
Aranda Virtual Support

title: Guía de Instalación AVS On Premise permalink: / —

Esta guía detalla los pasos necesarios para la instalación y configuración de Aranda Virtual Support (AVS) en un entorno local. AVS es una aplicación de soporte remoto desarrollada por Aranda Software que permite tomar control remoto y transferir archivos en tiempo real y de forma segura a estaciones de trabajo. \n## Pre requisitos — title: Pre requisitos chapter: "pre_requisitos" —

Requisitos del sistema

Los siguientes requerimientos se definen para la implementación de Aranda Virtual Support en una instalación en entorno local.

	Servidor de Aplicaciones Web / Servicios
Dedicación	Uso dedicado para AVS (No compartir su uso con otras aplicaciones)
Almacenamiento	- **Espacio Requerido**: Mínimo 64GB - **Tipo de Unidad**: Unidad de Estado Sólido(SSD) - **Particiones**: Se recomienda partición dedicada para la instalación del sitio. Se recomienda una partición dedicada para la base de datos (archivos MDF y LDF)(*) * En el caso de instalación de la solución en el mismo servidor donde reside la base de datos.
Procesamiento	4 CPU / 8 vCPU 2.1 GHz o superior.
Conectividad	Tarjeta de red Gigabit Ethernet (1GBps o superior)
Base de datos	**Versiones**: SQL Server 2019, SQL Server 2022 **Ediciones**: Estandar (para Entornos de Pruebas), Enterprise (para Entornos Productivos) y Express (sólo para Pruebas de Concepto). **Licenciamiento**: Se recomienda licenciar la base de datos por Core. **Collation**: SQL_Latin1_General_CP1_CI_AI **Permisos**: Usuario para la creación de la base de datos (DBTools): Miembro del rol fijo*db_owner*. Usuario de servicio de la base de datos: Miembro del rol fijo *db_datareader* y *db_datawriter*. Permisos de ejecución sobre el esquema dbo
Sistema Operativo	**Versión**: Windows Server 2019, Windows Server 2022. **Edición**: Estándar o Superior. **Cuenta de Instalación**: Se requiere credenciales de administrador local y/o de dominio para la instalación.
Protocolos	- La aplicación funciona solo con HTTPS. - Se debe habilitar Websockets en toda la red. Lo requerido para que WebRTC opere correctamente.
Puertos de entrada	- Se debe habilitar el puerto para hace uso de HTTPS (por ejemplo 443). - Así mismo el puerto configurado para el turn y stun server.
Servicio de actualización	El servidor del Worker debe configurarse para poder alcanzar el sitiohttps://download.arandasoft.com/updates y descargar archivos.

Requerimientos adicionales

- Internet Information Services (IIS) 10.0 o superior.
- Roles
  - File and Storage Services
    - Storage Services
  - Web Server
    - Common HTTP Features
      - Default Document
      - Directory Browsing
      - HTTP Errors
      - Static Content
    - Health and Diagnostics
      - HTTP Logging
    - Performance
      - Static Content
    - Security
      - Request Filtering
    - Application Development
      - WebSocket Protocol
  - Management Tools
    - IIS Management Console
- Características
  - .NET Framework 4.8 Features
    - .NET Framework 4.8
    - WCF Services
      - TCP Port Sharing

- BitLocker Drive Encryption
- Enhanced Storage
- Microsoft Defender Antivirus
- System Data Archiver
- Windows PowerShell
  - Windows PowerShell 5.1
- WoW64 Support
- XPS Viewer

- Módulo URL Rewrite versión 2.1 o superior Ver página de descarga
- ASP.NET Core Runtime 6.0.31 Hosting Bundle Ver página de descarga

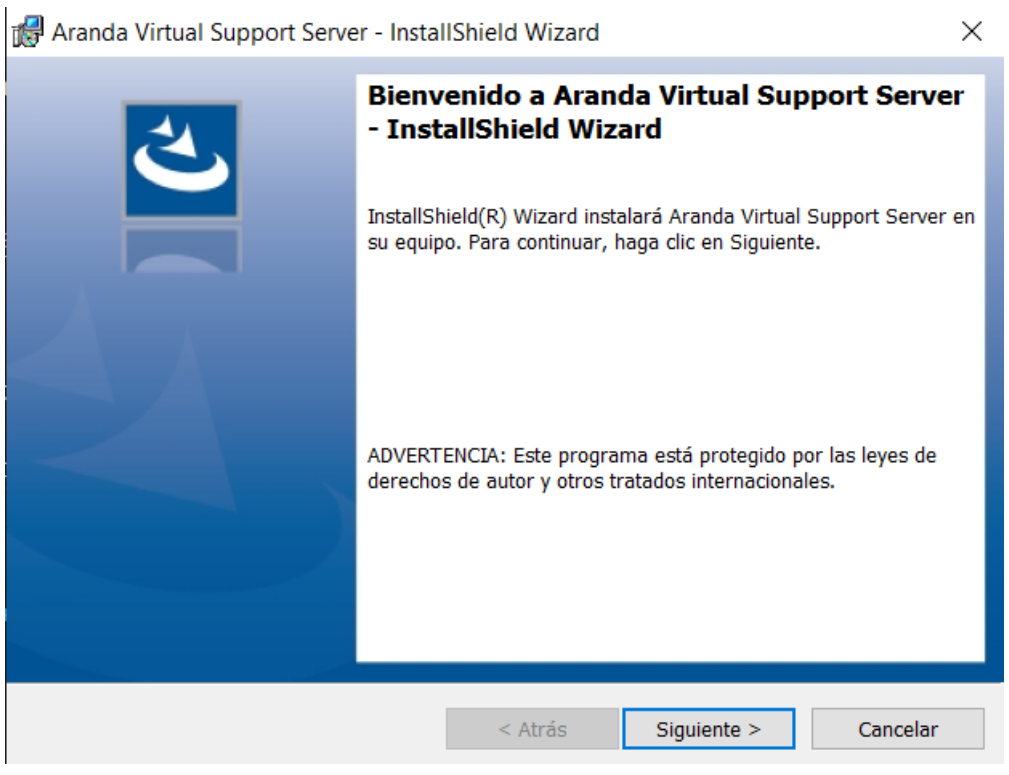
⚐ **Nota:** Antes de iniciar la instalación de Aranda Virtual Support es necesario crear el esquema de base de datos a través del módulo **Aranda Database Tools v9**.

Consulte el Manual de usuario de **Aranda Database Tools V9**

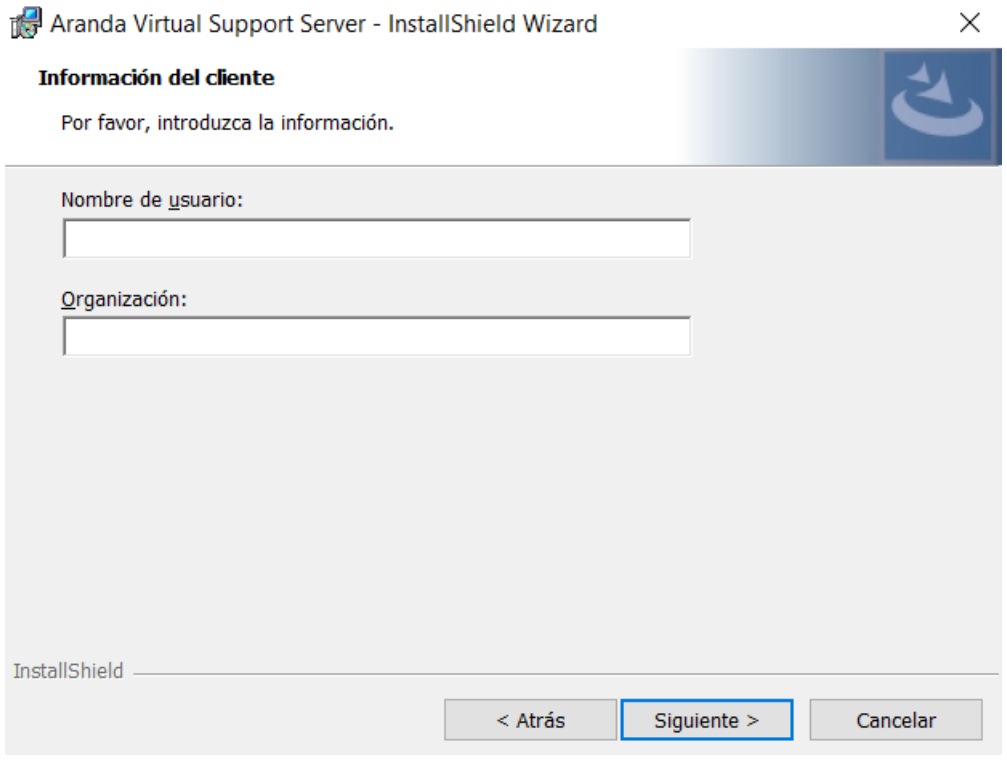
\n## Servicio de licenciamiento — title: Servicio de licenciamiento chapter: "pre_requisitos" — Aranda Virtual Support (AVS) utiliza el servicio común de licenciamiento de Aranda para autorizar el ingreso a usuarios al sitio web de AVS y controlar las licencias compradas, entre otras operaciones. Este es un servicio de Windows que normalmente es creado de manera automática por el instalador del producto. Una vez el usuario cargue desde el sitio web sus licencias compradas, el servicio común de licenciamiento debe permanecer en la misma máquina, de otra manera las licencias cargadas se perderán. Si su servidor de aplicaciones se encuentra ubicado en una máquina virtual se recomienda instalar el servicio común de licenciamiento en una máquina física, ya que al reiniciar máquinas virtuales existe una alta probabilidad de que la marca de hardware cambie y el servicio asuma incorrectamente que fue trasladado. Consulte con el proveedor para más detalles sobre el despliegue del servidor. \n## Instalación de AVS On Premise — title: Instalación de AVS On Premise chapter: "instalacion" —

El instalador **AVS.Server.Installer** instala tres sitios web (AVS, Notification, Recording) y cinco servicios (Aranda License Windows Service, Aranda Scheduler Windows Service, Aranda Worker Windows Service, Aranda AVS Turn Server y Aranda AVS Stun Server).

1. Haga doble clic sobre el archivo del instalador y visualizará la pantalla de bienvenida. Confirme la instalación haciendo clic en el botón **Siguiente.**



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

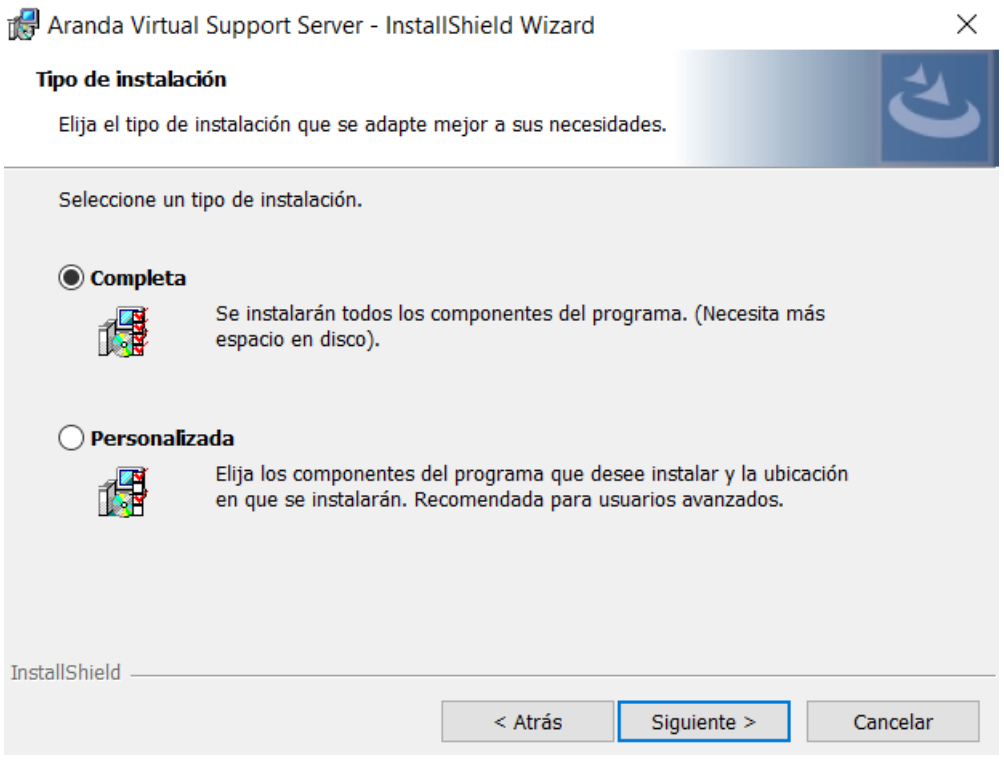


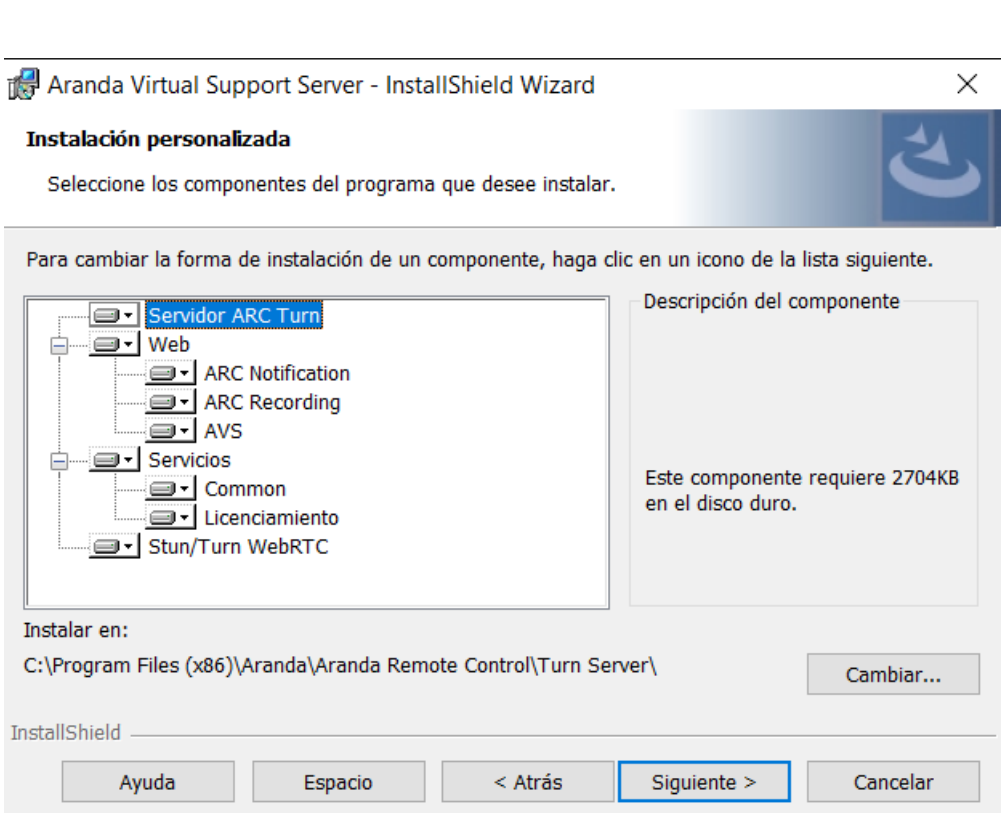
3. En la ventana **Tipo de instalación** podrá configurar las siguientes opciones:

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

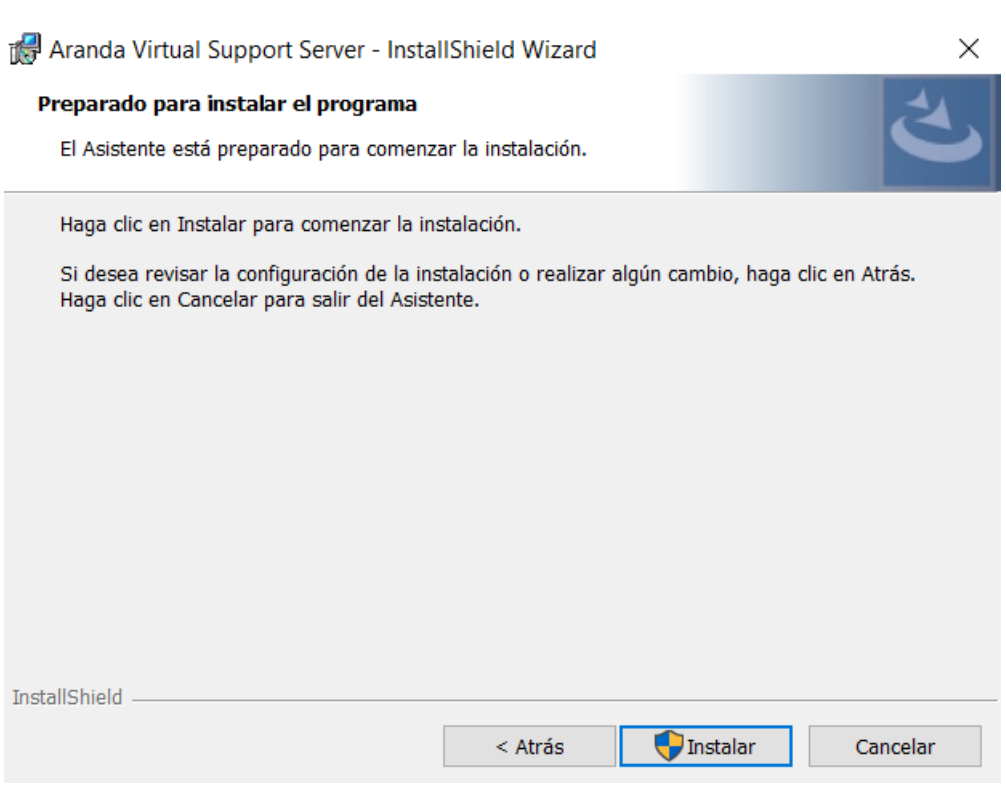
⚐ **Nota:** De forma predeterminada, seleccione el tipo de instalación **Completa**. En el caso de establecer separación de las capas de la solución (Web,

Aplicación) en servidores independientes, seleccione la opción **Personalizada**.





4. Configurado el tipo de instalación, en la ventana **Preparando para instalar el programa** haga clic en **Siguiente** y luego haga clic en el botón **Instalar**.



5. Al terminar el proceso de instalación, haga clic en el botón **Finalizar**.

\n## Configuración conexión con base de datos — title: Configuración conexión con base de datos chapter: "instalacion" —

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

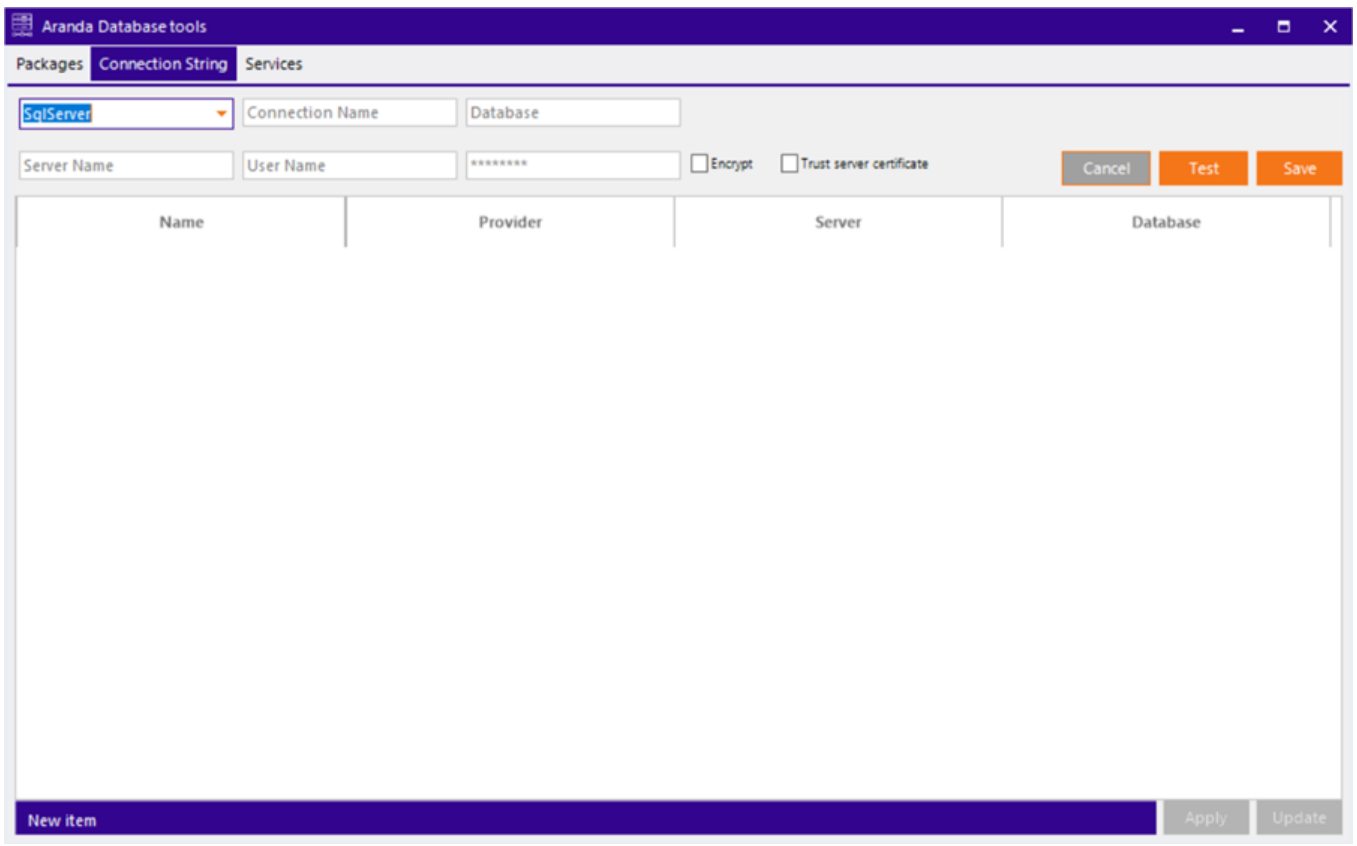
Para configurar los sitios web actualice el valor de la cadena de conexión, en la línea 6 dentro de los archivos appsettings.json de cada sitio; las rutas por defecto son:

```
C:\inetpub\wwwroot\arc\notification\appsettings.json

C:\inetpub\wwwroot\arc\recording\appsettings.json

C:\inetpub\wwwroot\avs\appsettings.json
```

Ejemplo de cómo debe quedar la cadena de conexión en el appsettings.json

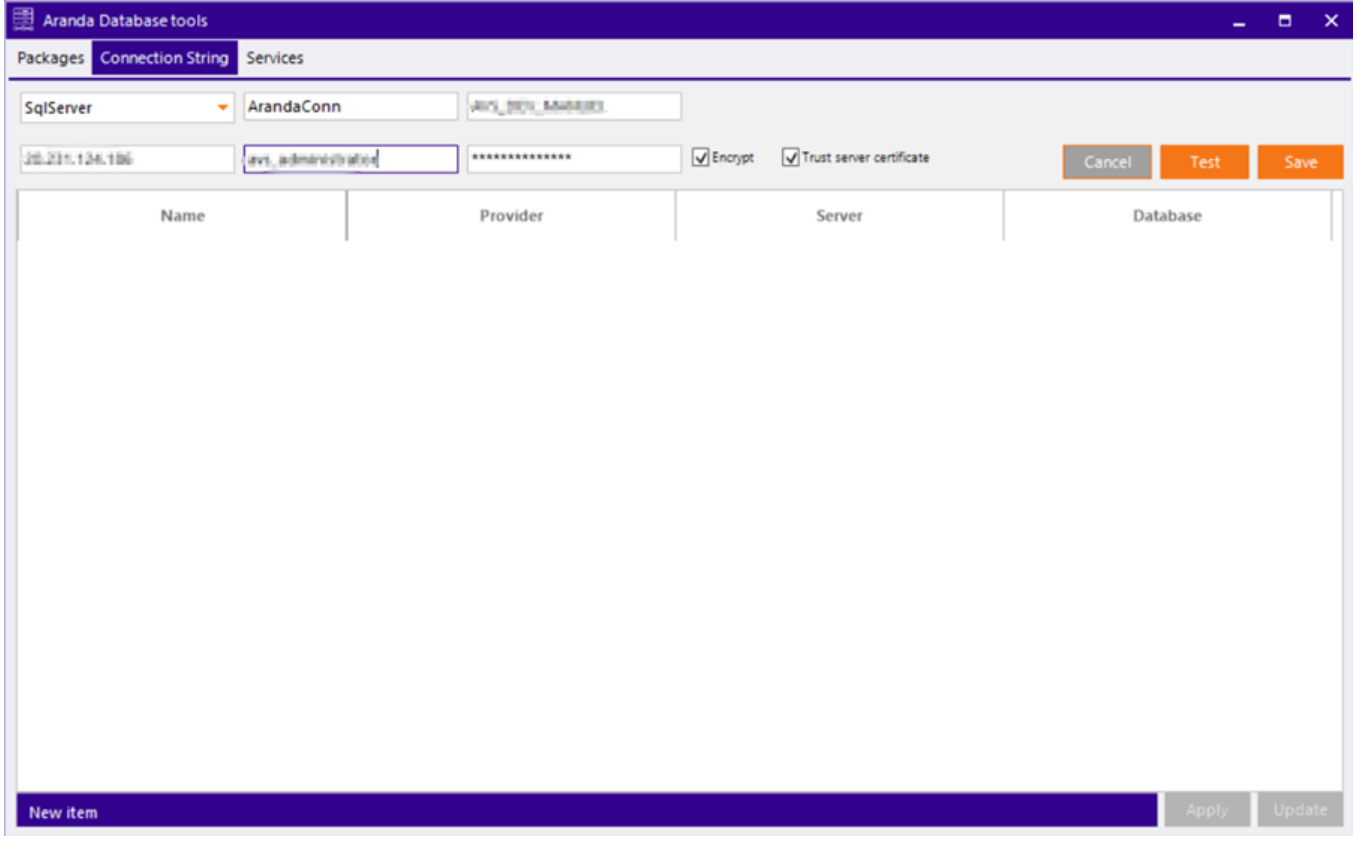
Para configurar los servicios Comunes y de Licenciamiento, se realiza a través del módulo **Aranda Database Tools v9**. Para ello:

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

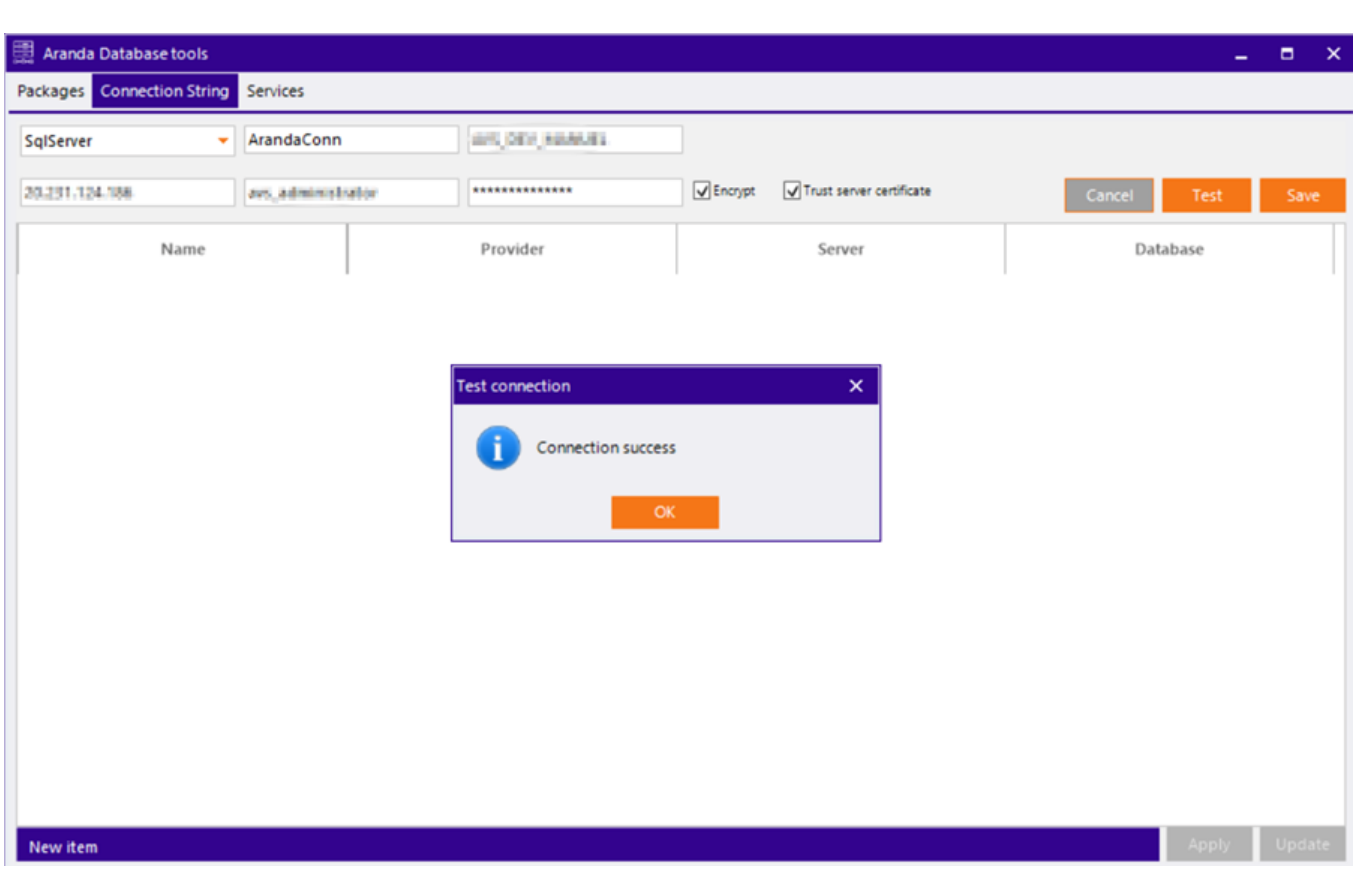


2. Complete los datos solicitados.

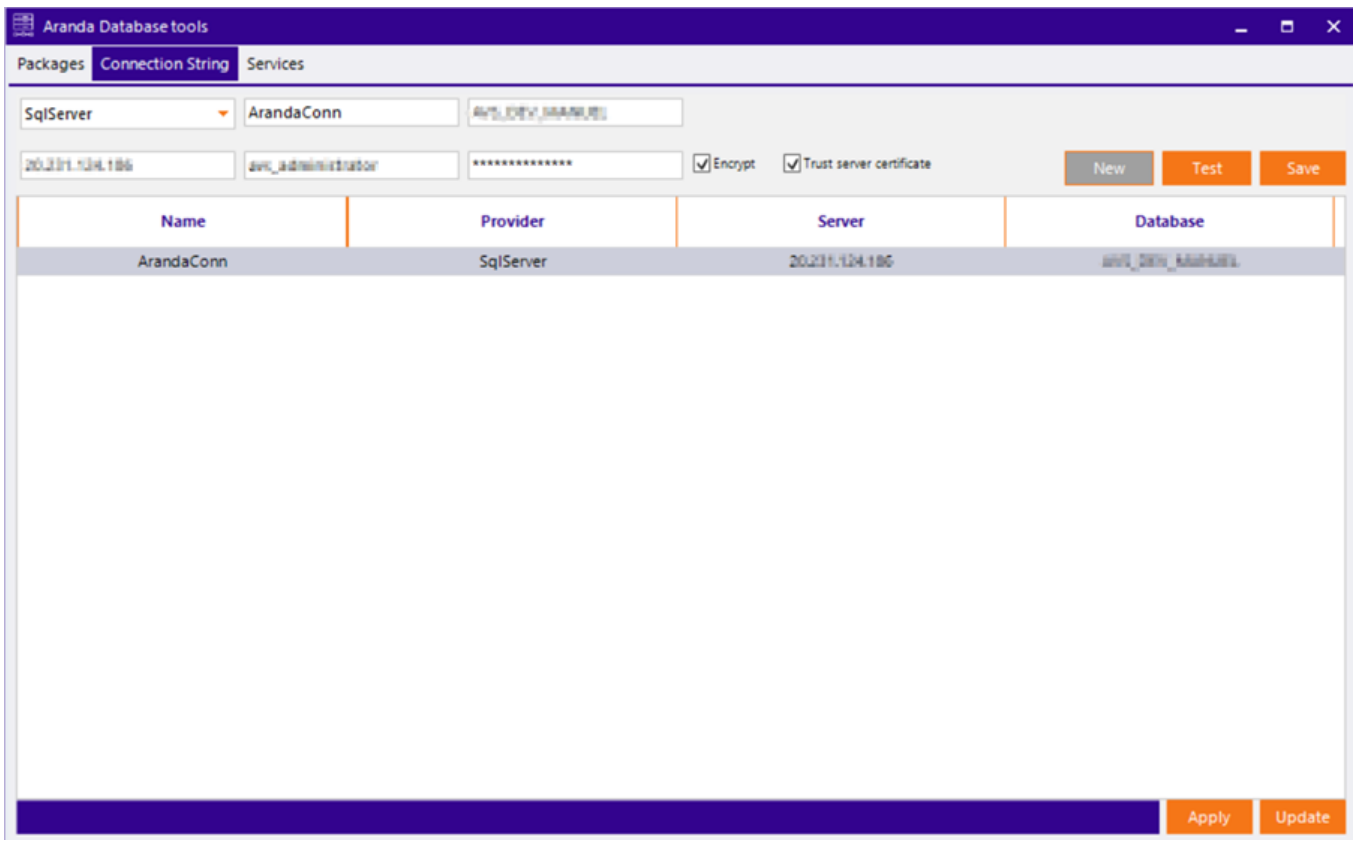
- Seleccione el motor de base de datos (SQL Server).
- Asigne un nombre para identificar la conexión.
- Registre los datos de conexión (nombre de la base de datos, nombre del servidor o dirección IP, y si se requiere usuario y contraseña).
- En caso que el puerto de base de datos sea distinto al puerto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



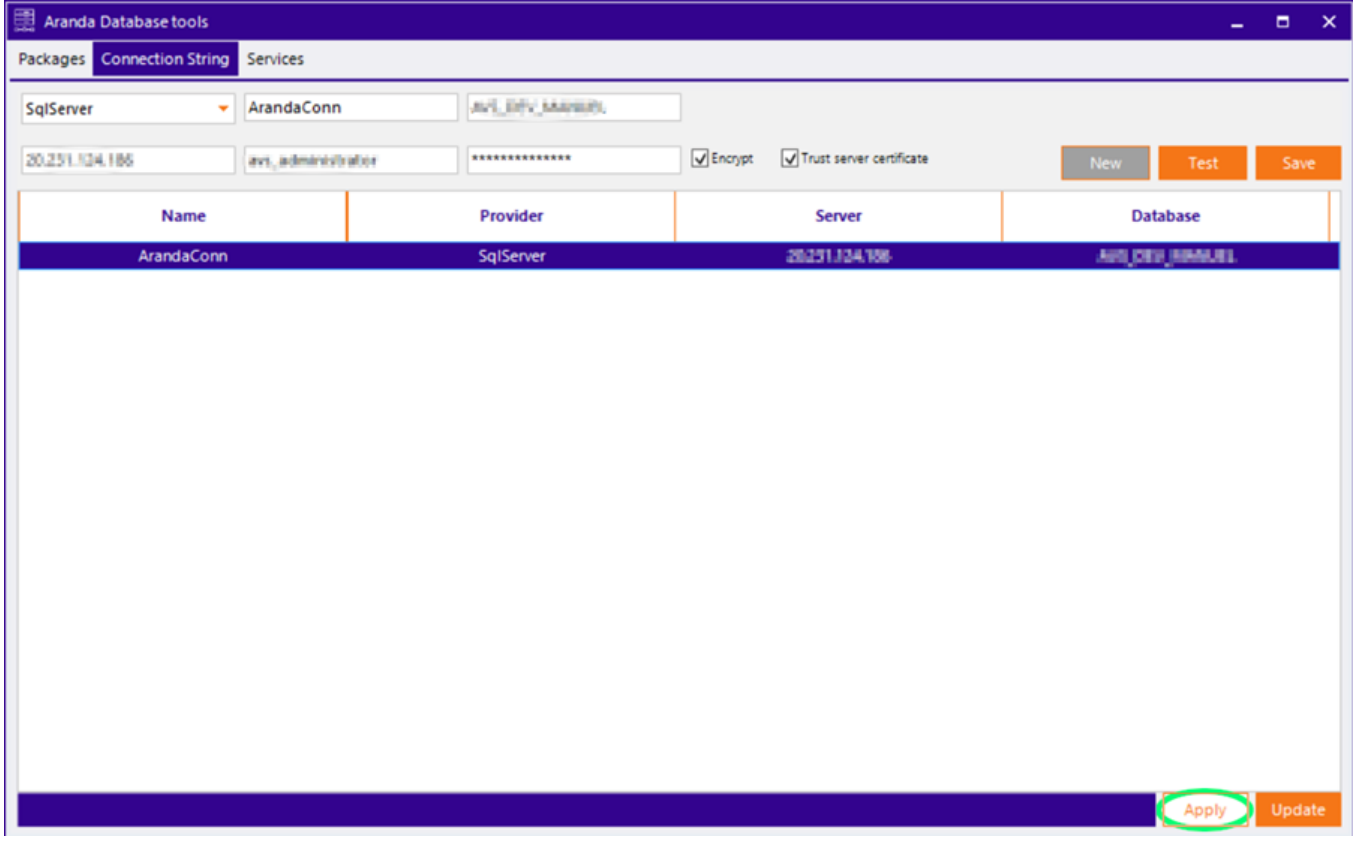
3. Haga clic en el botón**Test** para comprobar la conexión.



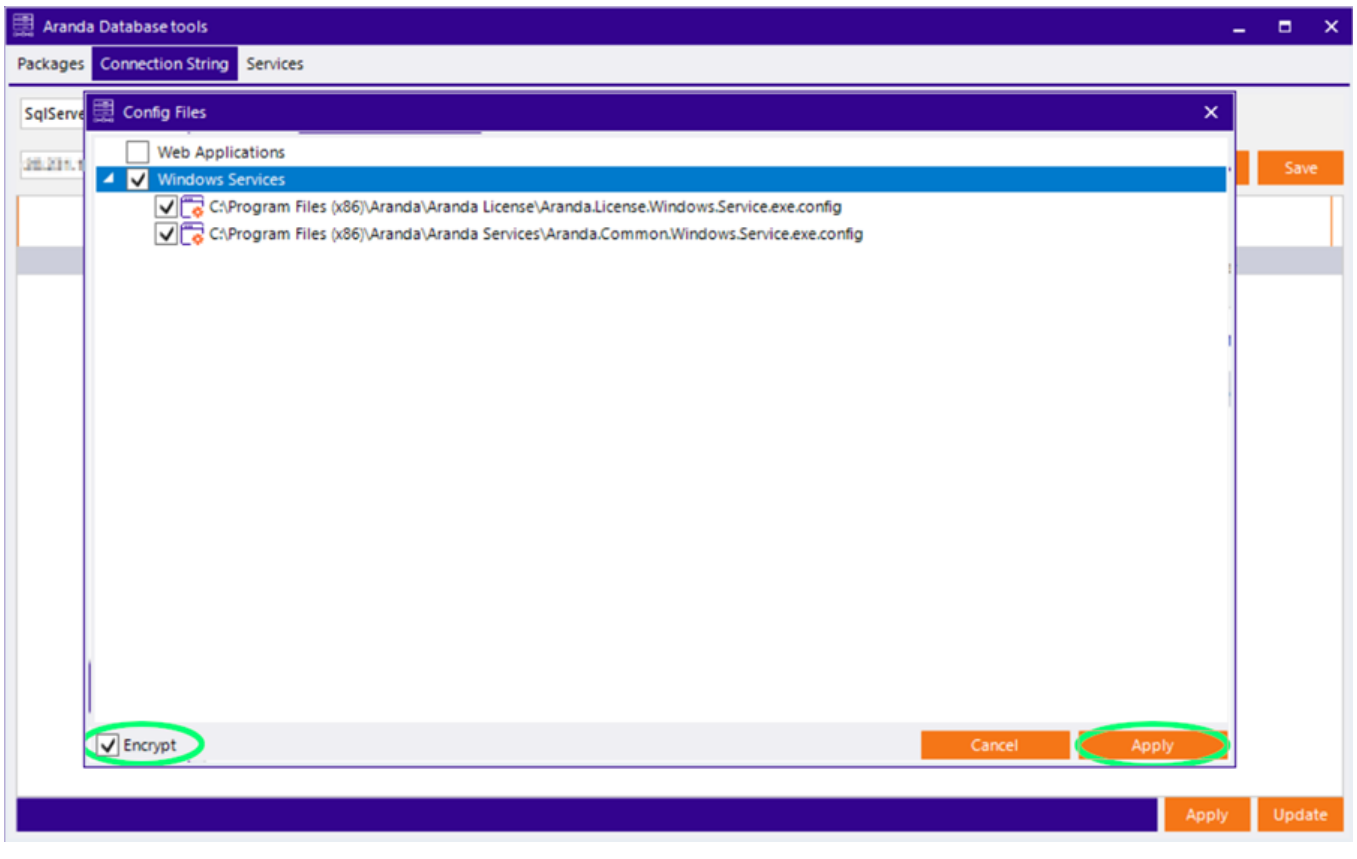
4. Para finalizar haga clic en el botón**Save** para guardar la conexión.



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

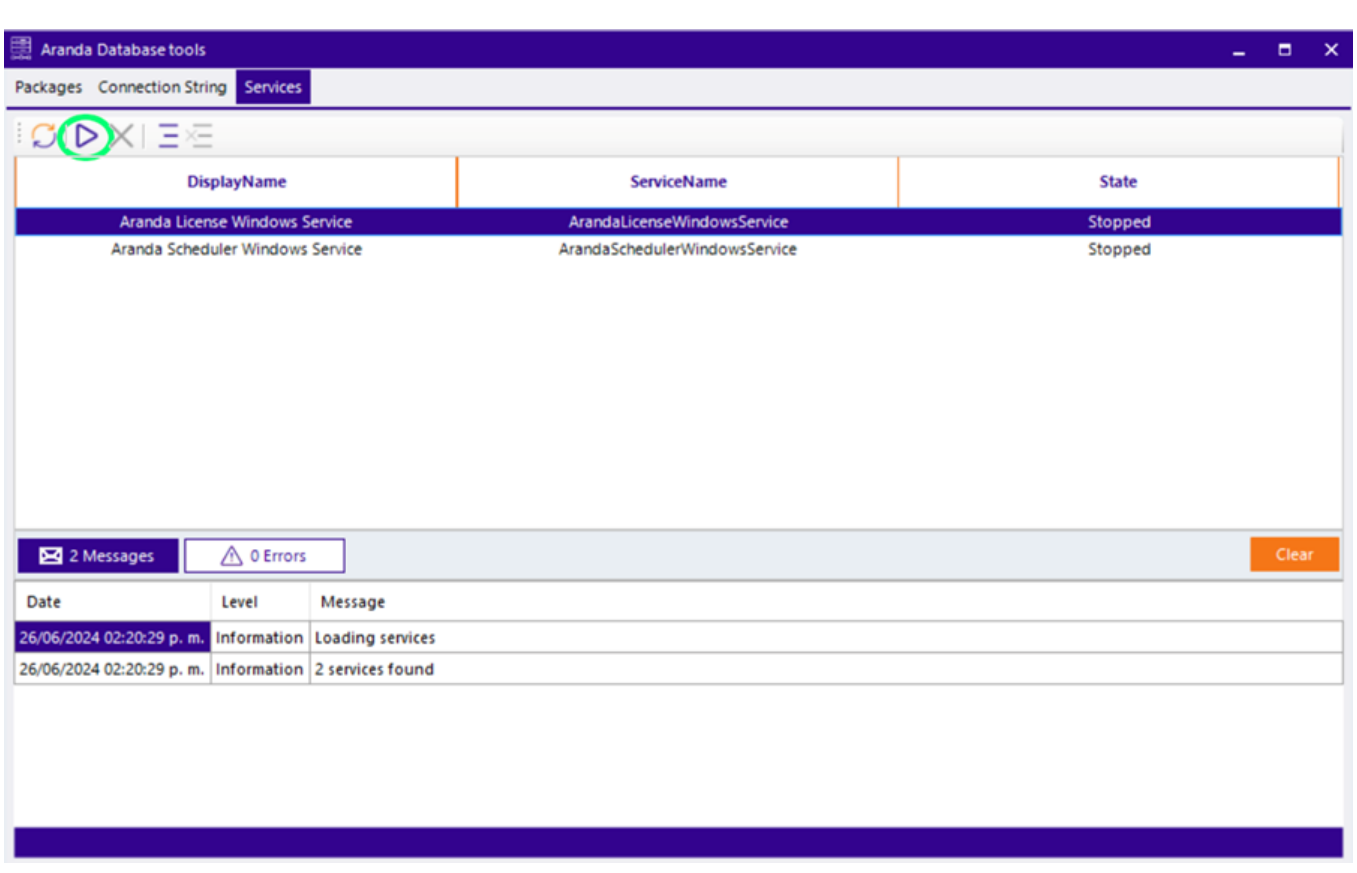


6. Se habilita una ventana con el listado de aplicaciones y servicios disponibles en el servidor.

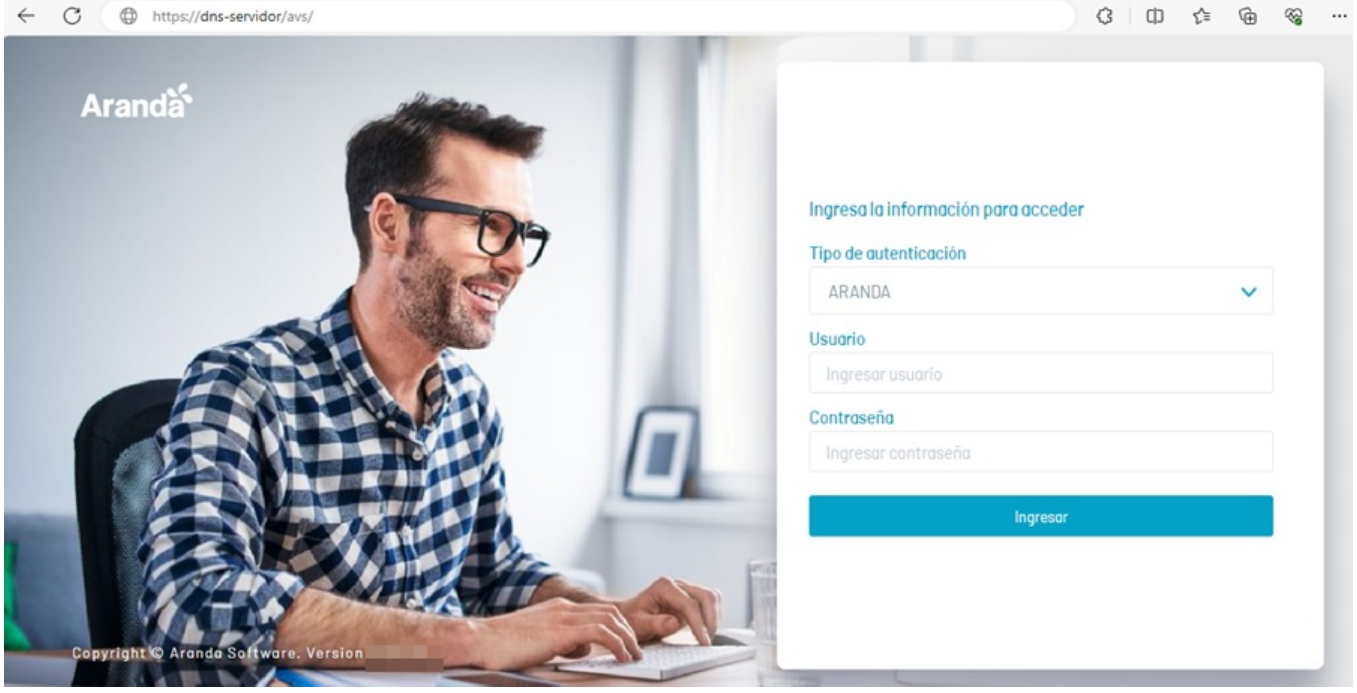


7. Seleccione los servicios correspondientes y haga clic en el botón**Apply**, si desea encriptar la conexión marque la casilla**Encrypt** ubicada en la esquina inferior izquierda.

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



9. Establecida la conexión, podrá acceder al sitio web de AVS donde podrá iniciar con la configuración de Aranda Virtual Support a través de la siguiente URL: *http(s)://nombre_servidor/avs/.*



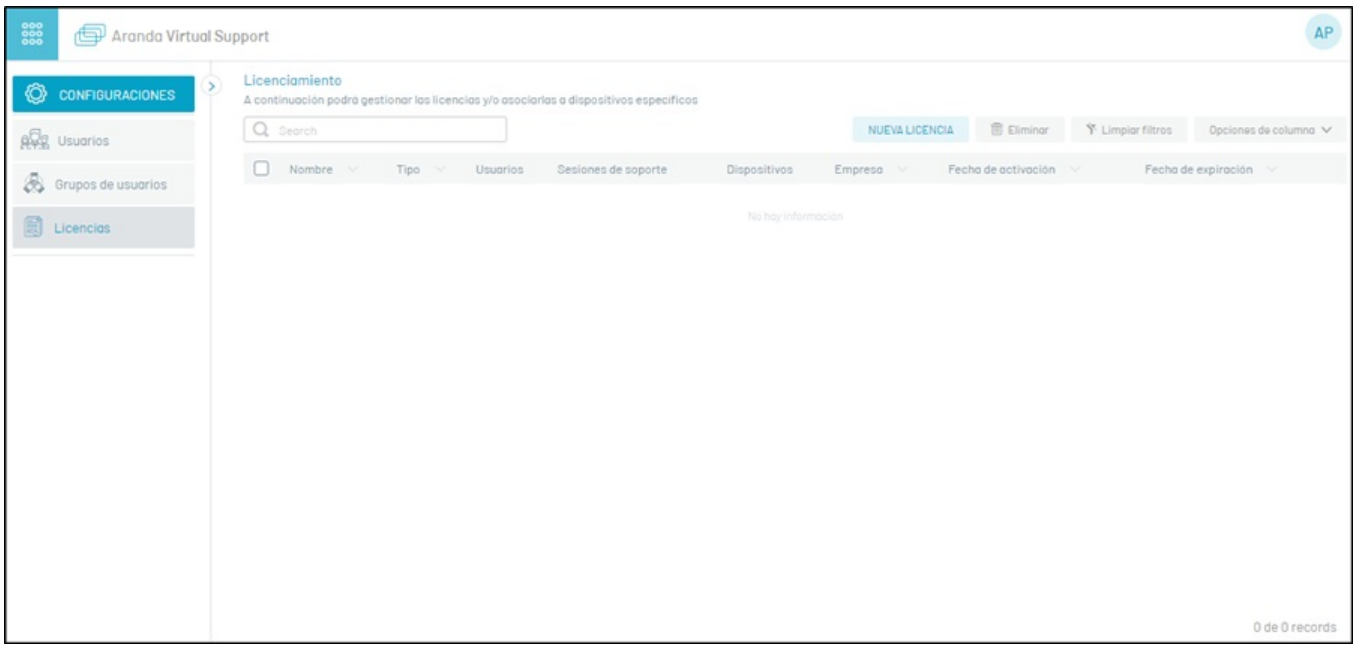
\n## Licenciamiento de AVS

title: Licenciamiento de AVS chapter: "instalacion" —

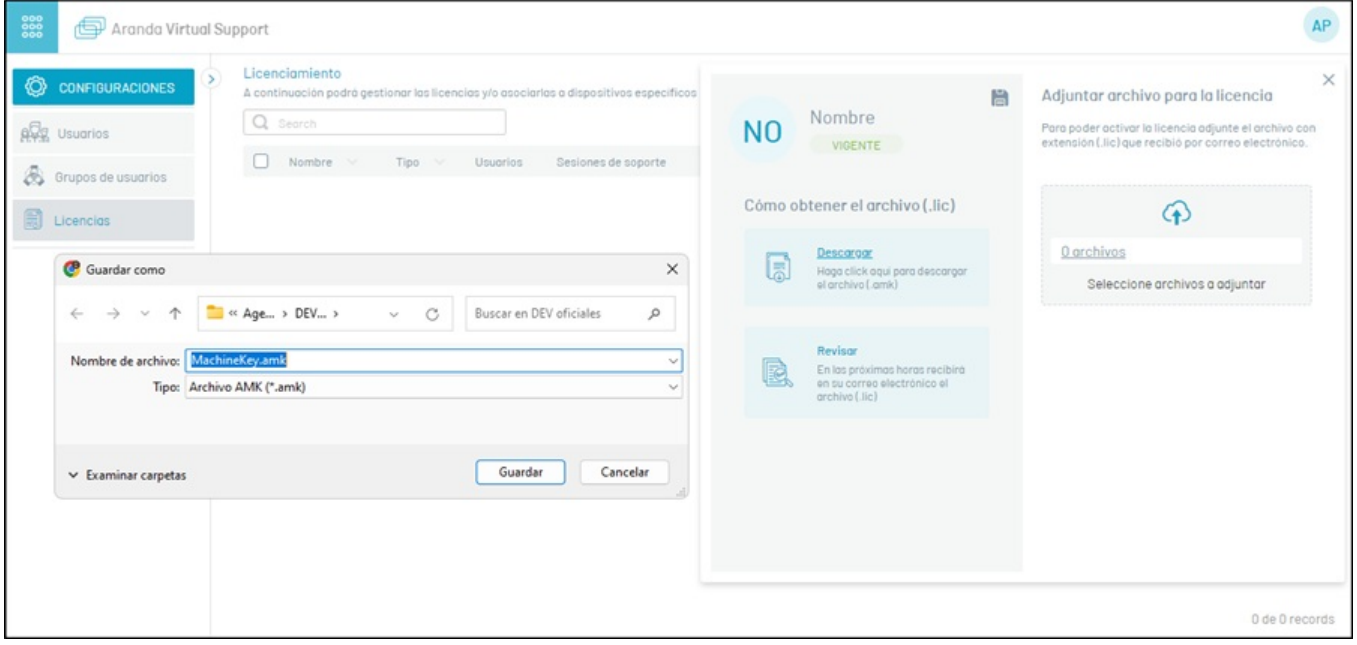
Todos los productos de Aranda Software requieren una licencia para su funcionamiento, por tal razón, la primera vez que ingrese al sitio web de Aranda Virtual Support (AVS), seleccione la opción **Licencias** del menú principal en donde podrá agregar nuevas licencias y visualizar el listado de licencias existentes agrupadas con los siguientes datos:

Columna	Descripción
Nombre	Es el nombre del producto de Aranda asignado a la licencia.
Tipo	Tipo de licencia.
Usuarios	Número de usuarios concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Sesiones de soporte	Número de sesiones de soporte concurrentes (Cantidad usada/cantidad total de licencias).
Dispositivos	Número de estaciones de trabajo concurrentes (Cantidad de licencias usadas/cantidad total de licencias).
Empresa	Empresa dueña de la licencia.
Fecha de activación	Fecha en la que son activadas las licencias.
Fecha de expiración	Fecha de caducidad de las licencias.

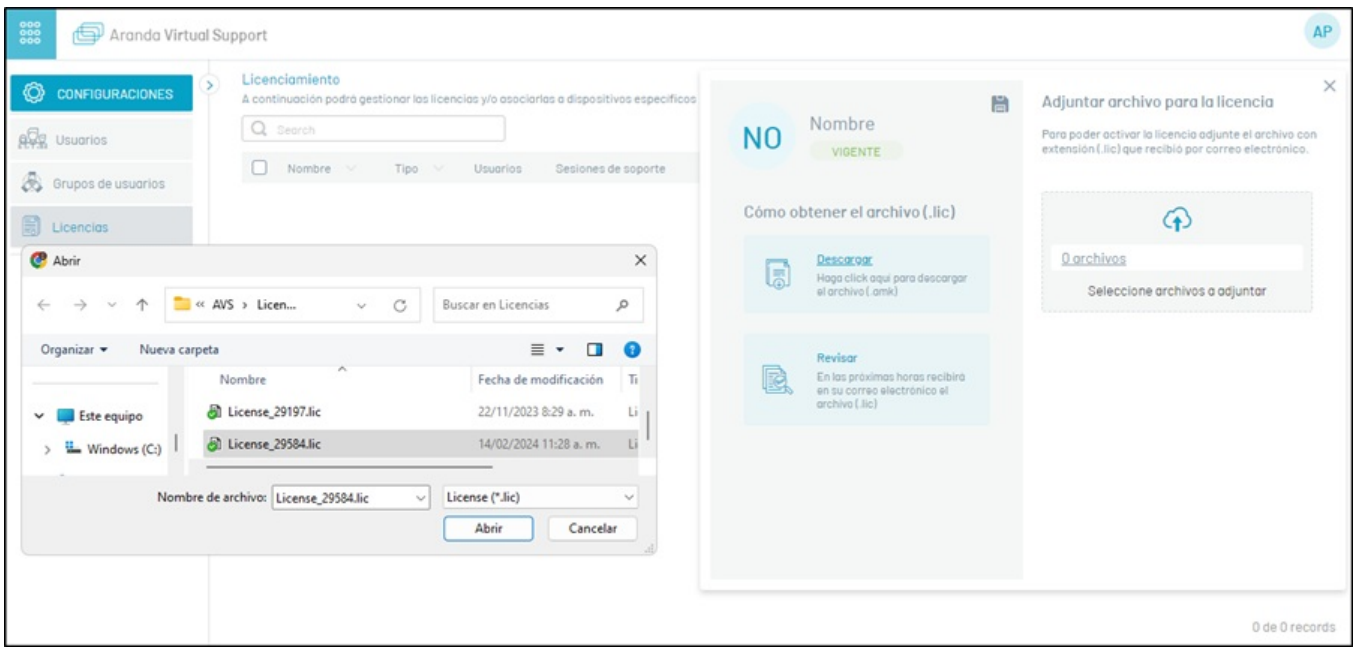
En la ventana Licenciamiento haga clic en **NUEVA LICENCIA**.



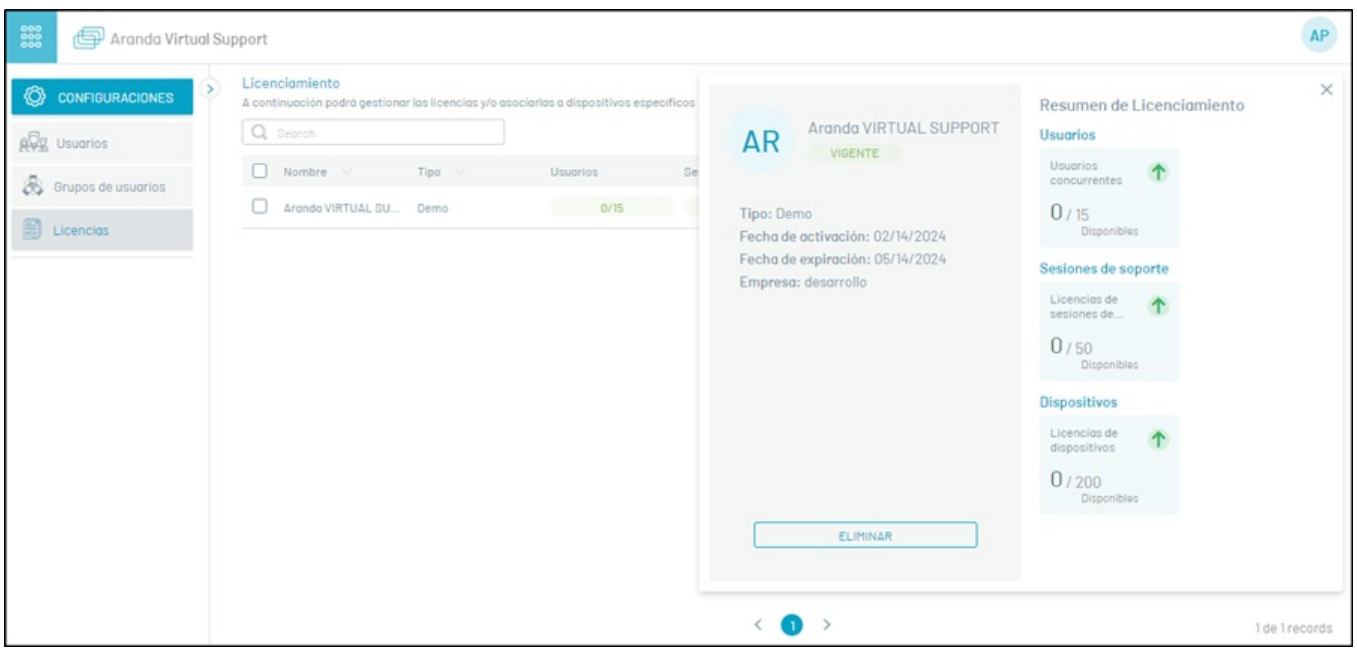
En la ventana emergente seleccione la opción **Descargar**, que permite la descarga del archivo MachineKey.amk, el cual debe ser enviado al área encargada en Aranda Software (Preventa y Proyectos) para la generación del archivo .lic (archivo de licenciamiento).



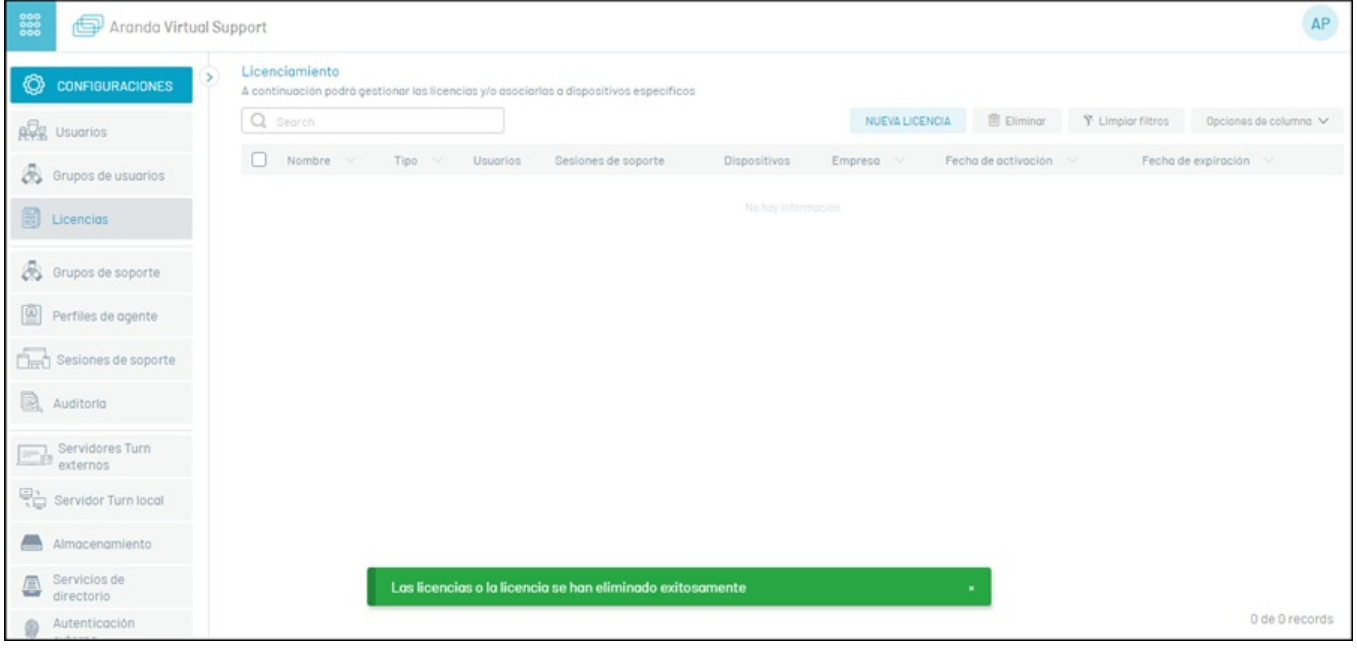
Una vez recibido el archivo .lic debe cargarlo al servidor, haga clic en el botón**Seleccione archivos a adjuntar** y luego en**Guardar** (ícono en forma de disquete). Al cargar la licencia es generada la alerta correspondiente.



Para conocer en detalle la licencia, en la ventana**Licenciamiento**, seleccione un registro del listado de licencias disponibles y en la ventana que se habilita podrá visualizar la vigencia de la licencia y el número de licencias que se han usado por usuarios, sesiones de soporte y dispositivos concurrentes (Cantidad de licencias usadas/cantidad total de licencias).



Para eliminar una licencia, en la ventana**Licenciamiento** seleccione el registro de la licencia que desea eliminar y haga clic en el botón**Eliminar**, se confirmará que la licencia ha sido eliminada satisfactoriamente.



\n## Configuración del Turn Server — title: Configuración del Turn Server chapter: "" —

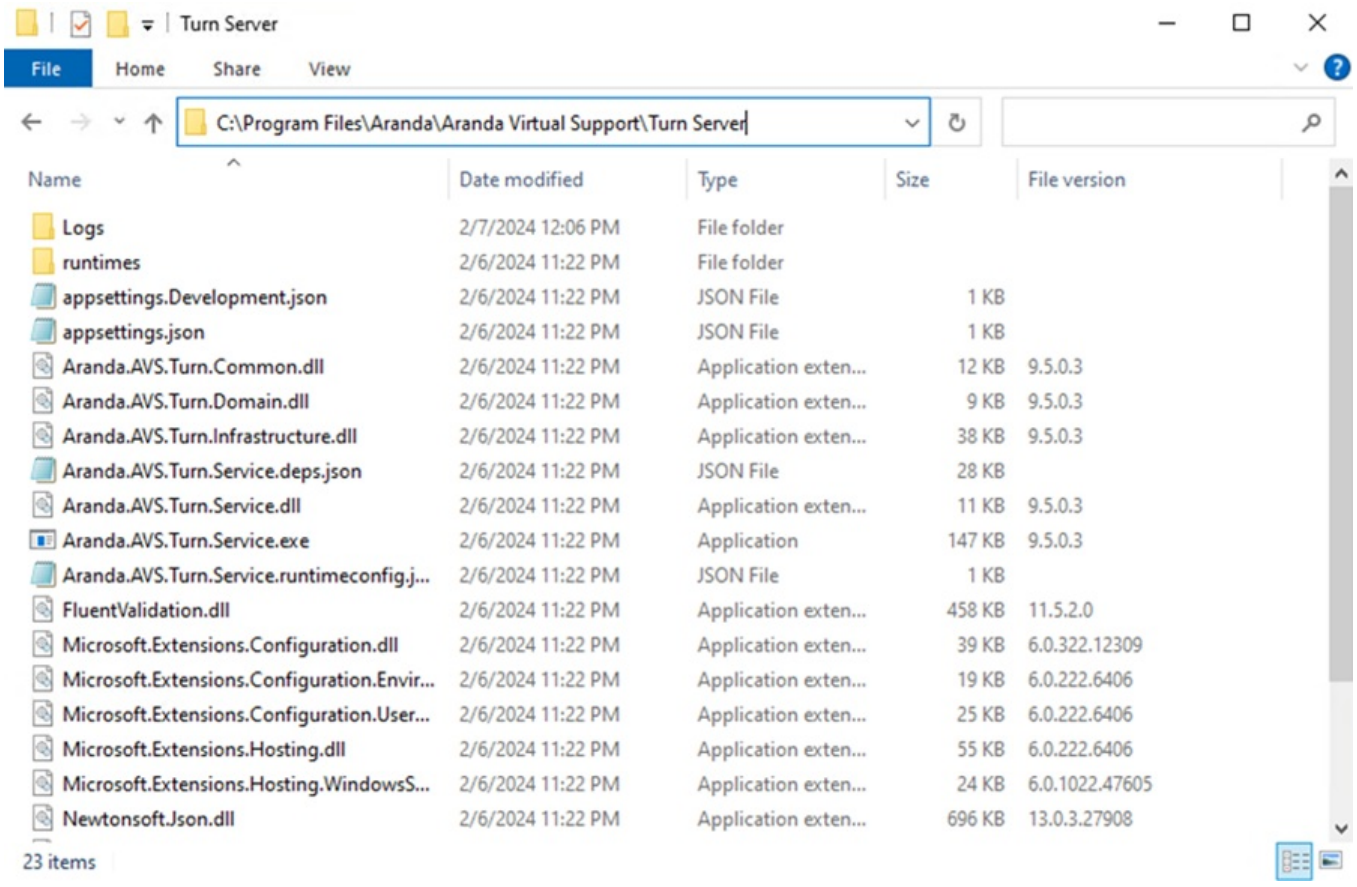
↩ Servidor Turn Local

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

1. Validación del Archivo appsettings.json

Antes de realizar cambios, verifique el archivo**appsettings.json** ubicado en la ruta de instalación del servicio (por defecto:C:\Program Files (86)\Aranda\Aranda Virtual Support\Turn Server) para asegurarse de que el puerto esté configurado por defecto en 8081. Si no es necesario modificar el puerto, no es necesario realizar más ajustes.

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



Configuración por defecto de appsettings.json:

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

2. Cambio de Configuración del Puerto

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

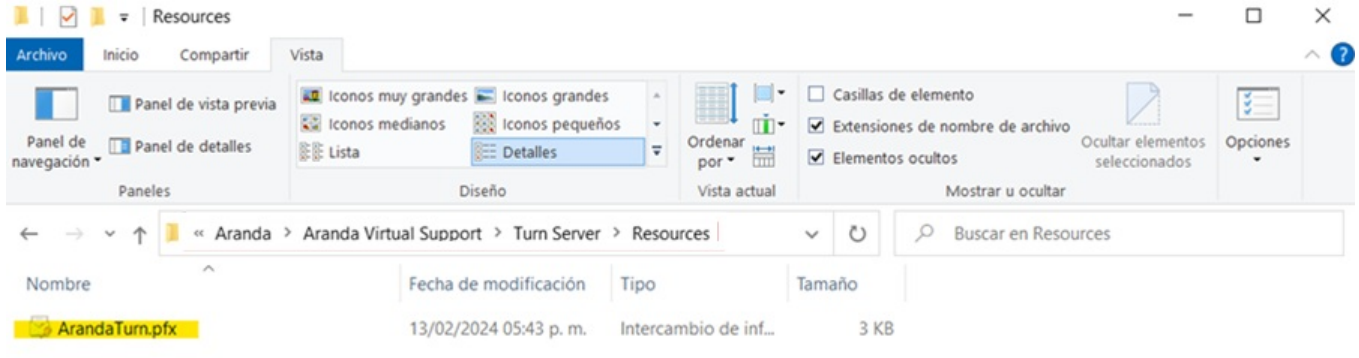
```
"TurnConfiguration": {
    "CertificateParam": "",
```

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

3. Configuración de conexión segura SSL

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

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



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

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

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

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

4. Reinicio del Servicio

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

5. Configuración del Firewall

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

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

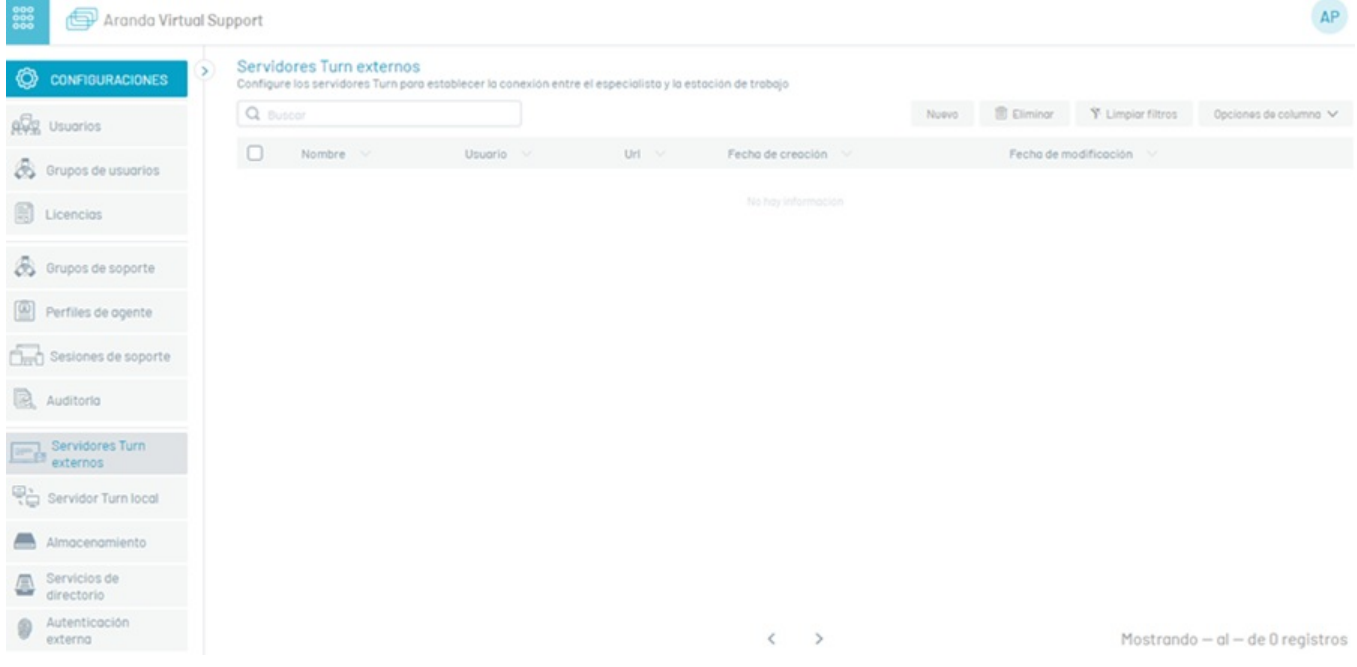
↩ Servidor Turn Local\n## Configuración de Infraestructura

title: Configuración de Infraestructura chapter: "configuracion" —

Después de instalar los sitios y servicios de Aranda Virtual Support (AVS), es necesario realizar algunas configuraciones desde el sitio web de AVS para garantizar el correcto funcionamiento de la aplicación durante los procesos de control remoto y transferencia de archivos. Por lo tanto, se recomienda seguir los siguientes pasos:

1. Ingresar al sitio web

Ingrese al sitio web de AVS con un usuario que tenga el rol de Administrador General o Infraestructura. Estos roles tienen los permisos necesarios para gestionar las opciones de Servidores Turn externos, Servidor Turn local y Almacenamiento. Es importante tener en cuenta que estas opciones están disponibles únicamente en instalaciones On Premise.



2. Servidores Turn Externos

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

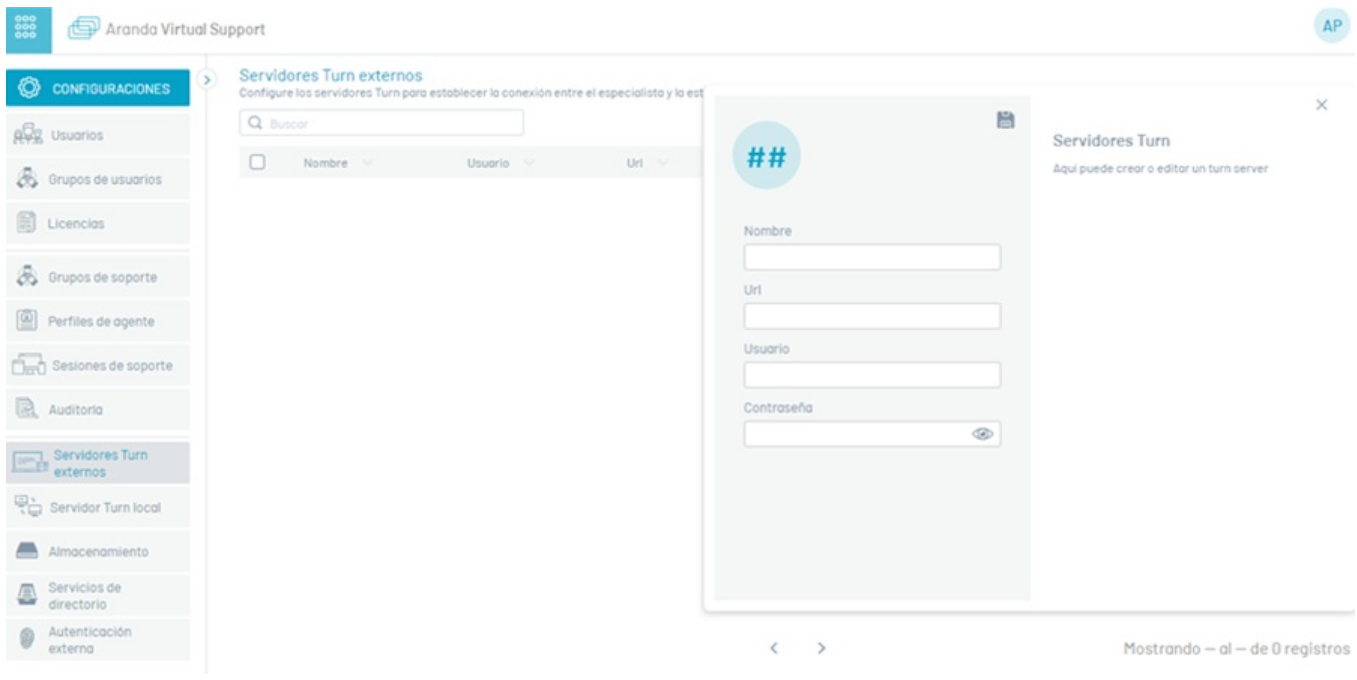
Para agregar un servidor Turn externo en la ventana de**Servidores Turn Externos**, siga estos pasos:

A. Haga clic en la opción**Nuevo**.

B. Complete los campos solicitados.

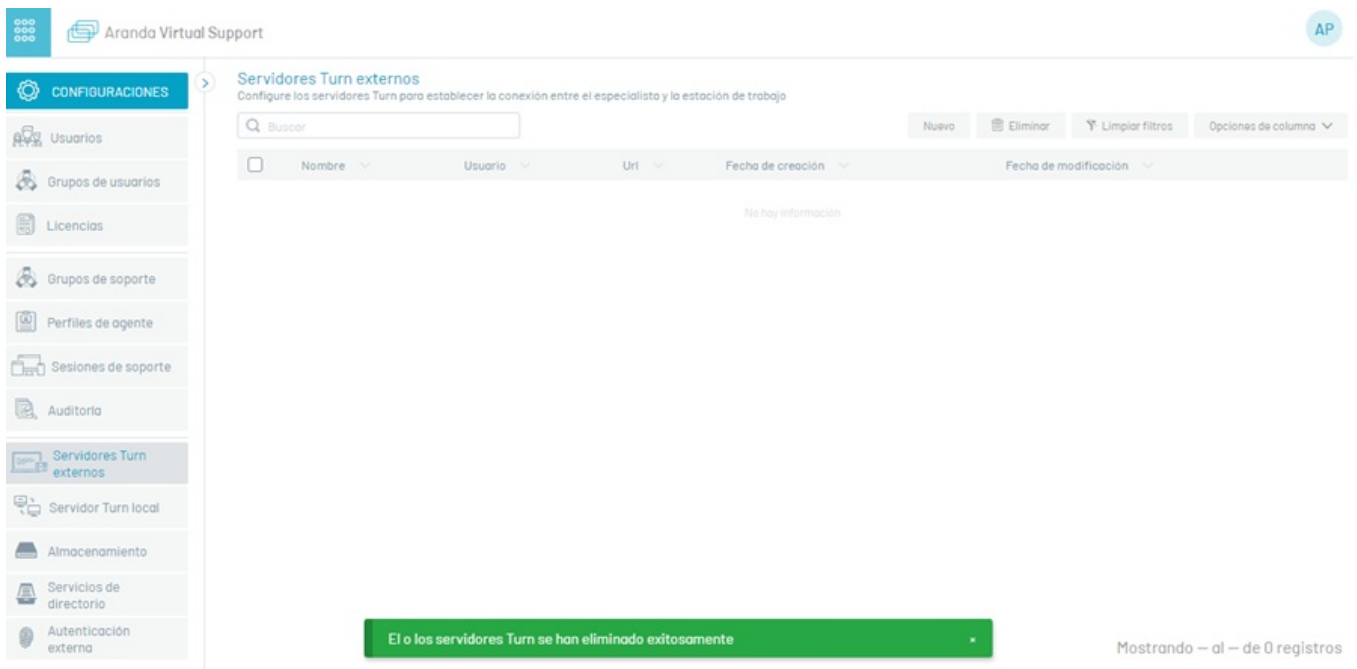
C. Finalice haciendo clic en el botón**Guardar** (ícono en forma de disquete).

> ⚐ **Nota:** Esta configuración es requerida para la transferencia de archivos cuando el agente especialista y el agente de la estación de trabajo no están en la mis red, por lo tanto se debe permitir la salida a internet.



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

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



Se pueden utilizar Stun/Turn WebRTC públicos. Para esto deben permitir la salida en el firewall a estas direcciones en las estaciones de trabajo y en los equipos especialistas. O se puede instalar el servidor provisto [realizando los ajustes en el servicio Aranda Turn Stun WebRTC Server Windows Service] en el instalador. También es posible tener stun/turn públicos junto con propios instalados como se mencionó anteriormente.

3. Servidor Turn Local

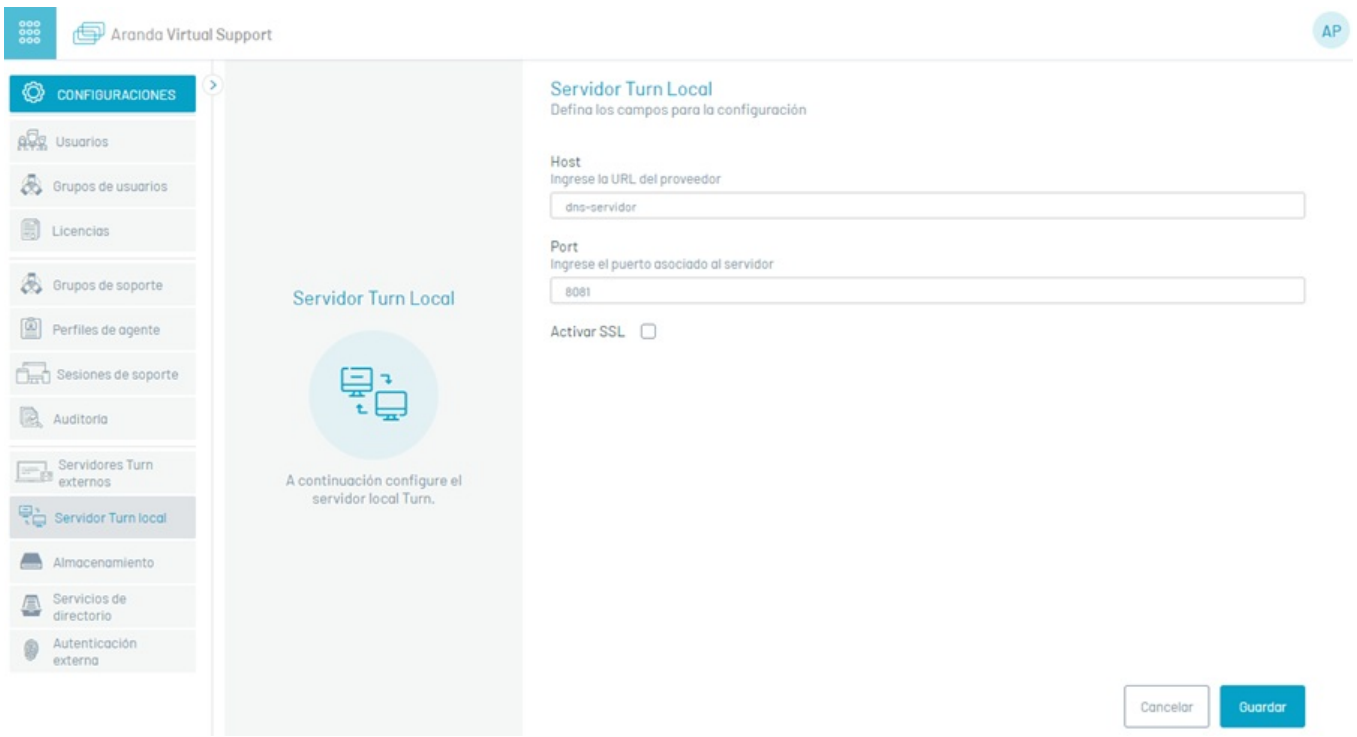
Para establecer la comunicación de toma de control remoto entre el agente especialista y el agente de la estación de trabajo, utilice un servidor Turn local que puede retransmitir el tráfico de red.

Para agregar un servidor Turn local, siga estos pasos:

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

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

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



4. Almacenamiento

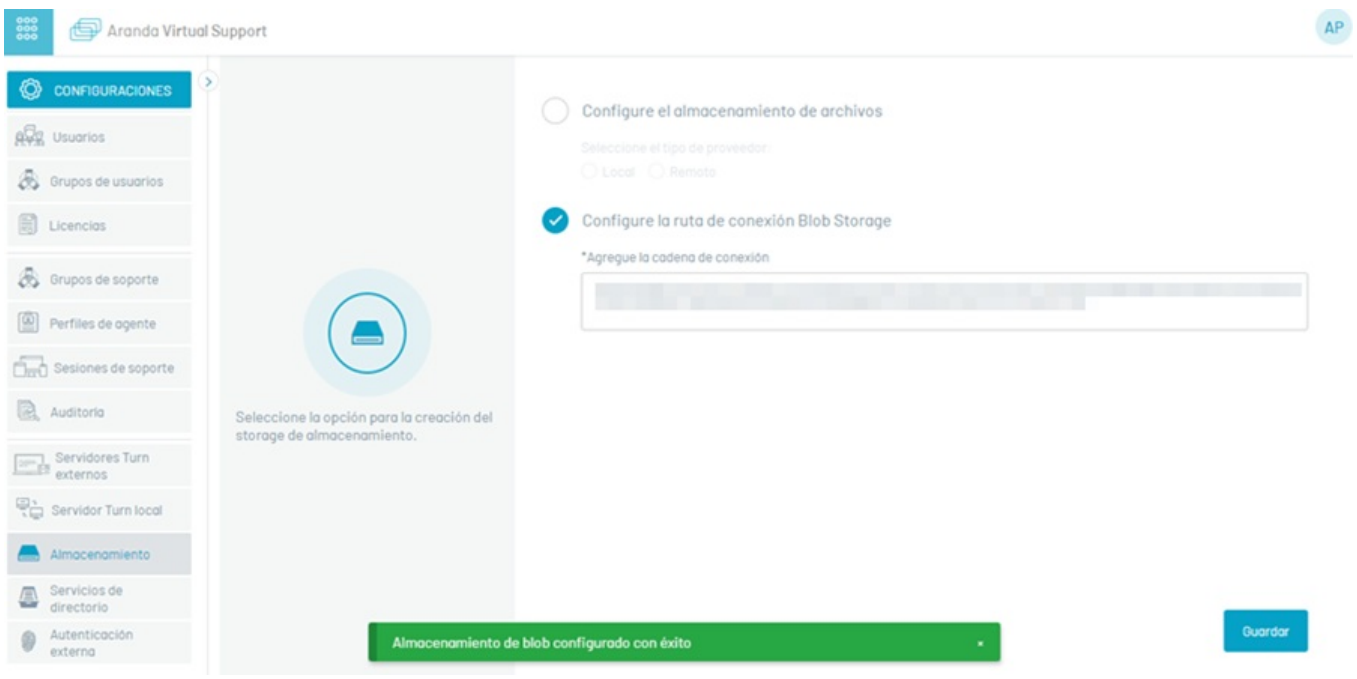
Esta configuración es necesaria para almacenar las grabaciones de la prestación del servicio de control remoto y los instaladores del agente para las estaciones de trabajo. Los archivos generados se envían a un proveedor de almacenamiento. El proveedor puede ser de tres tipos: local, remoto o Blob storage.

Para configurar el proveedor de almacenamiento, siga estos pasos:

A. Haga clic en la opción **Almacenamiento** del menú principal.

B. Complete el campo o los campos solicitados dependiendo del tipo de almacenamiento seleccionado.

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



⚐ **Notas:**
- Para que las grabaciones se almacenen de forma correcta, el servidor donde está instalado el sitio de grabaciones, debe contar con acceso al proveedor configurado. En caso de utilizar el proveedor tipo local, la ruta debe existir en el servidor y tener los permisos correspondientes.

- Para que los instaladores se almacenen de forma correcta, el servidor donde estén instalados los servicios Comunes, debe contar con acceso al proveedor configurado. En caso de utilizar el proveedor tipo local, la ruta debe existir en el servidor y tener los permisos correspondientes.

- Si, posterior a la configuración, se realizan cambios en el proveedor de almacenamiento, es necesario mover la información contenida en el proveedor anterior al actual. Si no se realiza esta acción, las actualizaciones de los agentes no se realizarán de forma correcta y no se podrá acceder a las grabaciones en las auditorías.

\n## Configuración del Servidor Stun/Turn WebRTC — title: Configuración del Servidor Stun/Turn WebRTC chapter: "" —

↩ Servidor Turn Externo

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

1. Validación del Archivo turn-server.toml

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

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

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

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

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

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

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

Para configuar el servicio Stun/Turn WebRTC se debe utilizar el archivo turn-server.toml:

Sección [turn]: Especifica el dominio donde se encuentra el servidor.

Sección [[turn.interfaces]]: Indica interfaces de escucha. Describe la interfaz a la que está vinculado el servidor turn/stun. Se pueden indicar varias interfaces

Sección [turn.interfaces.transport]: Indica el tipo de transporte de la interfaz. Puede ser udp o tcp.

Sección [turn.interfaces.bind]: Dirección IP y puerto de vinculación del socket interno.

Sección [turn.interfaces.external]: Se usa para enlazar a la dirección de su NIC local, por ejemplo, tiene dos NIC A y B en su servidor, la dirección IP de la NIC A es 192.168.1.2 y la dirección de la NIC B es 192.168.1.3, si se enlaza a la NIC A, debe enlazar a la dirección 192.168.1.2, y enlazar a 0.0.0.0 significa que escucha a todas ellas al mismo tiempo. La palabra external significa que su tarjeta de red para el cliente pueda "ver" la dirección ip. Continuando con el ejemplo anterior, tu tarjeta de red A en comunicación con el externo, si esta en la red de área local, entonces lo que ven los otros clientes es su dirección LAN, es decir, en realidad 192.168.1.2. Sin embargo, en la realidad, la topología de red donde está desplegado el servidor, habrá otra ip pública, como 1.1.1.1, que es tu dirección ip vista por los demás clientes. En cuanto a por qué se necesitan bind y external, esto se debe a que para el protocolo stun, la situación es más complicada, el servidor stun necesita informar su propia dirección IP externa, lo que permite que el cliente stun se conecte a la dirección especificada a través de la dirección IP informada por el servidor.

Sección [api.bind]: Escucha del api para consultar. Por ejemplo http://127.0.0.1:3000/info

Sección [log.level]: Nivel de log. Valores válidos "error", "warn", "info", "debug", "trace".

Sección [auth]: Pareja de usuarios y contraseñas para accedo al servidor

2. Inicio del Servicio

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

3. Configuración del Firewall

Abra el puerto o puertos configurados en el paso 1 en las reglas de entrada del firewall local. Este paso es relevante para permitir el tráfico a través del nuevo puerto y asegurar que el Stun Server pueda recibir conexiones entrantes en el puerto configurado.

Adicionalmente, si requiere que opere como turn webRTC debe abrir el rango 49152-65535 para el protocolo UDP.

↩ Servidor Turn Externo