select an activity time range.



For more details, Magic wand (on page 153).

Nodes

This dropdown lets you select node visualization configuration options.



Perspective: Roles

Roles: Choose a role

Exclude IDs: 192.168.1.1,192.168.1.2,...

ID filter: □ Exact match

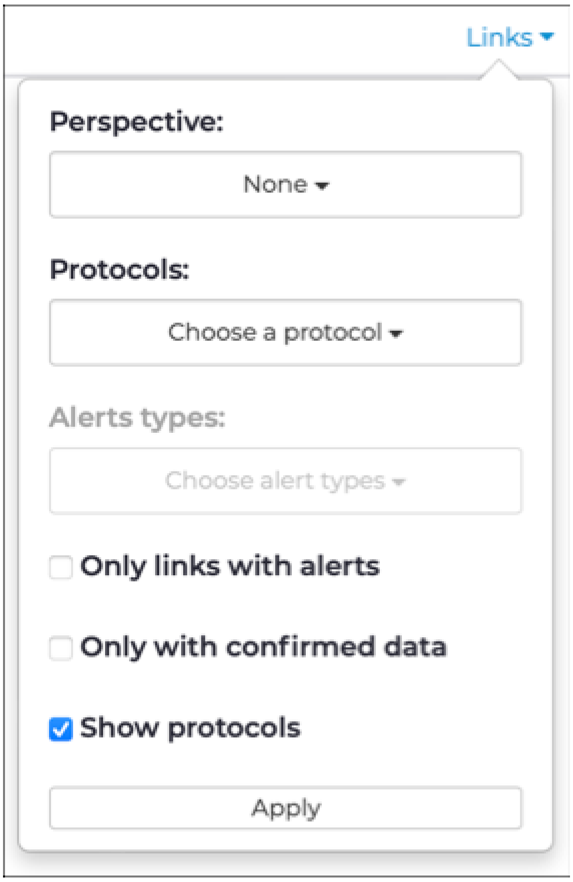
10.197.2,192.168.1.2,...

Display: ID (label)

□ Show broadcast

☑ Only confirmed nodes

Links



Perspective:

None ▾

Protocols:

Choose a protocol ▾

Alerts types:

Choose alert types ▾

□ Only links with alerts

□ Only with confirmed data

☑ Show protocols

This dropdown lets you configure visualization options.

Layout

This dropdown lets you select a layout for the graph. For more details, see Layout (on page 154).

Pause-play

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

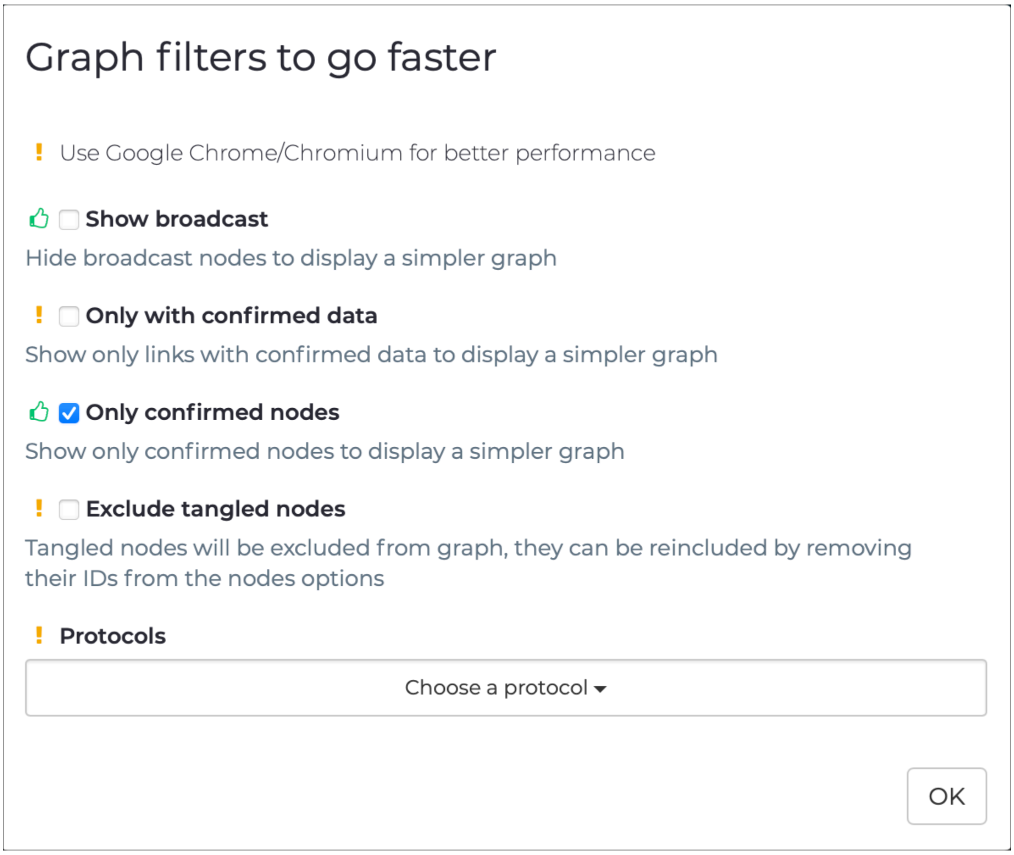
Increase-Decrease icon size

The increase ⤢ and decrease ⤡ icons lets you change the size of the icons in the graph.

Magic wand

The magic wand icon opens a wizard to help filter the graph and view only the desired information to help you reduce visualized data from large graphs.

The graph wizard gives hints to help you improve the graph performance. Settings that are annotated with an orange exclamation point are considered suboptimal. Settings annotated with green thumbs are considered helpful.



Graph filters to go faster

! Use Google Chrome/Chromium for better performance

👍 □ **Show broadcast**

Hide broadcast nodes to display a simpler graph

! □ **Only with confirmed data**

Show only links with confirmed data to display a simpler graph

👍 ☑ **Only confirmed nodes**

Show only confirmed nodes to display a simpler graph

! □ **Exclude tangled nodes**

Tangled nodes will be excluded from graph, they can be reincluded by removing their IDs from the nodes options

! **Protocols**

Figure 48. Magic wand dialog

Show broadcast

Broadcast addresses are not actual network nodes in that no asset is bound to a broadcast address. They are used to represent communications that a node uses towards an entire subnet. Removing broadcast nodes reduces the complexity of a graph.

Only with confirmed data

You can select this to hide unconfirmed links to reduce the complexity of an entangled graph.

Only confirmed nodes

You can select this to hide unconfirmed nodes to reduce the size of a large graph.

Exclude tangled nodes

To improve the readability of the graph, you can select this to exclude nodes whose connections cause the graph to be too complex.

Protocols

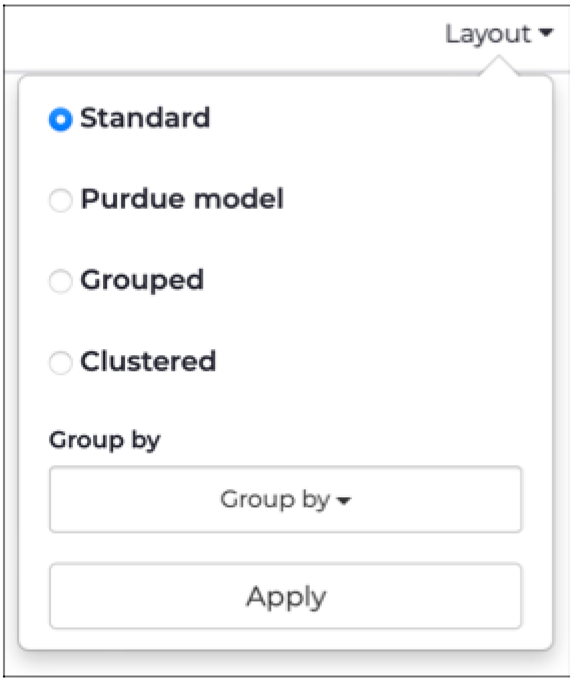
This dropdown lets you filter nodes and edges to show only those items that are communicating with the related protocol(s).

Layout

*The **Layout** dropdown lets you select a layout for the graph.*

The options are:

- Standard (on page 154)
- Purdue model (on page 154)
- Grouped (on page 155)
- Clustered (on page 155)



Layout ▾

● Standard

○ Purdue model

○ Grouped

○ Clustered

Group by: Group by ▾

Standard

This is the default layout. The type of visualization depends on the criteria defined in Group by (on page 155):

- Group by (on page 155) not defined: All of the nodes and links are shown
- Group by (on page 155) defined: Nodes that belong to the same group (based on the defined criteria) are collapsed into a single node

Purdue model

Nodes are arranged in separate rows, according to their level. You can distinguish the levels and isolate potential communication problems that cross two or more levels.

Grouped

Nodes are grouped according to the criteria defined in Group_by. The graph is visualized as follows:

- Group by (on page 155) not defined: All nodes and links are shown.
- Group by (on page 155) defined: Nodes that belong to the same group are shown and are placed inside a circle that represents the group. Links between nodes within the same group are shown. However, links between groups are replaced with lines that connect the circles

Clustered

Nodes are clustered according to the criteria below. Once nodes are clustered, a single circle represents the node cluster. Upon zoom-in, the circle expands and the internal nodes display. A cluster may contain multiple subclusters. This layout is useful when visualizing large graphs because it provides an overview of the graph, along with sufficient details.

Nodes are clustered depending on the values defined by Group_by:

- Group by (on page 155) not defined: Nodes are clustered based on connections. Nodes with a large number of links act as a cluster center with neighboring nodes assigned to the same cluster
- Group by (on page 155) defined: At the highest level, a cluster is created for each group. Inside each high level cluster are subclusters created around nodes with a high number of links. For example, if Group_by=Zones, then a cluster is created for each zone, and inside each zone other subclusters may be created around nodes with a high number of links

Group by

This dropdown lets you define the group used for Standard, Grouped, and Clustered layouts. Nodes with the chosen property, such as zone or subnet, are assigned to the same group. The group displays depending on the selected layout.

The **Group by** dropdown lets you select from:

- Asset
- Cluster
- Level
- Roles
- Subnet
- Type
- Zone
- Site
- Host

Zones/Topology graph

The Zones/Topology graph shows a visualization of the network topology or zones.

General

You can see a visualization of either the zones or the topology, but not both at the same time. You can control these views with the two toggle buttons.

Inside the Zones graph, each node represents a zone and each link represents all of the links between the nodes in the connected zones. When you select a zone, the information pane is populated with all of the nodes/links that are related to the selected zone. The main network graph is filtered to show only the nodes and the links for that zone, and the filtering icon shows.

In a similar way, when a link is selected in the **Zones** graph, the information pane is populated with all of the links between the two zones, and the Networks graph shows only the nodes and links that belong to one of the two connected zones. When you click in a region of the **Zones** graph that has no nodes or links, the visualization in the main networks graph is reset to show all the nodes and links.

Zones legend

The **?** icon opens the legend for link and nodes based on the selected perspective.

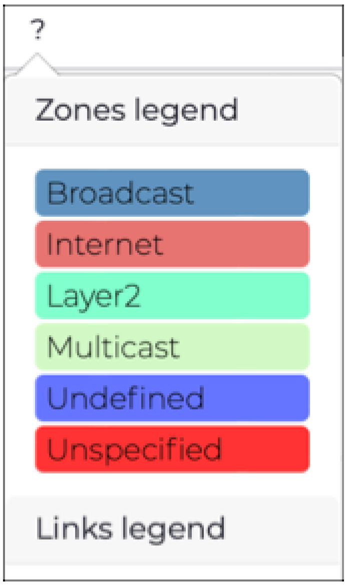
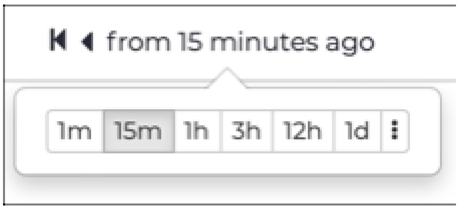


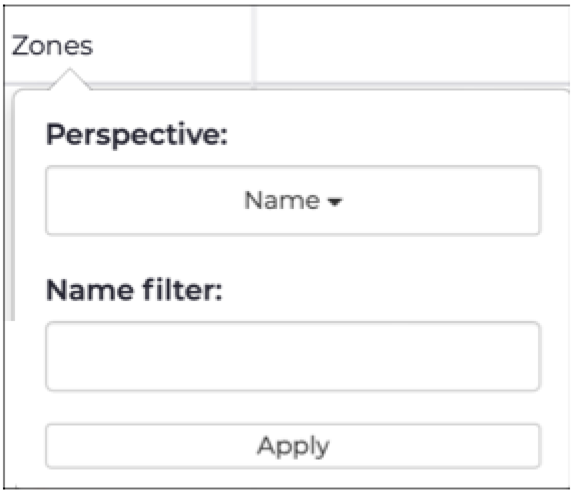
Figure 49. Legend

Time

These icons let you select an activity time range.



Zones



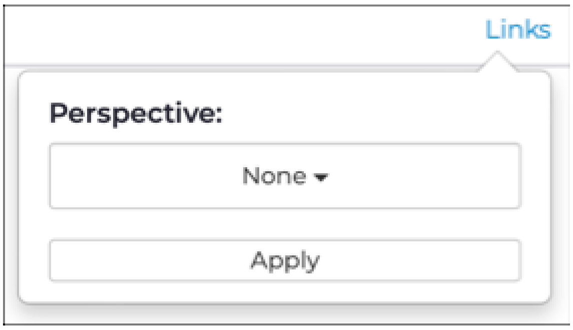
Zones

Perspective:

Name ▾

Name filter:

Links



Links

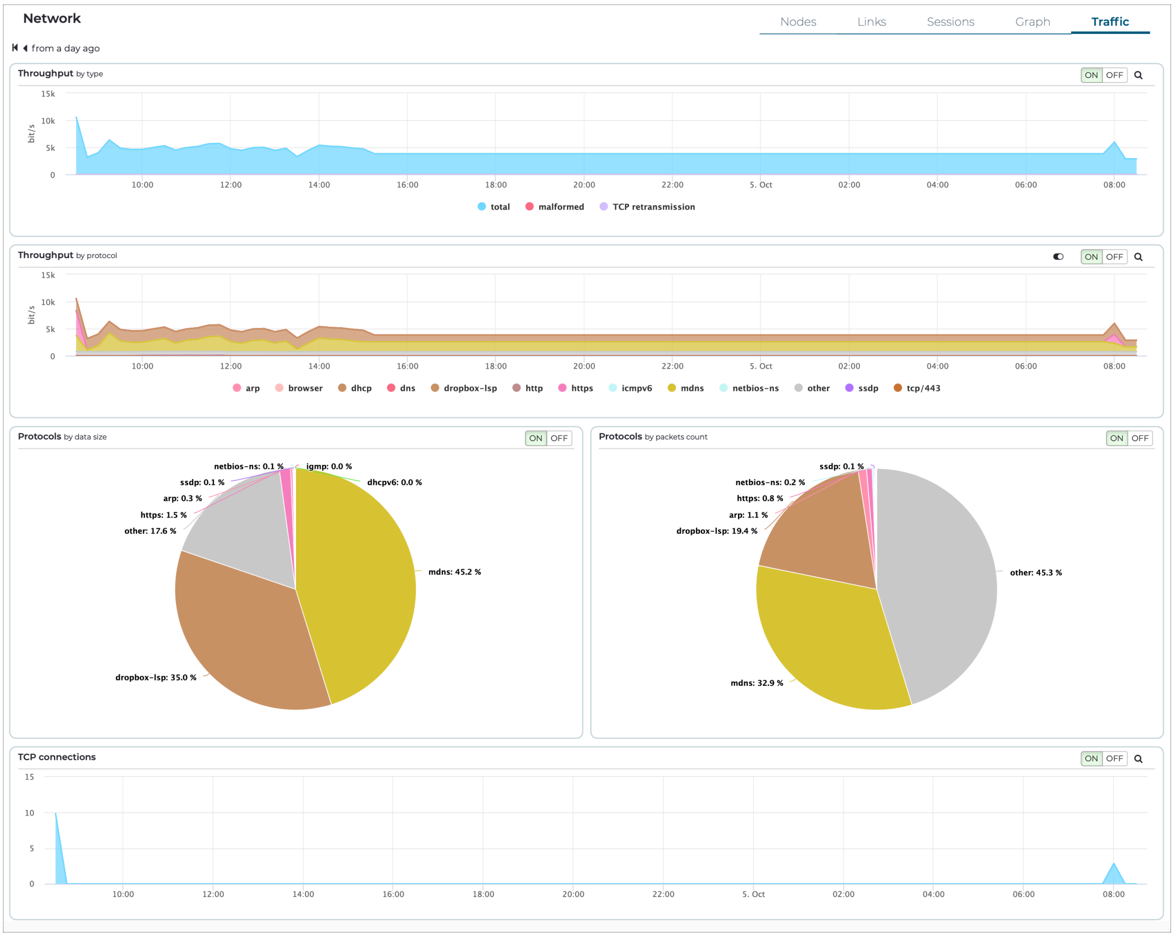
Perspective:

None ▾

This dropdown lets you configure visualization options.

Traffic

*The **Traffic** page shows charts with information about throughput, protocols, and open transmission control protocol (TCP) connections.*



Throughput by type

This section shows traffic by macro category.

Throughput by protocol

This section shows traffic by protocol.

Protocols by data size

This section shows the proportion of packets sent by protocol, in pie chart format.

Protocols by packets count

This section shows the proportion of traffic generated by protocol, in pie chart format.

TCP connections

This section shows the number of open TCP connections.

Graph controls

A list of the different control options in the graph view.

Move	Click and drag anywhere in the graph other than on a node.
Zoom (mode 1)	With the cursor positioned inside the graph window, scroll the mouse forward or backward. Zoom is centered on the mouse position.
Zoom (mode 2)	With the cursor positioned inside the graph window, press Z on the keyboard and move the mouse up or down. Zoom is centered on the mouse position.
Increase icon and text size.	Select the ⤢ icon.
Decrease icon and text size.	Select the ↗↙ icon.
View detailed information for a node or link in the information pane.	Select a node or link with a single click
Show a new window with additional information for a node	Select a node with a double click
Show a node or link	Move your mouse over the node or link
Show a node or link, and the elements directly connected to it	Click and hold your mouse button on a node or link without releasing it

Chapter 9. Process

Process

Process is a set of repeatable functions that a business does to deliver a core value.

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.

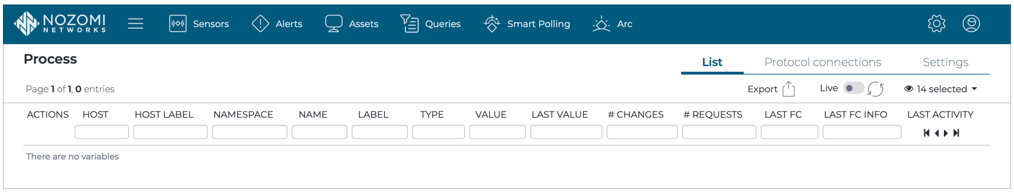
Individual values within operational devices are represented as variables, and Guardian tracks them over time in **Process**.

The **Process** page has these tabs:

- List (on page 164)
- Protocol connections (on page 165)
- Settings (on page 166)

List

*The **List** page shows detailed information about variables in your environment.*



Process

Page 1 of 1, 0 entries

ACTIONS	HOST	HOST LABEL	NAMESPACE	NAME	LABEL	TYPE	VALUE	LAST VALUE	# CHANGES	# REQUESTS	LAST FC	LAST FC INFO	LAST ACTIVITY

There are no variables

Figure 50. List page

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Live / refresh

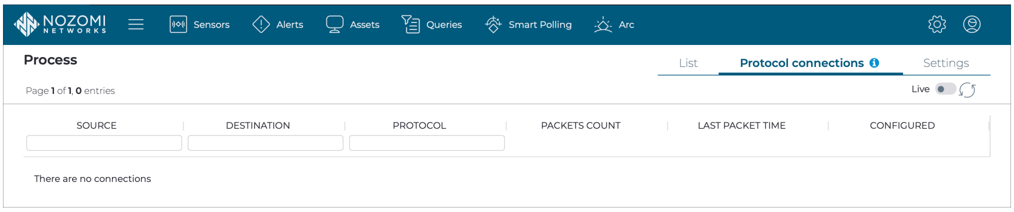
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Protocol connections

The ***Protocol connections*** *page lets you configure the additional parameters necessary to extract information contained inside certain protocols.*



Process

List | Protocol connections | Settings

Page 1 of 1, 0 entries

Live

SOURCE	DESTINATION	PROTOCOL	PACKETS COUNT	LAST PACKET TIME	CONFIGURED

There are no connections

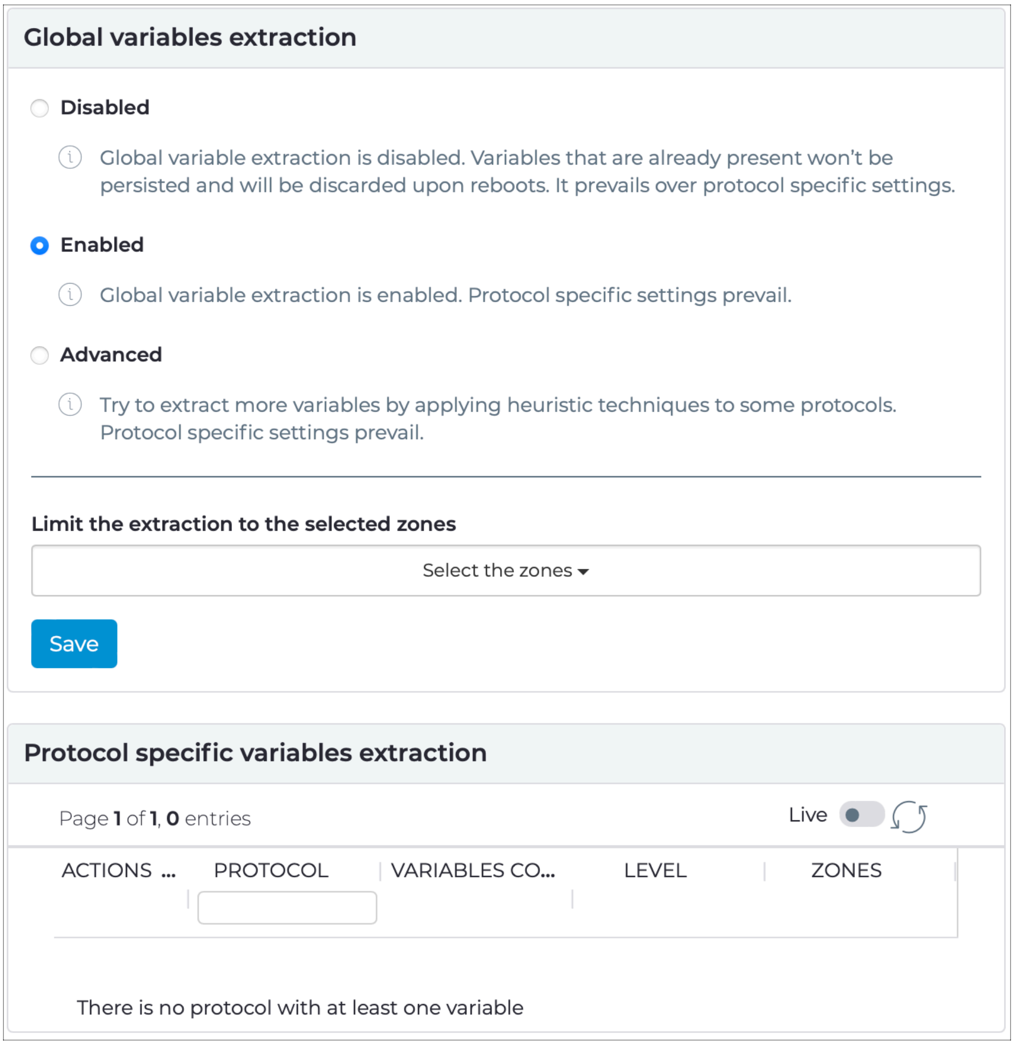
Figure 51. Protocol connections page

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Settings

*The **Settings** page lets you configure which strategy to use to extract variables inside the process that are being communicated over different protocols.*



Global variables extraction

○ Disabled

Global variable extraction is disabled. Variables that are already present won't be persisted and will be discarded upon reboots. It prevails over protocol specific settings.

● Enabled

Global variable extraction is enabled. Protocol specific settings prevail.

○ Advanced

Try to extract more variables by applying heuristic techniques to some protocols. Protocol specific settings prevail.

Limit the extraction to the selected zones

Select the zones

Save

Protocol specific variables extraction

Page **1** of **1**, **0** entries

Live

ACTIONS ...	PROTOCOL	VARIABLES CO...	LEVEL	ZONES

There is no protocol with at least one variable

Figure 52. Process variable extraction tuning

Disabled

This checkbox lets you disable global variables extraction.

Enabled

This checkbox lets you enable global variables extraction.

Advanced

This checkbox lets you try to apply heuristic techniques to some protocols to extract more variables. Protocol specific settings prevail.

Limit the extraction to the selected zones

This dropdown lets you Limit the extraction to the selected zones.

Configure a variable

*The **List** page lets you navigate to related nodes, links, vulnerabilities, or sessions.*

Procedure

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

   Result: The **Process** page opens.

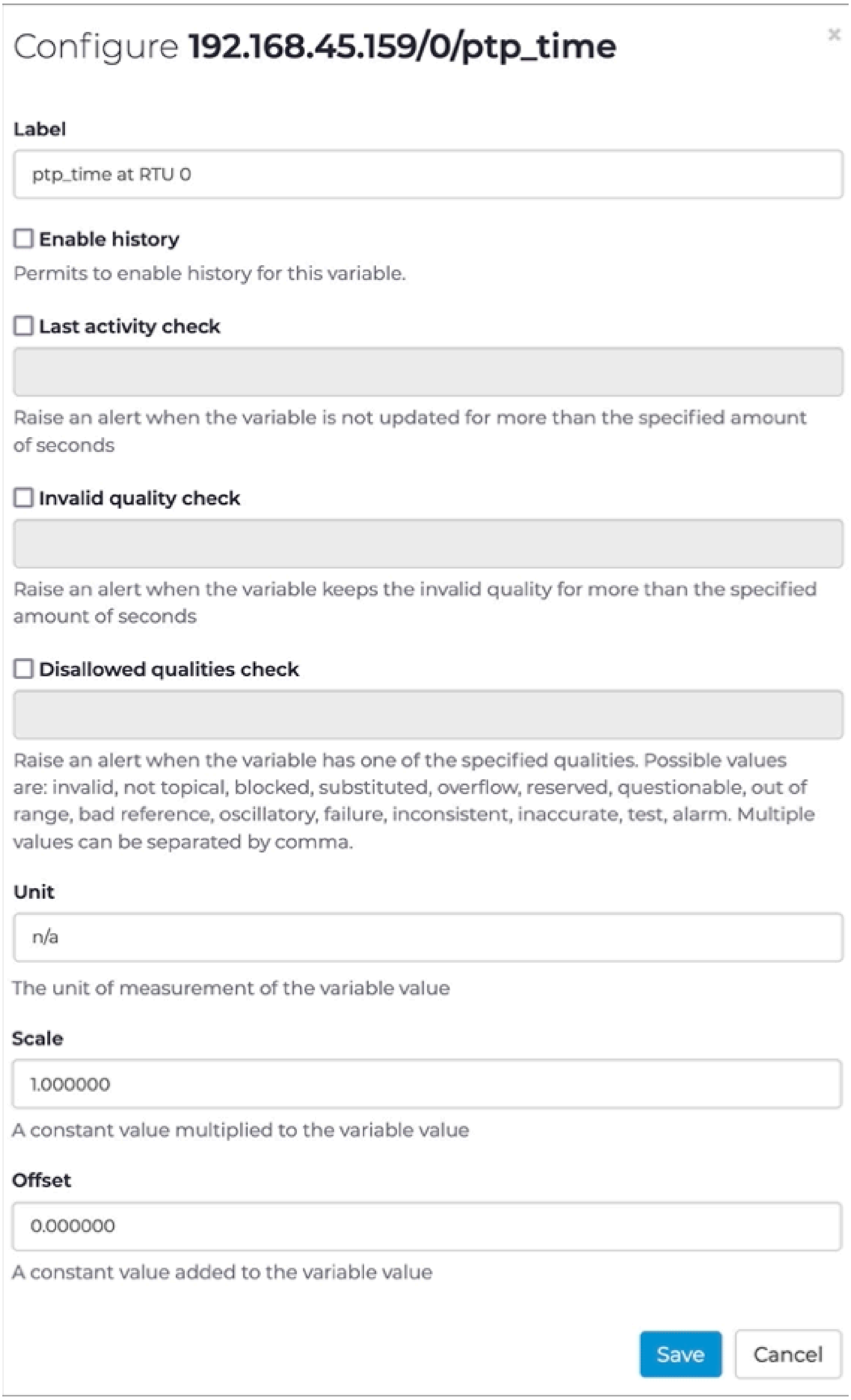
2. Select **List**.

   Result: The **List** page opens.

3. To the left of the applicable *variable*, select the configure ☰ icon.

   Result: A dialog shows.

4. In the **Label** field, enter a label for the *Variable*.



Configure **192.168.45.159/0/ptp_time**

Label

ptp_time at RTU 0

☐ **Enable history**

Permits to enable history for this variable.

☐ **Last activity check**

Raise an alert when the variable is not updated for more than the specified amount of seconds

☐ **Invalid quality check**

Raise an alert when the variable keeps the invalid quality for more than the specified amount of seconds

☐ **Disallowed qualities check**

Raise an alert when the variable has one of the specified qualities. Possible values are: invalid, not topical, blocked, substituted, overflow, reserved, questionable, out of range, bad reference, oscillatory, failure, inconsistent, inaccurate, test, alarm. Multiple values can be separated by comma.

Unit

n/a

The unit of measurement of the variable value

Scale

1.000000

A constant value multiplied to the variable value

Offset

0.000000

A constant value added to the variable value

5. **Optional:** If necessary, select the **Enable history**.

   > **Note:**
   > This lets you enable *Variable* history.

6. **Optional:** If necessary, select the **Last activity check**.

   > **Note:**
   > This triggers an alert when the *Variable* is not updated for more than the specified amount of seconds.

7. **Optional:** If necessary, select the **Invalid quality check**.

   > **Note:**
   > This triggers an alert when the *Variable* keeps the invalid quality for more than the specified amount of seconds.

8. **Optional:** If necessary, select the **Disallowed qualities check**.

   > **Note:**
   > This triggers an alert when the *Variable* has one of the listed qualities. You can use a comma to separate values.

9. In the **Unit** field, enter a value.
10. In the **Scale** field, enter a value.
11. In the **Offset** field, enter a value.

Results

The *Variable* has been configured.

View the details of a variable

*The **List** page lets you view the details of a variable.*

Procedure

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

   Result: The **Process** page opens.

2. Select **List**.

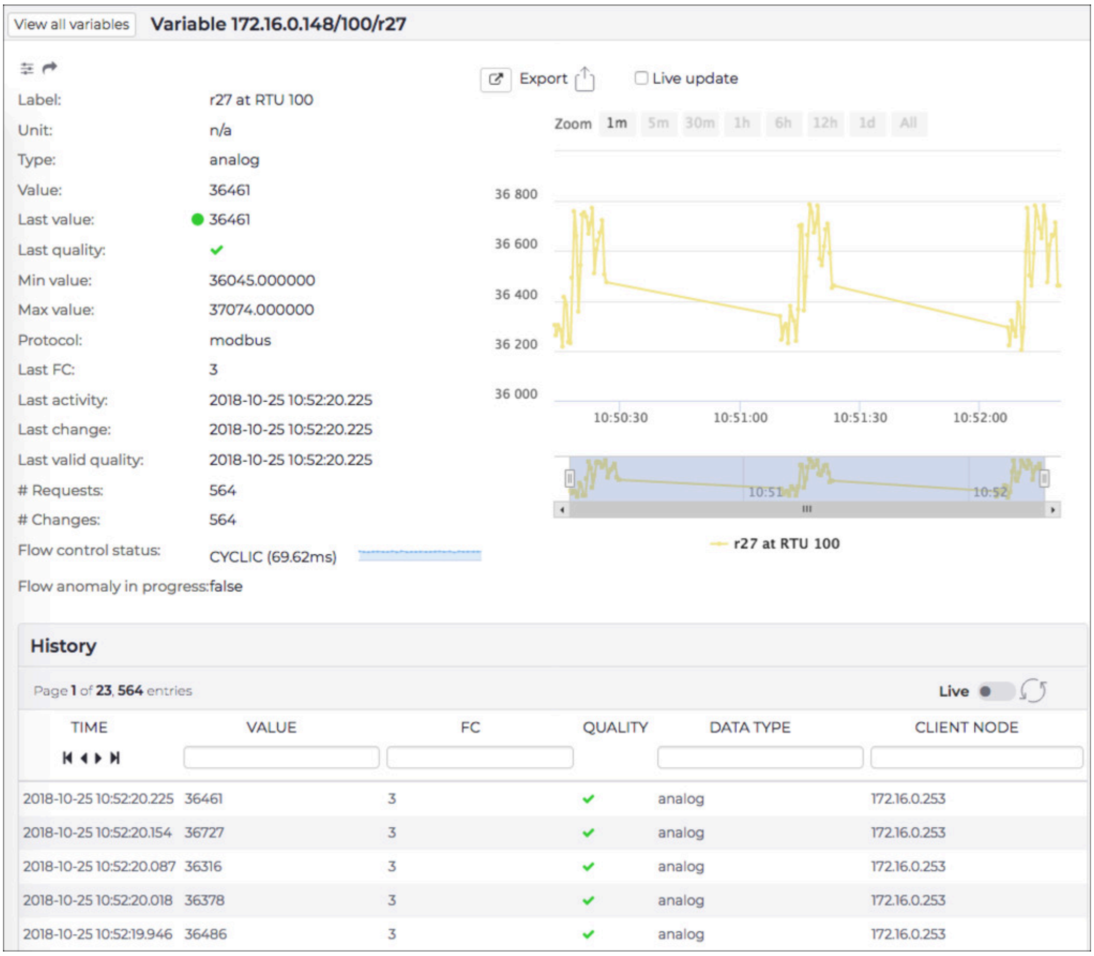
   Result: The **List** page opens.

3. To the left of the applicable *Variable*, select the search 🔍 icon.

   Result: The Variables details window opens.

4. **Optional:**

   To open the chart in another window, select the ↗ icon.



Variable 172.16.0.148/100/r27

Label: r27 at RTU 100
Unit: n/a
Type: analog
Value: 36461
Last value: ● 36461
Last quality: ✓
Min value: 36045.000000
Max value: 37074.000000
Protocol: modbus
Last FC: 3
Last activity: 2018-10-25 10:52:20.225
Last change: 2018-10-25 10:52:20.225
Last valid quality: 2018-10-25 10:52:20.225
Requests: 564
Changes: 564
Flow control status: CYCLIC (69.62ms)
Flow anomaly in progress:false

History

Page **1** of **23**, **564** entries

TIME	VALUE	FC	QUALITY	DATA TYPE	CLIENT NODE
2018-10-25 10:52:20.225	36461	3	✓	analog	172.16.0.253
2018-10-25 10:52:20.154	36727	3	✓	analog	172.16.0.253
2018-10-25 10:52:20.087	36316	3	✓	analog	172.16.0.253
2018-10-25 10:52:20.018	36378	3	✓	analog	172.16.0.253
2018-10-25 10:52:19.946	36486	3	✓	analog	172.16.0.253

5. **Optional:** To export the results, select **Export**

6. **Optional:** To update the chart to real-time, select **Live update**.

Favorite a variable

*The **List** page lets you add a Variable to the favorite variables.*

Procedure

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

   Result: The **Process** page opens.

2. Select **List**.

   Result: The **List** page opens.

3. To the left of the applicable *Variable*, select the search ★ icon.

   Result: The *Variable* is added to the Favorite variables list.

Navigate from a variable

*The **List** page lets you navigate to related nodes, links, vulnerabilities, or sessions.*

Procedure

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

   Result: The **Process** page opens.

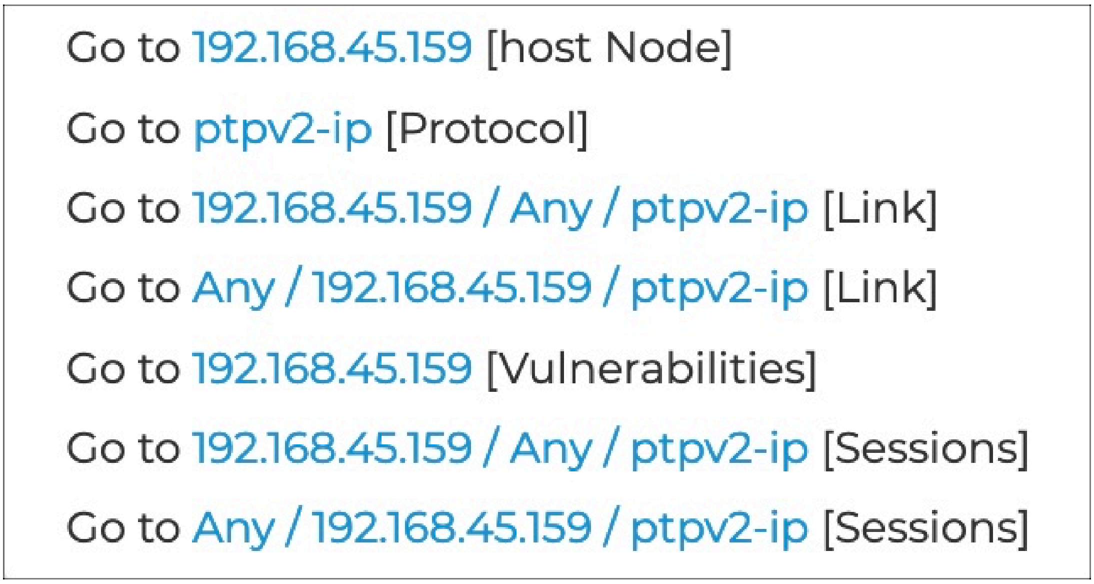
2. Select **List**.

   Result: The **List** page opens.

3. To the left of the applicable variable, select the navigate ↪ icon.

   Result: A dialog shows.

4. Select the desired link.



Go to 192.168.45.159 [host Node]

Go to ptpv2-ip [Protocol]

Go to 192.168.45.159 / Any / ptpv2-ip [Link]

Go to Any / 192.168.45.159 / ptpv2-ip [Link]

Go to 192.168.45.159 [Vulnerabilities]

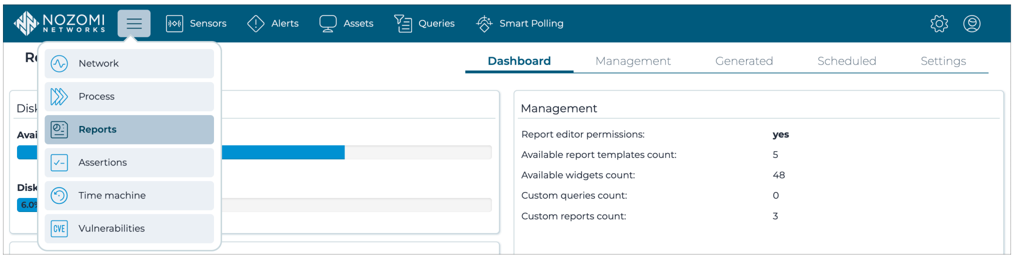
Go to 192.168.45.159 / Any / ptpv2-ip [Sessions]

Go to Any / 192.168.45.159 / ptpv2-ip [Sessions]

Chapter 10. Reports

Reports

*The **Reports** page lets you manage, generate, schedule and view reports.*



Management

Report editor permissions: **yes**
Available report templates count: 5
Available widgets count: 48
Custom queries count: 0
Custom reports count: 3

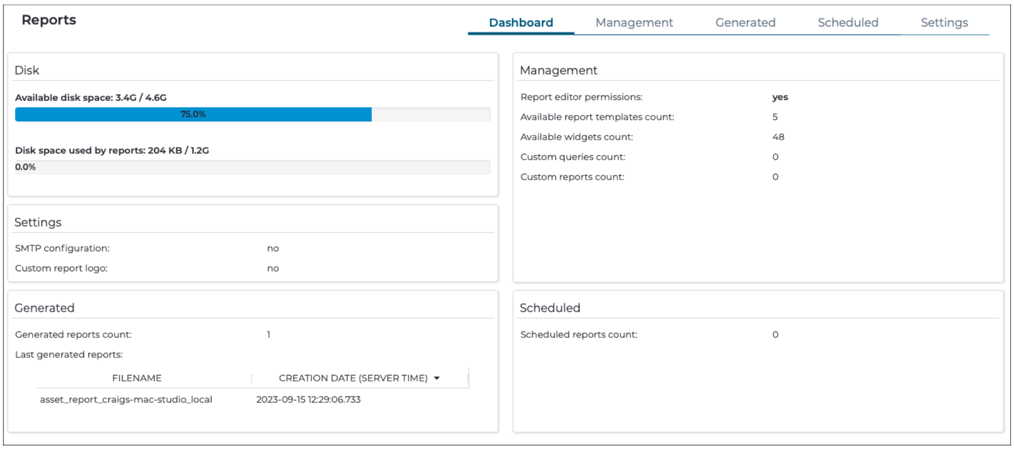
Figure 53. Reports page

The **Reports** page has these tabs:

- Dashboard (on page 176)
- Management (on page 177)
- Generated (on page 180)
- Scheduled (on page 181)
- Settings (on page 182)

Dashboard

The Dashboard page shows an overview of information related to reports, which includes disk availability, report settings, generated reports, report management, and scheduled reports.



Disk

Available disk space: 3.4G / 4.6G

75.0%

Disk space used by reports: 204 KB / 1.2G

0.0%

Settings

SMTP configuration:	no
Custom report logo:	no

Generated

Generated reports count:	1
Last generated reports:	

FILENAME	CREATION DATE (SERVER TIME) ▾
asset_report_craigs-mac-studio_local	2023-09-15 12:29:06.733

Management

Report editor permissions:	**yes**
Available report templates count:	5
Available widgets count:	48
Custom queries count:	0
Custom reports count:	0

Scheduled

Scheduled reports count:	0

Figure 54. Dashboard page

Disk

This section shows:

- Available disk space
- Disk space used by reports

Management

This section shows a summary of information from the Management (on page 177) page.

Settings

This section shows a summary of information from the Settings (on page 182) page.

Generated

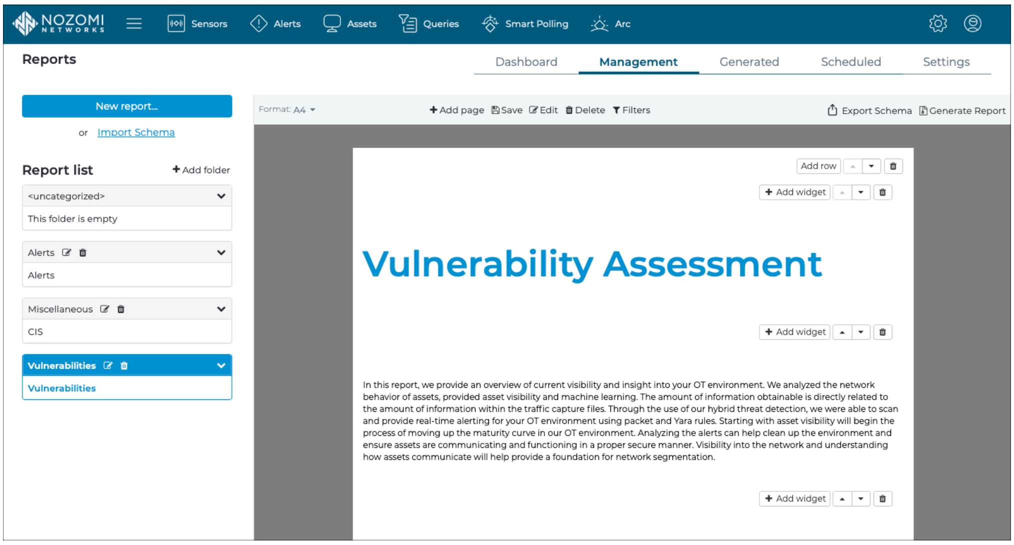
This section shows a summary of information from the Generated (on page 180) page.

Scheduled

This section shows a summary of information from the Scheduled (on page 181) page.

Management

*The **Management** page lets you manage all your reports.*



Vulnerability Assessment

In this report, we provide an overview of current visibility and insight into your OT environment. We analyzed the network behavior of assets, provided asset visibility and machine learning. The amount of information obtainable is directly related to the amount of information within the traffic capture files. Through the use of our hybrid threat detection, we were able to scan and provide real-time alerting for your OT environment using packet and Yara rules. Starting with asset visibility will begin the process of moving up the maturity curve in our OT environment. Analyzing the alerts can help clean up the environment and ensure assets are communicating and functioning in a proper secure manner. Visibility into the network and understanding how assets communicate will help provide a foundation for network segmentation.

Figure 55. Management page

New report

This button lets you Create a report (on page 183).

Import schema

This button lets you Import a schema (on page 190).

Report list

This section shows a list of created and saved reports. You can add folders (on page 188) to group the reports in.

Add page

This button lets you add a page to the bottom of the current report.

Save

This button lets you save the changes to the current report.

Edit

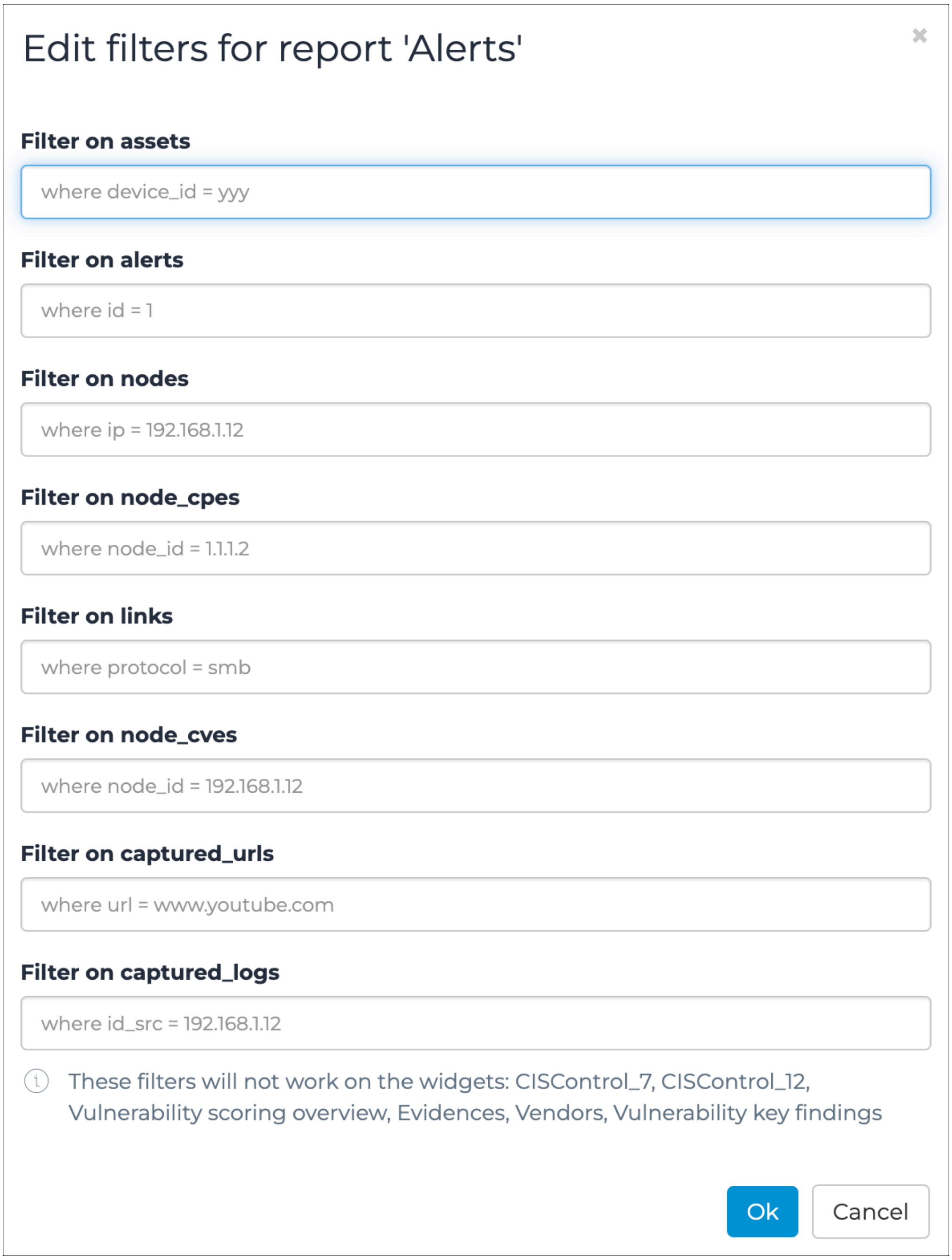
This button lets you edit the current report.

Delete

This button lets you delete the current report.

Filters

This button lets you filter the contents of the current report.



Edit filters for report 'Alerts'

Filter on assets

where device_id = yyy

Filter on alerts

where id = 1

Filter on nodes

where ip = 192.168.1.12

Filter on node_cpes

where node_id = 1.1.1.2

Filter on links

where protocol = smb

Filter on node_cves

where node_id = 192.168.1.12

Filter on captured_urls

where url = www.youtube.com

Filter on captured_logs

where id_src = 192.168.1.12

These filters will not work on the widgets: CISControl_7, CISControl_12, Vulnerability scoring overview, Evidences, Vendors, Vulnerability key findings

Figure 56. Filter dialog

Export schema

This button lets you export a schema (on page 191) for the current report in *JavaScript Object Notation (JSON)* format.

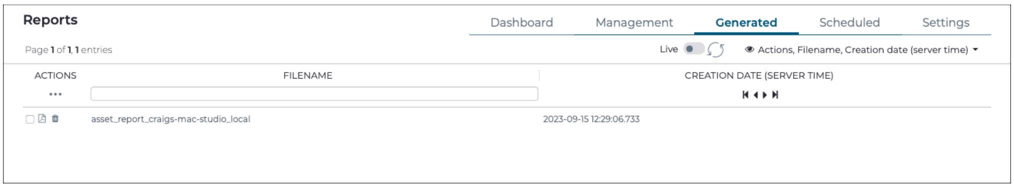
Generate report

The generate report icon lets you generate a report (on page 185) in one of these formats:

- *PDF*
- *CSV*
- Microsoft Excel

Generated

*The **Generated** page lets you view, download, edit, and delete generated reports.*



Page 1 of 1, 1 entries

ACTIONS	FILENAME	CREATION DATE (SERVER TIME)
☐	asset_report_craigs-mac-studio_local	2023-09-15 12:29:06.733

Figure 57. Generated page

Live / refresh

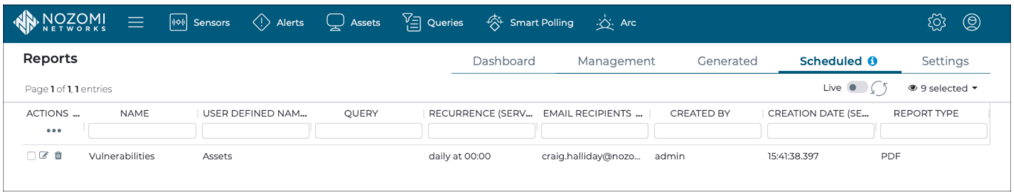
The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Scheduled

*The **Scheduled** page lets you view, download, edit, and delete scheduled reports.*



Page 1 of 1, 1 entries

ACTIONS ...	NAME	USER DEFINED NAM...	QUERY	RECURRENCE (SERV...	EMAIL RECIPIENTS ...	CREATED BY	CREATION DATE (SE...	REPORT TYPE
□	Vulnerabilities	Assets		daily at 00:00	craig.halliday@nozo...	admin	15:41:38.397	PDF

Figure 58. Scheduled page

Live / refresh

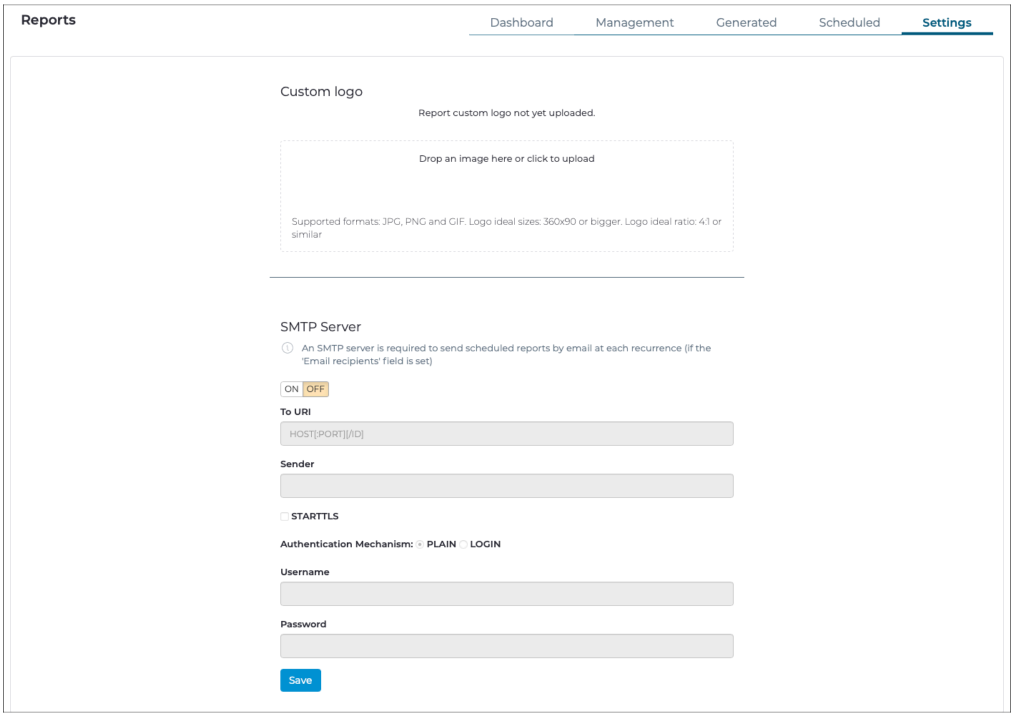
The **Live** ● ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection 👁 icon lets you choose which columns to show or hide.

Settings

*The **Settings** page lets you change report settings, upload custom logos, and configure simple mail transfer protocol (SMTP) settings.*



Custom logo

Report custom logo not yet uploaded.

Drop an image here or click to upload

Supported formats: JPG, PNG and GIF. Logo ideal sizes: 360x90 or bigger. Logo ideal ratio: 4:1 or similar

SMTP Server

ⓘ An SMTP server is required to send scheduled reports by email at each recurrence (if the 'Email recipients' field is set)

ON [✓ OFF]

To URI

HOST[:PORT][/ID]

Sender

□ **STARTTLS**

Authentication Mechanism: ● **PLAIN** ○ **LOGIN**

Username

Password

Figure 59. Settings page

Custom logo

This section lets you upload a custom logo (on page 192) that will show in your reports.

SMTP server

If you want to send emails that contain scheduled reports, you need to configure (on page 194) the *simple mail transfer protocol (SMTP)* server settings.

Create a report

*The **Management** page lets you create a new report.*

Procedure

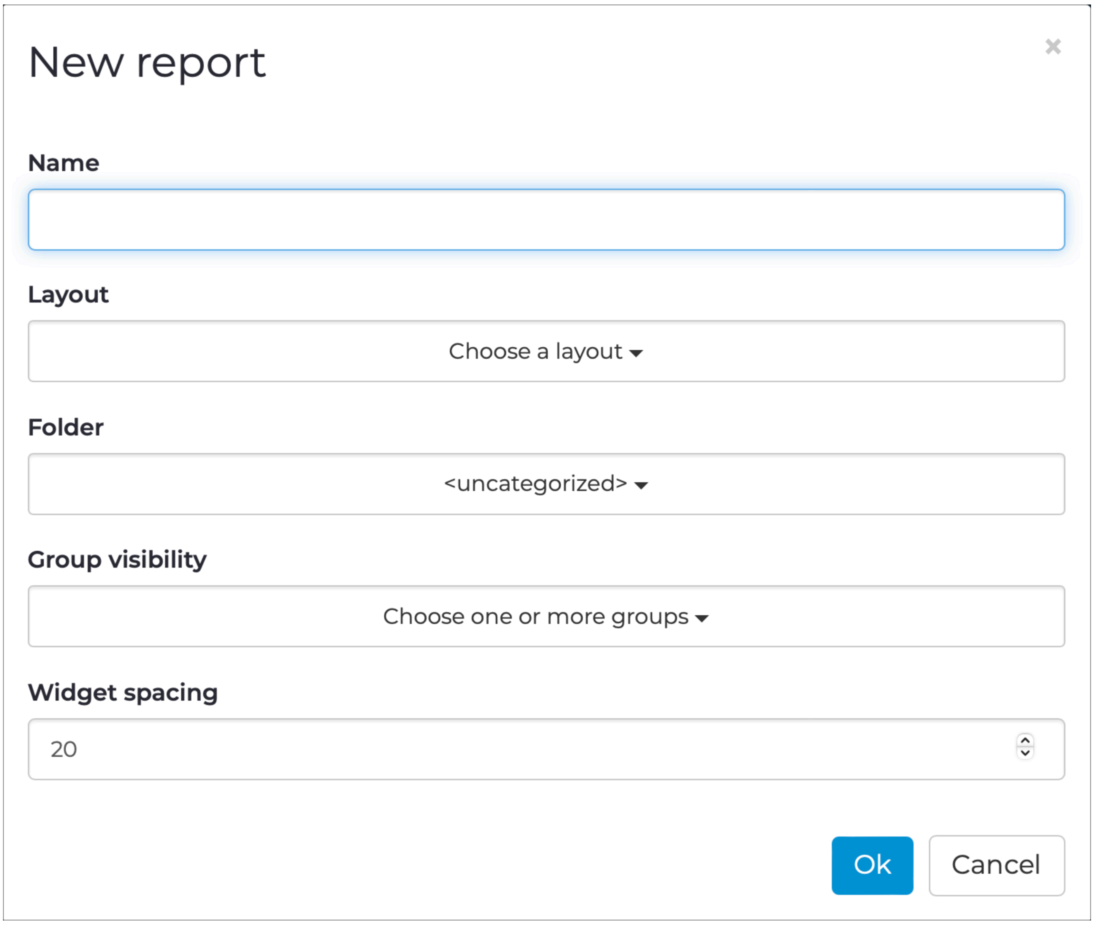
1. In the top navigation bar, select ≡ **icon** > **Reports**.

   Result: The **Reports** page opens.

2. Select **Management**.
3. In the section on the left, select **New report**.

   Result: A dialog shows.

4. In the **Name** field, enter a name for the report.



New report ×

Name

Layout

Choose a layout ▾

Folder

<uncategorized> ▾

Group visibility

Choose one or more groups ▾

Widget spacing

20

Ok Cancel

5. From the **Layout** dropdown, select a layout for the report.
6. From the **Folder** dropdown, select a folder for the report.
7. From the **Group visibility** dropdown, select the group(s) that will be able to view the report.
8. From the **Widget spacing** dropdown, enter a value.
9. Select **Ok**.

Results

The report has been created.

Generate a report

You can generate both scheduled, or on-demand, reports, in multiple file formats.

Procedure

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

   Result: The **Reports** page opens.

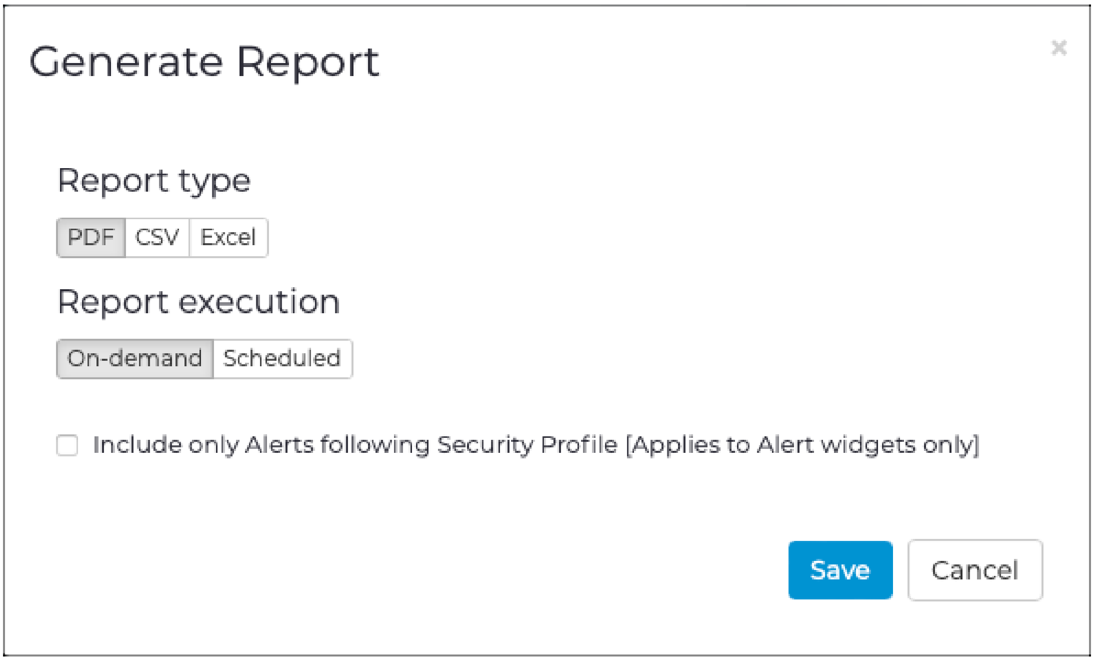
2. Select **Management**.
3. In the section on the left, select the report that you want to generate.
4. In the top right, select **Generate Report**.

   Result: A dialog shows.

5. In the **Report type** section, choose a format for the report:

   Choose from:

   - *PDF*
   - *CSV*
   - Excel



Generate Report

Report type

PDF | CSV | Excel

Report execution

On-demand | Scheduled

□ Include only Alerts following Security Profile [Applies to Alert widgets only]

6. In the **Report execution** section, choose the type of execution:

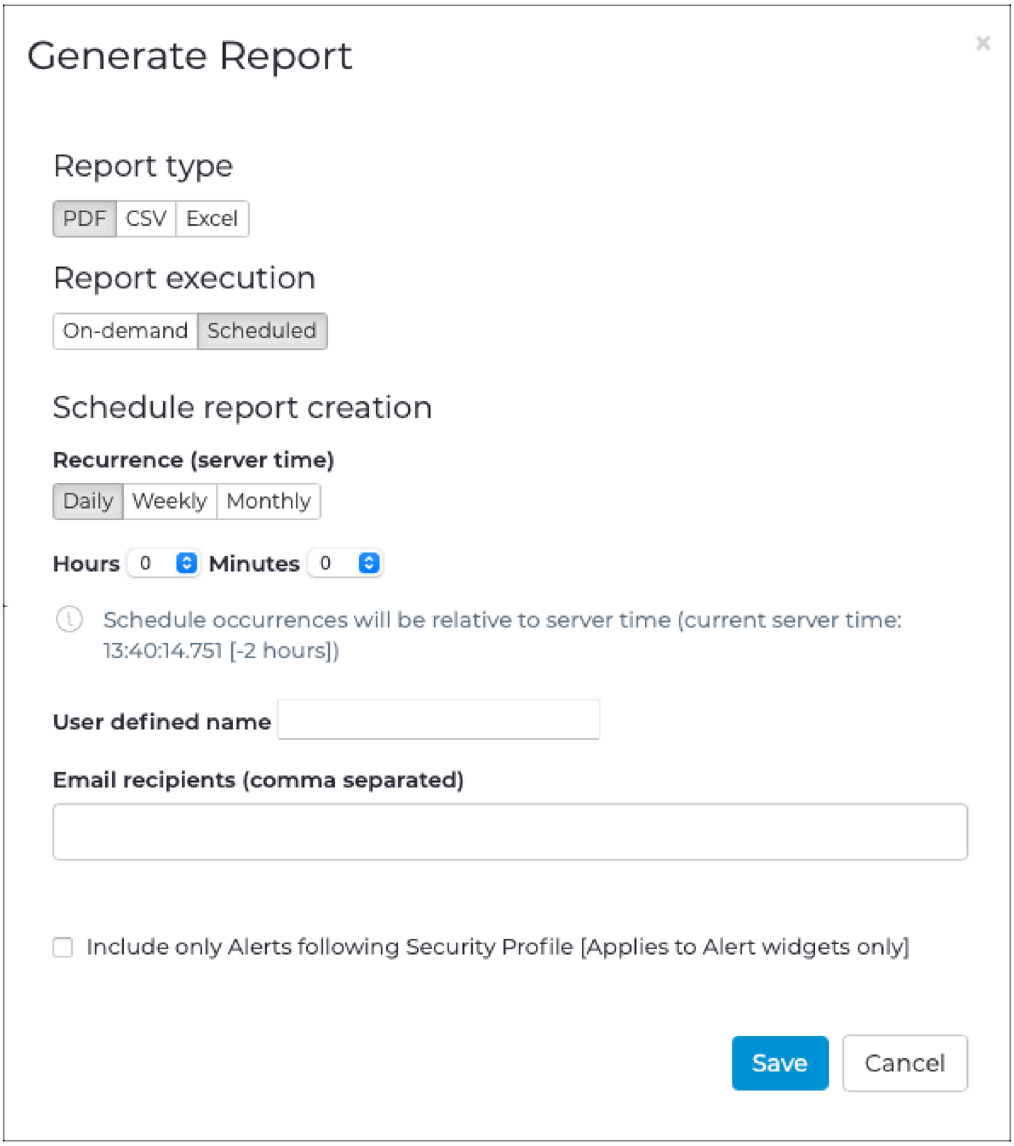
   Choose from:

   - On-demand
   - Scheduled

7. If you chose **On-demand**, select **Save**.

   Result: The report starts to generate. When the generation is complete, the report will show in the Generated (on page 180) page.

8. If you chose **Scheduled**, do the steps below.
   a. In the **Recurrence (server time)** section, enter the settings that you want.



Generate Report

Report type

PDF | CSV | Excel

Report execution

On-demand | Scheduled

Schedule report creation

Recurrence (server time)

Daily | Weekly | Monthly

Hours 0 **Minutes** 0

Schedule occurrences will be relative to server time (current server time: 13:40:14.751 [-2 hours])

User defined name

Email recipients (comma separated)

□ Include only Alerts following Security Profile [Applies to Alert widgets only]

   b. **Optional:** In the **User defined name** field, enter a name for the report.

   c. **Optional:** In the **Email recipients (comma separated)** field, enter the email addresses of the people that you would like to receive the reports.

   d. **Optional:** If necessary, select the **Include only Alerts following Security Profile [Applies to widgets only]** checkbox.

Results

The report has been generated, or scheduled, as applicable.

Download a report

*The **Generated** page lets you download reports.*

Procedure

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

   Result: The **Reports** page opens.

2. Select **Generated**.
3. To the left of the applicable report, select the download 📄 icon.

   Result: The download starts.

Results

The report has been downloaded to your downloads folder.

Delete a report

*The **Generated** page lets you delete generated reports.*

Procedure

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

   Result: The **Reports** page opens.

2. Select **Generated**.
3. To the left of the applicable report, select the download 🗑 icon.

Results

The report has been deleted.

Add a folder

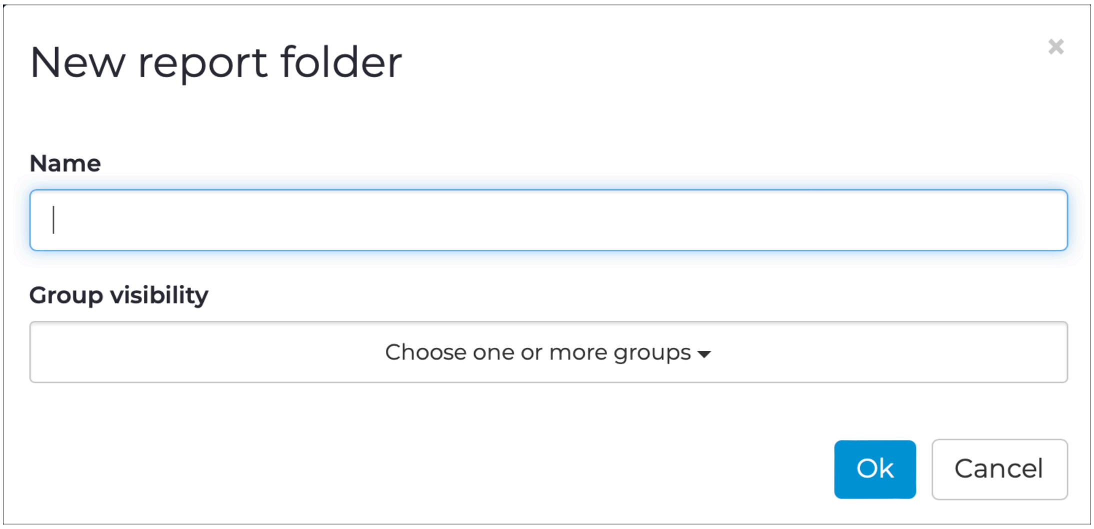
*The **Management** page lets you add folders for you to organize your reports.*

Procedure

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

   Result: The **Reports** page opens.
2. Select **Management**.
3. In the **Reports list** section on the left, select **Add folder**.

   Result: A dialog shows.
4. In the **Name** field, enter a name for the folder.



5. From the **Group visibility** dropdown, select the group(s) that will be able to view the reports.
6. Select **Ok**.

Results

The folder has been added.

Edit a folder

*The **Management** page lets you delete reports.*

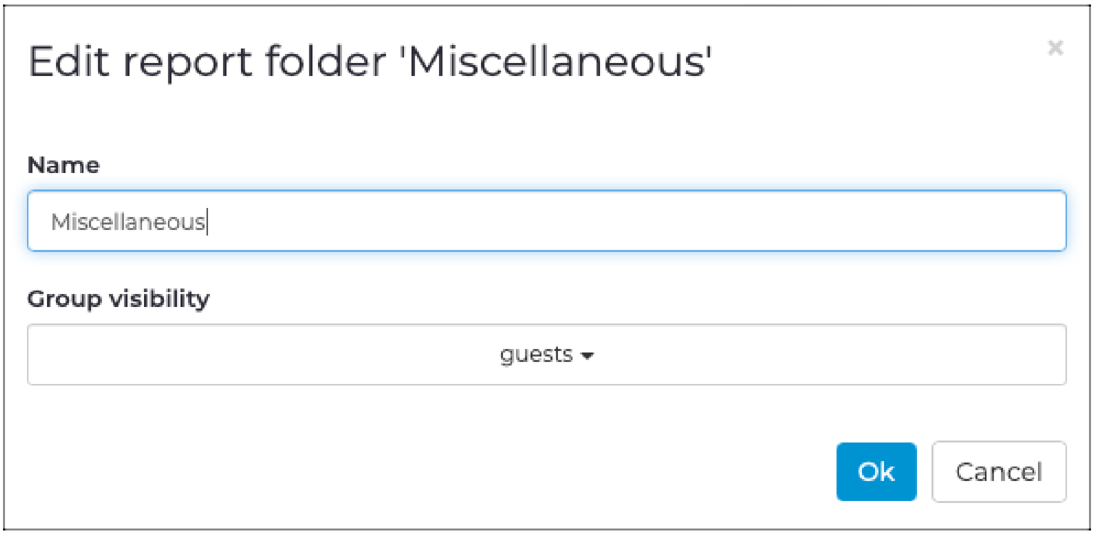
Procedure

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

   Result: The **Reports** page opens.
2. Select **Management**.
3. In the section on the left, to the right of the applicable folder's name, select the download ✎ icon.

   Result: A dialog shows.
4. **Optional:**

   If necessary, in the **Name** filed, edit the name of the folder.



Edit report folder 'Miscellaneous'

Name

Miscellaneous

Group visibility

guests ▾

5. **Optional:** If necessary, in the **Group visibility** filed, edit the visibility of the folder.
6. Select **Ok**.

Results

The report has been edited.

Delete a folder

*The **Management** page lets you delete reports.*

Procedure

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

   Result: The **Reports** page opens.

2. Select **Management**.
3. In the section on the left, to the right of the applicable folder's name, select the download 🗑 icon.

Results

The report has been deleted.

Import a schema

*The **Management** page lets you import a schema that has previously been exported.*

Procedure

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

   Result: The **Reports** page opens.

2. Select **Management**.
3. In the section on the left, select **Import Schema**.
4. Select the schema to import.

Results

The schema has been imported.

Export a schema

*The **Management** page lets you export a schema.*

Procedure

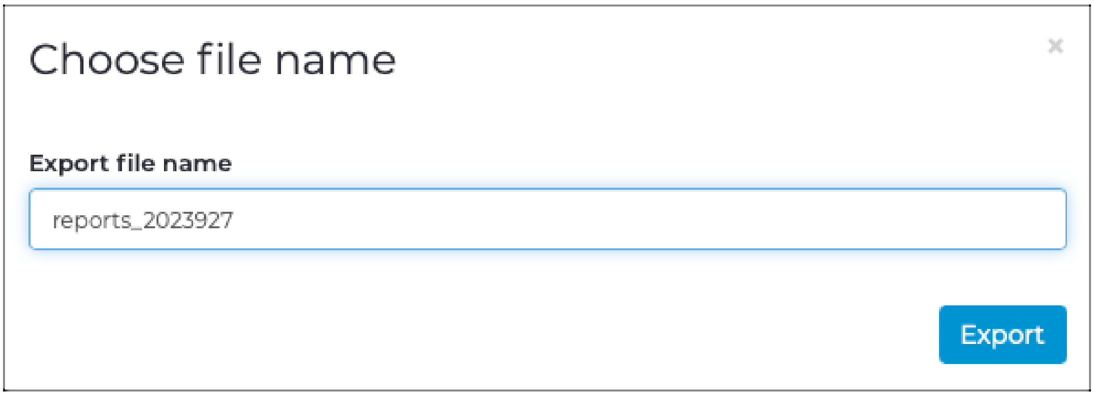
1. In the top navigation bar, select ≡ **icon** > **Reports**.

   Result: The **Reports** page opens.

2. Select **Management**.
3. In the top right, select **Export Schema**.

   Result: A dialog shows.

4. In the **Export file name** field, enter a name for the schema.



Choose file name

Export file name: reports_2023927

5. Select **Export**.

Results

The schema has been exported in *JSON* format.

Upload a custom logo

You can add a custom logo that will show in your reports.

Procedure

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

   Result: The **Reports** page opens.

2. Select **Settings**.

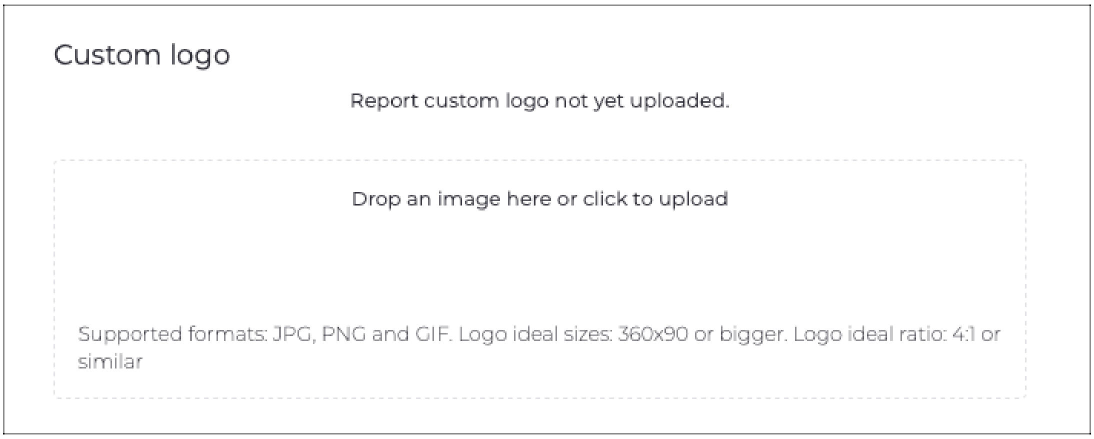
   Result: The Settings (on page 182) page opens.

3. Choose a method to upload a custom logo:

   Choose from:

   - Drag your image file into the **Drop an image here or click to upload** field
   - Click in the **Drop an image here or click to upload** field

4. If you chose the second method, select the correct file to upload.



Custom logo

Report custom logo not yet uploaded.

Drop an image here or click to upload

Supported formats: JPG, PNG and GIF. Logo ideal sizes: 360x90 or bigger. Logo ideal ratio: 4:1 or similar

Note:
Logos should be 360x90 pixels or bigger, with an ideal aspect ratio of 4:1, or similar.

Note:
Supported formats are:

- *graphics interchange format (GIF)*
- *joint photographic experts group (JPEG)*
- *portable network graphics (PNG)*

5. Wait for the file to upload.
6. Select **Save**.

Results

Your custom logo will now be added to your reports.

Configure SMTP settings

If you want to send emails that contain scheduled reports, you need to configure the simple mail transfer protocol (SMTP) server settings.

Procedure

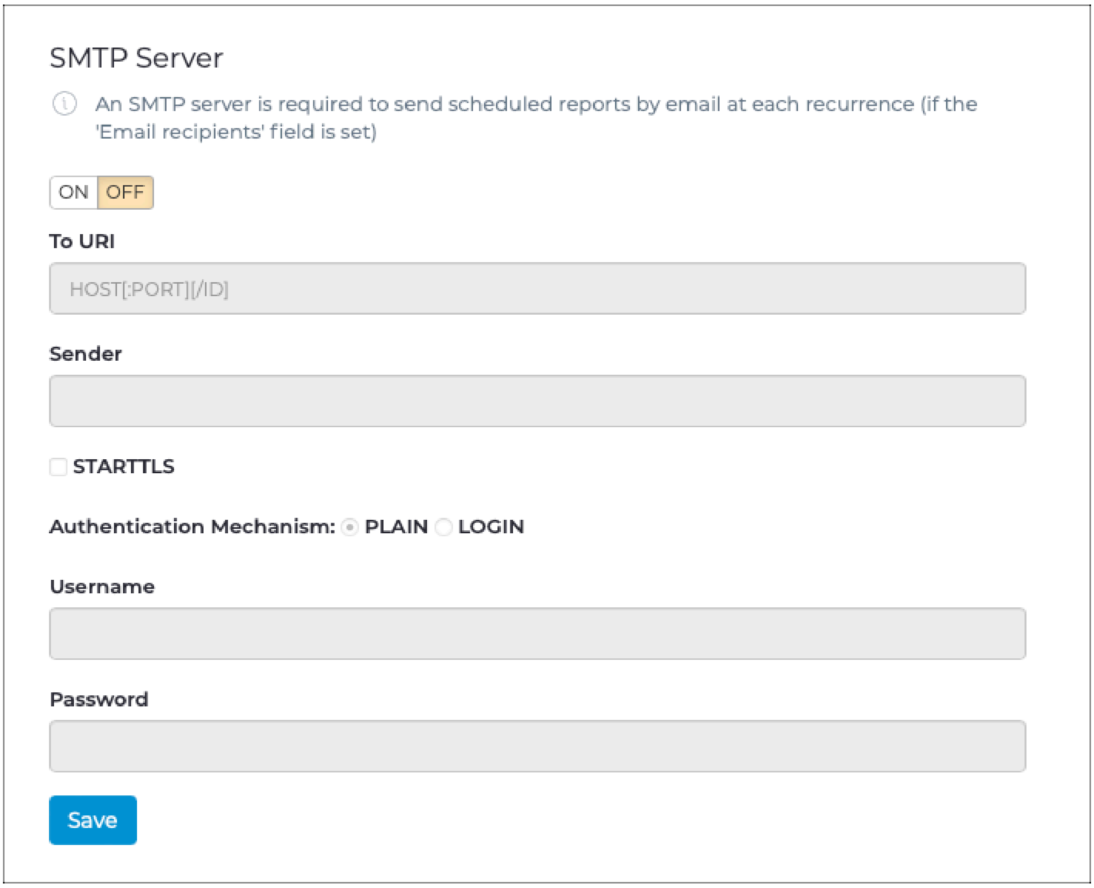
1. In the top navigation bar, select ≡ **icon > Reports**.

   Result: The **Reports** page opens.

2. Select **Settings**.

   Result: The Settings (on page 182) page opens.

3. In the **SMTP Server** section, set the toggle to **ON**.



SMTP Server

ⓘ An SMTP server is required to send scheduled reports by email at each recurrence (if the 'Email recipients' field is set)

ON [✓ OFF]

To URI

HOST[:PORT][/ID]

Sender

□ **STARTTLS**

Authentication Mechanism: ● **PLAIN** ○ **LOGIN**

Username

Password

4. In the **To URI** field, enter the host URI information. For example, `HOST[:PORT][/ID]`

5. In the **Sender** field, enter the sender identification information.

6. To use encryption, select the **STARTTLS** checkbox.

> **Note:**
> If you do not select this option, reports will be sent without encryption.

7. To start the authentication process, choose an Authentication Mechanism:

   Choose from:

   - **PLAIN**
   - **LOGIN**

> **Note:**
> The default setting is **PLAIN**.

8. If you chose **LOGIN**, enter your credentials.
   a. In the **Username** field, enter your username.
   b. In the **Password** field, enter your password.
9. Select **Save**.

Results

Emails for scheduled reports that have email recipients will now be sent at the next scheduled occurrence.

Filter a report globally

You can filter a report globally, which is the default filter. This lets you use a specific category to apply filters to the entire report.

Procedure

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

   Result: The **Reports** page opens.

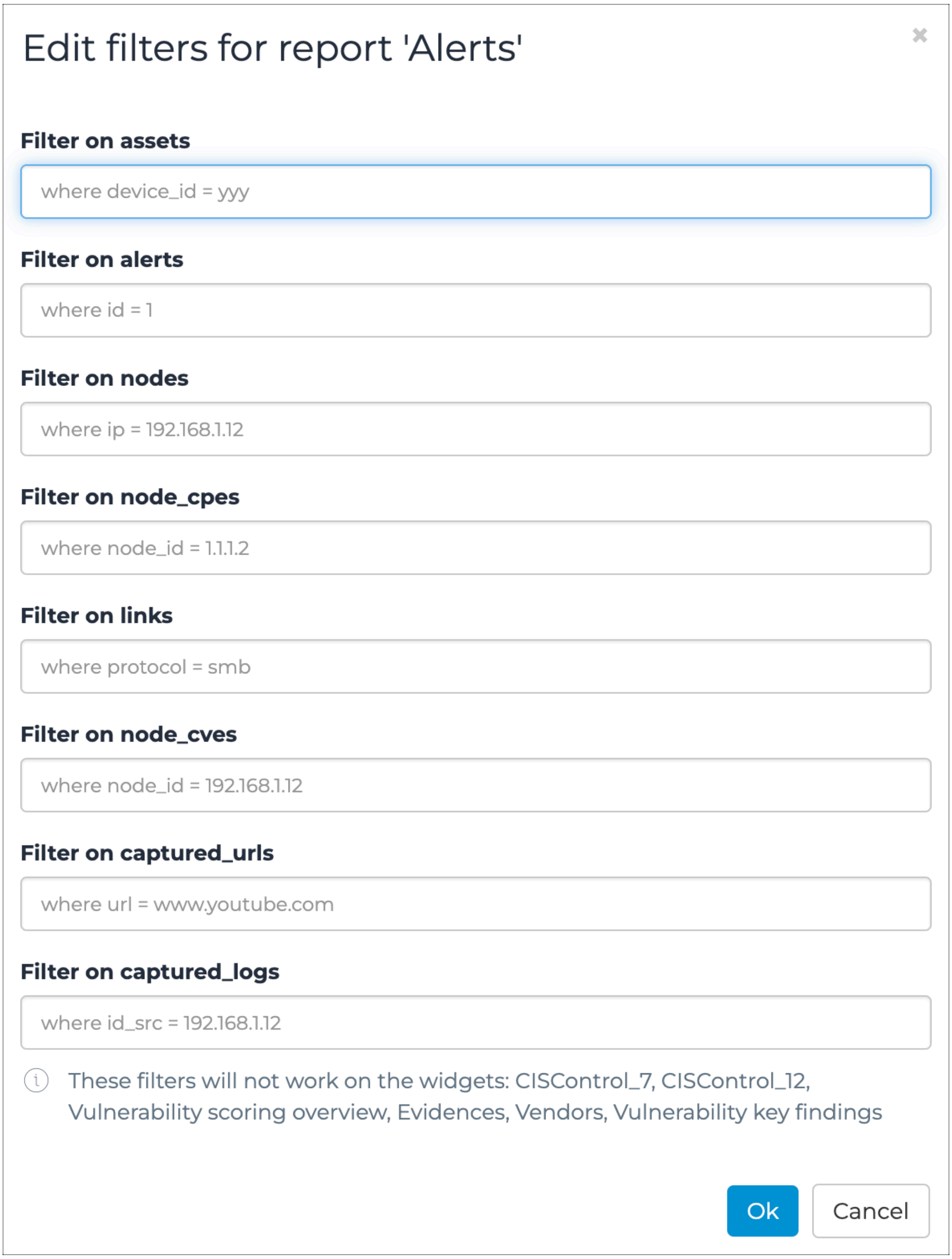
2. Select **Management**.

   Result: The Management (on page 177) page opens.

3. In the top section, select ▼ **Filters**.

   Result: A dialog shows.

4. Select the category on which to filter, then enter your filter query in the related field.



Edit filters for report 'Alerts'

Filter on assets

where device_id = yyy

Filter on alerts

where id = 1

Filter on nodes

where ip = 192.168.1.12

Filter on node_cpes

where node_id = 1.1.1.2

Filter on links

where protocol = smb

Filter on node_cves

where node_id = 192.168.1.12

Filter on captured_urls

where url = www.youtube.com

Filter on captured_logs

where id_src = 192.168.1.12

These filters will not work on the widgets: CISControl_7, CISControl_12, Vulnerability scoring overview, Evidences, Vendors, Vulnerability key findings

5. Select **Ok**.

> **Note:**
> At the bottom of the dialog is a list of widgets on which filters will not work.

Results

The filter(s) has (have) been applied to the report.

Add a widget to a report

*The **Management** page lets you add widgets to reports.*

Procedure

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

   Result: The **Reports** page opens.

2. Select **Management**.

   Result: The Management (on page 177) page opens.

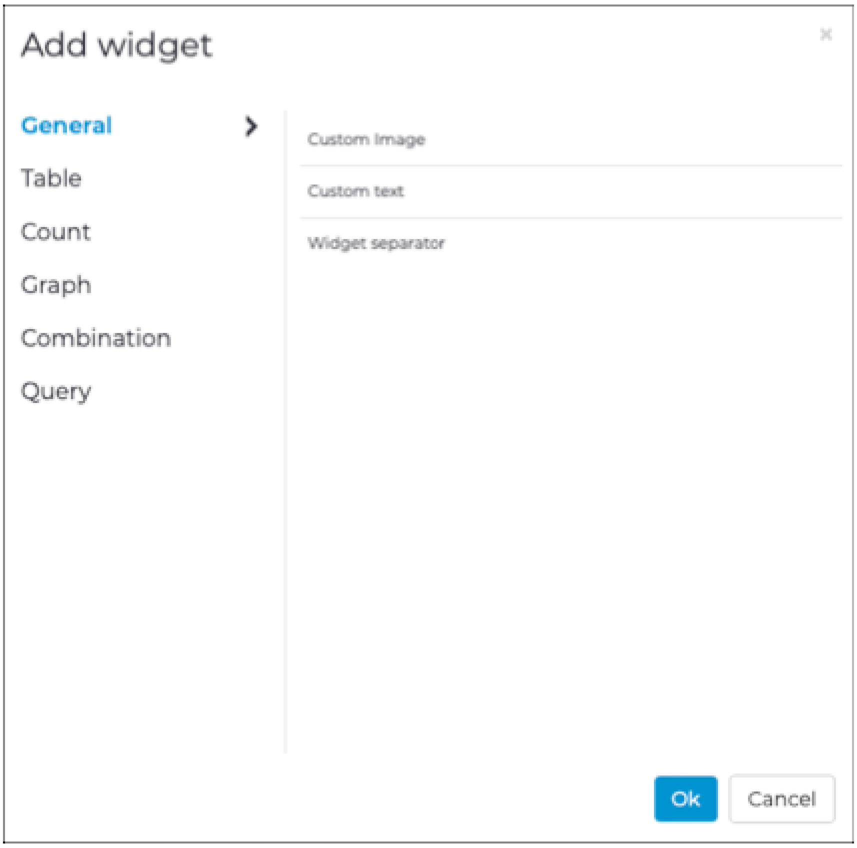
3. In the **Reports list** section on the left, select the applicable report.

   Result: The report opens.

4. On the right side of the report, choose the section that you want to add the widget to. Select **Add widget**.

   Result: A dialog shows.

5. In the left pane, choose the type of widget that you want to add.



6. From the list, select the widget that you want.

Results

The widget has been added to the report.

Filter a report with a widget

You can use widgets to filter a report.

Procedure

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

   Result: The **Reports** page opens.

2. Select **Management**.

   Result: The Management (on page 177) page opens.

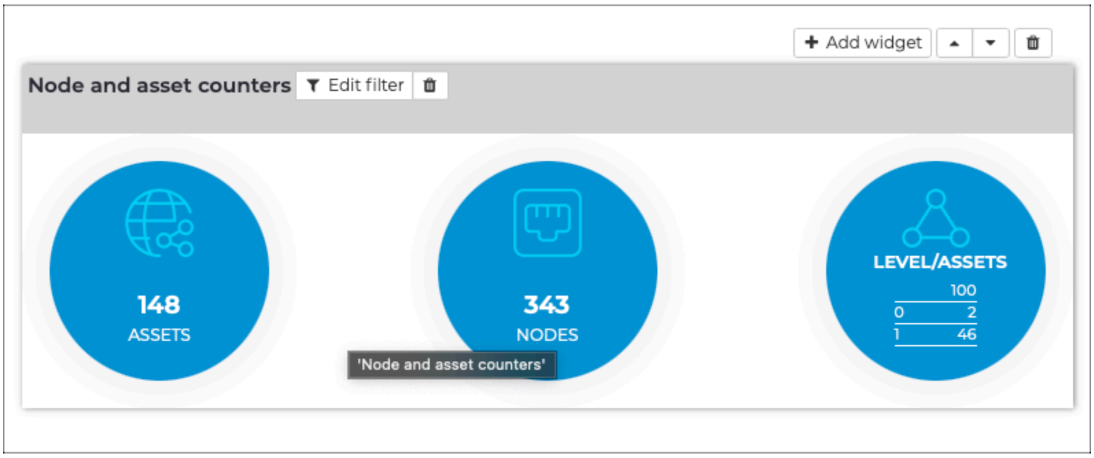
3. In the **Reports list** section on the left, select the applicable report.

   Result: The report opens.

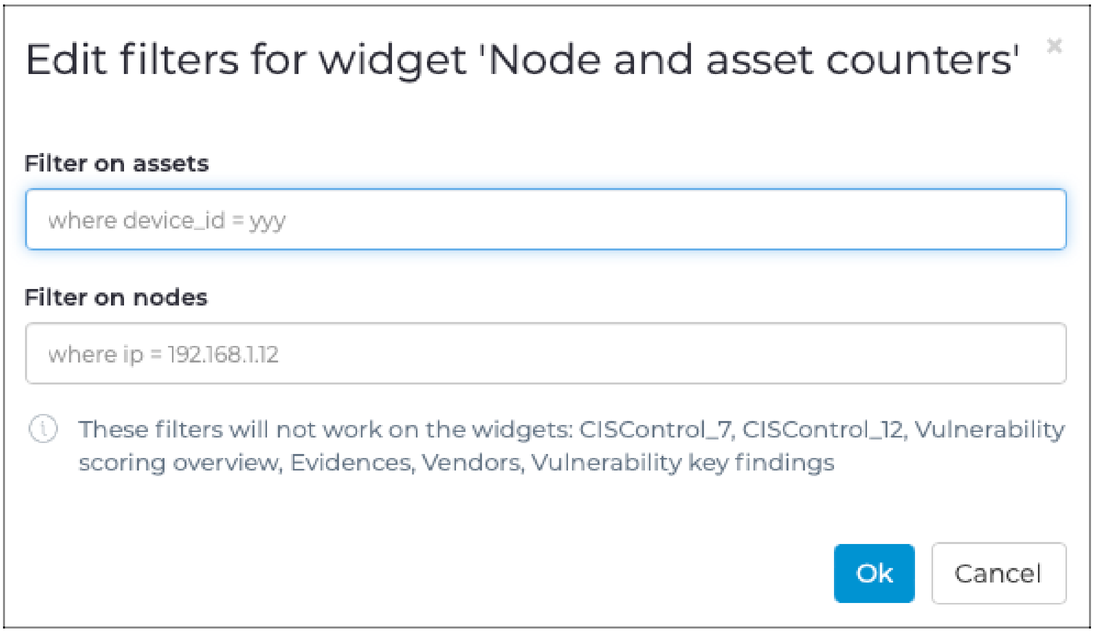
4. Find the widget that you would like to use and hover your mouse over it.

   Result: At the top of the widget, more buttons show.

5. Select **Edit filter**.



6. Select the category on which to filter, then enter your filter query in the related field.



Edit filters for widget 'Node and asset counters'

Filter on assets

where device_id = yyy

Filter on nodes

where ip = 192.168.1.12

These filters will not work on the widgets: CISControl_7, CISControl_12, Vulnerability scoring overview, Evidences, Vendors, Vulnerability key findings

7. Select **Ok**.

> **Note:**
> At the bottom of the dialog is a list of widgets on which filters will not work.

Results

The filter(s) has (have) been applied to the report.

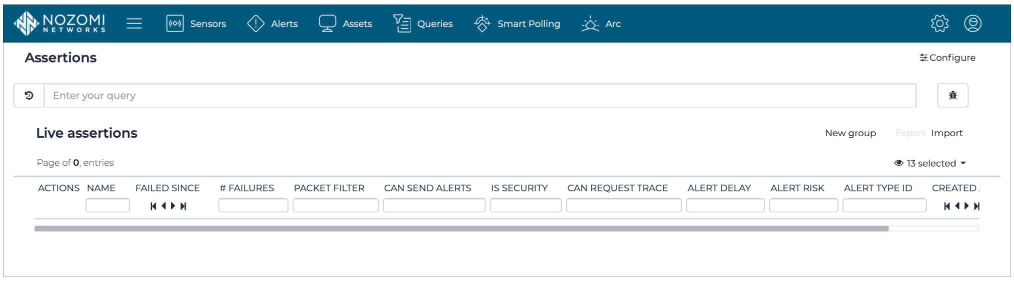
Chapter 11. Assertions

Assertions

*The **Assertions** page shows all the assertions and lets you configure them.*

A valid assertion is a normal query with a special command appended at the end. Assertions can be saved in a specific order and can be continuously executed in the system.

Queries are based on the *N2QL*, which you can use to ensure that certain conditions are met on the observed system. An assertion is typically either an empty value, or a specific value. When an unexpected value appears, or when the value is different than the expected, the system alerts the user.



Assertions

Enter your query

Live assertions

Page of **0**, entries

13 selected

ACTIONS	NAME	FAILED SINCE	# FAILURES	PACKET FILTER	CAN SEND ALERTS	IS SECURITY	CAN REQUEST TRACE	ALERT DELAY	ALERT RISK	ALERT TYPE ID	CREATED

Figure 60. Assertions page

Configure

This lets you configure the execution interval in seconds.

History button

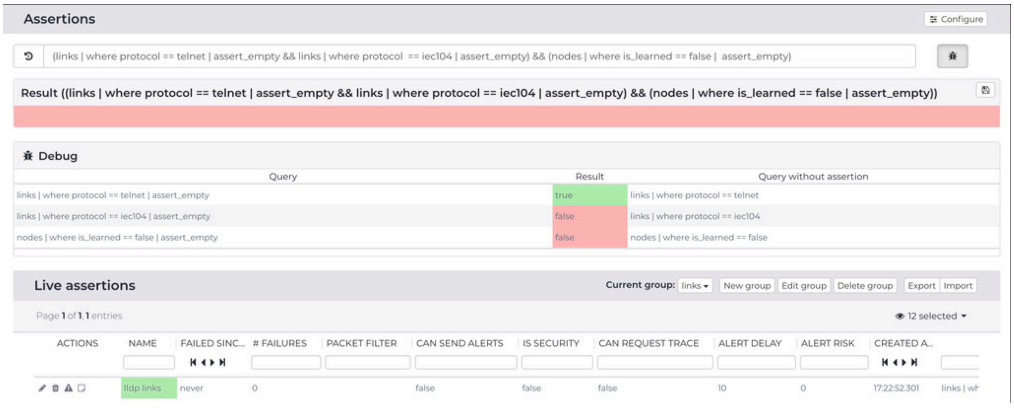
This button shows a history of the previous queries that have been entered in the query field.

Query field

This field is where you enter your query.

Debug button

Because assertions with logical operators and brackets can quickly become complex, the debug icon decomposes the query, and executes each part to show intermediate results.



```
(links | where protocol == telnet | assert_empty && links | where protocol  == iec104 | assert_empty) && (nodes | where is_learned == false |  assert_empty)
```

Result ((links | where protocol == telnet | assert_empty && links | where protocol == iec104 | assert_empty) && (nodes | where is_learned == false | assert_empty))

Query	Result	Query without assertion
links | where protocol == telnet | assert_empty	true	links | where protocol == telnet
links | where protocol == iec104 | assert_empty	false	links | where protocol == iec104
nodes | where is_learned == false | assert_empty	false	nodes | where is_learned == false

Page 1 of 1, 1 entries

ACTIONS	NAME	FAILED SINC...	# FAILURES	PACKET FILTER	CAN SEND ALERTS	IS SECURITY	CAN REQUEST TRACE	ALERT DELAY	ALERT RISK	CREATED A...	
	lldp links	never	0		false	false	false	10	0	17:22:52.301	links | wh

Figure 61. Complex assertion being debugged

New group

This lets you create a group to combine assertions to make viewing and management easier.

Export

This lets you export assertion groups in *JSON* format.

Import

This lets you import assertion groups in *JSON* format.

Assertion operators

Table 2. Assertion operators

Operator	Description
`assert_all <field> <op> <value>`	The assertion is satisfied when each element in the query result set matches the given condition.
`assert_any <field> <op> <value>`	The assertion is satisfied when at least one element in the query result set matches the given condition.
`assert_empty`	The assertion is satisfied when the query returns an empty result set.
`assert_not_empty`	The assertion is satisfied when the query returns a non-empty result set.

Save an assertion

You can save assertions to have them continuously executed in the system.

Procedure

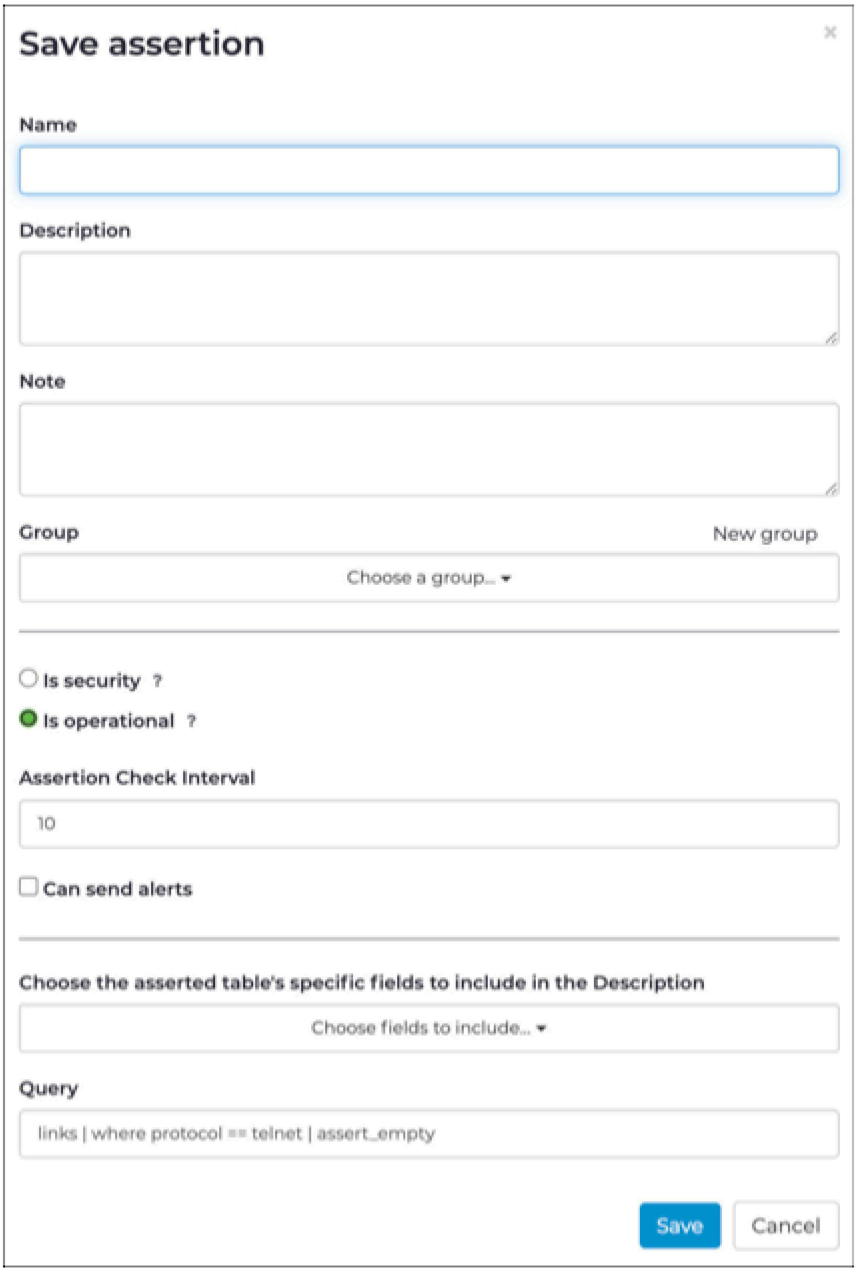
1. In the top navigation bar, select ≡ **icon > Assertions**.

   Result: The **Assertions** page opens.

2. In the query field, enter a query.
3. Select **Enter**.
4. To save the assertion, select **Save**.

   Result: A dialog shows.

5. In the **Name** field, enter a name for the query.



Save assertion

Name

Description

Note

Group

○ Is security ?

● Is operational ?

Assertion Check Interval

10

□ Can send alerts

Choose the asserted table's specific fields to include in the Description

Query

links | where protocol == telnet | assert_empty

6. In the **Description** field, enter a description.

7. To assign the assertion to a group, in the **Group** field, select one of the following
    a. From the dropdown menu, select an existing group.

    b. Select **Save**.

    c. To create a new group, select **New group**.
    Result: A dialog shows.

    d. In the **Group name** field, enter a group name for the assertion.

    e. Select **Save**.

8. Choose from one of these options:

    Choose from:

    - **Is security ?**
    - **Is operational ?**

9. In the **Assertion Check Interval** field, choose the interval in seconds at which the assertion will be rechecked.

    Note:
    You can select an interval between 10 seconds and 1 day.

10. **Optional:** If you want the assertion to trigger an alert, select the **Can send alerts** checkbox.
11. From the **Choose the asserted table's specific fields to include in the Description** dropdown, select the fields to include in the assertion description.
12. In the **Query** field, enter the assertion query.
13. Select **Save**.

    Result: The saved assertion will be listed at the bottom of the page with a green or red color to indicate the result.

Edit an assertion

This lets you edit the details for an existing assertion.

Procedure

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

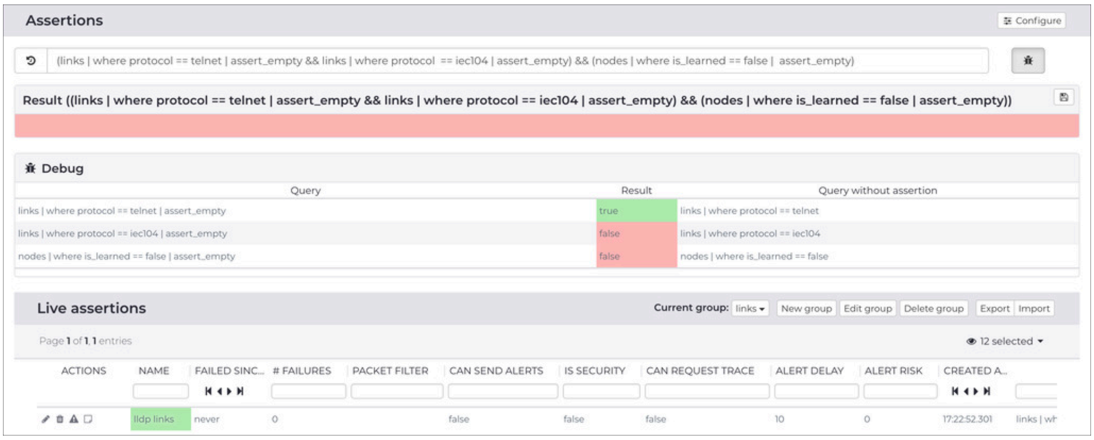
   Result: The **Assertions** page opens.

2. In the query field, enter a query.
3. To execute the query, elect **Enter**.

> **Note:**
> You can use the logical operators && (and) and || (or) to combine multiple assertions. Round brackets ( ) change the logical grouping as in a mathematical expression.

4. **Optional:** To the right of the query field, select the debug 🐞 icon.

> **Note:**
> Because assertions with logical operators and brackets can quickly become complex, the debug icon decomposes the query, and executes each part to show intermediate results.



(links | where protocol == telnet | assert_empty && links | where protocol == iec104 | assert_empty) && (nodes | where is_learned == false | assert_empty)

Result ((links | where protocol == telnet | assert_empty && links | where protocol == iec104 | assert_empty) && (nodes | where is_learned == false | assert_empty))

Debug

Query	Result	Query without assertion
links | where protocol == telnet | assert_empty	true	links | where protocol == telnet
links | where protocol == iec104 | assert_empty	false	links | where protocol == iec104
nodes | where is_learned == false | assert_empty	false	nodes | where is_learned == false

Page 1 of 1, 1 entries

12 selected

ACTIONS	NAME	FAILED SINC...	# FAILURES	PACKET FILTER	CAN SEND ALERTS	IS SECURITY	CAN REQUEST TRACE	ALERT DELAY	ALERT RISK	CREATED A...	
	lldp links	never	0		false	false	false	10	0	17:22:52.301	links | wh

Result: The debug section shows.

Configure an assertion

This lets you configure the execution interval of the assertions, in seconds.

Procedure

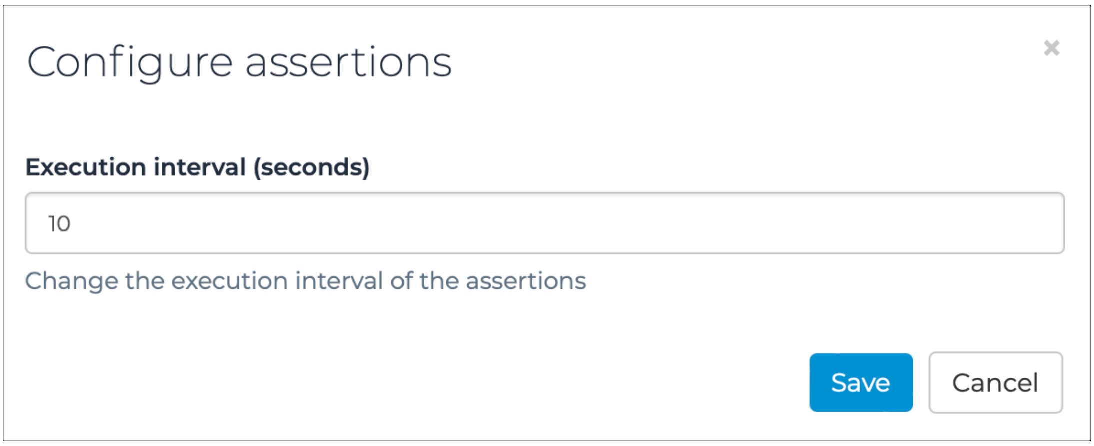
1. In the top navigation bar, select ☰ **icon > Assertions**.

   Result: The **Assertions** page opens.

2. In the top right, select **Configure**.

   Result: A dialog opens.

3. In the **Execution interval (seconds)** field, enter an interval.

   Configure assertions

   Execution interval (seconds)

   10

   Change the execution interval of the assertions

4. Select **Save**.

Configure an assertion on links

This lets you configure the scope of the assertion for the related links.

Procedure

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

   Result: The **Network** page opens.

2. Select **Links**.

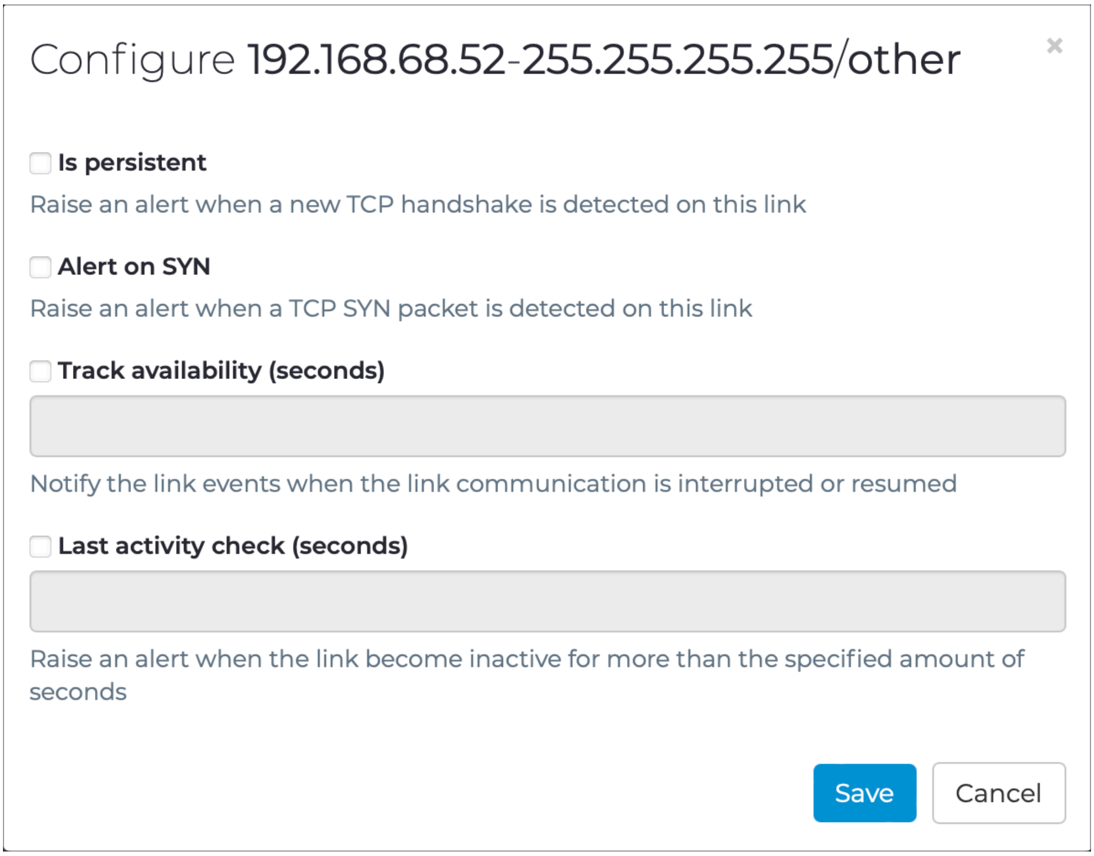
   Result: The **Links** page opens.

3. To the left of the applicable link, select the configure ☰ icon.

   Result: A dialog opens.

4. **Optional:**

   Select **Is persistent**.



Configure **192.168.68.52-255.255.255.255/other**

□ **Is persistent**

Raise an alert when a new TCP handshake is detected on this link

□ **Alert on SYN**

Raise an alert when a TCP SYN packet is detected on this link

□ **Track availability (seconds)**

Notify the link events when the link communication is interrupted or resumed

□ **Last activity check (seconds)**

Raise an alert when the link become inactive for more than the specified amount of seconds

Note:
When selected, this check raises a new alert whenever a *TCP* handshake is successfully completed on the link.

5. **Optional:** Select **Alert on SYN**.

   > **Note:**
   > When selected, this check raises a new alert whenever a client sends a TCP SYN on the link.

6. **Optional:** Select **Track availability (seconds)**.

   > **Note:**
   > When selected, a link is considered non-functioning if it is unresponsive for the specified time.

7. **Optional:** Select **Last activity check (seconds)**.

   > **Note:**
   > When selected, this check raises an alert when the link is not receiving data for more than the specified time.

8. Select **Save**.

Results

The assertion has been configured.

Configure an assertion on variables

This lets you configure the scope of the assertion for the related variables.

Procedure

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

   Result: The **Process** page opens.

2. Select **List**.

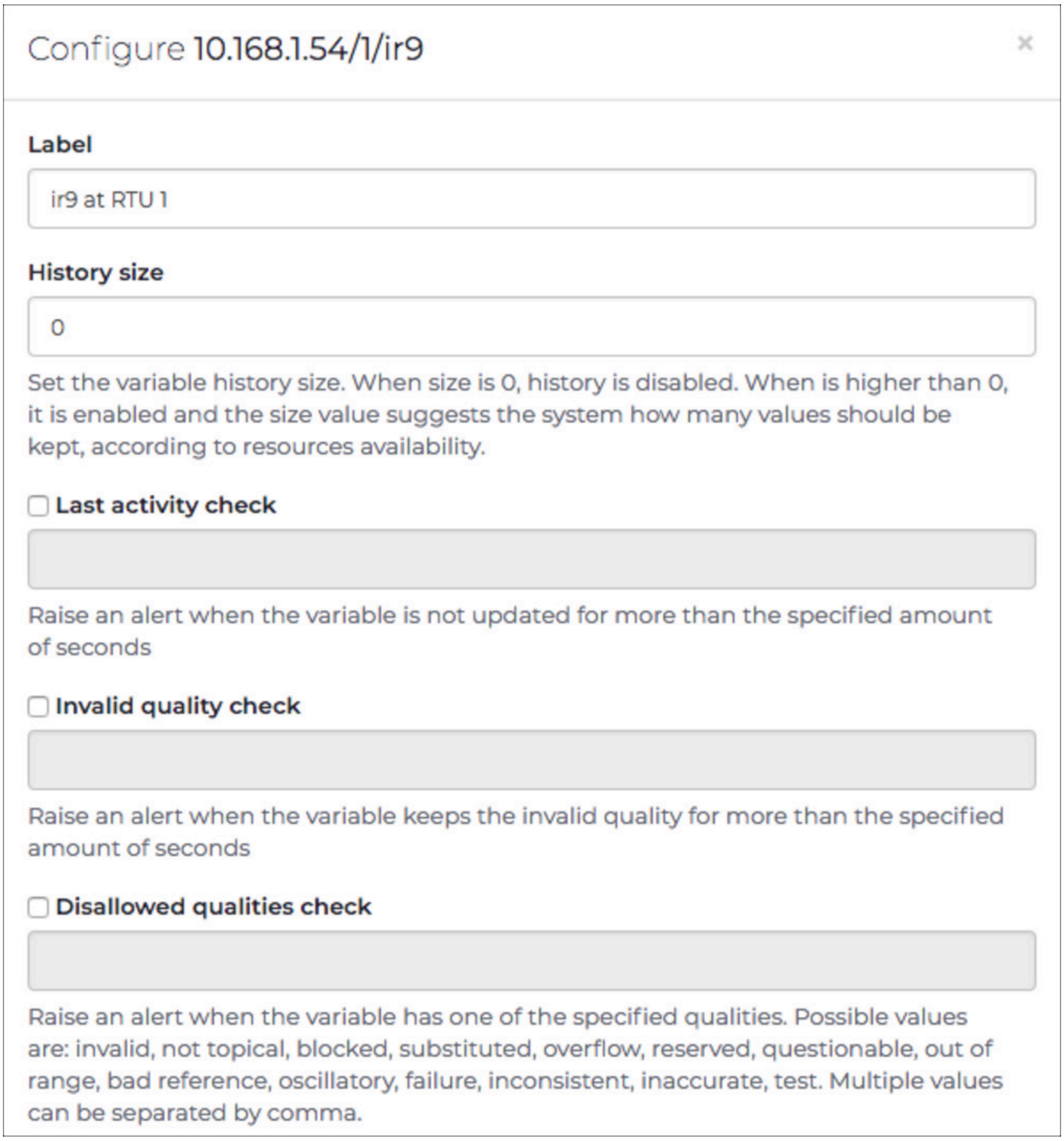
   Result: The **List** page opens.

3. To the left of the applicable link, select the configure ☰ icon.

   Result: A dialog opens.

4. **Optional:**

   In the **Label** field, enter a label for the assertion.



Configure 10.168.1.54/1/ir9

Label

ir9 at RTU 1

History size

0

Set the variable history size. When size is 0, history is disabled. When is higher than 0, it is enabled and the size value suggests the system how many values should be kept, according to resources availability.

☐ **Last activity check**

Raise an alert when the variable is not updated for more than the specified amount of seconds

☐ **Invalid quality check**

Raise an alert when the variable keeps the invalid quality for more than the specified amount of seconds

☐ **Disallowed qualities check**

Raise an alert when the variable has one of the specified qualities. Possible values are: invalid, not topical, blocked, substituted, overflow, reserved, questionable, out of range, bad reference, oscillatory, failure, inconsistent, inaccurate, test. Multiple values can be separated by comma.

5. **Optional:** In the **History size** field, enter a value.

> **Note:**
> This sets the *Variable* history size. When the size is 0, history is disabled. When it is higher than 0, it is enabled, and the size value suggests how many values that the system should keep, depending on the available resources.

6. **Optional:** In the **Last activity check** field, enter a value.

   > **Note:**
   > When selected, this check raises an alert when the *Variable* is either not measured or is changed for more than the specified number of seconds.

7. **Optional:** In the **Invalid quality check** field, enter a value.

   > **Note:**
   > When selected, this check raises an alert when the *Variable* maintains an invalid quality for more than the specified amount of seconds.

8. **Optional:** In the **Disallowed quality check** field, enter a value.

   > **Note:**
   > When selected, this check raises an alert when the *Variable* gains one of the specified qualities.

9. Select **Save**.

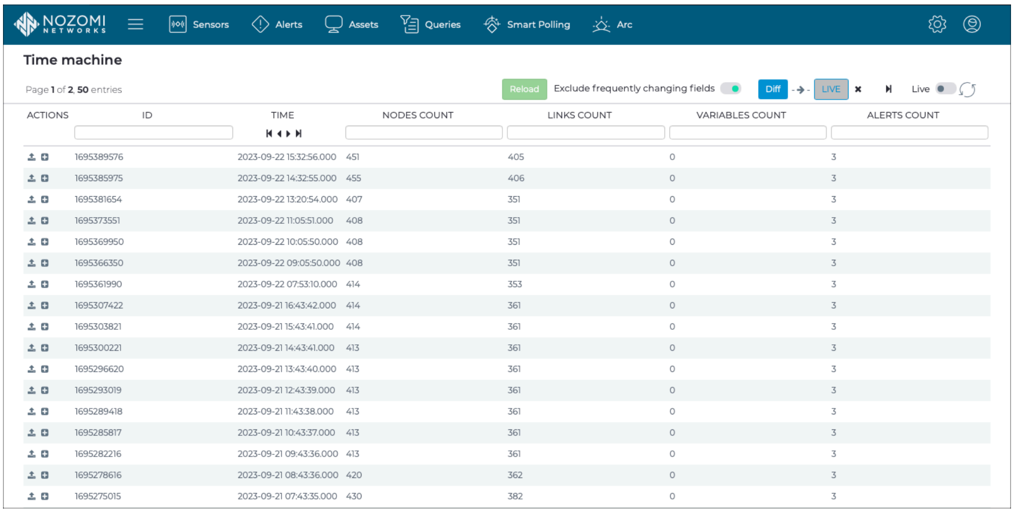
Results

The assertion has been configured.

Chapter 12. Time machine

Time machine

Time machine lets you load a snapshot, which is a previously saved state, and go back in time, to analyze the data from a past situation. You can load a single snapshot and use the platform as usual or load two snapshots and compare the user interface to highlight changes.



Time machine

Page 1 of 2, 50 entries

Exclude frequently changing fields

ACTIONS	ID	TIME	NODES COUNT	LINKS COUNT	VARIABLES COUNT	ALERTS COUNT
	1695389576	2023-09-22 15:32:56.000	451	405	0	3
	1695385975	2023-09-22 14:32:55.000	455	406	0	3
	1695381654	2023-09-22 13:20:54.000	407	351	0	3
	1695373551	2023-09-22 11:05:51.000	408	351	0	3
	1695369950	2023-09-22 10:05:50.000	408	351	0	3
	1695366350	2023-09-22 09:05:50.000	408	351	0	3
	1695361990	2023-09-22 07:53:10.000	414	353	0	3
	1695307422	2023-09-21 16:43:42.000	414	361	0	3
	1695303821	2023-09-21 15:43:41.000	414	361	0	3
	1695300221	2023-09-21 14:43:41.000	413	361	0	3
	1695296620	2023-09-21 13:43:40.000	413	361	0	3
	1695293019	2023-09-21 12:43:39.000	413	361	0	3
	1695289418	2023-09-21 11:43:38.000	413	361	0	3
	1695285817	2023-09-21 10:43:37.000	413	361	0	3
	1695282216	2023-09-21 09:43:36.000	413	361	0	3
	1695278616	2023-09-21 08:43:36.000	420	362	0	3
	1695275015	2023-09-21 07:43:35.000	430	382	0	3

Figure 62. Time machine page

Reload

If you initiate a diff and then navigate to another area of the software, when you return to this page you might not see the progress of the diff. The **Reload** button lets you either:

- Reload the progress bar (if the diff is still in progress)
- View the results (if the process has finished)

Exclude frequently changing fields

You can select the **Exclude frequently changing fields** ○ toggle to on to exclude the fields that change frequently. This excludes the diff all fields that are affected from normal traffic handling. Examples of frequently changing fields are the number of bytes received / sent, and the last activity time.

Diff

The **Diff** button starts the diff process. The system evaluates the diff baseline - target files and estimates how *CPU* / memory intensive the diff operation is going to be. If there is not enough free memory at the moment, the diff will be aborted with the appropriate message. If the diff is estimated to take more than a few minutes, a warning will show and a confirmation dialog will show.

Live

The **LIVE** button lets you choose the current view as part of the diff.

Step forward

The step forward ⏭ icon lets you go back to the present time view after you have viewed a snapshot.

Live / refresh

The **Live** ◐ ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Load snapshot

The load snapshot ⬆ icon lets you select a historical snapshot.

Select for diff

The select for diff ⊞ icon to choose the related snapshot as part of the diff.

Time machine diffs

You can use time machine to view diffs between historical snapshots, or an historical snapshot and the current live view.

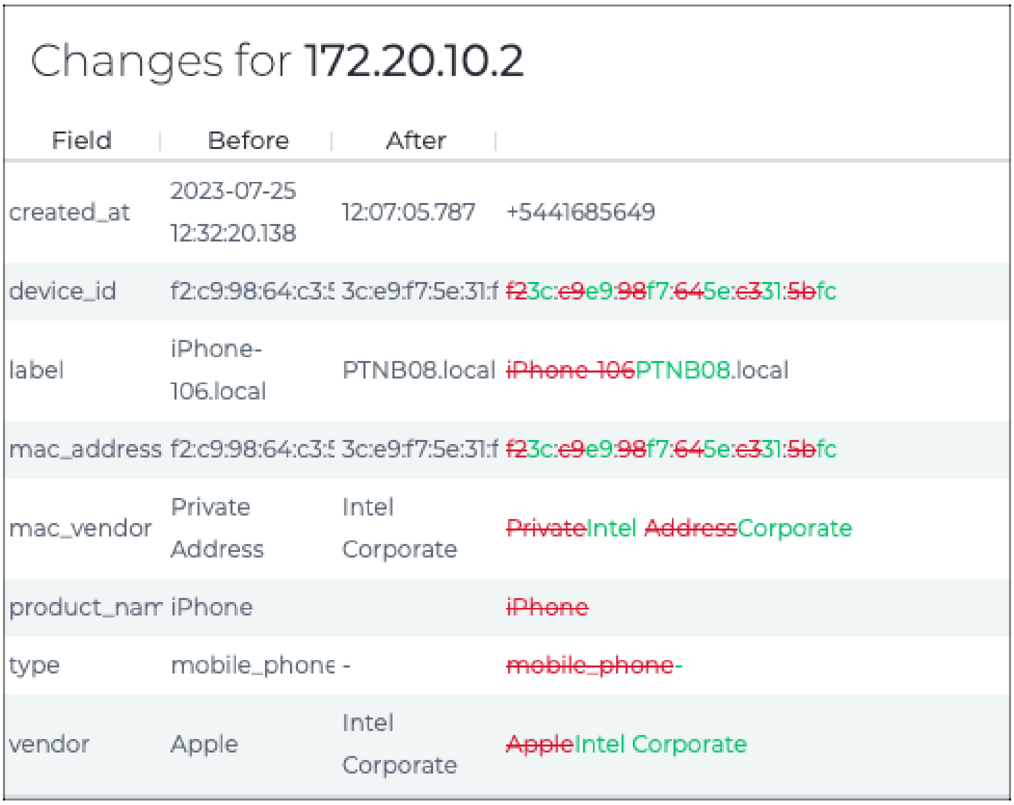
Snapshots

When you view a snapshot, the *graphical user interface (GUI)* will change to gray.

The graph view and the use of color let you quickly see the nodes, or links, that have been added, removed, or changed:

- Added items are green
- Removed items are red
- Changed items are blue

Diff views

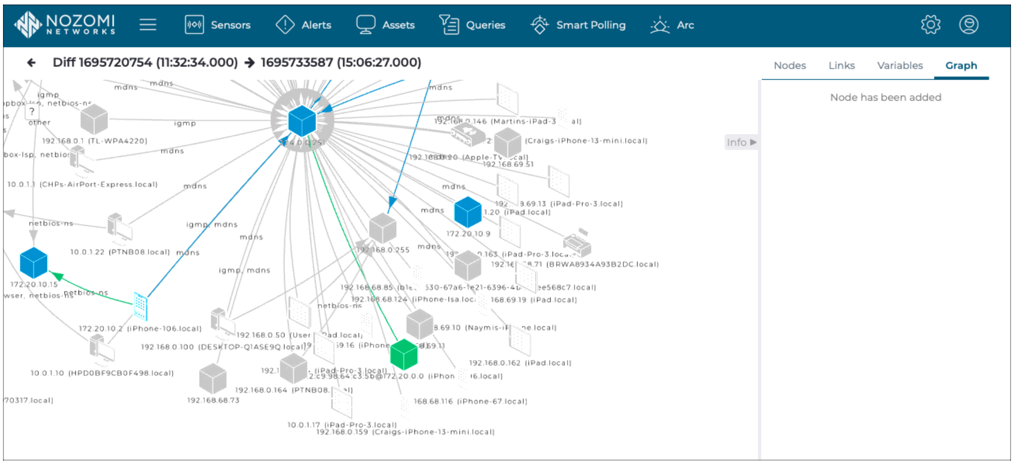


Changes for **172.20.10.2**

Field	Before	After	
created_at	2023-07-25 12:32:20.138	12:07:05.787	+5441685649
device_id	f2:c9:98:64:c3:5	3c:e9:f7:5e:31:f	~~f2~~3c:~~c9~~e9:~~98~~f7:~~64~~5e:~~c3~~31:~~5b~~fc
label	iPhone-106.local	PTNB08.local	~~iPhone-106~~PTNB08.local
mac_address	f2:c9:98:64:c3:5	3c:e9:f7:5e:31:f	~~f2~~3c:~~c9~~e9:~~98~~f7:~~64~~5e:~~c3~~31:~~5b~~fc
mac_vendor	Private Address	Intel Corporate	~~Private~~Intel ~~Address~~Corporate
product_nam	iPhone		~~iPhone~~
type	mobile_phone	-	~~mobile_phone~~-
vendor	Apple	Intel Corporate	~~Apple~~Intel Corporate

Figure 63. Table view

In the graph view, you can select a link or node to see more information in the pane on the right side.


NOZOMI NETWORKS
Sensors
Alerts
Assets
Queries
Smart Polling
Arc
Nodes
Links
Variables
Graph
Info ▸
mdns
igmp
netbios-ns
other
192.168.0.1 (TL-WPA4220)
10.0.1.1 (CHPs-AirPort-Express.local)
10.0.1.22 (PTNB08.local)
172.20.10.15
172.20.10.2 (iPhone-106.local)
10.0.1.10 (HPD0BF9CB0F498.local)
192.168.0.100 (DESKTOP-Q1ASE9Q.local)
192.168.68.73
192.168.0.164 (PTNB08.local)
10.0.1.17 (iPad-Pro-3.local)
192.168.0.159 (Craigs-iPhone-13-mini.local)
192.168.0.146 (Martins-iPad-3.local)
(Craigs-iPhone-13-mini.local)
192.168.69.51
192.168.69.13 (iPad-Pro-3.local)
172.20.10.9
192.168.0.255
192.168.68.85
192.168.68.124 (iPhone-Isa.local)
192.168.69.19 (iPad.local)
192.168.69.10
192.168.0.162 (iPad.local)
172.20.0.0
192.168.68.116 (iPhone-67.local)

← Diff 1695720754 (11:32:34.000) → 1695733587 (15:06:27.000)

Node has been added

Figure 64. Graph view

Load a snapshot

To create a diff, you must first load a snapshot.

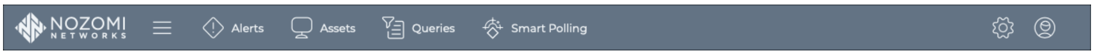
Procedure

1. In the top navigation bar, select ≡ **icon** > **Time machine**.

   Result: The **Time machine** page opens.

2. To the left of the applicable snapshot, select the load snapshot ⇪ icon.

   Result: The user interface turns gray to highlight that you are viewing a static snapshot.

3. To return to the present time view, select the ⏵ icon.

Request a diff

The time machine lets you create a diff between to historical snapshots, or a snapshot and the current view.

Procedure

1. In the top navigation bar, select ≡ **icon > Time machine**.

   Result: The **Time machine** page opens.

2. To select the baseline of the diff, to the left of the applicable snapshot, select the select for diff ⊞ icon.

   Result: At the top of the table, the details of the snapshot are loaded next to the **Diff** icon.

3. Choose a target for the diff:

   Choose from:

   - To select another snapshot from the past, to the left of the applicable snapshot, select the load snapshot ⤒ icon
   - To select the current, live environment, at the top of the table, select the **LIVE** icon
4. **Optional:** Select the **Exclude frequently changing fields** toggle to on.
5. Now that the baseline and the target have been set, select the **Diff** icon.

   Result: The system evaluates the diff baseline / target files and estimates how *CPU* / memory intensive the diff operation is going to be. If there is not enough free memory at the moment, the diff will be aborted with the appropriate message. If the diff is estimated to take more than a few minutes, a warning will show and a confirmation dialog will show.

6. As soon as the diff operation starts, a dialog shows the progress. To stop the diff operation, select **Abort**.

Results

After the diff has been computed, the diff results show.

Reload the diff operation progress

Diff operations can take a long time to conclude. While an operation is in progress, you can continue to use the software as normal.

Procedure

1. In the top navigation bar, select ≡ **icon** > **Time machine**.

   Result: The **Time machine** page opens.

2. At the top of the table, select **Reload**.

   Result: If the diff operation is still in progress, the progress dialog shows. If the operation has finished, the diff results show.

View a diff from an alert

This automatic feature will use the previous and subsequent snapshots according to the time of the alert.

Procedure

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

   Result: The **Alerts** 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 **Time machine diff**.

   Result: The time diff shows.

4. To see more details on the right side of the graph, select the applicable node or link.

Chapter 13. Vulnerabilities

Vulnerabilities

The Nozomi Networks software continuously discovers vulnerabilities in monitored assets.

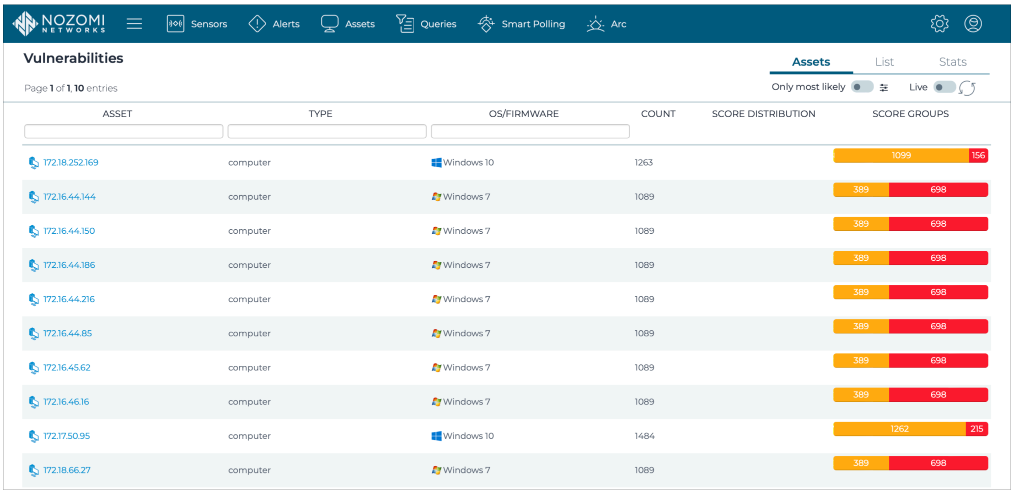
The Nozomi Networks software continuously discover vulnerabilities. To do this, it matches the *Common Platform Enumeration (CPE)* of a device with the National Vulnerability Database, and other data sources.

The Vulnerabilities page has these tabs:

- Assets (on page 232)
- List (on page 233)
- Stats (on page 234)

Assets

*The **Assets** page shows a list of assets with known vulnerabilities, along with a summary of the severity of the vulnerability.*



Vulnerabilities

Page **1** of **1**, **10** entries

ASSET	TYPE	OS/FIRMWARE	COUNT	SCORE DISTRIBUTION	SCORE GROUPS
172.18.252.169	computer	Windows 10	1263		1099 156
172.16.44.144	computer	Windows 7	1089		389 698
172.16.44.150	computer	Windows 7	1089		389 698
172.16.44.186	computer	Windows 7	1089		389 698
172.16.44.216	computer	Windows 7	1089		389 698
172.16.44.85	computer	Windows 7	1089		389 698
172.16.45.62	computer	Windows 7	1089		389 698
172.16.46.16	computer	Windows 7	1089		389 698
172.17.50.95	computer	Windows 10	1484		1262 215
172.18.66.27	computer	Windows 7	1089		389 698

Figure 65. Assets page

Only most likely

This toggle lets you filter the view to show only the assets the match the criteria that you have set for likelihood threshold.

Likelihood threshold settings

Likelihood threshold is a value between 0.1 and 1.0 where 1.0 represents the maximum likelihood of the *Common Vulnerabilities and Exposures (CVE)* to be present. Likelihood is the confidence of the software's correct assignment of a *CPE* to the hardware of the monitored asset. The higher the likelihood, the higher the software's confidence that the vulnerabilities assigned to an asset are in fact are relevant to that asset. **Likelihood threshold** is the minimum likelihood a vulnerability needs in order for it to be shown in this page when the **Only most likely** toggle is set to on. As a guideline, we suggest that you use:

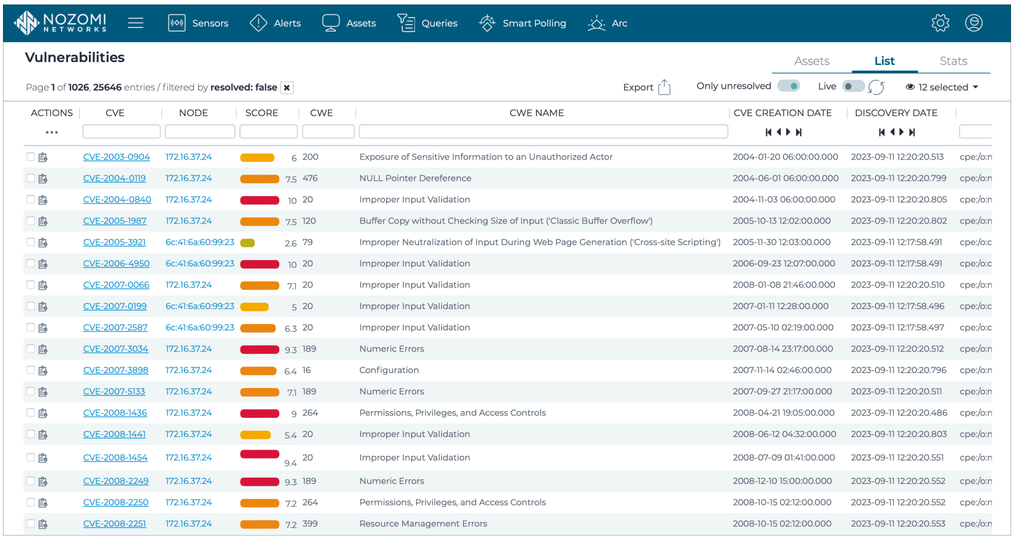
- 0.8 for a high level of confidence
- 0.5 for a medium level of confidence
- 0.3 for a low level of confidence

Live / refresh

The **Live** ● ↻ icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

List

*The **List** page shows a comprehensive list of vulnerabilities in the environment. This lets you perform global, in-depth analysis.*



Vulnerabilities

Page **1** of **1026**, **25646** entries / filtered by **resolved: false** ✖

ACTIONS	CVE	NODE	SCORE	CWE	CWE NAME	CVE CREATION DATE	DISCOVERY DATE	
☐	CVE-2003-0904	172.16.37.24	6	200	Exposure of Sensitive Information to an Unauthorized Actor	2004-01-20 06:00:00.000	2023-09-11 12:20:20.513	cpe:/o:n
☐	CVE-2004-0119	172.16.37.24	7.5	476	NULL Pointer Dereference	2004-06-01 06:00:00.000	2023-09-11 12:20:20.799	cpe:/o:n
☐	CVE-2004-0840	172.16.37.24	10	20	Improper Input Validation	2004-11-03 06:00:00.000	2023-09-11 12:20:20.805	cpe:/o:n
☐	CVE-2005-1987	172.16.37.24	7.5	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2005-10-13 12:02:00.000	2023-09-11 12:20:20.802	cpe:/o:n
☐	CVE-2005-3921	6c:41:6a:60:99:23	2.6	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2005-11-30 12:03:00.000	2023-09-11 12:17:58.491	cpe:/o:c
☐	CVE-2006-4950	6c:41:6a:60:99:23	10	20	Improper Input Validation	2006-09-23 12:07:00.000	2023-09-11 12:17:58.491	cpe:/o:c
☐	CVE-2007-0066	172.16.37.24	7.1	20	Improper Input Validation	2008-01-08 21:46:00.000	2023-09-11 12:20:20.510	cpe:/o:n
☐	CVE-2007-0199	6c:41:6a:60:99:23	5	20	Improper Input Validation	2007-01-11 12:28:00.000	2023-09-11 12:17:58.496	cpe:/o:c
☐	CVE-2007-2587	6c:41:6a:60:99:23	6.3	20	Improper Input Validation	2007-05-10 02:19:00.000	2023-09-11 12:17:58.497	cpe:/o:c
☐	CVE-2007-3034	172.16.37.24	9.3	189	Numeric Errors	2007-08-14 23:17:00.000	2023-09-11 12:20:20.512	cpe:/o:n
☐	CVE-2007-3898	172.16.37.24	6.4	16	Configuration	2007-11-14 02:46:00.000	2023-09-11 12:20:20.796	cpe:/o:n
☐	CVE-2007-5133	172.16.37.24	7.1	189	Numeric Errors	2007-09-27 21:17:00.000	2023-09-11 12:20:20.511	cpe:/o:n
☐	CVE-2008-1436	172.16.37.24	9	264	Permissions, Privileges, and Access Controls	2008-04-21 19:05:00.000	2023-09-11 12:20:20.486	cpe:/o:n
☐	CVE-2008-1441	172.16.37.24	5.4	20	Improper Input Validation	2008-06-12 04:32:00.000	2023-09-11 12:20:20.803	cpe:/o:n
☐	CVE-2008-1454	172.16.37.24	9.4	20	Improper Input Validation	2008-07-09 01:41:00.000	2023-09-11 12:20:20.551	cpe:/o:n
☐	CVE-2008-2249	172.16.37.24	9.3	189	Numeric Errors	2008-12-10 15:00:00.000	2023-09-11 12:20:20.552	cpe:/o:n
☐	CVE-2008-2250	172.16.37.24	7.2	264	Permissions, Privileges, and Access Controls	2008-10-15 02:12:00.000	2023-09-11 12:20:20.552	cpe:/o:n
☐	CVE-2008-2251	172.16.37.24	7.2	399	Resource Management Errors	2008-10-15 02:12:00.000	2023-09-11 12:20:20.553	cpe:/o:n

Figure 66. List page

Export

The **Export** icon lets you export the current list in either *CSV* or Microsoft Excel format.

Only resolved

This lets you show only `Unresolved` vulnerabilities. Vulnerability status options are:

- `Unresolved`
- `Mitigated`
- `Accepted`

`Mitigated` and `Accepted` lead to a resolution status that equals true.

Live / refresh

The **Live** icon lets you change live view on, or off. When live mode is on, the page will refresh approximately every five seconds.

Column selection

The columns selection icon lets you choose which columns to show or hide.

Stats

*The **Stats** page shows high level information in a graphical format that shows the top common platform enumerations (CPEs), common vulnerabilities and exposures (CVEs), and common weakness enumerations (CWEs).*

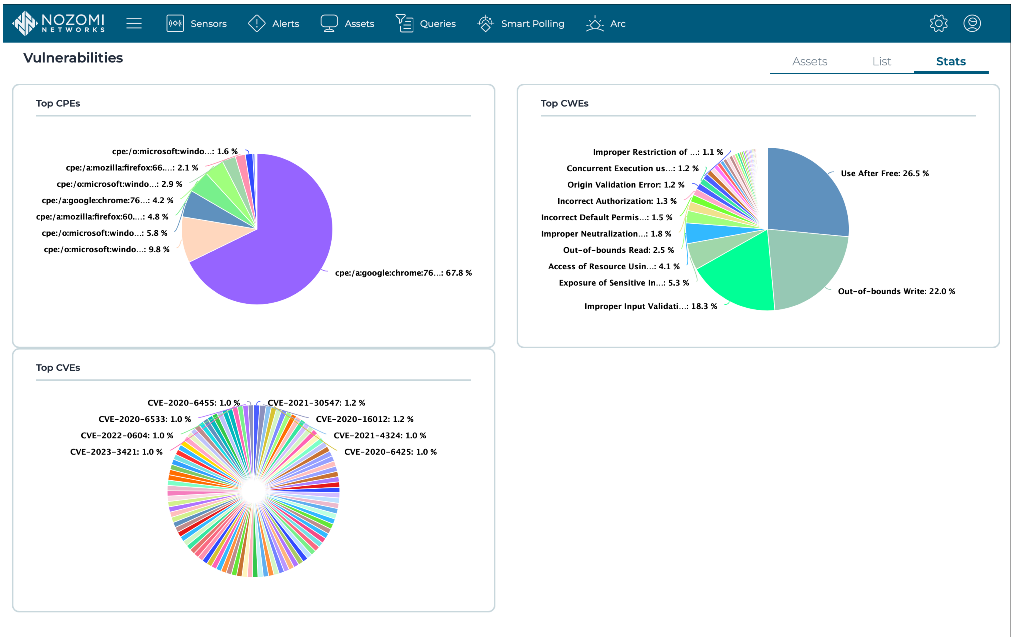

NOZOMI NETWORKS
Sensors
Alerts
Assets
Queries
Smart Polling
Arc
Vulnerabilities
Assets
List
Stats
Top CPEs
cpe:/o:microsoft:windo…: 1.6 %
cpe:/a:mozilla:firefox:66.…: 2.1 %
cpe:/o:microsoft:windo…: 2.9 %
cpe:/a:google:chrome:76…: 4.2 %
cpe:/a:mozilla:firefox:60.…: 4.8 %
cpe:/o:microsoft:windo…: 5.8 %
cpe:/o:microsoft:windo…: 9.8 %
cpe:/a:google:chrome:76…: 67.8 %
Top CWEs
Improper Restriction of …: 1.1 %
Concurrent Execution us…: 1.2 %
Origin Validation Error: 1.2 %
Incorrect Authorization: 1.3 %
Incorrect Default Permis…: 1.5 %
Improper Neutralization…: 1.8 %
Out-of-bounds Read: 2.5 %
Access of Resource Usin…: 4.1 %
Exposure of Sensitive In…: 5.3 %
Improper Input Validati…: 18.3 %
Use After Free: 26.5 %
Out-of-bounds Write: 22.0 %
Top CVEs
CVE-2020-6455: 1.0 %
CVE-2021-30547: 1.2 %
CVE-2020-6533: 1.0 %
CVE-2020-16012: 1.2 %
CVE-2022-0604: 1.0 %
CVE-2021-4324: 1.0 %
CVE-2023-3421: 1.0 %
CVE-2020-6425: 1.0 %

Figure 67. Stats page

Top CPEs

This section shows the:

- Title of vulnerability
- Percentage of the total vulnerabilities
- Actual count of that vulnerability

Top CWEs

This section shows the:

- Title of vulnerability
- Percentage of the total vulnerabilities
- Actual count of that vulnerability

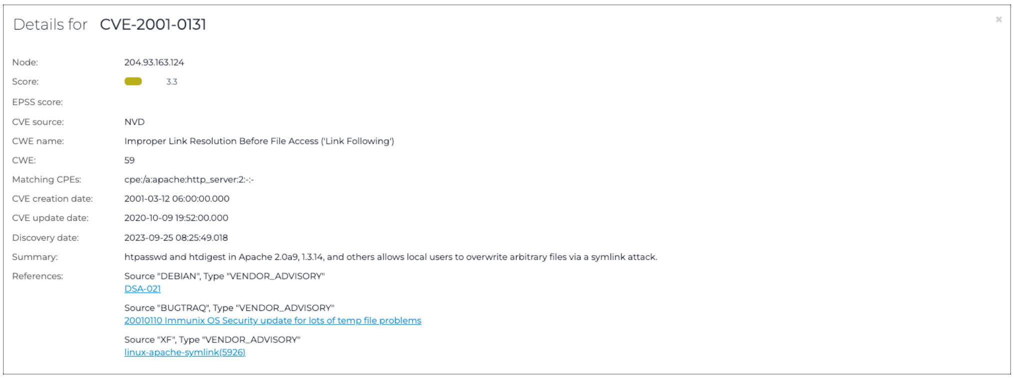
Top CVEs

This section shows the:

- Title of vulnerability
- Date of vulnerability type
- Percentage of the total vulnerabilities
- Actual count of that vulnerability

Details page

The details page shows you all the details for the related vulnerability.



Details for CVE-2001-0131

Node:	204.93.163.124
Score:	🟨 3.3
EPSS score:	
CVE source:	NVD
CWE name:	Improper Link Resolution Before File Access ('Link Following')
CWE:	59
Matching CPEs:	cpe:/a:apache:http_server:2:-:-
CVE creation date:	2001-03-12 06:00:00.000
CVE update date:	2020-10-09 19:52:00.000
Discovery date:	2023-09-25 08:25:49.018
Summary:	htpasswd and htdigest in Apache 2.0a9, 1.3.14, and others allows local users to overwrite arbitrary files via a symlink attack.
References:	Source "DEBIAN", Type "VENDOR_ADVISORY" DSA-021 Source "BUGTRAQ", Type "VENDOR_ADVISORY" 20010110 Immunix OS Security update for lots of temp file problems Source "XF", Type "VENDOR_ADVISORY" linux-apache-symlink(5926)

Figure 68. Details page

Chapter 14. Administration

Administration page

The administration page lets a user with administrator privileges configure settings and do other tasks.

For more details, see the Guardian **Administrator Manual**.

Chapter 15. Personal settings

Personal settings

The personal settings page lets you do actions that are specific to your profile.

General

You can select the 👤 icon to access the personal settings menu.

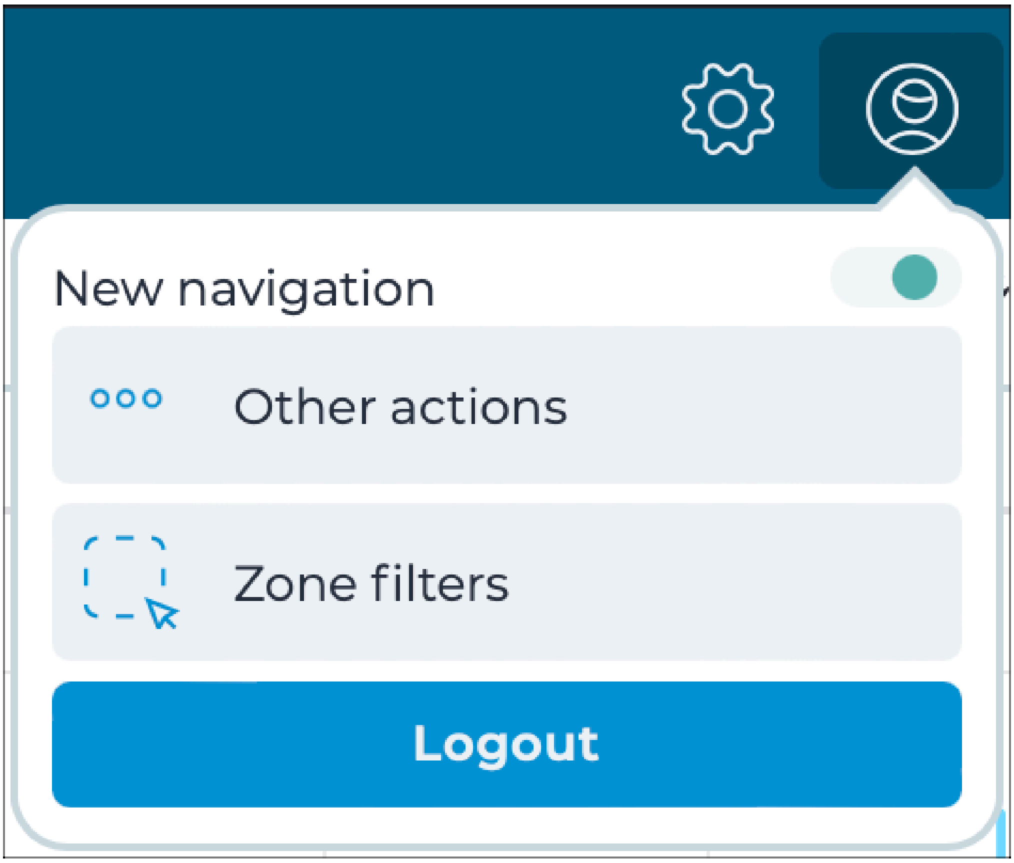


Figure 69. Personal settings menu

The personal settings page has these two sections:

- Other actions
- Zone filters (on page 254)

Logout

A button in the personal settings menu lets you log out of the software.

Other actions

Change your password

The profile settings menu lets you change your password.

Procedure

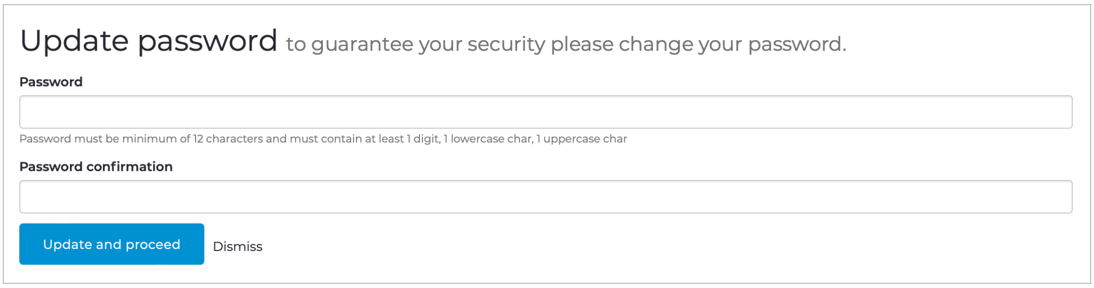
1. In the top navigation bar, select 👤

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Change password**.

   Result: A dialog shows.

4. In the **Password** field, enter a new password.



Update password to guarantee your security please change your password.

Password

Password must be minimum of 12 characters and must contain at least 1 digit, 1 lowercase char, 1 uppercase char

Password confirmation

5. In the **Password confirmation** field, enter the password again.
6. Select **Update and proceed**.

Results

Your password has been changed.

Edit an OpenAPI key

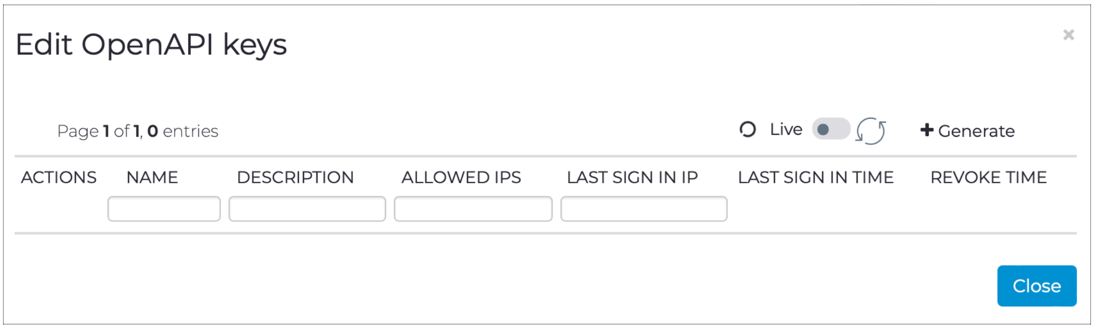
The profile settings menu lets you edit your OpenAPI keys.

Procedure

1. In the top navigation bar, select

   Result: A menu shows.
2. Select **Other actions**.
3. Select **Edit OpenAPI keys**.

   Result: A dialog shows.
4. Edit the OpenAPI keys as necessary.



Edit OpenAPI keys

Page **1** of **1**, **0** entries

ACTIONS	NAME	DESCRIPTION	ALLOWED IPS	LAST SIGN IN IP	LAST SIGN IN TIME	REVOKE TIME

5. Select **Close**.

Results

Your OpenAPI keys have been edited.

Generate an OpenAPI key

The profile settings menu lets you generate an OpenAPI key.

Procedure

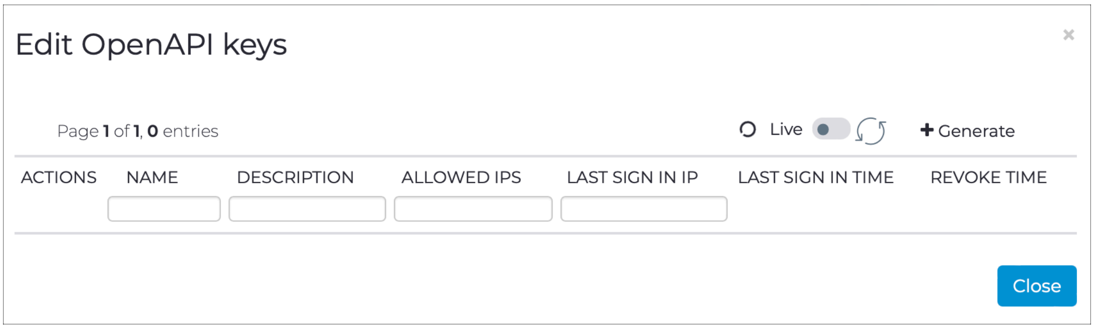
1. In the top navigation bar, select ☺

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Edit OpenAPI keys**.

   Result: A dialog shows.

4. In the top right, select **+ Generate**.



Edit OpenAPI keys ×

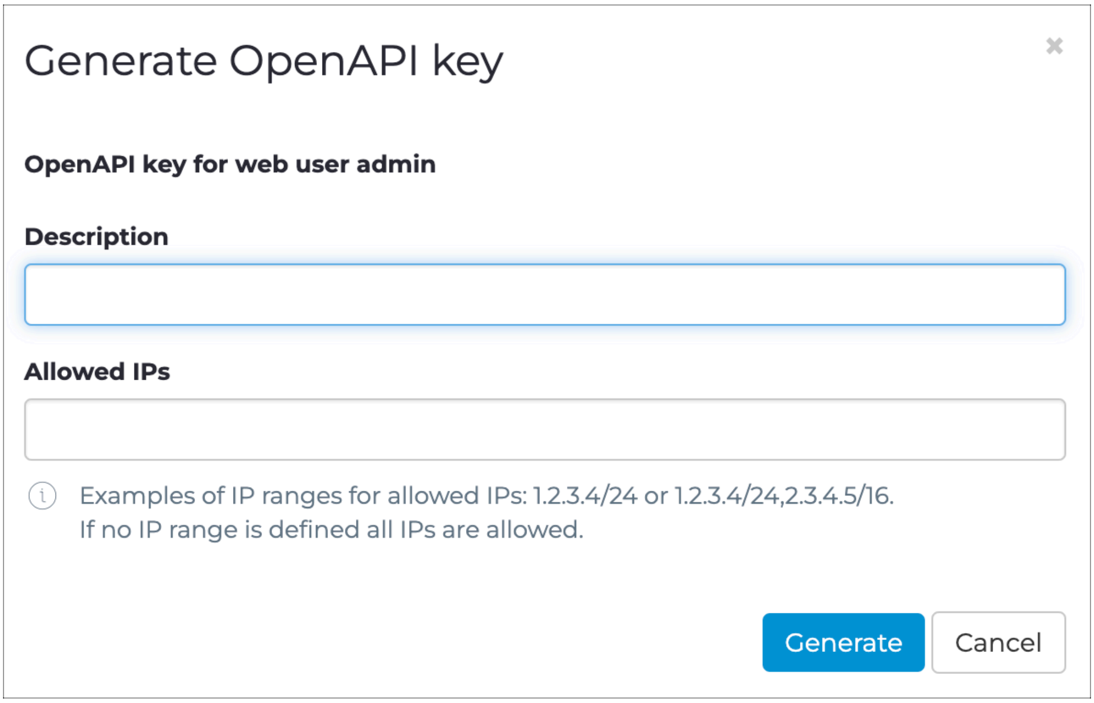
Page **1** of **1**, **0** entries ○ Live ● + Generate

ACTIONS	NAME	DESCRIPTION	ALLOWED IPS	LAST SIGN IN IP	LAST SIGN IN TIME	REVOKE TIME

Close

   Result: A dialog shows.

5. In the **Description** field, enter a description for the OpenAPI key.



Generate OpenAPI key ×

OpenAPI key for web user admin

Description

Allowed IPs

ⓘ Examples of IP ranges for allowed IPs: 1.2.3.4/24 or 1.2.3.4/24,2.3.4.5/16.
If no IP range is defined all IPs are allowed.

Generate Cancel

6. In the **Allowed IPs** field, enter the details of the allowed *IP* addresses.
7. Select **Generate**.

Results

Your OpenAPI key has been generated.

Clear your personal settings

The profile settings menu lets you clear your personal settings that are stored in the local browser local.

Procedure

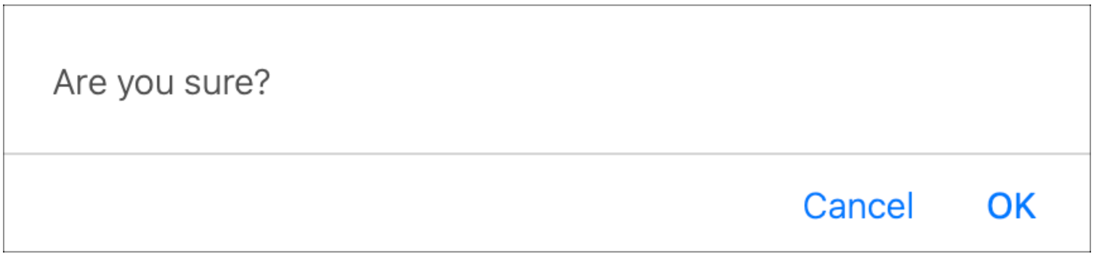
1. In the top navigation bar, select 👤

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Clear personal settings**.

   Result: A dialog shows.

4. Select **OK**.



Are you sure?

Results

Your personal settings have been cleared from the local browser.

Request a continuous trace

The profile settings menu lets you request a trace that has only the disk size constraint.

About this task

The maximum count of packets, and the run time, constrain regular traces. For example, being constrained to capture at most 1000 packets in no more than one minute. A continuous trace does not have such limits. It collects packets without constraints, as long as the disk has free space to store the captured traffic. The packets are then saved as individual files that are 100 *megabyte (MB)* in size.

Procedure

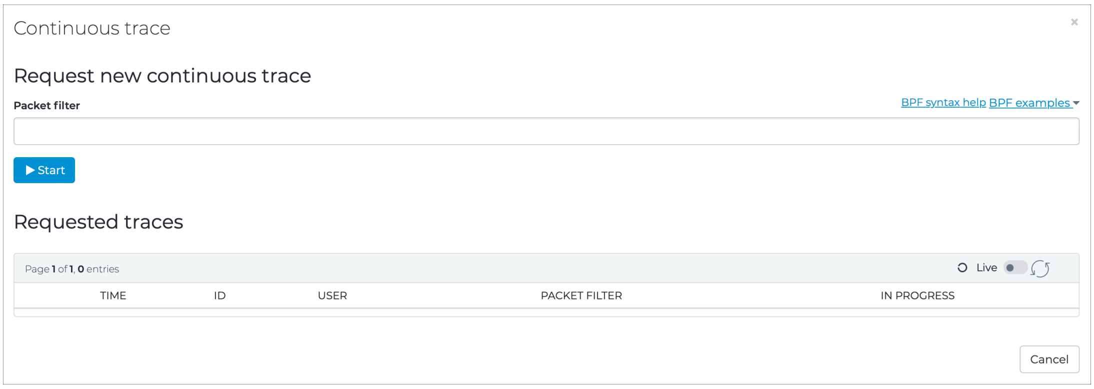
1. In the top navigation bar, select ☺

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Continuous trace**.

   Result: A dialog shows.

4. In the **Packet filter** field, enter a *BPF* filter.


Continuous trace

Request new continuous trace

Packet filter

BPF syntax help BPF examples ▾

▶ Start

Requested traces

Page 1 of 1, 0 entries Live

TIME	ID	USER	PACKET FILTER	IN PROGRESS

Cancel

5. Select **Start**.

Results

The trace has been requested.

Request a custom trace

The profile settings menu lets you request a trace specifying a custom packet filter.

Procedure

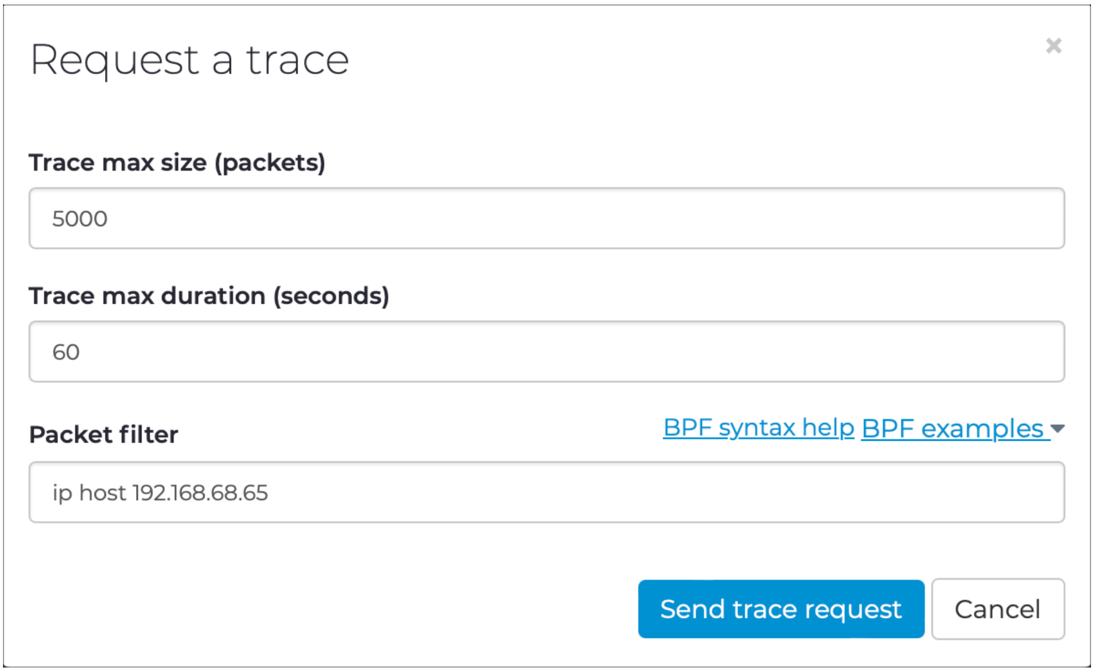
1. In the top navigation bar, select ☺

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Request custom trace**.

   Result: A dialog shows.

4. To set the maximum packet size, in the **Trace max size (packets)** field, enter a value.



Request a trace

Trace max size (packets)

5000

Trace max duration (seconds)

60

Packet filter

ip host 192.168.68.65

> **Note:**
> The default size is 5000 packets.

5. To set the maximum duration of the trace, in the **Trace max duration (seconds)** field, enter a value.

> **Note:**
> The default value is 60 seconds.

6. **Note:**

   The **Packet filter** field is automatically populated with a *BPF* that captures the packets to/from the selected node, but you can customize this.

   If necessary, customize this field.

   Note:

   You can select **BPF syntax help** to show more information on *BPF* syntax.

   Note:

   You can select **BPF examples** to see some examples.

7. Select **Send trace request**.

Results

The trace has been requested.

Show requested traces

The profile settings menu lets you show all the traces that you have requested.

Procedure

1. In the top navigation bar, select 👤

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Show requested traces**.

Results

All your requested traces show.

Download a requested trace

Once you have requested a trace, and it is ready, you can download it.

Procedure

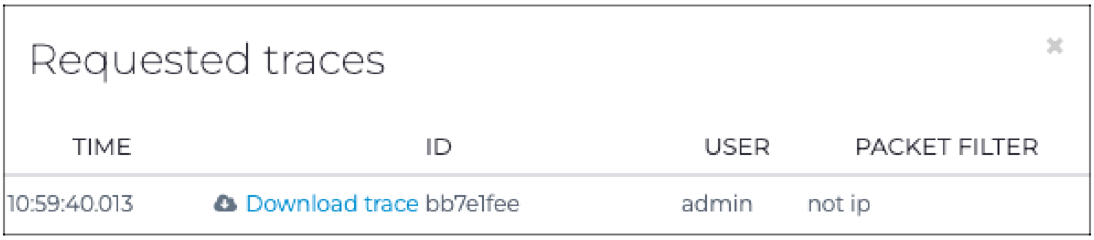
1. In the top navigation bar, select ☺

   Result: A menu shows.

2. Select **Other actions**.
3. Select **Show requested traces**.

   Result: All your requested traces show.

4. For the applicable trace, select **Download trace**.



Requested traces ×

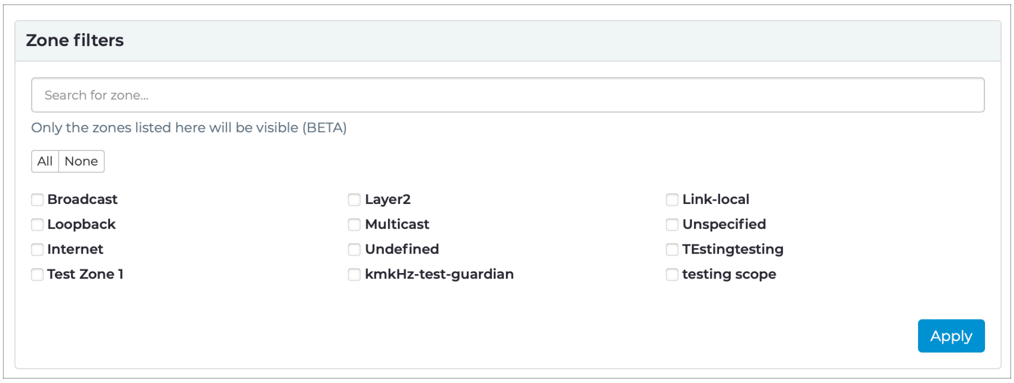
TIME	ID	USER	PACKET FILTER
10:59:40.013	Download trace bb7e1fee	admin	not ip

Results

The trace has been downloaded.

Zone filters

The personal settings menu lets you filter zones.



Zone filters

Search for zone...

Only the zones listed here will be visible (BETA)

□ Broadcast
□ Loopback
□ Internet
□ Test Zone 1
□ Layer2
□ Multicast
□ Undefined
□ kmkHz-test-guardian
□ Link-local
□ Unspecified
□ TEstingtesting
□ testing scope

Figure 70. Zone filters page

Glossary

Amazon Machine Image

An AMI is a type of virtual appliance that is used to create a virtual machine for the Amazon Elastic Compute Cloud (EC2), and is the basic unit of deployment for services that use EC2 for delivery.

Amazon Web Services

AWS is a subsidiary of the Amazon company that provides on-demand cloud computing platforms governments, businesses, and individuals on a pay-as-you-go basis.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

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.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

Central Management Console

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

Central Processing Unit

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

Certificate Authority

A certificate, or certification authority (CA) is an organization that stores, signs, and issues digital certificates. In cryptography, a digital certificate certifies the ownership of a public key by the named subject of the certificate.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Platform Enumeration

CPE is a structured naming scheme for information technology (IT) systems, software, and packages. CPE is based on the generic syntax for Uniform Resource Identifiers (URI) and includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

Common Weakness Enumeration

CWE is a category system for software and hardware weaknesses and vulnerabilities. It is a community project with the aim to understand flaws in software and hardware and create automated tools that can be used to identify, fix, and prevent those flaws.

Configuration file

A CFG file is a configuration, or config, file. They are files that are used to configure the parameters and initial settings for a computer program.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

ESXi

VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS). Instead, it includes and integrates vital OS components, such as a kernel.

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.

File Transfer Protocol

FTP is a standard communication protocol that is used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture that uses separate control and data connections between the client and the server.

Fully qualified domain name

An FQDN is a complete and specific domain name that specifies the exact location in the hierarchy of the Domain Name System (DNS). It includes all higher-level domains, typically consisting of a host name and domain name, and ends in a top-level domain.

Gigabit per second

Gigabit per second (Gb/s) is a unit of data transfer rate equal to: 1,000 Megabits per second.

Gigabyte

The gigabyte is a multiple of the unit byte for digital information. One gigabyte is one billion bytes.

Graphical User Interface

A GUI is an interface that lets humans interact with electronic devices through graphical icons.

Graphics Interchange Format

GIF is a bitmap image format that is widely used on the internet.

High Availability

High Availability is a mode that permits the CMC to replicate its own data on another CMC.

Host-based intrusion-detection system

HIDS is an internal Nozomi Networks solution that uses sensors to detect changes to the basic firmware image, and record the change.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

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.

Industrial Internet of Things

The IIoT is a name for interconnected devices, sensors, instruments, which are networked together with industrial applications. This connectivity allows for analysis and data collection, which can facilitate improvements in efficiency and productivity.

Internet Control Message Protocol

ICMP is a supporting protocol in the internet protocol suite. Network devices use it to send error messages and operational information to indicate success or failure when communicating with another IP address. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems.

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.

Intrusion Detection System

An intrusion detection system (IDS), which can also be known as an intrusion prevention system (IPS) is a software application, or a device, that monitors a computer network, or system, for malicious activity or policy violations. Such intrusion activities, or violations, are typically reported either to a system administrator, or collected centrally by a security information and event management (SIEM) system.

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.

Joint Photographic Experts Group

JPEG, or JPG, is a method of lossy compression that is used for digital images. The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality.

Lightweight Directory Access Protocol

LDAP is an open, vendor-neutral, industry standard application protocol that lets you access and maintain distributed directory information services over an internet protocol (IP) network.

Lightweight Directory Access Protocol Secure

LDAP over SSL or Secure LDAP is the secure version of LDAP.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

National Vulnerability Database

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Network Address Translation

NAT is a method of mapping an internet protocol (IP) address space into another one. This is done by modifying network address information in the IP header of packets while in transit across a traffic routing device.

Network Interface Controller

A network interface controller (NIC), sometimes known as a network interface card, is a computer hardware component that lets a computer connect to a computer network.

Network Time Protocol

The NTP is a networking protocol to synchronize clocks between computer systems over variable-latency, packet-switched data networks.

Nozomi Networks Operating System

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

Nozomi Networks Query Language (N2QL)

N2QL is the language used in queries in Nozomi Networks software.

Open Virtual Appliance

An OVA file is an open virtualization format (OVF) directory that is saved as an archive using the .tar archiving format. It contains files for distribution of software that runs on a virtual machine. An OVA package contains a .ovf descriptor file, certificate files, an optional .mf file along with other related files.

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).

Packet Capture Next Generation

A pcapNg is the latest version of a pcap file, an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Network Graphics

PNG is a raster graphics file format that supports lossless data compression.PNG was developed as an improved, non-patented replacement for graphics interchange format (GIF).

Privacy-Enhanced Mail

PEM is a standard file format that is used to store and send cryptographic keys, certificates, and other data. It is based on a set of 1993 IETF standards.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

Protected Extensible Authentication Protocol

PEAP is a protocol that encloses the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

Random-access Memory

Computer memory that can be read and changed in any order. It is typically used to store machine code or working data.

Representational State Transfer

Representational State Transfer (REST) is an architectural style for designing networked applications. It uses stateless, client-server communication via standard HTTP methods (GET, POST, PUT, DELETE) to access and manipulate web resources represented in formats like JSON or XML.

Secure Copy Protocol

SCP is a protocol for the secure transfer of computer files between a local host and a remote host, or between two remote hosts. It is based on the secure shell (SSH) protocol.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Secure Sockets Layer

A secure sockets layer ensures secure communication between a client computer and a server.

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.

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism.

Simple File Transfer Protocol

SFTP was proposed as an unsecured file transfer protocol with a level of complexity intermediate between TFTP and FTP. It was never widely accepted on the internet.

Simple Mail Transfer Protocol

SMTP is an internet standard communication protocol that is used for the transmission of email. Mail servers and other message transfer agents use SMTP to send and receive mail messages.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

Simple Text Oriented Messaging Protocol

STOMP is a simple text-based protocol, for working with message-oriented middleware (MOM). It provides an interoperable wire format that allows STOMP clients to talk with any message broker supporting the protocol.

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.

Supervisory control and data acquisition

SCADA is a control system architecture which has computers, networked data communications and graphical user interfaces for high-level supervision of processes and machines. It also covers sensors and other devices, such as programmable logic controllers (PLC), which interface with process plant or machinery.

Text-based User Interface

In computing, a text-based (or terminal) user interfaces (TUI) is a retronym that describes a type of user interface (UI). These were common as an early method of human–computer interaction, before the more modern graphical user interfaces (GUIs) were introduced. Similar to GUIs, they might use the entire screen area and accept mouse and other inputs.

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.

Transmission Control Protocol

One of the main protocols of the Internet protocol suite.

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.

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.

Uninterruptible Power Supply

A UPS is an electric power system that provides continuous power. When the main input power source fails, an automated backup system continues to supply power.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Interface

An interface that lets humans interact with machines.

Variable

In the context of control systems, a variable can refer to process values that change over time. These can be temperature, speed, pressure etc.

Virtual DOM

A virtual DOM, or vdom, is a lightweight JavaScript representation of the Document Object Model (DOM). It is used in declarative web frameworks such as Elm, React, and Vue.js. It enables the updating of the virtual DOM is comparatively faster than updating the actual DOM.

Virtual Hard Disk

VHD is a file format that represents a virtual hard disk drive (HDD). They can contain what is found on a physical HDD, such as disk partitions and a file system, which in turn can contain files and folders. They are normally used as the hard disk of a virtual machine (VM). They are the native file format for Microsoft's hypervisor (virtual machine system), Hyper-V.

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).

Virtual Machine

A VM is the emulation or virtualization of a computer system. VMs are based on computer architectures and provide the functionality of a physical computer.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.