Aranda Device Management

La integración de aplicaciones es un proceso de comunicación que facilita el intercambio de información y servicios permitiendo potenciar la gestión de activos y complementar la funcionalidad con recursos.

Aranda DEVICE MANAGEMENT facilita las siguientes soluciones de integración:

1.Integraciones Externas

Actualmente ADM se integra con las siguientes aplicaciones externas:

- La integración con **Intel® Endpoint Management Assistant (Intel® EMA)** permite la administración remota de computadores cuando los equipos están apagados o el sistema operativo no responde. Usando Intel® EMA, es posible utilizar opciones de control de energía y escritorio remoto, en computadores dentro o fuera del firewall, utilizando la tecnología Intel® Active Management (Intel® AMT), parte de la plataforma Intel® vPro™.

2. Integraciones Internas

ADM se integra nativamente con nuestras soluciones:

- Con **Aranda Remote Control ARC**, para tomar el control de las máquinas de manera sencilla y eficiente y transferir archivos de manera conveniente, facilitando la gestión a distancia de las estaciones de trabajo.
- Con **Aranda CMDB**, para mantener actualizados automáticamente los items de configuración de la CMDB con el descubrimiento o los cambios detectados en los inventarios de los dispositivos.
- Con **Aranda QUERY MANAGER AQM** como un sistema de reportería avanzada, permite la visibilidad de la infraestructura a través de indicadores en tiempo real y acceso a reoprtes personalizados.

¿Para Quién es este Manual?

Esta manual está diseñado para compartir y profundizar las integraciones posibles entre Aranda DEVICE MANAGEMENT ADM y diferentes aplicaciones.

¿Cuál es Nuestra Documentación?

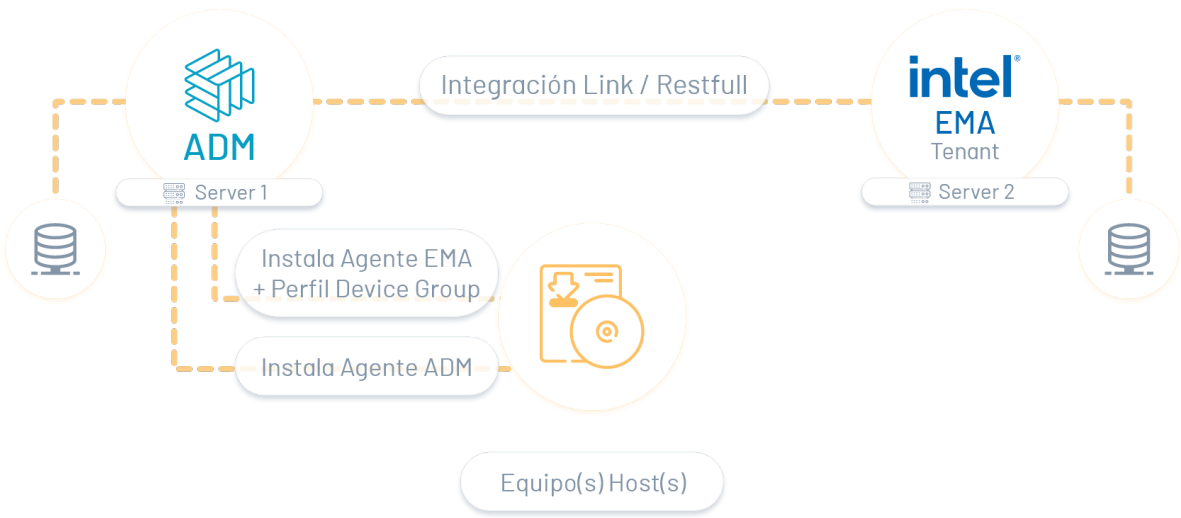
- Guia de Inicio Aranda Device Management ADM ↪
- Guía de Instalación Aranda Device Management ADM ↪
- Manual de Gestión Aranda Device Management ↪
- Manual de Integración ADM (Usted está AQUÍ)

Integración ADM intel Ema

Integración ADM Intel EMA

La nueva integración entre Aranda Device Management (ADM) e Intel® Endpoint Management Assistant (Intel® EMA), version 1.14 permite la administración remota de computadores cuando los equipos están apagados o el sistema operativo no responde.

Esta es una sincronización silenciosa, donde ADM procesa y verifica la información registrada por Intel® EMA, permitiendo así capacidades funcionales desde ADM con Intel® EMA para su gestión y administración.



En la integración se realizan diferentes actividades en paralelo a tener en cuenta y Se utilzan diferentes componentes que permiten el correcto funcionamiento de las aplicaciones a nivel interno y externo.

1. Actividades desde Intel EMMA

Para tener una integración se deben tener en cuenta las siguientes tareas a realizar desde Intel EMMA son:

Actividades Intel EMMA	Descripción
Instalación y Creacion Usuario	Para la integración externa con Intel EMA se requiere: - instalación del servidor EMA y la creación del usuario administrador del tenant.
Generación Agente Intel EMMA	Configure y despliegue el agente que requiere Intel® EMA con su respectivo perfil de configuración de grupo de tenant (perfil que tiene los parámetros de configuración de Intel® AMT).

2. Actividades desde ADM

Para tener una integración se deben tener en cuenta las siguientes tareas a realizar desde ADM son:

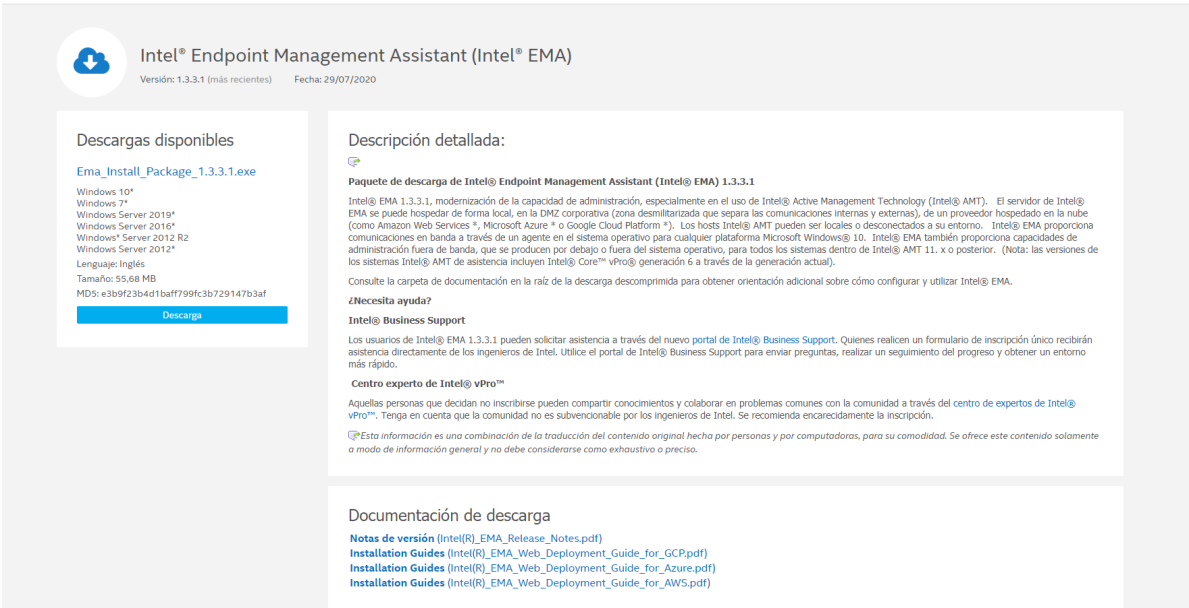
Actividades ADM	Descripción
Configuración Integración y acceso ADM	Desde la consola de administración ADM podrá: - Habilitar la integración Intel_EMMA. - Crear el usuario administrador de Tenant. - Acceder al detalle del dispositivo dentro del proceso de gestión de inventarios de ADM.
Configuración API	Desde la consola de administración ADM se realiza la Configuración del API que permite desarrollar e integrar el software de ADM con otras aplicaciones de software.

Instalación de servidor de EMA

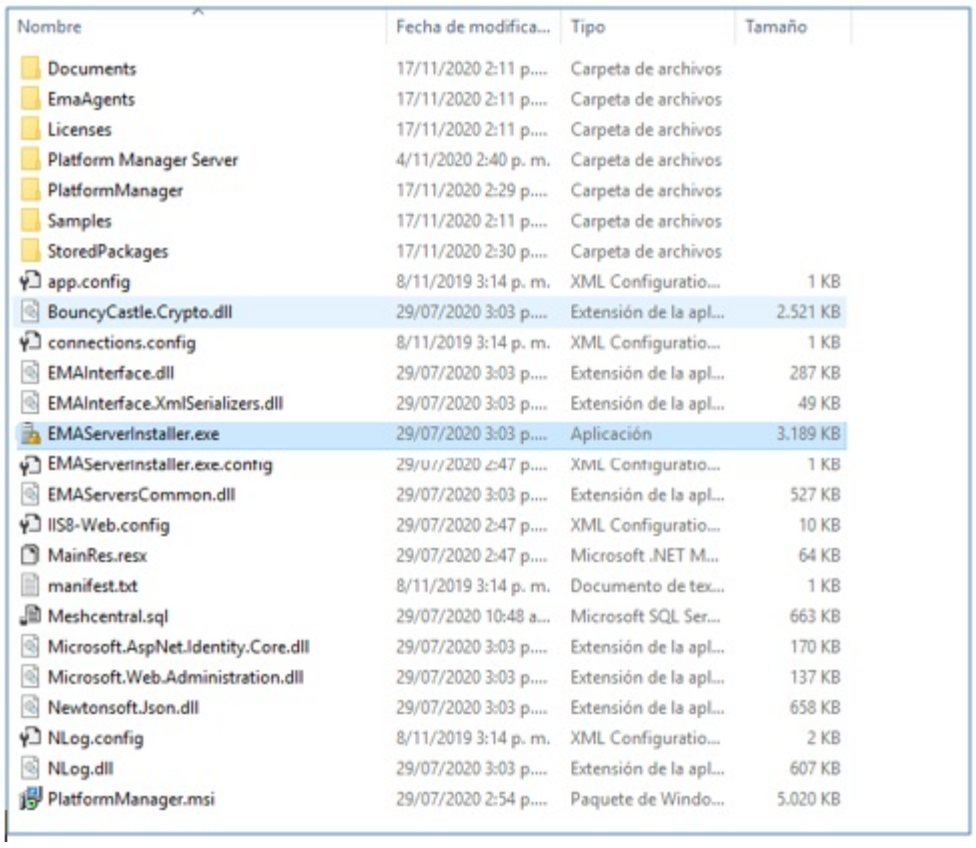
A continuación se describe la instalación básica de Intel EMA para llevar acabo la integración con ADM.

> ⚐ **Nota:** Para conocer todos los aspectos de configuración, consideraciones e instalación consulte la documentación oficial de Intel EMA

1. Descargue los paquetes de instalación de Ema en la siguiente ruta: Intel-Endpoint-Management-Assistant-Intel-EMA

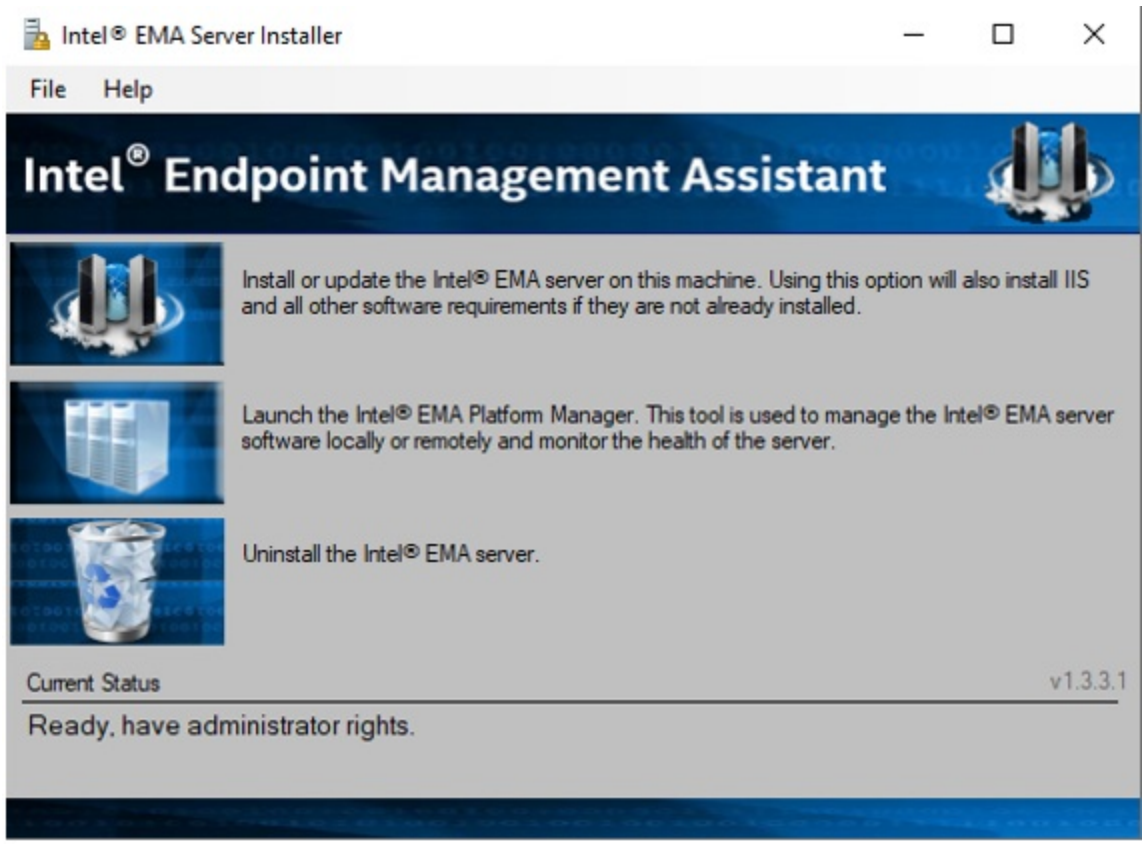


2. Ejecute el archivo **EMAServerInstaller.exe**.

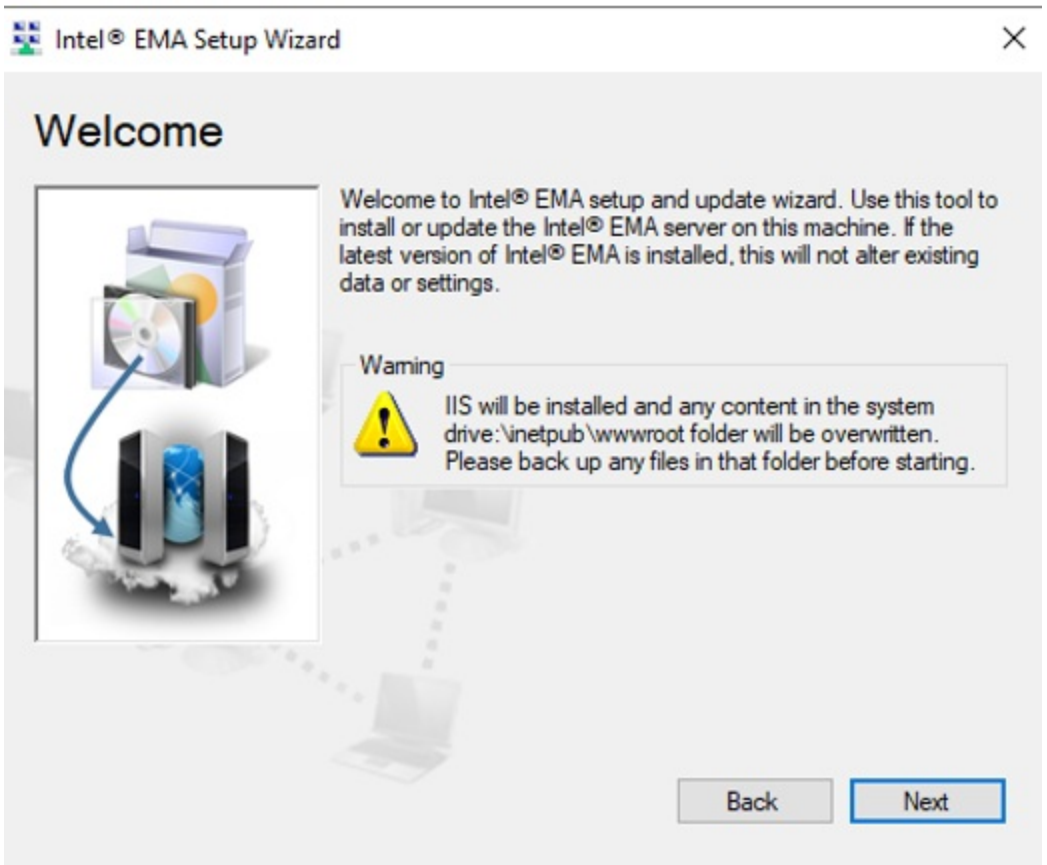


Nombre	Fecha de modifica...	Tipo	Tamaño
Documents	17/11/2020 2:11 p....	Carpeta de archivos	
EmaAgents	17/11/2020 2:11 p....	Carpeta de archivos	
Licenses	17/11/2020 2:11 p....	Carpeta de archivos	
Platform Manager Server	4/11/2020 2:40 p. m.	Carpeta de archivos	
PlatformManager	17/11/2020 2:29 p....	Carpeta de archivos	
Samples	17/11/2020 2:11 p....	Carpeta de archivos	
StoredPackages	17/11/2020 2:30 p....	Carpeta de archivos	
app.config	8/11/2019 3:14 p. m.	XML Configuratio...	1 KB
BouncyCastle.Crypto.dll	29/07/2020 3:03 p....	Extensión de la apl...	2.521 KB
connections.config	8/11/2019 3:14 p. m.	XML Configuratio...	1 KB
EMAInterface.dll	29/07/2020 3:03 p....	Extensión de la apl...	287 KB
EMAInterface.XmlSerializers.dll	29/07/2020 3:03 p....	Extensión de la apl...	49 KB
EMAServerInstaller.exe	29/07/2020 3:03 p....	Aplicación	3.189 KB
EMAServerInstaller.exe.config	29/07/2020 2:47 p....	XML Configuratio...	1 KB
EMAServersCommon.dll	29/07/2020 3:03 p....	Extensión de la apl...	527 KB
IIS8-Web.config	29/07/2020 2:47 p....	XML Configuratio...	10 KB
MainRes.resx	29/07/2020 2:47 p....	Microsoft .NET M...	64 KB
manifest.txt	8/11/2019 3:14 p. m.	Documento de tex...	1 KB
Meshcentral.sql	29/07/2020 10:48 a...	Microsoft SQL Ser...	663 KB
Microsoft.AspNet.Identity.Core.dll	29/07/2020 3:03 p....	Extensión de la apl...	170 KB
Microsoft.Web.Administration.dll	29/07/2020 3:03 p....	Extensión de la apl...	137 KB
Newtonsoft.Json.dll	29/07/2020 3:03 p....	Extensión de la apl...	658 KB
NLog.config	8/11/2019 3:14 p. m.	XML Configuratio...	2 KB
NLog.dll	29/07/2020 3:03 p....	Extensión de la apl...	607 KB
PlatformManager.msi	29/07/2020 2:54 p....	Paquete de Windo...	5.020 KB

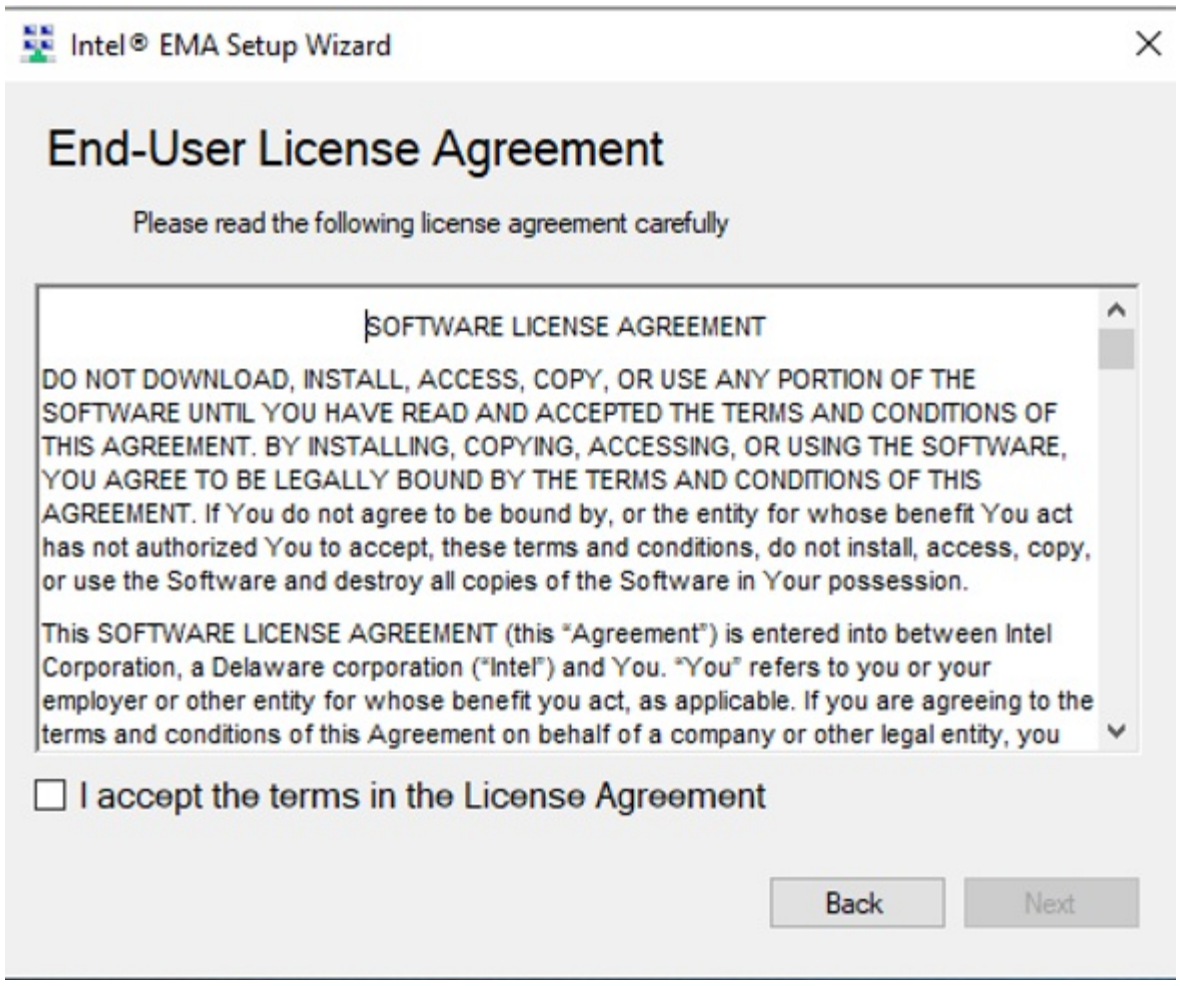
3. Instale el servidor de Ema y seleccione la opción 1.



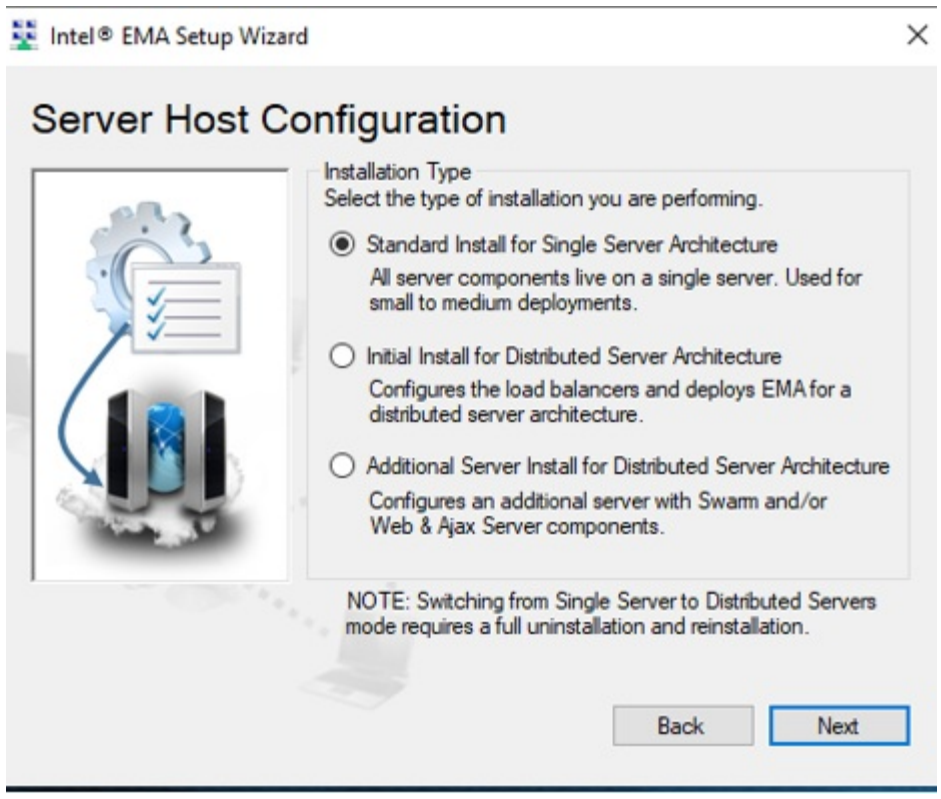
4. Debe cumplir la recomendación de tener el IIS configurado para el sistema operativo Windows.



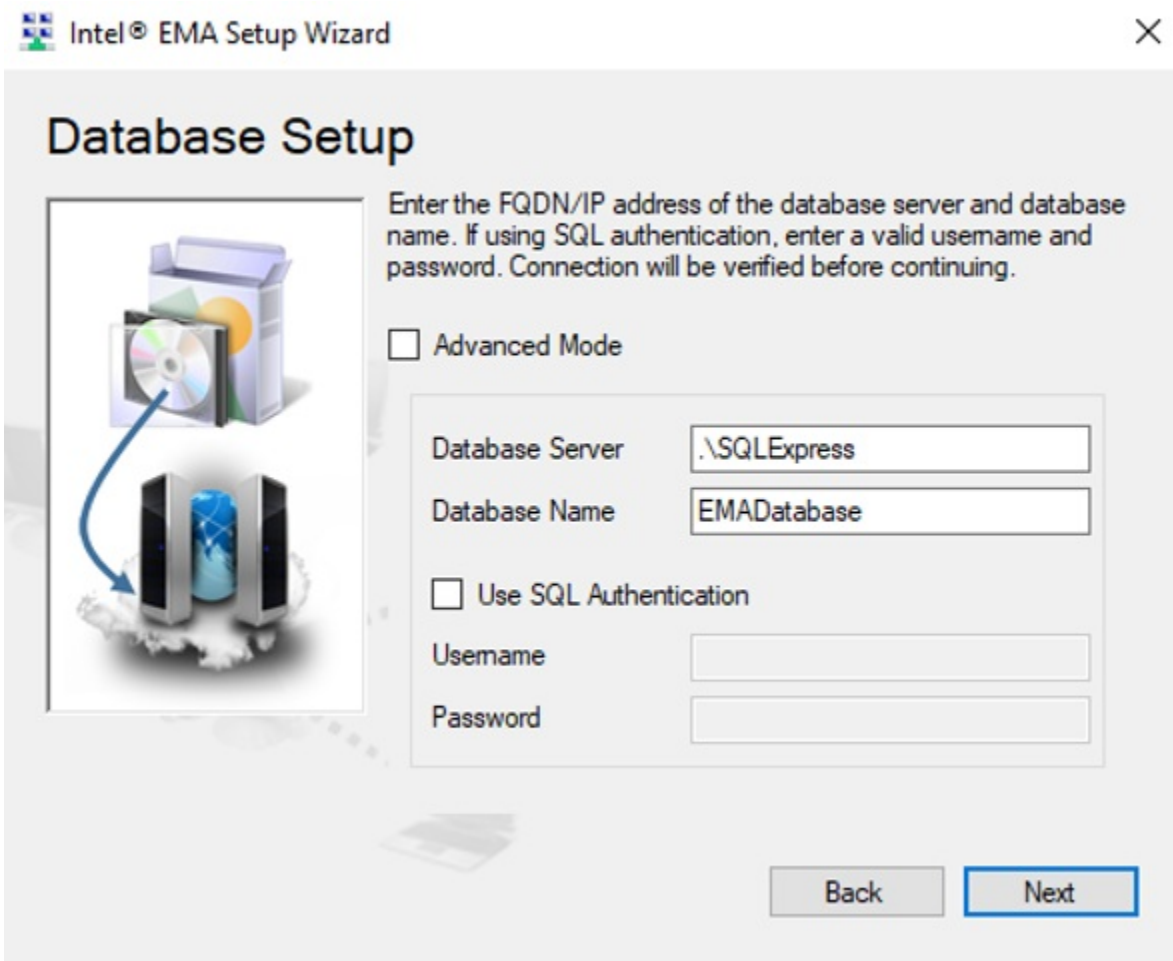
5. Lea el acuerdo de instalación y hacer clic en **Siguiente**.



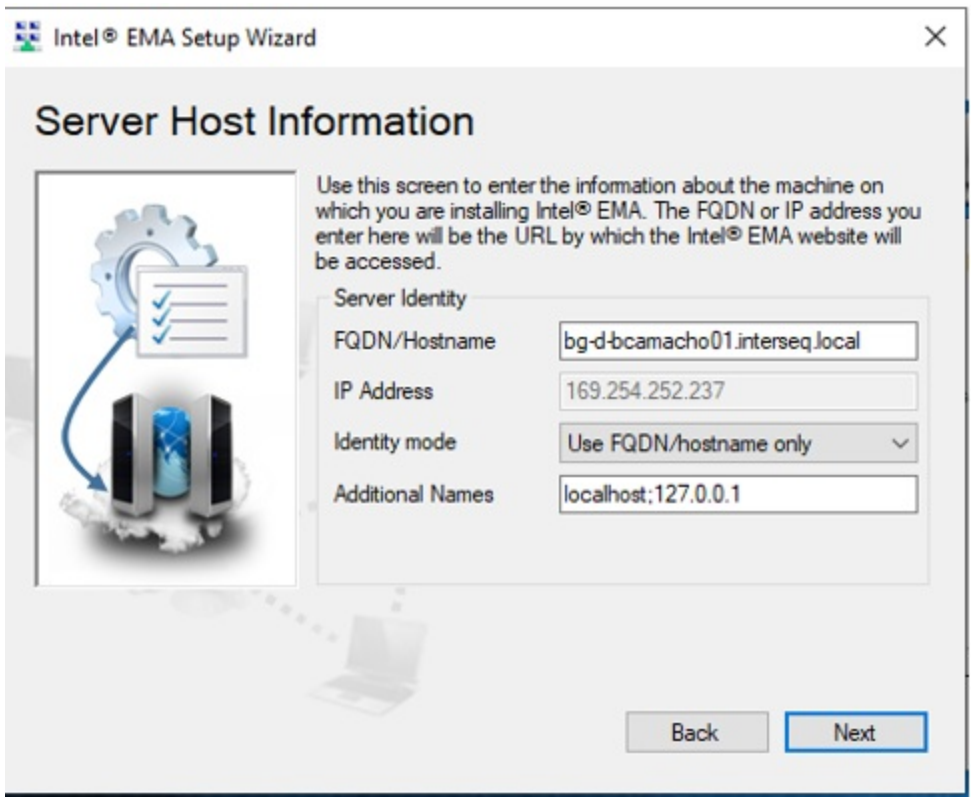
6. Seleccione el tipo de instalación:



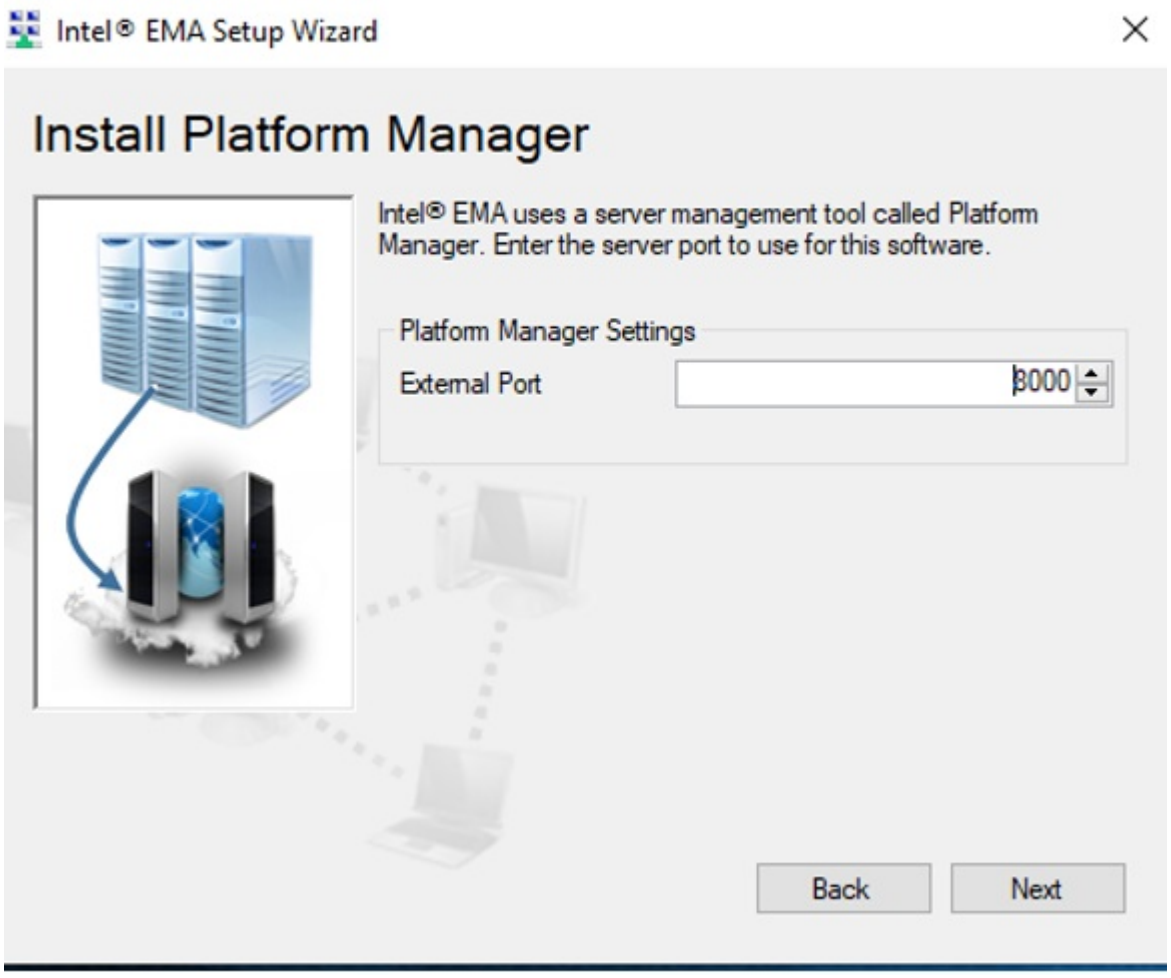
7. Seleccione la instancia de base de datos Sql Server.



8. Configure la información del Host.



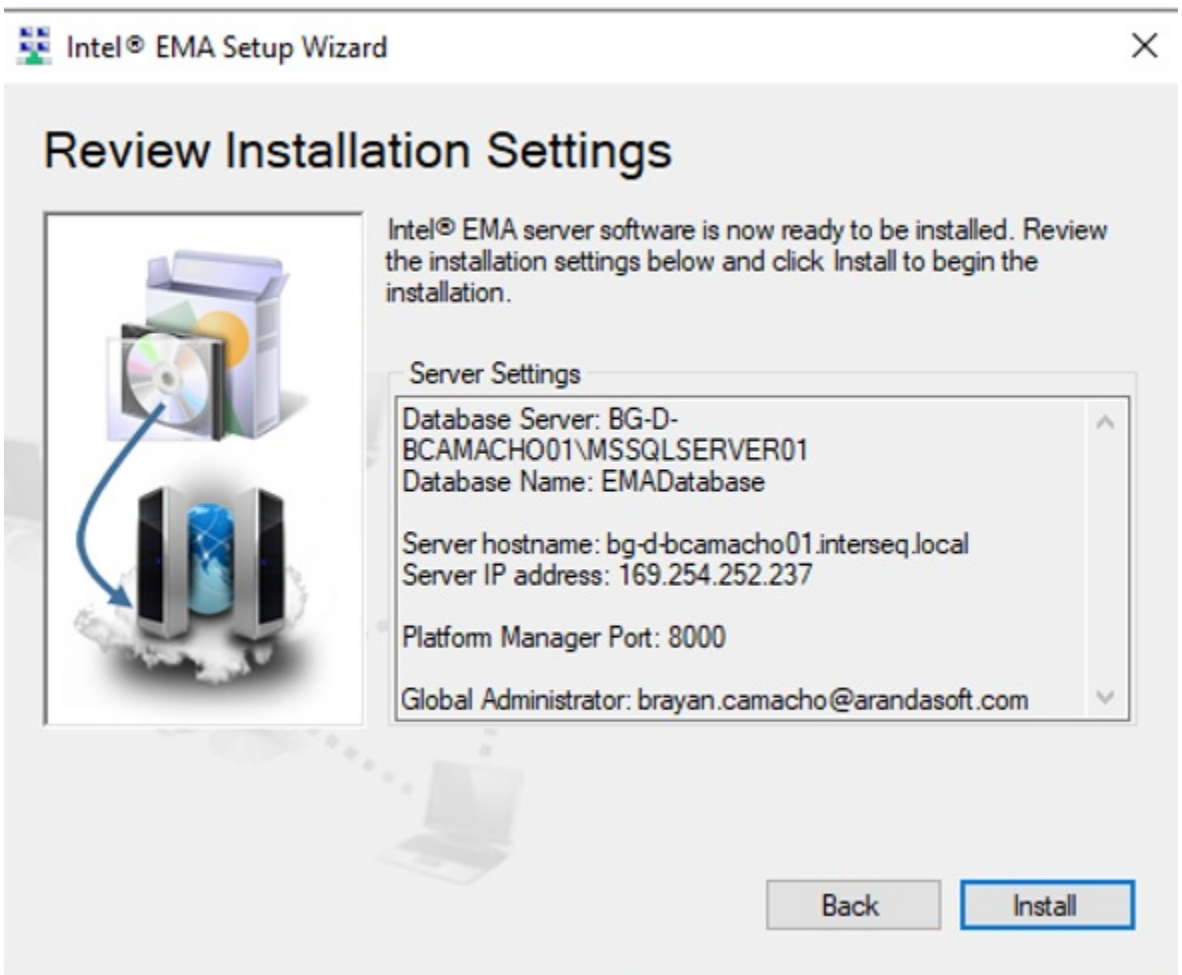
9. Instale el Platform Manager.



10. Configure el tipo de autenticación del usuario.

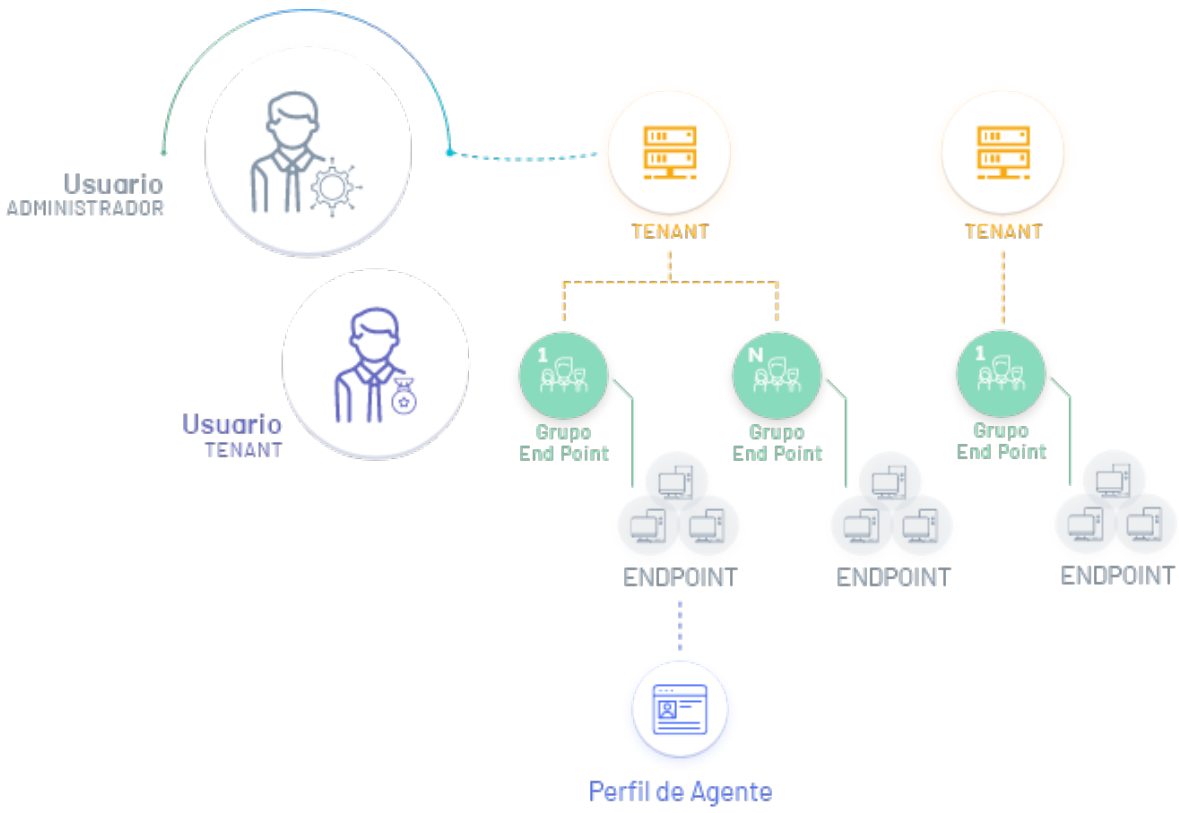
11. Agregue el nombre de usuario administrador de toda la instancia de EMA y guarde las credenciales para la administración general de EMA.

12. Hacer clic en **Instalar**.

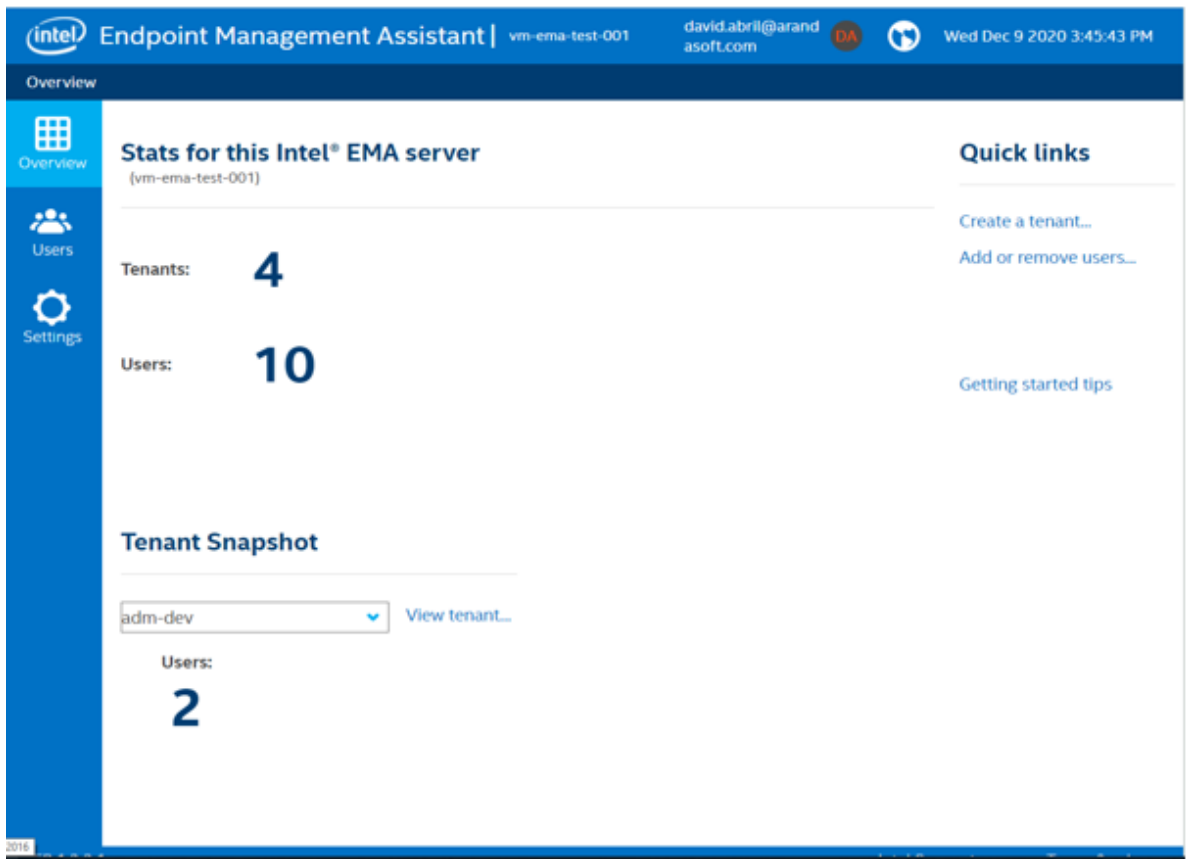


Configuración Tenant y Grupos Endpoint

En esta etapa de configuración desde Intel EMA se definen los permisos a nivel de jerarquía en la aplicación, donde el administrador local crea los tenant, luego los grupos de Endpoint, endpoint y perfil del agente.



1. Ingrese a la consola Enpoint Management Asistant como Administrador Global, con el usuario configurado durante la instalación. Enn la opción **Overview** del menú principal podrá visualizar los estados definidos.

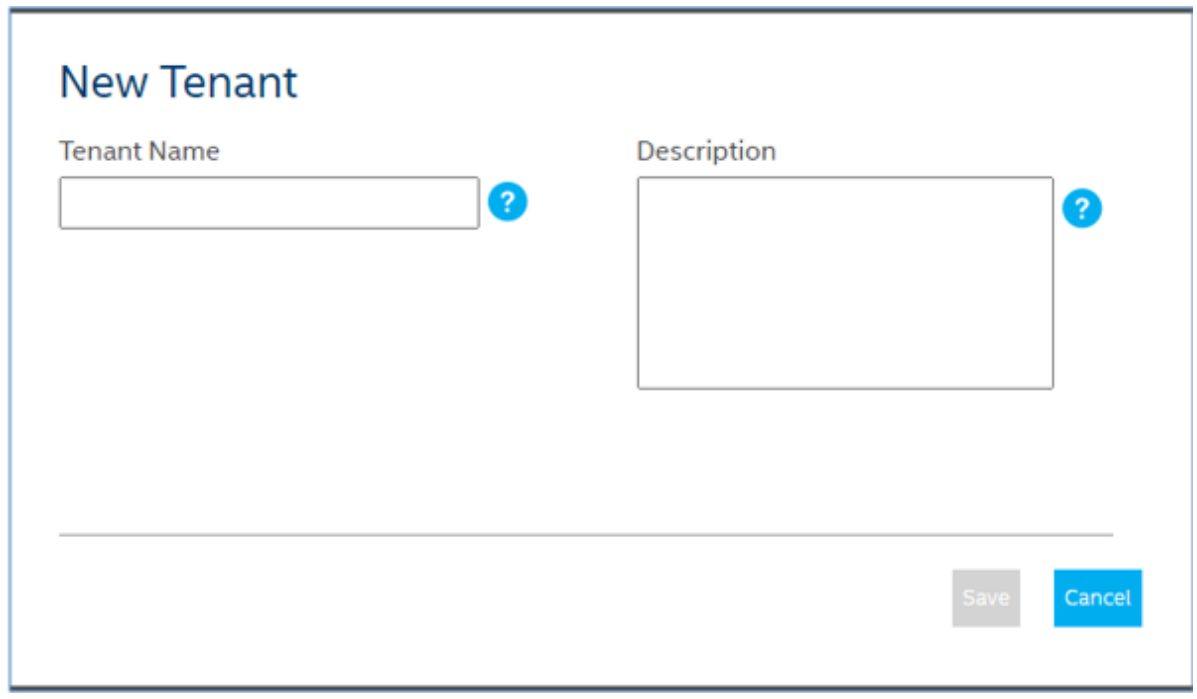


Crear Ternant

2. Para crear el tenant en la sección Quick Links de la vista de información seleccione la opción **Create a Tenant**. Se habilita la ventana para ingresar nombre y descripción.

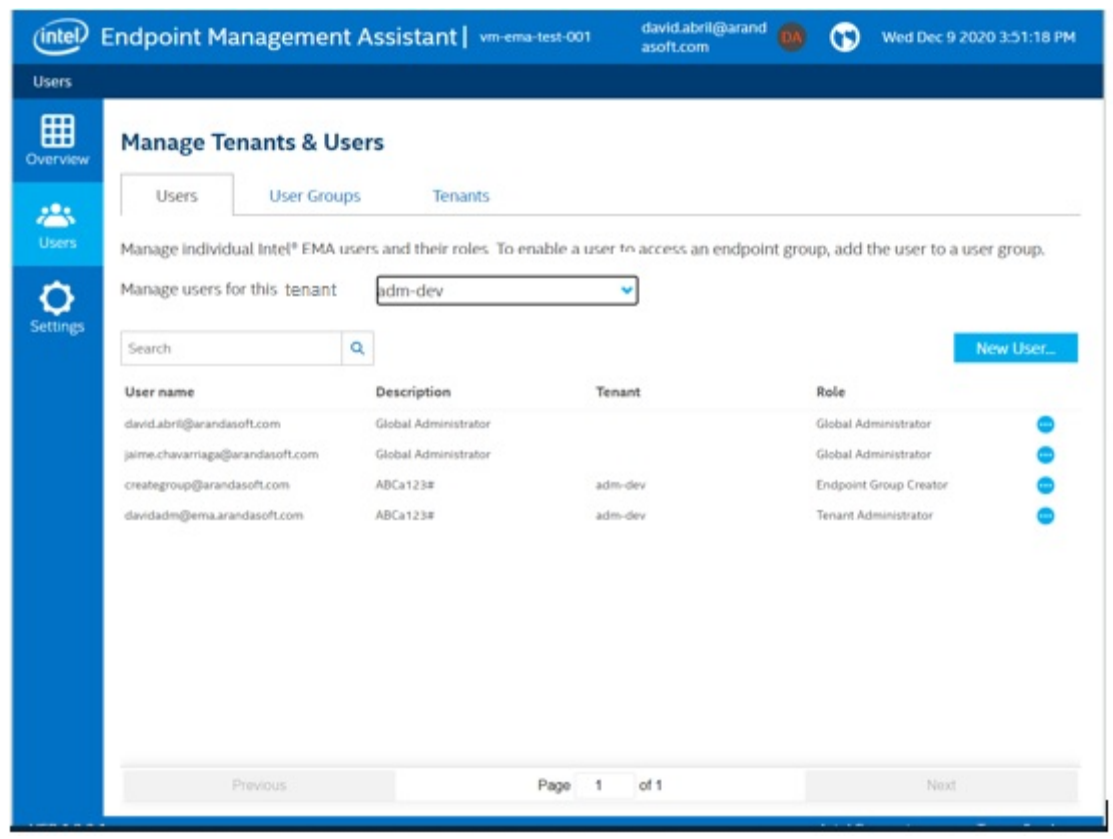
Este es el tenant que va integrar con ADM (Si va utilizar la instancia de EMA para sincronizar diferentes instancias de ADM, debe crear un tenant por cada instancia, se recomienda usar el nombre del cliente para diferenciar). }

3. Al completar la configuración haga clic en **Save**.



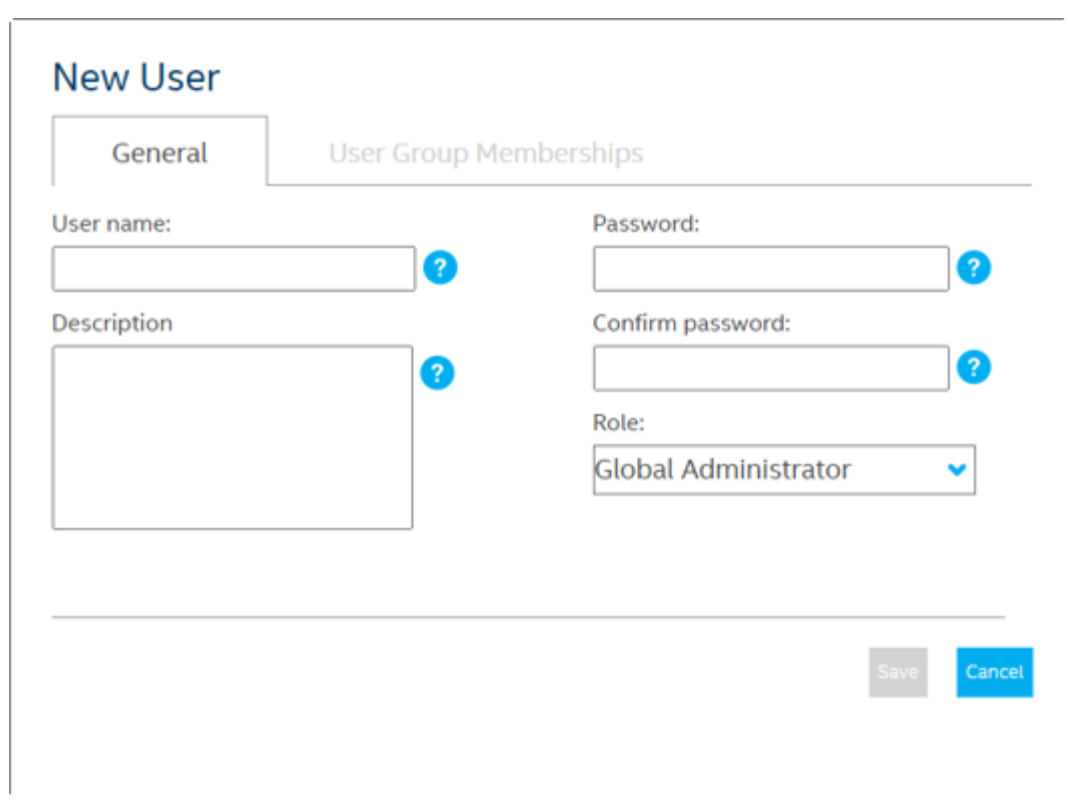
Crear Usuarios

4. Para crear usuarios adicionales al tenant (Global administrator, colaborador del tenant, etc.) en la sección Quick Links de la vista de información seleccione la opción **Add or Remove Users**. Se habilita la ventana **Manage Tenants and Users** donde podrá completar la información respectiva.



5. En la Pestaña **Users** seleccione el botón **New User** y en la ventana que se habilita podra ingresar información como nombre de usuario, descripción, contraseña y rol asociado al usuario.

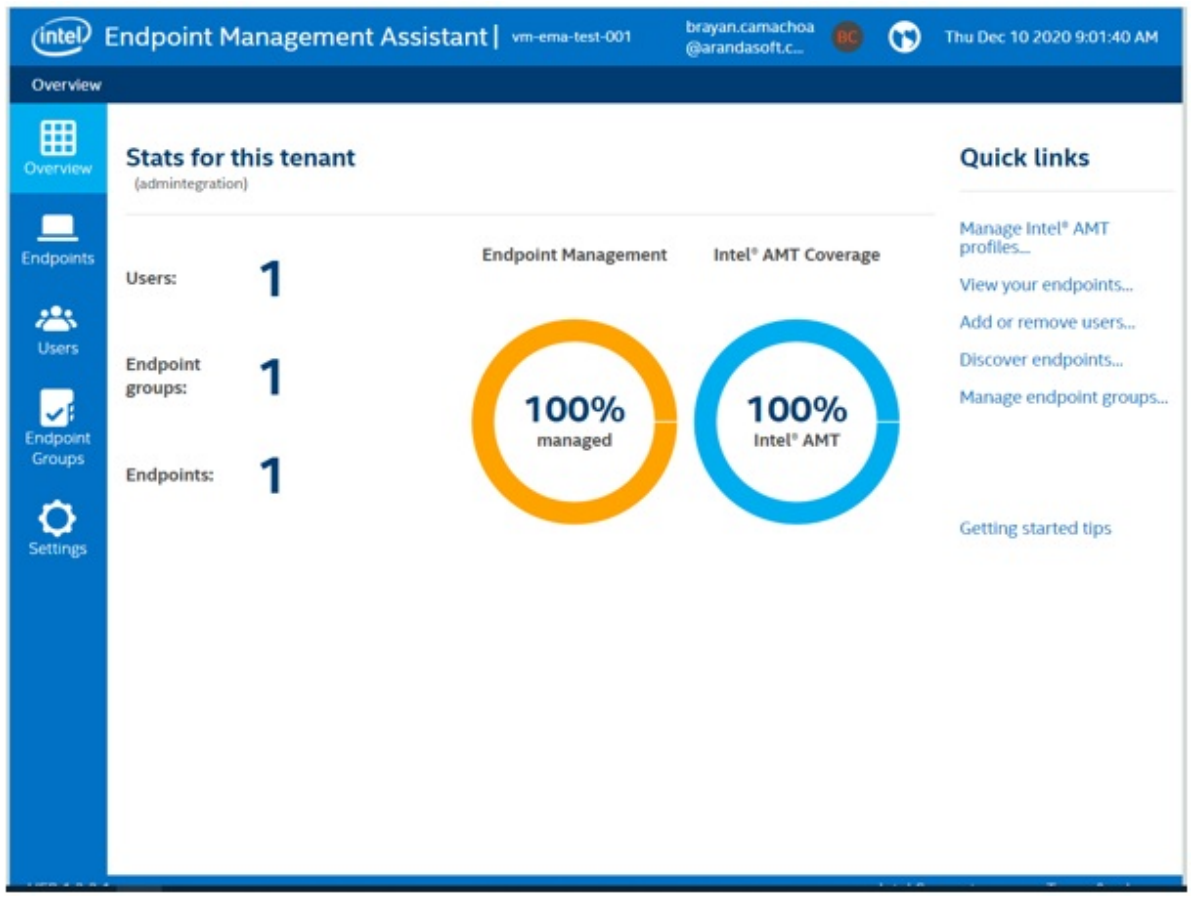
6. Al completar la configuración haga clic en **Save**.



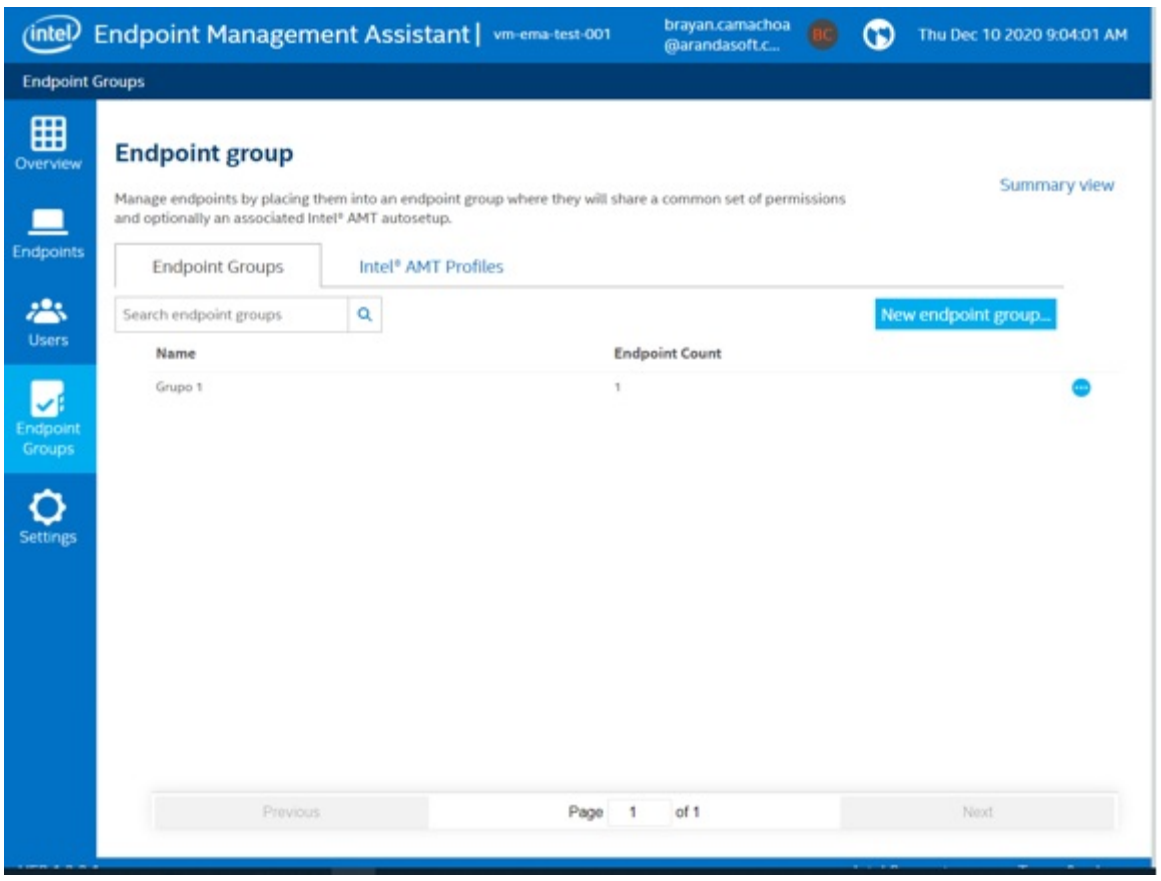
Generar Agente de Intel EMA

Crear Grupo Endpoint

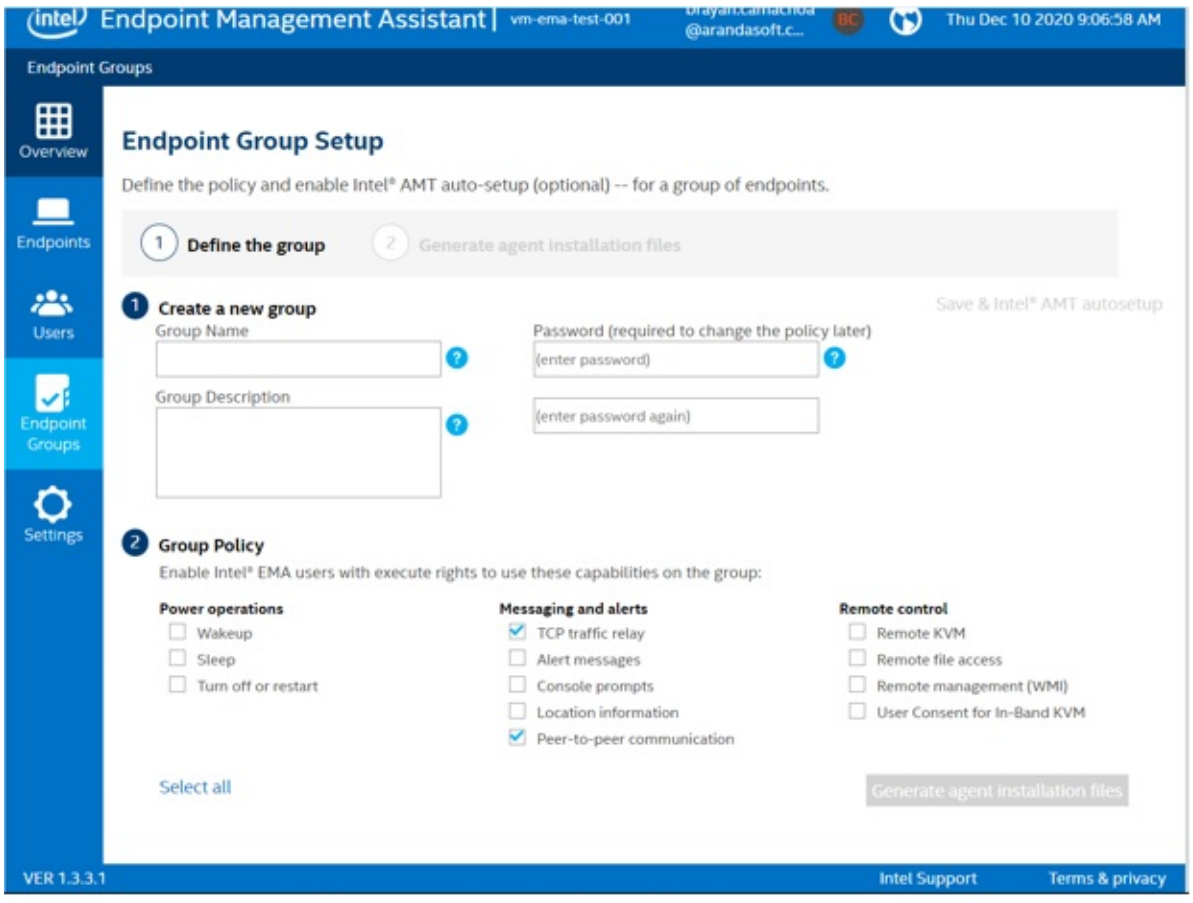
1. Ingrese a la consola Enpoint Management Asistant como Administrador de Tenant y seleccione la opción **Endpoint Group** del menú principal.



2. En la vista de información de **Endpoint Group** seleccione la opción **New endpoint group**.

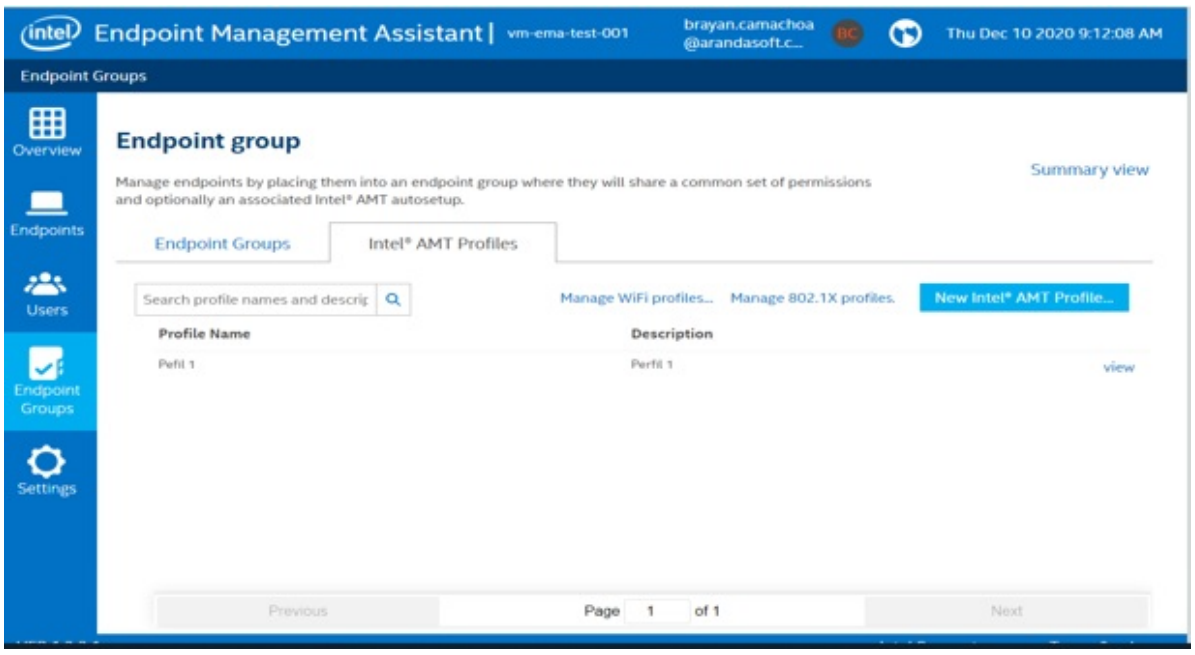


3. En la configuración del grupo ingrese nombre, descripción, contraseña y las políticas de acuerdo a las capacidades del grupo. Al terminar haga clic en la opción **Generate agent Instalation files** (Generar archivo de instalación de agente)

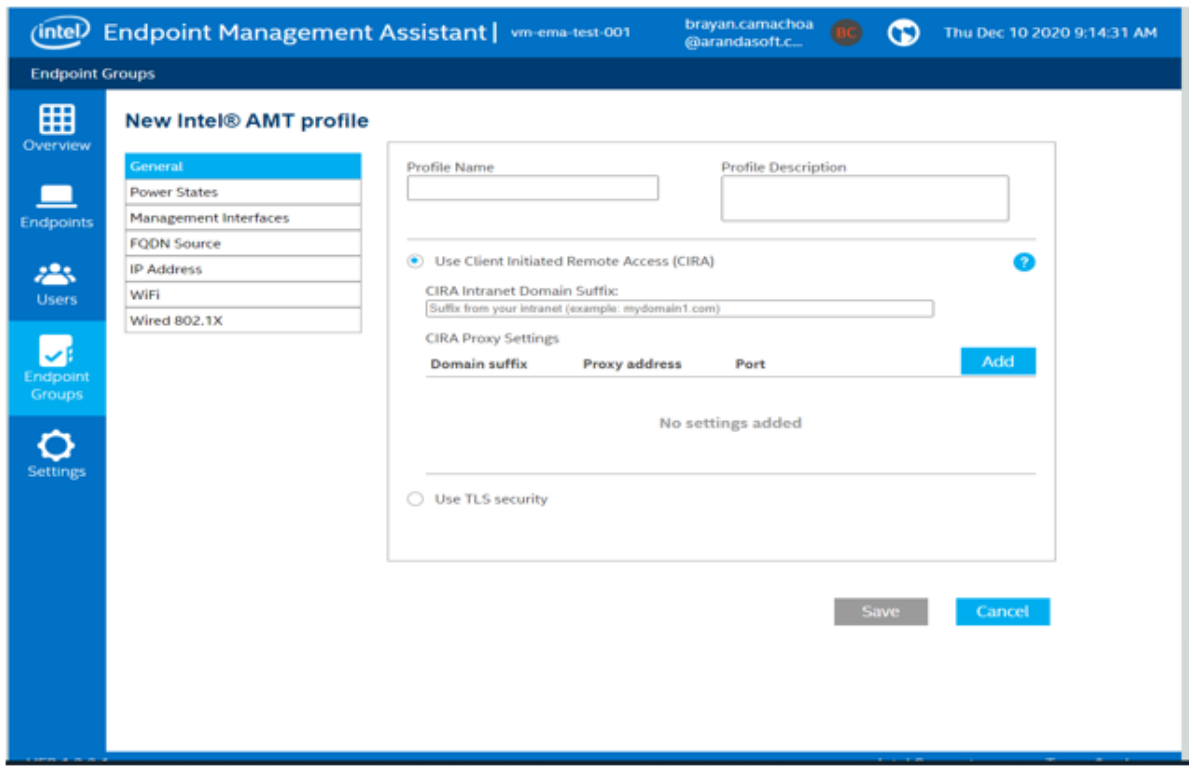


Perfil AMT

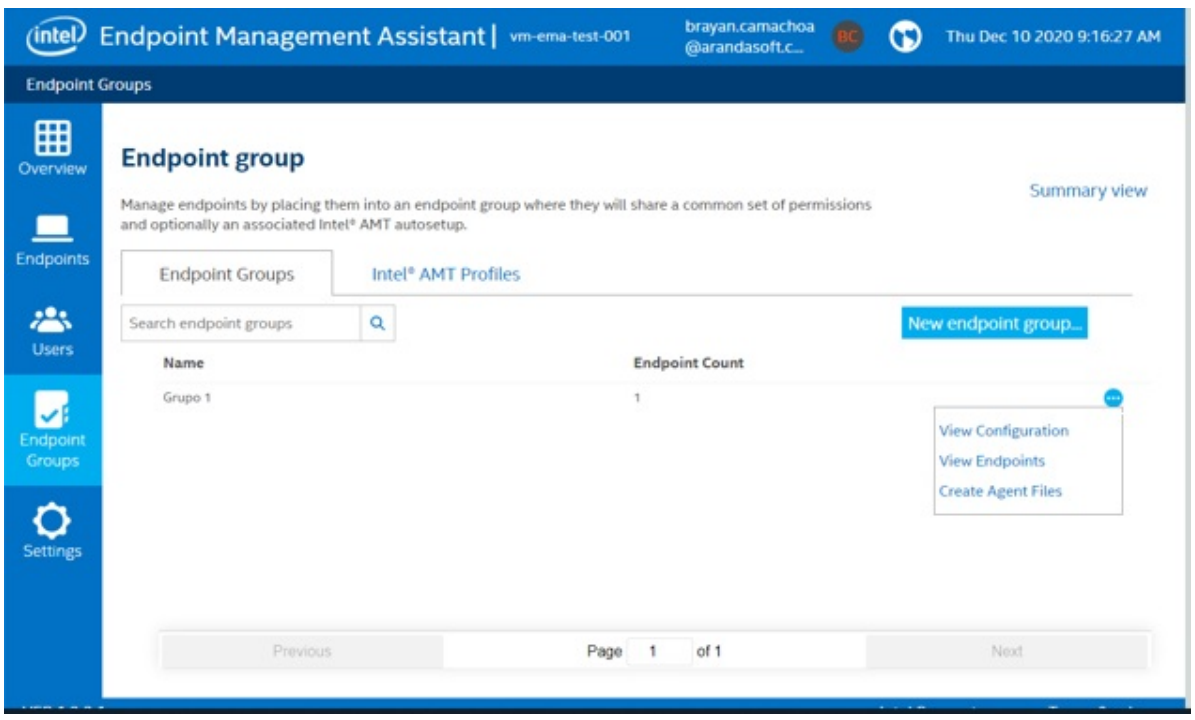
4. En la pestaña **Endpoint Groups** seleccione la opción **Generar un perfil de AMT**.



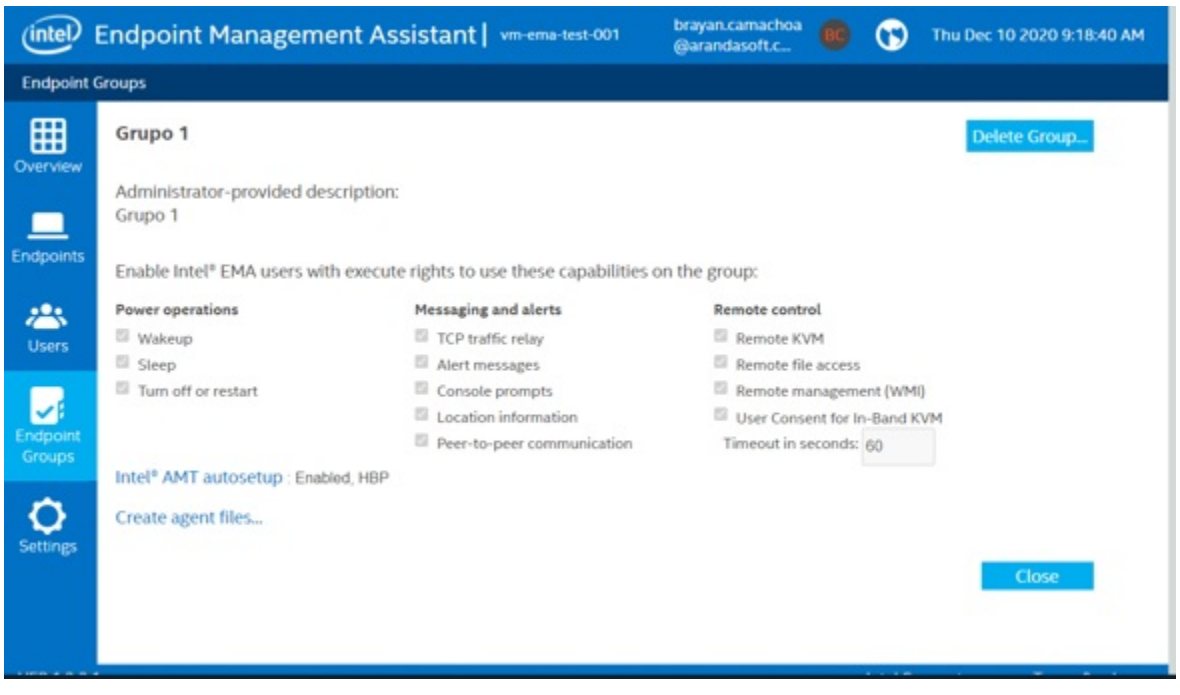
5. Configure la información relacionada al perfil de AMT.



6. Asigne el perfil de AMT al grupo de Endpoint.

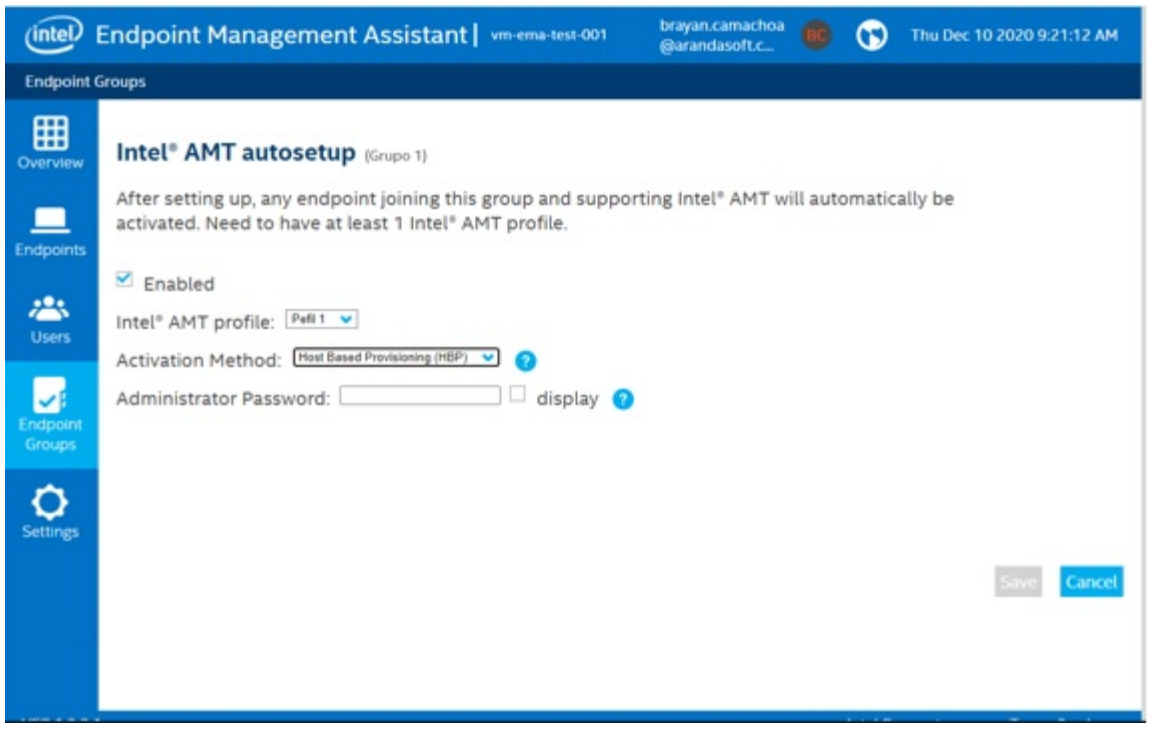


7. En el grupo haga clic en la opción **Intel AMT Autosetup**.

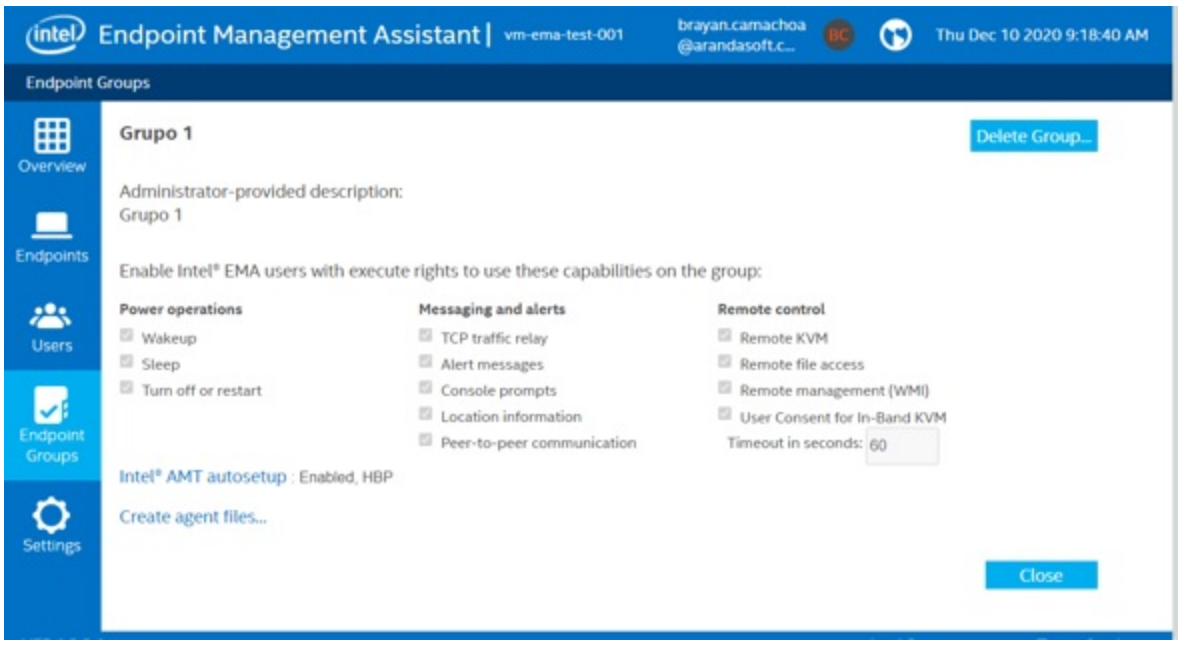


8. Seleccione el perfil de AMT y el método de activación. Ingrese el password de la BIOS; como administrador de TI asegure que todos los equipos tengan el mismo password para que este perfil les funcioné al instalarse.

> ⚐ **Nota:** Por defecto en los equipos de cómputo el password es "admin". se recomienda revisar doucmentación del modelo del dispositivo.

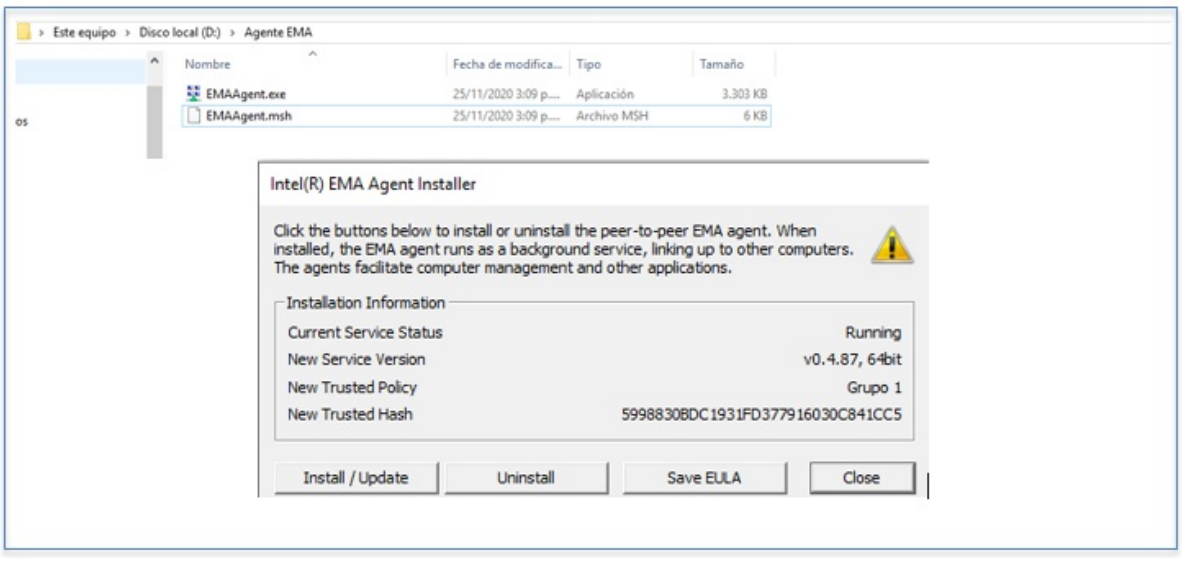


9. En el grupo haga clic en la opción **Create Agent Files** (Crear archivo de Agente).



9. Seleccione la versión del agente, descargue el servicio del agente y las políticas.

> ⚐ **Nota:** En la máquina cliente, que va a ser referenciada por EMA, debe tener los dos archivos (ejecutable y configuración) en la misma ruta, con el mismo nombre y ejecutar **EMAAgent.exe**.



> ⚐ **Nota:** Las máquinas que soporta EMA son aquellas que tienen firmware igual o superior a la versión 11, soportado generalmente por procesadores de 7ma Generación, algunos de 6ta Generación también lo soporta.

- Las versiones de los FW solo se pueden actualizar en subvsersiones de la versión que vienen de fabrica. Es decir que un procesado de 10 Generación no se puede actualizar de FW 14 a FW 15; lo que si puede hacer es actualizar de 14.1 a 14.2, 14.3, etc.

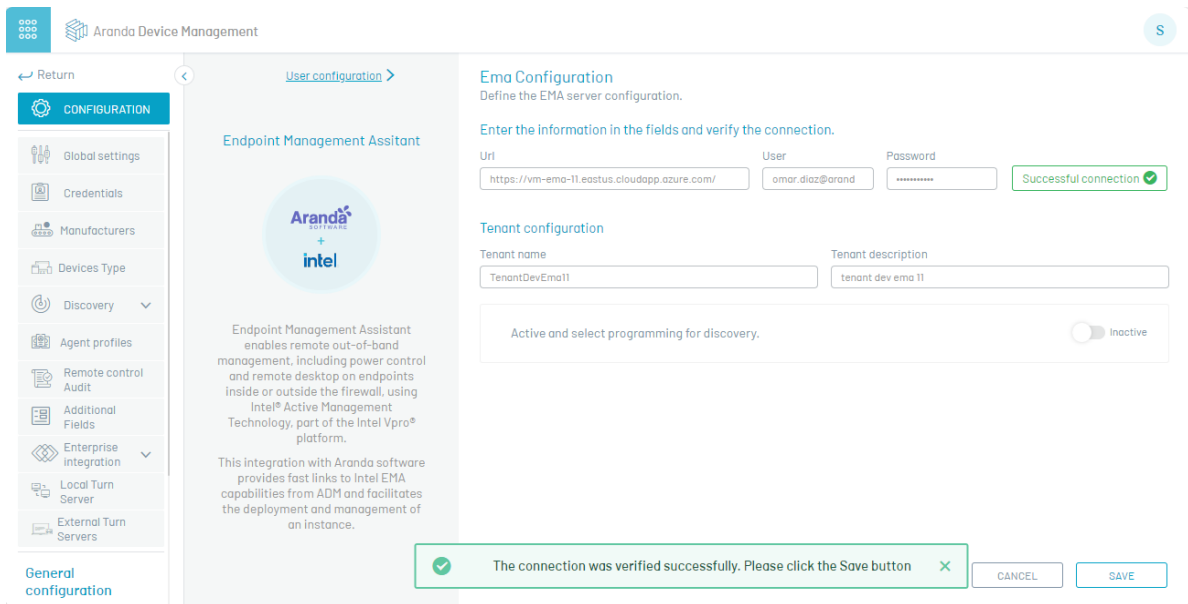
Intel® ME Firmwares Table

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

Habilitar Integración ADM - Intel EMA

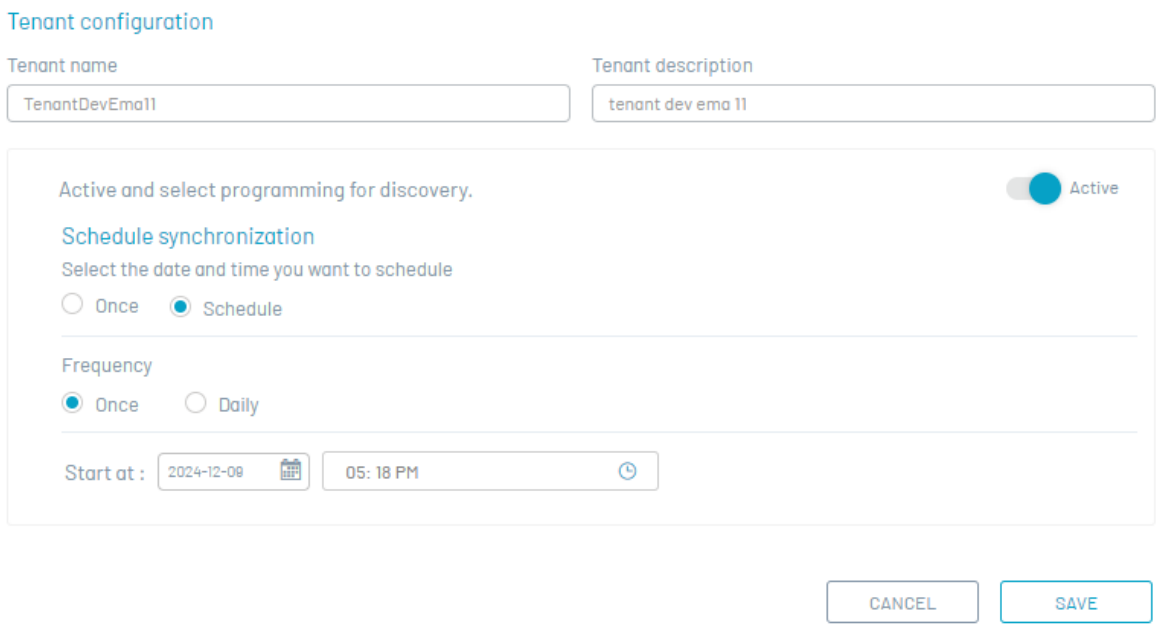
1. Para configurar la integración de Intel Ema, ingrese a la vista de Configuración de la consola de administración de ADM, en la sección **Generales** seleccione la opción **Integración Empresarial** y **Configuración EMA**.

2. En la vista de información ingrese la información básica como url, usuario administrador global y su contraseña. Haga clic en **Verificar Conexión** y si es válida se habilita la configuración de Tenant.



Configurar del Tenant

3. En la sección Configuración del Tenant podrá ingresar el nombre del tenant que creó previamente durante la exploración de la consola EMA y descripción del tenant. Active la opción para la programación para el descubrimiento desde el switch.



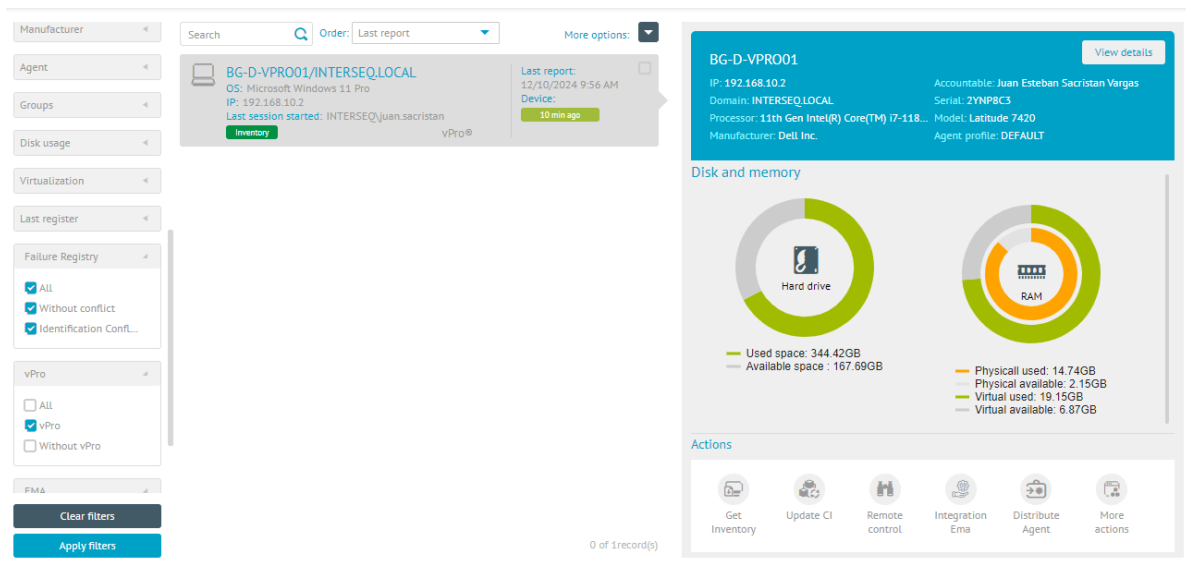
Programación para el Descubrimiento

4. Se puede ejecutar de inmediato o programar una tarea que permita sincronizar los dispositivos de ADM con los Endpoint de EMA. Esta tarea es la responsable de hacer "match" de las maquinas descubiertas por ADM y las maquinas que estan registradas en Intel EMA. (esto permte que exista una navegación desde la consla de ADM a Intel EMA sobre un dispositivo en específico)

5. Al hacer clic en **Guardar**, genera el servidor y el usuario con Administrador Global para las peticiones con el Api de EMA, luego procede a crear si no existe el Tenant y por último genera la tarea programada para la sincronización de los dispositivos.

Visualización dispositivos compatibles con Intel Ema

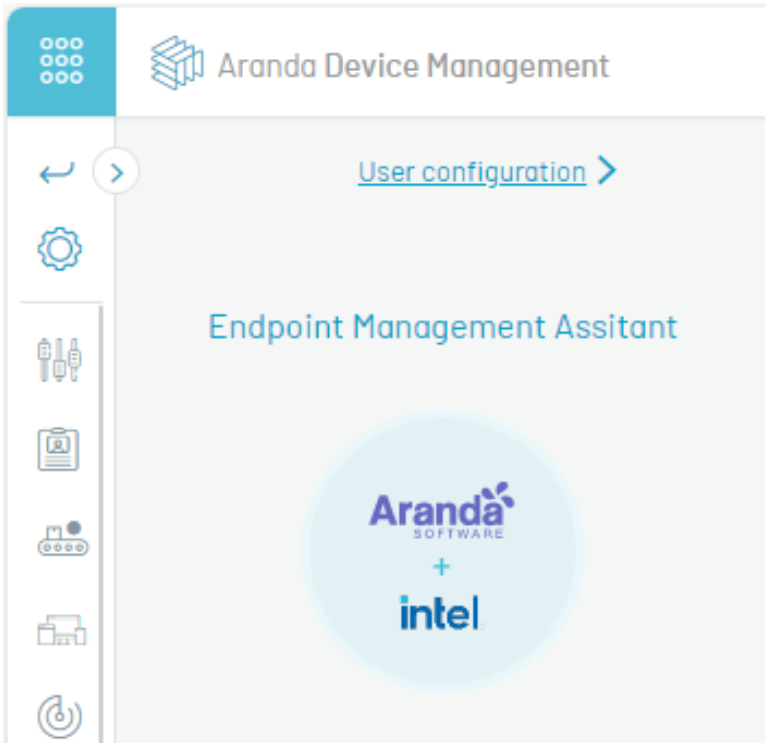
En el listado de dispositivos se visualizan los equipos que tienen procesador Vpro, puede usar los filtros para listar únicamente los dispositivos que tengan este tipo de procesador.



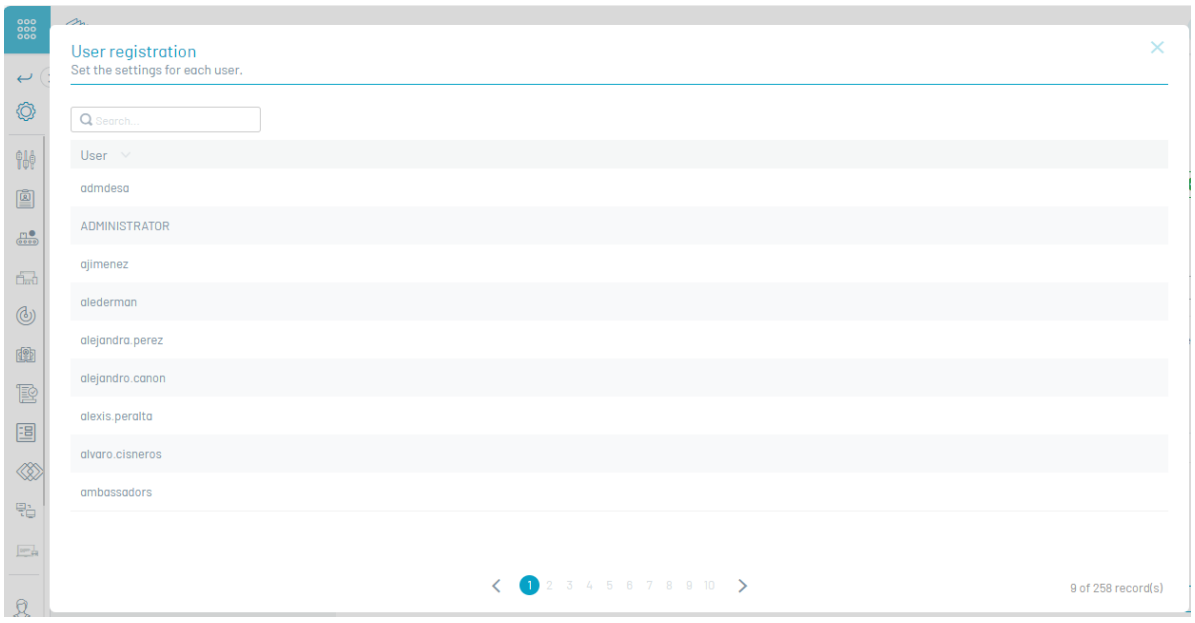
Con estos dispositivos de podrá acceder a todas las funcionalidades de Intel Ema después de realizar la instalación del agente.

Creación de Usuario Administrador de Tenant de EMA

1. Para crear el usuario administrador de Tenant de Ema, ingrese a la vista de Configuración de la consola de administración de ADM, en la sección **Generales** seleccione la opción **Integración Empresarial** luego **Configuración Ema** e ingrese a **Configuración de usuarios**.

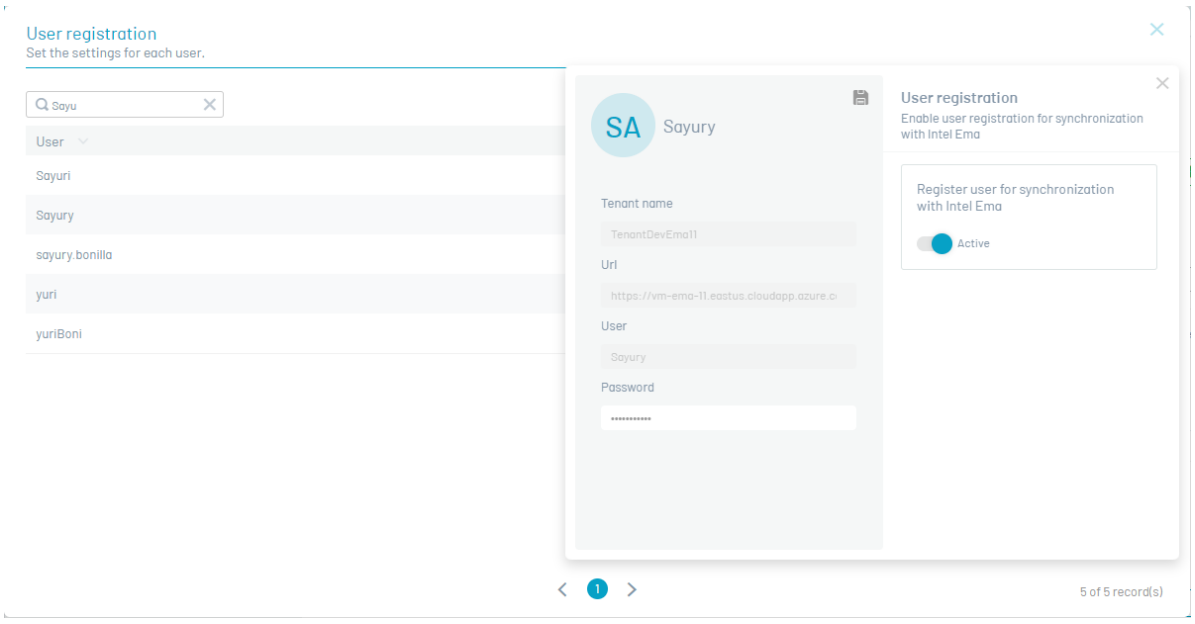


2. En la Vista **Registro de Usuarios**, podrá visualizar y filtrar los usuarios disponibles para configurar como administradores del tenant.



⚐ **Nota:** El usuario debe tener configurado un correo electrónico válido para crear el usuario Administrador de Tenant.

3. Seleccione el usuario de Integración Ema y proceda a editarlo. Ingrese la clave correspondiente y active el usuario de EMA; podrá registrar el usuario como el encargado de la sincronización.



4. Al terminar de configurar la información básica del usuario, Haga clic en **Guardar** para confirmar los cambios realizados.

Acceso directo con EMA

Una vez realizado todo el proceso de configuración y después de ejecutada la tarea de sincronización entre ADM e Intel EMA, el usuario podrá navegar desde el detalle de un dispositivo de ADM a la consola de EMA y hacer las operaciones que requiera.

Acceso desde ADM

1. Ingrese a la vista de Inicio de la consola de administración de ADM y seleccione el módulo **Inventario** del menú Encabezado y la opción **Dispositivos**. En la vista de información se podrá visualizar el listado dispositivos inventariados.

> ⚐ **Nota:** Si el dispositivo se sincroniza con EMA podrá visualizar el logo de **Integración EMA** en el listado de dispositivos.

---

2. En la vista detalle del dispositivo integrado, seleccione la acción **Integración Ema**

---

3. En la vista detalle del dispositivo se habilita la acción descrita. Haga clic en **Aceptar**, para redireccionar el proceso a la consola **Enpoint Management Asistant**

Acceso desde Intel EMMA

4. Si el usuario ya esta autenticado en la consola de EMA, podrá acceder directamente al dispositivo, si no lo está, el sistema le solicita credenciales para ingresar como usuario administrador de tenant, creado durante el proceso de configuración o en la sección de Creación de Usuario Administrador de Tenant de EMA.

Una vez autenticado, el usuario podrá visualizar el Endpoint (dispositivo) para acceder ejecutar acciones de administración desde Intel EMA.

Control Remoto ARC

Control remoto (ARC)

Permite tomar el control de las máquinas de manera sencilla y eficiente y transferir archivos de manera conveniente, facilitando la gestión a distancia de las estaciones de trabajo.

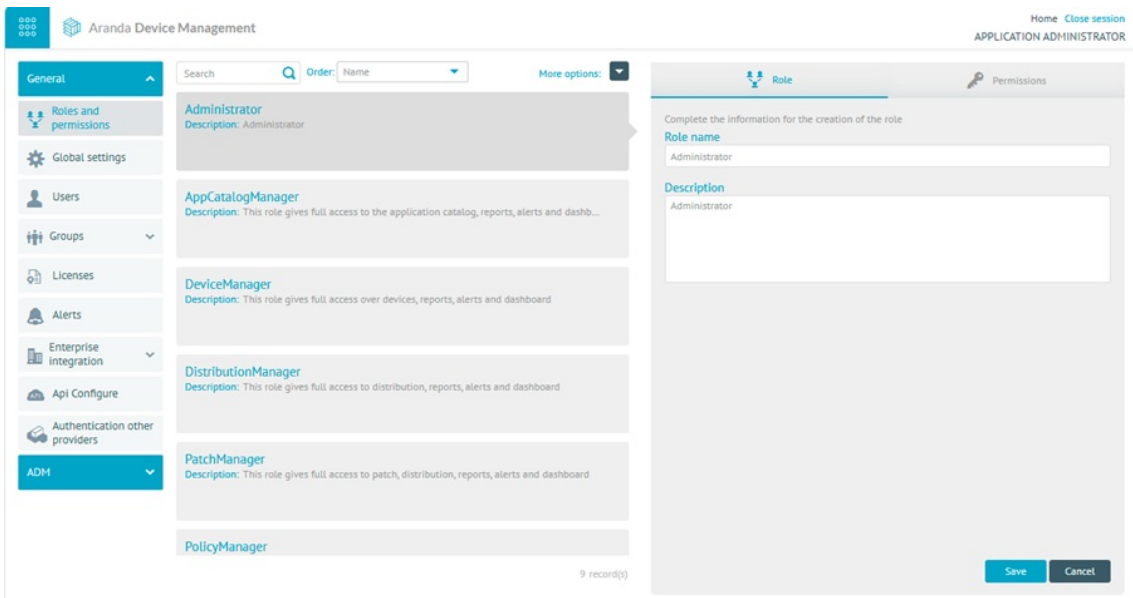
> ⚐ **Nota:** Tener en cuenta la siguiente arquitectura soportada para el control remoto:

- Esta funcionalidad no es soportada para versiones de agente liberadas de ADM inferiores a 9.19.2 (Cloud)
- Esta funcionalidad no es soportada en instalaciones OnPremises de ADM versiones inferiores a 9.21.1

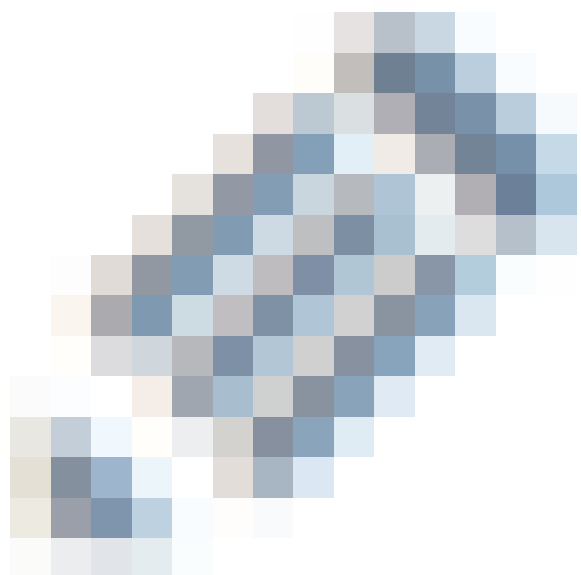
Proceso de configuración instalaciones OnPremises

Debe tener en cuenta los siguientes pasos para la configuración del control remoto en instalaciones OnPremise:

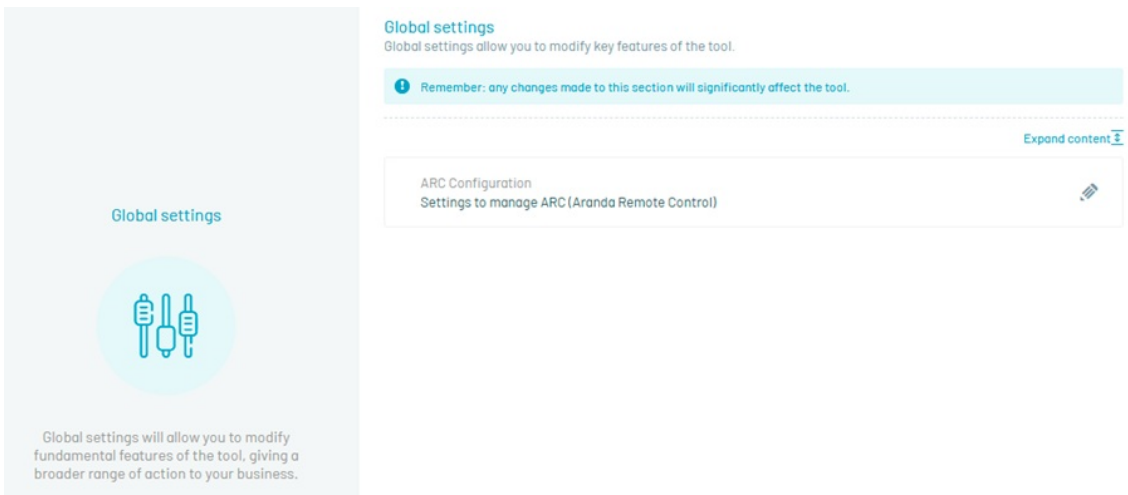
- Habilitar la funcionalidad en la consola de ADM ingresando a **Configuración** > **Generales** > **Configuraciones globales**.



- En la vista de información de **Configuraciones Globales**, seleccione la opción **Configuración ARC** haga clic en **Editar**

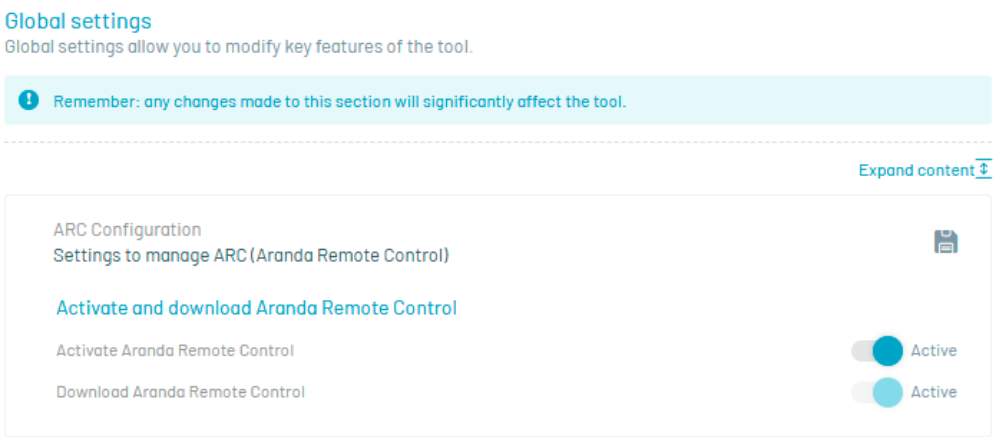


o en el botón **Expandir contendido**.



⚐ **Nota:** En implementaciones cloud, este campo solo podrá visualizarse, pero no editarse. {: #important}

- Validar que **Activate Aranda Remote Control** tenga el checkbox habilitado (valor por defecto). Si no lo está, habilítelo y haga clic en el botón **Guardar**.



- Realizar la configuración correspondiente posterior a la instalación de **Aranda.ADM.Web.Installer** en el servidor de aplicaciones. Ver configuración

Proceso de configuración e instalación de Agentes

Tenga en cuenta los siguientes pasos para la configuración e instalación de los agentes de control remoto:

- Para realizar control remoto se requiere tener la instalación del componente de control remoto en los dispositivos a los cuales se va a realizar la conexión remota.Instalación componente de control remoto
- Instalación del visor de control remoto, requerido en el dispositivo desde donde se realiza la conexión remota Instalación visor control remoto

Requerimientos de Uso Aranda Remote Control

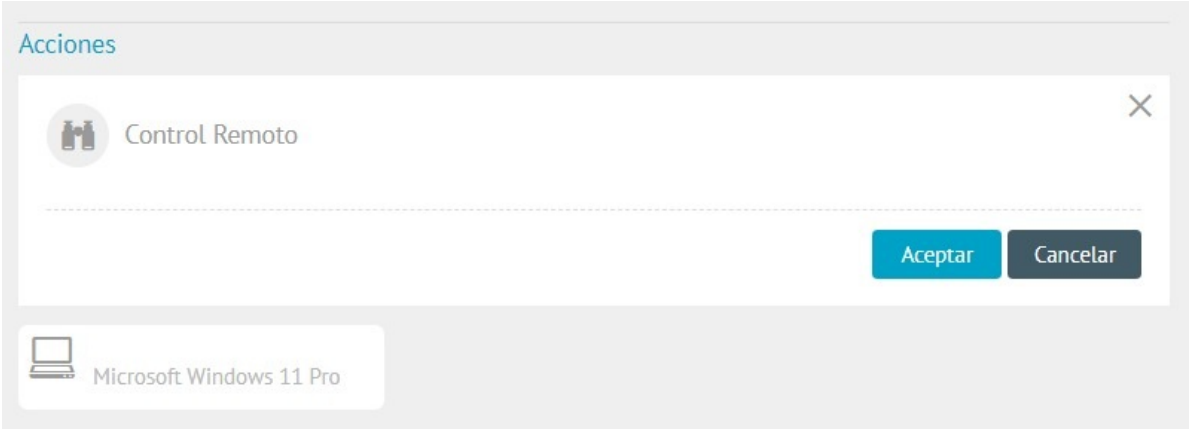
Tomar Control Remoto

Para realizar control remoto se debe tener configurado previamente lo siguiente:

- Para realizar control remoto se requiere tener activo el permiso de Soporte remoto en el rol del usuario de ADM.Roles y Permisos.
- El dispositivo debe estar asociado a un grupo de dispositivos. Grupos
- Se requiere crear una relación entre el grupo de dispositivos y el usuario o grupo de usuarios autorizado para realizar control remoto.Relaciones

Una vez realizada la configuración anterior:

- En el menú **Inventario** > **Dispositivos** debe seleccionar el dispositivo disponible, hacer clic en la acción control remoto y luego en **Aceptar**.



- En el navegador se habilita la pestaña **sesión de soporte**, donde podrá visualizar la información del dispositivo, abrir el visor de control remoto y realizar transferencia de archivos entre los dispositivos.

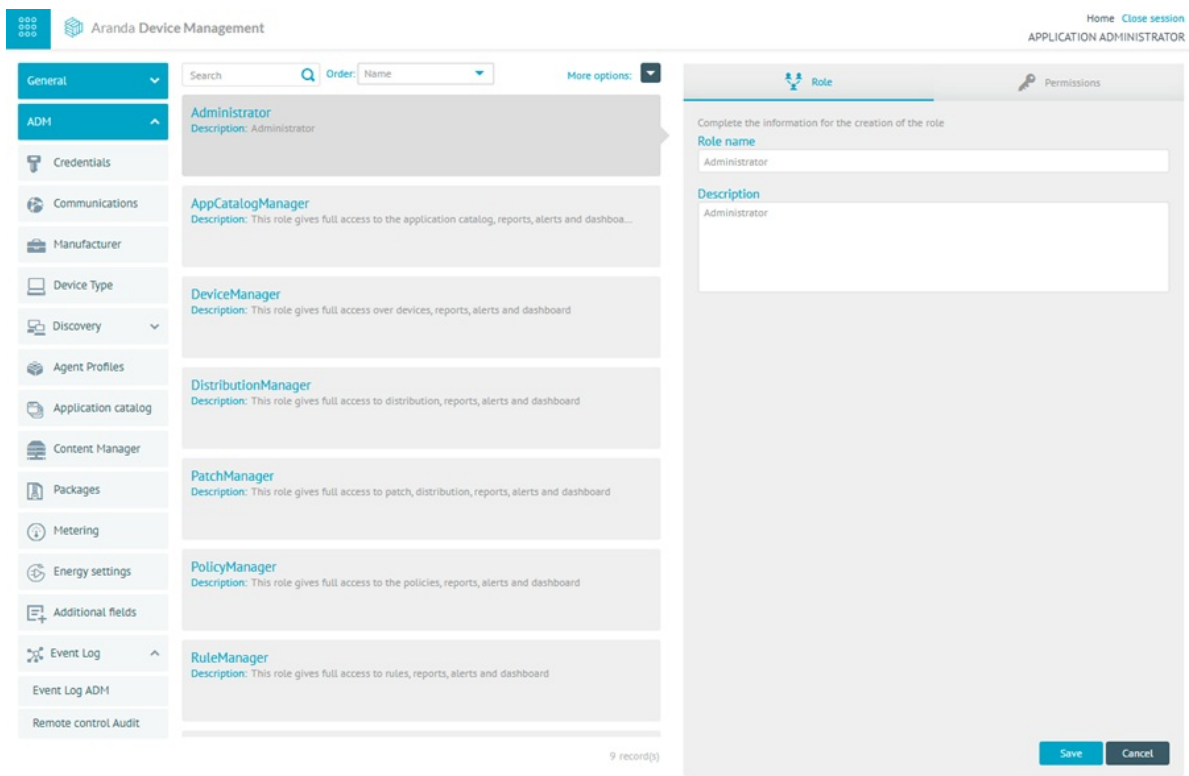
Tomar control remoto

Transferencias de archivos

Auditoría de control remoto

Esta función permite que los eventos registrados al ingresar a la sesión de soporte, sean visibles en la sección de Registro de Eventos. Es posible realizar búsquedas desde el filtro, agregar y/o ocultar columnas. Se registran los eventos al solicitar, iniciar o finalizar control remoto, al enviar o recibir archivos.

Para visualizar estos registros se debe dirigir en la consola de ADM a **Configuración > ADM > Registro de eventos > Auditoría de control remoto**.



Se habilita una pantalla donde podrá visualizar los todos los eventos realizados en la sesión de soporte.

Auditoría de Control Remoto

Instalación de Componentes

Instalación componente de control remoto

↩ Integración ARC

Los agentes de Windows de ADM desde la versión de ADM 9.19.2, después de realizar la instalación de cero o una actualización desde de una versión anterior, se instalará automáticamente el nuevo componente de control remoto transcurrido 30 minutos. Se visualizan los siguientes procesos y servicios en el dispositivo.

> ⚐ **Nota:** En caso de presentarse alguna falla de conexión al momento de la instalación o actualización del componente de control remoto, el agente de ADM realizará reintentos de instalación cada 4 horas.

Procesos y servicios componente de control remoto

Actualización componente de control remoto

↩ Integración ARC

Instalación visor control remoto

↩ Integración ARC

Instalacion visor control remoto

↩ Integración ARC

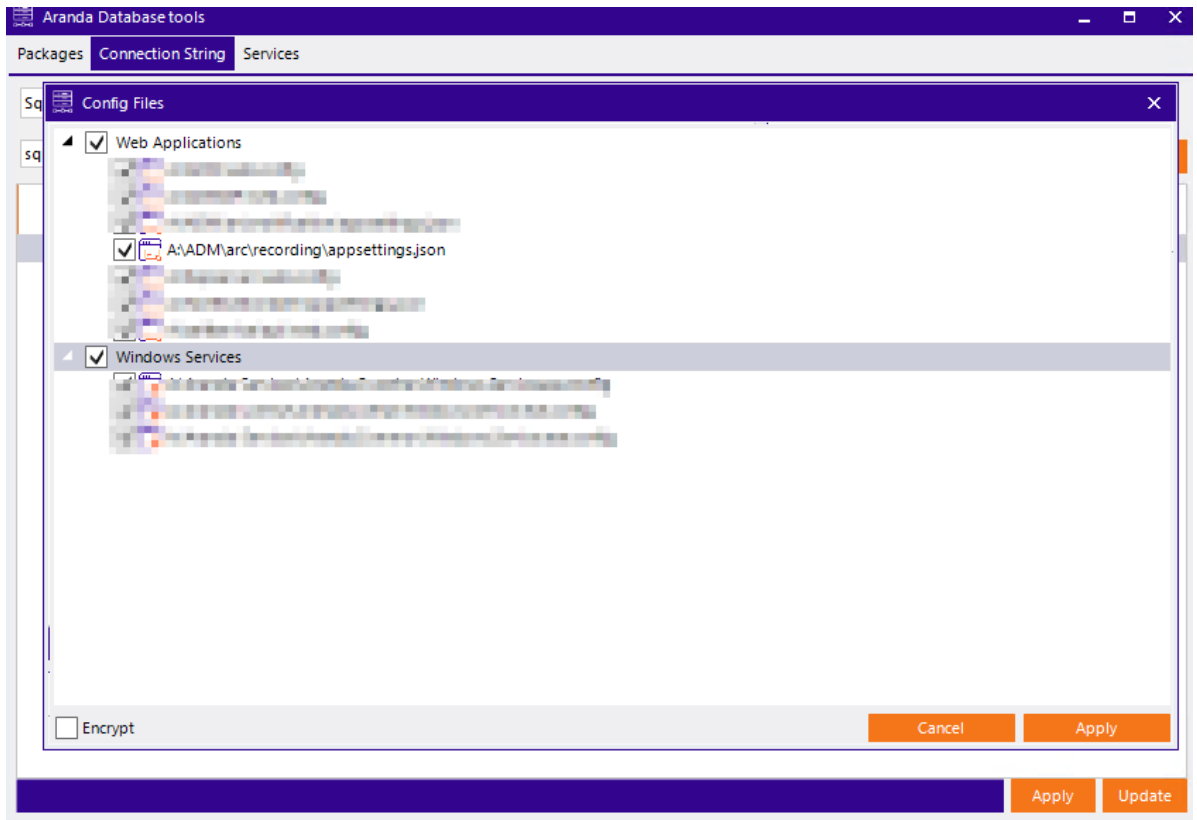
Configuración Ambientes OnPremises

Configuración control remoto ARC

Después de instalar el archivo **Aranda.ADM.Web.Installer** realice las configuraciones posteriores en el servidor de la aplicación y desde la consola de ADM para garantizar el correcto funcionamiento del nuevo control remoto, teniendo en cuenta los siguientes pasos:

1. Configurar cadena de conexión

Configure la cadena de conexión para el sitio de grabaciones, a través del módulo Aranda Database Tools v9. Los sitios de notificaciones no requieren configurar cadena de conexión.



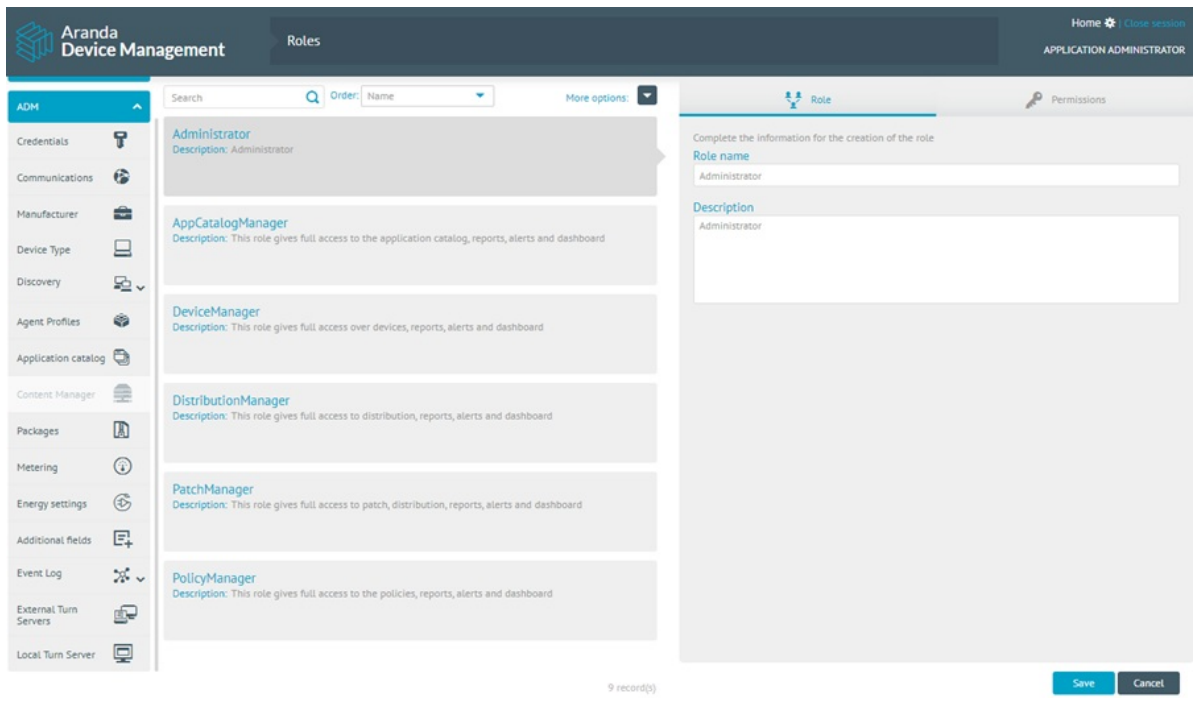
⚐ **Notas:**

- Cuando se aplique la configuración con el Encrypt habilitado se podrá visualizar un mensaje de alerta porque la encriptación no está soportada para archivos JSON.
- Al realizar cambios en la cadena de conexión de servidor de grabaciones reinicie el IIS para que los cambios se apliquen deforma correcta.
- Si, posterior a la configuración, se realizan cambios en el proveedor de almacenamiento, mueva 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 podrá acceder a las grabaciones en las auditorías..

2. Ingresar a la consola

Ingrese a la consola de ADM con el usuario con los permisos requeridos para gestionar las opciones de Servidores Turn externos y Servidor Turn local en la Configuración de ADM.

⚠ **Importante:** Las opciones de Turn Externo y Local están disponibles únicamente en instalaciones On Premise.



3. Servidores Turn Externos

La funcionalidad de transferencia de archivos del control remoto 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:

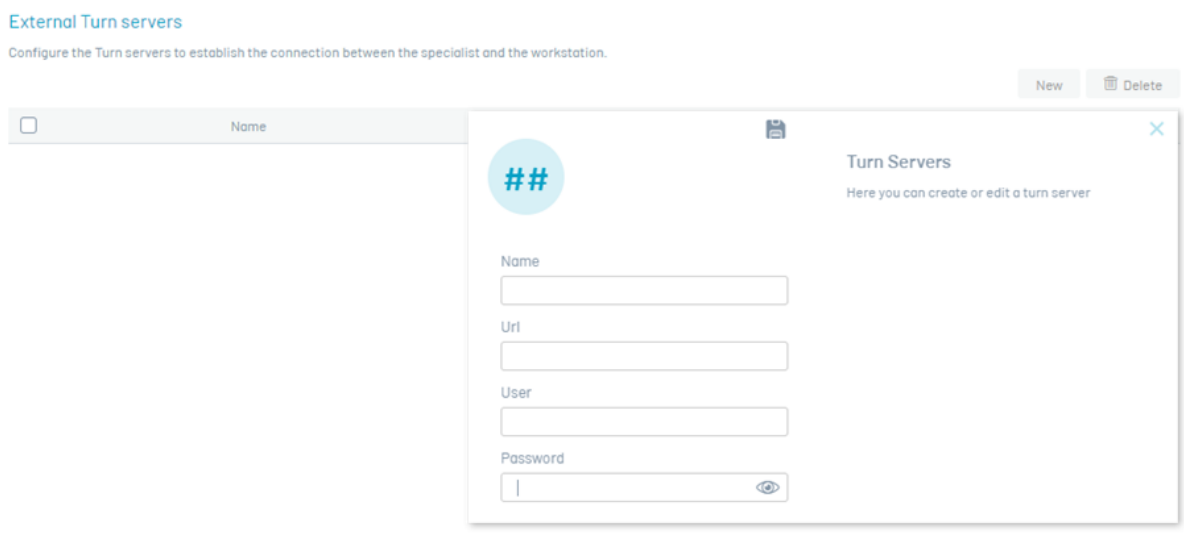
A. Haga clic en la opción **Nuevo**.

B. Complete los campos solicitados de acuerdo a la siguiente tabla:

Campo	Descripción
Nombre	Nombre que se le desea asignar a la configuración, entre 6 y 50 caracteres.
URL	Corresponde al sitio del servidor STUN/TURN, por ejemplo: turn:<server_public_ip>:puerto o stun:<server_public_ip>:puerto .
Usuario	Nombre del usuario autorizado para conectar al servidor STUN/TURN.
Contraseña	Contraseña asociada al usuario que permite la conexión con el servidor STUN/TURN.

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

> ⚐ **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 misma red, por lo tanto, se debe permitir la salida a Internet de ambos dispositivos por el puerto configurado.



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 ADM.

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, realizando una búsqueda en la web "STUN server list" se podrán listar los diferentes servidores STUN/TURN públicos disponibles. Al configurar servidores públicos en las estaciones de trabajo y en los equipos especialistas deben permitir la salida hacia los sitios de los servidores que se configuren. También es posible configurar el servidor STUN/TURN provisto en el instalador realizando los ajustes en el servicio Aranda Turn Stun WebRTC Server Windows Service. Además, se pueden utilizar STUN/TURN públicos junto con servidores propios instalados, como se mencionó anteriormente.

4. Servidor Turn Local

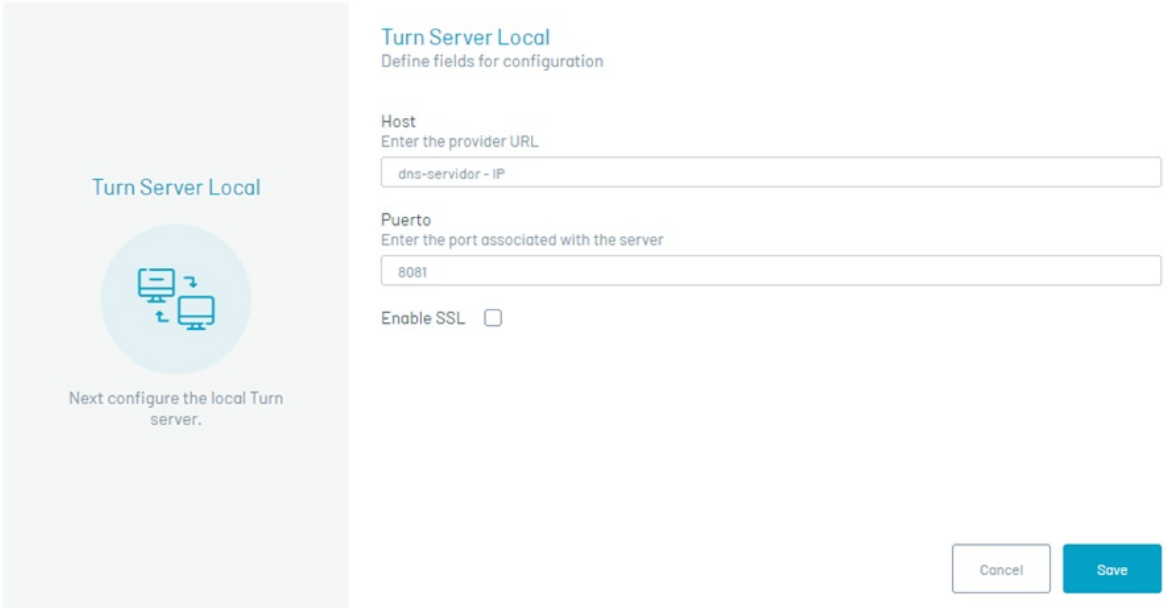
Para establecer la comunicación de toma de control remoto entre el agente especialista y el agente de la estación de trabajo, utilice un servidor Turn local que puede retransmitir el tráfico de red.

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 realice los ajustes en el servicio Aranda Turn Server instalado en el servidor.

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



Configuración Manual de Servicios

Configuración del Turn Server

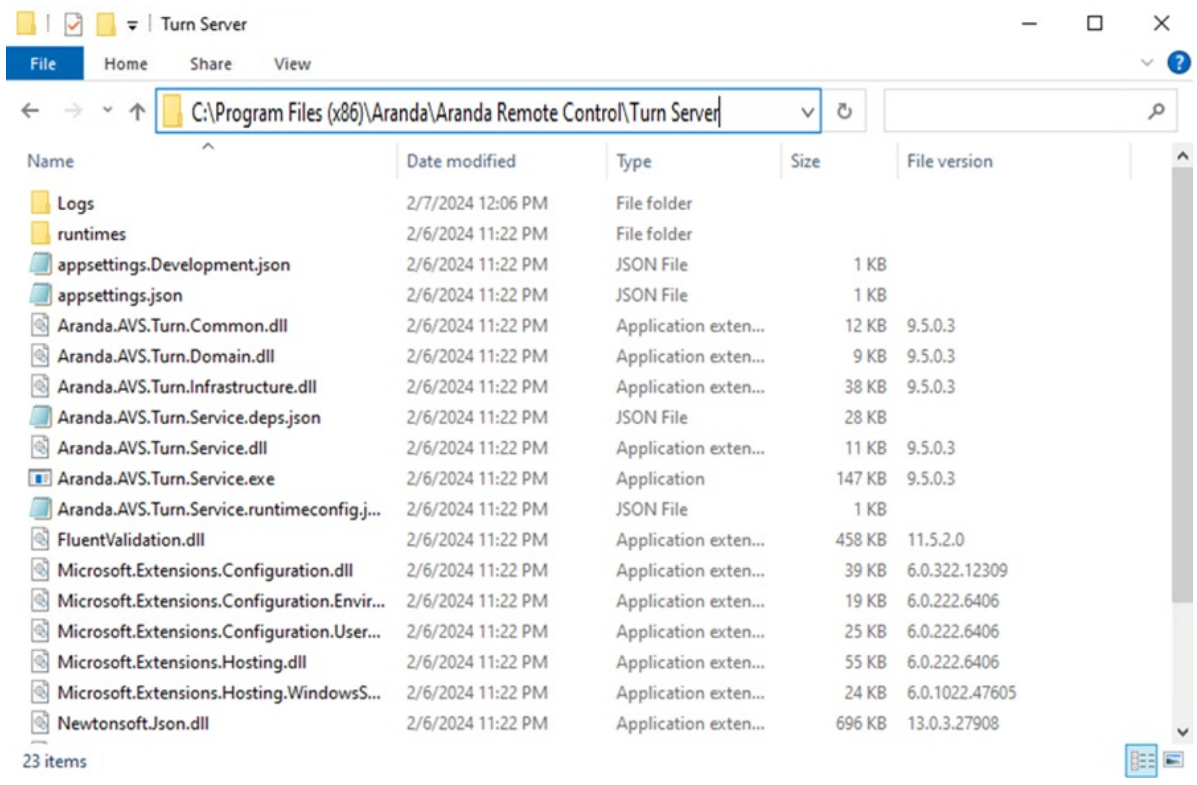
↩ Servidor Turn Local

Después de instalar el servicio Aranda 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 (x86)\Aranda\Aranda Remote Control\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

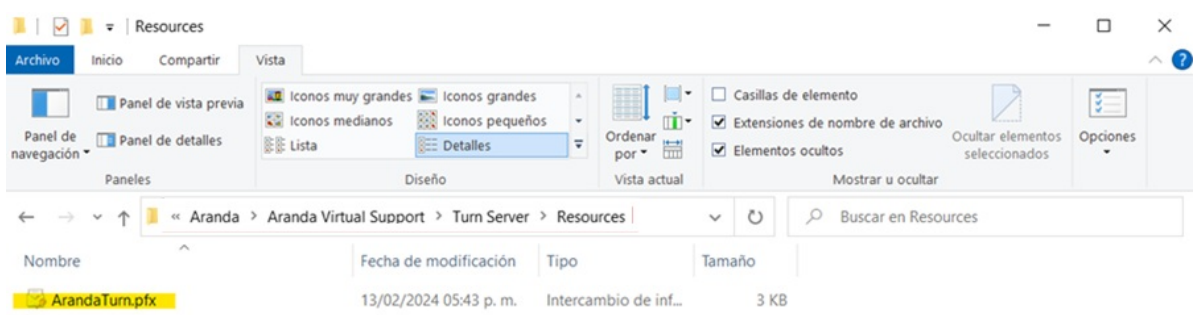
Edite el archivo *appsettings.json* y configure el puerto deseado reemplazando <puerto> por el número de puerto deseado.

```
"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 Turn Server Windows Service) 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

Configuración del Servidor Stun/Turn WebRTC

↩ Servidor Turn Externo

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

1. Validación del Archivo turn-server.toml

Antes de realizar cambios, verifique que el archivo **turn-server.toml** se encuentre ubicado en la ruta de instalación del servicio (por defecto: 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.
```

Para configurar el servicio STUN/TURN WebRTC, utilice el archivo turn-server.toml:

- **Sección [turn]:** Especifica el dominio donde se encuentra el servidor.
- **Sección [[turn.interfaces]]:** Indica las interfaces de escucha. Describe la interfaz a la que está vinculado el servidor STUN/TURN. Se pueden indicar varias interfaces.
- **Sección [turn.interfaces.transport]:** Define el tipo de transporte de la interfaz, que 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, si tiene dos NIC, A y B, en su servidor, y la dirección IP de la NIC A es 192.168.1.2 y la 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. Enlazar a 0.0.0.0 significa que escucha en todas las interfaces 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, si su tarjeta de red A se comunica con el exterior, los otros clientes verán su dirección LAN (es decir, 192.168.1.2). Sin embargo, en la realidad, la topología de red donde está desplegado el servidor podría tener otra IP pública, como 1.1.1.1, que es la dirección IP vista por los demás clientes. La razón por la que se necesitan bind y external es que, para el protocolo STUN, el servidor necesita informar su propia dirección IP externa, permitiendo así que el cliente STUN se conecte a la dirección especificada mediante la IP informada por el servidor.
- **Sección [api.bind]:** Escucha de la API para consultas, por ejemplo: http://127.0.0.1:3000/info.
- **Sección [log.level]:** Nivel de registro (log). Valores válidos: error, warn, info, debug, trace.
- **Sección [auth]:** Par de usuario y contraseña para acceder al servidor.

2. Inicio del Servicio

Inicie el servicio del STUN Server (Aranda Turn Stun WebRTC Server) para que los cambios en la configuración surtan

efecto.

3. Configuración del Firewall

Abra el puerto o los puertos configurados en el paso 1 en las reglas de entrada del firewall local y en los controladores de red presentes en la infraestructura del cliente, para los protocolos **TCP** y **UDP**. Este paso es esencial para permitir el tráfico a través del nuevo puerto y asegurar que el servidor STUN pueda recibir conexiones entrantes en el puerto configurado.

En las estaciones de trabajo (Agente ARC) y en los equipos especialistas (Agente especialista), deben permitir la salida por los puertos que se configuren.

Adicionalmente, si requiere que opere como TURN WebRTC, debe abrir el rango de puertos 49152-65535 para el protocolo **UDP**.

Ejemplo de configuración servicio STUN/TURN y escenarios

↩ Servidor Turn Externo

Ejemplo de configuración servicio STUN/TURN y Escenarios

↩ Servidor TURN Externo

Para que el servidor funcione tanto para dispositivos dentro como fuera de la red siga los siguientes pasos:

1. Configurar el realm

Cambie el valor de realm al dominio público o dirección IP externa de su servidor. Esto es importante para autenticar correctamente las solicitudes externas.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:

```
realm = "1.2.3.4"
```

2. Configurar bind

La sección bind asegura que el servidor STUN/TURN escuche en la IP privada para las conexiones dentro de la red local.

Si la dirección privada de su servidor es 192.168.1.25, configúrelo como:

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

Si requiere que el servicio STUN/TURN escuche en todas las interfaces al mismo tiempo, configúrelo como:

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

Estas configuraciones sólo son requeridas para [[turn.interfaces]].

3. Configurar external

La sección external es donde se define la IP pública del servidor para que los equipos externos puedan comunicarse correctamente con el servidor STUN/TURN.

Si la dirección pública de su servidor es 1.2.3.4, configúrelo como:

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

4. Autenticación

La sección [auth] está configurada con usuarios estáticos:

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

Esto permite conexiones autenticadas con las credenciales estáticas user1:test y user2:test. Asegúrese de usar credenciales más seguras si planea exponer este servicio a dispositivos externos.

Los demás secciones de pueden dejar por defecto.

Al realizar la parametrización en el archivo **turn-server.toml**, este deberá observarse de la siguiente forma:

```
[turn]

realm = "1.2.3.4" # IP pública del servidor

[[turn.interfaces]]
transport = "udp"
bind = "192.168.1.25:3478" # La IP privada del servidor en la red local o 0.0.0.0 cuando se desea escuchar todas las interfaces
external = "1.1.1.1:3478" # La IP pública del servidor visible desde el exterior

[[turn.interfaces]]
transport = "tcp"
bind = "192.168.1.25:3478" # La IP privada del servidor en la red local o 0.0.0.0 cuando se desea escuchar todas las interfaces
external = "1.1.1.1:3478" # La IP pública del servidor visible desde el exterior

[api]
bind = "127.0.0.1:3000"

[log]
level = "info"

[auth]
# Credenciales para autenticación TURN/STUN
user1 = "test"
user2 = "test"
```

Cada vez que realice una modificación al archivo **turn-server.toml**, reinicie el servicio **Aranda Turn Stun WebRTC Server** para que los cambios surtan efecto.

Escenarios

A continuación, se describen los siguientes escenarios y el resultado de acuerdo con la configuración del ejemplo.

Escenario	Especialista	Estado en Red	Agente ARC	Estado en Red	Resultado
1	Solo puede acceder al servidor TURN/STUN usando la IP pública	**Externo**	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
2	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
3	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	Puede acceder al servidor TURN/STUN usando la IP pública.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP pública.
4	Solo puede acceder al servidor TURN/STUN usando la IP privada.	**Interno**	Solo puede acceder al servidor TURN/STUN usando la IP privada.	**Interno**	El Especialista y el Agente ARC pueden establecer comunicación consumiendo el servidor TURN/STUN por la IP privada.
5	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido a la red interna (IP privada).	**Interno**	El Especialista y el Agente ARC no pueden establecer comunicación debido a un problema de conectividad entre redes (exterior e interior).
6	Solo puede acceder al servidor TURN/STUN usando la IP pública.	**Externo**	No puede usar la IP pública para conectarse al servidor TURN/STUN, ya que su acceso está restringido.	**Externo**	El Especialista y el Agente ARC no pueden establecer comunicación debido a un problema de conectividad entre redes.

⚠ **Nota:**

- Para cubrir los escenarios 1, 2 y 3, configure en el sitio web de AMD el servidor Turn Externo de la siguiente manera:
  Nombre: nombre de la configuración.
  URL: turn.1.2.3.4:3478 (1.2.3.4 hace referencia a la IP pública del servidor).
  Usuario: user1.
  Contraseña: test.

⚠ **Notas:**

- Para cubrir el escenario (4), configure en el sitio web de ADM el servidor Turn Externo de la siguiente

manera:
Nombre: nombre de la configuración.
URL: turn.192.168.1.25:3478 (192.168.1.25 hace referencia a la IP privada del servidor).
Usuario: user1.
Contraseña: test.

- Si en el archivo **turn-server.toml** se configuró 0.0.0.0 en el parámetro bind, se debe realizar la configuración en el sitio como se indicó anteriormente.

↩ Servidor TURN Externo