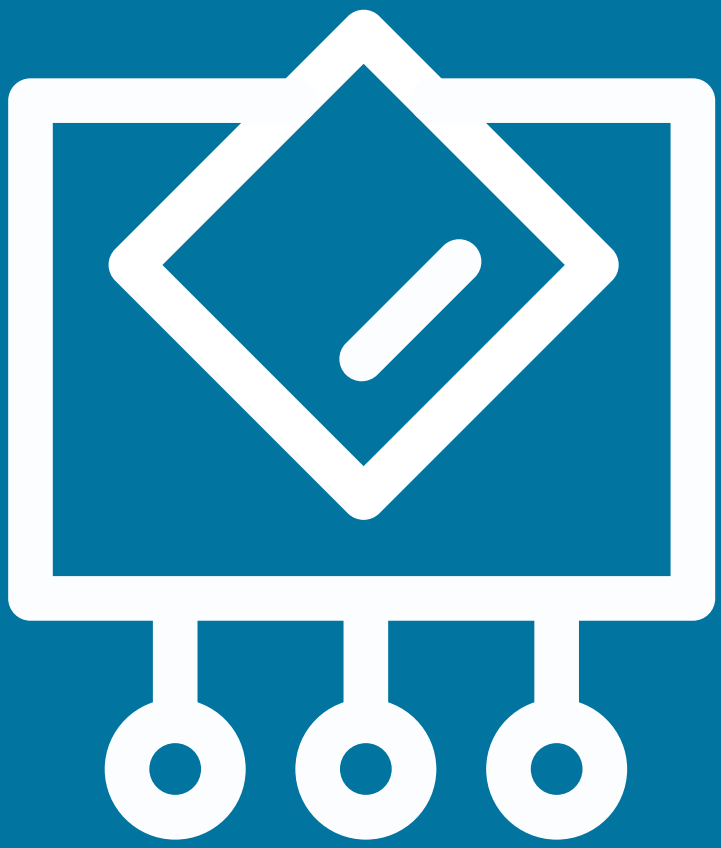
NOZOMI NETWORKS



Arc Embedded
Administrator Guide

Arc Embedded v1.14.0 — 2025-03-18

Legal notices

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

Copyright

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 programmable logic controllers (PLCs).

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

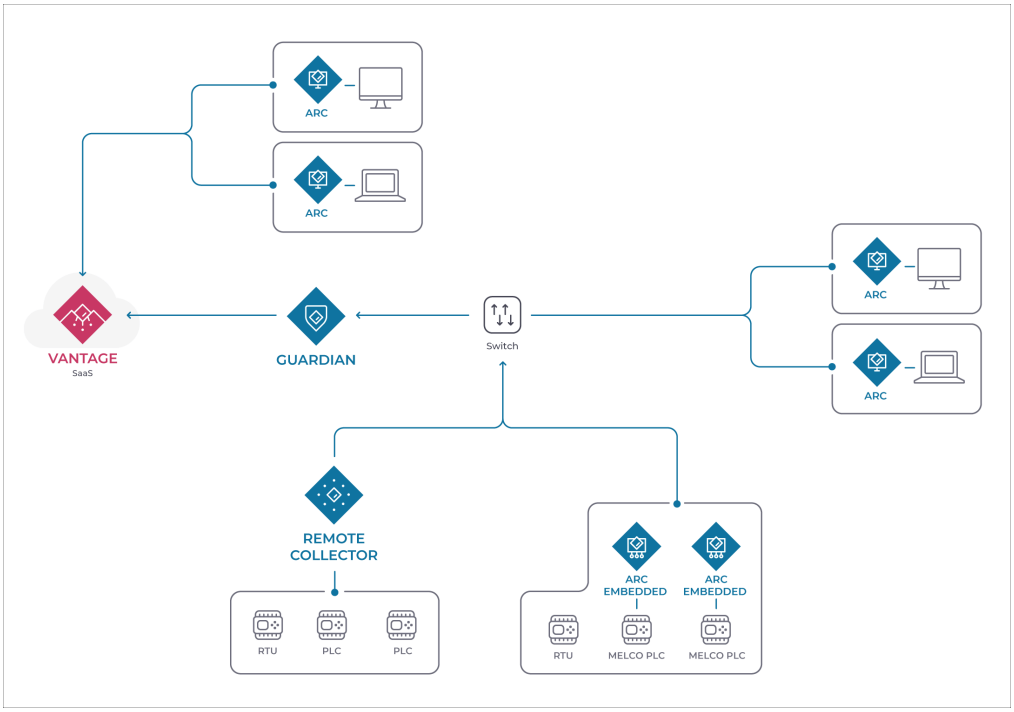


Figure 1. Arc architecture example

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

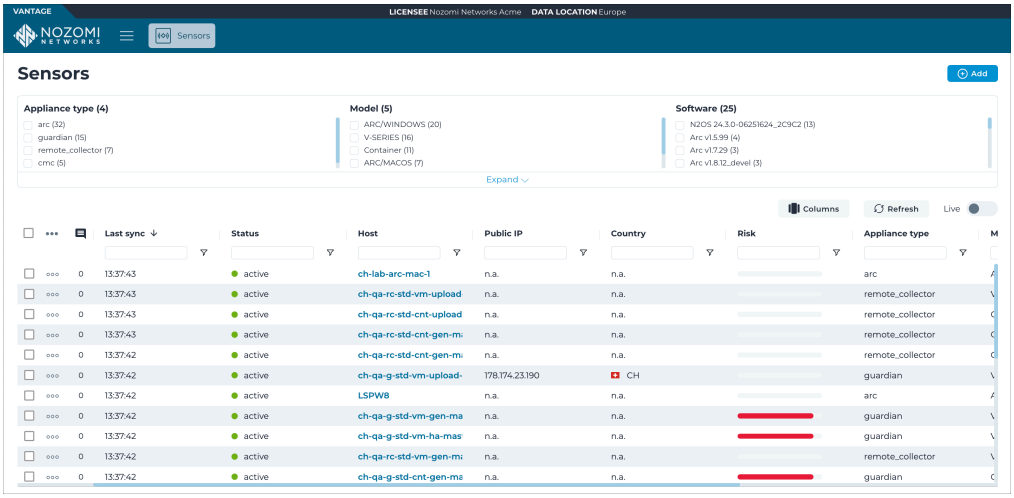


Figure 2. Vantage Sensors page

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

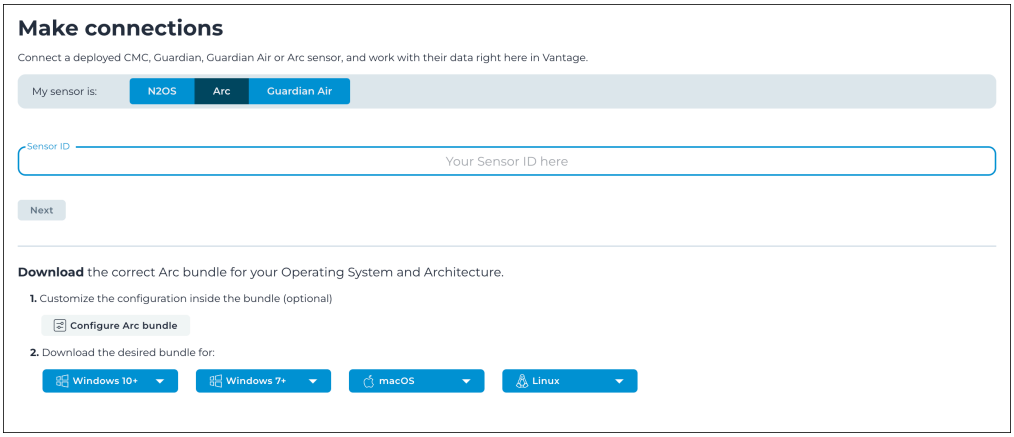


Figure 3. Make connections page

Configure an Arc sensor

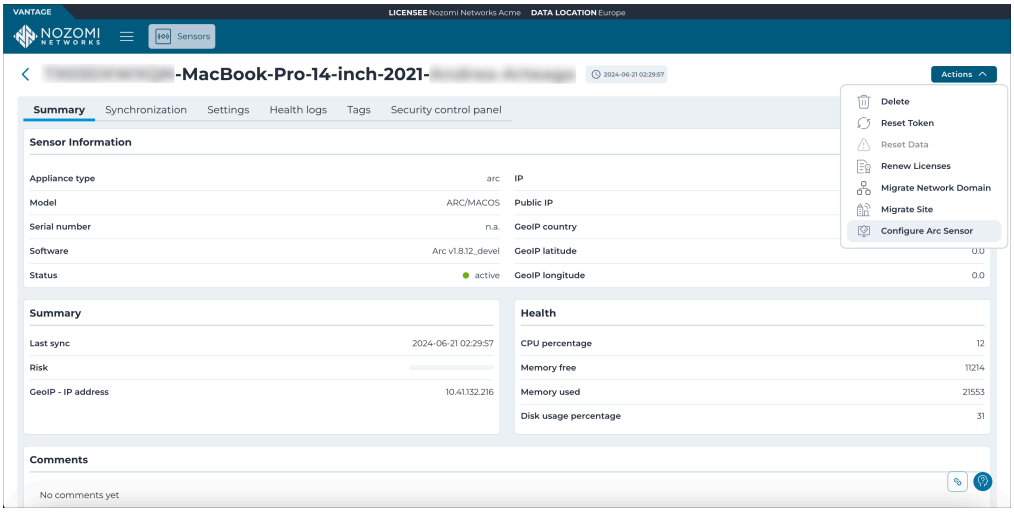


Figure 4. Actions menu in sensor details page

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

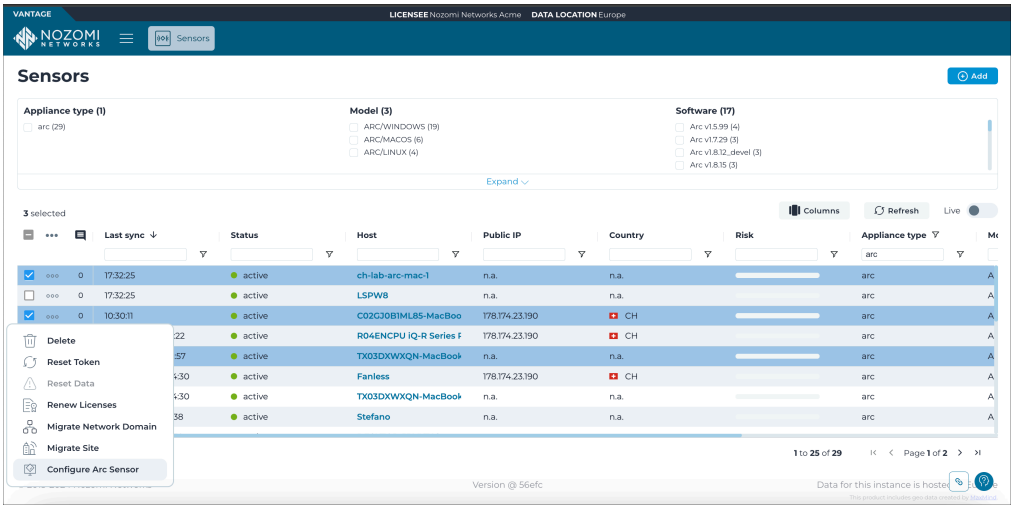


Figure 5. Configure multiple Arc sensors

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.*

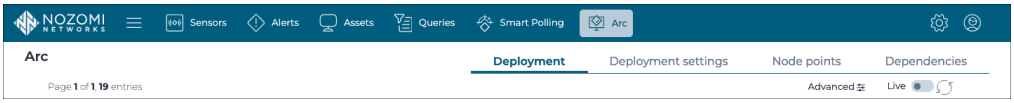


Figure 6. Arc button in Guardian Web UI

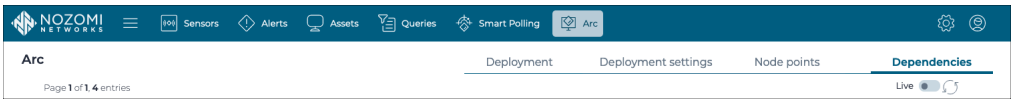


Figure 7. Arc button in Guardian Web UI (not connected to Vantage)

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

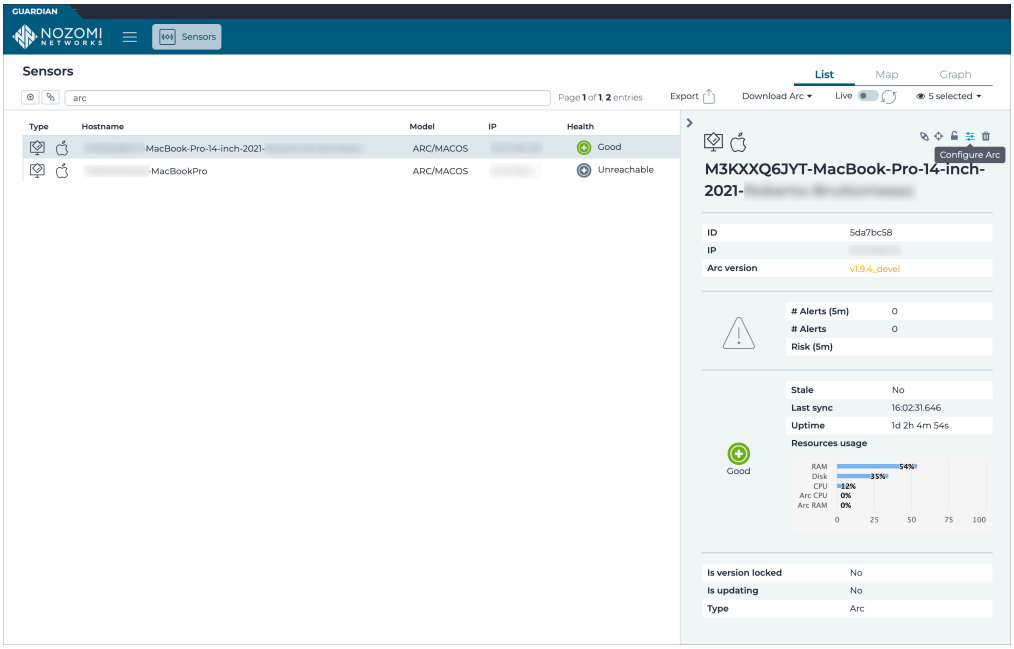


Figure 8. Configure an Arc sensor

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.

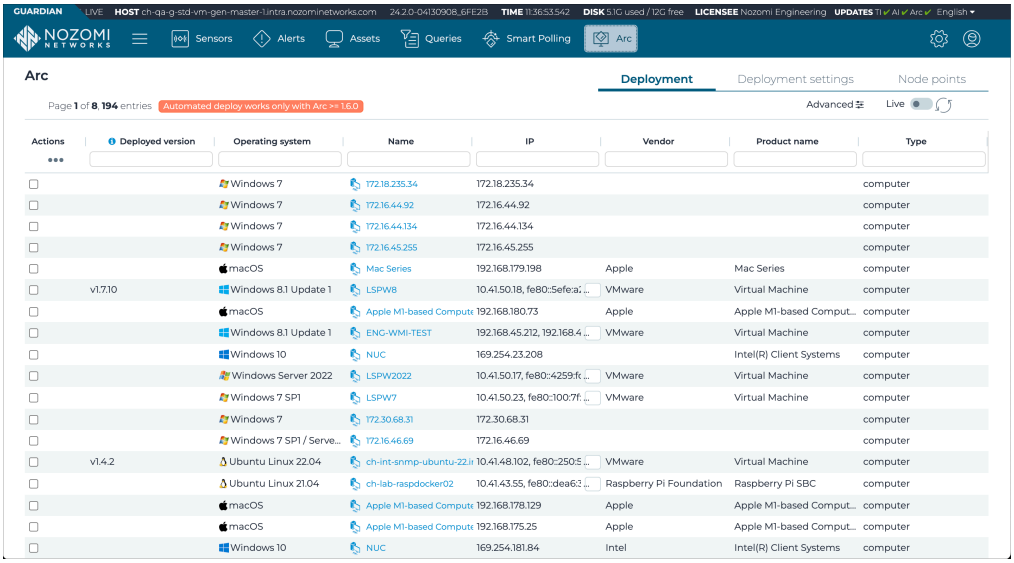


Figure 9. Deployment page

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.

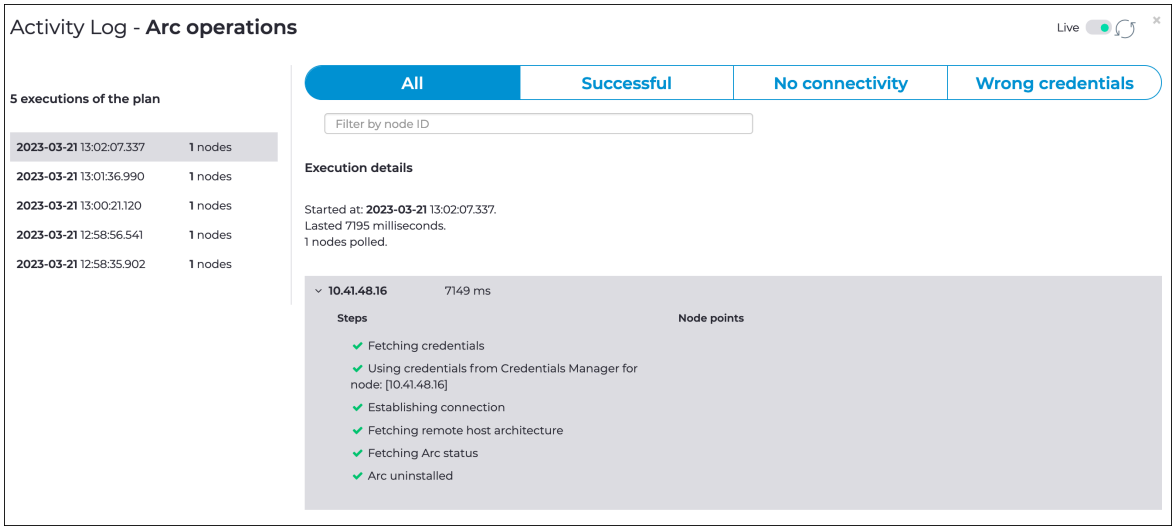
Execution details

*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

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

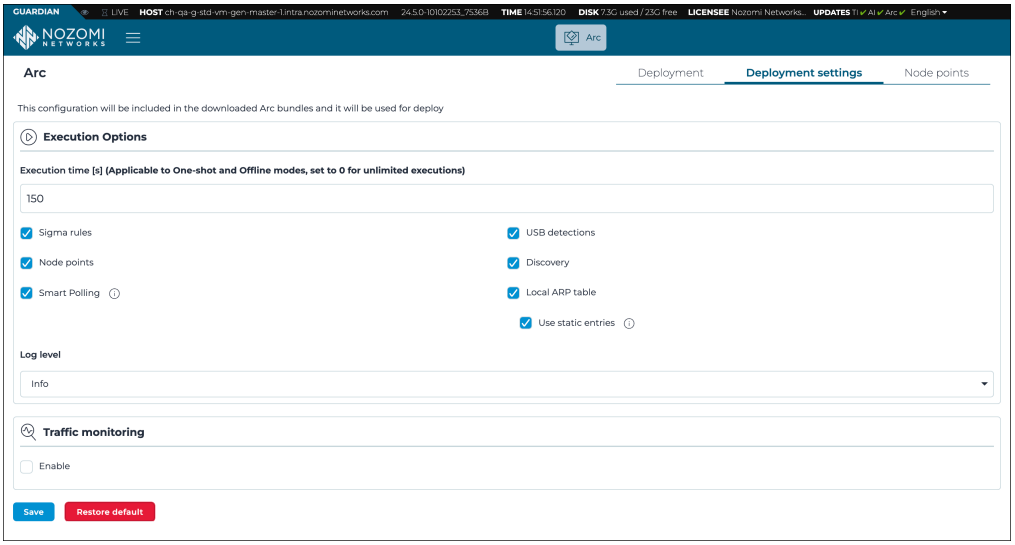


Figure 11. Deployment settings page

Execution Options

For more details, see Execution options (on page 17).

Traffic monitoring

For more details, see Traffic monitoring (on page 19).

Restore default

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

Execution options

*The **Execution options** page lets you configure how Arc collects data, manage detection features, and control network discovery and polling behaviors. You can also set logging levels and adjust specific execution parameters to optimize performance.*

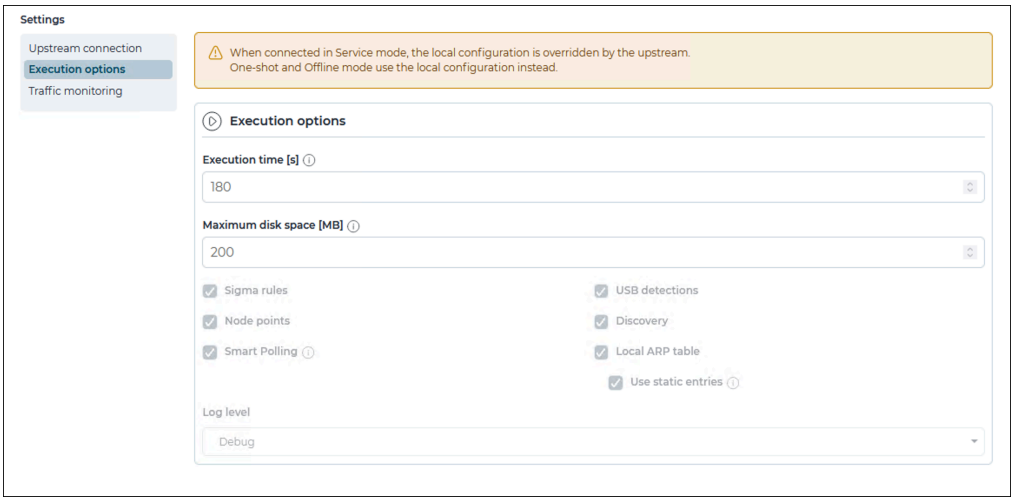


Figure 12. Execution options

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 that will be used for Offline mode.

Sigma rules (Windows only)

This lets you enable/disable Sigma rules.

USB detections (Windows only)

This lets you enable/disable *USB* detections.

Node points

This lets you enable/disable the production of node points.

Discovery

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

Discovery is a method of identification of actors in the network through the usage of lightweight protocol-specific broadcast messages. These messages cause the actors to reply with identity information. The process is repeated with interleaving, predefined intervals. On each repetition, the sensor will identify the suitable network interfaces and send broadcast messages through them to reach the subnetworks the sensor is connected to.

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.

Local ARP table

This lets you enable/disable the ability to use the local *address resolution protocol (ARP)* table to confirm addresses. The **Use static entries** checkbox lets you enable/disable the use of static entries in the *ARP* table. Static entries are user-defined. You should only use them if they can be trusted.

Log level

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

- Debug
- Info
- Error

Traffic monitoring

*The **Traffic monitoring** page lets you track network traffic using either intermittent or continuous modes. You can configure monitoring parameters, manage resource usage, and choose specific network interfaces to optimize performance.*

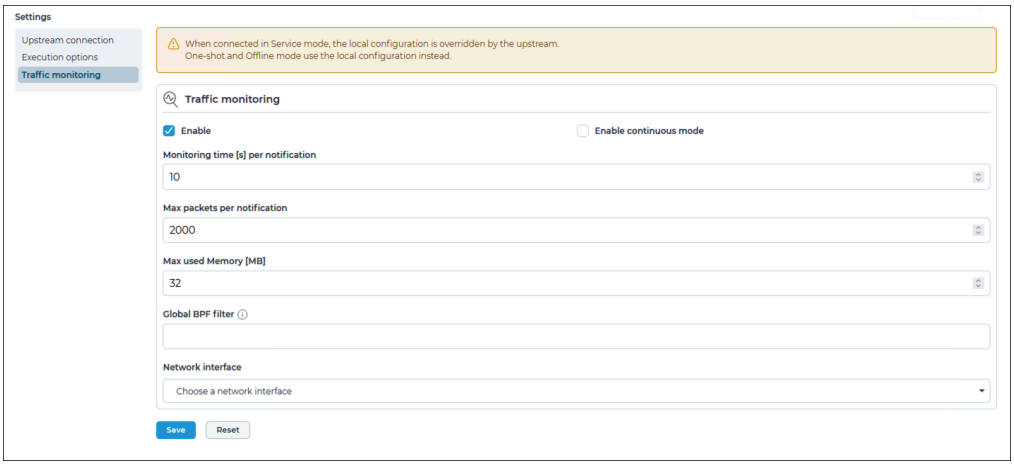


Figure 13. Traffic monitoring

Enable

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:

- **Monitoring 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

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:

- **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.

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 *identifier (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.*

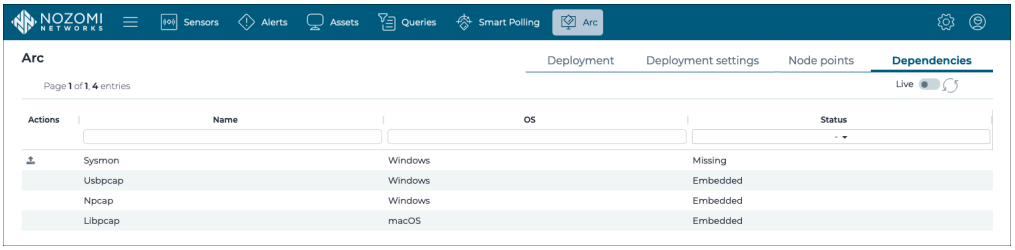


Figure 14. Dependencies page in Guardian (not connected to Vantage)

Arc in CMC

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

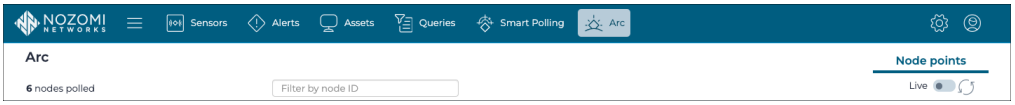


Figure 15. Arc button in CMC Web UI

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 23).

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 *transport layer security (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***:* **network** *and* **asset***. When the* **Category** *is listed as* **network***, it means that the detection is based on information that has been extracted from the network. When the* **Category** *is listed as* **asset***, it means that the detection is based on information that has been extracted from the asset.*

Detection information specific to Mitsubishi Electric

Category	Information	Supported by *	Configuration option
Asset	Nodes aggregation	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	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
Asset	Disconnection of Ethernet cable through: `SIGN:DEV-STATE-CHANGE`	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	Disconnection of module through: `SIGN:DEV-STATE-CHANGE`	RnP, RnPSF *CPU* models	Always on
Asset	Program transfer through: `SIGN:PROGRAM-TRANSFER`	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	Program change through: `SIGN:PROGRAM-CHANGE`	Rn *CPU* models	Always on
Asset	Firmware change through: `SIGN:FIRMWARE-CHANGE`	Rn, RnP, RnPSF *CPU* models	Always on
Asset	Remote login through: `SIGN:LOGIN`	RnSF, RnPSF *CPU* models	Always on

Category	Information	Supported by *	Configuration option
Asset	Attach of module through: `SIGN:DEV-STATE-CHANGE`	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	Insertion of SD card through: `SIGN:SD-CARD`	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	Removal of SD card through: `SIGN:SD-CARD`	Rn, RnP, RnSF, RnPSF *CPU* models	Always on
Asset	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
Asset	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
Asset	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).

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
network	Traffic monitoring	✓	Traffic monitoring
network	Smart Polling	✓	Smart Polling
asset	addresses	✓	always on
asset	*IP* addresses	✓	always on
asset	Product name	✓	always on
asset	Vendor	✓	always on
asset	Label/host name	✓	always on
asset	*OS*	✓	always on
asset	Serial number	✓	always on
asset	Local *ARP* table	✓	Local *ARP* table
asset	*USB* detections	✓	*USB* detections
asset	*CPU* usage	✓	node points
asset	Memory usage	✓	node points
asset	Disk usage	✓	node points
asset	Installed software	✓	node points
asset	Log4j detection	✓	node points
asset	Disk partitions	✓	node points

Category	Information	Linux	Configuration option
asset	*domain name server (DNS)*		node points

Chapter 2. Requirements

Operating System requirements

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

Operating System	Architecture	Version
Linux	arm	The correct Linux image needs to be installed. The default installed *OS* is VxWorks, which needs to be updated.

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.

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)*.

Software requirements

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

To use Arc Embedded, your other software must meet these minimum requirements:

- Vantage, or
- Guardian v23.1.0, or later

To deploy Arc Embedded automatically from Guardian, you need Guardian v24.4.0, 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

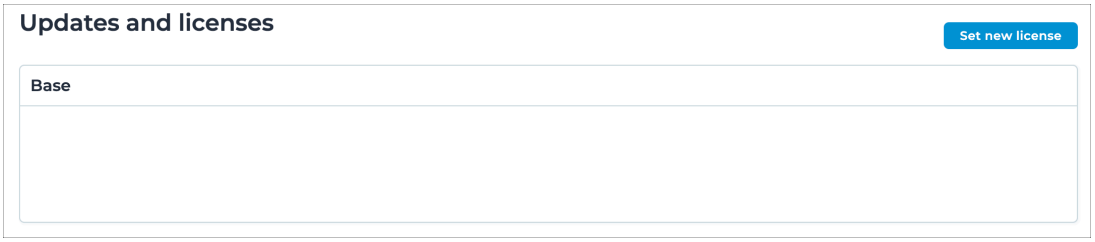
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

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

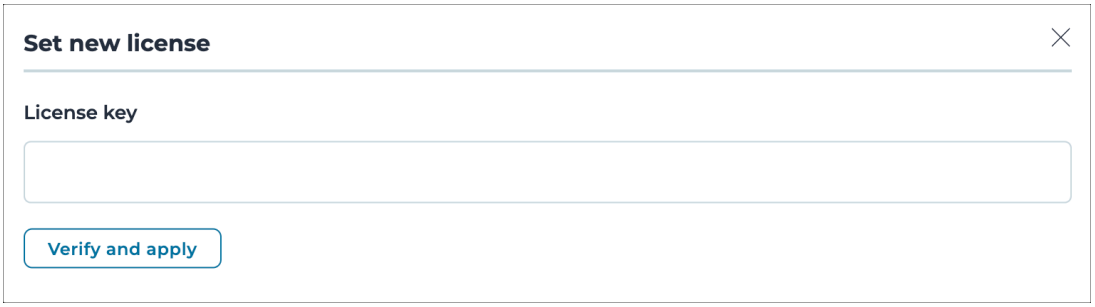
   Result: The **Updates and licenses** page opens.

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.

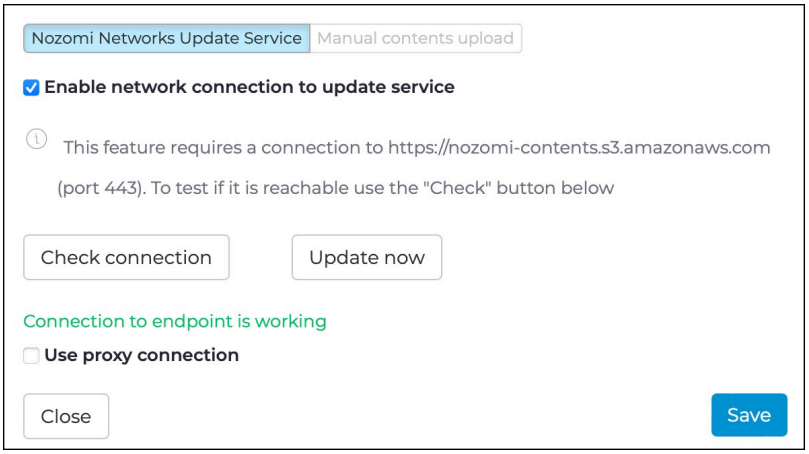
2. In the **System** section, select **Updates and licenses**.

   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.

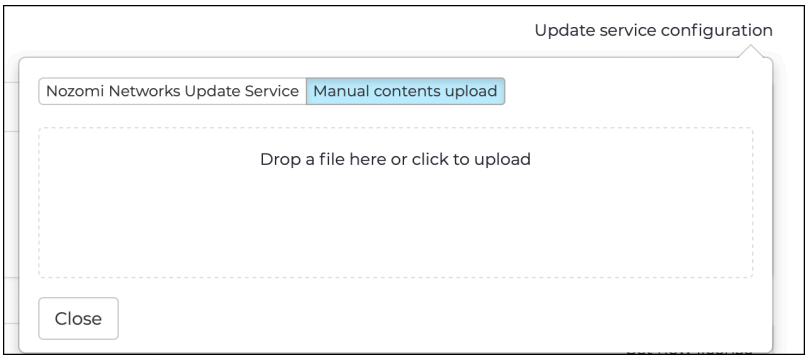
2. In the **System** section, select **Updates and licenses**.

   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 1. Linux dependencies

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 permissions

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

Linux

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

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

The recommended physical setup for the 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 Mitsubishi Electric MELSOFT strategy. The port used to connect to the upstream is also then used as a Smart Polling interface.

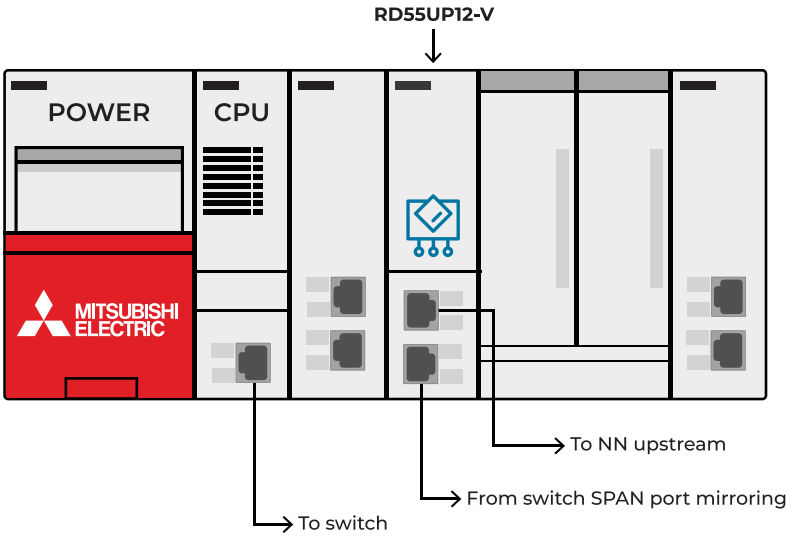


Figure 16. Mitsubishi Electric PLC

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.*

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

Shell commands

A list of available shell commands.

Table 2. 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

Note:
1 - Requires admin rights.

Chapter 5. Deployment

Automatically

Deploy Arc automatically from Guardian on Linux

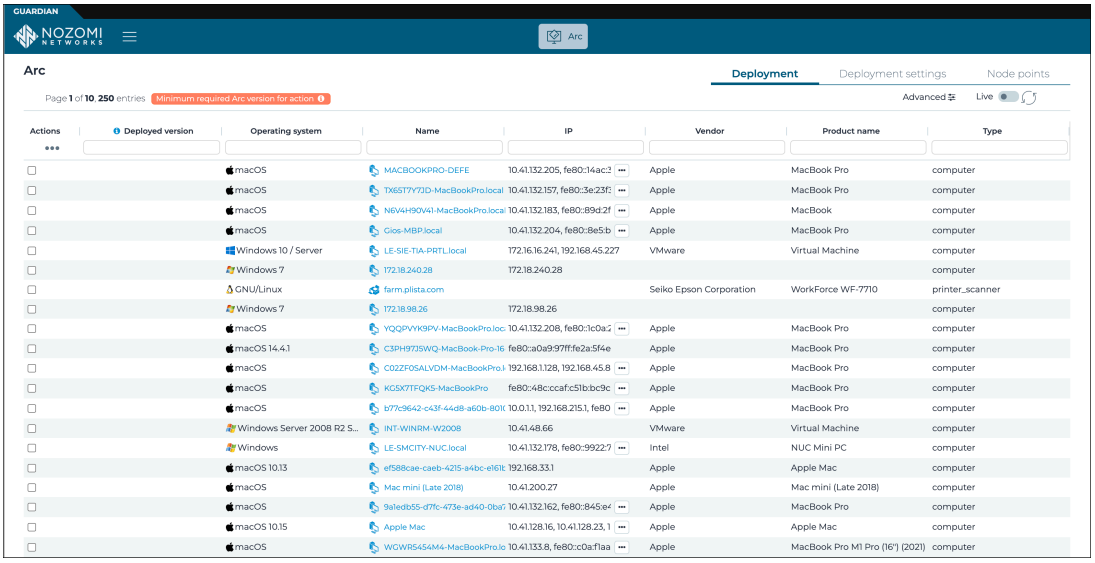
You can use Secure Shell (SSH) services to deploy Arc Embedded at scale for target machines that are reachable from Guardian.

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

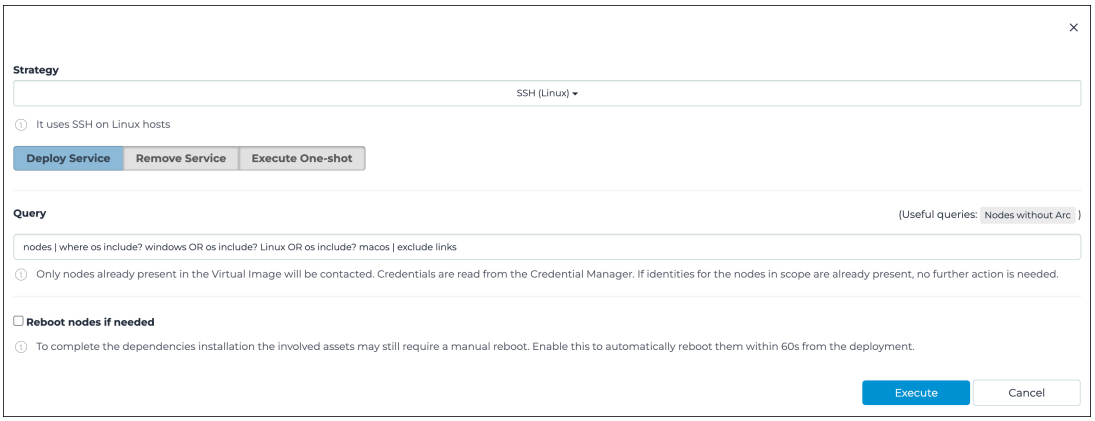
1. In the Web UI, go to **Arc > Deployment**.



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

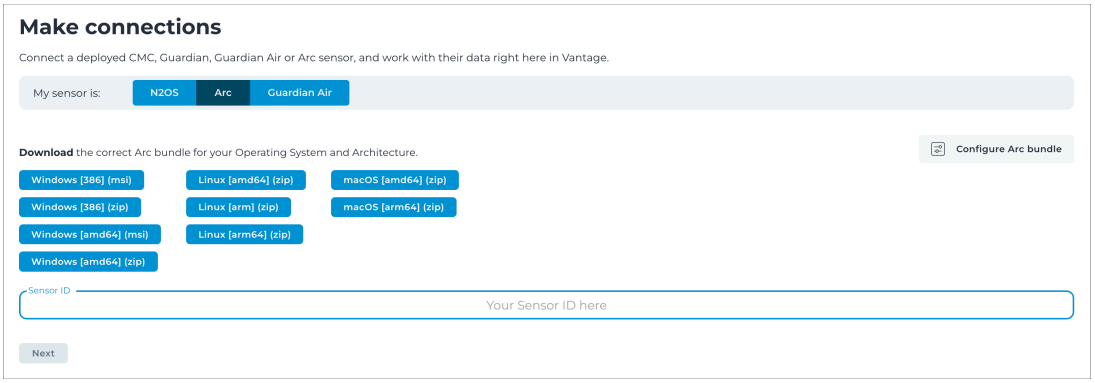
Download an Arc package from Vantage

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.

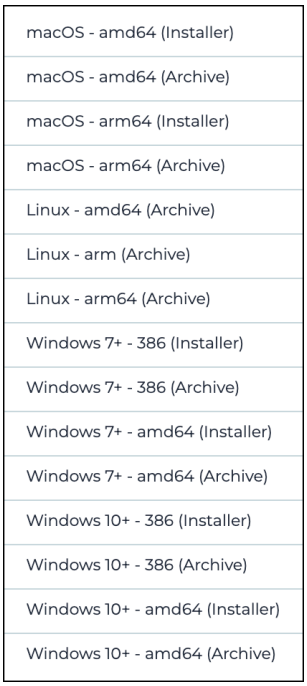
   Result: The package downloads to your computer.

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 manually in Service mode without a local UI

You can manually deploy Arc 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.

   Note:
   This location is not mandatory, but it will grant Arc superuser permissions when it needs them.

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. 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.

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 3. 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 4. Elastic notification values - virtual sensors

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

Table 4. 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 address, that is associated with a given internet layer address. This is typically an IPv4 address.

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 the similar method to 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.

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.

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.

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.

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.

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.

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.

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.

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 Interface

An interface that lets humans interact with machines.

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.