NOZOMI NETWORKS

Smart Polling
User Guide

2026-08-07

Legal notices

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

Copyright

Copyright © 2013-2026, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

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

Contents

Chapter 1. Introduction 7
About this guide 9
Smart Polling 10
Smart Polling plans 12
Chapter 2. Requirements 13
Smart Polling license 15
Network and credential requirements 16
Chapter 3. Smart Polling in Vantage 17
Overview 20
Plan creation 22
Automatically add a plan 26
Manually add a plan 30
Centralized plan management 36
Actions menu 39
Smart Polling results 43
Activity Log 45
Chapter 4. Smart Polling in CMC 47
Plans 50
Node points 51
Chapter 5. Smart Polling in Guardian 53
Plans 56
Progressive mode enablement in Guardian 57
Enable progressive mode in Guardian 58
Create a Smart Polling plan in Guardian 59
Edit a Smart Polling plan in Guardian 61
Add a network node to a Smart Polling plan 62
Add a node from the Network page 64
Edit the run interval of a progressive Smart Polling plan in Guardian 65
Node points 66
Settings 67
Log level customization 68
View the enriched information history for a node 69
Chapter 6. Smart Polling in Arc 71
Chapter 7. Strategies 75
Strategies overview 77
Advantech EdgeLink 78
Advantech EKI HTTPS 79

AutomationDirect Productivity 80
Avalue UWB TCP 81
Axis HTTP(S) 82
BACnet 83
Beckhoff 85
Belden/Hirschmann Rail Data Diode HTTP(S) 86
Bently Nevada 87
Bosch RCP+ cameras HTTP(S) 88
Dahua DHIP/DVRIP devices 89
Eaton EasyProtocol 90
EtherNet/IP 91
GE MDS TD Series Telnet 92
GE Telnet 93
Bosch Rexroth HTTP(S) 94
Cognex HTTP(S) 95
Fanuc HTTP(S) 96
GE Healthcare HTTP 97
GE Grid Solutions HTTP 98
Lanner BMC HTTP(S) 99
Schneider HTTP(S) 100
Sewio HTTP(S) 101
Tyan BMC HTTP(S) 102
Ubisense HTTP(S) 103
Inaba Choco Tei HTTP 104
Mitsubishi Electric MELSOFT 105
IEC 61850-8-1 (MMS) 107
Modbus 108
Moxa 109
Moxa HTTP(S) 110
ONVIF HTTP(S) 111
Owl OPDS SSH 112
Phoenix Contact FL SWITCH TSN 2000 Series HTTP(S) 113
Phoenix Contact WP6000 HTTPS 114
Phoenix Contact mGuard 115
Phoenix Contact PLCNext HTTPS 116
Reolink Baichuan 117
Siemens STEP7 118
SEL telnet 120
SEL Axion HTTPS 121
Sensor Net Connect 122
Shelly mDNS 123
Siemens SIPROTEC HTTP(S) 124
SNMP 125
SSH 128

Tattile NTCP....130
Tyco exacqVision....131
UPnP....132
Wago Management....133
WinRM....134
WMI....135
Zettler/Ezcare TCP Gateway HTTP....136
Glossary....137

Chapter 1. Introduction

About this guide

Configure, manage, and monitor Smart Polling in Vantage, Central Management Console (CMC), Guardian, and Arc.

Who should use this guide

This guide is for network administrators and security professionals who configure and manage Smart Polling in their Nozomi Networks deployment.

What you learn

This guide covers the following topics:

- **Requirements**: License requirements for Smart Polling
- **Smart Polling in Vantage**: Centrally manage Smart Polling across sensors in Vantage
- **Smart Polling in CMC**: View Smart Polling information across sensors in *Central Management Console (CMC)*
- **Smart Polling in Guardian**: Manage and monitor Smart Polling in Guardian
- **Smart Polling in Arc**: Run Smart Polling on Arc sensors
- **Strategies**: Reference information for all Smart Polling strategies

Smart Polling

Smart Polling uses active polling methods to collect network device attributes that are not present in network traffic. This enables accurate device vulnerability analysis, and enhances their identification on the Nozomi Networks platform.

Overview

Smart Polling™ extends the asset identification capability in Arc and Guardian. To do this, it adds active polling methods that provide more granular information about devices in your network. This non-invasive technique actively collects additional device details, such as:

- *operating system (OS)*
- Firmware versions
- Patch levels and more

With this additional device information, the platform creates a more precise list of vulnerabilities affecting your environment and a richer list of the devices in it.

Smart Polling is built around the concepts of identities, strategies, and plans. An identity is a relationship between a list of target devices and their matching credentials. A strategy defines how the platform will poll devices which is based on their communication protocols. For example, the SNMPv3 strategy uses the SNMPv3 protocol to poll devices. This ensures devices are polled appropriately and safely. A plan is the combination of a strategy, one or more identities, additional security settings, and the polling interval or schedule. The recommended mode for Smart Polling is Progressive Mode. When enabled, Guardian and/or Arc automatically creates Smart Polling plans for the user. This provides quicker visibility with minimal or no configuration.

Alternatively, you can select what devices you would like to poll, and when. When run successfully, strategies extract information that shows in the **Smart Polling** page. You can also view the device details throughout the platform.

Discovery and Smart Polling

Discovery and Smart Polling complement each other for accurate device profiling and risk assessment. Together, they detect and enrich devices without impacting network stability.

Discovery identifies devices on the network. Smart Polling then uses protocol-specific, low-impact methods to retrieve firmware versions, configurations, vulnerabilities, and other details unavailable through traffic monitoring.

Triggers

Smart Polling can be triggered in two ways:

- Through a Smart Polling plan: If devices match an active plan in Arc or Guardian
- After a successful Discovery: Newly discovered devices that match a Smart Polling strategy are automatically polled

Active sensor

Smart Polling on Guardian selects the sensor or sensors for execution based on the `capture_devices` field of the polled node. Smart Polling will engage the corresponding sensors. When at least one successful execution occurs from a sensor, Smart Polling remembers to use that sensor in future executions. If a future execution fails, or Smart Polling records no executions for more than a week, it reverts to the sensors in the `capture_devices` field.

To add a sensor to the applicable sensors for a node, you can use the Guardian *command-line interface (CLI)* to modify the `capture_devices` field. For example, to add an Arc to the applicable sensors for a node, use `vi node 192.168.1.1 capture_device arc[1e6a174c]`, where `192.168.1.1` is the node *identifier (ID)* and the value in brackets is the first eight characters of the Arc sensor's *ID*. The manually added sensor is then added to the node's `capture_devices` list, and may be chosen according to the algorithm described above. If a node is only visible to Arc sensors but you want to use Guardian instead, use `vi node 192.168.1.1 capture_device guardian`.

The *OS* of the sensor that polls the node decides which network interface to use based on the routing table. All Smart Polling strategies are based on the *internet protocol (IP)*, which means that all routing decisions are delegated to the *OS*.

Smart Polling safety

Smart Polling uses protocols that are designed to be non-intrusive and have no adverse effect on devices operating normally. However, these assurances apply only to devices in a functional, non-overloaded state. A device that is already experiencing severe resource exhaustion, degraded performance, or an active fault condition may not be suitable for monitoring. Even lightweight polling can trigger unpredictable behavior on a compromised device, up to and including loss of connectivity or an unplanned restart. Before adding a device to active monitoring, verify that it is operating within its normal parameters.

Smart Polling plans

Smart Polling uses polling plans to define which devices to query, what information to collect, and when to perform polling activities.

Polling plans

A polling plan defines a set of devices to query and the queries to execute. You can create and manage Smart Polling plans in Vantage, Guardian, and *CMC*. Arc sensors run Smart Polling, but their plans are managed centrally rather than on the sensor. There are two ways to create plans:

- **Progressive**
- **Manual**

Progressive

Progressive mode automates plan creation and execution. It polls devices with the correct parameters based on passively detected asset information. Smart Polling automatically identifies the optimal targets for polling based on discovered device characteristics.

Manual

Manual polling plans let you control polling activities. Create custom plans with specific device filters and query configurations.

Choose an approach

Use Progressive mode for automated polling based on discovered devices, or create manual plans for specific requirements. You can use both approaches.

Chapter 2. Requirements

Smart Polling license

Smart Polling requires a dedicated license. You can verify your license status from the Administration section of your Nozomi Networks product.

License requirements

A dedicated license is needed to enable the Smart Polling functionality. Contact your Nozomi Networks sales representative for licensing information.

Verify your license

To verify that your Smart Polling license is active:

- If you use Vantage, go to **Administration > Licenses**.
- If you use Guardian or *CMC*, go to **Administration > Updates and licenses**.
- If you use an Arc sensor, its Smart Polling licensed status is shown on the sensor, but the license itself is managed from the upstream Guardian, *CMC*, or Vantage.

Network and credential requirements

Besides a license, Smart Polling needs network access to target devices and credentials with the correct permissions to poll them.

Network access

The Arc sensor or Guardian must have network access to the devices you want to poll, and firewalls must allow the required traffic. Some devices also need a corresponding service or protocol enabled before Smart Polling can reach them, for example enabling WinRM on a Windows host or *simple network management protocol (SNMP)* on a network device.

Each strategy in Strategies (on page 77) lists the ports and any device-side configuration it requires.

Credentials and permissions

Some strategies require credentials with the correct scope to access target devices. Store and manage these credentials in **Credentials Manager**:

- If you use Guardian or *CMC*, find it under **Administration > Settings**.
- If you use Vantage, find it under **Organization settings**.
- If you use an Arc sensor, its credentials are managed from whichever upstream product manages that sensor: Guardian, *CMC*, or Vantage.

Each strategy in Strategies (on page 77) specifies the credential scope it requires.

Chapter 3. Smart Polling in Vantage

Smart Polling provides a centralized interface for creating, managing, and monitoring polling plans within your organization. It helps you streamline data collection and control monitoring activities from one location.

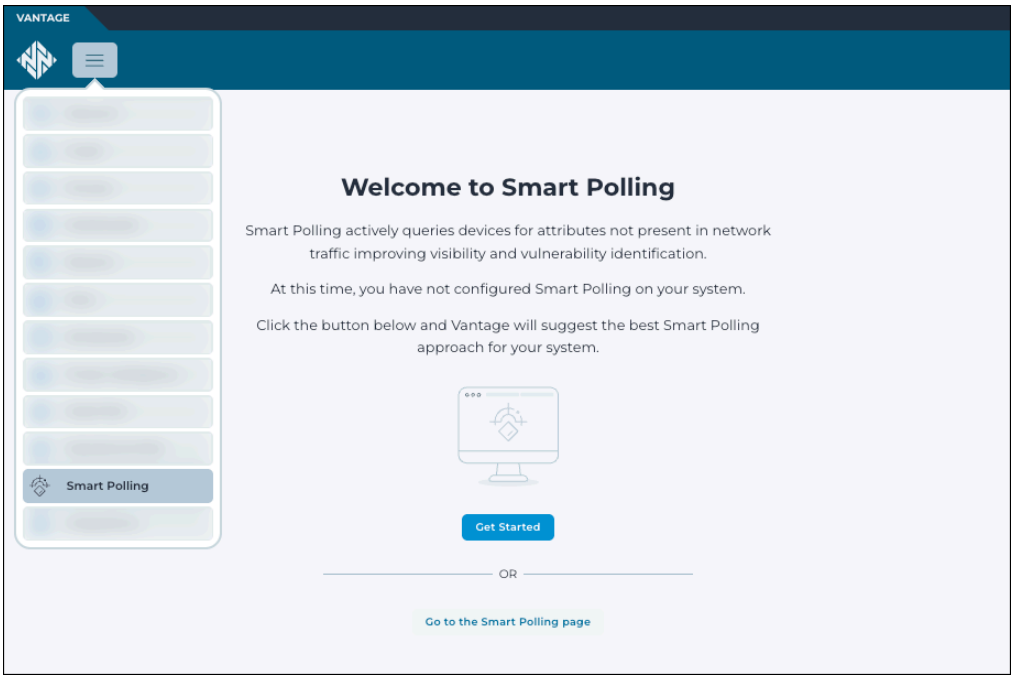


Figure 1. Smart Polling welcome page

The first time that you open the Smart Polling page, when no Smart Polling plans have been created for your organization, the welcome page shows.

The welcome page lets you choose from these two options:

- **Get Started** to Automatically add a Smart Polling plan from the onboarding page (on page 26)
- **Go to the Smart Polling page** to:
  - Add a Smart Polling plan that requires credentials (on page 30), or
  - Add a Smart Polling plan that does not require credentials (on page 33)

Once your organization has at least one Smart Polling plan, you no longer see the welcome page. Instead, the **Overview** page shows. Accept the suggestions in the plans list on this page to create progressive mode plans. For more details, see Overview (on page 20).

Vantage shows progressive plans from connected sensors and lets you merge duplicates into a single plan managed from Vantage. For more details, see Centralized plan management (on page 36).

Overview

Learn how Smart Polling plans are displayed, managed, and executed in the Vantage platform. This includes understanding plan statuses, how to add or search for plans, and how to interpret result data. Icons and table fields provide insight into device polling outcomes and plan performance. Plans can be defined in Vantage, but are executed in Guardian sensors, or Arc sensors that are connected to Guardian. Vantage receives the result of those executions via the usual synchronization process.

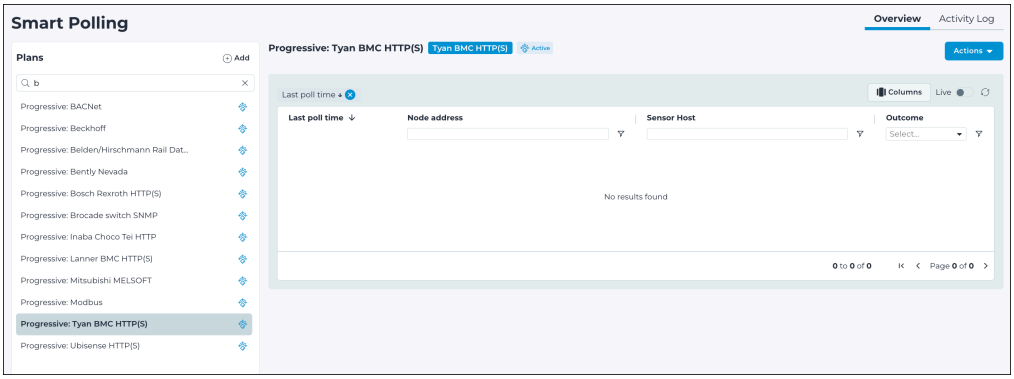


Figure 2. Populated Plans page

Plans

The **Plans** section shows a list of all the Smart Polling plans that have been added for your organization. The icons show the current status of the plan:

- : Active
- : Paused

Progressive plans from connected sensors are also shown here. You can merge duplicate progressive plans into a single plan managed from Vantage. For more details, see Centralized plan management (on page 36).

Add button

The **Add** icon lets you add a new Smart Polling plan.

Search field

The search field lets you easily find a specific Smart Polling plan.

Results

Once a Smart Polling plan has been executed, the results will show on the **Overview** page. When you select a specific plan, the table will show the:

- Status of the plan through the `ACTIVE` | `INACTIVE` indicator
- Result of the last polling of each node polled within the last two weeks

The table columns will show:

- **Node address**: The *IP* address of the node that was detected
- **Sensor Host**: The name of the sensor

- **Last poll time**: The time since the last execution of the plan for that node
- **Outcome**: The result of the last execution of the plan, which can be:
  - `Successful`: Smart Polling was able to poll the host and enrich the corresponding asset
  - `No connection`: Verify that the device is up, its services are running, that the sensor has a route to that host and no firewall is blocking the connection
  - `Missing credentials`: Add the credentials to the **Credentials Manager**
  - `Wrong credentials`: Update the credentials in the **Credentials Manager**
  - `Inconclusive`: This device is unsupported or only partly supported by Smart Polling
  - `Unsupported`: This strategy is not supported by the sensor that tried to poll the device
  - `Queued`: The sensor has not yet picked up the node for execution
  - `Denied`: The node lies in a subnet that Smart Polling does not have the permission to reach

For more details about the additional information that Smart Polling can provide, see Smart Polling results (on page 43).

Suggestions

Vantage regularly analyzes your organization and adds recommended Smart Polling plans to the **Suggestions** section based on the results. If there are no suggestions, this section will not show.

Plan creation

Learn how to create a Smart Polling plan by choosing a strategy, defining parameters, adding targets and credentials, and scheduling when data collection runs. Customize each step to control how and when your sensors gather information. Use recurrence or interval scheduling to automate plan execution.

Select the ⊕ **Add** icon to enter the plan creation wizard.

Strategy

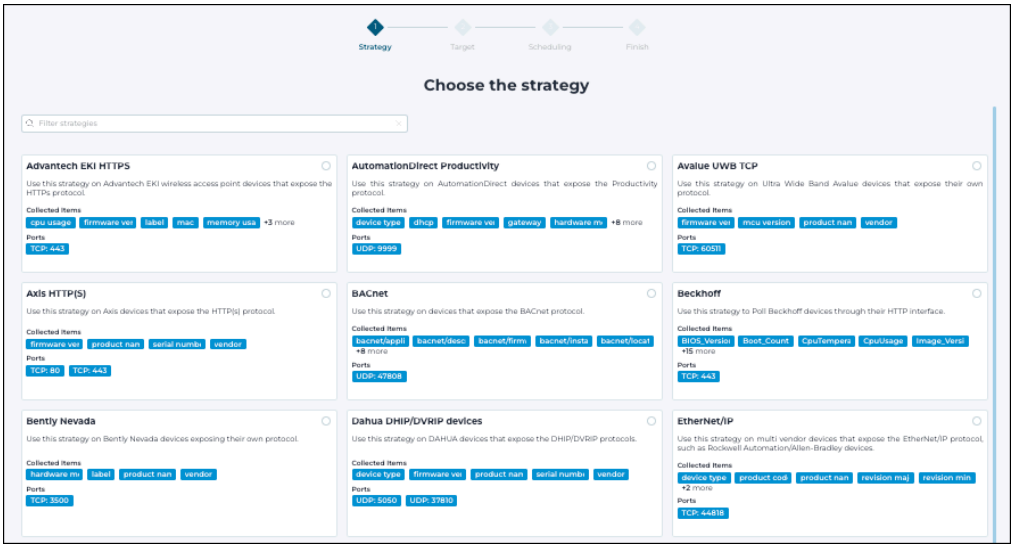


Figure 3. Choose the strategy page

Filter strategies: This field lets you enter text to easily find a specific strategy.

All available strategies show on the page with a summary. The summary section shows the:

- Name of the strategy
- A description of when it is useful to use the strategy
- The information that is collected
- Ports used

Parameters

Customize the plan with parameters used by the selected strategy, such as the port to use. Not all strategies accept parameters, in which case this step is skipped.

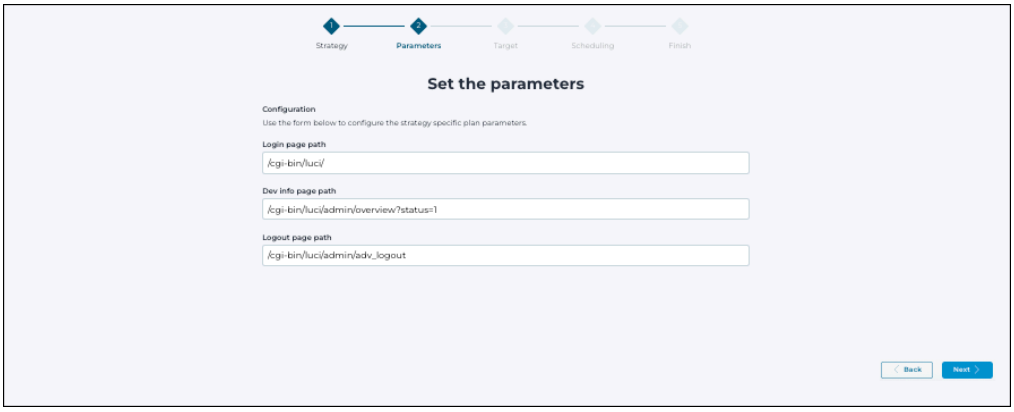


Figure 4. Parameters page

Target

Some of the strategies that are available require you to enter the related credentials. Therefore, there are two possible versions of the **Target** page that can show.

Figure 5. Target page (Query version shown)

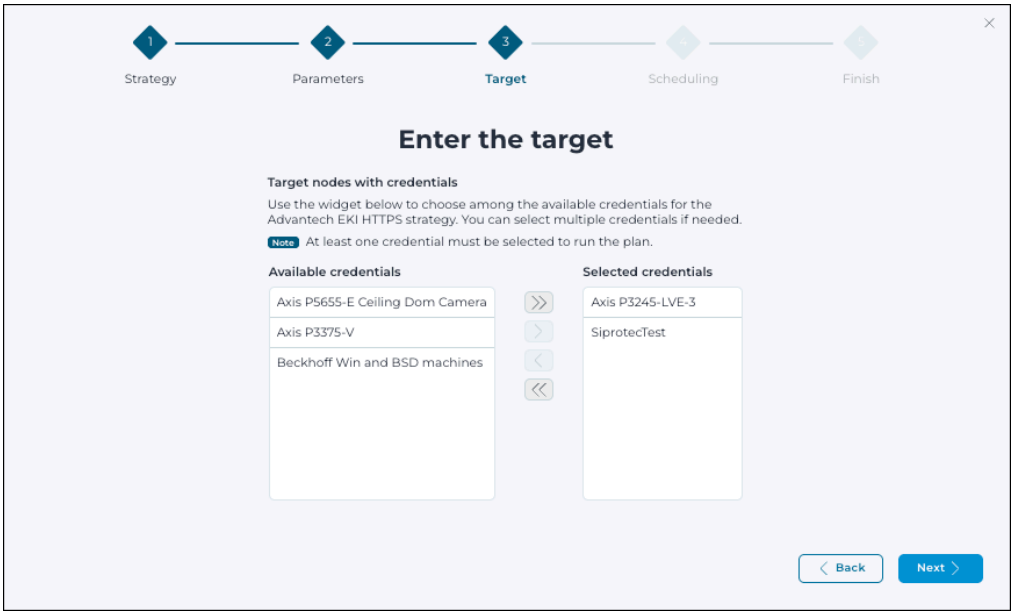


Figure 6. Target page (Credentials version shown)

For strategies that require credentials, you must select one, or more, of the available credentials that show in the panel on the left. To move the credentials to the panel on the right, you can use the:

- > icon to select one credential
- >> icon to select all credentials

Scheduling

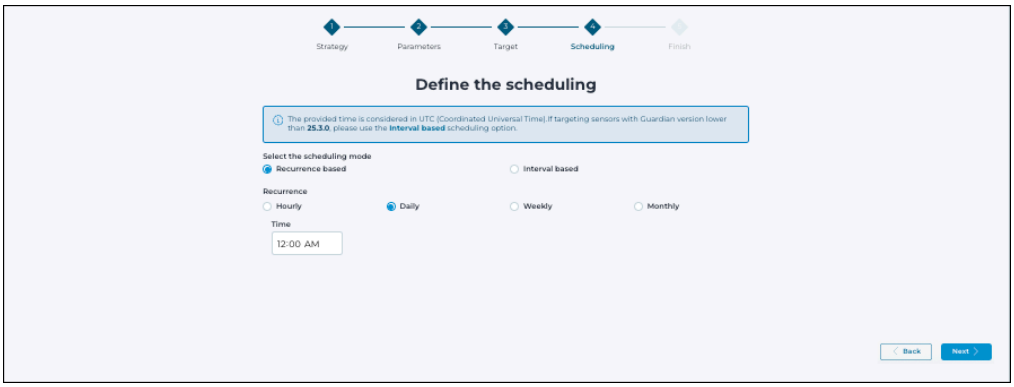


Figure 7. Scheduling page

Recurrence based: When this is selected, you can choose from these options:

- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**

Sensors that are *Nozomi Networks Operating System (N2OS)* v25.2.0 or lower do not fully support recurrence-based scheduling. However, if you have sensors with one of these older versions of *N2OS*, and you create a recurrence-based plan, there is a workaround. Under these circumstances, Vantage will still request that the sensor runs the plan at the desired frequency, but in a slightly different way. For example, if you choose the hourly-based scheduling, it will run the plan once an hour, but not necessarily at the minute that you specified. The same will happen if you selected the daily recurrence.

If you selected the weekly or monthly recurrence, the plan will be run once per week or month, regardless of whether you specified a single day or multiple days.

Time: You then must set the time that the Smart Polling plan will be executed. The time is set in *coordinated universal time (UTC)*.

Interval based: When this is selected, the sensors will run the plan immediately. Subsequently, it will run once at every interval. For example, if your interval is **Every 1 Day(s)**, and the current time is 10:15, then the plan will run immediately, and then every day at 10:15.

Finish

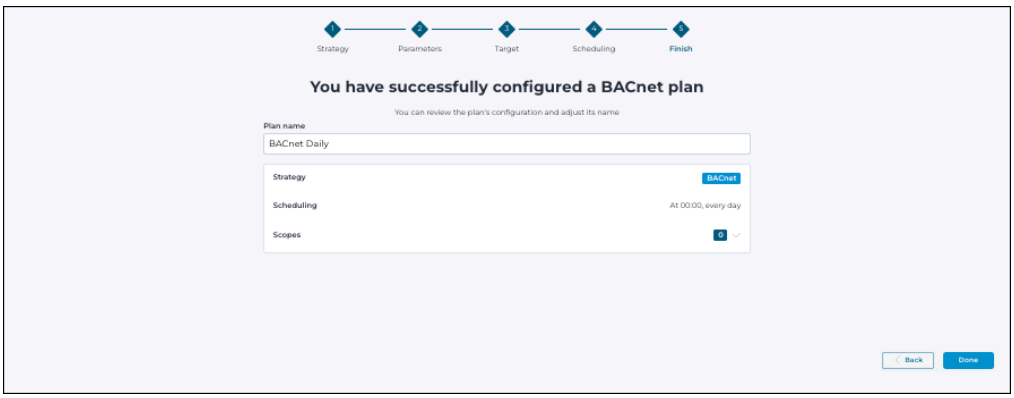


Figure 8. Finish page

On the **Finish** page, you can edit the **Plan name**, and configure **Scopes**.

If you select the arrow in the **Scopes** section, you can choose one of these options:

- Tag
- Site
- Sensor

Once you have made your selection, the number of item will show next to the arrow.

Automatically add a plan

Automatically add a Smart Polling plan from the onboarding page

*Use the **Get Started** button on the onboarding page to automatically create one or more Smart Polling plans.*

About this task

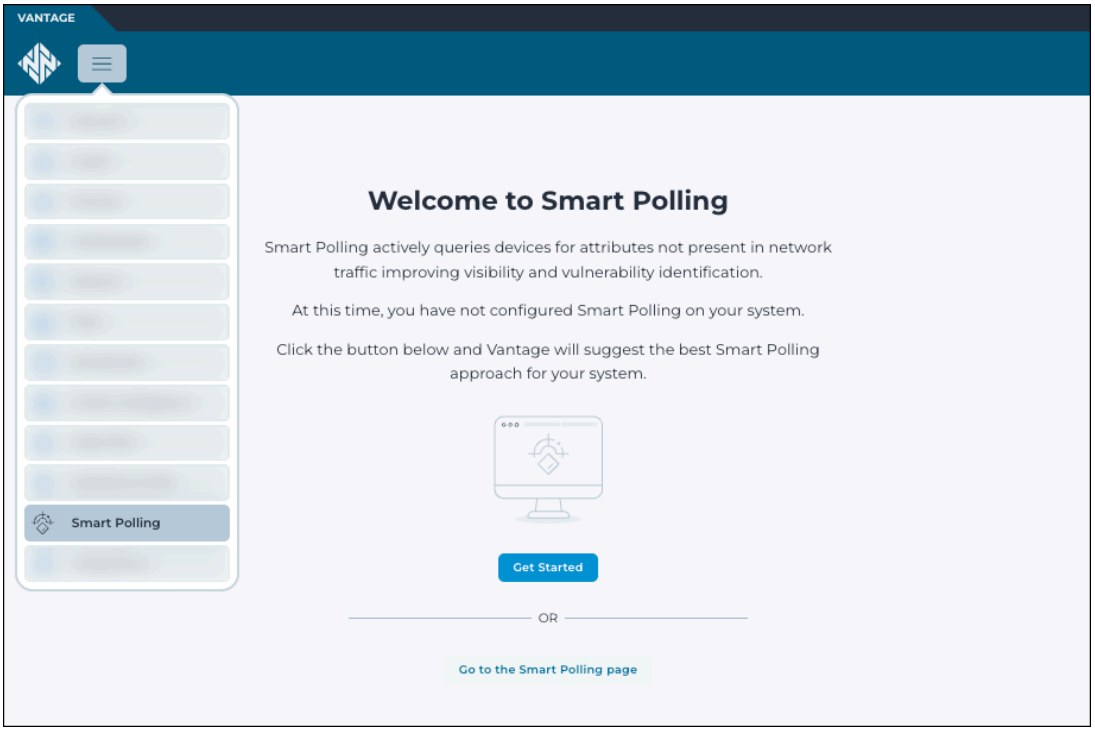
You will only see the onboarding page if no Smart Polling plans currently exist for your organization.

Procedure

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

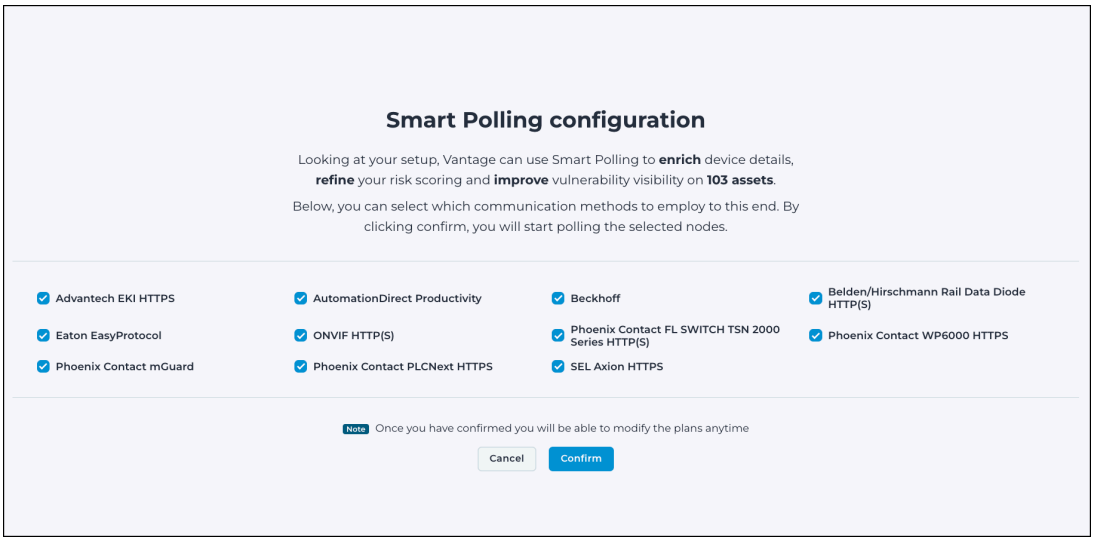
   Result: The **Smart Polling** page opens.

2. On the welcome page, select **Get Started**.



   Result: The **Smart Polling configuration** page opens. It will show a summary of what Vantage has detected in your environment, and the possible options that you can take.

3. Select one or more of the strategies that have been suggested.



4. Select **Confirm**.

Results

The Smart Polling plan(s) has (have) been added and they will run automatically.

Automatically add a Smart Polling plan from the suggestions section

*Use the **Suggestions** section on the **Smart Polling Plans** page to automatically create one or more Smart Polling plans.*

About this task

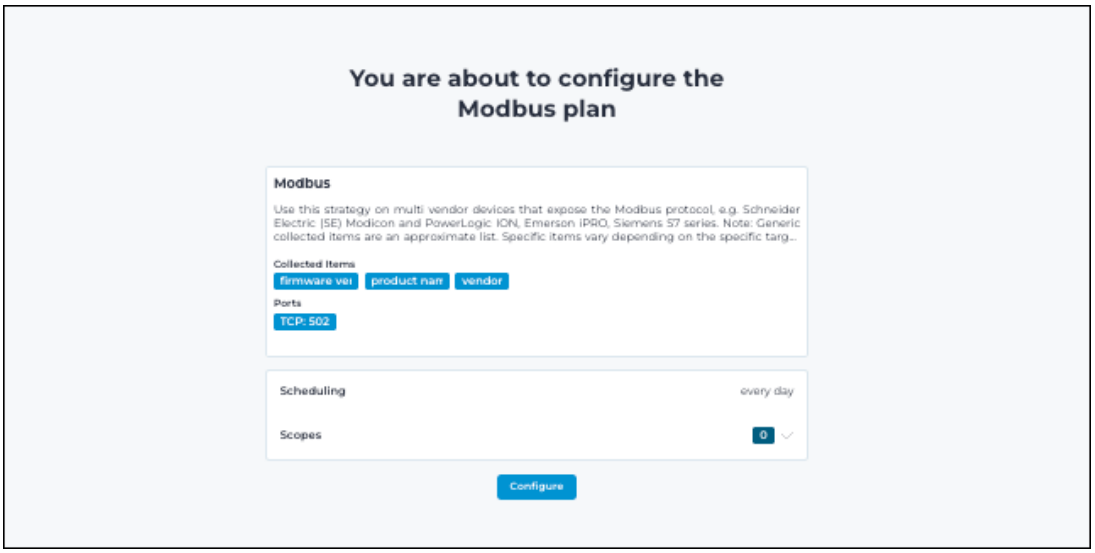
Use this process to create Smart Polling plans that automatically find the optimal target. This method allows for a single-click definition of plans that collect data from devices that the Nozomi Networks solution already recognizes in the environment.

Procedure

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

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

2. To select one of the strategies that have been suggested, in the bottom left corner, select the related ⚙ icon.



3. **Optional:** Expand the **Scopes** section and select **Add Scope**.
4. Select an option:

   Choose from:

   - Tag
   - Site
   - Sensor

   Result: A dialog shows.

5. Select one tag, site, or sensor.

   The option will depend on what you selected in the previous step.

6. Select **Configure**.

Results

The Smart Polling plan has been added and it will run automatically.

What to do next

If necessary, do the procedure above again for one or more of the other Smart Planning plans in the **Suggestions** section.

Manually add a plan

Add a Smart Polling plan that requires credentials

Create a Smart Polling plan that uses a strategy that requires credentials. Choose specific or all credentials, configure a schedule, and define the scope before completing the setup.

Before you begin

Make sure that the correct credentials for the Smart Polling plan you are about to add are in the **Credentials Manager**.

About this task

Use this process to create a Smart Polling plan that targets systems requiring authentication. This method allows the platform to access and collect data from sources that need credentials. You can configure the schedule and scope of the plan to suit your operational needs.

Procedure

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

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

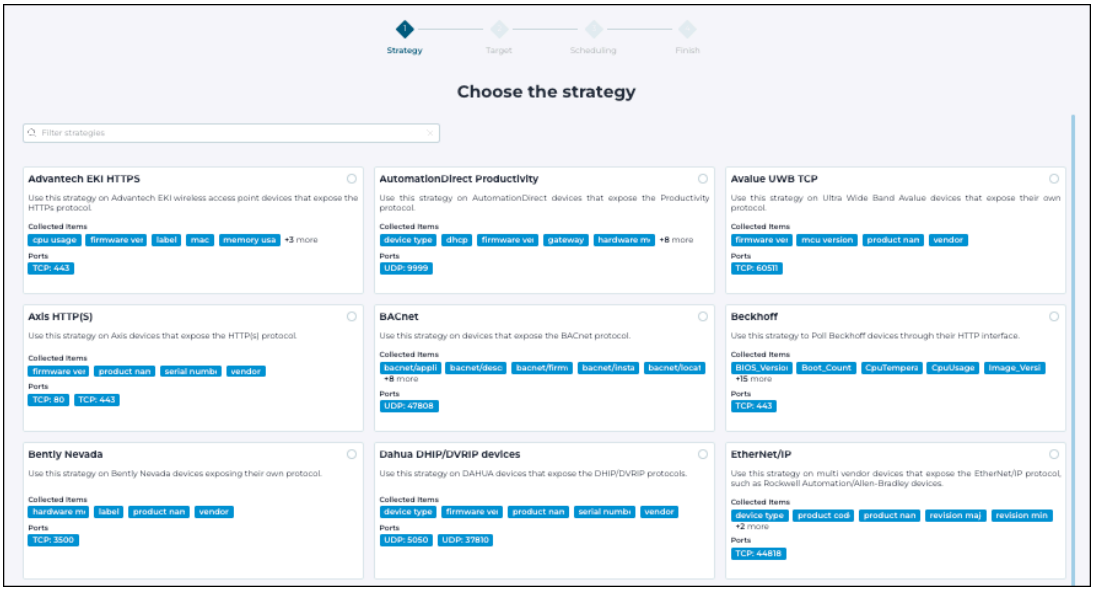
2. If the welcome page shows, select **Go to the Smart Polling page**.

3. On the **Smart Polling** page, select the ⊕ **Add** icon.

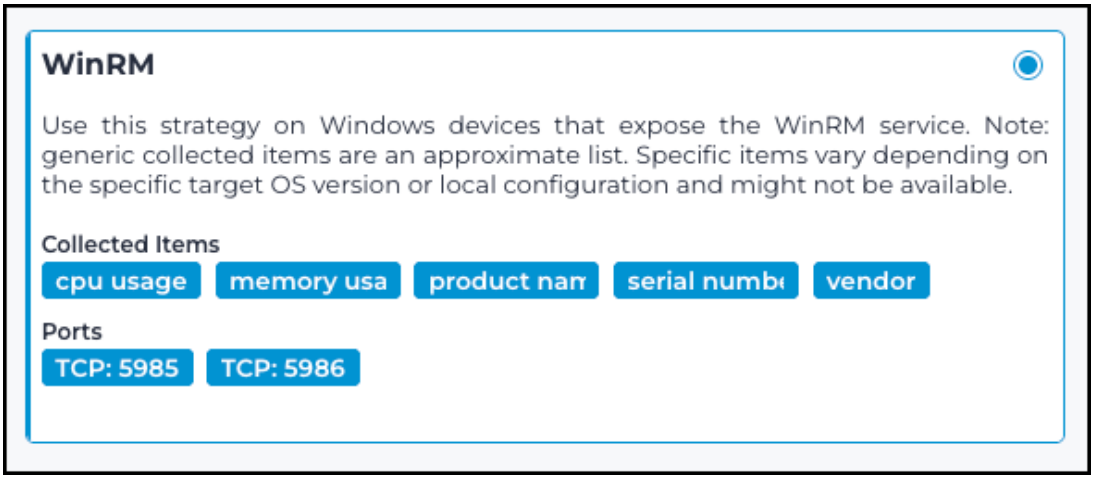
   Result: The **Choose the Strategy** page opens.

4. **Optional:**

   To find the correct strategy, enter text in the **Filter strategies** field.



5. In the top right corner of the relevant strategy, select the radio button.



6. Select **Next**.

   Result: Either the **Parameters** page or the **Target** page will show.

7. **Optional:** If the **Parameters** page shows, enter the necessary details.
8. Select **Next**.

   Result: The **Target** page will show.

9. From the **Available credentials** panel on the left, select the applicable credential.

10. Choose an option:

    Choose from:

    - To select one credential, select the > icon.
    - To select all the available credentials, select the >> icon.

11. Select **Next**.

    Result: The **Scheduling** page will show.

12. On the **Scheduling** page, select a scheduling type:

    > **Important:**
    > The **Recurrence based** option requires *N2OS* v25.3.0 or later. The **Interval based** option is available in all versions.

    Choose from:

    - Select **Interval based** to poll at a fixed interval
    - Select **Recurrence based** to poll at a specific frequency and time (requires *N2OS* v25.3.0 or later)

13. Configure the schedule:

    Choose from:

    - If you chose **Recurrence based**, set the frequency and the time
    - If you chose **Interval based**, set the interval

14. Select **Next**.

    Result: The **Finish** page will show.

15. **Optional:** In the **Plan name** field, edit the name of the plan.
16. **Optional:** Expand the **Scopes** section and select **Add Scope**.
17. Select an option:

    Choose from:

    - Tag
    - Site
    - Sensor

    Result: A dialog shows.

18. Select one tag, site, or sensor.
    The option will depend on what you selected in the previous step.
19. Select **Confirm**.
20. Select **Done**.

Results

The Smart Polling plan has been added.

Add a Smart Polling plan that does not require credentials

Create a Smart Polling plan for targets that do not require credentials. Define the query, configure the schedule, and set the scope to complete the setup.

About this task

Use this process to create a Smart Polling plan for devices or systems that do not require authentication. This method enables the platform to collect data from non-credentialed targets using a query-based selection. You can configure the schedule and scope of the plan to suit your operational needs.

Procedure

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

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

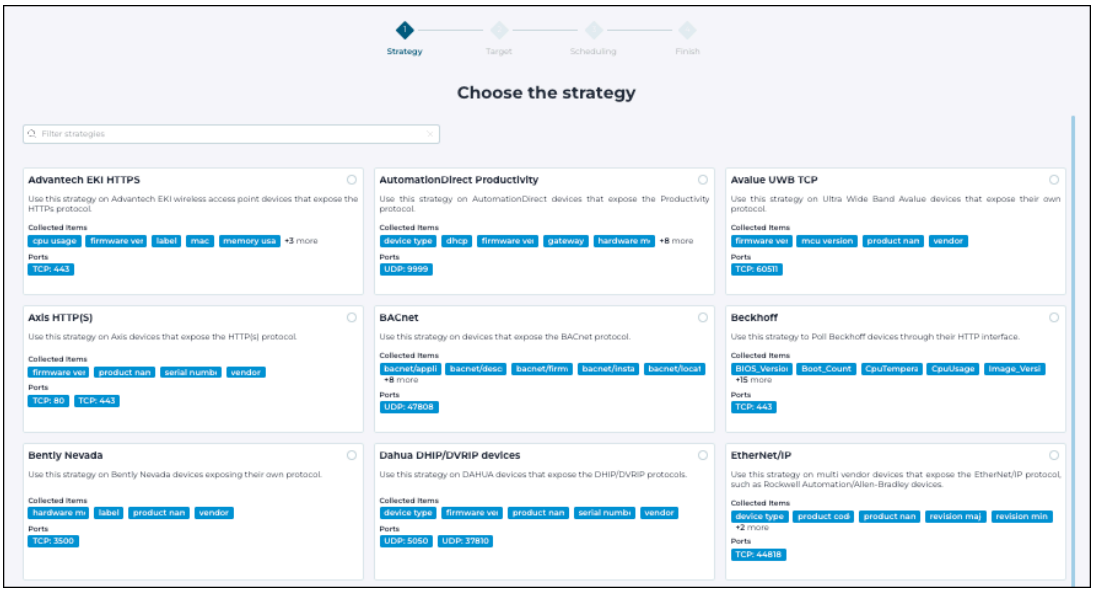
2. If the welcome page shows, select **Go to the Smart Polling page**.

3. On the **Smart Polling** page, select the ⊕ **Add** icon.

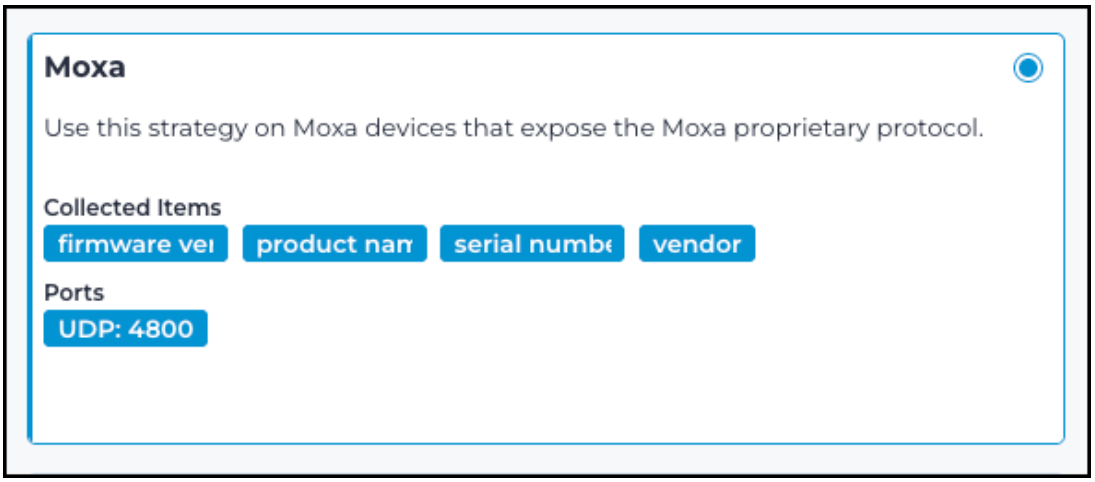
   Result: The **Choose the Strategy** page opens.

4. **Optional:**

   To find the correct strategy, enter text in the **Filter strategies** field.



5. In the top right corner of the relevant strategy, select the radio button.



6. Select **Next**.

   Result: Either the **Parameters** page or the **Target** page will show.

7. **Optional:** If the **Parameters** page shows, enter the necessary details.

> **Note:**
> Smart Polling proposes a safe default for each of these parameters. Unless you have specific requirements, we recommend that you use these parameters.

8. Select **Next**.

   Result: The **Target** page will show.

9. In the **Target nodes with a query** section, enter a query.
   For example, `nodes | where ip in_subnet? "192.168.45.0/24"`

10. Select **Test query**.

    If successful a `Success` indicator and the amount of nodes found will show and the **Next** button will be enabled.

11. Select **Next**.

    Result: The **Scheduling** page will show.

12. On the **Scheduling** page, select a scheduling type:

    > **Important:**
    > The **Recurrence based** option requires *N2OS* v25.3.0 or later. The **Interval based** option is available in all versions.

    Choose from:

    - Select **Interval based** to poll at a fixed interval
    - Select **Recurrence based** to poll at a specific frequency and time (requires *N2OS* v25.3.0 or later)

13. Configure the schedule:

    Choose from:

    - If you chose **Recurrence based**, set the frequency and the time
    - If you chose **Interval based**, set the interval

14. Select **Next**.

    Result: The **Finish** page will show.

15. **Optional:** In the **Plan name** field, edit the name of the plan.
16. **Optional:** Expand the **Scopes** section and select **Add Scope**.
17. Select an option:

    Choose from:

    - Tag
    - Site
    - Sensor

    Result: A dialog shows.

18. Select one tag, site, or sensor.

    The option will depend on what you selected in the previous step.

19. Select **Confirm**.
20. Select **Done**.

Results

The Smart Polling plan has been added.

Centralized plan management

Vantage displays progressive Smart Polling plans from connected sensors and lets you merge duplicates into a single centrally managed plan.

Progressive plans in Vantage

Progressive Smart Polling plans defined on connected sensors are shown on the Vantage **Smart Polling** page. These plans represent the progressive plans running on each connected Guardian.

Until the plans are consolidated, they do not yet contain historical data in Vantage.

Duplicate plan detection

When Vantage detects progressive plans defined on Guardian sensors, it shows a **Merge duplicates** message on the plan page. The message identifies how many duplicate plans exist and which sensors they come from.

You can merge the duplicates into a single plan and centralize its management in Vantage. After merging, the full polling history for the plan is immediately available in Vantage.

Effect of centralizing a plan

After you merge and centralize a progressive plan, Vantage manages the plan and propagates it to the connected sensors.

Important:

Once a progressive plan is centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Merge duplicate progressive plans

When multiple connected sensors have progressive plans for the same strategy, you can merge them into a single plan and manage it from Vantage.

About this task

When progressive mode is enabled on multiple connected sensors, each sensor may create its own progressive plan for the same strategy. Vantage detects these duplicates and lets you consolidate them into one plan. After merging, Vantage manages the plan and immediately shows the full polling history from all connected sensors.

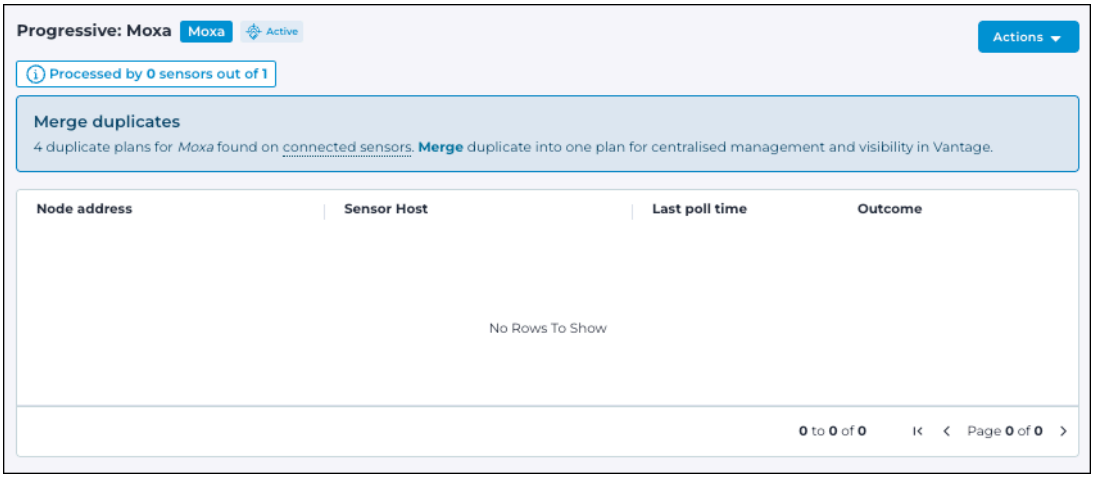
> **Important:**
> Once a plan is merged and centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Procedure

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

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

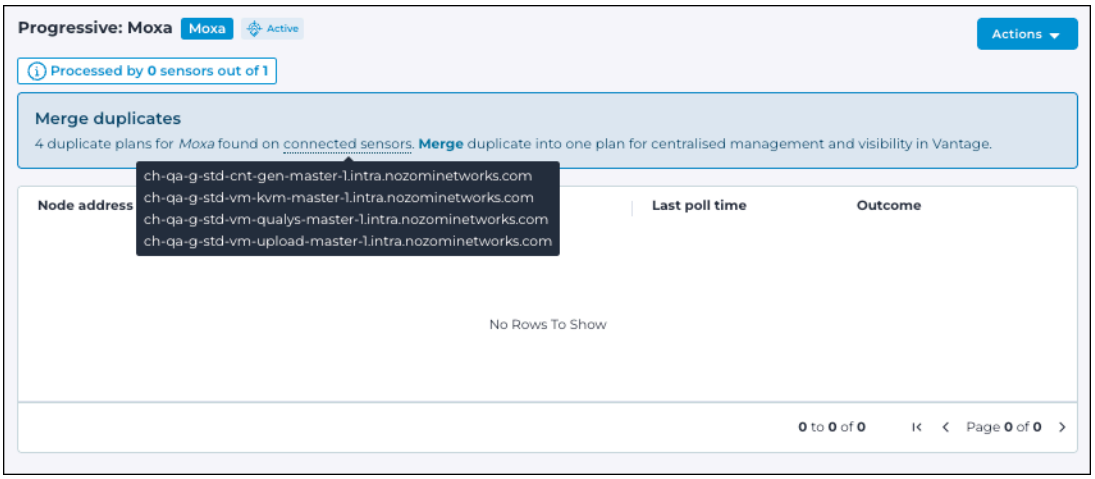
2. Select the progressive plan that shows a **Merge duplicates** message.



   Result: The plan page opens and shows the merge duplicates notification. The notification indicates how many duplicate plans exist across connected sensors.

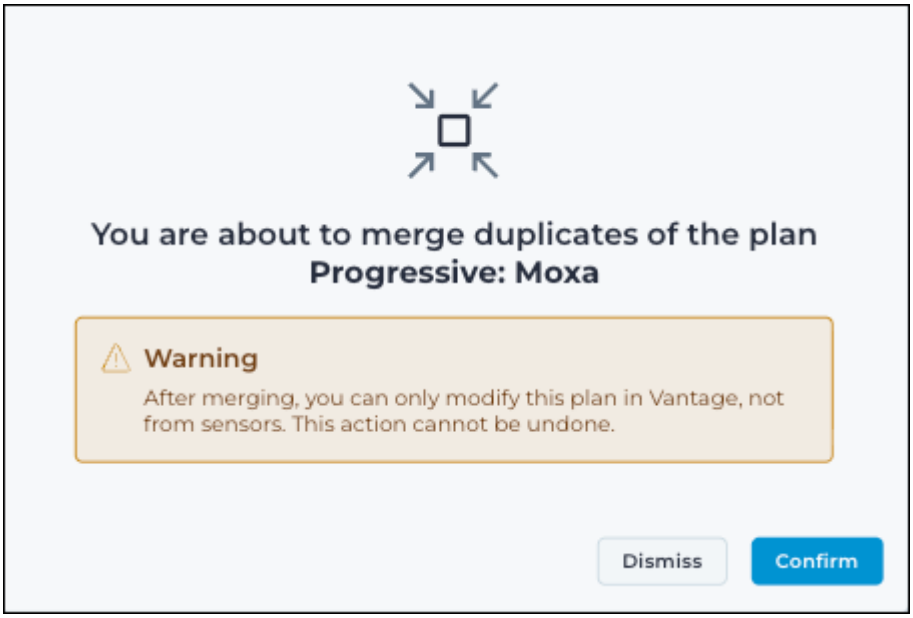
3. **Optional:**

   Hover over the **connected sensors** link in the notification to see which sensors have duplicate plans.



4. Select the option in the notification to merge the duplicates into this plan.

   Result: A confirmation dialog opens.



5. Select **Confirm**.

   Result: Vantage merges the duplicate plans and centralizes management of the plan. The polling history from all connected sensors is immediately available.

Actions menu

Pause a Smart Polling plan

Temporarily suspend a Smart Polling plan without deleting it. Use this option to stop polling activity while preserving the plan configuration. The plan can be resumed at any time.

About this task

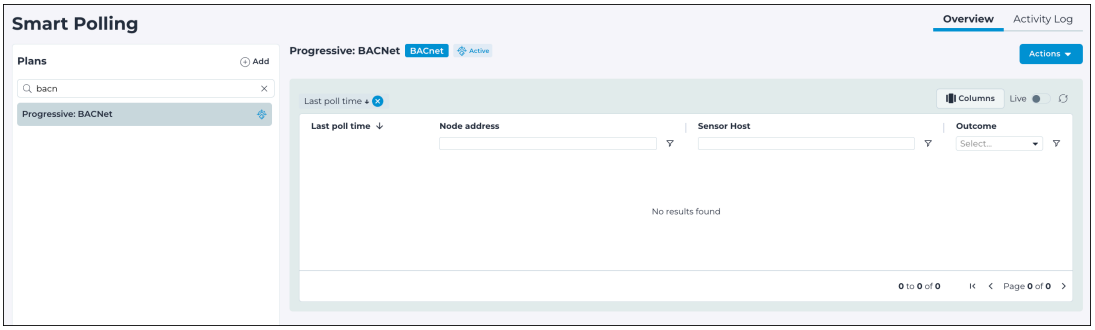
When you pause a Smart Polling plan, it temporarily disables its polling activity without removing its configuration. This is useful when you want to stop monitoring for maintenance, troubleshooting, or scheduling reasons, but plan to resume later.

Procedure

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

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

2. From the list of Smart Polling plans on the left, select the applicable plan.
3. In the top right corner, select **Actions**.



4. Select **Pause Plan**.

Results

The Smart Polling plan has been paused.

Resume a Smart Polling plan

Reactivate a previously paused Smart Polling plan to resume automated monitoring. This action restarts polling using the plan's saved configuration. Useful for restoring regular monitoring activity after a pause.

About this task

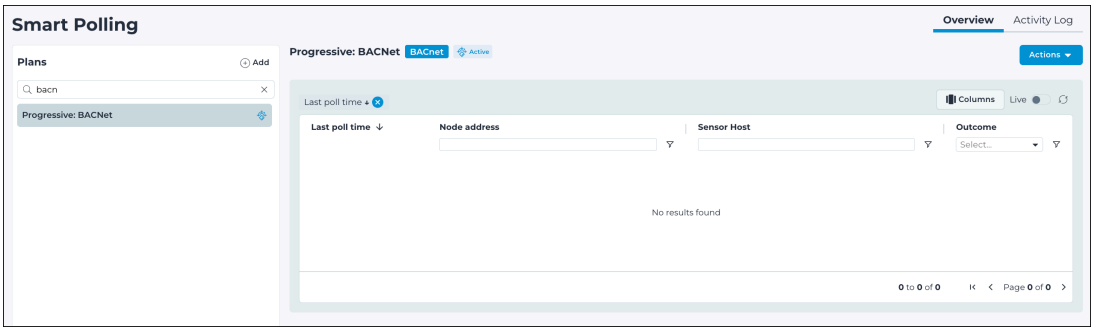
When you resume a Smart Polling plan, it restarts monitoring activity that was previously paused. This is useful after scheduled maintenance, issue resolution, or other intentional interruptions in polling. The plan resumes with its original configuration intact.

Procedure

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

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

2. From the list of Smart Polling plans on the left, select the applicable plan.
3. In the top right corner, select **Actions**.



4. Select **Resume Plan**.

Results

The Smart Polling plan has been resumed.

Edit a Smart Polling plan

Modify an existing Smart Polling plan to adjust its configuration or update associated settings. Editing a plan lets you fine-tune monitoring behavior. Ensure changes align with your system monitoring goals.

About this task

Editing a Smart Polling plan lets you change its targets, credentials, polling intervals, or other configurations. This is useful when your monitoring requirements change or you need to correct or refine existing settings.

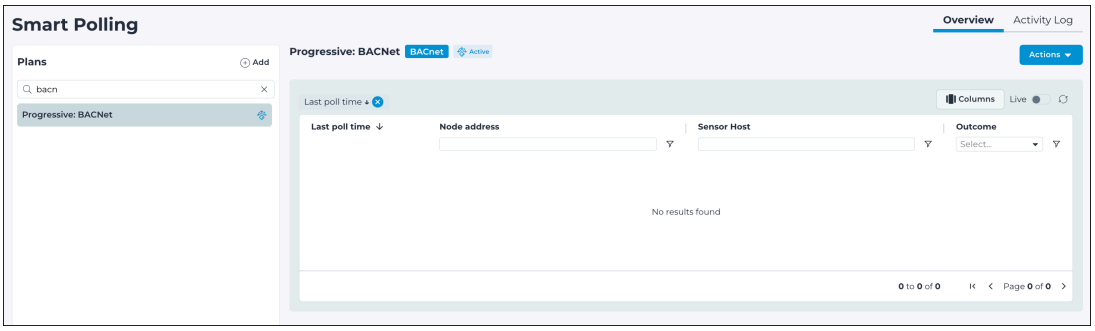
Procedure

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

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

2. From the list of Smart Polling plans on the left, select the applicable plan.

3. In the top right corner, select **Actions**.



4. Select **Edit Plan**.

   Result: The plan editing wizard opens in a modal window.

5. Use the applicable procedure to edit the plan:

   Choose from:

   - Add a Smart Polling plan that requires credentials (on page 30)
   - Add a Smart Polling plan that does not require credentials (on page 33)

   You can then confirm your edited details on the **Scheduling** and **Finish** pages.

Delete a Smart Polling plan

Delete an existing Smart Polling plan to remove obsolete or unneeded monitoring configurations. This action is permanent and cannot be undone. Use caution when confirming the deletion.

About this task

Deleting a Smart Polling plan permanently removes its configuration and stops all associated monitoring activity. Use this option when a plan is no longer relevant or needed. Be sure to confirm the deletion, as this action cannot be undone.

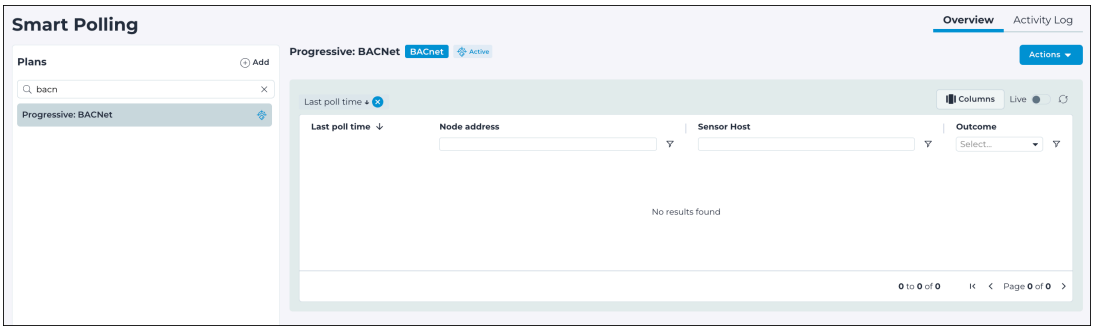
Procedure

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

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

2. From the list of Smart Polling plans on the left, select the applicable plan.

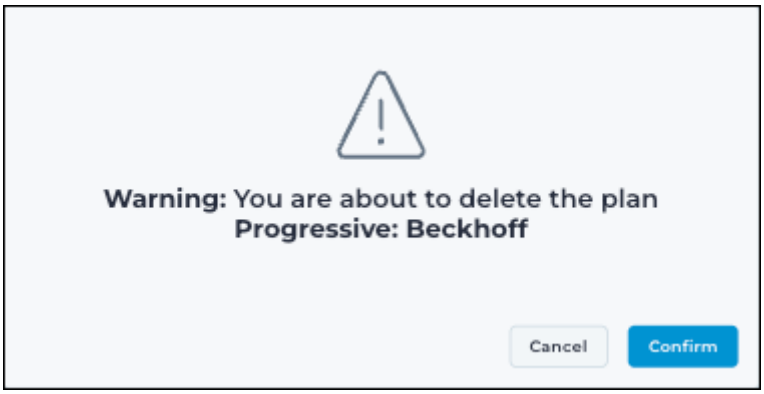
3. In the top right corner, select **Actions**.



4. Select **Delete Plan**.

   Result: A dialog shows

5. Select **Confirm**.



Results

The Smart Polling plan has been deleted.

Smart Polling results

*Smart Polling retrieves details from nodes to enrich asset data. This enriched information also enables other information to be enriched, such as hardware components, common platform enumeration (CPEs), and related vulnerabilities. When the Simple Network Management Protocol strategy (SNMP) strategy is used, it also populates the **Physical graph** in the **Graph** page.*

Once a Smart Polling plan has executed successfully, some or all of the information in sections of the Assets page should have been enriched.

Overview

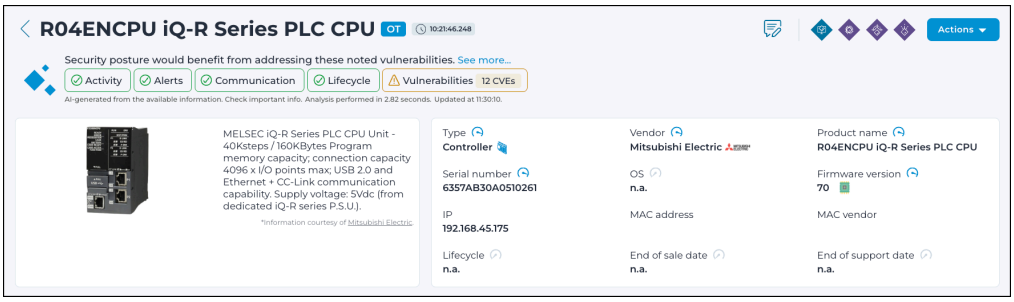


Figure 9. Assets page overview

Hardware Components tab

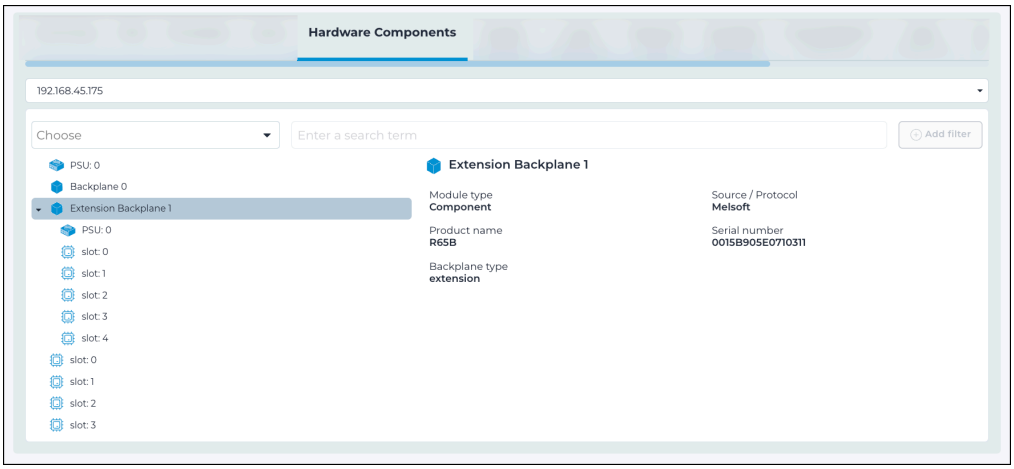


Figure 10. Assets page Hardware Components tab

CPEs tab

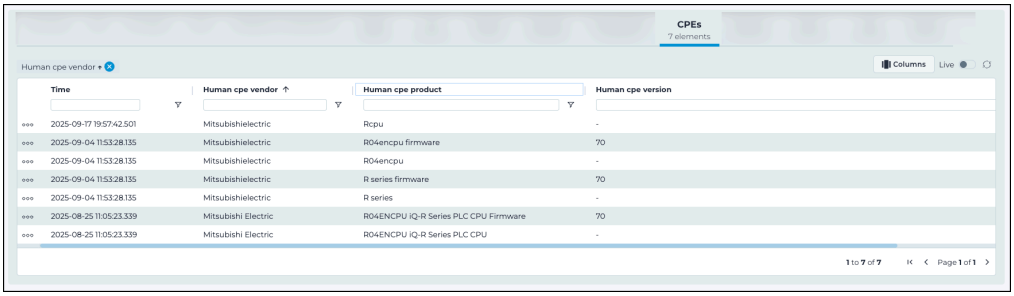


Figure 11. Assets page CPEs tab

Vulnerabilities tab

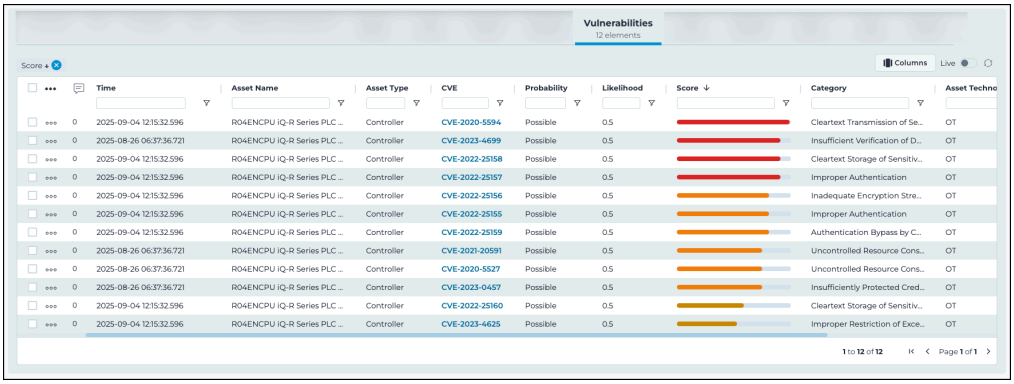


Figure 12. Assets page Vulnerabilities tab

Physical graph

In addition to the above sections, Smart Polling provides the necessary information to populate the **Physical graph**. To do this, you need to use the *SNMP* strategy to poll network switches or routers.

Activity Log

*Use the **Activity Log** page in Vantage to inspect the history of Smart Polling activities. Each record in the table represents an execution of a Smart Polling plan on a specific node from a Nozomi Networks sensor.*

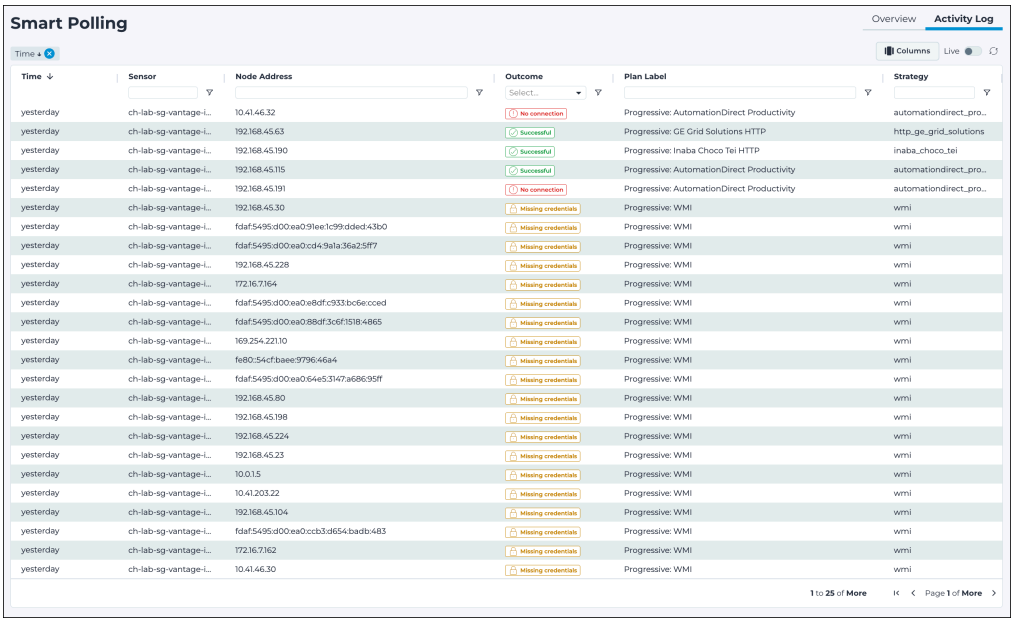


Figure 13. Activity Log page

Node executions

The **Activity Log** page shows the node executions. This is the individual executions of Smart Polling on a specific node with a configured plan. The table gives a view that you can filter and sort.

You can double-click a row in the table to open a sidebar with additional information. This includes a more granular report of the activity.

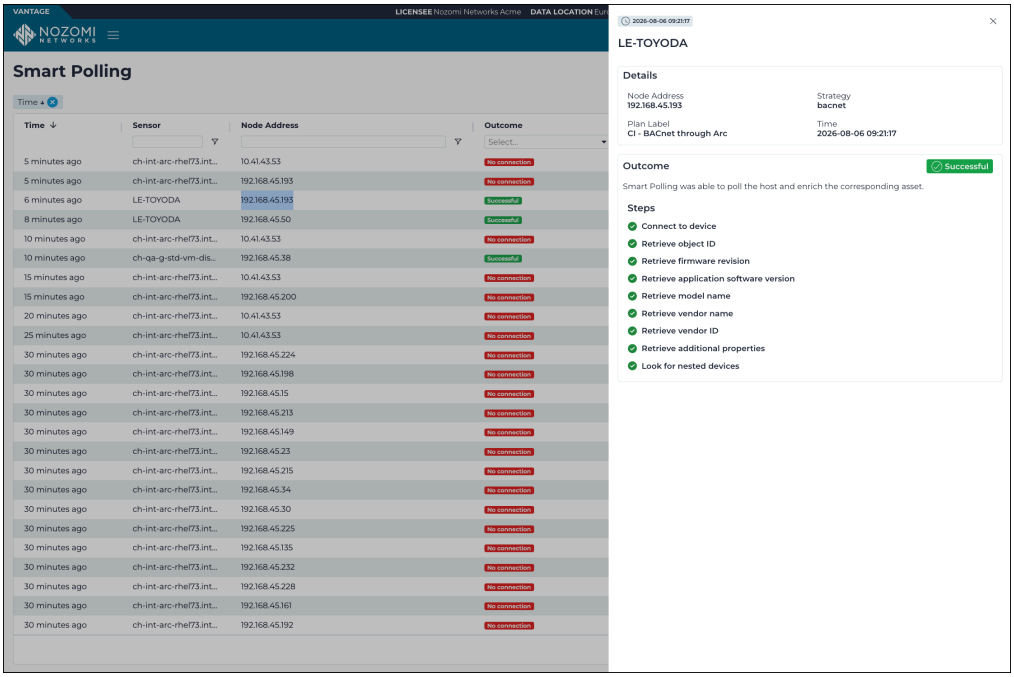


Figure 14. Activity Log sidebar

Column descriptions

Column label	Description
Time	The time this sensor connected to the monitored node.
Sensor	The hostname of the sensor performing the poll.
Node address	The address of the polled node.
Outcome	The result of the polling. For the list of possible outcomes, see Results (on page 20).
Plan label	The label of the executed plan.
Strategy	The strategy of the executed plan.

Chapter 4. Smart Polling in CMC

*The **Smart Polling** page gives you a read-only view of Smart Polling.*

In the *CMC*, Smart Polling plans are read-only. Plans created in Guardian can be synchronized, along with the associated data. By default, synchronization is disabled.

Smart Polling has these tabs:

- Plans (on page 50)
- Node points (on page 51)

Plans

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

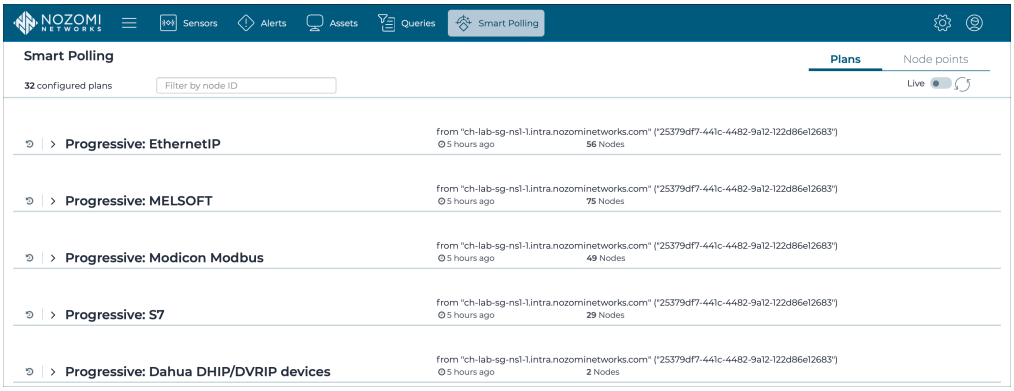


Figure 15. Plans page

> **Important:**
> Once a progressive plan is centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Filter

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

Node points

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

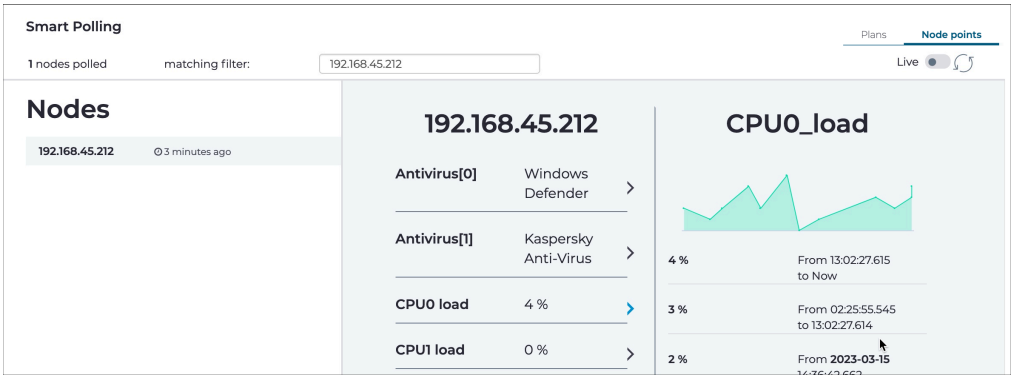


Figure 16. Node points page

Chapter 5. Smart Polling in Guardian

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

Smart Polling has these tabs:

- Plans (on page 56)
- Node points (on page 66)
- Settings (on page 67)

> **Note:**
> Arc sensors execute Smart Polling when Guardian requests it. Enable execution in the Arc local UI under **Execution options**.

Active sensor

Smart Polling on Guardian selects the sensor or sensors for execution based on the `capture_devices` field of the polled node. Smart Polling will engage the corresponding sensors. When at least one successful execution occurs from a sensor, Smart Polling remembers to use that sensor in future executions. If a future execution fails, or Smart Polling records no executions for more than a week, it reverts to the sensors in the `capture_devices` field.

To add a sensor to the applicable sensors for a node, you can use the Guardian *CLI* to modify the `capture_devices` field. For example, to add an Arc to the applicable sensors for a node, use `vi node 192.168.1.1 capture_device arc[1e6a174c]`, where `192.168.1.1` is the node *ID* and the value in brackets is the first eight characters of the Arc sensor's *ID*. The manually added sensor is then added to the node's `capture_devices` list, and may be chosen according to the algorithm described above. If a node is only visible to Arc sensors but you want to use Guardian instead, use `vi node 192.168.1.1 capture_device guardian`.

The *OS* of the sensor that polls the node decides which network interface to use based on the routing table. All Smart Polling strategies are based on the *IP*, which means that all routing decisions are delegated to the *OS*.

Plans

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

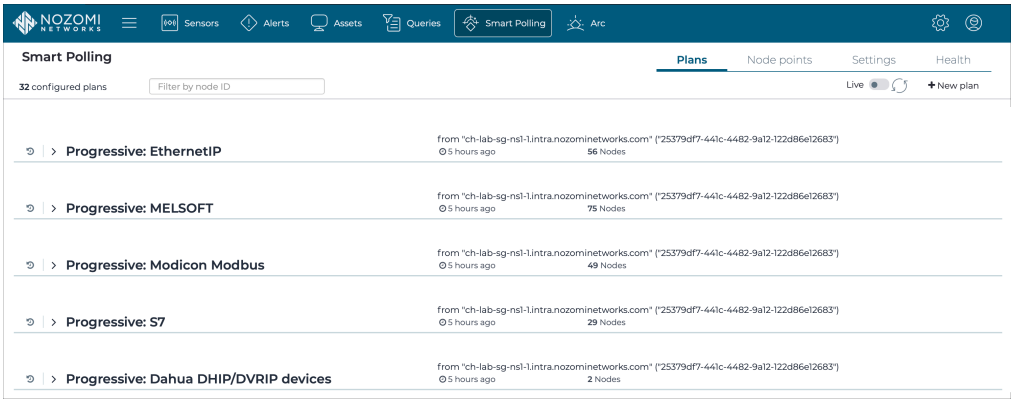


Figure 17. Plans page

> **Important:**
> Once a progressive plan is centralized in Vantage, you can no longer edit or delete it from the connected sensors.

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.

Progressive mode enablement in Guardian

You can enable Progressive mode in Guardian 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.

> **Important:**
> Once a progressive plan is centralized in Vantage, you can no longer edit or delete it from the connected sensors.

Enable progressive mode in Guardian

You can enable Progressive mode in Guardian to increase visibility.

Procedure

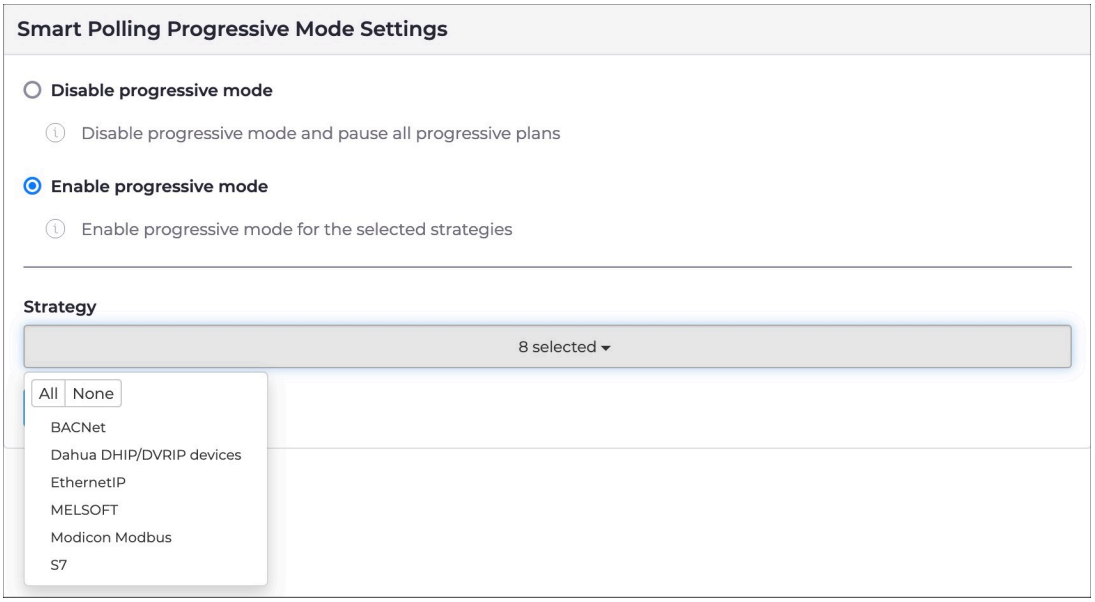
1. In the top navigation bar, select **Smart Polling**.

   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**.



> **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.

Create a Smart Polling plan in Guardian

*The **Plans** page in Guardian 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.

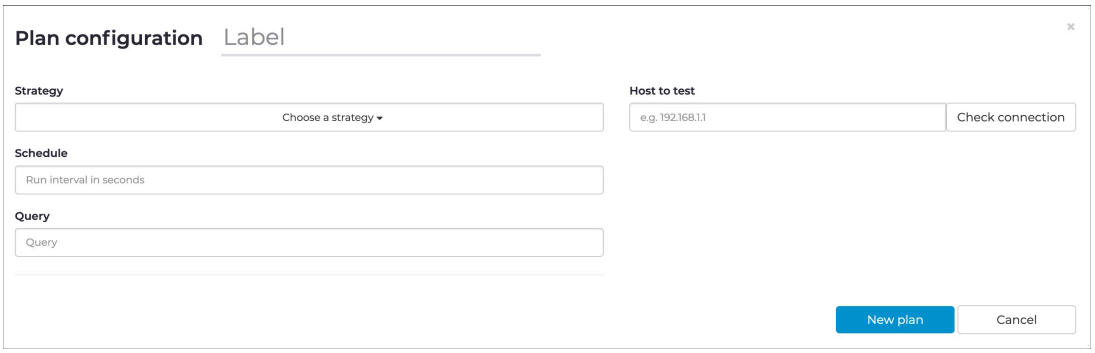
2. In the top right, select **Plans**.

   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 in Guardian

You can edit a Smart Polling plan in Guardian.

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.

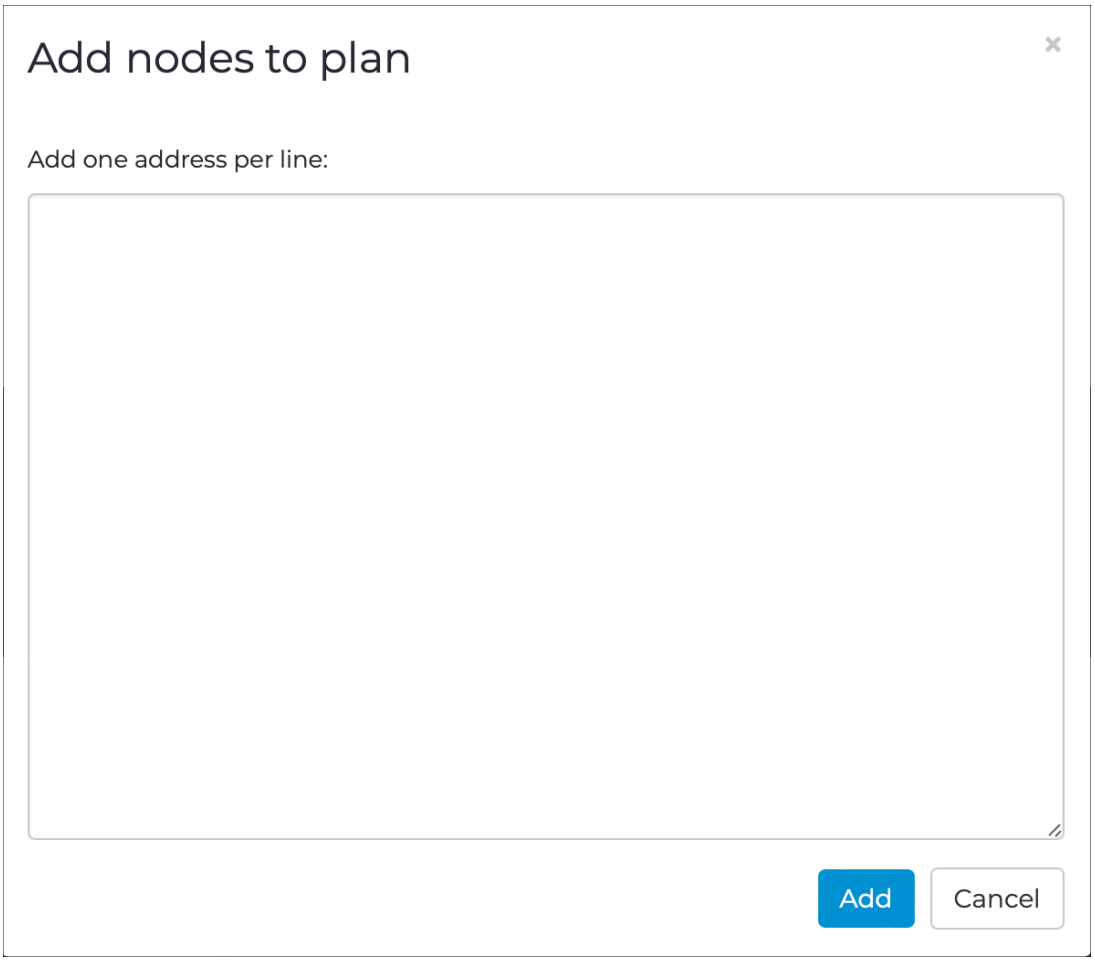
3. To the left of the name of the applicable plan, select the > icon.

   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.



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 in Guardian

You can adjust some aspects of Progressive mode plans in Guardian. By default, each plan runs every 24 hours, but you can 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**.

Node points

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

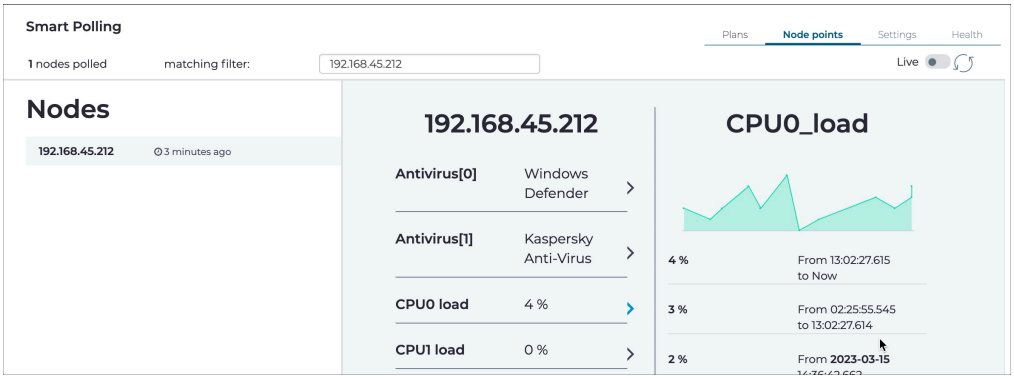


Figure 18. Node points page

Settings

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

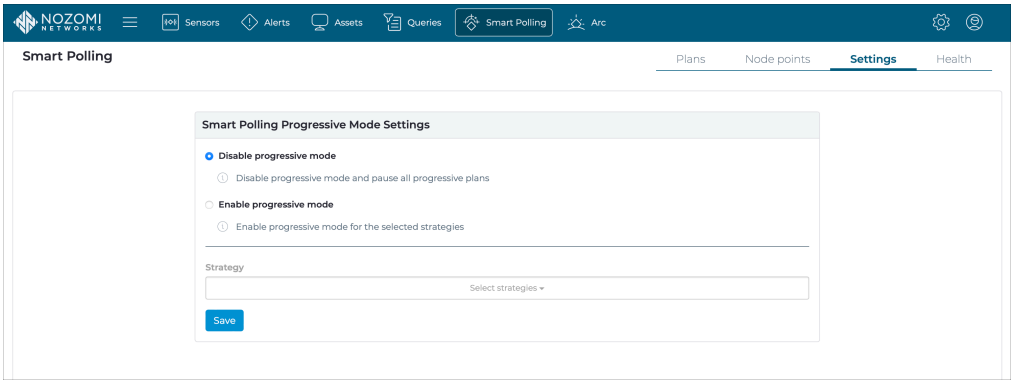


Figure 19. Settings page

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.

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 these files:

- `/data/log/n2os/n2ossp.log`
- `/data/log/n2os/n2os_strategist.log`

To change the level of detail in the logs, you can run this command in the *CLI*:

```
conf.user configure sp log_level <LEVEL>
```

The change applies immediately. You don't need to edit any files or restart any services. where `<LEVEL>` is one of the following values (in increasing order of verbosity):

- `FATAL`
- `ERROR`
- `WARN`
- `INFO`
- `DEBUG`

> **Note:**
> The default value is `INFO`.

> **Note:**
> The values are ordered from the most to the least important, and the configured level is the minimum to be printed. For example:
> - `ERROR` will print log lines for both `ERROR` and `FATAL` messages
> - `FATAL` will print log lines only for `FATAL` messages

To configure Smart Polling to only produce `ERROR` and `FATAL` messages, use this *CLI* rule:

```
conf.user configure sp log_level ERROR
```

View the enriched information history for a node

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

Procedure

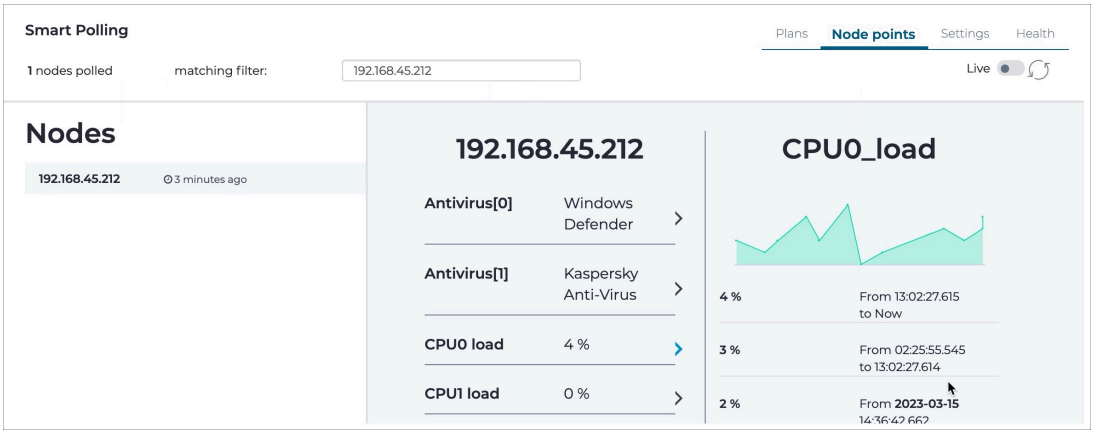
1. In the top navigation bar, select **Smart Polling**.

   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.



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

Chapter 6. Smart Polling in Arc

Arc sensors can run Smart Polling strategies in both offline and connected deployment modes.

The minimum conditions to run Smart Polling on Arc depend on whether Arc is running in offline or connected mode.

Arc offline mode

When Arc runs in Offline mode (disconnected from an upstream sensor), you configure Discovery and Smart Polling from the Arc local configuration UI.

Feature	License	Setting	Smart Polling triggers
Discovery	Not required	**Local UI > Discovery**	Not applicable
Smart Polling	Smart Polling	**Local UI > Smart Polling**	Discovery

Arc connected mode (Service and One-shot)

When Arc is connected to an upstream sensor (Service or One-shot mode), you configure Discovery and Smart Polling from the upstream installation.

Feature	License	Setting	Smart Polling triggers
Discovery	Not required	**Features > Discovery** (Vantage or Guardian)	Not applicable
Smart Polling	Smart Polling	**Vantage installations**: • Enable from **Features > Smart Polling** • Configure plans from Guardian **Guardian installations**: • Enabled by default — configure plans only	Plans, Discovery

Chapter 7. Strategies

Strategies overview

Smart Polling strategies are network-based methods that directly reach the monitored assets with concise, safe, and effective protocol-specific messages, enhancing visibility in the Nozomi Networks solution.

Strategies

Smart Polling strategies use various protocols to gain visibility in the network. They contact monitored assets directly, based on your configuration or through Discovery.

These strategies sometimes require credentials or other settings in the Smart Polling configuration. Make sure the Nozomi Networks sensor has network access to monitored assets and that firewalls do not block communications.

Credentials

Whether the strategy requires credentials to access target devices, and the credential scope it requires. Some strategies do not require credentials at all.

Device-side ports

The port or ports that must be reachable on the target device for the strategy to work. Make sure firewalls allow this traffic.

Arc availability

The Arc version since which the strategy is supported. Not every strategy is available on Arc.

Guardian availability

The Guardian version since which the strategy is supported. Not every strategy is available on Guardian.

Discovery trigger

For some strategies, whether devices found through a matching Discovery strategy are automatically polled by this strategy. Not every strategy has a corresponding Discovery strategy.

Collected items

The device attributes and properties that the strategy collects to enrich the monitored node. Collected items can vary depending on the device and its configuration.

Asset merging capabilities

Whether the strategy can merge nodes that represent the same physical device into a single asset, based on the information it collects.

Progressive mode queries

The query or queries that Progressive mode uses to automatically identify nodes that are suitable targets for the strategy.

Configuration parameters

For some strategies, the protocol-specific parameters you can configure from the *CLI* to fine-tune its behavior. Not every strategy has configurable parameters.

Advantech EdgeLink

Use this strategy on Advantech EdgeLink devices that expose the proprietary UDP protocol.

Credentials

This strategy does not require credentials.

Device-side ports

UDP/6513

Arc availability

Since 2.6.0

Guardian availability

Since 26.2.0

Collected items

This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- MAC address
- Operating System
- Product name
- Roles
- Vendor
- Node property: advantech_edgelink/dhcp
- Node property: advantech_edgelink/netmask

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where protocols include? advantech-edgelink | where roles
include? producer
```

Advantech EKI HTTPS

Use this strategy on Advantech EKI wireless access point devices that expose the HTTPS protocol.

Credentials

This strategy requires credentials with scope http-sp.

Device-side ports

TCP/443

Arc availability

Since 1.12.0

Guardian availability

Since 24.5.0

Collected items

This strategy enriches the monitored nodes with these items:

- CPU usage
- Firmware version
- Label
- MAC address
- Memory usage
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? advantech OR mac_vendor include? advantech
```

AutomationDirect Productivity

Use this strategy on AutomationDirect devices that expose the Productivity protocol.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/9999

Arc availability
Since 1.17.0

Guardian availability
Since 25.2.0

Discovery trigger
Nodes discovered through the automationdirect_productivity discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Hardware modules
- MAC address
- Product name
- Roles
- Vendor
- Node property: dhcp
- Node property: gateway
- Node property: network_mask
- Node property: physical_switch
- Node property: plc_name
- Node property: run_mode

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? AutomationDirect OR protocols include?
automationdirect_productivity | where roles include? producer
```

Avalue UWB TCP

Use this strategy on Ultra Wide Band Avalue devices that expose their own protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/60511

Arc availability
Not available

Guardian availability
Since 22.4.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Vendor
- Node property: mcu version

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? avalue OR mac_vendor include? avalue`

Axis HTTP(S)

Use this strategy on Axis devices that expose the HTTP(s) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Since 1.6.0

Guardian availability
Since 23.2.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? axis OR mac_vendor include? axis`

BACnet

Use this strategy on devices that expose the BACnet protocol.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/47808

Arc availability
Since 1.8.0

Guardian availability
Since 22.4.0

Discovery trigger
Nodes discovered through the bacnet discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Label
- Product name
- Roles
- Vendor
- Node property: bacnet/application_software
- Node property: bacnet/description
- Node property: bacnet/firmware
- Node property: bacnet/instance_id
- Node property: bacnet/location
- Node property: bacnet/object_name
- Node property: bacnet/sadr
- Node property: bacnet/snet
- Node property: bacnet/vendor_id

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where protocols include? bacnet-ip | where roles include? producer`

Configuration parameters
Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy bacnet
 <parameter> <value>
```

`max_traversal_responses`

Maximum number of BACnet gateway traversal responses processed per polling session

Default: `100`

Beckhoff

Use this strategy to poll Beckhoff devices through their HTTP interface.

Credentials

This strategy requires credentials with scope http-sp.

Device-side ports

TCP/443

Arc availability

Since 1.12.0

Guardian availability

Since 24.5.0

Collected items

This strategy enriches the monitored nodes with these items:

- Device type
- Label
- Operating System
- Product name
- Roles
- Serial number
- Vendor
- Node property: BIOS_Version
- Node property: Boot_Count
- Node property: CpuTemperature
- Node property: CpuUsage
- Node property: Image_Version
- Node property: MainBoard_Revision
- Node property: MainBoard_Serial_Number
- Node property: MainBoard_Type
- Node property: OSBuildVersion
- Node property: OSMajorVersion
- Node property: OSMinorVersion
- Node property: SoftwareUpTime
- Node property: uptime

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? "beckhoff"
```

Belden/Hirschmann Rail Data Diode HTTP(S)

Use this strategy on Belden/Hirschmann Rail Data Diode devices that expose the HTTP(S) protocol.

Credentials

This strategy does not require credentials.

Device-side ports

TCP/443, TCP/80

Arc availability

Since 2.5.0

Guardian availability

Since 26.2.0

Collected items

This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Operating System
- Product name
- Roles
- Vendor
- Node property: belden_hirschmann_rail_data_diode/name

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use 3 progressive mode queries to identify the targeted nodes:

- `nodes | where vendor include? belden`
- `nodes | where vendor include? hirschmann`
- `nodes | where mac_vendor include? belden`

Bently Nevada

Use this strategy on Bently Nevada devices exposing their own protocol.

Credentials

This strategy requires credentials with scope bently-nevada-sp.

Device-side ports

TCP/3500

Arc availability

Since 1.6.0

Guardian availability

Since 23.1.0

Collected items

This strategy enriches the monitored nodes with these items:

- Hardware modules
- Label
- Product name
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? bently OR mac_vendor include? bently
```

Bosch RCP+ cameras HTTP(S)

Use this strategy on Bosch Security Systems camera devices that expose RCP+ over the HTTP(S) protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80, TCP/443

Arc availability
Since 2.9.0

Guardian availability
Since 26.5.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- Product name
- Serial number
- Vendor
- Node property: UnitName
- Node property: bosch.cam_name

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor == "Bosch" | where type == "camera"`

Dahua DHIP/DVRIP devices

Use this strategy on DAHUA devices that expose the DHIP/DVRIP protocols.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/37810, UDP/5050

Arc availability
Not available

Guardian availability
Since 22.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? dahua OR mac_vendor include? dahua`

Eaton EasyProtocol

Use this strategy on Eaton devices that expose the easyProtocol protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/10001

Arc availability
Since 2.2.0

Guardian availability
Since 25.7.0

Discovery trigger
Nodes discovered through the eaton_easy_protocol discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Product name
- Roles
- Serial number
- Vendor
- Node property: eaton_easyprotocol/date_of_manufacture
- Node property: eaton_easyprotocol/firmware_build_number
- Node property: eaton_easyprotocol/hardware_revision

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? Eaton OR protocols include? eaton_easy |
where roles include? producer
```

EtherNet/IP

Use this strategy on devices that expose the EtherNet/IP protocol, such as Rockwell Automation/Allen-Bradley devices.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/44818

Arc availability
Since 1.6.0

Guardian availability
Since 19.0.0

Discovery trigger
Nodes discovered through the ethernetip discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Hardware modules
- Product name
- Serial number
- Vendor
- Node property: product code
- Node property: revision major
- Node property: revision minor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? rockwell OR mac_vendor include? rockwell
OR protocols include? ethernetip | where roles include? producer
```

GE MDS TD Series Telnet

Use this strategy on GE MDS TD Series radio control devices that expose the Telnet protocol.

Credentials
This strategy requires credentials with scope ge-mds-td-series-telnet-sp.

Device-side ports
TCP/23

Arc availability
Since 1.14.0

Guardian availability
Since 24.6.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Label
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? "General Electric" OR mac_vendor include?
"General Electric" | where roles include? producer
```

GE Telnet

Use this strategy on General Electric devices that expose GE's telnet protocol flavor (e.g. controllers, or Mark panels).

Credentials
This strategy requires credentials with scope ge-telnet-sp.

Device-side ports
TCP/23

Arc availability
Not available

Guardian availability
Since 22.3.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Product name
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? "GE Energy" OR vendor include? "General
Electric" OR mac_vendor include? "General Electric" OR mac_vendor
include? "Ge Energy" | where roles include? producer
```

Bosch Rexroth HTTP(S)

Use this strategy on Bosch Rexroth devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 23.4.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where mac_vendor include? ElectronicNetwork OR vendor include?
ElectronicNetwork OR mac_vendor include? bosch OR vendor include? bosch
| where protocols include? http OR protocols include? https
```

Cognex HTTP(S)

Use this strategy on Cognex devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 21.8.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where mac_vendor include? cognex OR vendor include? cognex |
where protocols include? http OR protocols include? https
```

Fanuc HTTP(S)

Use this strategy on Fanuc devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 21.8.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? fanuc OR product_name include? fanuc OR mac_vendor include? fanuc`

GE Healthcare HTTP

Use this strategy on General Electric devices hosting the Common Service Desktop web application.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/8100

Arc availability
Since 1.6.0

Guardian availability
Since 23.3.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Node property: gehealthcare/common_service_desktop_application_version

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? "general electric" OR mac_vendor include?
"general electric"
```

GE Grid Solutions HTTP

Use this strategy on General Electric Grid Solutions devices that expose the HTTP(S) protocol, such as the N60 Network Relay.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80

Arc availability
Since 1.9.0

Guardian availability
Since 24.4.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? "general electric" OR mac_vendor include?
"general electric"
```

Lanner BMC HTTP(S)

Use this strategy on Lanner devices mounting an American MegaTrends MegaRAC SP-X BMC solution that expose HTTP(S).

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 22.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? lanner OR mac_vendor include? lanner`

Schneider HTTP(S)

Use this strategy on Schneider APC devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Since 2.5.0

Guardian availability
Since 22.0.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- MAC address
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where product_name include? AP | where vendor include?
"schneider electric" OR mac_vendor include? "schneider electric"
```

Sewio HTTP(S)

Use this strategy on SEWIO UWB devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 23.0.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? sewio OR mac_vendor include? sewio`

Tyan BMC HTTP(S)

Use this strategy on Tyan devices mounting an American MegaTrends MegaRAC SP-X BMC solution that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 23.3.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? tyan OR mac_vendor include? tyan`

Ubisense HTTP(S)

Use this strategy on Ubisense assets that expose an HTTP user interface.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/80, TCP/443

Arc availability
Not available

Guardian availability
Since 23.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? ubisense OR product_name include? ubisense
OR mac_vendor include? ubisense
```

Inaba Choco Tei HTTP

Use this strategy on Inaba Choco Tei devices that expose the HTTP protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- Product name
- Roles
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? inaba OR mac_vendor include? inaba`

Mitsubishi Electric MELSOFT

Use this strategy on Mitsubishi Electric devices that expose the MELSOFT protocols, such as: GOT1000, GOT2000, Q-Series, iQ-R Series.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/5001, TCP/5002, UDP/5006, TCP/5007, TCP/5014, TCP/5015

Arc availability
Since 1.7.0

Guardian availability
Since 21.8.0

Discovery trigger
Nodes discovered through the melsoft discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Hardware modules
- MAC address
- Product name
- Serial number
- Vendor
- Node property: melsoft/gt_designer3_version
- Node property: melsoft/network_number
- Node property: melsoft/station_number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy can merge nodes into an asset.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor == "Mitsubishi Electric" OR mac_vendor ==
"Mitsubishi Electric" OR protocols include? melsoft | where roles
include? producer OR roles include? HMI
```

Configuration parameters
Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy melsoft
 <parameter> <value>
```

`inter_session_delay`

Delay in milliseconds between polling sessions for the same device

Default: `1000`

`cc_link_ie_crawled_devices_limit`

Maximum number of CC-Link IE devices enumerated per scan

Default: `1000`

`reuse_tcp_sessions`

Whether to reuse TCP sessions across polling iterations

Default: `true`

`enable_udp`

Enable UDP transport in addition to TCP for Q Series and iQ-R Series devices

Default: `false`

IEC 61850-8-1 (MMS)

Use this strategy on IED devices that expose the IEC 61850-8-1 protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/102

Arc availability
Since 2.1.0

Guardian availability
Since 25.5.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Product name
- Roles
- Serial number
- Vendor
- Node property: iec61850/config_rev
- Node property: iec61850/hw_rev
- Node property: iec61850/location
- Node property: iec61850/nam_plt_d
- Node property: iec61850/owner
- Node property: iec61850/phy_nam_d
- Node property: iec61850/sw_rev

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use 2 progressive mode queries to identify the targeted nodes:

- `nodes | where protocols include? goose`
- `nodes | where protocols include? mms | where type == "IED"`

Modbus

Use this strategy on devices that expose the Modbus protocol, e.g. Schneider Electric (SE) Modicon and PowerLogic ION, Emerson iPRO, Siemens S7 series. Note: Generic collected items are an approximate list. Specific items vary depending on the specific target OS version or local configuration and might not be available.

Credentials

This strategy does not require credentials.

Device-side ports

TCP/502

Arc availability

Since 1.8.0

Guardian availability

Since 19.0.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Vendor
- Node property: modbus/abb_firmware_build_date
- Node property: modbus/abb_product_code

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use 2 progressive mode queries to identify the targeted nodes:

- `nodes | where protocols include? modbus | where roles include? producer`
- `nodes | where mac_vendor include? schneider`

Moxa

Use this strategy on Moxa devices that expose the Moxa proprietary protocol.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/4800

Arc availability
Since 1.17.0

Guardian availability
Since 25.2.0

Discovery trigger
Nodes discovered through the moxa discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where protocols include? moxa | where roles include? producer`

Moxa HTTP(S)

Use this strategy on Moxa devices that expose the HTTP(S) protocol.

Credentials

This strategy requires credentials with scope moxa-http-sp.

Device-side ports

TCP/80, TCP/443

Arc availability

Since 2.0.0

Guardian availability

Since 25.4.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Label
- MAC address
- Product name
- Serial number
- Vendor
- Node property: uptime

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy can merge nodes into an asset.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? moxa OR mac_vendor include? moxa OR
protocols include? moxa | where roles include? producer
```

ONVIF HTTP(S)

Use this strategy on devices that expose the ONVIF protocol on HTTP/HTTPS.

Credentials

This strategy requires credentials with scope onvif-sp.

Device-side ports

TCP/80, TCP/443

Arc availability

Since 1.14.0

Guardian availability

Since 24.6.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor
- Node property: Hardware_ID

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use 2 progressive mode queries to identify the targeted nodes:

- `nodes | where protocols include? onvif | where roles include? producer`
- `nodes | where type == "camera"`

Owl OPDS SSH

Use this strategy on Owl OPDS devices that expose the SSH protocol.

Credentials
This strategy requires credentials with scope ssh-sp.

Device-side ports
TCP/22

Arc availability
Since 2.3.0

Guardian availability
Since 26.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Product name
- Vendor
- Node property: owl_opds/patch_cluster

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? Owl`

Phoenix Contact FL SWITCH TSN 2000 Series HTTP(S)

Use this strategy on Phoenix Contact FL SWITCH TSN 2000 series devices that expose the HTTP/HTTPS protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80, TCP/443

Arc availability
Since 2.3.0

Guardian availability
Since 26.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- MAC address
- Product name
- Roles
- Serial number
- Vendor
- Node property: uptime

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy can merge nodes into an asset.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? phoenix OR mac_vendor include? phoenix`

Phoenix Contact WP6000 HTTPS

Use this strategy on Phoenix Contact WP6000 (HMI) devices that expose the HTTPS protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/443

Arc availability
Since 1.6.0

Guardian availability
Since 23.2.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? phoenix OR mac_vendor include? phoenix`

Phoenix Contact mGuard

Use this strategy on Phoenix Contact mGuard devices that expose the HTTPS protocol.

Credentials

This strategy requires credentials with scope phoenix-contact-mguard-sp.

Device-side ports

TCP/443

Arc availability

Since 1.12.0

Guardian availability

Since 24.5.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? phoenix OR mac_vendor include? phoenix
```

Phoenix Contact PLCNext HTTPS

Use this strategy on Phoenix Contact PLCNext-based devices (e.g. AXC F 3152) that receive information by using the HTTPS protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/443

Arc availability
Since 1.15.0

Guardian availability
Since 25.1.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor
- Node property: Hardware_ID
- Node property: Order_Number

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? phoenix OR mac_vendor include? phoenix`

Reolink Baichuan

Use this strategy on Reolink devices that expose the TCP Baichuan protocol.

Credentials
This strategy requires credentials with scope reolink-sp.

Device-side ports
TCP/9000

Arc availability
Since 2.7.0

Guardian availability
Since 26.4.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- Product name
- Vendor
- Node property: reolink/uid

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? "Reolink" OR mac_vendor include? "Reolink"`

Siemens STEP7

Use this strategy on Siemens devices that expose the S7 protocol, such as 300/400/1200/1500.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/102

Arc availability
Since 1.6.0

Guardian availability
Since 21.8.0

Discovery trigger
Nodes discovered through the s7 discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Hardware modules
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? siemens OR mac_vendor include? siemens OR protocols include? s7 OR protocols include? s7plus | where roles include? producer`

Configuration parameters
Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy s7 <parameter>
 <value>
```

`timeout`

Timeout in milliseconds for S7 protocol operations

Default: `5000`

`requests_delay_ms`

Delay in milliseconds between consecutive S7 read requests

Default: `500`

SEL telnet

Use this strategy on Schweitzer Engineering Laboratories devices exposing SEL's telnet protocol flavor.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/23

Arc availability
Since 1.8.0

Guardian availability
Since 19.0.0

Collected items
This strategy enriches the monitored nodes with this item: Firmware version.

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? sel OR vendor include? schweitzer OR
mac_vendor include? sel OR mac_vendor include? schweitzer | where roles
include? producer
```

SEL Axion HTTPS

Use this strategy on SEL Axion/RTAC devices that expose the REST API over HTTPS.

Credentials

This strategy requires credentials with scope http-sp.

Device-side ports

TCP/443

Arc availability

Since 2.10.0

Guardian availability

Since 26.5.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Hardware modules
- Label
- MAC address
- Product name
- Serial number
- Vendor
- Node property: sel_axion/bios_version
- Node property: sel_axion/hardware_version
- Node property: sel_axion/project_name
- Node property: sel_axion/project_state

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy can merge nodes into an asset.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? sel OR vendor include? schweitzer | where
protocols include? https OR roles include? producer
```

Sensor Net Connect

Use this strategy on Sensor Net Connect devices that expose their proprietary UDP-based protocol.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/30303

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

Discovery trigger
Nodes discovered through the sensor_net_connect discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Label
- Product name
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
```
nodes | where vendor include? "Sensor Net Connect" OR mac_vendor
include? "Sensor Net Connect"
```

Shelly mDNS

Use this strategy on Shelly devices that expose the mDNS protocol.

Credentials
This strategy does not require credentials.

Device-side ports
UDP/5353

Arc availability
Since 2.2.0

Guardian availability
Since 25.6.0

Discovery trigger
Nodes discovered through the shelly discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Vendor
- Node property: product_description

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? shelly OR mac_vendor include? shelly`

Siemens SIPROTEC HTTP(S)

Use this strategy on SIPROTEC 4 or SIPROTEC 5 devices that expose the HTTP(S) protocol.

Credentials
This strategy requires credentials with scope http-sp.

Device-side ports
TCP/4443

Arc availability
Since 1.15.0

Guardian availability
Since 21.8.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Label
- Product name
- Serial number
- Vendor
- Node property: assigned_fct_points
- Node property: configuration_version
- Node property: mode
- Node property: mounting_position_1
- Node property: mounting_position_2
- Node property: port_e
- Node property: product code
- Node property: product_code
- Node property: short_product_code
- Node property: siprotec_version
- Node property: system_time

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where product_name include? "siprotec 4" OR product_name
include? "siprotec 5" | where vendor include? "siemens"
```

SNMP

Use this strategy on devices that expose the SNMP protocol (v1, v2c, v3). It includes vendor-specific data extraction for the following device types: Brocade switches, Fortinet switches, Hirschmann switches, N-Tron switches, Schneider Electric APC PDUs.

Credentials

This strategy requires credentials with scope snmpv3-sp.

Device-side ports

UDP/161

Arc availability

Since 1.7.0

Guardian availability

Since 19.0.0

Collected items

This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Hardware modules
- Label
- MAC address
- Operating System
- Product name
- Serial number
- Vendor
- Node property: active_sessions
- Node property: agent_config_module_description
- Node property: bootloader_version
- Node property: chassisComponenet
- Node property: chassis_architecture_type
- Node property: chassis_id_number
- Node property: cpu_usage
- Node property: disk_usage
- Node property: ethernet_ports_count
- Node property: firmware_build_date_and_time
- Node property: firmware_revision
- Node property: hardware_revision
- Node property: hm_sys_group_capacity
- Node property: hm_sys_group_map
- Node property: hm_sys_group_module_capacity
- Node property: hm_sys_max_fan
- Node property: hm_sys_max_power_supply
- Node property: hm_sys_module_port_capacity
- Node property: installed_ports_count

- Node property: intefaceAlias
- Node property: interfaceName
- Node property: ips_database_version
- Node property: ips_extended_database_version
- Node property: lldp_loc_sys_cap_enabled
- Node property: lldp_loc_sys_cap_supported
- Node property: local
- Node property: lowmem_usage
- Node property: macAddress
- Node property: management_virtual_domain
- Node property: memory_usage
- Node property: networkAddress
- Node property: number_of_ports
- Node property: portComponent
- Node property: snmp/vendor_id
- Node property: software_revision
- Node property: switch_location
- Node property: switch_module_type
- Node property: sysDescr.0
- Node property: sysObjectID
- Node property: time_since_reset
- Node property: total_disk_capacity
- Node property: total_flash
- Node property: total_lowmem_capacity
- Node property: total_ports_count
- Node property: total_ram
- Node property: valid_ports_count
- Node property: virtual_ports
- Node property: virus_database_version
- Node property: virus_extended_database_version

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy can merge nodes into an asset.

Progressive mode queries

This strategy can use 2 progressive mode queries to identify the targeted nodes:

- `nodes | where protocols include? snmp`
- `nodes | where protocols include? snmp-v3`

Configuration parameters

Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy snmp <parameter>
 <value>
```

`maxCustomWalkOids`

Maximum number of custom OIDs walked per polling session

Default: `200`

`maxStrategyWalkOids`

Maximum number of strategy-defined OIDs walked per polling session

Default: `5000`

`max_logical_entities`

Maximum number of logical entities processed per bridge-aware SNMP device

Default: `20`

SSH

Use this strategy on devices that expose the SSH protocol. Note: generic collected items are an approximate list. Specific items vary depending on the specific target OS version or local configuration and might not be available. It includes vendor-specific data extraction for the following device types: Tridium Niagara (e.g. JACE 8000 and 9000 controllers).

Credentials

This strategy requires credentials with scope ssh-sp.

Device-side ports

TCP/22

Arc availability

Since 2.7.0

Guardian availability

Since 19.0.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Installed Software
- Label
- MAC address
- Memory usage
- Operating System
- Product name
- Roles
- Serial number
- Vendor
- Node property: ssh/host_id
- Node property: ssh/host_key
- Node property: ssh/niagara_version

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where os include? linux OR os include? mac
```

Configuration parameters

Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy ssh <parameter>
 <value>
```

`use_fallback`

Use the legacy SSH polling strategy instead of the primary one

Default: `false`

Tattile NTCP

Use this strategy on Tattile devices that expose the NTCP protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/42000

Arc availability
Since 2.8.0

Guardian availability
Since 26.4.0

Discovery trigger
Nodes discovered through the tattile_ntcp discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- Label
- MAC address
- Operating System
- Product name
- Roles
- Serial number
- Vendor
- Node property: tattile_ntcp/hostname
- Node property: tattile_ntcp/product_code

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? tattile OR mac_vendor include? tattile`

Tyco exacqVision

Use this strategy on Tyco exacqVision assets that receive information by using the HTTP protocol.

Credentials

This strategy does not require credentials.

Device-side ports

TCP/80

Arc availability

Since 1.6.0

Guardian availability

Since 23.2.0

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:

```
nodes | where vendor include? tyco OR mac_vendor include? tyco
```

UPnP

Use this strategy on devices that expose the UPnP service over HTTP(S).

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80

Arc availability
Since 1.6.0

Guardian availability
Since 21.2.0

Discovery trigger
Nodes discovered through the upnp discovery strategy will be automatically smart-polled by this strategy.

Collected items
This strategy enriches the monitored nodes with these items:

- Label
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where is_empty(properties.ssdp/ssdp_location) == false`

Configuration parameters
Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy upnp <parameter>
 <value>
```

`http_timeout`

Timeout in milliseconds for UPnP HTTP requests

Default: `5000`

`idle_http_timeout`

Idle connection timeout in milliseconds for UPnP HTTP requests

Default: `3000`

Wago Management

Use this strategy on Wago devices that expose the Wago management protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/6626

Arc availability
Since 1.10.0

Guardian availability
Since 24.4.0

Collected items
This strategy enriches the monitored nodes with these items:

- Firmware version
- Product name
- Serial number
- Vendor
- Node property: wago/firmware_burn_date
- Node property: wago/product_description

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? wago OR mac_vendor include? wago`

WinRM

Use this strategy on Windows devices that expose the WinRM service. Note: generic collected items are an approximate list. Specific items vary depending on the specific target OS version or local configuration and might not be available.

Credentials

This strategy requires credentials with scope winrm-sp.

Device-side ports

TCP/5985, TCP/5986

Arc availability

Since 2.7.0

Guardian availability

Since 19.0.0

Collected items

This strategy enriches the monitored nodes with these items:

- CPU usage
- Hotfixes
- Installed Software
- Label
- MAC address
- Memory usage
- Operating System
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where os include? windows`

Configuration parameters

Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy winrm
 <parameter> <value>
```

`use_fallback`

Use the legacy WinRM polling strategy instead of the primary one

Default: `false`

WMI

Use this strategy on Windows devices that expose the WMI interface. Note: generic collected items are an approximate list. Specific items vary depending on the specific target OS version or local configuration and might not be available.

Credentials

This strategy requires credentials with scope wmi-sp.

Device-side ports

TCP/135

Arc availability

Since 2.5.0

Guardian availability

Since 19.0.0

Collected items

This strategy enriches the monitored nodes with these items:

- CPU usage
- Hotfixes
- Installed Software
- Label
- MAC address
- Memory usage
- Operating System
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities

The strategy does not feature asset merging capabilities.

Progressive mode queries

This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where os include? windows`

Configuration parameters

Use the following command to apply a configuration parameter:

```
conf.user configure smart_polling_and_discovery strategy wmi <parameter>
 <value>
```

`use_fallback`

Use the legacy WMI polling strategy instead of the primary one

Default: `false`

Zettler/Ezcare TCP Gateway HTTP

Use this strategy on Zettler/Ezcare TCP gateway devices that expose the HTTP protocol.

Credentials
This strategy does not require credentials.

Device-side ports
TCP/80

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

Collected items
This strategy enriches the monitored nodes with these items:

- Device type
- Firmware version
- MAC address
- Product name
- Serial number
- Vendor

Note: The collected items may vary depending on the device and its configuration.

Asset merging capabilities
The strategy does not feature asset merging capabilities.

Progressive mode queries
This strategy can use this progressive-mode query to identify the targeted nodes:
`nodes | where vendor include? zettler OR mac_vendor include? zettler`

Glossary

Central Management Console

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

Central Processing Unit

The main, or central, processor that executes instructions in a computer program.

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.

Coordinated Universal Time

Coordinated Universal Time (UTC) is the primary time standard by which the world regulates clocks and time. It is based on International Atomic Time (TAI) with leap seconds added to synchronize with Earth's rotation.

cURL

cURL is a command-line tool and library used to transfer data to or from a server. It supports many protocols, including HTTP, HTTPS, FTP, and more. In API contexts, curl is commonly used to test and interact with endpoints by sending requests and receiving responses.

Identifier

A label that identifies the related item.

Industrial Control Systems

An ICS is an electronic control system and related instrumentation that is used to control industrial processes.

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.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Object Identifier

In computing, OIDs are an identifier mechanism which is standardized by the International Telecommunication Union (ITU) and ISO/IEC for the naming of an object, concept, or other item with a globally-unambiguous persistent name.

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.

Programmable Logic Controller

A PLC is a ruggedized, industrial computer used in industrial and manufacturing processes.

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.

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.

Windows Management Instrumentation

WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM), an industry initiative to develop a standard technology for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. It allows querying and management of Windows systems.

Windows Remote Management

Is a Microsoft implementation of Web Services-Management in Windows which lets systems access or exchange management information across a common network. You can utilize the built-in command line tool, or scripting objects, WinRM can be used with remote computers that may have baseboard management controllers (BMCs) to acquire data.