

Sistema de Controle de Acesso de Usuários

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO
(SRMEx/1915 – C Infor Nr 11/1966)

MANUAL DO USUÁRIO

Brasília-DF, 24 de novembro de 2025.

Sumário

1 O que é o SisCAU? 2
2 “Desejo acessar a Internet. Como procedo?” 3
3 “Acessei o Portal, porém o botão ‘Iniciar sessão’ está desabilitado. O que eu faço?” 5
4 “O que são perfis de acesso?” 5
5 “Tentei acessar o Portal do Usuário, porém esqueci minha senha. Como faço para alterá-la?” 6
6 Autenticação de dois fatores (2FA) 9
7 “O que é FIDO2? É possível usar um token de segurança USB/NFC para acessar o Portal do SisCAU” 11
8 “Estou em casa e preciso acessar a EBNet (via VPN). Como procedo?” 14
8.1 Instalação e configuração do cliente VPN em ambiente desktop 14
8.1.1 Instalação do cliente VPN no Windows 14
8.1.2 Instalação do cliente VPN no macOS 17
8.1.3 Instalação do cliente VPN no Linux 19
8.1.4 Configuração do cliente VPN em ambiente desktop 20
8.1.4.1 Autenticação por senha e código de uso único 20
8.1.4.2 Autenticação por certificado digital (AC Defesa) 22
8.2 Instalação e configuração do cliente VPN em dispositivos móveis (Android e iOS) 26
8.3 Problemas comuns no acesso remoto (VPN) 30
8.3.1 Conta sem permissão de acesso remoto (VPN) 30
Anexo A – Perfis de Acesso 31

1 O que é o SisCAU?

O Sistema de Controle de Acesso de Usuários (SisCAU) visa prover acesso à EBNet, à Internet e aos serviços de TIC fornecidos pelo Sistema de Telemática do Exército (SisTEx) de forma confiável e segura.

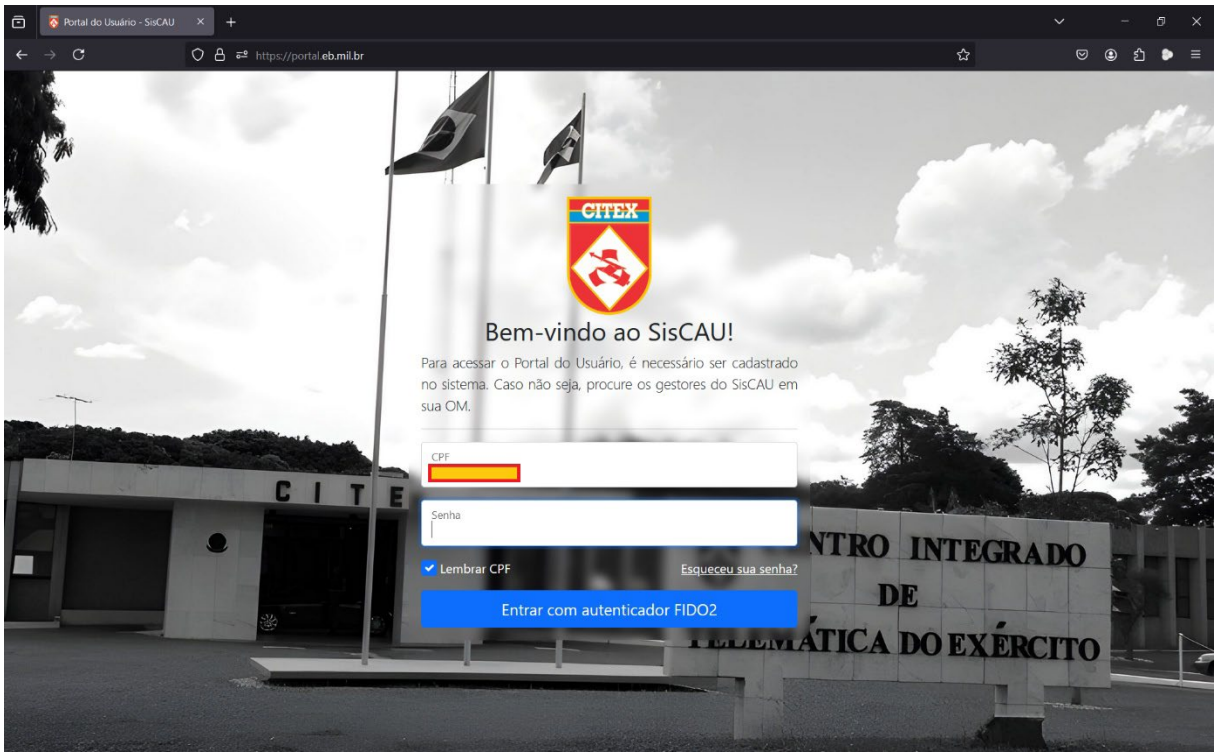
Além disso, o SisCAU visa atender às exigências previstas no Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), que impõe ao provedor de acesso a aplicações de Internet o dever da guarda de registros de conexão (*logs*), nos termos do art. 13 do referido diploma legal:

"Art. 13. Na provisão de conexão à internet, ***cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo****, em ambiente controlado e de segurança,* ***pelo prazo de 1 (um) ano****, nos termos do regulamento.*

> *§ 1º* ***A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros****.*
>
> *§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.*
>
> *§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.*
>
> *§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.*
>
> *§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial (...)"*

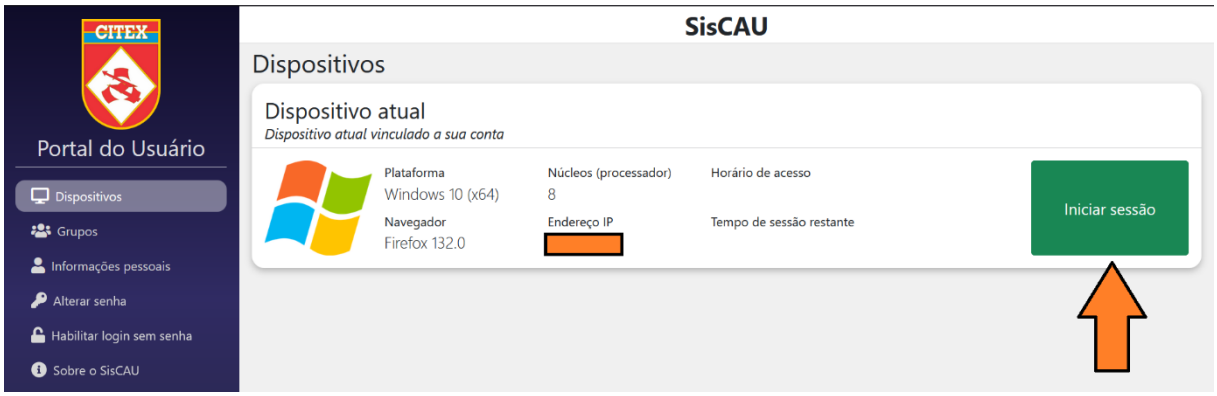
2 “Desejo acessar a Internet. Como procedo?”

Para acessar a Internet, o usuário deverá acessar o Portal do Usuário do SisCAU através do endereço eletrônico https://portal.eb.mil.br:

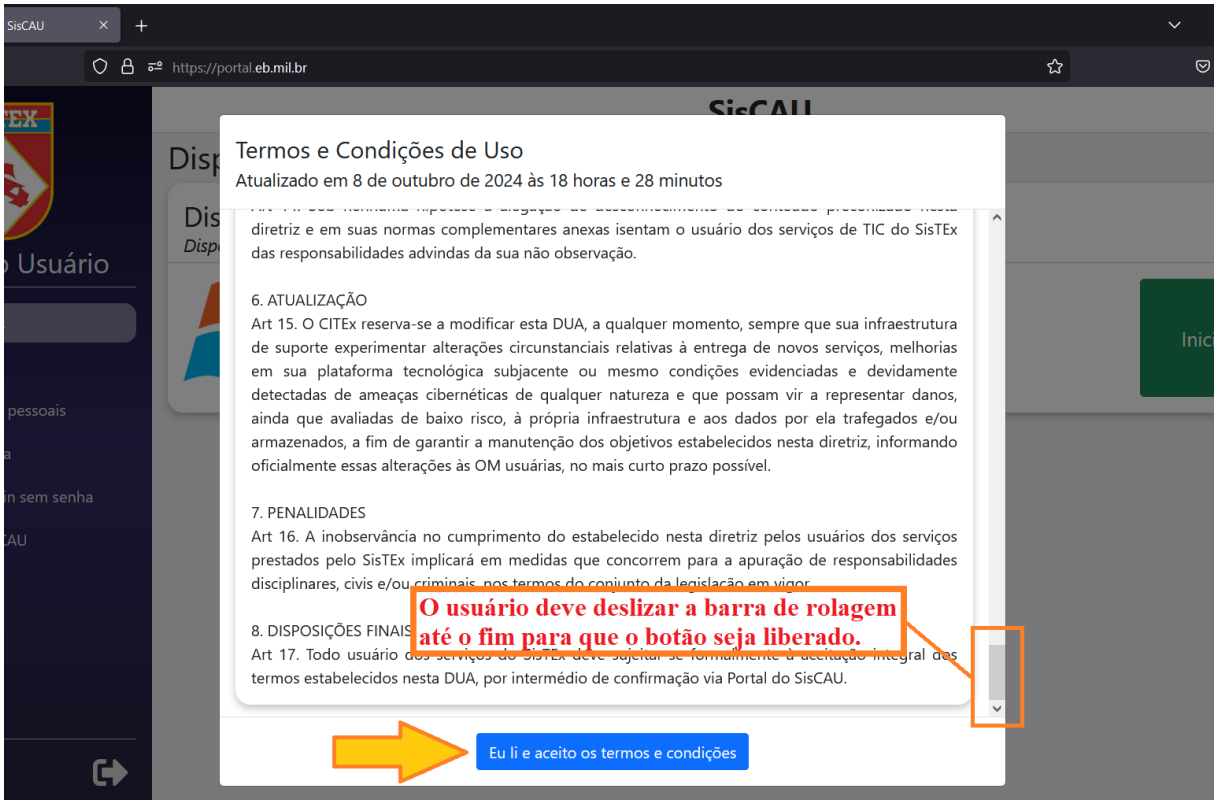


Obs: Vale ressaltar que o usuário deve ser cadastrado no Sistema para conseguir acessar o Portal. Caso não seja, entre em contato com os gestores do SisCAU em sua OM.

Ao acessar o Portal, basta clicar no botão “Iniciar sessão” na cor verde, conforme imagem abaixo:



Mediante prévia concordância dos Termos e Condições de Uso, o usuário estará autorizado a navegar na Internet.



Obs: O botão em destaque na imagem acima só é liberado quando o usuário desliza a barra de rolagem completamente.

ATENÇÃO: O usuário deverá se certificar que não há qualquer configuração de Proxy em sua máquina. Em caso de dúvida, procure a Seção de Informática ou Divisão de Tecnologia da Informação (ou equivalente) de sua OM.

3 “Acessei o Portal, porém o botão ‘Iniciar sessão’ está desabilitado. O que eu faço?”

É possível que ao acessar o Portal a seguinte mensagem seja exibida:



Neste caso, entre em contato com os gestores do SisCAU em sua OM e solicite-os que sua conta seja adicionada a um **Grupo de Acesso à Internet**.

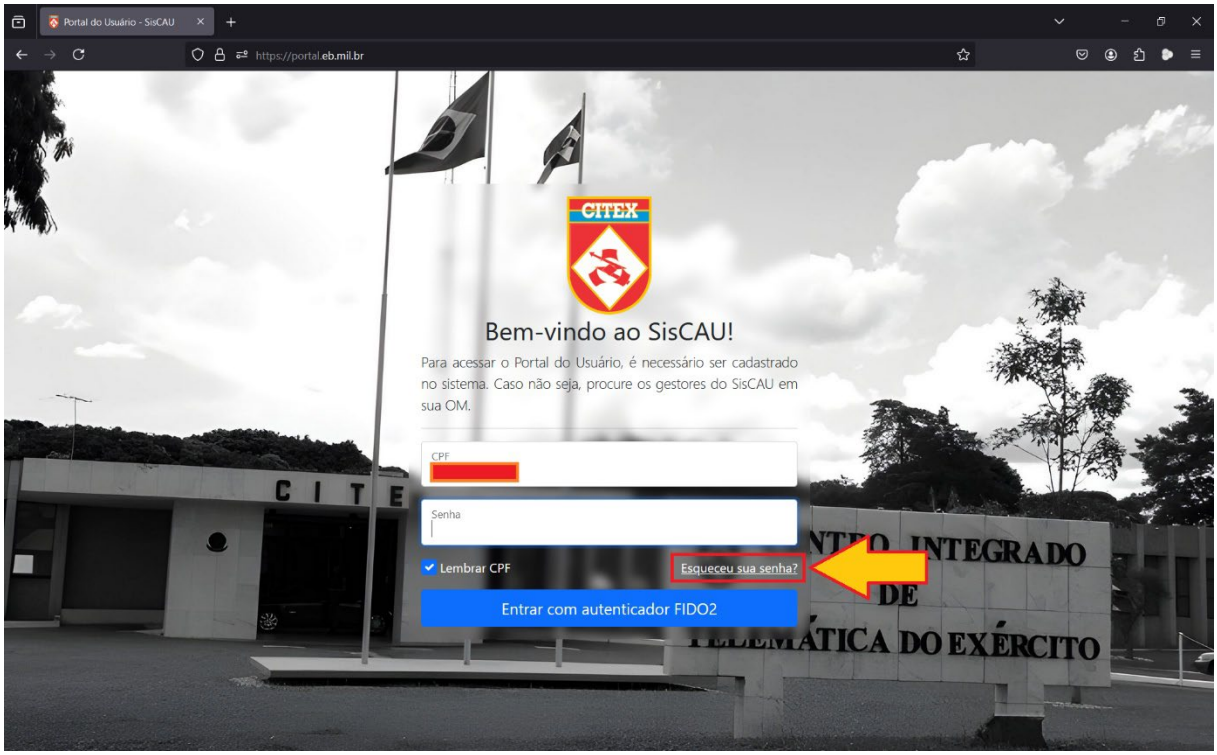
4 “O que são perfis de acesso?”

Um perfil de acesso determina que tipos de *sites* e aplicações um usuário pode acessar ao navegar na Internet.

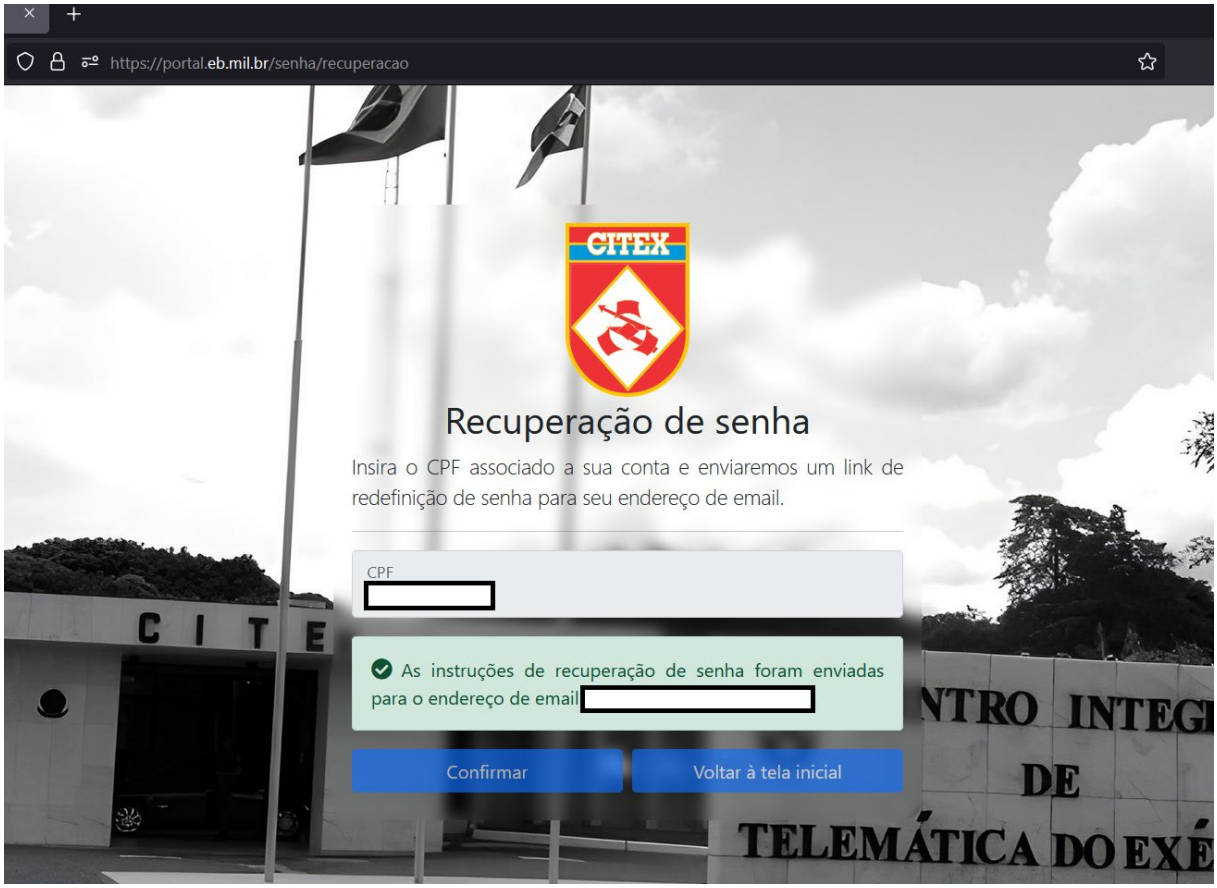
A descrição dos perfis está disponível no Anexo A do corrente documento.

5 “Tentei acessar o Portal do Usuário, porém esqueci minha senha. Como faço para alterá-la?”

Neste caso, na página de *login* do Portal clique em “Esqueceu sua senha?”:



Após inserir seu CPF, o sistema enviará para o endereço de email vinculado a sua conta do SisCAU uma mensagem com as instruções para redefinir a senha:



A mensagem de recuperação é remetida por siscau@7cta.eb.mil.br com assunto "Redefinição de senha – SisCAU":

Redefinição de senha - SisCAU

CITEX

Sistema de Controle de Acesso de Usuários

Caro(a) [redacted],

Recebemos uma requisição de redefinição de senha da sua conta do SisCAU.

Alterar senha

Alternativamente, você pode copiar e colar o *link* a seguir diretamente no seu navegador: https://portal.eb.mil.br/senha/redefinicao/[redacted]

Se você não requereu alteração de senha, ignore esta mensagem.

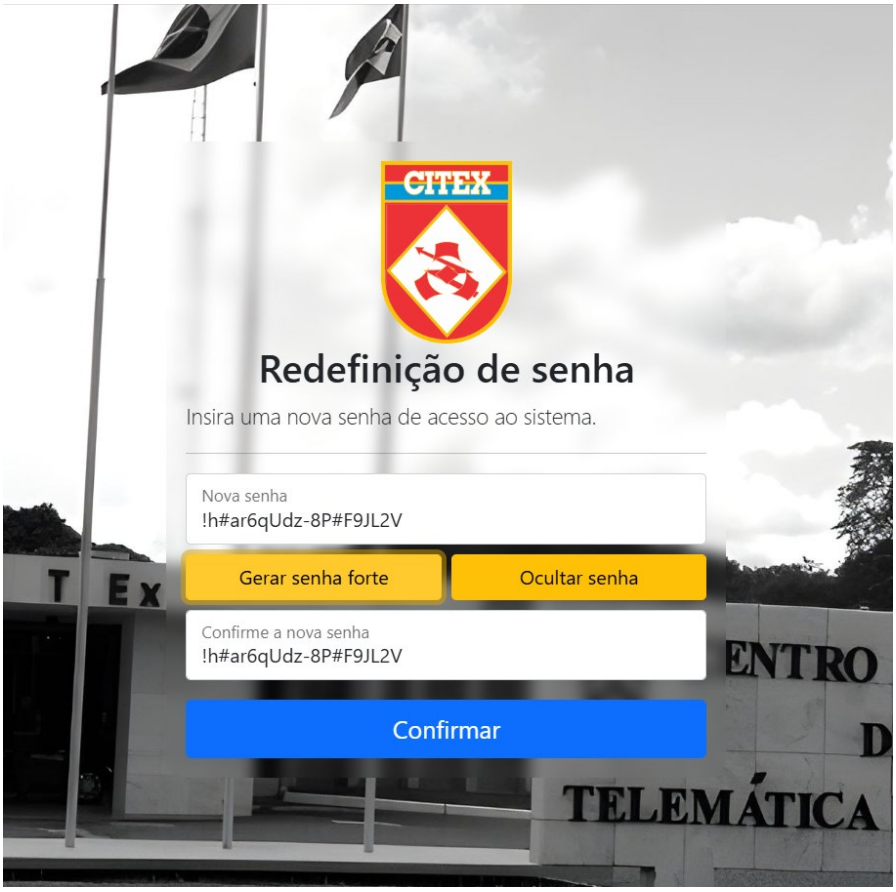
Esta é uma mensagem automática. Não responda este email.

Atenciosamente,

Divisão de Operação do 7º CTA.

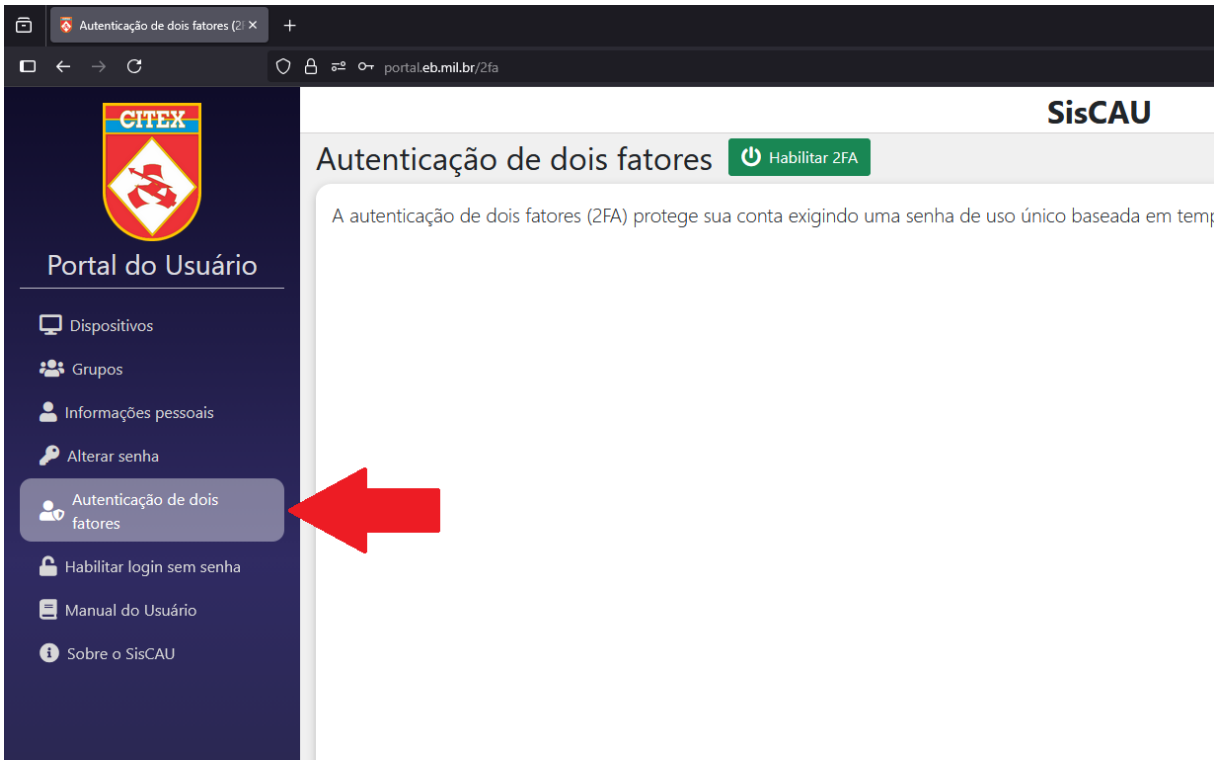
Centro Integrado de Telemática do Exército © 2024. Todos os direitos reservados.

Ao acessar o *link* de redefinição de senha, o usuário será redirecionado para a página de redefinição de senha:

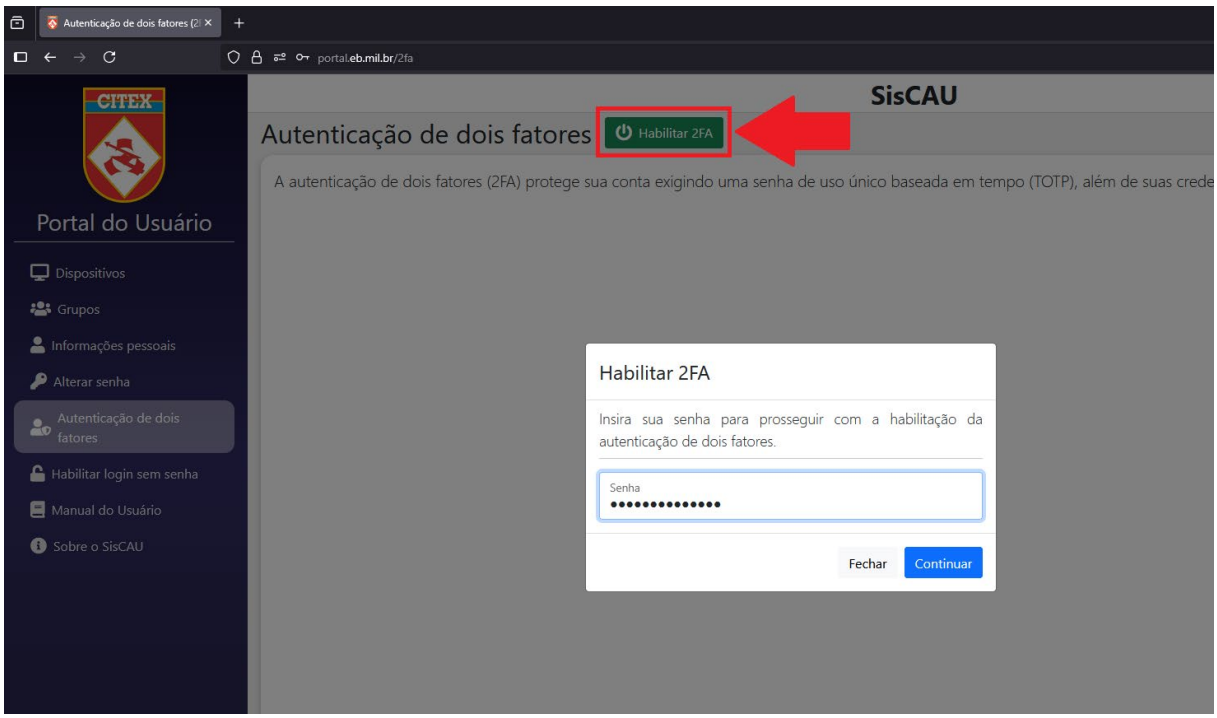


6 Autenticação de dois fatores (2FA)

Para habilitar a autenticação de dois fatores no SisCAU, o usuário deverá clicar em "Autenticação de dois fatores" no menu lateral do Portal do Usuário:



Em seguida, clique no botão "Habilitar 2FA" e insira sua senha:



Para concluir, siga as instruções exibidas na tela:



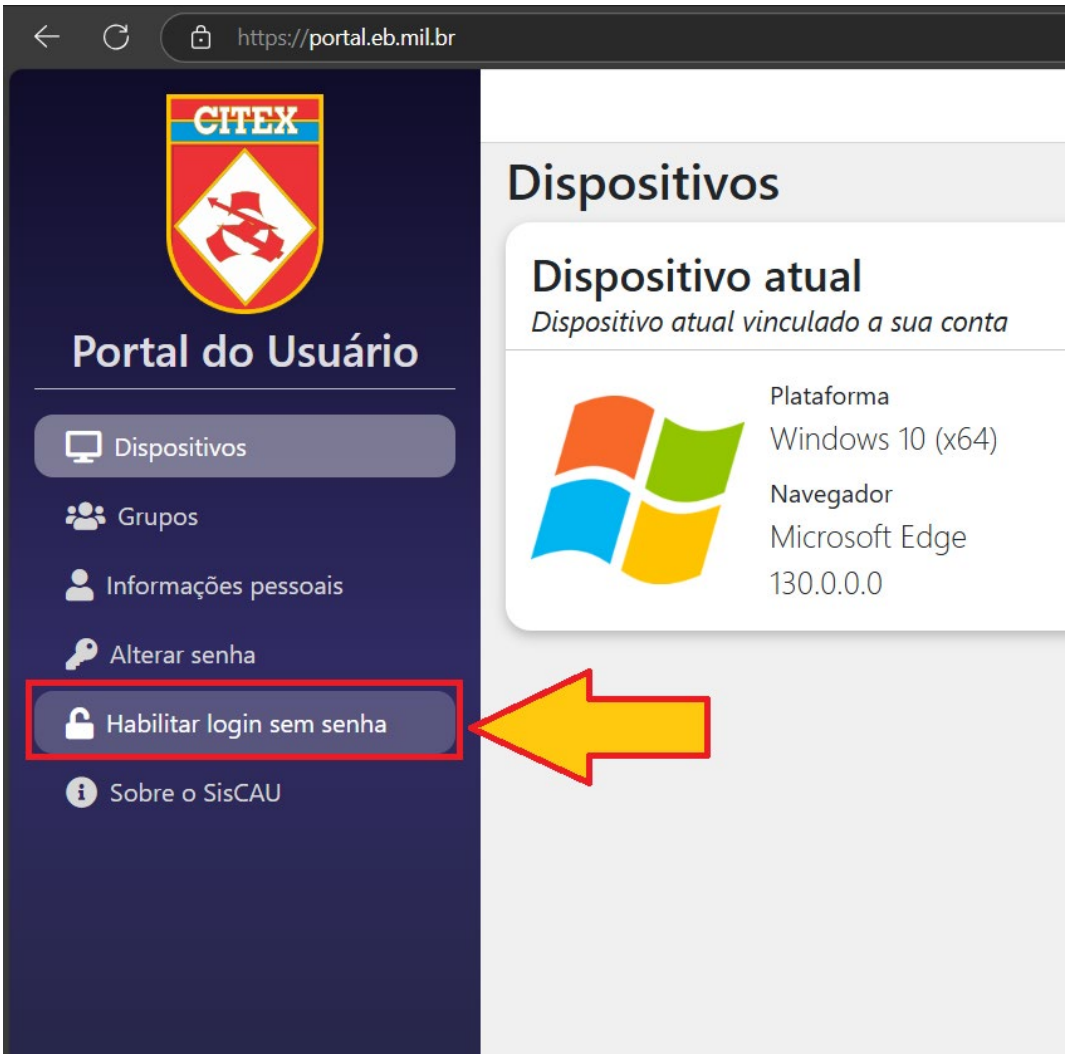
7 “O que é FIDO2? É possível usar um token de segurança USB/NFC para acessar o Portal do SisCAU”

O FIDO2 (*Fast IDentity Online*) é um conjunto de especificações técnicas abertas que definem um mecanismo rápido e extremamente seguro de autenticação em serviços Web.

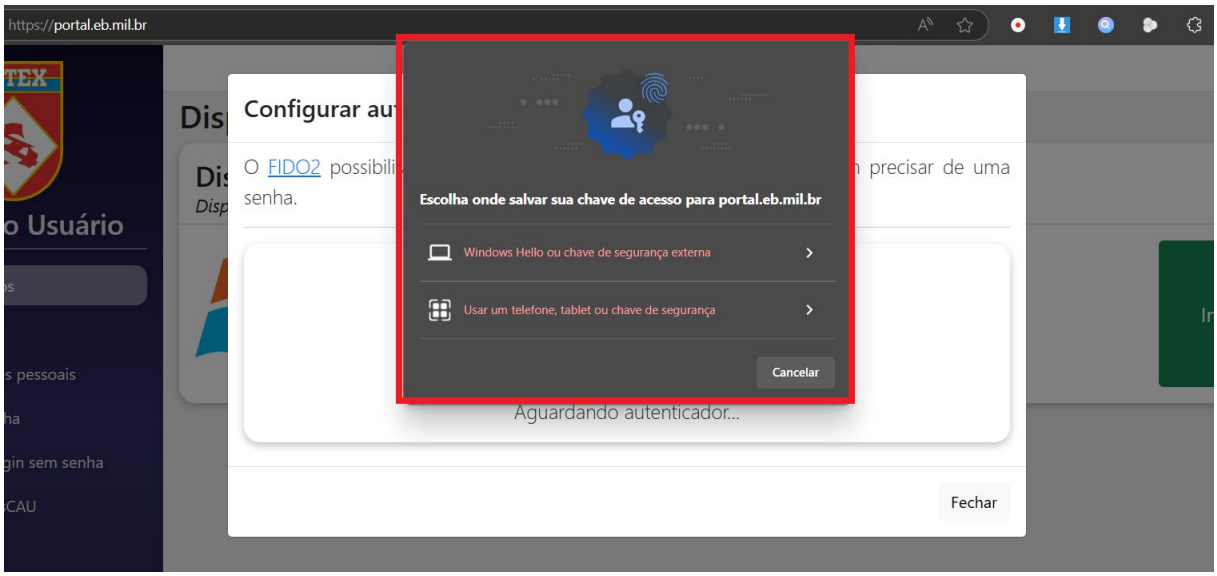
A aliança FIDO surgiu por iniciativa da indústria e empresas de tecnologia (Microsoft, Google, Apple, Meta, Mastercard, etc), que necessitavam de métodos de autenticação de usuários mais confiáveis.

Para habilitar o *login* sem senha no SisCAU, é necessário que o usuário disponha de um *token* de segurança USB/NFC com suporte à FIDO2 ou que a placa-mãe de seu computador seja equipada com um chip TPM (microcontrolador criptográfico). No último caso, o recurso de segurança Windows Hello deve estar habilitado.

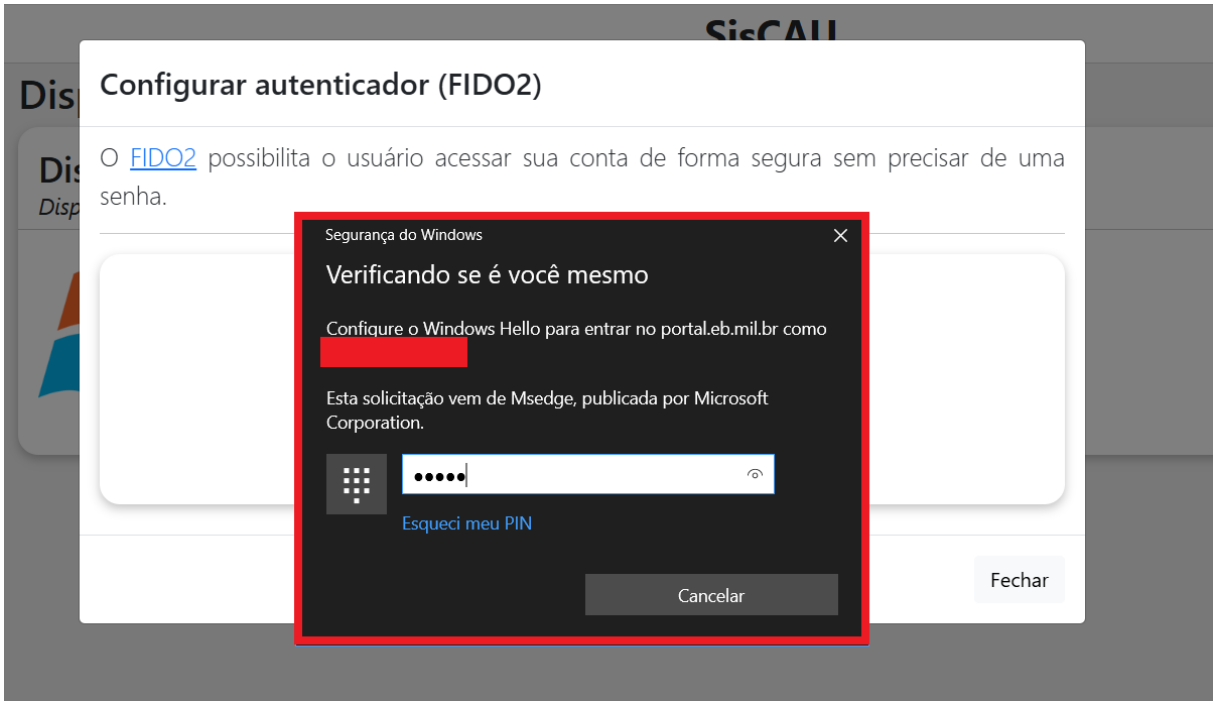
No Portal do Usuário, clique em “Habilitar login sem senha”:

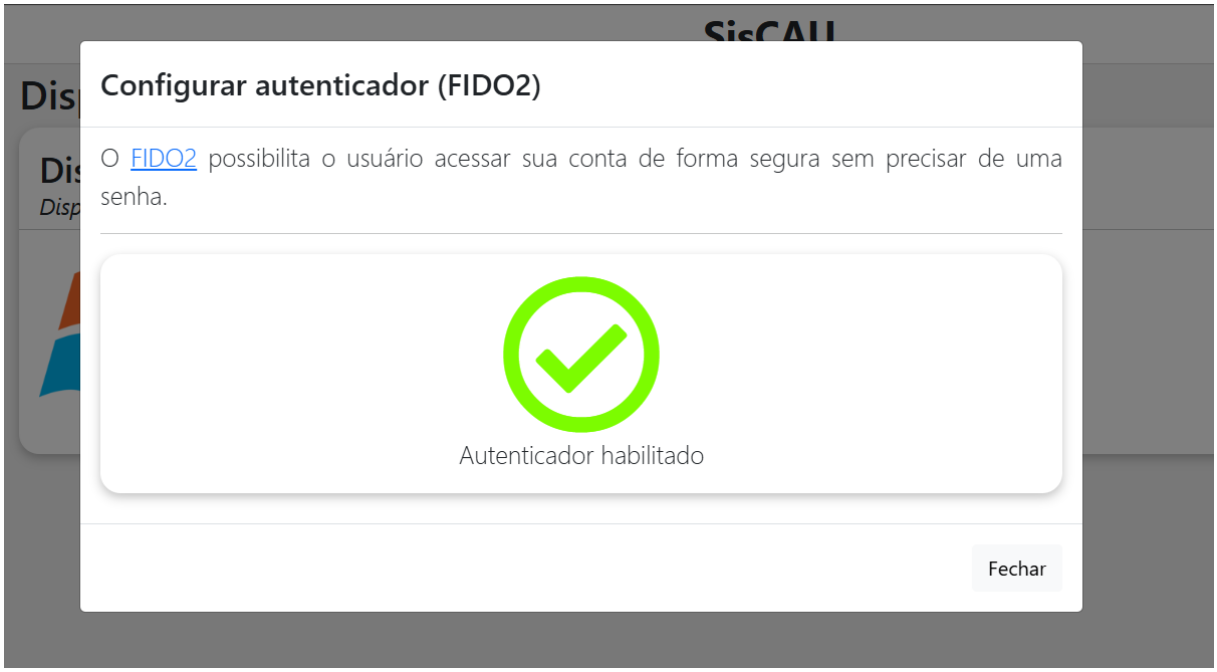


Selecione o local onde a chave RSA será armazenada:



No exemplo a seguir, a chave criptográfica foi armazenada no chip TPM através do Windows Hello:





Uma vez configurada a chave de acesso, o acesso ao Portal do Usuário pode ser feito usando o autenticador FIDO2:



8 “Estou em casa e preciso acessar a EBNet (via VPN). Como procedo?”

Para acessar a EBNet de forma remota, o usuário deverá primeiramente instalar em seu dispositivo o cliente VPN da Cisco (Cisco Secure Client).

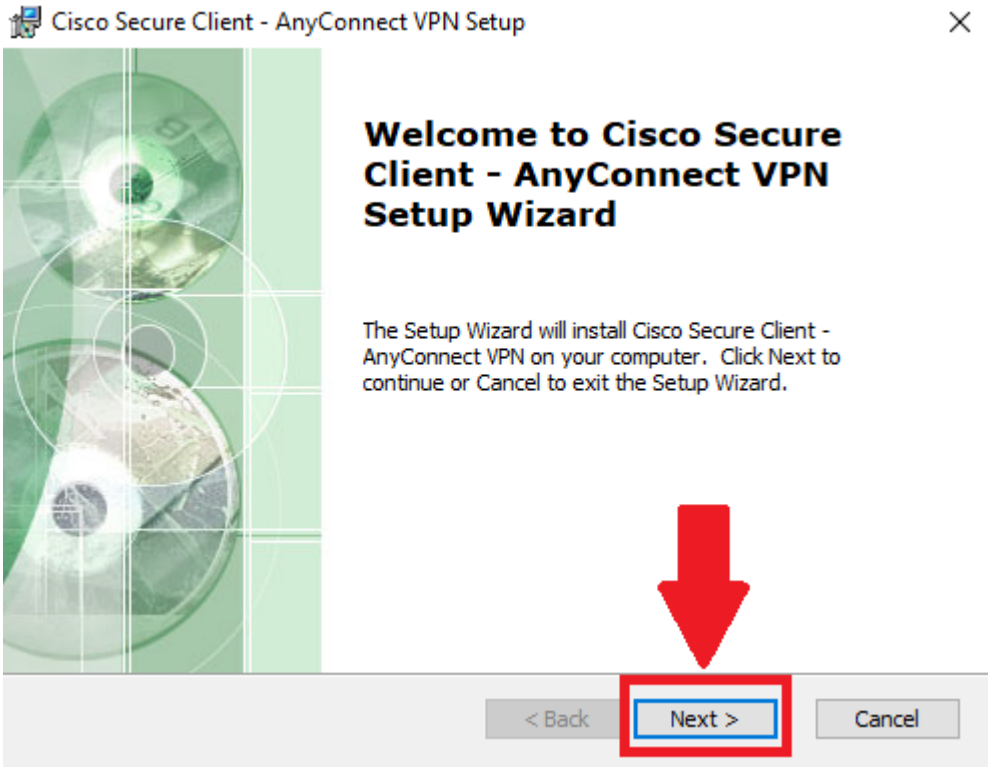
8.1 Instalação e configuração do cliente VPN em ambiente desktop

8.1.1 Instalação do cliente VPN no Windows

Baixe o instalador do Cisco Secure Client para Windows disponível em:

- https://sso-siscau.eb.mil.br/cisco/anyconnect/windows

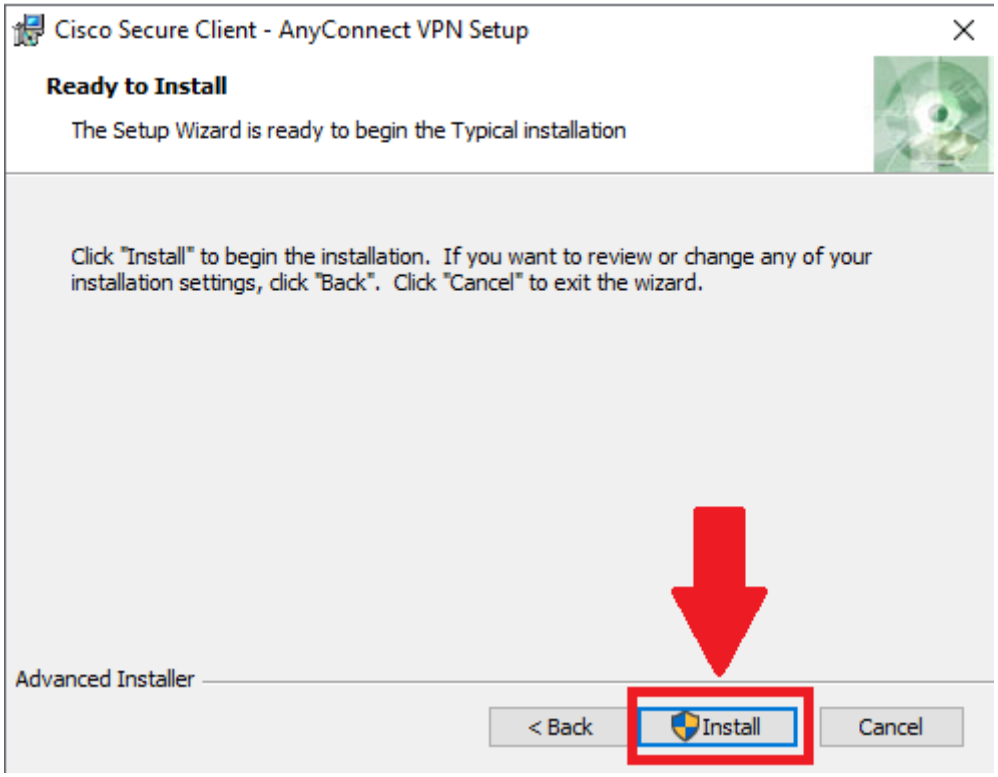
Concluído o download, execute o instalador e clique em “Next”:



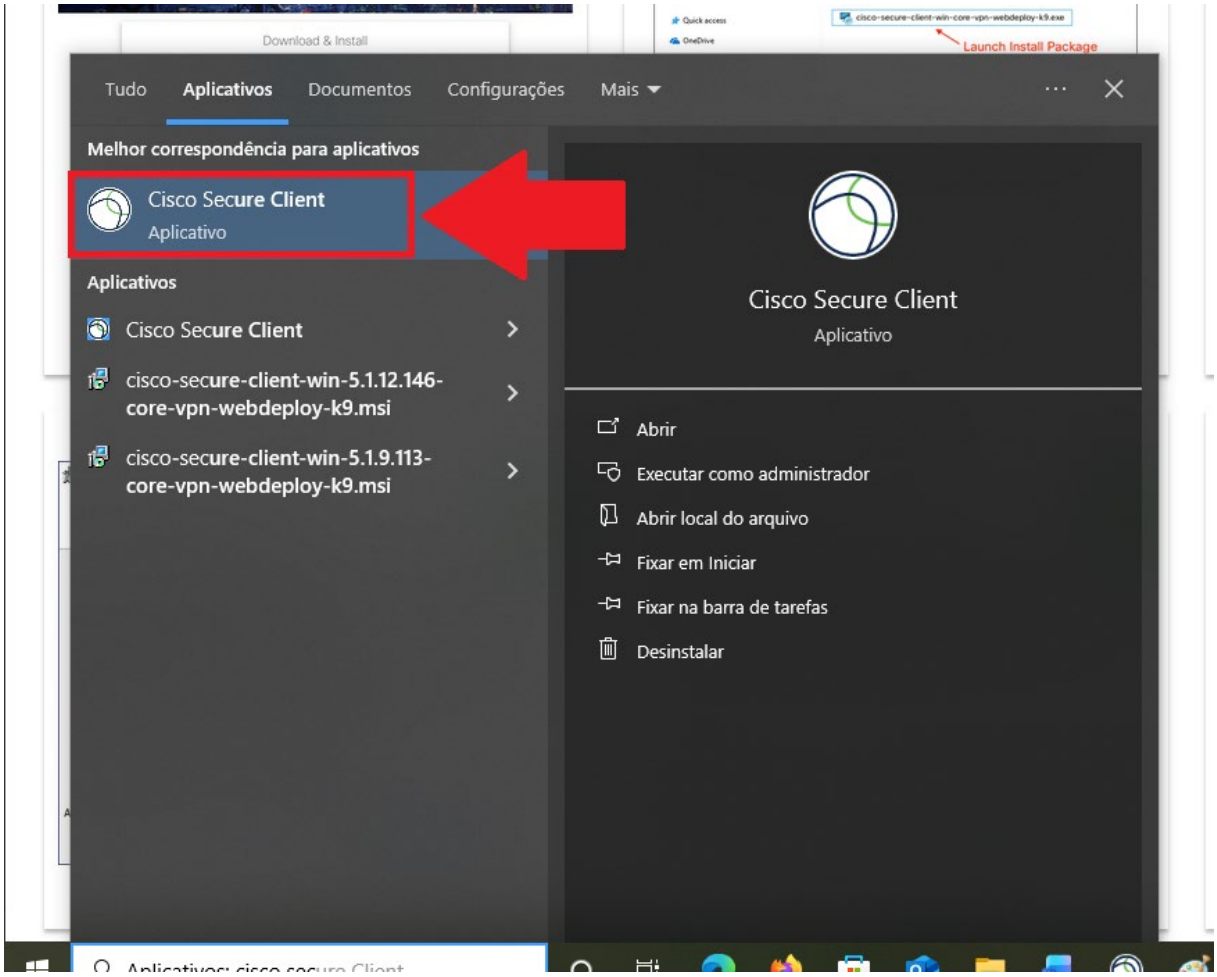
Aceite os termos e em seguida clique em “Next”:



Clique em “Install”:



Após a instalação do cliente VPN, execute-o. Para instruções de como configurar o cliente VPN, prossiga para esta seção:

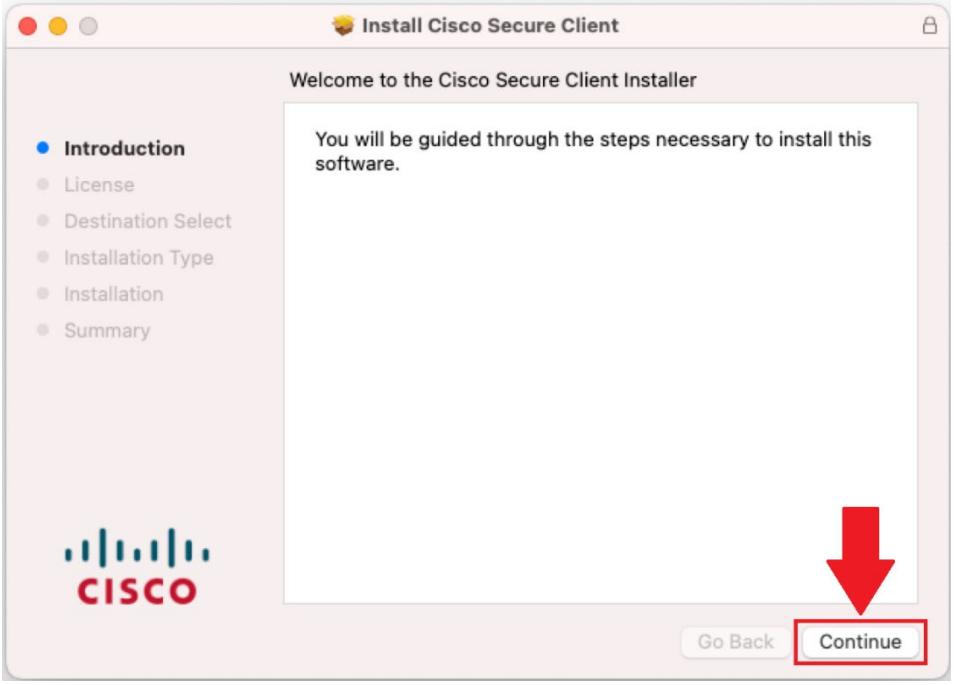


8.1.2 Instalação do cliente VPN no macOS

Baixe o instalador do Cisco Secure Client para macOS disponível em:

- https://sso-siscau.eb.mil.br/cisco/anyconnect/macos

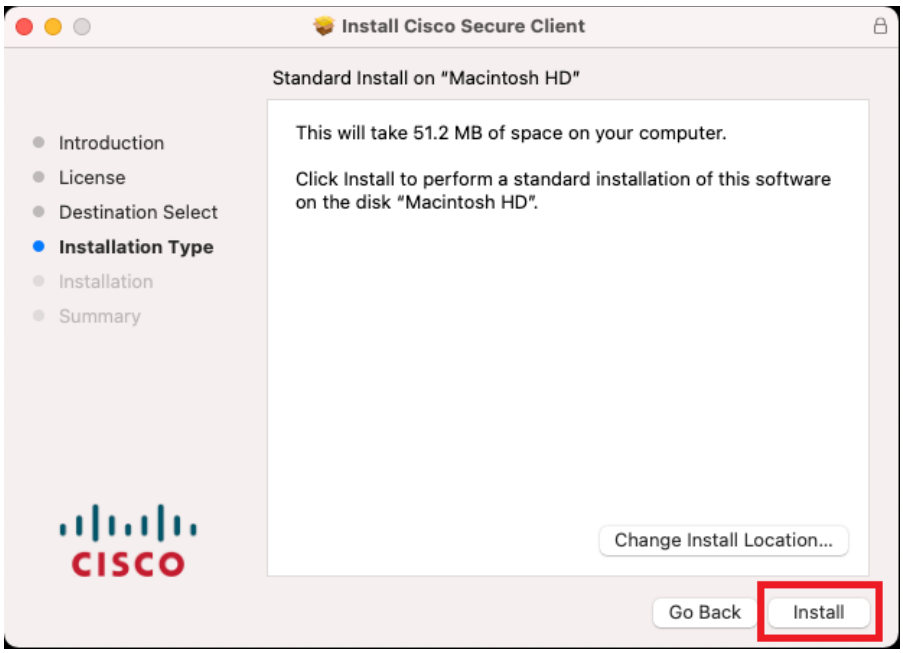
Concluído o download, execute o instalador:



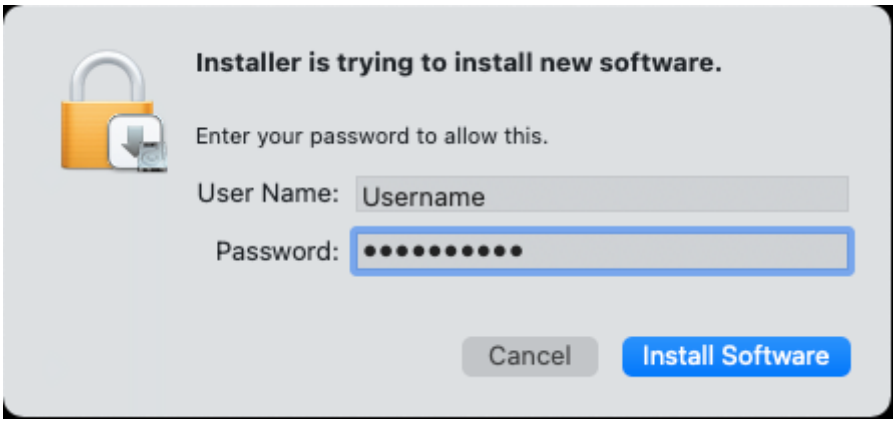
Aceite os termos de uso clicando em “Agree”:



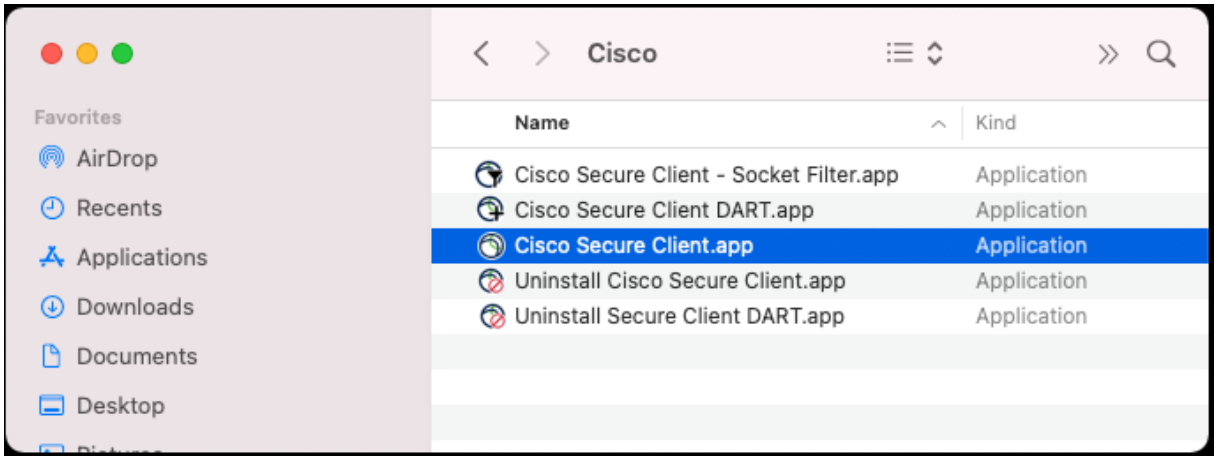
Clique em “Install”:



É necessário privilégio de administrador para prosseguir a instalação:



Após a instalação do cliente VPN, execute-o. Para instruções de como configurar o cliente VPN, prossiga para esta seção:

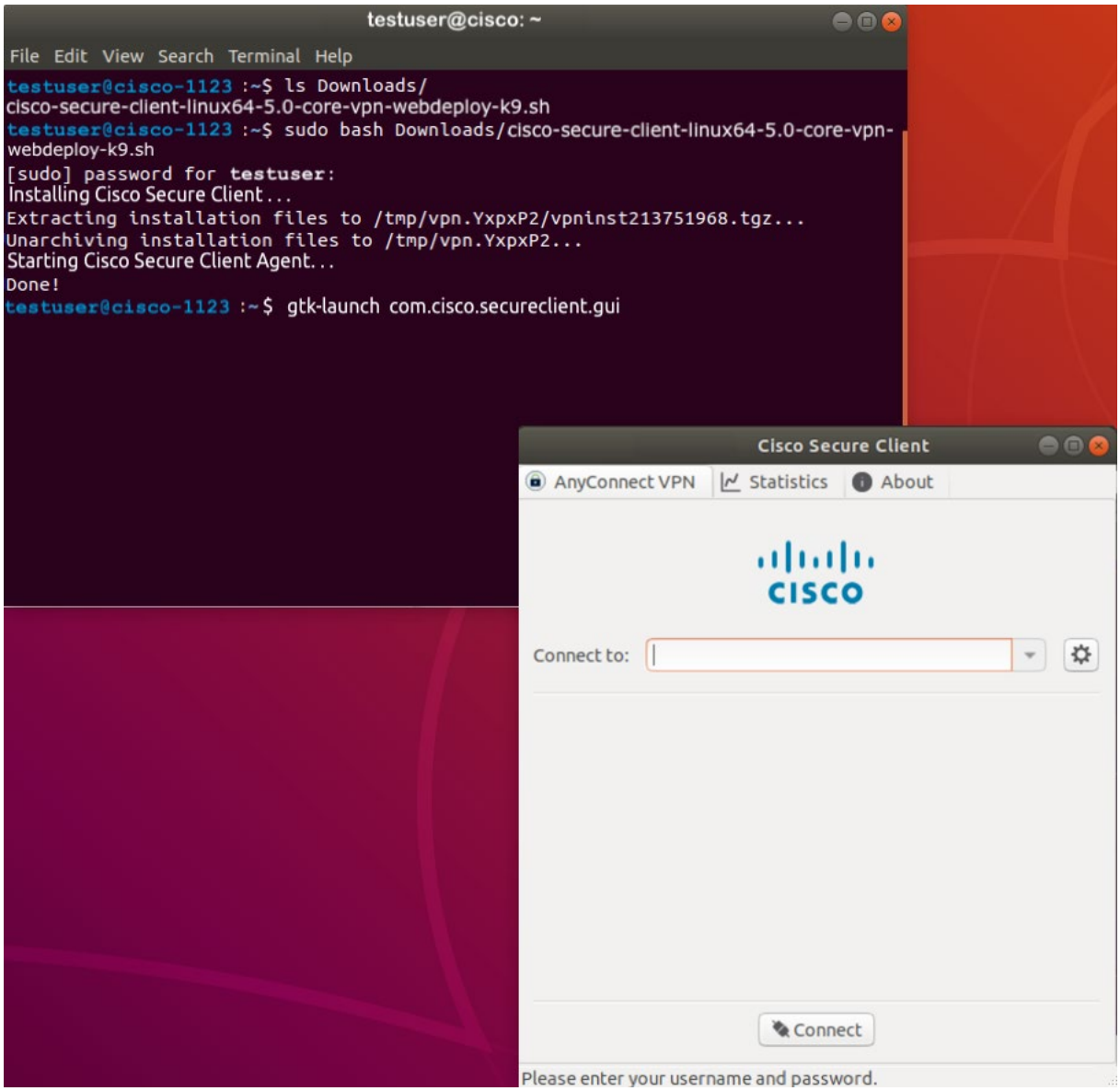


8.1.3 Instalação do cliente VPN no Linux

Baixe o instalador do Cisco Secure Client para Linux disponível em:

- https://sso-siscau.eb.mil.br/cisco/anyconnect/linux

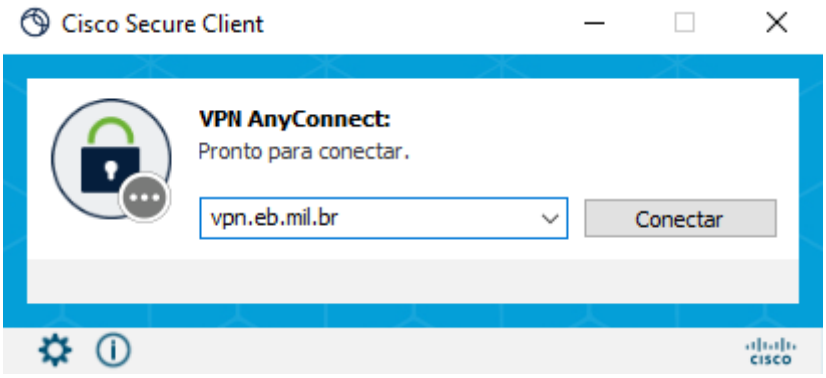
Concluído o download, execute o instalador (*shell script*). Uma vez instalado, para abrir o cliente VPN, execute o comando "gtk-launch com.cisco.secureclient.gui":



Para instruções de como configurar o cliente VPN, prossiga para esta seção.

8.1.4 Configuração do cliente VPN em ambiente desktop

Após abrir o cliente VPN, insira o endereço “vpn.eb.mil.br” e clique em “Conectar”:

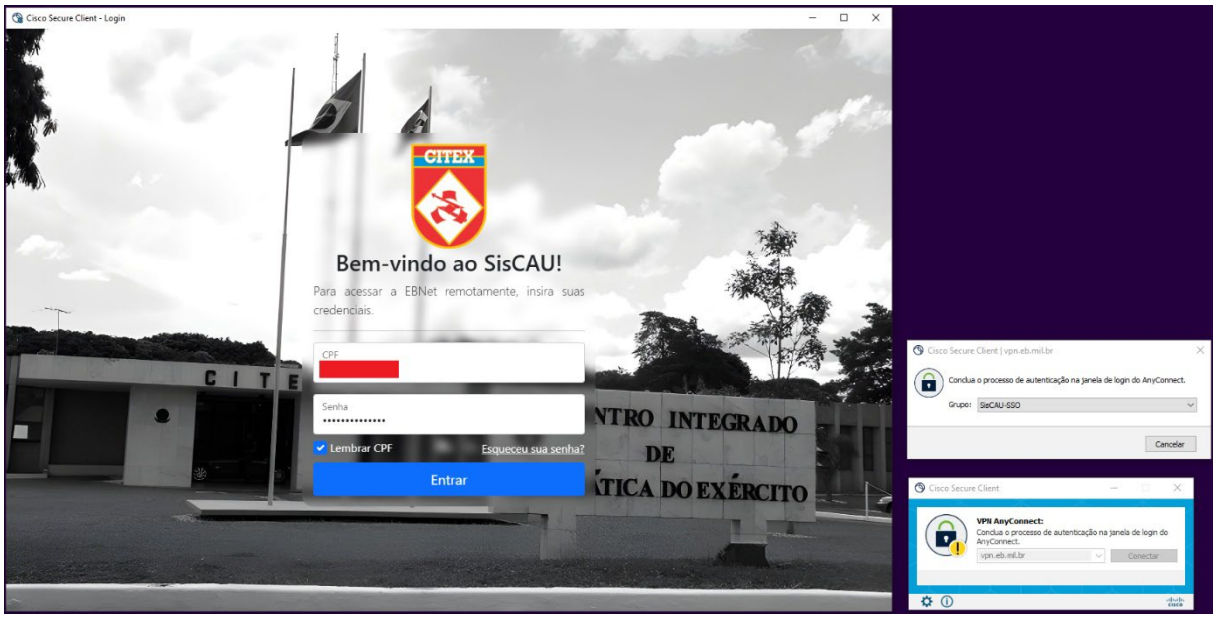


Nesse momento, o usuário será redirecionado para o portal de autenticação do SisCAU. Há dois métodos de autenticação disponíveis para que o usuário se conecte à EBNet via VPN:

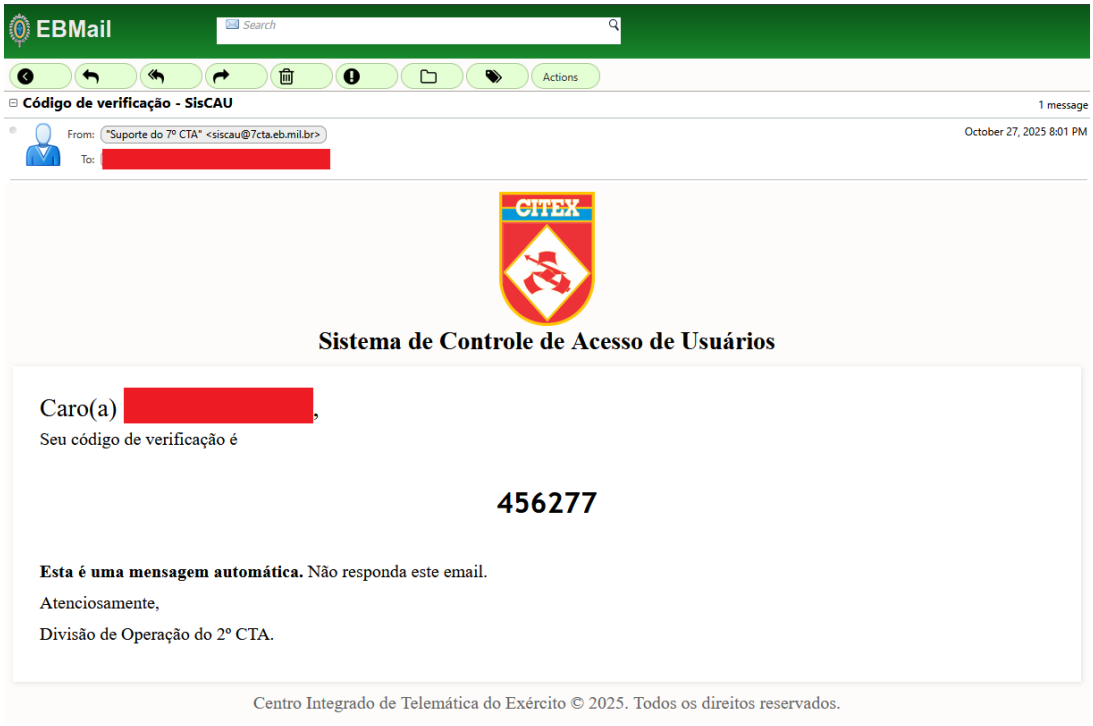
- autenticação por senha e código de uso único;
- autenticação por certificado digital (AC Defesa).

8.1.4.1 Autenticação por senha e código de uso único

Nesse método de autenticação, basta que o usuário insira o CPF e a senha previamente definida no sistema:

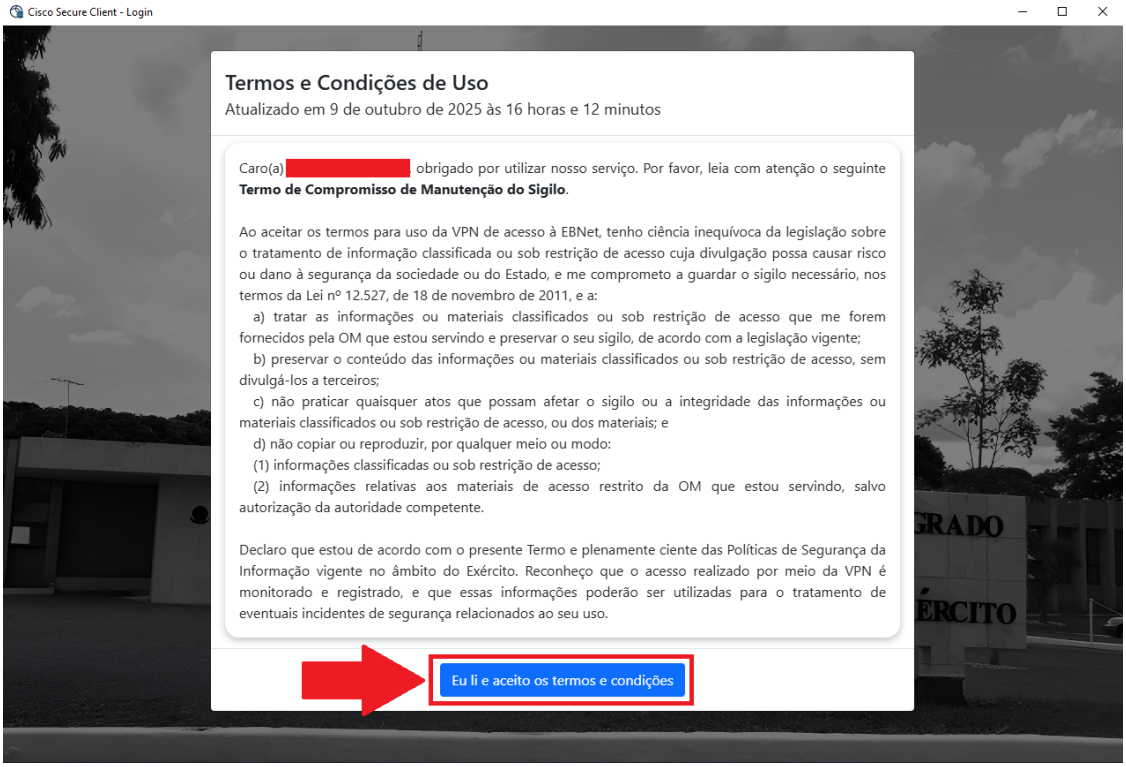


O sistema solicitará que o usuário insira um código enviado para o seu respectivo endereço de email:



Mensagem com o código de verificação enviado pelo SisCAU

Após inserir o código de verificação, os termos e condições de uso da VPN são exibidos ao usuário. Para prosseguir, o usuário deverá aceitar os termos:



Obs 1: Caso o usuário tenha habilitado a autenticação de dois fatores no Portal do Usuário como descrito nesta seção, o sistema solicitará o código de verificação gerado pelo aplicativo de autenticação (Authy, Google Authenticator, Microsoft Authenticator, etc). Portanto, ***nesse caso o sistema não enviará o código de verificação para o endereço de email do usuário****.*

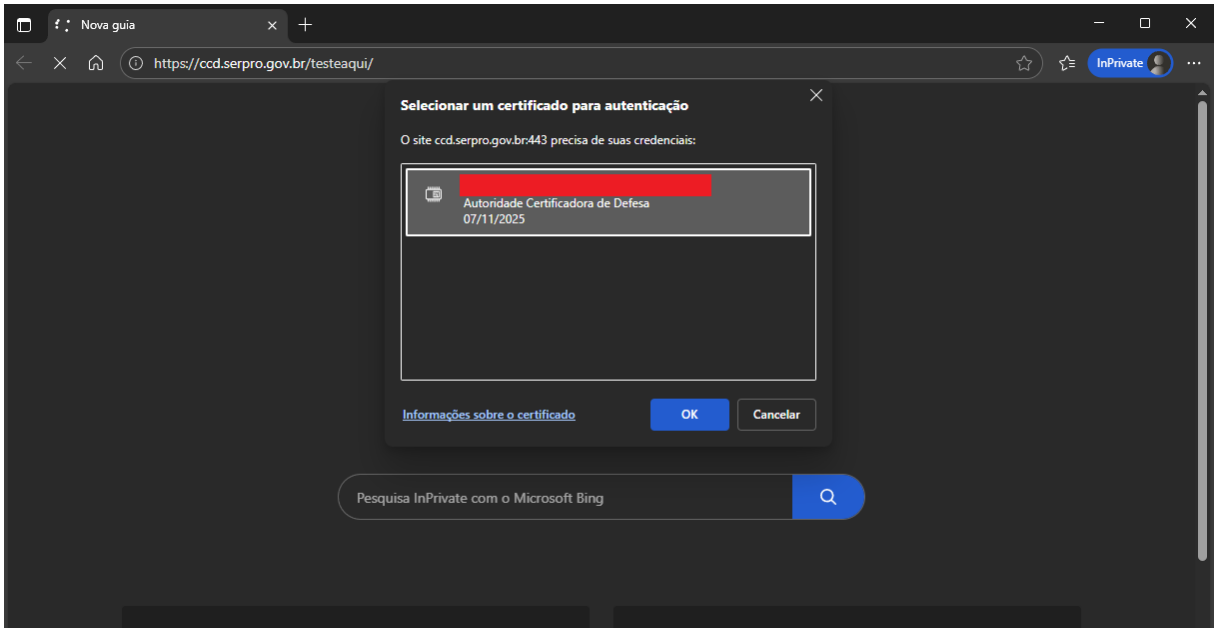
Obs 2: Caso o usuário não lembre a senha, basta clicar no link "Esqueceu sua senha?" e seguir as etapas descritas nesta seção do manual.

8.1.4.2 Autenticação por certificado digital (AC Defesa)

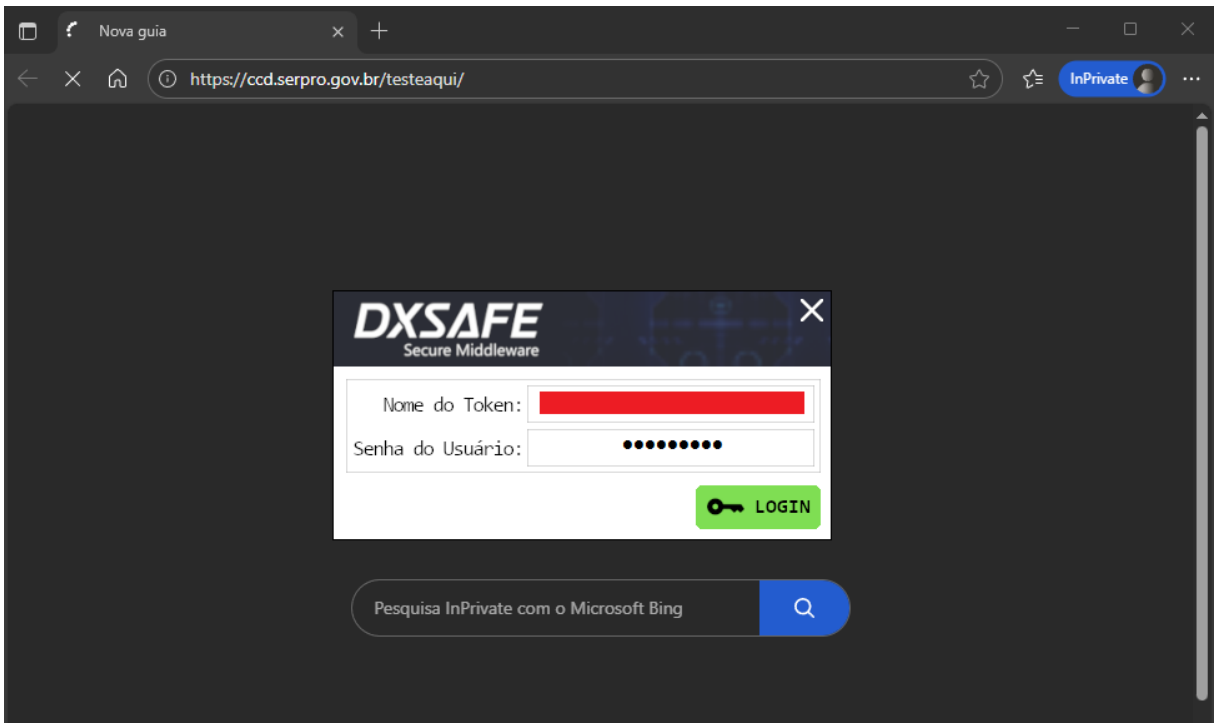
Para estabelecer conexão VPN com um certificado digital emitido pela Autoridade Certificadora do Ministério da Defesa (AC Defesa), é necessário, em primeiro lugar, que o usuário disponha de um certificado válido (A1 ou A3), devidamente reconhecido pelo Sistema Operacional.

Para orientações de como utilizar o certificado digital, acesse a documentação disponível no *website* da AC Defesa: https://www.acdefesa.mil.br/index.php/documentacao.

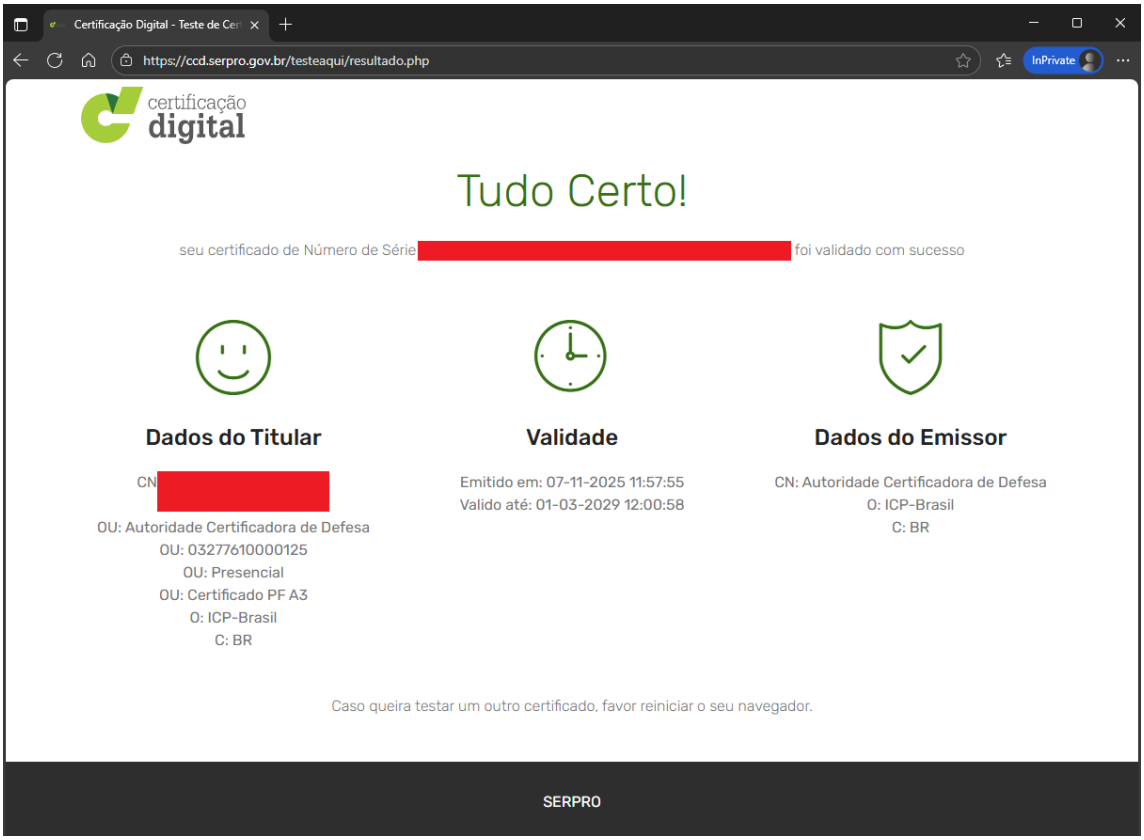
Para testar e validar o certificado digital, acesse o serviço de teste de certificado de cliente do Serpro, disponível em https://ccd.serpro.gov.br/testeaqui. Ao acessar este *link*, o navegador solicitará que o usuário selecione um certificado para autenticação:



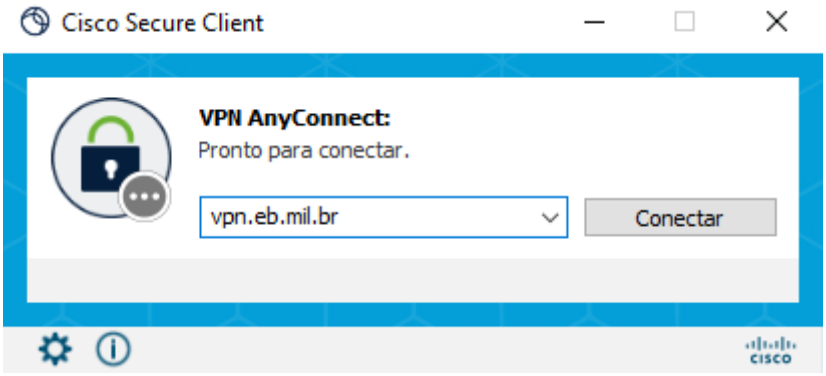
Caso esteja utilizando certificado A3, o *software* do token solicitará o PIN:



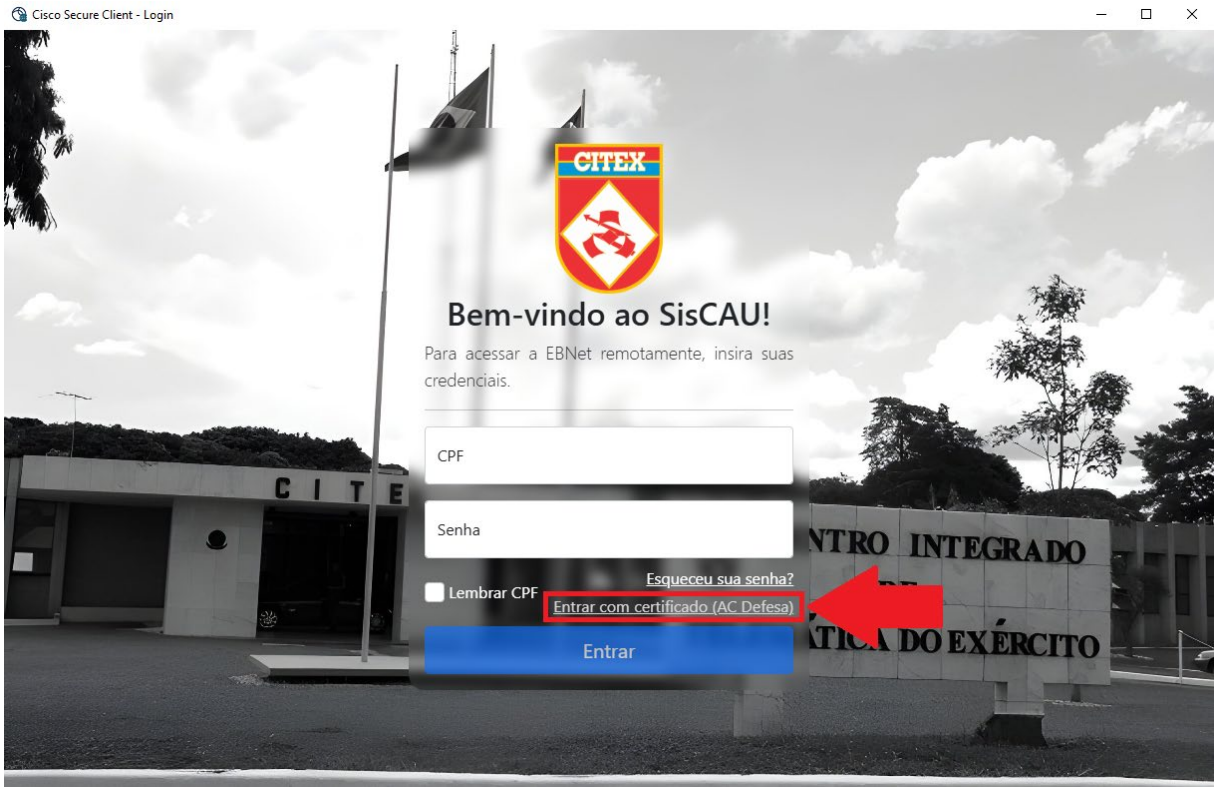
Uma vez carregada a página clique no botão “Testar”. Se a mensagem “Tudo Certo!” for exibida, seu certificado foi reconhecido pelo navegador e pelo sistema operacional e está pronto para uso:



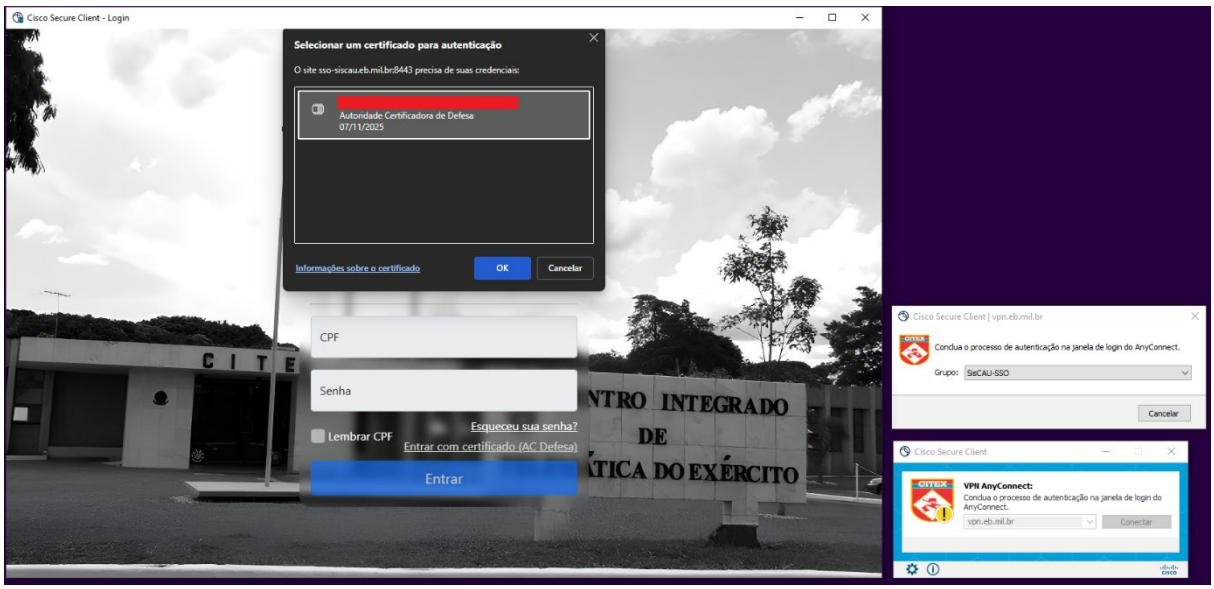
Após validar o certificado digital, abra o cliente VPN (Cisco Secure Client), insira o endereço "vpn.eb.mil.br" e clique em "Conectar":



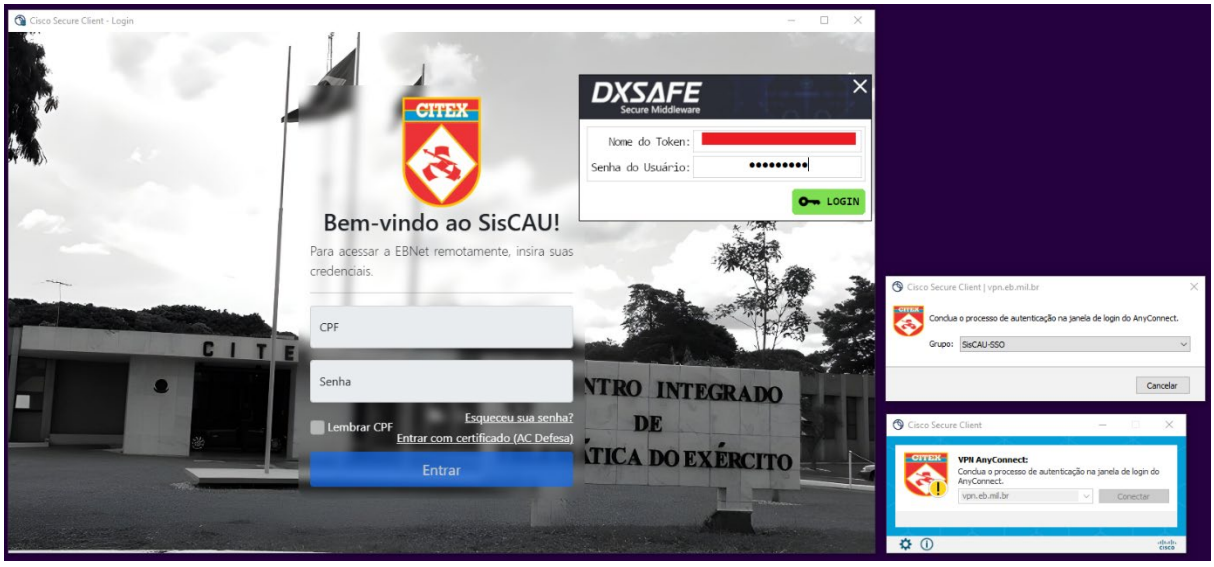
No portal de autenticação do SisCAU, clique em "Entrar com certificado (AC Defesa)":



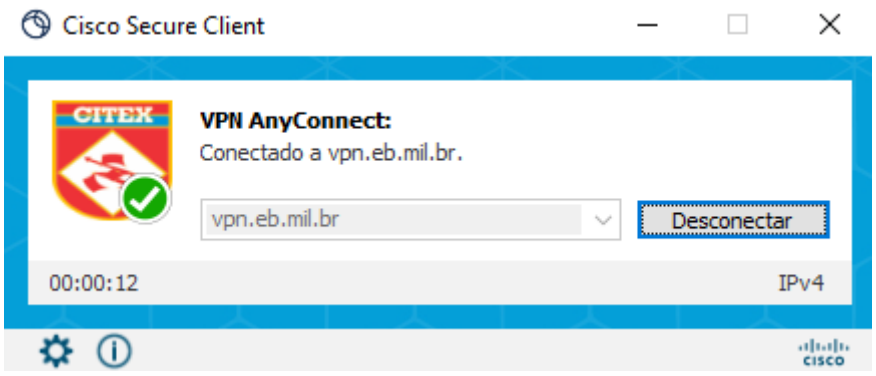
Selecione o certificado para autenticação:



Em caso de certificado A3, insira o PIN:

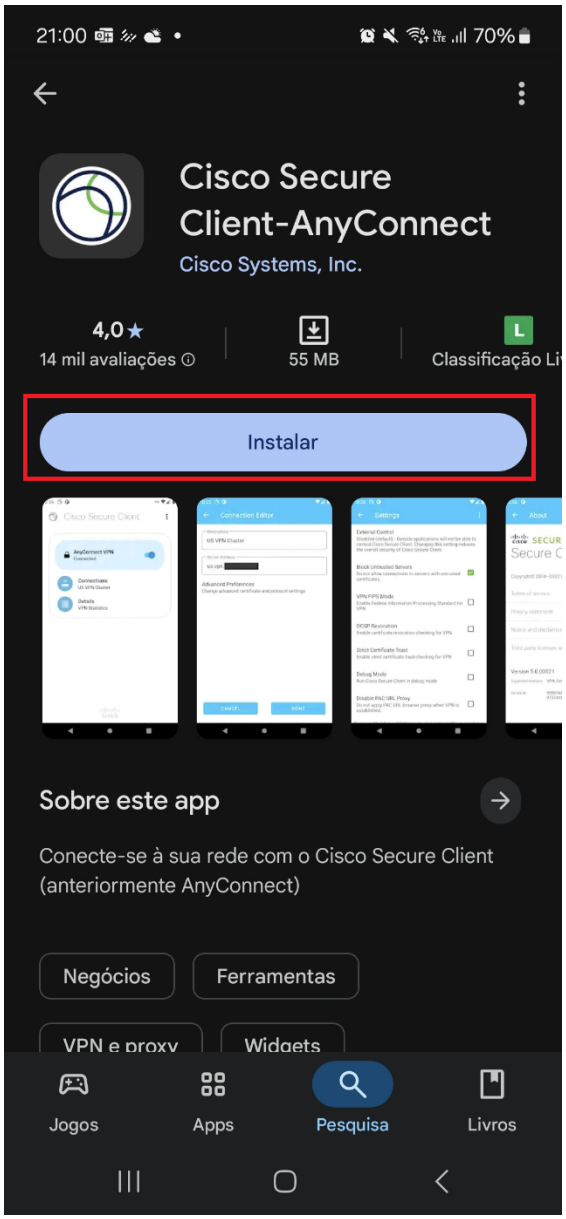


Uma vez autenticado no portal do SisCAU, o usuário estará conectado com sucesso à EBNet:

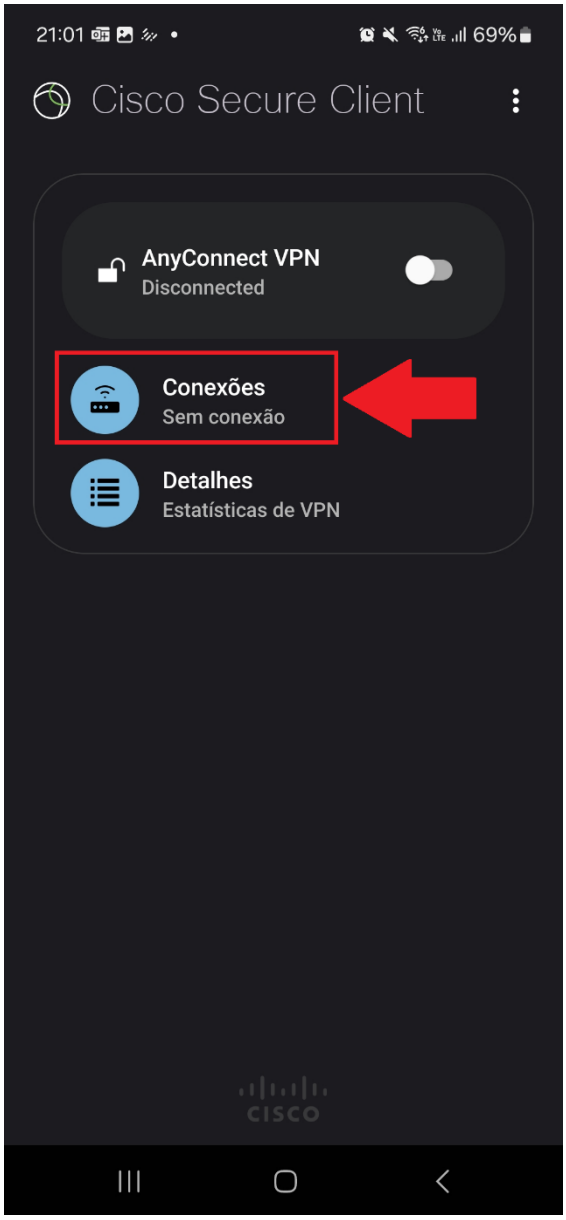


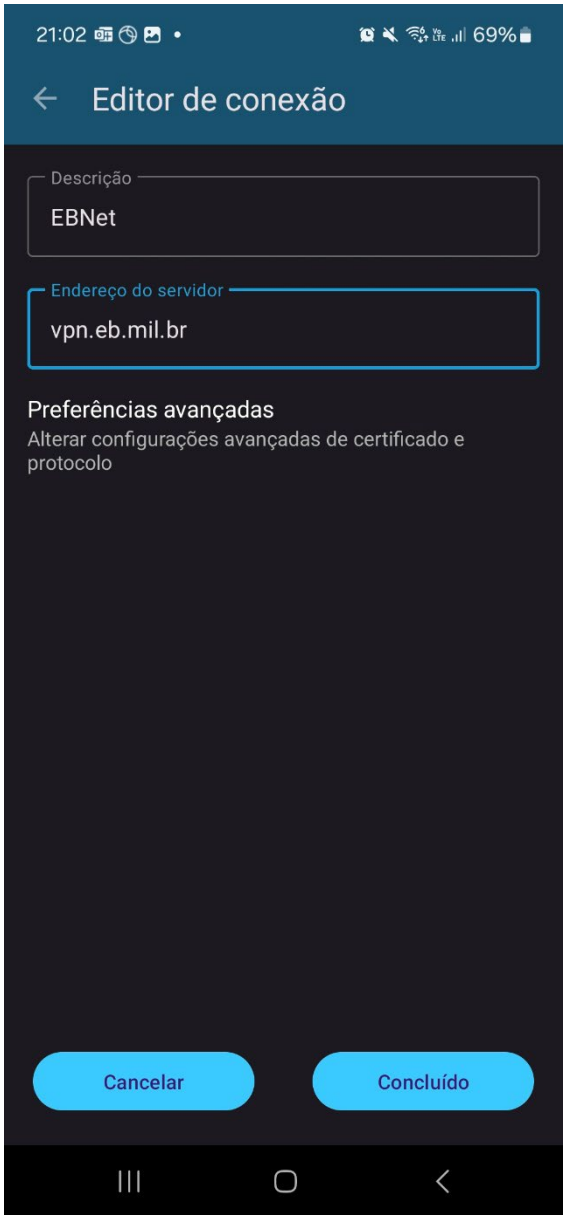
8.2 Instalação e configuração do cliente VPN em dispositivos móveis (Android e iOS)

O cliente VPN da Cisco encontra-se disponível nas respectivas lojas de aplicativos do Android e do iOS (Google Play Store e Apple App Store respectivamente). Na loja de *apps* correspondente ao seu dispositivo móvel, procure por "Cisco Secure Client" e instale o aplicativo:

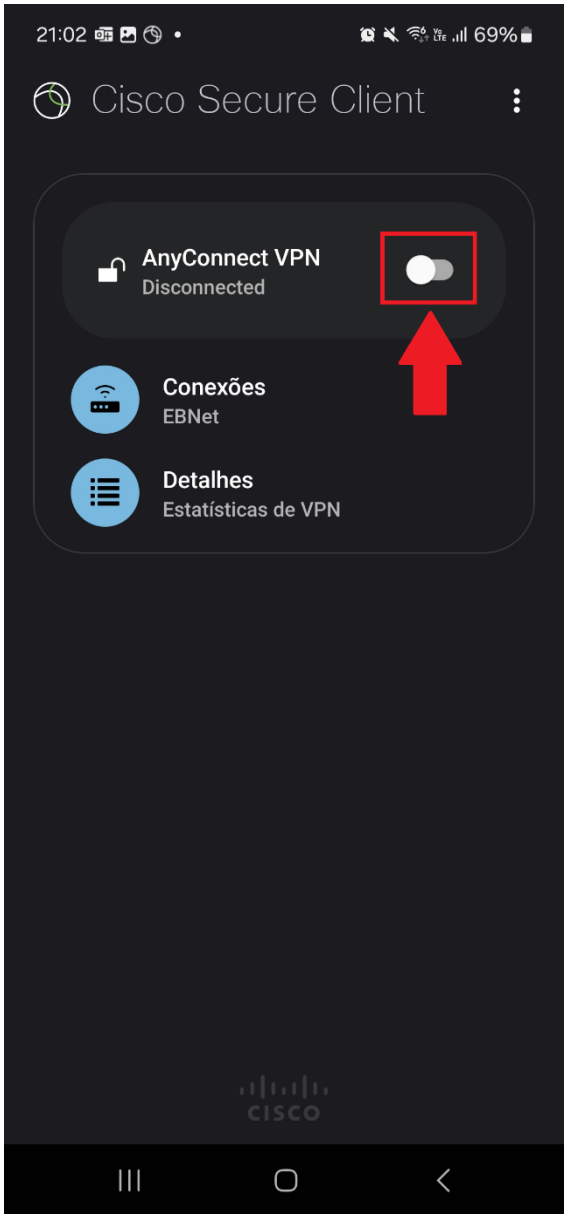


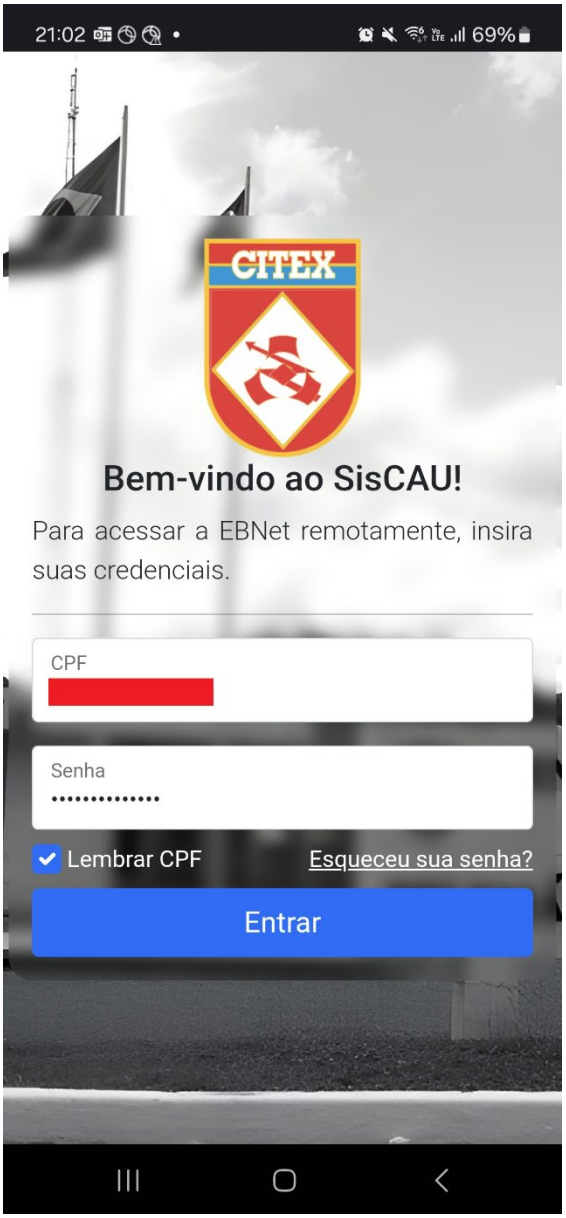
Clique em conexões e adicione uma nova conexão. Em descrição, insira um nome de sua preferência e em “endereço do servidor” insira “vpn.eb.mil.br”:



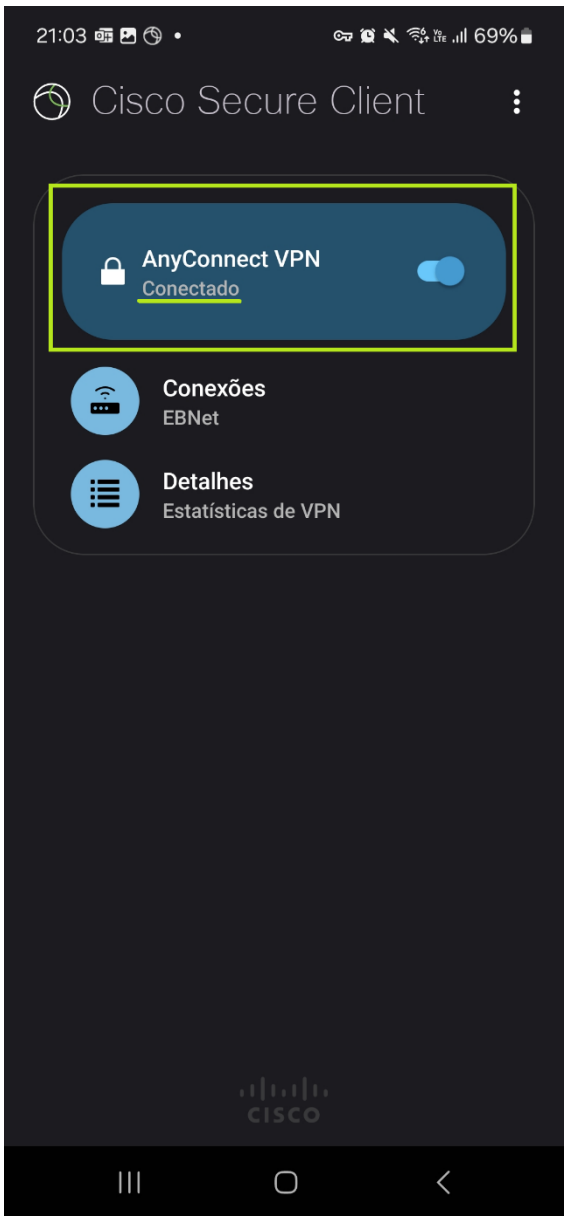


Para estabelecer uma conexão remota com a EBNet, basta clicar no botão em destaque na imagem a seguir. O cliente VPN redirecionará o usuário para o portal de autenticação do SisCAU:





Concluída a autenticação no SisCAU com sucesso, a conexão VPN será estabelecida:



8.3 Problemas comuns no acesso remoto (VPN)

8.3.1 Conta sem permissão de acesso remoto (VPN)

É possível que ao tentar estabelecer uma conexão VPN a seguinte mensagem seja exibida:



Nesse caso, entre em contato com os gestores do SisCAU em sua OM e solicite que sua conta seja adicionada a um **Grupo de Acesso Remoto**.

Anexo A – Perfis de Acesso

	Comandante (61)	Com Soc (51)	Jur/SALC (41)	TI (31)	Intlg (21)	Padrão (11)	Limitado (01)	Noturno (71)
Sites governamentais	✓	✓	✓	✓	✓	✓	✓	✓
Atualização de *softwares*	✗	✗	✗	✓	✗	✗	✗	✓
Armazenamento em nuvem	✓	✓	✓	✗	✓	✓	✗	✓
VPN/Anonimizador	✗	✗	✗	✗	✗	✗	✗	✗
Redes Sociais	✓	✓	✗	✗	✓	✗	✗	✓
YouTube	✓	✓	✓	✓	✓	✓	✗	✓
Plataformas de *Streaming*	✓	✗	✗	✗	✗	✗	✗	✓
Hacking	✗	✗	✗	✓	✓	✗	✗	✗
Sites sobre concursos públicos	✓	✓	✓	✓	✓	✗	✗	✓
Download de executáveis	✗	✗	✗	✓	✓	✗	✗	✗