Guia de Instalação Fhinck

Passo a passo para preparação, instalação e validação

Material de apoio para facilitar a implantação no cliente. A equipe continuará disponível durante todo o processo; este guia funciona como uma referência rápida para os principais passos.

Windows 10 e Windows 11

Importante

Em ambientes corporativos, algumas etapas podem depender da equipe de TI, principalmente quando houver domínio, antivírus corporativo, EDR, proxy ou regras de firewall.

Antes de começar

Uma preparação rápida evita retrabalho durante a instalação.

Antes de abrir o instalador, confirme os pontos abaixo. Em máquinas compartilhadas ou controladas por domínio, valide a identificação do usuário com a equipe responsável antes de realizar qualquer alteração.

1 Acesso administrativo

Tenha uma conta com permissão de administrador para alterar o usuário, executar o instalador e configurar exceções.

2 Usuário correto

Confirme o nome da pessoa que realmente utilizará a máquina. O padrão de identificação deve ser aplicado antes da instalação.

3 Segurança do endpoint

Identifique quais antivírus, EDR ou ferramentas de proteção estão instalados. A liberação precisa ser feita em todos os controles aplicáveis.

4 Rede corporativa

Se a empresa utiliza firewall, proxy, UTM, filtro web/DNS ou políticas internas, deixe o contato de TI disponível para eventual liberação.

! Máquina compartilhada

Se várias pessoas utilizam o mesmo computador, não escolha um nome de usuário por conta própria. Confirme com a Key Solution/Fhinck qual identificação deverá ser adotada para o cenário do cliente.

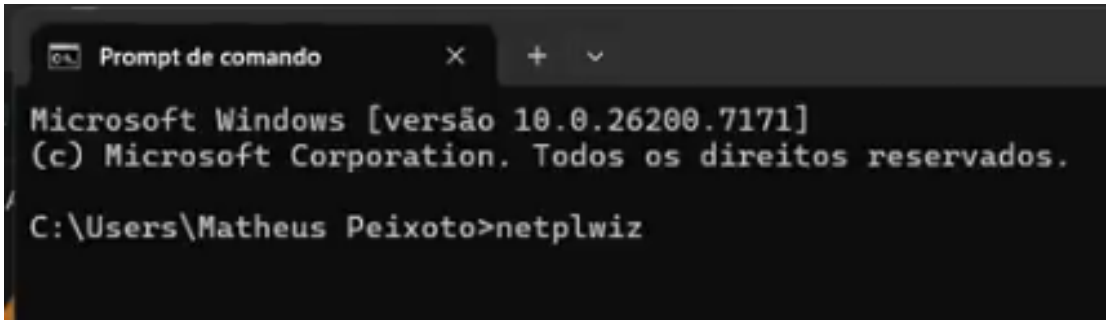
01 Abrir as Contas de Usuário

Ajuste a identificação do usuário antes de instalar a Fhinck.

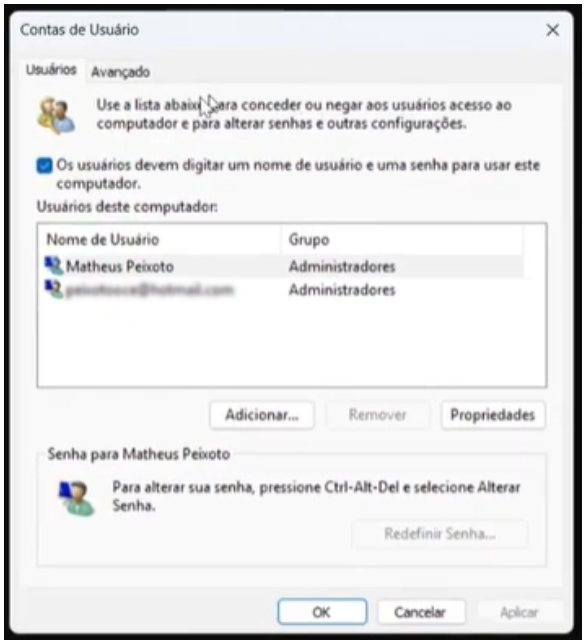
Abra o Prompt de Comando e execute:

```
netplwiz
```

A janela “Contas de Usuário” será exibida. Selecione a conta utilizada pela pessoa que trabalha nessa máquina e clique em “Propriedades”.



Exemplo: abertura do netplwiz pelo Prompt de Comando



Selecione o usuário correto e abra Propriedades

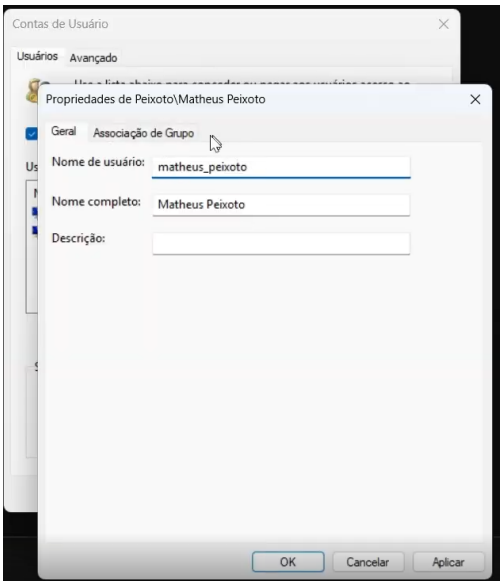
02 Padronizar o nome do usuário

O nome precisa representar a pessoa que utilizará a máquina.

Na aba “Geral”, ajuste o campo “Nome de usuário”.
Use o nome da pessoa que irá utilizar a estação.

Padrão recomendado

- Use o nome da pessoa que realmente utilizará a máquina.
- Quando precisar separar duas partes do nome, use somente o caractere “_”.
- Exemplo: matheus_peixoto
- Evite trocar o separador por espaço, hífen ou ponto.



Propriedades do usuário - exemplo

Ambiente gerenciado

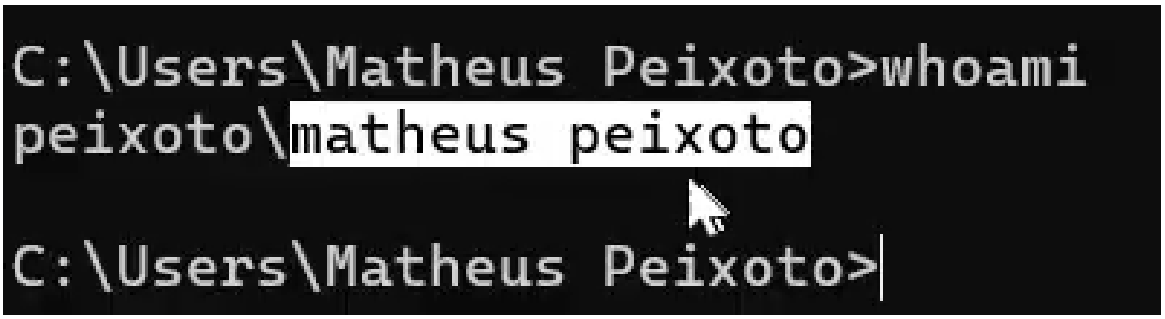
Se o computador estiver ligado a domínio/Active Directory/Entra ID ou tiver políticas corporativas, confirme com a TI antes de alterar a conta.

03 Confirmar com o comando whoami

Garanta que o Windows passou a reconhecer o usuário esperado.

Depois de salvar a alteração, abra novamente o Prompt de Comando e execute:

```
whoami
```



O retorno aparece no formato DOMÍNIO\usuário ou COMPUTADOR\usuário

✓ **Se o nome estiver correto**

Pode seguir para a instalação da Fhinck.

! **Se ainda aparecer o nome antigo**

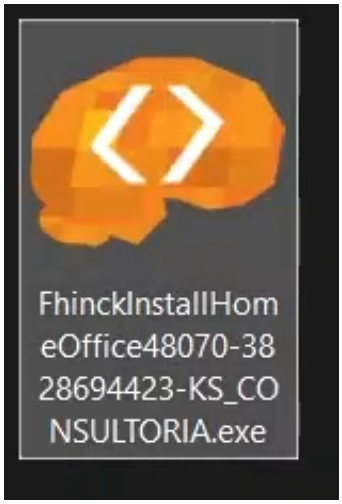
Reinicie o computador e execute “whoami” novamente. Após o reinício, confirme o resultado antes de continuar.

Exemplo de leitura

`empresa\matheus_peixoto → usuário identificado: matheus_peixoto`

04 Executar o instalador como administrador

Instale somente o executável oficial fornecido para o cliente.



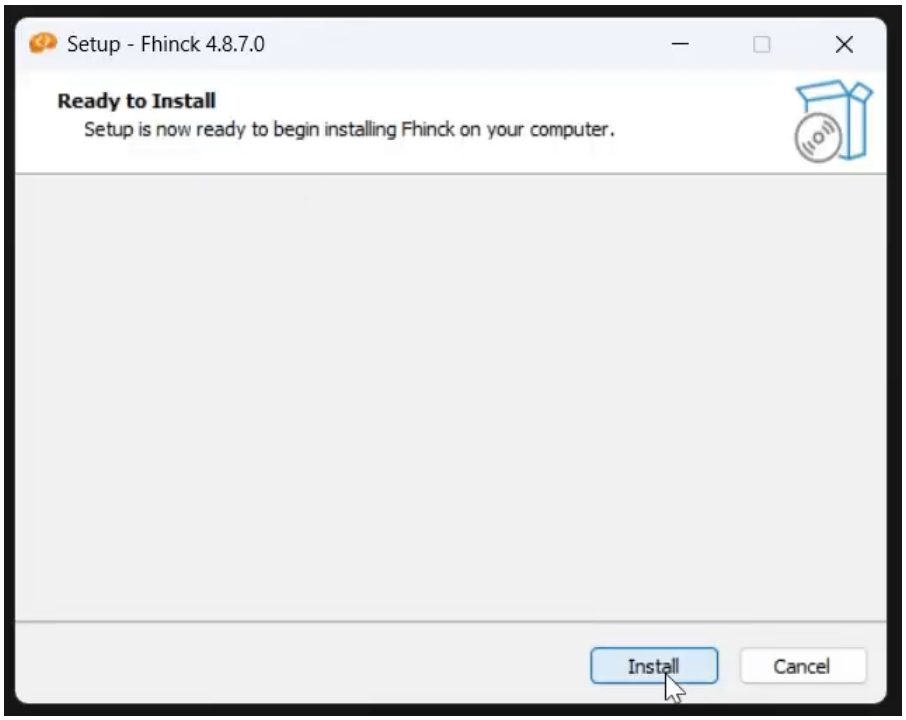
Arquivo instalador

Localize o instalador da Fhinck e execute-o com privilégios de administrador.

- Clique com o botão direito sobre o instalador.
- Escolha “Executar como administrador”.
- Ao chegar à tela “Ready to Install”, clique em “Install”.
- Aguarde o processo terminar. Não interrompa a instalação.

Versão do instalador

A versão exibida nas telas pode ser diferente do exemplo. Siga sempre o pacote enviado para o cliente pela equipe responsável.

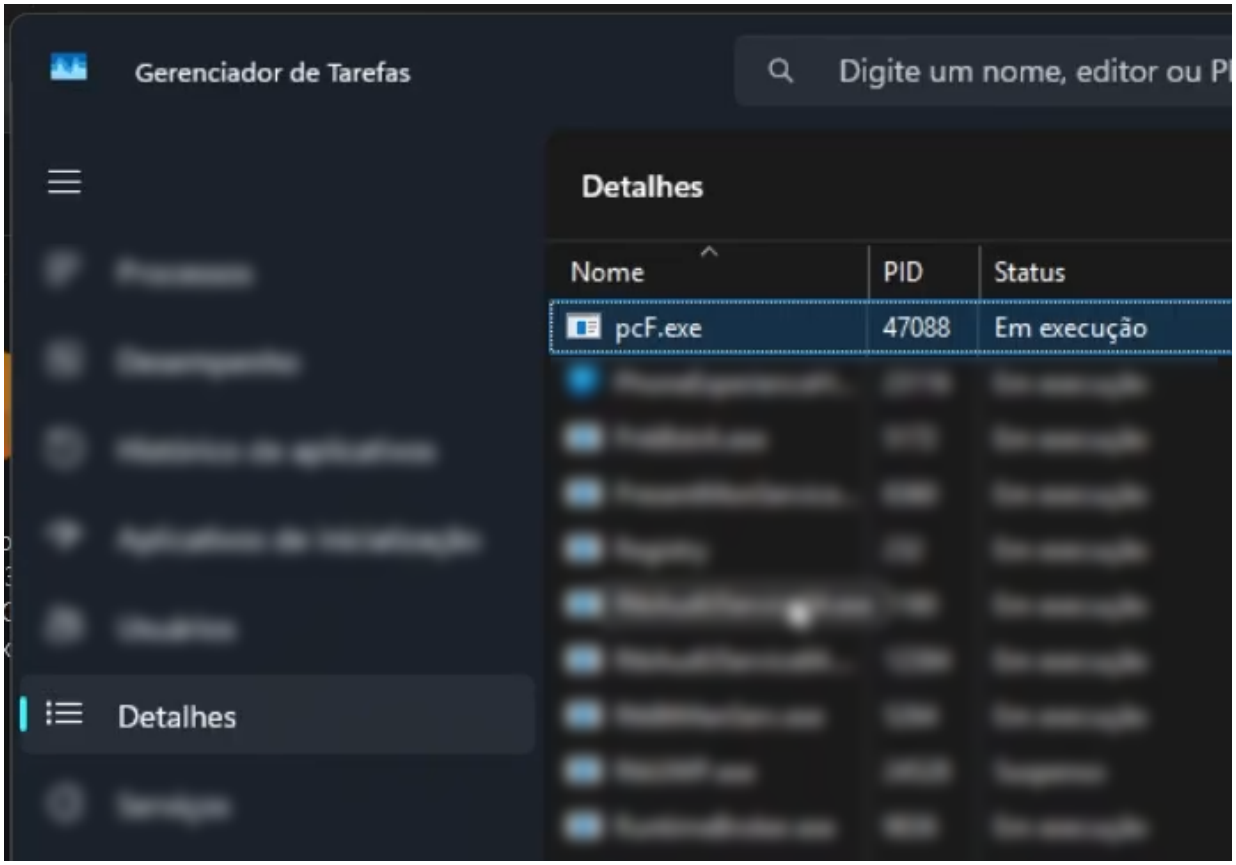


Tela de instalação - clique em Install e aguarde

05 Validar o processo pcf.exe

Após a instalação, confirme se o componente está em execução.

Abra o Gerenciador de Tarefas e procure pelo processo “pcf.exe”. A presença do processo em execução é uma das validações iniciais de que o componente foi iniciado.



Gerenciador de Tarefas > Detalhes > pcf.exe

Se não encontrar o pcf.exe

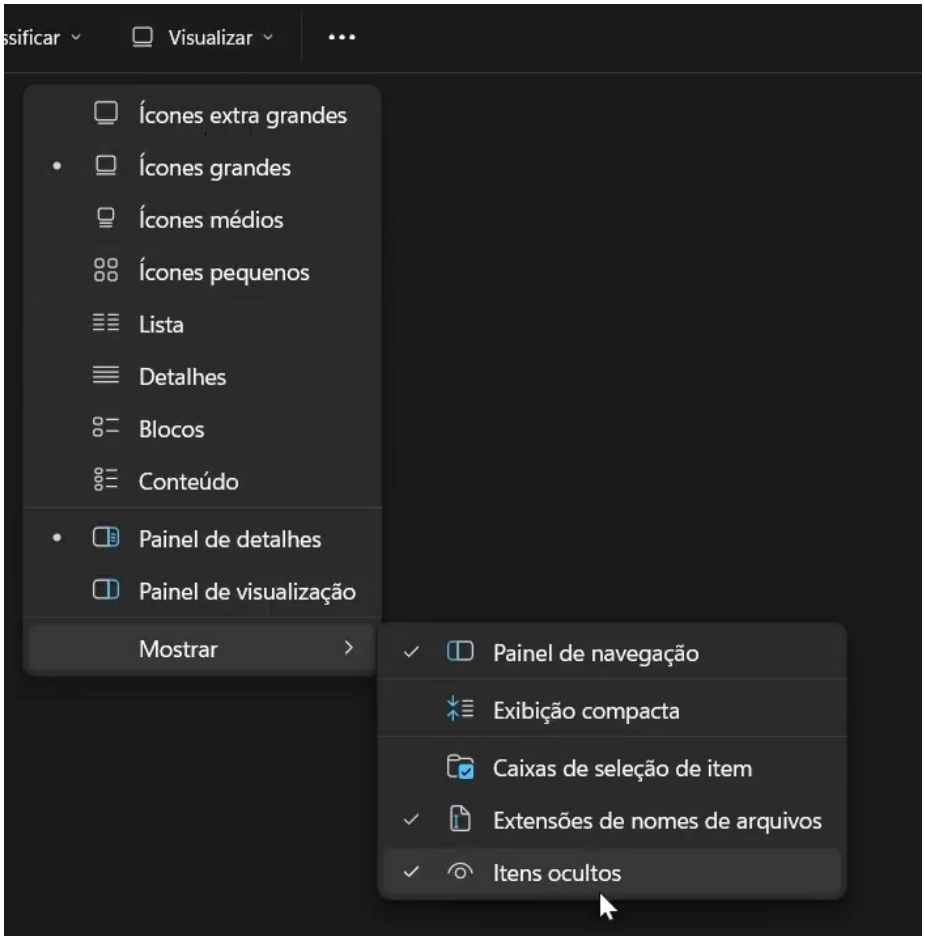
Não avance supondo que a instalação está concluída. Revalide a instalação e, se necessário, acione o suporte da Key Solution/Fhinck.

06 Exibir itens ocultos no Explorador

Essa opção permite acessar as pastas usadas na etapa de liberação do antivírus.

No Explorador de Arquivos, habilite a exibição de itens ocultos. No Windows 11, o caminho do exemplo é:

```
Visualizar  >  Mostrar  >  Itens ocultos
```



Windows 11 - opção “Itens ocultos” marcada

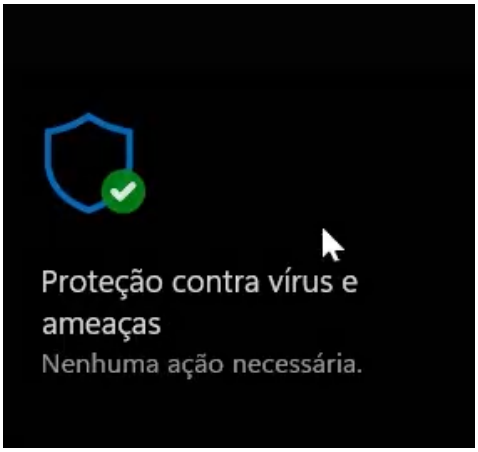
Windows 10

O caminho visual é um pouco diferente, mas a opção também se chama “Itens ocultos” e fica nas opções de Exibir/Visualizar do Explorador.

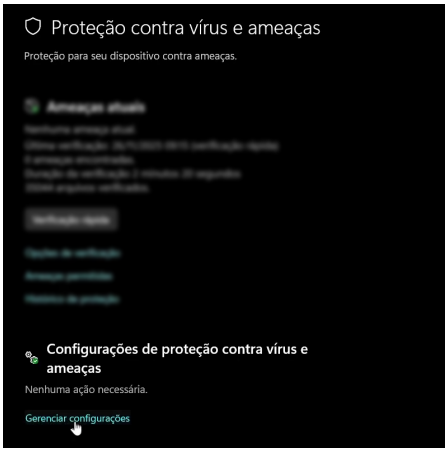
07 Criar as exclusões no antivírus

No exemplo usamos o Microsoft Defender. Em outros antivírus, a lógica é equivalente.

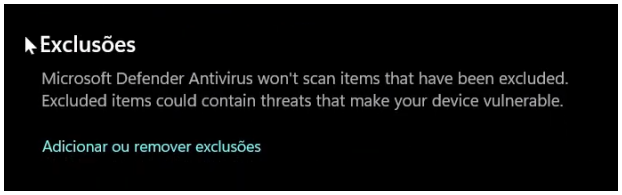
No Windows Defender, siga o fluxo abaixo. A interface pode variar levemente entre versões do Windows.



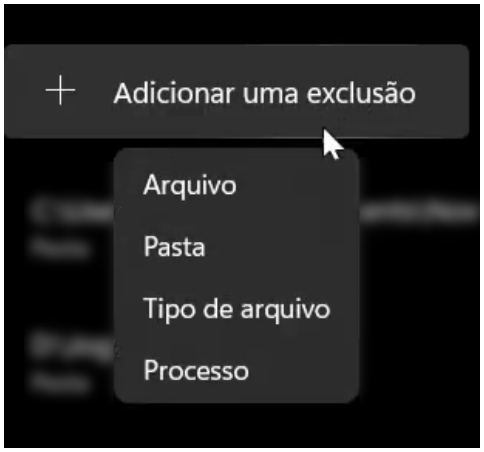
1. Abra Proteção contra vírus e ameaças



2. Entre em Gerenciar configurações



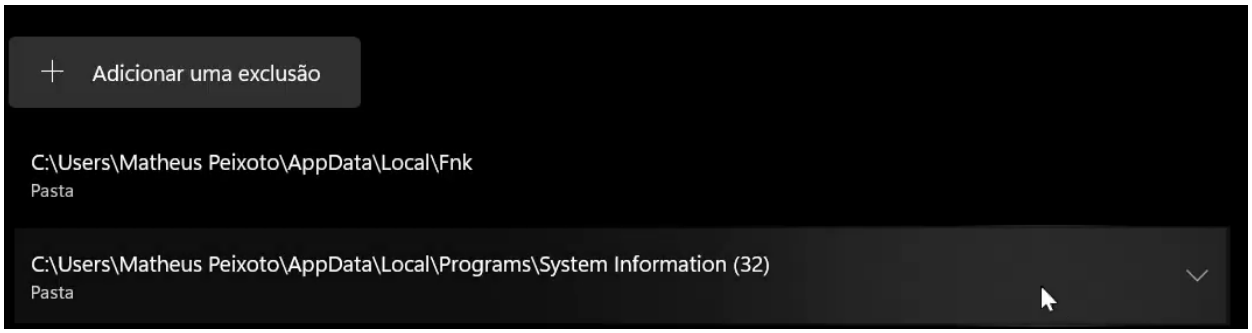
3. Abra Adicionar ou remover exclusões



4. Adicionar uma exclusão > Pasta

08 Liberar as duas pastas da Fhinck

As duas pastas devem constar na lista de exclusões.



Exemplo final das duas exclusões configuradas

Pastas a liberar

```
C:\Users\<PERFIL_DO_WINDOWS>\AppData\Local\Fnk
```

```
C:\Users\<PERFIL_DO_WINDOWS>\AppData\Local\Programs\System Information (32)
```

Não copie “Matheus Peixoto” do exemplo

Substitua pelo perfil existente na máquina do cliente. Em muitas instalações o nome da pasta acompanha o usuário; porém, em computadores já configurados, renomear a conta nem sempre renomeia a pasta dentro de C:\Users. Confirme o nome real da pasta antes de adicionar a exclusão.

Outros antivírus / EDR

Se houver Kaspersky, Sophos, CrowdStrike, SentinelOne, Trend Micro ou qualquer outra proteção corporativa, a liberação também precisa ser aplicada conforme a política da empresa. Quando a estação for gerenciada, solicite a liberação à TI.

09

Validar firewall e bloqueios corporativos

A instalação local pode estar correta e ainda assim a comunicação ser bloqueada pela rede.

Além do antivírus, empresas costumam usar camadas de segurança que controlam a comunicação dos computadores com a internet e com serviços externos. É importante envolver a TI quando houver qualquer bloqueio.

Firewall corporativo

Pode bloquear portas, destinos ou tráfego de saída mesmo quando o Firewall do Windows está liberado.

Proxy / filtro web

Pode exigir autenticação, bloquear categorias, domínios ou conexões feitas por aplicações em segundo plano.

UTM / IPS / IDS

Appliances de segurança podem inspecionar e bloquear conexões consideradas fora da política.

EDR / antivírus corporativo

Pode impedir execução, criação de arquivos ou comunicação do processo mesmo com o Defender liberado.

Filtro DNS / políticas de rede

Pode bloquear resolução de domínios, destinos externos ou regras por grupo de usuários/computadores.

Domínio / políticas internas

GPOs e controles centralizados podem sobrescrever configurações feitas localmente na máquina.

! **Quando acionar a TI**

Se o pcf.exe estiver em execução, as exclusões estiverem corretas e ainda assim a estação não comunicar, peça à TI para validar firewall/proxy/UTM/EDR e liberar os endereços, portas e processos oficiais informados pela Fhinck/Key Solution. Não desabilite a segurança corporativa de forma ampla.

Checklist final

Use esta página antes de considerar a instalação concluída.

- [ ] **Usuário**
  O nome foi padronizado e confirmado com o comando whoami.

- [ ] **Instalação**
  O instalador foi executado como administrador e finalizado sem interrupção.

- [ ] **Processo**
  O pcf.exe aparece em execução no Gerenciador de Tarefas.

- [ ] **Itens ocultos**
  A exibição de itens ocultos foi habilitada para acessar as pastas necessárias.

- [ ] **Exclusões**
  As duas pastas foram liberadas em todos os antivírus/EDRs aplicáveis.

- [ ] **Rede**
  Firewall, proxy e controles corporativos foram validados quando necessário.

Suporte durante a implantação

Este documento é um material adicional de apoio. Caso alguma etapa não se comporte como no exemplo, ou exista qualquer política interna do cliente impedindo a instalação/comunicação, acione a equipe responsável para acompanhamento.