
Aranda Device Management

A integração de aplicativos é um processo de comunicação que facilita a troca de informações e serviços, permitindo que o gerenciamento de ativos seja aprimorado e a funcionalidade seja complementada com recursos.

Aranda DEVICE MANAGEMENT fornece as seguintes soluções de integração:

1. Integrações externas

Atualmente, o ADM se integra com os seguintes aplicativos externos:

- Integração com Assistente de gerenciamento de endpoint Intel® (Intel® EMA) Ele permite a administração remota de computadores quando os computadores estão desligados ou o sistema operacional não responde. Usando o Intel® EMA, é possível usar opções de área de trabalho remota e controle de energia, em computadores dentro ou fora do firewall, usando a Intel® Active Management Technology (Intel® AMT), parte da plataforma Intel® vPro™.

2. Integrações internas

O ADM se integra nativamente às nossas soluções:

- Com Controle Remoto Aranda ARC, para assumir o controle das máquinas de forma fácil e eficiente e transferir arquivos de forma conveniente, facilitando o gerenciamento remoto das estações de trabalho.
- Com Aranda CMDB, para manter automaticamente os itens de configuração do CMDB atualizados com as alterações descobertas ou detectadas nos inventários de dispositivos.
- Com Aranda GERENCIADOR DE CONSULTAS AQM Como um sistema avançado de relatórios, permite visibilidade da infraestrutura por meio de indicadores em tempo real e acesso a relatórios personalizados.

Para quem é este Manual?

Este manual foi elaborado para compartilhar e aprofundar as possíveis integrações entre Aranda DEVICE MANAGEMENT ADM e diferentes aplicativos.

O que é a nossa documentação?

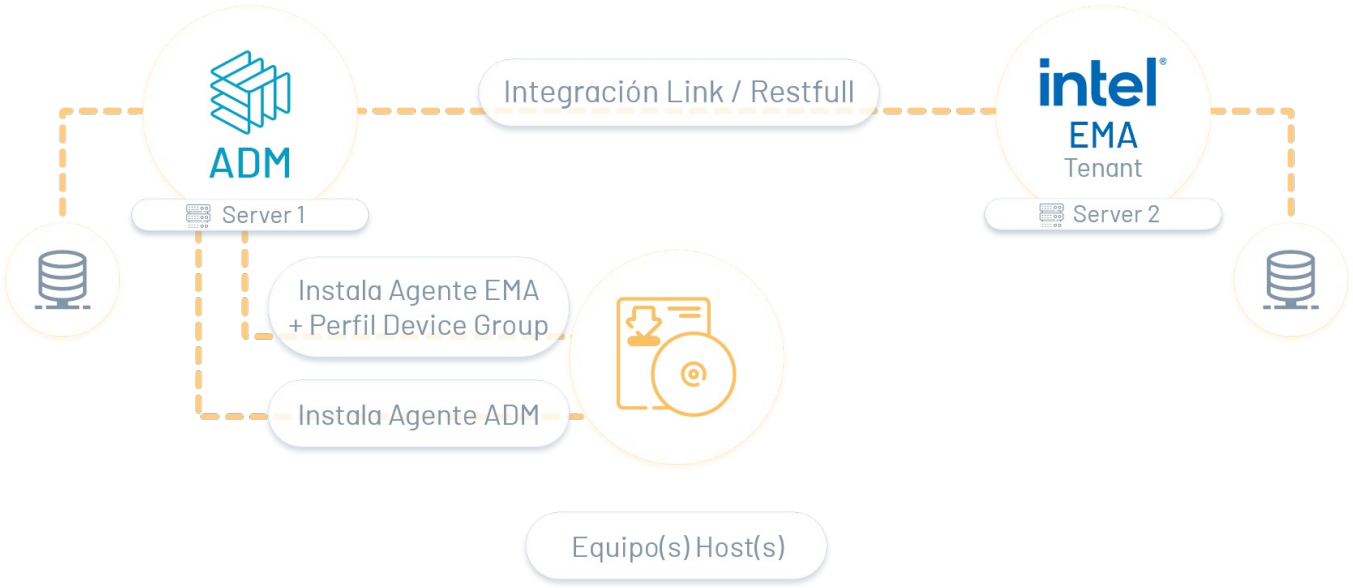
- Guia de introdução do ADM ↪ de gerenciamento de dispositivos Aranda
- Guia de instalação do Aranda Device Management ADM ↪
- Manual de gerenciamento de ↪ dispositivos Aranda
- Manual de Integração ADM (Você está AQUI)

Integração Intel Ema ADM

Integração Intel EMA ADM

A nova integração entre o Aranda Device Management (ADM) e o Intel® Endpoint Management Assistant (Intel® EMA) permite o gerenciamento remoto de computadores quando os computadores estão desligados ou o sistema operacional não está respondendo.

Esta é uma sincronização silenciosa, onde o ADM processa e verifica as informações registradas pelo Intel® EMA, permitindo assim recursos funcionais do ADM com o Intel® EMA para seu gerenciamento e administração.



Na integração, diferentes atividades são realizadas em paralelo para levar em consideração e São utilizados diferentes componentes que permitem o correto funcionamento das aplicações interna e externamente.

1. Atividades da Intel EMMA

Para ter uma integração, as seguintes tarefas a serem executadas a partir do Intel EMMA devem ser levadas em consideração:

Atividades do Intel EMMA	Descrição
Instalação e criação do usuário	Para integração externa com Intel EMA é necessário:- Instalação do servidor EMA e criação de usuário administrador de locatários.
Geração de agente Intel EMMA	Configurar e implantar o agente exigido pelo Intel® EMA com seu respectivo perfil de configuração do grupo de locatários (perfil que tem os parâmetros de configuração do Intel® AMT).

2. Atividades do ADM

Para ter uma integração, as seguintes tarefas a serem executadas a partir do ADM devem ser levadas em consideração:

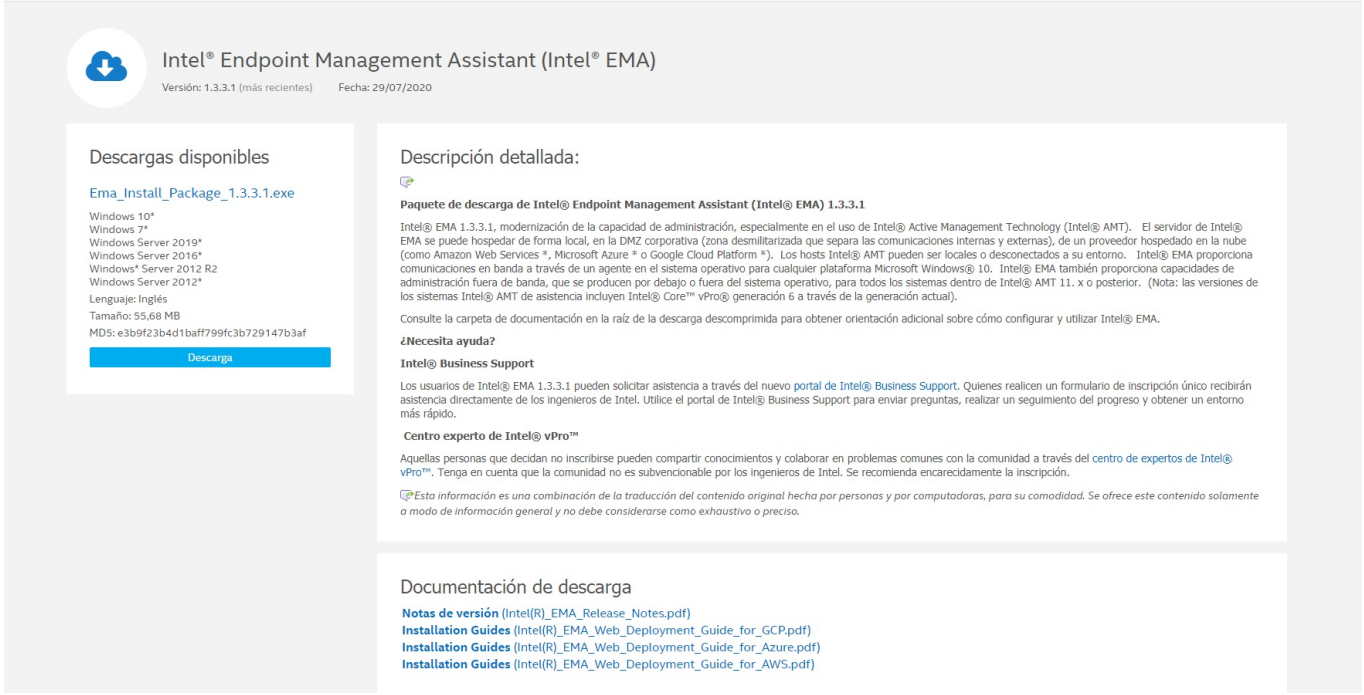
Atividades do ADM	Descrição
Integração de configuração e acesso ADM	No Console de Gerenciamento do ADM, você pode: - Ativar integração Intel_EMMA. - Criar o usuário administrador do locatário. - Acesse os detalhes do dispositivo dentro do processo de gerenciamento de estoque da ADM.
Configuração da API	No console de gerenciamento do ADM, o Configuração da API que permite que o software ADM seja desenvolvido e integrado a outros aplicativos de software.

Instalação do servidor EMA

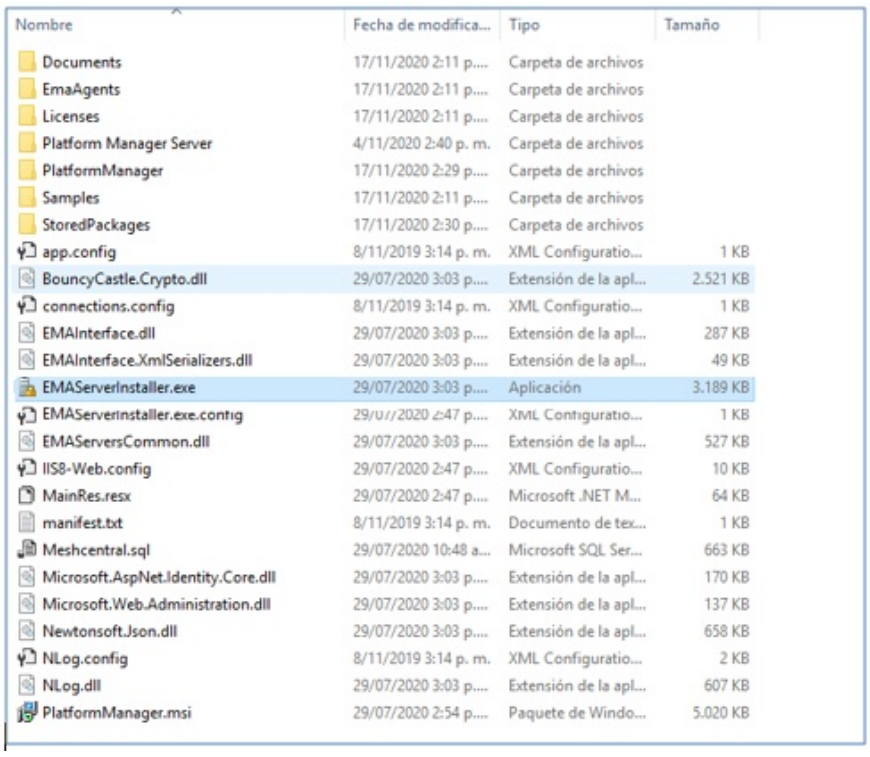
A seguir, descrevemos a instalação básica do Intel EMA para integração com o ADM.

> ⚐ Nota: Para todos os aspectos de configuração, considerações e instalação, consulte o Documentação oficial da Intel EMA

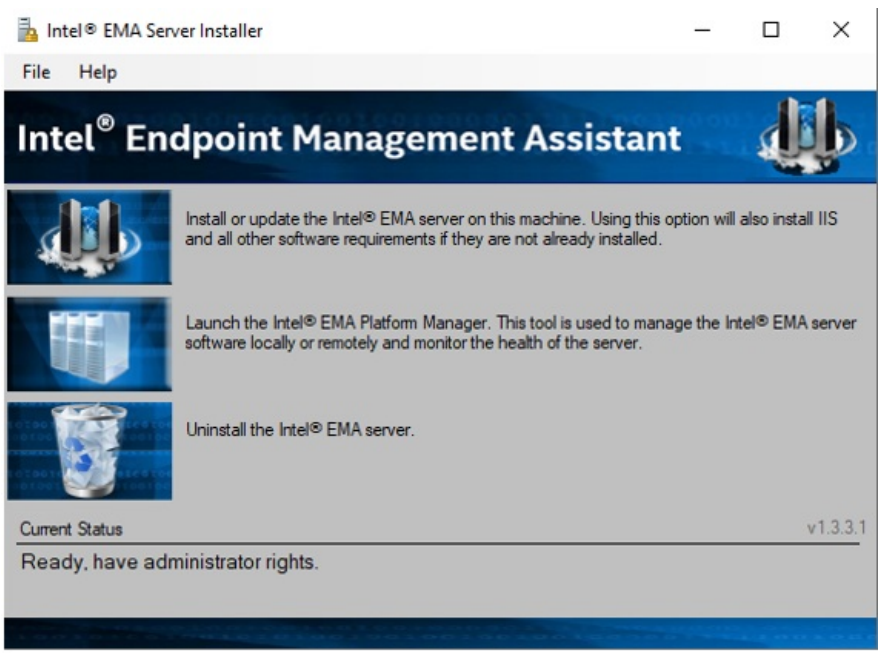
1. Baixe os pacotes de instalação do Ema no seguinte caminho: Assistente de gerenciamento de endpoint Intel-Intel-EMA



2. Ejecute el archivo EMAServerInstaller.exe.

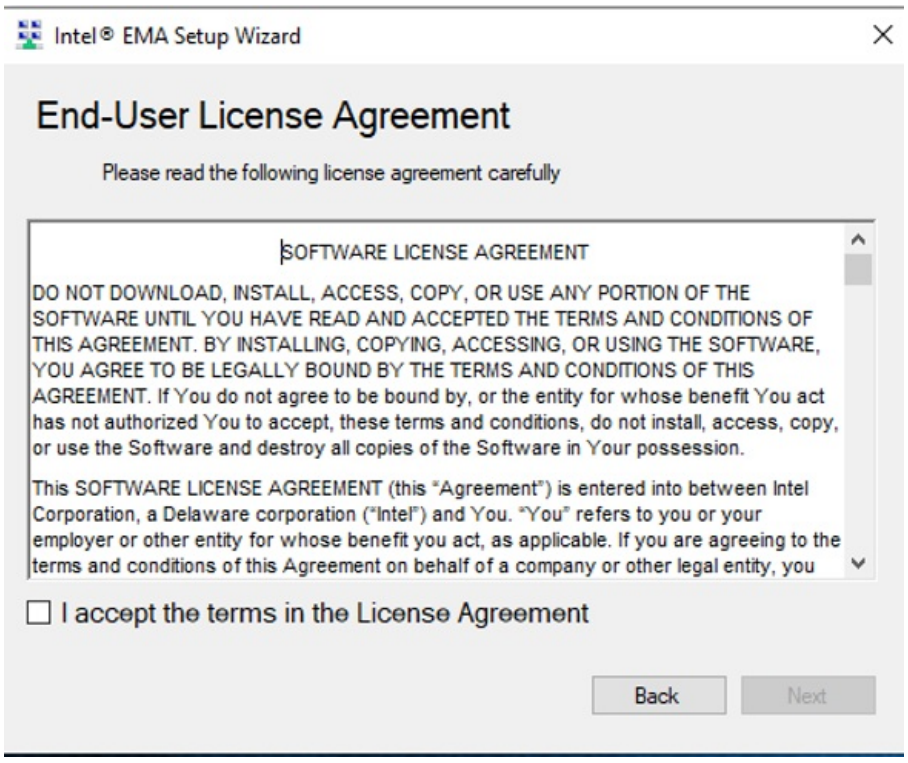


3. Instale o servidor Ema e selecione a opção 1.

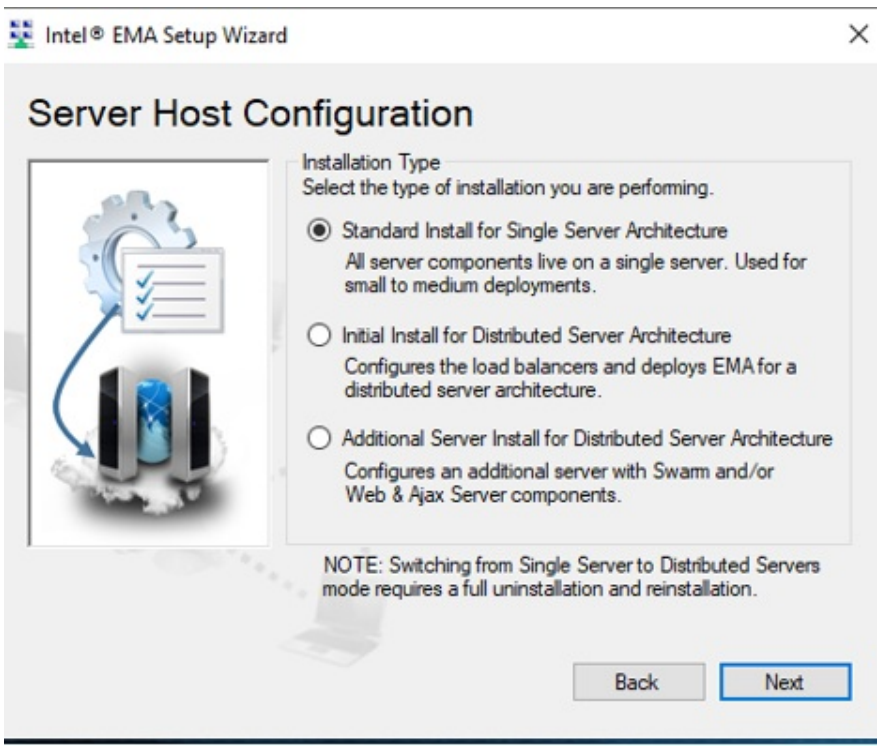


4. Você deve atender à recomendação de ter o IIS configurado para o sistema operacional Windows.

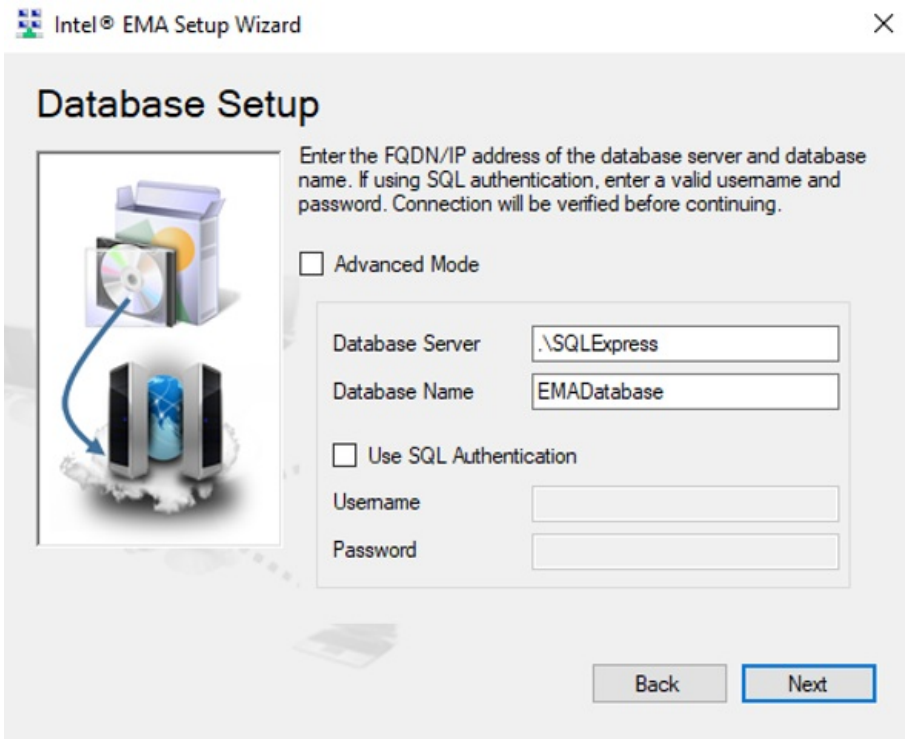
5. Lea el acuerdo de instalación y hacer clic en Siguiente.



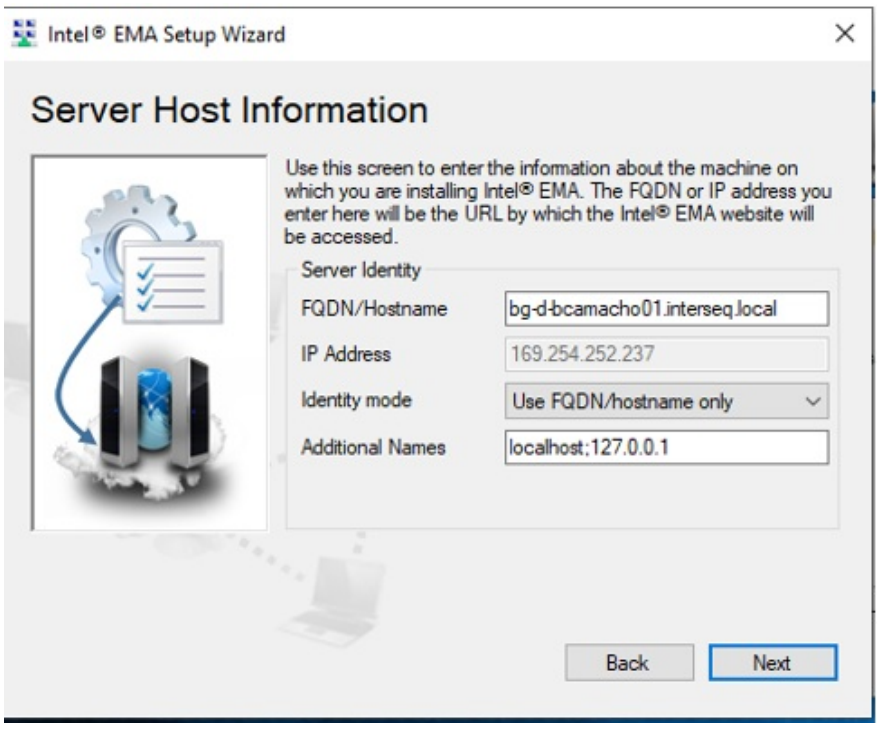
6. Selecione o tipo de instalação:



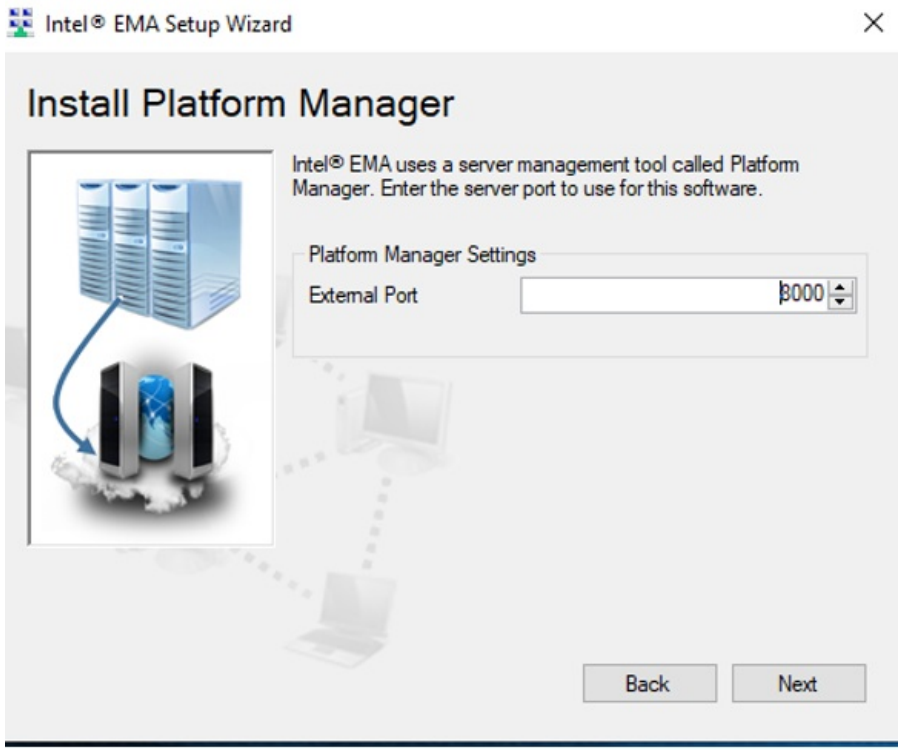
7. Seleccione la instancia de base de datos Sql Server.



8. Configure as informações do host.



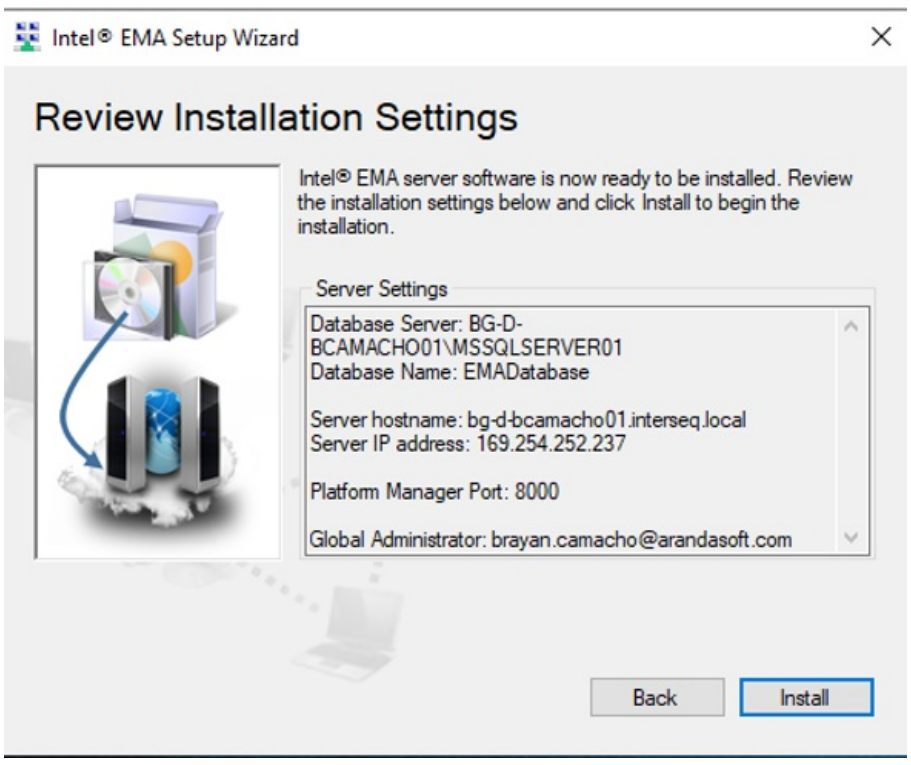
9. Instale o Platform Manager.



10. Configure o tipo de autenticação do usuário.

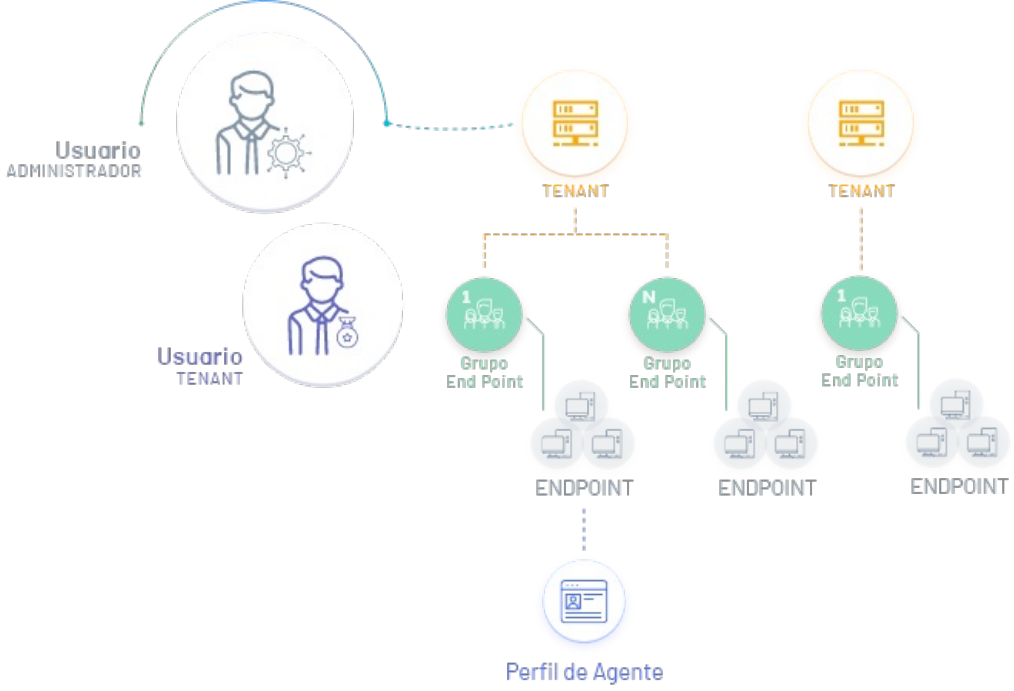
11. Adicione o nome de usuário administrador para toda a instância do EMA e salve as credenciais para o gerenciamento geral do EMA.

12. Clique Instalar.

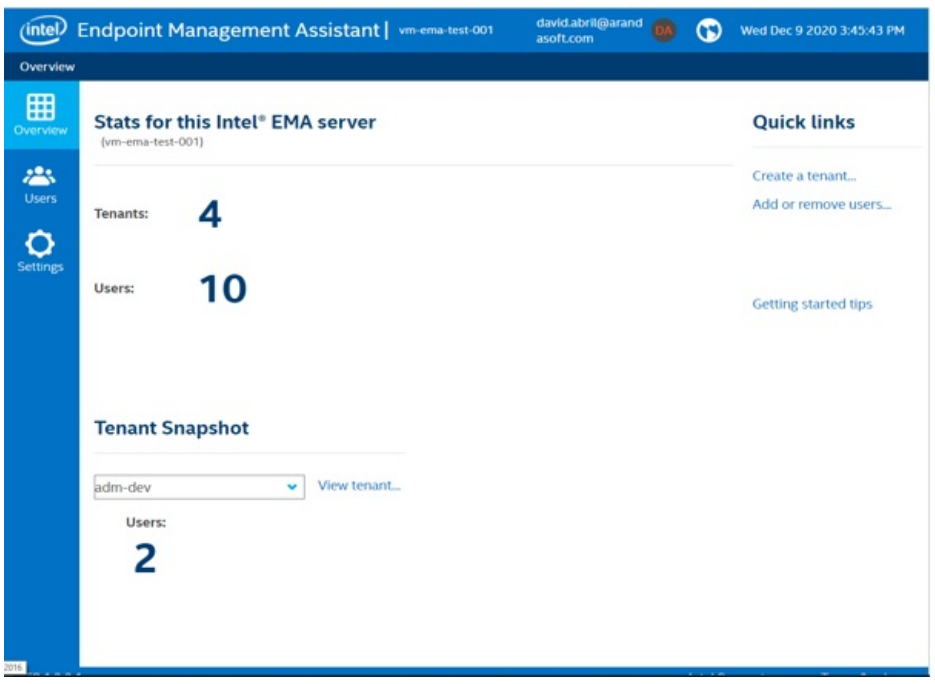


Configuração de locatários e grupos de endpoints

Neste estágio de configuração do Intel EMA, as permissões são definidas no nível de hierarquia no aplicativo, onde o administrador local cria os locatários e, em seguida, os grupos de perfis de endpoint, endpoint e agente.



1. Faça login no console do Enpoint Management Assistant como Administrador Global, com o usuário configurado durante a instalação. Enn a opção Visão geral No menu principal, você poderá ver os status definidos.

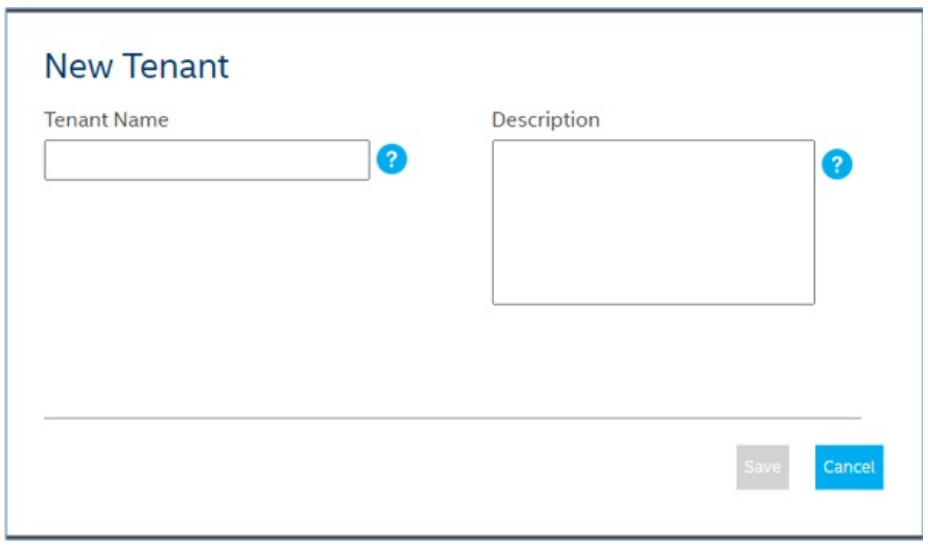


Criar Ternant

2. Para criar o locatário na seção Links Rápidos da exibição de informações, selecione o Criar um locatário. A janela para inserir o nome e a descrição está ativada.

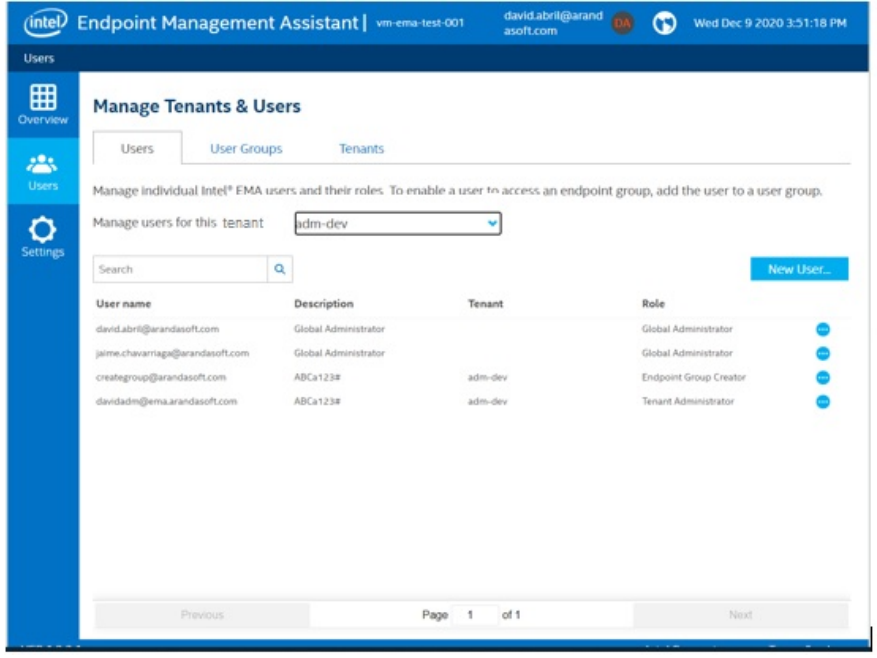
Este é o locatário que você integrará ao ADM (se você estiver usando a instância EMA para sincronizar diferentes instâncias do ADM, deverá criar um locatário para cada instância, é recomendável usar o nome do cliente para diferenciar). }

3. Quando a configuração estiver concluída, clique em Salvar.

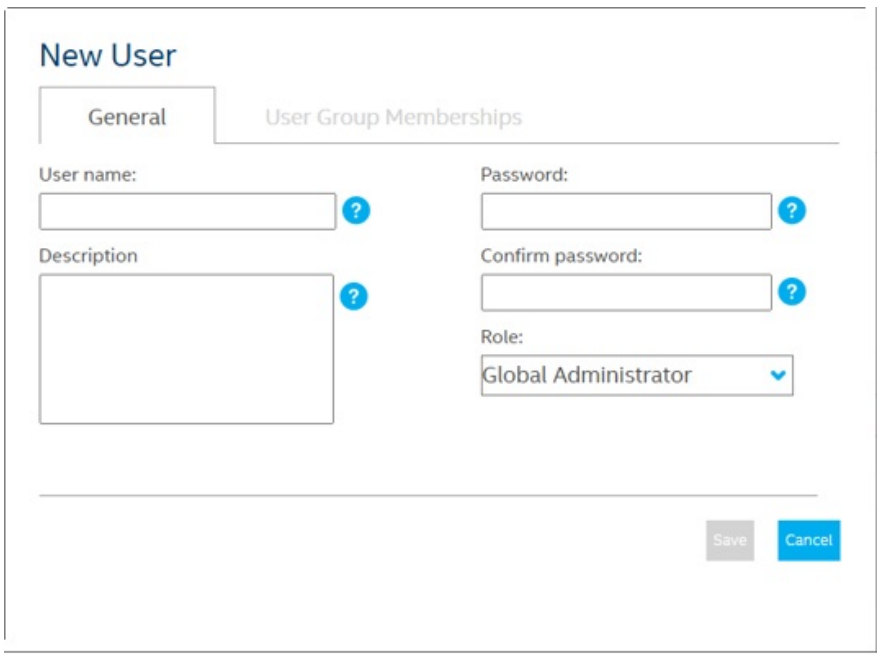


Criar usuários

4. Para criar usuários adicionais para o locatário (administrador global, colaborador do locatário etc.) na seção Links Rápidos da exibição de informações, selecione a opção Adicionar ou remover usuários. A janela está ativada Gerenciar locatários e usuários onde você pode preencher as respectivas informações.



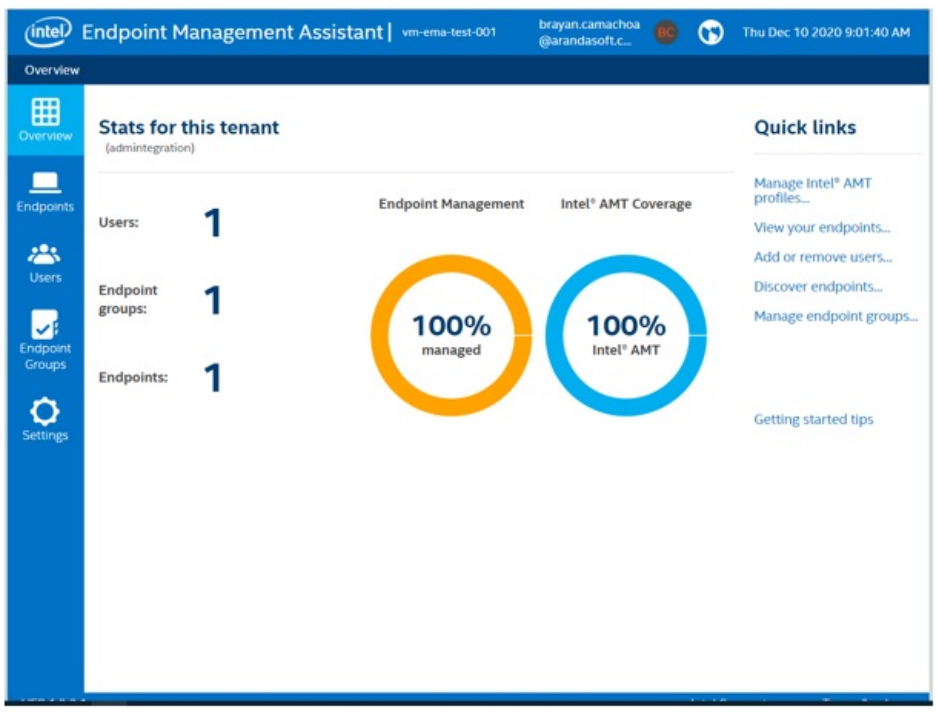
5. No Usuários Selecione o ícone Novo usuário E na janela habilitada você pode inserir informações como nome de usuário, descrição, senha e função associada ao usuário.
6. Quando a configuração estiver concluída, clique em Salvar.



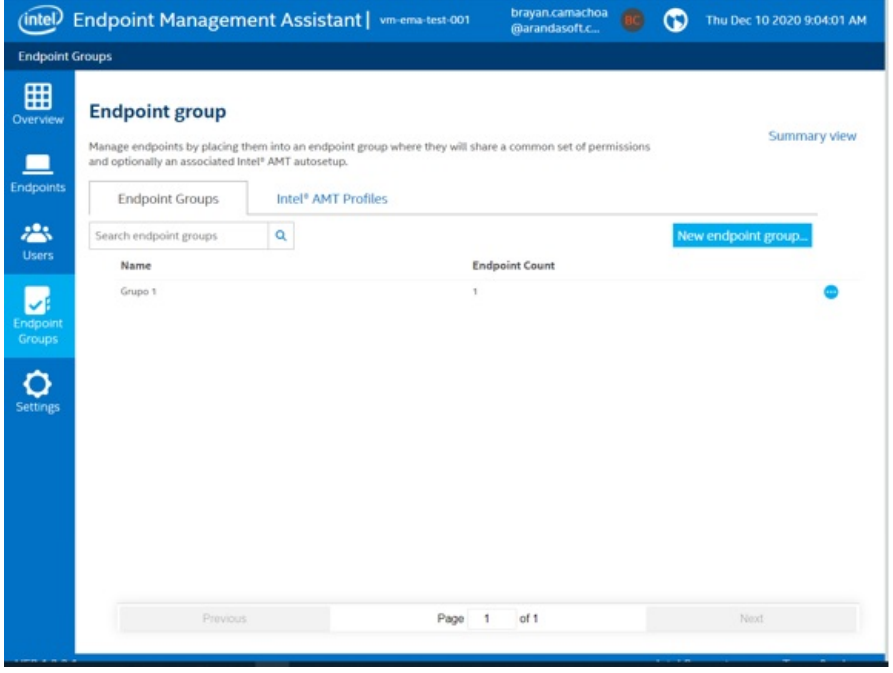
Gerar agente Intel EMA

Criar grupo de endpoints

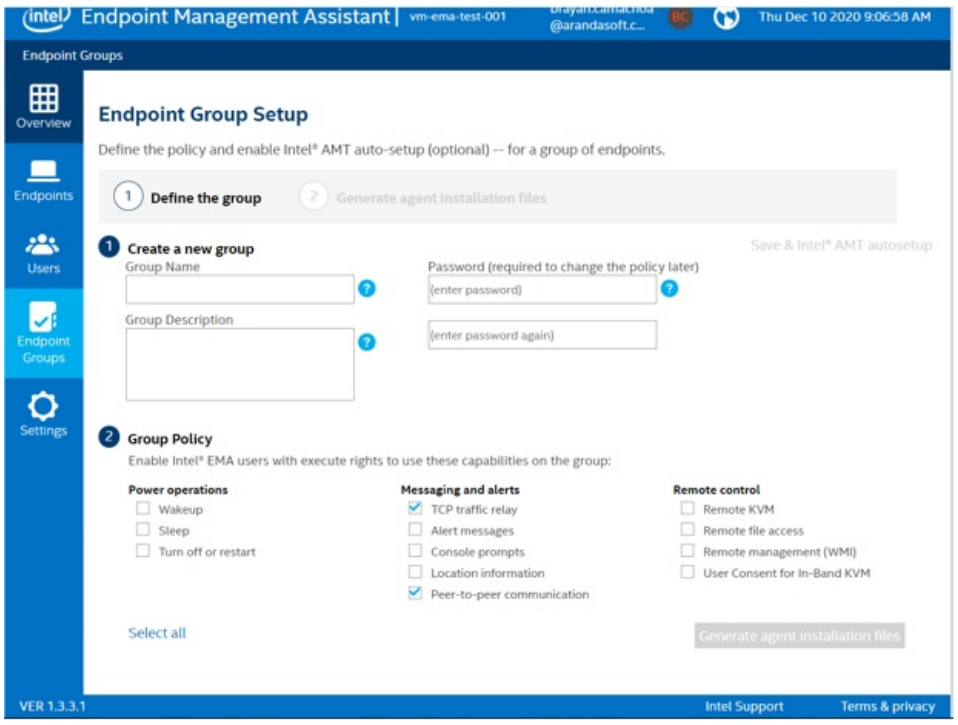
1. Faça login no console do Enpoint Management Assistant como administrador de tenants e selecione a opção Grupo de endpoints no menu principal.



2. Na visualização de informações de Grupo de endpoints Selecione a opção Novo grupo de endpoints.

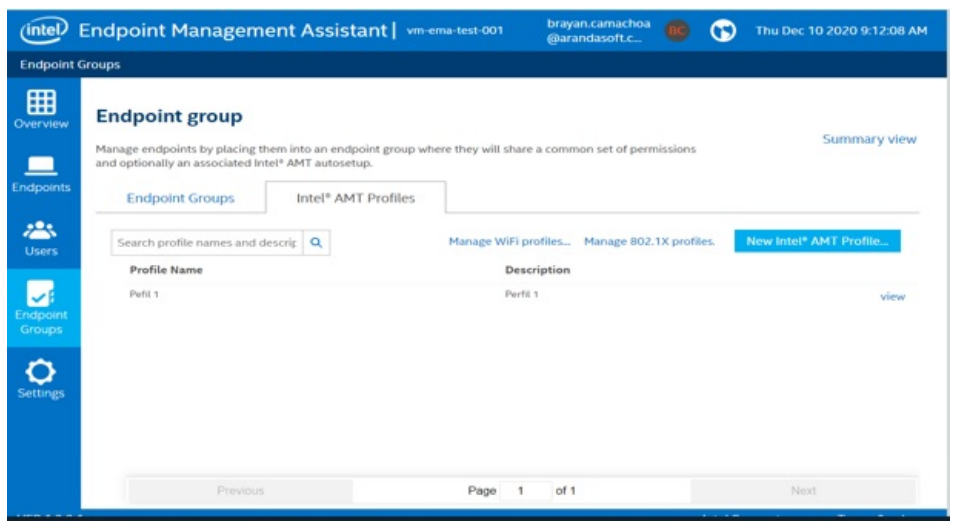


3. Nas configurações do grupo, insira nome, descrição, senha e políticas de acordo com os recursos do grupo. Quando terminar, clique no botão Gerar arquivos de instalação do agente (Gerar arquivo de instalação do agente)

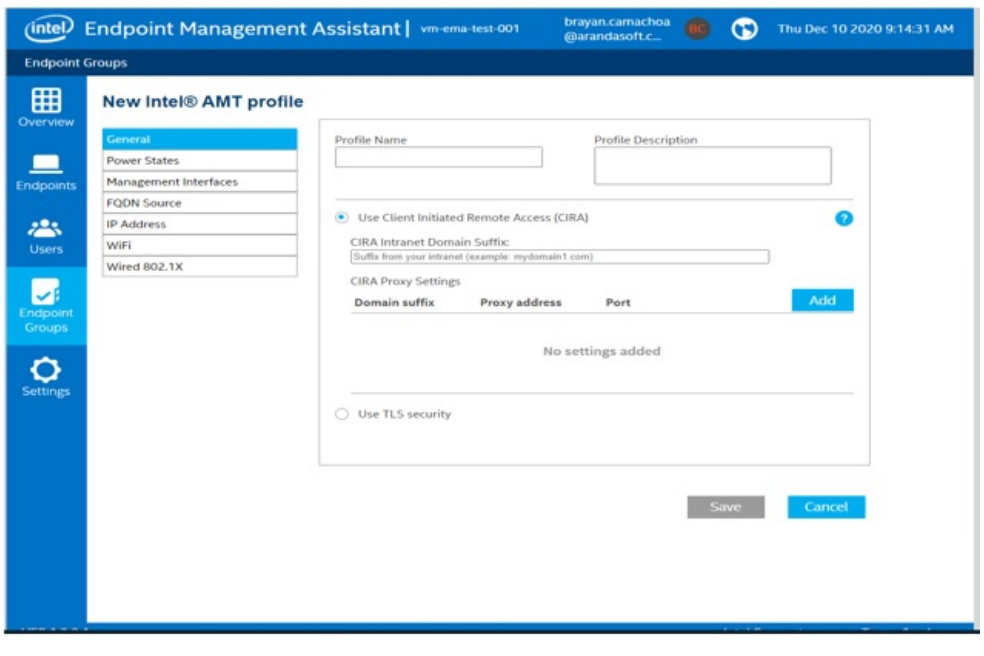


Perfil AMT

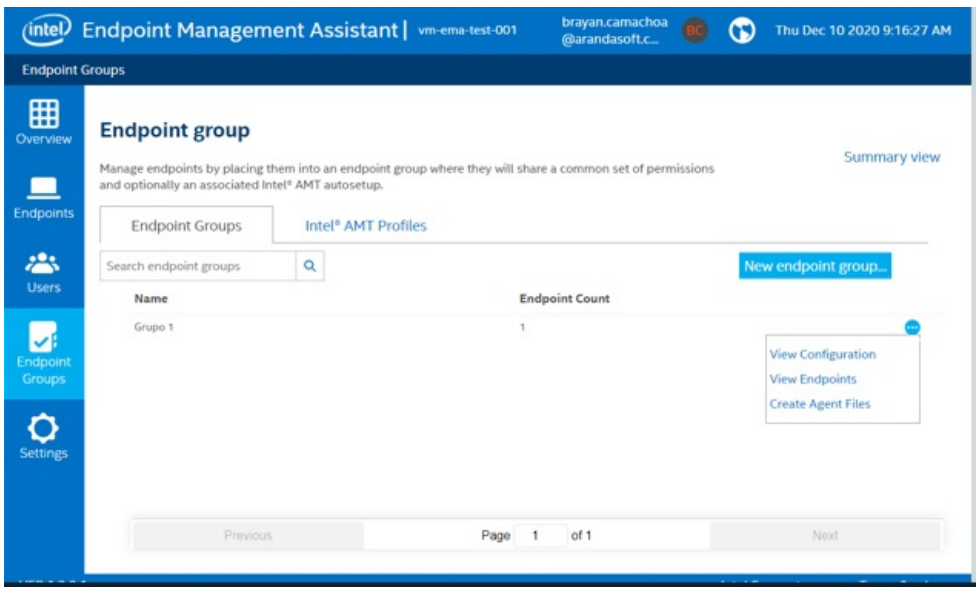
4. No Grupos de endpoints Selecione a opção Gerar um perfil AMT.



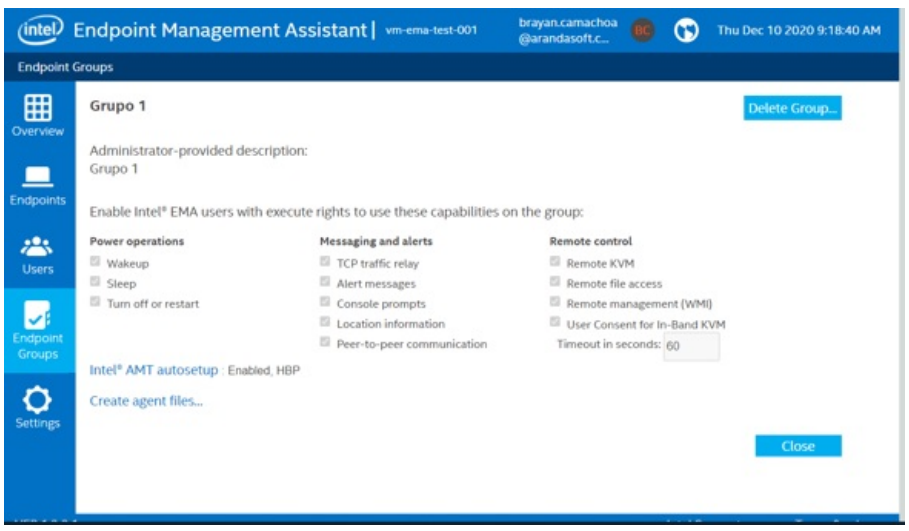
5. Configure as informações relacionadas ao perfil AMT.



6. Atribua o perfil AMT ao pool de pontos de extremidade.

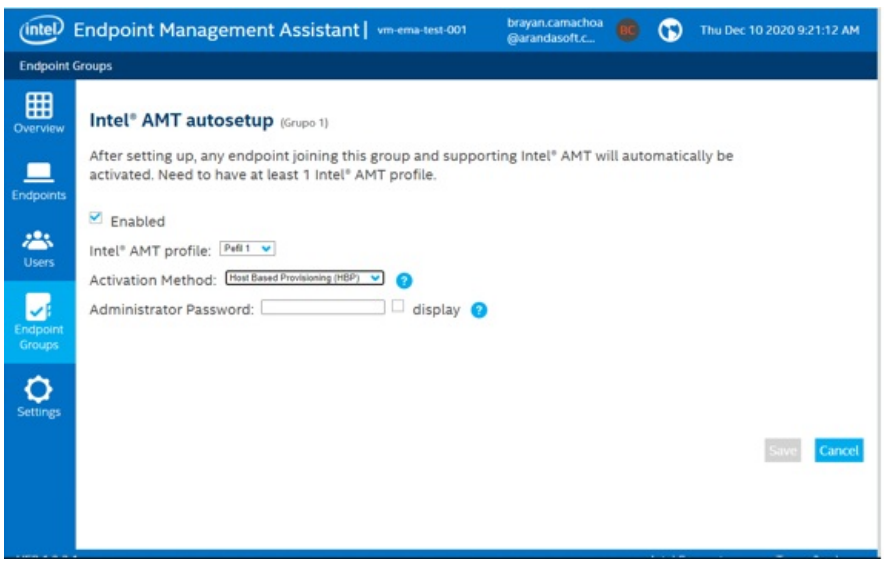


7. No grupo, clique no ícone Configuração automática da Intel AMT.

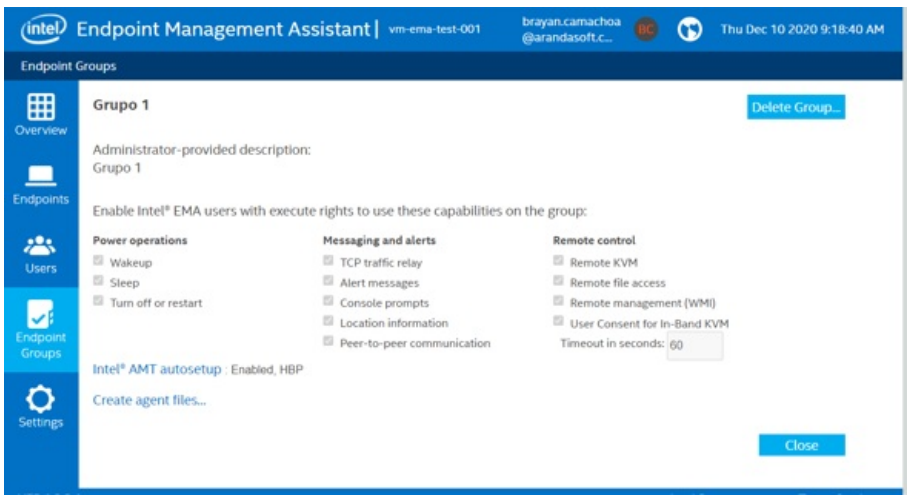


8. Selecione o perfil AMT e o método de ativação. Digite a senha do BIOS; Como administrador de TI, certifique-se de que todos os computadores tenham a mesma senha para que esse perfil funcione para eles quando forem instalados.

⚐ Nota: Por padrão, em equipamentos de informática, a senha é "admin". Recomenda-se revisar a duplicação do modelo do dispositivo.

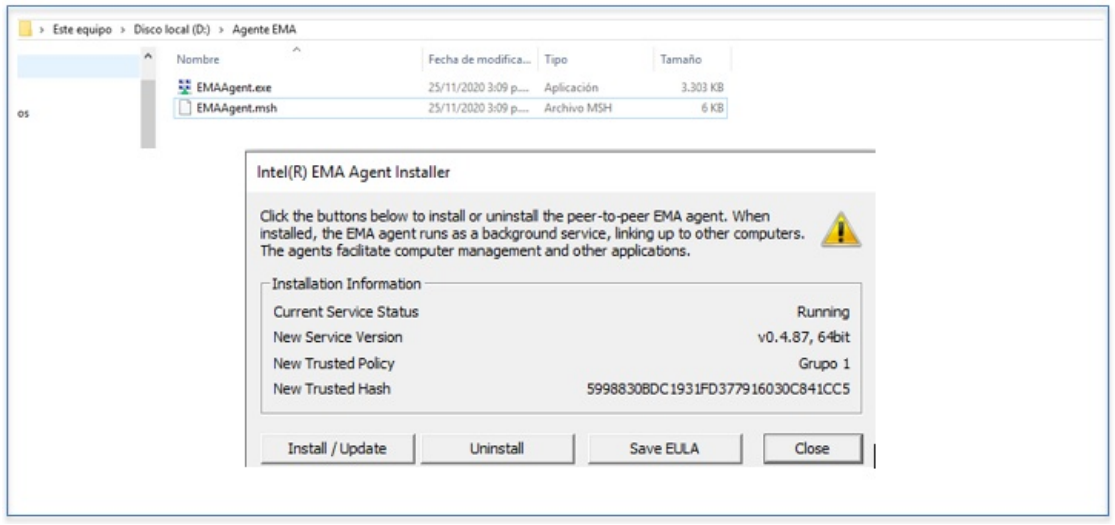


9. No grupo, clique no ícone Criar arquivos de agente (Criar arquivo do agente).



9. Selecione a versão do agente, baixe o serviço e as políticas do agente.

⚐ Nota: Na máquina cliente, que deve ser referenciada pela EMA, você deve ter os dois arquivos (executável e configuração) no mesmo caminho, com o mesmo nome e executar EMAAgent.exe.



⚐ Nota: As máquinas que suportam EMA são aquelas que possuem firmware igual ou superior à versão 11, geralmente suportadas por processadores de 7ª geração, alguns processadores de 6ª geração também o suportam.

- As versões de firmware só podem ser atualizadas em subversões da versão que vêm de fábrica. Isso quer dizer que um processamento de 10 gerações não pode ser atualizado de FW 14 para FW 15; O que ele pode fazer é atualizar de 14.1 para 14.2, 14.3, etc.

Tabela de firmwares Intel® ME

Versão FW	Geração do processador	TLS	Suportado pela EMA
15.xx.xx.xxx	11ª Geração	1.2	X
14.xx.xx.xxx	10ª Geração	1.2	X
13.xx.xx.xxx	9ª Geração	1.2	X
12.xx.xx.xxx	8ª Geração	1.2	X
11.xx.xx.3xx	7ª Geração / 6ª Geração	1.2 1.1	X
10.xx.xx.3xx	6ª Geração	1.1	Parcialmente
9.xx.xx.3xx	5ª Geração	1.0	
8.xx.xx.3xx	4ª Geração	1.0	

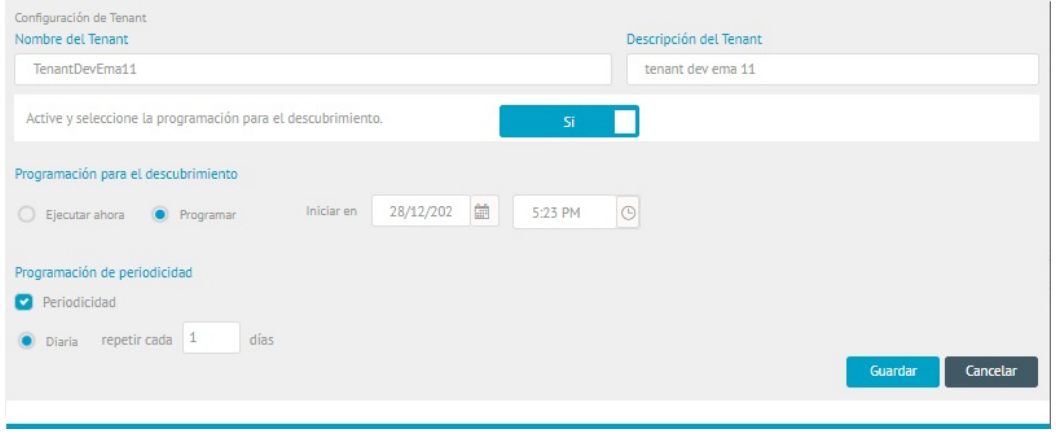
Ativar a integração do ADM - Intel EMA

1. Para configurar o Active Directory, vá para a visualização Configuração do Console de Gerenciamento do ADM, na seção Geral Selecione a opção Integração empresarial e Configuração EMMA. Na visualização de informações, exiba o Mais opções e LDAP

2. Na visualização de informações, insira as informações básicas, como url, usuário administrador global e sua senha. Clique Verificar conexão e, se válida, a configuração Locatário está habilitada.

Configuração do locatário

3. Na seção Configurações do locatário, você poderá inserir o nome do locatário criado anteriormente durante a verificação do console EMA e a descrição do locatário. Ative a opção de agendamento para descoberta clicando em SIM



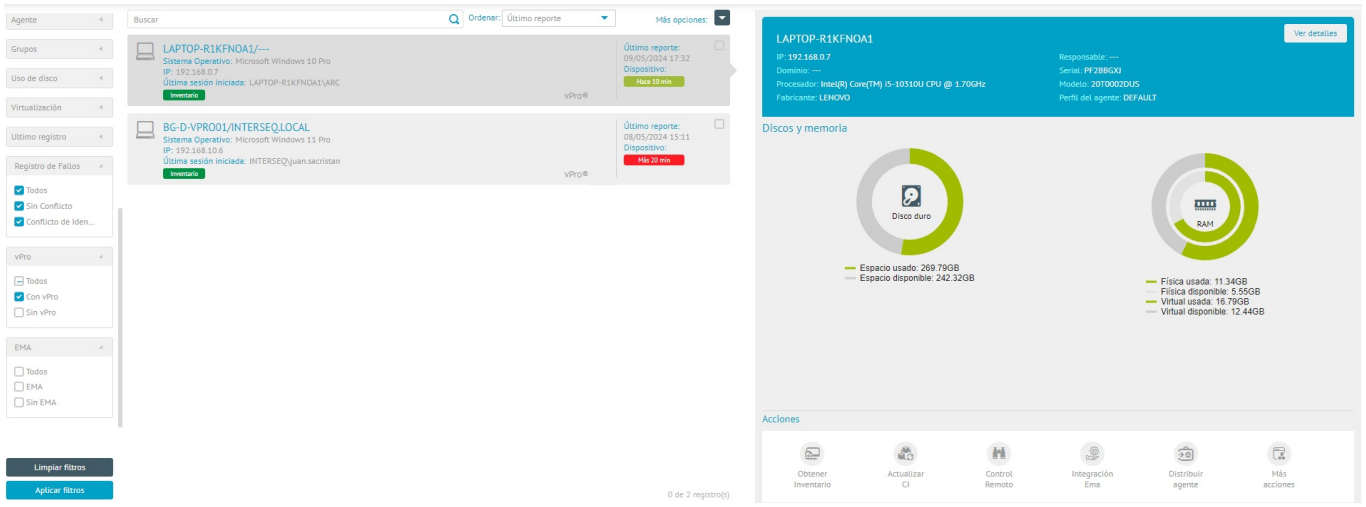
Programação para descoberta

4. Você pode executar imediatamente ou agendar uma tarefa que permita sincronizar dispositivos ADM com endpoints EMA. Essa tarefa é responsável por combinar as máquinas descobertas pelo ADM e as máquinas registradas no Intel EMA. (isso permite que haja uma navegação do ADM consla para Intel EMA em um dispositivo específico)

5. Clicando Salvar, gera o servidor e o usuário com o Administrador Global para as solicitações com a API EMA, depois passa a criar se o Tenant não existir e, finalmente, gera a tarefa agendada para a sincronização dos dispositivos.

Exibir dispositivos compatíveis com Intel EMA

Na lista de dispositivos você pode ver os computadores que possuem um processador Vpro, você pode usar os filtros para listar apenas os dispositivos que possuem esse tipo de processador.

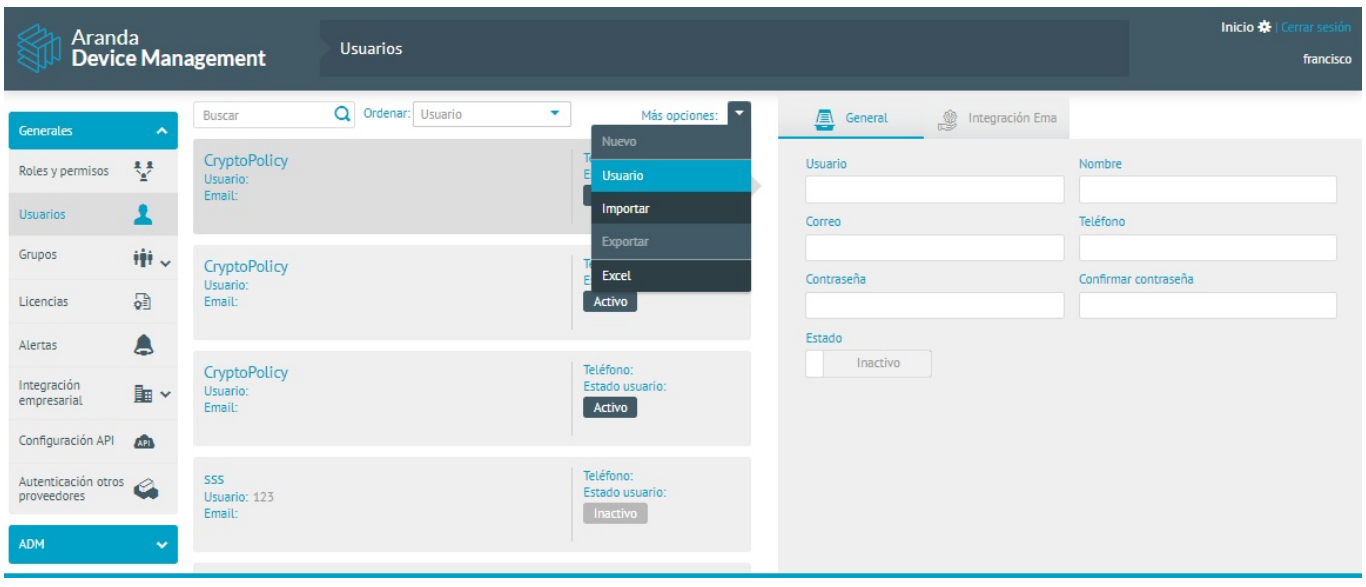


Com esses dispositivos, você poderá acessar todas as funcionalidades do Intel Ema após instalar o agente.

Criação de usuário administrador de locatário EMA

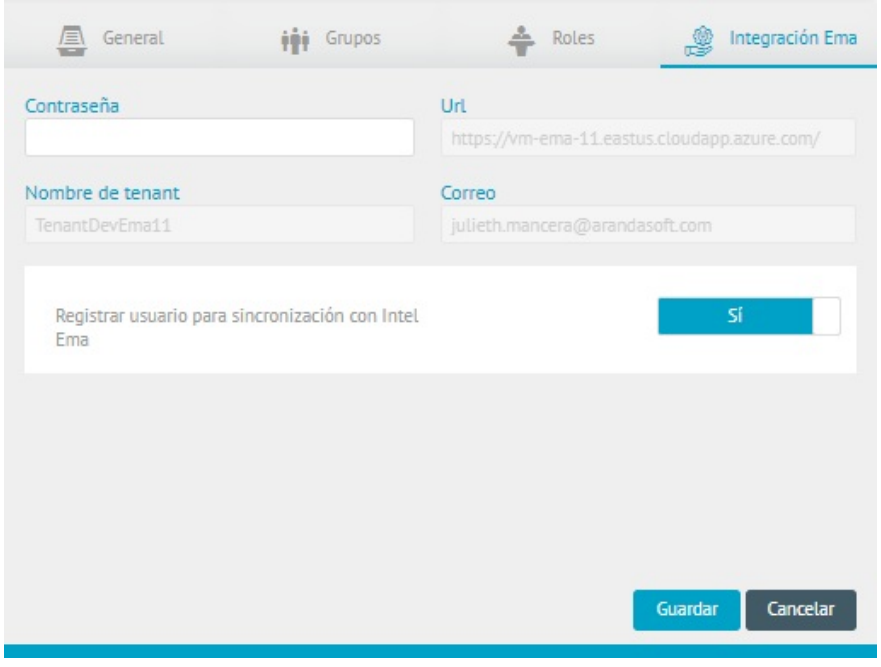
1. Para criar o usuário Emma Tenant Admin, vá para a visualização Configurações do ADM Management Console no Geral Selecione a opção Integração empresarial e LDAP. Na visualização de informações, exiba o Mais opções e Utilizador.

2. Na Visualização de detalhes do usuário, selecione o Geral onde você pode preencher os dados gerais do usuário a serem integrados à EMA como administrador de locatários e definir se seu status é ativo ou inativo.



⚐ Nota: O usuário deve ter um email válido configurado para criar o usuário Administrador de Locatários.

3. Na Visualização de detalhes do usuário, selecione o Integração Ema e digite a chave do usuário e ative o usuário da EMA; Você pode registrar o usuário como o usuário a ser usado para sincronizar.



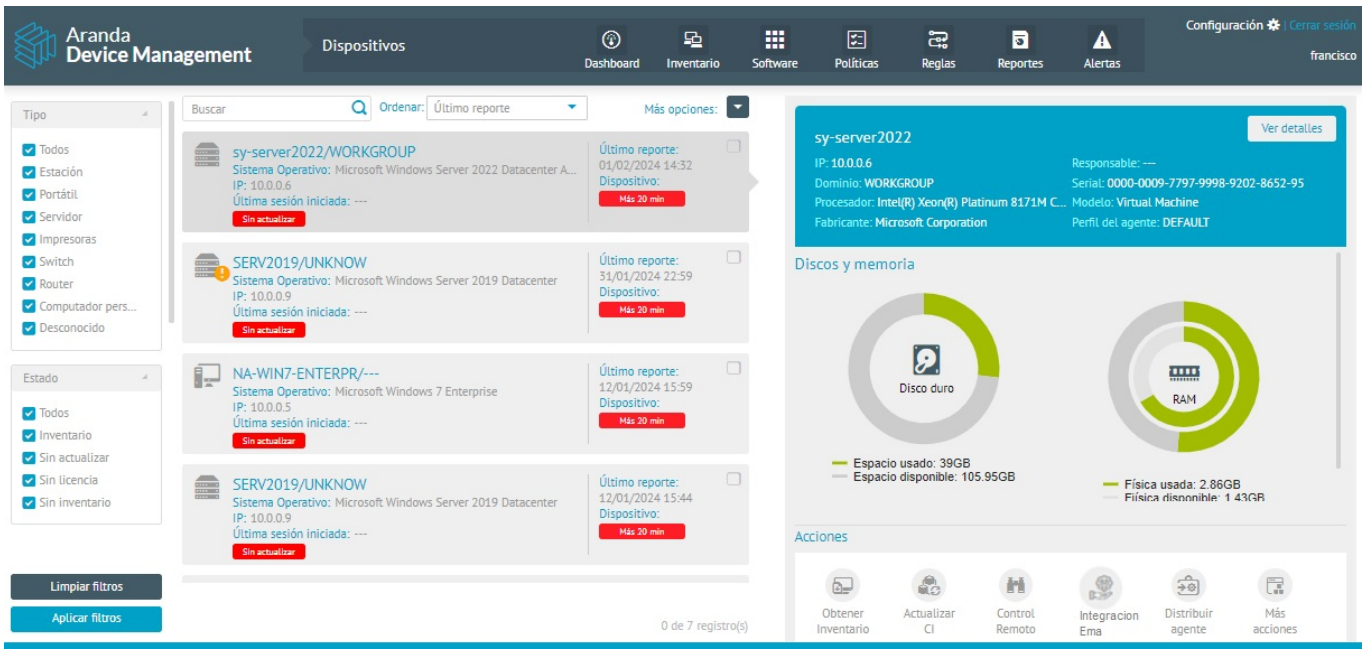
4. Quando terminar de configurar as informações básicas do usuário, clique em Salvar para confirmar as alterações feitas; na Exibição de detalhes, as guias Grupos e Funções estão ativadas

Acesso direto com EMA

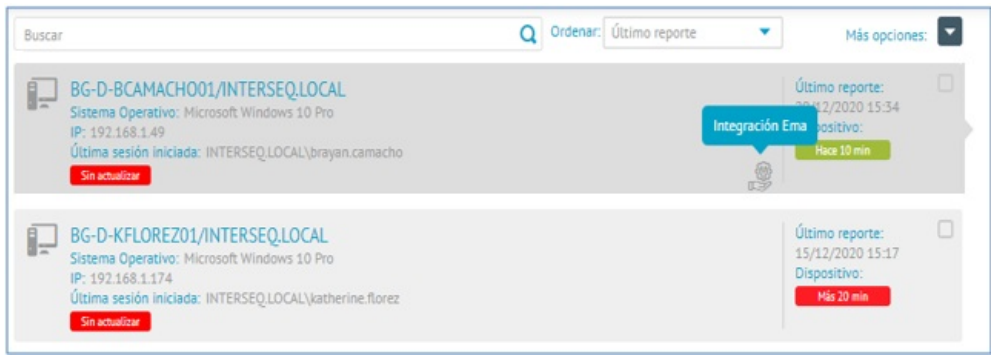
Uma vez concluído todo o processo de configuração e após a execução da tarefa de sincronização entre o ADM e o Intel EMA, o usuário poderá navegar dos detalhes de um dispositivo ADM para o console do EMA e realizar as operações necessárias.

Acesso a partir do ADM

1. Entre na visualização inicial do ADM Management Console e selecione o módulo Inventário e o menu Dispositivos. Na visualização de informações, a lista de dispositivos inventariados pode ser exibida.

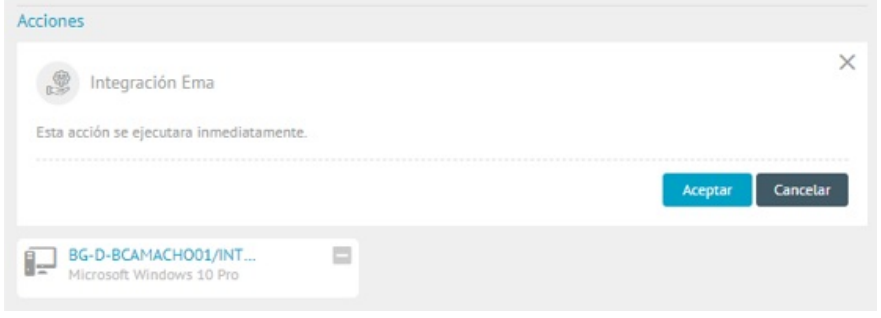


⚐ Nota: Se o dispositivo estiver sincronizado com a EMA, você poderá ver o logotipo da EMA.Integração EMA na lista de dispositivos.



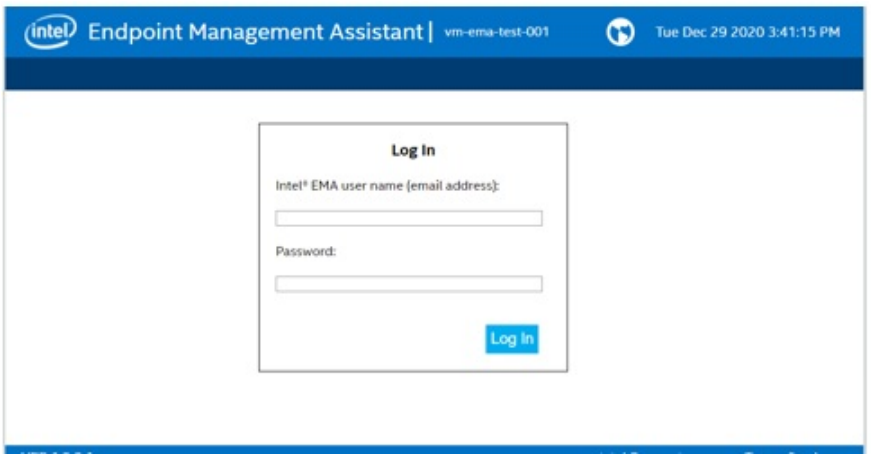
2. Na visualização Detalhes do dispositivo integrado, selecione o ícone Integração Ema

3. Na exibição de detalhes do dispositivo, a ação descrita está habilitada. Clique Aceitar, para redirecionar o processo para o console Assistente de gerenciamento de nomeação

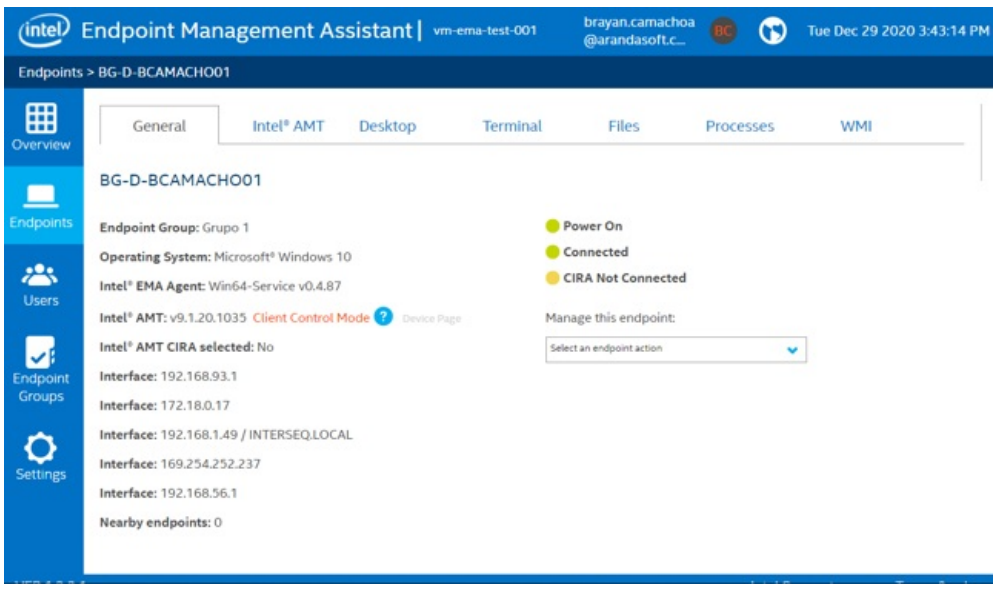


Acesso a partir do Intel EMMA

4. Se o usuário já estiver autenticado no console da EMA, ele poderá acessar o dispositivo diretamente, caso não esteja, o sistema solicitará credenciais para fazer login como usuário administrador de locatários, criado durante o processo de configuração ou no Criação de usuário administrador de locatário da EMA.



Uma vez autenticado, o usuário poderá visualizar o endpoint (dispositivo) para acessar o endpoint (dispositivo) para executar ações de gerenciamento do Intel EMA.



Controle remoto ARC

Controle remoto (ARC)

Ele permite que você assuma o controle das máquinas de forma simples e eficiente e transfira arquivos de forma conveniente, facilitando o gerenciamento remoto das estações de trabalho.

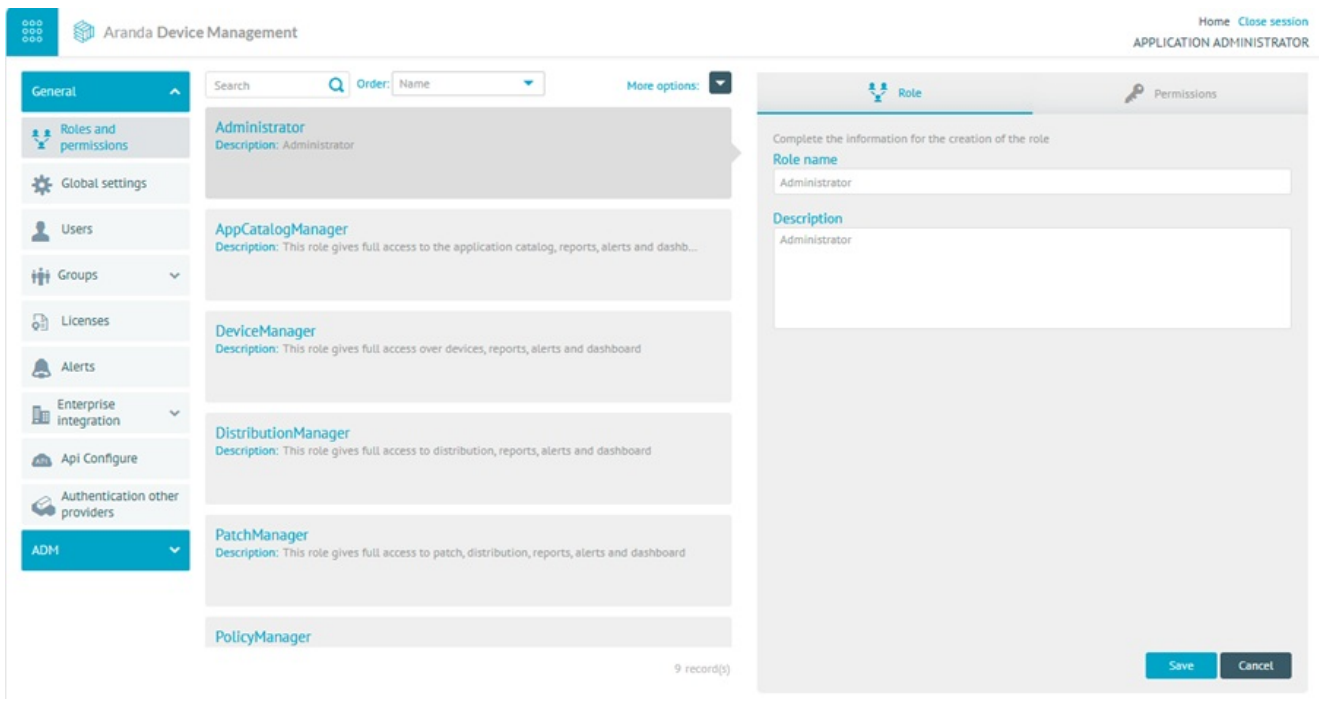
⚐ Nota: Considere a seguinte arquitetura com suporte para controle remoto:

- Essa funcionalidade não é compatível com versões de agente lançadas do ADM anteriores a 9.19.2 (Cloud)
- Essa funcionalidade não é compatível com instalações locais de versões do ADM anteriores à 9.21.1

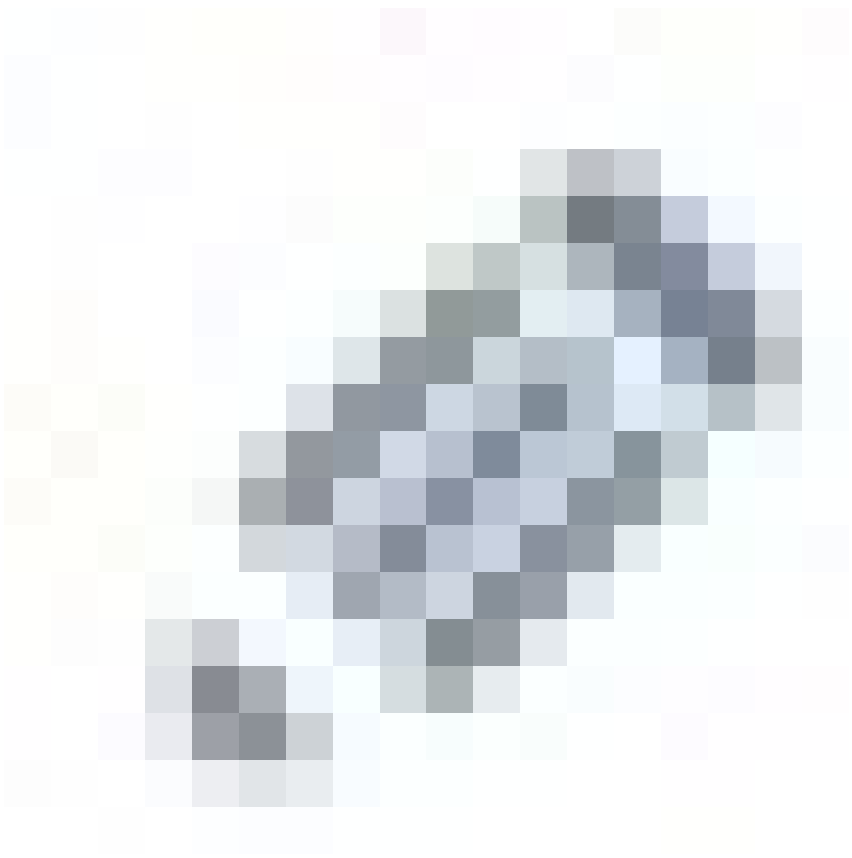
Processo de configuração de instalação local

Você deve considerar as seguintes etapas para configuração de controle remoto em instalações OnPremise:

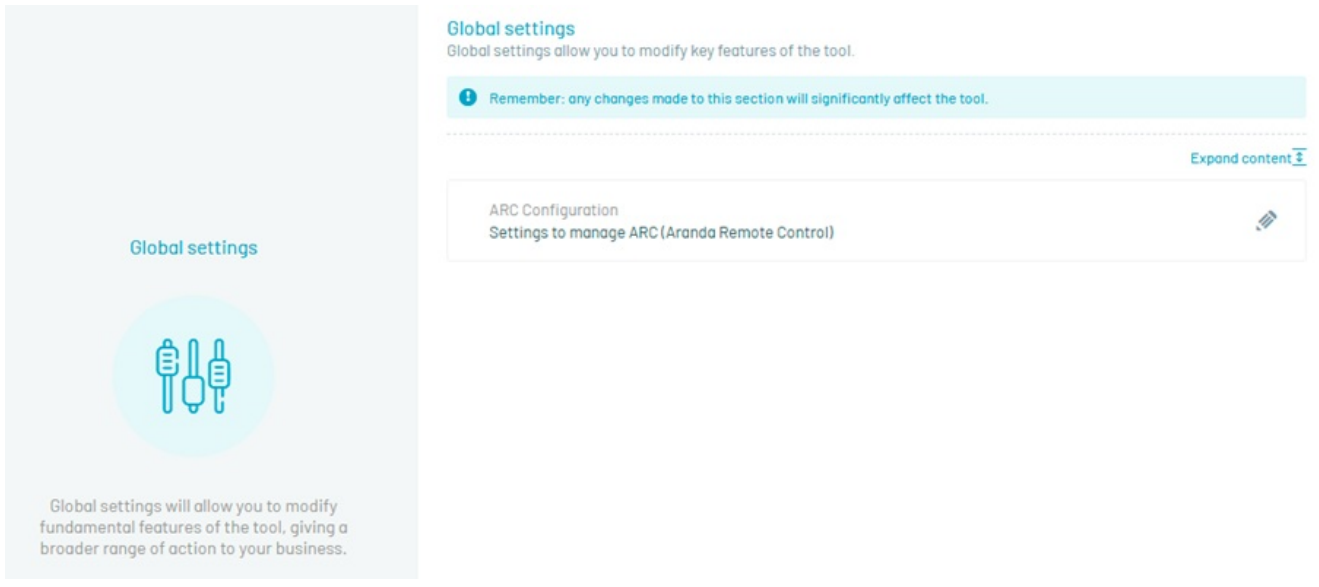
- Ative a funcionalidade no console do ADM acessando Configuração > Geral > Configurações globais.



- Na visualização de informações de Configurações globais, selecione o ícone Configuração do ARC Clique Editar

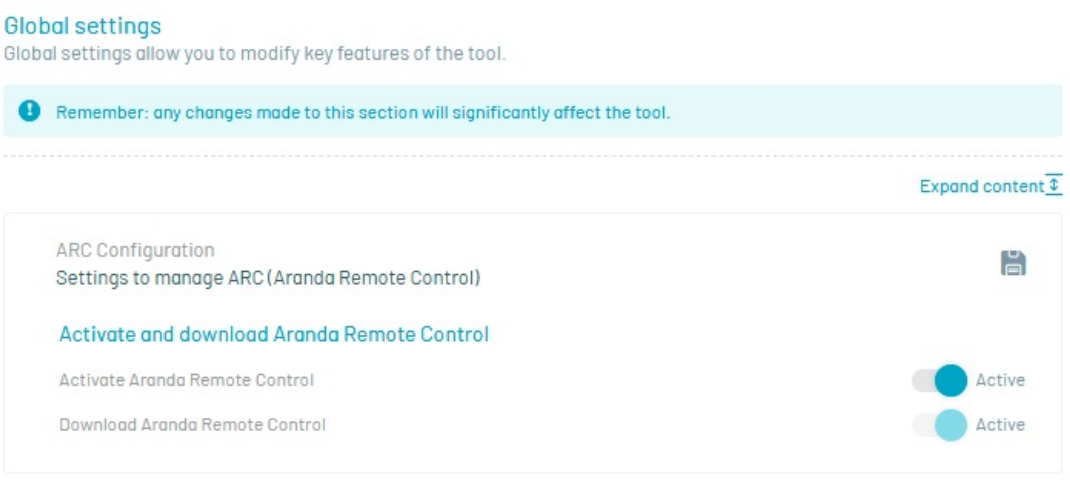


ou no Expandir conteúdo.



⚐ Nota: Em implantações nuvem, esse campo só pode ser exibido, mas não editado. {: #important}

- Valide isso Ativar o controle remoto Aranda Ter a caixa de seleção ativada (padrão). Se não estiver, habilite-o e clique no botão Salvar.



- Execute a configuração pós-instalação correspondente Aranda.ADM.Web.Installer no servidor de aplicativos. Exibir configurações

Processo de configuração e instalação do agente

Considere as seguintes etapas para a configuração e instalação dos agentes de controle remoto:

- Para realizar o controle remoto, é necessário ter o componente de controle remoto instalado nos dispositivos aos quais a conexão remota deve ser feita.Instalação de componentes de controle remoto
- Instalação do visualizador do controle remoto, necessário no dispositivo a partir do qual a conexão remota é feita Instalação do visualizador de controle remoto

Requisitos do aplicativo de controle remoto Aranda

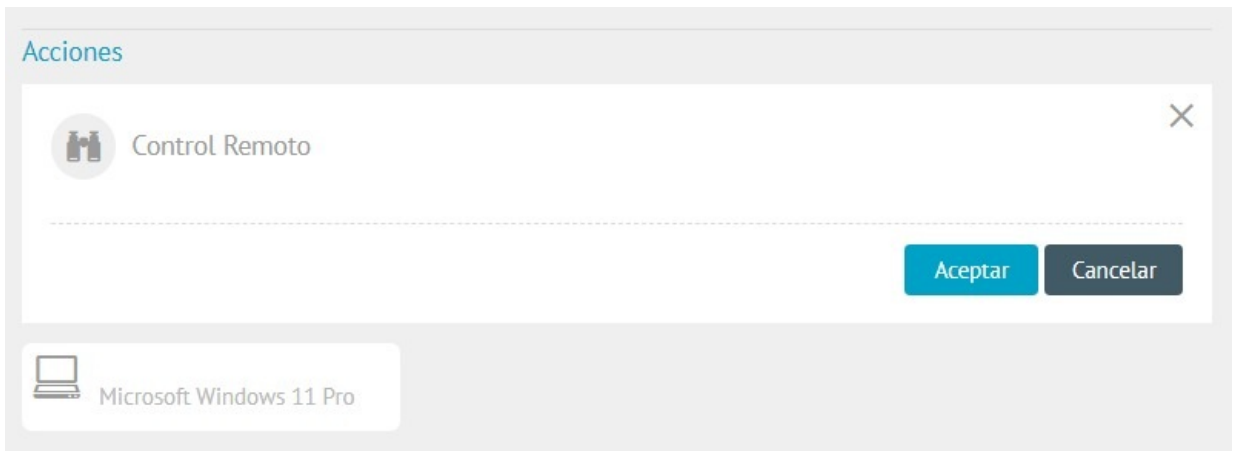
Pegue o controle remoto

Para realizar o controle remoto, o seguinte deve ser configurado previamente:

- O controle remoto requer ter a permissão de suporte remoto ativa na função de usuário ADM.Funções e permissões.
- O dispositivo deve estar associado a um grupo de dispositivos. Grupos
- É necessário criar uma relação entre o grupo de dispositivos e o usuário ou grupo de usuários autorizado a executar o controle remoto.Relações

Depois que a configuração acima for feita:

- No cardápio Inventário > Dispositivos Você precisa selecionar o dispositivo disponível, clicar na ação Controle Remoto e depois em Aceitar.



- No navegador, o Sessão de suporte, onde você pode visualizar informações do dispositivo, abrir o visualizador do controle remoto e transferir arquivos entre dispositivos.

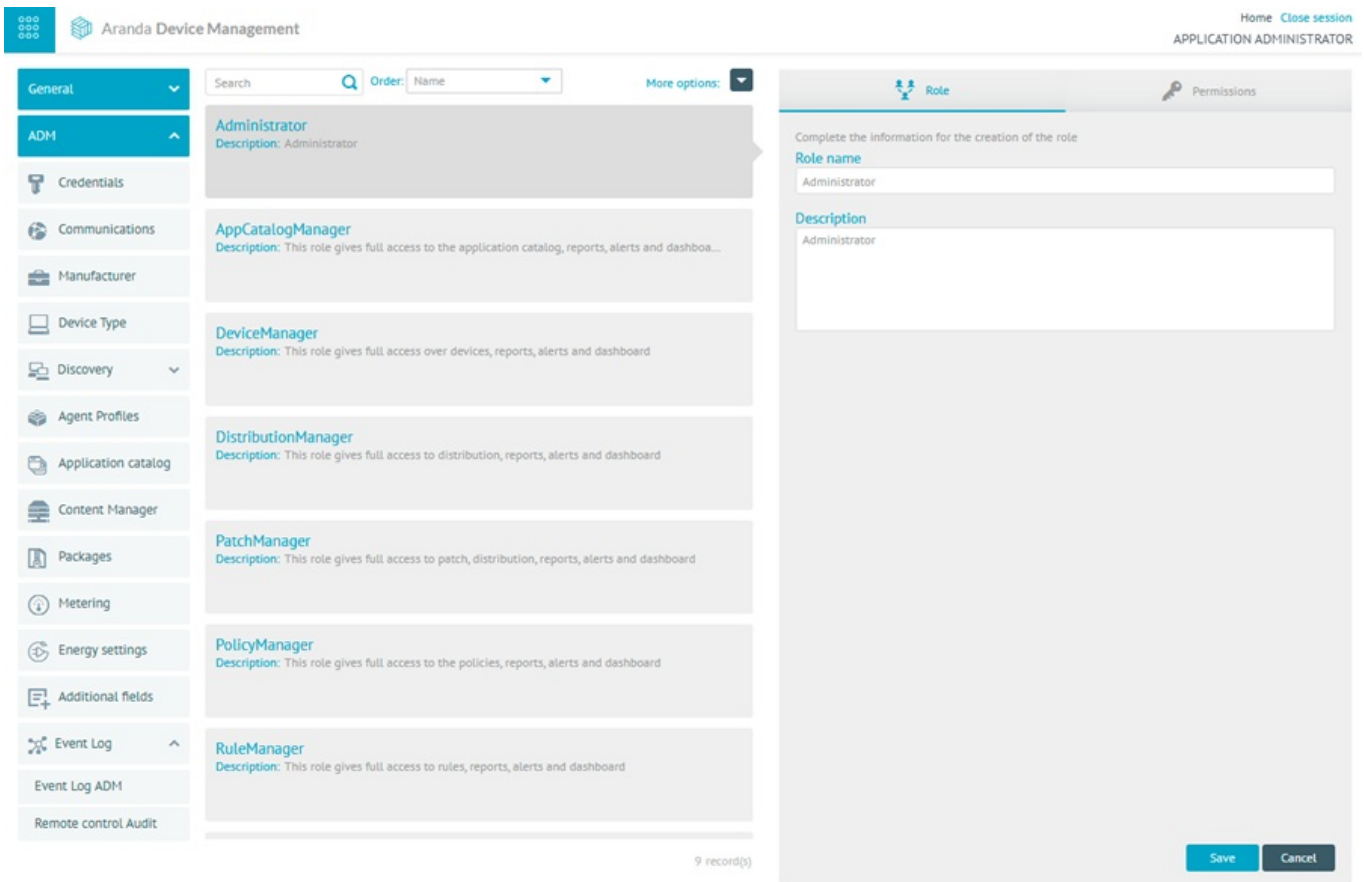
Pegue o controle remoto

Transferências de arquivos

Auditoria de controle remoto

Esse recurso permite que os eventos registrados ao entrar na sessão de suporte fiquem visíveis na seção Log de eventos. É possível pesquisar no filtro, adicionar e/ou ocultar colunas. Os eventos são registrados ao solicitar, iniciar ou encerrar o controle remoto, ao enviar ou receber arquivos.

Para visualizar esses logs, você deve ir para o console do ADM Configuração > ADM > Registro de eventos > Auditoria de controle remoto.



Uma tela é habilitada onde você pode visualizar todos os eventos realizados na sessão de suporte.

Auditoria de controle remoto

Instalação de componentes

Instalação de componentes de controle remoto

↩ Integração ARC

Os Agentes do ADM Windows do ADM versão 9.19.2, após executar a instalação zero ou uma atualização de uma versão anterior, instalarão automaticamente o novo componente de controle remoto após 30 minutos. Os seguintes processos e serviços são exibidos no dispositivo.

> ⚐ Nota: No caso de uma falha de conexão no momento da instalação ou atualização do componente de controle remoto, o agente ADM executará novas tentativas de instalação a cada 4 horas.

Processos e serviços de componentes de controle remoto

Atualização de componentes de controle remoto

↩ Integração ARC

Instalação do visualizador de controle remoto

↩ Integração ARC

Instalação do visualizador de controle remoto

↩ Integração ARC

Configuração de ambientes locais

Configuração do controle remoto ARC

Depois de instalar o arquivo Aranda.ADM.Web.Installer realizar configurações subsequentes no servidor de aplicativos e no console ADM para garantir a operação correta do novo controle remoto, levando em consideração as seguintes etapas:

1. Configurar cadeia de conexão

Configure a cadeia de conexão para o site de gravação, na linha 6 do arquivo appsettings.json do site; O caminho padrão é:

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

Exemplo de como a cadeia de conexão deve ser exibida no appsettings.json

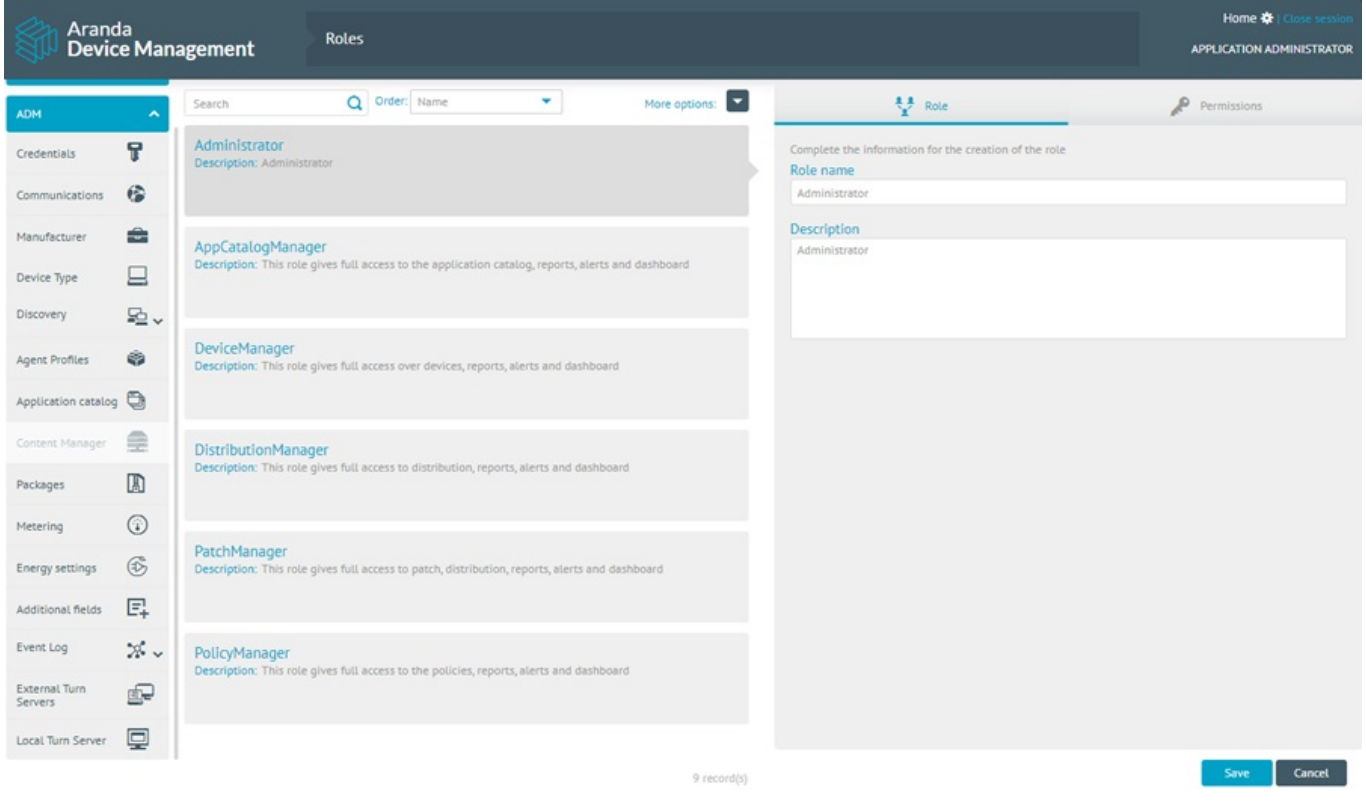
⚐ Anotações:
- Ao fazer alterações na cadeia de conexão do Recording Server, reinicie o IIS para que as alterações sejam aplicadas corretamente.

- Se forem feitas alterações no provedor de armazenamento após a configuração, mova as informações contidas no provedor anterior para o atual. Se essa ação não for executada, as atualizações do agente não serão bem-sucedidas e você não poderá acessar as gravações nas auditorias.

2. Faça login no console

Faça login no console do ADM com o usuário com as permissões necessárias para gerenciar as opções Servidores de turno externos e Servidor de turno local nas Configurações do ADM.

⚠ Importante: As opções de Torneamento Externo e Local estão disponíveis apenas em instalações On-Premise.



3. Servidores de turno externos

A funcionalidade de transferência de arquivos do controle remoto usa um protocolo P2P baseado em WebRTC. Quando dois dispositivos não conseguem estabelecer uma conexão direta entre si, é necessário um servidor Turn para facilitar a comunicação.

Para adicionar um servidor Turn externo no Servidores de turno externos, siga estas etapas:

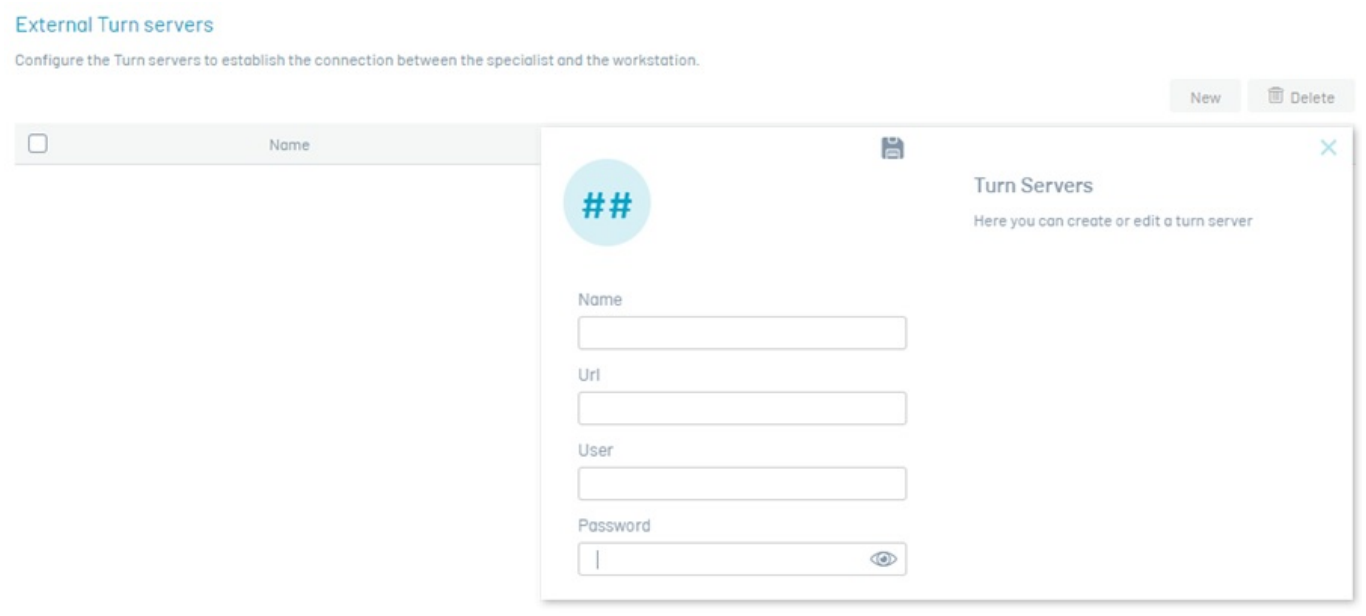
A. Clique na opção Novo.

B. Preencha os campos solicitados de acordo com a tabela a seguir:

Campo	Descrição
Nome	Nome que você deseja atribuir à configuração, entre 6 e 50 caracteres.
URL	Corresponde ao site do servidor STUN/TURN, por exemplo: turn:<server_public_ip>:puerto ou stun:<server_public_ip>:puerto .
Utilizador	Nome do usuário autorizado a se conectar ao servidor STUN/TURN.
Senha	Senha associada ao usuário que permite a conexão com o servidor STUN/TURN.

C. Finalize clicando no botão Salvar.

> ⚐ Nota: Essa configuração é necessária para transferência de arquivos quando o agente especialista e o agente da estação de trabalho não estão na mesma rede, portanto, ambos os dispositivos devem ter permissão para sair para a Internet pela porta configurada.



O usuário pode registrar o número de servidores externos do Turn que julgar necessário para ter uma boa comunicação entre os dispositivos do especialista e a estação de trabalho através do console ADM. Para excluir um servidor Turn externo, no Servidores de turno externos Selecione o(s) servidor(es) a serem excluídos e clique no botão Eliminar, será confirmado que o(s) servidor(es) foi(foram) excluído(s) com êxito.

Você pode usar o WebRTC público STUN/TURN, fazendo uma pesquisa na web "Lista de servidores STUN" você poderá listar os diferentes servidores STUN/TURN públicos disponíveis. Ao configurar servidores públicos em estações de trabalho e em computadores especializados, eles devem permitir a saída dos servidores configurados para os sites. Também é possível configurar o servidor STUN/TURN fornecido no instalador fazendo as configurações no Aranda Turn Stun WebRTC Server Windows Service. Além disso, o STUN/TURN público pode ser usado em conjunto com seus próprios servidores instalados, conforme mencionado acima.

4. Ativar servidor local

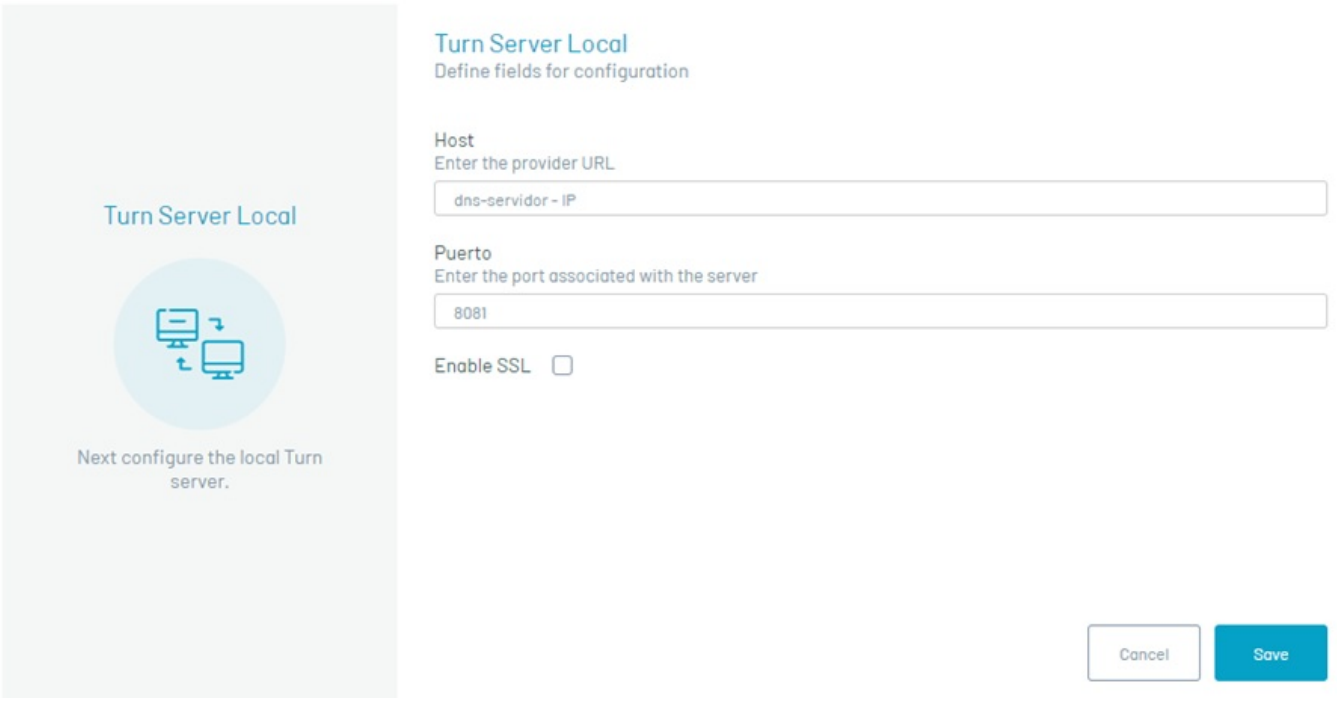
Para estabelecer a comunicação de controle remoto entre o agente especialista e o agente da estação de trabalho, use um servidor Turn local que possa retransmitir o tráfego de rede.

Para adicionar um servidor Turn local, siga estas etapas:

A. Clique na opção Servidor de turno local no menu principal.

B. Preencha o campo Anfitrião com o caminho para o servidor local, que pode ser o IP do servidor ou o DNS. O campo Porta ele é definido por padrão para o valor 8081 e o SSL está inativo; se a porta for alterada ou o SSL estiver ativado faça as configurações no serviço Aranda Turn Server instalado no servidor.

C. Finalize clicando no botão Salvar



Configuração manual de serviço

Configurando o Turn Server

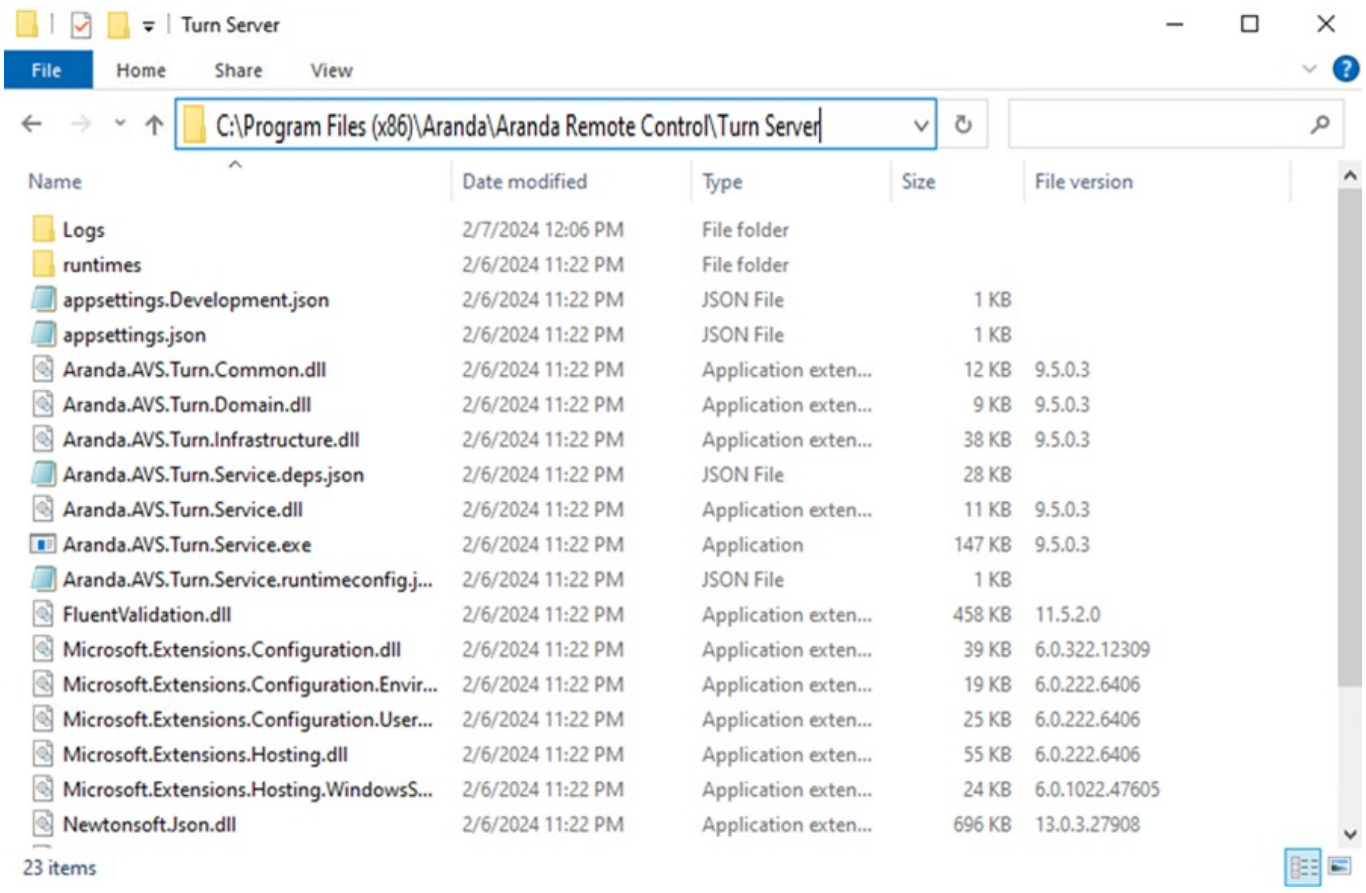
↩ Ativar servidor local

Depois de instalar o serviço Aranda Turn Server, você não precisa fazer nenhum ajuste para sua operação. No entanto, as parametrizações podem ser feitas de acordo com necessidades específicas, como alterar a porta de conexão (8081 por padrão) e habilitar o SSL (desabilitado por padrão). Se você precisar fazer essas configurações, siga estas etapas:

1. Validando o arquivo appsettings.json

Antes de fazer alterações, verifique o appsettings.json localizado no caminho de instalação do serviço (padrão: C:\Program Files (x86)\Aranda\Aranda Remote Control\Turn Server) para garantir que a porta esteja definida como 8081 por padrão. Se a porta não precisar ser modificada, nenhum ajuste adicional será necessário.

Além disso, valide se a porta 8081 está habilitada nas regras de firewall local para garantir o fluxo correto de tráfego. Nesse arquivo, você também pode encontrar a configuração para certificados SSL, que está desabilitada por padrão (IsSsl=false).



Configurações padrão appsettings.json:

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

```
}
```

2. Alteração da configuração da porta

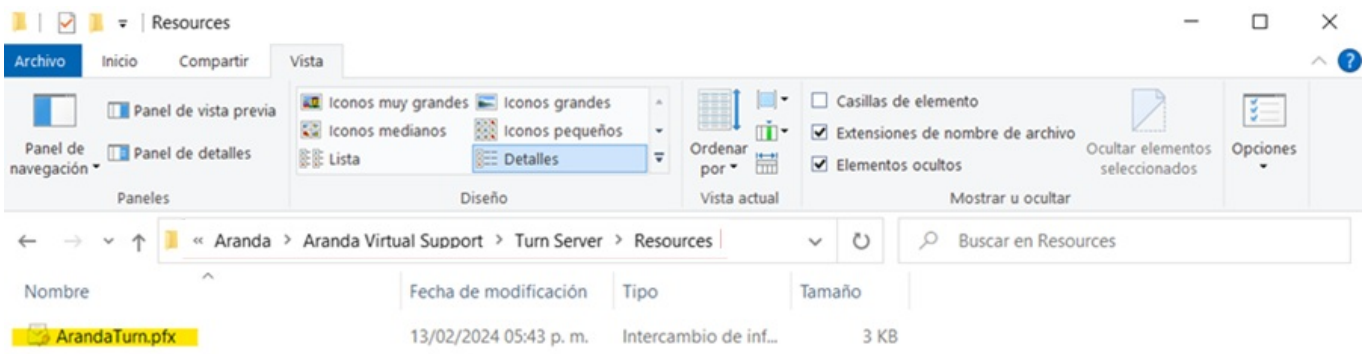
Edite o arquivo appsettings.json e configure a porta desejada substituindo <puerto> pelo número de porta desejado.

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

3. Configuração de conexão segura SSL

Edite o arquivo appsettings.json, altere "IsSsl" para true. Existem duas alternativas para adicionar o certificado SSL:

3.1. Adquira ou gere um certificado PFX, que deve estar localizado dentro da pasta Recursos (a pasta deve ser criada se não existir) no caminho de instalação do serviço.



O nome do arquivo é registrado no arquivo Caminho do certificado e a chave codificada em base 64 para gerar o certificado deve ser registrada em CertificadoParam, ambas as opções disponíveis no arquivo appsettings.json.

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

3.2. Se você tiver um certificado PFX armazenado no bucket de certificados, poderá configurá-lo nomeando o certificado no Assunto do certificado do arquivo appsettings.json.

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

4. Reinicialização do serviço

Reinicie o serviço Turn Server Windows para que as alterações de configuração entrem em vigor. O serviço agora deve escutar na porta recém-configurada e habilitar o uso do certificado SSL.

5. Configurações do firewall

Abra a porta que foi configurada na etapa 2 nas regras de entrada do firewall local. Esta etapa é crucial para permitir o tráfego pela nova porta e garantir que o Turn Server possa receber conexões de entrada na porta configurada.

Parametrizar a porta do Turn Server e o uso de SSL do serviço é um processo fundamental para garantir seu correto funcionamento e adaptá-lo às necessidades específicas de cada cliente. Seguindo estas etapas, você pode garantir que o Turn Server esteja configurado corretamente e pronto para lidar com as conexões conforme necessário.

↩ Ativar servidor local

Configurando o servidor WebRTC Stun/Turn

↩ Servidor de turno externo

Depois de instalar o serviço Aranda Vire o Servidor WebRTC Atordoamento, a configuração é necessária para que funcione corretamente.

1. Validação de arquivo turn-server.toml

Antes de fazer alterações, verifique se o virar-servidor.toml está localizado no caminho de instalação do serviço (por padrão: 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 o serviço STUN/TURN WebRTC, use o comando turn-server.toml:

- Secção [turn]: Especifica o domínio em que o servidor está localizado.
- Secção [[turn.interfaces]]: Indica as interfaces de escuta. Descreve a interface à qual o servidor STUN/TURN está vinculado. Várias interfaces podem ser indicadas.
- Secção [turn.interfaces.transport]: Define o tipo de transporte da interface, que pode ser udp ou tcp.
- Secção [turn.interfaces.bind]: Endereço IP e porta de ligação do soquete interno.
- Secção [turn.interfaces.external]: Ele é usado para vincular ao endereço da sua placa de rede local. Por exemplo, se você tiver duas NICs, A e B, em seu servidor, e o endereço IP da NIC A for 192.168.1.2 e o da NIC B é 192.168.1.3, se vinculado à IAS A, você deve vincular ao endereço 192.168.1.2. Link para 0.0.0.0 Isso significa que você ouve todas as interfaces ao mesmo tempo. A palavra external significa que sua placa de rede para o cliente pode "ver" o endereço IP. Continuando com o exemplo anterior, se sua placa de rede A se comunicar com o exterior, os outros clientes verão seu endereço LAN (ou seja, 192.168.1.2). No entanto, na realidade, a topologia de rede em que o servidor é implantado pode ter outro IP público, como 1.1.1.1, que é o endereço IP visto por outros clientes. A razão pela qual eles são necessários bind e external é que, para o protocolo STUN, o servidor precisa relatar seu próprio endereço IP externo, permitindo assim que o cliente STUN se conecte ao endereço especificado usando o IP relatado pelo servidor.
- Secção [api.bind]: Escutar a API para consultas, por exemplo: http://127.0.0.1:3000/info.
- Secção [log.level]: Nível de log. Valores válidos: error, warn, info, debug, trace.
- Secção [auth]: Nome de usuário e senha para acessar o servidor.

2. Início do serviço

Inicie o serviço STUN Server (Aranda Turn Stun WebRTC Server) para que as alterações de configuração entrem em vigor.

3. Configurações do firewall

Abra a porta ou portas configuradas na etapa 1 nas regras de entrada do firewall local e nos controladores de rede presentes na infraestrutura do cliente, para os protocolos TCP e UDP. Essa etapa é essencial para permitir o tráfego pela nova porta e garantir que o servidor STUN possa receber conexões de entrada na porta configurada.

As estações de trabalho (ARC Agent) e os computadores especializados (Specialist Agent) devem permitir a saída através das portas configuradas.

Além disso, se você precisar que ele opere como TURN WebRTC, deverá abrir o intervalo de portas 49152-65535 para o protocolo UDP.

Exemplo e cenários de configuração de serviço STUN/TURN

↩ Servidor de turno externo

Exemplo e cenários de configuração de serviço STUN/TURN

↩ Servidor TURN externo

Para fazer o servidor funcionar para dispositivos dentro e fora da rede, siga estas etapas:

1. Configure o reino

Altere o valor de realm para o domínio público ou endereço IP externo do seu servidor. Isso é importante para autenticar com êxito solicitações externas.

Se o endereço público do seu servidor for 1.2.3.4, defina-o como:

```
realm = "1.2.3.4"
```

2. Configurar ligação

O bind garante que o servidor STUN/TURN escute no IP privado para conexões dentro da rede local.

Se o endereço privado do seu servidor for 192.168.1.25, defina-o como:

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

Se você precisar que o serviço STUN/TURN escute em todas as interfaces ao mesmo tempo, configure-o como:

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

Essas configurações são necessárias apenas para [[turn.interfaces]].

3. Configurar externo

O external é onde o IP público do servidor é definido para que os computadores externos possam se comunicar adequadamente com o servidor STUN/TURN.

Se o endereço público do seu servidor for 1.2.3.4, defina-o como:

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

4. Autenticação

O [auth] Ele é configurado com usuários estáticos:

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

Isso permite conexões autenticadas com credenciais estáticas user1:test e user2:test. Certifique-se de usar credenciais mais seguras se você planeja expor esse serviço a dispositivos externos.

As outras seções podem ser deixadas por padrão.

Quando você executa a parametrização no virar-servidor.toml, isso deve ser observado da seguinte 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 você faz uma modificação no virar-servidor.toml, reinicie o serviço Aranda Vire o Servidor WebRTC Atordoamento para que as alterações entrem em vigor.

Cenários

Os cenários a seguir e o resultado são descritos abaixo de acordo com as configurações no exemplo.

Cenário	Especialista	Status da rede	Agente ARC	Status da rede	Resultado
1	Você só pode acessar o servidor TURN/STUN usando o IP público	Externo	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
2	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
3	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	Você pode acessar o servidor TURN/STUN usando o IP público.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP público.
4	Você só pode acessar o servidor TURN/STUN usando o IP privado.	Interno	Você só pode acessar o servidor TURN/STUN usando o IP privado.	Interno	O Especialista e o Agente ARC podem estabelecer comunicação consumindo o servidor TURN/STUN pelo IP privado.
5	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você não pode usar o IP público para se conectar ao servidor TURN/STUN, pois seu acesso é restrito à rede interna (IP privado).	Interno	O Especialista e o Agente ARC não conseguem estabelecer comunicação devido a um problema de conectividade entre as redes (externas e internas).
6	Você só pode acessar o servidor TURN/STUN usando o IP público.	Externo	Você não pode usar o IP público para se conectar ao servidor TURN/STUN, pois seu acesso é restrito.	Externo	O Especialista e o Agente ARC não conseguem estabelecer comunicação devido a um problema de conectividade entre as redes.

⚠ Nota:

- Para cobrir os cenários 1, 2 e 3, configure no Site da AMD o servidor External Turn da seguinte maneira:
  Nome: nome da configuração.
  URL: turn.1.2.3.4:3478 (1.2.3.4 refere-se ao IP público do servidor).
  Utilizador: usuário1.
  Senha: teste.

⚠ Anotações:

- Para cobrir o cenário (4), configure no Site da ADM o servidor External Turn da seguinte maneira:
  Nome: nome da configuração.
  URL: turn.192.168.1.25:3478 (192.168.1.25 refere-se ao IP privado do servidor).
  Utilizador: usuário1.
  Senha: teste.
- Se no virar-servidor.toml foi criado 0.0.0.0 no parâmetro bind, a configuração deve ser realizada no site como acima.

↩ Servidor TURN externo