Aranda Device Management

ADM es una solución que gestiona los activos informáticos de hardware y software de la organización, efectuando tareas de monitoreo y control remoto. A partir del conocimiento de inventarios puede distribuir y mantener actualizado el software en los dispositivos alcanzados.

El conocimiento y acceso a las etapas de instalación y actualización de ADM, le permite al usuario definir y configurar los componentes necesarios para el funcionamiento de la aplicación. Los lineamientos a tener en cuenta son:

1. Ruta de Instalación y Acceso

Conozca los requerimientos básicos para el funcionamiento correcto de la aplicación, siga el proceso de instalación de ADM de los diferentes componentes para su adecuado funcionamiento y acceda a la interfaz del producto para la gestión y control de los dispositivos descubiertos.

2. Actualización

Identifique cómo realizar las actualizaciones de los componentes de la funcionalidad, como el agente, el conserver y el visor de soporte remoto.

3. Estructuras

Conozca los componentes de la estructura de ADM e identifique cómo se relacionan en el funcionamiento general del producto.

¿Para quién es esta guía?

Esta guía está diseñada para ofrecer al usuario una ruta segura del proceso de instalación, configuración y actualización de ADM.

¿Cuál es nuestra documentación?

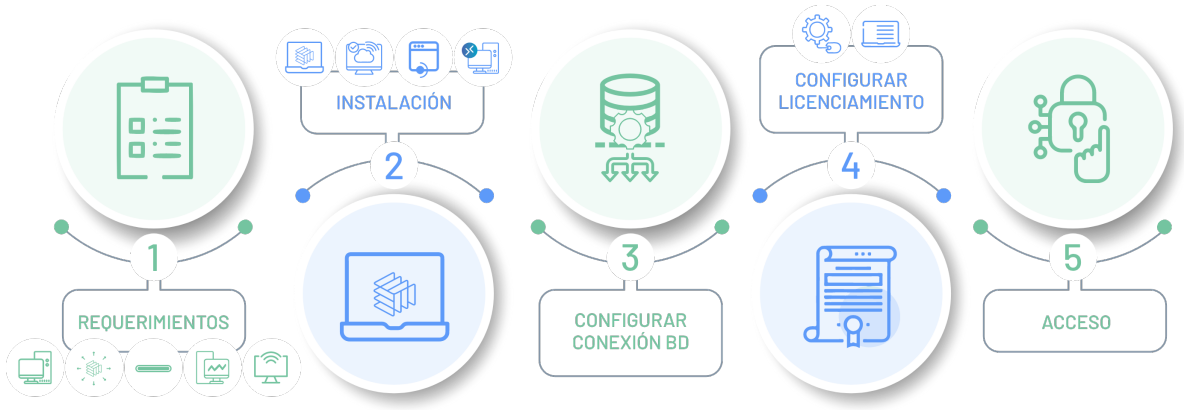
- Guia de Inicio Aranda Device Management ADM »
- Guía de Instalación y Configuración ADM OnPremise (Usted está AQUI)
- Guía de Instalación y Configuración ADM Cloud »
- Manual de Gestión Aranda Device Management ADM »
- Manual de Integración Aranda ADM »

Ruta de Instalación ADM OnPremise

Ruta de Instalación ADM/ Arquitectura OnPremise

A continuación se ofrece una visión general de los conceptos de la instalación del software y los diferentes componentes utilizados para el funcionamiento adecuado de Aranda Device Management ADM.

El proceso de instalación de ADM Versión OnPremise en una base de datos nueva, debe tener en cuenta los siguientes pasos:



1. Requerimientos

Valide los requerimientos mínimos de hardware y software para la instalación y funcionamiento de Aranda Device Management ADM.

Para mayor información consulte los requerimientos de instalación de ADM en ambientes Cloud:

- Requerimientos del Sistema
- Requerimientos / Puertos
- Requerimientos/Exclusiones Antivirus
- Requerimientos/ Administración Remota
- Requerimientos/Control Remoto

2. Instalación ADM

La instalación de Aranda Device Management ADM en arquitecturas Cloud debe tener en cuenta los siguientes pasos para instalar los difrentes componentes:

- Instalador Consola Web
- Instalador Conserver
- Instalador Agente de Descubrimiento
- Instalador MQTT Broker
- Instalador Mib Browser
- Instalador Control Remoto
- Instalador Visor Soporte Remoto Especialista
- Instalador Agente ADM

3. Configuración Base de Datos

Configure las cadenas de conexión hacia la base de datos de los sitios y servicios relacionados.

- Configuración Conexión Base de Datos

4. Licenciamiento

Administre las licencias adquiridas por el cliente y genere la solicitud de licencias para realizar una adecuada gestión del prducto.

- Licenciamiento ADM

5. Acceso ADM

El proceso de autenticación a la consola web de ADM se ejecutará de acuerdo al rol definido por la organización para desarrollar las diferentes tareas de gestión de inventarios.

- Acceso ADM

> ⚐ **Nota:** Si la instalación del software y los componentes de ADM se realiza sobre una base de datos nueva, puede tomar en cuenta las siguientes instrucciones:
> Instalación ADM en base de datos nueva

Requerimientos

Se recomienda la siguiente configuración para administrar entre 1 y 2500 dispositivos.

Servidor Conserver

Sistema Operativo	**Windows Server 2019 y Windows Server 2022**
Cores	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz 2.10 GHz
Memoria RAM	8 GB
Disco	128 GB (HDD o SSD)

⚐ A tener en cuenta:

1. Se recomienda un límite máximo de 10.000 dispositivos por conserver para garantizar un rendimiento óptimo, considerando las características del servidor y asegurando que el uso de CPU no afecte negativamente su funcionamiento.
2. Al instalar un conserver en el mismo servidor que la consola de ADM, se recomienda un límite máximo de 3.500 dispositivos.
3. Sí los agentes se conectan directamente a un Repserver Onpremises, se recomienda un límite máximo de 3.000 dispositivos.

Servidor Azure de Base de Datos

Tipo	SQL Database (MS SQL 2019 o superior en versión Estandar/ Enterprise Datacenter)
Tamaño	Mínimo 5 GB
Información Adicional	La base de datos debe ser creada con Collate: SQL_Latin1_General_CPI1_CI_AI
Observaciones	El espacio en base de datos varia conforme la cantidad de dispositivos y módulos que tenga habilitado en ADM.

⚐ Nota: Ver Excepciones

Agente de estación de trabajo

Las versiones de sistema operativo soportadas por este agente son:

Windows

Sistema operativo Windows	Versión
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

⚐ Nota:

La etiqueta de (32 bits) en el Administrador de tareas indica que el proceso se está ejecutando en modo de compatibilidad a través del subsistema WOW64 de Windows, que permite ejecutar aplicaciones de 32 bits en sistemas de 64 bits.

Tenga en cuenta que, dependiendo del equipo y la versión del sistema operativo, es posible que esta etiqueta no aparezca. Por ejemplo, en equipos con arquitectura de 32 bits, esta identificación no se muestra.

El agente de ADM para sistemas Windows está compilado en formato x86 (32 bits) para garantizar compatibilidad tanto en equipos de 64 bits como de 32 bits. Por ello, se instala en la ruta C:\Program Files (x86).

Esta condición no afecta el funcionamiento del agente ni tiene implicaciones en su rendimiento o características.

Mac

Sistema operativo Mac	Versión
MacOs	Sequoia
MacOs	Ventura
MacOs	Sonoma

⚐ Nota:
1. Se soportan los siguientes procesadores: Intel y Apple Silicon M1, M2 y M3
2. El agente no es soportado para versiones de MacOs de 32 bits.

Linux

Sistema operativo Linux	Versión
Ubuntu	24.04 LTS
Ubuntu	22.04 LTS
Ubuntu	20.04 LTS
Red Hat	Enterprise Linux 9 LTS
Red Hat	Enterprise Linux 8.7 LTS

⚐ Nota:

1. Las versiones de ubuntu se soportan tanto para server como para desktop en versiones LTS.
2. El agente no es soportado para distribuciones Linux de 32 bits.

Requerimientos/Puertos

Los siguientes son los puertos de comunicación usados por Aranda Device Management (ADM). Es necesario configurar la red para permitir las comunicaciones a través de estos puertos.

Servidor Consola de ADM

Los siguientes son los puertos y permisos requeridos en el servidor de la consola de ADM para la conexión de cada uno de los siguientes Componentes:

Sitio Web ADM

80 (HTTP) o 443 (HTTPS)	TCP,UDP	Puerto de entrada: Requerido para la conexión de los clientes con el servidor

⚐ Notas:
- Para el módulo de actualizaciones, el servidor debe tener salida completa a internet para la descarga de parches de actualizaciones, desde los sitios oficiales de cada proveedor y su posterior distribución en los dispositivos gestionados.

⚐ Notas:
- Se requiere configurar el servidor para permitir la visualización y descargas del sitio https://download.arandasoft.com/updates, con el fin de facilitar las descargas automáticas de los agentes en ADM

Notificaciones Control Remoto

443 (HTTPS)	TCP,UDP	Puerto de entrada: Requerido para la conexión de los agentes con en servidor de notificaciones
8081	TCP	Puerto de Entrada, destinado a la conexión del Agente Especialista y del agente de estación de trabajo con el Turn Server en la toma de control remoto, se debe habilitar en el servidor el uso de SSL.
	WebSockets	Establecen una conexión bidireccional persistente entre el agente y el servidor.
3478	TCP	Puerto de Entrada, destinado a la conexión del Agente Especialista y del agente de estación de trabajo con el Stun Server en la transferencia de archivos.
49152-65535	UDP	Puerto de Entrada, si requiere que opere como turn webRTC para recibir las conexiones entrantes. Configuración del Servidor Stun/Turn WebRTC

⚐ Notas:
- Se requiere configurar el servidor , para visualizar el sitio en caso de tener la funcionalidad de Control remoto. https://download.arandasoft.com/updates y descargar archivos

Repserver

80 (HTTP) o 443 (HTTPS)	TCP,UDP	Puerto de entrada: Requerido para la conexión de los agentes y/o Conserver según la arquitectura implementada
1884 (Opcional)	MQTT	Requerido únicamente para la salida, utilizado según la arquitectura implementada

Notificaciones del Repserver

WebSockets	Establecen una conexión bidireccional persistente entre el agente de ADM y el servidor, requerido para la funcionalidad de Administración Remota

⚐ Notas:
- - La funcionalidad de administración remota sólo se soportará en sitios seguros con protocolo (Https).

- Para la funcionalidad de administración remota, debe tener habilitada la comunicación por (TLS 1.2 o 1.3). Por seguridad de la comunicación no se soportan versiones inferiores de TLS.

Servidor ADM Conserver

Las máquinas en redes locales se pueden conectar a un Conserver (servidor en la red local) para trabajar con conexiones locales y contar con funcionalidades adicionales.

80 (HTTP) o 443 (HTTPS)	TCP,UDP	Puerto de entrada: Requerido para la conexión de los agentes con el servidor del conserver
1884	MQTT	Requerido únicamente para la salida, destinado para la conexión al MQTT Broker

⚐ **Notas:**
- Para la distribución del agente los dispositivos deben estar dentro de la misma red LAN, se requiere que los dispositivos tengan el recurso admin$ compartido.
- Se requiere que el Usuario de Windows de Aranda con el que se realizará la instalación y despliegue de Agentes tenga permisos de Instalación preferiblemente administrador de las máquinas correspondientes.
- Para sistemas operativos Linux y Mac se requiere el uso del usuario root para el despliegue del agente.

Agente de Descubrimiento

Cuando el cliente requiere la funcionalidad de descubrimiento, se deben habilitar los protocolos para que se puedan encontrar e identificar equipos en la red local.

137 (Opcional)	NETBIOS	Requerido únicamente para la salida, destinado al descubrimiento de dispositivos por el protocolo NETBIOS
22 (Opcional)	SSH	Requerido únicamente para la salida, destinado al descubrimiento de dispositivos por el protocolo SSH
389 (Opcional)	TCP,UDP	Requerido únicamente para la salida, destinado al descubrimiento de por LDAP
161 (Opcional)	SMNP	Requerido únicamente para la salida, destinado al descubrimiento de dispositivos por el protocolo SMNP

⚐ **Notas:**
- El puerto 80 (HTTP) es requerido si no se configuran el servidor con HTTPS y los certificados SSL apropiados. El cliente debe habilitar el protocolo HTTPS y no a través del protocolo HTTP.

- No es necesario habilitar siempre todos los protocolos. El módulo de descubrimiento de ADM permite habilitar los protocolos que se requieren en el proceso.

Servidor de base de datos

El servidor de ADM almacena la información en servidores, en SQL Server o SQL Azure. Si utiliza SQL Server como repositorio, es necesario habilitar las comunicaciones a este servidor.

1433	TCP	Puerto de entrada del protocolo de SQL Server en el servidor de bases de datos

MQTT Broker

Para generar notificaciones en tiempo real a los dispositivos, podrá utilizar un servidor MQTT en la red local. En consecuencia, tendrá que habilitar las comunicaciones hacia el MQTT Broker.

1884	MQTT	El puerto del MQTT Broker se puede modificar si se requiere. Sólo tendrá que habilitar el puerto de entrada en la máquina donde funciona el MQTT Broker, para ambientes cloud es definido por el área de operaciones de Aranda

ADM Gateway (Arquitectura Onpremises - Versiones de ADM inferiores a 9.21.1)

Para hacer conexiones de control remoto es posible instalar un ADM Gateway que permita la conexión entre equipos que estén en redes locales diferentes o cuando se requiera una conexión de un equipo en una red local con equipos en las casas de los empleados.

4443	TCP	El puerto del ADM Gateway se puede modificar si se requiere. Sólo tendrá que habilitar el puerto de entrada en la máquina donde funciona ADM Gateway

Aranda ADM Utils Installer (Arquitectura Onpremises - Versiones de ADM inferiores a 9.21.1)

Visor de Soporte Remoto,es un aplicativo que permite tomar control remoto de las máquinas gestionadas. Se instala en los dispositivos de los usuarios desde los cuales se va a realizar la conexión por control remoto, aplica para arquitecturas On-premises

9125 (Opcional)	TCP	Puerto de salida: Requerido para el control remoto entre dispositivos que se encuentran en la misma red LAN cuando no se utiliza un Gateway
4443 (Opcional)	TCP	Requerido únicamente para la salida, destinado para la conexión con ADM Gateway para el control remoto entre equipos que estén en redes locales diferentes

Agentes de ADM

Los Agentes se instalan en cada uno de los computadores que se van a gestionar a través de ADM. En arquitecturas con conserver los agentes son instalados en las máquinas a través de un proceso de distribución guiado desde la consola, sin embargo, existen múltiples alternativas de despliegue las cuales pueden combinarse para cubrir los diferentes escenarios de infraestructura.

Los puertos utilizados en ADM varian según la arquitectura y funcionalidades requeridas.

Agente ADM

80 (HTTP) o 443 (HTTPS)	TCP,UDP	Requerido únicamente para la salida, destinado para la conexión con ADM repserver o ADM Conserver
1884	MQTT	Requerido únicamente para la salida, destinado para la conexión con el MQTT Broker
9025 (Opcional)	TCP, UDP	Puerto de entrada: requerido para la comunicación del servidor con el agente para la Administración remota, utilizado cuando la arquitectura no permite visualizar el servidor de notificaciones del repserver para su comunicación. : **https://Dominio/repserver/Notificationmessage**.
	WebSockets (opcional)	Establecen una conexión bidireccional persistente entre el agente de ADM y el servidor de notificaciones del repserver, requerido para la Administración remota, utilizado cuando la arquitectura permite visualizar el servidor de notificaciones del repserver para su comunicación. : **https://Dominio/repserver/Notificationmessage**.
9125 (Opcional) - Versiones de ADM inferiores a 9.21.1	TCP	Puerto de entrada: Requerido para el control remoto entre dispositivos que se encuentran en la misma red LAN cuando no se utiliza un Gateway
4443 (Opcional) - Versiones de ADM inferiores a 9.21.1	TCP	Requerido únicamente para la salida, destinado para la conexión con ADM Gateway para el control remoto entre equipos que estén en redes locales diferentes

Agente ADM (Con funcionalidades de descubrimiento)

137 (Opcional)	NETBIOS	Puerto de entrada, destinado al descubrimiento de dispositivos por el protocolo NETBIOS
22 (Opcional)	SSH	Puerto de entrada, destinado al descubrimiento de dispositivos por el protocolo SSH
389 (Opcional)	TCP,UDP	Puerto de entrada, destinado al descubrimiento de por LDAP
161 (Opcional)	SMNP	Puerto de entrada, destinado al descubrimiento de dispositivos por el protocolo SMNP

⚐ **Notas:**
- No es necesario habilitar siempre todos los protocolos. El módulo de descubrimiento de ADM permite habilitar los protocolos que se requieran en el proceso.

- El agente de ADM utiliza dos puertos locales para establecer conexión saliente (TCP) como la conexión al MQTT Broker y comunicaciones entre procesos del agente, maneja la ip del localhost y es dinámico, elegido por la tarjeta de red, usualmente se usan rangos mayores a 1023 hasta 65535 el que se encuentre disponible. No requiere realizar nada en la configuración.

Agente ADM (Con funcionalidad de Control remoto)

Para la funcionalidad de control remoto en una arquitectura cloud y On-premises, el agente de ADM instala un Agente de estación de trabajo llamado "Aranda Remote Control Worksation", para que se realice la instalación automática el agente de ADM debe poder visualizar el dominio del repserver y todo lo que esté después de/ : **https://Dominio/repserver/api/** y descargar archivos de ese sitio. Para conectarse a estos dispositivos instale el visor agente especialista, teniendo en cuenta los siguientes Requisitos y puertos para los dos componentes de Control Remoto Cloud y Onpremises ↪.

Requerimientos/Exclusiones Antivirus

Los programas antivirus deberán configurarse con las siguientes inclusiones en los computadores donde se hará instalación del Agente de ADM:

Proceso: Aranda.Agent.ACOREService.exe

Nombre	Descripción	Ruta
Aranda Agent 9	Agente de servicio	{InstallDir}\Aranda\Aranda Agent 9

Proceso:Aranda.Agent.RemoteCommand.exe

Nombre	Descripción	Ruta
	Instalación en descubrimiento de equipo	C:\Windows\RemoteCommand \Device\HarddiskVolume3\Windows\RemoteCommand

procesos: Aranda.Agent.ARSService.exe

Nombre	Descripción	Ruta
Aranda Agent Remote Control 9	Servicio de control remoto	{InstallDir}\Aranda\Aranda Agent 9

procesos: APaaSPersist.msi

Nombre	Descripción	Ruta
APaaSPersist.msi	Agente de servicio	{InstallDir}\Aranda\Aranda Agent 9

- Sí el agente de ADM tiene la funcionalidad de Control remoto, debe agregar las siguientes inclusiones en el antivirus:

procesos: Aranda.ARC.Workstation.exe

Nombre	Descripción	Ruta
Aranda.ARC.Workstation.exe	Servicio del agente de ARC	{InstallDir}\Aranda\Aranda Remote Control\Workstation

procesos: Aranda.AVS.VNC.Application.exe

Nombre	Descripción	Ruta
Aranda.AVS.VNC.Application.exe	Servicio del agente de ARC	{InstallDir}\Aranda\Aranda Remote Control\Workstation

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

Nombre	Descripción	Ruta
Aranda.AVS.TransferFile.Service.Target.exe	Servicio del agente de ARC	{InstallDir}\Aranda\Aranda Remote Control\Workstation

Requerimientos/Módulo Administración Remota

Configurar la administración remota según la arquitectura instalada de ADM.

Puertos y permisos requeridos

1. Lea atentamente los puertos y permisos requeridos según la arquitectura de instalación de ADM antes de pasar al siguiente punto.

- Agente ADM Arquitectura Onpremises
- Consola Web, Repserver, servidor de notificaciones del Repserver

Configuración por base de datos

- Sí la comunicación para la administración remota se va a realizar por medio del servidor de notificaciones del repserver ejecute el siguiente script.:

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

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

> ⚐ **Nota:** En la vista detalle de los dispositivos inventariados por ADM podrá consultar la información del dispositivo con Administración Remota

Requerimientos/Control Remoto

Agente especialista (Visor)

Para acceder a las funciones de soporte remoto se debe instalar el agente especialista en un dispositivo que cumpla las siguientes condiciones mínimas:

	Dispositivo especialista
Procesador virtual	CPU de 2 núcleos
Memoria RAM	Mínimo 4 GB
Espacio de disco	Mínimo 4 GB

Las versiones de sistema operativo soportadas por el agente especialista son:

Sistema operativo	Versión
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
Windows 10	20H2
Windows 10	21H1
Windows 10	21H2
Windows 10	22H2
Windows 11	21H2
Windows 11	22H2

Los navegadores soportados son los siguientes:

Navegador	Versión
Edge	Versión >= 88
Google Chrome	Versión >= 97.0.4692.71

Puertos utilizados por el Agente Especialista

Puerto	Protocolo	Descripción
443	TCP	Requerido para la conexión del Agente Especialista con el servidor de Grabaciones, debe poder visualizar el sitio: https://Dominio/adm/arc/recording
8081	TCP	Requerido únicamente para la salida, destinado a la conexión del Agente Especialista con el Turn Server en la toma de control remoto.
	WebSockets	Establecen una conexión bidireccional persistente entre el agente y el servidor.
3478	TCP	Requerido únicamente para salida, destinado a la conexión del Agente Especialista con el Stun Server en la transferencia de archivos.
15000 - 65000	UDP	Rango requerido únicamente para salida, destinado a la conexión del Agente Especialista con el Stun Server en la transferencia de archivos.

Agente Aranda Remote Control de estación de trabajo

> ⚠ **Importante:** No se puede tener instalado en forma simultánea el Agente de AVS y el Agente Aranda Remote Control (ARC) en la misma estación de trabajo. Se pueden generar conflictos entre ambos agentes, impidiendo un uso adecuado.

Las condiciones mínimas para la instalación que debe cumplir la estación de trabajo son:

Requerimientos de la estación de trabajo	
Procesador virtual	CPU de 2 núcleos
Memoria RAM	Mínimo 4 GB
Espacio de disco	Mínimo 400 MB

Las versiones de sistema operativo soportadas por este agente son:

Sistema operativo	Versión
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
Windows 10	20H2
Windows 10	21H1
Windows 10	21H2
Windows 10	22H2
Windows 11	21H2
Windows 11	22H2
Windows Server 2016	
Windows Server 2019	1809
Windows Server 2022	

Puertos utilizados por el Agente de estación de trabajo .

Puerto	Protocolo	Descripción
443	TCP	Requerido para la conexión del Agente de estación de trabajo con el servidor de Notificaciones, debe poder visualizar el sitio: https://Dominio/adm/arc/notification
8081	TCP	Requerido únicamente para la salida, destinado a la conexión del Agente estación de trabajo con el Turn Server en la toma de control remoto.
	WebSockets	Establecen una conexión bidireccional persistente entre el agente y el servidor.
3478	TCP	Requerido únicamente para salida, destinado a la conexión del Agente de la estación de trabajo con el Stun server en la transferencia de archivos.
15000 - 65000	UDP	Rango requerido únicamente para salida, destinado a la conexión del Agente de la estación de trabajo con el Stun server en la transferencia de archivos.

Puertos locales usados para la comunicación interna de procesos del agente

Puerto	Protocolo	Descripción
5050	WebSocket	Usado por Aranda.ARC.Workstation.exe para recibir mensajes y peticiones de los demás procesos
5029	GRPC	Usado por Aranda.AVS.TransferFile.Service.Target.exe para recibir peticiones de transferencia de archivos
9087	GRPC	Usado por Aranda.AVS.VNC.Application.exe para recibir peticiones de control remoto

⚐ **Notas:**
- El agente de estación de trabajo debe poder visualizar la siguiente ruta del repserver para la actualización automática del agente y todo lo que esté después de **/** : **https://Dominio/repserver/api/** y descargar archivos de ese sitio

Instalador/Consola Web ADM

Requisitos para intalación OnPremises Windows Server

- Activación de roles y caracteristicas.
- Instalacion de .NET Framework Version 4.8
- Instalación de Windows Hosting Bundle Installer

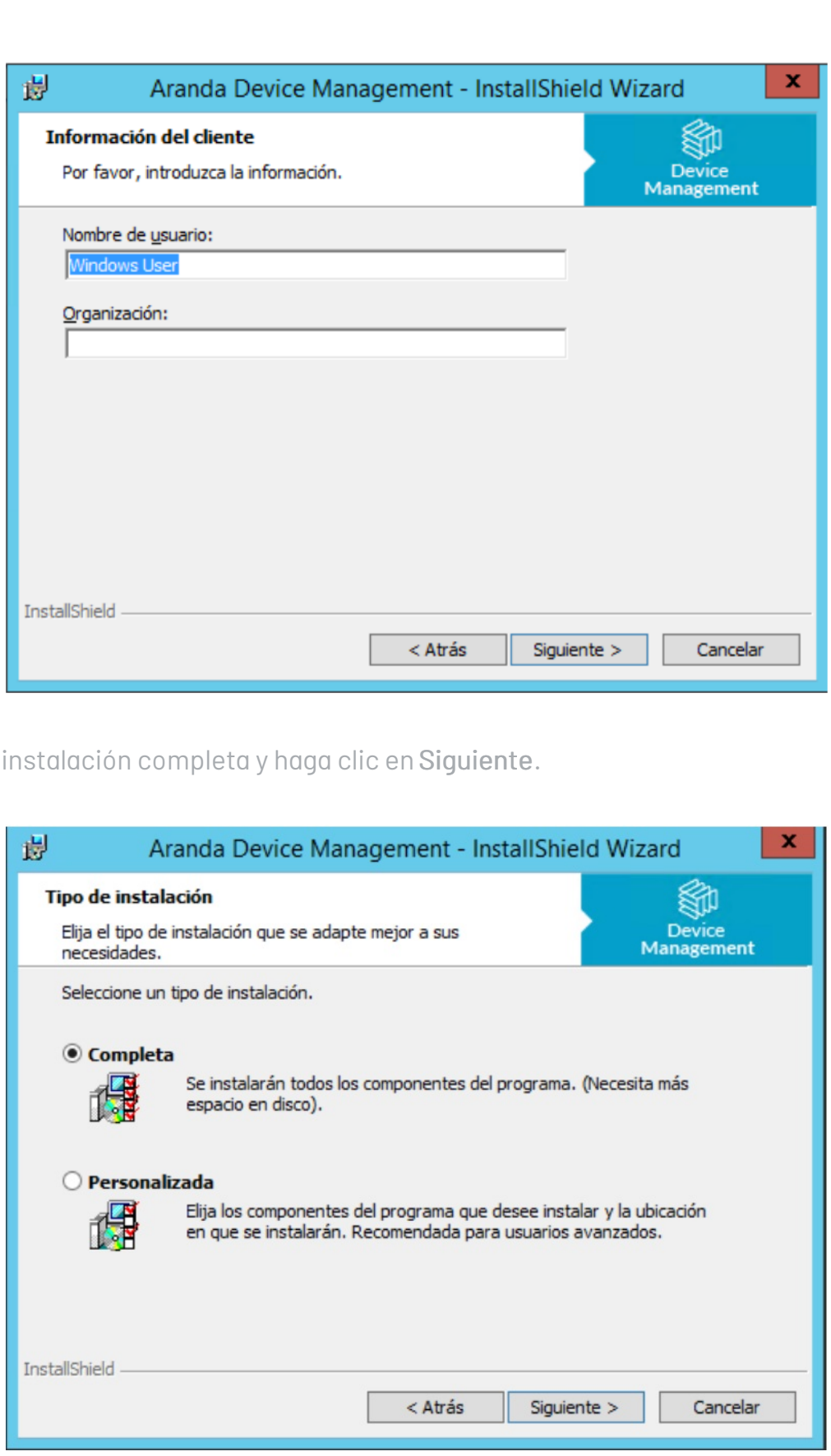
Instalador Consola ADM

El instalador **Aranda.ADM.Web.Installer** de la consola web de ADM, instala los sitios de la consola, el Repserver y los sitios para Control Remoto (Notificaciones y Grabaciones); adicionalmente crea los servicios de los Crunchers, License, Scheduler, Worker, Turn Stun WebRTC y Turn Server que se usan en la aplicación. A continuación, el paso a paso de la instalación.

1. Al hacer clic sobre el instalador se iniciará el asistente de instalación (wizard). Haga clic en **Siguiente**.

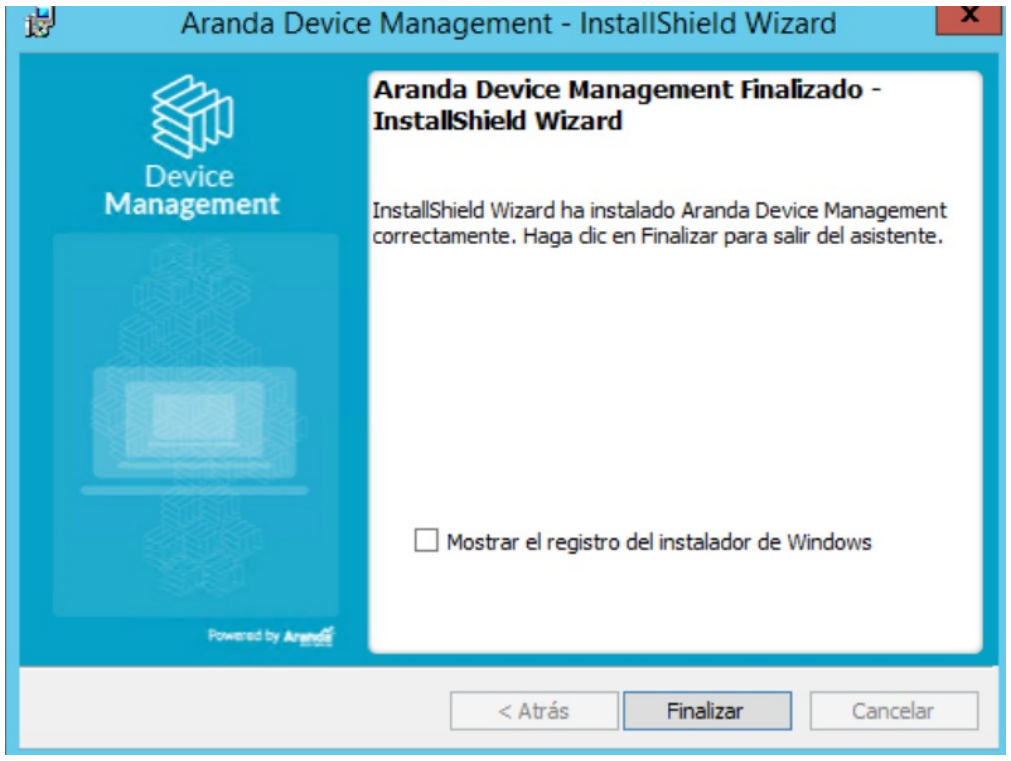
2. Ingrese la información del cliente y haga clic en **Siguiente**.

3. Seleccione el tipo de instalación completa y haga clic en **Siguiente**.



4. Haga clic en **Instalar**.

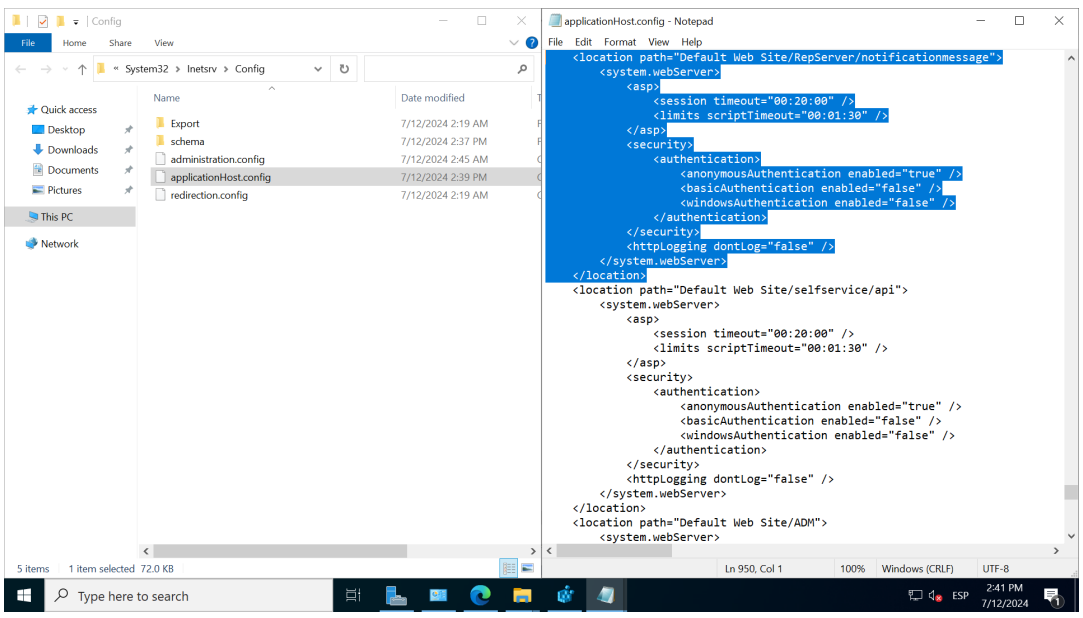
5. Terminado el proceso de instalación, haga clic en **Finalizar**.



⚐ Nota:

- Si el sitio web de ADM no sube correctamente, revise que se hayan ejecutado los requisitos de acuerdo el orden definido; ejecute nuevamente los instaladores reparando la instalación

- Si el error persiste busque el archivo WinDir%\System32\Inetsrv\Config\applicationHost.config y elimine el tag de location que corresponda al sitio “Repserver/notificationmessage” y reinicie el IIS

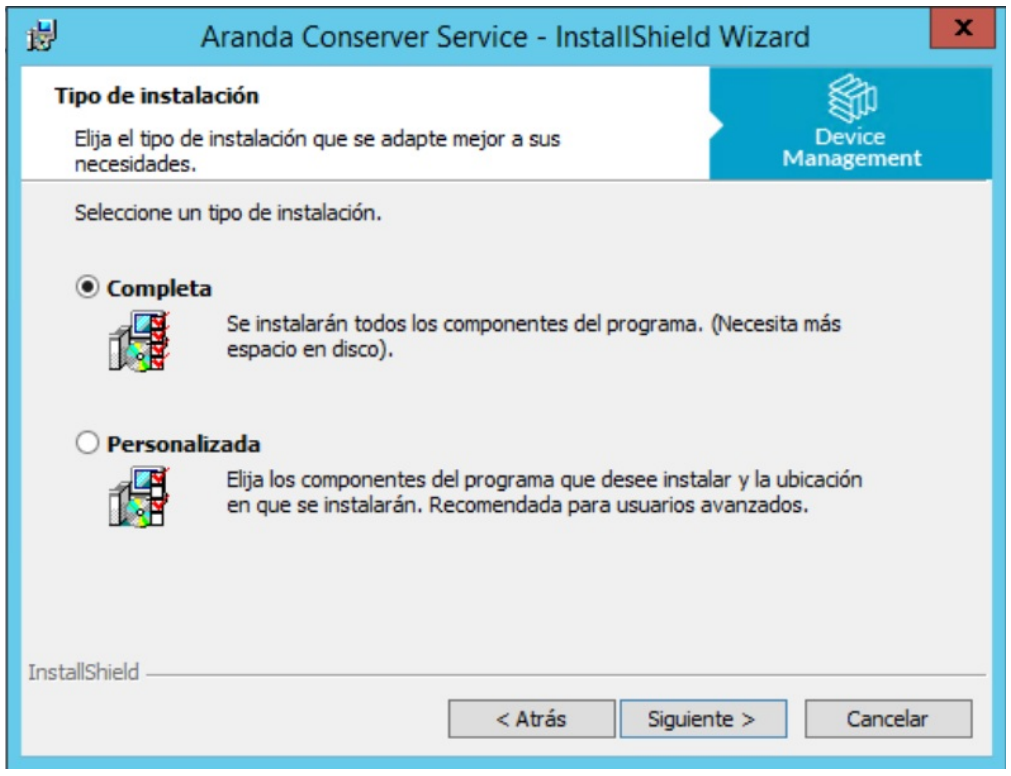


Instalador/Conserver

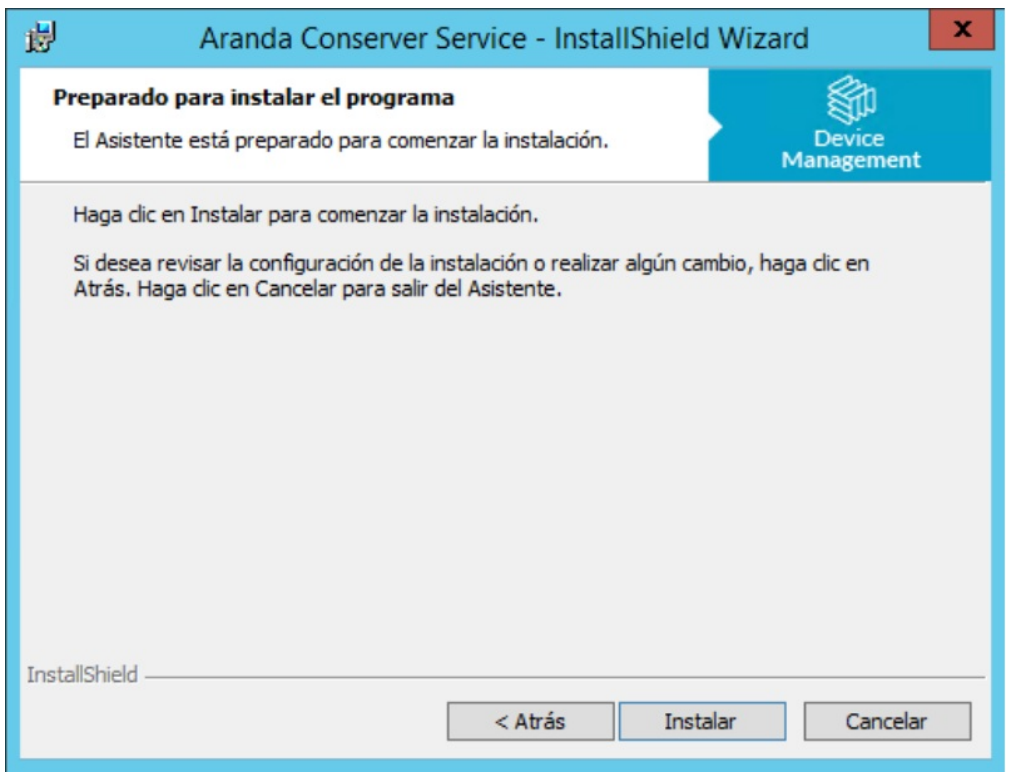
El segundo instalador es Aranda.Conserver.Installer. Se deberá instalar un servicio por cada segmento de red.

1. Al hacer clic sobre el instalador se iniciará el asistente de instalación (wizard).

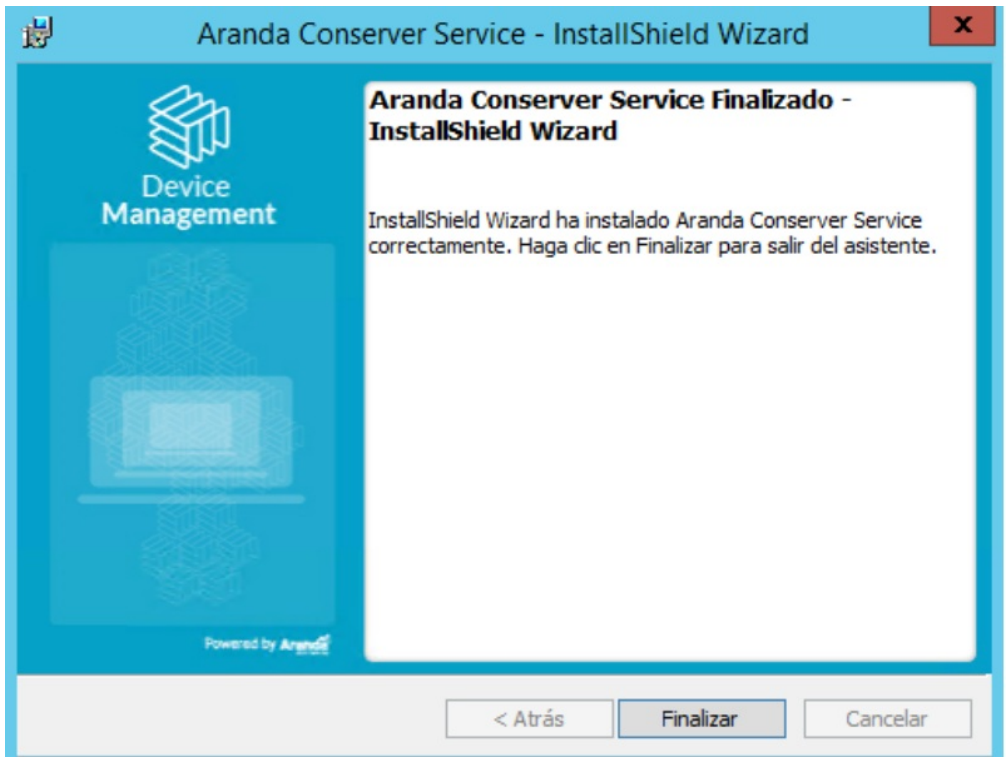
2. Seleccione el tipo de instalación completa y haga clic en **Siguiente**.



3. Haga clic en **Instalar**.



4. Al completar el proceso de instalación, haga clic en **Finalizar**.



—

Enlaces Relacionados:

- Configuracion Conserver
- Configuracion Conserver Consola

Configuración Conserver

Configuración Conserver

« Instalador Conserver

1. Al instalar un Conserver todos los archivos se guardan en la rutaC:\ Program Files (x86) \ Aranda \ Conserver, Configure el archivo Aranda.Conserver.Windows.Service.exe.config de la siguiente manera para que se comunique con el Repserver:

Configuración appSettings	
add key="dataConfiguration:defaultDatabase" value="local" /	Se utiliza para establecer la base de datos predeterminada que se utilizará en la aplicación.
add key="Serilog:MinimumLevel" value="Debug"	Se utiliza para establecer el nivel mínimo de registro de eventos para la biblioteca de registro Serilog.
add key="Serilog:WriteTo:0:Name" value="File"	Se utiliza para especificar el primer destino de registro que se utilizará para Serilog. El valor "File" indica que los eventos de registro se escribirán en un archivo.
add key="Serilog:WriteTo:0:Args:path" value="Logs\log.txt"	Se utiliza para especificar la ruta y el nombre del archivo donde se escribirán los eventos de registro.
add key="Serilog:WriteTo:0:Args:shared" value="true"	Se utiliza para especificar si el archivo de registro debe ser compartido por varios procesos o no.
add key="Serilog:WriteTo:0:Args:rollingInterval" value="Day"	Se utiliza para especificar el intervalo de tiempo en el que se crean nuevos archivos de registro.
add key="Logging:LogLevel:Default" value="Information"	Se utiliza para establecer el nivel de registro predeterminado para la biblioteca de registro de Microsoft.
add key="serverAddress" value=""	Dirección donde se encuentra el Repserver
	En caso de usar Proxy se habilita la etiqueta enableProxy

add key=”enableProxy” value=”false”	En caso de usar Proxy se habilita la etiqueta enableProxy con valor “true”

Configuración appSettings

add key=”proxyAddress” value=””	Dirección del proxy
add key=”proxyUser” value=””	Usuario del Proxy
add key=”proxyPassword” value=””	Contraseña del Proxy
add key=”logLevel” value=”Information”	Nivel de verbosidad log del conserver; “Information”, “Debug”, “Detailed”, “Verbose”. Por defecto se encuentra parametrizado en “Information”
add key=”privateIp” value=””	Identificador en la red interna del Conserver, deber ia la ip
add key=”publicIp” value=””	Identificador de la red del conserver desde el exterior, debe ir la ip. (En caso de que no se requiera se coloca la misma direccion privada)
add key=”mqttServerPort” value=”1884”	Puerto de Comunicación de mqtt, por defecto se encuentra parametrizado el “1884”
add key=”mqttIp” value=””	Identificador de Mqtt en la red interna, debe ir la IP
add key=”publicServerPort” value=”80”	Puerto de comunicacion red pública de Conserver, por defecto se encuentra parametizado el “80”.
add key=”privateServerPort” value=”80”	Puerto de comunicacion red privada de Conserver, por defecto se encuentra parametizado el “80”.
add key=”p2pPort” value=”9501”	Puerto apra conexiones p2p, por defecto se encuentra parametrizado el “9501”
add key=”maxDistributionSleepMsPerThread” value=”8”	-
add key=”maxDistributionThreads” value=”4”	Estos dos últimos tags son utilizados para el funcionamiento interno del sistema, se deben modificar

```
<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. Inicie el servicio Aranda Conserver V9, para permitir la comunicación con el Repserver.

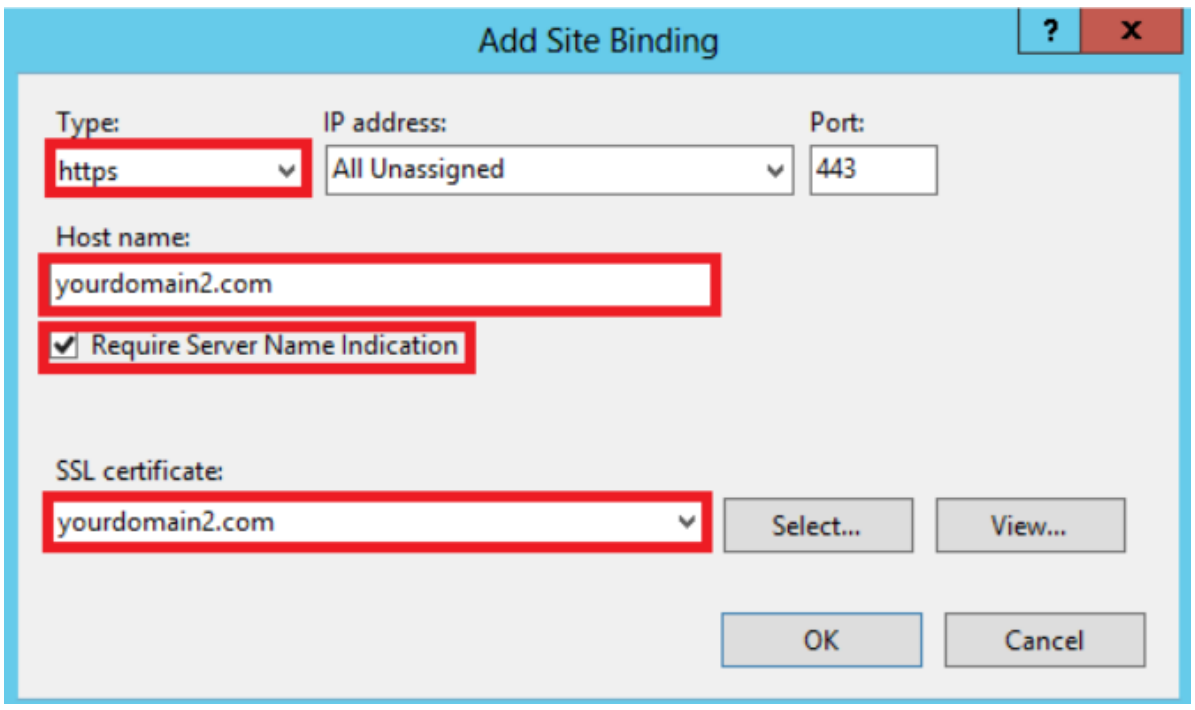
—

Configuración del conserver para recibir peticiones por https

Para configurar el conserver para recibir peticiones por https, en el iis debe estar habilitado https con el debido certificado.

Importante asegurar cualquier nombre de host adicional utilizando SNI.

Dirección IP: seleccione «All unassigned».



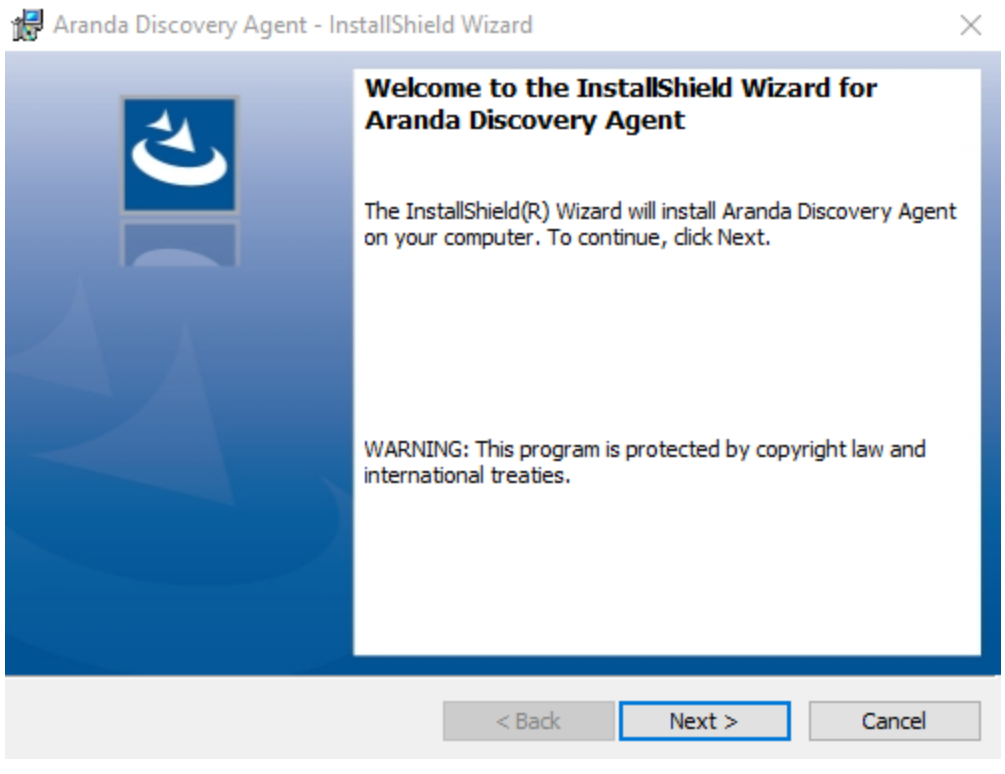
El valor de la etiqueta “enableSecurity” debe ser igual a “true”

```
<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>
```

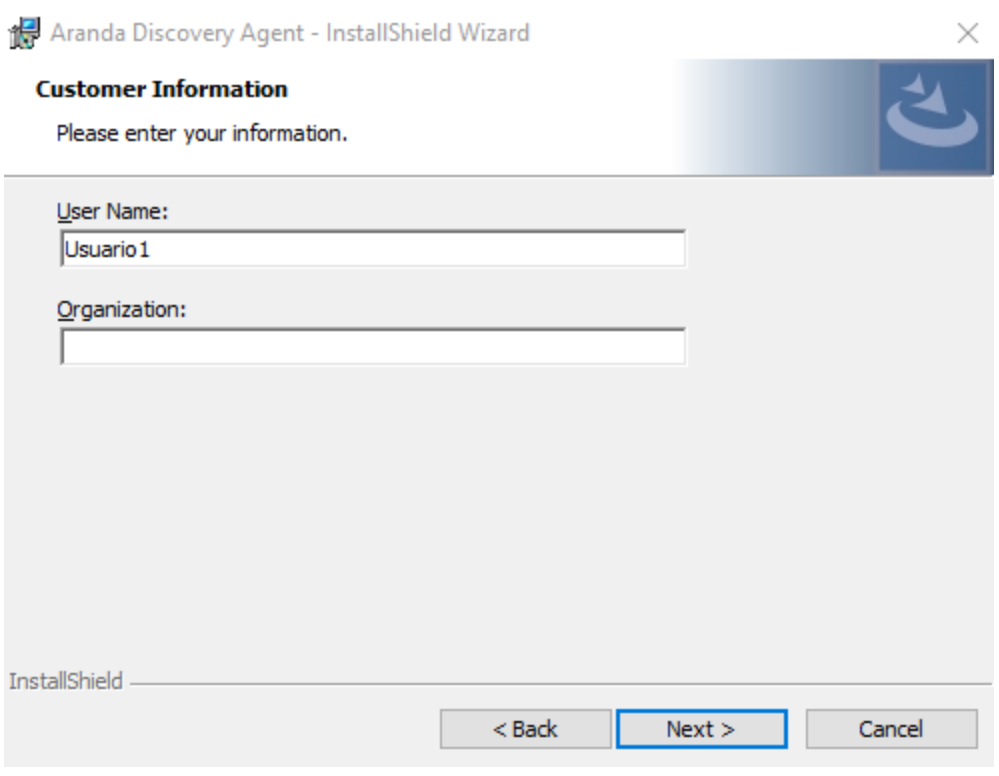
« Instalador Conserver

Instalador/Agente de descubrimiento

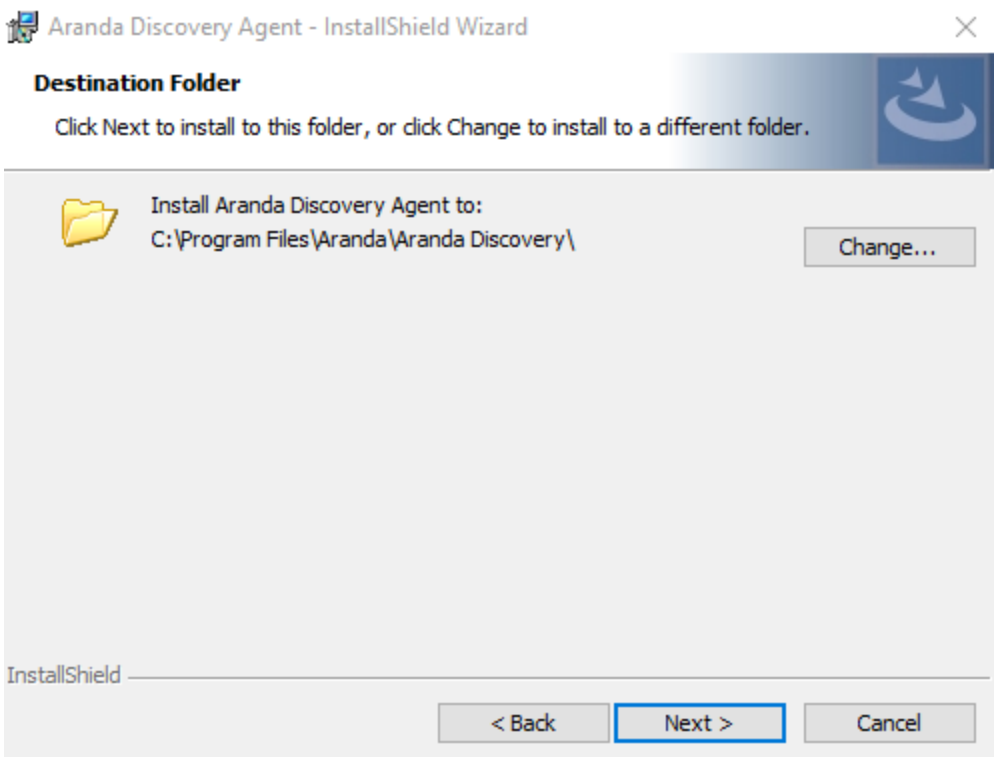
1. Ejecute el instalador Aranda.Discovery.Agent.x.x.x.exe



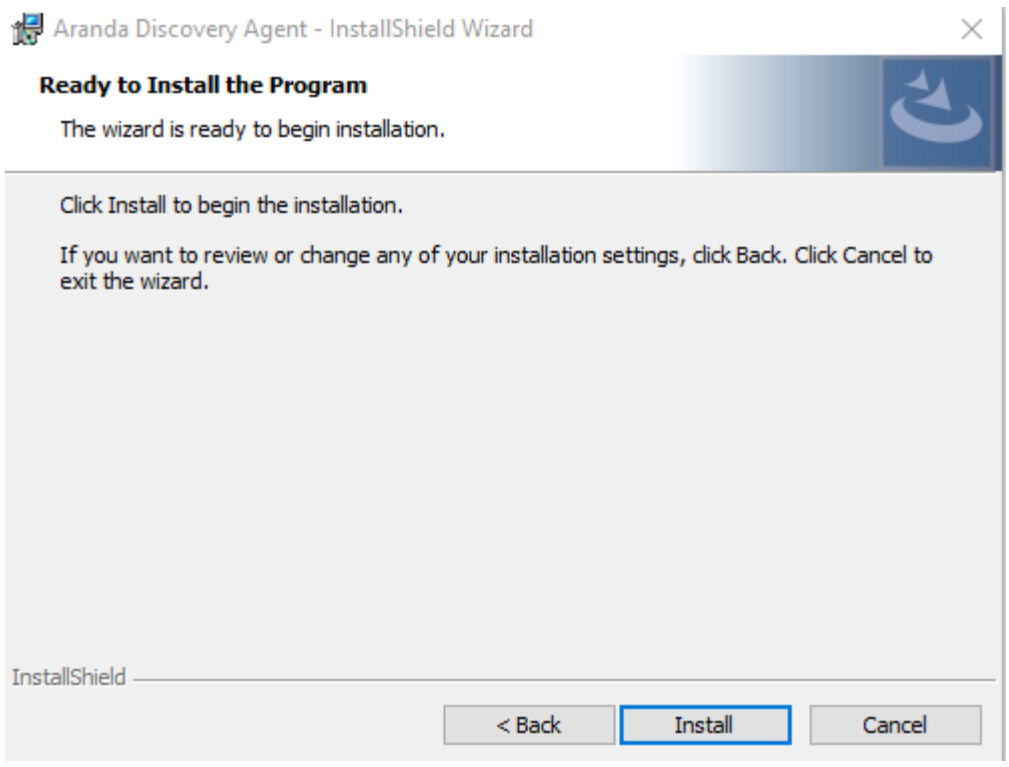
2. En la ventana Información del cliente, ingrese el nombre de usuario, la organización y haga clic en **Siguiente**. Estos campos pueden quedar vacíos.



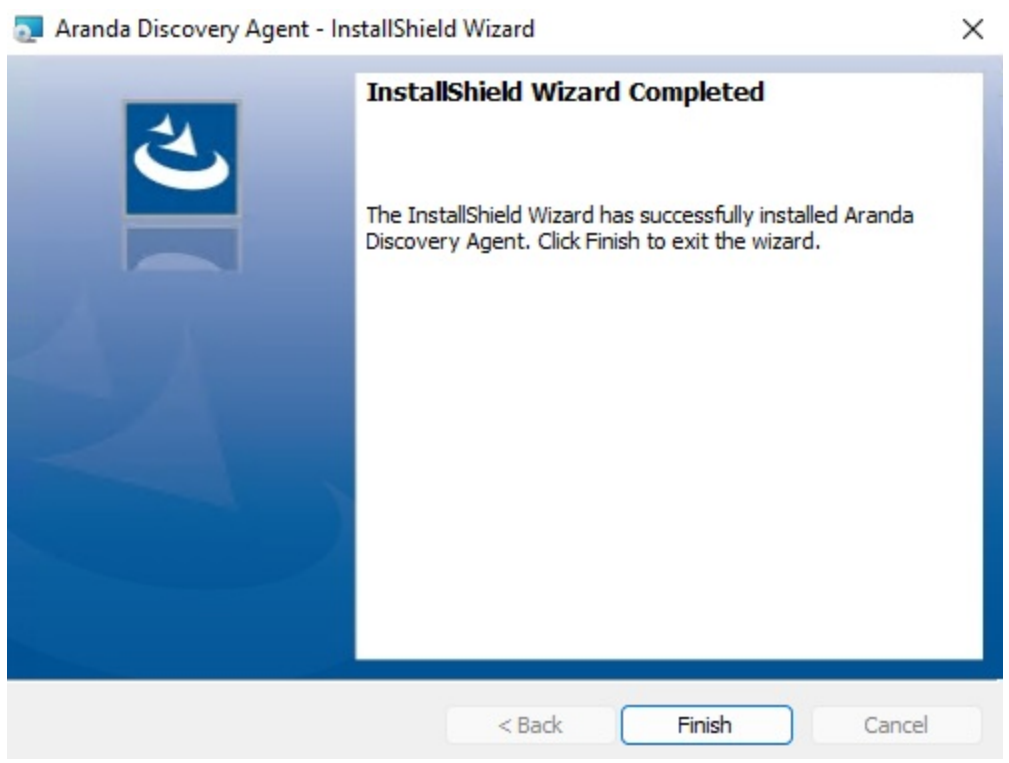
3. En la ventana Carpeta Destino, podrá cambiar la ruta de instalación del servicio o dejarlo por defecto donde lo sugiere la instalación, luego haga clic en **Siguiente**.



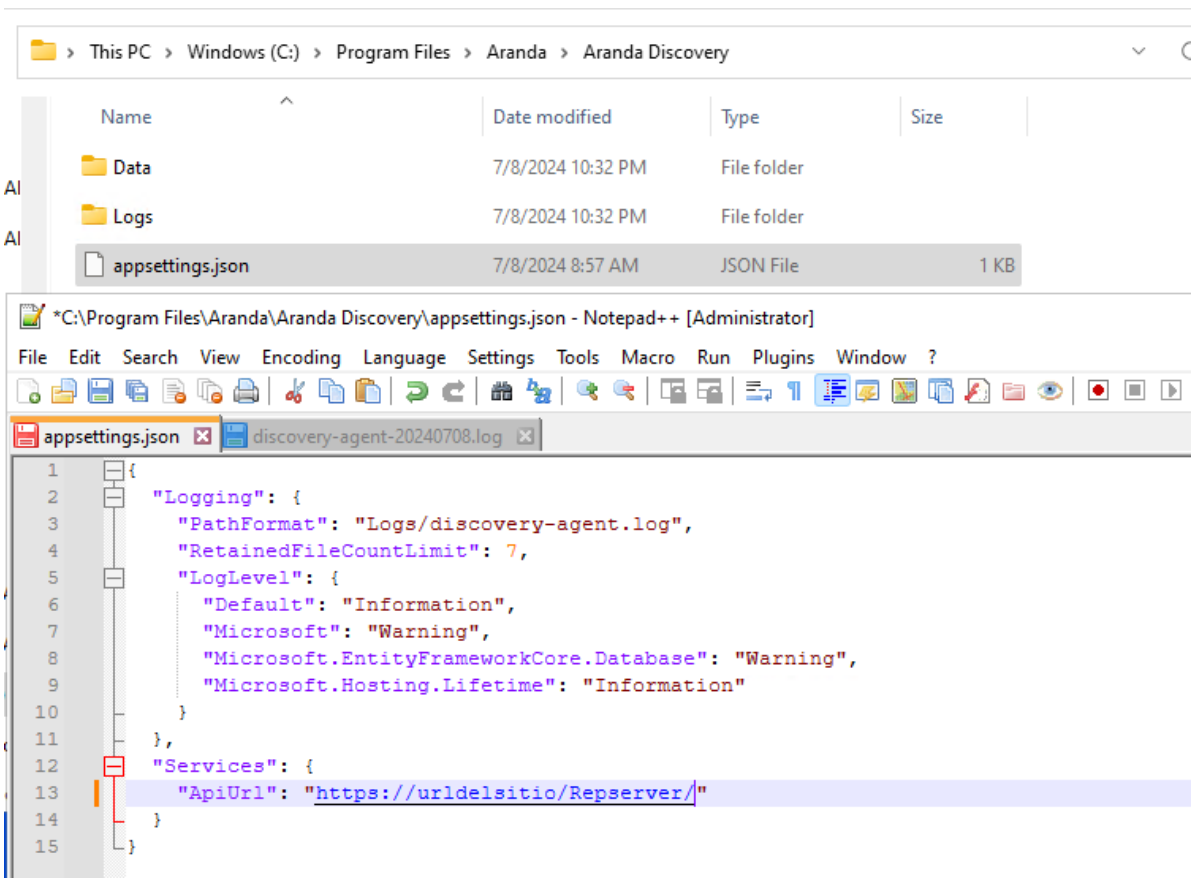
4. Haga clic en **Instalar**; se debe tener permisos como administrador de la máquina.



5. Cuando el proceso de instalación termine, haga clic en el botón **Finalizar**.

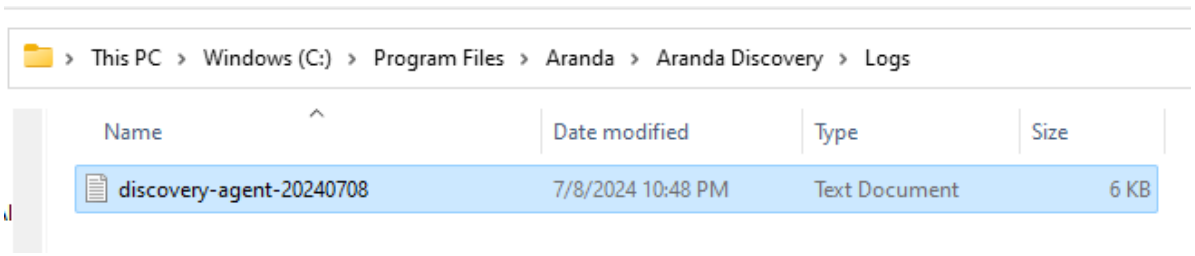


6. Para configurar el agente de descubrimiento abra el archivo **appsettings.json** que se encuentra en la carpeta donde está instalado el servicio y en la sección **Services** en **ApiUrl**, ingrese la url del Repserper del sitio.



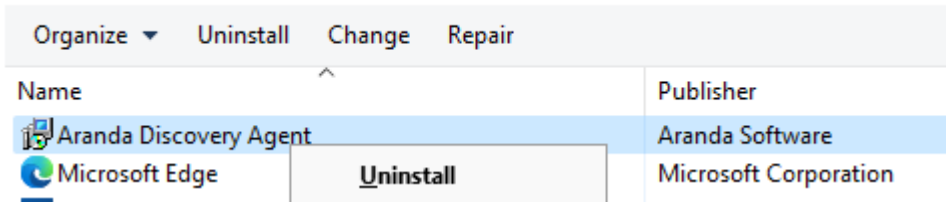
7. Una vez configurado el **appsettings** diríjase a los servicios y verifique que está instalado el servicio: Aranda Discovery Agent, luego reinicie el servicio para que tome los cambios configurados en el **appsettings**.

8. Los archivos de **log** quedarán almacenados en la siguiente ruta: **C:\Program Files\Aranda\Aranda Discovery\Logs**

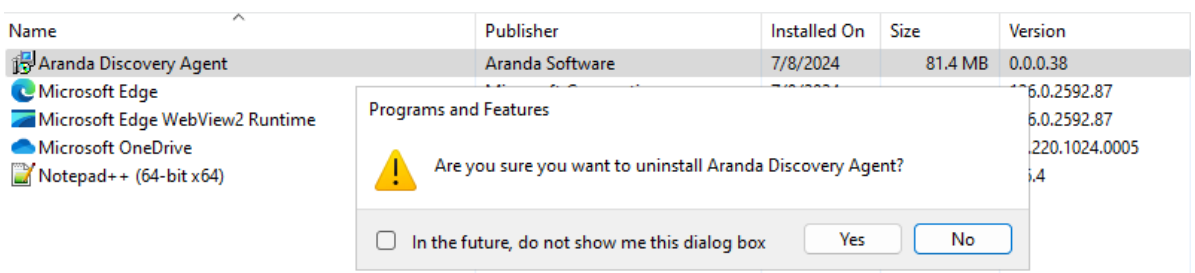


Desinstalación del Agente de descubrimiento

1. Ingrese al panel de control y haga clic derecho sobre la aplicación **Aranda Discovery Agent**, seleccione **uninstall**.



2. A la pregunta **"Esta seguro que quiere desinstalar Aranda Discovery Agent?"**, haga Clic en el botón SI del mensaje.



3. Revise de nuevo el servicio y la carpeta donde estaba instalado el servicio, ya no debe aparecer el registro.

Actualización automática del Agente de descubrimiento

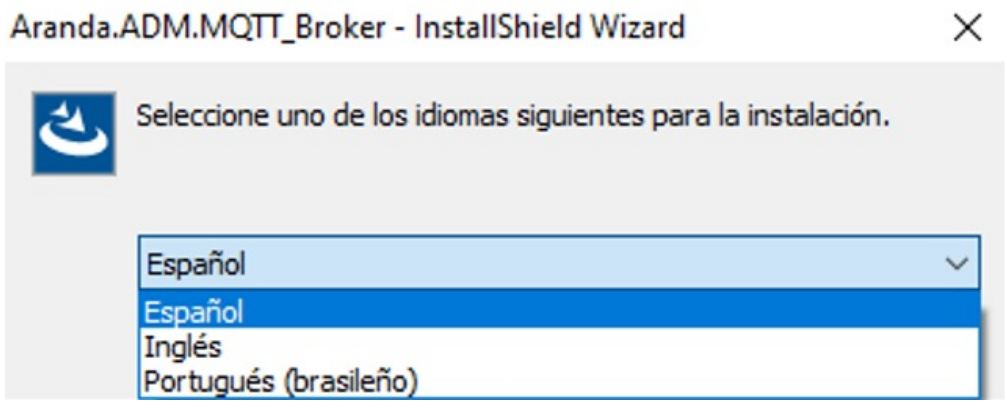
1. El agente de descubrimiento se actualizará automáicamente en el rango de un día después de la actualización del sitio de ADM.

Instalador/Aranda MQTT Broker

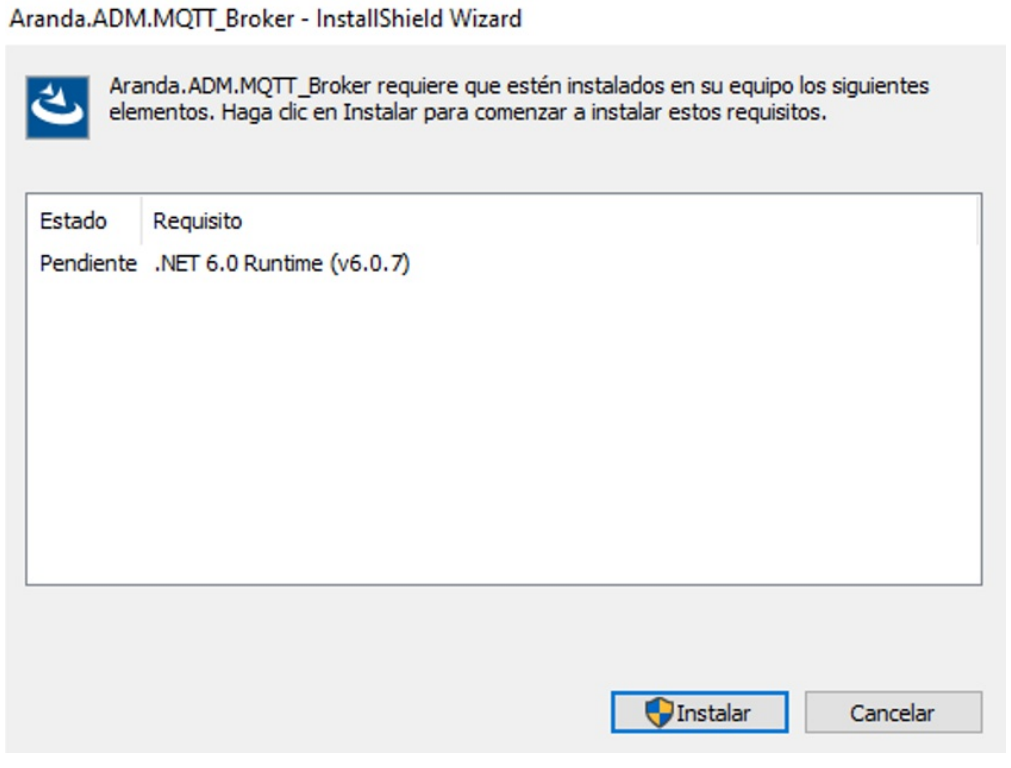
> ⚐ **Nota:** Se sugiere un numero máximo de 10.000 conexiones (dispositivos) por servidor broker de MQTT.

1. Ejecute el instalador Aranda.ADM.MQTT.Broker.exe

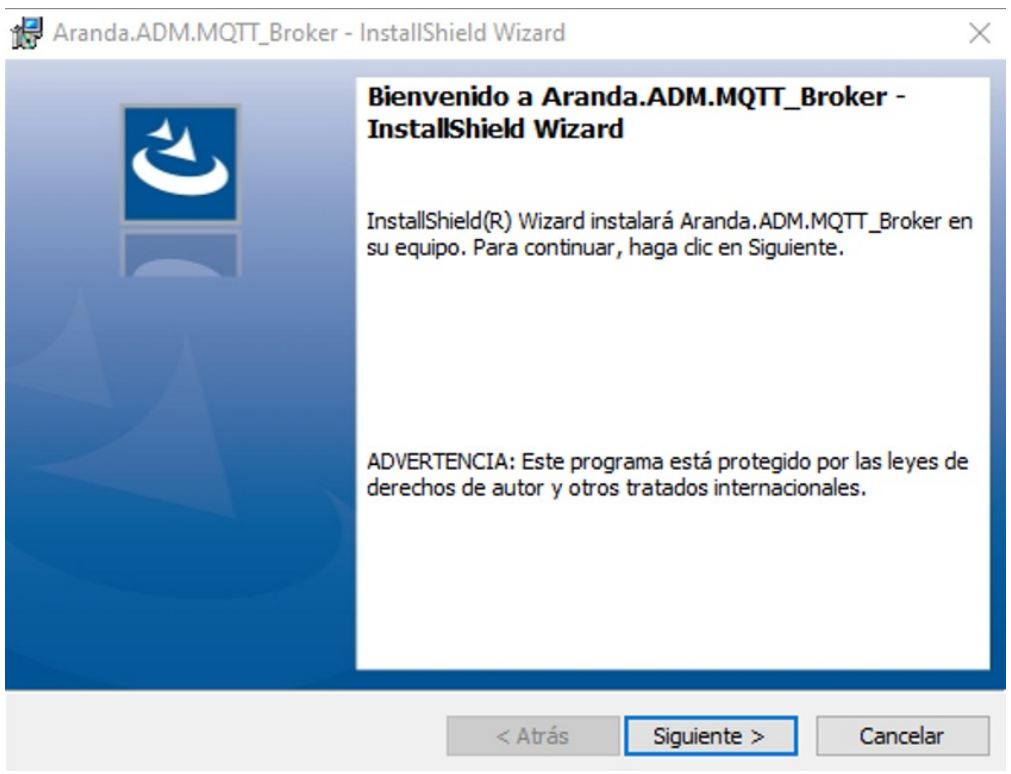
2. Defina el idioma para el proceso de instalación.



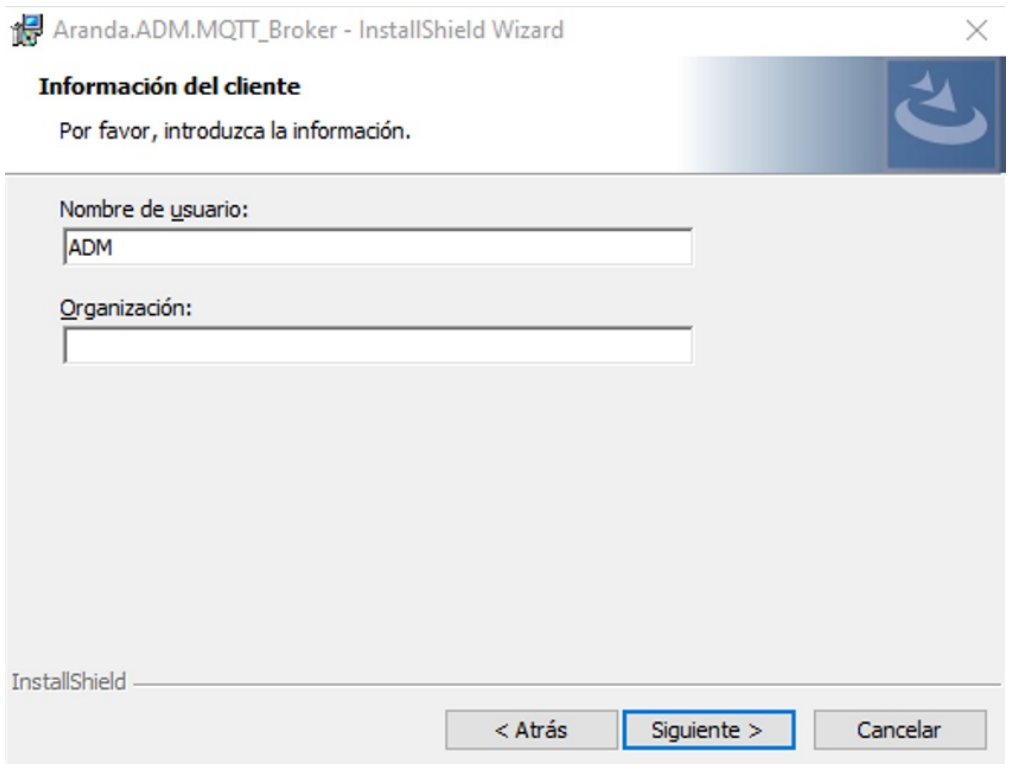
3. El instalador valida los prerequisitos que se deben cumplir para configurar el broker de Aranda. De no cumplirse, el sistema instalará la información requerida.



4. Al finalizar la instalación de los requisitos podrá visualizar la pantalla de bienvenida. Confirme la instalación haciendo clic en el botón **Siguiente**.

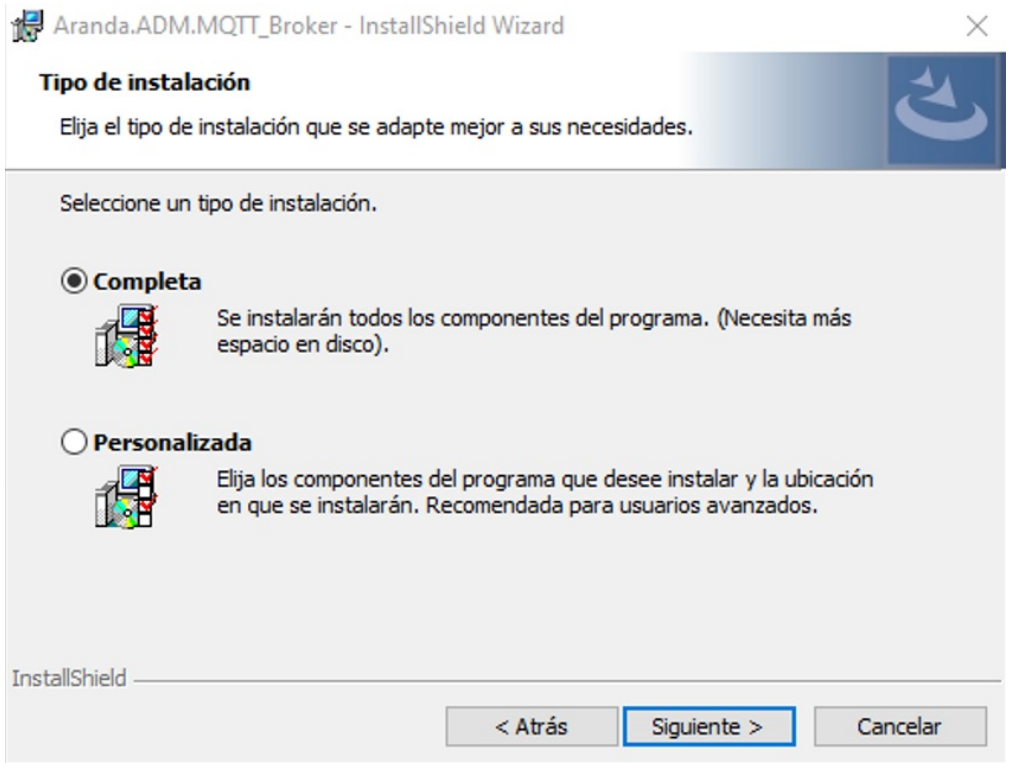


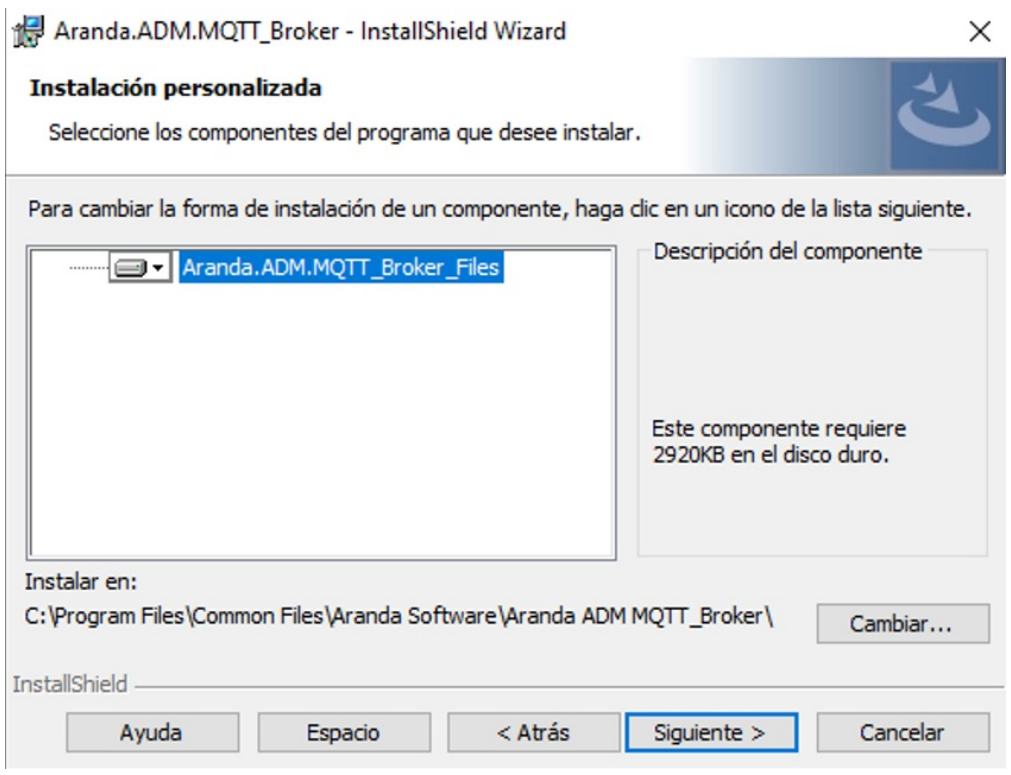
5. En la ventana Información del cliente, ingrese el nombre de usuario, la organización y haga clic en **Siguiente**. Estos campos pueden quedar vacíos.



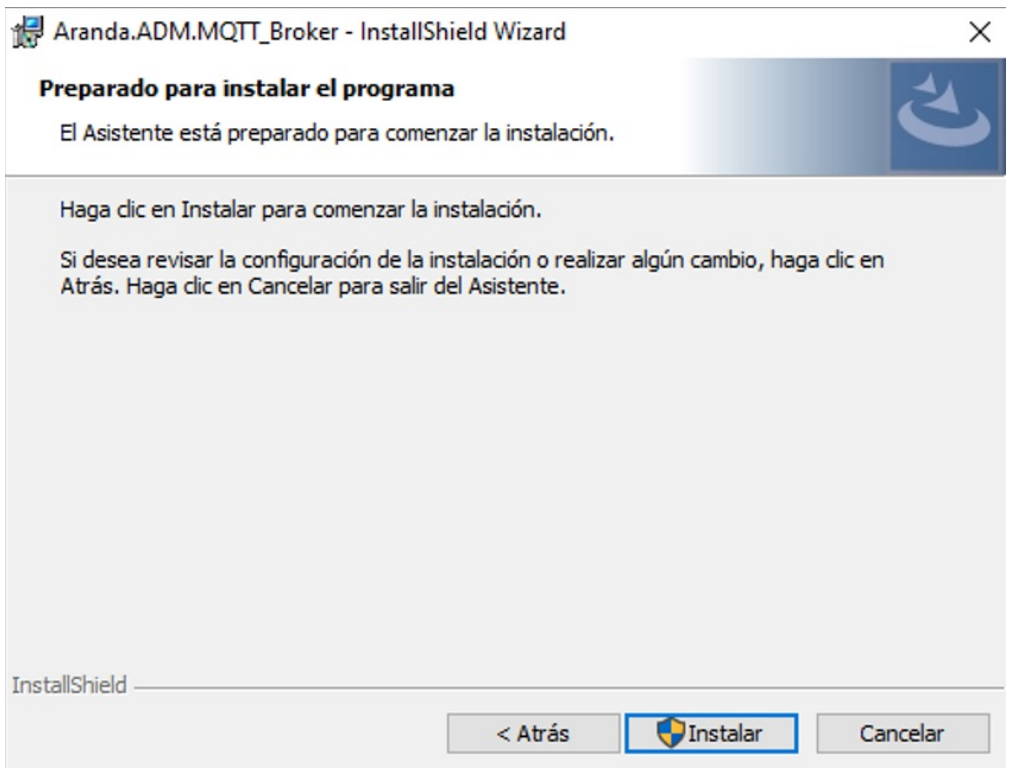
6. Defina el tipo de instalación, las opciones son:

- **Completa**: Se instalarán todos los sitios y servicios en las rutas por defecto.
- **Personalizada**: Podrá cambiar la ruta de instalación de los sitios web y los servicios.

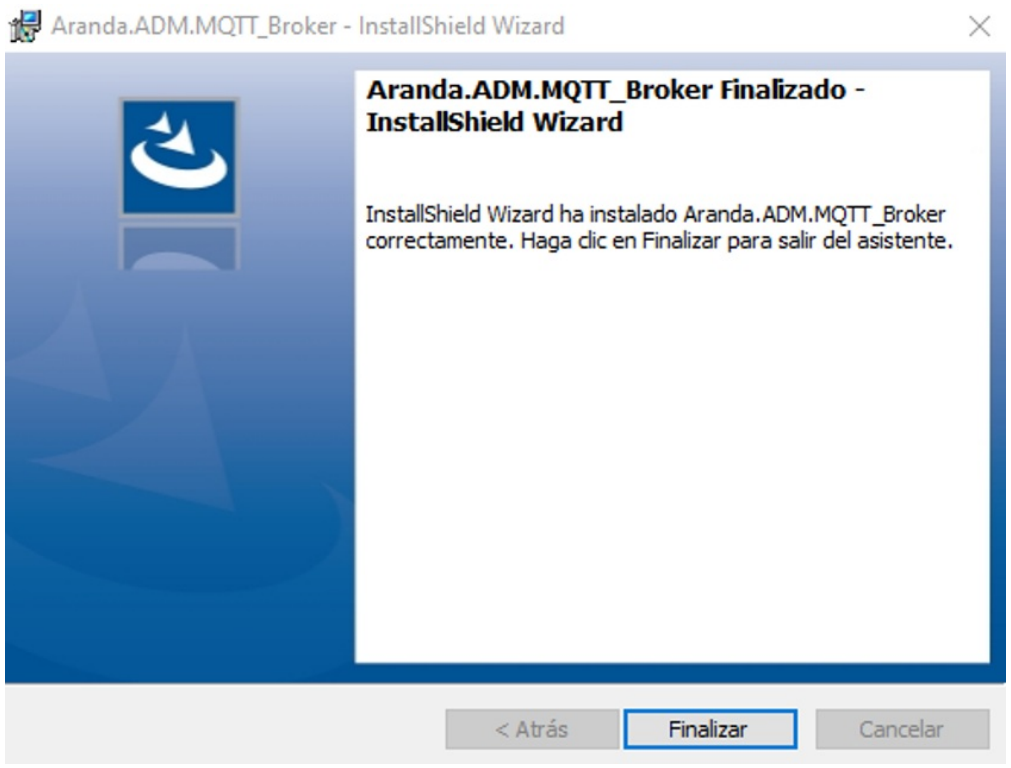




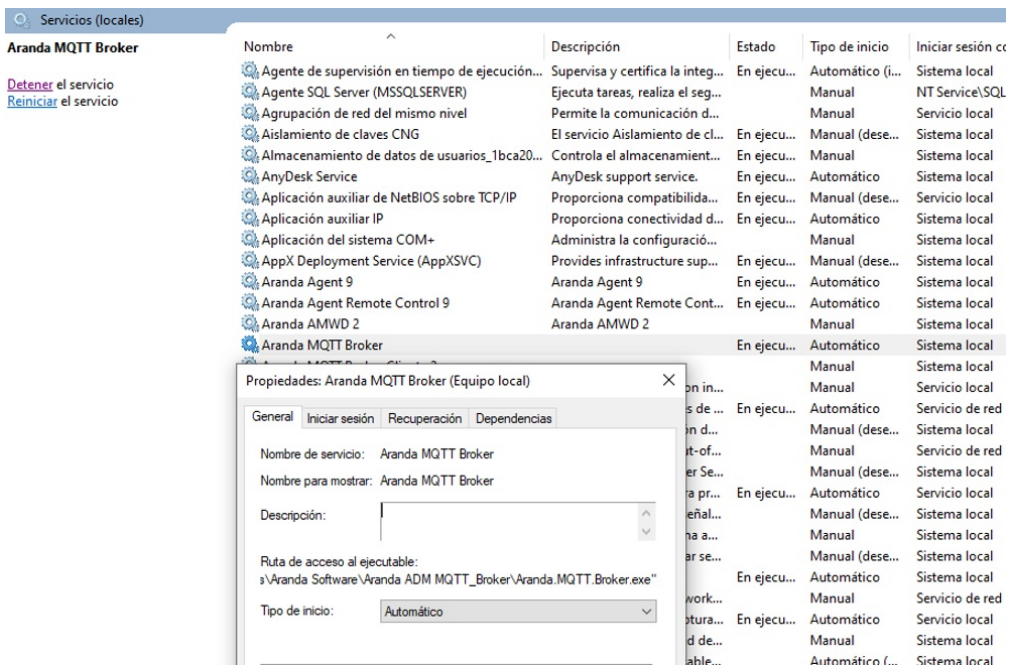
7. Una vez se elija la instalación Completa o Personalizada, haga clic en **Instalar**, se debe tener permisos como administrador de la máquina.



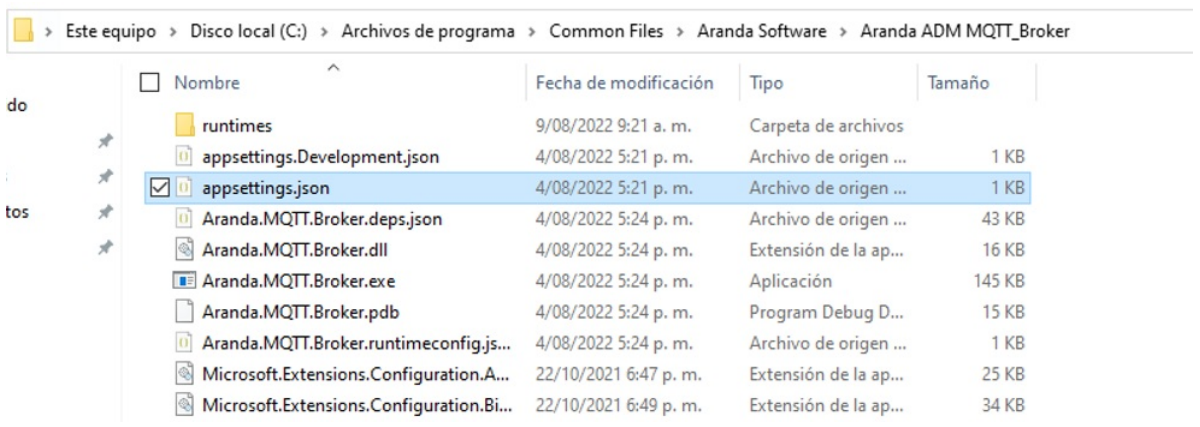
8. Cuando el proceso de instalación termine, haga clic en el botón **Finalizar**.



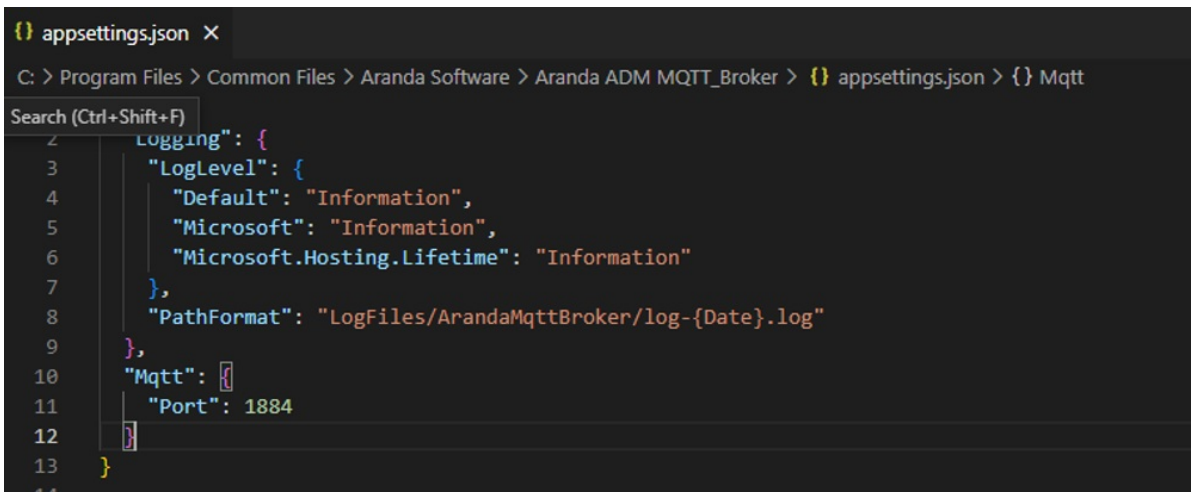
9. Terminado el proceso de instalación diríjase a los servicios y verifique que está instalado y en ejecución el servicio: Aranda MQTT Broker.



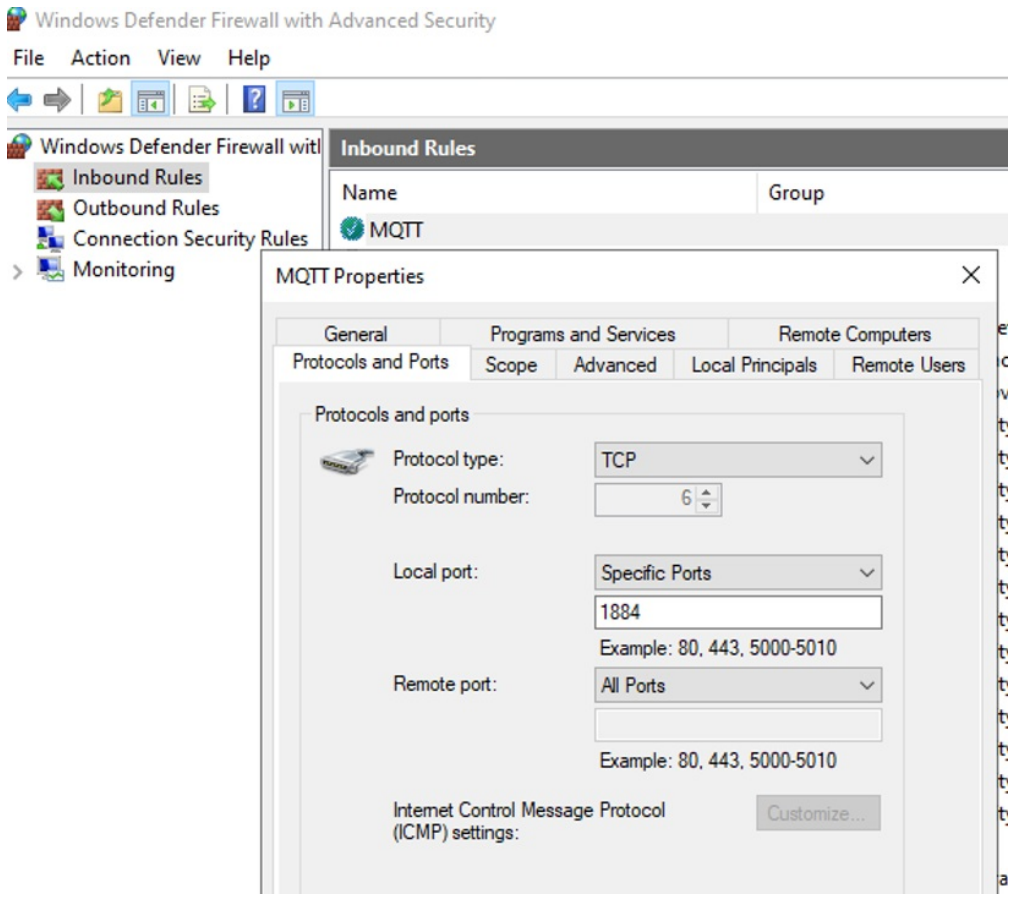
10. Para configurar el puerto que desea exponer, abra el archivo **appsettings.json** que se encuentra en la carpeta donde se encuentra instalado el servicio y realice las siguientes acciones:



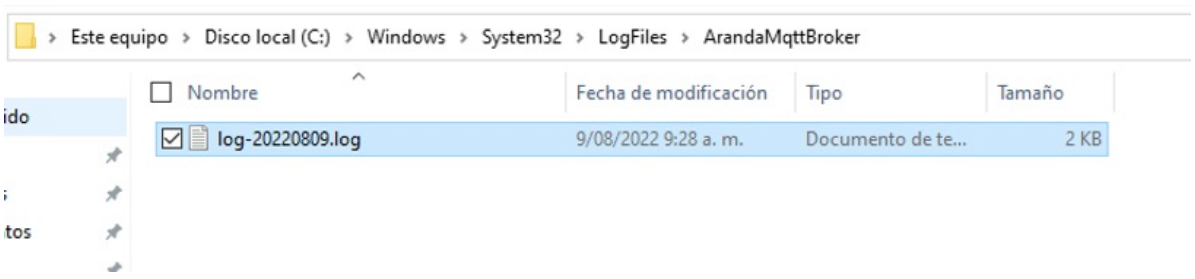
11. Modifique la sección **Mqtt:Port** para cambiar el puerto y reinicie el servicio para aplicar los cambios.



12. En el Windows defender Firewall, seleccione la opción Inbound rules y en las propiedades MQTT, valide que el puerto 1884/1883 está abierto en la máquina.



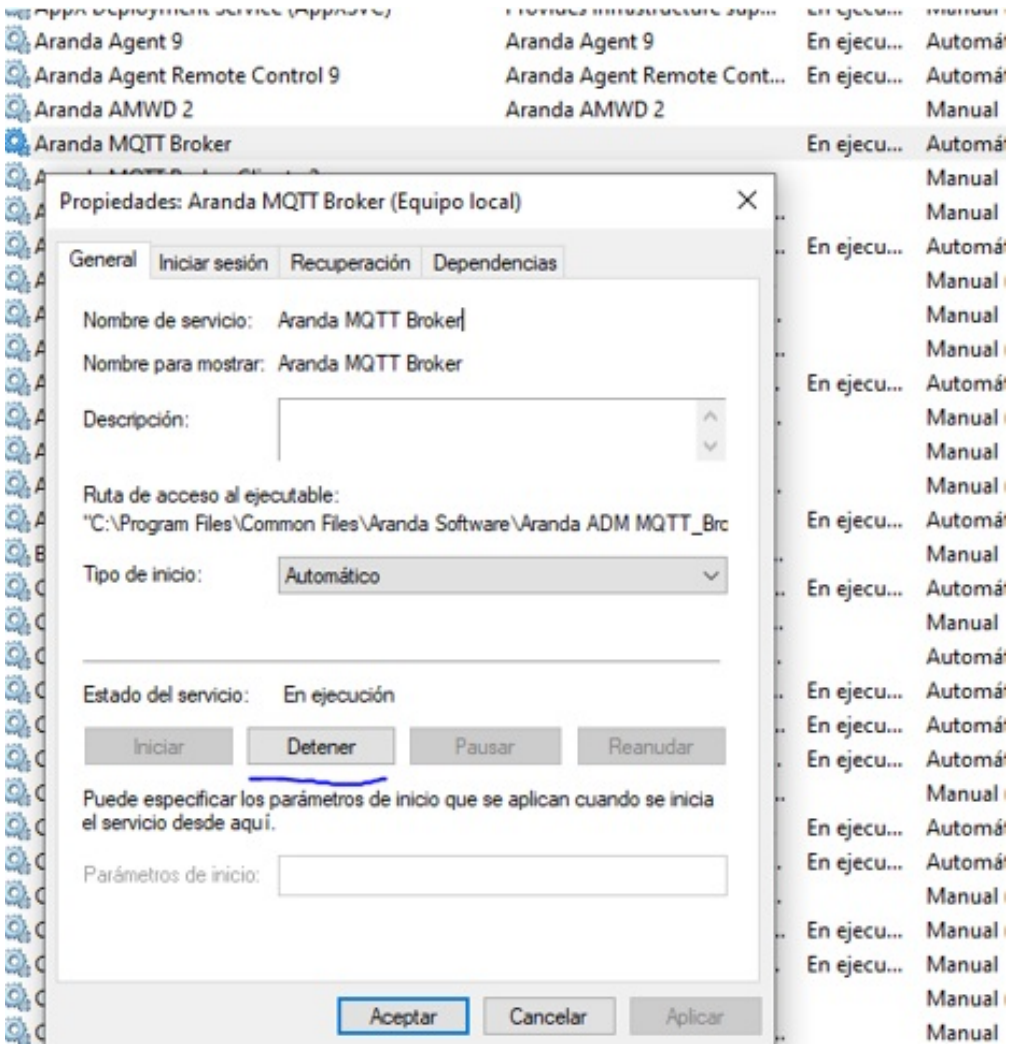
13.los archivos de log quedarán almacenados en la siguiente ruta: C:/Windows/System32/LogFiles/ArandaMqttBroker



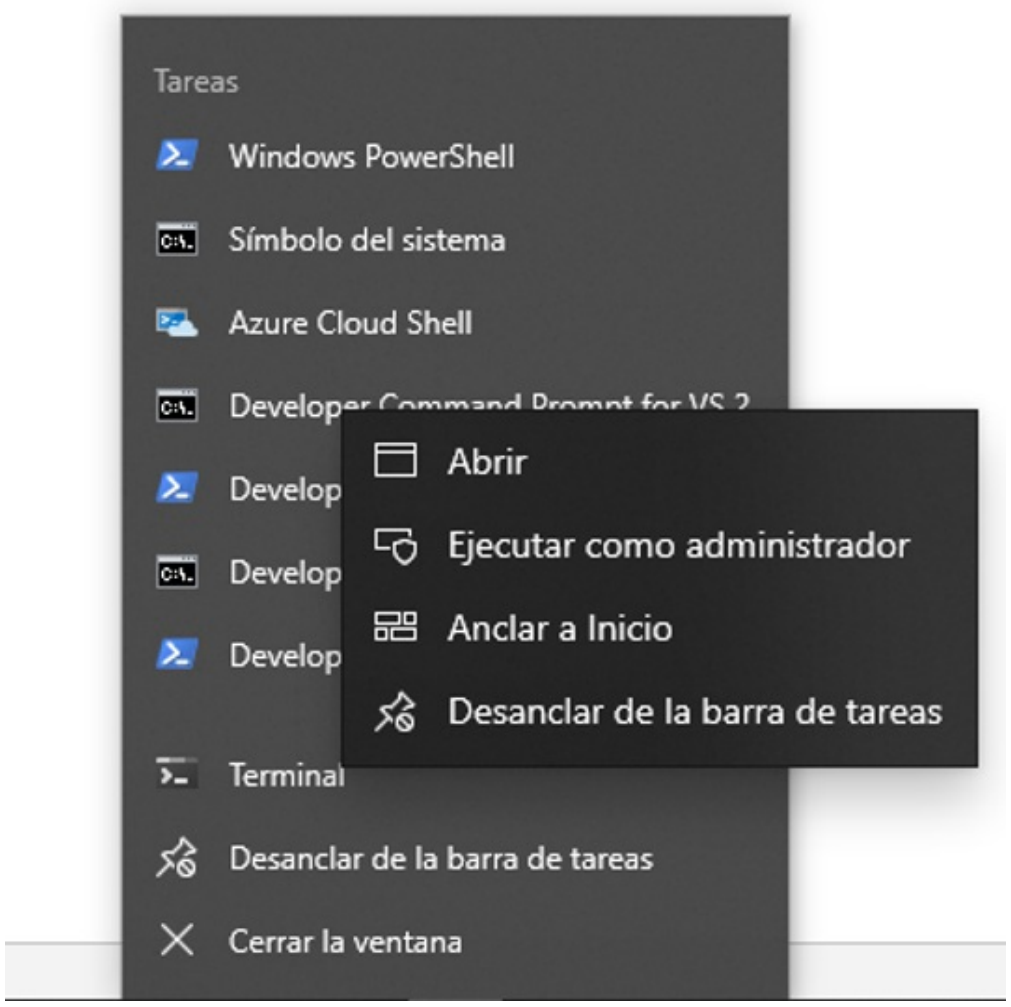
—

Desinstalación Broker MQTT

1. Abra el archivo Aranda MQTT Broker, se habilita la ventana propiedades y en la pestaña **General**, en el estado del servicio, seleccione la opción **Detener** y haga clic en el botón **Aplicar**.



2. Inicie una terminal en modo administrador y ejecute la siguiente información:



3. Ejecute el comando:

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

4. Ejecutado el comando el resultado es el siguiente:

```
[SC] DeleteService CORRECTO
```

5. Revise de nuevo los servicios y no debería estar instalado.

⚐ **Nota:** Se sugiere un numero máximo de 10.000 conexiones (dispositivos) por servidor broker de MQTT.

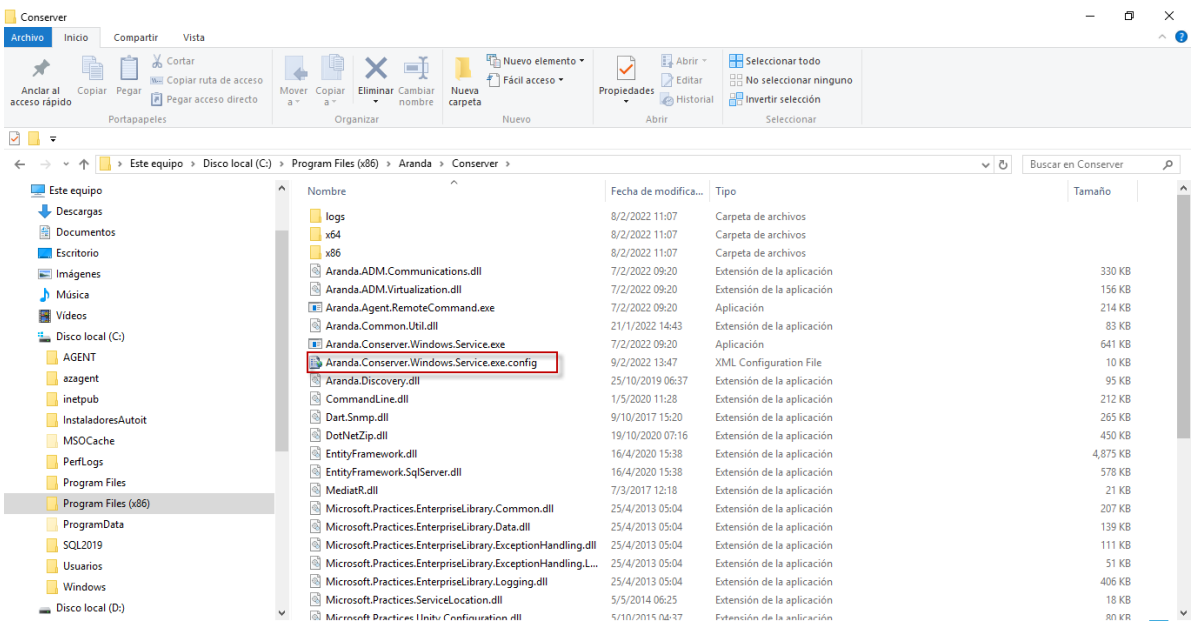
Enlaces Relacionados:
- Configuracion Broker

Configuración Broker

Configuración Broker

Instalador Aranda MQTT Broker

1. Para configurar la comunicación entre el conserver y el Bróker, se debe configurar el archivo "Aranda.Conserver.Windows.Service.exe.config" que está en la carpeta "%Program Files (x86)%\Aranda\Conserver"



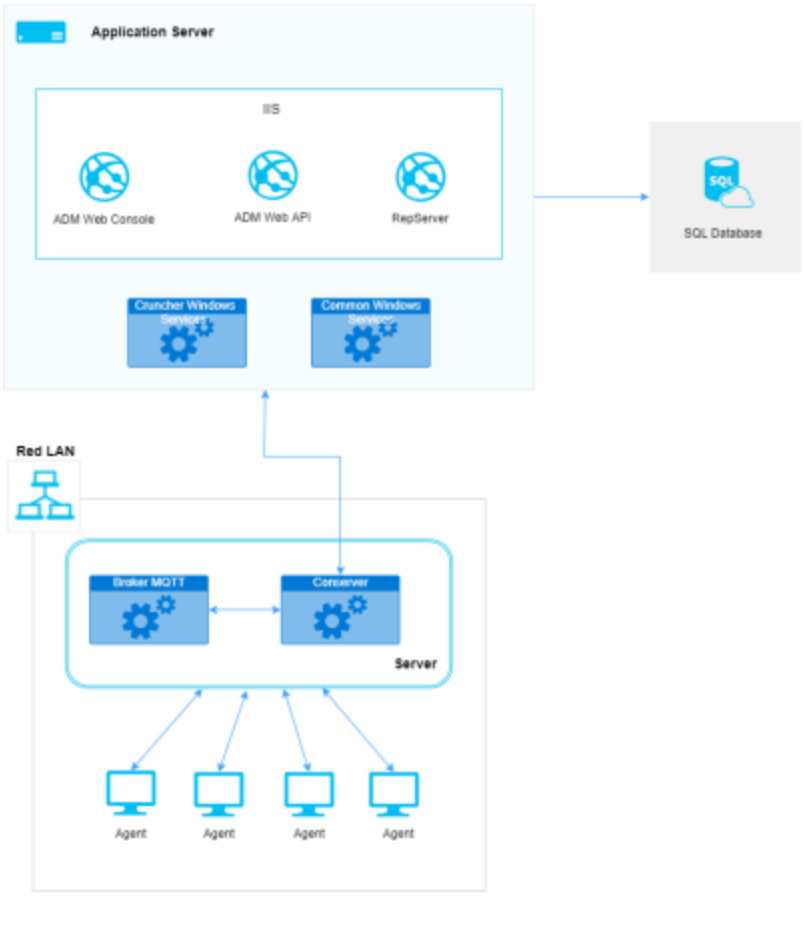
2. Cree los siguientes valores según el puerto parametrizado y la IP del servidor donde se encuentra instalado el bróker.

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

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

}
```

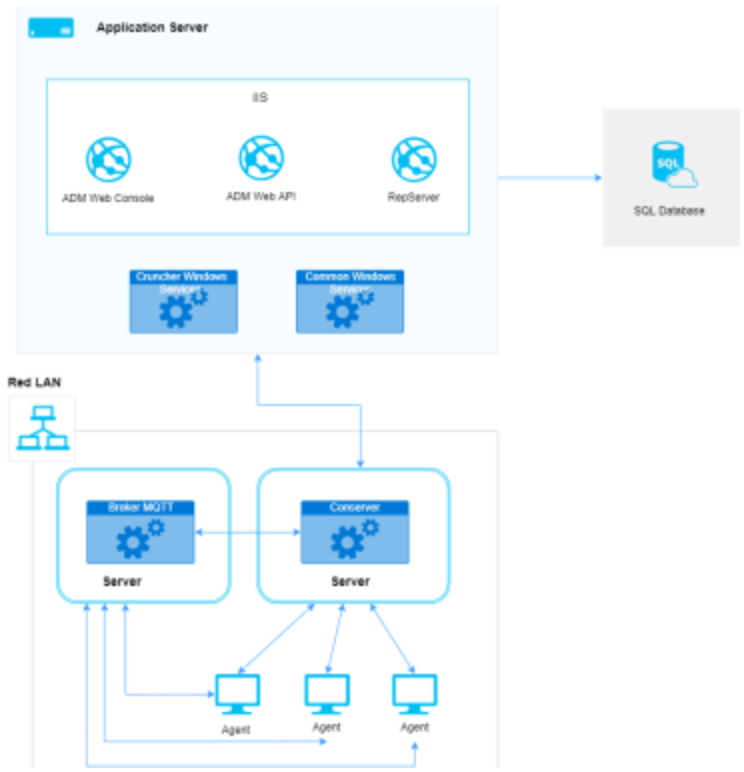
⚐ **Nota:** Al realizar una modificación al archivo de configuración del conserver debe reiniciar el servicio.

Topologias soportadas en ADM con la división del bróker del conserver

- Configuración del broker en el mismo servidor del conserver

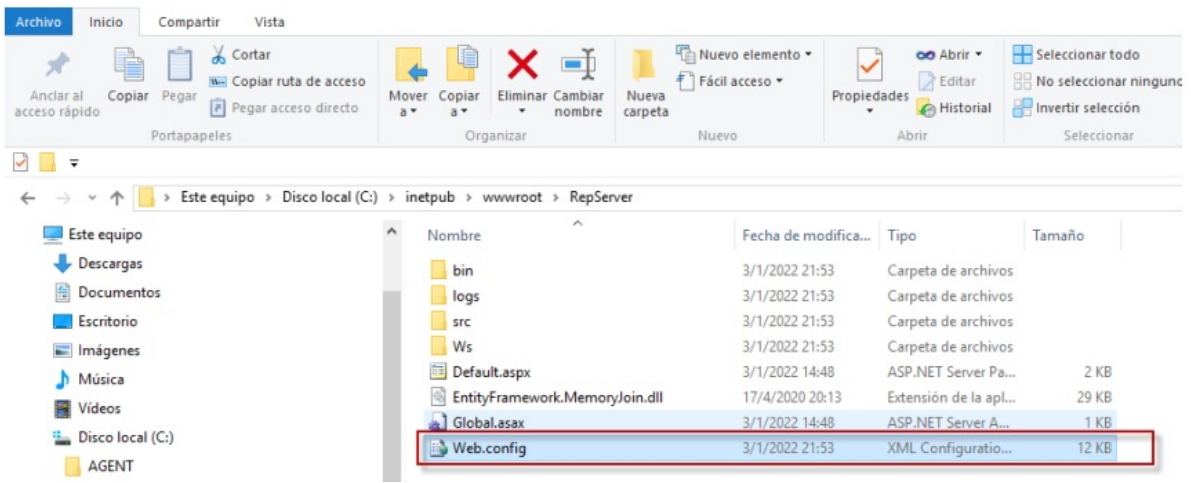


- Configuración del broker en diferente servidor del conserver



Configuración del broker desde el Repserver

1. Para configurar la comunicación entre el repserver directamente con el Broker, debe configurar el archivo **web.config** del repserver que se encuentra en la ruta '%inetpub\wwwroot\RepServer'.



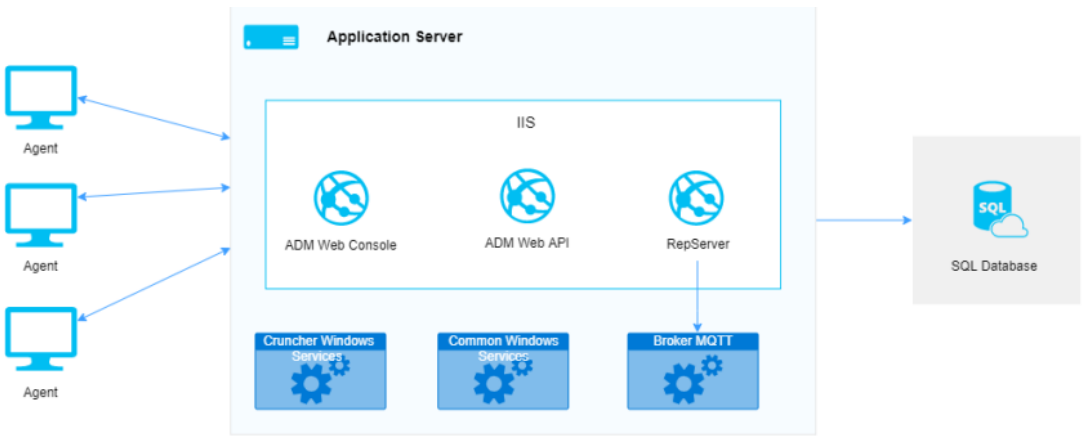
2. Agregue los siguientes valores en < appSettings > según el puerto parametrizado y el host del servidor donde se encuentra instalado el broker.

```
{

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

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

}
```

3. Para que los cambios queden aplicados es necesario reiniciar el dispositivo.

> ⚐ **Nota:** Para configurar el bróker directo hacia el repserver se debe tener en cuenta que, sólo funciona con una versión de agente desde 9.13, y las siguientes funcionalidades no son soportadas en esta arquitectura:
>
> - Descubrimiento.
> - Distribución de agente.
> - Regla de descubrimiento.
> - LDAP- Descubrimiento dispositivos.
> - Virtualización.
> - Monitoreo.

Configuración del broker apuntando directamente al Repserver

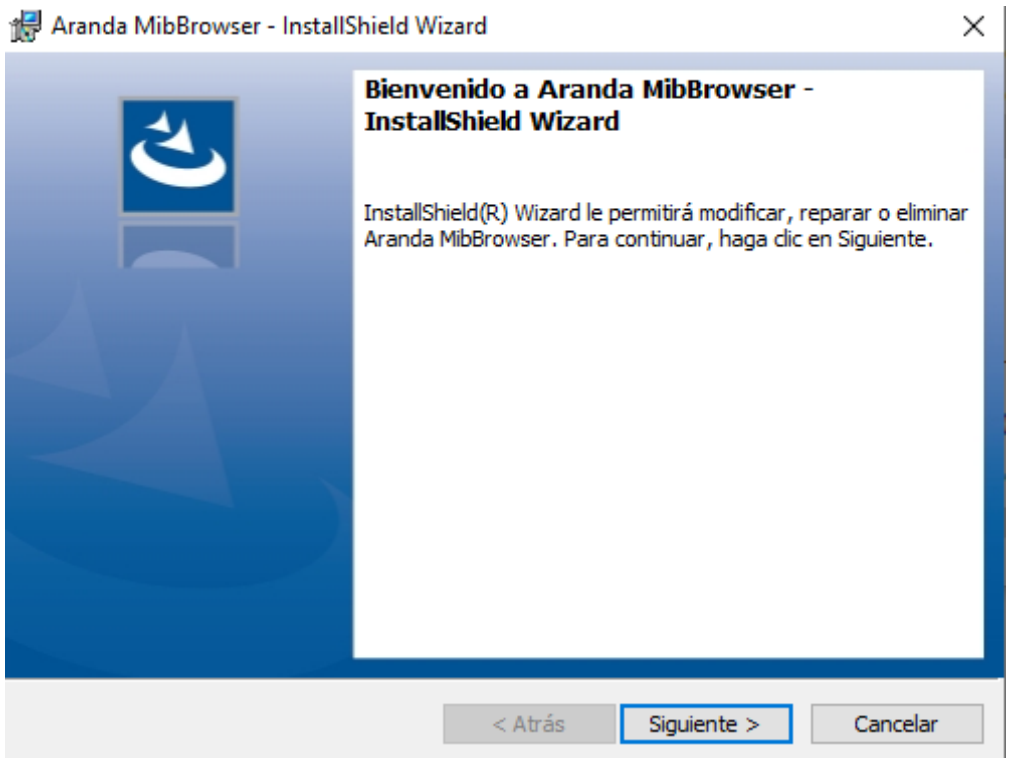


> ⚐ **Nota:** El broker puede o no estár dentro del mismo servidor del repserver.

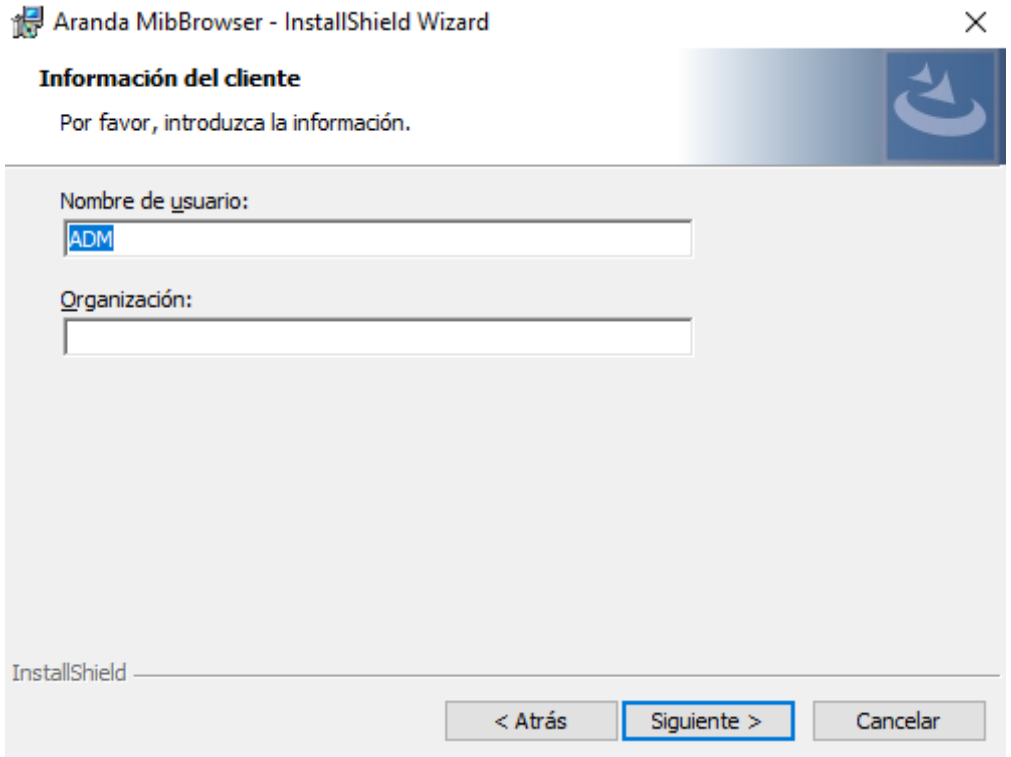
[Instalador Aranda MQTT Broker]

Instalador/Aranda MibBrowser

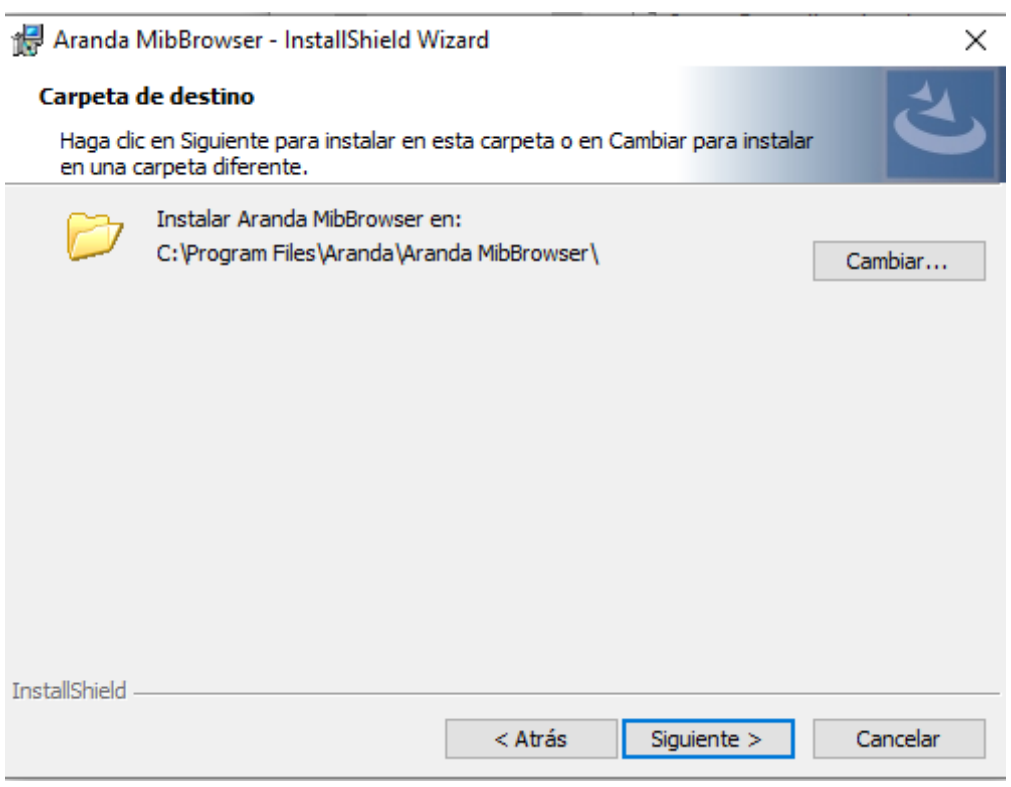
1. Ejecute el instalador Aranda.MibBrowser.exe



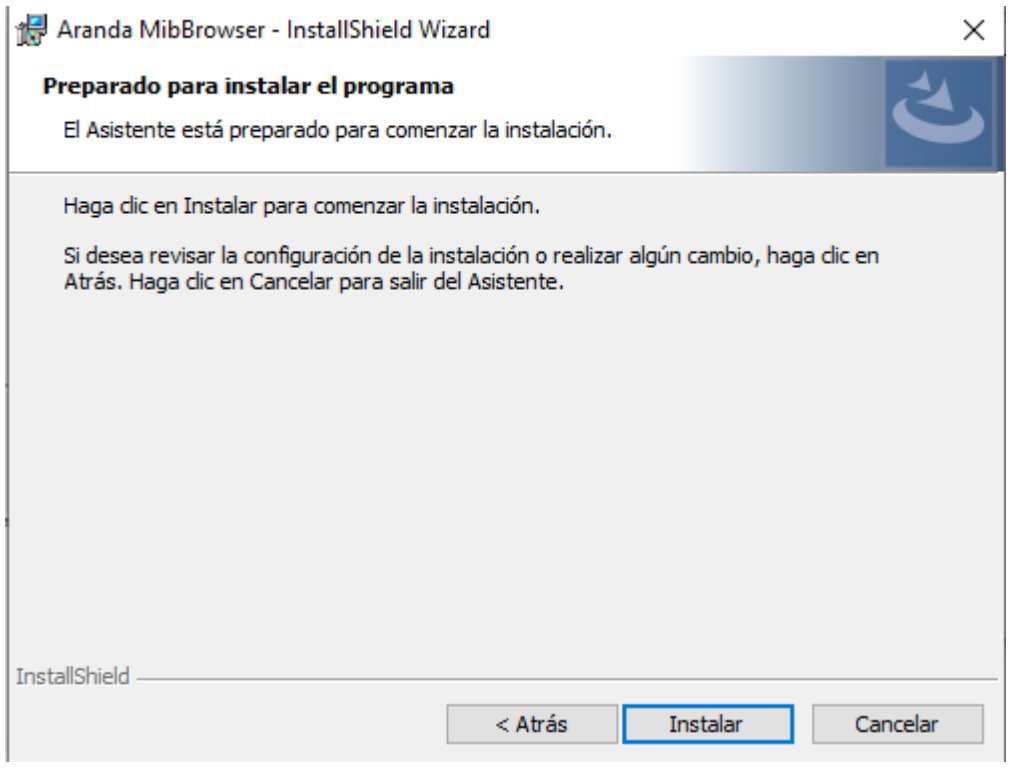
2. Puede definir el nombre de usuario u organización y haga clic en **Siguiente**. Estos campos pueden quedar vacíos..



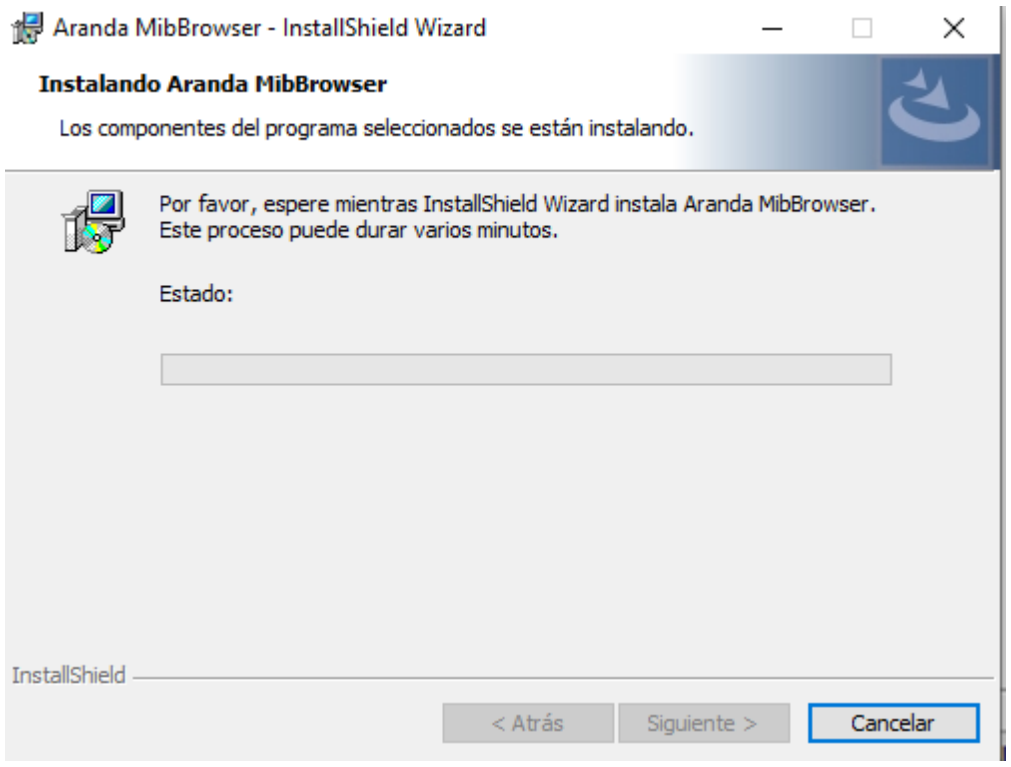
3. El instalador selecciona una ubicación para la instalación o puede cambiarla, luego haga clic en **Siguiente**.



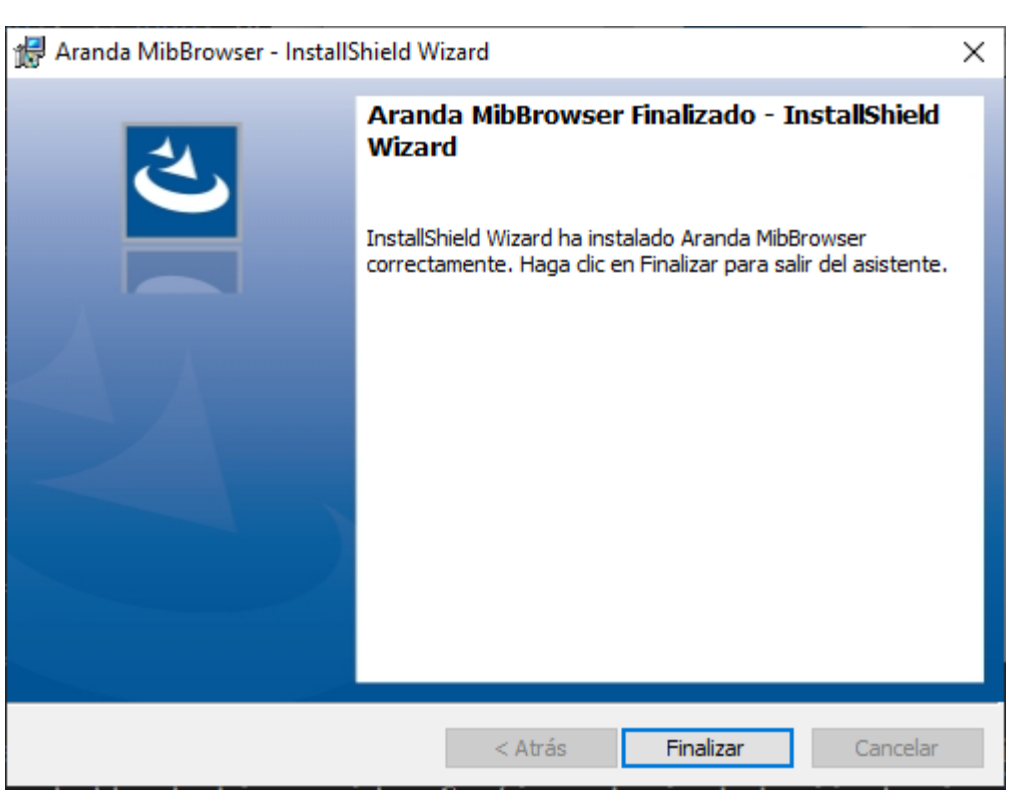
4. Luego procedemos a la instalación haga clic en **Instalar**.



5. Espere mientras el instalador termina el proceso.



6. Confirme la instalación haciendo clic en el botón **Finalizar**.



—

Enlaces Relacionados:
- Utilitario MibBrowser

Configuración Mib Browser

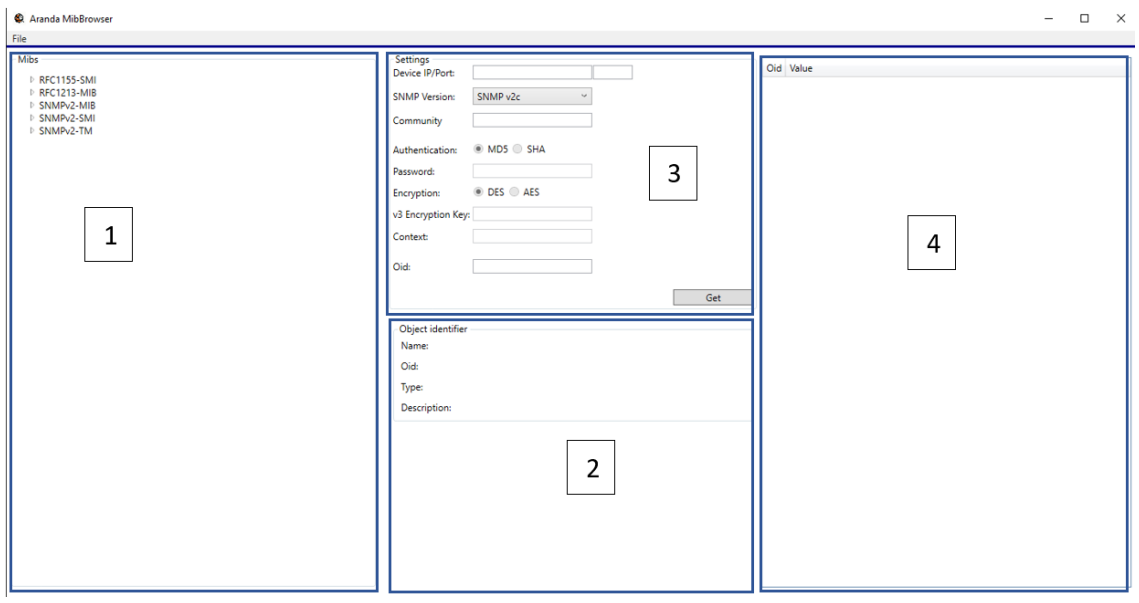
Configuración MibBrowser

« Instalador Aranda MibBrowser

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.

Cuando se inicia la aplicación se pueden identificar las siguientes secciones

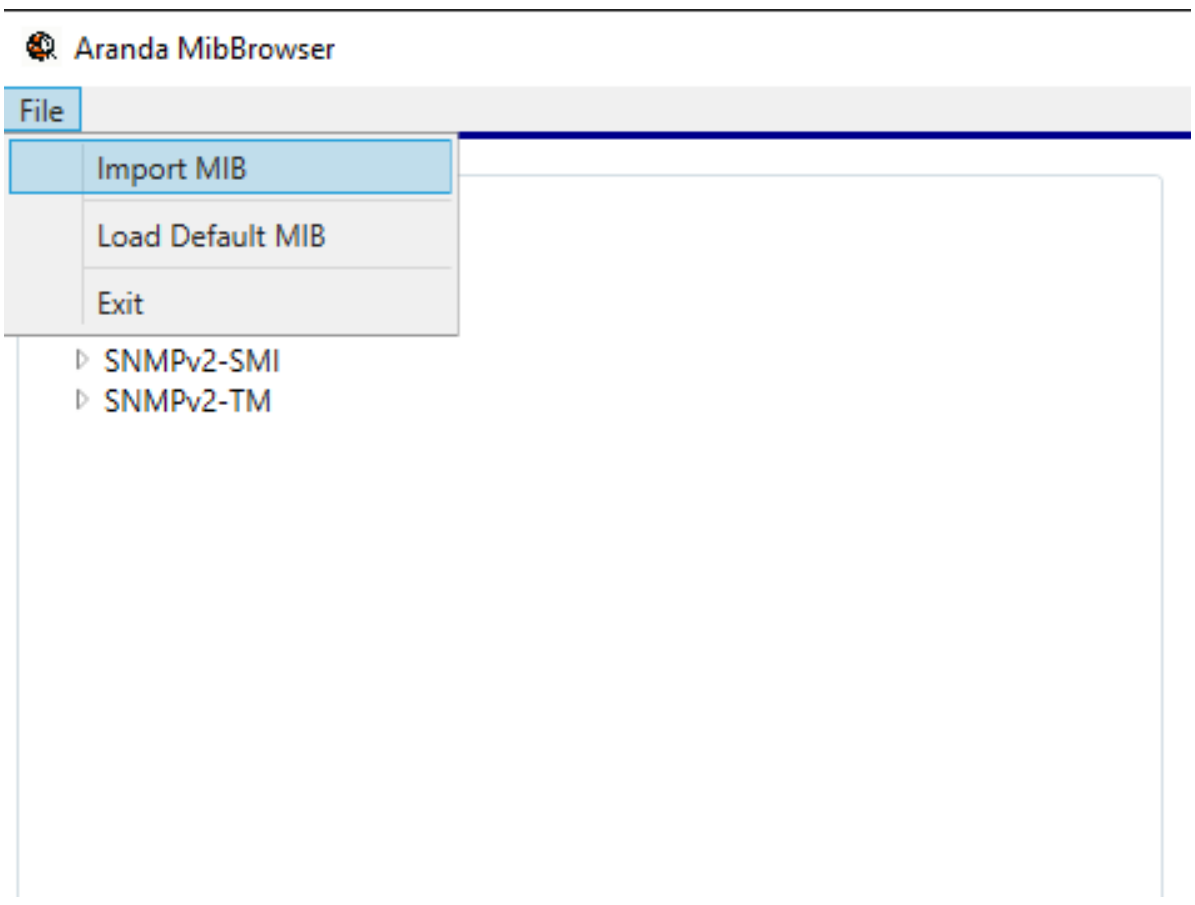
1. Mibs
2. ObjectIdentifier
3. Settings
4. Oid-Value



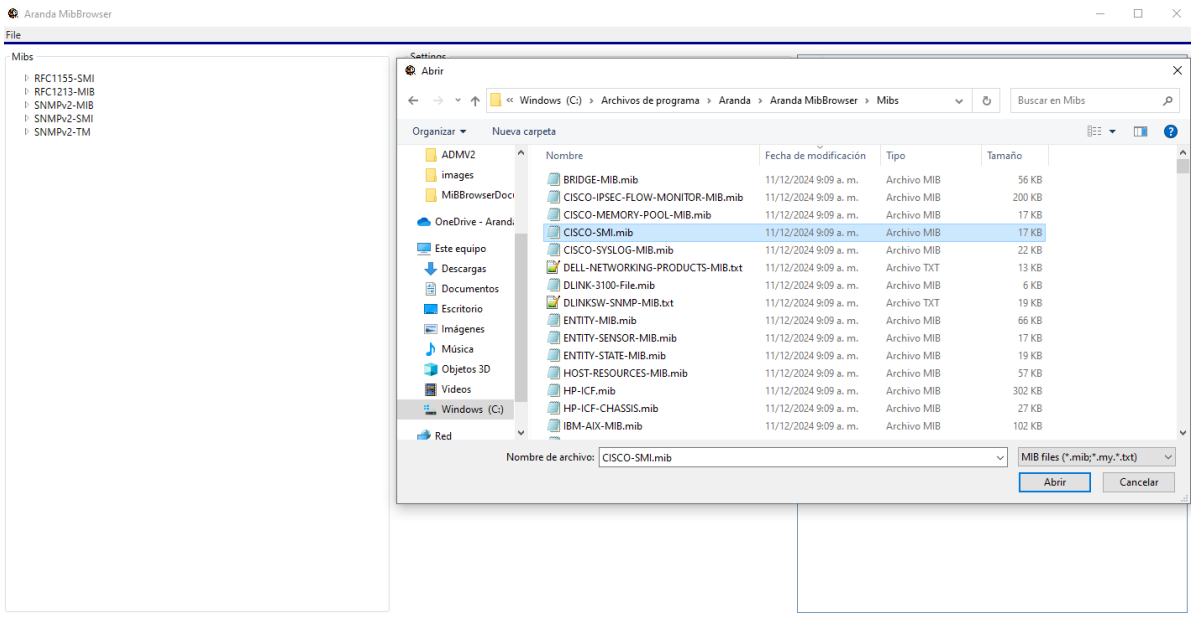
1. Los MIBs inicialmente compilados son los siguientes MIBs:

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

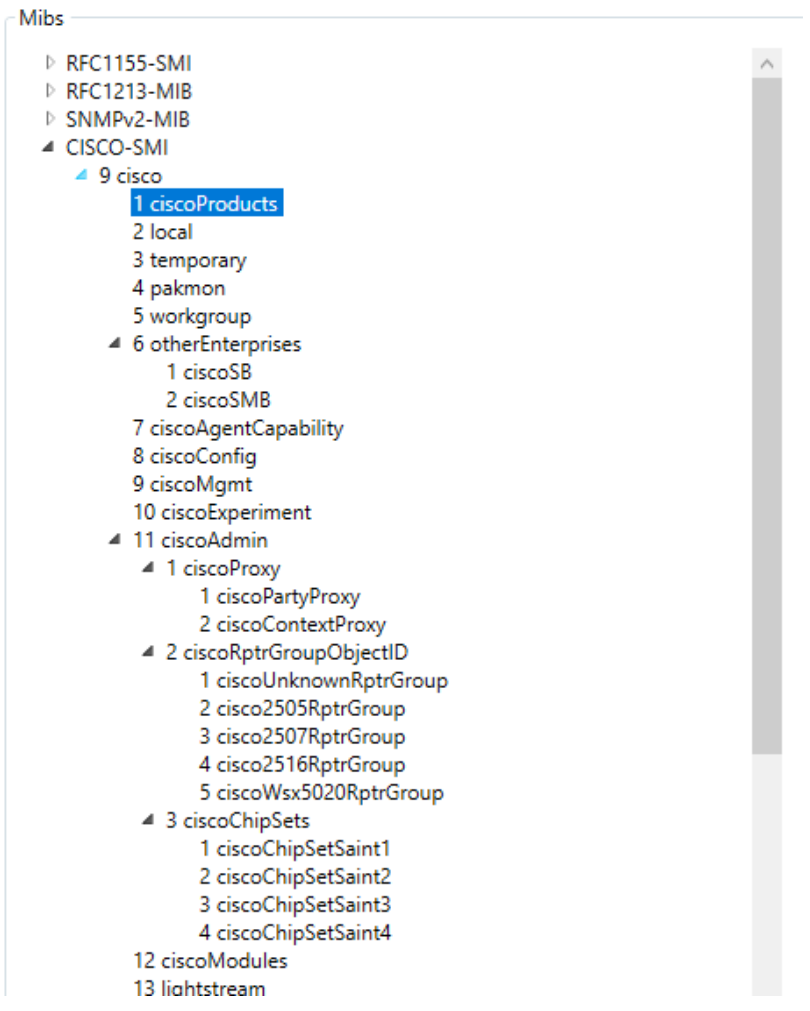
Si desea compilar otro MIB puede hacerlo a través de la opción de menú



Cuando cargue el MIB de manera correcta observara el árbol con todos los MIBS relacionados, para el ejemplo usamos el MIB CISCO-SMI.mib

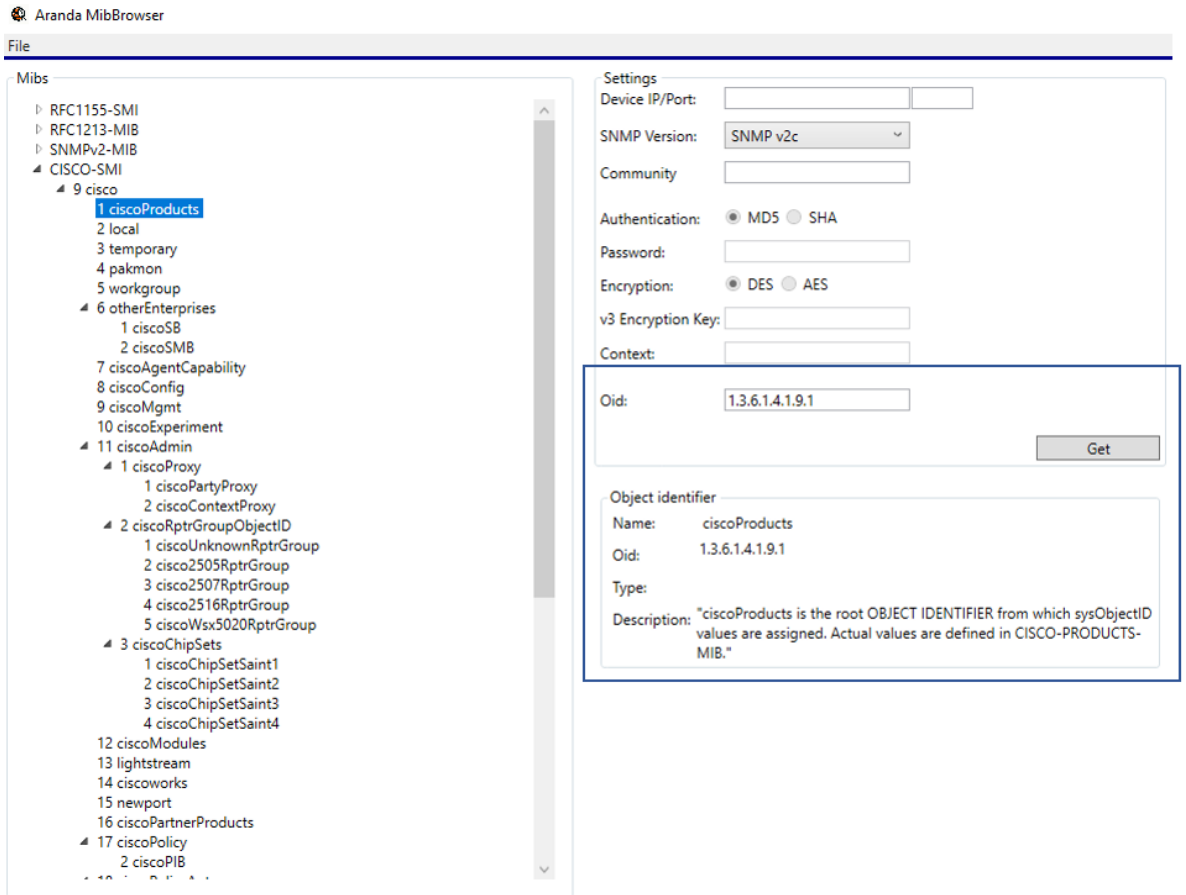


Consultamos el árbol de MIBS

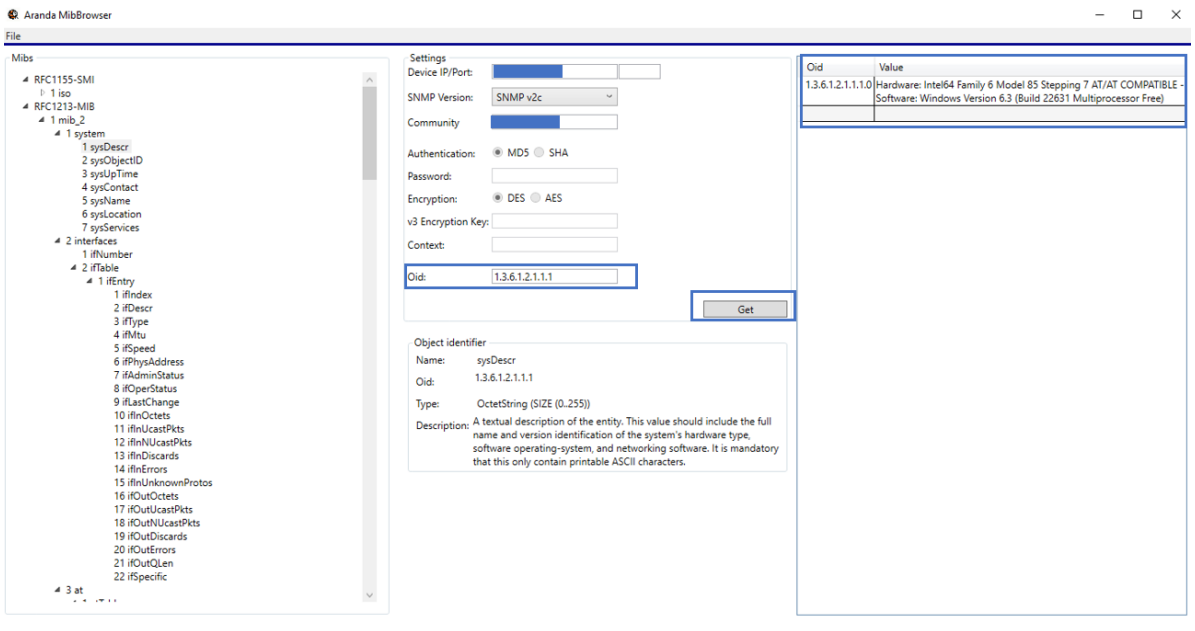


⚐ **Nota:** Un MIB suele tener dependencias las cuales se recomienda subirlo junto a su MIB principal o copiar de manera manual en el **directorio de instalación del MibBrowser** en la carpeta **MIBS**, ya que es la ruta donde el aplicativo consulta para tratar de resolver las dependencias de manera automática.

2. Cuando cargue un MIB puede ver los OID relacionados, si selecciona un nodo puede ver la información en la sección de Object Identifier



3. Para consultar un OID puede diligenciar el formulario con los datos requeridos luego presionar el boton Get y si existe información se mostrara en la sección OID y value.



⚐ **Nota:** Tenga en cuenta que el OID ingresado debe ir relacionado al dispositivo.

« Instalador Aranda MibBrowser

Control Remoto

Permite tomar el control de las máquinas de manera sencilla y eficiente y transferir archivos de manera conveniente, facilitando la gestión a distancia de las estaciones de trabajo.

⚐ **Nota:** Esta funcionalidad no es soportada en instalaciones OnPremises de ADM versiones inferiores a 9.21.1

Instalador/Control Remoto

Los agentes de Windows de ADM desde la versión de ADM 9.19.2, después de realizar la instalación de cero o una actualización desde de una versión anterior, se instalará automáticamente el nuevo componente de control remoto transcurrido 30 minutos. Se visualizan los siguientes procesos y servicios en el dispositivo.

⚐ **Nota:** En caso de presentarse alguna falla de conexión al momento de la instalación o actualización del componente de control remoto, el agente de ADM realizará reintentos de instalación cada 4 horas.

Procesos y servicios componente de control remoto

Actualización componente de control remoto

Instalador/Visor Soporte Remoto Especialista

Instalacion visor control remoto

Configuración Control Remoto

Proceso de Configuración Control Remoto

Debe tener en cuenta los siguientes pasos para la configuración del control remoto en instalaciones OnPremise:

- Habilitar la funcionalidad realizando un update a la base de datos del producto de ADM

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

- Relizar la configuración correspondiente posterior a la instalación de **Aranda.ADM.Web.Installer** en el servidor de aplicaciones. Ver configuración

Configuración e Instalación de Agentes

Tenga en cuenta los siguientes pasos para la configuración e instalación de los agentes de control remoto:

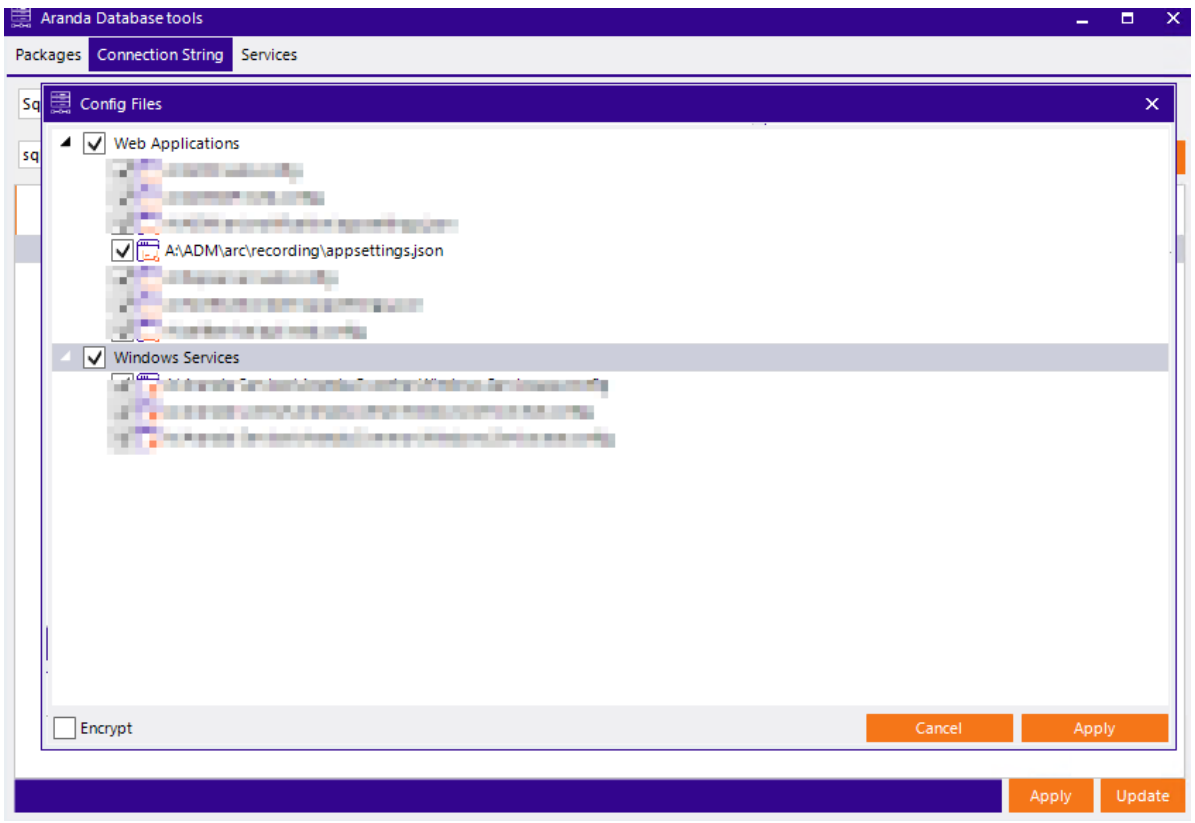
- Para realizar control remoto se requiere tener la instalación del componente de control remoto en los dispositivos a los cuales se va a realizar la conexión remota.Instalación componente de control remoto
- Instalación del visor de control remoto, requerido en el dispositivo desde donde se realiza la conexión remota Instalación visor soporte remoto especialista

Configuración Control Remoto

Después de instalar el archivo **Aranda.ADM.Web.Installer** realice las configuraciones posteriores en el servidor de la aplicación y desde la consola de ADM para garantizar el correcto funcionamiento del nuevo control remoto, teniendo en cuenta los siguientes pasos:

1. Configurar cadena de conexión

Configure la cadena de conexión para el sitio de grabaciones, a través del módulo Aranda Database Tools v9. Los sitios de notificaciones no requieren configurar cadena de conexión.



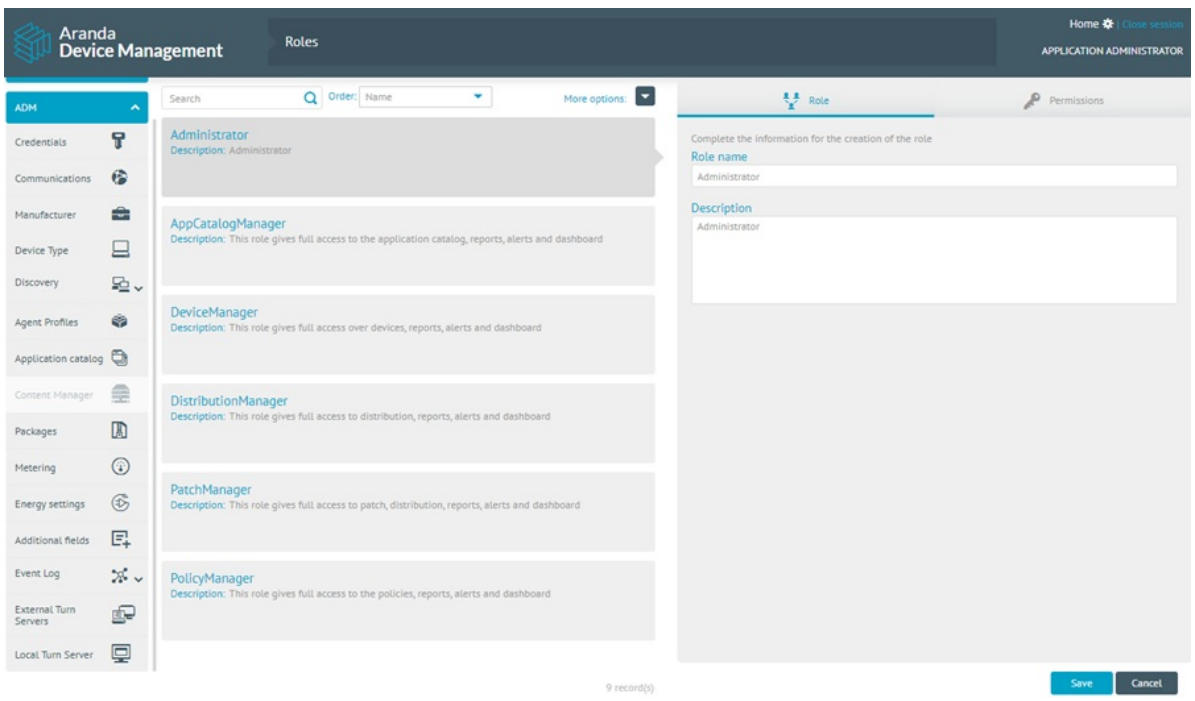
⚐ Notas:

- Cuando se aplique la configuración con el Encrypt habilitado se podrá visualizar un mensaje de alerta porque la encriptación no está soportada para archivos JSON.
- Al realizar cambios en la cadena de conexión de servidor de grabaciones reinicie el IIS para que los cambios se apliquen deforma correcta.
- Si, posterior a la configuración, se realizan cambios en el proveedor de almacenamiento, mueva la información contenida en el proveedor anterior al actual. Si no se realiza esta acción, las actualizaciones de los agentes no se realizarán de forma correcta y no podrá acceder a las grabaciones en las auditorías..

2. Ingresar a la consola

Ingrese a la consola de ADM con el usuario con los permisos requeridos para gestionar las opciones de Servidores Turn externos y Servidor Turn local en la Configuración de ADM.

⚠ **Importante:** Las opciones de Turn Externo y Local están disponibles únicamente en instalaciones On Premise.



3. Servidores Turn Externos

La funcionalidad de transferencia de archivos del control remoto utiliza un protocolo P2P basado en WebRTC. Cuando dos dispositivos no pueden establecer una conexión directa entre sí, se necesita un servidor Turn para facilitar la comunicación.

Para agregar un servidor Turn externo en la ventana de **Servidores Turn Externos**, siga estos pasos:

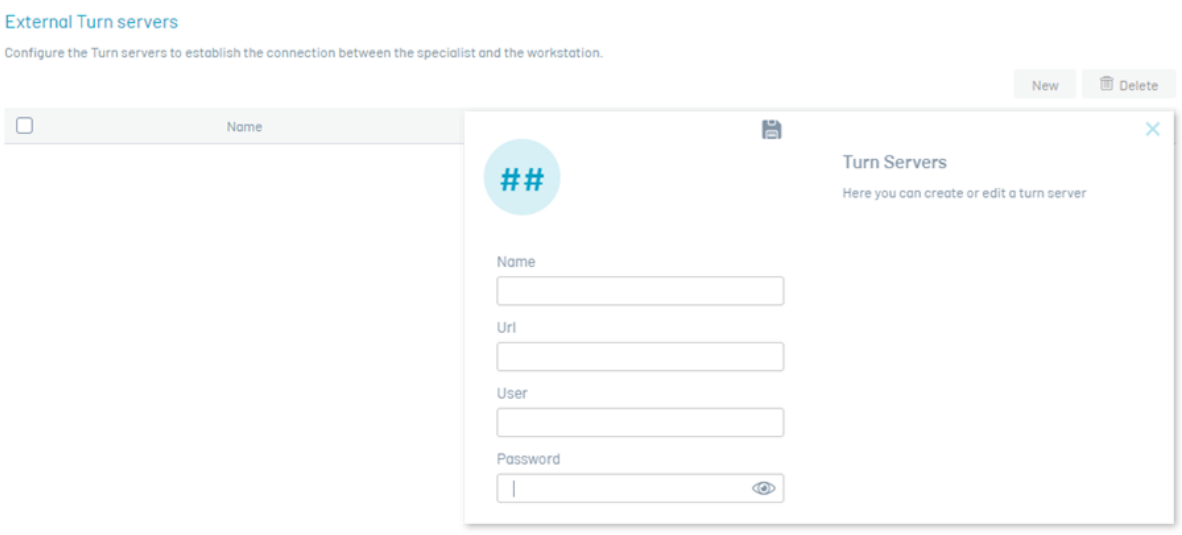
A. Haga clic en la opción **Nuevo**.

B. Complete los campos solicitados de acuerdo a la siguiente tabla:

Campo	Descripción
Nombre	Nombre que se le desea asignar a la configuración, entre 6 y 50 caracteres.
URL	Corresponde al sitio del servidor STUN/TURN, por ejemplo: turn:<server_public_ip>:puerto o stun:<server_public_ip>:puerto .
Usuario	Nombre del usuario autorizado para conectar al servidor STUN/TURN.
Contraseña	Contraseña asociada al usuario que permite la conexión con el servidor STUN/TURN.

C. Finalice haciendo clic en el botón **Guardar**.

⚐ **Nota:** Esta configuración es requerida para la transferencia de archivos cuando el agente especialista y el agente de la estación de trabajo no están en la misma red, por lo tanto, se debe permitir la salida a Internet de ambos dispositivos por el puerto configurado.



El usuario puede registrar la cantidad de servidores Turn externos que considere necesarios para tener una buena comunicación entre los dispositivos del especialista y la estación de trabajo a través de la consola de ADM.

Para eliminar un servidor Turn externo, en la ventana **Servidores Turn Externos** seleccione el o los servidores a eliminar y haga clic en el botón **Eliminar**, se confirmará que el o los servidores se han sido eliminada exitosamente.

Se pueden utilizar STUN/TURN WebRTC públicos, realizando una búsqueda en la web “STUN server list” se podrán listar los diferentes servidores STUN/TURN públicos disponibles. Al configurar servidores públicos en las estaciones de trabajo y en los equipos especialistas deben permitir la salida hacia los sitios de los servidores que se configuren. También es posible configurar el servidor STUN/TURN provisto en el instalador realizando los ajustes en el servicio Aranda Turn Stun WebRTC Server Windows Service. Además, se pueden utilizar STUN/TURN públicos junto con servidores propios instalados, como se mencionó anteriormente.

4. Servidor Turn Local

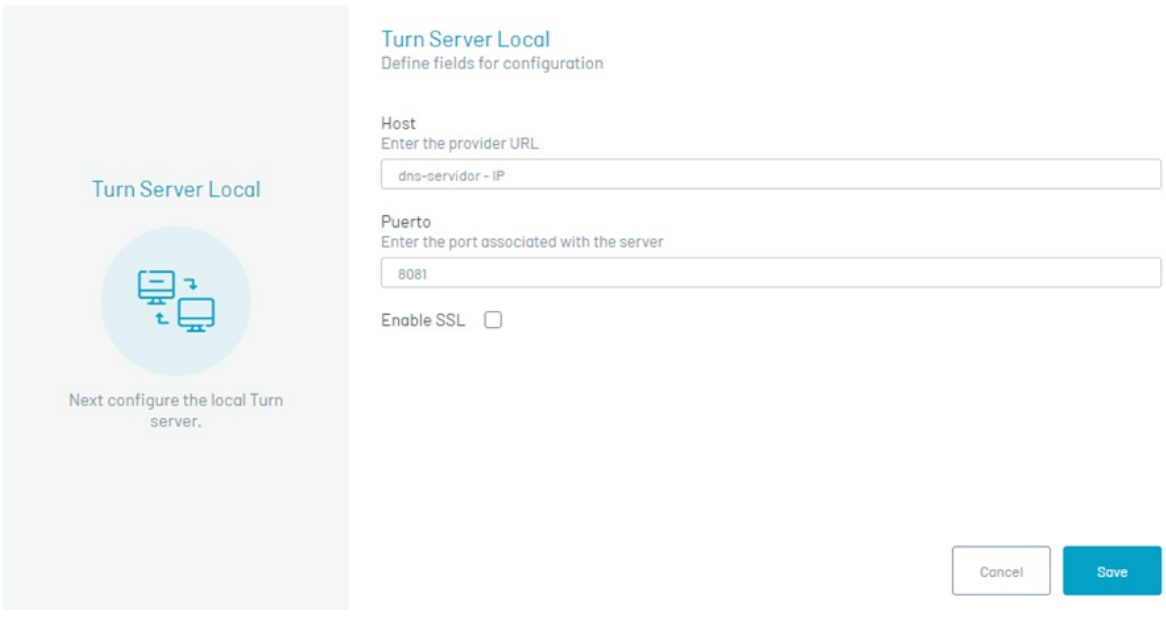
Para establecer la comunicación de toma de control remoto entre el agente especialista y el agente de la estación de trabajo, utilice un servidor Turn local que puede retransmitir el tráfico de red.

Para agregar un servidor Turn local, siga estos pasos:

A. Haga clic en la opción **Servidor Turn local** del menú principal.

B. Complete el campo **Host** con la ruta de acceso al servidor local, que puede ser la IP del servidor o el DNS. El campo **Port** esta configurado por defecto con el valor 8081 y el SSL inactivo; si se cambia el puerto o se activa el SSL realice los ajustes en el servicio Aranda Turn Server instalado en el servidor.

C. Finalice haciendo clic en el botón **Guardar**



Configuración Manual de Servicios

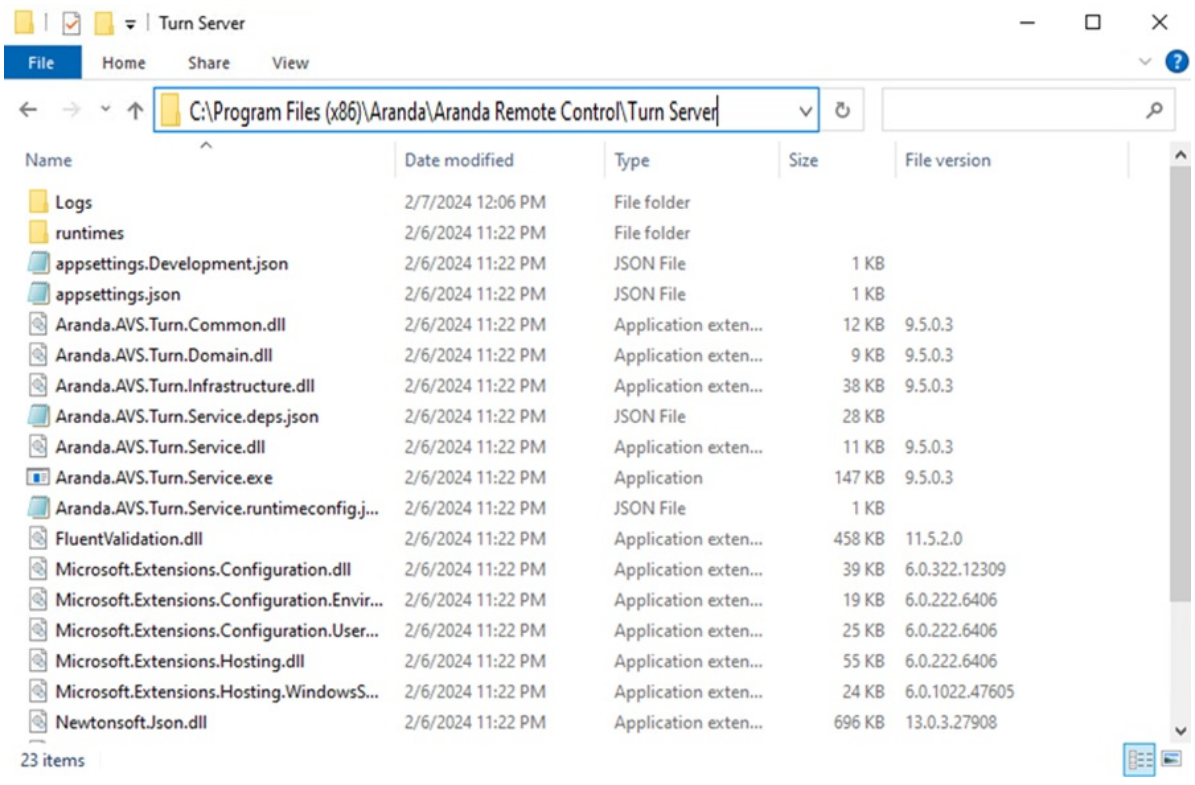
Configuración Turn Server

Después de instalar el servicio Aranda Turn Server, no es necesario realizar ningún ajuste para su funcionamiento. Sin embargo, se pueden realizar parametrizaciones según las necesidades específicas, como cambiar el puerto de conexión (8081 por defecto) y habilitar el SSL (deshabilitado por defecto). Si necesita realizar estas parametrizaciones, siga los siguientes pasos:

1. Validación del Archivo appsettings.json

Antes de realizar cambios, verifique el archivo **appsettings.json** ubicado en la ruta de instalación del servicio (por defecto: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) para asegurarse de que el puerto esté configurado por defecto en 8081. Si no es necesario modificar el puerto, no es necesario realizar más ajustes.

Adicionalmente valide que el puerto 8081 esté habilitado en las reglas del firewall local para garantizar el flujo correcto del tráfico. En este archivo, también puede encontrar la configuración para los certificados SSL, que por defecto se encuentra desactivada (**IsSsl=false**).



Configuración por defecto de appsettings.json:

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

```
  "TurnConfiguration": {
    "CertificateParam": "",
    "CertificatePath": "",
    "CertificateSubject": "",
    "IsSsl": false,
    "Port": 8081,
    "SSLProtocols": "Tls12"
  }
}
```

2. Cambio de Configuración del Puerto

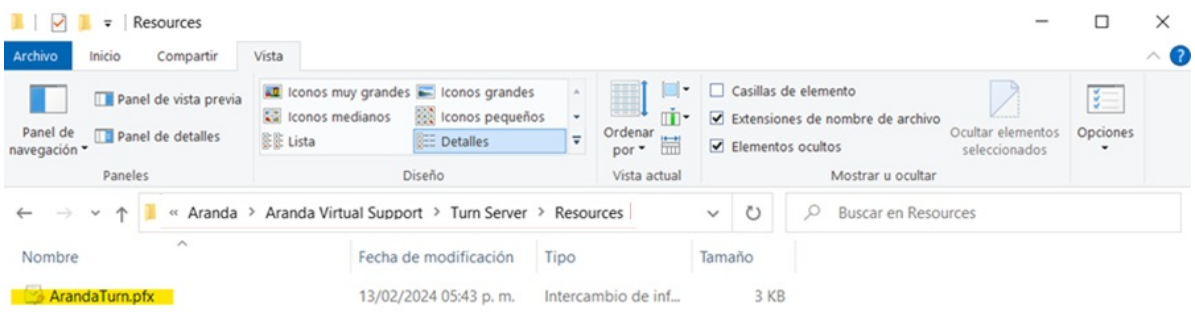
Edite el archivo *appsettings.json* y configure el puerto deseado reemplazando <puerto> por el número de puerto deseado.

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

3. Configuración de conexión segura SSL

Edite el archivo appsettings.json, cambie "IsSsl" a true. Para agregar el certificado SSL hay dos alternativas:

3.1. Adquirir o generar un certificado PFX, el cual deberá ser ubicado dentro de la carpeta **Resources** (la carpeta se debe crear si no existe) en la ruta de instalación del servicio.



El nombre del archivo se registra en la opción **CertificatePath** y la clave codificada en base 64 de generación del certificado se debe registrar en **CertificateParam**, ambas opciones disponibles en el archivo appsettings.json.

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

3.2. Si tiene almacenado un certificado PFX en el depósito de certificados, puede configurarlo mediante el nombre del mismo en la opción **CertificateSubject** del archivo appsettings.json.

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

4. Reinicio del Servicio

Reinicie el servicio del Turn Server (Aranda Turn Server Windows Service) para que los cambios en la configuración surtan efecto. El servicio ahora debería escuchar en el nuevo puerto configurado y habilitar el uso de certificado SSL.

5. Configuración del Firewall

Abra el puerto que se configuró en el paso 2 en las reglas de entrada del firewall local. Este paso es crucial para permitir el tráfico a través del nuevo puerto y asegurar que el Turn Server pueda recibir conexiones entrantes en el puerto configurado.

Parametrizar el puerto del Turn Server y el uso de SSL desde el servicio es un proceso fundamental para garantizar su correcto funcionamiento y adaptarlo a las necesidades específicas de cada cliente. Siguiendo estos pasos, puede asegurarse de que el Turn Server esté configurado correctamente y listo para manejar las conexiones según lo requerido.

Configuración Servidor Stun/Turn WebRTC

Después de instalar el servicio **Aranda Turn Stun WebRTC Server**, es necesario realizar la configuración para que este pueda funcionar correctamente.

1. Validación del Archivo turn-server.toml

Antes de realizar cambios, verifique que el archivo **turn-server.toml** se encuentre ubicado en la ruta de instalación del servicio (por defecto: C:\Program Files (x86)\Aranda\Aranda Remote Control\Stun Server).

turn-server.toml C:\turn-server.toml

```toml
[turn]
# turn server realm
#
# specify the domain where the server is located.
# for a single node, this configuration is fixed,
# but each node can be configured as a different domain.
# this is a good idea to divide the nodes by namespace.
realm = "localhost"

# turn server listen interfaces
#
# The address and port to which the UDP Server is bound. Multiple
# addresses can be bound at the same time. The binding address supports
# ipv4 and ipv6.
[[turn.interfaces]]
transport = "udp"
bind = "127.0.0.1:3478"
# external address
#
# specify the node external address and port.
# for the case of exposing the service to the outside,
# you need to manually specify the server external IP
# address and service listening port.
external = "127.0.0.1:3478"

[[turn.interfaces]]
transport = "tcp"
bind = "127.0.0.1:3478"
external = "127.0.0.1:3478"

[api]
# controller bind
#
# This option specifies the http server binding address used to control
# the turn server.
#
# Warn: This http server does not contain any means of authentication,
# and sensitive information and dangerous operations can be obtained
# through this service, please do not expose it directly to an unsafe
# environment.
bind = "127.0.0.1:3000"

# web hooks url
#
# This option is used to specify the http address of the hooks service.
#
# Warn: This http server does not contain any means of authentication,
# and sensitive information and dangerous operations can be obtained
# through this service, please do not expose it directly to an unsafe
# environment.
```

Para configurar el servicio STUN/TURN WebRTC, utilice el archivo turn-server.toml:

- **Sección [turn]:** Especifica el dominio donde se encuentra el servidor.
- **Sección [[turn.interfaces]]:** Indica las interfaces de escucha. Describe la interfaz a la que está vinculado el servidor STUN/TURN. Se pueden indicar varias interfaces.
- **Sección [turn.interfaces.transport]:** Define el tipo de transporte de la interfaz, que puede ser udp o tcp.
- **Sección [turn.interfaces.bind]:** Dirección IP y puerto de vinculación del socket interno.
- **Sección [turn.interfaces.external]:** Se usa para enlazar a la dirección de su NIC local. Por ejemplo, si tiene dos NIC, A y B, en su servidor, y la dirección IP de la NIC A es 192.168.1.2 y la de la NIC B es 192.168.1.3, si se enlaza a la NIC A, debe enlazar a la dirección 192.168.1.2. Enlazar a 0.0.0.0 significa que escucha en todas las interfaces al mismo tiempo. La palabra external significa que su tarjeta de red para el cliente pueda "ver" la dirección IP. Continuando con el ejemplo anterior, si su tarjeta de red A se comunica con el exterior, los otros clientes verán su dirección LAN (es decir, 192.168.1.2). Sin embargo, en la realidad, la topología de red donde está desplegado el servidor podría tener otra IP pública, como 1.1.1.1, que es la dirección IP vista por los demás clientes. La razón por la que se necesitan bind y external es que, para el protocolo STUN, el servidor necesita informar su propia dirección IP externa, permitiendo así que el cliente STUN se conecte a la dirección especificada mediante la IP informada por el servidor.
- **Sección [api.bind]:** Escucha de la API para consultas, por ejemplo: http://127.0.0.1:3000/info.
- **Sección [log.level]:** Nivel de registro (log). Valores válidos: error, warn, info, debug, trace.
- **Sección [auth]:** Par de usuario y contraseña para acceder al servidor.

2. Inicio del Servicio

Inicie el servicio del STUN Server (Aranda Turn Stun WebRTC Server) para que los cambios en la configuración surtan efecto.

3. Configuración del Firewall

Abra el puerto o los puertos configurados en el paso 1 en las reglas de entrada del firewall local y en los controladores de red presentes en la infraestructura del cliente, para los protocolos **TCP** y **UDP**. Este paso es esencial para permitir el tráfico a través del nuevo puerto y asegurar que el servidor STUN pueda recibir conexiones entrantes en el puerto configurado.

En las estaciones de trabajo (Agente ARC) y en los equipos especialistas (Agente especialista), deben permitir la salida por los puertos que se configuren.

Adicionalmente, si requiere que opere como TURN WebRTC, debe abrir el rango de puertos 49152-65535 para el protocolo **UDP**.

Ejemplo de configuración servicio STUN/TURN y Escenarios

Para que el servidor funcione tanto para dispositivos dentro como fuera de la red siga los siguientes pasos:

1. Configurar el realm

Cambie el valor de realm al dominio público o dirección IP externa de su servidor. Esto es importante para autenticar correctamente las solicitudes externas.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:

```
realm = "1.2.3.4"
```

2. Configurar bind

La sección bind asegura que el servidor STUN/TURN escuche en la IP privada para las conexiones dentro de la red local.

Si la dirección privada de su servidor es 192.168.1.25, configúrelo como:

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

Si requiere que el servicio STUN/TURN escuche en todas las interfaces al mismo tiempo, configúrelo como:

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

Estas configuraciones sólo son requeridas para [[turn.interfaces]].

3. Configurar external

La sección external es donde se define la IP pública del servidor para que los equipos externos puedan comunicarse correctamente con el servidor STUN/TURN.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:

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

4. Autenticación

La sección [auth] está configurada con usuarios estáticos:

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

Esto permite conexiones autenticadas con las credenciales estáticas user1:test y user2:test. Asegúrese de usar credenciales más seguras si planea exponer este servicio a dispositivos externos.

Los demás secciones de pueden dejar por defecto.

Al realizar la parametrización en el archivo **turn-server.toml**, este deberá observarse de la siguiente forma:

```
[turn]

realm = "1.2.3.4" # IP pública del servidor

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

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

[api]
bind = "127.0.0.1:3000"

[log]
level = "info"

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

Cada vez que realice una modificación al archivo **turn-server.toml**, reinicie el servicio **Aranda Turn Stun WebRTC Server** para que los cambios surtan efecto.

Escenarios

A continuación, se describen los siguientes escenarios y el resultado de acuerdo con la configuración del ejemplo.

Escenario	Especialista	Estado en Red	Agente ARC	Estado en Red	Resultado
1	Solo puede acceder al servidor TURN/STUN usando la IP pública	**Externo**	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
2	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
3	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
4	Solo puede acceder al servidor TURN/STUN usando la IP privada.	**Interno**	Solo puede acceder al servidor TURN/STUN usando la IP privada.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP privada.
5	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido a la red interna (IP privada).	**Interno**	El Especialista y el Agente ARC no pueden establecer comunicación debido a un problema de conectividad entre redes (exterior e interior).
6	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido.	**Externo**	El Especialista y el Agente ARC no pueden establecer comunicación debido a un problema de conectividad entre redes.

⚠ **Nota:**

- Para cubrir los escenarios 1, 2 y 3, configure en el sitio web de AMD el servidor Turn Externo de la siguiente manera:
  Nombre: nombre de la configuración.
  URL: turn.1.2.3.4:3478 (1.2.3.4 hace referencia a la IP pública del servidor).
  Usuario: user1.
  Contraseña: test.

⚠ **Notas:**

- Para cubrir el escenario (4), configure en el sitio web de ADM el servidor Turn Externo de la siguiente

manera:
Nombre: nombre de la configuración.
URL: turn.192.168.1.25:3478 (192.168.1.25 hace referencia a la IP privada del servidor).
Usuario: user1.
Contraseña: test.

- Si en el archivo **turn-server.toml** se configuró 0.0.0.0 en el parámetro bind, se debe realizar la configuración en el sitio como se indicó anteriormente.

Instalador/ Agente ADM

El Agente ADM es un programa instalado en los dispositivos gestionados que permite la generación de inventarios y las tareas de gestión asociadas a procesos de distribución, actualización y uso de software, gestión de políticas de energía y control remoto.

Al instalar el agente, se crea una serie de servicios en el dispositivo que permiten establecer la comunicación con el visor de control remoto y la gestión general del dispositivo.

Existe un agente para cada una de las plataformas soportadas:

- Instalador Agente ADM para Windows.
- Instalador Agente ADM para Mac.
- Instalador Agente ADM para Linux

Despliegue del Agente

El despliegue del agente es el proceso de distribución de este componente en los dispositivos que se requiere gestionar.El procceso de distribución e instalación del agente ADM,puede efectuarse desde la consola web de ADM o utilizando otras opciones de despliegue, así:

- Instalación por Política de Dominio
- Instalación y distribución con Aranda Device Management ADM

Instador/Agente ADM en Windows

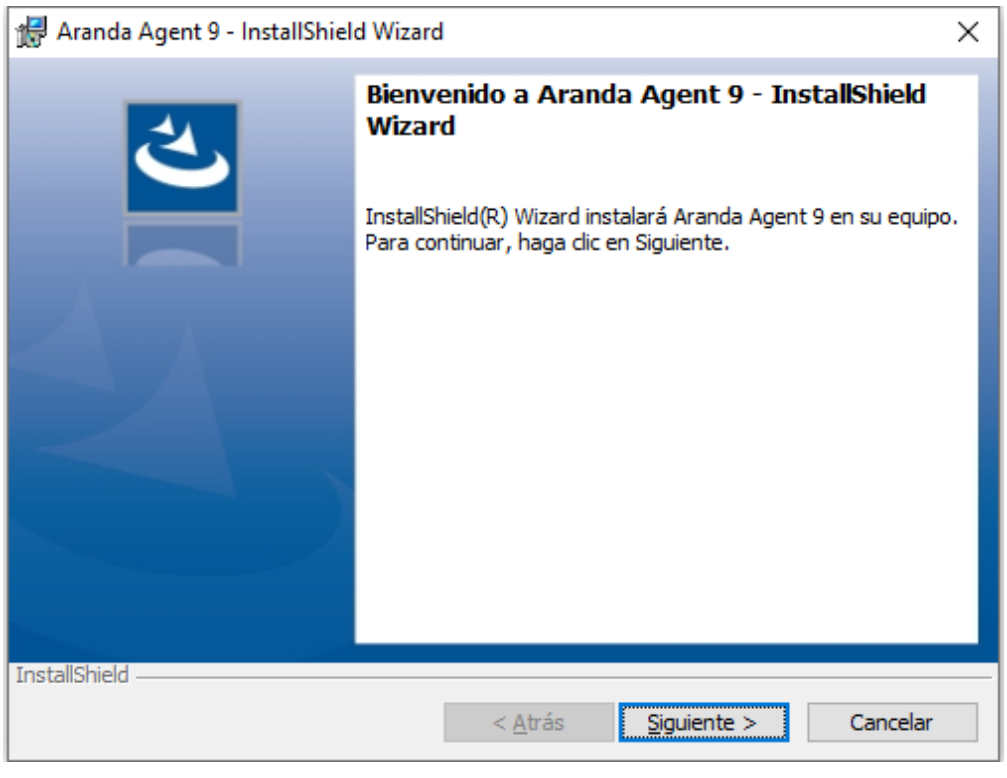
El tercer archivo ejecutable es Aranda.Agent.Windows.x86_x64 que corresponde al instalador del Agente ADM para Windows. Este archivo se encarga de la creación y configuración de los servicios requeridos para el funcionamiento del Agente ADM para Windows.

El instalador detecta de forma automática el idioma del sistema, soportando actualmente, inglés, español y portugués. Si la configuración está en un idioma diferente, el instalador queda por defecto en español.

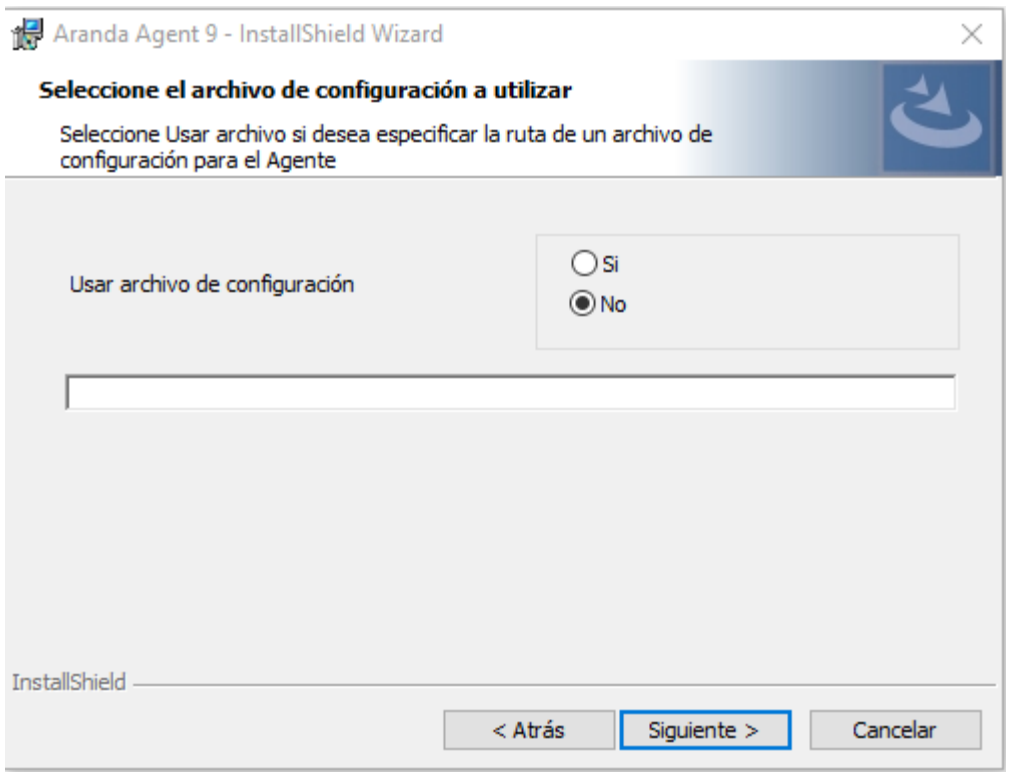
> ⚐ **Nota:** El agente puede instalarse de manera desatendida y automática a través de la funcionalidad de Distribución del Agente, o de forma manual.

Instalación Manual del Agente

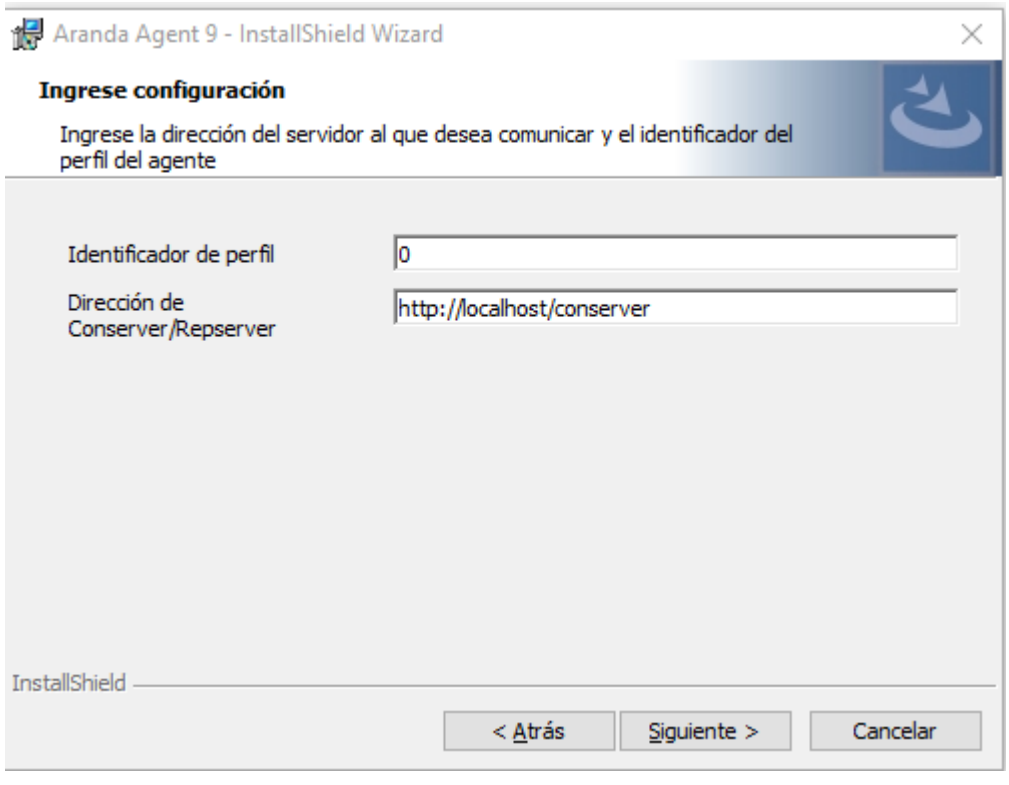
1. Haga clic sobre el instalador Aranda Agent. Se iniciará el asistente de instalación (wizard). Haga clic en**Siguiente**.



2. Si tiene un archivo de configuración seleccione **Sí** e ingrese la ruta, de lo contrario, seleccione **No** y haga clic en **Siguiente**.

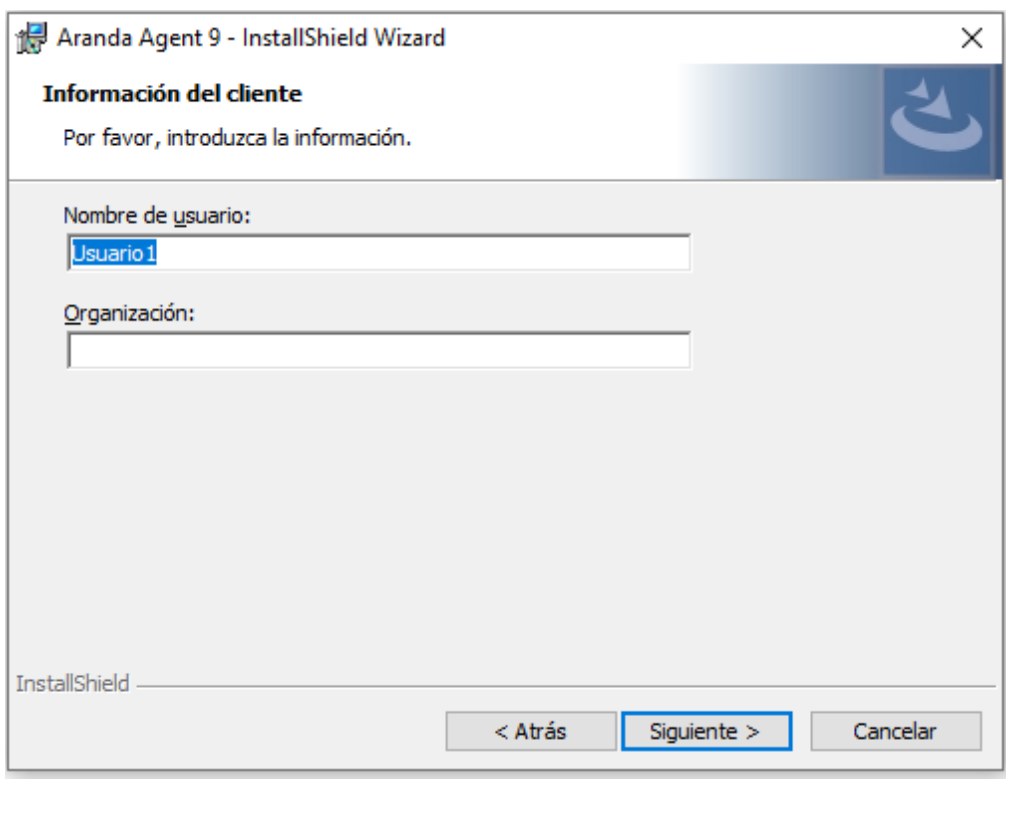


3. Ingrese el identificador de perfil, al ingresar 0 se descarga el perfil que esté configurado por defecto. Ingrese la dirección de Conserver o Repserver según el apuntamiento configurado en el broker MQTT [Configuración Broker MQTT](). Ingresando a la consola de ADM puede obtener la ruta de comunicación. **Configuración** > **ADM** > **Comunicaciones**

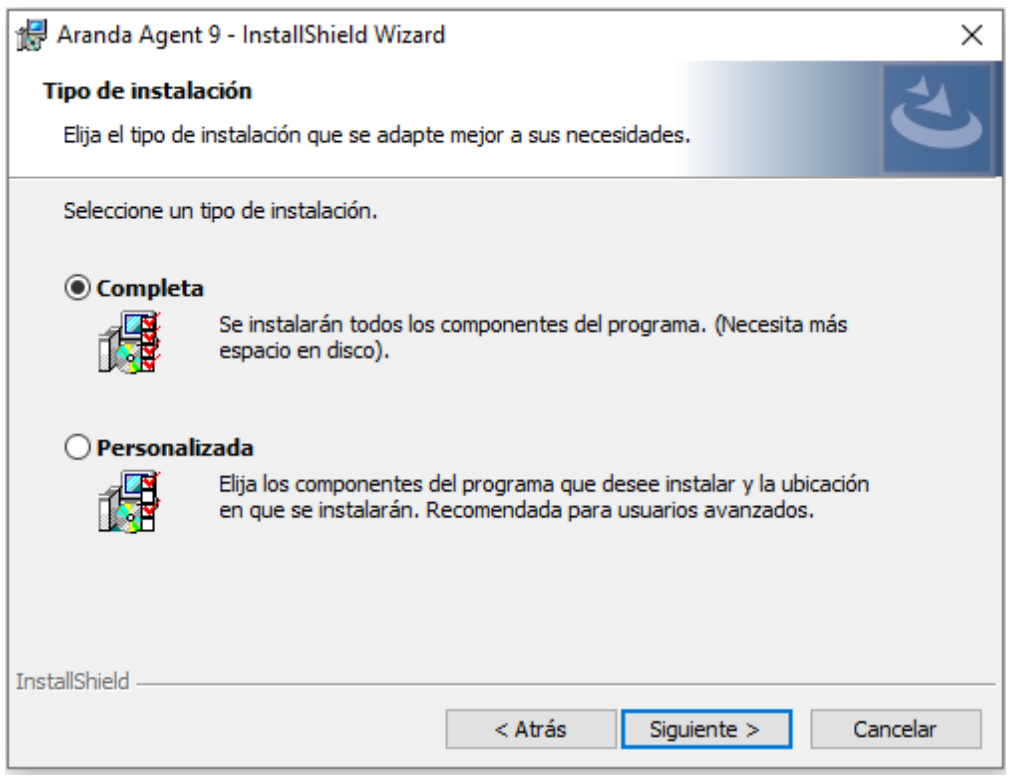


⚐ **Nota:** El direccionamiento del agente al repserver, sólo funciona con una versión de agente desde 9.13.

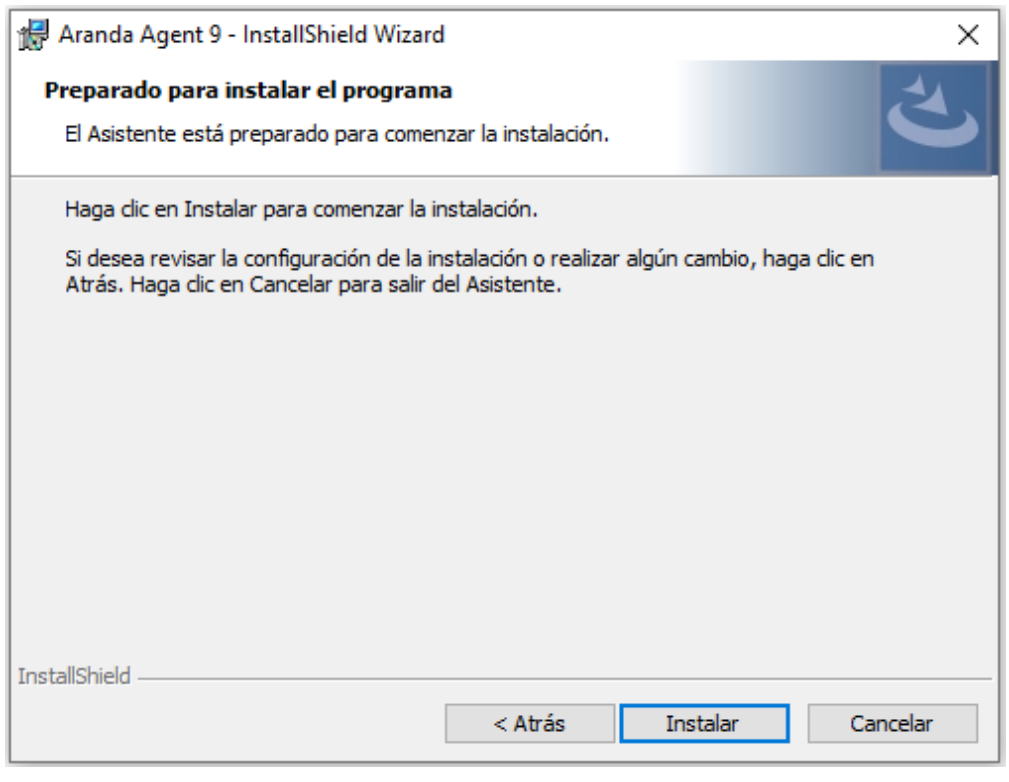
4. Ingrese el nombre de usuario y la organización donde se instalará el agente.



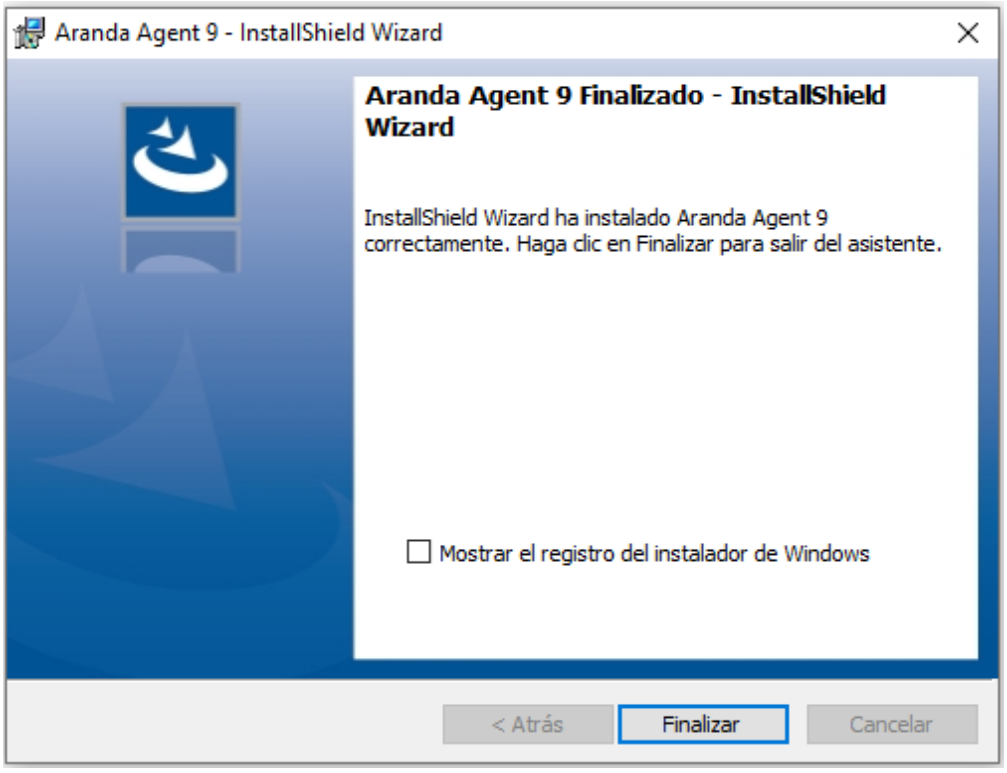
5. Seleccione el tipo de instalación que desea realizar (completa o personalizada) y haga clic en **Siguiente**.



6. Haga clic en **Instalar** para iniciar la instalación del agente.



7. Al completar la instalación del agente, haga clic en **Finalizar**



—

Instalación Manual del Agente por línea de comandos

Para realizar la instalación del Agente ADM por línea de comando se puede ejecutar la siguiente instrucción desde el *command promt* de Windows:

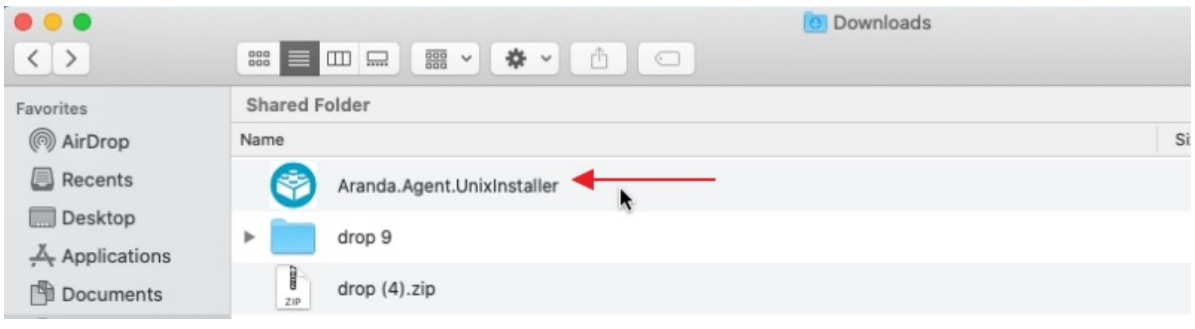
```
Aranda.Agent.Windows.x86_x64.9.xx.xxxx.xxxx.exe /S /V"/norestart /qn
AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=0"
```

AGENT_PROFILE_ID=[UNIT]	Identificador del perfil a instalar, 0 es un perfil seleccionado en la aplicación como perfil por defecto.
AGENT_SERVER_ADDRESS=[STRING]	Ruta del Conserver o Repserver.

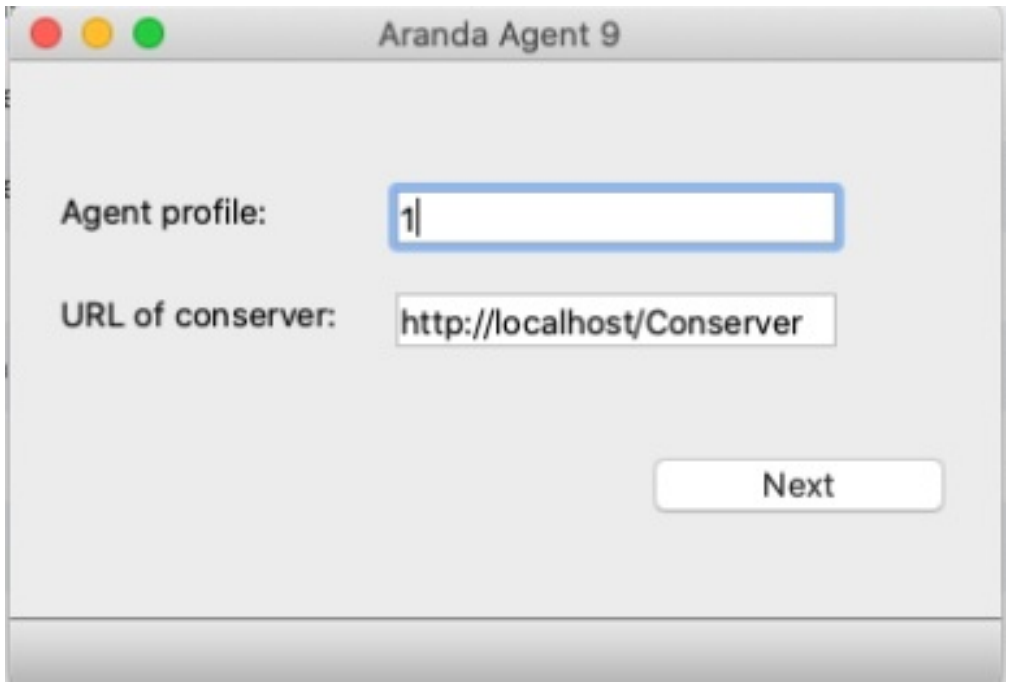
Instalador/Agente ADM en MacOS

Instalación del agente desde la interfaz del usuario

1. Ejecute el app del agente.

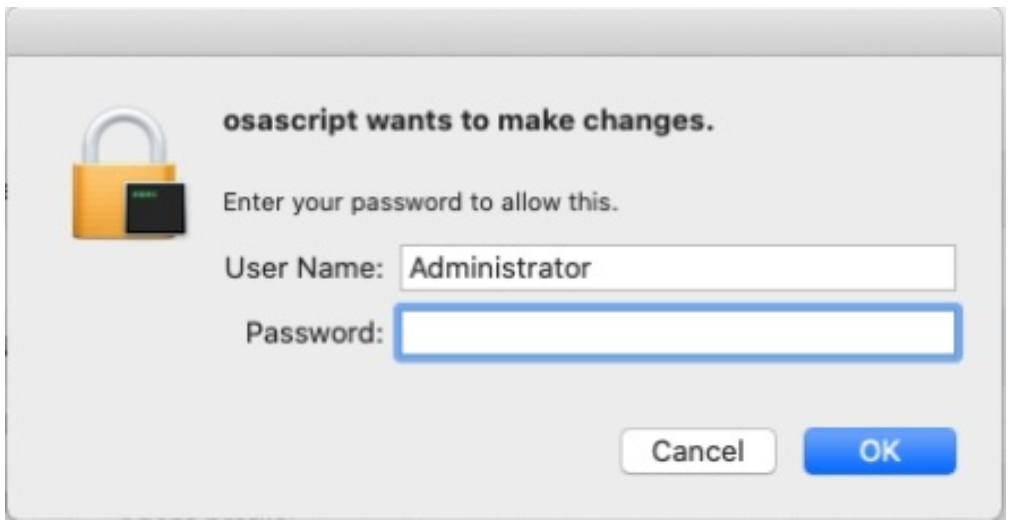


2. Ingrese el identificador de perfil, al digitar 0 se descarga el perfil que esté configurado por defecto. Registre la dirección de Conserver o Repserver según el apuntamiento configurado en el broker MQTT [Configuración Broker MQTT](). Al entrar a la consola de ADM podrá obtener la ruta de comunicación. **Configuración** > **ADM** > **Comunicaciones**

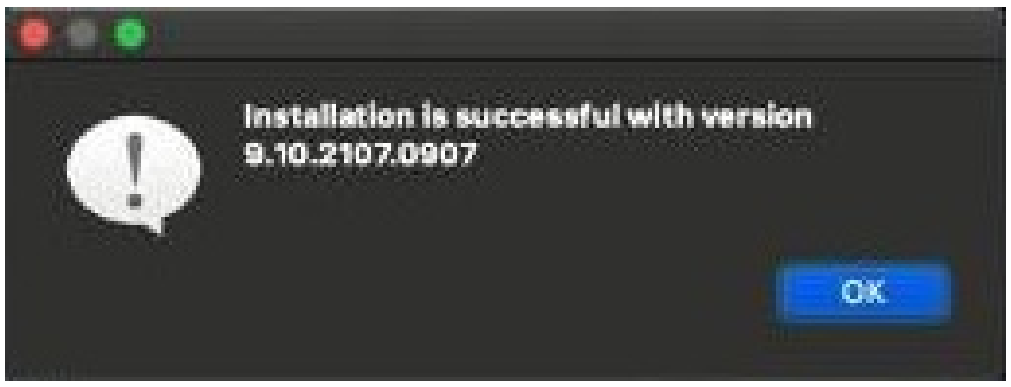


⚐ **Nota:** El direccionamiento del agente al repserver, sólo funciona con una versión de agente desde 9.13.

3. Ingrese las credenciales del dispositivo.



4. El agente se instalará y se visualizará un mensaje de éxito.



5. Al completar la instalación podrá ver el dispositivo en la consola de ADM.

⚐ **Nota:** Si ya se tiene un agente instalado se podrán visualizar los siguientes mensajes.

Mensaje	Descripción
La Versión a instalar igual a la versión instalada	Este caso se utiliza para actualizar los datos del conserver.
La Versión a instalar es menor a la versión instalada	En este caso se impedirá la instalación del agente que se está instalando.

Instalación del agente desde línea de comandos

1. Para instalar el Agente de Aranda DEVICE MANAGEMENT ADM por línea de comandos, ejecute la siguiente instrucción desde un intérprete de comandos de MacOS:

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

Línea	Instrucción
RUTA_INSTALADOR	Ruta donde se encuentra el instalador, puede ser relativa o absolut
AGENT_PROFILE_ID=[UNIT]	Identificador del perfil a instalar, 0 es un perfil seleccionado en la aplicación como perfil por defecto
AGENT_SERVER_ADDRESS=[STRING]	Ruta de Conserver o Repserver

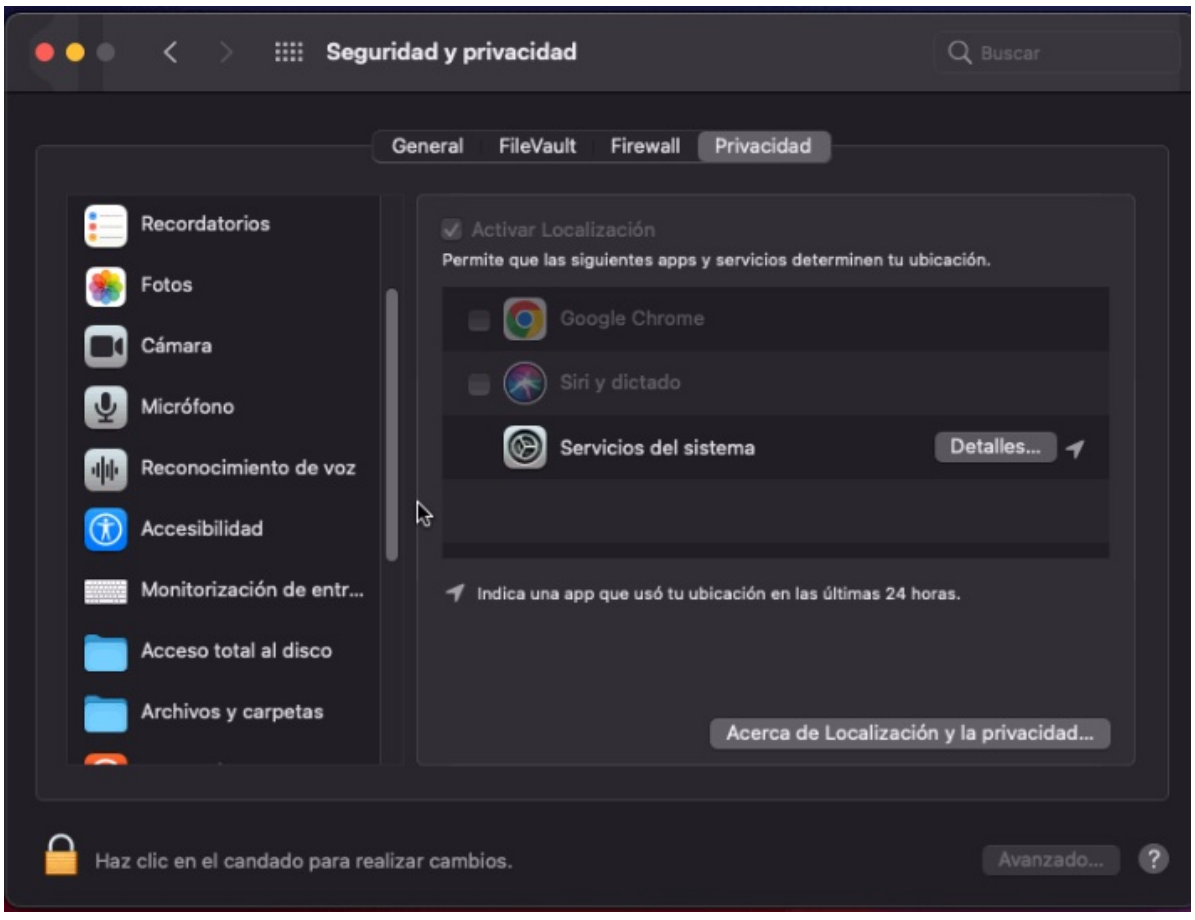
2. Después de instalar el agente, se crea una carpeta con el nombre Aranda en la ruta**'/Opt/local'** con las librerías, servicios del agente y otra carpeta en**'/etc/'** con el nombre Aranda, donde se guardan los logs y la base de datos del agente. Al borrar estas carpetas se desinstalará el agente.

Otorgar permisos al agente

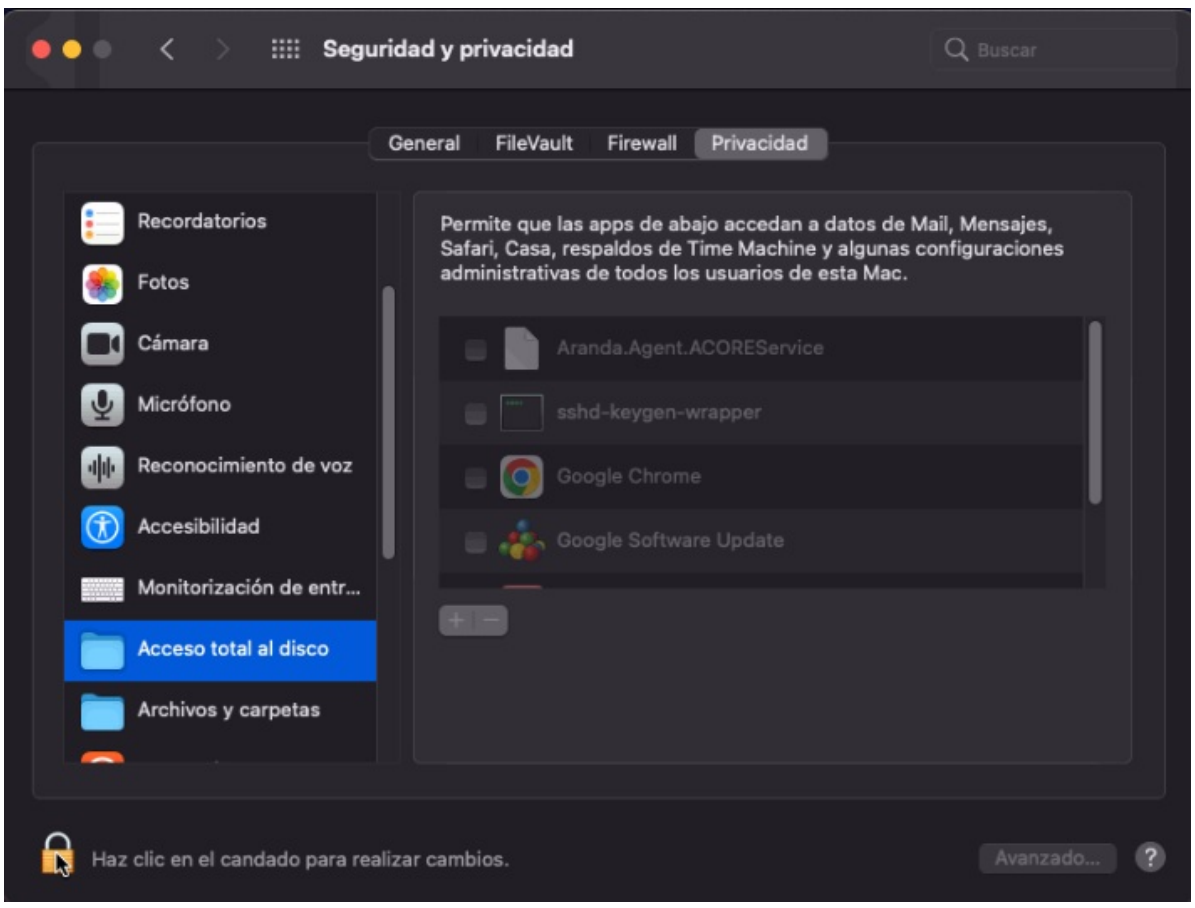
Se deben otorgar el permiso de acceso total al disco al agente, esta acción de realiza teniendo en cuenta los siguientes pasos:

1. Abra **Preferencias del sistema > Seguridad y privacidad.**

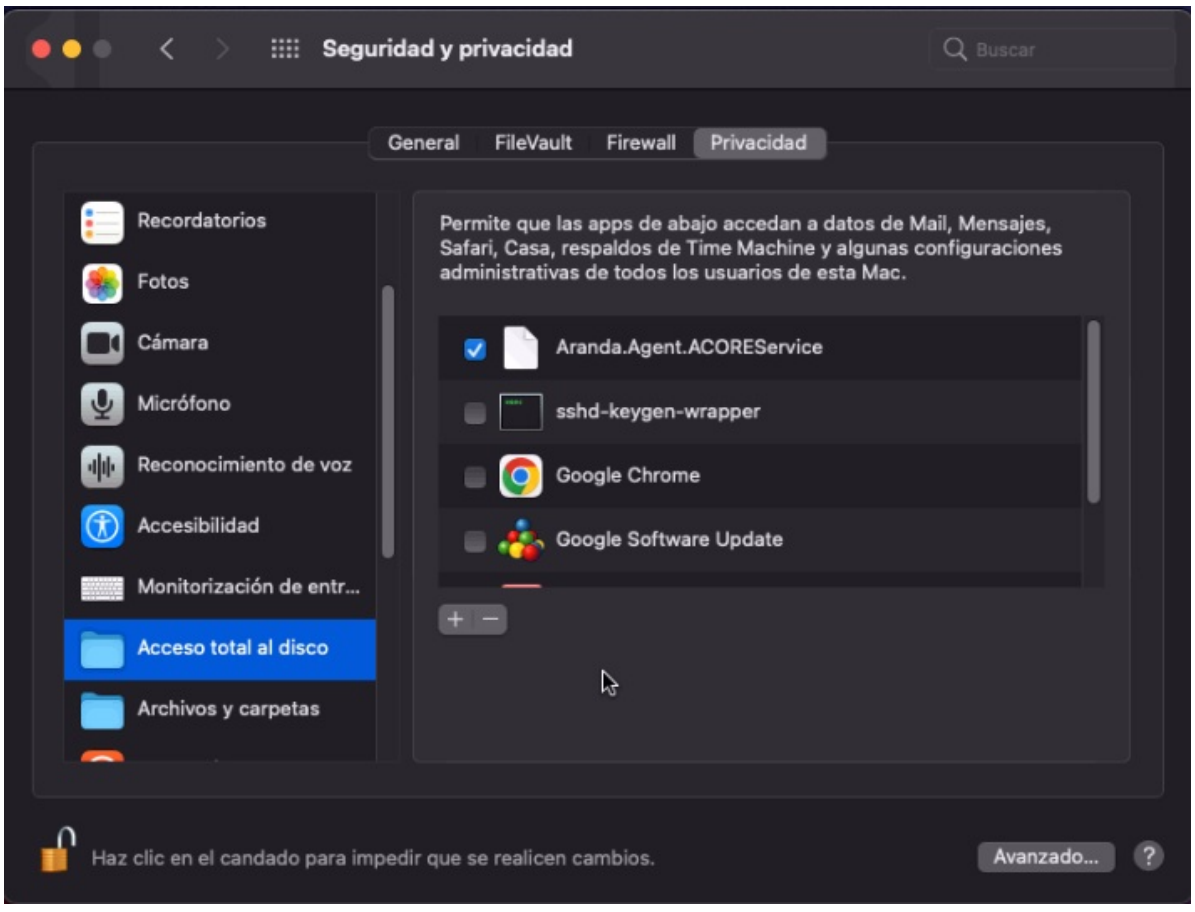
2.Seleccione la pestaña **Privacidad**.



3. Seleccione **Acceso total al disco** y haga clic en el ícono del candado. Ingrese las credenciales de administrador del sistema y haga clic en **Desbloquear**.



4. Seleccione el servicio **Aranda.Agent.ACOREService**, a continuación de clic en el ícono del candado.



—

Excepciones del agente en MacOs

Las funcionalidades soportadas actualmente en MAC son el módulo **Aranda Asset Manager** excepto las siguientes funcionalidades.

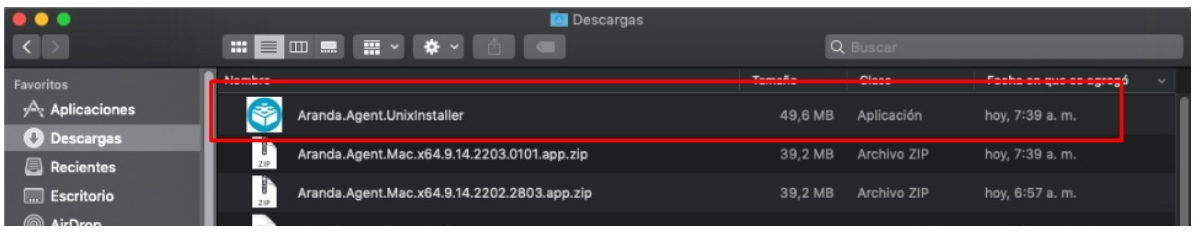
- Ubicación del dispositivo
- Eliminación de archivos por extensión
- Virtualización
- Monitoreo
- Envío de mensajes
- Envío de comandos (Únicamente se permite con el usuario actual del sistema)

Modificación del agente

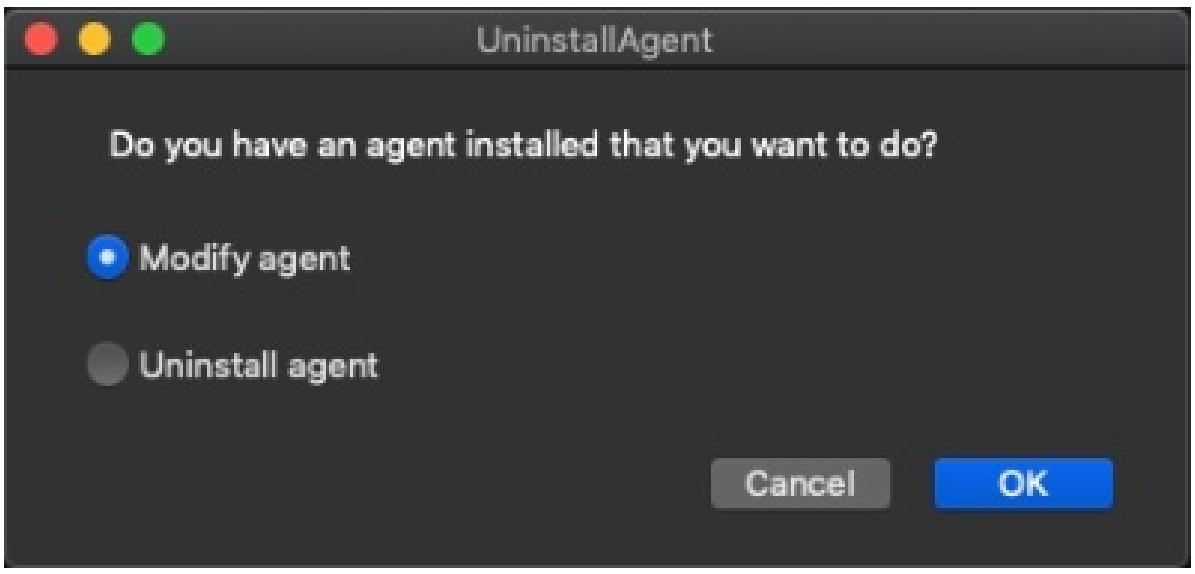
> ⚐ **Nota:** Disponible en la versión de agente superior a 9.14 ,
> si tiene instalado un agente anterior a este, la ventana de desinstalación no aparecerá.

Modificación del agente (Host del Repserver o Conserver y perfil)

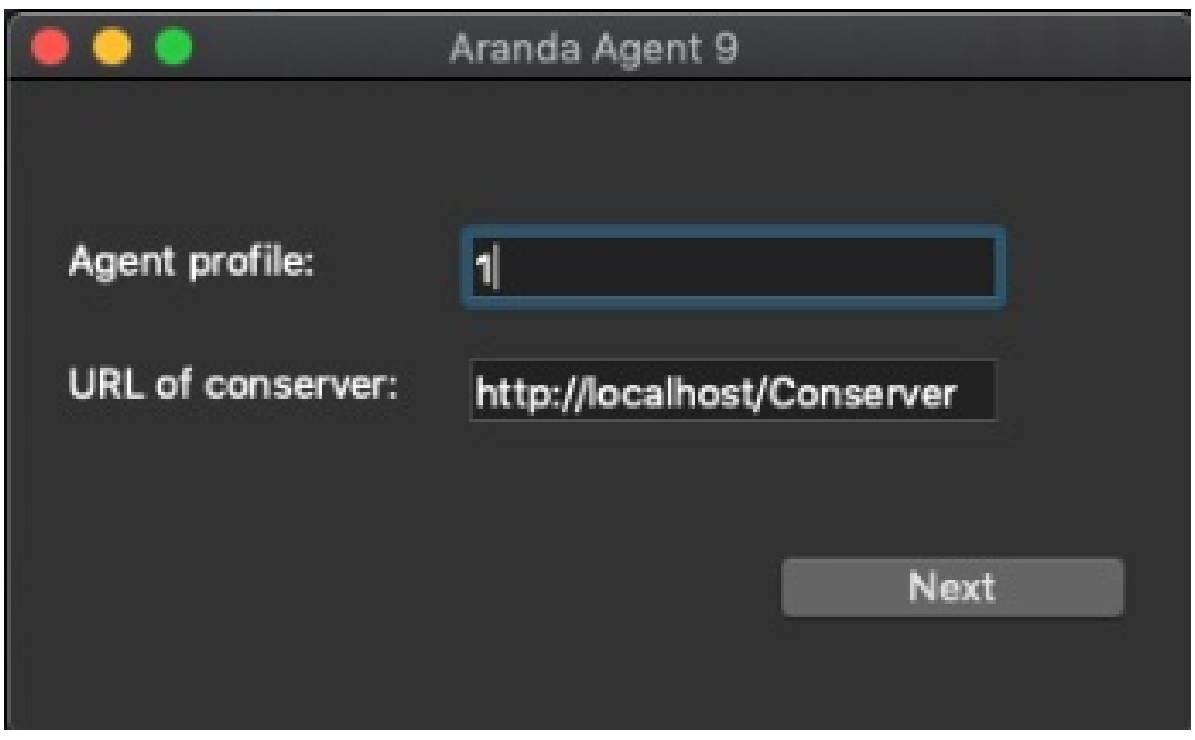
1. Para modificar el agente se puede realizar desde el instalador **Aranda.Agent.Unixinstaller.app**



2. Haga doble **clic** en el ejecutable y se habilita la siguiente ventana.



3. Por default la opción de **Modify agent** se encuentra seleccionada; haga clic en **OK** y se habilita la ventana de instalación. Después de actualizar haga clic en **next**.



—

Desinstalación de agente

Para desinstalar el agente tendrá dos opciones:

- Por línea de comandos usando el terminal.
- Utilizando la interfaz gráfica.

Línea de comandos

1. Abra una ventana del terminal y en la ruta definida utilice el siguiente comando:

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

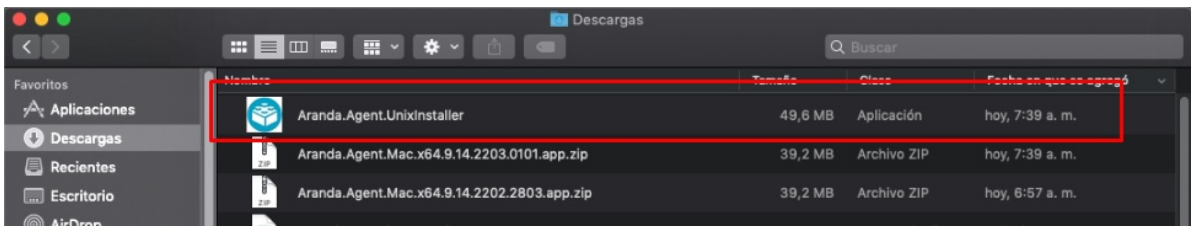
2. Una vez se ingresa a la carpeta **aranda** ejecutamos el siguiente comando.

```
sudo sh UninstallAgent.sh
```

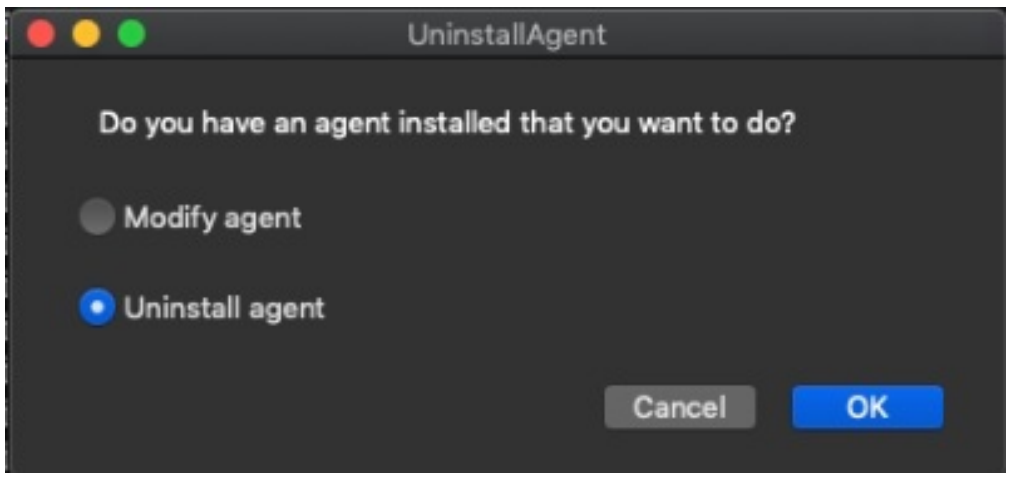
3. Ejecutado el comando se puede ver que el agente se desinstaló correctamente.

Interfaz gráfica

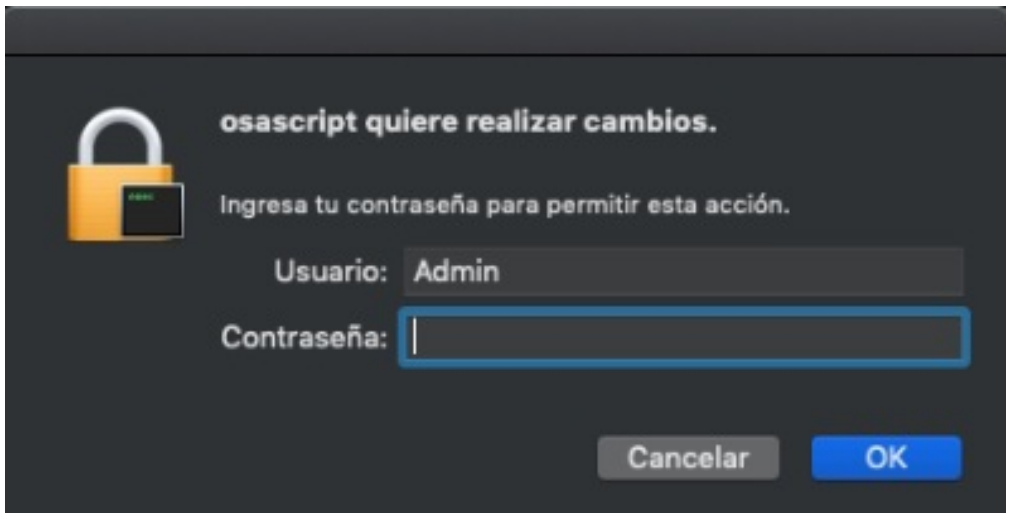
1. Ejecute el instalador **Aranda.Agent.Unixinstaller.app**.



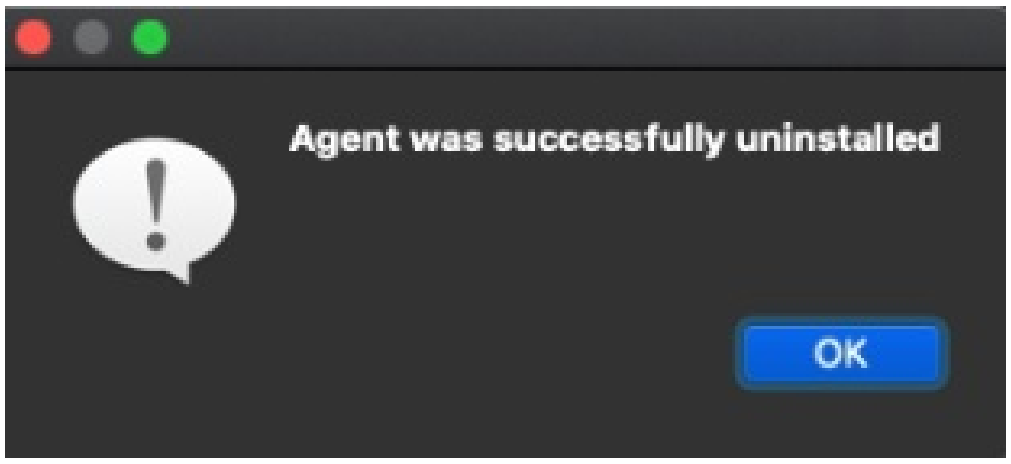
2. En la ventana Desinstalar Agente, seleccione la opción **Uninstall agent** y haga clic en **OK**



3. En la siguiente ventana se solicitan las credenciales del administrador del equipo; ingrese la contraseña y de clic en **OK**



4.Se espera unos segundos a que la desinstalación finalice y se habilita un mensaje de confirmación



Instalador/Agente ADM en Linux

Instalación manual del Agente por línea de comandos en Linux

1. Para realizar la instalación del Agente Aranda DEVICE MANAGEMENT ADM por línea de comando, se puede ejecutar la siguiente instrucción desde un intérprete de comandos de Linux o macOS.

Ingrese la dirección de Conserver o Repserver según la configuración del broker MQTT[Configuración Broker MQTT](). Ingresando a la consola de ADM puede obtener la ruta de comunicación **Configuración > ADM > Comunicaciones**.

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

Donde:

Línea	Descripción
RUTA_INSTALADOR	Ruta donde se encuentra el instalador, puede ser relativa o absoluta.
AGENT_PROFILE_ID=[UNIT]	Identificador del perfil a instalar, 0 es un perfil seleccionado en la aplicación como perfil por defecto
AGENT_SERVER_ADDRESS=[STRING]	Ruta de Conserver o Repserver.

⚐ **Nota:** El direccionamiento del agente al repserver, sólo funciona con una versión de agente desde 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.

Excepciones del agente en Linux

Actualmente se soporta el módulo **Aranda Asset Manager** expecto las siguientes funcionalidades:

- Ubicación del dispositivo
- Virtualización
- Monitoreo
- Envío de mensajes
- Envío de comandos (Únicamente se permite con el usuario actual del sistema)

Desinstalación manual del Agente por línea de comandos en Linux

⚐ **Nota:** Disponible en la versión de agente superior a 9.14.

Se puede desinstalar el agente Linux por la línea de comandos siguiendo los siguientes pasos:

1. Abra una ventana del terminal y en la ruta definida utilice el siguiente comando:

```
cd /opt/aranda
```

2. Una vez ingresa a la carpeta *aranda* ejecute el siguiente comando.

```
sudo sh UninstallAgent.sh
```

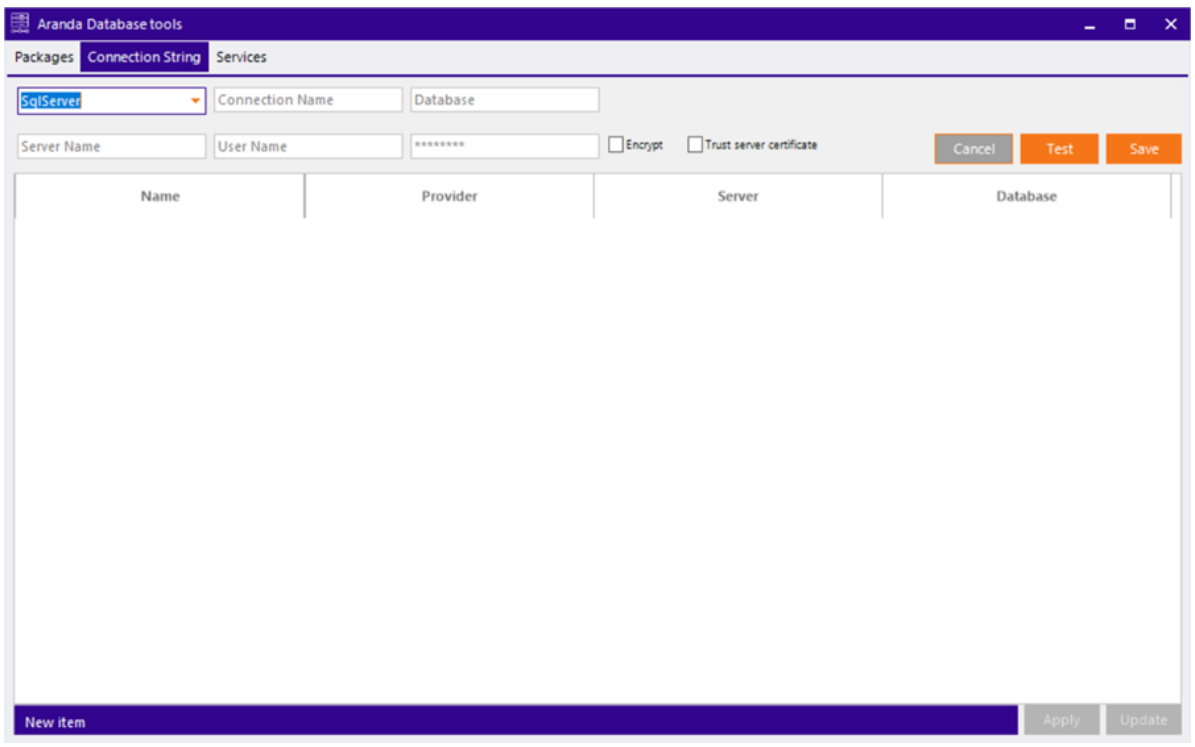
3. Ejecutado el comando podrá visualizar que el agente se desinstaló correctamente.

Configuración conexión con base de datos

Una vez finalice la instalación de **Aranda Device Management**, proceda a configurar las cadenas de conexión hacia la base de datos de los sitios y servicios.

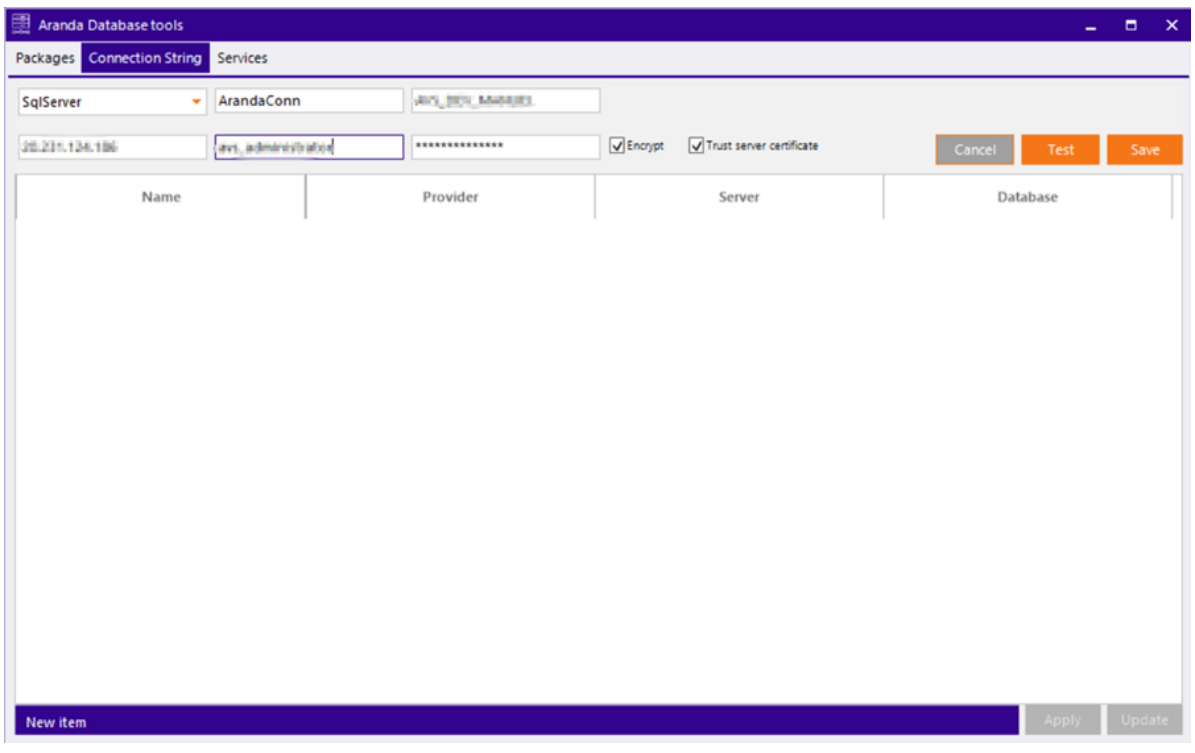
Para configurar los sitios, servicios Comunes y de Licenciamiento, se realiza a través del módulo**Aranda Database Tools v9**. Para ello:

1. Ejecute el módulo y haga clic en la pestaña **Connection String**.

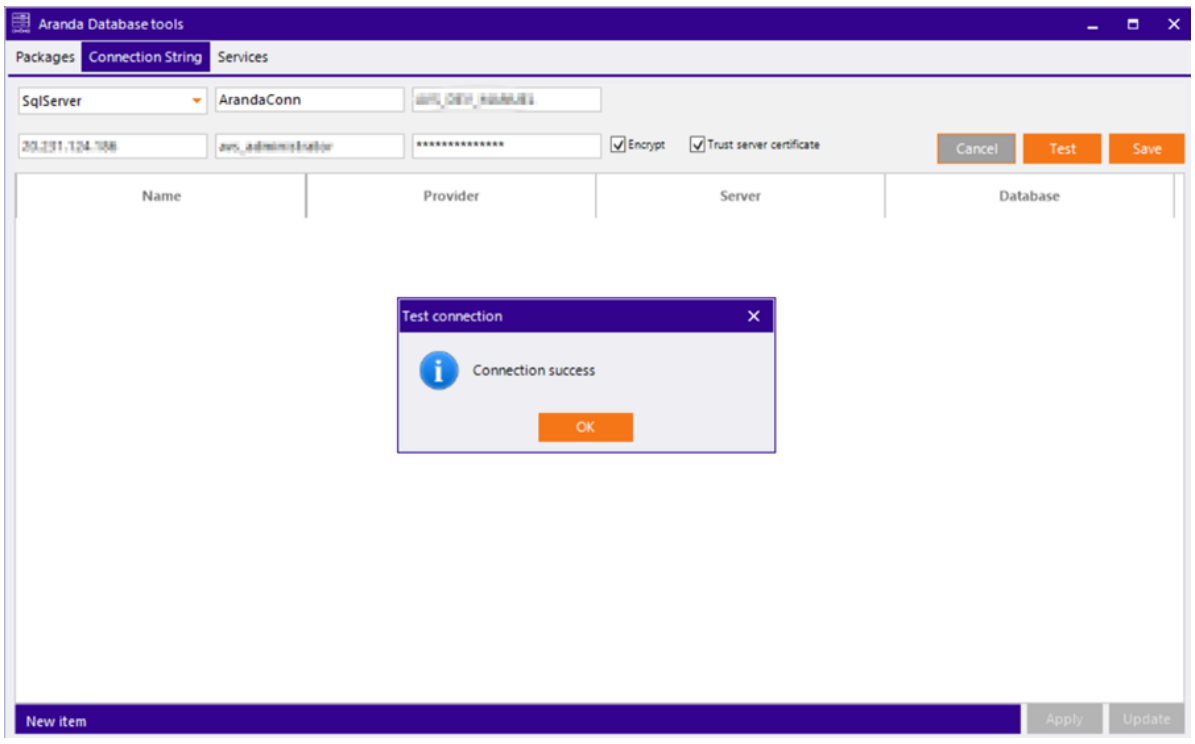


2. Complete los datos solicitados.

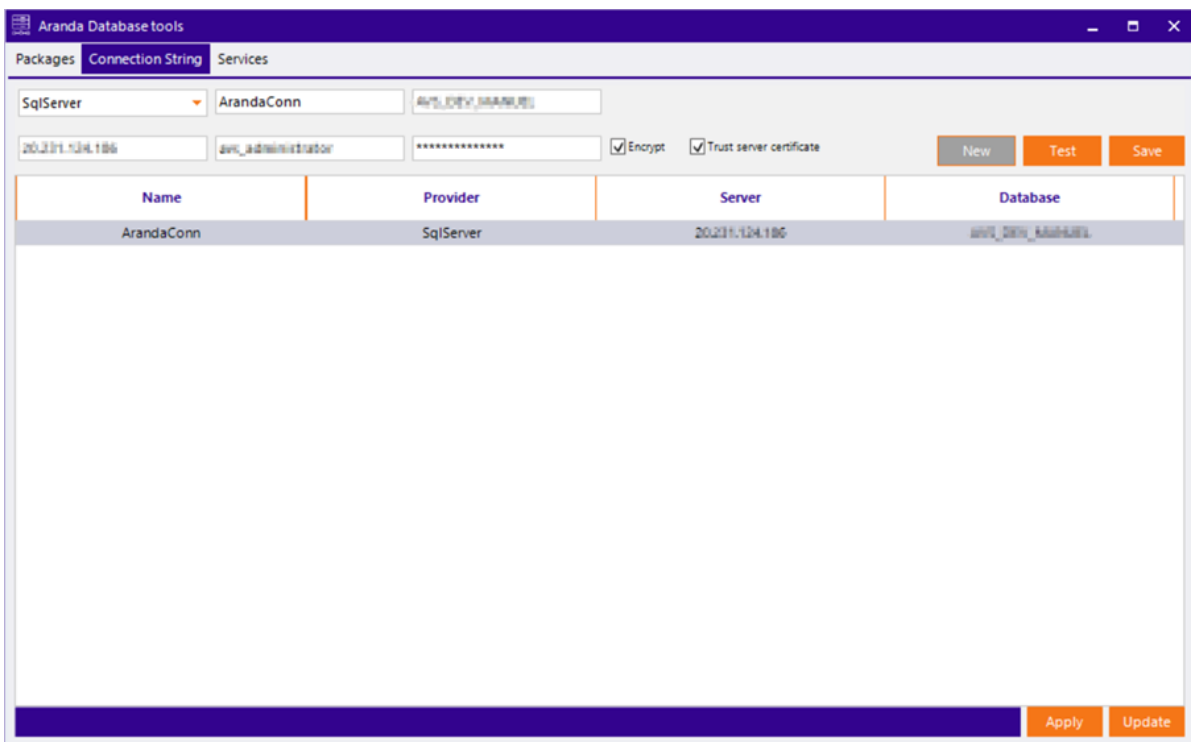
- Seleccione el motor de base de datos (SQL Server).
- Asigne un nombre para identificar la conexión.
- Registre los datos de conexión (nombre de la base de datos, nombre del servidor o dirección IP, y si se requiere usuario y contraseña).
- En caso que el puerto de base de datos sea distinto al puerto establecido por defecto (1433 para SQL Server), se debe escribir el servidor como servername:port (ej. ARANDADBSERVER:5555)
- De forma predeterminada, se debe marcar la opción "Encrypt" para asegurar que la conexión entre la solución y la base de datos está encriptada.



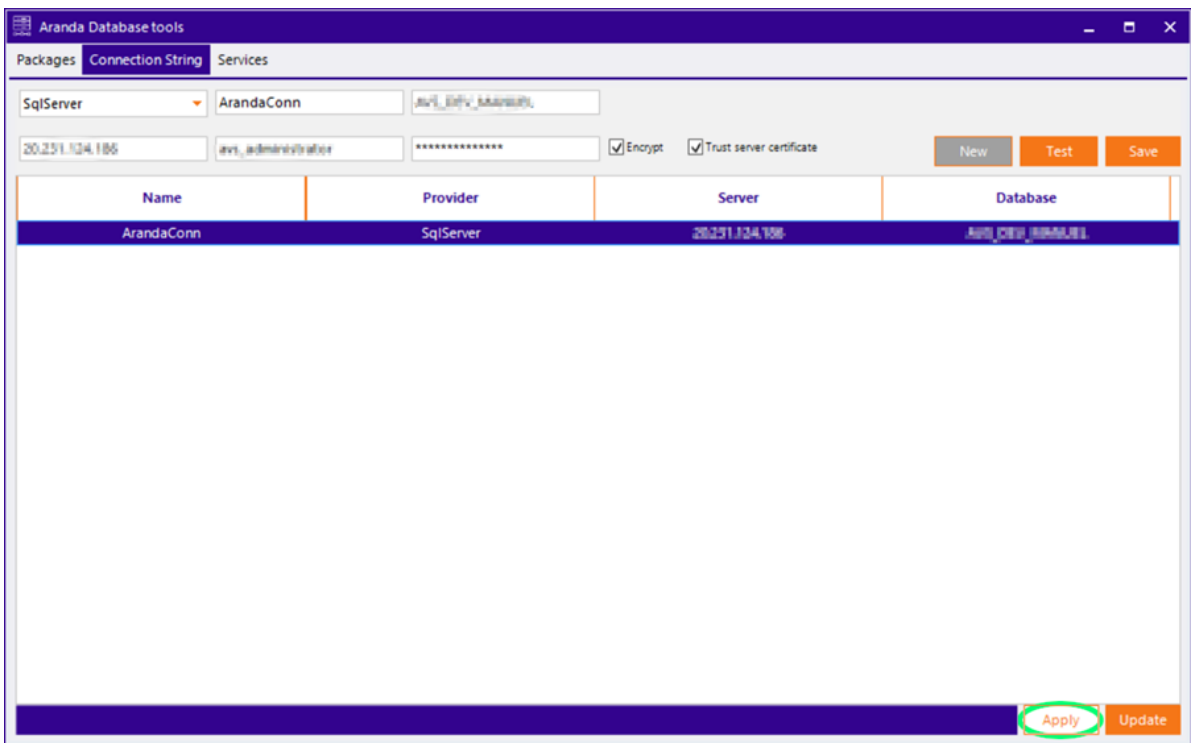
3. Haga clic en el botón **Test** para comprobar la conexión.



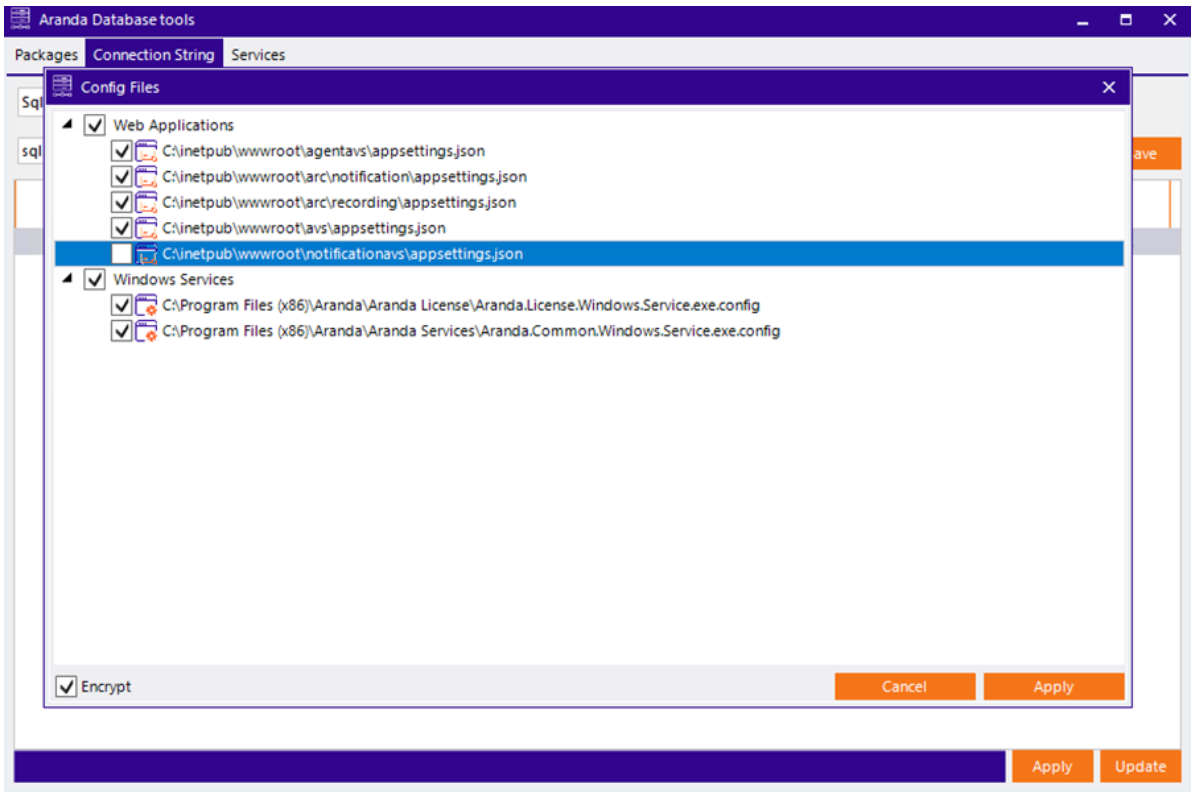
4. Para finalizar haga clic en el botón **Save** para guardar la conexión.



5. Para aplicar las cadenas de conexión a los servicios instalados, seleccione la conexión creada previamente y haga clic en el botón **Apply**.

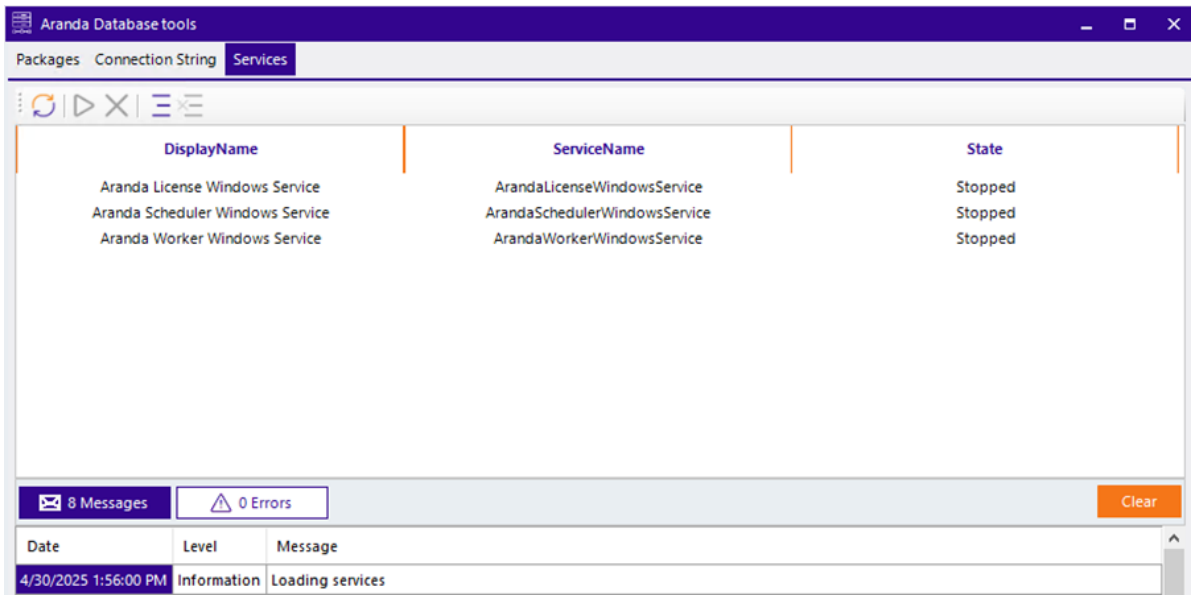


6. Se habilita una ventana con el listado de aplicaciones y servicios disponibles en el servidor. Para el sitio **notificationadm** no se requiere aplicar la configuración de la cadena de conexión.

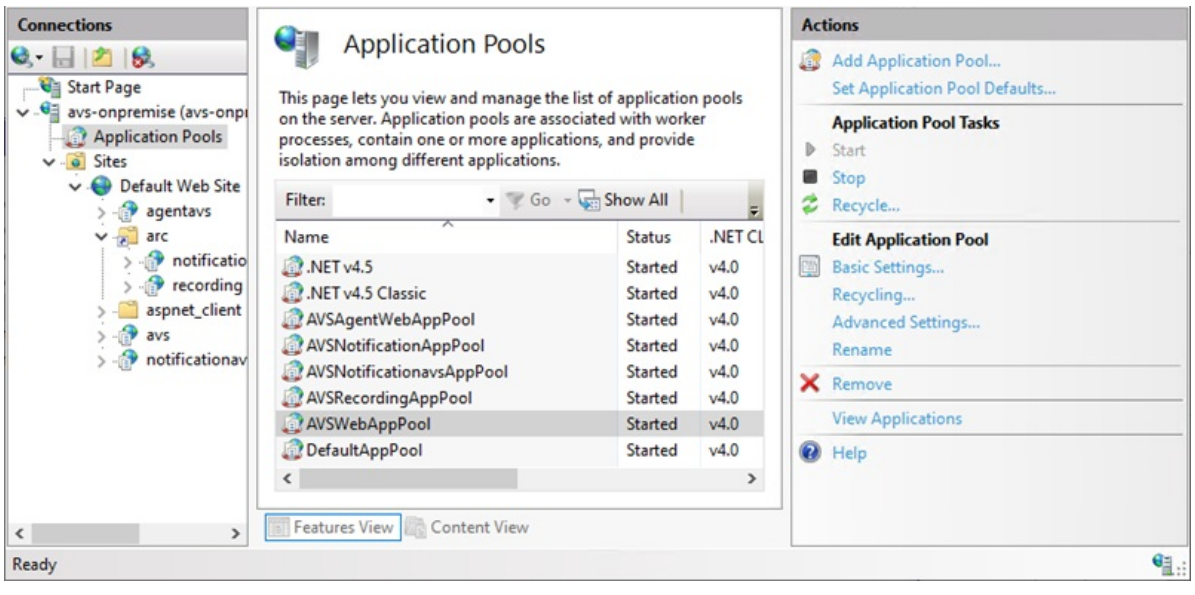


7. Seleccione los servicios correspondientes y haga clic en el botón **Apply**, si desea encriptar la conexión marque la casilla **Encrypt** ubicada en la esquina inferior izquierda. Se podrá visualizar un mensaje de alerta porque la encriptación no está soportada para archivos JSON.

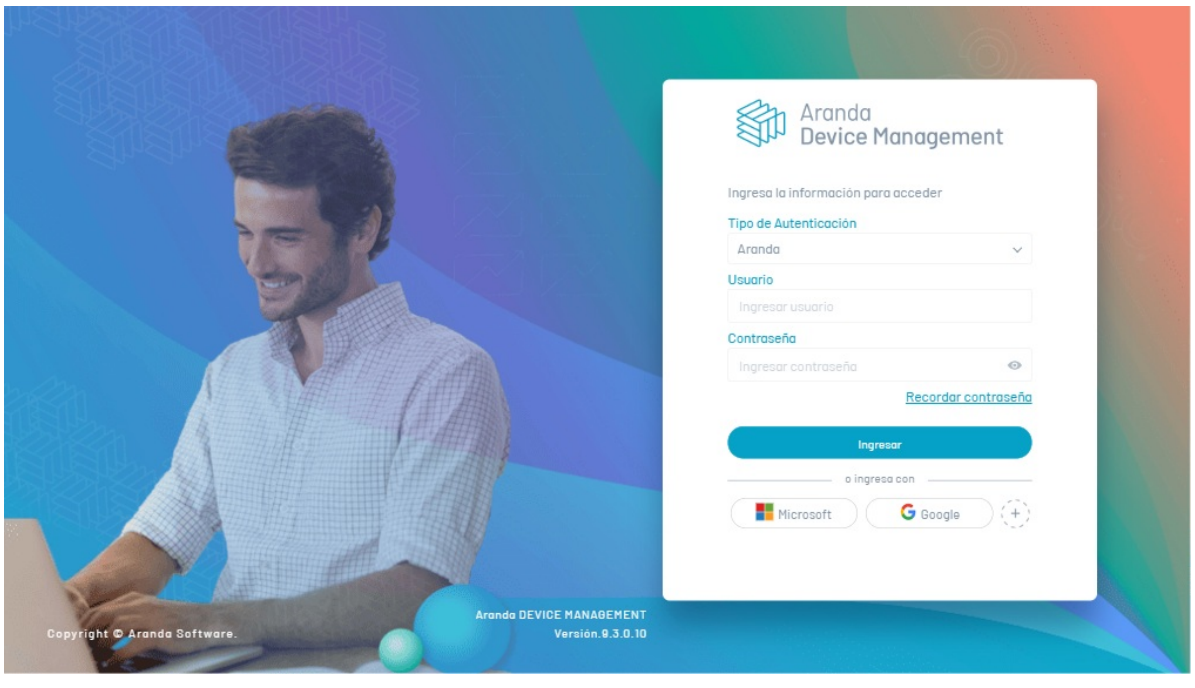
8. Para finalizar haga clic en la pestaña **Services** e inicie todos los servicios.



⚐ **Importante** Cuando se realicen cambios a las cadenas de conexión de los sitios, se debe reiniciar o reciclar el grupo de aplicaciones asociado al sitio para que el cambio se aplique inmediatamente.



9. Establecida la conexión, podrá acceder al sitio web de ADM donde podrá iniciar con la configuración de Aranda Device Management a través de la siguiente URL: *http(s)://nombre_servidor/adm/.*

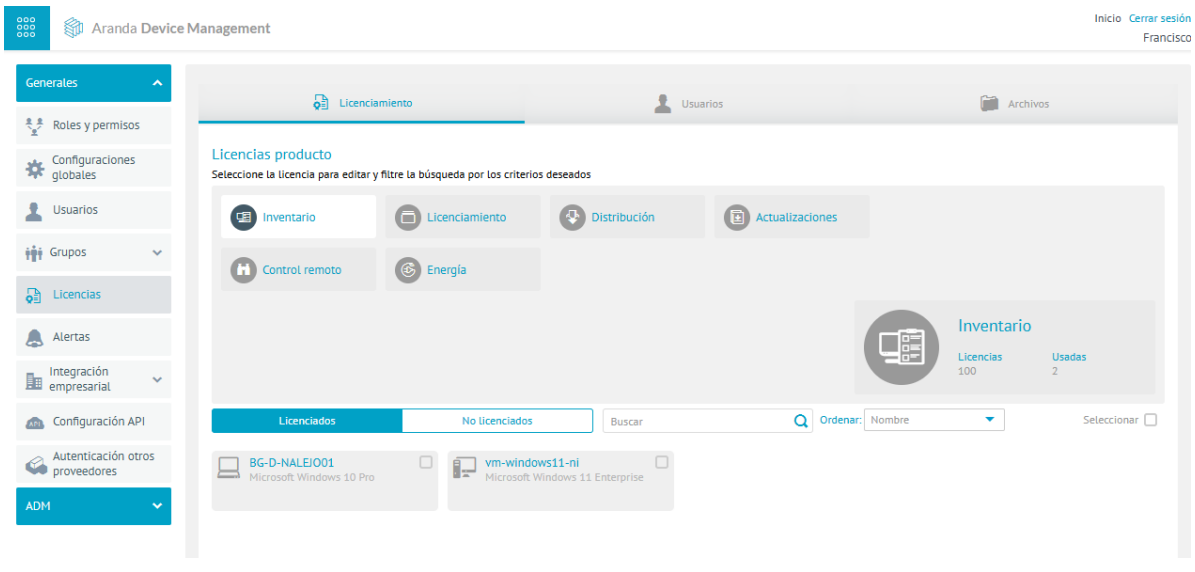


Licenciamiento ADM

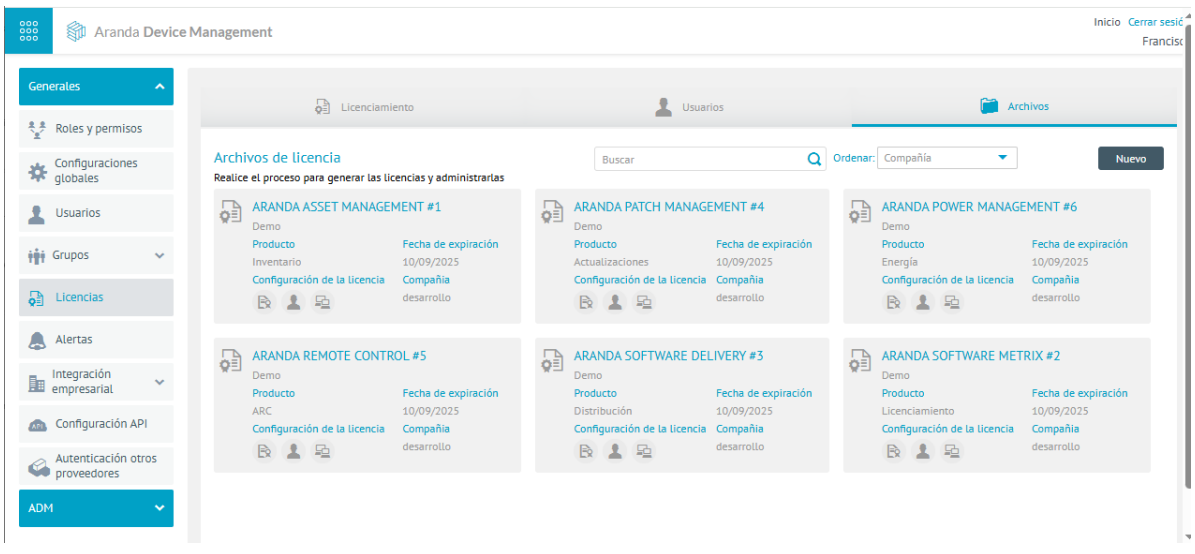
Todos los productos de Aranda Software requieren una licencia para su funcionamiento, por tal razón ADM utiliza el servicio común de licenciamiento de Aranda para autorizar el ingreso a usuarios a la consola y controlar las licencias compradas, entre otras operaciones.

Cargar Archivo de Licenciamiento

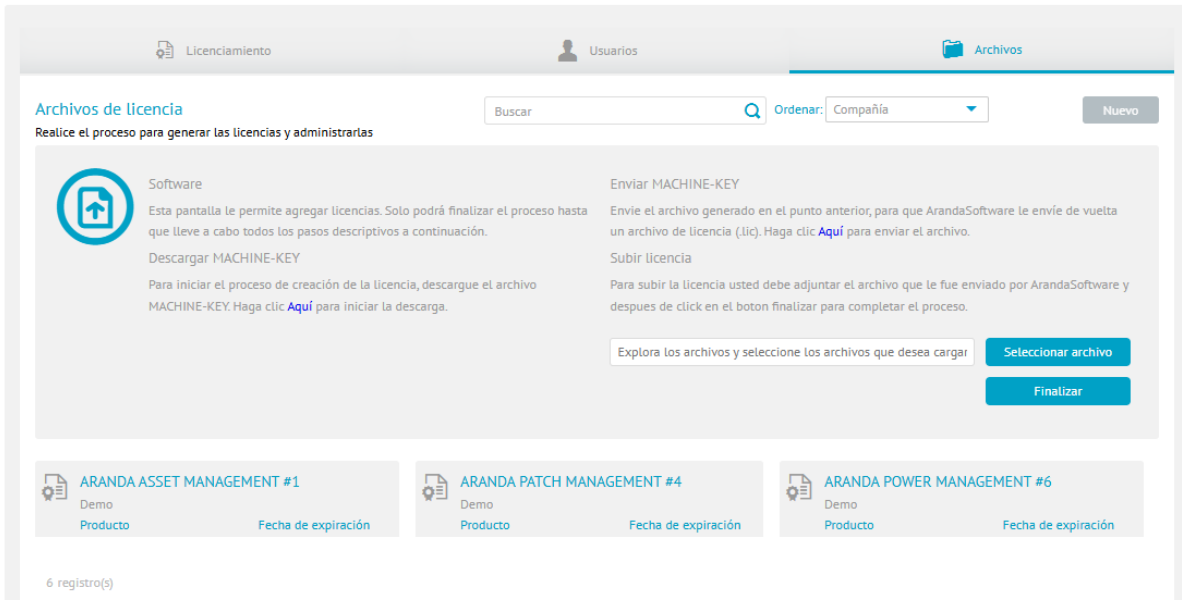
1. Para cargar el archivo de licenciamiento,la primera vez que ingrese al sitio web de Aranda Device Management (ADM), ingrese a la vista de configuración de la consola web de ADM, en la sección **Generales** del menú principal, seleccione la opción **Licencias**. En la vista de información podrá visualizar información asociada al licenciamiento.



2. En la vista de información seleccione la pestaña **Archivos** y haga clic en el botón **Nuevo**.



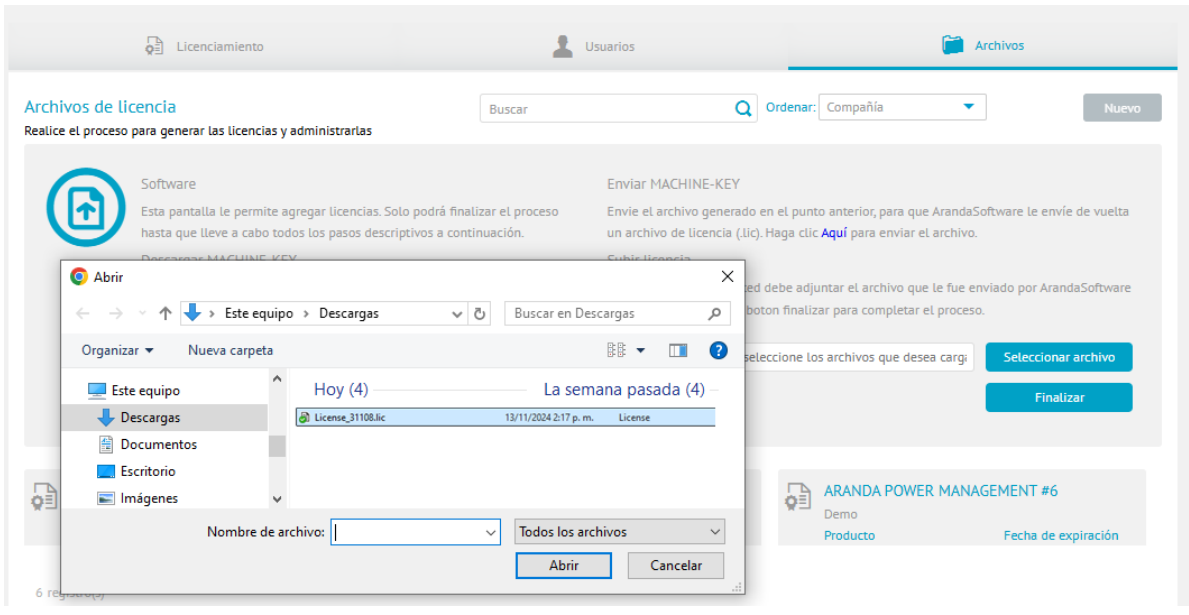
3. En la ventana que se habilita seleccione la opción Download MACHINE-KEY, haga clic en el enlace **Aquí**, que permite la descarga del archivo MachineKey.amk (archivo de licenciamiento), el cual debe ser enviado al área encargada en Aranda Software (Preventa y Proyectos) para la generación del archivo .lic (archivo de licenciamiento).



⚐ **Advertencia:** Una vez el usuario cargue desde la consola sus licencias compradas, el servicio común de licenciamiento debe permanecer en la misma máquina, de otra manera las licencias cargadas se perderán.

⚐ **Advertencia:** Si su servidor de aplicaciones se encuentra ubicado en una máquina virtual se recomienda instalar el servicio común de licenciamiento en una máquina física, ya que al reiniciar máquinas virtuales existe una alta probabilidad de que la marca de hardware cambie y el servicio asuma incorrectamente que fue trasladado.

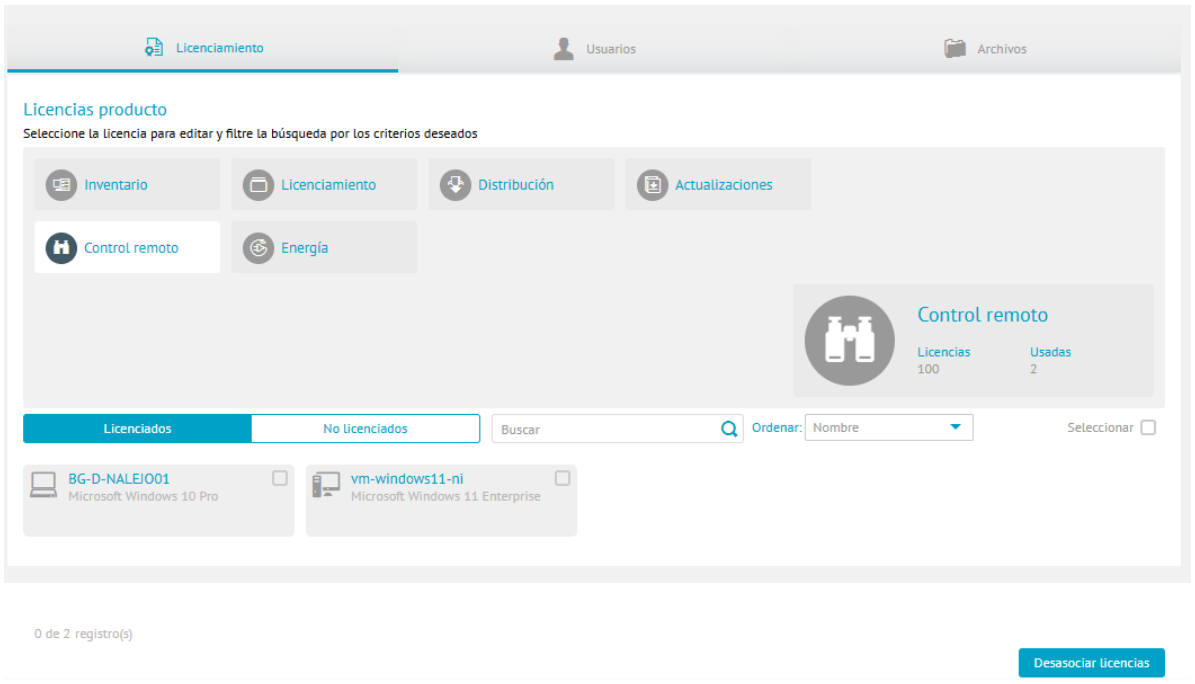
4. Una vez recibido el archivo .lic (archivo de licenciamiento), debe cargarlo al servidor, haga clic en el botón **Seleccionar archivo** y luego en **Finalizar**.



Visualizar/Asociar Dispositivos Licenciados

5. Para visualizar el detalle de la licencia y los dispositivos licenciados, en la vista de información de Licencias seleccione la pestaña **Licenciamiento** y la licencia por módulo de gestión de ADM (Inventario,Licenciamiento, distribución, actualizaciones, control remoto y energía). En las opciones Licenciados y No licenciados se agrupan los dispositivos encontrados.

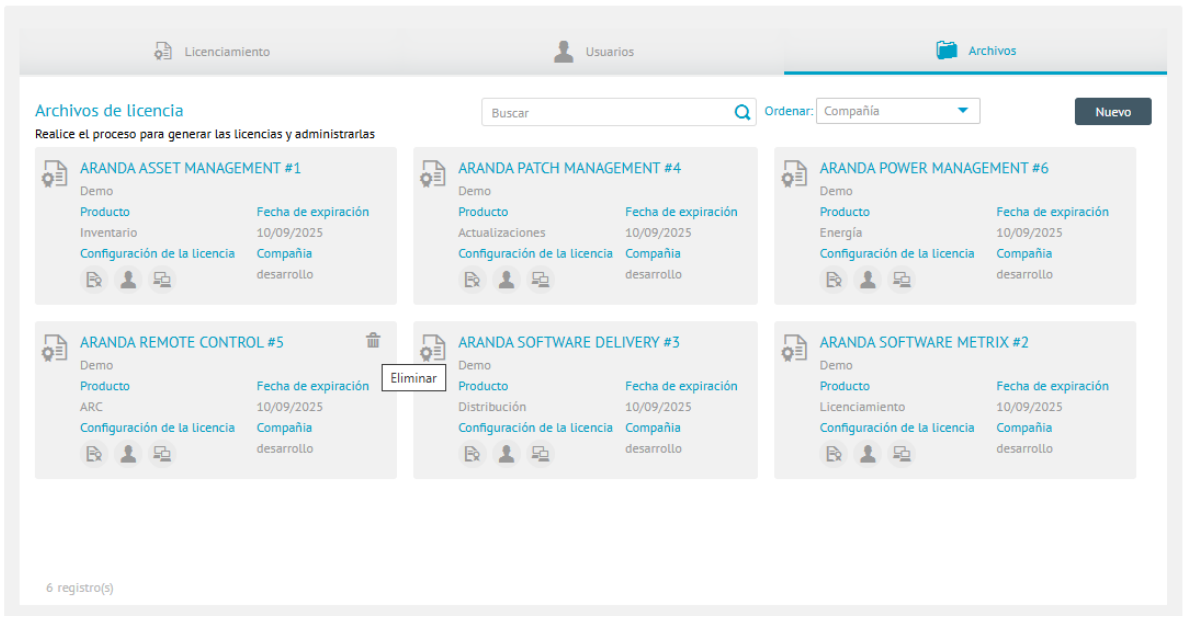
6. Al seleccionar uno o varios dispositivos podrá seleccionar el botón respectivo para **Asociar Licencias** o **Desasociar Licencias** a los dispositivos escogidos.



Eliminar Licencias

7. Para eliminar una licencias, en la vista de información de Licencias seleccione la pestaña **Archivos** y el registro de una licencia. Haga clic en el ícono de **Eliminar**

. Podrá visualizar un mensaje de confirmación de la acción; al dar Aceptar la licencia será eliminada.



Acceso ADM

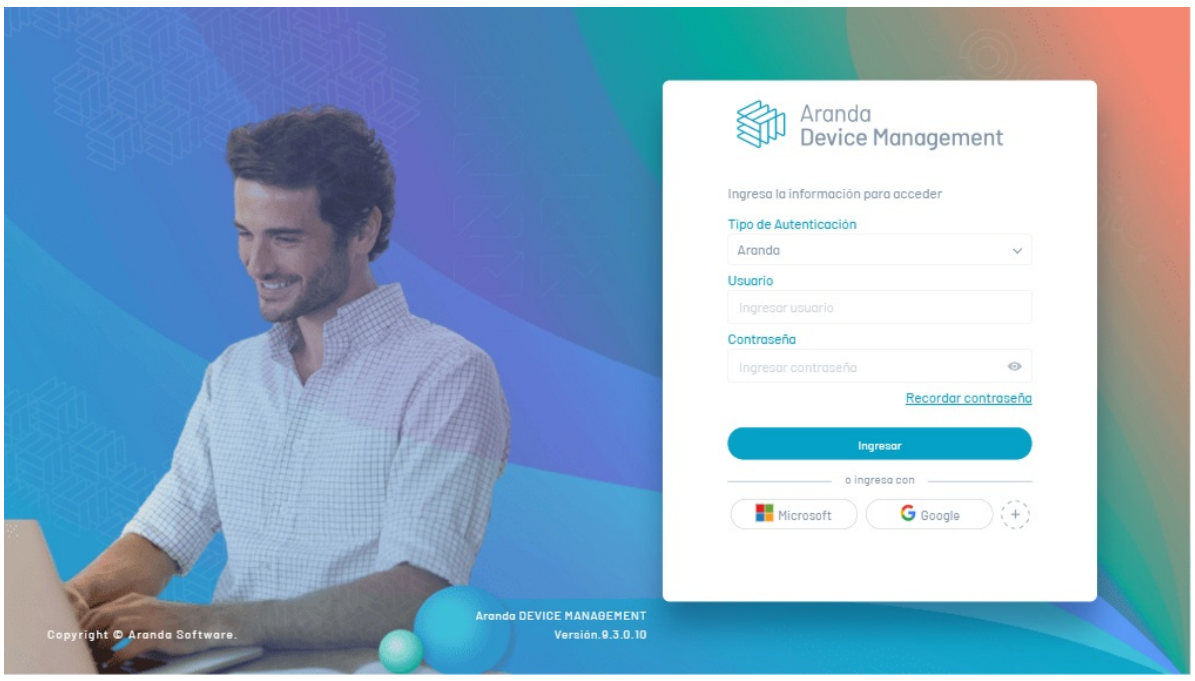
El proceso de autenticación a la consola web de ADM se ejecutará de acuerdo al rol definido por la organización para desarrollar las diferentes tareas de gestión y configuración de dispositivos. Las dos instancias de autenticación son:

Inicio de Sesión

1. Ingrese la url de la consola web de Aranda Device Management ADM.

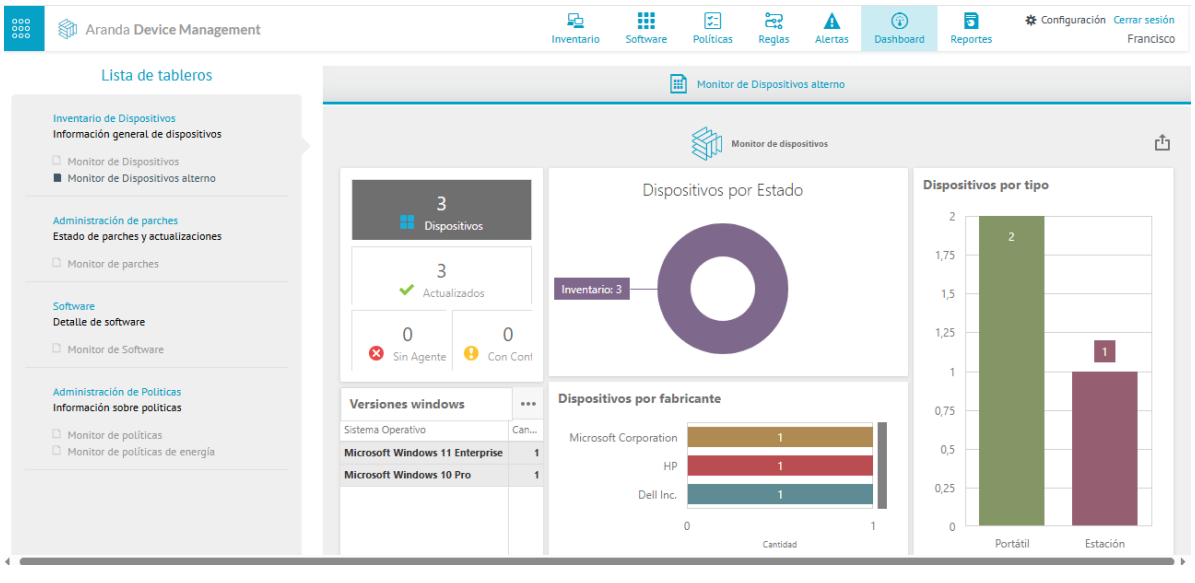
2. Para iniciar sesión en la aplicación de ADM ingrese el usuario y la contraseña que le han sido asignados.

> ⚐ **Nota:** Para ampliar la información de proceso de autenticación de los productos de Aranda (campos y proveedores de autenticación y olvido de contraseña), acceda al Módulo Login (Inicio de Sesión) de Aranda Common.



Cierre de Sesión

1. Cuando un usuario se encuentra en una sesión activa dentro de la consola web y requiere terminar la sesión y salir de la aplicación, en el menú encabezado de la consola selecciona el ícono de usuario y haga clic en **cerrar sesión**.



2. Una vez cerrada la sesión se vuelve a la pantalla de inicio y el usuario puede ingresar nuevamente a la consola.

Actualización

Actualización ADM

En los procesos de actualización de ADM, posterior a la instalación, debe tener en cuenta los siguientes componentes a actualizar:

- Actualización Consola ADM.
- Actualización del Agente ADM.
- Actualización Manual del Conserver.
- Actualización del Conserver por Proyecto de Distribución.
- Actualización Visor de Soporte Remoto.

> ⚐ **Importante:** Para garantizar el correcto funcionamiento de la aplicación después de una actualización a la versión más reciente, actualice los siguientes componentes:

- Agente de Descubrimiento (a partir de la versión 9.21.1, el agente de descubrimiento se actualiza automáticamente)
- Visor de soporte remoto (Aranda ADM Utils) o Visor de soporte remoto especialista (Aranda Virtual Support Specialist), dependiendo de la versión de control remoto que esté utilizando.
- Agentes de los dispositivos finales (a partir de la versión 9.21.2, los agentes de Windows se actualizan automáticamente)

⚐ **Nota:** La última versión publicada del Visor de soporte remoto (Aranda ADM Utils) es la 9.22.0. A partir de la versión ADM 9.22.1, no se lanzarán nuevas versiones de Aranda ADM Utils; sin embargo, se garantizará el correcto funcionamiento de futuras versiones de ADM en conjunto con la versión Aranda ADM Utils 9.22.0.

Actualización consola ADM

Antes de actualizar la consola ADM debe tener en cuenta las siguientes recomendaciones:

⚐ **CARPETAS A MOVER**: Durante la actualización, en caso de que existan, se deben mover las siguientes carpetas y su contenido desde el repositorio del repserver

- %dir_Repserver%\AgentUpdate
- %dir_Repserver%\Recordings

%dir_Repserver% hace referencia a la ruta configurada para el **Repserver** valor por defecto C:\Repserver\

Hacia el directorio configurado para el Content Manager.

La estructura debe conservarse tal cual, es decir:

- %dir_ContentManager%\AgentUpdate
- %dir_ContentManager%\Recordings

%dir_ContentManager% hace referencia a la ruta configurada para el **Content Manager** valor por defecto C:\ContentManager\

⚐ **IMPORTANTE:** Mantenga los nombres exactos de las carpetas (AgentUpdate y Recordings) para asegurar la compatibilidad con los servicios del sistema. Conserver.

⚐ **CONSECUENCIAS DE OMITIR LA ACCIÓN:** Si no se realiza el movimiento de estas carpetas:

- No se visualizarán correctamente las grabaciones en las auditorías.
- Se generarán inconsistencias en los registros de sistema.
- Los agentes no podrán ser descargados de forma correcta.

Para actualizar la consola de ADM tenga en cuenta las siguientes instrucciones:

1. Genere un backup de la base de datos que se va a actualizar.

2. Detenga los siguientes servicios Aranda manualmente o haciendo uso de Aranda DataBase Tools:

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

3. Desinstale desde el panel de control los programas Aranda Conserver Service y Aranda DEVICE MANAGEMENT.

4. Elimine los registros de las siguientes carpetas:

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

⚐ **Nota:**: No eliminar los contenidos de los repositorios del Contenedor, Repserver y Conserver.

1. Verifique los requisitos antes de ejecutar el instalador Aranda.ADM.Web.Installer.exe. Ver Instalación Consola ADM

2. Ejecute el instalador Aranda.Conserver.Installer.exe. No subir servicios hasta configurar el repserver y el **.config** de la carpeta del conserver. Ver Instalación Conserver

3. Ejecute Aranda DataBase Tools para que todos los archivos **.config** para que apunten a la base de datos migrada (ver pasos de ejecución en el documento de la KB).

4. Suba los servicios de Aranda, ya sea por la aplicación Aranda DataBase Tools o por la lista de servicios:

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

5. Verifique la conexión del repserver desde la consola web.

6. En caso de tener el servicio Mosquitto MQTT se debe desinstalarVer desintalacion en la sección Desinstalación Broker Mosquitto MQTT, luego ejecutar el instalador bróker MQTT.Instalación Aranda MQTT Broker

7. Configure el archivo Aranda.Conserver.Windows.Service.exe.config que está en la carpeta **%Program Files(x86)%\Aranda\Conserver**.

8. Inicie el servicio **Aranda Conserver V9**.

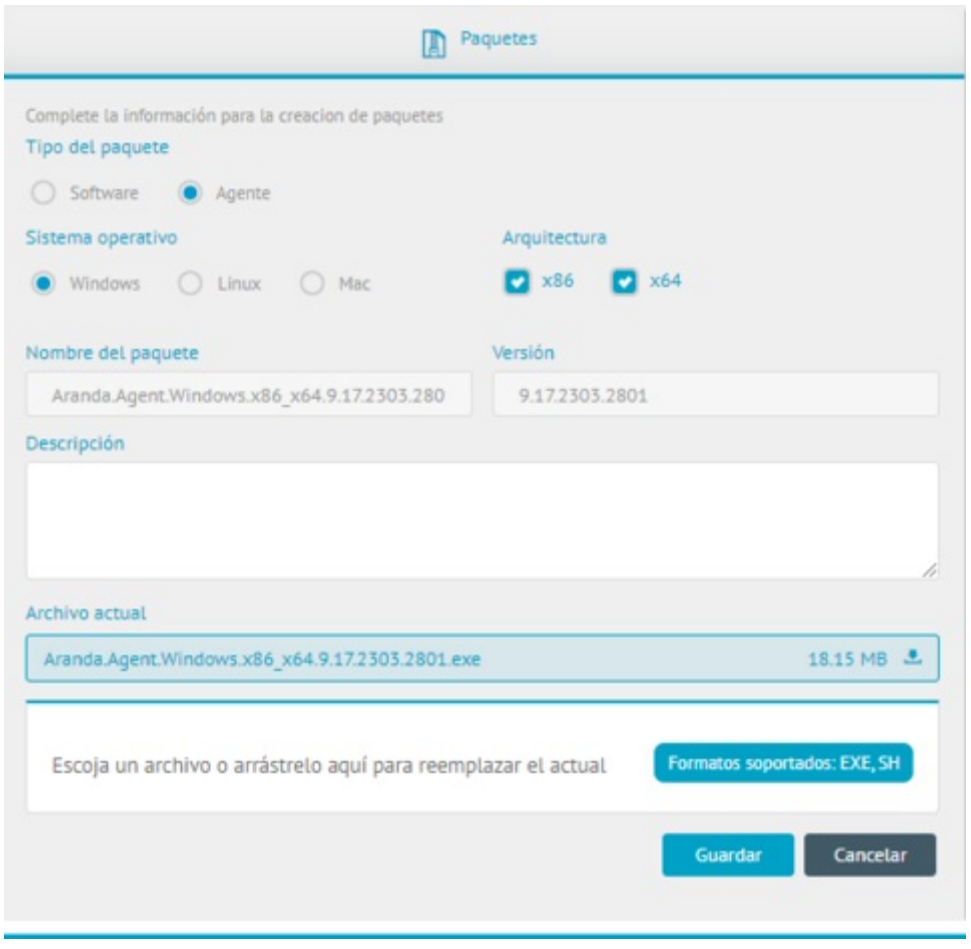
9. Verifique que todos los servicios de Aranda estén en ejecución.

> ⚐ **Nota:**
> - En caso de ser requerida la desinstalación de un producto de Aranda diferente de ADM, se genera un error al ingresar a la consola de ADM y no será posible acceder.
> - Para la instalación de la consola ADM y Conserver se requiere que el servidor tenga la versión 4.8 del framework de .NET (net48)
> - Recordar actualizar el agente de las diferentes máquinas para que puedan acceder a los últimos cambios; para esto recomendamos:
>
> Actualización por política de dominio.
> Actualización por distribución de agente (Conserver en la red del cliente).
> Actualización manual.

Actualización automática del Agente

Paquete de agente para Windows

1. El agente de windows con extensión **.exe** se cargara automáticamente en la consola de administración de ADM, en la sección de **Configuración ADM** del menú principal, opción **Paquetes** en el rango de un día después de la actualización del sitio de ADM.



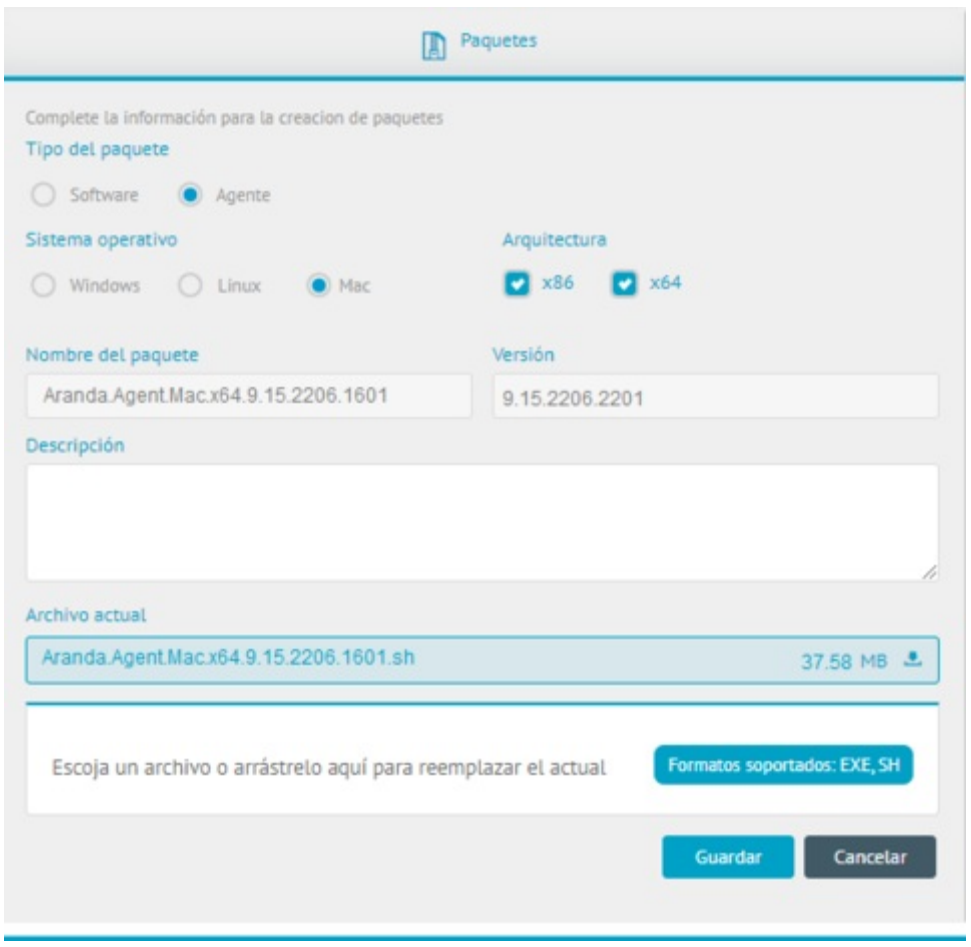
⚐ **Nota:**
-Transcurridas 12 horas, después de la instalación o actualización de la consola de ADM, el agente de ADM intentará actualizarse con la versión más reciente publicada para la versión de la consola. Si desea forzar la actualización, desde el listado de dispositivos, podrá ejecutar la acción de **Actualizar agente**

- A partir de la versión 9.23.0 del agente de ADM, ya no es necesario subir el paquete tipo Agente desde la consola de ADM para la actualización del agente.

Actualización del Agente MacOs

1. Para realizar la actualización automática del agente MacOs, ingrese a la consola de administración de ADM, en la sección de **Configuración ADM** del menú principal, seleccione la opción **Paquetes** . En la vista de información, haga clic en **Más Opciones** y **Paquete**.

Cargue el archivo de instalación con extensión **.sh**.



2. Al terminar de cargar el agente haga clic en **Guardar**

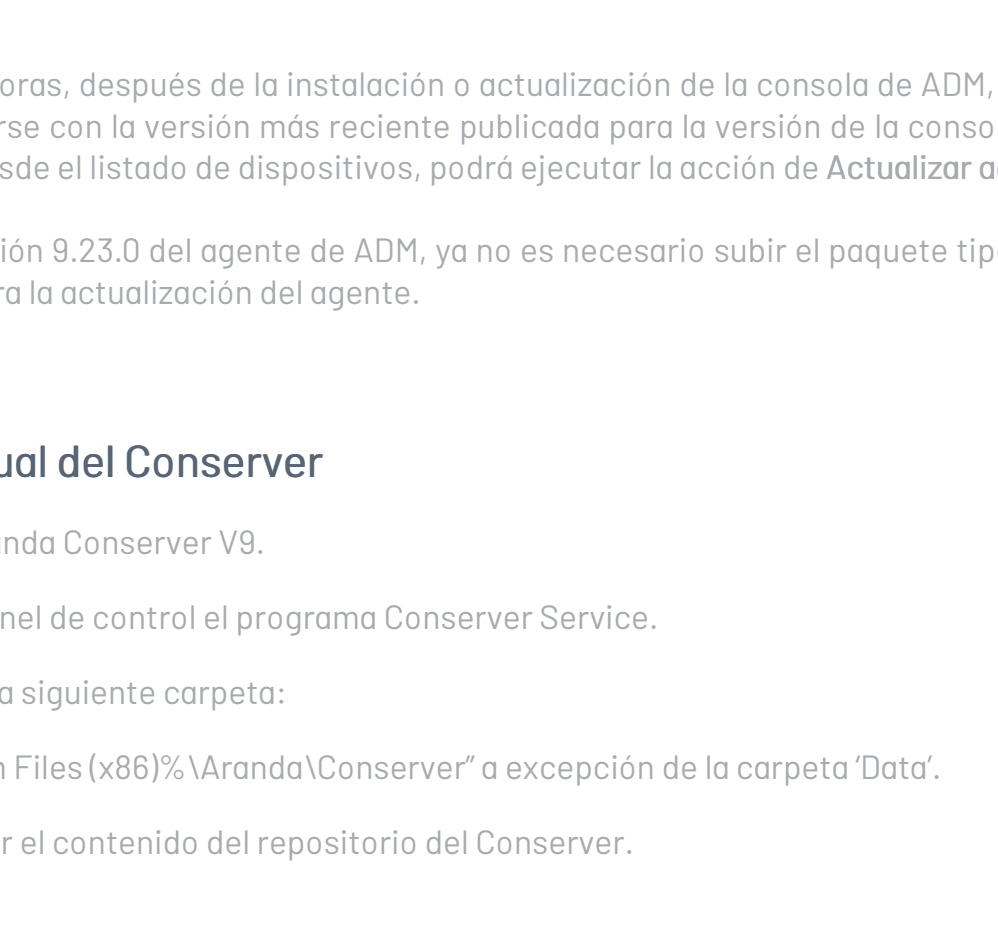
⚐ **Nota:**
-Transcurridas 12 horas, después de la instalación o actualización de la consola de ADM, el agente de ADM intentará actualizarse con la versión más reciente publicada para la versión de la consola. Si desea forzar la actualización, desde el listado de dispositivos, podrá ejecutar la acción de **Actualizar agente**

- A partir de la versión 9.23.0 del agente de ADM, ya no es necesario subir el paquete tipo Agente desde la consola de ADM para la actualización del agente.

Paquete de agente para Linux

1. Para realizar la actualización automática del agente Linux, ingrese a la consola de administración de ADM, en la sección de **Configuración ADM** del menú principal, seleccione la opción **Paquetes** . En la vista de información, haga clic en **Más Opciones** y **Paquete**.

Cargue el archivo de instalación con extensión **.sh**.



⚐ Nota:
-Transcurridas 12 horas, después de la instalación o actualización de la consola de ADM, el agente de ADM intentará actualizarse con la versión más reciente publicada para la versión de la consola. Si desea forzar la actualización, desde el listado de dispositivos, podrá ejecutar la acción de **Actualizar agente**

- A partir de la versión 9.23.0 del agente de ADM, ya no es necesario subir el paquete tipo Agente desde la consola de ADM para la actualización del agente.

Actualización Manual del Conserver

1. Detenga el servicio Aranda Conserver V9.

2. Desinstale desde el panel de control el programa Conserver Service.

3. Elimine el registro de la siguiente carpeta:

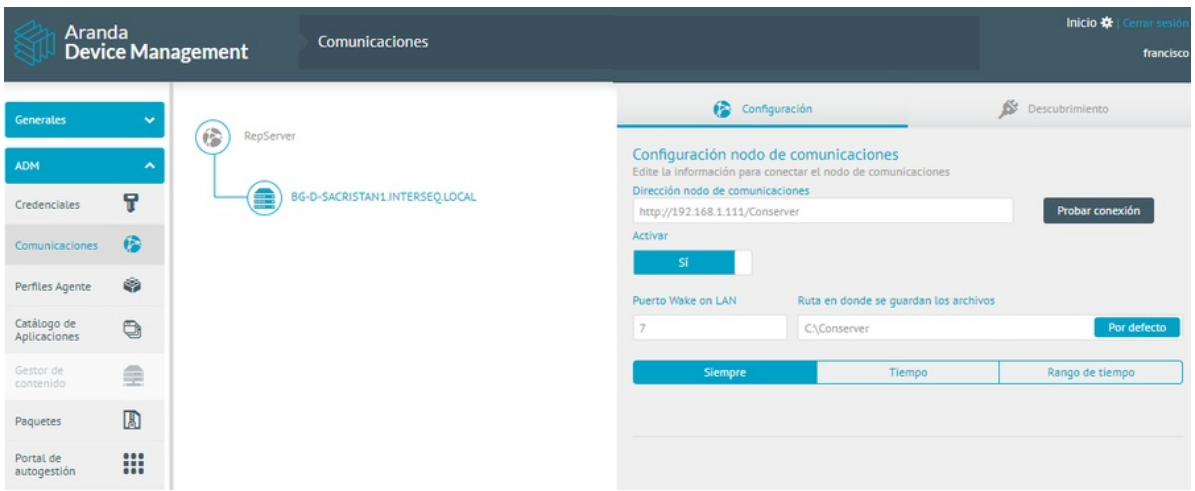
- Carpeta "%Program Files (x86)%\Aranda\Conserver" a excepción de la carpeta 'Data'.

  ⚐ **Nota:** No eliminar el contenido del repositorio del Conserver.

4. Ejecute el instalador Aranda.Conserver.Installer.exe. No subir el servicio hasta configurar el .config de la carpeta del conserver. Ver Instalación Conserver..

5. Inicie el servicio Aranda Conserver V9.

6. Para verificar la conexión exitosa del conserver, ingrese a la consola de administración de ADM, en la sección de **Configuración ADM** del menú principal, seleccione la opción **Comunicaciones** . En la vista de información, en el árbol de comunicaciones, haga clic sobre el nodo del Repserver y seleccione el conserver. En la vista detalle en la pestaña **Configuración** haga clic en el botón **Probar Conexión**



⚐ **Nota:** Para la instalación del Conserver se requiere que el servidor tenga la versión 4.8 del framework de .NET o una versión posterior.

Enlaces Relacionados: La actualización del conserver también puede realizarse a través de un proyecto de distribución. Actualización del Conserver por proyecto de distribucion

Actualización del conserver mediante proyecto de Distribución

Actualización de version 9.16 a 9.17 »

Actualización de versiones posteriores a 9.17 »

Precondiciones

- El servidor del conserver debe tener un agente instalado, apuntando al repserver y con el módulode distribucion activado en el perfil del agente.
- El agente instalado en el conserver debe tener un perfil de agente sin listado de nodos de comunicación.

Actualización de version 9.16 a 9.17

⚐ **Nota:** Para la instalación del Conserver se requiere que el servidor tenga la versión 4.8 del framework de .NET o una versión posterior

1. Crear un archivo con extensión .bat *(ej: UpdateConserver.bat)*

2. Copiar y editar el siguiente script en el archivo creado y guárdelo.

⚐ **Nota:**
- Ingresar en la variable path la ruta donde se encuentra instalado el conserver.
- Ingresar en la variable conserver el nombre completo del instalador del conserver
- Si tiene más de un conserver y se encuentran instalados en una ruta diferente debe crear un .bat y un proyecto diferente por cada uno de los conserver

```
:: 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. Crear un archivo con extensión .config y nombrarlo Aranda.Conserver.Windows.Service.exe.config

2. Copiar, configurar los campos de la llave <appSettings> y guardar.

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="dataConfiguration"
type="Microsoft.Practices.EnterpriseLibrary.Data.Configuration.DatabaseSettings,
Microsoft.Practices.EnterpriseLibrary.Data, Version=6.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
requirePermission="true" />
    <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 --
>
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection,
EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />
  </configSections>
  <connectionStrings>
    <add name="local" connectionString="Data Source=Data\local.dat;busytimeout=60"
providerName="System.Data.SQLite.EF6" />
  </connectionStrings>
  <appSettings>
    <add key="dataConfiguration:defaultDatabase" value="local" />
    <add key="Serilog:MinimumLevel" value="Debug" />
    <add key="Serilog:WriteTo:0:Name" value="File" />
    <add key="Serilog:WriteTo:0:Args:path" value="Logs\log.txt" />
    <add key="Serilog:WriteTo:0:Args:shared" value="true" />
  <add key="Serilog:WriteTo:0:Args:rollingInterval" value="Day" />
    <add key="Logging:LogLevel:Default" value="Information" />
    <add key="serverAddress" value="" />
    <add key="enableProxy" value="false" />
    <add key="proxyAddress" value="" />
    <add key="proxyUser" value="" />
    <add key="proxyPassword" value="" />
    <add key="privateIp" value="" />
    <add key="publicIp" value="" />
    <add key="mqttServerPort" value="1884" />
    <add key="mqttIp" value="" />
    <add key="publicServerPort" value="80" />
    <add key="privateServerPort" value="80" />
    <add key="p2pPort" value="9501" />
    <add key="maxDistributionSleepMsPerThread" value="8" />
    <add key="maxDistributionThreads" value="4" />
    <add key="enableDiscoveryCommon" value="1" />
    <add key="SecondsPingRemoteServer" value="60" />
    <add key="enableSecurity" value="false" />
  </appSettings>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.8" />
  </startup>
  <entityFramework>
    <providers>
      <provider invariantName="System.Data.SQLite" type="System.Data.SQLite.EF6.SQLiteProviderServices,
System.Data.SQLite.EF6" />
      <provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices,
EntityFramework.SqlServer" />
      <provider invariantName="System.Data.SQLite.EF6" type="System.Data.SQLite.EF6.SQLiteProviderServices,
System.Data.SQLite.EF6" />
    </providers>
    <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
      <parameters>
        <parameter value="mssqllocaldb" />
      </parameters>
    </defaultConnectionFactory>
  </entityFramework>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-13.0.0.0" newVersion="13.0.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <assemblyIdentity name="DotNetZip" publicKeyToken="6583c7c814667745" culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-1.14.0.0" newVersion="1.14.0.0" />
      </dependentAssembly>
      <dependentAssembly>
        <publisherPolicy apply="no" />
        <assemblyIdentity name="Oracle.ManagedDataAccess" publicKeyToken="89b483f429c47342" culture="neutral" />
        <bindingRedirect oldVersion="4.121.0.0 - 4.65535.65535.65535" newVersion="4.122.19.1" />
      </dependentAssembly>
      <dependentAssembly>
```

```
            <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Extensions.Configuration.Abstractions"
publicKeyToken="adb9793829ddae60" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Extensions.Configuration" publicKeyToken="adb9793829ddae60"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Extensions.Configuration.EnvironmentVariables"
publicKeyToken="adb9793829ddae60" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.IdentityModel.Logging" publicKeyToken="31bf3856ad364e35" culture="neutral"
/>
            <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.IdentityModel.Tokens" publicKeyToken="31bf3856ad364e35" culture="neutral"
/>
            <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.IdentityModel.Tokens.Jwt" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Diagnostics.DiagnosticSource" publicKeyToken="cc7b13ffcd2ddd51"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.ValueTuple" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.0.3.0" newVersion="4.0.3.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Threading.Tasks.Extensions" publicKeyToken="cc7b13ffcd2ddd51"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.2.0.1" newVersion="4.2.0.1" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Bcl.AsyncInterfaces" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Buffers" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.0.3.0" newVersion="4.0.3.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="RestSharp" publicKeyToken="598062e77f915f75" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-106.13.0.0" newVersion="106.13.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Extensions.Configuration.Binder" publicKeyToken="adb9793829ddae60"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Extensions.Logging.Abstractions" publicKeyToken="adb9793829ddae60"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.1" newVersion="6.0.0.1" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Owin" publicKeyToken="31bf3856ad364e35" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.2.2.0" newVersion="4.2.2.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Text.Encodings.Web" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.0.5.1" newVersion="4.0.5.1" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Text.Json" publicKeyToken="cc7b13ffcd2ddd51" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-6.0.0.6" newVersion="6.0.0.6" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="System.Web.Http" publicKeyToken="31bf3856ad364e35" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-5.2.9.0" newVersion="5.2.9.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Owin.Security" publicKeyToken="31bf3856ad364e35" culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.2.2.0" newVersion="4.2.2.0" />
          </dependentAssembly>
          <dependentAssembly>
            <assemblyIdentity name="Microsoft.Owin.Security.OpenIdConnect" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
            <bindingRedirect oldVersion="0.0.0.0-4.2.1.0" newVersion="4.2.1.0" />
```

```
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.Owin.Security.Cookies" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-4.2.1.0" newVersion="4.2.1.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.Extensions.Logging" publicKeyToken="adb9793829ddae60" culture="neutral"
/>
              <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.Extensions.DependencyInjection.Abstractions"
publicKeyToken="adb9793829ddae60" culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.Extensions.Options" publicKeyToken="adb9793829ddae60" culture="neutral"
/>
              <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.Extensions.Primitives" publicKeyToken="adb9793829ddae60"
culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.IdentityModel.JsonWebTokens" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.IdentityModel.Protocols" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.IdentityModel.Protocols.OpenIdConnect"
publicKeyToken="31bf3856ad364e35" culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="System.Net.Http.Formatting" publicKeyToken="31bf3856ad364e35" culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-5.2.9.0" newVersion="5.2.9.0" />
            </dependentAssembly>
            <dependentAssembly>
              <assemblyIdentity name="Microsoft.IdentityModel.Abstractions" publicKeyToken="31bf3856ad364e35"
culture="neutral" />
              <bindingRedirect oldVersion="0.0.0.0-6.23.1.0" newVersion="6.23.1.0" />
            </dependentAssembly>
          </assemblyBinding>
        </runtime>
        <system.data>
          <DbProviderFactories>
            <remove invariant="System.Data.SQLite.EF6" />
            <add name="SQLite Data Provider (Entity Framework 6)" invariant="System.Data.SQLite.EF6" description=".NET
Framework Data Provider for SQLite (Entity Framework 6)" type="System.Data.SQLite.EF6.SQLiteProviderFactory,
System.Data.SQLite.EF6" />
            <remove invariant="System.Data.SQLite" />
            <add name="SQLite Data Provider" invariant="System.Data.SQLite" description=".NET Framework Data Provider for
SQLite" type="System.Data.SQLite.SQLiteFactory, System.Data.SQLite" />
          </DbProviderFactories>
        </system.data>
        <system.serviceModel>
          <behaviors>
            <serviceBehaviors>
              <behavior name="">
                <serviceMetadata httpGetEnabled="true" httpsGetEnabled="true" />
                <serviceDebug includeExceptionDetailInFaults="false" />
              </behavior>
            </serviceBehaviors>
          </behaviors>
          <services>
            <service name="Aranda.Conserver.Ws.Service1">
              <endpoint address="" binding="basicHttpBinding" contract="Aranda.Conserver.Ws.IService1">
                <identity>
                  <dns value="localhost" />
                </identity>
              </endpoint>
              <endpoint address="mex" binding="mexHttpBinding" contract="IMetadataExchange" />
              <host>
                <baseAddresses>
                  <add baseAddress="http://localhost:8733/Design_Time_Addresses/Aranda.Conserver.Ws/Service1/" />
                </baseAddresses>
              </host>
            </service>
          </services>
        </system.serviceModel>
      </configuration>
```

3. Crear un Paquete de distribución tipo **copia** con el instalador del consever.

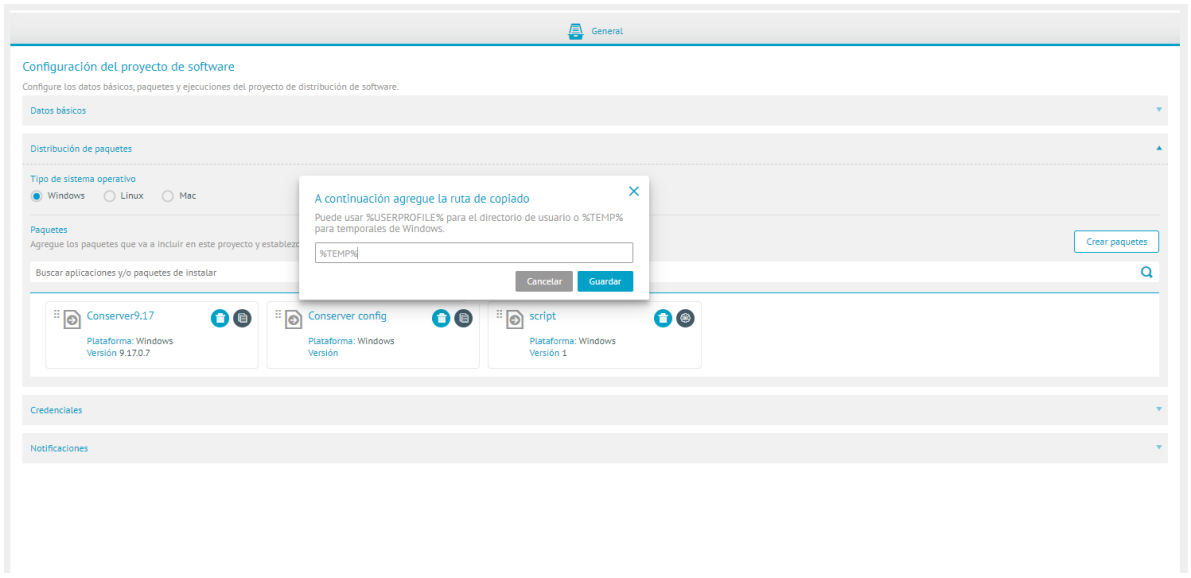
4. Crear un Paquete de distribución tipo **copia** con el archivo Aranda.Conserver.Windows.Service.exe.config creado en los pasos 3 y 4.

5. Crear un nuevo Paquete de distribución tipo **ejecución** con el archivo .bat creado en los pasos 1 y 2.

6. Ingrese a la gestión de Distribución de ADM y cree un proyecto de Distribución de Software.

7. En el proyecto agregue los paquetes creados en los pasos 5, 6 y 7 en el siguiente orden:

- Paquete del instalador del conserver *(Paquete tipo copia)* agregando como ruta %TEMP%.
- Paquete Aranda.Conserver.Windows.Service.exe.config *(Paquete tipo copia)* agregando como ruta %TEMP%.
- Paquete UpdateConserver.bat *(Paquete de tipo ejecución)*



8. Ejecute la distribución en el equipo a realizar la actualización del conserver.

> ⚐ **Nota:** Si tiene más de un conserver y se encuentran instalados en una ruta diferente, debe crear un .bat, un .config y un proyecto diferente por cada uno de los conserver. Si los conserver mantienen la ruta de instalación y tienen la misma configuración se pueden enviar en el mismo proyecto de distribución

9. En la configuración ADM defina los componentes de comunicación del reserver/conserver y compruebe la conexión.

Actualizacion de versiones posteriores a 9.17

Para realizar la actualización del conserver mediante proyecto de distribución es necesario seguir los siguientes pasos:

1. Crear un archivo con extensión .bat *(ej: UpdateConserver.bat)*

2. Copiar y editar el siguiente script en el archivo creado y guárdelo.

> ⚐ Nota:
> - Ingresar en la variable path la ruta donde se encuentra instalado el conserver.**
> - Ingresar en la variable conserver el nombre completo del instalador del conserver
> - Si tiene más de un conserver y se encuentran instalados en una ruta diferente debe crear un .bat y un proyecto diferente por cada uno de los conserver

```
:: 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
```

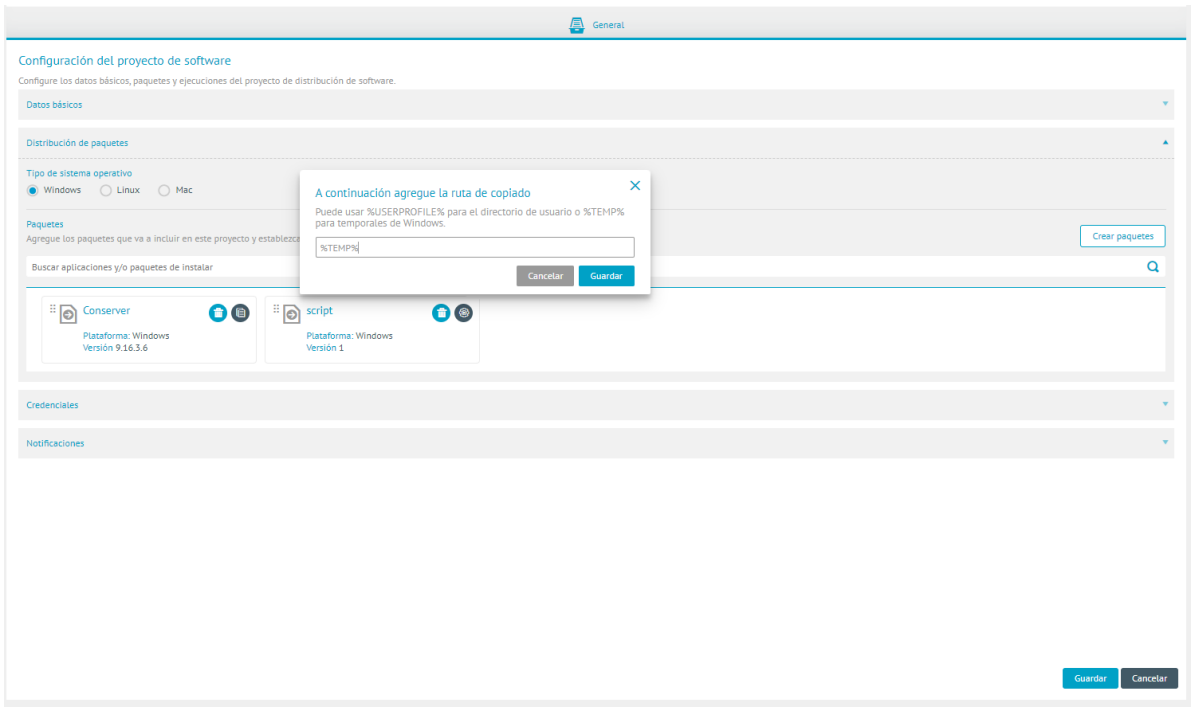
```
sc start ArandaConserverWindowsServiceV9

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

3. Crear un Paquete de distribución tipo **copia** con el instalador del consever.

4. Crear un nuevo Paquete de distribución tipo **ejecución** con el archivo .bat creado en los pasos 1 y 2.

5. Ingrese a la gestión de distribución de ADM y cree un proyecto de Distribución de software.

6. En el proyecto agregue los paquetes creados en el paso 3 y 4 adicionando primero el paquete del instalador del conserver *(Paquete tipo copia)*agregando como ruta %TEMP%.



7. Ejecute la distribución en el equipo a realizar la actualización del conserver.

> ⚐ **Nota:**
> - Si tiene más de un conserver y se encuentran instalados en una ruta diferente, debe crear un .bat y un proyecto diferente por cada uno de los conserver. Si los conserver mantienen la ruta de instalación se pueden enviar en el mismo proyecto de distribución.

Si la distribución ha sido exitosa, el conserver queda actualizado.

8. En la configuración ADM defina los componentes de comunicación del reserver/conserver y compruebe la conexión.

Actualización Visor de Soporte Remoto

Para actualizar el Visor de Soporte Remoto sigua los siguentes pasos:

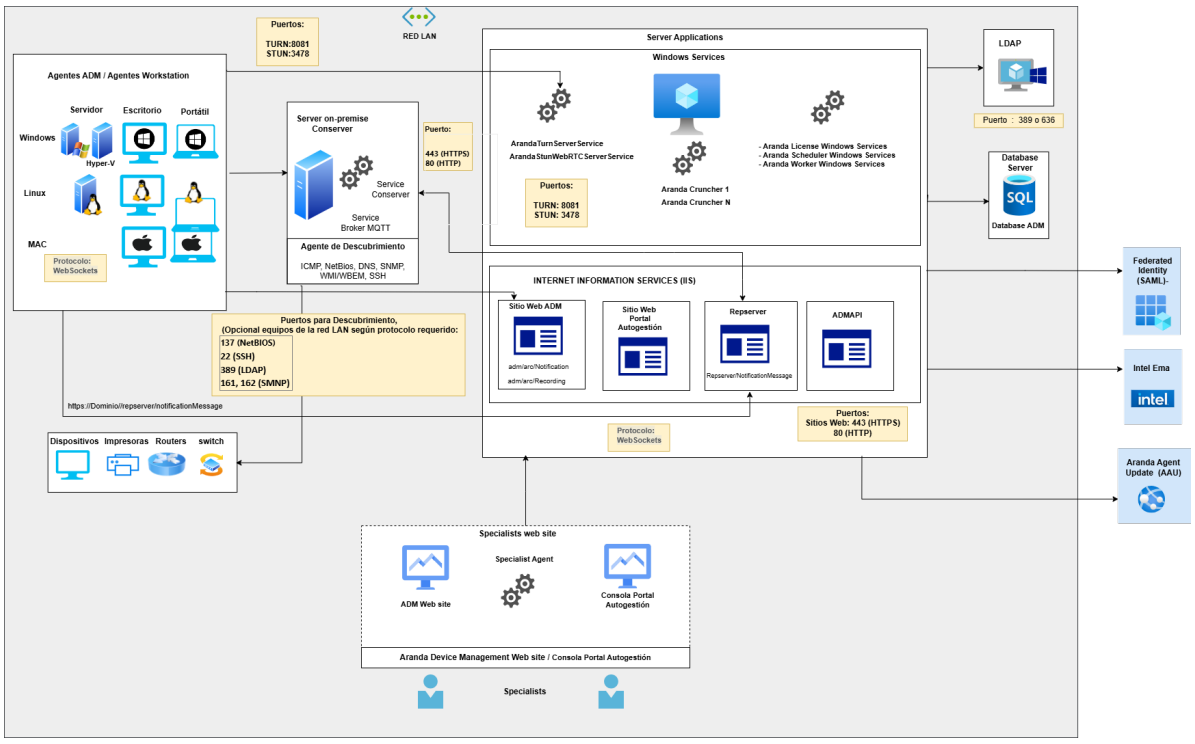
1. Ingrese a **Panel de control** > **Programas** > **Programas y Caracteristicas**, seleccione **Aranda ADM Utils** y haga clic en **Desinstalar**

2. Desintalada la version anterior podrá iniciar la instalación de la nueva version [Ver Instalación del Visor de Soporte Remoto]

Estructuras ADM

Estructura Onpremise

La estructura y funcionamiento de Aranda Device Management ADM es una aplicación distribuida en los siguientes componentes:



Base de Datos (servidor en la infraestructura del cliente)

Repositorio donde se almacena toda la información del sistema. La base de datos guarda la información de inventario de hardware, software y archivos de todas las estaciones de trabajo.

Servidor Aplicaciones

Este servidor contiene la lógica de negocio, así como también los módulos Mailer, DB Manager, Conserver y Cruncher. Adicionalmente, se comunica con la Consola Web para desplegar allí la información contenida en Base de Datos.

Conserver

El Conserver (servidor de comunicaciones) actúa como enlace entre los componentes del servidor de aplicaciones y la red LAN del cliente. Este es un servicio Windows que debe estar ubicado en la red LAN para poder enviar y recibir mensajes de los agentes instalados en cada máquina facilita los procesos de descubrimiento, distribución y administración remota. Dependiendo de la topología se deberá instalar un Conserver por cada segmento de red.

Cruncher

Servicio instalado en el servidor donde se instala la consola, es el encargado de procesar los inventarios guardarlos en la base de datos. Para esto, desencripta, descomprime y almacena los datos recogidos por cada estación. Existen 2 cruncher:

Agente ADM

El agente de Aranda Device Managment es el componente instalado en los dispositivos del cliente se encarga de

generar, comprimir, encriptar y enviar vía TCP/IP el inventario de hardware y software en cada una de las estaciones de trabajo; así mismo permite la generación de inventarios y la administración segura de comandos provenientes del servidor.

Este componente instalado del lado del cliente. Se puede instalar de forma local y/o remota en cada estación de trabajo.

Repserver

Este componente se instala en el servidor de aplicaciones y se encarga de recibir las solicitudes provenientes de la red LAN del cliente o de equipos que se encuentren conectados directamente a través de Internet.

Servidor Web Repserver

Este componente se instala en el servidor de aplicaciones y contiene el Internet Information Services IIS y .Net Framework, en el cual se instala la aplicación para la Consola Web de administración.

Consola Web

A través de esta interfaz que visualiza el cliente, el usuario o administrador, podrá gestionar y visualizar los inventarios de hardware y softtware por estación de trabajo, realizar seguimiento y control a sus recursos de TI, realizar tareas de control remoto.

Portal de autogestión

Esta interfaz que visualiza el cliente, permite a los usuarios responsables de los dispositivos, visualizar los proyectos de distribución de software disponibles y realizar la instalación de manera desatendida.

Broker MQTT

Este servicio ubicado en la red LAN del cliente, permite gestionar y controlar las acciones de mensajería enviadas a la consola web en tiempo real.

Facilita la comunicación con los diferentes dispositivos que se están gestionando, permite que las solicitudes a los dispositivos lleguen en tiempo real, para las comunicaciones de los dispositivos dentro de la red LAN empresarial, se puede instalar el servicio en el servidor del conserver u otro servidor que se encuentre en la red LAN, es necesario abrir el puerto 1884 o 1883.

Turn Server

Cuando dos dispositivos no pueden establecer una conexión directa entre sí, se necesita un servidor Turn para facilitar la comunicación.

Es un servicio Windows instalado en una máquina virtual, que hace de puente para el control remoto entre el agente especialista y el agente de la estación de trabajo. Para activar esta funcionalidad, ambos agentes establecen una conexión con el Turn Server, el cual está a la escucha en el puerto 8081 o el parametrizado para su funcionamiento en Onpremises, se retrasmiten los datos de un agente al otro. (Cloud, puerto de escucha definido 3478)

Agente Especialista

Está diseñada para permitir el acceso al control remoto, transferencias de archivos y realizar las grabaciones para las auditorías. Cada especialista debe instalar esta aplicación en la máquina donde trabaja.

Agente Workstation

Componente instalado en los dispositivos Windows en arquitecturas, se encargan de recibir el soporte remoto. Puede ubicarse tanto dentro como fuera de la infraestructura del cliente.

Puertos

Puertos de comunicación usados por Aranda Device Management (ADM) para permitir las comunicaciones requeridas.