
Aranda Device Management

ADM is a solution that manages the organization's hardware and software computer 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. Requirements

Learn the basic requirements for proper application operation.

2. ADM Installation

Learn the required installation path of the different components and applications that make up ADM device management.

3. Upgrade

Identify how to perform updates to the components of the functionality.

¿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 Installation and Configuration Guide (You are HERE)
- Aranda Device Management ADM ↪ Management Manual
- Aranda ADM ↪ Integration Manual

Hardware and Software Requirements

Hardware and Software Requirements

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

Azure Web Server ADM Console and Conserver

Operating system	Windows Server 2019 Datacenter
Cores	Intel® Xeon® CPU E5-2673 v4 @ 2.30GHz 2.29GHz
RAM	Minimum 4 GB
Disk	Minimum 64 GB

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_CPI1_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

Mac

Mac operating system	Version
MacOS	Sonoma
MacOS	Fortune
MacOS	Monterey

⚐ Note: The following processors are supported: Intel and Apple Silicon M1, M2 and M3

Linux

Linux Operating System	Version
Ubuntu	18.04
Ubuntu	20.04
Ubuntu	22.04
Red Hat	Enterprise Linux 8.0
Red Hat	Enterprise Linux 8.6
Red Hat	Enterprise Linux 9

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

Exceptions

Exceptions

↩ Hardware and Software Requirements

|[AAM_FILE_NAME]| [name] |SQL_Latin1_General_CP1_CS_AS| |[AAM_FILE_PRODUCT]| [name]| SQL_Latin1_General_CP1_CI_AS| |[AAM_LOCAL_USER]| [domain]| SQL_Latin1_General_CP1_CI_AS| |[AAM_LOCAL_USER]| [username]| SQL_Latin1_General_CP1_CI_AS| |[AAM_MANUFACTURER]| [name]| SQL_Latin1_General_CP1_CI_AS| |[AAM_NETWORKADAPTER]| [name]| SQL_Latin1_General_CP1_CI_AS| |[AAM_PATH]| [path]| SQL_Latin1_General_CP1_CI_AS| |[AAM_SOFTWARE_PRODUCT]| [name]| SQL_Latin1_General_CP1_CI_AS| |[AAM_SOFTWARE_UNINSTALL]| [uninstall_string]| SQL_Latin1_General_CP1_CI_AS| |[ASM_FILE_RULE]| [name]| SQL_Latin1_General_CP1_CI_AS| |[ASM_FILE_RULE]| [file_product_name]| SQL_Latin1_General_CP1_CI_AS| |[ASM_SOFTWARE_RULE]| [name]| SQL_Latin1_General_CP1_CI_AS| |[ASM_SOFTWARE_RULE]| [manufacturer_name]| SQL_Latin1_General_CP1_CI_AS| |[AAM_DRIVER]| [name]| SQL_Latin1_General_CP1_CI_AS|

Required Ports and Permissions on ADM Components

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.

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. Configuring the Stun/Turn WebRTC Server

⚐ 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 Remote Administration

⚐ 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 network local) 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)	SMNP	Required for egress only, intended for device discovery by SMNP 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 (Onpremises Architecture) 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 Remote Management, used when the architecture does not allow the repserver notification server to be displayed for communication. : https://Dominio/repserver/Notificationmessage.
	WebSockets (optional)	They establish a persistent bidirectional connection between the ADM agent and the repserver notification server, required for the Remote Management, used when the architecture allows the repserver notification server to be displayed for communication. : https://Dominio/repserver/Notificationmessage.
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)	SMNP	Input port, intended for device discovery by SMNP 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 (Cloud Architecture)

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
	WebSockets	They establish a persistent bidirectional connection between the ADM agent and the server, required for remote management functionality.

⚐ Notes:

- For remote administration functionality, the device where the agent is installed must be able to display the repserver's notification server site: https://Dominio/repserver/Notificationmessage.

- View functionality Remote Management

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)	SMNP	Input port, intended for device discovery by SMNP protocol

⚐ Notes:
- 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.
- 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 Worksation", 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 ↪.

ADM Reference Architecture Diagrams

To visualize the Ports and iteration with the components you can check the following links.

- Cloud with Conserver Onpremises ↪
- Cloud without a server↪
- Onpremises↪

Required Exclusions in Antivirus

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

Licensing Service

ADM uses Aranda's common licensing service to authorize users to enter to the console and control the purchased licenses, among other operations.

This is a Windows service that is usually created automatically by the product installer.

Once the user uploads their purchased licenses from the console, the common Licensing must remain on the same machine, otherwise the licenses loaded they will be lost.

If your application server is located in a virtual machine, it will be recommends 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 incorrectly assumes that he was transferred.

Check with the vendor for details on server deployment.

Requirements for Remote Administration Functionality

Configure remote management based on the installed ADM architecture.

- Remote administration configuration Cloud architecture
- Configuration of remote administration of Onpremises architecture

Requirements Remote Administration - Cloud Architecture

Enable Functionality by Database

1. To enable the Remote Management Configuration Cloud architecture or architectures with devices that are outside the LAN network, run the following script:

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

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

Required Ports and Permits 2. Validate the Required Ports and Permissions ADM Agents (Cloud Architecture).

⚐ Note: In the detail view of the devices inventoried by ADM, you can view the device information with Remote Administration

Remote Administration Requirements - Onpresmises 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'
```

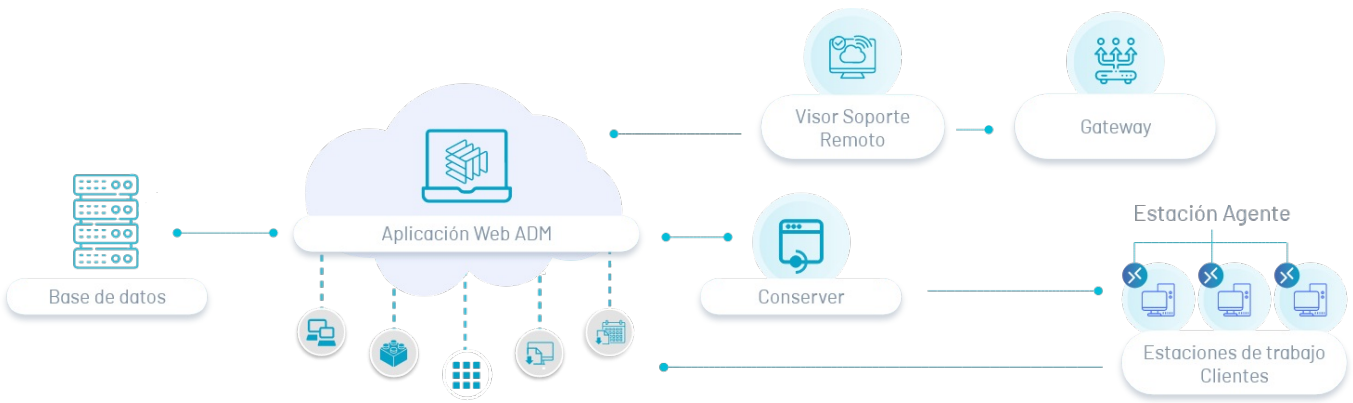
⚐ Note: In the detail view of the devices inventoried by ADM, you can view the device information with Remote Administration

ADM Installation

ADM Installation Path

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 ADM installation process should consider the following stages:



1. Web Console Installation

Through a web environment, the user, according to the established role, will be able to manage the different processes of definition, follow-up and monitoring of compliance policies on security issues in the different workstations.

2. Install Conserver (Not Required)

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.

3. Agent Installation

The Aranda Device Management agent is the component installed on the client's devices, which allows the generation of inventories and the secure management of commands coming from the server.

4. Remote Support Viewer Installation

Installing the Remote Support Viewer allows you to take remote control of the managed machines and must be installed on the LAN network in order to access them. This viewer must also have access to the application server in order to authorize and coordinate the session.

Gateway Installation

Installing this component allows remote control connections to be established outside the LAN network.

Broker Installation

Installing this service allows you to manage and control the messaging actions sent to the web console in real time.

⚐ 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

ADM Web Console Installer

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.

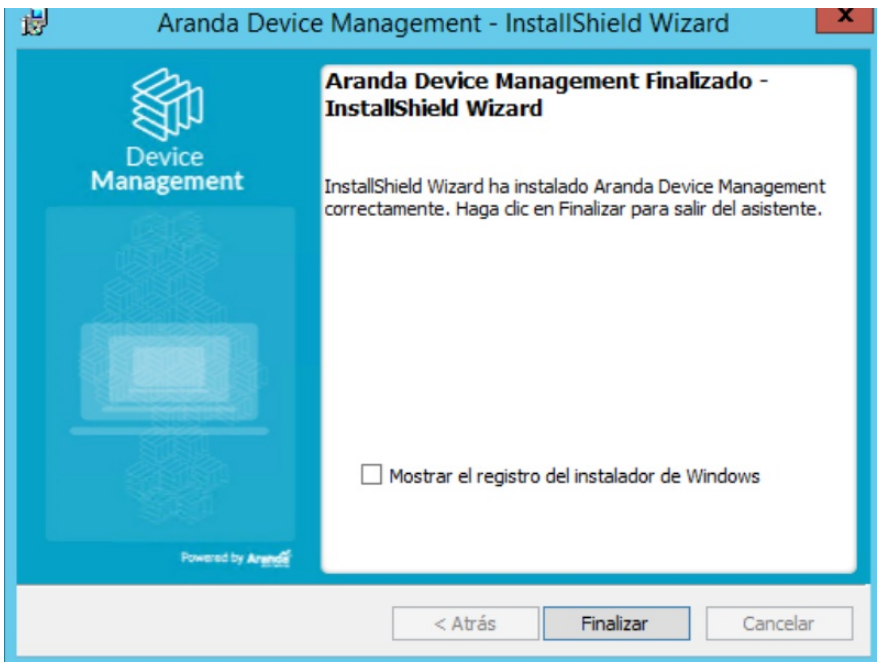
1. Clicking on the installer will launch the installation wizard. Click Following.

2. Enter the customer information and click Following.

3. Select the full installation type and click Following.

4. Click Install.

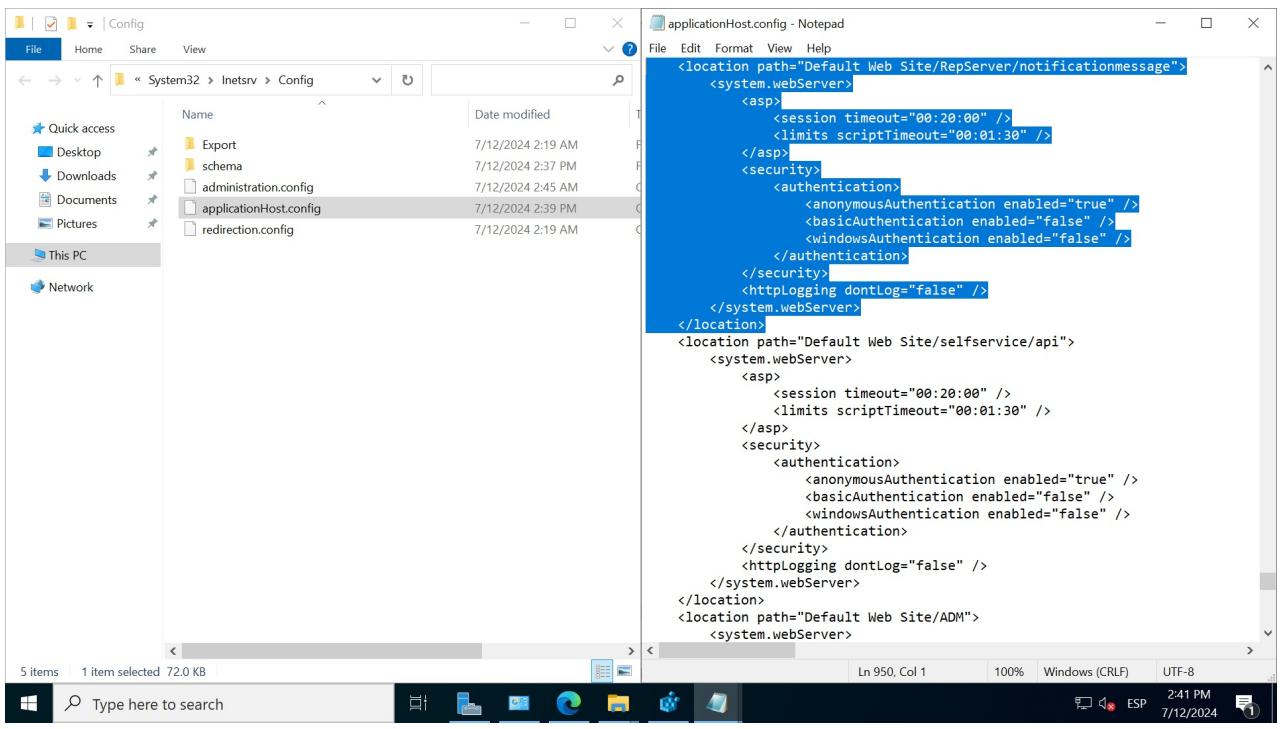
5. Once the installation process is complete, click End.



⚐ 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



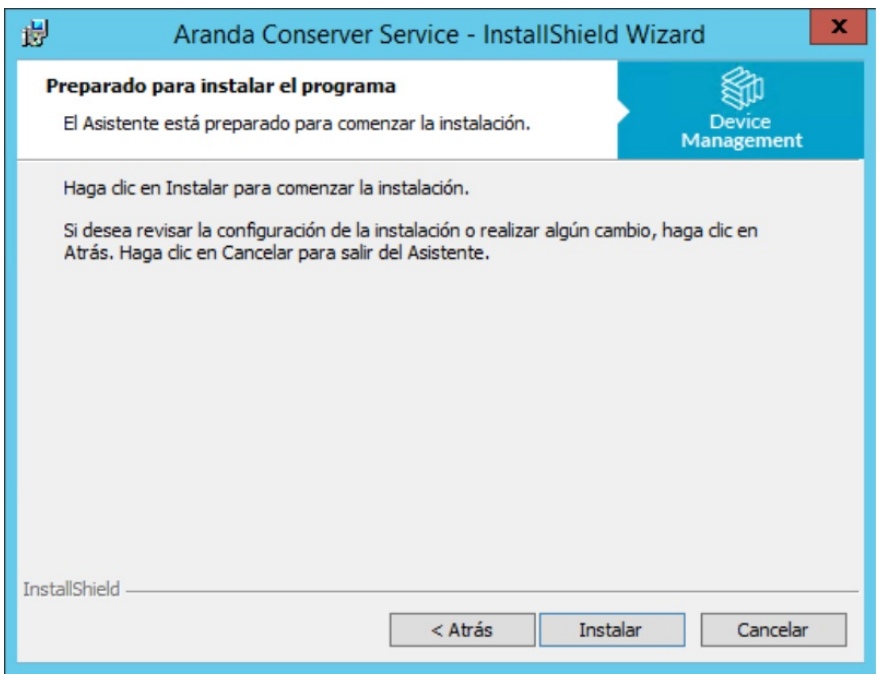
Installer Conserver

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

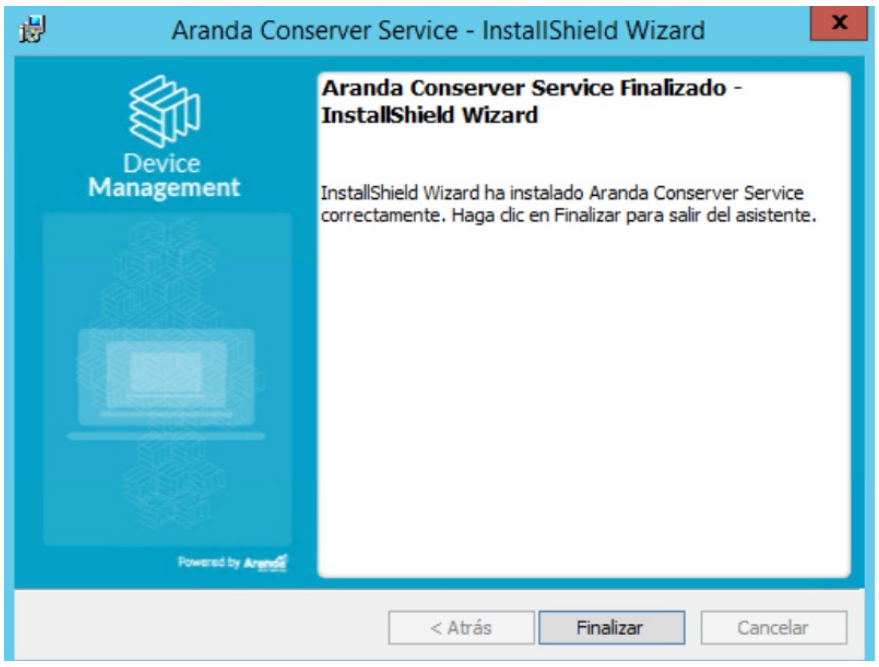
1. Clicking on the installer will launch the installation wizard.

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

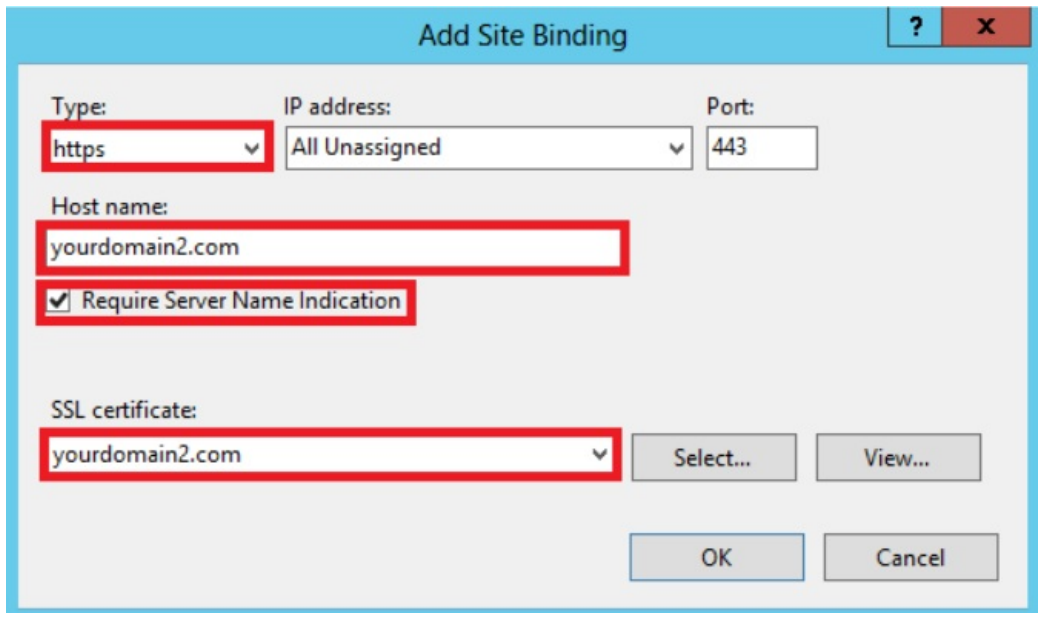
—

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”

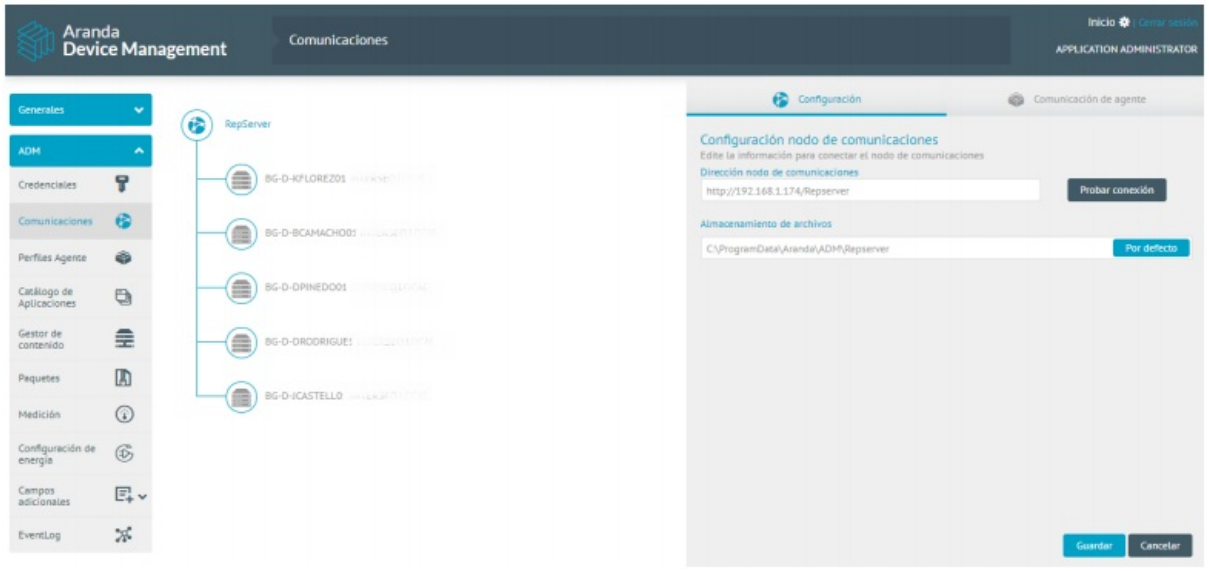
```
<appSettings>
    <add key="serverAddress" value="https://IP_SERVER/repserver"/>
    <add key="enableProxy" value="false"/>
    <add key="proxyAddress" value=""/>
    <add key="proxyUser" value=""/>
    <add key="proxyPassword" value=""/>
    <add key="logLevel" value="Information"/>
    <add key="privateIp" 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

Conserver Configuration in the ADM Web Console

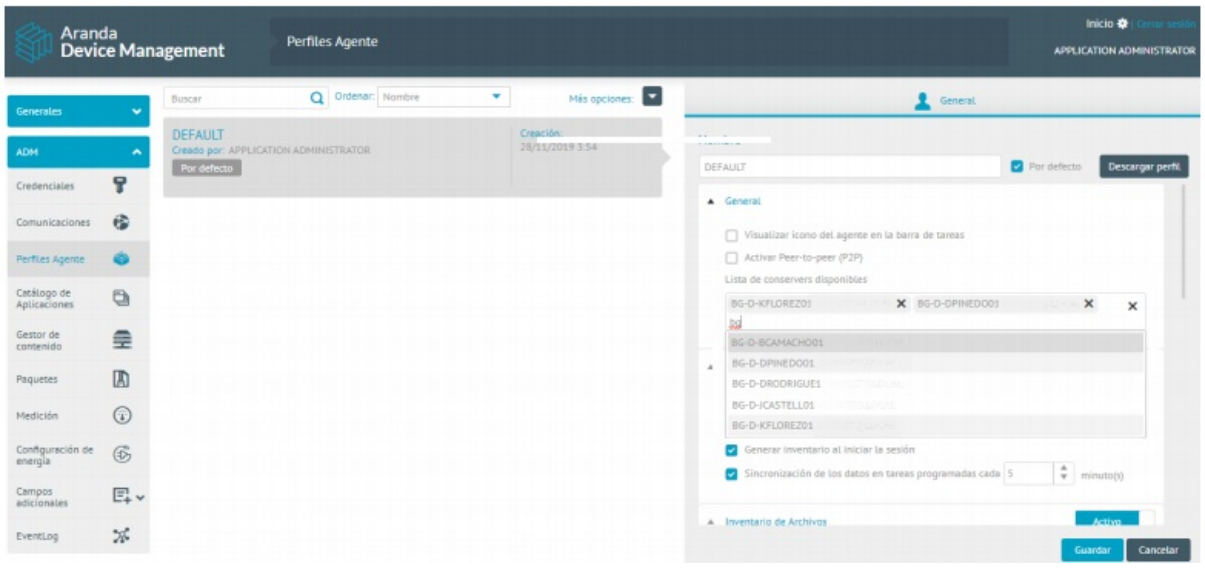
↩ Installer Conserver

1. To configure the conserver go 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, to display and identify all the Conservers that are communicating.



⚐ Note: Each Conserver must be included within the Agent's profile.

2. To add the conserver to the agent's profile, in the ADM Configuration from the main menu, select the Agent Profiles. In the information view, select a record of the agent profiles that you want to modify. In the detail view, display the General Module and in the countryside List of available conservers, search for and select the name of the Cannery to include. When finished, click Save

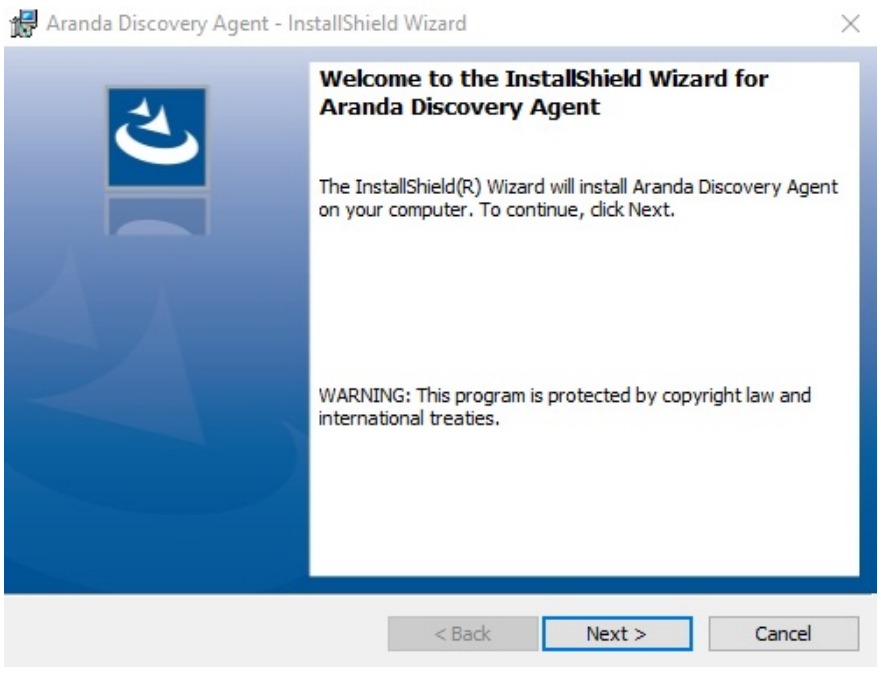


⚐ Note: In case of losing the connection with a Conserver, the Agent will try to re-establish communication with the conservers stored in the list of Conservers.

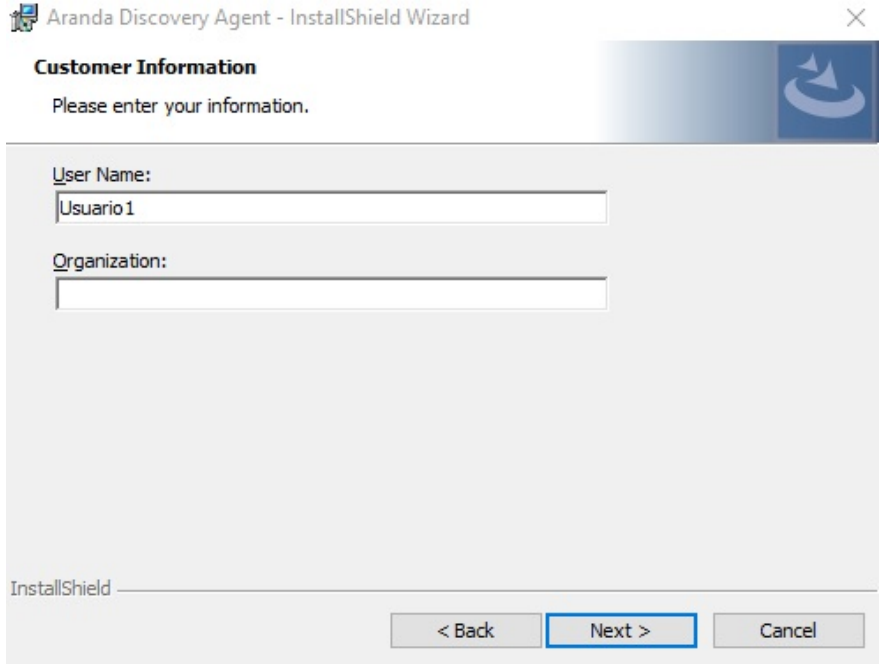
↩ Installer Conserver

Discovery agent installation

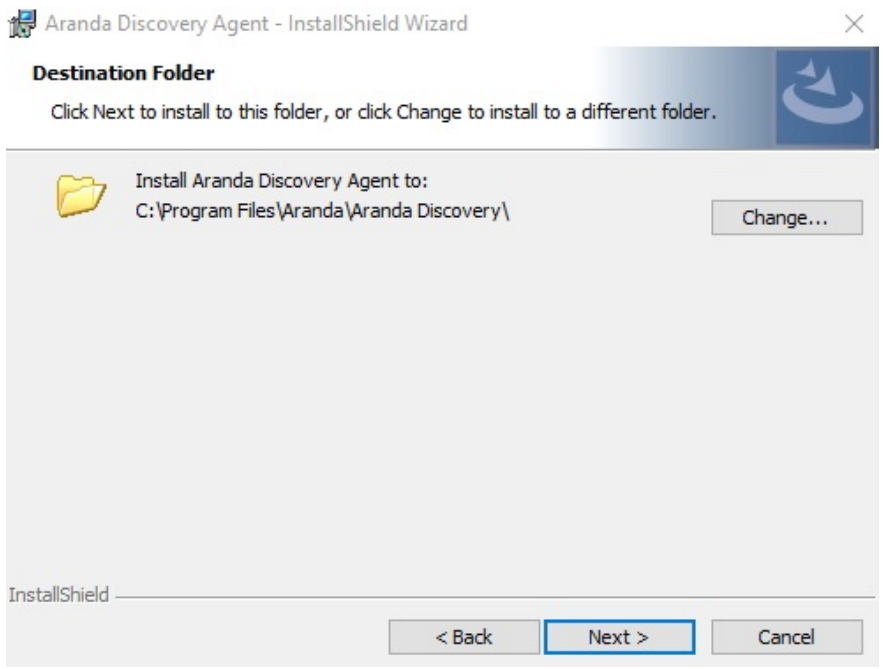
1. Run the installer Aranda.Discovery.Agent.x.x.x.exe



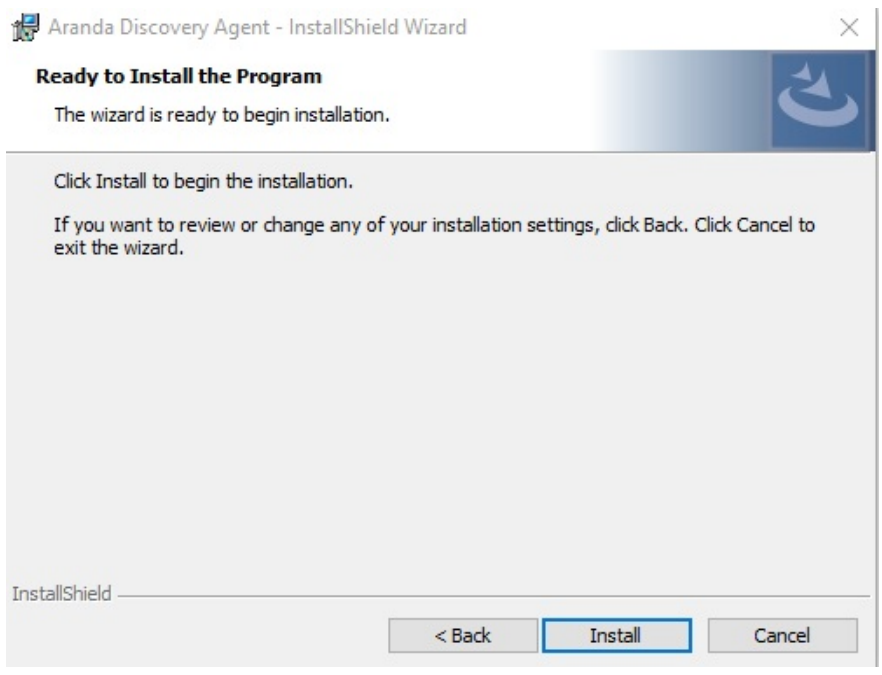
2. In the Customer Information window, enter the user name, organization, and click Following. These fields may be left empty.



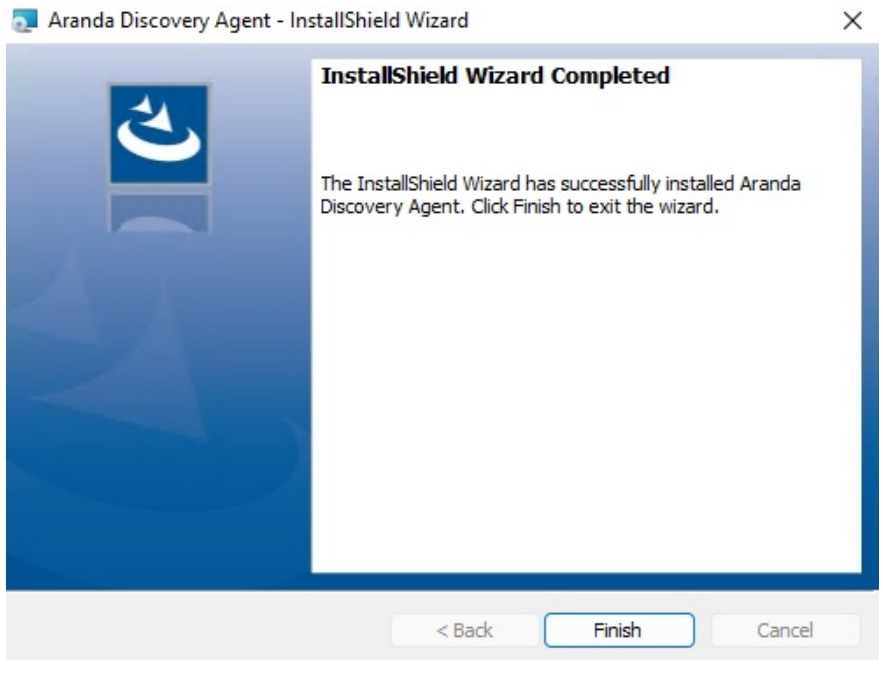
3. In the Destination Folder window, you can change the installation path of the service or leave it by default where the installation suggests, then click Following.



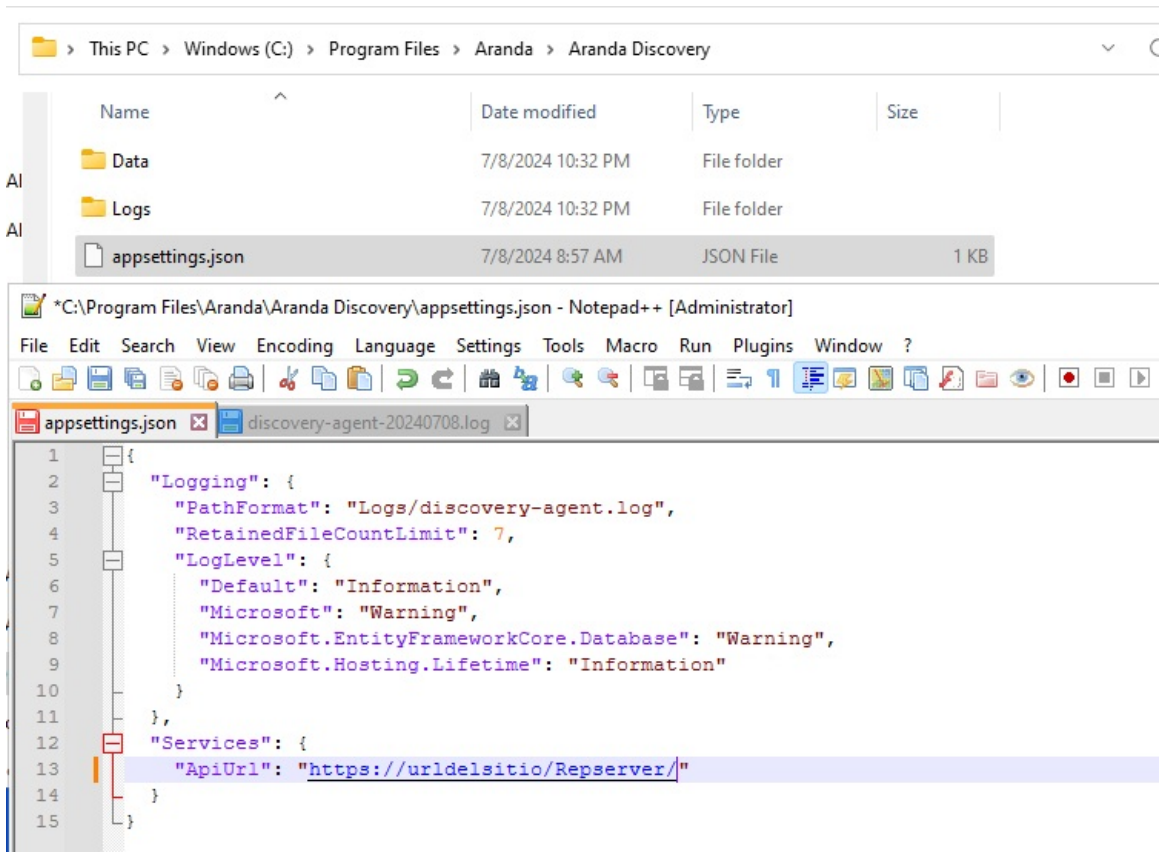
4. Click Install; You must have permissions as a machine administrator.



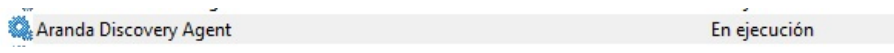
5. When the installation process is finished, click the End.



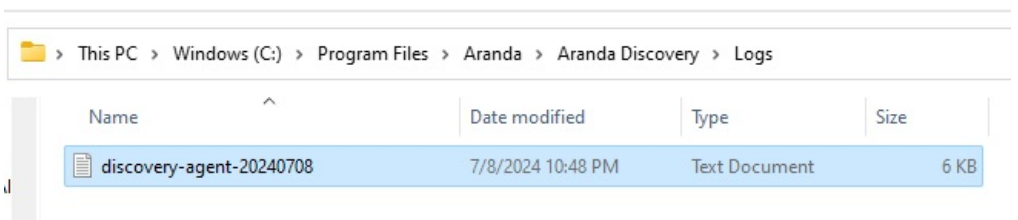
6. To configure the discovery agent, open the appsettings.json in the folder where the service is installed and in the Services in ApiUrl, enter the URL of the site's Repserper.



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.

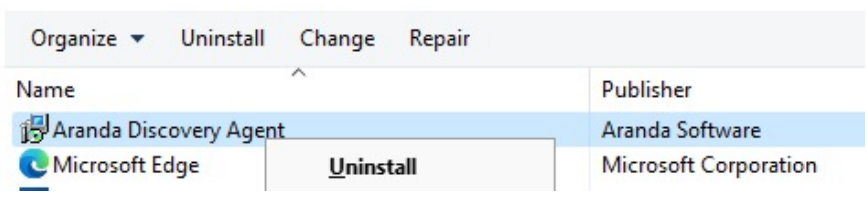


8. The archives of Log will be stored in the following path: C:\Program Files\Aranda\Aranda Discovery\Logs

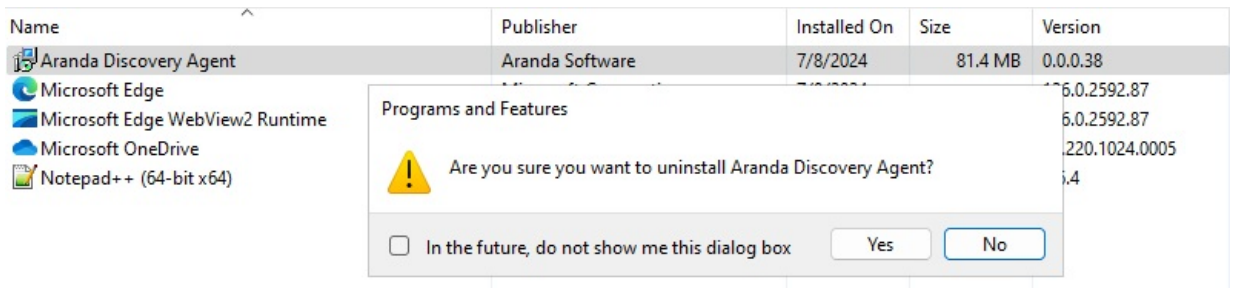


Uninstalling the Discovery Agent

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.

ADM Agent Installer

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

Agents

ADM Agent Installer for Windows

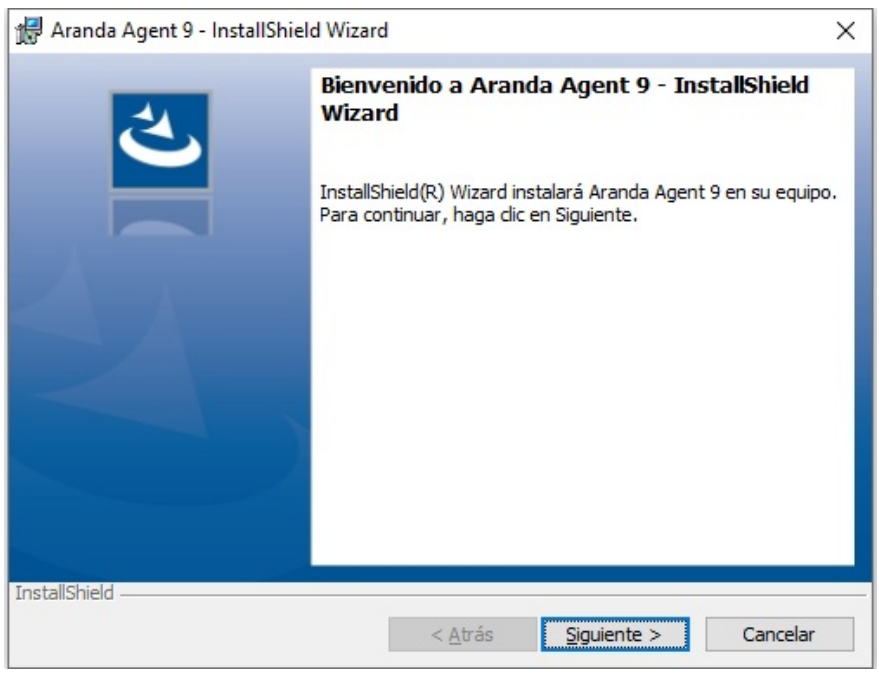
↩ ADM Agent Installer

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.

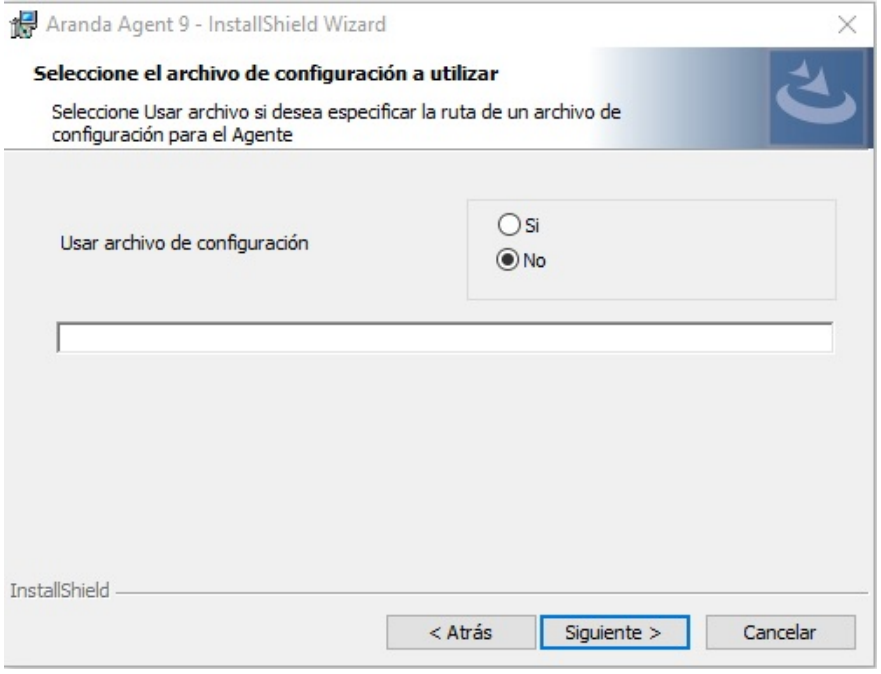
> ⚐ Note: The agent can be installed unattended and automatically through the Agent Distribution, or manually.

Manual Agent Installation

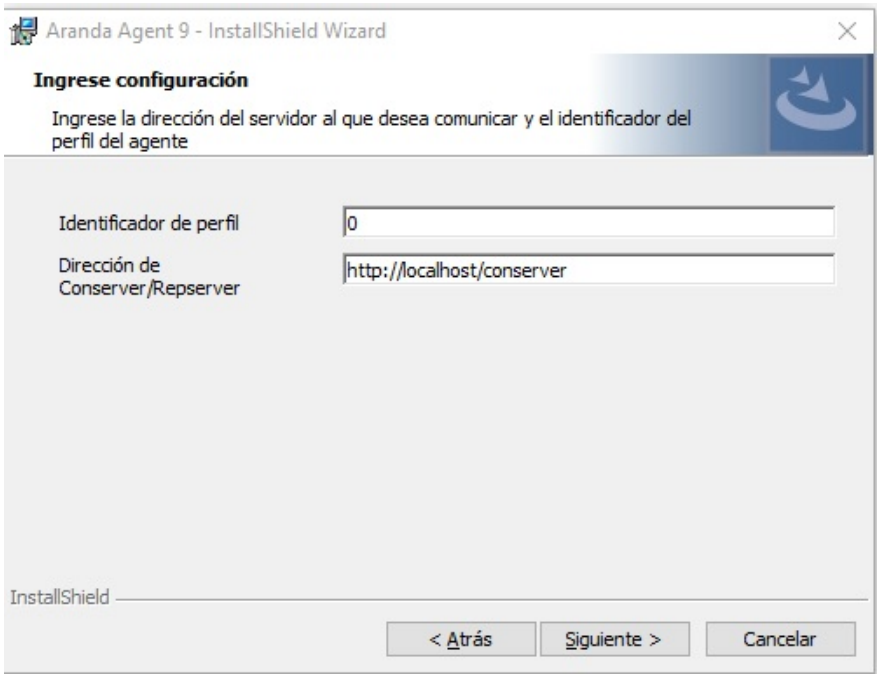
1. Click on the Aranda Agent installer. The wizard will start. Click Following.



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

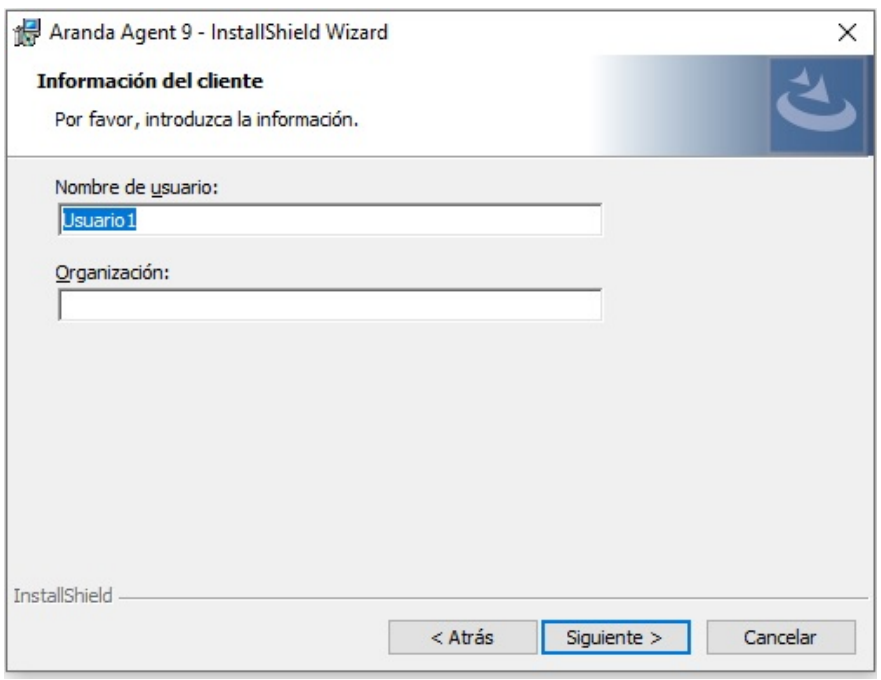


3. Enter the profile identifier, entering 0 downloads the profile that is configured by default. Enter the address of Conserver or Repserver according to the pointing configured in the MQTT broker [MQTT Broker Configuration]. By entering the ADM console you can obtain the communication route. Configuration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

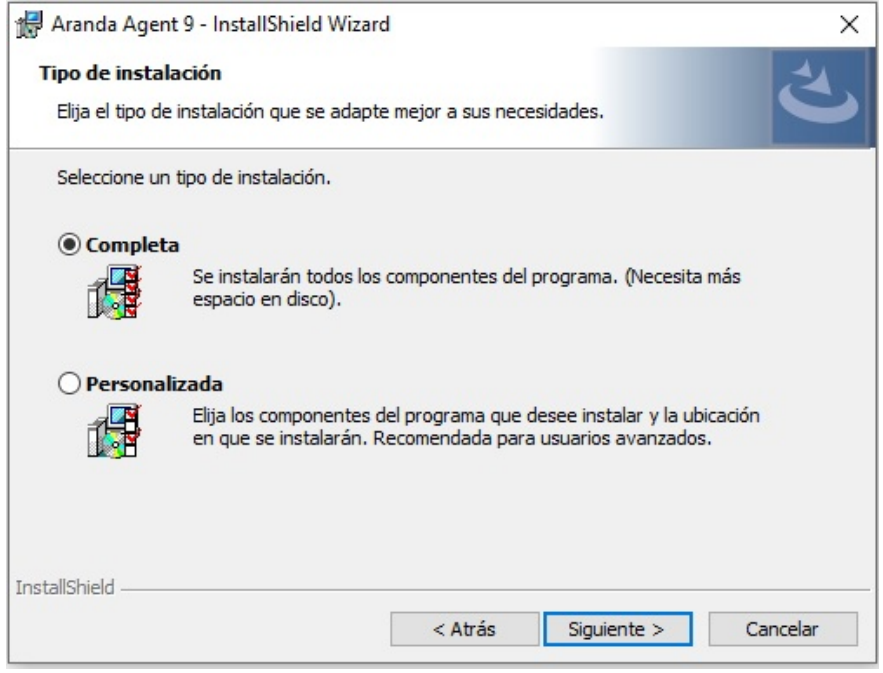


⚐ Note: Agent addressing when repserver only works with an agent version since 9.13.

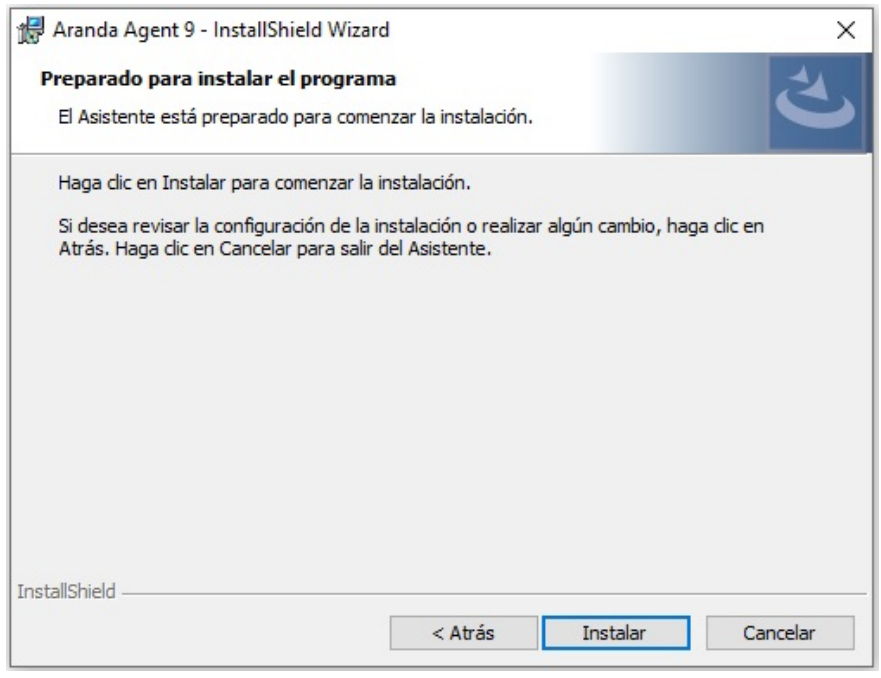
4. Enter the username and organization where the agent will be installed.



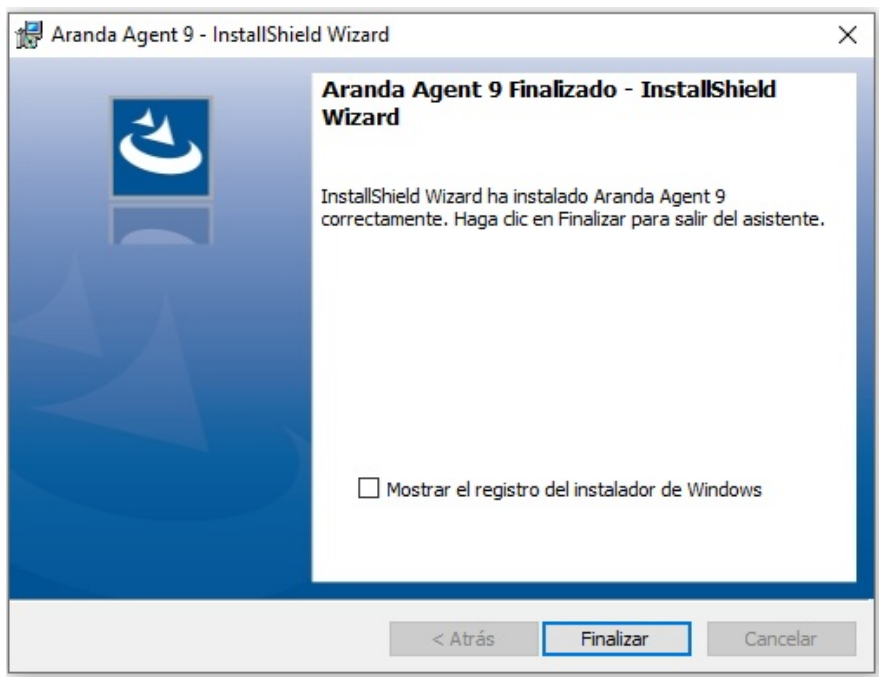
5. Select the type of installation you want to perform (complete or customized)) and click Following.



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



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 promt 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.

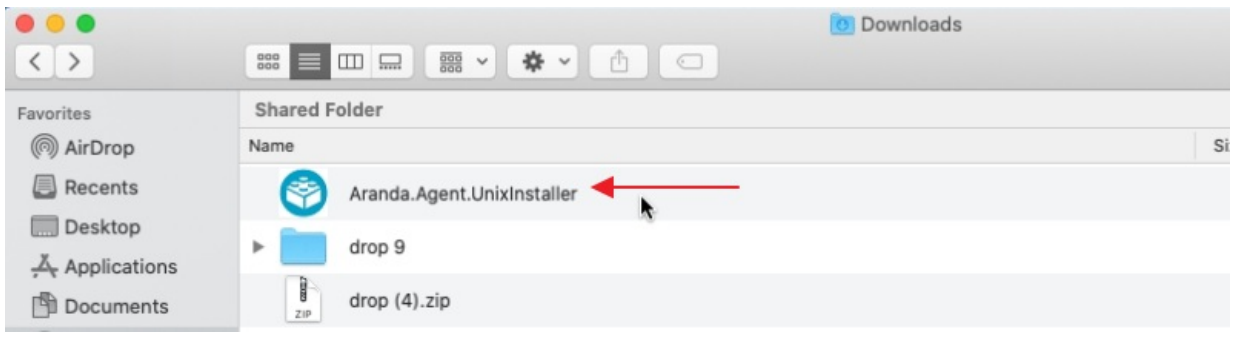
↩ ADM Agent Installer

Installing the Agent on MacOS

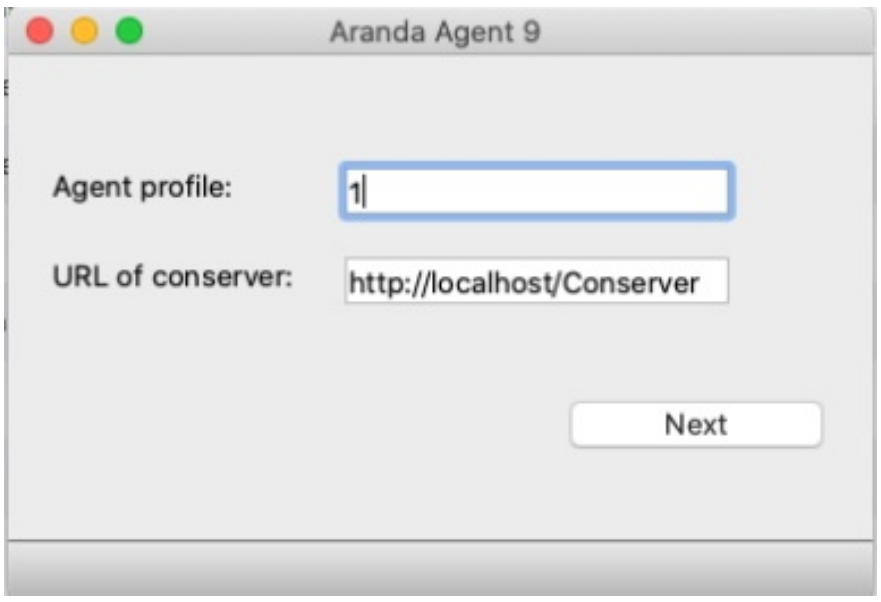
↩ ADM Agent Installer

Installing the agent from the UI

1. Run the agent app.

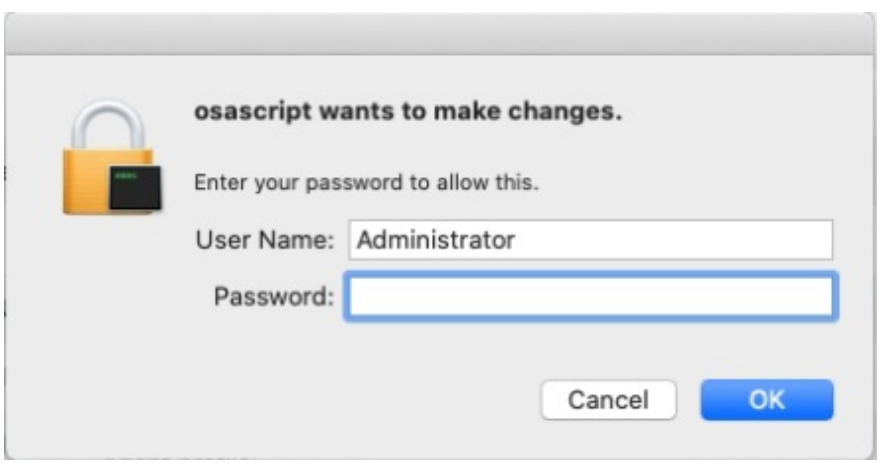


2. Enter the profile identifier, typing 0 downloads the profile that is configured by default. Register the Conserver or Repserver address according to the pointing configured in the MQTT broker [MQTT Broker Configuration]. When you enter the ADM console you will be able to obtain the communication path.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

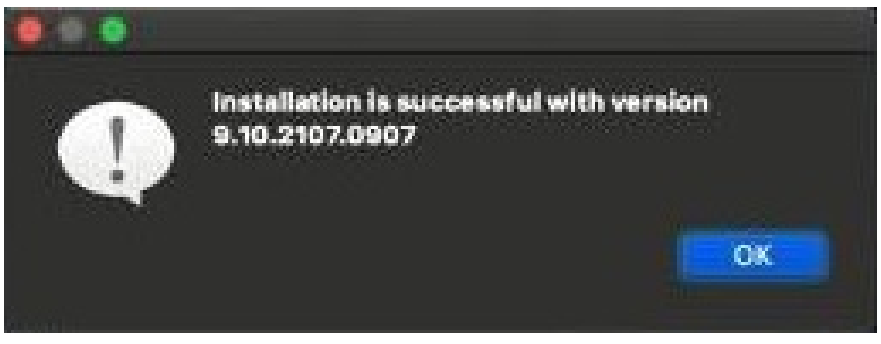


⚐ Note: Agent addressing when repserver only works with an agent version since 9.13.

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

Line	Instruction
RUTA_INSTALADOR	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

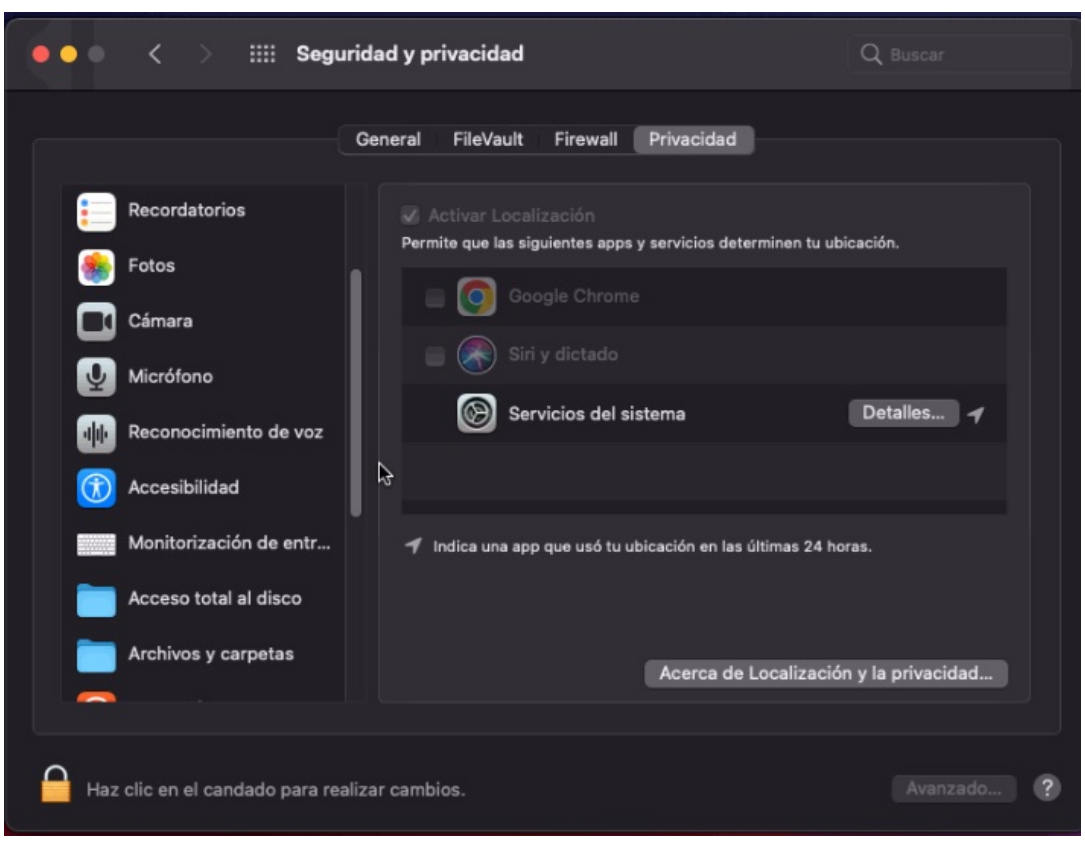
2. After installing the agent, a folder named Aranda is created in the path '/Opt/local' with the libraries, agent services, and another folder in '/etc/' with the name Aranda, where the agent's logs and database are stored. Deleting these folders will uninstall the agent.
—

Grant agent permissions

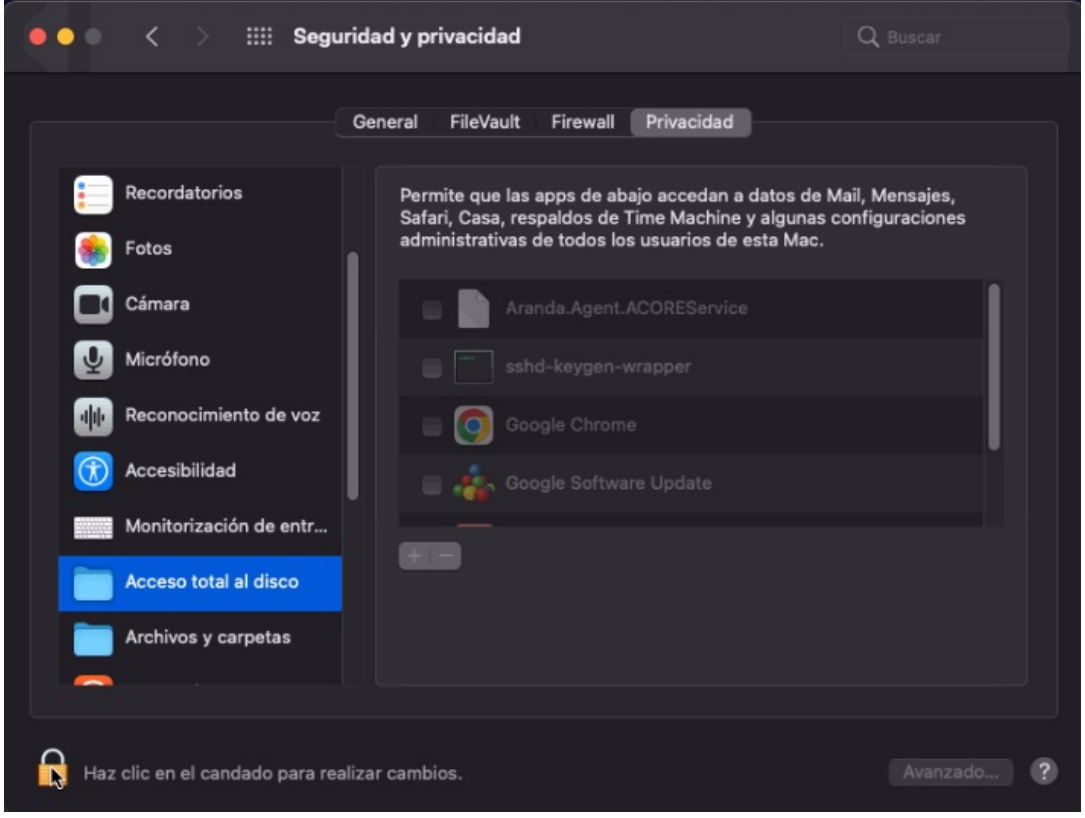
Full disk access permission must be granted to the agent, this action is performed taking into account the following steps:

1. Open System Preferences > Security & Privacy.

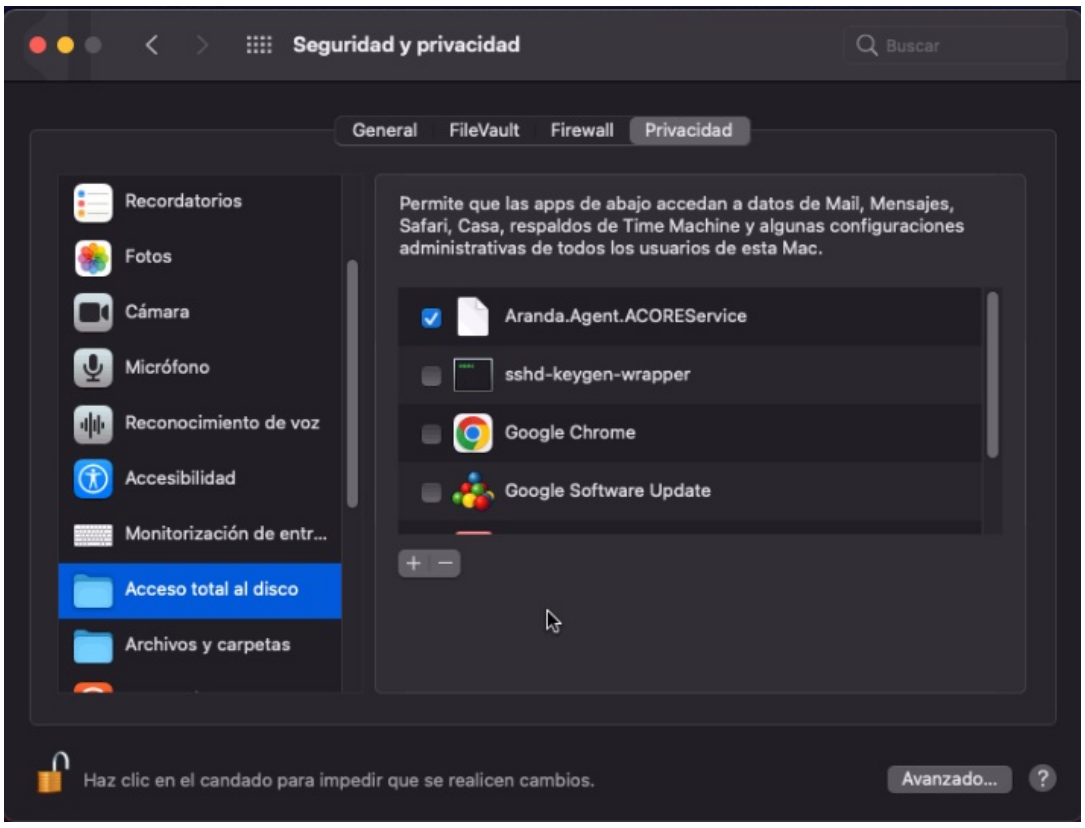
2.Select the Privacy.



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



4. Select Service Aranda.Agent.ACOREServiceicon, 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.

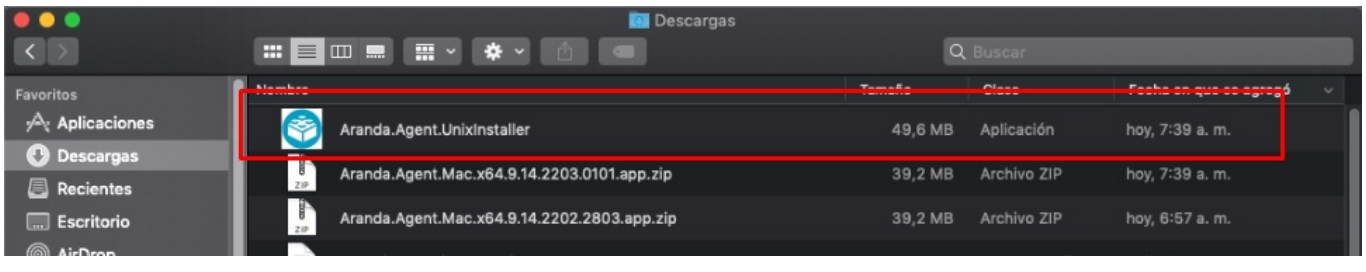
- Device Location
- Deleting Files by Extension
- Virtualization
- Monitoring
- Sending messages
- Sending Commands (Only allowed with the current system user)

Agent Modification

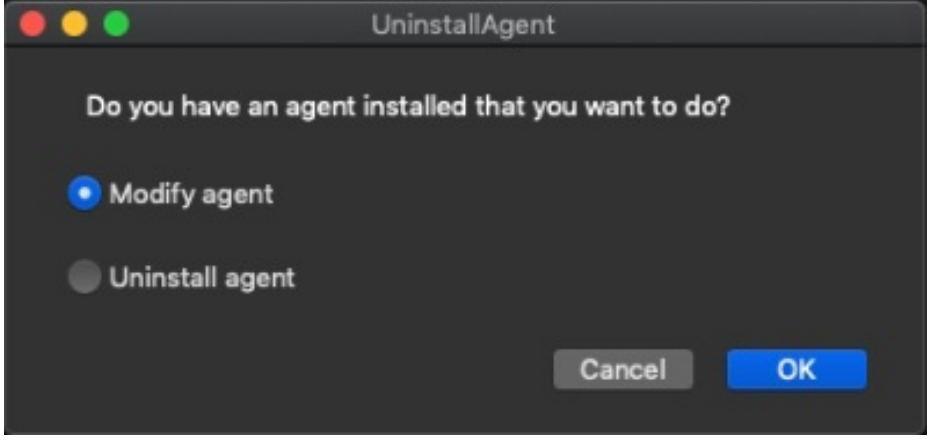
> ⚐ Note: Available in the agent version higher than 9.14,
> If you have an agent installed earlier than this, the uninstall window will not appear.

Agent Modification (Repserver Host or Conserver and Profile)

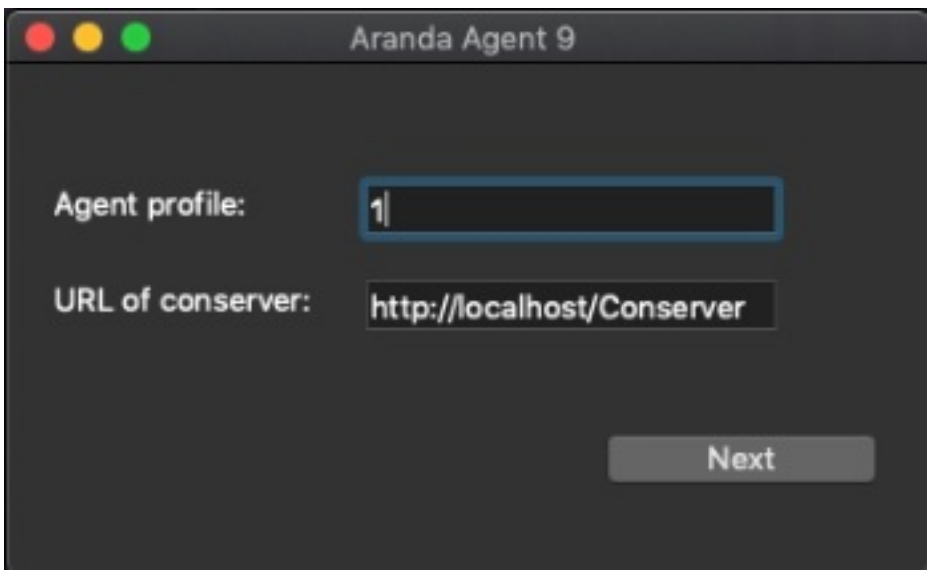
1. To modify the agent you can do it from the installer Aranda.Agent.Unixinstaller.app



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
```

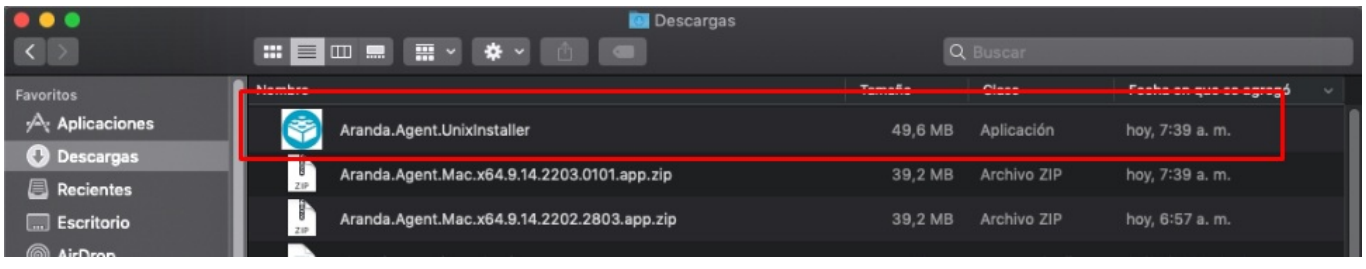
2. Once the folder is entered Aranda We run the following command.

```
sudo sh UninstallAgent.sh
```

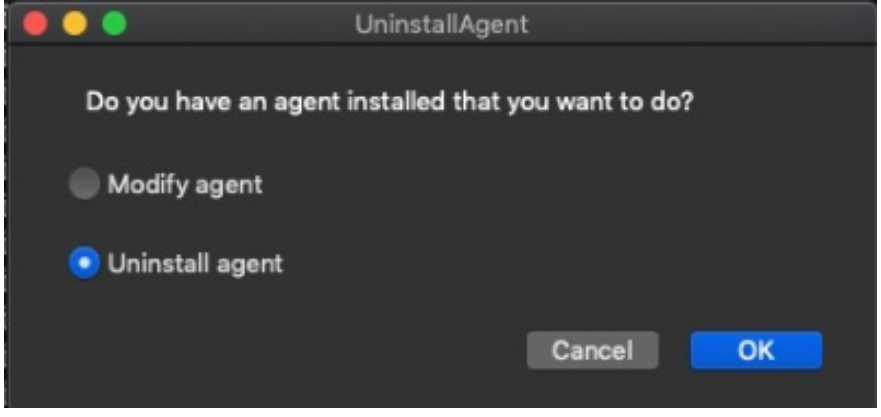
3. Once the command is executed, you can see that the agent was successfully uninstalled.

Graphical Interface

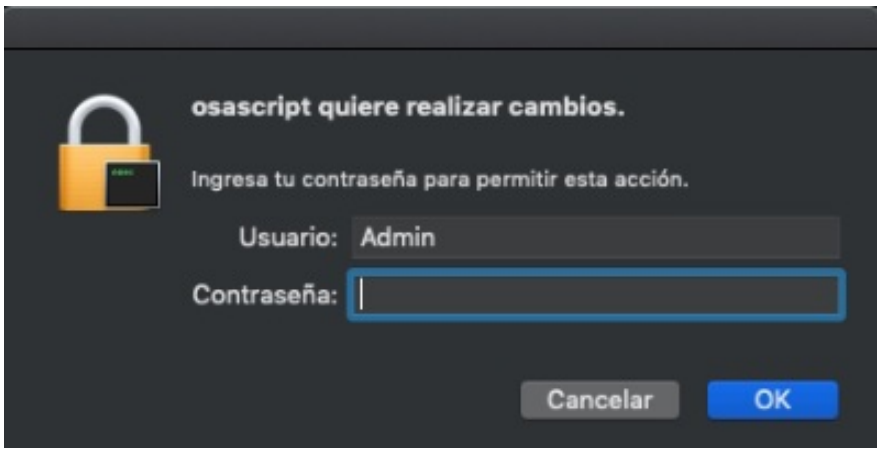
1. Run the installer Aranda.Agent.Unixinstaller.app.



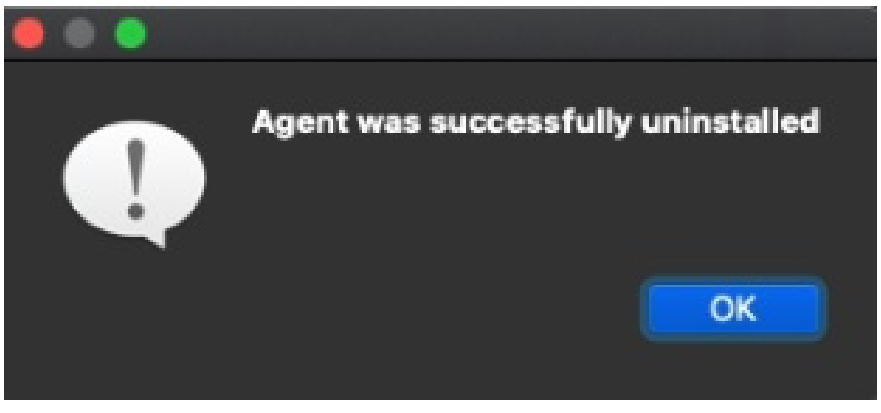
2. In the Uninstall Agent window, select the Uninstall agent and click OK



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



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



↩ ADM Agent Installer

Installing the Agent on Linux

↩ ADM Agent Installer

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_INSTALADOR/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.
↩ ADM Agent Installer

Deploying the ADM Agent by Domain Policy

↩ ADM Agent Installer

Create Execution Files

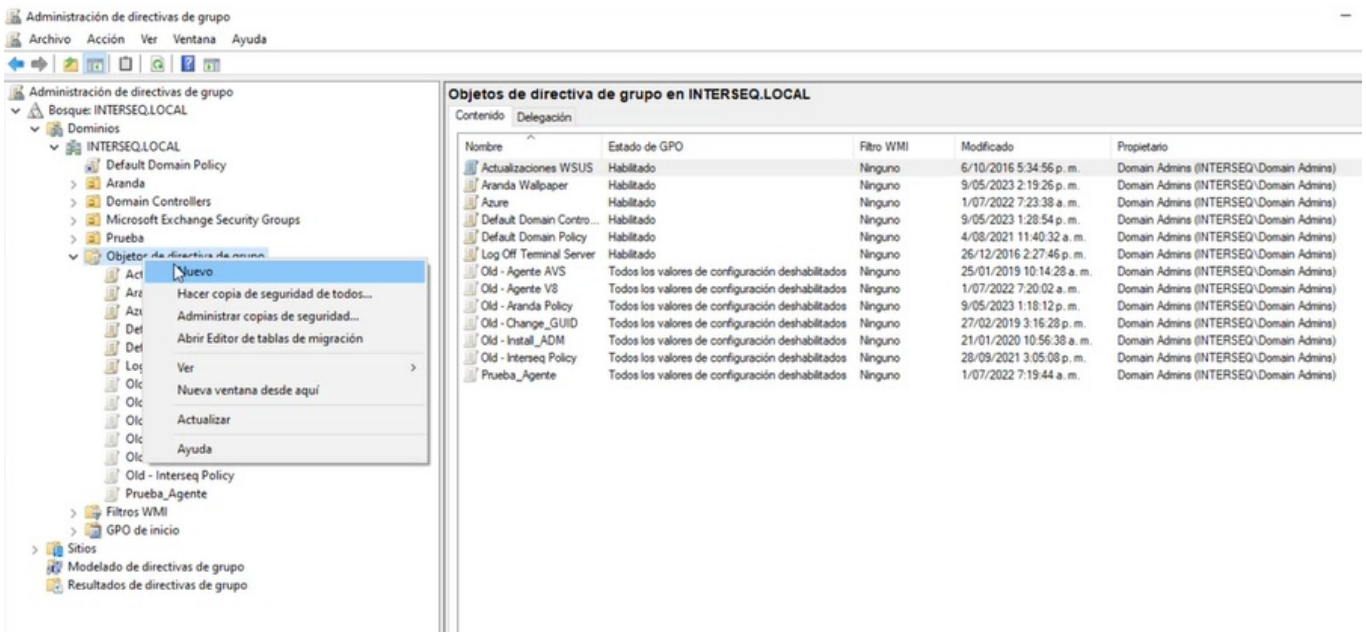
1. Define a file .bat with the ADM Agent .msi installation command.

```
msiexec /i "Aranda Agent 9.msi" /norestart /qn AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=13
```

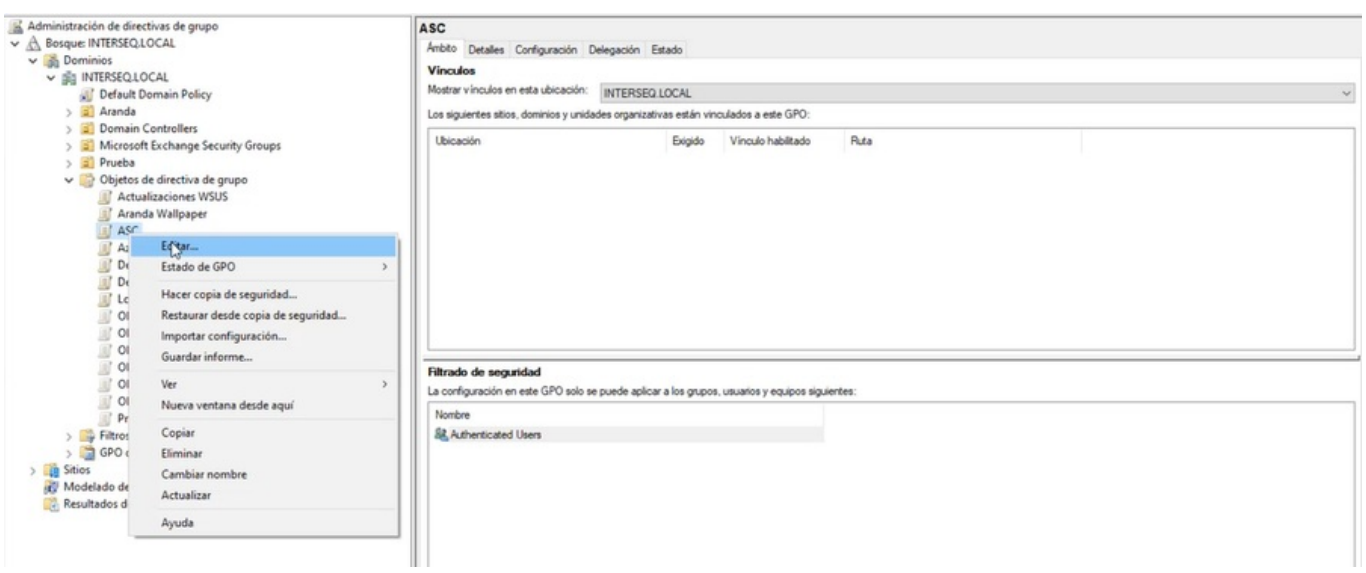
AGENT_PROFILE_ID=[UNIT]	Identifier of the profile to be installed, 0 is a profile selected in the application as the default profile.
AGENT_SERVER_ADDRESS=[STRING]	Path of the Server.

Create Group Policies

1. Enter the option of Group Policy Management, in the local domain, select the Group Policy Objects and click on the New.

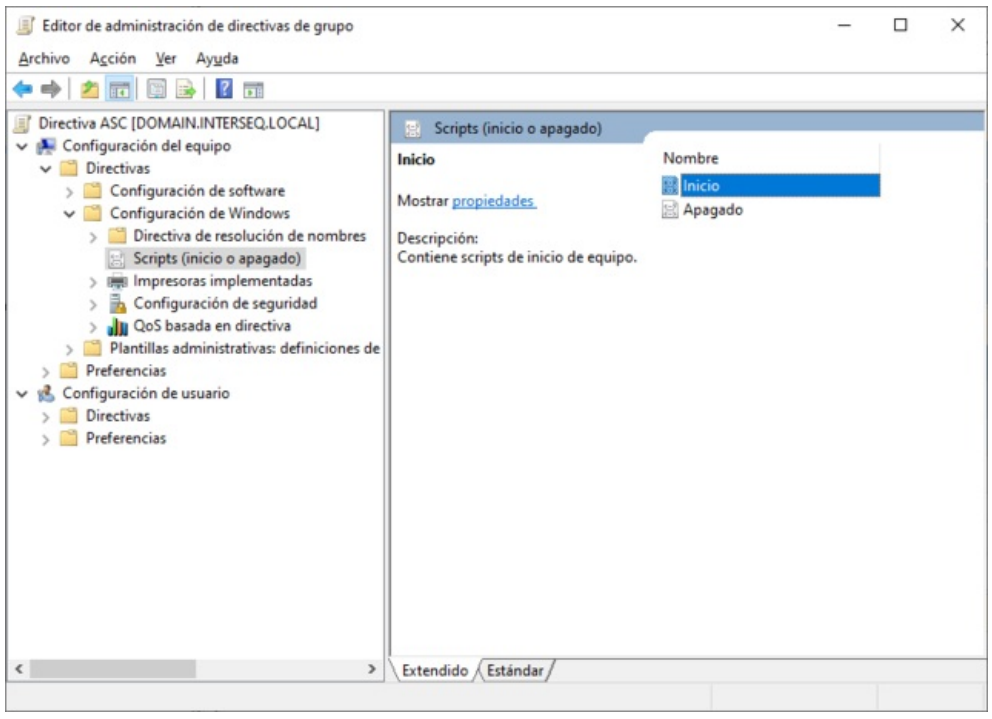


2. In the window New GPO Enter a name of the new policy. Example: ADM. 3. Select the newly created policy and click the option Edit.

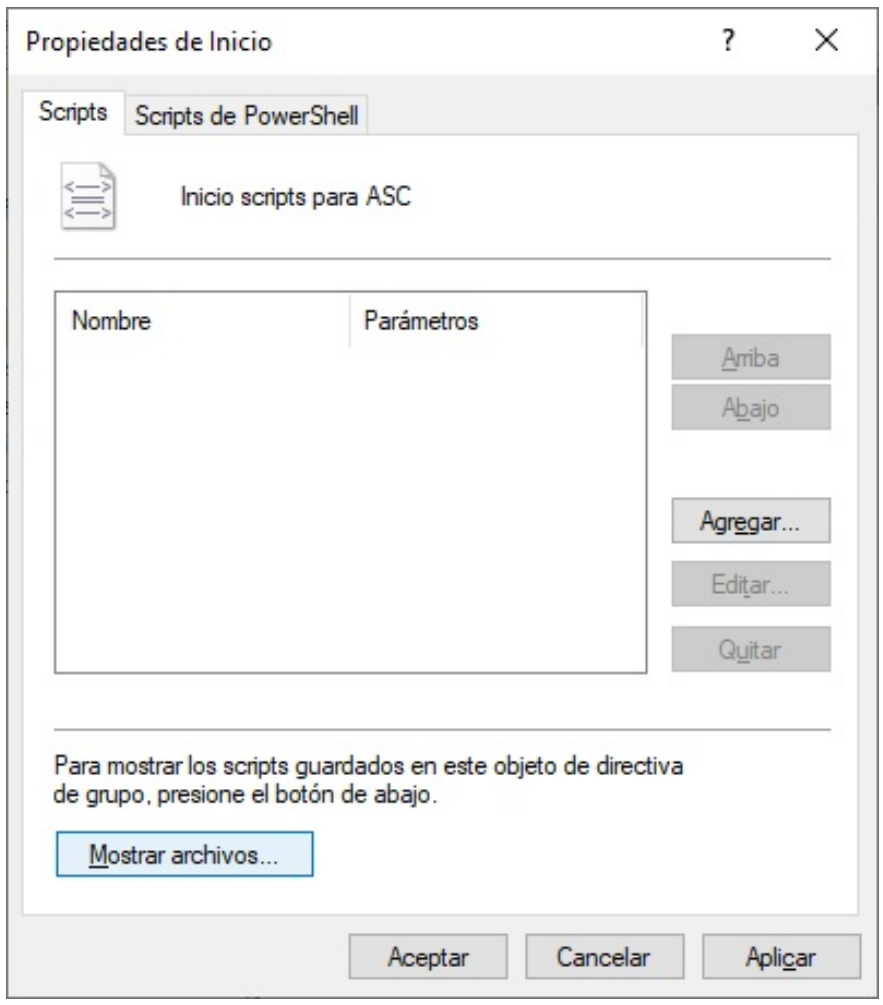


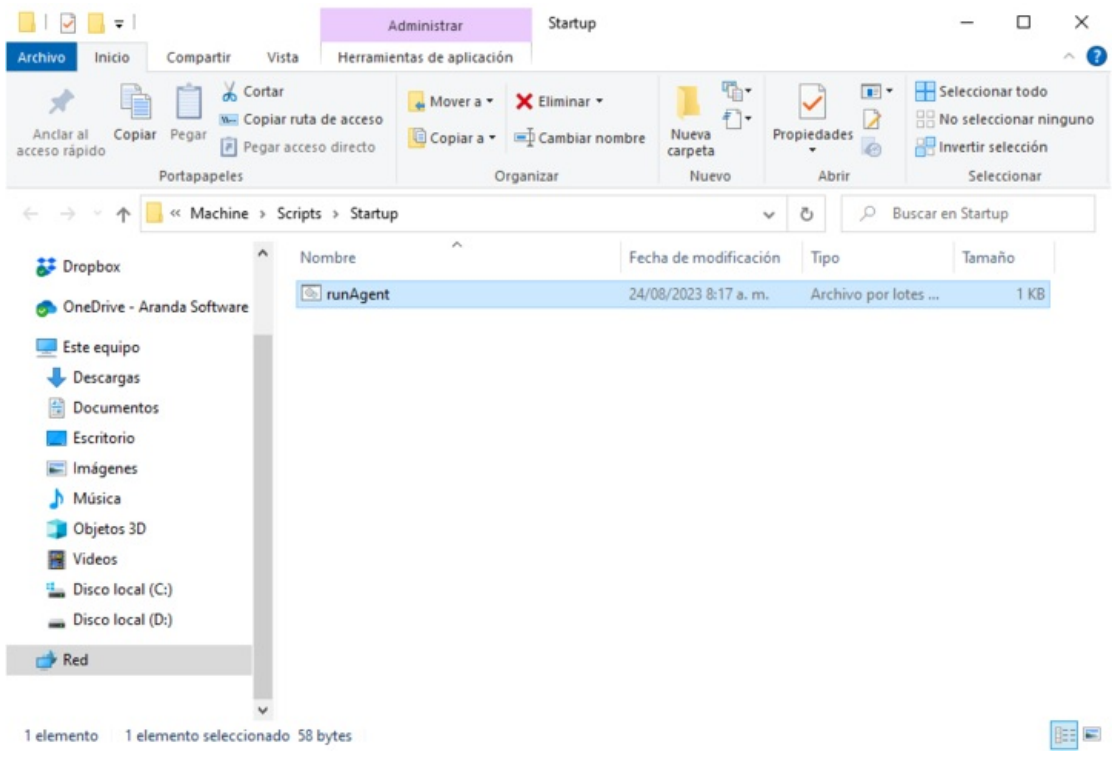
4. In the Group Policy Management Editor, select the Computer Configuration, Policies, Windows Settings option, and select the Scripts. In the information view, select the Beginning .

⚐ Note: Configure the startup policy allows the ADM agent to run at logon time.

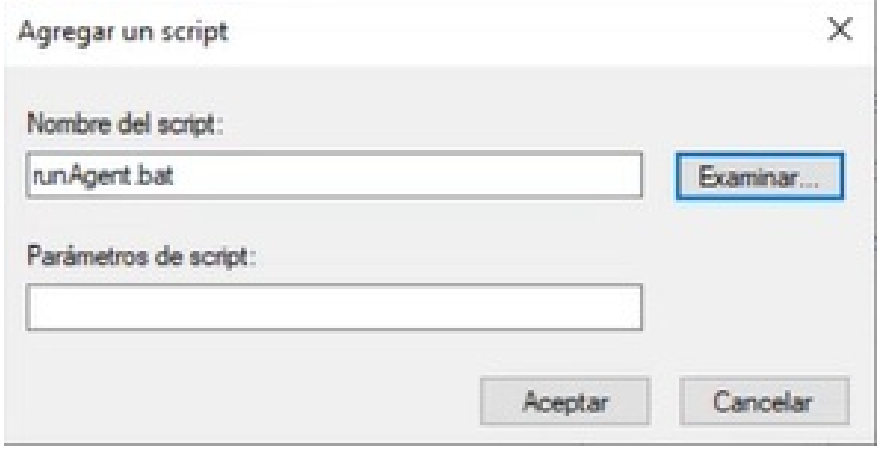


5. In the window Startup properties, select the Show Files to paste the file .bat of the ADM agent.



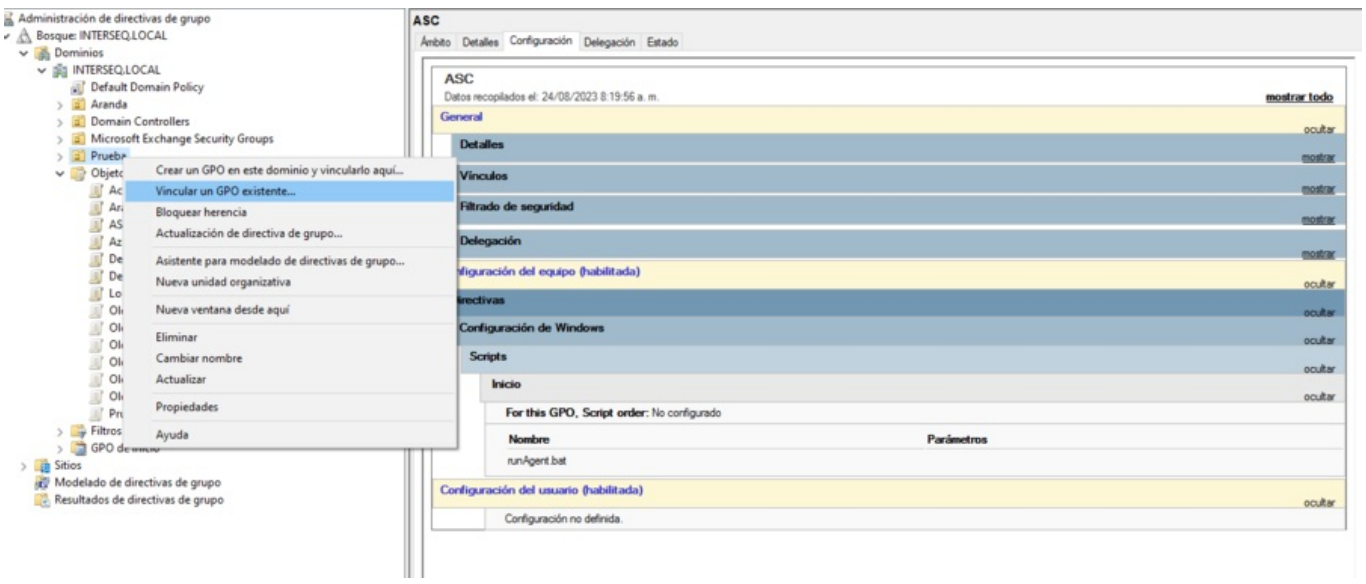


6. In the window Startup properties, select the Add and in the window Add a Script Select the Examine to select the .bat file on the ADM agent, when finished click Accept.



Associating the Policy with the Organizational Unit

1. Enter the option of Group Policy Management, in the local domain, select the organizational unit to which you are linking the created GPO, and click the Link an existing GPO.



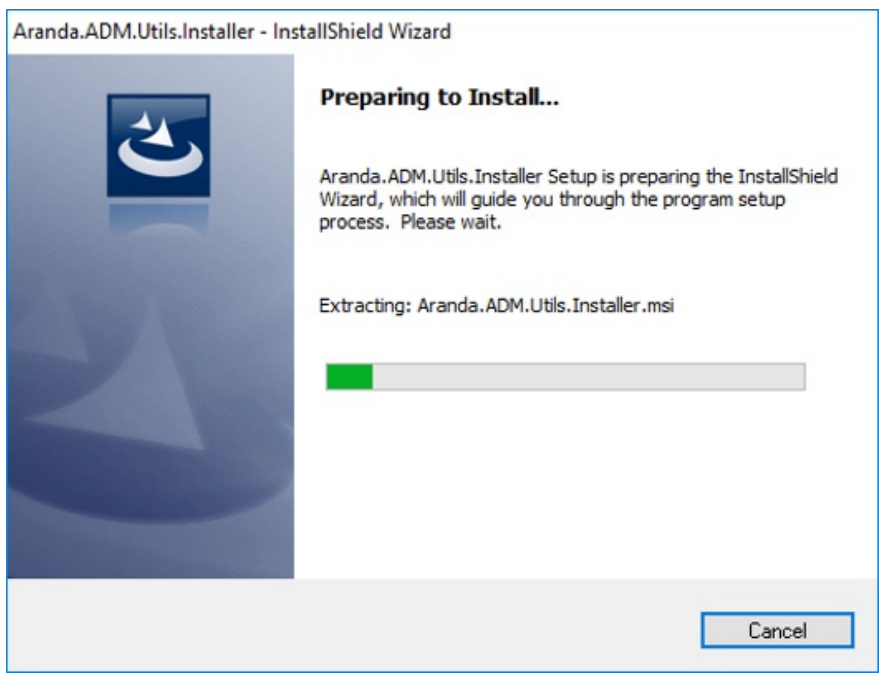
2. In the window that is enabled, select the policy of the created policy.

> ⚐ Note: In the information view, select the configuration to validate that the policy configured with the ADM agent is enabled.

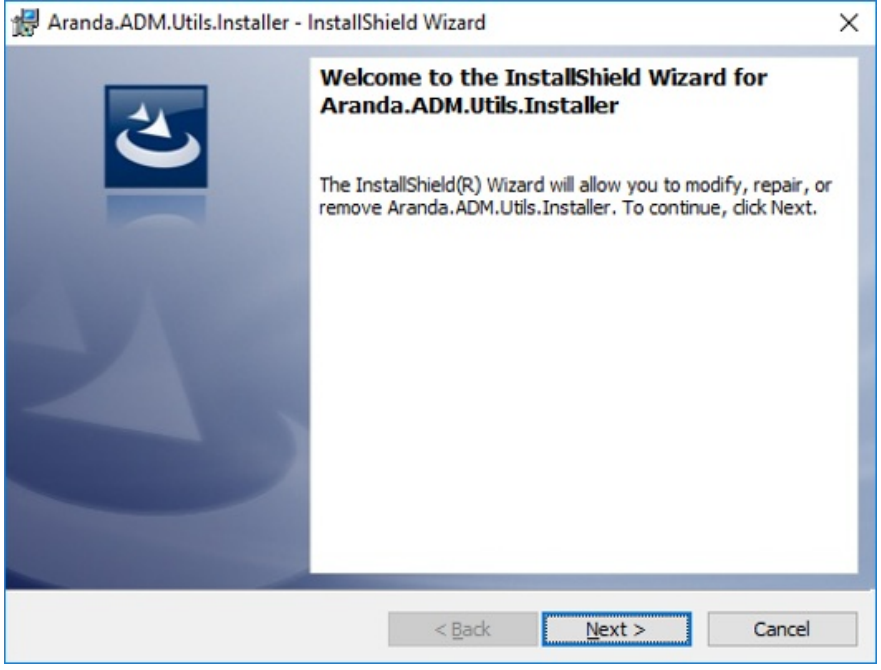
↩ ADM Agent Installer

Remote Support Viewer Installer

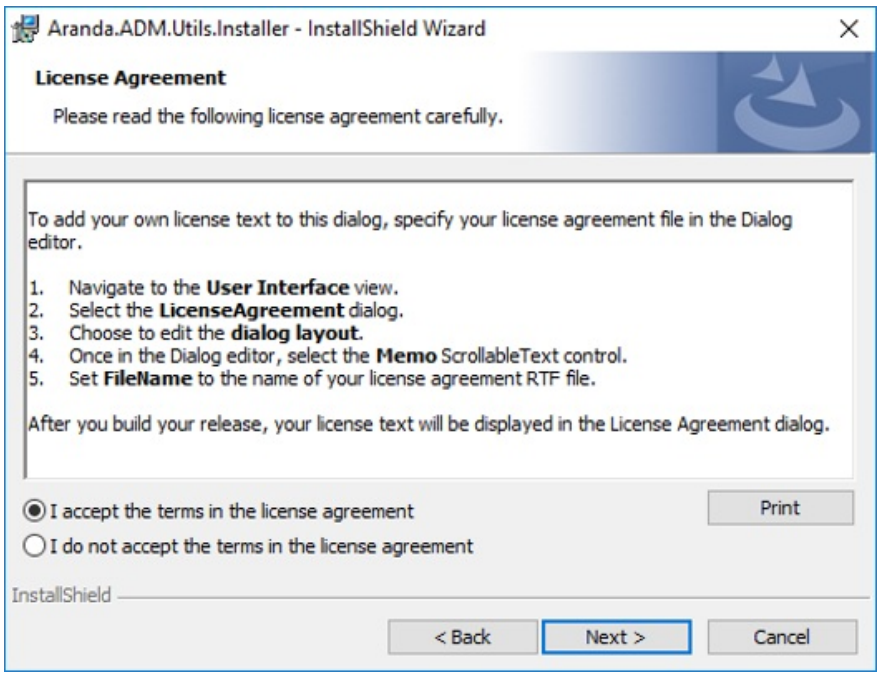
1. To install the Remote Support Viewer click on the utility component: Aranda.ADM.Utils.Installer.



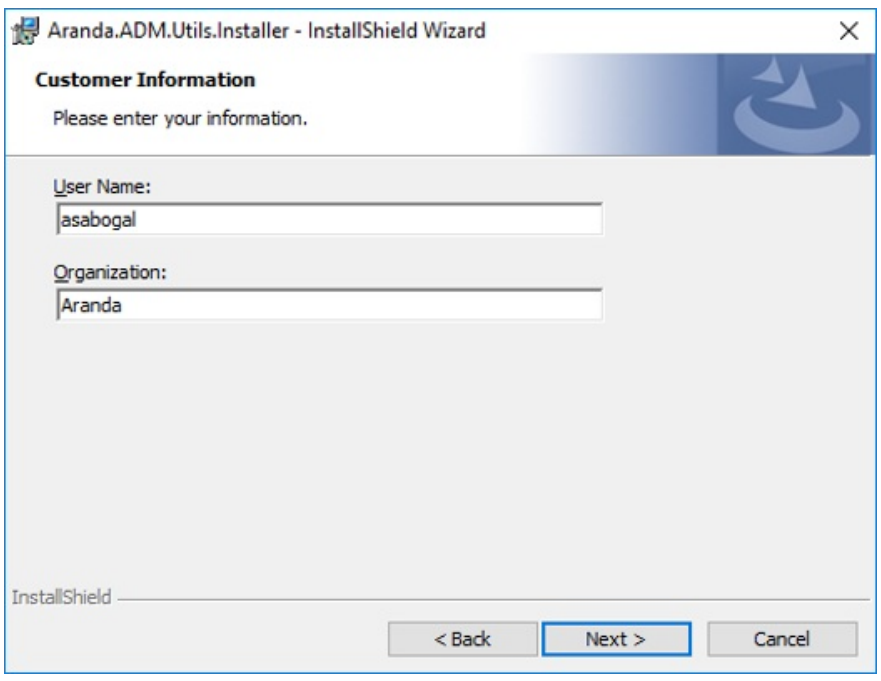
2. A message will be displayed informing you that it is going to be installed Aranda.ADM.Utils.Installer. Click Next.



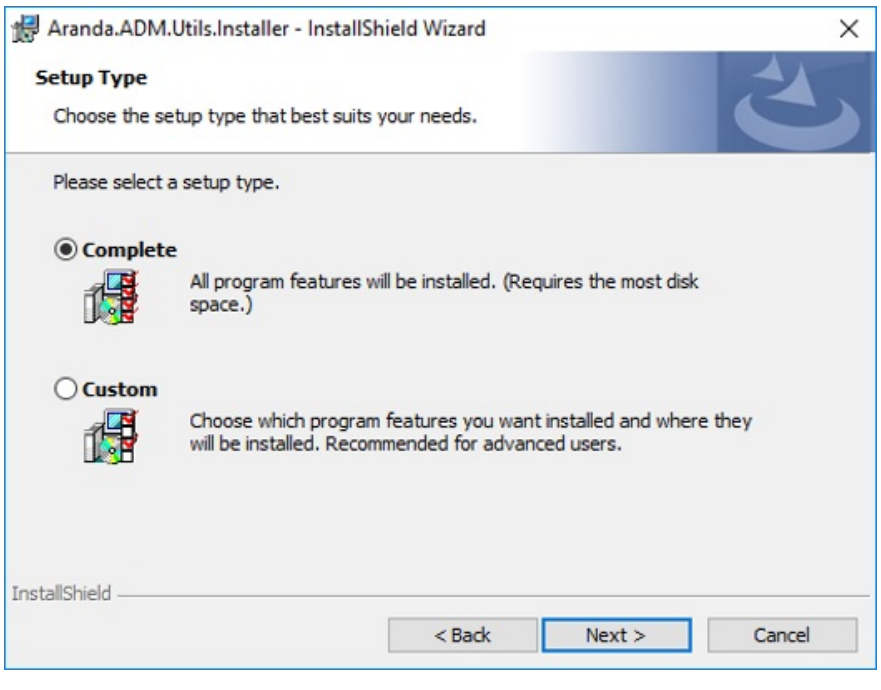
3. In the Licensing Agreements window, select the option: I accept the terms in the license agreement and click Next



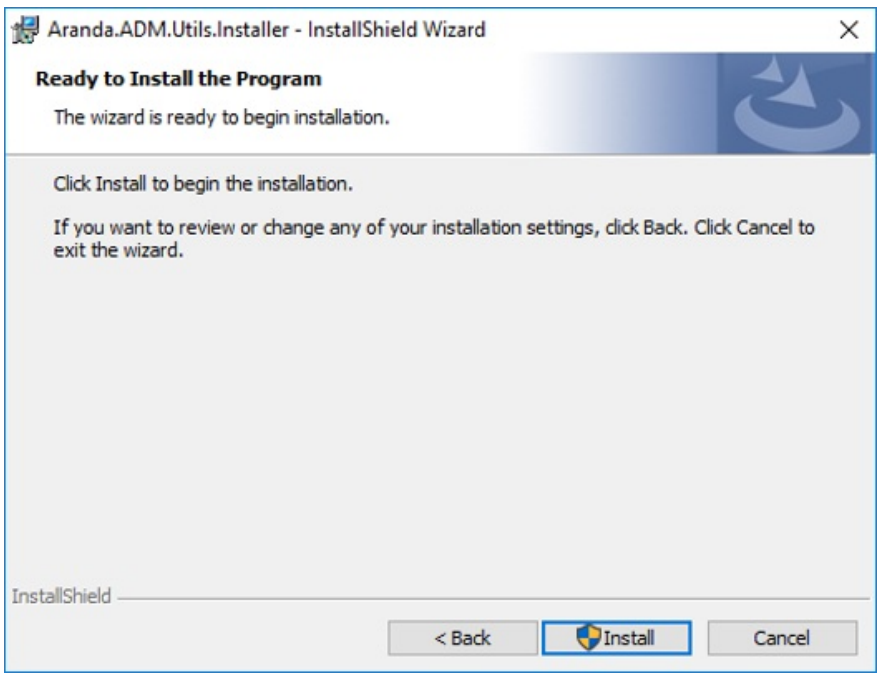
4. In the Customer Information window, enter the username and organization where the utility will be installed. Click Next.



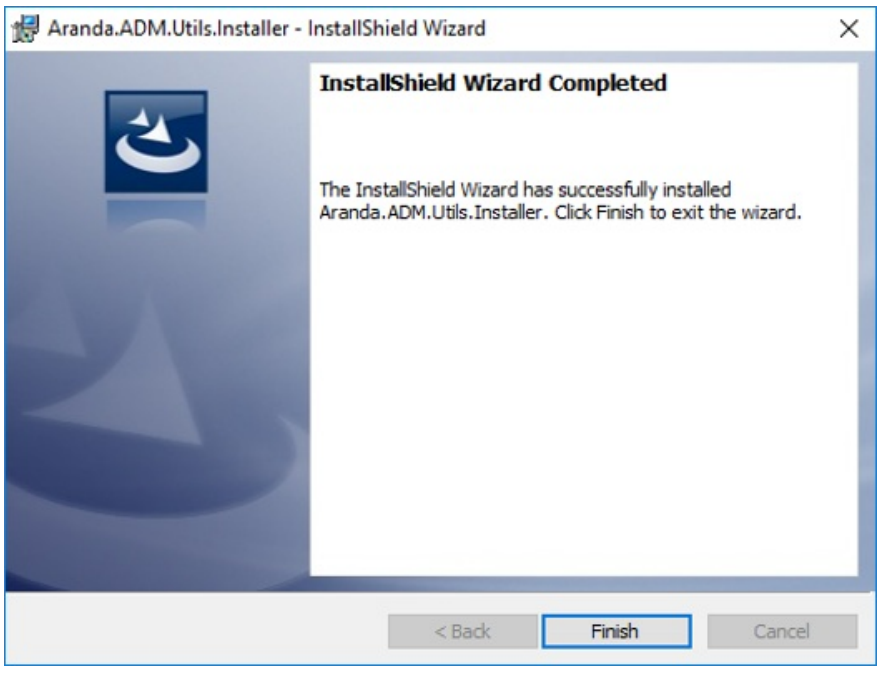
5. In the Configuration Type section select the required installation type; Complete (complete) or Custom (customized) and click Next.



6. Click the Install to start the installation process.

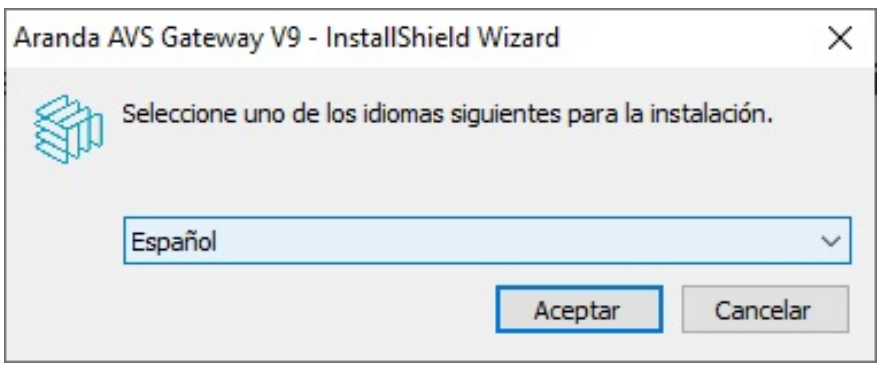


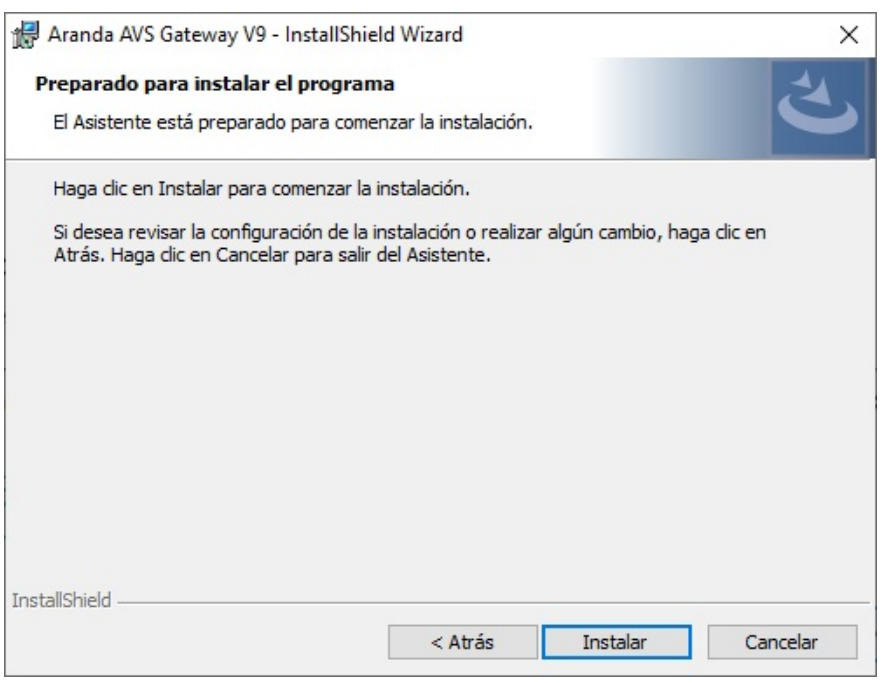
7. After the viewer installation is complete, you will be able to display the following confirmation message. Click Finish.



Gateway V9 Installer on ADM

1. To perform the integration of the V9 Gateway in ADM, you must run the Aranda.AVS.Gateway.V9.x.x.x.exe following the default instructions and settings.





2. Once installed you will be able to view the following program :

Aranda AVS Gateway V9	Aranda Software	28/09/2021	2,21 MB	9.0.0.8

—

Related Links:
- Gateway Configuration
- Gateway Configuration in ADM Web Console

Gateway Configuration

Gateway V9 Configuration

↩ Gateway Installer

1. To configure the Gateway you must go to the C:\Program Files (x86)\Aranda\AVS Gateway V9 and open the Aranda.AVS.Gateway.V9.exe.config.

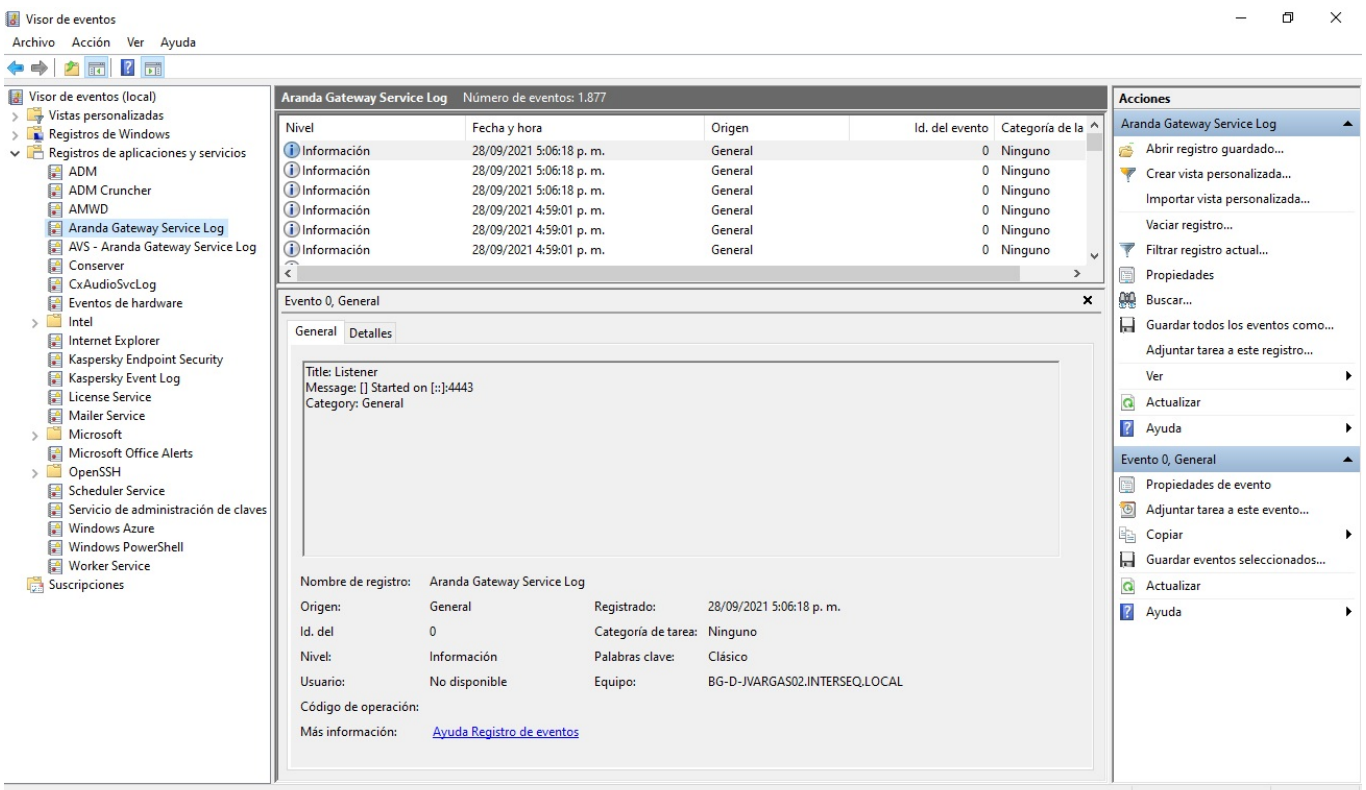
```
  <appSettings>
    <add key="CertificateParam" value="QXJhbmRAR2F0ZXdheTIwMTA="/>
    <add key="CertificatePath" value="ArandaGateway.pfx"/>
    <add key="ReadTimeOut" value="5"/>
    <add key="MaxBuffer" value="32768"/>
    <add key="Port" value="4443"/>
    <add key="SSL" value="true"/>
    <add key="KeepTime" value="2"/>
    <add key="General" value="true" />
    <add key="State" value="false" />
    <add key="Debugging" value="false" />
    <add key="Notification" value="false" />
    <add key="CertificateSubject" value=""/>
  </appSettings>
</configuration>
```

⚐ Note: It is recommended to leave SSL at true. The Gateway is installed with a default certificate, this can be changed by the user. To do this, you must specify the file name of the PFX certificate in the path C:\Program Files (x86)\Aranda\AVS Gateway V9\Resources on the key CertificatePath. The password of the same is set to base64 in the key CertificateParam .

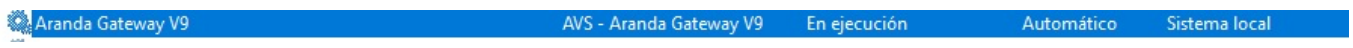
2. The port can be chosen at liberty. Set the firewall rules of the machine and the cloud provider in case of being deployed in the cloud.

3. The port must be enabled on the destination machine to make remote control.
To increase the level of logs, you must set true to Debugging (optionally also to Notification and State).

4. The logs can be viewed in the Windows Event Viewer under Application and Service Log, searching for Aranda Gateway Service Log.



5. When the setup is complete, you must restart the following service:



—-

Gateway download by the Agent

The agent downloads the gateway through the conserver. To do this, the conserver saves this information in the folder:

```
C:\Conserver\Downloads\Gateway\0
```

Only the Gateway that is currently selected as the default and active will be saved here.
The agent downloads the Gateway on startup and updates it every hour. If any modifications are made to the previously created Gateway, the agent must be expected to download it under the above scenarios.

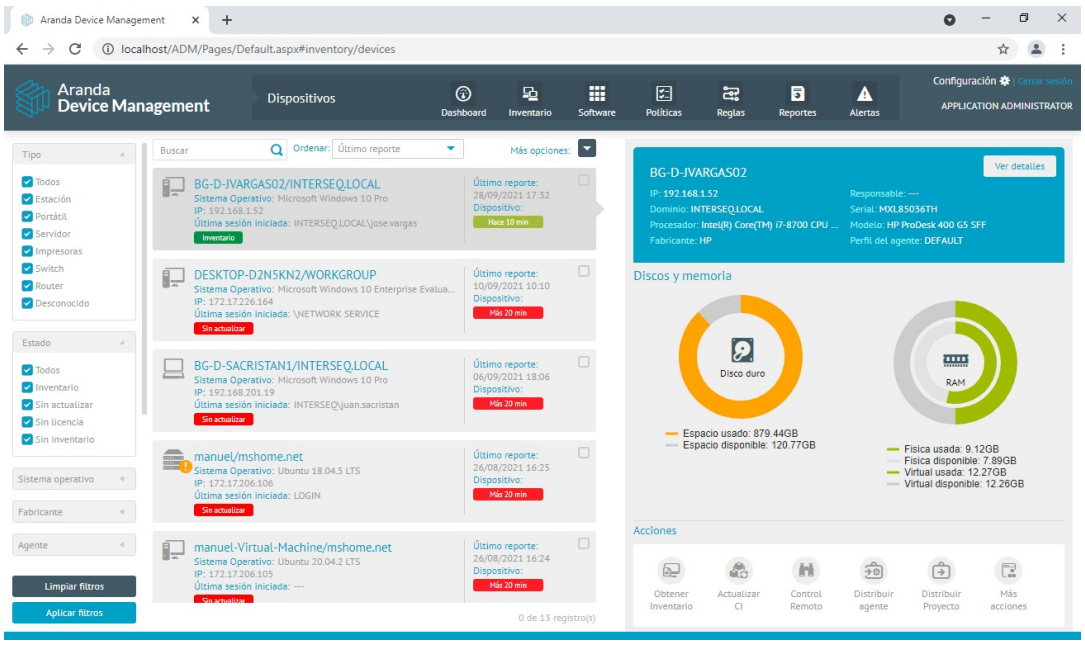
Gateway download by the Viewer

The viewer downloads the gateway when it boots on REST request. So you always receive the latest configuration from the ADM console.

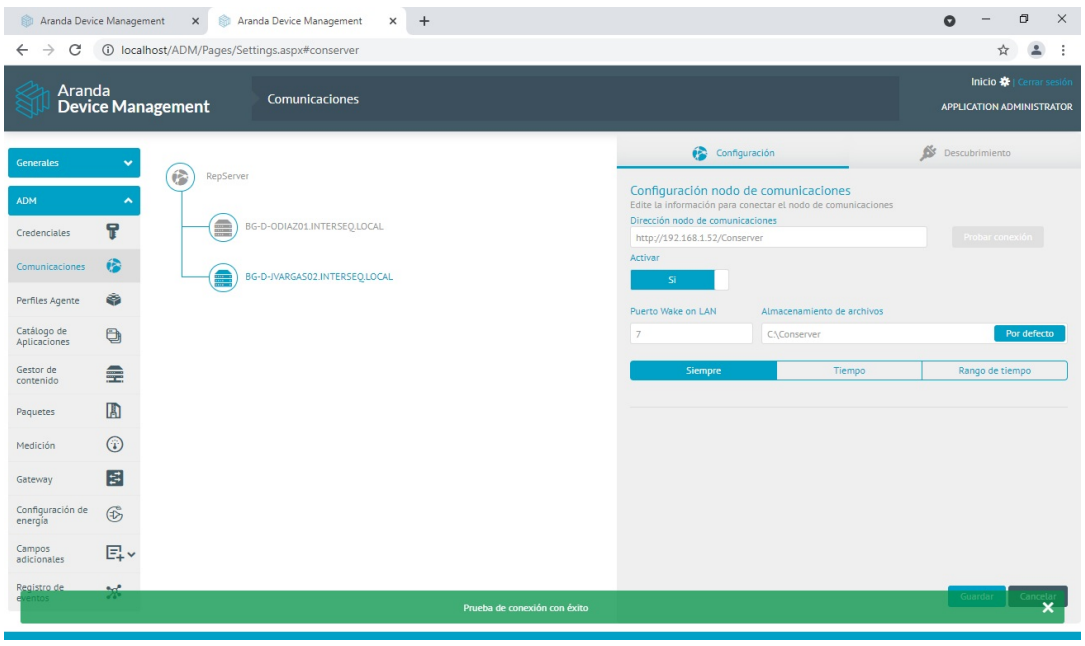
Requirements for Remote Control Outbound Connection via Gateway

In order for a remote control to occur between the viewfinder and the remote equipment, the following conditions must be met

- Have a Gateway de Aranda V9 previously installed and with a valid configuration.
- Have the Gateway configured in the ADM console and have given sufficient time for the agent on the remote computer to download the configuration.
- Make sure the agent is online.



- Ensure that the conservator with whom the agent communicates can receive tasks and communicate them to the agent. One way to test this is to perform the connection test from the console



- Ensure that the gateway can be reached from the agent's computer and the computer where the ADM viewer will be launched.
  As long as these conditions are met, remote control can be taken in different scenarios. For example:

- Cloud or team gateway with public IP.
- LAN Network gateway reachable from both ends.
- Store on LAN Network.
- Cloud console.
- LAN network console.
- Viewer via VPN.
  The conserver can go in the cloud, but from there the agent must be reachable, which would possibly require public IP

Outbound Connection Security

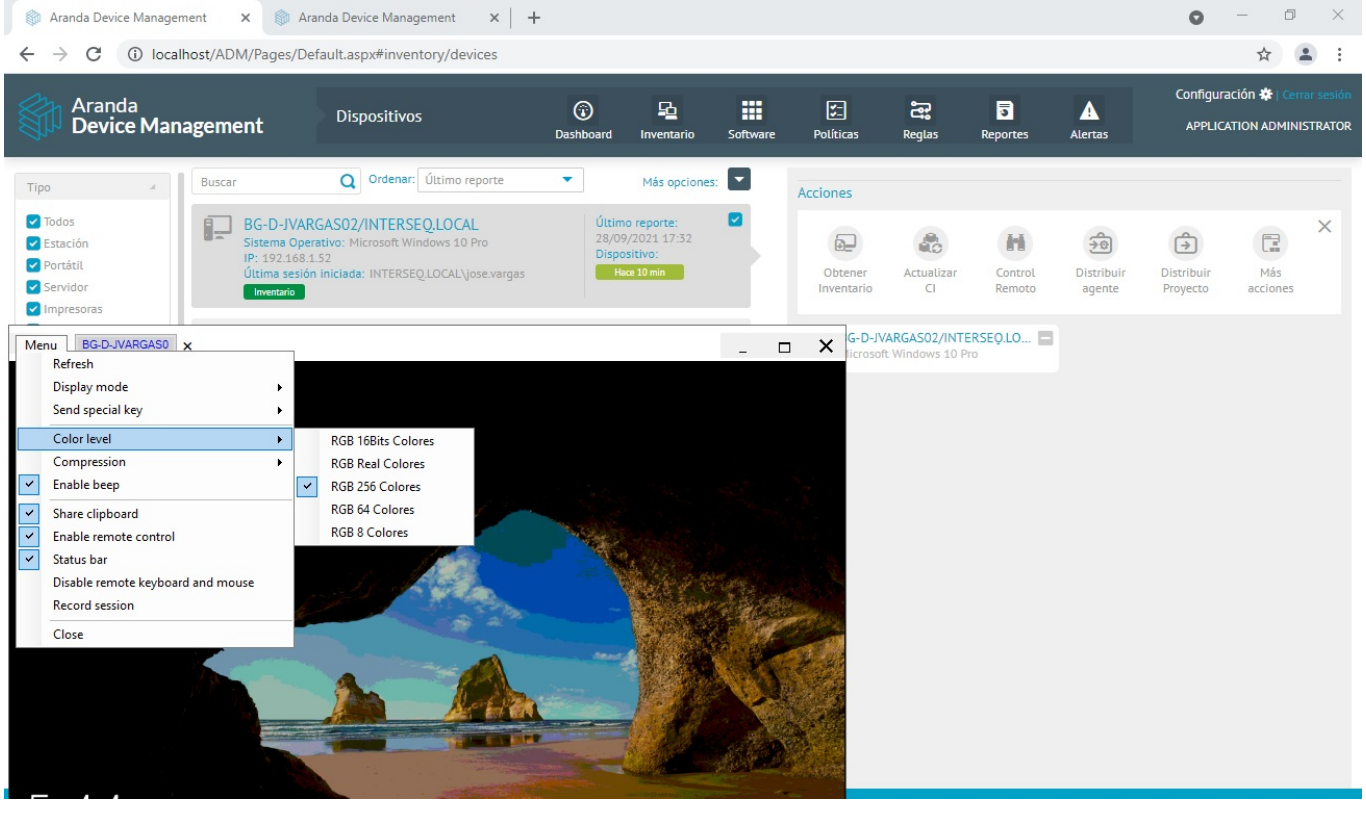
Both the agent and the viewer support SSL-encrypted communication in the case of an outbound connection. For this to be the case, SSL must be enabled on the gateway (both in the Aranda.AVS.Gateway.V9.exe.config as in the ADM console). The agent does not make an outbound connection until ordered by the ADM console.

Direct Connect Support

If you do not configure Gateway in the ADM console, the viewer will automatically choose to make a direct connection to the agent. In this case, the equipment must be reachable from the viewfinder in order to take remote control. The connection will not be encrypted via SSL

Remote Control Socket

Even when an outbound connection is made by the gateway, the functions of the ADM viewer remain the same. There is no change in this aspect



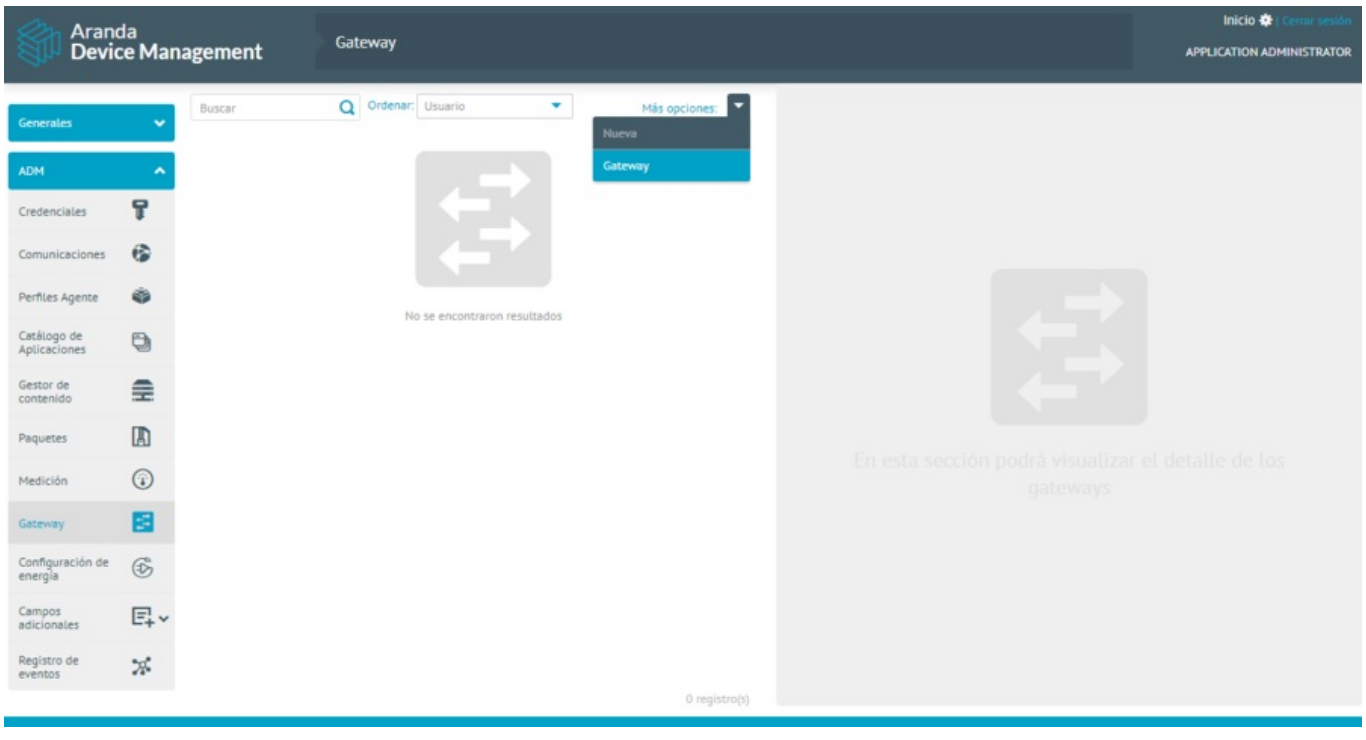
↩ Gateway Installer

ADM Web Console Gateway Configuration

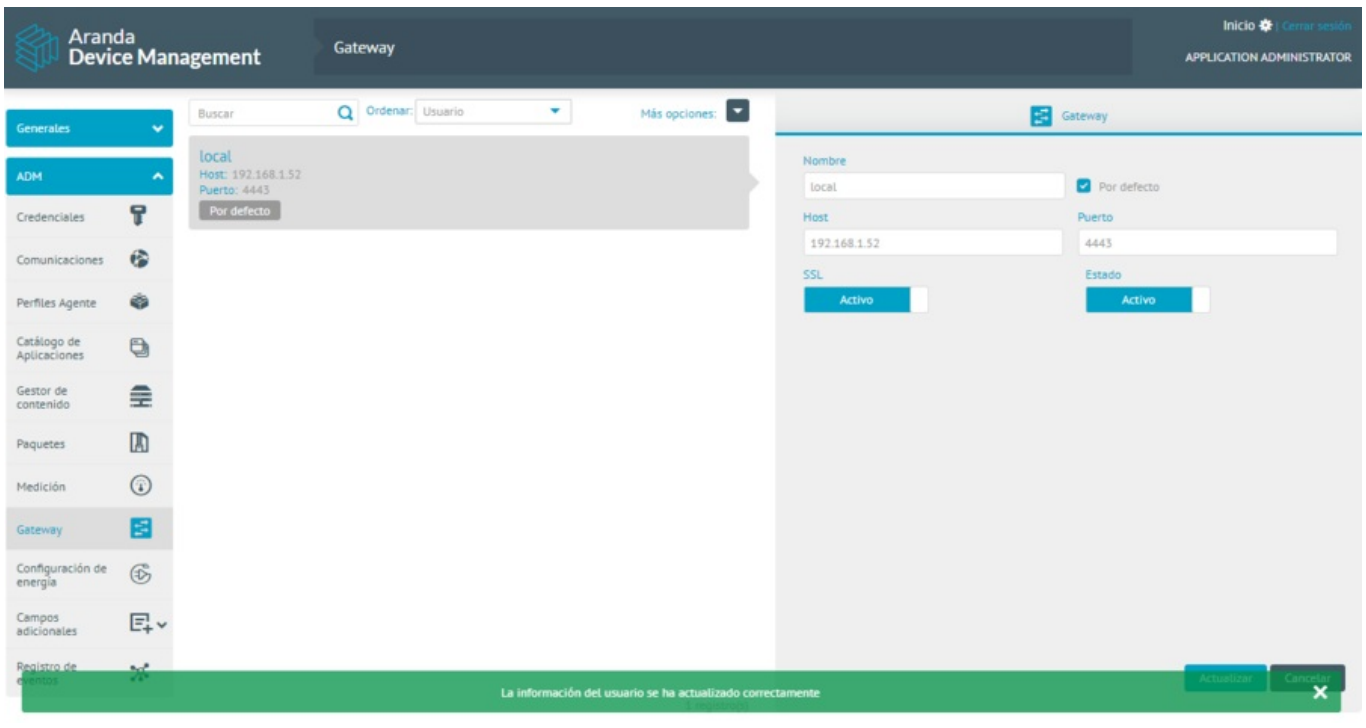
↩ Gateway Installer

Create Gateway

1. To configure the gateway, go to the ADM Management Console, in the ADM Configuration from the main menu, select the Gateway . In the information view, select More options and New Gateway.



2. In the detail view of the Gateway, enter the host values (it can be an IP address or a domain, without any schema, i.e. without http://, https://, etc.). The port. It must be the same as the one that was set on the Gateway. SSL should be the same value that was set on the gateway.



⚐ Note: It is possible to create more than one Gateway. The Gateway that is Active and marked as Default will be used.

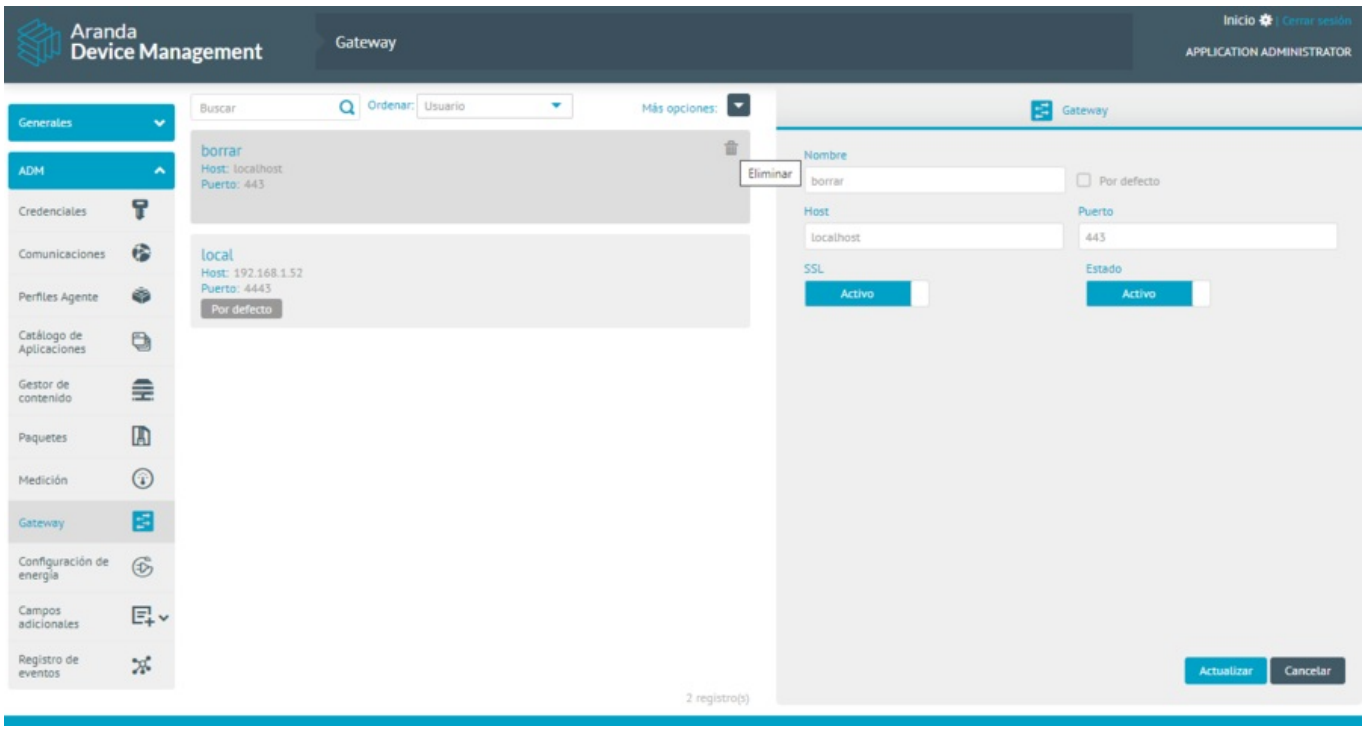
Edit Gateway

1. To edit a gateway, in the information view of the ADM web console, select a record from the existing gateway listing, in the detail view modify the required information (fields).

2. When you finish editing the Gateway, click Update to confirm the changes made.

Remove Gateway

1. To delete a gateway, in the information view, select one or more records from the list of existing gateways; In the Detail view, uncheck the option Default and click the Update.



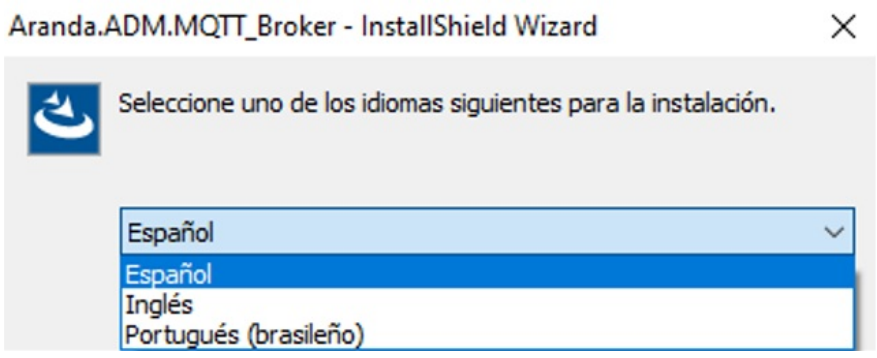
2. In the updated gateway information view, select the Eliminate to clear the associated information. ↩ Gateway Installer

Aranda MQTT Broker Installer

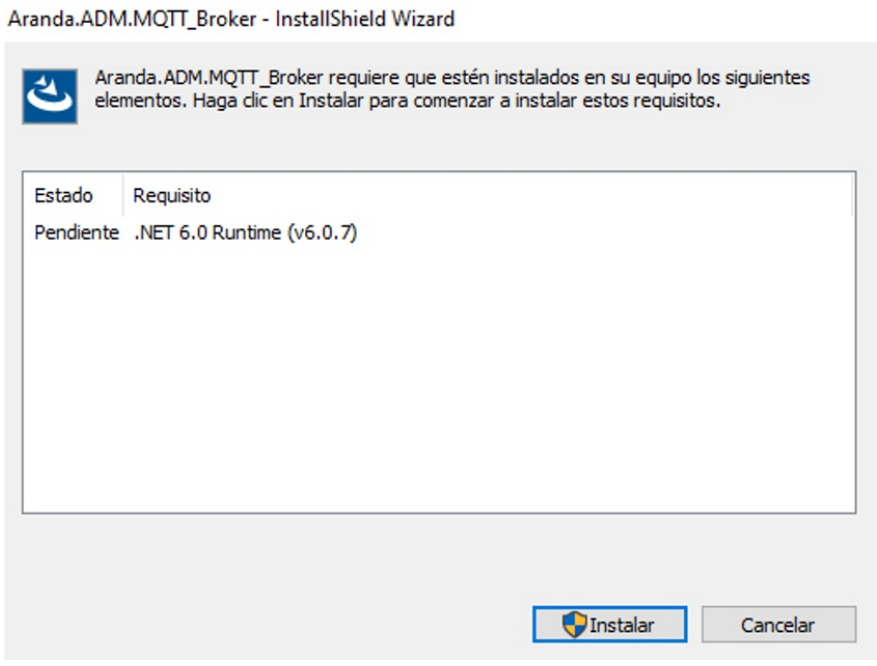
> ⚐ Note: A maximum number of 10,000 connections (devices) per MQTT broker server is suggested.

1. Run the installer Aranda.ADM.MQTT.Broker.exe

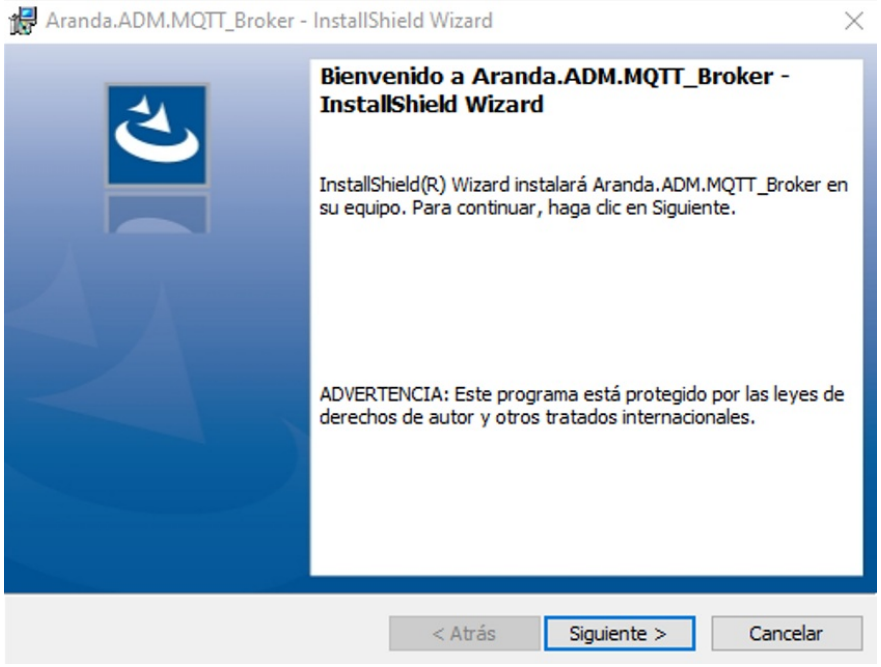
2. Define the language for the installation process.



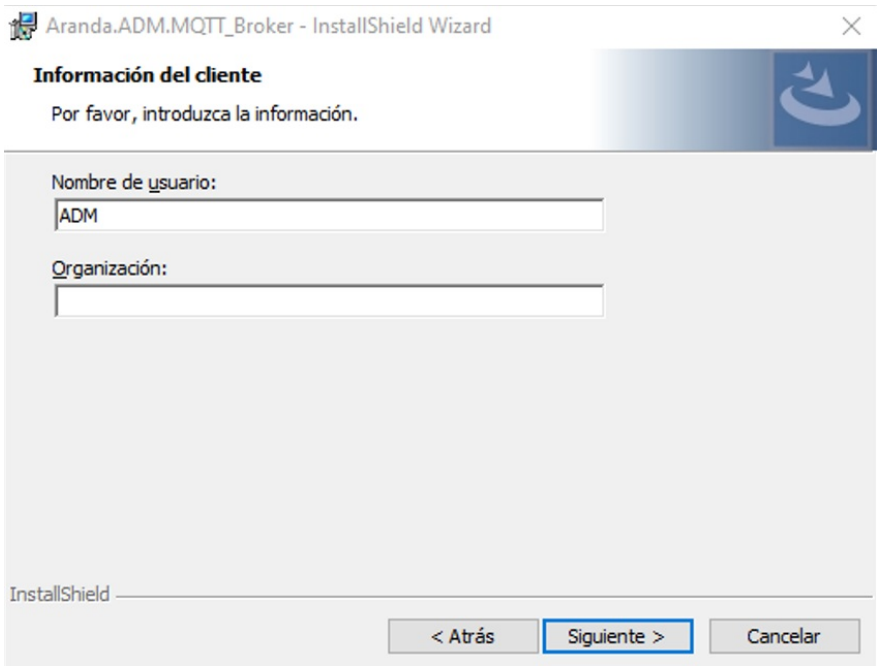
3. The installer validates the prerequisites that must be met to configure the Aranda broker. If this is not met, the system will install the required information.



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

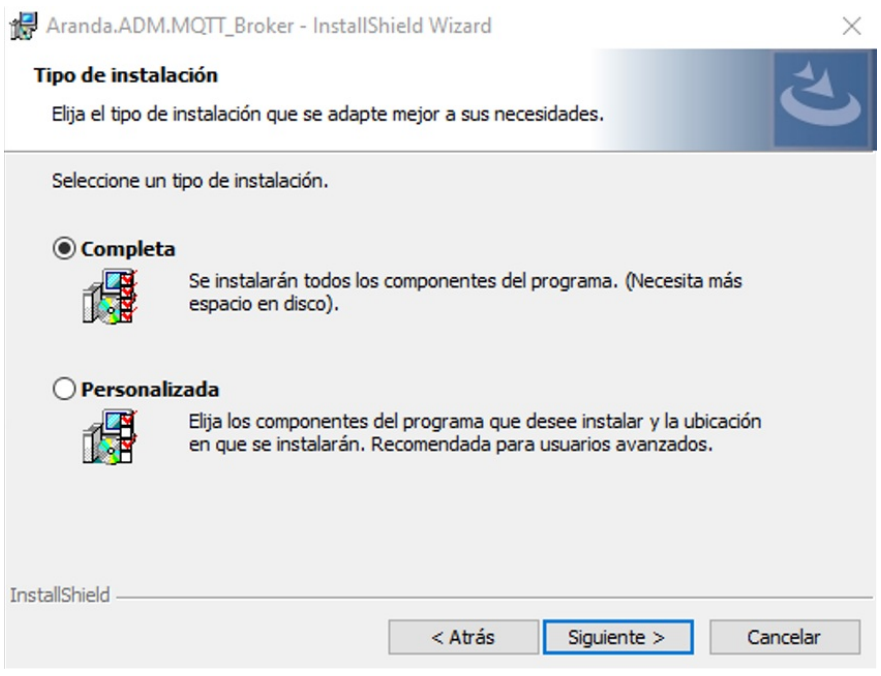


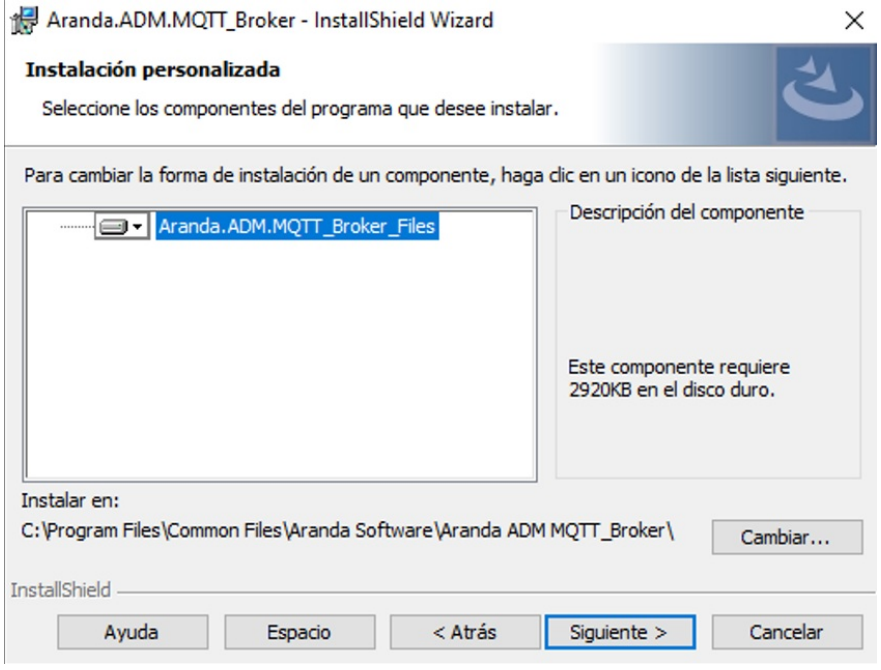
5. In the Customer Information window, enter the user name, organization, and click Following. These fields may be left empty.



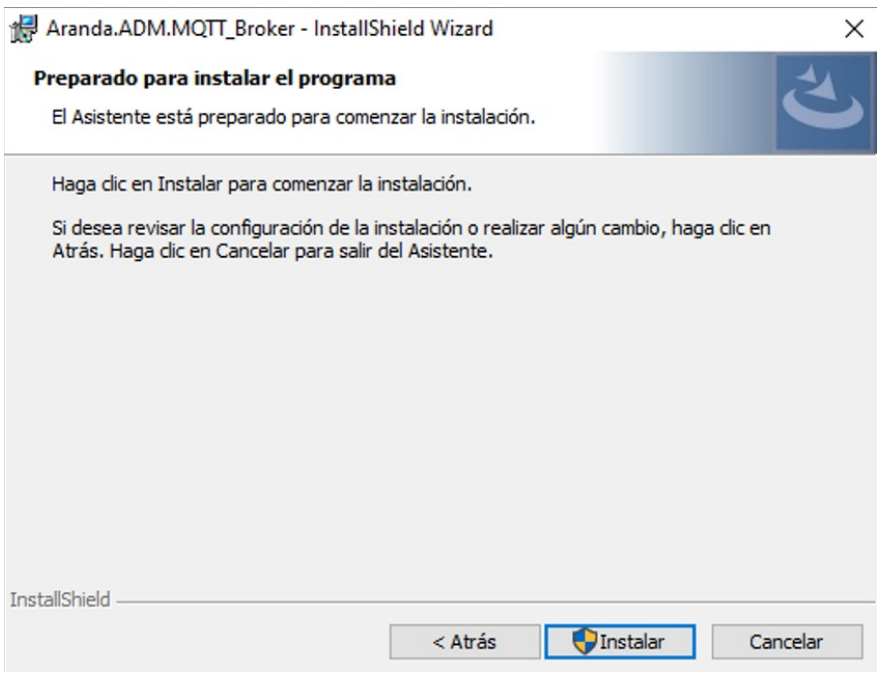
6. Define the type of installation, the options are:

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

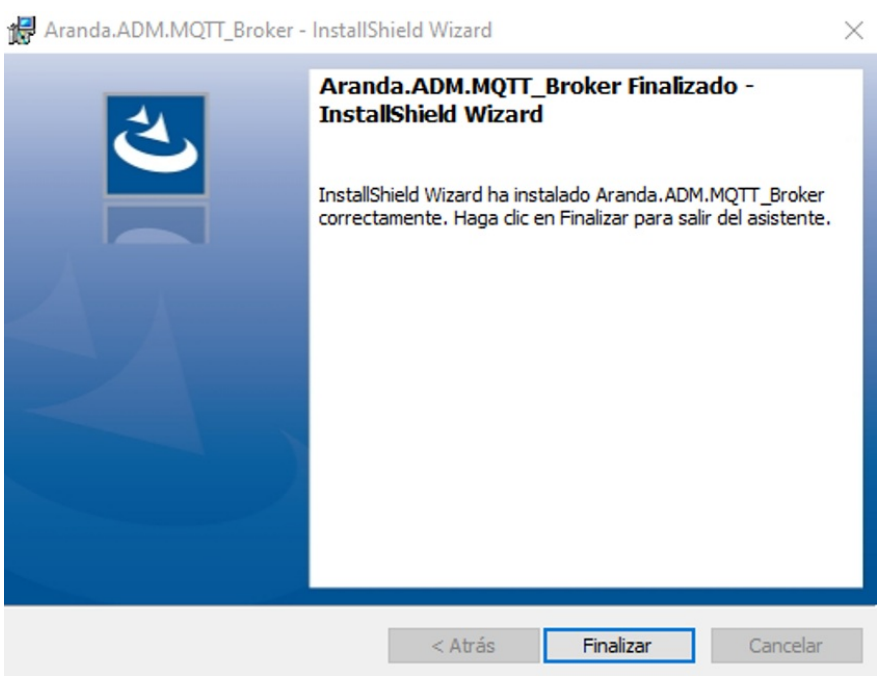




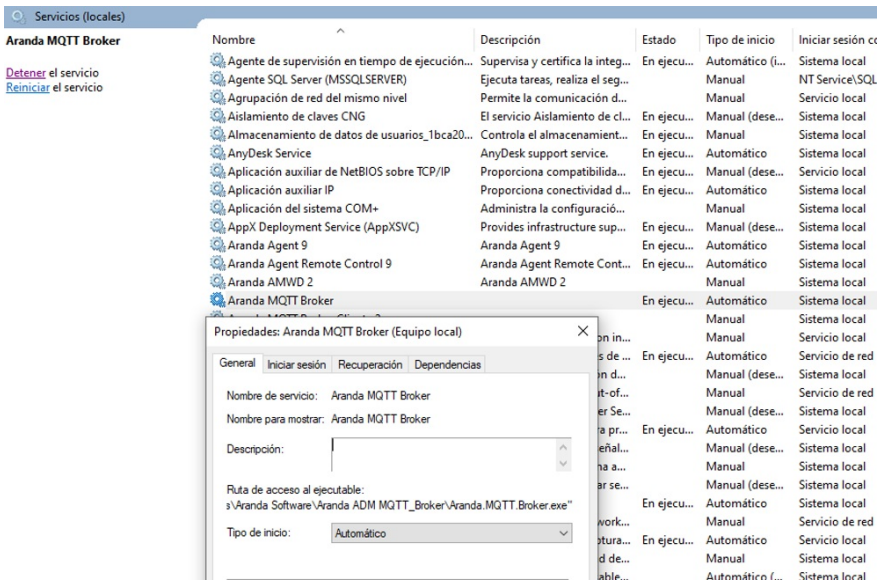
7. Once the Full or Custom installation is chosen, click Install, you must have permissions as a machine administrator.



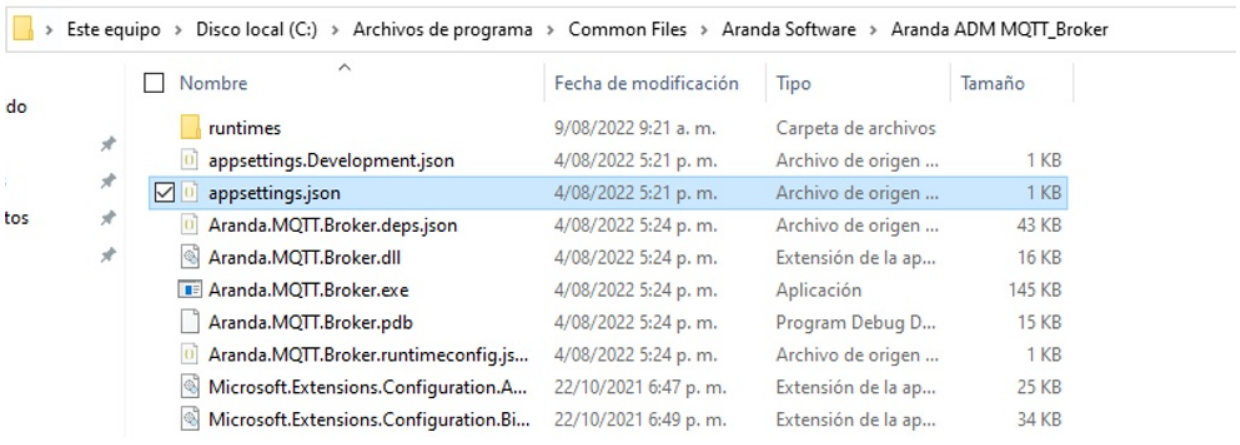
8. When the installation process is finished, click the End.



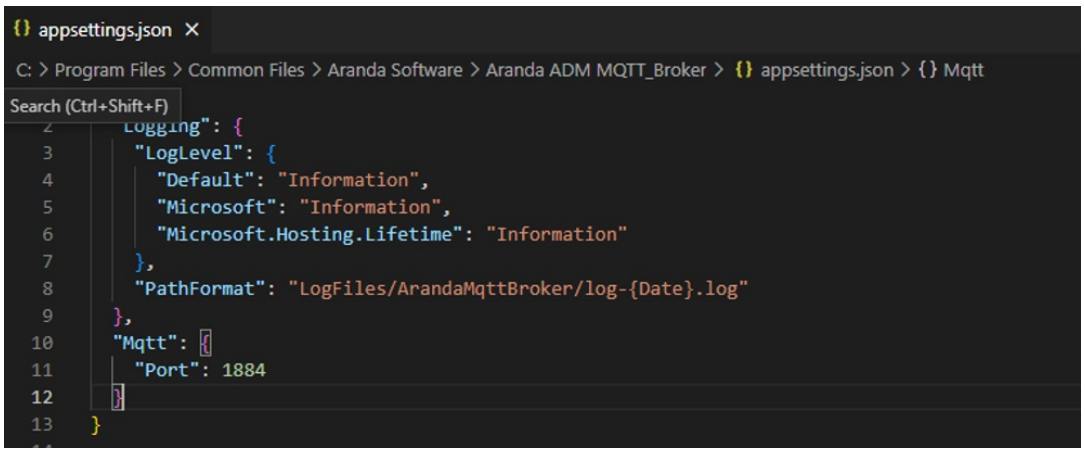
9. Once the installation process is finished, go to the services and verify that the service: Aranda MQTT Broker is installed and running.



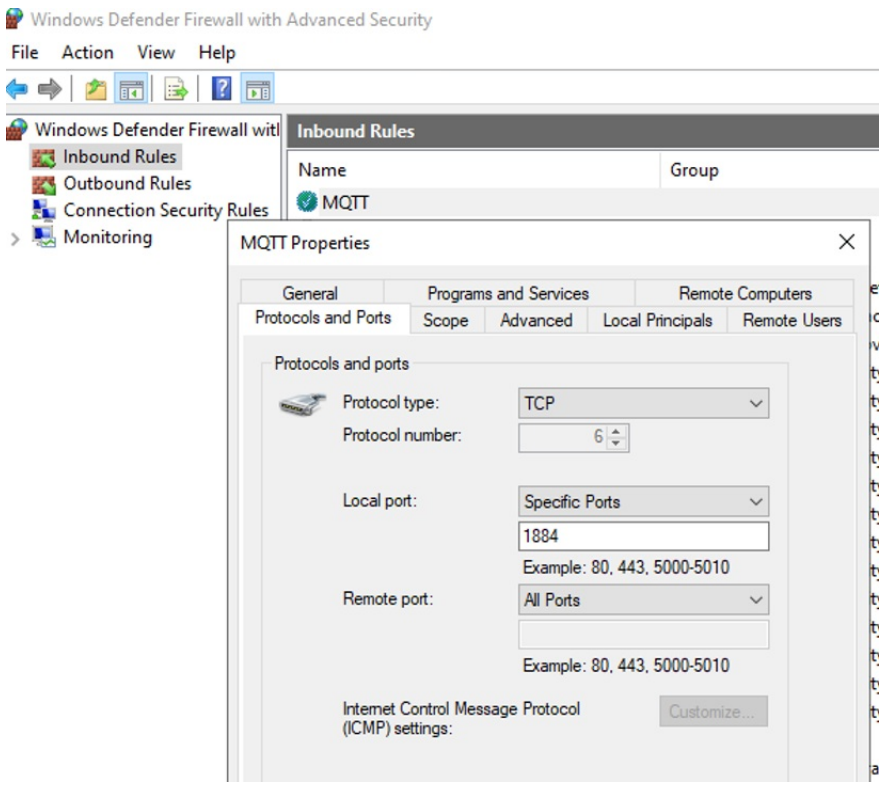
10. To configure the port you want to expose, open the appsettings.json in the folder where the service is installed, and do the following:



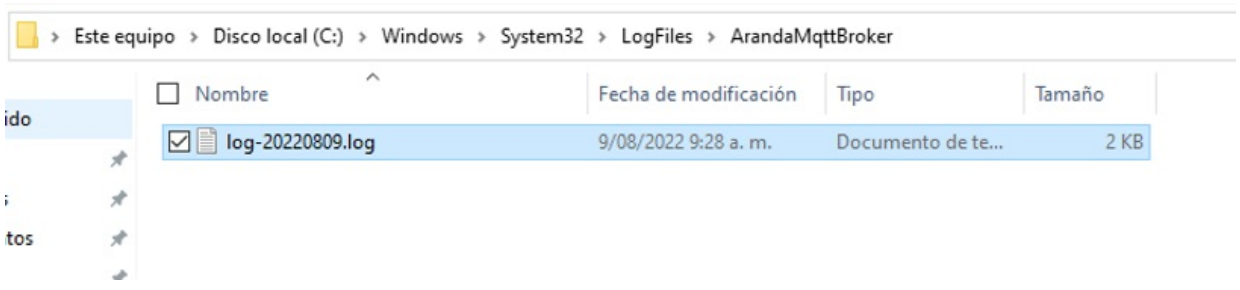
11. Modify the section Mqtt:Port to change the port and restart the service to apply the changes.



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.



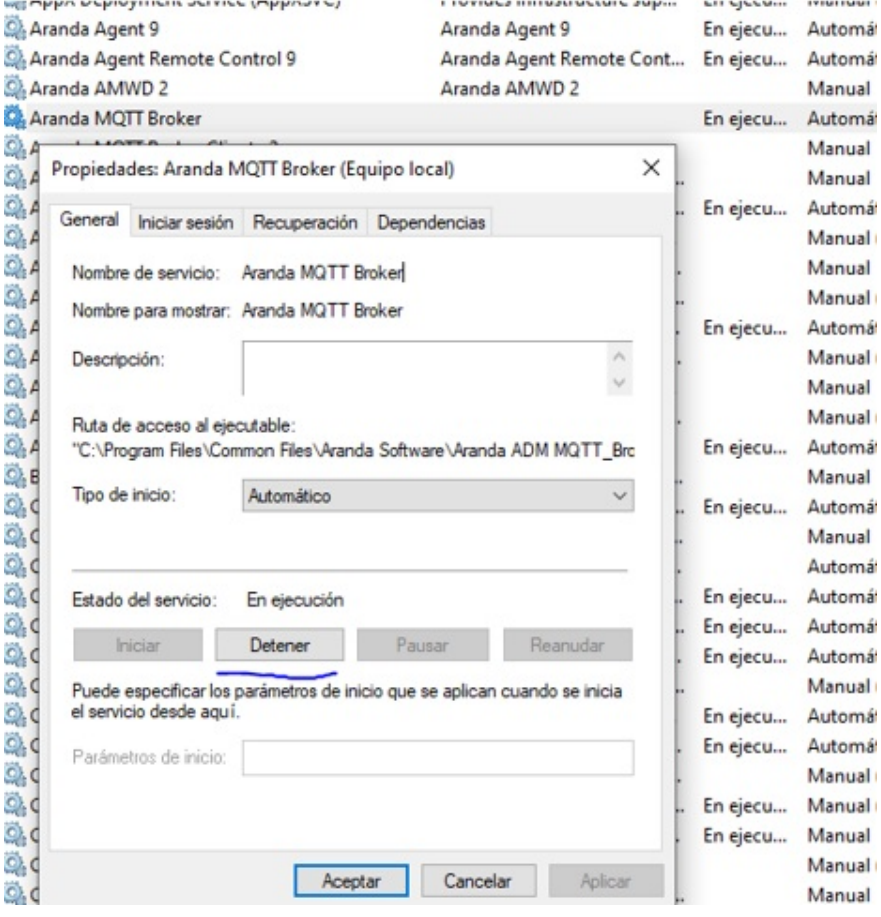
13.The archives of Log will be stored in the following path: C:/Windows/System32/LogFiles/ArandaMqttBroker



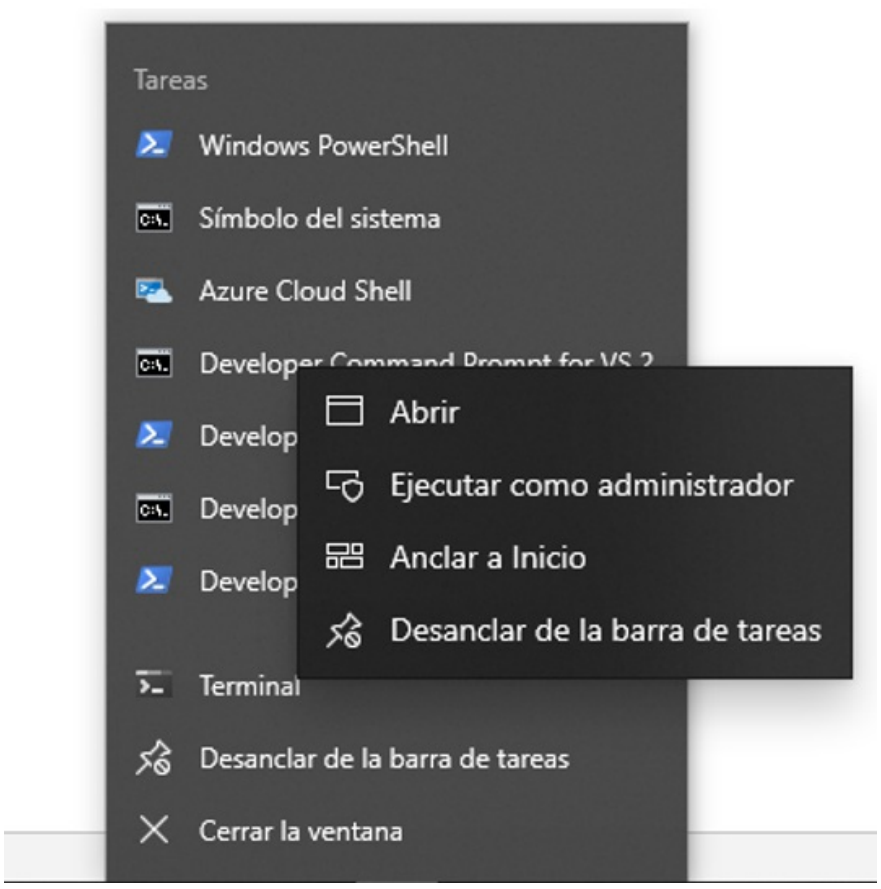
—

Uninstalling MQTT Broker

1. Open the Aranda MQTT Broker file, the Properties window is enabled, and in the General, 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.

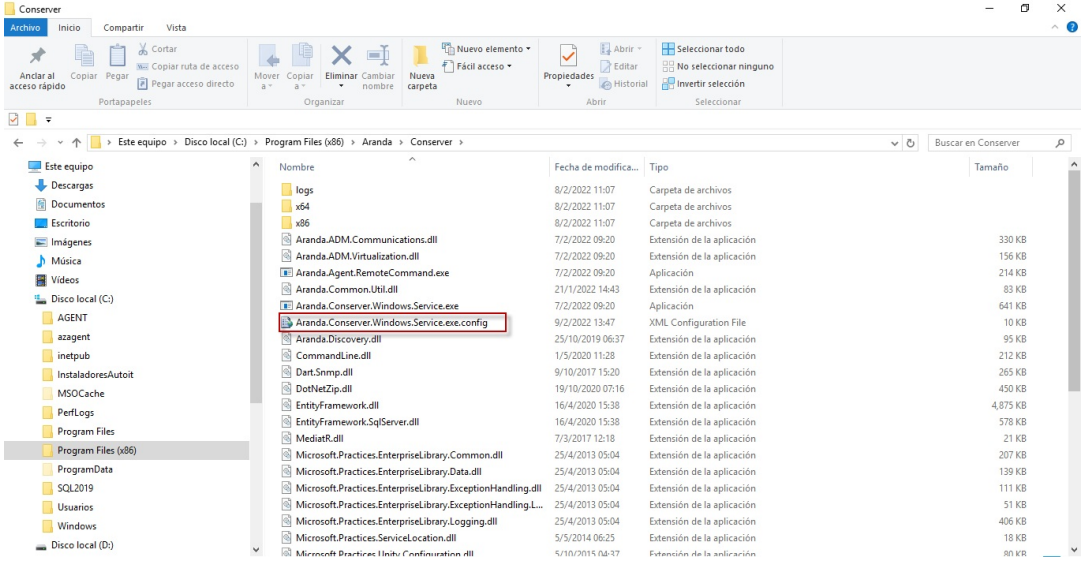
— Related Links:
- Broker Configuration

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"



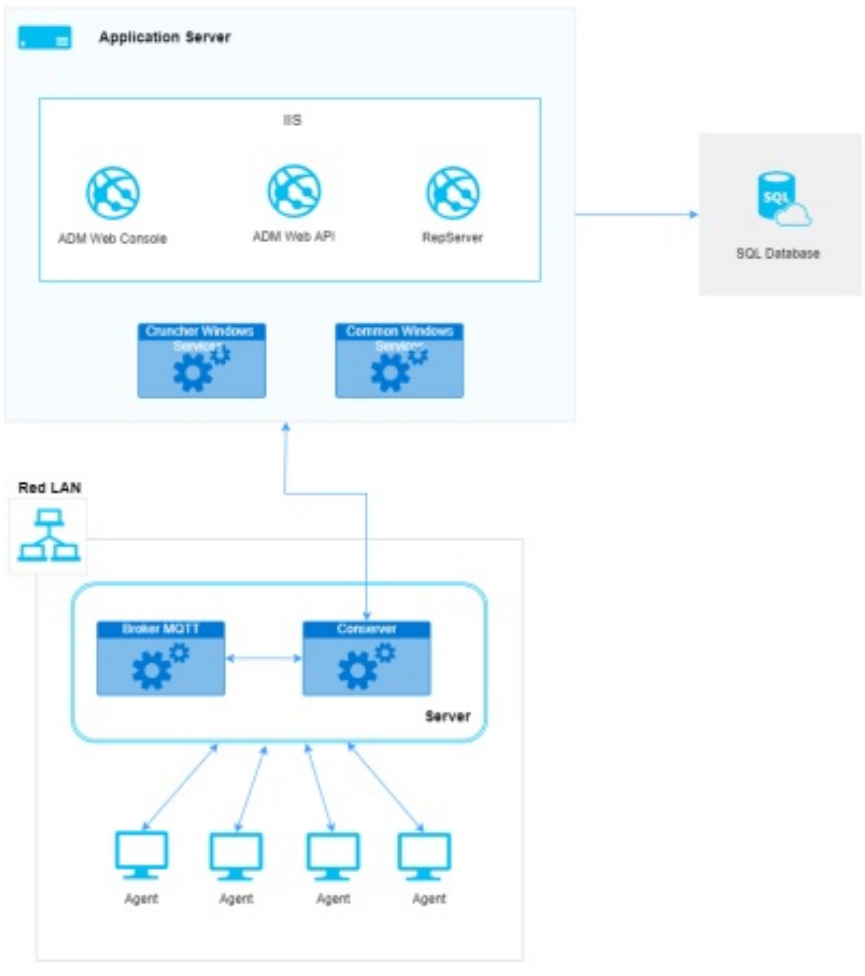
2. Create the following values based on the parameterized port and the IP of the server where the broker is installed.

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

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

}
```

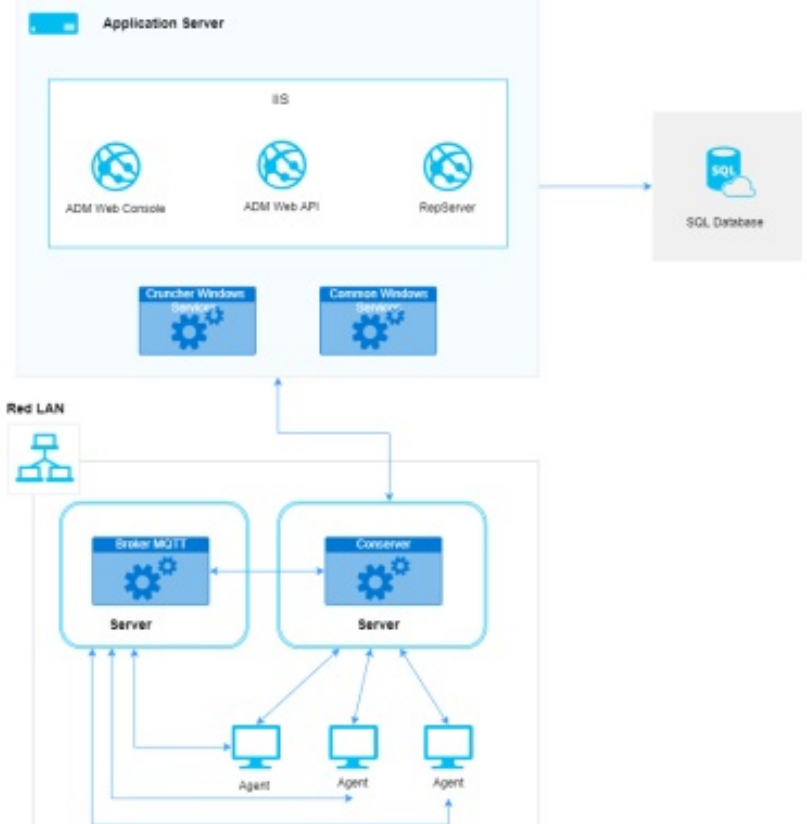
⚐ Note: When you make a modification to the conserver configuration file, you must restart the service.

Topologies supported in ADM with conserver broker division

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

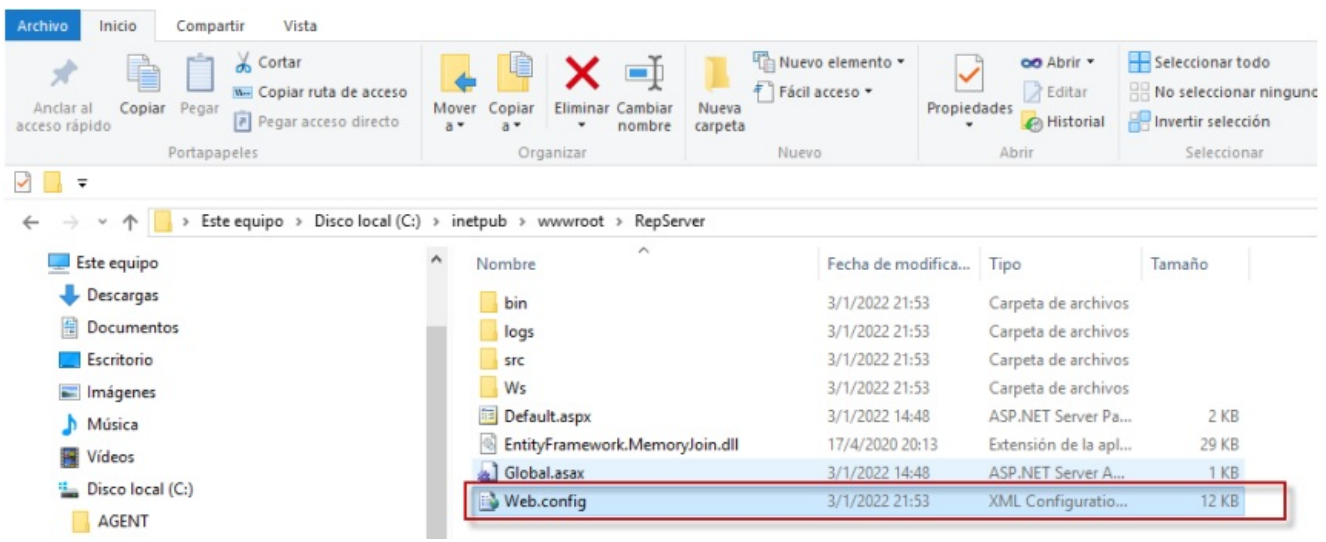


- Configuring the broker on different server of the conserver



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'.



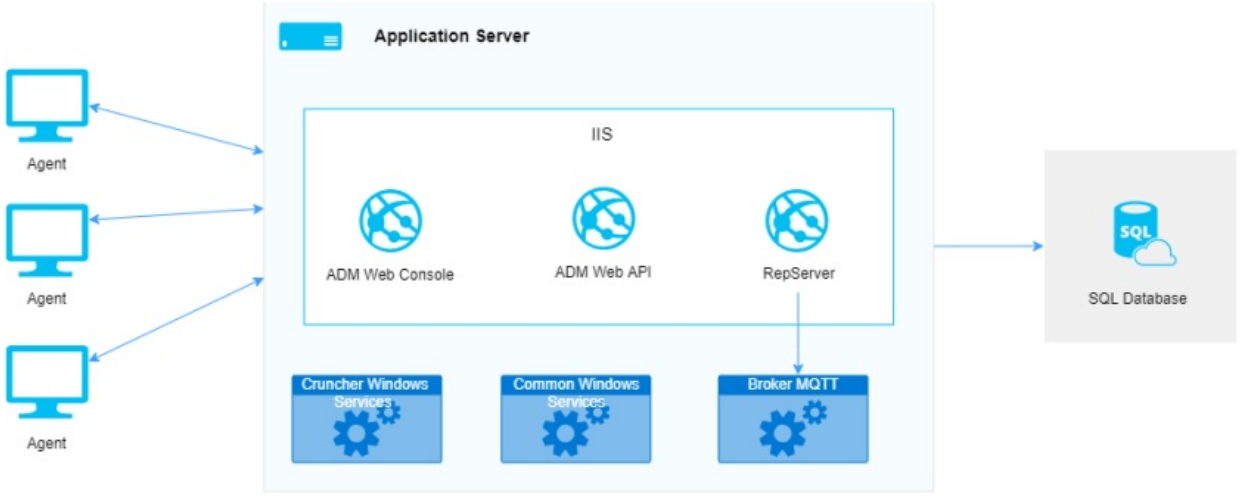
2. Add the following values in < appSettings > based on the parameterized port and host of the server where the broker is installed.

```
{
<add key="mqttServerPort" value="1884"/>
<add key="mqttIp" value="192.168.X.XXX"/>
}
```

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



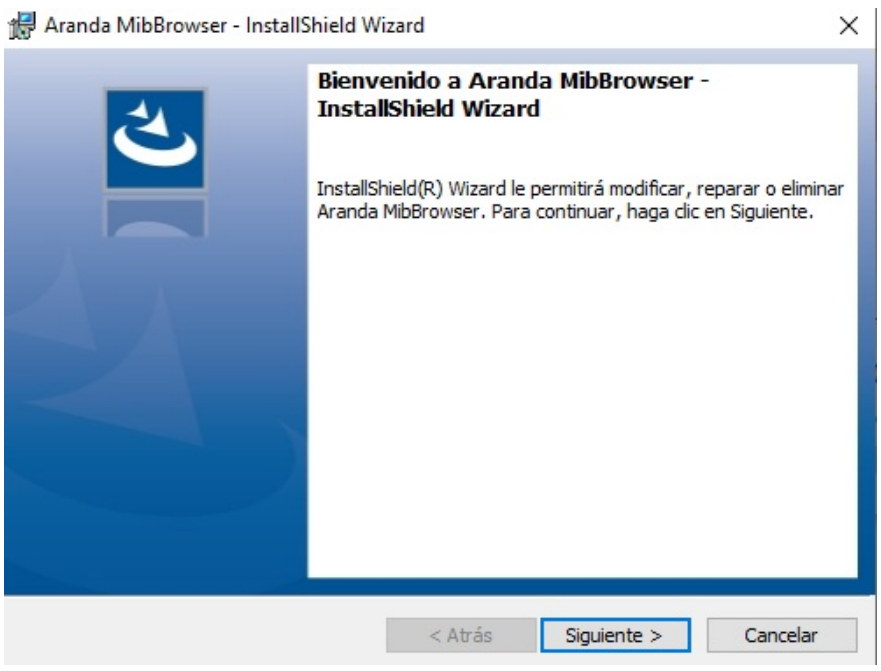
⚐ Note: The broker may or may not be within the same server as the repserver.

↩ Aranda MQTT Broker Installer

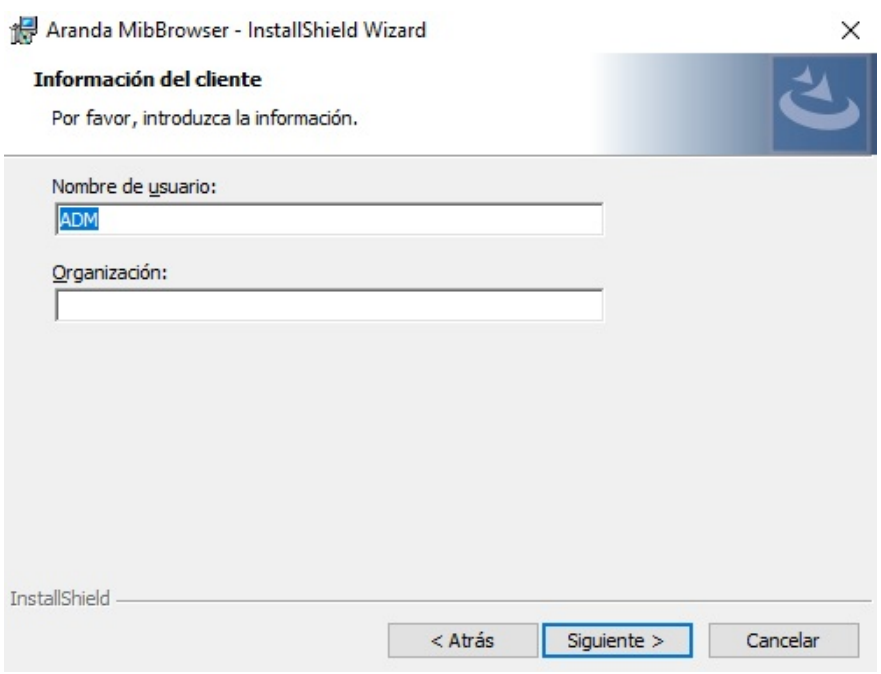
MibBrowser Settings

Aranda MibBrowser Installer

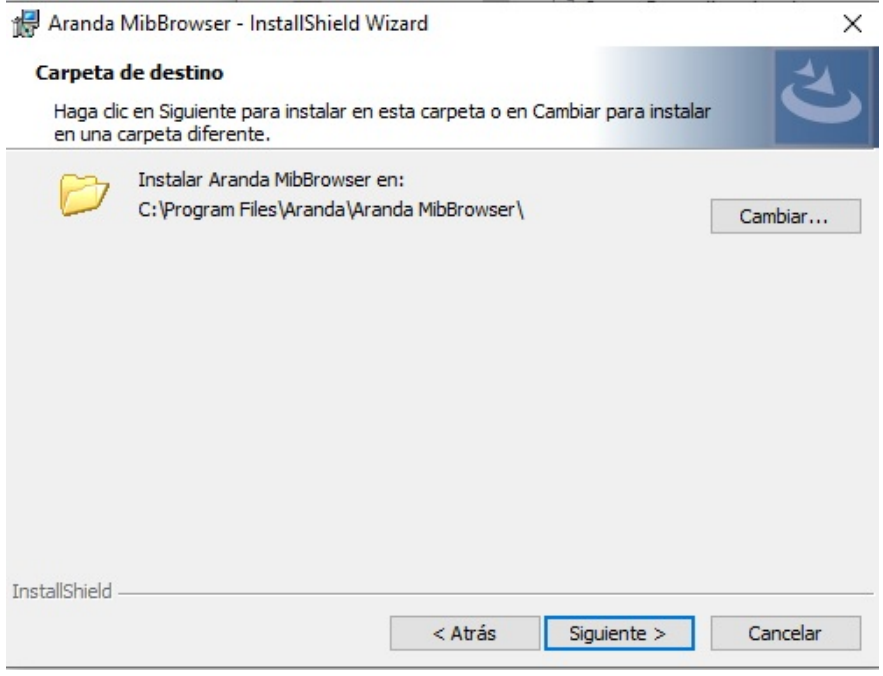
1. Run the installer Aranda.MibBrowser.exe



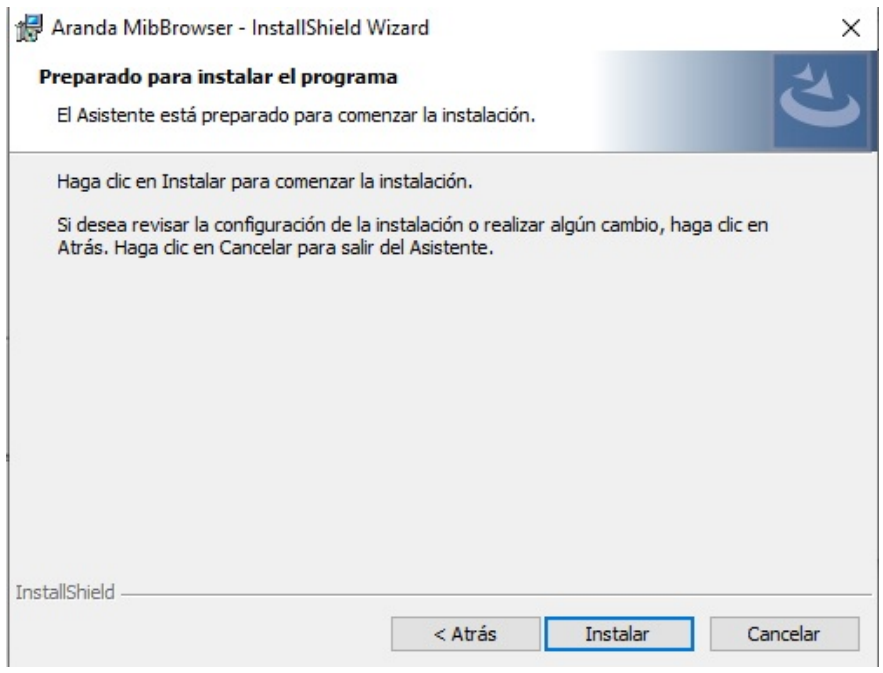
2. You can define the username or organization and click Following. These fields may be left empty.



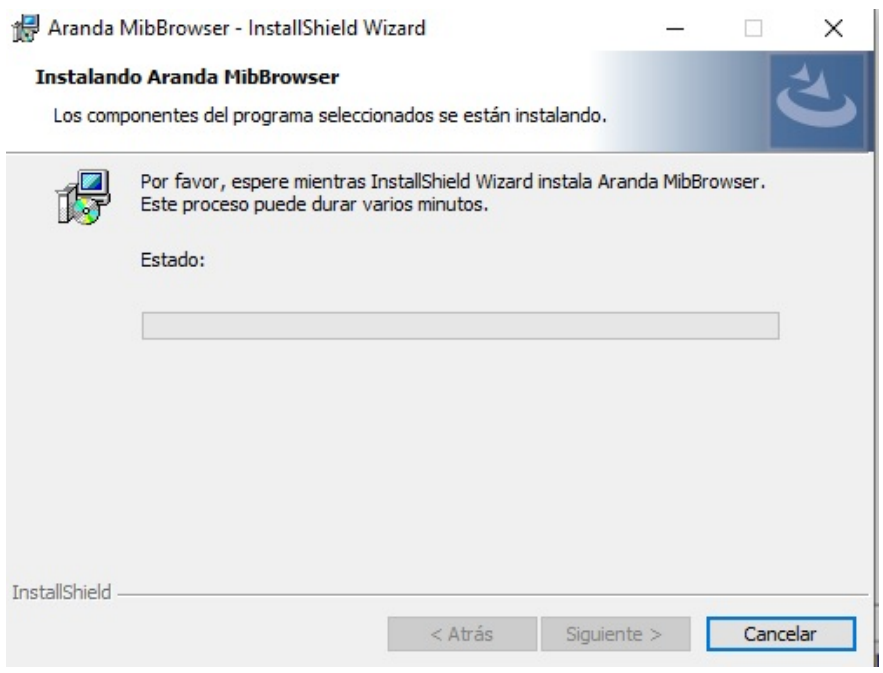
3. The installer selects a location for installation or you can change it, then click Following.



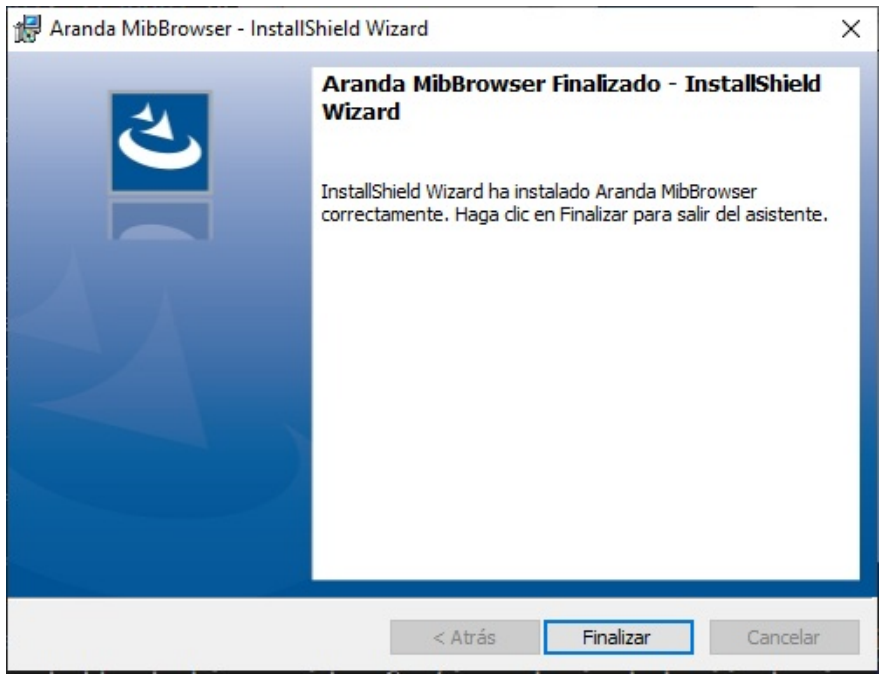
4. Then we proceed to the installation, click on Install.



5. Wait while the installer finishes the process.



6. Confirm the installation by clicking the End.



—

Related Links:
- MibBrowser Utility

MibBrowser Settings

↩ Aranda MibBrowser Installer

El MibBrowser permite compilar MIB(Management Information Base) los cuales contienen información sobre los OIDs(Object Identifiers) que se pueden consultar usando el protocolo SNMP(Simple Network Management Protocol) acerca de un dispositivo por ejemplo un router,switch o impresora etc.

When the application is launched, the following sections can be identified

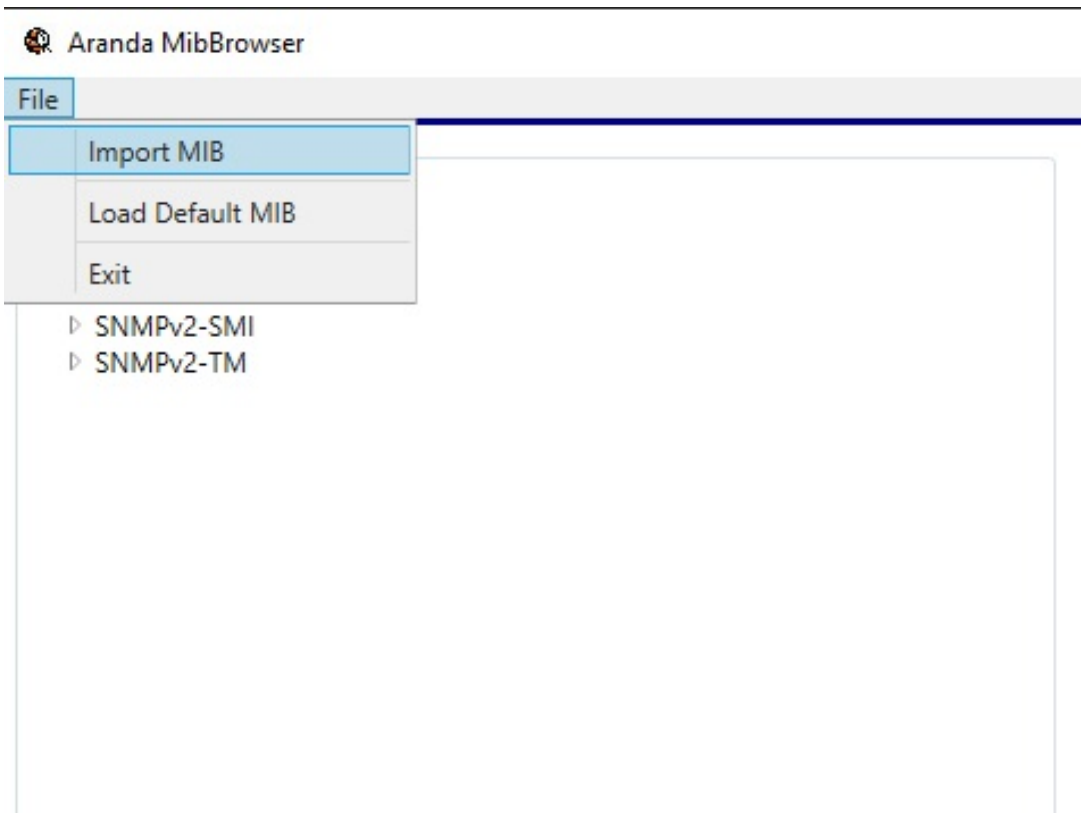
1. Mibs
2. ObjectIdentifier
3. Settings
4. Oid-Value

```
<center><img src="/adm-install/en/assets/images/02-instalacion/08-mib_browser/caso_uso_mib_browser_0.png" style="width:700px;"></center>
```

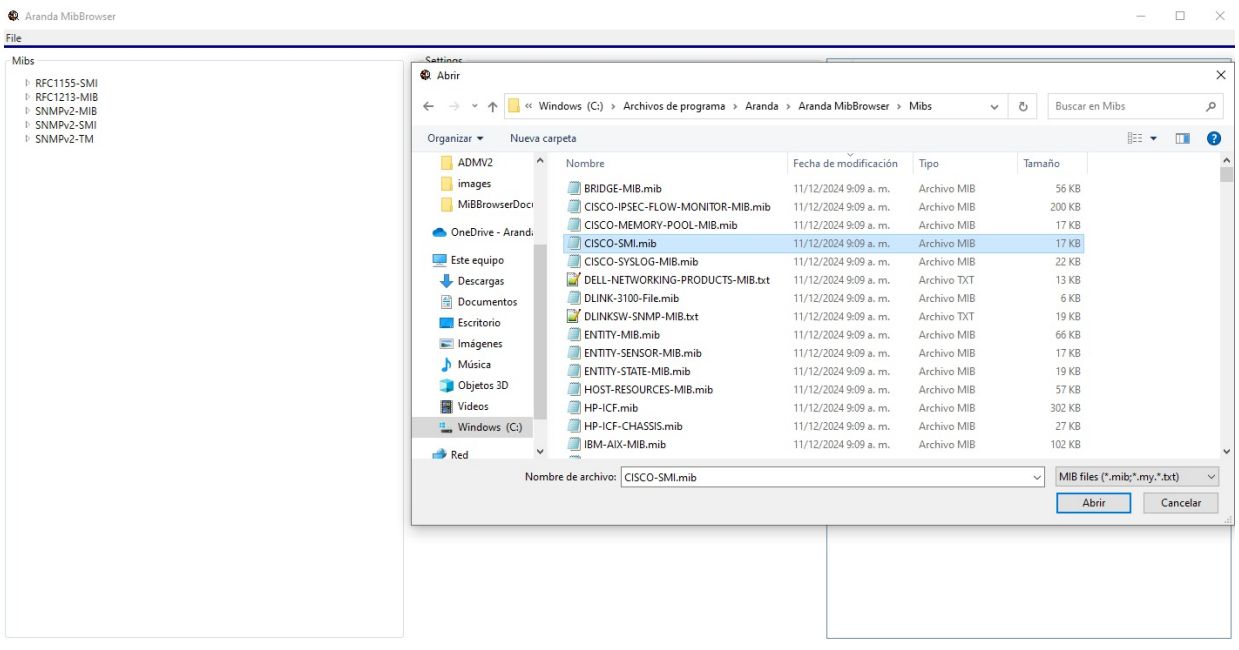
1. The MIBs initially compiled are the following MIBs:

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

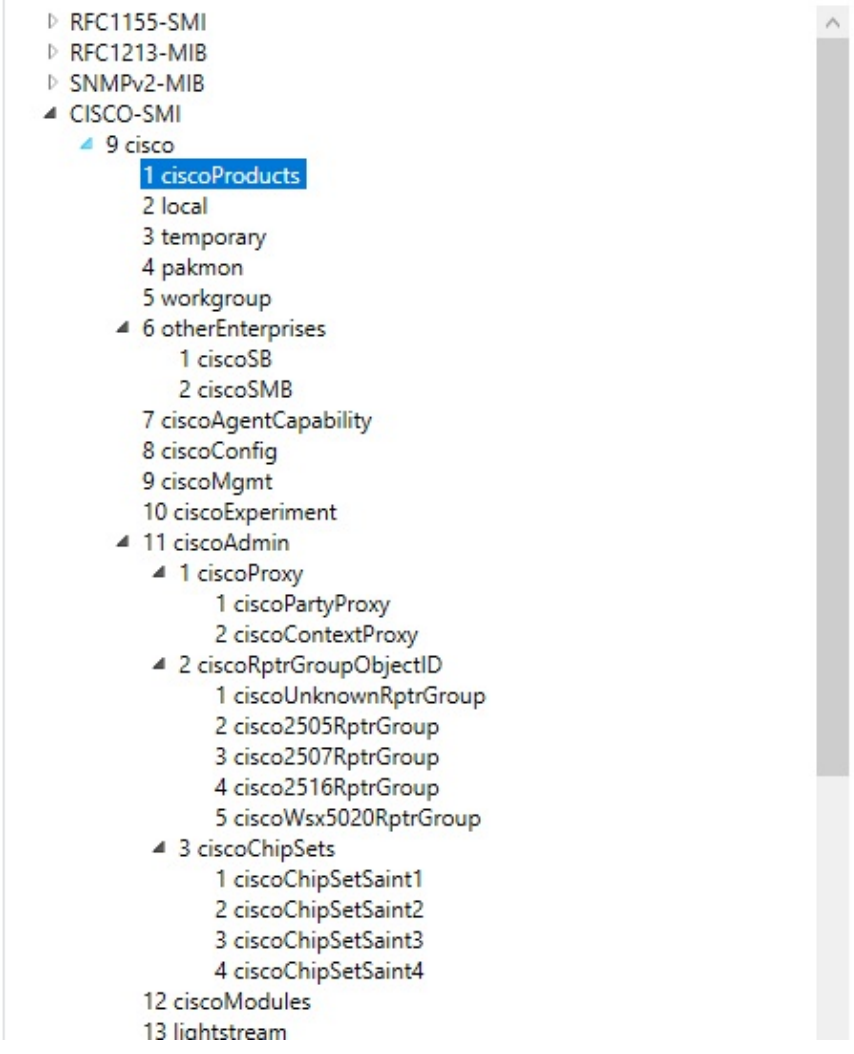
If you want to compile another MIB you can do so via the menu option



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.

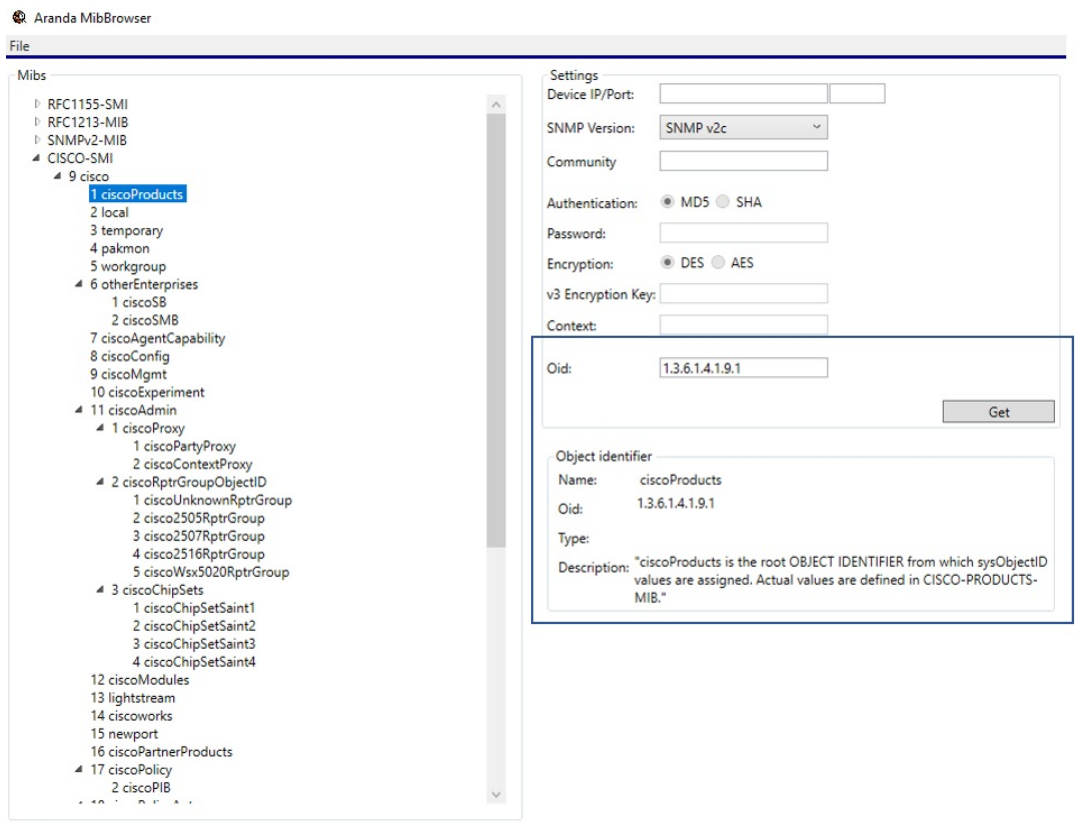


We consult the MIBS tree

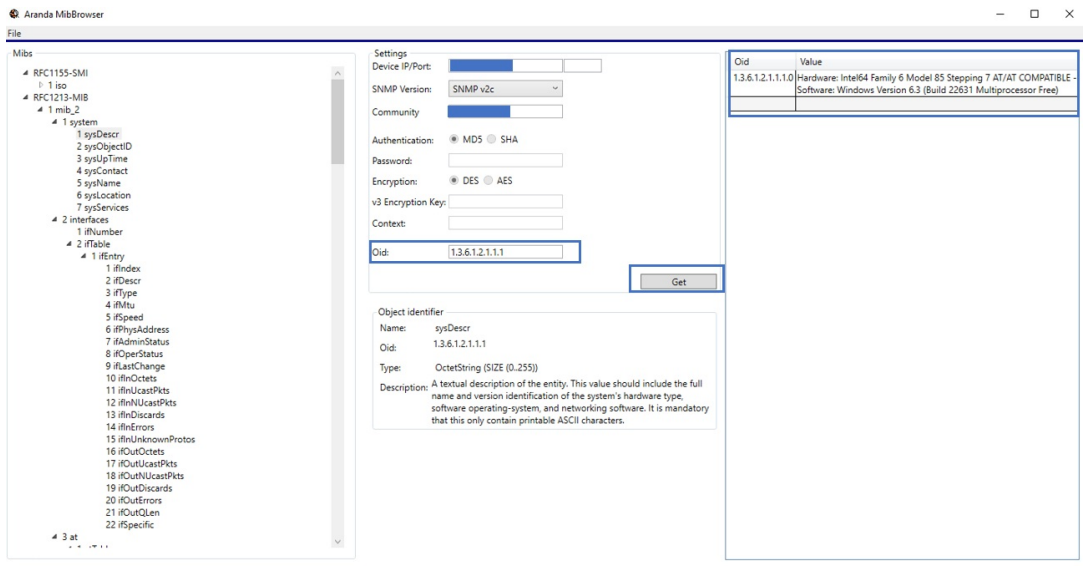


⚐ Note: A MIB usually has dependencies which it is recommended to upload it to its main MIB or manually copy it to the MIB. MibBrowser installation directory in the folder MIBS, since it is the path where the application consults to try to resolve dependencies automatically.

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

ADM Structures

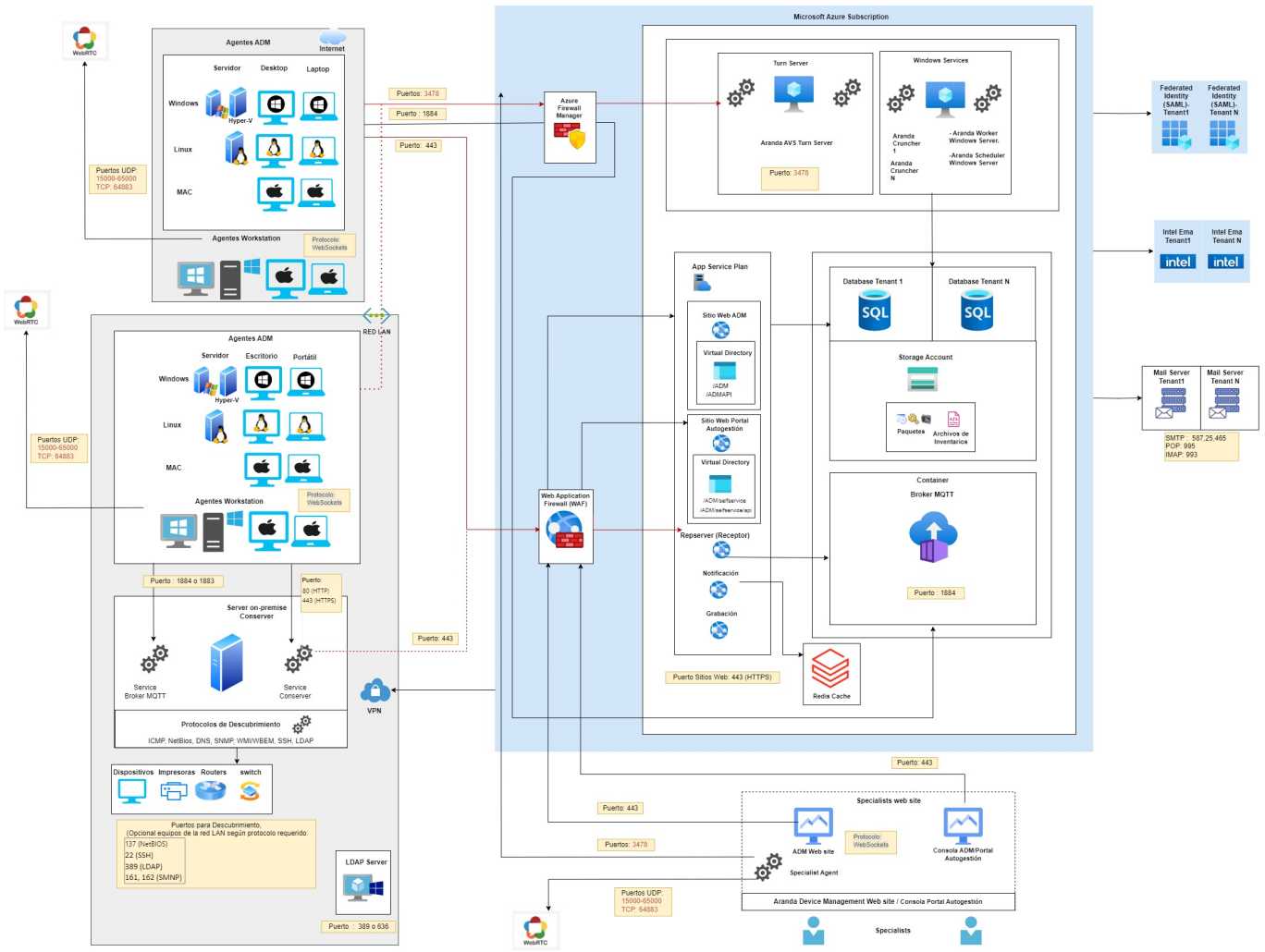
Structures and Components

To view the Ports and iteration with the components you can check the following links.

- Cloud with Conserver Onpremises ↪
- Cloud without a server↪
- Onpremises↪

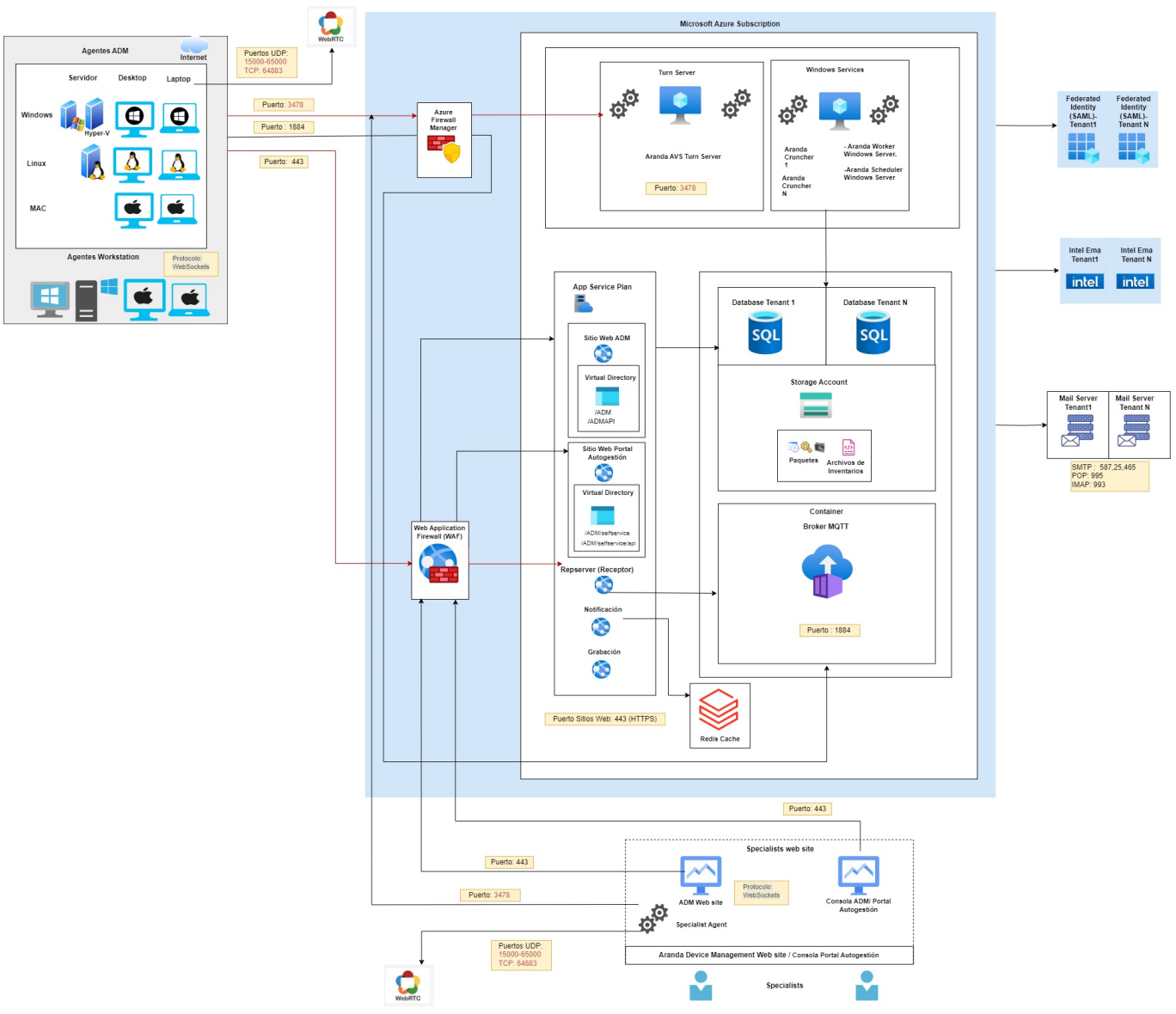
Cloud con conserver onpremises

↩ ADM Structures and Components



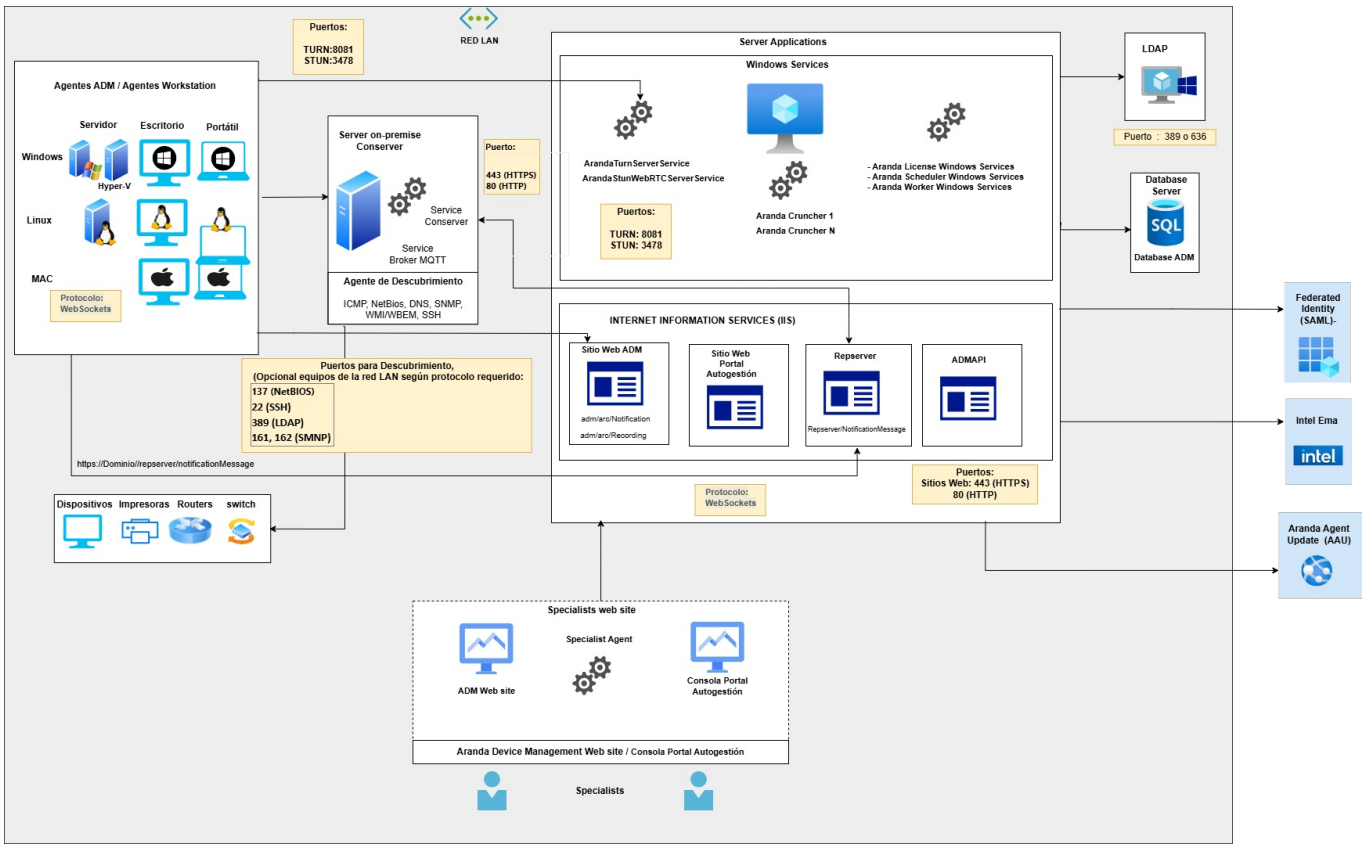
Unpreserved cloud

↩ ADM Structures and Components



Onpremise

↩ ADM Structures and Components

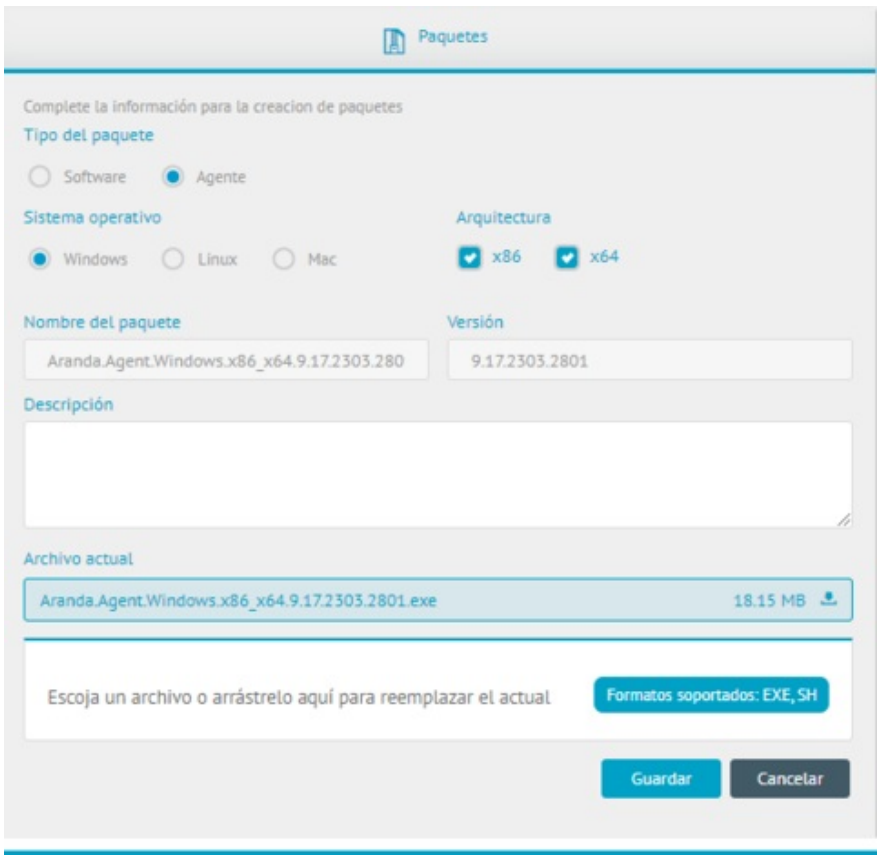


Update

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.

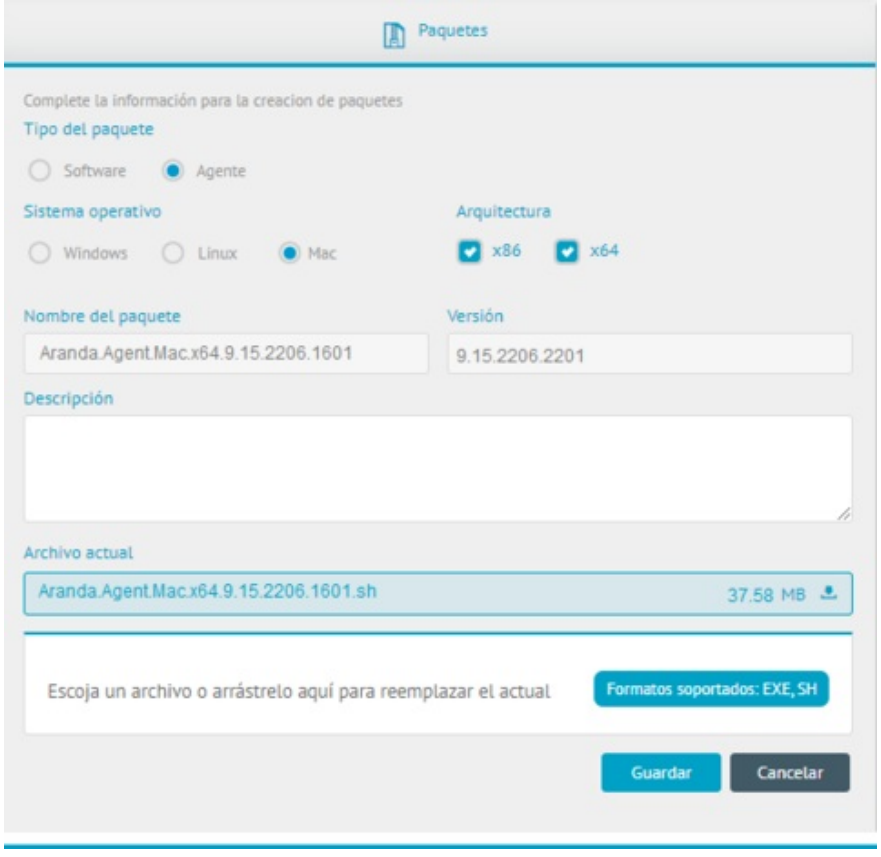


⚐ Note: After 8 hours, the ADM agent will attempt to update to the latest version published in the console. If you want to force the update, from the list of devices, you can execute the Update Agent

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.



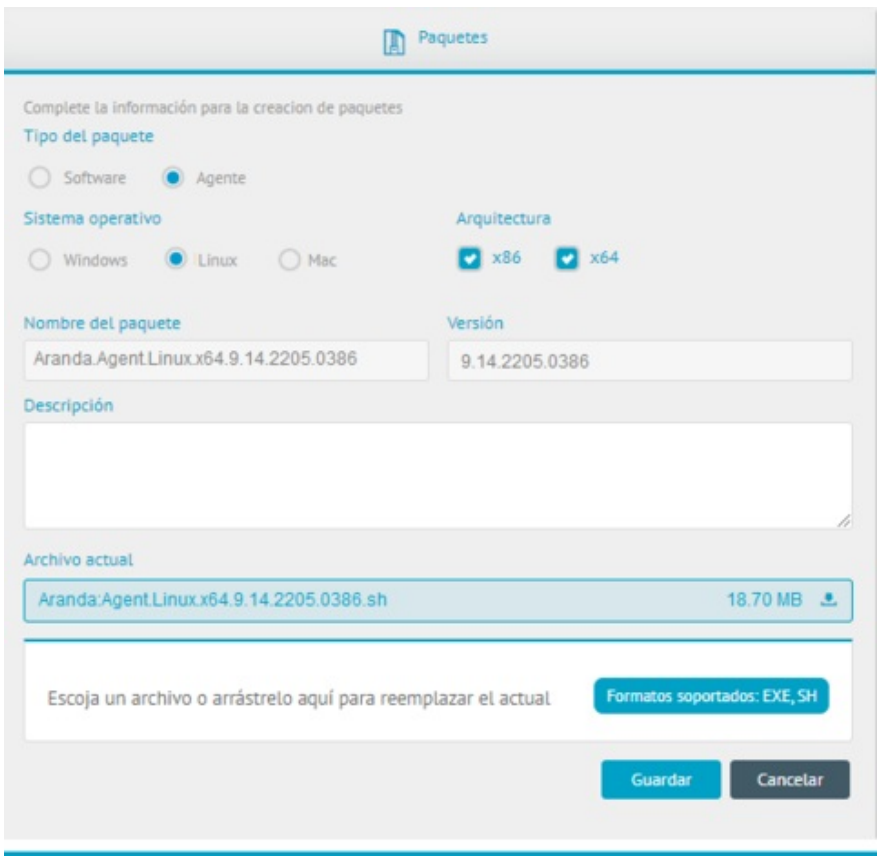
2. When the agent finishes loading, click Save

⚐ Note: After 8 hours, the ADM agent will attempt to update to the latest version published in the console. If you want to force the update, from the list of devices, you can execute the Update Agent

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.



⚐ Note: After 8 hours, the ADM agent will attempt to update to the latest version published in the console. If you want to force the update, from the list of devices, you can execute the Update Agent

Manual Upgrade of the Shelf

1. Stop the Aranda Conserver V9 service.

2. Uninstall the Conserver Service program from the control panel.

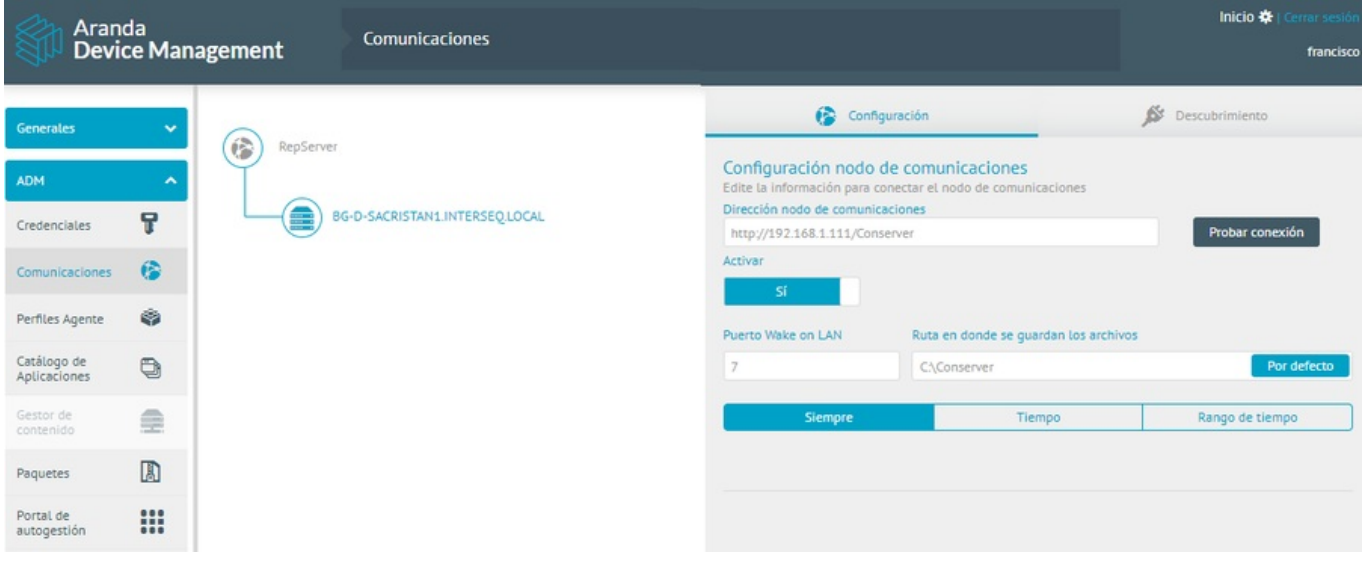
3. Delete the record from the following folder:

- 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



⚐ 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 ↪

Upgrading 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>
      </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>
```

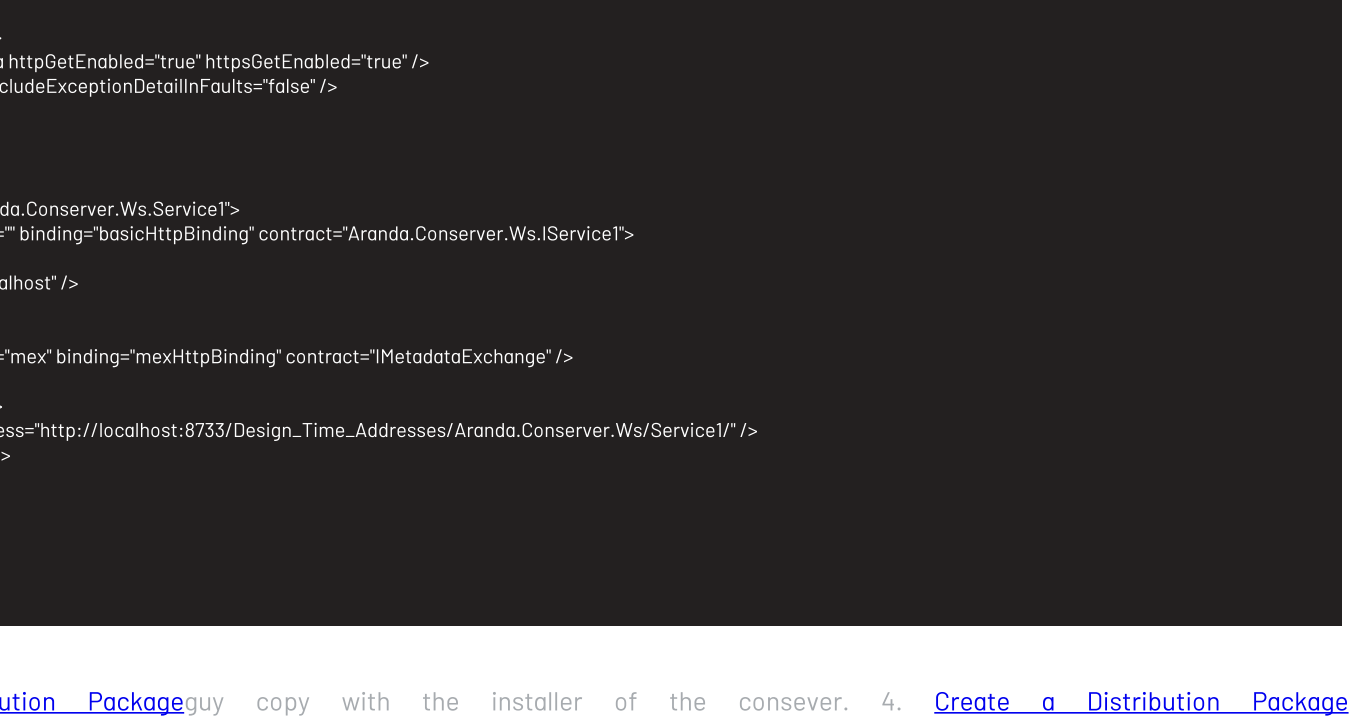
3. Create a Distribution Packageguy copy with the installer of the consever. 4. Create a Distribution Package guy copy with the Aranda.Conserver.Windows.Service.exe.config created in steps 3 and 4.

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 .batone .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.
—

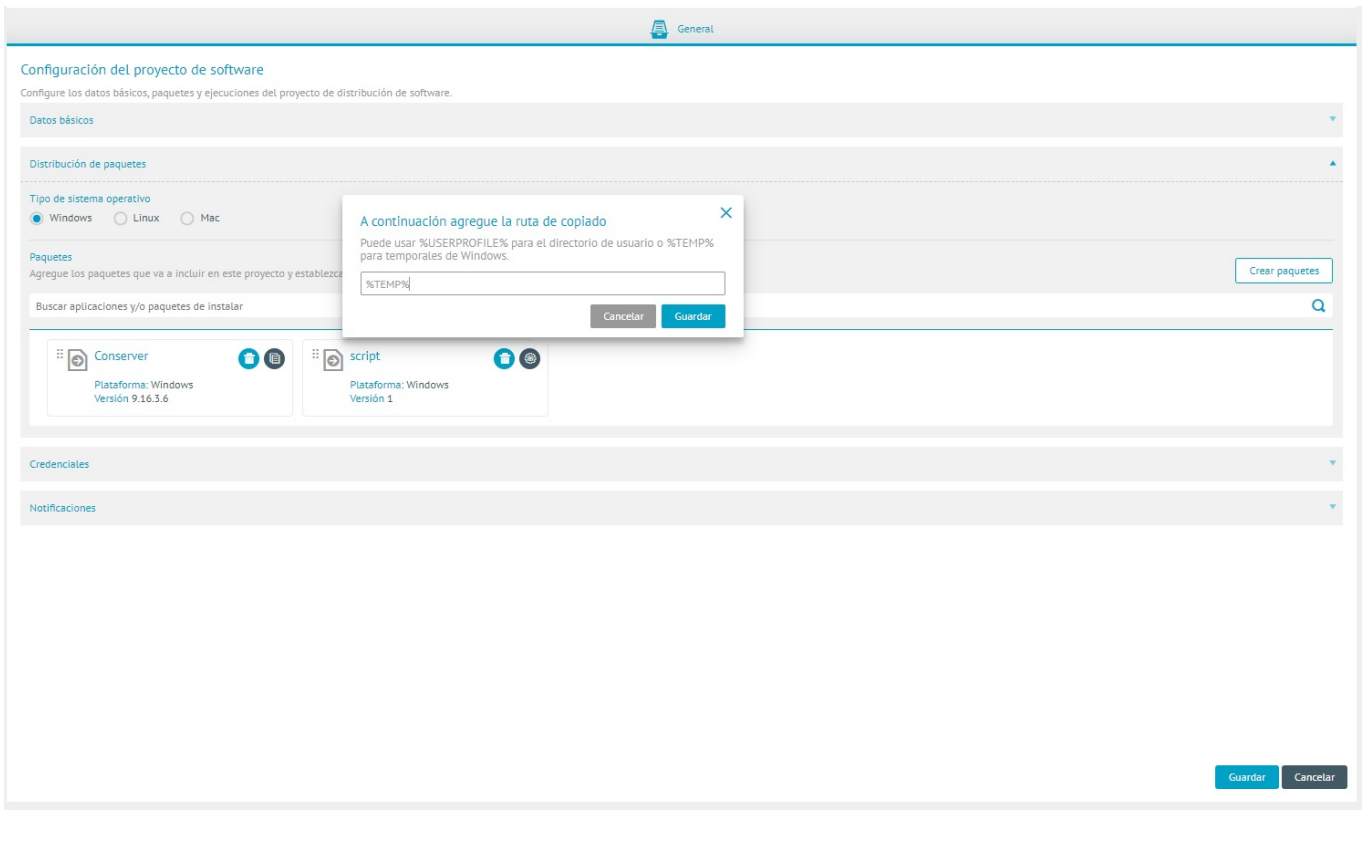
Upgrading from versions after 9.17

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 conserver SET 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 consever.

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]