NOZOMI NETWORKS

Discovery Strategies
Reference Guide

2026-10-06

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
Discovery overview 7
Chapter 2. Strategies 9
Strategies overview 11
Advantech EdgeLink 12
ARP 13
AutomationDirect CLICK KOP 14
AutomationDirect Productivity 15
BACnet 16
Beckhoff 17
Bernecker & Rainer Ethernet SNMP 18
CODESYS 19
Cognex 20
SICK CoLa 21
Eaton EasyProtocol 22
EtherNet/IP 23
Tridium Niagara 24
IKEA Dirigera mDNS 25
Mitsubishi Electric MELSOFT 26
Moxa 27
ONVIF 28
Pepperl+Fuchs 29
Reolink Baichuan 30
Siemens STEP7/Profinet 31
Sensor Net Connect 32
Shelly mDNS 33
SMB 34
Tattile NTCP 35
Ubiquiti 36
UPnP 37

Chapter 1. Introduction

Discovery overview

Discovery identifies previously undetected network devices. It sends protocol-specific broadcast messages to devices and examines the replies. The sensor repeats this process at predefined intervals transmitting diverse messages based on the devices.

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

On Arc, intervals are fixed to 5 minutes, while on Guardian, the intervals start at 5 minutes and gradually increase to a maximum of 60 minutes. Discovery listens for replies on the these ports:

- UDP/48888 for most protocols
- UDP/1911 for the Fox protocol
- UDP/30718 for the SICK CoLa protocol
- UDP/47808 for the BACnet protocol

Important:

For Discovery to work correctly, the firewall must allow communication over these ports.

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.

Related information

Strategies overview (on page 11)

Chapter 2. Strategies

Strategies overview

Discovery strategies are network-based methods that identify devices across subnetworks using broadcast messages, enhancing visibility in Nozomi Networks environments.

Strategies

Discovery strategies use protocol-specific broadcast messages to identify devices connected to a network. These lightweight messages prompt devices to return identity information, which Nozomi Networks sensors collect and analyze. The process is repeated at defined intervals to maintain current visibility into the network.

Operation

Each Nozomi Networks sensor selects the appropriate network interfaces and sends out broadcast messages to the subnetworks it can access. On Arc, this process repeats every 15 minutes. On Guardian, the interval starts at 5 minutes and increases progressively, up to a maximum of 60 minutes.

The system listens for responses on the following ports:

- UDP/48888 for most protocols
- UDP/1911 for the Fox protocol
- UDP/30718 for the SICK CoLa protocol
- UDP/47808 for the BACnet protocol

Availability on Arc and Guardian

Most discovery 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

Discovery overview (on page 7)

Advantech EdgeLink

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

Device-side ports
UDP/6513

Sensor-side ports
UDP/48888

Outbound network throughput
42 bytes

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.

Arc availability
Since 2.6.0

Guardian availability
Since 26.2.0

ARP

Use this strategy to discover devices on the network through ARP requests.

Device-side ports
This strategy uses ARP

Sensor-side ports
Not applicable

Collected items
This strategy enriches the monitored nodes with this item: MAC address.

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

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

Arc availability
Since 1.14.0

Guardian availability
Not available

AutomationDirect CLICK KOP

Use this strategy to discover AutomationDirect CLICK devices that expose the KOP protocol.

Device-side ports
UDP/25425

Sensor-side ports
UDP/48888

Outbound network throughput
14 bytes

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

- Device type
- Firmware version
- MAC address
- Product name
- Roles
- Vendor
- Node property: gateway
- Node property: network_mask
- 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.

Arc availability
Since 1.15.0

Guardian availability
Since 25.1.0

AutomationDirect Productivity

Use this strategy to discover AutomationDirect devices that expose the Productivity protocol.

Device-side ports
UDP/9999

Sensor-side ports
UDP/48888

Outbound network throughput
24 bytes

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

- Device type
- 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.

Arc availability
Since 1.17.0

Guardian availability
Since 25.2.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy automationdirect_productivity.

BACnet

Use this strategy to discover devices that expose the BACnet protocol.

Device-side ports
UDP/47808

Sensor-side ports
UDP/48888, UDP/47808

Outbound network throughput
12 bytes

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

- Roles
- Vendor
- Node property: bacnet/instance_id
- 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.

Arc availability
Since 1.14.0

Guardian availability
Since 24.6.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy bacnet.

Beckhoff

Use this strategy to discover Beckhoff devices that expose the ADS protocol.

Device-side ports
UDP/48899

Sensor-side ports
UDP/48888

Outbound network throughput
24 bytes

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

- Firmware version
- Label
- Operating System
- Node property: Fingerprint
- Node property: TwinCAT 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.

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

Bernecker & Rainer Ethernet SNMP

Use this strategy to discover Bernecker & Rainer devices that expose the SNMP over Ethernet protocol.

Device-side ports
This strategy uses SNMP over Ethernet

Sensor-side ports
This strategy uses SNMP over Ethernet

Outbound network throughput
340 bytes

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: gateway
- Node property: network_mask

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

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

Arc availability
Since 2.6.0

Guardian availability
Not available

CODESYS

Use this strategy to discovery assets that use the CODESYS Control software.

Device-side ports
UDP/1740, UDP/1741, UDP/1742, UDP/1743

Sensor-side ports
UDP/1740

Outbound network throughput
72 bytes

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

- Device type
- Product name
- Roles
- Vendor
- Node property: codesys.device_name
- Node property: codesys.node_name
- Node property: codesys.serial_number
- Node property: codesys.vendor_name
- Node property: codesys.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.

Arc availability
Since 1.17.0

Guardian availability
Since 25.2.0

Cognex

Use this strategy to discover Cognex devices that expose the Cognex protocol.

Device-side ports
UDP/1069

Sensor-side ports
UDP/48888

Outbound network throughput
9 bytes

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

- Device type
- Firmware version
- Label
- Product name
- Serial number
- Node property: Description
- Node property: Family

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

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

Arc availability
Since 1.14.0

Guardian availability
Since 24.5.0

SICK CoLa

Use this strategy on SICK devices that implement the CoLa command language.

Device-side ports
UDP/30718

Sensor-side ports
UDP/48888, UDP/30718

Outbound network throughput
24 bytes

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

- Firmware version
- Product name
- Serial number
- Vendor
- Node property: location
- Node property: network_gateway
- Node property: network_mask

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

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

Arc availability
Since 1.17.0

Guardian availability
Since 25.1.0

Eaton EasyProtocol

Use this strategy to discover Eaton devices that expose the easyProtocol protocol.

Device-side ports
UDP/11111

Sensor-side ports
UDP/11111

Outbound network throughput
12 bytes

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

- Device type
- MAC address
- Product name
- Roles
- Vendor
- Node property: eaton_easyprotocol/gateway
- Node property: eaton_easyprotocol/network_mask
- Node property: eaton_easyprotocol/protocol_version
- Node property: eaton_easyprotocol/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.

Arc availability
Since 2.2.0

Guardian availability
Since 25.7.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy eaton_easy_protocol.

EtherNet/IP

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

Device-side ports
UDP/44818

Sensor-side ports
UDP/48888

Outbound network throughput
24 bytes

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

Arc availability
Since 1.8.0

Guardian availability
Since 24.5.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy ethernetip.

Tridium Niagara

Use this strategy to discover Tridium devices that expose the FOX protocol.

Device-side ports
UDP/1911

Sensor-side ports
UDP/1911

Outbound network throughput
74 bytes

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

- Label
- Operating System
- Vendor
- Node property: host_id
- Node property: 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.

Arc availability
Since 1.11.0

Guardian availability
Since 24.5.0

IKEA Dirigera mDNS

Use this strategy to discover IKEA Dirigera smart home hub devices using the mDNS network protocol.

Device-side ports
UDP/5353

Sensor-side ports
UDP/48888

Outbound network throughput
34 bytes

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

- Device type
- Firmware version
- Label
- Product name
- Vendor
- Node property: ikea_dirigera/api_version
- Node property: ikea_dirigera/uuid

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

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

Arc availability
Since 1.10.0

Guardian availability
Since 26.2.0

Mitsubishi Electric MELSOFT

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

Device-side ports
UDP/5009, UDP/49153

Sensor-side ports
UDP/48888

Outbound network throughput
185 bytes

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

Arc availability
Since 1.7.0

Guardian availability
Since 24.5.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy melsoft.

Moxa

Use this strategy to discover Moxa devices that expose the Moxa Discovery protocol.

Device-side ports
UDP/4800

Sensor-side ports
UDP/48888

Outbound network throughput
8 bytes

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

- Device type
- MAC address
- 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.

Arc availability
Since 1.17.0

Guardian availability
Since 25.2.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy moxa.

ONVIF

Use this strategy to discover devices that expose the ONVIF protocol (mostly CCTV cameras).

Device-side ports
UDP/3702

Sensor-side ports
UDP/48888

Outbound network throughput
749 bytes

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

- Device type
- Product name
- Vendor
- Node property: onvif/endpoint

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

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

Arc availability
Since 1.9.0

Guardian availability
Since 24.5.0

Pepperl+Fuchs

Use this strategy to discover Pepperl+Fuchs devices that expose the Pepperl+Fuchs Discovery protocol.

Device-side ports
UDP/4606

Sensor-side ports
UDP/48888

Outbound network throughput
64 bytes

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

- Firmware version
- Product name
- Serial number
- Vendor
- Node property: pepperl+fuchs/ArticleNumber

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

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

Arc availability
Since 2.1.0

Guardian availability
Since 25.5.0

Reolink Baichuan

Use this strategy to discover Reolink devices that expose the UDP Baichuan protocol.

Device-side ports
UDP/2000

Sensor-side ports
UDP/3000

Outbound network throughput
4 bytes

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

- Device type
- Label
- MAC address
- 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.

Arc availability
Since 2.7.0

Guardian availability
Since 26.4.0

Siemens STEP7/Profinet

Use this strategy to discover Siemens devices that expose the Profinet protocol.

Device-side ports
This strategy uses PROFINET

Sensor-side ports
This strategy uses PROFINET

Outbound network throughput
46 bytes

Collected items
This strategy enriches the monitored nodes with this item: MAC address.

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

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

Arc availability
Since 1.7.0

Guardian availability
Not available

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy s7.

Sensor Net Connect

Use this strategy to discover Sensor Net Connect IoT smart sensors that expose the Sensor Net Connect Discovery protocol.

Device-side ports
UDP/30303

Sensor-side ports
UDP/48888

Outbound network throughput
28 bytes

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

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy sensor_net_connect.

Shelly mDNS

Use this strategy to discover Shelly devices using the mDNS network protocol.

Device-side ports
UDP/5353

Sensor-side ports
UDP/48888, UDP/5353

Outbound network throughput
57 bytes

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.

Arc availability
Since 2.2.0

Guardian availability
Since 25.6.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy shelly.

SMB

Use this strategy for devices that expose the SMB protocol.

Device-side ports
TCP/445

Sensor-side ports
Not applicable

Outbound network throughput
412 bytes

Collected items
This strategy enriches the monitored nodes with this item: Operating System.

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

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

Arc availability
Since 2.0.0

Guardian availability
Since 25.4.0

Tattile NTCP

Use this strategy to discover Tattile devices that expose the NTCP protocol.

Device-side ports
UDP/42000

Sensor-side ports
UDP/48888

Outbound network throughput
68 bytes

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.

Arc availability
Since 2.8.0

Guardian availability
Since 26.4.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy tattile_ntcp.

Ubiquiti

Use this strategy to discover Ubiquiti devices that expose the Ubiquiti Discovery protocol.

Device-side ports
UDP/10001

Sensor-side ports
UDP/48888

Outbound network throughput
8 bytes

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

- Firmware version
- Product name
- Vendor
- Node property: Essid
- Node property: Hostname

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

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

Arc availability
Since 1.12.0

Guardian availability
Since 24.5.0

UPnP

Use this strategy to discover devices that expose the UPnP protocol.

Device-side ports
UDP/1900

Sensor-side ports
UDP/48888

Outbound network throughput
91 bytes

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

Arc availability
Since 1.7.0

Guardian availability
Since 24.5.0

Smart Polling trigger
Nodes discovered through this strategy can trigger a Smart Polling execution with strategy upnp.