NOZOMI NETWORKS

Arc
Administrator Guide

Arc v1.17.0 — 2025-07-03

Legal notices

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

Copyright

Third Party Software

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

Contents

Chapter 1. Introduction

Arc 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 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 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.

Architecture

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

You can connect Arc:

- To Guardian
- To Vantage

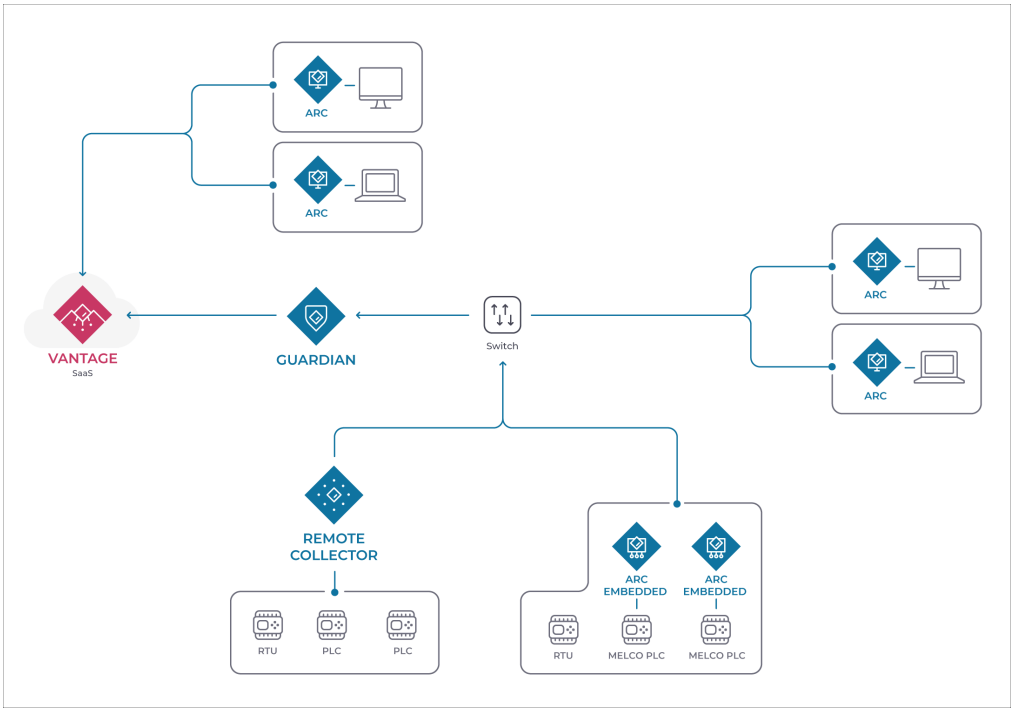


Figure 1. Arc architecture example

Arc in Vantage

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

Vantage Sensors page

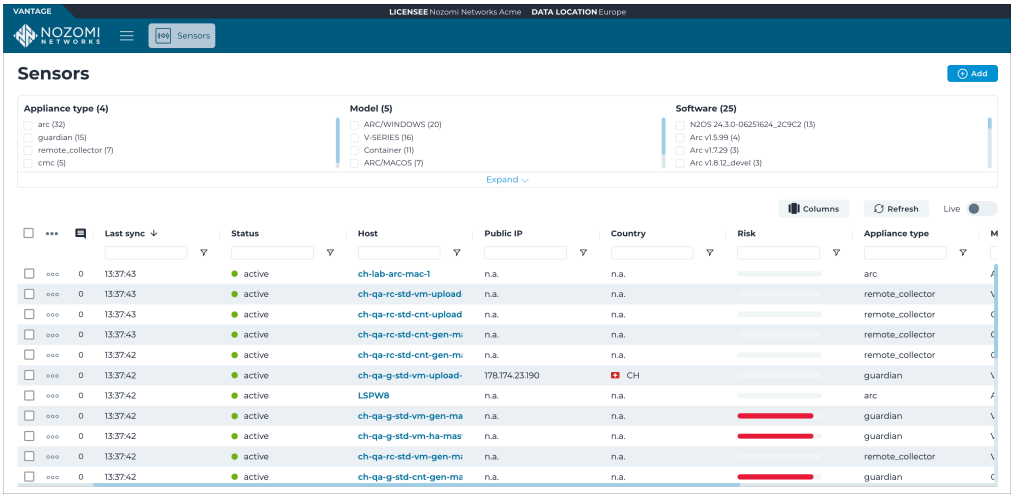


Figure 2. Vantage Sensors page

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

Make connections page

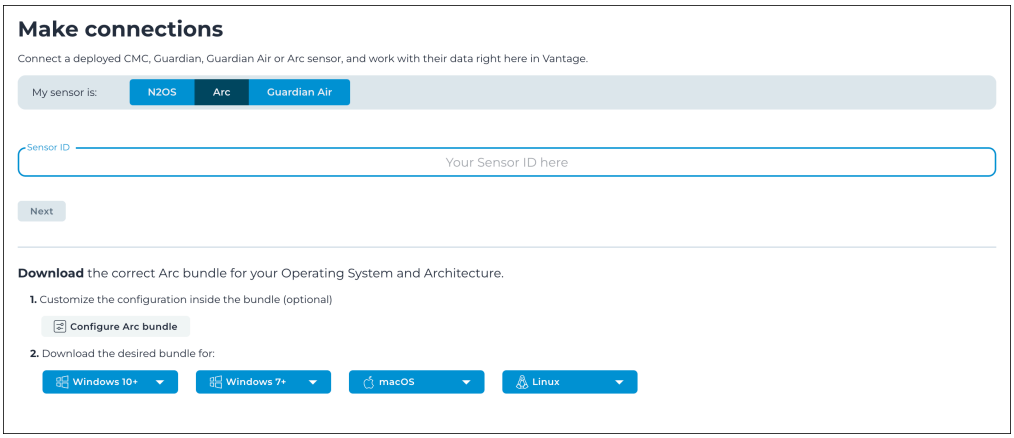


Figure 3. Make connections page

Configure an Arc sensor

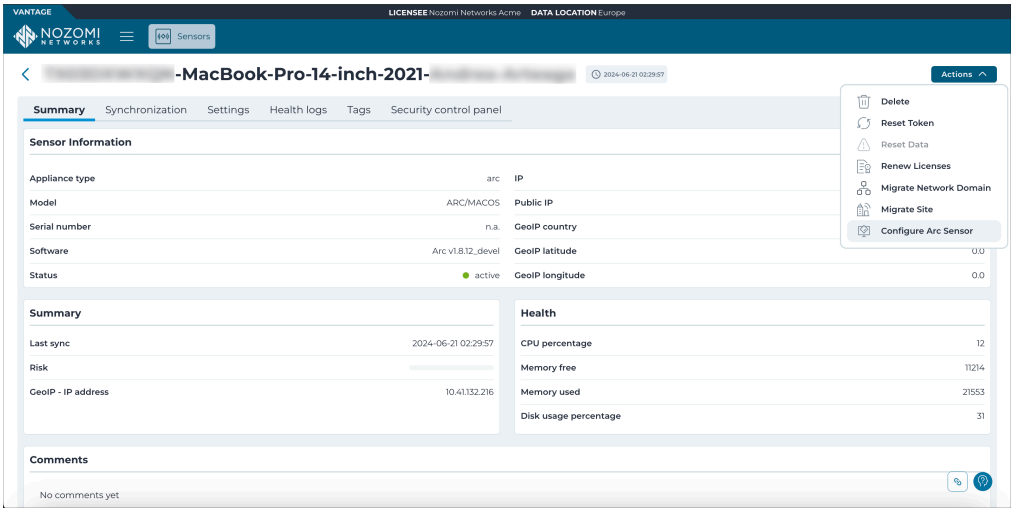


Figure 4. Actions menu in sensor details page

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

Configure multiple Arc sensors

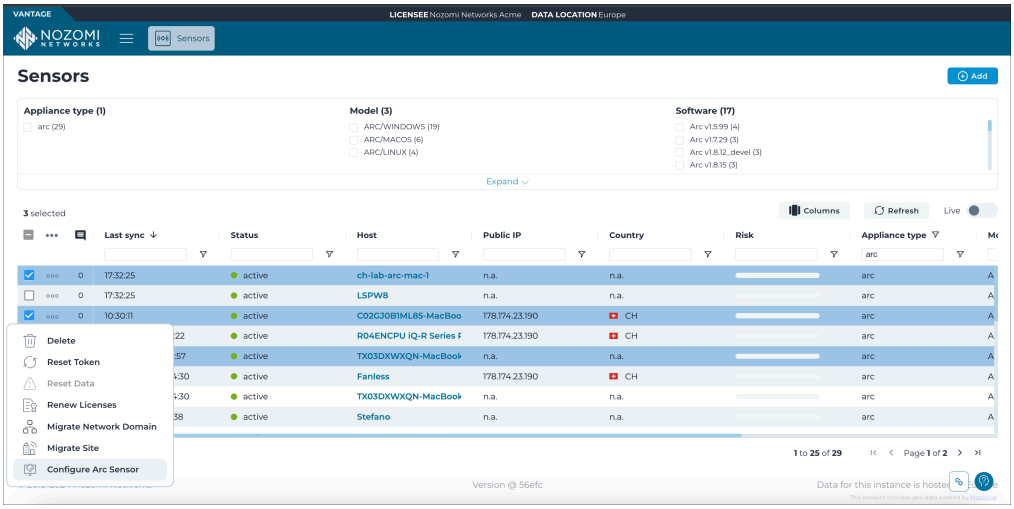


Figure 5. Configure multiple Arc sensors

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

Arc in Guardian

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

Figure 6. Arc button in Guardian Web UI

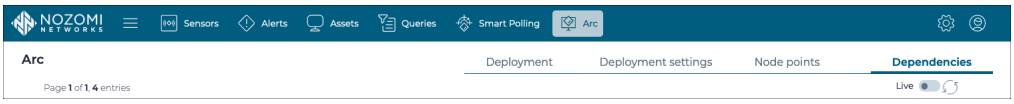


Figure 7. Arc button in Guardian Web UI (not connected to Vantage)

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

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

Configure an Arc sensor

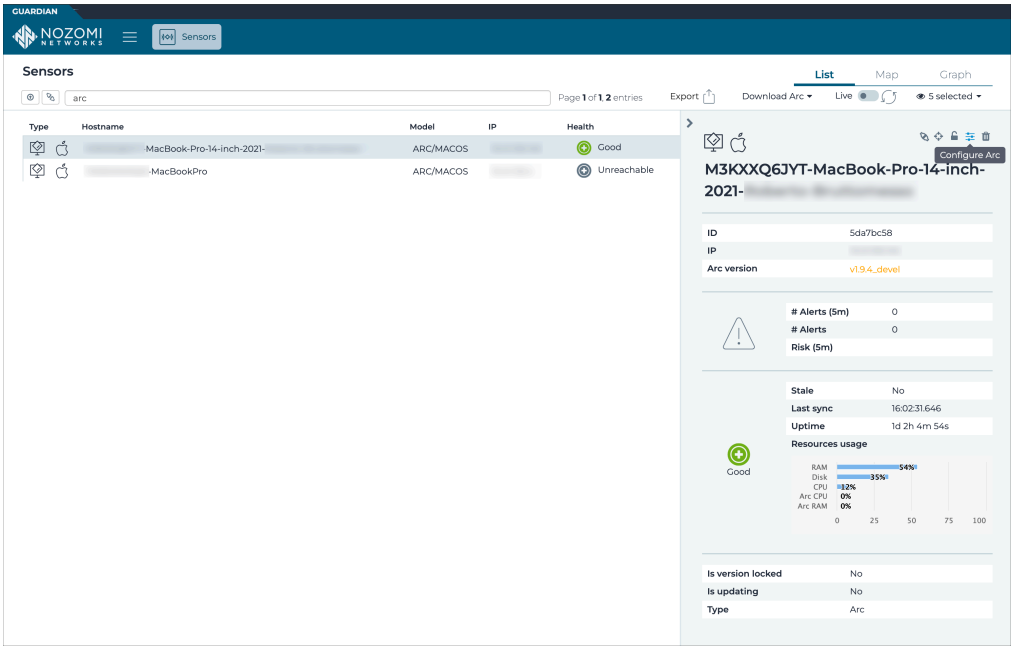


Figure 8. Configure an Arc sensor

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

Deployment

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

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

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

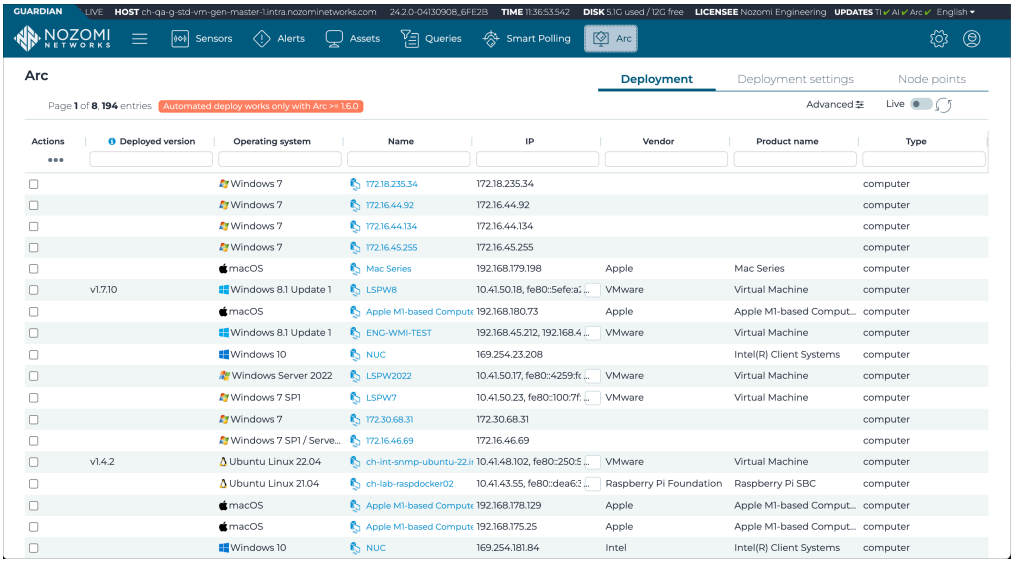


Figure 9. Deployment page

Advanced

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

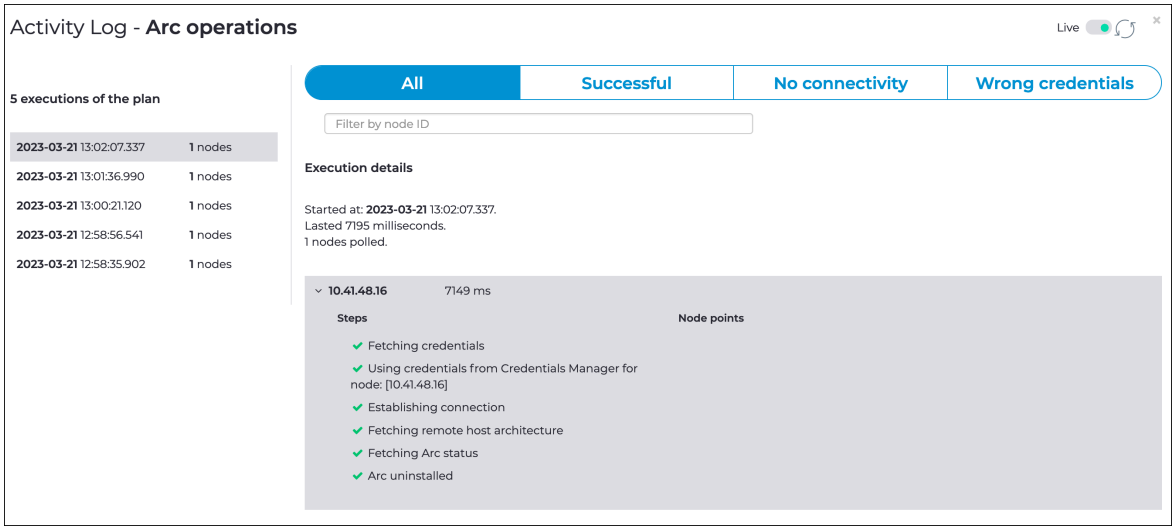
Execution details

*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



Live toggle

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

Refresh

The icon lets you immediately refresh the current view.

Deployment settings

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

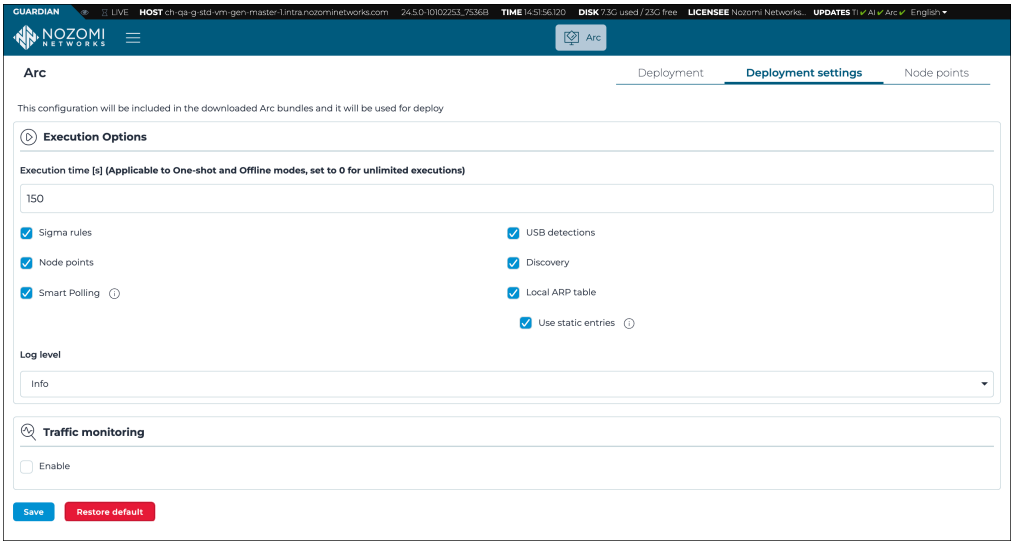


Figure 11. Deployment settings page

Execution Options

For more details, see Execution options (on page 61).

Traffic monitoring

For more details, see Traffic monitoring (on page 63).

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 *identifier (ID)* to filter the nodes.

Live toggle

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

Refresh

The icon lets you immediately refresh the current view.

Nodes

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

Dependencies

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

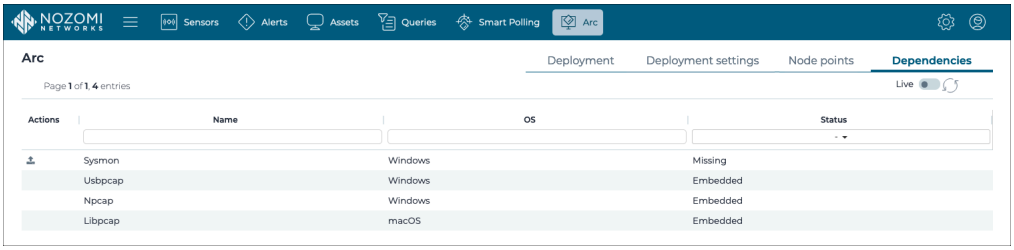


Figure 12. Dependencies page in Guardian (not connected to Vantage)

Arc in CMC

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

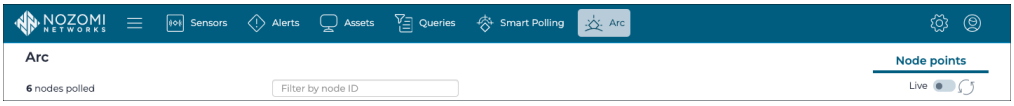


Figure 13. Arc button in CMC Web UI

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 20).

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 *transport layer security (TLS)* 1.2/1.3 communication to the upstream machine.

Data availability

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

Detection information

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

Table 1. Detection information

Category	Information	Windows	macOS	Linux	Configuration option
sensor	Traffic monitoring	✓	✓	✓	Traffic monitoring
sensor	Discovery	✓	✓	✓	Discovery
sensor	Smart Polling	✓	✓	✓	Smart Polling
endpoint	addresses	✓	✓	✓	always on
endpoint	*IP* addresses	✓	✓	✓	always on
endpoint	Product name	✓	✓	✓	always on
endpoint	Vendor	✓	✓	✓	always on
endpoint	Label/host name	✓	✓	✓	always on
endpoint	*OS*	✓	✓	✓	always on
endpoint	Serial number	✓	✓	✓	always on
endpoint	Hardware components	✓		✓	always on
endpoint	Local *address resolution protocol (ARP)* table	✓	✓	✓	Local *ARP* table

Table 1. Detection information (continued)

Category	Information	Windows	macOS	Linux	Configuration option
endpoint	Sigma rules	✓			Sigma rules
endpoint	*USB* detections	✓			*USB* detections
endpoint	*central processing unit (CPU)* usage	✓	✓	✓	node points
endpoint	Memory usage	✓	✓	✓	node points
endpoint	Disk usage	✓	✓	✓	node points
endpoint	Installed software	✓		✓	node points
endpoint	Hotfixes	✓			node points
endpoint	Antivirus	✓			node points
endpoint	Log4j detection	✓	✓	✓	node points
endpoint	User accounts	✓	✓	✓	node points
endpoint	Logged in users	✓	✓	✓	node points
endpoint	*USB* interfaces	✓			node points
endpoint	Network interfaces	✓	✓	✓	node points
endpoint	Processes and ports	✓	✓	✓	node points
endpoint	Disk partitions	✓	✓	✓	node points

Table 1. Detection information (continued)

Category	Information	Windows	macOS	Linux	Configuration option
endpoint	*domain name server (DNS)*	✓	✓	✓	node points
endpoint	*CPU*	✓	✓	✓	node points

Chapter 2. Requirements

Operating System requirements

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

Operating System	Architecture	Version
Windows	x86, x86_64	Windows 7 (Service Pack 1), or later
		Windows Server 2012, or later
macOS	x86_64, arm64	macOS 10.10 Yosemite, or later
Linux	x86_64, arm, arm64	Ubuntu 16.04, or later
		Debian Jessie, or later
		CentOS 7, or later
		Raspbian Jessie, or later
		RedHat Linux Enterprise 7.3, or later
		Suse Linux Enterprise Server 15, or later

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.

Software requirements

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

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

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

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

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 2. 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 31)

Enable Audit Policy on Microsoft Windows

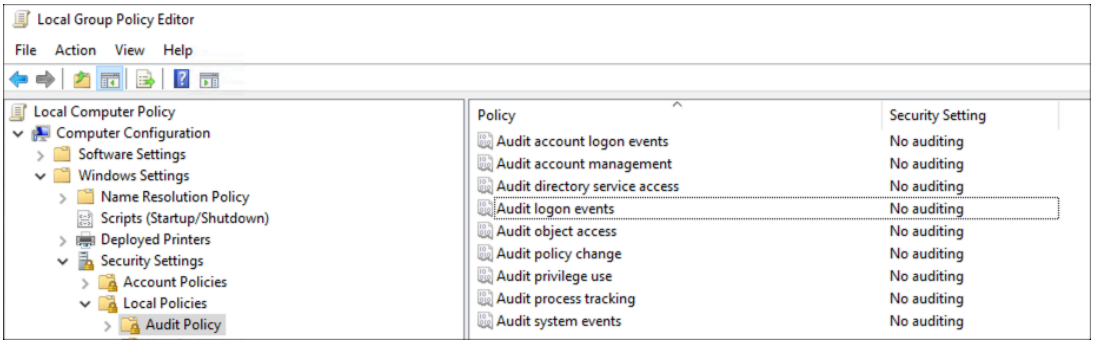
*If you want Arc to detect user logon activities, you must enable **Audit logon events** of Microsoft Windows.*

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.

Enable FIPS on Microsoft Windows

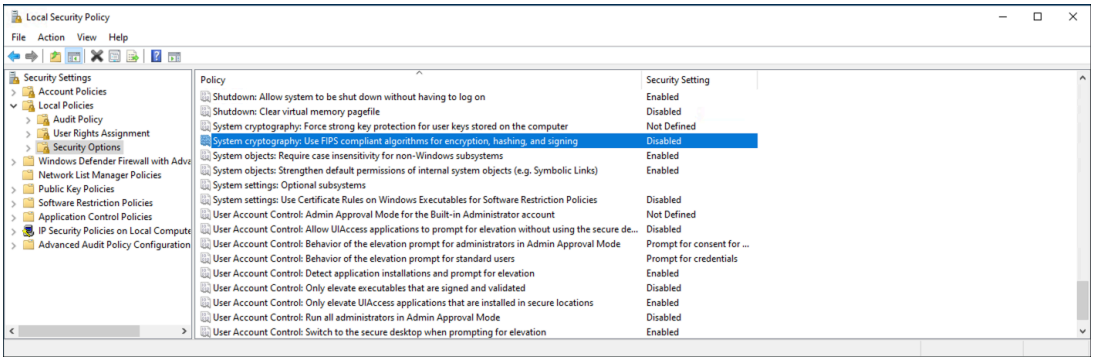
*Before you can use Arc in FIPS-compliant mode, you must enable FIPS in the **Local Security Policy** of Microsoft Windows.*

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.

Guardian

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

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

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

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

Vantage

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

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

CMC

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

Install a license in Guardian or CMC

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

Before you begin

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

Procedure

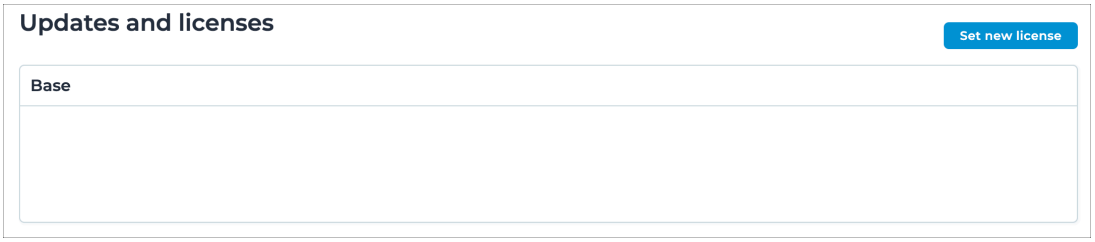
1. In the top navigation bar, select ⚙

   Result: The administration page opens.

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

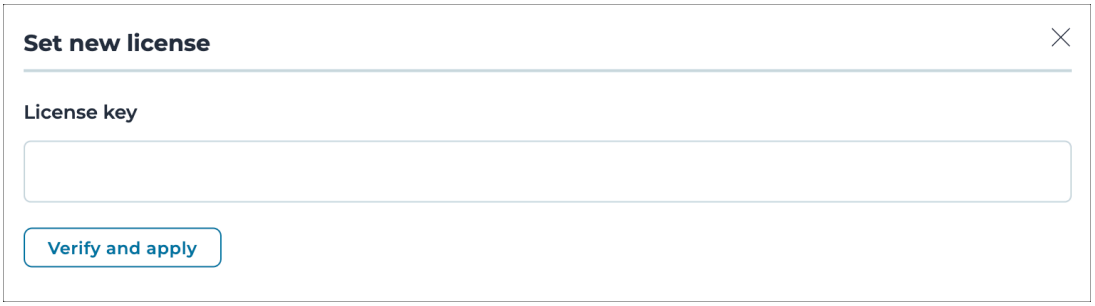
   Result: The **Updates and licenses** page opens.

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



   Result: A dialog shows.

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



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

Results

The license has been installed.

Import Arc through the update service in Guardian or CMC

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

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

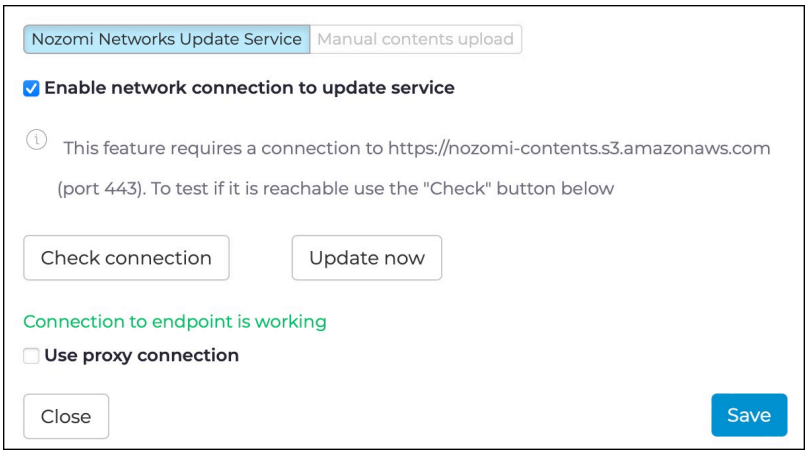
2. In the **System** section, select **Updates and licenses**.

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

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

   Result: A dialog opens.

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



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

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

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

Import Arc through a manual contents upload in Guardian or CMC

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

Before you begin

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

Procedure

1. In the top navigation bar, select ⚙

   Result: The administration page opens.

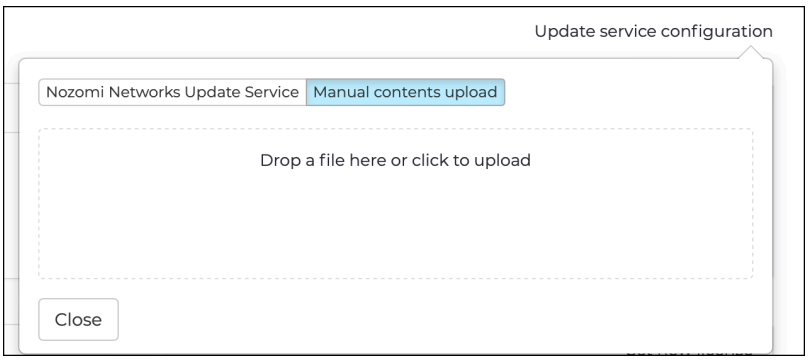
2. In the **System** section, select **Updates and licenses**.

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

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

   Result: A dialog opens.

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



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

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

6. Select **Close**.

Dependencies

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

Table 3. Windows dependencies

Sigma rules	*Sysmon*
	PowerShell-script block-logging
	PowerShell Core-script block-logging
USB detections	*USBPcap*
Traffic monitoring	*WinPcap* or *Npcap*
Asset details	Not needed

Table 4. Linux dependencies

Sigma rules	Not supported
USB detections	Not supported
Traffic monitoring	Not needed
Asset details	*dmidecode*

Table 5. macOS dependencies

Sigma rules	Not supported
USB detections	Not supported
Traffic monitoring	*libpcap*
Asset details	Not needed

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.

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*

For *Sysmon*, the installation is semi-automatic. First, you must upload the latest *Sysmon* bundle to the applicable Guardian page. The bundle is then used for automatic installation during subsequent deployments.

If Arc is connected to Vantage, *Sysmon* is automatically fetched from the original website, and no other actions are required.

Note:
After you have installed *USBPcap*, you must reboot the host machine to make the dependency active.

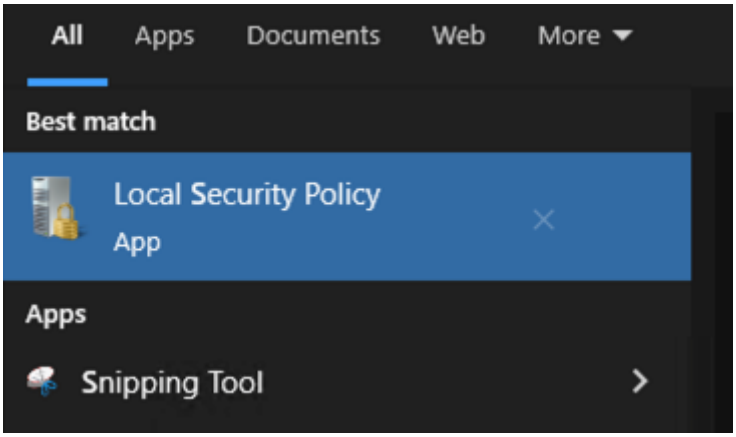
Note:
After a dependency is installed, you must restart Arc to make it active. When Guardian automatically installs dependencies during deployment, no user actions are necessary.

Enable security log events

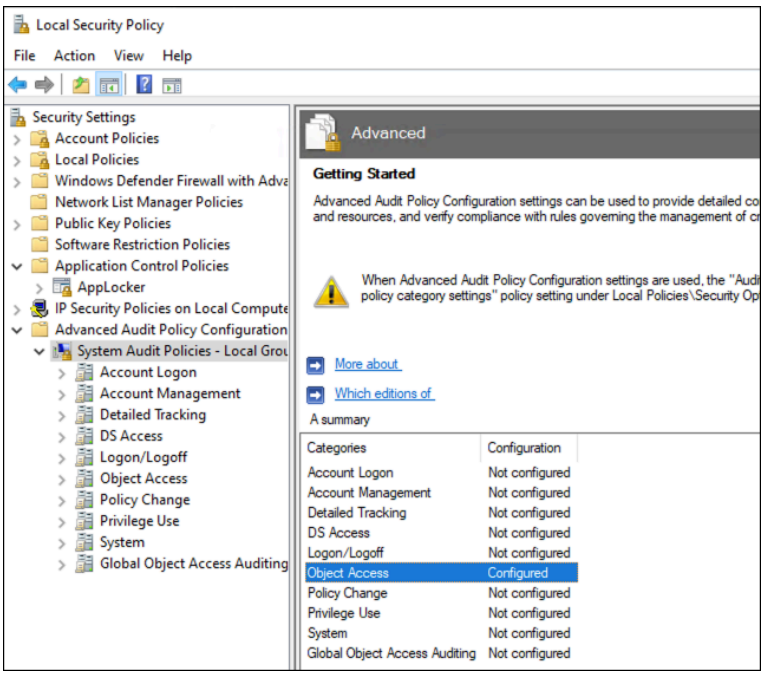
Before you can use Sigma rules related to security log events, you will need to enable them.

Procedure

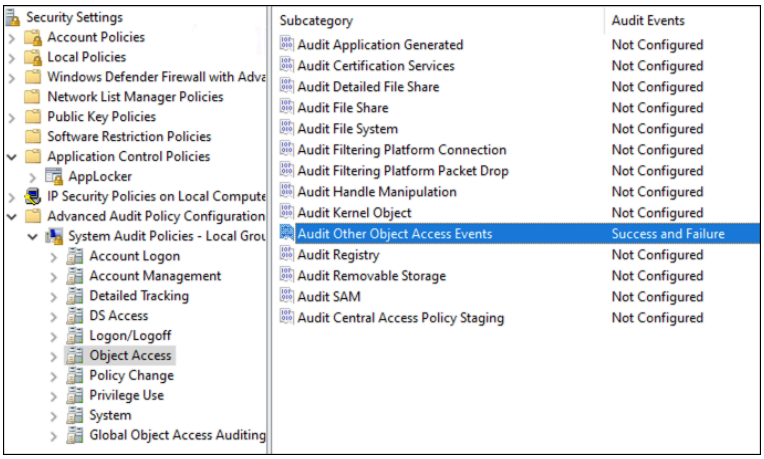
1. Open the Windows **Start** menu and search for the **Local Security Policy** application. Launch the application.



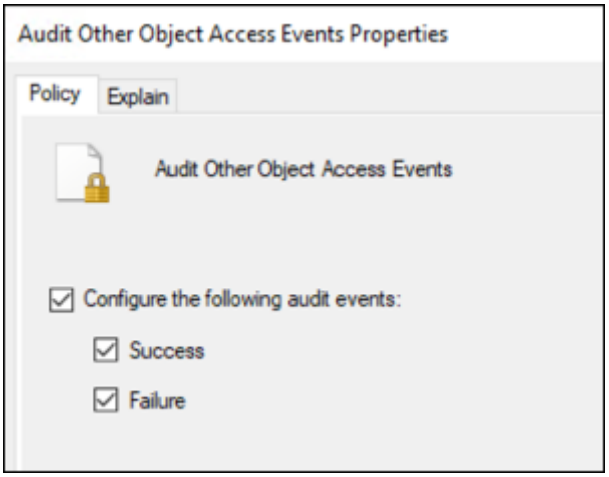
2. Select **Security Settings > System Audit Policies - Local Group**.



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

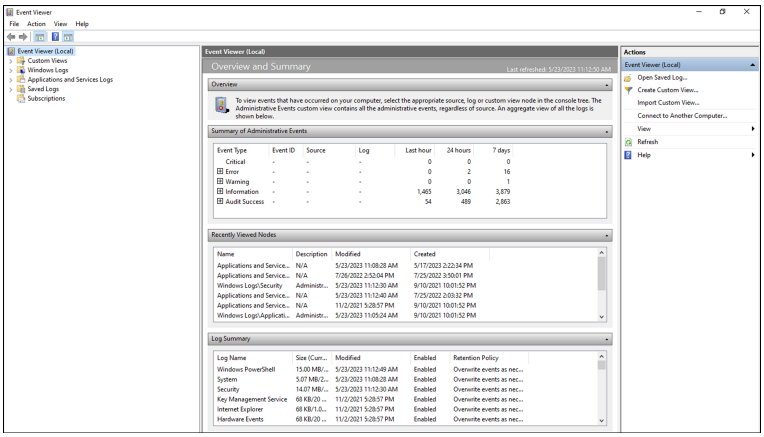
Security log events are now enabled in Windows.

Enable printservice log events

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

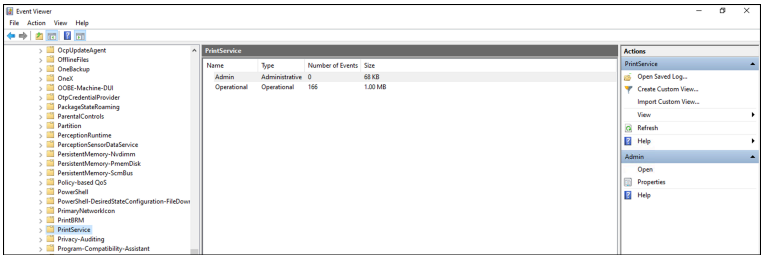
Procedure

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



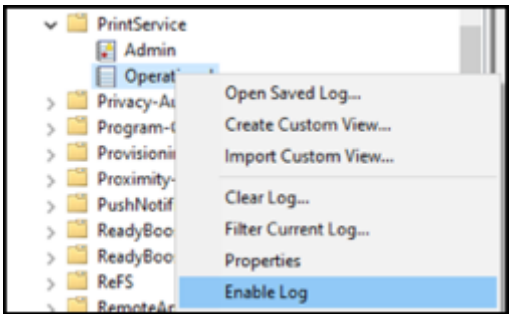
Result: The **Event Viewer** application opens.

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.

Local permissions

It is important to understand the different local permissions 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.

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.

Chapter 4. Configuration

Configure an Arc sensor in Guardian

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

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

Configure an Arc sensor in Vantage

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

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

Local UI

The default method to manage Arc is through the parent system software. However, it is also possible to manage Arc through a local UI.

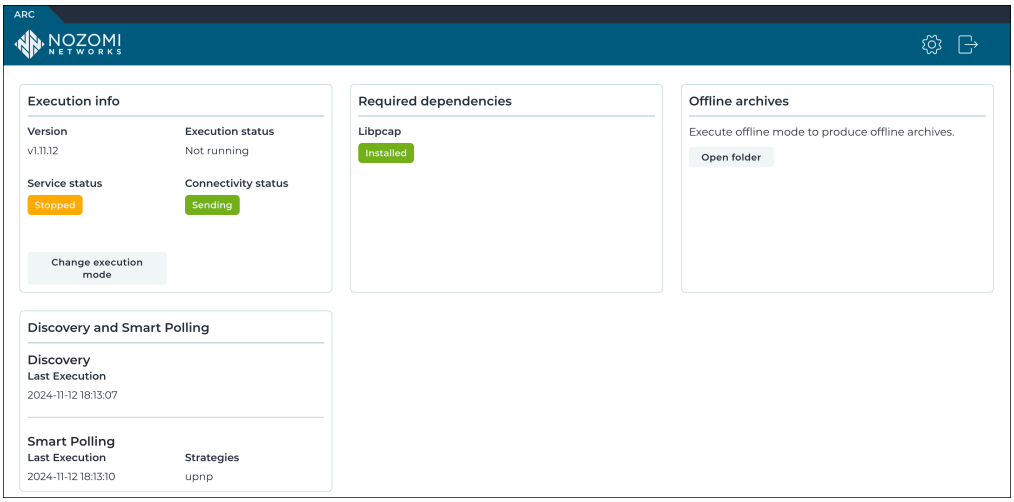


Figure 14. Local UI

The local *UI* has these sections:

- Execution info(rmation) (on page 50)
- Required dependencies (on page 56)
- Offline archives (on page 57)
- Discovery and Smart Polling (on page 58)

To access the Settings (on page 59) 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**.

> **Note:**
> To use the commands `install` and `uninstall`, you must run the local *UI* with admin rights. When you double-click the executable file, a request for admin rights will be made. In Windows, and additional prompt will show when you do this. To have full control, use the shell.

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.

Execution info(rmation)

*The **Execution Info** section displays the status of Arc's sensors, execution modes, and network connectivity. It also provides details about service status, version, and execution controls.*

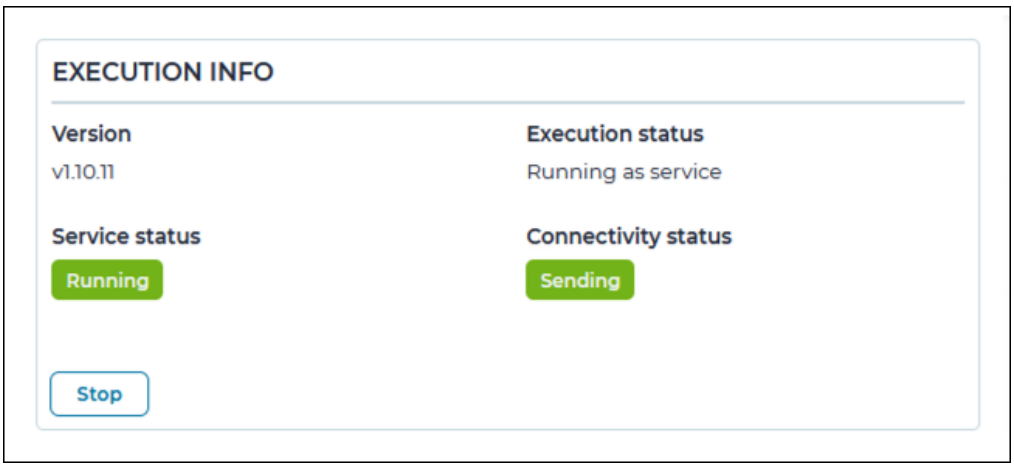


Figure 15. Execution info(rmation)

Version

This shows the version of Arc that has been deployed.

Execution status

`Running, remaining time XXXX s` - in case of **One-shot** or **Offline** executions

`Running as service`

`Stopped`

Service status

`Not installed`

`Stopped`

`Running`

`Unknown` - in case of generic issues

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.

Actions button

This button lets you:

- Change the execution mode
- Run the Arc process, if it is not currently running
- Stop the Arc process, if it is currently running

For more details, see Execution modes (on page 52).

Note:

You can also stop the Arc process from the terminal with the command: `CTRL+C`.

Execution modes

*The **Change execution mode** button lets you select and manage how Arc collects data. You can configure execution time, start or stop processes, and optimize data collection based on the selected mode.*

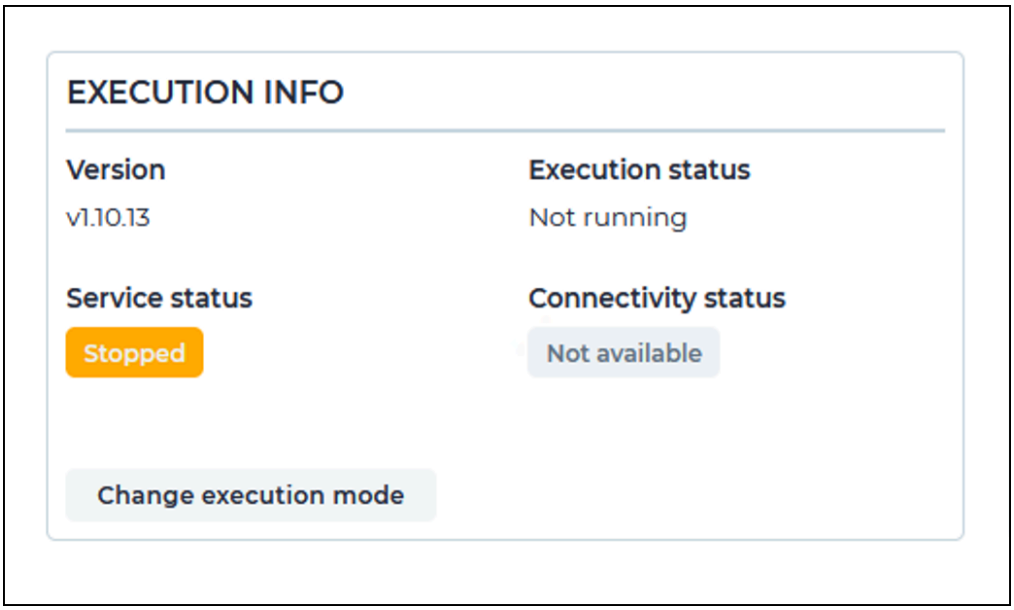


Figure 16. Choose execution mode

This shows a radio button for each of the three execution modes:

- Service mode (on page 53)
- Offline mode (on page 54)
- Oneshot mode (on page 55)

Service mode

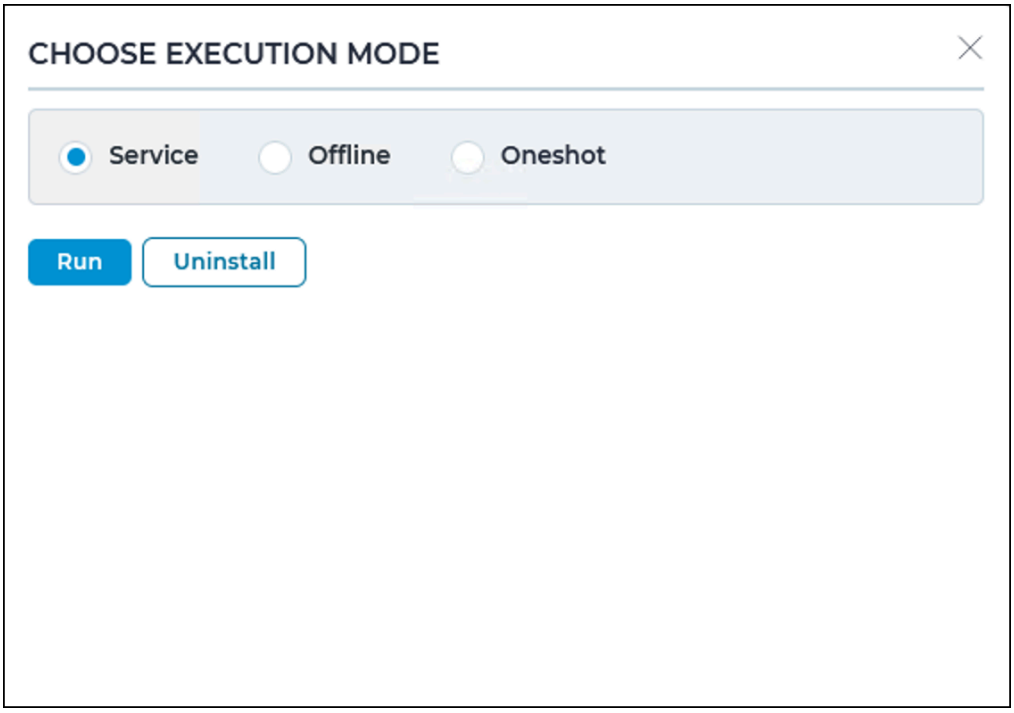


Figure 17. Service mode

The button options are:

- **Run**
- **Uninstall**
- **Stop**

Offline mode

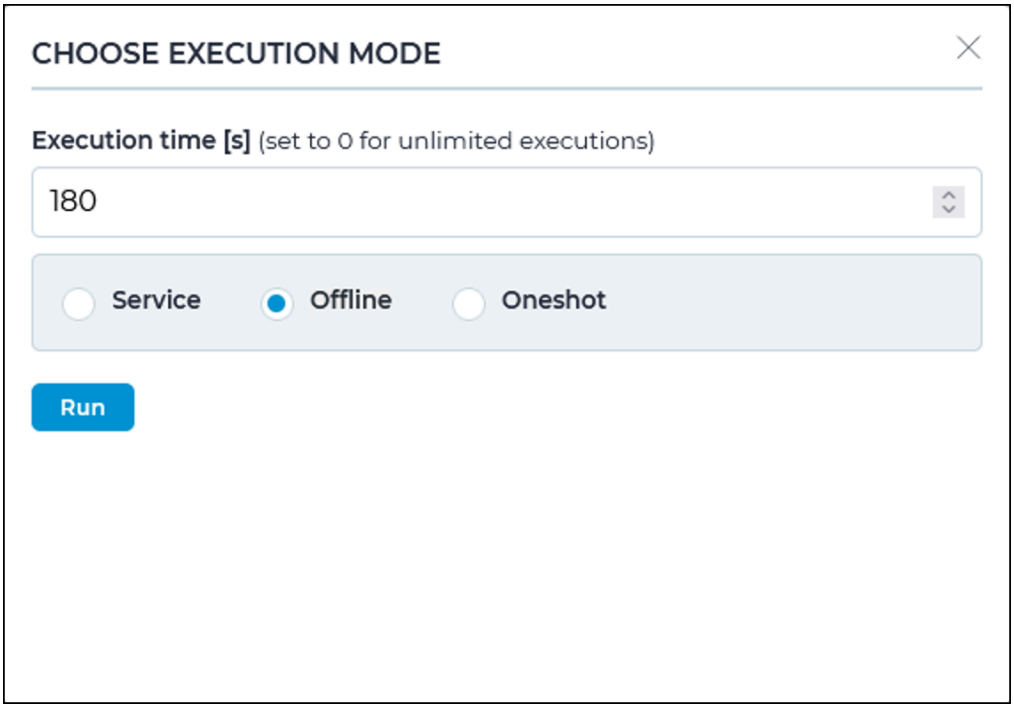


Figure 18. Service mode

Execution time dropdown: This sets the time that Arc will run to collect data. This is applicable for Oneshot and Offline modes.

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

The button options are:

- **Run**
- **Stop**

Oneshot mode

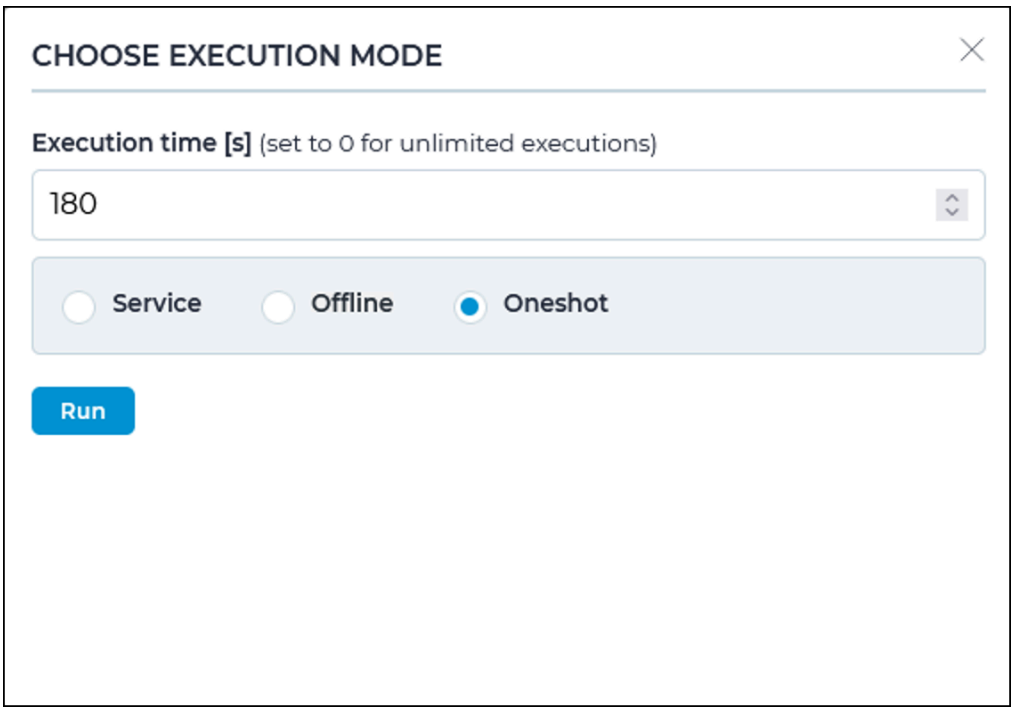


Figure 19. Service mode

Execution time dropdown: This sets 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.

The button options are:

- **Run**
- **Stop**

Required dependencies

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

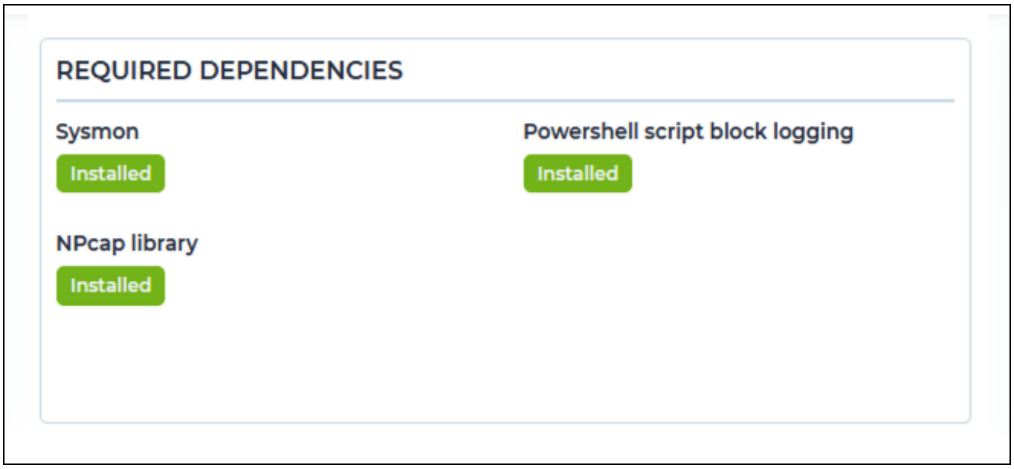


Figure 20. Required dependencies

Offline archives

*The **Offline archives** section gives you access to the archives that have been created in Offline mode for the current session.*

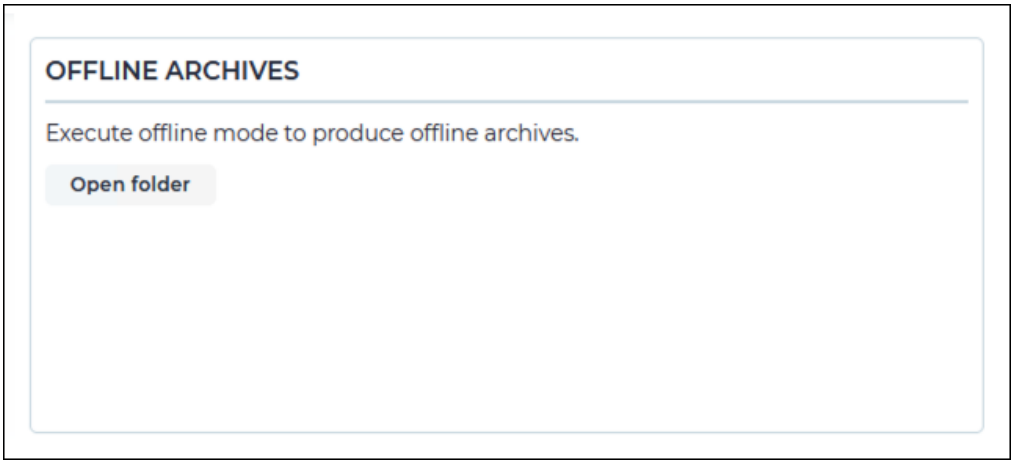


Figure 21. Offline archives

Discovery and Smart Polling

*The **Discovery and Smart Polling** section shows up-to-date execution details and status for Discovery and Smart Polling operations.*

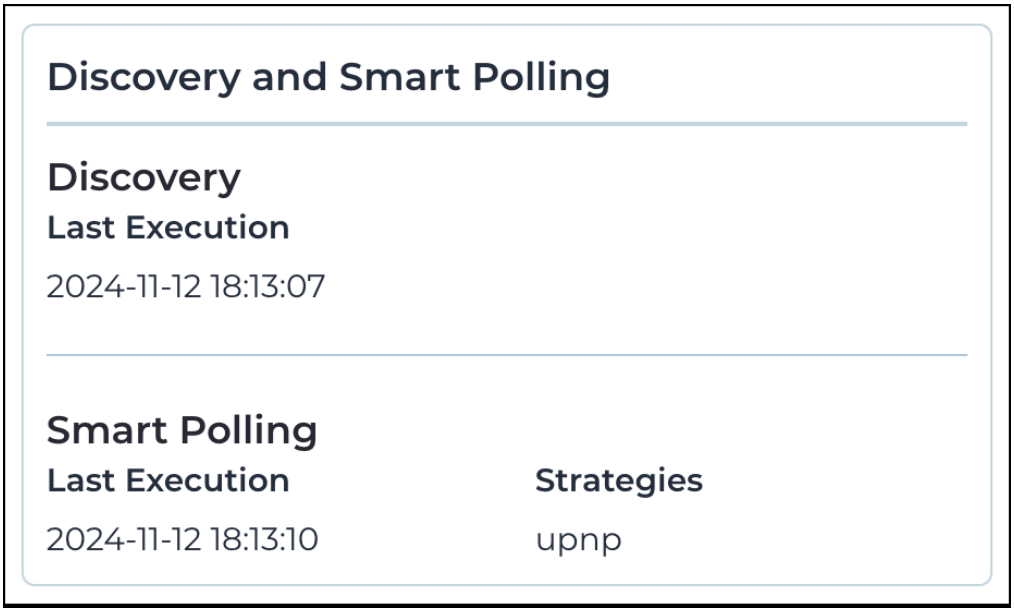


Figure 22. Discovery and Smart Polling

Discovery

This shows the last date and time of execution.

Smart Polling

This shows the last date and time of execution, and the strategy used.

Settings

*The **Settings** page gives you access to the **Upstream connection**, **Execution options**, and **Traffic monitoring** pages.*

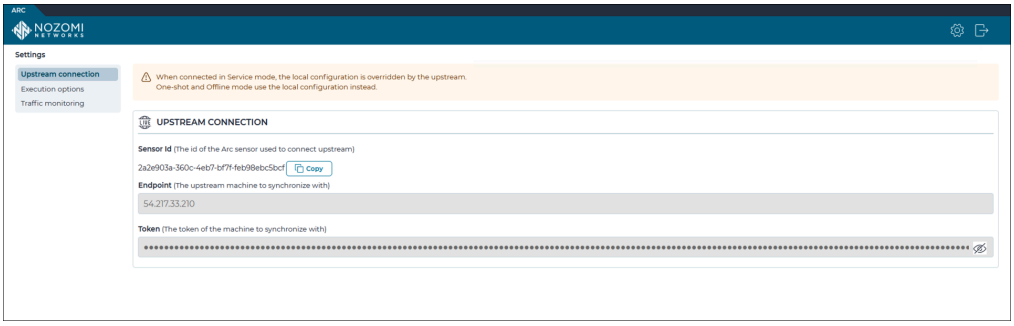


Figure 23. Settings page

The **Settings** page has these sections:

- Upstream connection (on page 60)
- Execution options (on page 61)
- Traffic monitoring (on page 63)

Upstream connection

*The **Upstream connection** page lets you configure and verify the connection between the Arc sensor and the Guardian/Vantage endpoint. Key parameters include the endpoint internet protocol (IP) address and authentication token.*

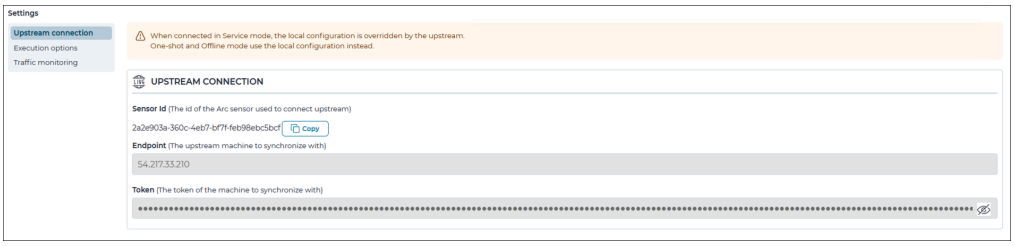


Figure 24. Upstream connection

Sensor id

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

Endpoint

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

> **CAUTION:**
> After the endpoint 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 endpoint manually. This is best done with the help of Nozomi Networks Customer Support.

Token

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

Check connection

This button checks if the connection parameters are correct.

Execution options

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

Figure 25. Execution options

Execution time

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

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

Maximum disk space

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

Sigma rules (Windows only)

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

YARA rules (Windows only)

This lets you enable/disable YARA rules. YARA rules are applied to every newly-detected non-signed *portable executable (PE)* on the host machine's file system.

USB detections (Windows only)

This lets you enable/disable *USB* detections.

Node points

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

Discovery

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

Discovery 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 *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.

Local ARP table

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

Log level

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

- Debug
- Info
- Warning
- Error

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

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

Traffic monitoring

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

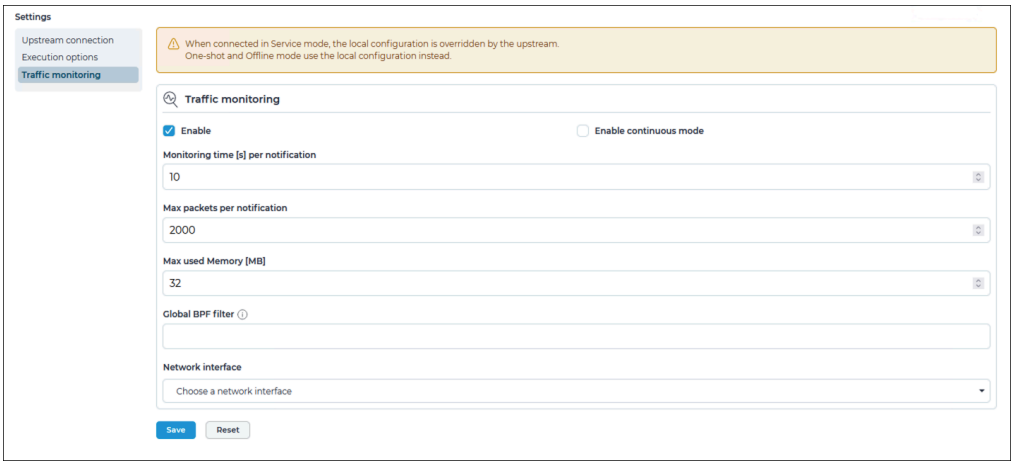


Figure 26. Traffic monitoring

Enable

This checkbox lets you enable/disable traffic monitoring.

Enable continuous mode

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

Arc uses two different methods for traffic monitoring:

- Intermittent mode
- Continuous mode

Intermittent mode

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

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

Continuous mode

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

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

Global BPF filter

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

Network interface

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

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

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.

Shell commands

A list of available shell commands.

Table 6. Shell commands - Linux

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

Note:
1 - Requires admin rights.

Table 7. Shell commands - Windows

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

Note:
1 - Requires admin rights.

Table 8. Shell commands - macOS

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

Note:

1 - Requires admin rights.

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

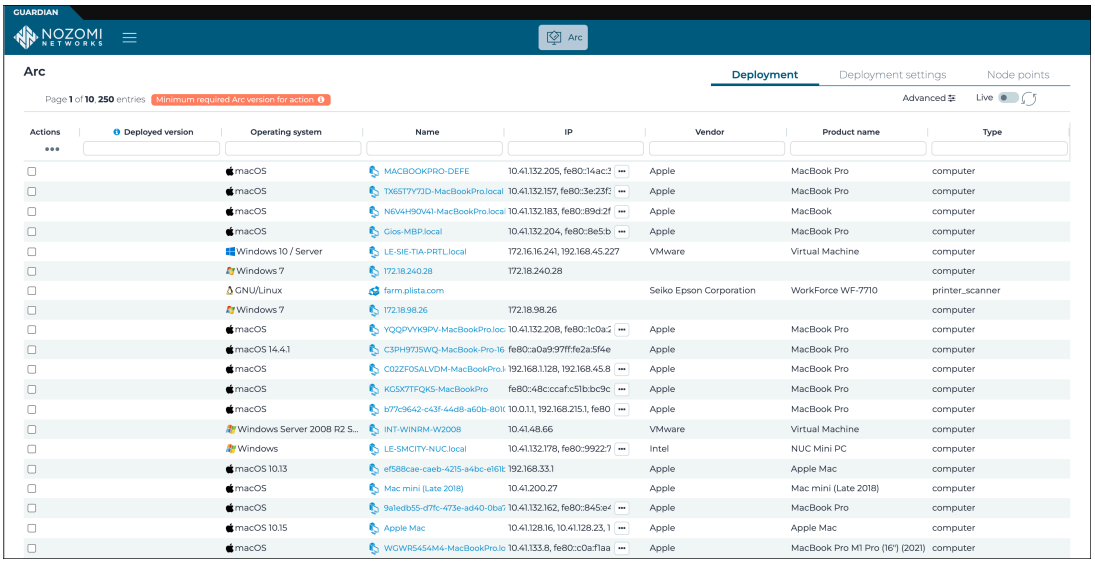
You can use the Windows Remote Management (WinRM) or Secure Shell (SSH) services to deploy Arc at scale for target machines that are reachable from Guardian.

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**.



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 47).

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

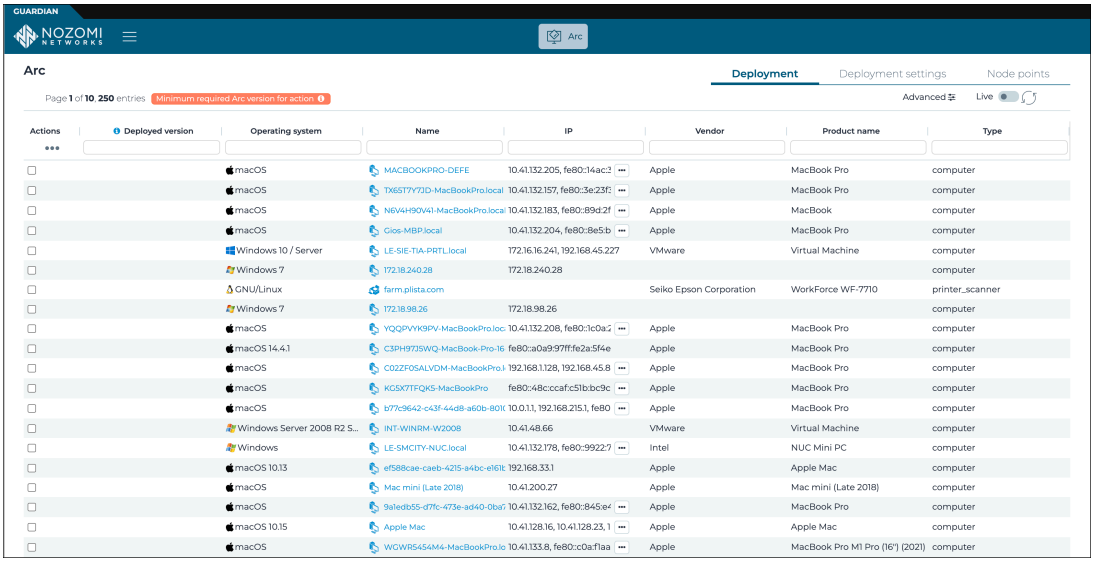
You can use Secure Shell (SSH) services to deploy Arc at scale for target machines that are reachable from Guardian.

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**.



   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 47).
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

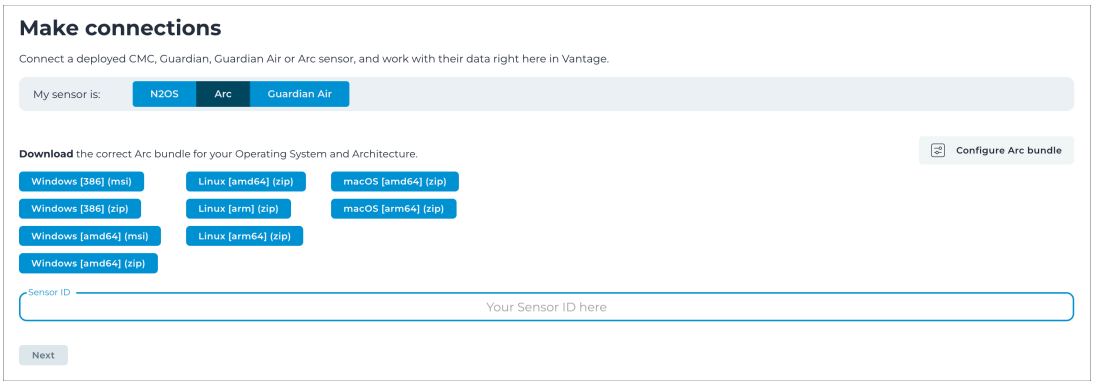
Download an Arc package from Vantage

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.



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 `--%`, example: `msiexec --% /i "arc.windows.amd64.msi" /L*v "installer.log"`

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

Supported arguments list:

- --mode=[silent|gui] (Select if start setup in GUI mode or in silent mode.)
- --acceptLicense=true (If set skips license (EULA) acceptance, mandatory for silent mode.)
- --endpoint=<ip address of guardian or vantage>
- --token=<token to connect to guardian>
- --installDeps=[all|sysmon|usbpcap|npcap|psscriptblocklogging] (It supports multiple values separated by "," Example: `sysmon,usbpcap,npcap`
- --uninstallDeps=[all|sysmon|usbpcap|npcap|psscriptblocklogging] (Same as above.)
- --sysmonPath=<path of sysmon.zip> (To be used to provide the path of sysmon installed, otherwise it will be downloaded from guardian/vantage or from Microsoft. It is required to install an old version of sysmon (Windows 7).)
- --rebootIfRequired=false (It will not reboot the machine if required.)
- --createShortcutIcon=false (This will not create a desktop shortcut.)
- --startArcService=false (It will not install/start arc service.)

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.

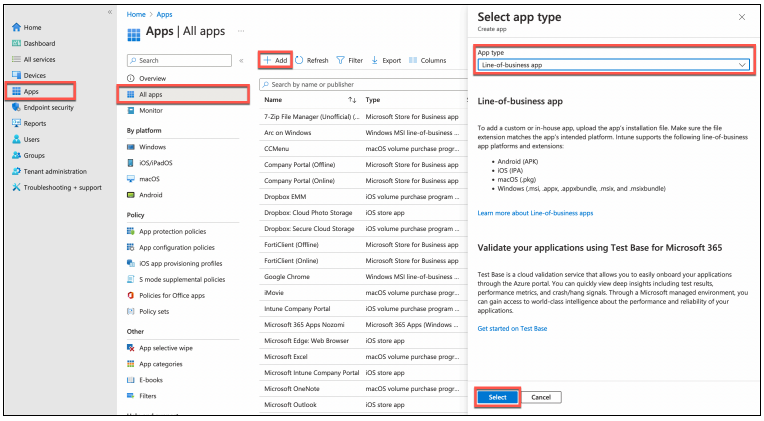
Before you begin

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

- Downloaded the correct Arc package for your *OS*
- Compiled the *MSI* file

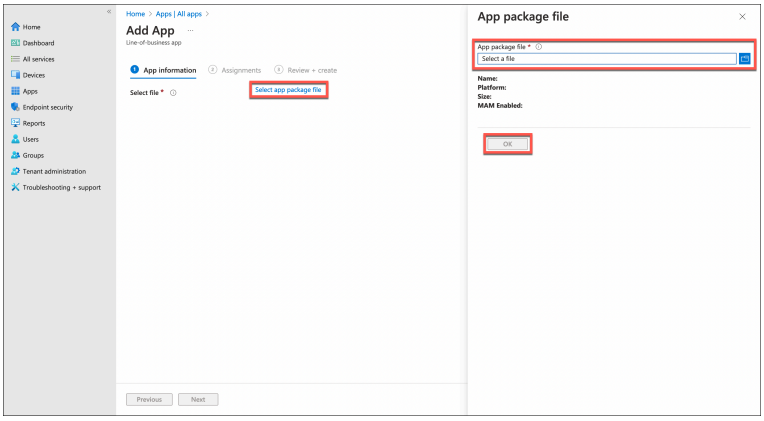
Procedure

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**.



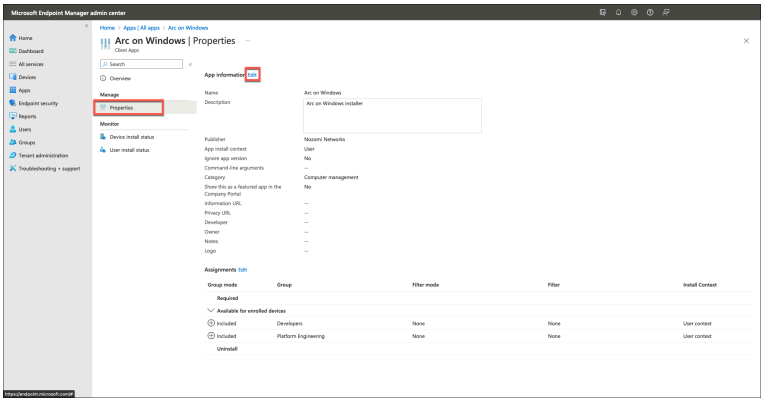
8. Go to **Apps > All apps**.
9. In the search bar on the right side, enter the first part of the name of the package that you just uploaded, and select **Enter**.
10. Select the name of the correct file.

    Result: The details for the app show.

11. Select **Properties**.

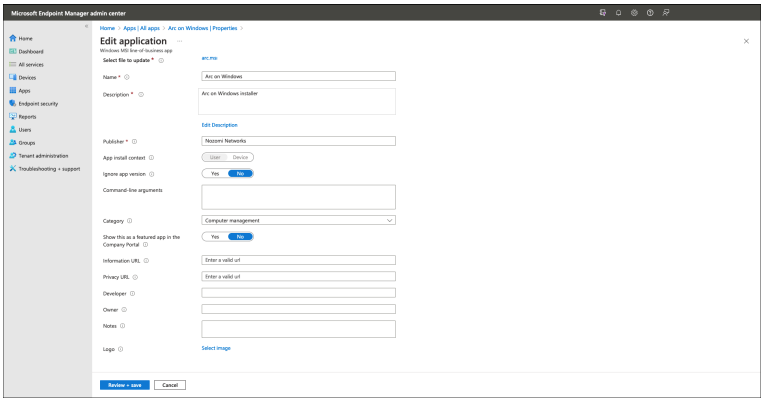
    Result: The information for the app shows on the right.

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

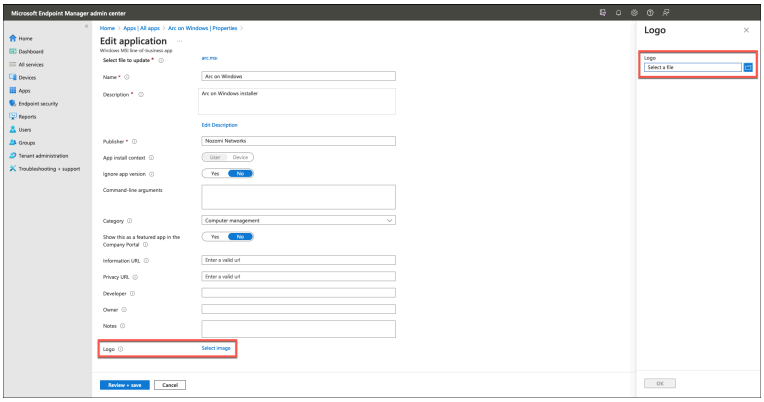


13. Enter the information as necessary.

> **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 79).

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.

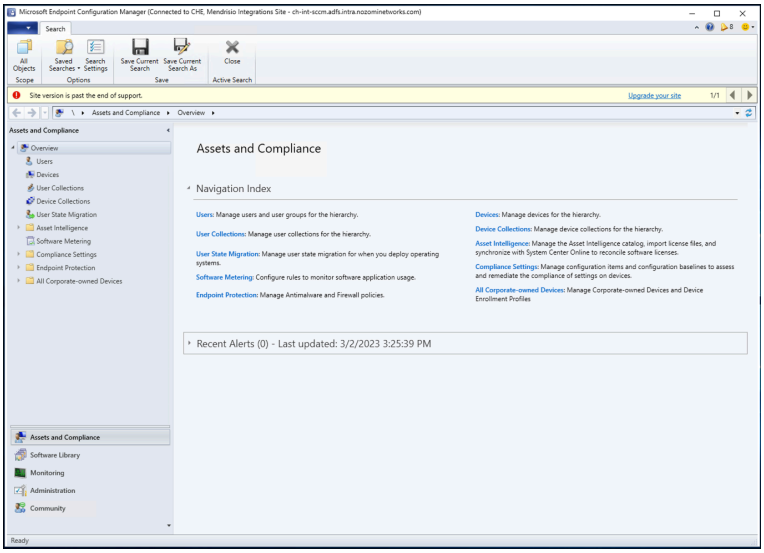
Before you begin

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

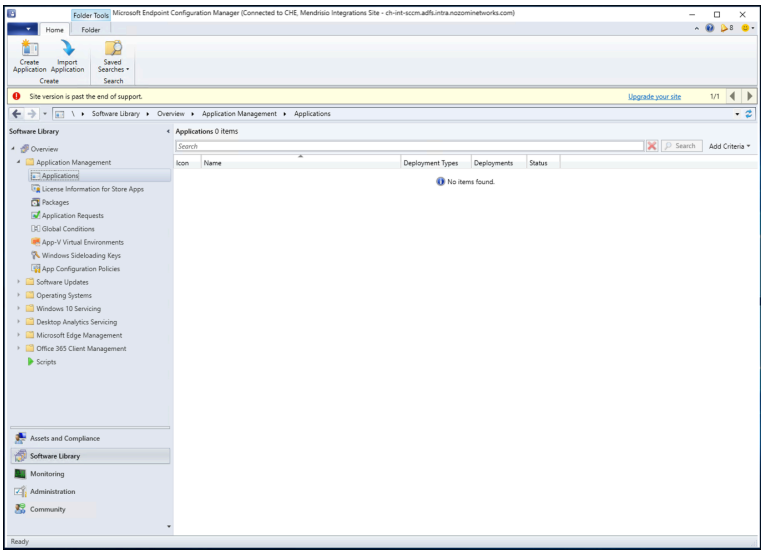
- Downloaded the correct Arc package for your *OS*
- Compiled the *MSI* file

Procedure

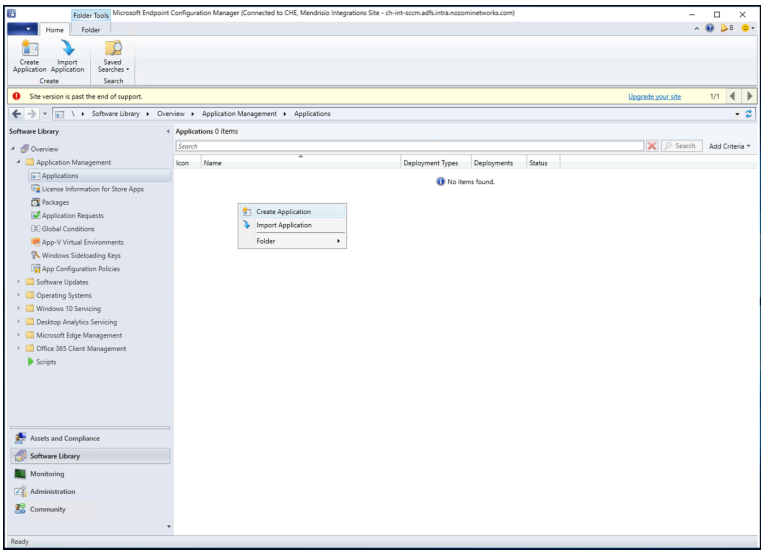
1. Open **Microsoft Endpoint Configuration Manager**.



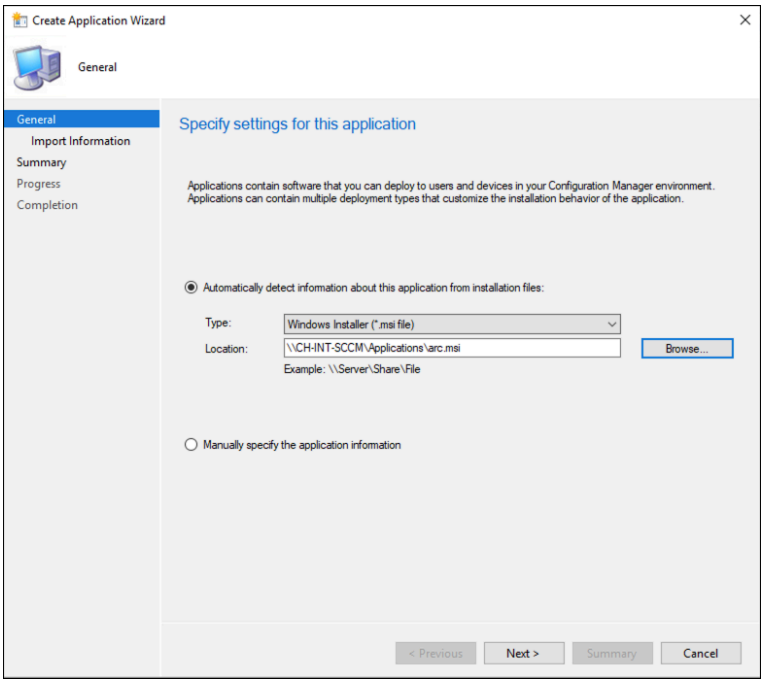
2. Go to **Software Library > Overview > Application Management > Applications**.



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

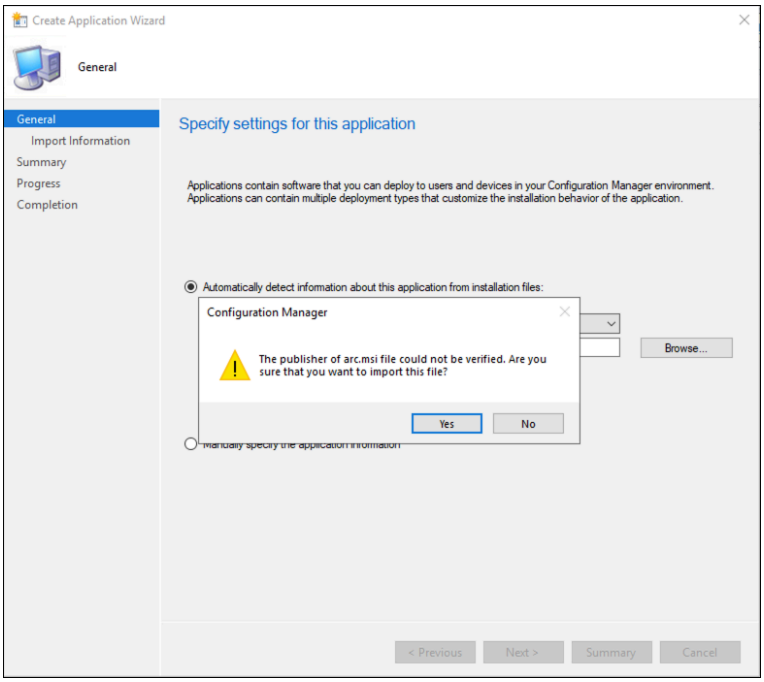


4. Browse and select the location of the *MSI* file, and then select **Next**.

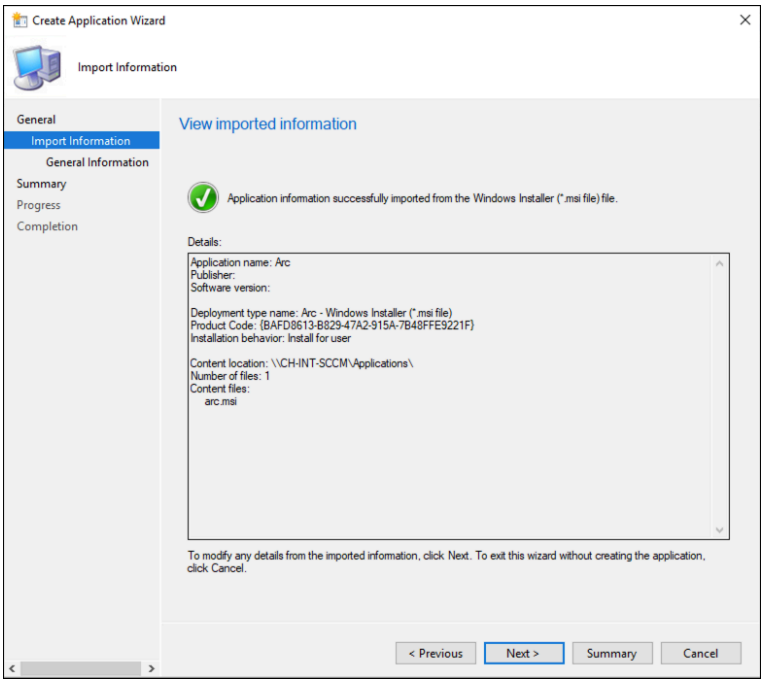


Result: A dialog shows.

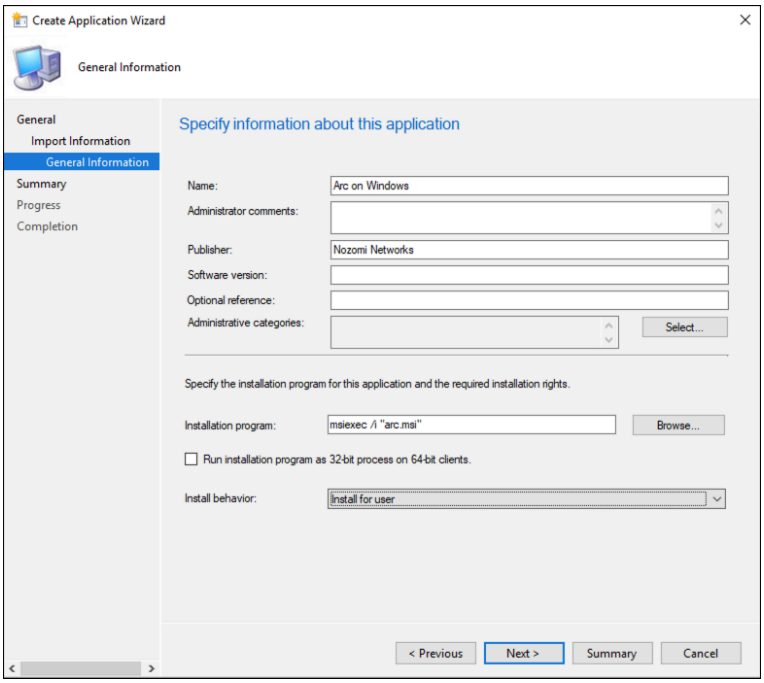
5. To confirm the import of the package, select **Yes**.



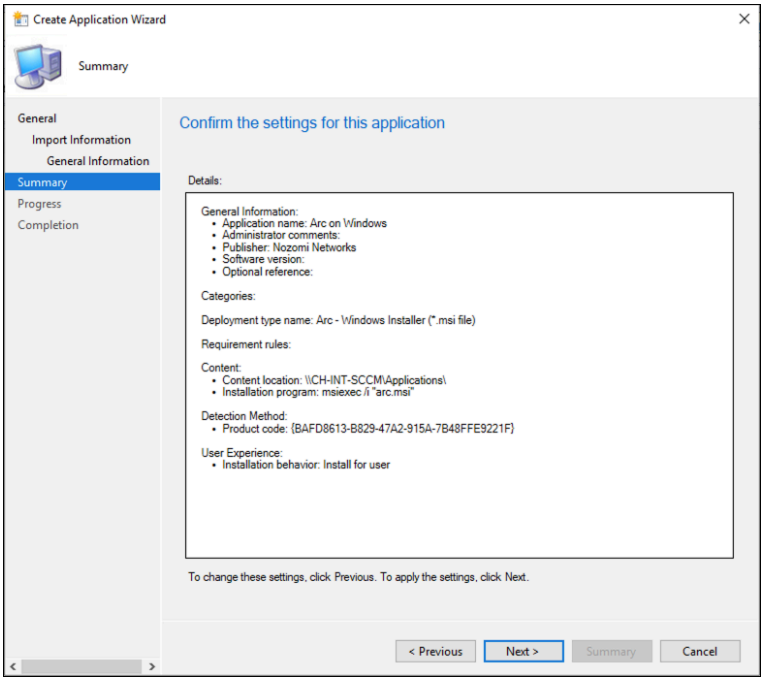
6. Make sure that the file has been imported successfully, and then select **Next**.



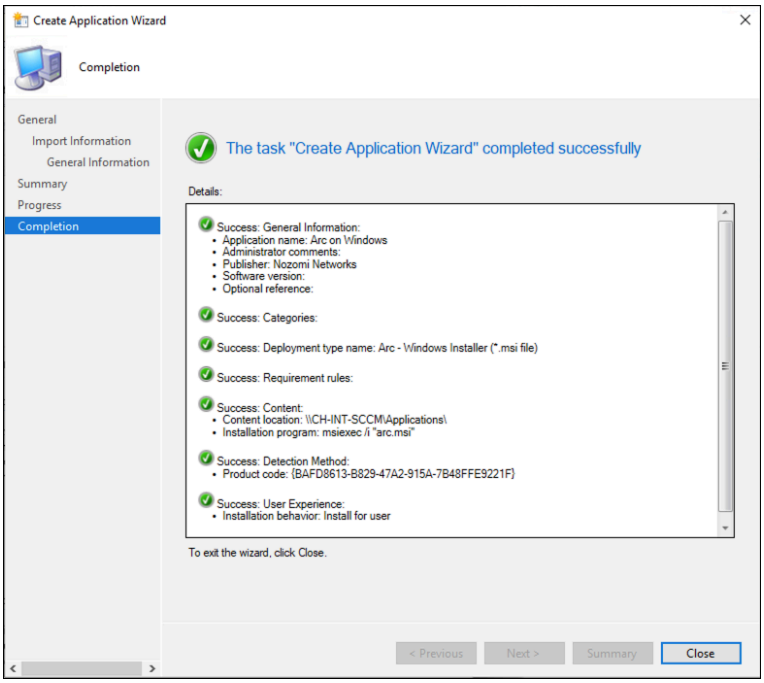
7. On the **General Information** page, enter details in the fields as necessary. Select **Next**.



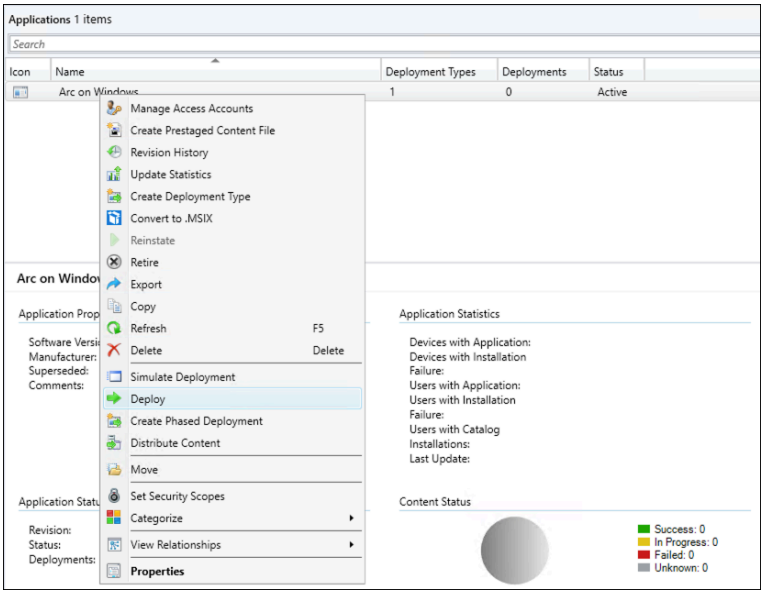
8. Review the settings, and then select **Next**.



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

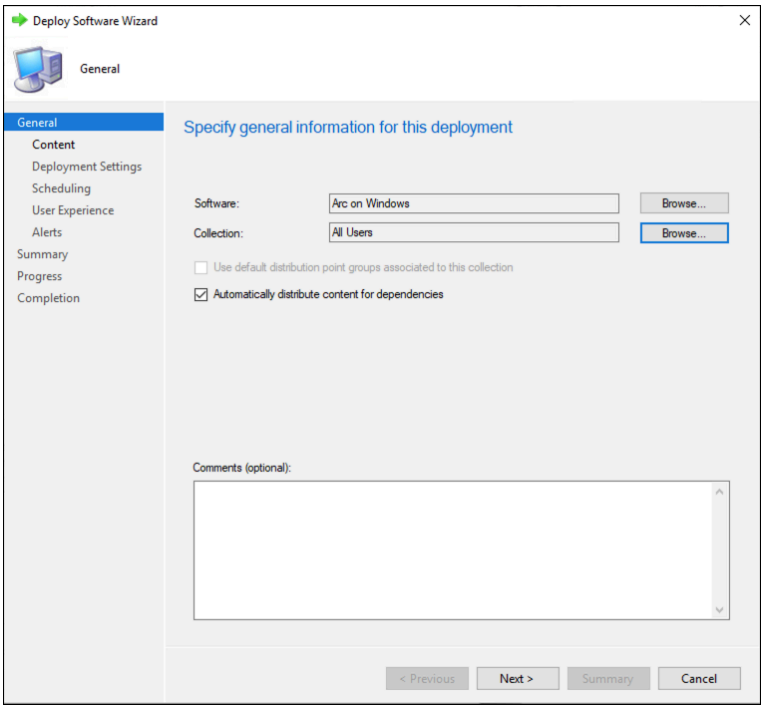


10. Right-click on the application and select **Deploy**.

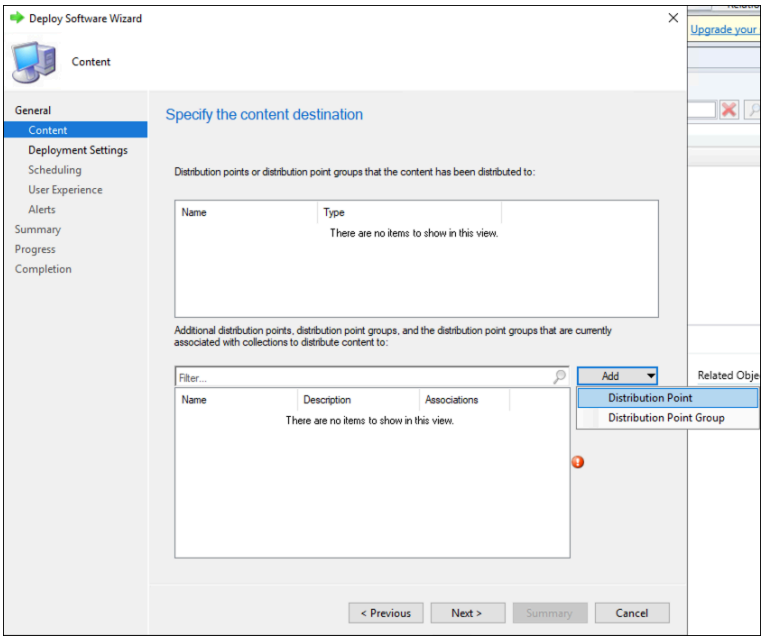


Result: The **Deploy Software Wizard** shows.

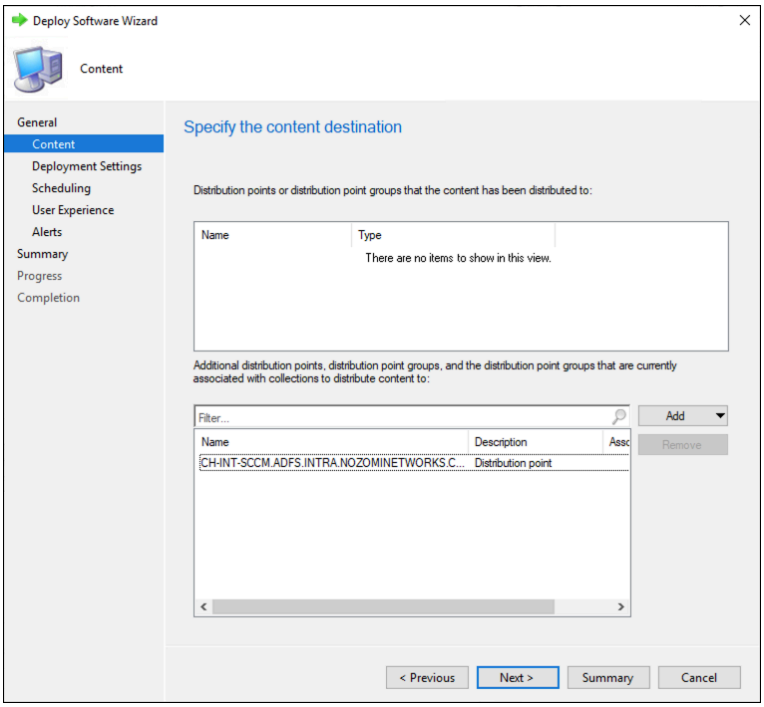
11. On the **General** page, open the **Collection** dropdown and choose the type of deployment. Select **Next**.



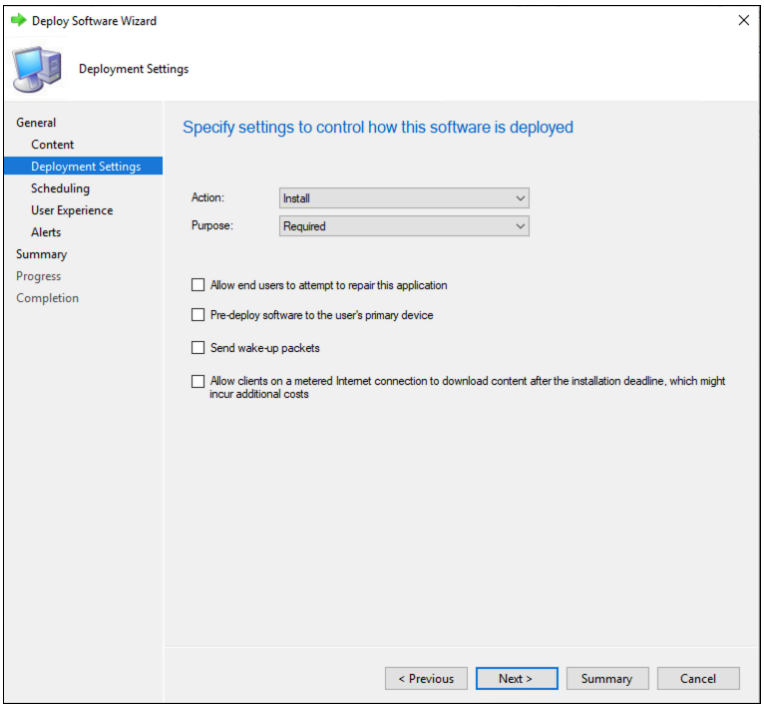
12. On the **Content** page, open the **Add** dropdown and select the type of distribution. Select **Next**.



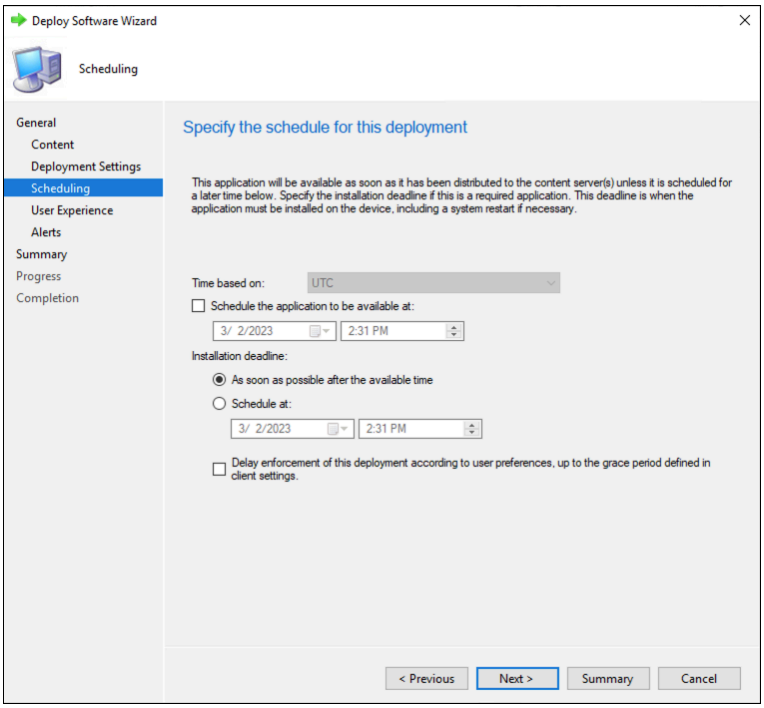
13. Make sure that the distribution point shows in the list, and select **Next**.



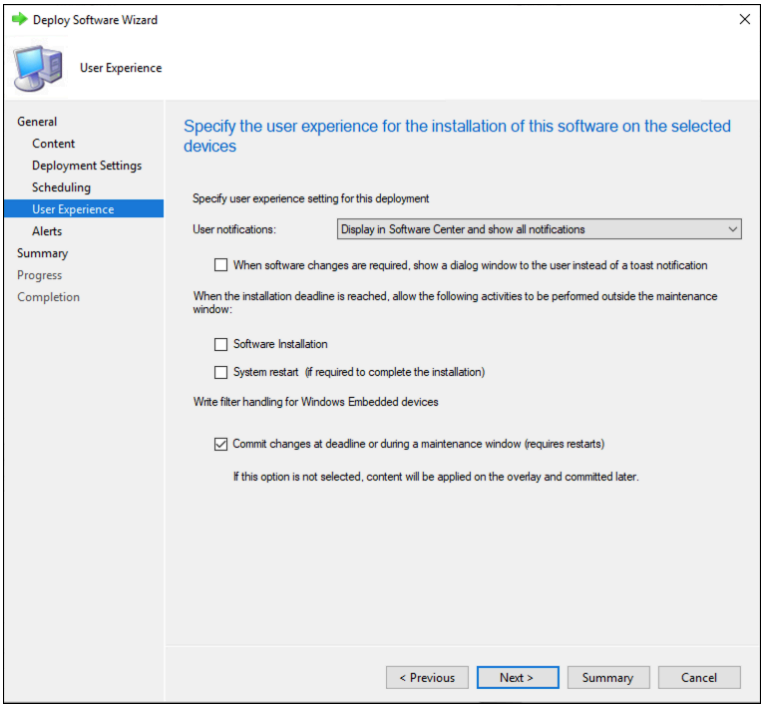
14. On the **Deployment Settings** page, open the **Purpose** dropdown and select **Required**. Select **Next**.



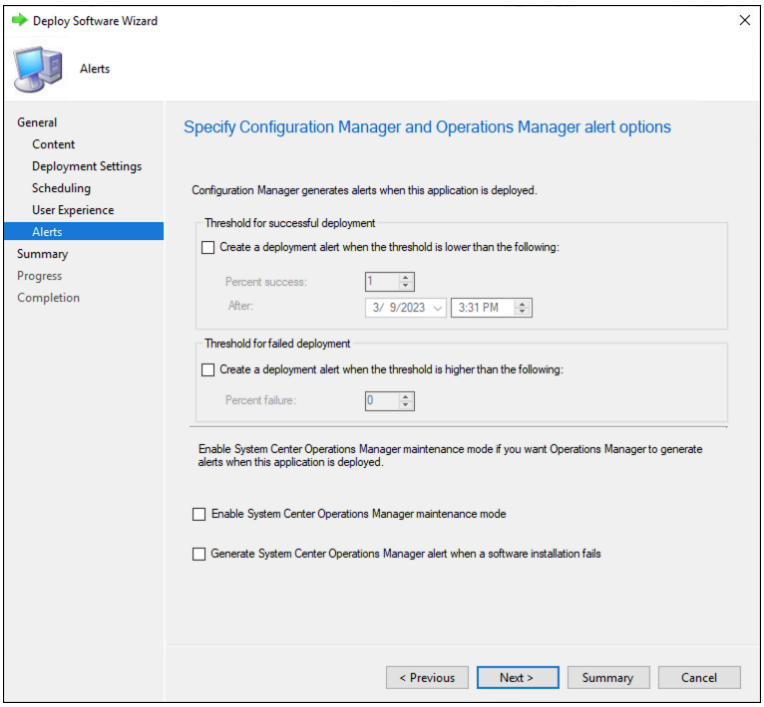
15. On the **Scheduling** page, set the desired schedule settings, and then select **Next**.



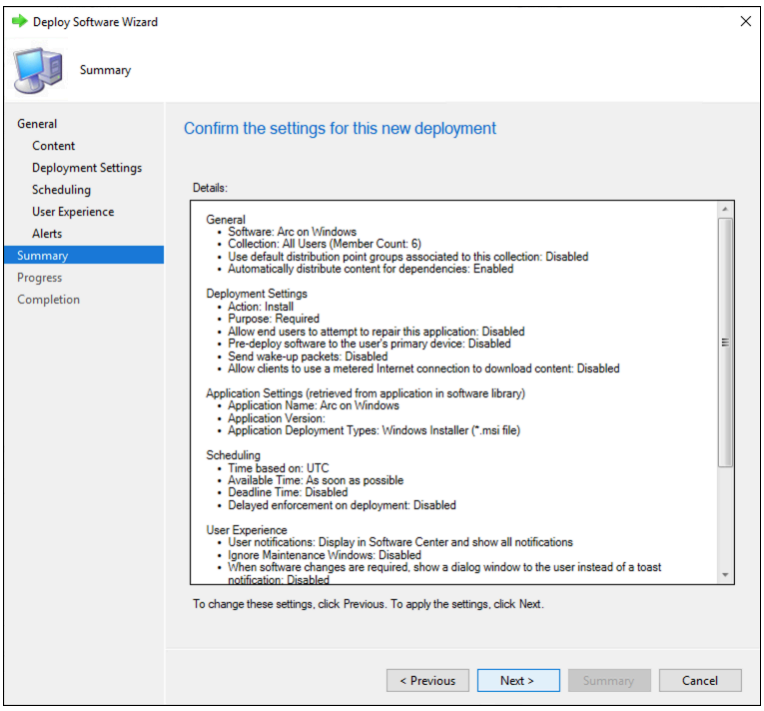
16. On the **User Experience** page, select the desired settings, and then select **Next**.



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



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



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

Results

The deployment starts.

Deploy Arc manually

Download an Arc package

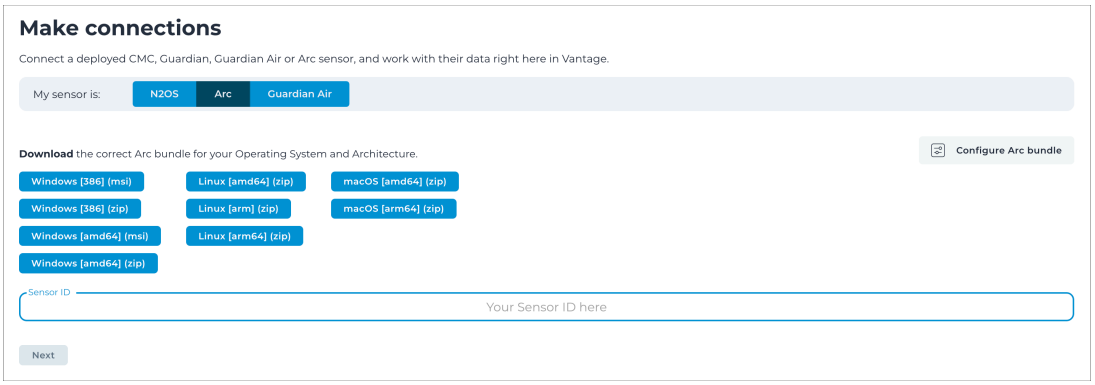
Download an Arc package from Vantage

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.



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.

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

   Result: The **Arc setup wizard** shows.
5. Follow the steps in the wizard.

Results

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

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 65).
4. In the **Configuration** page of the local *UI*, set these parameters:
   a. **Endpoint**: 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 65).
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. **Endpoint** (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 65).
4. In the **Configuration** page of the local *UI*, set these parameters:
   a. **Endpoint**: 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 65).
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 65).
4. In the **Configuration** page of the local *UI*, set these parameters:
   a. **Endpoint**: 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 65).
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 9. 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 10. Elastic notification values - virtual sensors

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

Table 10. 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.

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 65).
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

WinPcap is not installed.

> **Note:**
> If *WinPcap* 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 *WinPcap*.
2. Restart Arc to make sure that *WinPcap* 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 65).
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 65).
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 37).
3. Alternatively, Import Arc through a manual contents upload in Guardian or CMC (on page 38).

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

If you install Arc through Guardian, logs will be created in:
`users/administrator/arc/logs`

This location might be different if Arc was installed:

- Manually
- Through Microsoft Intune
- Through Microsoft Endpoint Manager

> **Note:**
> When Arc is installed with one of the methods above, the user can decide the location of the logs folder.

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`

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 will be 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 address, that is associated with a given internet layer address. This is typically an IPv4 address.

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.

Central Management Console

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

Central Processing Unit

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

Command-line interface

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

Desktop Window Manager

DWM is a 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.

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.

Hypertext Transfer Protocol

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

Hypertext Transfer Protocol Secure

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

Identifier

A label that identifies the related item.

Internet of Things

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

Internet Protocol

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

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.

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.

Operating System

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

Operational Technology

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

Portable Executable

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

Programmable Logic Controller

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

Random-access Memory

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

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.

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.

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.

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 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.

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.

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.