
Aranda Device Management

Application integration is a communication process that facilitates the exchange of information and services, allowing asset management to be enhanced and functionality to be complemented with resources.

Aranda DEVICE MANAGEMENT provides the following integration solutions:

1. External Integrations

ADM currently integrates with the following external applications:

- Integration with Intel® Endpoint Management Assistant (Intel® EMA) It allows remote administration of computers when computers are turned off or the operating system is unresponsive. Using Intel® EMA, it is possible to use remote desktop and power control options, on computers inside or outside the firewall, using Intel® Active Management Technology (Intel® AMT), part of the Intel® vPro™ platform.

2. Internal Integrations

ADM natively integrates with our solutions:

- With Aranda Remote Control ARC, to take control of machines easily and efficiently and transfer files conveniently, facilitating remote management of workstations.
- With Aranda CMDB, to automatically keep CMDB configuration items up to date with discovered or detected changes to device inventories.
- With Aranda QUERY MANAGER AQM As an advanced reporting system, it allows visibility of the infrastructure through real-time indicators and access to customized reports.

Who is this Handbook for?

This manual is designed to share and deepen the possible integrations between Aranda DEVICE MANAGEMENT ADM and different applications.

What is Our Documentation?

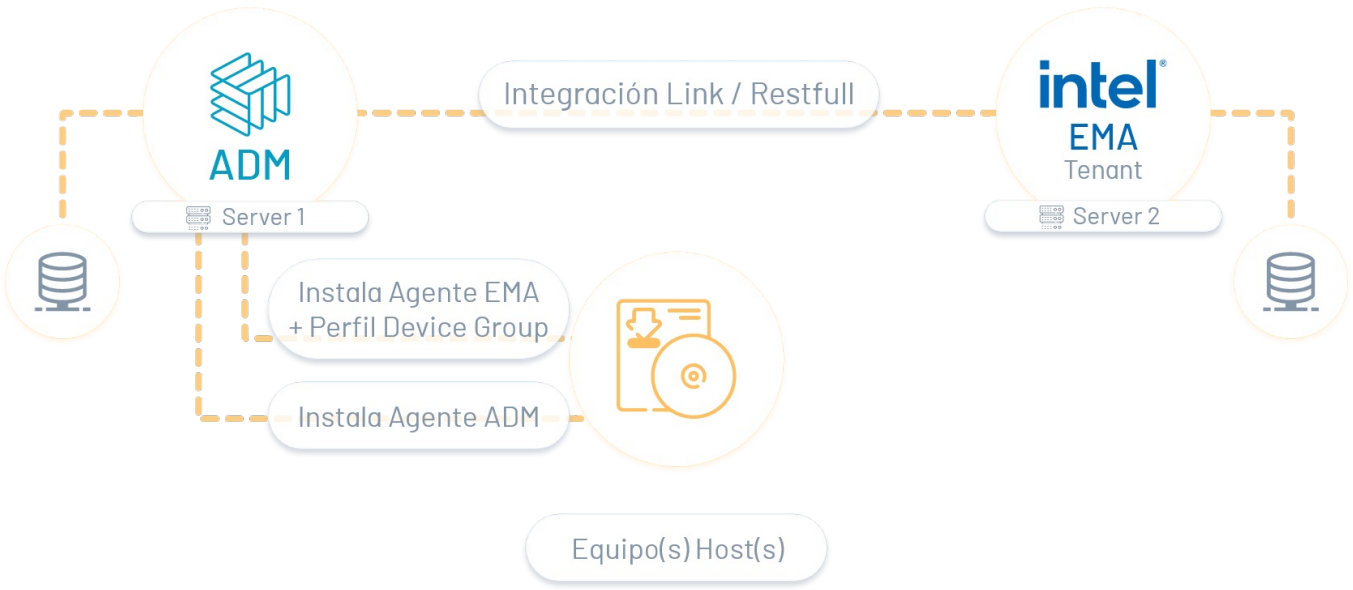
- Aranda Device Management ADM ↪ Getting Started Guide
- Aranda Device Management ADM ↪ Installation Guide
- Aranda Device Management ↪ Manual
- ADM Integration Manual (You are HERE)

Intel Ema ADM Integration

Intel EMA ADM Integration

The new integration between Aranda Device Management (ADM) and Intel® Endpoint Management Assistant (Intel® EMA) allows remote management of computers when computers are turned off or the operating system is not responding.

This is a silent synchronization, where ADM processes and verifies the information recorded by Intel® EMA, thus allowing functional capabilities from ADM with Intel® EMA for its management and administration.



In integration, different activities are carried out in parallel to take into account and Different components are used that allow the correct functioning of the applications internally and externally.

1. Activities from Intel EMMA

To have an integration, the following tasks to be performed from Intel EMMA must be taken into account:

Intel EMMA Activities	Description
User Installation and Creation	For external integration with Intel EMA is required:- EMA Server Installation and Tenant Administrator User Creation.
Intel EMMA Agent Generation	Configure and deploy the agent required by Intel® EMA with its respective tenant group configuration profile (profile that has the Intel® AMT configuration parameters).

2. Activities from ADM

To have an integration, the following tasks to be performed from ADM must be taken into account:

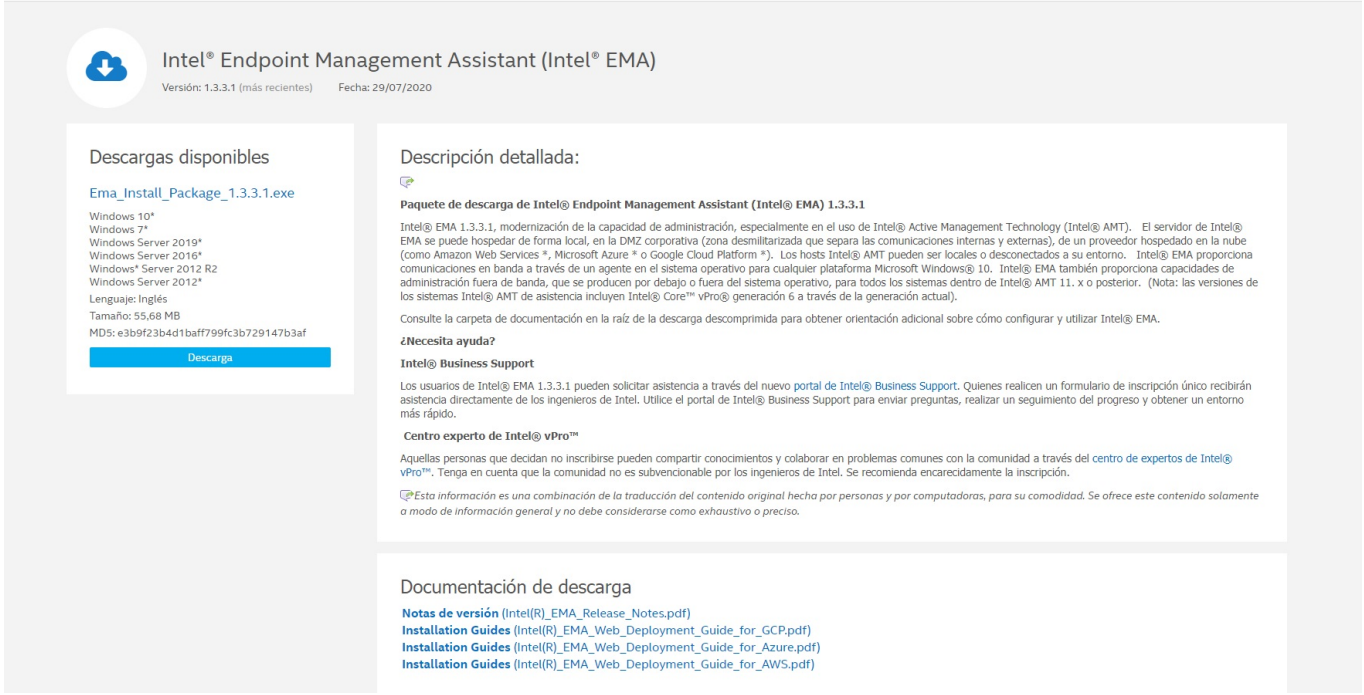
ADM Activities	Description
Configuration Integration and ADM Access	From the ADM Management Console you can: - Enable Intel_EMMA integration. - Create the Tenant Admin User. - Access the device detail within ADM's inventory management process.
API Configuration	From the ADM management console, the API Configuration which allows ADM software to be developed and integrated with other software applications.

EMA Server Installation

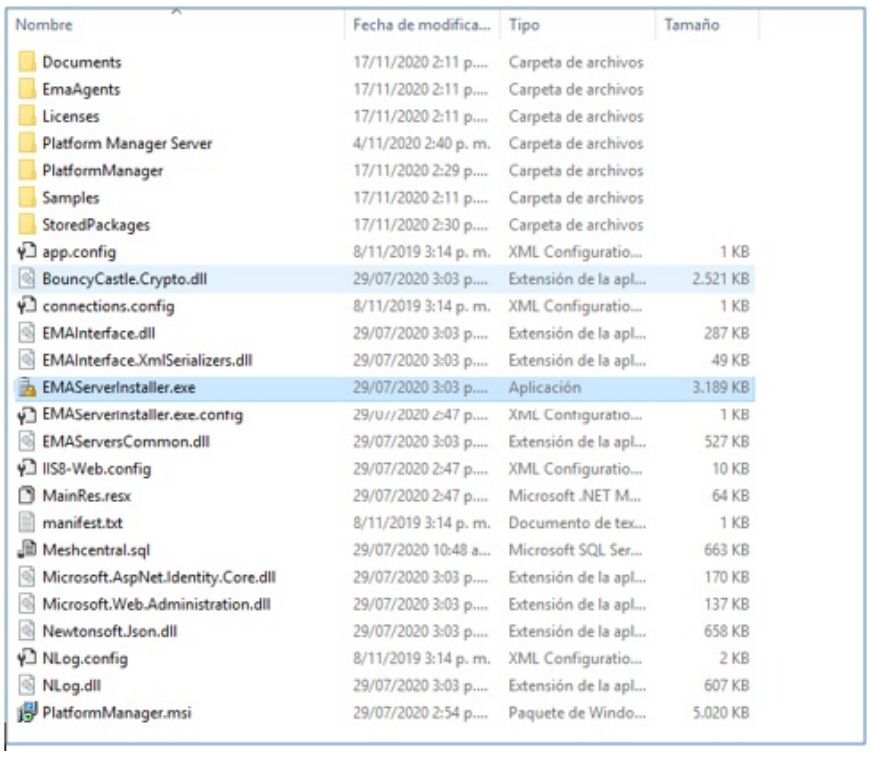
The following describes the basic Intel EMA installation for integrating with ADM.

> ⚐ Note: For all aspects of configuration, considerations, and installation, see the Intel EMA Official Documentation

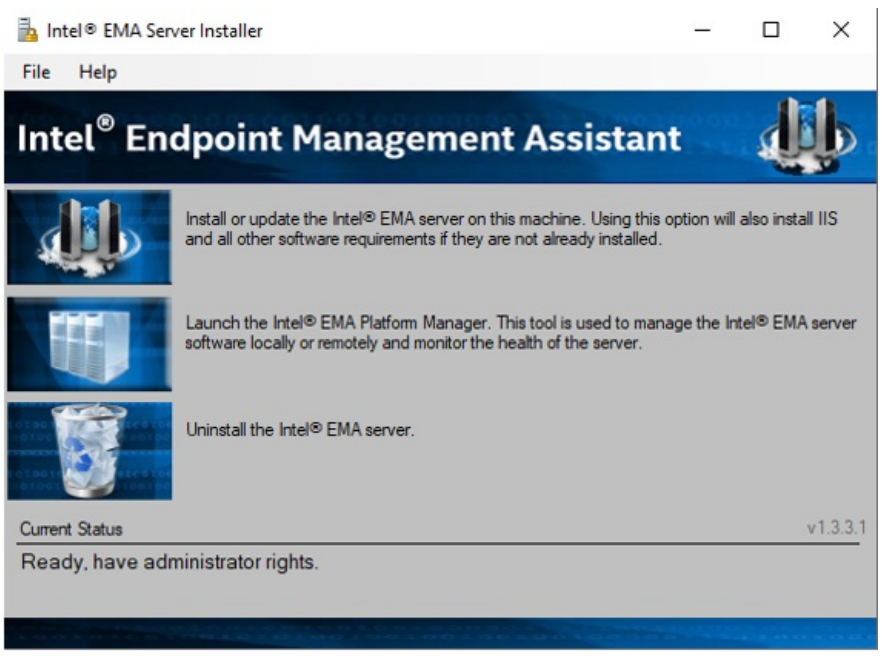
1. Download the Ema installation packages at the following path: Intel-Endpoint-Management-Assistant-Intel-EMA



2. Ejecute el archivo EMAServerInstaller.exe.

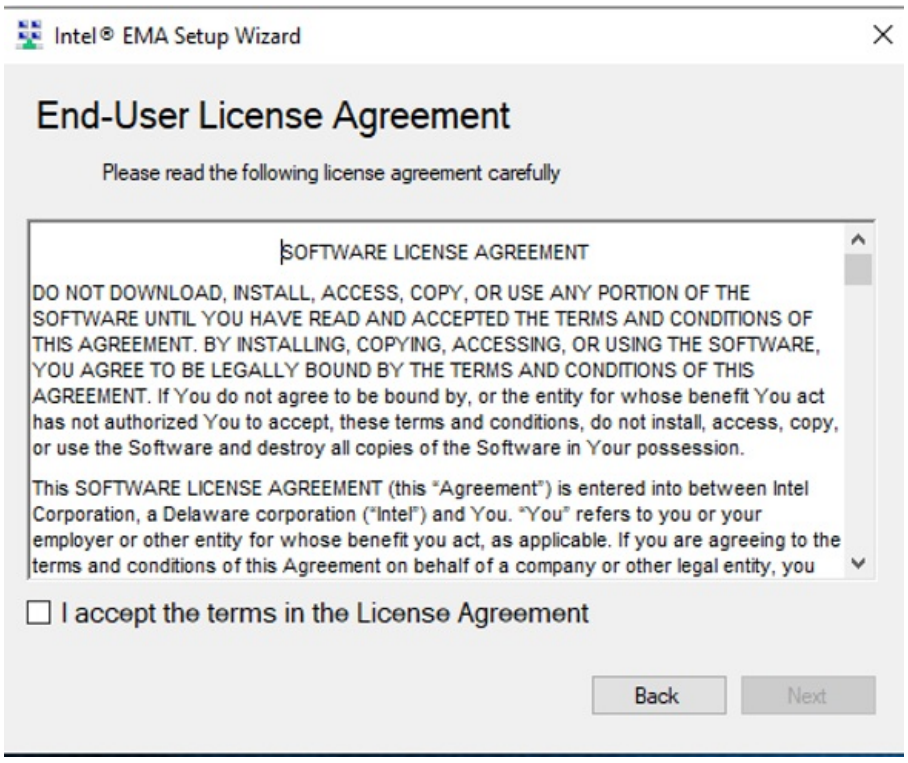


3. Install the Ema server and select option 1.

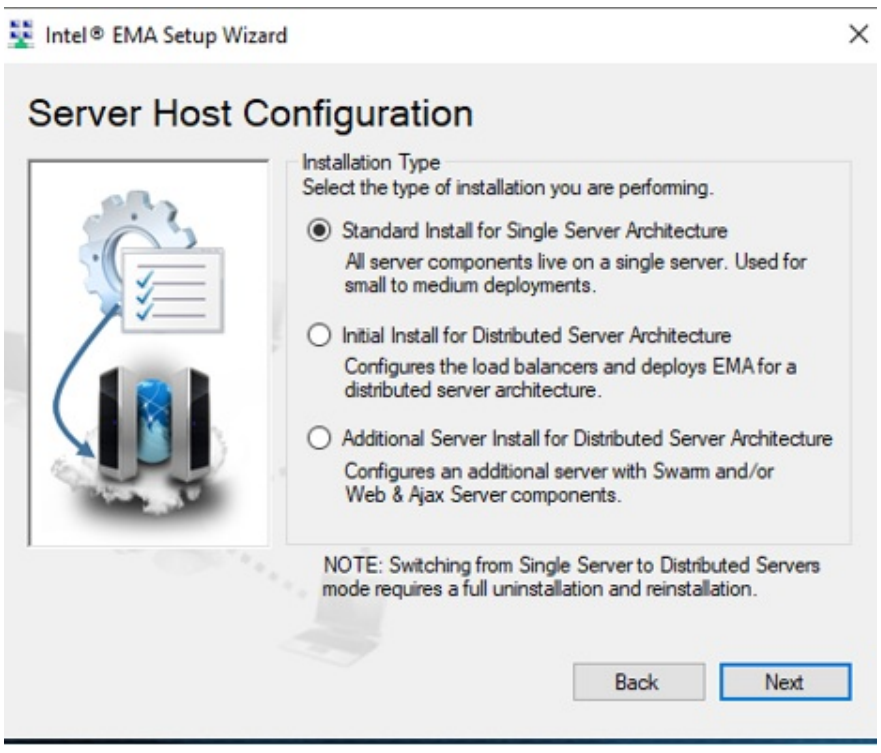


4. You must meet the recommendation to have the IIS configured for the Windows operating system.

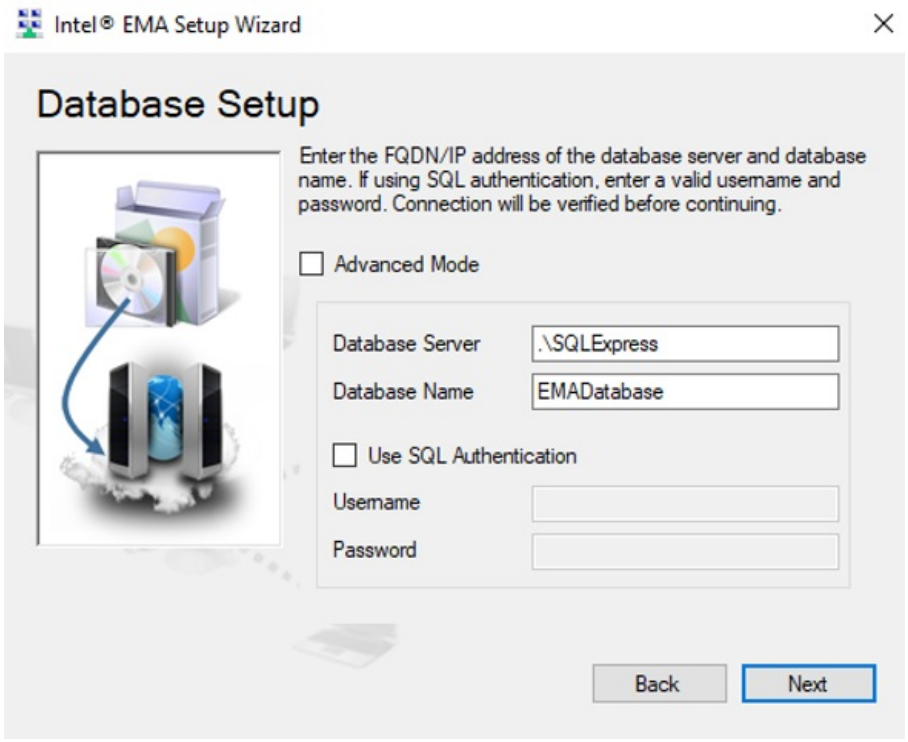
5. Lea el acuerdo de instalación y hacer clic en Siguiente.



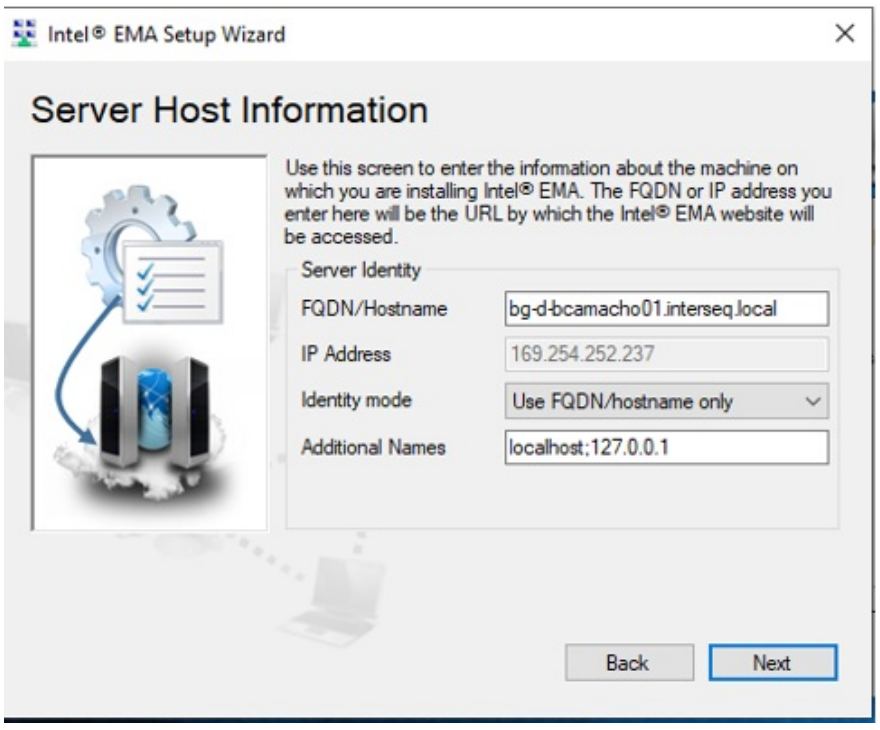
6. Select the type of installation:



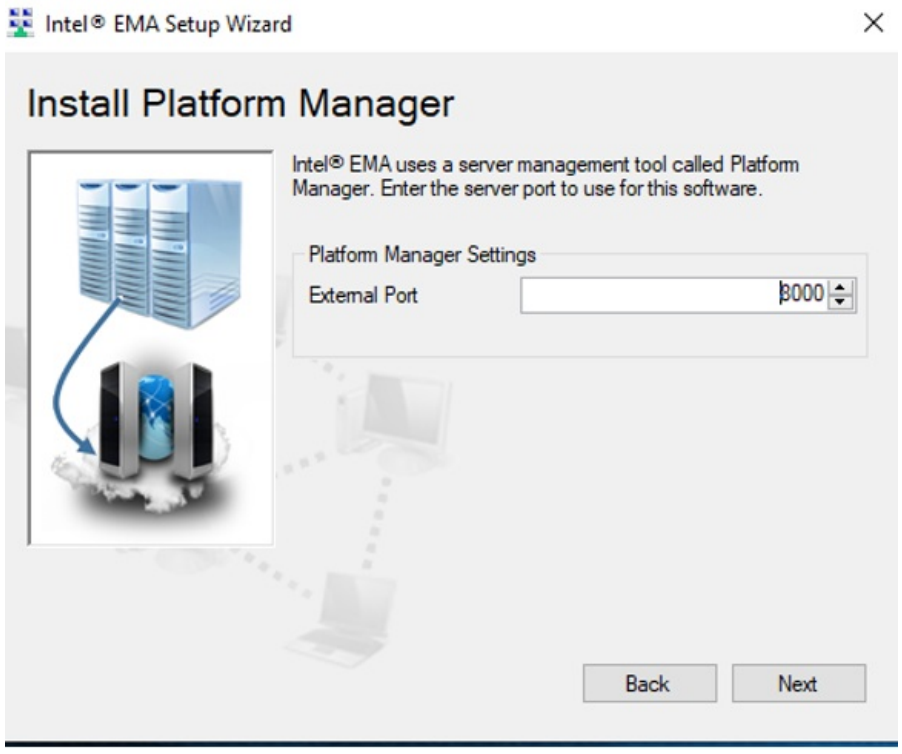
7. Seleccione la instancia de base de datos Sql Server.



8. Configure the Host Information.

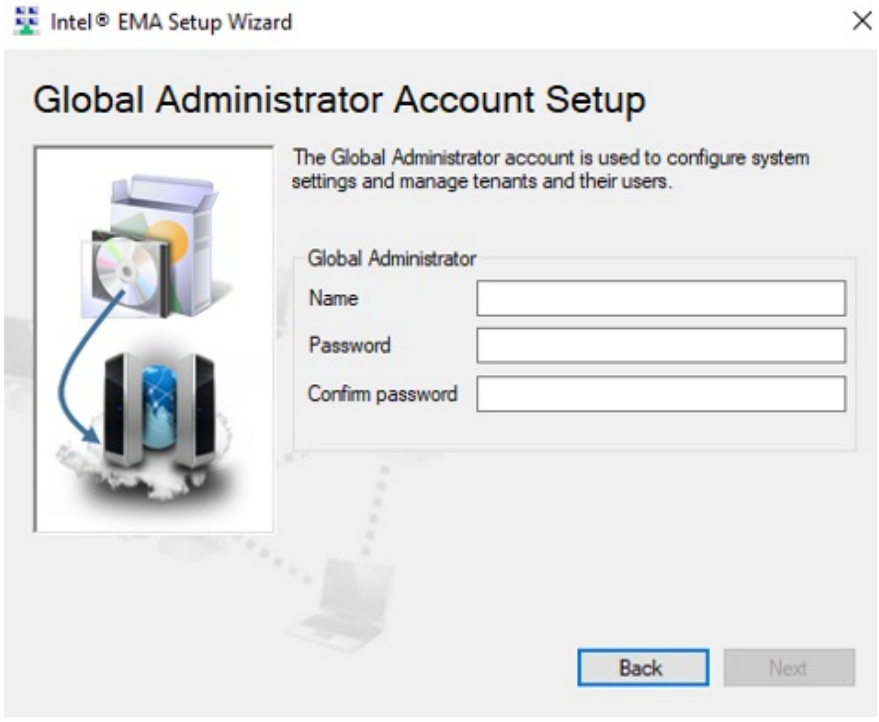


9. Install the Platform Manager.

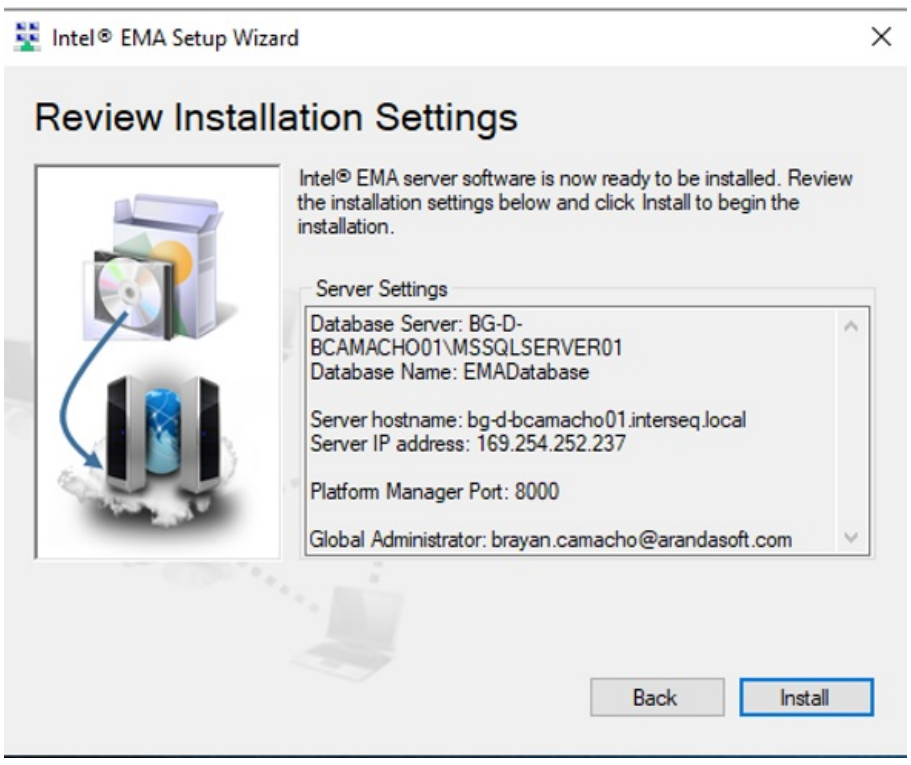


10. Configure the user authentication type.

11. Add the administrator user name for the entire EMA instance and save the credentials for general EMA management.

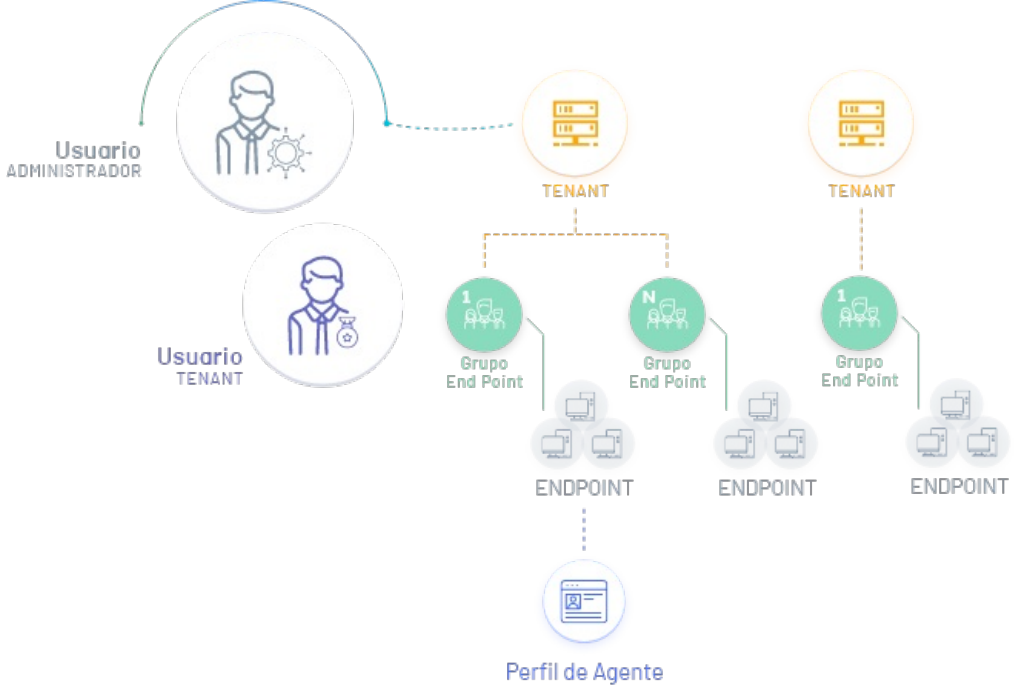


12. Click Install.

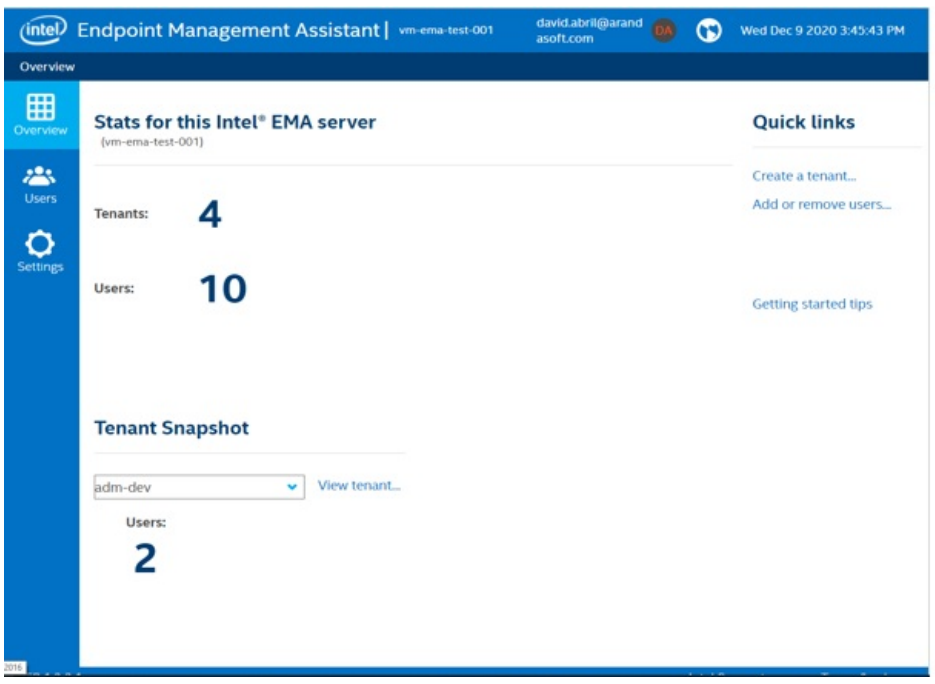


Tenant Configuration and Endpoint Groups

In this stage of configuration from Intel EMA, permissions are defined at the hierarchy level in the application, where the local administrator creates the tenants, then the Endpoint, endpoint and agent profile groups.



1. Log in to the Enpoint Management Assistant console as a Global Administrator, with the user configured during installation. Enn the option Overview from the main menu you will be able to see the defined statuses.

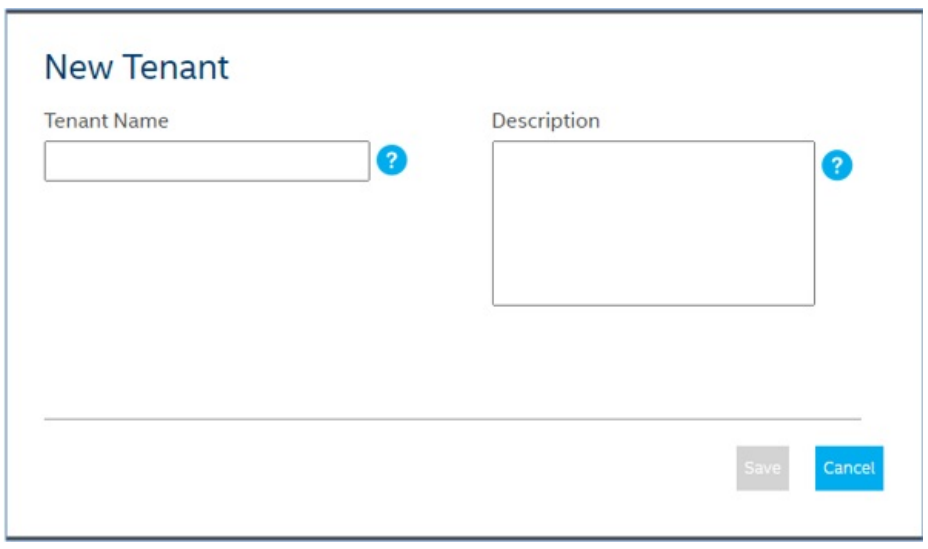


Create Ternant

2. To create the tenant in the Quick Links section of the information view, select the Create a Tenant. The window to enter name and description is enabled.

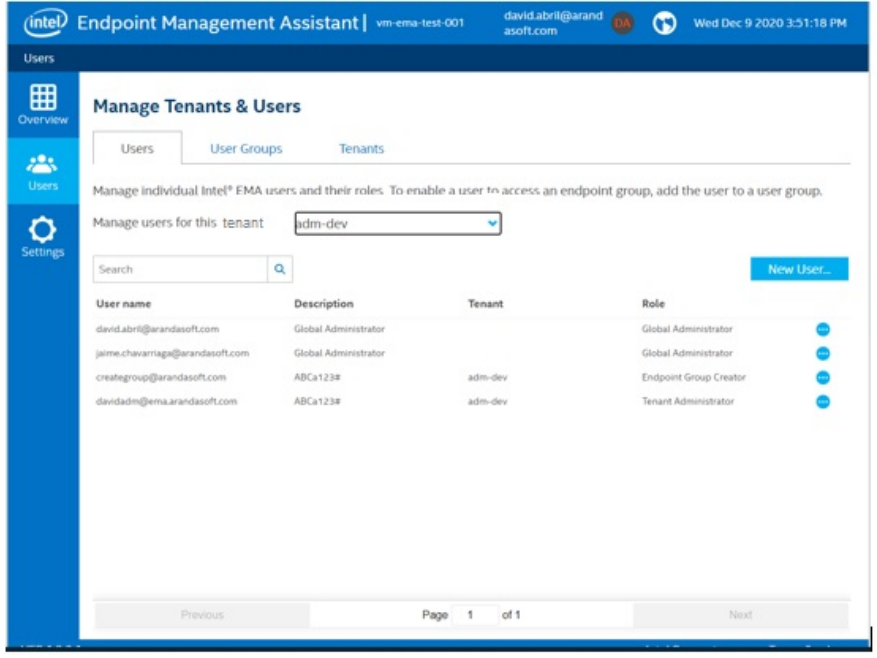
This is the tenant that you will integrate with ADM (If you are using the EMA instance to synchronize different ADM instances, you must create a tenant for each instance, it is recommended to use the client's name to differentiate). }

3. When the setup is complete, click Save.

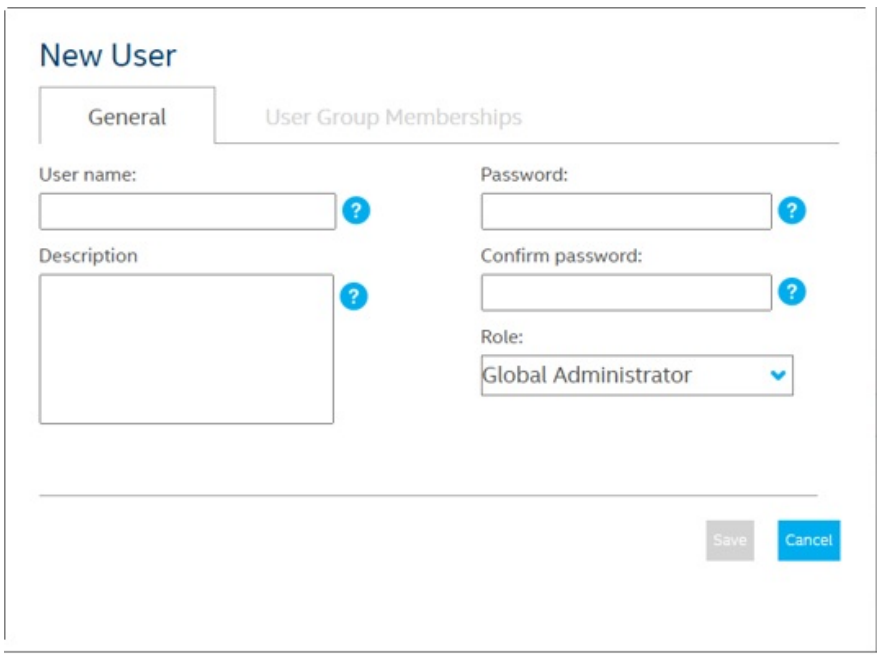


Create Users

4. To create additional users to the tenant (Global administrator, tenant collaborator, etc.) in the Quick Links section of the information view, select the option Add or Remove Users. The window is enabled Manage Tenants and Users where you can complete the respective information.



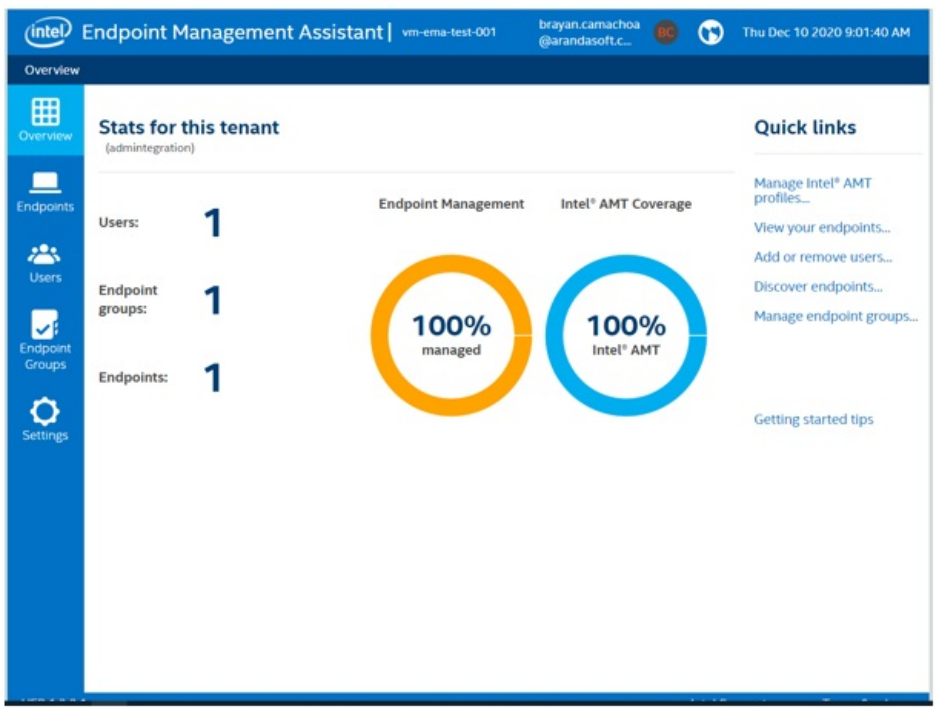
5. In the Users Select the New User and in the window that is enabled you can enter information such as username, description, password and role associated with the user.
6. When the setup is complete, click Save.



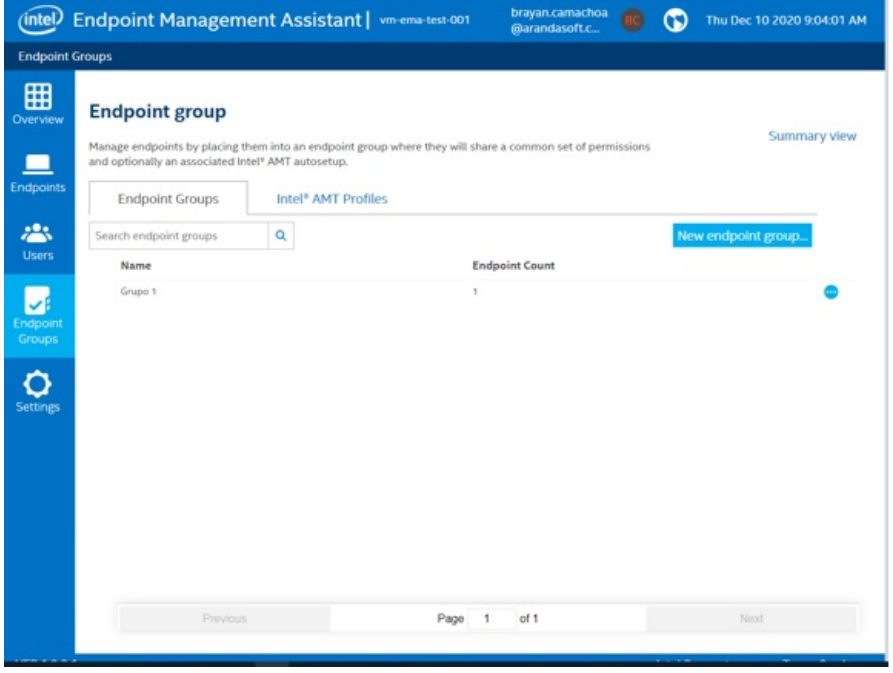
Generate Intel EMA Agent

Create Endpoint Group

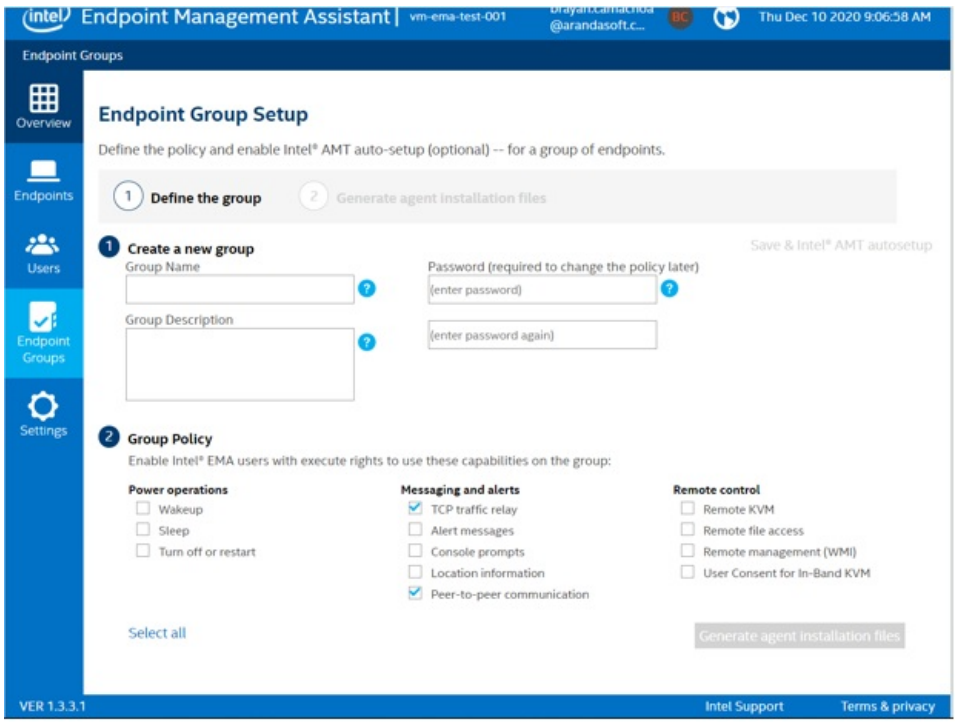
1. Log in to the Enpoint Management Assistant console as a Tenant Administrator and select the option Endpoint Group from the main menu.



2. In the information view of Endpoint Group Select the option New endpoint group.

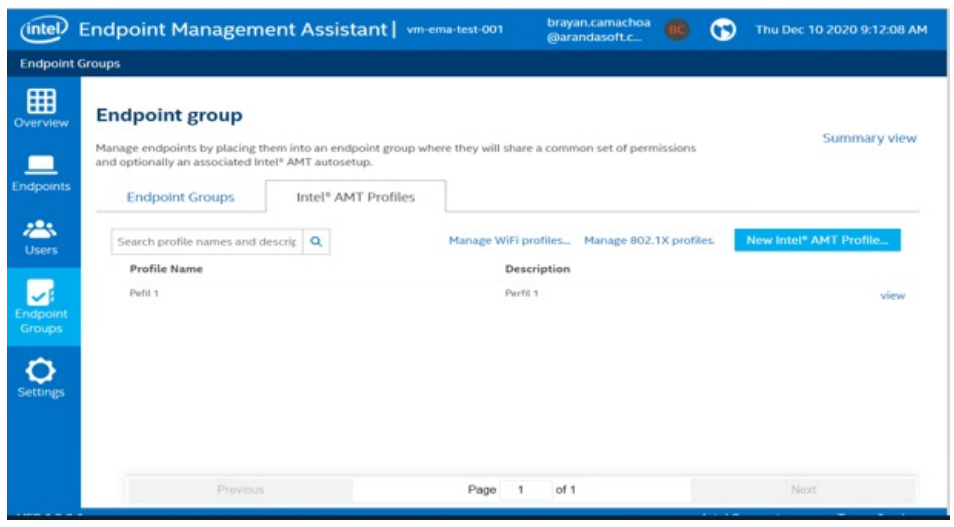


3. In the group settings enter name, description, password and policies according to the group's capabilities. When finished, click on the Generate agent Instalation files (Generate Agent Installation File)

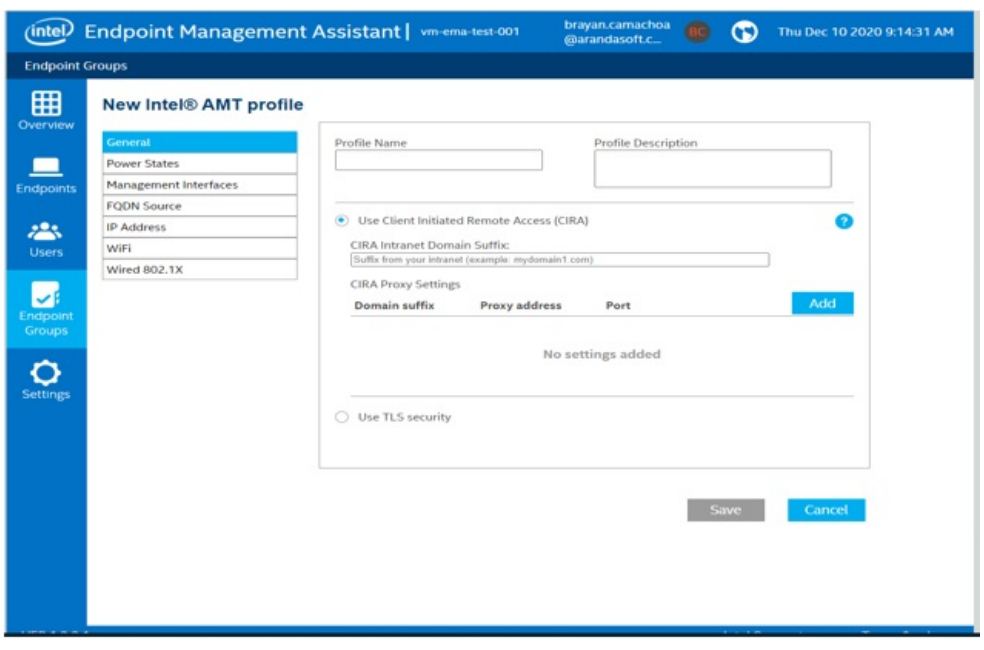


AMT Profile

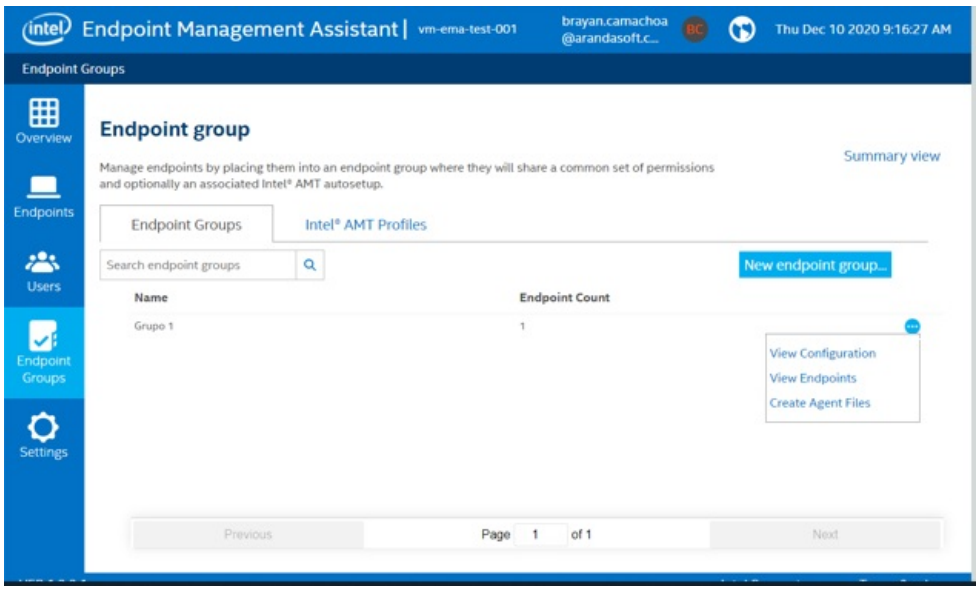
4. On the Endpoint Groups Select the option Generate an AMT profile.



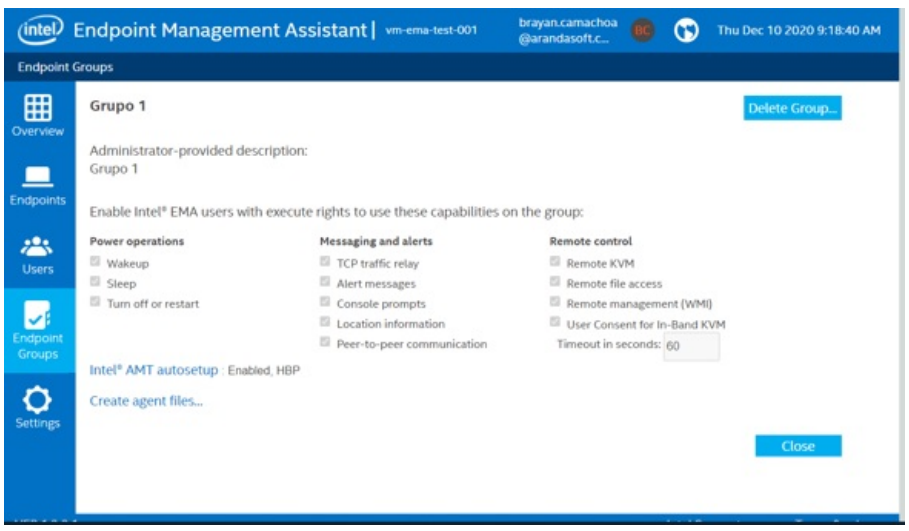
5. Configure the information related to the AMT profile.



6. Assign the AMT profile to the endpoint pool.

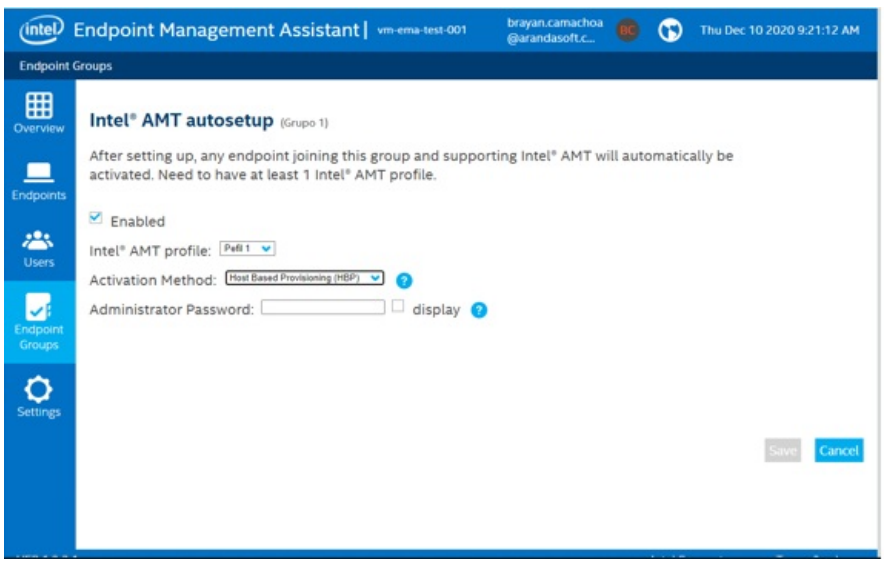


7. In the group, click the Intel AMT Autosetup.

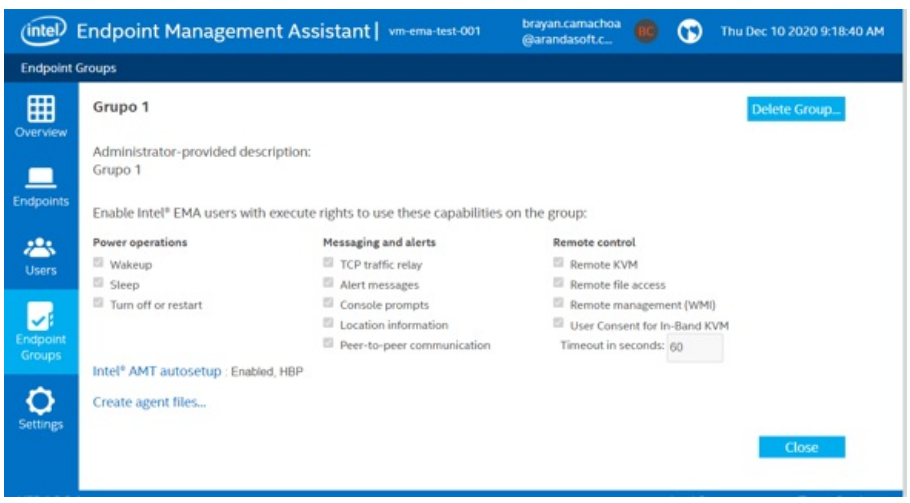


8. Select the AMT profile and activation method. Enter the BIOS password; As an IT administrator, make sure that all computers have the same password so that this profile works for them when they are installed.

⚐ Note: By default in computer equipment, the password is “admin”. It is recommended to review the doubling of the device model.

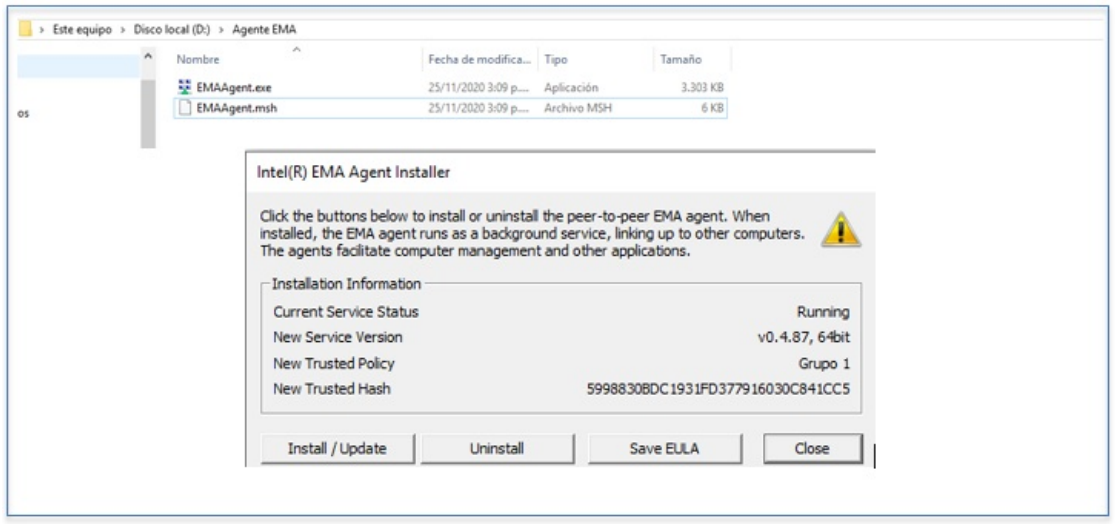


9. In the group, click the Create Agent Files (Create Agent file).



9. Select the agent version, download the agent service and policies.

⚐ Note: On the client machine, which is to be referenced by EMA, you must have the two files (executable and configuration) in the same path, with the same name and run EMAAgent.exe.



⚐ Note: The machines that support EMA are those that have firmware equal to or higher than version 11, generally supported by 7th Generation processors, some 6th Generation processors also support it.

- FW versions can only be upgraded in subversions of the version that come from the factory. That is to say that a 10 Generation processing cannot be upgraded from FW 14 to FW 15; What it can do is upgrade from 14.1 to 14.2, 14.3, etc.

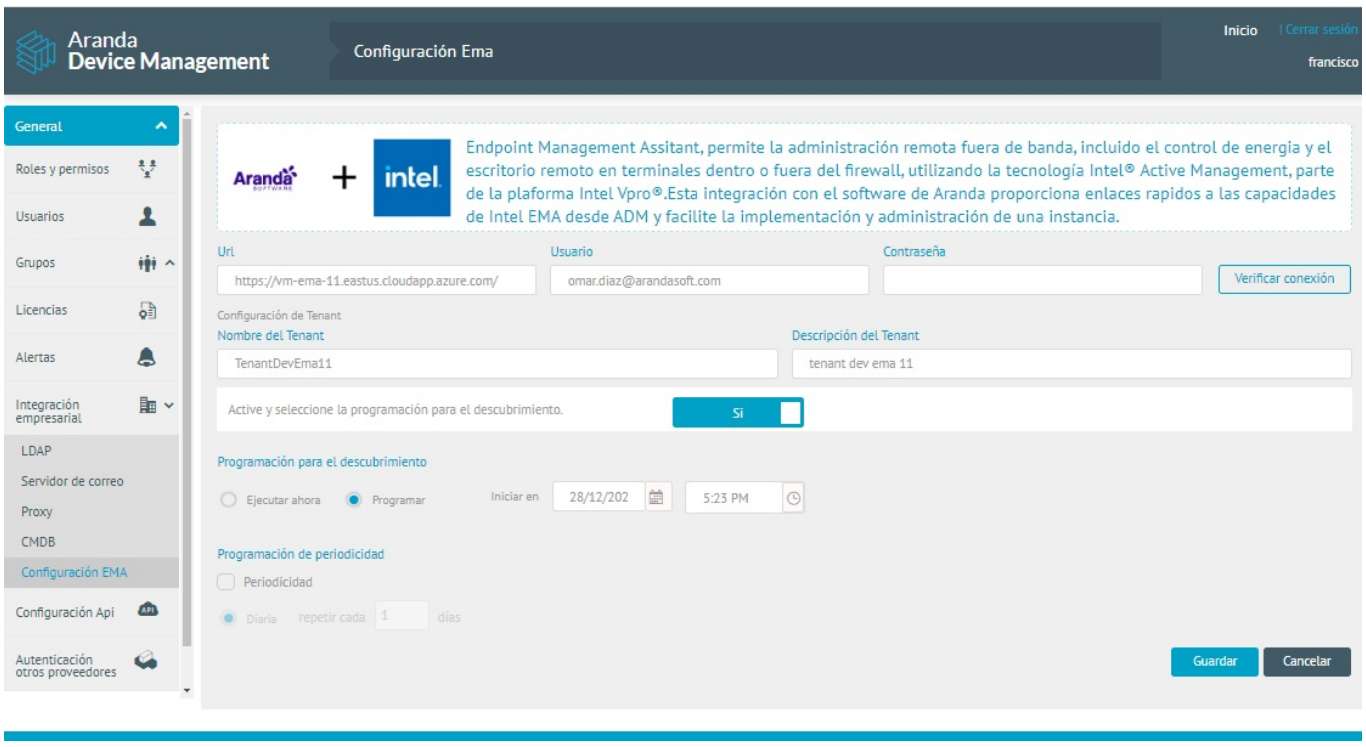
Intel® ME Firmwares Table

FW Version	Processor Gen	TLS	EMA Supported
15.xx.xx.xxx	11th Generation	1.2	X
14.xx.xx.xxx	10th Generation	1.2	X
13.xx.xx.xxx	9th Generation	1.2	X
12.xx.xx.xxx	8th Generation	1.2	X
11.xx.xx.3xx	7th Generation / 6th Generation	1.2 1.1	X
10.xx.xx.3xx	6th Generation	1.1	Partially
9.xx.xx.3xx	5th Generation	1.0	
8.xx.xx.3xx	4th Generation	1.0	

Enable ADM Integration - Intel EMA

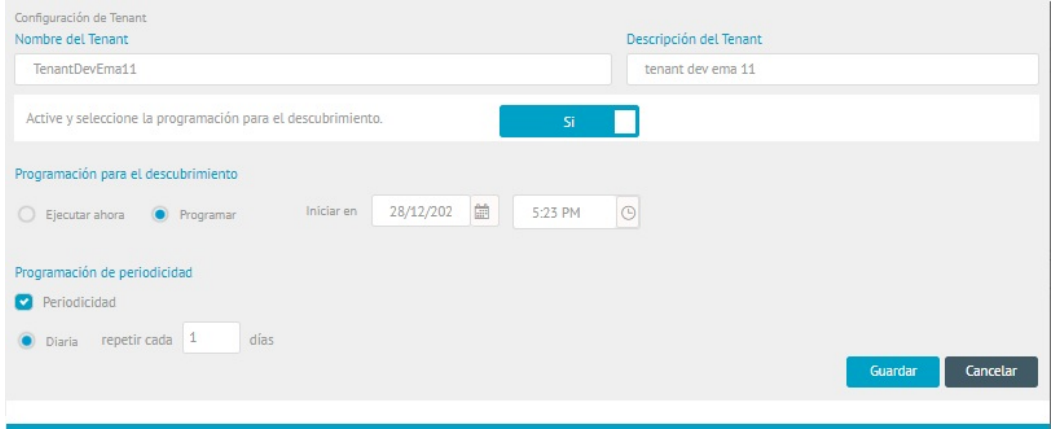
1. To configure the Active Directory, go to the Configuration view of the ADM Management Console, in the General Select the option Enterprise Integration and EMMA Configuration. In the information view, display the More Options and LDAP

2. In the information view, enter the basic information such as url, global admin user, and your password. Click Verfify Connection and if valid, the Tenant setting is enabled.



Tenant Configuration

3. In the Tenant Settings section, you will be able to enter the tenant name that you previously created during the EMA console scan and tenant description. Enable the option for scheduling for discovery by clicking YES



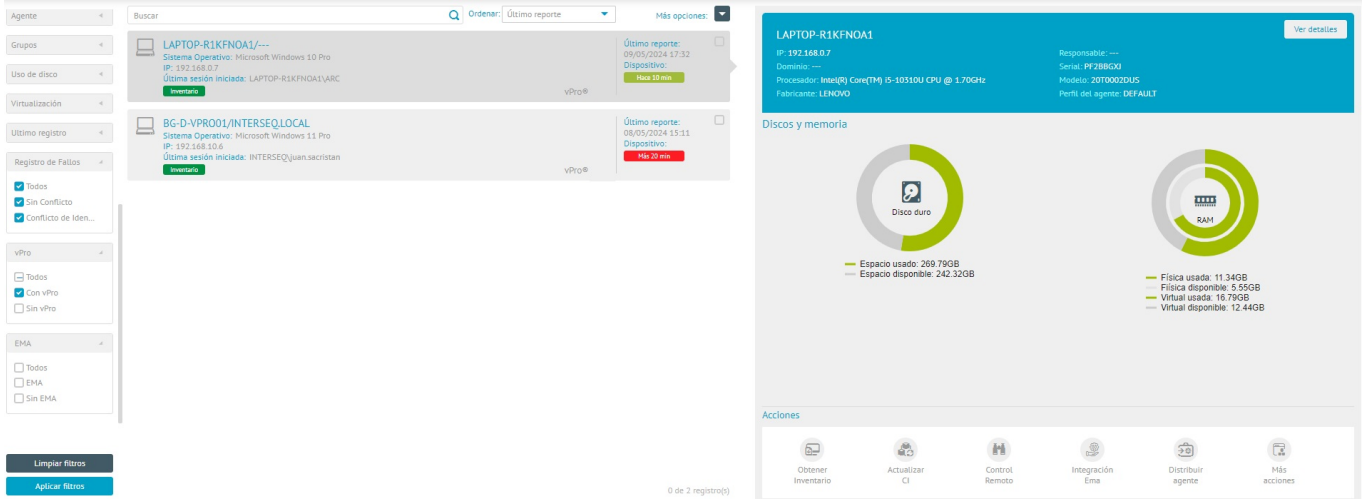
Programming for Discovery

4. You can run immediately or schedule a task that allows you to synchronize ADM devices with EMA endpoints. This task is responsible for matching the machines discovered by ADM and the machines that are registered with Intel EMA. (this allows there to be a navigation from the ADM consla to Intel EMA on a specific device)

5. By clicking Save, generates the server and the user with Global Administrator for the requests with the EMA API, then proceeds to create if the Tenant does not exist and finally generates the scheduled task for the synchronization of the devices.

Display Intel EMA-compatible devices

In the list of devices you can see the computers that have a Vpro processor, you can use the filters to list only the devices that have this type of processor.

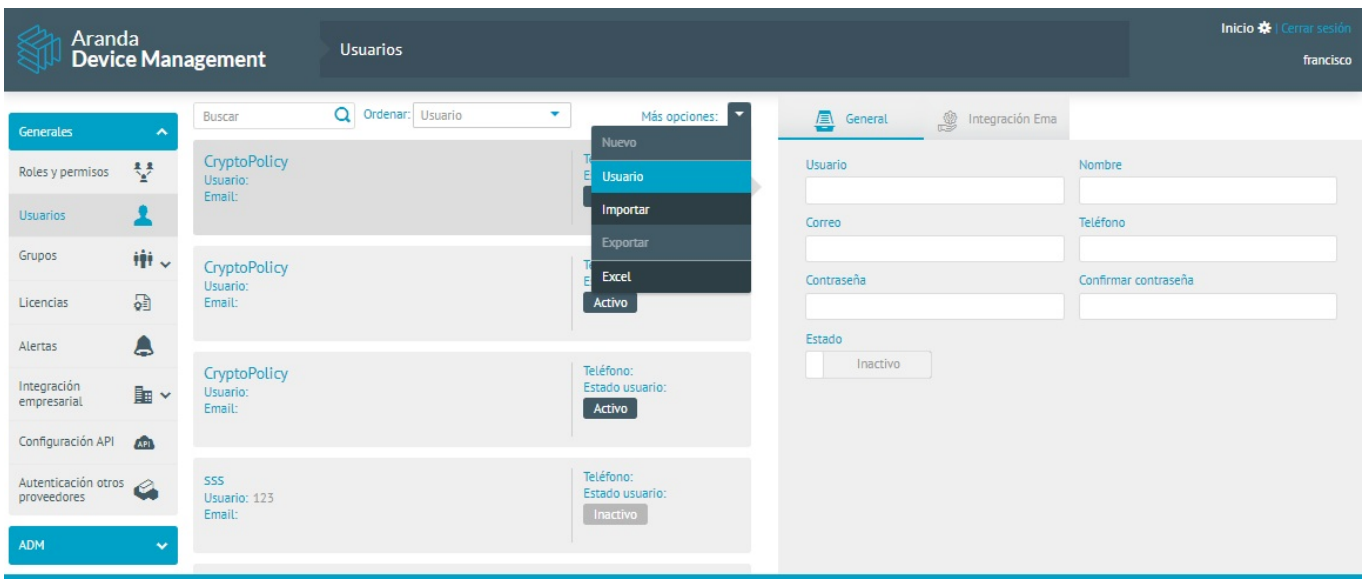


With these devices, you will be able to access all Intel Ema functionalities after installing the agent.

EMA Tenant Admin User Creation

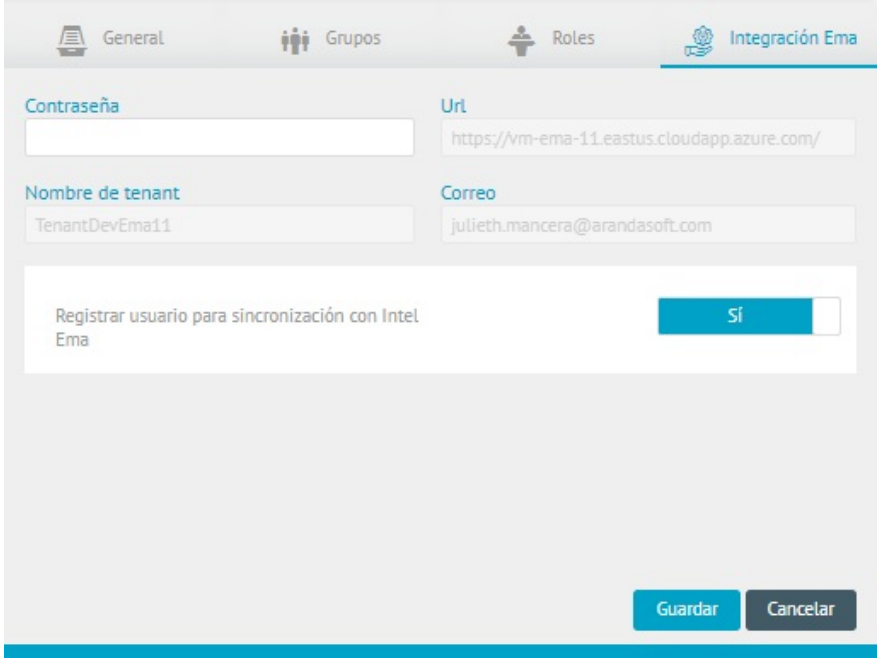
1. To create the Emma Tenant Admin user, go to the Settings view of the ADM Management Console in the General Select the option Enterprise Integration and LDAP. In the information view, display the More Options and User.

2. In the Users Detail View, select the General where you can fill in the general user data to be integrated with EMA as a Tenant administrator and define whether their status is active or inactive.



⚐ Note: The user must have a valid email configured to create the Tenant Admin user.

3. In the Users Detail View, select the Ema Integration and enter the user key and activate the EMA user; You can register the user as the user to be used to synchronize.



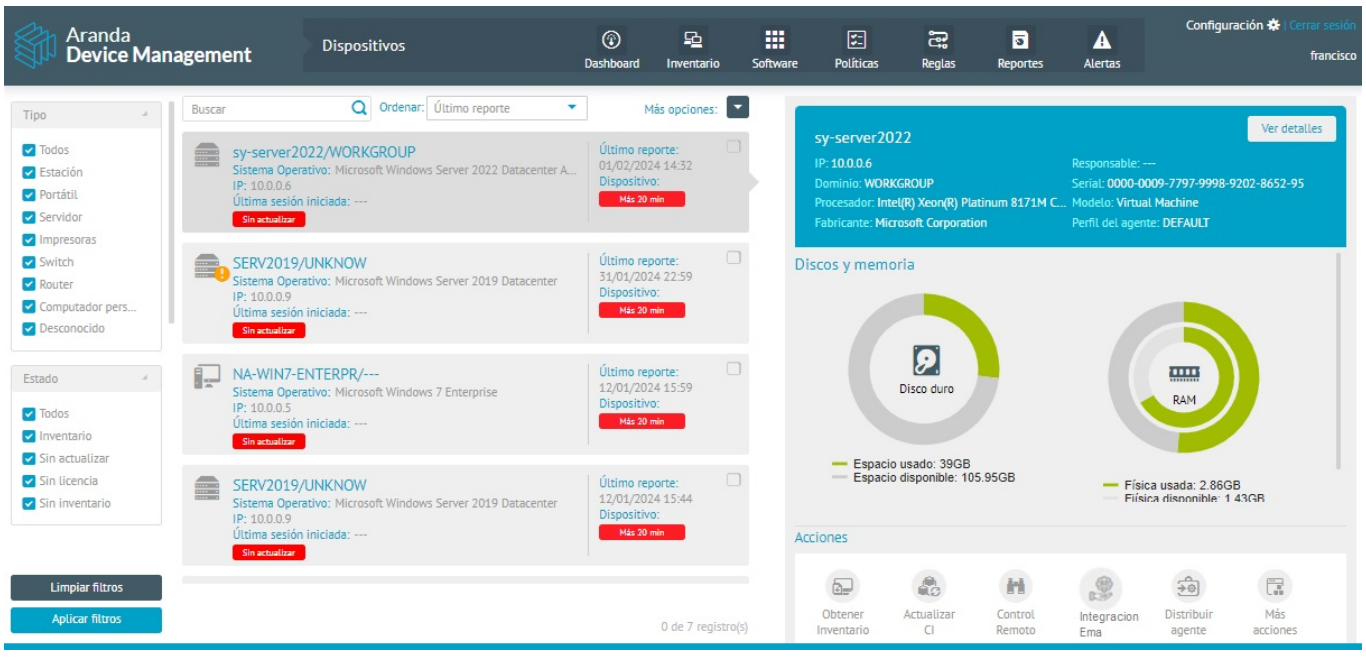
4. When you finish setting up the basic user information, click Save to confirm changes made; in the Detail View, the Groups and Roles tabs are enabled

Direct access with EMA

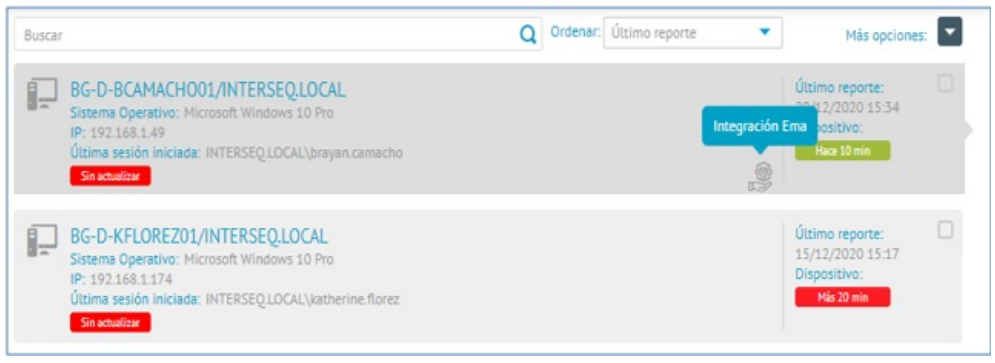
Once the entire configuration process has been completed and after the synchronization task between ADM and Intel EMA has been executed, the user will be able to navigate from the detail of an ADM device to the EMA console and perform the operations required.

Access from ADM

1. Enter the Home view of the ADM Management Console and select the module Inventory menu and the Devices. In the information view, the list of inventoried devices can be displayed.



⚐ Note: If the device is synchronized with EMA, you will be able to see the EMA logo.EMA Integration in the device list.

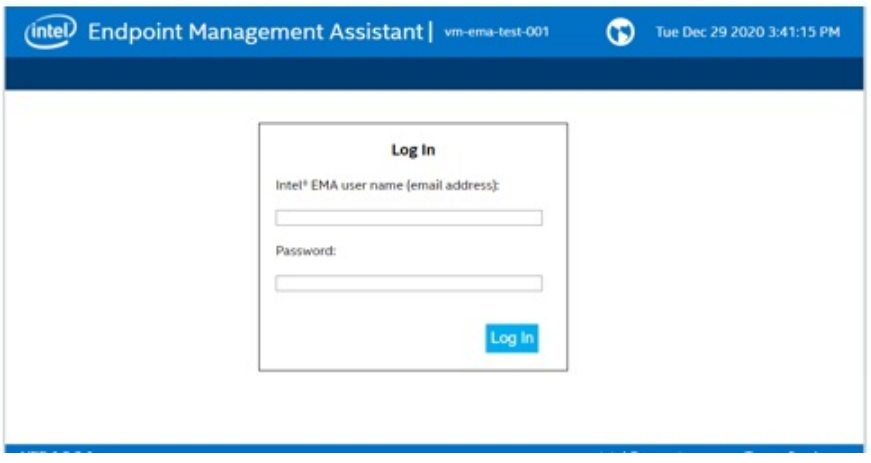


2. In the Built-in Device Detail view, select the Ema Integration

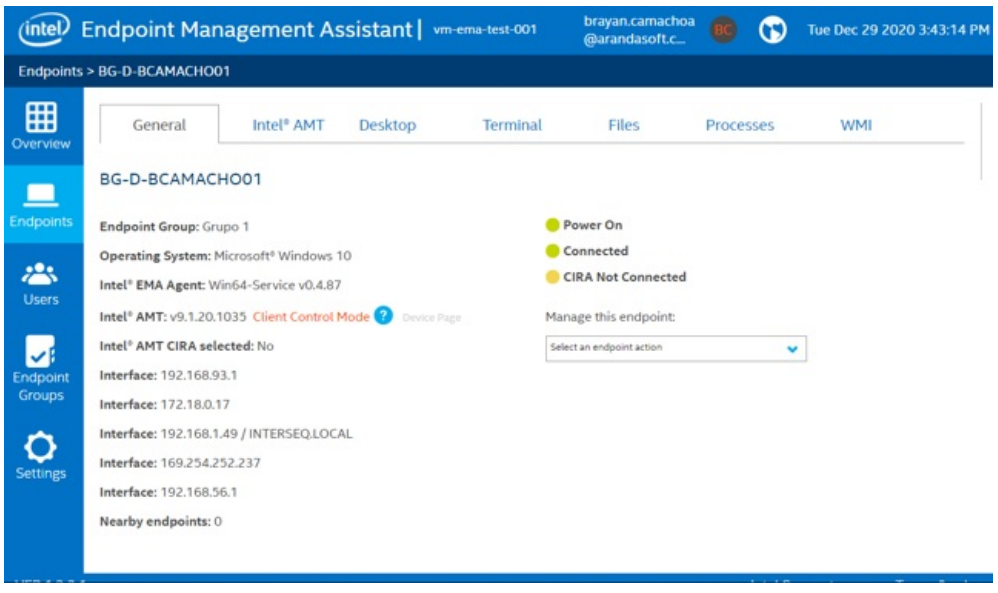
3. In the device detail view, the described action is enabled. Click Accept, to redirect the process to the console Enpoint Management Assistant

Access from Intel EMMA

4. If the user is already authenticated in the EMA console, they will be able to access the device directly, if they are not, the system asks them for credentials to log in as a tenant administrator user, created during the configuration process or in the Tenant Admin User Creation of EMA.



Once authenticated, the user will be able to view the Endpoint (device) to access the Endpoint (device) to execute management actions from Intel EMA.



ARC Remote Control

Remote Control (ARC)

It allows you to take control of machines in a simple and efficient way and transfer files conveniently, facilitating remote management of workstations.

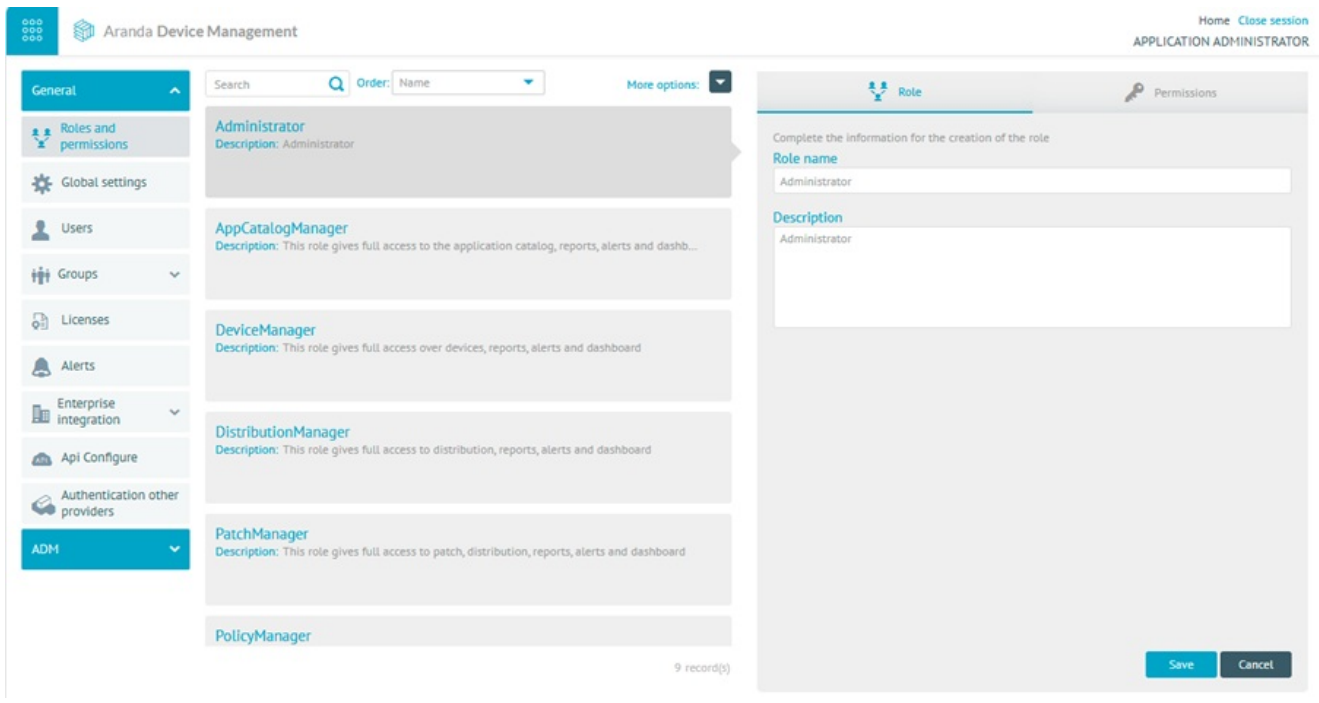
⚐ Note: Consider the following supported architecture for remote control:

- This functionality is not supported for agent versions released from ADM lower than 9.19.2 (Cloud)
- This functionality is not supported on OnPremises installations of ADM versions lower than 9.21.1

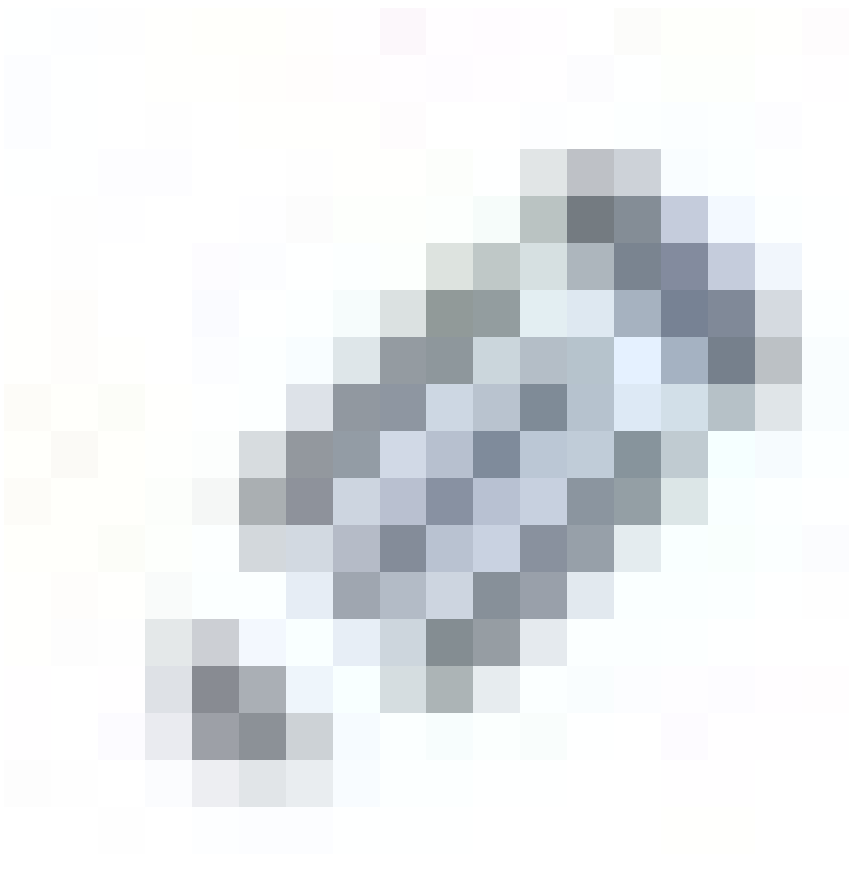
OnPremises Installation Configuration Process

You should consider the following steps for remote control setup in OnPremise installations:

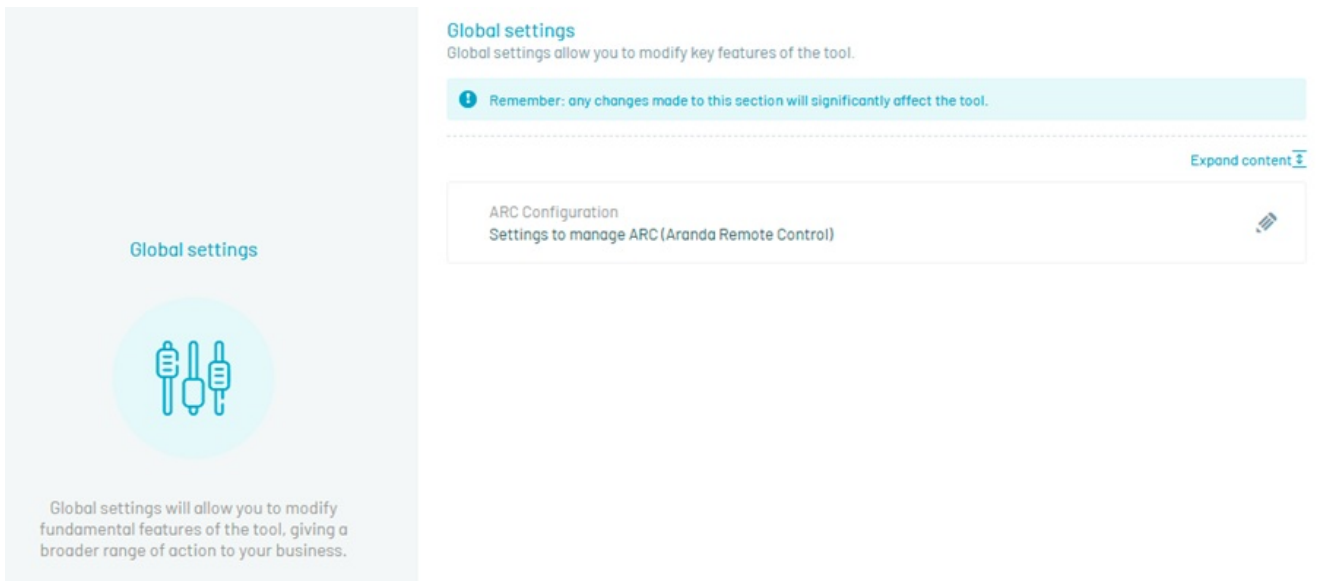
- Enable the functionality in the ADM console by going to Configuration > General > Global Settings.



- In the information view of Global Settings, select the ARC Configuration Click Edit

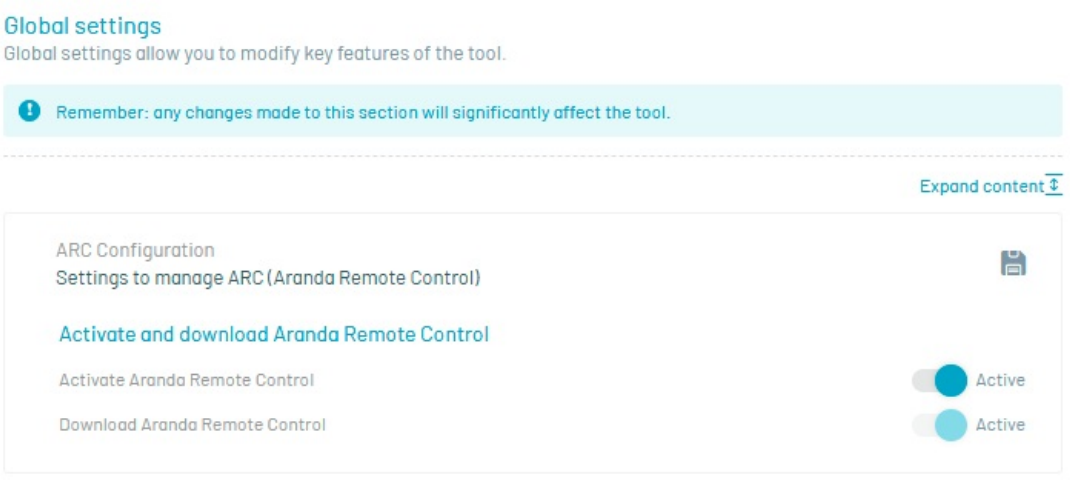


or on the Expand content.



⚐ Note: In deployments cloud, this field can only be displayed, but not edited. {: #important}

- Validate that Activate Aranda Remote Control Have the checkbox enabled (default). If it is not, enable it and click the Save.



- Perform the corresponding post-installation setup Aranda.ADM.Web.Installer on the application server. View Settings

Agent setup and installation process

Consider the following steps for the configuration and installation of the remote control agents:

- To perform remote control, it is required to have the remote control component installed on the devices to which the remote connection is to be made.Remote Control Component Installation
- Installation of the remote control viewer, required on the device from which the remote connection is made Remote control viewer installation

Aranda Remote Control Application Requirements

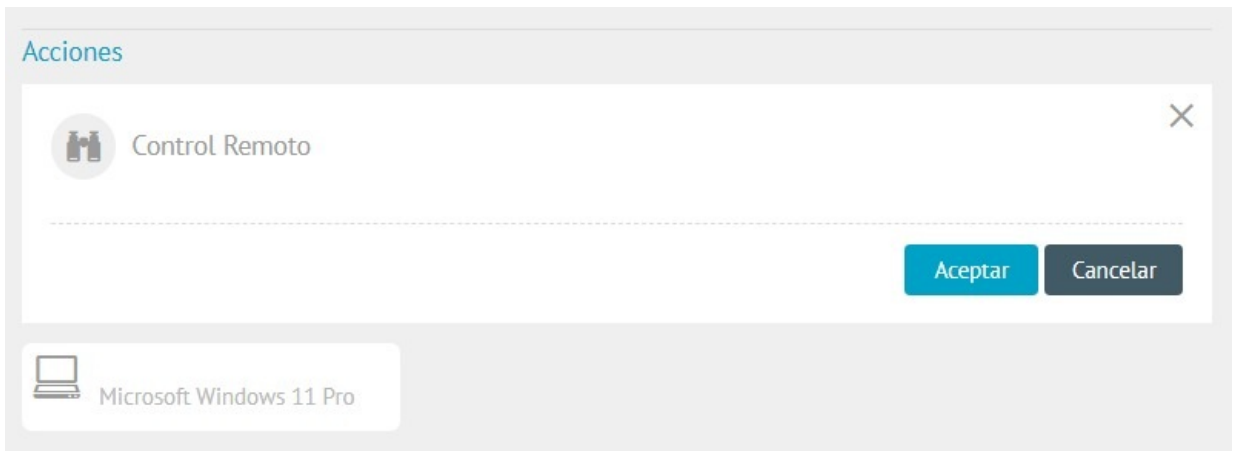
Take Remote Control

To perform remote control, the following must be previously configured:

- Remote control requires having the Remote Support permission active on the ADM user role.Roles and Permissions.
- The device must be associated with a device group. Groups
- It is required to create a relationship between the device group and the user or user group authorized to perform remote control.Relations

Once the above configuration is done:

- On the menu Inventory > Devices You need to select the available device, click on the Remote Control action and then on Accept.



- In the browser, the Support session, where you can view device information, open the remote control viewer, and transfer files between devices.

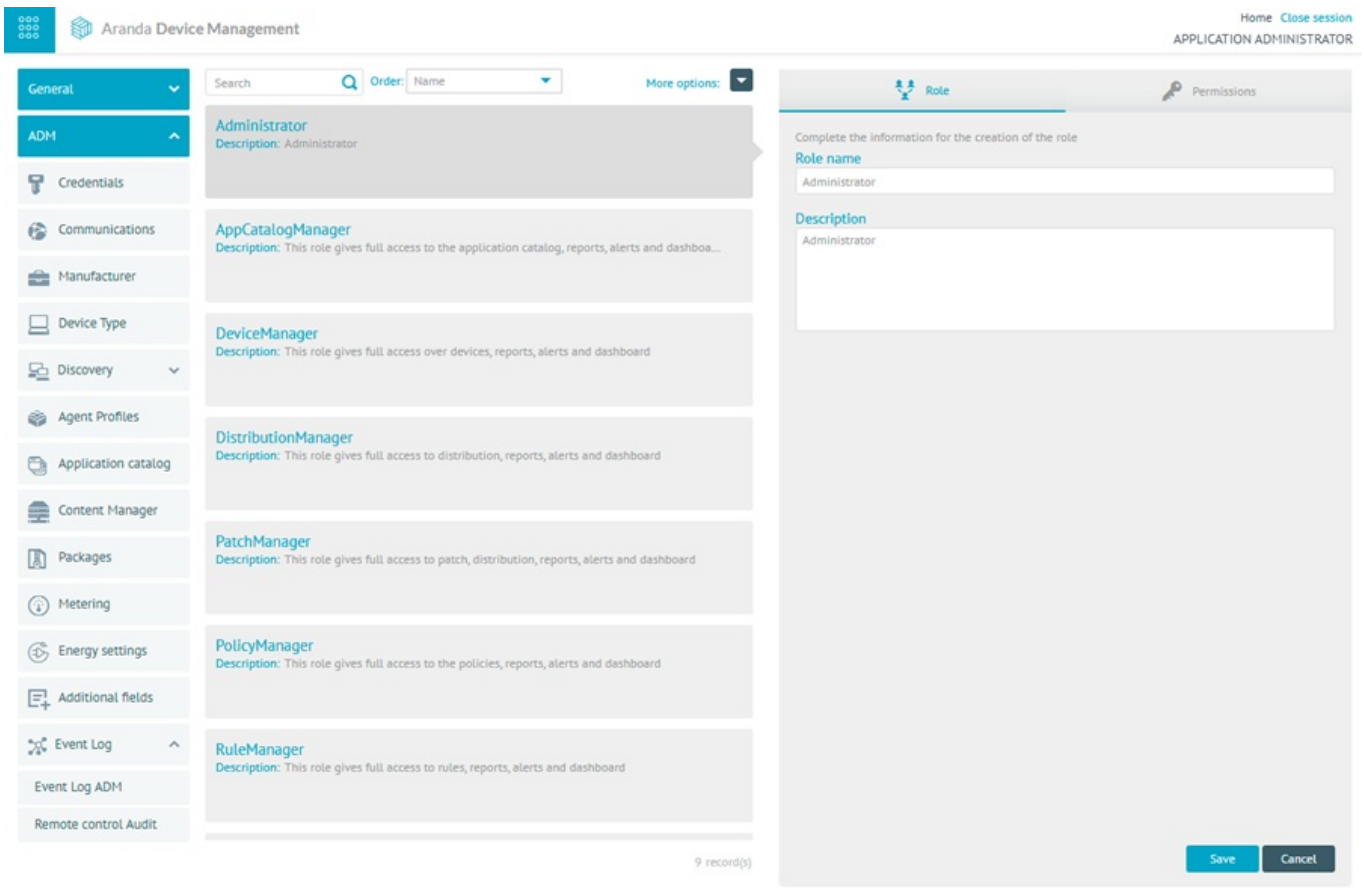
Take Remote Control

File Transfers

Remote Control Audit

This feature allows events logged upon entering the support session to be visible in the Event Log section. It is possible to search from the filter, add and/or hide columns. Events are logged when requesting, starting, or terminating remote control, when sending or receiving files.

To view these logs, you must go to the ADM console Configuration > ADM > Event Log > Remote Control Audit.



A screen is enabled where you can view all the events performed in the support session.

Remote Control Audit

Component Installation

Remote Control Component Installation

↩ ARC Integration

ADM Windows Agents from ADM version 9.19.2, after performing the zero installation or an upgrade from a previous version, will automatically install the new remote control component after 30 minutes. The following processes and services are displayed on the device.

> ⚐ Note: In the event of a connection failure at the time of installation or update of the remote control component, the ADM agent will perform installation retries every 4 hours.

Remote Control Component Processes and Services

Remote Control Component Upgrade

↩ ARC Integration

Remote control viewer installation

↩ ARC Integration

Remote control viewer installation

↩ ARC Integration

OnPremises Environments Configuration

ARC Remote Control Configuration

After installing the file Aranda.ADM.Web.Installer perform subsequent configurations on the application server and from the ADM console to ensure the correct operation of the new remote control, taking into account the following steps:

1. Configure connection chain

Set up the connection string for the recording site, on line 6 within the file appsettings.json of the site; The default path is:

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

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

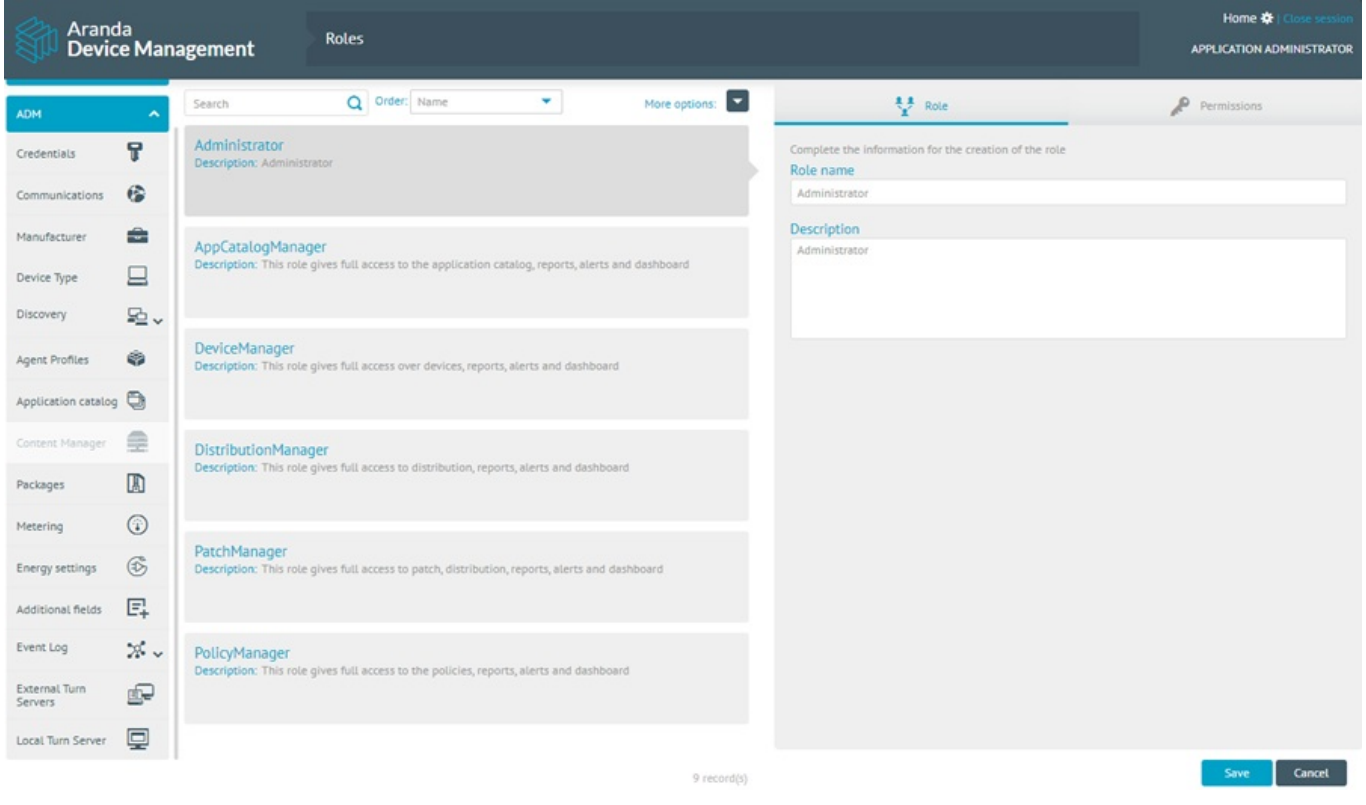
⚐ Notes:
- When making changes to the Recording Server connection string, restart the IIS so that the changes are applied correctly.

- If changes are made to the storage provider after configuration, move the information contained in the previous provider to the current one. If this action is not taken, agent updates will not be successful, and you will not be able to access recordings in audits.

2. Log in to the console

Log in to the ADM console with the user with the required permissions to manage the External Turn Servers and Local Turn Server options in the ADM Settings.

⚠ Important: External and Local Turn options are available on On-Premise installations only.



3. External Turn Servers

The file transfer functionality of the remote control 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:

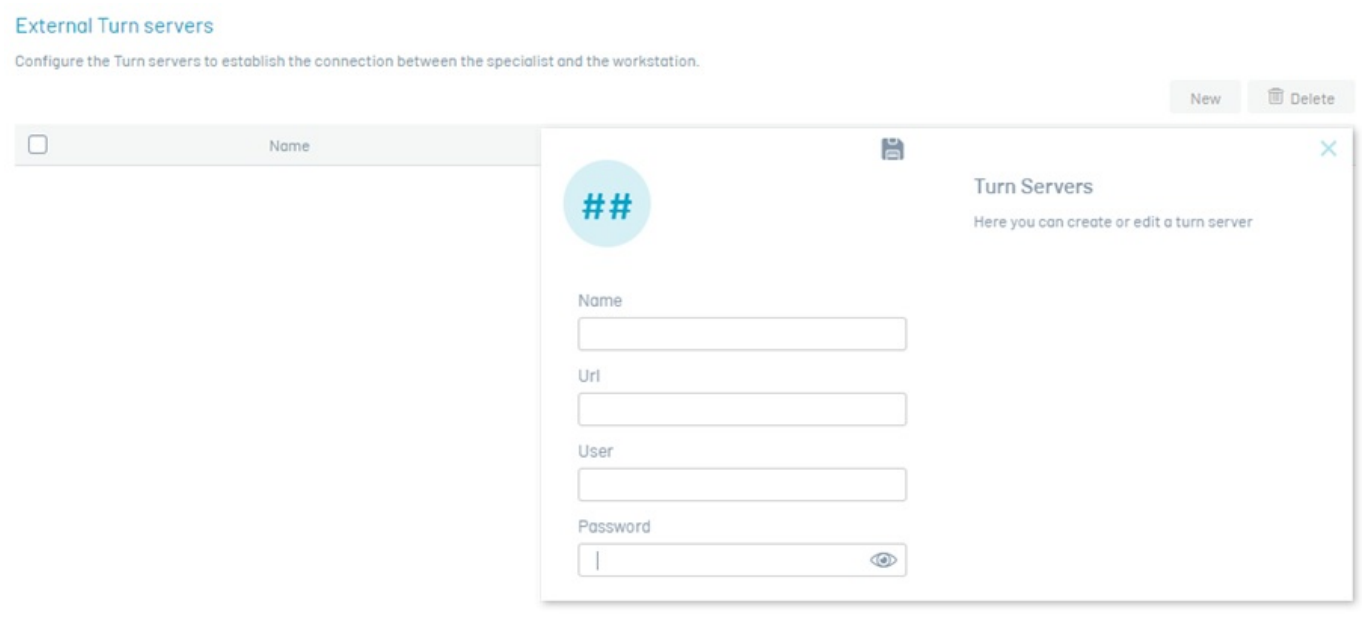
A. Click on the option New.

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.



The user can register the number of external Turn servers that he or she deems necessary to have good communication between the specialist's devices and the workstation through the ADM 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.

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.

4. Turn Local Server

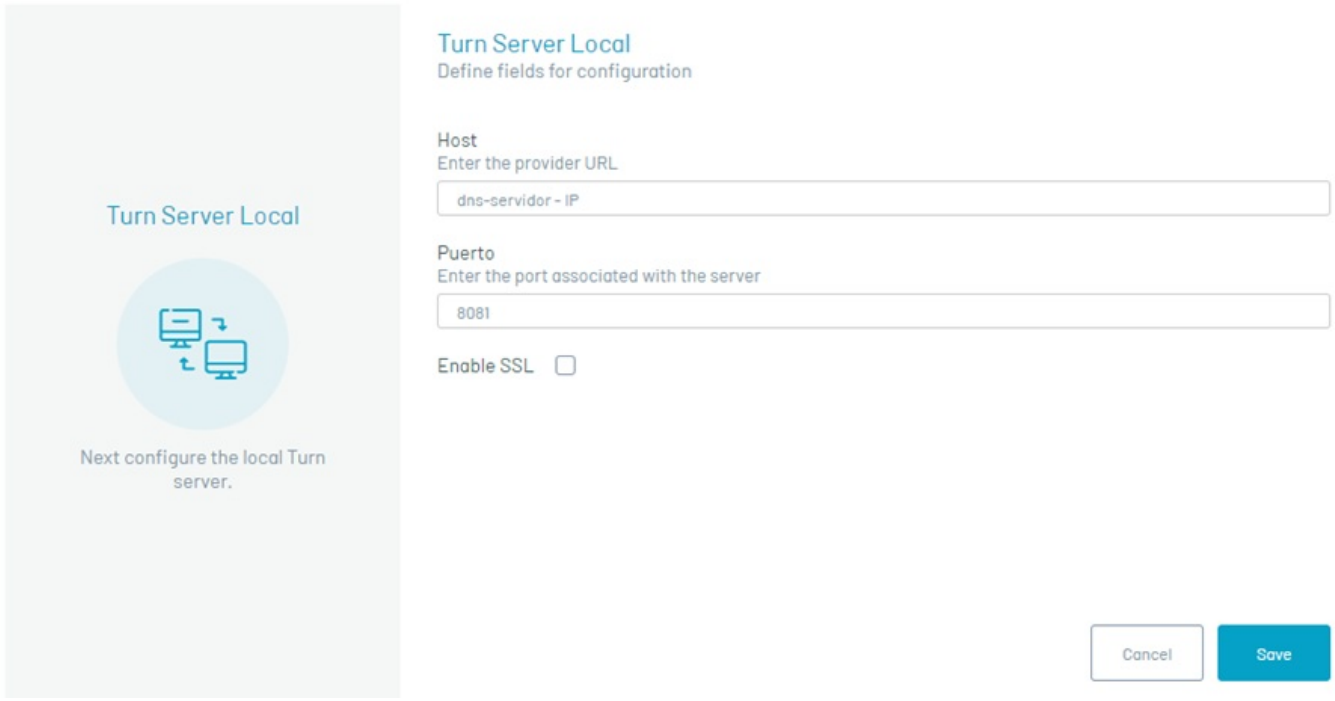
To establish remote takeover communication between the specialist agent and the workstation agent, use a local Turn server that can relay network traffic.

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 it is set by default to the value 8081 and SSL is inactive; if the port is changed or SSL is enabled [make the settings in the Aranda Turn Server service](#) installed on the server.

C. Finish by clicking the Save



Manual Service Configuration

Configuring the Turn Server

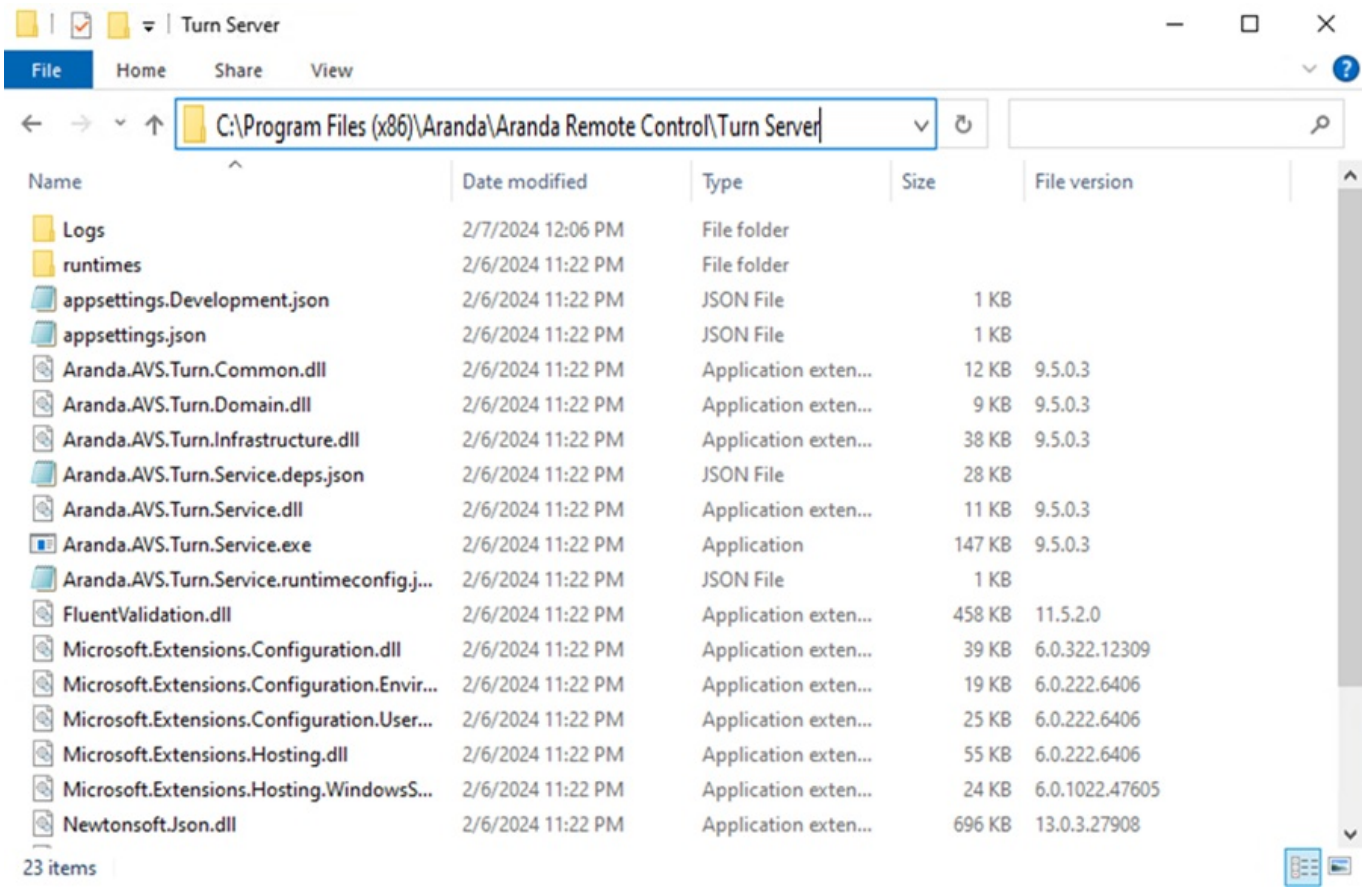
↩ Turn Local Server

After installing the Aranda 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).



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

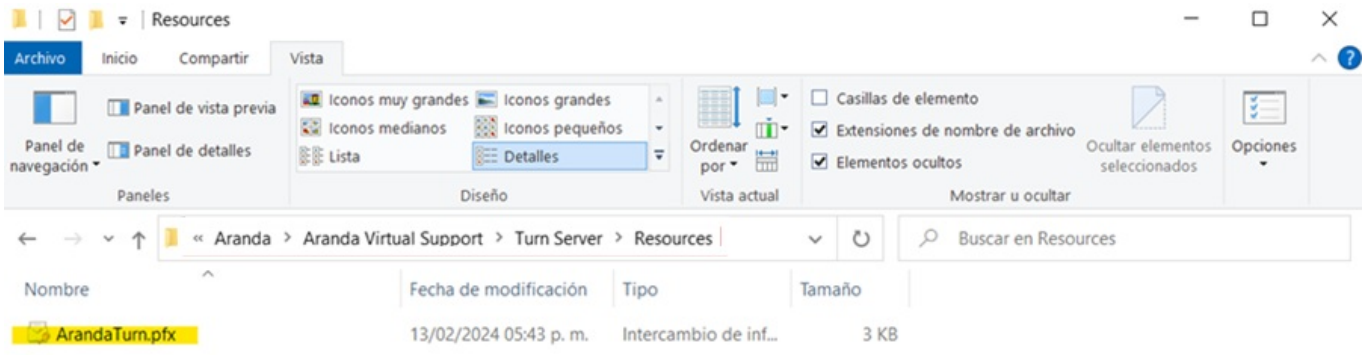
Edit the file appsettings.json and configure the desired port by replacing <puerto> by the desired port number.

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

3. SSL Secure Connection Configuration

Edit the appsettings.json file, 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.



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 file.

```
"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 appsettings.json archive.

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

4. Service Restart

Restart the Turn Server Windows Service 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-server.toml C:\turn-server.toml

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

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

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

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

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

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.

Workstations (ARC Agent) and specialist computers (Specialist Agent) 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	ARC 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 ARC 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 ARC 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 ARC 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 ARC 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 ARC 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 ARC Agent are unable to establish communication due to a connectivity problem between networks.

⚠ Note:

- To cover scenarios 1, 2, and 3, configure in the AMD 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 ADM 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