

Este guia detalha as etapas necessárias para instalar e configurar o Aranda Virtual Support (AVS) em um ambiente local. AVS é um aplicativo de suporte remoto desenvolvido pela Aranda Software que permite assumir o controle remoto e transferir arquivos em tempo real e com segurança para estações de trabalho.

Qual é a nossa documentação?

- [Guia de introdução do AVS](#)
- [Manual do usuário de gerenciamento AVS](#)
- [Manual do agente AVS](#)
- Manual de instalação local

Pré-requisitos

Pré-requisitos

Requisitos do sistema

Os requisitos a seguir são definidos para a implementação do Aranda Virtual Support em uma instalação local.

	Servidor de aplicativos da Web / Serviços
Dedicatória	Uso dedicado para AVS (não compartilhe seu uso com outros aplicativos)
Armazenamento	- Espaço necessário: Mínimo de 64 GB - Tipo de unidade: Unidade de estado sólido (SSD) - Partições: A partição dedicada é recomendada para instalação no site. Uma partição dedicada é recomendada para o banco de dados (arquivos MDF e LDF)(*) * No caso de instalação da solução no mesmo servidor onde reside o banco de dados.
Processamento	4 CPUs/8 vCPUs a 2,1 GHz ou superior.
Conectividade	Placa de rede Gigabit Ethernet (1 GBps ou superior)
Base de dados	Versões: SQL Server 2019, SQL Server 2022 Edições: Standard (para Ambientes de Teste), Enterprise (para Ambientes de Produção) e Express (apenas para Provas de Conceito). Licenciamento: É recomendável licenciar o banco de dados por Core. Agrupamento: SQL_Latin1_General_CP1_CI_AI Permissões: Usuário para criação de banco de dados (DBTools): Membro de função fixo db_owner. Usuário do Serviço de Banco de Dados: Membro de Função Fixa db_datareader e db_datawriter. Executar permissões no esquema dbo
Sistema Operacional	Versão: Windows Server 2019, Windows Server 2022. Edição: Padrão ou Superior. Conta de instalação: Credenciais de administrador local e/ou de domínio são necessárias para a instalação.
Protocolos	- O aplicativo funciona apenas com HTTPS. - Os websockets devem ser ativados em toda a rede. O que é necessário para que o WebRTC funcione corretamente.
Portas de entrada	- A porta deve estar habilitada para usar HTTPS (por exemplo, 443). - Também a porta configurada para o servidor de turno e atordoamento.
Serviço de atualização	O servidor de trabalho deve ser configurado para acessar o site https://download.arandasoft.com/updates e baixar arquivos.

Requisitos adicionais

- Serviços de Informações da Internet (IIS) 10.0 ou superior.
- Papéis
 - Serviços de arquivo e armazenamento
 - Serviços de armazenamento
- Servidor Web
 - Recursos comuns de HTTP
 - Documento padrão
 - Navegação no diretório
 - Erros HTTP
 - Conteúdo estático
 - Saúde e diagnóstico
 - Registro HTTP
 - Arte performática

- Conteúdo estático
- Segurança
- Filtragem de solicitações
- Desenvolvimento de aplicativos
- Extensibilidade do .NET 4.8
- APS.NET 4,8
- Extensões ISAPI
- Filtros ISAPI
- Protocolo WebSocket
- Ferramentas de gerenciamento
 - Console de Gerenciamento do IIS
- Características
- Recursos do .NET Framework 4.8
 - .NET Framework 4.8
 - Serviços WCF
 - Compartilhamento de porta TCP
- Criptografia de unidade de disco BitLocker
- Armazenamento aprimorado
- Microsoft Defender Antivirus
- Arquivador de dados do sistema
- Windows PowerShell
 - Windows PowerShell 5.1
- Suporte para WoW64
- Visualizador XPS
- Módulo de reescrita de URL versão 2.1 ou superior [Ver página de download](#)
- ASP.NET Pacote de hospedagem do Core Runtime 6.0.32 [Ver página de download](#)

▮ Nota: Antes de iniciar a instalação do Aranda Virtual Support, é necessário criar o esquema do banco de dados através do Ferramentas de banco de dados Aranda v9.

Veja o [Manual do usuário Ferramentas de banco de dados Aranda V9](#)

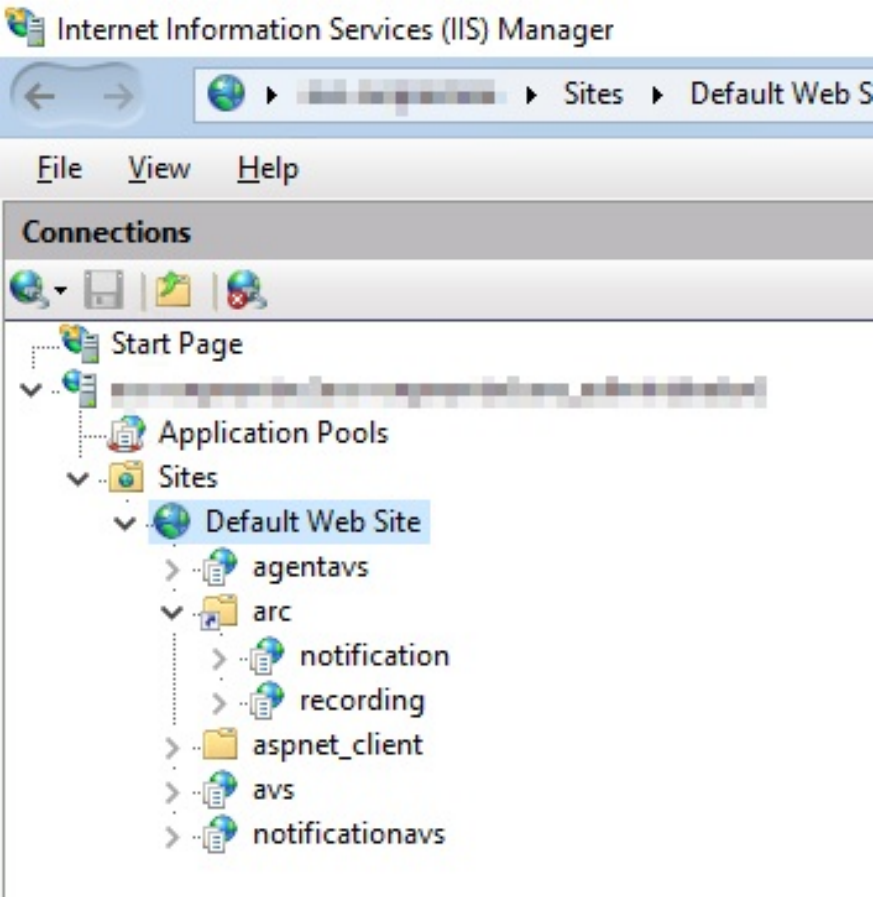
Serviço de Licenciamento

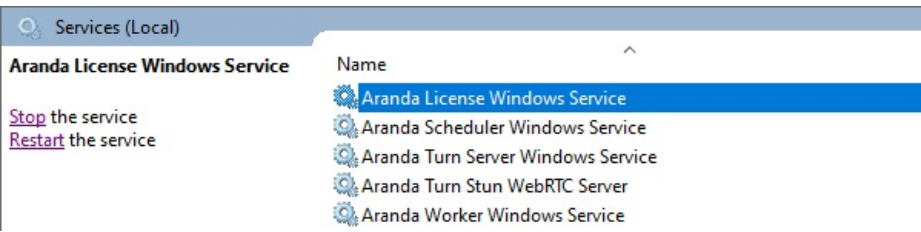
O Aranda Virtual Support (AVS) usa o serviço de licenciamento comum da Aranda para autorizar os usuários a acessar o site da AVS e controlar as licenças adquiridas, entre outras operações. Este é um serviço do Windows que geralmente é criado automaticamente pelo instalador do produto. Depois que o usuário carrega suas licenças adquiridas do site, o serviço de licenciamento comum deve permanecer na mesma máquina, caso contrário, as licenças carregadas serão perdidas. 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. Verifique com o fornecedor para obter detalhes sobre a implantação do servidor.

Instalação AVS

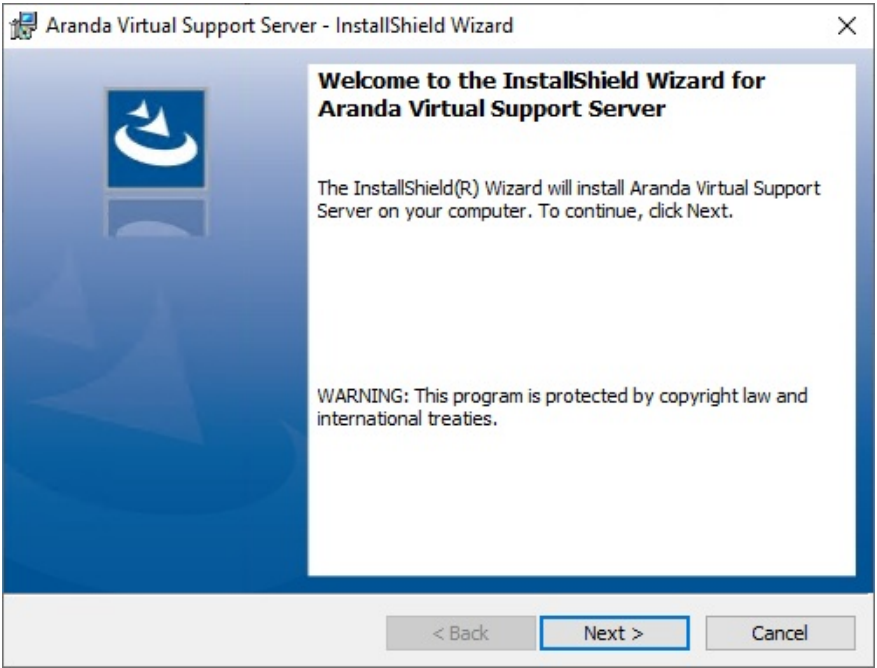
Instalando o AVS no local

O instalador AVS. Server.Installer Ele instala cinco sites (agentavs, arc/notification, arc/Recording, avs, notificationavs).

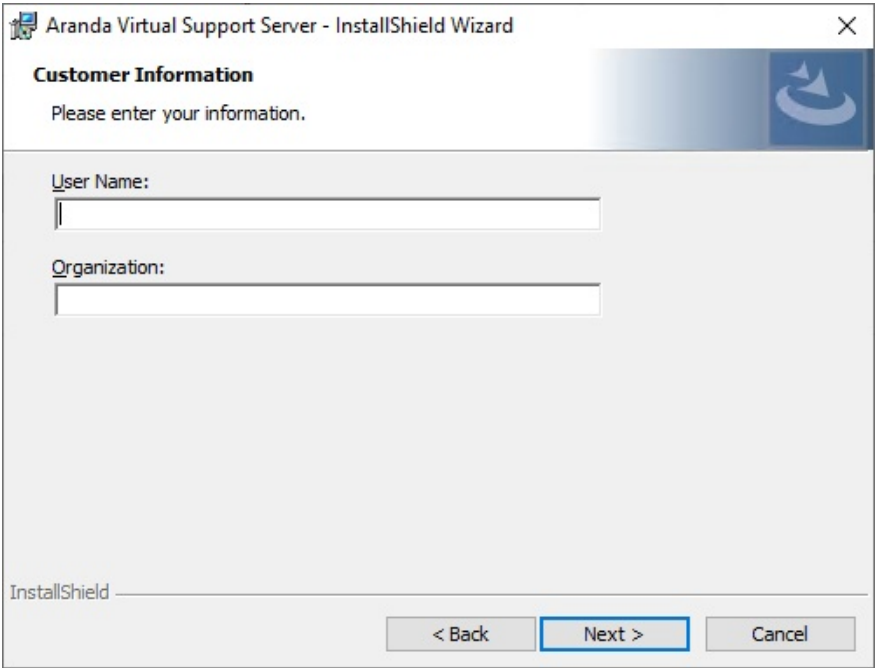




1. Clique duas vezes no arquivo do instalador e você verá a tela de boas-vindas. Confirme a instalação clicando no botão Seguinte.



2. Na janela Informações ao cliente, insira o nome de usuário, a organização e clique em Seguinte.

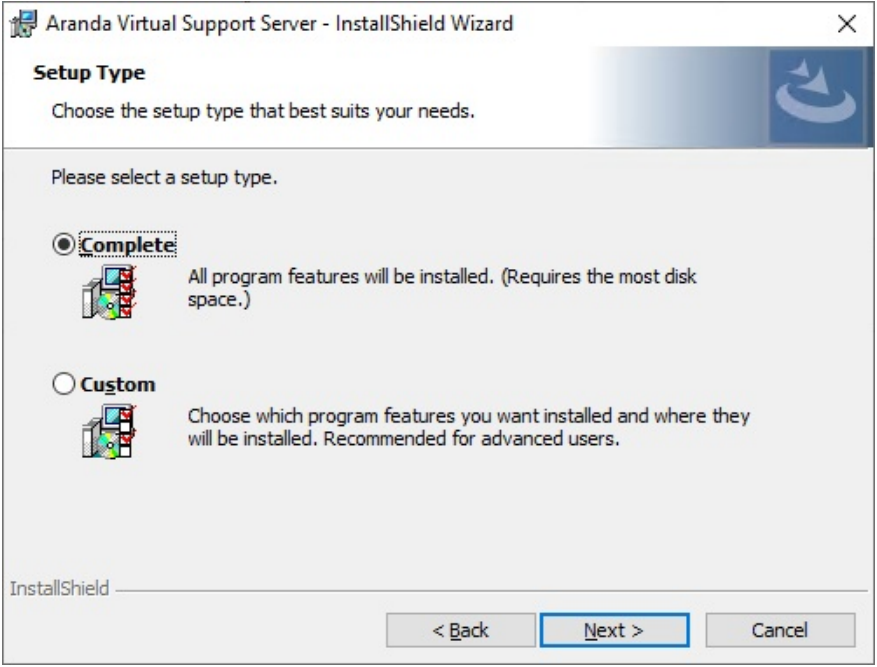


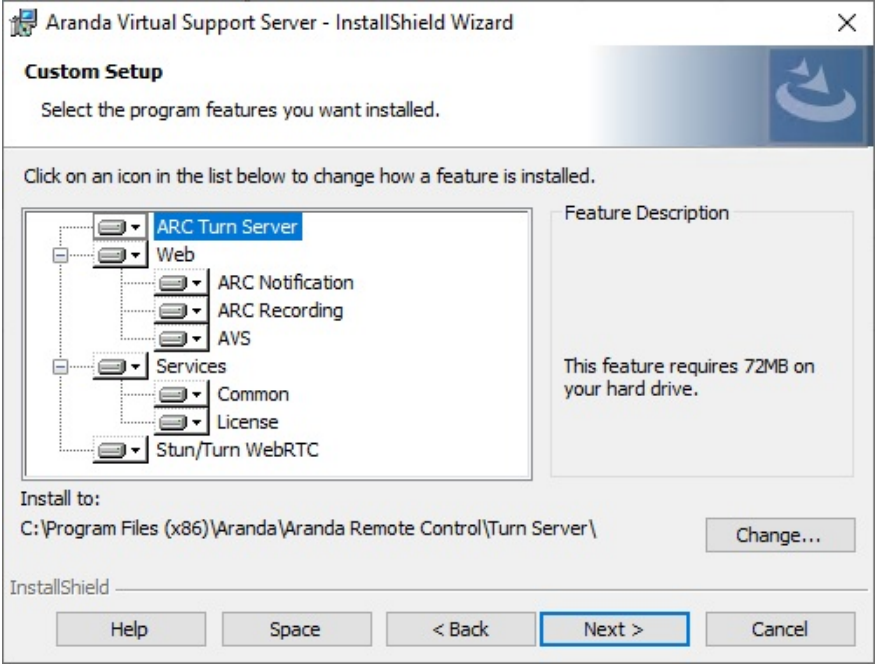
3. Na janela Tipo de instalação Você pode configurar as seguintes opções:

- Completar: Todos os sites e serviços serão instalados nas rotas padrão.
- Costume: Você poderá selecionar os sites ou serviços que deseja instalar.

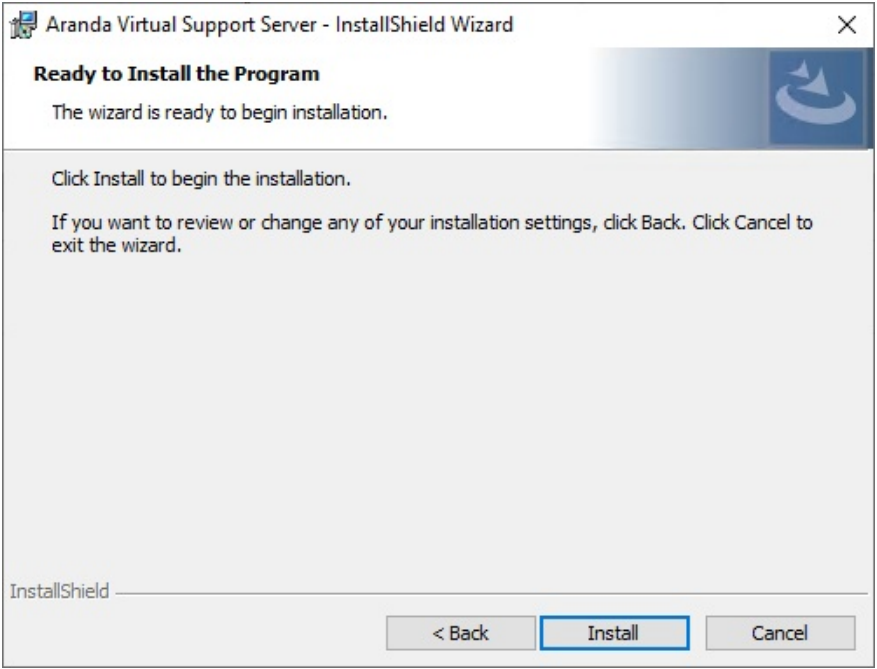
▮ Nota: Por padrão, selecione o tipo de instalação Completar. No caso de separar as camadas da solução (Web, Aplicativo) em servidores separados, selecione o Costume.

⚠ Importante: Se você estiver executando uma instalação personalizada, não modifique o caminho de instalação.





4. Configurando o tipo de instalação, na janela Preparando-se para instalar o programa clique Seguinte e depois no Instalar.



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

Configuração de conexão de banco de dados

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

Configurar sites

Para configurar os sites, atualize o valor da string de conexão, na linha 6 dentro dos arquivos appsettings.json de cada local; As rotas padrão são:

```
C:\inetpub\wwwroot\agentavs\appsettings.json
C:\inetpub\wwwroot\arc\recording\appsettings.json
C:\inetpub\wwwroot\avs\appsettings.json
C:\inetpub\wwwroot\notificationavs\appsettings.json
```

Exemplo de como a cadeia de conexão deve ser exibida no appsettings.json

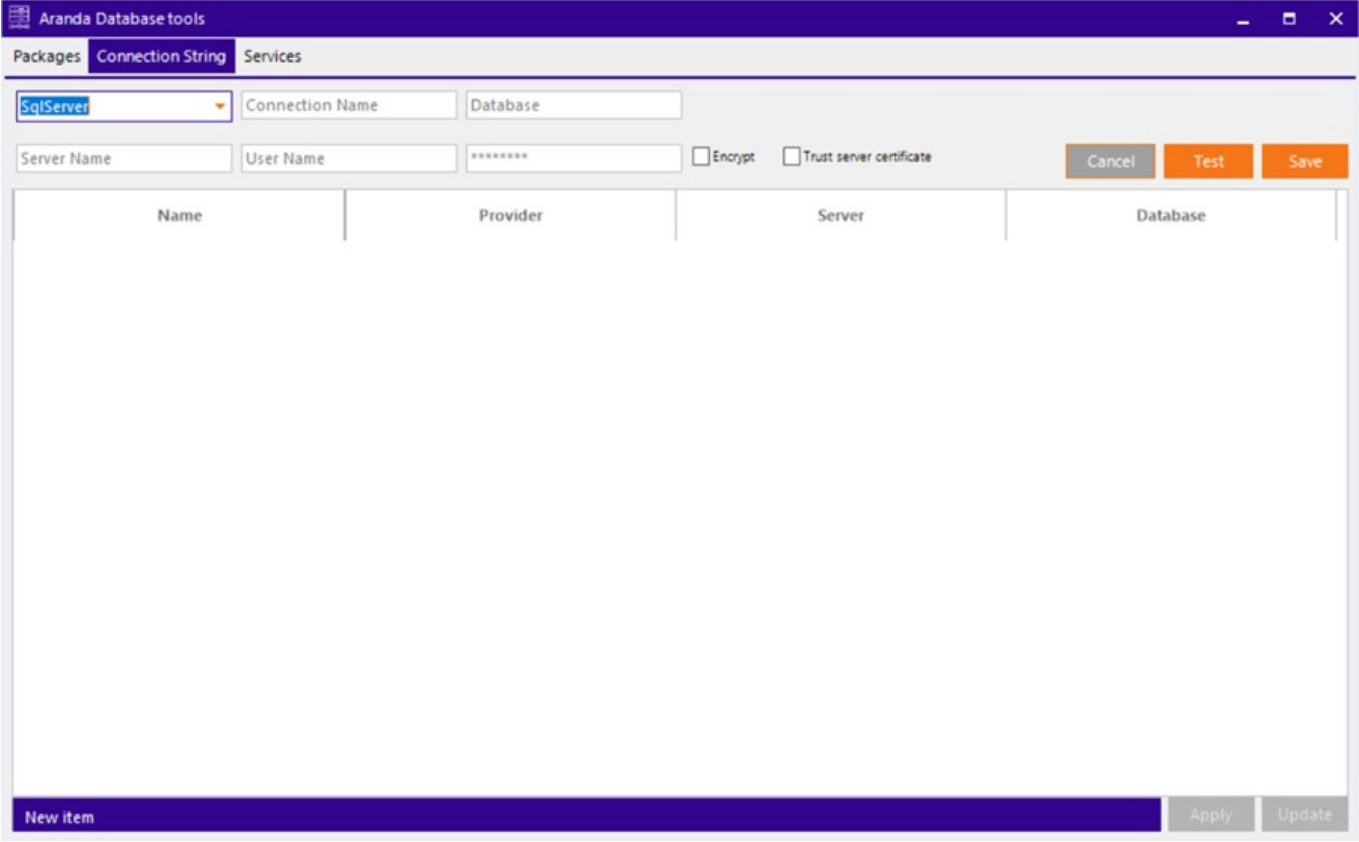


Lembre-se de que as propriedades devem ser incluídas Encrypt e TrustServerCertificate e o valor é atribuído de acordo com as regras de negócio do cliente. [Veja a documentação da Microsoft](#)

Configurar serviços comuns

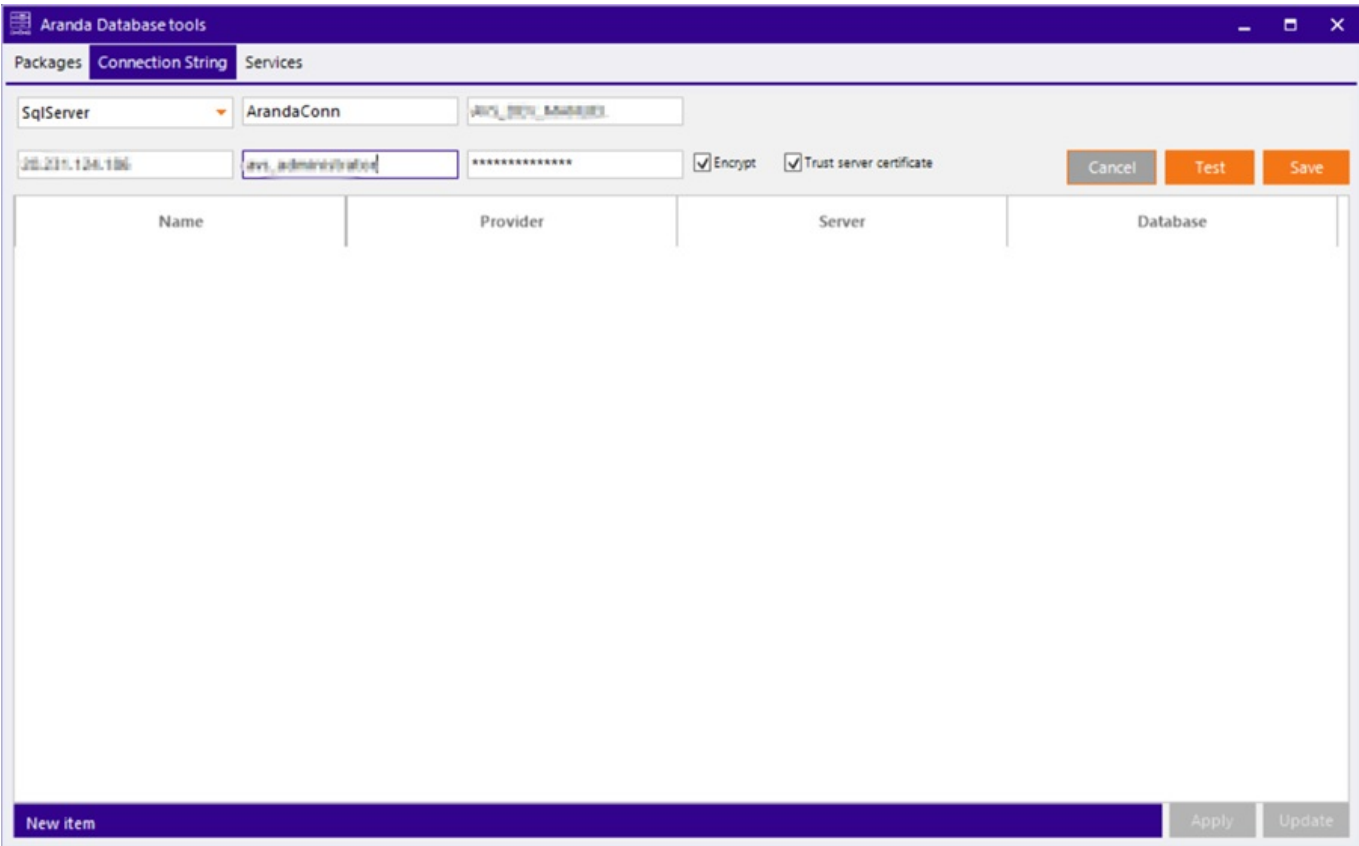
Para configurar os serviços Common e Licenciamento, isso é feito por meio do Ferramentas de banco de dados Aranda v9. Para fazer isso:

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

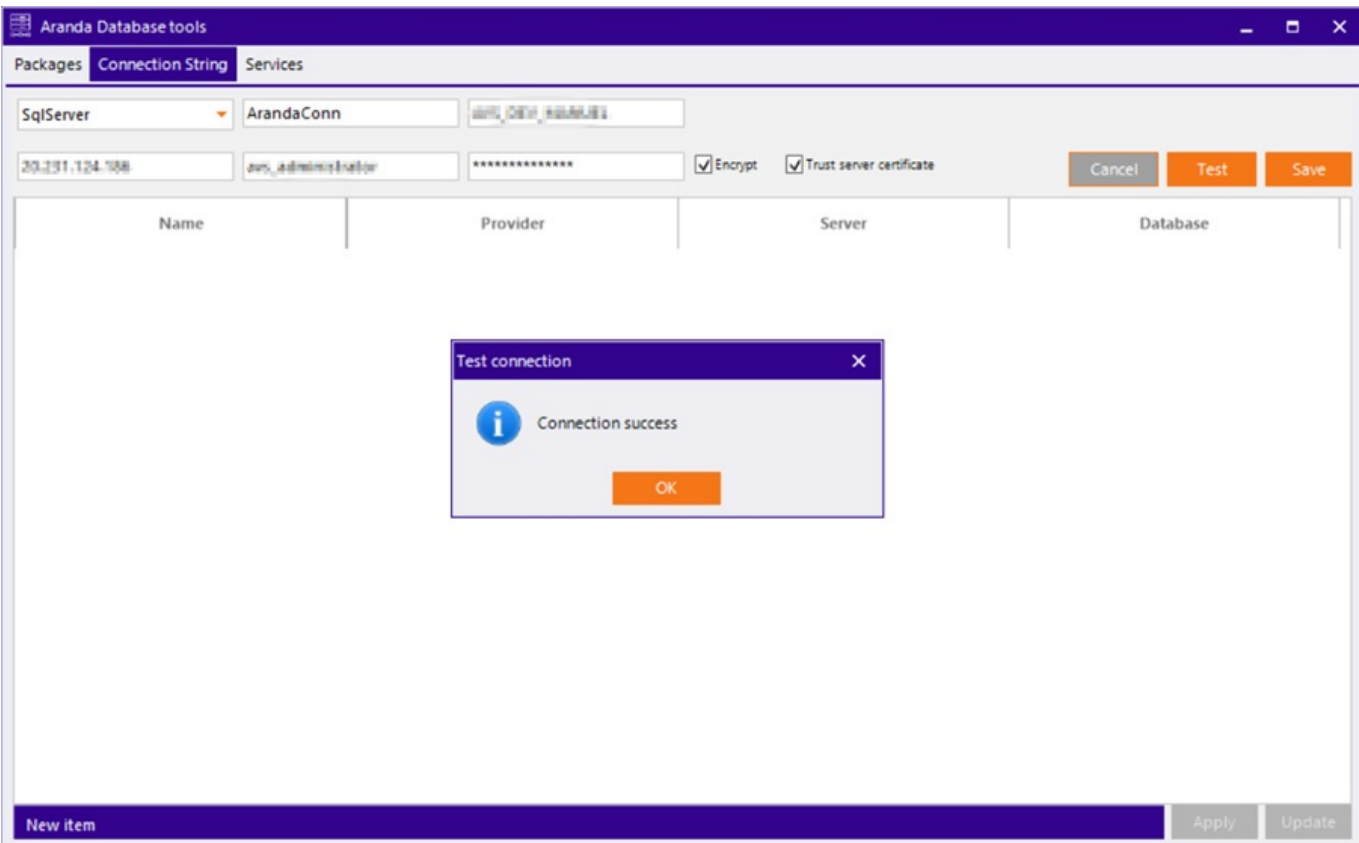


2. Preencha os dados solicitados.

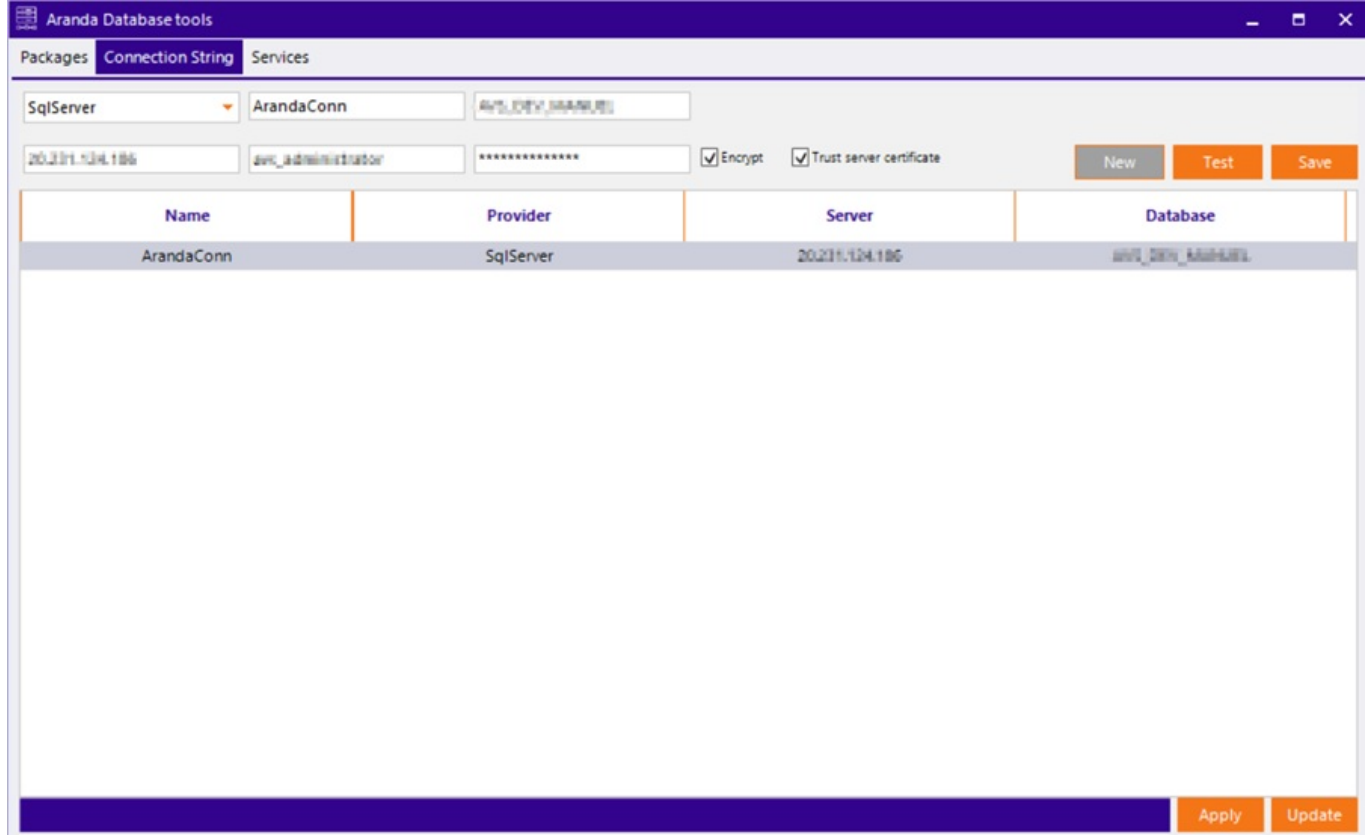
- Selecione o mecanismo de banco de dados (SQL Server).
- Dê um nome para identificar a conexão.
- Registre os dados de conexão (nome do banco de dados, nome do servidor ou endereço IP e, se necessário, nome de usuário e senha).
- Caso a porta do banco de dados seja diferente da porta padrão (1433 para 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.



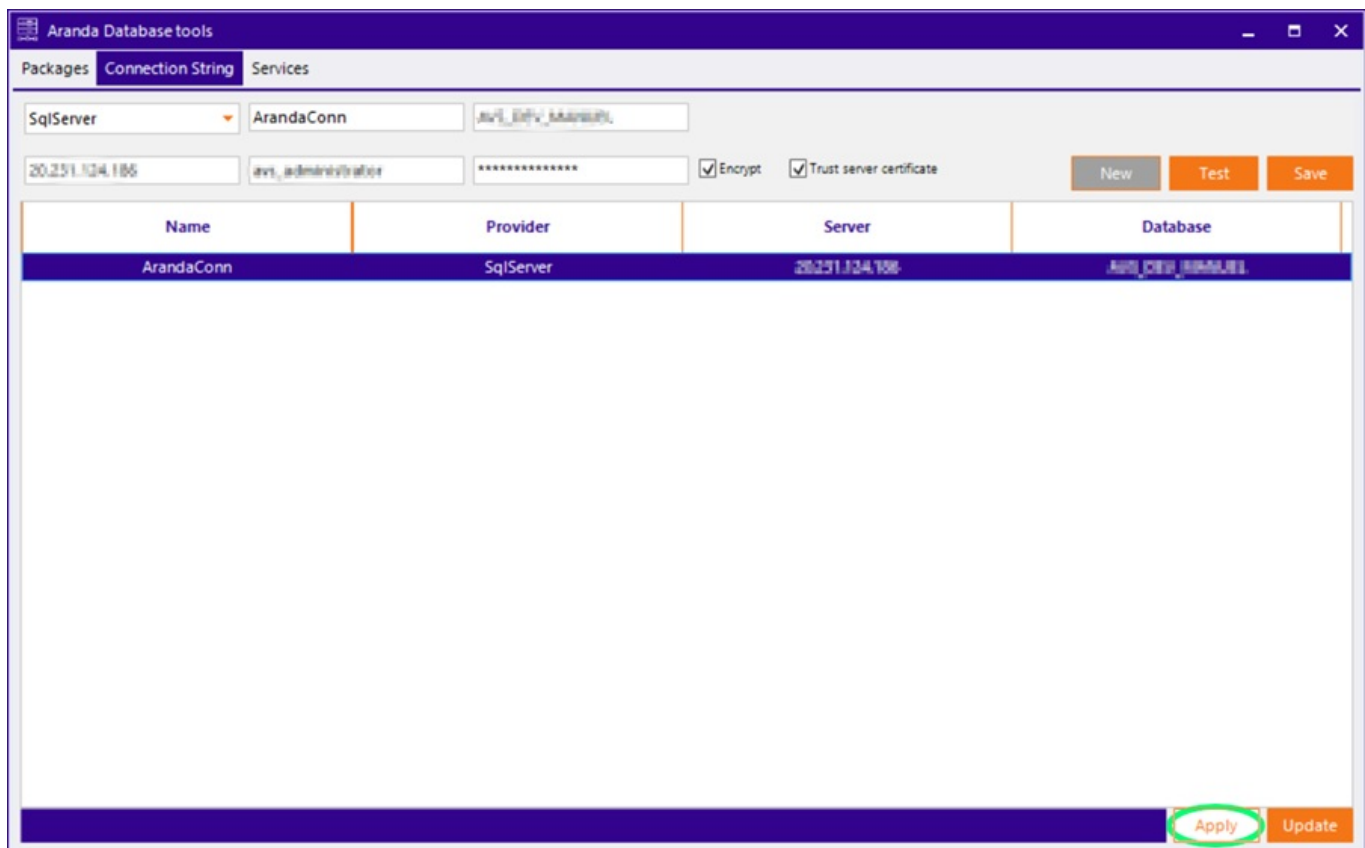
3. Clique no botão Teste para verificar a conexão.



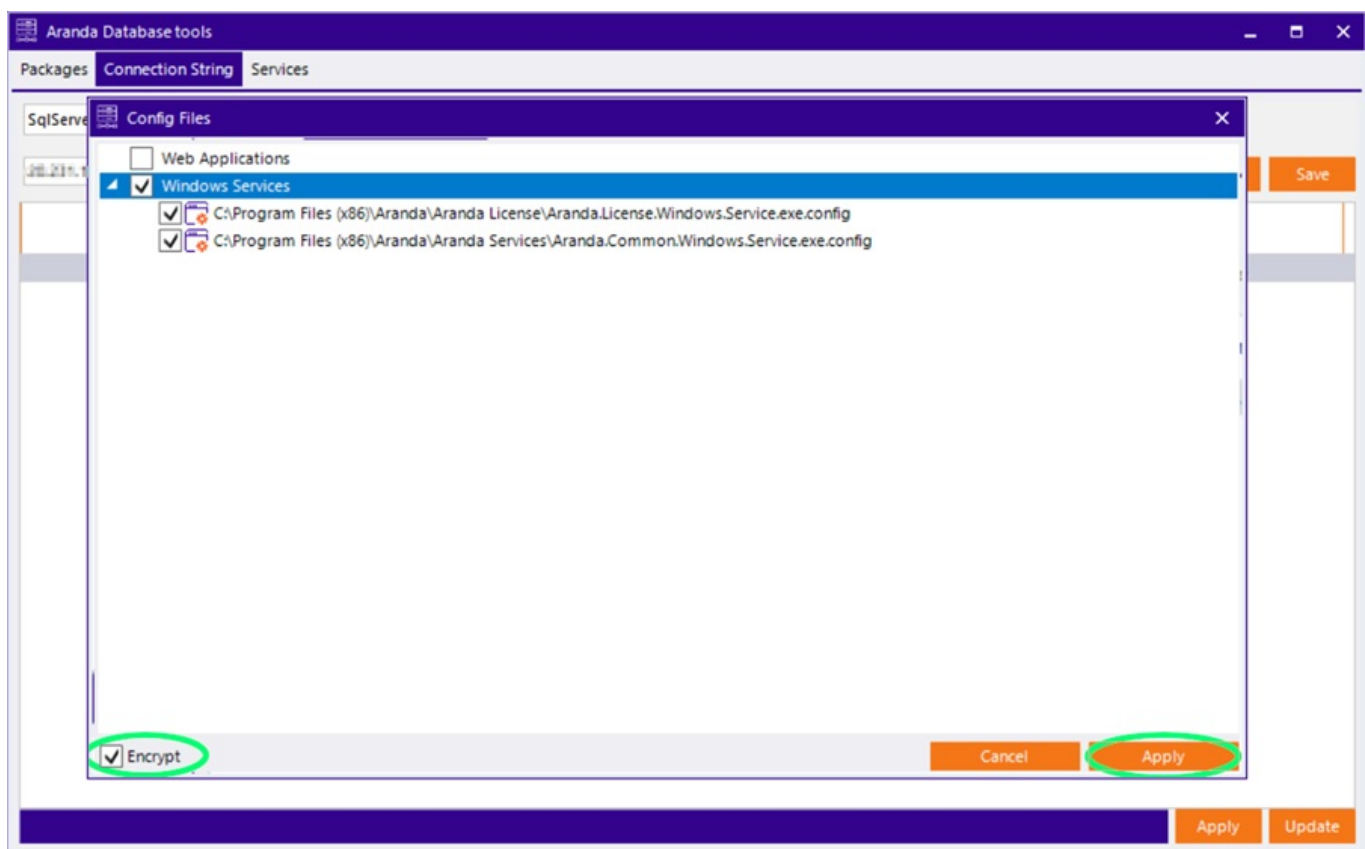
4. Para finalizar, clique no botão Salvar para salvar a conexão.



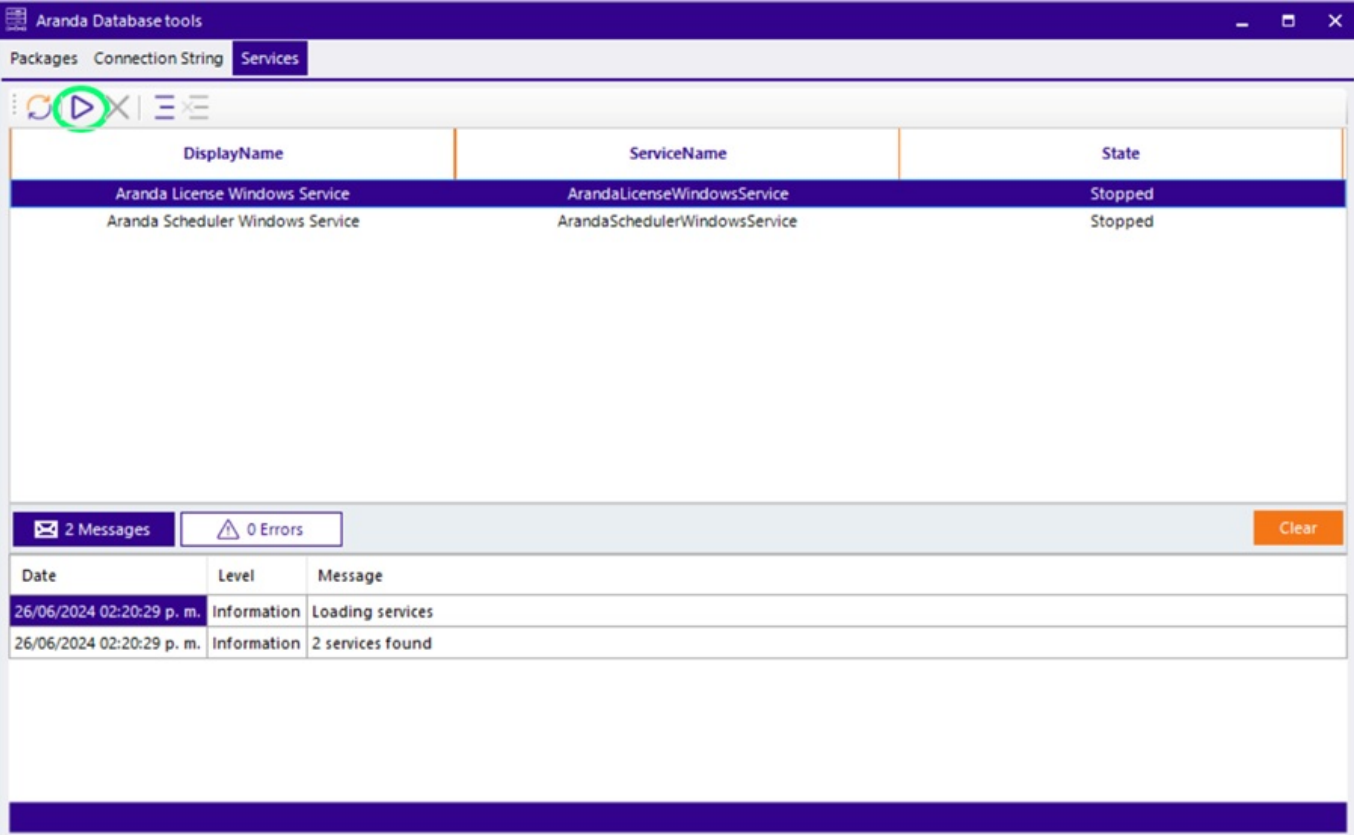
5. Para aplicar cadeias de conexão aos serviços instalados, selecione a conexão criada anteriormente e clique no botão Aplicar.



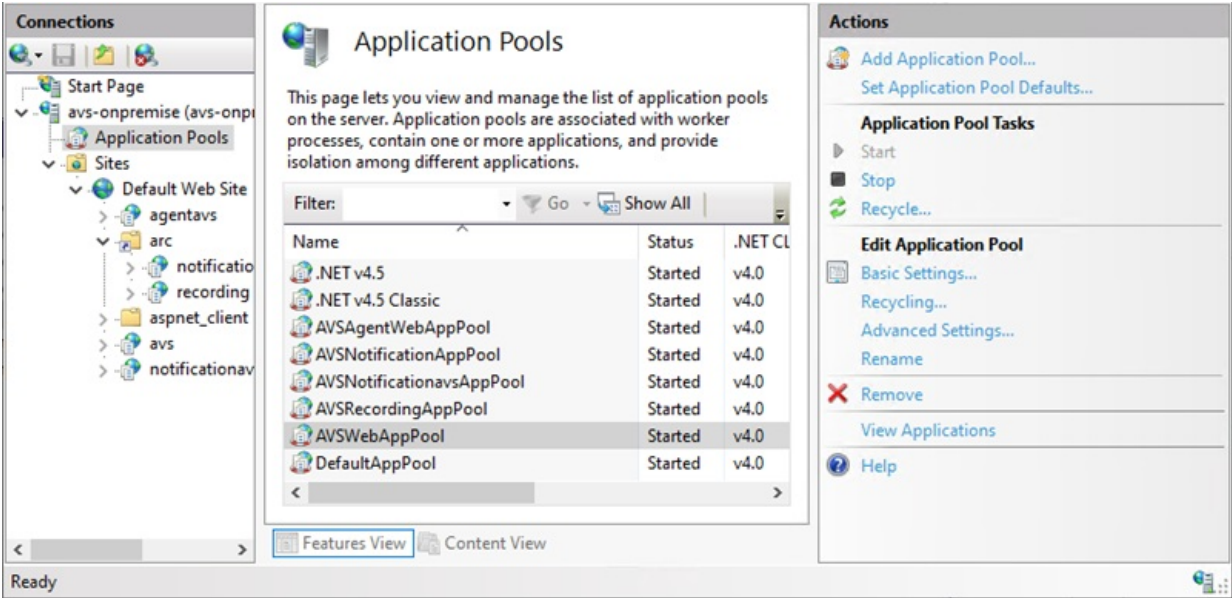
6. Uma janela é habilitada com a lista de aplicativos e serviços disponíveis no servidor.



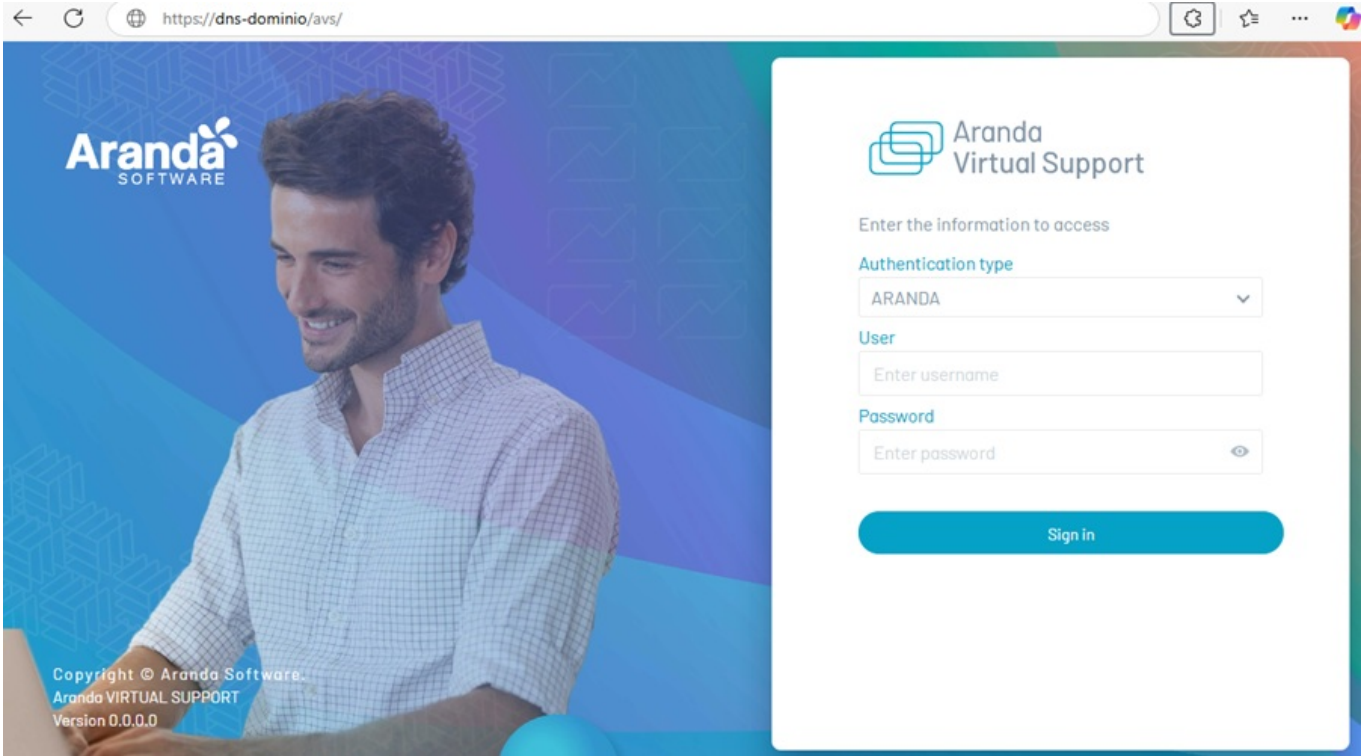
7. Selecione os serviços apropriados e clique no botão Aplicar Se você quiser criptografar a conexão, marque a caixa Criptografar no canto inferior esquerdo. Uma mensagem de alerta pode ser exibida porque a criptografia não é suportada para arquivos JSON. 8. Para finalizar, clique no botão Serviços e 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 da AVS onde poderá iniciar a configuração do Aranda Virtual Support através da seguinte URL: https://dns_servidor/avs/.

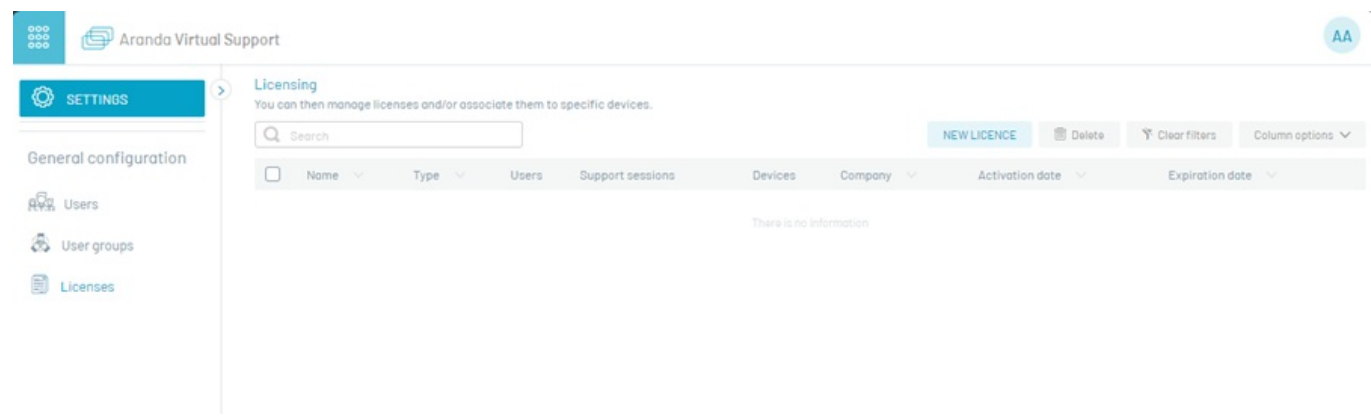


Licenciamento AVS

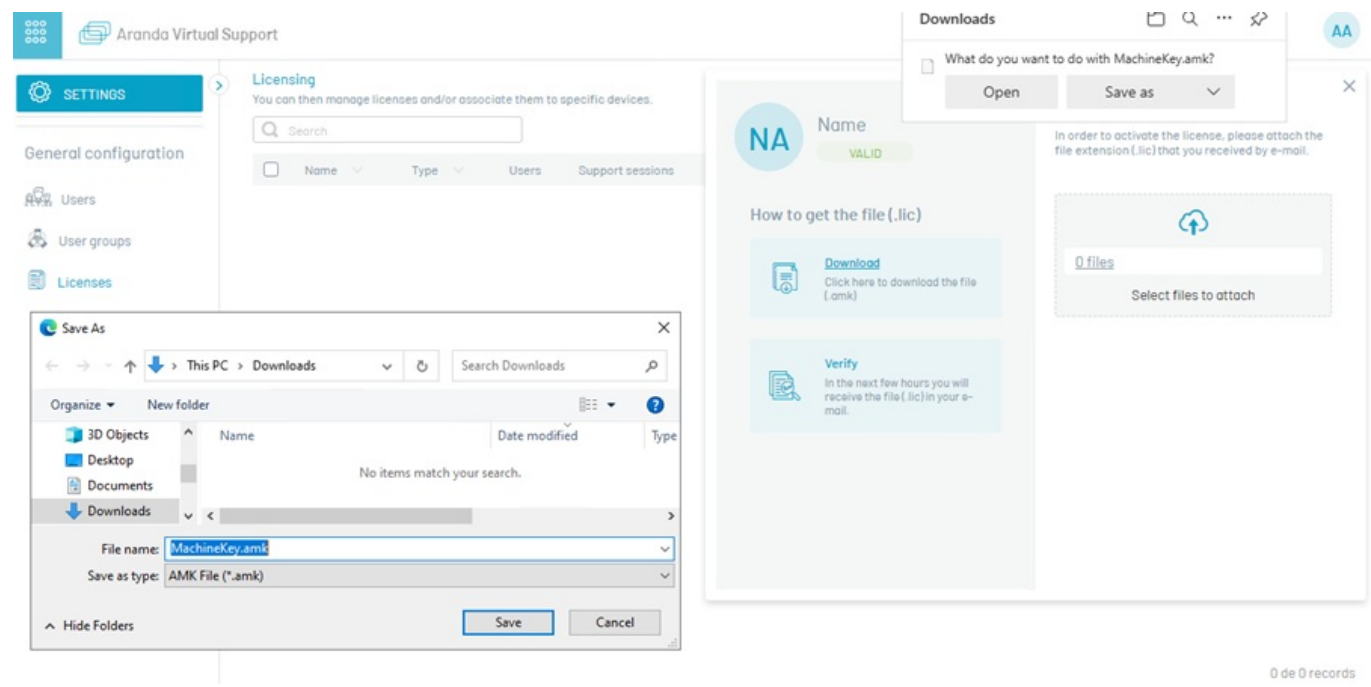
Todos os produtos da Aranda Software exigem uma licença para operar, portanto, na primeira vez que você entrar no site do Aranda Virtual Support (AVS), selecione a opção Certificados No menu principal, você pode adicionar novas licenças e visualizar a lista de licenças existentes agrupadas com os seguintes dados:

Coluna	Descrição
Nome	É o nome do produto Aranda atribuído à licença.
Cara	Tipo de licença.
Usuários	Número de usuários simultâneos (número de licenças usadas/número total de licenças).
Sessões de suporte	Número de sessões de suporte simultâneas (número usado/número total de licenças).
Dispositivos	Número de estações de trabalho simultâneas (número de licenças usadas/número total de licenças).
Empresa	Empresa proprietária da licença.
Data de ativação	Data em que as licenças são ativadas.
Data de validade	Data de expiração das licenças.

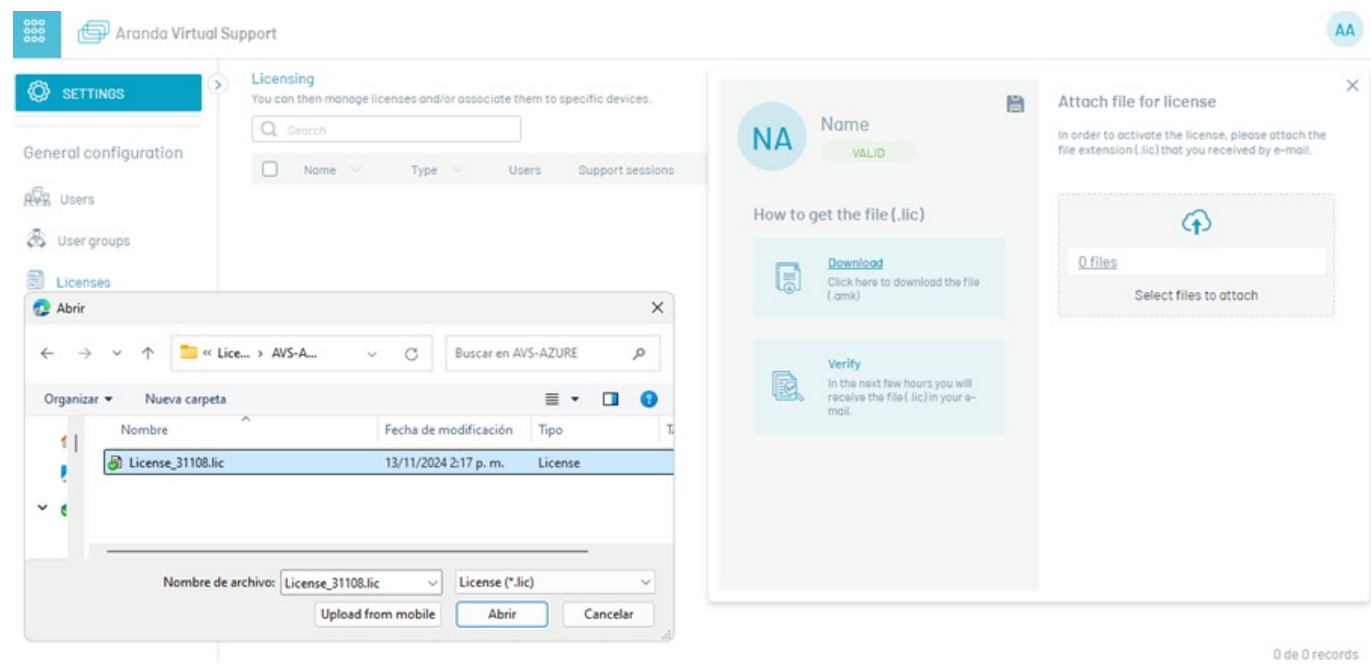
Na janela Licenciamento, clique em NOVA LICENÇA.



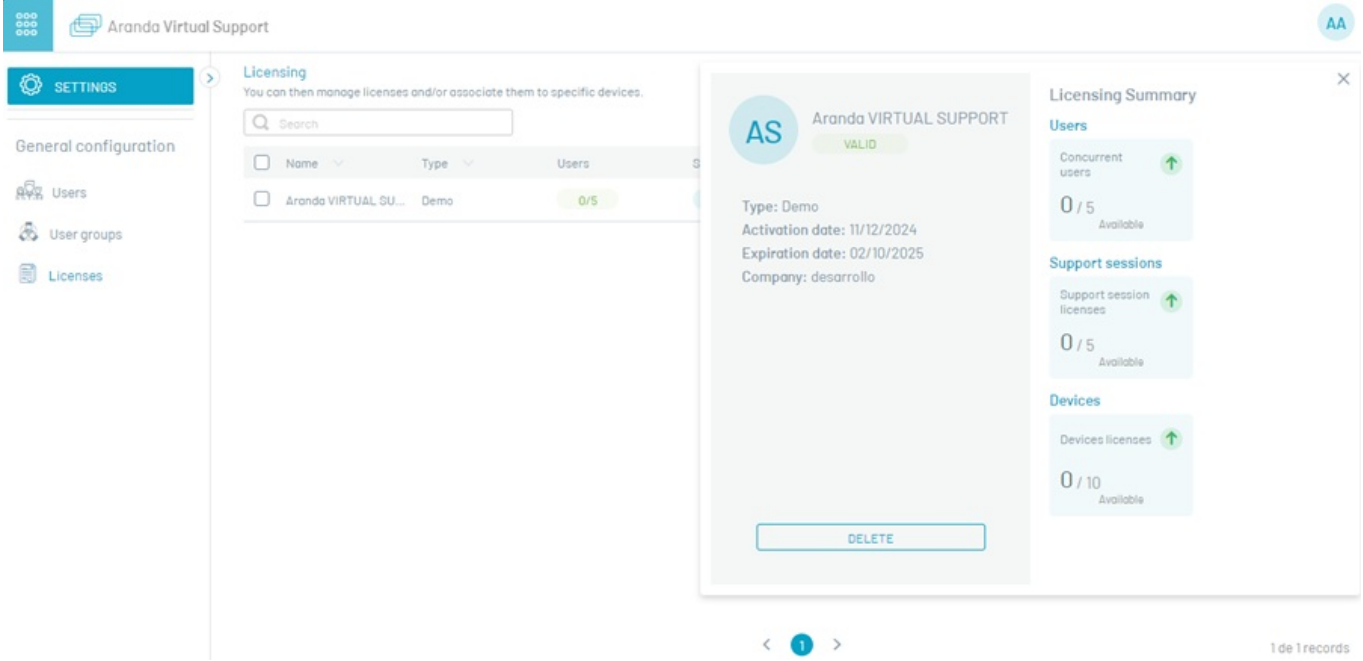
Na janela pop-up, selecione a opção Baixar, que permite o download do arquivo MachineKey.amk, que deve ser enviado para a área responsável pela Aranda Software (Pré-Vendas e Projetos) para a geração do arquivo .lic (arquivo de licenciamento).



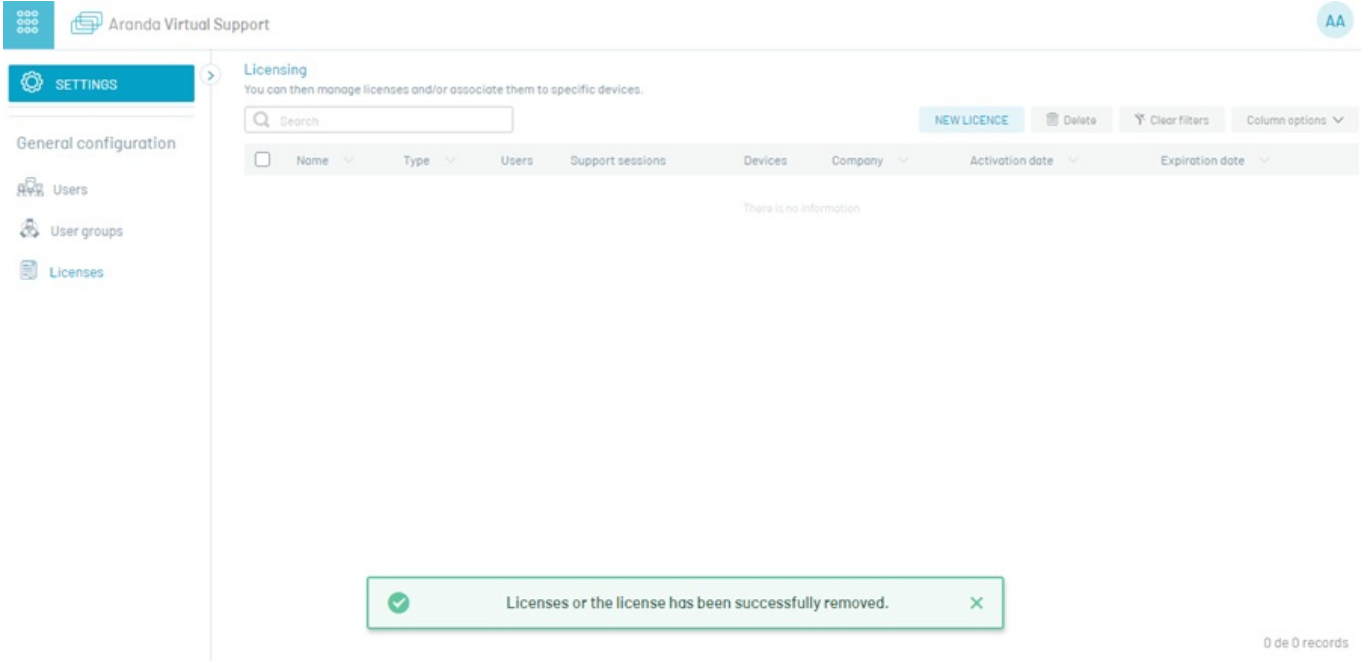
Depois de receber o arquivo .lic, você deve carregá-lo no servidor, clique no botão Selecione os arquivos a serem anexados e depois em Salvar (icone em forma de disquete). Quando a licença é carregada, o alerta correspondente é gerado.



Para saber em detalhes a licença, na janela Licenciamento, selecione um registro na lista de licenças disponíveis e, na janela habilitada, você poderá exibir a validade da licença e o número de licenças que foram usadas por usuários, sessões de suporte e dispositivos simultâneos (Número de licenças usadas/número total de licenças).



Para excluir uma licença, na seção Licenciamento Selecione o registro de licença que deseja excluir e clique no botão Eliminar, será confirmado que a licença foi excluída com sucesso.



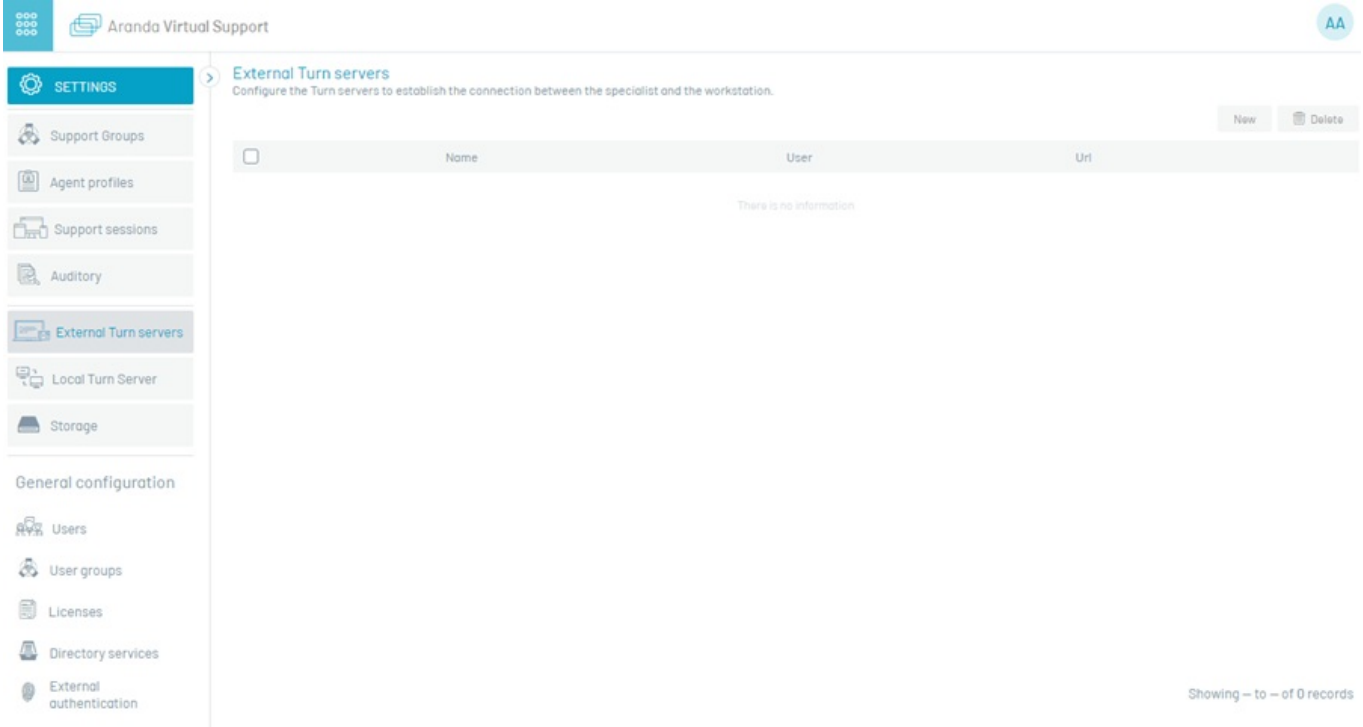
Configurações subsequentes

Configuração de infraestrutura

Após a instalação dos sites e serviços do Aranda Virtual Support (AVS), é necessário fazer algumas configurações no site do AVS para garantir o correto funcionamento do aplicativo durante os processos de controle remoto e transferência de arquivos. Portanto, é recomendável seguir os seguintes passos:

1. Entre no site

Faça login no site do AVS com um usuário que tenha a função de Administrador Geral ou Infraestrutura. Essas funções têm as permissões necessárias para gerenciar as opções External Turn Servers, Local Turn Server e Storage. É importante observar que essas opções estão disponíveis apenas nas instalações On Premise.



2. Servidores de turno externos

A funcionalidade de transferência de arquivos AVS 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:

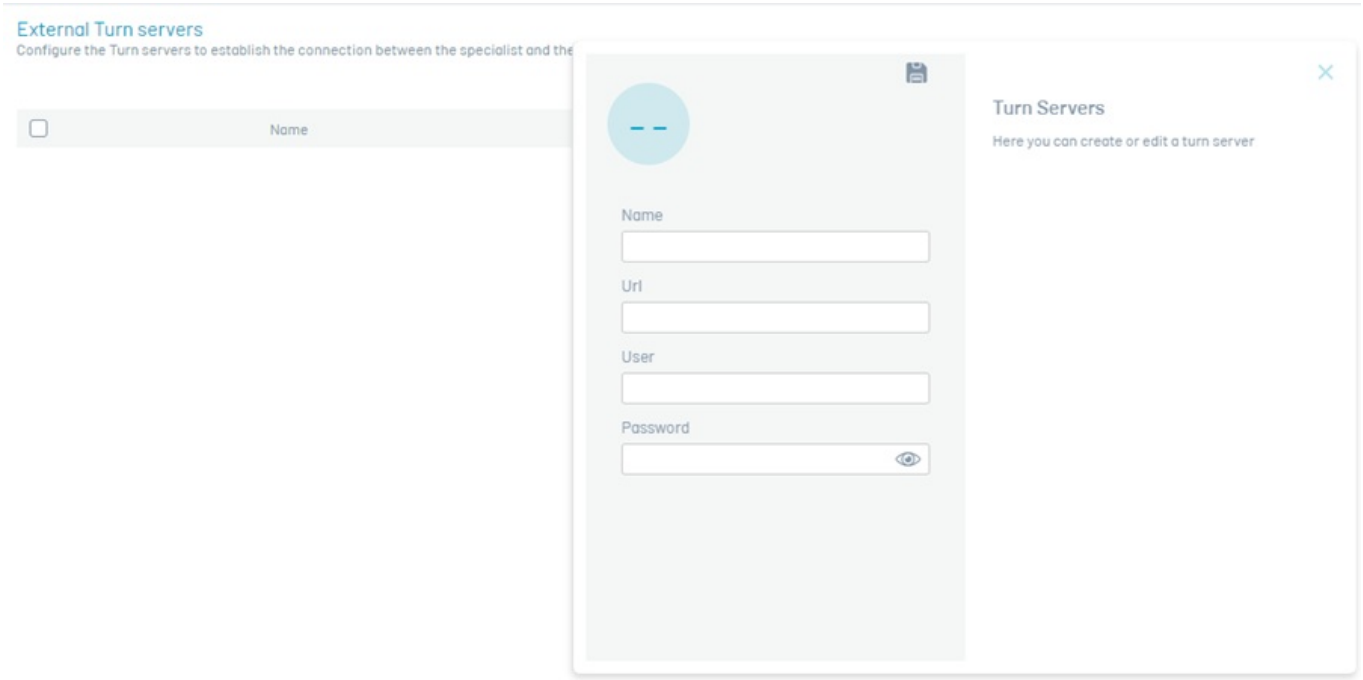
A. Clique na opção Novo.

B. Preencha os campos solicitados de acordo com a tabela a seguir:

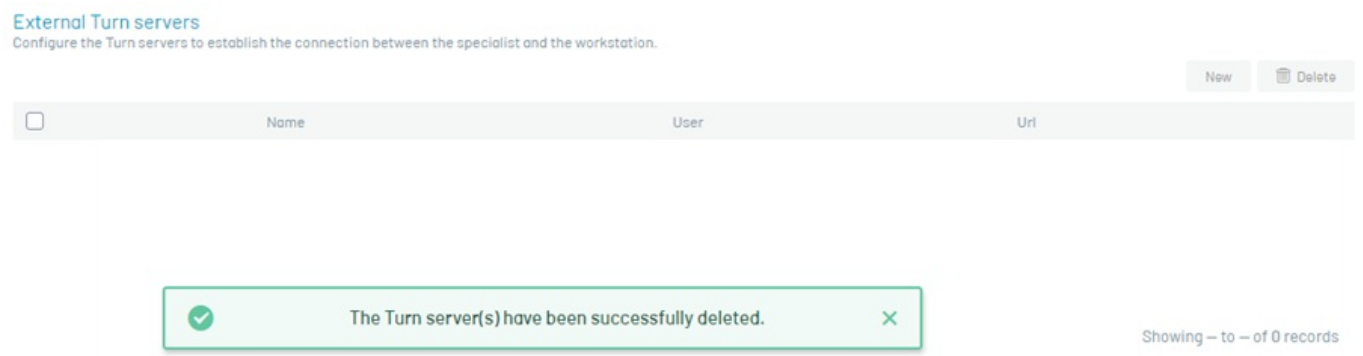
Campo	Descrição
Nome	Nome que você deseja atribuir à configuração, entre 6 e 50 caracteres.
URL	Corresponde ao site do servidor STUN/TURN, por exemplo: turn:<server_public_ip>:puerto ou stun:<server_public_ip>:puerto .
Utilizador	Nome do usuário autorizado a se conectar ao servidor STUN/TURN.
Senha	Senha 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 Turn externos que julgar necessários (máximo 10) para ter uma boa comunicação entre os dispositivos do especialista e a estação de trabalho através do console AVS. 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 sucesso.



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.

3. Ativar servidor local

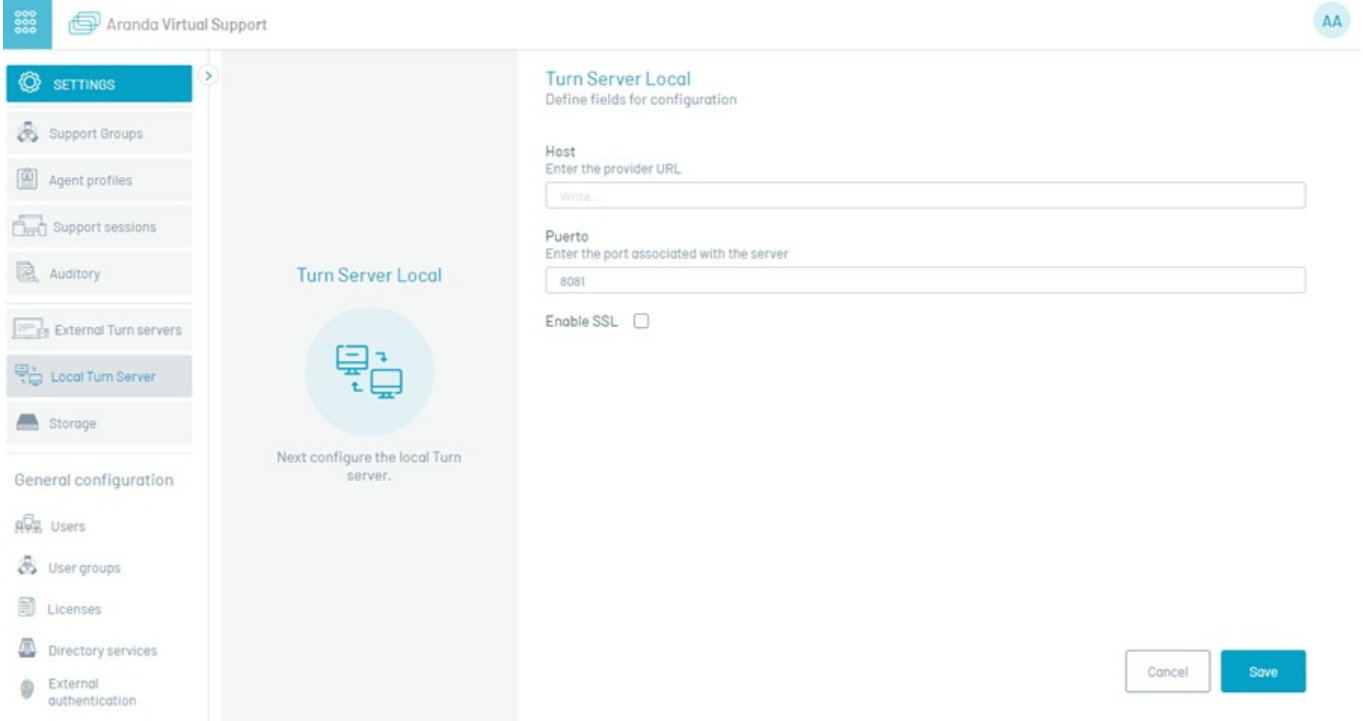
Para estabelecer a comunicação de controle remoto entre o agente especialista e o agente da estação de trabalho, use um servidor Turn local que possa retransmitir o tráfego de rede.

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 está configurado por padrão com o valor 8081 e o SSL está inativo, se a porta for alterada ou o SSL estiver ativado, o seguinte deverá ser [faça as configurações no serviço Aranda AVS Turn Server](#) instalado no servidor.

C. Finalize clicando no botão Salvar

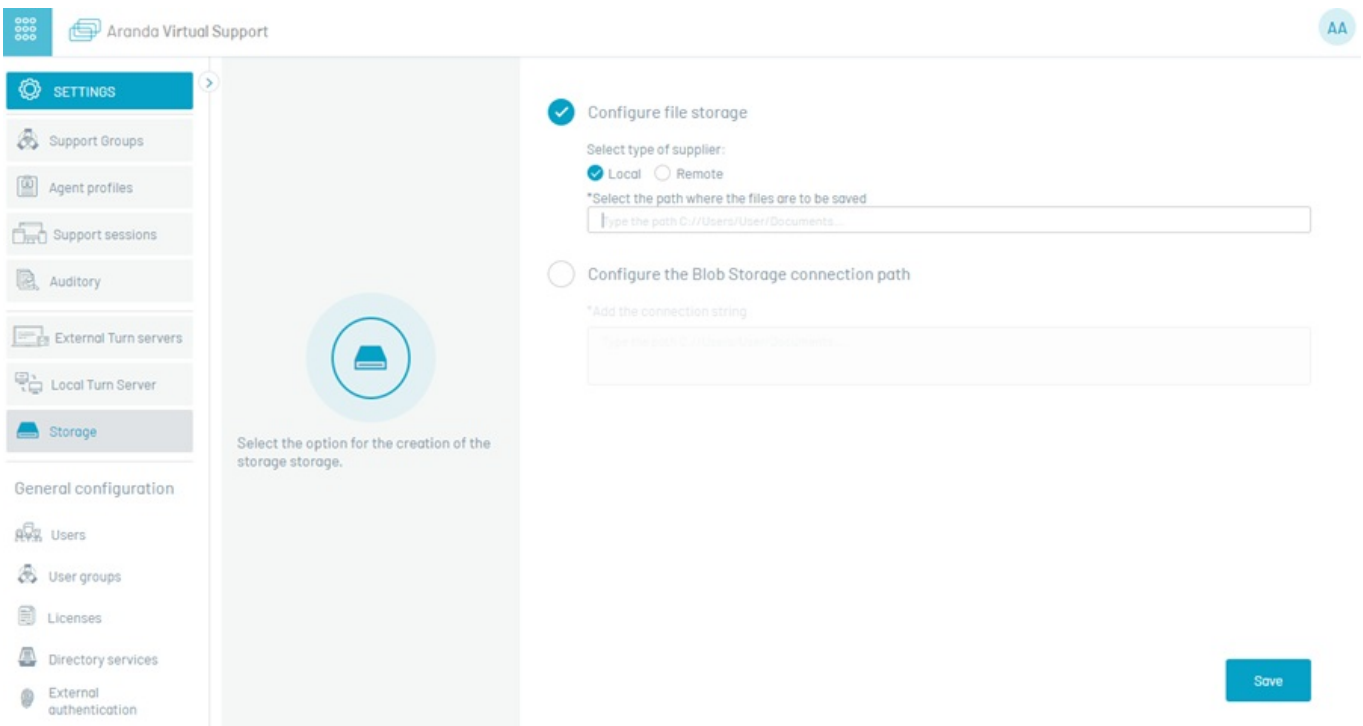


4. Armazenamento

Essa configuração é necessária para armazenar gravações da Entrega de Serviço de Controle Remoto e Instaladores de Agente para estações de trabalho. Os arquivos gerados são enviados para um provedor de armazenamento. O provedor pode ser de três tipos: local, remoto ou armazenamento de blobs.

Para configurar seu provedor de armazenamento, siga estas etapas:

- A. Clique na opção Armazenamento no menu principal.
- B. Preencha o(s) campo(s) solicitado(s) dependendo do tipo de armazenamento selecionado.
- C. Finalize clicando no botão Salvar



📌 Anotações:

- Para que as gravações sejam armazenadas corretamente, o servidor onde o site está instalado será Avs e arco/gravação Você deve ter acesso ao provedor configurado. Se você estiver usando o provedor de tipos local, o caminho deverá existir no servidor e ter as permissões correspondentes.
- Para que os instaladores sejam armazenados corretamente, o servidor em que os serviços comuns estão instalados (Trabalhador) deve ter acesso ao provedor configurado. Se você estiver usando o provedor de tipos local, o caminho deverá existir no servidor e ter as permissões correspondentes.
- Se o Trabalhador e o site do Agentes estão instalados em servidores separados, deve-se garantir que ambos possam acessar o armazenamento configurado, para que a atualização do agente seja realizada corretamente.
- Se, após a configuração, forem feitas alterações no provedor de armazenamento, é necessário mover as informações contidas no provedor anterior para o atual. Se essa ação não for executada, as atualizações do agente não serão bem-sucedidas e as gravações não estarão acessíveis nas auditorias.

Configuração manual de serviço

Configurando o Turn Server

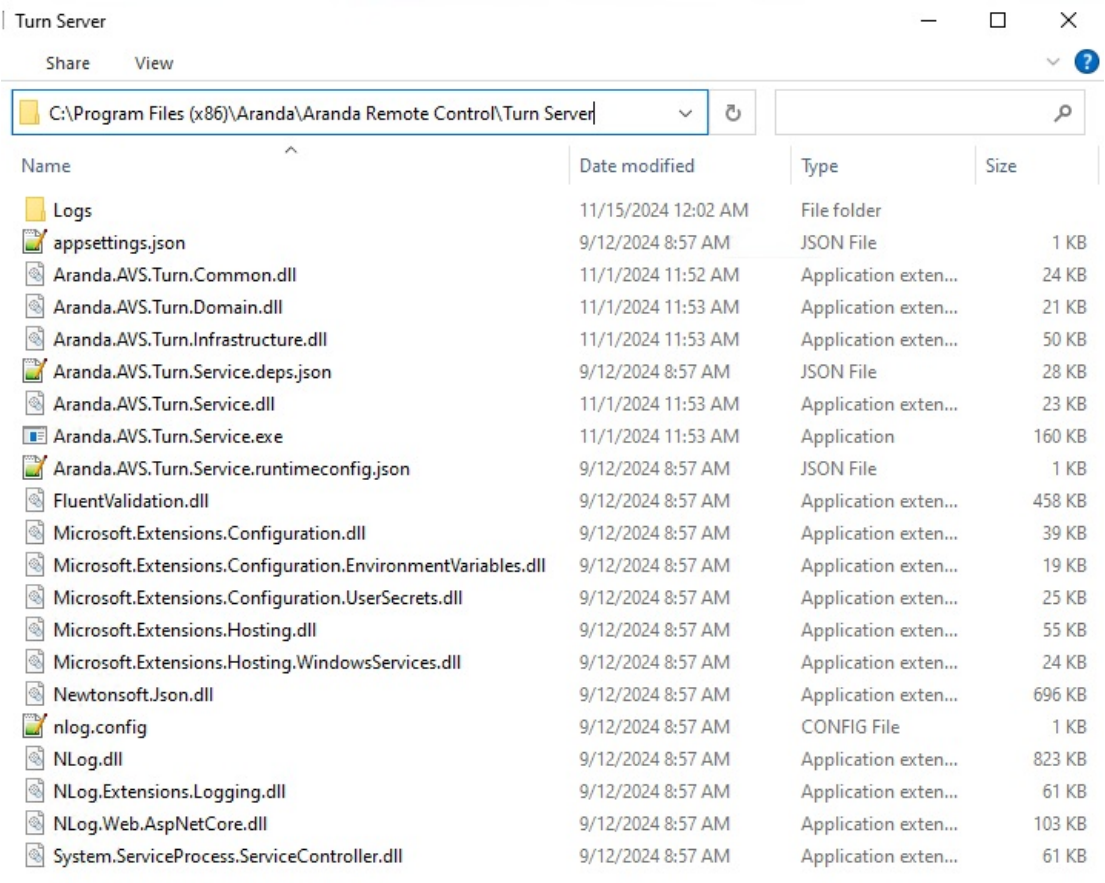
↩ Ativar servidor local

Depois de instalar o serviço Aranda AVS Turn Server, você não precisa fazer nenhum ajuste para seu funcionamento. 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

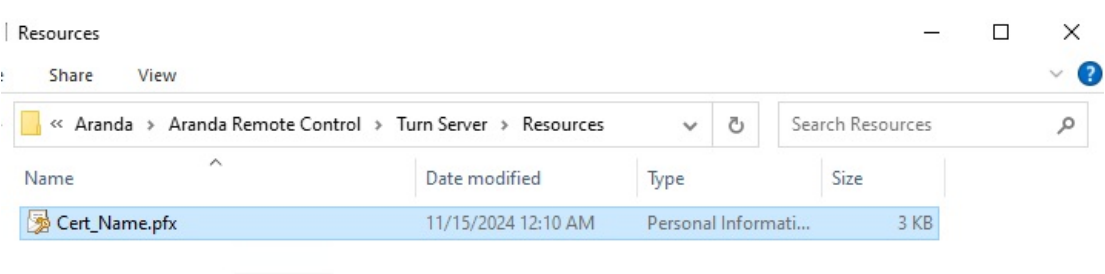
Edite o arquivo appsettings.json e configure a porta desejada substituindo <puerto> pelo número de porta desejado.

```
"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. Adquirir ou gerir 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 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": "<nome-certificado>",
"IsSsl": true,
"Port": 8081,
"SSLProtocols": "Tls12"
}
```

4. Reinicialização do serviço

Reinicie o serviço Turn Server (Aranda AVS Turn Server) 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.

[← Ativar servidor local](#)

Configurando o servidor WebRTC STUN/TURN

[← Servidor TURN externo](#)

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.

Em estações de trabalho (AVS Agent) e em computadores especializados (Specialist Agent), eles devem permitir a saída através das portas configuradas.

Além disso, se você precisar que ele opere como TURN WebRTC, deverá abrir o intervalo de portas 49152–65535 para o protocolo UDP.

[Exemplo e cenários de configuração de serviço STUN/TURN](#)

[← Servidor TURN externo](#)

Exemplo e cenários de configuração de serviço STUN/TURN

[← Servidor TURN externo](#)

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]
# Credenciais para autenticação 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 AVS	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 AVS 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 AVS 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 AVS 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 AVS 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 AVS não conseguem estabelecer comunicação devido a um problema de conectividade entre 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 AVS 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 AVS](#) 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 AVS](#) 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.

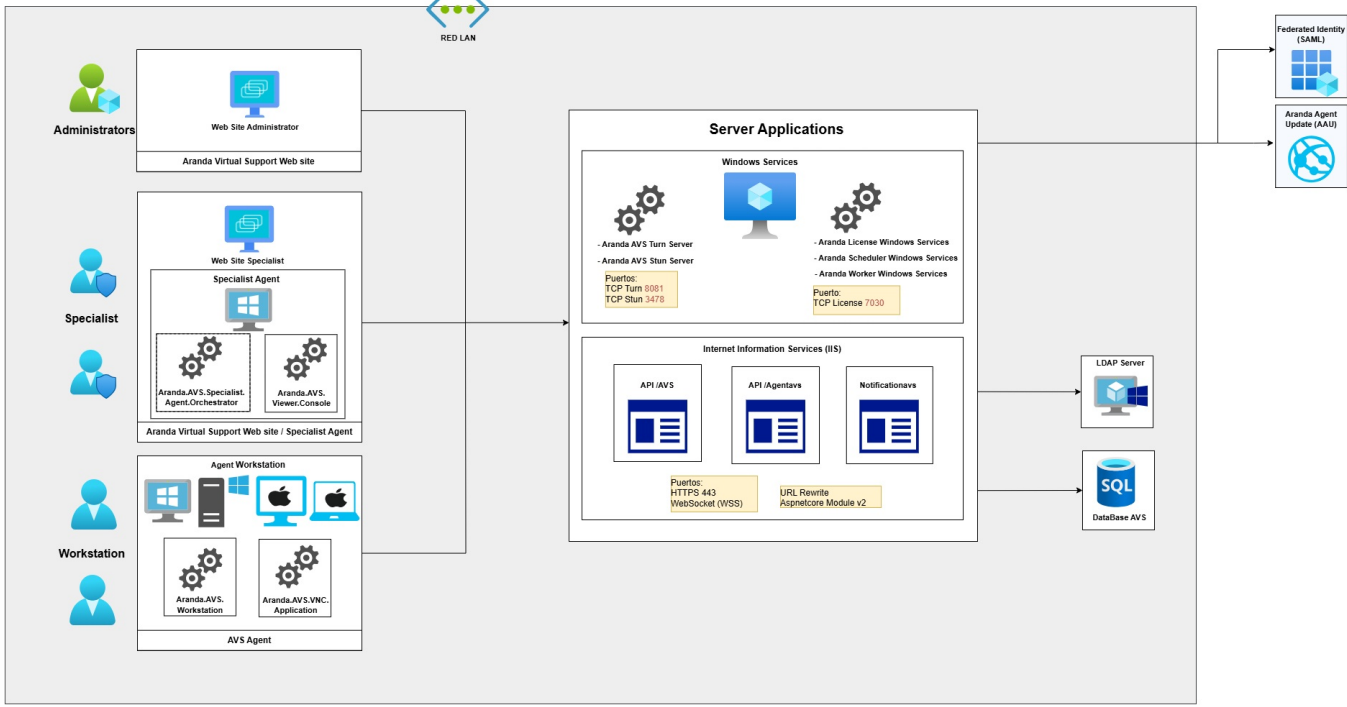
[↩ Servidor TURN externo](#)

Implantação

Diagrama de implantação

1. Diagrama

A figura a seguir mostra o diagrama de implantação:



2. Servidores

A instalação do servidor é composta pelos seguintes elementos:

Serviços do Windows: Permitem a execução de tarefas, agendas, entre outras funcionalidades em segundo plano.

- Aranda AVS Turn Server: Permite a conexão das pontas em uma sessão de controle remoto. Requer escuta na porta 8081, embora possa ser configurado. Usa o protocolo TCP configurável para usar SSL/TLS
- Aranda AVS Stun Server: Permite que você tenha um servidor WebRTC atordoado/girado para funcionalidade de transferência de arquivos. Ouça pelo menos na porta 3478 por TCP e UDP. Para permitir a retransmissão, mais portas podem ser configuradas por TCP ou UDP.
- Serviços comuns: Serviços comuns de aplicativos Aranda.

Aplicativos Web: Eles permitem que aplicativos da Web sejam expostos por HTTPS. Todos eles usam a porta TCP 443. É necessário ativar o HTTPS

- API/AVS: Fornece os recursos da página inicial do produto de Suporte Virtual.
- API/Agentavs: Permite registrar e atualizar estações de trabalho.
- Notificationavs: Permite o envio de mensagens entre especialistas e estações de trabalho. Usa o protocolo WebSocket

Servidor de banco de dados: SQL Server Persiste dados estruturados

3. Usuários

Administradores: Gerencie as configurações do produto. Eles usam um navegador da web.

Especialistas: Eles usam serviços de suporte, como controle remoto, transferência de arquivos e bate-papo

- Site: Use funcionalidades de suporte
- Aranda.AVS.Viewer.Console: Visualizador que permite o controle remoto em estações de trabalho.
- Aranda.AVS.Specialist.Orchestrator: Um serviço do Windows que permite a funcionalidade de transferência de arquivos e o envio de gravações de controle remoto.

Estações: Eles recebem ajuda por meio das funcionalidades de suporte. Suporte para Windows e Mac OS

- Aranda.AVS.Workstation: serviço do Windows que oferece as principais funcionalidades
- Aranda.AVS.VNC.Application: Um serviço do Windows que permite que você assuma o controle remoto.