



Smart Polling 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
Smart Polling overview.....	7
Chapter 2. Strategies.....	9
Strategies overview.....	11
Advantech EKI HTTPS.....	12
AutomationDirect Productivity.....	13
Avalue UWB TCP.....	14
Axis HTTP(S).....	15
BACnet.....	16
Beckhoff.....	17
Bently Nevada.....	18
Dahua DHIP/DVRIP devices.....	19
EtherNet/IP.....	20
GE MDS TD Series Telnet.....	21
GE Telnet.....	22
Bosch Rexroth HTTP(S).....	23
Cognex HTTP(S).....	24
Fanuc HTTP(S).....	25
GE Healthcare HTTP.....	26
GE Grid Solutions HTTP.....	27
Lanner BMC HTTP(S).....	28
Schneider HTTP(S).....	29
Sewio HTTP(S).....	30
Tyan BMC HTTP(S).....	31
Ubisense HTTP(S).....	32
Inaba Choco Tei HTTP.....	33
Mitsubishi Electric MELSOFT.....	34
IEC 61850-8-1 (MMS).....	35
Modbus.....	36
Moxa.....	37
Moxa HTTP(S).....	38
Onvif HTTP(S).....	39
Phoenix Contact WP6000 HTTPS.....	40
Phoenix Contact mGuard.....	41
Phoenix Contact PLCNext HTTPS.....	42
Siemens STEP7.....	43
SEL telnet.....	44
Sensor Net Connect.....	45
Shelly mDNS.....	46

Siemens SIPROTEC HTTP(S).....47

SNMP.....48

SSH.....49

Tyco exacqVision.....50

UPnP.....51

Wago Management.....52

WinRM.....53

WMI.....54

Zettler/Ezcare TCP Gateway HTTP.....55

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



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 EKI HTTPS

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

Device-side ports

TCP/443

Arc availability

Available

Guardian availability

Available

AutomationDirect Productivity

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

Device-side ports

UDP/9999

Arc availability

Available

Guardian availability

Available

Avalue UWB TCP

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

Device-side ports

TCP/60511

Arc availability

Not available

Guardian availability

Available

Axis HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Available

Guardian availability

Available

BACnet

Use this strategy on devices that expose the BACnet protocol.

Device-side ports

UDP/47808

Arc availability

Available

Guardian availability

Available

Beckhoff

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

Device-side ports

TCP/443

Arc availability

Available

Guardian availability

Available

Bently Nevada

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

Device-side ports

TCP/3500

Arc availability

Available

Guardian availability

Available

Dahua DHIP/DVRIP devices

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

Device-side ports

UDP/37810, UDP/5050

Arc availability

Not available

Guardian availability

Available

EtherNet/IP

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

Device-side ports

TCP/44818

Arc availability

Available

Guardian availability

Available

GE MDS TD Series Telnet

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

Device-side ports

TCP/23

Arc availability

Available

Guardian availability

Available

GE Telnet

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

Device-side ports

TCP/23

Arc availability

Not available

Guardian availability

Available

Bosch Rexroth HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Cognex HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Fanuc HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

GE Healthcare HTTP

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

Device-side ports

TCP/8100

Arc availability

Available

Guardian availability

Available

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.

Device-side ports

TCP/80

Arc availability

Available

Guardian availability

Available

Lanner BMC HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Schneider HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Sewio HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

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.

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Ubisense HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Not available

Guardian availability

Available

Inaba Choco Tei HTTP

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

Device-side ports

TCP/80

Arc availability

Available

Guardian availability

Available

Mitsubishi Electric MELSOFT

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

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

Available

Guardian availability

Available

IEC 61850-8-1 (MMS)

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

Device-side ports

TCP/102

Arc availability

Available

Guardian availability

Available

Modbus

Use this strategy on multi vendor 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.

Device-side ports

TCP/502

Arc availability

Available

Guardian availability

Available

Moxa

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

Device-side ports

UDP/4800

Arc availability

Available

Guardian availability

Available

Moxa HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Available

Guardian availability

Available

Onvif HTTP(S)

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

Device-side ports

TCP/80, TCP/443

Arc availability

Available

Guardian availability

Available

Phoenix Contact WP6000 HTTPS

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

Device-side ports

TCP/443

Arc availability

Available

Guardian availability

Available

Phoenix Contact mGuard

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

Device-side ports

TCP/443

Arc availability

Available

Guardian availability

Available

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.

Device-side ports

TCP/443

Arc availability

Available

Guardian availability

Available

Siemens STEP7

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

Device-side ports

TCP/102

Arc availability

Available

Guardian availability

Available

SEL telnet

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

Device-side ports

TCP/23

Arc availability

Available

Guardian availability

Available

Sensor Net Connect

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

Device-side ports

UDP/30303

Arc availability

Available

Guardian availability

Available

Shelly mDNS

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

Device-side ports

This strategy uses udp

Arc availability

Available

Guardian availability

Available

Siemens SIPROTEC HTTP(S)

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

Device-side ports

TCP/4443

Arc availability

Available

Guardian availability

Available

SNMP

Use this strategy on multi vendor 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.

Device-side ports

UDP/161

Arc availability

Available

Guardian availability

Available

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).

Device-side ports

TCP/23

Arc availability

Not available

Guardian availability

Available

Tyco exacqVision

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

Device-side ports

TCP/80

Arc availability

Available

Guardian availability

Available

UPnP

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

Device-side ports

TCP/80

Arc availability

Available

Guardian availability

Available

Wago Management

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

Device-side ports

TCP/6626

Arc availability

Available

Guardian availability

Available

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.

Device-side ports

TCP/5985, TCP/5986

Arc availability

Not available

Guardian availability

Available

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.

Device-side ports

TCP/135

Arc availability

Not available

Guardian availability

Available

Zettler/Ezcare TCP Gateway HTTP

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

Device-side ports

TCP/80

Arc availability

Available

Guardian availability

Available

