



Discovery Strategies Reference Guide

2025-11-03

Legal notices

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

Copyright

Copyright © 2013-2025, 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
ARP.....	12
AutomationDirect CLICK KOP.....	13
AutomationDirect Productivity.....	14
BACnet.....	15
Beckhoff.....	16
CODESYS.....	17
Cognex.....	18
SICK CoLa.....	19
EtherNet/IP.....	20
Tridium Niagara.....	21
Mitsubishi Electric MELSOFT.....	22
Moxa.....	23
Onvif.....	24
Pepperl+Fuchs.....	25
Siemens STEP7/Profinet.....	26
Sensor Net Connect.....	27
Shelly mDNS.....	28
SMB.....	29
Ubiquiti.....	30
UPnP.....	31



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 to ensure that devices are safely detected and enriched for accurate profiling and risk assessment, without impacting network stability. Discovery identifies devices on the network, while Smart Polling uses protocol-specific, low-impact methods to retrieve firmware versions, configurations, potential vulnerabilities, and other details that are not available 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 5 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 \(on page 7\)](#)

ARP

Use this strategy to discover multi vendor devices in the network through ARP requests.

Device-side ports

This strategy uses ARP

Sensor-side ports

Not applicable

Arc availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

EtherNet/IP

Use this strategy to discover multi vendor 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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

Onvif

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

Device-side ports

UDP/3702

Sensor-side ports

UDP/48888

Outbound network throughput

749 bytes

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Not available

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

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

SMB

Use this strategy on multi vendor devices that expose the SMB protocol.

Device-side ports

Not applicable

Sensor-side ports

TCP/445

Outbound network throughput

412 bytes

Arc availability

Available

Guardian availability

Available

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

Arc availability

Available

Guardian availability

Available

UPnP

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

Device-side ports

UDP/1900

Sensor-side ports

UDP/48888

Outbound network throughput

91 bytes

Arc availability

Available

Guardian availability

Available

