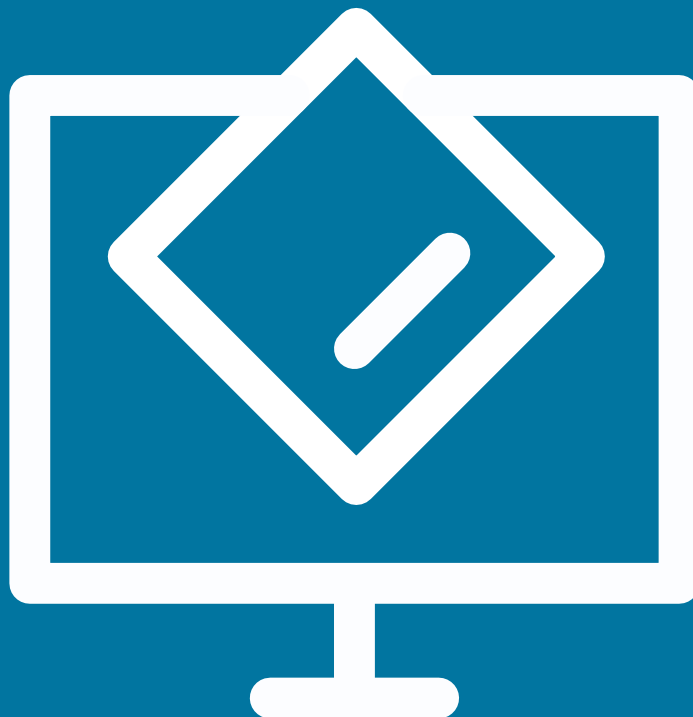




Arc

Administrator Guide

Legal notices

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

Copyright

Copyright © 2013-2026, Nozomi Networks. All rights reserved. Nozomi Networks believes the information it furnishes to be accurate and reliable. However, Nozomi Networks assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of Nozomi Networks except as specifically described by applicable user licenses. Nozomi Networks reserves the right to change specifications at any time without notice.

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at <https://security.nozominetworks.com/licenses>.

Contents

Chapter 1. Introduction.....	5
Arc overview.....	7
Architecture.....	9
Arc in Vantage.....	10
Arc in Guardian.....	12
Deployment.....	13
Deployment settings.....	17
Node points.....	26
Dependencies.....	27
Arc in CMC.....	27
Viewing data from Arc.....	28
Security measures.....	29
Detection information.....	30
Chapter 2. Requirements.....	33
Endpoint operating system requirements.....	35
Endpoint hardware requirements.....	35
Supported web browsers.....	36
Nozomi Networks software requirements.....	37
Federal Information Processing Standards (FIPS) on Linux.....	37
Federal Information Processing Standards (FIPS) on Microsoft Windows.....	38
Enable FIPS on Microsoft Windows.....	39
Chapter 3. Preparation.....	41
Arc licenses.....	43
Install a license in Guardian or CMC.....	44
Import Arc through the update service in Guardian or CMC.....	45
Import Arc through a manual contents upload in Guardian or CMC.....	46
Dependencies.....	47
Local services.....	55
User permissions.....	55
Connectivity.....	55
Enable Audit Policy on Microsoft Windows.....	56
Chapter 4. Configuration.....	57
Configure an Arc sensor in Guardian.....	59
Configure an Arc sensor in Vantage.....	59
Discovery and Smart Polling conditions.....	60
Local UI.....	61
Configuration.....	64
Status.....	74

Latest run.....	75
Asset inventory.....	76
Last 100 runs.....	77
This asset.....	78
Alerts.....	89
Compliance.....	91
Offline archives.....	106
Open the local UI.....	107
Compliance scanning.....	108
Shell commands.....	109
Chapter 5. Deployment.....	113
Automatically.....	116
Deploy Arc automatically from Guardian on Windows.....	116
Deploy Arc automatically from Guardian on Linux/macOS.....	118
Deploy Arc with MDM (Windows).....	119
Download an Arc package.....	119
Deploy Arc to run in Service mode.....	122
Deploy Arc manually.....	139
Download an Arc package.....	139
Deploy Arc to run in Service mode.....	142
Deploy Arc to run in One-shot or Offline mode.....	147
Chapter 6. Execution.....	155
Execution modes.....	157
Chapter 7. Troubleshooting.....	159
Sigma rule alerts do not show.....	161
Traffic monitoring does not work.....	163
USB detections do not work.....	164
Arc does not update to the latest version.....	165
Log files.....	166
Glossary.....	169

Chapter 1. Introduction



Arc overview

Arc™ is a host-based sensor that detects and defends against malicious or compromised endpoints, and insider attacks. You can use Arc sensors to aggregate data for analysis and reports, either on-premises, or in the Vantage cloud.

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

Operating Systems (OS)

Arc sensors are endpoint executables that run on hosts on these [operating system \(OS\)](#)s:

- Microsoft Windows
- Linux
- Apple macOS

The data that is collected can be sent to either Guardian or Vantage.

Use cases and deployment scenarios

Arc lets you:

- Incorporate air-gapped devices into the analysis and reporting system
- Gain deeper intelligence or insight on critical endpoint devices
- Continuously monitor and protect endpoints
- Automatically deploy sensors across thousands of devices
- Use a low-impact process to scan air-gapped networks
- Deploy with [mobile device management \(MDM\)](#) solutions

Continuous monitoring

Because the Arc sensor is on the host, it can monitor traffic continuously, even when the device is not sending or receiving traffic.

User-specific activity monitoring

With more access to endpoint data, Arc lets you connect network traffic and anomalies with specific users. This helps to identify potential insider threats and makes corrective actions both easier and quicker.

Local behavioral analysis (Sigma rules)

Sigma is a common open-source standard that lets you analyze log files to identify malicious events. They are not necessarily related to network artifacts, and as such, would not be detected without residing on a machine. Nozomi Networks Labs curates all the Sigma rules that are loaded into Arc. A [Threat Intelligence \(TI\)](#) active license is needed to receive curated rules from the upstream Nozomi Networks endpoint.

Temporary deployment

It is not necessary to keep the Arc executable on a host after you have collected information. This means that you can remove it after data has been collected to conserve host resources, and maintain a clean host environment.

Threat prevention

Starting with v2.0, Arc enforces actions to prevent threats in addition to monitoring.

Architecture

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

You can connect Arc:

- To Guardian
- To Vantage

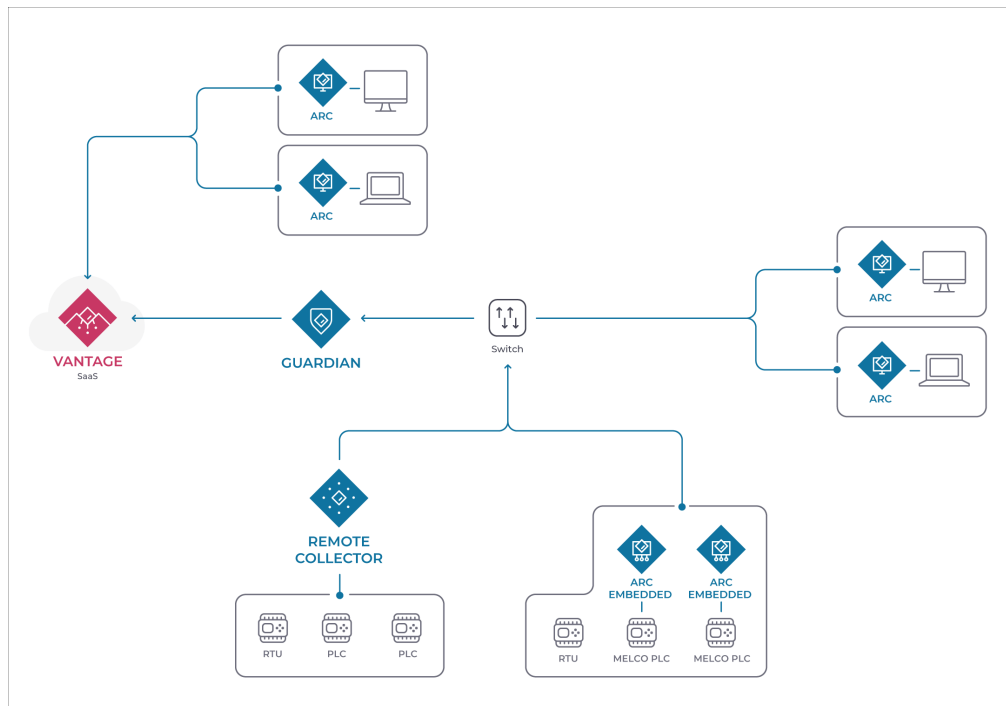


Figure 1. Arc architecture example

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

The screenshot shows the Vantage Sensors page. At the top, there are filters for Appliance type (4), Model (5), and Software (25). Below these filters is a table of sensors. The table has columns for Last sync, Status, Host, Public IP, Country, Risk, and Appliance type. The sensors listed include various models like ch-lab-arc-mac-1, ch-qa-rc-std-vm-upload, and ch-qa-g-std-vm-upload, with their respective public IPs and countries.

Appliance type (4)	Model (5)	Software (25)
arc (32)	ARC/WINDOWS (20)	NZOS 24.3.0-06251624_2C9C2 (13)
guardian (16)	V-SERIES (16)	Arc v1.5.99 (4)
remote_collector (7)	Container (1)	Arc v1.7.29 (3)
cmc (5)	ARC/MACOS (7)	Arc v1.8.12-devel (3)

Last sync	Status	Host	Public IP	Country	Risk	Appliance type
0 13:37:43	active	ch-lab-arc-mac-1	n.a.	n.a.		arc
0 13:37:43	active	ch-qa-rc-std-vm-upload	n.a.	n.a.		remote_collector
0 13:37:43	active	ch-qa-rc-std-cnt-upload	n.a.	n.a.		remote_collector
0 13:37:43	active	ch-qa-rc-std-cnt-gen-m	n.a.	n.a.		remote_collector
0 13:37:42	active	ch-qa-rc-std-cnt-gen-m	n.a.	n.a.		remote_collector
0 13:37:42	active	ch-qa-g-std-vm-upload	178.174.23.190	CH		guardian
0 13:37:42	active	LSPW8	n.a.	n.a.		arc
0 13:37:42	active	ch-qa-g-std-vm-gen-ma	n.a.	n.a.		guardian
0 13:37:42	active	ch-qa-g-std-vm-ha-mas	n.a.	n.a.		guardian
0 13:37:42	active	ch-qa-rc-std-vm-gen-mu	n.a.	n.a.		remote_collector
0 13:37:42	active	ch-qa-g-std-cnt-gen-mu	n.a.	n.a.		guardian

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

The screenshot shows the 'Make connections' page. It starts with a heading 'Make connections' and a subheading 'Connect a deployed CMC, Guardian, Guardian Air or Arc sensor, and work with their data right here in Vantage.' Below this, there are three buttons: 'My sensor is: NZOS', 'Arc', and 'Guardian Air'. The 'Arc' button is selected. Below these buttons is a text input field for 'Sensor ID' with a placeholder 'Your Sensor ID here'. Below the input field is a 'Next' button. Below the 'Next' button is a section titled 'Download the correct Arc bundle for your Operating System and Architecture.' with two steps: 1. 'Customize the configuration inside the bundle (optional)' with a 'Configure Arc bundle' button, and 2. 'Download the desired bundle for:' with four buttons: 'Windows 10+', 'Windows 7+', 'macOS', and 'Linux'.

Figure 3. Make connections page

Configure an Arc sensor

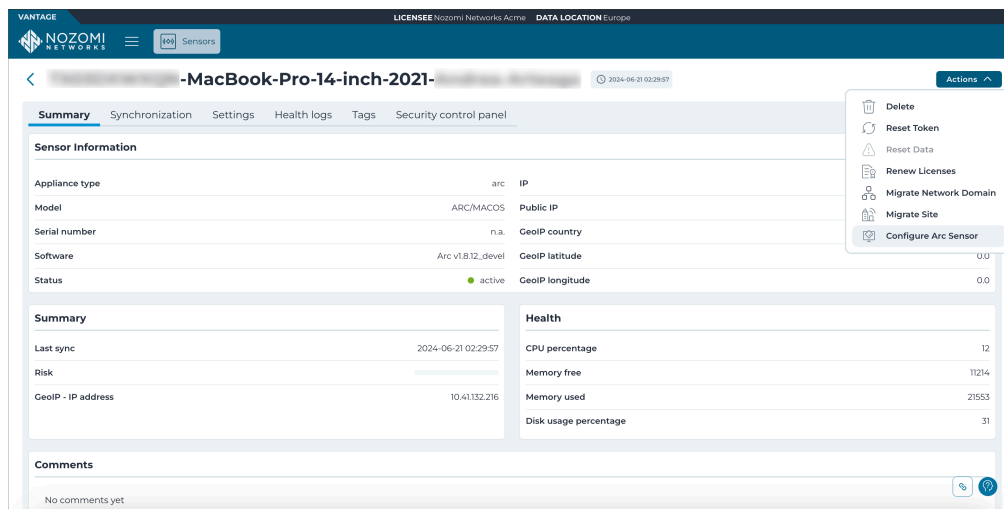


Figure 4. Actions menu in sensor details page

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

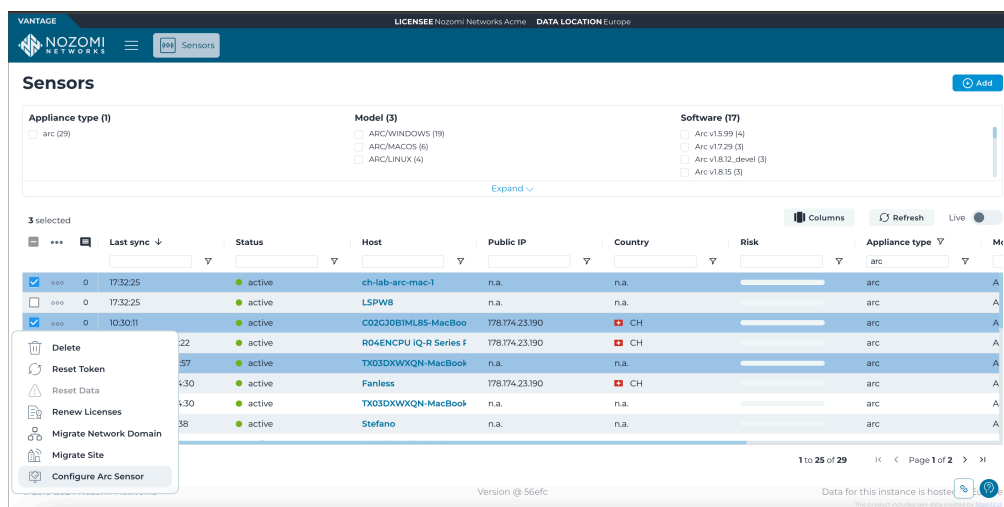


Figure 5. Configure multiple Arc sensors

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

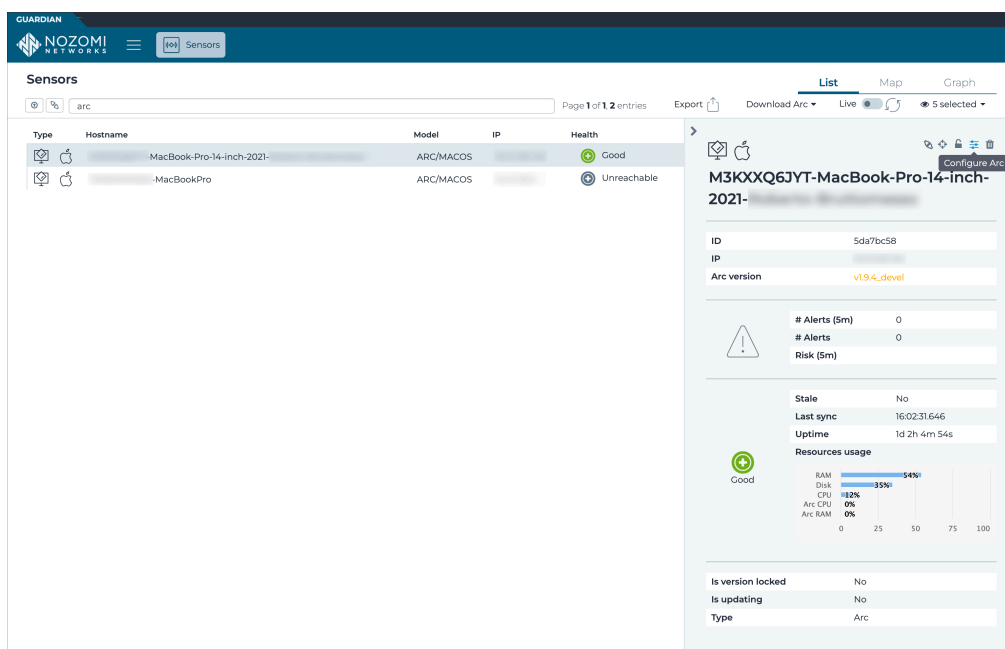


Figure 8. Configure an Arc sensor

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.

Actions	Deployed version	Operating system	Name	IP	Vendor	Product name	Type
☐		Windows 7	172.18.235.34	172.18.235.34			computer
☐		Windows 7	172.16.44.92	172.16.44.92			computer
☐		Windows 7	172.16.44.134	172.16.44.134			computer
☐		Windows 7	172.16.45.255	172.16.45.255			computer
☐		Mac OS	Mac Series	192.168.179.198	Apple	Mac Series	computer
☐	v1.7.10	Windows 8.1 Update 1	LSPW8	10.41.50.18, fe80::5efea...	VMware	Virtual Machine	computer
☐		Mac OS	Apple M1-based Comput	192.168.180.73	Apple	Apple M1-based Comput...	computer
☐		Windows 8.1 Update 1	ENG-WMI-TEST	192.168.45.212, 192.168.4...	VMware	Virtual Machine	computer
☐		Windows 10	NUC	169.254.23.208		Intel(R) Client Systems	computer
☐		Windows Server 2022	LSPW2022	10.41.50.17, fe80::4259fr...	VMware	Virtual Machine	computer
☐		Windows 7 SP1	LSPW7	10.41.50.23, fe80::1007f...	VMware	Virtual Machine	computer
☐		Windows 7		172.30.68.31			computer
☐		Windows 7 SP1 / Serve...		172.16.46.69			computer
☐	v1.4.2	Ubuntu Linux 22.04	ch-int-snmip-ubuntu-22.0	10.41.48.102, fe80::2505...	VMware	Virtual Machine	computer
☐		Ubuntu Linux 21.04	ch-lab-raspdocker02	10.41.43.55, fe80::dea63...	Raspberry Pi Foundation	Raspberry Pi SBC	computer
☐		Mac OS	Apple M1-based Comput	192.168.178.129	Apple	Apple M1-based Comput...	computer
☐		Mac OS	Apple M1-based Comput	192.168.175.25	Apple	Apple M1-based Comput...	computer
☐		Windows 10	NUC	169.254.181.84	Intel	Intel(R) Client Systems	computer

Figure 9. Deployment page

Advanced

The **Advanced** button lets you access the **Advanced** page. For more details, see [Advanced \(on page 15\)](#).

Execution details

The **Execution details** lets you access the **Activity Log**. For more details, see [Execution details \(on page 16\)](#).

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
- Execute One-shot: this executes a One-shot run for the selected devices, which are left clean after an execution. Arc self destroys after its execution

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.

WinRM: This selection will force the *Windows Remote Management (WinRM)* strategy, regardless of the OS, and deploy the correct Arc package for Windows.

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

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

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

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

Activity Log - Arc operations Live 

5 executions of the plan

Execution ID	Nodes
2023-03-21 13:02:07.337	1 nodes
2023-03-21 13:01:36.990	1 nodes
2023-03-21 13:00:21.120	1 nodes
2023-03-21 12:58:56.541	1 nodes
2023-03-21 12:58:35.902	1 nodes

Filter by node ID

Execution details

Started at: 2023-03-21 13:02:07.337.
Lasted 7195 milliseconds.
1 nodes polled.

10.41.48.16 7149 ms

Steps

- ✓ Fetching credentials
- ✓ Using credentials from Credentials Manager for node: [10.41.48.16]
- ✓ Establishing connection
- ✓ Fetching remote host architecture
- ✓ Fetching Arc status
- ✓ Arc uninstalled

Node points

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.

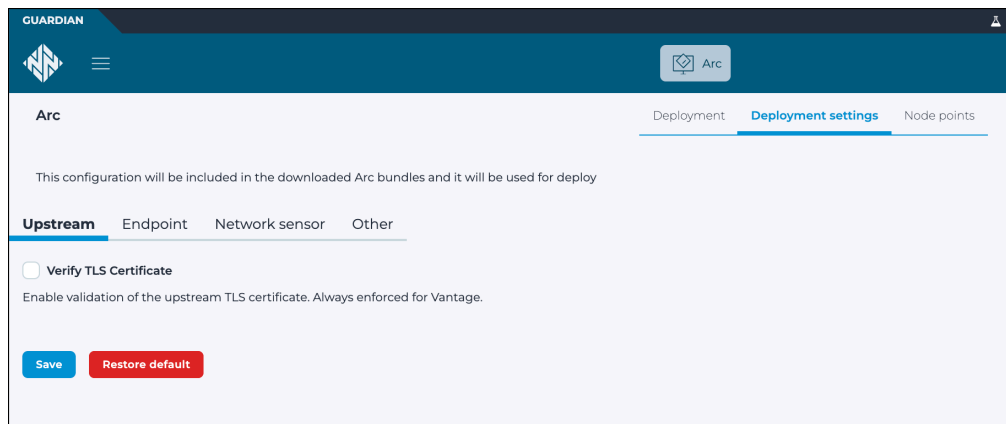


Figure 11. Deployment settings page

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

- [Upstream](#) (on page 18)
- [Endpoint](#) (on page 19)
- [Network sensor](#) (on page 21)
- [Other](#) (on page 24)

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.

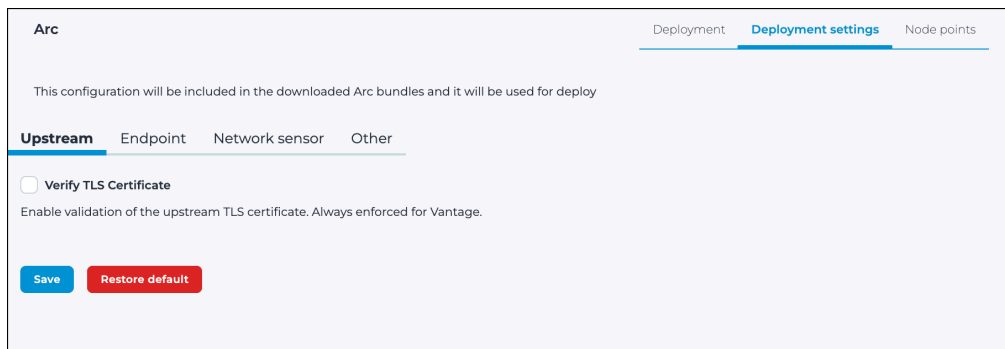


Figure 12. Upstream page

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.

Arc

Deployment **Deployment settings** Node points Dependencies

This configuration will be included in the downloaded Arc bundles and it will be used for deploy

Sensor mode

Full
All features are active. Network settings are available in the Network sensor tab.

Upstream **Endpoint** Network sensor Other

Select which information to detect:

- ☒ **Asset information**
Extract detailed asset information that can be plotted over time.
- ☐ CPU usage
- ☐ RAM usage
- ☐ Disk usage
- ☐ Logged-in users
- ☐ Processes with network activity
- ☐ Hotfixes
- ☒ User accounts
- ☒ DNS
- ☒ Installed softwares
- ☒ Unusual behaviors
Use Sigma indicators to monitor local events for signs of suspicious activity.
- ☒ Valid assets (using ARP)
Use the local address resolution protocol (ARP) table to confirm media access control (MAC) addresses.
 - ☒ Use static entries
User-defined (disable in case these entries are not trusted).
- ☒ USB devices
Detect the use of USB devices and malicious HID.
- ☒ Malware
Use Yara and STIX indicators to detect malicious file patterns before they get transferred over the network.

Action to perform on malware detection [New](#)

Only alert

Directory exclusions [+](#)

[Save](#) [Restore default](#)

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.

Arc

Deployment **Deployment settings** Node points

This configuration will be included in the downloaded Arc bundles and it will be used for deploy

Upstream Endpoint **Network sensor** Other

Select how to monitor your network.

☒ **Discovery**
Leverage lightweight network announcements to discover neighboring devices.

☒ **Smart Polling** License required
Use surgical active queries to enrich asset data.

☒ **Traffic monitoring**
Monitor network traffic using either intermittent or continuous modes.

☐ **Enable continuous mode**

Time per notification
5 seconds

Max packets per notification
10 packets

Max used Memory
32 MB

Global BPF filter
Applied to all network interfaces where a local BPF filter is not set. Syntactically incorrect filters will cause Traffic monitoring to stop.
e.g. tcp dst port not 443

Save Restore default

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

Traffic summary

This checkbox lets you enable or disable traffic summary. This option is available when traffic monitoring is enabled, and is disabled by default.

When enabled, Arc extracts only metadata from traffic for which deep packet inspection is not effective, such as encrypted or multimedia traffic. This metadata is sent upstream instead of the full payloads.

Heavy multimedia traffic, such as high-quality video feeds from security cameras or video conference software, can create a substantial load. With traffic summary enabled, this traffic is summarized as metadata, which reduces the upstream bandwidth consumption considerably without any loss of data. On the upstream appliance, the result is the same, and the data is available as usual, in the form of assets, links, and other information.

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.

The screenshot shows the 'Arc' configuration interface. At the top, there are tabs for 'Deployment', 'Deployment settings' (which is active), and 'Node points'. Below the tabs, a message states: 'This configuration will be included in the downloaded Arc bundles and it will be used for deploy'. Underneath, there are sub-tabs: 'Upstream', 'Endpoint', 'Network sensor', and 'Other' (which is active). The 'Other' section contains the following settings:

- Log level:** A dropdown menu currently set to 'Info'. The text above it says: 'Select event logging and endpoint space use preferences. How much information would you like in your log files? Choose from minimal log information ('Error' will only log unexpected errors) to more comprehensive log files for debugging purposes ('Debug').'
- Execution time:** A text input field containing '150' followed by 'seconds'. The text above it says: 'Applicable to One-shot and Offline modes, set to 0 for unlimited executions.'
- Maximum disk space:** A text input field containing '300' followed by 'MB'. The text above it says: 'Applicable to Offline mode, minimum 5. Set to 0 for unlimited space. 1GB of free disk space is always preserved.'
- Offline archive naming strategy:** A dropdown menu with the text 'Choose a naming strategy'. The text above it says: 'Select the information to be included in the name of the archive file when running Offline mode. Example: arc_data_archive_MyComputer_192.168.1.10_1761552820.zip'

At the bottom of the form, there are two buttons: 'Save' (blue) and 'Restore default' (red).

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 OSs, 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 \(on page 166\)](#).

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

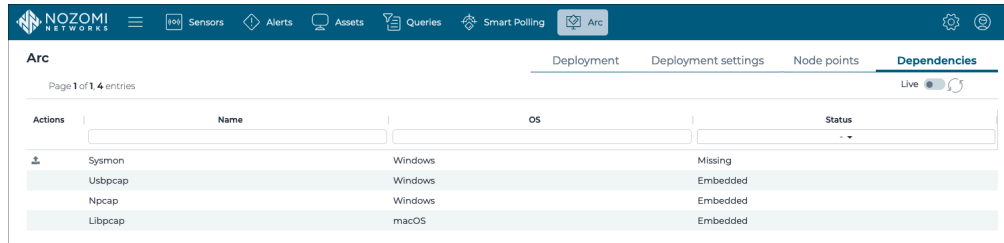
The  icon lets you immediately refresh the current view.

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.



Actions	Name	OS	Status
	Sysmon	Windows	Missing
	Usbpcap	Windows	Embedded
	Npcap	Windows	Embedded
	Libpcap	macOS	Embedded

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.

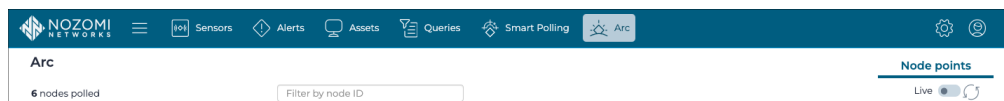


Figure 17. Arc button in CMC Web UI

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 \(on page 28\)](#).

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

Digital signature

Nozomi Networks signs all delivered executable files for Windows and macOS.

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 **License**: **sensor** and **endpoint**. When the **License** is listed as **sensor**, it means that the detection is based on information that has been extracted from the sensor. When the **License** is listed as **endpoint**, it means that the detection is based on information that has been extracted from the endpoint.

Table 1. Detection information

License	Information	Windows 	macOS 	Linux 	Configuration option
sensor	Discovery				Discovery
sensor	Smart Polling				Smart Polling
sensor	Traffic monitoring				Traffic monitoring
endpoint	Antivirus				node points
endpoint	<i>CPU</i>				node points
endpoint	<i>CPU</i> usage				node points
endpoint	Disk partitions				node points
endpoint	Disk usage				node points
endpoint	<i>DNS</i>				node points
endpoint	Hardware components				always on
endpoint	Hotfixes				node points
endpoint	Installed software				node points

Table 1. Detection information (continued)

License	Information	Windows 	macOS 	Linux 	Configuration option
endpoint	<i>IP</i> addresses				always on
endpoint	Label/host name				always on
endpoint	Local <i>ARP</i> table				Local <i>ARP</i> table
endpoint	Log4j detection				node points
endpoint	Logged in users				node points
endpoint	<i>MAC</i> addresses				always on
endpoint	Malware detection				malware
endpoint	Memory usage				node points
endpoint	Network interfaces				node points
endpoint	<i>OS</i>				always on
endpoint	Processes and ports				node points
endpoint	Product name				always on
endpoint	Serial number				always on
endpoint	Sigma rules				Sigma rules
endpoint	<i>USB</i> detections				<i>USB</i> detections
endpoint	<i>USB</i> interfaces				node points

Table 1. Detection information (continued)

License	Information	Windows 	macOS 	Linux 	Configuration option
endpoint	User accounts				node points
endpoint	Vendor				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.

Operating System	Architecture	Version
Windows	x86, x86_64	Windows 7 (Service Pack 1), or later
		Windows Server 2008 RC2 (Service Pack 1) or later
macOS	x86_64, arm64	macOS 10.10 Yosemite, or later
Linux	x86_64, arm, arm64	AlmaLinux OS 8, or later
		CentOS 7, or later
		Debian Jessie, or later
		Raspbian Jessie, or later
		RedHat Linux Enterprise 7.3, or later
		Suse Linux Enterprise Server 15, or later
		Ubuntu 16.04, or later

Endpoint hardware requirements

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

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 \(RAM\)](#).

Supported web browsers

The Nozomi Networks software supports recent versions of these browsers:

[Google Chrome](#)
[Chromium](#)
[Safari](#) (for macOS)
[Firefox](#)
[Microsoft Edge](#)
[Opera](#)

**Important:**

Microsoft Internet Explorer is not supported.

Nozomi Networks software requirements

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

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

- Vantage, or
- Guardian v25.2.0, or later

Federal Information Processing Standards (FIPS) on Linux

Arc for Linux FIPS is available as an additional bundle, and that has been tested on Debian 12 configured as FIPS. It may work out-of-the-box on other Linux distributions configured in FIPS mode.

Table 2. Software version requirements for FIPS-compliance

Software	Version
Linux	Debian 12, or higher

Federal Information Processing Standards (FIPS) on Microsoft Windows

For Arc to be deployed successfully on FIPS-enabled Windows machines, the versions of both Arc and Microsoft Windows must be correct. Only Windows 10 and higher are FIPS-compliant.

Microsoft Windows versions that are earlier than Windows 10 are not supported. It is the [OS](#) that provides the cryptographic functions that you need to use, and they need to be dynamically loaded from the [OS](#).

Earlier versions of Microsoft Windows have cryptographic functions that are now obsolete, and they are not [Federal Information Processing Standards \(FIPS\)](#)-compliant. It is possible to have an executable file with updated cryptographic functions, but it would not be [FIPS](#)-compliant.

Table 3. Software version requirements for FIPS-compliance

Software	Version
Arc	1.6.0, or higher
Windows	10, or higher

Further requirements

All software in the Nozomi Networks installation must be [FIPS](#)-compatible. Therefore, all these conditions must be met:

- The complete upstream chain of Nozomi machines (Vantage, [CMC](#), or Guardian) need to be [FIPS](#)-enabled
- An Arc [FIPS](#) executable needs to be installed on the endpoint



Note:

The correct [FIPS](#) executable files are made available once the previous condition is met.

- [FIPS](#) must be enabled on the endpoint before hosting Arc, for more details, see [Enable FIPS on Microsoft Windows \(on page 39\)](#)

Enable FIPS on Microsoft Windows

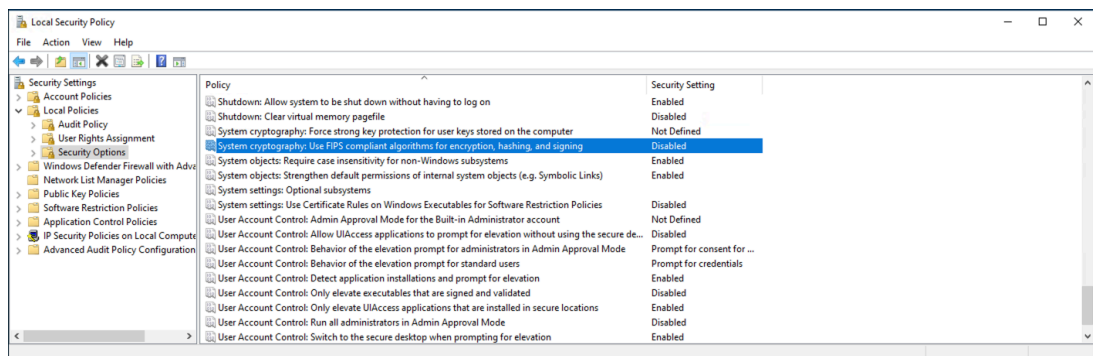
Before you can use Arc in FIPS-compliant mode, you must enable FIPS in the **Local Security Policy** of Microsoft Windows.

About this task

Arc **FIPS** works with Microsoft Windows 10, or higher.

Procedure

1. Right-click the Windows  icon.
2. Go to **Control Panel > Administrative Tools**
3. Double-click **Local Security Policy**
4. Select **Local Policies > Security Options**.



5. Set **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing** to **Enabled**.

Results

Microsoft Windows is now enabled for **FIPS**.



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.

License types

There are two types of Arc license:

- Endpoint
- Sensor

For more details, see [Detection information \(on page 30\)](#).

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](#).



UPDATES TI ✓ AI ✓ Arc ✓

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

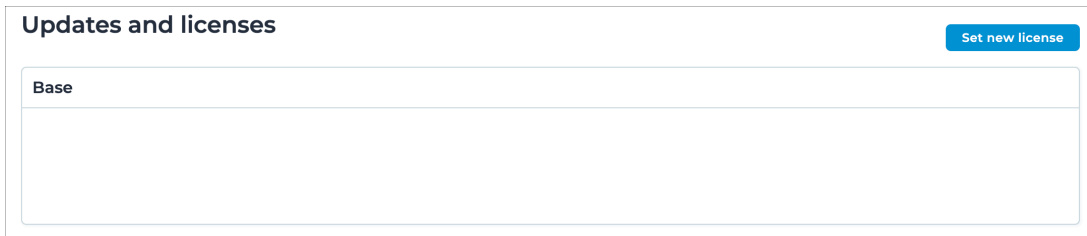
Before you can use Arc you must install the applicable license.

Before you begin

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

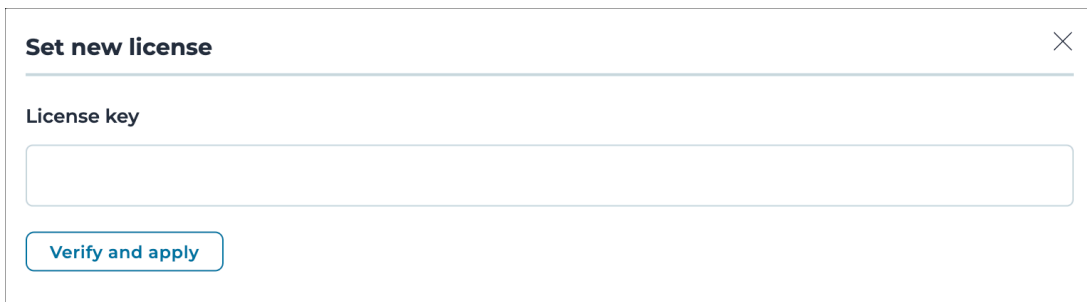
Procedure

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 are 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.

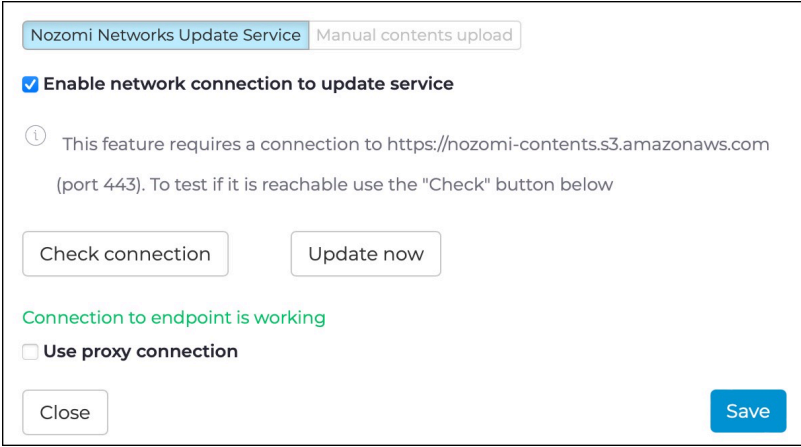
2. In the **System** section, select **Updates and licenses**.

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**.



Nozomi Networks Update Service Manual contents upload

☒ Enable network connection to update service

 This feature requires a connection to <https://nozomi-contents.s3.amazonaws.com> (port 443). To test if it is reachable use the "Check" button below

Check connection Update now

Connection to endpoint is working

☐ Use proxy connection

Close Save

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

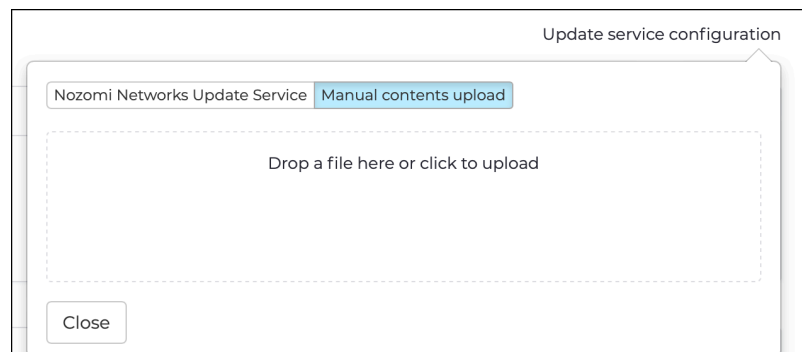
Before you can deploy Arc, you must import it first. There are two methods you can use to do this, one method is through a manual contents upload. The alternative method is through the Nozomi Networks Update Service.

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 4. Windows dependencies

Sigma rules	Sysmon
	PowerShell-script block-logging
	PowerShell Core-script block-logging
USB detections	USBPcap
Traffic monitoring	Npcap
Asset details	Not needed
Threat Prevention	EaseFilter (optional, for enhanced real-time performance)
Compliance scanning	SCAP Compliance Checker (SCC)

Table 5. Linux dependencies

Sigma rules	Not supported
USB detections	Not supported
Traffic monitoring	Not needed
Asset details	dmidecode
Compliance scanning	SCC

Table 6. macOS dependencies

Sigma rules	Not supported
USB detections	Not supported
Traffic monitoring	libpcap
Asset details	Not needed
Compliance scanning	SCC

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

[SCC](#) is never installed by default on any platform. On Windows it can be installed through the Arc setup when connected to Vantage. On Linux and macOS, [SCC](#) needs to be downloaded from the Arc dependencies page on Vantage and installed manually. Arc detects an existing installation automatically on any platform. For more information about Compliance scanning on Arc, see [Compliance scanning \(on page 108\)](#).

Windows

On Windows, you can use the command `install_dependencies` to automatically install these dependencies on the target machine:

- PowerShell-script block-logging
- PowerShell Core-script block-logging
- [USBPcap](#)
- [Npcap](#)
- [SCC](#)
- [EaseFilter](#)



Attention:

For security reasons, since Arc v1.17.0, [WinPcap](#) is no longer supported. For traffic monitoring, use [Npcap](#) instead.

Since Windows 11 24H2 (build 26100.8037) or Windows Server 2025 (build 26100), Windows includes [Sysmon](#) as a native component. Neither Arc nor Guardian can install it, and you cannot install it manually either.

Windows 7, 8, 10, and Windows 11 builds earlier than 26100.8037 do not include [Sysmon](#), so you must install it. For [Sysmon](#), the installation is semi-automatic. First, you must upload the latest [Sysmon](#) bundle to the applicable Guardian page. Guardian then uses the bundle for automatic installation during subsequent deployments.

If you are connected to Vantage, or to a Guardian with Vantage as upstream, Vantage automatically fetches [Sysmon](#) from the Microsoft website. You do not need to take any further action.



Note:

After you have installed [USBPcap](#), you must reboot the host machine to make the dependency active.



Note:

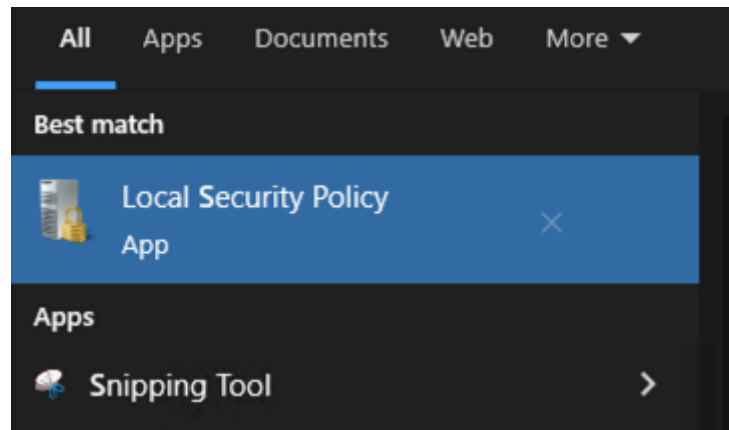
After a dependency is installed, you must restart Arc to make it active. When Guardian automatically installs dependencies during deployment, no user actions are necessary.

Enable security log events

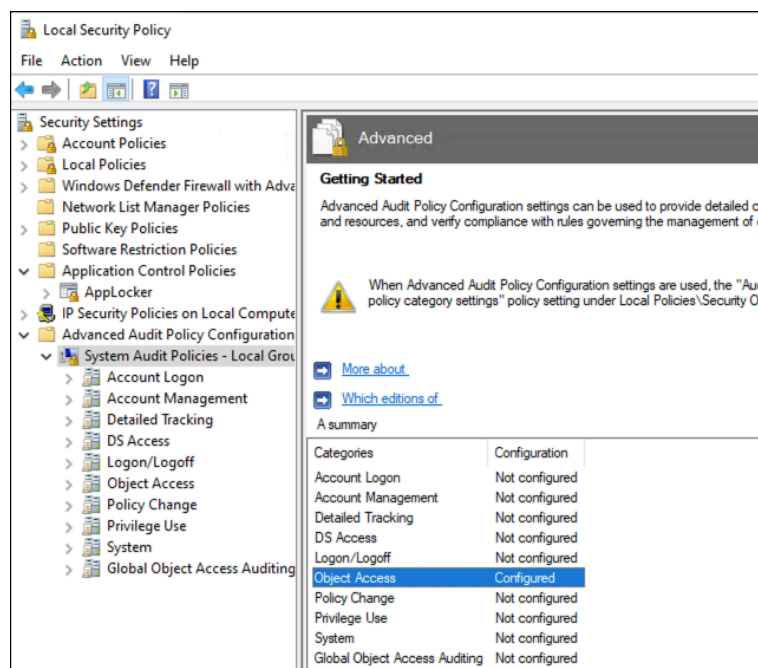
Before you can use Sigma rules related to security log events, you will need to enable them.

Procedure

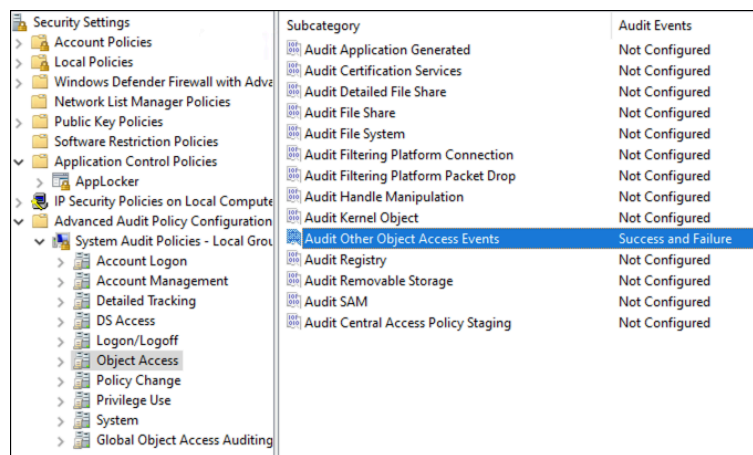
1. Open the Windows **Start** menu and search for the **Local Security Policy** application. Launch the application.



2. Select **Security Settings > System Audit Policies - Local Group**.

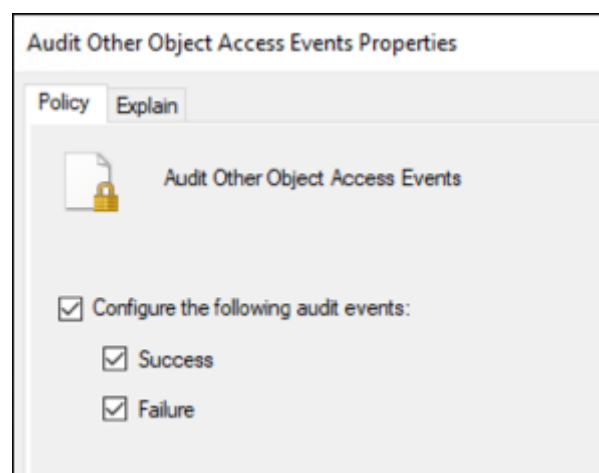


3. Select **Object Access > Audit Other Object Access Events**.



4. In the **Policy** tab, select these checkboxes:

- **Configure the following audit events**
- **Success**
- **Failure**



Results

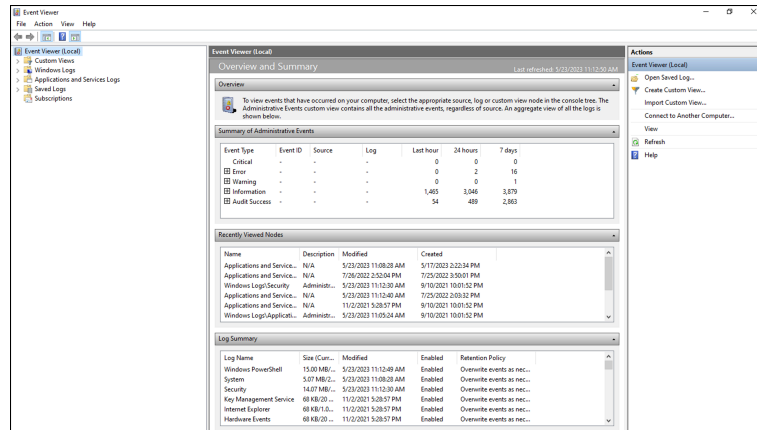
Security log events are now enabled in Windows.

Enable printservice log events

Before you can use Sigma rules related to printservice log events, you will need to enable them.

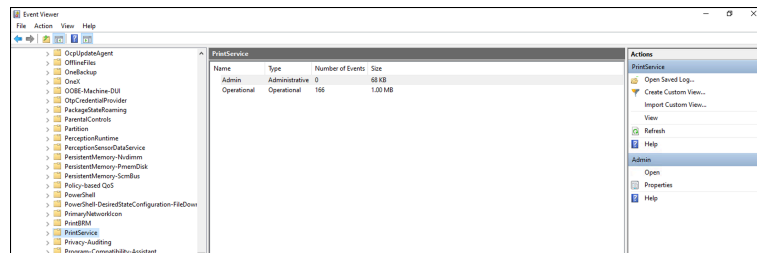
Procedure

1. Open the Windows **Start** menu and search for the **Event Viewer** application. Launch the application.



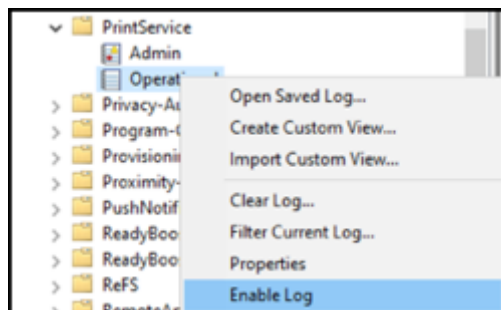
Result: The **Event Viewer** application opens.

2. Select **Windows > PrintService**.



Result: The **PrintService** page opens.

3. Right-click on **Operational** and select **Enable Log**.



Results

Printservice log events are now enabled in Windows.

Install EaseFilter manually

If your Arc installation was updated from an older version, EaseFilter may not have been installed automatically. You can install it manually using the Arc setup wizard.

About this task

[EaseFilter](#) is recommended for enhanced threat prevention performance. It is optional: threat prevention can still function if [Sysmon](#) is installed instead.

**Note:**

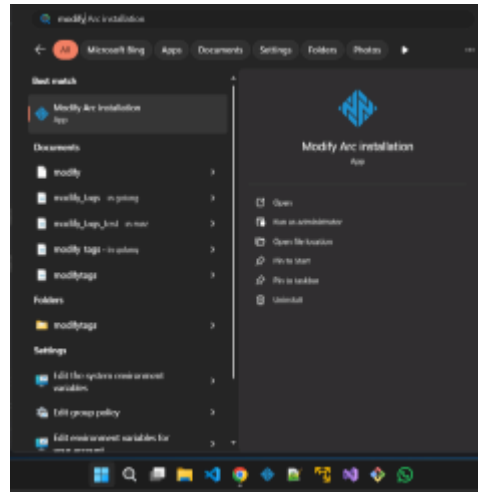
This procedure applies to Windows installations only.

Procedure

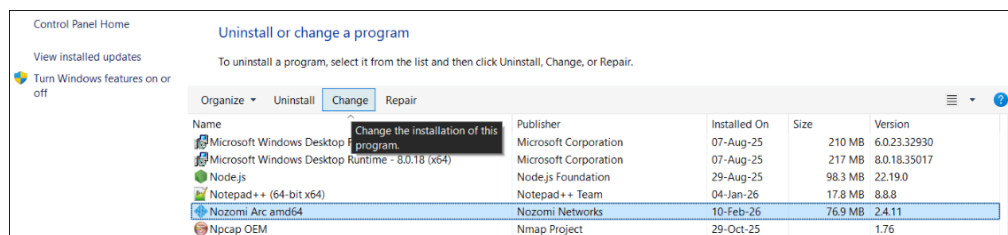
1. Open the Arc setup wizard using one of these methods:

Choose from:

- Open the Windows **Start** menu, search for **Modify Arc installation** and launch the result.



- Open **Control Panel > Programs and Features**, select **Nozomi Arc** from the list of installed programs, and select **Change**.



Result: The Arc setup wizard opens.

2. Select **Next**.
3. Select **EaseFilter** and complete the installation.

Results

EaseFilter is installed. Restart Arc to make the dependency active.

Local services

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

Windows

On Windows, you need to enable [WinRM](#) to deploy Arc automatically through Guardian.

Linux

On Linux, you need the [SSH](#) service to deploy Arc automatically through Guardian.

macOS

On macOS, 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) for Windows, Linux, and macOS
- [server message block \(SMB\)](#) ([TCP](#)/445) for Windows



Note:

[SMB](#) is required only for Guardian sensors running versions earlier than [Nozomi Networks Operating System \(N2OS\)](#) v25.1.0.

Enable Audit Policy on Microsoft Windows

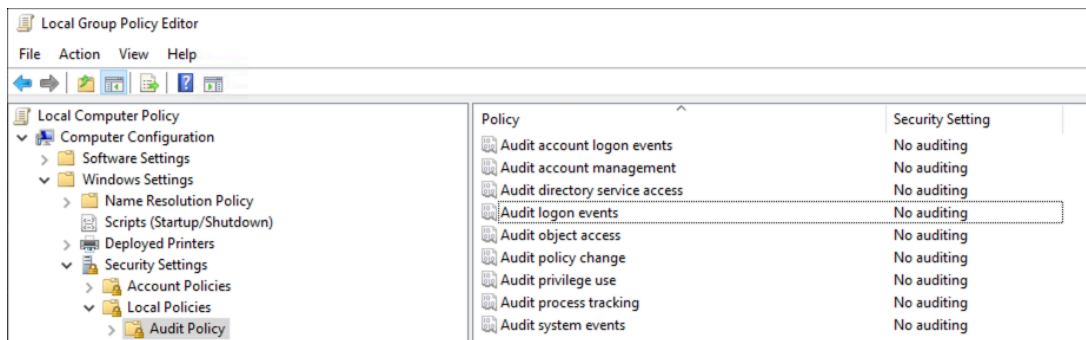
If you want Arc to detect user logon activities, you must enable **Audit logon events** of Microsoft Windows.

About this task

If you do not enable Audit Policy, Arc will not detect user logon activities.

Procedure

1. Right-click the Windows  icon.
2. Go to **Control Panel > Administrative Tools**
3. Double-click **Local Security Policy**
4. Select **Local Policies > Audit Policy**.



5. Set **Audit logon events** to **Enabled**.

Results

Arc will now detect user logon activities.

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

Local UI

The default method to manage Arc is through the upstream Nozomi Networks product, which applies configurations to all Arc sensors in Service mode. However, it is also possible to manage Arc through a local UI for One-shot and Offline executions.

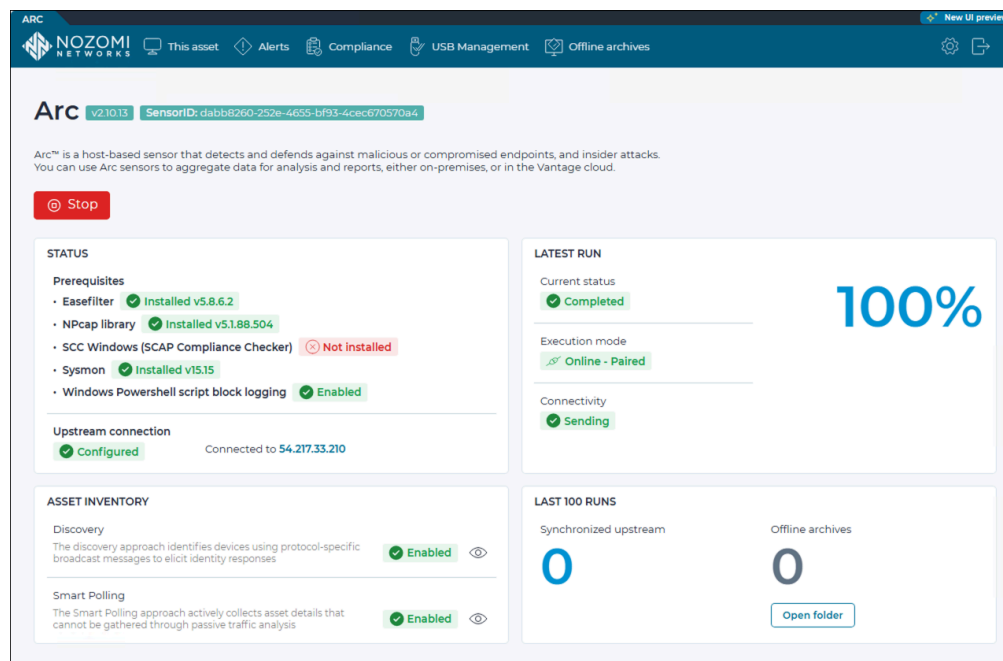


Figure 18. Local UI

The local [UI](#) has these sections:

Version: This shows the version of Arc that has been deployed.

Sensor ID: This shows the [ID](#) of the sensor.

Start button: This lets you choose and control a mode. You can choose between:

- Start (in Service mode)
- Start in One-shot mode
- Start in Offline mode

For more details, see [Execution modes \(on page 157\)](#).

- [Status \(on page 74\)](#)
- [Latest run \(on page 75\)](#)
- [Asset inventory \(on page 76\)](#)
- [Last 100 runs \(on page 77\)](#)
- [This asset \(on page 78\)](#)

To access the [Alerts \(on page 89\)](#) page, you can select the **Alerts** icon.

To access the [Offline archives \(on page 106\)](#) page, you can select the  **Archives** icon.

To access the [Configuration \(on page 64\)](#) page, you can select the  icon.

To log out, you can select the  icon.

The main method to manage Arc is through the system that it connects to. This can be:

- Guardian
- [CMC](#), or
- Vantage

Default settings are set for Arc the moment that it is deployed. However, you can access the local [UI](#), which is in the form of a web server, if you need to:

- Check the status of Arc locally
- Change the settings after Arc has been downloaded
- Run it locally during a manual deployment

To get access to the local [UI](#), you can:

- Double-click the executable file, or
- From a shell, invoke it from a terminal without a parameter, with a command like `.\arc-windows-amd64.exe`

**Note:**

On macOS, before you can open the local [UI](#), you might need to enable Arc in **System Preferences > Security & Privacy**.

When you do this, Arc will open a page in your default browser at the address `http://127.0.0.1:4510`

**Note:**

If the port 4510 is in use, the first open port above 4510 will be used.

**Note:**

To open the browser page automatically, you need to consider:

- That the browser will only open when a default browser is installed and configured
- That the double-click action will only work if the application is recognized as an executable. For Linux and macOS, this means that it needs to be associated to the Terminal (shell) application
- For Ubuntu distribution, you can only open the browser when the package `xdg-utils` is installed
- For Linux, the root user cannot open a browser, so you must not open the local [UI](#) as root
- If the browser does not open for one of the reasons listed above, you can open the browser and page manually

**Note:**

Closing the browser won't unlock the process. Make sure that you escape from your command line so that you can execute more operations on your executable.

Configuration

The **Configuration** page lets you define upstream connection settings, execution options, protection preferences, and traffic monitoring parameters for the Arc sensor.

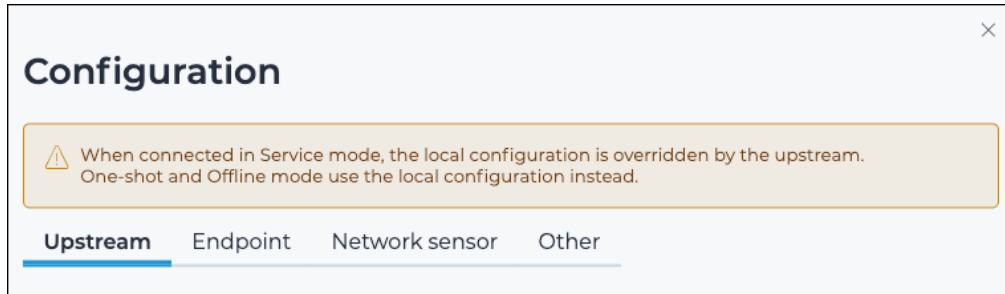


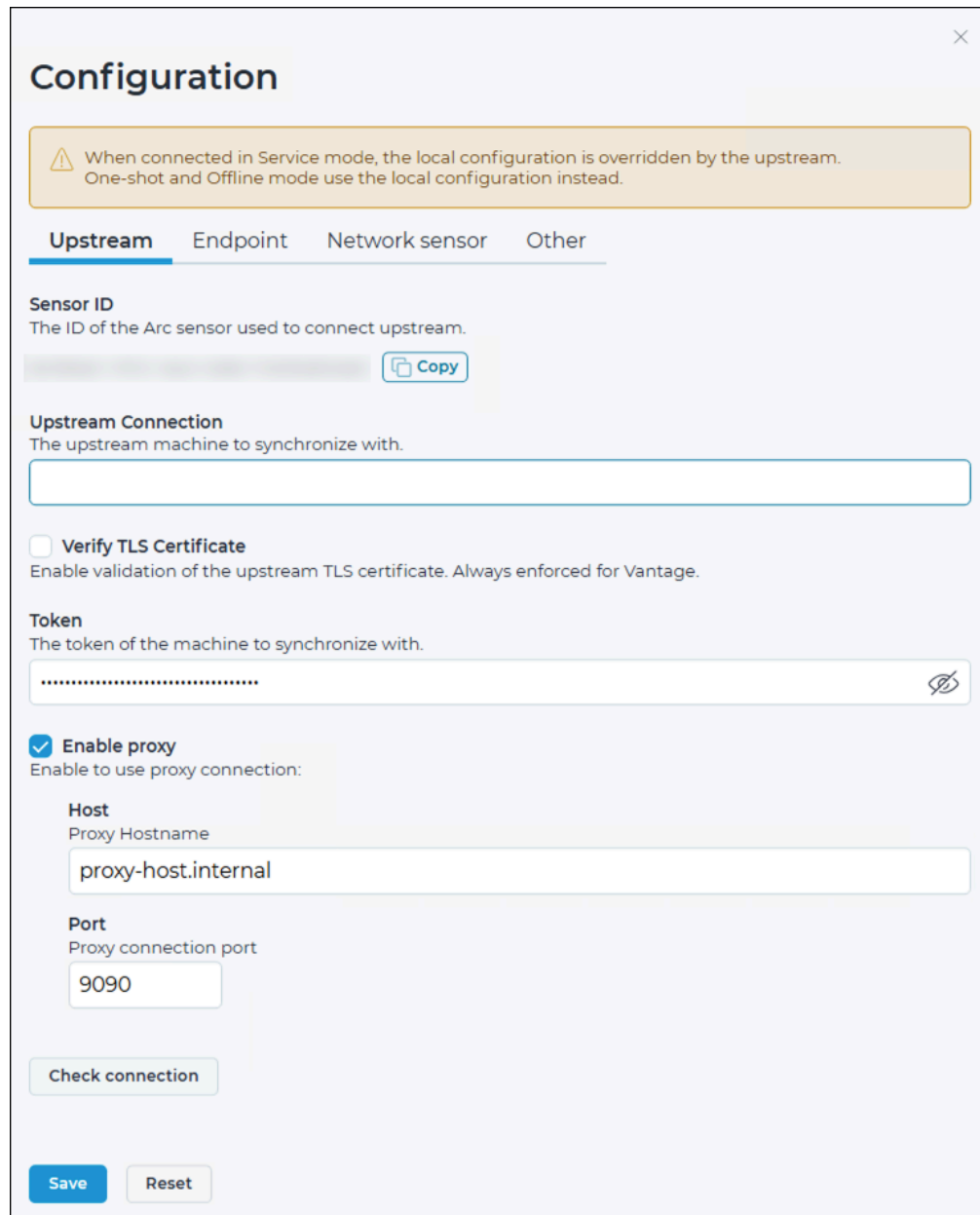
Figure 19. Configuration page

The **Configuration** page has these sections:

- [Upstream \(on page 65\)](#)
- [Endpoint \(on page 67\)](#)
- [Network sensor \(on page 69\)](#)
- [Other \(on page 72\)](#)

Upstream

Configure and verify the connection between the Arc sensor and the upstream machine using an IP address and authentication token. The page also displays the sensor ID and optional certificate validation and web proxy settings.



The screenshot shows the 'Configuration' window with the 'Upstream' tab selected. At the top, a warning box states: 'When connected in Service mode, the local configuration is overridden by the upstream. One-shot and Offline mode use the local configuration instead.' Below this, the 'Upstream' tab is active, showing the 'Sensor ID' field with a 'Copy' button. The 'Upstream Connection' section includes a text input for the upstream machine, a 'Verify TLS Certificate' checkbox (unchecked), and a 'Token' field with a masked input and an eye icon. The 'Enable proxy' checkbox is checked, leading to 'Host' (proxy-host.internal) and 'Port' (9090) fields. A 'Check connection' button is below these fields. At the bottom are 'Save' and 'Reset' buttons.

Figure 20. Upstream

Sensor ID

This is the *ID* of the Arc sensor that is used to connect to the upstream sensor.

Upstream Connection

This shows the *IP* address of the upstream machine that the sensor is connected to.

**CAUTION:**

After the upstream connection is initially set to a Guardian under the [CMC](#), it is not possible to update it to another Guardian under the same [CMC](#). You need to reconfigure the upstream connection manually. This is best done with the help of Nozomi Networks [Customer Support](#).

Verify TLS Certificate

Select this option to enforce verification of the upstream [TLS](#) certificate when connecting to Guardian. When using Vantage, [TLS](#) certificate validation is always enforced, regardless of this setting.

Token

The token Arc needs to authenticate to the Guardian/Vantage endpoint.

Enable proxy

Select this option to connect to the upstream endpoint through a web proxy.

- **Host:** The hostname of the proxy server
- **Port:** The port that the proxy server uses for connections

Check connection

This button checks if the connection parameters are correct.

Endpoint

Configure detection options for endpoint monitoring in Arc. Arc collects endpoint data, validates assets using ARP, and detects malware with configurable response actions.

Configuration

⚠ When connected in Service mode, the local configuration is overridden by the upstream. One-shot and Offline mode use the local configuration instead.

Upstream **Endpoint** Network sensor Other

Select which information to detect:

☒ **Main asset information** ⓘ
Always enabled.

☒ **Additional asset information**

Every synchronization (~1 minute)	Every 24 hours
☐ CPU usage	☒ Installed softwares
☐ RAM usage	☒ Hotfixes
☐ Disk usage	☒ User accounts
☒ Logged-in users	☐ DNS
☒ Processes with network activity	

☒ **Unusual behaviors**
Use Sigma indicators to monitor local events for signs of suspicious activity.

☒ **Valid assets (using ARP)**
Use the local address resolution protocol (ARP) table to confirm media access control (MAC) addresses.

☒ **Use static entries**
User-defined (disable in case these entries are not trusted).

☒ **USB devices**
Detect the use of USB devices and malicious HID.

☒ **Malware**
Use Yara and STIX indicators to detect malicious file patterns before they get transferred over the network.

Action to perform on malware detection [New](#)

Only alert ▼

Directory exclusions

Figure 21. Endpoint

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 [DNS](#) servers and configuration of the endpoint.
- **Installed software:** The software packages installed on the endpoint.

Valid assets (using ARP)

Enable this option to use the local [ARP](#) table to confirm [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.

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.

Network sensor

Configure Arc network sensor features such as Discovery, Smart Polling, and traffic monitoring. These options help identify neighboring devices, enrich asset data, and analyze network traffic patterns.

Configuration

⚠ When connected in Service mode, the local configuration is overridden by the upstream. One-shot and Offline mode use the local configuration instead.

Upstream

Endpoint

Network sensor

Other

Select how to monitor your network.

☒ **Discovery**

Leverage lightweight network announcements to discover neighboring devices. Continuous traffic monitoring is required for ARP and S7 discovery strategies to work properly.

☒ **Smart Polling** License required

Use surgical active queries to enrich asset data.

☐ **Traffic monitoring**

Monitor network traffic using either intermittent or continuous modes.

☐ Enable continuous mode

Time per notification

10

seconds

Max packets per notification

2000

packets

Max used Memory

32

MB

Global BPF filter

Applied to all network interfaces where a local BPF filter is not set. Syntactically incorrect filters will cause Traffic monitoring to stop.

e.g. tcp dst port not 443

Network interfaces

All interfaces are enabled by default.

Choose a network interface to configure

Save

Figure 22. Network sensor

Discovery

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

arc-admin v2.11.0 2026-10-01

69

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 [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 [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 [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

Traffic summary

This checkbox lets you enable or disable traffic summary. This option is available when traffic monitoring is enabled, and is disabled by default.

When enabled, Arc extracts only metadata from traffic for which deep packet inspection is not effective, such as encrypted or multimedia traffic. This metadata is sent upstream instead of the full payloads.

Heavy multimedia traffic, such as high-quality video feeds from security cameras or video conference software, can create a substantial load. With traffic summary enabled, this traffic is summarized as metadata, which reduces the upstream bandwidth consumption considerably without any loss of data. On the upstream appliance, the result is the same, and the data is available as usual, in the form of assets, links, and other information.

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.

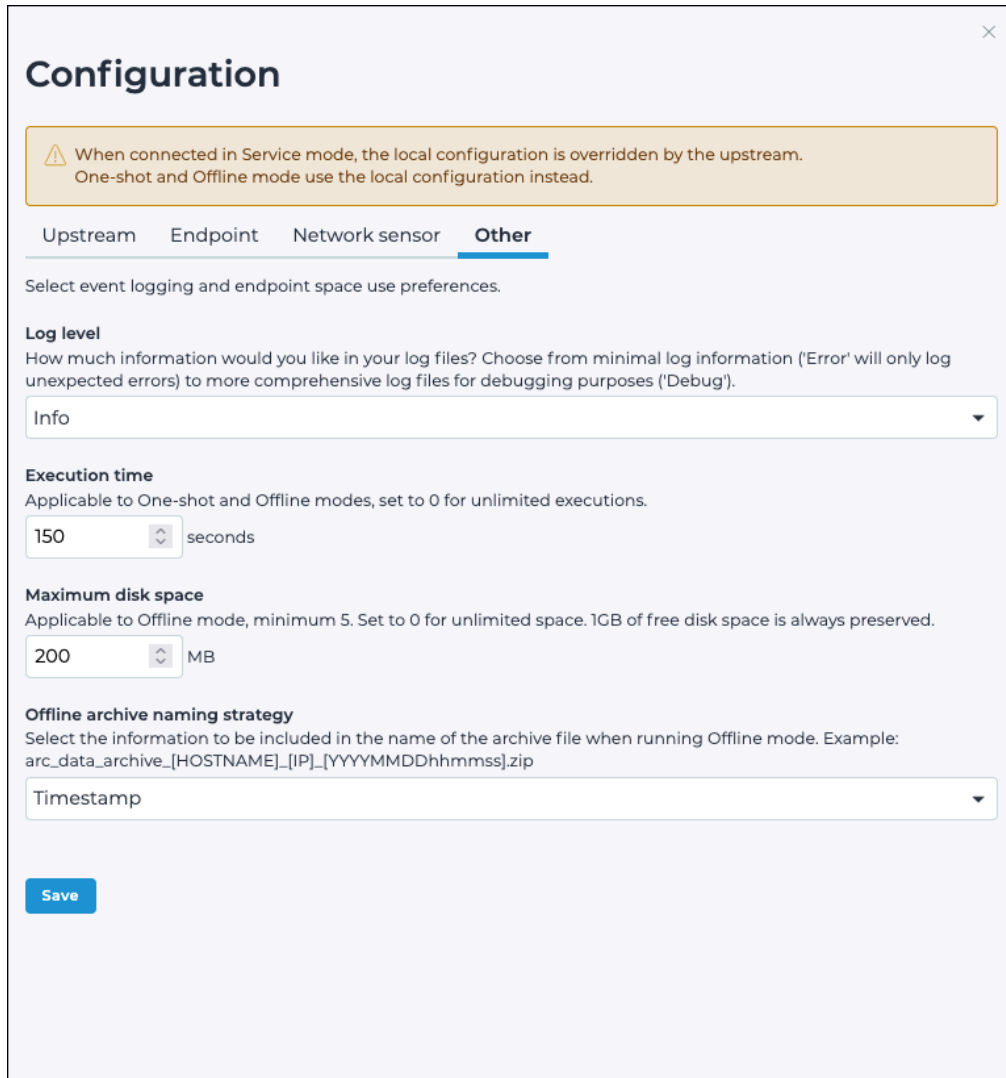
Network interface

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.

Other

Set Arc log verbosity, data collection duration, disk space usage limits, and the offline archive naming strategy for One-shot and Offline modes. These options help manage local resource usage and troubleshoot performance.



The screenshot shows a 'Configuration' window with a close button (X) in the top right corner. Below the title bar is a warning message: 'When connected in Service mode, the local configuration is overridden by the upstream. One-shot and Offline mode use the local configuration instead.' Below this is a tabbed interface with four tabs: 'Upstream', 'Endpoint', 'Network sensor', and 'Other' (which is selected and highlighted with a blue underline). Under the 'Other' tab, there is a heading 'Select event logging and endpoint space use preferences.' followed by three sections: 'Log level' with a description and a dropdown menu set to 'Info'; 'Execution time' with a description and a spinner set to '150' seconds; and 'Maximum disk space' with a description and a spinner set to '200' MB. Below these is the 'Offline archive naming strategy' section with a description and a dropdown menu set to 'Timestamp'. At the bottom left of the window is a blue 'Save' button.

Configuration

⚠ When connected in Service mode, the local configuration is overridden by the upstream. One-shot and Offline mode use the local configuration instead.

Upstream Endpoint Network sensor **Other**

Select event logging and endpoint space use preferences.

Log level
How much information would you like in your log files? Choose from minimal log information ('Error' will only log unexpected errors) to more comprehensive log files for debugging purposes ('Debug').

Info

Execution time
Applicable to One-shot and Offline modes, set to 0 for unlimited executions.

150 seconds

Maximum disk space
Applicable to Offline mode, minimum 5. Set to 0 for unlimited space. 1GB of free disk space is always preserved.

200 MB

Offline archive naming strategy
Select the information to be included in the name of the archive file when running Offline mode. Example: arc_data_archive_[HOSTNAME]_[IP]_[YYYYMMDDhhmmss].zip

Timestamp

Save

Figure 23. Other

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 [OSs](#), 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 \(on page 166\)](#).

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 [MB](#) that will be used for Offline mode.

Offline archive naming strategy

This dropdown lets you select the information to include in the name of the archive file that Arc creates when running in Offline mode. For example:

`arc_data_archive_[HOSTNAME]_[IP]_[YYYYMMDDhhmmss].zip`.

Status

The **Status** section shows a list of all the required dependencies for the selected sensor, and the installation status for each dependency.

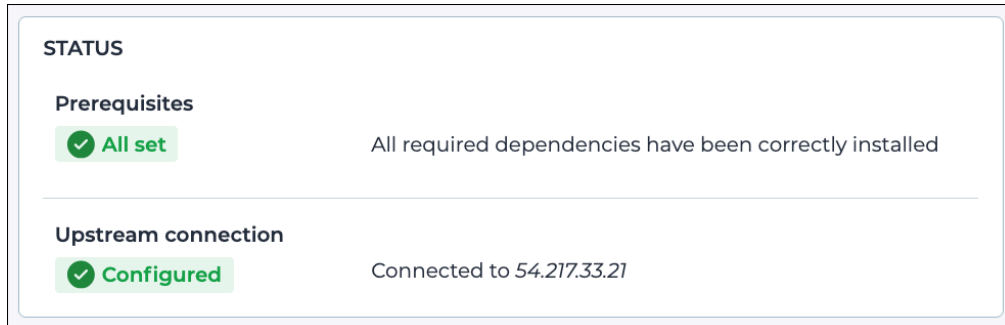


Figure 24. Status

Prerequisites

This shows the status of the dependencies. If a dependency is not installed, a warning message will show.

Upstream connection

This shows the status and the *IP* address of the upstream connection.

Latest run

The **Latest run** section shows the status and mode of the latest run that was executed.

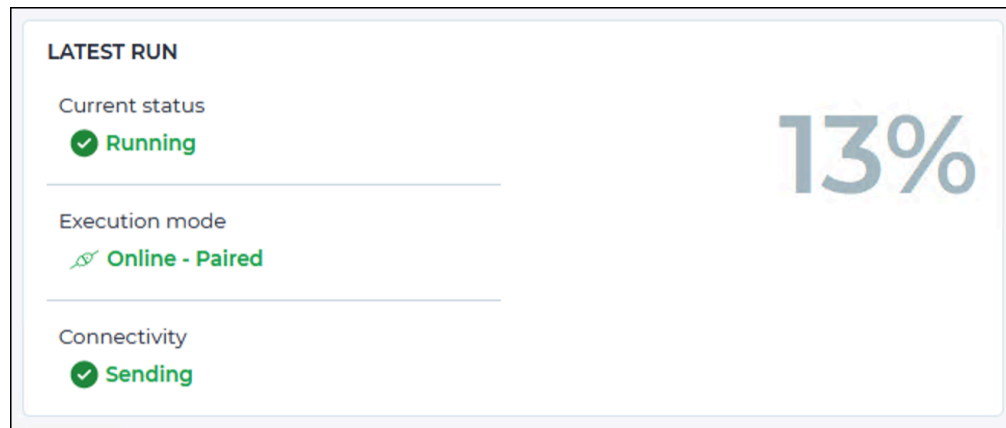


Figure 25. Latest run

Current status

This shows the current status of the latest run. A percentage value will show.

Execution mode

This shows the current execution mode and connectivity status.

Not available - while not running.

Disconnected - while in **Offline** mode.

Sending - standard behavior, data goes upstream.

Sending, Buffering - data is being sent and buffering is happening due to incoming data.

Sending, Dropping - data is being sent and dropped because incoming data and buffering limits were reached.

Disconnected (never connected) - network was absent before Arc could ever connect to the upstream.

Buffering (never connected) - network was absent before Arc could ever connect to the upstream: buffering started due to incoming data.

Dropping (never connected) - network was absent before Arc could ever connect to the upstream: dropping started due to reaching buffering limits.

Disconnected (last connection at dd-mm-yyyy hh:mm:ss) - network was absent since the indicated time.

Buffering (last connection at dd-mm-yyyy hh:mm:ss) - network was absent since the indicated time: buffering started due to incoming data.

Dropping (last connection at dd-mm-yyyy hh:mm:ss) - network was absent since the indicated time: dropping started due to incoming data and buffering limits were reached.

Asset inventory

The **Asset inventory** section displays the status of Discovery and Smart Polling. These features provide visibility into networked devices and asset details.

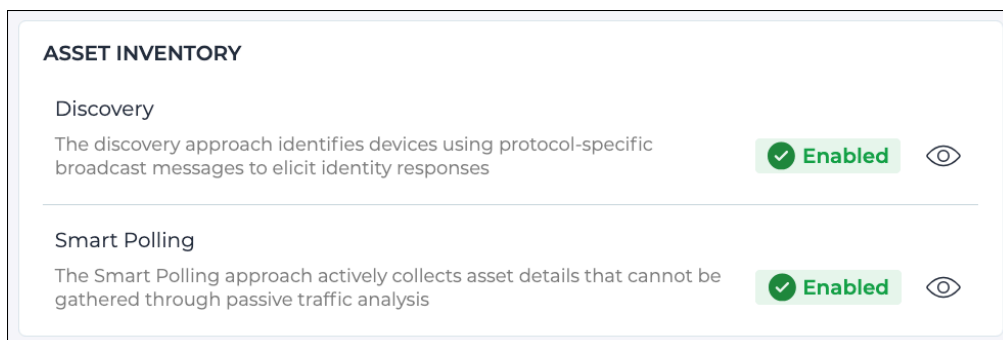


Figure 26. Asset inventory

Discovery

This shows if Discovery mode is enabled or not. The  icon shows details of the: Last execution.

Smart Polling

This shows if Smart Polling mode is enabled or not. The  icon shows details of the:

- Last execution
- Smart Polling strategies

Last 100 runs

The **Last 100 runs** section shows the status of the last 100 runs.

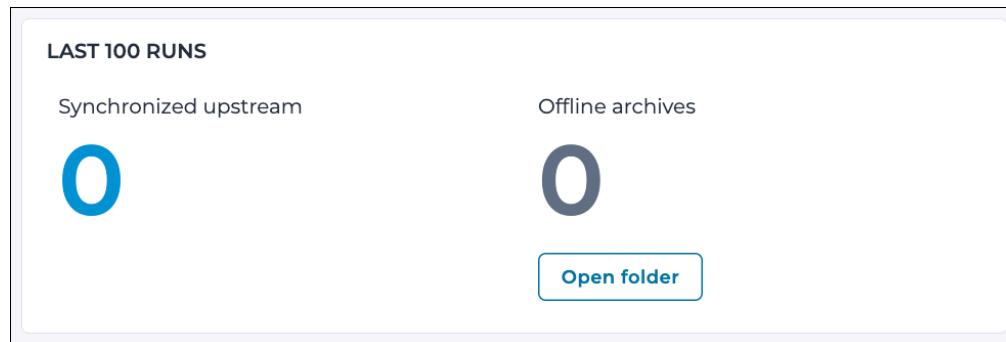


Figure 27. Last 100 runs

Synchronized upstream

The amount of times that Arc has communicated with the upstream since the start of the run.

Offline archives

This shows the amount of offline archives that have been created in the last 100 runs. The **Open folder** button lets you browse and access local archive files using your system's file explorer.

This asset

The **This asset** tab displays information about the host on which Arc is running, across several tabs.

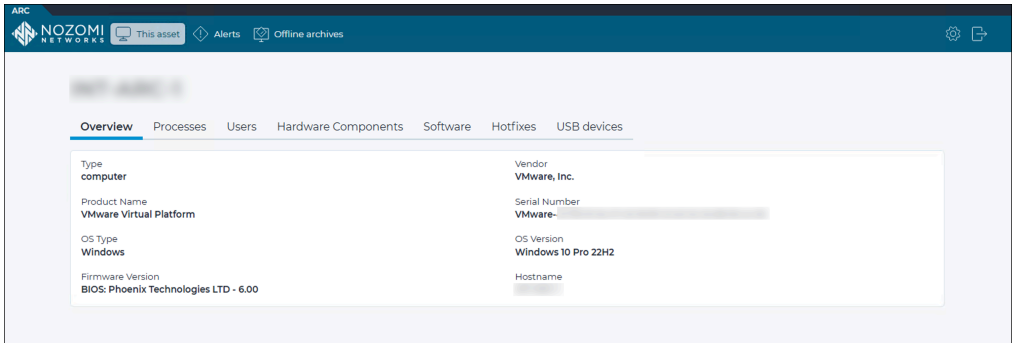


Figure 28. This asset tab

The **This asset** tab provides the following tabs:

- [Overview \(on page 79\)](#)
- [Processes \(on page 80\)](#)
- [Users \(on page 81\)](#)
- [Hardware components \(on page 82\)](#)
- [Software \(on page 84\)](#)
- [Hotfixes \(on page 85\)](#)
- [USB devices \(on page 87\)](#)

Related information

[Local UI \(on page 61\)](#)

Overview

The **Overview** tab shows identity and system information about the host on which Arc is running.

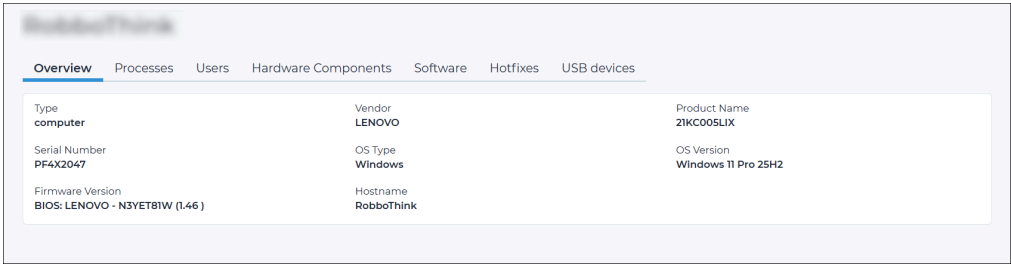


Figure 29. Overview

The **Overview** tab displays identity and system information about the host on which Arc is running. The tab shows the following fields:

Type

The device type, for example, **Computer**.

Vendor

The hardware vendor of the device.

Product name

The product name of the device.

Serial number

The serial number of the device.

OS type

The **OS** running on the host, for example, **Windows**.

OS version

The version of the **OS** running on the host.

Firmware version

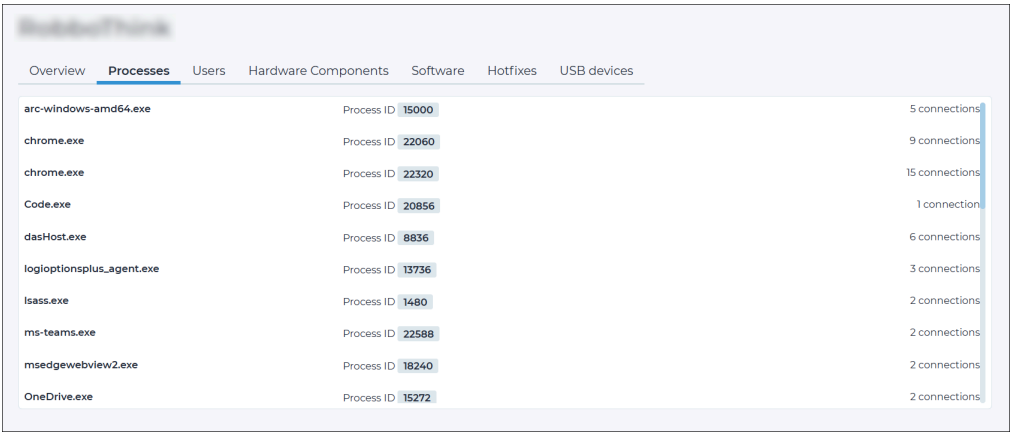
The firmware version of the device.

Hostname

The network hostname of the device.

Processes

The **Processes** tab shows the list of active processes on the host that have open ports.



Overview	Processes	Users	Hardware Components	Software	Hotfixes	USB devices
arc-windows-amd64.exe	Process ID	15000				5 connections
chrome.exe	Process ID	22060				9 connections
chrome.exe	Process ID	22320				15 connections
Code.exe	Process ID	20856				1 connection
dasHost.exe	Process ID	8836				6 connections
logioptionsplus_agent.exe	Process ID	13736				3 connections
lsass.exe	Process ID	1480				2 connections
ms-teams.exe	Process ID	22588				2 connections
msedgewebview2.exe	Process ID	18240				2 connections
OneDrive.exe	Process ID	15272				2 connections

Figure 30. Processes

The **Processes** tab displays the list of active processes on the host that have open ports. The list includes the following columns:

Name

The executable name of the process.

Process ID

The unique numeric identifier assigned to the process by the [OS](#).

Connections

The number of active network connections associated with the process.

Users

The **Users** tab shows the list of users on the host.

Name	Description	Account type	Domain	Password changeable	Password required	Password expires	Lockout	Status
Administrator		Admin	Domain: MicrosoftAccount	Password info				
arcuser		Admin	Domain: \\\	Password info				Status: Disabled
DefaultAccount		Guest	Domain: \\\	Password info				Status: OK
Guest		Guest	Domain: \\\	Password info				Status: Disabled
Guest		Guest	Domain: \\\	Password info				Status: Disabled
Admin		Admin	Domain: \\\	Password info				Status: OK

Figure 31. Users

The **Users** tab displays the list of user accounts on the host. The list includes the following columns:

Name

The username of the account, including the full name in parentheses where available.

Description

A brief description of the account.

Account type

The type of the account, for example, a local or domain account.

Domain

The domain to which the account belongs.

Password changeable

Indicates whether the account password can be changed.

Password required

Indicates whether a password is required for the account.

Password expires

Indicates whether the account password expires.

Lockout

Indicates whether the account is locked out.

Status

The current status of the account.

Hardware components

The **Hardware components** tab shows the list of hardware devices connected to the host.

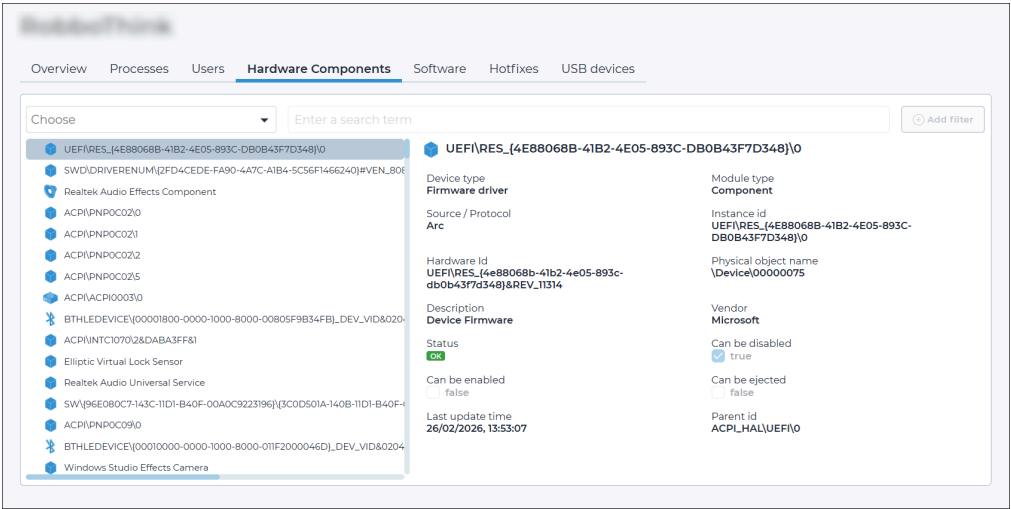


Figure 32. Hardware components

The **Hardware components** tab displays the hardware devices detected on the host. Selecting a device in the list shows its detailed properties in the detail panel, which includes the following fields:

Friendly name

The human-readable name of the device.

Device type

The category of the device, for example, **Disk drives** or **Network adapters**.

Description

A description of the device as reported by the [OS](#).

Vendor

The manufacturer of the device.

Hardware ID

The hardware identifier string used by the [OS](#) to match the device against drivers.

Physical object name

The physical object name of the device in the kernel namespace.

Status

The operational status of the device.

Can be disabled

Indicates whether the device can be disabled.

Can be enabled

Indicates whether the device can be enabled.

Can be ejected

Indicates whether the device can be safely ejected.

Parent ID

The instance identifier of the parent device in the hardware tree.

Location information

A text string identifying the physical location of the device as reported by the bus driver, for example, `Port_#0001.Hub_#0002` for [USB](#) devices.

Location paths

One or more structured paths that trace the device's position through the Windows device tree, from the [peripheral component interconnect \(PCI\)](#) root down to the specific port. For example, `PCIR00T(0)#PCI(1400)#USB00T(0)#USB(1)`.

Related information

USB devices (on page 87)

Software

The **Software** tab shows the list of software installed on the host.

Name	Version	Vendor	Install date	Install location	Size (MB)
Microsoft.WebplImageExt...	1.2.14.0	CN=Microsoft Corporatio...		C:\Program Files\Window...	
System Informer	3.2.25011.2103	Winsider Seminars & Solu...		C:\Program Files\SystemI...	
Windows SDK Desktop LI...	10.1.26100.7463	Microsoft Corporation	2026-01-08		65.36
SynapticsIncorporated.Sy...	11.20.0	CN=2424ED03-11AD-4252...		C:\Program Files\Window...	
Microsoft.AccountsControl	10.0.26100.1	CN=Microsoft Windows, ...		C:\Windows\SystemAppa...	
Microsoft.Windows.XGpu...	10.0.26100.1	CN=Microsoft Windows, ...		C:\Windows\SystemAppa...	
Microsoft.Office.ActionsS...	16.0.19628.20214	CN=Microsoft Corporatio...		C:\Program Files\Window...	
SDK ARM64 Redistributa...	10.1.26100.7463	Microsoft Corporation	2026-01-08		0.43
Windows SDK DirectX x8...	10.1.26100.7463	Microsoft Corporation	2026-01-08		0.43
Windows Software Devel...	10.1.26100.4188	Microsoft Corporation			2287.96

Figure 33. Software

The **Software** tab displays the list of software installed on the host. The list includes the following columns:

Name

The name of the installed software.

Version

The version of the installed software.

Vendor

The vendor or publisher of the software.

Install date

The date on which the software was installed.

Install location

The directory path where the software is installed.

Install source

The source path or medium from which the software was installed.

Size

The disk space used by the installed software, in [MB](#).

Related information

Hotfixes (on page 85)

Hotfixes

The **Hotfixes** tab shows the list of Windows hotfixes installed on the host.

Name	Caption	Description	Fix comments	Installed date
Lenovo - System - 4.3.11.0		Lenovo System driver update relea...	https://learn.microsoft.com/en-us/windows-hardw...	2025-07-15 17:26:45.167
Intel - SoftwareComponent - ...		Intel SoftwareComponent driver up...	https://learn.microsoft.com/en-us/windows-hardw...	2025-07-15 17:28:27.878
Intel(R) Corporation - HIDCla...		Intel(R) Corporation HIDClass driver...	https://learn.microsoft.com/en-us/windows-hardw...	2025-07-15 17:28:32.738
Windows 11, version 24H2		Install the latest version of Window...	https://go.microsoft.com/fwlink/?linkid=2132062#w...	2025-08-07 04:33:21.024
Security Intelligence Update ...		Install this update to revise the files...	https://go.microsoft.com/fwlink/?linkid=2007160	2025-10-10 01:31:03.866
Security Intelligence Update ...		Install this update to revise the files...	https://go.microsoft.com/fwlink/?linkid=2007160	2025-12-22 21:56:23.330
Microsoft.People_8wekyb3d8...				2026-02-25 10:22:54.821
KB5064081	KB5064081		Package_for_RollupFix~31bf3856ad364e35~amd64...	2025-09-03 09:45:26.000
KB5054156	KB5054156		Package_for_KB5054156~31bf3856ad364e35~amd6...	2025-10-13 05:27:26.000
KB5077869	KB5077869		Package_for_ServicingStack_7839~31bf3856ad364...	2026-02-22 04:41:13.000

Figure 34. Hotfixes

The **Hotfixes** tab displays the list of Windows hotfixes installed on the host. The list includes the following columns:

Name

The *knowledge base (KB)* article identifier for the hotfix, for example, **KB5017264**.

Computer name

The name of the computer system on which the hotfix is recorded.

Caption

A link to the support article for the hotfix.

Description

The type of update, for example, **Update** or **Security Update**.

Fix comments

Additional notes or comments about the hotfix.

Installed by

The user account that installed the hotfix.

Installed date

The date on which the hotfix was installed.

Status

The current status of the hotfix.

Service pack in effect

The service pack that was in effect when the hotfix was installed.

Related information

Software (on page 84)

USB devices

The **USB devices** tab shows a tree-like presentation of the USB hardware devices connected to the host.

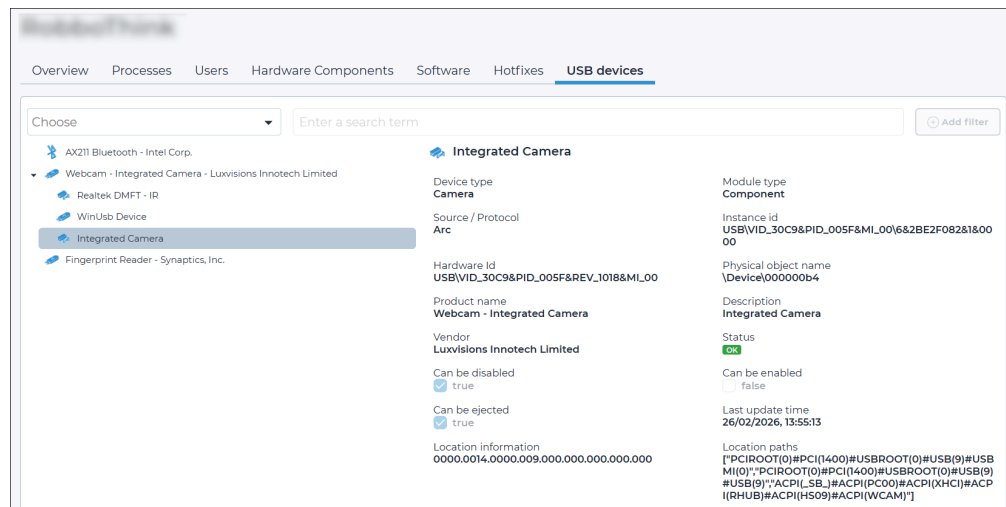


Figure 35. USB devices

The **USB devices** tab displays a hierarchical tree of the **USB** devices connected to the host. Selecting a device in the tree shows its detailed properties in the detail panel, which includes these fields:

Choose

A dropdown for selecting the field to filter the tree by.

Search field

A text field for entering the filter value.

Add filter

Applies the selected field and entered value as a filter to the tree.

Friendly name

The human-readable name of the **USB** device.

Product name

The product name resolved from the **USB** vendor and product ID database.

Vendor

The vendor resolved from the **USB** vendor ID database.

Device type

The category of the USB device, for example, **Universal Serial Bus controllers** or **Human Interface Devices**.

Description

A description of the device as reported by the **OS**.

Physical object name

The physical object name of the device in the kernel namespace.

Hardware ID

The hardware identifier string, including the [USB](#) vendor ID (VID) and product ID (PID), used by the [OS](#) to match the device against drivers.

Status

The operational status of the device, for example, **OK**.

Can be disabled

Indicates whether the device can be disabled.

Can be enabled

Indicates whether the device can be enabled.

Can be ejected

Indicates whether the device can be safely ejected.

Parent ID

The instance identifier of the parent device in the hardware tree.

Location information

A text string identifying the port and hub where the device is connected, for example, **Port_#0001.Hub_#0002**.

Location paths

One or more structured paths that trace the device's position through the Windows device tree, from the [PCI](#) root down to the specific [USB](#) port. For example, **PCIROOT(0)#PCI(1400)#USBROOT(0)#USB(1)#USB(3)**.

Related information

Hardware components (on page 82)

Alerts

The **Alerts** page lists every alert that the sensor has generated.

Act...	Time	Name	Type	Risk	Source	Destination	Desc
	15/16/05/835	Sigma rule match	SIGN SIGMA-RULE	5	INT-ARC-1		The
	15/16/05/772	Sigma rule match	SIGN SIGMA-RULE	2	INT-ARC-1		The
	15/16/05/660	Sigma rule match	SIGN SIGMA-RULE	2	INT-ARC-1		The
	15/16/05/660	Sigma rule match	SIGN SIGMA-RULE	5	INT-ARC-1		The
	15/16/05/464	Sigma rule match	SIGN SIGMA-RULE	5	INT-ARC-1		The
	15/16/05/374	Sigma rule match	SIGN SIGMA-RULE	2	INT-ARC-1		The
	15/16/05/034	Sigma rule match	SIGN SIGMA-RULE	5	INT-ARC-1		The
	15/16/05/033	Sigma rule match	SIGN SIGMA-RULE	2	INT-ARC-1		The
	15/16/05/007	Sigma rule match	SIGN SIGMA-RULE	9	INT-ARC-1		The
	15/16/02/469	Sigma rule match	SIGN SIGMA-RULE	9	INT-ARC-1		The

Figure 36. Alerts page

Live

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

Refresh

The **Refresh**  icon lets you immediately refresh the current view.

Columns

The **Columns** button lets you select which of the available columns for the current page will show.

Time

The date and time at which the alert was generated. By default, alerts are sorted by time, most recent first.

Name

The name of the alert.

Type

The type of alert.

Risk

The risk level associated with the alert.

Source

The label or *IP* address of the source associated with the alert.

Destination

The label or *IP* address of the destination associated with the alert.

Description

A description of the alert.

Alert sources

The sensor generates alerts from the following detection sources:

- [USB](#) events: A [USB](#) device is plugged in or unplugged, draws unusual power, releases a scripted key, or transfers data
- Sigma rule matches
- [Structured Threat Information Expression \(STIX\)](#) indicator matches
- Windows Defender detections
- Malware rule matches

Related information

Local UI (on page 61)

Compliance

The **Compliance** tab shows compliance information for the host on which Arc is running, across several tabs.

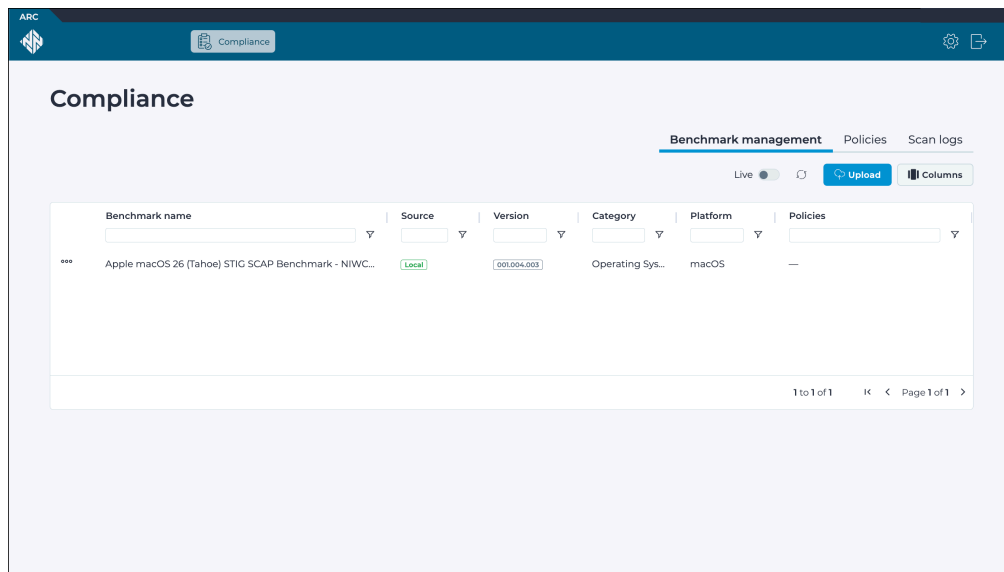


Figure 37. Compliance tab

For more details, see [Compliance scanning \(on page 108\)](#).

The **Compliance** tab provides the following tabs:

- [Benchmark management \(on page 93\)](#)
- [Policies \(on page 96\)](#)
- [Scan logs \(on page 99\)](#)

Related information

[Local UI \(on page 61\)](#)

Why use Compliance

Compliance runs standards-based hardening benchmarks against the host on which Arc is running, replacing one-off manual audits with auditable evidence of its security posture.

Confirming that an asset meets a security-hardening standard is traditionally a manual exercise. Someone works through a checklist against a benchmark by hand, on however many assets they can reach. The result is a snapshot that starts going stale the moment it is taken. Repeating that consistently, on a schedule, with a defensible record of every exception, is difficult to do by hand at any real scale.

What Compliance gives you

- **Standards-based scanning, not ad hoc checklists.** A benchmark is a file that follows the [Security Content Automation Protocol \(SCAP\)](#) standard and is written in [Extensible Configuration Checklist Description Format \(XCCDF\)](#) format, the same machine-readable format used by issuing bodies such as DISA for [Security Technical Implementation Guide \(STIG\)](#) benchmarks, so a scan checks the same rules the same way every time.
- **Policies that repeat themselves.** A policy groups benchmarks into a versioned, reusable unit, so scanning the same target again means running the same policy rather than rebuilding a checklist from scratch.
- **An audit trail for exceptions, not silence.** When a rule genuinely cannot be met, an override records a reason code and a mandatory justification, keeping a history of who changed the result and why, rather than letting the failure quietly disappear.

On Arc

Arc has no scheduling of its own: scans run when the upstream system requests them, and the Arc **Compliance** page is read-only. Scan history remains available on the **Scan logs** tab.

Benchmark management

The **Benchmark management** tab lists the benchmarks available on this Arc sensor.

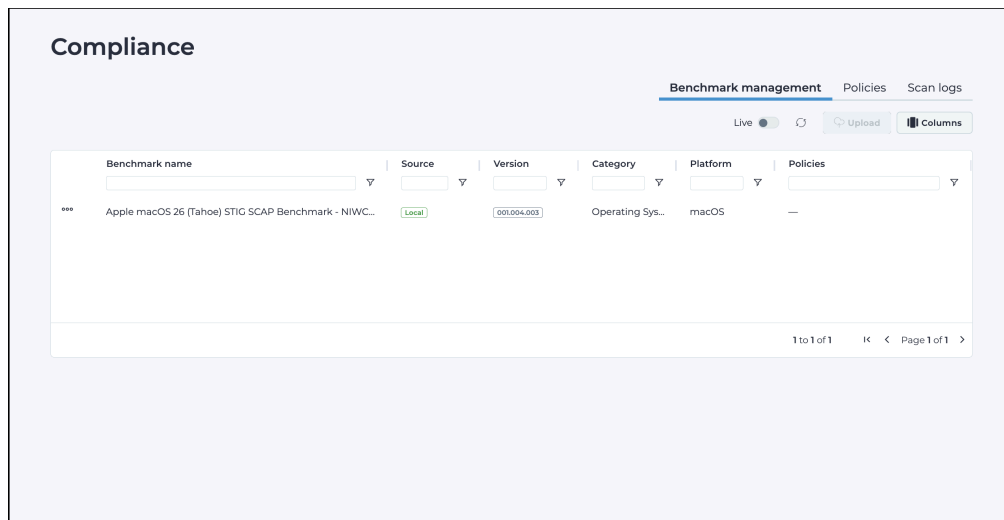


Figure 38. Benchmark management page

For more details, see [Compliance benchmarks \(on page 95\)](#).

The Benchmark management page is read-only: you cannot upload or delete benchmarks from Arc. Benchmarks are managed from the upstream system, and you can upload them only from Vantage. Arc stores benchmark files locally.

Column descriptions

The Rules, Published at, and Uploaded at columns are hidden by default.

Column label	Description
Benchmark name	The name of the benchmark.
Source	Which system provided the benchmark. In Vantage: provided by DISA (DISA) or uploaded by a user (Users). On Arc: uploaded on this sensor (Local) or fetched from the upstream system that manages this sensor (Remote).
Version	The version of the benchmark.
Category	The category of the benchmark, for example Operating System, Application, or Network Device.
Platform	The OS family the benchmark applies to, for example Windows or Linux.
Rules	The number of rules in the benchmark.

Column label	Description
Policies	The policies that use this benchmark. Select View JSON to see the full list.
Published at	The date the benchmark was published by its issuing body.
Uploaded at	When the benchmark was uploaded.
Uploaded by	The name of the user who uploaded the benchmark, or Update Service for Nozomi Networks-provided benchmarks. This column is shown in Vantage only; the Arc Benchmark management page does not include it.

Compliance benchmarks

A compliance benchmark is a file that defines the checks used to assess whether a system meets a security standard such as SCAP or STIG.

A benchmark file follows the [SCAP](#) standard and is written in [XCCDF](#) format. You obtain benchmarks from an issuing body, such as DISA for [STIG](#) benchmarks, rather than authoring your own.

Benchmarks come from two sources:

- **DISA-provided (DISA)**: These benchmarks sync automatically on a nightly basis. They are read-only and cannot be deleted.
- **User-uploaded (Users)**: The user uploads these benchmarks. An uploaded benchmark file must be an [eXtensible Markup Language \(XML\)](#) file, in [XCCDF](#) format, and no larger than the maximum file size shown in the upload dialog. You can only delete a user-uploaded benchmark if no policy references it.

When you upload a benchmark, it is validated against the expected format, and non-conforming files are rejected. Benchmarks are deduplicated by file content, not by filename: uploading a file whose content is identical to an existing benchmark refreshes that existing entry rather than creating a new one. Uploading a file with the same parsed benchmark name and version but different content replaces the content of the existing entry. A policy cannot include two benchmarks with the same [SCAP](#) benchmark [ID](#) and version.

**Note:**

On Arc, the **Benchmark management** page is read-only: you cannot upload or delete benchmarks from Arc. Benchmarks are managed from the upstream system, and you can upload them only from Vantage.

Policies

The **Policies** tab lists the policies configured on this Arc sensor.

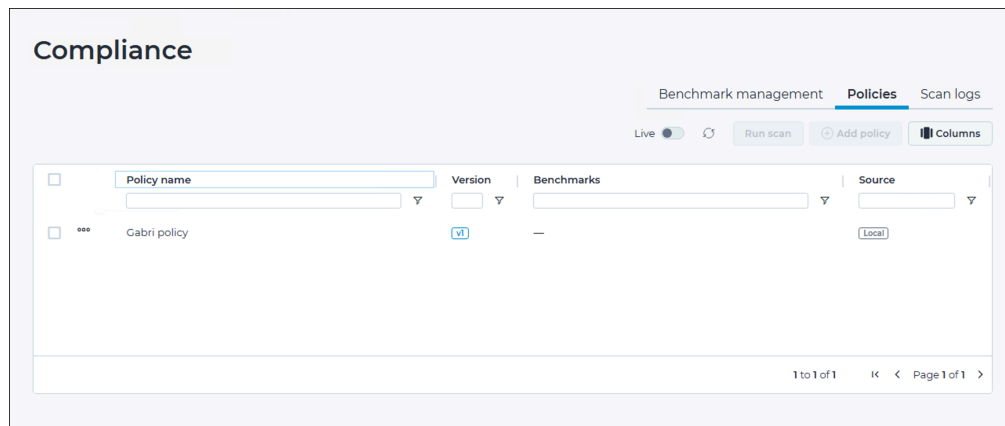


Figure 39. Policies page

For more details, see [Compliance policies \(on page 97\)](#).

The Policies page is read-only: policies are created and managed from the upstream system, and each scan requested from upstream creates a policy on this sensor. The Policies page has no **Schedules** column. Instead, it has a **Source** column. For more details, see [Policy source \(on page 98\)](#).

Column descriptions

The Rules, Updated, and Description columns are hidden until you enable them from the column panel.

Column label	Description
Policy name	The name of the policy.
Version	The current version number of the policy.
Benchmarks	The benchmarks included in the policy.
Rules	The number of rules in the policy, across all of its benchmarks.
Updated	When the policy was last updated.
Description	The description of the policy.
Source	Whether the policy was created locally (Local), or was created automatically by a scan requested from upstream (Remote).

Compliance policies

A compliance policy groups one or more benchmarks together so you can run them as a single scan.

A policy selects the benchmarks to run and the platform they apply to. Every change you make to a policy, such as adding or removing a benchmark, creates a new version of that policy.

You can view a policy's version history at any time, and roll it back to an earlier version if needed.

**Note:**

On Arc, the **Policies** page is read-only: you cannot create, edit, or delete policies from Arc. Policies are managed from the upstream system.

Policy source

The **Source** column on the *Policies* page shows how a policy was created.

- **Local:** A policy that was created on this Arc sensor rather than by an upstream request. You can no longer create policies from Arc, so you only see this value for policies that already existed on the sensor.
- **Remote:** The upstream system that manages this Arc sensor requested a scan, and Arc created the policy automatically to run it

The Arc local UI is read-only: you cannot create, edit, or delete policies, regardless of their source. Policies are managed from the upstream system.

Each scan requested from upstream creates a new policy; it does not reuse an existing **Remote** policy from an earlier request. If the upstream system requests the same kind of scan repeatedly, you will see more than one **Remote** policy accumulate over time.

Scan logs

The **Scan logs** tab lists the compliance scans that have run on this Arc sensor.

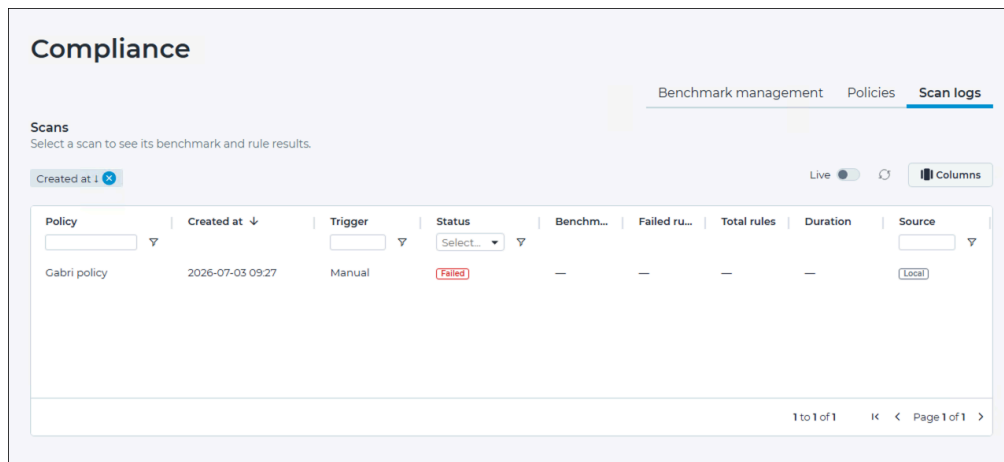


Figure 40. Scan logs page

For more details, see [Compliance scan logs \(on page 100\)](#).

Because Arc scans only the host it runs on, the Scan logs page has no **Target** column. Because Arc has no scheduling, it has no **Schedule** column either. Instead, it has a **Source** column, matching the one on the Policies page.

Column descriptions

Column label	Description
Policy	The policy the scan ran.
Created at	When the scan was created.
Trigger	How the scan was triggered: Manual .
Status	The scan's status. See Compliance statuses (on page 101) .
Benchmarks	The number of benchmarks included in the scan.
Failed rules	The number of rules that failed.
Total rules	The total number of rules evaluated.
Duration	How long the scan took to run.
Source	Whether the scan ran from a locally-created policy (Local), or was requested from upstream (Remote).

Compliance scan logs

A scan log entry records how a compliance scan was triggered and what it found.

Each scan log entry shows how the scan was triggered, along with its execution status and overall compliance result.

From a scan log entry, you can drill down into the benchmarks that ran. You can also drill into the individual rule results within each benchmark.

Compliance statuses

Describes the status values used at each level of a compliance scan.

A compliance scan reports status at several levels: the scan itself, each benchmark it runs, and each rule within a benchmark. The wording differs slightly at each level.

Not every value applies in every product. Arc has no scheduling, so it never shows a **Schedule status** or the **Scheduled** trigger value.

Level	Values
Scan status	Queued, Running, Cancelling. Once the scan completes: Cancelled, Compliant, Non-compliant, Not applicable, Not run, Error, Unknown
Status reason	For a scan or benchmark status, a more specific reason can replace the general status when known: Target not found, Not delivered, Failed, Timed out, Cancelled, Target unsupported, Target metadata missing, No eligible benchmarks, All benchmarks not applicable, Unreadable result, Platform mismatch, Benchmark metadata missing, Benchmark unavailable, No result returned, No rules applied. The Scan logs status filter offers the specific labels a row can display. A scan always shows its specific reason when it has one, so Error and Not run never appear as bare labels.
Benchmark status	Uses the same values as Scan status
Rule result	Pass, Fail, Error, Unknown, Not applicable, Not checked, Not selected, Informational
Severity	Critical, High, Medium, Low, Unknown
Schedule status	Draft, Active, Paused
Trigger	Manual, Scheduled

A rule's severity is set by the author of the benchmark file, for example DISA for a [STIG](#) benchmark. It cannot be changed by Nozomi Networks or by you.

Results aggregation

When a scan includes more than one benchmark, Nozomi Networks combines the individual benchmark results into a single overall verdict for the scan:

- If any benchmark is **Non-compliant**, the scan is **Non-compliant**.
- Otherwise, if at least one benchmark is **Compliant**, the scan is **Compliant**. A benchmark that returns **Not applicable**, for example because the target does not have the software the benchmark checks, does not prevent this.
- If every benchmark in the scan returns **Not applicable**, the scan is **Not applicable**.

For example, a scan runs three benchmarks: one for Linux, one for Google Chrome, and one for Adobe Reader. Chrome is not installed on the target, so that benchmark returns **Not applicable**, while the other two return **Compliant**. The scan is still **Compliant**, because a benchmark that could not run does not count against the result.

View scan results

Review the results of a completed compliance scan.

Procedure

1. In the top navigation bar, select **Compliance**.

Result: The **Compliance** page opens.

2. Select the **Scan logs** tab.
3. Select the applicable scan.

Results

The **Scan overview** section shows the policy that ran, its version, and its overall status, for example **Non-compliant**. Expand the overview to see the scan's **Duration**, **Scan started at**, and **Scan completed at**. Below the overview, the **Benchmarks** section lists each benchmark that ran, with counts of evaluated benchmarks and failed rules. Each benchmark row shows its version, status, highest severity, and rule counts, and lets you select **Download XML**, **Download HTML**, or **View rules**. Expand a benchmark to see its details. See [View benchmark rules \(on page 105\)](#).

Download scan results

Download the raw scan artifact for a benchmark, in XML or HTML format.

Procedure

1. In the top navigation bar, select **Compliance**.

Result: The **Compliance** page opens.

2. Select the **Scan logs** tab.
3. Select the applicable scan.
4. Select the applicable benchmark to expand its details.
5. Select **Download XML** or **Download HTML**, depending on which artifact you need.

Not every benchmark result has both formats available.

Results

The artifact downloads to your computer.

View benchmark rules

Review the individual rule results within a benchmark that ran as part of a scan.

Procedure

1. In the top navigation bar, select **Compliance**.

Result: The **Compliance** page opens.

2. Select the **Scan logs** tab.
3. Select the applicable scan.
4. Select the applicable benchmark to expand its details, then select **View rules**.

Result: If the benchmark's status is **Not applicable**, the benchmark was sent to the scan but returned no result. This is most likely because it does not apply to the **OS** family of the host it ran against.

5. Select the applicable rule to expand its details.

Result: Along with its rule **ID** and override status, the rule detail panel shows:

- **Description:** Background information about what the rule checks and why it matters
- **Remediation:** The recommended action to bring the host into compliance with the rule
- **Evidence:** The technical scan output used to evaluate the rule, including the specific test results

Results

The **Benchmark rules** panel opens, showing counts of failed, passed, and overridden rules, and the total number of rules. The rule list shows each rule's result, for example **Pass** or **Fail**, and its severity. You can filter the list by status (**All**, **Failed**, **Passed**, **Overridden**), by severity (**All severities**, **Critical**, **High**, **Medium**, **Low**), or search by rule **ID** or title.

Offline archives

The **Offline archives** page shows a list of the offline archives created on the host.

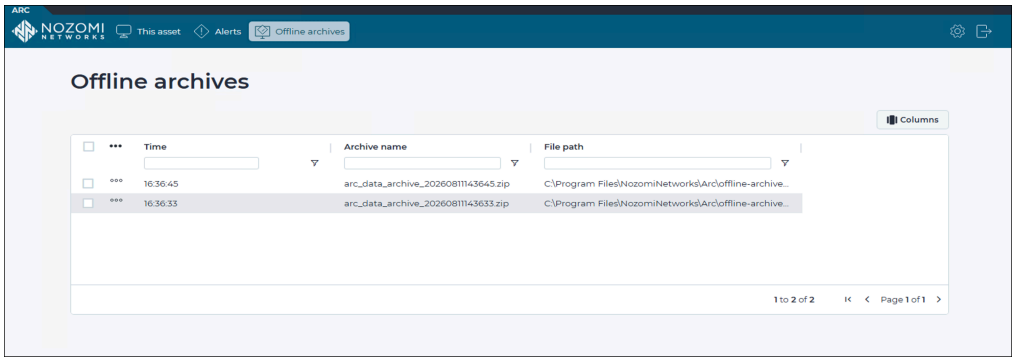


Figure 41. Offline archives page

The **Offline archives** page lists the offline archives available on the host. Each entry includes the following columns:

Time

The date and time at which the archive was created.

Archive name

The file name of the archive.

File path

The full path to the archive file on the host.

Open the local UI

The local UI lets you manage Arc without the use of a parent system software. It gives you access to the **Status** page to monitor the status of Arc executions, and the **Configuration** page to configure Arc executions. You can double-click the executable file to open it, or use the command-line interface (CLI).

Before you begin

Before you do this procedure, make sure that you have downloaded the correct Arc package for your [OS](#).

About this task

You can use either one of the two different methods given below to open the local [UI](#).

**Note:**

On macOS, before you can open the local [UI](#), you might need to enable Arc in **System Preferences > Security & Privacy**.

Procedure

1. Double-click the Arc package that you downloaded for your [OS](#) and architecture.

Result: In the Terminal that you used to launch Arc, a one-time password has been generated, and a dialog shows in the web [UI](#).

2. Alternatively, open a Terminal and enter a command, without a parameter. For example: `.\arc-windows-amd64.exe`

Result: In the Terminal that you used to launch Arc, a one-time password has been generated, and a dialog shows in the web [UI](#).

3. Copy the password from the Terminal.
4. In the **Enter the password** field, paste the password.
5. Select **Log in**.

Results

The local [UI](#) is now open.

Compliance scanning

Arc is the sensor that Compliance scans run against. Compliance scans run only when they are requested from the upstream system that manages the sensor.

Configuration

Compliance scanning is enabled or disabled from the upstream system that manages this Arc sensor. This setting does not appear in Arc's own local configuration [UI](#).

Supported platforms

Compliance scanning is supported on Windows, Linux, and macOS Arc sensors.

On-disk layout

Arc stores compliance data in a **compliance** folder next to the Arc executable, with **benchmarks** and **results** subfolders. This folder is preserved across a re-setup of Arc.

Licensing and availability

Compliance is a licensed feature, and the license comes from the upstream system that manages this Arc sensor. The **Compliance** item appears in Arc's local navigation bar only when both of these conditions are met:

- A valid Compliance license has been received from the upstream system.
- The Compliance feature is enabled for this sensor, from the upstream machine.

You enable the Compliance feature for a sensor from the upstream machine. For the steps, see [Enable or disable Compliance on an Arc sensor](#) (on page [108](#)).

Shell commands

A list of available shell commands.

Table 7. Shell commands - Linux

Command	Function	Note
<code>./arc-linux-arm install</code>	Install Arc as an OS-service, ready to be started. On reboot Arc is automatically started.	1
<code>./arc-linux-arm start</code>	Start the Arc service.	
<code>./arc-linux-arm stop</code>	Stop the Arc service.	
<code>./arc-linux-arm restart</code>	Restart the Arc service.	
<code>./arc-linux-arm uninstall</code>	Uninstall Arc.	1
<code>./arc-linux-arm version</code>	Return the Arc version.	
<code>./arc-linux-arm status</code>	Return the Arc service status.	
<code>./arc-linux-arm oneshot</code>	Start Arc in One-shot mode.	
<code>./arc-linux-arm offline</code>	Start Arc in Offline mode.	
<code>./arc-linux-arm</code>	Launch the local configuration UI .	
<code>./arc-linux-arm install_dependencies</code>	Trigger the dependencies installation.	1

Table 8. Shell commands - Windows

Command	Function	Note
<code>.\arc-windows-amd64.exe install</code>	Install Arc as an OS-service, ready to be started. On reboot Arc is automatically started.	1
<code>.\arc-windows-amd64.exe start</code>	Start the Arc service.	
<code>.\arc-windows-amd64.exe stop</code>	Stop the Arc service.	
<code>.\arc-windows-amd64.exe restart</code>	Restart the Arc service.	
<code>.\arc-windows-amd64.exe uninstall</code>	Uninstall Arc.	1
<code>.\arc-windows-amd64.exe version</code>	Return the Arc version.	
<code>.\arc-windows-amd64.exe status</code>	Return the Arc service status.	
<code>.\arc-windows-amd64.exe oneshot</code>	Start Arc in One-shot mode.	
<code>.\arc-windows-amd64.exe offline</code>	Start Arc in Offline mode.	
<code>.\arc-windows-amd64.exe</code>	Launch the local configuration UI .	
<code>.\arc-windows-amd64.exe install_dependencies</code>	Trigger the dependencies installation.	1

Table 9. Shell commands - macOS

Command	Function	Note
<code>./arc-darwin-amd64 install</code>	Install Arc as an OS-service, ready to be started. On reboot Arc is automatically started.	1
<code>./arc-darwin-amd64 start</code>	Start the Arc service.	
<code>./arc-darwin-amd64 stop</code>	Stop the Arc service.	
<code>./arc-darwin-amd64 restart</code>	Restart the Arc service.	
<code>./arc-darwin-amd64 uninstall</code>	Uninstall Arc.	1
<code>./arc-darwin-amd64 version</code>	Return the Arc version.	
<code>./arc-darwin-amd64 status</code>	Return the Arc service status.	
<code>./arc-darwin-amd64 oneshot</code>	Start Arc in One-shot mode.	
<code>./arc-darwin-amd64 offline</code>	Start Arc in Offline mode.	
<code>./arc-darwin-amd64</code>	Launch the local configuration UI .	
<code>./arc-darwin-amd64 install_dependencies</code>	Trigger the dependencies installation.	1



Chapter 5. Deployment



Deployment is defined as the process which results in one Arc sensor, or multiple Arc sensors, running on the chosen target machine(s).

Preparation

The preparation steps that you need to do will depend on the deployment option that you choose. The different options are:

- A deployment-ready Guardian
- Downloading the Arc package from the Nozomi Networks support portal
- Downloading the Arc package from Vantage

MDM deployment

When [MDM](#) software is in use in the applicable network, you can use it to automatically deploy Arc.

To use this method, you can use software such as:

- Microsoft Intune
- Microsoft Endpoint Configuration Manager

When you use this method to deploy Arc, you need to:

- Download the applicable Arc package
- Compile the [Microsoft Software Installer \(MSI\)](#) file
- Deploy the [MSI](#) file

Manual deployment

When you deploy Arc manually, you need to download the applicable Arc package first.

Manual deployment to run Service mode on Windows

If you want to run Arc in Service mode on Windows, you need to choose the provided [MSI](#) package. You can install and uninstall the software with the [MSI](#) package. You can also uninstall the application from the **Control Panel**. This can be run from any location.

Manual deployment for all other cases

1. Put the applicable Arc package on the target machine.
2. Run the Arc package locally.

Automatic deployment with Guardian

When connectivity to the target machine and their credentials can be granted to one or multiple Guardian, this can be also used to automatically deploy Arc.

Updates

Starting from v1.7.0, the Arc update mechanism no longer supports the update of an Arc that is installed outside of: **C:\Program Files\NozomiNetworks\Arc**

If you have Arc sensors that have previously been manually deployed outside of this path, you must manually uninstall them, and install them again.

Antivirus software

Arc is security software. It does not contain malicious behavior. If your antivirus software detects Arc as malware, treat it as a false positive. If this happens, please contact our [Customer Support](#) team.

Automatically

Deploy Arc automatically from Guardian on Windows

You can use the Windows Remote Management (WinRM) or Secure Shell (SSH) services to deploy Arc at scale for target machines that are reachable from Guardian.

Before you begin

- Credentials of the target machines are stored into the Credentials Manager
- An Administrator user is granted to access the target machine and to be used by Guardian in the process
- If you want to deploy with [WinRM](#):
 - [WinRM](#) is enabled locally and accepting incoming connections from the Guardian machine(s) used for deployment
 - [SMB](#) is enabled locally and accepting incoming connections from the Guardian machine(s) used for deployment
 - Connectivity is granted for the services above, namely [TCP/5985](#) and [TCP/445](#)
- If you want to deploy with [SSH](#) (Windows):
 - [SSH](#) is enabled locally and accepting incoming connections from the Guardian machine(s) used for deployment
 - Connectivity is granted for the services above, namely [TCP/22](#)

Procedure

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

Actions	Deployed version	Operating system	Name	IP	Vendor	Product name	Type
☐		macOS	MACBOOKPRO-DEFE	10.41.132.205, fe80:14ac2	Apple	MacBook Pro	computer
☐		macOS	TX6ST7Y7JD-MacBookPro.local	10.41.132.157, fe80:3e23f2	Apple	MacBook Pro	computer
☐		macOS	N6V4H90V4J-MacBookPro.local	10.41.132.183, fe80:89d2f	Apple	MacBook	computer
☐		macOS	Gios-MBP.local	10.41.132.204, fe80:8e5b	Apple	MacBook Pro	computer
☐		Windows 10 / Server	LE-SIE-TIA-PRTL.local	172.16.16.241, 192.168.45.227	VMware	Virtual Machine	computer
☐		Windows 7	172.18.240.28	172.18.240.28			computer
☐		CNU/Linux	farm.plista.com		Seiko Epson Corporation	WorkForce WF-7710	printer_scanner
☐		Windows 7	172.18.98.26	172.18.98.26			computer
☐		macOS	YQQPVYKSPV-MacBookPro.local	10.41.132.208, fe80:1c0a2	Apple	MacBook Pro	computer
☐		macOS 14.4.1	C3PH97J5WQ-MacBook-Pro-16	fe80:a0a997fffe2a5f4e	Apple	MacBook Pro	computer
☐		macOS	C02ZF05ALVDM-MacBookPro.l	192.168.1.128, 192.168.45.8	Apple	MacBook Pro	computer
☐		macOS	KG5K7TFQK5-MacBookPro	fe80:48ccafcc51b1bc9c	Apple	MacBook Pro	computer
☐		macOS	e77c9642-c43f-44d8-a60b-801c	10.0.1.1, 192.168.215.1, fe80	Apple	MacBook Pro	computer
☐		Windows Server 2008 R2 S...	INT-WINRM-W2008	10.41.48.66	VMware	Virtual Machine	computer
☐		Windows	LE-5MCTY-NUC.local	10.41.132.178, fe80:992277	Intel	NUC Mini PC	computer
☐		macOS 10.13	e1588cae-caeb-4215-a4bc-e161c	192.168.33.1	Apple	Apple Mac	computer
☐		macOS	Mac mini (Late 2018)	10.41.200.27	Apple	Mac mini (Late 2018)	computer
☐		macOS	9a1ed855-d7fc-473e-ad40-0ba7	10.41.132.162, fe80:845e4	Apple	MacBook Pro	computer
☐		macOS 10.15	Apple Mac	10.41.128.16, 10.41.128.23, 1	Apple	Apple Mac	computer
☐		macOS	WGWR5454M4-MacBookPro.lo	10.41.133.8, fe80:cc0aflaa	Apple	MacBook Pro M1 Pro (16") (2021)	computer

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

2. Select **Deployment settings** and configure the sensors to be deployed. For more details, see [Local UI \(on page 61\)](#).

3. Select the machine(s) to deploy Arc on, and choose from the available Arc deployment options.
4. If Guardian has not yet identified an [OS](#), you can use the **Advanced options** to manually specify the deployment scope via a query, and the deployment strategy.

Deploy Arc automatically from Guardian on Linux/macOS

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

Before you begin

- Credentials of the target machines are stored into the Credentials Manager
- An Administrator user is granted to access the target machine and to be used by Guardian in the process
- To deploy with [SSH](#) (Linux/macOS):
 - [SSH](#) is enabled locally and accepting incoming connections from the Guardian machine(s) used for deployment
 - Connectivity is granted for the services above, namely [TCP/22](#)

Procedure

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

Actions	Operating system	Name	IP	Vendor	Product name	Type
☐	macOS	MACBOOKPRO-DEFE	10.41.132.205, fe80:14ac2	Apple	MacBook Pro	computer
☐	macOS	TX6ST7Y73D-MacBookPro.local	10.41.132.157, fe80:3e:23f2	Apple	MacBook Pro	computer
☐	macOS	N6V4H90V4I-MacBookPro.local	10.41.132.183, fe80:89d2f	Apple	MacBook Pro	computer
☐	macOS	Gios-MBP.local	10.41.132.204, fe80:8e5b	Apple	MacBook Pro	computer
☐	Windows 10 / Server	LE-SIE-TIA-PRTL.local	172.16.16.241, 192.168.45.227	VMware	Virtual Machine	computer
☐	Windows 7	172.18.240.28	172.18.240.28			computer
☐	GNU/Linux	farm.plista.com		Seiko Epson Corporation	WorkForce WF-7710	printer_scanner
☐	Windows 7	172.18.98.26	172.18.98.26			computer
☐	macOS	YQQPVYK9PV-MacBookPro.local	10.41.132.208, fe80:3cda2	Apple	MacBook Pro	computer
☐	macOS 14.4.1	C3PH9735WQ-MacBook-Pro-16	fe80:a0a997fffe2a5f4e	Apple	MacBook Pro	computer
☐	macOS	C02ZF05ALVDM-MacBookPro.i	192.168.1.128, 192.168.45.8	Apple	MacBook Pro	computer
☐	macOS	KG5X7TFQK5-MacBookPro	fe80:48cccafcd5bcb9c	Apple	MacBook Pro	computer
☐	macOS	b77c9642-c43f-44d8-a60b-801c	10.0.1.1, 192.168.215.1, fe80	Apple	MacBook Pro	computer
☐	Windows Server 2008 R2 S...	INT-WINRM-W2008	10.41.48.66	VMware	Virtual Machine	computer
☐	Windows	LE-SMCTY-NUC.local	10.41.132.178, fe80:99227	Intel	NUC Mini PC	computer
☐	macOS 10.13	ef588cae-caeb-4215-a4bc-e61t	192.168.33.1	Apple	Apple Mac	computer
☐	macOS	Mac mini (Late 2018)	10.41.200.27	Apple	Mac mini (Late 2018)	computer
☐	macOS	9a1ed855-d7fc-473e-ad40-dba7	10.41.132.162, fe80:845e4	Apple	MacBook Pro	computer
☐	macOS 10.15	Apple Mac	10.41.128.16, 10.41.128.23, 1	Apple	Apple Mac	computer
☐	macOS	WGWRS454M4-MacBookPro.io	10.41.133.8, fe80:c0a7f1aa	Apple	MacBook Pro M1 Pro (16") (2021)	computer

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

2. Select **Deployment settings** and configure the sensors to be deployed. For more details, see [Local UI \(on page 61\)](#).
3. Select the machine(s) to deploy Arc on, and choose from the available Arc deployment options.
4. If Guardian has not yet identified an [OS](#), you can use the **Advanced options** to manually specify the deployment scope via a query, and the deployment strategy.

Deploy Arc with MDM (Windows)

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.

Make connections

Connect a deployed CMC, Guardian, Guardian Air or Arc sensor, and work with their data right here in Vantage.

My sensor is: **N2OS** **Arc** Guardian Air

Download the correct Arc bundle for your Operating System and Architecture.

Windows [386] (msi) Linux [amd64] (zip) macOS [amd64] (zip)
Windows [386] (zip) Linux [arm] (zip) macOS [arm64] (zip)
Windows [amd64] (msi) Linux [arm64] (zip)
Windows [amd64] (zip)

Sensor ID Your Sensor ID here

Next

3. In the **My sensor is:** section, click **Arc**.
4. Download the applicable package for your **OS** and architecture.

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**.

macOS - amd64 (Installer)
macOS - amd64 (Archive)
macOS - arm64 (Installer)
macOS - arm64 (Archive)
Linux - amd64 (Archive)
Linux - arm (Archive)
Linux - arm64 (Archive)
Windows 7+ - 386 (Installer)
Windows 7+ - 386 (Archive)
Windows 7+ - amd64 (Installer)
Windows 7+ - amd64 (Archive)
Windows 10+ - 386 (Installer)
Windows 10+ - 386 (Archive)
Windows 10+ - amd64 (Installer)
Windows 10+ - amd64 (Archive)

2. Download the applicable package for your [OS](#) and architecture.

**Note:**

When available, the [MSI](#) file is a user friendly option to install Arc. The archive file for Windows is still available to use for offline executions without installing Arc.

**Note:**

Two separate packages are available for Windows.

- For Windows 7 or later, but < 10, download the Windows7+ package
- For Windows 10 or later, download the Windows10+ 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 applicable package for your [OS](#) and architecture.

Result: The package downloads to your computer.

Deploy Arc to run in Service mode

MSI file configuration from a shell

A description of how to execute a Microsoft Software Installer (MSI) from a shell.

The [Microsoft Documentation](#) describes how to execute an [MSI](#) from a shell:

- Install Arc: `msiexec /i "arc.windows.amd64.msi" /L*v "installer.log"`
- Uninstall Arc: `msiexec /x "arc.windows.amd64.msi" /L*v "installer.log"`

To execute `msiexec` from PowerShell preserving arguments, use `--%`. For example:
`msiexec --% /i "arc.windows.amd64.msi" /L*v "installer.log"`

You can pass custom arguments to the setup installer by setting the `ARGS` property. For example: `msiexec /i "arc.windows.amd64.msi" /L*v "installer.log" ARGS="--mode=silent"`

MSI installer parameters

The following table describes all supported parameters for the Arc [MSI](#) installer.

Parameter	Valid values	Default	Description
<code>--mode</code>	<code>gui, silent</code>	<code>gui</code>	Select the setup mode.
<code>--acceptLicense</code>	<code>true, false</code>	<code>false</code>	Set the license as accepted. Mandatory for silent mode.
<code>--endpoint</code>	endpoint address	—	Set the connection endpoint.
<code>--token</code>	token string	—	Set the connection token.
<code>--verifyCertificate</code>	<code>true, false</code>	<code>false</code>	Enable validation of the upstream TLS certificate. Always enforced for Vantage. Uses the value from the <code>arc.json</code> configuration file if not set.
<code>--proxy</code>	<code>true, false</code>	<code>false</code>	Enable a web proxy for the upstream connection.
<code>--proxy-host</code>	proxy hostname or address	<code>' '</code> (empty)	Set the hostname or address of the proxy server.

Parameter	Valid values	Default	Description
<code>--proxyPort</code>	0–65535	—	Set the port used to connect to the proxy server.
<code>--installDeps</code>	<code>all</code> , <code>easefilter</code> , <code>npcap</code> , <code>pscorescriptblocklogging</code> , <code>psscriptblocklogging</code> , <code>usbpcap</code> , <code>sysmon</code>	<code>all</code>	Set the list of dependencies to install. Separate multiple values with a comma. Set all to install all dependencies.
<code>--uninstallDeps</code>	<code>all</code> , <code>easefilter</code> , <code>npcap</code> , <code>pscorescriptblocklogging</code> , <code>psscriptblocklogging</code> , <code>usbpcap</code> , <code>sysmon</code>	<code>''</code> (empty)	Set the list of dependencies to uninstall. Separate multiple values with a comma. Set all to uninstall all dependencies.
<code>--sysmonPath</code>	file path	—	Set the path to the sysmon.zip installer archive. If not set, Sysmon is downloaded from Guardian, Vantage, or Microsoft.
<code>--rebootIfRequired</code>	<code>true</code> , <code>false</code>	<code>true</code>	Reboot the system automatically if required.
<code>--createShortcutIcon</code>	<code>true</code> , <code>false</code>	<code>true</code>	Create a desktop shortcut icon.
<code>--startService</code>	<code>true</code> , <code>false</code>	<code>true</code>	Start the Arc service automatically after installation.
<code>--configFile</code>	file path	—	Specify an arc.json file to use for configuration.
<code>--removeLogs</code>	<code>true</code> , <code>false</code>	—	Remove Arc logs during cleanup.

Parameter	Valid values	Default	Description
<code>--preserveConfig</code>	true, false	—	Preserve the <code>arc.json</code> configuration during uninstallation.

Deploy Arc with Microsoft Intune

Upload an Arc package to Microsoft Intune

If you manage your network with mobile device management (MDM), you can use it to deploy Arc.

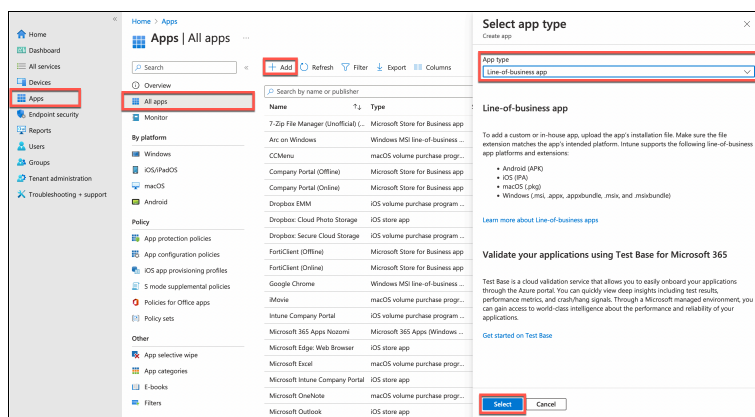
Before you begin

Before you do this procedure, make sure that you have:

- Downloaded the correct Arc package for your [OS](#)
- Compiled the [MSI](#) file

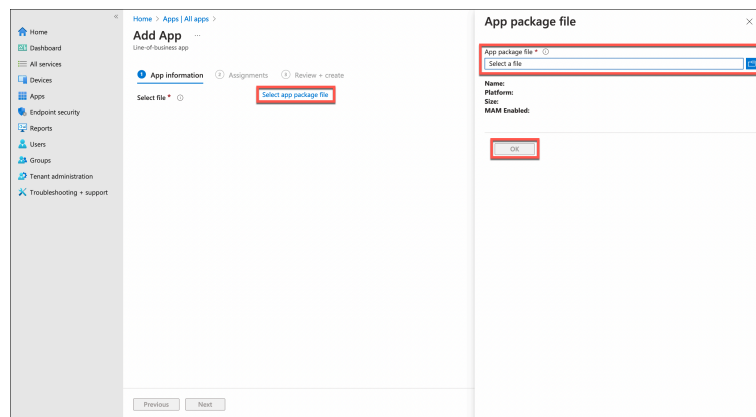
Procedure

1. In Microsoft Intune, go to **Apps > All apps**.
2. Select **Add**.
3. In the **Select app type** section on the right side, open the **App type** dropdown. Select **Line-of-business app**.
4. Select the **Select** button.



5. In the **Add App** section, select **Select app package file**.
6. In the **App package file** section on the right side, open the **App package file** dropdown. Select the Arc package file from the folder on your computer.

7. Select **OK**.



8. Go to **Apps > All apps**.

9. In the search bar on the right side, enter the first part of the name of the package that you just uploaded, and select **Enter**.

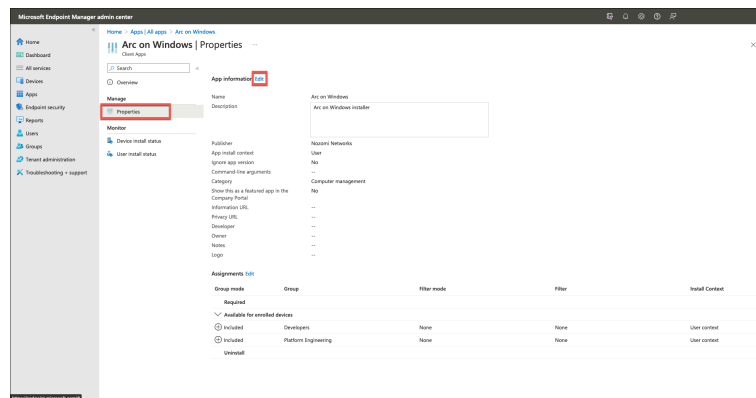
10. Select the name of the correct file.

Result: The details for the app show.

11. Select **Properties**.

Result: The information for the app shows on the right.

12. To the right of the **App information** title, select **Edit**.



13. Enter the information as necessary.

**Note:**

Because this information will show in the system later, Nozomi Networks recommends that you enter as much useful information as possible.

14. If you want to assign a logo to the Arc app, go to the right of **Logo**, and select **Select image**.

15. In the **Logo** section on the right side, open the **Select a file** dropdown, and select the applicable file.

16. When you have added all the information, select **Review + save**.

Assign an Arc package with Microsoft Intune

Once you have uploaded the Arc package, you need to assign it to designated groups or computers for deployment.

Before you begin

Before you can assign an Arc package, you must [Upload an Arc package to Microsoft Intune \(on page 125\)](#).

About this task

You can assign the Arc package with one of these options:

- **Required** - Installed automatically on enrolled devices.
- **Available for enrolled devices** - Made available in the **Company Portal** app for users to optionally install.

Procedure

1. Go to **Apps > All apps**.
2. Search for the Arc on Windows application.

**Note:**

The name will depend on what was assigned previously.

3. Select **Properties**.
4. To the right of the **Assignments** title, select **Edit**.

Result: The **Assignments** tab shows.

5. Select the **Required** section, and/or the **Available for enrolled devices** section as applicable.
6. Select the group, users or devices, as necessary.

**Note:**

You can select from:

- **Add group**
- **Add all users**
- **Add all devices (Required section only)**

7. Select **Review + save**.

Result: If you selected the **Required** option, no further action is necessary.

8. If you selected the **Available for enrolled devices** option, continue with the steps that follow.
9. In the [OS](#) of your device, open the local application **Company Portal**.

10. In the search bar, enter the name of the Arc package and select **Enter**.

Result: The Arc package shows.

11. Select the **Install** button.

Result: The Arc package is now installed.

Deploy Arc with Microsoft Endpoint Configuration Manager

If you manage your network with Microsoft Endpoint Manager, you can use it to deploy Arc.

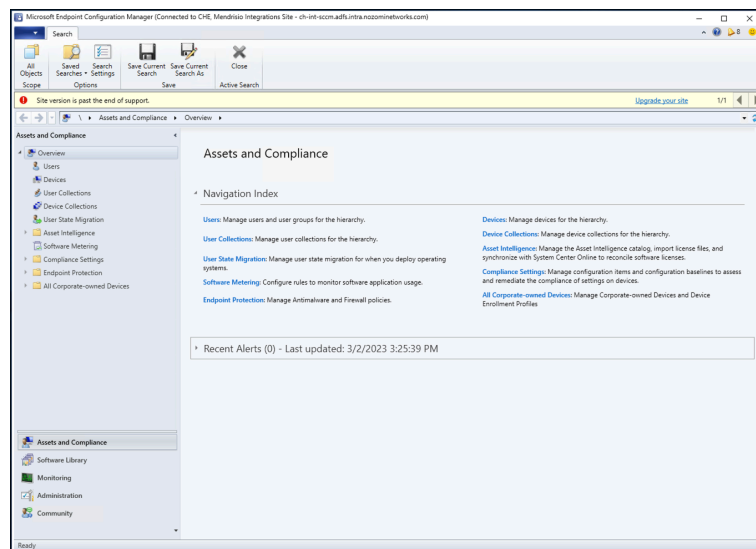
Before you begin

Before you do this procedure, make sure that you have:

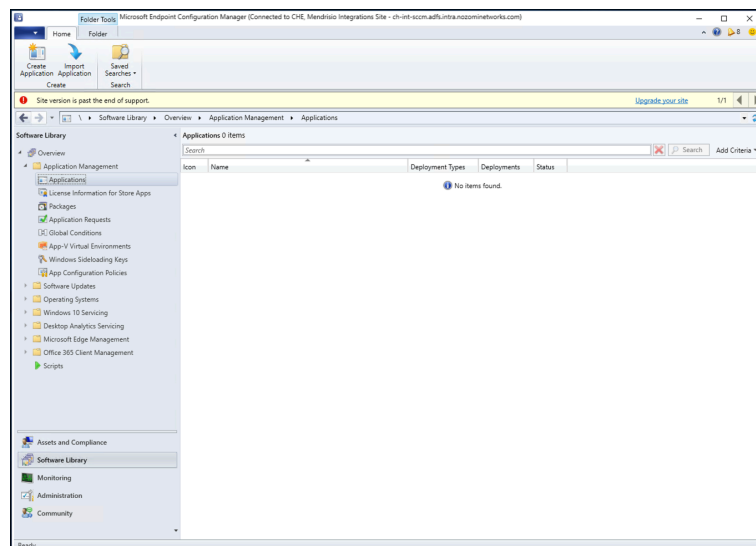
- Downloaded the correct Arc package for your [OS](#)
- Compiled the [MSI](#) file

Procedure

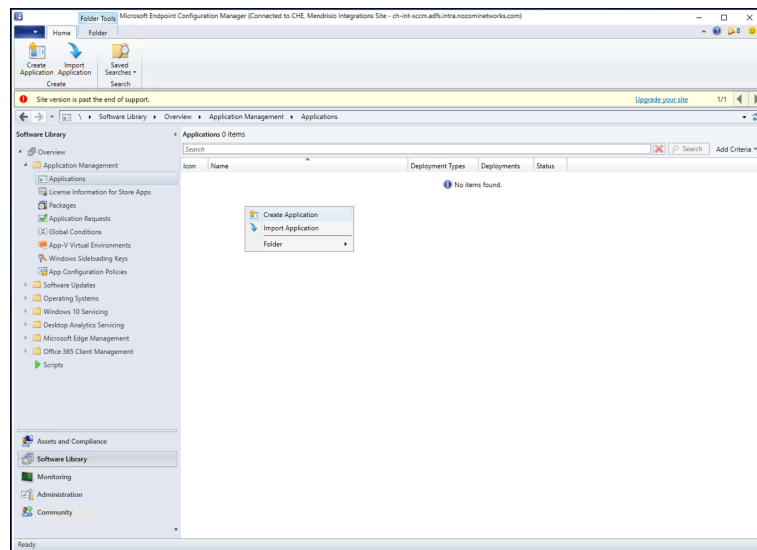
1. Open Microsoft Endpoint Configuration Manager.



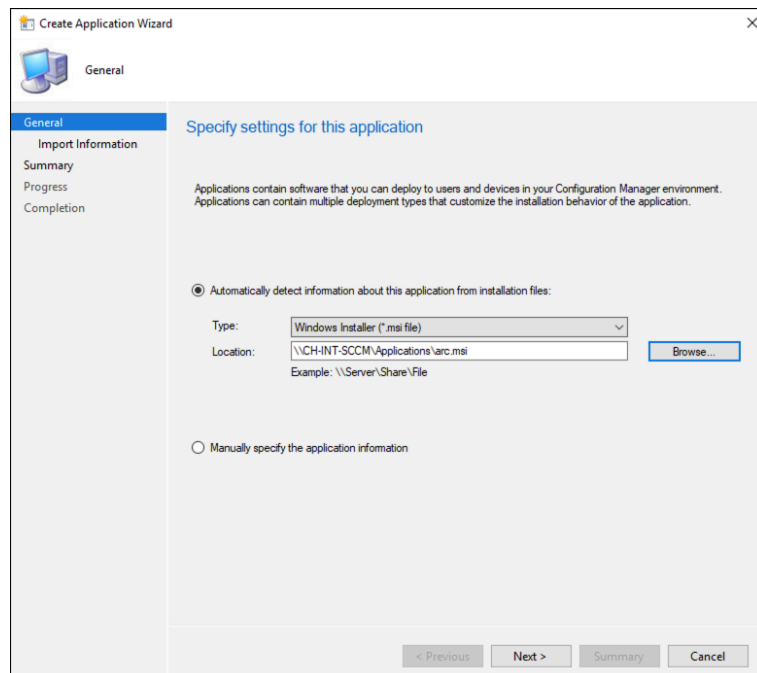
2. Go to **Software Library > Overview > Application Management > Applications**.



3. Right-click and select **Create Application**.

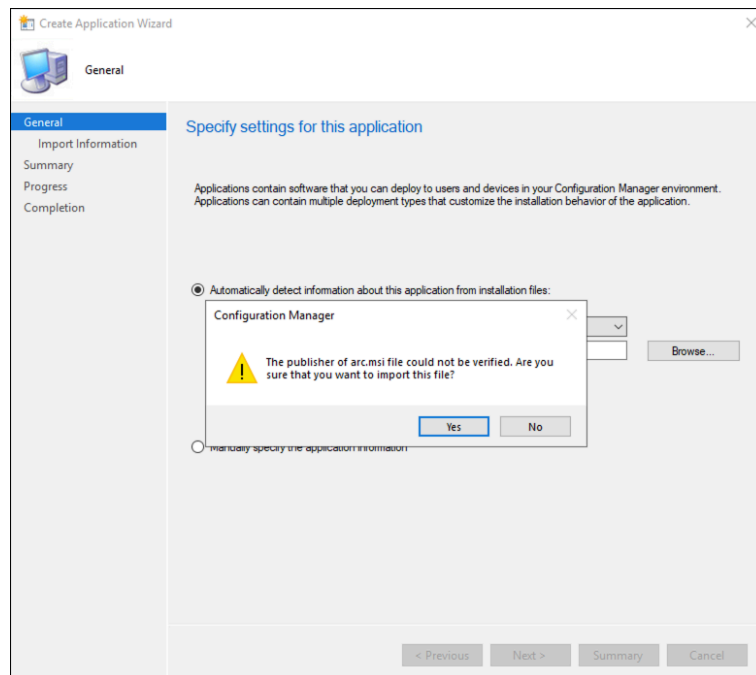


4. Browse and select the location of the *MSI* file, and then select **Next**.

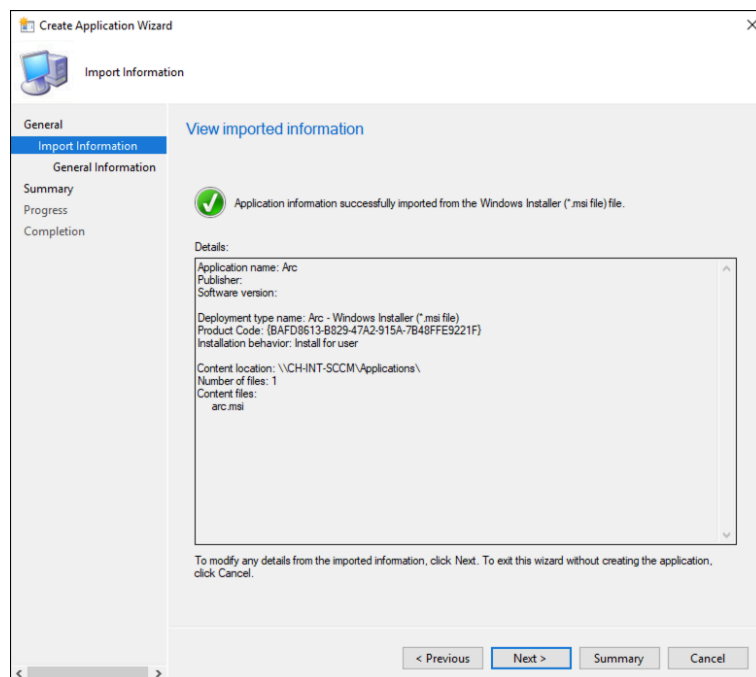


Result: A dialog shows.

5. To confirm the import of the package, select **Yes**.



6. Make sure that the file has been imported successfully, and then select **Next**.



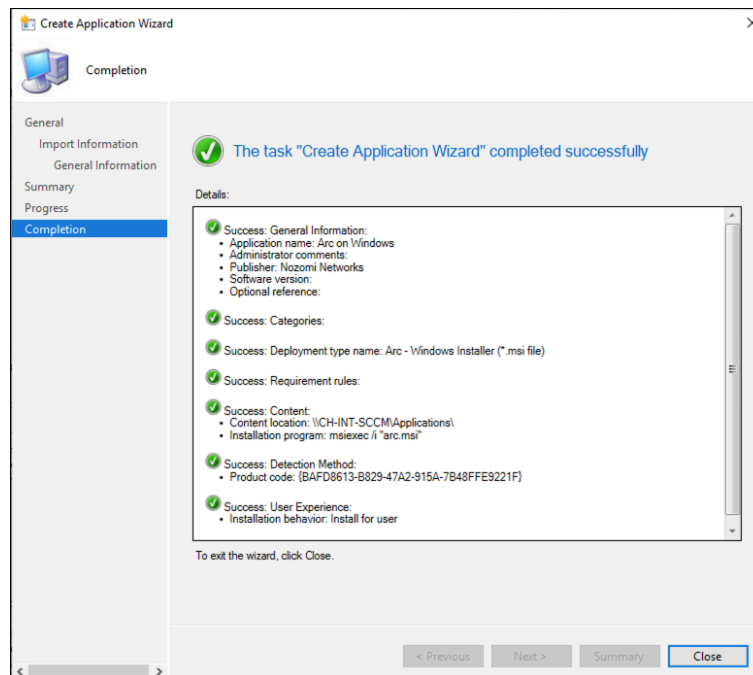
7. On the **General Information** page, enter details in the fields as necessary. Select **Next**.

The screenshot shows the 'Create Application Wizard' window, specifically the 'General Information' page. The left sidebar contains a tree view with 'General Information' selected. The main area is titled 'Specify information about this application'. It contains several input fields: 'Name' (filled with 'Arc on Windows'), 'Administrator comments' (empty), 'Publisher' (filled with 'Nozomi Networks'), 'Software version' (empty), 'Optional reference' (empty), and 'Administrative categories' (empty with a 'Select...' button). Below these is a section 'Specify the installation program for this application and the required installation rights.' with an 'Installation program' field (filled with 'msiexec /i "arc.msi"' and a 'Browse...' button), a checkbox 'Run installation program as 32-bit process on 64-bit clients.' (unchecked), and an 'Install behavior' dropdown (set to 'Install for user'). At the bottom are navigation buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

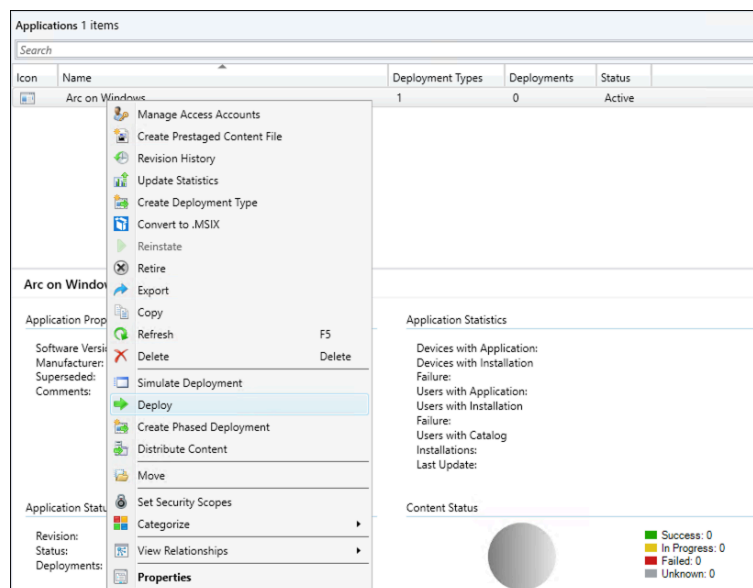
8. Review the settings, and then select **Next**.

The screenshot shows the 'Create Application Wizard' window, specifically the 'Summary' page. The left sidebar contains a tree view with 'Summary' selected. The main area is titled 'Confirm the settings for this application'. It contains a 'Details' section with a list of settings: 'General Information' (Application name: Arc on Windows, Administrator comments, Publisher: Nozomi Networks, Software version, Optional reference), 'Categories' (Deployment type name: Arc - Windows Installer (*.msi file)), 'Requirement rules', 'Content' (Content location: \\CH-INT-SCCMApplications\, Installation program: msiexec /i "arc.msi"), 'Detection Method' (Product code: {BAFD8613-B829-47A2-915A-7B48FFE9221F}), and 'User Experience' (Installation behavior: Install for user). Below the details is a note: 'To change these settings, click Previous. To apply the settings, click Next.' At the bottom are navigation buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

9. Make sure that the application has been created successfully, and then select **Close**.



10. Right-click on the application and select **Deploy**.



Result: The **Deploy Software Wizard** shows.

11. On the **General** page, open the **Collection** dropdown and choose the type of deployment. Select **Next**.

The screenshot shows the 'Deploy Software Wizard' window, specifically the 'General' tab. The left sidebar lists the steps: General, Content, Deployment Settings, Scheduling, User Experience, Alerts, Summary, Progress, and Completion. The main area is titled 'Specify general information for this deployment'. It contains two dropdown menus: 'Software' with 'Arc on Windows' selected and 'Collection' with 'All Users' selected. Both have 'Browse...' buttons to the right. Below these are two checkboxes: 'Use default distribution point groups associated to this collection' (unchecked) and 'Automatically distribute content for dependencies' (checked). At the bottom is a large text area for 'Comments (optional)'. Navigation buttons at the bottom right include '< Previous', 'Next >', 'Summary', and 'Cancel'.

12. On the **Content** page, open the **Add** dropdown and select the type of distribution. Select **Next**.

The screenshot shows the 'Deploy Software Wizard' window, specifically the 'Content' tab. The left sidebar highlights 'Content'. The main area is titled 'Specify the content destination'. It features a table with columns 'Name' and 'Type' and a message 'There are no items to show in this view.' Below this is a section for 'Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:'. This section contains a table with columns 'Name', 'Description', and 'Associations', also with a 'There are no items to show in this view.' message. To the right of this table is an 'Add' dropdown menu, which is open, showing 'Distribution Point' and 'Distribution Point Group' as options. Navigation buttons at the bottom right include '< Previous', 'Next >', 'Summary', and 'Cancel'.

13. Make sure that the distribution point shows in the list, and select **Next**.

The screenshot shows the 'Content' page of the 'Deploy Software Wizard'. The left sidebar has 'Content' selected. The main area is titled 'Specify the content destination'. It contains a table with columns 'Name' and 'Type'. Below the table, there is a section for 'Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:'. This section includes a search filter, an 'Add' button, and a table with columns 'Name', 'Description', and 'Assoc'. The table contains one entry: 'CH-INT-SCCM.ADFS.INTRA.NOZOMINETWORKS.C...' with the description 'Distribution point'. At the bottom, there are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

Name	Type
There are no items to show in this view.	

Name	Description	Assoc
CH-INT-SCCM.ADFS.INTRA.NOZOMINETWORKS.C...	Distribution point	

14. On the **Deployment Settings** page, open the **Purpose** dropdown and select **Required**. Select **Next**.

The screenshot shows the 'Deployment Settings' page of the 'Deploy Software Wizard'. The left sidebar has 'Deployment Settings' selected. The main area is titled 'Specify settings to control how this software is deployed'. It contains two dropdown menus: 'Action' (set to 'Install') and 'Purpose' (set to 'Required'). Below these are four checkboxes: 'Allow end users to attempt to repair this application', 'Pre-deploy software to the user's primary device', 'Send wake-up packets', and 'Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs'. At the bottom, there are buttons for '< Previous', 'Next >', 'Summary', and 'Cancel'.

Action:

Purpose:

☐ Allow end users to attempt to repair this application

☐ Pre-deploy software to the user's primary device

☐ Send wake-up packets

☐ Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

15. On the **Scheduling** page, set the desired schedule settings, and then select **Next**.

The screenshot shows the 'Deploy Software Wizard' window with the 'Scheduling' tab selected in the left-hand navigation pane. The main area is titled 'Specify the schedule for this deployment'. It contains a text block explaining that the application will be available as soon as it is distributed to the content server(s) unless it is scheduled for a later time. Below this, there are two main sections: 'Time based on:' with a dropdown menu set to 'UTC', and 'Schedule the application to be available at:' with a date and time picker set to '3/ 2/2023' and '2:31 PM'. There is also an 'Installation deadline:' section with two radio button options: 'As soon as possible after the available time' (which is selected) and 'Schedule at:' with a date and time picker set to '3/ 2/2023' and '2:31 PM'. At the bottom of the main area, there is a checkbox for 'Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.' The bottom of the window has four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

16. On the **User Experience** page, select the desired settings, and then select **Next**.

The screenshot shows the 'Deploy Software Wizard' window with the 'User Experience' tab selected in the left-hand navigation pane. The main area is titled 'Specify the user experience for the installation of this software on the selected devices'. It contains a text block explaining that the user experience setting for this deployment is specified. Below this, there are several sections: 'User notifications:' with a dropdown menu set to 'Display in Software Center and show all notifications', a checkbox for 'When software changes are required, show a dialog window to the user instead of a toast notification', and a section titled 'When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:' with two checkboxes: 'Software Installation' and 'System restart (if required to complete the installation)'. There is also a section titled 'Write filter handling for Windows Embedded devices' with a checkbox for 'Commit changes at deadline or during a maintenance window (requires restarts)'. Below this, there is a note: 'If this option is not selected, content will be applied on the overlay and committed later.' The bottom of the window has four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

17. On the **Alerts** page, select the desired settings, and then select **Next**.

Deploy Software Wizard

Alerts

Specify Configuration Manager and Operations Manager alert options

Configuration Manager generates alerts when this application is deployed.

Threshold for successful deployment

☐ Create a deployment alert when the threshold is lower than the following:

Percent success: 1

After: 3/9/2023 3:31 PM

Threshold for failed deployment

☐ Create a deployment alert when the threshold is higher than the following:

Percent failure: 0

Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.

☐ Enable System Center Operations Manager maintenance mode

☐ Generate System Center Operations Manager alert when a software installation fails

< Previous **Next >** Summary Cancel

18. On the **Summary** page, review the settings.

Deploy Software Wizard

Summary

Confirm the settings for this new deployment

Details:

- General**
 - Software: Arc on Windows
 - Collection: All Users (Member Count: 6)
 - Use default distribution point groups associated to this collection: Disabled
 - Automatically distribute content for dependencies: Enabled
- Deployment Settings**
 - Action: Install
 - Purpose: Required
 - Allow end users to attempt to repair this application: Disabled
 - Pre-deploy software to the user's primary device: Disabled
 - Send wake-up packets: Disabled
 - Allow clients to use a metered Internet connection to download content: Disabled
- Application Settings (retrieved from application in software library)**
 - Application Name: Arc on Windows
 - Application Version:
 - Application Deployment Types: Windows Installer (*.msi file)
- Scheduling**
 - Time based on: UTC
 - Available Time: As soon as possible
 - Deadline Time: Disabled
 - Delayed enforcement on deployment: Disabled
- User Experience**
 - User notifications: Display in Software Center and show all notifications
 - Ignore Maintenance Windows: Disabled
 - When software changes are required, show a dialog window to the user instead of a toast notification: Disabled

To change these settings, click Previous. To apply the settings, click Next.

< Previous **Next >** Summary Cancel

19. If the settings are correct, select **Next** to start the deployment.

Results

The deployment starts.

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.

Make connections

Connect a deployed CMC, Guardian, Guardian Air or Arc sensor, and work with their data right here in Vantage.

My sensor is: **N2OS** **Arc** **Guardian Air**

Download the correct Arc bundle for your Operating System and Architecture.

Windows [386] (msi) Linux [amd64] (zip) macOS [amd64] (zip)
Windows [386] (zip) Linux [arm] (zip) macOS [arm64] (zip)
Windows [amd64] (msi) Linux [arm64] (zip)
Windows [amd64] (zip)

Sensor ID Your Sensor ID here

Next

3. In the **My sensor is:** section, click **Arc**.
4. Download the applicable package for your **OS** and architecture.

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**.

macOS - amd64 (Installer)
macOS - amd64 (Archive)
macOS - arm64 (Installer)
macOS - arm64 (Archive)
Linux - amd64 (Archive)
Linux - arm (Archive)
Linux - arm64 (Archive)
Windows 7+ - 386 (Installer)
Windows 7+ - 386 (Archive)
Windows 7+ - amd64 (Installer)
Windows 7+ - amd64 (Archive)
Windows 10+ - 386 (Installer)
Windows 10+ - 386 (Archive)
Windows 10+ - amd64 (Installer)
Windows 10+ - amd64 (Archive)

2. Download the applicable package for your [OS](#) and architecture.

**Note:**

When available, the [MSI](#) file is a user friendly option to install Arc. The archive file for Windows is still available to use for offline executions without installing Arc.

**Note:**

Two separate packages are available for Windows.

- For Windows 7 or later, but < 10, download the Windows7+ package
- For Windows 10 or later, download the Windows10+ 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 applicable package for your OS and architecture.

Result: The package downloads to your computer.

Deploy Arc to run in Service mode

Windows

Install Arc with Microsoft Software Installer (MSI)

You can manually deploy Arc to run in Service mode.

Procedure

1. Double-click the [ZIP](#) file to extract these files:
 - An [MSI](#) file
 - A [batch file \(.bat\)](#)
2. To install Arc, choose from one of these options:

Choose from:

- Double-click the [MSI](#) file
- Run the [.bat](#)



Note:

The [.bat](#) will pre-fill the [MSI](#) with the parameters that you have set in the **Configuration** page.



Note:

When you try to install Arc on a Windows machine that does not have OpenGL, the installation will fail. When this happens, this error message will show:

There is a problem with this Windows Installer package...

If this happens, do step [3 \(on page 142\)](#) below.

3. If you received the error message above, in a PowerShell, enter these commands:

```
$global:ProgressPreference = "SilentlyContinue"

$params = '/i', 'arc.windows.amd64.msi', '/QN', '/L*v',
'installer.log', 'ARGS="--mode=silent --acceptLicense=true
--endpoint=test.endpoint --token=test.token
--rebootIfRequired=false"'

Start-Process 'msiexec.exe' -ArgumentList $params -NoNewWindow -Wait
-PassThru
```

4. Wait for the **User Account Control** dialog to show.
5. Select **Yes**.

Result: The **Arc setup wizard** shows.

6. Follow the steps in the wizard.

Results

The installer:

- Starts a new installation process if Arc is not installed, or if a previous version is detected
- Starts a modify installation process, if the same version of Arc is detected

Related information

MSI file configuration from a shell (on page 122)

Linux

Deploy Arc manually in Service mode with a local UI

You can manually deploy Arc to run in Service mode with a local user interface (UI).

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Go to `/usr/local/sbin` and create a folder called `arc`
3. [Open the local UI \(on page 107\)](#).
4. In the **Configuration** page of the local [UI](#), set these parameters:
 - a. **Upstream connection:** This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - b. **Token:** This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - c. **Execution options:** Tune these options as necessary.
5. Select **Install**.

Result: The **Service status** changes from **Not installed** to **Stopped**.

6. Select **Run**.

Result: The **Execution status** changes from **Stopped** to **Running as service**. The **Connectivity status** changes from **Disconnected** to **Connected**.

Results

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

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.



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. 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.

macOS

Deploy Arc manually in Service mode on macOS

You can manually deploy Arc to run in Service mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Choose a folder where you will copy the folder containing the Arc files.
3. To install Arc, run the [package file \(.pkg\)](#) file.

Result: A dialog shows.

4. Follow the steps on screen.

When you connect the Arc sensor to Vantage, you should start the **Add Sensor** procedure from Vantage to be able to connect it.

Results

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

Deploy Arc to run in One-shot or Offline mode

Windows

Deploy Arc manually with a local UI

You can manually deploy Arc to run in One-shot or Offline mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Go to `C:\Program Files\` and create a folder called `NozomiNetworks\Arc`
3. [Open the local UI \(on page 107\)](#).
4. Choose a mode:
Choose from:
 - For One-shot mode, in the **Status** page of the local configuration [UI](#), select the **One-shot** checkbox.
 - For Offline mode, in the **Status** page of the local configuration [UI](#), select the **Offline** checkbox.
5. In the **Configuration** page of the local configuration [UI](#), set these parameters:
 - a. **Upstream connection** (One-shot only): This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - b. **Token** (One-shot only): This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary. Take the value shown in the image above.
 - c. **Execution options**: Tune these options as necessary.
6. Select **Run**.

One-shot mode only: When you connect the Arc sensor to Vantage, you should start the **Add Sensor** procedure from Vantage to be able to connect it.

**Note:**

A counter will show the execution time that remains.

Results

The Arc sensor is now running from `C:\Program Files\NozomiNetworks\Arc` and you can view collected data in Guardian or Vantage.

Linux

Deploy Arc manually in One-shot mode with a local UI

You can manually deploy Arc to run in One-shot mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Go to `/usr/local/sbin` and create a folder called **arc**
3. [Open the local UI \(on page 107\)](#).
4. In the **Configuration** page of the local [UI](#), set these parameters:
 - a. **Upstream connection**: This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - b. **Token**: This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - c. **Execution options**: Tune these options as necessary.
5. In the **Execution Info** page of the local [UI](#), select the **One-shot** checkbox.
6. Select **Run**.

When you connect the Arc sensor to Vantage, you should start the **Add Sensor** procedure from Vantage to be able to connect it.

**Note:**

A counter will show the execution time that remains.

Results

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

Deploy Arc manually in Offline mode with a local UI

You can manually deploy Arc to run in Offline mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Go to `/usr/local/sbin` and create a folder called **arc**
3. [Open the local UI \(on page 107\)](#).
4. In the **Configuration** page of the local [UI](#), configure the **Execution options** as necessary.
5. In the **Execution Info** page of the local [UI](#), select the **Offline** checkbox.
6. Select **Run**.

**Note:**

A counter will show the execution time that remains.

7. Wait for the execution to finish.
8. Import the generated offline archive into Guardian or Vantage.

Results

You can now view the collected data in Guardian or Vantage.

Deploy Arc manually in One-shot mode without a local UI

You can manually deploy Arc in One-shot 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 host.
2. If the folder `/usr/local/sbin` does not exist, create it.
3. Copy the Arc [ZIP](#) package into the folder `/usr/local/sbin/arc`
4. Extract the [ZIP](#) package.
5. Enter this command: `./arc-linux-arm oneshot`

Results

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

Deploy Arc manually in Offline mode without a local UI

You can manually deploy Arc in Offline 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 host.
2. If the folder `/usr/local/sbin` does not exist, create it.
3. Copy the Arc [ZIP](#) package into the folder `/usr/local/sbin/arc`
4. Extract the [ZIP](#) package.
5. Enter this command: `./arc-linux-arm offline`
6. Wait for the execution to finish.
7. Import the generated offline archive into Guardian or Vantage.

Results

You can now view the collected data in Guardian or Vantage.

macOS

Deploy Arc manually in One-shot mode with a local UI

You can manually deploy Arc to run in One-shot mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Choose a folder where you will copy the folder containing the Arc files.

**Note:**

On macOS, due to security protection, do not put the Arc folder on the **Desktop**, or in the **Downloads** folder. Choose a folder like: `/Users/<user_name>`

3. [Open the local UI \(on page 107\)](#).
4. In the **Configuration** page of the local [UI](#), set these parameters:
 - a. **Upstream connection:** This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - b. **Token:** This is automatically populated with the Guardian instance that you used to download the package. Change this only if it is necessary.
 - c. **Execution options:** Tune these options as necessary.
5. In the **Execution Info** page of the local [UI](#), select the **One-shot** checkbox.
6. Select **Run**.

When you connect the Arc sensor to Vantage, you should start the **Add Sensor** procedure from Vantage to be able to connect it.

**Note:**

A counter will show the execution time that remains.

Results

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

Deploy Arc manually in Offline mode with a local UI

You can manually deploy Arc to run in Offline mode.

Before you begin

Make sure that you have downloaded an Arc package.

Procedure

1. Use an administrator account to extract the [ZIP](#) file to your machine.
2. Choose a folder where you will copy the folder containing the Arc files.

**Note:**

On macOS, due to security protection, do not put the Arc folder on the **Desktop**, or in the **Downloads** folder. Choose a folder like: `/Users/<user_name>`

3. [Open the local UI \(on page 107\)](#).
4. In the **Configuration** page of the local [UI](#), configure the **Execution options** as necessary.
5. In the **Execution Info** page of the local [UI](#), select the **Offline** checkbox.
6. Select **Run**.

**Note:**

A counter will show the execution time that remains.

7. Wait for the execution to finish.
8. Import the generated offline archive into Guardian or Vantage.

Results

You can now view the 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 10. 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 11. Elastic notification values - virtual sensors

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

Table 11. 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

One-shot mode

In this mode, Arc runs as a portable application, that collects the data in a single execution. After it has been executed, you can then delete it from the target machine.

This mode is recommended for:

- Users who cannot run Arc continuously due to compliance reasons
- Networks where Arc can be granted connectivity to Guardian, or Vantage

Offline mode

In this mode, Arc runs as a portable application, and it is not installed on the target machine. This mode is similar to One-shot mode because Arc is used for a single execution, but the data is collected locally and then exported in an archive file from the machine. The archive file can then be manually imported into Guardian or Vantage.

When Arc runs in Offline mode, a Smart Polling license is automatically granted. Because it is not possible to define Smart Polling plans in Arc, only the devices that Discovery identifies are polled.

Chapter 7. Troubleshooting



Sigma rule alerts do not show

Possible cause

[Sysmon](#) has not been installed.



Note:

If [Sysmon](#) is installed and working correctly:

- You can use the Windows **Event Viewer** to view Sysmon-generated events. (You can find these in: **Applications and Services Logs > Microsoft > Windows > Sysmon > Operational**.)
- You should get a message similar to this in the log file:

```
... Sysmon Event Generator | Events added 45, events  
discarded 0, in 1715 ms
```

Procedure

1. Download and install [Sysmon](#).
2. Restart Arc to make sure that [Sysmon](#) is active.
3. Make sure that **Sigma rules** is enabled in the local configuration [UI](#).

Possible cause

You do not have **Sigma rules** enabled in the local configuration [UI](#).

Procedure

1. [Open the local UI \(on page 107\)](#).
2. Select **Configuration**.
Result: The **Configuration** page opens.
3. Select the **Sigma rules** checkbox.
4. Select **Save**.
5. Check to see if Sigma rule alerts now show.

Possible cause

You have [Sysmon](#) installed and enabled, but you do not get a message similar to this in the log file:

```
... Matcher for EventID 1 | Matches found 1, in 0 ms
```

Procedure

**Note:**

This is not an error. It means that an event that would trigger an alert has not been detected yet.

Wait for Arc to show an alert that is based on Sigma rules.

Possible cause

You have [Sysmon](#) installed and enabled, but you do not get a message similar to this in the log file:

```
... Matcher for EventID 1 | Sending 1 alert rules 200 OK
```

Procedure

**Note:**

This can mean that the host was too busy to communicate.

**Note:**

If a different result than 200 (204 on Vantage) is obtained, then the alert might have been produced, but there was a communication failure when it was sent to Guardian.

Wait for Arc to make another attempt to communicate with the host.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Traffic monitoring does not work

Possible cause

[Npcap](#) is not installed.



Note:

If [Npcap](#) is installed, and traffic monitoring is enabled in the local configuration [UI](#), you should get a message similar to this in the log file:

```
LiveCapture(\Device\NPF_{5CFC7BFE}) | Setting filter not (host
10.41.43.129 and port 443)
LiveCapture(\Device\NPF_{026414DD}) | Capture completed after
sniffing 2000 packets, 208675 bytes
LiveCapture(\Device\NPF_{026414DD}) | Sending packets: 200 OK
```

Procedure

1. Download and install [Npcap](#).
2. Restart Arc to make sure that [Npcap](#) is active.
3. Make sure that **Traffic monitoring** is enabled in the local configuration [UI](#).

Possible cause

You do not have **Traffic monitoring** enabled in the local configuration [UI](#).

Procedure

1. [Open the local UI \(on page 107\)](#).
2. Select **Configuration**.
Result: The **Configuration** page opens.
3. Select the **Traffic monitoring** checkbox.
4. Select **Save**.
5. Check to see if traffic monitoring now works.

If none of the previous solutions work, please contact our [Customer Support](#) team.

USB detections do not work

Possible cause

[USBPcap](#) is not installed.



Note:

If [USBPcap](#) is installed, and **USB detections** is enabled, in the local configuration [UI](#), you should get a message similar to this in the log file:

```
... 10 total usb detections
... 10 usb alerts to send
... Sent 10 usb alerts 200 OK
```

Procedure

1. Download and install [USBPcap](#).
2. Restart Arc to make sure that [USBPcap](#) is active.
3. Make sure that **USB detections** is enabled in the local [UI](#).

Possible cause

You do not have **USB detections** enabled in the local [UI](#).

Procedure

1. [Open the local UI \(on page 107\)](#).
2. Select **Configuration**.
Result: The **Configuration** page opens.
3. Select the **USB detections** checkbox.
4. Select **Save**.
5. Check to see if the [USB](#) detection feature now works.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Arc does not update to the latest version

Possible cause

Guardian only: The expected version has not been imported into Guardian.

Procedure

1. In the Web UI, go to  > **System** > **Updates & Licenses**.
2. [Import Arc through the update service in Guardian or CMC \(on page 45\)](#).
3. Alternatively, [Import Arc through a manual contents upload in Guardian or CMC \(on page 46\)](#).

Possible cause

Guardian only: The Arc sensor has not been allowed in the Guardian.

Procedure

1. The Arc sensor is not accessible as it is being used by another process.
2. Find and select the applicable Arc sensor.
3. In the top-right corner of the Web UI, click the  icon.

Result: The icon changes to  and the sensor is now allowed.

Possible cause

The Arc sensor is not accessible as it is being used by another process.



Note:

If this is the case, you will see a message similar to this in the update.log file:

```
04/13/2023 10:19:56 The process cannot access the file
'C:\Users\Nozomier\arc\arc-windows-amd64.exe' because it is
being used by another process.
```

Procedure

1. Close the local [UI](#).
2. If Arc is running in One-shot or Offline mode, wait for it to finish.
3. In the top-left corner of the **Sensors** page, click the  icon to force the update.

If none of the previous solutions work, please contact our [Customer Support](#) team.

Log files

Log files are produced to help you with troubleshooting. The Arc installation method, and the execution mode, will affect the name and location of the logs files.

Location

On Linux, the install location is: `/usr/local/sbin/arc.linux.[architecture]/logs`

On macOS, the install location is:

`/usr/local/sbin/arc.darwin.[architecture]/logs`

On Windows, the install location is: `C:\Program Files\NozomiNetworks\Arc\logs`

If Arc is run from a different directory, for example in Offline or One-shot mode, the log folder is always created in the same location as the Arc executable.

Log name

When the log file is created in Service mode, the log file will have the name:

`arc_service.log.txt`

When the log file is created in One-shot or Offline mode, the log file will have the name:

`arc.log.txt`

Additional log files are also produced:

- `setup.log`: covers Arc's initialization process, before the Arc configuration has been loaded and applied
- `sp.log.txt`: covers Smart Polling activity
- `compliance_scc.log.txt`: covers Compliance scan activity

Verbosity

The configured log level applies to these log files (including their archived, numbered versions):

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

It doesn't apply to `setup.log`

`compliance_scc.log.txt` is different: it is written only when the log level is set to **Debug**, and produces no output at any other level.

`setup.log` covers Arc's initialization process, which happens before the Arc configuration is loaded and applied. For this reason, very few log lines might be logged in **Info** mode before Arc is able to load and apply the configuration.

For more details about the log level setting, see [Other \(on page 72\)](#).

Limits

The maximum file size of a log is 10 MB. Once this limit is reached, the log file is archived with a numerical suffix, such as `arc.log.txt.1`

This will continue up to `arc.log.txt.9`

After this, rotation is applied, and the `.1` suffix is used again. A maximum of nine archived logs are retained.



Glossary



.pkg

A .pkg file is a package file used on macOS to distribute and install software, containing all files needed for installation and scripts to guide the process.

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.

Application Programming Interface

An API is a software interface that lets two or more computer programs communicate with each other.

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.

Batch file

A batch file is a script file containing a series of commands executed by a command-line interpreter, typically on Windows. It automates routine tasks and manages system operations, stored with a .bat or .cmd extension.

Berkeley Packet Filter

The BPF is a technology that is used in some computer operating systems for programs that need to analyze network traffic. A BPF provides a raw interface to data link layers, permitting raw link-layer packets to be sent and received.

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.

Classless Inter-Domain Routing

CIDR is a method for IP routing and for allocating IP addresses.

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.

Desktop Window Manager

DWM is a Windows service that enables visual effects on the desktop, such as transparent windows and 3D window transitions.

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.

Dynamic Link Library

A DLL is a Microsoft Windows system file that contains code, data, and resources used by multiple programs simultaneously. It enables code sharing and reuse, enhancing efficiency and reducing software size by allowing on-demand code execution.

EaseFilter

EaseFilter is a software library that provides file system filter driver solutions for real-time file monitoring, control, and encryption. It enables developers to intercept, inspect, or block file I/O operations in Windows environments.

Event Tracing for Windows

ETW is a Microsoft Windows kernel-level logging mechanism that lets applications and the operating system record and consume events in real time, without the overhead of writing to a debugger or log file.

Extensible Configuration Checklist Description Format

XCCDF is an XML-based specification, part of SCAP, for authoring security checklists, benchmarks, and related configuration documentation in a structured, automatable form.

Extensible Markup Language

XML is a markup language and file format for the storage and transmission of data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

File Allocation Table

FAT is a file system architecture used in computers for managing disk space. It maintains a table to track the allocation of files on a disk, supporting efficient data storage, access, and management

Gigabyte

The gigabyte is a multiple of the unit byte for digital information. One gigabyte is one billion bytes.

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.

Knowledge Base

A Microsoft knowledge base article provides information about a software update, hotfix, or security patch, identified by a unique article number prefixed with KB.

Libpcap

Libpcap is a portable C/C++ library for network traffic capture that provides a common interface across various OS-specific backends like BPF, netfilter, packet filter, netfilter, and NPF.

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.

Microsoft Software Installer

MSI files are database files used by the Microsoft Software Installer (MSI). The files contain information about an application, which is divided into features and components, such as shortcuts, files, and registry data.

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.

Npcap

Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows. It implements the open Pcap API using a custom Windows kernel driver alongside a Windows build of the libpcap library.

Object Identifier

In computing, OIDs are an identifier mechanism which is standardized by the International Telecommunication Union (ITU) and ISO/IEC for the naming of an object, concept, or other item with a globally-unambiguous persistent name.

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.

Packet Capture

A pcap is an application programming interface (API) that captures live network packet data from the OSI model (layers 2-7).

Peripheral Component Interconnect

Peripheral component interconnect (PCI) is a hardware bus standard for connecting peripheral devices to a computer's motherboard.

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.

Process ID

A PID is a unique number that an operating system assigns to a running process, used to identify and manage it while it is active.

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.

SCAP Compliance Checker

SCC is a tool, distributed by the Defense Information Systems Agency, that scans a host against SCAP-formatted benchmarks and reports the results.

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 Content Automation Protocol

SCAP is a suite of specifications, maintained by the National Institute of Standards and Technology, for expressing and checking system security configuration and vulnerability information in a standardized, machine-readable format.

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.

Security Technical Implementation Guide

A STIG is a configuration standard published by the U.S. Defense Information Systems Agency that specifies secure configuration settings for an operating system, application, or network device.

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

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.

Sysmon

System Monitor (Sysmon) is a Windows system service and device driver that is installed on a system to monitor and log system activity and write it to the Windows event log. Once installed, it remains across system reboots. It provides detailed information about changes to file creation time, network connections, and process creations. It uses SIEM or Windows Event Collection agents to collect the events it generates and then analyzes them to identify anomalous or malicious activity to help you understand how intruders and malware operate on a network.

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 Plug and Play

UPnP is a network protocol that enables devices to automatically discover and communicate with each other using broadcast messages. While it facilitates easy device identification and connectivity, UPnP lacks robust authentication, making it vulnerable to unauthorized access in cybersecurity contexts.

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.

USBPcap

USBPcap is an open-source [USB](#) sniffer for Windows.

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.

User-Mode Font Driver

A Windows component that handles font rendering in user mode, separate from the kernel.

Virtual Local Area Network

A VLAN is a broadcast domain that is isolated and partitioned in a computer network at the data link layer (OSI layer 2).

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.

WinPcap

WinPcap is a freeware tool for link-layer network access in Windows environments. It lets applications capture and transmit network packets bypassing the protocol stack, and including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

YARA

YARA is a tool designed to help identify and classify malware samples by describing them in terms of textual or binary patterns. YARA rules are used to detect files, processes, or network traffic that match known malware signatures.

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.

