
Aranda Device Management

\n## Exclusiones Requeridas en el Antivirus

title: Exclusiones Requeridas en el Antivirus chapter: "integracion_absolute" —

Exclusiones Requeridas en el Antivirus

Los programas antivirus no deben bloquear las rutas del sistema del documento adjunto. VerDocumentación Oficial Absolute

> ⚐ **Nota:** Tener en cuenta que el antivirus no siempre los va a detectar, pero en caso que genere algún tipo de alerta tener en cuenta el listado adjunto.

\n## Integración Absolute

title: Integración Absolute chapter: "absolute" —

Permite instalar, activar y eliminar la persistencia de los dispositivos registrados en la consola ADM, con el fin de mantener el reporte de los equipos sin importar si el agente es eliminado con un usuario que no sea administrador, o si se formatea la máquina.

}

> ⚐ **Nota:** Los sistemas operativos compatibles con esta funcionalidad son Windows 10 y Windows 11.

Para activar o desactivar la funcionalidad de Absolute se debe configurar lo siguiente desde la Base de datos:

Activar:

```
Update afw_settings set sett_value = 'true'
where sett_key = 'EnableAbsolutePersistence'
```

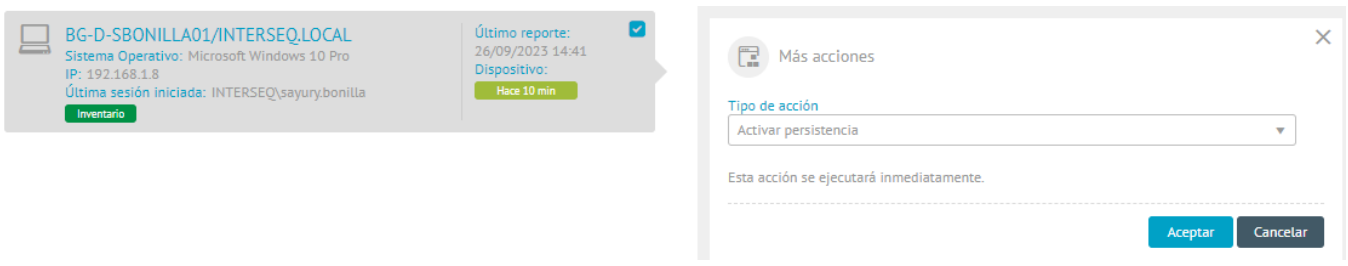
Desactivar:

```
Update afw_settings set sett_value = 'false'
where sett_key = 'EnableAbsolutePersistence'
```

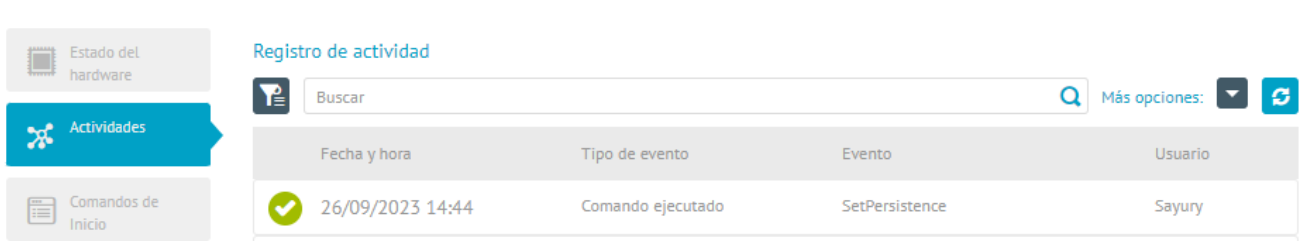
Activar Persistencia:

1. Ingrese a la consola de Inicio de ADM, en la sección**Inventario** del menú encabezado, seleccione la opción**Dispositivos**. En la vista de información podrá visualizar el listado de dispositivos. Seleccione uno o más dispositivos a los que requiere habilitar la persistencia.

2. En la vista detalle del(los) dispositivo(s), en la sección Acciones, seleccione la opción**Más Acciones** y en la ventana que se habilita, en el campo Tipo de acción, elija la opción **Activar Persistencia** y haga clic en **Aceptar**.

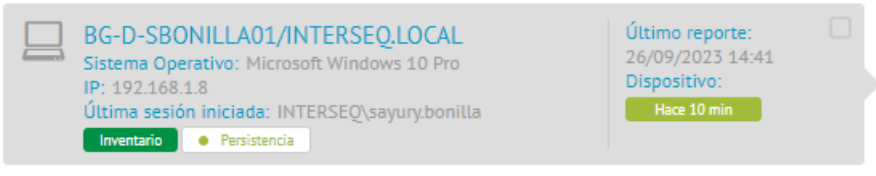


1. Después de activada la persistencia, en la vista detalle del dispositivo, seleccione el botón**Ver Detalles**. En la ventana que se habilita seleccione la pestaña General y en la opción Actividades del Menú se verifica el envío de la petición.



Una vez el proceso de activación de la persistencia de Absolute se ha completado de manera correcta en el dispositivo, se visualizará la siguiente etiqueta que indica que la persistencia está habilitada.

> ⚐ **Nota:** La aplicación de la persistencia de Absolute puede tardar máximo 1 hora.

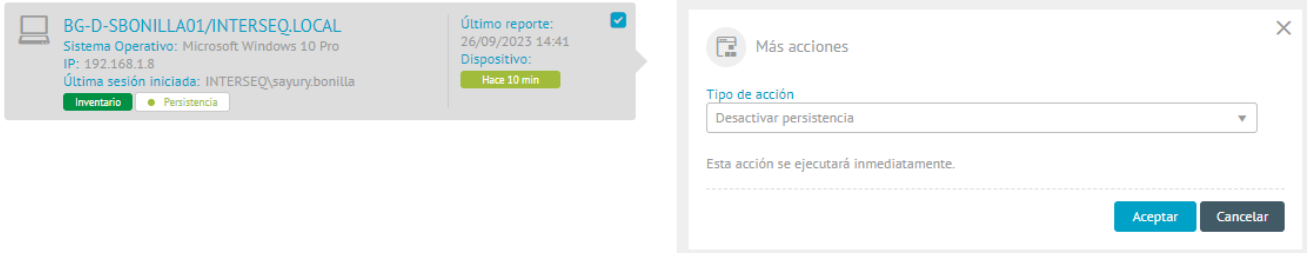


> ⚐ **Nota:** Después de un período de tiempo, la llave de registro de Absolute desaparece. En ADM se utiliza esta llave para verificar el estado de la persistencia. Cada vez que se reinicia el servicio del agente, se verifica el estado de la persistencia, lo que puede hacer que en la consola parezca que no hay persistencia, pero en realidad el agente sigue siendo persistente.

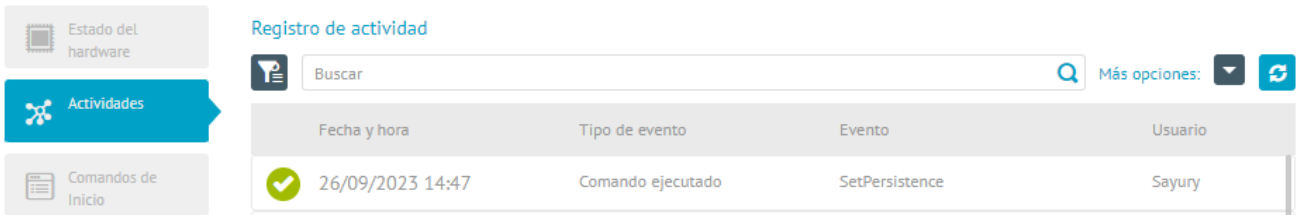
Desactivar Persistencia:

1. Ingrese a la consola de Inicio de ADM, en la sección**Inventario** del menú encabezado, seleccione la opción**Dispositivos**. En la vista de información podrá visualizar el listado de dispositivos. Seleccione uno o más dispositivos a los que requiere deshabilitar la persistencia.

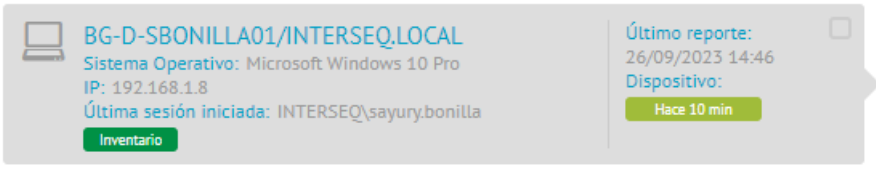
2. En la vista detalle del(los) dispositivo(s), en la sección Acciones, seleccione la opción**Más Acciones** y en la ventana que se habilita, en el campo Tipo de acción, elija la opción **Desactivar Persistencia** y haga clic en **Aceptar**.



3. Después de desactivada la persistencia, en la vista detalle del dispositivo, seleccione el botón **Ver Detalles**. En la ventana que se habilita seleccione la pestaña General y en la opción Actividades del Menú se verifica el envío de la petición.



La aplicación de la persistencia en Absolute puede tardar un máximo de 45 minutos. Después de que la persistencia se desactiva en Absolute, se deshabilita la etiqueta de persistencia



⚐ **Nota:** En el archivo exportado (Excel o PDF), los dispositivos que tienen activa la persistencia aparecerán con el valor **true** en la columna **Is persistence**.

Reporte Persistencia:

1. Para generar los reportes de la persistencia ingrese a la consola de Inicio de ADM, en la sección **Inventario** del menú encabezado, seleccione la opción **Dispositivos**.
2. En la vista de información en el menú **Mas Opciones** seleccione **Excel** o **PDF** para exportar el archivo correspondiente.

   ⚐ **Nota:** En el archivo exportado (Excel o PDF), los dispositivos que tienen activa la persistencia aparecerán con el valor **true** en la columna **Is persistence**.

- Exportar a Excel:

Description	Discovered	Has Conflicts	Is persistence	Last inventory	Last Update	Responsible User Email	Responsible User Name	Status	User	Vpro	Agent profile	Agent Version	Guid	Hardware hash	Manufacturer	Model	OS	Serial	Device name	Domain	Ip Address	Type
	9/13/2023 3:33:47 PM	False	True	9/13/2023 3:46:28 PM	9/14/2023 10:17:31 AM			InventoryUpdated	LAPTOP-R1KFNOA1\ARC	True	DEFAULT	9.18.2308.302	{45BE224D-1267a01411fb88393e		Lenovo	20T0002DUS	Microsoft Wi	PF2BB0XJ	LAPTOP-R1KFNOA1		192.168.0.9	Laptop
	9/13/2023 9:23:52 AM	False	True	9/14/2023 9:30:19 AM	9/14/2023 10:16:27 AM			InventoryUpdated	INTERSEQ\nidia.alejo	False	DEFAULT	9.18.2308.302	{5A54654B-1db7d40bce3699d5f4		Dell Inc.	Latitude 3420	Microsoft Wi	G32NGL3	BG-D-NALEJO01	INTERSEQ.LOCAL	192.168.1.17	Laptop
	9/13/2023 6:20:04 PM	False	False	9/14/2023 8:22:15 AM	9/14/2023 10:14:48 AM			InventoryUpdated		False	DEFAULT	9.18.2309.1302	{FF481F7E-A2f511881697702f598		Microsoft Corporation	Virtual Machine	Microsoft Wi	0000-0004-2	Wna-windows10		10.0.0.10	Desktop
	9/13/2023 2:21:25 PM	False	False	9/14/2023 8:05:04 AM	9/14/2023 10:14:21 AM			InventoryUpdated		False	DEFAULT	9.18.2308.302	{47DECA7D-1a379fe59b9571025		Microsoft Corporation	Virtual Machine	Microsoft Wi	0000-0006-9	ra-adm-ser2019		10.0.0.7	Server
	9/14/2023 9:46:52 AM	False	False	9/14/2023 9:47:37 AM	9/14/2023 10:14:20 AM			InventoryUpdated		False	DEFAULT	9.18.2308.302	{0BF0E185-9a42326c95954c504d		Microsoft Corporation	Virtual Machine	Microsoft Wi	0000-0003-4	win10-apa		10.0.0.6	Desktop
	9/13/2023 3:53:58 PM	False	False	9/14/2023 10:04:17 AM	9/14/2023 10:14:02 AM			InventoryUpdated	DESKTOP-LNA9N7T\sangie.pinzon	False	DEFAULT	9.17.2305.3001	{D26F446C-7759b75172943c286		HP	HP ProBook 440 G3	Microsoft Wi	5CD70203DC	DESKTOP-LNA9N7T		192.168.0.105	Laptop
	9/13/2023 2:25:29 PM	False	False	9/14/2023 8:26:20 AM	9/14/2023 10:13:58 AM	Sayury@gmail.com	Sayury	InventoryUpdated	INTERSEQ\sayury.bonilla	False	PRUEBA	9.18.2308.302	{70037E0C-124596ecd89191Dcaa		Dell Inc.	Latitude 3420	Microsoft Wi	3VWW4N63	BG-D-SBONILLA01	INTERSEQ.LOCAL	192.168.0.6	Laptop
	9/13/2023 5:33:39 PM	False	False	9/14/2023 5:45:46 PM	9/14/2023 10:13:56 AM			InventoryUpdated	INTERSEQ.LOCAL\jose.vargas	False	DEFAULT	9.18.2309.1302	{5D19F3F7-C8c65e9028d9224964		Hewlett-Packard	HP EliteBook 820 G1	Microsoft Wi	5CG4501ZY0	BG-D-SACRISTAN1	INTERSEQ.LOCAL	192.168.1.111	Laptop
	9/13/2023 4:54:54 PM	False	False	9/13/2023 4:59:58 PM	9/13/2023 6:39:22 PM			InventoryUpdated	INTERSEQ\juan.sacristan	True	DEFAULT	9.19.2304.129	{88861256-E80e0f8b80e860688		Dell Inc.	Latitude 7420	Microsoft Wi	2YNP8C3	BG-D-VPR001	INTERSEQ.LOCAL	192.168.10.10	Laptop

- Exportar a PDF:

Description	Discovered	Has Conflicts	Is persistence	Last inventory
	9/13/2023 9:23:52 AM	False	True	9/14/2023 9:30:19 AM
	9/13/2023 6:20:04 PM	False	False	9/14/2023 8:22:15 AM
	9/13/2023 2:21:25 PM	False	False	9/14/2023 8:05:04 AM
	9/14/2023 9:46:52 AM	False	False	9/14/2023 9:47:37 AM
	9/13/2023 3:53:58 PM	False	False	9/14/2023 10:04:17 AM
	9/13/2023 2:25:29 PM	False	False	9/14/2023 8:26:20 AM
	9/13/2023 5:33:39 PM	False	False	9/14/2023 5:45:46 PM
	9/13/2023 3:33:47 PM	False	True	9/14/2023 3:46:28 PM
	9/13/2023 4:54:54 PM	False	False	9/14/2023 4:59:58 PM

Last Update	Responsible User Email	Responsible User Name	Status	User
9/14/2023 10:21:27 AM			InventoryUpdated	INTERSEQ\nidia.alejo
9/14/2023 10:19:49 AM			InventoryUpdated	
9/14/2023 10:19:21 AM			InventoryUpdated	
9/14/2023 10:19:20 AM			InventoryUpdated	
9/14/2023 10:19:02 AM			InventoryUpdated	DESKTOP-LNA9N7T\sangie.pinzon
9/14/2023 10:18:59 AM	Sayury@gmail.com	Sayury	InventoryUpdated	INTERSEQ\sayury.bonilla
9/14/2023 10:18:56 AM			InventoryUpdated	INTERSEQ.LOCAL\jose.vargas
9/14/2023 10:17:31 AM			InventoryUpdated	LAPTOP-R1KFNOA1\ARC
9/13/2023 6:39:22 PM			InventoryUpdated	INTERSEQ\juan.sacristan

Vpro	Agent profile	Agent Version	Guid	Hardware hash
False	DEFAULT	9.18.2308.302	{5A54654B-F4EF-4E00-8295-DD7494817ACA}	db7d40bce3699d5f40456d12a7902c45
False	DEFAULT	9.18.2309.1302	{FF481F7E-AA0B-4A03-AF06-05BE82448C34}	2f511881697702f598889d3ea0ddc2fc
False	DEFAULT	9.18.2308.302	{47DECA7D-1D9B-49D1-A72C-0000EE223B7F}	8a379fe59b9571025ee073ba3977e6a1
False	DEFAULT	9.18.2308.302	{0BF0E185-9664-4AD9-A8CD-4CEE24F21A13}	a42326c95954c504d1c93ec3863f5409
False	DEFAULT	9.17.2305.3001	{D26F446C-3B49-4DA7-B066-CF99EA30A2BF}	7759b75172943c286cfb42a8b85b43c3

\n## Puertos utilizados por la aplicación

title: Puertos utilizados por la aplicación chapter: "integracion_absolute" —

En el centro de soporte de Absolute se listan los sitios y puertos utilizados para la comunicación de Aranda Device Management (ADM), para la integración con Absolute.

⚐ **Nota:** Los puertos son de salida, el antivirus no debe bloquear la salida a internet para los sitios web, Ip y puertos mencionados en el listado.

title: Puertos utilizados por la aplicación chapter: "integracion_absolute" —

Puertos utilizados por la aplicación

En el centro de soporte de Absolute se listan los sitios y puertos utilizados para la comunicación de Aranda Device Management (ADM), para la integración con

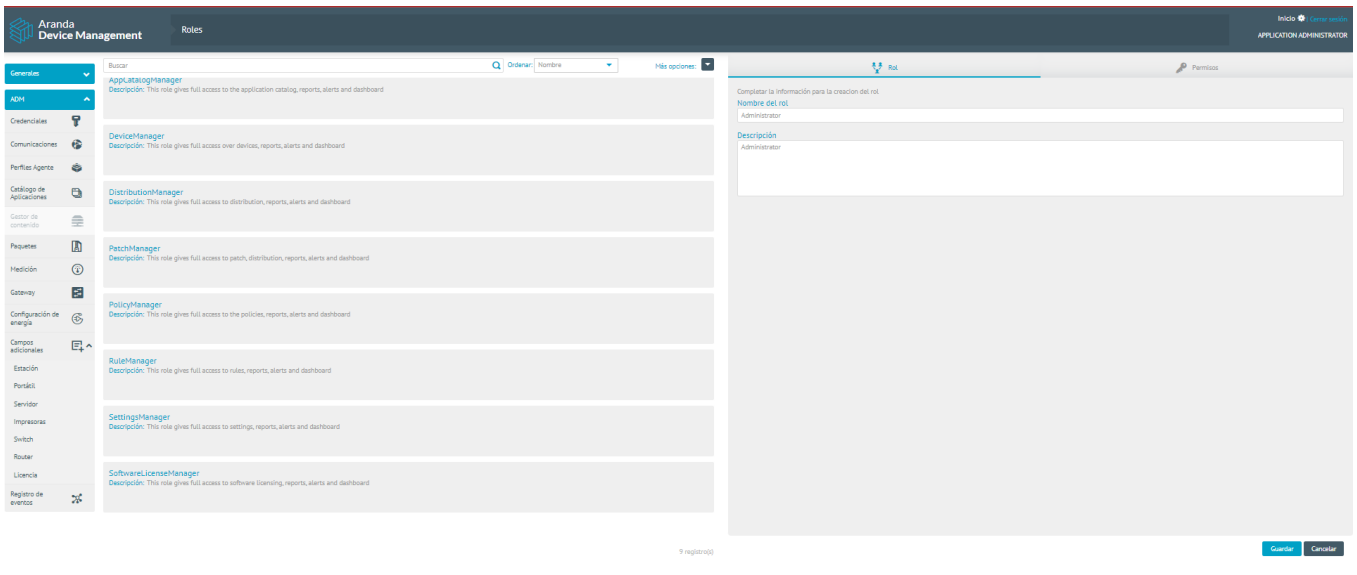
Absolute.

> ⚐ **Nota:** Los puertos son de salida, el antivirus no debe bloquear la salida a internet para los sitios web, Ip y puertos mencionados en el listado.

\n## Auditoría de control remoto — title: Auditoría de control remoto chapter: “arc” —

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 ARC**



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

Auditoría de Control Remoto

\n## Instalación componente de control remoto

title: 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

\n## Instalación visor control remoto

title: Instalación visor control remoto

↩ Integración ARC

Instalacion visor control remoto

↩ Integración ARC

\n## Control remoto (ARC)

title: 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 realizando un update a la base de datos del producto de ADM

```
update AFW_SETTINGS set sett_value = 'true' WHERE sett_key='EnableARC'
```

- Relizar 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 \n## Requerimientos de Uso Aranda Remote Control — title: Requerimientos de Uso Aranda Remote Control chapter: "arc" —

\n## Tomar Control Remoto

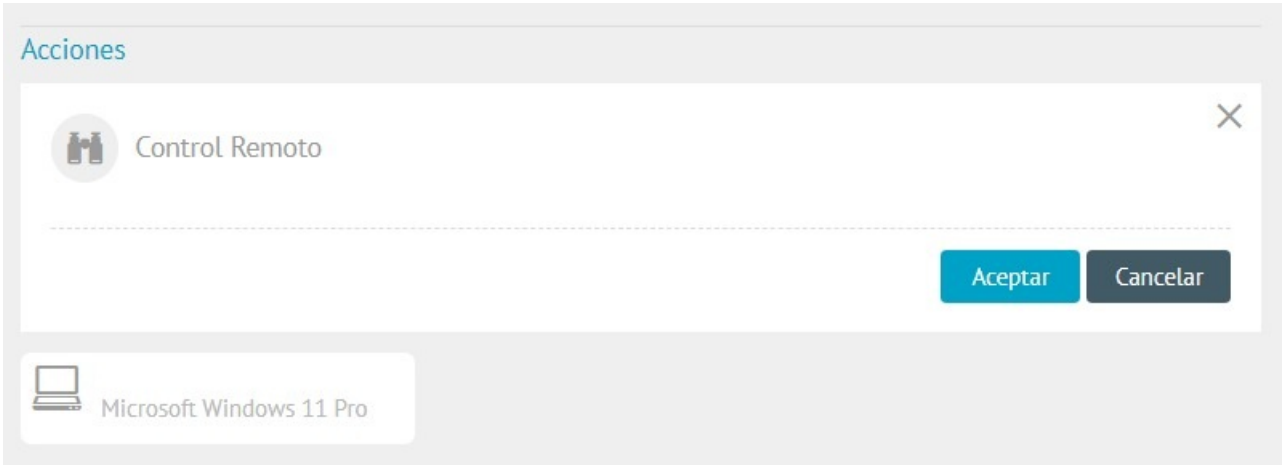
title: Tomar Control Remoto chapter: "arc" —

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

\n## Transferencias de archivos — title: Transferencias de archivos chapter: "arc" —

\n## Configuración control remoto ARC — title: 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, en la línea 6 dentro del archivœappsettings.json del sitio; la ruta por defecto es:

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

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

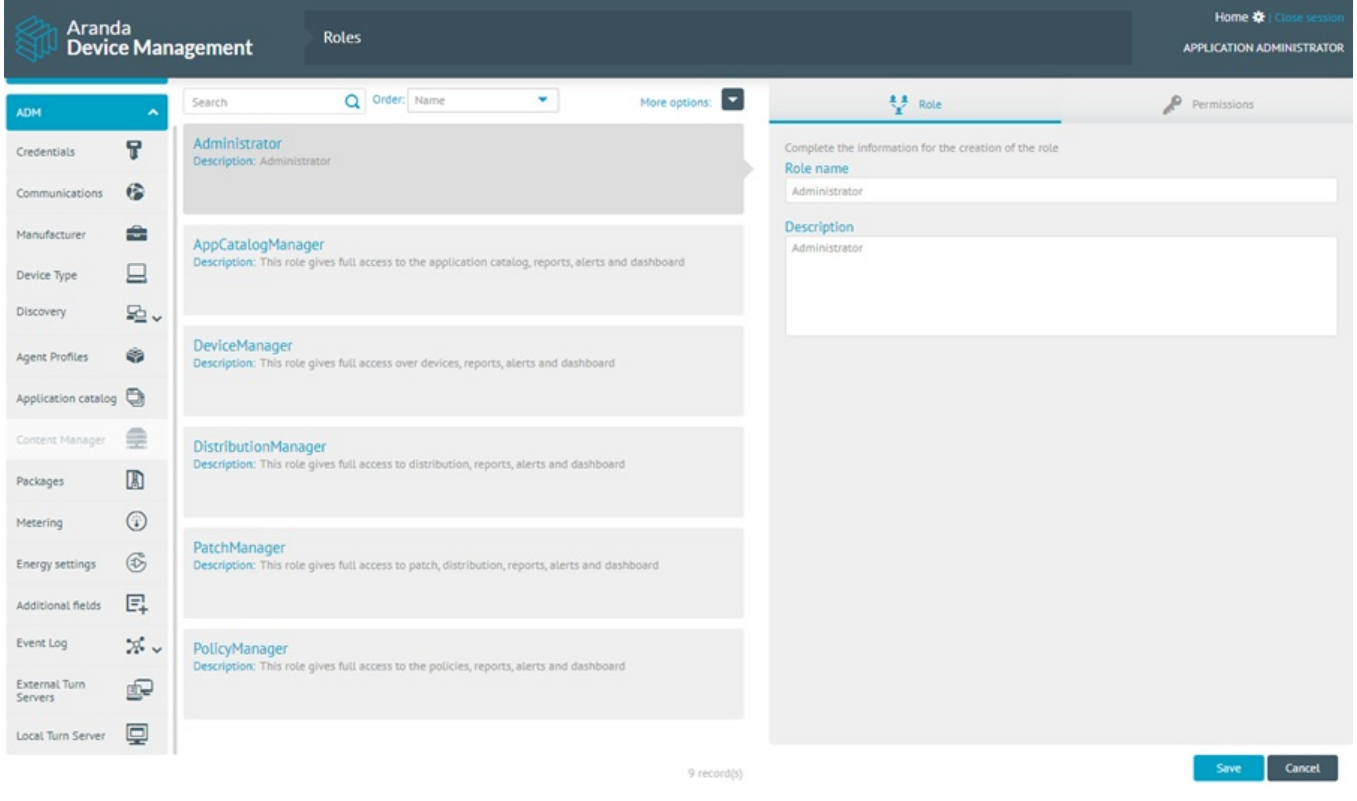
⚐ **Notas:**
- Al realizar cambios en la cadena de conexión de servidor de grabaciones reinicie el IIS para que los cambios se apliquen deforma correcta.

- 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.

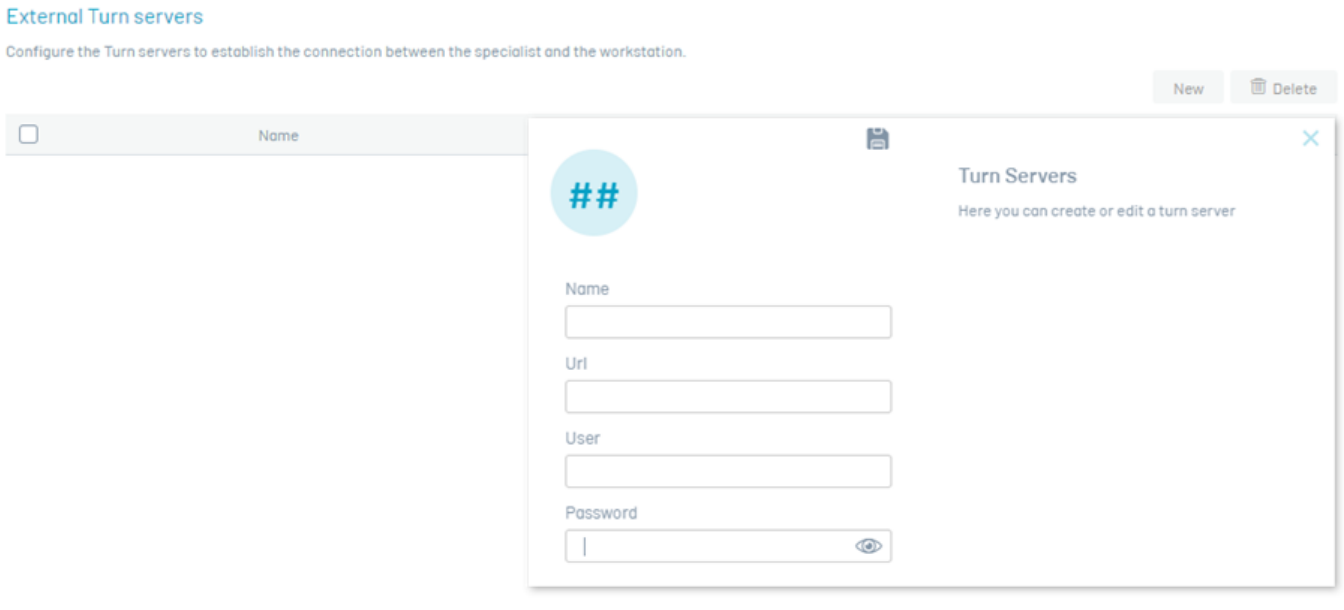
Para agregar un servidor Turn externo en la ventana de**Servidores Turn Externos**, siga estos pasos:

A. Haga clic en la opción**Nuevo**.

B. Complete los campos solicitados.

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.



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. Para esto deben permitir la salida en el firewall a estas direcciones en las estaciones de trabajo y en los equipos especialistas. También podrá instalar el servidor provisto [realizando los ajustes en el servicio Aranda Turn Stun WebRTC Server Windows Service](#) en el instalador. Es posible tener stun/turn públicos con propios instalados como se describió anteriormente.

4. Servidor Turn Local

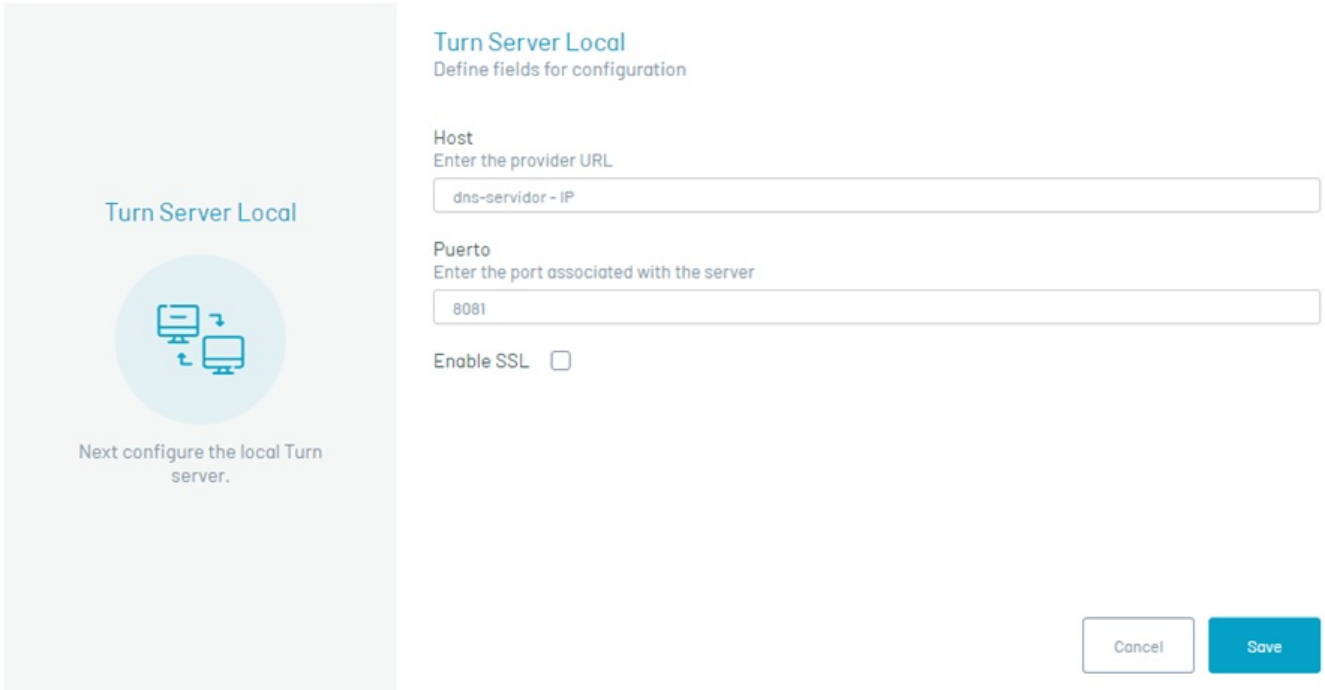
Para establecer la comunicación de toma de control remoto entre el agente especialista y el agente de la estación de trabajo, utilice un servidor Turn local que puede retransmitir el tráfico de red.

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**



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

↩ Servidor Turn Externo

Después de instalar el servicio Aranda Turn Stun WebRTC Server Windows Service, realice la configuración para que sea funcional.

1. Validación del Archivo turn-server.toml

Antes de realizar cambios, verifique que encuentre el archivo**turn-server.toml** 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 configuar 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 interfaces de escucha. Describe la interfaz a la que está vinculado el servidor turn/stun. Se pueden indicar varias interfaces

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

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

Sección [turn.interfaces.external]: Se usa para enlazar a la dirección de su NIC local, por ejemplo, tiene dos NIC A y B en su servidor, la dirección IP de la NIC A es

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

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

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

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

2. Inicio del Servicio

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

3. Configuración del Firewall

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

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

↩ Servidor Turn Externo \n## Configuración del Turn Server — title: Configuración del Turn Server —

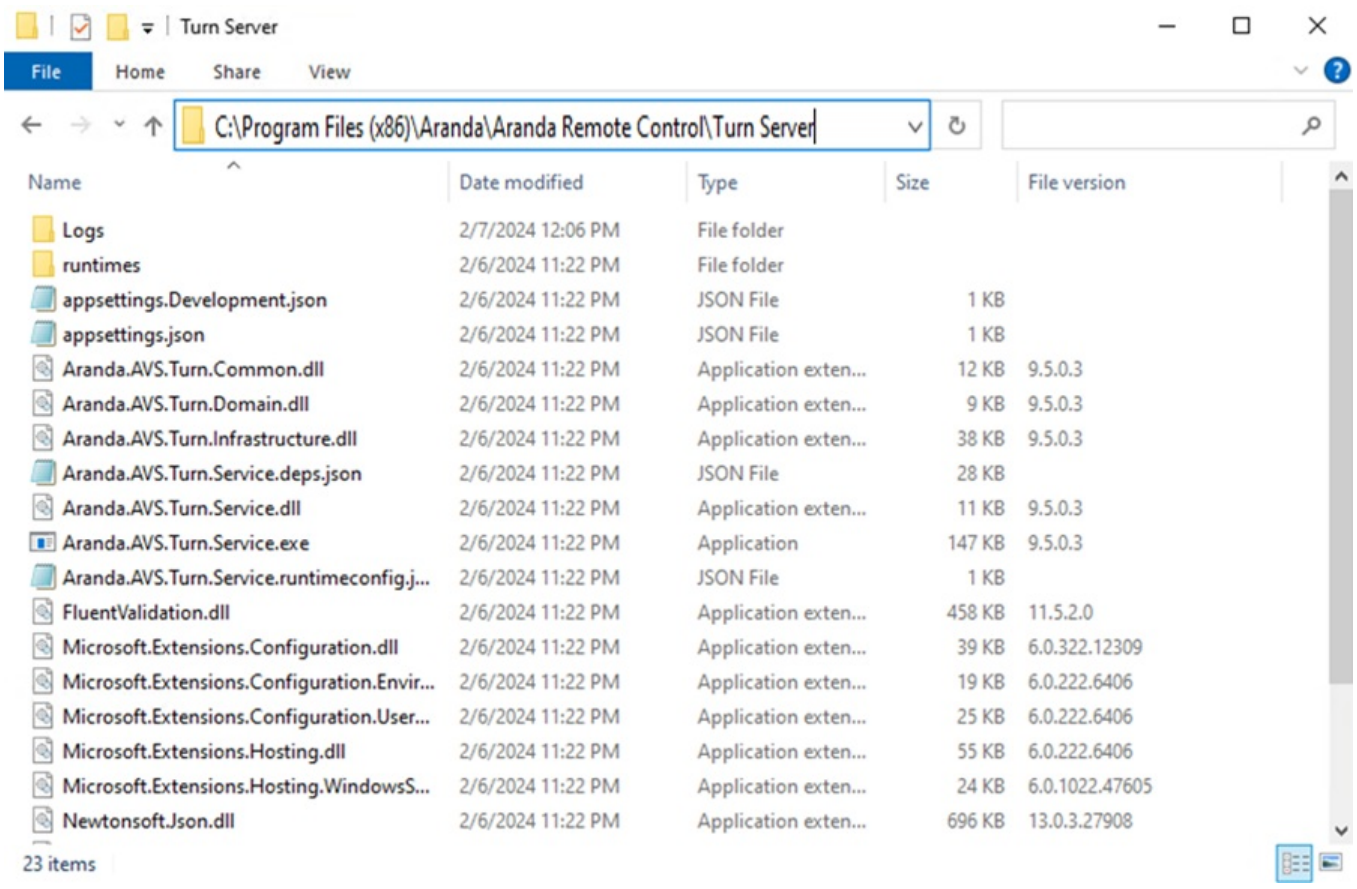
↩ Servidor Turn Local

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

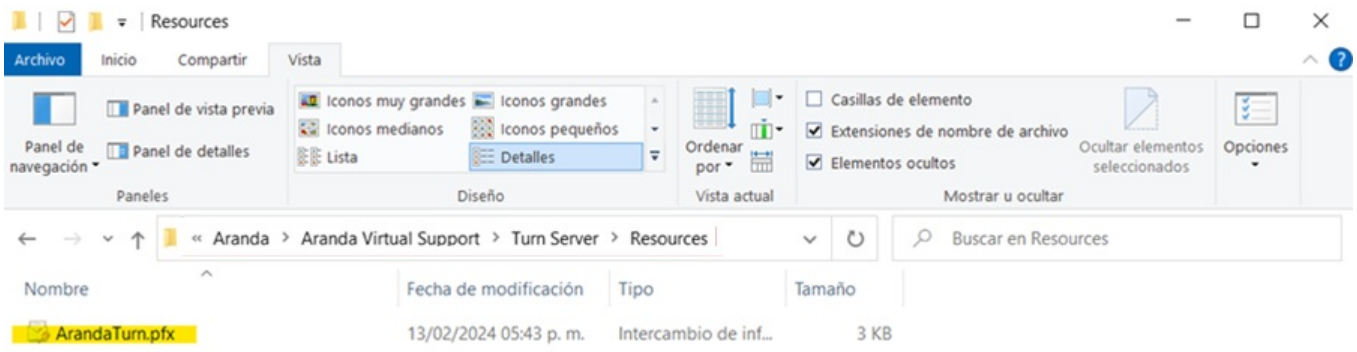
Edite el archivo *appsettings.json* y configure el puerto deseado reemplazando<puerto> por el número de puerto deseado.

```
"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– title: Integraciones ADM permalink: / –

English

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)

\n## ADM Integrations

title: ADM Integrations chapter: “” —

Español

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 facilitates the following integration solutions:

1. Internal Integrations

ADM integrates natively with our solutions:

- With **Aranda CMDB**, to automatically keep the CMDB configuration items updated with the discovery or changes detected in the 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 personalized reports.

2. External Integrations

Currently ADM integrates with the following external applications:

- Integration with **Intel® Endpoint Management Assistant (Intel® EMA)**allows remote management of computers when computers are turned off or the operating system is not responding. 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.

Who is this Manual for?

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

What is Our Documentation?

- 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**)

\n## Acceso directo con EMA

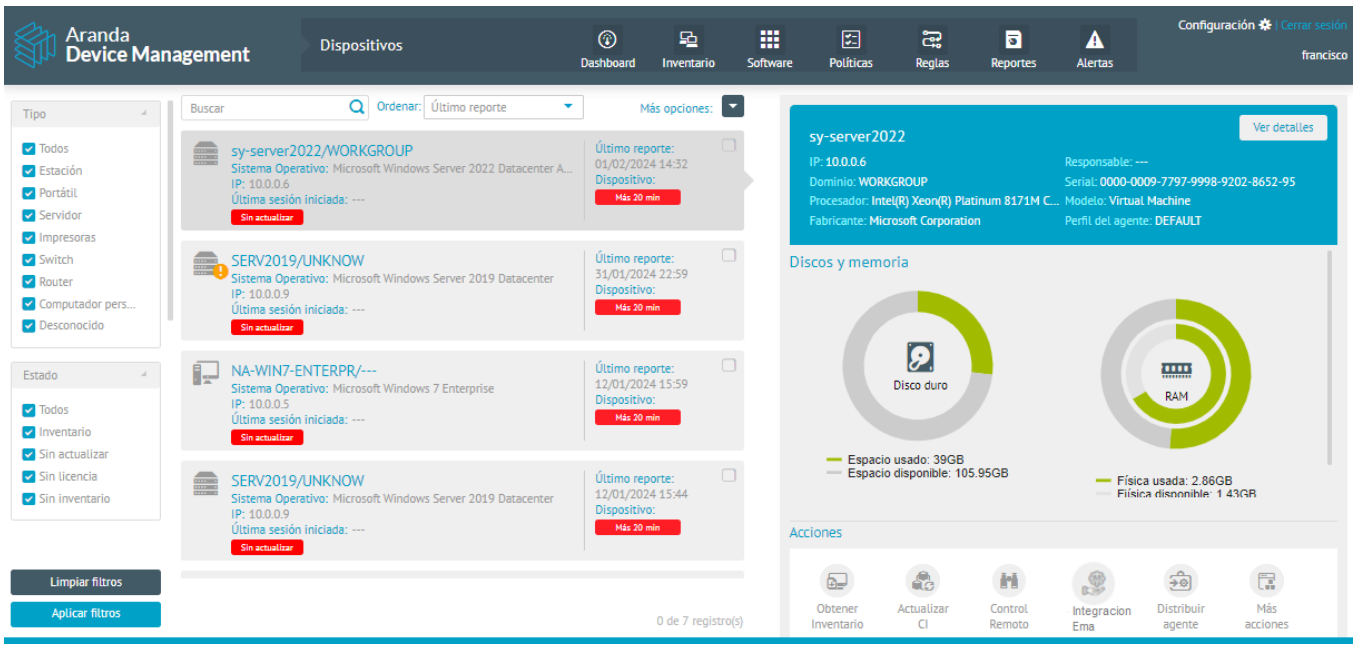
title: Acceso directo con EMA
chapter: "intel_ema" —

English

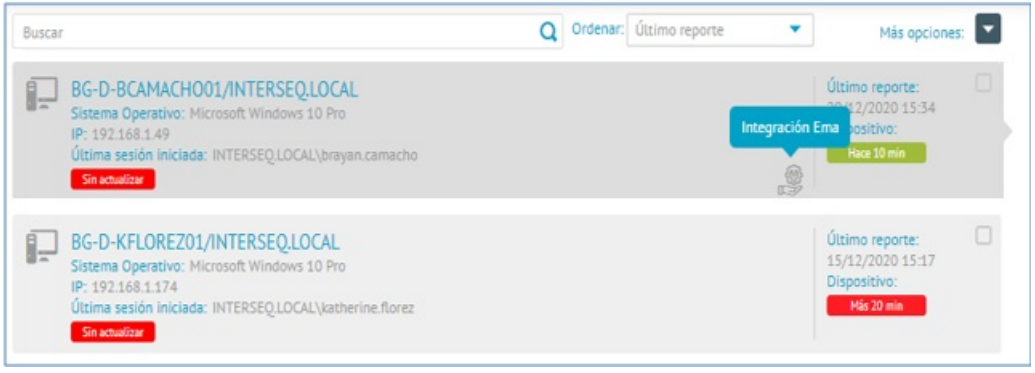
Una vez realizado todo el proceso de configuración y después de ejecutada la tarea de sincronización entre ADM e Intel EMA, el usuario podrá navegar desde el detalle de un dispositivo de ADM a la consola de EMA y hacer las operaciones que requiera.

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 d**ntegración EMA** en el listado de dispositivos.

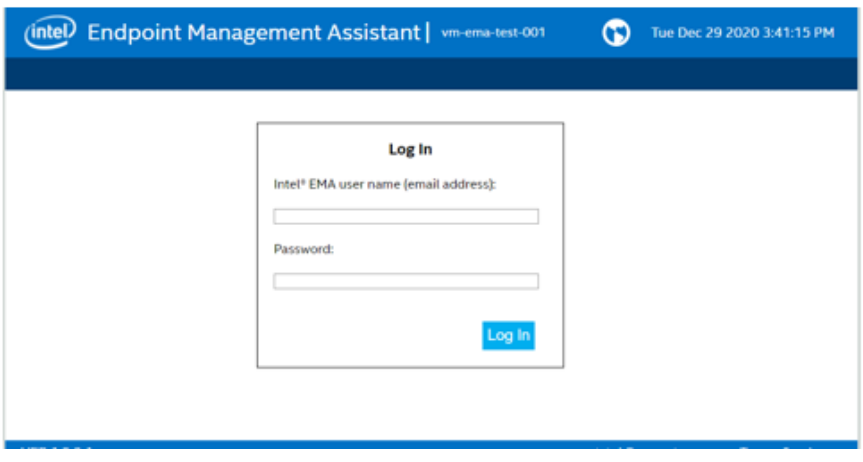


2. En la vista detalle del dispositivo integrado, seleccione la acción**Integración Ema**

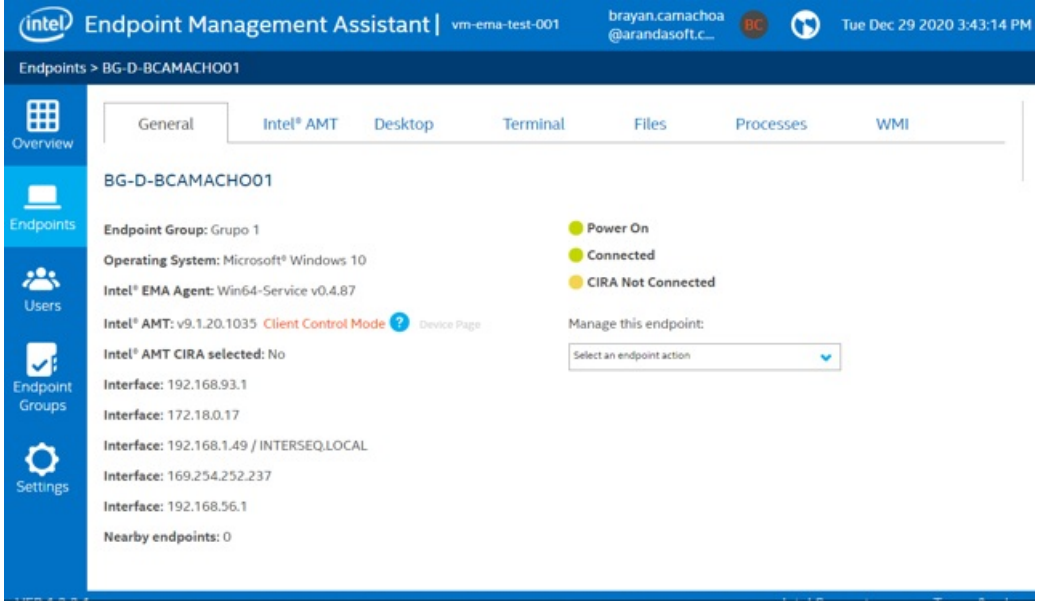
3. En la vista detalle del dispositivo se habilita la acción descrita. Haga clic en**Aceptar**, para redireccionar el proceso a la consola**Enpoint Management Asistant**

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.



\n## Beneficios

title: Beneficios chapter: “” —

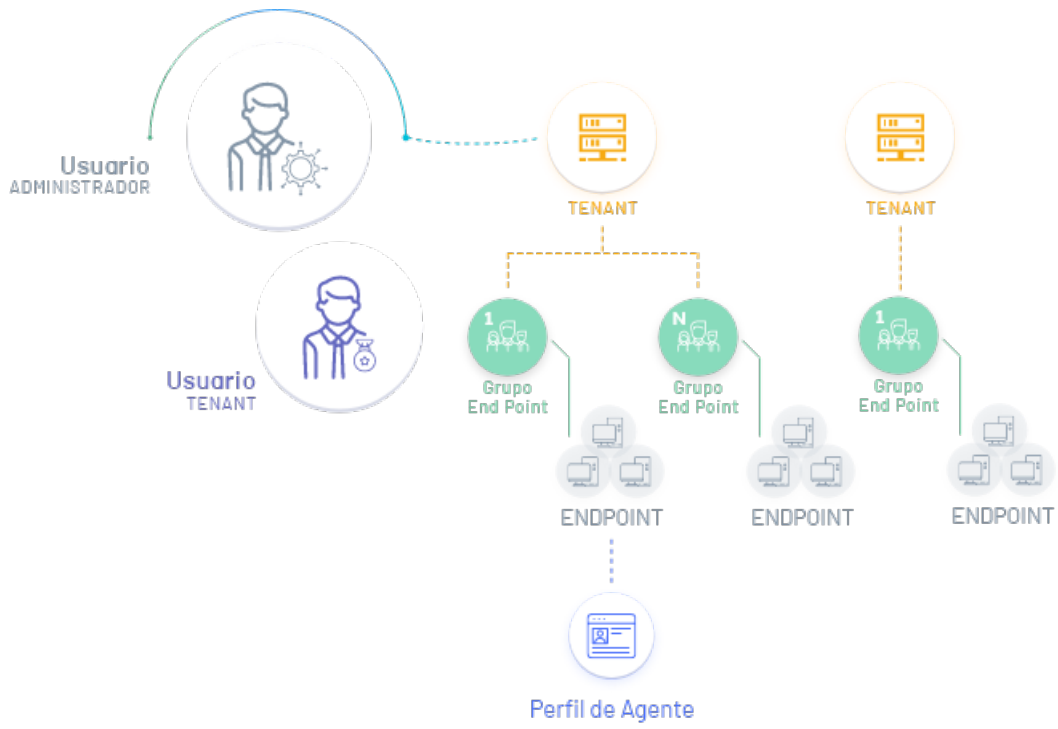
La combinación de Aranda Device Management + Intel® Endpoint Management Assistant, potencia las fortalezas de sus funcionalidades

Funcionalidad ADM	Beneficios
Gestión de Activos a través de descubrimiento y enrolamiento de dispositivos	- Conocimiento de activos. - Potenciar los recursos de TI. - Disminuir costos de soporte y gestión.

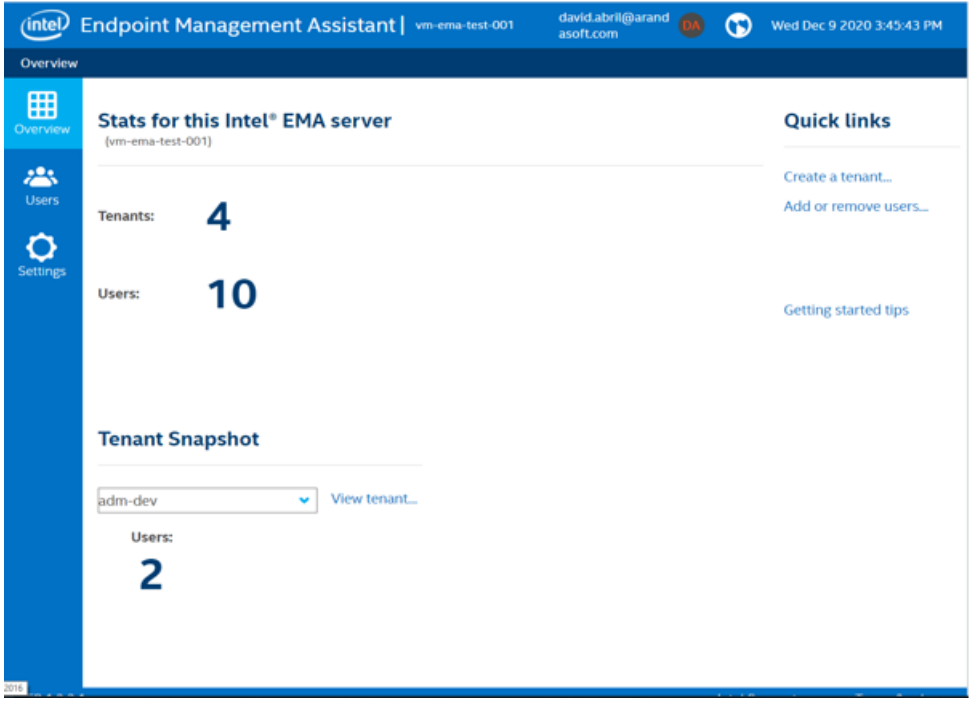
| Funcionalidad ADM + Intel EMA | Beneficios | | ——— | ——————————— | | Gestión de Distribución de Hardware y Software + Agente Intel EMA | - Fortalecer la seguridad y la administración de los dispositivos.
-Reducir costos de asistencia técnica.
- Agilizar plazos de resolución. |\n## Configuración Tenant y Grupos Endpoint — title: Configuración Tenant y Grupos Endpoint chapter: “intel_ema” —

English

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.

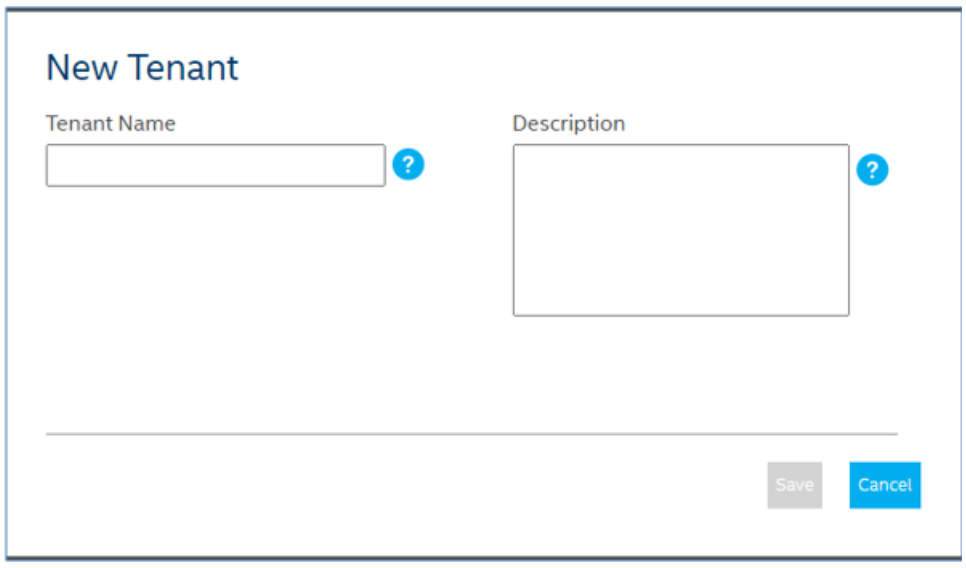


Crear Ternant

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.

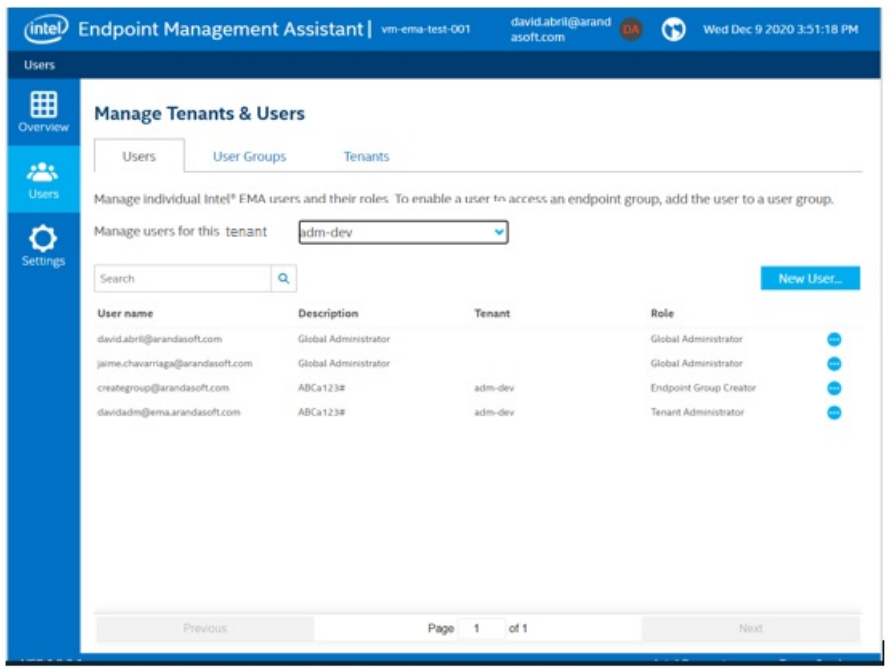
Este es el tenant que va integrar con ADM (Si va utilizar la instancia de EMA para sincronizar diferentes instancias de ADM, debe crear un tenant por cada instancia, se recomienda usar el nombre del cliente para diferenciar). }

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



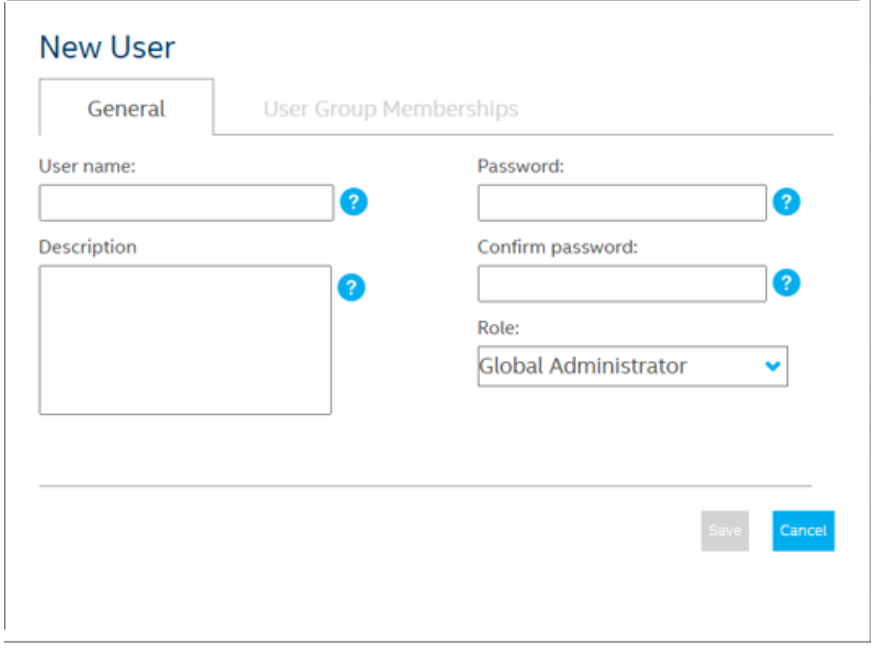
Crear Usuarios

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**.



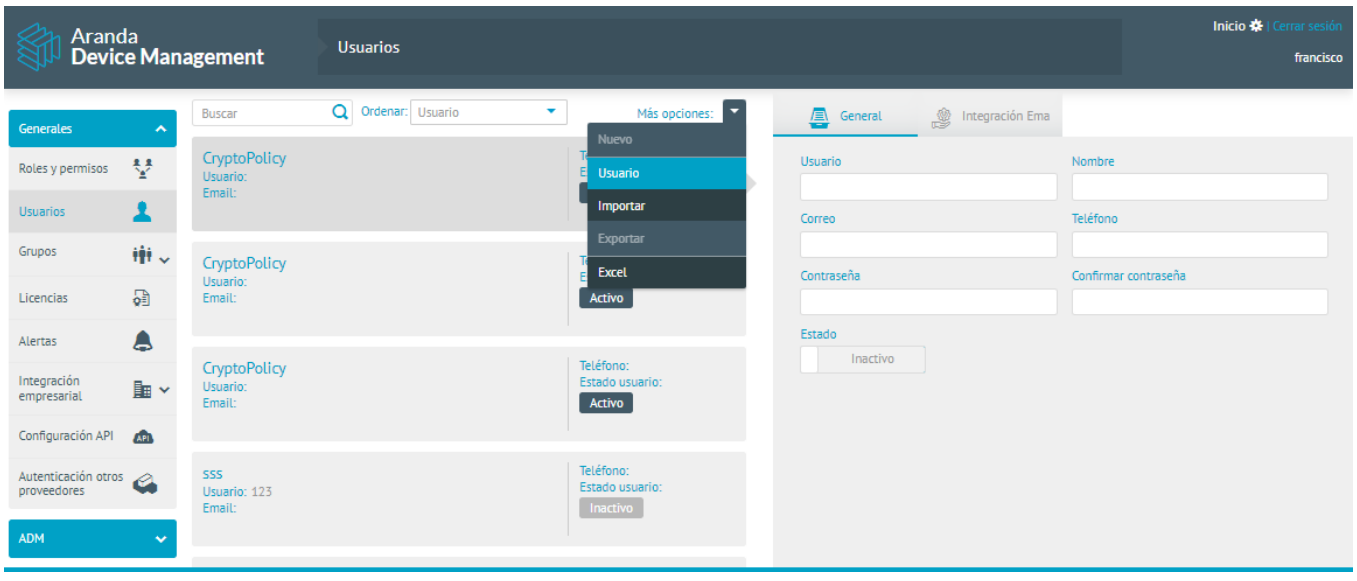
\n## Creación de Usuario Administrador de Tenant de EMA

title: Creación de Usuario Administrador de Tenant de EMA
chapter: "intel_ema" —

English

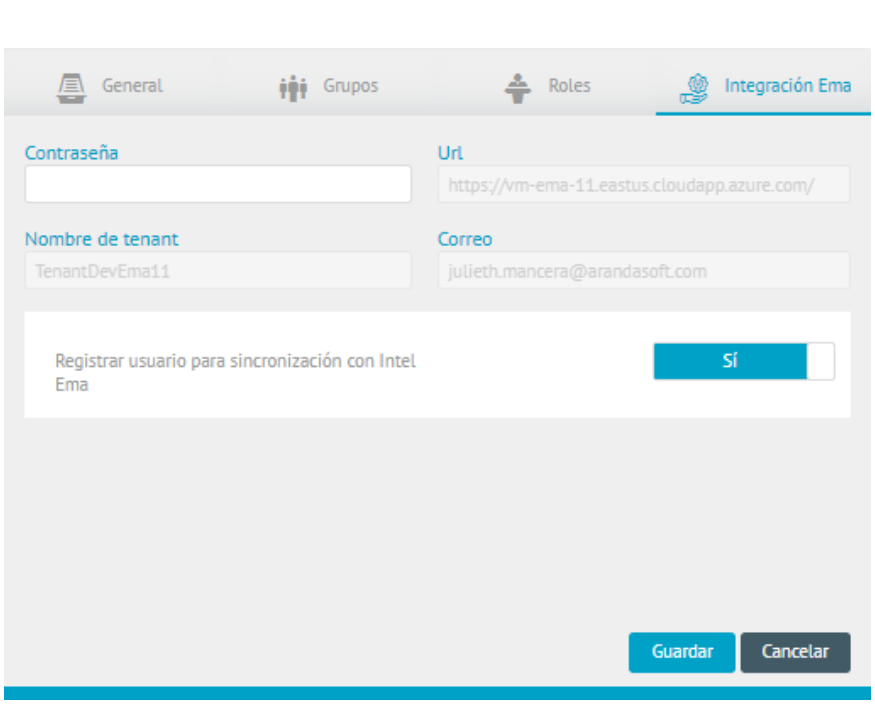
1. Para crear el usuario administrador de Tenant de Emma, ingrese a la vista de Configuración de la consola de administración de ADM, en la sección **Generales** seleccione la opción **Integración Empresarial** y **LDAP**. En la vista de información despliegue la opción **Más Opciones** y **Usuario**.

2. En la Vista detalle de Usuarios , seleccione la pestaña **General** donde podrá completar los datos generales del usuario a integrar con EMA como administrador de Tenant y definir si su estado es activo o inactivo.



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

3. En la Vista detalle de Usuarios , seleccione la pestaña **Integración Ema** e ingrese la clave del usuario y active el usuario de EMA; se puede registrar el usuario como el usuario que se va a usar para sincronizar.

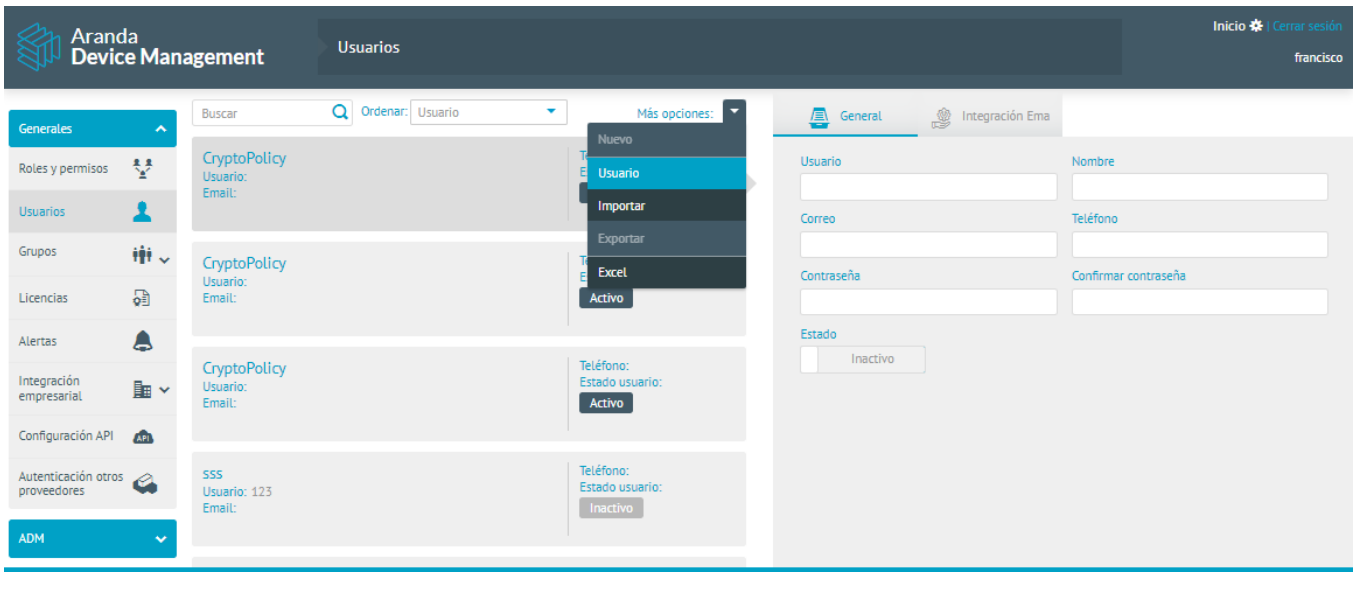


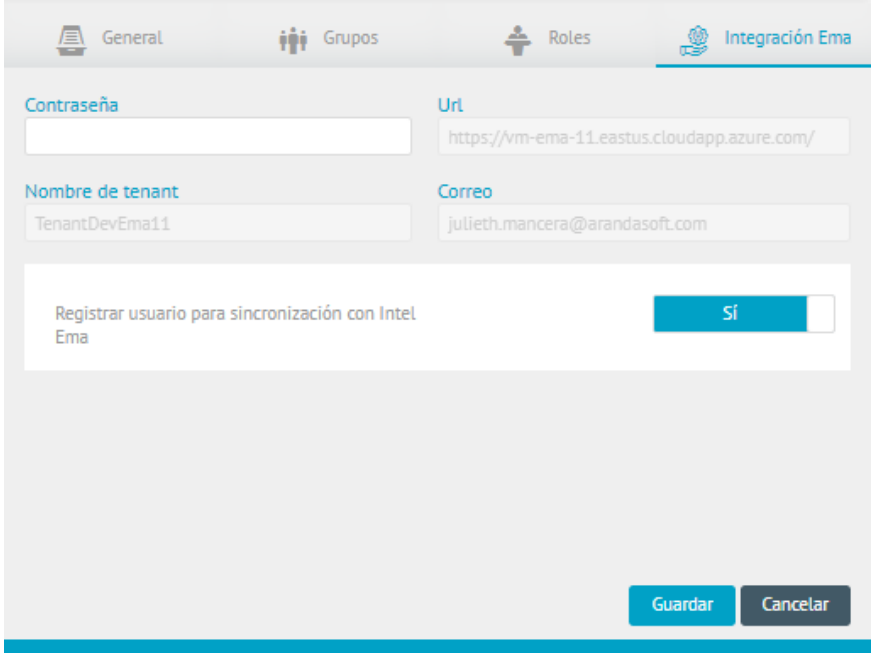
4. Al terminar de configurar la información básica del usuario, Haga clic en **Guardar** para confirmar los cambios realizados; en la Vista detalle se habilita las pestañas Grupos y Roles \n## Creation of EMA Tenant Administrator User — title: Creation of EMA Tenant Administrator User chapter: —

Español

1. To create the Emma Tenant administrator user, enter the Configuration view of the ADM administration console, in the**General** section select the**Enterprise Integration** option and **LDAP**. In the information view, display the option**More Options** and **User**.

2. In the User Detail View, select the**General** tab where you can complete the general data of the user to integrate 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 Administrator user.

3. In the User Detail View, select the**Ema Integration** tab and enter the user password and activate the EMA user; You can register the user as the user to use for synchronization.

4. When you finish configuring the basic user information, Click**Save** to confirm the changes made; In the Detail View, the Groups and Roles tabs are enabled.

\n## Direct link with EMA

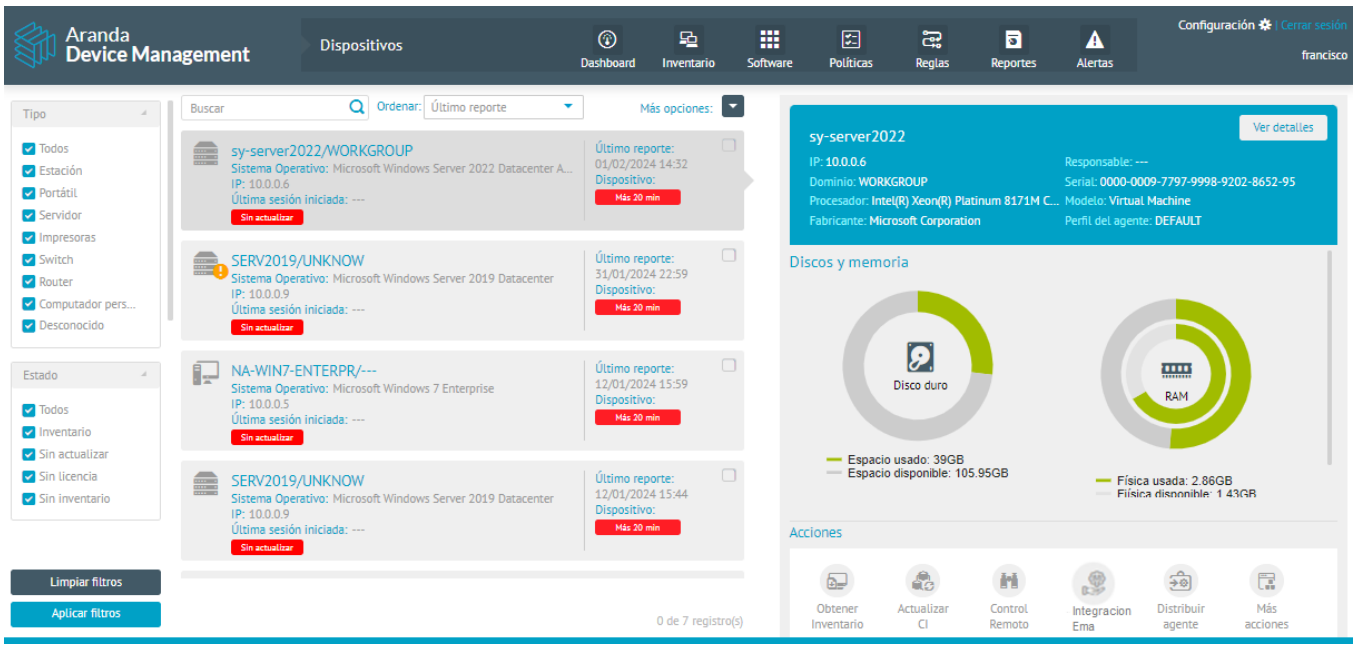
title: Direct link with EMA chapter: —

Español

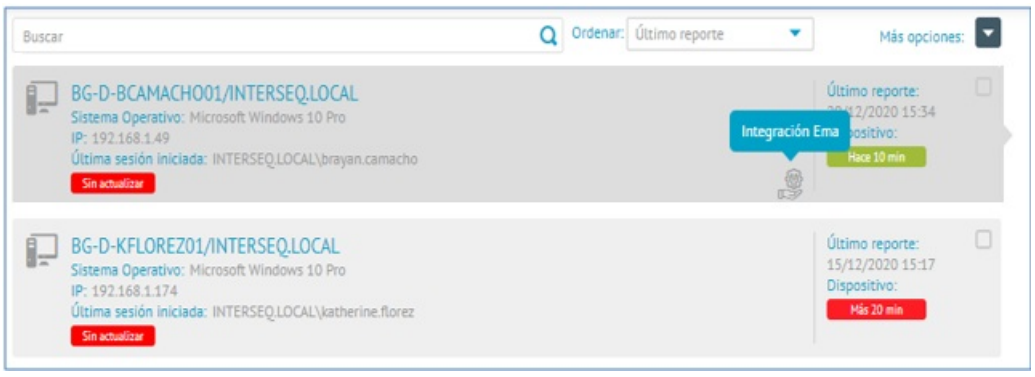
Once the entire configuration process has been completed and the synchronization task between ADM and Intel EMA has been executed, the user will be able to navigate from the details of an ADM device to the EMA console and perform the operations required.

Access from ADM

1. Enter the Home view of the ADM management console and select the**Inventory** module from the Header menu and the**Devices** option. In the information view you can view the list of inventoried devices.

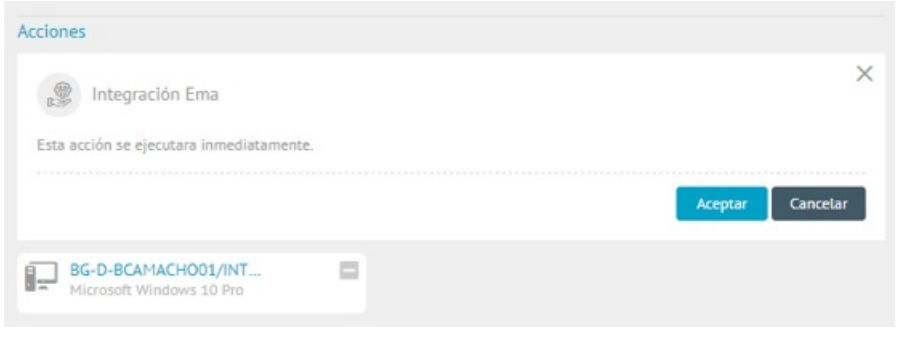


⚐ **Note:** If the device is synchronized with EMA, you will be able to see the **EMA Integration** logo in the list of devices.



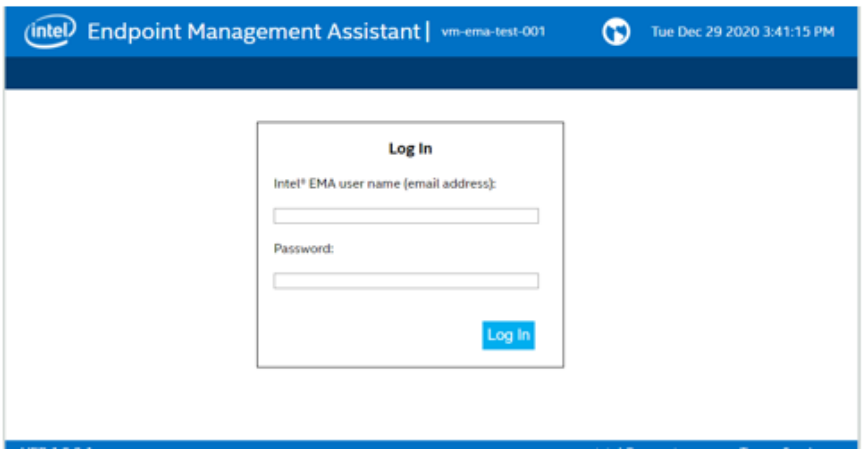
2. In the detail view of the integrated device, select the action **Ema Integration**

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

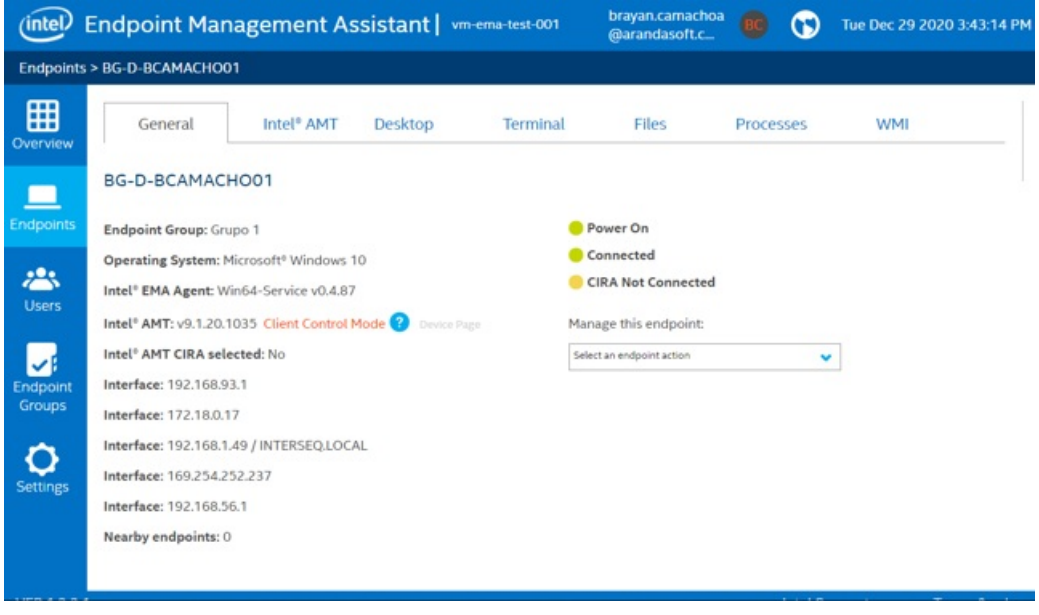


Access from Intel EMMA

4. If the user is already authenticated in the EMA console, they will be able to directly access the device, if not, the system asks for credentials to log in as the tenant administrator user, created during the registration process. configuration or in the [Creation of Tenant Administrator User](#) section of EMA.



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



\n## EMA server Installation

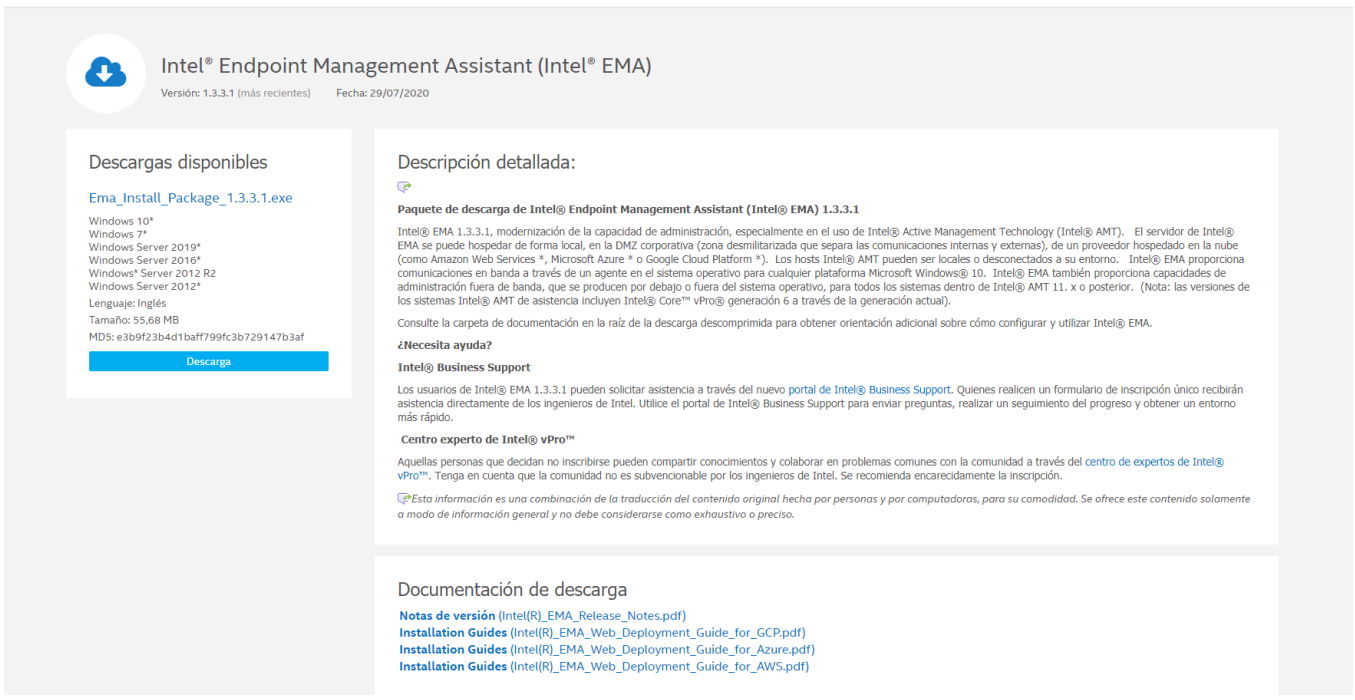
title: EMA server Installation chapter: —

Español

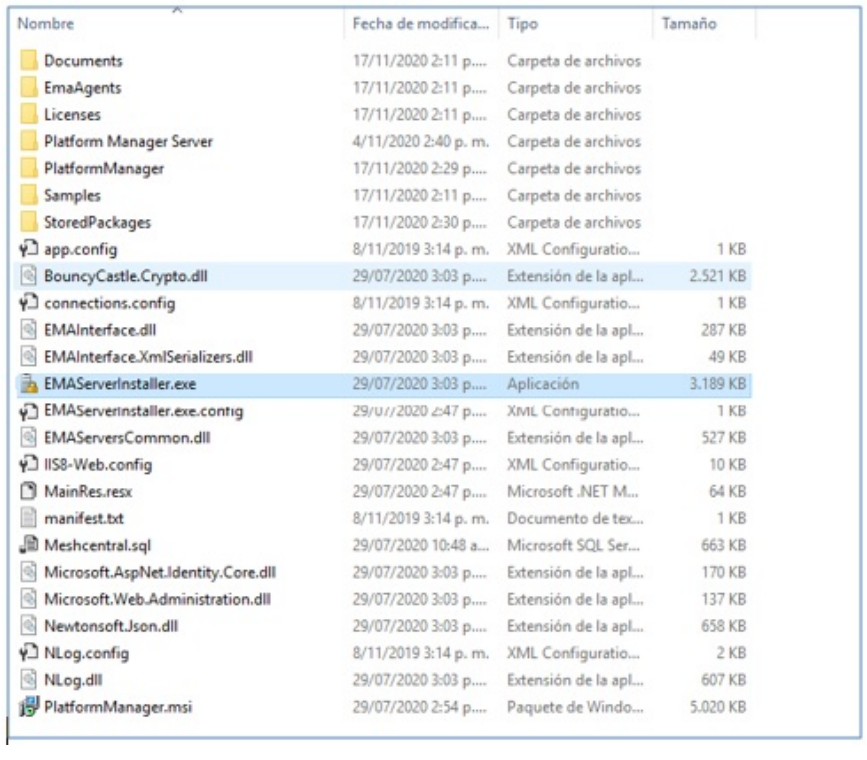
The basic installation of Intel EMA to carry out the integration with ADM is described below.

⚐ **Nota:** For complete configuration, considerations, and installation issues, seethe official Intel EMA documentation

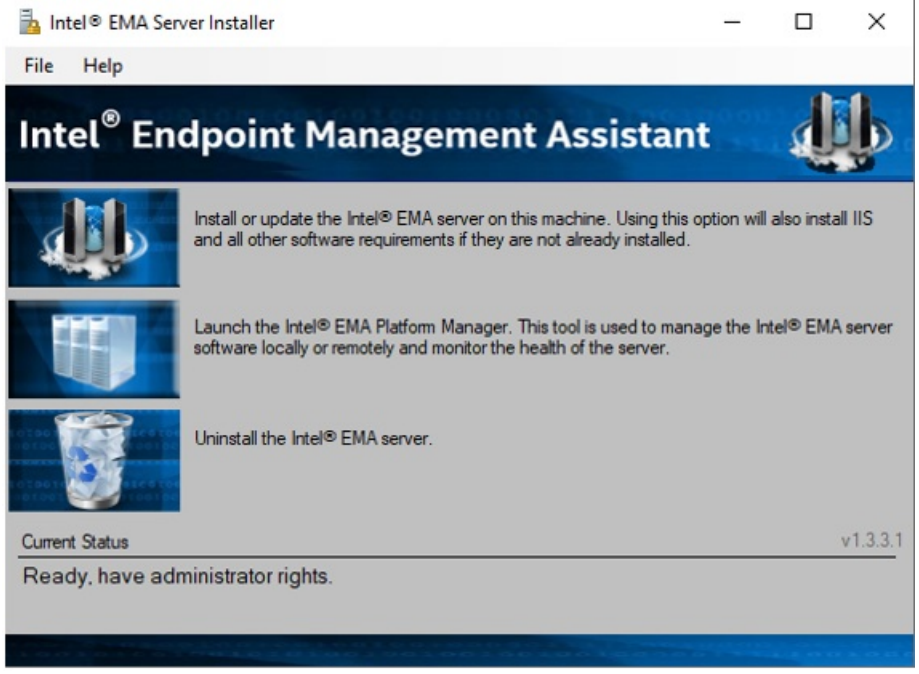
1. Download the Ema installation packages at the following path:Intel-Endpoint-Management-Assistant-Intel-EMA



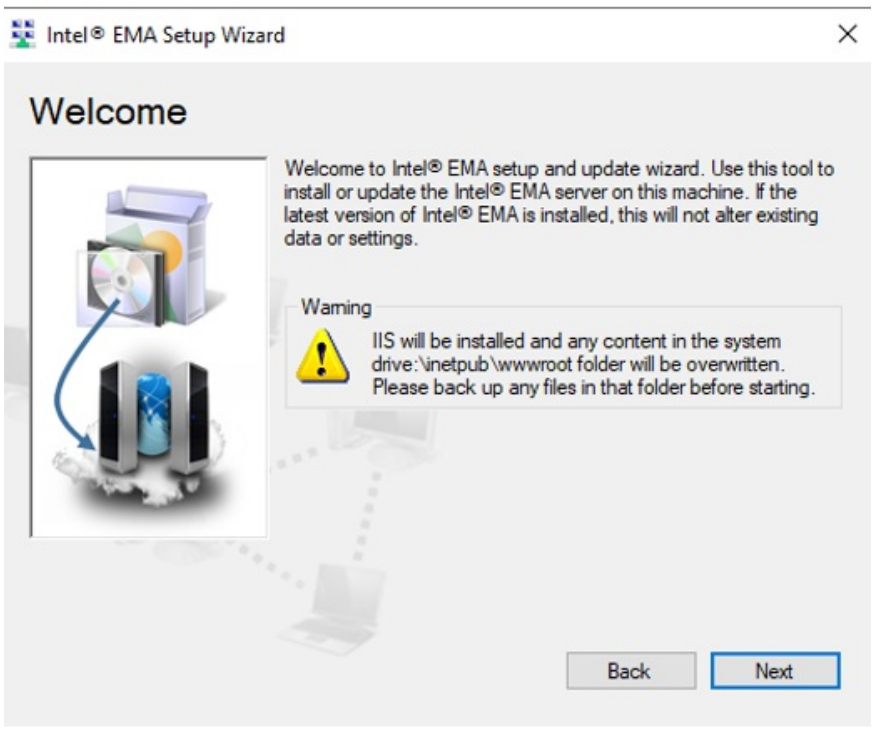
2. Run the file **EMAServerInstaller.exe**.



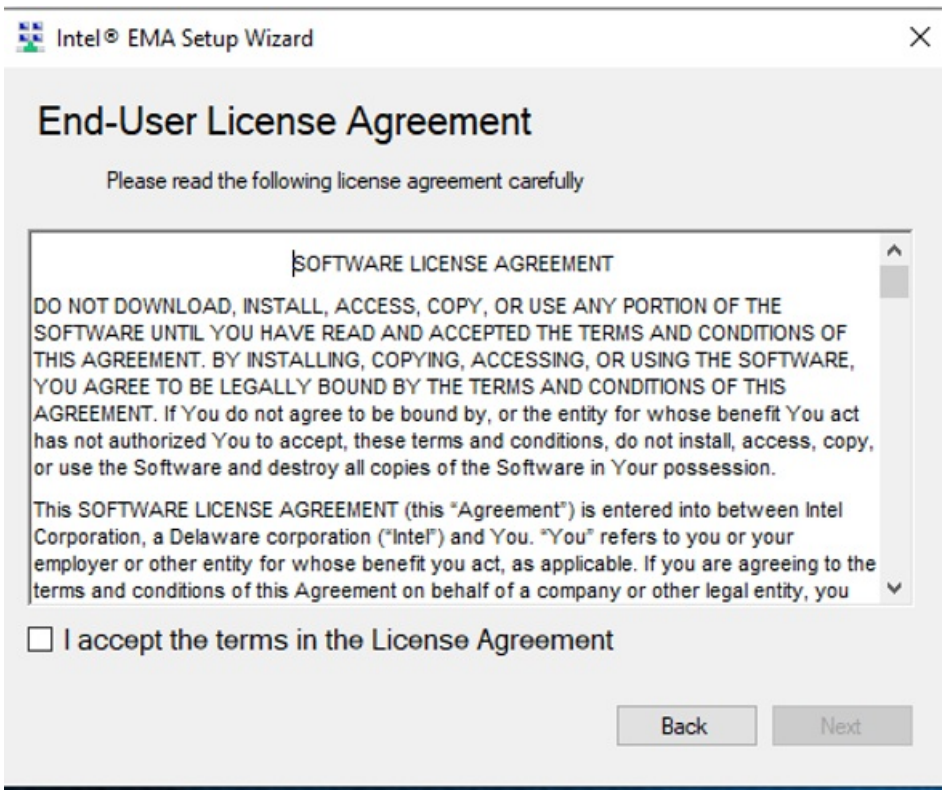
3. Install Ema server and select option 1.



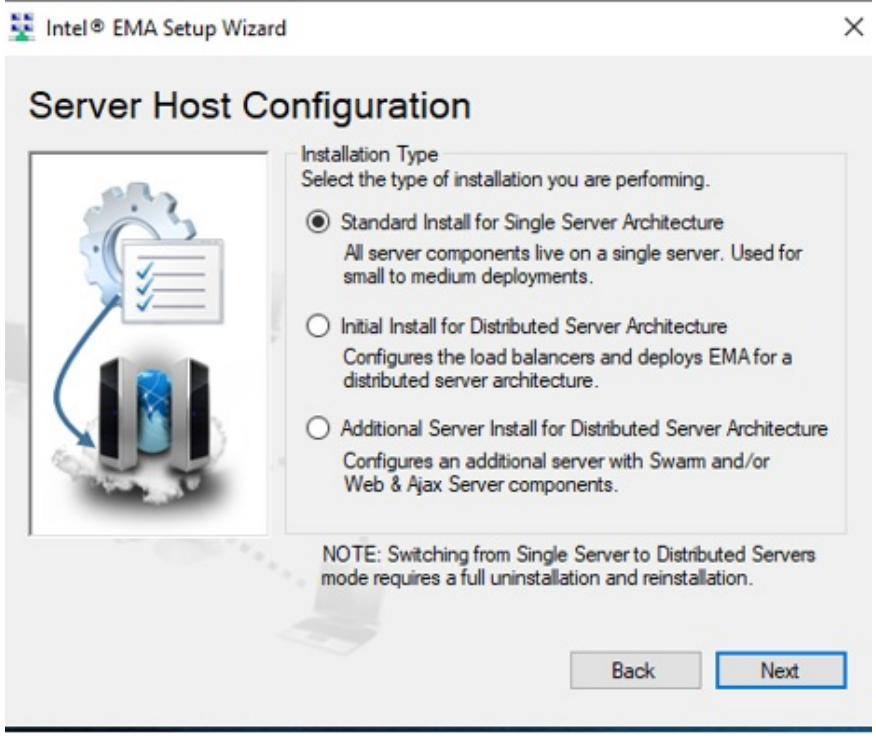
4. The recommendation to have IIS configured for the Windows operating system must be followed.



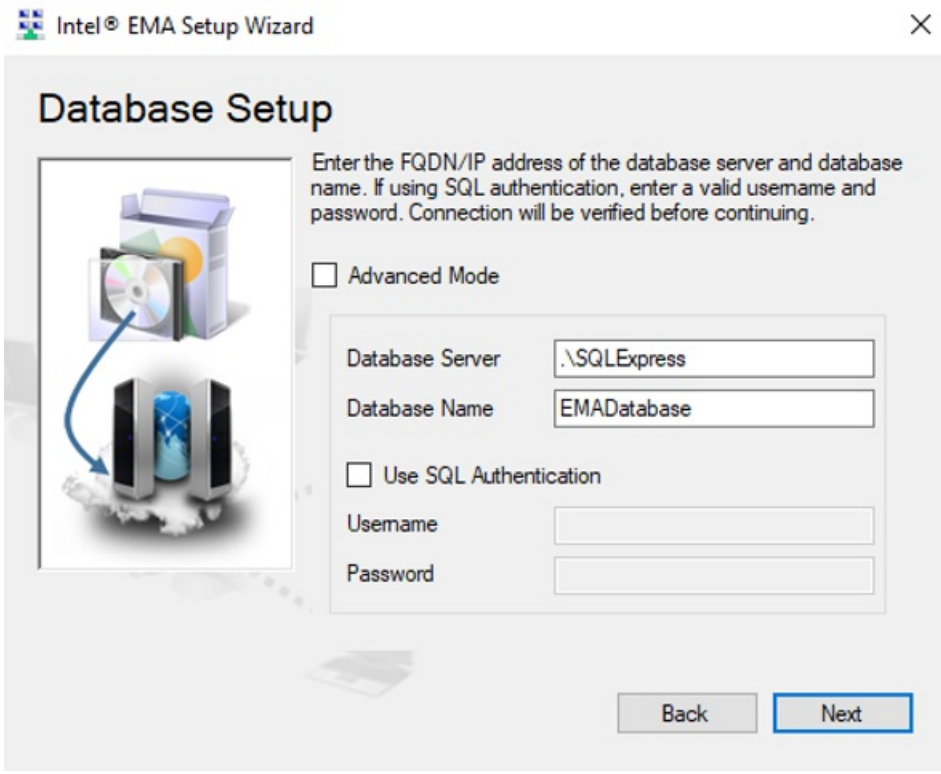
5. Read the installation agreement and click**Next**.



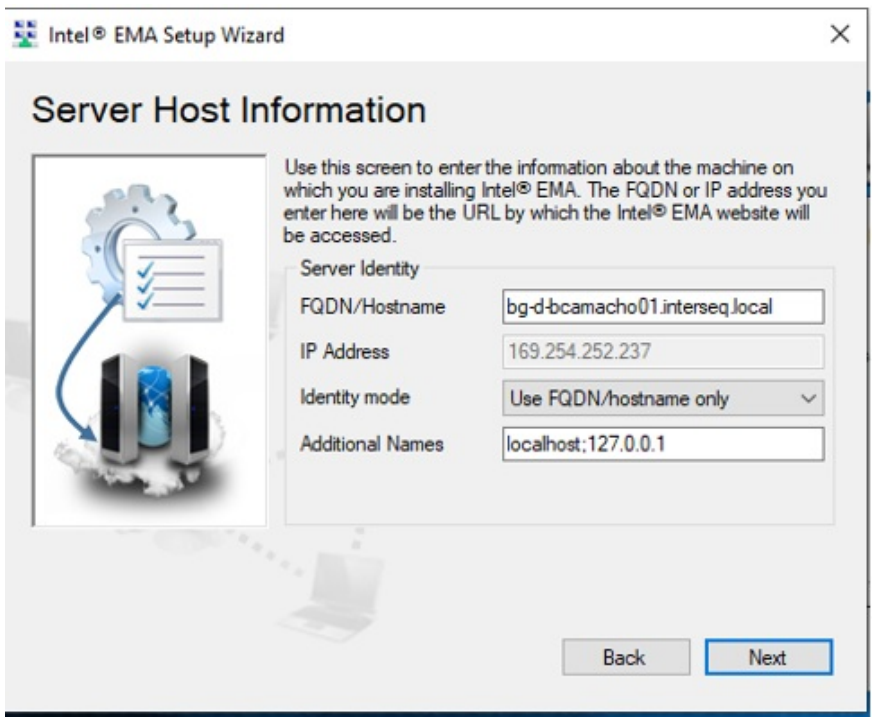
6. Select the type of installation



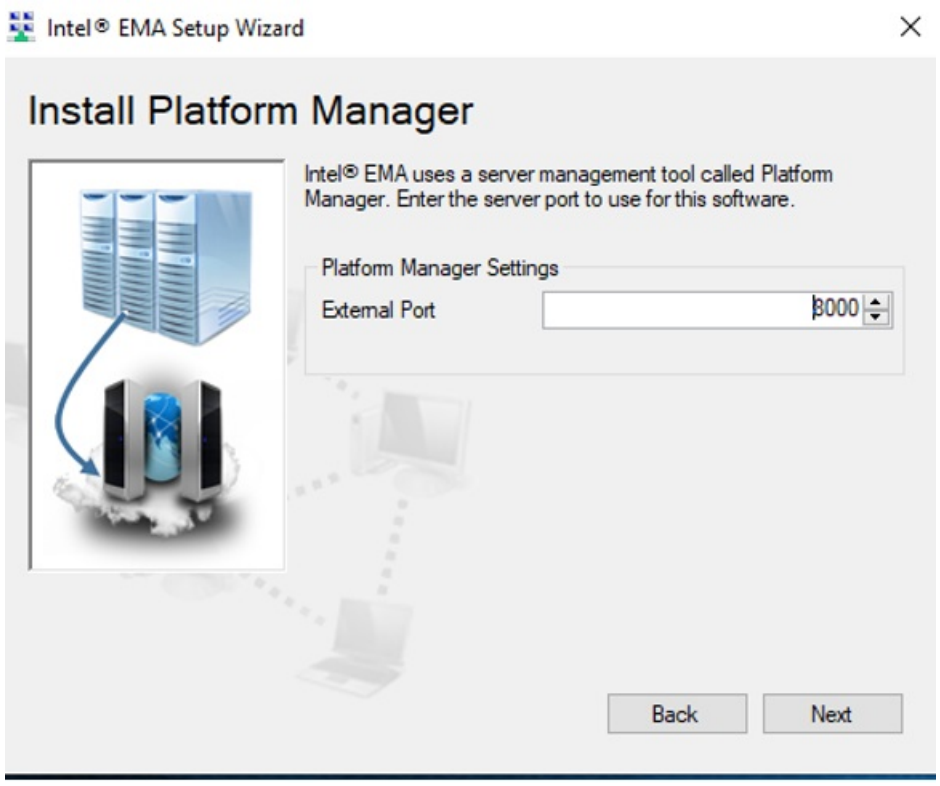
7. Select SQL Server database instance.



8. Configure Host Information



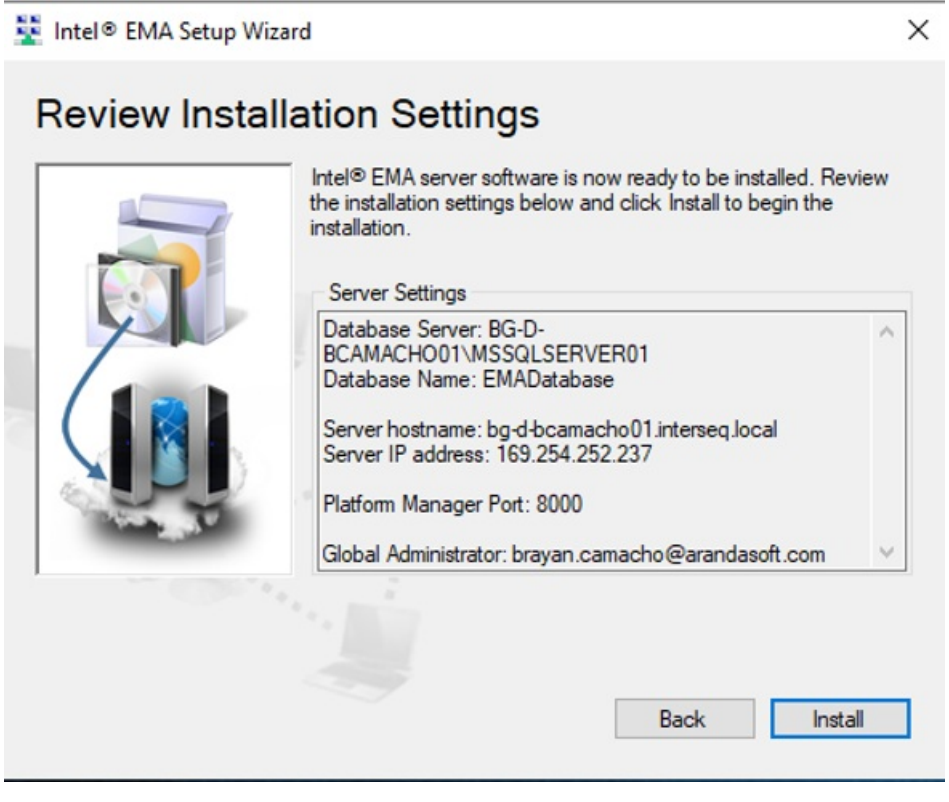
9. Install Platform Manager.



10. Configure the type of user authentication.

11. In this step add the admin username of the entire EMA instance; it is necessary to save these credentials for the general administration of EMA.

12. Click on install.

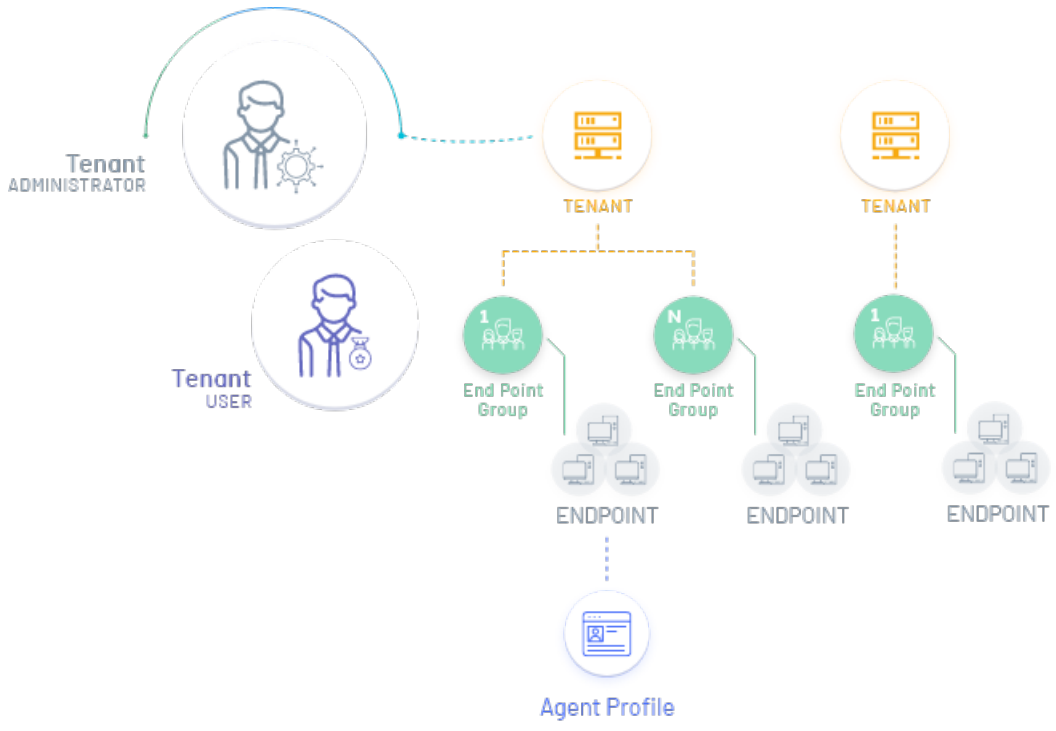


\n## EMA Console

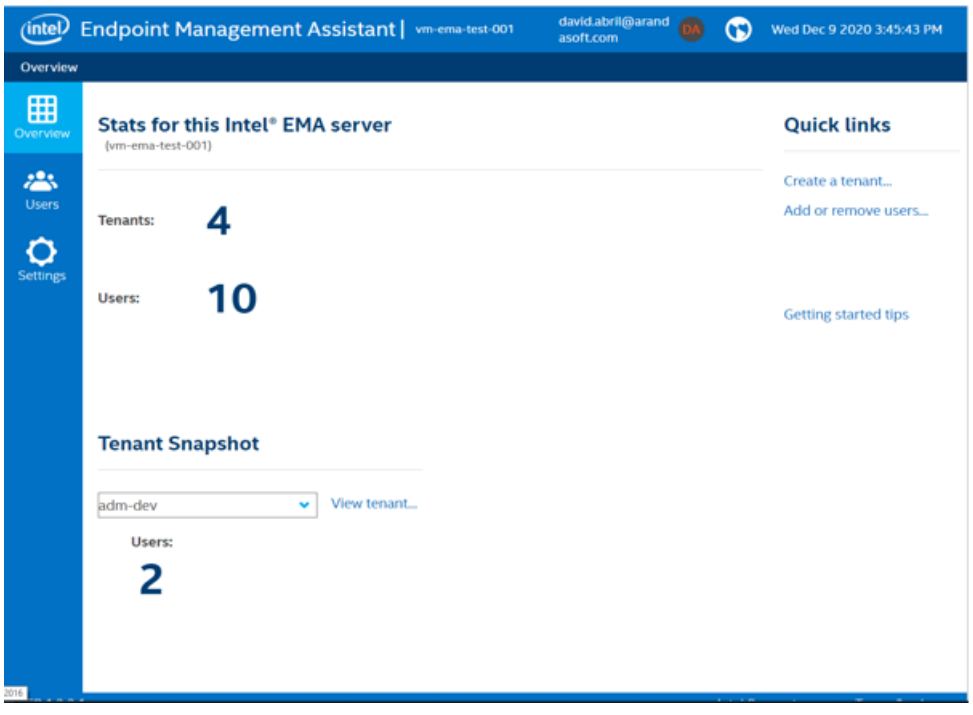
title: EMA Console chapter: —

Español

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



1. Log in to the Enpoint Management Assistant console as a Global Administrator, with the user configured during installation. In the **Overview** option of the main menu you can view the defined states.

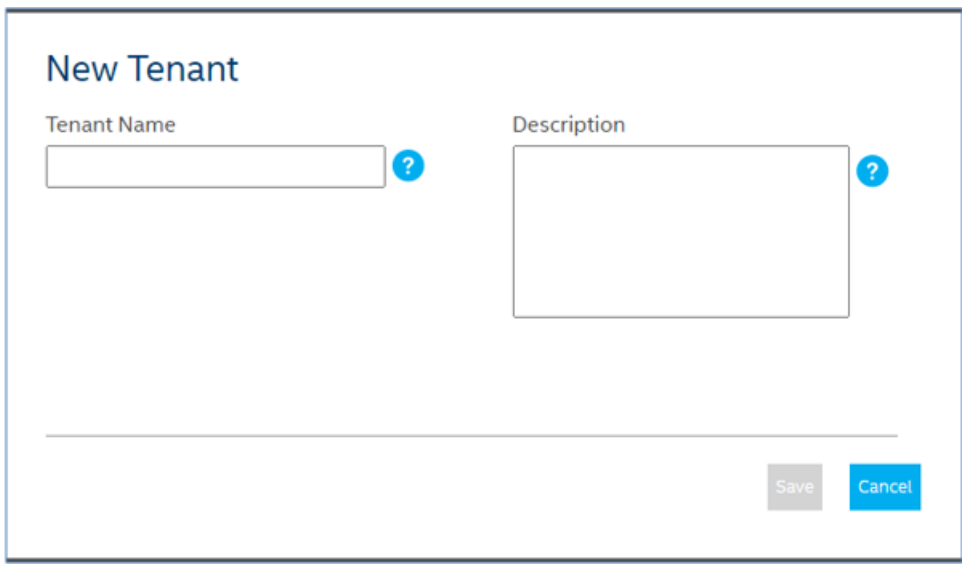


Create the tenants to use

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

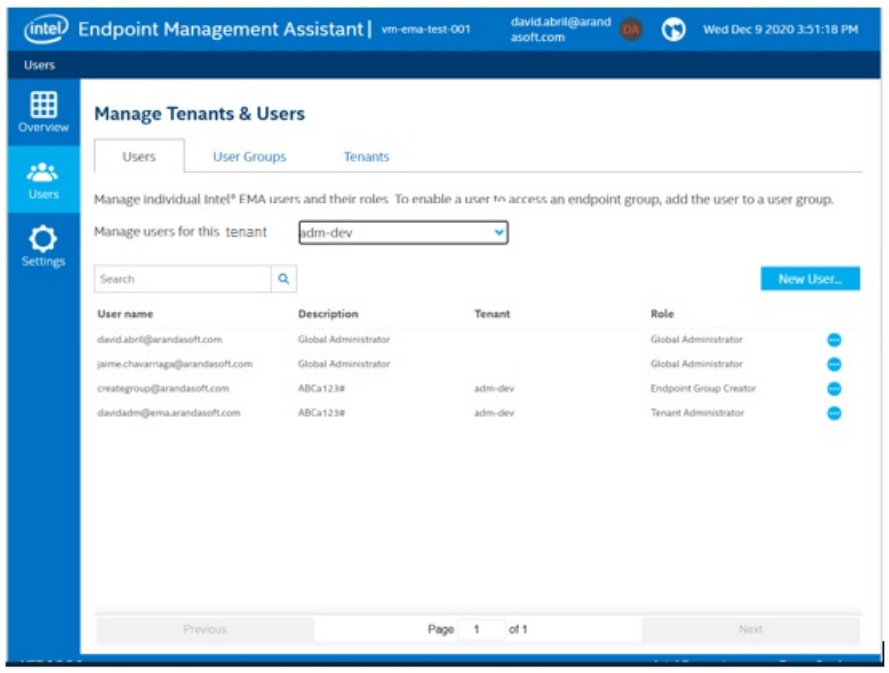
This is the tenant that will integrate with ADM (If you are going to use the EMA instance to synchronize different ADM instances, you must create a tenant for each instance, it is recommended to use the client name to differentiate).

3. When the configuration is complete, click **Save**.



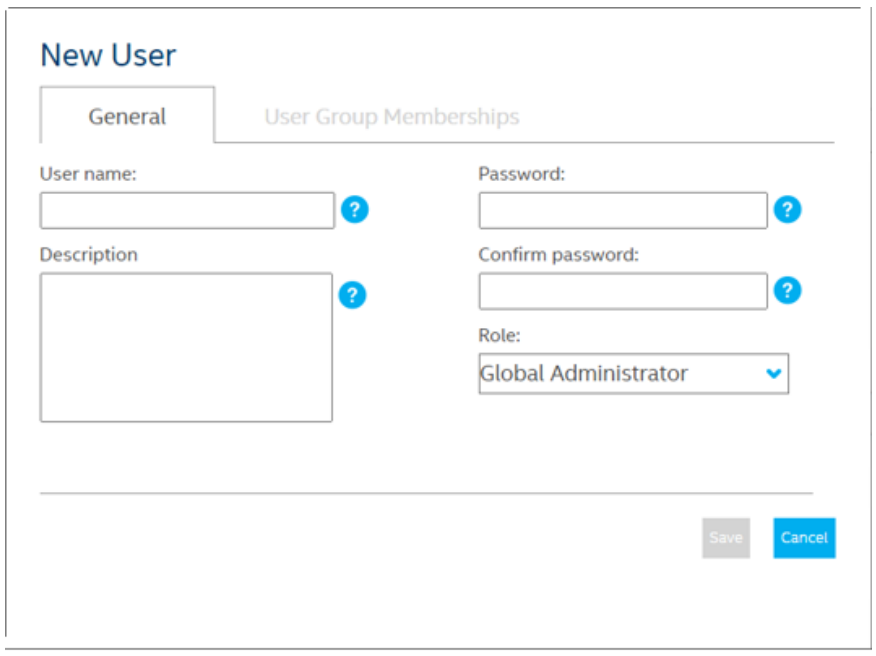
Create the tenant users

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



5. In the **Users** Tab, select the **New User** button and in the window that is enabled you can enter information such as user name, description, password and role associated with the user.

6. When completing the configuration click **Save**.



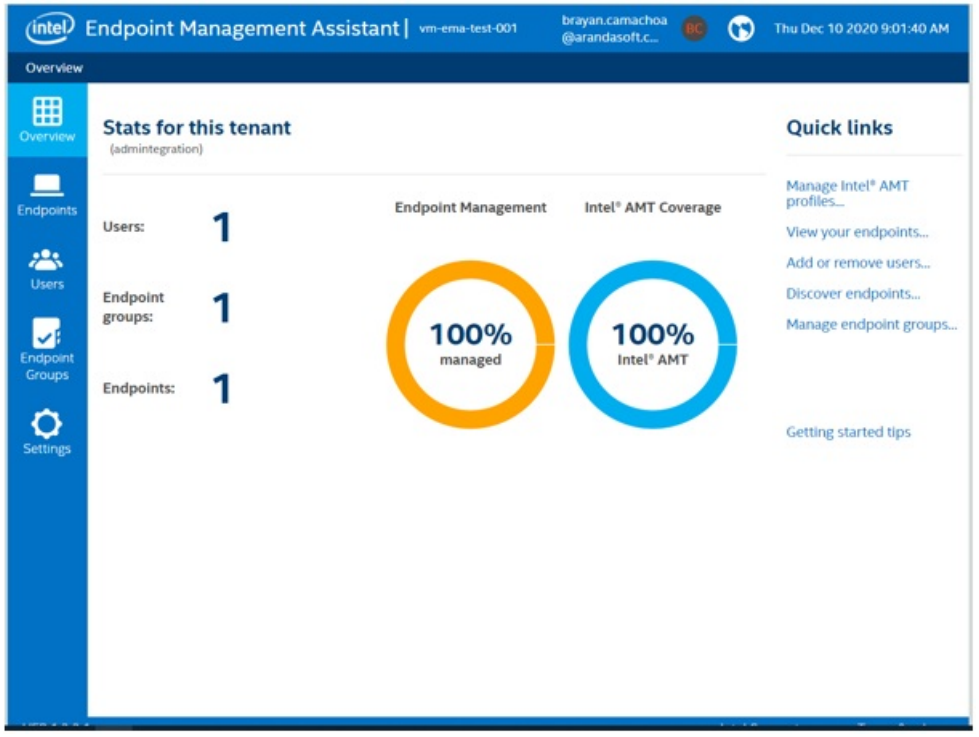
\n## Generar Agente de Intel EMA

title: Generar Agente de Intel EMA chapter: "intel_ema" —

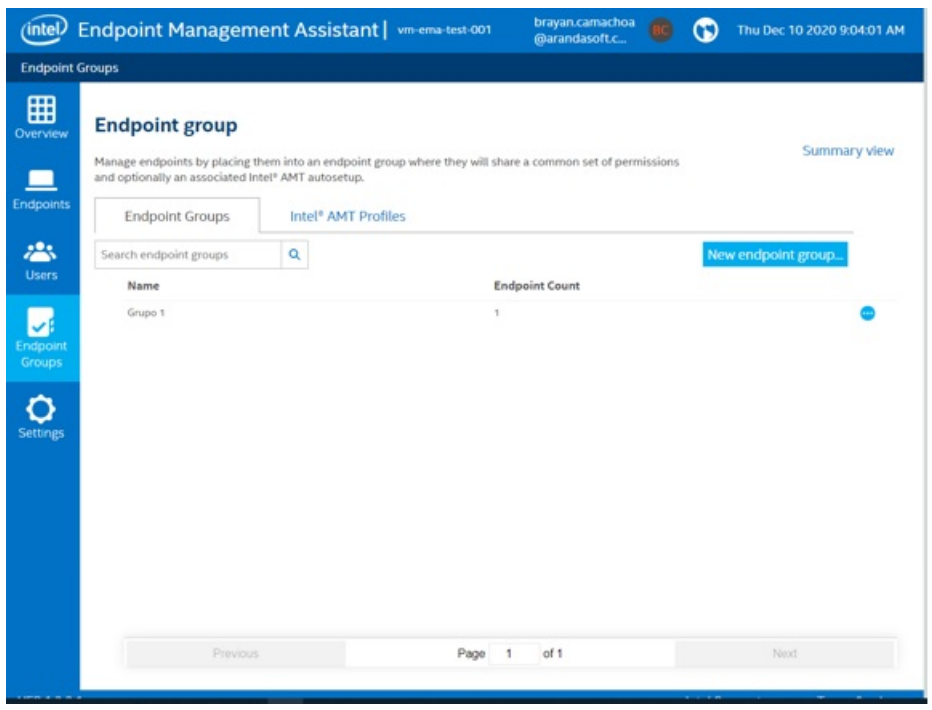
English

Crear Grupo Endpoint

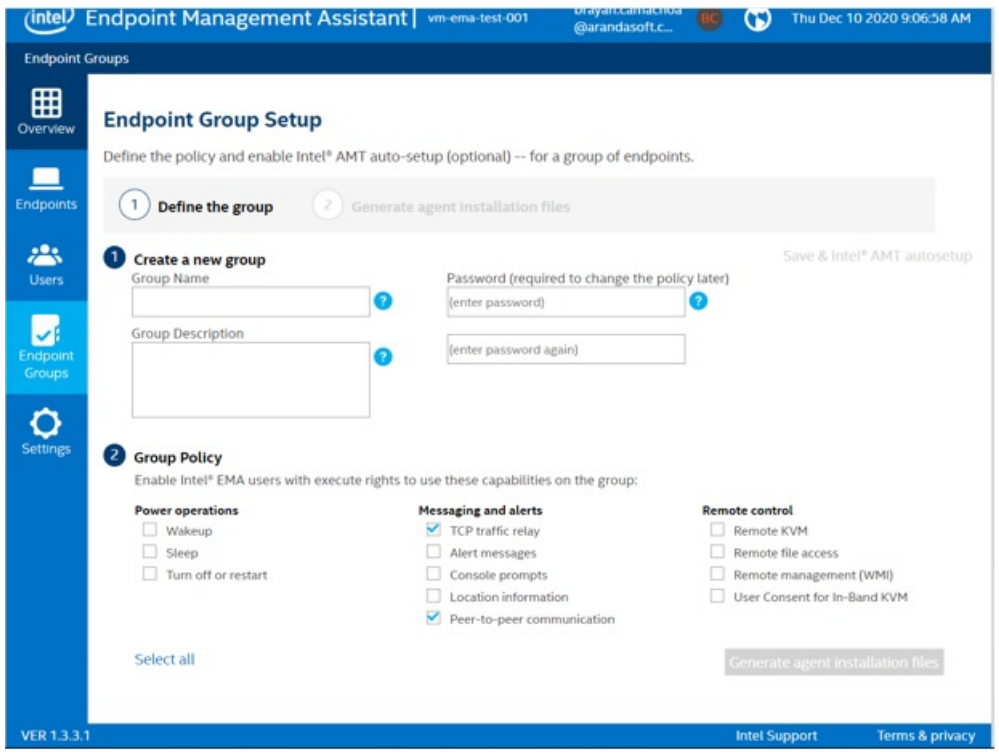
1. Ingrese a la consola Enpoint Management Asistant como Administrador de Tenant y seleccione la opción **Endpoint Group** del menú principal.



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

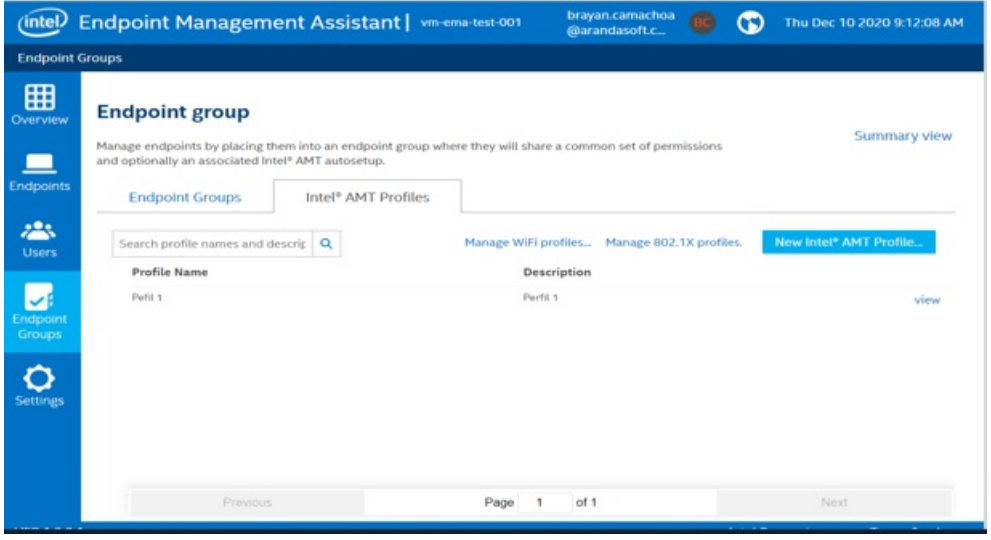


3. En la configuración del grupo ingrese nombre, descripción, contraseña y las políticas de acuerdo a las capacidades del grupo. Al terminar haga clic en la opción **Generate agent Instalation files** (Generar archivo de instalación de agente)

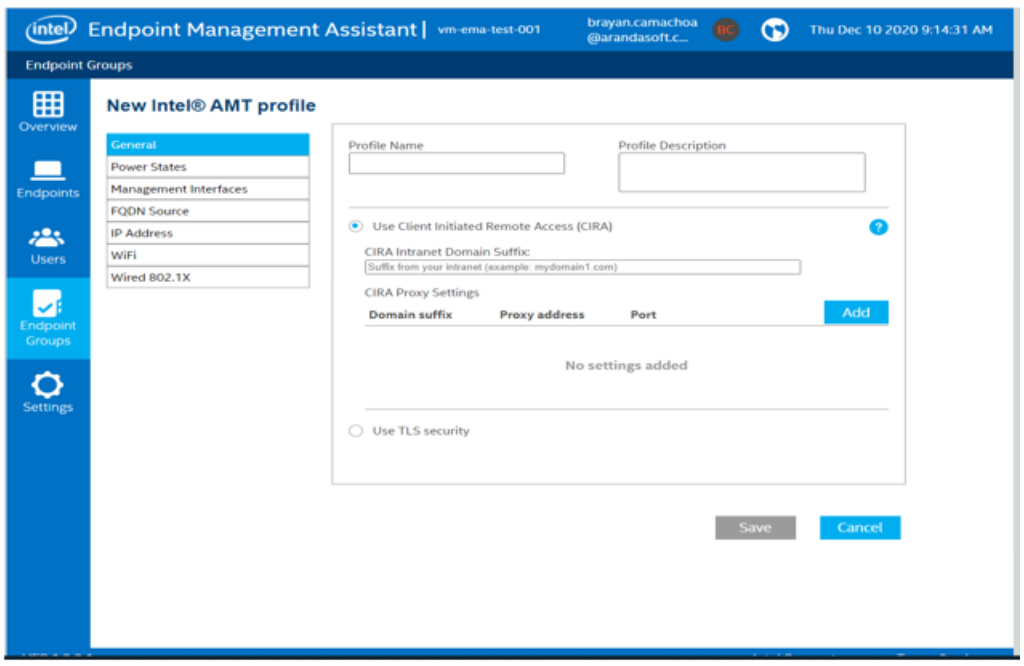


Perfil AMT

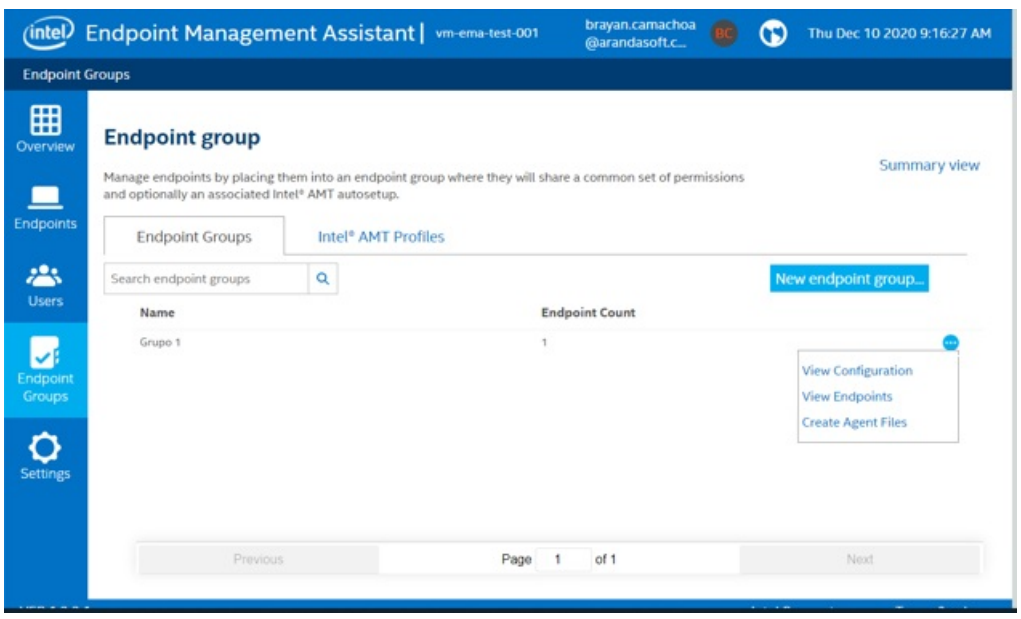
4. En la pestaña**Endpoint Groups** seleccione la opción **Generar un perfil de AMT**.



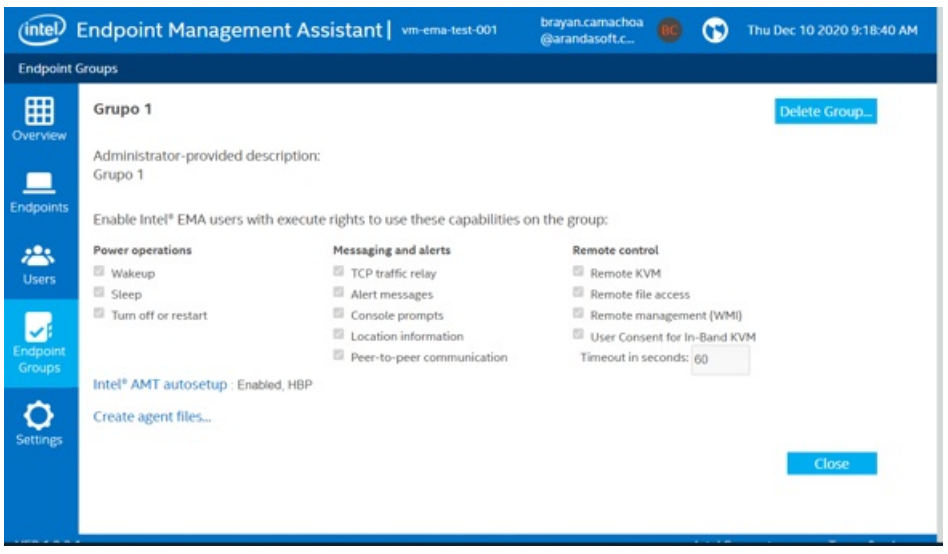
5. Configure la información relacionada al perfil de AMT.



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

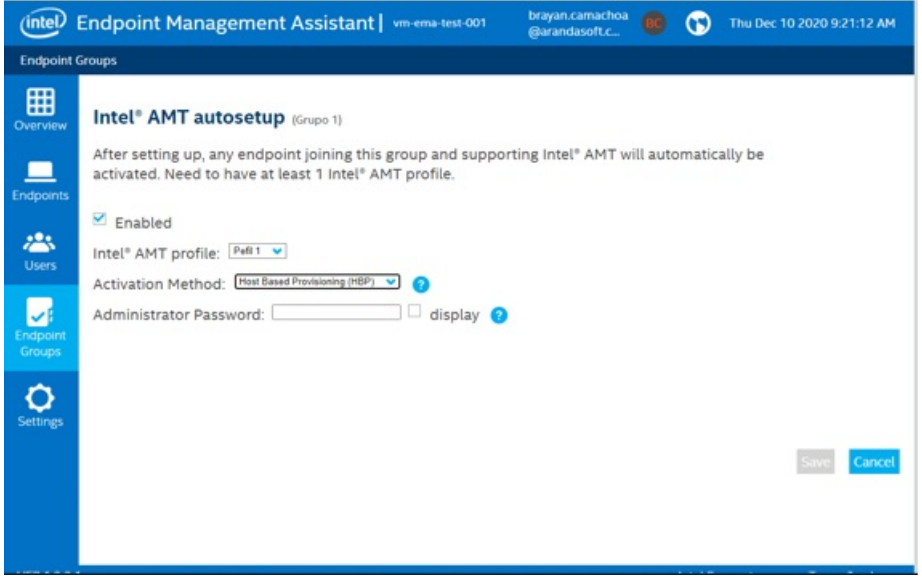


7. En el grupo haga clic en la opción **Intel AMT Autosetup**.

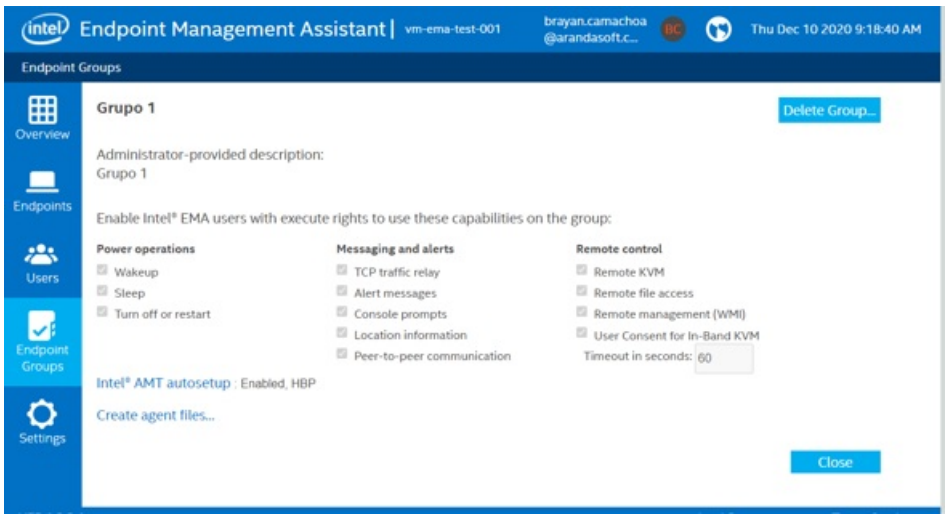


8. Seleccione el perfil de AMT y el método de activación. Ingrese el password de la BIOS; como administrador de TI asegure que todos los equipos tengan el mismo password para que este perfil les funcioné al instalarse.

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

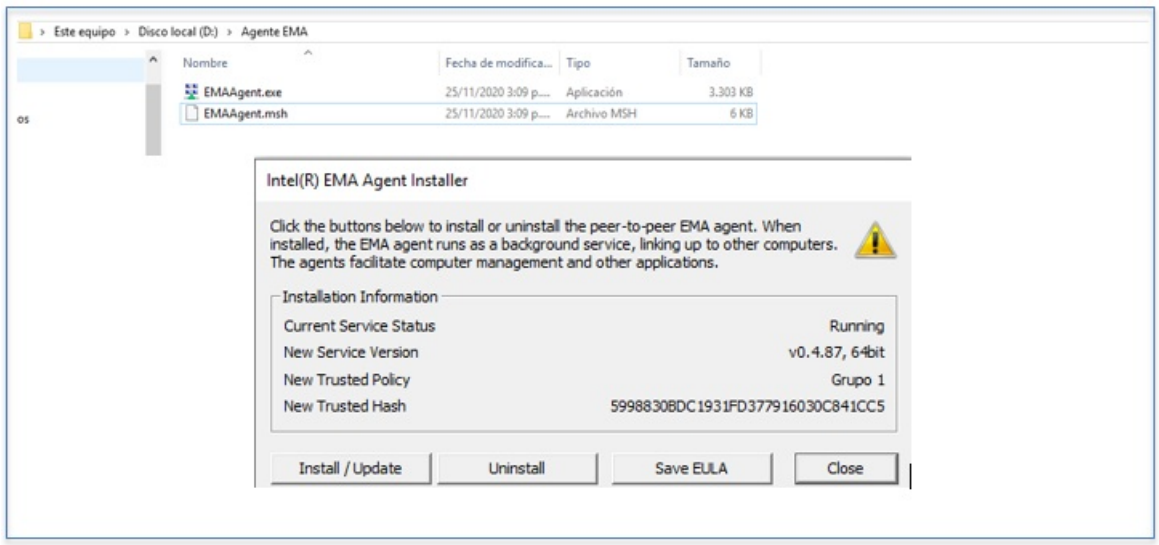


9. En el grupo haga clic en la opción **Create Agent Files** (Crear archivo de Agente).



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	

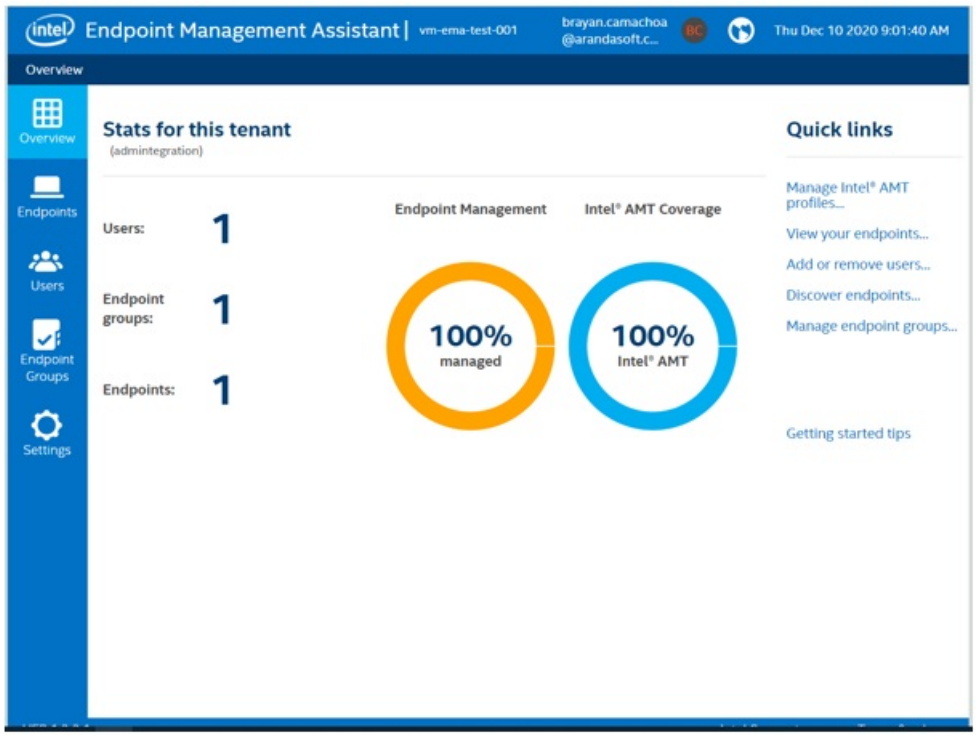
\n## Generate Intel Ema Agent

title: Generate Intel Ema Agent chapter: —

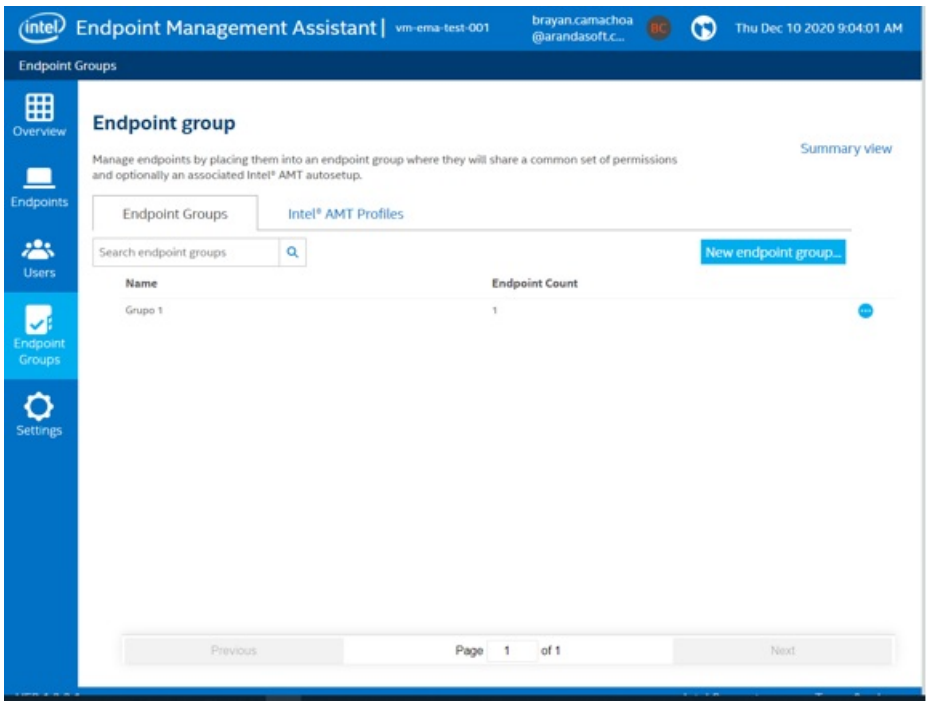
Español

Create Endpoint Group

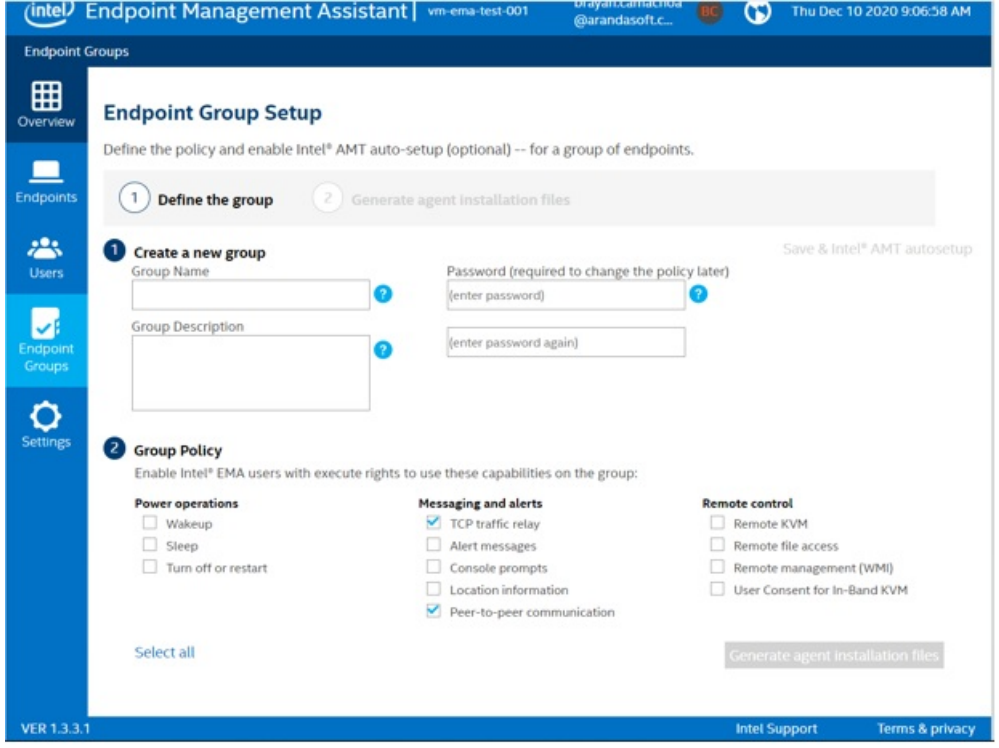
1. Log in to the Endpoint Management Assistant console as a Tenant Administrator and select the **Endpoint Group** option from the main menu.



2. In the **Endpoint Group** information view select the **New endpoint group** option.

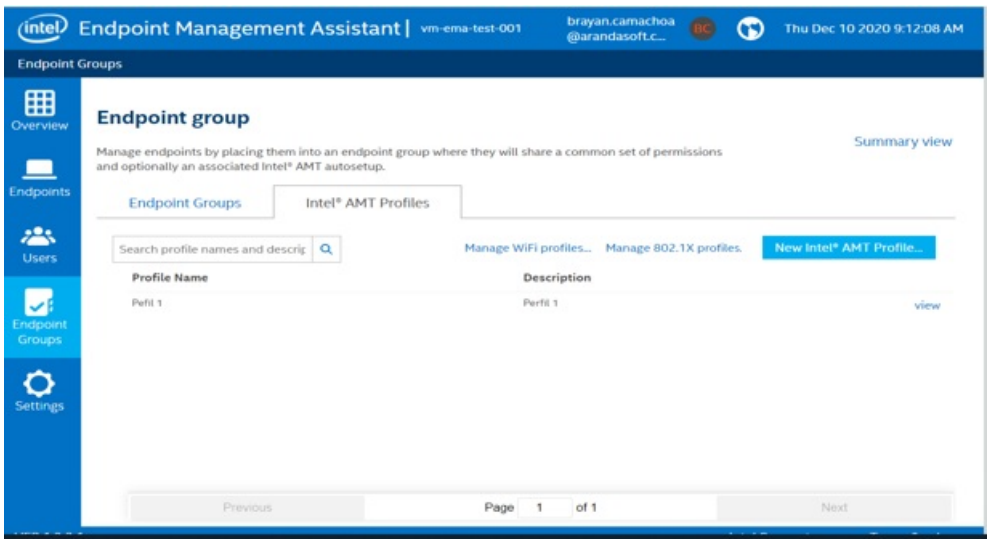


3. In the group configuration enter name, description, password and policies according to the group's capabilities. When finished, click on the **Generate agent Installation files** option.

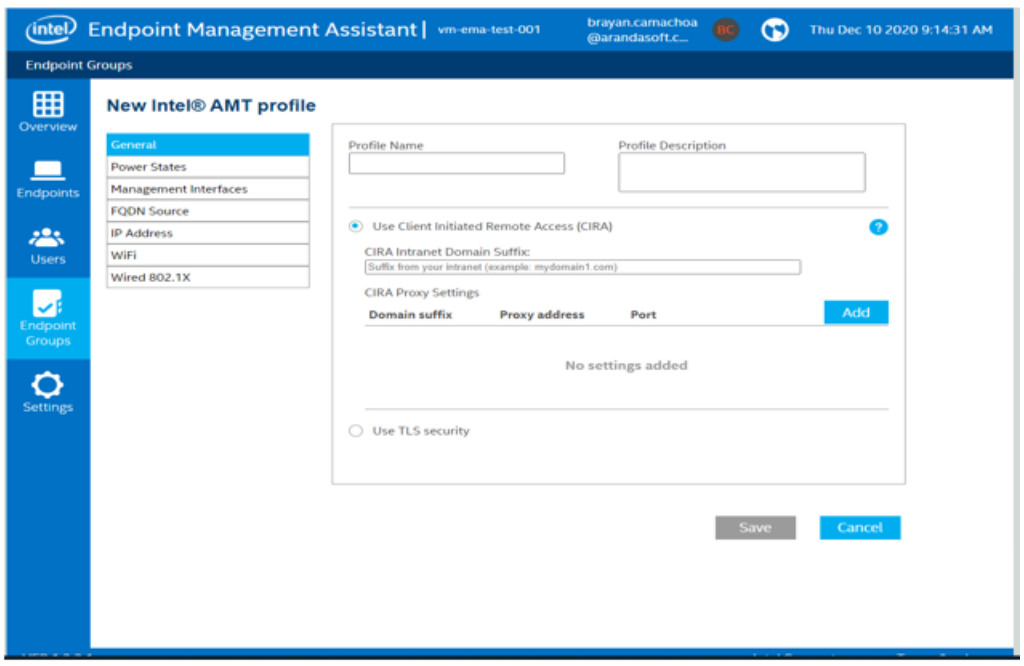


AMT Profile

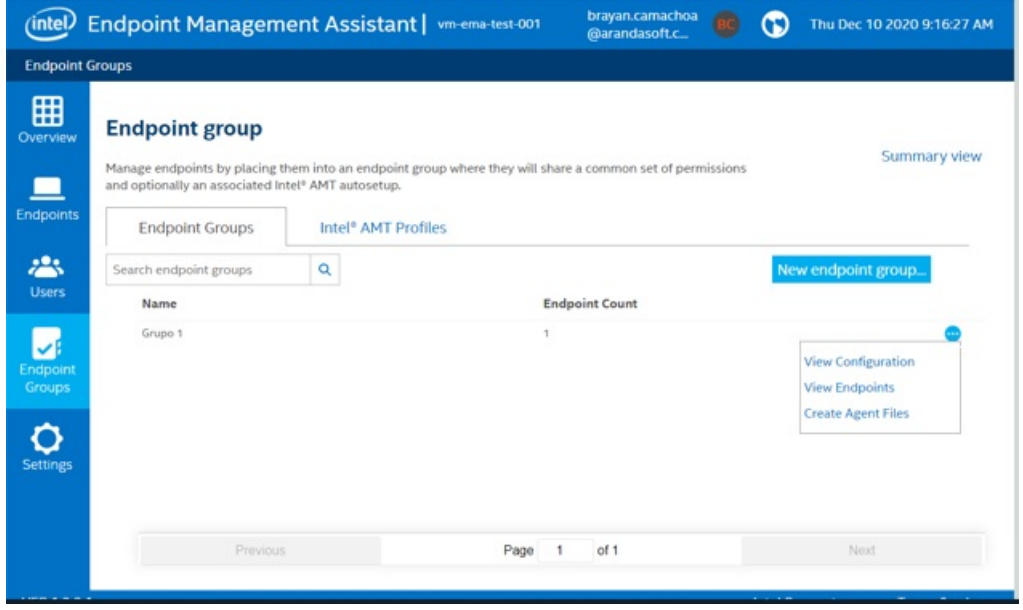
4. In the **Endpoint Groups** tab select the **Generate an AMT Profile** option.



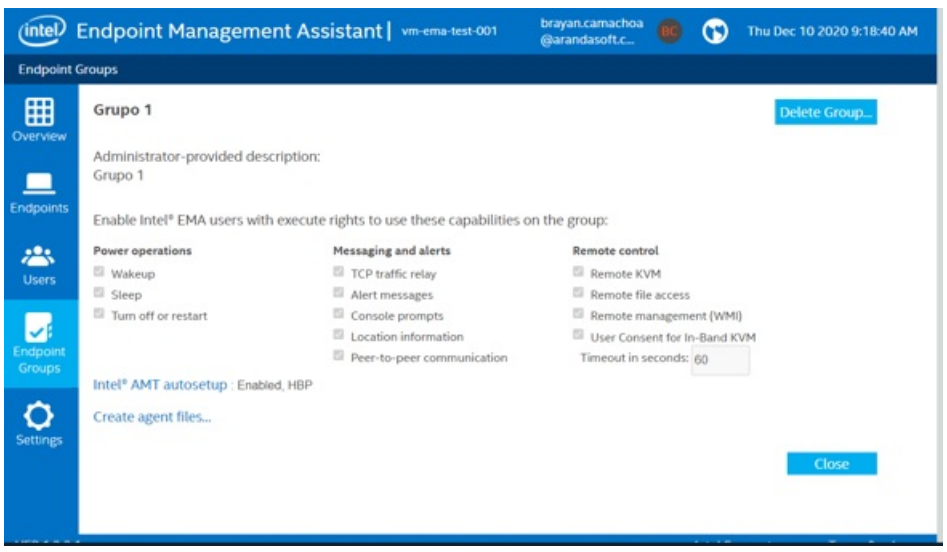
5. Configure the information related to the AMT profile.



6. Assign the AMT profile to the Endpoint group.

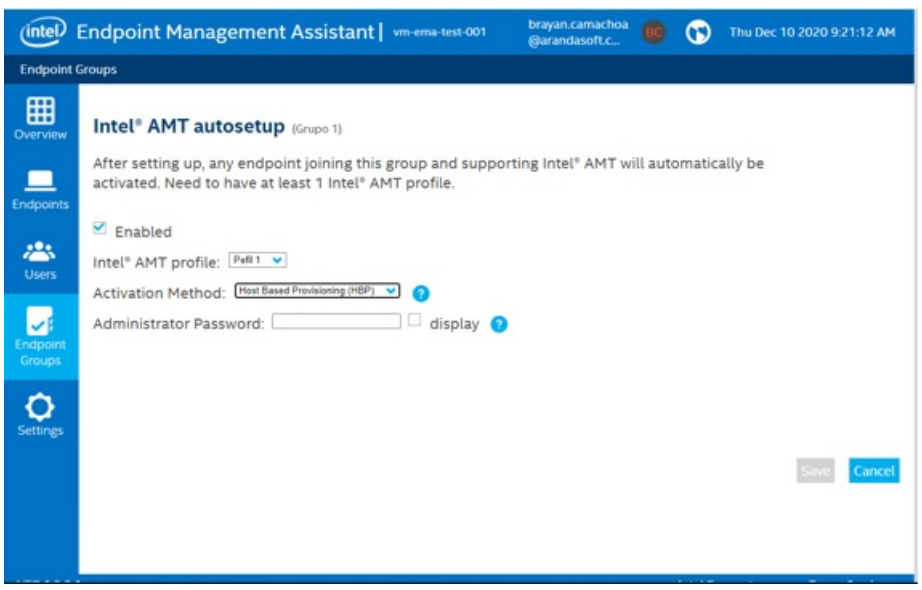


7. In the group click on the**Intel AMT Autosetup** option.

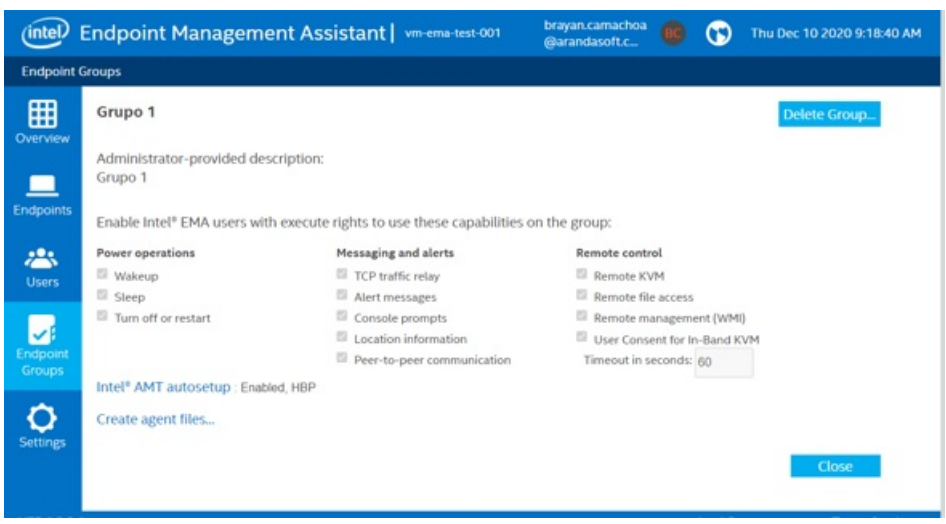


8. Select the AMT profile and activation method. Enter the BIOS password; As an IT administrator, ensure that all computers have the same password so that this profile works for them when installed.

⚐ **Note:** By default on computer equipment the password is “admin”. It is recommended to review the device model documentation.

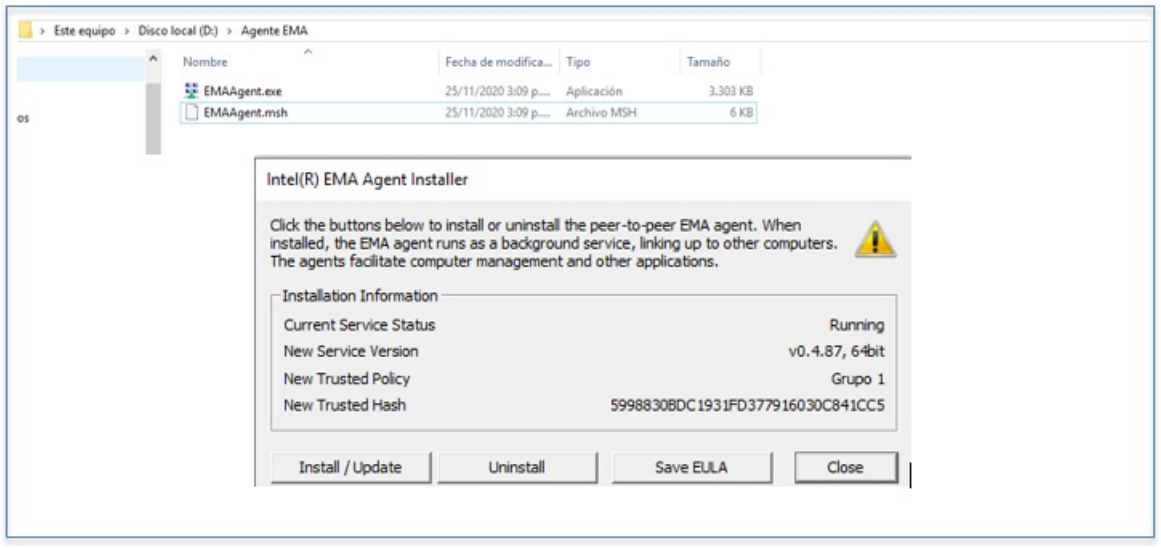


9. In the group click on the**Create Agent Files** option .



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

⚐ **Note:** On the client machine, which is going 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 supported by EMA are those that have firmware equal to or greater than version 11, generally supported by 7th Generation processors, some 6th Generation processors also support it.

- FW versions can only be updated in subversions of the factory version. That is to say, a Generation 10 process cannot be updated from FW 14 to FW 15; What you can do is update from 14.1 to 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	

\n## Instalación de servidor de EMA

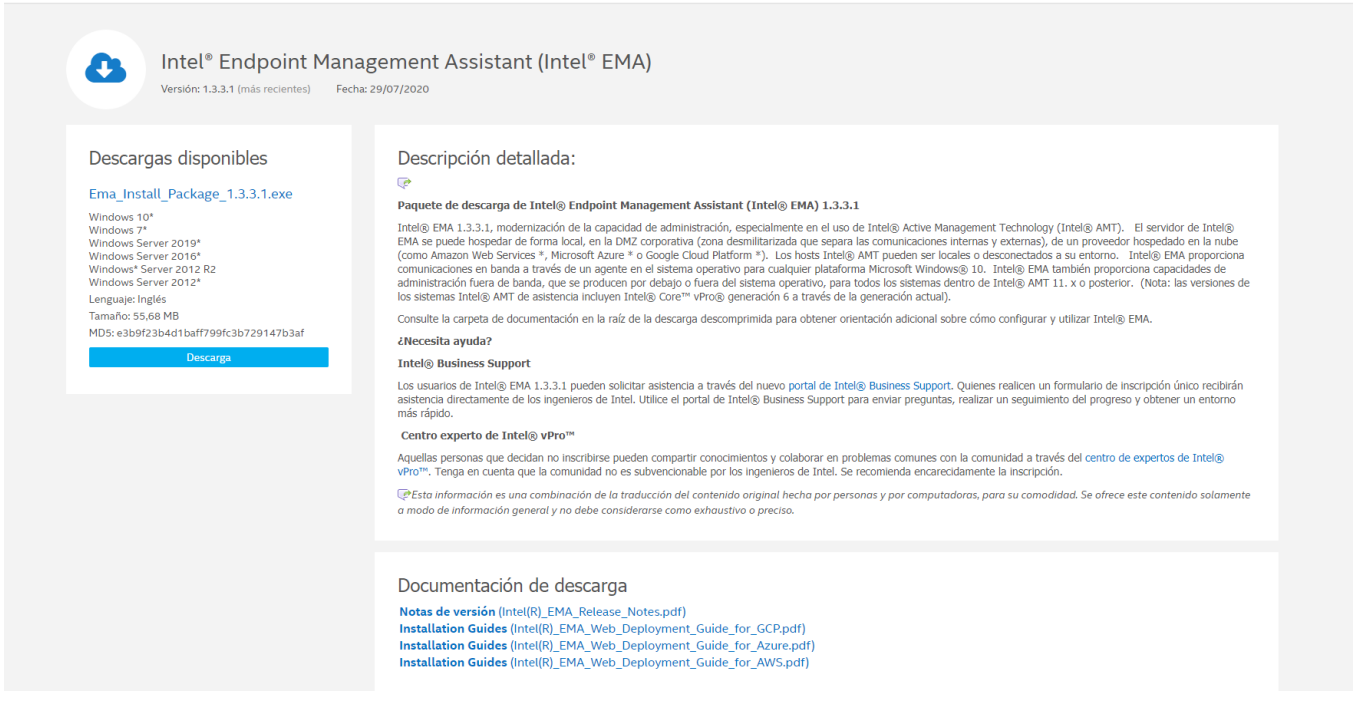
title: Instalación de servidor de EMA chapter: "intel_ema" —

English

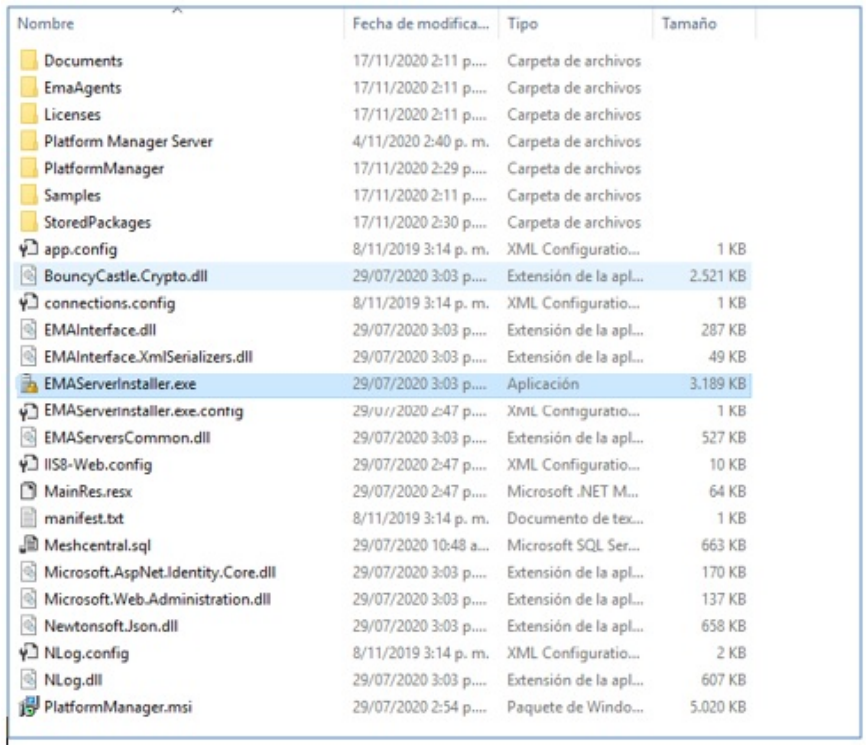
A continuación se describe la instalación básica de Intel EMA para llevar acabo la integración con ADM.

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

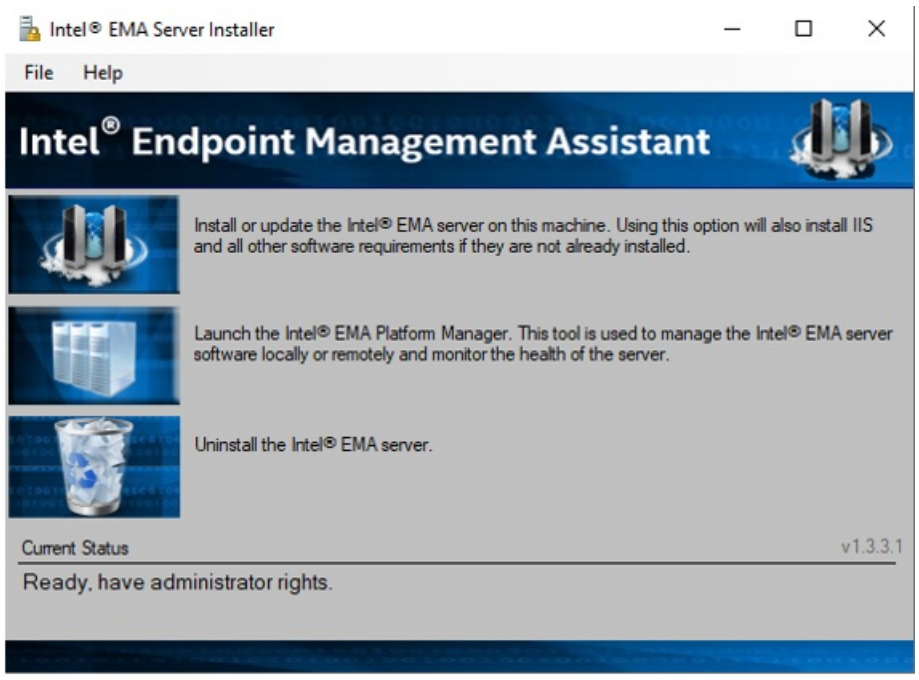
1. Descargue los paquetes de instalación de Ema en la siguiente ruta: Intel-Endpoint-Management-Assistant-Intel-EMA



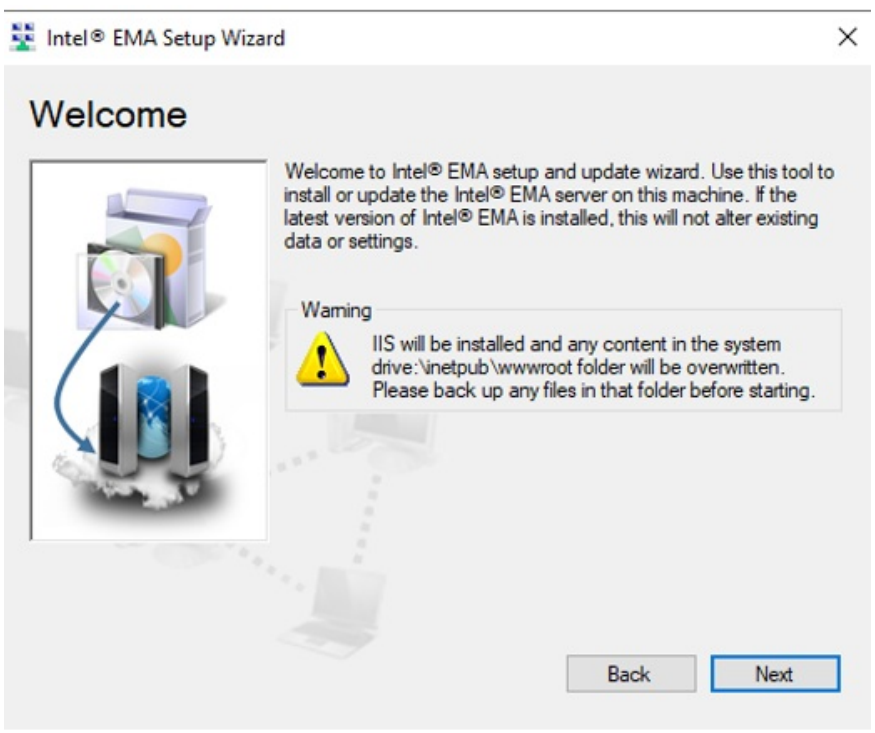
2. Ejecute el archivo **EMAServerInstaller.exe**.



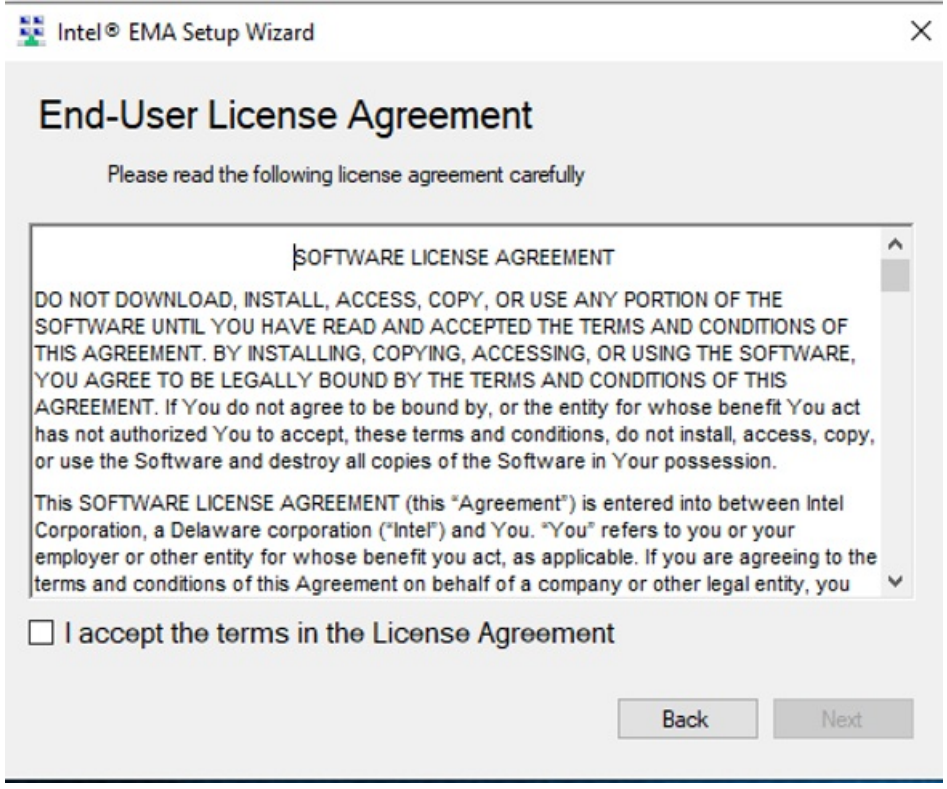
3. Instale el servidor de Ema y seleccione la opción 1.



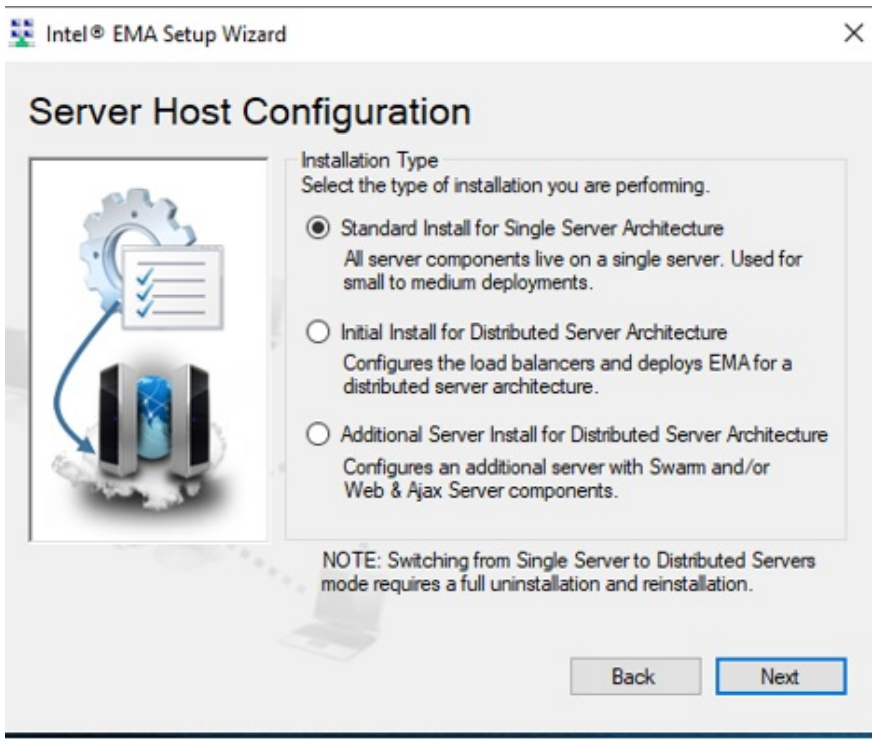
4. Debe cumplir la recomendación de tener el IIS configurado para el sistema operativo Windows.



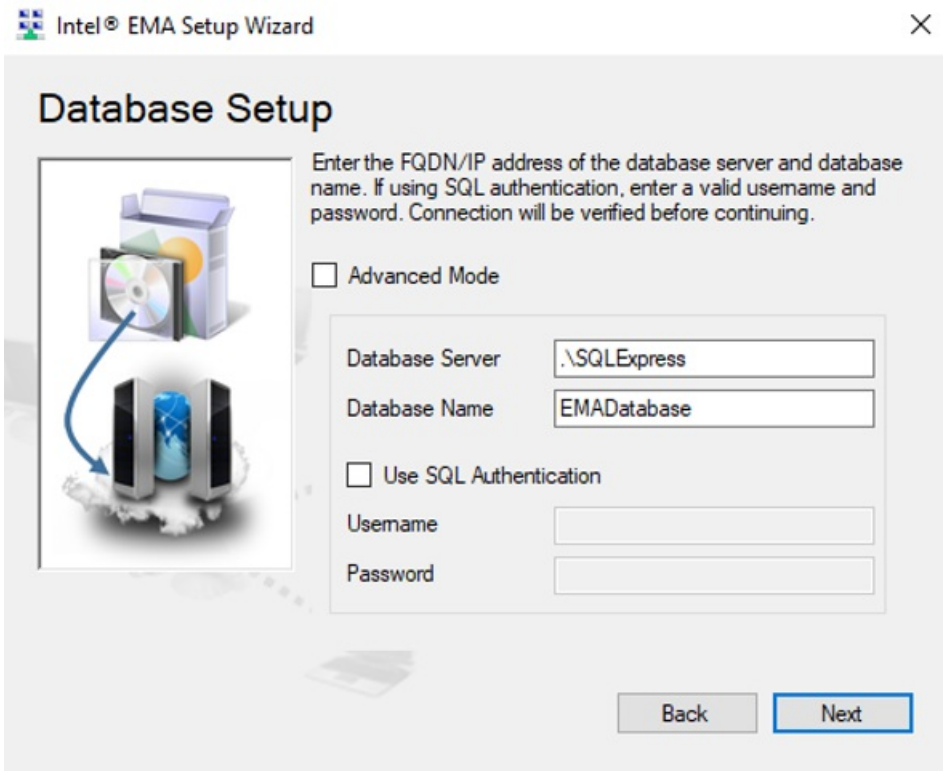
5. Lea el acuerdo de instalación y hacer clic en**Siguiente**.



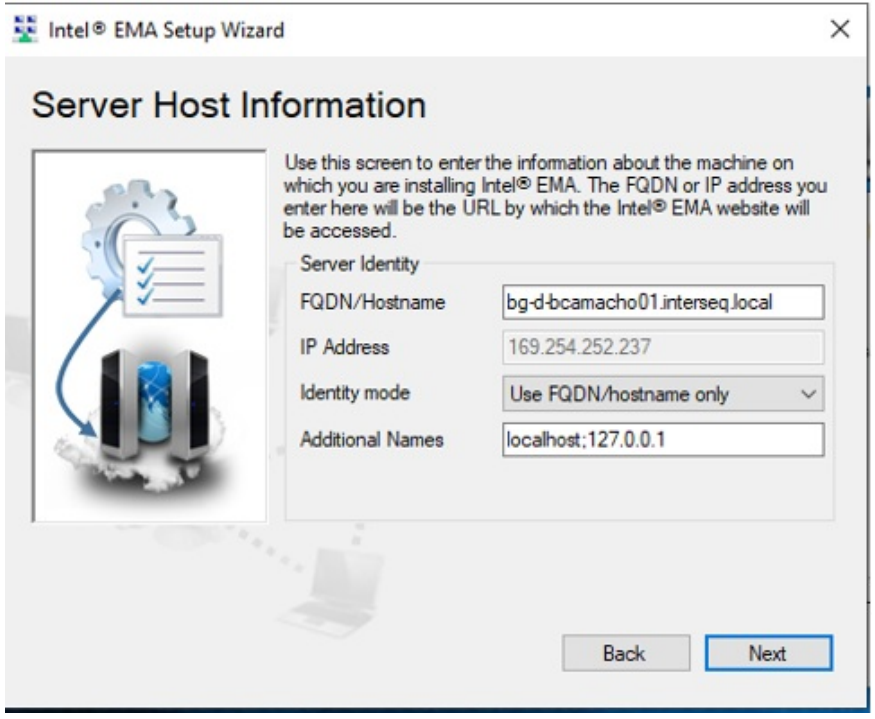
6. Seleccione el tipo de instalación:



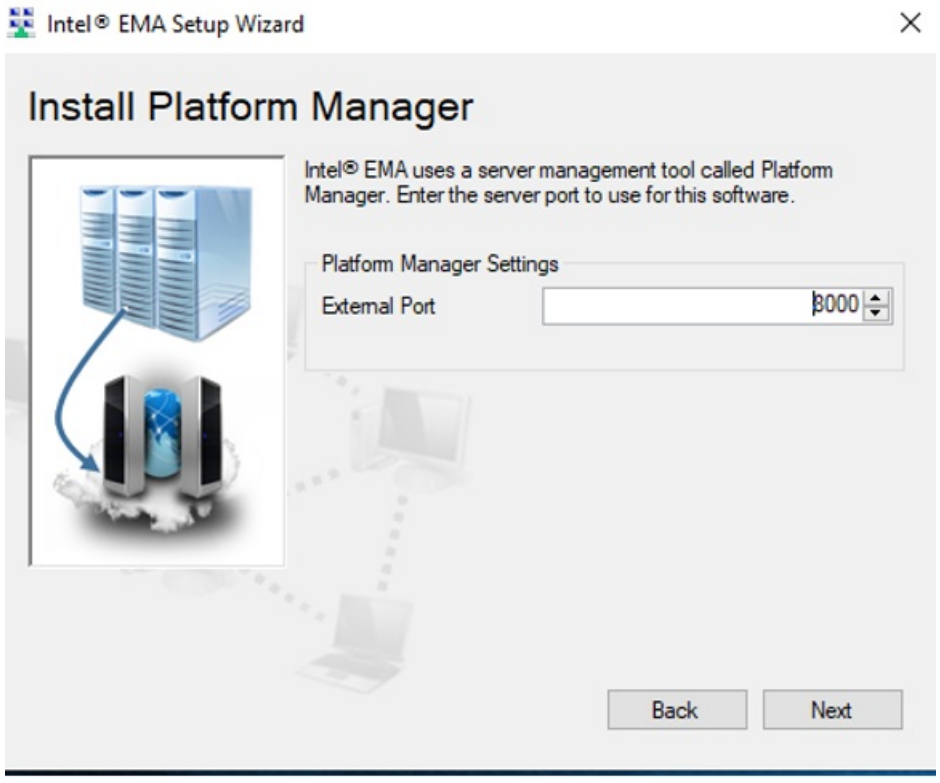
7. Seleccione la instancia de base de datos Sql Server.



8. Configure la información del Host.



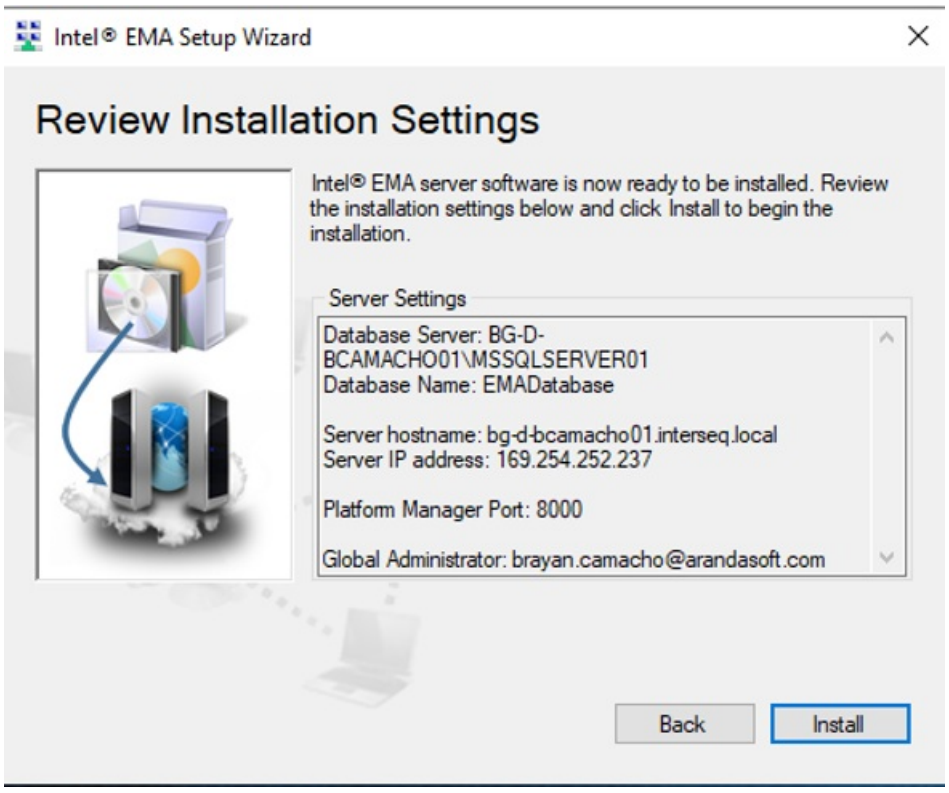
9. Instale el Platform Manager.



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**.



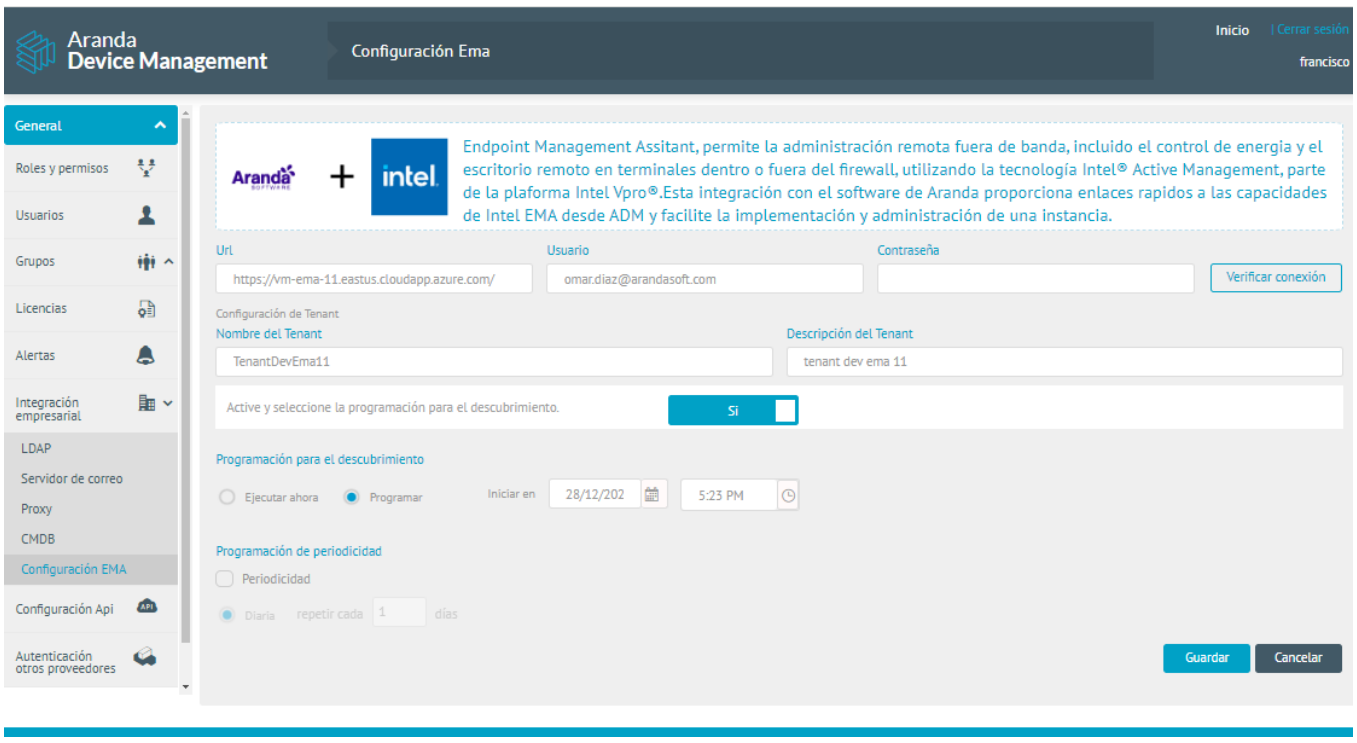
\n## Habilitar Integración ADM - Intel EMA

title: Habilitar Integración ADM - Intel EMA chapter: "intel_ema" —

English

1. Para configurar el directorio activo, ingrese a la vista de Configuración de la consola de administración de ADM, en la sección **Generales** seleccione la opción **Integración Empresarial** y **Configuración EMMA**. En la vista de información despliegue la opción **Más Opciones** y LDAP

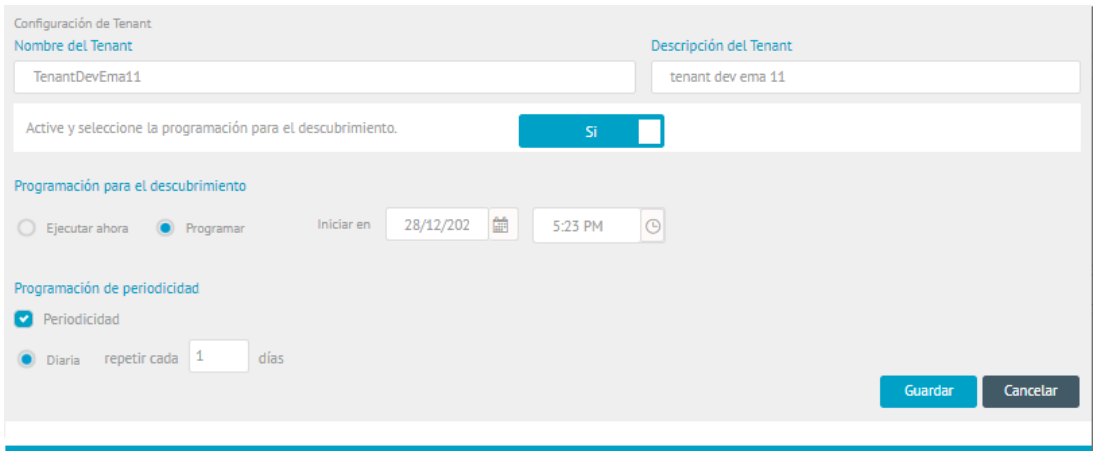
2. En la vista de información ingrese la información básica como url, usuario administrador global y su contraseña. Haga clic en **Verificar Conexión** y si es válida se habilita la configuración de Tenant.



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, al hacer clic en SI



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.

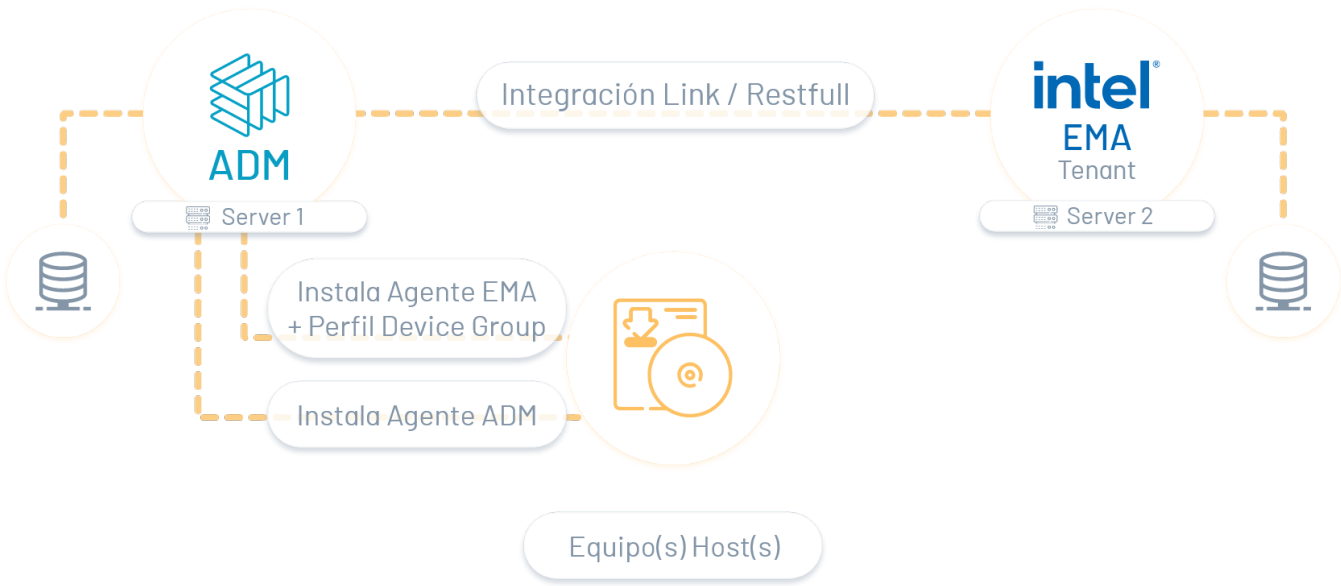
\n## Integración ADM Intel EMA

title: Integración ADM Intel EMA chapter: "intel_ema" —

English

La nueva integración entre Aranda Device Management (ADM) e Intel® Endpoint Management Assistant (Intel® EMA) 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 laConfiguración del API que permite desarrollar e integrar el software de ADM con otras aplicaciones de software.

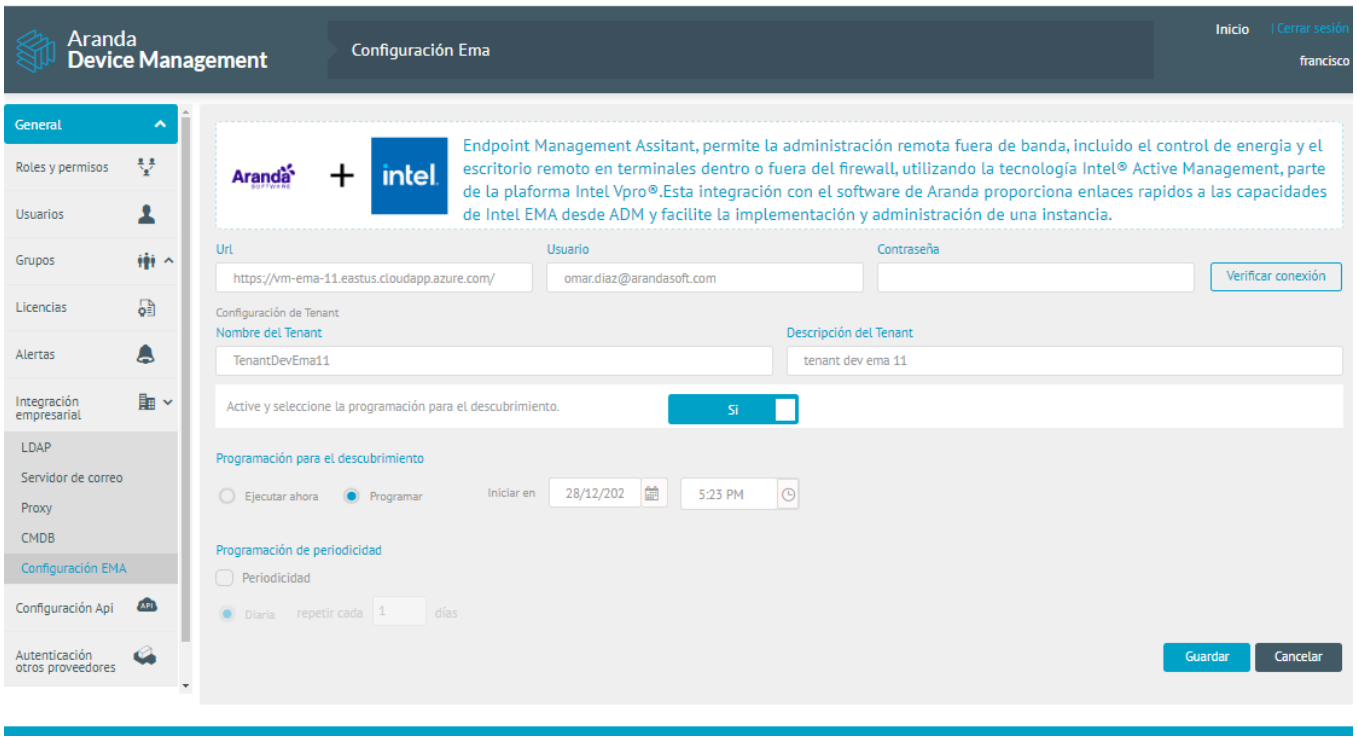
\n## Intel EMA - ADM Integration

title: Intel EMA - ADM Integration chapter: —

Español

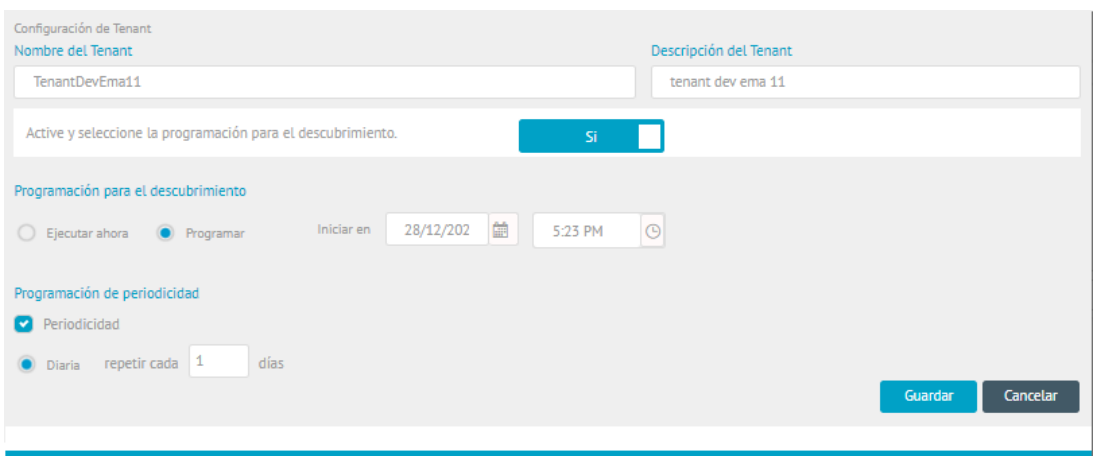
1. To configure the active directory, enter the Configuration view of the ADM administration console, in the**General** section select the**Enterprise Integration** option and **Configuration EMMA**. In the information view, display the option**More Options** and **LDAP**

2. In the information view enter basic information such as url, global administrator user and your password. Click**Verify Connection** and if valid the Tenant configuration is enabled.



Tenant Setup

3. In the Tenant Configuration 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 discovery scheduling by clicking YES



Programming for Discovery

4. A task can be executed immediately or scheduled to synchronize ADM devices with EMA Endpoints. This task is responsible for matching the machines discovered by ADM and the machines that are registered in Intel EMA. (this allows navigation from the ADM console to Intel EMA on a specific device)

5. When you click**Save**, generate the server and the user with Global Administrator for requests with the EMA API, then proceed to create if the Tenant does not exist and finally generate the scheduled task for device synchronization.

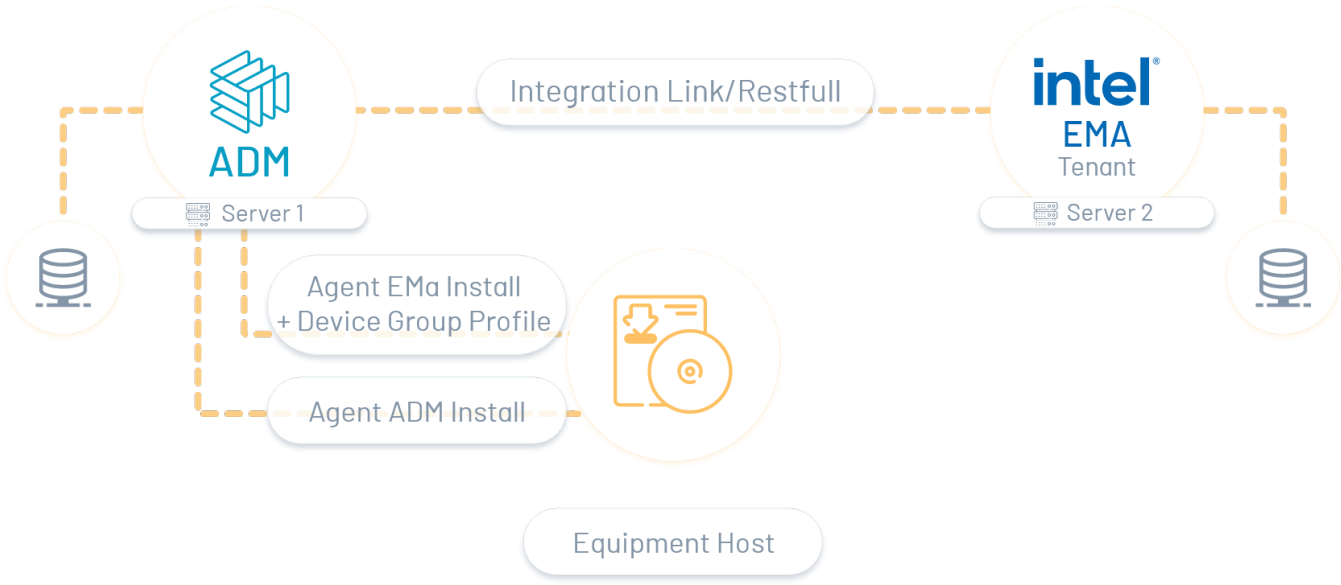
\n## Integration with Intel Ema

title: Integration with Intel Ema chapter: “integracion_ema” —

Español

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 enabling functional capabilities from ADM with Intel® EMA for management and administration.



In the 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 carried out from Intel EMMA must be taken into account:

Intel EMMA Activities	Description
Installation and User Creation	For external integration with Intel EMA the following is required: -installation of the EMA server and creation of the tenant administrator user.
Intel EMMA Agent Generation	Configure and deploy the agent that requires Intel® EMA with its respective tenant group configuration profile (profile that has the Intel® AMT configuration parameters).

2. Activities from ADM

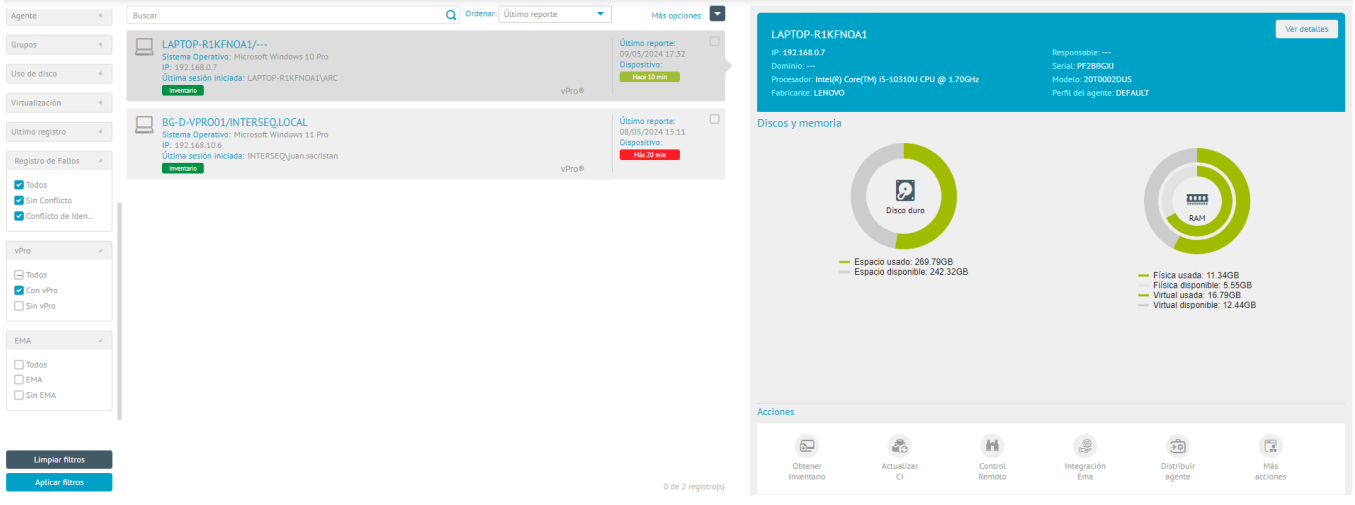
To have an integration, the following tasks to be carried out from ADM must be taken into account:

ADM Activities	Description
Configuration Integration and ADM access	From the ADM administration console you can: - Enable Intel_EMMA integration. - Create the Tenant administrator user. - Access device details within the ADM inventory management process.
API Configuration	From the ADM administration console theAPI Configuration is carried out, which allows developing and integrating the ADM software with other software applications.

\n## Visualización dispositivos compatibles con Intel Ema

title: Visualización dispositivos compatibles con Intel Ema chapter: "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.