

Smart Polling Strategies Reference Guide

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.....	5
Smart Polling overview.....	7
Chapter 2. Strategies.....	9
Strategies overview.....	11
Advantech EdgeLink.....	12
Advantech EKI HTTPS.....	13
AutomationDirect Productivity.....	14
Avalue UWB TCP.....	15
Axis HTTP(S).....	16
BACnet.....	17
Beckhoff.....	18
Belden/Hirschmann Rail Data Diode HTTP(S).....	19
Bently Nevada.....	20
Dahua DHIP/DVRIP devices.....	21
Eaton EasyProtocol.....	22
EtherNet/IP.....	23
GE MDS TD Series Telnet.....	24
GE Telnet.....	25
Bosch Rexroth HTTP(S).....	26
Cognex HTTP(S).....	27
Fanuc HTTP(S).....	28
GE Healthcare HTTP.....	29
GE Grid Solutions HTTP.....	30
Lanner BMC HTTP(S).....	31
Schneider HTTP(S).....	32
Sewio HTTP(S).....	33
Tyan BMC HTTP(S).....	34
Ubisense HTTP(S).....	35
Inaba Choco Tei HTTP.....	36
Mitsubishi Electric MELSOFT.....	37
IEC 61850-8-1 (MMS).....	38
Modbus.....	39
Moxa.....	40
Moxa HTTP(S).....	41
ONVIF HTTP(S).....	42
Owl OPDS SSH.....	43
Phoenix Contact FL SWITCH TSN 2000 Series HTTP(S).....	44
Phoenix Contact WP6000 HTTPS.....	45
Phoenix Contact mGuard.....	46

Phoenix Contact PLCNext HTTPS.....	47
Reolink Baichuan.....	48
Siemens STEP7.....	49
SEL telnet.....	50
Sensor Net Connect.....	51
Shelly mDNS.....	52
Siemens SIPROTEC HTTP(S).....	53
SNMP.....	54
SSH.....	56
Tattile NTCP.....	57
Tyco exacqVision.....	58
UPnP.....	59
Wago Management.....	60
WinRM.....	61
WMI.....	62
Zettler/Ezcare TCP Gateway HTTP.....	63

Chapter 1. Introduction



Smart Polling overview

Smart Polling actively contacts nodes to retrieve information for new nodes, and to enrich the information for existing nodes.

Smart Polling lets you create plans and define polling instructions for Guardian to use. For example, you can define:

- Polling for specific nodes
- Polling for specific times
- The methods to use

**Note:**

For example, use the EtherNet/IP protocol to poll known s in the subnet `192.168.38.0/24` every hour.

Guardian uses the data that Smart Polling extracts to enrich its knowledge about the assets in the environment. For example:

- PLC nodes polled using the EtherNet/IP protocol are enriched with information, such as vendor, device type, or serial number in **Assets** or **Network**
- Windows computers polled using the protocol provide a list of the installed software in the **Node points** tab
- Linux machines polled using show in **Assets** and **Network** with the exact name of the distribution and their uptime

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 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 and the value in brackets is the first eight characters of the Arc sensor's . 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 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 , which means that all routing decisions are delegated to the .



Chapter 2. 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 by directly contacting the monitored assets upon the user's configuration or through the cooperation with Discovery.

For these strategies to work effectively, it is occasionally necessary to introduce credentials or other settings into the Smart Polling configuration, to make sure the Nozomi sensor has a network access to the monitored assets, and that the firewalls don't block the communications.

Availability on Arc and Guardian

Most Smart Polling strategies are supported on both Arc and Guardian platforms, although some are platform-specific. For each protocol, the guide specifies availability details to help with deployment planning.

Related information

[Smart Polling overview \(on page 7\)](#)

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_edgelinek/dhcp
- Node property: advantech_edgelinek/netmask

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

Progressive mode queries

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

- nodes | where protocols include? advantech-edgelinek | 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.

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-pollled 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.

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.

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.

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-pollled by this strategy.

Collected items

This strategy enriches the monitored nodes with these items:

- Firmware version
- 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.

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

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.

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.

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.

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

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.

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.

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-pollled 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

TCP/5000, TCP/5001, TCP/5002, TCP/5003, TCP/5004, TCP/5005, TCP/5006, TCP/5007, TCP/5008, TCP/5009

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-pollled 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.

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

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.

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.

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-pollled 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.

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.

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.

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 does not require credentials.

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.

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.

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.

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.

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.

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.

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-pollled 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.

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

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 these items:

- Firmware version

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

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

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-pollled 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.

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-pollled 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.

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.

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
- Product name
- Serial number
- Vendor
- Node property: active_sessions
- Node property: agent_config_module_description
- Node property: bootloader_version
- Node property: chassisComponent
- 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: interfaceAlias

- 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.

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

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.

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

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-pollled 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.

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.

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-pollled 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.

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`

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.

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.

Progressive mode queries

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

- nodes | where os include? windows

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.

Progressive mode queries

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

- nodes | where os include? windows

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.

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

