Aranda Virtual Support

This guide details the steps required for installing and configuring Aranda Virtual Support (AVS) in an on-premises environment. AVS is a remote support application developed by Aranda Software that allows you to take remote control and transfer files in real time and securely to workstations.

What is our documentation?

- AVS Getting Started Guide
- AVS Management User Manual
- AVS Agent Manual
- On-premises installation manual

Prerequisites

Prerequisites

System Requirements

The following requirements are defined for the implementation of Aranda Virtual Support in an on-premises installation.

	Web Application Server / Services
Dedication	Dedicated use for AVS (Do not share your usage with other applications)
Storage	- Space Required: Minimum 64GB - Unit Type: Solid State Drive (SSD) - Partitions: Dedicated partition is recommended for site installation. A dedicated partition is recommended for the database (MDF and LDF files)(*) * In the case of installation of the solution on the same server where the database resides.
Processing	4 CPU / 8 vCPU 2.1 GHz or higher.
Connectivity	Gigabit Ethernet network card (1GBps or higher)
Database	Versions: SQL Server 2019, SQL Server 2022 Editions: Standard (for Test Environments), Enterprise (for Production Environments) and Express (only for Proofs of Concept). Licensing: It is recommended that you license the database by Core. Collation: SQL_Latin1_General_CP1_CI_AI Permissions: User for database creation (DBTools): Fixed role member db_owner. Database Service User: Fixed Role Member db_datareader and db_datawriter. Execute permissions on the dbo schema
Operating system	Version: Windows Server 2019, Windows Server 2022. Edition: Standard or Superior. Installation Account: Local and/or domain administrator credentials are required for installation.
Protocols	- The app works with HTTPS only. - Websockets must be enabled throughout the network. What is required for WebRTC to operate properly.
Input Ports	- The port must be enabled to make use of HTTPS (e.g. 443). - Also the port configured for the turn and stun server.
Update Service	The Worker server must be configured in order to reach the site https://download.arandasoft.com/updates and download files.

Additional Requirements

- Internet Information Services (IIS) 10.0 or higher.
- 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 art
  - Static Content

    - Security

    - Request Filtering

    - Application Development

    - .NET Extensibility 4.8
    - APS.NET 4.8
    - ISAPI Extensions
    - ISAPI Filters
    - WebSocket Protocol

- Management Tools

    - IIS Management Console

- Characteristics

- .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
- URL Rewrite Module version 2.1 or higher See download page
- ASP.NET Core Runtime 6.0.32 Hosting Bundle See download page

⚐ Note: Before starting the installation of Aranda Virtual Support it is necessary to create the database schema through the Aranda Database Tools v9.

See the User Manual Aranda Database Tools V9

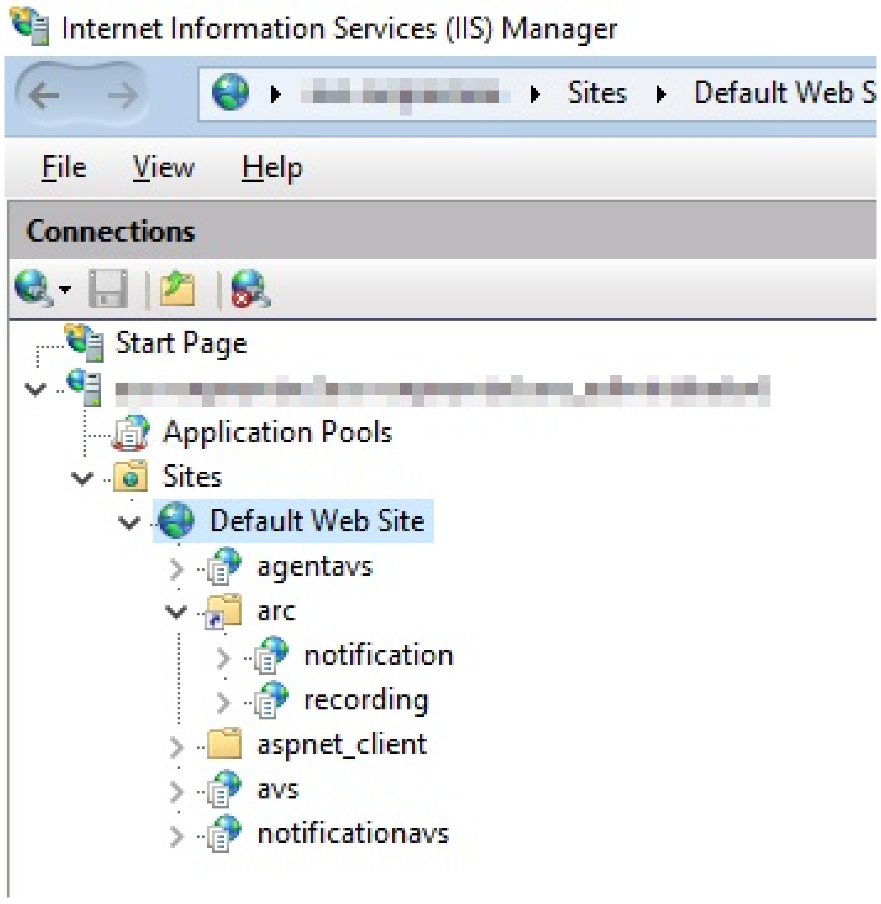
Licensing Service

Aranda Virtual Support (AVS) uses Aranda's common licensing service to authorize users to access the AVS website and control the licenses purchased, among other operations. This is a Windows service that is usually created automatically by the product installer. Once the user uploads their purchased licenses from the website, the common licensing service must remain on the same machine, otherwise the uploaded licenses will be lost. If your application server is located on a virtual machine, it is recommended that you install the Common Licensing Service on a physical machine, because when you restart virtual machines, there is a high probability that the hardware brand will change and the service will incorrectly assume that it was moved. Check with the vendor for details on server deployment.

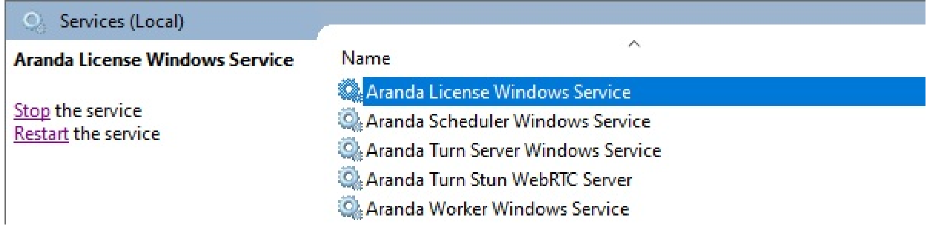
AVS Installation

Installing AVS On Premise

The installer AVS. Server.Installer It installs five websites (agentavs, arc/notification, arc/Recording, avs, notificationavs).



And five Windows services (Aranda License Windows Service, Aranda Scheduler Windows Service, Aranda Worker Windows Service, Aranda AVS Turn Server and Aranda AVS Stun Server).



Services (Local)

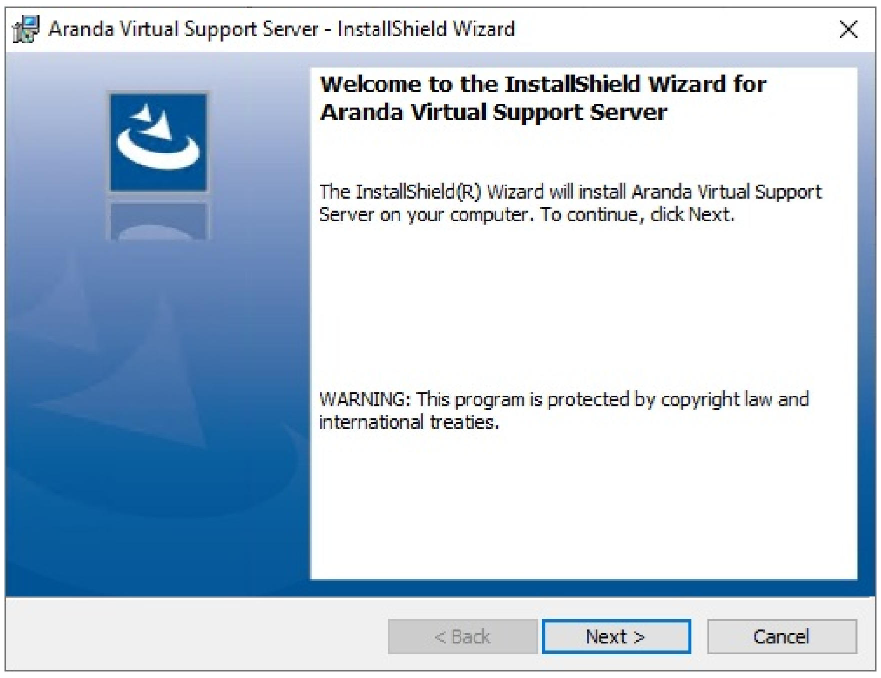
Aranda License Windows Service

Stop the service
Restart the service

Name

- Aranda License Windows Service
- Aranda Scheduler Windows Service
- Aranda Turn Server Windows Service
- Aranda Turn Stun WebRTC Server
- Aranda Worker Windows Service

1. Double-click on the installer file and you will see the welcome screen. Confirm the installation by clicking the Following.



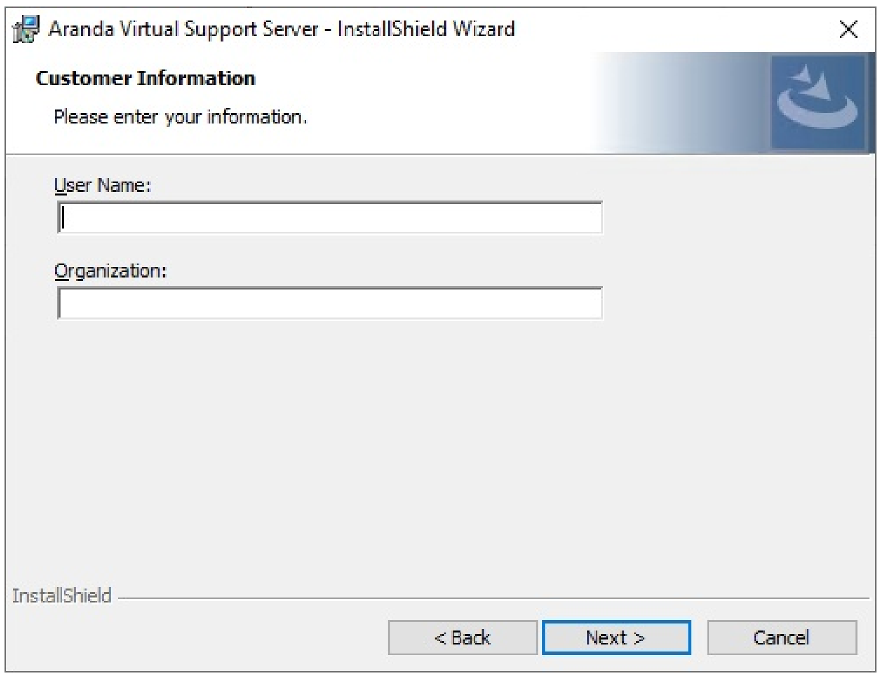
Aranda Virtual Support Server - InstallShield Wizard

Welcome to the InstallShield Wizard for Aranda Virtual Support Server

The InstallShield(R) Wizard will install Aranda Virtual Support Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

2. In the window Customer Information, enter the user name, organization, and click Following.



Aranda Virtual Support Server - InstallShield Wizard

Customer Information

Please enter your information.

User Name:

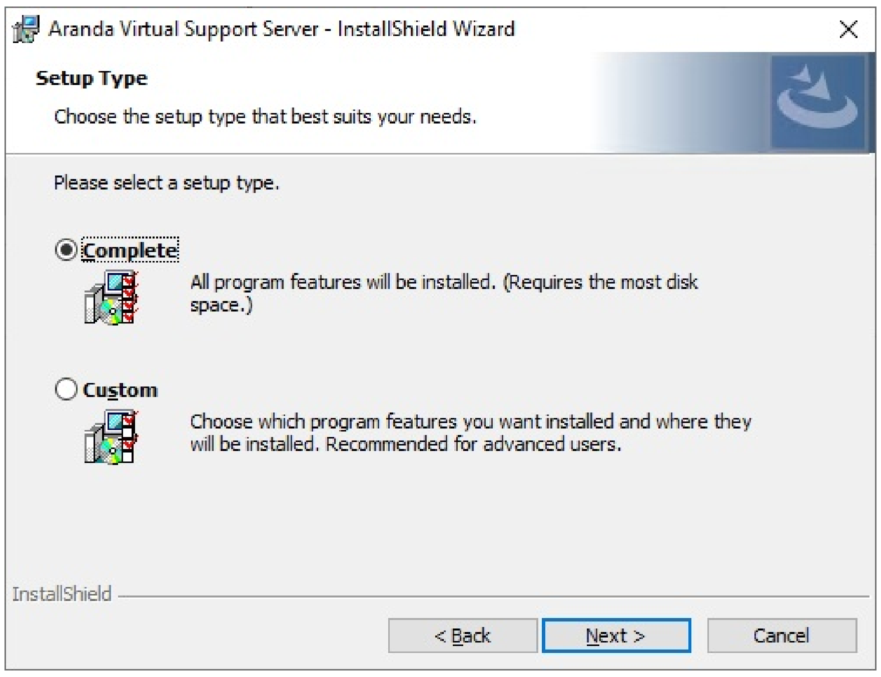
Organization:

3. In the window Type of installation You can configure the following options:

- Complete: All sites and services will be installed on the default routes.
- Custom: You will be able to select the sites or services you want to install.

⚐ Note: By default, select the installation type Complete. In the case of separating the solution layers (Web, Application) on separate servers, select the Custom.

⚠ Important: If you are performing a custom installation, do not modify the installation path.



Aranda Virtual Support Server - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

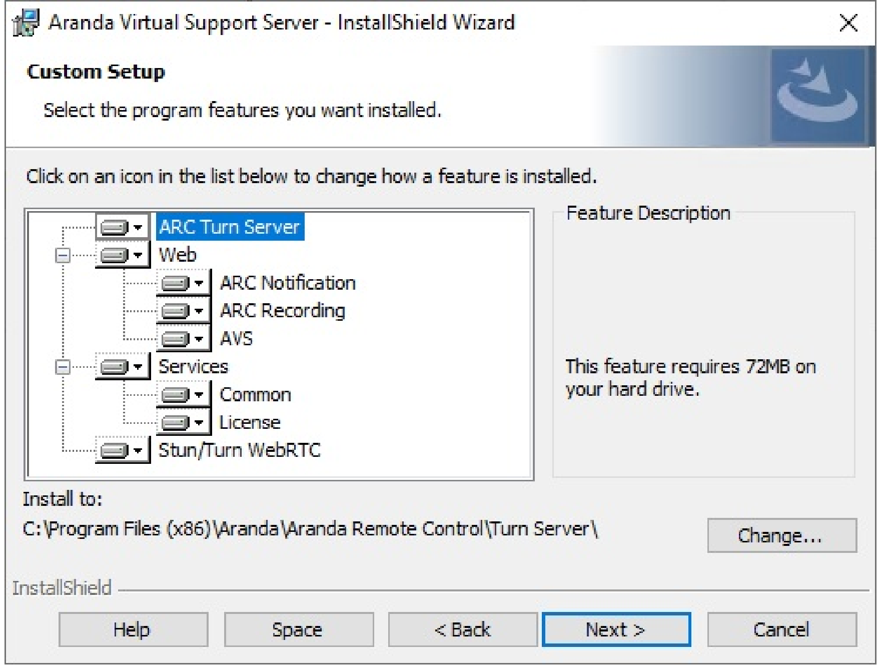
Please select a setup type.

● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- ARC Turn Server
- Web
  - ARC Notification
  - ARC Recording
  - AVS
- Services
  - Common
  - License
- Stun/Turn WebRTC

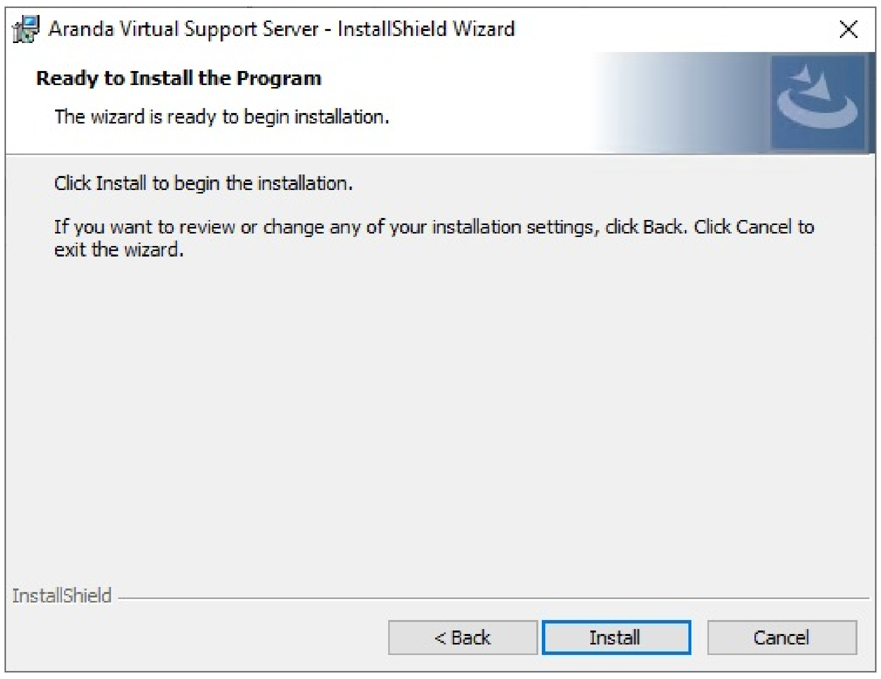
Feature Description

This feature requires 72MB on your hard drive.

Install to:

C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server\

4. Setting the installation type, in the window Preparing to install the program, click Following and then on the Install.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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

Database connection configuration

Once the installation of Aranda Virtual Support, proceed to configure the connection strings to the database of the sites and services.

Configure sites

To configure the websites, update the value of the connection string, on line 6 inside the files appsettings.json of each site; The default routes are:

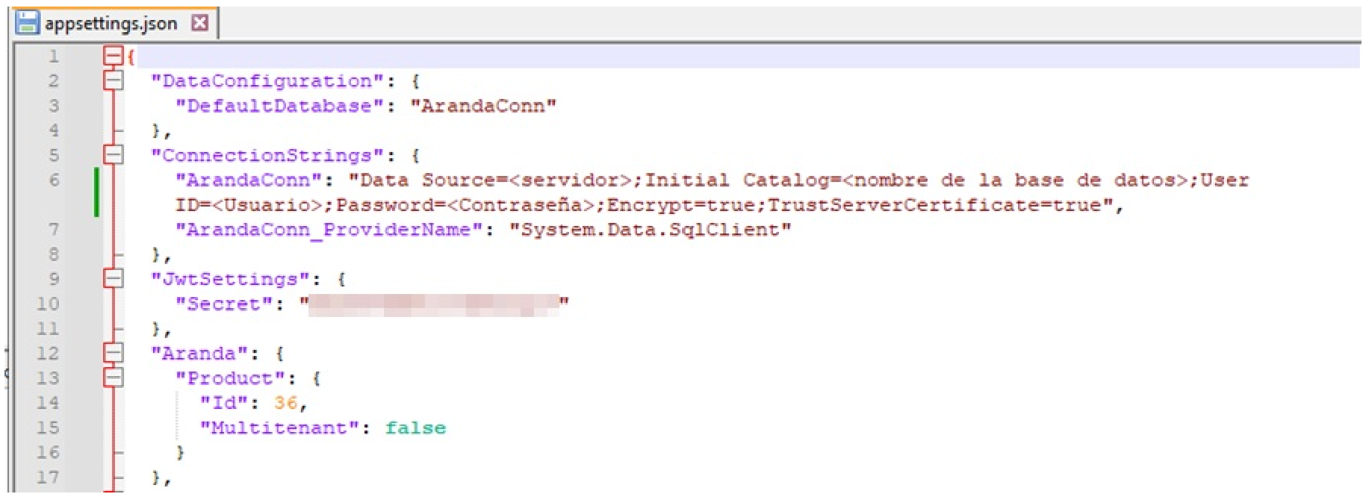
```
C:\inetpub\wwwroot\agentavs\appsettings.json

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

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

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

Example of how the connection string should look in the appsettings.json



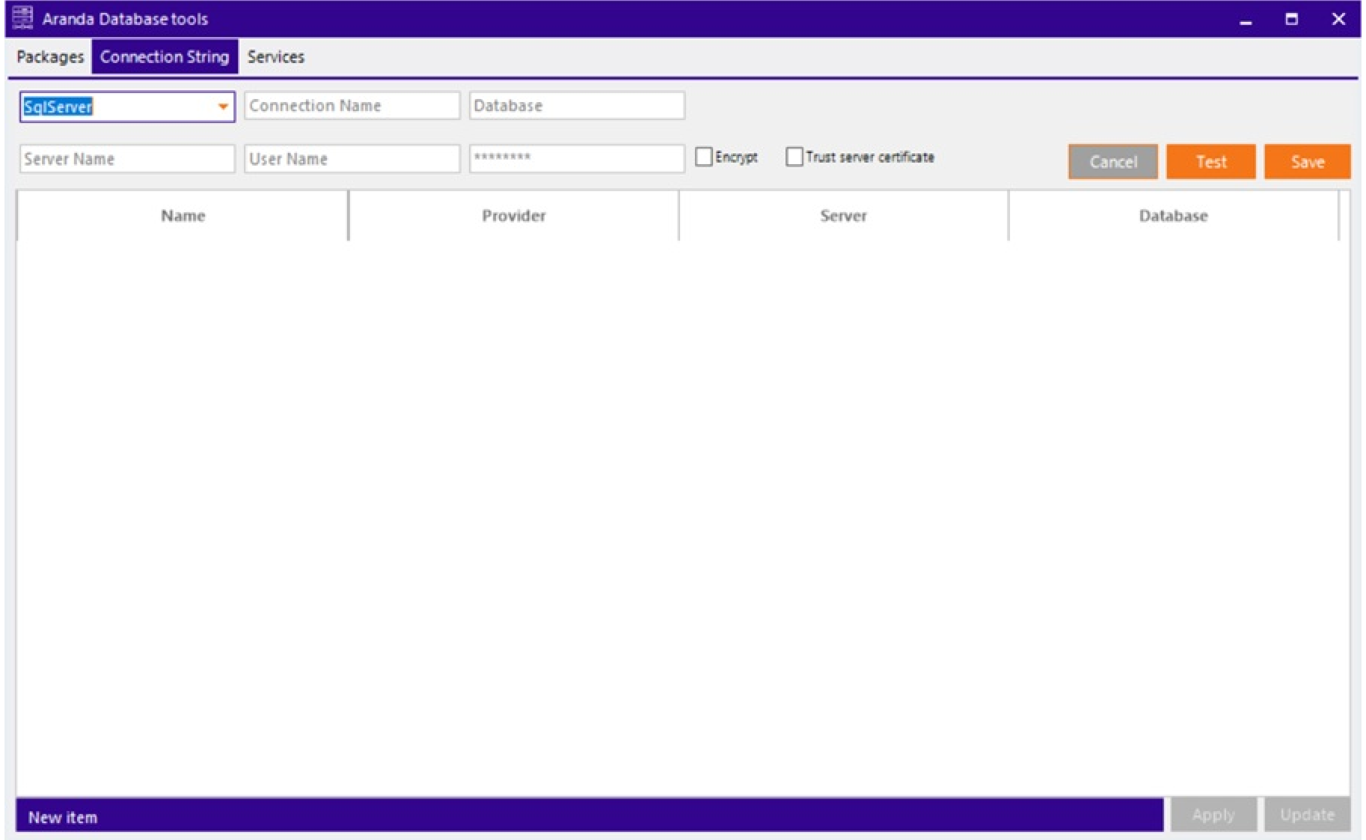
```
1  {
2    "DataConfiguration": {
3      "DefaultDatabase": "ArandaConn"
4    },
5    "ConnectionStrings": {
6      "ArandaConn": "Data Source=<servidor>;Initial Catalog=<nombre de la base de datos>;User
       ID=<Usuario>;Password=<Contraseña>;Encrypt=true;TrustServerCertificate=true",
7      "ArandaConn_ProviderName": "System.Data.SqlClient"
8    },
9    "JwtSettings": {
10     "Secret": "[redacted]"
11   },
12   "Aranda": {
13     "Product": {
14       "Id": 36,
15       "Multitenant": false
16     }
17   },
```

Keep in mind that the properties must be included Encrypt and TrustServerCertificate and the value is assigned according to the customer's business rules. [View Microsoft documentation]

Configure common services

To configure the Common and Licensing services, it is done through the Aranda Database Tools v9. To do this:

1. Run the module and click on the Connection String.


Aranda Database tools

Packages | Connection String | Services

SqlServer | Connection Name | Database

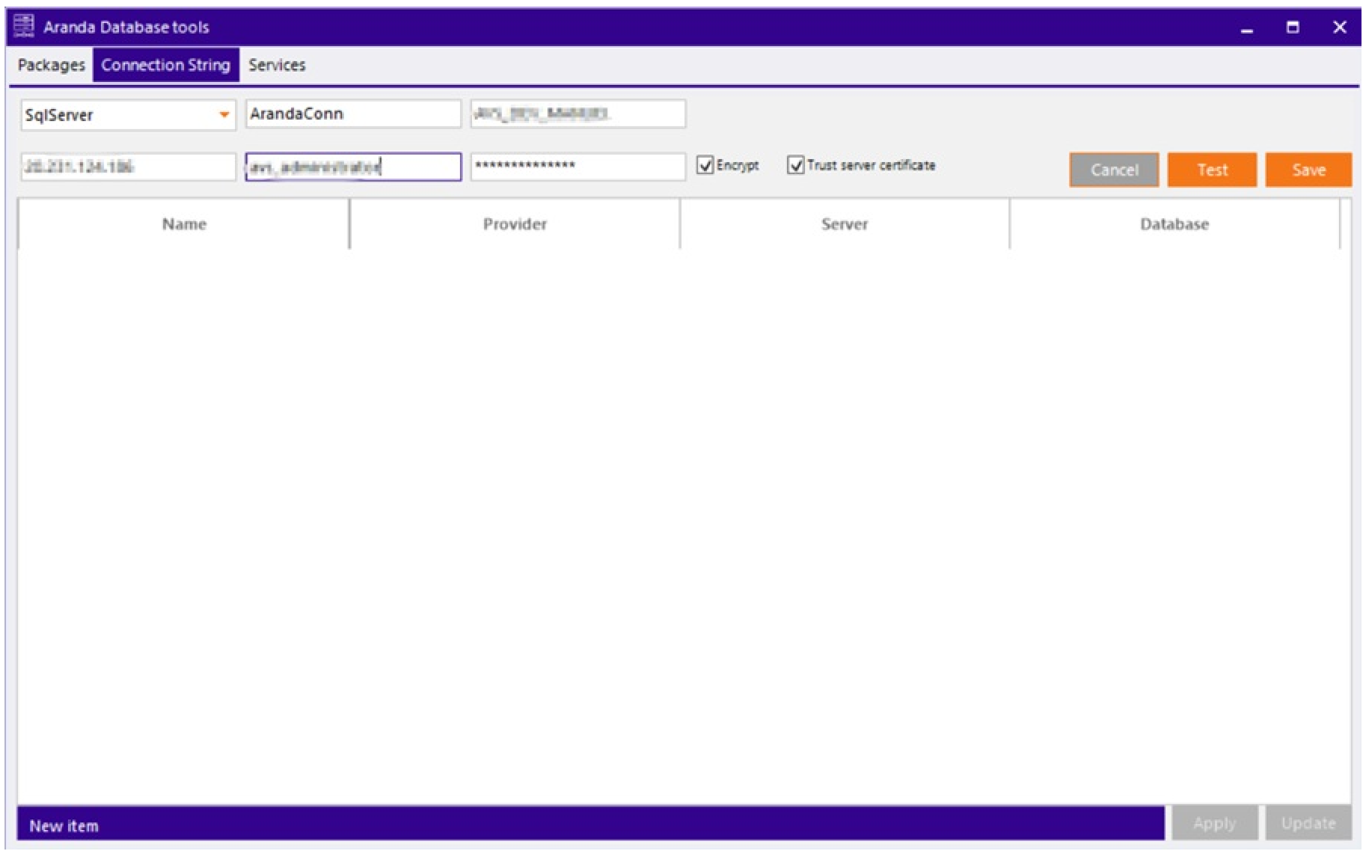
Server Name | User Name | ******** | ☐ Encrypt | ☐ Trust server certificate

Name	Provider	Server	Database

New item

2. Fill in the requested data.

- Select the database engine (SQL Server).
- Give it a name to identify the connection.
- Record the connection data (database name, server name or IP address, and if required username and password).
- In case the database port is different from the default port (1433 for SQL Server), the server must be written as servername:port (e.g. ARANDADBSERVER:5555)
- By default, the "Encrypt" option should be checked to ensure that the connection between the solution and the database is encrypted.


Aranda Database tools

Packages | Connection String | Services

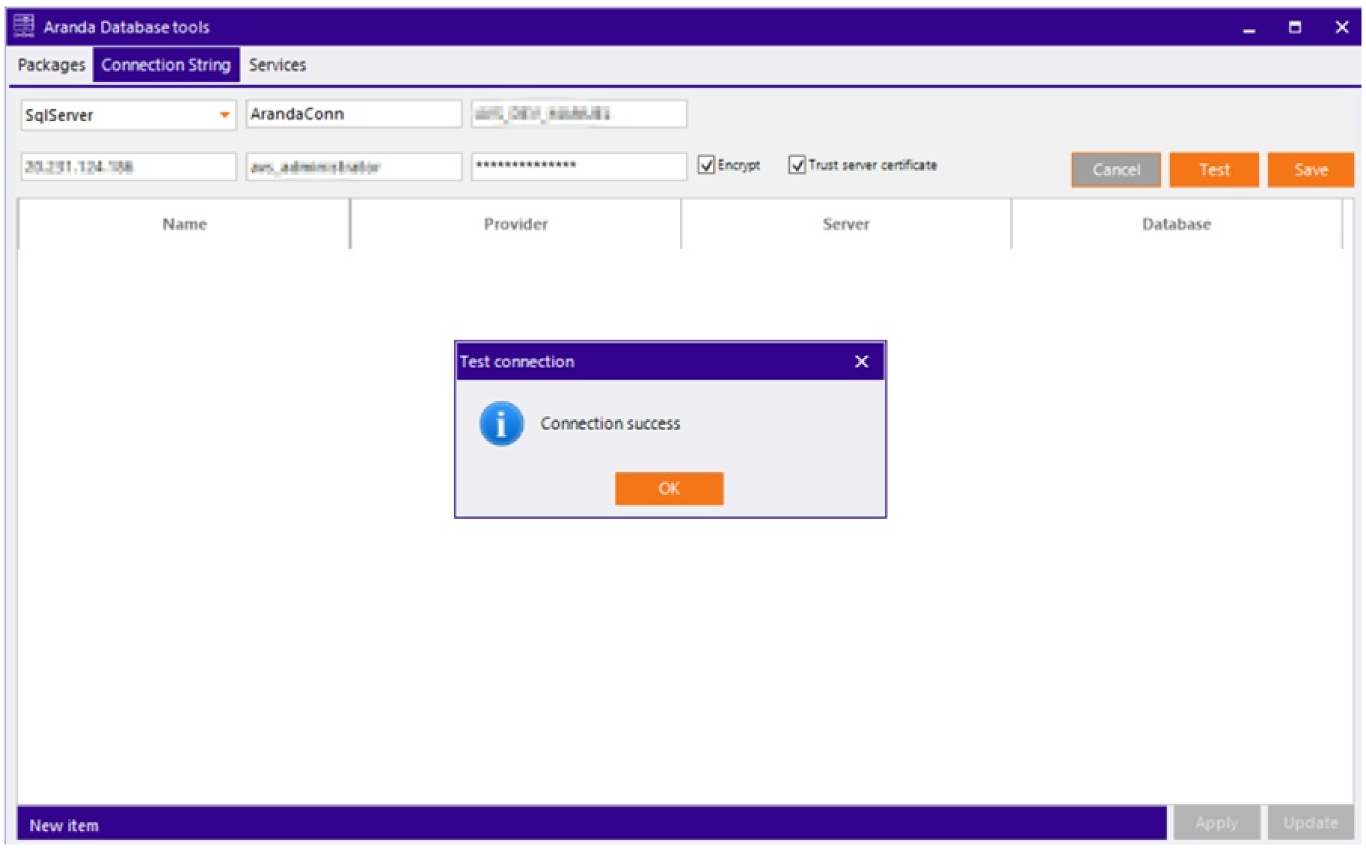
SqlServer | ArandaConn | [redacted]

[redacted] | [redacted] | ************** | ☑ Encrypt | ☑ Trust server certificate

Name	Provider	Server	Database

New item

3. Click the Test to check the connection.


Aranda Database tools

Packages | Connection String | Services

SqlServer | ArandaConn | [redacted]

[redacted] | [redacted] | ************** | ☑ Encrypt | ☑ Trust server certificate

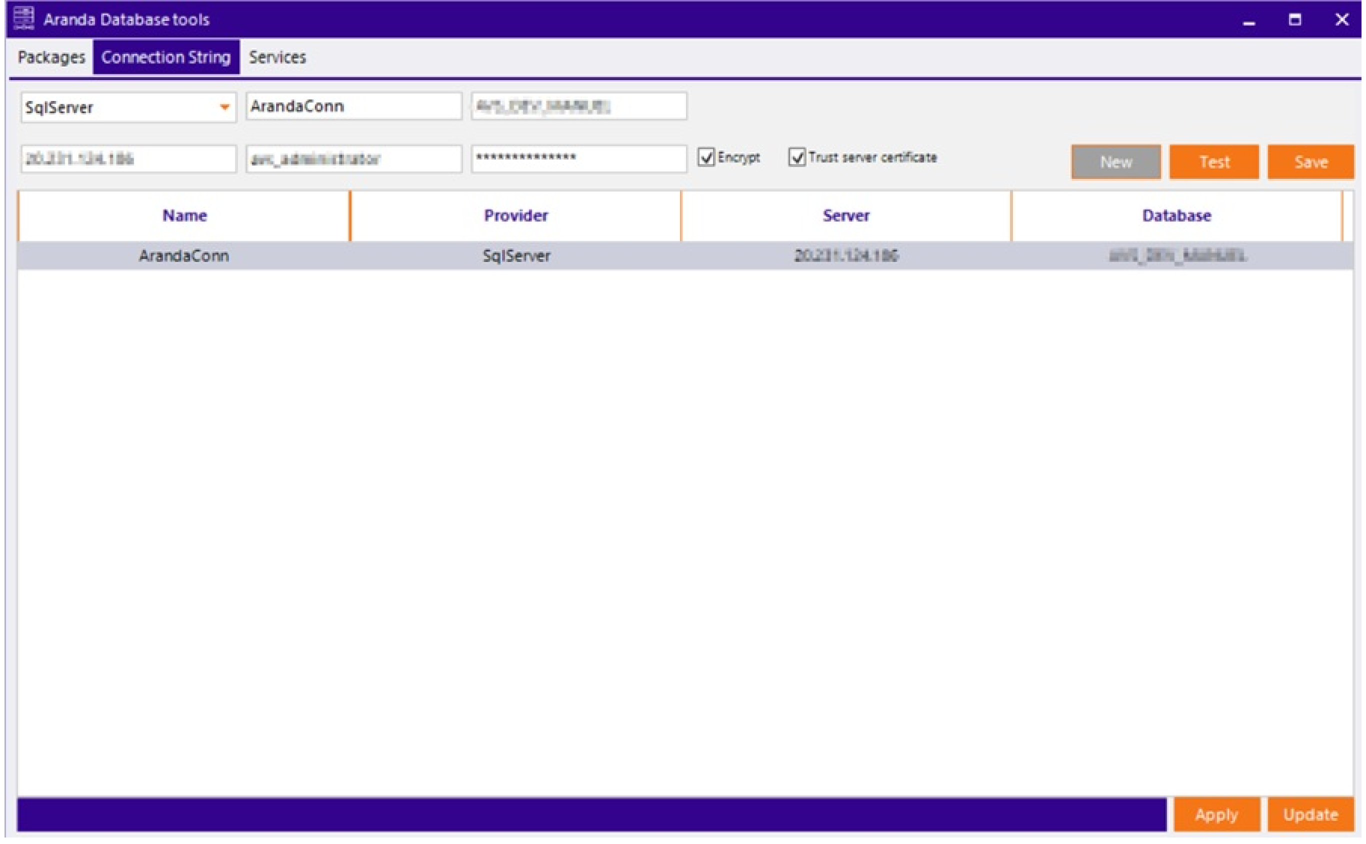
Name	Provider	Server	Database

Test connection

Connection success

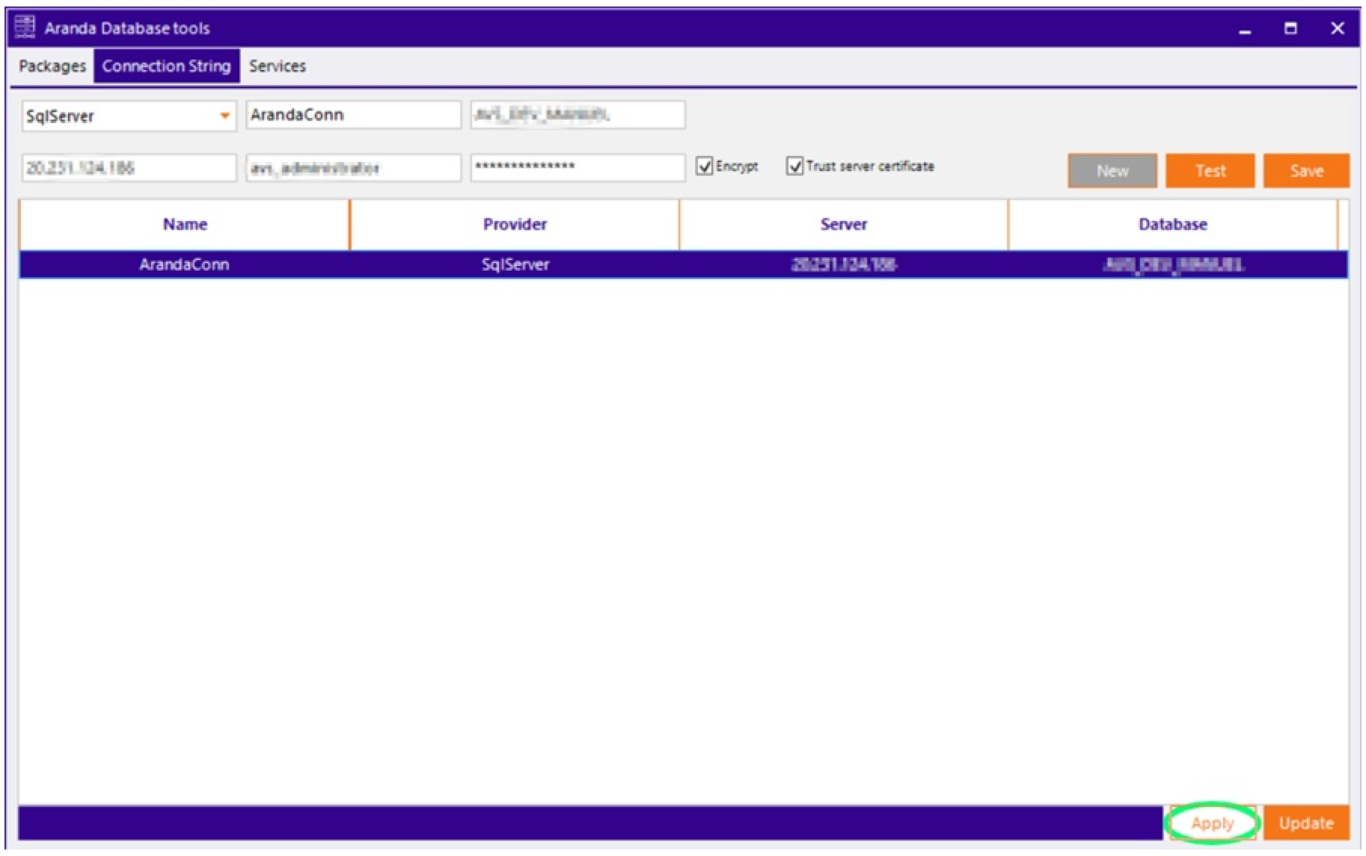
New item

4. To finish click on the Save to save the connection.



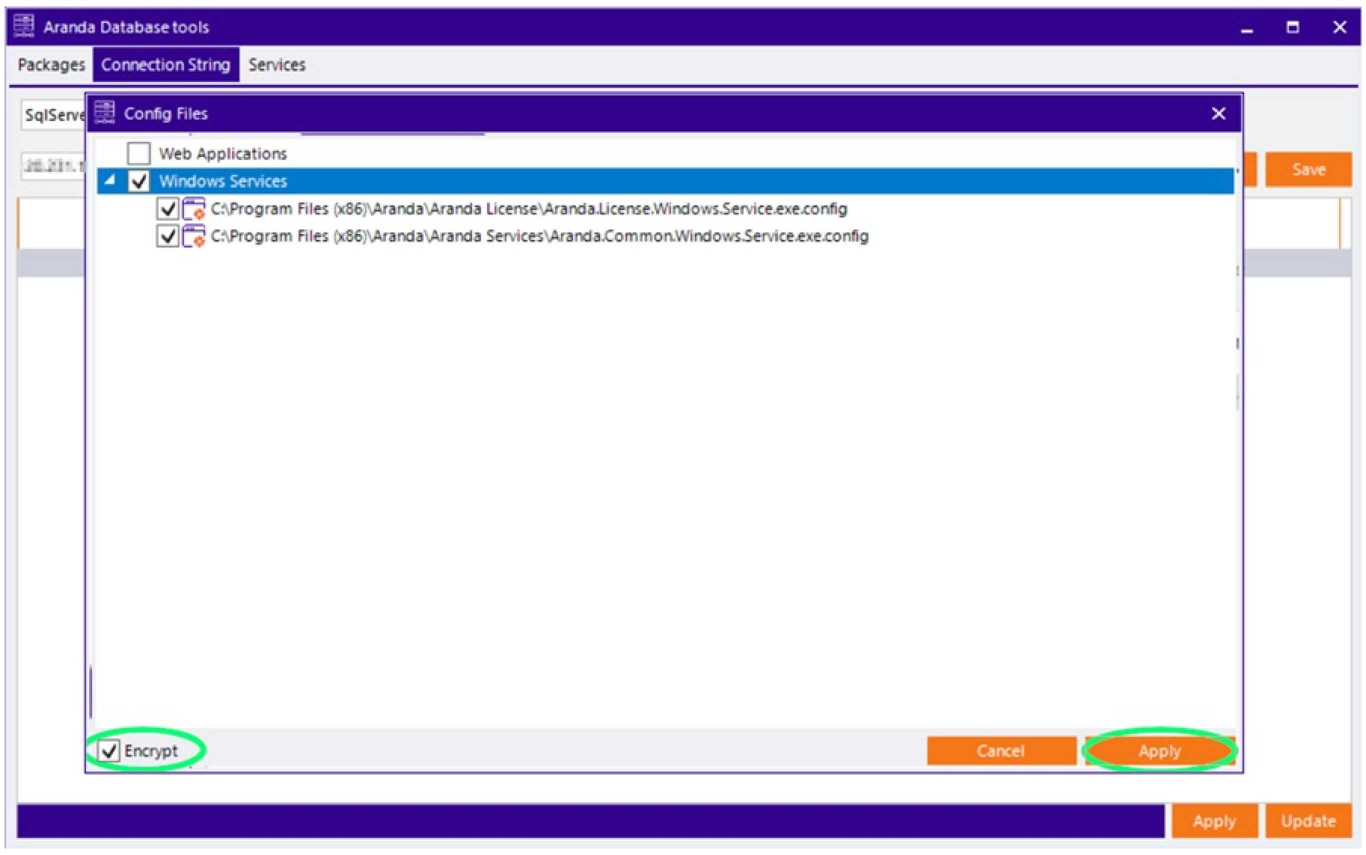
Name	Provider	Server	Database
ArandaConn	SqlServer	[redacted]	[redacted]

5. To apply connection strings to installed services, select the previously created connection and click the Apply.



Name	Provider	Server	Database
ArandaConn	SqlServer	[redacted]	[redacted]

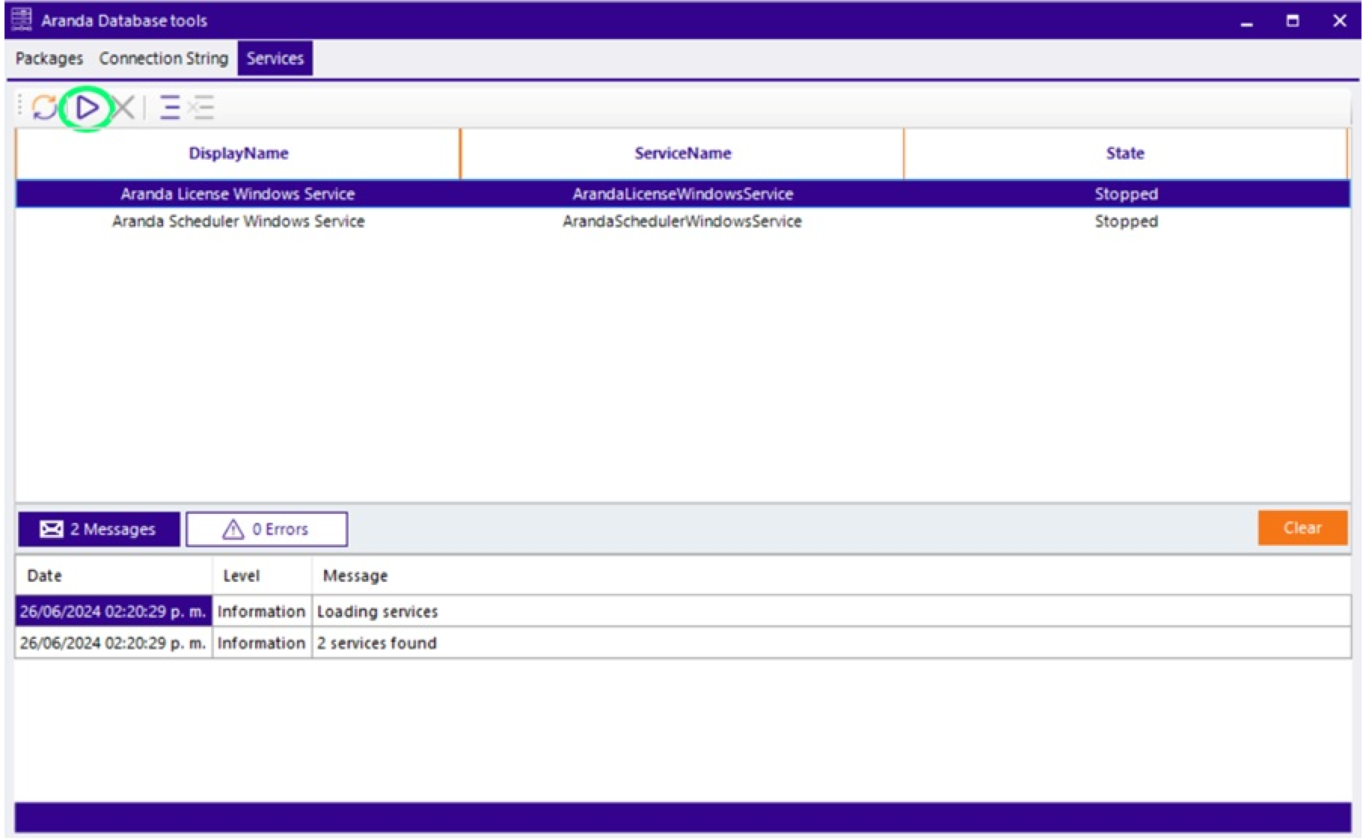
6. A window is enabled with the list of applications and services available on the server.



□ Web Applications
☑ Windows Services
☑ C:\Program Files (x86)\Aranda\Aranda License\Aranda.License.Windows.Service.exe.config
☑ C:\Program Files (x86)\Aranda\Aranda Services\Aranda.Common.Windows.Service.exe.config

☑ Encrypt

7. Select the appropriate services and click the Apply, If you want to encrypt the connection, check the box Encrypt in the lower-left corner. An alert message may be displayed because encryption is not supported for JSON files. 8. To finish, click on the Services and start all services.



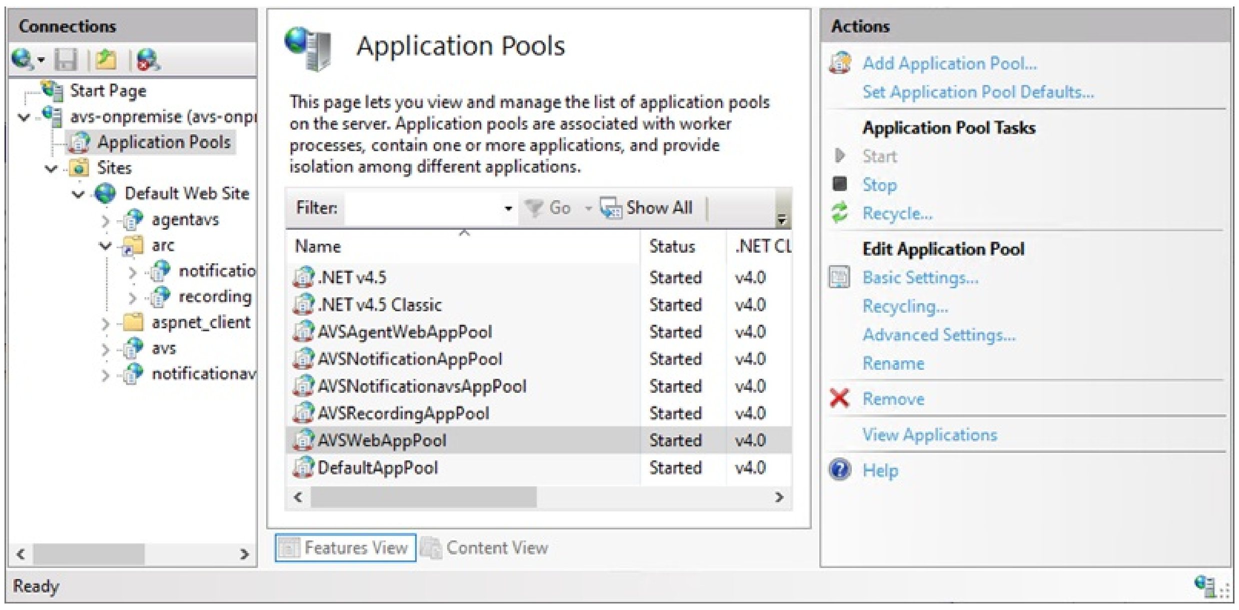
DisplayName	ServiceName	State
Aranda License Windows Service	ArandaLicenseWindowsService	Stopped
Aranda Scheduler Windows Service	ArandaSchedulerWindowsService	Stopped

2 Messages

0 Errors

Date	Level	Message
26/06/2024 02:20:29 p. m.	Information	Loading services
26/06/2024 02:20:29 p. m.	Information	2 services found

⚠ Important When changes are made to the connection strings of the sites, the application pool associated with the site must be restarted or recycled so that the change is applied immediately.

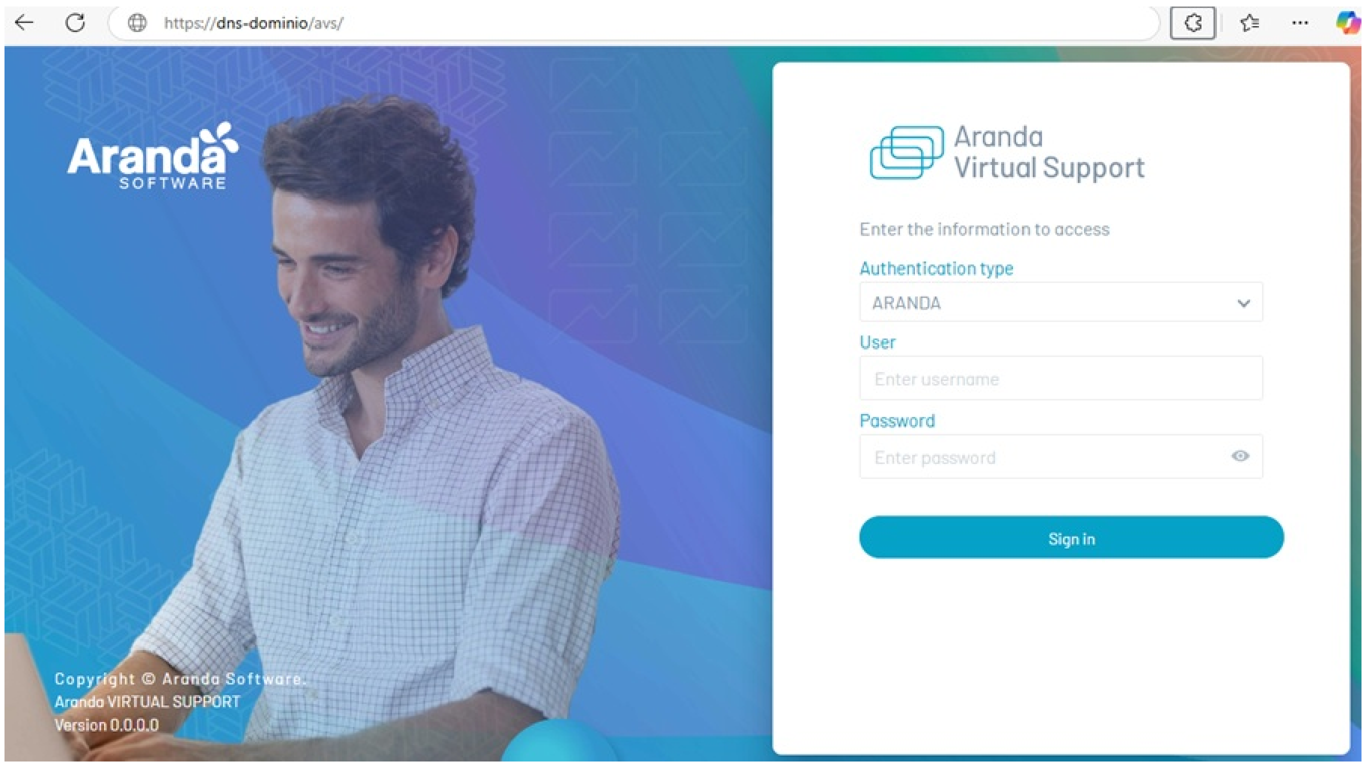


Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CL
.NET v4.5	Started	v4.0
.NET v4.5 Classic	Started	v4.0
AVSAgentWebAppPool	Started	v4.0
AVSNotificationAppPool	Started	v4.0
AVSNotificationavsAppPool	Started	v4.0
AVSRecordingAppPool	Started	v4.0
AVSWebAppPool	Started	v4.0
DefaultAppPool	Started	v4.0

9. Once the connection is established, you will be able to access the AVS website where you can start with the configuration of Aranda Virtual Support through the following URL: https://dns_servidor/avs/.



Enter the information to access

Authentication type
ARANDA

User
Enter username

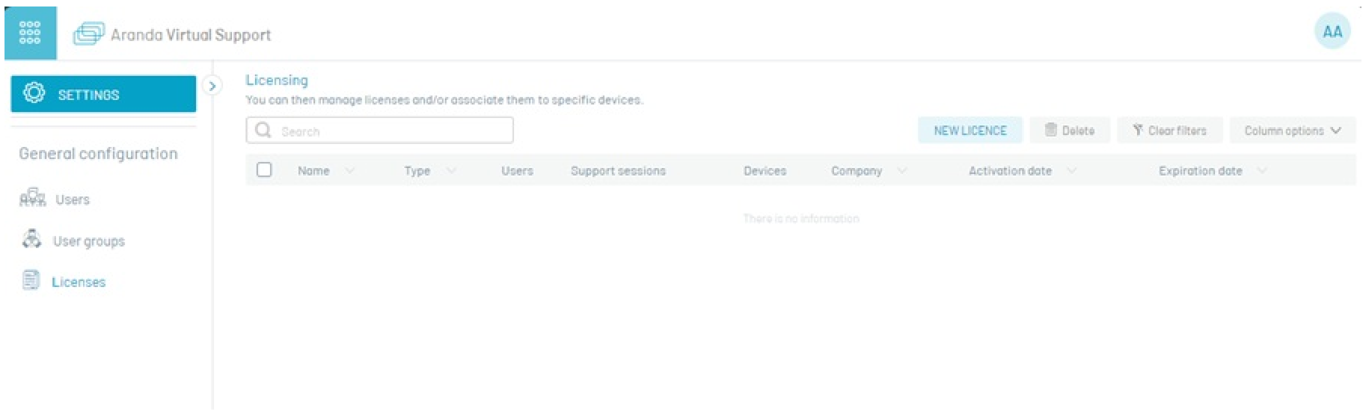
Password
Enter password

AVS Licensing

All Aranda Software products require a license to operate, so the first time you enter the Aranda Virtual Support (AVS) website, select the option Licences from the main menu where you can add new licenses and view the list of existing licenses grouped with the following data:

Column	Description
Name	It is the name of the Aranda product assigned to the license.
Guy	Type of license.
Users	Number of concurrent users (Number of licenses used/total number of licenses).
Support sessions	Number of concurrent support sessions (Number used/total number of licenses).
Devices	Number of Concurrent Workstations (Number of Licenses Used/Total Number of Licenses).
Enterprise	Company that owns the license.
Activation Date	Date on which the licenses are activated.
Expiration Date	Expiration date of licenses.

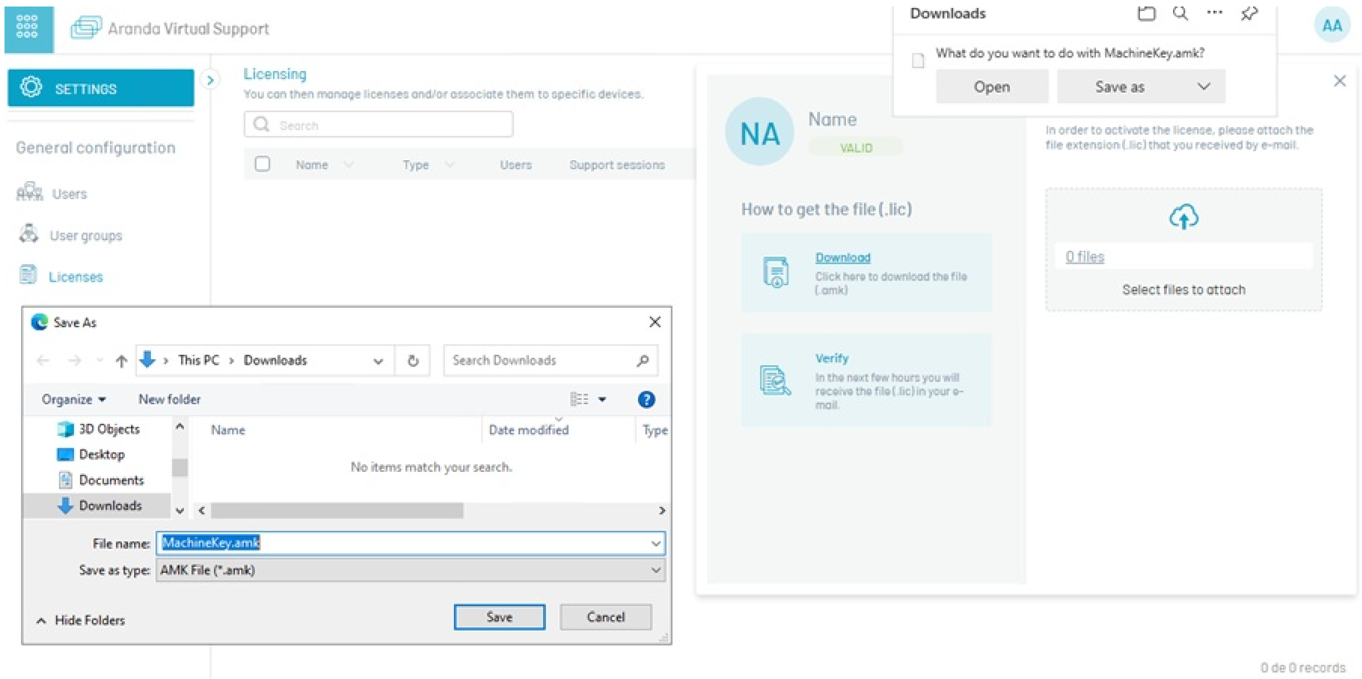
In the Licensing window, click NEW LICENSE.



You can then manage licenses and/or associate them to specific devices.

There is no information

In the pop-up window, select the option Download, which allows the download of the MachineKey.amk file, which must be sent to the area in charge of Aranda Software (Pre-Sales and Projects) for the generation of the .lic file (licensing file).



What do you want to do with MachineKey.amk?

You can then manage licenses and/or associate them to specific devices.

Click here to download the file (.amk)

In the next few hours you will receive the file (.lic) in your e-mail.

In order to activate the license, please attach the file extension (.lic) that you received by e-mail.

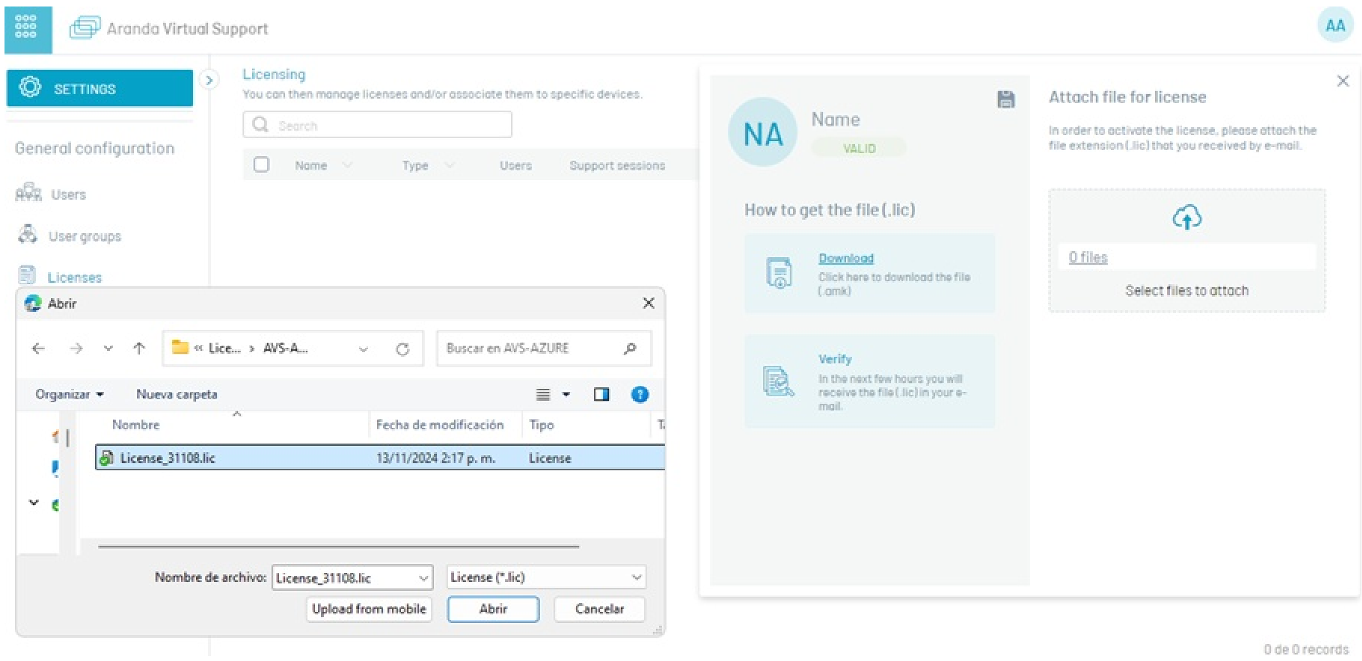
No items match your search.

File name: MachineKey.amk

Save as type: AMK File (*.amk)

0 de 0 records

Once you have received the .lic file you must upload it to the server, click on the Select files to attach and then in Save (diskette-shaped icon). When the license is loaded, the corresponding alert is generated.



You can then manage licenses and/or associate them to specific devices.

Click here to download the file (.amk)

In the next few hours you will receive the file (.lic) in your e-mail.

In order to activate the license, please attach the file extension (.lic) that you received by e-mail.

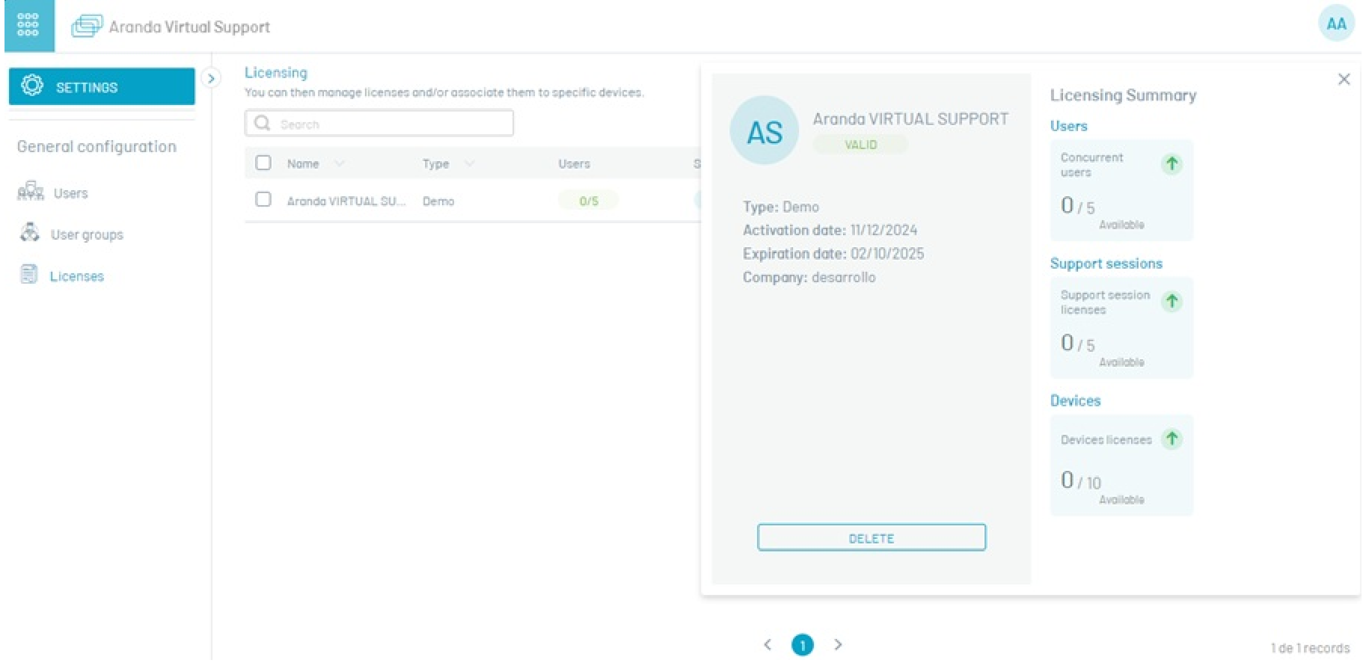
License_31108.lic 13/11/2024 2:17 p. m. License

Nombre de archivo: License_31108.lic

License (*.lic)

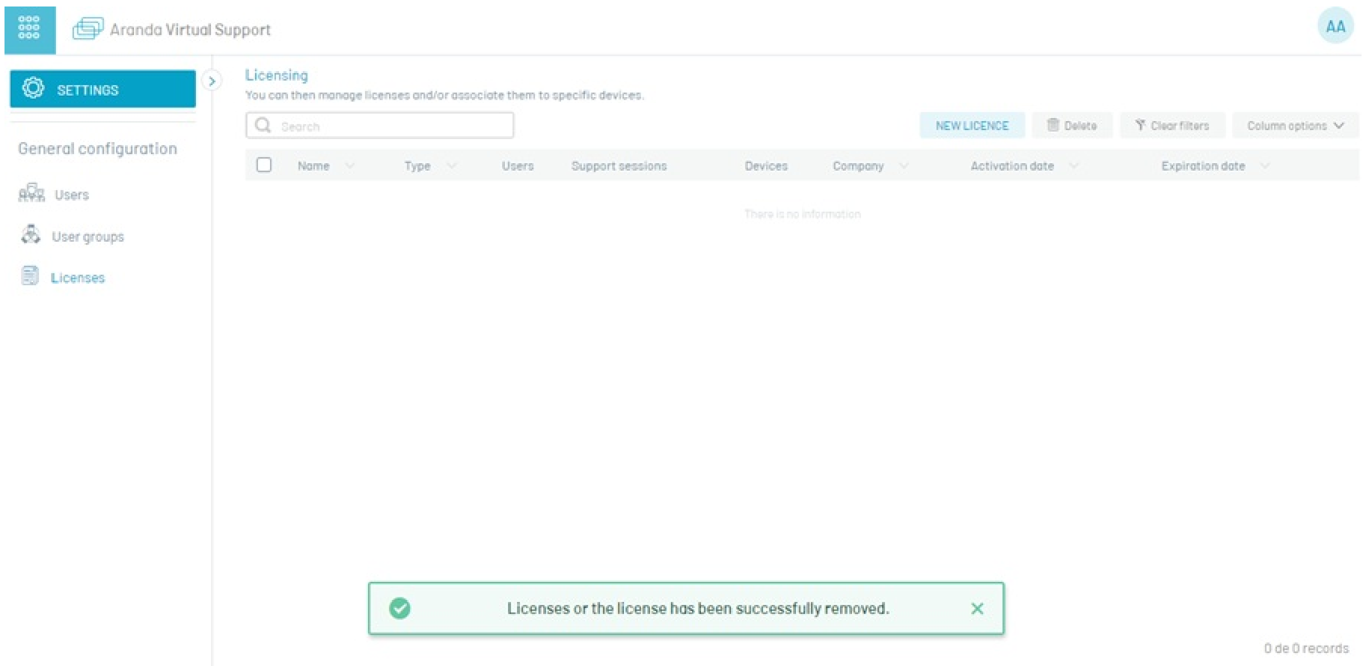
0 de 0 records

To know in detail the license, in the window Licensing, select a record from the list of available licenses and in the window that is enabled you will be able to view the validity of the license and the number of licenses that have been used by users, support sessions and concurrent devices (Number of licenses used/total number of licenses).



Type: Demo
Activation date: 11/12/2024
Expiration date: 02/10/2025
Company: desarrollo

To delete a license, in the Licensing Select the license record you want to delete and click the Eliminate, it will be confirmed that the license has been successfully deleted.



Licenses or the license has been successfully removed.

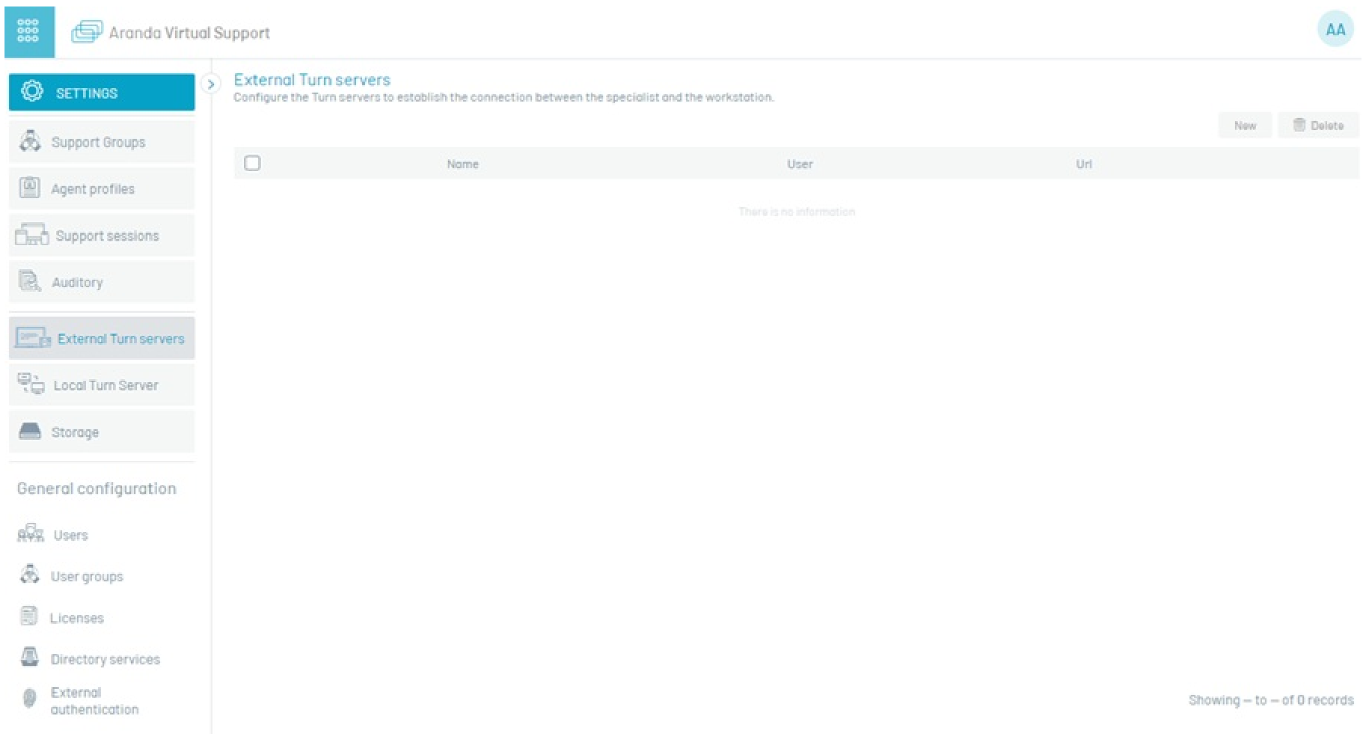
Subsequent configurations

Infrastructure Configuration

After installing the Aranda Virtual Support (AVS) sites and services, it is necessary to make some configurations from the AVS website to ensure the correct functioning of the application during the remote control and file transfer processes. Therefore, it is recommended to follow the following steps:

1. Enter the website

Log in to the AVS website with a user who has the General Administrator or Infrastructure role. These roles have the necessary permissions to manage the External Turn Servers, Local Turn Server, and Storage options. It is important to note that these options are only available in On Premise facilities.



2. External Turn Servers

AVS file transfer functionality uses a WebRTC-based P2P protocol. When two devices are unable to establish a direct connection to each other, a Turn server is needed to facilitate communication.

To add an external Turn server in the External Turn Servers, follow these steps:

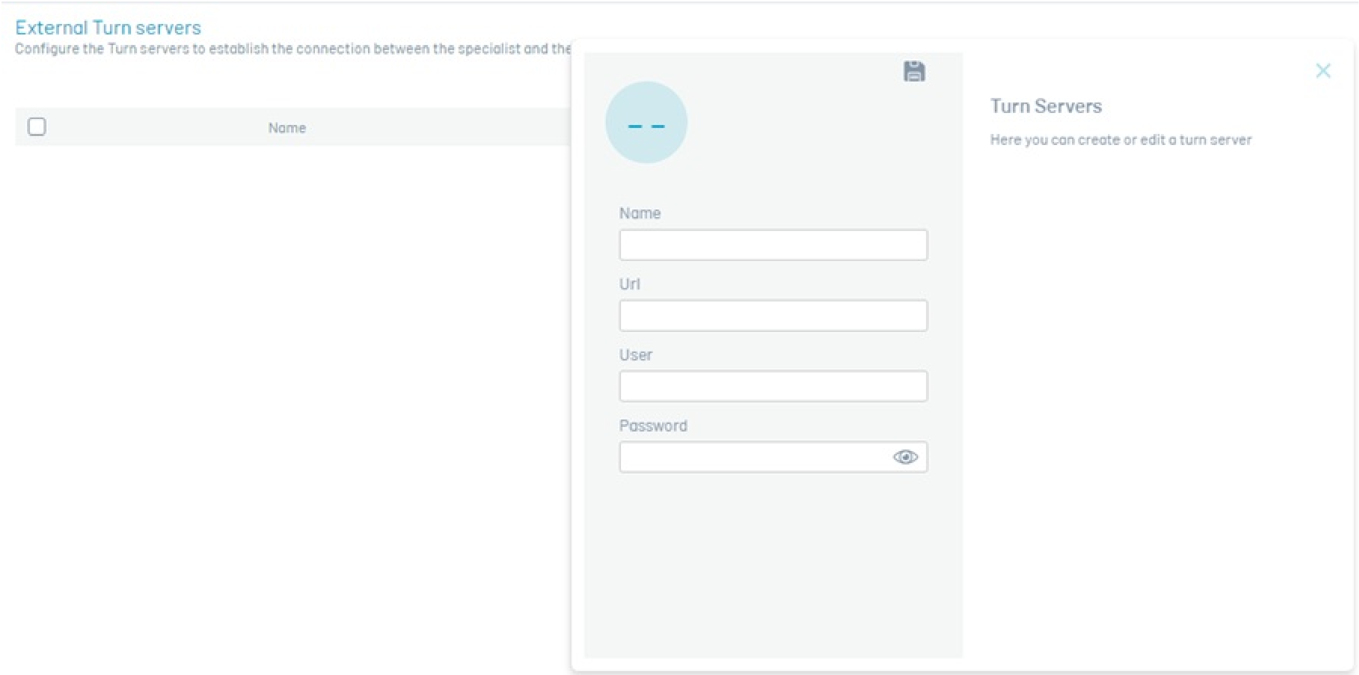
A. Click on the option New.

B. Complete the requested fields according to the following table:

Field	Description
Name	Name that you want to assign to the configuration, between 6 and 50 characters.
URL	It corresponds to the STUN/TURN server site, for example: turn:<server_public_ip>:puerto or stun:<server_public_ip>:puerto .
User	Name of the user authorized to connect to the STUN/TURN server.
Password	Password associated with the user that allows the connection to the STUN/TURN server.

C. Finish by clicking the Save.

> ⚐ Note: This configuration is required for file transfer when the specialist agent and the workstation agent are not on the same network, therefore, both devices must be allowed to exit to the Internet through the configured port.



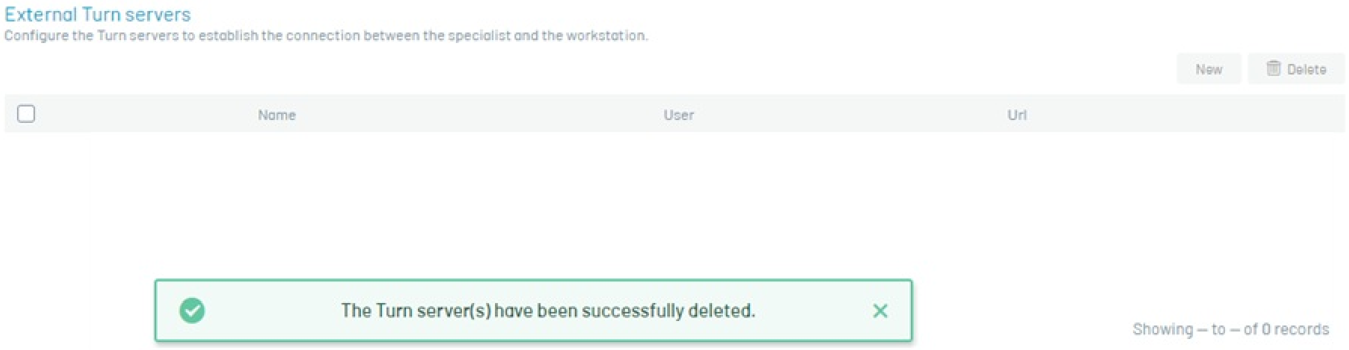
External Turn servers

Configure the Turn servers to establish the connection between the specialist and the

Turn Servers

Here you can create or edit a turn server

The user can register the number of external Turn servers that he or she deems necessary (maximum 10) to have good communication between the specialist's devices and the workstation through the AVS console. To delete an external Turn server, in the External Turn Servers Select the server(s) to delete and click the Eliminate. It will be confirmed that the server(s) have been successfully deleted.



External Turn servers

Configure the Turn servers to establish the connection between the specialist and the workstation.

The Turn server(s) have been successfully deleted.

Showing – to – of 0 records

You can use public STUN/TURN WebRTC, by doing a web search "STUN server list" you will be able to list the different public STUN/TURN servers available. When configuring public servers on workstations and on specialist computers, they must allow the output of the servers that are configured to the sites. It is also possible to configure the STUN/TURN server provided in the installer by making the settings in the Aranda Turn Stun WebRTC Server Windows Service. In addition, public STUN/TURN can be used in conjunction with your own installed servers, as mentioned above.

3. Turn Local Server

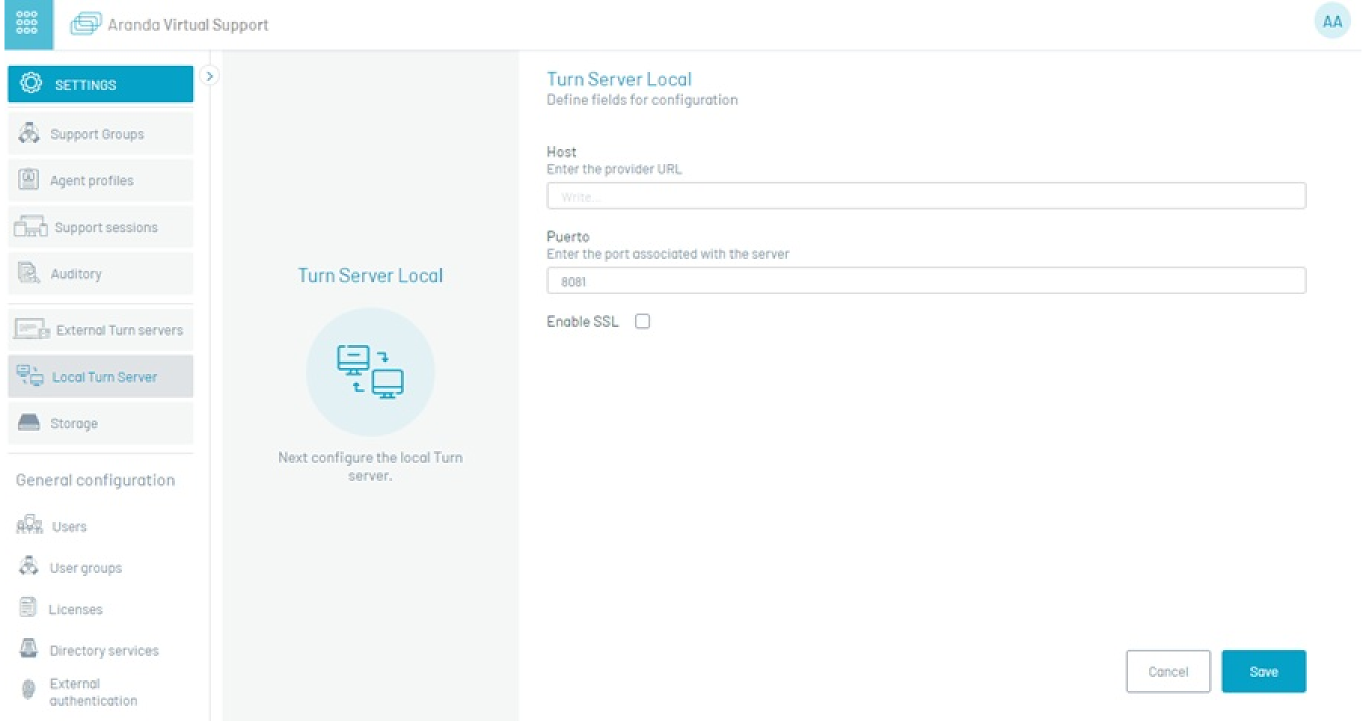
To establish remote takeover communication between the specialist agent and the workstation agent, use a local Turn server that can relay network traffic.

To add a local Turn server, follow these steps:

A. Click on the option Local Turn Server from the main menu.

B. Complete the field Host with the path to the local server, which can be the IP of the server or the DNS. The countryside Port is configured by default with the value 8081 and SSL is inactive, if the port is changed or SSL is activated, the following must be make the settings in the Aranda AVS Turn Server service installed on the server.

C. Finish by clicking the Save



Turn Server Local
Define fields for configuration

Host
Enter the provider URL
Write...

Puerto
Enter the port associated with the server
8081

Enable SSL ☐

4. Storage

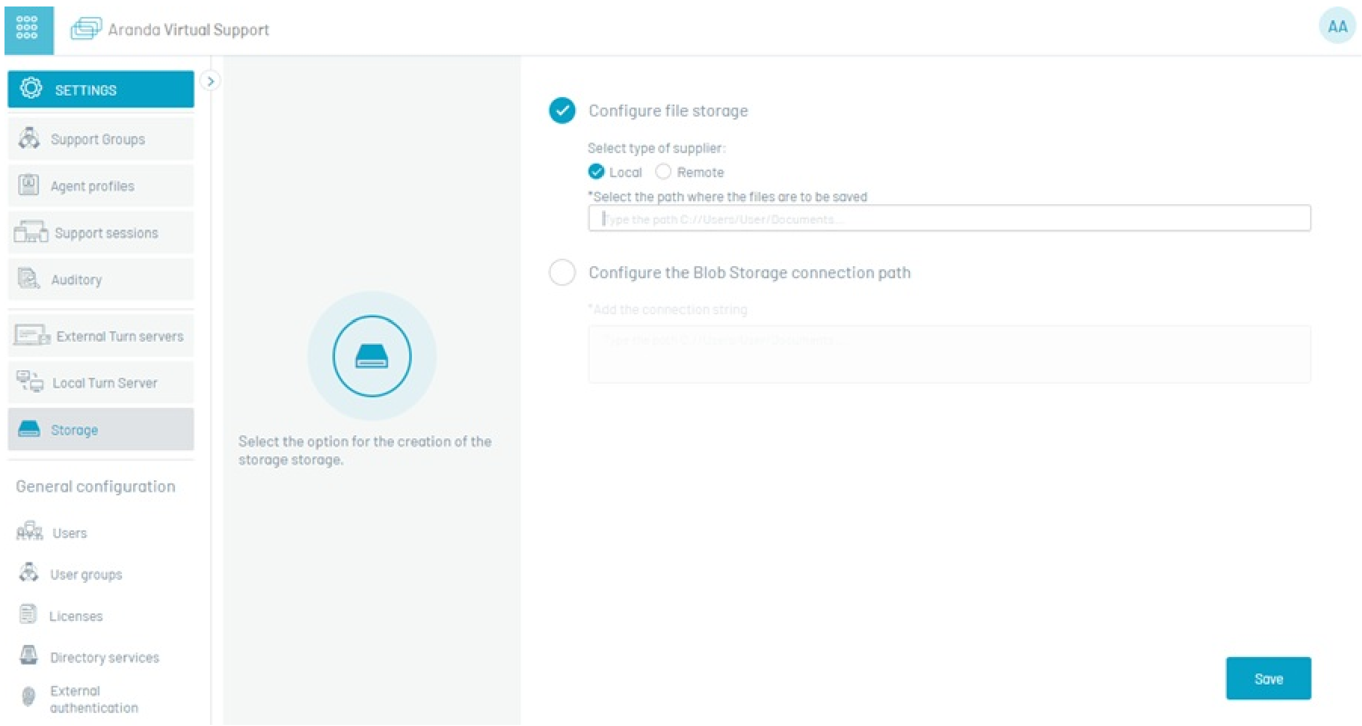
This configuration is required to store recordings of the Remote Control Service Delivery and Agent Installers for workstations. The generated files are sent to a storage provider. The provider can be of three types: local, remote, or blob storage.

To configure your storage provider, follow these steps:

A. Click on the option Storage from the main menu.

B. Fill in the requested field(s) depending on the type of storage selected.

C. Finish by clicking the Save



● Configure file storage

Select type of supplier:
● Local ○ Remote
*Select the path where the files are to be saved
Type the path C://Users/User/Documents...

○ Configure the Blob Storage connection path

*Add the connection string
Type the path C://Users/User/Documents...

⚐ Notes:

- In order for the recordings to be stored correctly, the server where the site is installed will be Avs and arc/recording You must have access to the configured provider. If you are using the local type provider, the path must exist on the server and have the corresponding permissions.
- In order for installers to be stored correctly, the server where the Common services are installed (Worker) must have access to the configured provider. If you are using the local type provider, the path must exist on the server and have the corresponding permissions.
- If the Worker and the site of the Agents are installed on separate servers, it must be ensured that both can access the configured storage, so that the agent update is carried out correctly.
- If, after configuration, changes are made to the storage provider, it is necessary to move the information contained in the previous provider to the current one. If this action is not performed, agent updates will not be successful and recordings will not be accessible in audits.

Manual Service Configuration

Configuring the Turn Server

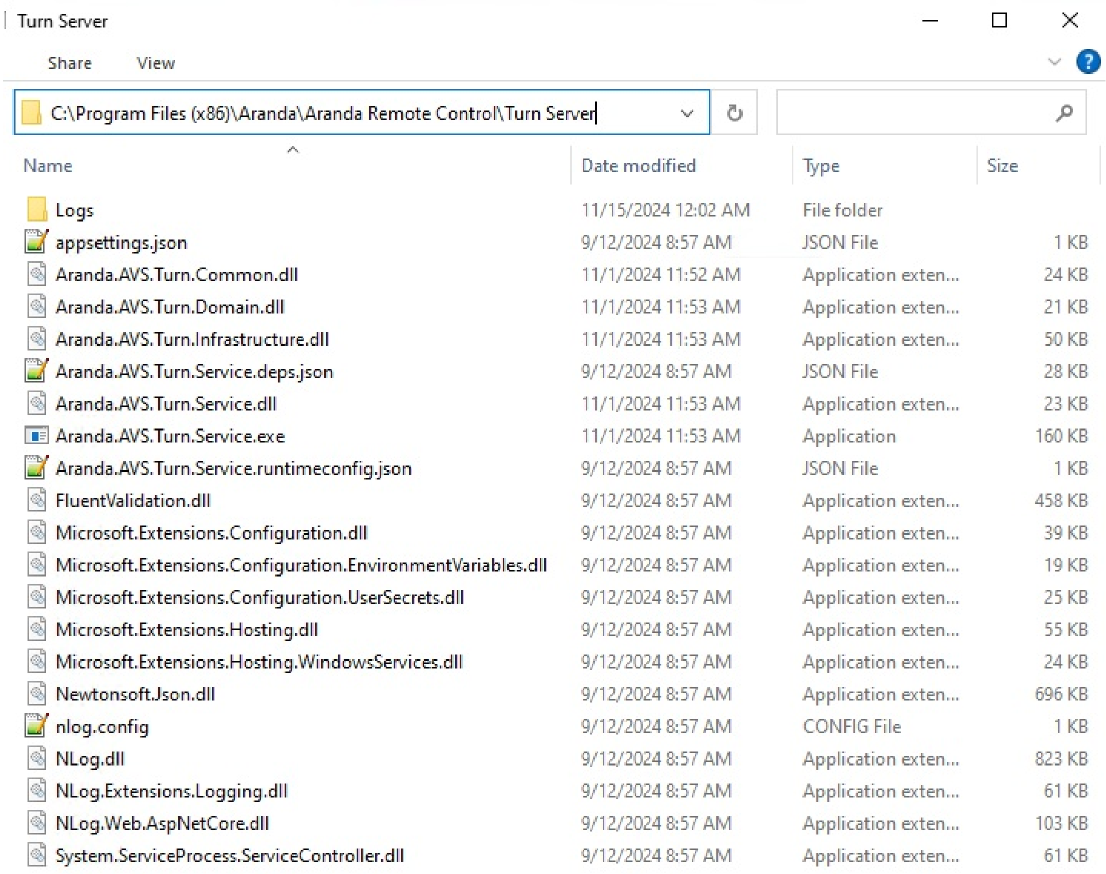
↩ Turn Local Server

After installing the Aranda AVS Turn Server service, you don't need to make any adjustments for its operation. However, parameterizations can be made according to specific needs, such as changing the connection port (8081 by default) and enabling SSL (disabled by default). If you need to make these settings, follow these steps:

1. Validating the appsettings.json File

Before making changes, check the appsettings.json located in the service installation path (default: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) to ensure that the port is set to 8081 by default. If the port does not need to be modified, no further adjustments are required.

Additionally, validate that port 8081 is enabled in the local firewall rules to ensure the correct flow of traffic. In this file, you can also find the setting for SSL certificates, which is disabled by default (IsSsl=false).



Turn Server

C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server

Name	Date modified	Type	Size
Logs	11/15/2024 12:02 AM	File folder	
appsettings.json	9/12/2024 8:57 AM	JSON File	1 KB
Aranda.AVS.Turn.Common.dll	11/1/2024 11:52 AM	Application exten...	24 KB
Aranda.AVS.Turn.Domain.dll	11/1/2024 11:53 AM	Application exten...	21 KB
Aranda.AVS.Turn.Infrastructure.dll	11/1/2024 11:53 AM	Application exten...	50 KB
Aranda.AVS.Turn.Service.deps.json	9/12/2024 8:57 AM	JSON File	28 KB
Aranda.AVS.Turn.Service.dll	11/1/2024 11:53 AM	Application exten...	23 KB
Aranda.AVS.Turn.Service.exe	11/1/2024 11:53 AM	Application	160 KB
Aranda.AVS.Turn.Service.runtimeconfig.json	9/12/2024 8:57 AM	JSON File	1 KB
FluentValidation.dll	9/12/2024 8:57 AM	Application exten...	458 KB
Microsoft.Extensions.Configuration.dll	9/12/2024 8:57 AM	Application exten...	39 KB
Microsoft.Extensions.Configuration.EnvironmentVariables.dll	9/12/2024 8:57 AM	Application exten...	19 KB
Microsoft.Extensions.Configuration.UserSecrets.dll	9/12/2024 8:57 AM	Application exten...	25 KB
Microsoft.Extensions.Hosting.dll	9/12/2024 8:57 AM	Application exten...	55 KB
Microsoft.Extensions.Hosting.WindowsServices.dll	9/12/2024 8:57 AM	Application exten...	24 KB
Newtonsoft.Json.dll	9/12/2024 8:57 AM	Application exten...	696 KB
nlog.config	9/12/2024 8:57 AM	CONFIG File	1 KB
NLog.dll	9/12/2024 8:57 AM	Application exten...	823 KB
NLog.Extensions.Logging.dll	9/12/2024 8:57 AM	Application exten...	61 KB
NLog.Web.AspNetCore.dll	9/12/2024 8:57 AM	Application exten...	103 KB
System.ServiceProcess.ServiceController.dll	9/12/2024 8:57 AM	Application exten...	61 KB

Default appsettings.json settings:

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

2. Port Configuration Change

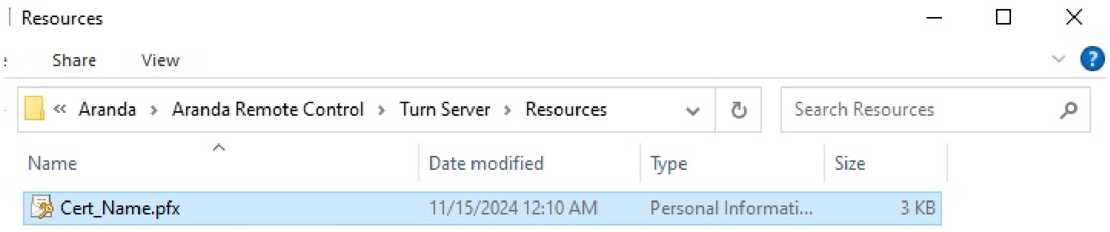
Edit the file appsettings.json and configure the desired port by replacing <puerto> by the desired port number.

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

3. SSL Secure Connection Configuration

Edit the file appsettings.json, change "IsSsl" to true. There are two alternatives to add the SSL certificate:

3.1. Acquire or generate a PFX certificate, which must be located inside the folder Resources (the folder must be created if it does not exist) in the installation path of the service.



Resources

« Aranda › Aranda Remote Control › Turn Server › Resources

Name	Date modified	Type	Size
Cert_Name.pfx	11/15/2024 12:10 AM	Personal Informati...	3 KB

The file name is recorded in the CertificatePath and the base-64 encoded key for generating the certificate must be registered in CertificateParam, both options available in the appsettings.json.

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

3.2. If you have a PFX certificate stored in the certificate bucket, you can configure it by naming the certificate in the CertificateSubject from the archive appsettings.json.

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

4. Service Restart

Restart the Turn Server service (Aranda AVS Turn Server) for the configuration changes to take effect. The service should now listen on the newly configured port and enable the use of SSL certificate.

5. Firewall Settings

Open the port that was configured in step 2 in the local firewall inbound rules. This step is crucial to allow traffic over the new port and ensure that the Turn Server can receive incoming connections on the configured port.

Parameterizing the Turn Server port and the use of SSL from the service is a fundamental process to ensure its correct functioning and adapt it to the specific needs of each customer. By following these steps, you can ensure that the Turn Server is configured correctly and ready to handle connections as required.

↩ Turn Local Server

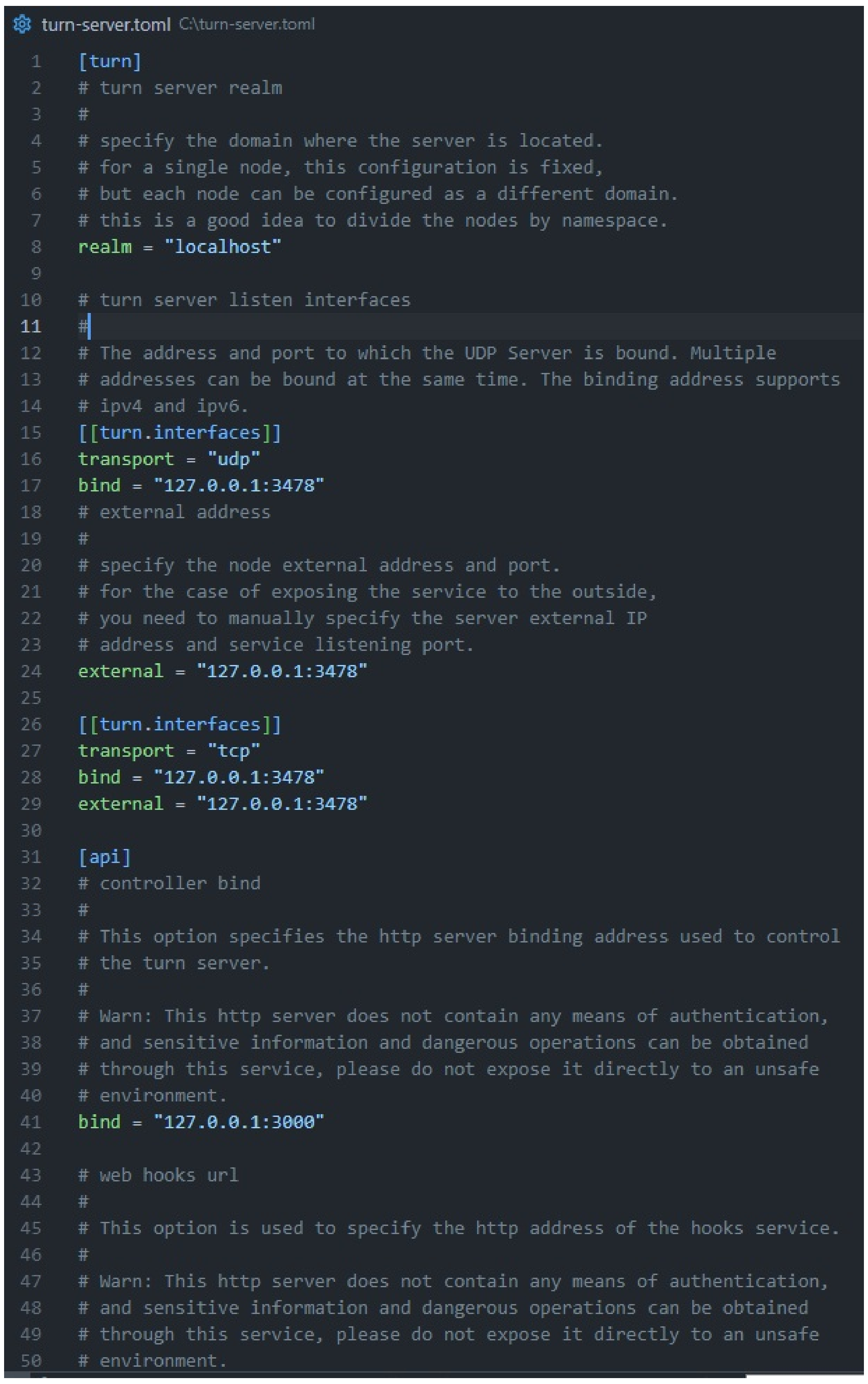
Configuring the STUN/TURN WebRTC Server

↩ External TURN Server

After you install the service Aranda Turn Stun WebRTC Server, the configuration is necessary for it to work properly.

1. File Validation turn-server.toml

Before making changes, verify that the turn-server.toml is located in the service installation path (by default: C:\Program Files (x86)\Aranda\Aranda Remote Control\Stun Server).



```
[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.
```

To configure the STUN/TURN WebRTC service, use the turn-server.toml:

- Section [turn]: Specifies the domain where the server is located.
- Section [[turn.interfaces]]: Indicates the listening interfaces. Describes the interface to which the STUN/TURN server is linked. Various interfaces can be indicated.
- Section [turn.interfaces.transport]: Defines the type of transport of the interface, which can be udp or tcp.
- Section [turn.interfaces.bind]: IP address and binding port of the internal socket.
- Section [turn.interfaces.external]: It is used to link to the address of your local NIC. For example, if you have two NICs, A and B, on your server, and the IP address of NIC A is 192.168.1.2 and that of NIC B is 192.168.1.3, if bound to IAS A, you must bind to the address 192.168.1.2. Link to 0.0.0.0 It means that you listen to all interfaces at the same time. The word external means that your network card for the customer can "see" the IP address. Continuing with the previous example, if your network card A communicates with the outside, the other clients will see your LAN address (i.e., 192.168.1.2). However, in reality, the network topology where the server is deployed might have another public IP, such as 1.1.1.1, which is the IP address seen by other clients. The reason why they are needed bind and external is that, for the STUN protocol, the server needs to report its own external IP address, thus allowing the STUN client to connect to the specified address using the IP reported by the server.
- Section [api.bind]: Listening to the API for queries, for example: http://127.0.0.1:3000/info.
- Section [log.level]: Log level. Valid values: error, warn, info, debug, trace.

- Section [auth]: Username and password to access the server.

2. Start of Service

Start the STUN Server service (Aranda Turn Stun WebRTC Server) for the configuration changes to take effect.

3. Firewall Settings

Open the port or ports configured in step 1 in the local firewall inbound rules and in the network controllers present in the client infrastructure, for the protocols TCP and UDP. This step is essential to allow traffic through the new port and ensure that the STUN server can receive incoming connections on the configured port.

On workstations (AVS Agent) and on specialist computers (Specialist Agent), they must allow egress through the ports that are configured.

Additionally, if you require it to operate as TURN WebRTC, you must open the port range 49152-65535 for the protocol UDP.

STUN/TURN Service Configuration Example and Scenarios

↩ External TURN Server

STUN/TURN Service Configuration Example and Scenarios

↩ External TURN Server

To make the server work for both devices inside and outside the network, follow these steps:

1. Set up the realm

Change the value of realm to the public domain or external IP address of your server. This is important for successfully authenticating external requests.

If your server's public address is 1.2.3.4, set it to:

```
realm = "1.2.3.4"
```

2. Set up bind

The bind ensures that the STUN/TURN server listens on the private IP for connections within the local network.

If your server's private address is 192.168.1.25, set it to:

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

If you require the STUN/TURN service to listen on all interfaces at the same time, configure it as:

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

These configurations are only required for [[turn.interfaces]].

3. Set up external

The external is where the server's public IP is defined so that external computers can properly communicate with the STUN/TURN server.

If your server's public address is 1.2.3.4, set it to:

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

4. Authentication

The [auth] It is configured with static users:

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

This allows authenticated connections with static credentials user1:test and user2:test. Be sure to use more secure credentials if you plan to expose this service to external devices.

The other sections can be left by default.

When you perform the parameterization in the turn-server.toml, this must be observed as follows:

```
[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"
```

Each time you make a modification to the turn-server.toml, restart the service Aranda Turn Stun WebRTC Server for the changes to take effect.

Scenarios

The following scenarios and the result are described below according to the settings in the sample.

Scenario	Specialist	Network Status	AVS Agent	Network Status	Result
1	You can only access the TURN/STUN server using the public IP	External	You can only access the TURN/STUN server using the public IP.	External	The Specialist and the AVS Agent can establish communication by consuming the TURN/STUN server over the public IP.
2	You can only access the TURN/STUN server using the public IP.	External	You can access the TURN/STUN server using the public IP.	Internal	The Specialist and the AVS Agent can establish communication by consuming the TURN/STUN server over the public IP.
3	You can access the TURN/STUN server using the public IP.	Internal	You can access the TURN/STUN server using the public IP.	Internal	The Specialist and the AVS Agent can establish communication by consuming the TURN/STUN server over the public IP.
4	You can only access the TURN/STUN server using the private IP.	Internal	You can only access the TURN/STUN server using the private IP.	Internal	The Specialist and the AVS Agent can establish communication by consuming the TURN/STUN server over the private IP.
5	You can only access the TURN/STUN server using the public IP.	External	You cannot use the public IP to connect to the TURN/STUN server, as your access is restricted to the internal network (private IP).	Internal	The Specialist and the AVS Agent are unable to establish communication due to a connectivity problem between networks (external and internal).
6	You can only access the TURN/STUN server using the public IP.	External	You cannot use the public IP to connect to the TURN/STUN server, as its access is restricted.	External	The Specialist and the AVS Agent are unable to establish communication due to a connectivity problem between networks.

⚠ Note:

- To cover scenarios 1, 2, and 3, configure in the AVS website the External Turn server as follows:
  Name: configuration name.
  URL: turn.1.2.3.4:3478 (1.2.3.4 refers to the server's public IP).
  User: user1.
  Password: test.

⚠ Notes:

- To cover the scenario (4), configure in the AVS website the External Turn server as follows:
  Name: configuration name.
  URL: turn.192.168.1.25:3478 (192.168.1.25 refers to the server's private IP).
  User: user1.
  Password: test.
- If in the turn-server.toml was set up 0.0.0.0 in the parameter bind, the configuration must be performed on the site as above.

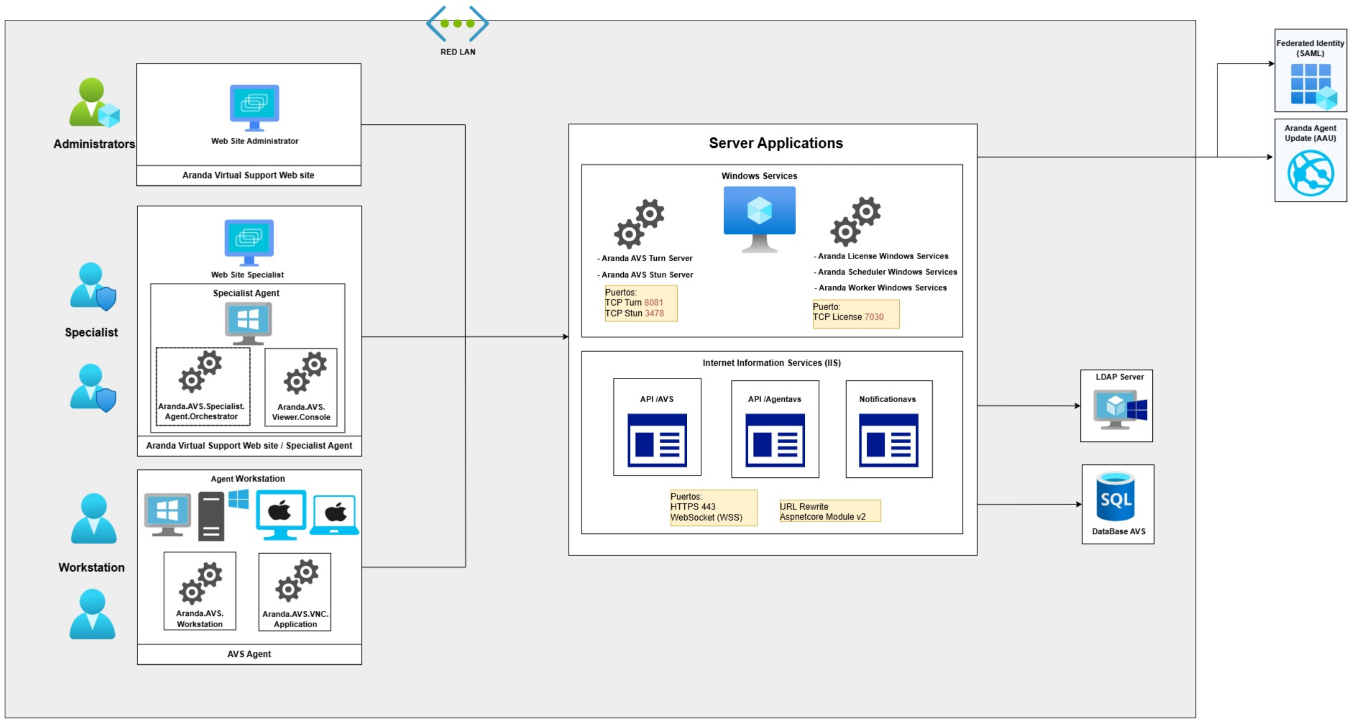
↩ External TURN Server

Deployment

Deployment Diagram

1. Diagram

The following figure shows the deployment diagram:



2. Servers

Server installation is made up of the following elements:

Windows Services: They allow the execution of tasks, agendas, among other functionalities in the background.

- Aranda AVS Turn Server: Allows the connection of the tips in a remote control session. It requires listening on port 8081, although it can be configured. Uses TCP protocol configurable to use SSL/TLS
- Aranda AVS Stun Server: Allows you to have a stun/turn WebRTC server for file transfer functionality. Listen at least on port 3478 over TCP and UDP. To allow relay, more ports can be configured over TCP or UDP.
- Common services: Common services of Aranda applications.

Web Applications: They allow web applications to be exposed over HTTPS. They all use TCP port 443. Enabling HTTPS is required

- API/AVS: Provides the capabilities of the Virtual Support product homepage.
- API/Agentavs: Allows you to register and update workstations.
- Notificationavs: Allows messages to be sent between specialists and workstations. Uses WebSocket protocol

Database Server: SQL Server Persist Structured Data

3. Users

Administrators: Manage product configurations. They use a web browser.

Specialists: They use support services such as remote control, file transfer, and chat

- Website: Use support functionalities
- Aranda.AVS.Viewer.Console: Viewer that allows remote control on workstations.
- Aranda.AVS.Specialist.Orchestrator: A Windows service that allows file transfer functionality and send remote control recordings.

Workstations: They receive help through the support functionalities. Windows and Mac OS support

- Aranda.AVS.Workstation: Windows service that offers the main functionalities
- Aranda.AVS.VNC.Application: A Windows service that allows you to take remote control.