



Aranda Device Management

ADM is a solution that manages the organization's hardware and software IT assets, performing remote monitoring and control tasks. Based on inventory knowledge, you can distribute and keep the software updated on the devices reached.

Knowledge and access to the installation and update stages of ADM allows the user to define and configure the components necessary for the operation of the application. The guidelines to be taken into account are:



## 1. Installation and Access Path

Learn the basic requirements for the correct operation of the application, follow the ADM installation process of the different components for proper operation and access the product interface for the management and control of the discovered devices.

## 2. Update

Identify how to perform updates to functionality components, such as the agent, conserver, and remote support viewer.

## 3. Structures

Learn about the components of the ADM structure and identify how they relate to the overall operation of the product.

## ¿Para quién es esta guía?

This guide is designed to provide the user with a secure path through the ADM installation, configuration, and update process.

## What is our documentation?

- [Aranda Device Management ADM » Getting Started Guide](#)
- [ADM OnPremise Installation and Configuration Guide\(You are HERE\)](#)
- [ADM Cloud » Installation and Configuration Guide](#)
- [Aranda Device Management ADM » Management Manual](#)
- [Aranda ADM Integration Manual »](#)

## ADM OnPremise Installation Path

### ADM Installation Path / OnPremise Architecture

Below is an overview of the concepts of software installation and the different components used for the proper operation of Aranda Device Management ADM.

The process of installing ADM OnPremise Version on a new database should take into account the following steps:



## 1. Requirements

Validate the minimum hardware and software requirements for the installation and operation of Aranda Device Management ADM.

For more information, see the requirements for installing ADM in Cloud environments:

- [System Requirements](#)
- [Requirements / Ports](#)
- [Antivirus Requirements/Exclusions](#)
- [Requirements/Remote Administration](#)
- [Remote Control Requirements/Control](#)

## 2. ADM Installation

The installation of Aranda Device Management ADM in Cloud architectures must take into account the following steps to install the different components:

- [Web Console Installer](#)
- [Installer Conserver](#)
- [Discovery Agent Installer](#)
- [MQTT Broker Installer](#)
- [Mib Browser Installer](#)
- [Remote Control Installer](#)
- [Installer Viewer Remote Support Specialist](#)
- [ADM Agent Installer](#)

## 3. Database Configuration

Configure connection strings to the database for related sites and services.

- [Database Connection Configuration](#)

## 4. Licensing

Manage the licenses acquired by the customer and generate the license request to carry out proper product management.

- [ADM Licensing](#)

## 5. ADM Access

The authentication process to the ADM web console will be executed according to the role defined by the organization to develop the different inventory management tasks.

- [ADM Access](#)

▮ **Note:** If you are installing the ADM software and components on a new database, you can consider the following instructions:

[ADM Installation in New Database](#)

## Requirements

The following settings are recommended for managing between 1 and 2500 devices.

### Server Server

Operating system	Windows Server 2019 and Windows Server 2022
Cores	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz 2.10 GHz
RAM	8 GB
Disk	128 GB (HDD or SSD)

⚠ Bear in mind:

1. A maximum limit of 10,000 devices to keep is recommended to ensure optimal performance, considering the characteristics of the server and ensuring that CPU usage does not negatively affect its operation.
2. When installing a conserver on the same server as the ADM console, a maximum limit of 3,500 devices is recommended.
3. If agents connect directly to an onpremises Repserver, a maximum limit of 3,000 devices is recommended.

### Azure Database Server

Guy	SQL Database (MS SQL 2019 or higher in Standard/Enterprise Datacenter version)
Size	Minimum 5 GB
Additional information	The database must be created with Collate: SQL_Latin1_General_CP1_CI_AI
Remarks	Database space varies depending on the number of devices and modules you have enabled in ADM.

⚠ Note: [See Exceptions](#)

### Workstation Agent

The operating system versions supported by this agent are:

#### Windows

Windows Operating System	Version
Windows 8.1	Pro
Windows 10	Pro
Windows 10	Home
Windows 10	Enterprise
Windows 11	Pro
Windows 11	Home
Windows 11	Enterprise
Windows Server	2016
Windows Server	2019
Windows Server	2022

**Note:**

The (32-bit) label in Task Manager indicates that the process is running in compatibility mode via the [Windows WOW64 subsystem](#), which allows you to run 32-bit applications on 64-bit systems.

Note that depending on your computer and operating system version, this label may not appear. For example, on computers with 32-bit architecture, this ID is not displayed.

The ADM Agent for Windows systems is compiled in x86 (32-bit) format to ensure compatibility on both 64-bit and 32-bit computers. Therefore, it is installed in the C:\Program Files (x86) path.

This condition does not affect the operation of the agent nor does it have implications for its performance or characteristics.

**Mac**

Mac operating system	Version
MacOS	Sequoia
MacOS	Fortune
MacOS	Sonoma

**Note:**

- 1. The following processors are supported: Intel and Apple Silicon M1, M2 and M3
- 2. The agent is not supported for 32-bit versions of MacOS.

# Linux

Linux Operating System	Version
Ubuntu	24.04 LTS
Ubuntu	22.04 LTS
Ubuntu	20.04 LTS
Red Hat	Enterprise Linux 9 LTS
Red Hat	Enterprise Linux 8.7 LTS

📌 **Note:**

- 1. Ubuntu versions are supported for both server and desktop in LTS versions.
- 2. The agent is not supported for 32-bit Linux distributions.

## Requirements/Ports

The following are the communication ports used by Aranda Device Management (ADM). The network needs to be configured to allow communications over these ports.

### ADM Console Server

The following are the ports and permissions required on the ADM console server for the connection of each of the following Components:

### ADM Website

80 (HTTP) or 443 (HTTPS)	TCP, UDP	Input port: Required for connection of clients to the server
--------------------------	----------	--

📌 **Notes:**

- For the update module, the server must have a complete output to the internet for downloading update patches, from the official sites of each provider and their subsequent distribution on managed devices.

📌 **Notes:**

- Configuring the server to allow viewing and downloads of the <https://download.arandasoft.com/updates> site is required to facilitate automatic downloads of agents in ADM

## Remote Control Notifications

443 (HTTPS)	TCP, UDP	Inbound port: Required for agents connection to notification server
8081	TCP	Input Port, intended for the connection of the Specialist Agent and the Workstation Agent with the Turn Server on the remote takeover, the use of SSL must be enabled on the server.
	WebSockets	They establish a persistent two-way connection between the agent and the server.
3478	TCP	Input Port, intended for connecting the Specialist Agent and Workstation Agent to the Stun Server in file transfer.
49152-65535	UDP	Input port, if you require it to operate as a webRTC turn to receive incoming connections. <a href="#">Configuring the Stun/Turn WebRTC Server</a>

📌 **Notes:**  
- It is required to configure the server, to view the site in case of having the Remote Control functionality.  
<https://download.arandasoft.com/updates> and download files

Repserver

80 (HTTP) or 443 (HTTPS)	TCP, UDP	Inbound port: Required for the connection of agents and/or Conserver depending on the implemented architecture
1884 (Optional)	MQTT	Required for output only, used according to the implemented architecture

Repserver Notifications

WebSockets	They establish a persistent bidirectional connection between the ADM agent and the server, which is required for the <a href="#">Remote Administration</a>
------------	--

📌 **Notes:**  
- - Remote administration functionality will only be supported on secure sites with protocol (Https).  

- For remote administration functionality, you must have communication enabled by (TLS 1.2 or 1.3). For communication security, lower versions of TLS are not supported.

Servidor ADM Conserver

Machines on local networks can connect to a Conserver (server on the networklocal) to work with local connections and have additional functionalities.

80 (HTTP) or 443 (HTTPS)	TCP, UDP	Input port: Required for agents connection to the conserver server
1884	MQTT	Required for output only, intended for connection to the MQTT Broker

- 📌 **Notes:**
- For agent distribution devices must be within the same LAN, the devices are required to have the shared admin\$ resource.
  - It is required that the Windows User of Aranda with whom the installation and deployment of Agents will be carried out has Installation permissions, preferably administrator of the corresponding machines.
  - For Linux and Mac operating systems, the use of the root user is required for the deployment of the agent.

## Discovery Agent

When the client requires discovery functionality, it is must enable protocols so that equipment can be found and identified on the local network.

137(Optional)	NETBIOS	Required for egress only, intended for device discovery by the NETBIOS protocol
22(Optional)	SSH	Required for egress only, intended for device discovery by SSH protocol
389 (Optional)	TCP, UDP	Required for output only, intended for discovery by LDAP
161(Optional)	SNMP	Required for egress only, intended for device discovery by SNMP protocol

- 📌 **Notes:**
- Port 80 (HTTP) is required if the server is not configured with HTTPS and the appropriate SSL certificates. The client must enable the HTTPS protocol and not through the HTTP protocol.
  - It is not necessary to always enable all protocols. The ADM Discovery Module allows you to enable the protocols that are required in the process.

## Database Server

The ADM server stores the information on servers, in SQL Server or SQL Azure. If you are using SQL Server as a repository, you need to enable the communications to this server.

1433	TCP	SQL Server protocol input port on the database server
------	-----	---

## MQTT Broker

To generate real-time notifications to devices, you can use a MQTT server on the local network. As a result, you will need to enable the communications to the MQTT Broker.

1884	MQTT	The port of the MQTT Broker can be modified if required. You will only have to enable the entry port on the machine where the MQTT Broker works, for cloud environments it is defined by the Aranda operations area
------	------	---

## ADM Gateway (Onpremises Architecture – ADM versions lower than 9.21.1)

To make remote control connections, it is possible to install an ADM Gateway that allow connection between computers that are on different local networks or when a connection of a computer on a local network with computers in the homes of employees.

4443	TCP	The port of the ADM Gateway can be modified if required. You will only need to enable the inbound port on the machine where ADM Gateway works
------	-----	---

## Aranda ADM Utils Installer (Onpremises Architecture – ADM versions lower than 9.21.1)

Remote Support Viewer is an application that allows you to take remote control of managed machines. It is installed on the users’ devices from which the connection is to be made by remote control, it applies to On-premises architectures

9125 (Optional)	TCP	Outbound Port: Required for remote control between devices that are on the same LAN when not using a Gateway
4443 (Optional)	TCP	Required for egress only, intended for connection to ADM Gateway for remote control between computers on different local networks

## ADM Agents

The Agents are installed on each of the computers that are going to be managed through the through ADM. In conserver architectures, agents are installed on machines through a distributed process guided from the console, however, there are multiple deployment alternatives which can be combined to cover different infrastructure scenarios.

The ports used in ADM vary depending on the architecture and functionalities required.

## ADM Agent

80 (HTTP) or 443 (HTTPS)	TCP, UDP	Required for output only, intended for connection to ADM repserver or ADM Conserver
1884	MQTT	Required for output only, intended for connection to the MQTT Broker
9025 (Optional)	TCP, UDP	Input port: required for server communication with the agent for <a href="#">Remote Management</a> , used when the architecture does not allow the repserver notification server to be displayed for communication. : <a href="https://Dominio/repserver/Notificationmessage">https://Dominio/repserver/Notificationmessage</a> .
	WebSockets (optional)	They establish a persistent bidirectional connection between the ADM agent and the repserver notification server, required for the <a href="#">Remote Management</a> , used when the architecture allows the repserver notification server to be displayed for communication. : <a href="https://Dominio/repserver/Notificationmessage">https://Dominio/repserver/Notificationmessage</a> .
9125 (Optional) - ADM versions lower than 9.21.1	TCP	Input Port: Required for remote control between devices that are on the same LAN when not using a Gateway
4443 (Optional) - ADM versions lower than 9.21.1	TCP	Required for egress only, intended for connection to ADM Gateway for remote control between computers on different local networks

### ADM Agent (With Discovery Capabilities)

137(Optional)	NETBIOS	Ingress port, intended for device discovery by the NETBIOS protocol
22 (Optional)	SSH	Input port, intended for device discovery via the SSH protocol
389(Optional)	TCP, UDP	Inbound port, intended for discovery by LDAP
161(Optional)	SNMP	Input port, intended for device discovery by SNMP protocol

- 📌 **Notes:**
- It is not necessary to always enable all protocols. The ADM discovery allows you to enable the protocols that are required in the process.
  - The ADM agent uses two local ports to establish outbound connection (TCP) such as the connection to the MQTT Broker and communications between agent processes, it handles the ip of the localhost and is dynamic, chosen by the network card, usually ranges greater than 1023 to 65535 are used. It does not require you to do anything in the configuration.

### ADM Agent (With Remote Control Functionality)

For remote control functionality in a cloud and on-premises architecture, the ADM agent installs a Workstation Agent

called "Aranda Remote Control Workstation", for the automatic installation to be performed the ADM agent must be able to visualize the domain of the repserver and everything that is after the installation is performed./ : <https://Dominio/repserver/api/> and download files from that site. To connect to these devices, install the Specialist Agent viewer, taking into account the following [Requirements and ports for the two components of Remote Control Cloud and Onpremises ↗](#).

### Antivirus Requirements/Exclusions

Antivirus programs must be configured with the following inclusions on the computers where the ADM Agent will be installed:

#### Process: Aranda.Agent.ACOREService.exe

Name	Description	Route
Aranda Agent 9	Service Agent	{InstallDir}\Aranda\Aranda Agent 9

#### Proceso:Aranda.Agent.RemoteCommand.exe

Name	Description	Route
	Installation in Computer Discovery	C:\Windows\RemoteCommand \Device\HarddiskVolume3\Windows\RemoteCommand

#### Processes: Aranda.Agent.ARSService.exe

Name	Description	Route
Aranda Agent Remote Control 9	Remote Control Service	{InstallDir}\Aranda\Aranda Agent 9

#### Processes: APaaSPersist.msi

Name	Description	Route
APaaSPersist.msi	Service Agent	{InstallDir}\Aranda\Aranda Agent 9

- If the ADM agent has Remote Control functionality, you must add the following inclusions in the antivirus:

Processes: Aranda.ARC.Workstation.exe

Name	Description	Route
Aranda.ARC.Workstation.exe	ARC Agent Service	{InstallDir}\Aranda\Aranda Remote Control\Workstation

Processes: Aranda.AVS.VNC.Application.exe

Name	Description	Route
Aranda.AVS.VNC.Application.exe	ARC Agent Service	{InstallDir}\Aranda\Aranda Remote Control\Workstation

Processes: Aranda.AVS.TransferFile.Service.Target.exe

Name	Description	Route
Aranda.AVS.TransferFile.Service.Target.exe	ARC Agent Service	{InstallDir}\Aranda\Aranda Remote Control\Workstation

Requirements/Remote Administration Module

Configure remote management based on the installed ADM architecture.

Required Ports and Permits

1. Please read carefully the required ports and permissions based on the ADM installation architecture before moving on to the next point.

- [ADM Agent Onpremises Architecture](#)
- [Web Console, Repserver, Repserver Notification Server](#)

Configuration by Database

- If the communication for remote administration is to be done through the repserver’s notification server, run the following script:

```
SELECT *FROM afw_settings WHERE sett_key='EnableServerNotification'

UPDATE afw_settings SET sett_value = 'true' WHERE sett_key='EnableServerNotification'
```

📌 **Note:** In the detail view of the devices inventoried by ADM, you can view the device information with [Remote Administration](#)

## Remote Control Requirements/Control

### Specialist Agent (Viewer)

To access the remote support features, the specialist agent must be installed on a device that meets the following minimum conditions:

Specialist device	
Virtual processor	2-core CPU
RAM	Minimum 4 GB
Disk Space	Minimum 4 GB

The operating system versions supported by the specialist agent are:

Operating system	Version
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
Windows 10	20H2
Windows 10	21H1
Windows 10	21H2
Windows 10	22H2
Windows 11	21H2
Windows 11	22H2


The supported browsers are as follows:

Browser	Version
Edge	Version >= 88
Google Chrome	Version >= 97.0.4692.71

### Ports used by the Specialist Agent

Port	Protocol	Description
443	TCP	Required for the Specialist Agent’s connection to the Recording server, he must be able to view the site: https://Dominio/adm/arc/recording
8081	TCP	Required only for output, intended for the connection of the Specialist Agent with the Turn Server at the remote takeover.
	WebSockets	They establish a persistent two-way connection between the agent and the server.
3478	TCP	Required only for output, intended for the connection of the Specialist Agent with the Stun Server in the file transfer.
15000 - 65000	UDP	Range required only for output, intended for the connection of the Specialist Agent with the Stun Server in the file transfer.

## Workstation Aranda Remote Control Agent

 **Important:** You cannot have the AVS Agent and the Aranda Remote Control (ARC) Agent installed simultaneously on the same workstation. Conflicts can be generated between both agents, preventing proper use.

The minimum conditions for installation that the workstation must meet are:

Workstation Requirements	
Virtual processor	2-core CPU
RAM	Minimum 4 GB
Disk Space	Minimum 400 MB

The operating system versions supported by this agent are:

Operating system	Version
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
Windows 10	20H2
Windows 10	21H1
Windows 10	21H2
Windows 10	22H2
Windows 11	21H2
Windows 11	22H2
Windows Server 2016	
Windows Server 2019	1809
Windows Server 2022	

Ports used by the Workstation Agent.

Port	Protocol	Description
443	TCP	Required for the Workstation Agent connection to the Notifications server, you must be able to view the site: <a href="https://Dominio/adm/arc/notification">https://Dominio/adm/arc/notification</a>
8081	TCP	Required only for output, intended for connecting the Workstation Agent to the Turn Server on the remote control socket.
	WebSockets	They establish a persistent two-way connection between the agent and the server.
3478	TCP	Required for output only, intended for connecting the Workstation Agent to the Stun server in file transfer.
15000 - 65000	UDP	Range required only for output, intended for the connection of the Workstation Agent with the Stun server in file transfer.

Local Ports Used for Internal Agent Process Communication

Port	Protocol	Description
5050	WebSocket	Used by Aranda.ARC.Workstation.exe to receive messages and requests from other processes
5029	GRPC	Used by Aranda.AVS.TransferFile.Service.Target.exe to receive file transfer requests
9087	GRPC	Used by Aranda.AVS.VNC.Application.exe to receive remote control requests

- 📌 **Notes:**
- The workstation agent should be able to display the next repserver path for automatic agent update and everything after / : <https://Dominio/repserver/api/> and download files from that site

## ADM Installer/Web Console

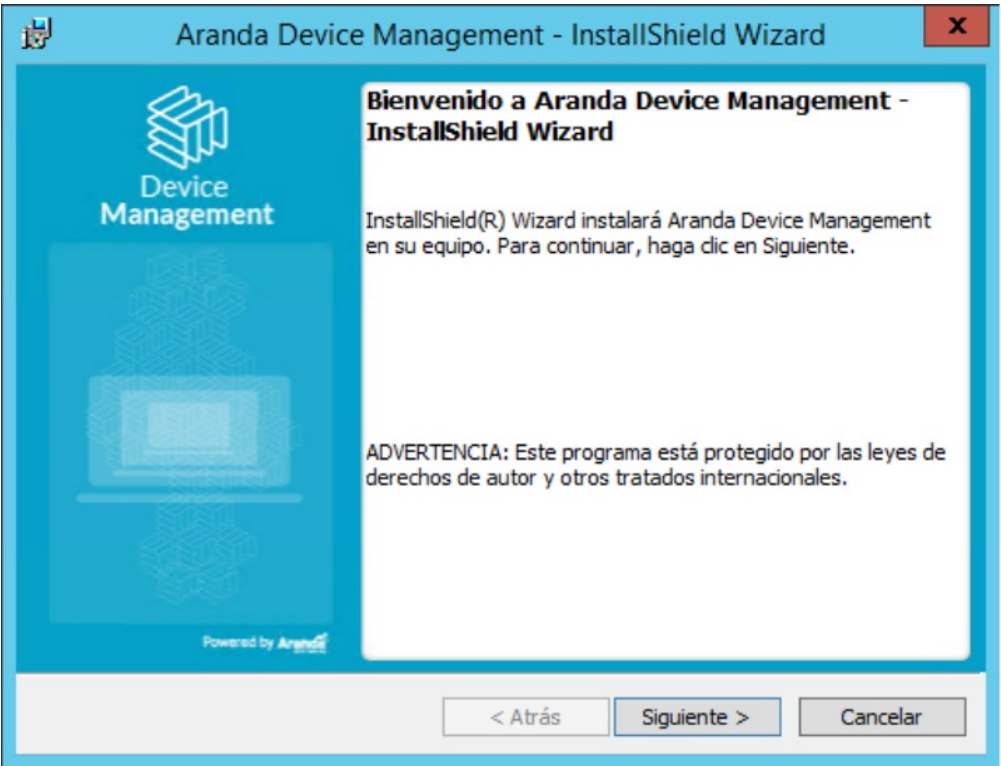
### OnPremises Windows Server Installation Requirements

- [Role and feature activation.](#)
- [Installing the .NET Framework Version 4.8](#)
- [Installing Windows Hosting Bundle Installer](#)

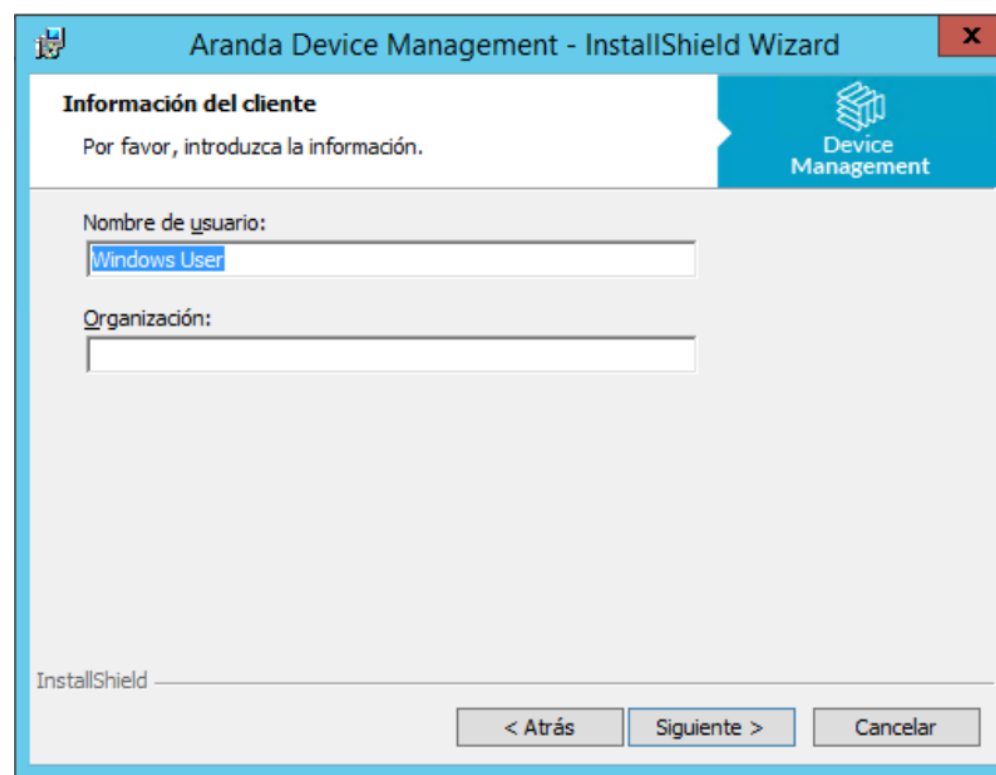
### ADM Console Installer

The installer `Aranda.ADM.Web.Installer` from the ADM web console, installs the console sites, the Repserver, and the Remote Control (Notifications and Recordings) sites; additionally, it creates the Crunchers, License, Scheduler, Worker, Turn Stun WebRTC and Turn Server services that are used in the application. Here is the step-by-step of the installation.

1. Clicking on the installer will launch the installation wizard. ClickFollowing.



2. Enter the customer information and clickFollowing.



**Aranda Device Management - InstallShield Wizard**

**Información del cliente**  
 Por favor, introduzca la información.

Nombre de usuario:

Organización:

InstallShield

< Atrás    Siguiente >    Cancelar

3. Select the full installation type and click Following.



**Aranda Device Management - InstallShield Wizard**

**Tipo de instalación**  
 Elija el tipo de instalación que se adapte mejor a sus necesidades.

Seleccione un tipo de instalación.


☒ **Completa**  
 Se instalarán todos los componentes del programa. (Necesita más espacio en disco).

☐ **Personalizada**  
 Elija los componentes del programa que desee instalar y la ubicación en que se instalarán. Recomendada para usuarios avanzados.

InstallShield

< Atrás    Siguiente >    Cancelar

4. Click Install.



**Aranda Device Management - InstallShield Wizard**

**Preparado para instalar el programa**  
 El Asistente está preparado para comenzar la instalación.

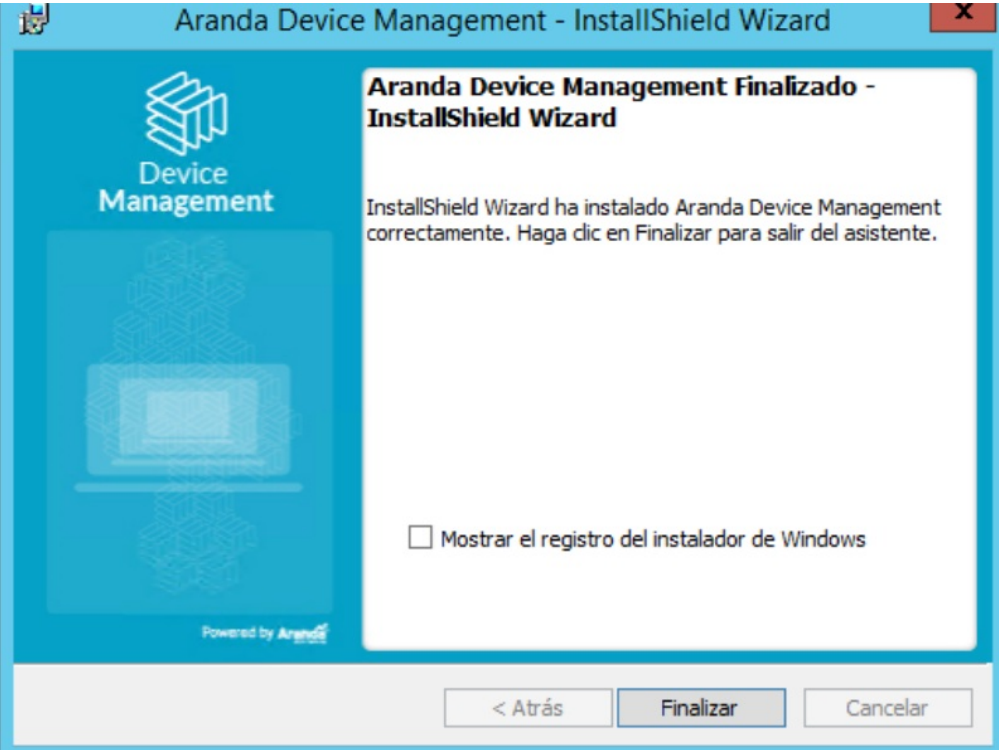
Haga clic en Instalar para comenzar la instalación.

Si desea revisar la configuración de la instalación o realizar algún cambio, haga clic en Atrás. Haga clic en Cancelar para salir del Asistente.

InstallShield

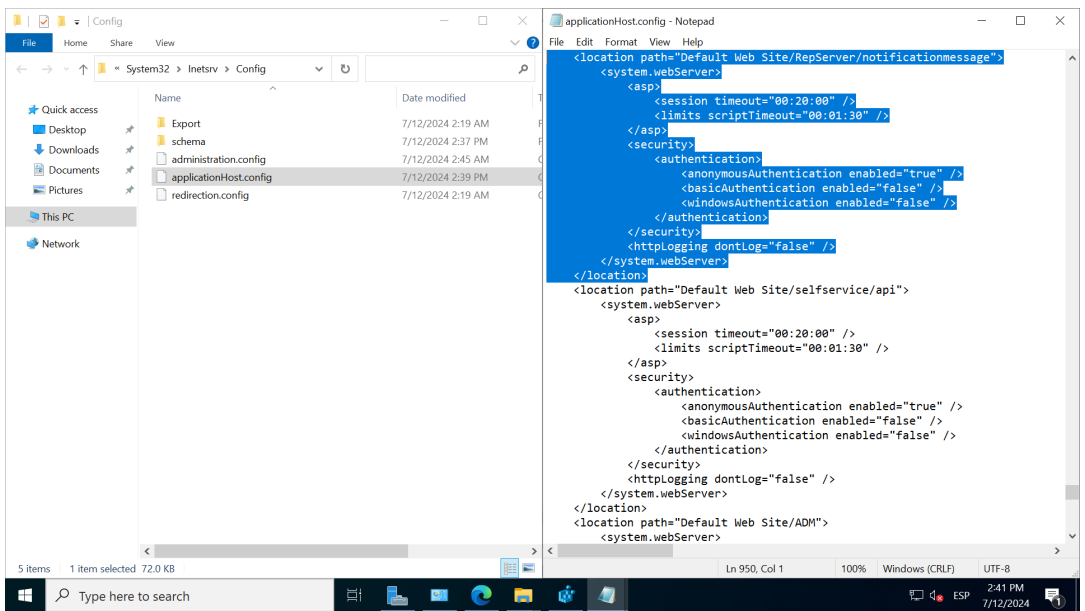
< Atrás    Instalar    Cancelar

5. Once the installation process is complete, click End.



Note:

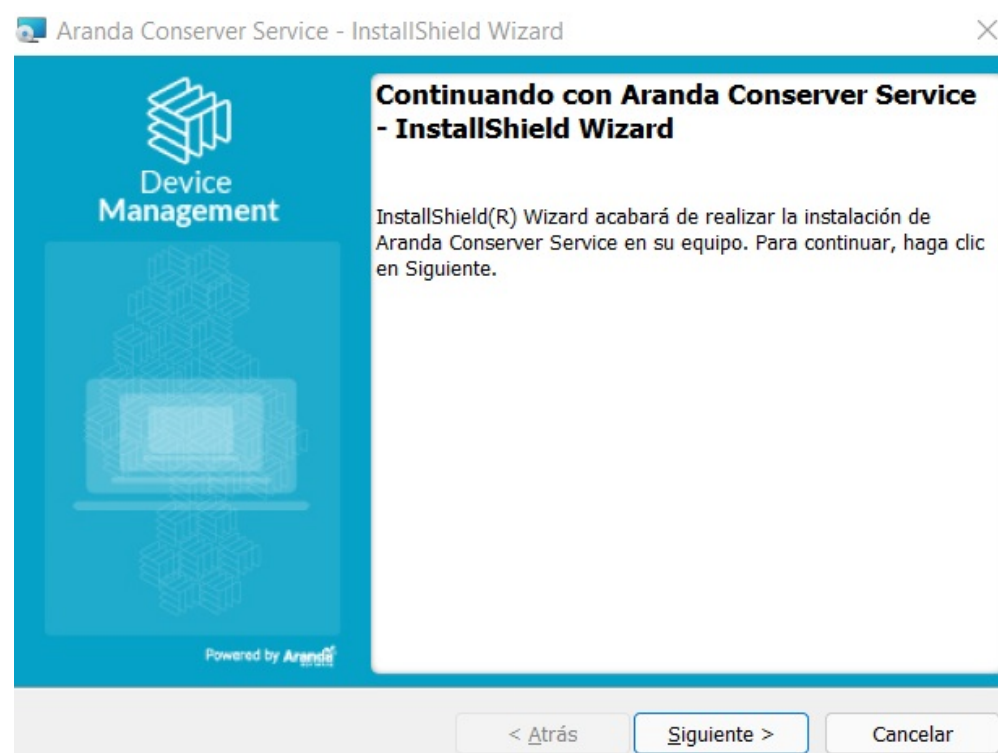
- If the ADM website does not upload correctly, check that the requirements have been executed according to the defined order; Run the installers again by repairing the installation
- If the error persists, find the WinDir%\System32\Inetsrv\Config\applicationHost.config file and remove the location tag that corresponds to the site "Repserver/notificationmessage" and restart the IIS



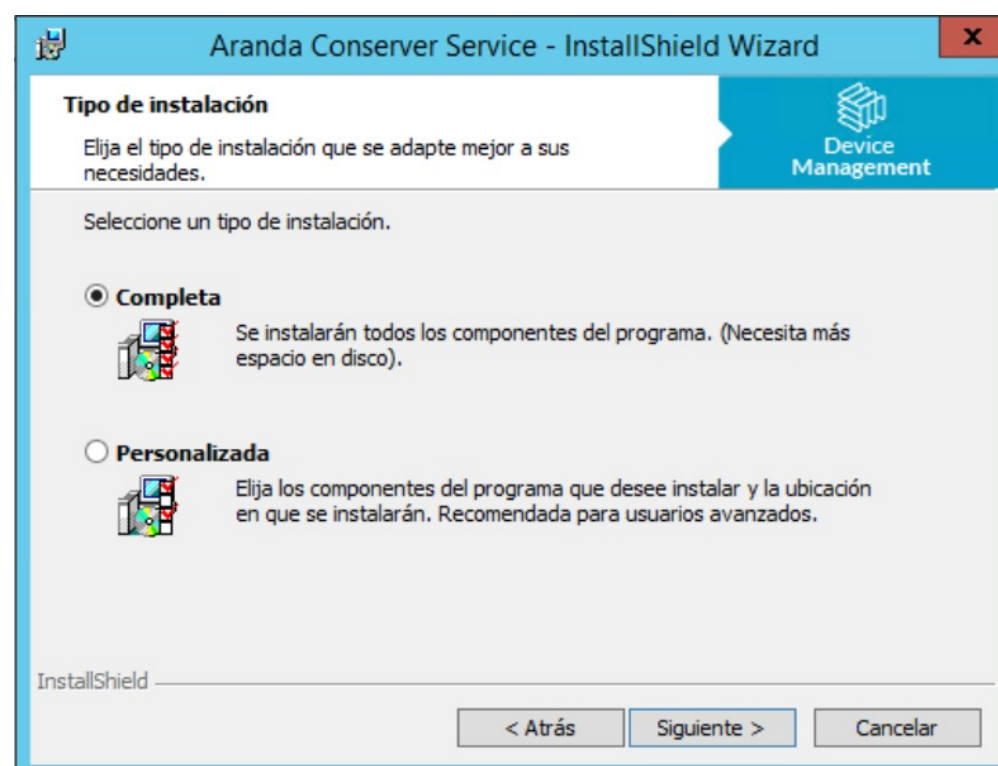
Installer/Serverer

The second installer is Aranda.Conserver.Installer. A service must be installed for each network segment.

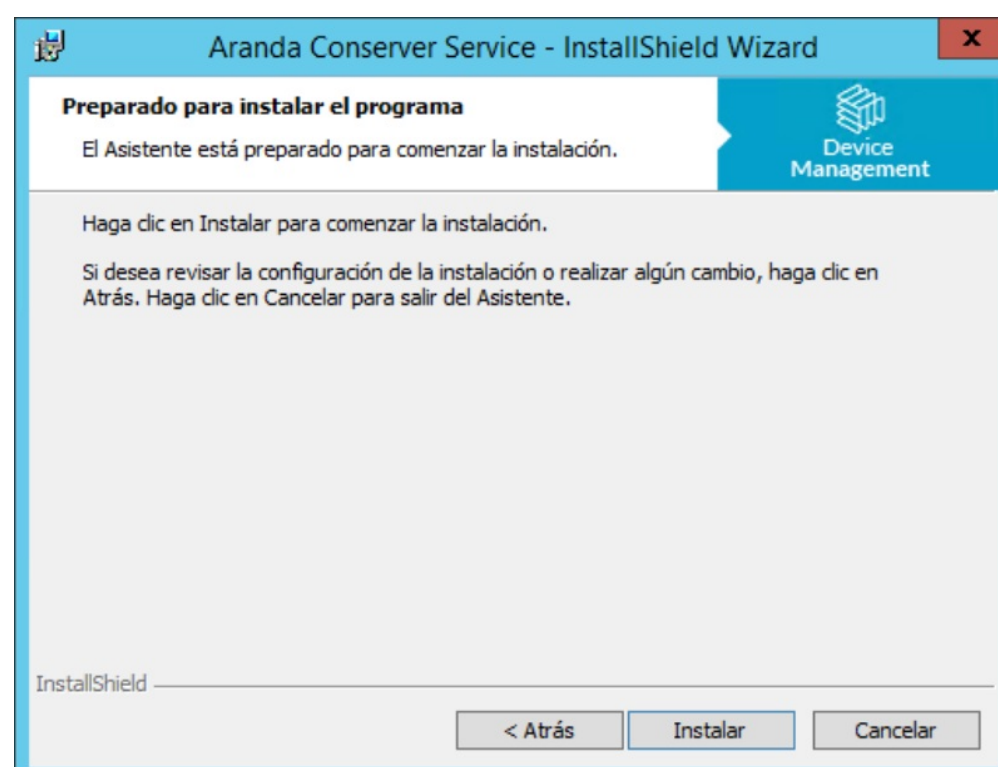
1. Clicking on the installer will launch the installation wizard.



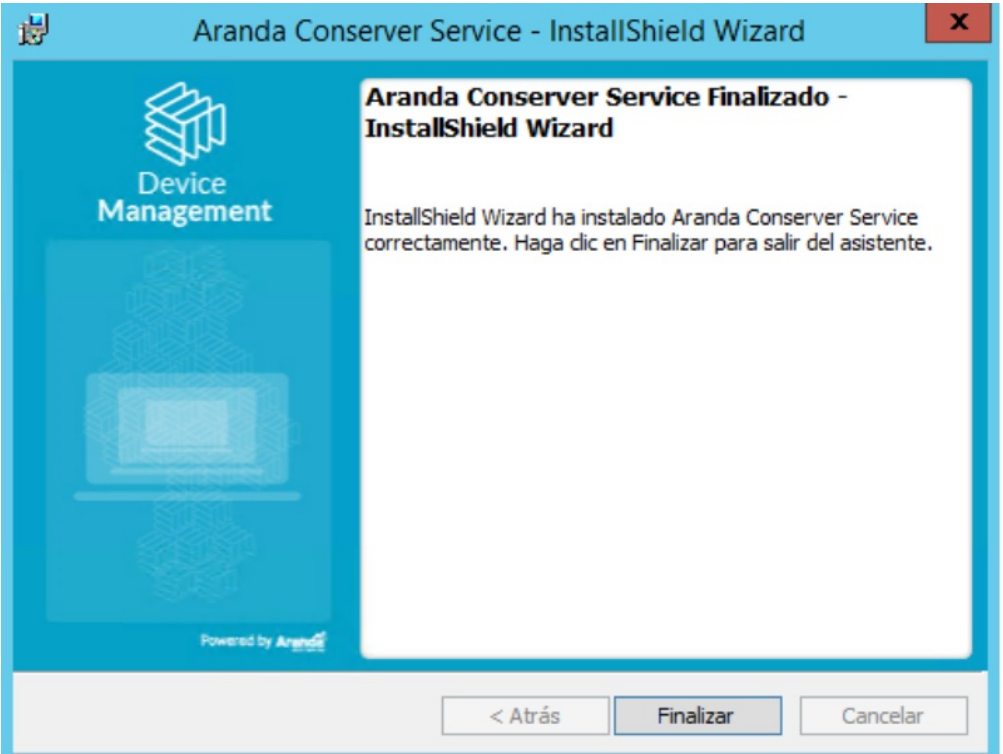
2. Select the full installation type and click Following.



3. Click Install.



4. When the installation process is complete, click End.



—

- 🔗 Related Links:
- [Conserver Configuration](#)
  - [Conserver Console Configuration](#)

## Conserver Configuration

## Conserver Configuration

[« Installer Conserver](#)

1. When you install a Conserver, all files are saved in the path `C:\Program Files (x86)\Aranda\Conserver`, Configure the `Aranda.Conserver.Windows.Service.exe.config` in the following way to communicate with the Repserver:

AppSettings Settings		
<hr/>		
<code>add</code> <code>key="dataConfiguration:defaultDatabase"</code> <code>value="local" /</code>		It is used to set the default database to be used in the application.
<code>add key="Serilog:MinimumLevel"</code> <code>value="Debug"</code>		Used to set the minimum level of event logging for the Serilog log library.
<code>add key="Serilog:WriteTo:0:Name"</code> <code>value="File"</code>		Used to specify the first log target to be used for Serilog. The value "File" indicates that log events will be written to a file.
<code>add key="Serilog:WriteTo:0:Args:path"</code> <code>value="Logs\log.txt"</code>		It is used to specify the path and name of the file where log events will be written.
<code>add key="Serilog:WriteTo:0:Args:shared"</code> <code>value="true"</code>		It is used to specify whether the log file should be shared by multiple processes or not.
<code>add</code> <code>key="Serilog:WriteTo:0:Args:rollingInterval"</code> <code>value="Day"</code>		Used to specify the time interval at which new log files are created.
<code>add key="Logging:LogLevel:Default"</code> <code>value="Information"</code>		It is used to set the default logging level for the Microsoft logging library.
<code>add key="serverAddress" value=""</code>		Address where the Repserver is located
<code>add key="enableProxy" value="false"</code>		If you use Proxy, the enableProxy tag is enabled with a value of "true"

AppSettings Settings	
add key="proxyAddress" value=""	Proxy address
add key="proxyUser" value=""	Proxy User
add key="proxyPassword" value=""	Proxy Password
add key="logLevel" value="Information"	Verbosity level log of the conserver; "Information", "Debug", "Detailed", "Verbose". By default it is parameterized in "Information"
add key="privateIp" value=""	Identifier on the internal network of the Conserver, should ia the ip
add key="publicIp" value=""	Consevar network identifier from the outside, the ip must go. (In case it is not required, the same private address is placed)
add key="mqttServerPort" value="1884"	MQTT Communication port, by default "1884" is parameterized
add key="mqttIp" value=""	Mqtt identifier on the internal network, the IP must go
add key="publicServerPort" value="80"	Conserver's public network communication port, by default "80" is parameterized.
add key="privateServerPort" value="80"	Conserver private network communication port, by default "80" is parameterized.
add key="p2pPort" value="9501"	Port for p2p connections, by default the "9501" is parameterized
add key="maxDistributionSleepMsPerThread" value="8"	-
add key="maxDistributionThreads" value="4"	These last two tags are used for the internal functioning of the system, they must be modified

```
<appSettings>
  <add key="dataConfiguration:defaultDatabase" value="local" />
  <add key="Serilog:MinimumLevel" value="Debug" />
  <add key="Serilog:WriteTo:0:Name" value="File" />
  <add key="Serilog:WriteTo:0:Args:path" value="Logs\log.txt" />
  <add key="Serilog:WriteTo:0:Args:shared" value="true" />
  <add key="Serilog:WriteTo:0:Args:rollingInterval" value="Day" />
  <add key="Logging:LogLevel:Default" value="Information" />
  <add key="serverAddress" value="" />
  <add key="enableProxy" value="false" />
  <add key="proxyAddress" value="" />
  <add key="proxyUser" value="" />
  <add key="proxyPassword" value="" />
  <add key="privateIp" value="" />
  <add key="publicIp" value="" />
  <add key="mqttServerPort" value="1884" />
  <add key="mqttIp" value="" />
  <add key="publicServerPort" value="80" />
  <add key="privateServerPort" value="80" />
  <add key="p2pPort" value="9501" />
  <add key="maxDistributionSleepMsPerThread" value="8" />
  <add key="maxDistributionThreads" value="4" />
  <add key="enableDiscoveryCommon" value="1" />
  <add key="SecondsPingRemoteServer" value="60" />
  <add key="enableSecurity" value="false" />
</appSettings>
```

2. Start the service Aranda Conserver V9, to allow communication with the Repserver.

Aranda Conserver V9

En ejecu...

Automático

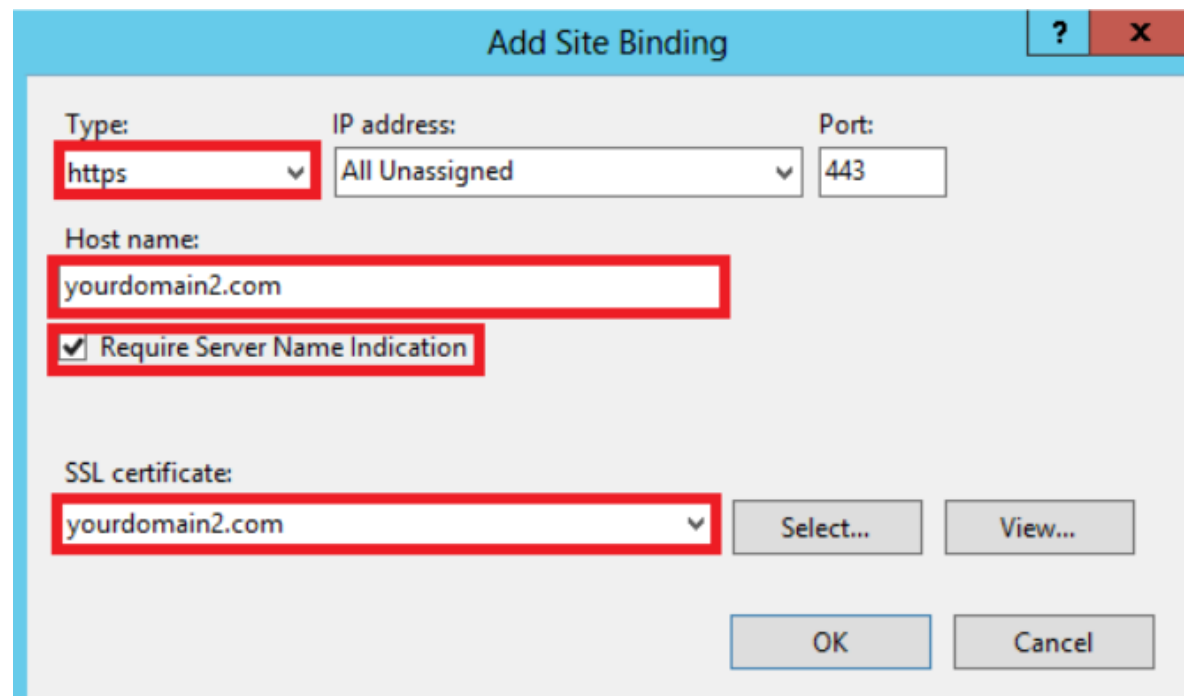
Sistema local

## Configuring the conserver to receive requests over https

To configure the conserver to receive https requests, https must be enabled in the iis with the proper certificate.

Important to secure any additional hostnames using SNI.

IP address: select "All unassigned".



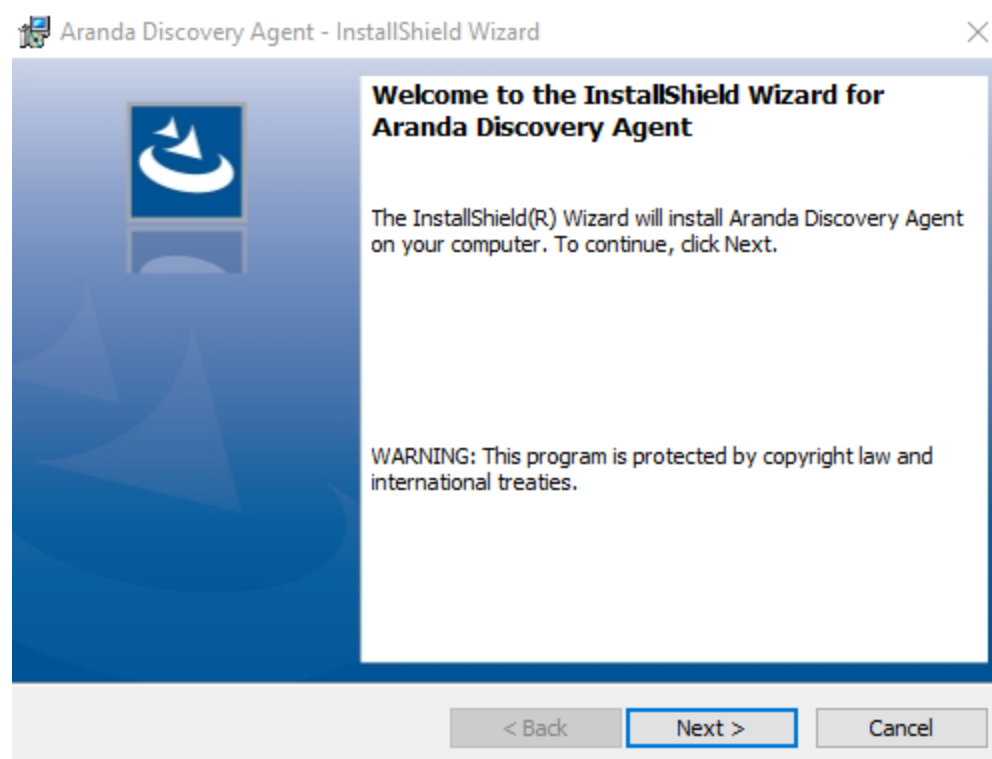
The value of the label "enableSecurity" must be equal to "true"

```
<appSettings>
  <add key="serverAddress" value="https://IP_SERVER/repserver"/>
  <add key="enableProxy" value="false"/>
  <add key="proxyAddress" value=""/>
  <add key="proxyUser" value=""/>
  <add key="proxyPassword" value=""/>
  <add key="logLevel" value="Information"/>
  <add key="privateIp" value="IP_SERVER"/>
  <add key="publicIp" value="IP_SERVER"/>
  <add key="mqttServerPort" value="1884"/>
  <add key="mqttIp" value="IP_SERVER"/>
  <add key="publicServerPort" value="443"/>
  <add key="privateServerPort" value="443"/>
  <add key="p2pPort" value="9501"/>
  <add key="maxDistributionSleepMsPerThread" value="8"/>
  <add key="maxDistributionThreads" value="4"/>
  <add key="enableDiscoveryCommon" value="1"/>
  <add key="SecondsPingRemoteServer" value="60"/>
  <add key="enableSecurity" value="true"/>
</appSettings>
```

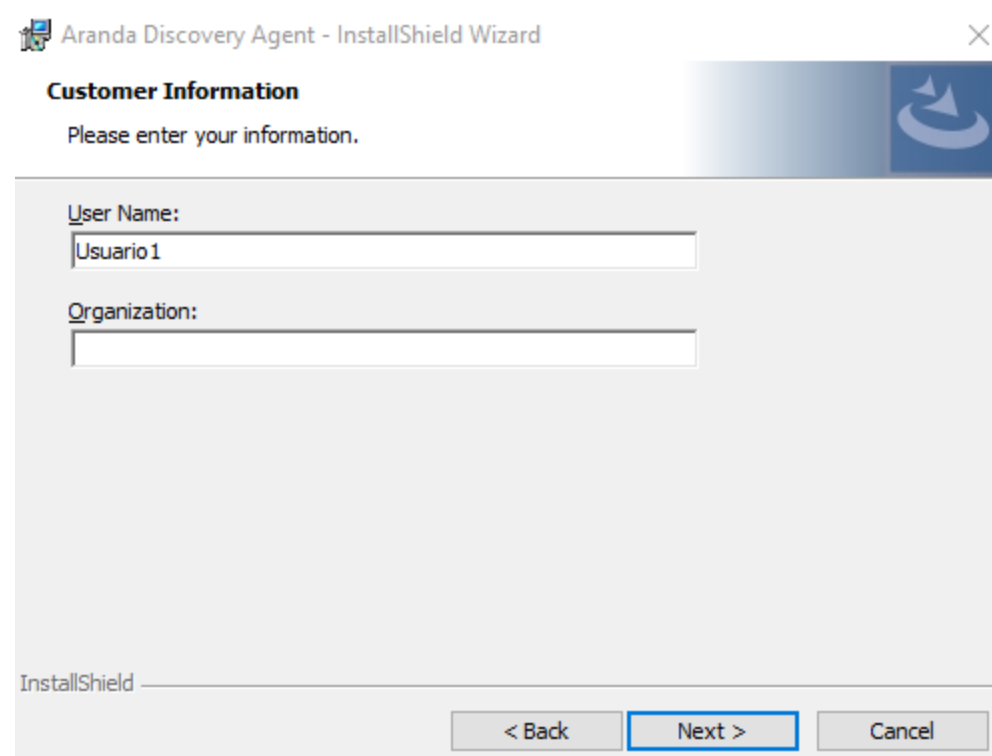
[« Installer Conserver](#)

## Installer/Discovery Agent

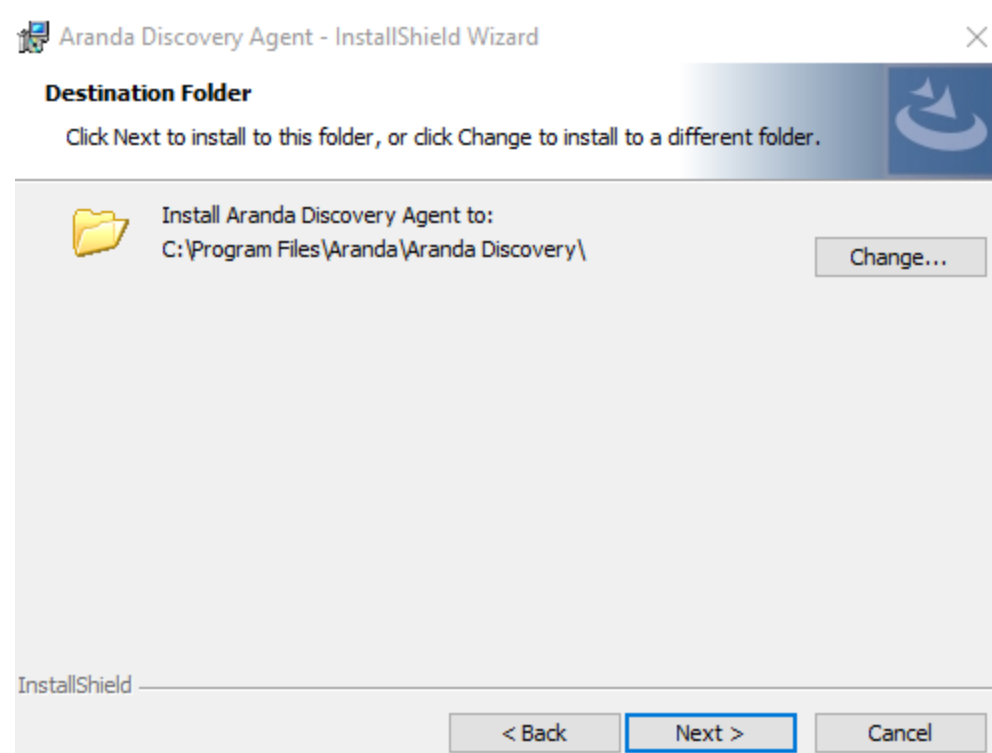
1. Run the installer Aranda.Discovery.Agent.x.x.x.exe



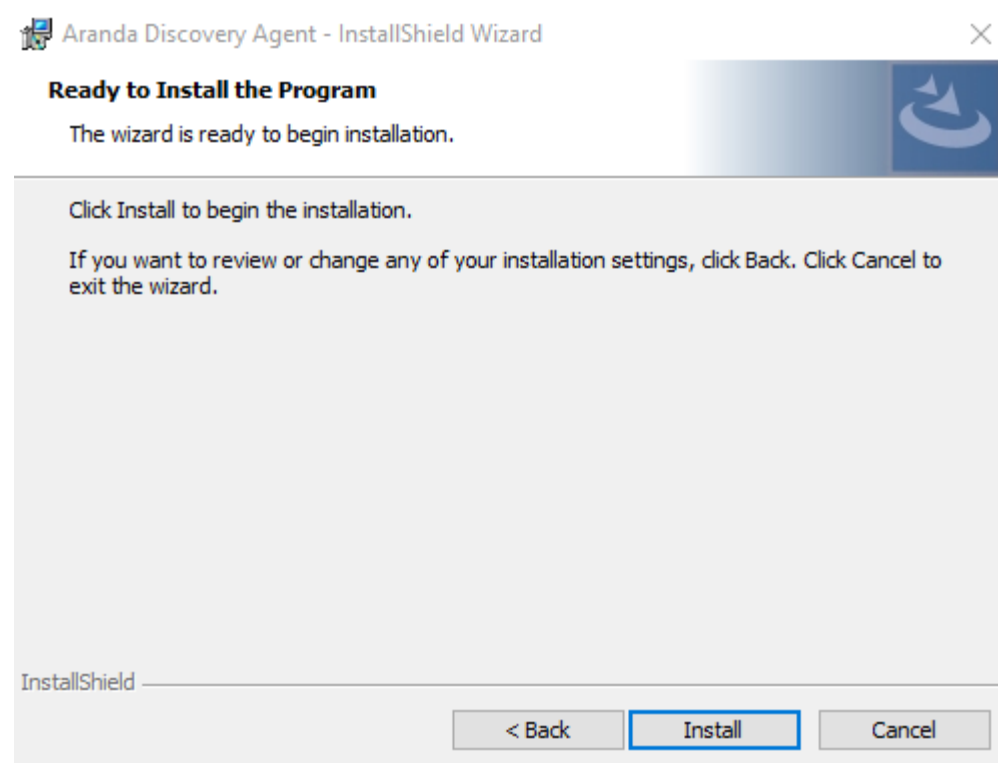
2. In the Customer Information window, enter the user name, organization, and click Following. These fields may be left empty.



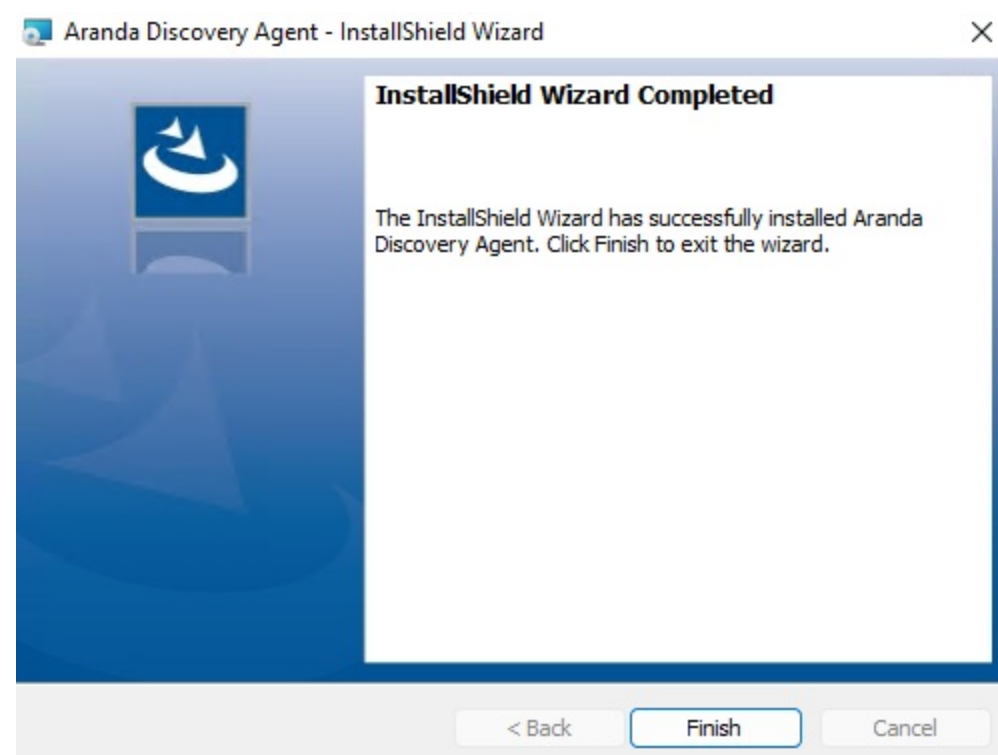
3. In the Destination Folder window, you can change the installation path of the service or leave it by default where the installation suggests, then click Following.



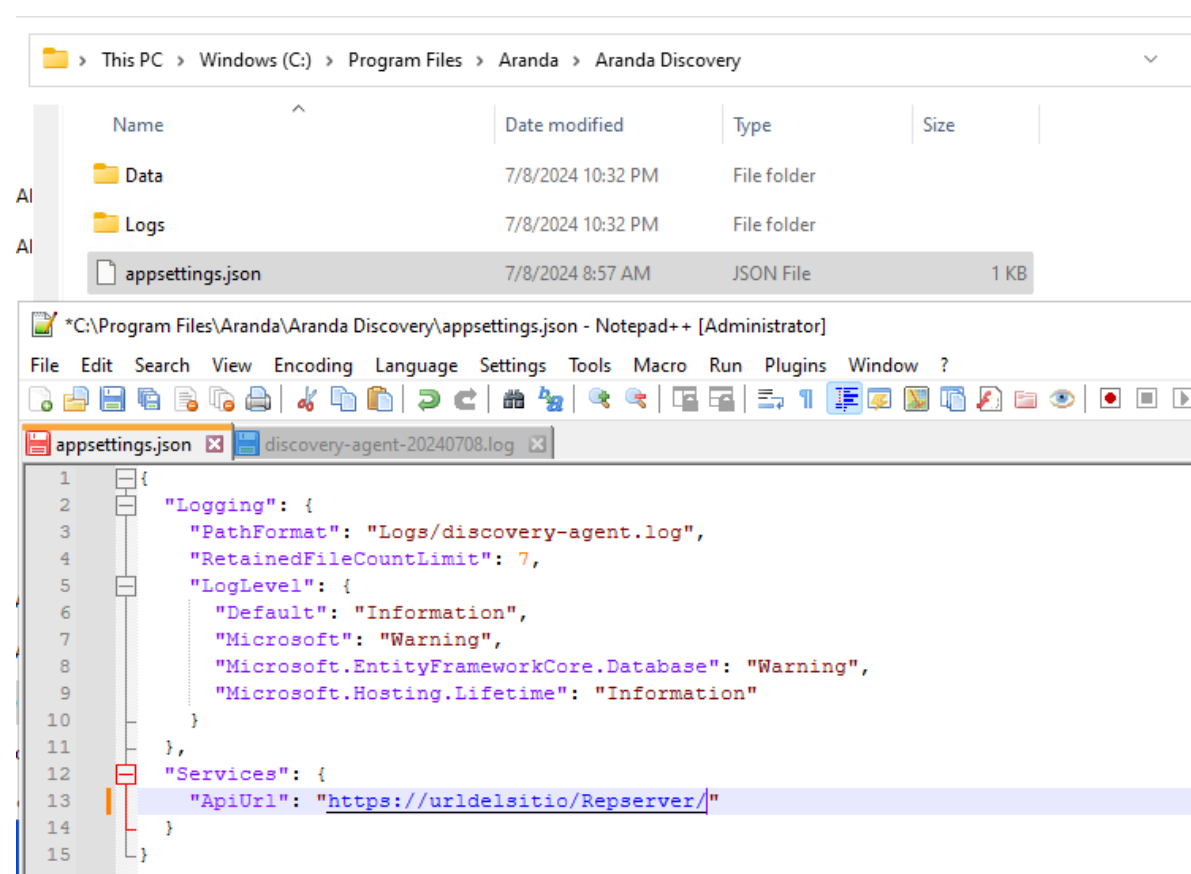
4. Click Install; You must have permissions as a machine administrator.



5. When the installation process is finished, click the End.

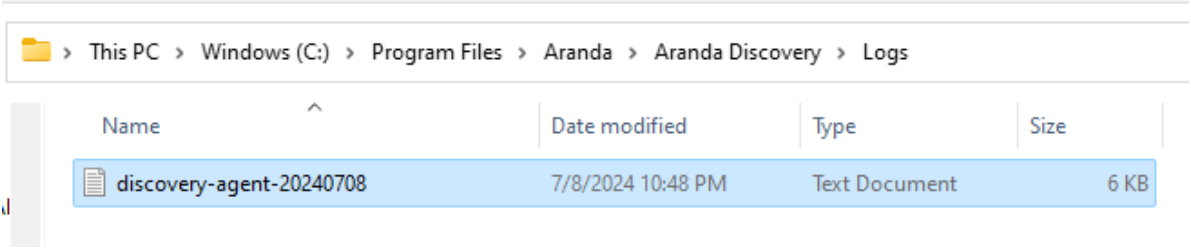


6. To configure the discovery agent, open the appsettings.json in the folder where the service is installed and in the Services in ApiUrl, enter the URL of the site's Repserver.



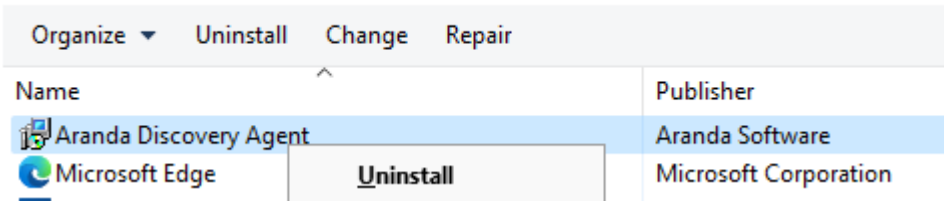
7. Once the AppSettings go to the services and verify that the service: Aranda Discovery Agent is installed, then restart the service so that it takes the changes configured in the AppSettings.

8. The archives of Log will be stored in the following path: C:\Program Files\Aranda\Aranda Discovery\Logs

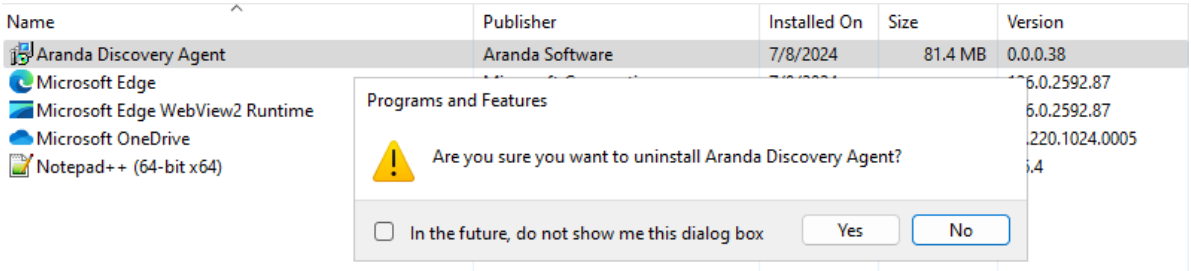


### Uninstalling the Discovery Agent

1. Enter the control panel and right-click on the app Aranda Discovery AgentSelect uninstall.



2. To the question “Esta seguro que quiere desinstalar Aranda Discovery Agent?”, click the SI button in the message.



3. Check the service again and the folder where the service was installed, the record should no longer appear.

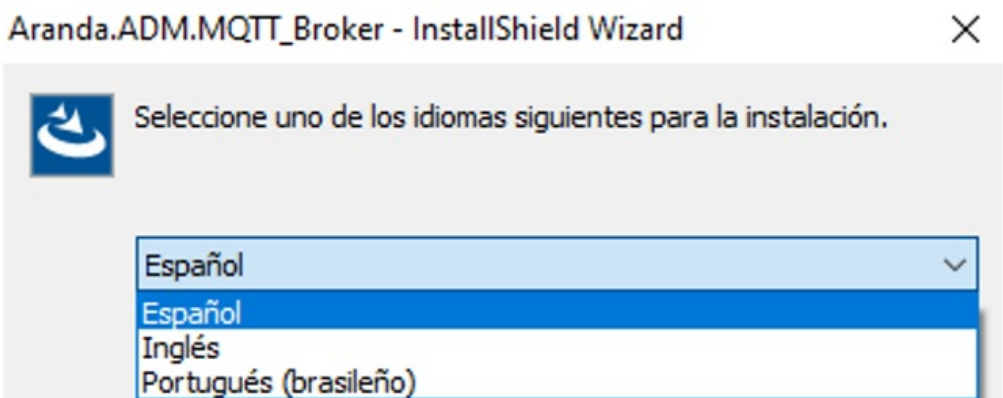
### Automatic Discovery Agent Update

1. The discovery agent will automatically update within one day of the ADM site update.

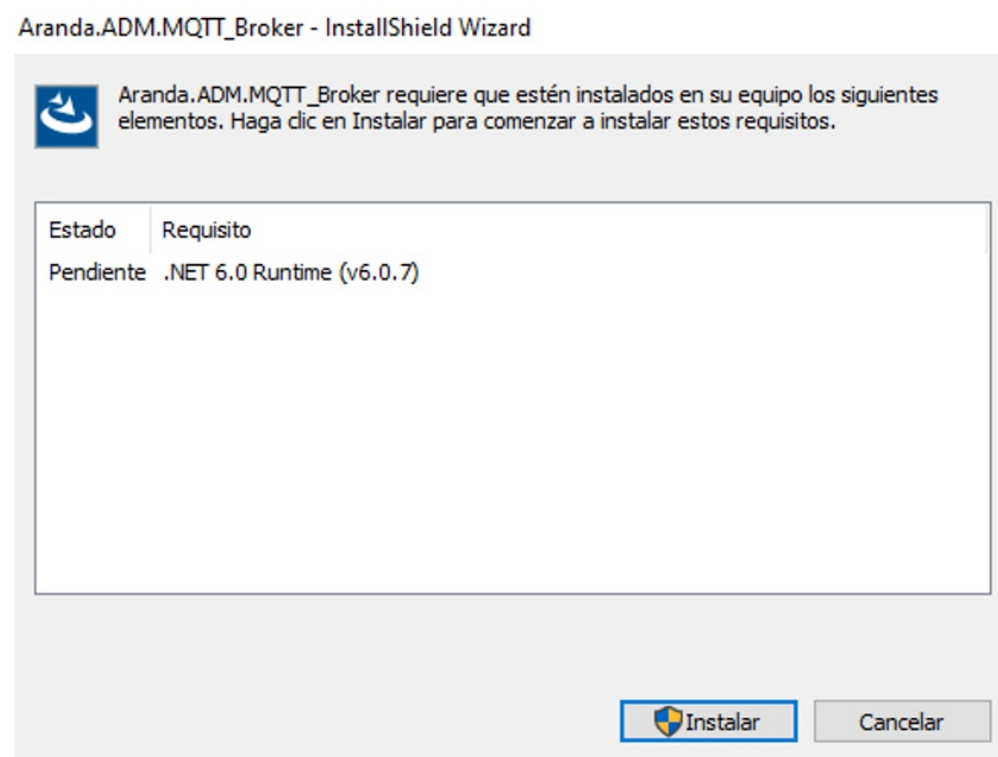
### MQTT Broker Installer/Washer

**Note:** A maximum number of 10,000 connections (devices) per MQTT broker server is suggested.

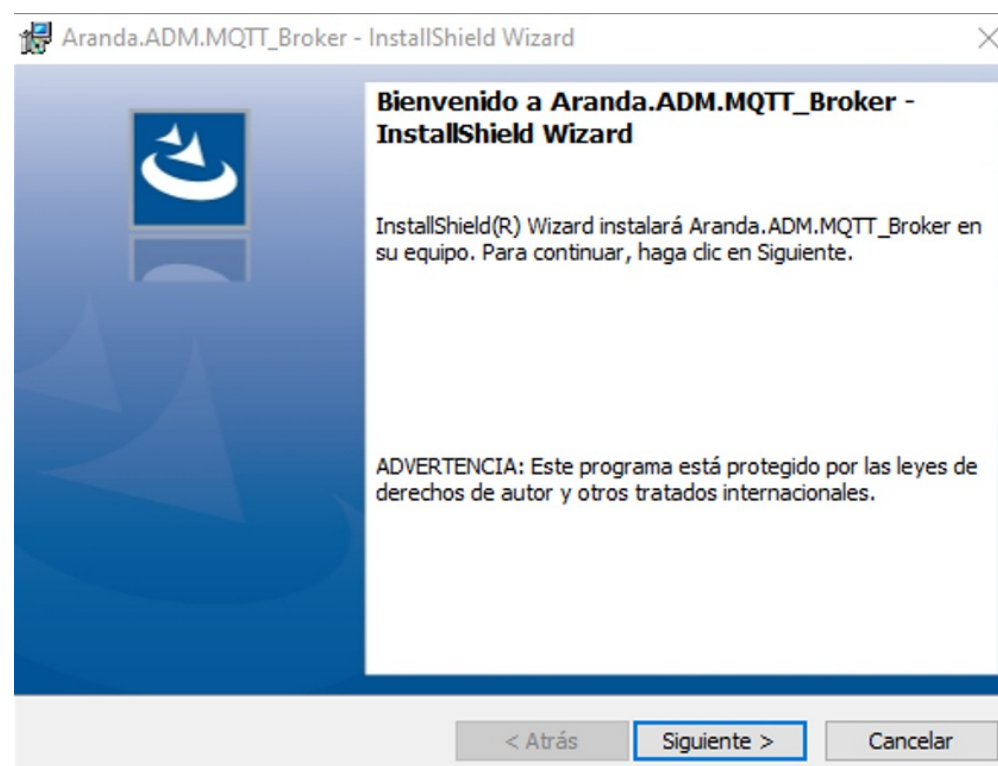
- 1. Run the installer Aranda.ADM.MQTT.Broker.exe
- 2. Define the language for the installation process.



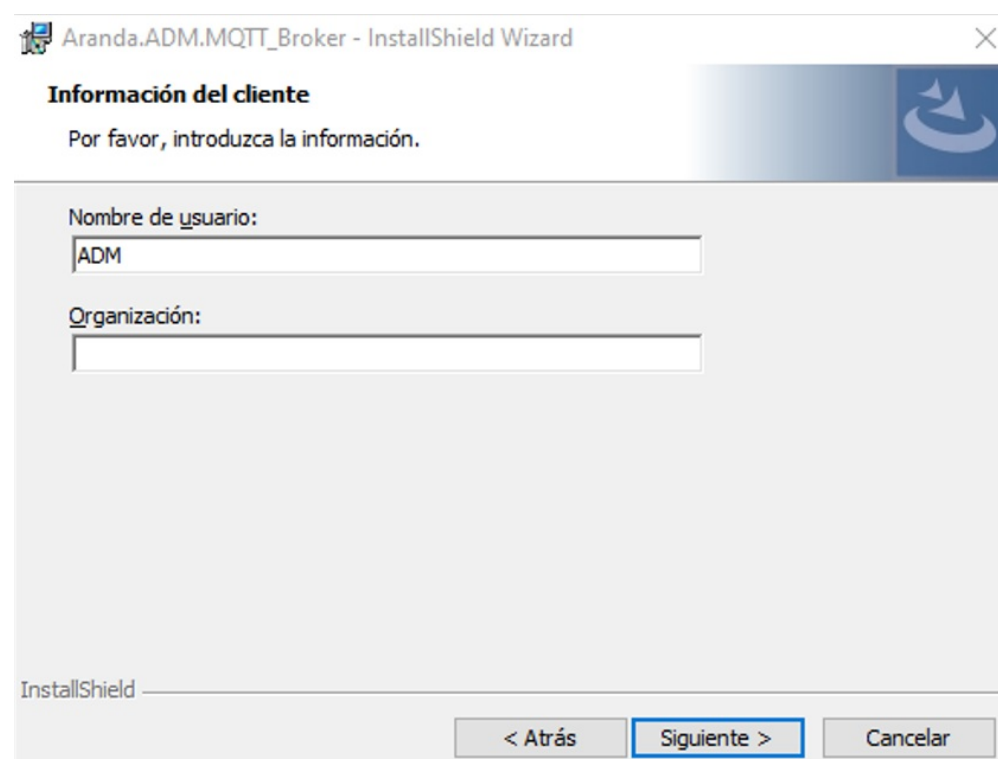
3. The installer validates the prerequisites that must be met to configure the Aranda broker. If this is not met, the system will install the required information.



4. When you finish installing the requirements, you will be able to see the welcome screen. Confirm the installation by clicking the Following.

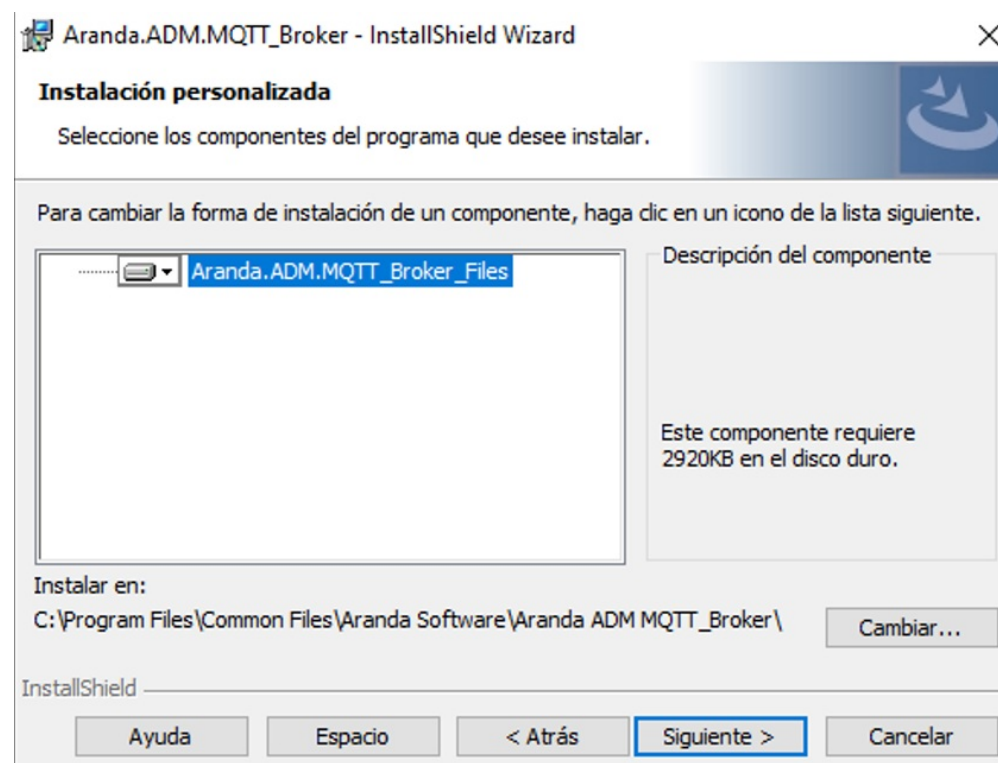
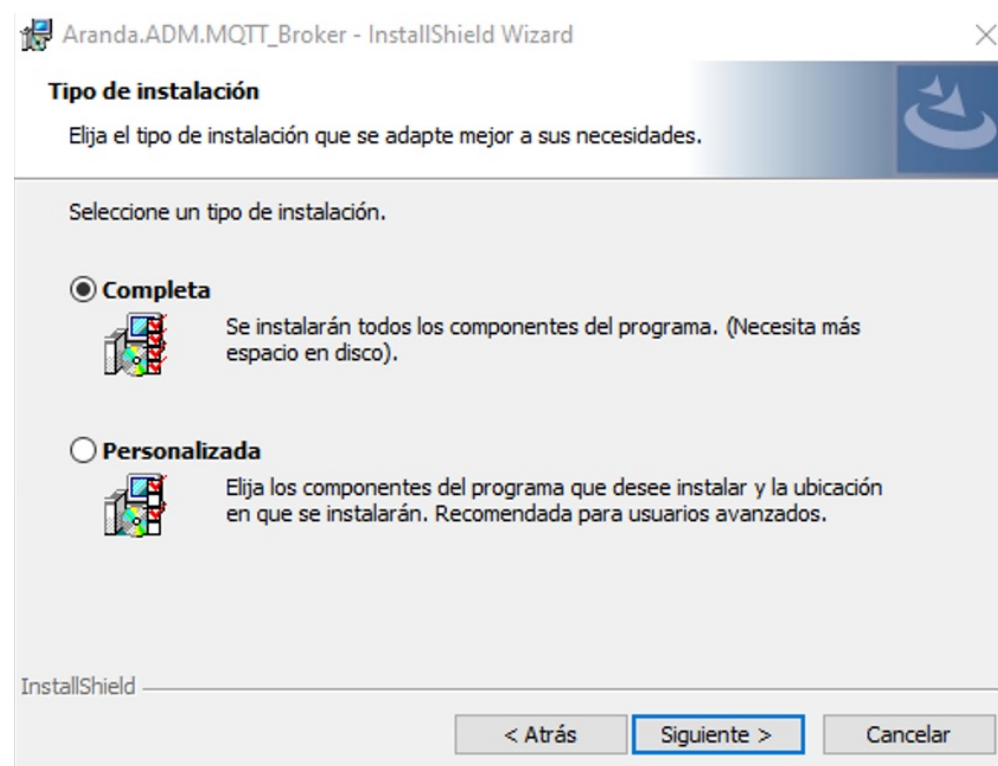


5. In the Customer Information window, enter the user name, organization, and click Following. These fields may be left empty.

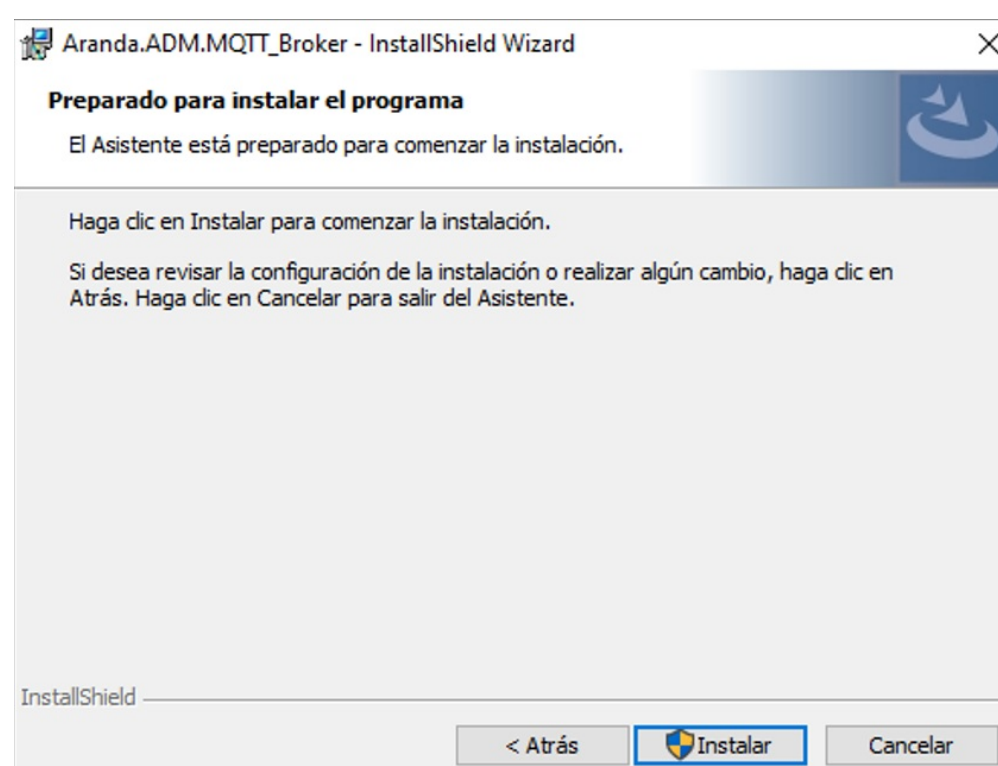


6. Define the type of installation, the options are:

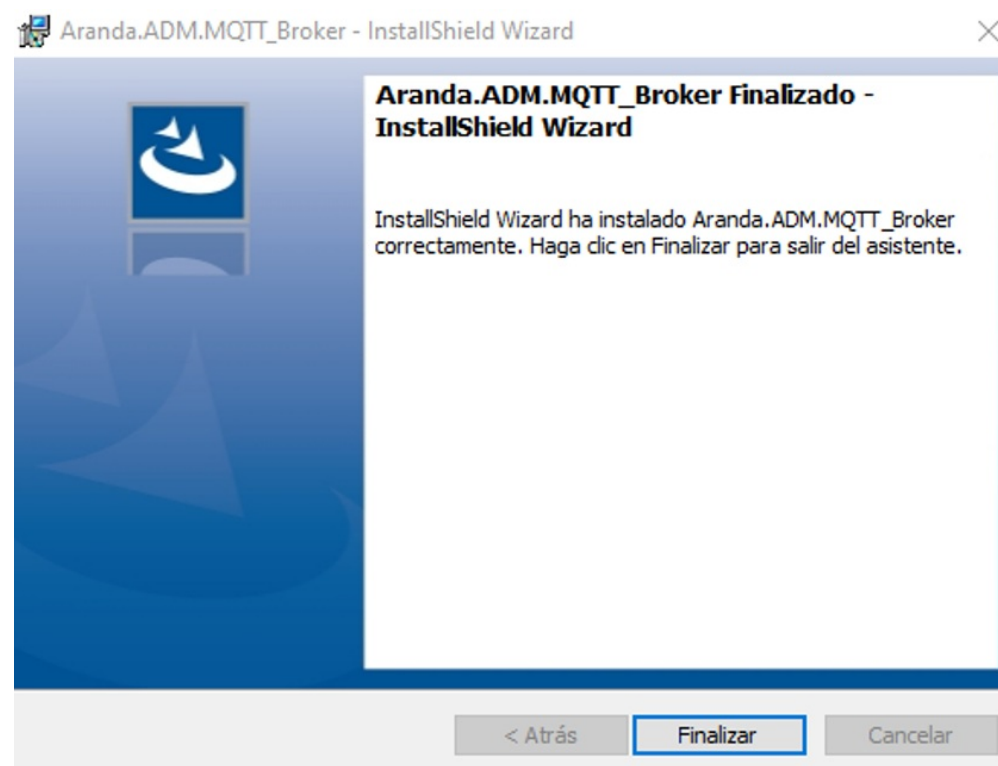
- **Complete:** All sites and services will be installed on the default routes.
- **Custom:** You can change the installation path of websites and services.



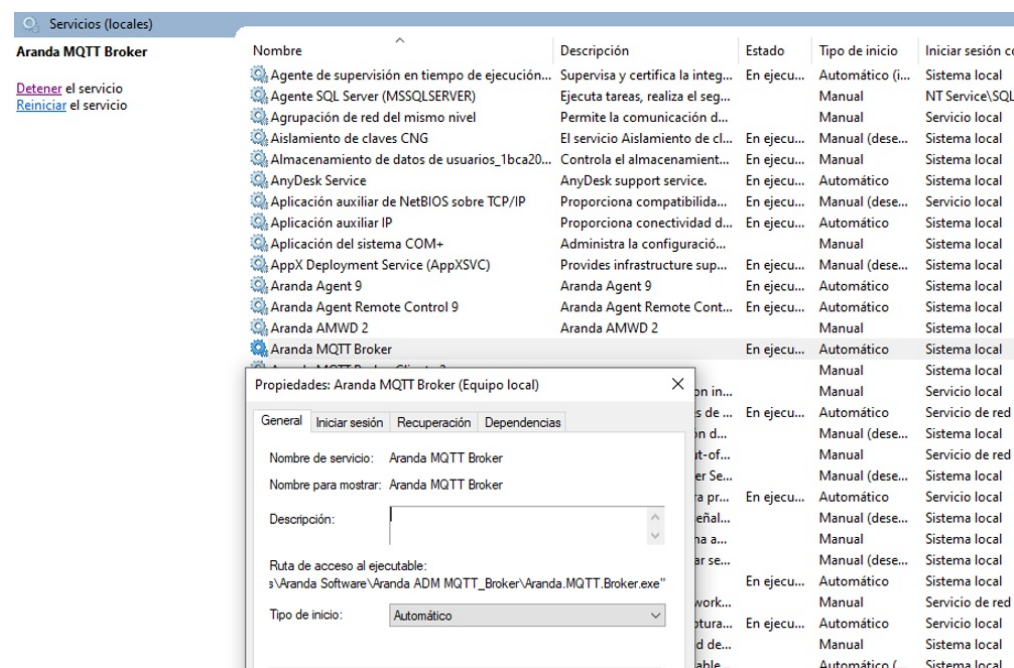
7. Once the Full or Custom installation is chosen, click **Install**, you must have permissions as a machine administrator.



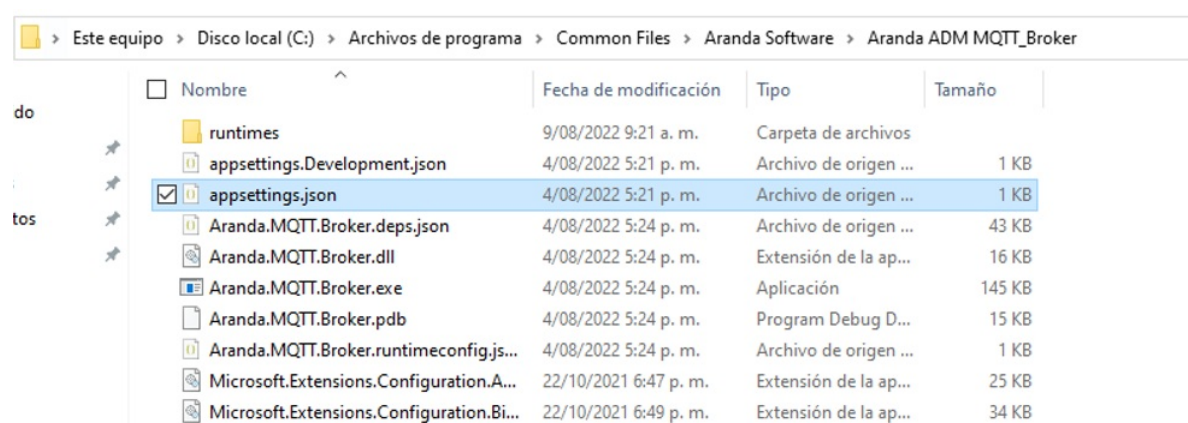
8. When the installation process is finished, click the **End**.



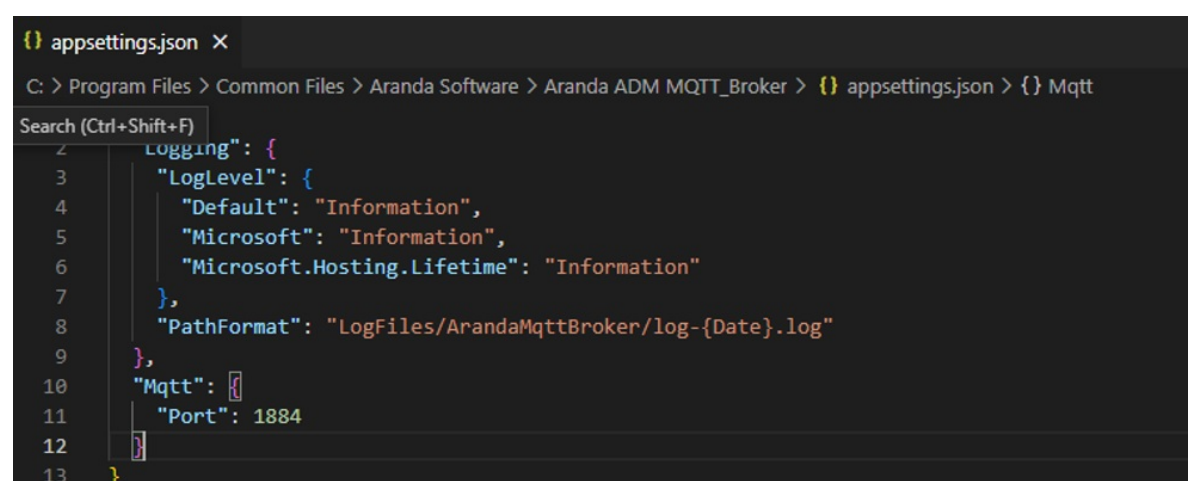
9. Once the installation process is finished, go to the services and verify that the service: Aranda MQTT Broker is installed and running.



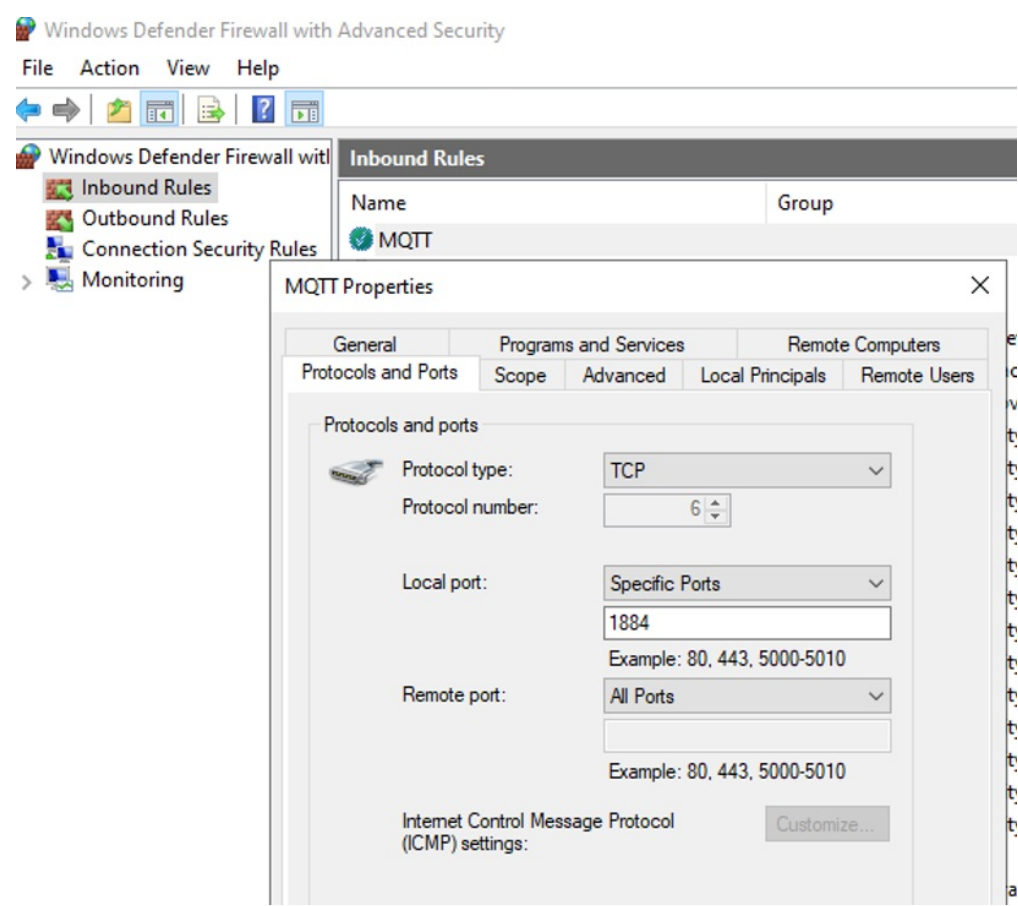
10. To configure the port you want to expose, open the `appsettings.json` in the folder where the service is installed, and do the following:



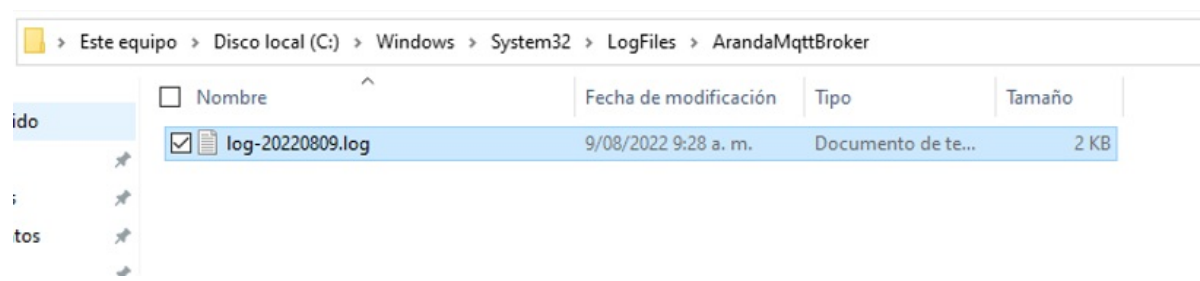
11. Modify the section `Mqtt:Port` to change the port and restart the service to apply the changes.



12. In Windows Defender Firewall, select the Inbound rules option and in the MQTT properties, validate that port 1884/1883 is open on the machine.

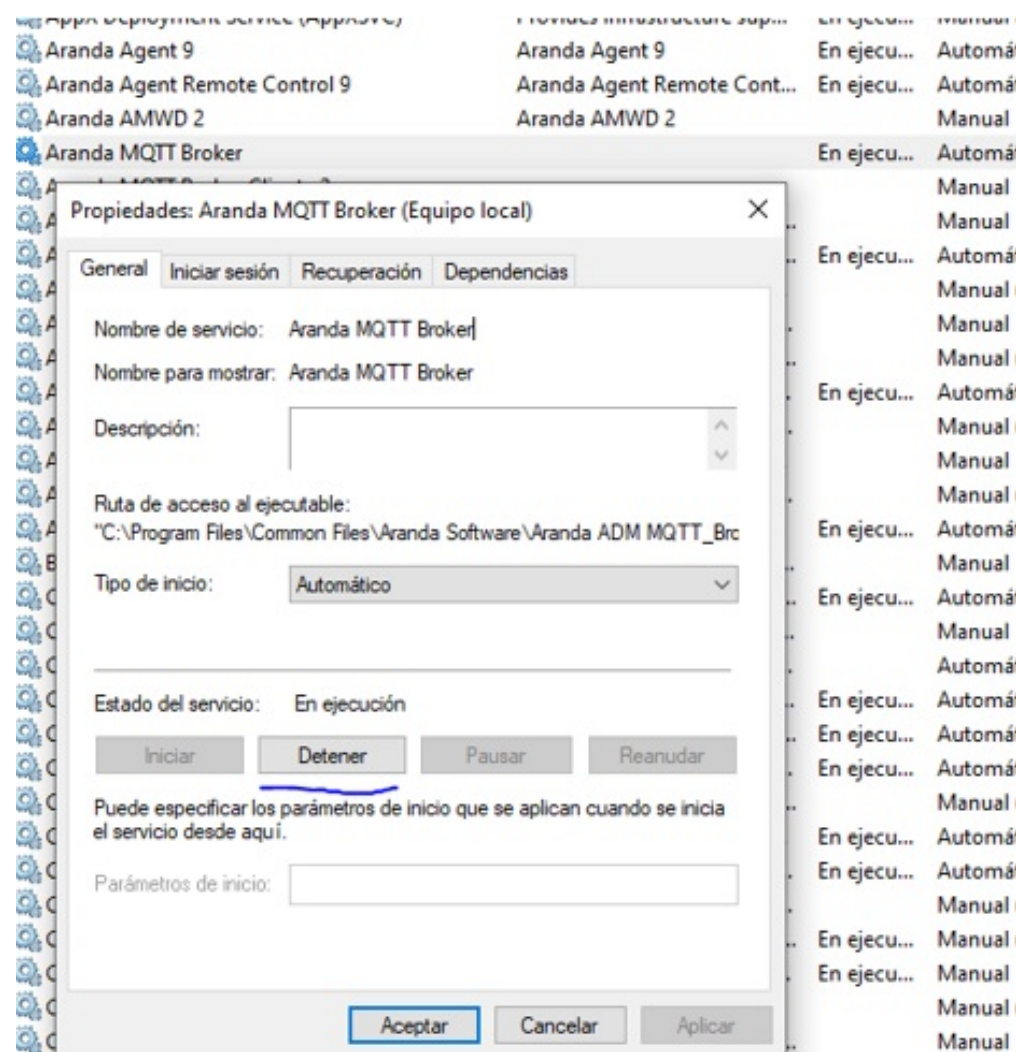


13.The archives of Log will be stored in the following path:C:/Windows/System32/LogFiles/ArandaMqttBroker

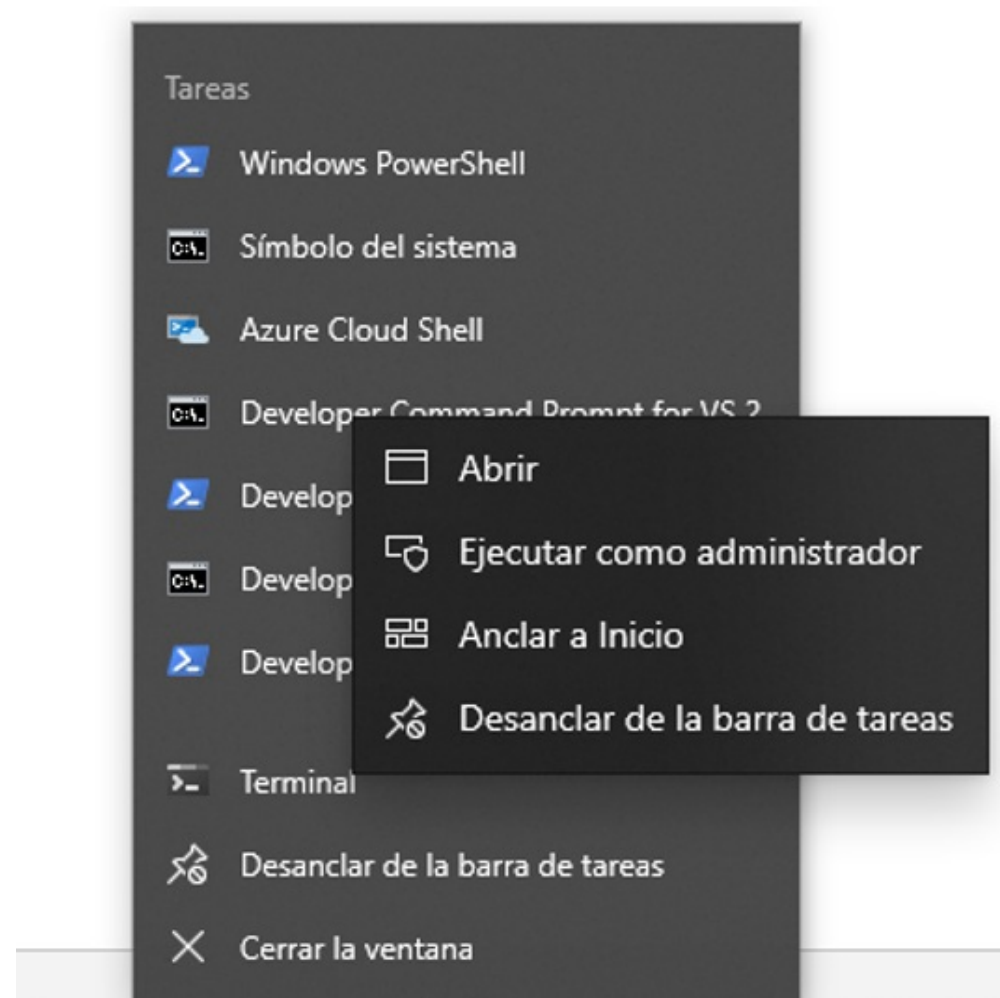


## Uninstalling MQTT Broker

1. Open the Aranda MQTT Broker file, the Properties window is enabled, and in theGeneral, under the Service Status, select the Detain and click the Apply.



2. Start a terminal in administrator mode and run the following information:



3. Run the command:

```
SC DELETE "Aranda MQTT Broker"
```

4. Once the command is executed, the result is as follows:

```
[SC] DeleteService CORRECTO
```

5. Check the services again and it should not be installed.

📌 **Note:** A maximum number of 10,000 connections (devices) per MQTT broker server is suggested.

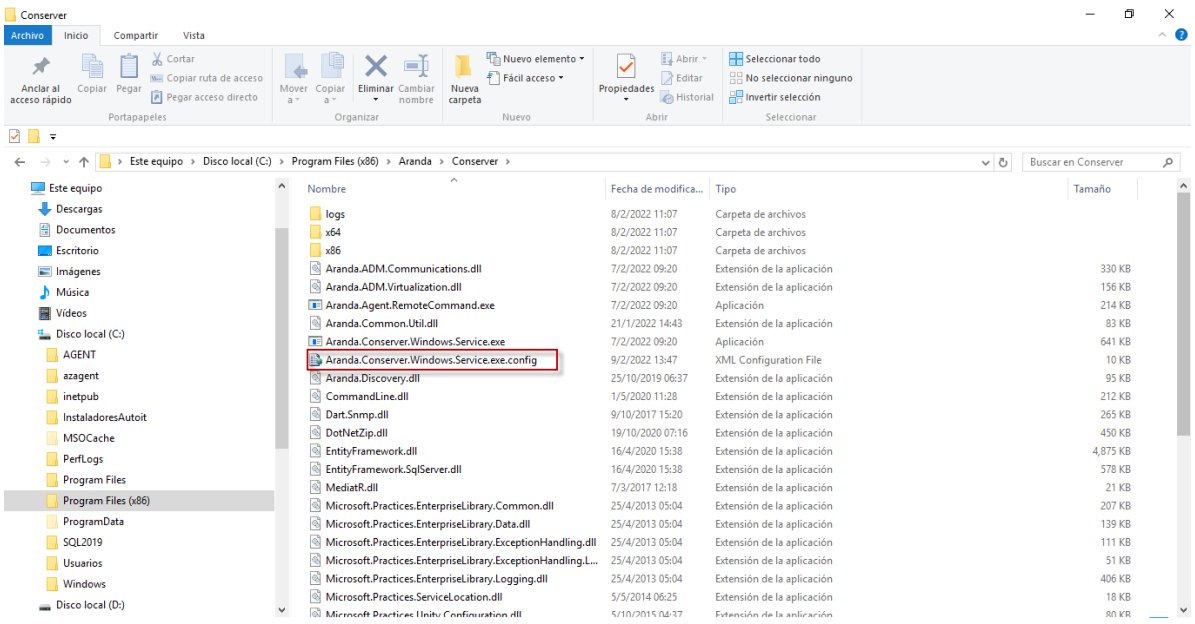
-  Related Links:
- [Broker Configuration](#)

## Broker Configuration

## Broker Configuration

### [Aranda MQTT Broker Installer](#)

1. To configure the communication between the conservator and the Broker, you must configure the file “Aranda.Conserver.Windows.Service.exe.config” which is in the folder “%Program Files (x86)%\Aranda\Conserver”



2. Create the following values based on the parameterized port and the IP of the server where the broker is installed.

```
{
<add key="mqttServerPort" value="1884"/>

<add key="mqttIp" value="192.168.X.XXX"/>

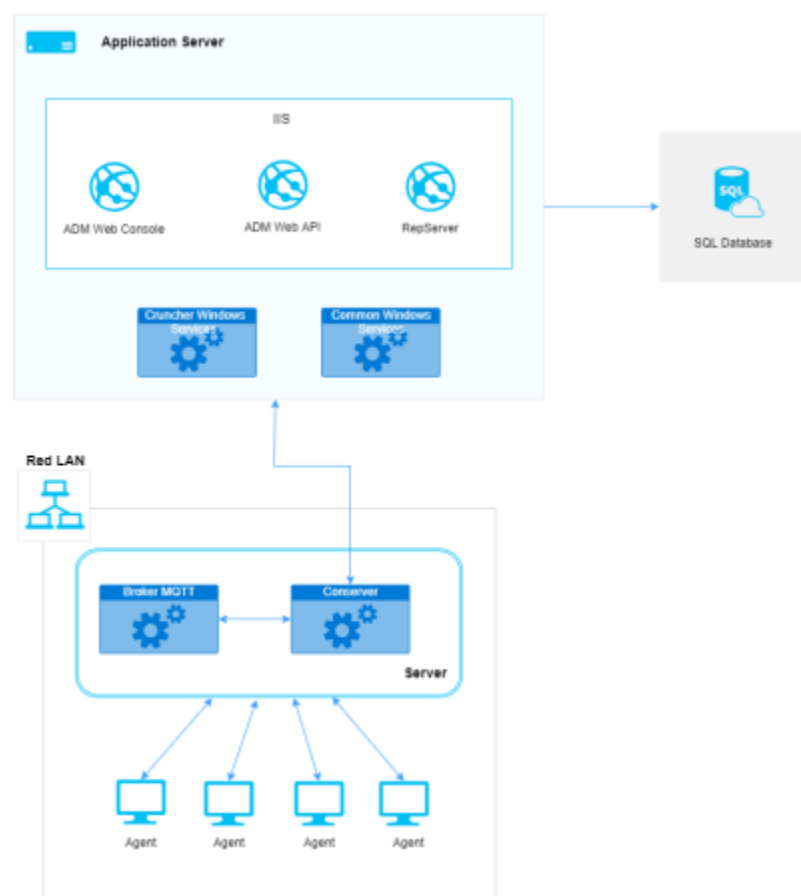
}
```



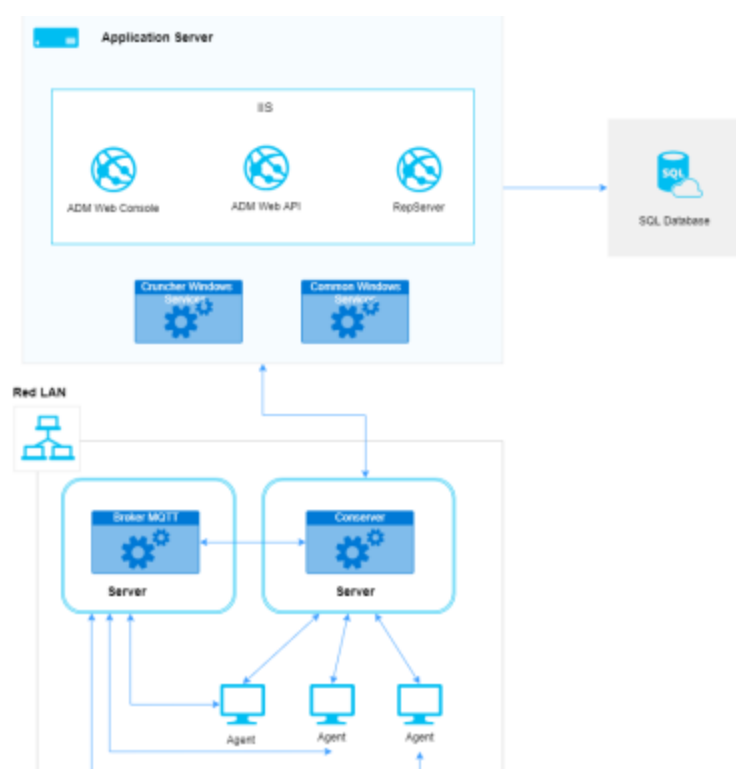
 Note: When you make a modification to the conserver configuration file, you must restart the service.

## Topologies supported in ADM with conserver broker division

- Configuration of the broker on the same server as the conserver

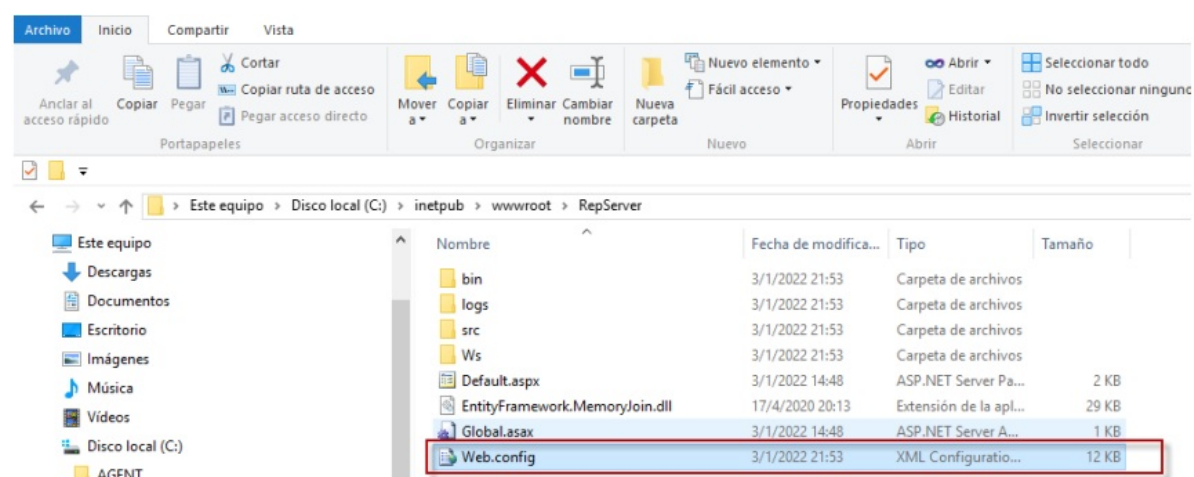


- Configuring the broker on different server of the conserver



## Configuring the broker from the Repserver

1. To configure the communication between the repserver directly with the Broker, you must configure the web.config of the repserver that is located in the path '%inetpub\wwwroot\RepServer'.



2. Add the following values in < appSettings > based on the parameterized port and host of the server where the broker is installed.

```
{
<add key="mqttServerPort" value="1884"/>

<add key="mqttIp" value="192.168.X.XXX"/>

}
```

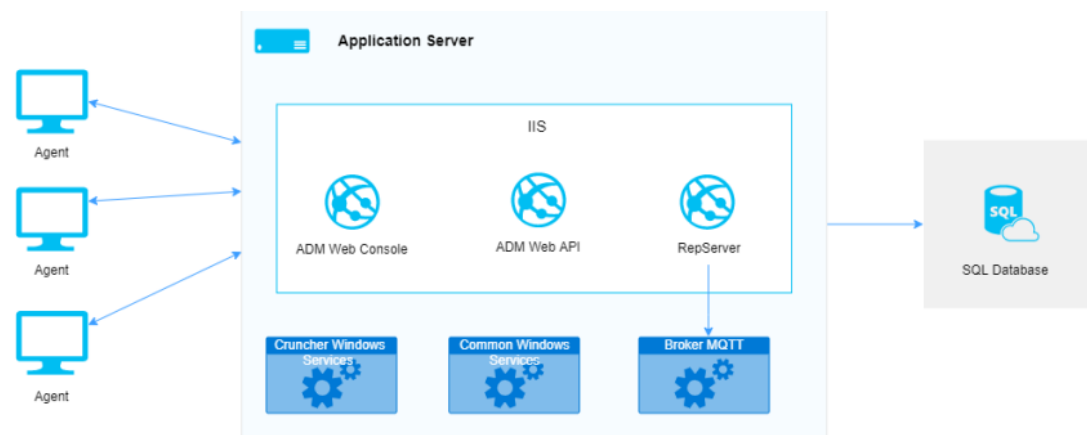
```
118 <provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" />
119 <provider invariantName="Oracle.ManagedDataAccess.Client" type="Oracle.ManagedDataAccess.EntityFramework.EFOracleProviderServices, Oracle.ManagedDataAccess" />
120 </providers>
121 <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
122 <parameters>
123 <parameter value="v11.0" />
124 </parameters>
125 </defaultConnectionFactory>
126 </entityFramework>
127 <appSettings>
128 <add key="vs:EnableBrowserLink" value="false" />
129 <add key="logLevel" value="Information" />
130 <add key="%EntityFramework_Extensions_LicenseName" value="4339:100-arandasoft.com" />
131 <add key="%EntityFramework_Extensions_LicenseKey" value="2a228917-e440-1205-c78b-d06a907829f5" />
132 <add key="mqttServerPort" value="" />
133 <add key="mqttIp" value="" />
134 </appSettings>
135 <runtime>
136 <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
137 <dependentAssembly>
138 <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
139 <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0" />
140 </dependentAssembly>
141 <dependentAssembly>
142 <assemblyIdentity name="DotNetZip" publicKeyToken="6595c6414667745" culture="neutral" />
143 <bindingRedirect oldVersion="0.0.0.0-1.14.0.0" newVersion="1.14.0.0" />
144 </dependentAssembly>
145 <dependentAssembly>
146 <publisherPolicy apply="no" />
147 <assemblyIdentity name="Oracle.ManagedDataAccess" publicKeyToken="89b483f429c47342" culture="neutral" />
148 </dependentAssembly>
149 <dependentAssembly>
150 <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a" culture="neutral" />
151 <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="5.0.0.0" />
152 </dependentAssembly>
153 </assemblyBinding>
154 </runtime>
155 </configuration>
```

3. For the changes to be applied, the device must be restarted.

⚠ **Note:** To configure the broker directly to the repserver, it must be taken into account that it only works with an agent version since 9.13, and the following functionalities are not supported in this architecture:

- Discovery.
- Agent distribution.
- Discovery rule.
- LDAP- Device discovery.
- Virtualization.
- Monitoring.

## Configuring the broker by pointing directly to the Repserver

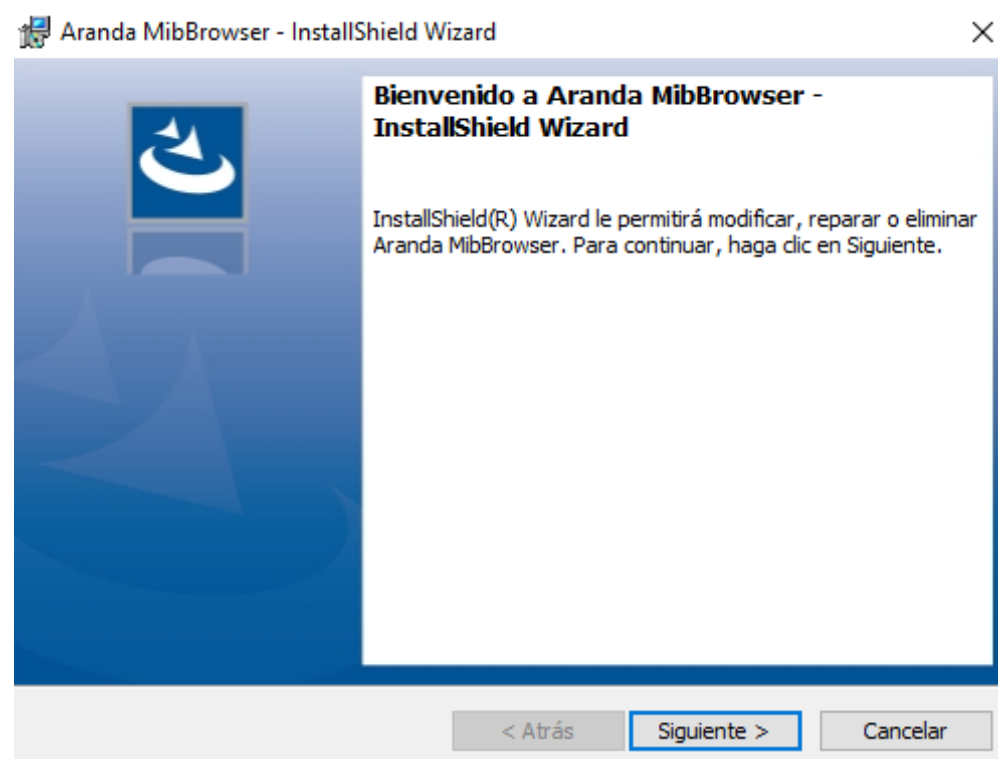


⚠ **Note:** The broker may or may not be within the same server as the repserver.

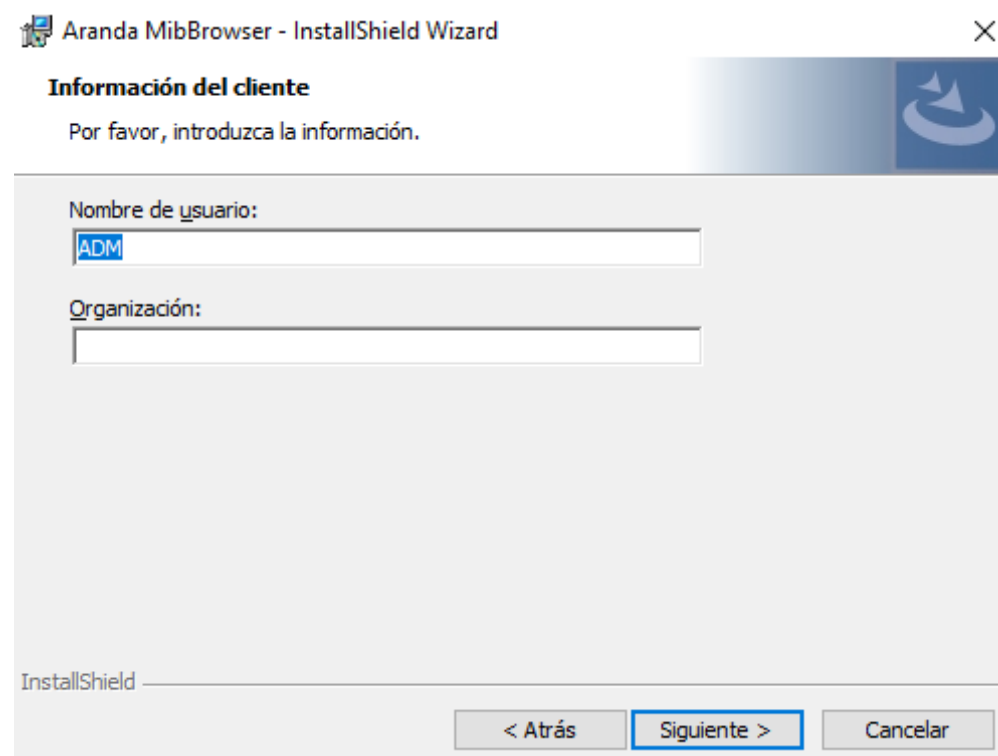
[Aranda MQTT Broker Installer](#)

## MibBrowser Installer/Washer

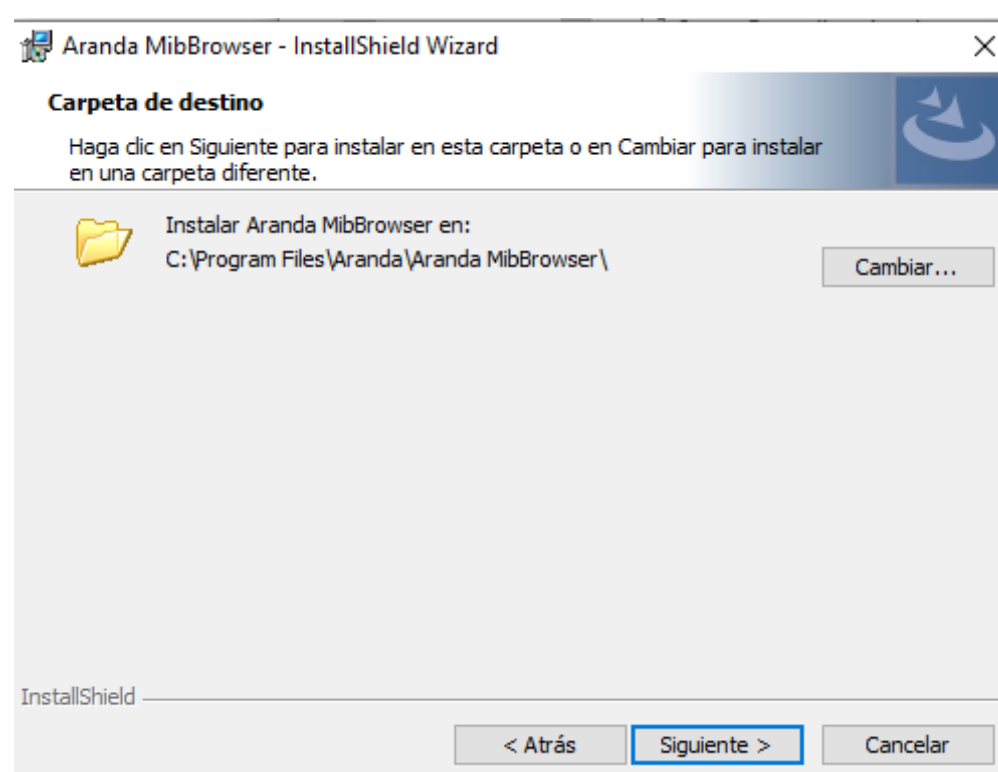
1. Run the installer Aranda.MibBrowser.exe



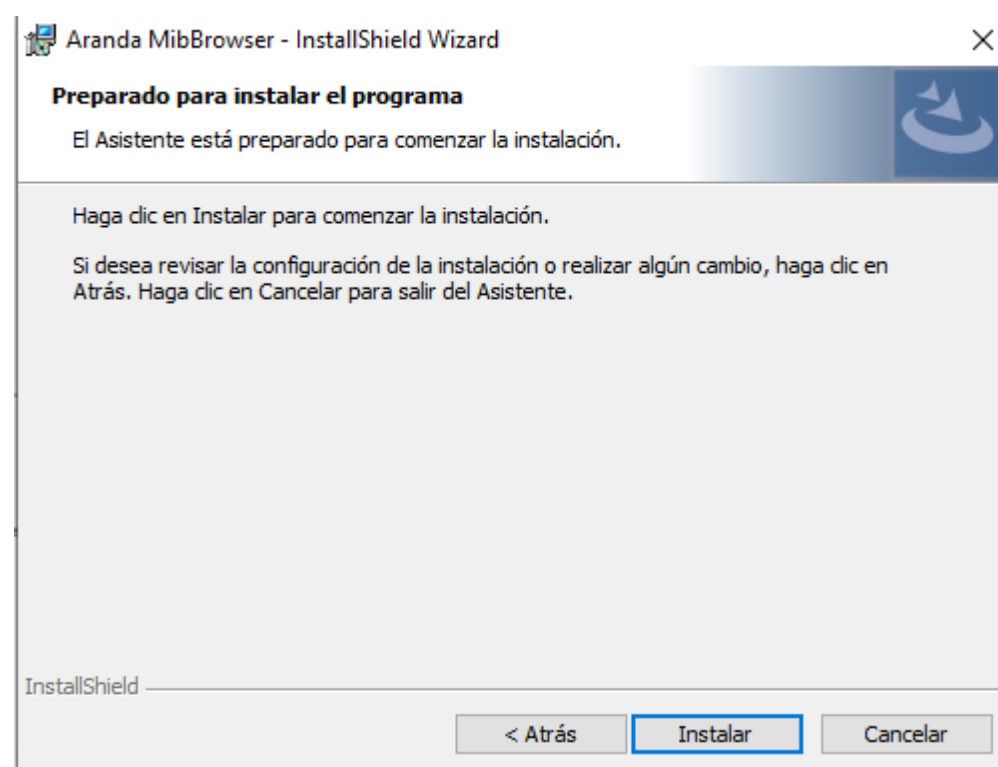
2. You can define the username or organization and click Following. These fields may be left empty.



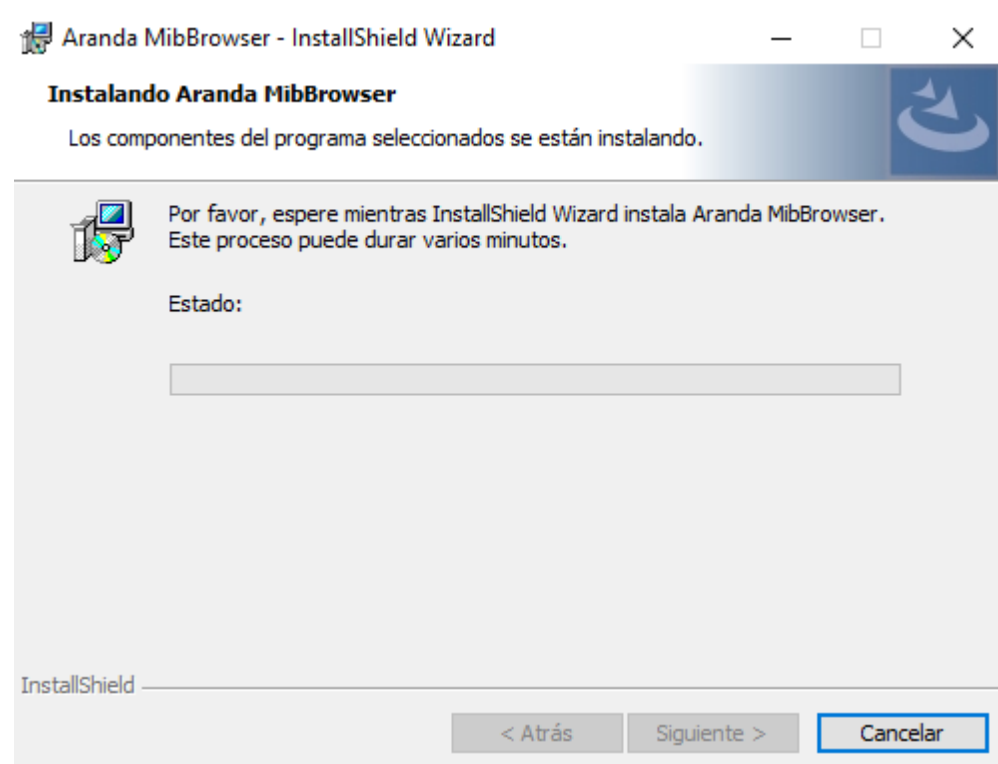
3. The installer selects a location for installation or you can change it, then click Following.



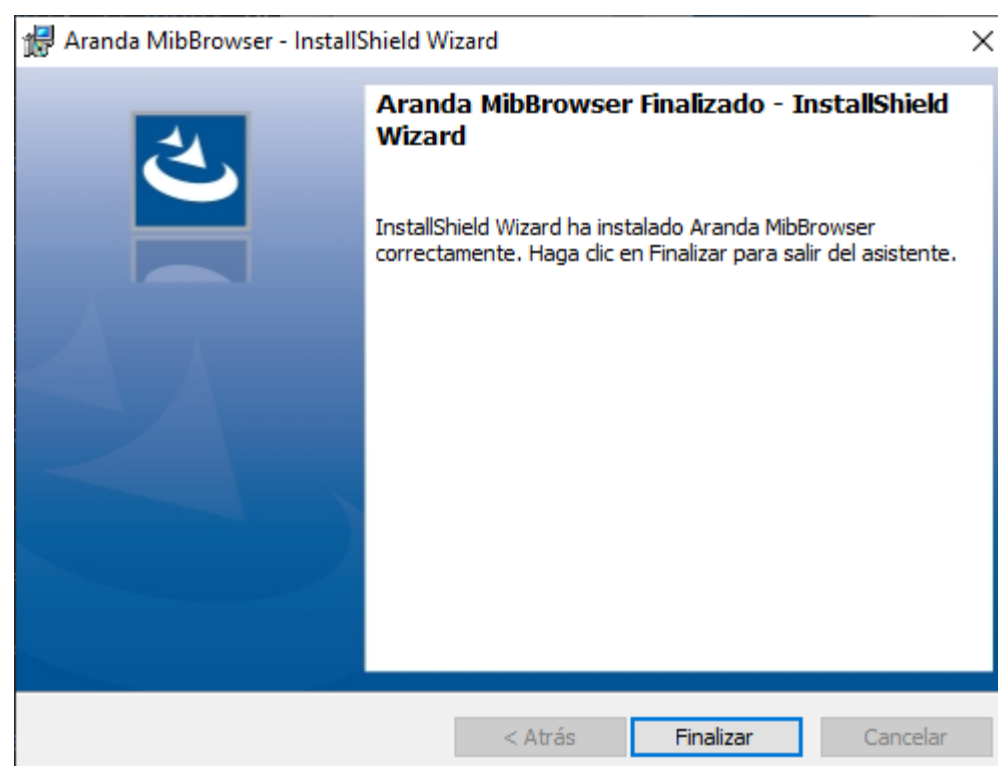
4. Then we proceed to the installation, click on Install.



5. Wait while the installer finishes the process.



6. Confirm the installation by clicking the End.



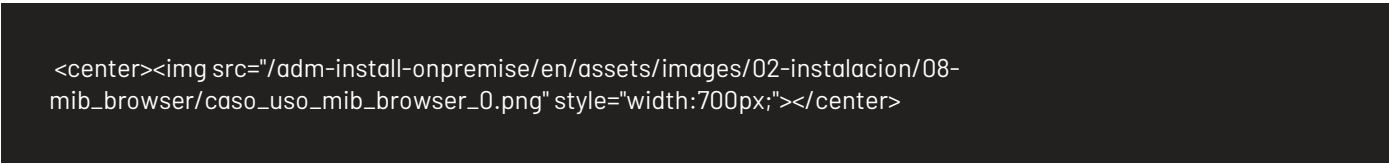
# Mib Browser Settings

## MibBrowser Settings

[« Aranda MibBrowser Installer](#)

The MibBrowser allows you to compile MIBs (Management Information Bases) which contain information about the OIDs (Object Identifiers) that can be queried using the SNMP (Simple Network Management Protocol) about a device for example a router, switch or printer etc.  
When the application is launched, the following sections can be identified

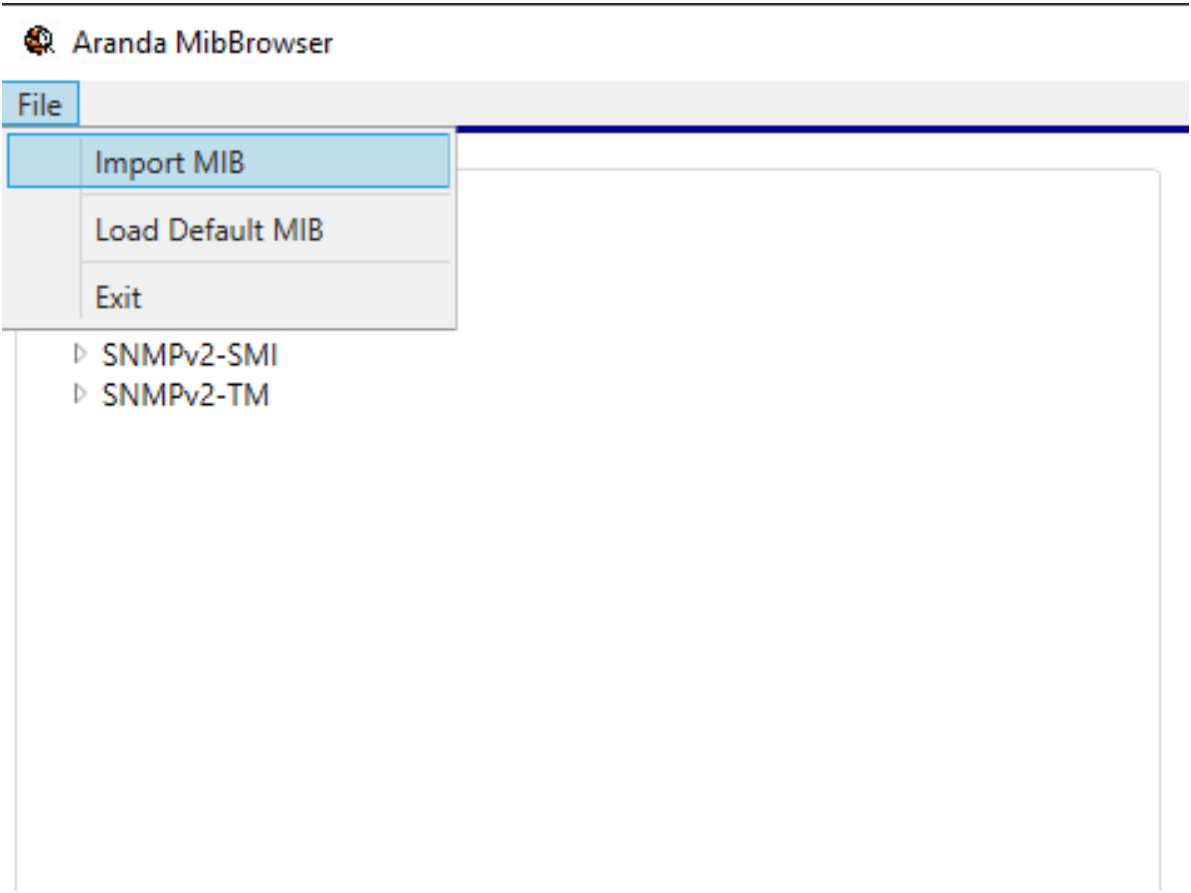
- 1. Mibs
- 2. ObjectIdentifier
- 3. Settings
- 4. Oid-Value



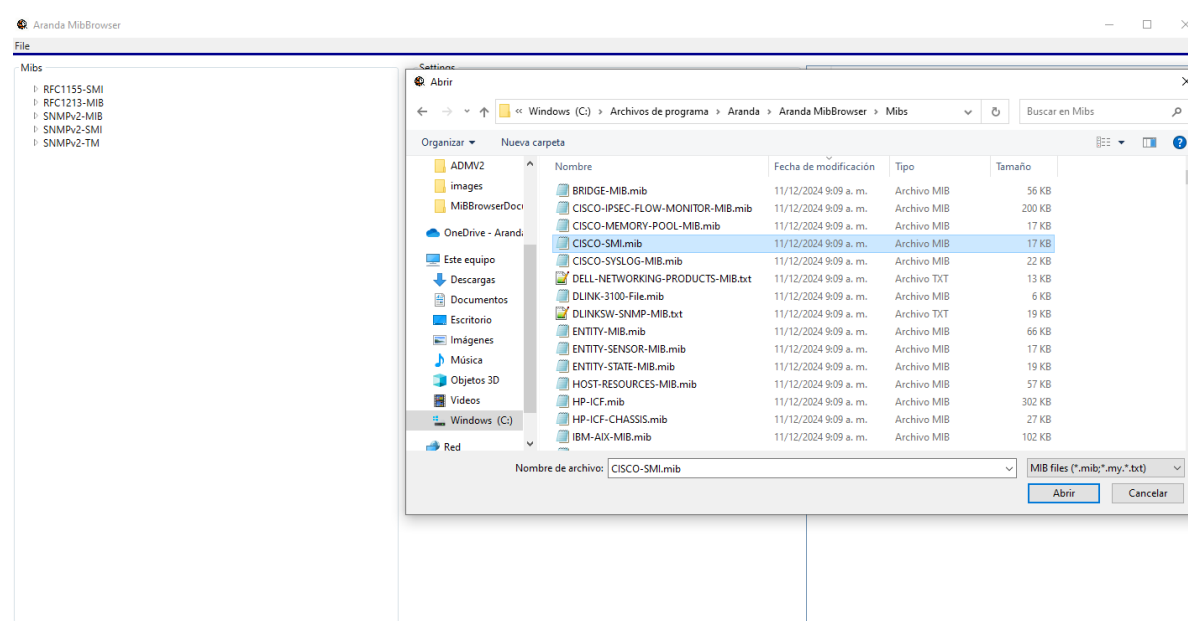
1. The MIBs initially compiled are the following MIBs:

- RFC1115-SMI
- RFC1213-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TM

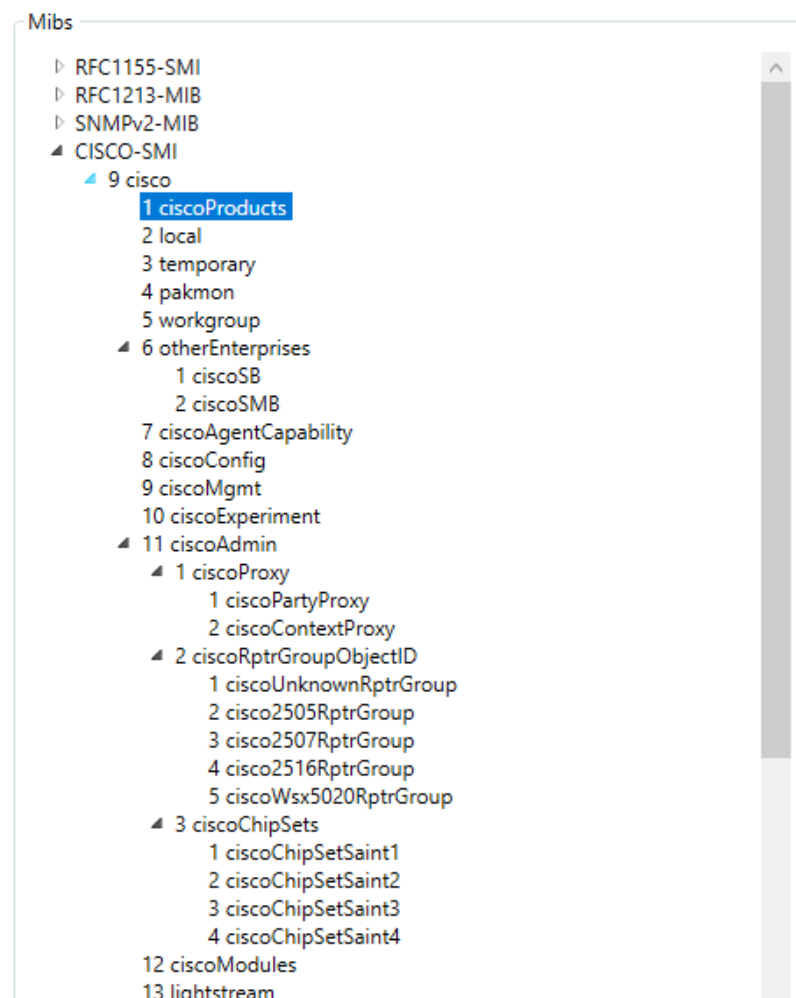
If you want to compile another MIB you can do so via the menu option



When you load the MIB correctly you will see the tree with all the related MIBS, for the example we use the CISCO-SMI MIB.

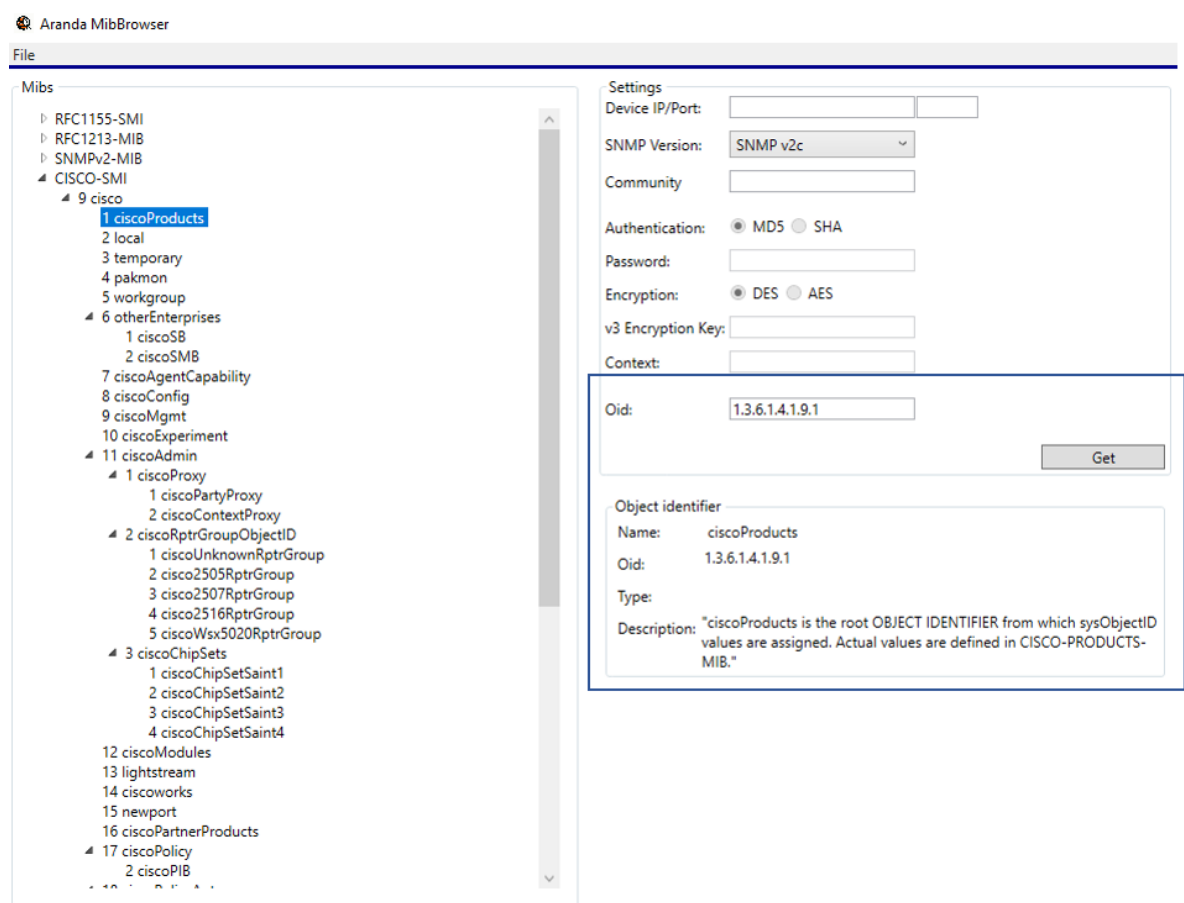


We consult the MIBS tree

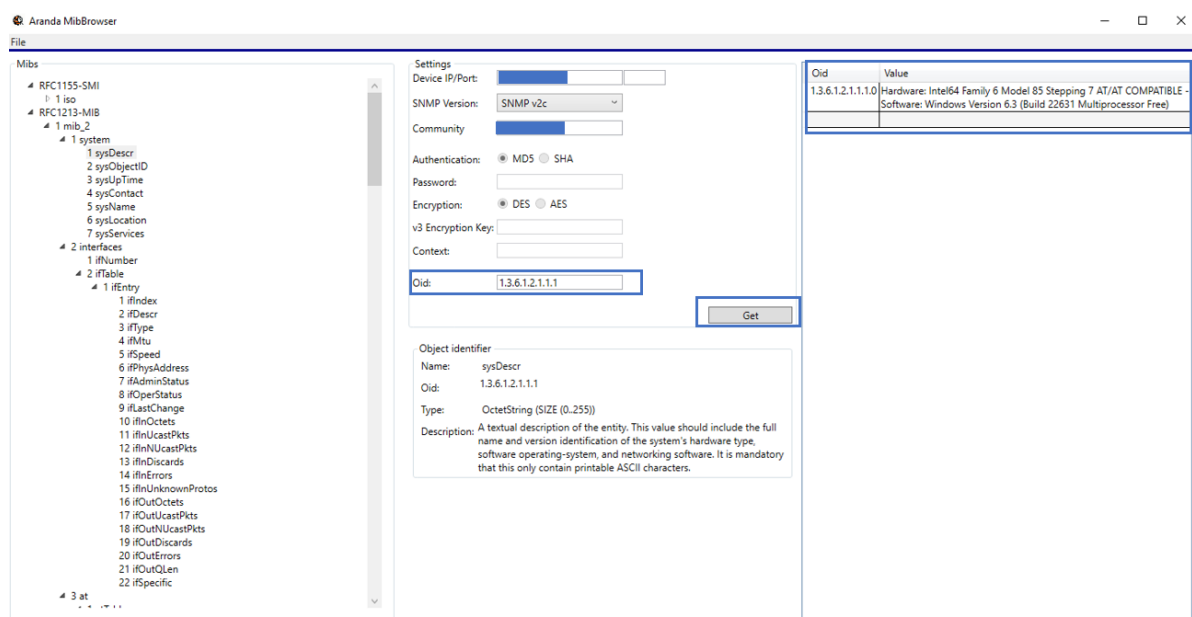


⚠ **Note:** A MIB usually has dependencies which it is recommended to upload it to its main MIB or manually copy it to the MIB. MibBrowser installation directory in the folder **MIBS**, since it is the path where the application consults to try to resolve dependencies automatically.

2. When you load a MIB you can see the related OIDs, if you select a node you can see the information in the Object Identifier section



3. To consult an OID you can fill out the form with the required data, then press the Get button and if there is information it will be shown in the OID and value section.



⌞ **Note:** Note that the OID entered must be related to the device.

[« Aranda MibBrowser Installer](#)

## Remote control

It allows you to take control of machines in a simple and efficient way and transfer files conveniently, facilitating remote management of workstations.

⌞ **Note:** This functionality is not supported on OnPremises installations of ADM versions lower than 9.21.1

## Installer/Remote Control

ADM Windows Agents from ADM version 9.19.2, after performing the zero installation or an upgrade from a previous version, will automatically install the new remote control component after 30 minutes. The following processes and services are displayed on the device.

⌞ **Note:** In the event of a connection failure at the time of installation or update of the remote control component, the ADM agent will perform installation retries every 4 hours.

## Remote Control Component Processes and Services

## Remote Control Component Upgrade

## Installer/Viewer Remote Support Specialist

### Remote control viewer installation

## Remote Control Configuration

### Remote Control Setup Process

You should consider the following steps for remote control setup in OnPremise installations:

- Enable the functionality by performing an update to the ADM product database

```
update AFW_SETTINGS set sett_value = 'true' WHERE sett_key='EnableARC'
```

- Perform the corresponding post-installation configuration **Aranda.ADM.Web.Installer** on the application server.  
[View Settings](#)

## Agent Configuration and Installation

Consider the following steps for the configuration and installation of the remote control agents:

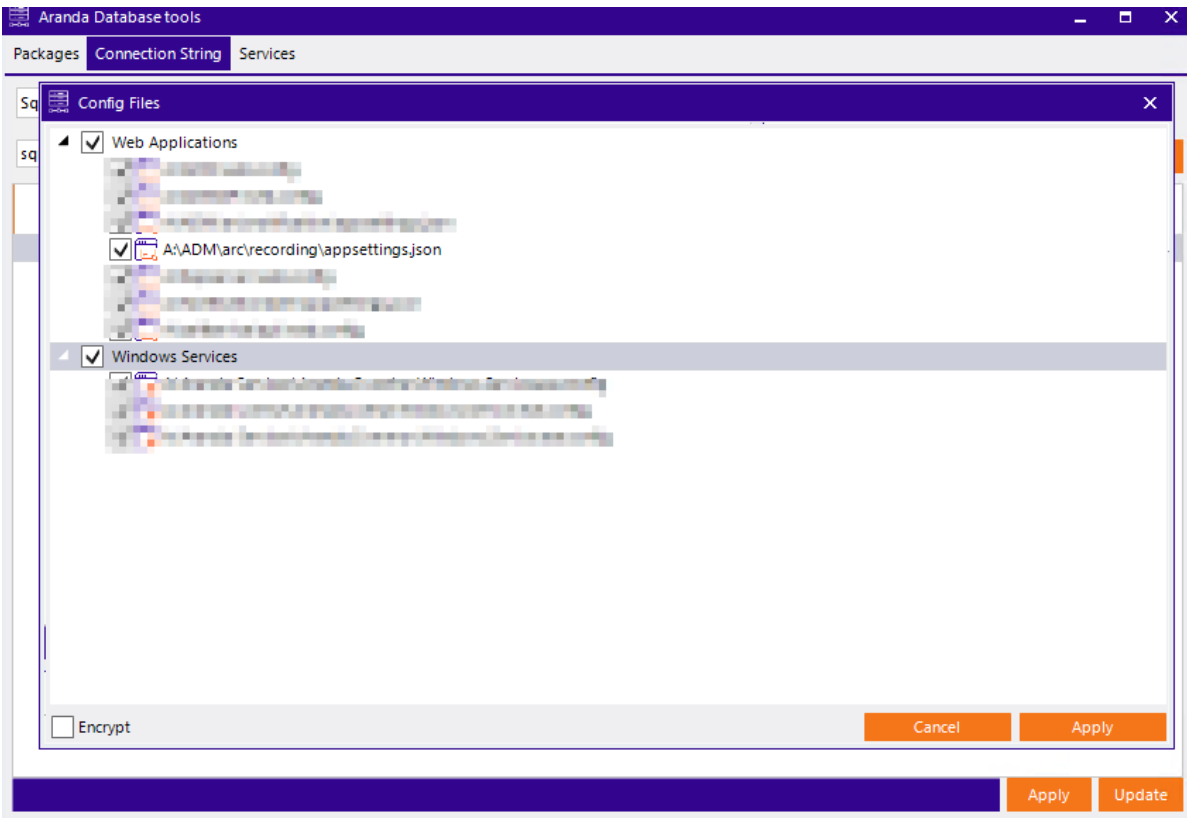
- To perform remote control, it is required to have the remote control component installed on the devices to which the remote connection is to be made. [Remote Control Component Installation](#)
- Installation of the remote control viewer, required on the device from which the remote connection is made  
[Installation viewer remote support specialist](#)

## Remote Control Configuration

After installing the file **Aranda.ADM.Web.Installer** perform subsequent configurations on the application server and from the ADM console to ensure the correct operation of the new remote control, taking into account the following steps:

# 1. Configure connection chain

Configure the connection string for the recording site, via the Aranda Database Tools v9 module. Notification sites do not require configuring connection string.



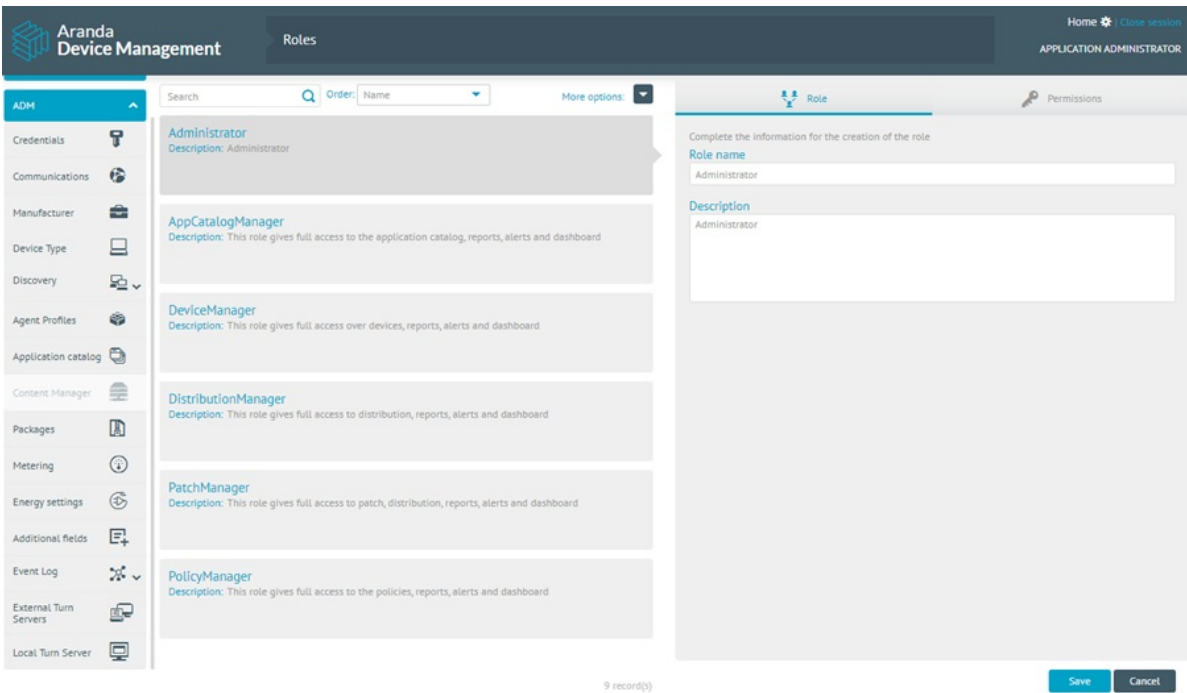
Notes:

- When the configuration is applied with Encrypt enabled, an alert message may be displayed because encryption is not supported for JSON files.
- When you make changes to the recording server connection string, restart the IIS so that the changes are applied correctly.
- If changes are made to the storage provider after configuration, move the information contained in the previous provider to the current one. If this action is not taken, agent updates will not be successful, and you will not be able to access recordings in audits.

# 2. Log in to the console

Log in to the ADM console with the user with the required permissions to manage the External Turn Servers and Local Turn Server options in the ADM Settings.

**Important:** External and Local Turn options are available on On-Premise installations only.



# 3. External Turn Servers

The file transfer functionality of the remote control uses a WebRTC-based P2P protocol. When two devices are unable to establish a direct connection to each other, a Turn server is needed to facilitate communication.

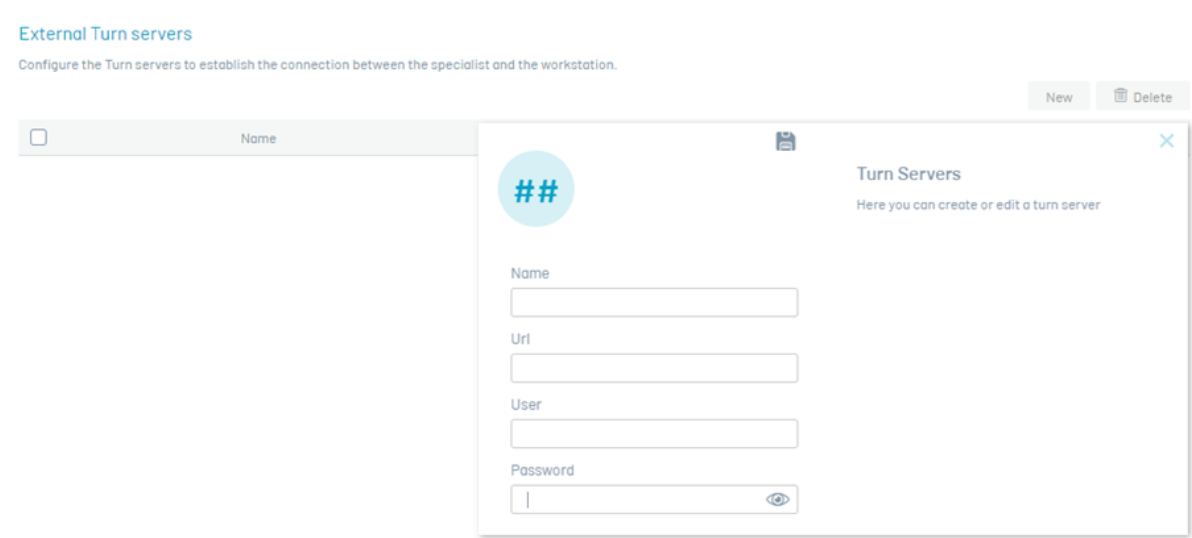
To add an external Turn server in the External Turn Servers, follow these steps:

- A. Click on the option **New**.
- B. Complete the requested fields according to the following table:

Field	Description
Name	Name that you want to assign to the configuration, between 6 and 50 characters.
URL	It corresponds to the STUN/TURN server site, for example: turn:<server_public_ip>:puerto or stun:<server_public_ip>:puerto .
User	Name of the user authorized to connect to the STUN/TURN server.
Password	Password associated with the user that allows the connection to the STUN/TURN server.

C. Finish by clicking the **Save**.

📌 **Note:** This configuration is required for file transfer when the specialist agent and the workstation agent are not on the same network, therefore, both devices must be allowed to exit to the Internet through the configured port.



The user can register the number of external Turn servers that he or she deems necessary to have good communication between the specialist’s devices and the workstation through the ADM console. To delete an external Turn server, in the **External Turn Servers** Select the server(s) to delete and click the **Eliminate**, it will be confirmed that the server(s) have been successfully deleted.

You can use public STUN/TURN WebRTC, by doing a web search “STUN server list” you will be able to list the different public STUN/TURN servers available. When configuring public servers on workstations and on specialist computers, they must allow the output of the servers that are configured to the sites. It is also possible to configure the STUN/TURN server provided in the installer [by making the settings in the Aranda Turn Stun WebRTC Server Windows Service](#). In addition, public STUN/TURN can be used in conjunction with your own installed servers, as mentioned above.


## 4. Turn Local Server

To establish remote takeover communication between the specialist agent and the workstation agent, use a local Turn server that can relay network traffic.

To add a local Turn server, follow these steps:

- A. Click on the option **Local Turn Server** from the main menu.
- B. Complete the field **Host** with the path to the local server, which can be the IP of the server or the DNS. The countryside **Port** it is set by default to the value 8081 and SSL is inactive; if the port is changed or SSL is enabled [make the settings in the Aranda Turn Server service](#) installed on the server.
- C. Finish by clicking the **Save**

Turn Server Local



Next configure the local Turn server.

Turn Server Local

Define fields for configuration

Host

Enter the provider URL

dns-servidor - IP

Puerto

Enter the port associated with the server

8081

Enable SSL

☐

Cancel

Save

## Manual Service Configuration

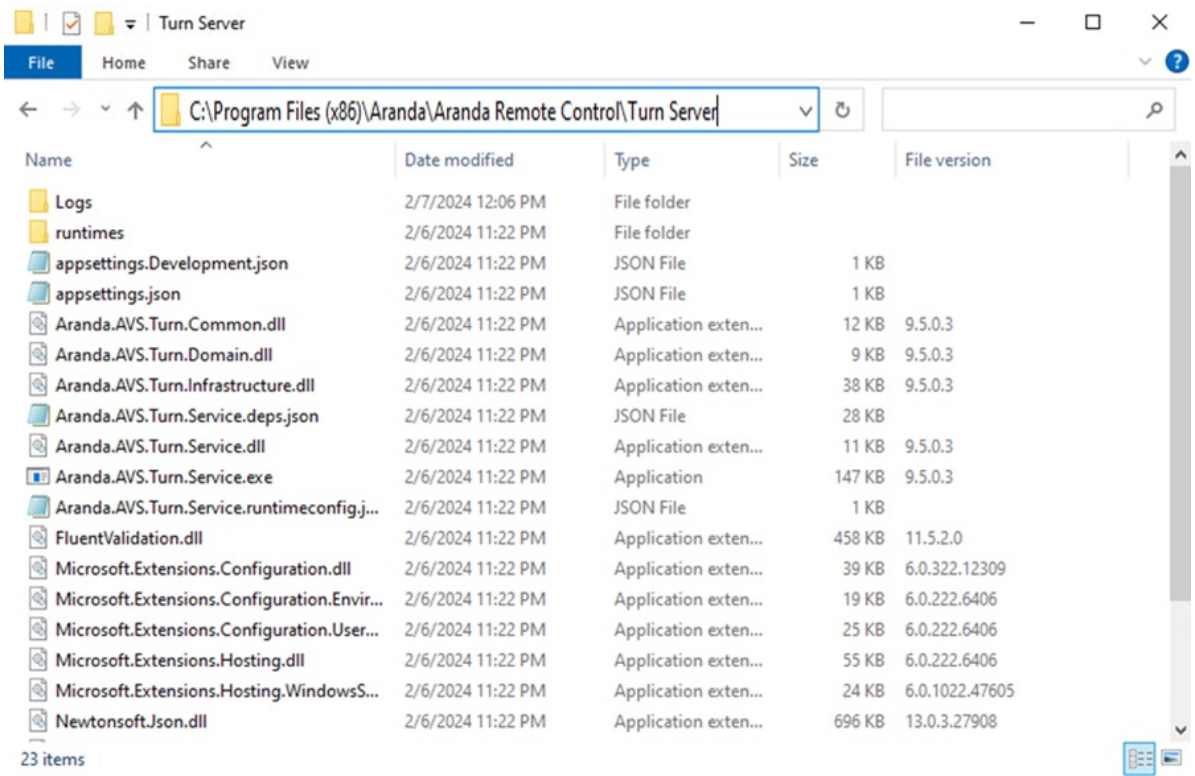
### Turn Server Configuration

After installing the Aranda Turn Server service, you don't need to make any adjustments for its operation. However, parameterizations can be made according to specific needs, such as changing the connection port (8081 by default) and enabling SSL (disabled by default). If you need to make these settings, follow these steps:

#### 1. Validating the appsettings.json File

Before making changes, check the appsettings.json located in the service installation path (default:C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) to ensure that the port is set to 8081 by default. If the port does not need to be modified, no further adjustments are required.

Additionally, validate that port 8081 is enabled in the local firewall rules to ensure the correct flow of traffic. In this file, you can also find the setting for SSL certificates, which is disabled by default (IsSsl=false).



Default appsettings.json settings:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "TurnConfiguration": {
    "CertificateParam": "",
    "CertificatePath": ""
  }
}
```

```
"CertificateSubject": "",
"IsSsl": false,
"Port": 8081,
"SSLProtocols": "Tls12"
}
}
```

## 2. Port Configuration Change

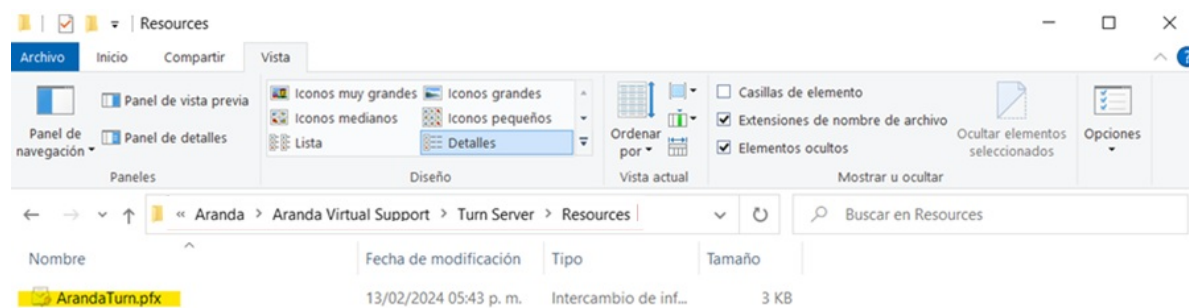
Edit the file *appsettings.json* and configure the desired port by replacing <puerto> by the desired port number.

```
"TurnConfiguration": {
  "CertificateParam": "",
  "CertificatePath": "",
  "CertificateSubject": "",
  "IsSsl": false,
  "Port": <Puerto>,
  "SSLProtocols": "Tls12"
}
```

## 3. SSL Secure Connection Configuration

Edit the *appsettings.json* file, change "IsSsl" to true. There are two alternatives to add the SSL certificate:

3.1. Acquire or generate a PFX certificate, which must be located inside the folder **Resources** (the folder must be created if it does not exist) in the installation path of the service.



The file name is recorded in the **CertificatePath** and the base-64 encoded key for generating the certificate must be registered in **CertificateParam**, both options available in the *appsettings.json* file.

```
"TurnConfiguration": {
  "CertificateParam": "<clave-base64>",
  "CertificatePath": "<nombre-archivo.pfx>",
  "CertificateSubject": "",
  "IsSsl": true,
  "Port": 8081,
  "SSLProtocols": "Tls12"
}
```

3.2. If you have a PFX certificate stored in the certificate bucket, you can configure it by naming the certificate in the **CertificateSubject** from the *appsettings.json* archive.

```
"TurnConfiguration": {
  "CertificateParam": "",
  "CertificatePath": "",
  "CertificateSubject": "<nombre-certificado>",
  "IsSsl": true,
  "Port": 8081,
  "SSLProtocols": "Tls12"
}
```

## 4. Service Restart

Restart the Turn Server Windows Service for the configuration changes to take effect. The service should now listen on the newly configured port and enable the use of SSL certificate.

## 5. Firewall Settings

Open the port that was configured in step 2 in the local firewall inbound rules. This step is crucial to allow traffic over the new port and ensure that the Turn Server can receive incoming connections on the configured port.

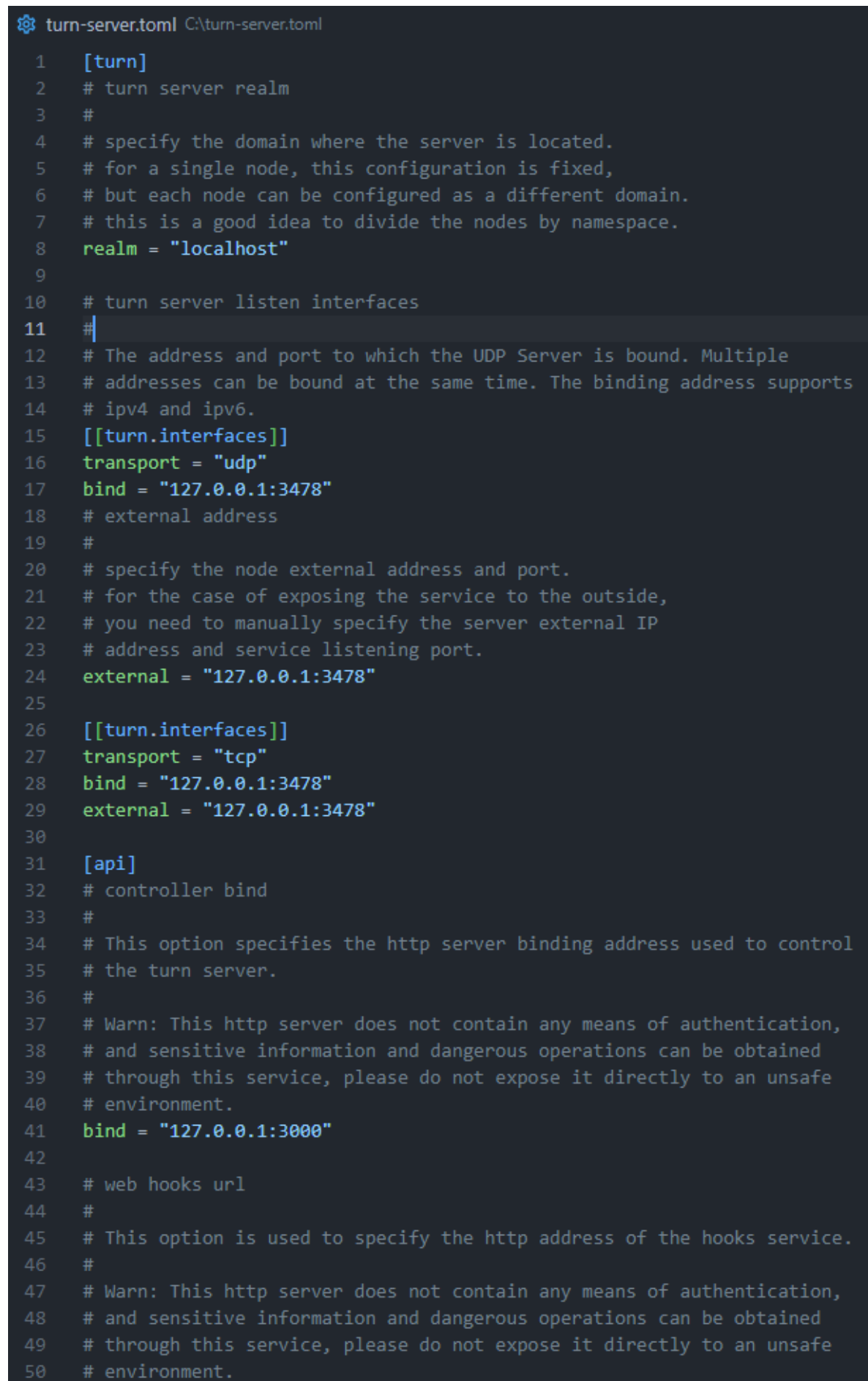
Parameterizing the Turn Server port and the use of SSL from the service is a fundamental process to ensure its correct functioning and adapt it to the specific needs of each customer. By following these steps, you can ensure that the Turn Server is configured correctly and ready to handle connections as required.

## Stun/Turn WebRTC Server Configuration

After you install the service **Aranda Turn Stun WebRTC Server**, the configuration is necessary for it to work properly.

### 1. File Validation turn-server.toml

Before making changes, verify that the **turn-server.toml** is located in the service installation path (by default: C:\Program Files (x86)\Aranda\Aranda Remote Control\Stun Server).

A screenshot of a code editor showing the configuration file 'turn-server.toml' located at 'C:\turn-server.toml'. The file contains 50 lines of configuration for a STUN/TURN WebRTC server. The configuration is organized into sections: [turn], [[turn.interfaces]] (for UDP and TCP), and [api]. Comments provide detailed instructions for each parameter, such as specifying the domain, listening interfaces, and external addresses. The current configuration sets the realm to 'localhost', binds to '127.0.0.1:3478' for both UDP and TCP, and sets the API bind to '127.0.0.1:3000'.

```
1  [turn]
2  # turn server realm
3  #
4  # specify the domain where the server is located.
5  # for a single node, this configuration is fixed,
6  # but each node can be configured as a different domain.
7  # this is a good idea to divide the nodes by namespace.
8  realm = "localhost"
9
10 # turn server listen interfaces
11 #
12 # The address and port to which the UDP Server is bound. Multiple
13 # addresses can be bound at the same time. The binding address supports
14 # ipv4 and ipv6.
15 [[turn.interfaces]]
16 transport = "udp"
17 bind = "127.0.0.1:3478"
18 # external address
19 #
20 # specify the node external address and port.
21 # for the case of exposing the service to the outside,
22 # you need to manually specify the server external IP
23 # address and service listening port.
24 external = "127.0.0.1:3478"
25
26 [[turn.interfaces]]
27 transport = "tcp"
28 bind = "127.0.0.1:3478"
29 external = "127.0.0.1:3478"
30
31 [api]
32 # controller bind
33 #
34 # This option specifies the http server binding address used to control
35 # the turn server.
36 #
37 # Warn: This http server does not contain any means of authentication,
38 # and sensitive information and dangerous operations can be obtained
39 # through this service, please do not expose it directly to an unsafe
40 # environment.
41 bind = "127.0.0.1:3000"
42
43 # web hooks url
44 #
45 # This option is used to specify the http address of the hooks service.
46 #
47 # Warn: This http server does not contain any means of authentication,
48 # and sensitive information and dangerous operations can be obtained
49 # through this service, please do not expose it directly to an unsafe
50 # environment.
```

To configure the STUN/TURN WebRTC service, use the turn-server.toml:

- **Section [turn]:** Specifies the domain where the server is located.
- **Section [[turn.interfaces]]:** Indicates the listening interfaces. Describes the interface to which the STUN/TURN server is linked. Various interfaces can be indicated.
- **Section [turn.interfaces.transport]:** Defines the type of transport of the interface, which can be udp or tcp.
- **Section [turn.interfaces.bind]:** IP address and binding port of the internal socket.
- **Section [turn.interfaces.external]:** It is used to link to the address of your local NIC. For example, if you have two NICs, A and B, on your server, and the IP address of NIC A is 192.168.1.2 and that of NIC B is 192.168.1.3, if bound

to IAS A, you must bind to the address 192.168.1.2. Link to 0.0.0.0 It means that you listen to all interfaces at the same time. The word external means that your network card for the customer can “see” the IP address. Continuing with the previous example, if your network card A communicates with the outside, the other clients will see your LAN address (i.e., 192.168.1.2). However, in reality, the network topology where the server is deployed might have another public IP, such as 1.1.1.1, which is the IP address seen by other clients. The reason why they are needed bind and external is that, for the STUN protocol, the server needs to report its own external IP address, thus allowing the STUN client to connect to the specified address using the IP reported by the server.

- **Section [api.bind]:** Listening to the API for queries, for example: http://127.0.0.1:3000/info.
- **Section [log.level]:** Log level. Valid values: error, warn, info, debug, trace.
- **Section [auth]:** Username and password to access the server.

## 2. Start of Service

Start the STUN Server service (Aranda Turn Stun WebRTC Server) for the configuration changes to take effect.

## 3. Firewall Settings

Open the port or ports configured in step 1 in the local firewall inbound rules and in the network controllers present in the client infrastructure, for the protocols **TCP** and **UDP**. This step is essential to allow traffic through the new port and ensure that the STUN server can receive incoming connections on the configured port.

Workstations (ARC Agent) and specialist computers (Specialist Agent) must allow egress through the ports that are configured.

Additionally, if you require it to operate as TURN WebRTC, you must open the port range 49152-65535 for the protocol UDP.

## STUN/TURN Service Configuration Example and Scenarios

To make the server work for both devices inside and outside the network, follow these steps:

### 1. Set up the realm

Change the value of realm to the public domain or external IP address of your server. This is important for successfully authenticating external requests.

If your server’s public address is 1.2.3.4, set it to:

```
realm = "1.2.3.4"
```

### 2. Set up bind

The bind ensures that the STUN/TURN server listens on the private IP for connections within the local network.

If your server’s private address is 192.168.1.25, set it to:

```
bind = "192.168.1.25:3478"
```

If you require the STUN/TURN service to listen on all interfaces at the same time, configure it as:

```
bind = "0.0.0.0:3478"
```

These configurations are only required for [[turn.interfaces]].

### 3. Set up external

The external is where the server’s public IP is defined so that external computers can properly communicate with the STUN/TURN server.

If your server’s public address is 1.2.3.4, set it to:

```
external = "1.2.3.4"
```

```
external = "1.2.3.4:3478"
```

## 4. Authentication

The `[auth]` It is configured with static users:

```
[auth]
user1 = "test"
user2 = "test"
```

This allows authenticated connections with static credentials `user1:test` and `user2:test`. Be sure to use more secure credentials if you plan to expose this service to external devices.

The other sections can be left by default.

When you perform the parameterization in the `turn-server.toml`, this must be observed as follows:

```
[turn]

realm = "1.2.3.4" # IP pública del servidor

[[turn.interfaces]]
transport = "udp"
bind = "192.168.1.25:3478" # La IP privada del servidor en la red local o 0.0.0.0 cuando se desea escuchar todas las interfaces
external = "1.1.1.1:3478" # La IP pública del servidor visible desde el exterior

[[turn.interfaces]]
transport = "tcp"
bind = "192.168.1.25:3478" # La IP privada del servidor en la red local o 0.0.0.0 cuando se desea escuchar todas las interfaces
external = "1.1.1.1:3478" # La IP pública del servidor visible desde el exterior

[api]
bind = "127.0.0.1:3000"

[log]
level = "info"

[auth]
# Credenciales para autenticación TURN/STUN
user1 = "test"
user2 = "test"
```

Each time you make a modification to the `turn-server.toml`, restart the service `Aranda Turn Stun WebRTC Server` for the changes to take effect.

## Scenarios

The following scenarios and the result are described below according to the settings in the sample.

Scenario	Specialist	Network Status	ARC Agent	Network Status	Result
1	You can only access the TURN/STUN server using the public IP	External	You can only access the TURN/STUN server using the public IP.	External	The Specialist and the ARC Agent can establish communication by consuming the TURN/STUN server over the public IP.
2	You can only access the TURN/STUN server using the public IP.	External	You can access the TURN/STUN server using the public IP.	Internal	The Specialist and the ARC Agent can establish communication by consuming the TURN/STUN server over the public IP.
3	You can access the TURN/STUN server using the public IP.	Internal	You can access the TURN/STUN server using the public IP.	Internal	The Specialist and the ARC Agent can establish communication by consuming the TURN/STUN server over the public IP.
4	You can only access the TURN/STUN server using the private IP.	Internal	You can only access the TURN/STUN server using the private IP.	Internal	The Specialist and the ARC Agent can establish communication by consuming the TURN/STUN server over the private IP.
5	You can only access the TURN/STUN server using the public IP.	External	You cannot use the public IP to connect to the TURN/STUN server, as your access is restricted to the internal network (private IP).	Internal	The Specialist and the ARC Agent are unable to establish communication due to a connectivity problem between networks (external and internal).
6	You can only access the TURN/STUN server using the public IP.	External	You cannot use the public IP to connect to the TURN/STUN server, as its access is restricted.	External	The Specialist and the ARC Agent are unable to establish communication due to a connectivity problem between networks.

⚠ Note:

- To cover scenarios 1, 2, and 3, configure in the [AMD website](#) the External Turn server as follows:  
Name: configuration name.  
URL: turn.1.2.3.4:3478 (1.2.3.4 refers to the server’s public IP).  
User: user1.  
Password: test.

⚠ Notes:

- To cover the scenario (4), configure in the [ADM website](#) the External Turn server as follows:  
Name: configuration name.  
URL: turn.192.168.1.25:3478 (192.168.1.25 refers to the server’s private IP).

User: user1.

Password: test.

- If in the `turn-server.toml` was set up 0.0.0.0 in the parameter bind, the configuration must be performed on the site as above.

## ADM Installer/Agent

The ADM Agent is a program installed on managed devices that allows the generation of inventories and management tasks associated with distribution processes, updating and use of software, management of energy policies and remote control.

When you install the agent, a number of services are created on the device that allow you to establish communication with the remote control viewer and the overall management of the device.



There is an agent for each of the supported platforms:

- [ADM Agent Installer for Windows.](#)
- [ADM Agent Installer for Mac.](#)
- [ADM Agent Installer for Linux](#)

## Agent Deployment

Agent deployment is the process of distributing this component to the devices that need to be managed. The process of distributing and installing the ADM agent can be carried out from the ADM web console or using other deployment options, as follows:

- [Installation by Domain Policy](#)
- [Installation and distribution with Aranda Device Management ADM](#)

## ADM Installer/Agent on Windows

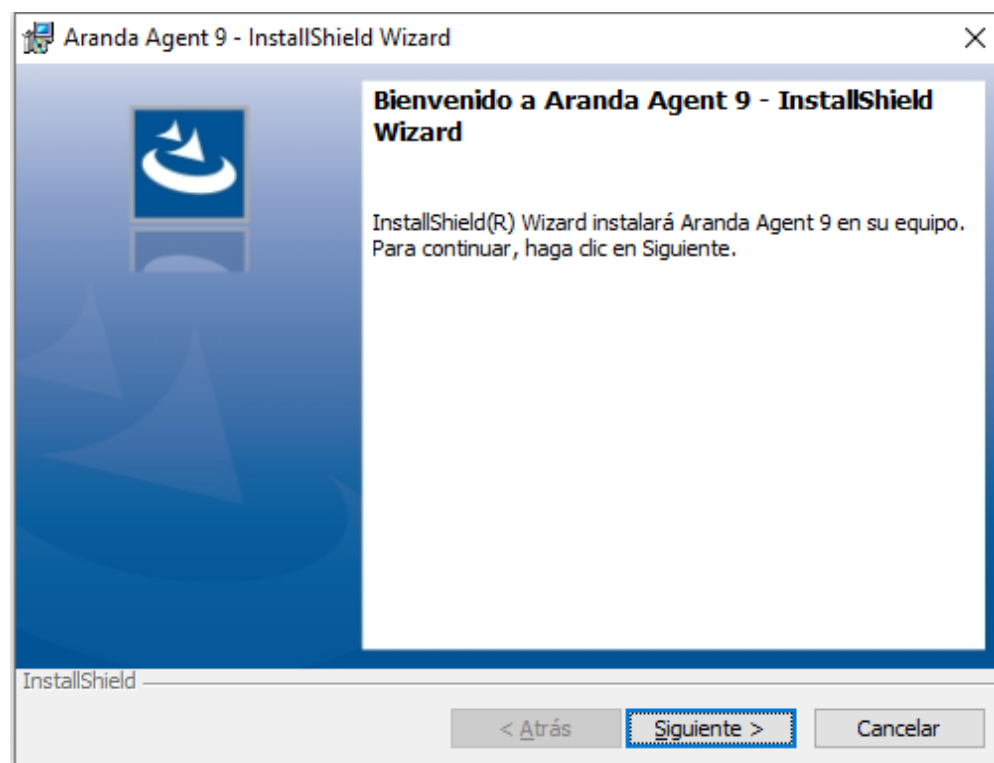
The third executable file is `Aranda.Agent.Windows.x86\_x64` which corresponds to the installer of the ADM Agent for Windows. This file is responsible for the creation and configuration of the services required for the operation of the ADM Agent for Windows.

The installer automatically detects the system language, currently supporting English, Spanish and Portuguese. If the configuration is in a different language, the installer defaults to Spanish.

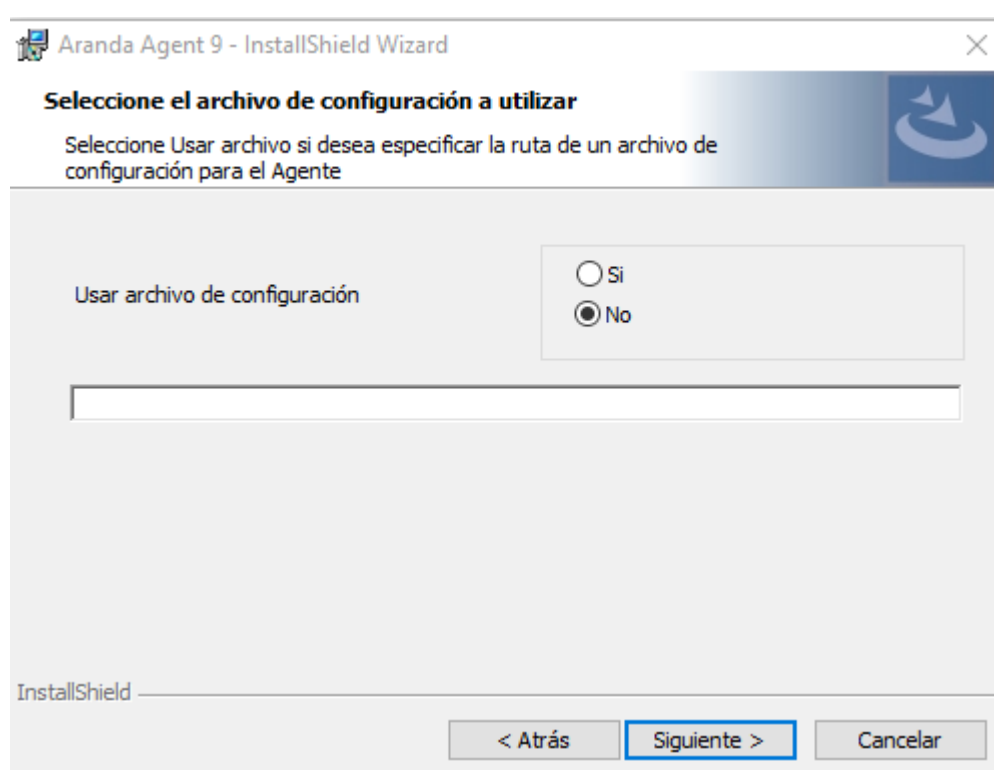
📌 **Note:** The agent can be installed unattended and automatically through the [Agent Distribution](#), or manually.

## Manual Agent Installation

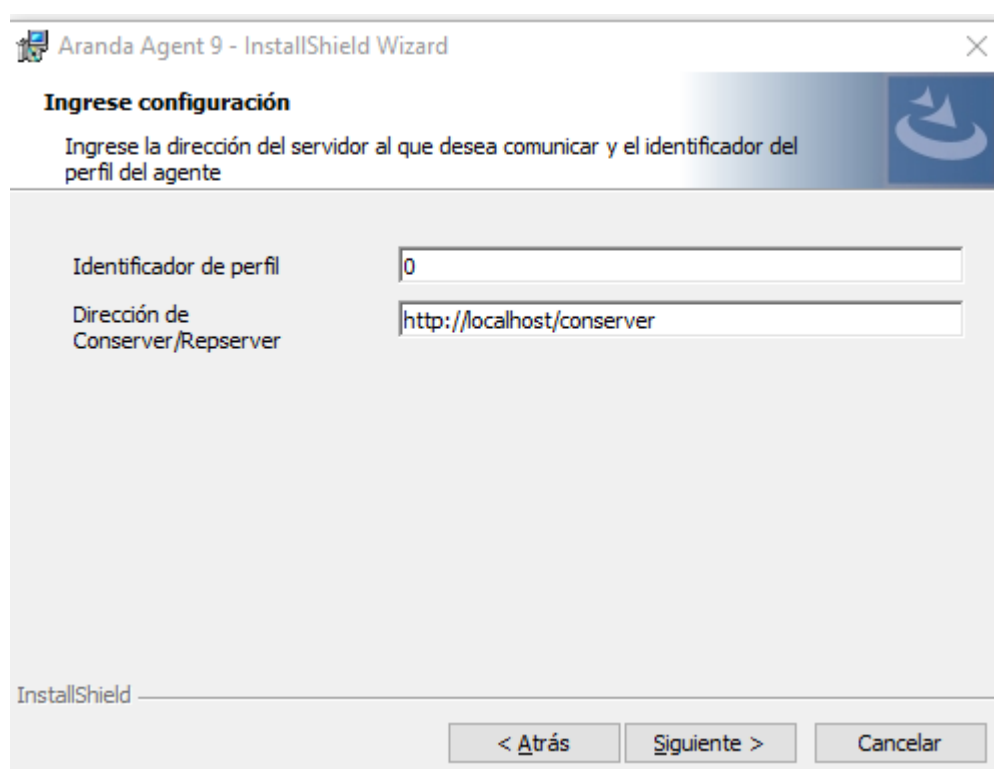
1. Click on the Aranda Agent installer. The wizard will start. Click **Following**.



2. If you have a configuration file select Yes and enter the path, otherwise select No and click Following.

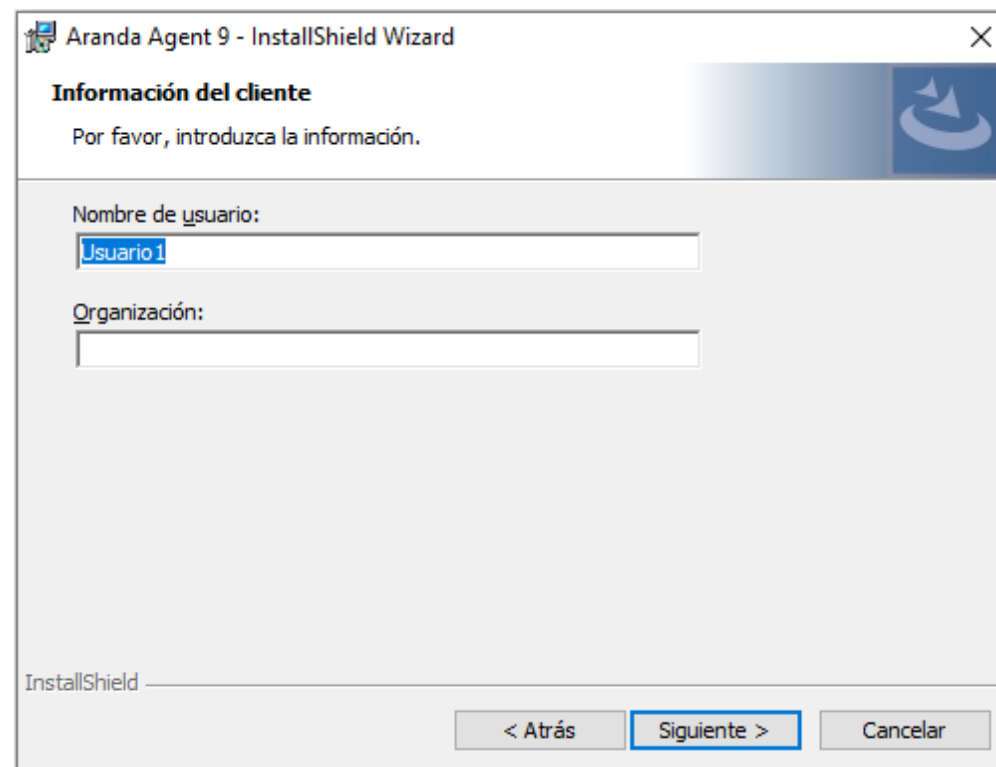


3. Enter the profile identifier, entering 0 downloads the profile that is configured by default. Enter the address of Conserver or Repserver according to the pointing configured in the MQTT broker [MQTT Broker Configuration](#). By entering the ADM console you can obtain the communication route. Configuration > ADM > Communications



📌 **Note:** Agent addressing when repserver only works with an agent version since 9.13.

4. Enter the username and organization where the agent will be installed.



Aranda Agent 9 - InstallShield Wizard

**Información del cliente**

Por favor, introduzca la información.

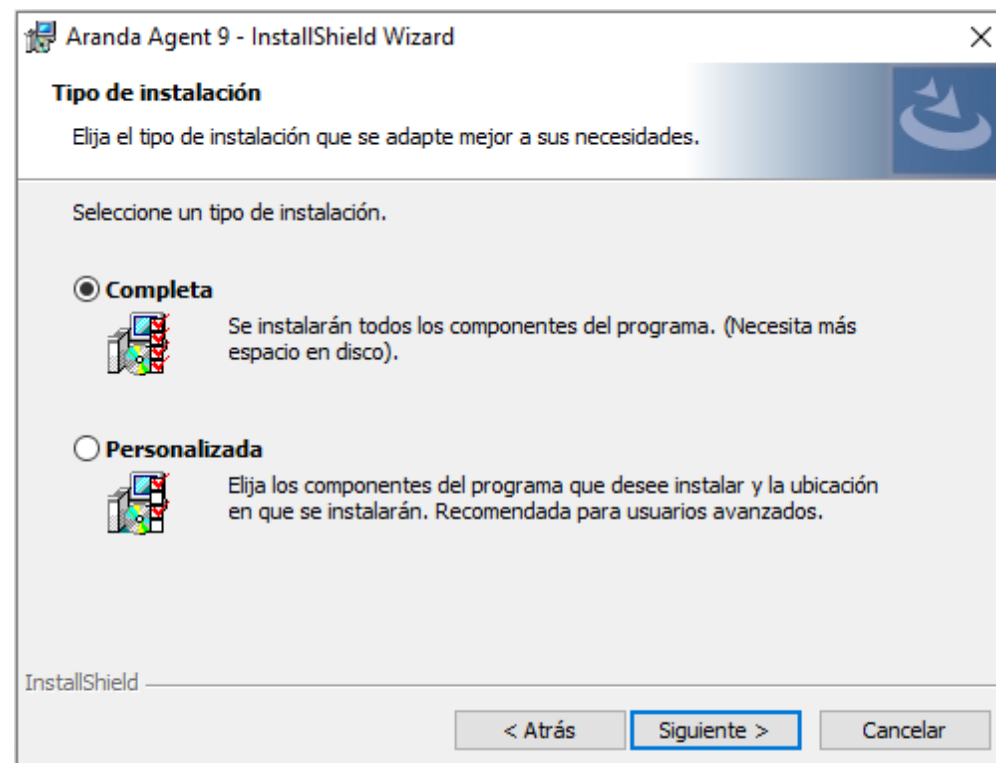
Nombre de usuario:

Organización:

InstallShield

< Atrás    **Siguiente >**    Cancelar

5. Select the type of installation you want to perform (complete or customized)) and click **Following**.





Aranda Agent 9 - InstallShield Wizard

**Tipo de instalación**

Elija el tipo de instalación que se adapte mejor a sus necesidades.

Seleccione un tipo de instalación.

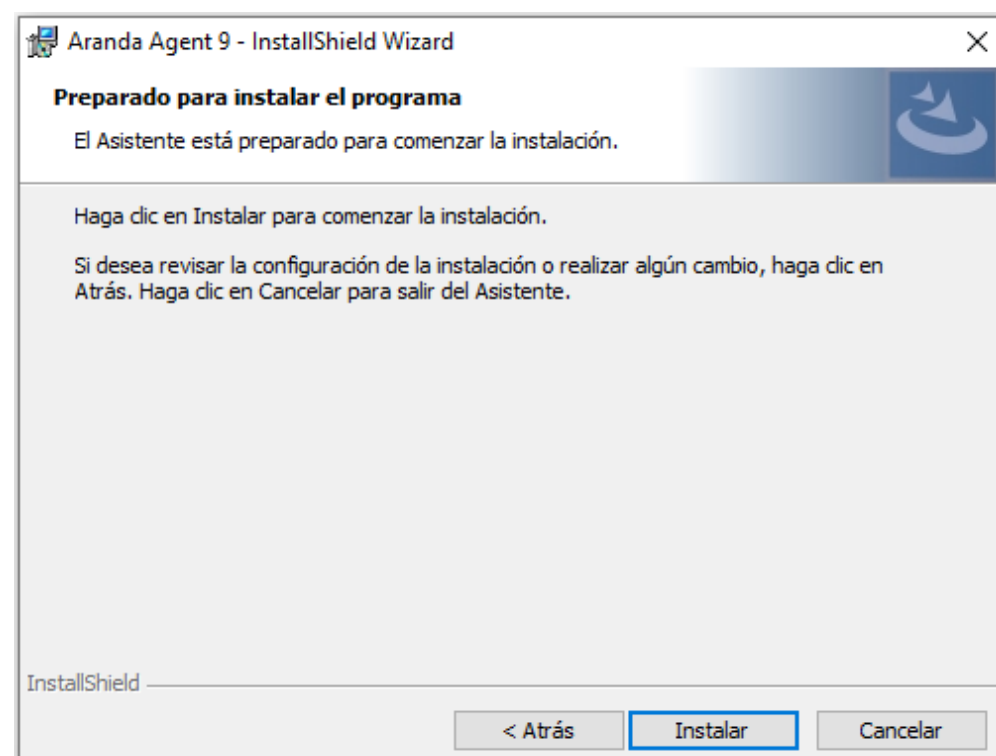
☒ **Completa**  
 Se instalarán todos los componentes del programa. (Necesita más espacio en disco).

☐ **Personalizada**  
 Elija los componentes del programa que desee instalar y la ubicación en que se instalarán. Recomendada para usuarios avanzados.

InstallShield

< Atrás    **Siguiente >**    Cancelar

6. Click **Install** to start the installation of the agent.



Aranda Agent 9 - InstallShield Wizard

**Preparado para instalar el programa**

El Asistente está preparado para comenzar la instalación.

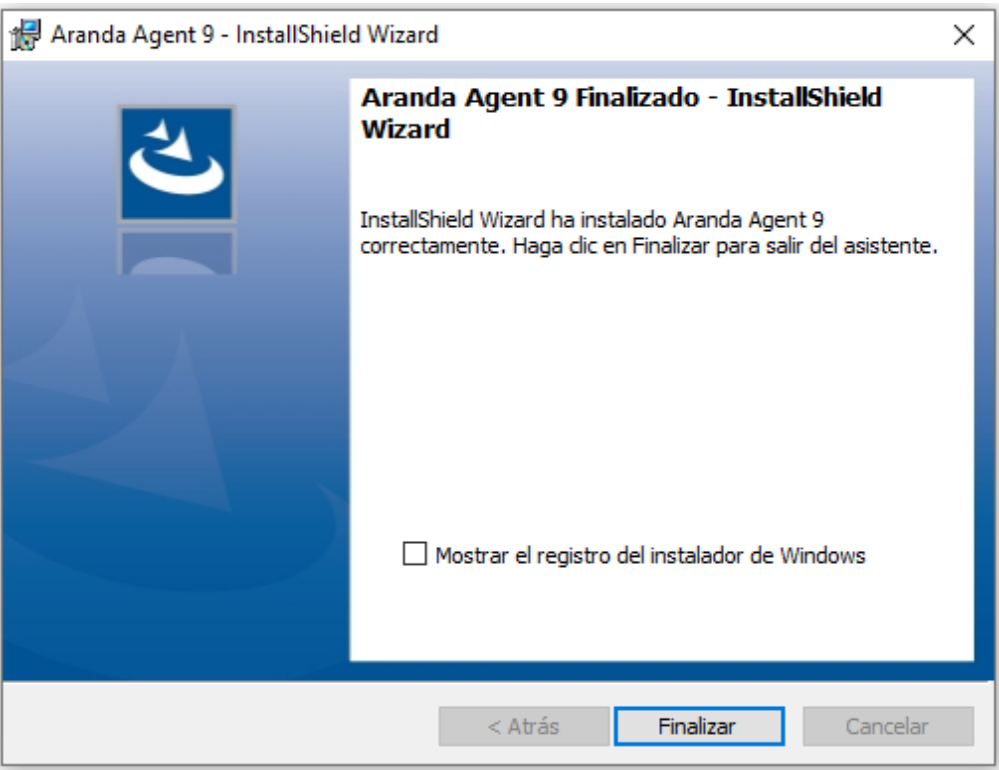
Haga clic en **Instalar** para comenzar la instalación.

Si desea revisar la configuración de la instalación o realizar algún cambio, haga clic en **Atrás**. Haga clic en **Cancelar** para salir del Asistente.

InstallShield

< Atrás    **Instalar**    Cancelar

7. When the agent installation is complete, click **End**



—

## Manual Agent Installation by Command Line

To install the ADM Agent by command line, you can execute the following statement from the *command prompt* of Windows:

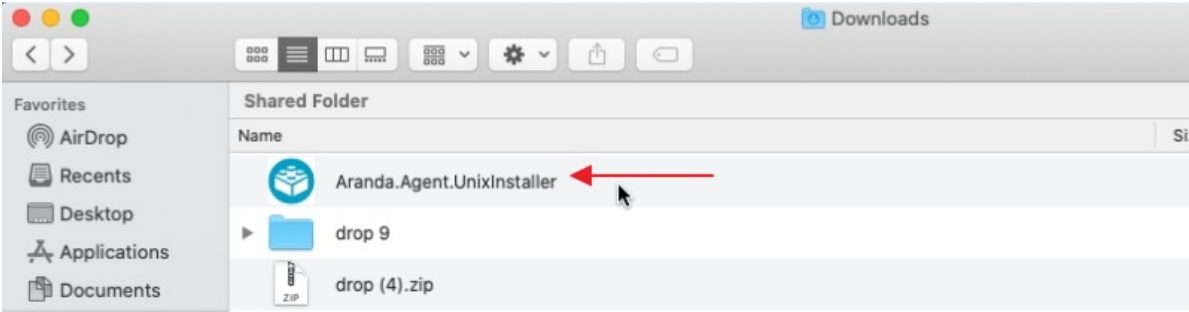
```
Aranda.Agent.Windows.x86_x64.9.xx.xxxx.xxxx.exe /S /V"/norestart /qn
AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=0"
```

AGENT_PROFILE_ID=[UNIT]	Identifier of the profile to be installed, 0 is a profile selected in the application as the default profile.
AGENT_SERVER_ADDRESS=[STRING]	Path of the Server.

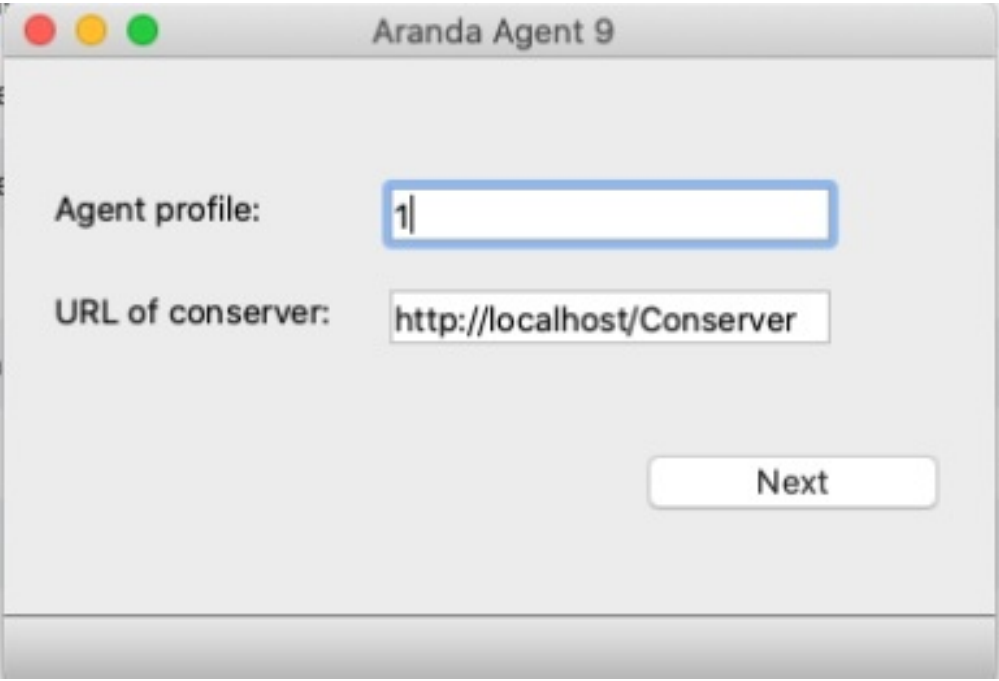
## ADM Installer/Agent on MacOS

### Installing the agent from the UI

1. Run the agent app.

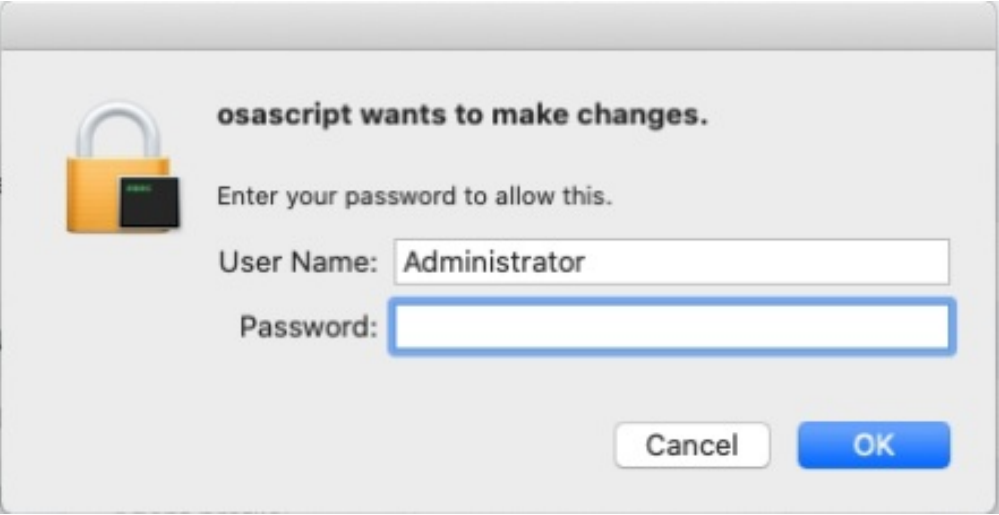


2. Enter the profile identifier, typing 0 downloads the profile that is configured by default. Register the Conserver or Repserver address according to the pointing configured in the MQTT broker [MQTT Broker Configuration](#). When you enter the ADM console you will be able to obtain the communication path. Configuration > ADM > Communications

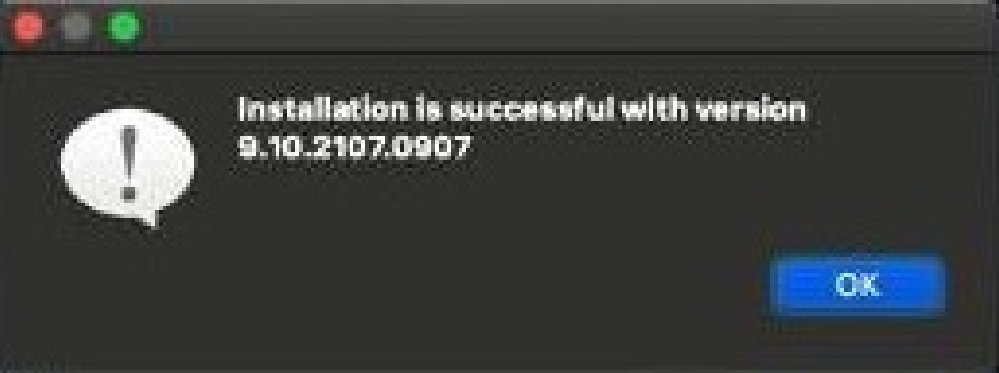


⚠ **Note:** Agent addressing when repserver only works with an agent version since 9.13.

3. Enter the device credentials.



4. The agent will be installed and a success message will be displayed.



5. When the installation is complete, you will be able to view the device in the ADM console.

⚠ **Note:** If you already have an agent installed, you will be able to see the following messages.

Message	Description
The version to be installed is the same as the installed version	This case is used to update the data in the conserver.
The version to be installed is lower than the installed version	In this case, the installation of the agent being installed will be prevented.

### Installing the agent from the command line

1. To install the Aranda DEVICE MANAGEMENT ADM agent via command line, run the following statement from a MacOS shell:

```
sudo sh RUTA_INSTALLADOR/Aranda.Agent.Mac.x64.9.3.1801.3001.sh --
AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=0
```

Line	Instruction
RUTA_INSTALLADOR	Path where the installer is located, can be relative or absolute
AGENT_PROFILE_ID=[UNIT]	Identifier of the profile to be installed, 0 is a profile selected in the application as the default profile
AGENT_SERVER_ADDRESS=[STRING]	Conserver or Repserver Path

2. After installing the agent, a folder named Aranda is created in the path `/Opt/local` with the libraries, agent services, and another folder in `/etc/` with the name Aranda, where the agent’s logs and database are stored. Deleting these folders will uninstall the agent.

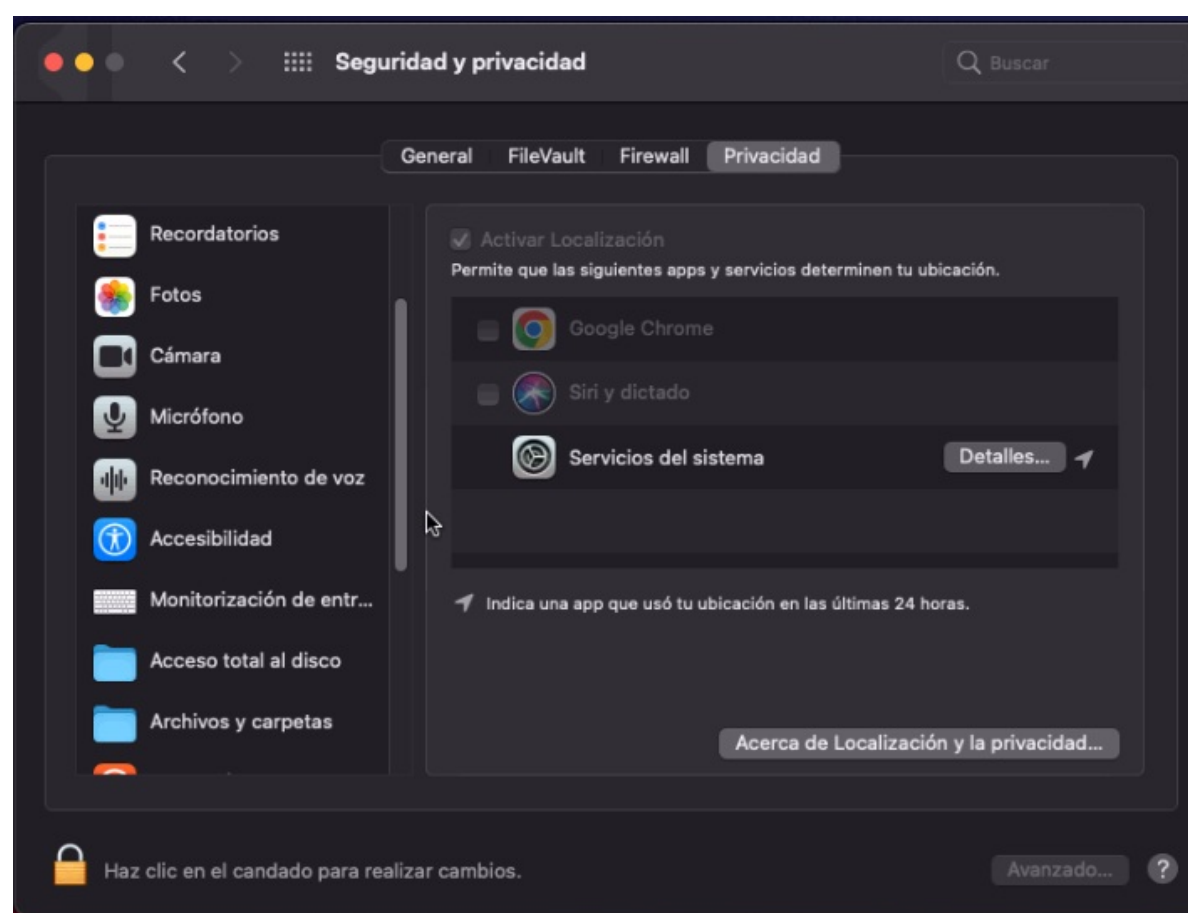
## Grant agent permissions

Full disk access permission must be granted to the agent, this action is performed taking into account the following steps:

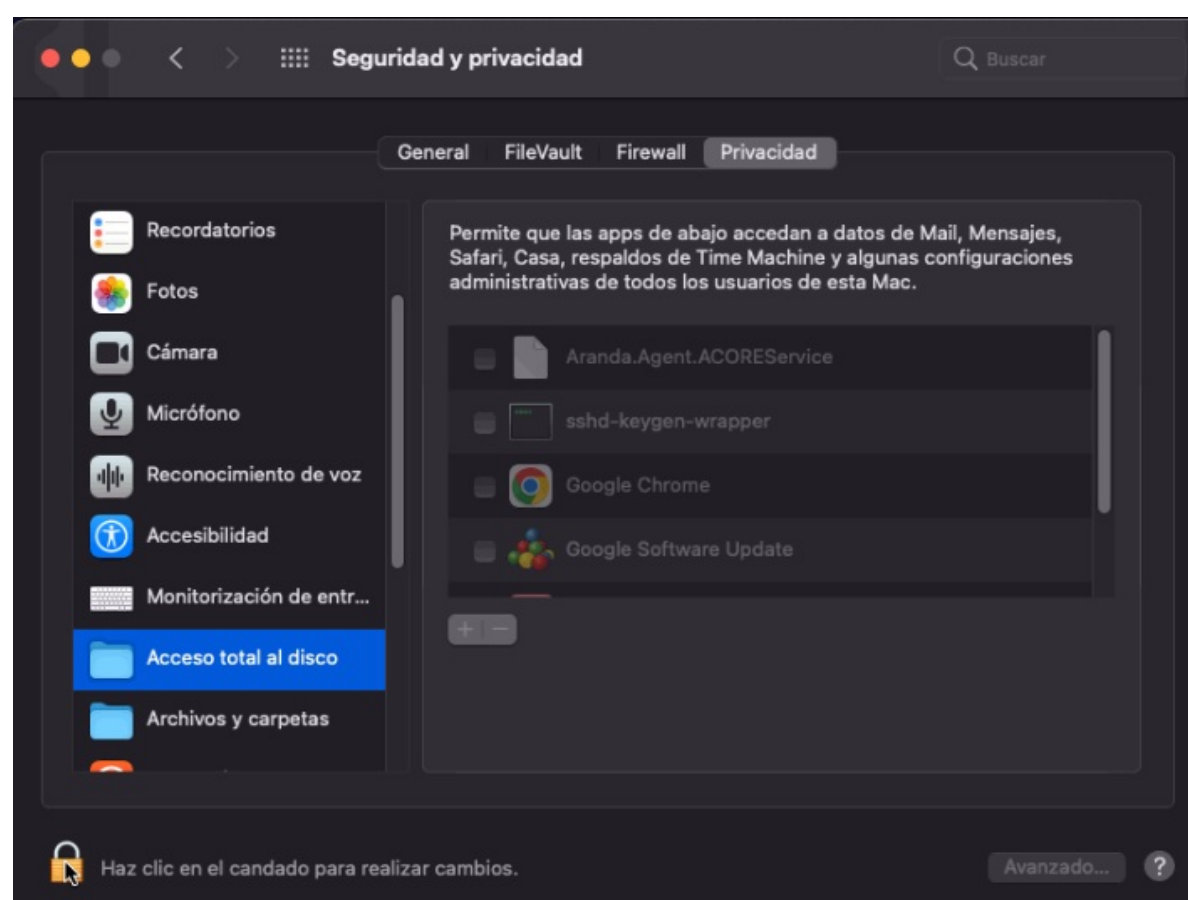
1. Open System Preferences > Security & Privacy.



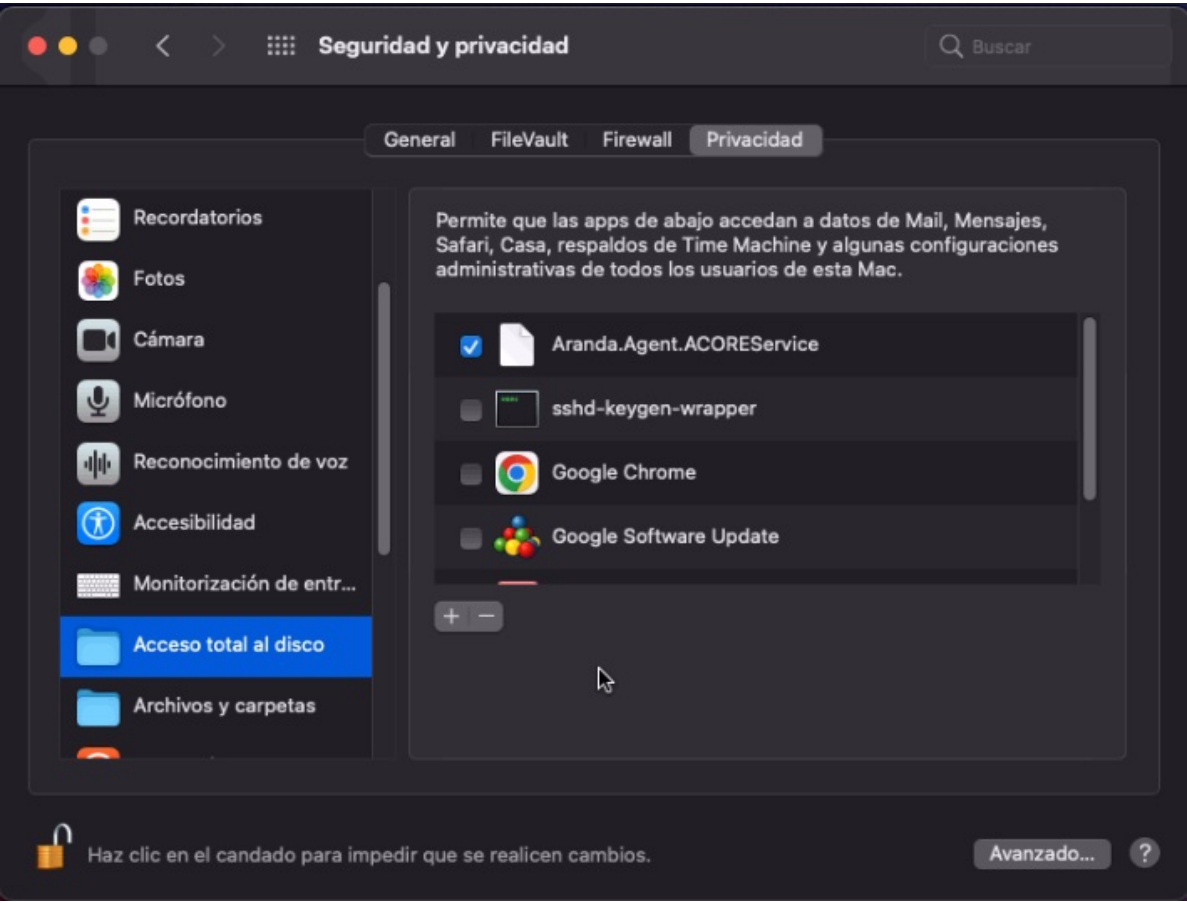
2.Select the Privacy.



3. Select Full disk access and click the lock icon. Enter the system administrator credentials and click Unblock.



4. Select Service Aranda.Agent.ACOREService icon, then click the lock icon.



—

## Agent exceptions on macOS

The functionalities currently supported in MAC are the Aranda Asset Manager except for the following functionalities.

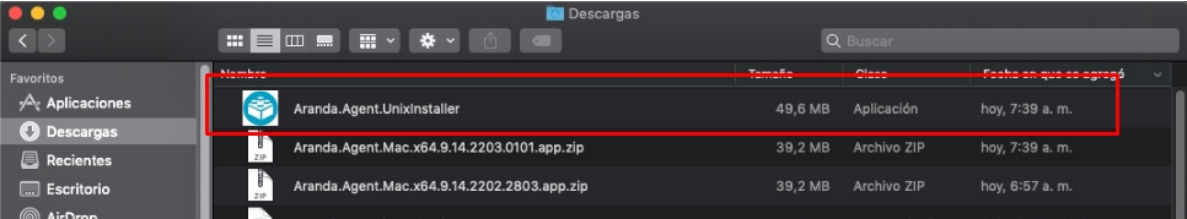
- Device Location
- Deleting Files by Extension
- Virtualization
- Monitoring
- Sending messages
- Sending Commands (Only allowed with the current system user)

## Agent Modification

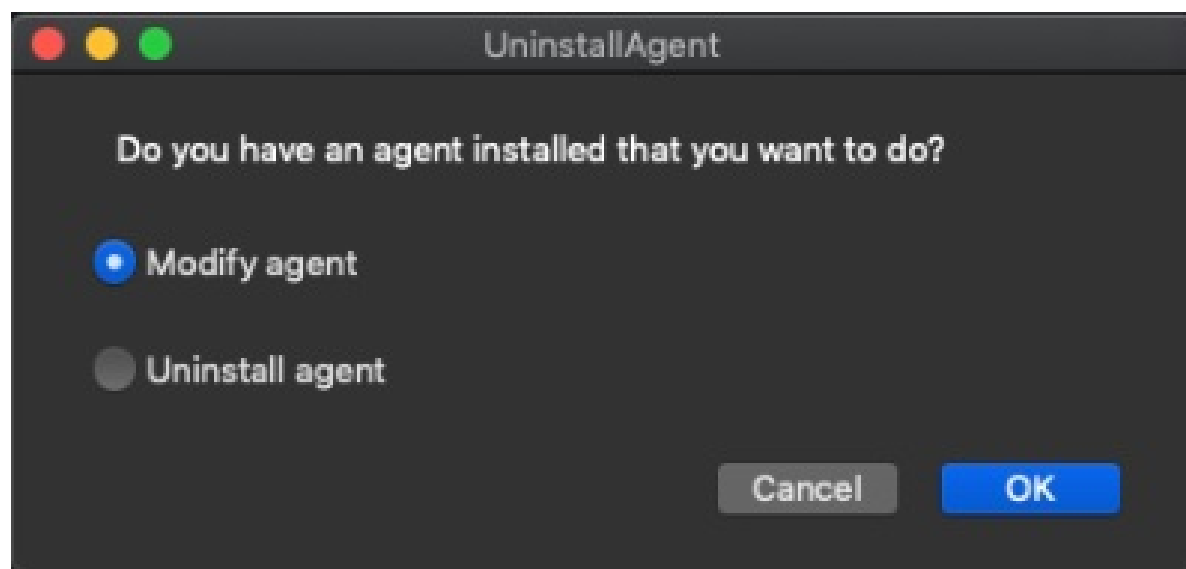
📌 **Note:** Available in the agent version higher than 9.14,  
If you have an agent installed earlier than this, the uninstall window will not appear.

## Agent Modification (Repserver Host or Conserver and Profile)

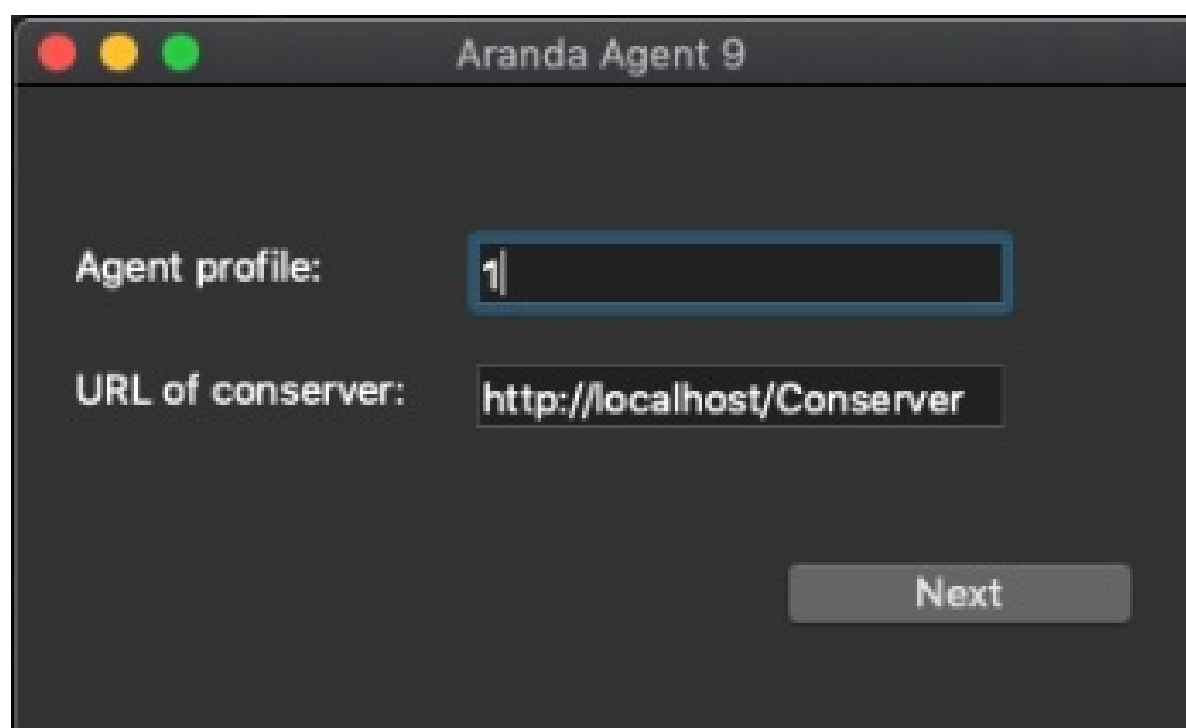
1. To modify the agent you can do it from the installer `Aranda.Agent.Unixinstaller.app`



2. Double click in the executable and the following window is enabled.



3. By default the option of Modify agent is selected; Click OK and the installation window is enabled. After upgrading click Next.



—

## Uninstalling Agent

To uninstall the agent you will have two options:

- By [Command Line](#) using the terminal.
- Using the [graphical interface](#).

## Command Line

1. Open a terminal window and in the defined path use the following command:

```
cd /opt/local/aranda
```

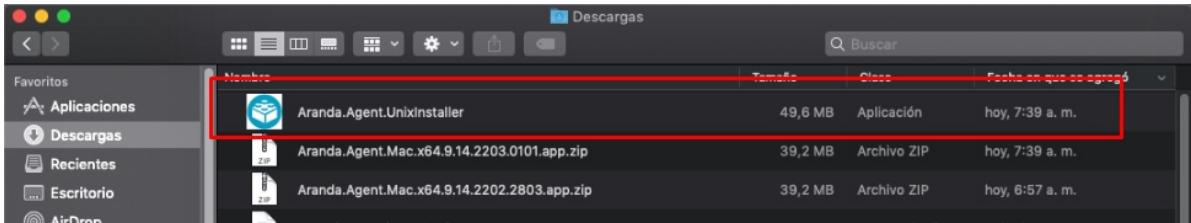
2. Once the folder is entered Aranda We run the following command.

```
sudo sh UninstallAgent.sh
```

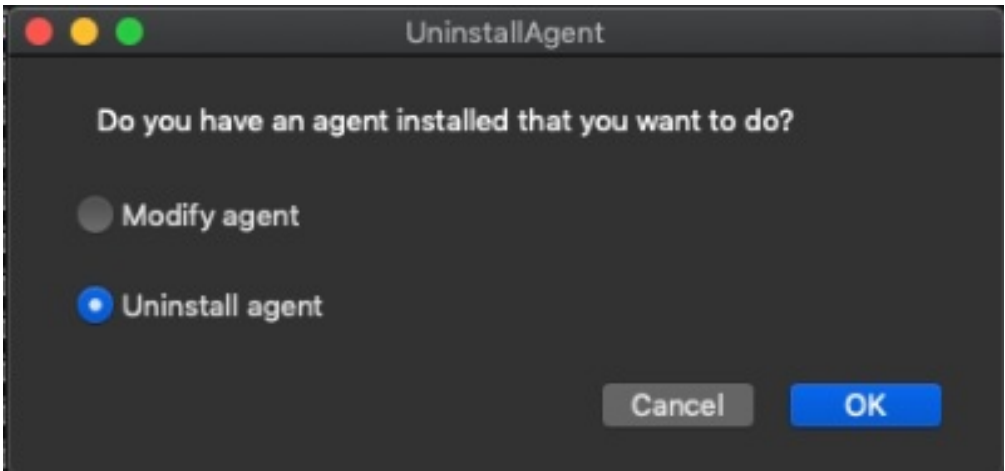
3. Once the command is executed, you can see that the agent was successfully uninstalled.

## Graphical Interface

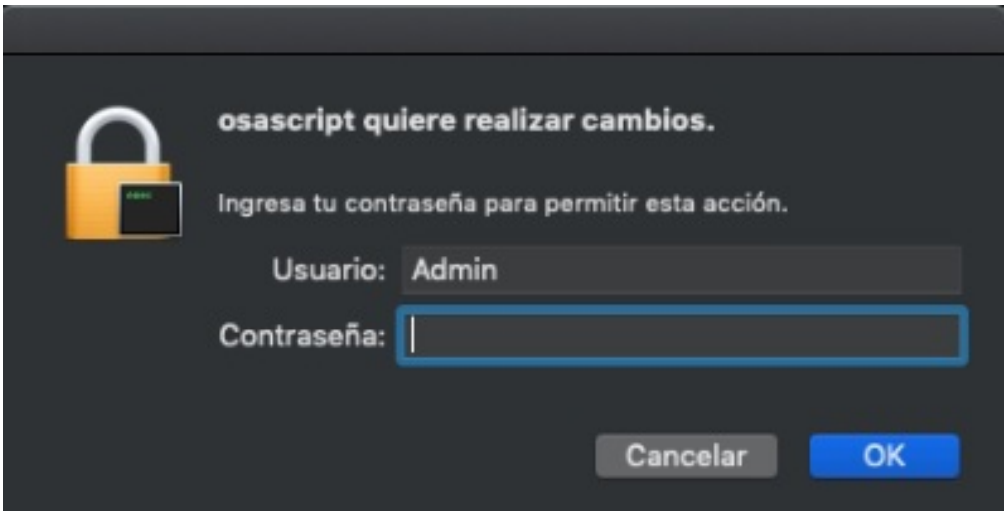
1. Run the installer Aranda.Agent.Unixinstaller.app.



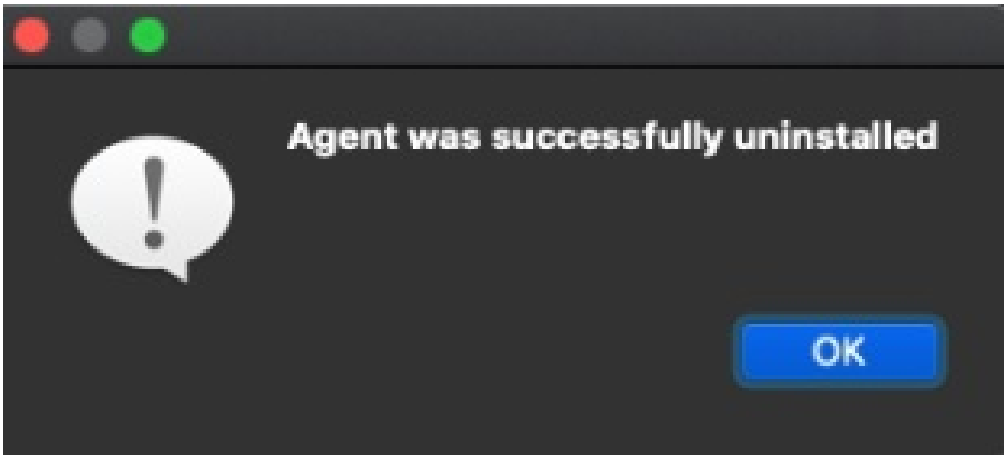
2. In the Uninstall Agent window, select the Uninstall agent and click OK



3. The next window asks for the credentials of the computer administrator; Enter the password and clickOK



4.Wait a few seconds for the uninstall to finish and a confirmation message is enabled



## Linux ADM Installer/Agent

### Manually installing the Command-Line Agent on Linux

1. To perform the Aranda DEVICE MANAGEMENT ADM Agent installation by command line, the following statement can be executed from a Linux or macOS shell.

Enter the Conserver or Repserver address depending on the MQTT broker configuration [MQTT Broker Configuration](#). By entering the ADM console you can obtain the communication route **Configuration > ADM > Communications**.

```
sudo sh RUTA_INSTALLADOR/Aranda.Agent.Linux.x64.9.3.1801.3001.sh --
AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=0
```

Donde:

Line	Description
ROUTE_INSTALLER	Path where the installer is located, can be relative or absolute.
AGENT_PROFILE_ID=[UNIT]	Identifier of the profile to be installed, 0 is a profile selected in the application as the default profile
AGENT_SERVER_ADDRESS=[STRING]	Conserver or Repserver path.

📌 **Note:** Agent addressing when repserver only works with an agent version since 9.13.

2. Después de instalar el agente se crea una carpeta con el nombre Aranda en la ruta ‘/Opt/’ con las librerías, servicios del agente y otra carpeta en ‘/etc/ ’ con el nombre Aranda, donde se guardan los logs y la base de datos del agente. Al borrar estas carpetas se desinstalará el agente.

### Agent exceptions on Linux

The module is currently supported Aranda Asset Manager I expect the following functionalities:

- Device Location
- Virtualization
- Monitoring
- Sending messages
- Sending Commands (Only allowed with the current system user)

### Manual uninstallation of the Command Line Agent on Linux

📌 **Note:** Available in the agent version higher than 9.14.

You can uninstall the Linux agent via the command line by following these steps: 1. Open a terminal window and in the defined path use the following command:

```
cd /opt/aranda
```

2. Once you enter the folder *Aranda* Run the following command.

```
sudo sh UninstallAgent.sh
```

3. Once the command is executed, you will be able to see that the agent has been successfully uninstalled.

### Database connection configuration

Once the installation of Aranda Device Management, proceed to configure the connection strings to the database of the sites and services.

To configure the sites, Common and Licensing services, it is done through the Aranda Database Tools v9. To do this:

1. Run the module and click on the Connection String.

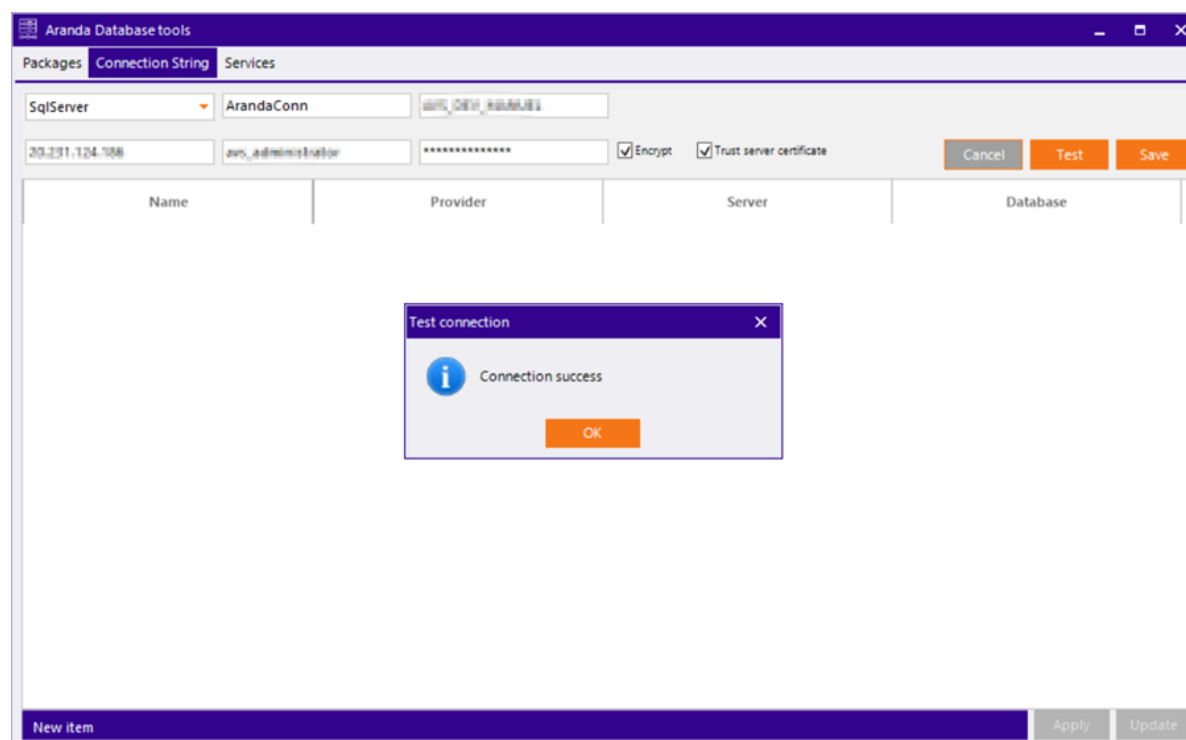
The screenshot shows the 'Aranda Database tools' window with the 'Connection String' tab selected. The 'Packages' dropdown is set to 'SqlServer'. The 'Connection Name' field is empty, and the 'Database' field is empty. The 'Server Name' field is empty, the 'User Name' field is empty, and the 'Password' field is masked with asterisks. The 'Encrypt' checkbox is unchecked, and the 'Trust server certificate' checkbox is unchecked. The 'Cancel', 'Test', and 'Save' buttons are visible. Below the input fields is a table with columns 'Name', 'Provider', 'Server', and 'Database'. The table is currently empty. At the bottom, there is a 'New item' button and 'Apply' and 'Update' buttons.

2. Fill in the requested data.

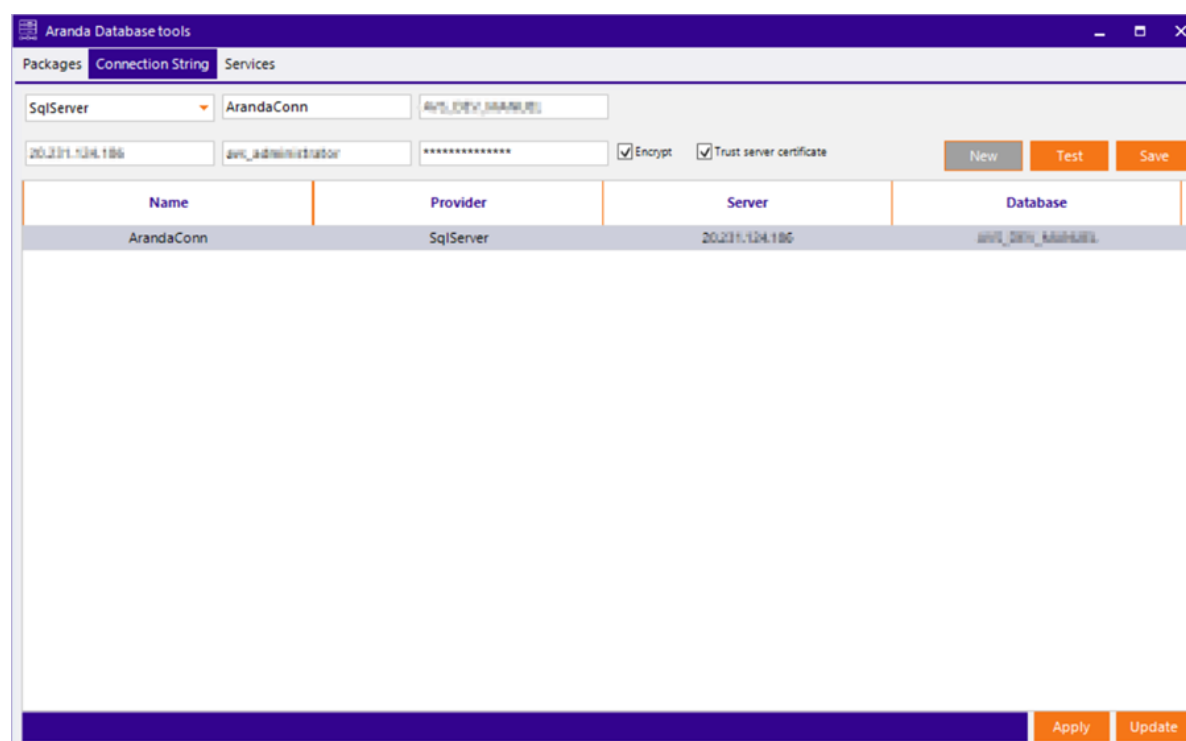
- Select the database engine (SQL Server).
- Give it a name to identify the connection.
- Record the connection data (database name, server name or IP address, and if required username and password).
- In case the database port is different from the default port (1433 for SQL Server), the server must be written as servername:port (e.g. ARANDADBSERVER:5555)
- By default, the "Encrypt" option should be checked to ensure that the connection between the solution and the database is encrypted.

The screenshot shows the 'Aranda Database tools' window with the 'Connection String' tab selected. The 'Packages' dropdown is set to 'SqlServer'. The 'Connection Name' field is filled with 'ArandaConn'. The 'Database' field is filled with 'ARANDA\_DB'. The 'Server Name' field is filled with 'dev\_134.136'. The 'User Name' field is filled with 'dev\_administrator', and the 'Password' field is masked with asterisks. The 'Encrypt' checkbox is checked, and the 'Trust server certificate' checkbox is checked. The 'Cancel', 'Test', and 'Save' buttons are visible. Below the input fields is a table with columns 'Name', 'Provider', 'Server', and 'Database'. The table is currently empty. At the bottom, there is a 'New item' button and 'Apply' and 'Update' buttons.

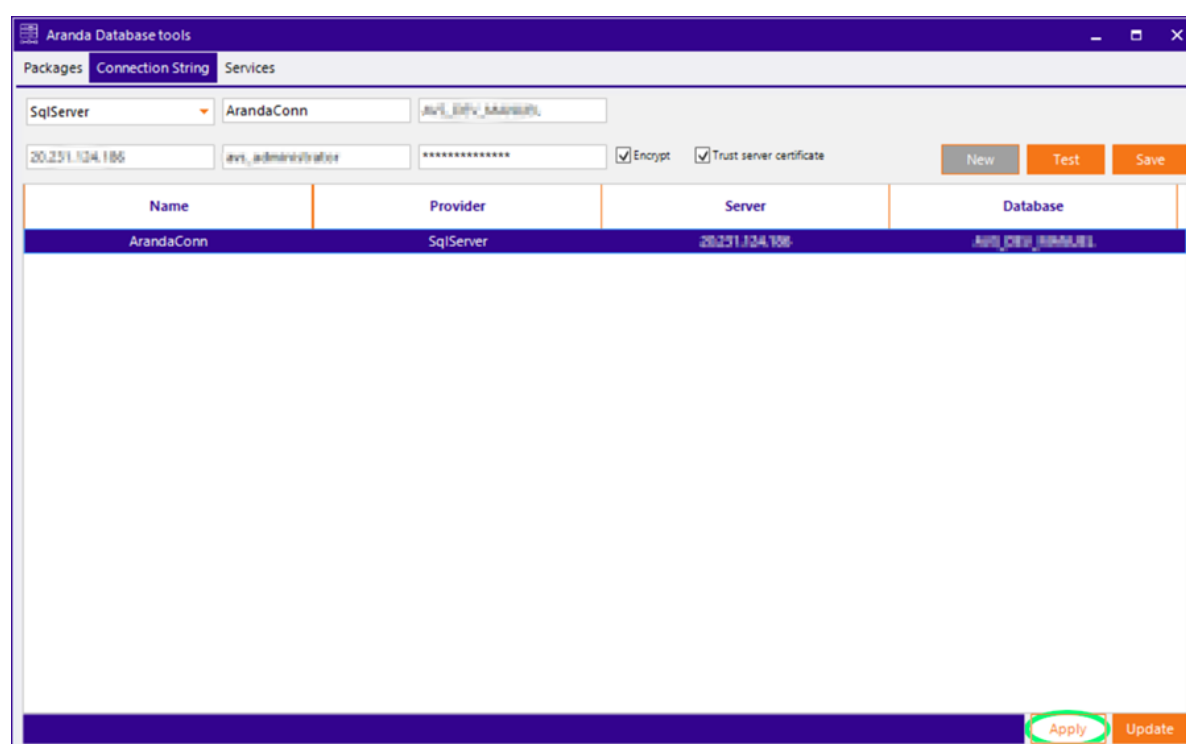
3. Click the Test to check the connection.



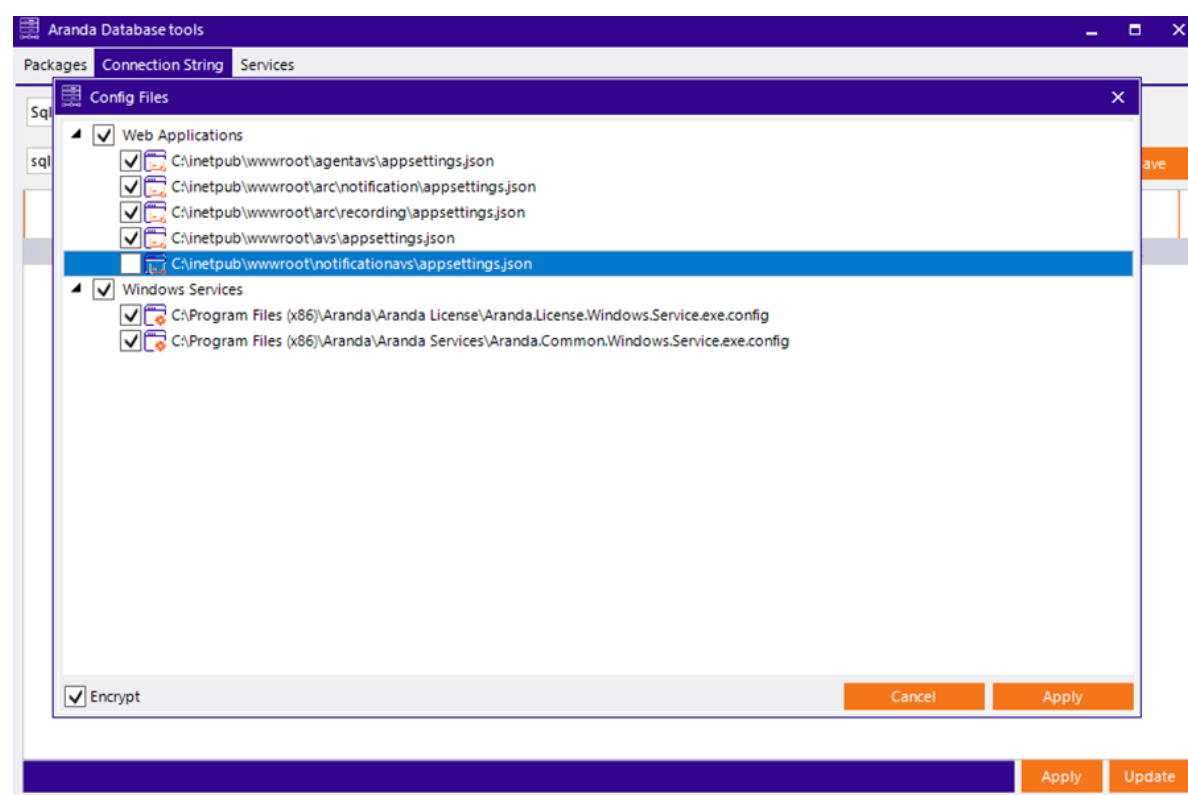
4. To finish click on the Save to save the connection.



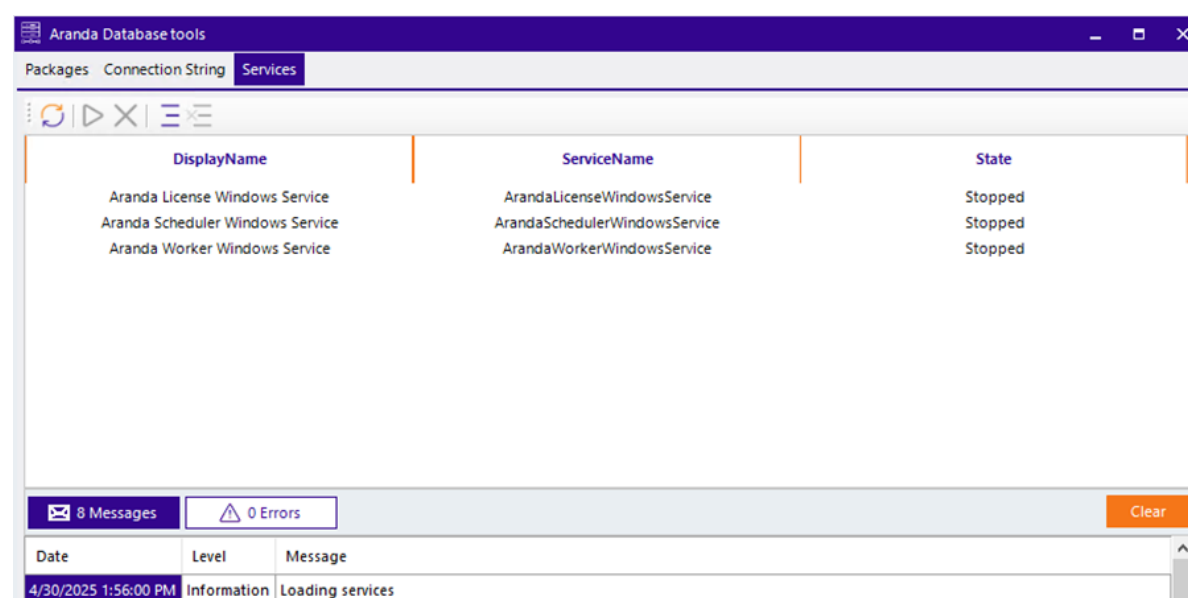
5. To apply connection strings to installed services, select the previously created connection and click the Apply.



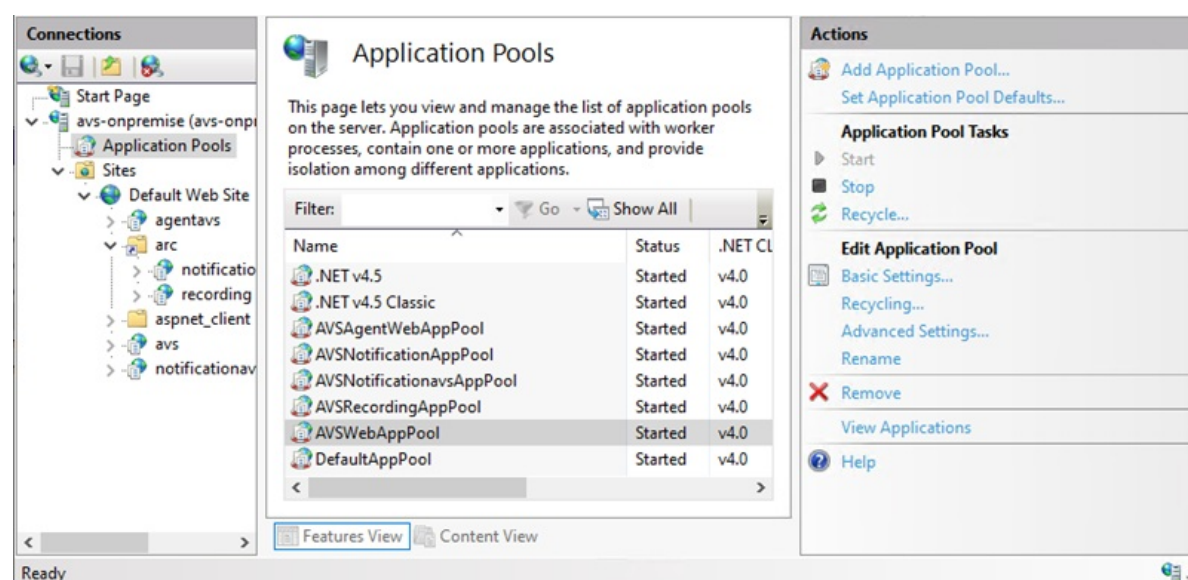
6. A window is enabled with the list of applications and services available on the server. For the sitenotificationADM You don't need to apply the connection string settings.



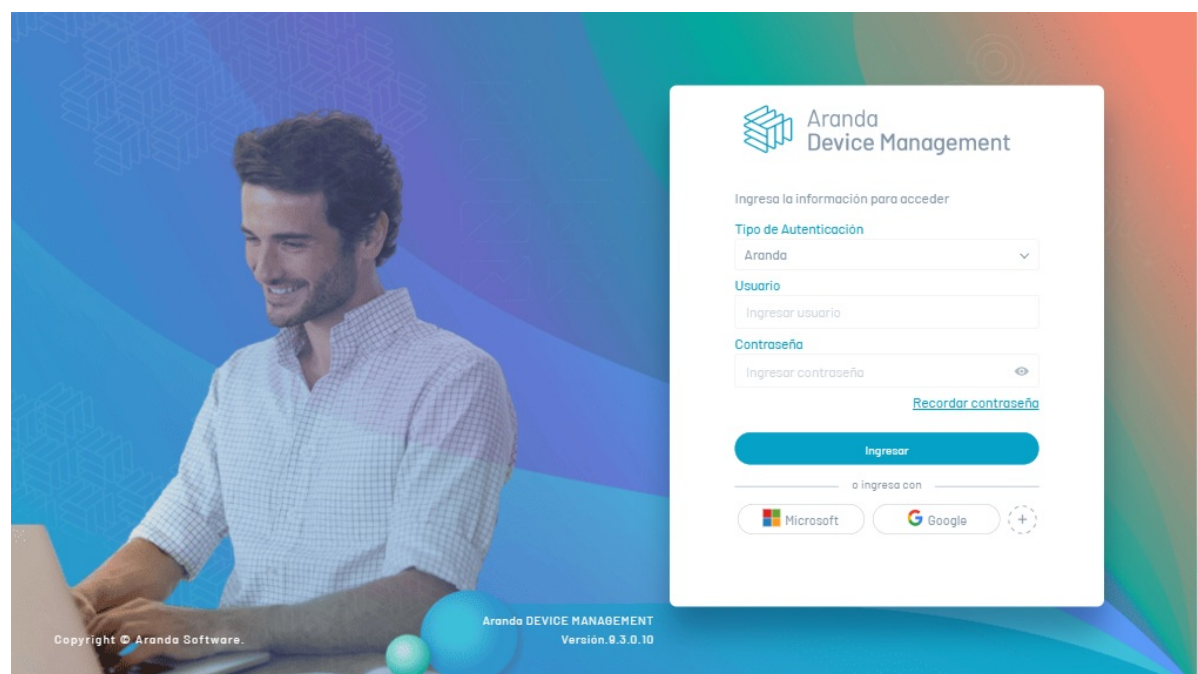
7. Select the appropriate services and click the **Apply**. If you want to encrypt the connection, check the box **Encrypt** in the lower-left corner. An alert message may be displayed because encryption is not supported for JSON files. 8. To finish, click on the **Services** and start all services.



⚠ **Important** When changes are made to the connection strings of the sites, the application pool associated with the site must be restarted or recycled so that the change is applied immediately.



9. Once the connection is established, you will be able to access the ADM website where you can start with the configuration of Aranda Device Management through the following URL: [http\(s\)://name\\_servidor/adm/](http(s)://name_servidor/adm/).

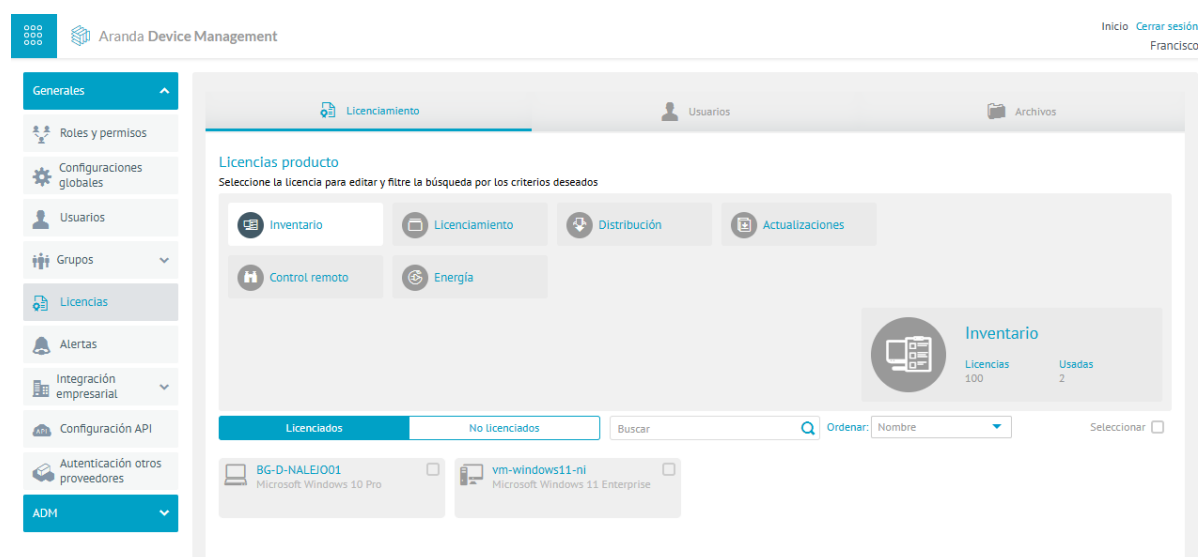


## ADM Licensing

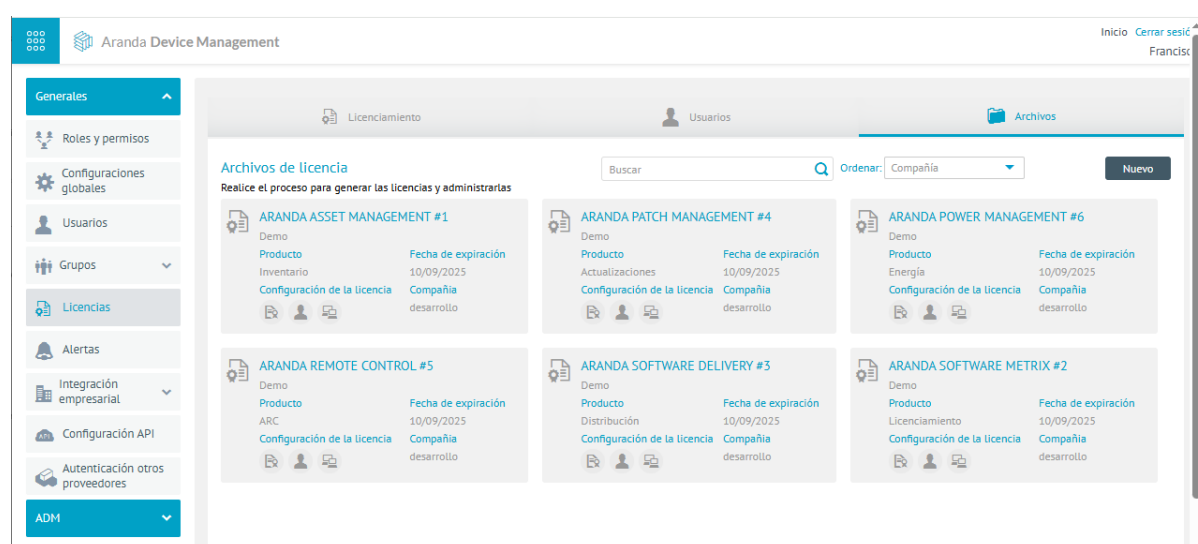
All Aranda Software products require a license to operate, for this reason ADM uses Aranda's common licensing service to authorize users to enter the console and control the licenses purchased, among other operations.

## Upload Licensing File

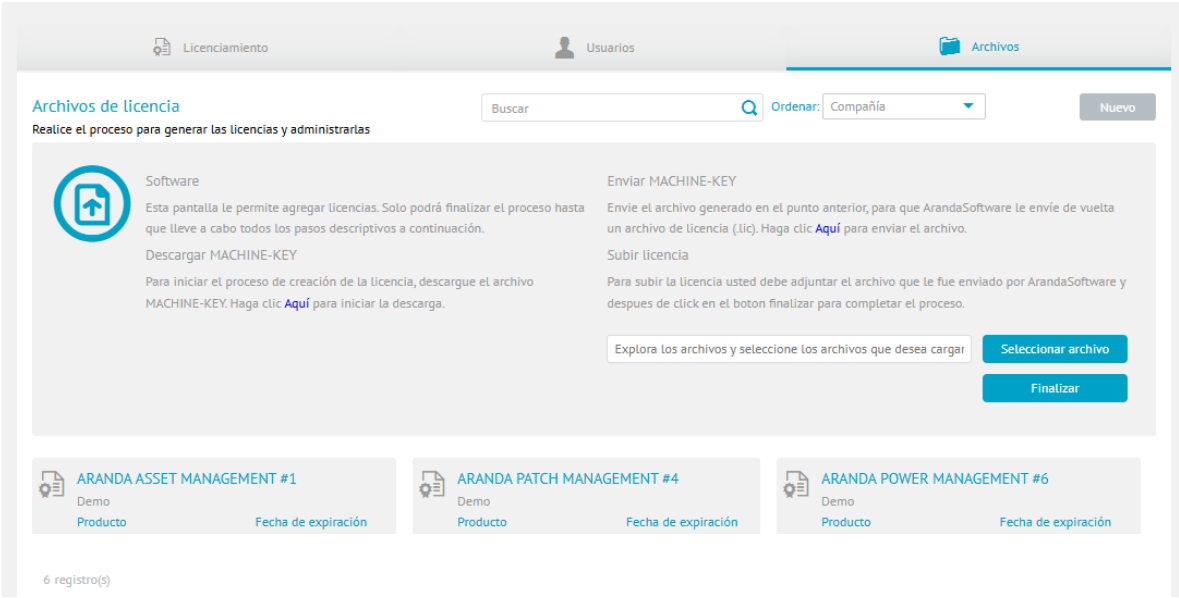
1. To upload the licensing file, the first time you enter the Aranda Device Management (ADM) website, go to the configuration view of the ADM web console, in the **General** from the main menu, select the **Licences**. In the information view, you can view information associated with licensing.



2. In the information view, select the **Records** and click the **New**.



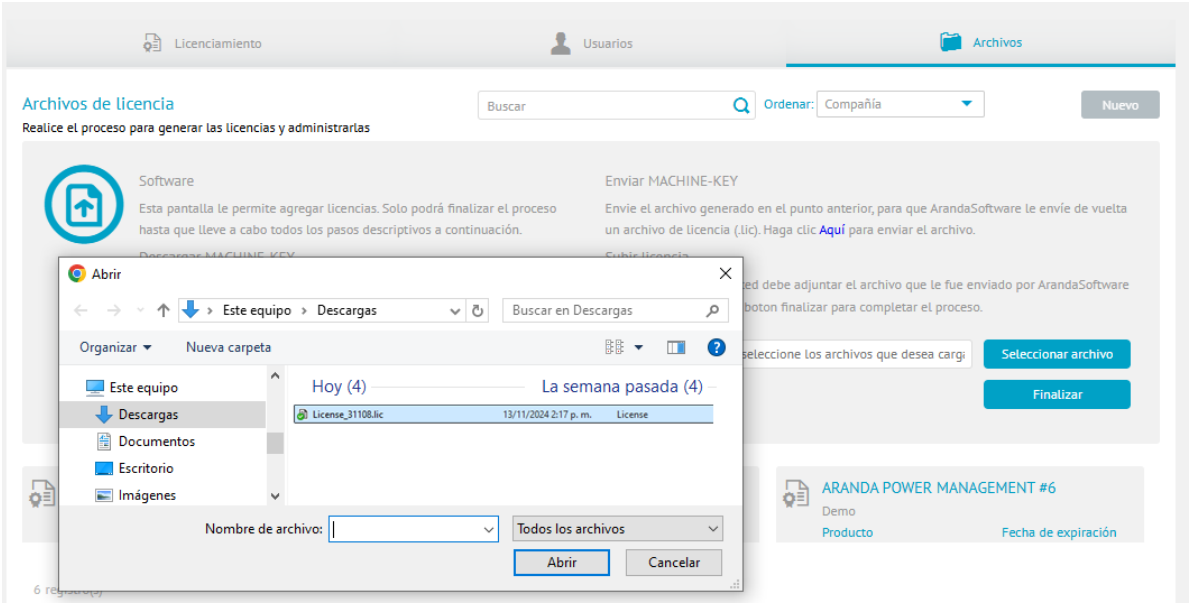
3. In the window that is enabled select the **Download MACHINE-KEY** option, click on the link [Here](#), which allows the download of the MachineKey.amk file (licensing file), which must be sent to the area in charge of Aranda Software (Pre-Sales and Projects) for the generation of the .lic file (licensing file).



⚠ **Warning:** Once the user uploads their purchased licenses from the console, the common licensing service must remain on the same machine, otherwise the uploaded licenses will be lost.

⚠ **Warning:** If your application server is located on a virtual machine, it is recommended that you install the Common Licensing Service on a physical machine, because when you restart virtual machines, there is a high probability that the hardware brand will change and the service will incorrectly assume that it was moved.

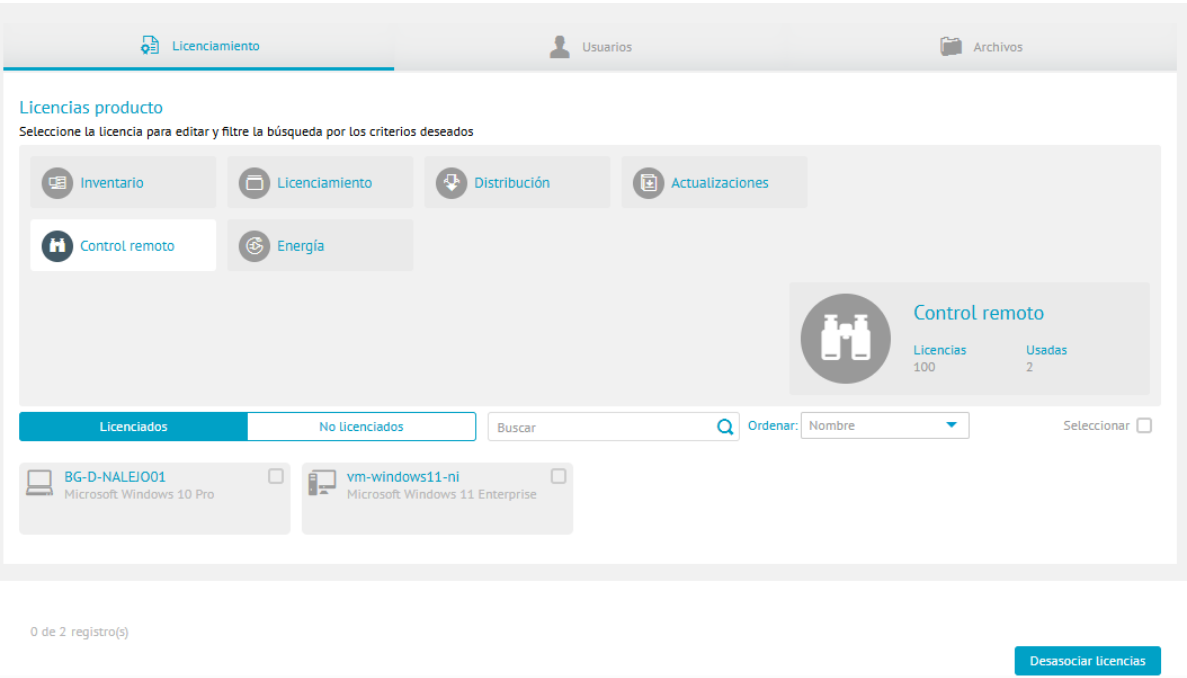
4. Once you have received the .lic file (licensing file), you need to upload it to the server, click on the **Select File** and then in **End**.



## View/Associate Licensed Devices

5. To view the license detail and licensed devices, in the Licensing information view, select the **Licensing** and the license by ADM management module (Inventory, Licensing, Distribution, Updates, Remote Control and Energy). The **Licensed** and **Unlicensed** options group the devices found.

6. By selecting one or more devices, you can select the respective button to **Associate Licenses** or **Disassociate Licenses** to the chosen devices.

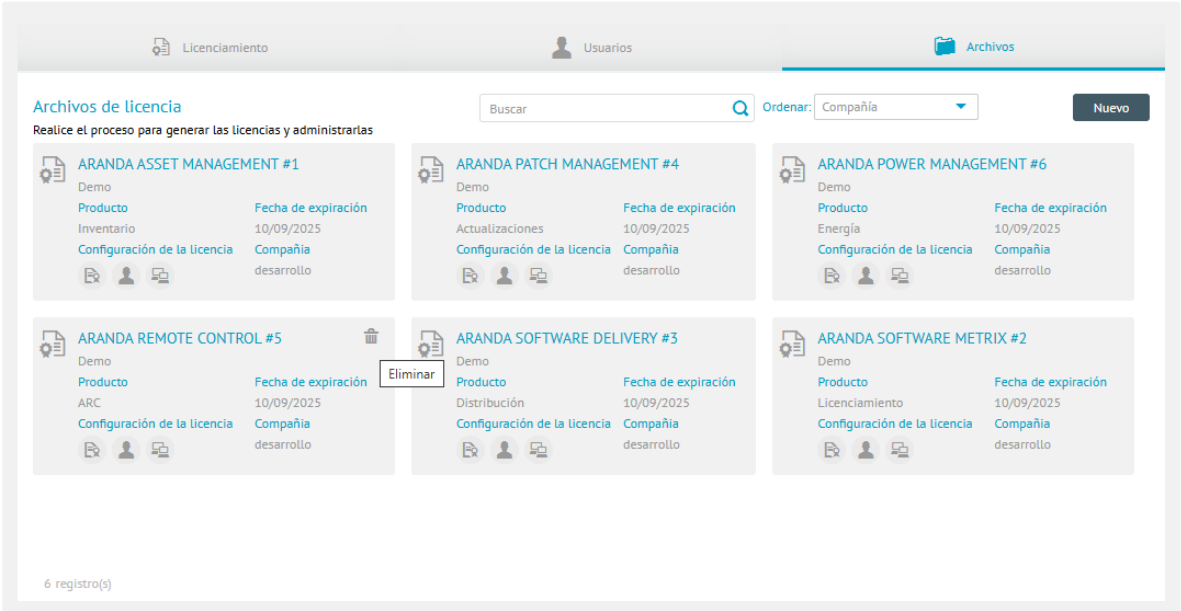


## Delete Licenses

7. To delete a license, in the Licenses information view, select the Records and the registration of a license. Click the Eliminate



. You will be able to display a message confirming the action; when you click Accept the license will be deleted.



## ADM Access

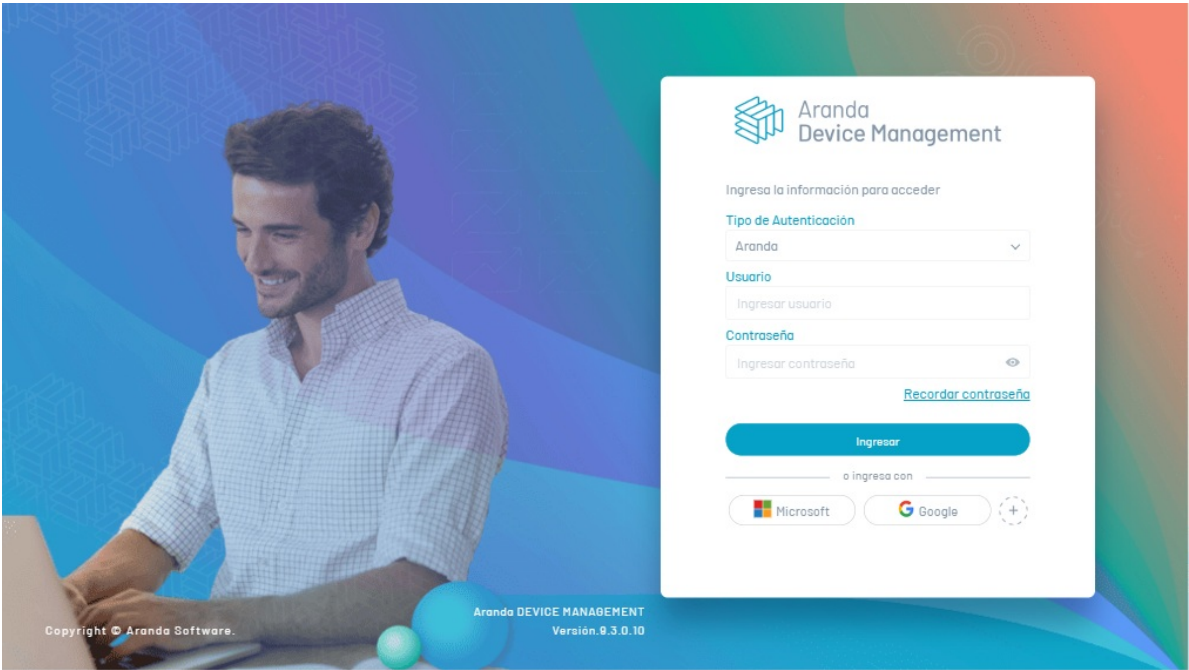
The authentication process to the ADM web console will be executed according to the role defined by the organization to develop the different tasks of device management and configuration. The two instances of

authentication are:

## Login

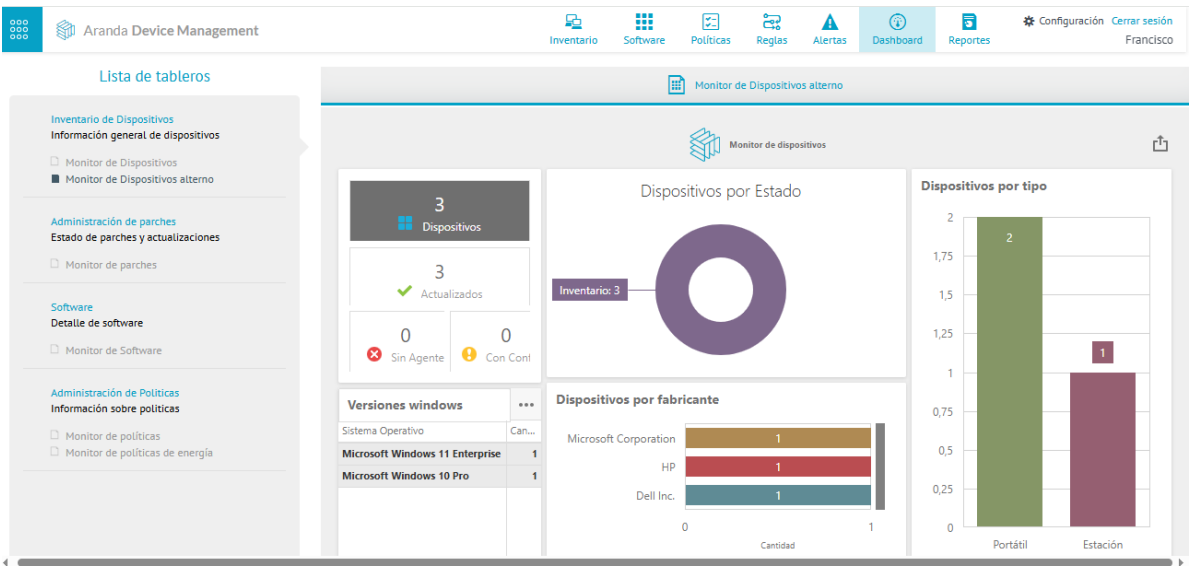
1. Enter the URL from the Aranda Device Management ADM web console.
2. To log in to the ADM application, enter the username and password assigned to you.

📌 **Note:** For more information on the authentication process of Aranda products (authentication and forgot password fields and providers), go to the [Aranda Common Login Module](#).



## Logging Out

1. When a user is in an active session within the web console and requires to end the session and exit the application, in the console header menu select the user icon and click **log off**.



2. Once the session is closed, the user returns to the home screen and the user can enter the console again.

## Update

### ADM Update

In the ADM upgrade processes, after installation, you must take into account the following components to be updated:

- ADM Console Update.
- ADM Agent Update.
- Manual Upgrade of the Server.
- Updating the Conserver by Distribution Project.
- Remote Support Viewer Update.

📌 **Important:** To ensure that your application is working properly after an update to the latest version, update the following components:

- Discovery Agent (starting with version 9.21.1, the Discovery Agent is automatically updated)

- Remote Support Viewer (Aranda ADM Utils) or Remote Support Viewer (Aranda Virtual Support Specialist), depending on the version of remote control you are using.
- End device agents (starting with version 9.21.2, Windows agents are automatically updated)

📌 **Note:** The latest released version of the Remote Support Viewer (Aranda ADM Utils) is 9.22.0. As of ADM version 9.22.1, no new versions of Aranda ADM Utils will be released; however, the correct operation of future versions of ADM in conjunction with the Aranda ADM Utils 9.22.0 version will be guaranteed.

## ADM Console Update

Before upgrading the ADM console, you should consider the following recommendations:

📌 **FOLDERS TO MOVE:** During the upgrade, if they exist, the following folders and their contents must be moved from the repserver repository

- %dir\_Repserver%\AgentUpdate
- %dir\_Repserver%\Recordings

%dir\_Repserver% refers to the path configured for the **Repserver** default C:\Repserver\

To the directory configured for the Content Manager.

The structure must be preserved as is, that is:

- %dir\_ContentManager%\AgentUpdate
- %dir\_ContentManager%\Recordings

%dir\_ContentManager% refers to the path configured for the **Content Manager** default C:\ContentManager\

📌 **IMPORTANT:** Keep the exact names of the folders (AgentUpdate and Recordings) to ensure compatibility with system services. Keep.

📌 **CONSEQUENCES OF OMITTING THE ACTION:** If these folders are not moved:

- Recordings will not be displayed correctly in audits.
- Inconsistencies will occur in system logs.
- Agents will not be able to be downloaded correctly.

To update the ADM console, consider the following instructions: 1. Generate a backup of the database to be updated.

2. Stop the following Aranda services manually or by using Aranda DataBase Tools:

```
- Aranda Conserver V9
- Aranda Cruncher Catalog
- Aranda Cruncher Energy
- Aranda Cruncher File
- Aranda Cruncher Inventory
- Aranda Cruncher Patch
- Aranda Cruncher Usage
- Aranda License Windows Service
- Aranda Scheduler Windows Service
- Aranda Worker Windows Service
```

3. Uninstall the Aranda Conserver Service and Aranda DEVICE MANAGEMENT programs from the control panel.

4. Delete the records in the following folders:

```
- Borrar el contenido que se encuentra en la carpeta "%Program Files (x86)%\Aranda\Aranda Services"
- Excepción de la carpeta 'Downloads', debido a que en esta se guarda el catálogo de parches.
- Carpeta "%Program Files (x86)%\Aranda\Conserver" a excepción de la carpeta 'Data'.
- Carpeta "% inetpub\wwwroot\ADM"
- Carpeta "% inetpub\wwwroot\RepServer"
```

📌 **Note::** Do not delete the contents of the Container, Repserver, and Conserver repositories.

1. Check the requirements before running the installer Aranda.ADM.Web.Installer.exe. [View ADM Console Installation](#)

2. Run the installer Aranda.Conserver.Installer.exe. Do not upload services until the repserver and the.config from the conserver's folder. [View Installation Conserver](#)

3. Run Aranda DataBase Tools so that all files .config to point to the migrated database (see execution steps in the KB

document).

4. Upload Aranda services, either by the Aranda DataBase Tools application or by the list of services:



5. Verify the repserver connection from the web console.

6. If you have the Mosquitto MQTT service, you must uninstall it [View installation](#) in the Uninstall Mosquitto MQTT Broker section, then run the MQTT broker installer. [Aranda MQTT Broker Installation](#)

7. Configure the file Aranda.Conserver.Windows.Service.exe.config what's in the folder %Program Files(x86)%\Aranda\Conserver.

8. Start the service **Aranda Conserver V9**.

9. Verify that all Aranda services are running.

📌 **Note:**

- If you are required to uninstall an Aranda product other than ADM, an error is generated when entering the ADM console and it will not be possible to access it.
- For the installation of the ADM and Conserver console, the server is required to have version 4.8 of the .NET framework (net48)
- Remember to update the agent of the different machines so that they can access the latest changes; For this we recommend:

Update by domain policy.  
Update by agent distribution (Conserver on the client network).  
Manual update.

## Automatic Agent Update

## Agent Pack for Windows

1. The Windows Agent with Extension.exe will be automatically uploaded to the ADM Management Console, in the ADM Configuration from the main menu, option **Packages** within one day of the ADM site update.

A screenshot of a web application window titled 'Paquetes'. The window has a light gray background and a blue header bar. Below the header, there's a section 'Complete la información para la creación de paquetes'. It contains several form fields: 'Tipo del paquete' with radio buttons for 'Software' and 'Agente' (selected); 'Sistema operativo' with radio buttons for 'Windows' (selected), 'Linux', and 'Mac'; 'Arquitectura' with checkboxes for 'x86' and 'x64' (both selected); 'Nombre del paquete' with a text input containing 'Aranda.Agent.Windows.x86\_x64.9.17.2303.280'; and 'Versión' with a text input containing '9.17.2303.2801'. Below these is a 'Descripción' section with a large text area. At the bottom, there's an 'Archivo actual' section showing a file 'Aranda.Agent.Windows.x86\_x64.9.17.2303.2801.exe' with a size of '18.15 MB'. Below this is a box for uploading a new file, with the text 'Escoja un archivo o arrástrelo aquí para reemplazar el actual' and a button 'Formatos soportados: EXE, SH'. At the very bottom are 'Guardar' and 'Cancelar' buttons.

📌 **Note:**

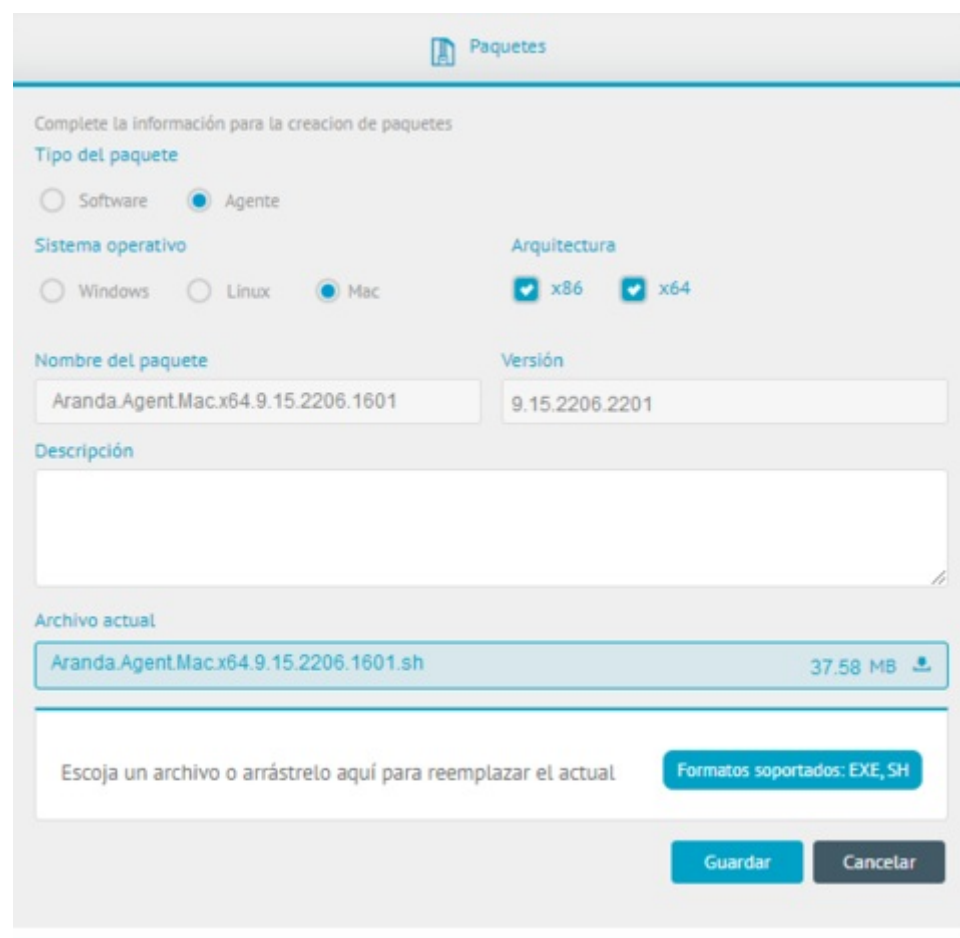
- After 12 hours, after the installation or update of the ADM console, the ADM agent will attempt to update to the latest version released for the console version. If you want to force the update, from the list of devices, you can execute the **Update Agent**

- Starting with ADM Agent version 9.23.0, it is no longer necessary to upload the Agent package from the ADM console for agent update.

## Updating the MacOs Agent

1. To perform the automatic update of the MacOs agent, enter the ADM management console, in the section of **ADM Configuration** from the main menu, select the **Packages** . In the information view, click **More Options** and **Package**.

Upload the installation file with extension **.Sh**.



2. When the agent finishes loading, click **Save**

📌 **Note:**

- After 12 hours, after the installation or update of the ADM console, the ADM agent will attempt to update to the latest version released for the console version. If you want to force the update, from the list of devices, you can execute the **Update Agent**

- Starting with ADM Agent version 9.23.0, it is no longer necessary to upload the Agent package from the ADM console for agent update.

## Linux Agent Package

1. To perform the automatic update of the Linux agent, go to the ADM Management Console, in the **ADM Configuration** from the main menu, select the **Packages** . In the information view, click **More Options** and **Package**.

Upload the installation file with extension **.Sh**.

Paquetes

Complete la información para la creación de paquetes

Tipo del paquete

Software

Agente

Sistema operativo

Windows

Linux

Mac

Arquitectura

x86

x64

Nombre del paquete

Aranda.Agent.Linux.x64.9.14.2205.0386

Versión

9.14.2205.0386

Descripción

Archivo actual

Aranda.Agent.Linux.x64.9.14.2205.0386.sh18.70 MB

Escoja un archivo o arrástrelo aquí para reemplazar el actual

Formatos soportados: EXE, SH

Guardar

Cancelar

- 📌

Note:
- After 12 hours, after the installation or update of the ADM console, the ADM agent will attempt to update to the latest version released for the console version. If you want to force the update, from the list of devices, you can execute the **Update Agent**

- Starting with ADM Agent version 9.23.0, it is no longer necessary to upload the Agent package from the ADM console for agent update.

## Manual Upgrade of the Shelf

1. Stop the Aranda Conserver V9 service.
2. Uninstall the Conserver Service program from the control panel.
3. Delete the record from the following folder:
  - Folder “%Program Files (x86)%\Aranda\Conserver” except for the ‘Data’.
- 📌

Note:

Do not delete the contents of the Conserver repository.
4. Run the installer Aranda.Conserver.Installer.exe. Do not upload the service until configuring the .config of the conserver folder. [See Installation Conserver.](#)
5. Start the Aranda Conserver V9 service.
6. To verify the successful connection of the conserver, log in to the ADM Management Console, in the **ADM Configuration** from the main menu, select the **Communications** . In the Information View, in the Communications Tree, click on the Repserver node and select Keep. In the detail view on the **Configuration** Click the **Test Connection**

Aranda Device Management

Comunicaciones

Inicio 

Cerrar sesión

francisco

Generales

ADM

Credenciales

Comunicaciones

Perfiles Agente

Catálogo de Aplicaciones

Gestor de contenido

Paquetes

Portal de autogestión

RepServer

BG-D-SACRISTAN1.INTERSEQ.LOCAL

Configuración

Descubrimiento

Configuración nodo de comunicaciones

Edite la información para conectar el nodo de comunicaciones

Dirección nodo de comunicaciones

http://192.168.1.111/Conserver

Probar conexión

Activar

Si

Puerto Wake on LAN

7

Ruta en donde se guardan los archivos

C:\Conserver

Por defecto

Siempre

Tiempo

Rango de tiempo

- 📌

Note:
- Installation of the Conserver requires that the server has version 4.8 of the .NET framework or later.

📖 **Related Links:** Updating the conserver can also be done through a distribution project. [Updating the Conserver by Distribution Project](#)

## Maintaining the Conserver via Distribution Project

[Upgrade from version 9.16 to 9.17 »](#)

[Upgrade from versions later than 9.17 »](#)

### Preconditions

- The conserver server must have an agent installed, pointing to the repserver and with the distribution module enabled in the agent profile.
- The agent installed on the conserver must have an agent profile with no list of communication nodes.

### Upgrade from version 9.16 to 9.17

📌 **Note:** Installation of the Conserver requires that the server has version 4.8 of the .NET framework or later

1. Create a file with .bat extension (*e.g., UpdateConserver.bat*) 2. Copy and edit the following script in the created file and save it.

📌 **Note:**

- Enter in the variable path the route where the conserver is installed.
- Enter in the variable conserver the full name of the conserver installer
- If you have more than one conserver and they are installed on a different path, you must create a different .bat and project for each of the conservers

```
:: Ingresar en la variable path la ruta donde se encuentra instalado el conserver
SET path = C:\Program Files (x86)\Aranda\Conserver
:: Ingresar el nombre del instalador .exe del conserver
SET conserver = Aranda.Conserver.Installer.9.17.0.0.exe
SET config = Aranda.Conserver.Windows.Service.exe.config
```

```
MsiExec.exe /X{96E7810B-02CE-40D1-A17D-4FDAC64B5B0C} /qn
@timeout /t 6 /nobreak
cd %TEMP%
cmd.exe /c %conserver% /S /v /qn
@timeout /t 20 /nobreak
```

```
del %path%\%config%
copy %TEMP%\%config% %path%
```

```
sc start ArandaConserverWindowsServiceV9
```

```
del %TEMP%\%conserver%
del %TEMP%\%config%
```

1. Create a file with an extension .config and name it Aranda.Conserver.Windows.Service.exe.config

2. Copy, configure key fields <appSettings> and save.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="dataConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.Data.Configuration.DatabaseSettings,
Microsoft.Practices.EnterpriseLibrary.Data, Version=6.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
requirePermission="true" />
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->
  >
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection,
EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />
  </configSections>
  <connectionStrings>
```

```
<add name="local" connectionString="Data Source=Data\local.dat;busytimeout=60"
providerName="System.Data.SQLite.EF6" />
</connectionStrings>
<appSettings>
  <add key="dataConfiguration:defaultDatabase" value="local" />
  <add key="Serilog:MinimumLevel" value="Debug" />
  <add key="Serilog:WriteTo:0:Name" value="File" />
  <add key="Serilog:WriteTo:0:Args:path" value="Logs\log.txt" />
  <add key="Serilog:WriteTo:0:Args:shared" value="true" />
  <add key="Serilog:WriteTo:0:Args:rollingInterval" value="Day" />
  <add key="Logging:LogLevel:Default" value="Information" />
  <add key="serverAddress" value="" />
  <add key="enableProxy" value="false" />
  <add key="proxyAddress" value="" />
  <add key="proxyUser" value="" />
  <add key="proxyPassword" value="" />
  <add key="privateIp" value="" />
  <add key="publicIp" value="" />
  <add key="mqttServerPort" value="1884" />
  <add key="mqttIp" value="" />
  <add key="publicServerPort" value="80" />
  <add key="privateServerPort" value="80" />
  <add key="p2pPort" value="9501" />
  <add key="maxDistributionSleepMsPerThread" value="8" />
  <add key="maxDistributionThreads" value="4" />
  <add key="enableDiscoveryCommon" value="1" />
  <add key="SecondsPingRemoteServer" value="60" />
  <add key="enableSecurity" value="false" />
</appSettings>
<startup>
  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.8" />
</startup>
<entityFramework>
  <providers>
    <provider invariantName="System.Data.SQLite" type="System.Data.SQLite.EF6.SQLiteProviderServices,
System.Data.SQLite.EF6" />
    <provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices,
EntityFramework.SqlServer" />
    <provider invariantName="System.Data.SQLite.EF6" type="System.Data.SQLite.EF6.SQLiteProviderServices,
System.Data.SQLite.EF6" />
  </providers>
  <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
    <parameters>
      <parameter value="mssqllocaldb" />
    </parameters>
  </defaultConnectionFactory>
</entityFramework>
<runtime>
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
      <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-13.0.0.0" newVersion="13.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="DotNetZip" publicKeyToken="6583c7c814667745" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-1.14.0.0" newVersion="1.14.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <publisherPolicy apply="no" />
      <assemblyIdentity name="Oracle.ManagedDataAccess" publicKeyToken="89b483f429c47342" culture="neutral" />
      <bindingRedirect oldVersion="4.121.0.0 - 4.65535.65535.65535" newVersion="4.122.19.1" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a"
culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.Extensions.Configuration.Abstractions"
publicKeyToken="adb9793829ddae60" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.Extensions.Configuration" publicKeyToken="adb9793829ddae60"
culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.Extensions.Configuration.EnvironmentVariables"
publicKeyToken="adb9793829ddae60" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.IdentityModel.Logging" publicKeyToken="31bf3856ad364e35" culture="neutral"
/>
      <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.IdentityModel.Tokens" publicKeyToken="31bf3856ad364e35" culture="neutral"
/>
      <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.IdentityModel.Tokens.Jwt" publicKeyToken="31bf3856ad364e35"
```

```

culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Diagnostics.DiagnosticSource" publicKeyToken="cc7b13ffcd2ddd51"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.ValueTuple" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.0.3.0" newVersion="4.0.3.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Threading.Tasks.Extensions" publicKeyToken="cc7b13ffcd2ddd51"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.2.0.1" newVersion="4.2.0.1" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Bcl.AsyncInterfaces" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Buffers" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.0.3.0" newVersion="4.0.3.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="RestSharp" publicKeyToken="598062e77f915f75" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-106.13.0.0" newVersion="106.13.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.Configuration.Binder" publicKeyToken="adb9793829ddae60"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.Logging.Abstractions" publicKeyToken="adb9793829ddae60"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Owin" publicKeyToken="31bf3856ad364e35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.2.2.0" newVersion="4.2.2.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Text.Encodings.Web" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.0.5.1" newVersion="4.0.5.1" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Text.Json" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.6" newVersion="6.0.0.6" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="System.Web.Http" publicKeyToken="31bf3856ad364e35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.2.9.0" newVersion="5.2.9.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Owin.Security" publicKeyToken="31bf3856ad364e35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.2.2.0" newVersion="4.2.2.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Owin.Security.OpenIdConnect" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.2.1.0" newVersion="4.2.1.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Owin.Security.Cookies" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-4.2.1.0" newVersion="4.2.1.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.Logging" publicKeyToken="adb9793829ddae60" culture="neutral"
/>
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.DependencyInjection.Abstractions"
publicKeyToken="adb9793829ddae60" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.Options" publicKeyToken="adb9793829ddae60" culture="neutral"
/>
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.Extensions.Primitives" publicKeyToken="adb9793829ddae60"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
</dependentAssembly>
<dependentAssembly>
    <assemblyIdentity name="Microsoft.IdentityModel.JsonWebTokens" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
</dependentAssembly>
```

```

    <dependentAssembly>
      <assemblyIdentity name="Microsoft.IdentityModel.Protocols" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.IdentityModel.Protocols.OpenIdConnect"
publicKeyToken="31bf3856ad364e35" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Net.Http.Formatting" publicKeyToken="31bf3856ad364e35" culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-5.2.9.0" newVersion="5.2.9.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="Microsoft.IdentityModel.Abstractions" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
      <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
    </dependentAssembly>
  </assemblyBinding>
</runtime>
<system.data>
  <DbProviderFactories>
    <remove invariant="System.Data.SQLite.EF6" />
    <add name="SQLite Data Provider (Entity Framework 6)" invariant="System.Data.SQLite.EF6" description=".NET
Framework Data Provider for SQLite (Entity Framework 6)" type="System.Data.SQLite.EF6.SQLiteProviderFactory,
System.Data.SQLite.EF6" />
    <remove invariant="System.Data.SQLite" />
    <add name="SQLite Data Provider" invariant="System.Data.SQLite" description=".NET Framework Data Provider for
SQLite" type="System.Data.SQLite.SQLiteFactory, System.Data.SQLite" />
  </DbProviderFactories>
</system.data>
<system.serviceModel>
  <behaviors>
    <serviceBehaviors>
      <behavior name="">
        <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true" />
        <serviceDebug includeExceptionDetailInFaults="false" />
      </behavior>
    </serviceBehaviors>
  </behaviors>
  <services>
    <service name="Aranda.Conserver.Ws.Service1">
      <endpoint address="" binding="basicHttpBinding" contract="Aranda.Conserver.Ws.IService1">
        <identity>
          <dns value="localhost" />
        </identity>
      </endpoint>
      <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
      <host>
        <baseAddresses>
          <add baseAddress="http://localhost:8733/Design_Time_Addresses/Aranda.Conserver.Ws/Service1/" />
        </baseAddresses>
      </host>
    </service>
  </services>
</system.serviceModel>
</configuration>

```

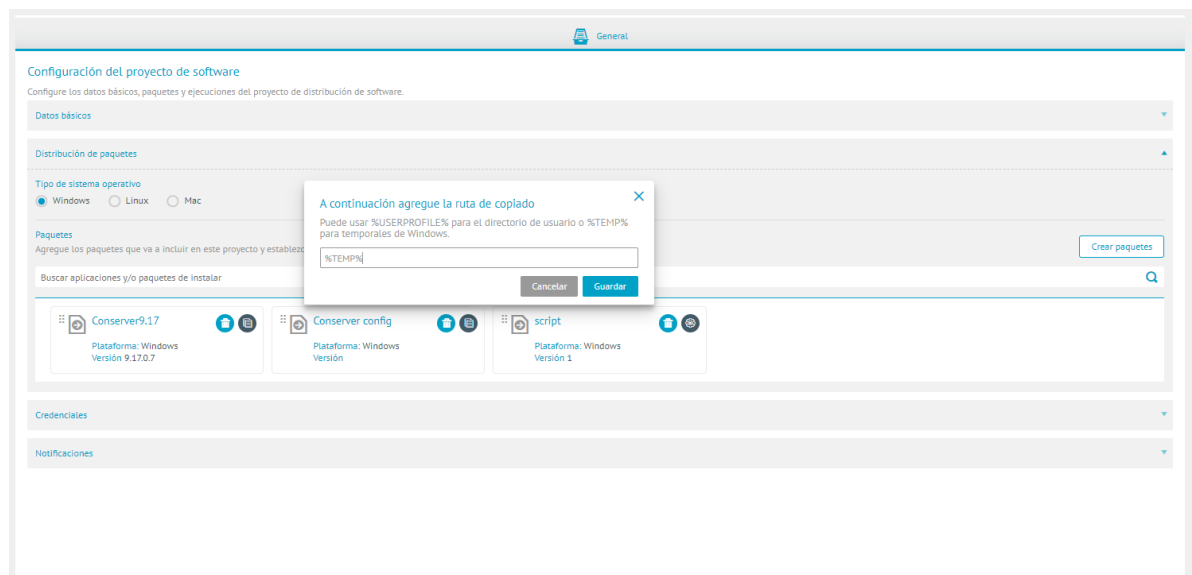
3. [Create a Distribution Package](#) guy copy with the installer of the conserver. 4. [Create a Distribution Package](#) guy copy with the Aranda.Conserver.Windows.Service.exe.config created in steps 3 and 4.

5. [Create a new Distribution Pack](#) guy execution with the file .bat created in steps 1 and 2.

6. Log in to ADM Distribution management and create a [Software Distribution Project](#).

7. In the project, add the packages created in steps 5, 6, and 7 in the following order:

- Conserver Installer Package (*Copy type package*) adding %TEMP% as a path.
- Package Aranda.Conserver.Windows.Service.exe.config (*Copy type package*) adding %TEMP% as a path.
- Package UpdateConserver.bat (*Run-type package*)



8. Run the distribution on the computer to perform the Conserver update.

📌 **Note:** If you have more than one conserver and they are installed on a different path, you must create a .bat one .config and a different project for each of the conservers. If the conservers maintain the installation path and have the same configuration, they can be submitted in the same distribution project

9. In the ADM configuration, define the [Reserver/Conserver Communication Components](#) and check the connection.

## Upgrading from versions after 9.17

To update the conserver using a distribution project, you need to follow the following steps:

1. Create a file with .bat extension (*e.g., UpdateConserver.bat*)
2. Copy and edit the following script in the created file and save it.

📌 **Note:**

- Enter in the variable path the route where the conserver is installed.\*\*
- Enter in the variable conserver the full name of the conserver installer
- If you have more than one conserver and they are installed on a different path, you must create a different .bat and project for each of the conservers

```
~~~batch :: Ingresar en la variable path la ruta donde se encuentra instalado el conserver SET path = C:"Program Files (x86)"\Aranda\Conserver :: Ingresar el nombre del instalador .exe del conserverSET conserver = Aranda.Conserver.Installer.9.16.3.6.exe
```

```
copy %path%\Aranda.Conserver.Windows.Service.exe.config %TEMP% @timeout /t 3 /nobreak
```

```
MsiExec.exe /X{96E7810B-02CE-40D1-A17D-4FDAC64B5B0C} /qn @timeout /t 6 /nobreak cd %TEMP% cmd.exe /c %conserver% /S /v/qn @timeout /t 20 /nobreak
```

```
del %path%\Aranda.Conserver.Windows.Service.exe.config @timeout /t 3 /nobreak copy %TEMP%\Aranda.Conserver.Windows.Service.exe.config %path% @timeout /t 3 /nobreak
```

```
sc start ArandaConserverWindowsServiceV9
```

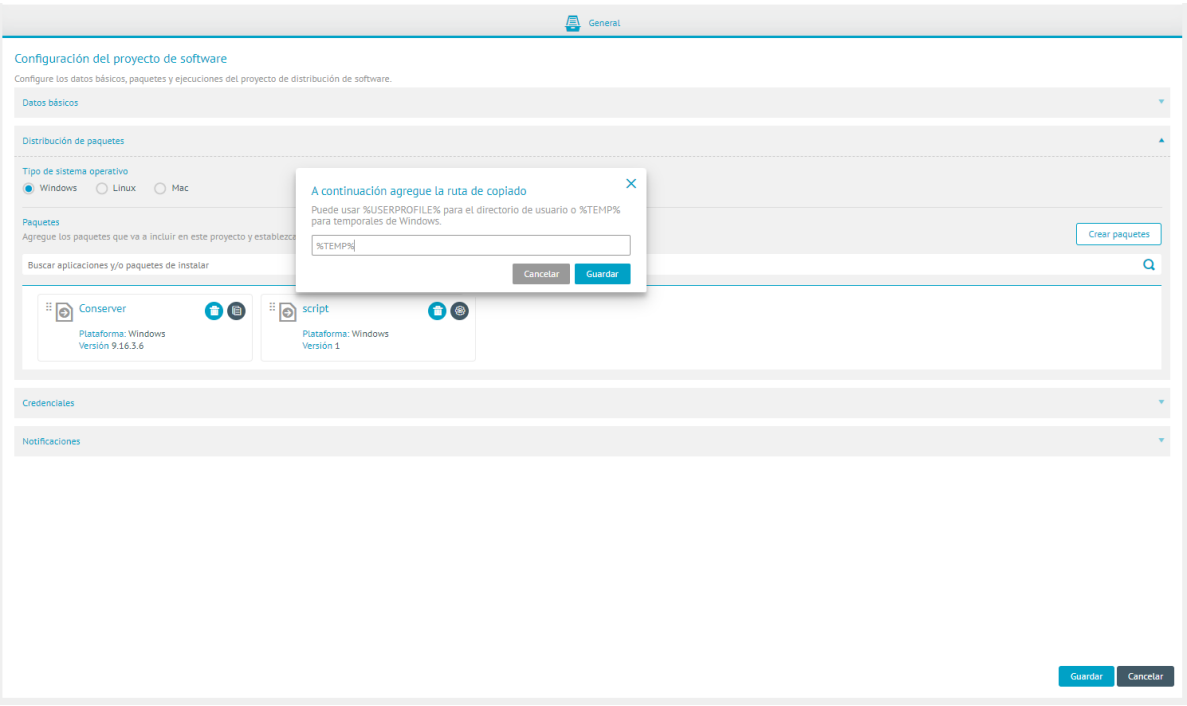
```
del %TEMP%\Aranda.Conserver.Windows.Service.exe.config del %TEMP%\%conserver%
```

3. [Create a Distribution Package](#) guy copy with the installer of the conserver.

4. [Create a new Distribution Pack](#) guy execution with the file .bat created in steps 1 and 2.

5. Log in to ADM Distribution Management and create a [Software Distribution Project](#).

6. In the project add the packages created in step 3 and 4 by first adding the conserver installer package(*Copy type package*)adding %TEMP% as a path.



7. Run the distribution on the computer to perform the Conserver update.

📌 **Note:**

- If you have more than one conserver and they are installed on a different path, you must create a different .bat and project for each of the conservers. If the conservers maintain the installation path, they can be submitted in the same distribution project.

If the distribution has been successful, the conserver is updated.

8. In the ADM configuration, define the [Reserver/Conserver Communication Components](#) and check the connection.

## Remote Support Viewer Update

To update the Remote Support Viewer follow the steps below:

1. Log in to Control Panel > Programmes > Programs and FeaturesSelect Aranda ADM Utils and click Uninstall

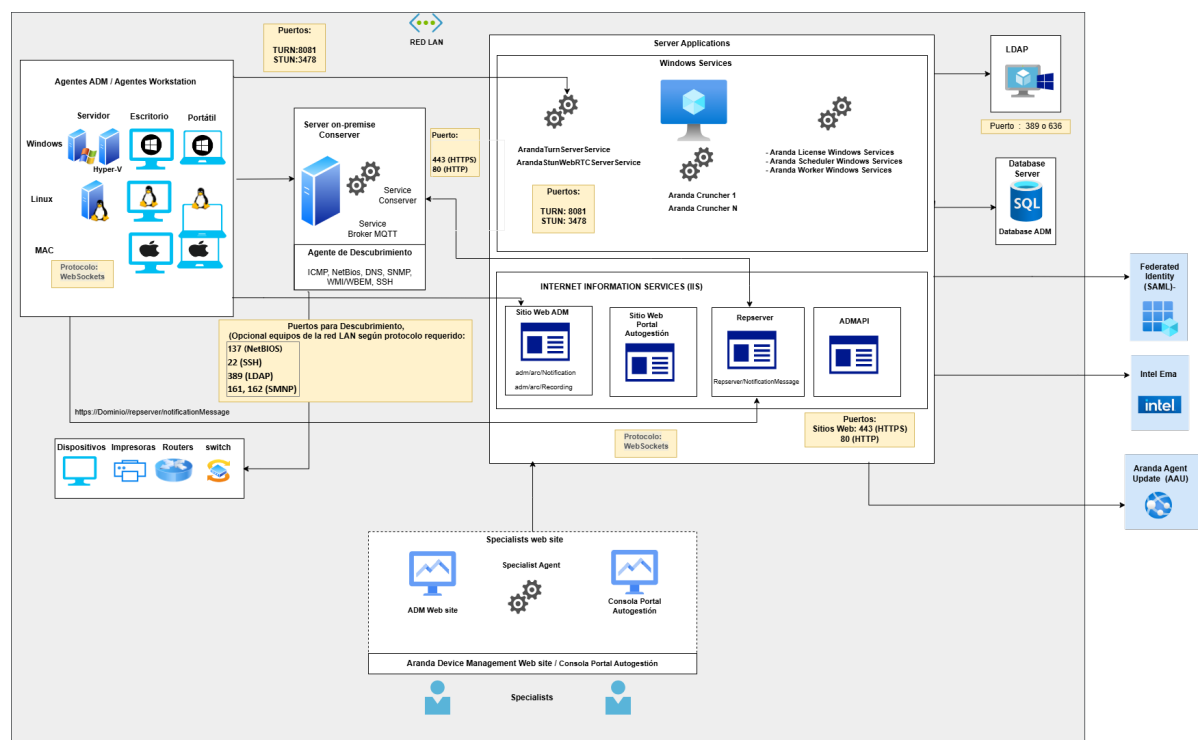


2. Once the previous version is uninstalled, you can start the installation of the new version[View Remote Support Viewer Installation](#)

## ADM Structures

### Onpremise Structure

The structure and operation of Aranda Device Management ADM is an application distributed in the following components:



## Database (server in the client's infrastructure)

Repository where all system information is stored. The database stores hardware, software, and file inventory information for all workstations.

## Application Server

This server contains the business logic, as well as the Mailer, DB Manager, Conserver, and Cruncher modules. Additionally, it communicates with the Web Console to display the information contained in the Database there.

## Preserve

The Conserver acts as a link between the application server components and the client's LAN. This is a Windows service that must be located on the LAN network in order to send and receive messages from the agents installed on each machine facilitates the processes of discovery, distribution, and remote management. Depending on the topology, a Conserver must be installed for each network segment.

## Cruncher

Service installed on the server where the console is installed, is responsible for processing the inventories and saving them in the database. To do this, it decrypts, decompresses, and stores the data collected by each station. There are 2 crunchers:

## ADM Agent

The Aranda Device Management agent is the component installed on the customer's devices it is responsible for generating, compressing, encrypting and sending via TCP/IP the hardware and software inventory in each of the workstations; it also allows the generation of inventories and the secure management of commands from the server.

This component is installed on the client side. It can be installed locally and/or remotely on each workstation.

## Repserver

This component is installed on the application server and is responsible for receiving requests from the client's LAN network or from computers that are directly connected through the Internet.

## Web Server Repserver

This component is installed on the application server and contains the Internet Information Services IIS and .Net Framework, on which the application for the Administration Web Console is installed.

## Web Console

Through this interface that the customer, user or administrator visualizes, they will be able to manage and view hardware and software inventories by workstation, track and control their IT resources, perform remote control tasks.

## Self-Management Portal

This interface that the client visualizes, allows the users responsible for the devices to visualize the available software distribution projects and perform the installation in an unattended manner.

## Broker MQTT

This service, located on the customer's LAN network, allows you to manage and control the messaging actions sent to the web console in real time.

It facilitates communication with the different devices that are being managed, it allows requests to the devices to arrive in real time, for the communications of the devices within the business LAN network, the service can be installed on the server of the conserver or another server that is on the LAN network, it is necessary to open port 1884 or 1883.

## Turn Server

When two devices are unable to establish a direct connection to each other, a Turn server is needed to facilitate communication.

It is a Windows service installed in a virtual machine, which acts as a bridge for remote control between the specialist agent and the workstation agent. To activate this functionality, both agents establish a connection with the Turn Server, which is listening on port 8081 or the parameterized for operation on Onpremises, transmitting the data from one agent to the other. (Cloud, defined listening port 3478)

## Specialist Agent

It is designed to allow remote control access, file transfers, and recordings for audits. Each specialist must install this application on the machine where he works.

## Workstation Agent

Component installed on Windows devices in architectures, they are responsible for receiving remote support. It can be located both inside and outside the customer's infrastructure.

## Harbours

Communication ports used by Aranda Device Management (ADM) to enable required communications.