



Aranda Device Management

O ADM é uma solução que gerencia os ativos de TI de hardware e software da organização, realizando tarefas remotas de monitoramento e controle. Com base no conhecimento do inventário, você pode distribuir e manter o software atualizado nos dispositivos alcançados.

O conhecimento e acesso às etapas de instalação e atualização do ADM permite ao usuário definir e configurar os componentes necessários para o funcionamento do aplicativo. As orientações a ter em conta são as seguintes:



1. Instalação e caminho de acesso

Conheça os requisitos básicos para o correto funcionamento do aplicativo, acompanhe o processo de instalação do ADM dos diferentes componentes para o bom funcionamento e acesse a interface do produto para o gerenciamento e controle dos dispositivos descobertos.

2. Atualização

Identifique como executar atualizações nos componentes de funcionalidade, como o agente, o servidor e o visualizador de suporte remoto.

3. Estruturas

Aprenda sobre os componentes da estrutura ADM e identifique como eles se relacionam com a operação geral do produto.

¿Para quién es esta guía?

Este guia foi projetado para fornecer ao usuário um caminho seguro por meio do processo de instalação, configuração e atualização do ADM.

Qual é a nossa documentação?

- [Guia de introdução do ADM » de gerenciamento de dispositivos Aranda](#)
- [Guia de instalação e configuração do ADM OnPremise \(Você está AQUI\)](#)
- [Guia de instalação e configuração do ADM Cloud »](#)
- [Manual de gerenciamento de » ADM de gerenciamento de dispositivos Aranda](#)
- [Manual de Integração do Aranda ADM »](#)

Caminho de instalação do ADM OnPremise

Caminho de instalação do ADM / Arquitetura OnPremise

Abaixo está uma visão geral dos conceitos de instalação de software e os diferentes componentes usados para o bom funcionamento do Aranda Device Management ADM.

O processo de instalação da versão ADM OnPremise em um novo banco de dados deve levar em consideração as seguintes etapas:



1. Requisitos

Valide os requisitos mínimos de hardware e software para a instalación e operación do Aranda Device Management ADM.

Para obter mais informações, consulte os requisitos para instalar o ADM em ambientes de nuvem:

- [Requisitos do sistema](#)
- [Requisitos / Portas](#)
- [Requisitos/exclusões de antivírus](#)
- [Requisitos/Administração Remota](#)
- [Requisitos/control remoto](#)

2. Instalação ADM

A instalação do Aranda Device Management ADM em arquiteturas Cloud deve levar em consideração as seguintes etapas para instalar os diferentes componentes:

- [Instalador do Console da Web](#)
- [Instalador Conservador](#)
- [Instalador do Discovery Agent](#)
- [Instalador do MQTT Broker](#)
- [Instalador do navegador Mib](#)
- [Instalador de controle remoto](#)
- [Especialista em suporte remoto do Installer Viewer](#)
- [Instalador do Agente ADM](#)

3. Configuração do banco de dados

Configure cadeias de conexão para o banco de dados para sites e serviços relacionados.

- [Configuração de conexão de banco de dados](#)

4. Licenciamento

Gerencie as licenças adquiridas pelo cliente e gere a solicitação de licença para realizar o gerenciamento adequado do produto.

- [Licenciamento ADM](#)

5. Acesso ADM

O processo de autenticação no console da web do ADM será executado de acordo com a função definida pela organização para desenvolver as diferentes tarefas de gerenciamento de inventário.

- [Acesso ADM](#)

📌 **Nota:** Se você estiver instalando o software e os componentes do ADM em um novo banco de dados, poderá considerar as seguintes instruções:

[Instalação do ADM no novo banco de dados](#)

Requisitos

Configuração recomendada para a instalação de um conservador em um servidor, considerando as seguintes características e especificações:

Servidor Servidor

Sistema Operacional	Windows Server 2019 e Windows Server 2022
Núcleos	CPU Intel(R) Xeon(R) Platinum 8171M @ 2,60 GHz 2,10 GHz
CARNEIRO	8 GB
Disco	128 GB (HDD ou SSD)

📌 Tenha em mente:

1. Recomenda-se um limite máximo de 10.000 dispositivos a serem mantidos para garantir o desempenho ideal, considerando as características do servidor e garantindo que o uso da CPU não afete negativamente sua operação.
2. Ao instalar um conservador no mesmo servidor que o console ADM, recomenda-se um limite máximo de 3.500 dispositivos.
3. Se os agentes se conectarem diretamente a um Repserver local, é recomendável um limite máximo de 3.000 dispositivos.

Servidor de Banco de Dados do Azure

Cara	Banco de dados SQL (MS SQL 2019 ou superior na versão Standard/Enterprise Datacenter)
Tamanho	Mínimo de 5 GB
Informações adicionais	O banco de dados deve ser criado com Collate: SQL_Latin1_General_CP1_CI_AI
Observações	O espaço do banco de dados varia de acordo com o número de dispositivos e módulos que você ativou no ADM.

📌 Nota: [Consulte Exceções](#)

Agente de estação de trabalho

As versões do sistema operacional suportadas por este agente são:

Windows

Sistema operacional Windows	Versão
Windows 8.1	Pró
janelas 10	Pró
janelas 10	Casa
janelas 10	Empresa
janelas 11	Pró
janelas 11	Casa
janelas 11	Empresa
Servidor Windows	2016
Servidor Windows	2019
Servidor Windows	2022

📌 Nota:

O rótulo (32 bits) no Gerenciador de Tarefas indica que o processo está sendo executado no modo de compatibilidade por meio do [Subsistema Windows WOW64](#), que permite executar aplicativos de 32 bits em sistemas de 64 bits.

Observe que, dependendo da versão do seu computador e do sistema operacional, esse rótulo pode não aparecer. Por exemplo, em computadores com arquitetura de 32 bits, essa ID não é exibida.

O ADM Agent para sistemas Windows é compilado no formato x86 (32 bits) para garantir a compatibilidade em computadores de 64 bits e 32 bits. Portanto, ele é instalado no caminho C:\Arquivos de Programas (x86).

Esta condição não afeta o funcionamento do agente nem tem implicações para seu desempenho ou características.

Mac

Sistema operacional Mac	Versão
MacOS	Sequoia
MacOS	Fortuna
MacOS	Sonoma

📌 Nota:

- 1. Os seguintes processadores são suportados: Intel e Apple Silicon M1, M2 e M3
- 2. O agente não é compatível com versões de 32 bits do MacOS.

Linux

Sistema operacional Linux	Versão
Ubuntu	24.04 LTS
Ubuntu	22.04 LTS
Ubuntu	20.04 LTS
Chapéu vermelho	Enterprise Linux 9 LTS
Chapéu vermelho	Enterprise Linux 8.7 LTS

📌 Nota:

- 1. As versões do Ubuntu são suportadas para servidor e desktop nas versões LTS.
- 2. O agente não é suportado para distribuições Linux de 32 bits.

Requisitos/Portas

A seguir estão as portas de comunicação usadas pelo Aranda Device Management (ADM). A rede precisa ser configurada para permitir comunicações por essas portas.

Servidor de Console ADM

A seguir estão as portas e permissões necessárias no servidor de console ADM para a conexão de cada um dos seguintes componentes:

Site da ADM

80 (HTTP) ou 443 (HTTPS)	TCP, UDP	Porta de entrada: necessária para conexão de clientes ao servidor
--------------------------	----------	---

📌 Anotações:

- Para o módulo de atualização, o servidor deve ter uma saída completa para a internet para download de patches de atualização, dos sites oficiais de cada provedor e sua posterior distribuição em dispositivos gerenciados.

📌 Anotações:

- A configuração do servidor para permitir a visualização e downloads do site <https://download.arandasoft.com/updates> é necessária para facilitar os downloads automáticos de agentes no ADM

Notificações de controle remoto

443 (HTTPS)	TCP, UDP	Porta de entrada: necessária para a conexão dos agentes com o servidor de notificação
8081	TCP	Porta de entrada, destinada à conexão do Agente Especialista e do Agente da Estação de Trabalho com o Turn Server na tomada de controle remota, o uso de SSL deve estar habilitado no servidor.
	WebSockets	Eles estabelecem uma conexão bidirecional persistente entre o agente e o servidor.
3478	TCP	Porta de entrada, destinada a conectar o Specialist Agent e o Workstation Agent ao Stun Server na transferência de arquivos.
49152-65535	UDP	Porta de entrada, se você precisar que ele opere como um turno webRTC para receber conexões de entrada. Configurando o servidor WebRTC Stun/Turn

📌 **Anotações:**
- É necessário configurar o servidor, para visualizar o site no caso de ter a funcionalidade de Controle Remoto. <https://download.arandasoft.com/updates> e baixar arquivos

Repserver

80 (HTTP) ou 443 (HTTPS)	TCP, UDP	Porta de entrada: Necessária para a conexão de agentes e/ou Conservador, dependendo da arquitetura implementada
1884 (Opcional)	MQTT	Necessário apenas para saída, usado de acordo com a arquitetura implementada

Notificações do Repserver

WebSockets	Eles estabelecem uma conexão bidirecional persistente entre o agente ADM e o servidor, que é necessária para o Administração Remota
------------	---

📌 **Anotações:**
-- A funcionalidade de administração remota só será suportada em sites seguros com protocolo (Https).

- Para a funcionalidade de administração remota, você deve ter a comunicação habilitada por (TLS 1.2 ou 1.3). Para segurança de comunicação, versões anteriores do TLS não são suportadas.

Servidor ADM Conserver

Máquinas em redes locais podem se conectar a um servidor (servidor na rede local) para trabalhar com conexões locais e ter funcionalidades adicionais.

80 (HTTP) ou 443 (HTTPS)	TCP, UDP	Porta de entrada: Necessária para a conexão dos agentes com o servidor conservador
1884	MQTT	Necessário apenas para saída, destinado à conexão com o MQTT Broker

- 📌 **Anotações:**
- Para dispositivos de distribuição de agente devem estar dentro da mesma LAN, os dispositivos devem ter o recurso admin\$ compartilhado.
 - É necessário que o Usuário Windows do Aranda com quem será realizada a instalação e implantação dos Agentes tenha permissões de Instalação, preferencialmente administrador das máquinas correspondentes.
 - Para sistemas operacionais Linux e Mac, o uso do usuário raiz é necessário para a implantação do agente.

Agente de descoberta

Quando o cliente requer a funcionalidade de descoberta, ele é deve habilitar protocolos para que o equipamento possa ser encontrado e identificado na rede local.

137 (Opcional)	NETBIOS	Necessário apenas para saída, destinado à descoberta de dispositivos pelo protocolo NETBIOS
22 (Opcional)	SSH	Necessário apenas para saída, destinado à descoberta de dispositivos pelo protocolo SSH
389 (Opcional)	TCP, UDP	Necessário apenas para saída, destinado à descoberta pelo LDAP
161 (Opcional)	SNMP	Necessário apenas para saída, destinado à descoberta de dispositivos pelo protocolo SNMP

- 📌 **Anotações:**
- A porta 80 (HTTP) é necessária se o servidor não estiver configurado com HTTPS e os certificados SSL apropriados. O cliente deve habilitar o protocolo HTTPS e não por meio do protocolo HTTP.
 - Não é necessário habilitar sempre todos os protocolos. O ADM Discovery Module permite habilitar os protocolos necessários no processo.

Servidor de banco de dados

O servidor ADM armazena as informações em servidores, no SQL Server ou SQLAzul. Se você estiver usando o SQL Server como um repositório, precisará habilitar o comunicações com este servidor.

1433	TCP	Porta de entrada de protocolo do SQL Server no servidor de banco de dados
------	-----	---

Corretor MQTT

Para gerar notificações em tempo real para dispositivos, você pode usar um Servidor MQTT na rede local. Como resultado, você precisará habilitar o comunicações com o Broker MQTT.

1884	MQTT	A porta do MQTT Broker pode ser modificada, se necessário. Você só terá que habilitar a porta de entrada na máquina onde o MQTT Broker trabalha, para ambientes de nuvem ela é definida pela área de operações da Aranda
------	------	--

Gateway do ADM (Arquitetura Local – versões do ADM inferiores a 9.21.1)

Para fazer conexões de controle remoto, é possível instalar um ADM Gateway que permitir a conexão entre computadores que estão em redes locais diferentes ou quando uma conexão de um computador em uma rede local com computadores nas casas de empregados.

4443	TCP	A porta do ADM Gateway pode ser modificada, se necessário. Você só precisará habilitar a porta de entrada na máquina em que o ADM Gateway funciona
------	-----	--

Aranda ADM Utils Installer (Arquitetura local – versões ADM inferiores a 9.21.1)

Remote Support Viewer é um aplicativo que permite que você assuma o controle remoto de máquinas gerenciadas. Ele é instalado nos dispositivos dos usuários a partir dos quais a conexão deve ser feita por controle remoto, aplica-se a arquiteturas locais

9125 (Opcional)	TCP	Porta de saída: necessária para controle remoto entre dispositivos que estão na mesma LAN quando não estão usando um gateway
4443 (Opcional)	TCP	Necessário apenas para saída, destinado à conexão com o ADM Gateway para controle remoto entre computadores em diferentes redes locais

Agentes ADM

Os Agentes são instalados em cada um dos computadores que serão gerenciados por meio do através do ADM. Nas arquiteturas de conservador, os agentes são instalados em máquinas por meio de um processo distribuído guiado a partir do console, no entanto, existem várias alternativas de implantação que podem ser combinadas para cobrir diferentes cenários de infraestrutura.

As portas usadas no ADM variam dependendo da arquitetura e das funcionalidades necessárias.

Agente ADM

80 (HTTP) ou 443 (HTTPS)	TCP, UDP	Necessário apenas para saída, destinado à conexão com o ADM repserver ou ADM Conserver
1884	MQTT	Necessário apenas para saída, destinado à conexão com o MQTT Broker
9025 (Opcional)	TCP, UDP	Porta de entrada: necessária para a comunicação do servidor com o agente para Gerenciamento remoto , usado quando a arquitetura não permite que o servidor de notificação repserver seja exibido para comunicação. : https://Dominio/repserver/Notificationmessage .
	WebSockets (opcional)	Eles estabelecem uma conexão bidirecional persistente entre o agente ADM e o servidor de notificação repserver, necessária para o Gerenciamento remoto , usado quando a arquitetura permite que o servidor de notificação repserver seja exibido para comunicação. : https://Dominio/repserver/Notificationmessage .
9125 (opcional) - Versões ADM inferiores a 9.21.1	TCP	Porta de entrada: Necessária para controle remoto entre dispositivos que estão na mesma LAN quando não estão usando um Gateway
4443 (opcional) - Versões ADM inferiores a 9.21.1	TCP	Necessário apenas para saída, destinado à conexão com o ADM Gateway para controle remoto entre computadores em diferentes redes locais

Agente ADM (com recursos de descoberta)

137 (Opcional)	NETBIOS	Porta de entrada, destinada à descoberta de dispositivos pelo protocolo NETBIOS
22 (Opcional)	SSH	Porta de entrada, destinada à descoberta de dispositivos por meio do protocolo SSH
389 (Opcional)	TCP, UDP	Porta de entrada, destinada à descoberta pelo LDAP
161 (Opcional)	SNMP	Porta de entrada, destinada à descoberta de dispositivos pelo protocolo SNMP

- 📌 **Anotações:**
- Não é necessário habilitar sempre todos os protocolos. O A descoberta do ADM permite que você habilite os protocolos necessários no processo.
 - O agente ADM usa duas portas locais para estabelecer conexão de saída (TCP), como a conexão com o MQTT Broker e comunicações entre os processos do agente, ele lida com o ip do localhost e é dinâmico, escolhido pela placa de rede, geralmente são usados intervalos maiores que 1023 a 65535. Não exige que você faça nada na configuração.

Agente ADM (com funcionalidade de controle remoto)

Para a funcionalidade de controle remoto em uma arquitetura em nuvem e local, o agente ADM instala um Workstation Agent chamado “Aranda Remote Control Worksation”, para que a instalação automática seja realizada o agente ADM deve ser capaz de visualizar o domínio do repserver e tudo o que é após a instalação ser realizada. / : <https://Dominio/repserver/api/> e baixar arquivos desse site. Para se conectar a esses dispositivos, instale o visualizador do Agente Especialista, levando em consideração o seguinte [Requisitos e portas para os dois componentes do Remote Control Cloud e Onpremises ↗](#).

Requisitos/exclusões de antivírus

Os programas antivírus devem ser configurados com as seguintes inclusões nos computadores em que o ADM Agent será instalado:

Processo: Aranda.Agent.ACOREService.exe

Nome	Descrição	Rota
Aranda Agente 9	Agente de serviço	{InstallDir}\Aranda\Aranda Agente 9

Proceso:Aranda.Agent.RemoteCommand.exe

Nome	Descrição	Rota
	Instalação no Computer Discovery	C: \ Windows \ RemoteCommand \ Device \ HarddiskVolume3 \ Windows \ RemoteCommand

Processos: Aranda.Agent.ARSService.exe

Nome	Descrição	Rota
Controle Remoto Aranda Agent 9	Serviço de controle remoto	{InstallDir}\Aranda\Aranda Agente 9

Processos: APaaSPersist.msi

Nome	Descrição	Rota
APaaSPersist.msi	Agente de serviço	{InstallDir}\Aranda\Aranda Agente 9

- Se o agente ADM tiver a funcionalidade Controle remoto, você deverá adicionar as seguintes inclusões no antivírus:

Processos: Aranda.ARC.Workstation.exe

Nome	Descrição	Rota
Aranda.ARC.Workstation.exe	Serviço de agente ARC	{InstallDir} \ Aranda \ Aranda Controle Remoto \ Estação de Trabalho

Processos: Aranda.AVS.VNC.Application.exe

Nome	Descrição	Rota
Aranda.AVS.VNC.Application.exe	Serviço de agente ARC	{InstallDir} \ Aranda \ Aranda Controle Remoto \ Estação de Trabalho

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

Nome	Descrição	Rota
Aranda.AVS.TransferFile.Service.Target.exe	Serviço de agente ARC	{InstallDir} \ Aranda \ Aranda Controle Remoto \ Estação de Trabalho

Requisitos/Módulo de Administração Remota

Configure o gerenciamento remoto com base na arquitetura ADM instalada.

Portas e licenças necessárias

1. Por favor, leia atentamente as portas e permissões necessárias com base na arquitetura de instalação do ADM antes de passar para o próximo ponto.

- [Arquitetura local do agente ADM](#)
- [Console Web, Repserver, Servidor de Notificação Repserver](#)

Configuração por banco de dados

- Se a comunicação para administração remota for feita por meio do servidor de notificação do repserver, execute o seguinte script:

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

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

📌 **Nota:** Na visualização detalhada dos dispositivos inventariados pelo ADM, é possível visualizar as informações do dispositivo com [Administração Remota](#)

Requisitos/control remoto

Agente Especialista (Visualizador)

Para acessar os recursos de suporte remoto, o agente especializado deve ser instalado em um dispositivo que atenda às seguintes condições mínimas:

Dispositivo especializado	
Processador virtual	CPU de 2 núcleos
CARNEIRO	Mínimo de 4 GB
Espaço em disco	Mínimo de 4 GB

As versões do sistema operacional suportadas pelo agente especializado são:

Sistema Operacional	Versão
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
janelas 10	20H2
janelas 10	21H1
janelas 10	21H2
janelas 10	22H2
janelas 11	21H2
janelas 11	22H2

Os navegadores suportados são os seguintes:

Navegador	Versão
Borda	Versão >= 88
Google Chrome	Versão >= 97.0.4692.71

Portas usadas pelo Agente Especialista

Porta	Protocolo	Descrição
443	TCP	Necessário para a conexão do Agente Especialista com o servidor de gravação, ele deve ser capaz de visualizar o site: https://Dominio/adm/arc/recording
8081	TCP	Necessário apenas para saída, destinado à conexão do Agente Especialista com o Turn Server na tomada de controle remota.
	WebSockets	Eles estabelecem uma conexão bidirecional persistente entre o agente e o servidor.
3478	TCP	Necessário apenas para a saída, destinado à conexão do Agente Especialista com o Servidor de Atordoamento na transferência de arquivos.
15000 - 65000	UDP	Intervalo necessário apenas para a saída, destinado à conexão do Agente Especialista com o Stun Server na transferência de arquivos.

Agente de controle remoto Workstation Aranda

 **Importante:** Você não pode ter o AVS Agent e o Aranda Remote Control (ARC) Agent instalados simultaneamente na mesma estação de trabalho. Conflitos podem ser gerados entre os dois agentes, impedindo o uso adequado.

As condições mínimas de instalação que a estação de trabalho deve atender são:

Requisitos da estação de trabalho	
Processador virtual	CPU de 2 núcleos
CARNEIRO	Mínimo de 4 GB
Espaço em disco	Mínimo de 400 MB

As versões do sistema operacional suportadas por este agente são:

Sistema Operacional	Versão
Windows 10 LTS 2019	1809
Windows 10 Enterprise LTSC 2021	20H1
janelas 10	20H2
janelas 10	21H1
janelas 10	21H2
janelas 10	22H2
janelas 11	21H2
janelas 11	22H2
Windows Server 2016	
Windows Server 2019	1809
Servidor Windows 2022	

Portas usadas pelo Workstation Agent.

Porta	Protocolo	Descrição
443	TCP	Necessário para a conexão do Workstation Agent com o servidor de notificações, você deve ser capaz de exibir o site: https://Dominio/adm/arc/notification
8081	TCP	Necessário apenas para saída, destinado a conectar o Workstation Agent ao Turn Server no soquete do controle remoto.
	WebSockets	Eles estabelecem uma conexão bidirecional persistente entre o agente e o servidor.
3478	TCP	Necessário apenas para saída, destinado a conectar o Workstation Agent ao servidor Stun na transferência de arquivos.
15000 - 65000	UDP	Intervalo necessário apenas para a saída, destinado à conexão do Workstation Agent com o servidor Stun na transferência de arquivos.

Portas locais usadas para comunicação de processo de agente interno

Porta	Protocolo	Descrição
5050	Soquete Web	Usado pelo Aranda.ARC.Workstation.exe para receber mensagens e solicitações de outros processos
5029	GRPC	Usado pelo Aranda.AVS.TransferFile.Service.Target.exe para receber solicitações de transferência de arquivos
9087	GRPC	Usado por Aranda.AVS.VNC.Application.exe para receber solicitações de controle remoto

📌 **Anotações:**

- O agente da estação de trabalho deve ser capaz de exibir o próximo caminho do repserver para atualização automática do agente e tudo depois / : <https://Dominio/repserver/api/> e baixar arquivos desse site

Instalador ADM/Console Web

Requisitos de instalação do Windows Server local

- [Ativação de função e recurso.](#)
- [Instalando o .NET Framework versão 4.8](#)
- [Instalando o Windows Hosting Bundle Installer](#)

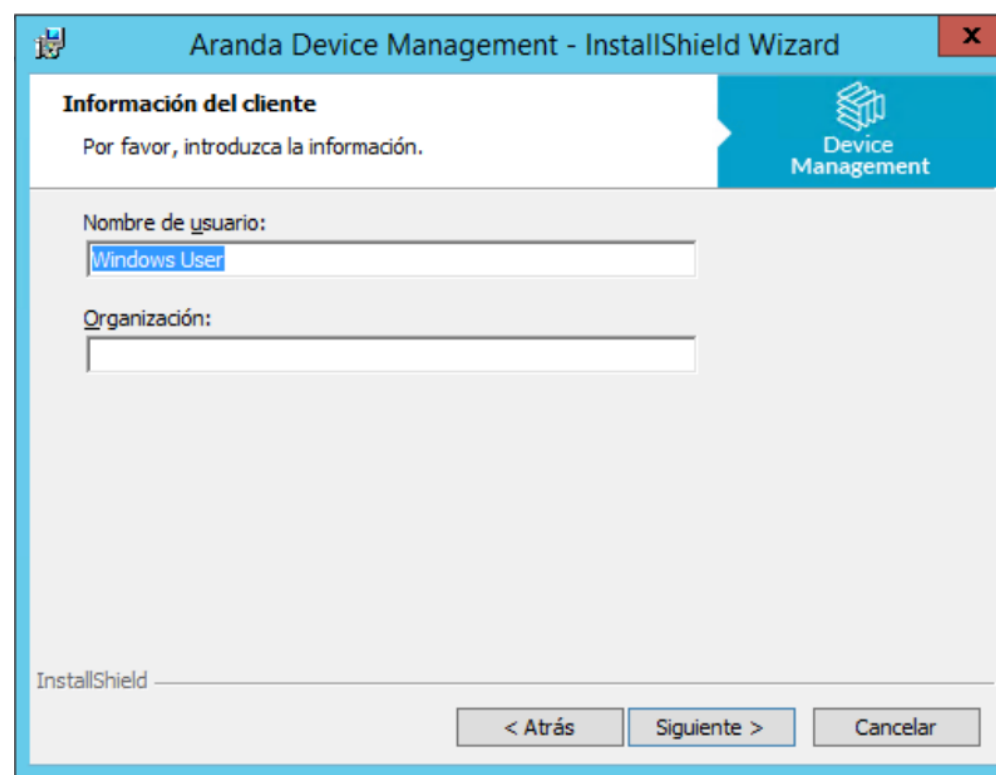
Instalador do ADM Console

O instalador `Aranda.ADM.Web.Installer` a partir do console da Web do ADM, instala os sites do console, o Repserver e os sites de Controle Remoto (Notificações e Gravações); além disso, ele cria os serviços Crunchers, License, Scheduler, Worker, Turn Stun WebRTC e Turn Server que são usados no aplicativo. Aqui está o passo a passo da instalação.

1. Clicar no instalador iniciará o assistente de instalação. Clique Seguinte.



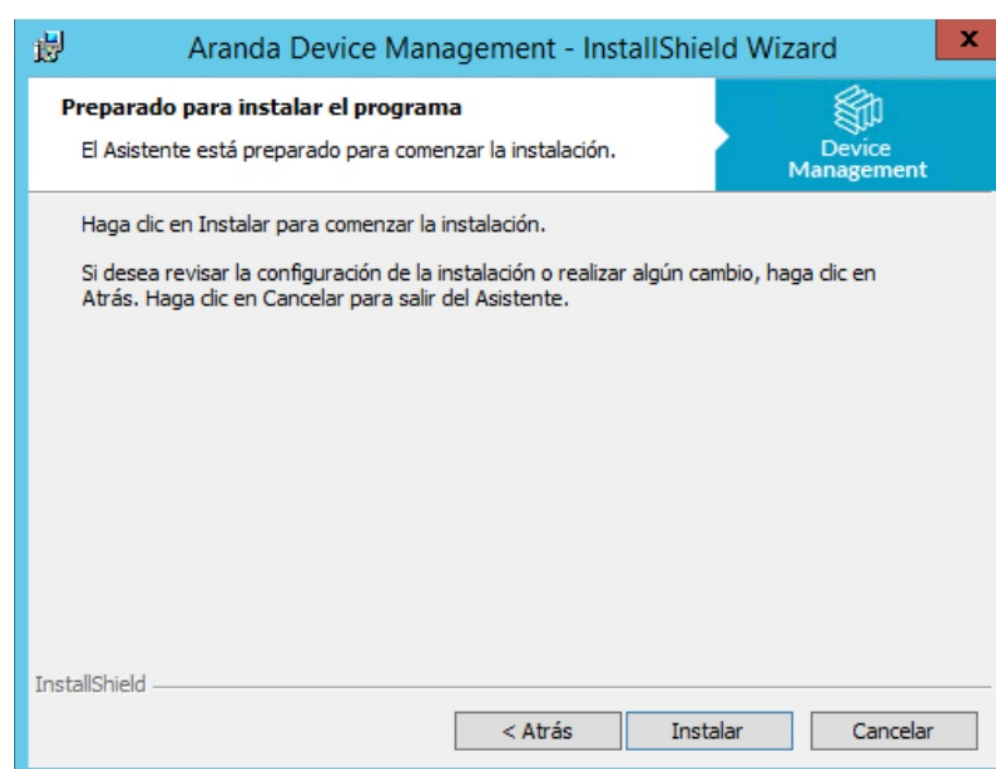
2. Insira as informações do cliente e clique em Seguinte.



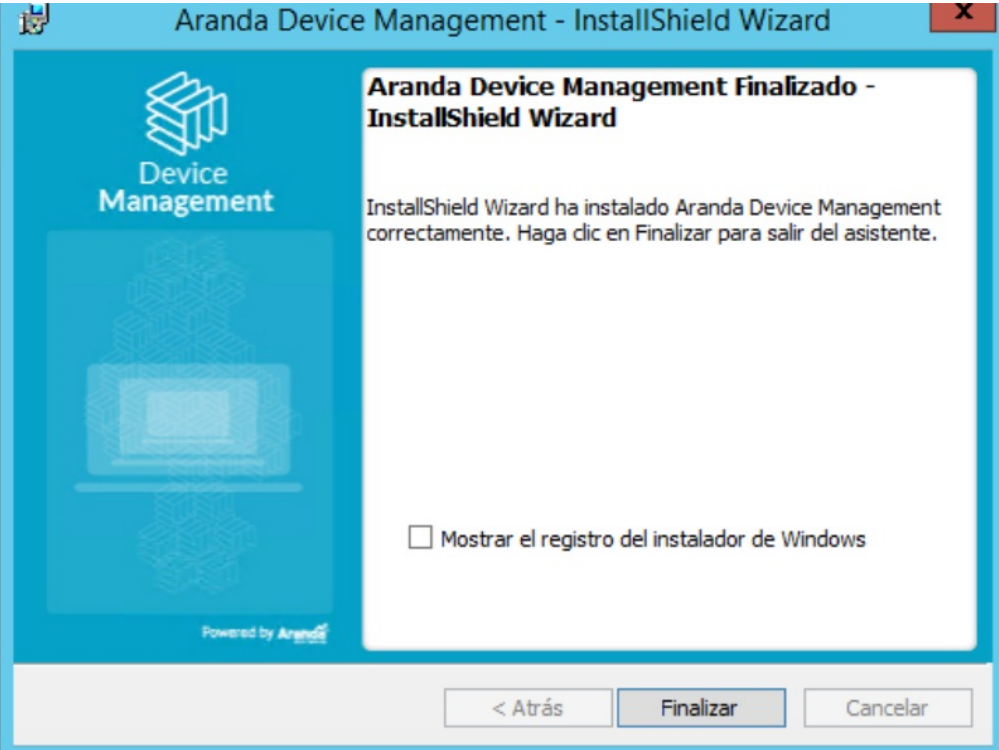
3. Selecione o tipo de instalação completo e clique em Seguinte.



4. Clique Instalar.

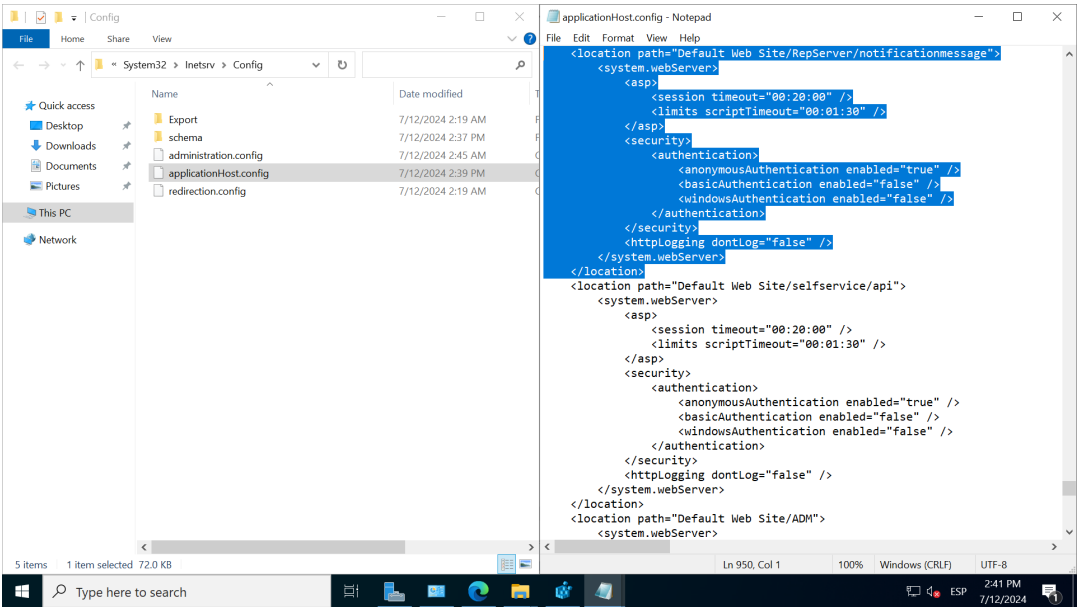


5. Quando o processo de instalação estiver concluído, clique em Fim.



Nota:

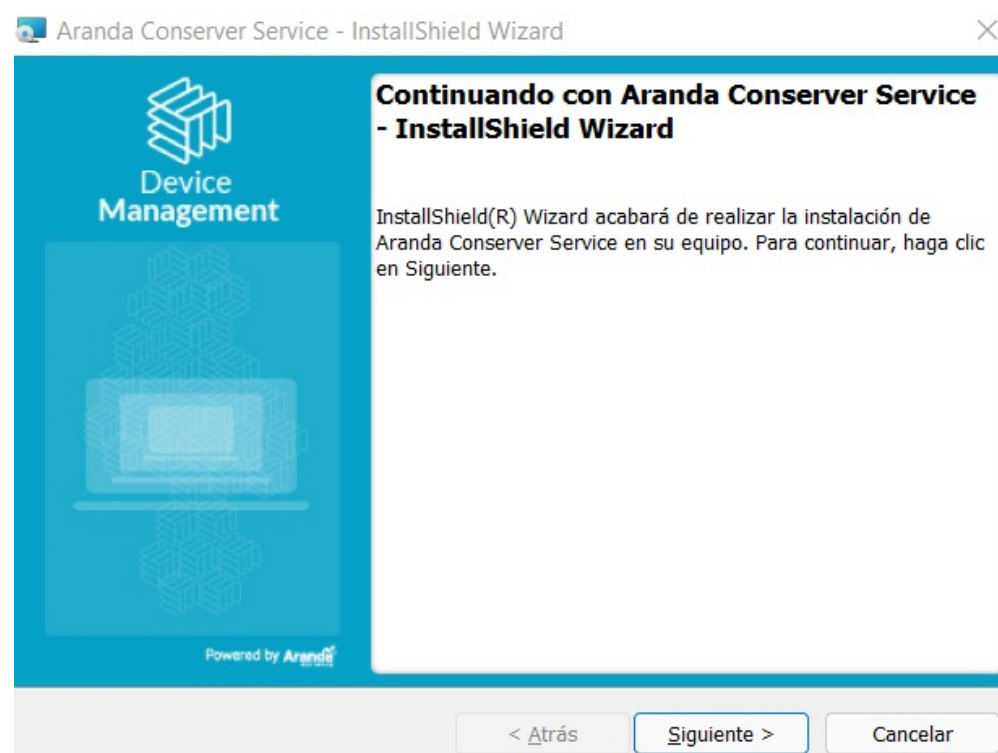
- Se o site da ADM não fizer o upload corretamente, verifique se os requisitos foram executados de acordo com a ordem definida; Execute os instaladores novamente reparando a instalação
- Se o erro persistir, localize o arquivo WinDir%\System32\Inetsrv\Config\applicationHost.config e remova a marca de localização que corresponde ao site "Repserver/notificationmessage" e reinicie o IIS



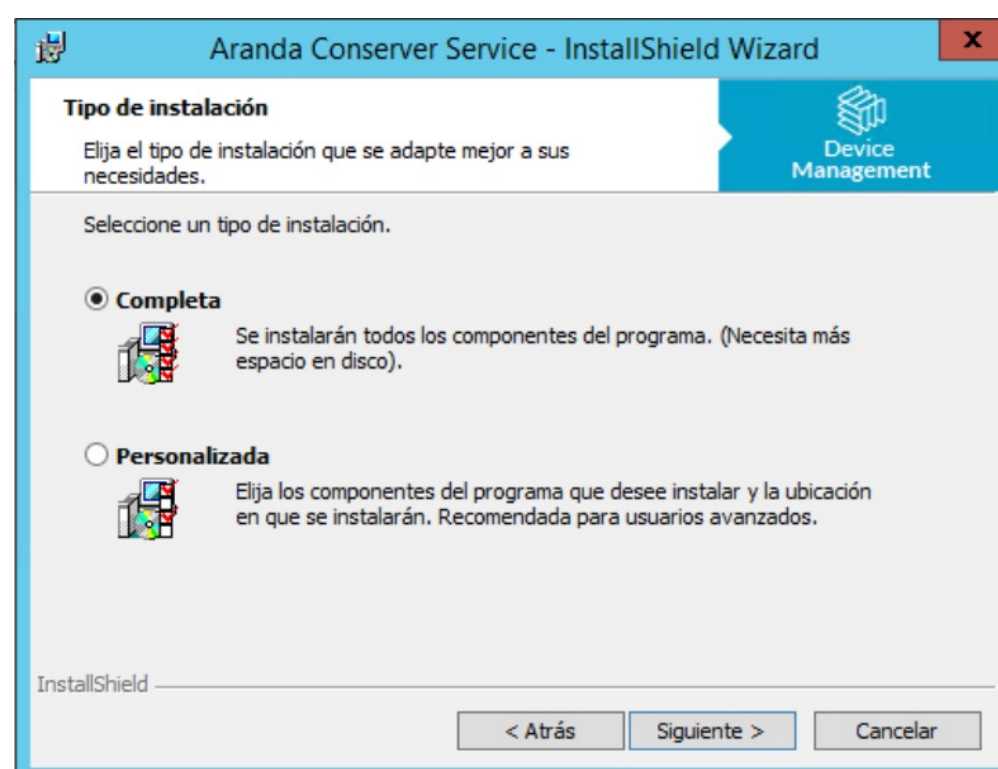
Instalador/servidor

O segundo instalador é Aranda.Conserver.Installer. Um serviço deve ser instalado para cada segmento de rede.

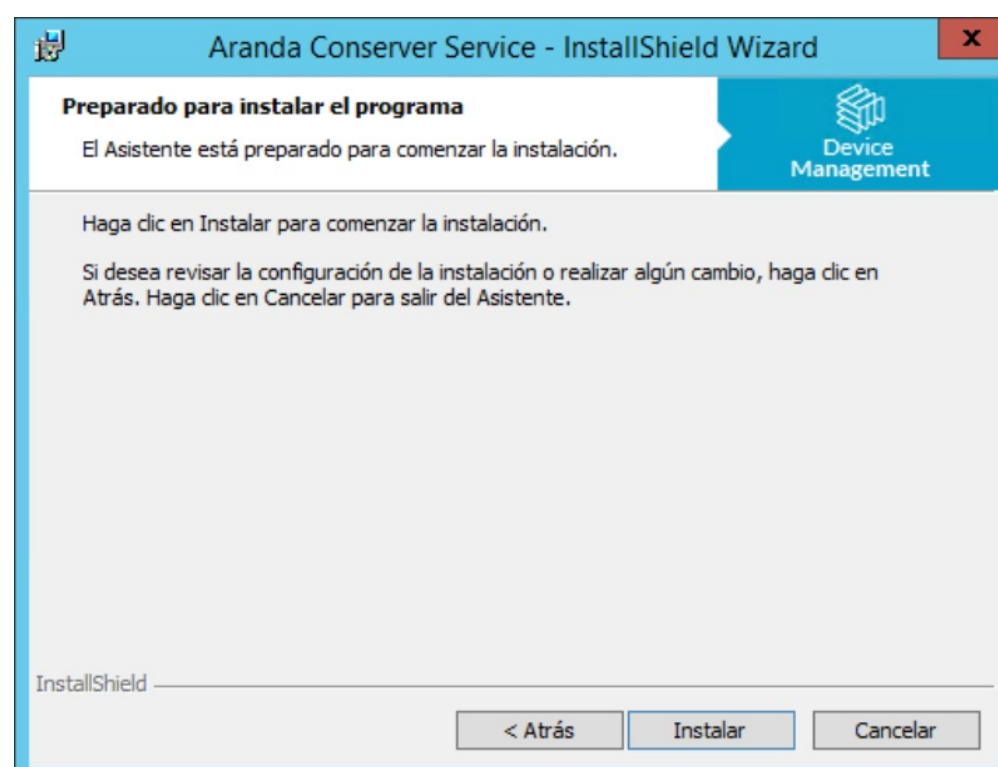
1. Clicar no instalador iniciará o assistente de instalação.



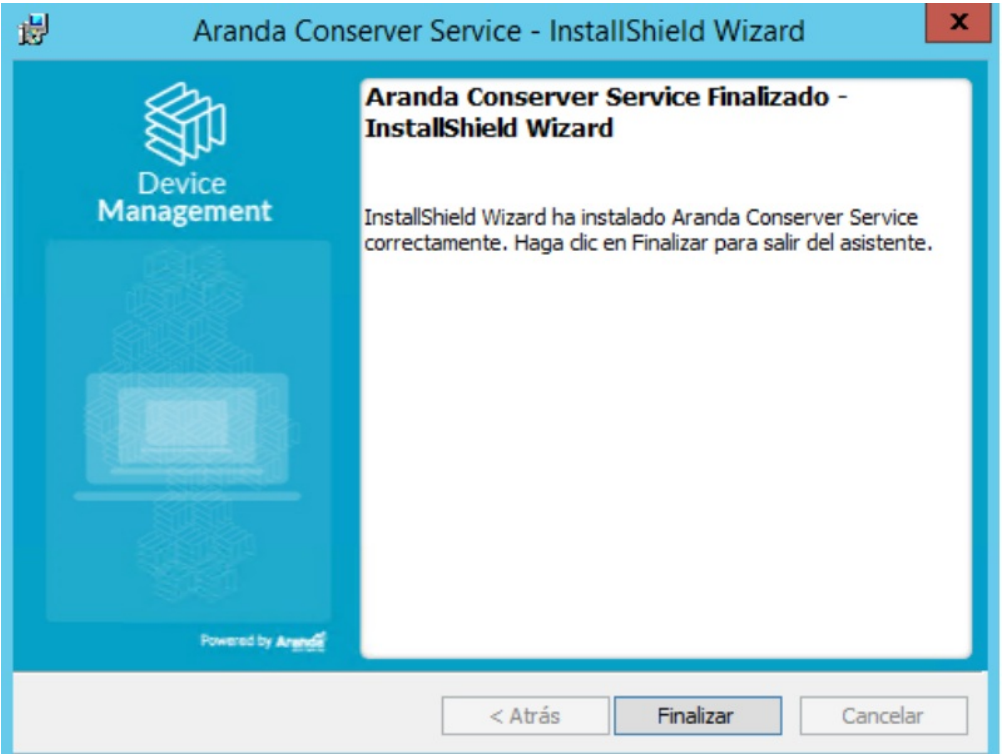
2. Seleccione o tipo de instalação completo e clique em Siguiente.



3. Clique Instalar.



4. Quando o processo de instalação estiver concluído, clique em Fim.



—

- 🔗 Links Relacionados:
- [Configuração do Conservador](#)
 - [Configuração do console do conservador](#)

Configuração do Conservador

Configuração do Conservador

« [Instalador Conservador](#)

1. Quando você instala um Servidor, todos os arquivos são salvos no caminhoC:\Arquivos de Programas (x86)\Aranda\Conserver, Configure o Aranda.Conserver.Windows.Service.exe.config da seguinte maneira para se comunicar com o Repserver:

Configurações do AppSettings		
adicionar		
chave="dataConfiguration:defaultDatabase"	Ele é usado para definir o banco de dados padrão a ser usado no aplicativo.	
value="local" /		
add key="Serilog:MinimumLevel"	Usado para definir o nível mínimo de log de eventos para a biblioteca de logs do Serilog.	
value="Depurar"		
add key="Serilog:WriteTo:0:Name"	Usado para especificar o primeiro destino de log a ser usado para Serilog. O valor "Arquivo" indica que os eventos de log serão gravados em um arquivo.	
value="Arquivo"		
add key="Serilog:WriteTo:0:Args:path"	Ele é usado para especificar o caminho e o nome do arquivo onde os eventos de log serão gravados.	
value="Logs\log.txt"		
add key="Serilog:WriteTo:0:Args:shared"	Ele é usado para especificar se o arquivo de log deve ser compartilhado por vários processos ou não.	
value="true"		
add		
key="Serilog:WriteTo:0:Args:rollingInterval"	Usado para especificar o intervalo de tempo no qual novos arquivos de log são criados.	
value="Dia"		
add key="Logging:LogLevel:Default"	Ele é usado para definir o nível de log padrão para a biblioteca de log da Microsoft.	
value="Informações"		
adicionar chave="serverAddress" value=""	Endereço onde o Repserver está localizado	
Se você usar Proxy, a tag enableProxy será ativada com um		

adicionar chave="enableProxy" valor="false" Configurações do AppSettings	Se você usar Proxy, a tag enableProxy será ativada com um valor de "true"
adicionar chave="proxyAddress" valor=""	Endereço de proxy
adicionar chave="proxyUser" valor=""	Usuário proxy
adicionar chave="proxyPassword" valor=""	Senha do proxy
add key="logLevel" value="Informações"	Log de nível de verbosidade do conservador; "Informação", "Depuração", "Detalhado", "Detalhado". Por padrão, é parametrizado em "Informações"
adicionar chave="privateIp" valor=""	Identificador na rede interna do Conservador, deve ser o ip
adicionar chave="publicIp" valor=""	Conservar identificador de rede do lado de fora, o ip deve ir. (Caso não seja necessário, o mesmo endereço privado é colocado)
adicionar chave = "mqttServerPort" valor = "1884"	A porta de comunicação MQTT, por padrão, "1884" é parametrizada
adicionar chave="mqttIp" valor=""	Mqtt na rede interna, o IP deve ir
adicionar chave="publicServerPort" valor="80"	A porta de comunicação de rede pública do conservador, por padrão "80", é parametrizada.
adicionar chave="privateServerPort" valor="80"	Preservar a porta de comunicação da rede privada, por padrão "80" é parametrizada.
adicionar chave="p2pPort" valor="9501"	Porta para conexões p2p, por padrão o "9501" é parametrizado
adicionar chave="maxDistributionSleepMsPerThread" valor="8"	-
adicionar chave="maxDistributionThreads" valor="4"	Essas duas últimas tags são usadas para o funcionamento interno do sistema, elas devem ser modificadas

```
<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 o serviço Aranda Conserver V9, para permitir a comunicação com o Repserver.

Aranda Conserver V9

En ejecu...

Automático

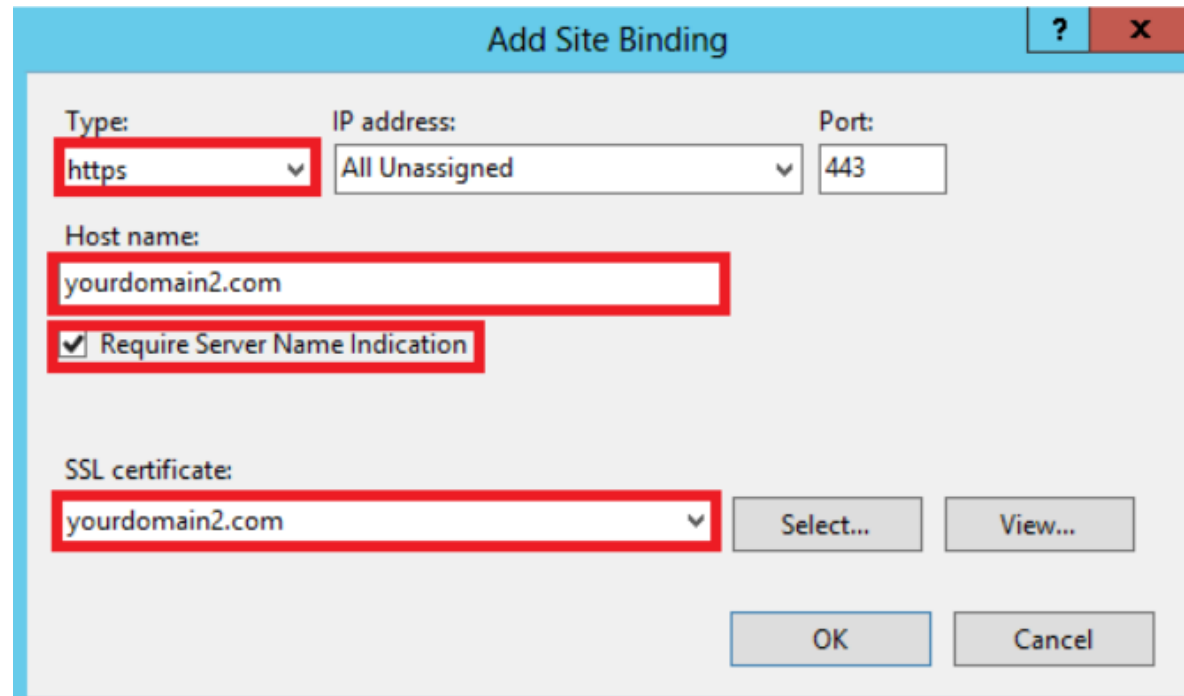
Sistema local

Configurando o conservador para receber solicitações por https

Para configurar o servidor para receber solicitações https, https deve ser habilitado no iis com o certificado adequado.

Importante proteger quaisquer nomes de host adicionais usando SNI.

Endereço IP: selecione "Todos não atribuídos".



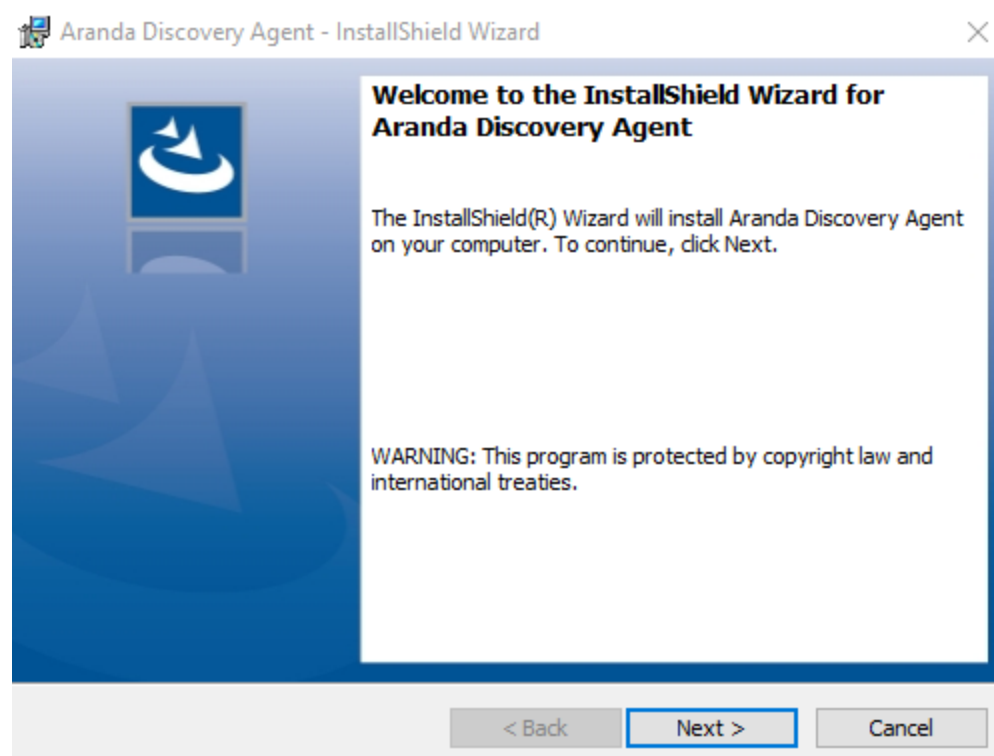
O valor do rótulo "enableSecurity" deve ser igual a "true"

```
<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>
```

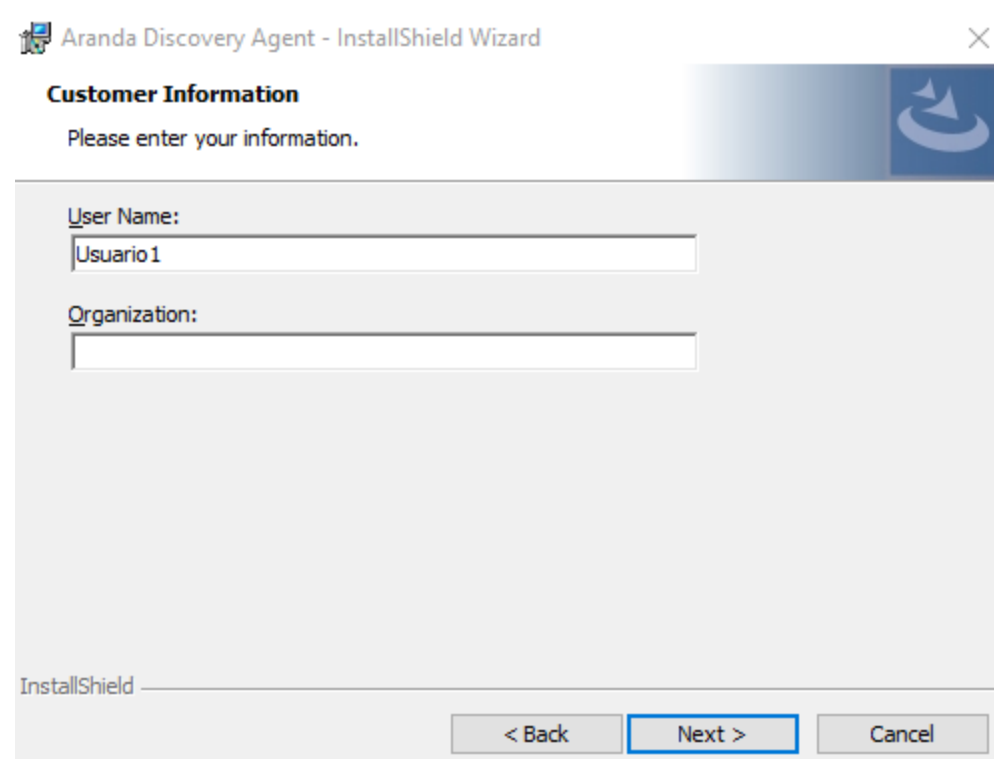
[« Instalador Conservador](#)

Instalador/Agente de Descoberta

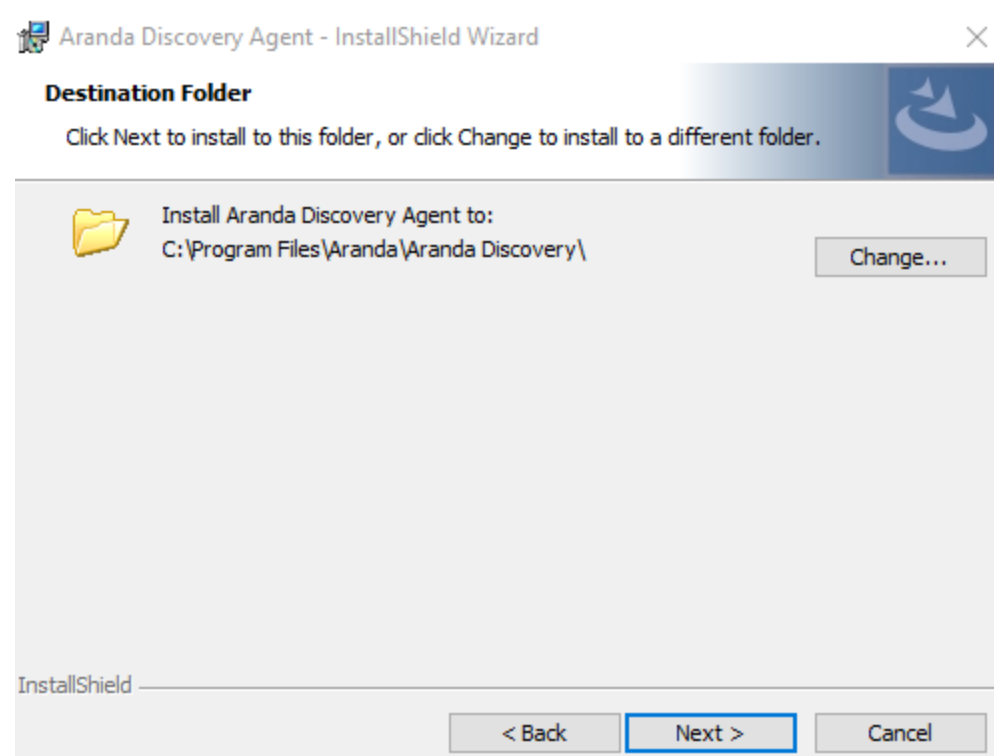
1. Execute o instalador Aranda.Discovery.Agent.x.x.x.exe



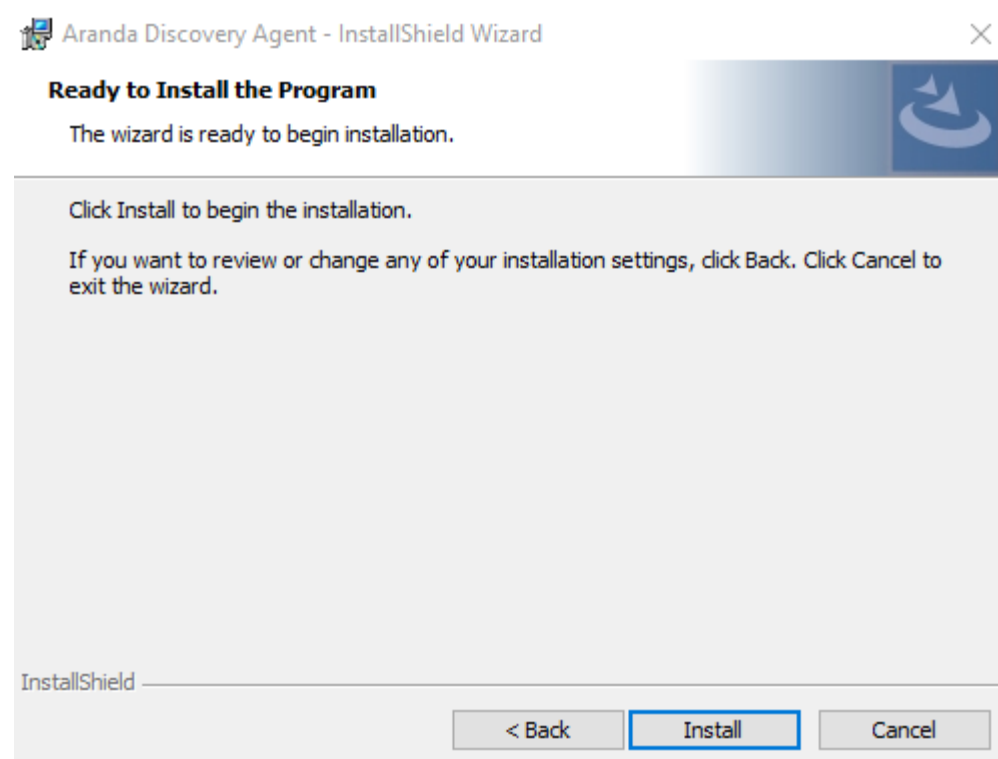
2. Na janela Informações do Cliente, insira o nome de usuário, a organização e clique em **Seguinte**. Esses campos podem ser deixados em branco.



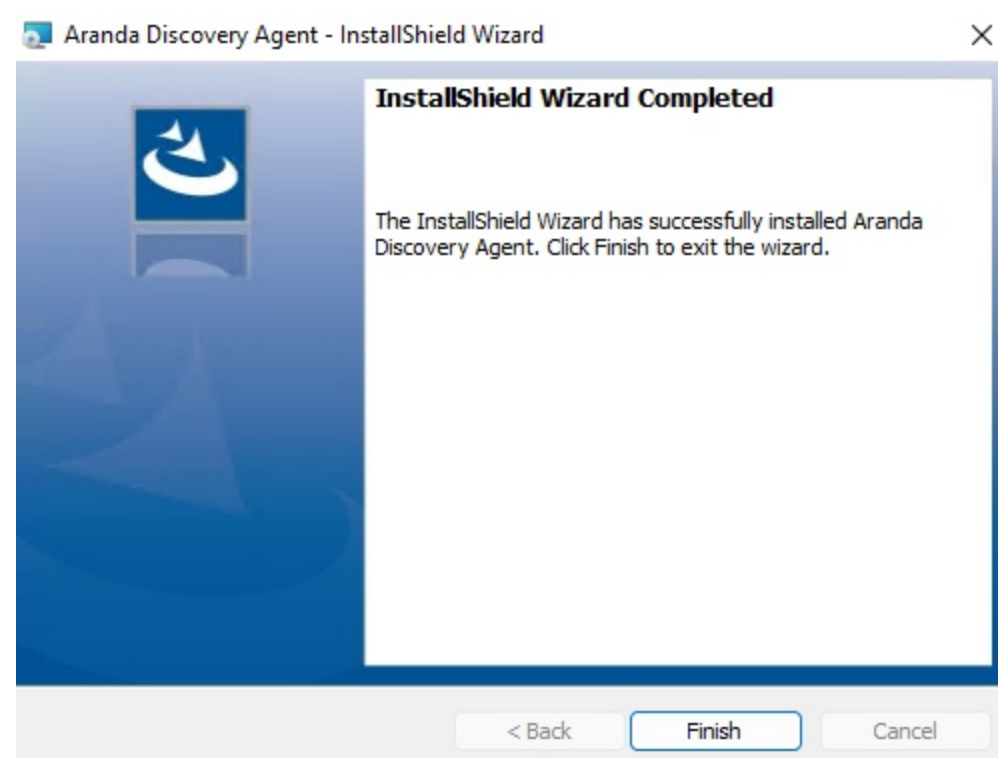
3. Na janela Pasta de destino, você pode alterar o caminho de instalação do serviço ou deixá-lo por padrão onde a instalação sugerir e clicar em **Seguinte**.



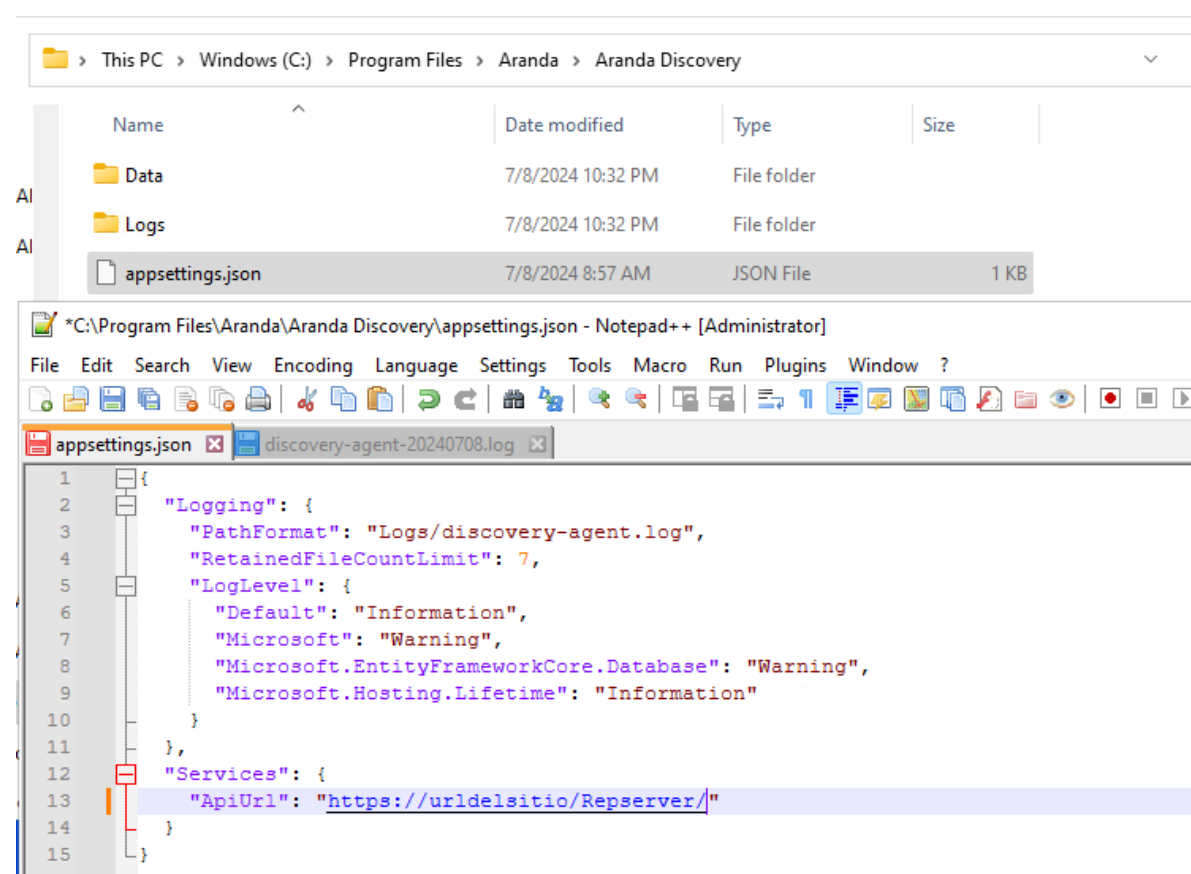
4. Clique **Instalar**; Você deve ter permissões como administrador da máquina.



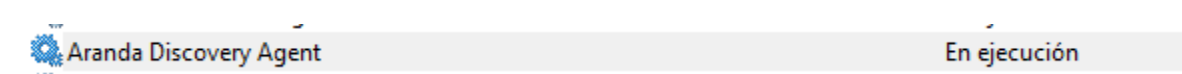
5. Quando o processo de instalação estiver concluído, clique no botão Fim.



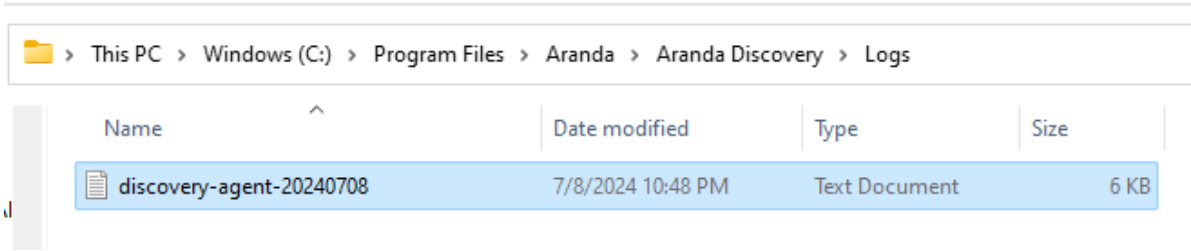
6. Para configurar o agente de descoberta, abra o `appsettings.json` na pasta onde o serviço está instalado e no `Serviços em ApiUrl`, insira a URL do Repserver do site.



aplicativo.

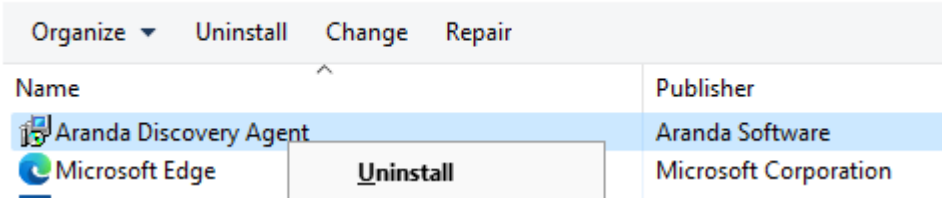


8. Os arquivos de Tora será armazenado no seguinte caminho: C:\Arquivos de Programas\Aranda\Aranda Discovery\Logs

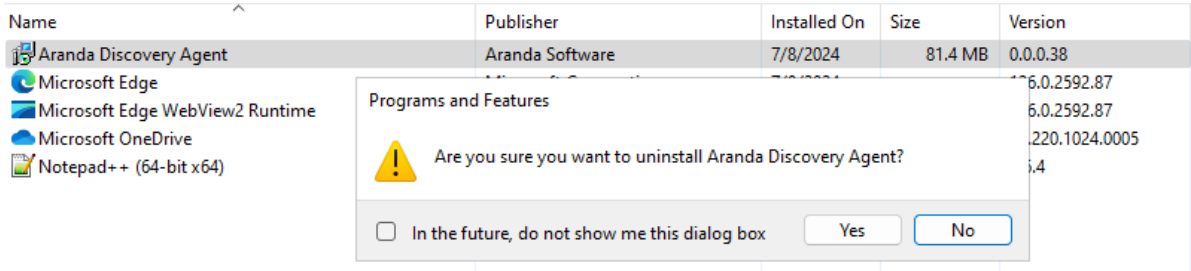


Desinstalando o Discovery Agent

1. Entre no painel de controle e clique com o botão direito do mouse no aplicativo Agente de Descoberta de ArandaSelecionar desinstalar.



2. Para a pergunta “Esta seguro que quiere desinstalar Aranda Discovery Agent?”, clique no botão SI na mensagem.



3. Verifique o serviço novamente e a pasta onde o serviço foi instalado, o registro não deve mais aparecer.

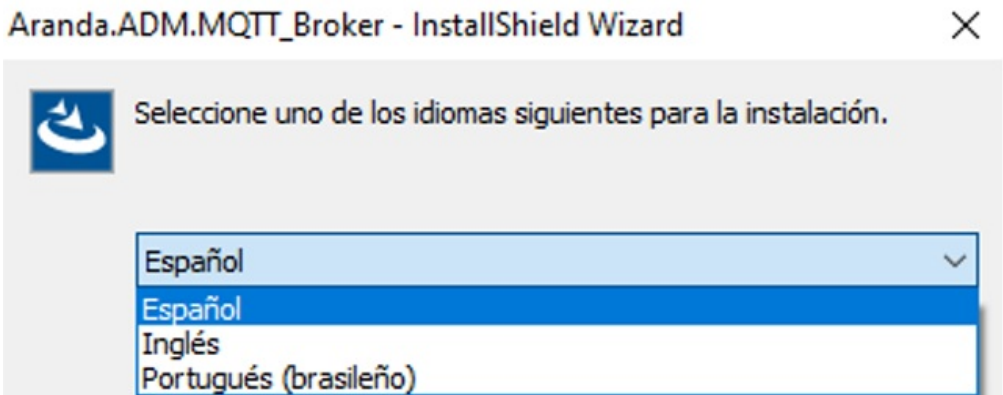
Atualização automática do agente de descoberta

1. O agente de descoberta será atualizado automaticamente dentro de um dia após a atualização do site do ADM.

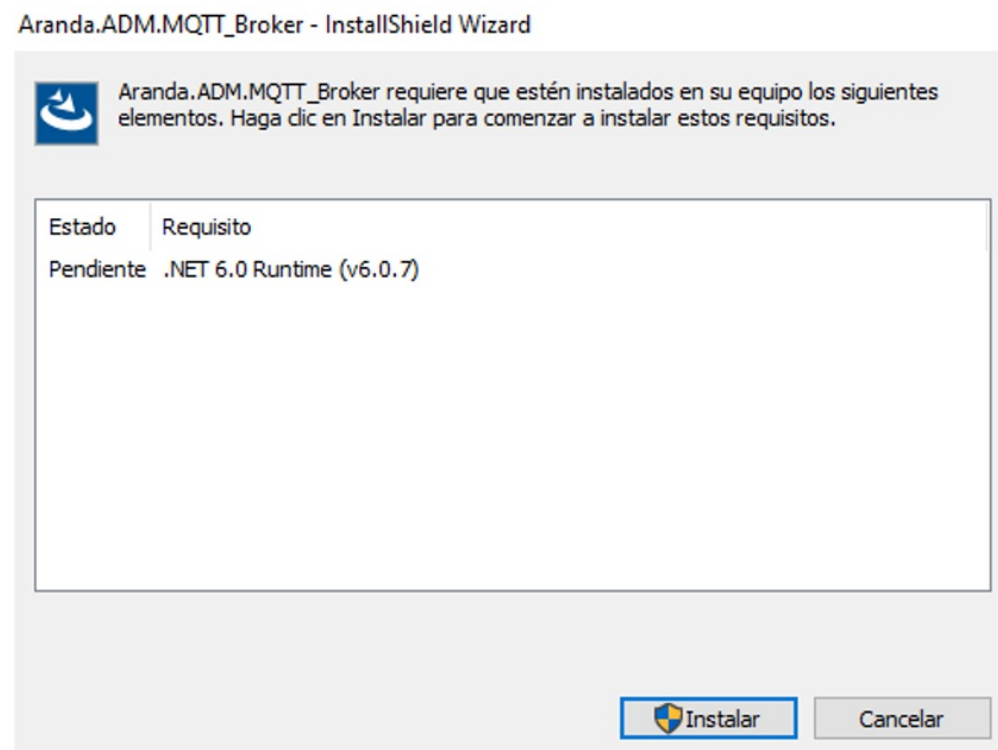
Instalador/lavador do MQTT Broker

📌 **Nota:** Um número máximo de 10.000 conexões (dispositivos) por servidor do agente MQTT é sugerido.

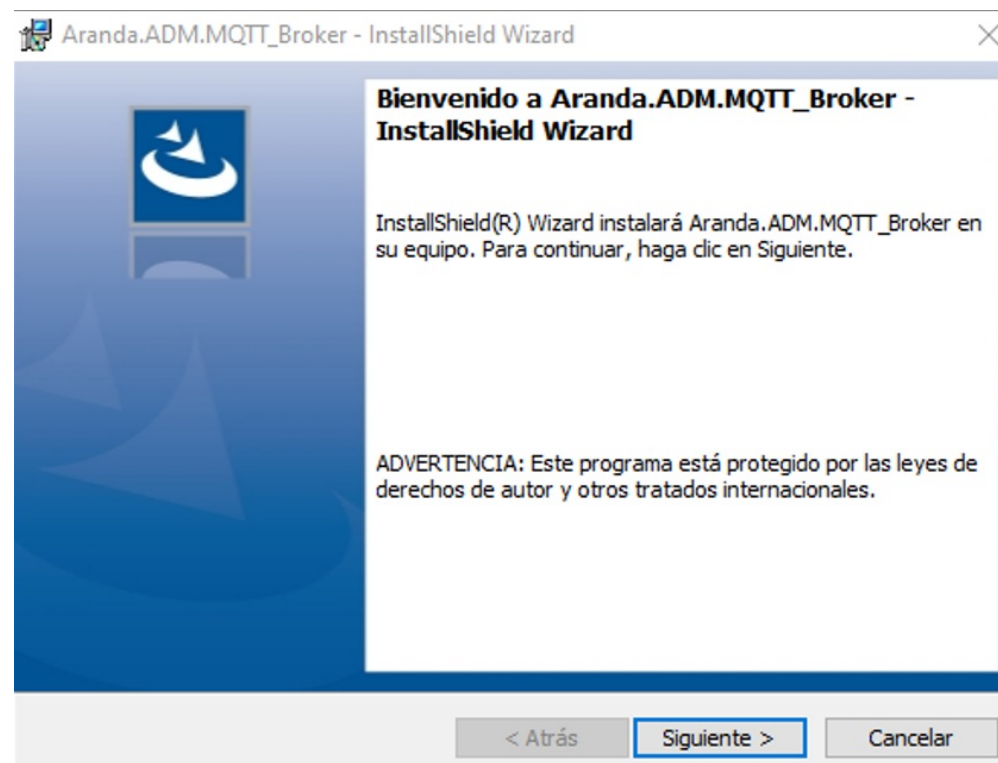
- 1. Execute o instalador Aranda.ADM.MQTT.Broker.exe
- 2. Defina o idioma para o processo de instalação.



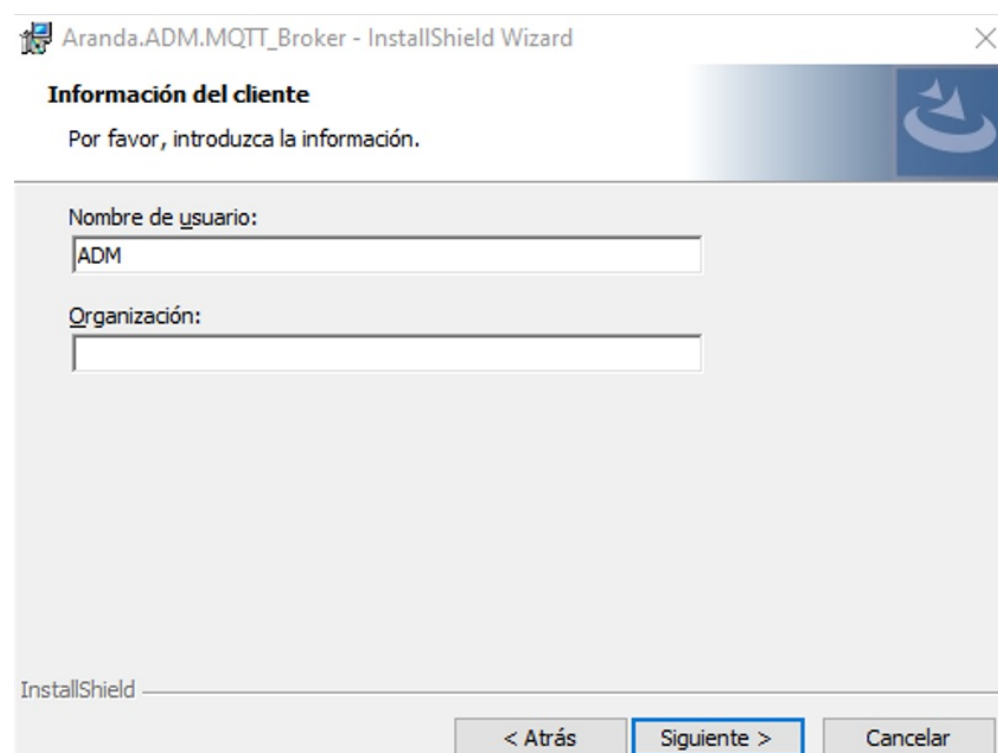
3. O instalador valida os pré-requisitos que devem ser atendidos para configurar o agente Aranda. Se isso não for atendido, o sistema instalará as informações necessárias.



4. Ao terminar de instalar os requisitos, você poderá ver a tela de boas-vindas. Confirme a instalação clicando no botão Seguinte.

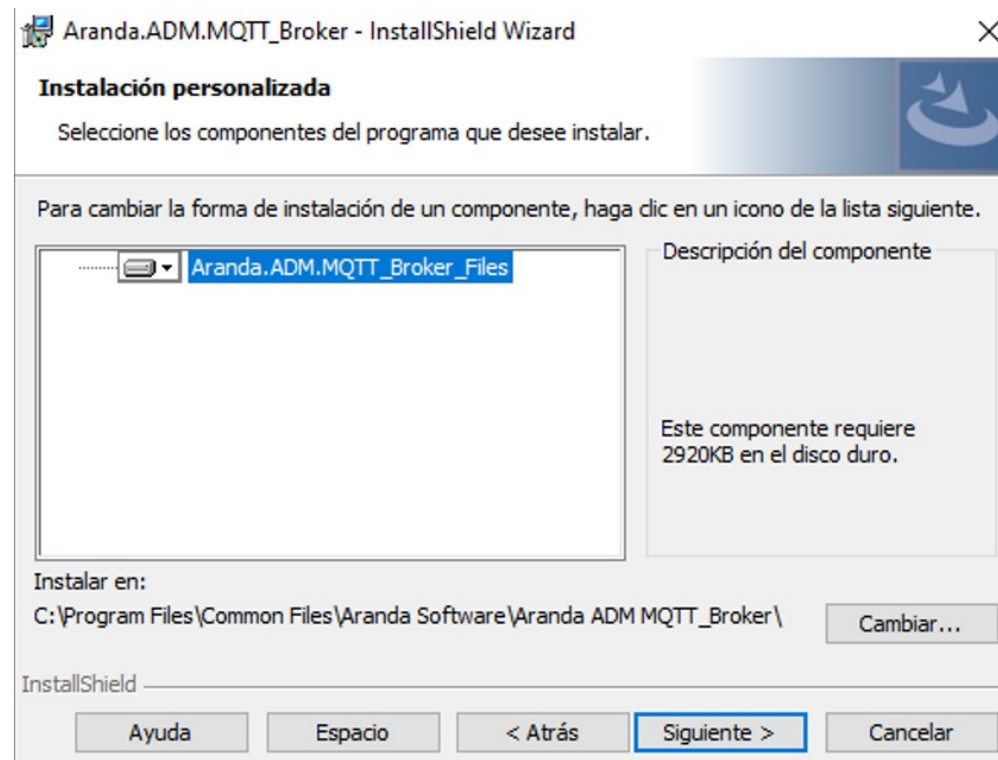
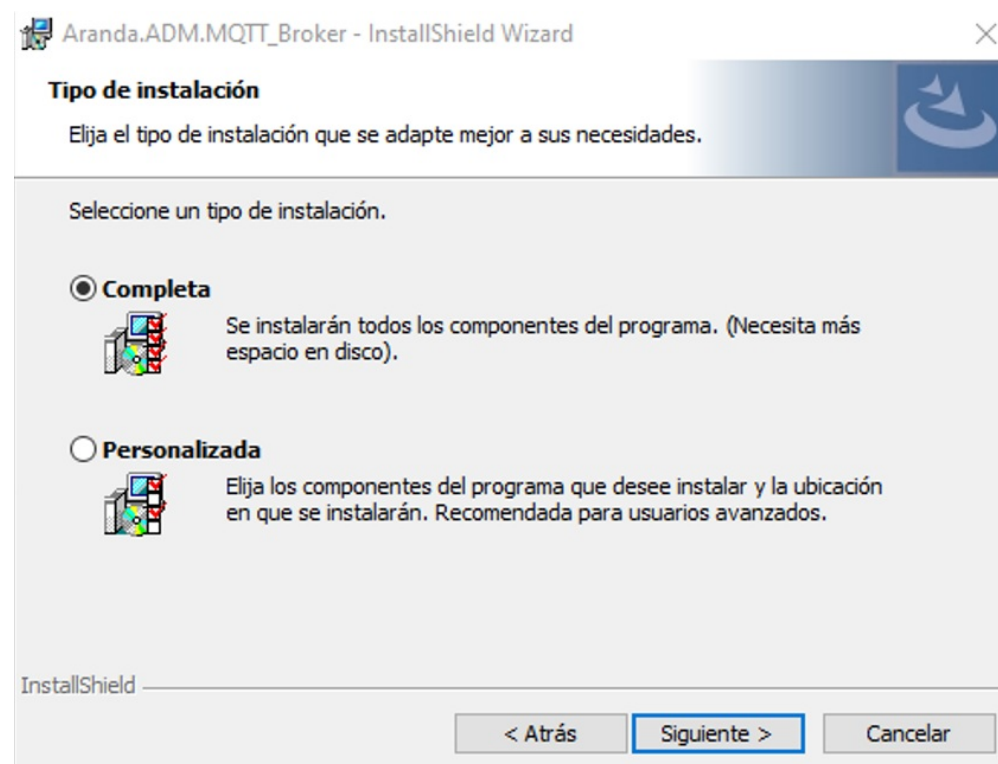


5. Na janela Informações do Cliente, insira o nome de usuário, a organização e clique em Seguinte. Esses campos podem ser deixados em branco.

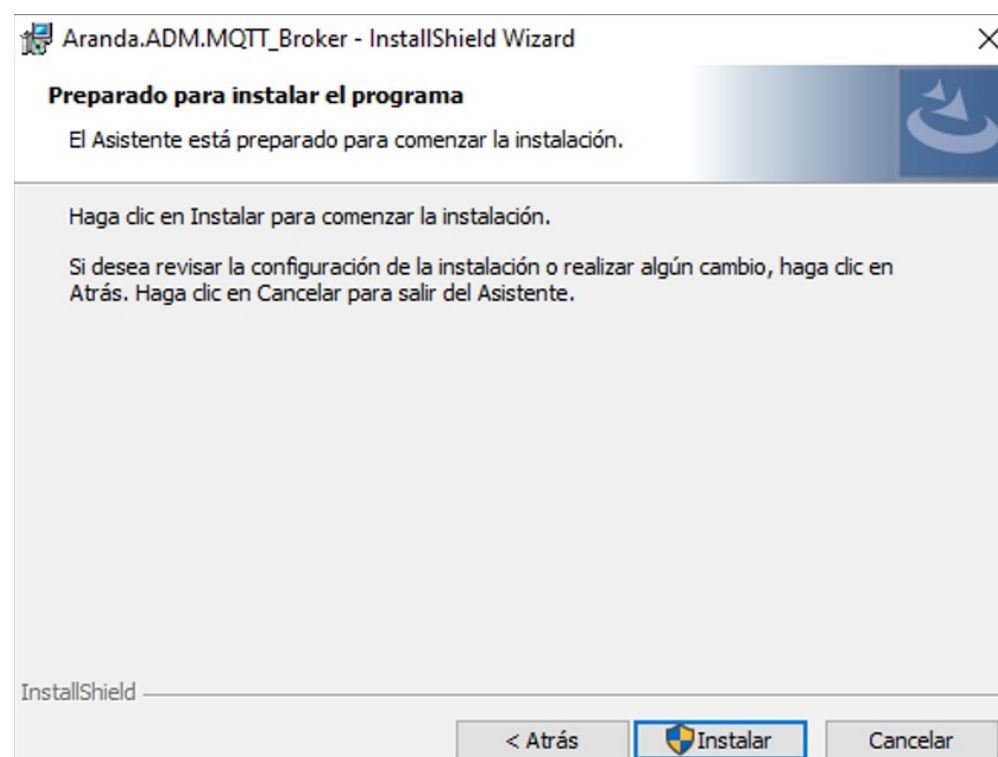


6. Defina o tipo de instalação, as opções são:

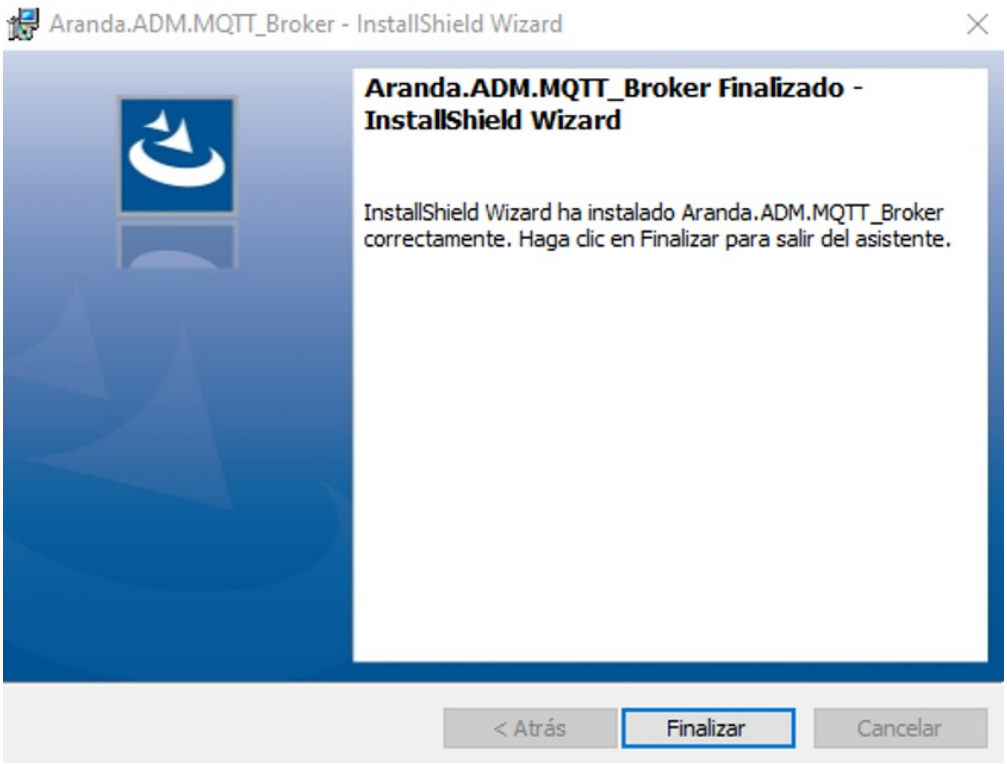
- **Completar:** Todos os sites e serviços serão instalados nas rotas padrão.
- **Costume:** Você pode alterar o caminho de instalação de sites e serviços.



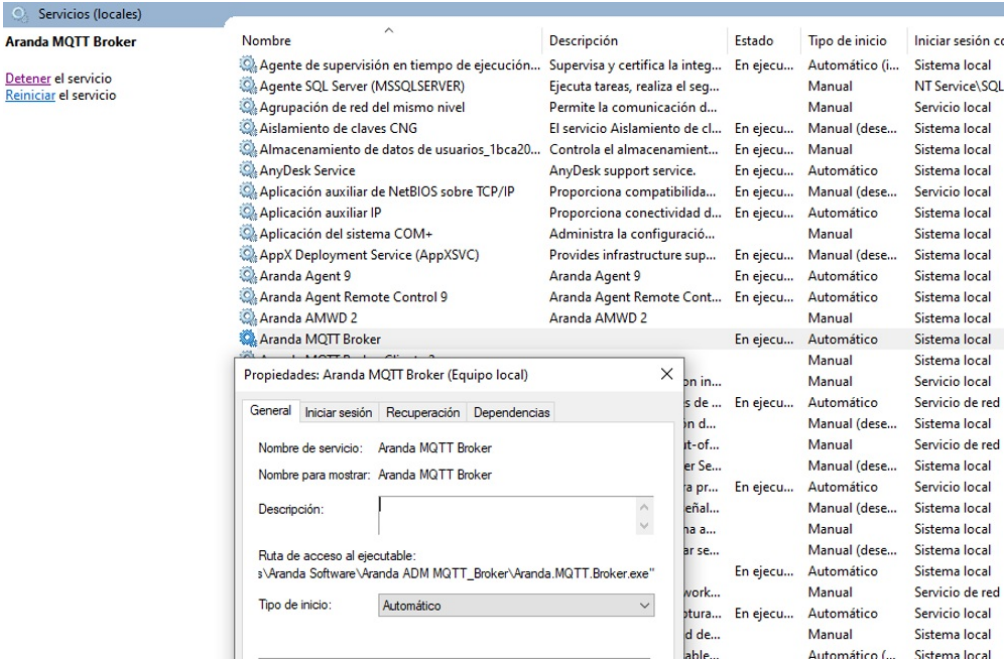
7. Depois que a instalação completa ou personalizada for escolhida, clique em Instalar, você deve ter permissões como administrador da máquina.



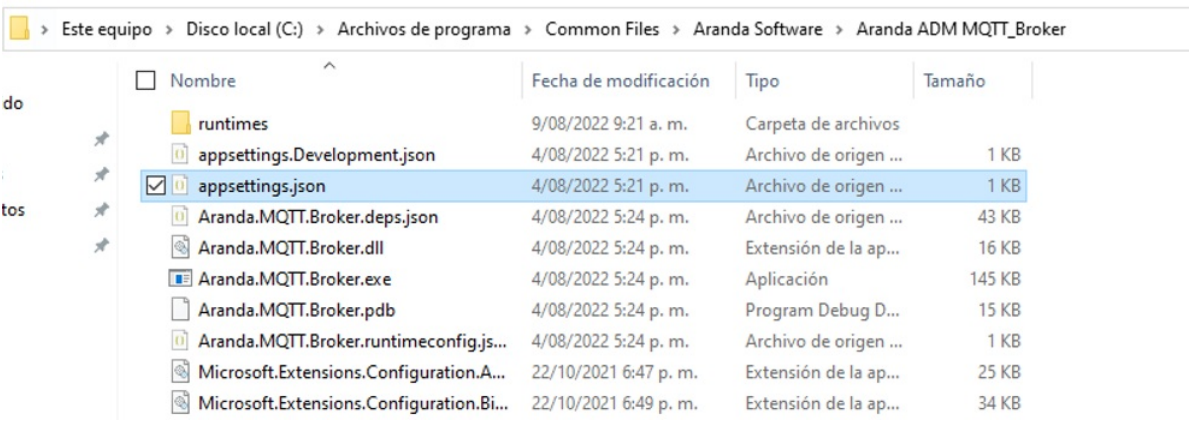
8. Quando o processo de instalação estiver concluído, clique no botão Fim.



9. Quando o processo de instalação estiver concluído, vá para os serviços e verifique se o serviço: Aranda MQTT Broker está instalado e em execução.



10. Para configurar a porta que você deseja expor, abra o `appsettings.json` na pasta em que o serviço está instalado e faça o seguinte:

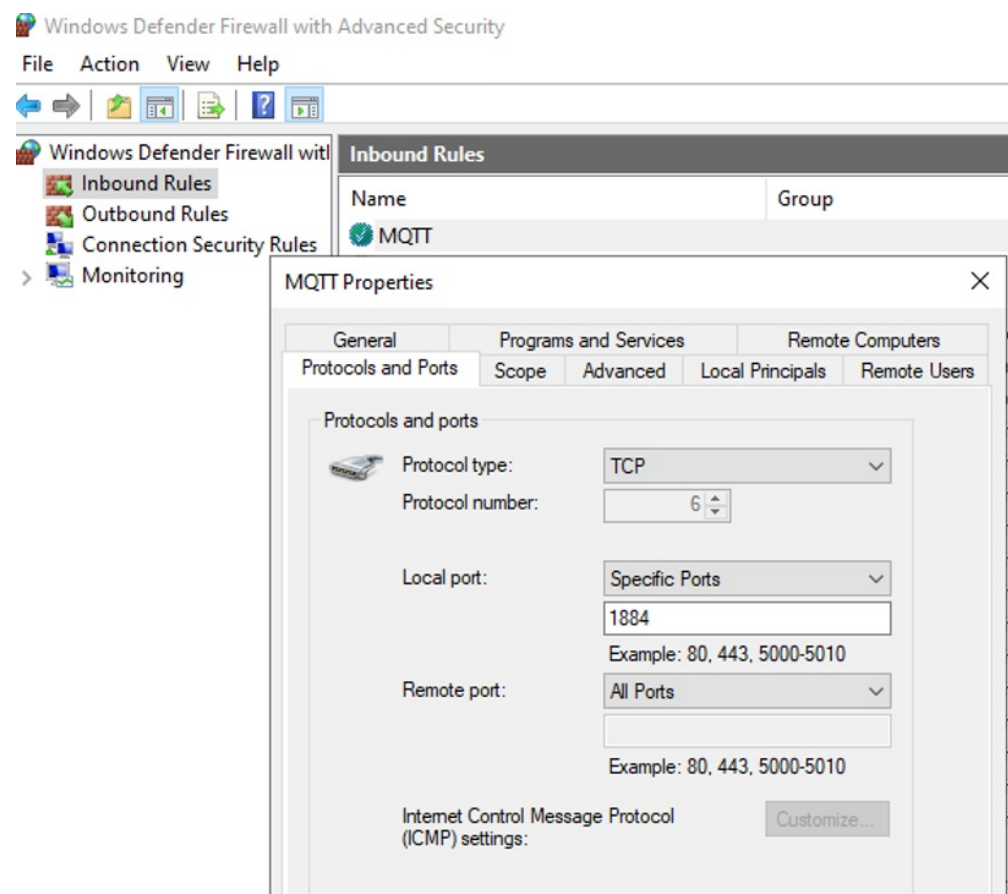


11. Modifique a seção `Mqtt:Porta` para alterar a porta e reiniciar o serviço para aplicar as alterações.

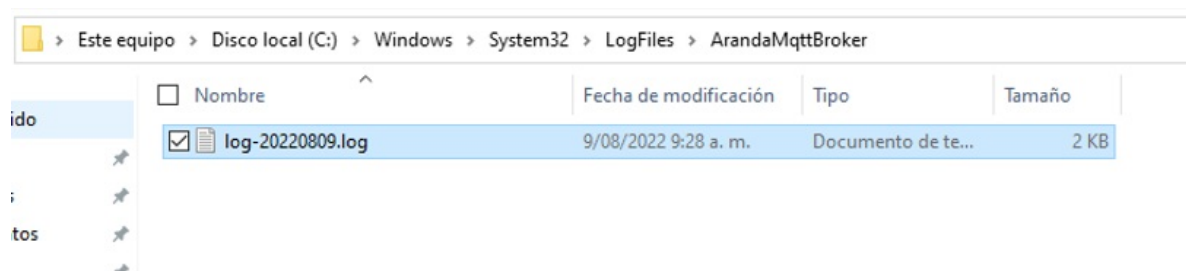

```
appsettings.json X
C: > Program Files > Common Files > Aranda Software > Aranda ADM MQTT_Broker > {} appsettings.json > {} Mqtt

Search (Ctrl+Shift+F)
2      "Logging": {
3        "LogLevel": {
4          "Default": "Information",
5          "Microsoft": "Information",
6          "Microsoft.Hosting.Lifetime": "Information"
7        },
8        "PathFormat": "LogFiles/ArandaMqttBroker/log-{Date}.log"
9      },
10     "Mqtt": {
11       "Port": 1884
12     }
13   }
14 }
```

12. No Windows Defender Firewall, selecione a opção Regras de entrada e, nas propriedades MQTT, valide se a porta 1884/1883 está aberta no computador.

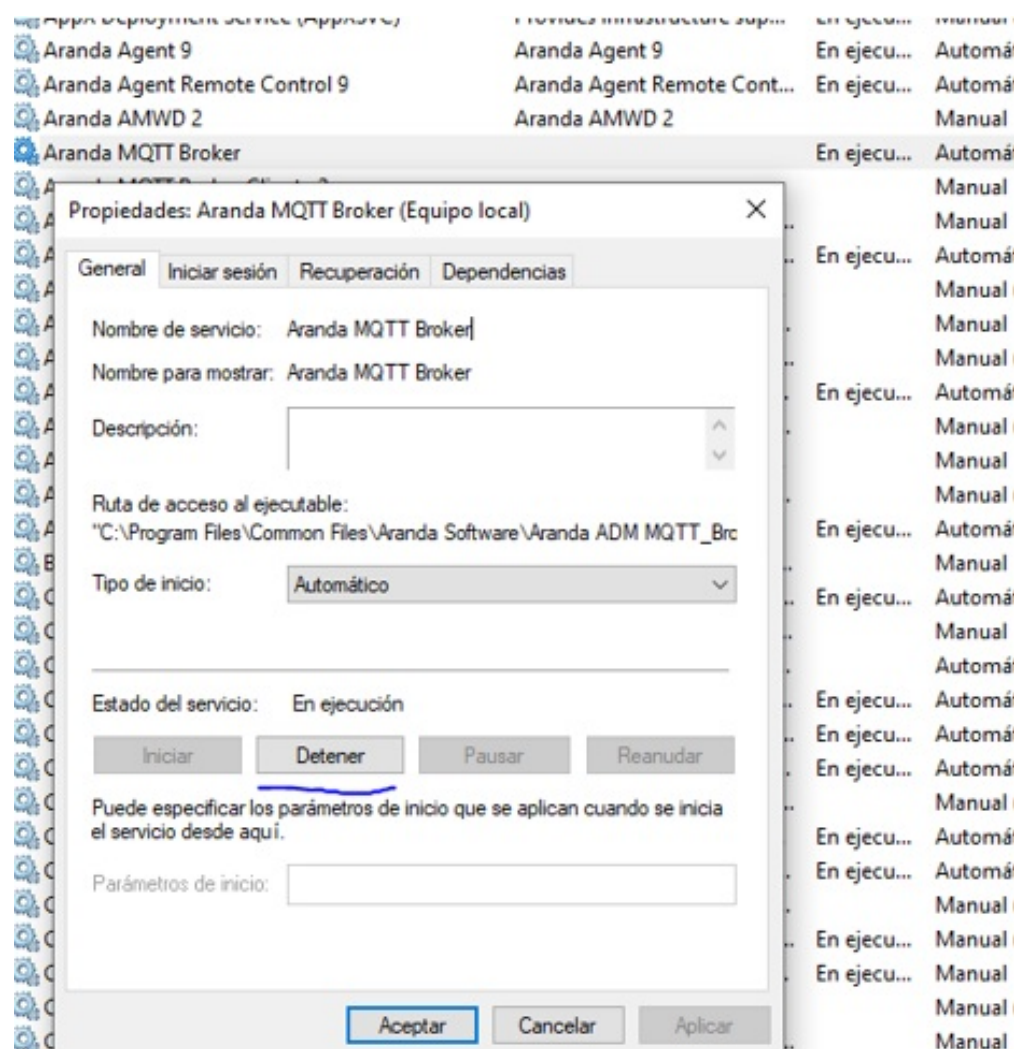


13.Os arquivos de Tora será armazenado no seguinte caminho: C:/Windows/System32/LogFiles/ArandaMqttBroker

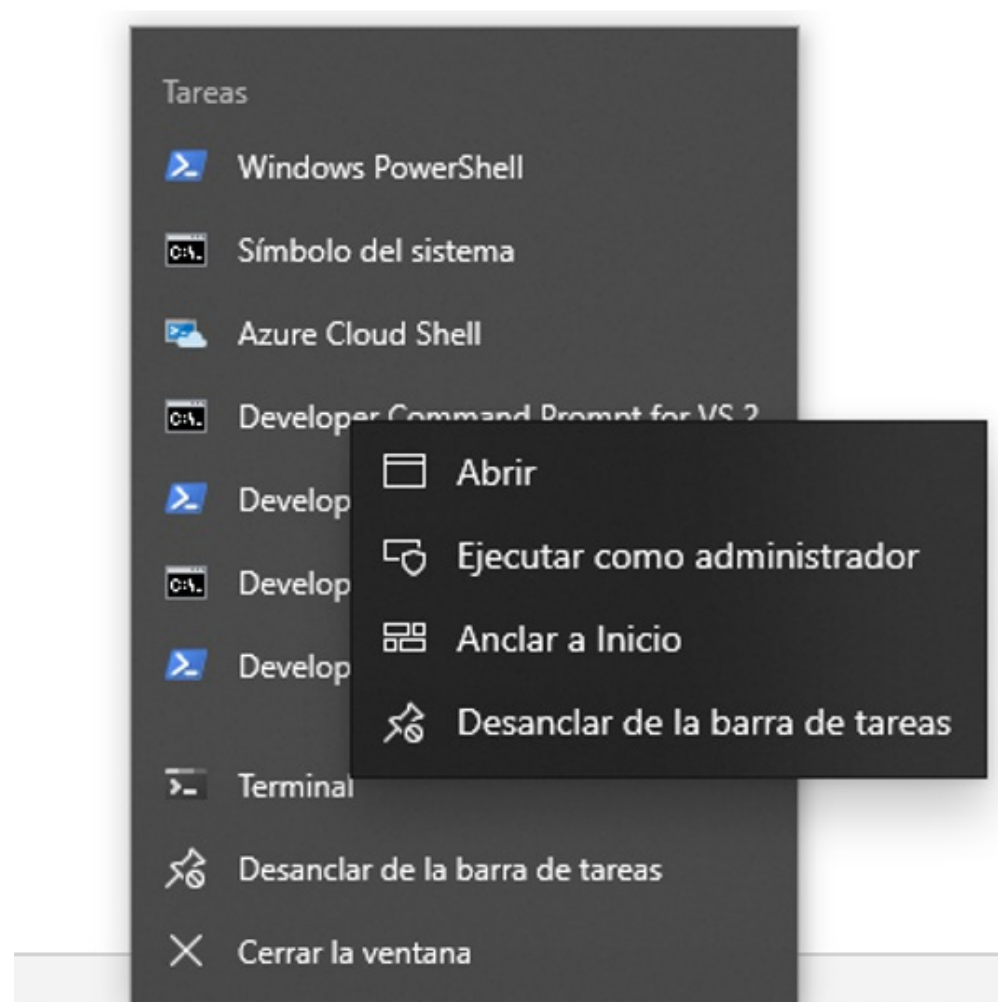


Desinstalando o MQTT Broker

1. Abra o arquivo Aranda MQTT Broker, a janela Propriedades está ativada e, no Geral, em Status do serviço, selecione o ícone Deter e clique no ícone Aplicar.



2. Inicie um terminal no modo de administrador e execute as seguintes informações:



3. Execute o comando:

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

4. Depois que o comando é executado, o resultado é o seguinte:

```
[SC] DeleteService CORRECTO
```

5. Verifique os serviços novamente e ele não deve ser instalado.

✉ **Nota:** Um número máximo de 10.000 conexões(dispositivos) por servidor do agente MQTT é sugerido.

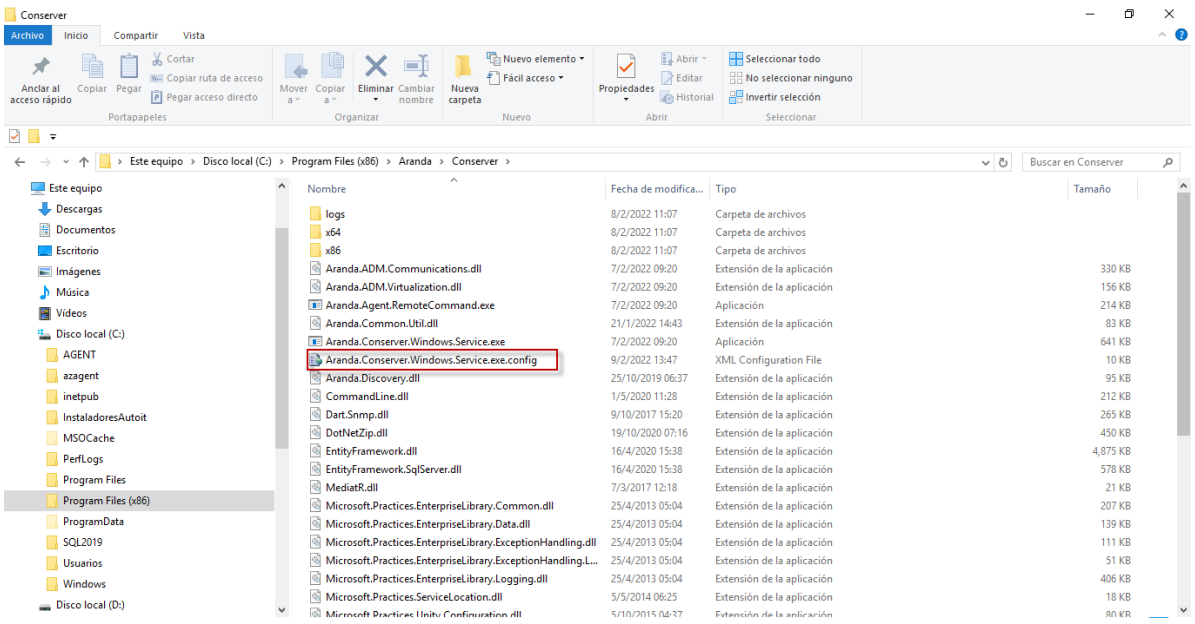
-  Links Relacionados:
- [Configuração do agente](#)

Configuração do agente

Configuração do agente

Instalador do Aranda MQTT Broker

1. Para configurar a comunicação entre o conservador e o Broker, você deve configurar o arquivo “Aranda.Conserver.Windows.Service.exe.config” que está na pasta “%Program Files (x86)%\Aranda\Conserver”



2. Crie os valores a seguir com base na porta parametrizada e no IP do servidor em que o agente está instalado.

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

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

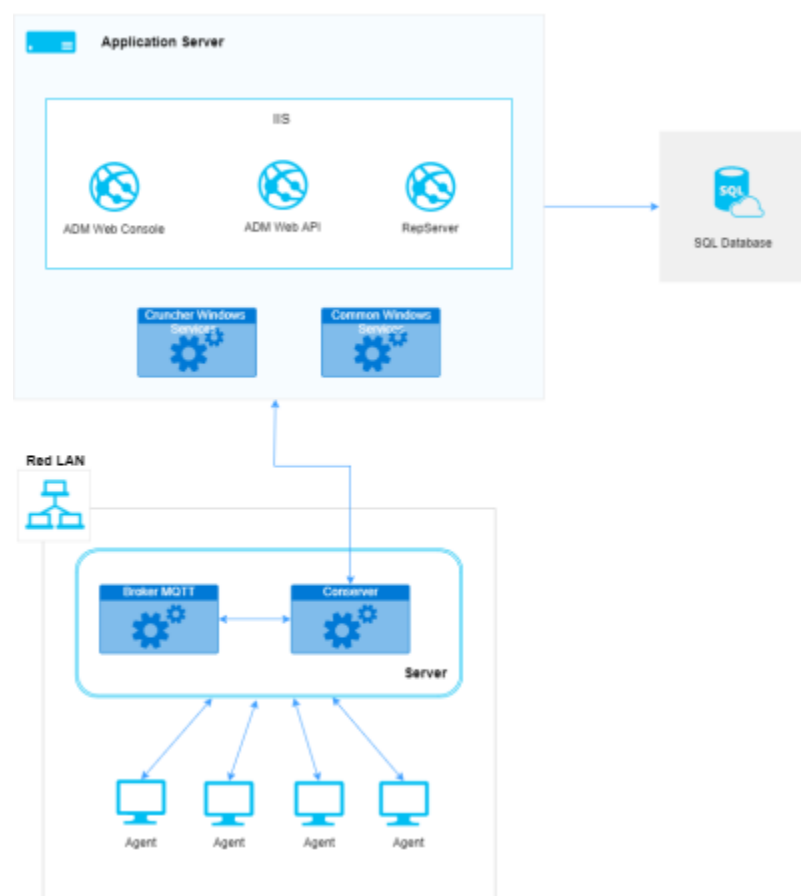
}
```



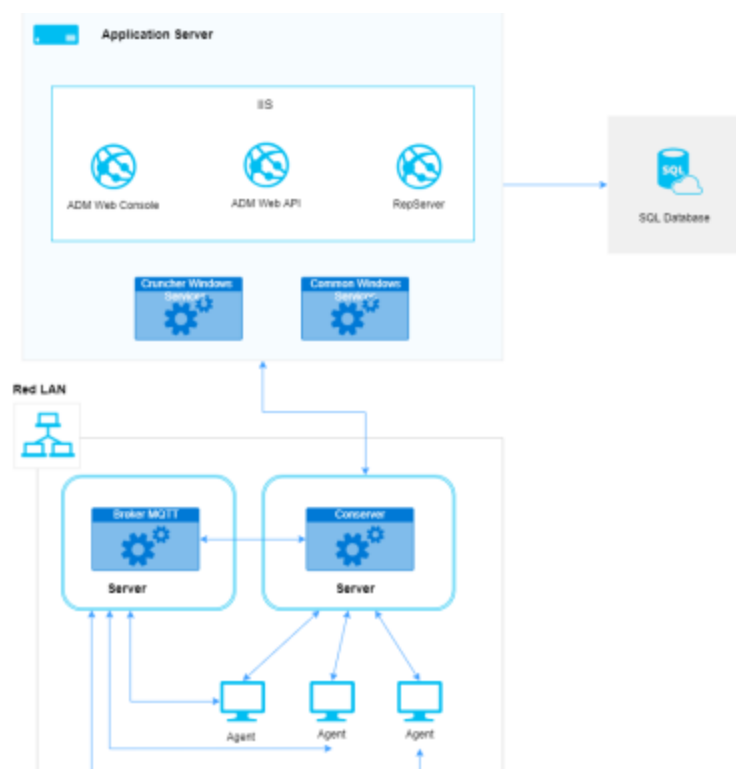
⚠ Nota: Ao fazer uma modificação no arquivo de configuração do conservador, você deve reiniciar o serviço.

Topologias suportadas no ADM com divisão de agente conservador

- Configuração do broker no mesmo servidor que o conservador

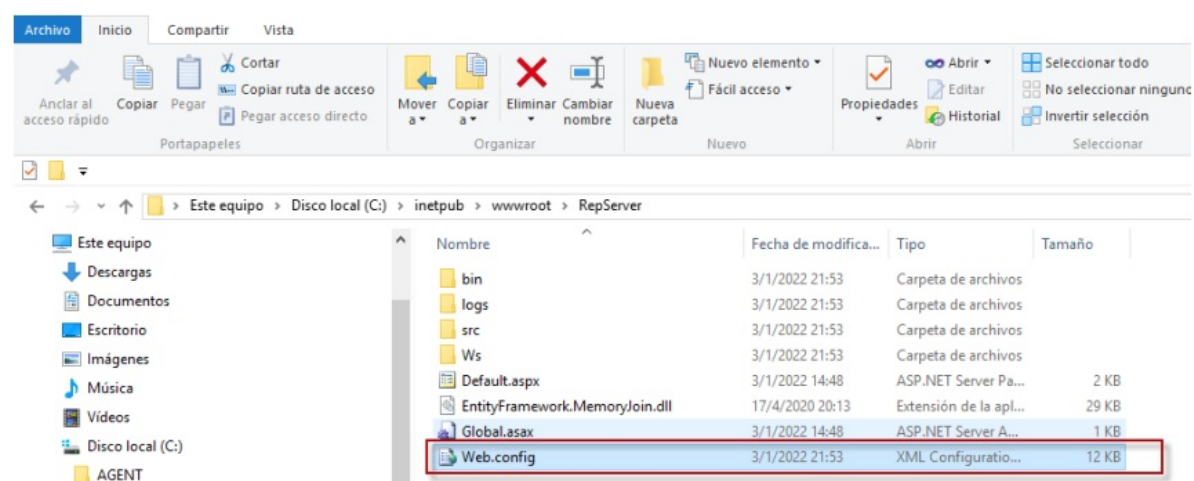


- Configurando o agente em um servidor diferente do conservador



Configurando o agente a partir do Repserver

1. Para configurar a comunicação entre o repserver diretamente com o Broker, você deve configurar o `web.config` do repserver localizado no caminho `'%inetpub\wwwroot\RepServer'`.



2. Adicione os seguintes valores em `<appSettings>` com base na porta parametrizada e no host do servidor em que o agente está instalado.


```
{

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

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

}
```

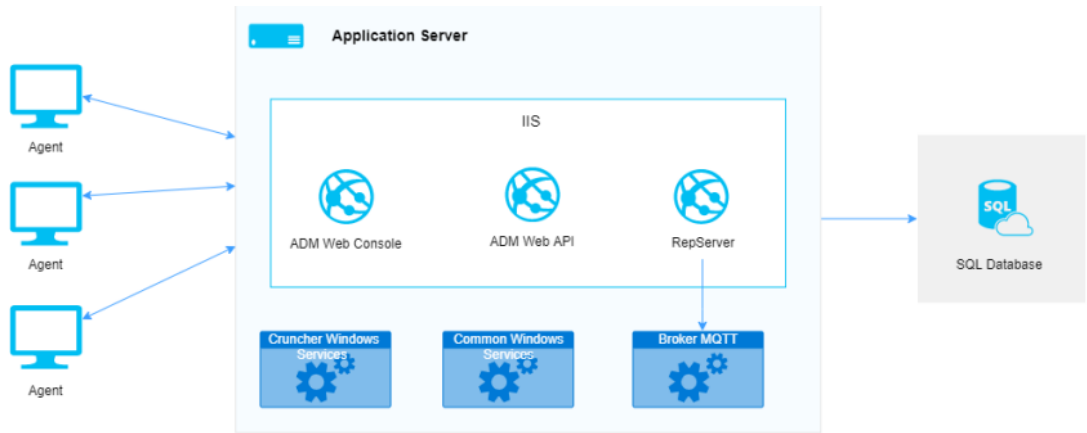
```
118 <provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" />
119 <provider invariantName="Oracle.ManagedDataAccess.Client" type="Oracle.ManagedDataAccess.EntityFramework.EFOracleProviderServices, Oracle.ManagedDataAccess" />
120 </providers>
121 <defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">
122 <parameters>
123 <parameter value="v11.0" />
124 </parameters>
125 </defaultConnectionFactory>
126 </entityFramework>
127 <appSettings>
128 <add key="vs:EnableBrowserLink" value="false" />
129 <add key="logLevel" value="Information" />
130 <add key="% EntityFramework_Extensions_LicenseName" value="4339:100-arandasoft.com" />
131 <add key="% EntityFramework_Extensions_LicenseKey" value="2a228917-e440-1205-c78b-d06a907829f5" />
132 <add key="mqttServerPort" value="" />
133 <add key="mqttIp" value="" />
134 </appSettings>
135 <runtime>
136 <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
137 <dependentAssembly>
138 <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
139 <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0" />
140 </dependentAssembly>
141 <dependentAssembly>
142 <assemblyIdentity name="DotNetZip" publicKeyToken="6595c70814667745" culture="neutral" />
143 <bindingRedirect oldVersion="0.0.0.0-1.14.0.0" newVersion="1.14.0.0" />
144 </dependentAssembly>
145 <dependentAssembly>
146 <publisherPolicy apply="no" />
147 <assemblyIdentity name="Oracle.ManagedDataAccess" publicKeyToken="89b483f429c47342" culture="neutral" />
148 </dependentAssembly>
149 <dependentAssembly>
150 <assemblyIdentity name="System.Runtime.CompilerServices.Unsafe" publicKeyToken="b03f5f7f11d50a3a" culture="neutral" />
151 <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="5.0.0.0" />
152 </dependentAssembly>
153 </assemblyBinding>
154 </runtime>
155 </configuration>
```

3. Para que as alterações sejam aplicadas, o dispositivo deve ser reiniciado.

➤ **Nota:** Para configurar o broker diretamente para o repserver, deve-se levar em consideração que ele só funciona com uma versão do agente desde a 9.13, e as seguintes funcionalidades não são suportadas nesta arquitetura:

- Descobrimento.
- Distribuição de agentes.
- Regra de descoberta.
- LDAP- Descoberta de dispositivos.
- Virtualização.
- Monitorização.

Configurando o agente apontando diretamente para o Repserver

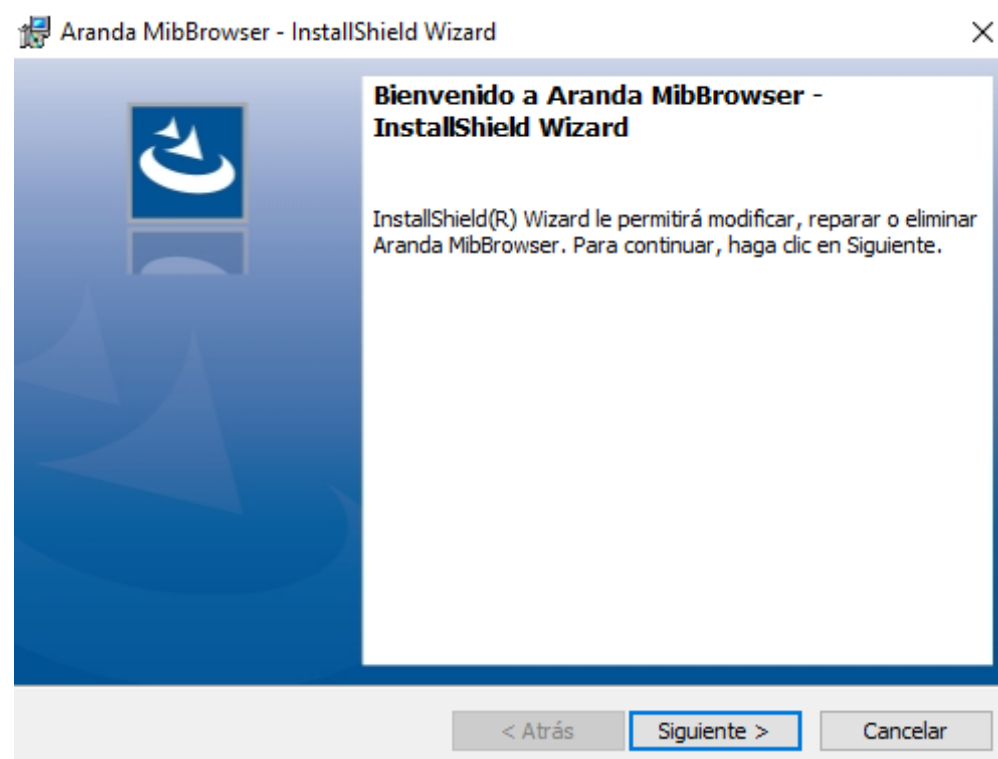


➤ **Nota:** O agente pode ou não estar no mesmo servidor que o repserver.

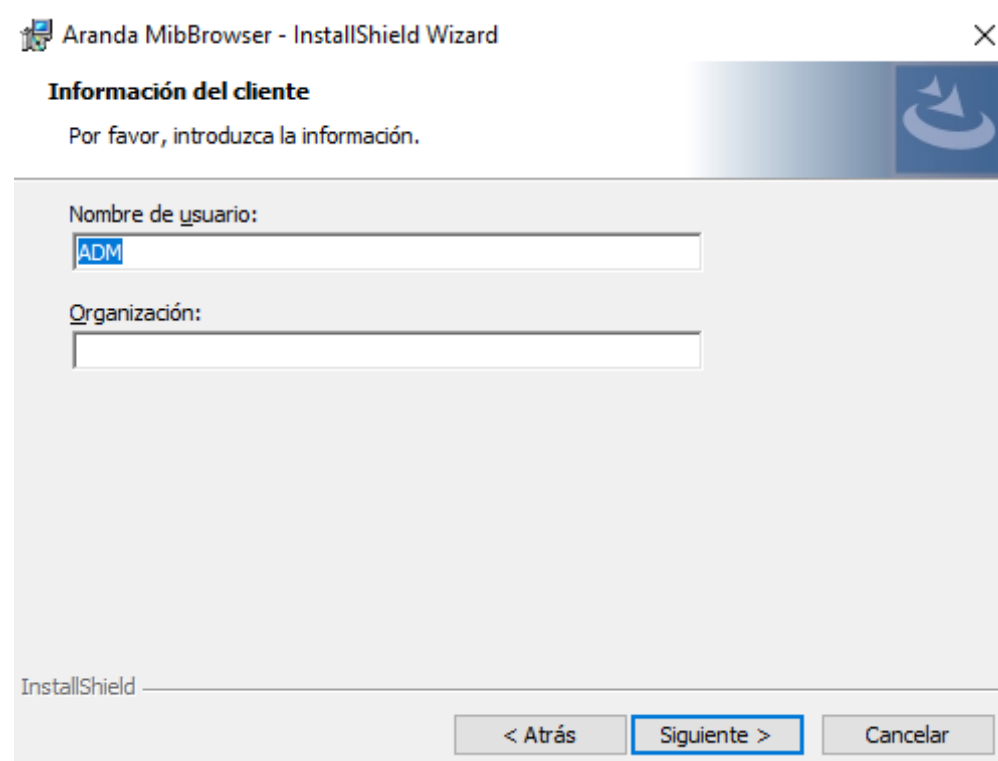
[Instalador do Aranda MQTT Broker](#)

Instalador/Lavador MibBrowser

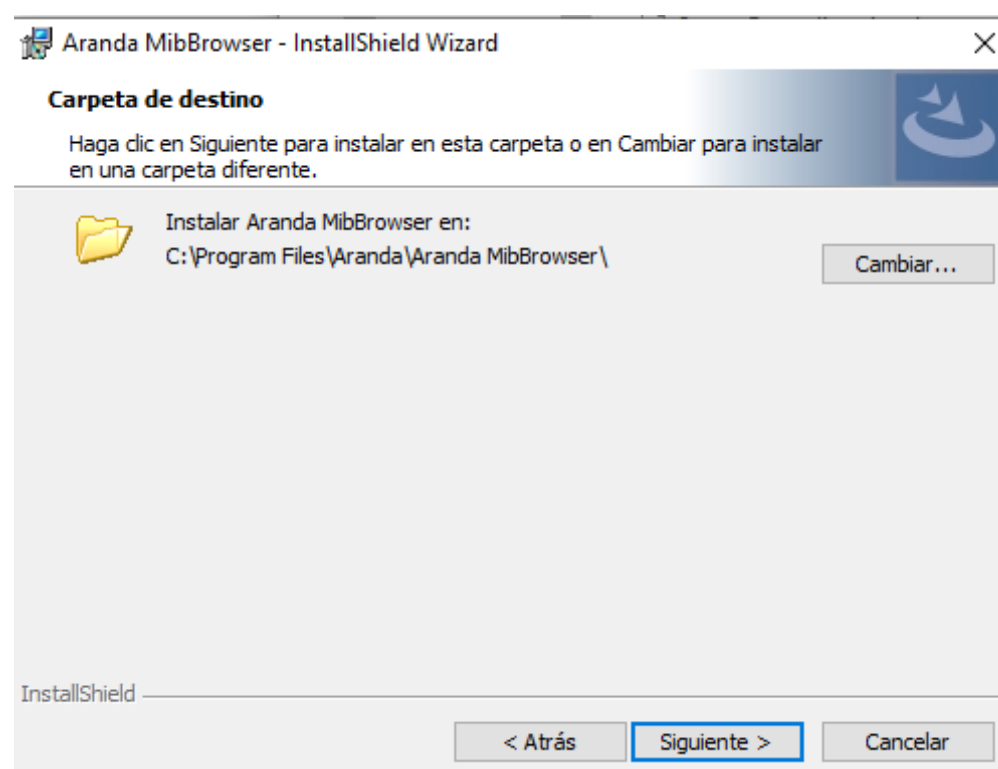
1. Execute o instalador Aranda.MibBrowser.exe



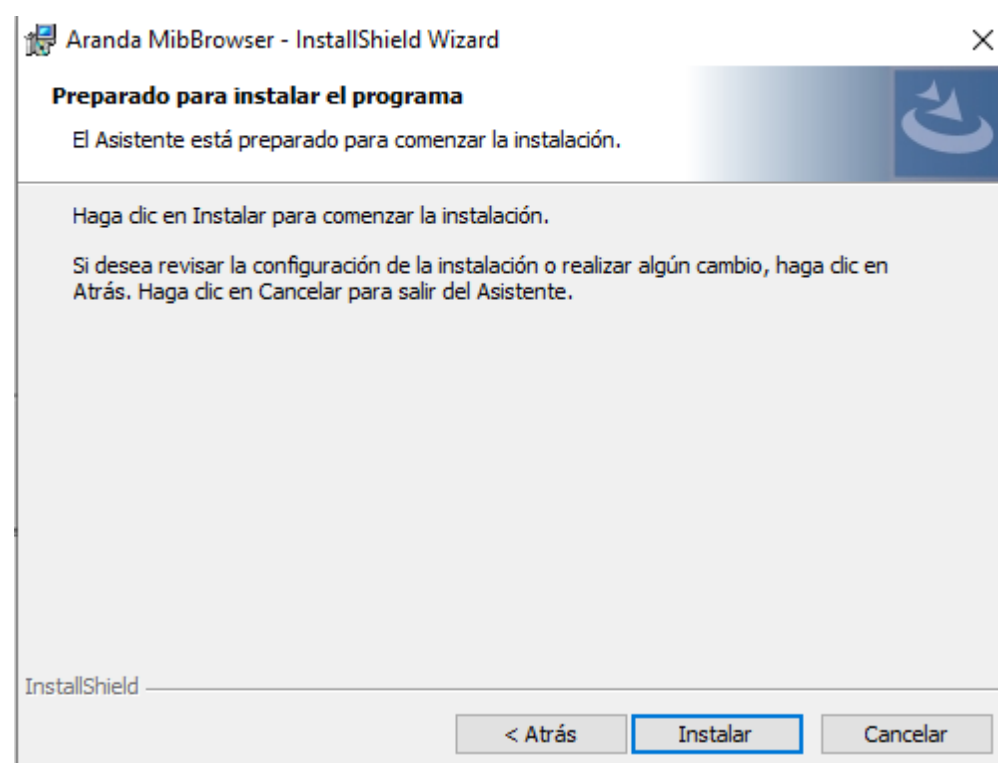
2. Você pode definir o nome de usuário ou a organização e clicar em Seguinte. Esses campos podem ser deixados em branco.



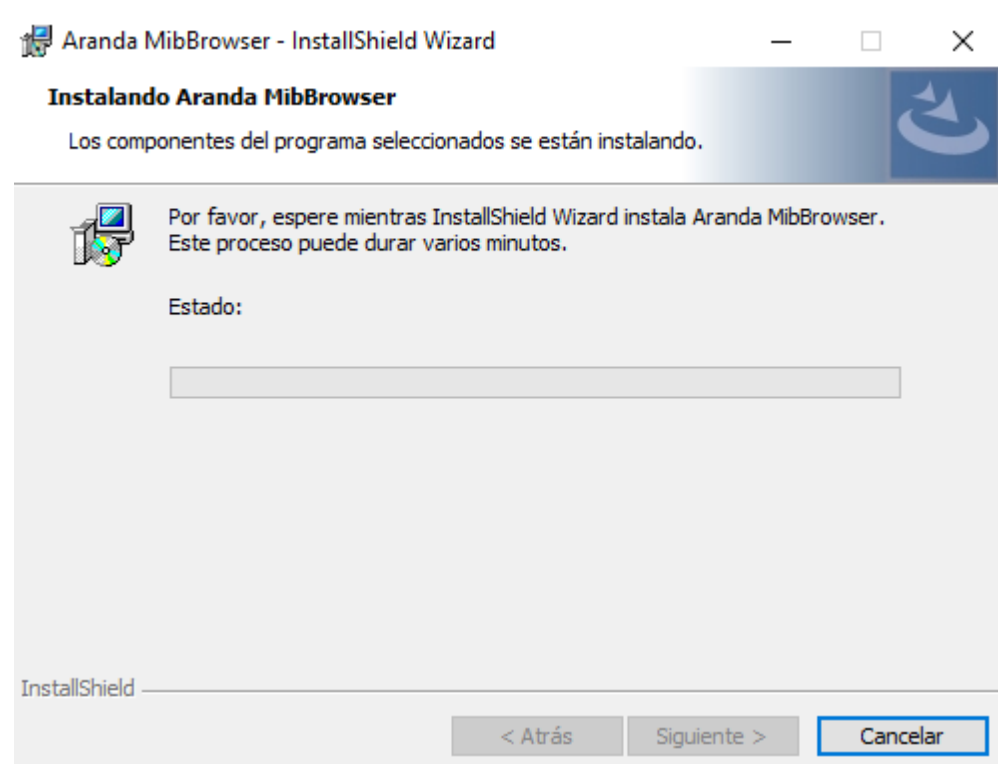
3. O instalador seleciona um local para instalação ou você pode alterá-lo e clicar em Seguinte.



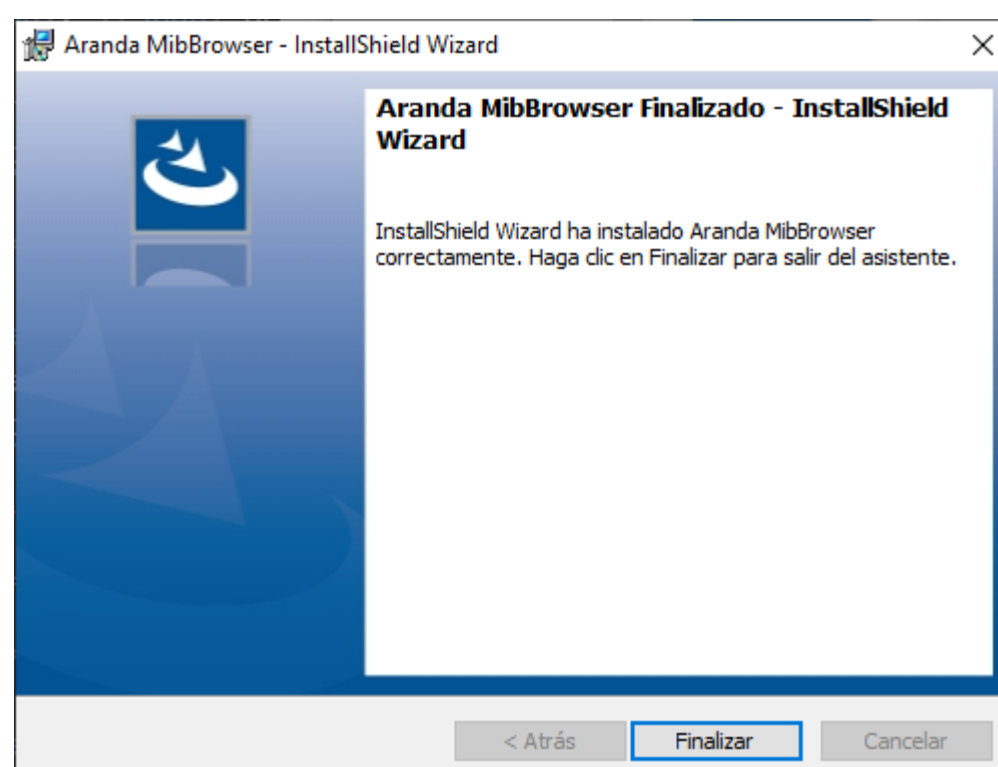
4. Em seguida, prosseguimos para a instalação, clique em Instalar.



5. Aguarde enquanto o instalador conclui o processo.



6. Confirme a instalação clicando no botão Fim.



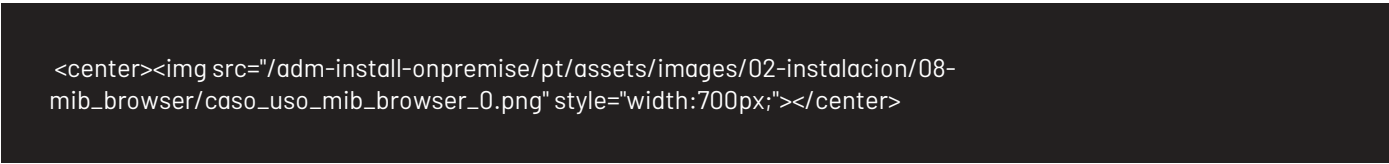
Configurações do navegador Mib

Configurações do MibBrowser

[« Instalador do Aranda MibBrowser](#)

O MibBrowser permite compilar MIBs (Bases de Informações de Gerenciamento) que contêm informações sobre os OIDs (Object Identifiers) que podem ser consultados usando o SNMP (Simple Network Management Protocol) sobre um dispositivo, por exemplo, um roteador, switch ou impressora, etc.
Quando o aplicativo é iniciado, as seguintes seções podem ser identificadas

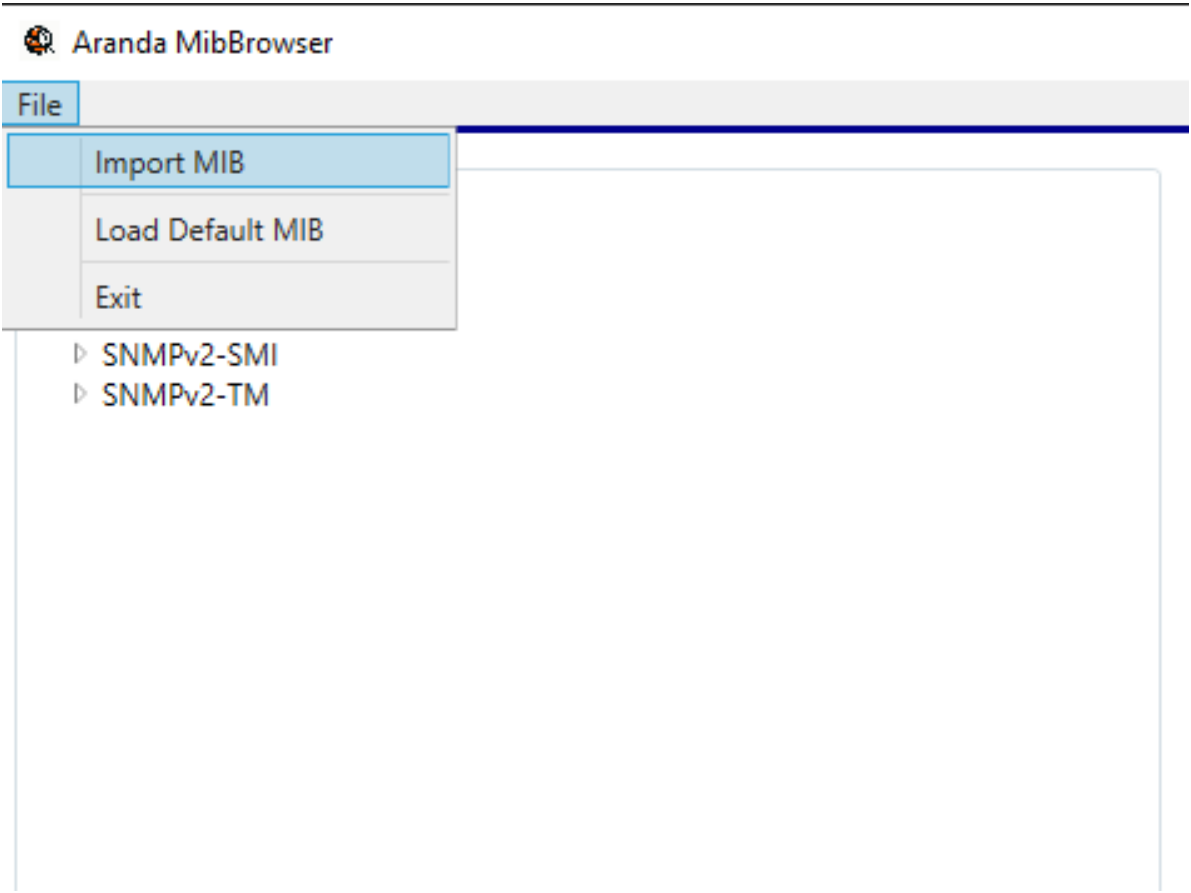
- 1. Mibs
- 2. Identificador de objeto
- 3. Configurações
- 4. Valor Oid



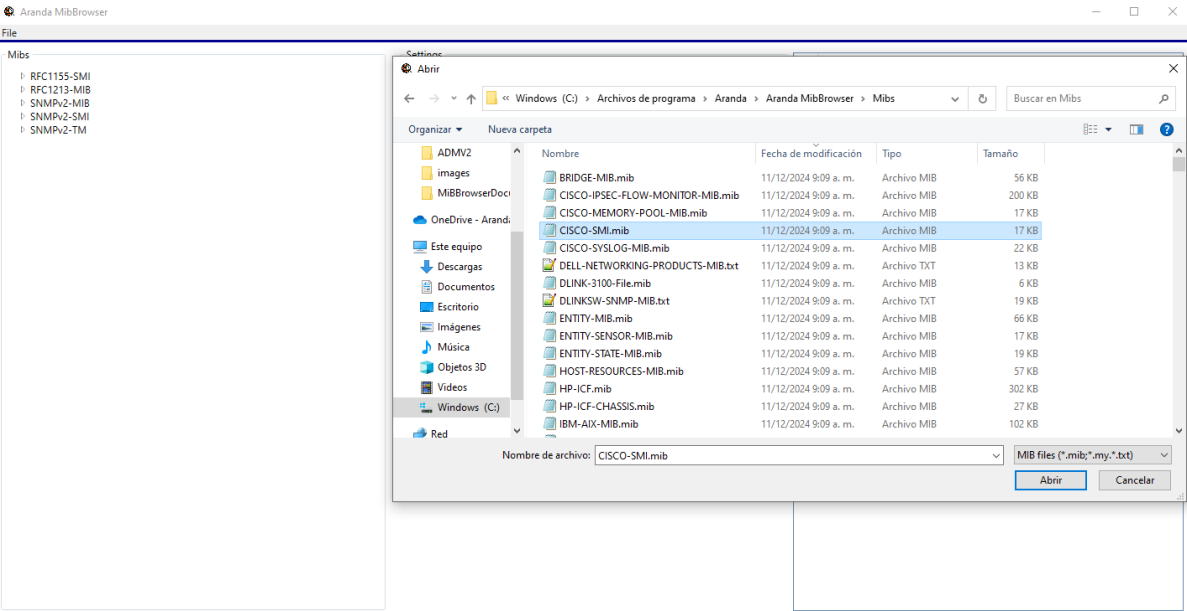
1. Os MIBs inicialmente compilados são os seguintes MIBs:

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

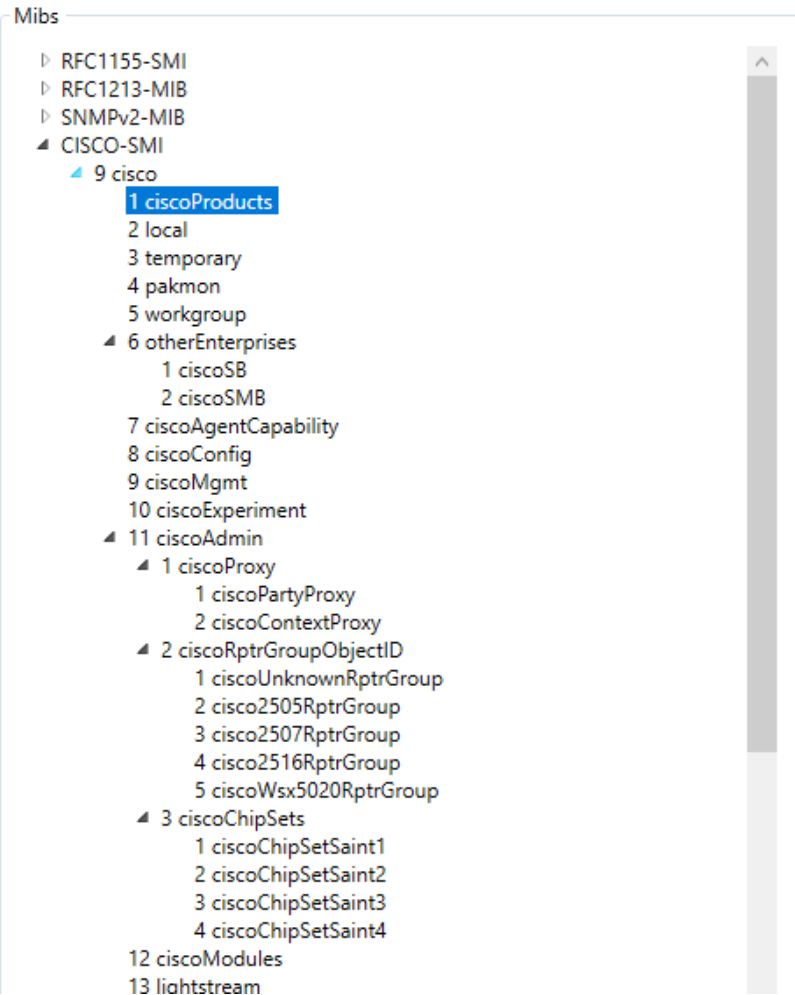
Se você deseja compilar outro MIB, pode fazê-lo através da opção de menu



Ao carregar o MIB corretamente, você verá a árvore com todos os MIBS relacionados, por exemplo, usamos o CISCO-SMI MIB.

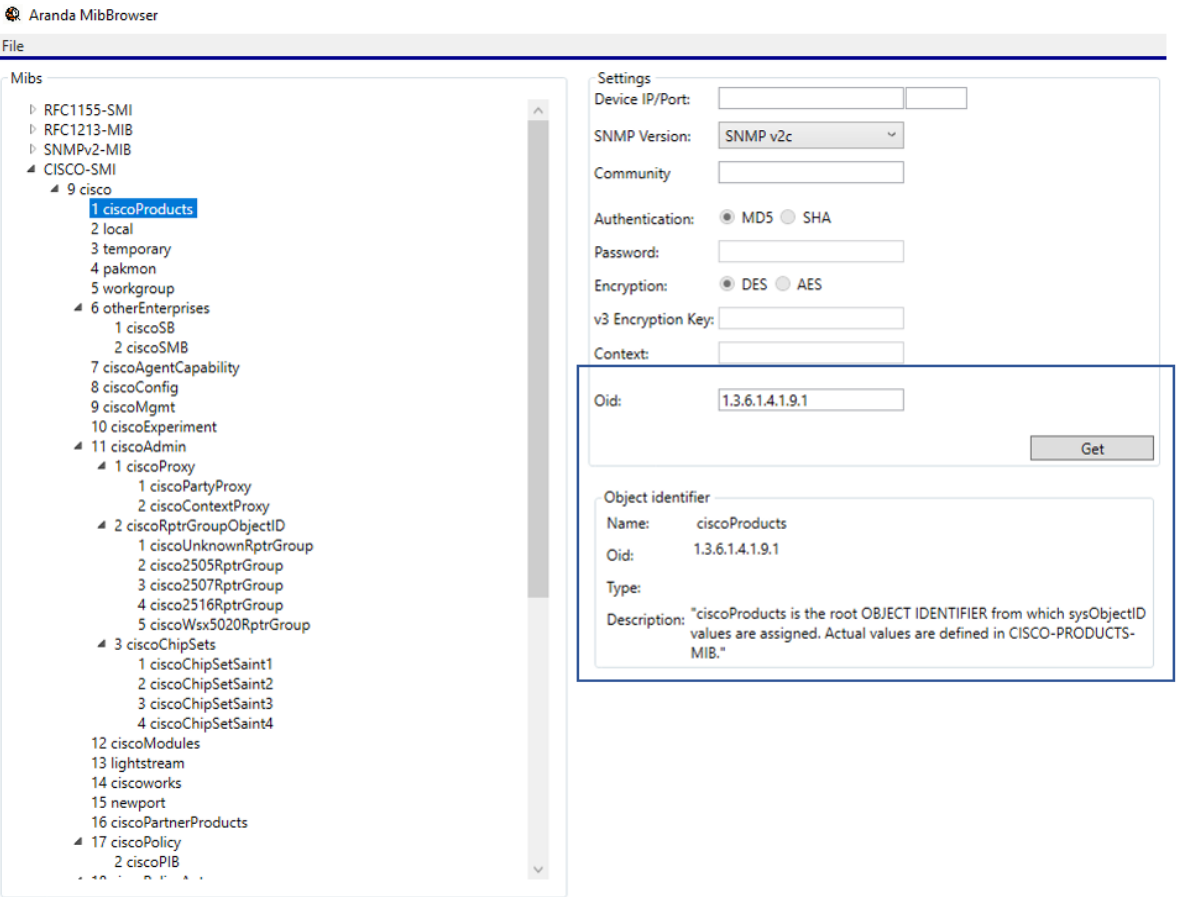


Consultamos a árvore MIBS

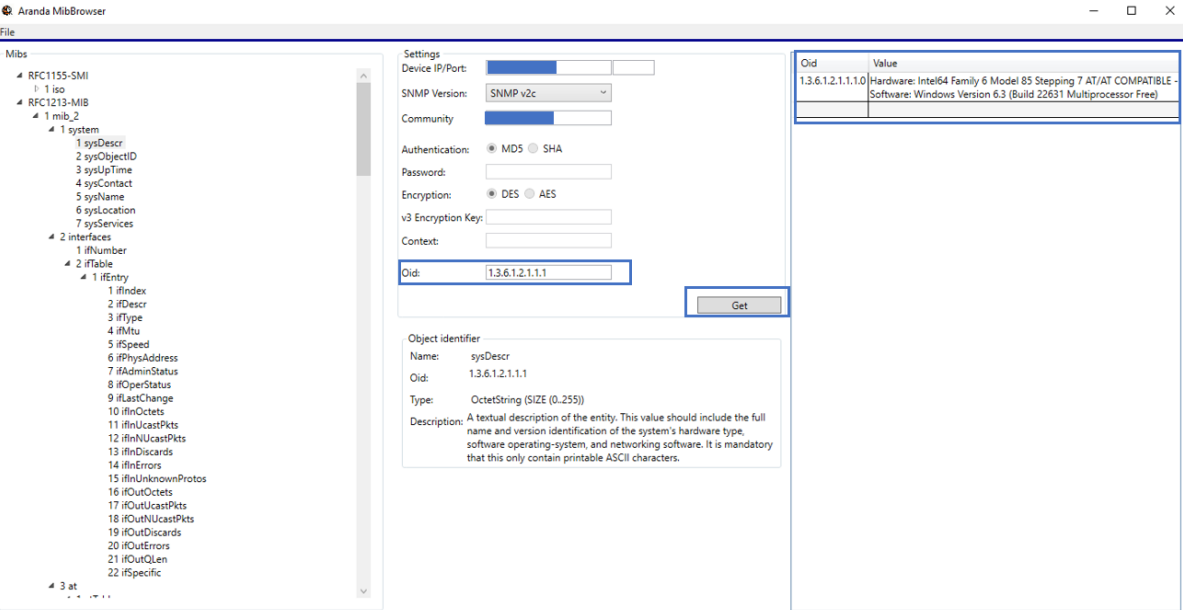


✎ **Nota:** Um MIB geralmente tem dependências que é recomendável carregá-lo em seu MIB principal ou copiá-lo manualmente para o MIB. Diretório de instalação do MibBrowser na pasta **MIBS**, pois é o caminho onde o aplicativo consulta para tentar resolver dependências automaticamente.

2. Quando você carrega um MIB, pode ver os OIDs relacionados, se selecionar um nó, poderá ver as informações na seção Identificador de objeto



3. Para consultar um OID, você pode preencher o formulário com os dados necessários, pressionar o botão Obter e, se houver informações, elas serão mostradas na seção OID e valor.



⚠ **Nota:** Observe que o OID inserido deve estar relacionado ao dispositivo.

[« Instalador do Aranda MibBrowser](#)

Controle remoto

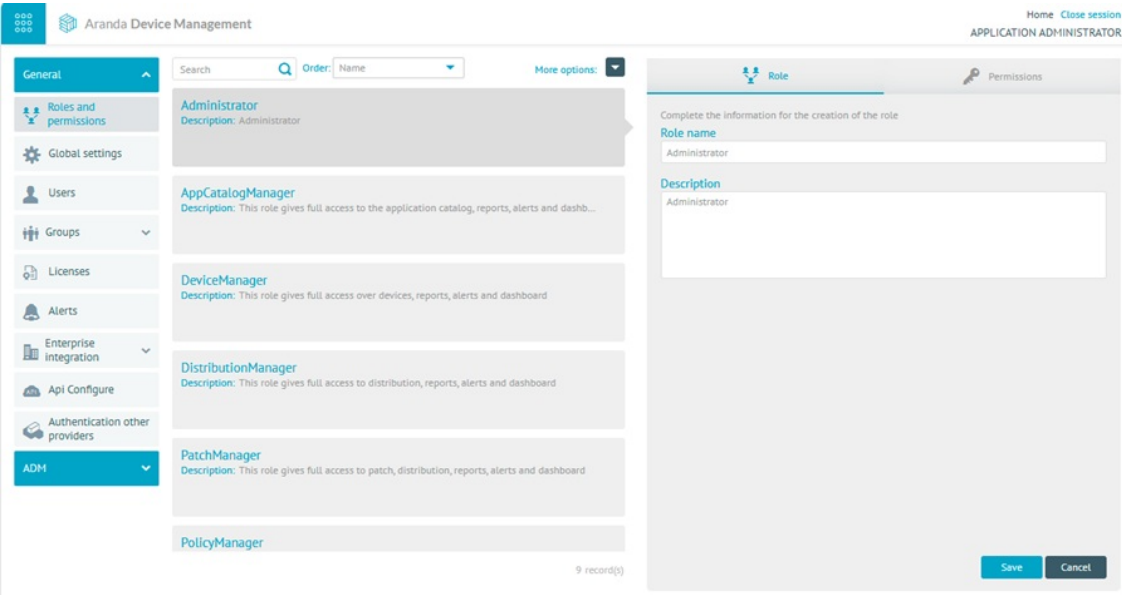
Ele permite que você assuma o controle das máquinas de forma simples e eficiente e transfira arquivos de forma conveniente, facilitando o gerenciamento remoto das estações de trabalho.

⚠ **Nota:** Essa funcionalidade não é compatível com instalações locais de versões do ADM anteriores à 9.21.1

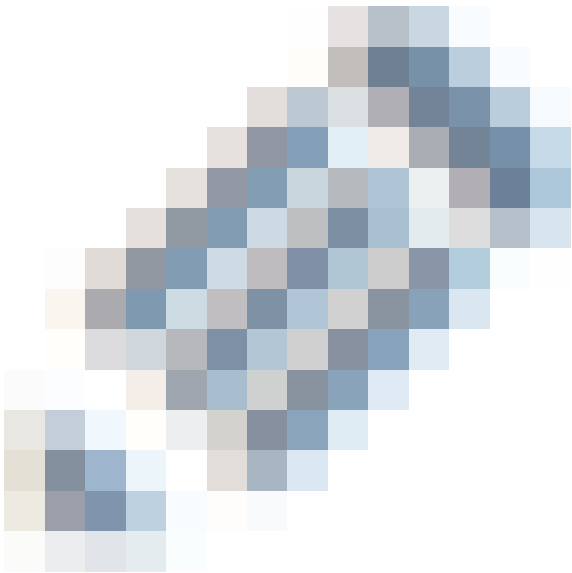
Processo de configuração de instalação local

Você deve considerar as seguintes etapas para configuração de controle remoto em instalações OnPremise:

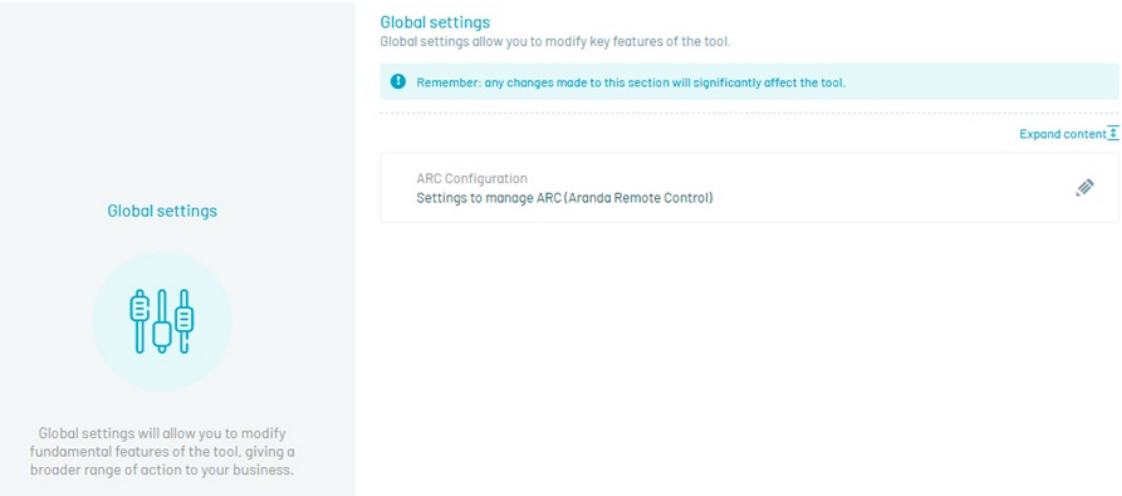
- Ative a funcionalidade no console do ADM acessando **Configuração > Geral > Configurações globais**.



- Na visualização de informações de Configurações globais, selecione o ícone Configuração do ARC Clique Editar

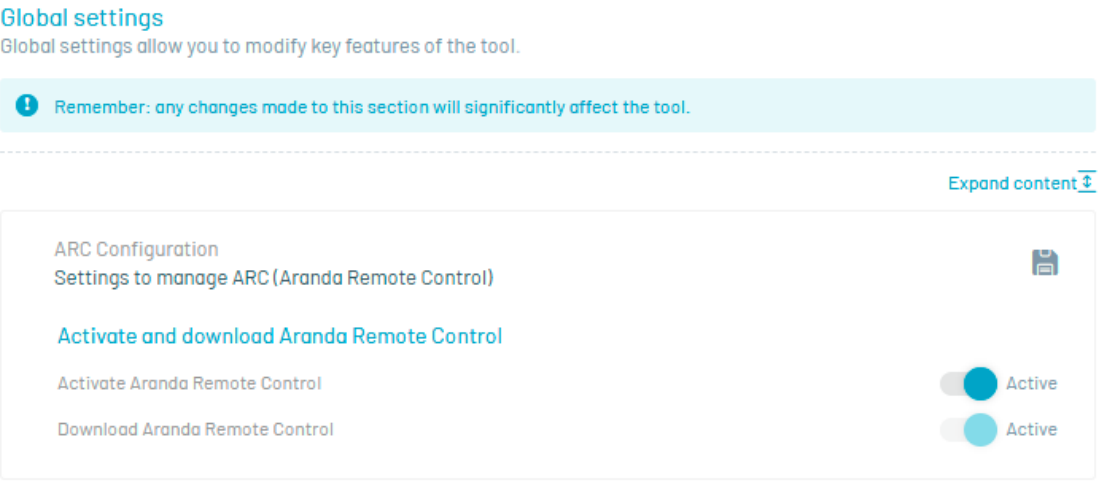


ou no Expandir conteúdo.



📌 **Nota:** Em implantações nuvem, esse campo só pode ser exibido, mas não editado. {:#important}

- Valide isso Ativar o controle remoto Aranda Ter a caixa de seleção ativada (padrão). Se não estiver, habilite-o e clique no botão Salvar.



- Execute a configuração pós-instalação correspondente **Aranda.ADM.Web.Installer** no servidor de aplicativos.
[Exibir configurações](#)

Instalador/Controle Remoto

Os Agentes do ADM Windows do ADM versão 9.19.2, após executar a instalação zero ou uma atualização de uma versão anterior, instalarão automaticamente o novo componente de controle remoto após 30 minutos. Os seguintes processos e serviços são exibidos no dispositivo.

📌 **Nota:** No caso de uma falha de conexão no momento da instalação ou atualização do componente de controle remoto, o agente ADM executará novas tentativas de instalação a cada 4 horas.

Processos e serviços de componentes de controle remoto

Atualização de componentes de controle remoto

Especialista em suporte remoto do instalador/visualizador

Instalação do visualizador de controle remoto

Configuração do controle remoto

Processo de configuração do controle remoto

Você deve considerar as seguintes etapas para configuração de controle remoto em instalações OnPremise:

- Ativar a funcionalidade executando uma atualização no banco de dados do produto ADM

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

- Execute a configuração pós-instalação correspondente **Aranda.ADM.Web.Installer** no servidor de aplicativos.
[Exibir configurações](#)

Configuração e instalação do agente

Considere as seguintes etapas para a configuração e instalação dos agentes de controle remoto:

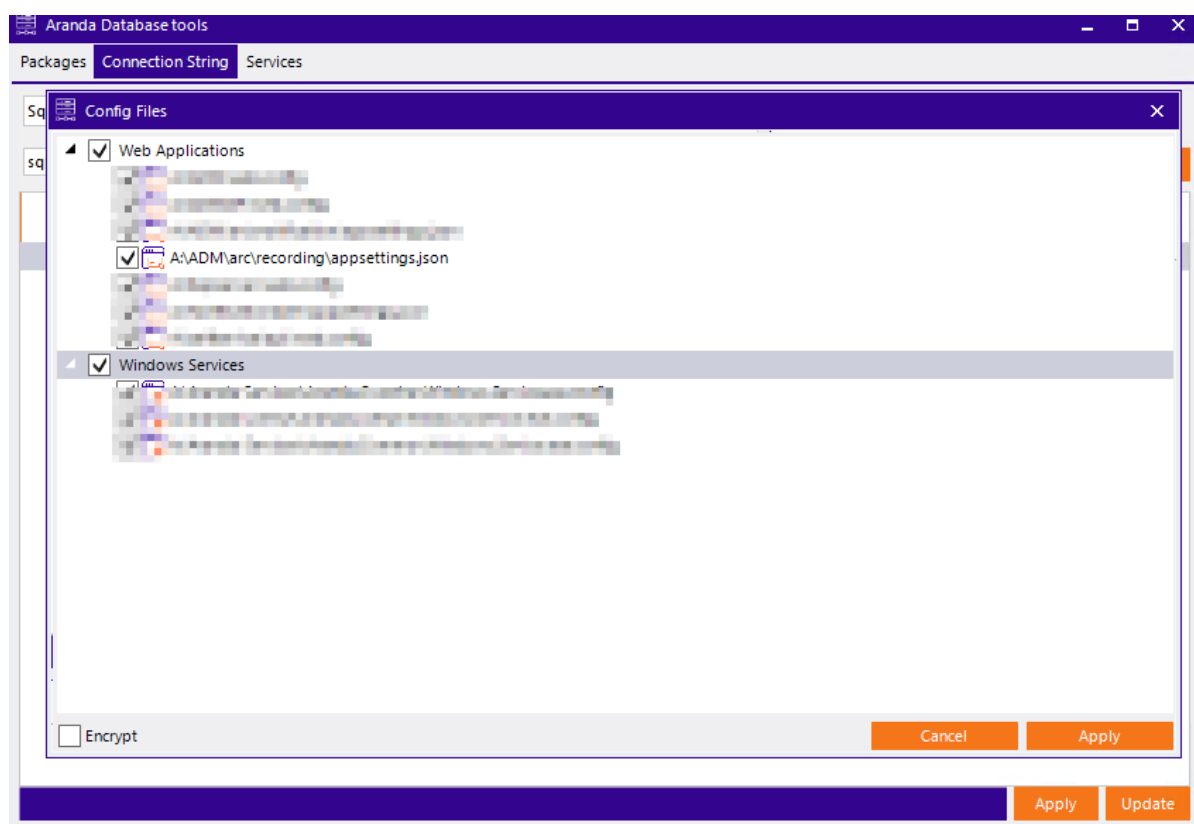
- Para realizar o controle remoto, é necessário ter o componente de controle remoto instalado nos dispositivos aos quais a conexão remota deve ser feita. [Instalação de componentes de controle remoto](#)
- Instalação do visualizador do controle remoto, necessário no dispositivo a partir do qual a conexão remota é feita [Especialista em suporte remoto do visualizador de instalação](#)

Configuração do controle remoto

Depois de instalar o arquivo Aranda.ADM.Web.Installer realizar configurações subsequentes no servidor de aplicativos e no console ADM para garantir a operação correta do novo controle remoto, levando em consideração as seguintes etapas:

1. Configurar cadeia de conexão

Configure a string de conexão para o site de gravação, por meio do módulo Aranda Database Tools v9. Os sites de notificação não exigem a configuração da cadeia de conexão.



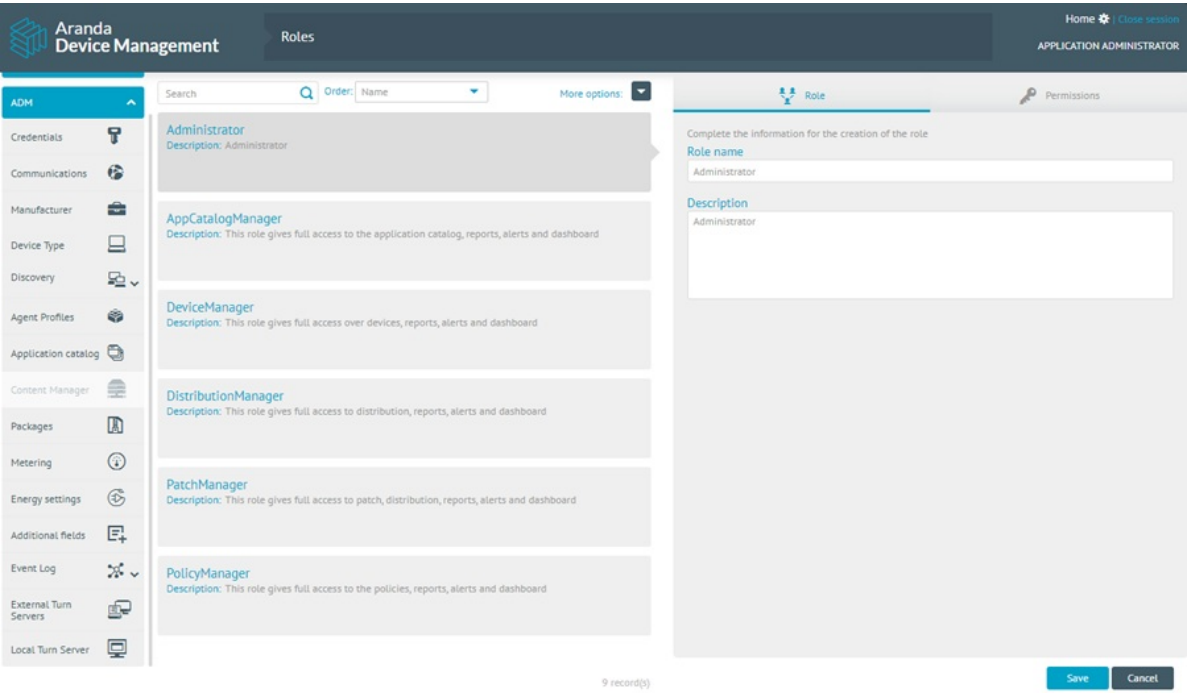
📌 **Anotações:**

- Quando a configuração é aplicada com Criptografar habilitado, uma mensagem de alerta pode ser exibida porque a criptografia não é suportada para arquivos JSON.
- Ao fazer alterações na cadeia de conexão do servidor de gravação, reinicie o IIS para que as alterações sejam aplicadas corretamente.
- Se forem feitas alterações no provedor de armazenamento após a configuração, mova as informações contidas no provedor anterior para o atual. Se essa ação não for executada, as atualizações do agente não serão bem-sucedidas e você não poderá acessar as gravações nas auditorias.

2. Faça login no console

Faça login no console do ADM com o usuário com as permissões necessárias para gerenciar as opções Servidores de turno externos e Servidor de turno local nas Configurações do ADM.

⚠ **Importante:** As opções de Torneamento Externo e Local estão disponíveis apenas em instalações On-Premise.



3. Servidores de turno externos

A funcionalidade de transferência de arquivos do controle remoto usa um protocolo P2P baseado em WebRTC. Quando dois dispositivos não conseguem estabelecer uma conexão direta entre si, é necessário um servidor Turn para facilitar a comunicação.

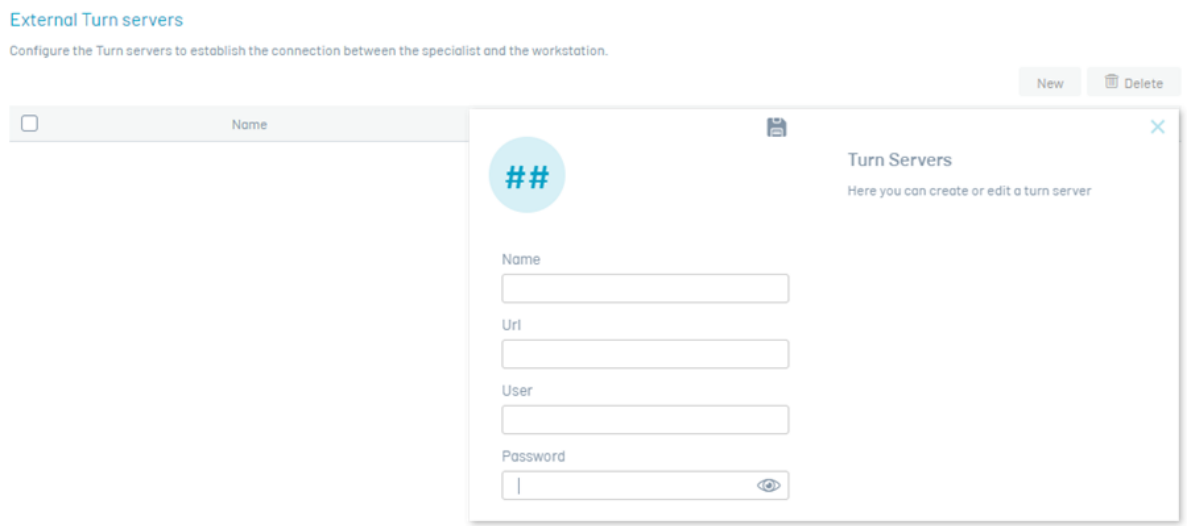
Para adicionar um servidor Turn externo no **Servidores de turno externos**, siga estas etapas:

- A. Clique na opção **Novo**.
- B. Preencha os campos solicitados de acordo com a tabela a seguir:

Campo	Descrição
Nome	Nome que você deseja atribuir à configuração, entre 6 e 50 caracteres.
URL	Corresponde ao site do servidor STUN/TURN, por exemplo: turn:<server_public_ip>:puerto ou stun:<server_public_ip>:puerto .
Utilizador	Nome do usuário autorizado a se conectar ao servidor STUN/TURN.
Senha	Senha associada ao usuário que permite a conexão com o servidor STUN/TURN.

- C. Finalize clicando no botão **Salvar**.

📌 **Nota:** Essa configuração é necessária para transferência de arquivos quando o agente especialista e o agente da estação de trabalho não estão na mesma rede, portanto, ambos os dispositivos devem ter permissão para sair para a Internet pela porta configurada.



O usuário pode registrar o número de servidores externos do Turn que julgar necessário para ter uma boa comunicação entre os dispositivos do especialista e a estação de trabalho através do console ADM. Para excluir um servidor Turn externo, no **Servidores de turno externos** Selecione o(s) servidor(es) a serem excluídos e clique no

botão **Eliminar**, será confirmado que o(s) servidor(es) foi(foram) excluído(s) com êxito.

Você pode usar o WebRTC público STUN/TURN, fazendo uma pesquisa na web “Lista de servidores STUN” você poderá listar os diferentes servidores STUN/TURN públicos disponíveis. Ao configurar servidores públicos em estações de trabalho e em computadores especializados, eles devem permitir a saída dos servidores configurados para os sites. Também é possível configurar o servidor STUN/TURN fornecido no instalador [fazendo as configurações no Aranda Turn Stun WebRTC Server Windows Service](#). Além disso, o STUN/TURN público pode ser usado em conjunto com seus próprios servidores instalados, conforme mencionado acima.

4. Ativar servidor local

Para estabelecer a comunicação de controle remoto entre o agente especialista e o agente da estação de trabalho, use um servidor Turn local que possa retransmitir o tráfego de rede.

Para adicionar um servidor Turn local, siga estas etapas:

A. Clique na opção **Servidor de turno local** no menu principal.

B. Preencha o campo **Anfitrião** com o caminho para o servidor local, que pode ser o IP do servidor ou o DNS. O campo **Porta** ele é definido por padrão para o valor 8081 e o SSL está inativo; se a porta for alterada ou o SSL estiver ativado [faça as configurações no serviço Aranda Turn Server](#) instalado no servidor.

C. Finalize clicando no botão **Salvar**

Turn Server Local



Next configure the local Turn server.

Turn Server Local

Define fields for configuration

Host

Enter the provider URL

dns-servidor - IP

Puerto

Enter the port associated with the server

8081

Enable SSL

☐

Cancel

Save

Configuração manual de serviço

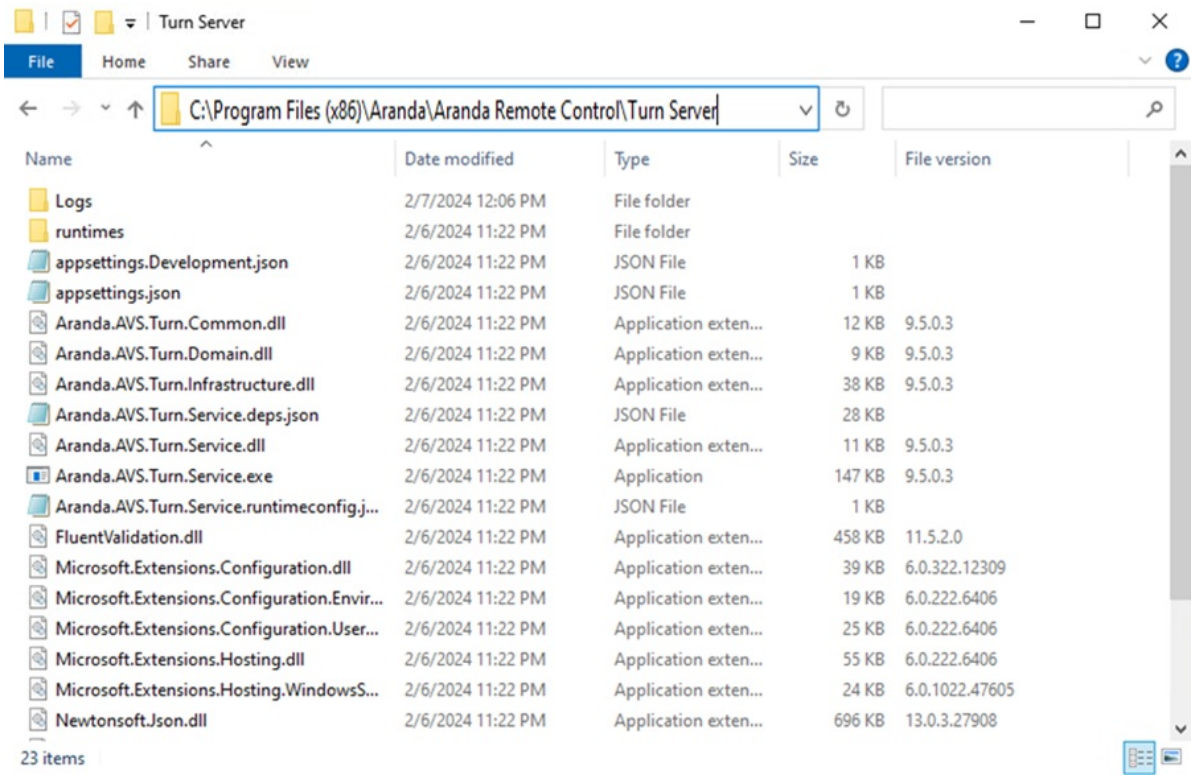
Virar configuração do servidor

Depois de instalar o serviço Aranda Turn Server, você não precisa fazer nenhum ajuste para sua operação. No entanto, as parametrizações podem ser feitas de acordo com necessidades específicas, como alterar a porta de conexão (8081 por padrão) e habilitar o SSL (desabilitado por padrão). Se você precisar fazer essas configurações, siga estas etapas:

1. Validando o arquivo appsettings.json

Antes de fazer alterações, verifique o **appsettings.json** localizado no caminho de instalação do serviço (padrão: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) para garantir que a porta esteja definida como 8081 por padrão. Se a porta não precisar ser modificada, nenhum ajuste adicional será necessário.

Além disso, valide se a porta 8081 está habilitada nas regras de firewall local para garantir o fluxo correto de tráfego. Nesse arquivo, você também pode encontrar a configuração para certificados SSL, que está desabilitada por padrão (IsSsl=false).



Configurações padrão appsettings.json:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "TurnConfiguration": {
    "CertificateParam": "",
    "CertificatePath": "",
    "CertificateSubject": "",
    "IsSsl": false,
    "Port": 8081,
    "SSLProtocols": "Tls12"
  }
}
```

2. Alteração da configuração da porta

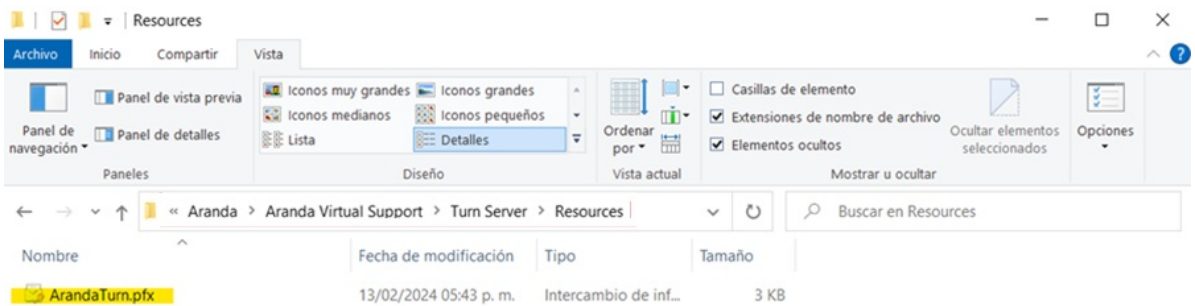
Edite o arquivo *appsettings.json* e configure a porta desejada substituindo <puerto> pelo número de porta desejado.

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

3. Configuração de conexão segura SSL

Edite o arquivo *appsettings.json*, altere “IsSsl” para true. Existem duas alternativas para adicionar o certificado SSL:

3.1. Adquira ou gere um certificado PFX, que deve estar localizado dentro da pasta Recursos (a pasta deve ser criada se não existir) no caminho de instalação do serviço.



O nome do arquivo é registrado no arquivo Caminho do certificado e a chave codificada em base 64 para gerar o

certificado deve ser registrada em **CertificadoParam**, ambas as opções disponíveis no arquivo appsettings.json.

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

3.2. Se você tiver um certificado PFX armazenado no bucket de certificados, poderá configurá-lo nomeando o certificado no **Assunto do certificado** do arquivo appsettings.json.

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

4. Reinicialização do serviço

Reinicie o serviço Turn Server Windows para que as alterações de configuração entrem em vigor. O serviço agora deve escutar na porta recém-configurada e habilitar o uso do certificado SSL.

5. Configurações do firewall

Abra a porta que foi configurada na etapa 2 nas regras de entrada do firewall local. Esta etapa é crucial para permitir o tráfego pela nova porta e garantir que o Turn Server possa receber conexões de entrada na porta configurada.

Parametrizar a porta do Turn Server e o uso de SSL do serviço é um processo fundamental para garantir seu correto funcionamento e adaptá-lo às necessidades específicas de cada cliente. Seguindo estas etapas, você pode garantir que o Turn Server esteja configurado corretamente e pronto para lidar com as conexões conforme necessário.

Configuração do servidor WebRTC Stun/Turn

Depois de instalar o serviço **Aranda Vire o Servidor WebRTC Atordoamento**, a configuração é necessária para que funcione corretamente.

1. Validação de arquivo turn-server.toml

Antes de fazer alterações, verifique se o **virar-servidor.toml** está localizado no caminho de instalação do serviço (por padrão: C:\Program Files(x86)\Aranda\Aranda Remote Control\Stun Server).


```

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

```

Para configurar o serviço STUN/TURN WebRTC, use o comando turn-server.toml:

- **Secção [turn]:** Especifica o domínio em que o servidor está localizado.
- **Secção [[turn.interfaces]]:** Indica as interfaces de escuta. Descreve a interface à qual o servidor STUN/TURN está vinculado. Várias interfaces podem ser indicadas.
- **Secção [turn.interfaces.transport]:** Define o tipo de transporte da interface, que pode ser udp ou tcp.
- **Secção [turn.interfaces.bind]:** Endereço IP e porta de ligação do soquete interno.
- **Secção [turn.interfaces.external]:** Ele é usado para vincular ao endereço da sua placa de rede local. Por exemplo, se você tiver duas NICs, A e B, em seu servidor, e o endereço IP da NIC A for 192.168.1.2 e o da NIC B é 192.168.1.3, se vinculado à IAS A, você deve vincular ao endereço 192.168.1.2. Link para 0.0.0.0 Isso significa que você ouve todas as interfaces ao mesmo tempo. A palavra external significa que sua placa de rede para o cliente pode “ver” o endereço IP. Continuando com o exemplo anterior, se sua placa de rede A se comunicar com o exterior, os outros clientes verão seu endereço LAN (ou seja, 192.168.1.2). No entanto, na realidade, a topologia de rede em que o servidor é implantado pode ter outro IP público, como 1.1.1.1, que é o endereço IP visto por outros clientes. A razão pela qual eles são necessários bind e external é que, para o protocolo STUN, o servidor precisa relatar seu próprio endereço IP externo, permitindo assim que o cliente STUN se conecte ao endereço especificado usando o IP relatado pelo servidor.
- **Secção [api.bind]:** Escutar a API para consultas, por exemplo: http://127.0.0.1:3000/info.
- **Secção [log.level]:** Nível de log. Valores válidos: error, warn, info, debug, trace.
- **Secção [auth]:** Nome de usuário e senha para acessar o servidor.

2. Início do serviço

Inicie o serviço STUN Server (Aranda Turn Stun WebRTC Server) para que as alterações de configuração entrem em

vigor.

3. Configurações do firewall

Abra a porta ou portas configuradas na etapa 1 nas regras de entrada do firewall local e nos controladores de rede presentes na infraestrutura do cliente, para os protocolos TCP e UDP. Essa etapa é essencial para permitir o tráfego pela nova porta e garantir que o servidor STUN possa receber conexões de entrada na porta configurada.

As estações de trabalho (ARC Agent) e os computadores especializados (Specialist Agent) devem permitir a saída através das portas configuradas.

Além disso, se você precisar que ele opere como TURN WebRTC, deverá abrir o intervalo de portas49152-65535 para o protocolo UDP.

Exemplo e cenários de configuração de serviço STUN/TURN

Para fazer o servidor funcionar para dispositivos dentro e fora da rede, siga estas etapas:

1. Configure o reino

Altere o valor de realm para o domínio público ou endereço IP externo do seu servidor. Isso é importante para autenticar com êxito solicitações externas.

Se o endereço público do seu servidor for 1.2.3.4, defina-o como:

```
realm = "1.2.3.4"
```

2. Configurar ligação

O bind garante que o servidor STUN/TURN escute no IP privado para conexões dentro da rede local.

Se o endereço privado do seu servidor for 192.168.1.25, defina-o como:

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

Se você precisar que o serviço STUN/TURN escute em todas as interfaces ao mesmo tempo, configure-o como:

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

Essas configurações são necessárias apenas para [[turn.interfaces]].

3. Configurar externo

O external é onde o IP público do servidor é definido para que os computadores externos possam se comunicar adequadamente com o servidor STUN/TURN.

Se o endereço público do seu servidor for 1.2.3.4, defina-o como:

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

4. Autenticação

O [auth] Ele é configurado com usuários estáticos:

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

Isso permite conexões autenticadas com credenciais estáticas `user1:test` e `user2:test`. Certifique-se de usar credenciais mais seguras se você planeja expor esse serviço a dispositivos externos.

As outras seções podem ser deixadas por padrão.

Quando você executa a parametrização no `virar-servidor.toml`, isso deve ser observado da seguinte 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 você faz uma modificação no `virar-servidor.toml`, reinicie o serviço **Aranda Vire o Servidor WebRTC** **Atordoamento** para que as alterações entrem em vigor.

Cenários

Os cenários a seguir e o resultado são descritos abaixo de acordo com as configurações no exemplo.

Cenário	Especialista	Status da rede	Agente ARC	Status da rede	Resultado
1	Você só pode acessar o servidor TURN/STUN usando o IP público	Externo	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
2	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
3	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
4	Você só pode acessar o servidor TURN/STUN usando o IP privado.	Interno	Você só pode acessar o servidor TURN/STUN usando o IP privado.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP privado.
5	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você não pode usar o IP público para se conectar ao servidor TURN/STUN, pois seu acesso é restrito à rede interna (IP privado).	Interno	O Especialista e o Agente ARC não conseguem estabelecer comunicação devido a um problema de conectividade entre as redes (externas e internas).
6	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você não pode usar o IP público para se conectar ao servidor TURN/STUN, pois seu acesso é restrito.	Externo	O Especialista e o Agente ARC não conseguem estabelecer comunicação devido a um problema de conectividade entre as redes.

⚠ Nota:

- Para cobrir os cenários 1, 2 e 3, configure no [Site da AMD](#) o servidor External Turn da seguinte maneira:
Nome: nome da configuração.
URL: turn.1.2.3.4:3478 (1.2.3.4 refere-se ao IP público do servidor).
Utilizador: usuário1.
Senha: teste.

⚠ Anotações:

- Para cobrir o cenário (4), configure no [Site da ADM](#) o servidor External Turn da seguinte maneira:
Nome: nome da configuração.

URL: turn.192.168.1.25:3478 (192.168.1.25 refere-se ao IP privado do servidor).

Utilizador: usuário1.

Senha: teste.

- Se no **virar-servidor.toml** foi criado 0.0.0.0 no parâmetro bind, a configuração deve ser realizada no site como acima.

Instalador/Agente ADM

O ADM Agent é um programa instalado em dispositivos gerenciados que permite a geração de inventários e tarefas de gerenciamento associadas a processos de distribuição, atualização e uso de software, gerenciamento de políticas de energia e controle remoto.

Quando você instala o agente, vários serviços são criados no dispositivo que permitem estabelecer comunicação com o visualizador do controle remoto e o gerenciamento geral do dispositivo.



Há um agente para cada uma das plataformas suportadas:

- [Instalador do Agente ADM para Windows.](#)
- [Instalador do ADM Agent para Mac.](#)
- [Instalador do ADM Agent para Linux](#)

Implantação do agente

A implantação do agente é o processo de distribuição desse componente para os dispositivos que precisam ser gerenciados. O processo de distribuição e instalação do agente ADM pode ser realizado a partir do console web do ADM ou usando outras opções de implantação, da seguinte forma:

- [Instalação por Política de Domínio](#)
- [Instalação e distribuição com Aranda Device Management ADM](#)

Instalador/Agente ADM no Windows

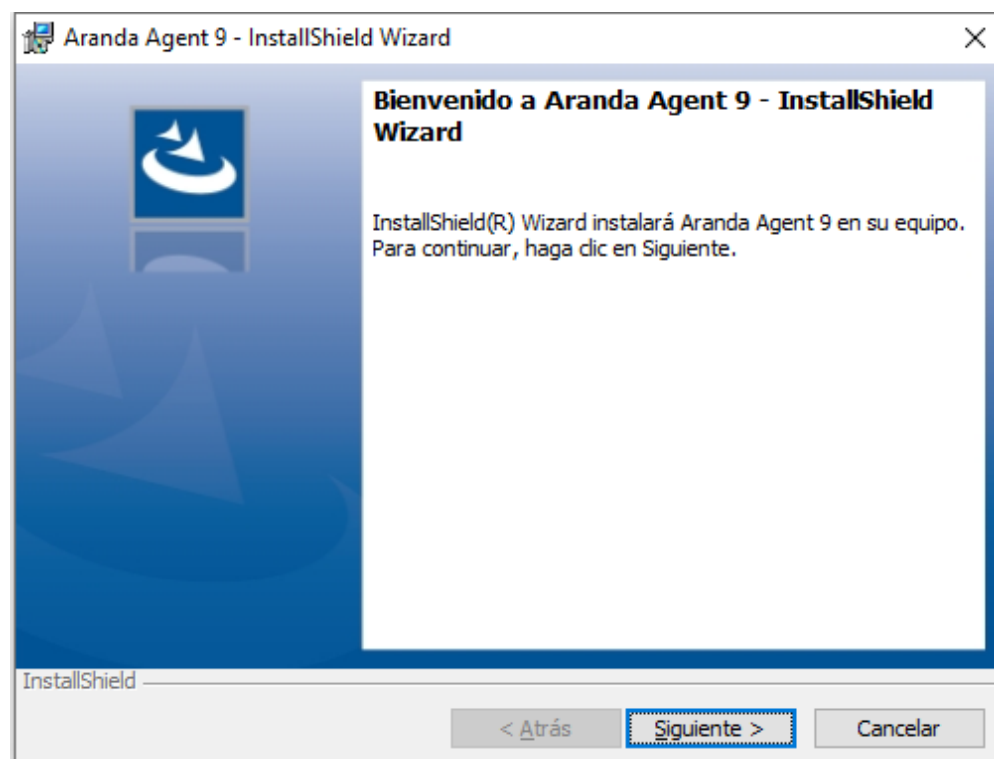
O terceiro arquivo executável é Aranda.Agent.Windows.x86_x64 que corresponde ao instalador do ADM Agent para Windows. Esse arquivo é responsável pela criação e configuração dos serviços necessários para a operação do ADM Agent for Windows.

O instalador detecta automaticamente o idioma do sistema, atualmente suportando inglês, espanhol e português. Se a configuração estiver em um idioma diferente, o instalador usará o espanhol como padrão.

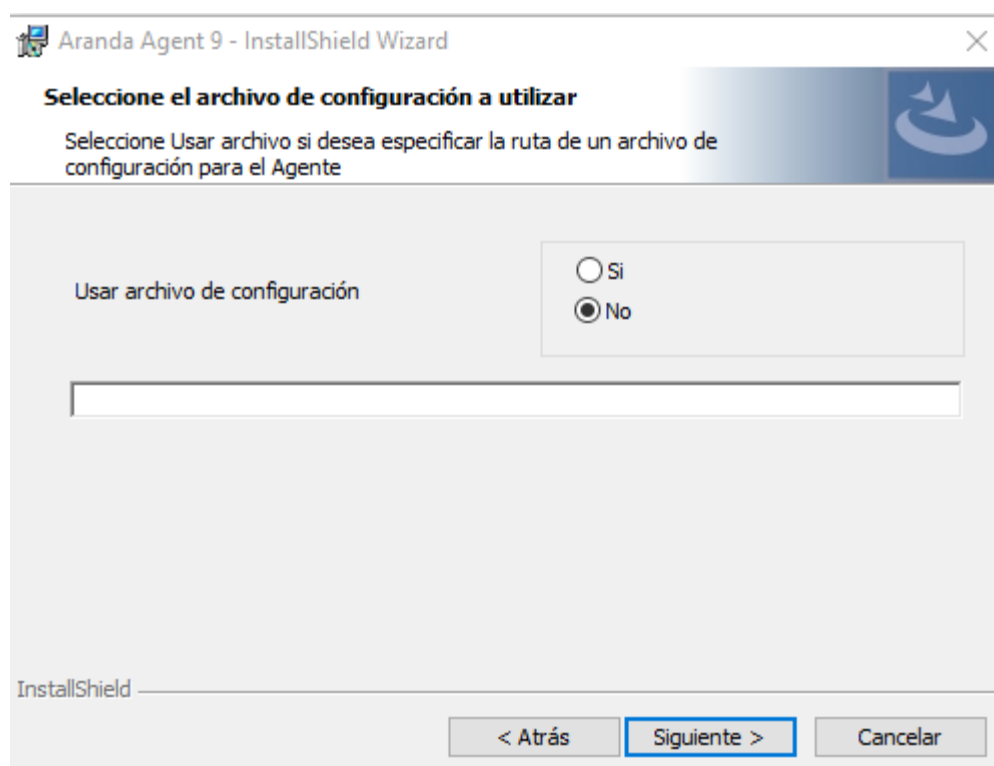
📌 **Nota:** O agente pode ser instalado de forma autônoma e automática por meio do [Distribuição de agentes](#) ou manualmente.

Instalação manual do agente

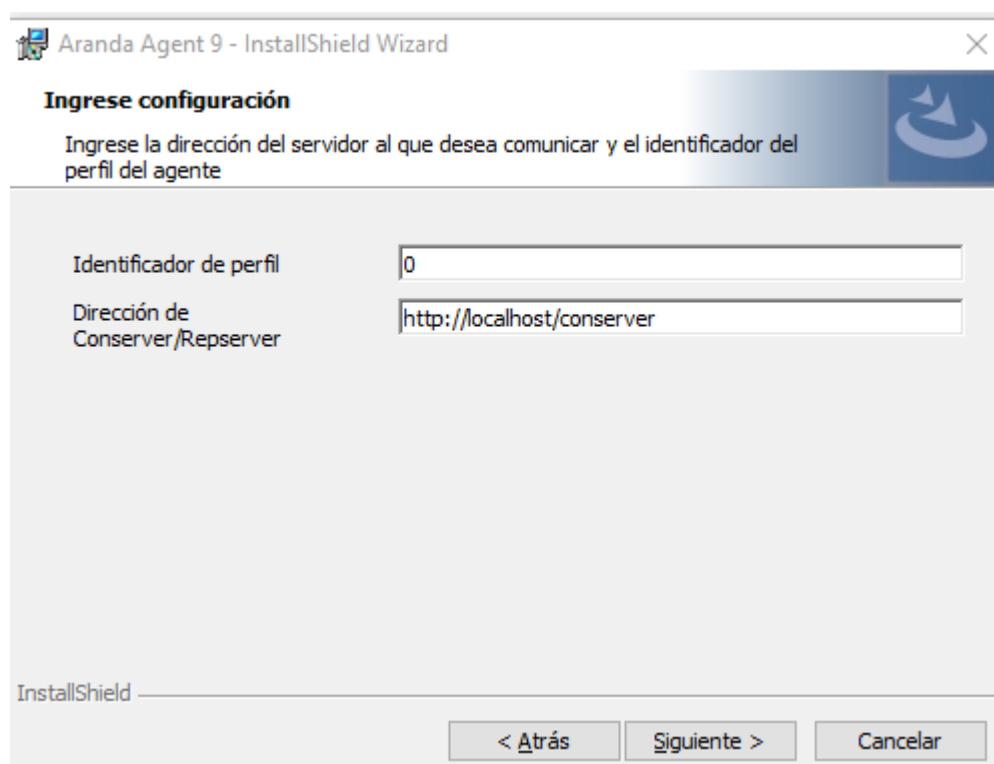
1. Clique no instalador do Aranda Agent. O assistente será iniciado. Clique **Seguinte**.



2. Se você tiver um arquivo de configuração, selecione Sim e insira o caminho, caso contrário, selecione Não e clique em Seguinte.



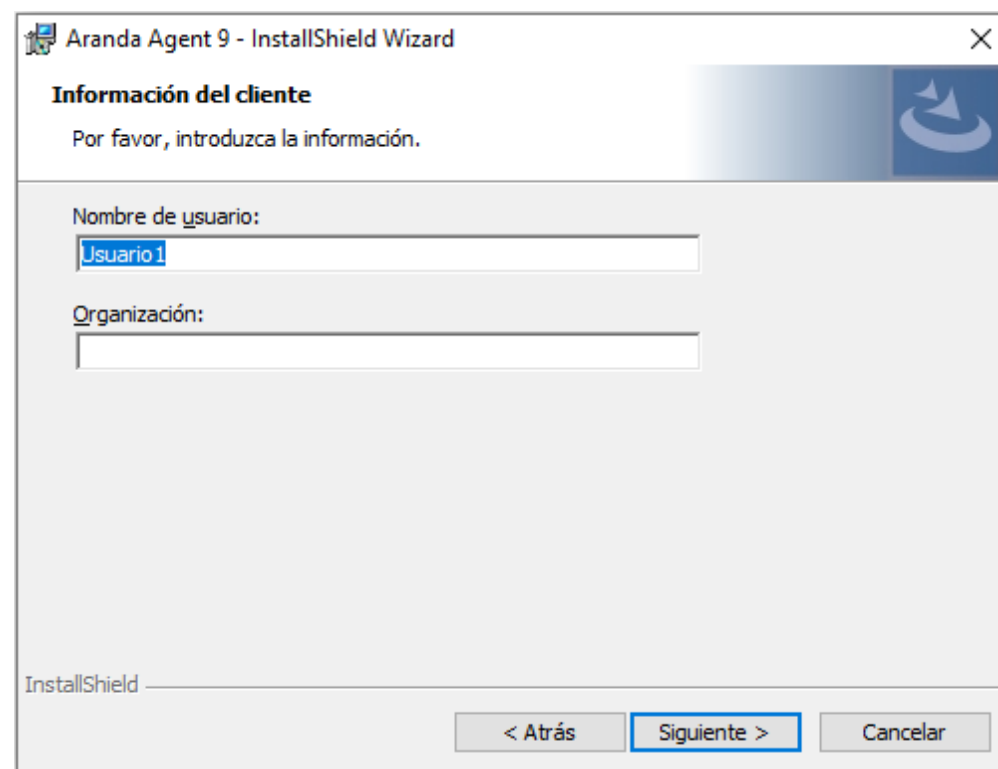
3. Insira o identificador de perfil, inserir 0 baixa o perfil configurado por padrão. Insira o endereço de Conserver ou Repserver de acordo com o apontamento configurado no broker MQTT [Configuração do Broker MQTT](#). Ao entrar no console ADM, você pode obter a rota de comunicação. Configuração > ADM > Comunicações



📌 **Nota:** Endereçamento do agente quando o repserver só funciona com uma versão do agente desde a

9.13.

4. Insira o nome de usuário e a organização em que o agente será instalado.



Aranda Agent 9 - InstallShield Wizard

Información del cliente
Por favor, introduzca la información.

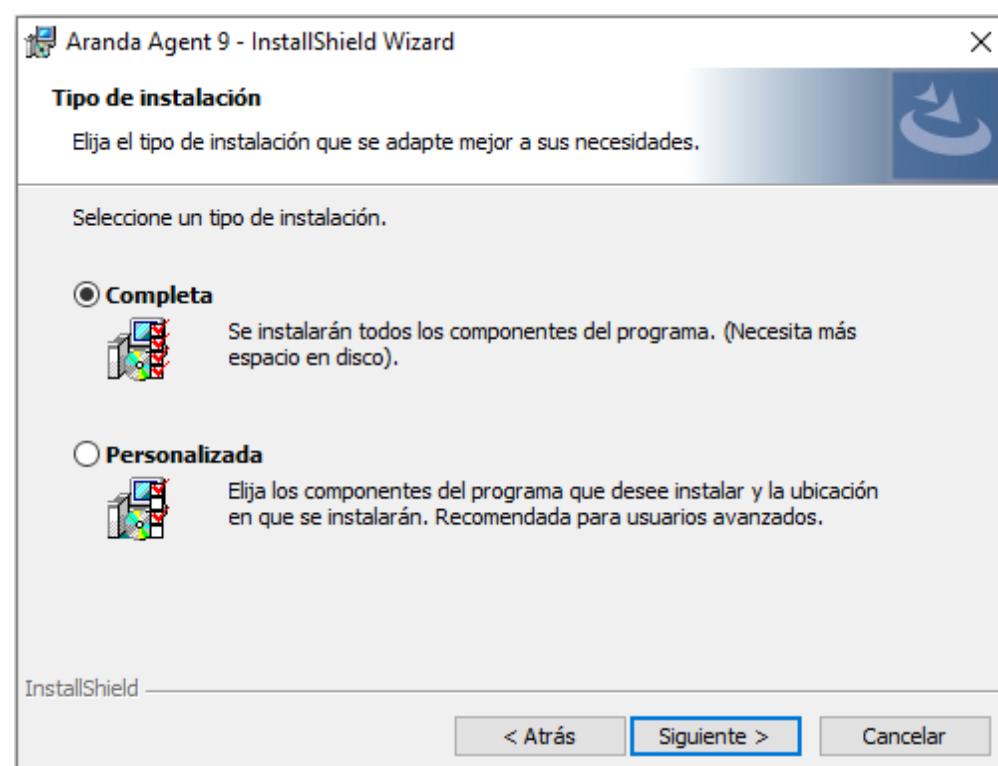
Nombre de usuario:

Organización:

InstallShield

< Atrás **Siguiente >** Cancelar

5. Seleccione o tipo de instalação que deseja executar (completo ou personalizado)) e clique em Seguinte.



Aranda Agent 9 - InstallShield Wizard

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

Seleccione un tipo de instalación.

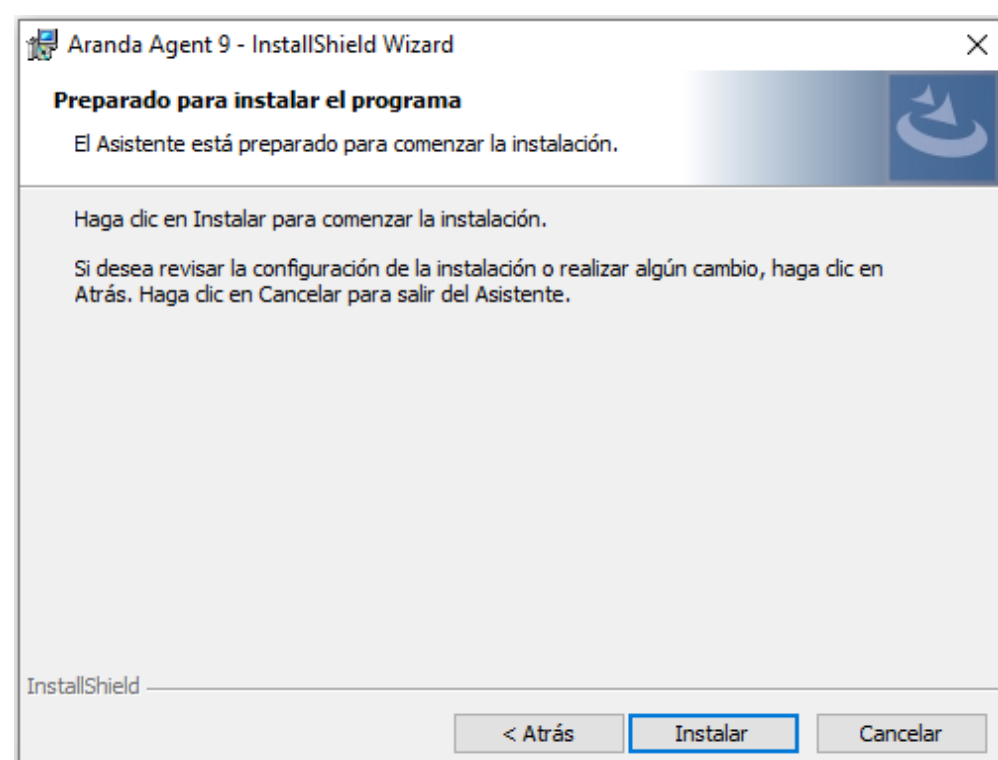
☒ **Completa**
 Se instalarán todos los componentes del programa. (Necesita más espacio en disco).

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

InstallShield

< Atrás **Siguiente >** Cancelar

6. Clique Instalar para iniciar a instalação do agente.



Aranda Agent 9 - InstallShield Wizard

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

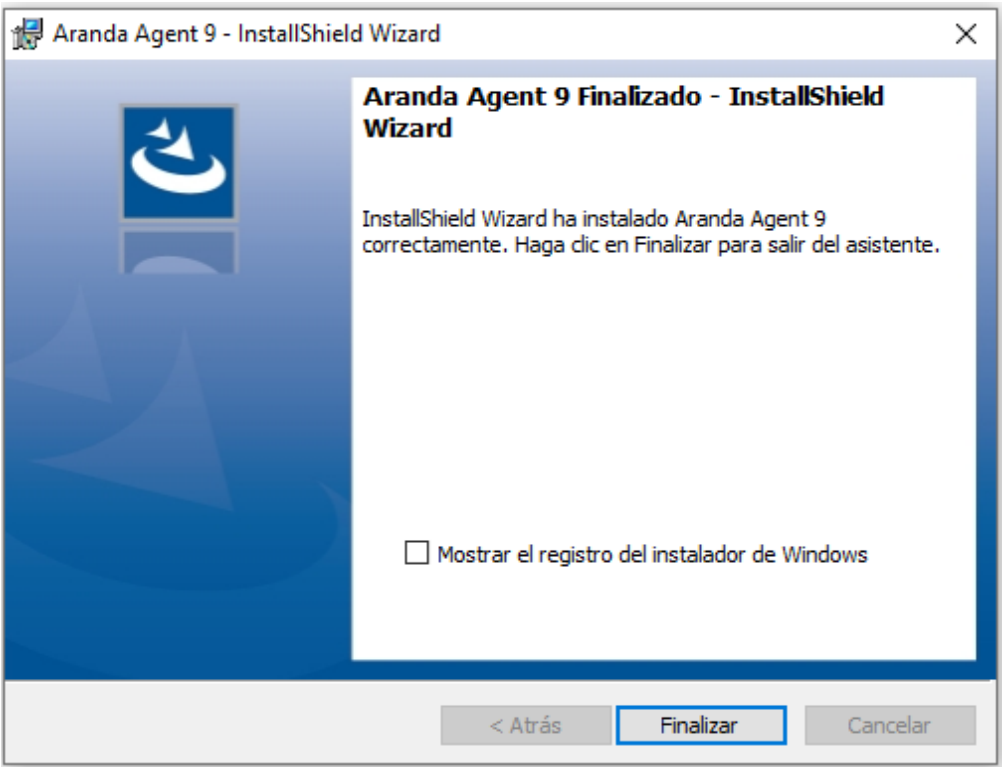
Haga clic en Instalar para comenzar la instalación.

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

InstallShield

< Atrás **Instalar** Cancelar

7. Quando a instalação do agente estiver concluída, clique em Fim



—

Instalação manual do agente por linha de comando

Para instalar o ADM Agent por linha de comando, você pode executar a seguinte instrução a partir do *comando prompt* do Windows:

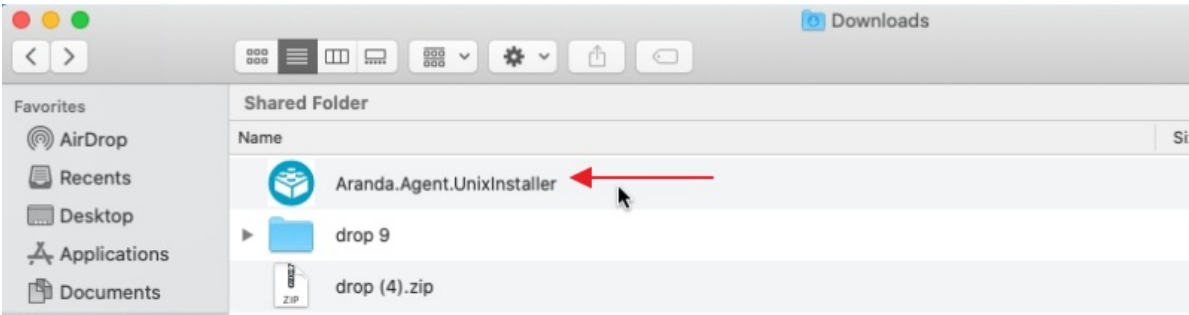
```
Aranda.Agent.Windows.x86_x64.9.xx.xxxx.xxxx.exe /S /V"/norestart /qn
AGENT_SERVER_ADDRESS=http://localhost/Conserver AGENT_PROFILE_ID=0"
```

AGENT_PROFILE_ID=[UNIT]	Identificador do perfil a ser instalado, 0 é um perfil selecionado no aplicativo como o perfil padrão.
AGENT_SERVER_ADDRESS=[STRING]	Caminho do servidor.

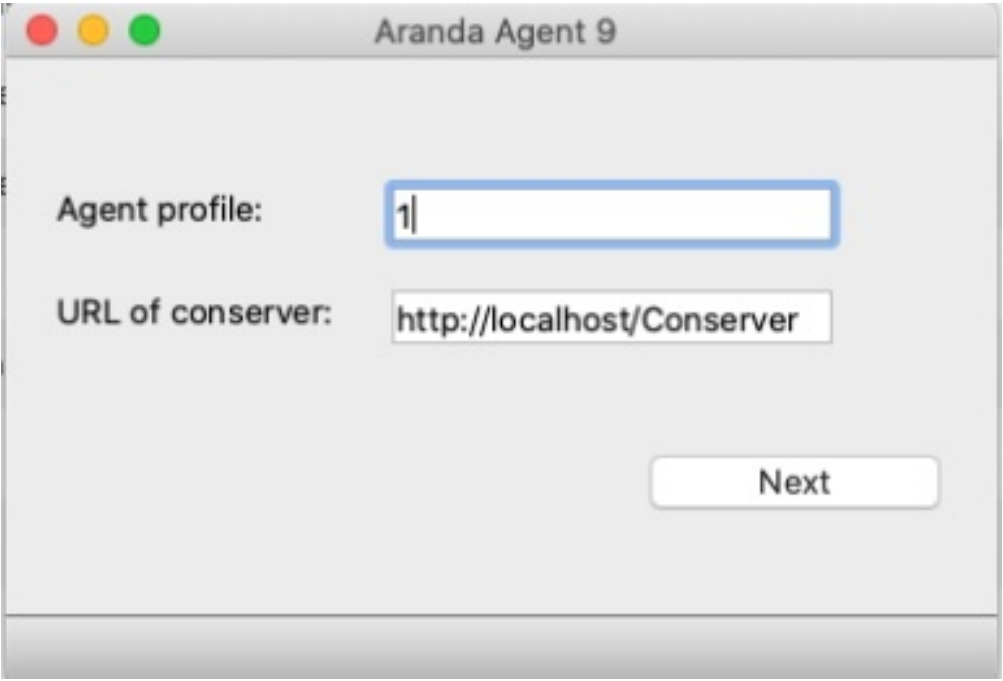
Instalador/Agente ADM no MacOS

Instalando o agente a partir da interface do usuário

1. Execute o aplicativo do agente.

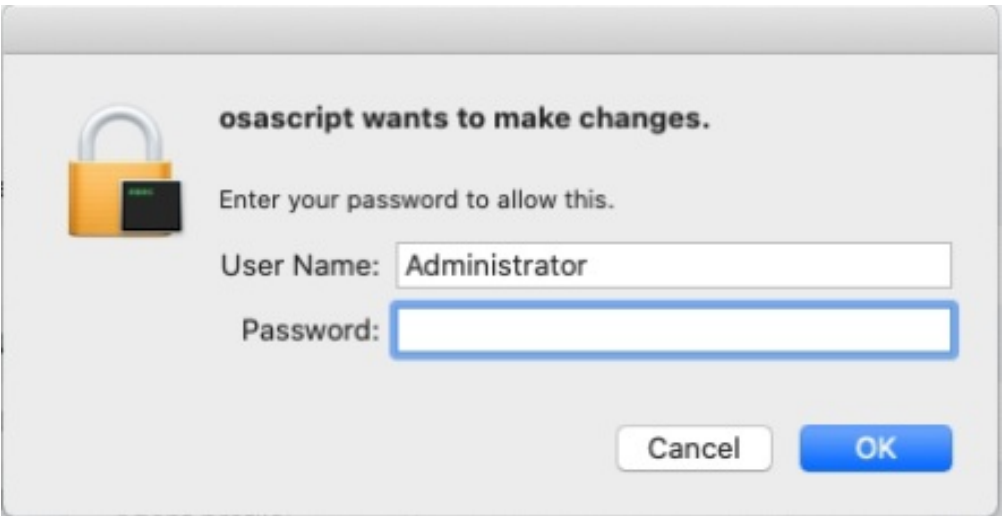


2. Insira o identificador do perfil, digitar 0 baixa o perfil configurado por padrão. Registre o endereço do Conserver ou do Repserver de acordo com o apontamento configurado no broker MQTT [Configuração do Broker MQTT](#). Ao entrar no console ADM, você poderá obter o caminho de comunicação. Configuração > ADM > Comunicações



⚠ **Nota:** Endereçamento do agente quando o repserver só funciona com uma versão do agente desde a 9.13.

3. Insira as credenciais do dispositivo.



4. O agente será instalado e uma mensagem de sucesso será exibida.



5. Quando a instalação estiver concluída, você poderá visualizar o dispositivo no console do ADM.

⚠ **Nota:** Se você já tiver um agente instalado, poderá ver as seguintes mensagens.

Mensagem	Descrição
A versão a ser instalada é a mesma que a versão instalada	Este caso é usado para atualizar os dados no conservador.
A versão a ser instalada é inferior à versão instalada	Nesse caso, a instalação do agente que está sendo instalado será impedida.

Instalando o agente a partir da linha de comando

1. Para instalar o agente Aranda DEVICE MANAGEMENT ADM via linha de comando, execute a seguinte instrução em um shell do MacOS:

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

Linha	Instrução
RUTA_INSTALLADOR	Caminho onde o instalador está localizado, pode ser relativo ou absoluto
AGENT_PROFILE_ID=[UNIDADE]	Identificador do perfil a ser instalado, 0 é um perfil selecionado no aplicativo como o perfil padrão
AGENT_SERVER_ADDRESS=[SEQUÊNCIA]	Caminho do conservador ou do servidor de representação

2. Depois de instalar o agente, uma pasta chamada Aranda é criada no caminho `/opt/local` com as bibliotecas, os serviços do agente e outra pasta em `/etc/` com o nome Aranda, onde os logs e o banco de dados do agente são armazenados. A exclusão dessas pastas desinstalará o agente.

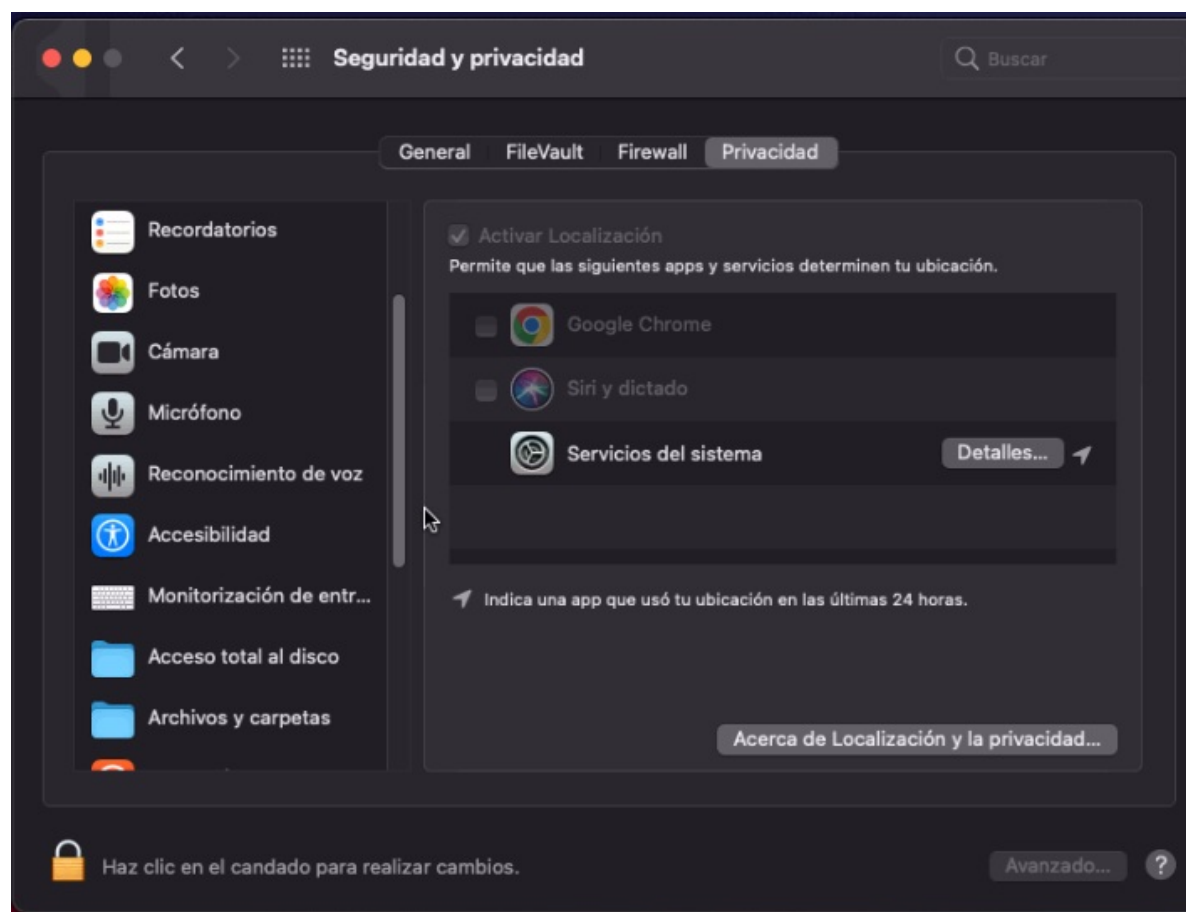
Conceder permissões de agente

A permissão de acesso total ao disco deve ser concedida ao agente, esta ação é executada levando em consideração as seguintes etapas:

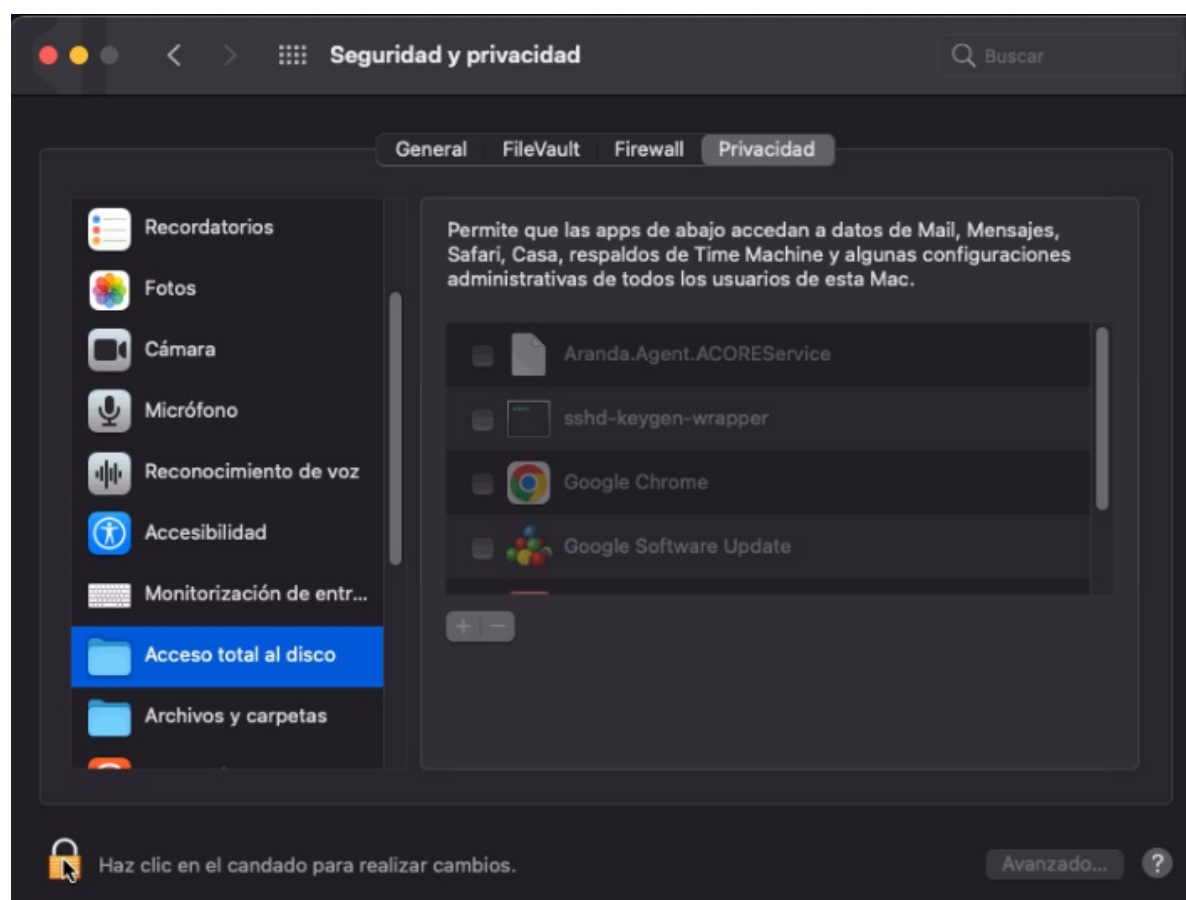
1. Abrir Preferências do Sistema > Segurança e Privacidade.



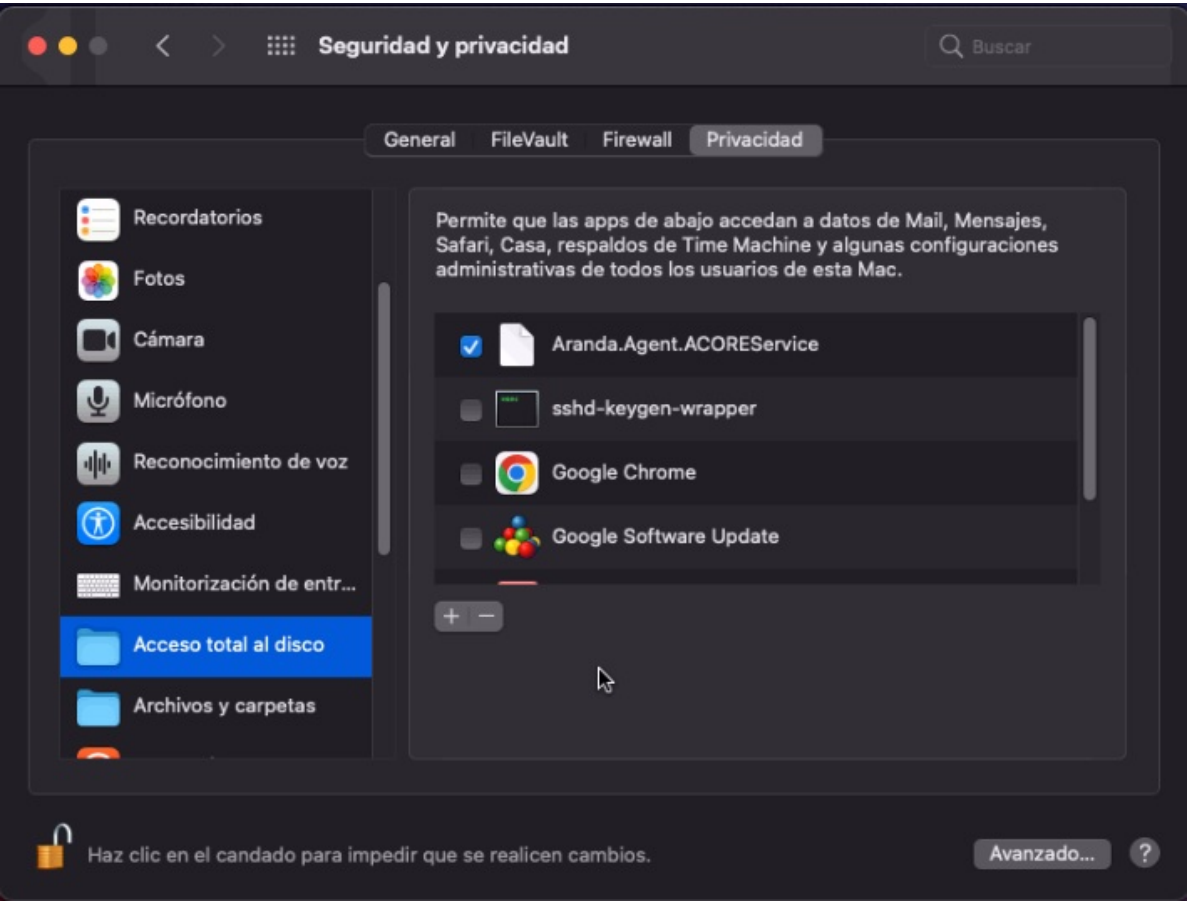
2. Selecione o ícone Privacidade.



3. Seleccionar Acceso total al disco e clique no ícone de cadeado. Insira as credenciais de administrador do sistema e clique em Desbloquear.



4. Seleccione Serviço Aranda.Agent.ACOREService e clique no ícone de cadeado.



—

Exceções de agente no macOS

As funcionalidades atualmente suportadas no MAC são asGestor de Ativos Aranda exceto para as seguintes funcionalidades.

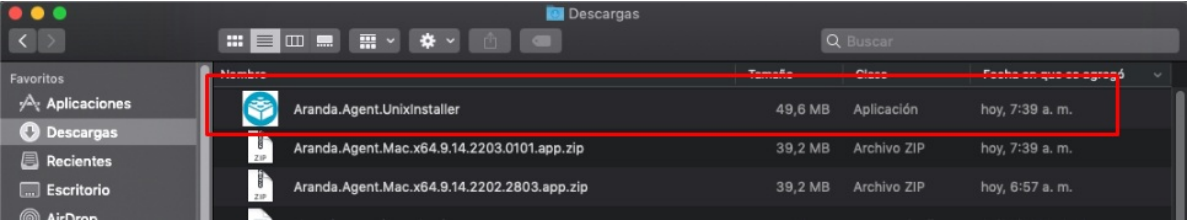
- Localização do dispositivo
- Excluindo arquivos por extensão
- Virtualização
- Monitorização
- Enviando mensagens
- Envio de comandos (permitido apenas com o usuário atual do sistema)

Modificação do agente

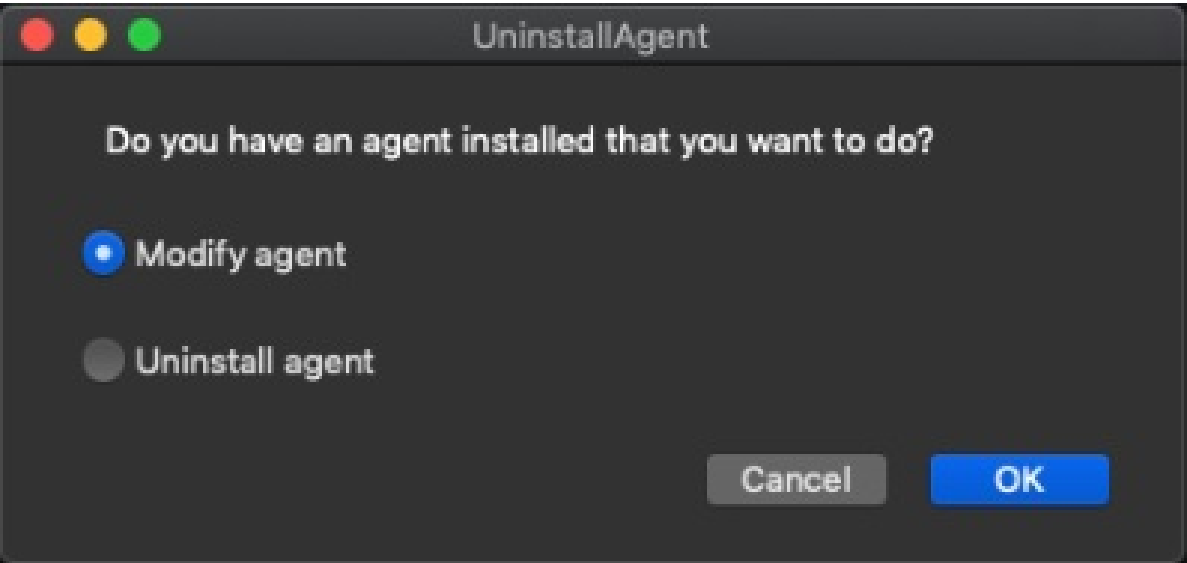
📌 **Nota:** Disponível na versão do agente superior a 9.14,
Se você tiver um agente instalado antes disso, a janela de desinstalação não será exibida.

Modificação do agente (host repserver ou conservador e perfil)

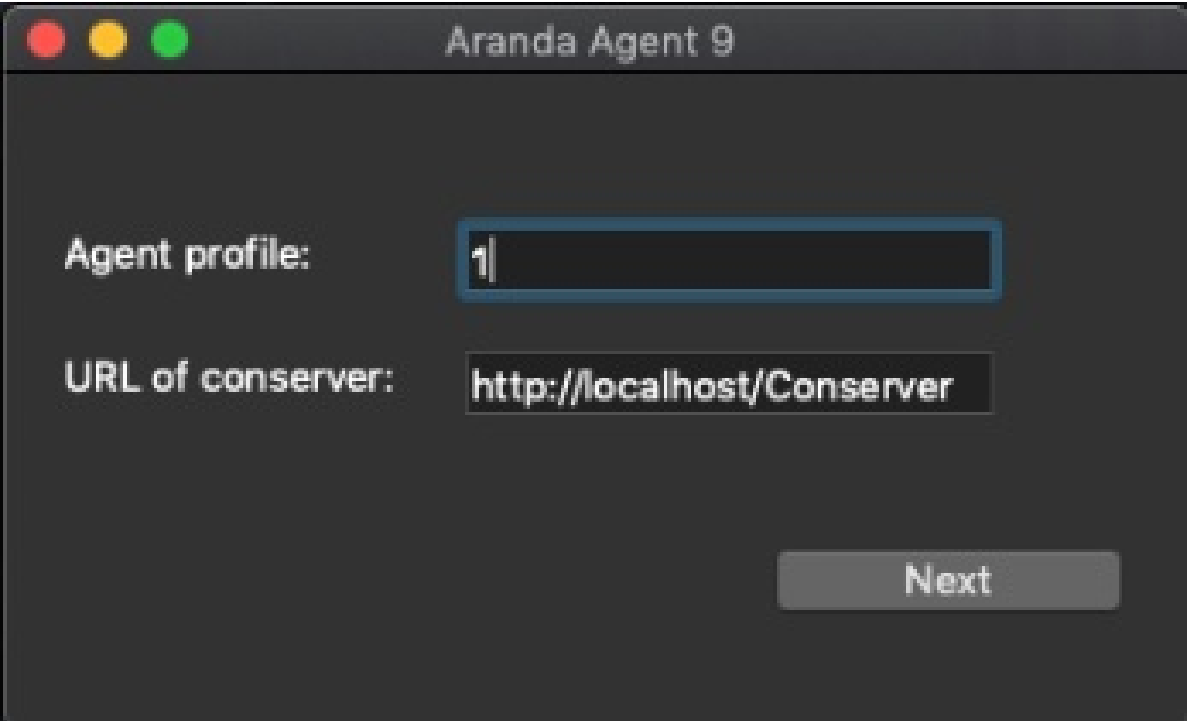
1. Para modificar o agente, você pode fazê-lo a partir do instalador Aranda.Agent.Unixinstaller.app



2. Dobrar clique no executável e a janela a seguir está habilitada.



3. Por padrão, a opção de Modificar agente é selecionado; Clique OKEY e a janela de instalação está ativada. Após a atualização, clique em Próximo.



—

Desinstalando o Agente

Para desinstalar o agente, você terá duas opções:

- Por [Linha de comando](#) usando o terminal.
- Usando o [interface gráfica](#).

Linha de comando

1. Abra uma janela de terminal e no caminho definido use o seguinte comando:

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

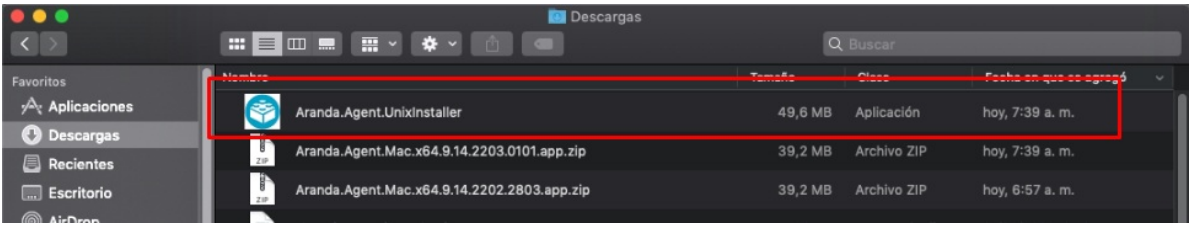
2. Assim que a pasta for inserida Aranda Executamos o seguinte comando.

```
sudo sh UninstallAgent.sh
```

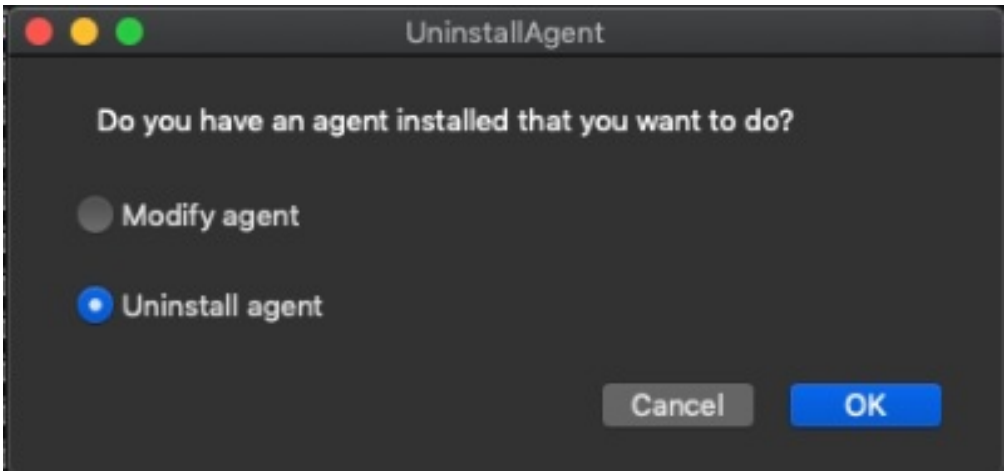
3. Depois que o comando for executado, você poderá ver que o agente foi desinstalado com êxito.

Interface gráfica

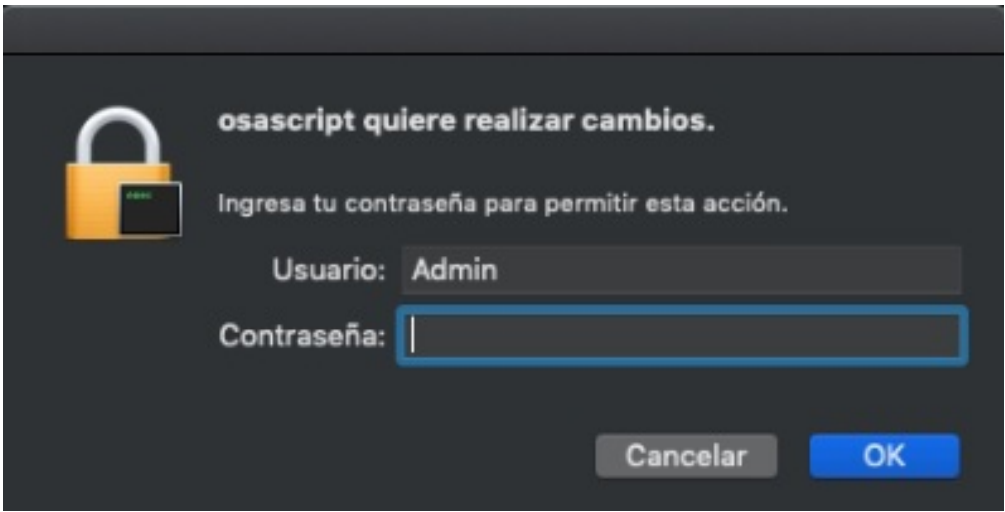
1. Execute o instalador Aranda.Agent.Unixinstaller.app.



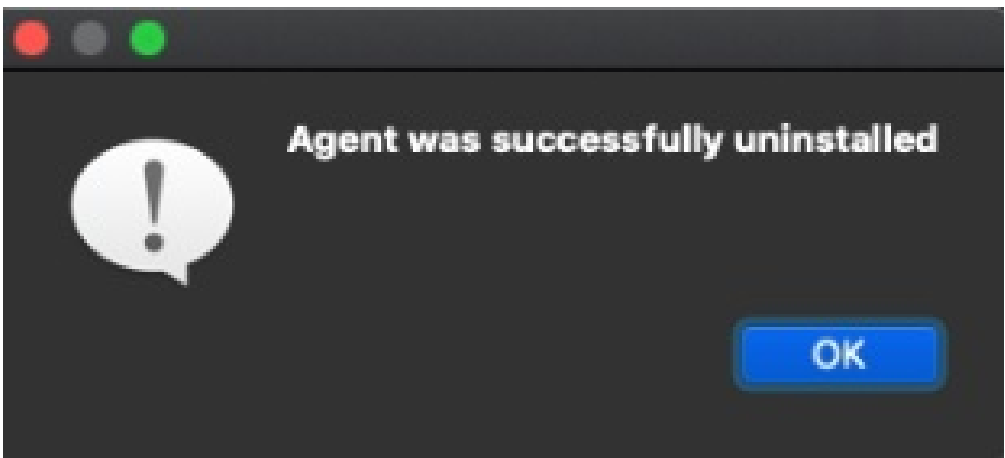
2. Na janela Desinstalar Agente, selecione o ícone Desinstalar agente e clique em OKEY



3. A próxima janela solicita as credenciais do administrador do computador; Digite a senha e clique em OKEY



4.Aguarde alguns segundos para que a desinstalação seja concluída e uma mensagem de confirmação seja ativada



Instalador/Agente ADM do Linux

Instalando manualmente o Command-Line Agent no Linux

1. Para executar a instalação do Aranda DEVICE MANAGEMENT ADM Agent por linha de comando, a instrução a seguir pode ser executada a partir de um shell Linux ou macOS.

Insira o endereço Conserver ou Repserver, dependendo da configuração do broker MQTT [Configuração do Broker MQTT](#). Ao entrar no console ADM, você pode obter a rota de comunicação [Configuração > ADM > Comunicações](#).


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

Donde:

Linha	Descrição
ROTA_INSTALLADOR	Caminho onde o instalador está localizado, pode ser relativo ou absoluto.
AGENTE_PERFIL_ID=[UNIDADE]	Identificador do perfil a ser instalado, 0 é um perfil selecionado no aplicativo como o perfil padrão
AGENTE_SERVIDOR_ADDRESS=[SEQUÊNCIA]	Caminho Conserver ou Repserver.

📌 **Nota:** Endereçamento do agente quando o repserver só funciona com uma versão do agente desde a 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.

Exceções de agente no Linux

O módulo é suportado atualmente Gestor de Ativos Aranda Espero as seguintes funcionalidades:

- Localização do dispositivo
- Virtualização
- Monitorização
- Enviando mensagens
- Envio de comandos (permitido apenas com o usuário atual do sistema)

Desinstalação manual do Command Line Agent no Linux

📌 **Nota:** Disponível na versão do agente superior a 9.14.

Você pode desinstalar o agente do Linux por meio da linha de comando seguindo estas etapas: 1. Abra uma janela de terminal e no caminho definido use o seguinte comando:

```
cd /opt/aranda
```

2. Depois de entrar na pasta *Aranda* Execute o comando a seguir.

```
sudo sh UninstallAgent.sh
```

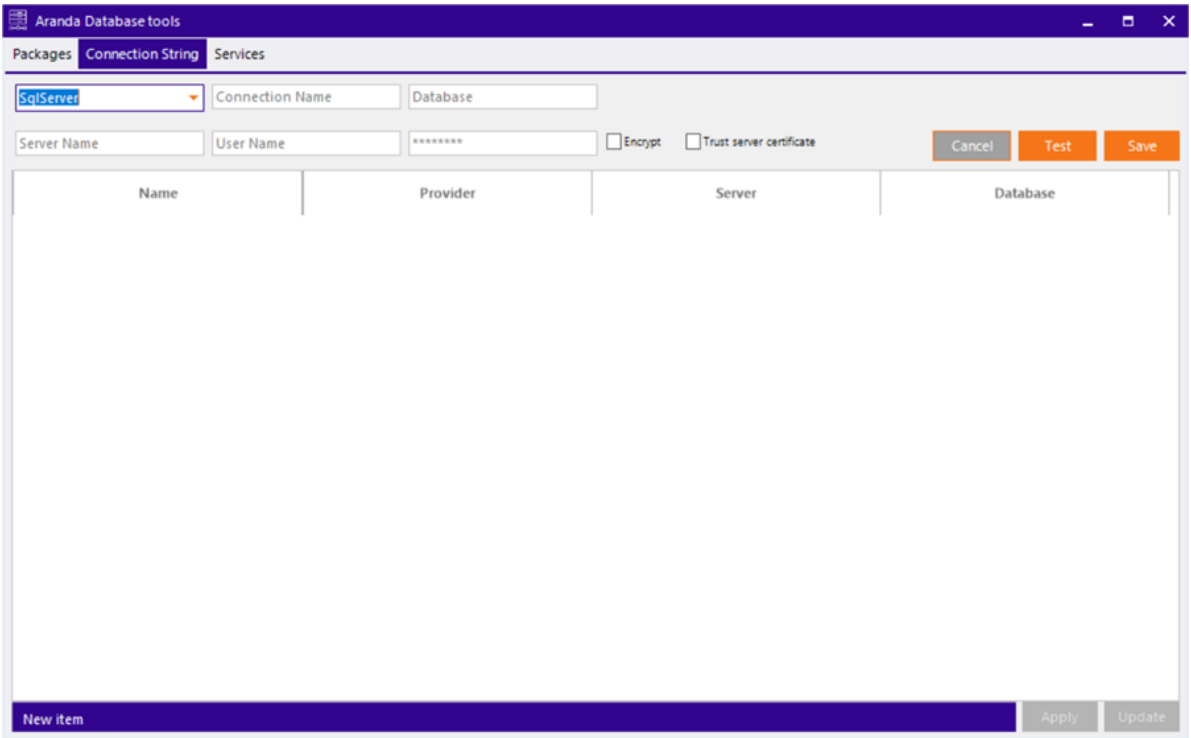
3. Depois que o comando for executado, você poderá ver que o agente foi desinstalado com sucesso.

Configuração de conexão de banco de dados

Uma vez que a instalação do Gerenciamento de dispositivos Aranda, prossiga para configurar as cadeias de conexão para o banco de dados dos sites e serviços.

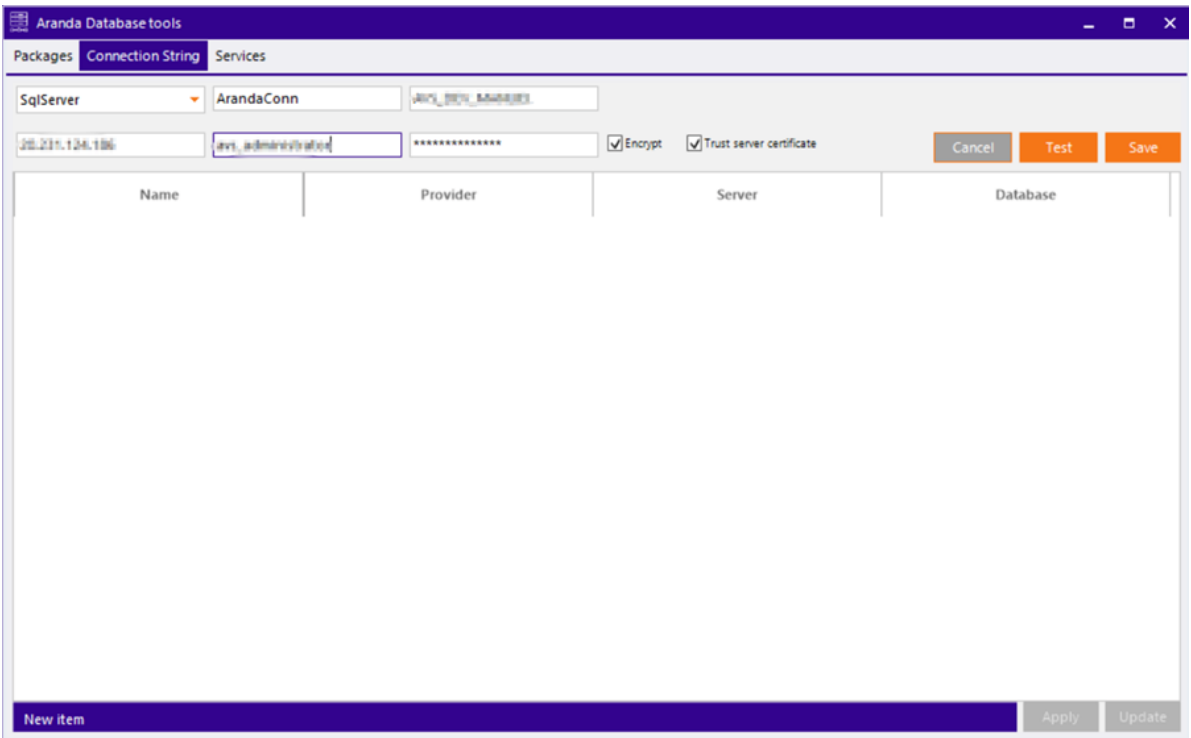
Para configurar os sites, serviços Comuns e de Licenciamento, é feito através do Ferramentas de banco de dados Aranda v9. Para fazer isso:

1. Execute o módulo e clique no botão Cadeia de conexão.

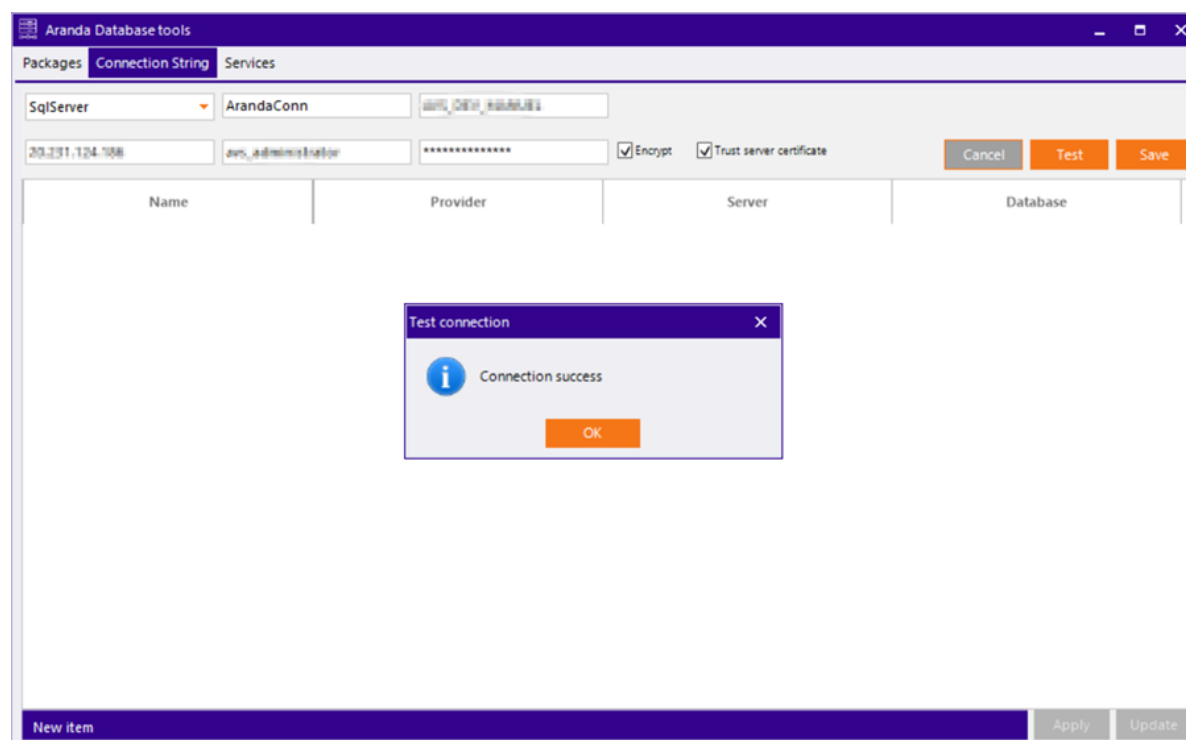


2. Preencha os dados solicitados.

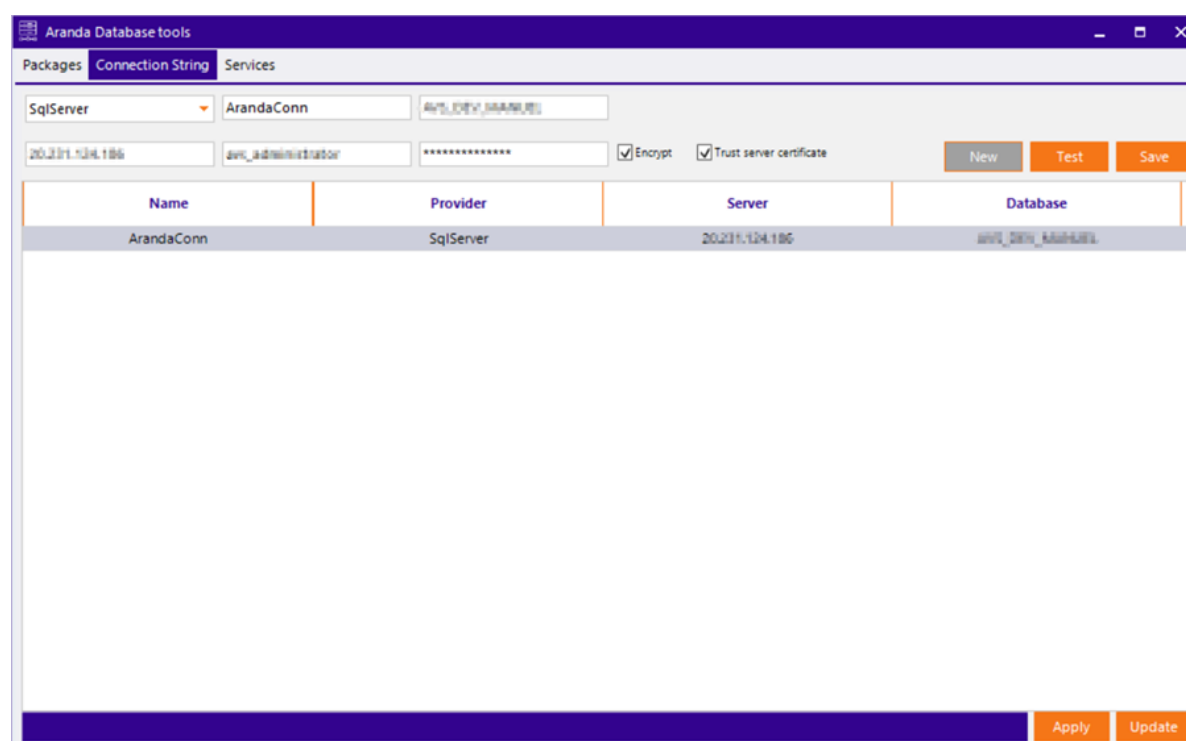
- Selecione o mecanismo de banco de dados (SQL Server).
- Dê um nome para identificar a conexão.
- Registre os dados de conexão (nome do banco de dados, nome do servidor ou endereço IP e, se necessário, nome de usuário e senha).
- Caso a porta do banco de dados seja diferente da porta padrão (1433 para SQL Server), o servidor deve ser escrito como servername:port (por exemplo, ARANDADBSERVER:5555)
- Por padrão, a opção “Criptografar” deve ser marcada para garantir que a conexão entre a solução e o banco de dados seja criptografada.



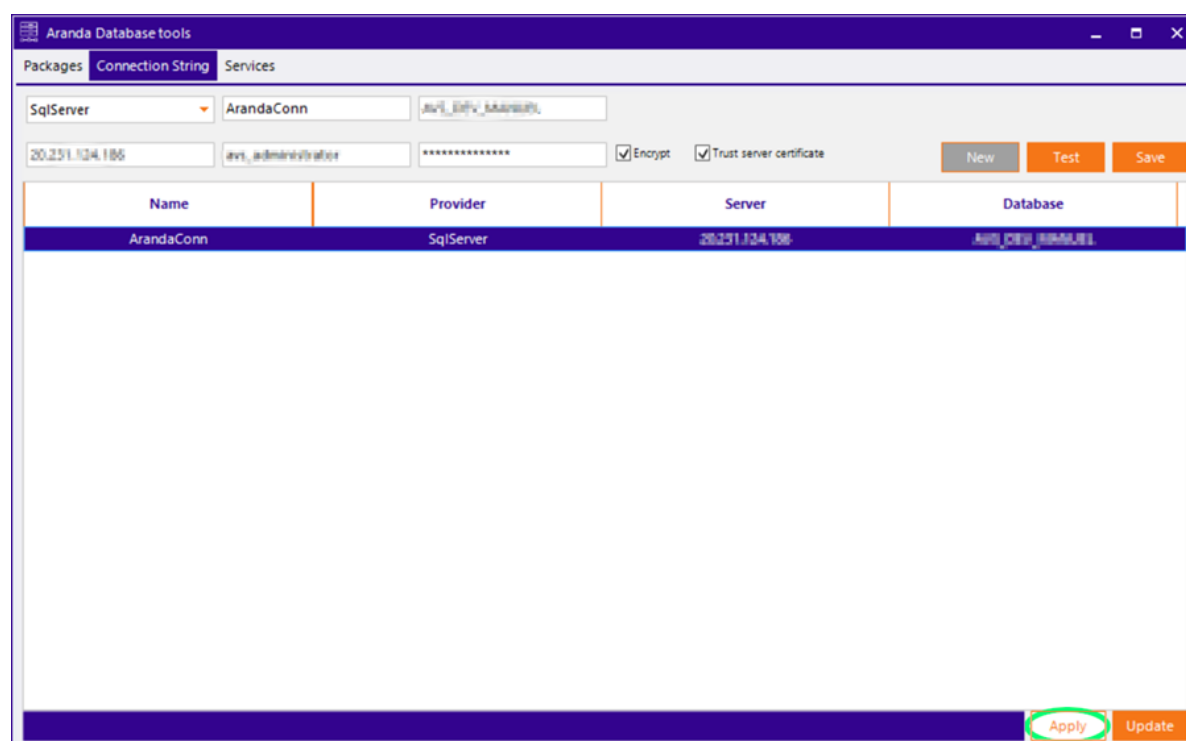
3. Clique no botão Teste para verificar a conexão.



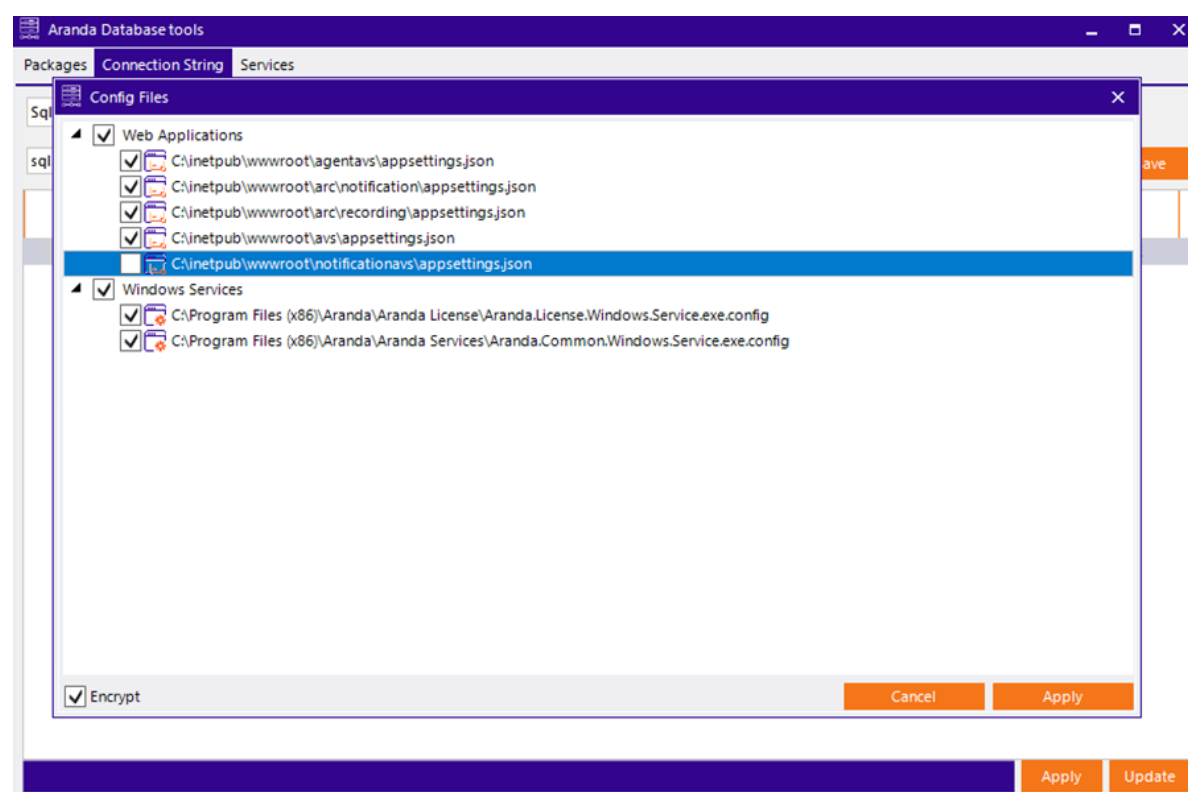
4. Para finalizar, clique no botão Salvar para salvar a conexão.



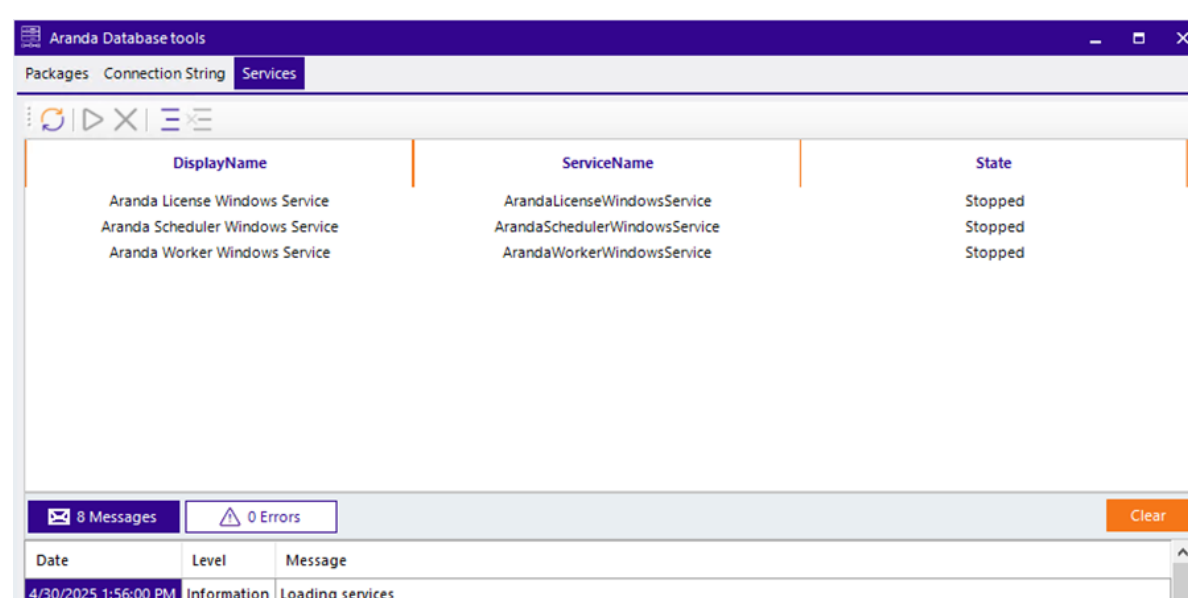
5. Para aplicar cadeias de conexão aos serviços instalados, selecione a conexão criada anteriormente e clique no botão Aplicar.



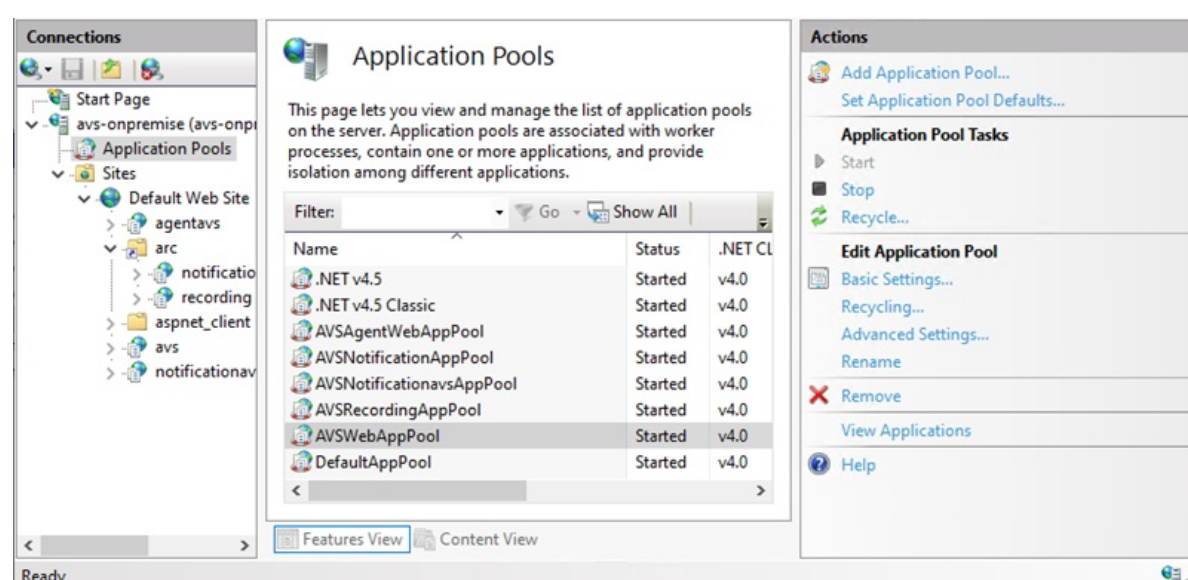
6. Uma janela é habilitada com a lista de aplicativos e serviços disponíveis no servidor. Para o site de notificaçãoADM Você não precisa aplicar as configurações da cadeia de conexão.



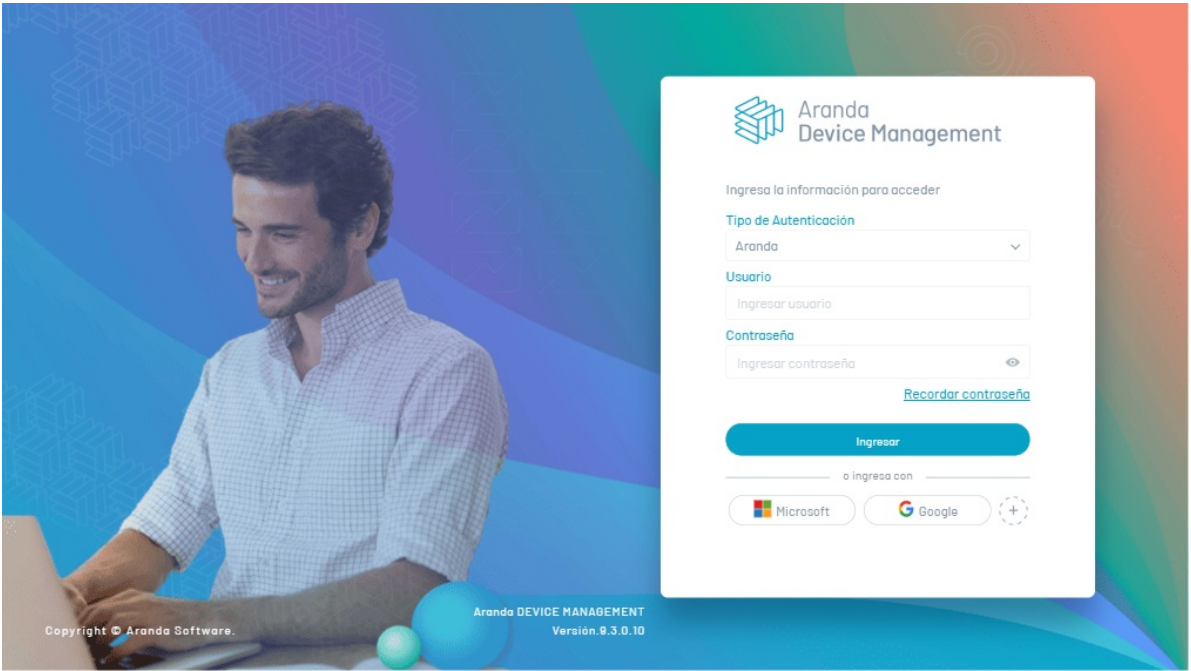
7. Selecione os serviços apropriados e clique no botão **Aplicar**. Se você quiser criptografar a conexão, marque a caixa **Criptografar** no canto inferior esquerdo. Uma mensagem de alerta pode ser exibida porque a criptografia não é suportada para arquivos JSON. 8. Para finalizar, clique no botão **Serviços** e iniciar todos os serviços.



✎ **Importante** Quando são feitas alterações nas cadeias de conexão dos sites, o pool de aplicativos associado ao site deve ser reiniciado ou reciclado para que a alteração seja aplicada imediatamente.



9. Uma vez estabelecida a conexão, você poderá acessar o site do ADM, onde poderá iniciar a configuração do Aranda Device Management através do seguinte URL: [http\(s\)://nome_servidor/adm/](http(s)://nome_servidor/adm/).

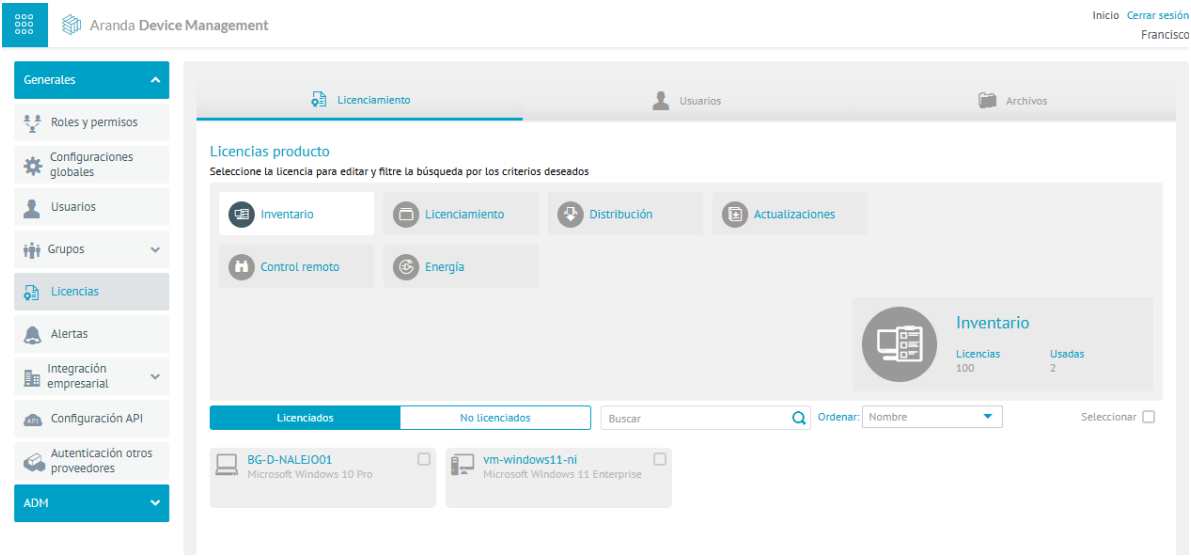


Licenciamento ADM

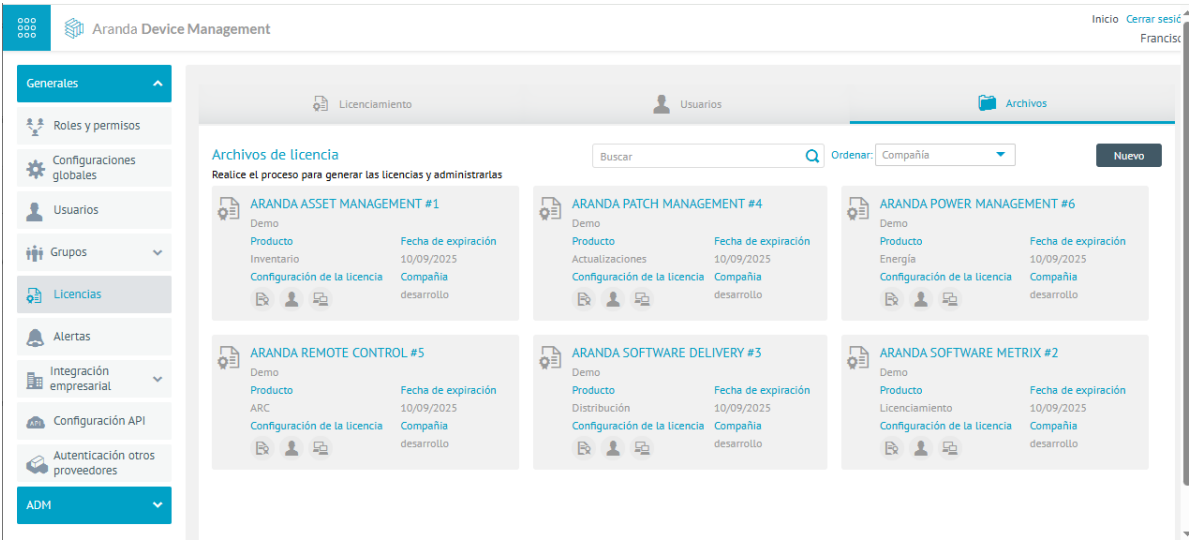
Todos os produtos da Aranda Software requerem uma licença para operar, por esse motivo, a ADM usa o serviço de licenciamento comum da Aranda para autorizar os usuários a entrar no console e controlar as licenças adquiridas, entre outras operações.

Carregar arquivo de licenciamento

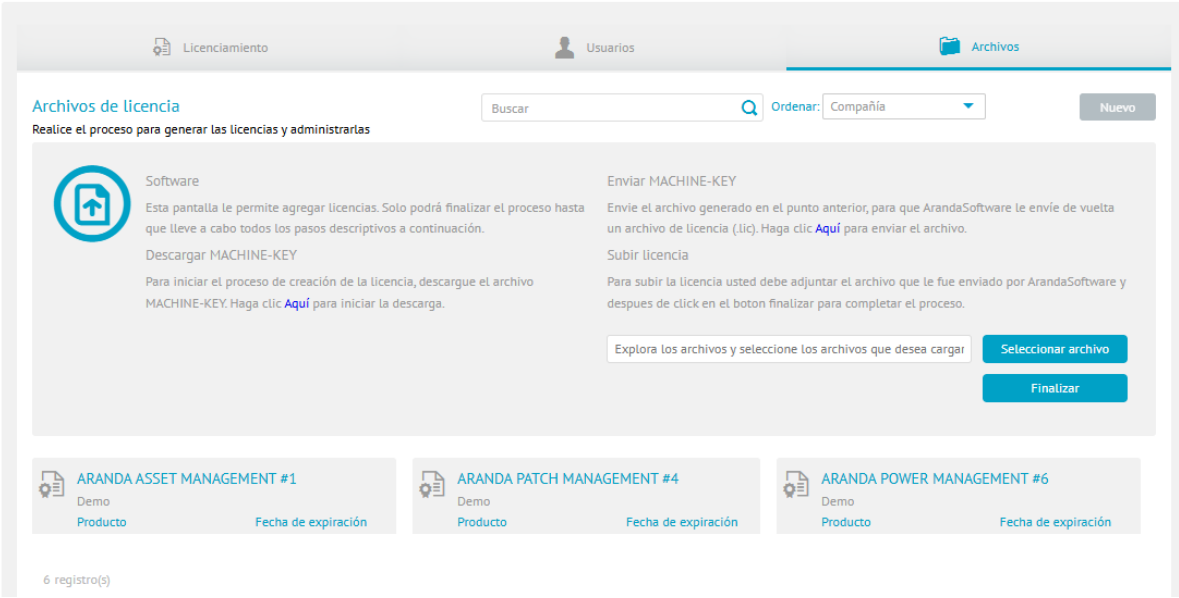
1. Para carregar o arquivo de licenciamento, na primeira vez que você entrar no site do Aranda Device Management (ADM), vá para a visualização de configuração do console da Web do ADM, no Geral No menu principal, selecione o ícone **Certificados**. Na visualização de informações, você pode visualizar informações associadas ao licenciamento.



2. Na visualização de informações, selecione o **Arquivo** e clique no ícone **Novo**.



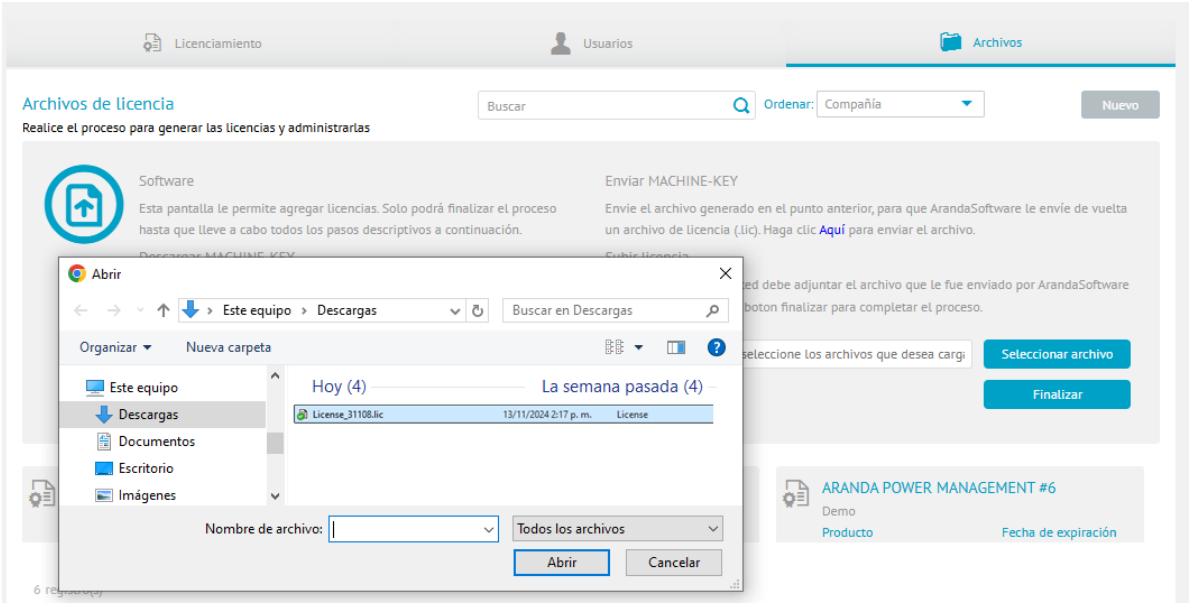
3. Na janela habilitada, selecione a opção **Baixar MACHINE-KEY**, clique no link **Aqui**, que permite o download do arquivo MachineKey.amk (arquivo de licenciamento), que deve ser enviado para a área responsável da Aranda Software (Pré-Vendas e Projetos) para a geração do arquivo .lic (arquivo de licenciamento).



⚠ **Aviso:** Depois que o usuário carrega suas licenças adquiridas do console, o serviço de licenciamento comum deve permanecer na mesma máquina, caso contrário, as licenças carregadas serão perdidas.

⚠ **Aviso:** Se o servidor de aplicativos estiver localizado em uma máquina virtual, é recomendável instalar o Common Licensing Service em uma máquina física, pois quando você reiniciar máquinas virtuais, há uma alta probabilidade de que a marca do hardware seja alterada e o serviço assuma incorretamente que ele foi movido.

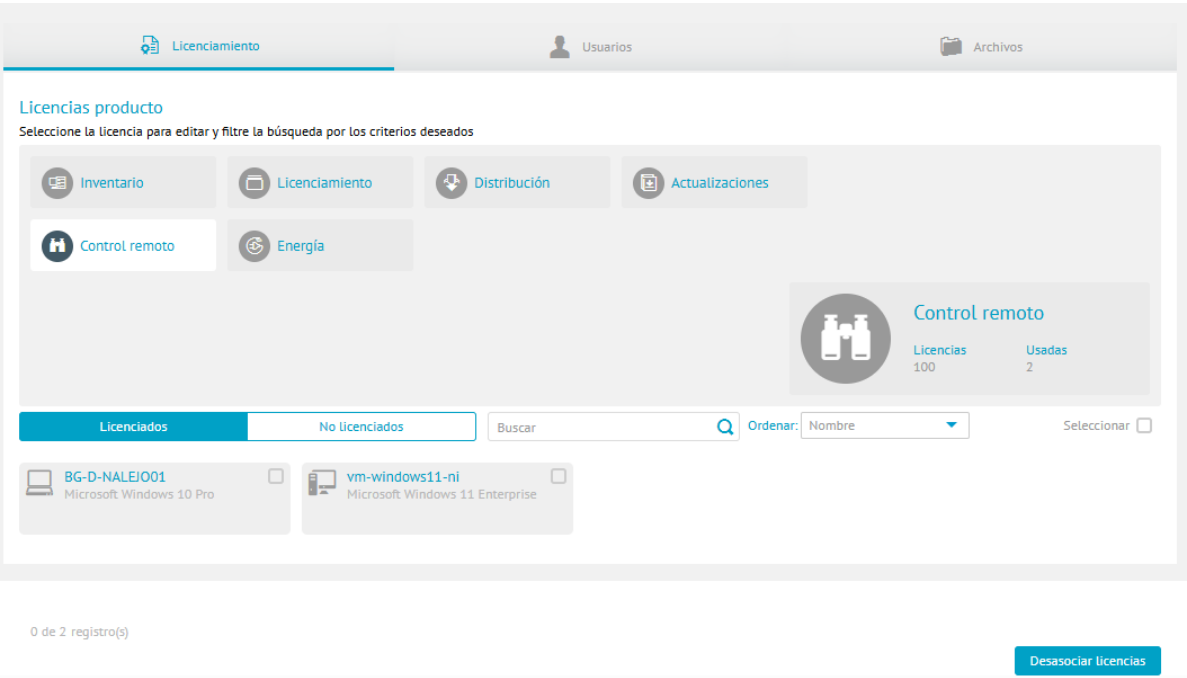
4. Depois de receber o arquivo .lic (arquivo de licenciamento), você precisa carregá-lo no servidor, clicar no botão **Selecione o arquivo** e depois em **Fim**.



Exibir/associar dispositivos licenciados

5. Para exibir os detalhes da licença e os dispositivos licenciados, na exibição Informações de licenciamento, selecione o botão **Licenciamento** e a licença pelo módulo de gerenciamento ADM (Inventário, Licenciamento, Distribuição, Atualizações, Controle Remoto e Energia). As opções **Licenciado** e **Não licenciado** agrupam os dispositivos encontrados.

6. Ao selecionar um ou mais dispositivos, você pode selecionar o respectivo botão para **Licenças de associado** ou **Desassociar licenças** para os dispositivos escolhidos.

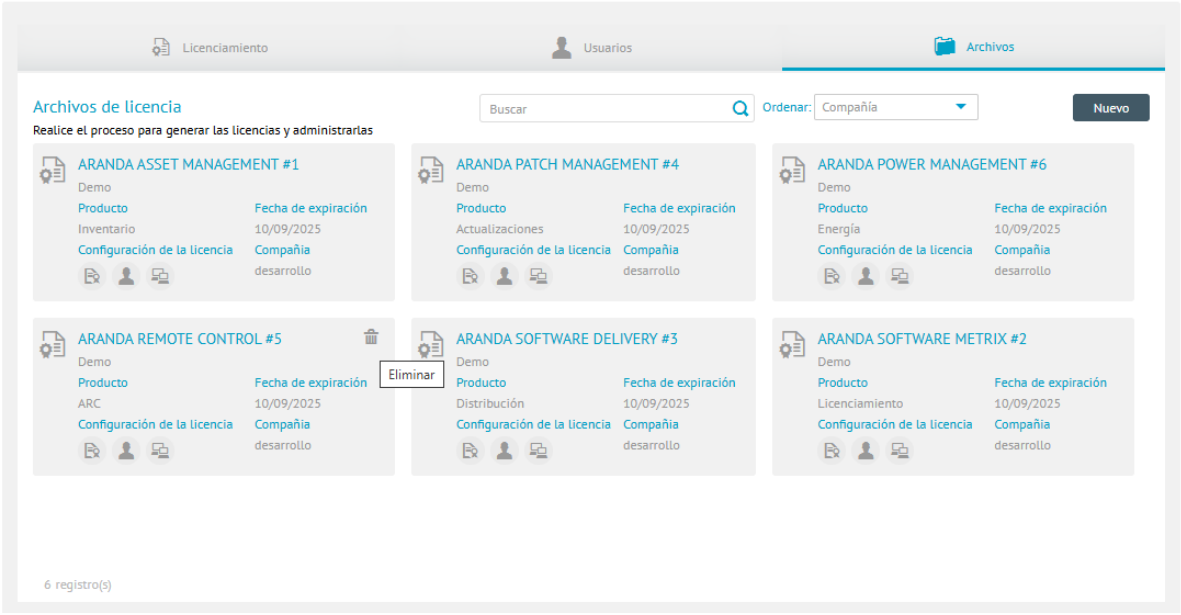


Excluir licenças

7. Para excluir uma licença, na exibição Informações de licenças, selecione o botão **Arquivo** e o registro de uma licença. Clique no botão **Eliminar**



. Você poderá exibir uma mensagem confirmando a ação; quando você clicar em Aceitar, a licença será excluída.



Acesso ADM

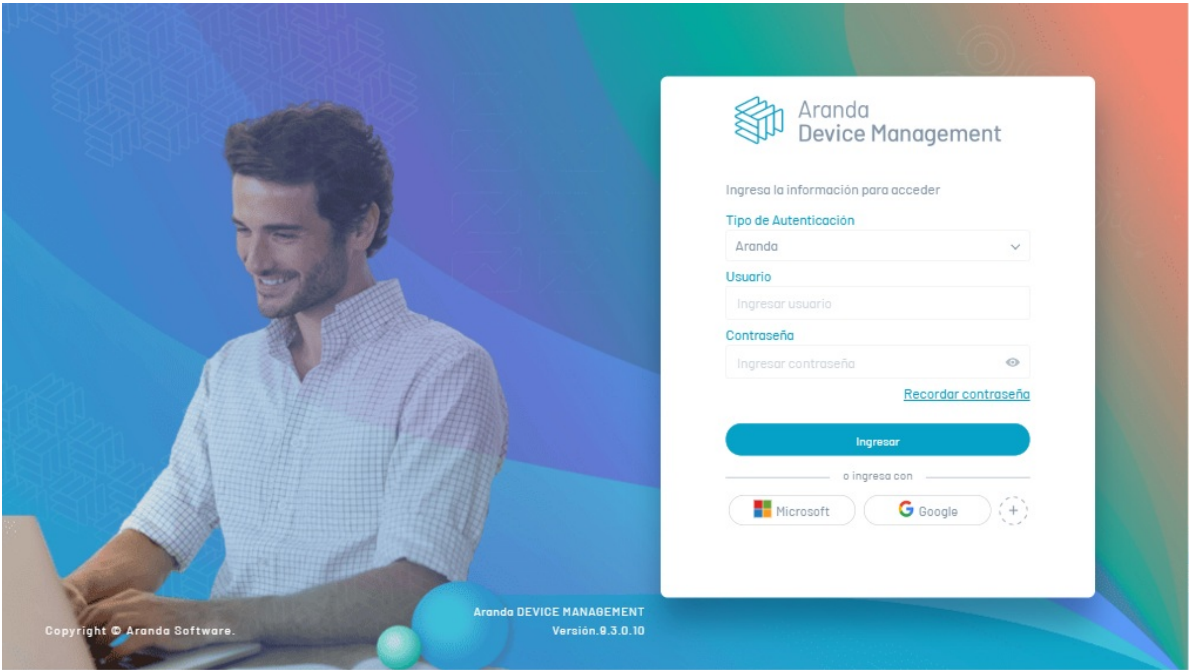
O processo de autenticação para o console web do ADM será executado de acordo com a função definida pela organização para desenvolver as diferentes tarefas de gerenciamento e configuração de dispositivos. As duas

instâncias de autenticação são:

Login

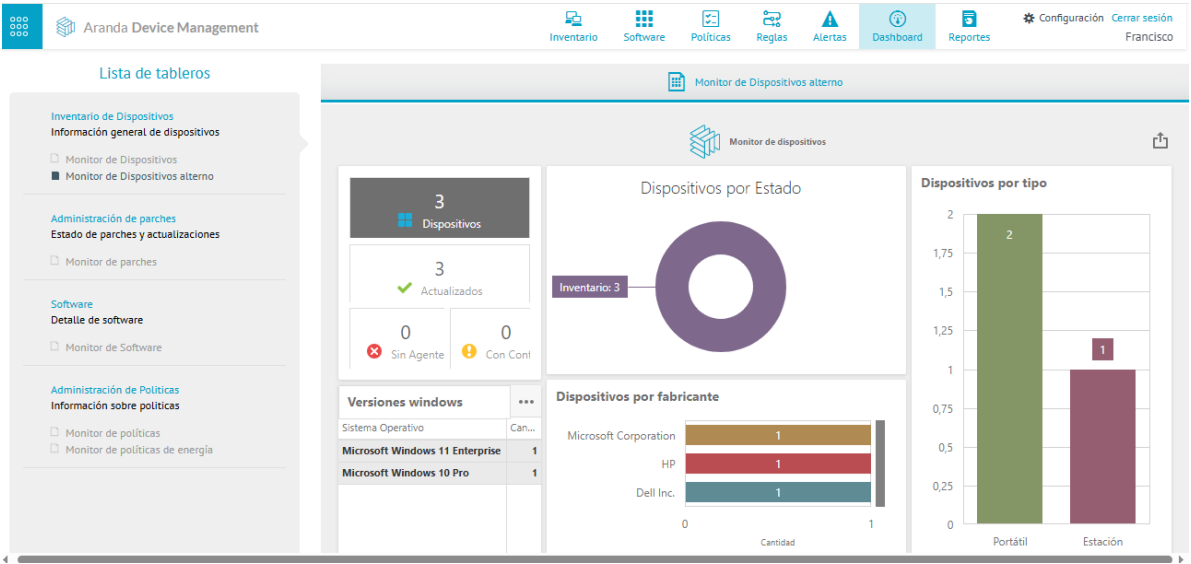
1. Insira o URL do console da Web do Aranda Device Management ADM.
2. Para fazer login no aplicativo ADM, digite o nome de usuário e a senha atribuídos a você.

➤ **Nota:** Para obter mais informações sobre o processo de autenticação dos produtos Aranda (campos e provedores de autenticação e senha esquecida), acesse o [Módulo de login comum de Aranda](#).



Saindo

1. Quando um usuário está em uma sessão ativa no console da Web e precisa encerrar a sessão e sair do aplicativo, no menu de cabeçalho do console, selecione o ícone do usuário e clique em **Fazer logoff**.



2. Depois que a sessão é fechada, o usuário retorna à tela inicial e pode entrar no console novamente.

Atualização

Atualização do ADM

Nos processos de atualização do ADM, após a instalação, você deve levar em consideração os seguintes componentes a serem atualizados:

- Atualização do ADM Console.
- Atualização do agente ADM.
- Atualização manual do servidor.
- Atualizando o projeto de servidor por distribuição.
- Atualização do visualizador de suporte remoto.

➤ **Importante:** Para garantir que seu aplicativo esteja funcionando corretamente após uma atualização para a versão mais recente, atualize os seguintes componentes:

- Discovery Agent (a partir da versão 9.21.1, o Discovery Agent é atualizado automaticamente)

- Remote Support Viewer (Aranda ADM Utils) ou Remote Support Viewer (Aranda Virtual Support Specialist), dependendo da versão do controle remoto que você está usando.
- Agentes de dispositivo final (a partir da versão 9.21.2, os agentes do Windows são atualizados automaticamente)

📌 **Nota:** A versão mais recente lançada do Remote Support Viewer (Aranda ADM Utils) é 9.22.0. A partir da versão 9.22.1 do ADM, nenhuma nova versão do Aranda ADM Utils será lançada; no entanto, será garantido o correto funcionamento das versões futuras do ADM em conjunto com a versão Aranda ADM Utils 9.22.0.

Atualização do ADM Console

Antes de atualizar o console do ADM, você deve considerar as seguintes recomendações:

📌 **PASTAS PARA MOVER:** Durante a atualização, se existirem, as seguintes pastas e seu conteúdo devem ser movidos do repositório repserver

- %dir_Repserver%\Atualização do Agente
- %dir_Repserver%\Gravações

%dir_Repserver% refere-se ao caminho configurado para o **Repserver** padrão C:\Repserver\

Para o diretório configurado para o Content Manager.

A estrutura deve ser preservada como está, ou seja:

- %dir_ContentManager%\Atualização do Agente
- %dir_ContentManager%\Gravações

%dir_ContentManager% refere-se ao caminho configurado para o **Gerenciador de conteúdo** padrão C:\ContentManager\

📌 **IMPORTANTE:** Mantenha os nomes exatos das pastas (AgentUpdate e Recordings) para garantir a compatibilidade com os serviços do sistema. Guardar.

📌 **CONSEQUÊNCIAS DA OMISSÃO DA AÇÃO:** Se essas pastas não forem movidas:

- As gravações não serão exibidas corretamente nas auditorias.
- Ocorrerão inconsistências nos logs do sistema.
- Os agentes não poderão ser baixados corretamente.

Para atualizar o console do ADM, considere as seguintes instruções: 1. Gere um backup do banco de dados a ser atualizado.

2. Pare os seguintes serviços da Aranda manualmente ou usando as ferramentas do Aranda DataBase:

```
- 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 os programas Aranda Conserver Service e Aranda DEVICE MANAGEMENT do painel de controle.

4. Exclua os registros nas seguintes pastas:

```
- 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::** Não exclua o conteúdo dos repositórios Container, Repserver e Conserver.

1. Verifique os requisitos antes de executar o instalador Aranda.ADM.Web.Installer.exe. [Exibir a instalação do ADM Console](#)

2. Execute o instalador Aranda.Conserver.Installer.exe. Não carregue serviços até que o repserver e o.config da

pasta do conservador. [Ver Servidor de Instalação](#)

3. Execute o Aranda DataBase Tools para que todos os arquivos .config para apontar para o banco de dados migrado (consulte as etapas de execução no documento da base de conhecimento).
4. Carregue os serviços da Aranda, seja pelo aplicativo Aranda DataBase Tools ou pela lista de serviços:



5. Verifique a conexão repserver a partir do console da web.
6. Se você tiver o serviço Mosquitto MQTT, deverá desinstalá-lo [Ver instalação](#) na seção Desinstalar o Mosquitto MQTT Broker e, em seguida, execute o instalador do MQTT broker. [Instalação do Aranda MQTT Broker](#)
7. Configurar o arquivo Aranda.Conserver.Windows.Service.exe.config O que há na pasta %Arquivos de Programas(x86)%\Aranda\Conserver.
8. Inicie o serviço Conservador Aranda V9.
9. Verifique se todos os serviços Aranda estão em execução.

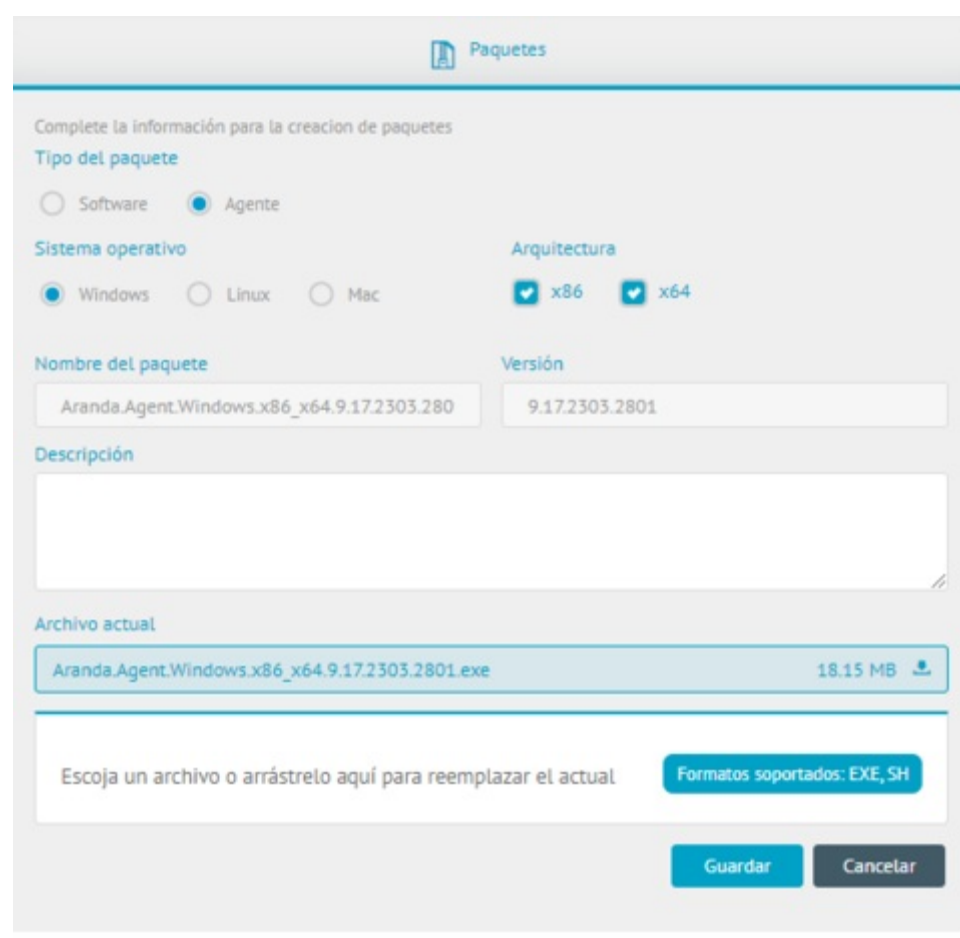
- 📌 **Nota:**
- Se for necessário desinstalar um produto Aranda diferente do ADM, será gerado um erro ao entrar no console do ADM e não será possível acessá-lo.
 - Para a instalação do console ADM e Conserver, o servidor deve ter a versão 4.8 do .NET framework (net48)
 - Lembre-se de atualizar o agente das diferentes máquinas para que eles possam acessar as alterações mais recentes; Para isso, recomendamos:

- Atualizar por política de domínio.
- Atualização por distribuição de agente (Conservador na rede do cliente).
- Atualização manual.

Atualização automática do agente

Pacote de agentes para Windows

1. O Agente do Windows com extensão .exe será carregado automaticamente no ADM Management Console, no Configuração do ADM No menu principal, opção Pacotes dentro de um dia após a atualização do site do ADM.



Paquetes

Complete la información para la creación de paquetes

Tipo del paquete

☐ Software ☒ Agente

Sistema operativo

☒ Windows ☐ Linux ☐ Mac

Arquitectura

☒ x86 ☒ x64

Nombre del paquete

Aranda.Agent.Windows.x86_x64.9.17.2303.280

Versión

9.17.2303.2801

Descripción

Archivo actual

Aranda.Agent.Windows.x86_x64.9.17.2303.2801.exe 18.15 MB

Escoja un archivo o arrástrelo aquí para reemplazar el actual

Formatos soportados: EXE, SH

Guardar Cancelar

Nota:

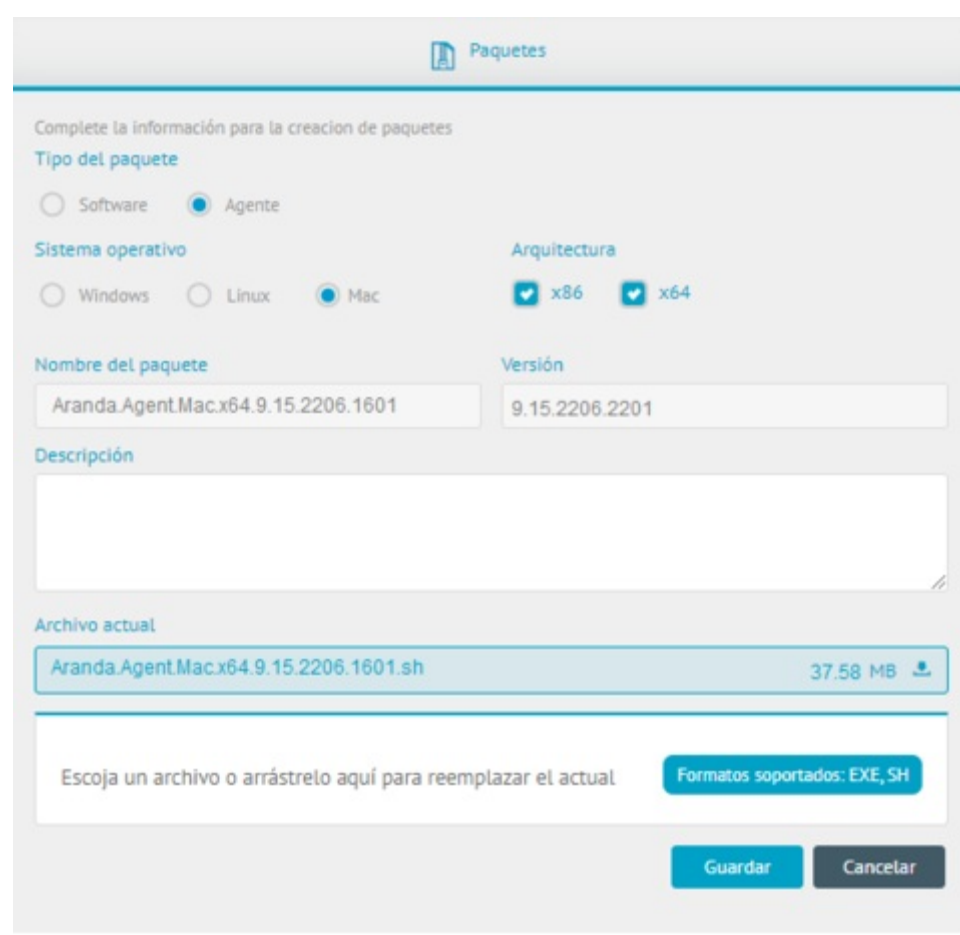
- Após 12 horas, após a instalação ou atualização do console do ADM, o agente do ADM tentará atualizar para a versão mais recente lançada para a versão do console. Se você quiser forçar a atualização, na lista de dispositivos, você pode executar o **Agente de atualização**

- A partir da versão 9.23.0 do ADM Agent, não é mais necessário carregar o pacote do agente do console do ADM para atualização do agente.

Atualizando o Agente do MacOs

1. Para realizar a atualização automática do agente MacOs, entre no console de gerenciamento do ADM, na seção de Configuração do ADM No menu principal, selecione o ícone **Pacotes** . Na visualização de informações, clique em **Mais opções e Pacote**.

Carregue o arquivo de instalação com extensão **.Sh**.



Paquetes

Complete la información para la creación de paquetes

Tipo del paquete

☐ Software ☒ Agente

Sistema operativo

☐ Windows ☐ Linux ☒ Mac

Arquitectura

☒ x86 ☒ x64

Nombre del paquete

Aranda.Agent.Mac.x64.9.15.2206.1601

Versión

9.15.2206.2201

Descripción

Archivo actual

Aranda.Agent.Mac.x64.9.15.2206.1601.sh 37.58 MB

Escoja un archivo o arrástrelo aquí para reemplazar el actual

Formatos soportados: EXE, SH

Guardar Cancelar

2. Quando o agente terminar de carregar, clique em **Salvar**

📌 **Nota:**

- Após 12 horas, após a instalação ou atualização do console do ADM, o agente do ADM tentará atualizar para a versão mais recente lançada para a versão do console. Se você quiser forçar a atualização, na lista de dispositivos, você pode executar o **Agente de atualização**

- A partir da versão 9.23.0 do ADM Agent, não é mais necessário carregar o pacote do agente do console do ADM para atualização do agente.

Pacote do Agente Linux

1. Para executar a atualização automática do agente Linux, vá para o ADM Management Console, no **Configuração do ADM** No menu principal, selecione o ícone **Pacotes** . Na visualização de informações, clique em **Mais opções e Pacote**.

Carregue o arquivo de instalação com extensão **.Sh**.

Paquetes

Complete la información para la creación de paquetes

Tipo del paquete

☐ Software ☒ Agente

Sistema operativo

☐ Windows ☒ Linux ☐ Mac

Arquitectura

☒ x86 ☒ x64

Nombre del paquete

Aranda.Agent.Linux.x64.9.14.2205.0386

Versión

9.14.2205.0386

Descripción

Archivo actual

Aranda.Agent.Linux.x64.9.14.2205.0386.sh	18.70 MB
--	----------

Escoja un archivo o arrástrelo aquí para reemplazar el actual

Formatos soportados: EXE, SH

Guardar Cancelar

📌 **Nota:**

- Após 12 horas, após a instalação ou atualização do console do ADM, o agente do ADM tentará atualizar para a versão mais recente lançada para a versão do console. Se você quiser forçar a atualização, na lista de dispositivos, você pode executar o **Agente de atualização**

- A partir da versão 9.23.0 do ADM Agent, não é mais necessário carregar o pacote do agente do console do ADM para atualização do agente.

Atualização manual da prateleira

1. Pare o serviço Aranda Conserver V9.

2. Desinstale o programa Conserver Service do painel de controle.

3. Exclua o registro da seguinte pasta:

- Pasta “%Program Files (x86)%\Aranda\Conserver” exceto para o ‘Data’.

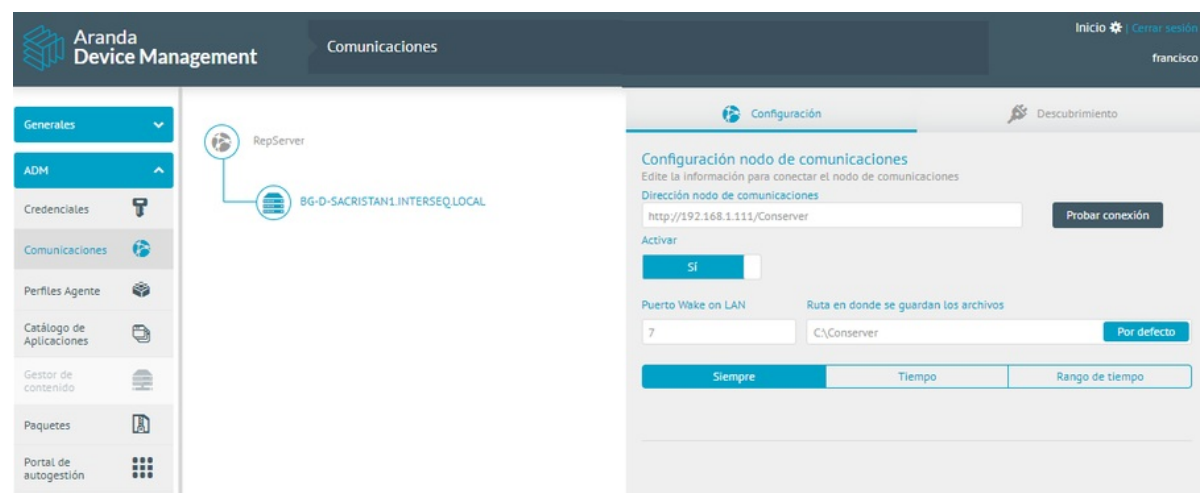
📌 **Nota:** Não exclua o conteúdo do repositório Conserver.

4. Execute o instalador Aranda.Conserver.Installer.exe. Não carregue o serviço até configurar o **.config** da pasta do conservador. [Consulte Servidor de instalação.](#)

5. Inicie o serviço Aranda Conserver V9.

6. Para verificar se a conexão foi bem-sucedida do servidor, efetue login no ADM Management Console, no

Configuração do ADM No menu principal, selecione o ícone **Comunicações** . Na Visualização de Informações, na Árvore de Comunicações, clique no nó Repserver e selecione Manter. Na visualização de detalhes no **Configuração** Clique no botão **Conexão de teste**



- 📌 **Nota:** A instalação do Servidor requer que o servidor tenha a versão 4.8 do .NET Framework ou posterior.
- 🔗 **Links Relacionados:** A atualização do conservador também pode ser feita por meio de um projeto de distribuição. [Atualizando o projeto de servidor por distribuição](#)

Atualização do conservador via projeto de distribuição

[Atualize da versão 9.16 para a 9.17 »](#)

[Atualizar de versões posteriores à 9.17 »](#)

Pré-condições

- O servidor conservador deve ter um agente instalado, apontando para o repserver e com o módulo de distribuição habilitado no perfil do agente.
- O agente instalado no conservador deve ter um perfil de agente sem lista de nós de comunicação.

Atualizar da versão 9.16 para a 9.17

- 📌 **Nota:** A instalação do Servidor requer que o servidor tenha a versão 4.8 do .NET Framework ou posterior
1. Crie um arquivo com .bat extensão (*por exemplo, UpdateConserver.bat*)2. Copie e edite o script a seguir no arquivo criado e salve-o.
- 📌 **Nota:**

 - Insira a variável path a rota onde o conservador está instalado.
 - Insira a variável conserver O nome completo do instalador do Conservador
 - Se você tiver mais de um conservador e eles estiverem instalados em um caminho diferente, você deverá criar um .bat e um projeto diferentes para cada um dos conservadores

```
:: 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. Criar um arquivo com uma extensão .config e nomeá-lo Aranda.Conserver.Windows.Service.exe.config
2. Copiar, configurar campos-chave <appSettings> e salve.

```
<?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 -->  
  </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>
```

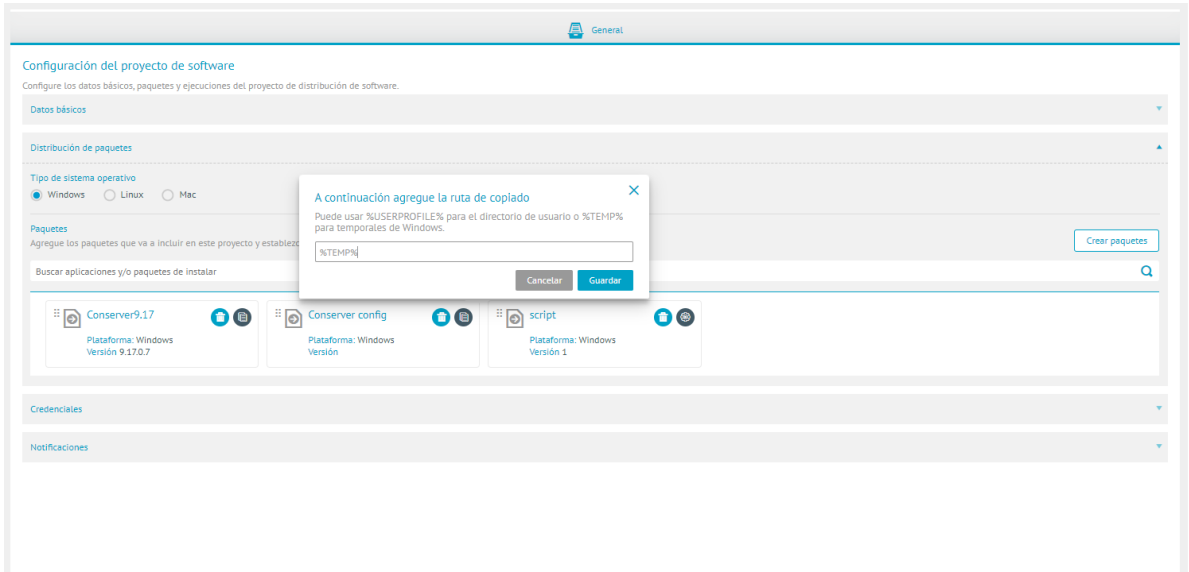
```

        <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. [Criar um pacote de distribuição](#) para copiar com o instalador do servidor. 4. [Criar um pacote de distribuição](#) para copiar com o Aranda.Conserver.Windows.Service.exe.config criado nas etapas 3 e 4.

5. [Criar um novo Pacote de Distribuição](#) cara execução com o arquivo .bat criado nas etapas 1 e 2.
6. Faça login no gerenciamento de distribuição do ADM e crie um [Projeto de Distribuição de Software](#).
7. No projeto, adicione os pacotes criados nas etapas 5, 6 e 7 na seguinte ordem:
- Pacote do instalador do conservador (*Pacote do tipo de cópia*)adicionando %TEMP% como um caminho.
 - Pacote Aranda.Conserver.Windows.Service.exe.config (*Pacote do tipo de cópia*)adicionando %TEMP% como um caminho.
 - Pacote UpdateConserver.bat (*Pacote do tipo execução*)



8. Execute a distribuição no computador para executar a atualização do Conservador.

📌 **Nota:** Se você tiver mais de um conservador e eles estiverem instalados em um caminho diferente, você deverá criar um .batU m.config e um projeto diferente para cada um dos conservadores. Se os conservadores mantiverem o caminho de instalação e tiverem a mesma configuração, eles poderão ser enviados no mesmo projeto de distribuição

9. Na configuração do ADM, defina o [Componentes de comunicação de reserva/conservação](#) e verifique a conexão.

Atualizando de versões posteriores à 9.17

Para atualizar o conservador usando um projeto de distribuição, você precisa seguir as seguintes etapas:

1. Crie um arquivo com .bat extensão (*por exemplo, UpdateConserver.bat*)
2. Copie e edite o script a seguir no arquivo criado e salve-o.

📌 **Nota:**

- Insira a variável path a rota onde o conservador está instalado.**
- Insira a variável conserver O nome completo do instalador do Conservador
- Se você tiver mais de um conservador e eles estiverem instalados em um caminho diferente, você deverá criar um .bat e um projeto diferentes para cada um dos conservadores

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

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

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

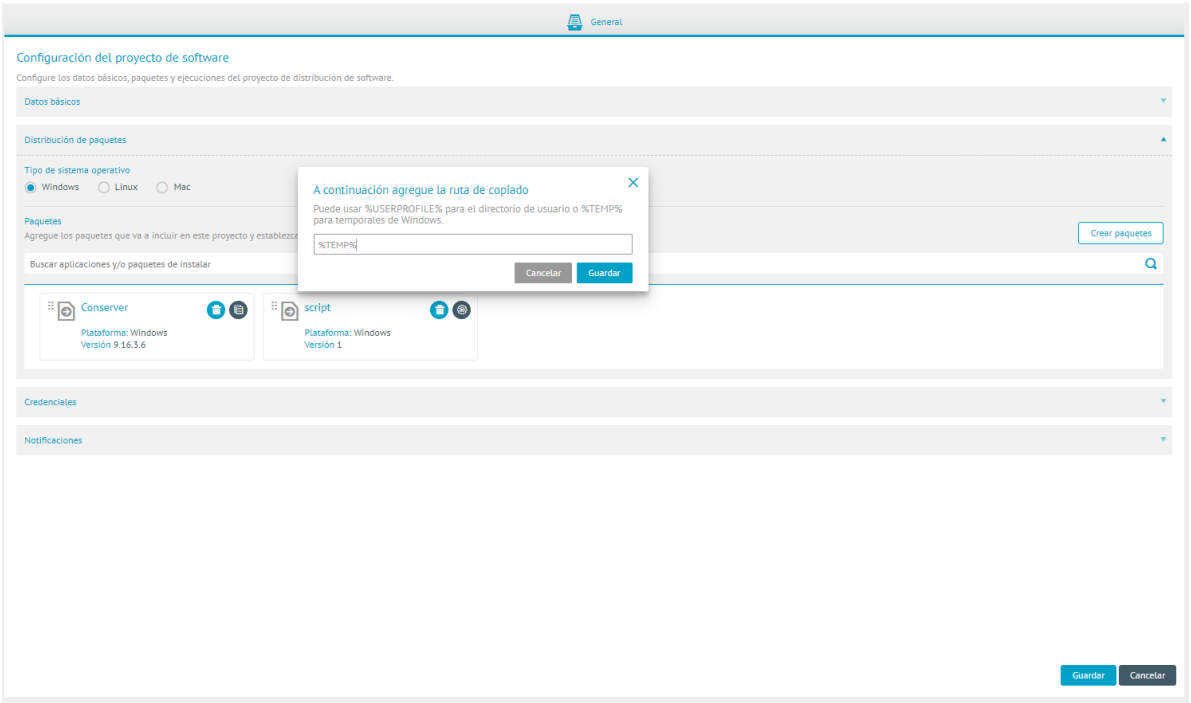
del %path%\Aranda.Conserver.Windows.Service.exe.config @timeout /t 3 /nobreak copy %TEMP%\Aranda.Conserver.Windows.Service.exe.config %path% @timeout /t 3 /nobreak

sc start ArandaConserverWindowsServiceV9

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

3. [Criar um pacote de distribuição](#) cara copiar com o instalador do servidor.
4. [Criar um novo Pacote de Distribuição](#) cara execução com o arquivo .bat criado nas etapas 1 e 2.
5. Faça login no ADM Distribution Management e crie um arquivo [Projeto de Distribuição de Software](#).

6. No projeto, adicione os pacotes criados nas etapas 3 e 4 adicionando primeiro o pacote do instalador do conservador (*Pacote do tipo de cópia*)adicionando %TEMP% como um caminho.



7. Execute a distribuição no computador para executar a atualização do Conservador.

📌 **Nota:**

- Se você tiver mais de um conservador e eles estiverem instalados em um caminho diferente, você deverá criar um .bat e um projeto diferentes para cada um dos conservadores. Se os conservadores mantiverem o caminho de instalação, eles poderão ser enviados no mesmo projeto de distribuição.

Se a distribuição tiver sido bem-sucedida, o conservador será atualizado.

8. Na configuração do ADM, defina o [Componentes de comunicação de reserva/conservação](#) e verifique a conexão.

## Atualização do Visualizador de Suporte Remoto

Para atualizar o Remote Support Viewer, siga as etapas abaixo:

1. Faça login em Painel de controle > Programas > Programas e recursosSelecione Aranda ADM Utils e clique em Desinstalar

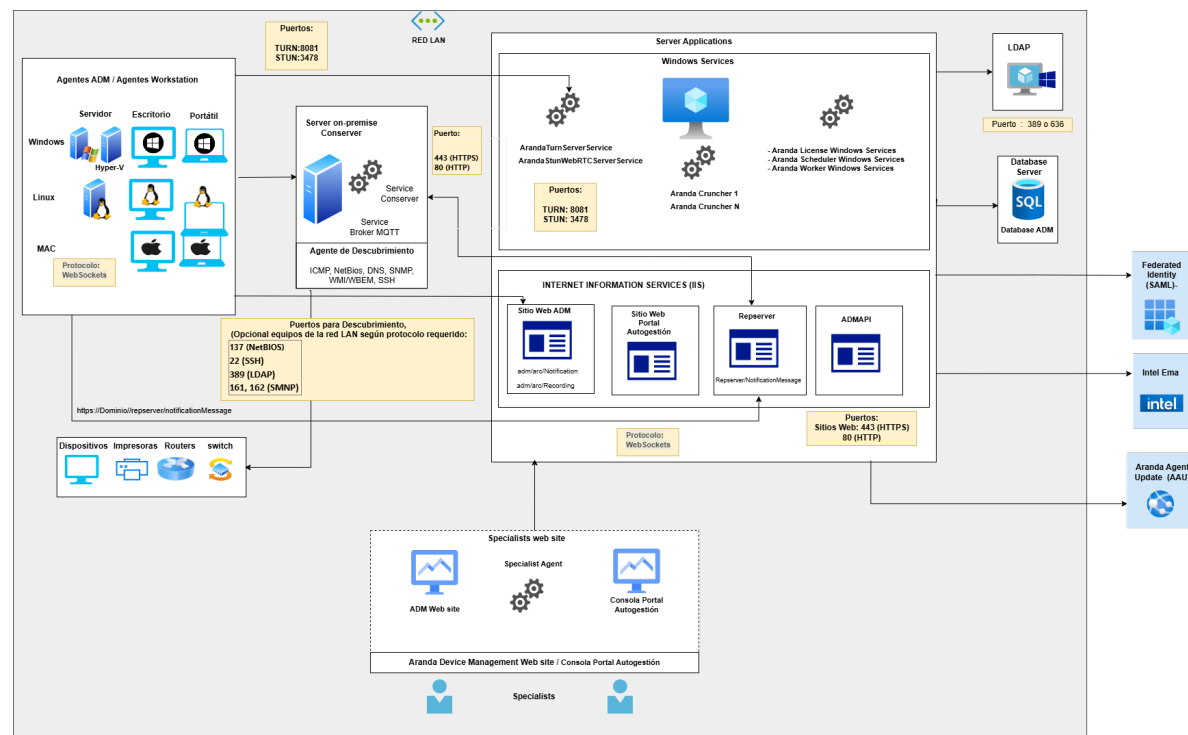


2. Depois que a versão anterior for desinstalada, você poderá iniciar a instalação da nova versão [Exibir a instalação do Remote Support Viewer](#)

## Estruturas ADM

## Estrutura Onpremise

A estrutura e operação do Aranda Device Management ADM é um aplicativo distribuído nos seguintes componentes:



Banco de dados (servidor na infraestrutura do cliente)

Repositório onde todas as informações do sistema são armazenadas. O banco de dados armazena informações de inventário de hardware, software e arquivos para todas as estações de trabalho.

## Servidor de aplicativos

Este servidor contém a lógica de negócios, bem como os módulos Mailer, DB Manager, Conserver e Cruncher. Além disso, ele se comunica com o Console Web para exibir as informações contidas no banco de dados lá.

## Preservar

O Conservador atua como um link entre os componentes do servidor de aplicativos e a LAN do cliente. Este é um serviço do Windows que deve estar localizado na rede LAN para enviar e receber mensagens dos agentes instalados em cada máquina facilita os processos de descoberta, distribuição e gerenciamento remoto. Dependendo da topologia, um Conservador deve ser instalado para cada segmento de rede.

## Cruncher

Serviço instalado no servidor onde o console está instalado, é responsável por processar os inventários e salvá-los no banco de dados. Para fazer isso, ele descriptografa, descompacta e armazena os dados coletados por cada estação. Existem 2 trituradores:

## Agente ADM

O agente de gerenciamento de dispositivos Aranda é o componente instalado nos dispositivos do cliente é responsável por gerar, compactar, criptografar e enviar via TCP/IP o inventário de hardware e software em cada uma das estações de trabalho; Também permite a geração de inventários e o gerenciamento seguro de comandos do servidor.

Esse componente é instalado no lado do cliente. Ele pode ser instalado localmente e/ou remotamente em cada estação de trabalho.

## Repserver

Esse componente é instalado no servidor de aplicativos e é responsável por receber solicitações da rede LAN do cliente ou de computadores conectados diretamente pela Internet.



## Servidor Web Repserver

Esse componente é instalado no servidor de aplicativos e contém o IIS dos Serviços de Informações da Internet e o .Net Framework, nos quais o aplicativo para o Console da Web de Administração está instalado.

## Web Console

Através desta interface que o cliente, usuário ou administrador visualiza, eles poderão gerenciar e visualizar inventários de hardware e software por estação de trabalho, rastrear e controlar seus recursos de TI, executar tarefas de controle remoto.

## Portal de Autogestão

Essa interface que o cliente visualiza, permite que os usuários responsáveis pelos dispositivos visualizem os projetos de distribuição de software disponíveis e realizem a instalação de forma autônoma.

## Corretor MQTT

Este serviço, localizado na rede LAN do cliente, permite gerenciar e controlar as ações de mensagens enviadas ao console web em tempo real.

Facilita a comunicação com os diferentes dispositivos que estão sendo gerenciados, permite que as solicitações aos dispositivos cheguem em tempo real, para as comunicações dos dispositivos dentro da rede LAN empresarial, o serviço pode ser instalado no servidor do conservador ou outro servidor que esteja na rede LAN, é necessário abrir a porta 1884 ou 1883.

## Servidor de turno

Quando dois dispositivos não conseguem estabelecer uma conexão direta entre si, é necessário um servidor Turn para facilitar a comunicação.

É um serviço do Windows instalado em uma máquina virtual, que atua como uma ponte para controle remoto entre o agente especialista e o agente da estação de trabalho. Para ativar essa funcionalidade, ambos os agentes estabelecem uma conexão com o Turn Server, que está escutando na porta 8081 ou o parametrizado para operação no Onpremises, transmitindo os dados de um agente para o outro. (Nuvem, porta de escuta definida 3478)

## Agente Especialista

Ele foi projetado para permitir acesso por controle remoto, transferências de arquivos e gravações para auditorias. Cada especialista deve instalar este aplicativo na máquina onde trabalha.

## Agente de estação de trabalho

Componente instalado em dispositivos Windows em arquiteturas, eles são responsáveis por receber suporte remoto. Ele pode ser localizado dentro e fora da infraestrutura do cliente.

## Portos

Portas de comunicação usadas pelo Aranda Device Management (ADM) para permitir as comunicações necessárias.