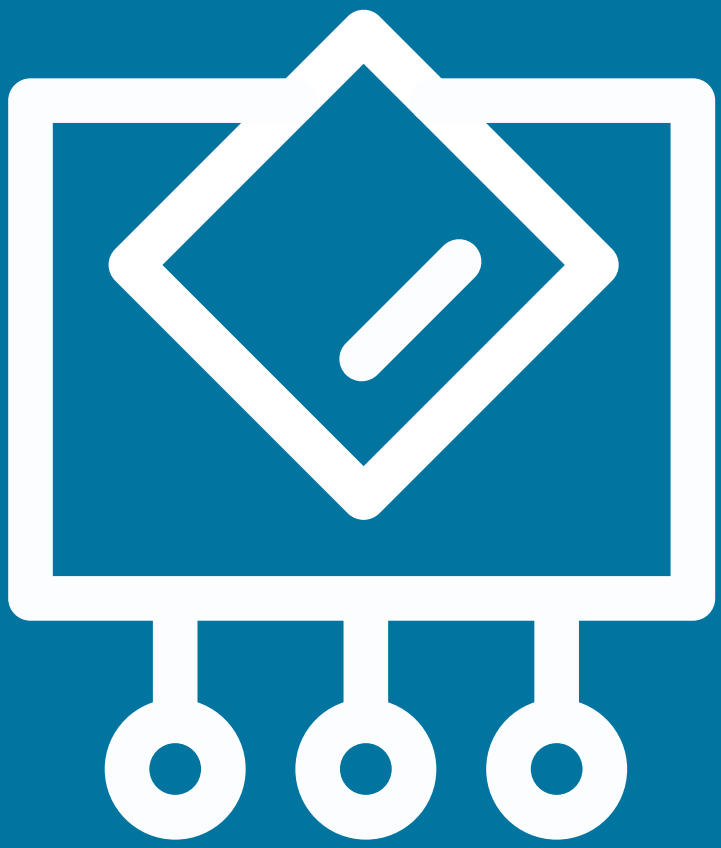
NOZOMI NETWORKS



Arc Embedded
Administrator Guide

Arc Embedded v2.10.0 — 2026-09-02

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

Arc Embedded

This version of Arc can be embedded directly on specific operational technology (OT) devices.

Arc Embedded is an innovative way to deploy Arc not only on computers, but also on devices used specifically in *operational technology (OT)* and *Internet of Things (IoT)* networks.

Arc Embedded is a particular instance of Arc, which adds detection that is based on the specific implementation. As such, this guide shows information and references to the non-embedded version of Arc, and references the applicable *operating system (OS)* of that specific implementation. For example, because Arc Embedded for Mitsubishi Electric runs on a Linux architecture, you will find references to applicable commands, and deployment options, for Linux.

General

When detecting cyberthreats, identifying vulnerabilities, or analyzing anomalies in your processes, it is critical to have as much detailed network and system information as possible. More accurate and timely access to data leads to better diagnostics and a faster time to repair.

Arc gives you enhanced endpoint data collection and asset visibility for your networks. This enhanced visibility gives you more:

- Vulnerability assessment capabilities
- Endpoint protection
- Traffic analysis capabilities
- Accurate diagnostics of in-progress threats and anomalies

Arc lets you easily identify compromised hosts that have:

- Malware
- Rogue applications
- Unauthorized *universal serial bus (USB)* devices
- Suspicious user activity

Architecture

It is important to understand the different architecture possibilities that are available with Arc.

You can connect Arc:

- To Guardian
- To Vantage

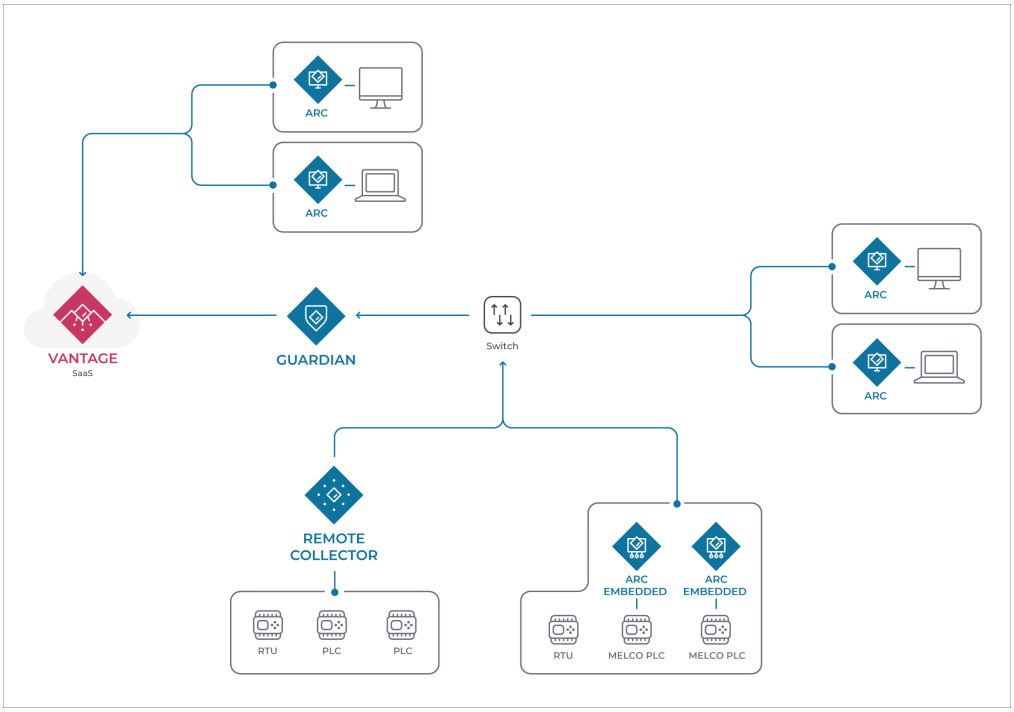


Figure 1. Arc architecture example

Arc in Vantage

*The **Sensors** page shows all the Arc sensors in the network. It also lets you connect an Arc sensor.*

Vantage Sensors page

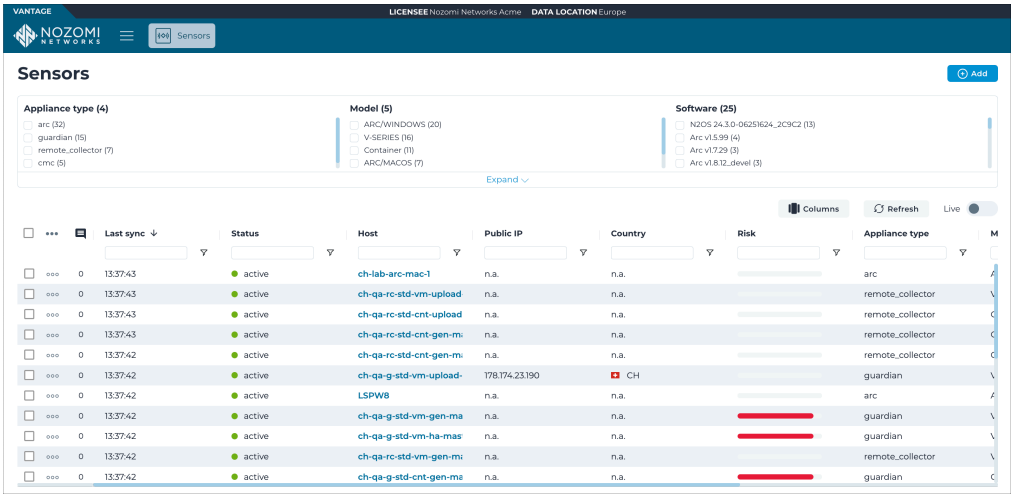


Figure 2. Vantage Sensors page

All Arc sensors in the network will show in the table on the **Sensors** page. The **Add new** button gives you access to the **Make connections** page. When you select **Arc**, you will see a list of Arc packages to download. This lets you select the correct Arc package for your *OS* and architecture.

Make connections page

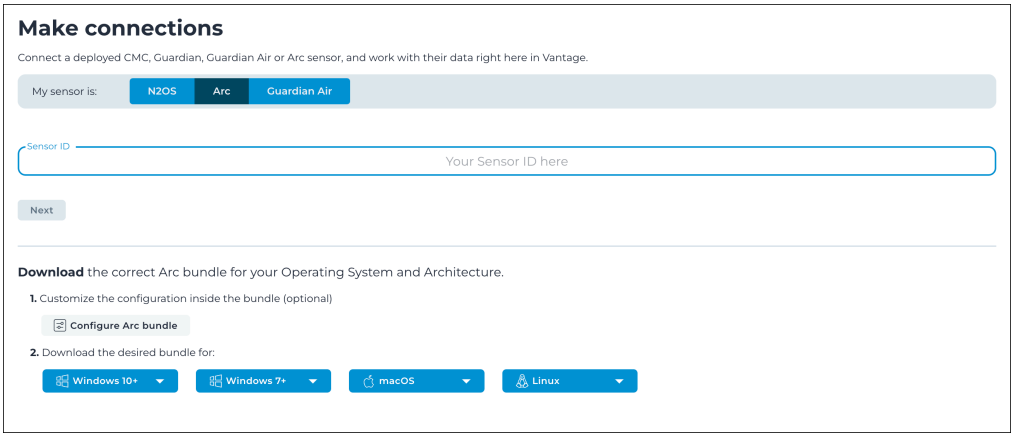


Figure 3. Make connections page

Configure an Arc sensor

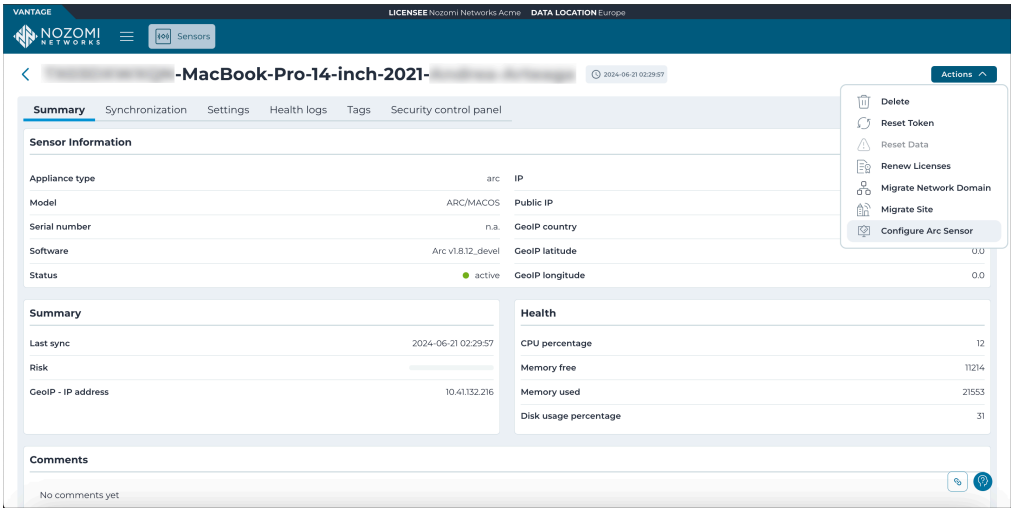


Figure 4. Actions menu in sensor details page

You can configure an individual Arc sensor directly from Vantage. To do this, in the details page for the related Arc sensor, select **Actions > Configure Arc Sensor**.

Configure multiple Arc sensors

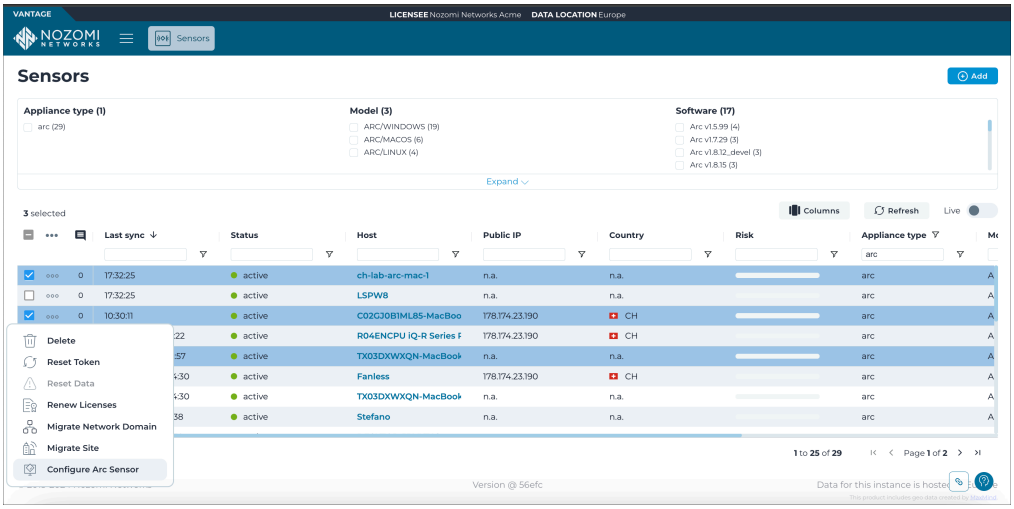


Figure 5. Configure multiple Arc sensors

You can configure multiple Arc sensors at the same time. To do this, select multiple Arc sensors in the table, then select ••• **> Configure Arc Sensor**.

Arc in Guardian

*The **Arc** button in the Guardian Web UI lets you access the different pages for Arc.*

Figure 6. Arc button in Guardian Web UI

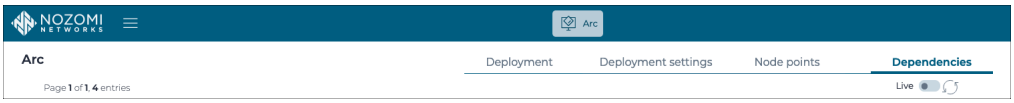


Figure 7. Arc button in Guardian Web UI (not connected to Vantage)

When you select **Arc** in the Guardian Web *user interface (UI)*, you get access to these pages:

- **Deployment**
- **Deployment settings**
- **Node points**
- **Dependencies** (only for Guardians that are not connected to Vantage)

Configure an Arc sensor

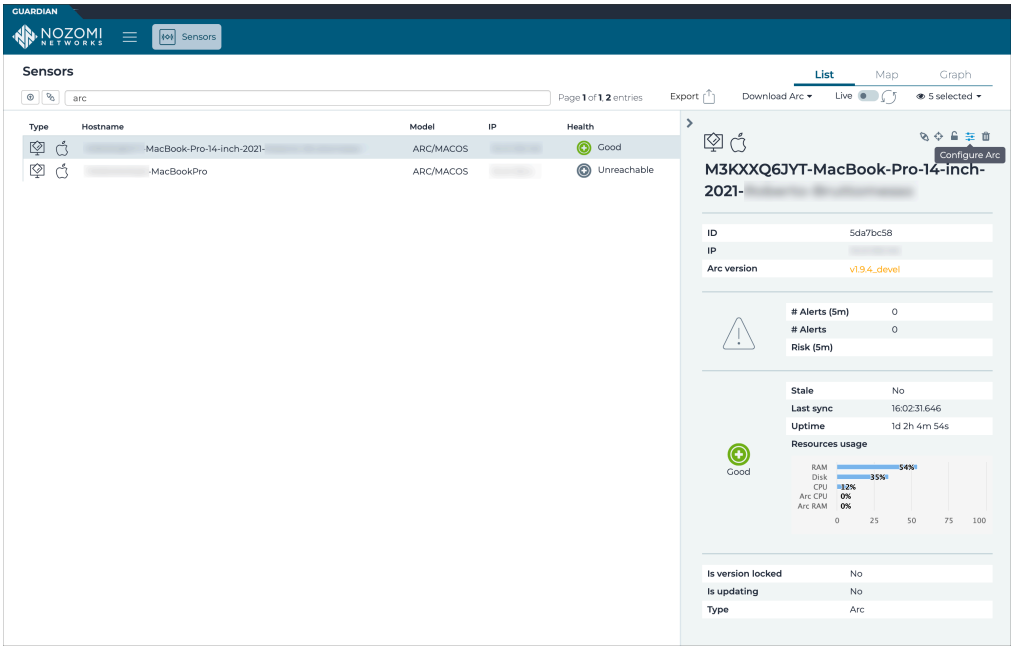


Figure 8. Configure an Arc sensor

You can configure an individual Arc sensor directly from Guardian. To do this, you can select the applicable Arc sensor from the **Sensors** list, and select the ⚙ icon.

Deployment

*The **Deployment** page shows a table of all the devices available for Arc deployment.*

The table only shows machines which have an *OS* that matches one that Arc supports.

As Guardian detects the installed *OS*, the correct Arc package will be automatically deployed.

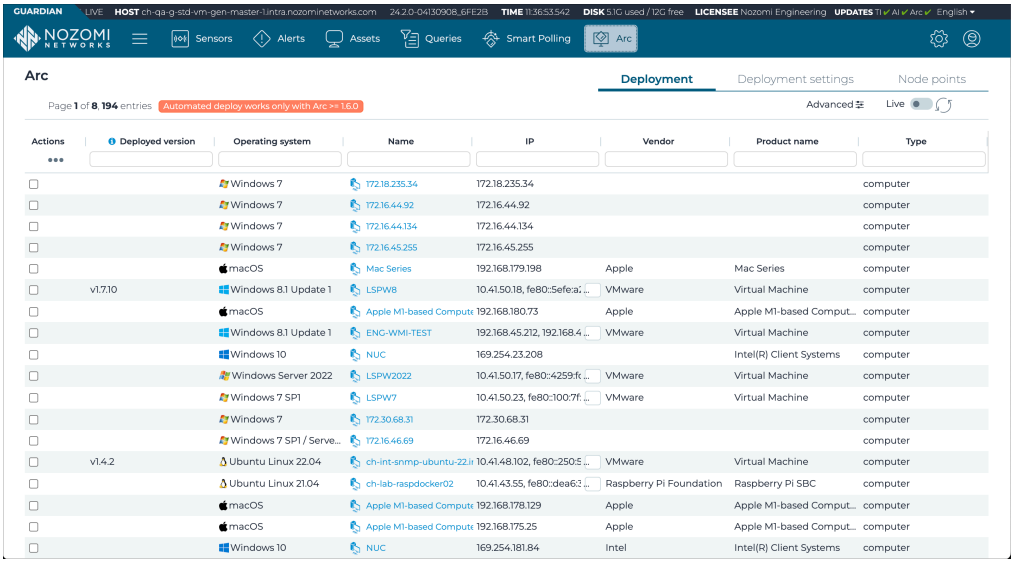


Figure 9. Deployment page

Advanced

The **Advanced** button lets you access the **Advanced** page. For more details, see Advanced (on page 14).

To deploy Arc Embedded sensors, you must select the **Advanced** page.

Execution details

The **Execution details** lets you access the **Activity Log**. For more details, see Execution details (on page 15).

Live toggle

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The icon lets you immediately refresh the current view.

Actions

The **ACTIONS** column has a checkbox for each row in the table. This lets you select multiple nodes before you then apply an action to them.

The **ACTIONS** menu icon ••• gives you access to these options:

- Select all in current page
- Select none in current page
- Invert selection in current page
- Deploy Service mode: this installs Arc in Service mode for the selected devices
- Remove Service mode: this removes the Arc previously installed in Service mode for the selected devices

Operating System

The **OPERATING SYSTEM** column shows the *OS* for each of the Arc sensors in the table. The field at the top of the column lets you use the *OS* to filter the table.

IP

The **IP** column shows the *internet protocol (IP)* for each of the Arc sensors in the table. The field at the top of the column lets you use the *IP* to filter the table.

Vendor

The **VENDOR** column shows the vendor name for each of the Arc sensors in the table. The field at the top of the column lets you use the vendor name to filter the table.

Product name

The **PRODUCT NAME** column shows the product name for each of the Arc sensors in the table. The field at the top of the column lets you use the product name to filter the table.

Type

The **TYPE** column shows the device type for each of the Arc sensors in the table. The field at the top of the column lets you use the device type to filter the table.

Advanced

The **Advanced** *page lets you interact with nodes that have no operating system (OS) detected, or do not show on the same page in the table.*

The default table view only shows nodes that have had their *OS* detected. Also, if you select multiple nodes, actions will only be applied to a single page of nodes. To overcome these limitations, you can use the **Advanced** button to go to the **Advanced** page. This will let you interact with a:

- Set of nodes that cannot be shown on a single page
- Set of nodes that have no *OS* detected

Figure 10. Advanced page

Strategy

Automatic: This selection will use the *OS* that has been detected on the node to automatically choose a deployment strategy. You can select multiple nodes that have a different *OS*. This strategy will ignore a host if it has no *OS*.

SSH (Linux): This selection will force the *secure shell (SSH)* strategy, regardless of the *OS*, and deploy the correct Arc package for Linux.

Query

This field lets you create and execute queries on the nodes. This lets you filter and selectively install packages.

Timeout (seconds)

The **Timeout** dropdown lets you set the amount of time that Arc will try to communicate with a host machine before it skips it and goes to the next one.

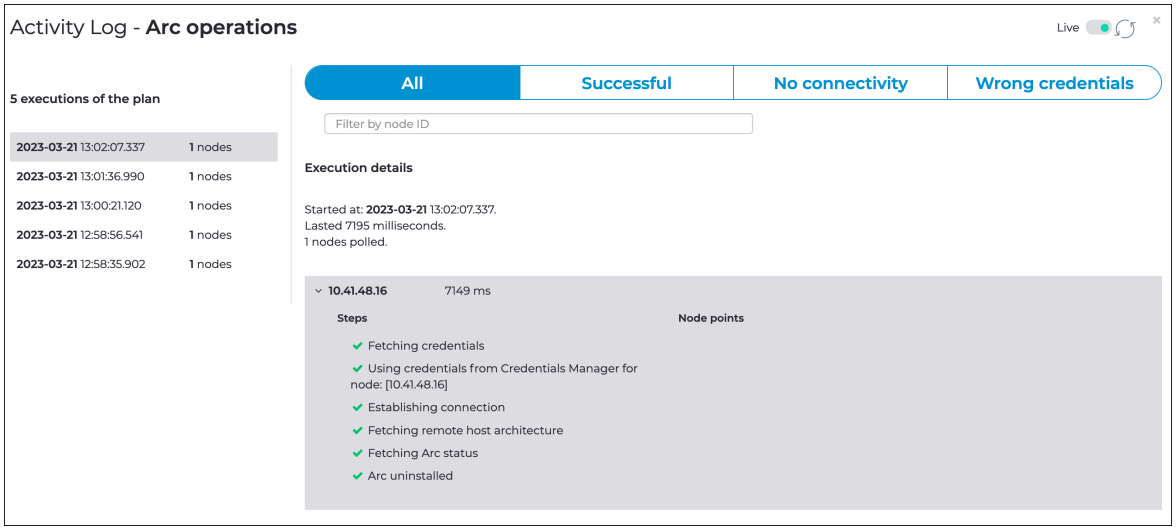
Execution details

*The **Execution details** button gives you access to the **Activity Log**.*

The **Activity Log** lets you troubleshoot the results of the executed deployments. When you select an execution on the left side of the page, you can analyze the selection.

You can use the **Filter by node ID** to focus on a single issue, such as:

- Credential missing, or
- Wrong credentials



Live toggle

The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh

The  icon lets you immediately refresh the current view.

Deployment settings

Configure Arc deployment parameters that will be included in downloaded Arc bundles. These settings define how Arc will behave when deployed from Guardian.

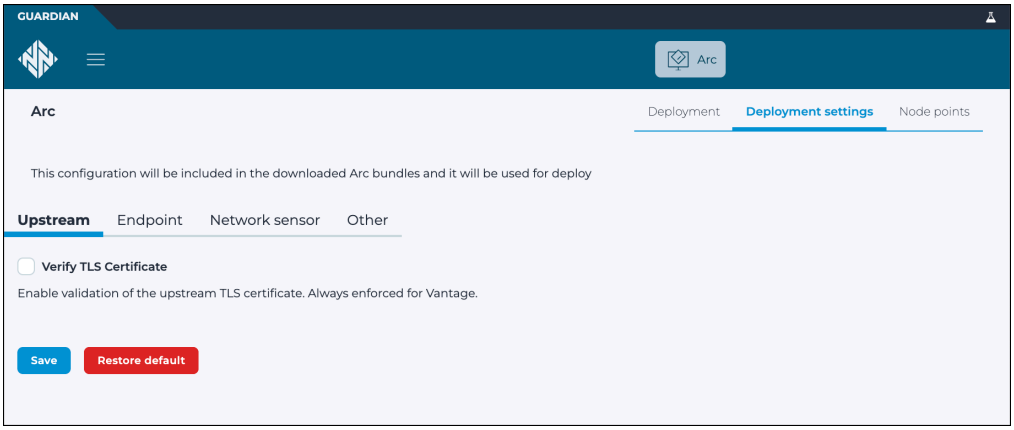


Figure 11. Deployment settings page

The **Deployment settings** page has these tabs:

- Upstream (on page 17)
- Endpoint (on page 18)
- Network sensor (on page 20)
- Other (on page 22)

Restore default

Once the settings have been saved, you can use this button to restore the default configuration.

Upstream

*The **Upstream** page lets you configure the settings for your Arc deployment.*

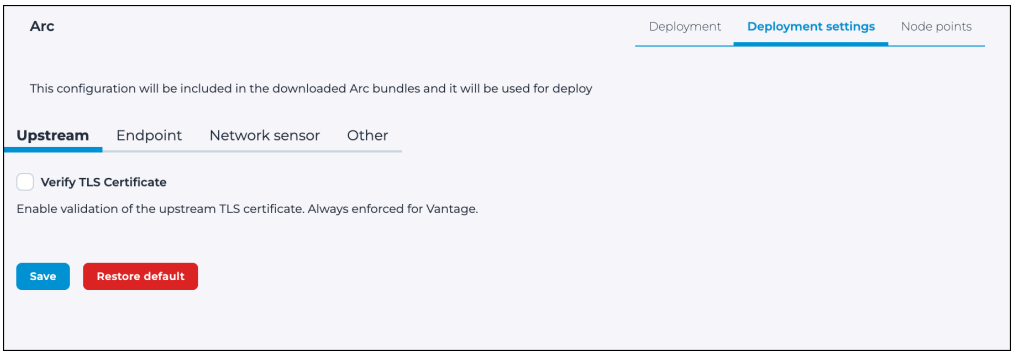


Figure 12. Upstream page

Verify TLS Certificate

Select this option to enforce verification of the upstream *transport layer security (TLS)* certificate when connecting to Guardian. When using Vantage, *TLS* certificate validation is always enforced, regardless of this setting.

Restore default

Once the settings have been saved, you can use this button to restore the default configuration.

Endpoint

*The **Endpoint** page lets you configure the settings for your Arc deployment.*

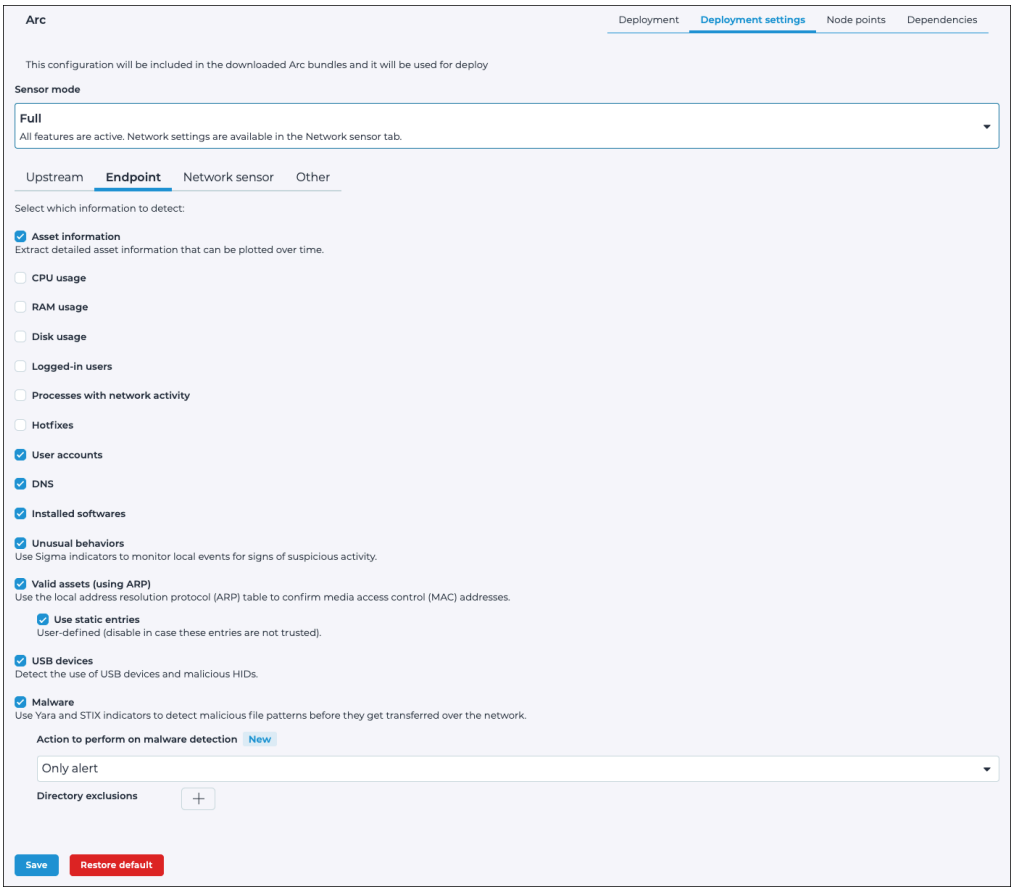


Figure 13. Endpoint page

Asset information

Enable **Asset information** to collect detailed information about the endpoint. Arc collects the following data:

- **CPU usage**: The current processor load of the endpoint.
- **RAM usage**: The amount of memory currently in use on the endpoint.
- **Disk usage**: The current disk space usage on the endpoint.
- **Logged-in users**: The users currently logged in to the endpoint.
- **Processes with network activity**: The running processes that have active network connections, including the local and remote addresses and ports.
- **Hotfixes**: The security patches and updates installed on the endpoint (Windows only).
- **User accounts**: The local user accounts configured on the endpoint.
- **DNS**: The *domain name server (DNS)* servers and configuration of the endpoint.
- **Installed software**: The software packages installed on the endpoint.

Unusual behaviors (Windows only)

This lets you enable/disable Sigma rules for local behavior analysis.

Valid assets (using ARP)

Enable this option to use the local *address resolution protocol (ARP)* table to confirm *media access control (MAC)* addresses for connected assets.

Enable **Use static entries** to include user-defined static *ARP* table entries in the validation. Only enable this if the static entries are trusted.

USB devices (Windows only)

This lets you enable/disable *USB* detections.

Malware (Windows only)

The **Malware** checkbox lets you enable protection mode and select from the **Action to perform on malware detection** dropdown. This lets you set the action that Arc will take when it finds a malicious file.

You can choose from these options:

- **Only alert**: Receive an alert with no further action
- **Quarantine**: Move the malicious file to the `quarantine` folder, which is located in the Arc installation folder
- **Delete**: Immediately delete the malicious file. Once deleted, the files cannot be recovered

You can also use the **Directory exclusions** feature to exclude specific directories from malware scanning. Select + to open a file browser and select a directory. You can add as many directories as needed. Arc skips the selected directories when scanning for malware.

Restore default

Once the settings have been saved, you can use this button to restore the default configuration.

Network sensor

*The **Network sensor** page lets you configure the settings for your Arc deployment.*

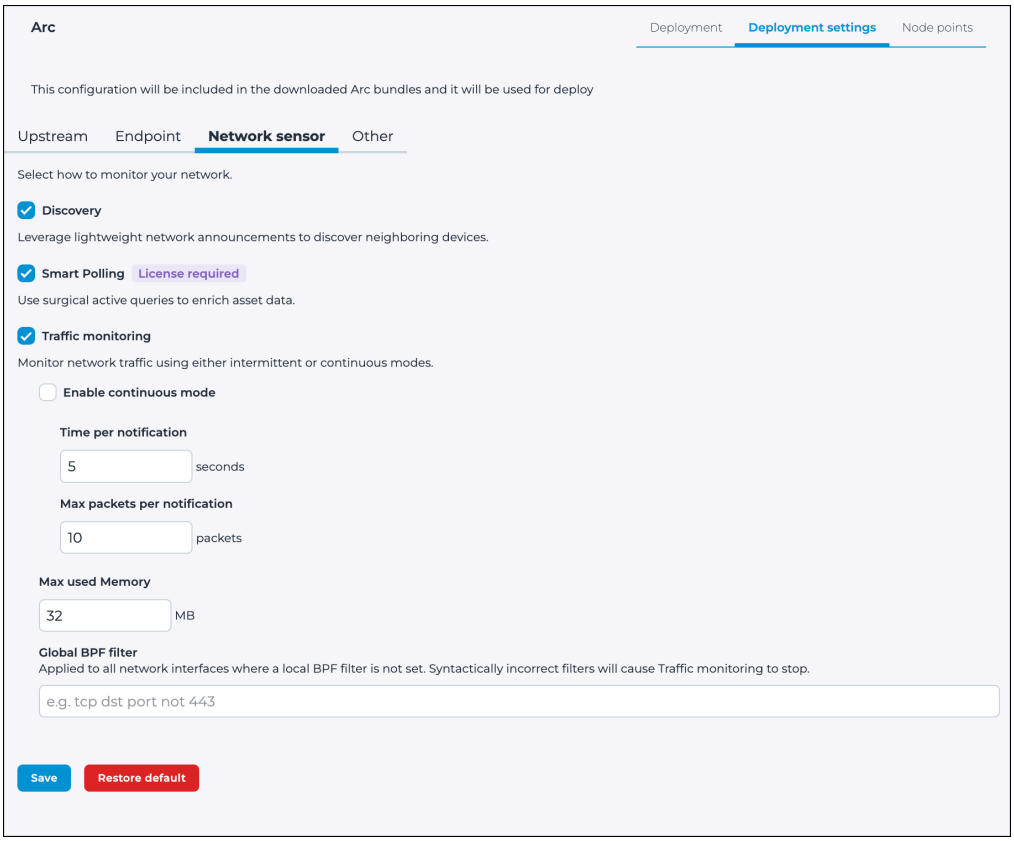


Figure 14. Endpoint page

Discovery

When enabled, this sends out unsolicited lightweight network announcements to discover neighboring nodes.

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.

Smart Polling

This lets you enable/disable the execution of Smart Polling strategies from Arc. When enabled, this sends out Smart Polling queries following remote requests coming from Guardian to poll assets that Arc can reach, or assets that have been identified with Discovery.

Note:

Smart Polling requires that a Smart Polling license is enabled upstream.

To force Smart Polling from a specific Arc sensor, even when Guardian was the first to monitor a node, you can use a *command-line interface (CLI)* command such as: `vi node 192.168.1.1 capture_device arc[1e6a174c]` In this example, `192.168.1.1` is an *IP* address of a node you want to poll from a specific Arc sensor. `1e6a174c` are the first eight characters of the Arc sensor *identifier (ID)* that you want to poll the node with. To find that sensor *ID*, you can select the Arc sensor from the **Sensors** page of your Guardian and read the **ID** field in the right pane. To reset the behavior, you can set the `capture_device` back to the value of the Guardian interface.

Traffic monitoring

When enabled, this checkbox lets you enable/disable traffic monitoring.

Enable continuous mode

This checkbox lets you enable/disable continuous mode. For more details, see **Continuous mode**.

Arc uses two different methods for traffic monitoring:

- Intermittent mode
- Continuous mode

Intermittent mode: This is the default mode, the traffic is monitored, or sniffed, for a duration of 10 seconds at each notify. The purpose of this limitation is to preserve the resources of the host machine, which prevents excessive memory, or *central processing unit (CPU)*, spikes. You can configure these options:

Continuous mode: This mode sniffs traffic continuously from the host's network interface controllers. Depending on the amount of sniffed traffic, continuous mode might utilize more *CPU* and memory on the host. As the traffic is processed upstream, the performance of the remote endpoint is also affected. You can configure:

- **Time [s] per notification**
- **Max packets per notification**
- **Max used Memory (MB)**: this value can be tuned to allow more or less traffic buffering in case the traffic to process exceeds the Arc and network capacity to send it out

Global BPF filter

This field lets you set a Global BPF filter to apply to all the network interfaces. Filters that are applied to single interfaces will take precedence over the global one.

Network interface

This dropdown lets you select a network interface to configure. Each network interface can then be enabled, and be tuned with a monitoring filter.

If you add, remove, or edit the network interfaces on the host, Arc does not automatically add it to the list of sniffing interfaces. For example, if you add a new network card, to enable Arc to use it, you should stop Arc, and then start it again.

Restore default

Once the settings have been saved, you can use this button to restore the default configuration.

Other

*The **Other** page lets you configure the settings for your Arc deployment.*

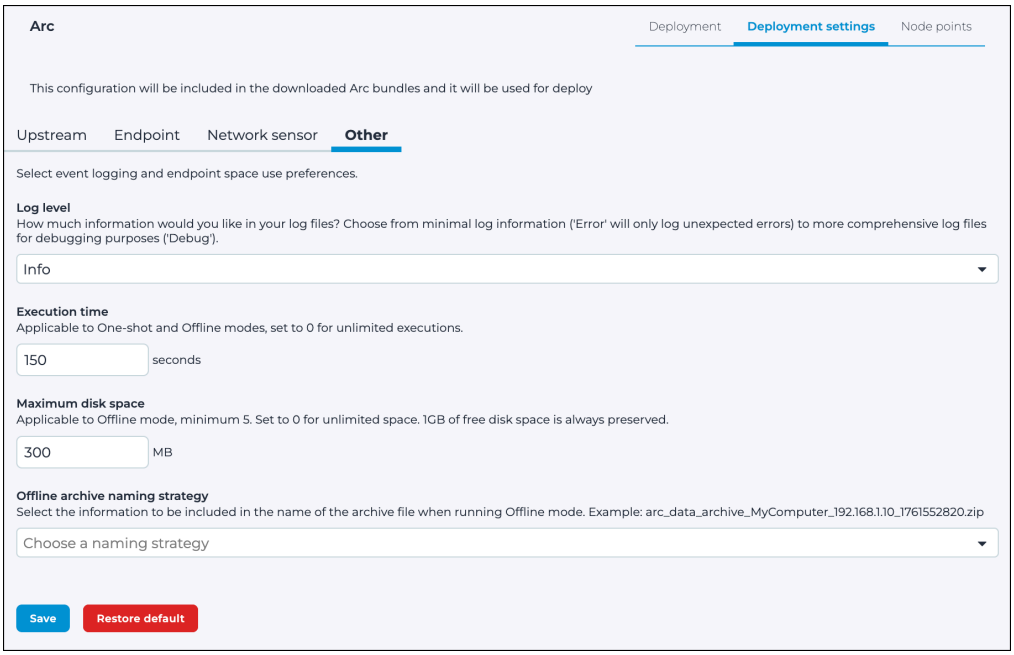


Figure 15. Other page

Log level

This dropdown lets you select the verbosity level for the log files. The options are:

- Debug
- Info
- Warning
- Error

The logging system options have an increasing level of verbosity, from the least verbose to the most verbose. Error < Warning < Info < Debug.

- Error: Creates a minimalistic log, only unexpected errors are logged
- Warning: Creates extra errors that might show on some *OS*s, but that are generally considered as acceptable
- Info: Logs relevant successful events, it shows the program's progress (recommended)
- Debug: Logs extra events that are normally useful for debugging purposes. Given its verbosity it is best to activate it only when debugging activities are involved

Note:

This setting applies to:

- `arc.log.txt`
- `arc_service.log.txt`
- `sp.log.txt`

It doesn't apply to `setup.log`, which covers Arc's initialization process, before the configuration has been loaded and applied.

For more details, see Log files (on page).

Execution time

This field lets you set the time that Arc will run to collect data. This is applicable for One-shot and Offline modes.

Note:
When this is set to 0, the execution time is interpreted as infinite.

Maximum disk space

This field lets you control the maximum amount of disk space in *megabyte (MB)* that will be used for Offline mode.

Offline archive naming strategy

This lets you select the information that will be included in the name of archive files created while running Offline mode.

Restore default

Once the settings have been saved, you can use this button to restore the default configuration.

Node points

*The **Node points** page shows data points that are collected over time, and represent the state of the target machine.*

Node points count
This shows the number of the nodes polled.

Filter by node ID
This field lets you use the node *ID* to filter the nodes.

Live toggle
The **Live** toggle lets you change live view on, or off. When live mode is on, the page will refresh periodically.

Refresh
The  icon lets you immediately refresh the current view.

Nodes
The list of nodes that show at least one node point.

Dependencies

*The **Dependencies** page shows the status of the dependencies. When a dependency is missing, you can use the upload icon in the **Actions** column to upload it.*

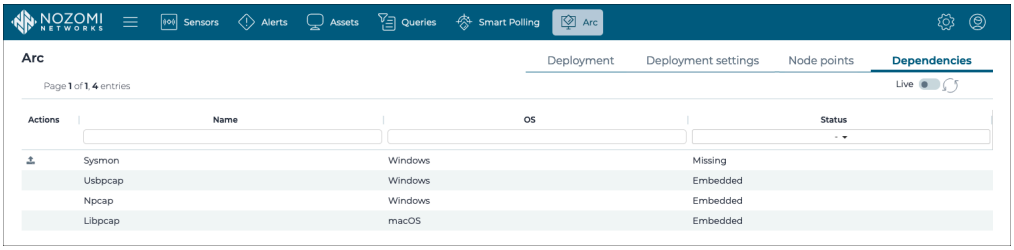


Figure 16. Dependencies page in Guardian (not connected to Vantage)

Arc in CMC

*The **Arc** button in the Central Management Console (CMC) Web UI lets you access the different pages for Arc.*

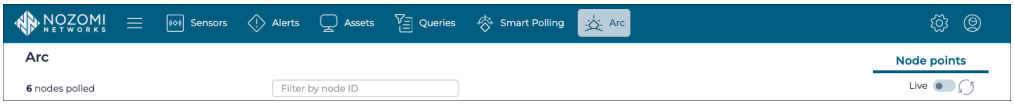


Figure 17. Arc button in CMC Web UI

When you select **Arc** in the *Central Management Console (CMC)* Web *UI*, you get access to the **Node points** page.

Viewing data from Arc

The data Arc acquires can be viewed in different places, and in different formats.

Nodes discovered

You can view nodes by their capture device:

- In **Network view > Nodes**, check that the **capture_device** field contains `arc`
- In **Queries**, with the term: `nodes | where capture_device include? arc`

Asset view information sources

When Arc asset detections populate a field, an Arc dedicated source is used. When Arc uses network monitoring to discover nodes, the source will show as passive. See Nodes discovered (on page 26).

Node points

When Smart Polling is not enabled, all node points come from Arc. When both Arc and Smart Polling are active in Guardian, you can find nodes that are from Arc:

- In **Arc > Node points**
- In **Queries**, with the term: `node_points | where source.type == arc`

Dedicated alerts

In addition to the standard alerts, the alerts shown below come only from Arc:

- `SIGN:SIGMA-RULE`
- `SIGN:MALICIOUS-HID`
- `SIGN:USB-DEVICE`
- `SIGN:USB-FILE-TRANSFER`
- `SIGN:BOOT-SECURITY-ERROR`
- `SIGN:SD-CARD`
- `SIGN:FIRMWARE:CHANGE`
- `SIGN:LOGIN`

Users field in alerts

Alerts that are generated from Arc, or involve a node hosting Arc, include information about the logged users. In case of SIGN:SIGMA-RULE alerts, the user associated to the process triggering the Sigma rule is used.

Security measures

A description of the security measures that Arc uses.

Management

Admin/root users should manage Arc and should do the:

- Install
- Uninstall
- Execution

Obfuscation

Executable files are subject to obfuscation.

Unidirectional communication

It is not possible for an external host to establish communication to Arc to use it as an attack vector to the machine hosting it.

Communication

Arc uses *TLS* 1.2/1.3 communication to the upstream machine.

Data availability

If the communication link between Arc and Vantage/Guardian becomes unavailable, Arc keeps the collected information locally. Once the communication link is available again, the information will be sent. The maximum amount of collected information depends on the resource usage limits that have been set.

Detection information

The information that Arc detects. The table shows two types of **Category***:* **sensor** *and* **endpoint***. When the* **Category** *is listed as* **sensor***, it means that the detection is based on information that has been extracted from the sensor. When the* **Category** *is listed as* **endpoint***, it means that the detection is based on information that has been extracted from the endpoint.*

Linux-native detection information

The native detection information in the table below applies to the Linux module hosting Arc Embedded.

Category	Information	Linux	Configuration option
sensor	Traffic monitoring	✓	Traffic monitoring
sensor	Discovery	✓	Discovery
sensor	Smart Polling	✓	Smart Polling
endpoint	*MAC* addresses	✓	always on
endpoint	*IP* addresses	✓	always on
endpoint	Product name	✓	always on
endpoint	Vendor	✓	always on
endpoint	Label/host name	✓	always on
endpoint	*OS*	✓	always on
endpoint	Serial number	✓	always on
endpoint	Local *ARP* table	✓	Local *ARP* table
endpoint	*USB* detections	✓	*USB* detections

Category	Information	Linux	Configuration option
endpoint	*CPU* usage	✓	node points
endpoint	Memory usage	✓	node points
endpoint	Disk usage	✓	node points
endpoint	Installed software	✓	node points
endpoint	Log4j detection	✓	node points
endpoint	Disk partitions	✓	node points
endpoint	*DNS*	✓	node points

Detection information specific to Mitsubishi Electric MELSEC iQ-R

The information that Arc detects. The table shows two types of **Category***:* **sensor** *and* **endpoint***. When the* **Category** *is listed as* **sensor***, it means that the detection is based on information that has been extracted from the sensor. When the* **Category** *is listed as* **endpoint***, it means that the detection is based on information that has been extracted from the endpoint.*

Detection information specific to Mitsubishi Electric MELSEC iQ-R

Category	Information	Supported by *	Configuration option
endpoint	Nodes aggregation	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Local state (light-emitting diode (LED) panel information) through these alert types: • `SIGN:DEV-STATE-CHANGE` • `SIGN:OT_DEVICE-START` • `SIGN:OT_DEVICE-STOP`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Disconnection of Ethernet cable through: `SIGN:DEV-STATE-CHANGE`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Disconnection of module through: `SIGN:DEV-STATE-CHANGE`	RnP, RnPSF *CPU* models	always on
endpoint	Program transfer through: `SIGN:PROGRAM-TRANSFER`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Program change through: `SIGN:PROGRAM-CHANGE`	Rn *CPU* models	always on
endpoint	Firmware change through: `SIGN:FIRMWARE-CHANGE`	Rn, RnP, RnPSF *CPU* models	always on
endpoint	Remote login through: `SIGN:LOGIN`	RnSF, RnPSF *CPU* models	always on

Category	Information	Supported by *	Configuration option
endpoint	Attach of module through: `SIGN:DEV-STATE-CHANGE`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Insertion of SD card through: `SIGN:SD-CARD`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Removal of SD card through: `SIGN:SD-CARD`	Rn, RnP, RnSF, RnPSF *CPU* models	always on
endpoint	Remote password successful login through: `SIGN:LOGIN`	R120SFCPU, R00CPU, R01CPU, R02CPU, R04CPU, R04ENCPU, R08CPU, R08ENCPU, R08PCPU, R08PSFCPU, R08SFCPU, R16CPU, R16ENCPU, R16PCPU, R16PSFCPU, R16SFCPU, R32CPU, R32ENCPU, R32PCPU, R32PSFCPU, R32SFCPU, R120CPU, R120ENCPU, R120PCPU, R120PSFCPU	always on
endpoint	Remote password login failure through: `SIGN:LOGIN`	R120SFCPU, R00CPU, R01CPU, R02CPU, R04CPU, R04ENCPU, R08CPU, R08ENCPU, R08PCPU, R08PSFCPU, R08SFCPU, R16CPU, R16ENCPU, R16PCPU, R16PSFCPU, R16SFCPU, R32CPU, R32ENCPU, R32PCPU, R32PSFCPU, R32SFCPU, R120CPU, R120ENCPU, R120PCPU, R120PSFCPU	always on
endpoint	Boot function security error through: `SIGN:BOOT-SECURITY-ERROR`	Rn, RnP, RnSF, RnPSF *CPU* models	always on

* Reference: MELSEC iQ-R Ethernet User's Manual (Application).

Detection information specific to Schneider Electric SCADAPack 47xi RTU

The information that Arc detects. The table shows two types of **Category***:* **sensor** *and* **endpoint***. When the* **Category** *is listed as* **sensor***, it means that the detection is based on information that has been extracted from the sensor. When the* **Category** *is listed as* **endpoint***, it means that the detection is based on information that has been extracted from the endpoint.*

Detection information specific to Schneider Electric SCADAPack 47xi RTU

Category	Information	Configuration option
endpoint	RTU identification	always on
endpoint	Process variables information	always on
endpoint	Insertion of *USB* drive through: `SIGN:USB-DEVICE`	always on
endpoint	Insertion of *secure digital (SD)* memory card through: `SIGN:SD-CARD`	always on
endpoint	Removal of *SD* memory card through: `SIGN:SD-CARD`	always on
endpoint	Operation on device mechanical switch through: `SIGN:DEV-STATE-CHANGE`	always on
endpoint	Device time change through: `SIGN:SUSP-TIME`	always on
endpoint	Firmware change through: `SIGN:FIRMWARE-CHANGE`	always on
endpoint	A low power supply input through: `SIGN:DEV-STATE-CHANGE`	always on
endpoint	A program change through: `SIGN:PROGRAM-CHANGE`	always on

Chapter 2. Requirements

Endpoint operating system requirements

To operate Arc, you will need to make sure that you have the correct operating system (OS) installed on the endpoint.

Table 1. Mitsubishi Electric

Operating System	Architecture	Description
Linux	arm (Use MELCO-specific bundle)	The correct Linux image needs to be installed. The default installed *OS* is VxWorks, which needs to be updated.

Table 2. Schneider Electric

Operating System	Architecture	Description
Linux	arm	The SCADAPack 47xi filesystem image is read-only but can accept a read/write filesystem overlay that is installed on the Edge platform's SD card. To install the overlay, see the Schneider Electric documentation.

Endpoint hardware requirements

The resource requirements for Arc will depend on the traffic loads and other options.

Arc Embedded is only compatible with:

- MELSEC iQ-R series with a RD55UP12-V intelligent function module
- Schneider Electric SCADAPack 47xi RTU

A baseline installation of Arc, with no traffic monitoring, requires:

- Up to 100 MB of free disk space
- Up to 80 MB of free RAM

Both the options that are activated, and the traffic load on the machine, will affect the resource consumption of both the *CPU* and the *random-access memory (RAM)*.

Nozomi Networks software requirements

For a successful deployment, your Nozomi Networks software must meet the minimum requirements.

To use Arc Embedded for MELSEC iQ-R series, your other software must meet these minimum requirements:

- Vantage, or
- Guardian v25.2.0, or later
- Arc v1.10.0, or later

To use Arc Embedded for SCADAPack 47xi *remote terminal unit (RTU)*, your other software must meet these minimum requirements:

- Vantage, or
- Guardian v25.2.0, or later
- Arc v2.0.0, or later

Chapter 3. Preparation

Arc licenses

Before you can deploy and use Arc, you will need to buy a license. How Arc licenses are installed will depend on the existing installation that you have. Arc and Arc Embedded require separate licenses.

Guardian

If you buy an Arc license for a Guardian installation, you will need to install the license. The Arc license enabled in Guardian provides for the Arc sensors that are downstream.

When the licensed Arc sensors are all connected and allowed, additional sensors can be added, but in a disallowed state. Disallow some sensors to allow the new ones.

Arc will be automatically updated when a new version is released. When the latest version of Arc is installed, a green tick will show adjacent to the **Arc** in the **UPDATES** section of the Web *UI*.

Without the update service, you will need to download the new package from the Support Portal and install the update manually.

Vantage

If you buy an Arc license for a Vantage installation, Vantage will act as a license server, and no other action is necessary. As soon as this license is active, Vantage is ready to accept incoming Arc sensor connections. All Arc updates will happen automatically, through any combination of *CMC* and Guardian sensors downstream.

When the licensed Arc sensors are all connected, in order to connect more sensors you will need to buy additional licenses.

CMC

If you buy an Arc license for a *CMC* installation, you will need to install the license. The Arc license enabled in *CMC* provides for the Arc sensors that are downstream, either through one Guardian, or multiple Guardian sensors.

Install a license in Guardian or CMC

Before you can use Arc you must install the applicable license.

Before you begin

If you are installing an additional license, make sure that you have installed a base license first.

Procedure

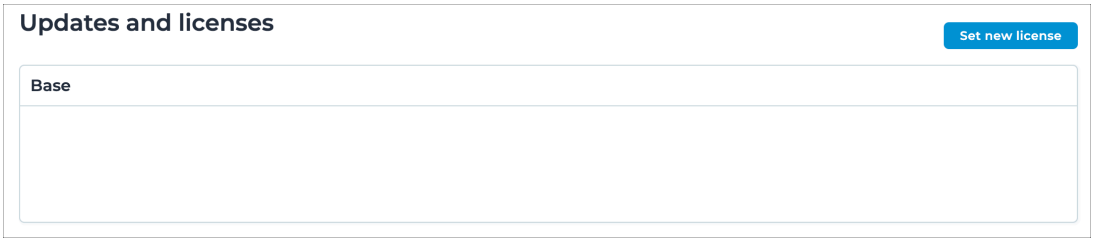
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

2. In the **System** section, select **Updates and licenses**.

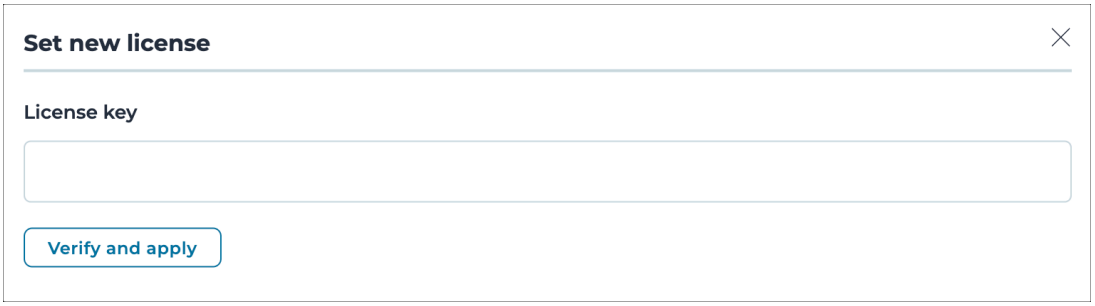
   Result: The **Updates and licenses** page opens.

3. In the top right of the section, select **Set new license**.



   Result: A dialog shows.

4. To copy the **Machine ID**, select **Copy**.



5. Send the machine *ID* to Nozomi Networks with your license request.
6. Wait to receive your license key from Nozomi Networks.
7. In the **License key** field, paste the license key.
8. Select **Verify and apply**.

Results

The license has been installed.

Import Arc through the update service in Guardian or CMC

Before you can deploy Arc, you must import it first. There a two methods you can use to do this, one method is through the Nozomi Networks Update Service. The alternative method is through a manual contents upload.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

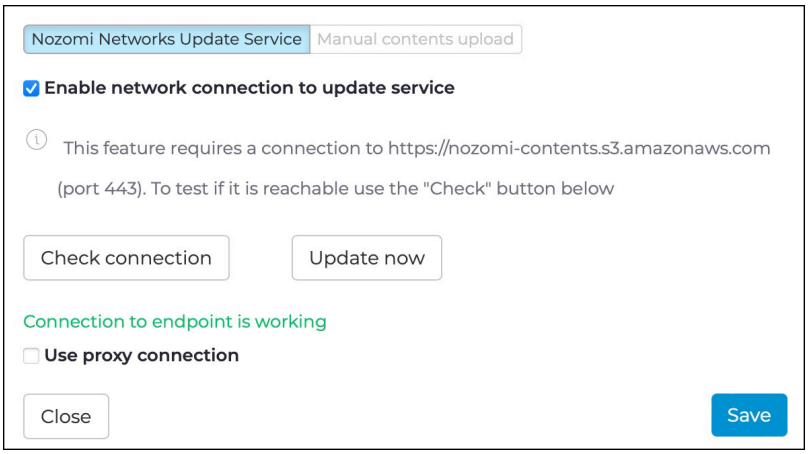
2. In the **System** section, select **Updates and licenses**.

   Result: The **Updates and licenses** page opens.

3. In the top, right corner, select **Update service configuration**.

   Result: A dialog opens.

4. Select **Nozomi Networks Update Service**.



5. To make sure that the connection is okay, select **Check connection**.

   Result: A message shows to confirm that the `Connection to endpoint is working`.

6. Select **Update now** to immediately download the Arc packages.

Import Arc through a manual contents upload in Guardian or CMC

Before you can deploy Arc, you must import it first. There a two methods you can use to do this, one method is through a manual contents upload. The alternative method is through the Nozomi Networks Update Service.

Before you begin

Make sure that you have downloaded the Arc .bin package.

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

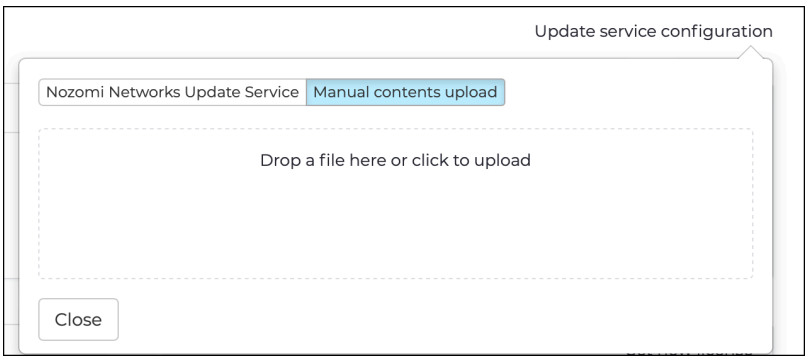
2. In the **System** section, select **Updates and licenses**.

   Result: The **Updates and licenses** page opens.

3. In the top, right corner, select **Update service configuration**.

   Result: A dialog opens.

4. Select the **Manual contents upload** button.



5. Drag and drop the `.bin` Arc package, that you downloaded from the Nozomi Networks support portal, into the upload field.

   Result: A progress bar shows and the update is verified.

6. Select **Close**.

Dependencies

To enable all the functions of Arc, you need to have certain items installed on the host machine.

Table 3. Linux dependencies

Traffic monitoring	Not needed
Asset details	*dmidecode*

During Automatic deployment, dependencies are also installed. To install the dependencies manually, download them and install them individually. Alternatively, you can use a *mobile device management (MDM)* tool to install them across the managed network.

Local services

It is important to understand the different local services that are necessary for the different operating systems.

Linux

On Linux, you need the *SSH* service to deploy Arc automatically through Guardian.

User permissions

Arc collects a diverse set of information from the hosting machine, and can take control of the network interfaces. To grant full functionality, Administration/root permissions are needed.

To collect system and network data, Arc requires administrative or root permissions on the host system. These permissions enable full control of network interfaces and ensure complete functionality.

Connectivity

Arc connects to Guardian and Vantage through designated protocols and ports.

Arc communicates to Guardian or Vantage through the *hypertext transfer protocol secure (HTTPS)* protocol (*transmission control protocol (TCP)*/443).

Automatic deployment

For automatic deployment, you need *SSH* (*TCP*/22).

Hardware setup for Mitsubishi Electric MELSEC iQ-R PLC

The recommended physical setup for the Mitsubishi Electric MELSEC iQ-R programmable logic controller (PLC).

The RD55UP12-V module has two network interfaces. Arc uses one of these to connect to the upstream sensor. It is recommended to use the second network interface to monitor and have it connected to a switch SPAN port to get all the data from the *CPU* module.

This setup works best in combination with Smart Polling enabled, leveraging the Mitsusbishi Electric MELSOFT strategy. The port used to connect to the upstream is also then used as a Smart Polling interface.

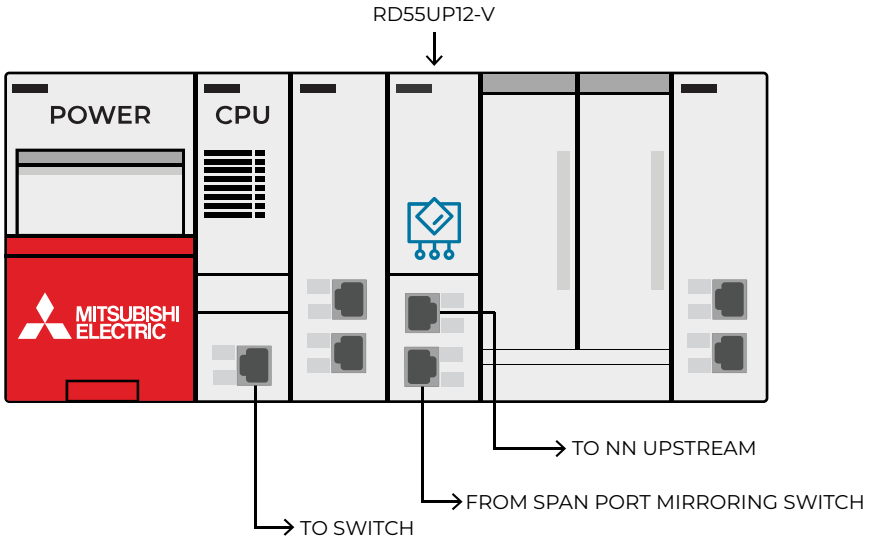


Figure 18. Mitsubishi Electric MELSEC iQ-R PLC

Hardware setup for Schneider Electric SCADAPack 47xi RTU

The recommended physical setup for the Schneider Electric SCADAPack 47xi remote terminal unit (RTU).

The SCADAPack edge module has two network interfaces. Arc uses one of these to connect to the upstream sensor. It is recommended to use the second network interface to monitor and have it connected to a switch SPAN port to get all the data from the *RTU* module.

This setup works best when Smart Polling is enabled. The port used to connect to the upstream is then also used as a Smart Polling interface.

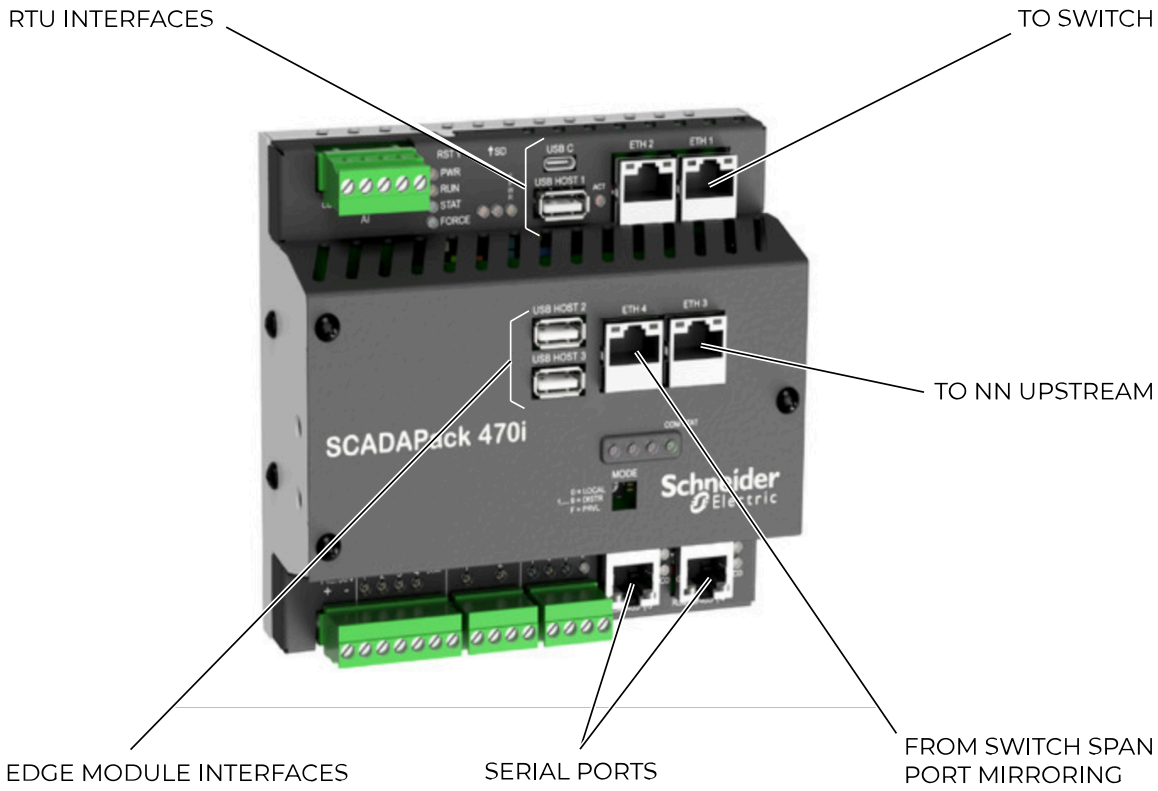


Figure 19. Schneider Electric SCADAPack 47xi RTU

Chapter 4. Configuration

Configure an Arc sensor in Guardian

*You can configure an individual Arc sensor in Guardian directly from the **Sensors** details page for the related sensor.*

To configure Arc in Guardian, see **Configure an Arc sensor** in the **Sensors** section of the **Guardian User Guide**.

Configure an Arc sensor in Vantage

*You can configure an individual Arc sensor in Vantage directly from the **Sensors** details page for the related sensor. Arc sensors in Service mode use these settings.*

To configure Arc in Vantage, see **Configure an Arc sensor** in the **Sensors** section of the **Vantage User Guide**.

Discovery and Smart Polling conditions

The minimum conditions required to run Discovery and Smart Polling on Arc depend on the Arc deployment mode.

Arc offline mode

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

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

Arc connected mode (Service and One-shot)

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

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

Shell commands

A list of available shell commands.

Table 4. Shell commands - Linux

Command	Function	Note
`./arc-linux-arm install`	Install Arc as an OS-service, ready to be started. On reboot Arc is automatically started.	1
`./arc-linux-arm start`	Start the Arc service.	
`./arc-linux-arm stop`	Stop the Arc service.	
`./arc-linux-arm restart`	Restart the Arc service.	
`./arc-linux-arm uninstall`	Uninstall Arc.	1
`./arc-linux-arm version`	Return the Arc version.	
`./arc-linux-arm status`	Return the Arc service status.	
`./arc-linux-arm install_dependencies`	Trigger the dependencies installation.	1

Chapter 5. Deployment

Automatically

Deploy Arc automatically from Guardian on Linux

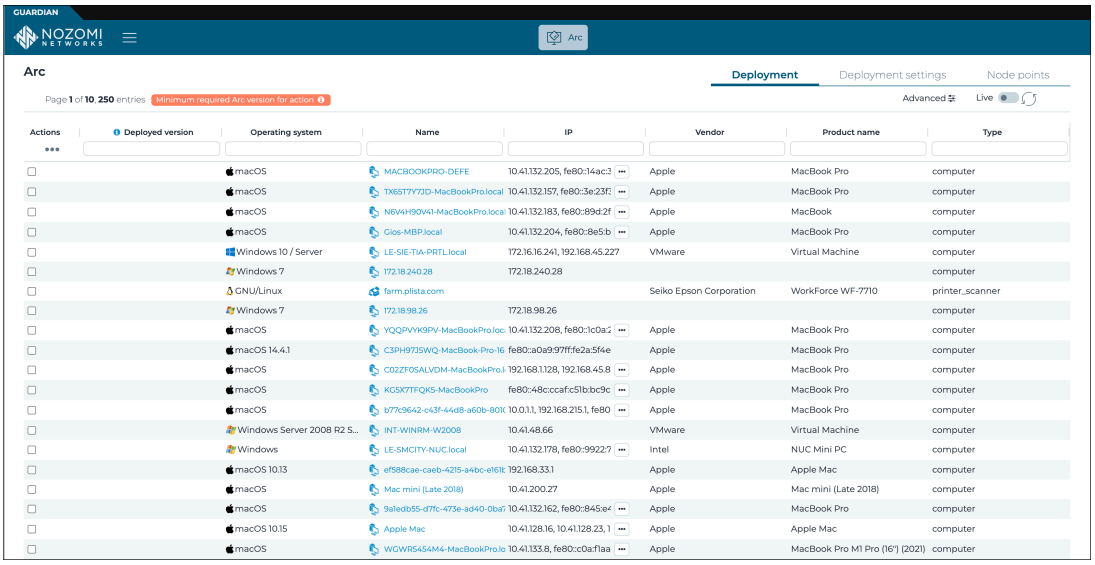
You can use Secure Shell (SSH) services to deploy Arc Embedded at scale for target machines that are reachable from Guardian.

Before you begin

- Credentials of the target machines are stored into the Credentials Manager
- *SSH* is enabled locally and accepting incoming connections from the Guardian machine(s) used for deployment
- Connectivity is granted for the service above, namely *TCP*/22
- If necessary, configure the deployment settings

Procedure

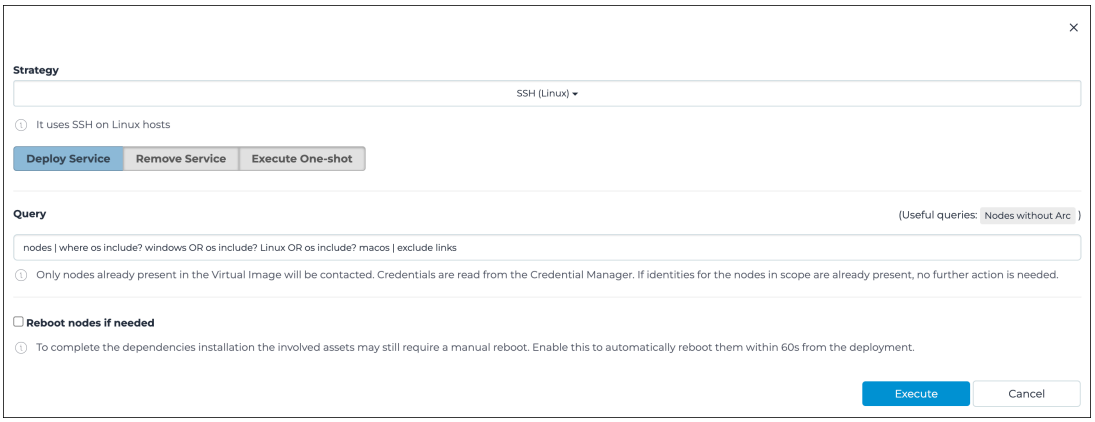
1. In the Web UI, go to **Arc > Deployment**.



Result: A list of machines that are suitable for Arc deployment shows.

2. Select **Advanced**.

3. From the **Strategy** dropdown, select **SSH (Linux)**.



4. Select **Deploy Service**.
5. In the **Query** field, define the machine range that you want to install to.
   For example: `nodes | where ip == 10.0.0.1 OR ip == 10.0.0.2`
6. Select **Execute**.

Deploy Arc manually

Download an Arc package

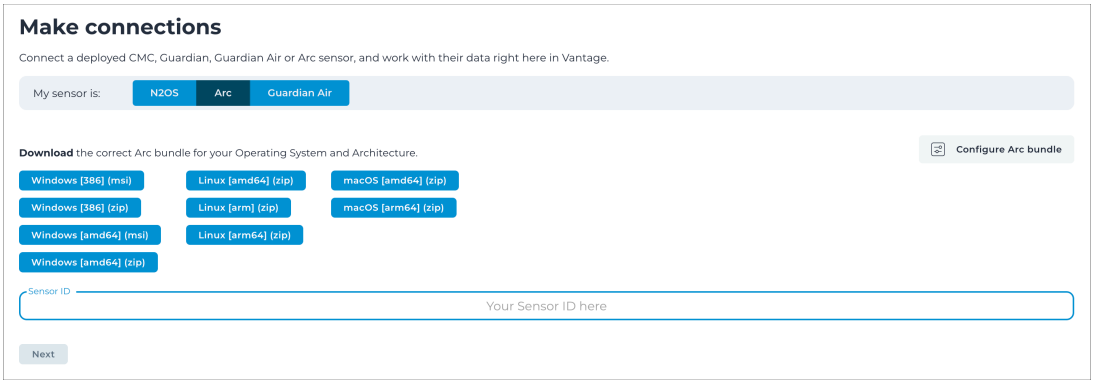
Download an Arc package from Vantage

Before you can deploy Arc manually, or through a mobile device management (MDM) system, you must download the correct package for your operating system (OS). You can do that from Vantage.

Procedure

1. In the navigation bar, go to **Sensors**.
2. In the top-right corner of the Web UI, click **Add new**.

   Result: The **Make connections** page opens.



3. In the **My sensor is:** section, click **Arc**.
4. Download the Arm 32 bits Linux package.

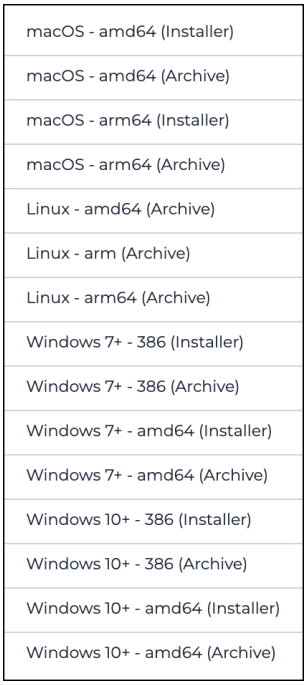
   Result: The package downloads to your computer.

Download an Arc package from Guardian

Before you can deploy Arc manually, or through a mobile device management (MDM) system, you must download the correct package for your operating system (OS). You can do that from Guardian.

Procedure

1. In Guardian, go to **Sensors > Download Arc**.



2. Download the Arm 32 bits Linux package.

   Result: The package downloads to your computer.

Download an Arc package from the Nozomi Networks support portal

Before you can deploy Arc manually, or through a mobile device management (MDM) system, you must download the correct package for your operating system (OS). You can do this from the Nozomi Networks support portal.

Procedure

1. Go to https://nozominetworks.my.site.com/support/s/article/Arc-Release-Package
2. Download the Arm 32 bits Linux package.

   Result: The package downloads to your computer.

Deploy Arc Embedded manually in Service mode without a local UI

You can manually deploy Arc Embedded to run in Service mode without a local user interface (UI).

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use *SSH* to log in to the target machine.
2. If the folder `/usr/local/sbin` does not exist, create it.

   Important:
   You can choose a different location, but make sure that only administrator accounts have write access. This is to prevent standard users from modifying the folder's contents.

3. Copy the Arc *ZIP* package into the folder `/usr/local/sbin/arc`
4. Extract the contents of the *ZIP* archive into the folder `/usr/local/sbin/arc`
5. To register Arc as a service (daemon), enter this command: `./arc-linux-arm install`

   Note:
   This example assumes that the Arc package you downloaded is `arc-linux-arm`

6. **Optional:** For Mitsubishi Electric MELSEC iQ-R only. If your Guardian doesn't have the **libmelco** package installed, then you can install it manually (on page 61).

   Note:
   If an upstream Guardian has the **libmelco** package, it will be automatically installed. However, if the upstream Guardian is air-gapped, you will need to manually install it.

7. To start Arc, enter the command: `./arc-linux-arm start`

Results

The Arc sensor is now running from `/usr/local/sbin/arc` and you can view collected data in Guardian or Vantage.

Manually install the libmelco package

Users of Mitsubishi Electric MELSEC iQ-R can use this procedure to manually install the **libmelco** *package when it cannot be downloaded from the update service.*

Before you begin

Download the Linux (for MELCO) Arm 32 bit package from Guardian.

About this task

If an upstream Guardian has the **libmelco** package, it will be automatically installed. However, if the upstream Guardian is air-gapped, you will need to manually install it.

Procedure

1. Unzip the **libmelco** package to `/usr/local/sbin/arc/`
2. Open a shell console.
3. Enter the command: `./arc-linux-arm install_libmelco`

   This command extracts `libmelco.so` from the encrypted `libmelco.bin` file to `/usr/local/lib` as if it had been downloaded from the update service.

   If Arc Embedded gets access to the update service after a manual installation, the **libmelco** package will be replaced with the most recent package available.

Results

The **libmelco** package is now installed.

What to do next

Continue the Deploy Arc Embedded manually in Service mode without a local UI (on page 60) procedure.

Chapter 6. Execution

Execution modes

Arc has three different execution modes: Service, One-shot, and Offline. It is important to understand the different modes, and how they can be used.

You can either set the execution modes manually, through the local *UI*, or they will be set when you deploy Arc from Guardian.

Service mode

This is the standard mode, where Arc monitors and reports data back to Guardian or Vantage. In this mode, Arc is installed as a service/daemon, and runs automatically when a machine is booted.

This mode is recommended for:

- Continuous monitoring
- Users who can host Arc for a longer time than with the two modes below
- Networks where Arc can be granted connectivity to Guardian or Vantage

Arc sensors periodically synchronize data to Guardian or Vantage. The frequency of transmitted data that can be received will vary, depending on the type and number of sensors. As more Arc sensors are connected, the communication interval is increased to protect Guardian or Vantage. In particular, because the default notification period is every 1 [minute], it holds as long as the number of Arc sensors is below the thresholds shown in the tables below.

For example, if more than 400 Arc sensors are connected to an NSG-HS sensor, the notification period will be increased to > 1 (minute). This is to make sure that the limit for this type of sensor, 400 (notifications per minute), is not exceeded.

Table 5. Elastic notification values - physical sensors

Sensor	Value (notifications per minute)
NSG-HS	400
NSG-H	300
NSG-M N750R1 N750R2 N1000R1 N1000R2	200
NSG-L NG-500R	60
P550 P500	30
NSG-R50 NSG-R150	6

Table 6. Elastic notification values - virtual sensors

Sensor (memory size in gigabytes)	Value (notifications per minute)
≥ 64	300

Table 6. Elastic notification values - virtual sensors (continued)

Sensor (memory size in gigabytes)	Value (notifications per minute)
≥ 48 — < 64	250
≥ 32 — < 48	200
≥ 24 — < 32	150
≥ 16 — < 24	100
≥ 12 — < 16	60
≥ 10 — < 12	30
< 10	6

Glossary

Address Resolution Protocol

ARP is a communication protocol that is used to discover the link layer address, such as a *MAC* address, that is associated with a given internet layer address. This is typically an IPv4 address.

Asset Intelligence™

Asset Intelligence is a continuously expanding database of modeling asset behavior used by N2OS to enrich asset information, and improve overall visibility, asset management, and security, independent of monitored network data.

Central Management Console

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

Central Processing Unit

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

Command-line interface

A command-line processor uses a command-line interface (CLI) as text input commands. It lets you invoke executables and provide information for the actions that you want them to do. It also lets you set parameters for the environment.

Comma-separated Value

A CSV file is a text file that uses a comma to separate values.

Common Event Format

CEF is a text-based log file format that is used for event logging and information sharing between different security devices and software applications.

Common Vulnerabilities and Exposures

CVEs give a reference method information-security vulnerabilities and exposures that are known to the public. The United States' National Cybersecurity FFRDC maintains the system.

cURL

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

dmidecode

dmidecode is a Linux command-line tool that retrieves detailed hardware information from the system's DMI/SMBIOS tables, including BIOS, processor, memory, and motherboard details, requiring root access.

Domain Name Server

The DNS is a distributed naming system for computers, services, and other resources on the Internet, or other types of Internet Protocol (IP) networks.

Hypertext Transfer Protocol

HTTP is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Identifier

A label that identifies the related item.

Industrial Control Systems

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

Internet of Things

The IoT describes devices that connect and exchange information through the internet or other communication devices.

Internet Protocol

An Internet Protocol address, or IP address, identifies a node in a computer network that uses the Internet Protocol to communicate. The IP label is numerical.

JavaScript Object Notation

JSON is an open standard file format for data interchange. It uses human-readable text to store and transmit data objects, which consist of attribute–value pairs and arrays.

Light-emitting Diode

An LED (Light Emitting Diode) is an electronic component that emits light when an electric current passes through it, offering energy-efficient, long-lasting illumination for displays, indicators, and lighting applications.

Media Access Control

A MAC address is a unique identifier for a network interface controller (NIC). It is used as a network address in network segment communications. A common use is in most IEEE 802 networking technologies, such as Bluetooth, Ethernet, and Wi-Fi. MAC addresses are most commonly assigned by device manufacturers and are also referred to as a hardware address, or physical address. A MAC address normally includes a manufacturer's organizationally unique identifier (OUI). It can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism.

Megabyte

The megabyte is a multiple of the unit byte for digital information. One megabyte is one million bytes.

Mobile Device Management

This is the administration of mobile devices, such as tablet computers, laptops, and smartphones. It is often implemented with a third-party product with features for specific vendors of mobile devices.

Nozomi Networks Operating System

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

Operating System

An operating system is computer system software that is used to manage computer hardware, software resources, and provide common services for computer programs.

Operational Technology

OT is the software and hardware that controls and/or monitors industrial assets, devices and processes.

Portable Document Format

PDF is a Adobe file format that is used to present documents. It is independent of operating systems (OS), application software, hardware.

Portable Executable

PE is a file format used by Windows operating systems (OS) for executable files, object code, and dynamic link libraries (DLLs). PE files contain the code and resources needed to run programs on Windows.

Programmable Logic Controller

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

Random-access Memory

Computer memory that can be read and changed in any order. It is typically used to store machine code or working data.

Remote Terminal Unit

An RTU is a microprocessor-controlled electronic device that acts as an interface between a SCADA (supervisory control and data acquisition) system, or distributed control system, to a physical object. It transmits telemetry data to a master system, and uses messages from the master supervisory system to control connected objects.

Secure Digital

A type of flash memory storage card used in devices like cameras, smartphones, and embedded systems.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Security Information and Event Management

SIEM is a field within the computer security industry, where software products and services combine security event management (SEM) and security information management (SIM). SIEMs provide real-time analysis of security alerts.

Structured Threat Information Expression

STIX™ is a language and serialization format for the exchange of cyber threat intelligence (CTI). STIX is free and open source.

Threat Intelligence™

Nozomi Networks **Threat Intelligence™** feature monitors ongoing OT and IoT threat and vulnerability intelligence to improve malware anomaly detection. This includes managing packet rules, YARA rules, STIX indicators, Sigma rules, and vulnerabilities. **Threat Intelligence™** allows new content to be added, edited, and deleted, and existing content to be enabled or disabled.

Transmission Control Protocol

One of the main protocols of the Internet protocol suite.

Transport Layer Security

TLS is a cryptographic protocol that provides communications security over a computer network. The protocol is widely used in applications such as: HTTPS, voice over IP, instant messaging, and email.

Uniform Resource Locator

An URL is a reference to a resource on the web that gives its location on a computer network and a mechanism to retrieving it.

Universally unique identifier

A UUID is a 128-bit label that is used for information in computer systems. When a UUID is generated with standard methods, they are, for all practical purposes, unique. Their uniqueness is not dependent on an authority, or a centralized registry. While it is not impossible for the UUID to be duplicated, the possibility is generally considered to be so small, as to be negligible. The term globally unique identifier (GUID) is also used in some, mostly Microsoft, systems.

Universal Serial Bus

Universal Serial Bus (USB) is a standard that sets specifications for protocols, connectors, and cables for communication and connection between computers and peripheral devices.

User Datagram Protocol

UDP is a lightweight, connectionless communication protocol used for fast, time-sensitive data transmission, such as video streaming, online gaming, and VoIP. UDP prioritizes speed and low latency over guaranteed delivery or error correction.

User Interface

An interface that lets humans interact with machines.

Windows Remote Management

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

Windows Server Update Services

WSUS is a Microsoft tool that enables centralized management and deployment of software updates and patches for Windows operating systems and other Microsoft products. It helps organizations enhance security by automating patch management, ensuring compliance, and reducing vulnerabilities.

ZIP

An archive file format that supports lossless data compression. The format can use a number of different compression algorithms, but DEFLATE is the most common one. A ZIP file can contain one or more compressed files or directories.