# Manual do Usuário para utilização da VPN Check Point



# 1 - Visão Geral de Como utilizar

Para utilizar a VPN com a CAPES, é necessário:

- **Autorização** - a concessão do acesso está atrelada à política de uso do serviço;
- **Geração de Certificado** - será disponibilizado um certificado digital individual para o usuário;
  - **NOTA**: O certificado expira em **2 anos**.
- **Instalação de Software** - o usuário necessitará instalar um software, de acordo com seu sistema operacional, e utilizá-lo juntamente com o certificado gerado;
- **Configuração navegador** - Para navegação na internet o usuário deve remover a opção do proxy e detecção automática do seu navegador de preferência. O acesso a internet não é realizado pela VPN.

**Estou conectado, o que devo fazer?**

- A sua estação local recebe um endereçamento ip privado valido na rede da Capes (10.10.0.xx), por isso é possível acessar os serviços diretamente da sua estação.
- Utilizando o seu navegador acesse https://intranet.capes.gov.br ou pelo **Putty**, acesse um servidor via ssh, bem como demais serviços que são necessários para o desenvolvimento do seu trabalho, a maioria dos serviços já foram mapeados e liberados de comum acordo com os responsáveis pelas áreas, mas se algum serviços não esteja liberado, por favor registre um chamado para avaliação.
- Está liberado também o acesso remoto às estações Windows da DTI pela VPN, para isso é necessário que a sua estação esteja ligada, que o seu usuário faça parte do grupo local "**Usuários da área de trabalho remota**" (caso não esteja solicite ao suporte a inclusão do seu usuário) e que você memorize o nome ou IP da estação. O acesso pode ser realizado pelo "**Conexão de área de trabalho remoto**" do Windows, pelo "**Microsoft Remote Desktop**" no MAC ou o "**rdesktop**" no Linux, verifique na sua distribuição qual a melhor opção.

> IMPORTANTE As configurações abaixo devem ser realizadas no computador de casa.

# 2 - Windows

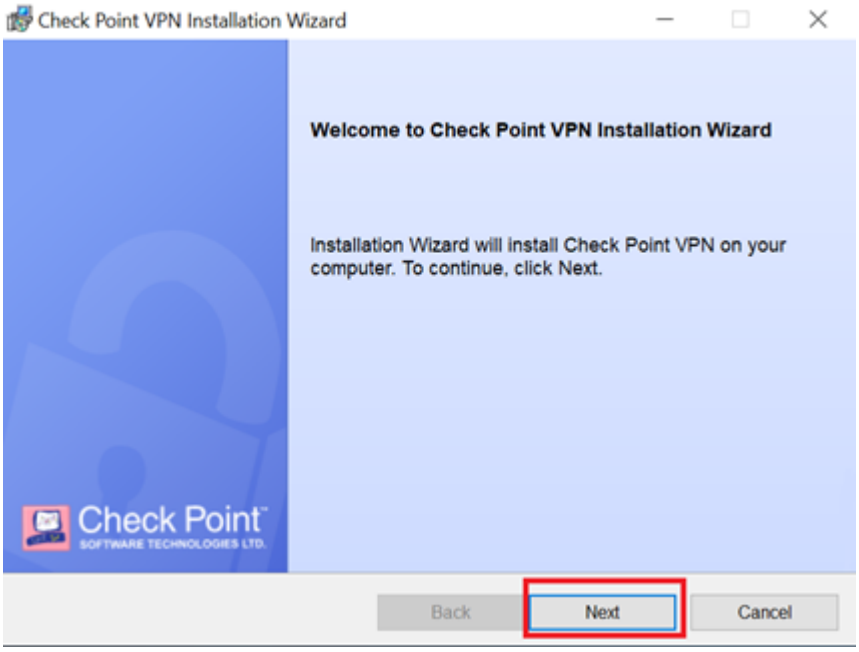
Existem duas formas de utilizar a VPN (**software cliente e via navegador**). Escolha a que melhor lhe atender.

## 2.1 - Instalando software cliente (**Opção 1 - RECOMENDADO**)

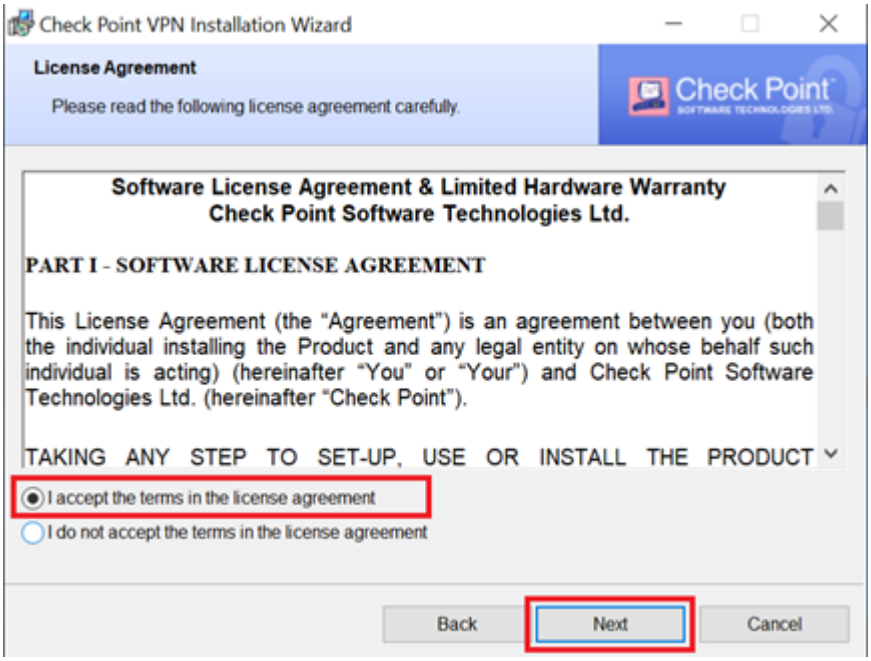
Instalação de pacote personalizado para Windows:

> O procedimento abaixo foi validado no **Windows 10 e 11**.

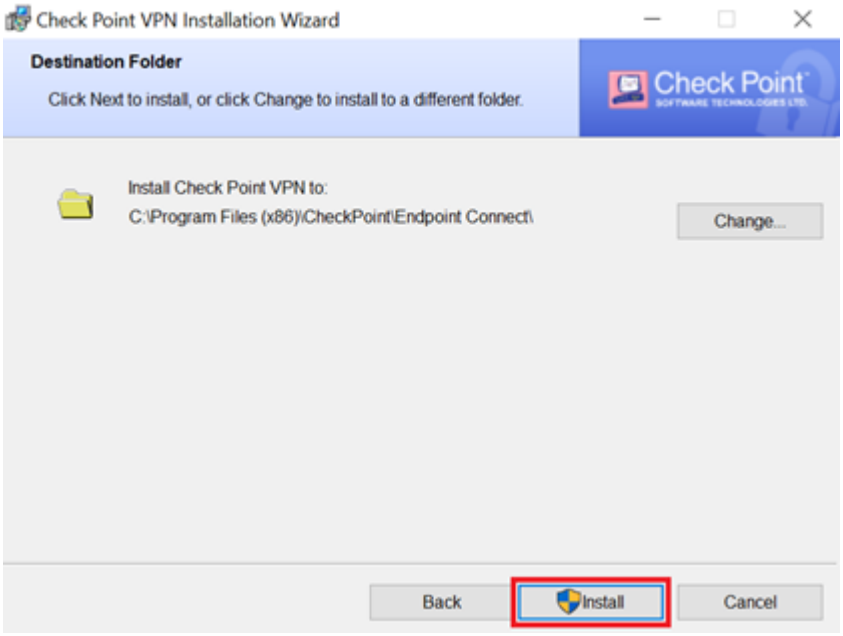
- Faça **download** do instalador da VPN em https://vpn.capes.gov.br/faq/VPN_CLIENT-CAPES.msi
- Depois execute o arquivo de instalação.
- Siga os passos conforme imagens abaixo:



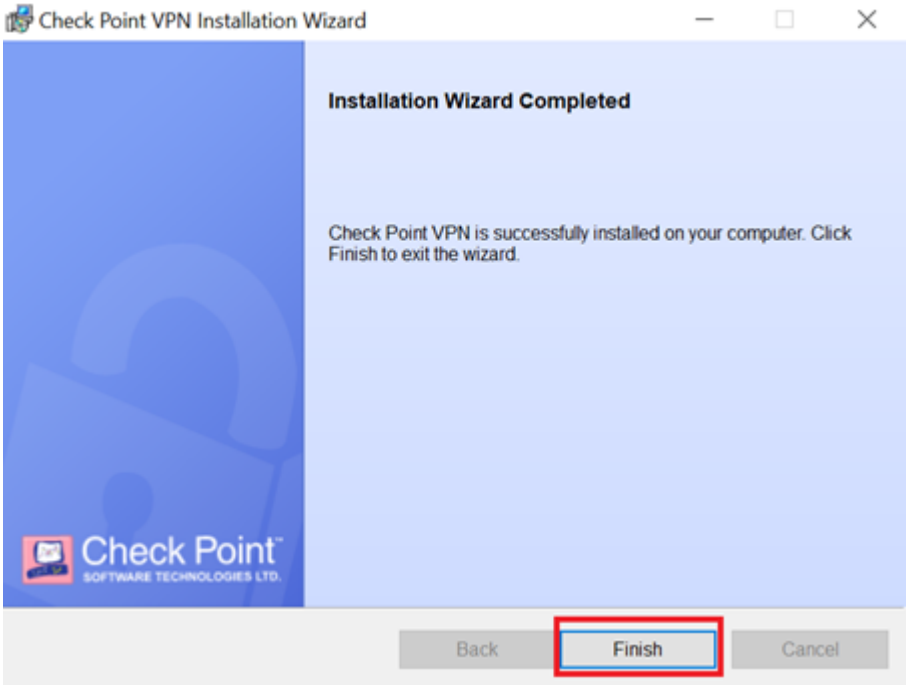

- Veja o Termos da licença.




- Instale.

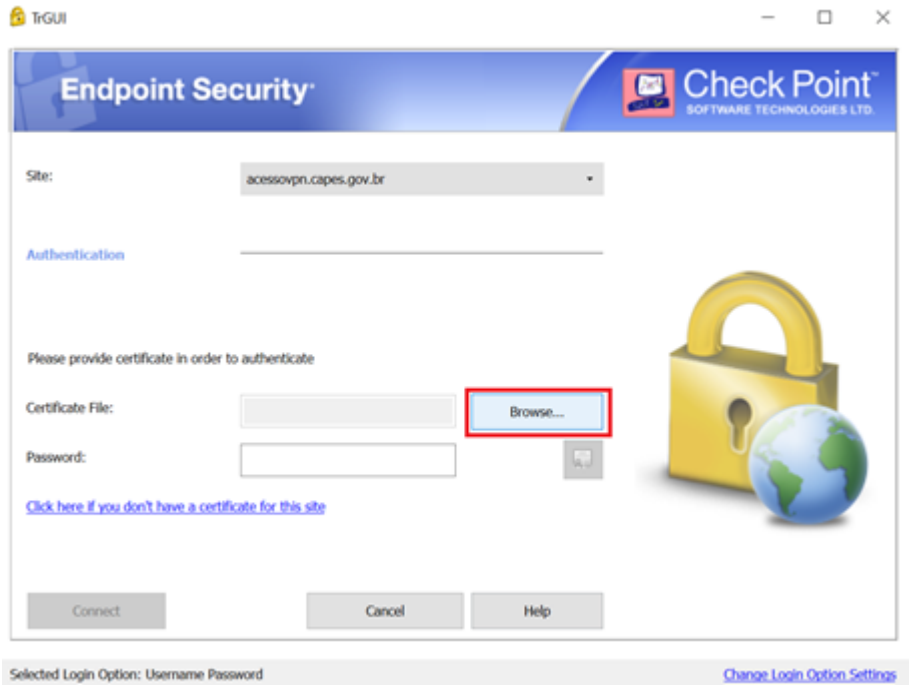



- E finalize.



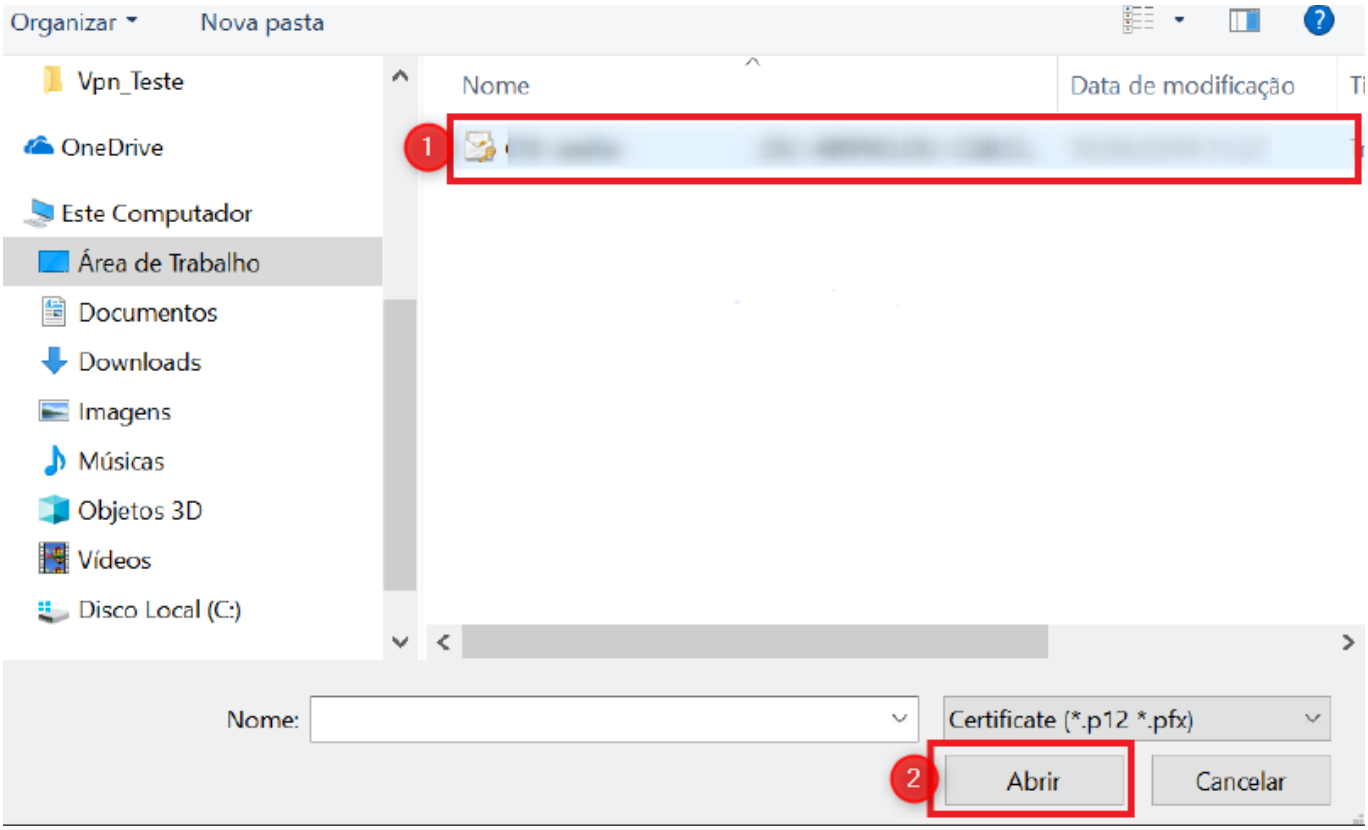

- Ao finalizar a instalação, para o primeiro acesso será necessário a autenticação com o seu certificado digital, previamente enviado por e-mail, por isso salve o certificado em uma pasta de sua preferência.

Para importar o certificado selecione o botão “**Browse**”.



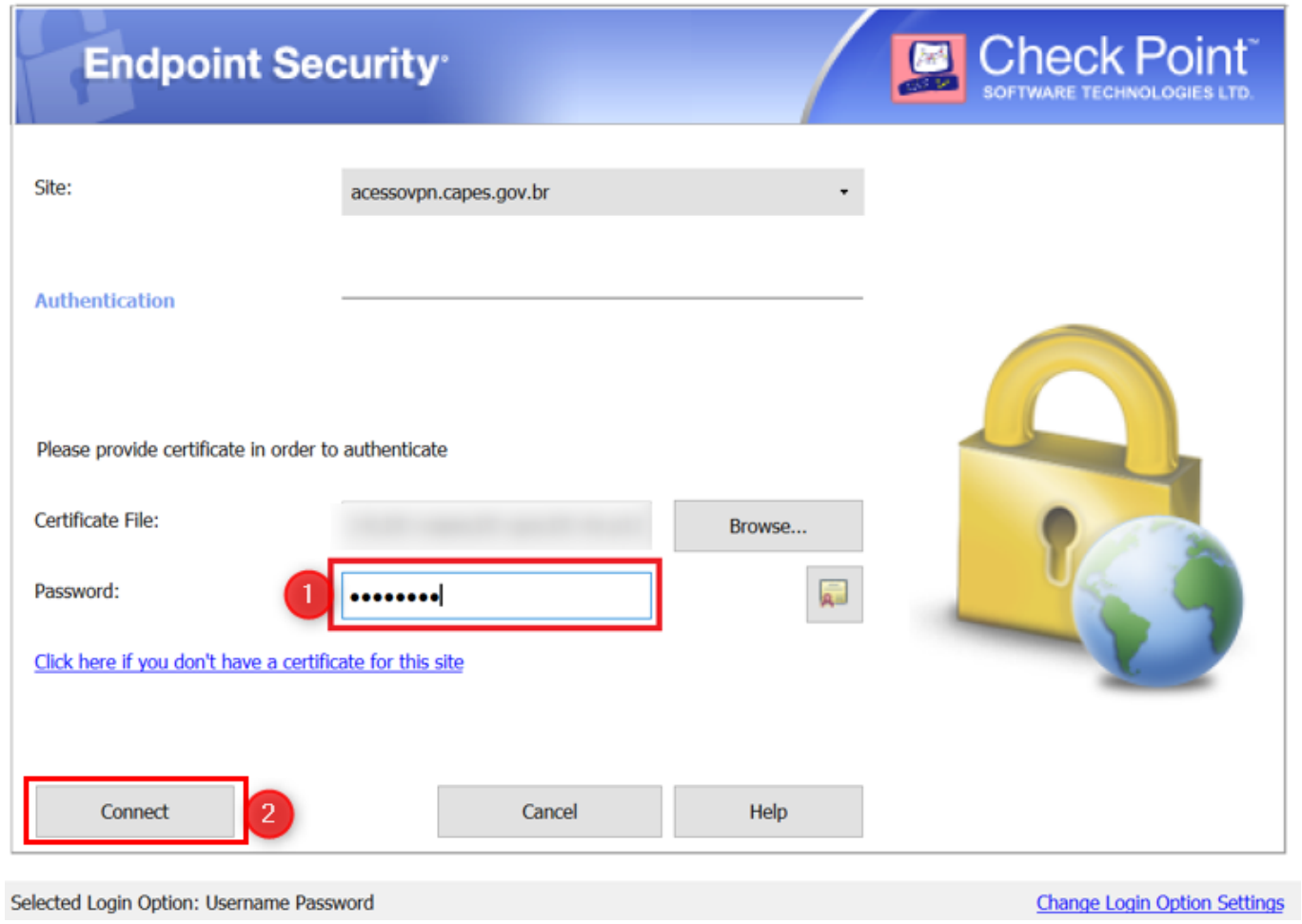

- Selecione o `seu certificado digital`, salvo na sua pasta de preferência, em seguida selecione "**Abrir**". Não mova o certificado de local após configura-lo no aplicativo.

> **NOTA:** Lembre-se de **apagar** o certificado de seu e-mail e guardá-lo em local **seguro**.

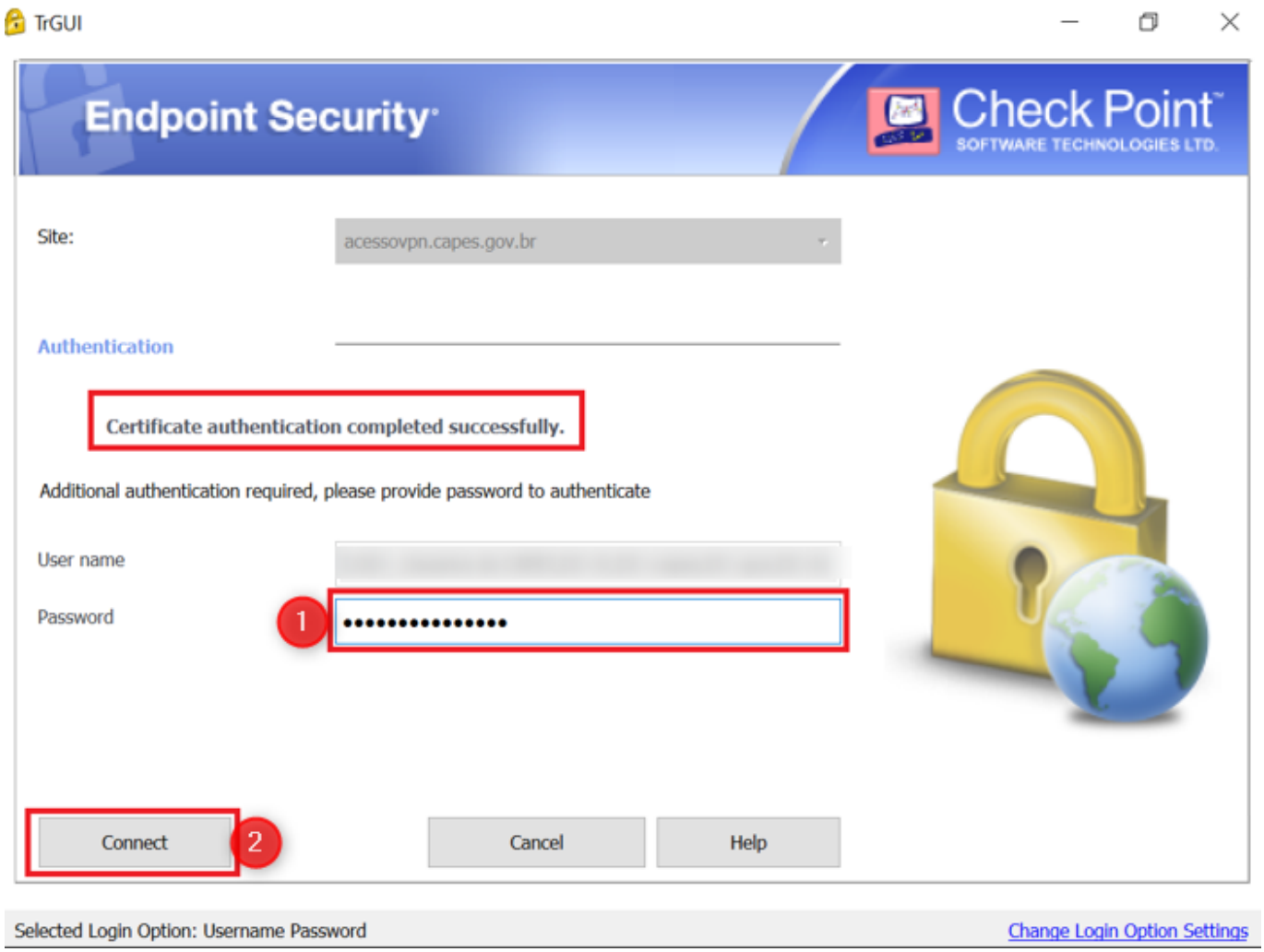



### 2.1.1 - Conectar

- Após a importação será necessário autenticar com a `senha do certificado`. Depois selecione "**Connect**".



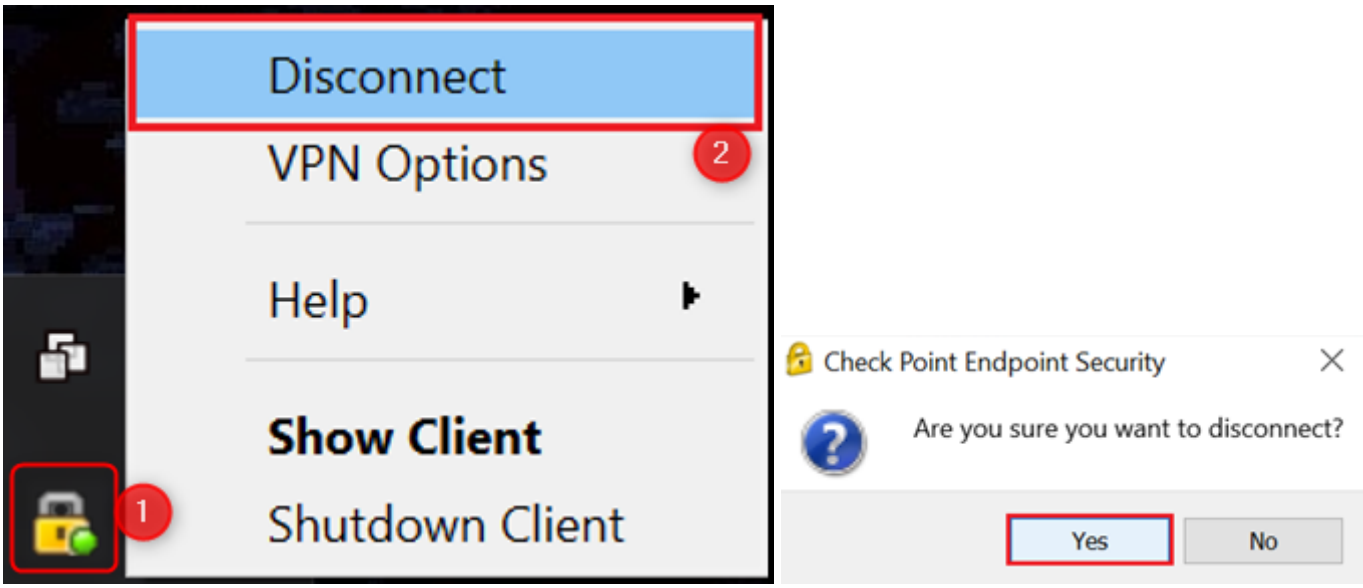

- Em seguida será necessário se autenticar com `sua senha da Rede CAPES (login)` e selecionar o botão "**Connect**".




- Espere enquanto a conexão é estabelecida. As janelas fecharão automaticamente.
- Pronto! Acesse os serviços que foram permitidos.

### 2.1.2 - Desconectar

- Para desconectar da VPN de forma segura, na barra de tarefas, selecione o ícone de cadeado e "**Disconnect**".




### 2.1.3 - Atualizar software client

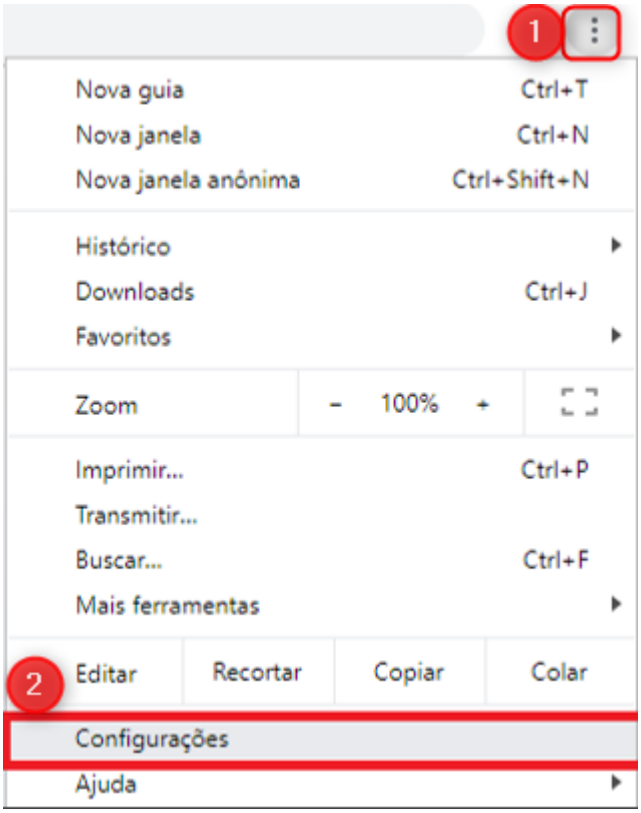
- Vá em **Painel de Controle** >> **Programas** >> **Desinstalar um programa**
  - Selecionar o client: **Check Point VPN**
  - Clicar no menu superior: **Desinstalar**
- Para instalar a versão mais recente vá na opção 2.1 - Instalar Software Client.

## 2.2 - Utilizando Navegador (**Opção 2**)

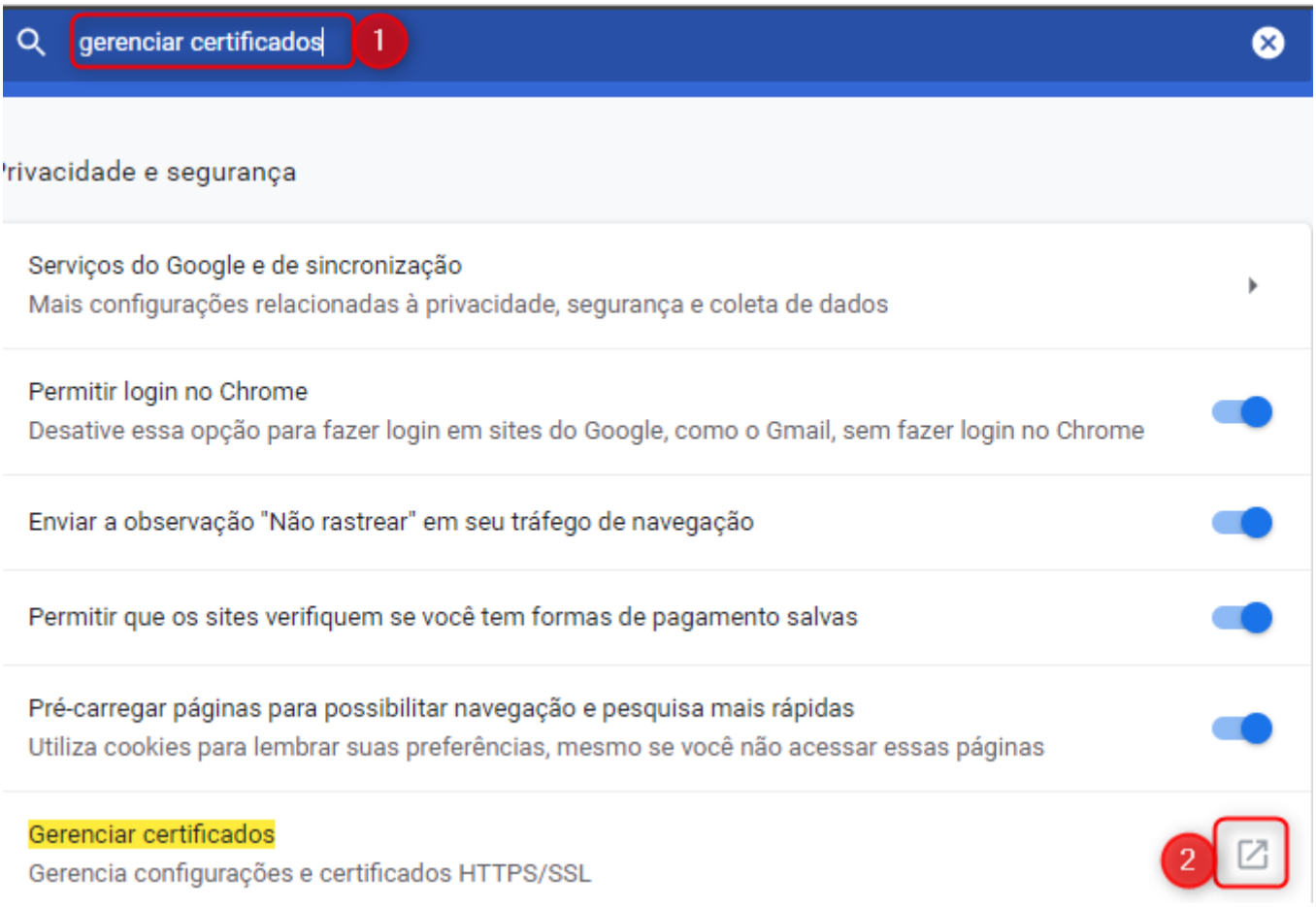
Outra forma de utilizar a VPN é utilizando o navegador.

> O procedimento abaixo foi validado no **Google Chrome**.

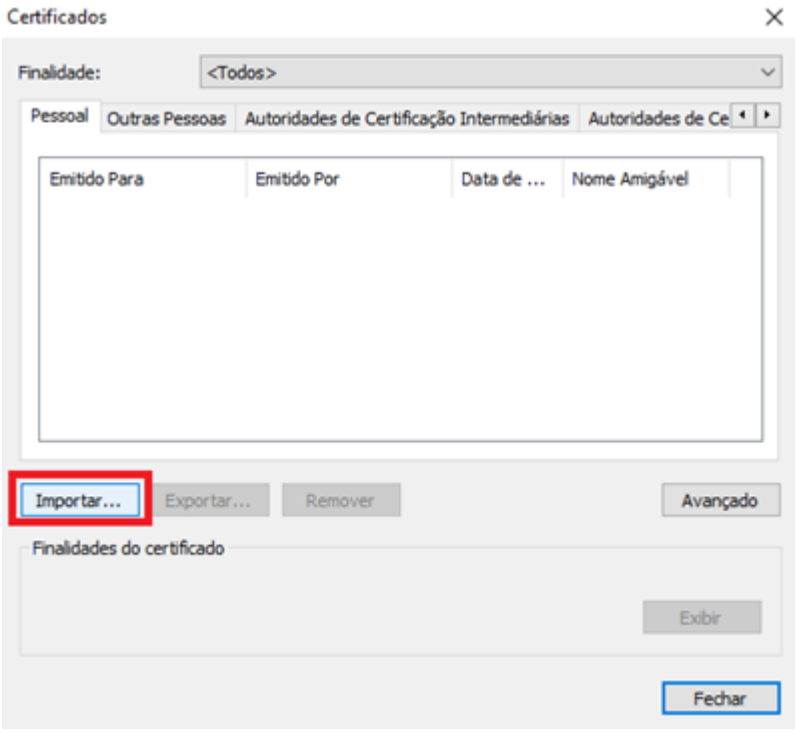
- Acesse https://acessovpn.capes.gov.br
- Adicione o seu certificado digital no repositório do navegador da seguinte forma.
- Abra as configurações do navegador.



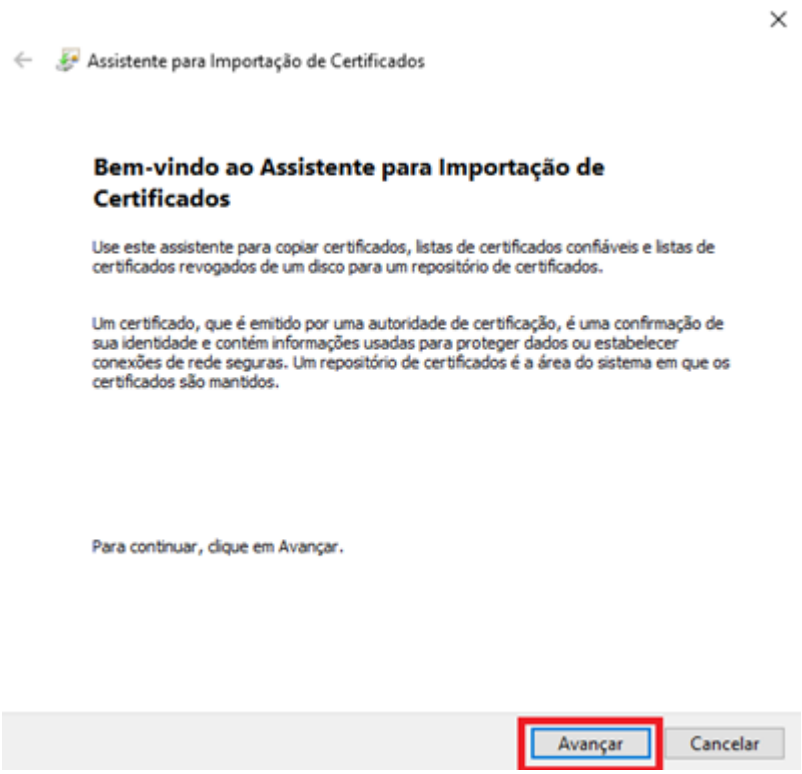

- Abra a opção de gerenciar certificados.



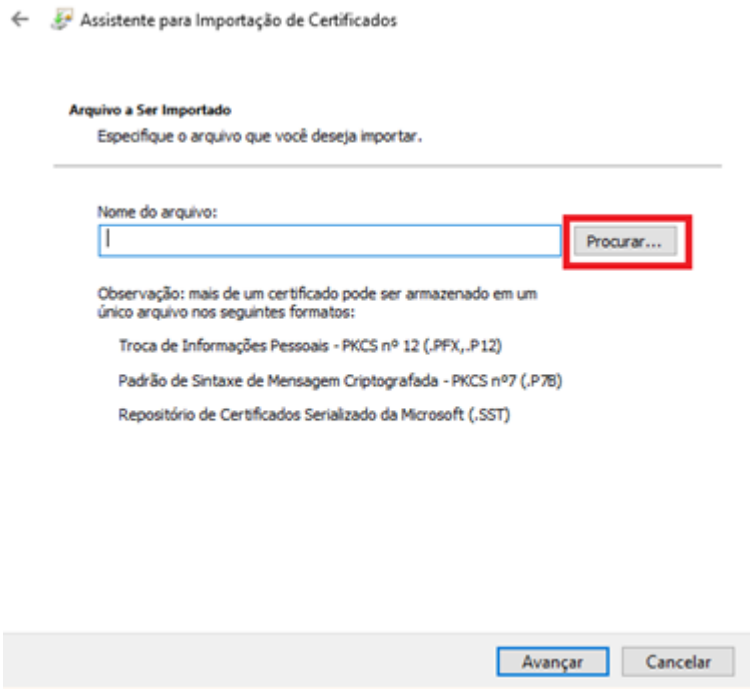

- Importe o certificado.




- Siga com o passos do assistente de importação.

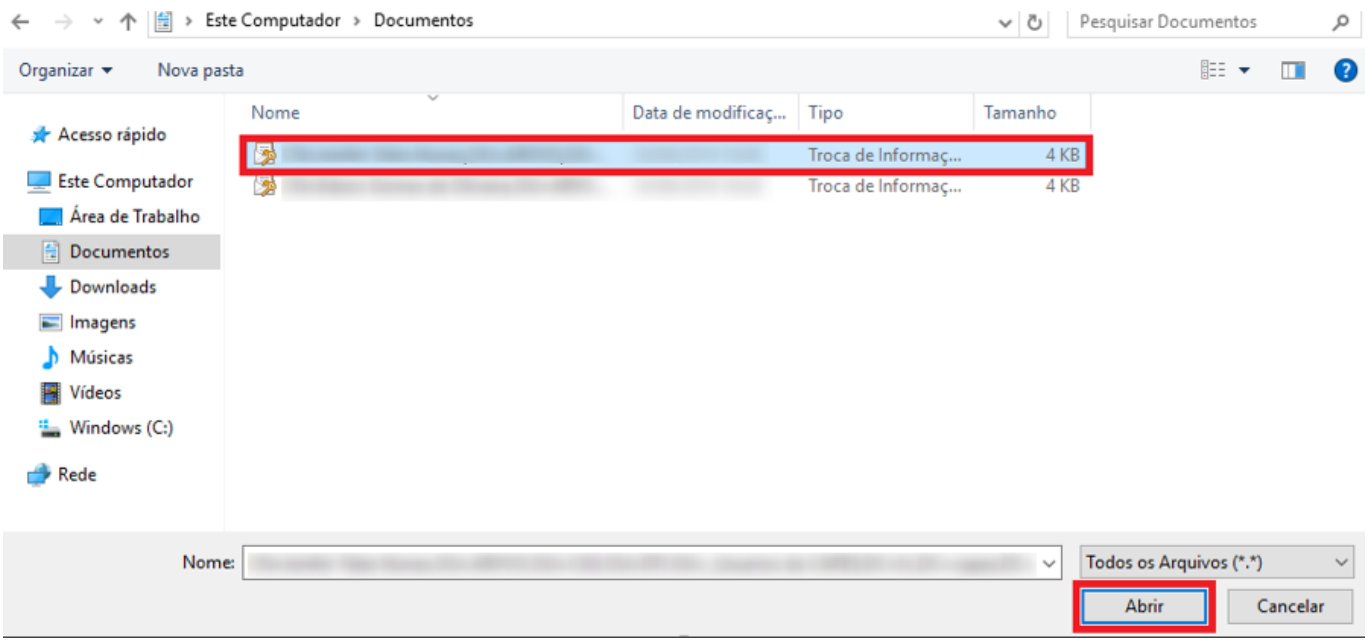



- Localize o certificado.

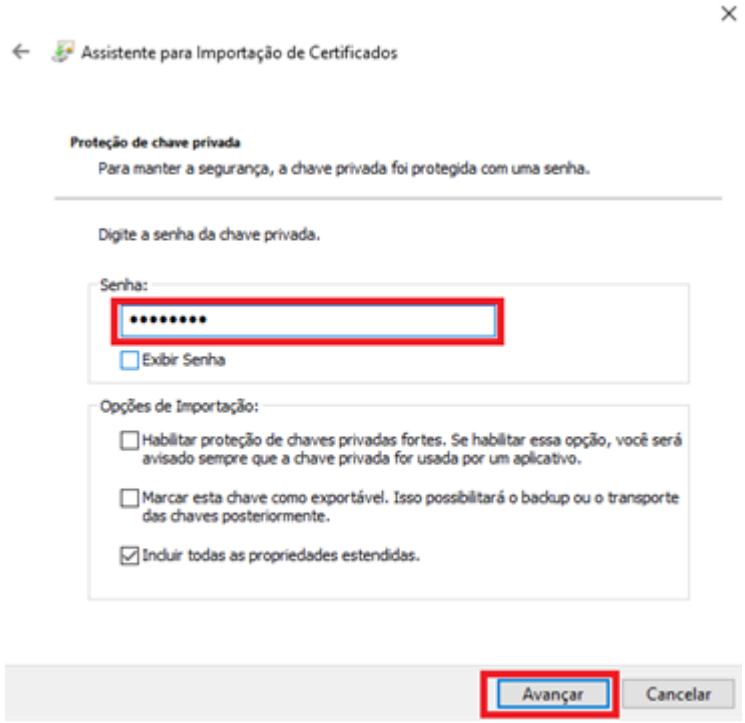



- Selecione o `seu certificado digital` (enviado por e-mail), salvo na sua pasta de preferência, em seguida selecione "**Abrir**".

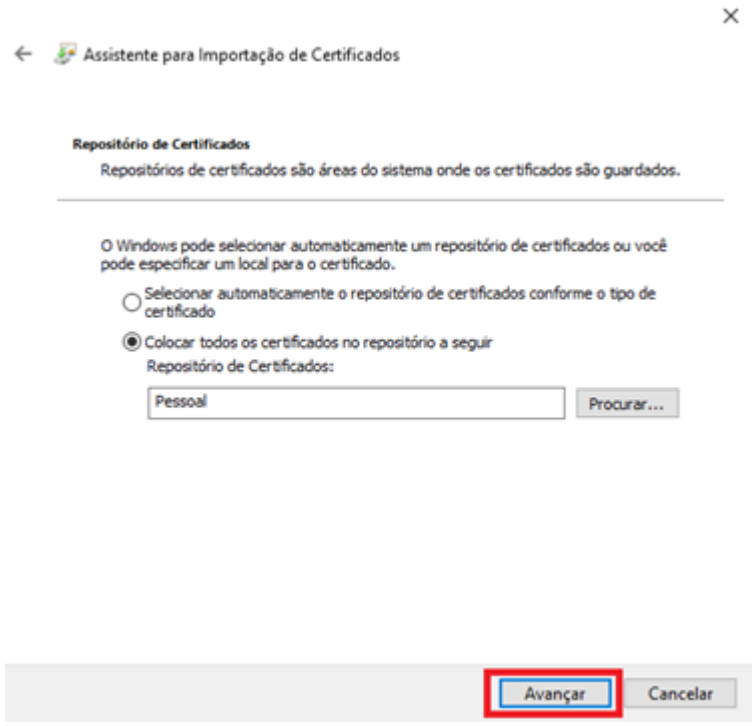
> **NOTA:** Lembre-se de **apagar** o certificado de seu e-mail e guardá-lo em local **seguro**.



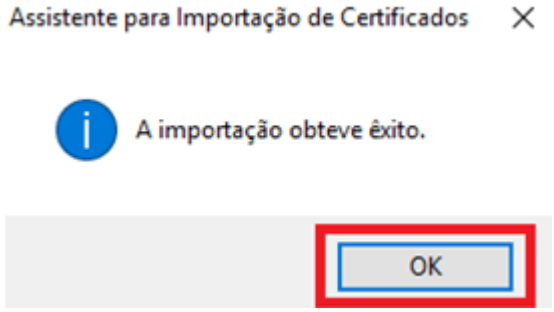

- Clique em "**Avançar**" e depois digite a `senha do certificado`.




- E siga em avançar.

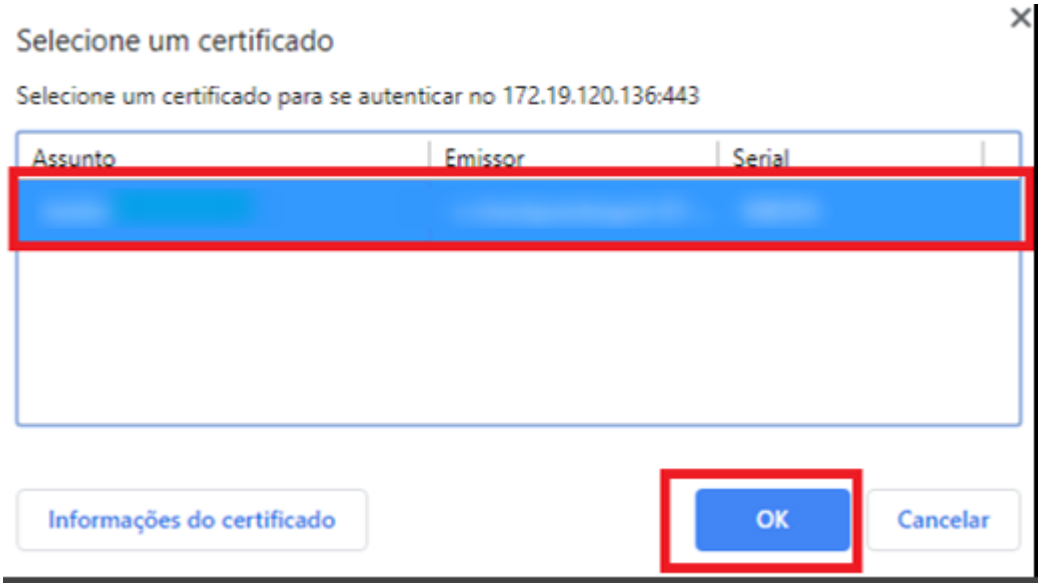



- Ao concluir a instalação aparecerá a mensagem:



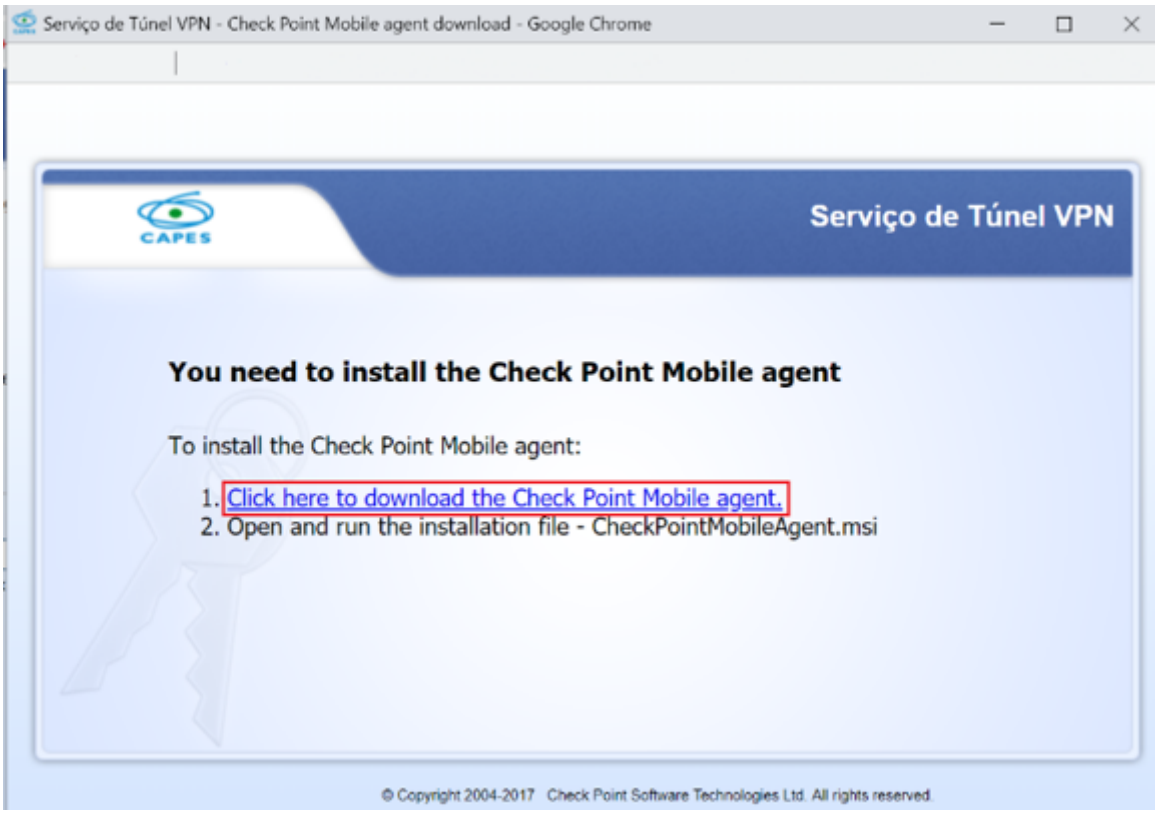
### 2.2.1 - Conectar

- Após a importação do certificado, volte para a página https://acessovpn.capes.gov.br e clique em "**Entrar**". Surgirá uma janela para seleção do certificado, selecione o seu e clique “OK”.

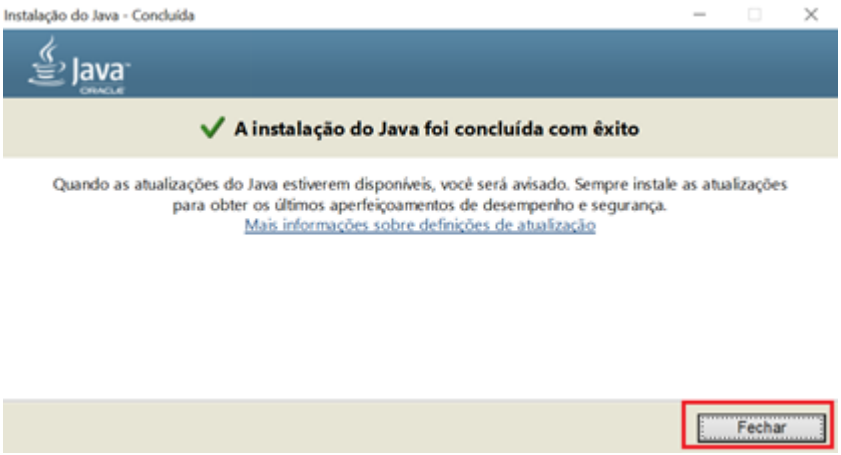



- Autentique-se utilizando `sua senha da Rede CAPES (login)`

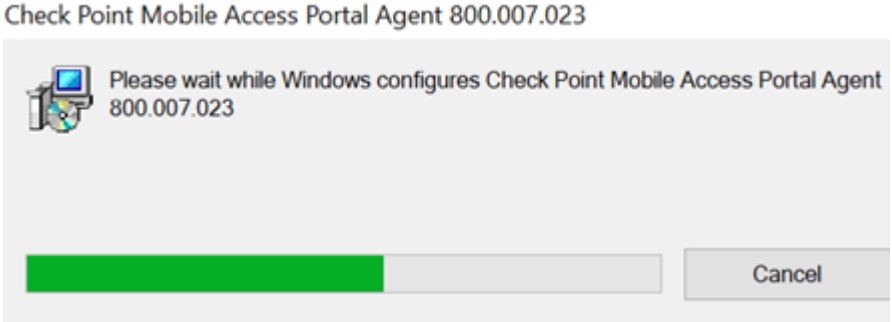

- Ao conectar será necessário fazer o **download do Check Point Mobile agent**.



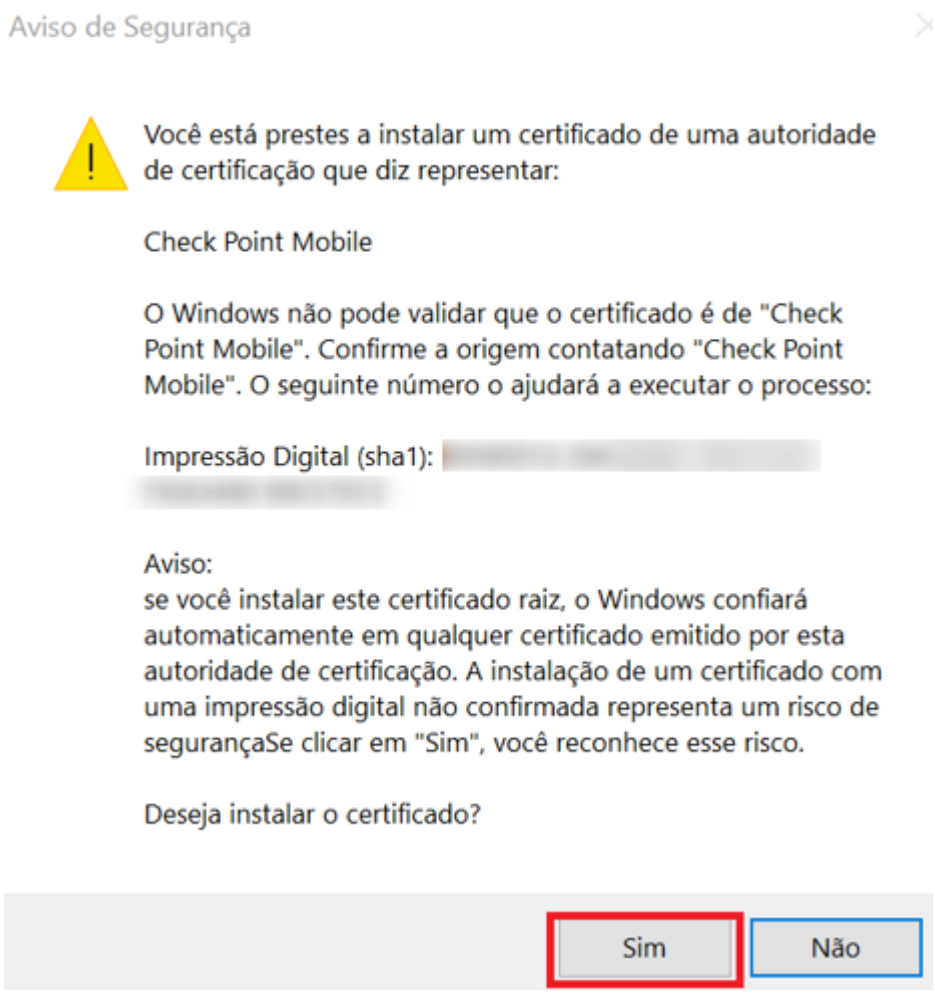

- Você precisa ter o **Java** instalado na sua máquina para usar o Checkpoint Mobile Access Agent, caso você não tenha, será redirecionado para o portal da Check Point no qual informa a necessidade de possuir o Java.
    - Faça download do Java em https://www.java.com/pt_BR e siga orientações de instalação.



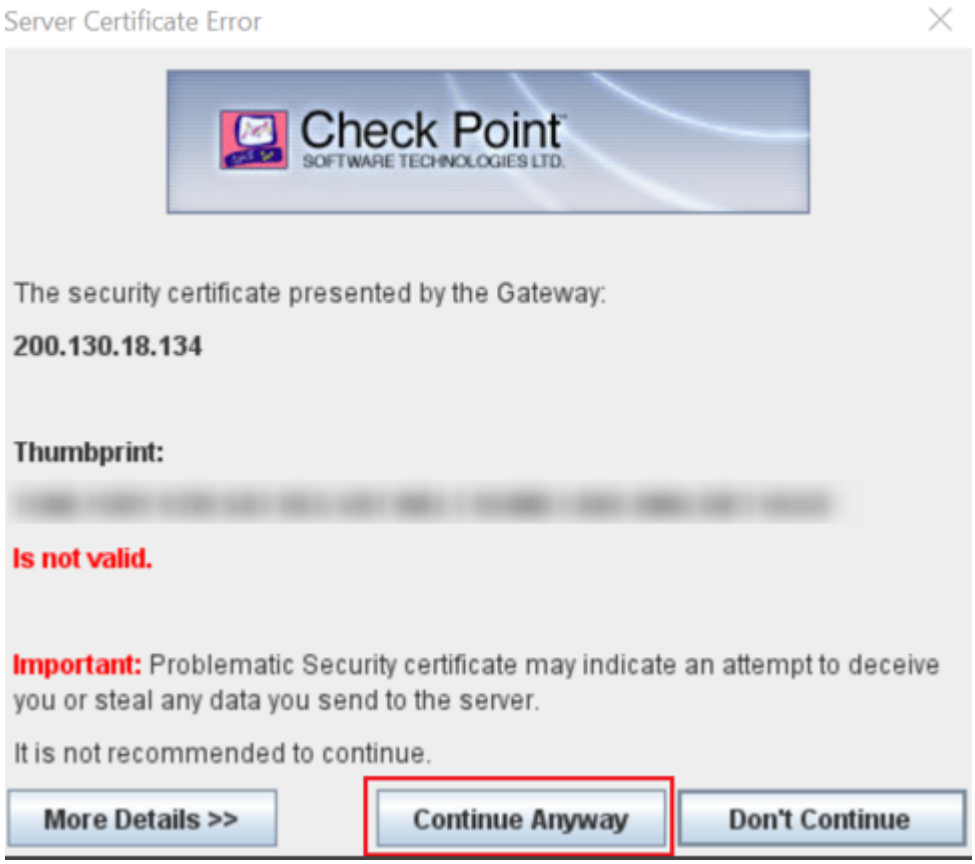

- Depois, aguarde enquanto o Windows configura o Checkpoint Mobile Access Portal Agent.



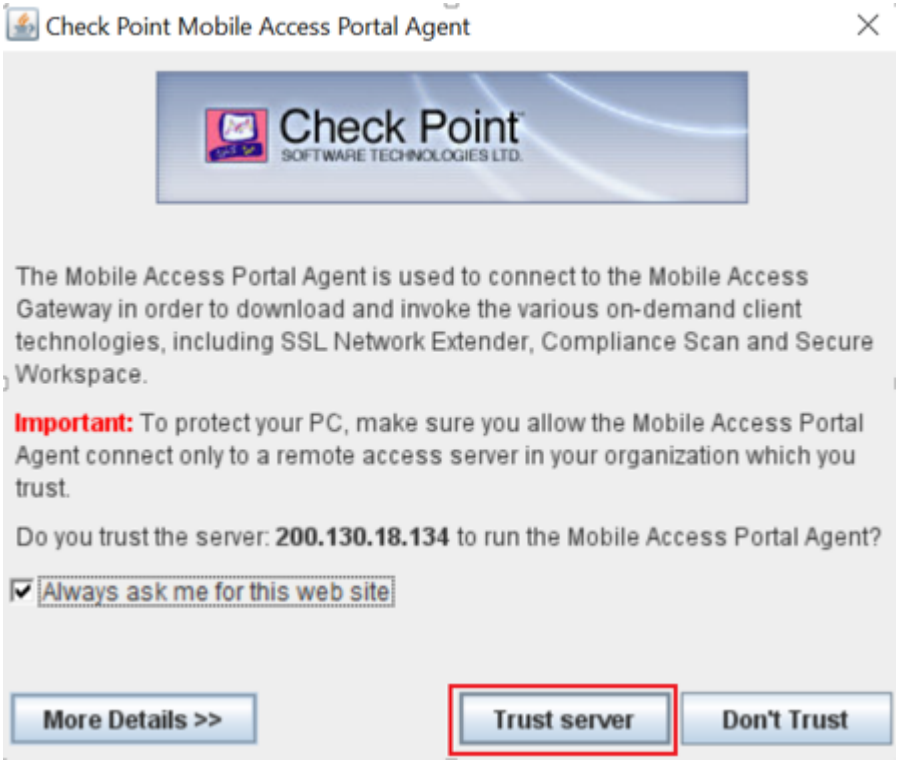

- No aviso de segurança, confirme.




- Nas próximas janelas selecione "**Continue Anyway**".



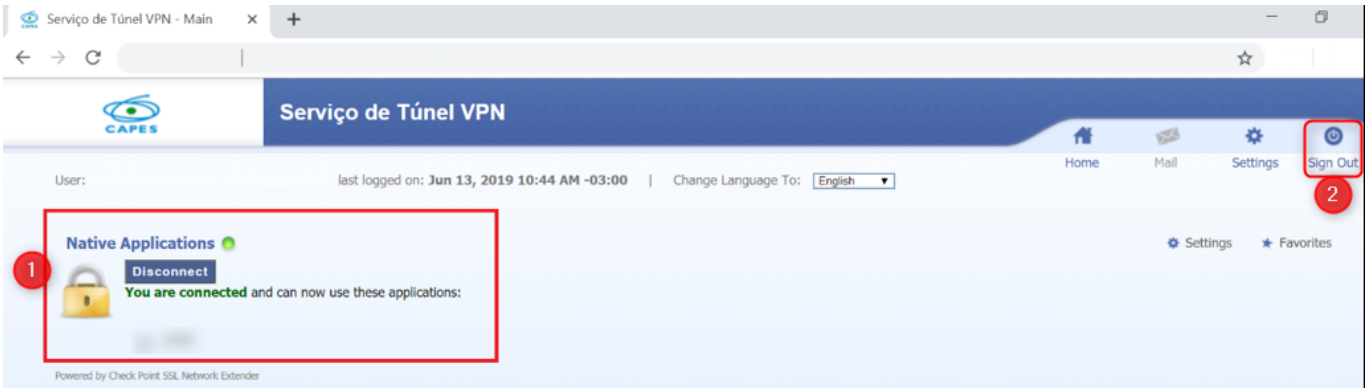

- E também "**Trust server**".




- Aguarde enquanto o Windows configura o serviço.
- Pronto! Acesse os serviços que foram permitidos para sua conta.

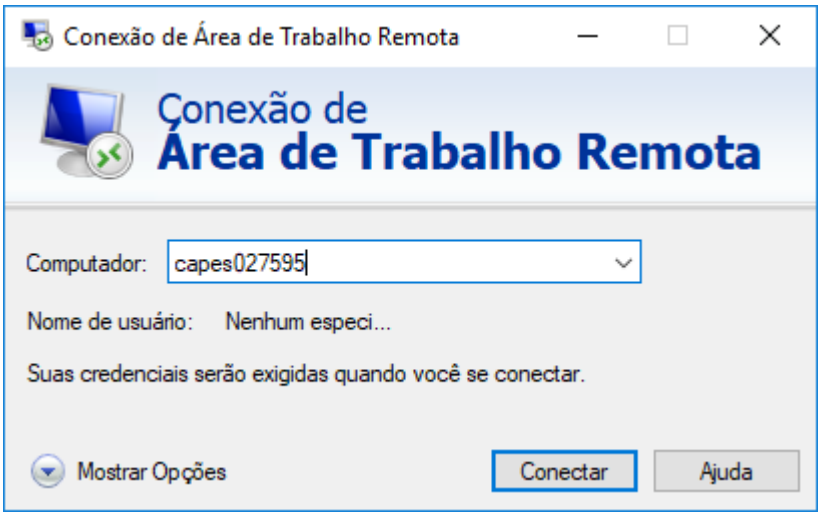
### 2.2.2 - Desconectar

- Para desconectar da VPN de forma segura, clique em "**Disconnect** e depois faça "**Logoff**".

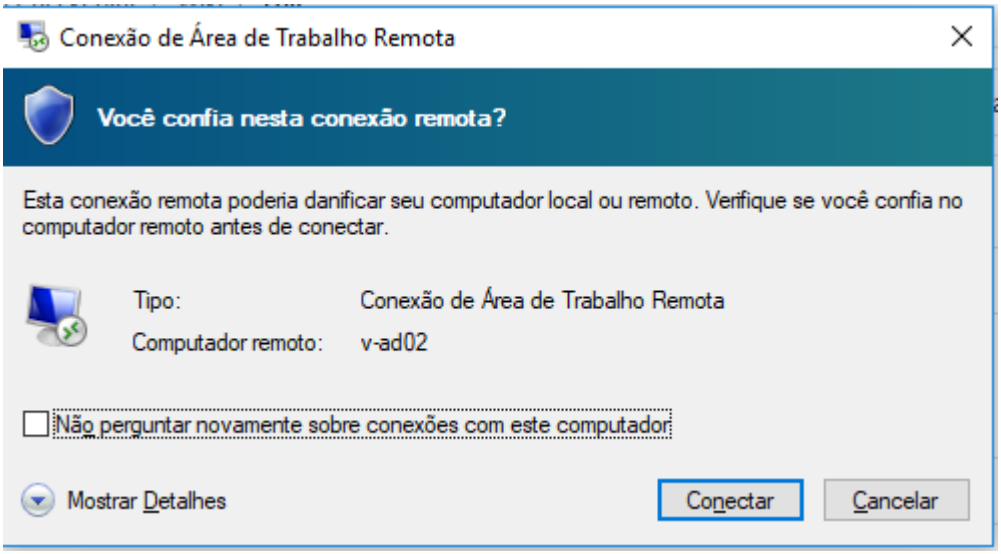



## 2.3 - Acesso Remoto a Estação Windows

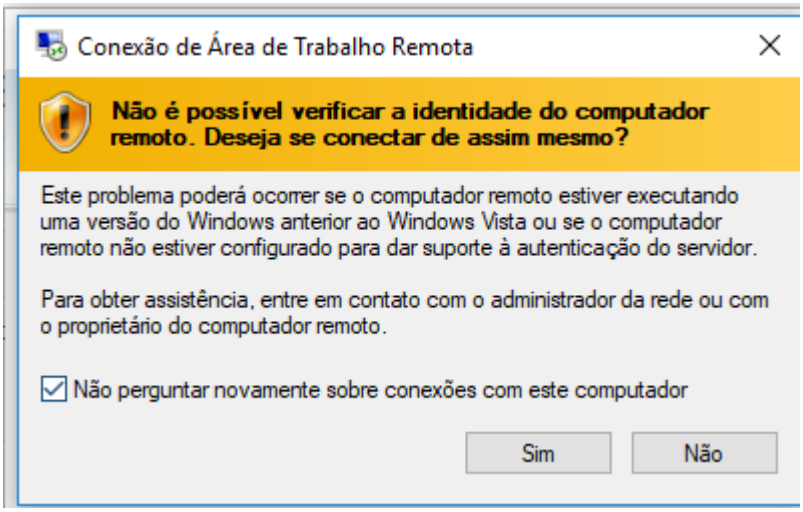
Utilize o aplicativo **Conexão de Área de Trabalho Remota** > Digite o nome da estação no campo **Computador** e clique em **Conectar**



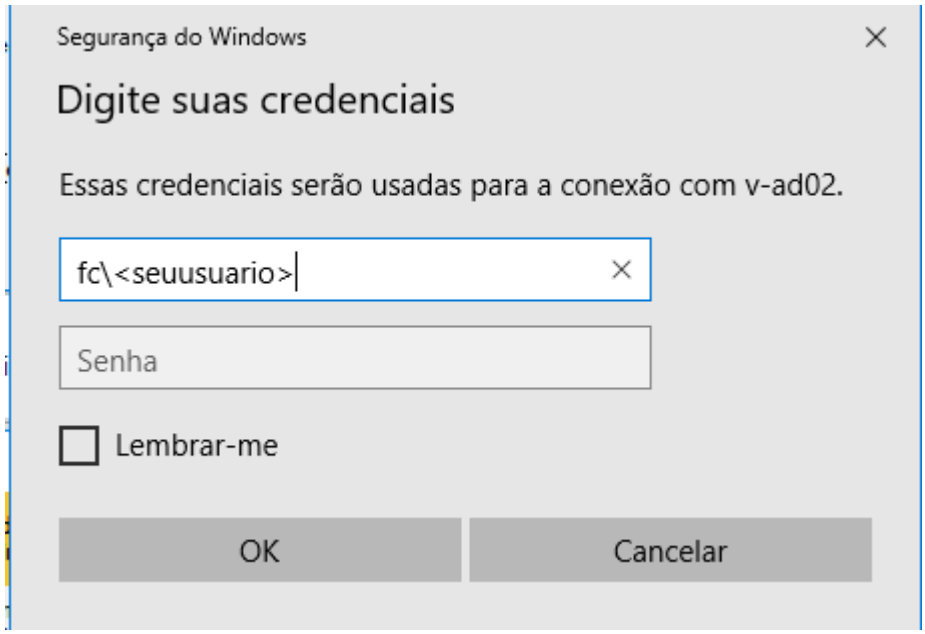

Confie na sessão remota




Clique em **Sim** na próxima janela que abrirá.




Digite o no campo usuário:fc<seuusuario> e a senha, clique em Ok.




# 3 - Linux

## 3.1 - Utilizando Navegador (**Opção Única**)

Os sistemas operacionais Linux não possuem uma versão do cliente VPN, utilize seu navegador e sigas os passos a seguir:

- **Java** - verifique se você possui o Java habilitado em seu computador junto com todas as bibliotecas atualizadas.
- **Bibliotecas** - instale as bibliotecas de acordo com a sua distribuição, as bibliotecas estão disponíveis aqui: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk119772
- Distribuição - **Ubuntu** instalação do JAVA e Bibliotecas

```
sudo apt-get install -y openjdk-17-jdk
sudo apt-get install -y libnss3-tools openssl xterm
```

## 3.2 - Plataforma Suportada

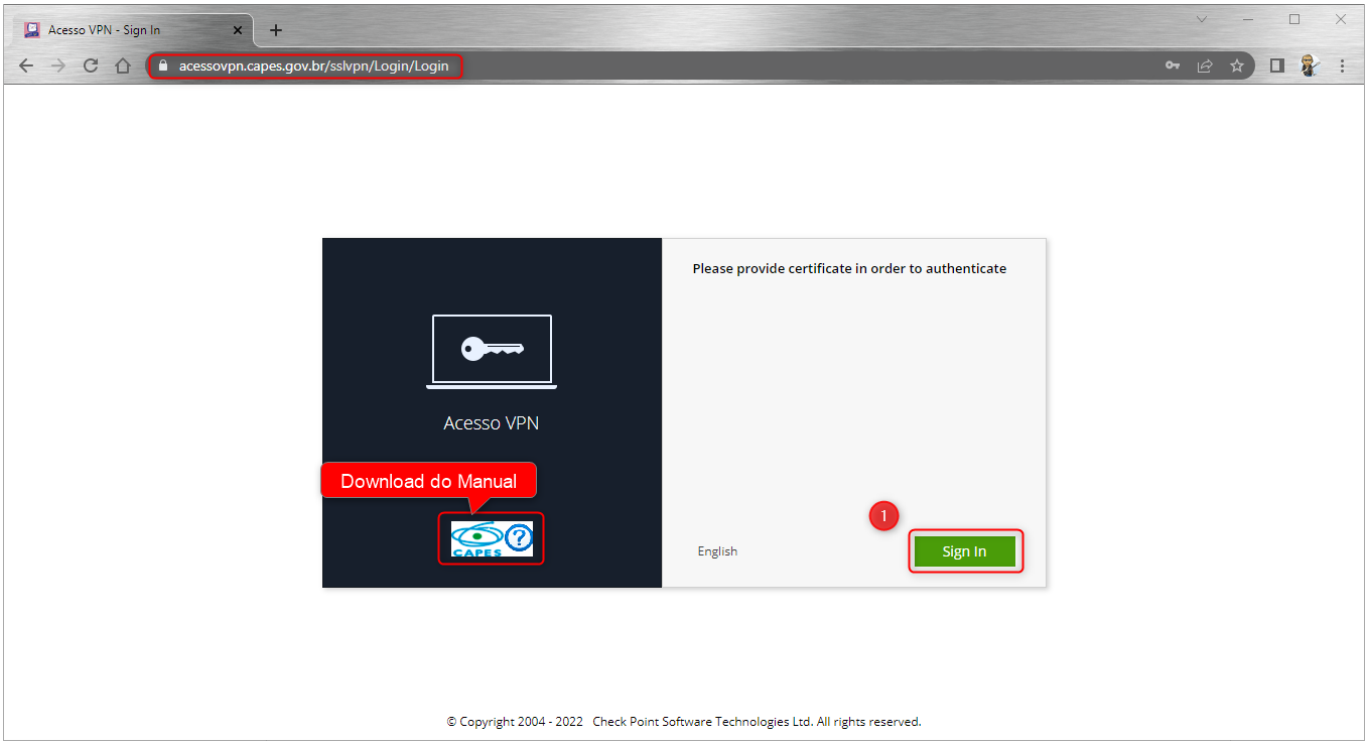
- Mobile Access Portal Agent is supported on these *nix Systems.
    - **openSUSE** 42.1, 42.2, 42.3, Leap 15 – 15.5
    - **CentOS** 7.3 - 9
    - **Fedora** 24 - 39

    - **Ubuntu** 16.04 - 23.10
    - **RHEL** 7.3 - 9.3 (Workstation)

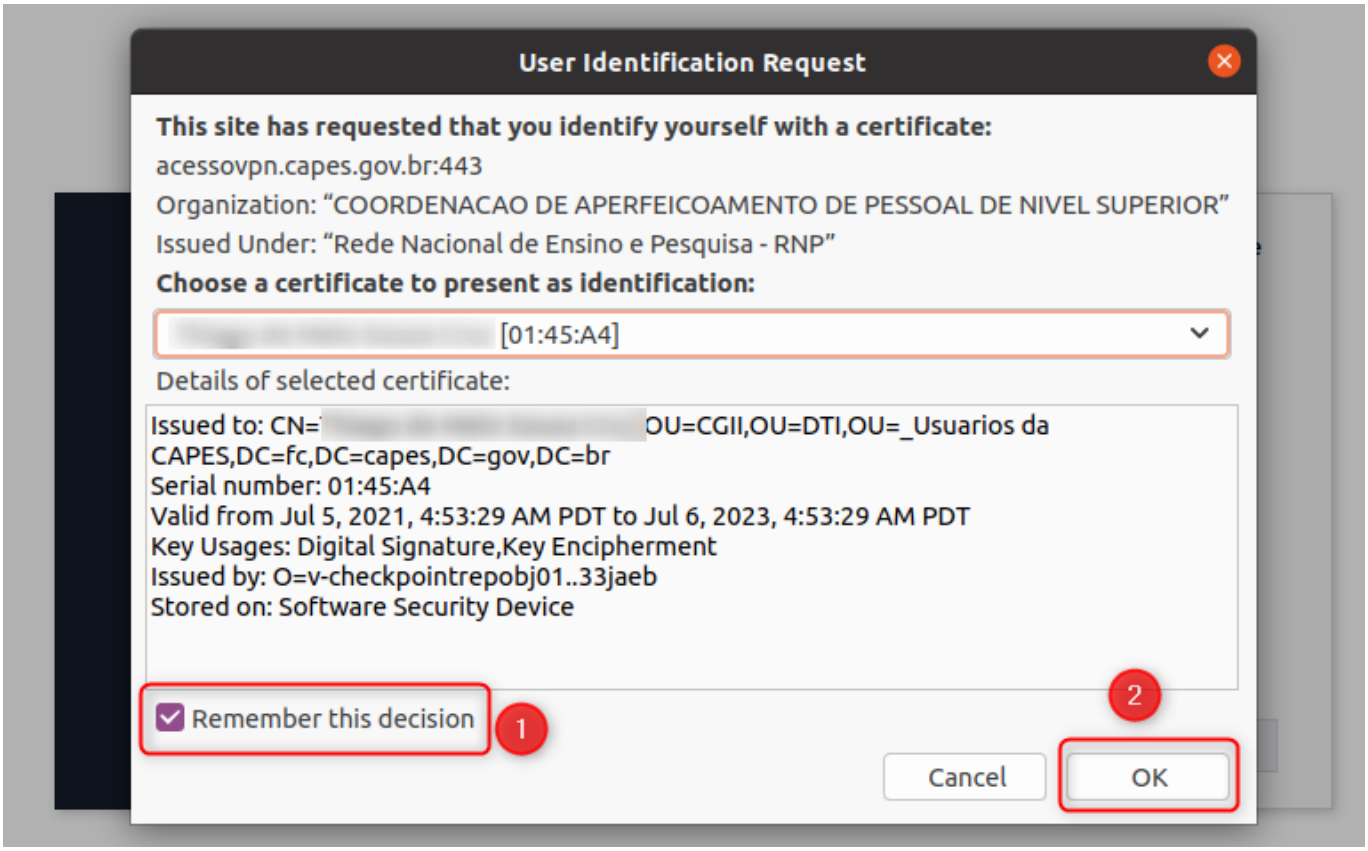
- Importe o `seu certificado digital` no Browser (enviado por e-mail), salvo na sua pasta de preferência.

> **NOTA:** Lembre-se de **apagar** o certificado de seu e-mail e guardá-lo em local **seguro**.

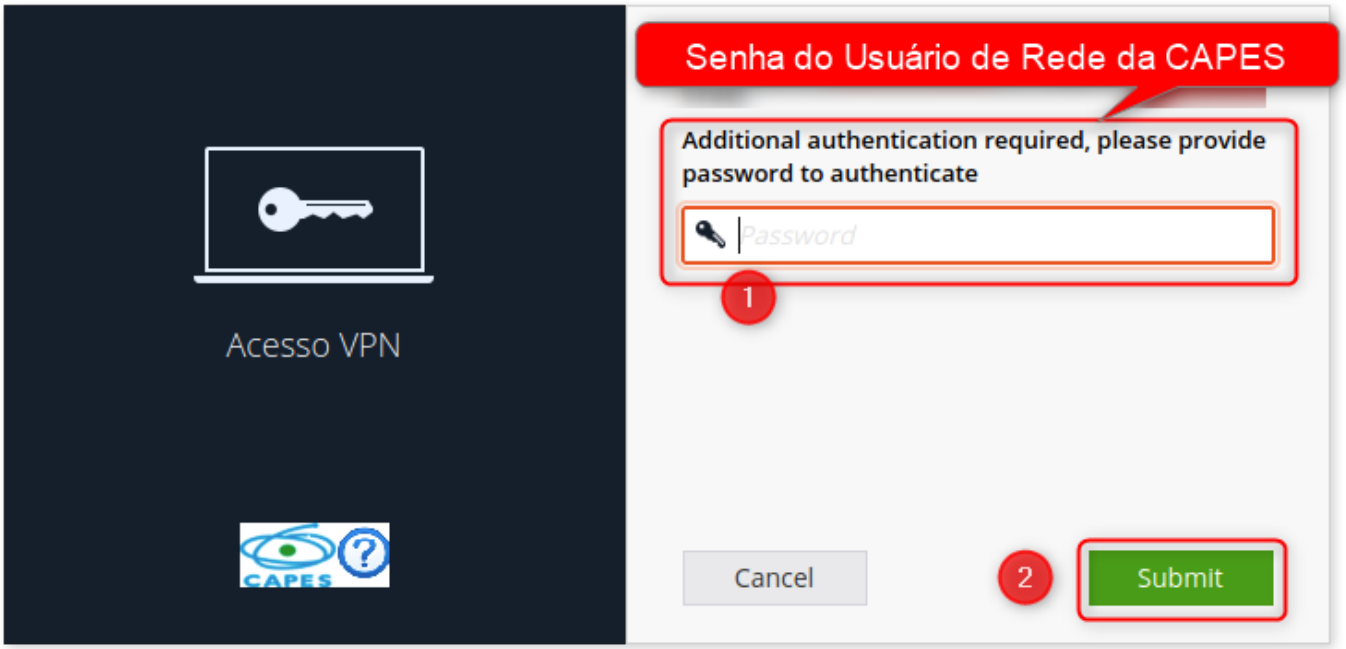
- Acesse https://acessovpn.capes.gov.br




- Selecione o certificado importado.

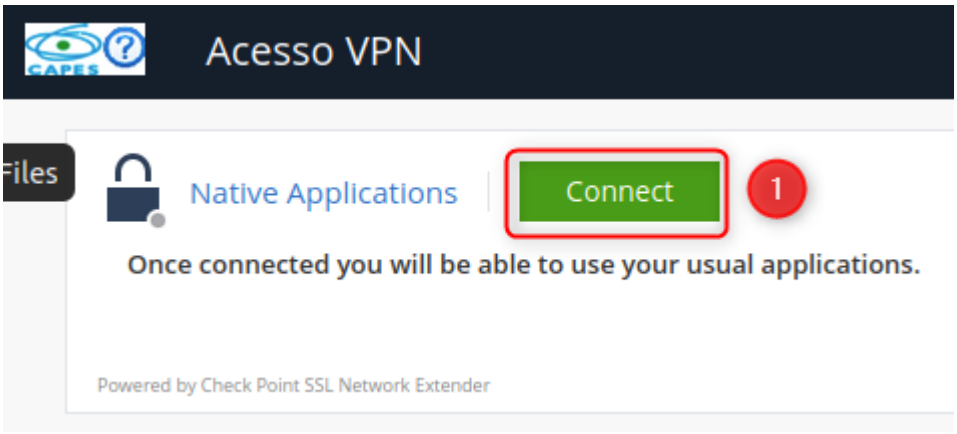


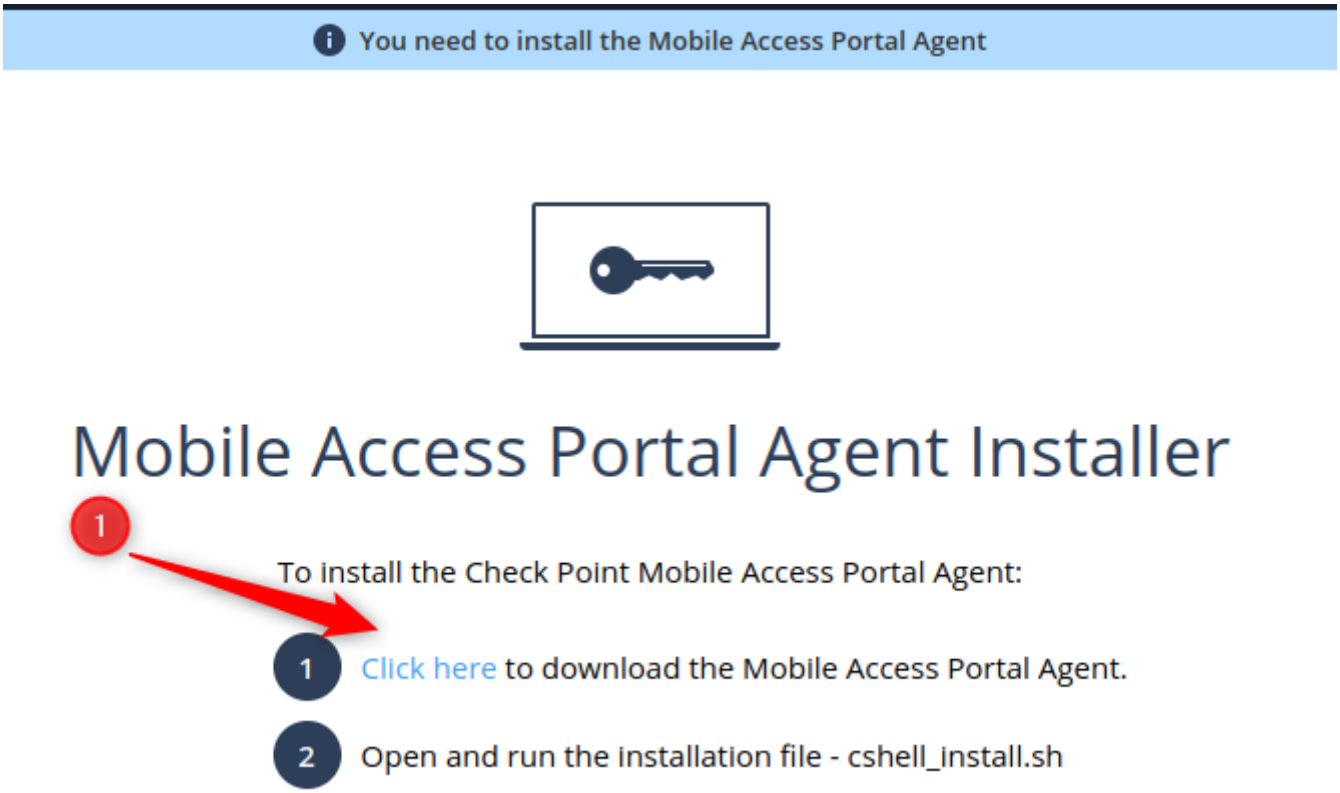

- Digite a senha do seu usuário de rede da CAPES




### 3.2.1 - Conectar

- Após as configurações acima, selecione o botão "**Conectar**".
- Irá surgir uma janela para a instalação do CheckPoint Mobile Access. Faça Download do arquivo.




> **NOTA:** Lembre-se de fechar o Browser

- Instalar o pacote abaixo

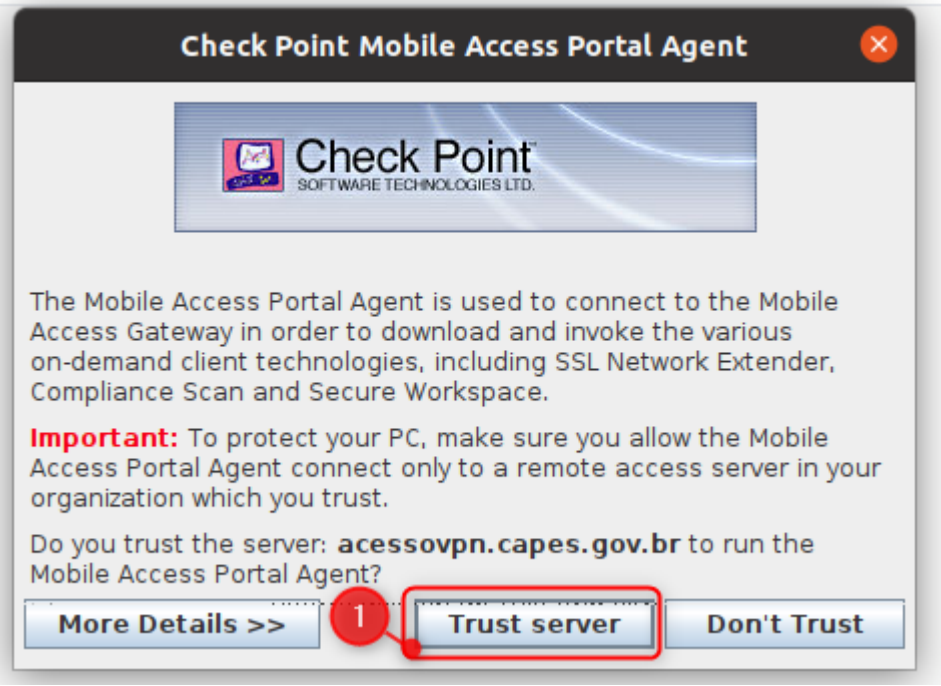
```
sudo apt-get install -y gcc-multilib
```

- Instale o arquivo em sua máquina com o comando:

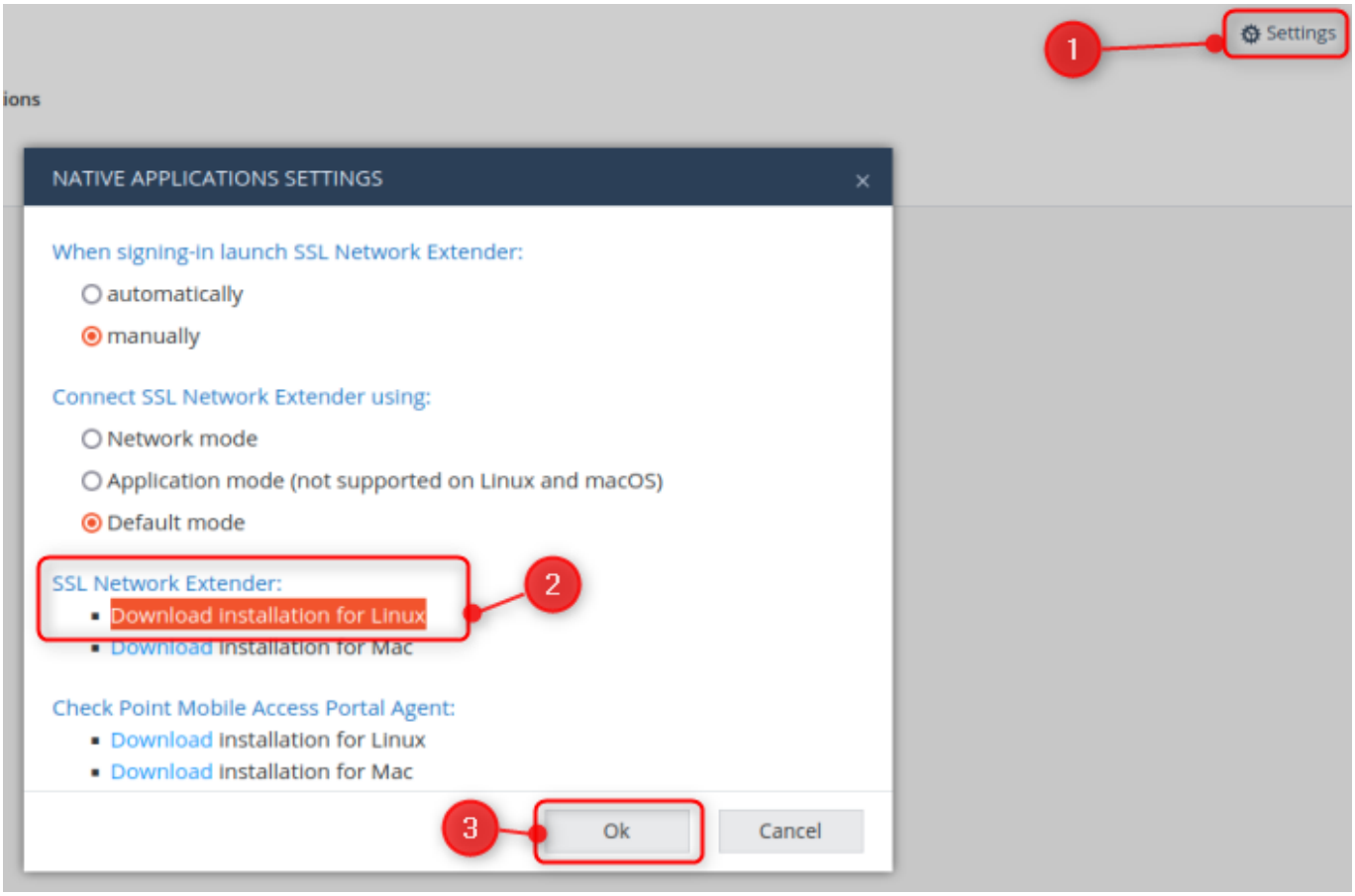
```
sudo sh ./cshell_install.sh
```

```
tc@ubuntu:~/Downloads$ sudo sh ./cshell_install.sh
Start Check Point Mobile Access Portal Agent installation
Extracting Mobile Access Portal Agent... Done
Installing Mobile Access Portal Agent... Done
Installing certificate...
Firefox must be closed to proceed with Mobile Access Portal Agent installation.
Press [ENTER] key to continue...
```

- Clicar em: "**Trust server**".



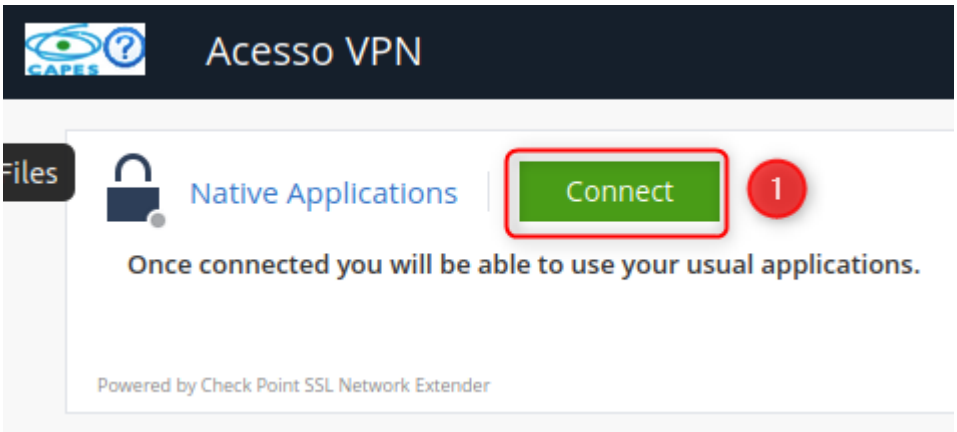

- Acesse https://acessovpn.capes.gov.br
  - Clicar no canto superior direito em: **Settings**
  - Na opção SSL Network Extender: clicar em **Download installation for Linux**
  - Clicar no botão: **OK**



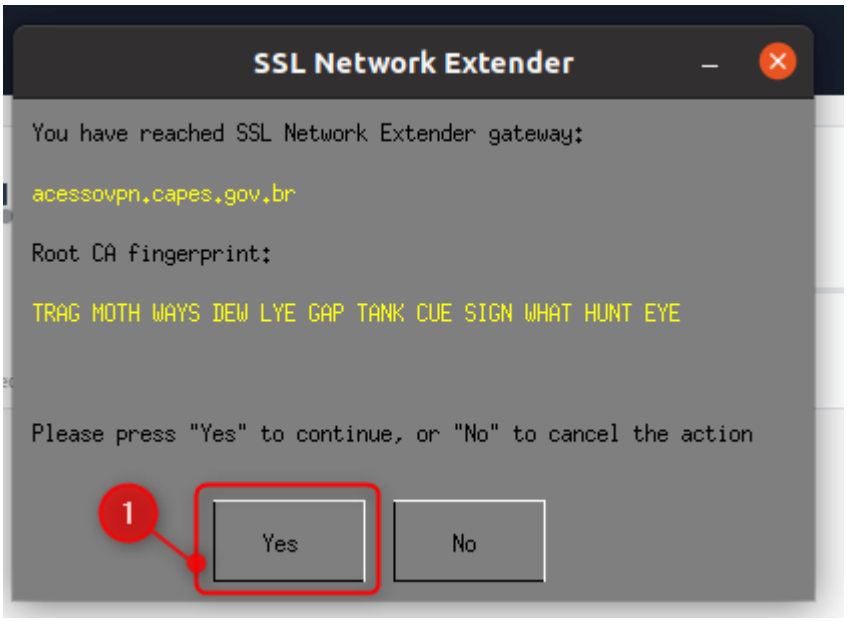

- Instale o arquivo em sua máquina com o comando:

```
sudo sh ./snx_install.sh
```

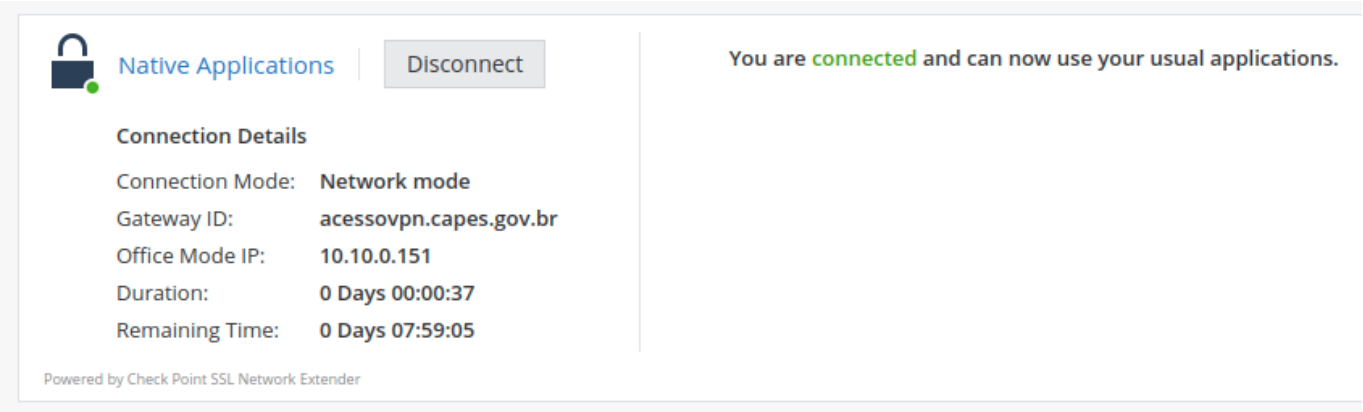
- Clicar no botão: Connect




- Clicar no botão: **Yes**

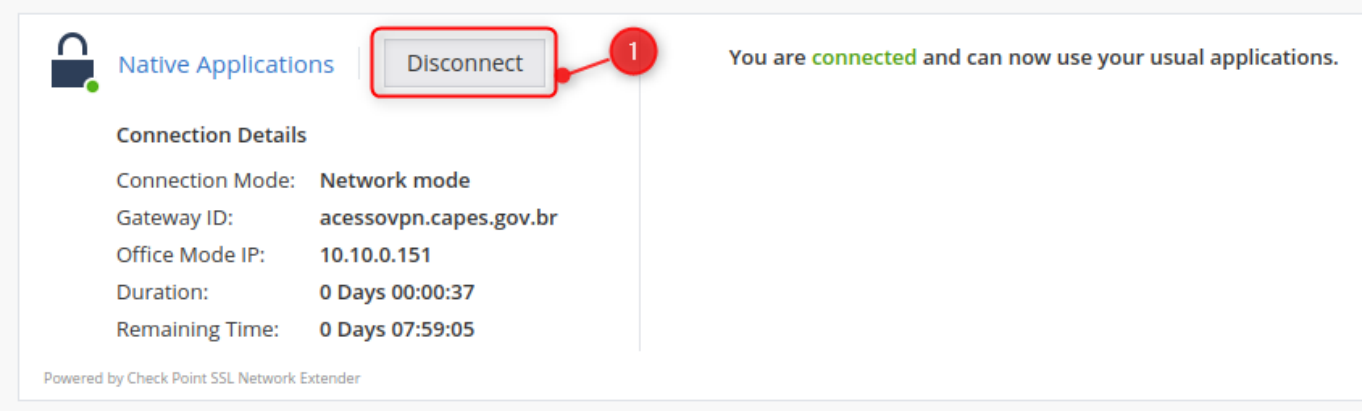



- Detalhes da conexão:




### 3.2.2 - Desconectar

- Para desconectar da VPN de forma segura, clique em "**Disconnect** e depois faça "**Logoff**".



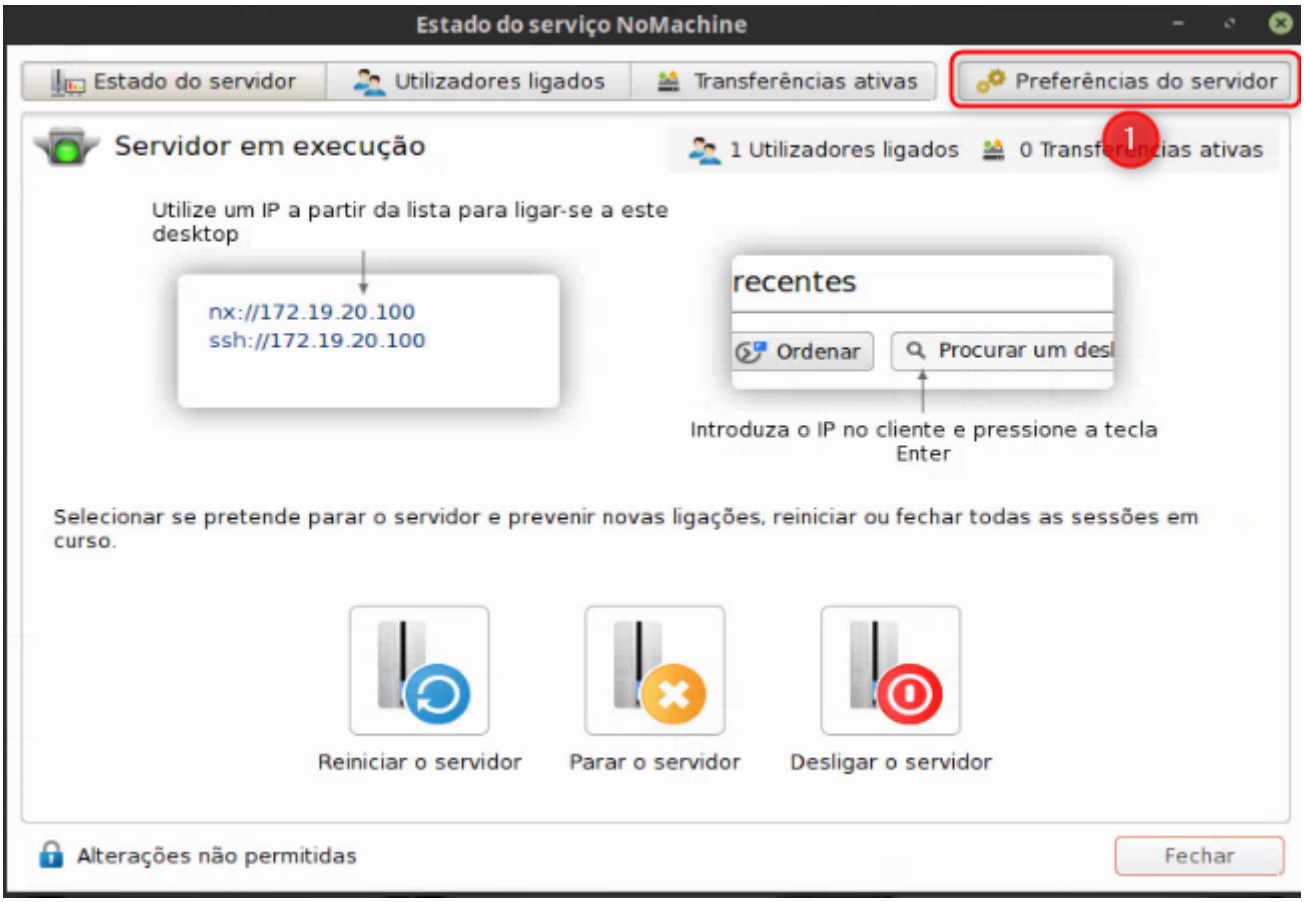
## 3.3 - Acesso Remoto a Estação

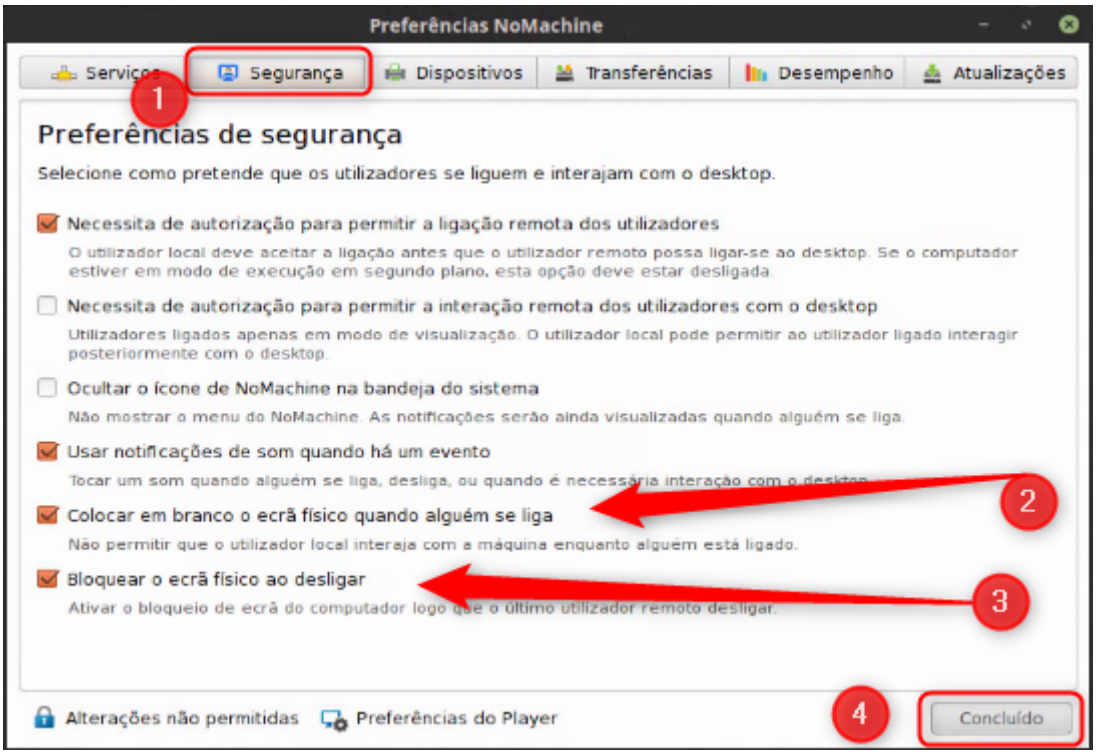
Para o acesso a uma estação de trabalho **Linux** de forma remota, siga os passos:

**Download** - o aplicativo homologado para uso e recomendado é:

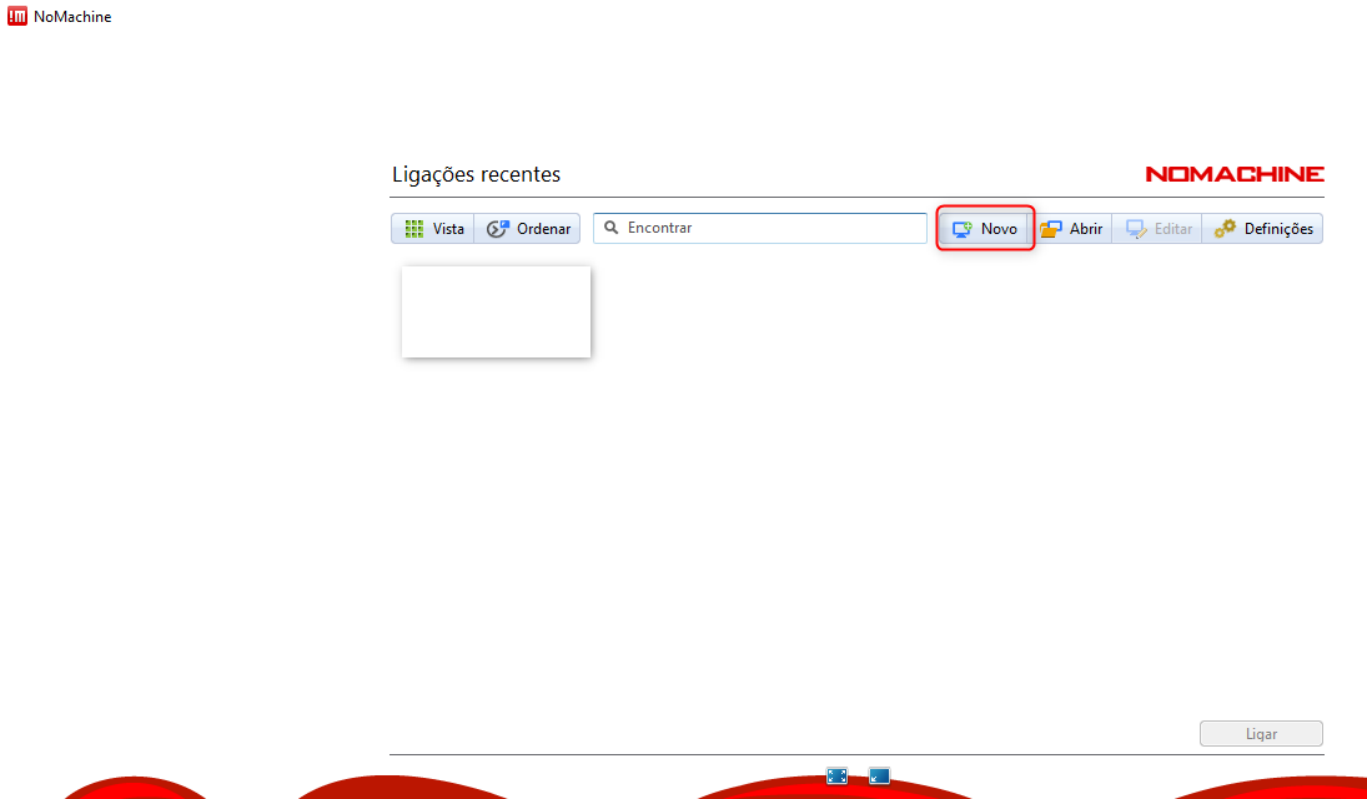
- **Nomachine** - https://www.nomachine.com/pt-pt/download
- Configuração para a estação linux depois da instalação.

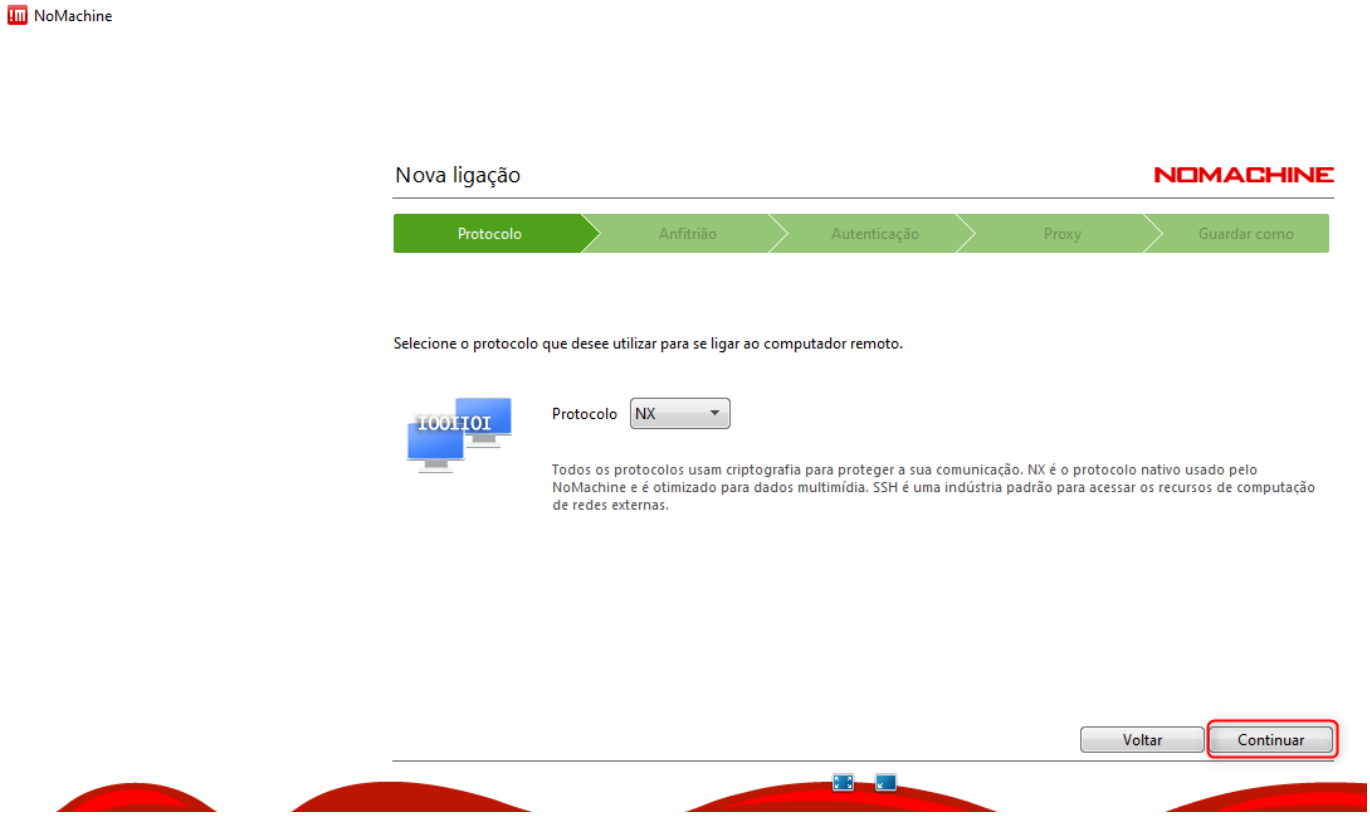
**Configuração na estação Linux** - Após o download e instalação do aplicativo nomachine: realizar as seguintes configurações conforme imagens abaixo para sua tela ficar bloqueada quando for realizado o acesso remoto:

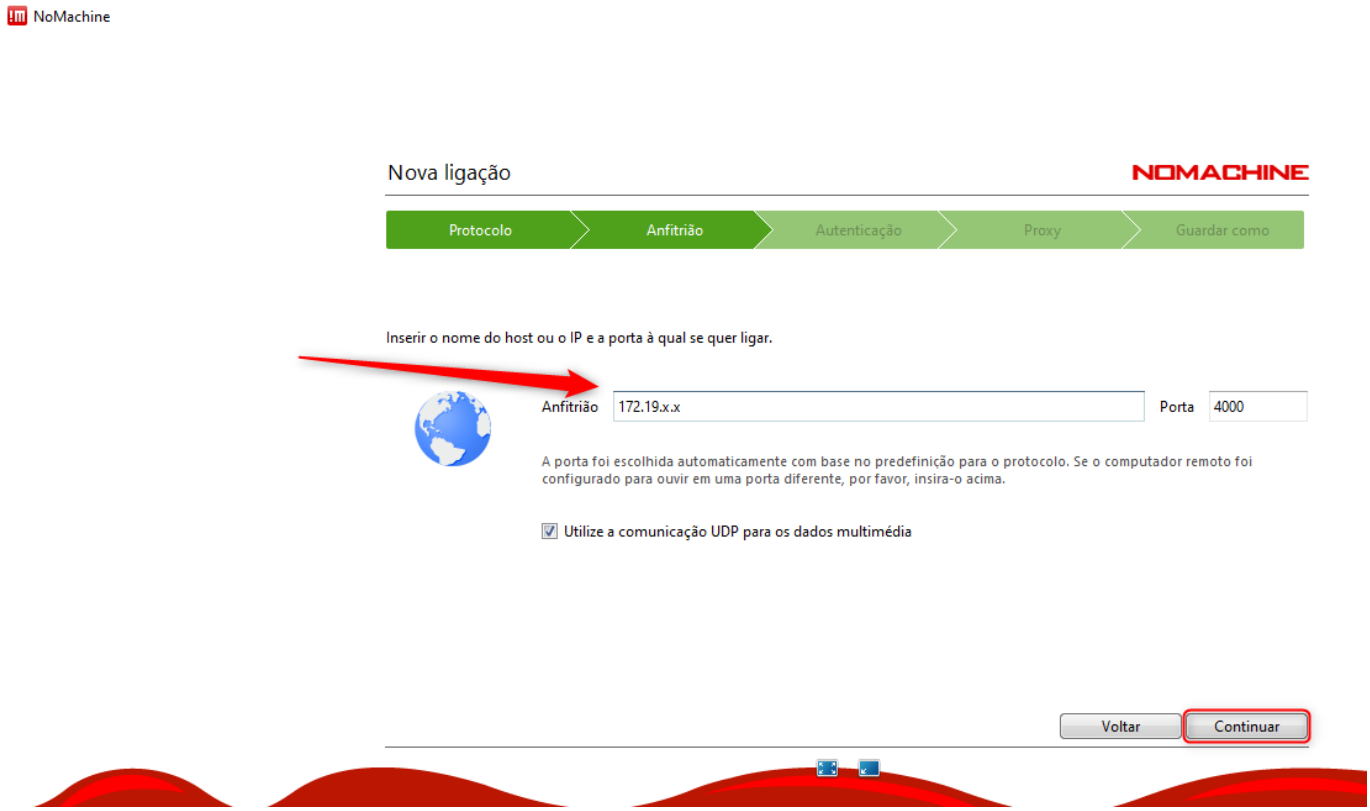


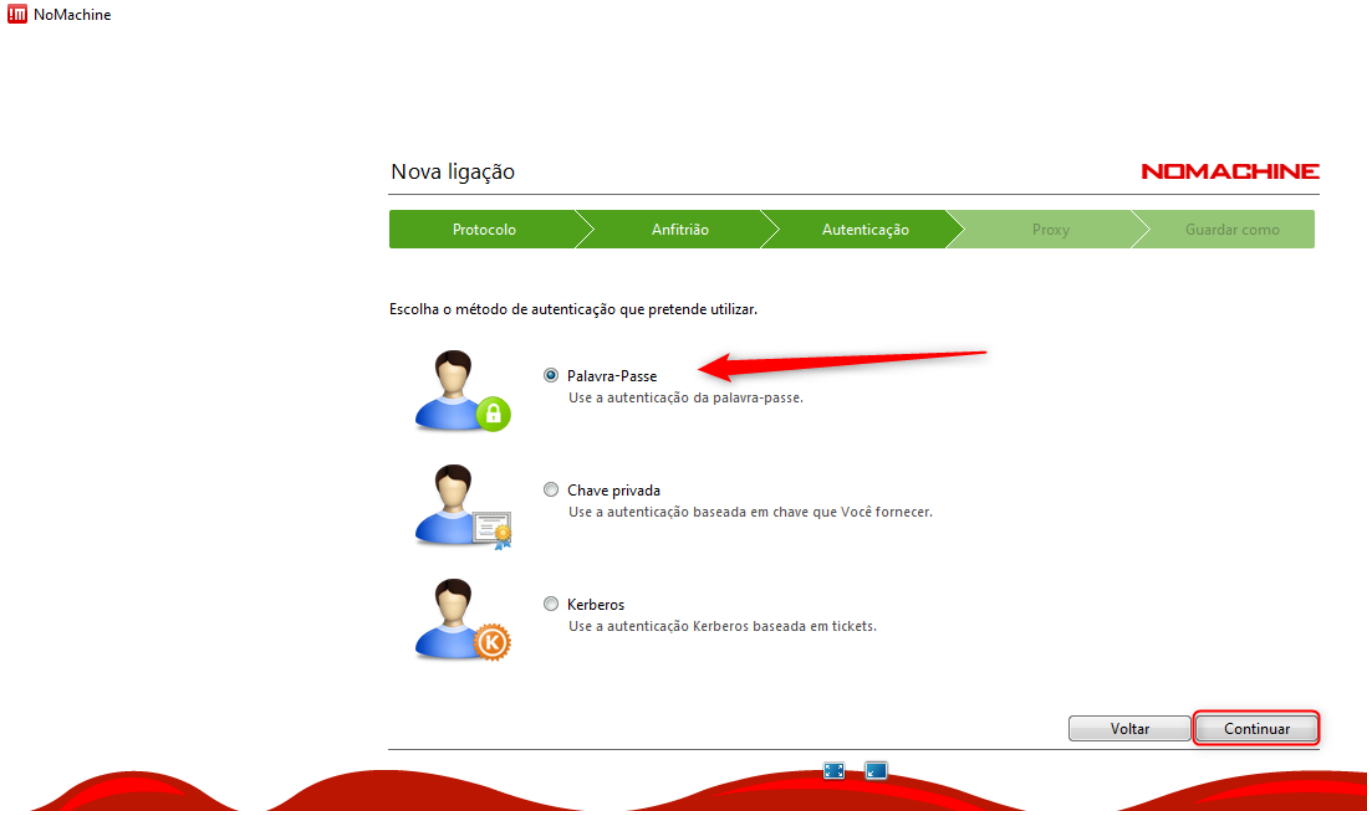



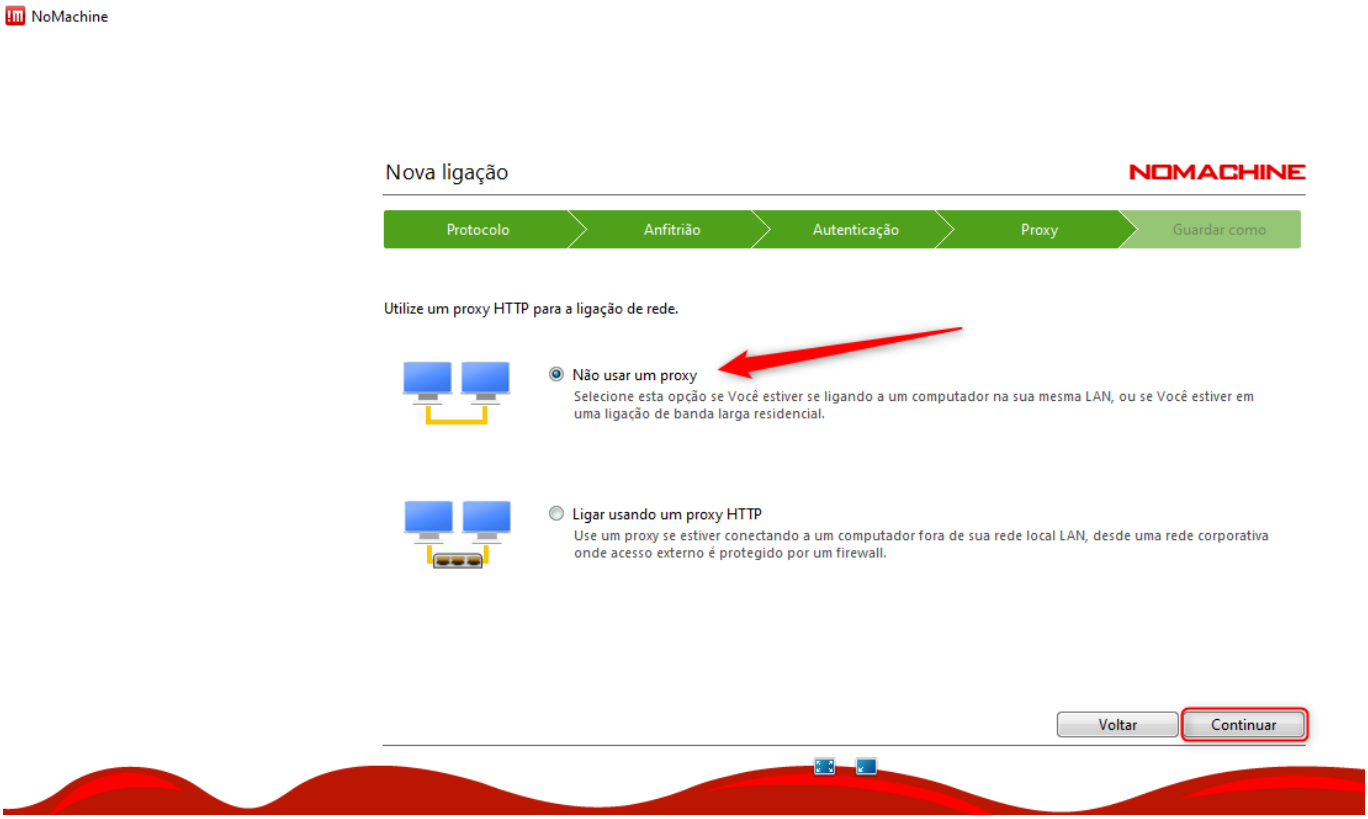

**Configuração na desktop pessoal** - Abra o aplicativo realize as seguintes configurações conforme imagem abaixo:

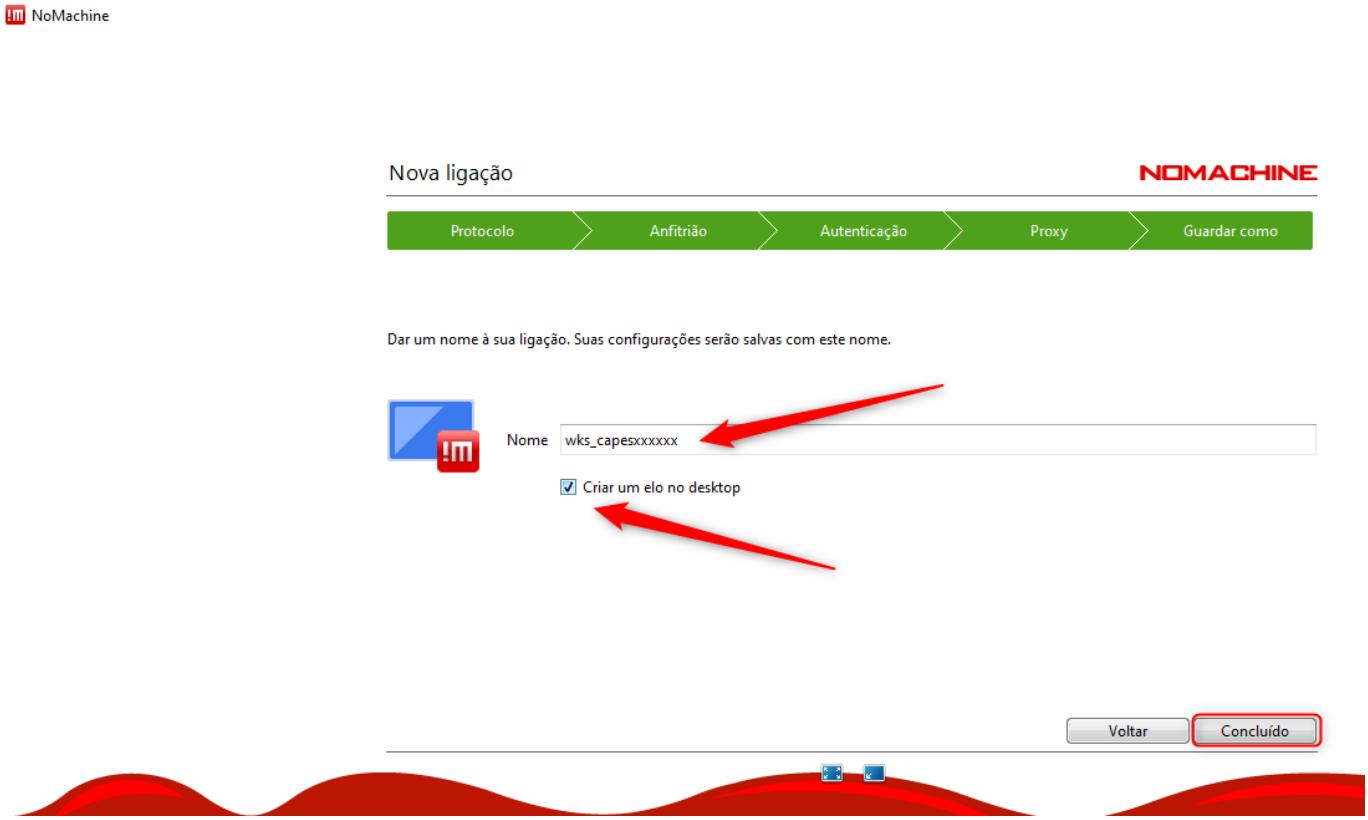

NoMachine
Ligações recentes
NOMACHINE
Vista
Ordenar
Encontrar
Novo
Abrir
Editar
Definições
Ligar

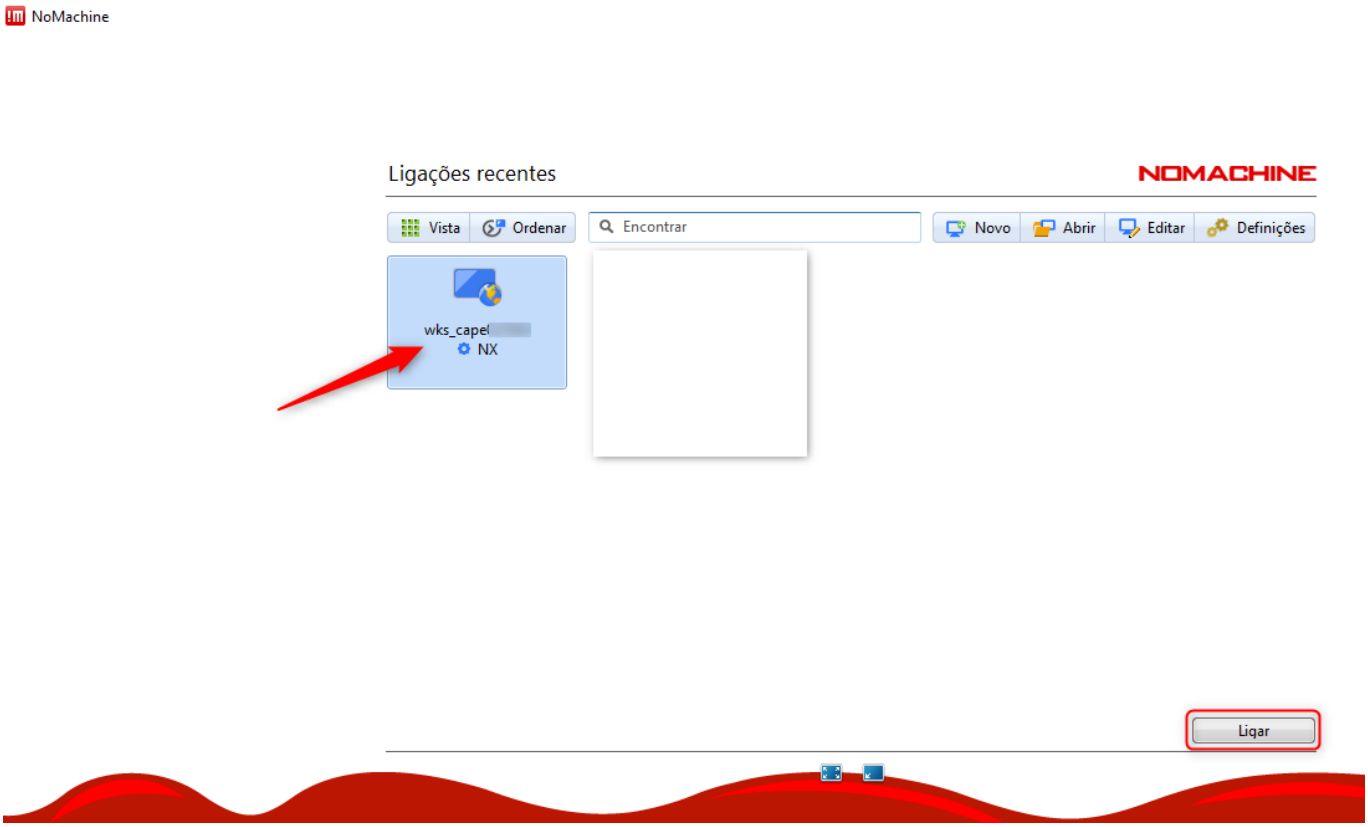

NoMachine
Nova ligação
NOMACHINE
Protocolo
Anfitrião
Autenticação
Proxy
Guardar como
Selecione o protocolo que desee utilizar para se ligar ao computador remoto.
Protocolo
NX
Todos os protocolos usam criptografia para proteger a sua comunicação. NX é o protocolo nativo usado pelo NoMachine e é otimizado para dados multimídia. SSH é uma indústria padrão para acessar os recursos de computação de redes externas.
Voltar
Continuar


NoMachine
Nova ligação
NOMACHINE
Protocolo
Anfitrião
Autenticação
Proxy
Guardar como
Inserir o nome do host ou o IP e a porta à qual se quer ligar.
Anfitrião
172.19.x.x
Porta
4000
A porta foi escolhida automaticamente com base no predefinição para o protocolo. Se o computador remoto foi configurado para ouvir em uma porta diferente, por favor, insira-o acima.
Utilize a comunicação UDP para os dados multimédia
Voltar
Continuar

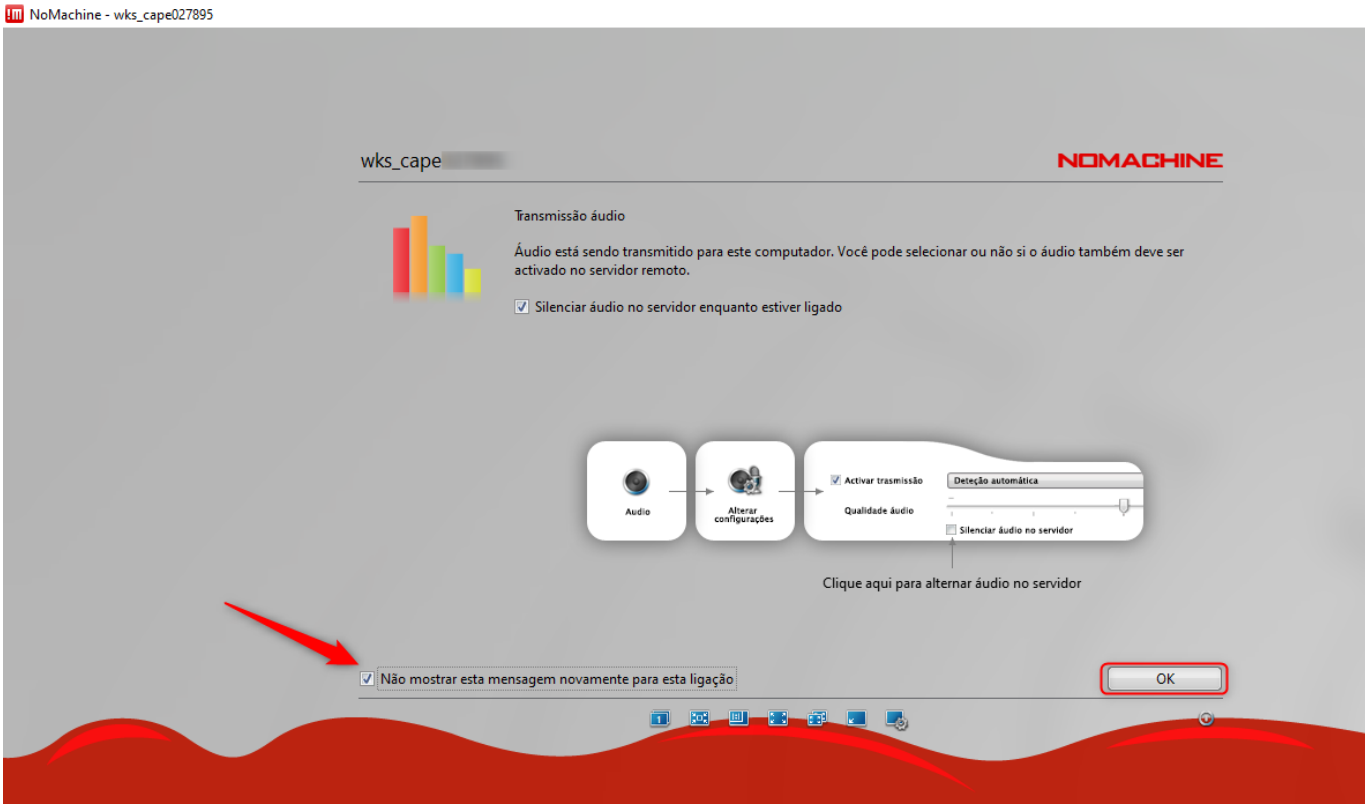

NoMachine
Nova ligação
NOMACHINE
Protocolo
Anfitrião
Autenticação
Proxy
Guardar como
Escolha o método de autenticação que pretende utilizar.
Palavra-Passe
Use a autenticação da palavra-passe.
Chave privada
Use a autenticação baseada em chave que Você fornecer.
Kerberos
Use a autenticação Kerberos baseada em tickets.
Voltar
Continuar

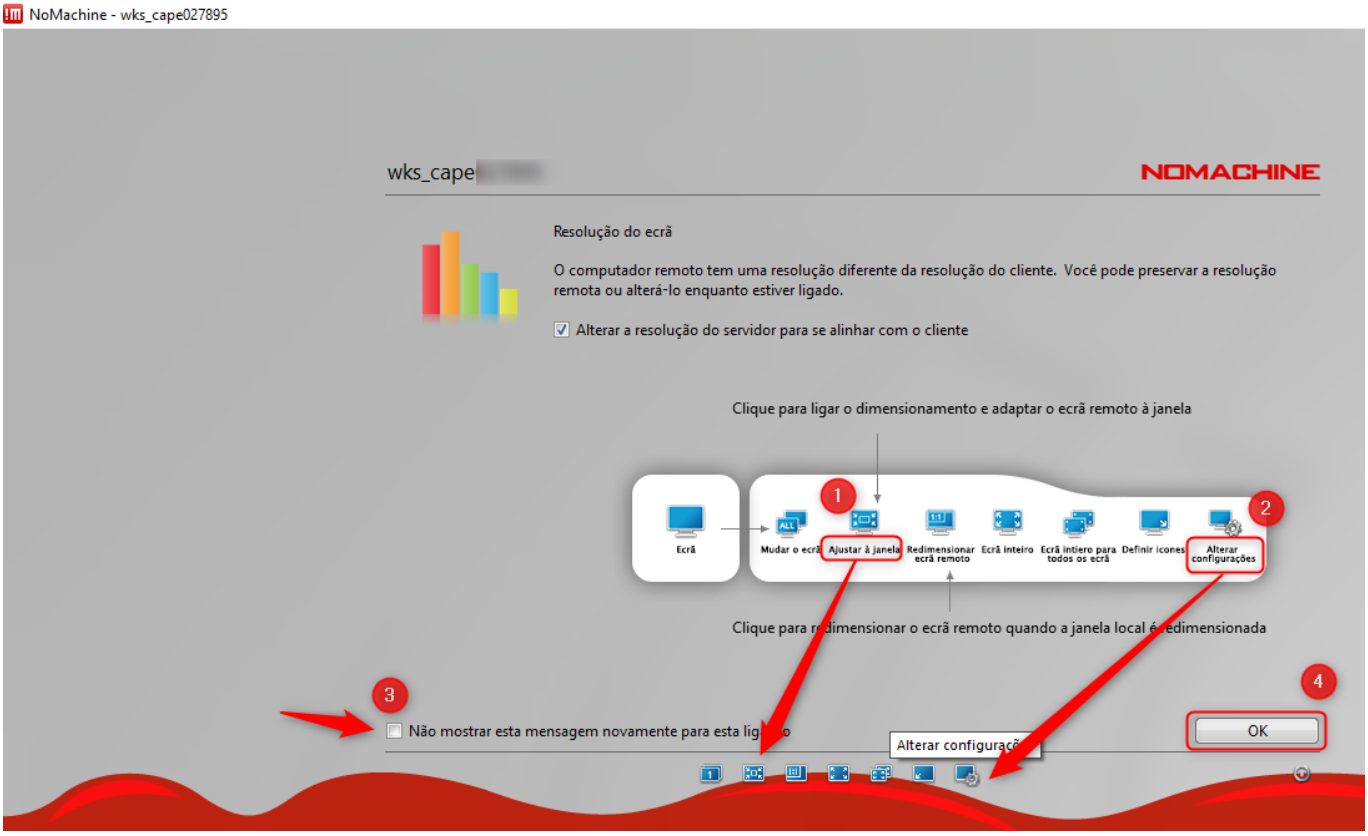

NoMachine
Nova ligação
NOMACHINE
Protocolo
Anfitrião
Autenticação
Proxy
Guardar como
Utilize um proxy HTTP para a ligação de rede.
Não usar um proxy
Selecione esta opção se Você estiver se ligando a um computador na sua mesma LAN, ou se Você estiver em uma ligação de banda larga residencial.
Ligar usando um proxy HTTP
Use um proxy se estiver conectando a um computador fora de sua rede local LAN, desde uma rede corporativa onde acesso externo é protegido por um firewall.
Voltar
Continuar


NoMachine
Nova ligação
NOMACHINE
Protocolo
Anfitrião
Autenticação
Proxy
Guardar como
Dar um nome à sua ligação. Suas configurações serão salvas com este nome.
Nome
wks_capesxxxxxx
Criar um elo no desktop
Voltar
Concluído


NoMachine
Ligações recentes
NOMACHINE
Vista
Ordenar
Encontrar
Novo
Abrir
Editar
Definições
wks_cape
NX
Ligar


NoMachine - wks_cape
wks_cape
NOMACHINE
Digite o nome de utilizador e a palavra-passe para entrar.
Nome do Utilizador
usuario do seu desktop linux
Palavra-Passe
Guarde esta palavra-passe no ficheiro de ligação
Voltar
OK


NoMachine - wks_cape027895
wks_cape
NOMACHINE
Transmissão áudio
Áudio está sendo transmitido para este computador. Você pode selecionar ou não si o áudio também deve ser activado no servidor remoto.
Silenciar áudio no servidor enquanto estiver ligado
Audio
Alterar configurações
Activar trasmissão
Detecção automática
Qualidade áudio
Silenciar áudio no servidor
Clique aqui para alternar áudio no servidor
Não mostrar esta mensagem novamente para esta ligação
OK


NoMachine - wks_cape027895
wks_cape
NOMACHINE
Resolução do ecrã
O computador remoto tem uma resolução diferente da resolução do cliente. Você pode preservar a resolução remota ou alterá-lo enquanto estiver ligado.
Alterar a resolução do servidor para se alinhar com o cliente
Clique para ligar o dimensionamento e adaptar o ecrã remoto à janela
Ecrã
Mudar o ecrã
Ajustar à janela
Redimensionar ecrã remoto
Ecrã inteiro
Ecrã intiero para todos os ecrã
Definir ícones
Alterar configurações
1
2
3
4
OK

# 4 - MacOSX

Para este sistema operacional, há duas formas

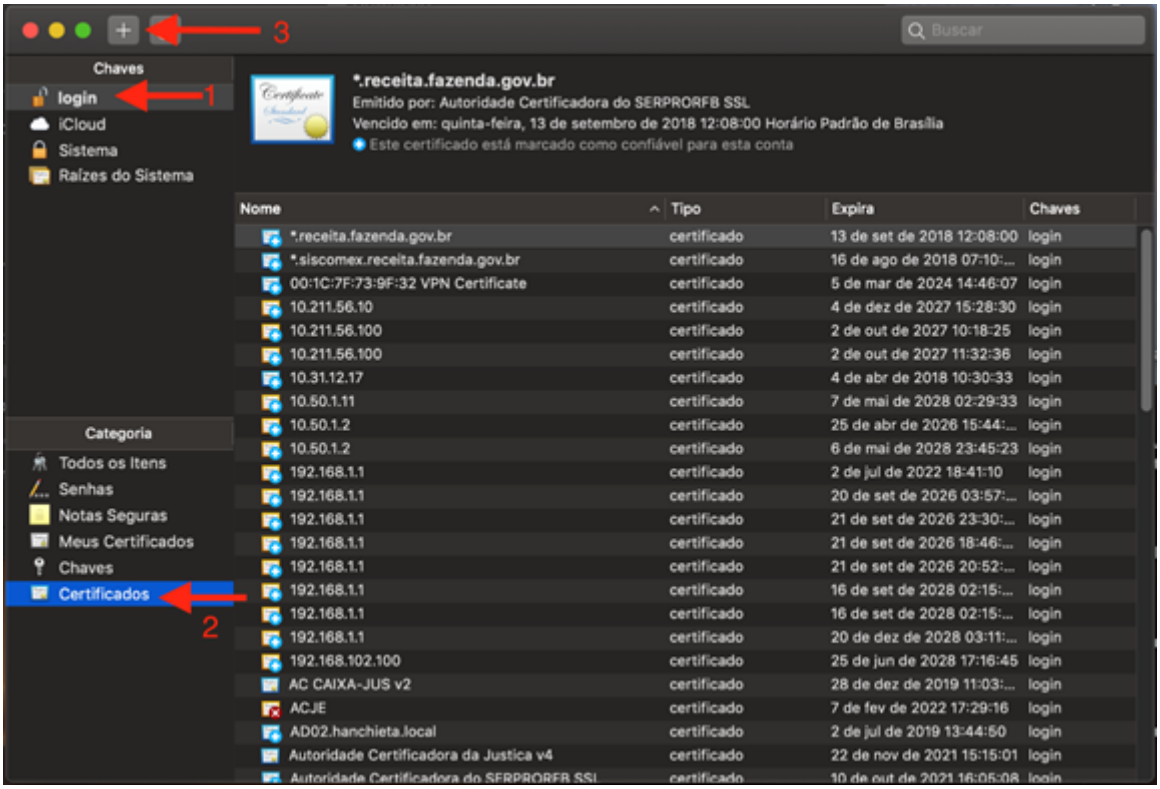
## 4.1 - Utilizando software Cliente (**Opção 1 - RECOMENDADO**)

Para os sistemas operacionais MacOSX há um pacote para instalação do **Endpoint Security VPN**. Para instalar, siga os passos abaixo.

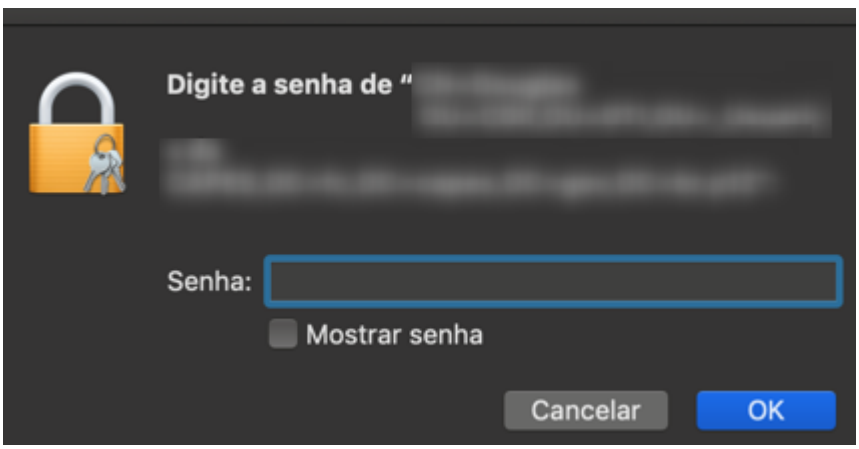
### 4.1.1 - Adicionar Certificado

- Abra o aplicativo **Keychain Access.app** e importe o `seu certificado digital` (enviado por e-mail), salvo na sua pasta de preferência.

> **NOTA:** Lembre-se de **apagar** o certificado de seu e-mail e guardá-lo em local **seguro**.

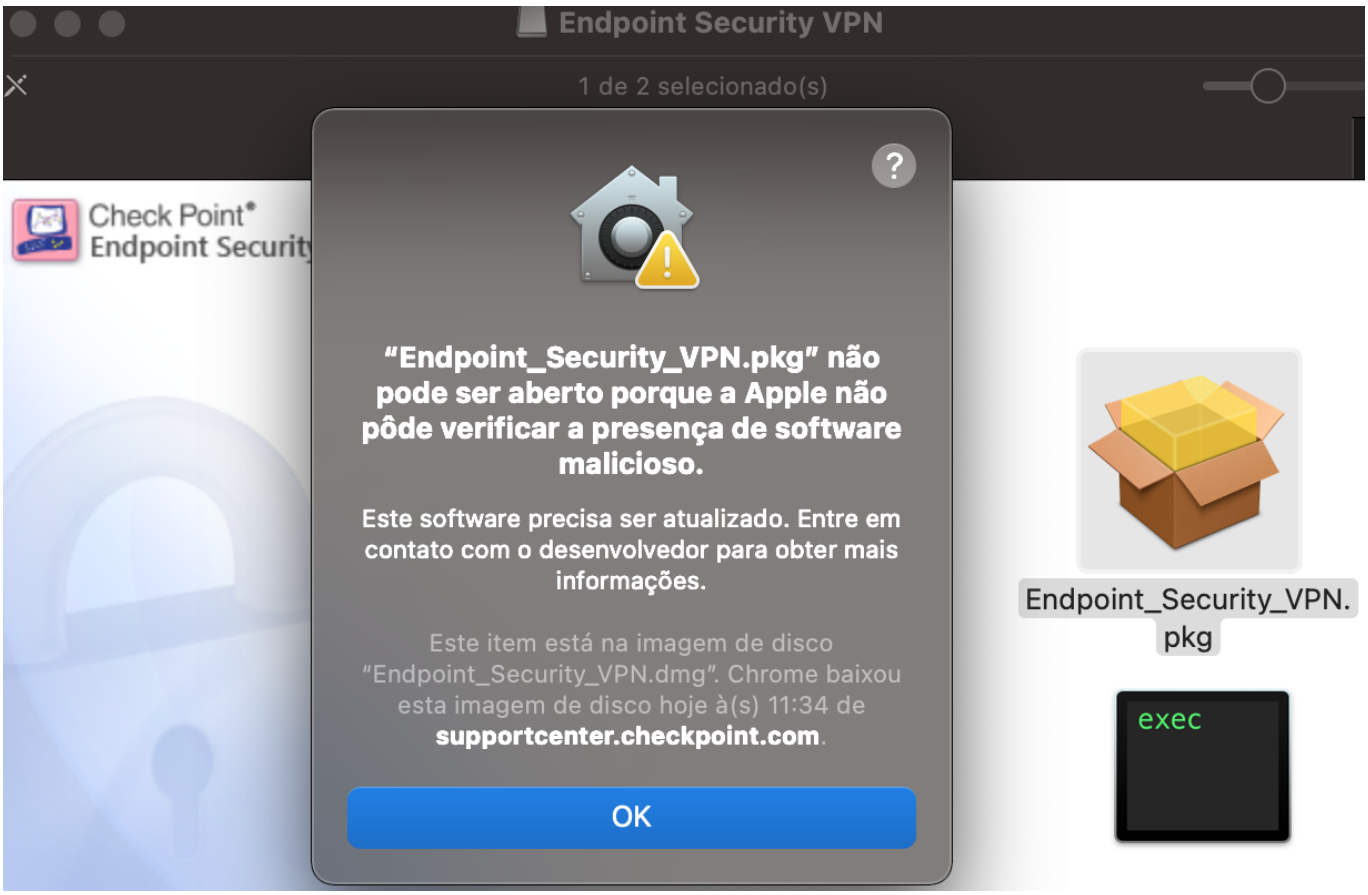



- Ao importar, será necessário digitar a `senha do certificado` e verifique se ela é exibido na listagem de certificados.

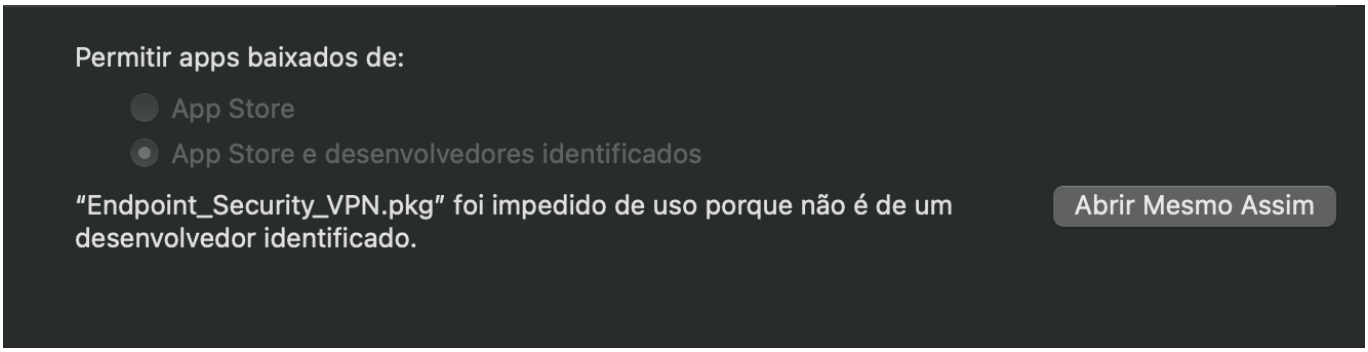


### 4.1.2 - Instalar software

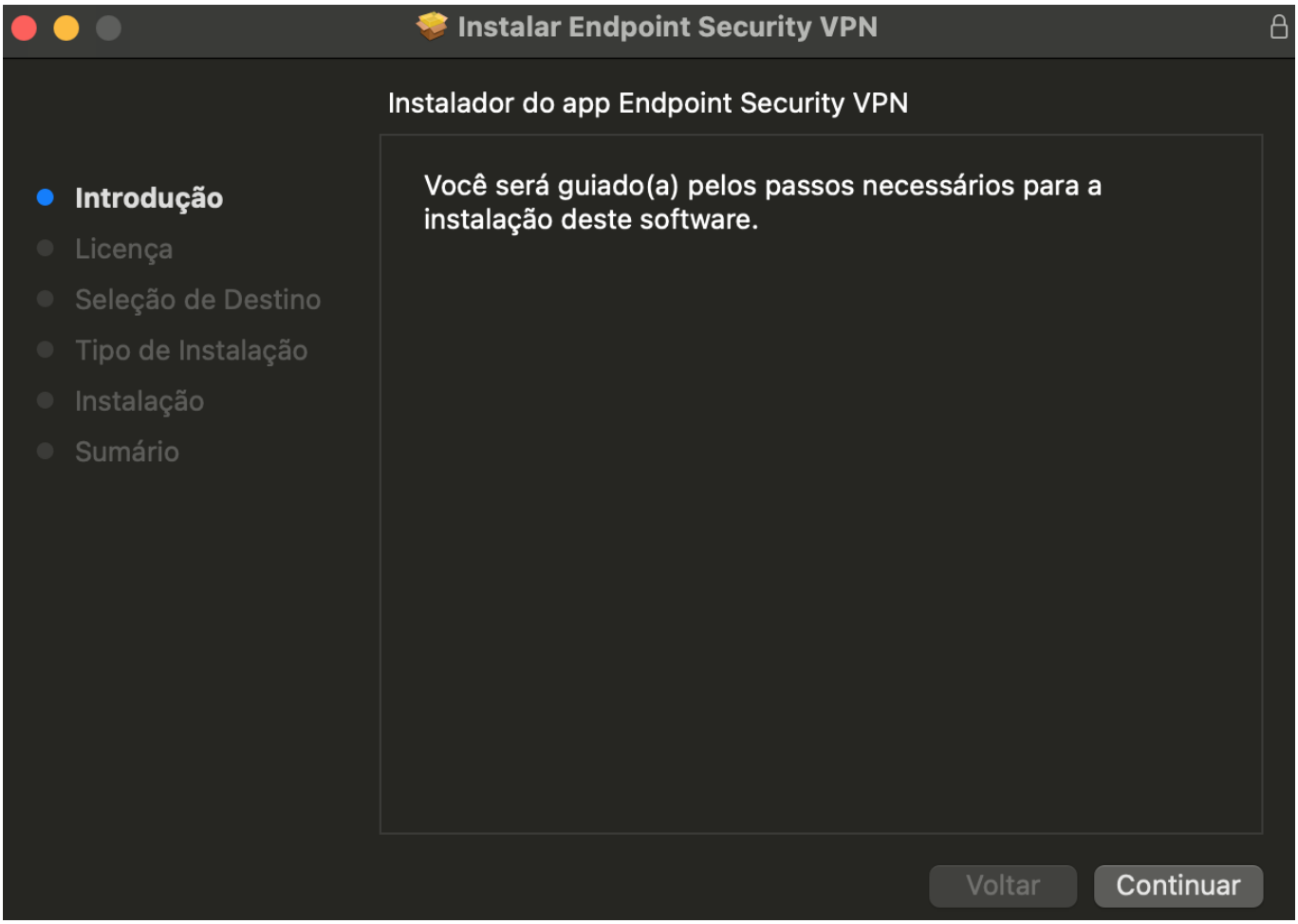
- Faça Download do pacote:
    - **MacOS versão 10.15 até 14** - https://vpn.capes.gov.br/faq/Endpoint_Security_VPN.dmg
- Abra o pacote e execute o instalador **Endpoint_Security_VPN.pkg**
    - Pode ser que uma mensagem de aviso apareça, conforme imagem abaixo.

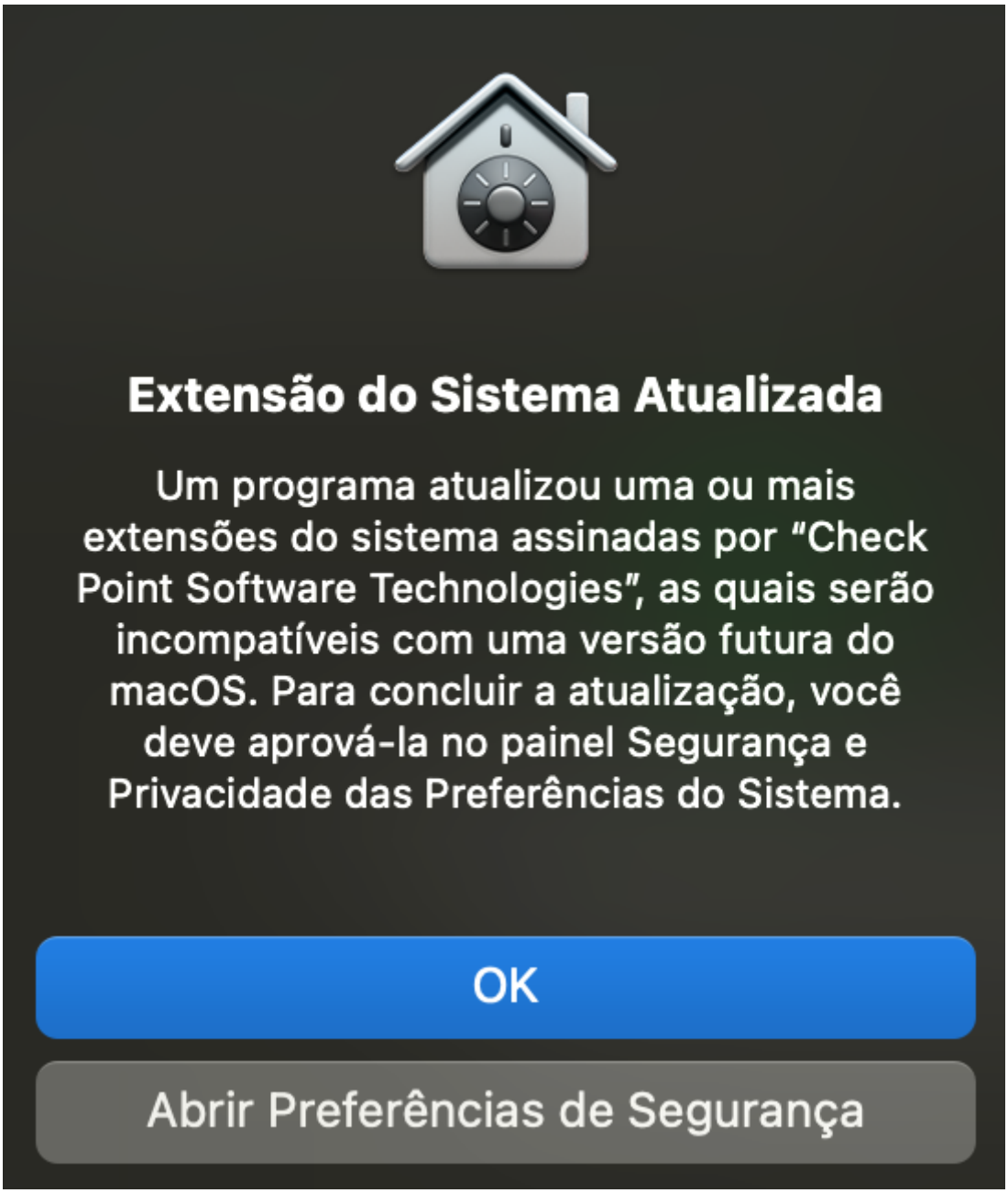



- Para **permitir apps baixados** de outros desenvolvedores. Vá em `Ícone da maça > Preferências do Sistema > Segurança e Privacidade` na aba `Geral` clique em **Abrir mesmo assim**.

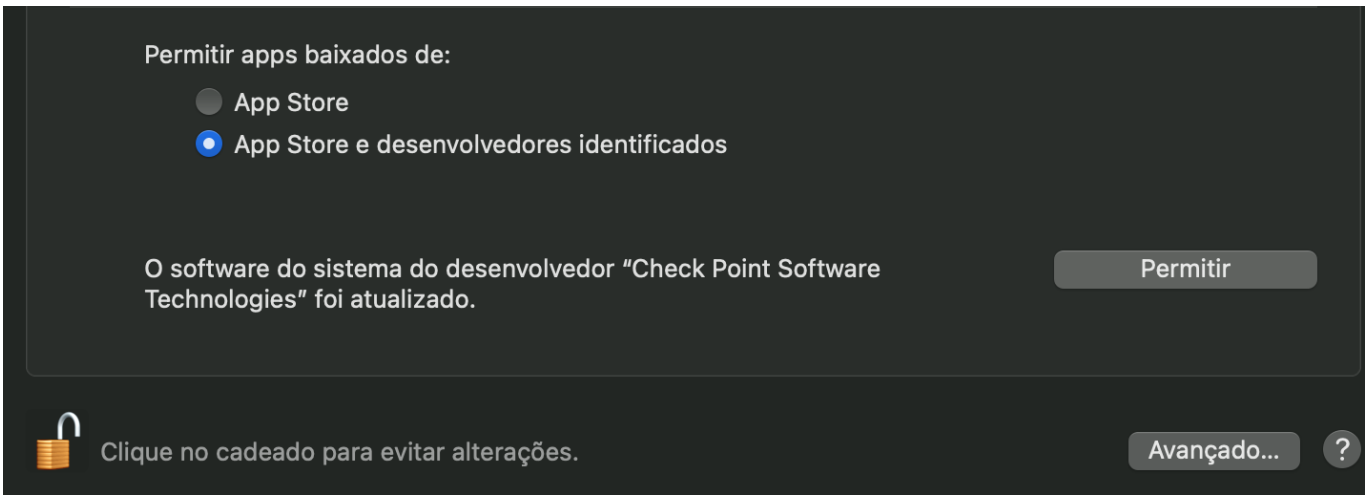



- Agora prossiga com a instalação.


Instalar Endpoint Security VPN
Instalador do app Endpoint Security VPN
Introdução
Licença
Seleção de Destino
Tipo de Instalação
Instalação
Sumário
Você será guiado(a) pelos passos necessários para a instalação deste software.
Voltar
Continuar

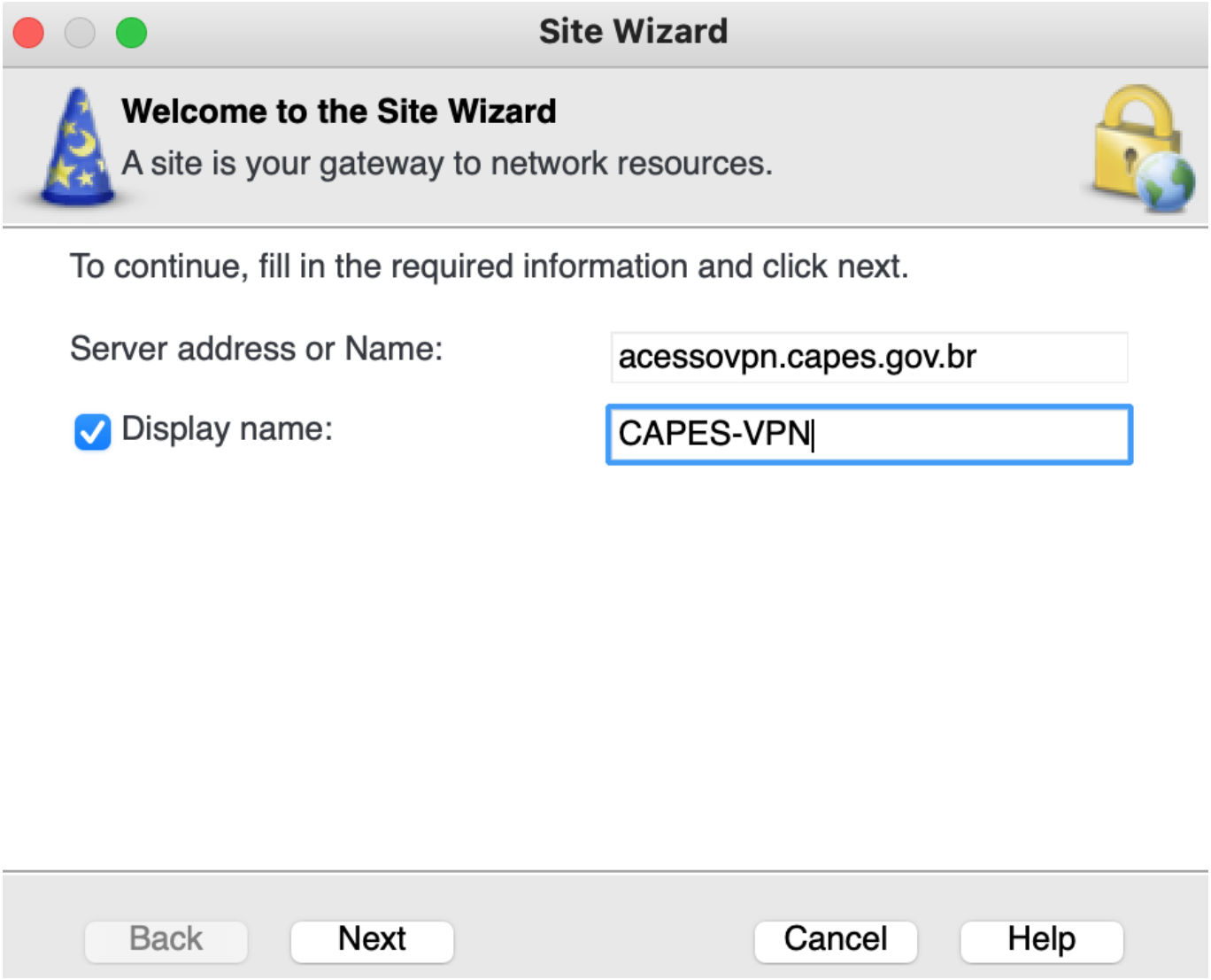


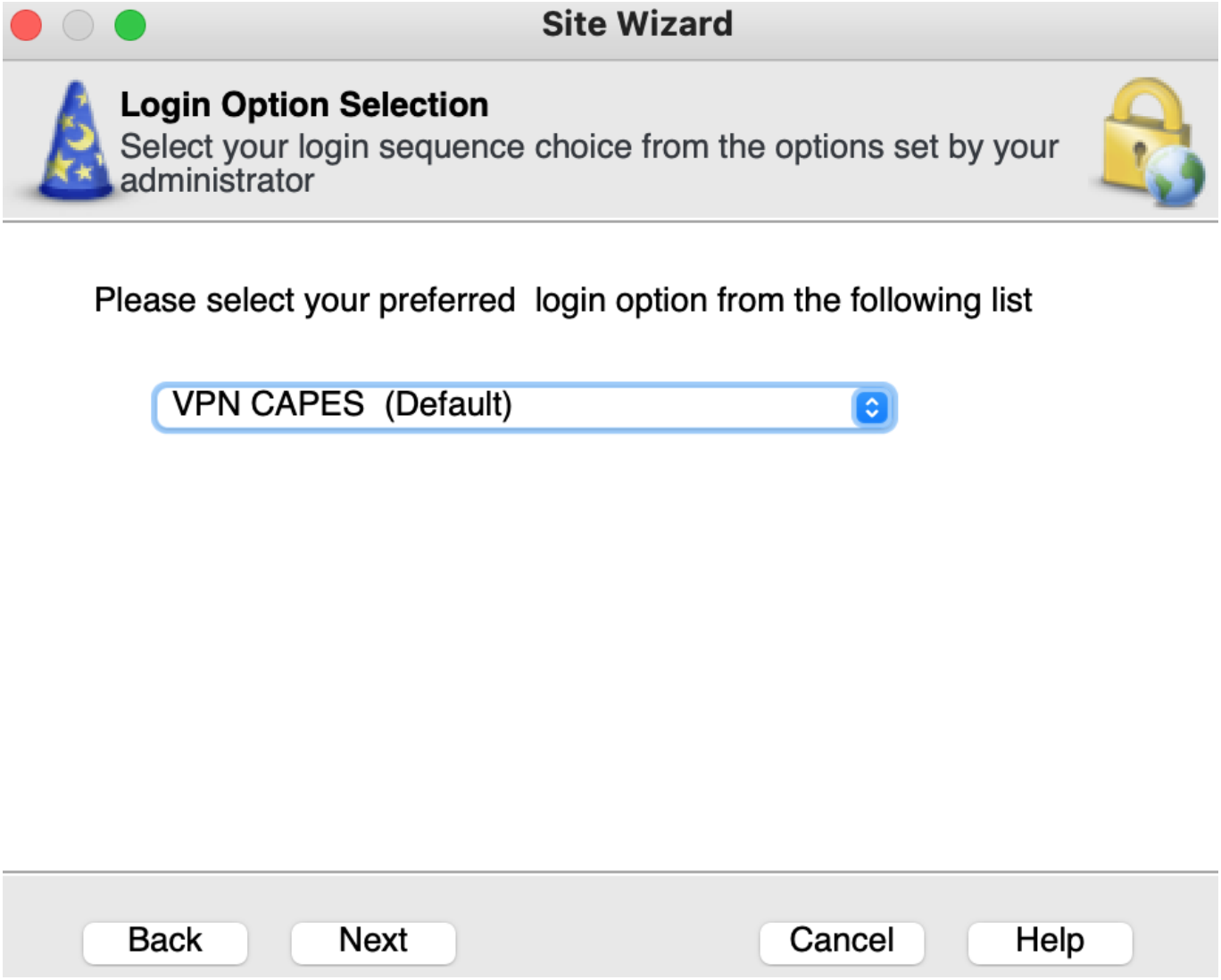

- Caso tenha fechado, volte em `Ícone da maça > Preferências do Sistema > Segurança e Privacidade` na aba `Geral` clique em **Permitir**.

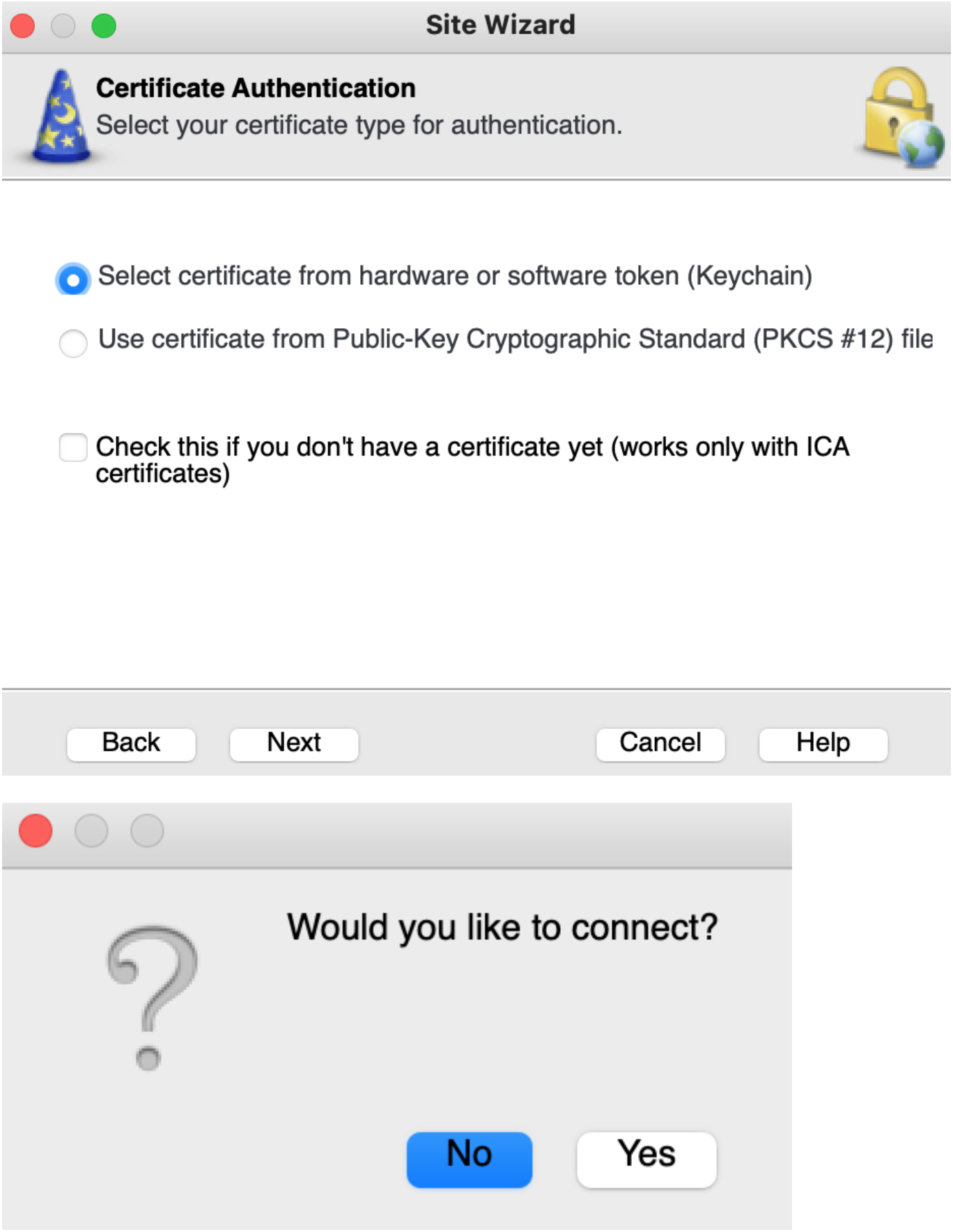


- Será necessário um reboot para ajustes da extensão no sistema. Após isto, o software estará instalado nos seus aplicativos. Execute-o e um ícone do cliente VPN aparecerá no menu superior (perto do relógio).

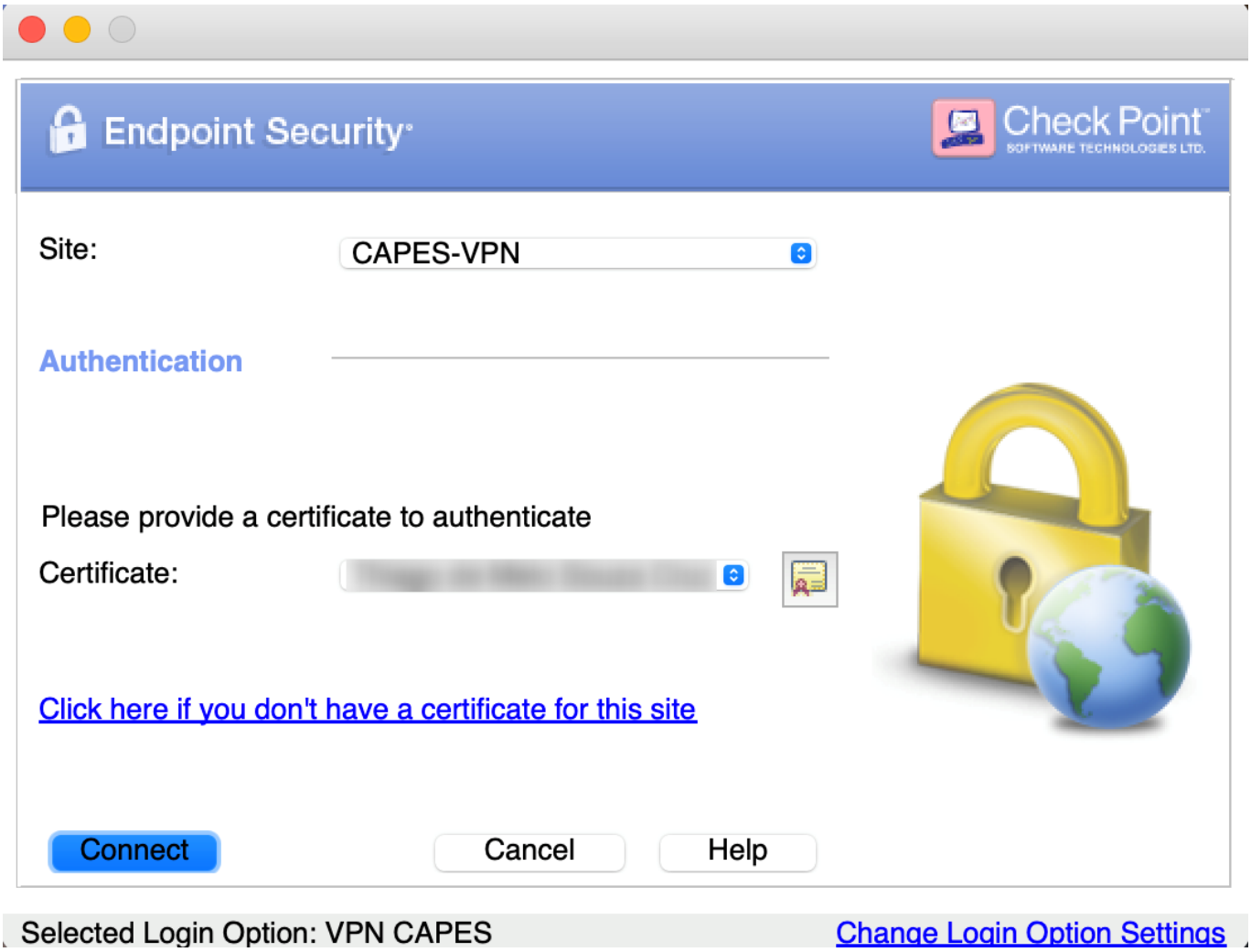

- Faça a configuração para o site da CAPES. Ao clicar em **Connect** será solicitada a criação de uma configuração. coloque o endereço:
  - **Server address or Name**: `acessovpn.capes.gov.br`


Site Wizard
Welcome to the Site Wizard
A site is your gateway to network resources.
To continue, fill in the required information and click next.
Server address or Name:
acessovpn.capes.gov.br
Display name:
CAPES-VPN
Back
Next
Cancel
Help


Site Wizard
Login Option Selection
Select your login sequence choice from the options set by your administrator
Please select your preferred login option from the following list
VPN CAPES (Default)
Back
Next
Cancel
Help



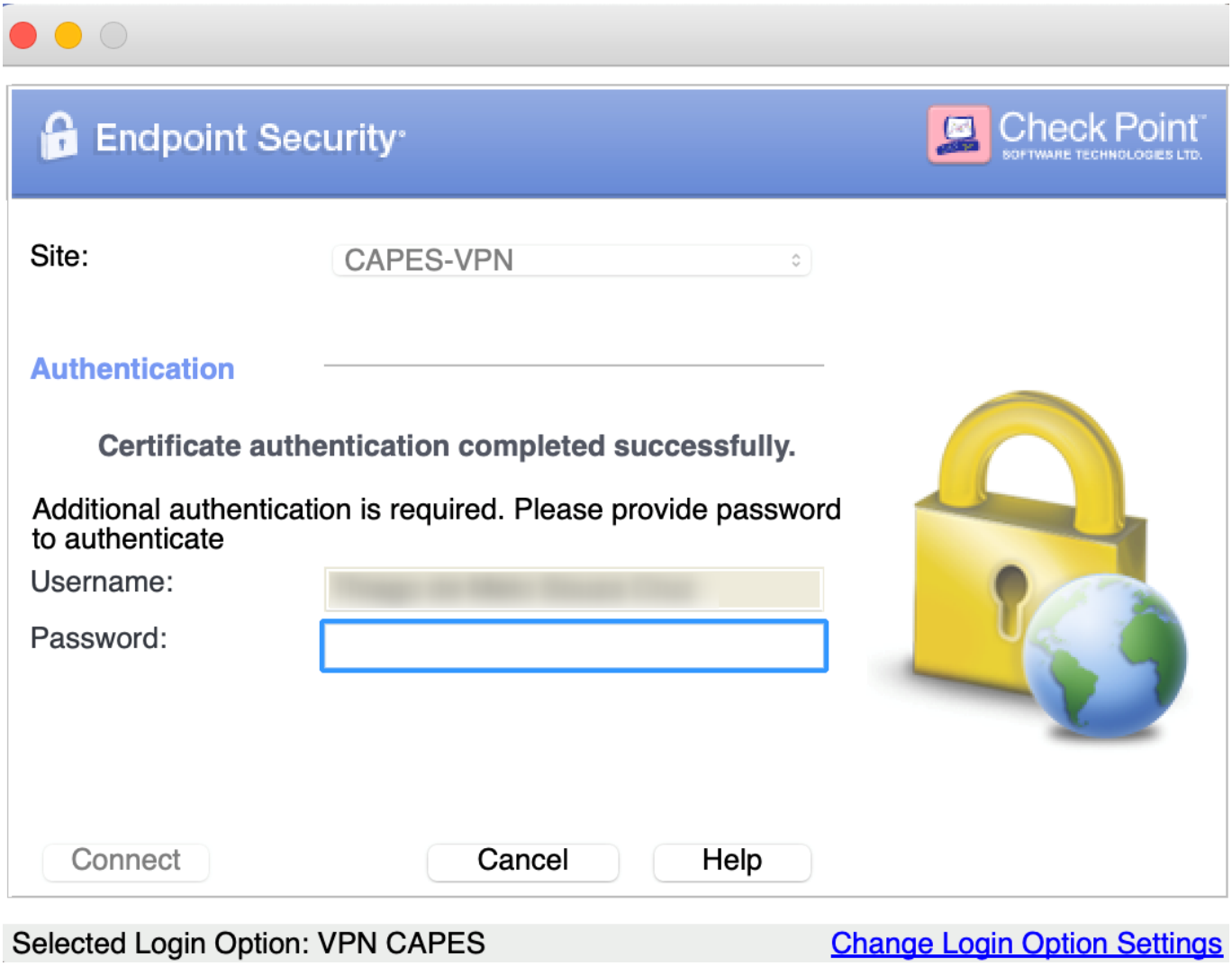

- Certifique-se que o seu certificado está aparecendo e clique em **Connect**. Talvez seja solicitada a senha do seu Mac para acesso ao certificado.



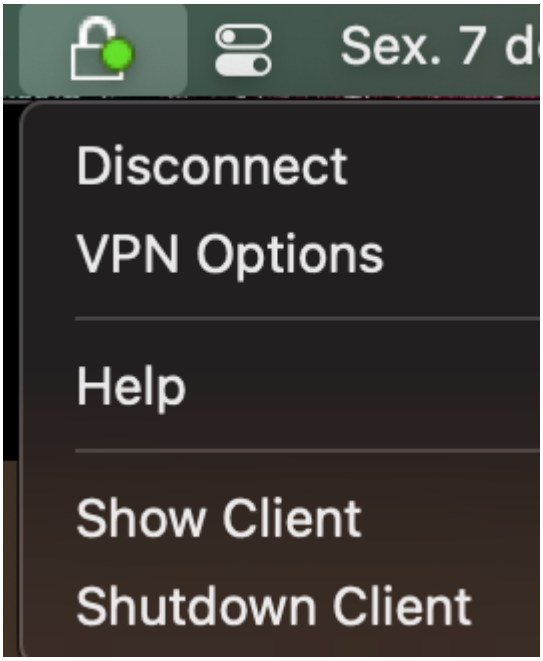


### 4.1.3 - Conectar / Desconectar

- Entre com a sua senha da **Rede CAPES** e pronto, vocês estará conectado.

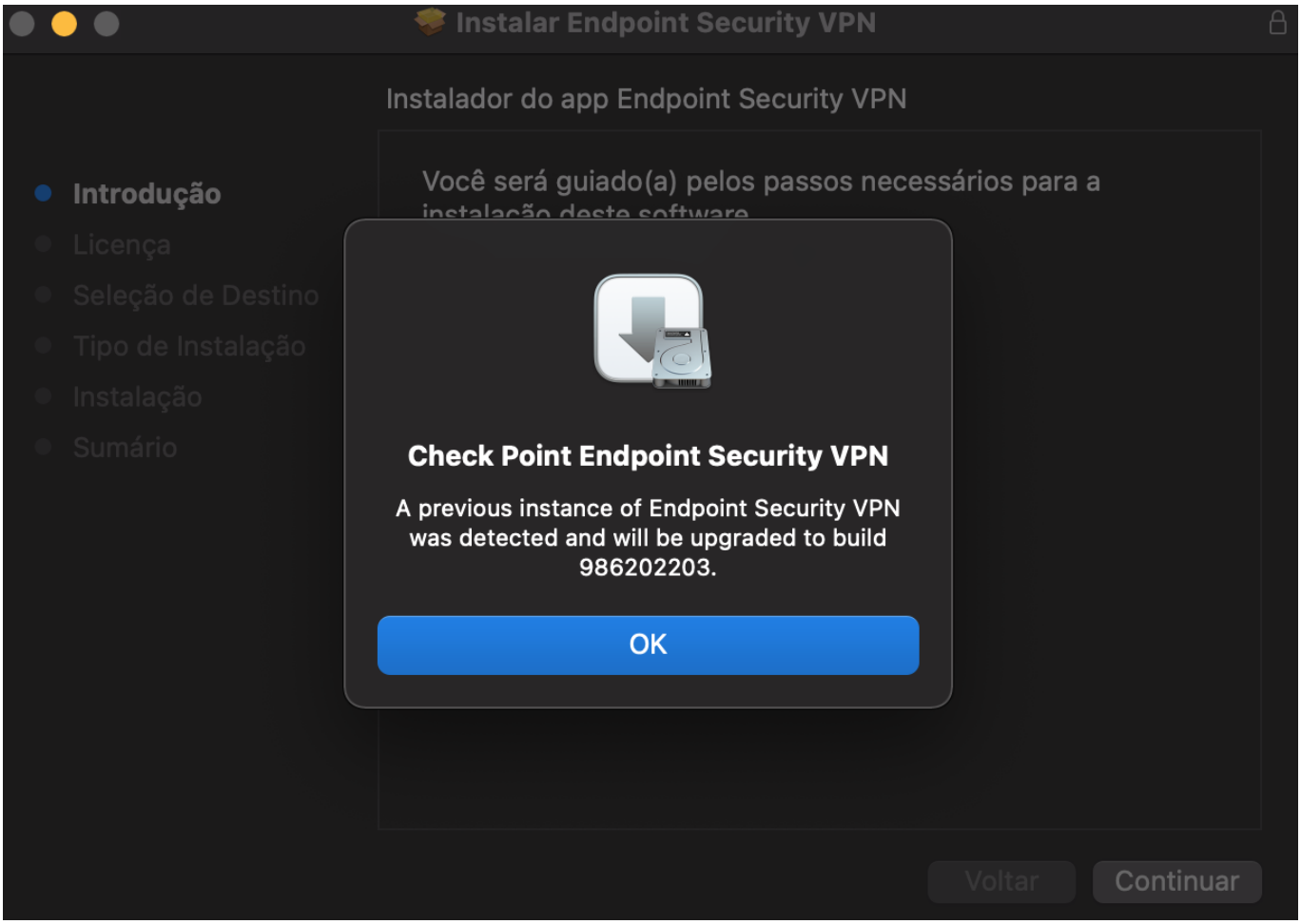



- Para descontar, basta clicar no ícone e em **Disconnect**.

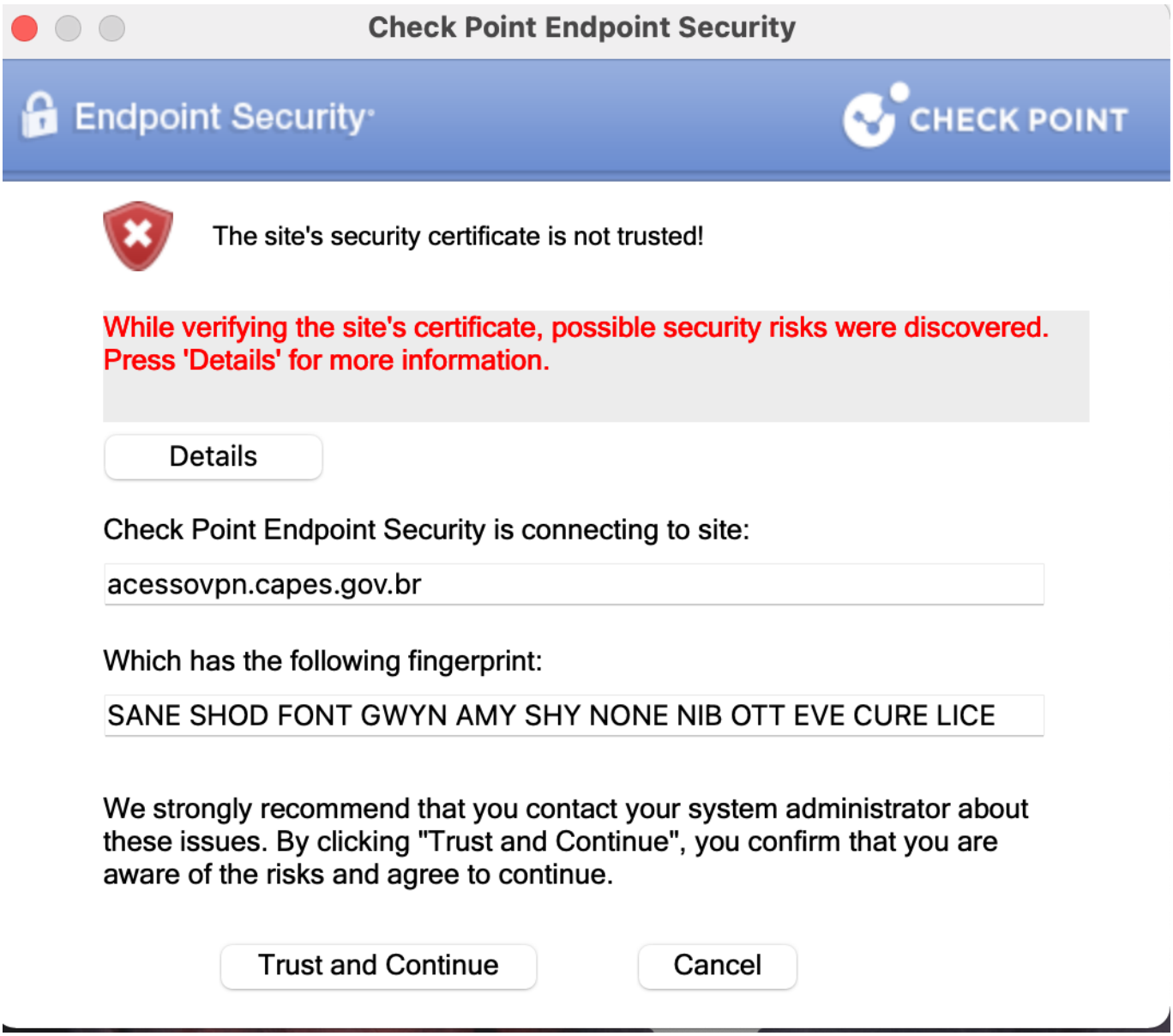



### 4.1.4 - Atualizar software client

Para atualizar o software em uma sistema com MacOS, basta fazer o download do pacote (item 4.1.2) e seguir o processo de instalação. Será informado que o pacote será atualizado, bastando aceitar




Caso apareca a tela abaixo, pode clicar em "Trust and Continue".




## 4.2 - Utilizando navegador (**Opção 2**)

Para os sistemas operacionais MacOSX utilize seu navegador e sigas os passos a seguir:

- Instale o Java pelo site https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html
- Escolha a versão do seu MacOS e faça o Download;

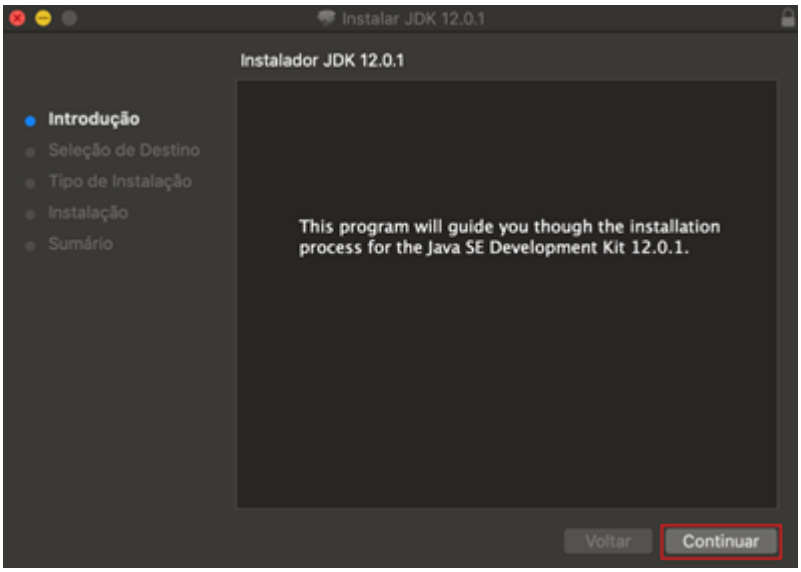
## Java SE Development Kit 8u211

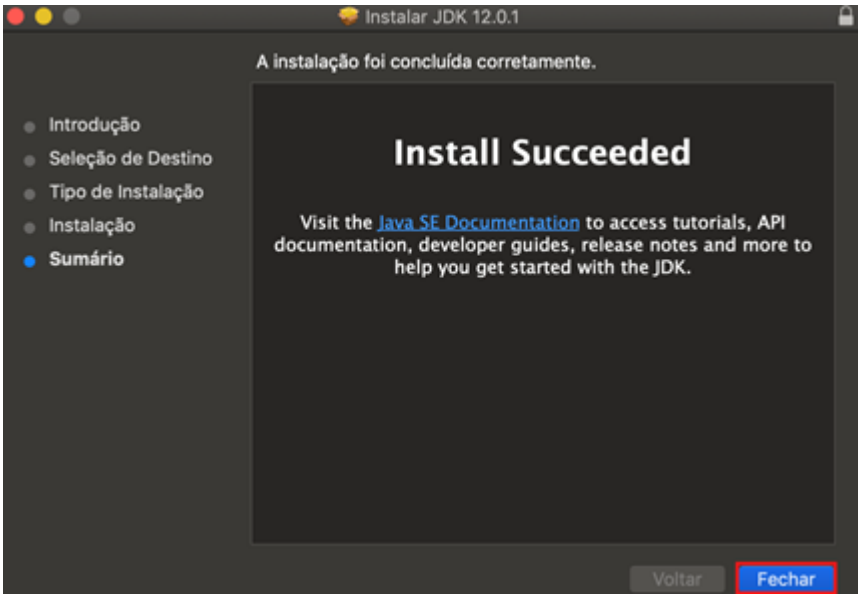
You must accept the Oracle Technology Network License Agreement for Oracle Java SE to download this software.

○ Accept License Agreement ◉ Decline License Agreement

| Product / File Description | File Size | Download |
|---|---|---|
| Linux ARM 32 Hard Float ABI | 72.86 MB | jdk-8u211-linux-arm32-vfp-hflt.tar.gz |
| Linux ARM 64 Hard Float ABI | 69.76 MB | jdk-8u211-linux-arm64-vfp-hflt.tar.gz |
| Linux x86 | 174.11 MB | jdk-8u211-linux-i586.rpm |
| Linux x86 | 188.92 MB | jdk-8u211-linux-i586.tar.gz |
| Linux x64 | 171.13 MB | jdk-8u211-linux-x64.rpm |
| Linux x64 | 185.96 MB | jdk-8u211-linux-x64.tar.gz |
| Mac OS X x64 | 252.23 MB | jdk-8u211-macosx-x64.dmg |
| Solaris SPARC 64-bit (SVR4 package) | 132.98 MB | jdk-8u211-solaris-sparcv9.tar.Z |
| Solaris SPARC 64-bit | 94.18 MB | jdk-8u211-solaris-sparcv9.tar.gz |
| Solaris x64 (SVR4 package) | 133.57 MB | jdk-8u211-solaris-x64.tar.Z |
| Solaris x64 | 91.93 MB | jdk-8u211-solaris-x64.tar.gz |
| Windows x86 | 202.62 MB | jdk-8u211-windows-i586.exe |
| Windows x64 | 215.29 MB | jdk-8u211-windows-x64.exe |

- Execute o arquivo e faça a instalação;
- Na janela de instalação do JDK selecione "**Continuar**" e siga as instruções.



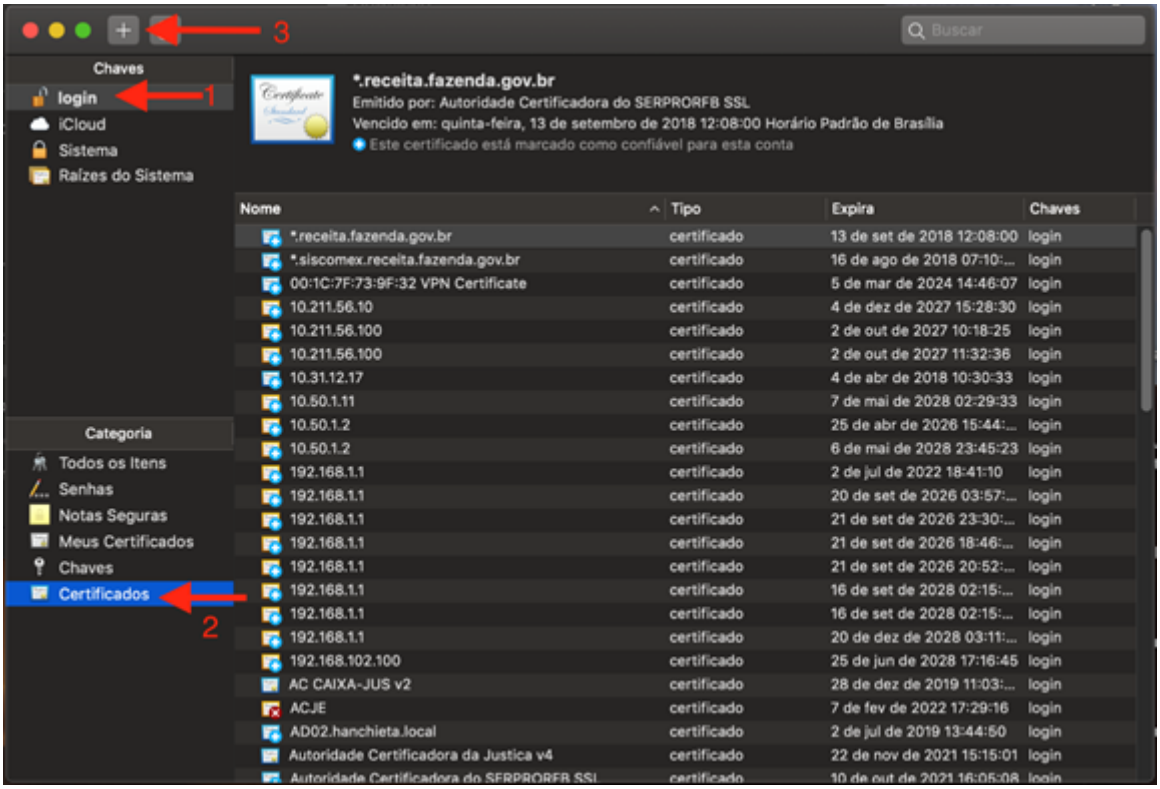



- Caso tenha dúvidas, verifique a versão instalada com os comandos:

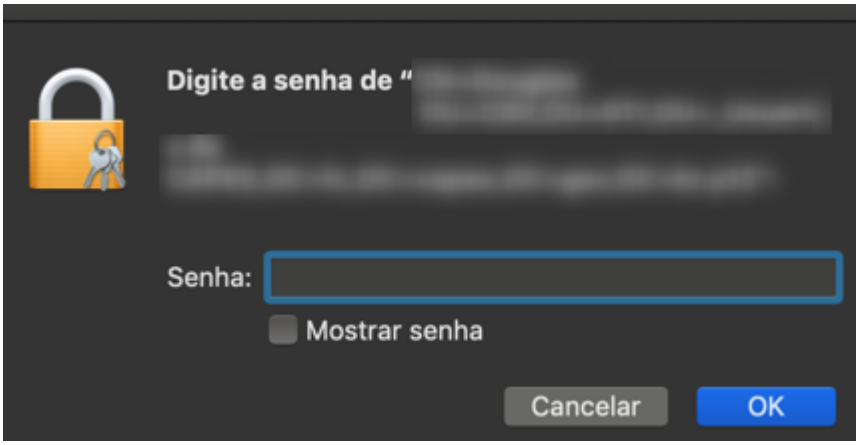
```
java –version
javac –version
```

- Abra o aplicativo **Keychain Access.app** e importe o `seu certificado digital` (enviado por e-mail), salvo na sua pasta de preferência.

> **NOTA:** Lembre-se de **apagar** o certificado de seu e-mail e guardá-lo em local **seguro**.



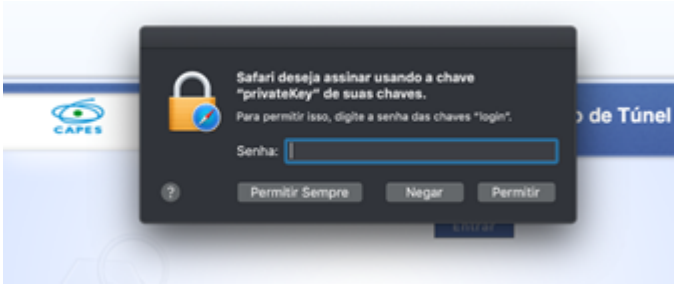

- Ao importar, será necessário digitar a `senha do certificado` e verifique se ela é exibido na listagem de certificados.




### 4.2.1 - Conectar

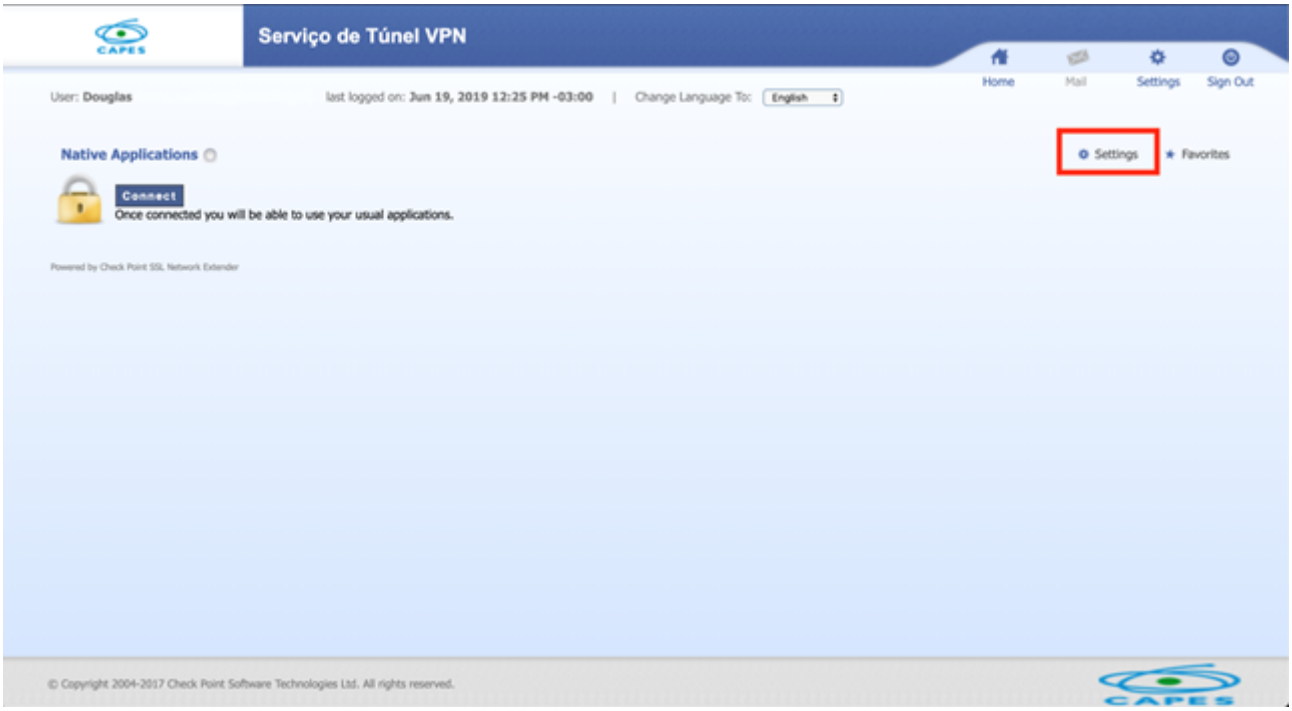
Observa-se que alguns passos abaixo serão necessários somente uma primeira vez.

- Acesse https://acessovpn.capes.gov.br e clique em "**Entrar**".
- Será solicitado o seu certificado, previamente importado.
- A senha do seu usuário do MacOSX será solicitada.

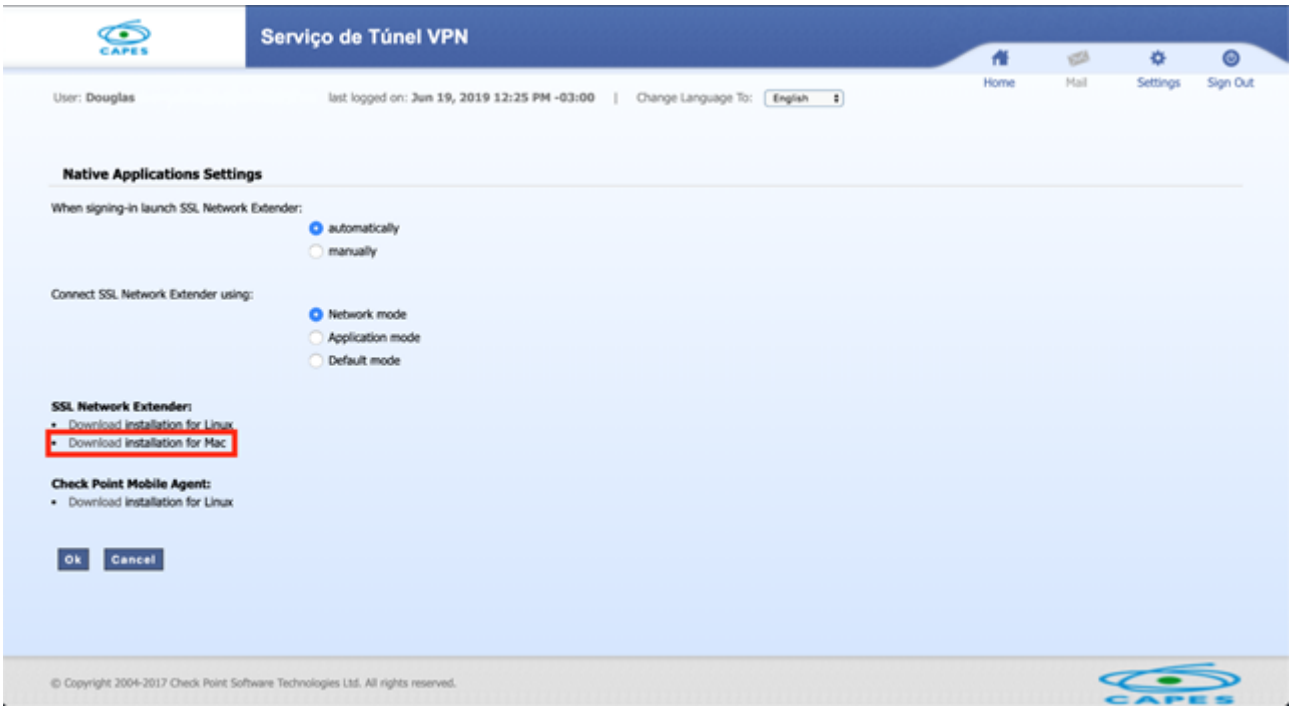



- Em seguida autentique utilizando `sua senha da Rede CAPES (login)`


- Antes de se conectar será necessário fazer download e a instalar o arquivo SNX no MacOS. Vá em "**Settings (Configurações)**".



- Selecione "**Download installation for Mac**".



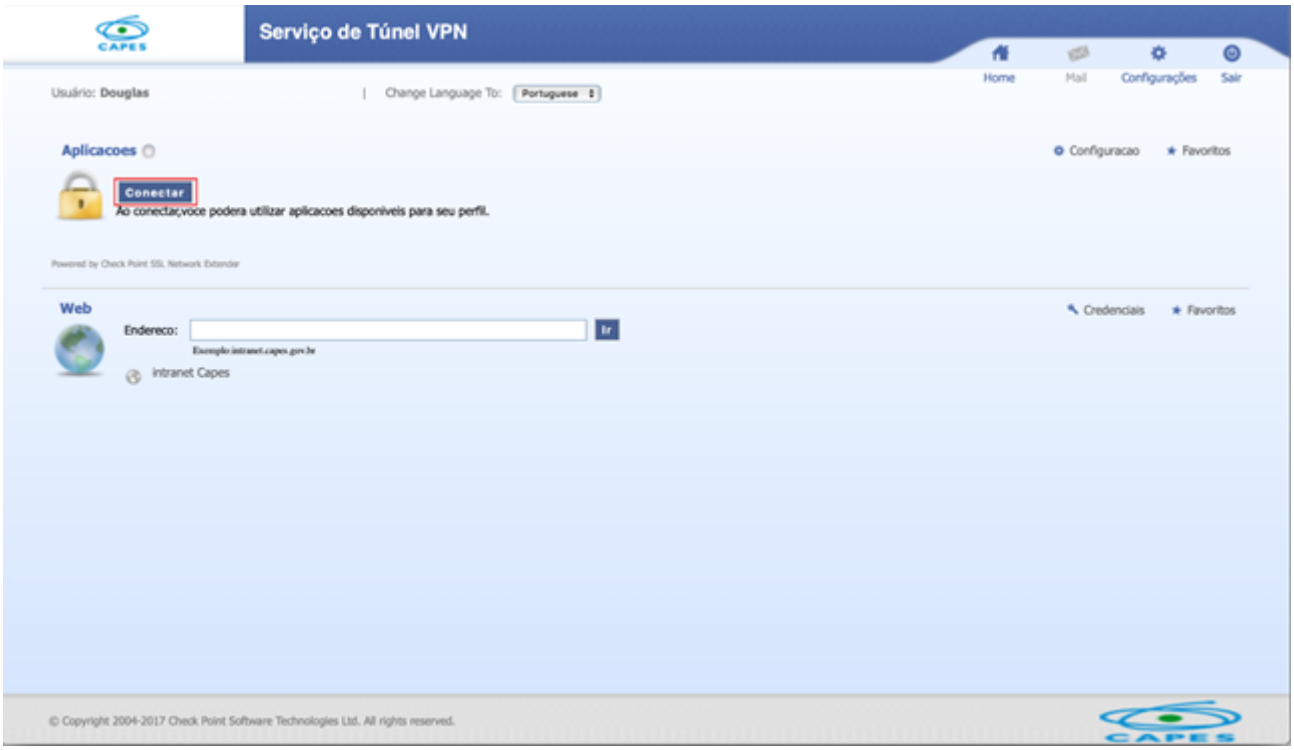

- Abra o terminal para instalar o SNX e entre com o comando:

```
sudo ./snx_install_osx.sh
```

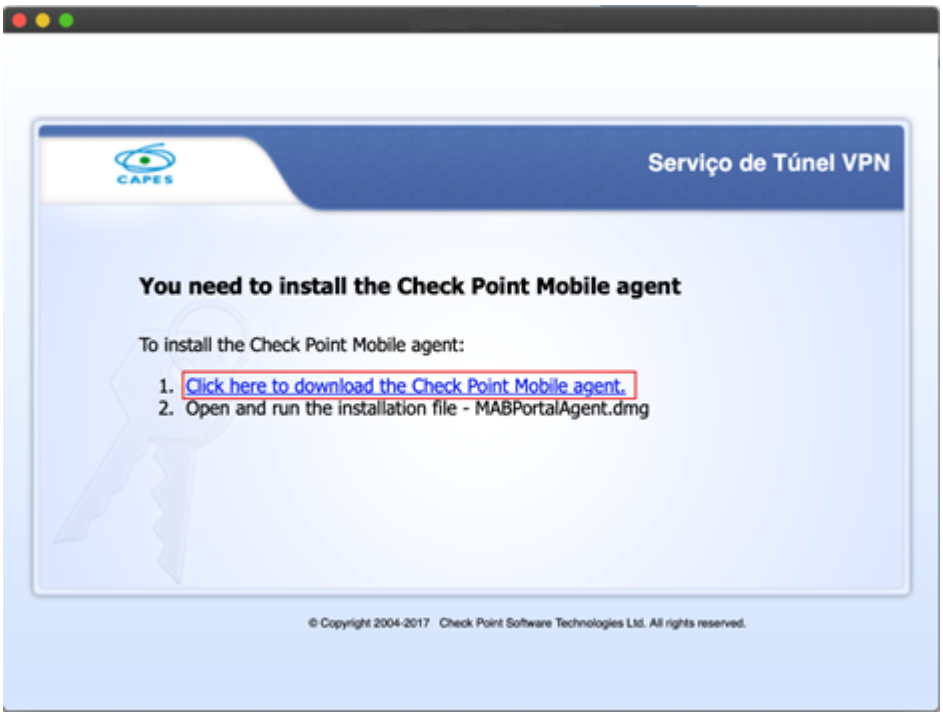
- Caso seja necessário, coloque permissão de escrita no executável do SNX, via terminal:

```
sudo chmod a+x /usr/local/bin/snx
```

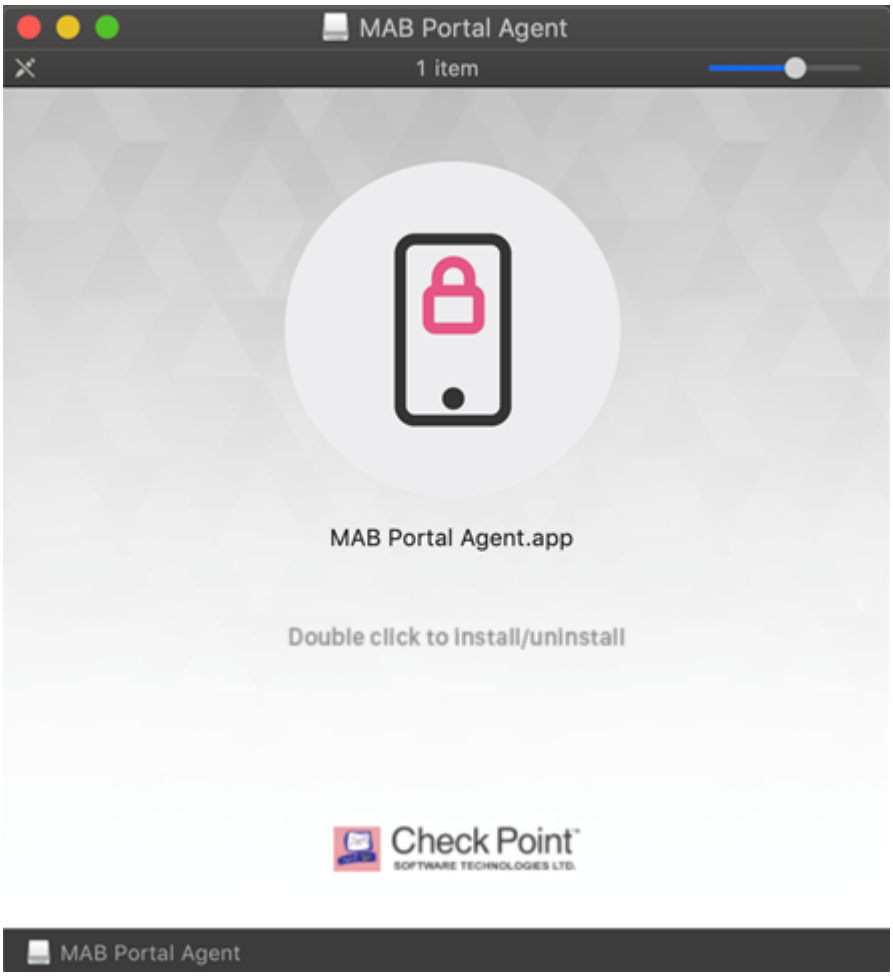
- Em seguida volte a página inicial e selecione o botão "**Conectar**".




- Será necessário a instalação do **Check Point Mobile agent**. Faça download selecionando "**Click here to download the Check Point Mobile agent**".

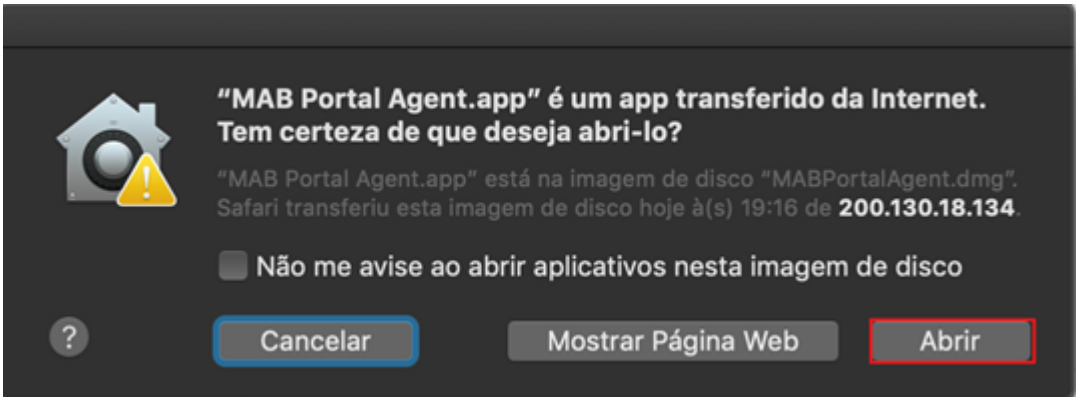



- Salve o arquivo e execute-o.

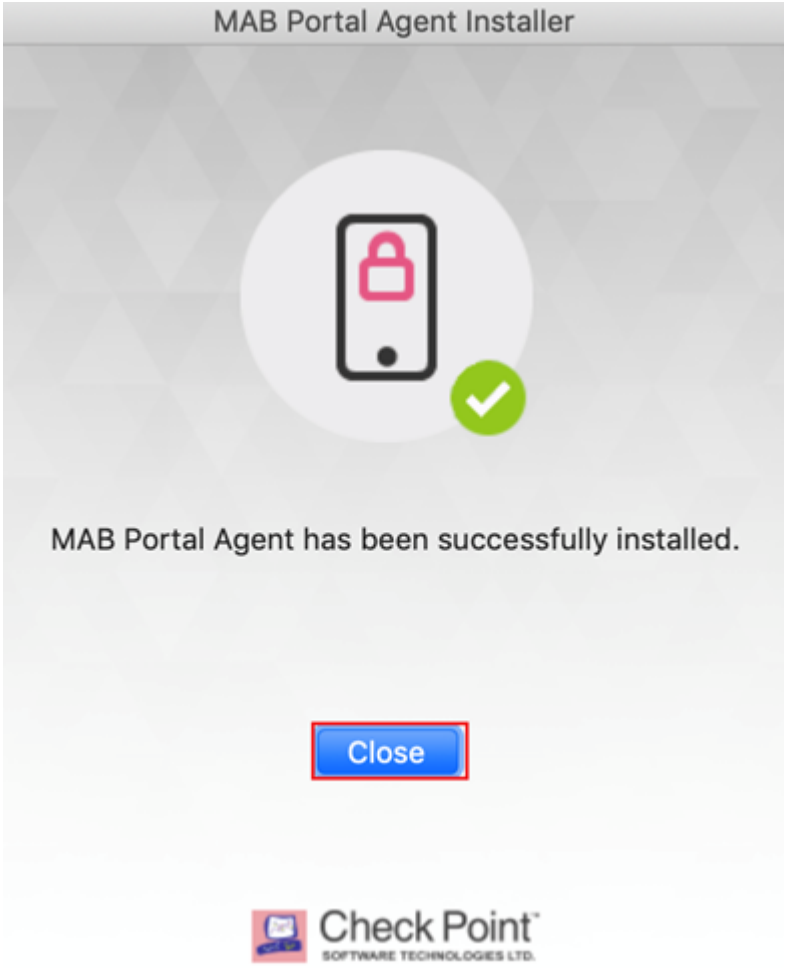




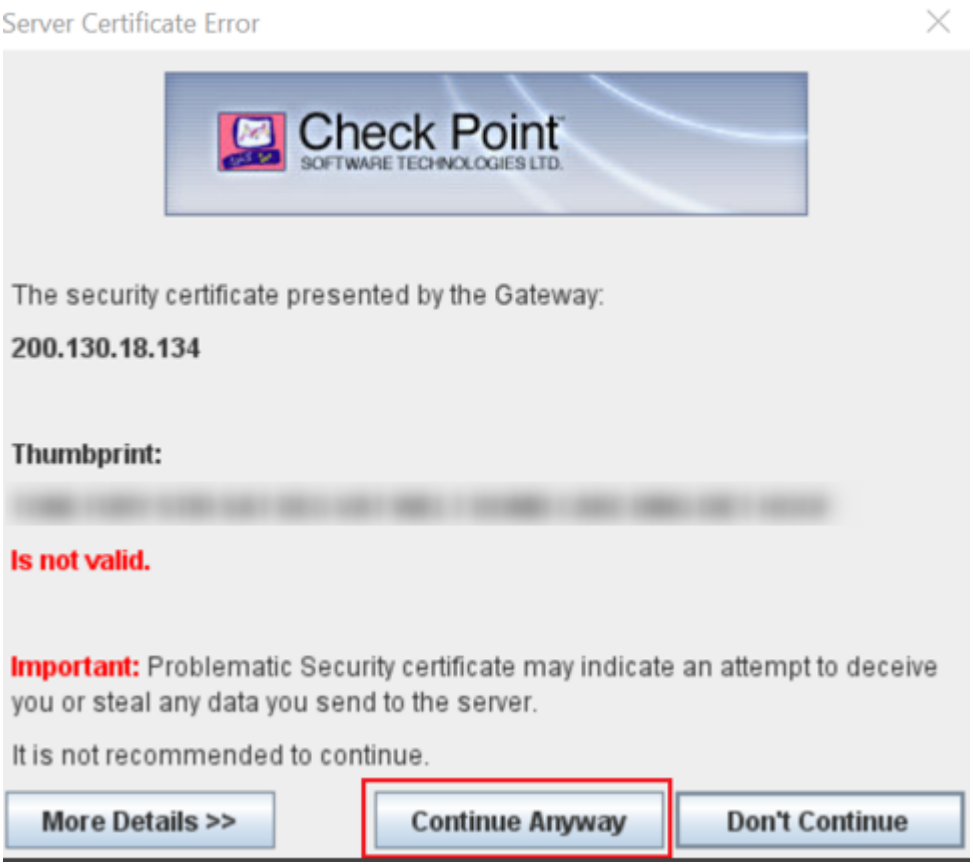


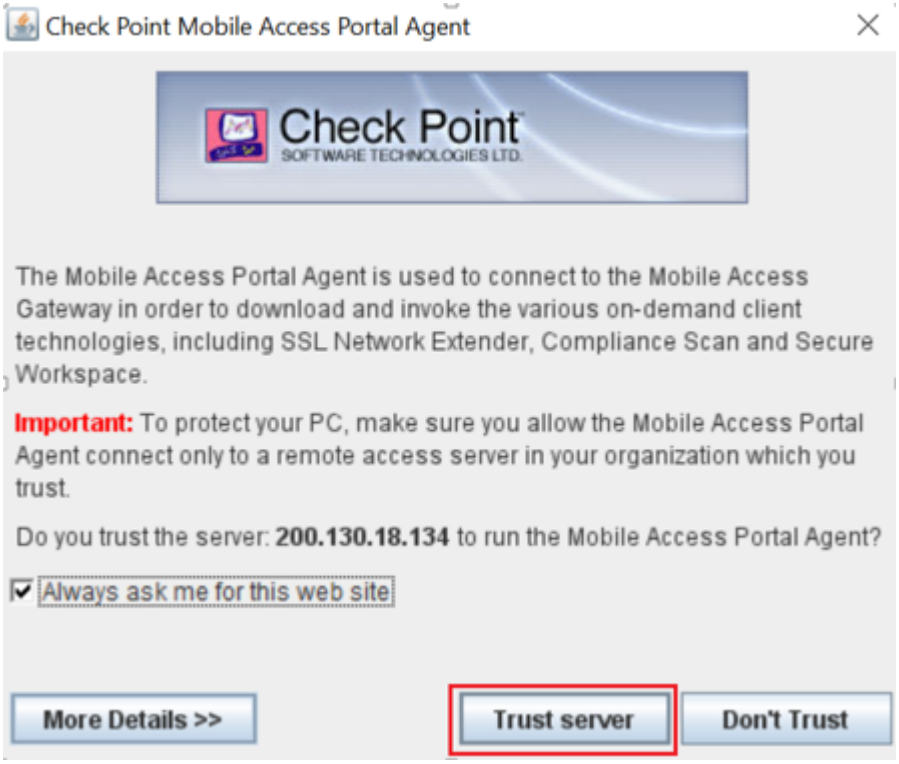



- Entre com sua senha do MacOS para continuar com a instalação e após a instalação selecione "**Close**".




- Selecione Conectar novamente e irá surgir a janela de **Server Certificate Error**, selecione "**Continue Anyway**" e em seguida selecione "**Trust Server**" e irá se conectar.

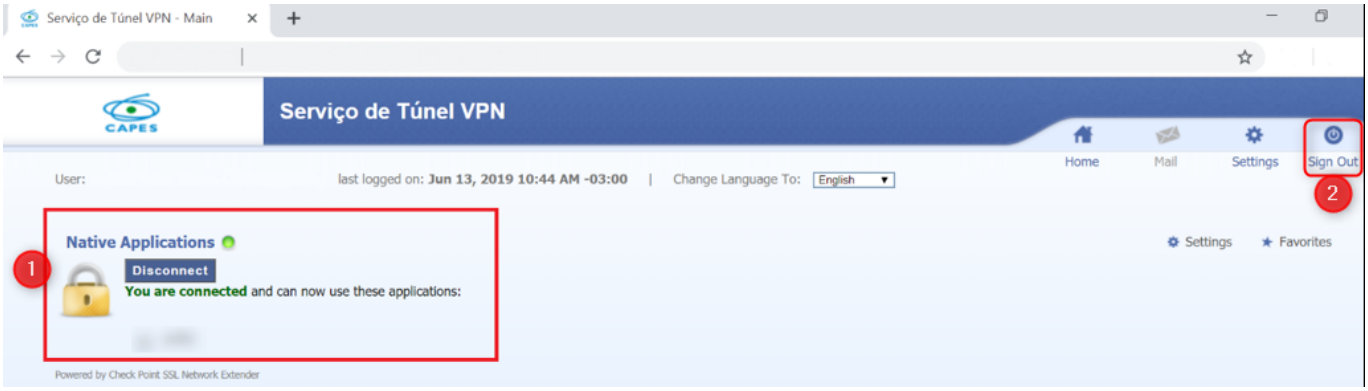





- Pronto! Acesse os serviços que foram permitidos para sua conta.

### 4.2.2 - Desconectar

- Para desconectar da VPN de forma segura, clique em "**Disconnect** e depois faça "**Logoff**".




## 4.3 - Acesso Remoto a Estação

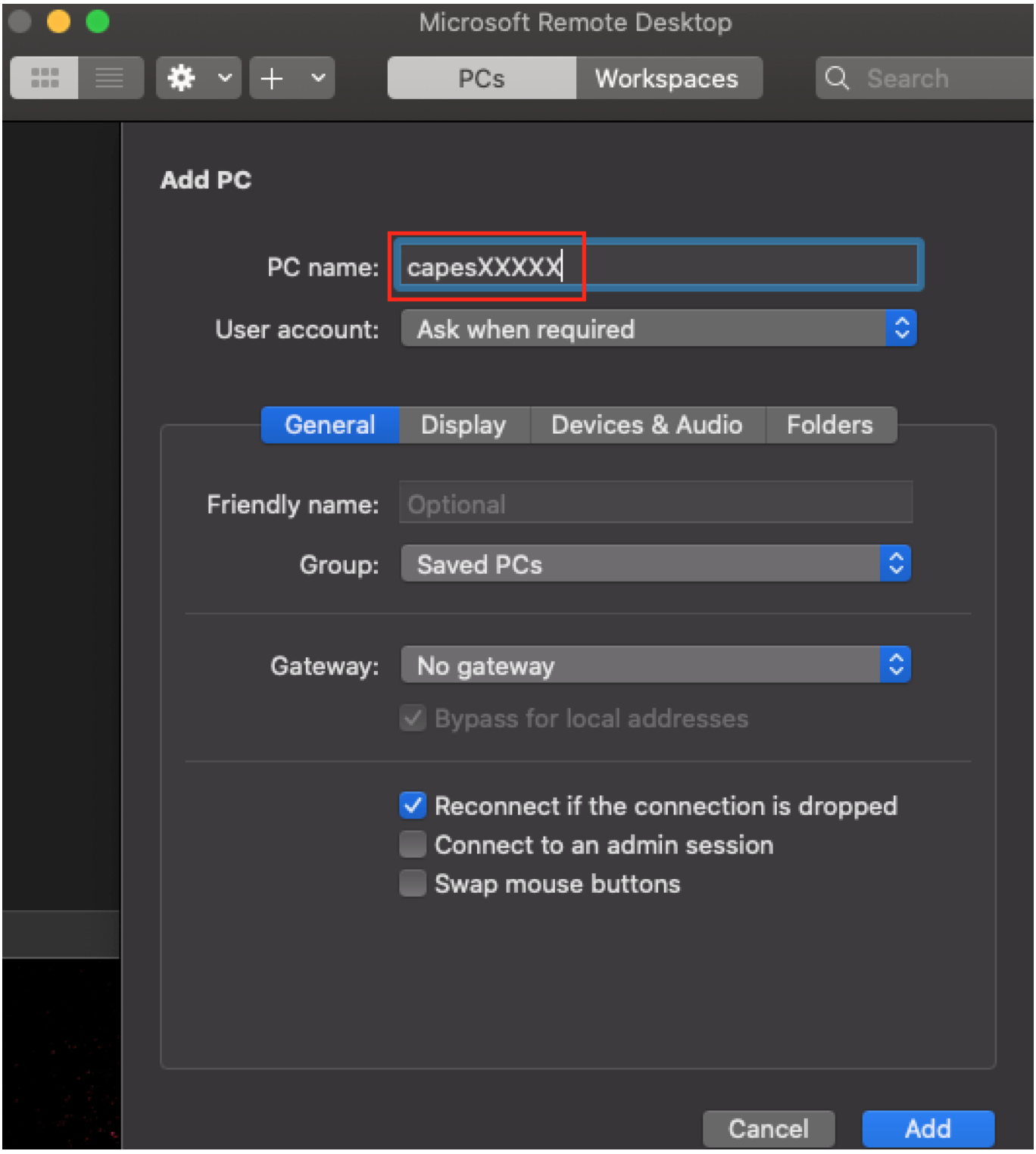
Para o acesso a uma estação de trabalho **Windows** de forma remota, siga os passos:

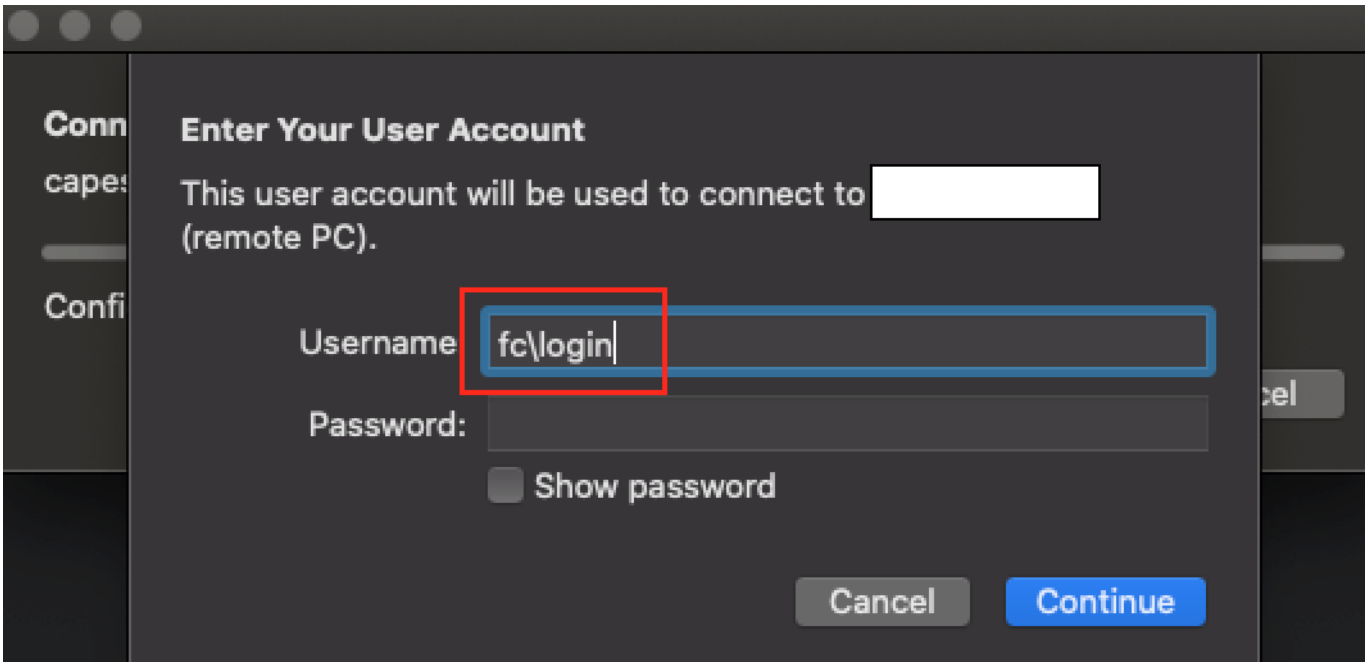
**Instalação** - o aplicativo homologado para uso e recomendado é:

- **Microsoft Remote Desktop** - disponível na Apple Store


**Configuração** - Abra o aplicativo e insira dados conforme imagem abaixo:

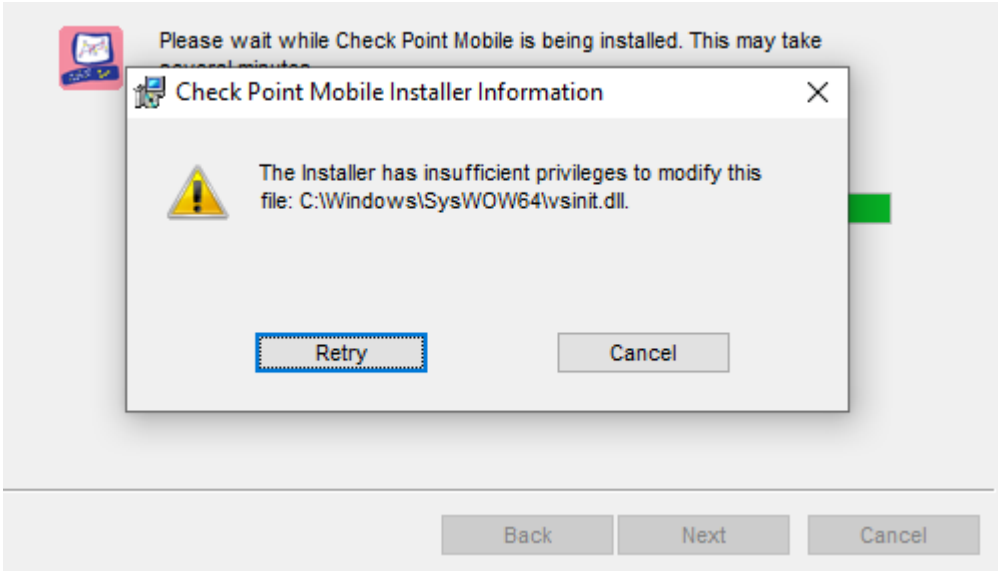
- **Adicionar Computador** - clique em **Add PC** e insira:
  - **Nome da Estação** - em **PC Name** coloque o nome da máquina. Não é recomendado o uso de IP, pois eles podem mudar com o tempo.
- **Conecte** - selecione o computador criado e clique em **Connect**. Informe seu login de rede. Veja imagens abaixo.


Microsoft Remote Desktop
PCs
Workspaces
Search
Add PC
PC name:
capesXXXXX
User account:
Ask when required
General
Display
Devices & Audio
Folders
Friendly name:
Optional
Group:
Saved PCs
Gateway:
No gateway
Bypass for local addresses
Reconnect if the connection is dropped
Connect to an admin session
Swap mouse buttons
Cancel
Add

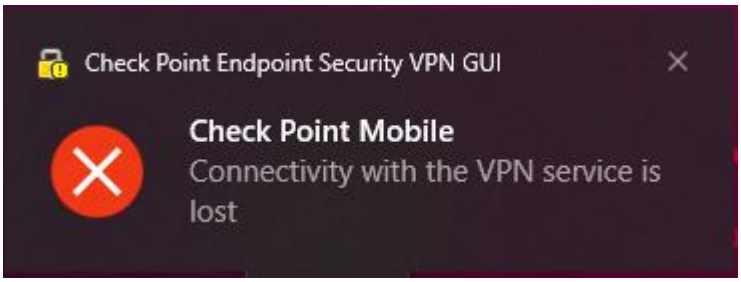



# 5 - Problemas Conhecidos

- **Conflito de Endereçamento de IP** - pode ocorrer de que sua rede local tenha as mesma faixa de IP utilizada na CAPES, gerando um conflito de endereçamento. Verifique que sua rede não utiliza a mesma faixa de IPs da CAPES.
- Problema na desinstalação de pacote anterior para a instalação do novo pacote:




- Realizar o download do pacote - EPPatcher_for_users.exe
- Problema da atualização do Windows:**Erro para iniciar o serviço**




- Executar a correção no regedit

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vna_ap]
"Start"=dword:00000000
```