

Cliente Citrix Secure Access para dispositivos Android

O cliente Citrix Secure Access para Android fornece a melhor solução de acesso a aplicativos e proteção de dados da categoria, oferecida pelo NetScaler Gateway. Agora você pode acessar com segurança aplicativos críticos de negócios, desktops virtuais e dados corporativos de qualquer lugar a qualquer momento.

Observações:

- A partir da versão 23.12.1, o Citrix SSO para Android foi renomeado para Citrix Secure Access. Estamos atualizando nossa documentação e as capturas de tela da interface do usuário para refletir essa mudança de nome.
- Para obter instruções específicas do administrador sobre o Citrix Secure Access para Android, consulte [Citrix Secure Access para dispositivos Android](#).

Como usar o Citrix Secure Access no seu dispositivo Android

Instale o Citrix Secure Access na sua Play Store. Usuários iniciantes devem criar uma conexão com o NetScaler Gateway adicionando o servidor no caso não-MDM. Para usos subsequentes, você pode se conectar a uma conexão existente ou adicionar uma conexão, e também editar conexões existentes, se permitido pelo seu administrador em uma implantação MDM. Você também pode visualizar os logs e tomar as ações apropriadas de acordo.

Notas:

- Conexões implantadas via MDM não podem ser editadas.
- Você pode ser solicitado a conceder o consentimento [Consultar todos os pacotes](#) ao aplicativo Citrix Secure Access. Uma vez concedido o consentimento, o aplicativo Citrix Secure Access:

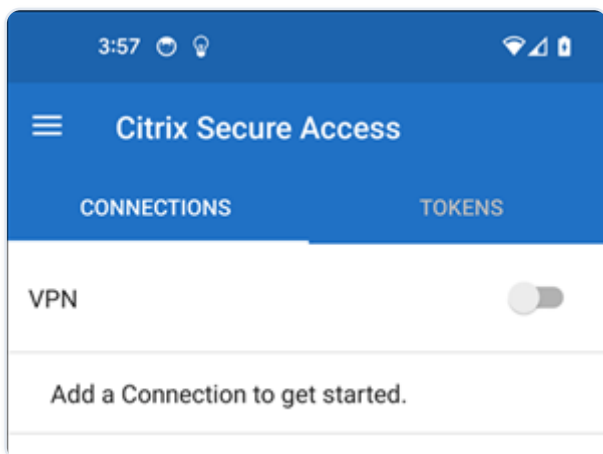
- Recebe a notificação de instalação do pacote do sistema operacional.
- Reinicia a VPN Always On.

Ao se conectar ao seu perfil VPN pela primeira vez, você será solicitado a fornecer consentimento (exigido pelas políticas do Google) para coletar informações sobre o pacote instalado. Se você conceder o consentimento, a conexão VPN será iniciada. Se você negar o consentimento, a conexão VPN será abortada. A tela de consentimento não reaparecerá uma vez que o consentimento tenha sido concedido.

Adicionar uma conexão

Observação: Esta etapa é necessária apenas em um caso não-MDM.

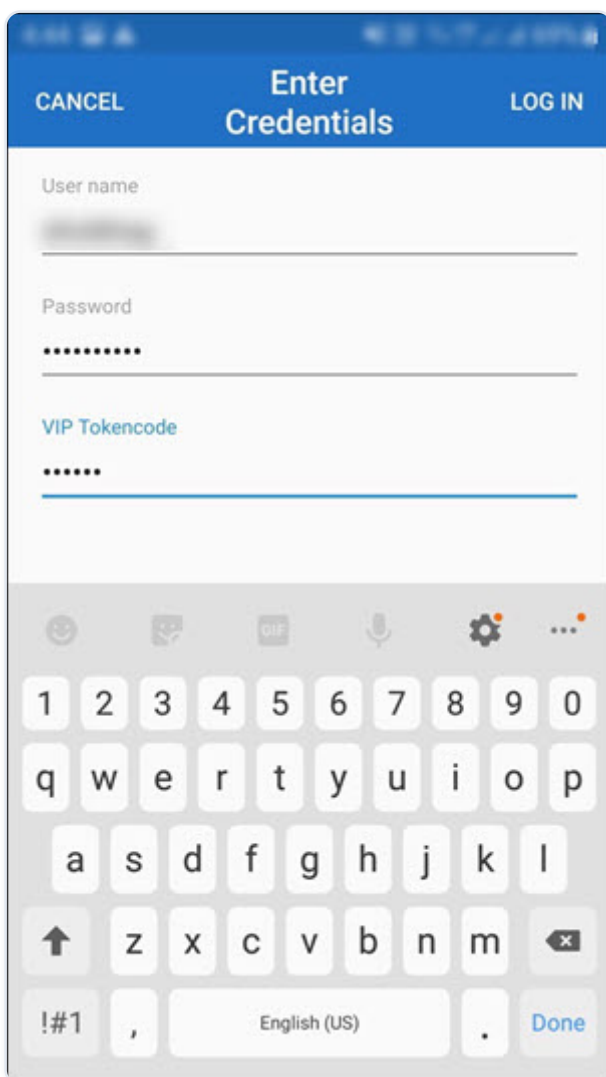
Depois de instalar o Citrix Secure Access e abrir o aplicativo no seu dispositivo Android, a seguinte tela aparece.



1. Clique em + para adicionar uma conexão.
2. Insira a URL base (por exemplo, [Minha empresa](#)) e o nome para a conexão VPN. Opcionalmente, você pode inserir o nome de usuário.
3. Clique em **Salvar** e depois em **Salvar e Conectar** ou **Apenas Salvar**, conforme apropriado.

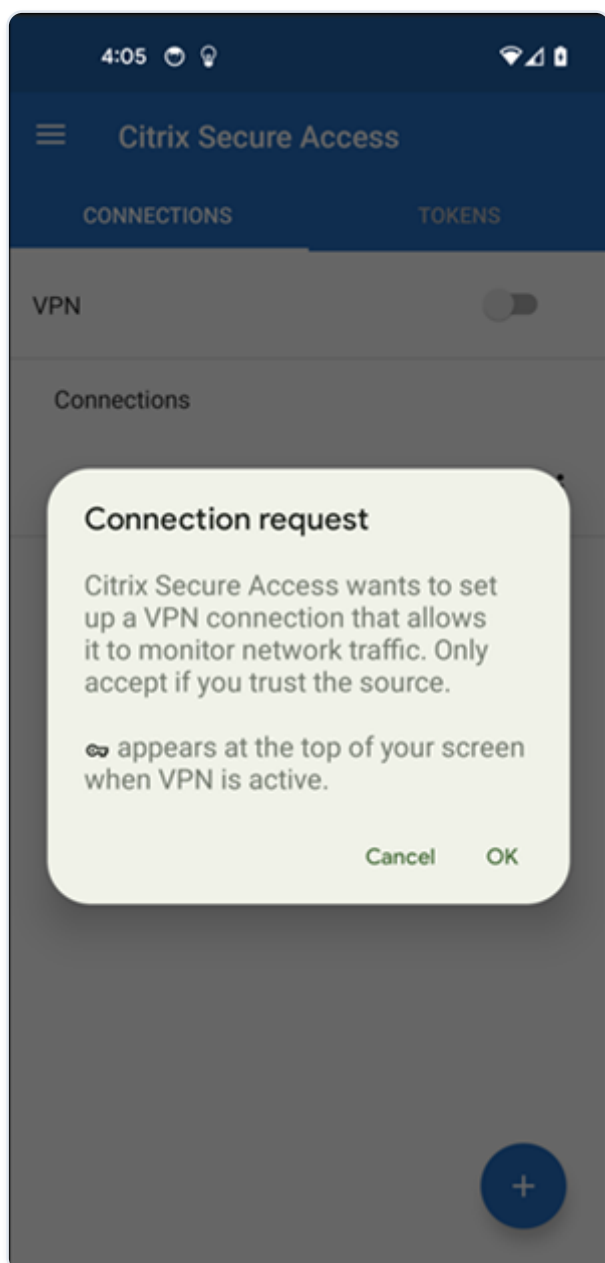
The screenshot shows the 'Add Connection' screen in the Citrix Secure Access mobile app. The interface includes a blue header bar with 'CANCEL', 'Add Connection', and 'SAVE' buttons. Below the header, there are three input fields labeled 'Server', 'Description', and 'User Name'. At the bottom of the screen, there are three buttons: 'Save and Connect', 'Just Save', and 'Cancel'. Red boxes highlight the 'SAVE' button in the header and the 'Save and Connect' and 'Just Save' buttons at the bottom.

4. Forneça as credenciais de autenticação para o seu servidor e toque em **LOG IN** ou **Done** no teclado.

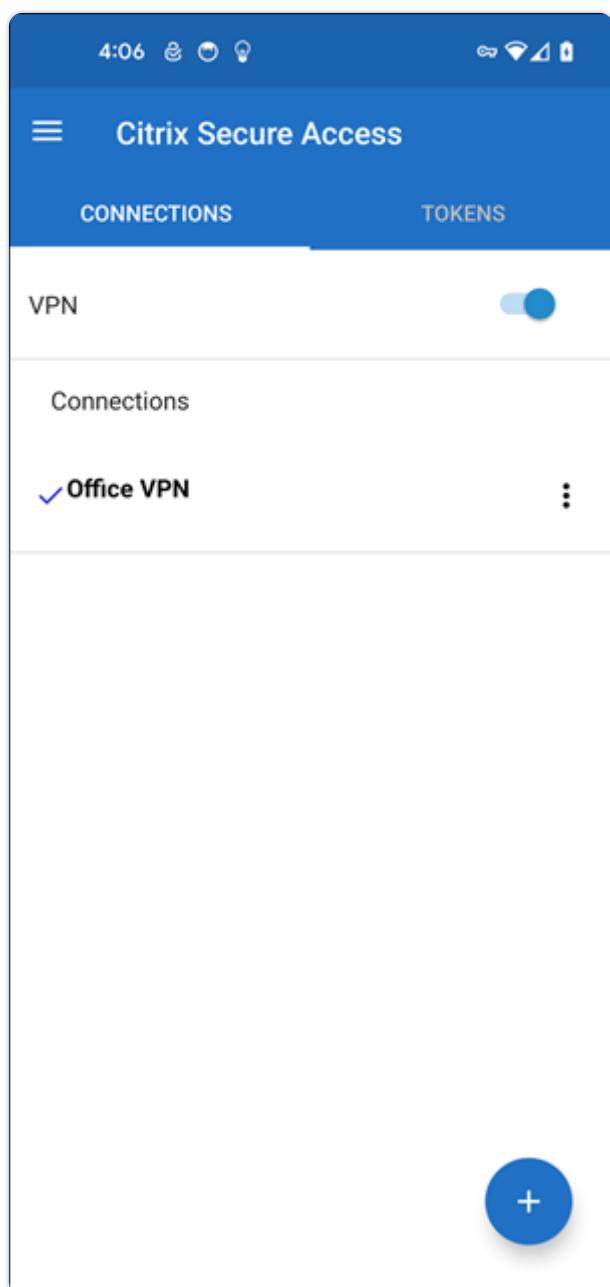


A mensagem de solicitação de conexão é exibida. Clique em **OK**.

Nota: Esta mensagem aparece apenas na primeira vez que qualquer conexão VPN é estabelecida pelo Citrix Secure Access. Se o usuário permitir a conexão pela primeira vez, esta mensagem não será exibida novamente até que o usuário desinstale e reinstale o aplicativo.



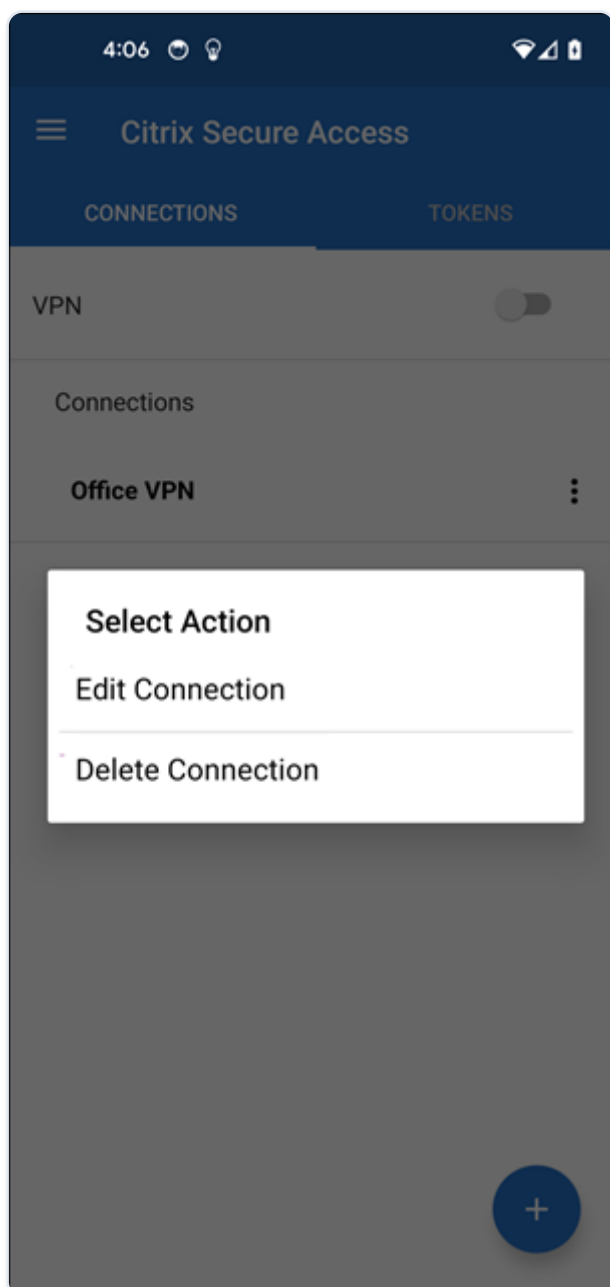
Nota: Para sair do Citrix Secure Access, desative o **VPN switch**.



Modificar ou excluir uma conexão existente

Você pode editar ou excluir uma conexão depois de sair do Citrix Secure Access.

Toque e segure o nome do servidor e selecione **Editar Conexão** ou **Excluir Conexão**.

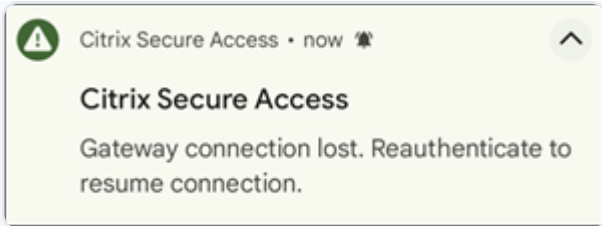


Reconectar ao NetScaler Gateway após uma falha de conexão VPN - Visualização

O cliente Citrix Secure Access para Android solicita que você se reautentique com o NetScaler Gateway quando uma conexão VPN é perdida. Você é notificado na interface do usuário e no painel de notificações do seu dispositivo Android, indicando que a conexão com o NetScaler Gateway foi perdida e que você deve se reautenticar para retomar a conexão.

Nota:

Este recurso está em pré-visualização.



Permitir permissão de acesso à rede local no Android 17 e posterior

A partir do Citrix Secure Access para Android versão 26.08.1, os usuários que instalam, reinstalam ou atualizam o aplicativo no Android 17 e posterior são solicitados a permitir o acesso à rede local. Se o acesso for negado, certos serviços de rede local, como impressoras Wi-Fi, podem ficar indisponíveis quando uma sessão VPN é iniciada.

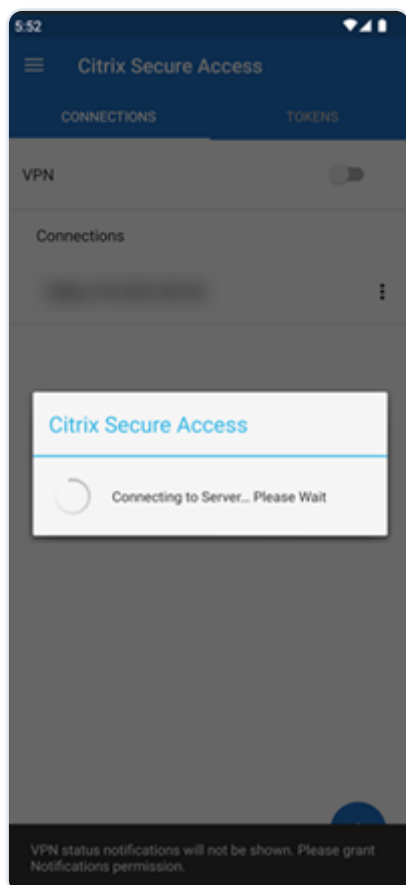
Os administradores de MDM são aconselhados a pré-conceder esta permissão ao aplicativo Citrix Secure Access.

Receber ou bloquear notificações no Android 13 e posterior

A partir do Citrix Secure Access para Android versão 23.12.1, os usuários que instalam, reinstalam ou atualizam o aplicativo no Android 13 e posterior são solicitados a permitir notificações. Se as notificações forem negadas, os usuários não receberão o status da VPN ou notificações push do Citrix Secure Access.

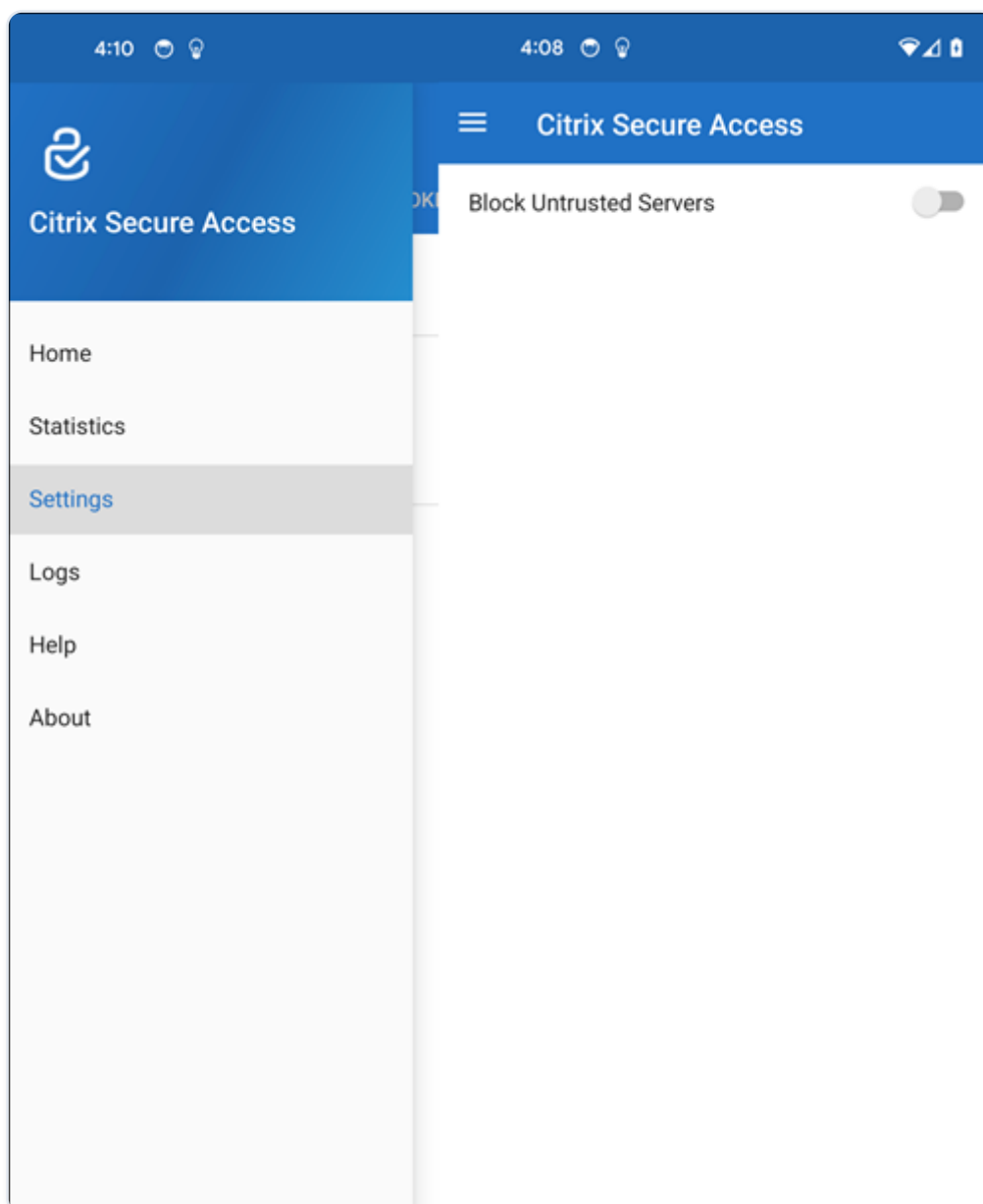
Você pode navegar para **Configurações > Notificações** no seu dispositivo Android para alterar as permissões de notificação.

No exemplo a seguir, as notificações de status da VPN foram desativadas.



Bloquear servidores não confiáveis

Por padrão, o Citrix Secure Access não se conecta a servidores não confiáveis. Servidores não confiáveis referem-se a servidores que usam certificados autoassinados ou que não possuem um certificado raiz confiável para o gateway. Para permitir esses tipos de conexões, você pode desativar o interruptor **Bloquear Servidores Não Confiáveis** e colocá-lo em **DESLIGADO**.



Ativar logs de depuração

A captura de logs de depuração é uma parte crítica da solução de problemas ou do relato de problemas ao Suporte Citrix. Toque no interruptor **Registro de Depuração** para **LIGAR** o registro de depuração para o Citrix Secure Access. Você pode enviar os logs por e-mail ao solucionar problemas de conexão usando o link **Enviar Logs por E-mail**.

Exibir logs de depuração(/en-us/citrix-sso/media/sso-andr-logs.png)

Exibir estatísticas

Você pode visualizar as estatísticas de conexão quando a VPN estiver conectada.

Exibir estatísticas de conexão(/en-us/citrix-sso/media/sso-andr-stats.png)

Tokens de senha

Você pode adicionar um token de senha de 6 dígitos como um segundo fator de autenticação. Este código usa o protocolo de senha de uso único baseada em tempo para gerar o código OTP.

Você pode adicionar um token de senha manualmente ou registrar um token de senha usando o método de leitura de código QR. A autenticação de segundo fator usando notificações push não é ativada se você optar por inserir o token manualmente.

Registrar um token de senha

1. Faça login na página de gerenciamento de PIN de uso único da sua organização no seu navegador da web em um desktop ou laptop.
2. Clique em **Adicionar Dispositivo**.
3. Insira um nome para o seu dispositivo e clique em **Ir**.

Um código QR é gerado.

Adicionar um token de senha digitalizando o código QR no navegador

1. Navegar para a guia **Tokens** na visualização **Início**.
2. Toque em **+** e toque em **Digitalizar Código QR**.
3. Foque a câmera no código QR no seu navegador.

O Citrix Secure Access preenche automaticamente o nome do dispositivo e a chave secreta.

Alternativamente, você pode inserir manualmente a chave secreta que aparece acima do código QR.

O Citrix Secure Access valida o código QR e, em seguida, se registra no gateway para notificações push. Se não houver erros no processo de registro, o token será adicionado com sucesso à guia de tokens.

Nota:

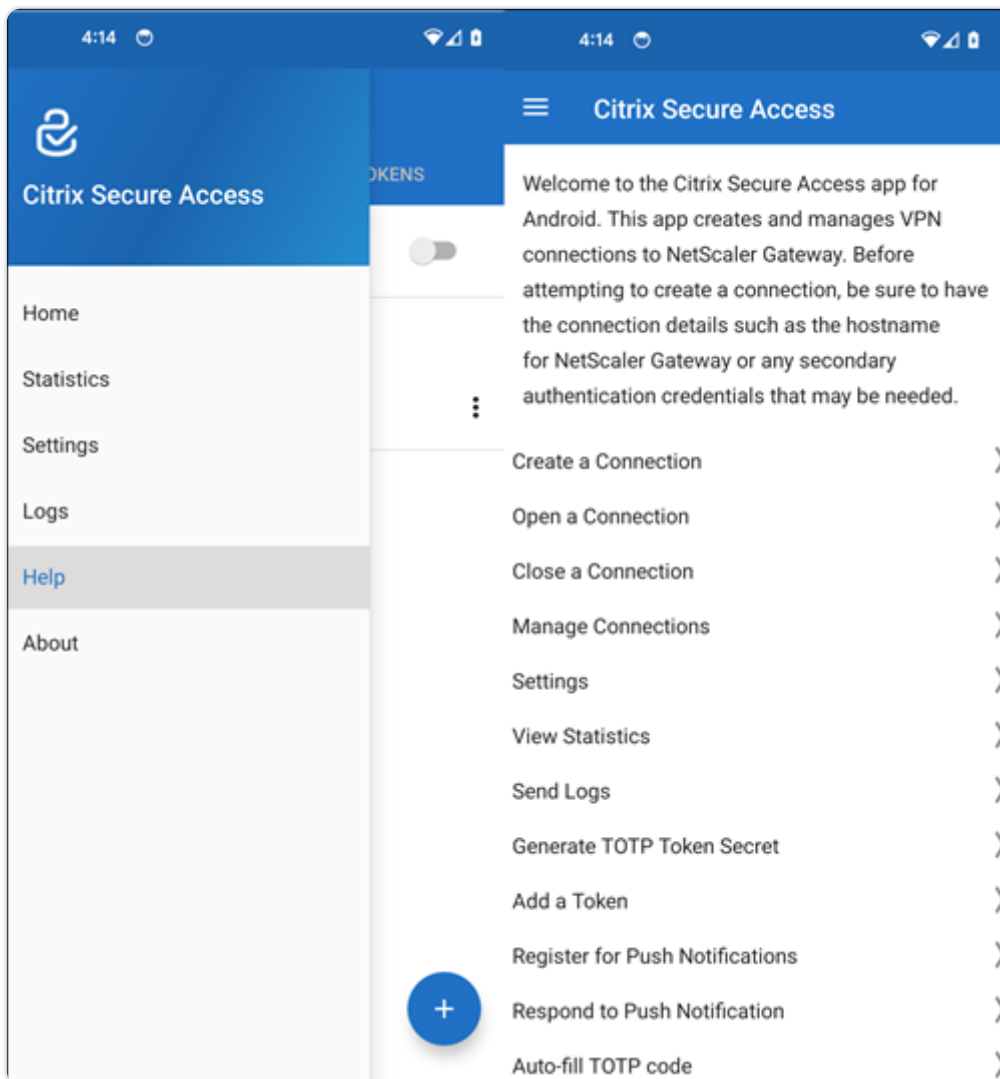
- Você deve permitir as permissões da câmera para que o Citrix Secure Access capture o código QR.
- Você deve habilitar o PIN/senha do dispositivo no seu aparelho.

Adicionar um token de senha manualmente

1. navegar para a guia **Tokens** na visualização **Home**.
2. Toque em + e toque em **Inserir Manualmente**.
3. Insira o nome do dispositivo e a chave secreta conforme aparecem no token de senha gerado no navegador.

Tópicos de ajuda

Para obter mais informações sobre como usar o Citrix Secure Access, consulte **Ajuda**.



Conecte-se à sua rede corporativa usando o Citrix Secure Access configurado em um ambiente Intune

Nota:

Para instruções específicas do administrador sobre o Citrix Secure Access para Android, consulte [Citrix Secure Access para dispositivos Android](#).

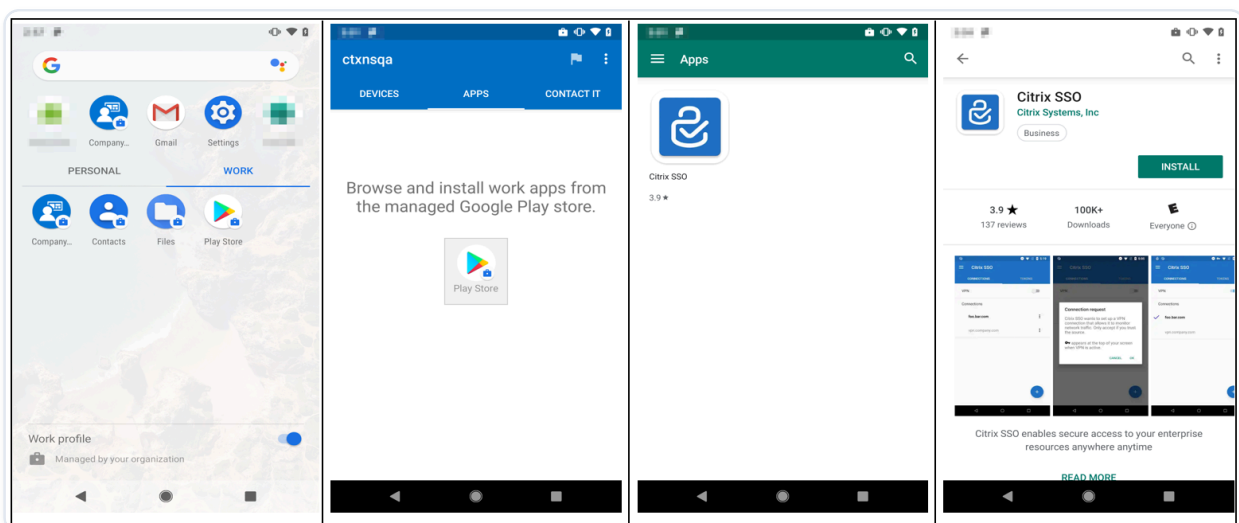
Este tópico detalha como se conectar à sua rede corporativa usando o cliente Citrix Secure Access configurado no ambiente Microsoft Intune Android Enterprise.

Suposições:

- Você registrou o dispositivo no Intune usando o aplicativo Intune Company Portal.
- O perfil de trabalho para o usuário está configurado no dispositivo.

1. Abra o aplicativo **Intune Company Portal** no dispositivo a partir do perfil de trabalho.
2. Clique no menu de três pontos para abrir as configurações do aplicativo e role até a parte inferior da tela. Toque em **SYNC** para sincronizar com o servidor Intune e, em seguida, navegar para a tela principal do aplicativo.
3. Toque na guia **APPS** e toque no link **Managed Google Play Store**.

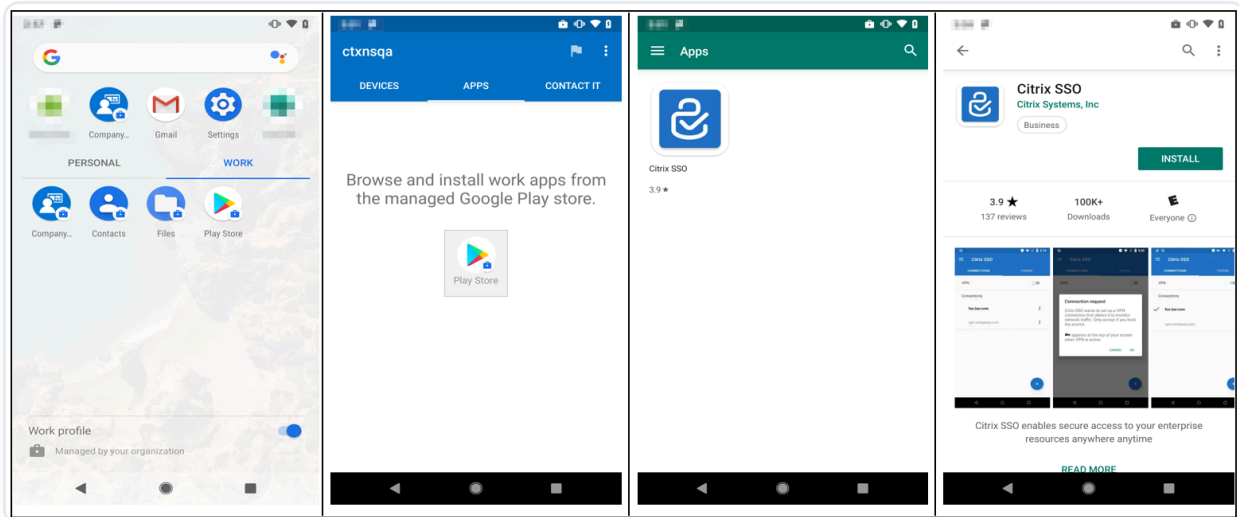
A lista de aplicativos aprovados para o usuário aparece.



4. Toque em **Citrix Secure Access**.

O cliente Citrix Secure Access aparece na loja Managed Google Play.

5. Toque em **INSTALAR**.
6. navegar de volta à lista de aplicativos do perfil de trabalho. O Citrix Secure Access é adicionado à lista de aplicativos instalados.
7. Toque no ícone do Citrix Secure Access na lista de aplicativos do perfil **TRABALHO** para abri-lo.



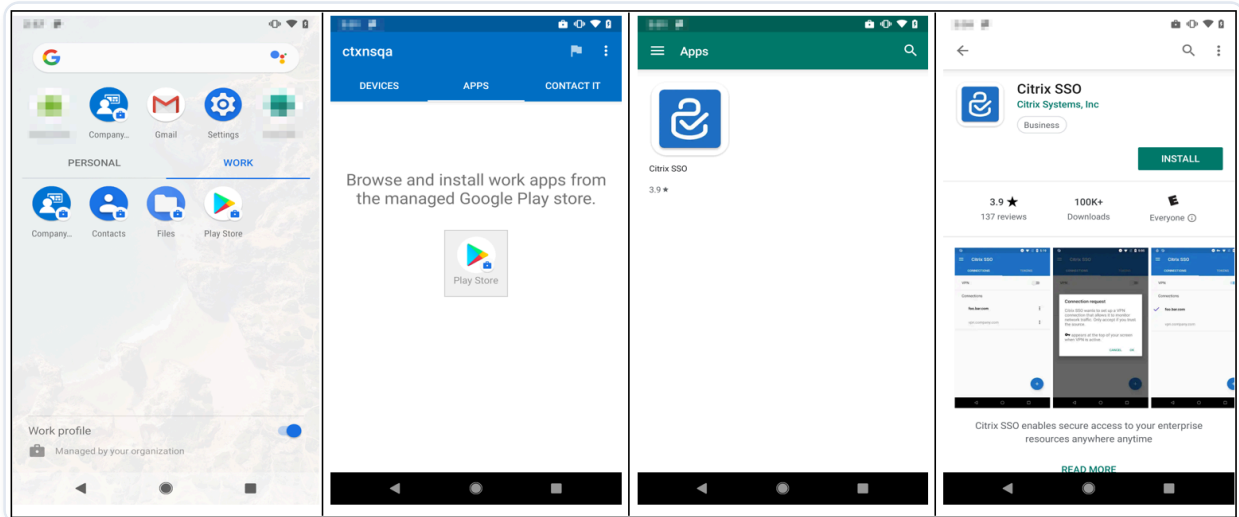
O Citrix Secure Access é aberto. Você será solicitado a permitir ou não a permissão para se comunicar de forma segura com a rede interna da sua empresa.

8. Toque em **PERMITIR** para conceder a permissão. O Citrix Secure Access será fechado se você escolher **NÃO PERMITIR** e você não poderá usar o cliente Citrix Secure Access.

Observação:

Você pode ser solicitado a permitir ou negar a **permissão para gerenciar e fazer chamadas telefônicas** (se ainda não tiver sido concedida via Intune). Toque em **Permitir** para conceder a permissão. Você pode negar essa permissão, mas se a verificação NAC do Intune for necessária para a autenticação do dispositivo no NetScaler Gateway, você não poderá se conectar à rede interna da sua empresa até conceder essa permissão.

9. O **My Corporate VPN** (ou o nome que você escolheu na configuração do Citrix Secure Access no Intune) é listado na seção Conexões Gerenciadas da guia **CONEXÕES**. Toque nesta conexão, você será solicitado a fornecer as credenciais para autenticar com o NetScaler Gateway.
10. Forneça as credenciais para autenticação com o NetScaler Gateway e toque em **FAZER LOGIN**.



Você pode ser solicitado a selecionar um certificado se a autenticação por certificado de cliente estiver configurada no NetScaler Gateway. Você pode fornecer acesso ao certificado.

11. O sistema Android solicitará que você permita a **Solicitação de conexão** para a configuração do túnel VPN. Toque em **OK** para conceder ao Citrix Secure Access permissão para estabelecer uma conexão segura com a rede interna da sua empresa.

Observação: Este prompt é exibido apenas quando você estabelece uma conexão segura com o NetScaler Gateway pela primeira vez. Ele não é exibido para tentativas de conexão subsequentes até que o Citrix Secure Access seja desinstalado e instalado novamente no dispositivo.

Você está conectado à rede interna da sua empresa. Um ícone de chave aparece na barra de status do dispositivo, notificando que a conexão VPN está ativa. O ícone de notificação do serviço VPN do cliente Citrix Secure Access também aparece na barra de status. O botão de conexão muda seu estado para conectado e um ícone de marca de seleção aparece ao lado do nome do perfil VPN.

Cliente Citrix Secure Access para dispositivos iOS

O cliente Citrix Secure Access para iOS oferece a melhor solução de acesso a aplicativos e proteção de dados da categoria, fornecida pelo NetScaler Gateway. Agora você pode acessar com segurança aplicativos críticos de negócios, desktops virtuais e dados corporativos de qualquer lugar a qualquer momento.

O aplicativo Citrix Secure Access oferece suporte completo a Mobile Device Management (MDM) no iOS. Com um servidor MDM, um administrador agora pode configurar e gerenciar remotamente perfis VPN de nível de dispositivo e perfis VPN por aplicativo.

Importante:

- A partir da versão 23.11.1, o Citrix SSO para iOS foi renomeado para Citrix Secure Access. Estamos atualizando nossa documentação e as capturas de tela da interface do usuário para refletir essa mudança de nome.
- Para instruções específicas do administrador sobre o Citrix Secure Access para iOS, consulte [Citrix SSO para iOS e Citrix Secure Access para macOS](#).

Importar e instalar certificados no aplicativo Citrix Secure Access

O Citrix Secure Access no iOS oferece suporte à autenticação de certificado de cliente com o NetScaler Gateway. Os certificados podem ser entregues ao Citrix Secure Access das seguintes maneiras:

- **Servidor MDM** - Abordagem preferencial para clientes MDM. Os certificados são configurados diretamente no perfil VPN gerenciado por MDM. Ambos os perfis VPN e os certificados são então enviados para os dispositivos registrados quando o dispositivo se registra no servidor MDM. Siga os documentos específicos do fornecedor MDM para esta abordagem.

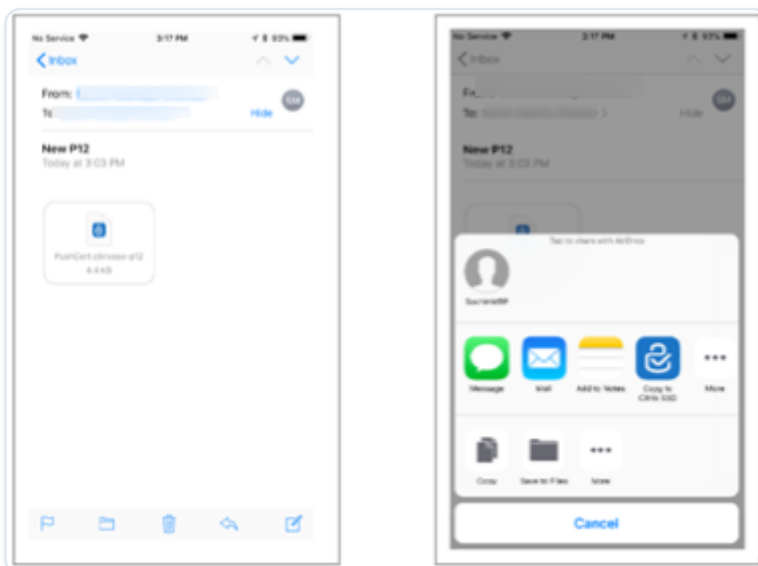
- **E-mail** - Única abordagem para clientes não-MDM. Os administradores enviam um e-mail com a identidade do Certificado do Usuário (Certificado e chave privada) anexada como um arquivo PKCS#12 para os usuários. Os usuários devem ter suas contas de e-mail configuradas em seu dispositivo iOS para receber o e-mail com um anexo. O arquivo pode então ser importado para o Citrix Secure Access no iOS.

Nota:

As extensões de nome de arquivo `.pfx` e `.p12` são reivindicadas pelo sistema iOS e não podem ser reivindicadas por aplicativos de terceiros, como o Citrix Secure Access. Portanto, os administradores devem alterar o tipo de Extensão/MIME do certificado do usuário, de `.pfx` ou `.p12` padrão para `.citrixsso-pfx` ou `.citrixsso-p12`, respectivamente.

1. Abra o e-mail com a identidade do certificado do usuário (certificado e chave privada) anexada como um arquivo PKCS#12.

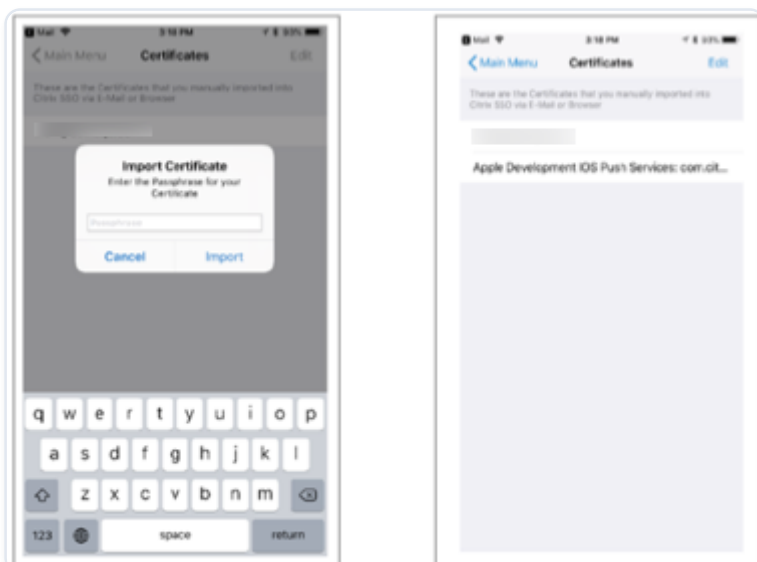
- Toque no anexo para revelar o menu **OpenIn** do sistema.
- Toque em **Copiar para Citrix SSO**.



2. Instale o certificado no Citrix Secure Access.

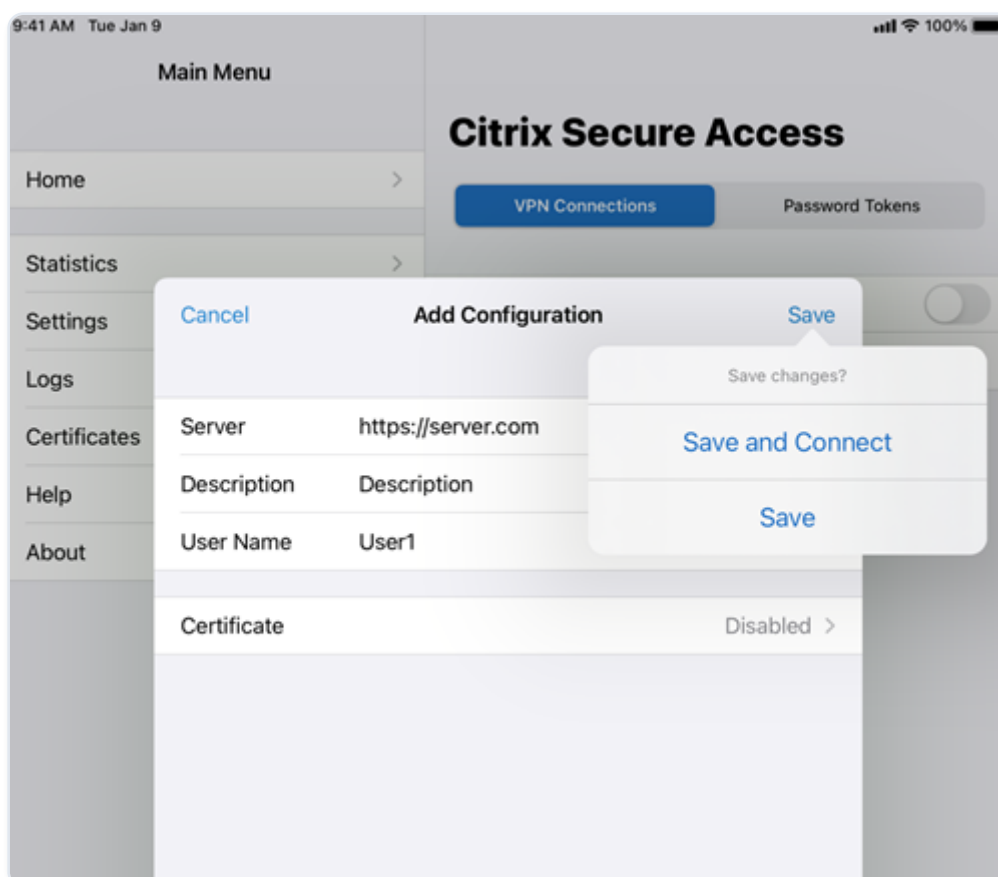
O aplicativo é agora iniciado e um prompt para a senha do certificado é exibido. Digite a senha correta para que o certificado seja instalado no chaveiro do aplicativo e clique em **Importar**.

Após a validação bem-sucedida, o certificado é importado.

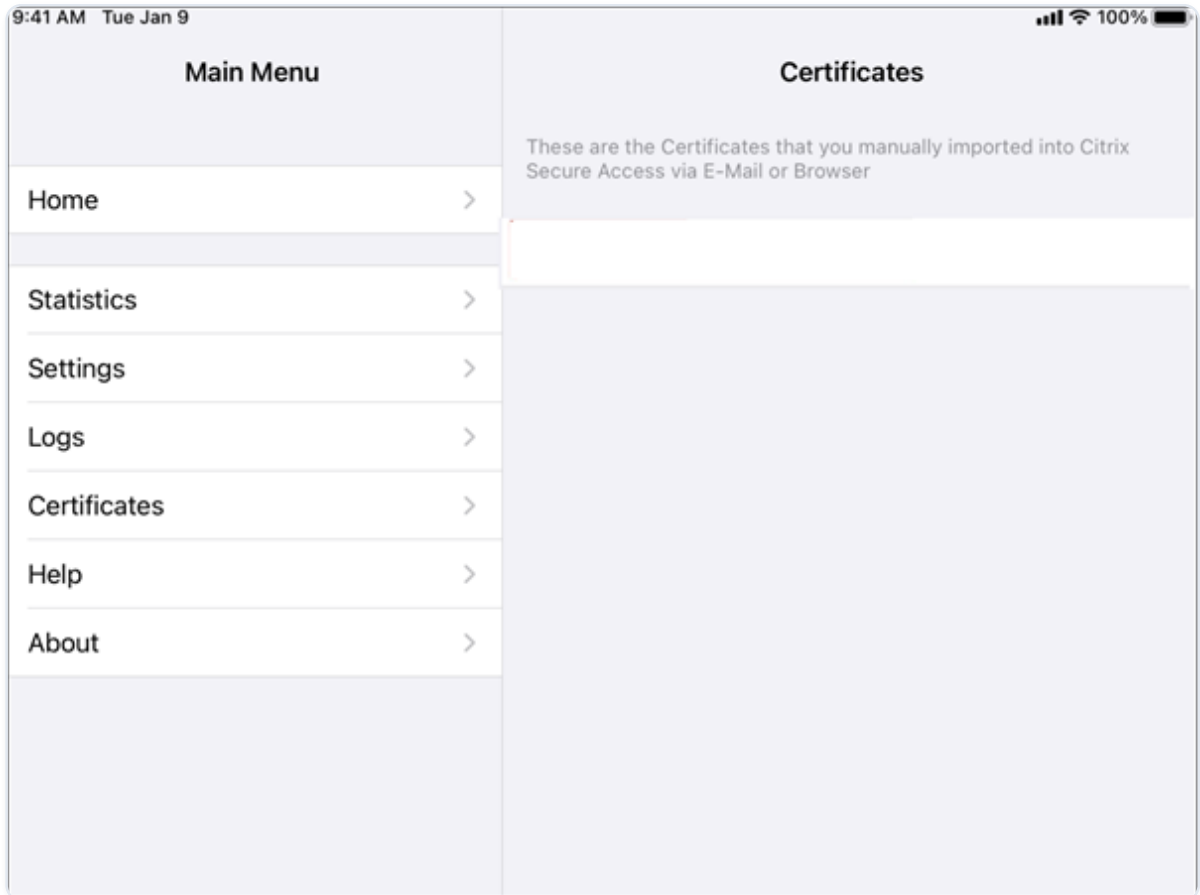


3. Use a autenticação baseada em certificado com VPN.

- Para usar o certificado para autenticação VPN, você deve primeiro criar uma configuração VPN ou um perfil no Citrix Secure Access.
 - navegar para a visualização **Conexões VPN** e toque em **Adicionar Configuração VPN**.
 - Na visualização de configuração do perfil VPN, você pode selecionar o certificado importado na seção **Certificados**.



- Toque em **Salvar** para importar o certificado.



4. Gerenciar certificados.

Para gerenciar os certificados importados para o Citrix Secure Access, navegar para a guia **Certificados** no **Menu Principal**.

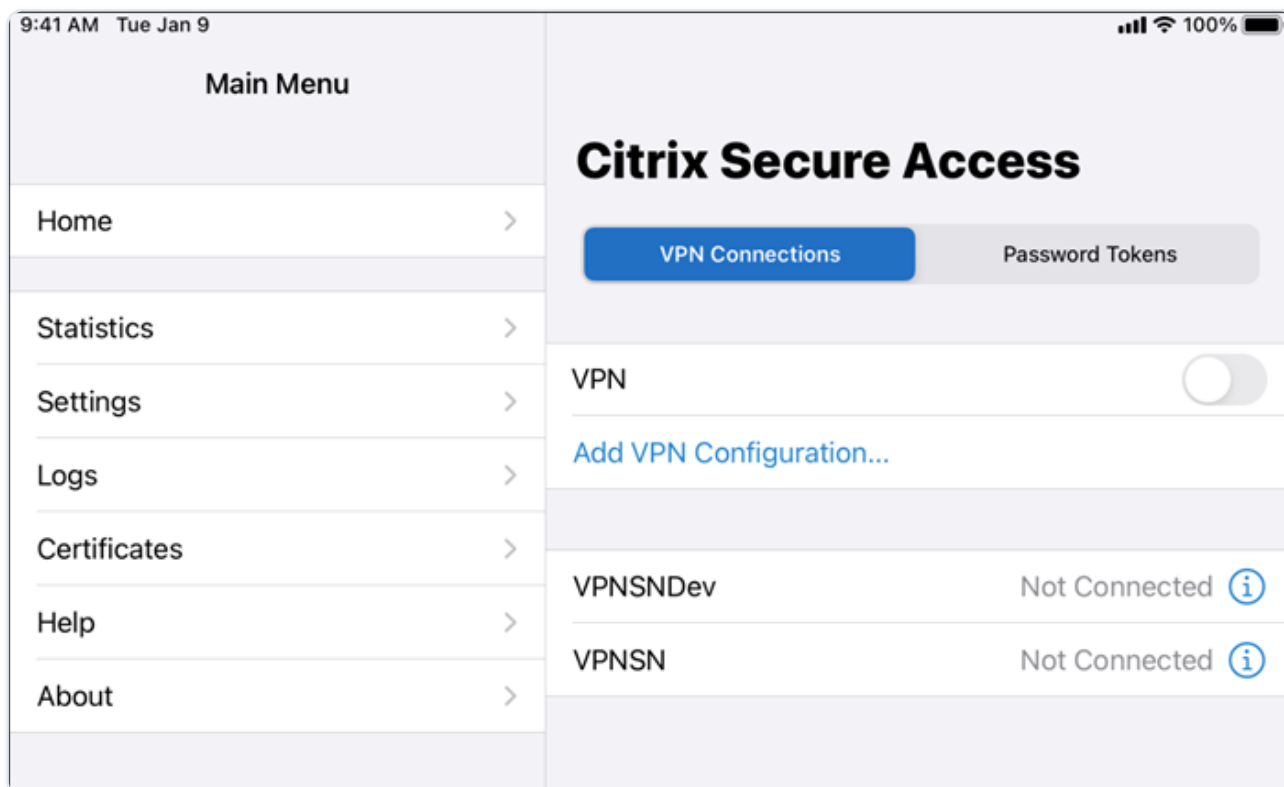
Como usar o Citrix Secure Access no seu dispositivo iOS

Instale o aplicativo Citrix Secure Access na App Store. Após instalar o aplicativo, na primeira vez você deve criar uma conexão com o NetScaler Gateway adicionando o servidor. Para usos subsequentes, você pode se conectar a uma conexão existente ou adicionar uma nova conexão, e também editar conexões existentes. Você também pode visualizar os logs e tomar as ações apropriadas de acordo.

Para clientes MDM, seu administrador pode ter conexões VPN pré-configuradas que aparecem automaticamente quando você registra seu dispositivo. Você pode iniciar as conexões diretamente selecionando a conexão e ativando o interruptor VPN. Essas conexões VPN não são editáveis pelos usuários.

Adicionar uma conexão

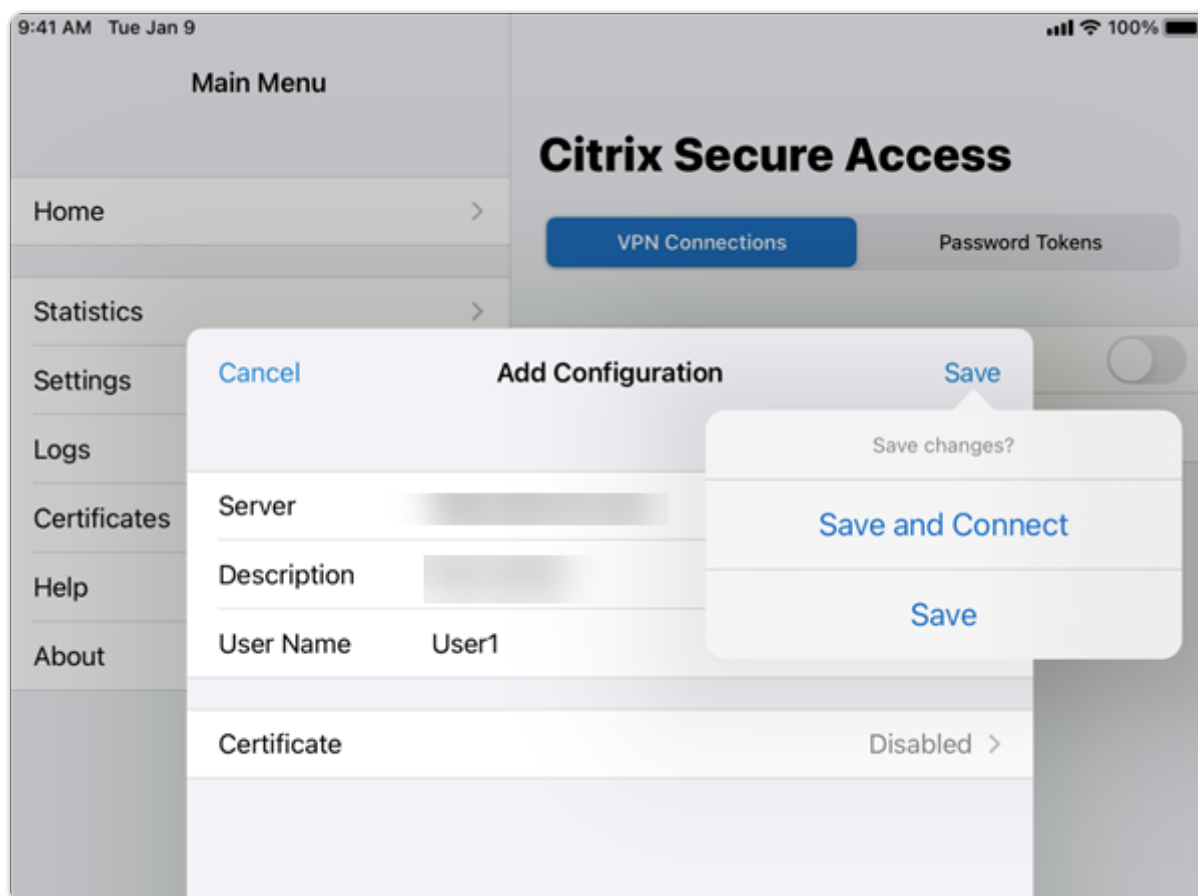
Depois de instalar o Citrix Secure Access e abrir o aplicativo, a seguinte tela aparece.



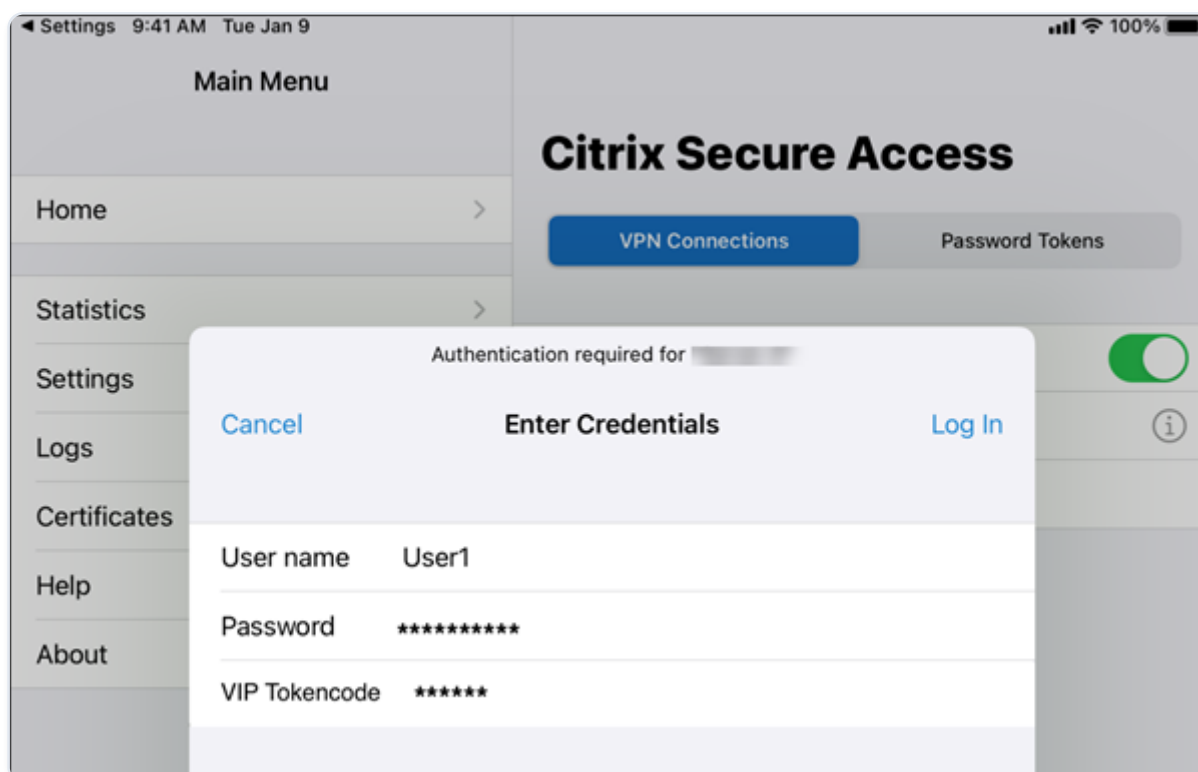
1. Toque em **Adicionar Configuração VPN** para adicionar uma nova conexão.
2. Insira os detalhes do servidor.

Você também pode, opcionalmente, adicionar o nome de usuário.

3. Toque em **Salvar** e, em seguida, toque em **Salvar e Conectar** ou **Salvar**, conforme apropriado.



4. Forneça as credenciais de autenticação para o seu servidor e toque em **Fazer Login**.



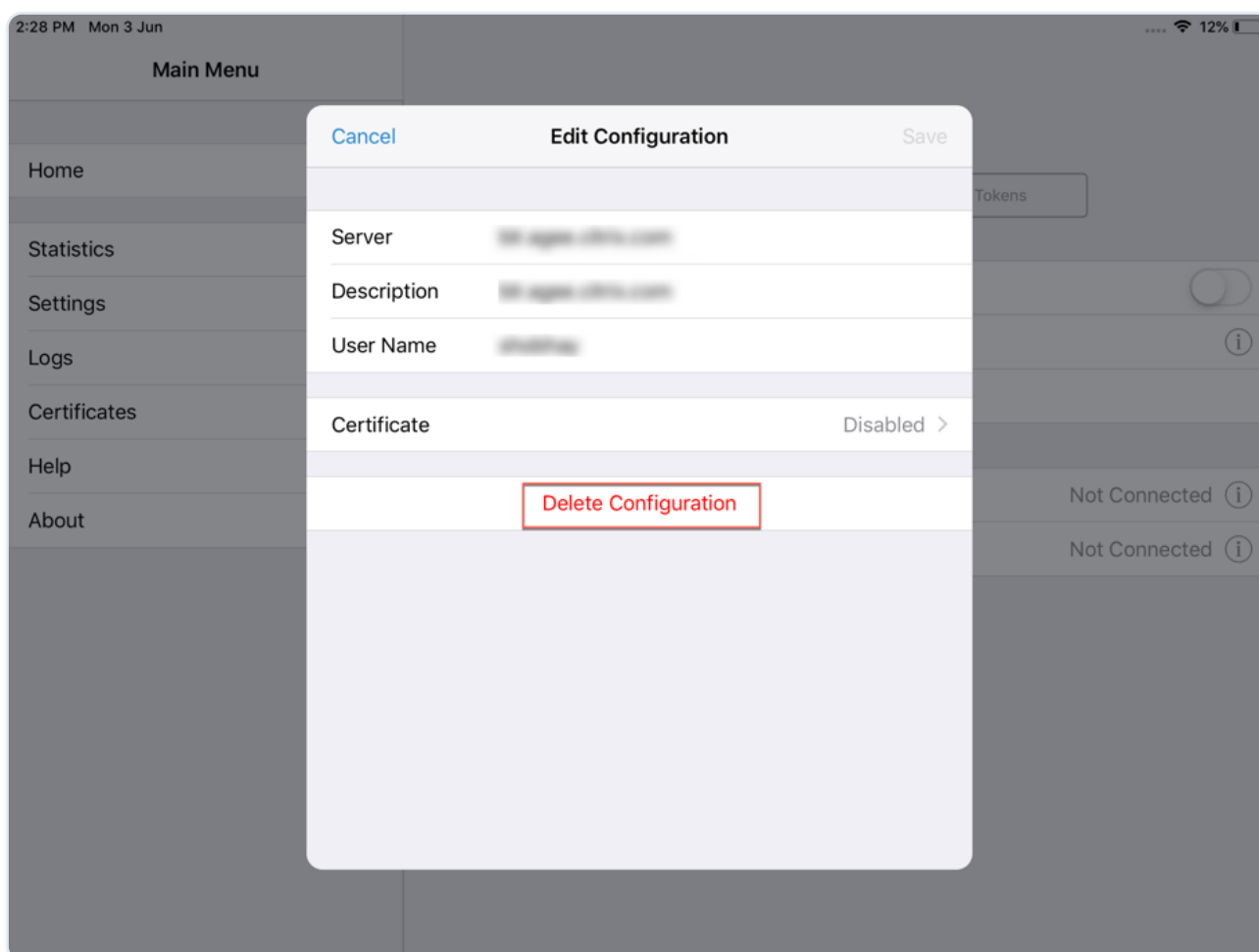
Nota: Para sair do Citrix Secure Access, desative a VPN.

Reconectar ao NetScaler Gateway após uma falha de conexão VPN

O aplicativo Citrix Secure Access para iOS solicita que você se reautentique com o NetScaler Gateway quando uma conexão VPN é perdida. Você é notificado na interface do usuário que a conexão com o NetScaler Gateway foi perdida e que você deve se reautenticar para retomar a conexão.

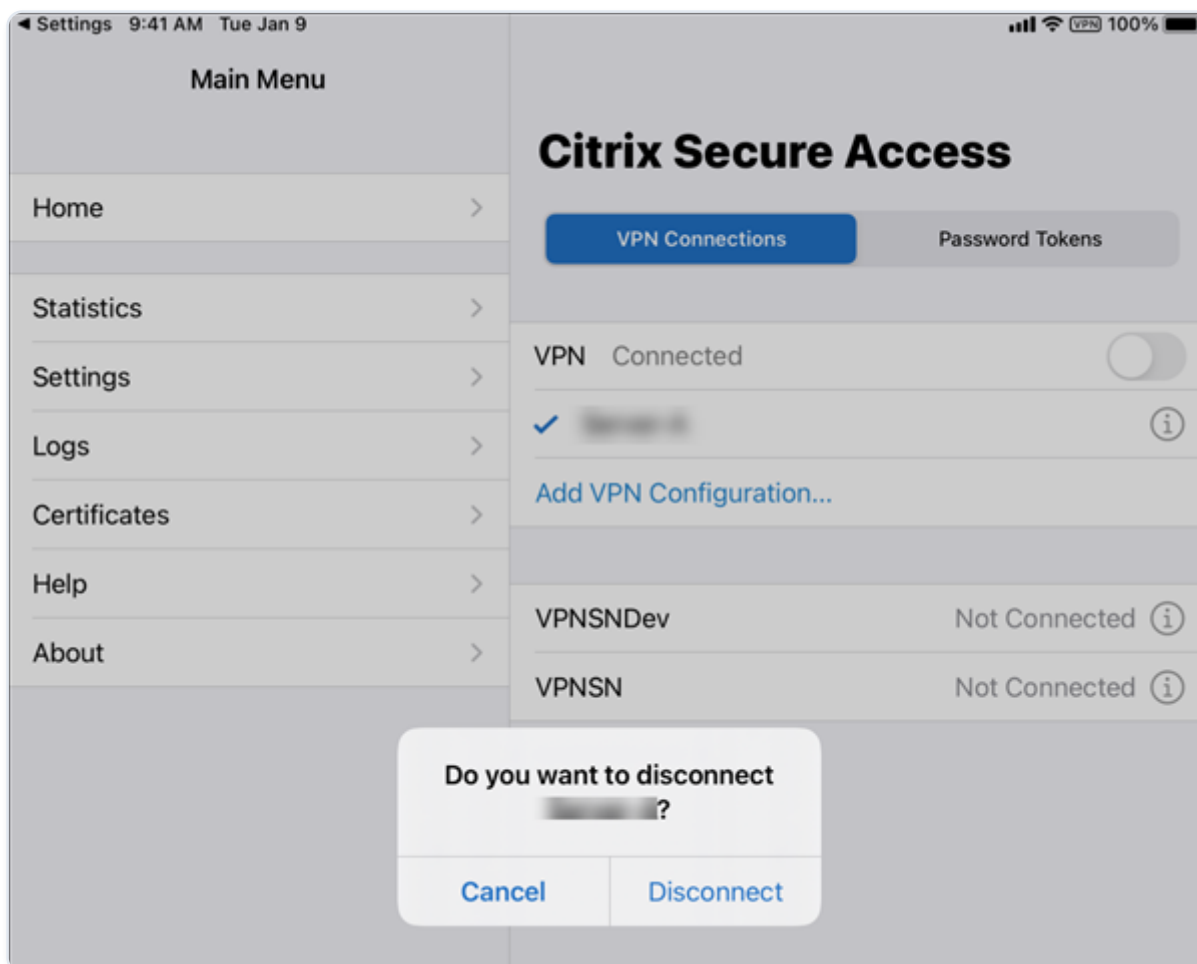
Excluir uma conexão existente

Toque no ícone ao lado da conexão e, em seguida, toque em Excluir Configuração.



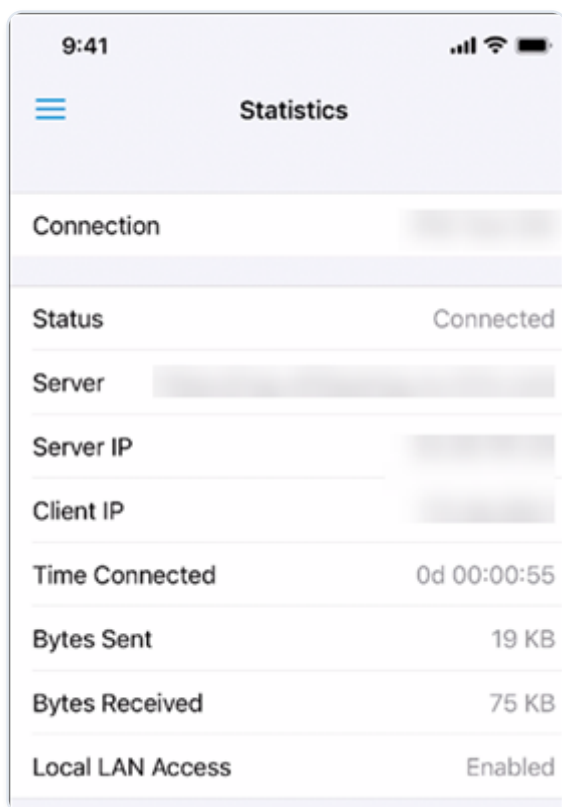
Desconectar uma conexão

Altere o botão VPN para DESLIGADO e, em seguida, toque em Desconectar.



Visualizar estatísticas

Você pode visualizar as estatísticas de conexão quando a VPN estiver conectada.



Bloquear servidores não confiáveis

Por padrão, o Citrix SSO não se conecta a servidores não confiáveis (servidores que usam certificados autoassinados ou que não possuem um certificado raiz confiável para o gateway). Para permitir esses tipos de conexões, você pode desativar a opção Bloquear Servidores Não Confiáveis.

Main Menu	Settings
Home >	Block Untrusted Servers ☒
Statistics >	Allow Local LAN Access ☒
Settings >	
Logs >	
Certificates >	
Help >	
About >	

Acesso à LAN local

O Citrix SSO para iOS 23.10.1 oferece suporte ao recurso de acesso à LAN local, no qual você pode determinar se deseja acessar os recursos da LAN local em seu dispositivo cliente assim que uma conexão VPN for estabelecida. Você pode usar esse recurso somente se o seu administrador tiver configurado a configuração de acesso à LAN local no NetScaler Gateway.

Para configurar o acesso à LAN local na interface do usuário do Citrix Secure Access:

1. navegar para o menu principal e clique em **Configurações**.
2. Habilite **Permitir Acesso à LAN Local**.

Você pode verificar o status do acesso à LAN local na página **Estatísticas**.

Enviar logs

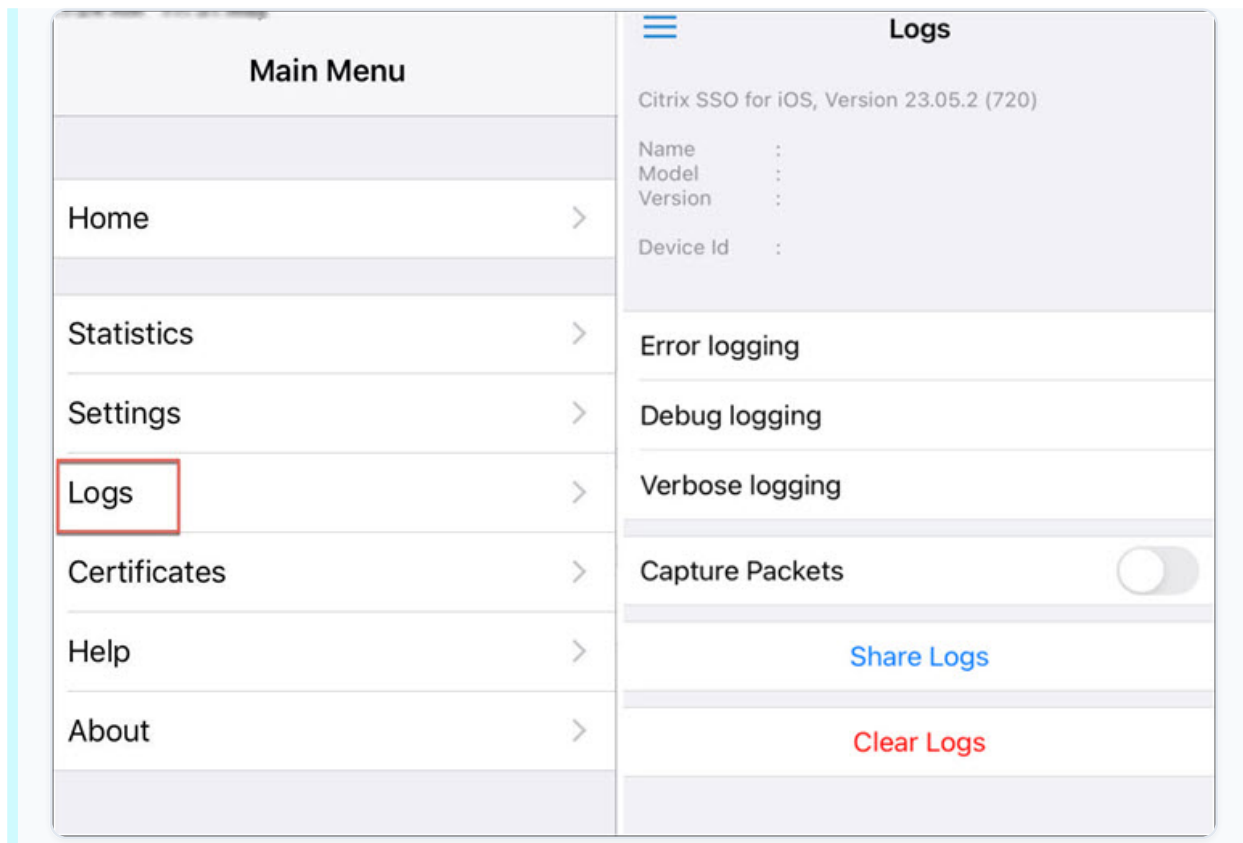
A captura de logs de depuração é uma parte crítica da solução de problemas ou do relato de problemas ao Suporte Citrix.

A seguir estão as etapas para capturar e compartilhar os logs de depuração:

1. Defina o botão **Registro de Depuração** como ATIVADO.
2. Compartilhe os logs usando opções como e-mail, chat, salvar em arquivos e assim por diante.

Nota:

- Para gerar um novo conjunto de logs, exclua os logs mais antigos primeiro usando **Limpar Logs**.
- A partir da versão 23.07.1, a opção **Logs de E-mail** é substituída pela opção **Compartilhar Logs**. Compartilhar Logs oferece várias opções para compartilhar os arquivos de log compactados.



Visualizar certificados de cliente

Você pode visualizar os certificados de cliente que são importados para o Citrix Secure Access. Os certificados importados aparecem na seção **Certificados**. Você pode excluir os certificados de uma das seguintes maneiras.

- Na célula do certificado, execute um gesto de deslizar da direita para a esquerda para revelar o botão **Excluir**. Em seguida, toque em **Excluir**.
- Toque em **Editar** para revelar o botão **Excluir** e, em seguida, toque em **Excluir**.

Visualizar ou excluir um certificado(/en-us/citrix-sso/media/sso-ios-certificates.png)

Tópicos de ajuda

Para obter ajuda sobre vários itens, consulte **Ajuda**.

Visualizar os tópicos de ajuda(/en-us/citrix-sso/media/sso-ios-help.png)

Cliente Citrix Secure Access para dispositivos macOS

O aplicativo Citrix Secure Access oferece a melhor solução de acesso a aplicativos e proteção de dados da categoria, fornecida pelo NetScaler Gateway. Agora você pode acessar com segurança aplicativos críticos para os negócios, desktops virtuais e dados corporativos de qualquer lugar a qualquer momento. O aplicativo Citrix Secure Access é o cliente VPN de próxima geração para NetScaler Gateway, construído usando a estrutura Network Extension da Apple. Ele substitui o cliente VPN Citrix legado na App Store.

O aplicativo Citrix Secure Access oferece suporte completo a Gerenciamento de Dispositivos Móveis (MDM) no macOS. Com um servidor MDM, um administrador agora pode configurar e gerenciar remotamente perfis VPN em nível de dispositivo e perfis VPN por aplicativo.

Importante:

- O aplicativo Citrix Secure Access oferece suporte a acesso de rede Zero-trust. Além do URL do NetScaler Gateway, você também pode se conectar ao URL do Workspace.
- Para obter instruções específicas do administrador sobre o Citrix Secure Access para macOS, consulte [Citrix SSO para iOS e Citrix Secure Access para macOS](#).

Instalar o cliente Citrix Secure Access para macOS

A partir do cliente Citrix Secure Access para macOS versão 25.06.1.1, você pode baixar e instalar o aplicativo usando o arquivo de pacote (`.pkg`) disponível em [Citrix Secure Access para macOS](#) ou na App Store. O arquivo `.pkg` pode ser instalado manualmente ou usando ferramentas de gerenciamento como Jamf e Intune. Anteriormente, os usuários estavam limitados a instalar o cliente Citrix Secure Access para macOS apenas pela App Store.

Instalar o aplicativo Citrix Secure Access no macOS usando o arquivo .pkg

Pré-requisitos

Antes de instalar o arquivo `.pkg` para o aplicativo Citrix Secure Access, certifique-se de que os seguintes pré-requisitos sejam atendidos:

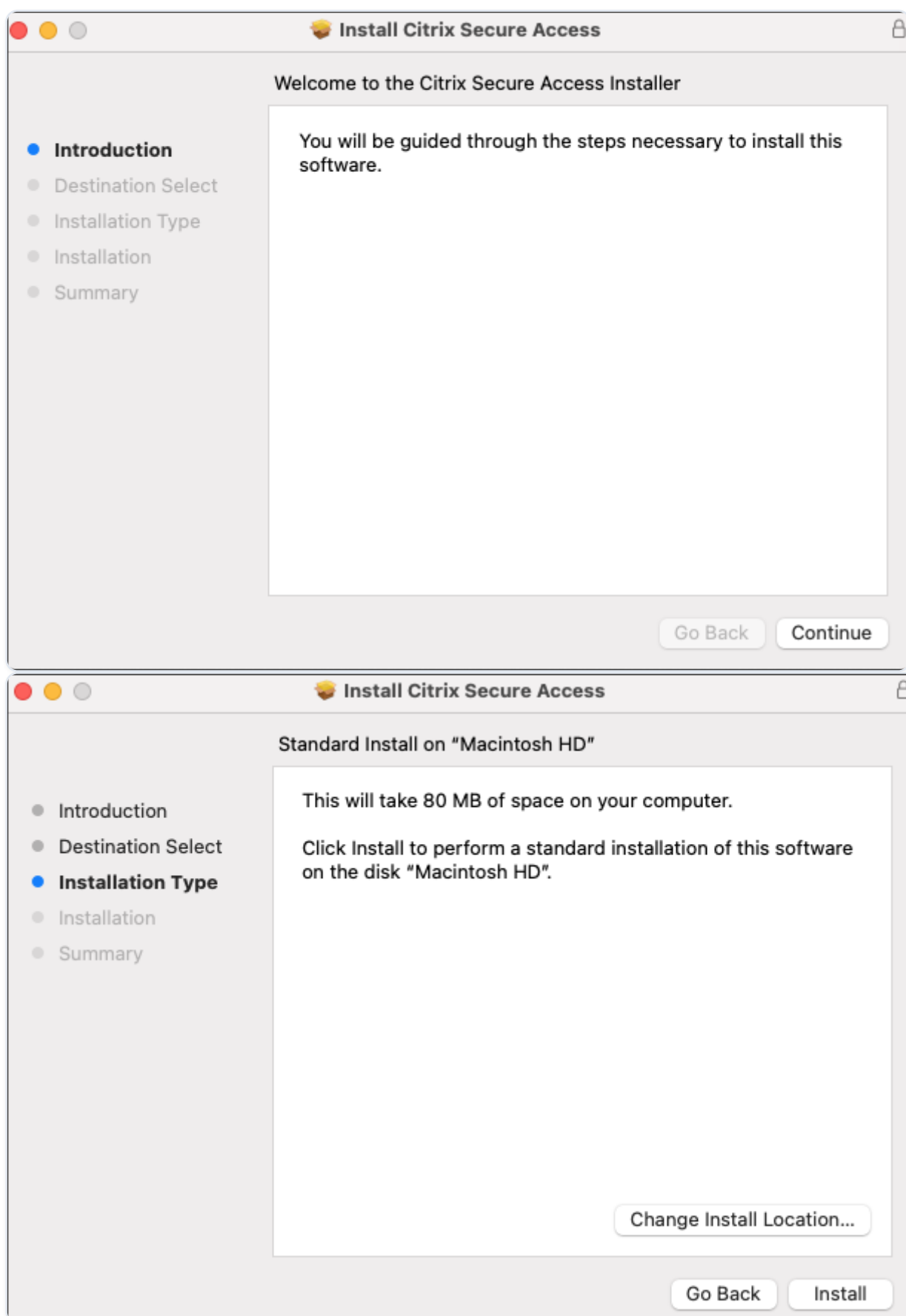
- O computador Mac está executando macOS 13.0 ou posterior.
- O usuário tem privilégios de administrador no computador Mac. Em máquinas gerenciadas, os administradores devem garantir que as permissões de instalação de aplicativos estejam ativadas e que a extensão do sistema com o identificador "com.citrix.NSG.macos.app.vpnplugin" esteja ativada.
- Saia do aplicativo Citrix Secure Access se ele estiver em execução.
- Exclua qualquer versão do aplicativo Citrix Secure Access instalada anteriormente pela App Store.

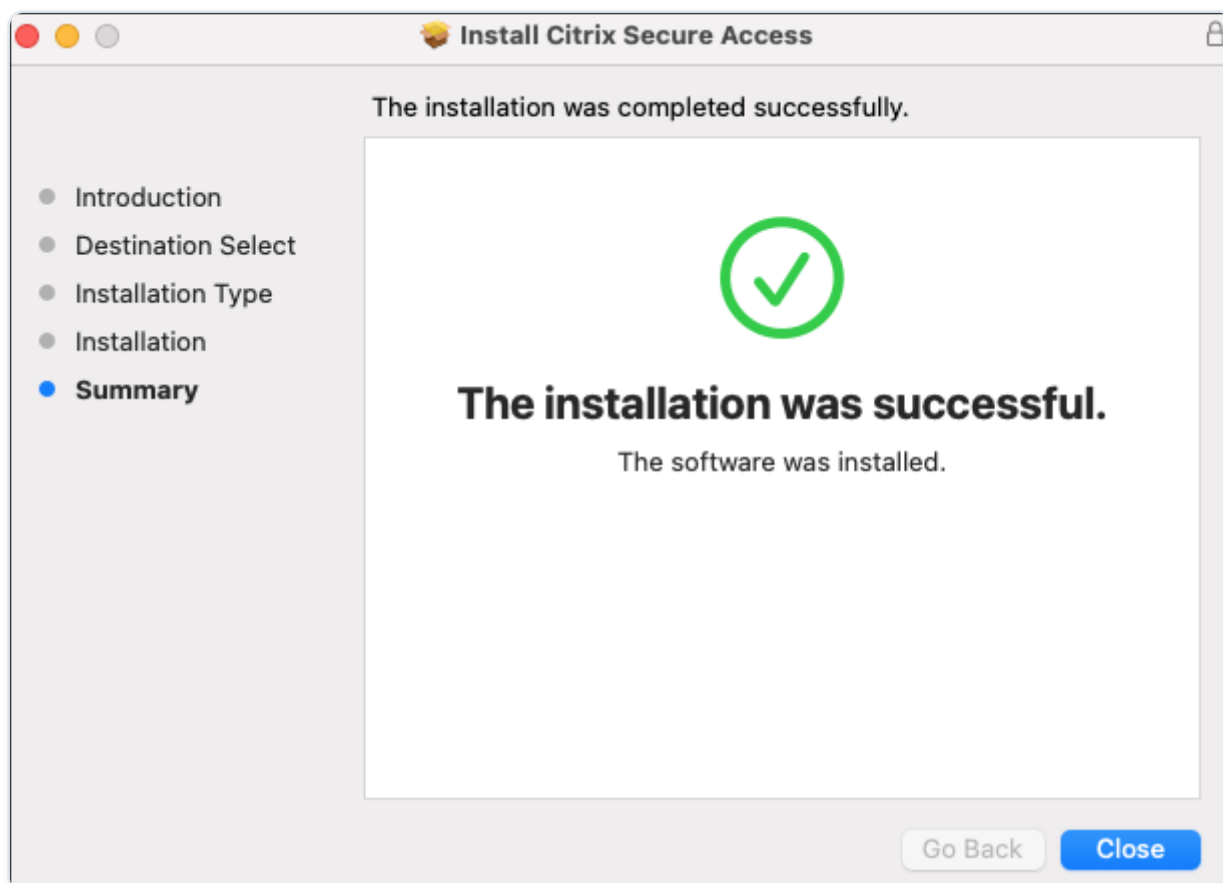
Como instalar o aplicativo Citrix Secure Access no macOS

Importante:

- O arquivo `.pkg` do aplicativo Citrix Secure Access usa a extensão do sistema com o identificador "com.citrix.NSG.macos.app.vpnplugin" para conexões VPN.
- Para autenticação de certificado de cliente, os certificados devem ser instalados no **System Keychain** porque as extensões do sistema macOS não podem acessar certificados do **login Keychain**.
- Se o mesmo certificado estiver instalado tanto no **System Keychain** quanto no **login Keychain**, exclua o certificado junto com sua chave do **login Keychain**.

1. Baixe o arquivo `.pkg` em [Citrix Secure Access para macOS](#).
2. Instale o aplicativo usando a ferramenta de gerenciamento (Jamf ou Intune) ou manualmente. Para instalar o aplicativo manualmente, clique duas vezes no arquivo `.pkg` e siga as instruções na tela.

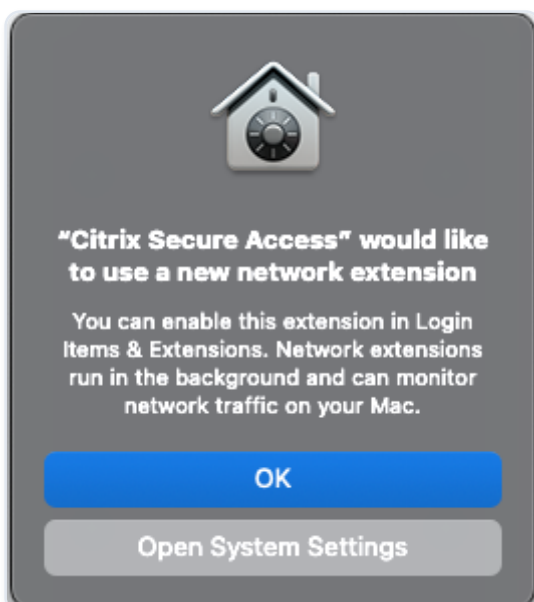




Configuração inicial

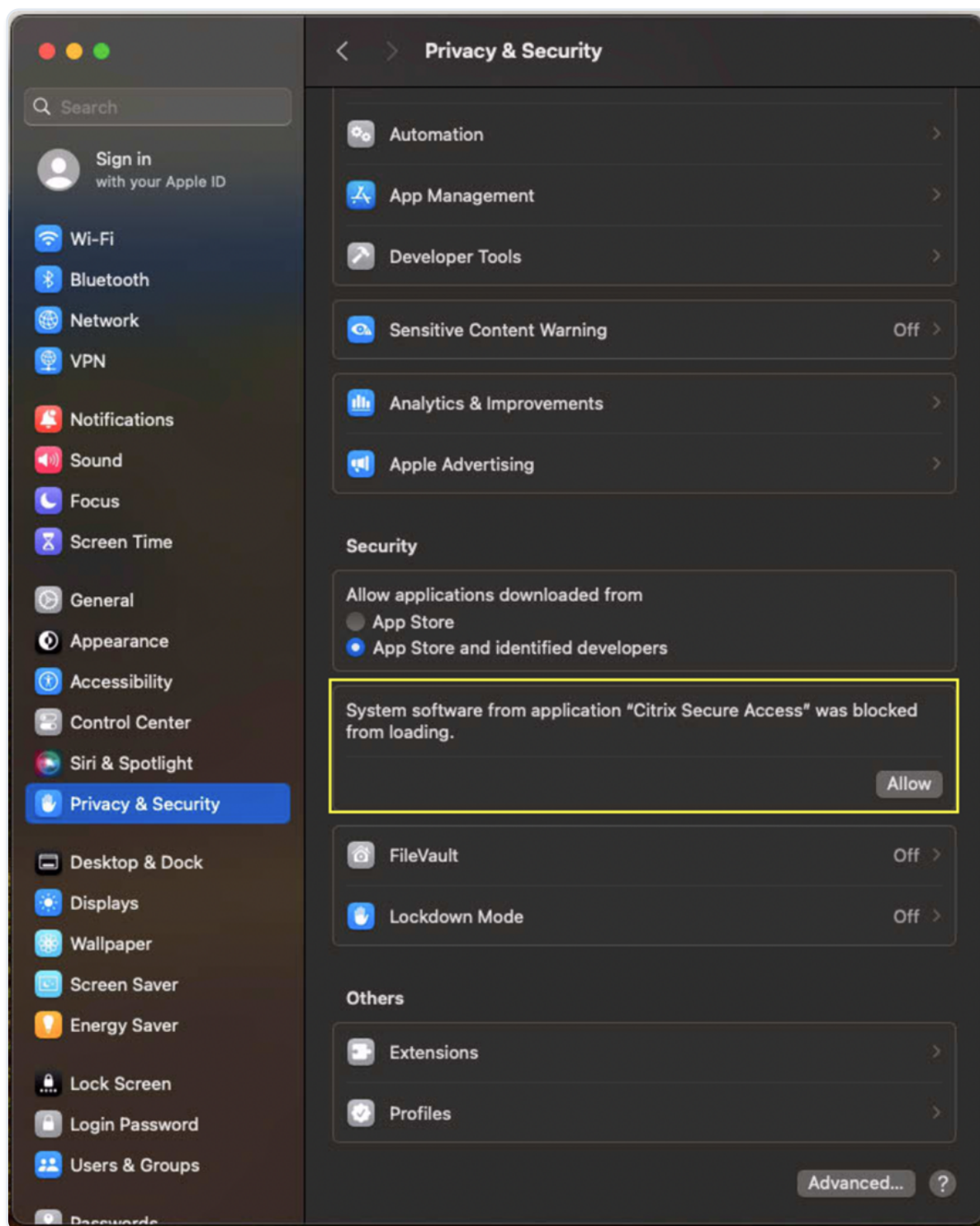
Após instalar o aplicativo Citrix Secure Access, siga as instruções abaixo para usar o aplicativo Citrix Secure Access em seu dispositivo macOS:

1. Abra a pasta **Aplicativos** e clique duas vezes no ícone do aplicativo Citrix Secure Access para iniciá-lo.
2. No primeiro lançamento, o sistema solicita permissão para instalar a extensão do sistema. Clique em **OK** no prompt do sistema.

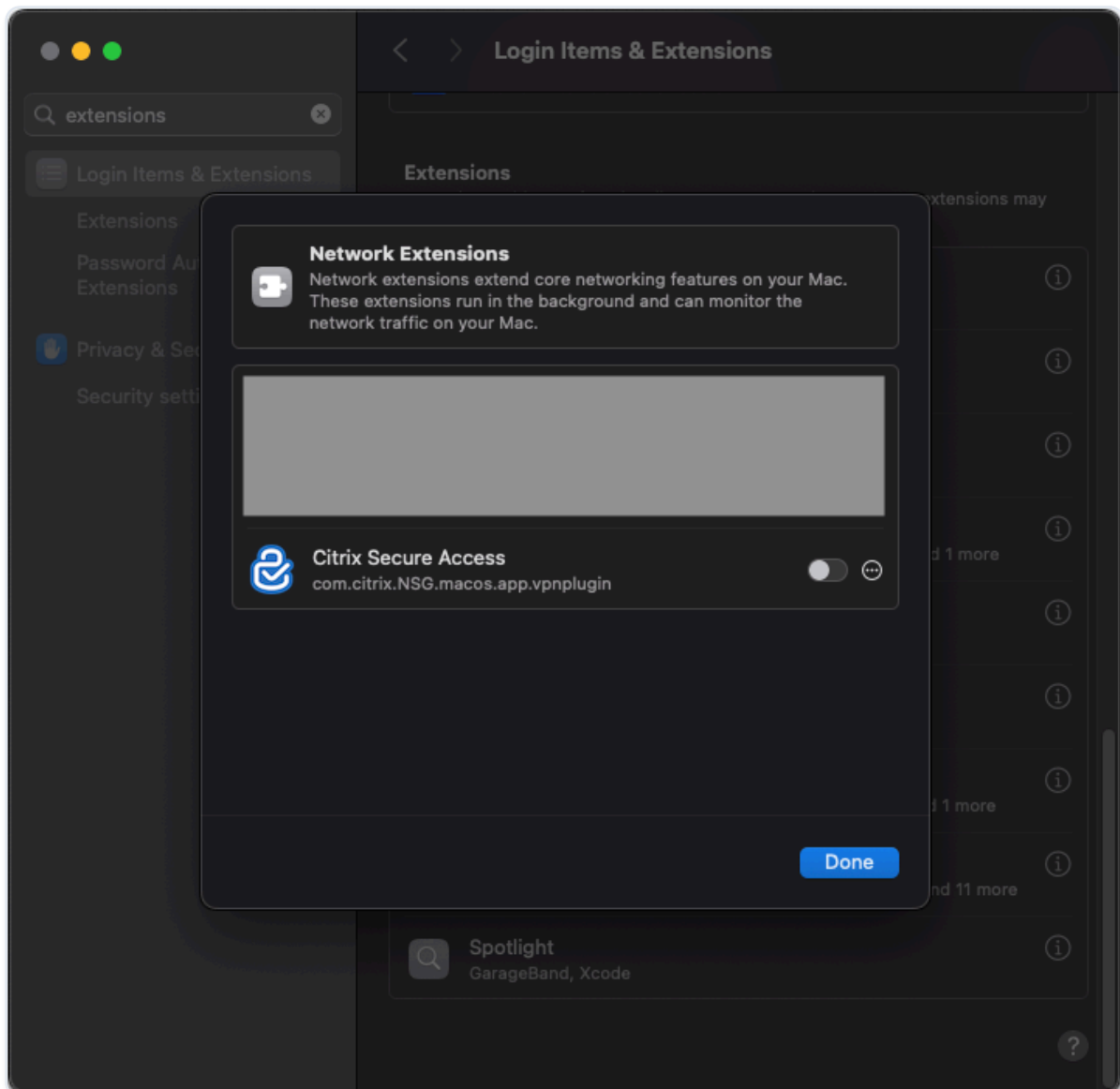


Se o prompt do sistema não aparecer, vá para **Ajustes do Sistema** para habilitar a instalação da extensão do sistema com o identificador "com.citrix.NSG.macos.app.vpnplugin".

- Para macOS 14.x, a opção **Ajustes do Sistema** está na aba **Privacidade e Segurança**.



- Para macOS 15.x e posterior, a opção **Ajustes do Sistema** está em **Itens de Início de Sessão e Extensões -> Extensões de Rede**.



Suporte para instalação automática do plug-in Endpoint Analysis™ com o aplicativo Citrix Secure Access

A partir da versão 25.11.1.1, o aplicativo Citrix Secure Access inclui a instalação automática do plug-in Endpoint Analysis (EPA). O plug-in EPA agora é empacotado por padrão com todas as instalações e atualizações, eliminando a necessidade de instalação separada e simplificando o processo de configuração. Este recurso não está disponível para a versão da App Store do aplicativo.

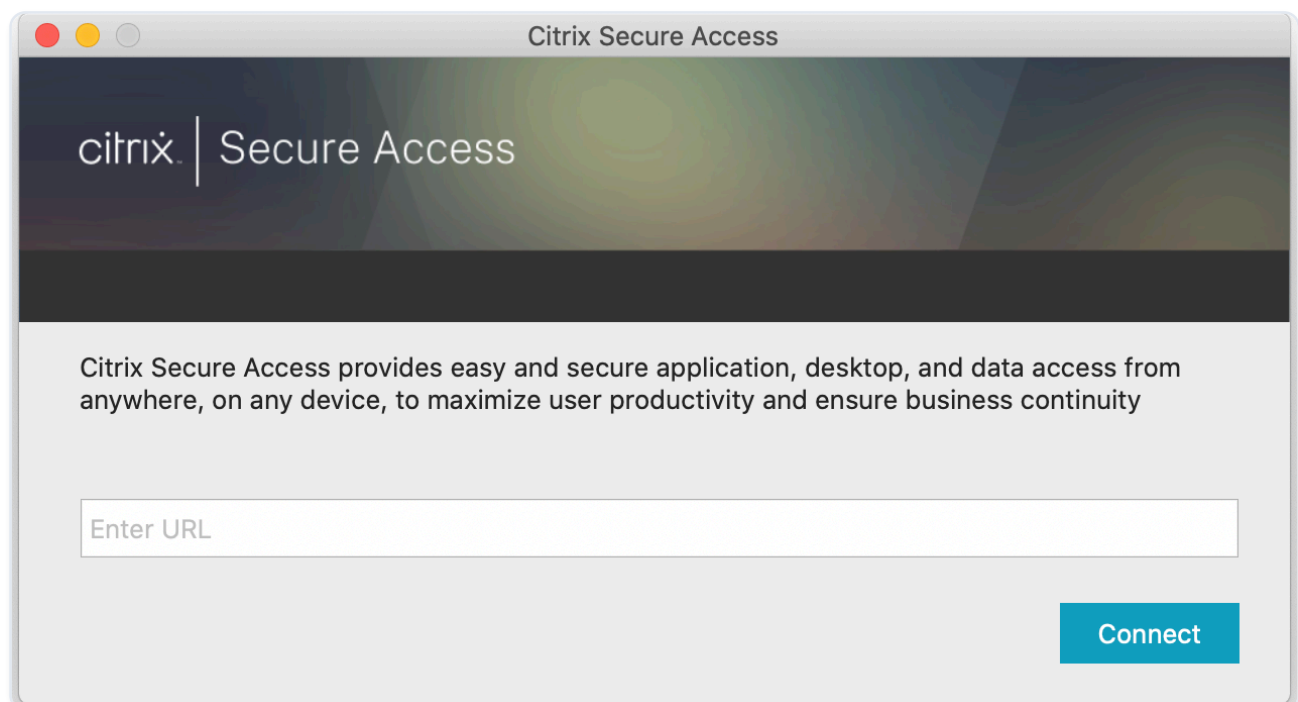
Anteriormente, os usuários tinham que baixar e instalar manualmente o plug-in EPA durante o login no aplicativo Citrix Secure Access.

Como usar o aplicativo Citrix Secure Access no seu dispositivo macOS

Usuários iniciantes devem criar uma conexão com o NetScaler Gateway adicionando o servidor. Usuários existentes podem se conectar a uma conexão existente ou adicionar uma nova conexão, e também editar conexões existentes. Você também pode visualizar os logs e tomar as ações apropriadas de acordo.

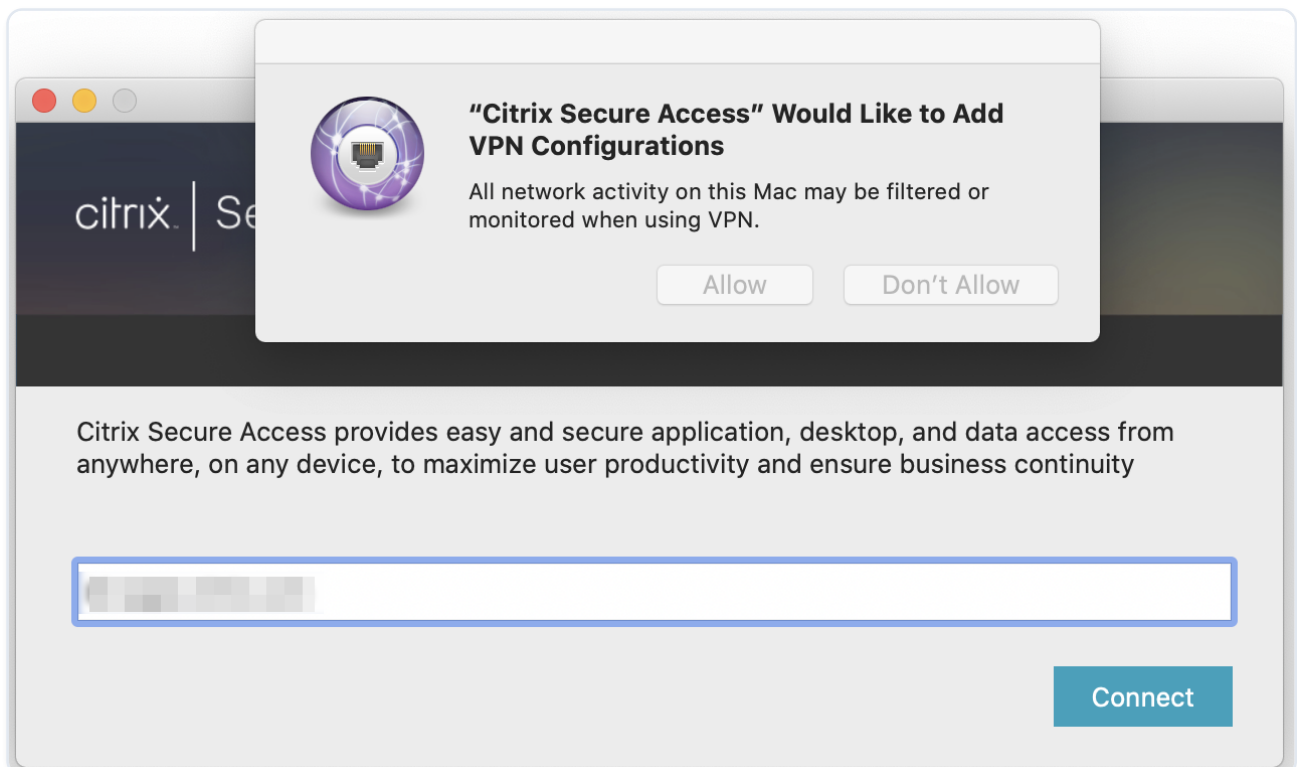
Experiência do usuário iniciante

Depois de instalar o aplicativo Citrix Secure Access e abri-lo pela primeira vez, a seguinte tela aparece.

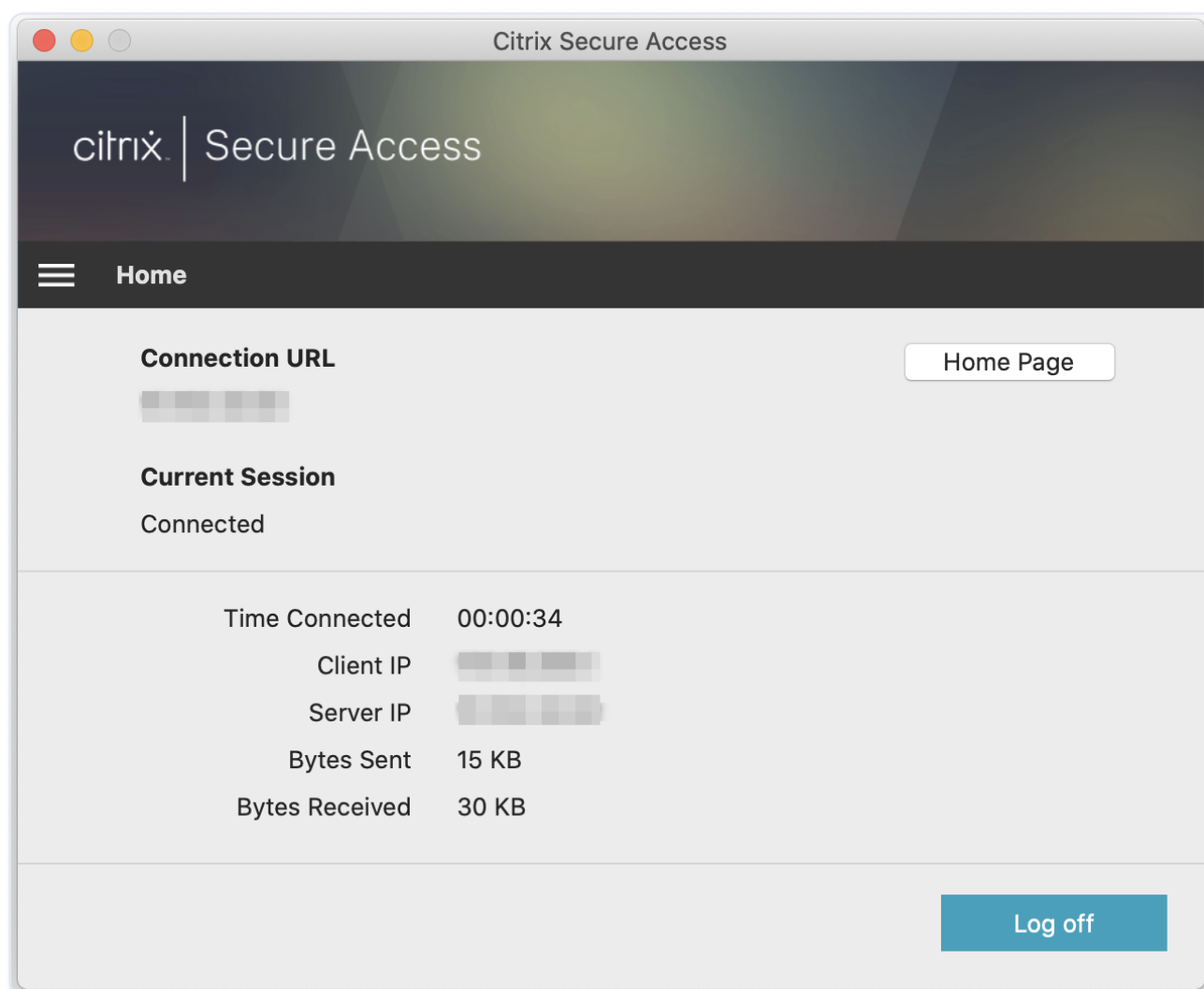


Insira a URL base do NetScaler Gateway ou a URL do Citrix Workspace e clique em **Conectar**.

Uma mensagem pop-up aparece. Clique em **Permitir** para habilitar a adição de uma conexão. Esta mensagem aparece apenas na primeira vez. Para novas conexões subsequentes, esta mensagem não aparece.



Nota: Para sair do Citrix Secure Access, é recomendável que você primeiro clique em **Log Off** no aplicativo e depois saia do aplicativo pelo dock. Não use a opção **Sair** do dock.

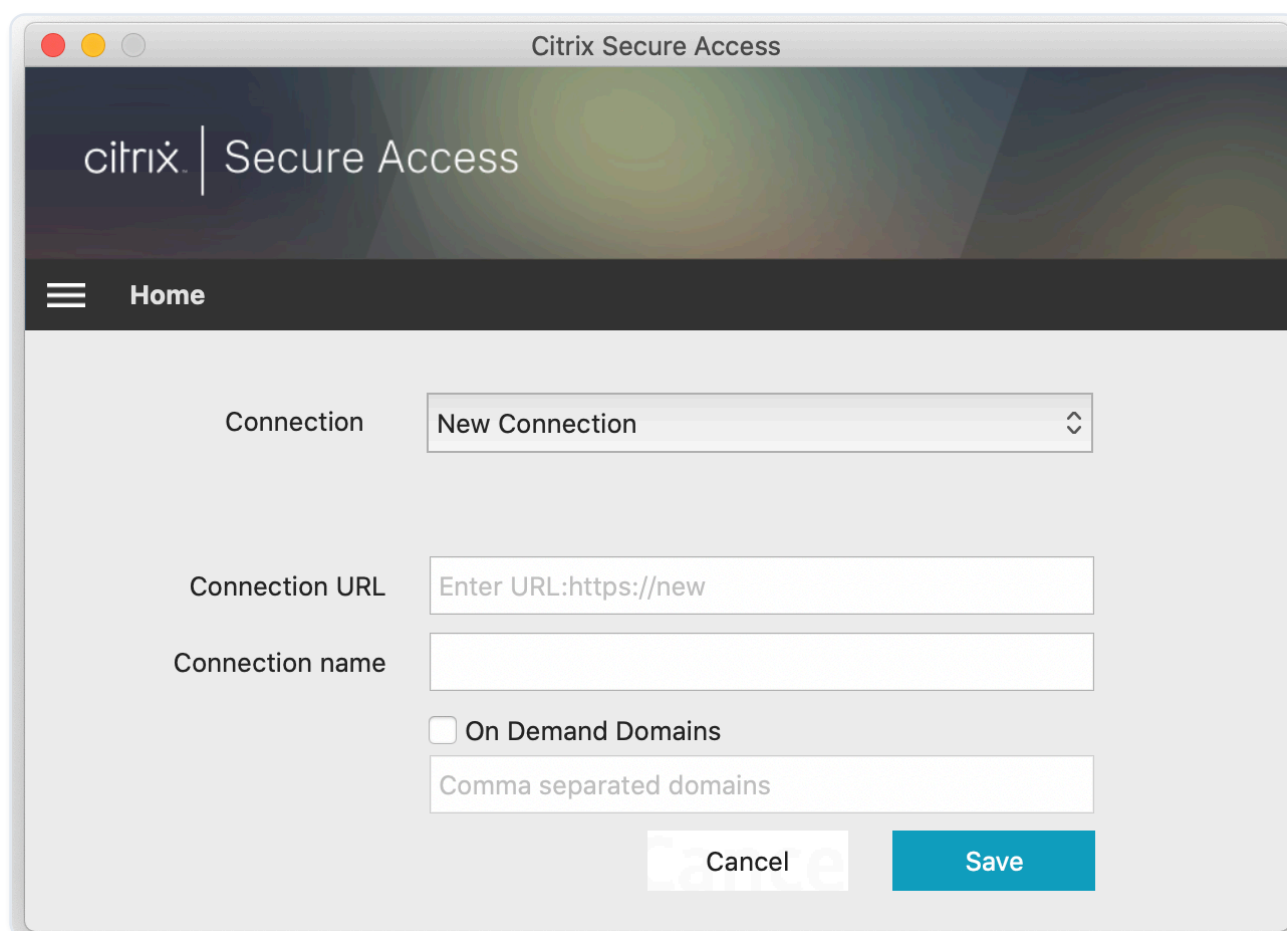


Conectar ao NetScaler Gateway

Após adicionar a primeira conexão, para conexões subsequentes, você pode se conectar a um NetScaler Gateway ou Citrix Workspace existente ou adicionar uma conexão.

Adicionar uma conexão

Insira a URL base (por exemplo, [Minha empresa <https://gateway.mycompany.com>](https://gateway.mycompany.com)) e o nome para a conexão VPN.

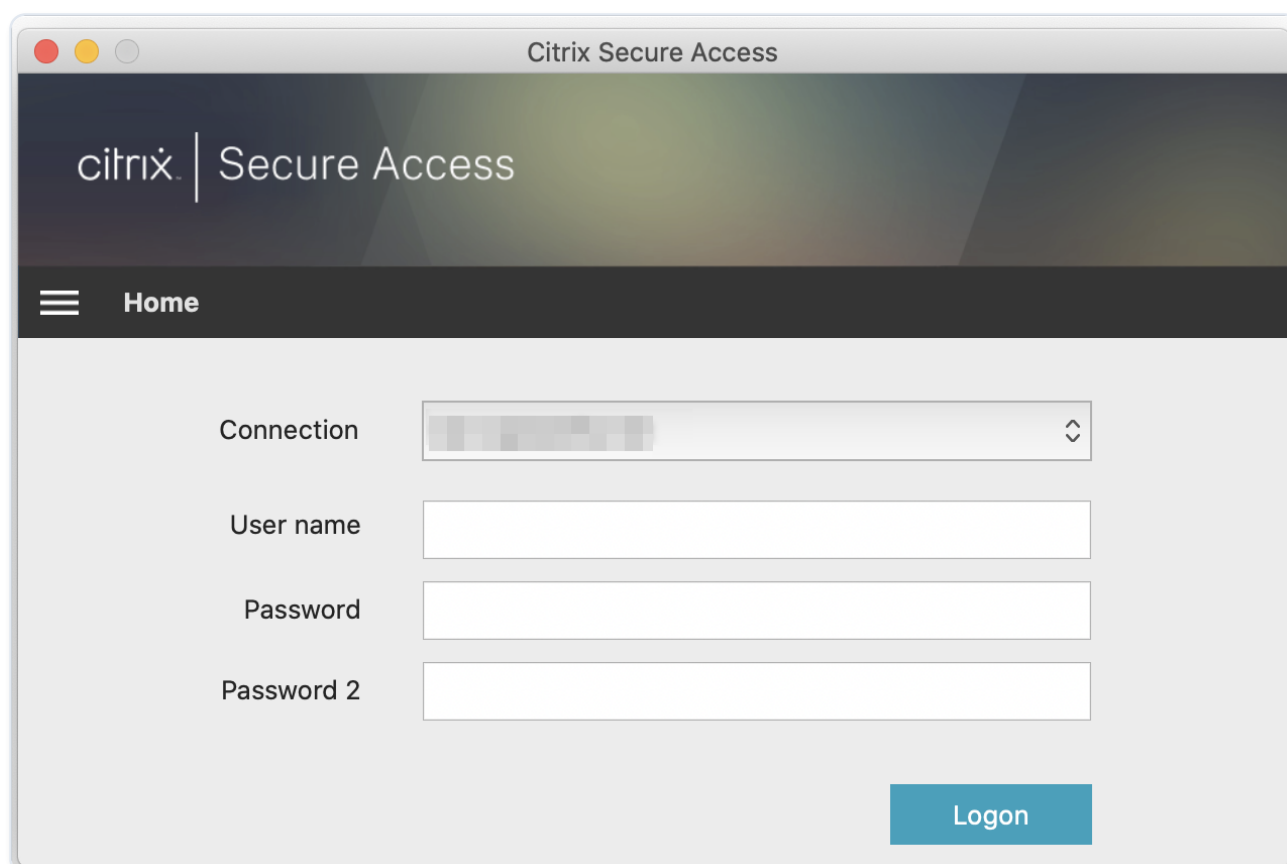


The screenshot shows a web browser window titled "Citrix Secure Access". The page has a dark header with the Citrix logo and "Secure Access" text. Below the header is a navigation bar with a hamburger menu icon and the word "Home". The main content area is a light gray form titled "New Connection". The form contains the following fields and controls:

- Connection:** A dropdown menu with "New Connection" selected.
- Connection URL:** A text input field with the placeholder text "Enter URL:https://new".
- Connection name:** A text input field.
- On Demand Domains:** A checkbox that is currently unchecked.
- Comma separated domains:** A text input field.
- Buttons:** "Cancel" and "Save" buttons at the bottom right.

Conectar-se ao NetScaler Gateway existente

Selecione uma conexão existente e forneça as credenciais de autenticação para o seu servidor e selecione **Logon**.



Reconectar-se ao NetScaler Gateway após uma falha de conexão VPN

A partir da versão 23.09.1, o cliente Citrix Secure Access para macOS solicita que você se reautentique com o NetScaler Gateway quando uma conexão VPN é perdida. Você é notificado na interface do usuário do cliente Citrix Secure Access indicando que a conexão com o NetScaler Gateway foi perdida e que você deve se reautenticar para retomar a conexão.



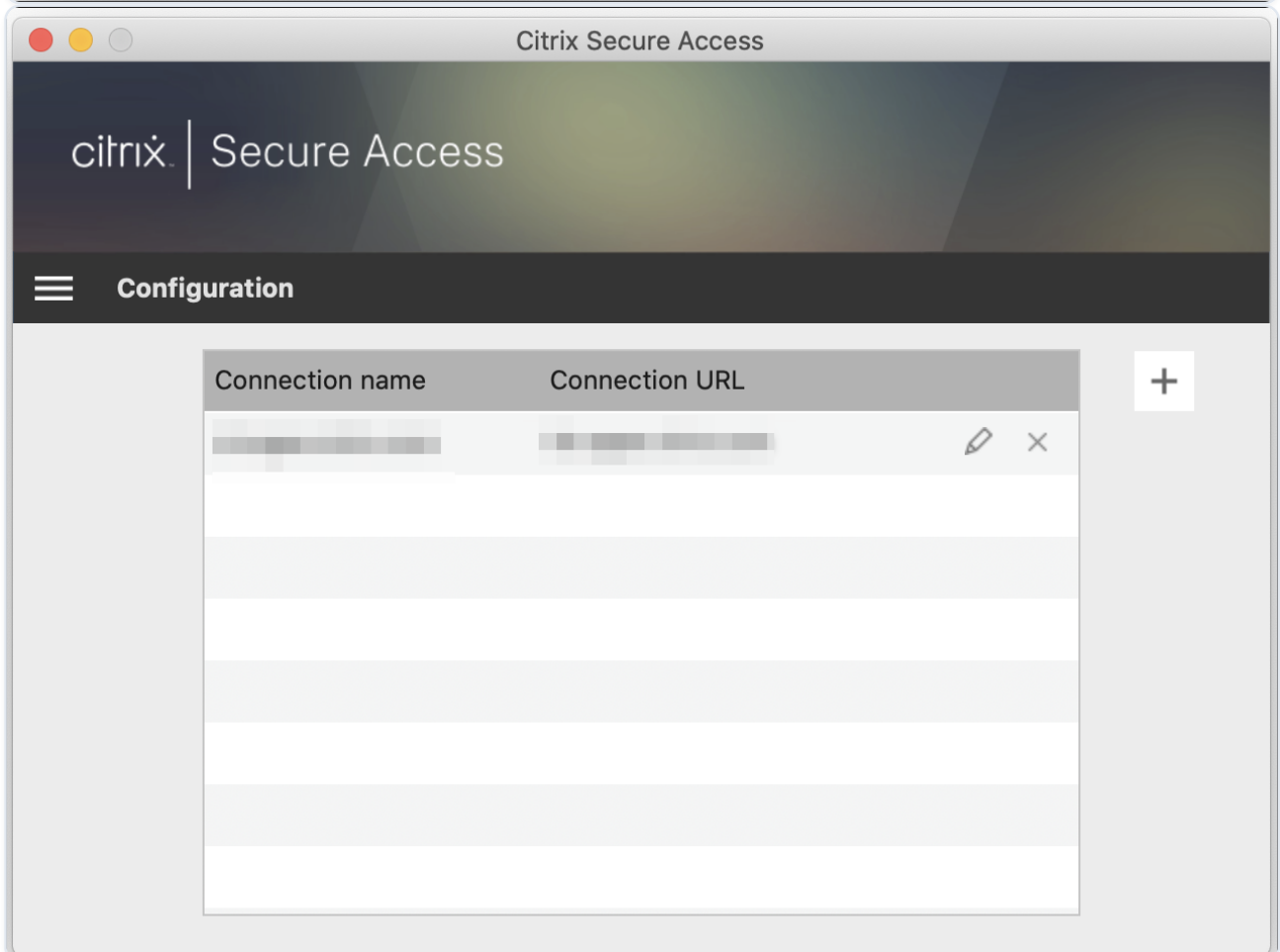
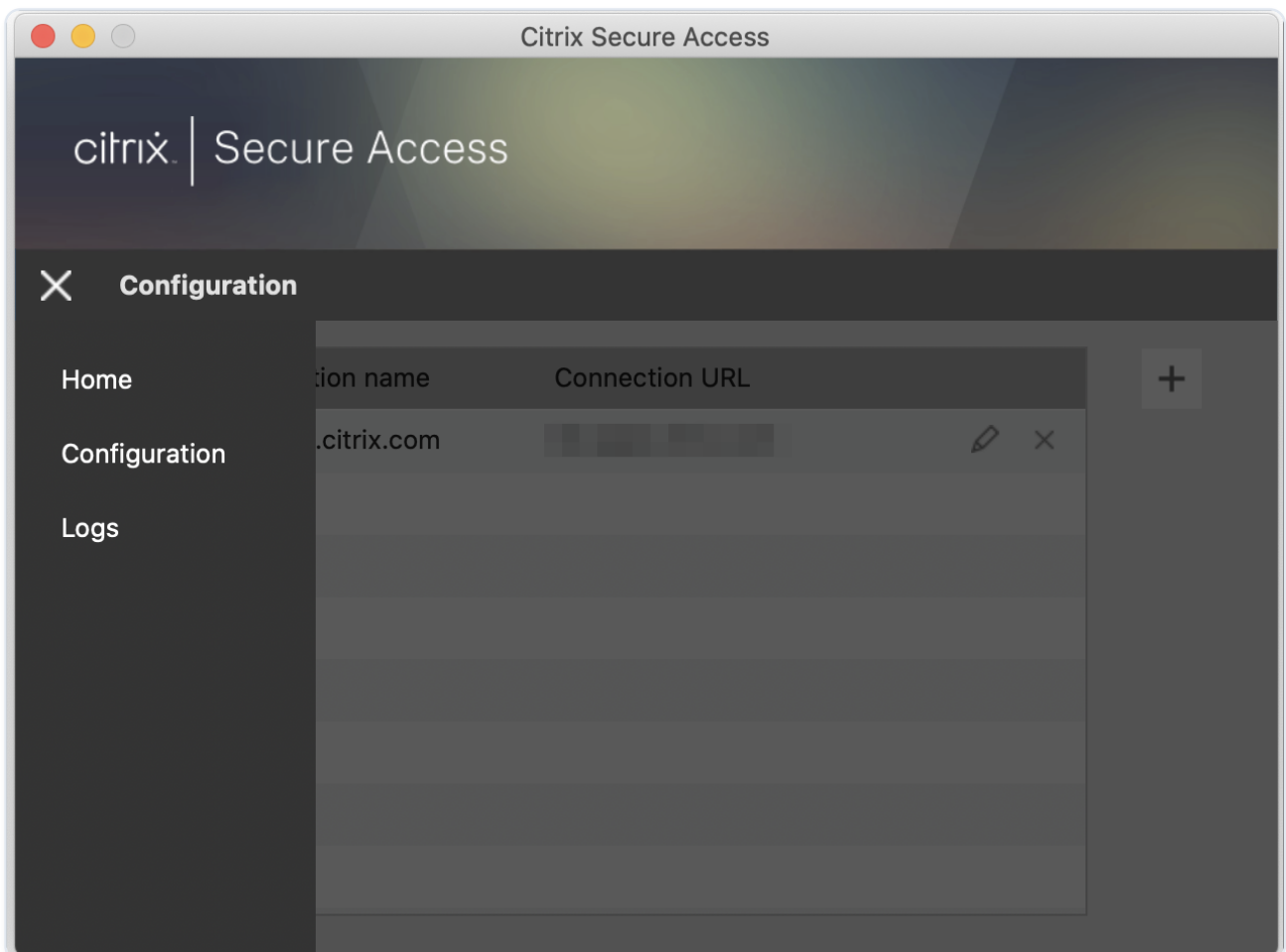
Reauthentication Needed

Gateway connection lost. Reauthenticate to resume connection.

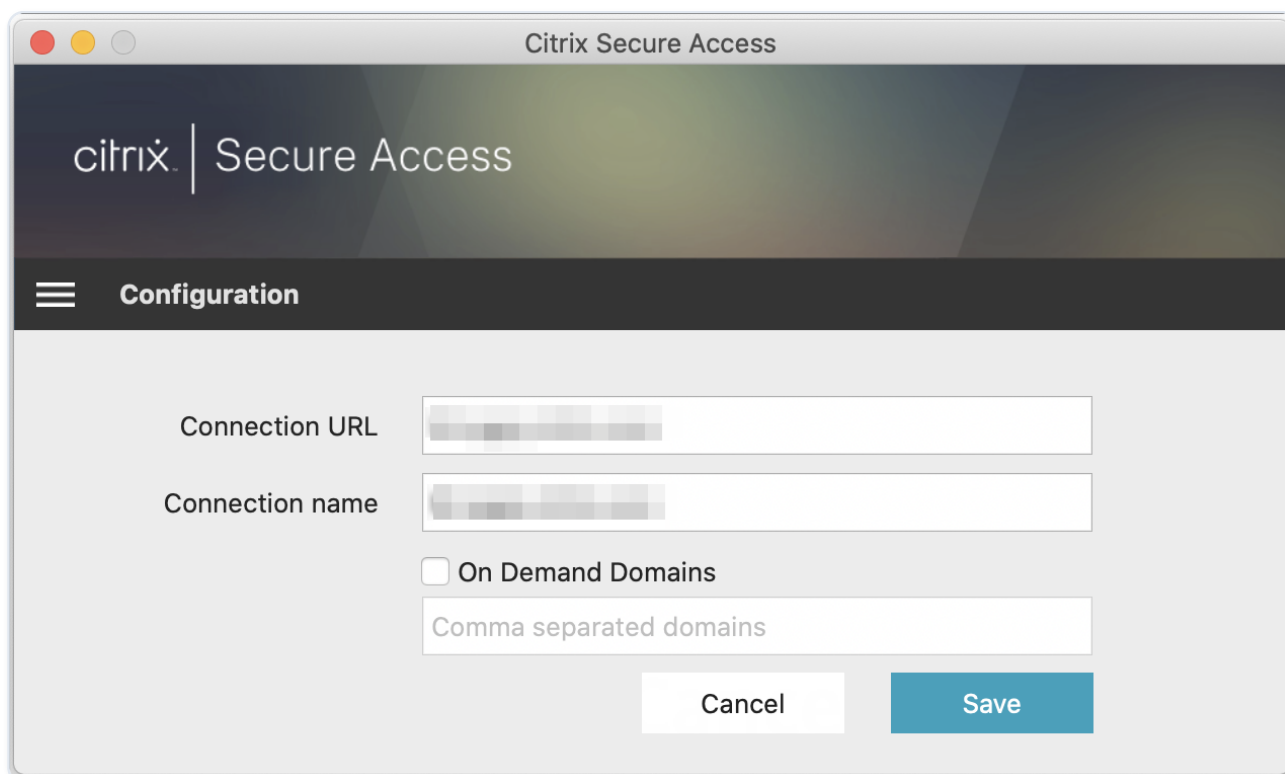
Ok

Modificar uma conexão existente

Você pode modificar ou excluir uma conexão existente.



Modifique os detalhes da conexão conforme necessário.

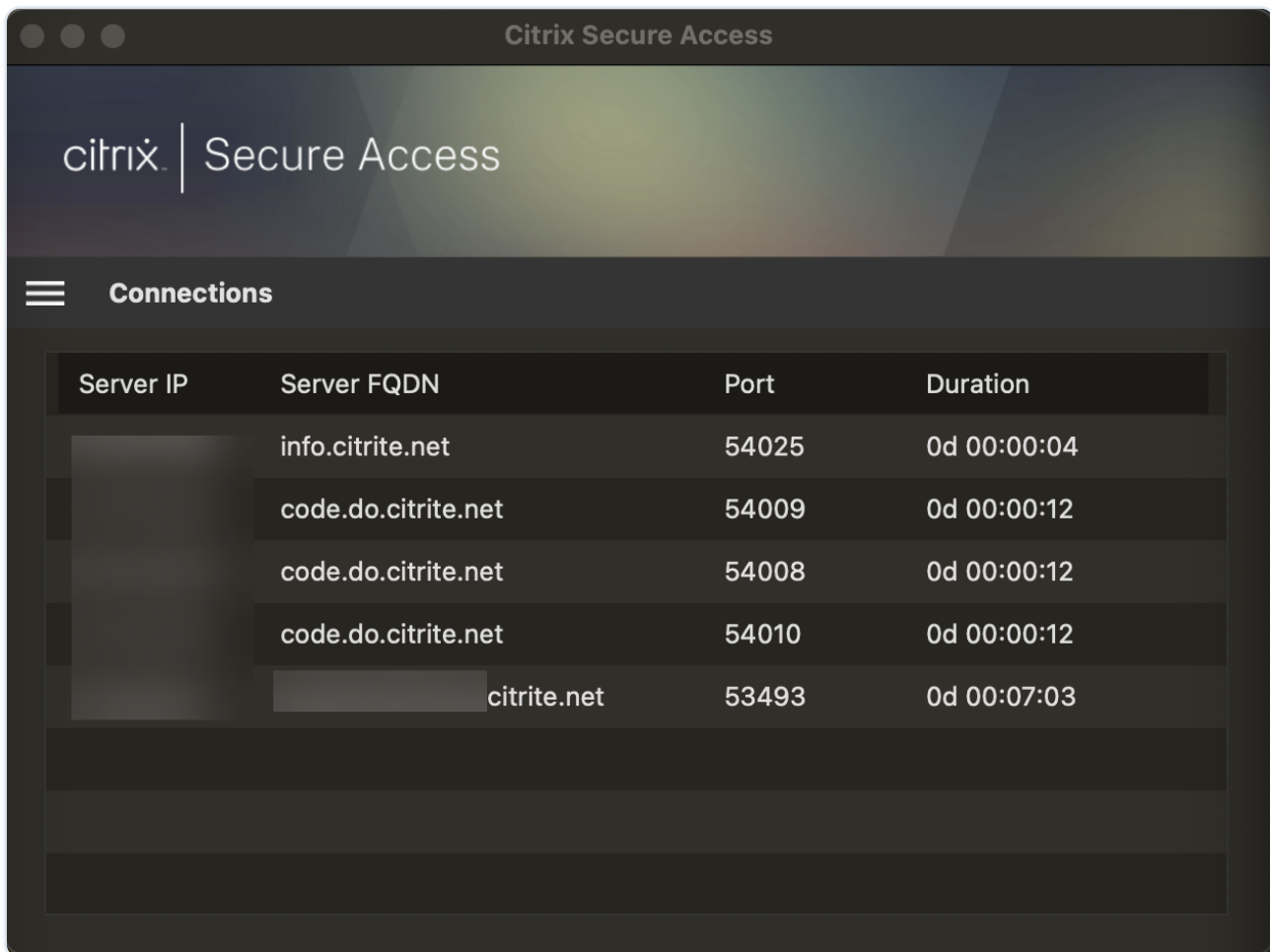


The screenshot shows a macOS-style window titled "Citrix Secure Access". The window has a dark header bar with the Citrix logo and the text "Secure Access". Below the header is a dark navigation bar with a hamburger menu icon and the word "Configuration". The main content area is light gray and contains the following fields:

- "Connection URL" with a text input field.
- "Connection name" with a text input field.
- A checkbox labeled "On Demand Domains".
- A text input field with the placeholder text "Comma separated domains".
- At the bottom right, there are two buttons: "Cancel" (white with gray border) and "Save" (blue).

Informações sobre conexões seguras

A partir da versão 23.09.1, você pode visualizar os detalhes da conexão segura que incluem o endereço IP, FQDN, porta de destino e duração da conexão. Para visualizar esses detalhes, clique no menu hambúrguer na interface do usuário e navegar para **Connections**.



The screenshot shows the Citrix Secure Access application window on a macOS system. The title bar reads 'Citrix Secure Access'. The main header area displays the Citrix logo and the text 'Secure Access'. Below this, a sidebar menu is visible with the 'Connections' option selected. The main content area displays a table of active connections.

Server IP	Server FQDN	Port	Duration
[REDACTED]	info.citrite.net	54025	0d 00:00:04
[REDACTED]	code.do.citrite.net	54009	0d 00:00:12
[REDACTED]	code.do.citrite.net	54008	0d 00:00:12
[REDACTED]	code.do.citrite.net	54010	0d 00:00:12
[REDACTED]	[REDACTED].citrite.net	53493	0d 00:07:03

Acesso à LAN local

O cliente Citrix Secure Access para macOS 23.10.1 oferece suporte ao recurso de acesso à LAN local, onde você pode determinar se deseja acessar os recursos da LAN local em sua máquina cliente assim que uma conexão VPN for estabelecida. Você pode usar esse recurso somente se o seu administrador tiver configurado a configuração de acesso à LAN local no NetScaler Gateway.

Para habilitar o acesso à LAN local na interface do usuário do cliente Citrix Secure Access, navegar para a página inicial e habilite a caixa de seleção **Permitir Acesso à LAN Local**.

Após uma conexão ter sido estabelecida, você pode verificar o status do acesso à LAN local na mesma página.

Logon único automático no Citrix Secure Access através do aplicativo Citrix Workspace

Importante:

Esta funcionalidade está desabilitada por padrão. Para usar esta funcionalidade, entre em contato com seu administrador.

A partir do Citrix Secure Access para macOS 24.03.1, um login no aplicativo Citrix Workspace pode realizar o logon único (SSO) dos usuários finais no Citrix Secure Access, estabelecer um túnel de usuário e fornecer acesso contínuo a aplicativos TCP/UDP. Se você estiver conectado ao aplicativo Citrix Workspace, o Citrix Secure Access para macOS pode ser iniciado automaticamente e você pode fazer login sem problemas usando o logon único.

Quando você faz login no aplicativo Citrix Workspace, o cliente Citrix Secure Access é iniciado automaticamente e você é conectado ao cliente com logon único. Quando você sai do aplicativo Citrix Workspace, o Citrix Secure Access automaticamente desconecta você do aplicativo sem sua intervenção manual. Esse recurso economiza tempo, pois os usuários finais devem fazer login em apenas um aplicativo, proporcionando assim uma experiência unificada.

Nota:

Para que este recurso funcione, a URL principal que é acessada via aplicativo Citrix Workspace e cliente Citrix Secure Access deve ser a mesma.

Pré-requisitos

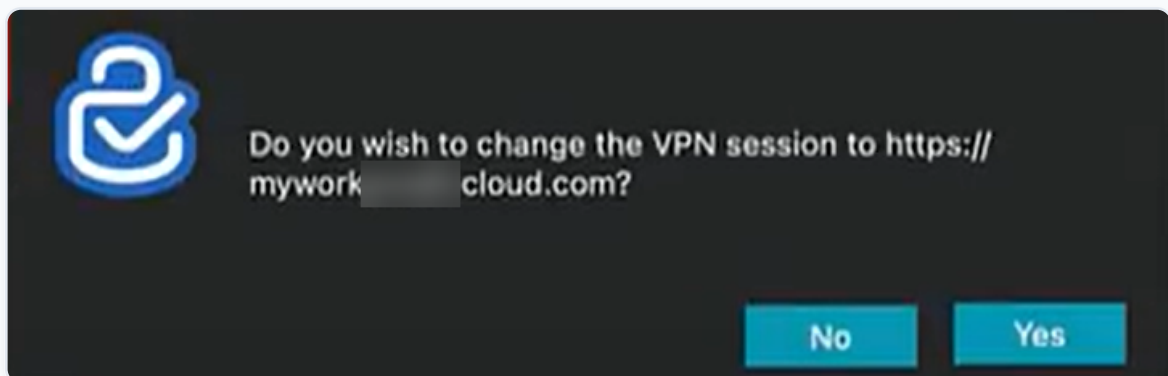
1. Os usuários finais devem estar no [aplicativo Citrix Workspace 2402](#) ou posterior. Para obter detalhes sobre a instalação do aplicativo Citrix Workspace para Mac, consulte [aplicativo Citrix Workspace para Mac](#).
2. Os usuários finais devem estar no [Citrix Secure Access para macOS 24.03.1](#) ou posterior.

Pontos a serem observados:

- Se os usuários finais já estiverem conectados ao aplicativo Citrix Workspace antes de usar esta funcionalidade, eles devem fazer login novamente no aplicativo Citrix Workspace para que o aplicativo possa acionar um logon único no cliente Citrix Secure Access.
- Quando um usuário sai do aplicativo Citrix Workspace devido a um tempo limite, logout manual do usuário e assim por diante, o Citrix Secure Access também é

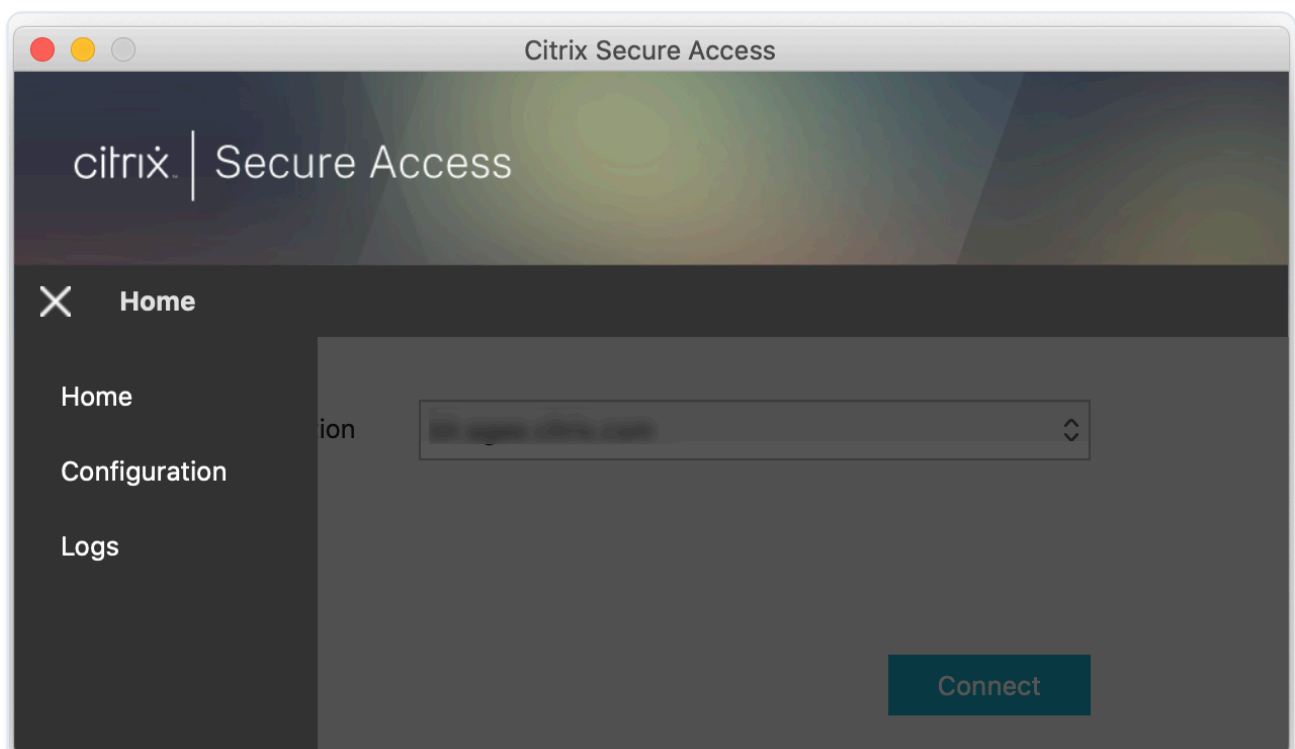
desconectado e a sessão do usuário é encerrada (isso ocorre apenas se o Citrix Secure Access foi iniciado automaticamente via aplicativo Citrix Workspace).

- O logon único do aplicativo Citrix Workspace para o Citrix Secure Access é suportado apenas em um único domínio primário. O logon único em vários domínios não é suportado.
- Se você mudar sua conexão do aplicativo Citrix Workspace para uma URL diferente depois de ter feito logon único no Citrix Secure Access através deste recurso, você será solicitado a escolher a URL de conexão do seu aplicativo Citrix Workspace.



Enviar logs

A captura de logs de depuração é uma parte crítica da solução de problemas ou do relato de problemas ao Suporte Citrix. Para solucionar problemas nos logs, navegar até **Início > Logs**.



Selecione um dos seguintes níveis de log de sessão:

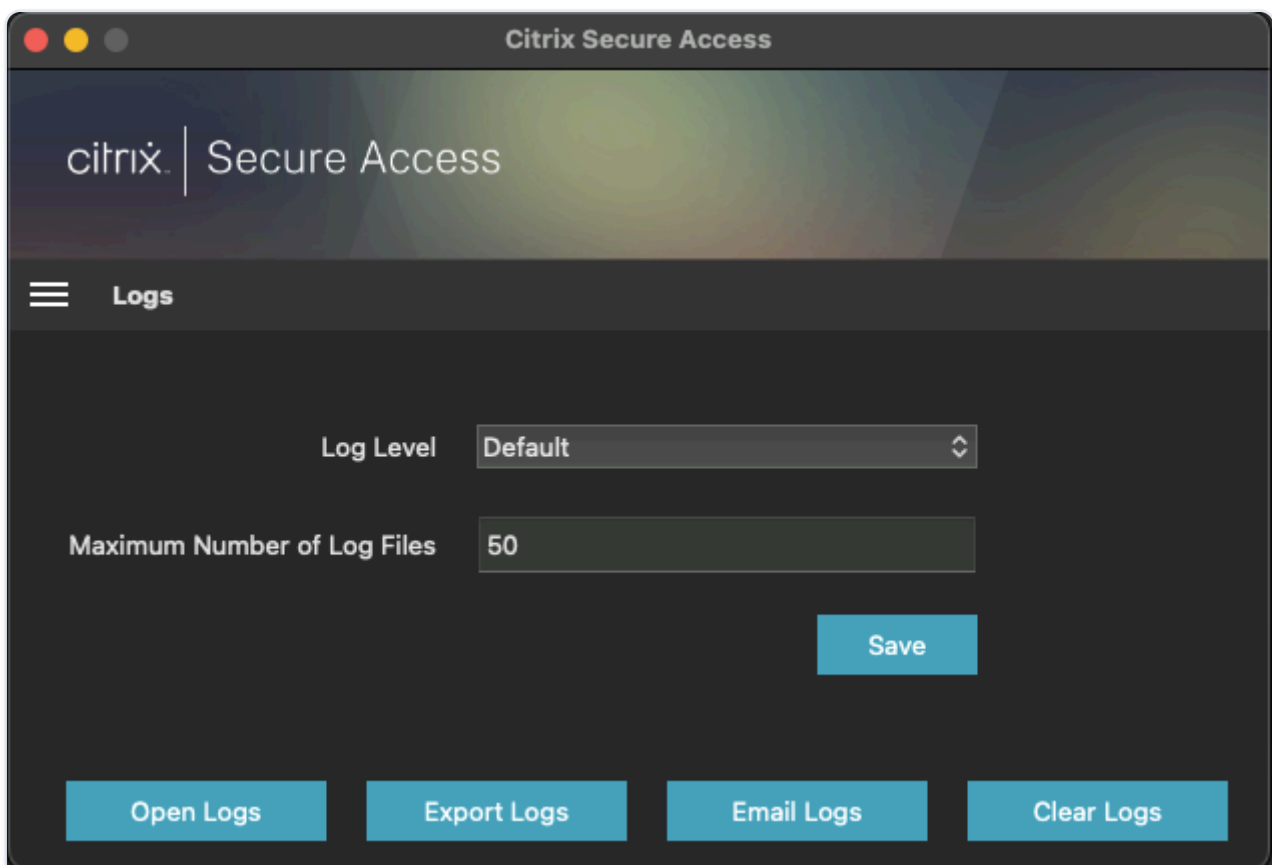
- **Padrão:** Imprime os logs mínimos para solução de problemas básicos.
- **Mensagens de Depuração:** Imprime todos os logs.
- **Detalhado:** Imprime os logs detalhados, incluindo mensagens de túnel e informações de configuração.

A partir da versão 23.07.1, você pode usar o campo **Número Máximo de Arquivos de Log** para especificar o número de arquivos que deseja adicionar para coleta de logs. Você pode adicionar até 50 arquivos de log.

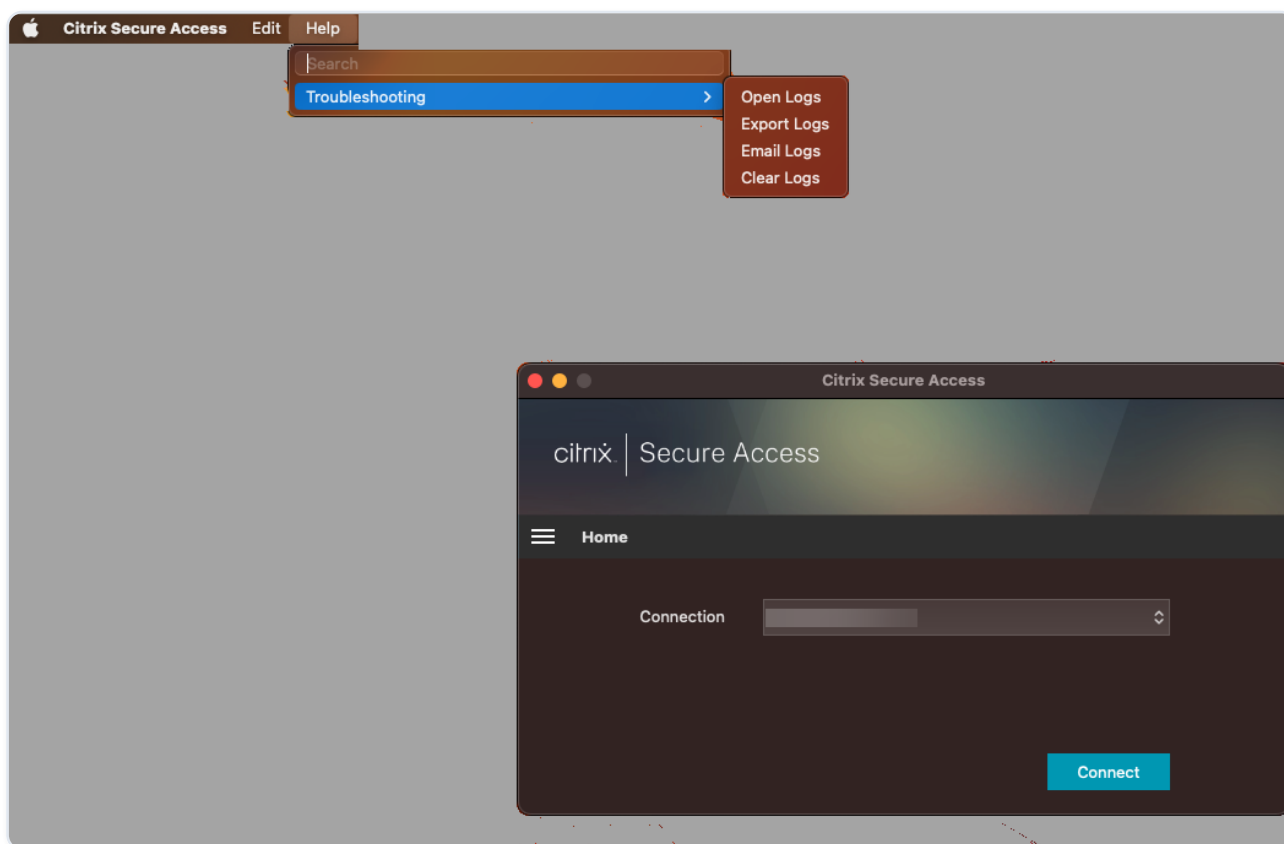
- Clique em **Abrir Logs** para visualizar os logs.
- Clique em **Exportar Logs** para exportar os logs para o seu diretório local.
- Clique em **Email Logs** para enviar os logs por e-mail.
- Clique em **Clear Logs** para excluir logs mais antigos.

Nota:

A partir da versão 23.07.1 do Citrix Secure Access para macOS, a opção **Email Logs** está disponível na página **Logs**.



A partir do Citrix Secure Access para macOS 23.06.1, um menu Ajuda é introduzido na barra de navegação do cliente Citrix Secure Access. Este menu pode ser usado como um local alternativo para capturar e enviar os logs de depuração.



Referência

Para obter instruções específicas do administrador sobre o Citrix SSO para iOS, consulte [Citrix SSO para iOS](#) e [Citrix Secure Access para macOS](#).

Cliente Citrix Secure Access para Linux

O cliente Citrix Secure Access para Linux é um software cliente VPN gerenciado pelo NetScaler Gateway que permite acessar dados e aplicativos corporativos remotamente.

O cliente Citrix End Point Analysis (EPA) é um software cliente gerenciado pelo NetScaler Gateway. Ele verifica os critérios do endpoint antes de conceder acesso a dados corporativos através do NetScaler Gateway. O cliente Citrix EPA e o cliente Citrix Secure Access são independentes um do outro.

Você pode instalar o cliente Citrix EPA somente se o seu administrador o tiver configurado. Para instruções específicas do administrador, consulte [Cliente Citrix Secure Access para Linux](#).

Atualização importante:

Estamos atualizando nossa interface de usuário e documentação do produto para a nova marca NetScaler. Você poderá ver referências a Citrix e NetScaler sendo usadas de forma intercambiável durante este período de transição.

Instalar o cliente Citrix Secure Access e o cliente Citrix EPA

Observações:

- Ao instalar o cliente Citrix Secure Access e o cliente Citrix EPA a partir do Software Center, você deve desinstalar as versões existentes se elas não estiverem atualizadas antes de fazer o upgrade para a versão mais recente. Isso é necessário porque, ao contrário do Ubuntu 18.04, as versões atuais não podem ser substituídas pelas versões mais recentes.
- No Ubuntu 20.x, se você baixar o cliente Citrix Secure Access de um navegador Firefox e depois abri-lo usando a opção **Abrir com**, a instalação pode falhar. Isso ocorre porque o

Firefox baixa o cliente em um local temporário e a instalação do cliente Citrix Secure Access falha a partir desse local.

Como solução alternativa, recomendamos que você selecione a opção **Salvar arquivo**. Essa opção baixa o cliente Citrix Secure Access na pasta **Downloads**. Você pode então clicar duas vezes no arquivo baixado e instalar o cliente Citrix Secure Access.

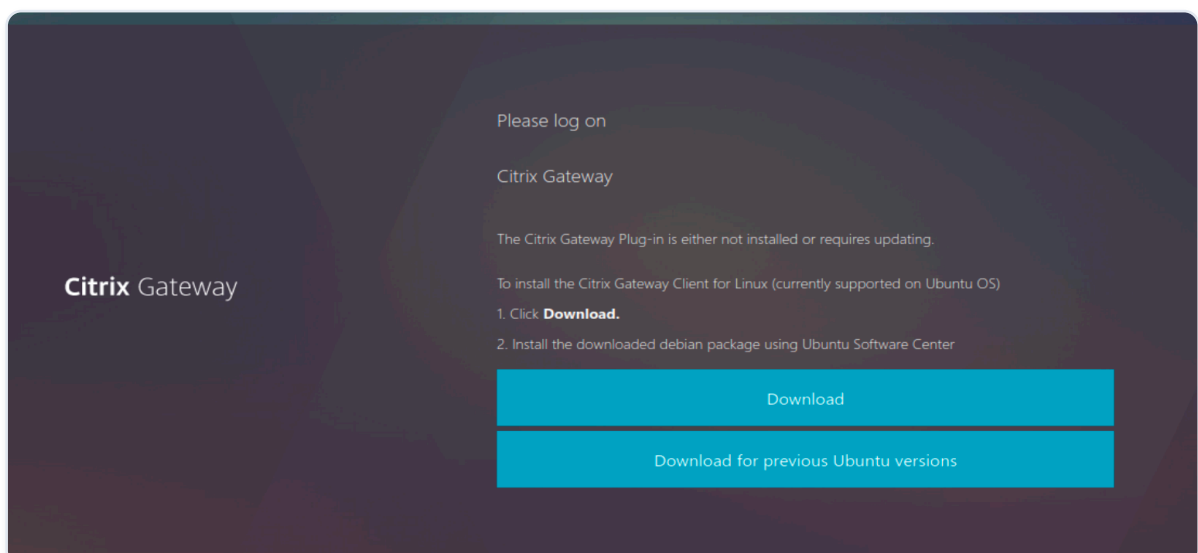
- Em clientes Linux finos como eLux e IGEL OS, o cliente Citrix Secure Access e o cliente Citrix EPA são gerenciados pelo administrador. Os usuários não podem instalar o cliente Citrix Secure Access e o cliente Citrix EPA diretamente.

Instalar o cliente Citrix Secure Access e o cliente Citrix EPA para Ubuntu 20.04

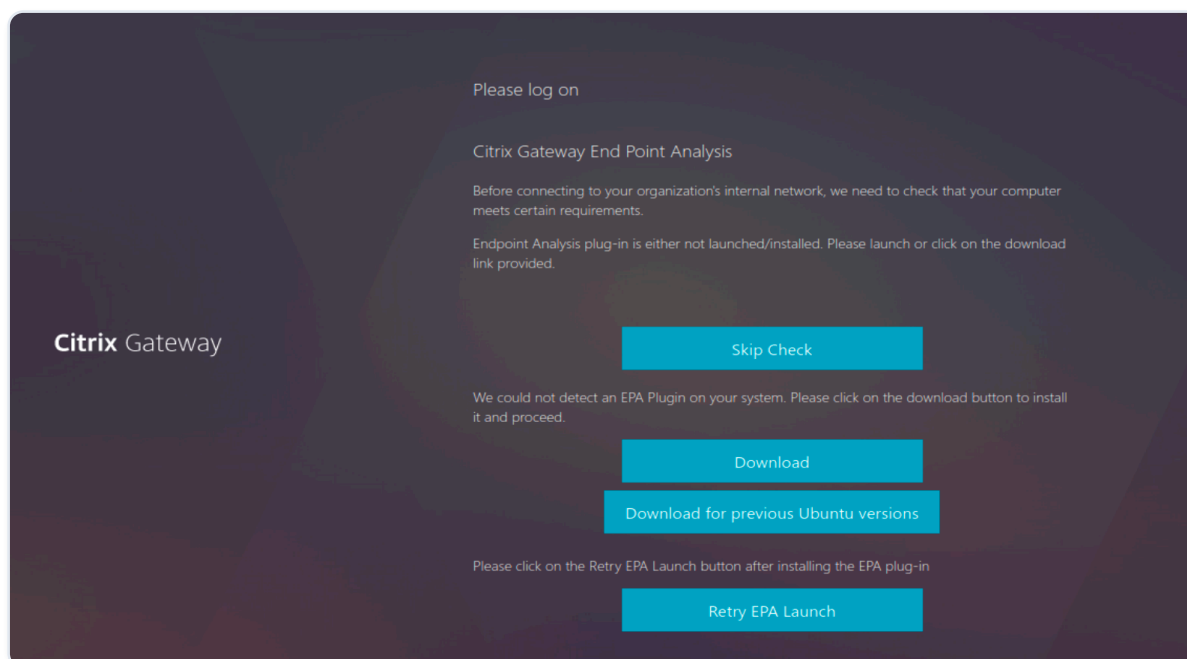
Você pode instalar o cliente Citrix Secure Access e o cliente Citrix EPA usando as seguintes instruções:

1. Baixe o cliente Citrix Secure Access e o cliente Citrix EPA usando uma das seguintes opções:
 - **Opção 1:** Abra um navegador da web e insira a URL do NetScaler Gateway fornecida pelo seu administrador. Clique no botão **Baixar para versões anteriores do Ubuntu** na tela de download que aparece após alguns segundos.

A seguinte tela aparece para o download do cliente Citrix Secure Access:



A seguinte tela aparece para o download do cliente Citrix EPA:



- **Opção 2:** Vá para [Clientes Citrix Secure Access para Ubuntu](#) e clique no botão **Baixar** abaixo da seção Ubuntu 20 para baixar o cliente Citrix Secure Access e o cliente Citrix EPA.

Citrix EPA client 25.5.3 for Ubuntu 20
May 19, 2025
9.9 M - (.deb) [Download File](#)
Checksums
SHA-256 - eb4feda271c9be8e4392b5a8ec733565ae29b5ce4bf32c338352757554824138

Citrix EPA client 25.5.3 for Ubuntu 22/24
May 19, 2025
9.9 M - (.deb) [Download File](#)
Checksums
SHA-256 - 460081aaae9d4625e27a07fcdcdb3646c8ff791d88da1a07200315954bdb7f40

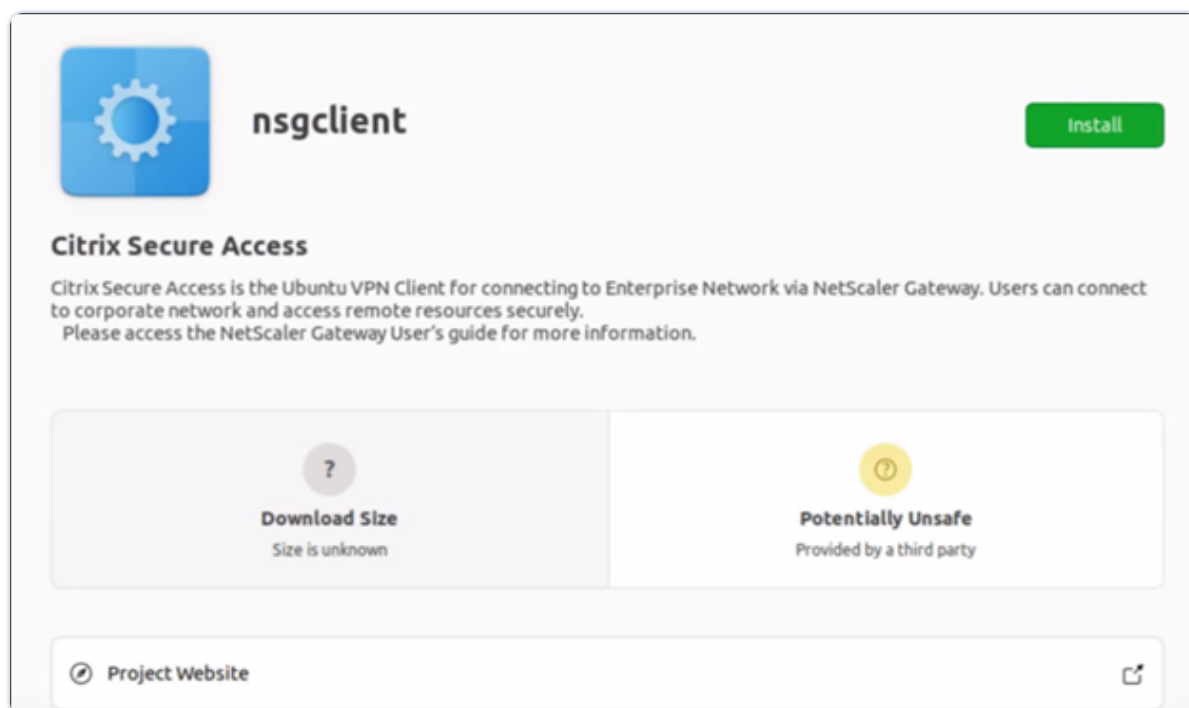
Citrix Secure Access client 25.5.3 for Ubuntu 20
May 19, 2025
4.9 M - (.deb) [Download File](#)
Checksums
SHA-256 - c802dc70e762245150a2741816a4b9b299fb8762ace8f56868ba2f66ae2b1b10

Citrix Secure Access client 25.5.3 for Ubuntu 22/24
May 19, 2025
4.9 M - (.deb) [Download File](#)
Checksums
SHA-256 - 66458c71b6ff6039686939954519c57fdb745b13707473ded9c00de996318766

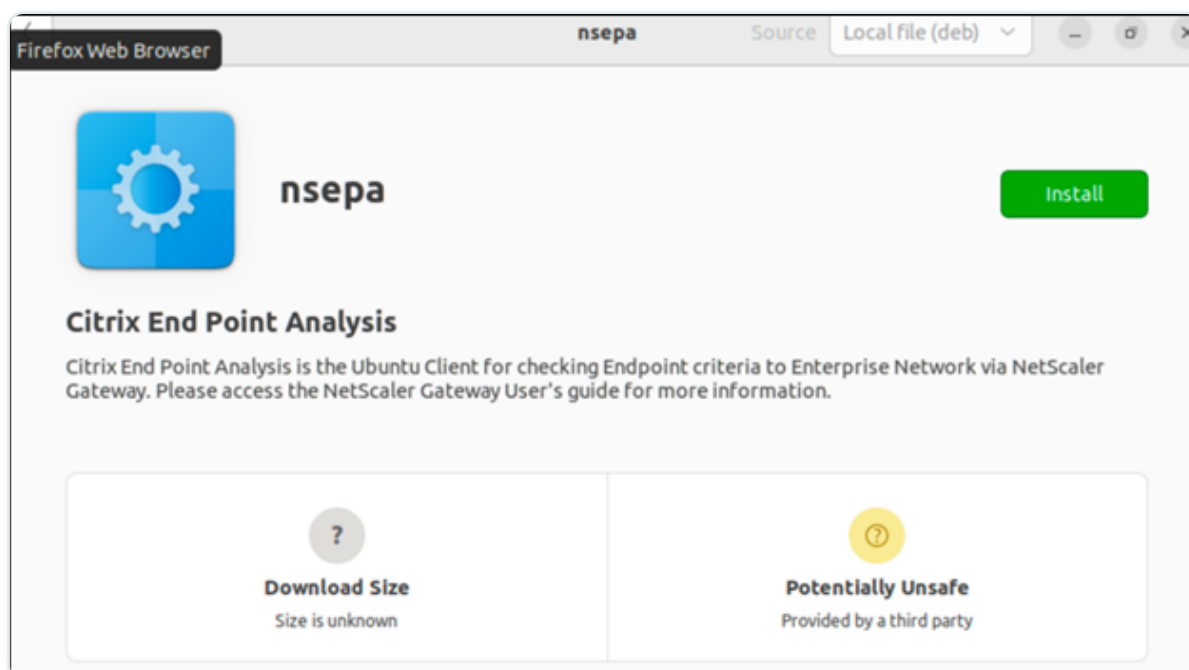
2. Instale o cliente Citrix Secure Access e o cliente Citrix EPA tanto pela GUI quanto usando o terminal Ubuntu.

- Dê um duplo clique no arquivo baixado e instale o cliente Citrix Secure Access e o cliente Citrix EPA.

A seguinte tela aparece quando você dá um duplo clique no cliente Citrix Secure Access baixado:

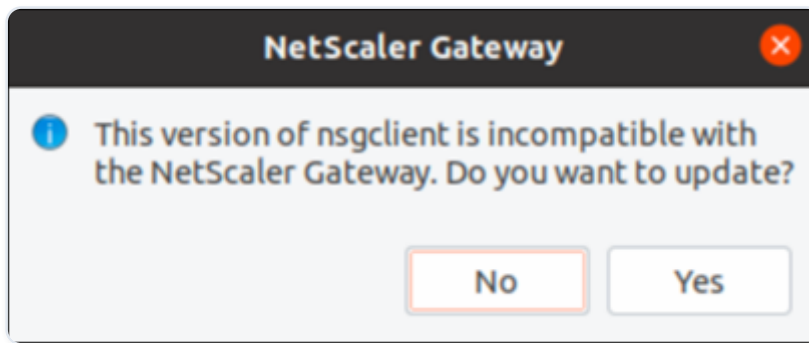


A seguinte tela aparece quando você dá um duplo clique no cliente Citrix EPA baixado:



Se o cliente Citrix Secure Access já estiver instalado, mas não atualizado, você será solicitado a fazer upgrade para a versão mais recente. Clique em **Sim** para fazer upgrade para a versão mais recente, conforme mostrado na tela a seguir:

Este upgrade não se aplica ao cliente Citrix EPA.



- Instale o cliente Citrix Secure Access e o cliente Citrix EPA usando o terminal Ubuntu.

Para instalar o cliente Citrix Secure Access, no terminal, digite:

```
sudo apt install ./nsgclient18_64.deb  
  
sudo apt install -f
```

Para instalar o cliente Citrix EPA, no terminal, digite:

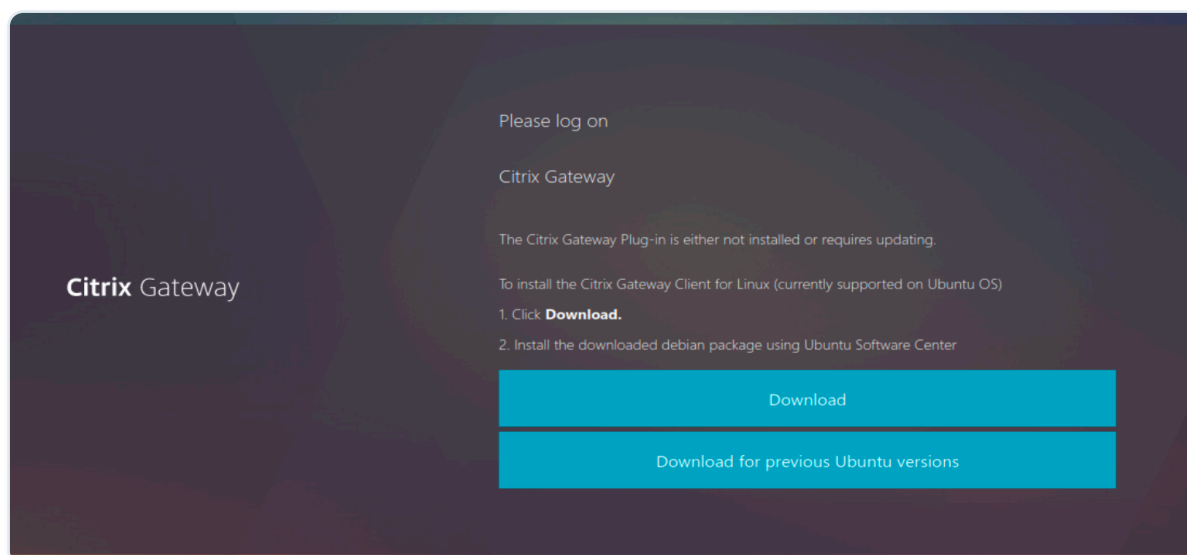
```
sudo apt install ./nsepa18.deb  
  
sudo apt install -f
```

Instalar o cliente Citrix Secure Access e o cliente Citrix EPA para Ubuntu 22.04 e superior

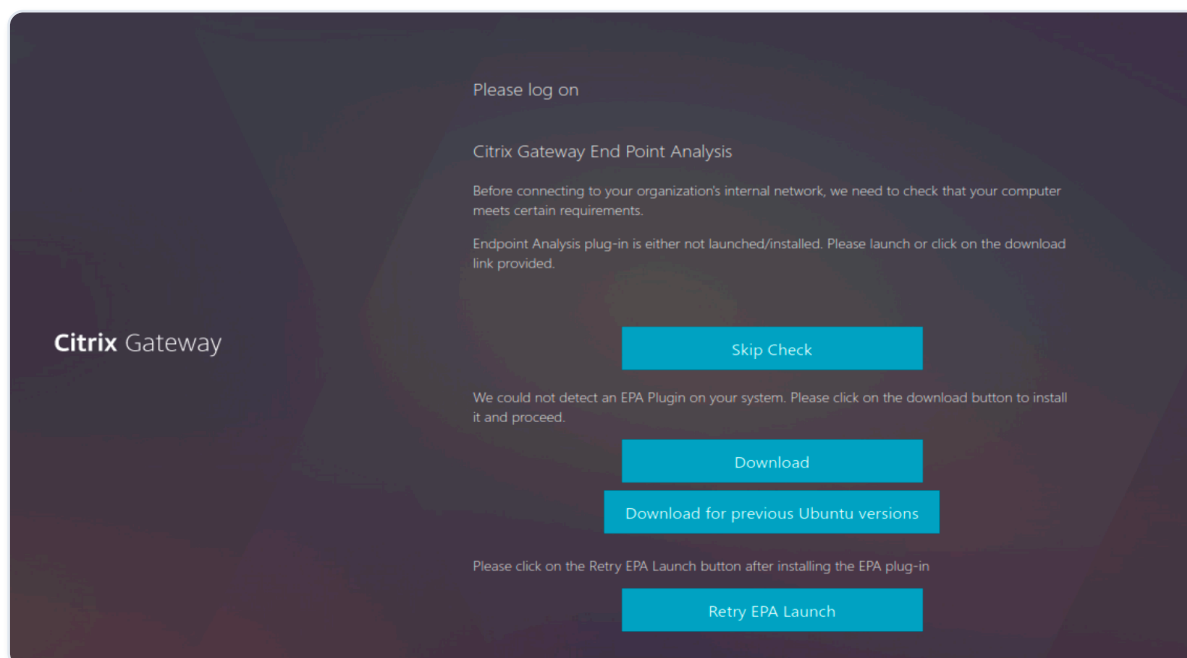
Você pode instalar o cliente Citrix Secure Access e o cliente Citrix EPA usando as seguintes instruções:

1. Baixe o cliente Citrix Secure Access e o cliente Citrix EPA usando uma das seguintes opções:
 - **Opção 1:** Abra um navegador da web e insira a URL do NetScaler Gateway fornecida pelo seu administrador. Clique no botão **Download** na tela de download que aparece após alguns segundos.

A seguinte tela aparece para o download do cliente Citrix Secure Access:



A seguinte tela aparece para o download do cliente Citrix EPA:



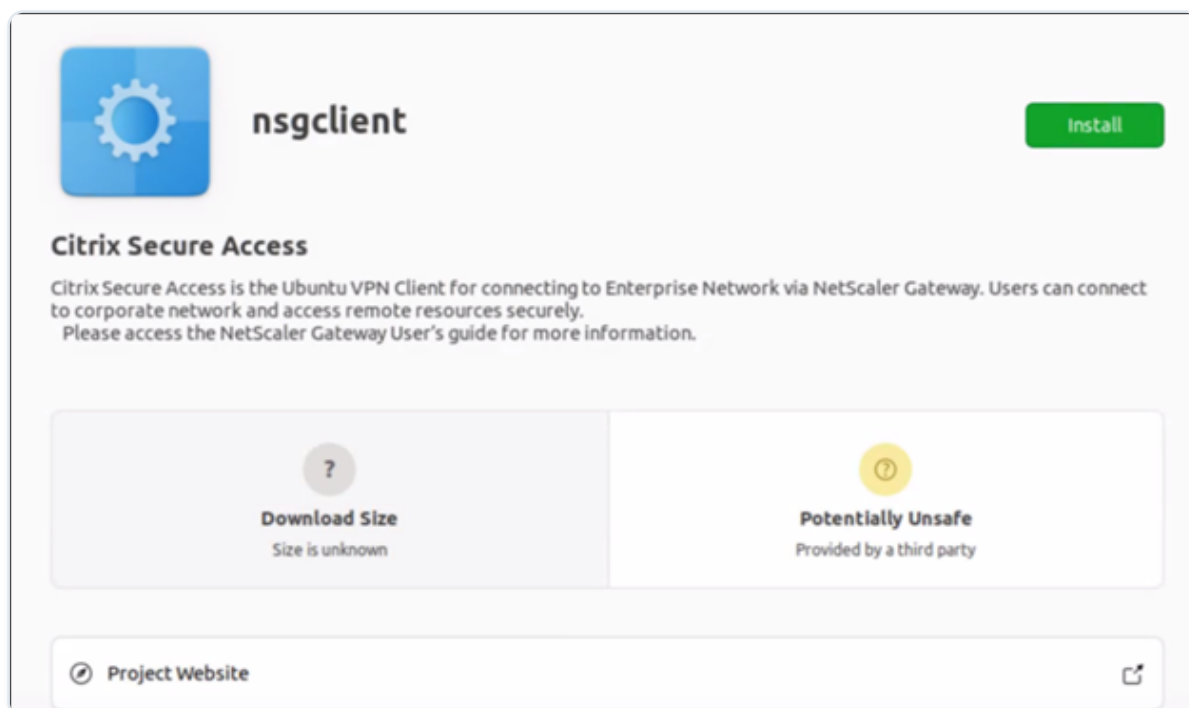
- **Opção 2:** Vá para [Clientes Citrix Secure Access para Ubuntu](#) e clique no botão **Download** abaixo da seção Ubuntu 22/24 para baixar o cliente Citrix Secure Access e o cliente Citrix EPA.

Citrix EPA client 25.5.3 for Ubuntu 20 May 19, 2025 9.9 M - (.deb) Download File Checksums SHA-256 - eb4feda271c9be8e4392b5a8ec733565ae29b5ce4bf32c338352757554824138
Citrix EPA client 25.5.3 for Ubuntu 22/24 May 19, 2025 9.9 M - (.deb) Download File Checksums SHA-256 - 460081aaae9d4625e27a07fcdcdb3646c8ff791d88da1a07200315954bdb7f40
Citrix Secure Access client 25.5.3 for Ubuntu 20 May 19, 2025 4.9 M - (.deb) Download File Checksums SHA-256 - c802dc70e762245150a2741816a4b9b299fb8762ace8f56868ba2f66ae2b1b10
Citrix Secure Access client 25.5.3 for Ubuntu 22/24 May 19, 2025 4.9 M - (.deb) Download File Checksums SHA-256 - 66458c71b6ff6039686939954519c57fdb745b13707473ded9c00de996318766

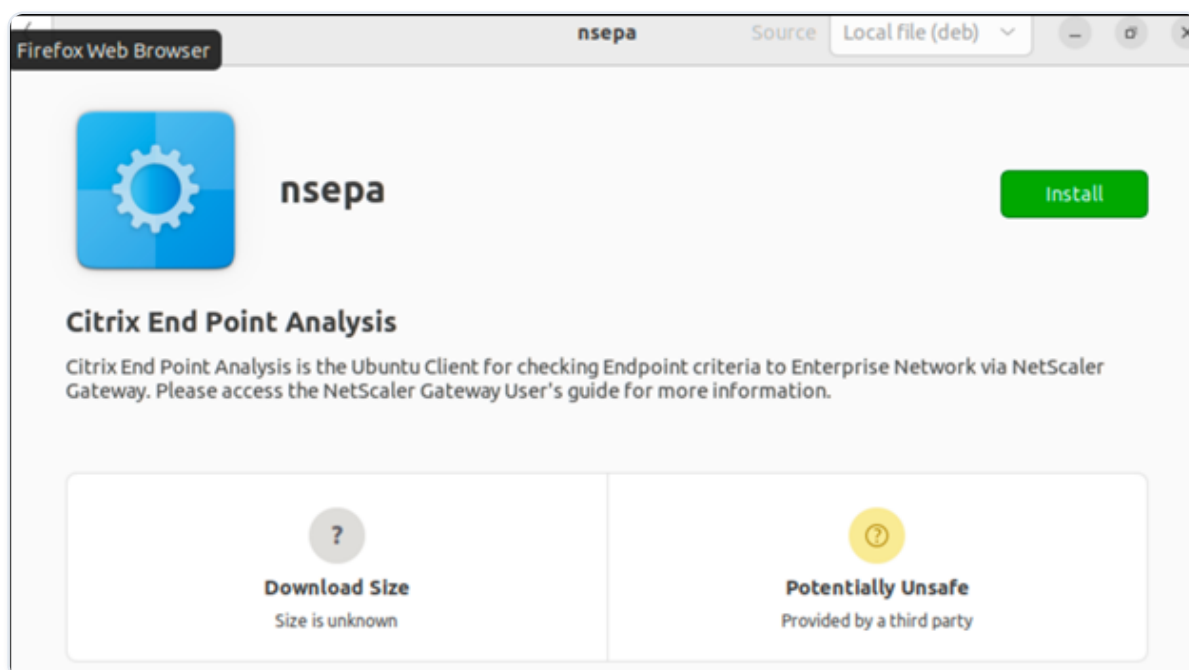
2. Instale o cliente Citrix Secure Access e o cliente Citrix EPA a partir da GUI ou usando o terminal Ubuntu.

- Dê um duplo clique no arquivo baixado e instale o cliente Citrix Secure Access e o cliente Citrix EPA.

A seguinte tela aparece quando você dá um duplo clique no cliente Citrix Secure Access baixado:

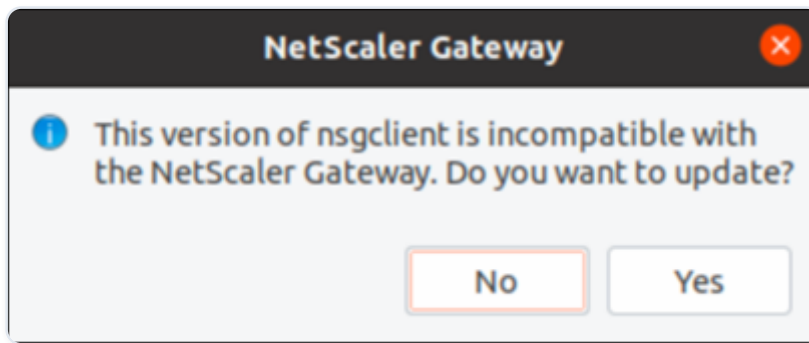


A seguinte tela aparece quando você dá um duplo clique no cliente Citrix EPA baixado:



Se o cliente Citrix Secure Access já estiver instalado, mas não atualizado, você será solicitado a atualizar para a versão mais recente. Clique em **Sim** para atualizar para a versão mais recente, conforme mostrado na tela a seguir:

Esta atualização não é aplicável ao cliente Citrix EPA.



- Instale o cliente Citrix Secure Access e o cliente Citrix EPA usando o terminal Ubuntu.

Para instalar o cliente Citrix Secure Access, no terminal, digite:

```
sudo apt install ./nsginstaller64.deb

sudo apt install -f
```

Para instalar o cliente Citrix EPA, no terminal, digite:

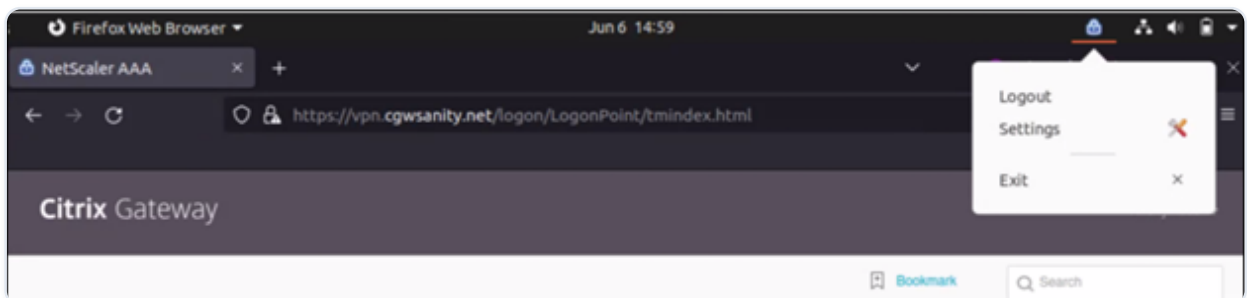
```
sudo apt install ./nsepa.deb

sudo apt install -f
```

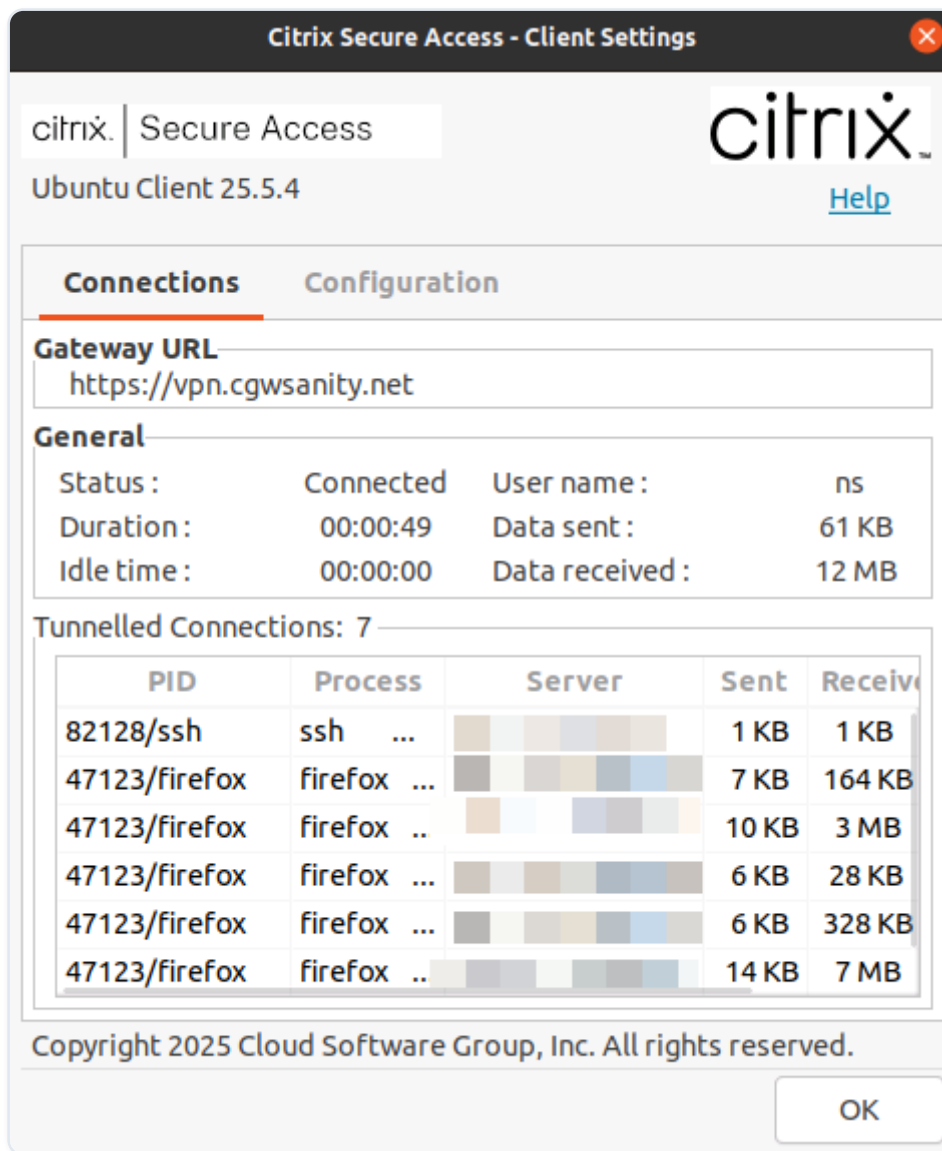
Como usar o cliente Citrix Secure Access para Linux

Insira a URL do NetScaler Gateway no seu navegador para autenticar com o cliente Citrix Secure Access. Assim que a autenticação for bem-sucedida, o navegador solicitará que você inicie o cliente Citrix Secure Access.

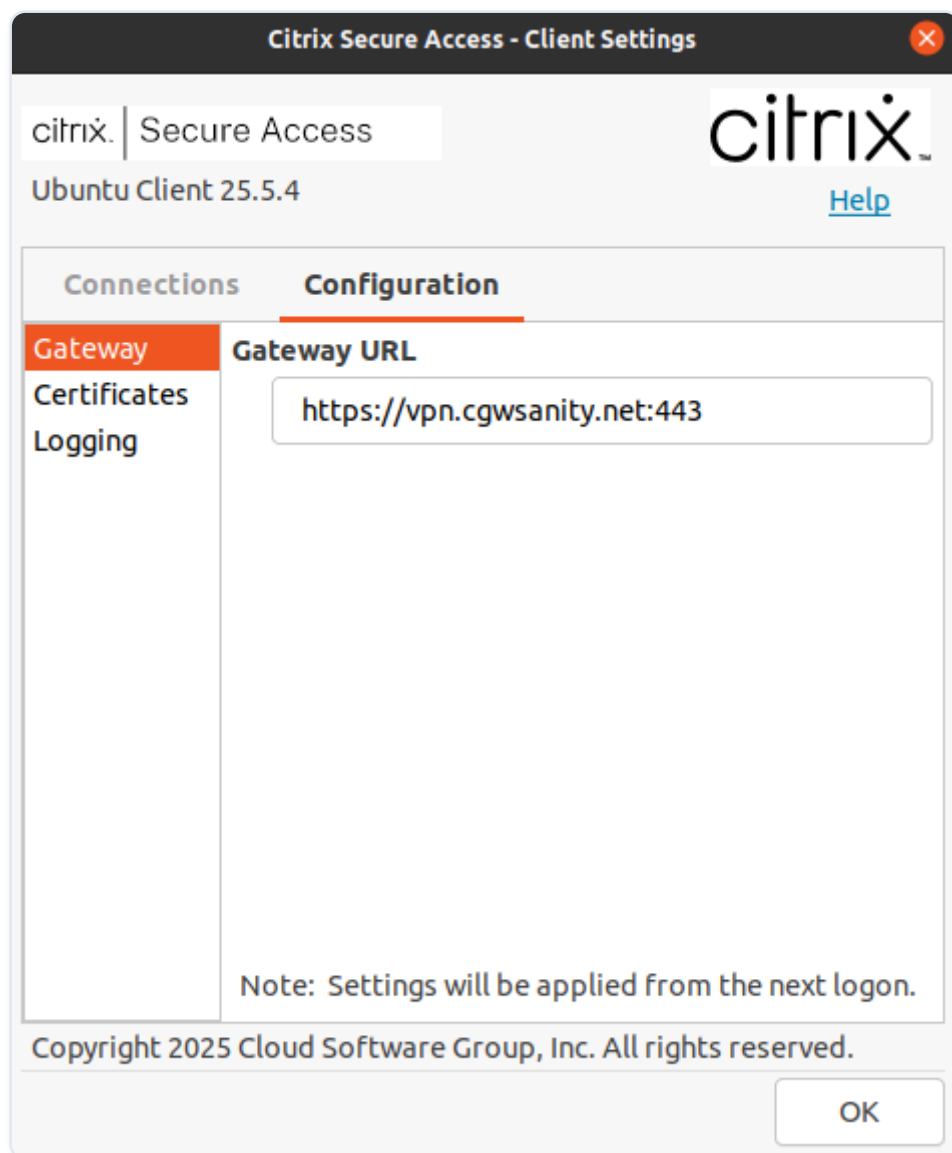
- Selecione o ícone do cliente Citrix Secure Access na barra de tarefas e clique em **Configurações**.



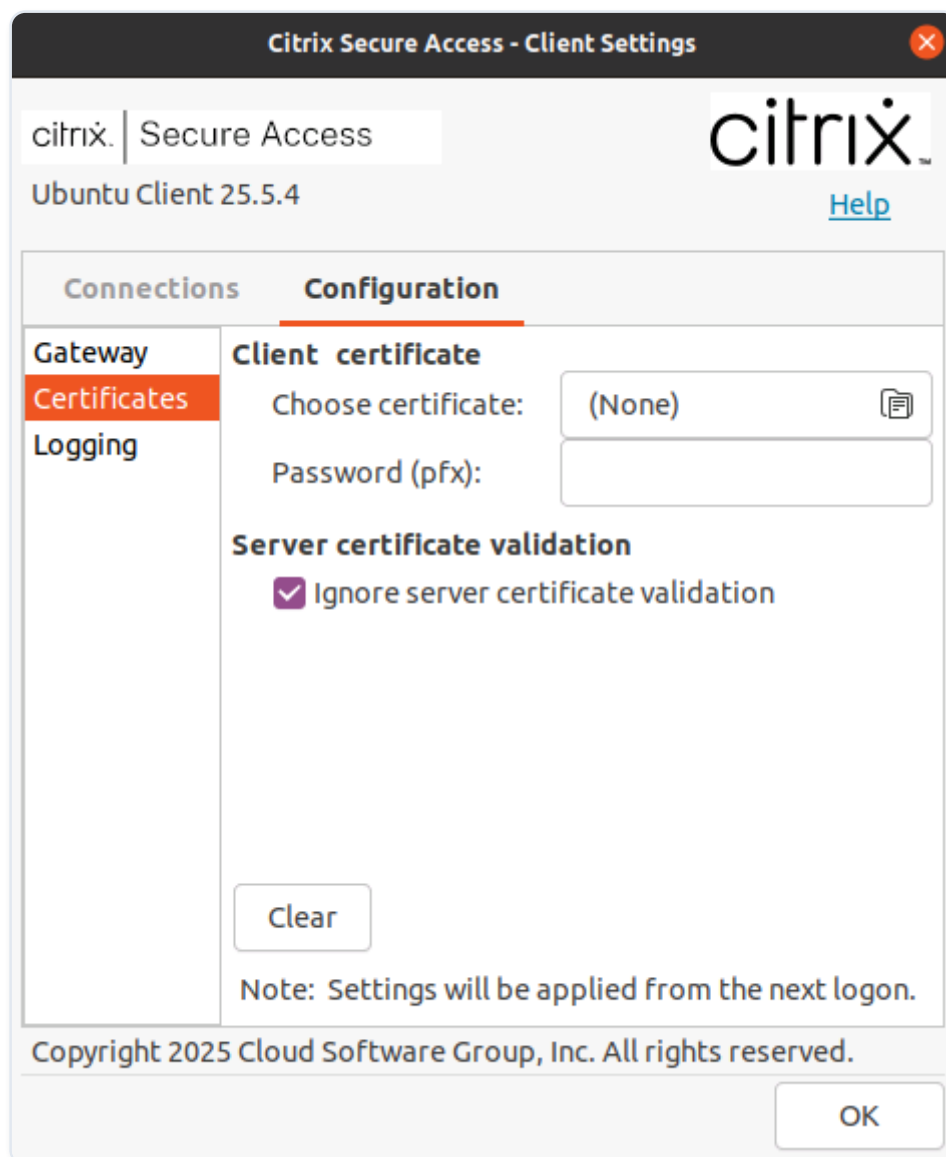
- A guia **Conexões** exibe detalhes como status da conexão, informações do usuário, conexões tuneladas e uso de dados.



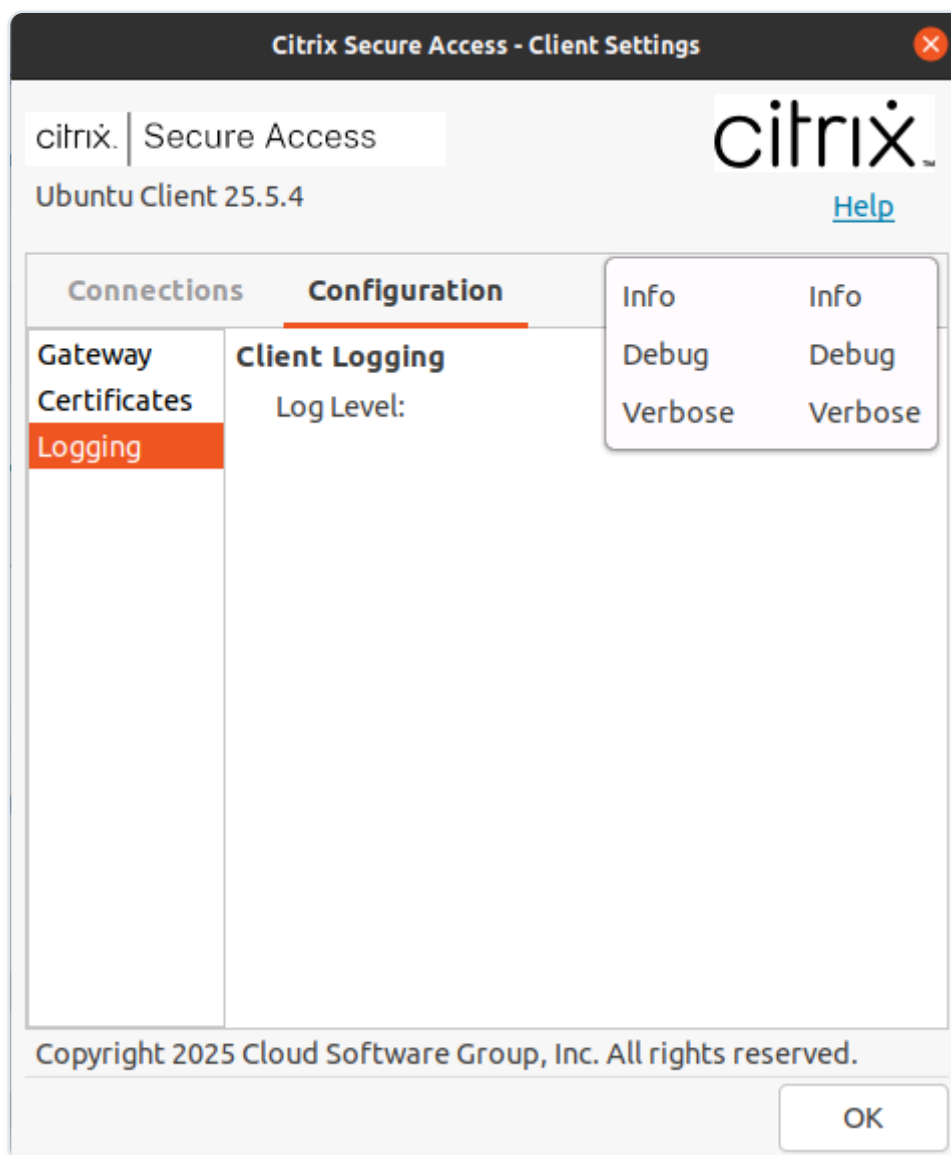
- A guia **Configuração** exibe as informações do NetScaler Gateway, uma opção para carregar um certificado de cliente e opções de registro em log.



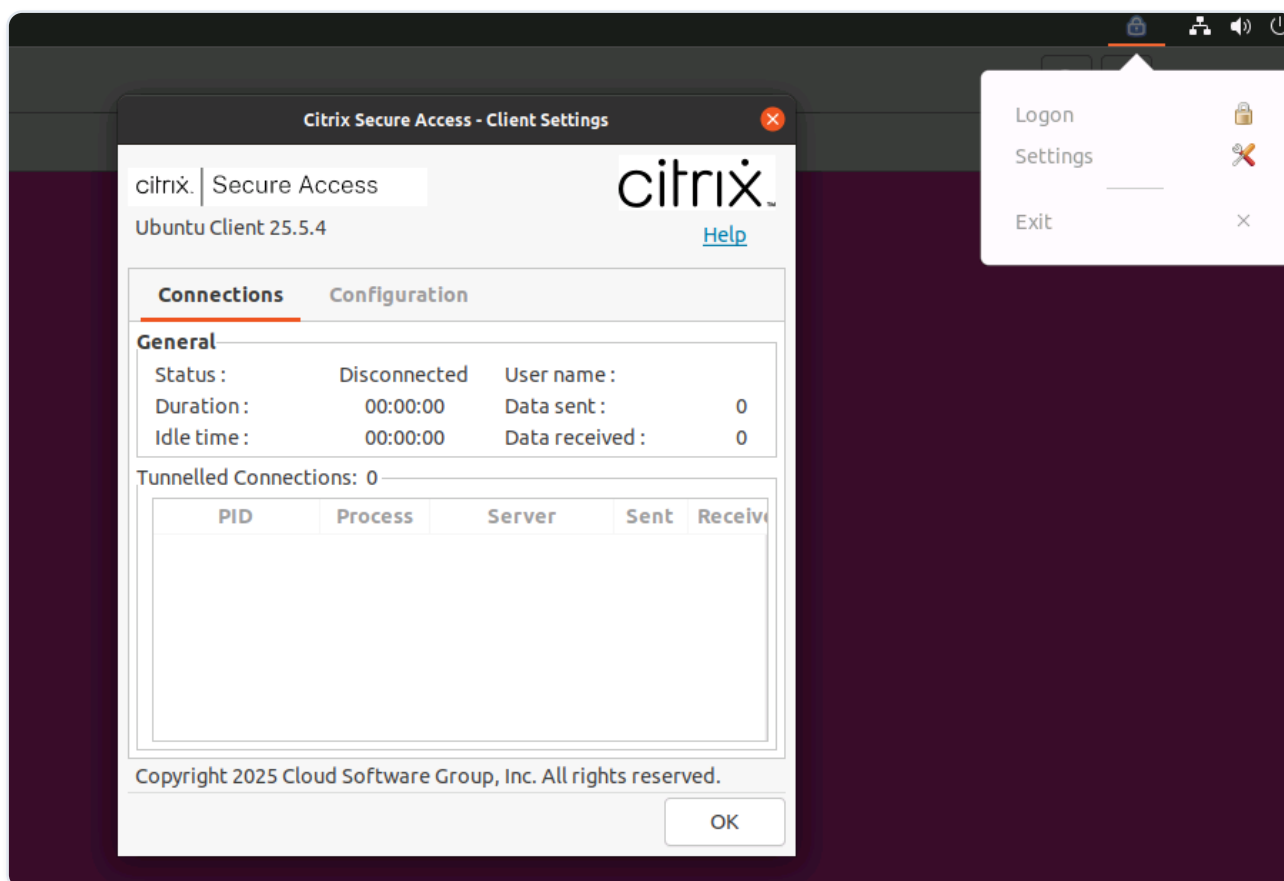
- Certificados: navegar para esta seção para configurar um certificado de cliente. Esta etapa é necessária apenas se o seu administrador tiver fornecido um certificado de cliente para você autenticar com o NetScaler Gateway.



- Registro em log: navegar para esta seção para capturar os logs de depuração. A captura de logs de depuração é uma parte crítica da solução de problemas ou do relato de problemas ao Suporte Citrix.



Alternativamente, você pode iniciar o cliente Citrix Secure Access e clicar em **Logon**. Se você for um usuário iniciante, será solicitado a fornecer a URL do NetScaler Gateway ou a URL do seu espaço de trabalho.



Enviar logs

Os arquivos de log que você envia ao seu administrador são do formato `nsgcepa.txt`, `nsepa.txt`, `nssslvpn.txt` e `epalibv2.log`. Esses arquivos estão no diretório `~/.citrix/`. Eles capturam os seguintes detalhes:

- **Info:** Imprime os logs básicos e de erro.
- **Debug:** Imprime todos os logs. Recomendamos que você selecione esta opção para coletar os logs e compartilhá-los com seu administrador.
- **Verbose:** Imprime os logs detalhados, incluindo mensagens de túnel e informações de configuração.

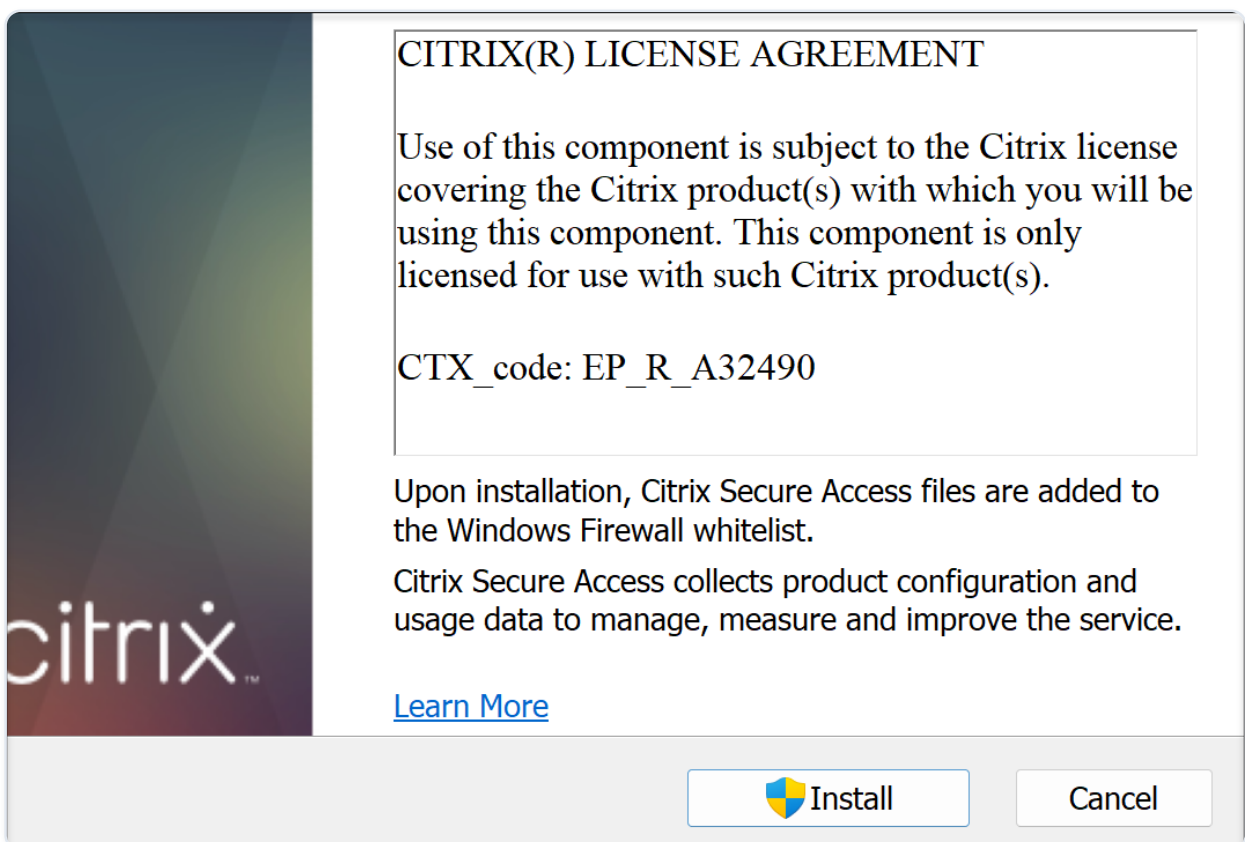
Cliente Citrix Secure Access para Windows

O cliente Citrix Secure Access para Windows é um software cliente VPN que permite acessar dados e aplicativos corporativos remotamente usando o NetScaler Gateway e o Secure Private Access.

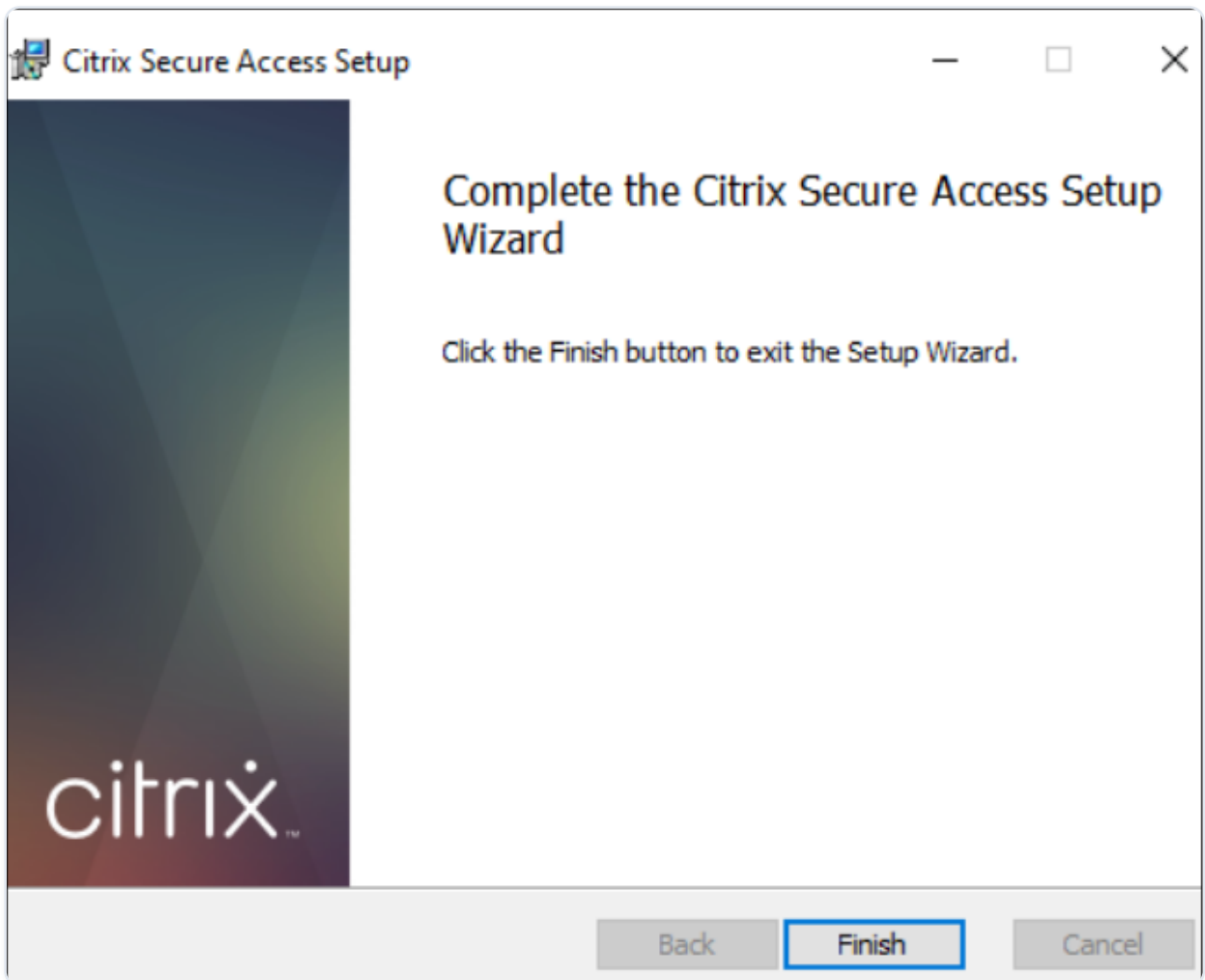
Instalar o cliente Citrix Secure Access para Windows

Você pode instalar o cliente Citrix Secure Access usando as seguintes instruções, que exigem direitos de administrador:

1. Baixe o cliente Citrix Secure Access em [Clientes Citrix Secure Access para Windows](#).
2. Clique em **Instalar** para instalar o cliente em sua máquina Windows. Se você já tiver um cliente Citrix Secure Access existente, ele será atualizado.



3. Clique em **Concluir** para finalizar a instalação.



Como usar o cliente Citrix Secure Access para Windows

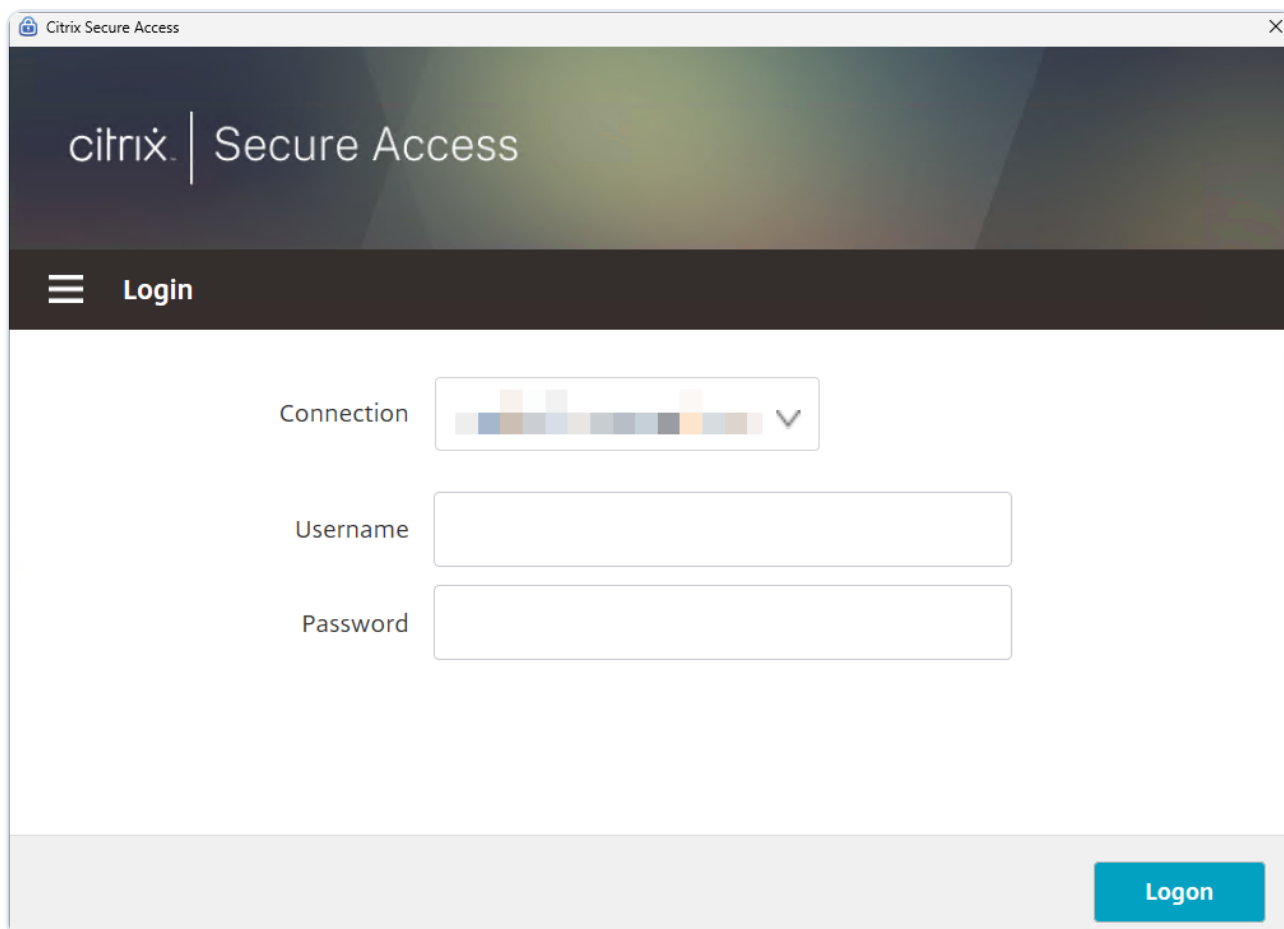
Os usuários iniciantes devem criar uma conexão com o NetScaler Gateway ou Secure Private Access adicionando o URL de conexão, caso seu administrador não o tenha adicionado para seu aplicativo. Para usos subsequentes, você pode se conectar a uma conexão existente, adicionar uma conexão e também editar conexões existentes. Você também pode visualizar os logs e tomar as ações apropriadas.

Adicionar uma conexão

Importante:

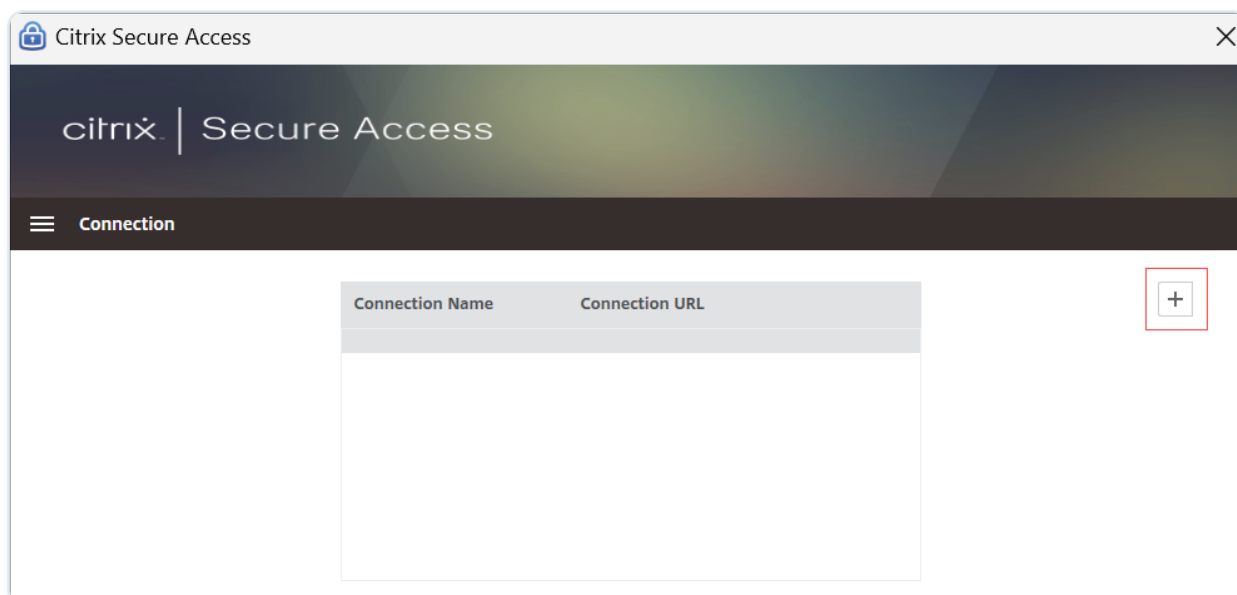
Após a conexão ser adicionada, o cliente Citrix Secure Access solicita autenticação. O prompt depende do método de autenticação configurado no NetScaler Gateway ou Secure Private Access. Pode ser necessário inserir uma senha ou uma senha de uso único. Alternativamente, você pode ser redirecionado para um URL de autenticação SAML.

Se o seu administrador já adicionou uma conexão ao seu aplicativo, selecione a conexão na lista suspensa na página **Home**, insira seu nome de usuário e senha (ou senha de uso único) e clique em **Logon**.

The image shows a screenshot of the Citrix Secure Access application window. The window has a title bar with the text "Citrix Secure Access" and a close button. The main content area features the Citrix logo and the text "Secure Access" at the top. Below this is a dark navigation bar with a hamburger menu icon and the word "Login". The main body of the window contains a "Connection" dropdown menu with a list of colored squares and a downward arrow. Below the dropdown are two input fields labeled "Username" and "Password". At the bottom right of the window is a blue button labeled "Logon".

Se o seu administrador não adicionou o URL de conexão, você deve adicionar uma conexão usando as seguintes etapas:

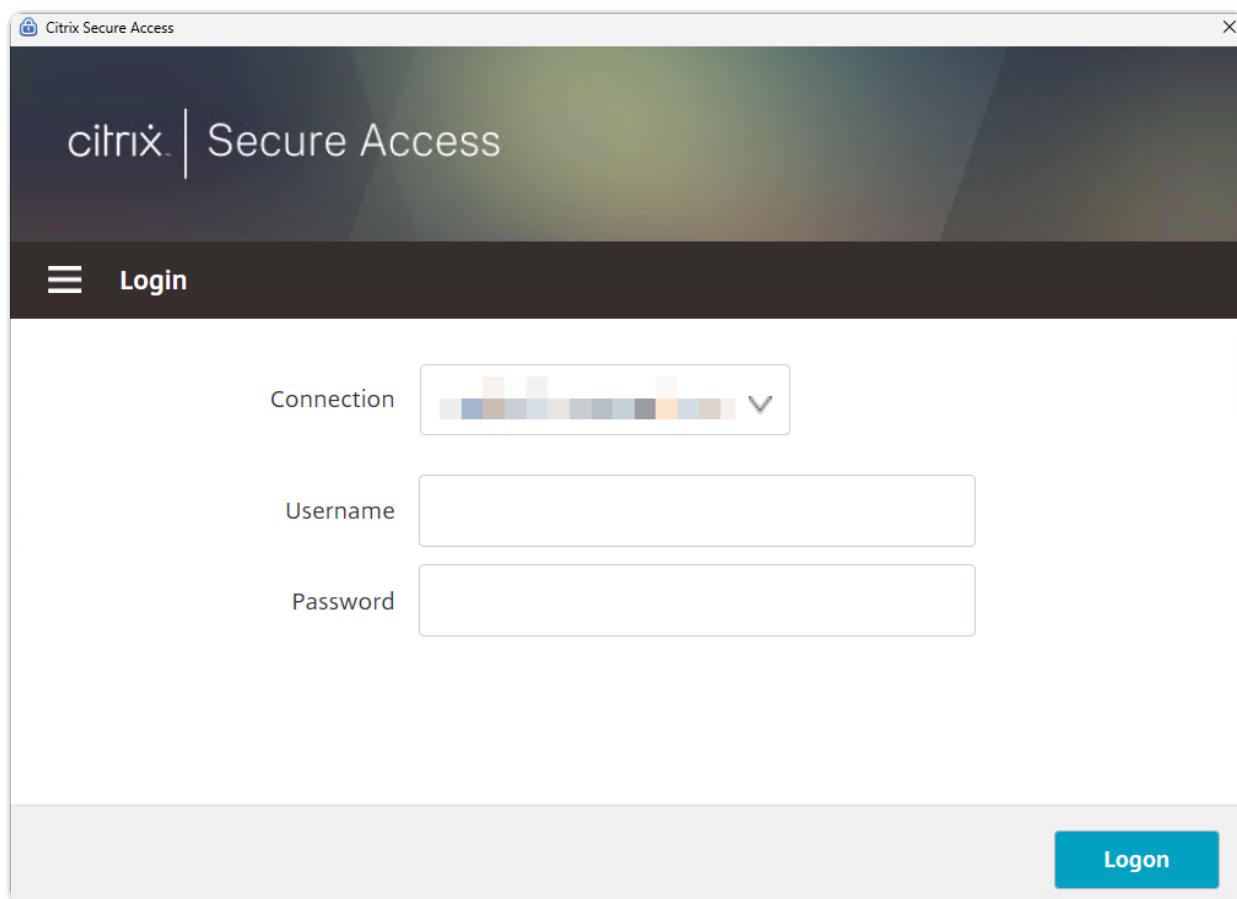
1. Após instalar o cliente Citrix Secure Access para Windows, abra o aplicativo em sua máquina Windows.
2. navegar para a guia **Connection** e clique em **+** para adicionar uma conexão.



3. Insira o URL fornecido pelo seu administrador na caixa de texto **Connection URL**, forneça um nome para a conexão e clique em **Save**.

This screenshot shows the same Citrix Secure Access interface, but now with input fields. The 'Connection URL' and 'Connection Name' labels are positioned to the left of their respective text input boxes. At the bottom right of the page, there is a blue button labeled 'Save'.

4. Uma vez que a conexão é adicionada, navegar para a guia **Home**, selecione a conexão na lista suspensa, insira seu nome de usuário e senha (ou senha de uso único) e clique em **Logon**.

A screenshot of the Citrix Secure Access login window. The window has a title bar with the Citrix logo and the text 'Citrix Secure Access'. The main header area features the 'citrix | Secure Access' logo. Below the header is a dark navigation bar with a hamburger menu icon and the word 'Login'. The main content area contains a 'Connection' dropdown menu with a color-coded bar and a downward arrow. Below this are two text input fields labeled 'Username' and 'Password'. At the bottom right, there is a blue 'Logon' button.

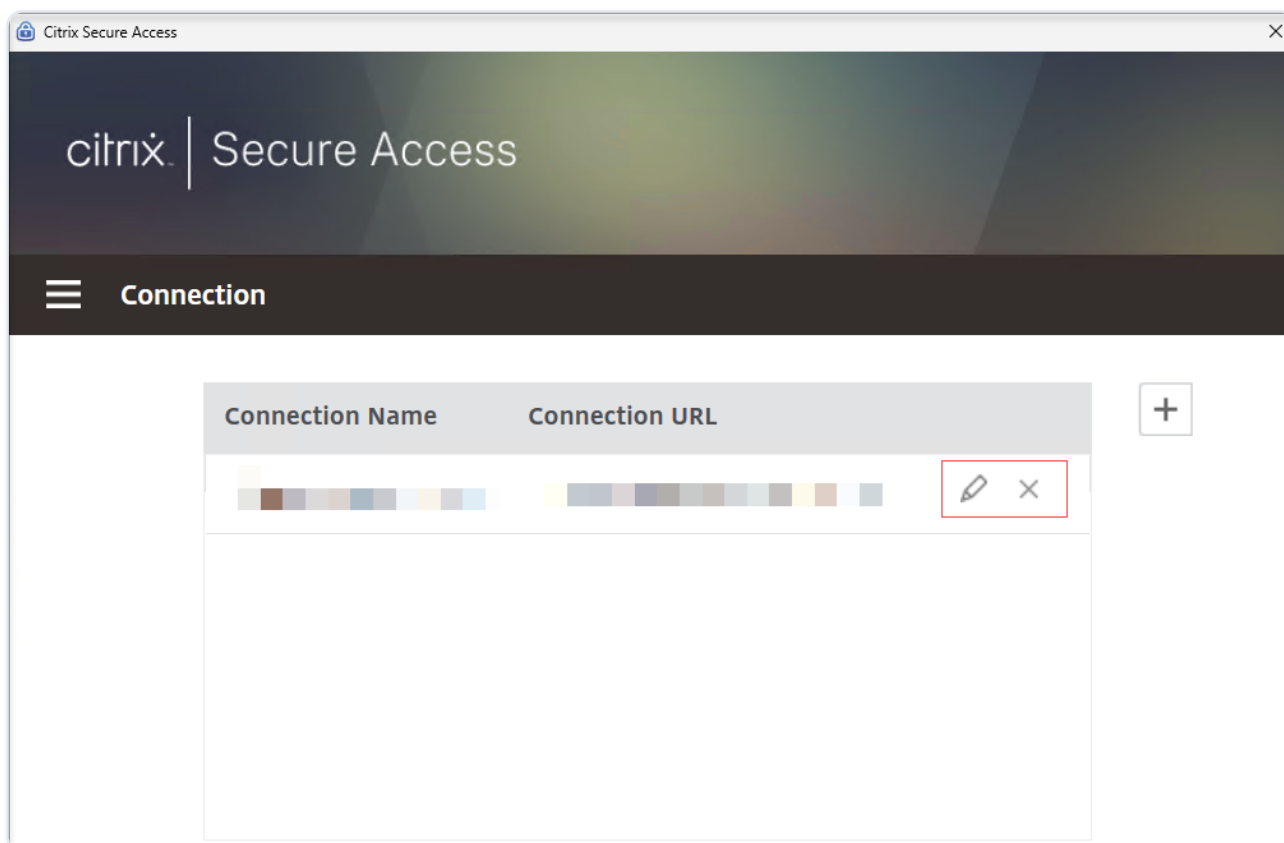
Quando a autenticação for bem-sucedida, você poderá acessar os aplicativos da intranet.

Nota:

Após o login inicial, você não pode conectar ou desconectar manualmente a VPN se o administrador tiver ativado o perfil [Always On](#) ou [Always On before Windows Logon](#) no NetScaler Gateway ou Secure Private Access.

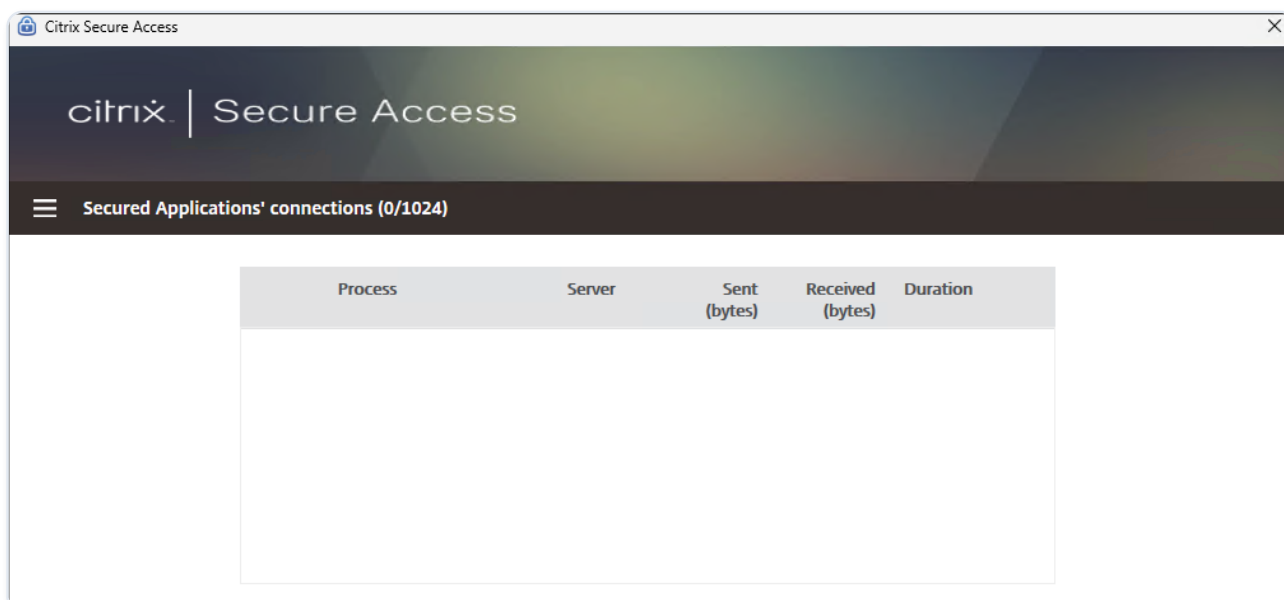
Modificar ou excluir uma conexão existente

Na guia **Conexão**, clique no ícone de edição ou no ícone de cancelamento para modificar ou excluir a conexão existente.



Visualizar aplicativos seguros

Você pode visualizar os aplicativos conectados ao servidor, IP do servidor, dados enviados e recebidos e duração da conexão na guia **Aplicativos Seguros**.



Configurar registro em log

Você pode configurar o nível de log, o tamanho do arquivo e o número máximo de arquivos de log na guia **Registro em Log**.

1. **Selecionar Nível de Log:** O cliente Citrix Secure Access para Windows possui dois níveis de registro em log:
 - **Informações:** Este nível inclui mensagens informativas e eventos relevantes para a execução do programa. Também inclui erros e exceções.
 - **Detalhado:** Este nível inclui todas as mensagens de log relatadas pelo nível **Informações** e outras mensagens que podem ajudar na solução de problemas.
2. **Limite de Tamanho do Arquivo de Log:** Insira o tamanho do arquivo de cada arquivo de log. O valor máximo é 600 MB.
3. **Número Máximo de Arquivos de Log:** Insira o número de arquivos que você deseja adicionar para a coleta de log. O valor máximo é 5.
4. Clique em **Salvar** para salvar as configurações de log adicionadas.

A guia **Log** inclui as seguintes opções:

- **Enviar Arquivos de Log por E-mail:** Envia os arquivos de log para o seu administrador no formato nssslvpn.txt.
- **Iniciar Novo Arquivo de Log:** Cria um novo arquivo de log, geralmente para iniciar um novo registro para uma nova sessão ou após um evento específico para solução de problemas.
- **Coletar Arquivos de Log:** Cria um arquivo zip com todos os arquivos de log do aplicativo. Este arquivo zip é salvo na sua área de trabalho.
- **Abrir Arquivo de Log:** Abre o arquivo csa_nssslvpn*.txt mais recente.

The screenshot displays the Citrix Secure Access web interface. The top navigation bar includes the Citrix logo and the text 'Secure Access'. A dark sidebar on the left contains a hamburger menu icon and the word 'Logging'. The main content area is titled 'Logging' and features a configuration section. This section includes a 'Select Log Level' dropdown menu currently showing 'Info', with a list of options (Info, Verbose (Default)) visible. Below this are two input fields: 'Log Files Size Limit (MB)' and 'Maximum Number of Log Files'. At the bottom of the page, a row of five buttons is present: 'Email Log Files' (blue), 'Start New Log File' (white), 'Collect Log Files' (white), 'Open Log File' (white), and 'Save' (blue).

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.