

Client Citrix Secure Access per dispositivi Android

Il client Citrix Secure Access per Android fornisce la migliore soluzione di accesso alle applicazioni e protezione dei dati offerta da NetScaler Gateway. Ora è possibile accedere in modo sicuro ad applicazioni aziendali critiche, desktop virtuali e dati aziendali da qualsiasi luogo e in qualsiasi momento.

Note:

- A partire dalla versione 23.12.1, Citrix SSO per Android è stato rinominato in Citrix Secure Access. Stiamo aggiornando la nostra documentazione e gli screenshot dell'interfaccia utente per riflettere questo cambio di nome.
- Per istruzioni specifiche per l'amministratore su Citrix Secure Access per Android, vedere [Citrix Secure Access per dispositivi Android](#).

Come usare Citrix Secure Access dal tuo dispositivo Android

Installa Citrix Secure Access dal tuo Play Store. Gli utenti che accedono per la prima volta devono creare una connessione a NetScaler Gateway aggiungendo il server nel caso non-MDM. Per gli utilizzi successivi, puoi connetterti a una connessione esistente o aggiungerne una, e modificare anche le connessioni esistenti, se consentito dall'amministratore in una distribuzione MDM. Puoi anche visualizzare i log e intraprendere le azioni appropriate di conseguenza.

Note:

- Le connessioni distribuite tramite MDM non possono essere modificate.
- Potrebbe esserti richiesto di concedere il consenso [Query all packages](#) all'app Citrix Secure Access. Una volta concesso il consenso, l'app Citrix Secure Access:

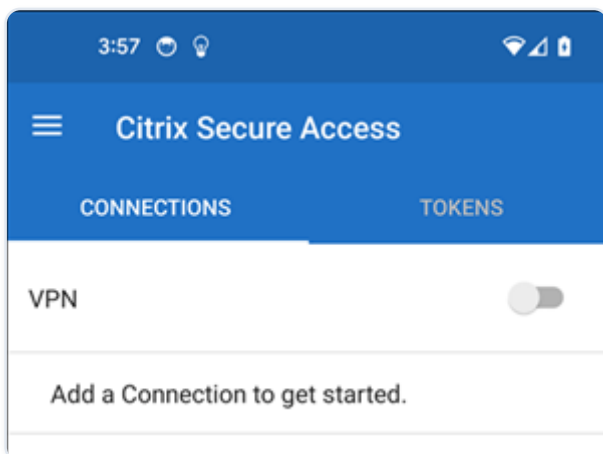
- Riceve la notifica di installazione del pacchetto dal sistema operativo.
- Riavvia la VPN Always On.

Quando ti connetti al tuo profilo VPN per la prima volta, ti viene richiesto di fornire il consenso (richiesto dalle normative di Google) per raccogliere informazioni sul pacchetto installato. Se concedi il consenso, la connessione VPN viene avviata. Se neghi il consenso, la connessione VPN viene interrotta. La schermata di consenso non riappare una volta che il consenso è stato concesso.

Aggiungere una connessione

Nota: Questo passaggio è richiesto solo in un caso non-MDM.

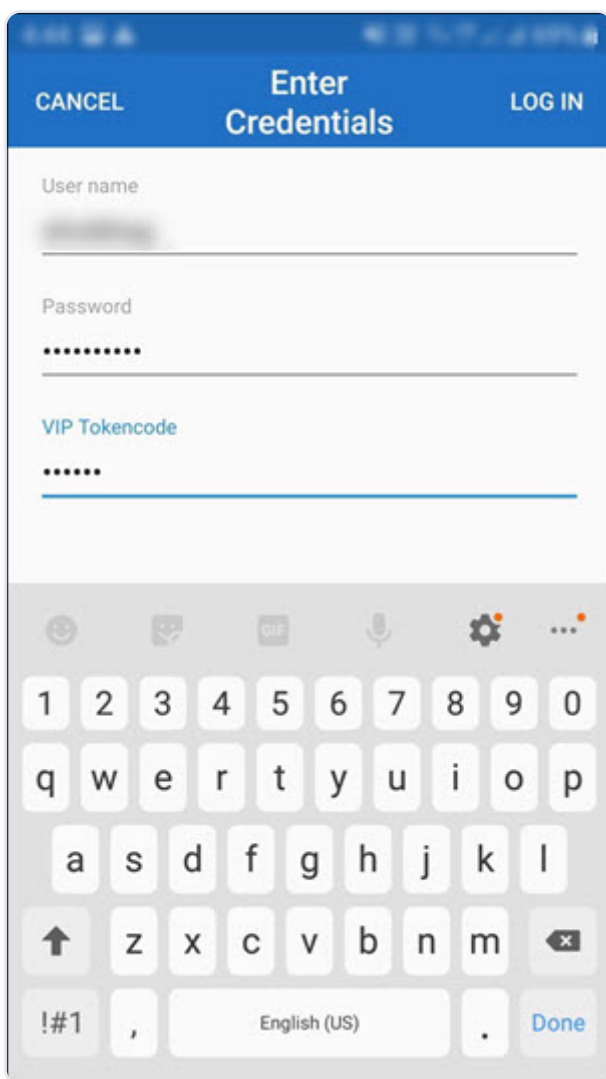
Dopo aver installato Citrix Secure Access e aperto l'app sul tuo dispositivo Android, appare la seguente schermata.



1. Fai clic su + per aggiungere una connessione.
2. Inserisci l'URL di base (ad esempio, [La mia azienda](#)) e il nome per la connessione VPN. Facoltativamente, puoi inserire il nome utente.
3. Fai clic su **Salva** e poi su **Salva e connetti** o **Solo Salva** a seconda dei casi.

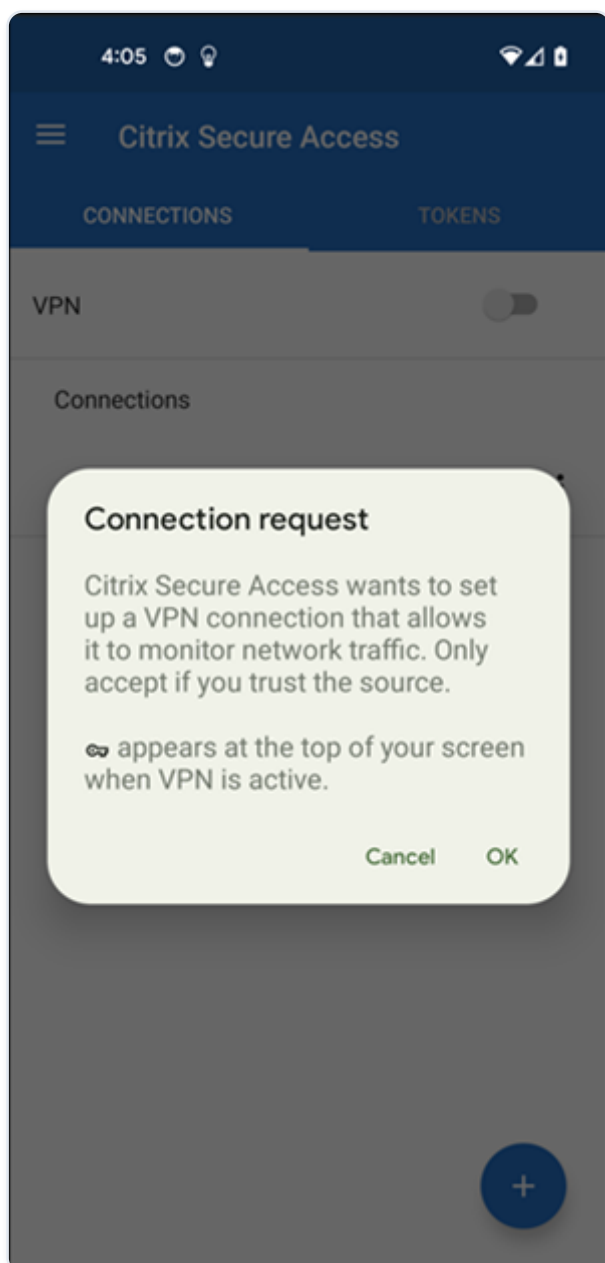
The screenshot shows the 'Add Connection' screen in the Citrix Secure Access mobile app. The interface includes a blue header bar with 'CANCEL', 'Add Connection', and 'SAVE' buttons. Below the header, there are three input fields labeled 'Server', 'Description', and 'User Name'. At the bottom of the 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. Fornisci le credenziali di autenticazione per il tuo server e tocca **LOG IN** o **Done** sulla tastiera.

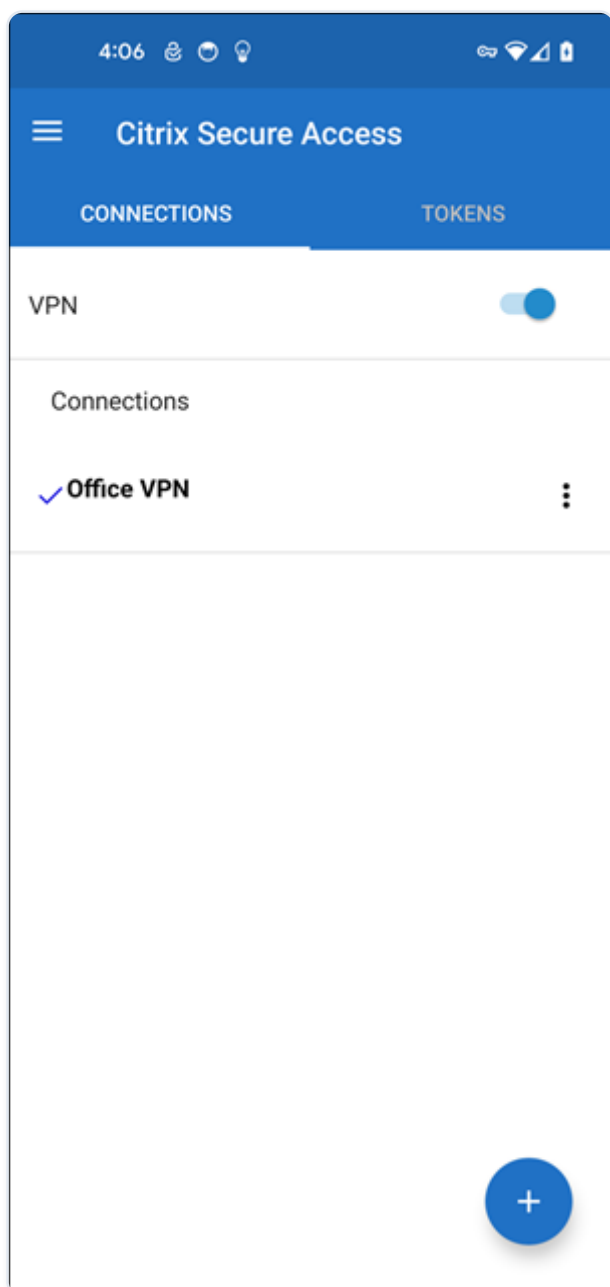


Viene visualizzato il messaggio di richiesta di connessione. Fai clic su **OK**.

Nota: Questo messaggio viene visualizzato solo la prima volta che viene stabilita una connessione VPN da Citrix Secure Access. Se l'utente consente la connessione per la prima volta, questo messaggio non viene più mostrato finché l'utente non disinstalla e reinstalla l'app.



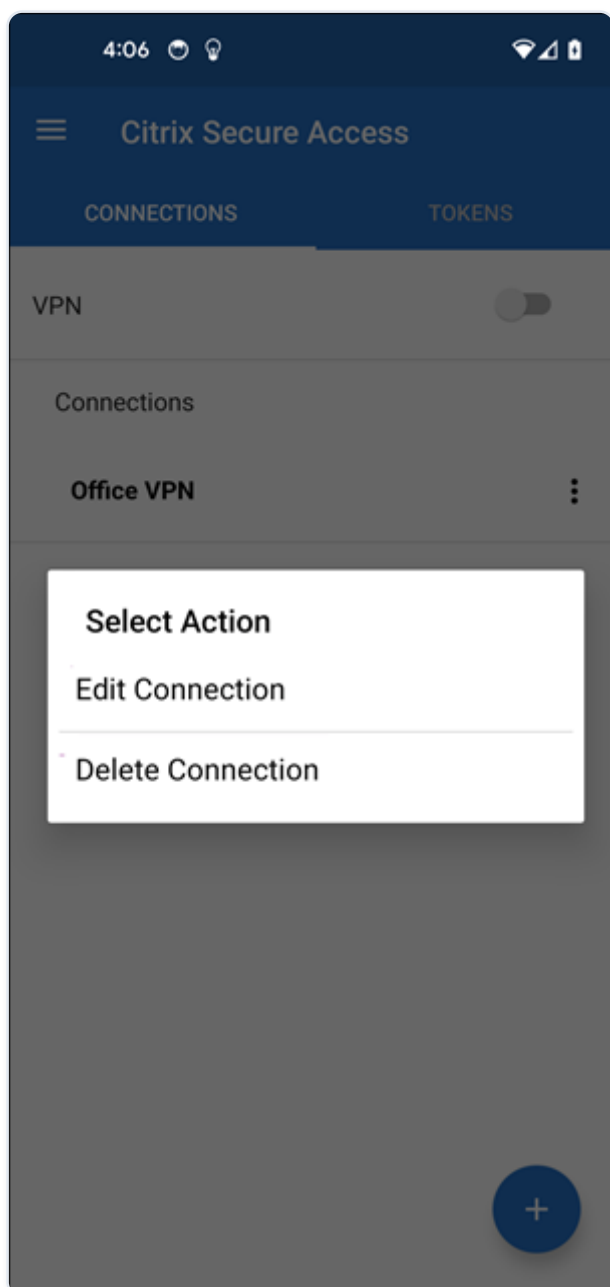
Nota: Per disconnettersi da Citrix Secure Access, disattiva l'**interruttore VPN**.



Modificare o eliminare una connessione esistente

È possibile modificare o eliminare una connessione dopo aver effettuato il logout da Citrix Secure Access.

Tieni premuto il nome del server e seleziona **Modifica connessione** o **Elimina connessione**.

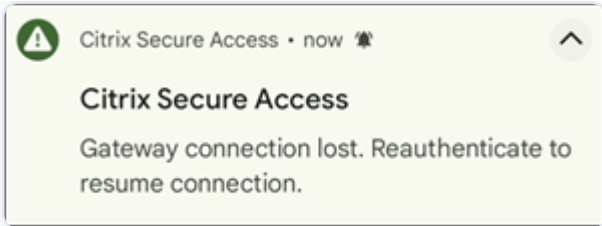


Riconnettersi a NetScaler Gateway dopo un errore di connessione VPN - Anteprima

Il client Citrix Secure Access per Android richiede di eseguire nuovamente l'autenticazione con NetScaler Gateway quando una connessione VPN viene persa. Si riceve una notifica sull'interfaccia utente e nel pannello delle notifiche del dispositivo Android che indica che la connessione a NetScaler Gateway è stata persa e che è necessario eseguire nuovamente l'autenticazione per riprendere la connessione.

Nota:

Questa funzionalità è in anteprima.



Consentire l'accesso alla rete locale su Android 17 e versioni successive

A partire dalla versione 26.08.1 di Citrix Secure Access per Android, agli utenti che installano, reinstallano o aggiornano l'applicazione su Android 17 e versioni successive viene richiesto di consentire l'accesso alla rete locale. Se l'accesso viene negato, alcuni servizi di rete locali, come le stampanti Wi-Fi, potrebbero non essere disponibili all'inizio di una sessione VPN.

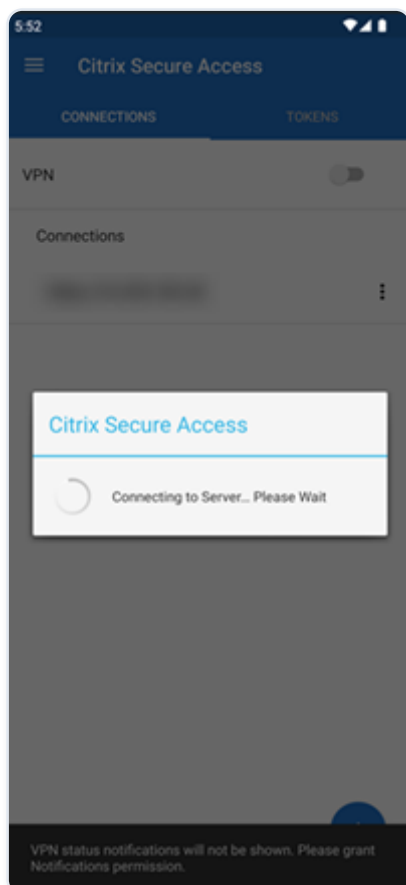
Si consiglia agli amministratori MDM di pre-concedere questa autorizzazione all'applicazione Citrix Secure Access.

Ricevere o bloccare le notifiche su Android 13 e versioni successive

A partire dalla versione 23.12.1 di Citrix Secure Access per Android, agli utenti che installano, reinstallano o aggiornano l'applicazione su Android 13 e versioni successive viene richiesto di consentire le notifiche. Se le notifiche vengono negate, gli utenti non ricevono lo stato della VPN o le notifiche push da Citrix Secure Access.

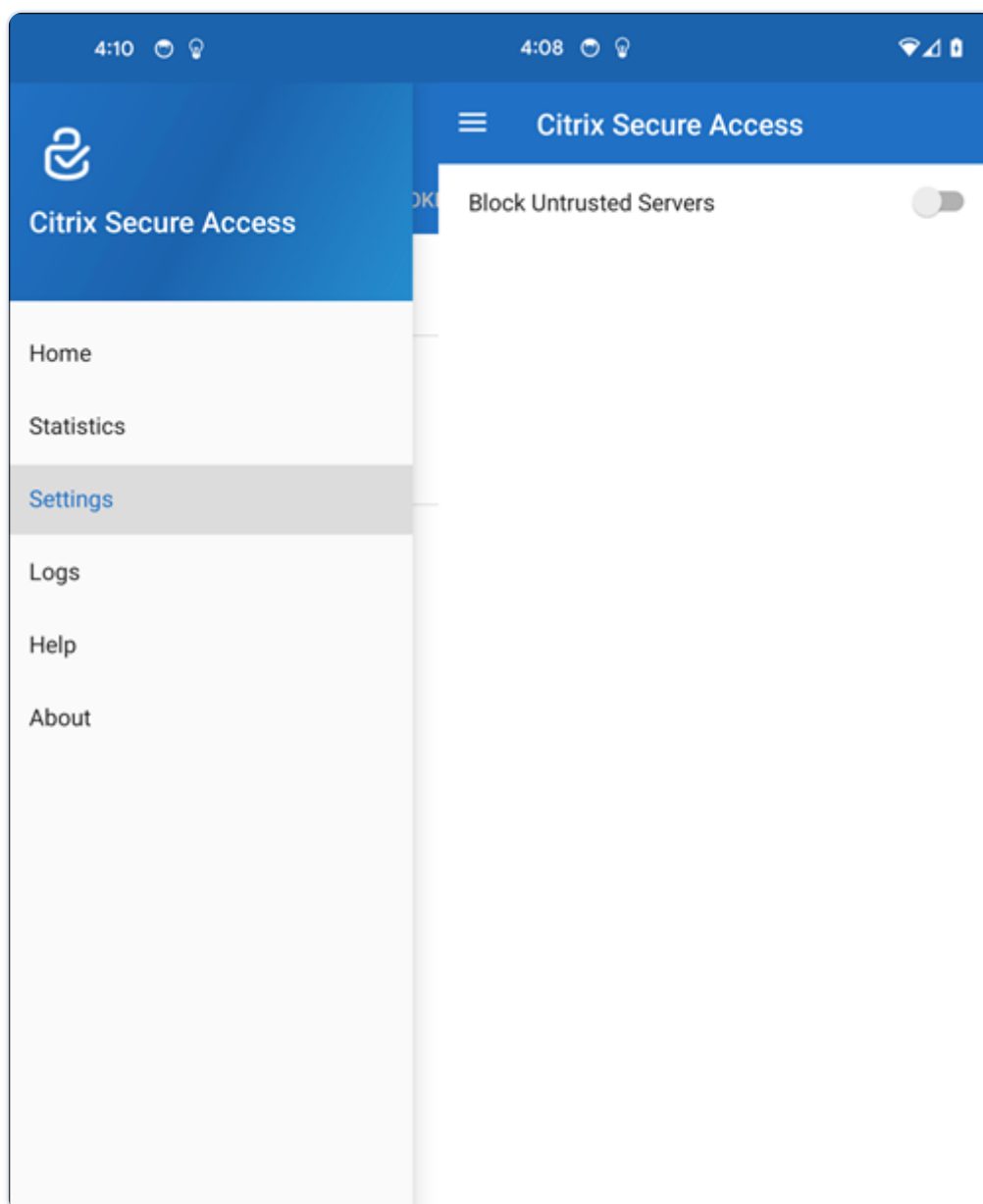
È possibile accedere a **Impostazioni > Notifiche** sul dispositivo Android per modificare le autorizzazioni di notifica.

Nell'esempio seguente, le notifiche sullo stato della VPN sono state disabilite.



Bloccare i server non attendibili

Citrix Secure Access non si connette ai server non attendibili, per impostazione predefinita. I server non attendibili si riferiscono a server che utilizzano certificati autofirmati o che non dispongono di un certificato radice attendibile per il gateway. Per consentire questi tipi di connessioni, è possibile disattivare l'interruttore **Blocca server non attendibili** impostandolo su **OFF**.



Abilitare i log di debug

L'acquisizione dei log di debug è una parte fondamentale della risoluzione dei problemi o della segnalazione di problemi al supporto Citrix. Attivare l'interruttore **Debug Logging** (Registrazione debug) impostandolo su **ON** per abilitare la registrazione debug per Citrix Secure Access. È possibile inviare i log via e-mail durante la risoluzione dei problemi di connessione utilizzando il collegamento **Email Logs** (Invia log via e-mail).

Visualizza log di debug(</en-us/citrix-sso/media/sso-andr-logs.png>)

Visualizza statistiche

È possibile visualizzare le statistiche di connessione quando la VPN è connessa.

Visualizza statistiche di connessione(</en-us/citrix-sso/media/sso-andr-stats.png>)

Token password

È possibile aggiungere un token password a 6 cifre come autenticazione a secondo fattore. Questo codice utilizza il protocollo password monouso basato sul tempo per generare il codice OTP.

È possibile aggiungere un token password manualmente o registrarne uno utilizzando il metodo di scansione del codice QR. L'autenticazione a secondo fattore tramite notifiche push non è abilitata se si sceglie di inserire il token manualmente.

Registra un token password

1. Accedere alla pagina di gestione del PIN monouso dell'organizzazione nel browser Web su un computer desktop o portatile.
2. Fare clic su **Aggiungi dispositivo**.
3. Immettere un nome per il dispositivo, quindi fare clic su **Vai**.

Viene generato un codice QR.

Aggiungere un token password scansionando il codice QR nel browser

1. Passare alla scheda **Token** nella vista **Home**.
2. Toccare **+** e toccare **Scansiona codice QR**.
3. Punta la fotocamera sul codice QR nel tuo browser.

Citrix Secure Access compila automaticamente il nome del dispositivo e la chiave segreta.

In alternativa, è possibile inserire manualmente la chiave segreta che appare sopra il codice QR.

Citrix Secure Access convalida il codice QR e quindi si registra con il gateway per le notifiche push. Se non ci sono errori nel processo di registrazione, il token viene aggiunto correttamente alla scheda dei token.

Nota:

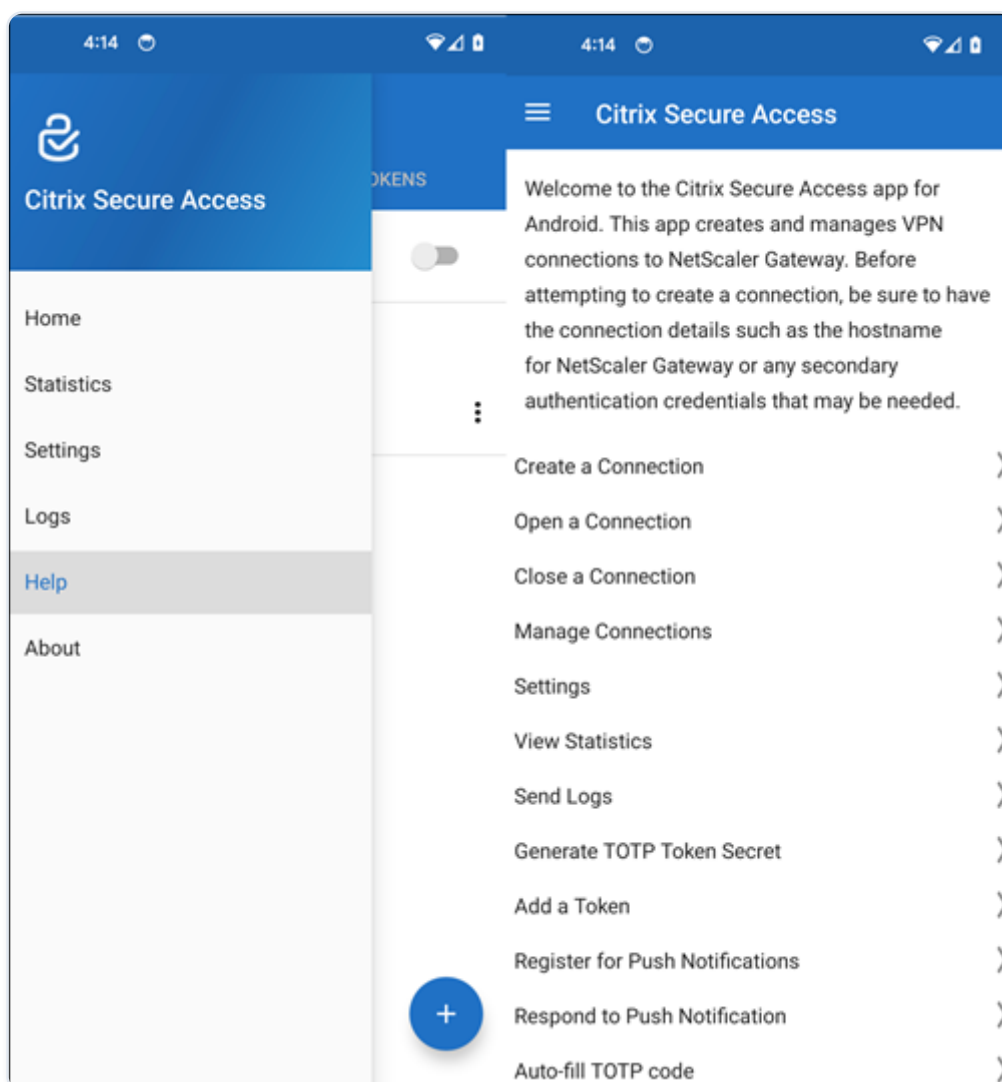
- È necessario consentire le autorizzazioni della fotocamera affinché Citrix Secure Access possa acquisire il codice QR.
- È necessario abilitare il PIN/password del dispositivo sul proprio dispositivo.

Aggiungere un token password manualmente

1. Passare alla scheda **Token** nella vista **Home**.
2. Toccare + e toccare **Inserisci manualmente**.
3. Inserire il nome del dispositivo e la chiave segreta come appaiono sul token password generato nel browser.

Argomenti della guida

Per maggiori informazioni su come utilizzare Citrix Secure Access, consultare la **Guida**.



Connettersi alla rete aziendale utilizzando Citrix Secure Access configurato in un ambiente Intune

Nota:

Per istruzioni specifiche per l'amministratore su Citrix Secure Access per Android, vedere [Citrix Secure Access per dispositivi Android](#).

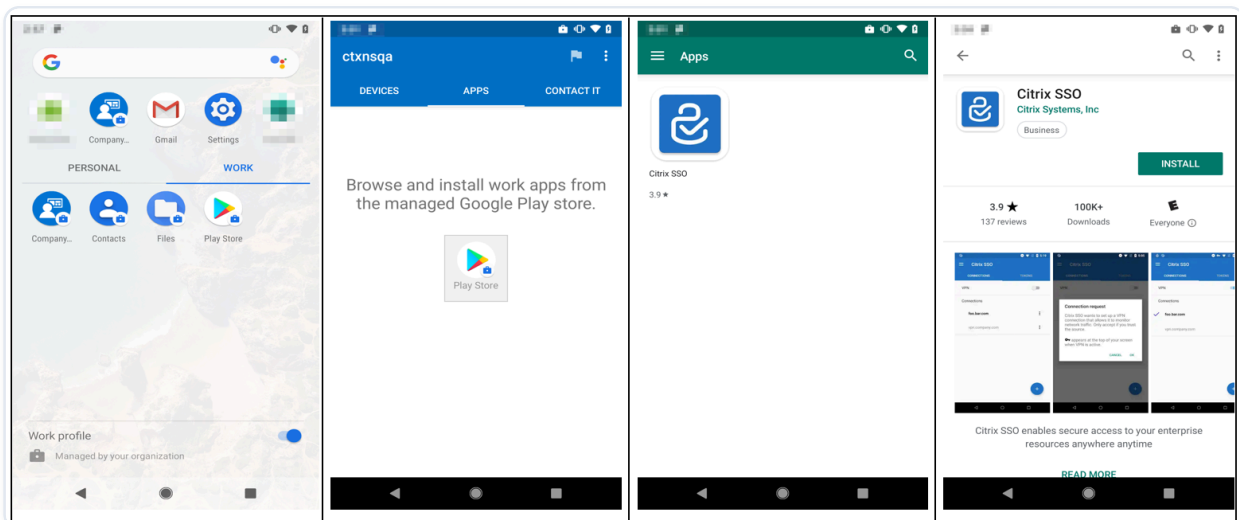
Questo argomento contiene i dettagli sulla connessione alla rete aziendale utilizzando il client Citrix Secure Access configurato nell'ambiente Microsoft Intune Android Enterprise.

Presupposti:

- Il dispositivo è stato registrato in Intune utilizzando l'app Intune Company Portal.
- Il profilo di lavoro per l'utente è configurato sul dispositivo.

1. Aprire l'app **Intune Company Portal** sul dispositivo dal profilo di lavoro.
2. Fare clic sul menu con i tre puntini per aprire le impostazioni dell'app e scorrere fino alla fine della schermata. Toccare **SYNC** per sincronizzare con il server Intune e quindi tornare alla schermata principale dell'app.
3. Toccare la scheda **APPS** e toccare il link **Managed Google Play Store**.

Viene visualizzato l'elenco delle app approvate per l'utente.



4. Toccare **Citrix Secure Access**.

Il client Citrix Secure Access viene visualizzato nel Managed Google Play Store.

5. Toccare **INSTALLA**.
6. Torna all'elenco delle app del profilo di lavoro. Citrix Secure Access viene aggiunto all'elenco delle app installate.
7. Tocca l'icona di Citrix Secure Access nell'elenco delle app del profilo **LAVORO** per aprirla.

Installa il client Citrix Secure Access e concedi le autorizzazioni(/en-us/citrix-ssso/media/citrix-ssso-andr-intune1.png)

Citrix Secure Access si apre. Ti viene chiesto di consentire o negare l'autorizzazione a comunicare in modo sicuro con la rete interna della tua azienda.

8. Tocca **CONSENTI** per concedere l'autorizzazione. Citrix Secure Access si chiude se scegli **NON CONSENTIRE** e non puoi utilizzare il client Citrix Secure Access.

Nota:

Potrebbe esserti chiesto di consentire o negare l'**autorizzazione a gestire ed effettuare chiamate telefoniche** (se non già concessa tramite Intune). Tocca **Consenti** per concedere l'autorizzazione. Puoi negare questa autorizzazione, ma se è richiesto il controllo NAC di Intune per l'autenticazione del dispositivo su NetScaler Gateway, non potrai connetterti alla rete interna della tua azienda finché non concederai questa autorizzazione.

9. La **VPN aziendale** (o il nome scelto nella configurazione di Citrix Secure Access in Intune) è elencata nella sezione Connessioni gestite della scheda **CONNESSIONI**. Tocca questa connessione, ti verranno richieste le credenziali per l'autenticazione con NetScaler Gateway.
10. Fornisci le credenziali per l'autenticazione con NetScaler Gateway e tocca **ACCEDI**.

Inserisci le credenziali e consenti le richieste di connessione(/en-us/citrix-ssso/media/citrix-ssso-andr-intune1.png)

Potrebbe esserti chiesto di selezionare un certificato se l'autenticazione tramite certificato client è configurata su NetScaler Gateway. Puoi fornire l'accesso al certificato.

11. Il sistema Android ti chiede di consentire la **richiesta di connessione** per la configurazione del tunnel VPN. Tocca **OK** per concedere a Citrix Secure Access l'autorizzazione a stabilire una connessione sicura con la rete interna della tua azienda.

Nota: Questo messaggio viene visualizzato solo quando si stabilisce una connessione sicura a NetScaler Gateway per la prima volta. Non viene visualizzato per i tentativi di connessione successivi finché Citrix Secure Access non viene disinstallato e quindi installato di nuovo sul dispositivo.

Sei connesso alla rete interna della tua azienda. Un'icona a forma di chiave appare nella barra di stato del dispositivo, indicando che la connessione VPN è attiva. L'icona di notifica del servizio

VPN del client Citrix Secure Access appare anche sulla barra di stato. L'interruttore di connessione cambia il suo stato in connesso e un'icona di spunta appare accanto al nome del profilo VPN.

Client Citrix Secure Access per dispositivi iOS

Il client Citrix Secure Access per iOS fornisce la migliore soluzione di accesso alle applicazioni e protezione dei dati della categoria offerta da NetScaler Gateway. Ora è possibile accedere in modo sicuro ad applicazioni aziendali critiche, desktop virtuali e dati aziendali da qualsiasi luogo e in qualsiasi momento.

L'app Citrix Secure Access fornisce il supporto completo per la gestione dei dispositivi mobili (MDM) su iOS. Con un server MDM, un amministratore può ora configurare e gestire da remoto i profili VPN a livello di dispositivo e i profili VPN per app.

Importante:

- A partire dalla versione 23.11.1, Citrix SSO per iOS è stato rinominato in Citrix Secure Access. Stiamo aggiornando la nostra documentazione e gli screenshot dell'interfaccia utente per riflettere questo cambiamento di nome.
- Per istruzioni specifiche per l'amministratore su Citrix Secure Access per iOS, vedere [Citrix SSO per iOS](#) e [Citrix Secure Access per macOS](#).

Importa e installa i certificati nell'app Citrix Secure Access

Citrix Secure Access su iOS supporta l'autenticazione con certificato client con NetScaler Gateway. I certificati possono essere distribuiti a Citrix Secure Access nei seguenti modi:

- **Server MDM** - Approccio preferito per i clienti MDM. I certificati vengono configurati direttamente sul profilo VPN gestito da MDM. Sia i profili VPN che i certificati vengono quindi inviati ai dispositivi registrati quando il dispositivo si registra nel server MDM. Per questo approccio, seguire i documenti specifici del fornitore MDM.
- **Email** - Unico approccio per i clienti non MDM. Gli amministratori inviano un'e-mail agli utenti con l'identità del certificato utente (certificato e chiave privata) allegata come file PKCS#12. Gli

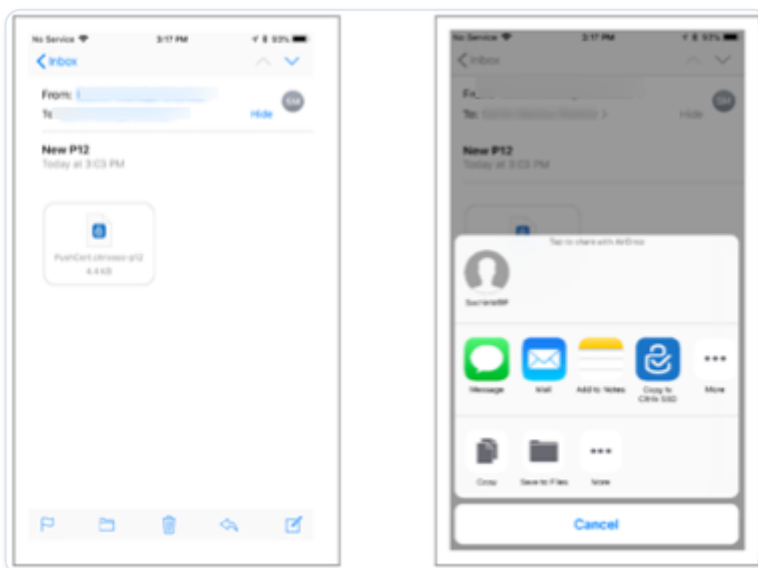
utenti devono avere i propri account e-mail configurati sul proprio dispositivo iOS per ricevere l'e-mail con un allegato. Il file può quindi essere importato in Citrix Secure Access su iOS.

Nota:

Le estensioni dei nomi di file `.pfx` e `.p12` sono rivendicate dal sistema iOS e non possono essere rivendicate da app di terze parti come Citrix Secure Access. Pertanto, gli amministratori devono modificare il tipo di estensione/MIME del certificato utente, da `.pfx` o `.p12` standard a `.citrixsso-pfx` o `.citrixsso-p12` rispettivamente.

1. Aprire l'e-mail con l'identità del certificato utente (certificato e chiave privata) allegata come file PKCS#12.

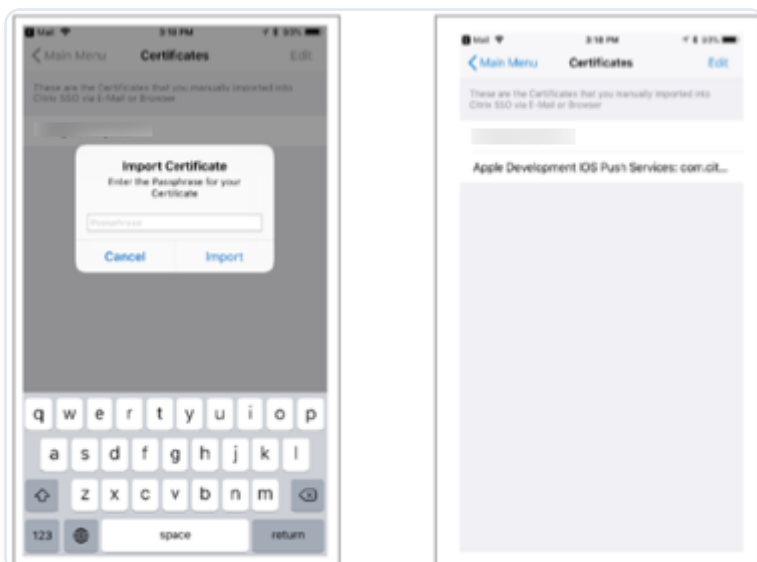
- Toccare l'allegato per visualizzare il menu di sistema **Apri in**.
- Toccare **Copia in Citrix SSO**.



2. Installare il certificato in Citrix Secure Access.

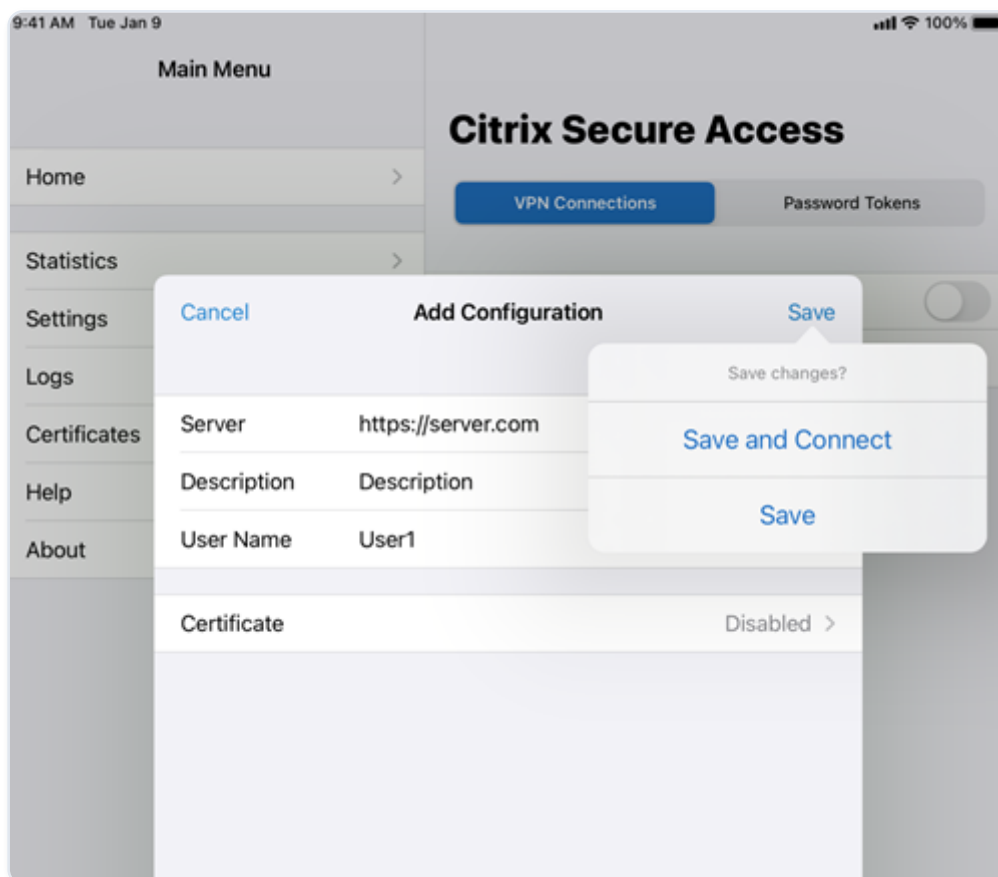
L'app viene ora avviata e viene visualizzato un prompt per la passphrase del certificato. Immettere la passphrase corretta affinché il certificato venga installato nel portachiavi dell'app e fare clic su **Importa**.

Dopo la convalida riuscita, il certificato viene importato.

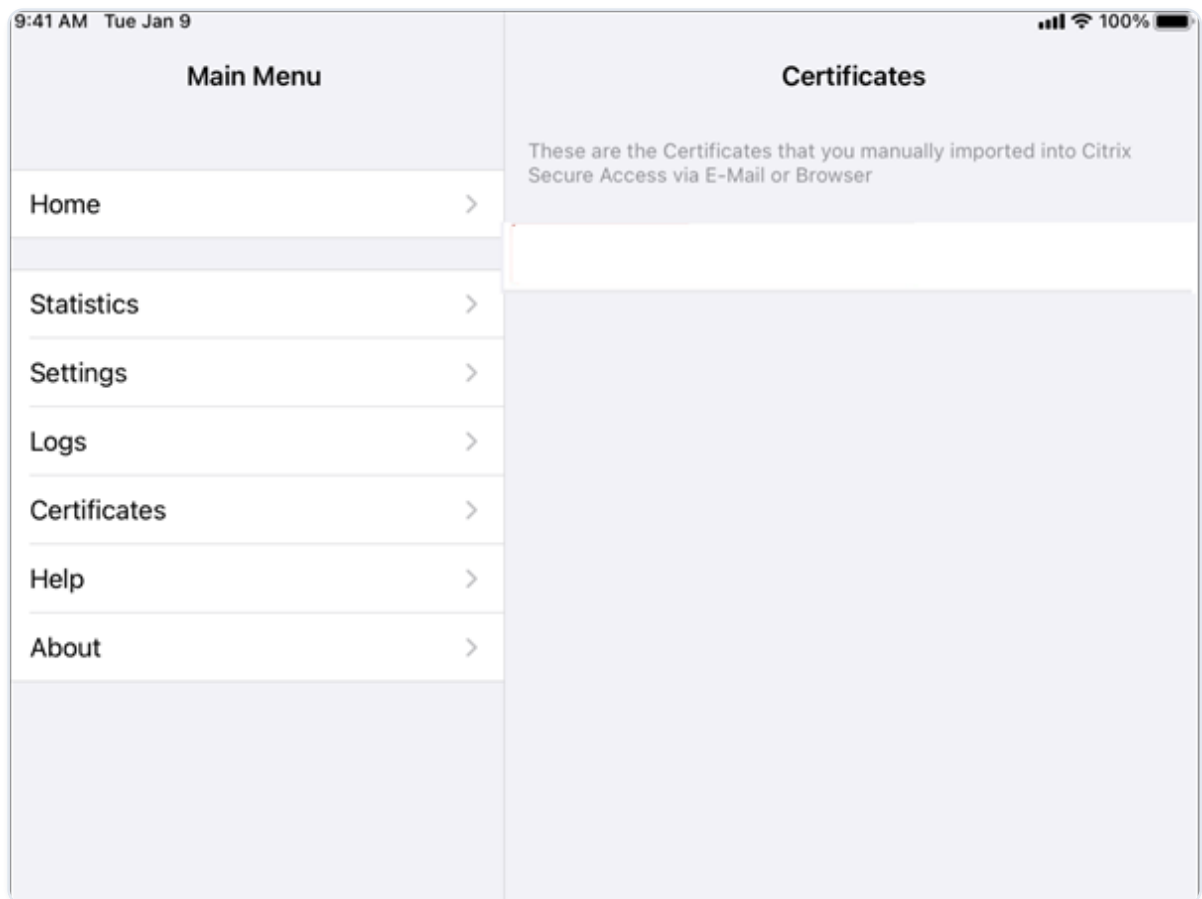


3. Utilizzare l'autenticazione basata su certificato con VPN.

- Per utilizzare il certificato per l'autenticazione VPN, è necessario prima creare una configurazione VPN o un profilo su Citrix Secure Access.
 - Accedere alla vista **Connessioni VPN** e toccare **Aggiungi configurazione VPN**.
 - Nella vista di configurazione del profilo VPN, è possibile selezionare il certificato importato nella sezione **Certificati**.



- Toccare **Salva** per importare il certificato.



4. Gestisci certificati.

Per gestire i certificati importati in Citrix Secure Access, accedere alla scheda **Certificati** nel **Menu principale**.

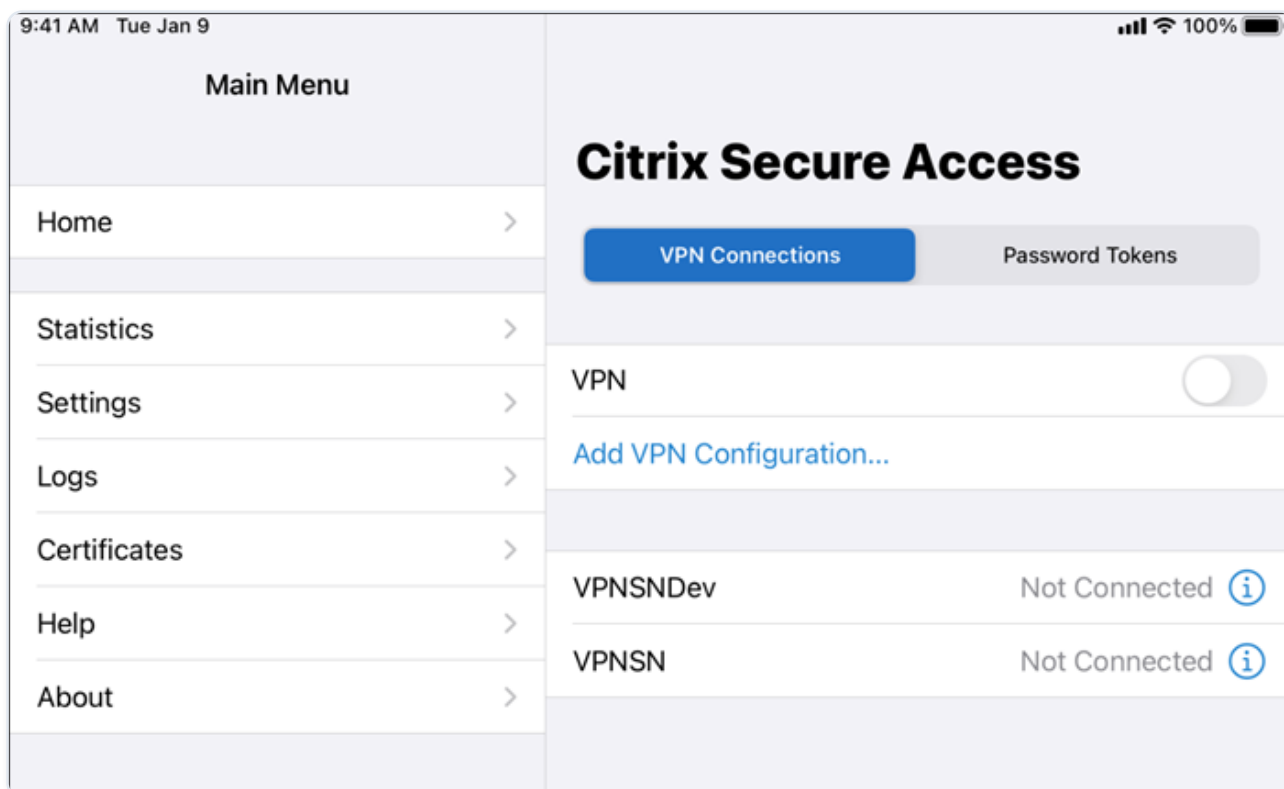
Come usare Citrix Secure Access dal tuo dispositivo iOS

Installa l'app Citrix Secure Access dall'App Store. Dopo aver installato l'app, la prima volta devi creare una connessione a NetScaler Gateway aggiungendo il server. Per gli usi successivi, puoi connetterti a una connessione esistente o aggiungerne una nuova, e anche modificare le connessioni esistenti. Puoi anche visualizzare i log e intraprendere le azioni appropriate di conseguenza.

Per i clienti MDM, l'amministratore potrebbe aver preconfigurato le connessioni VPN che appaiono automaticamente quando registri il tuo dispositivo. Puoi avviare le connessioni direttamente selezionando la connessione e attivando l'interruttore VPN. Queste connessioni VPN non sono modificabili dagli utenti.

Aggiungere una connessione

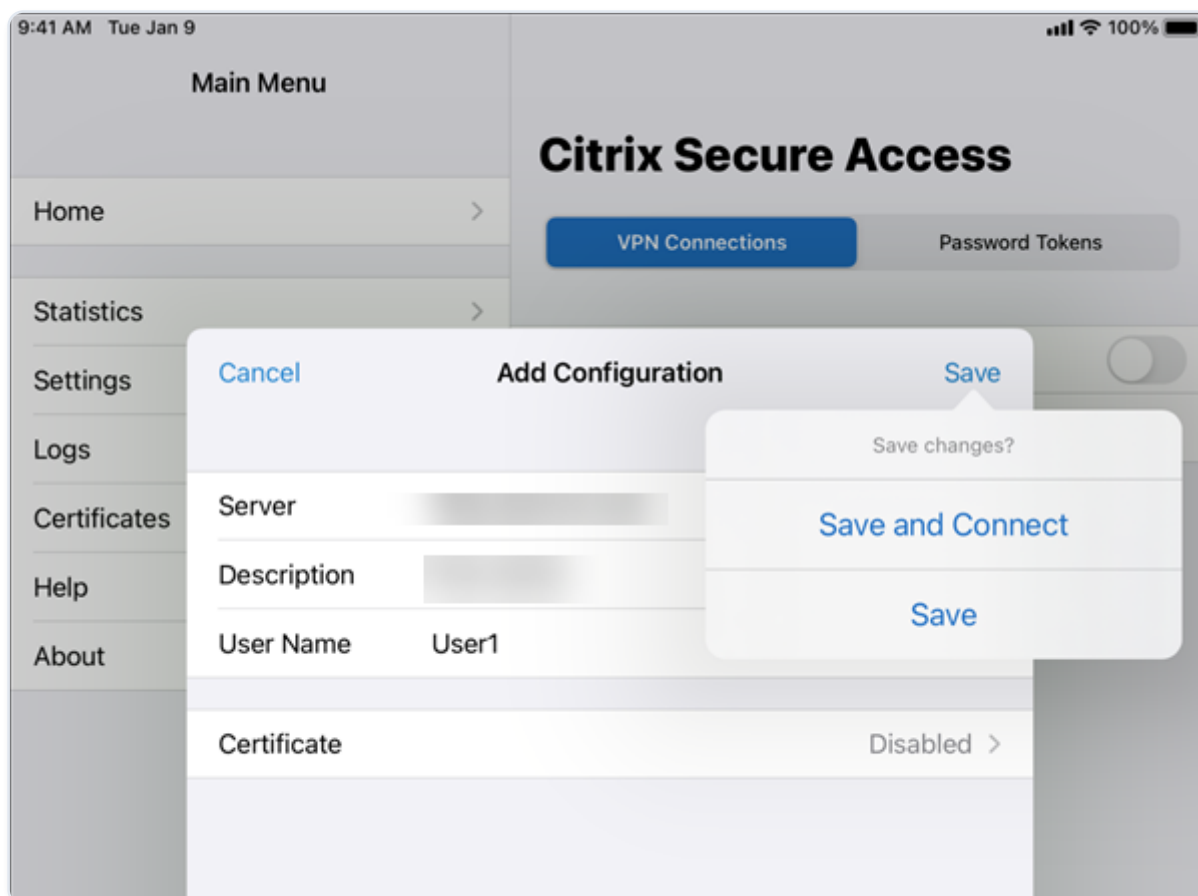
Dopo aver installato Citrix Secure Access e aperto l'app, viene visualizzata la seguente schermata.



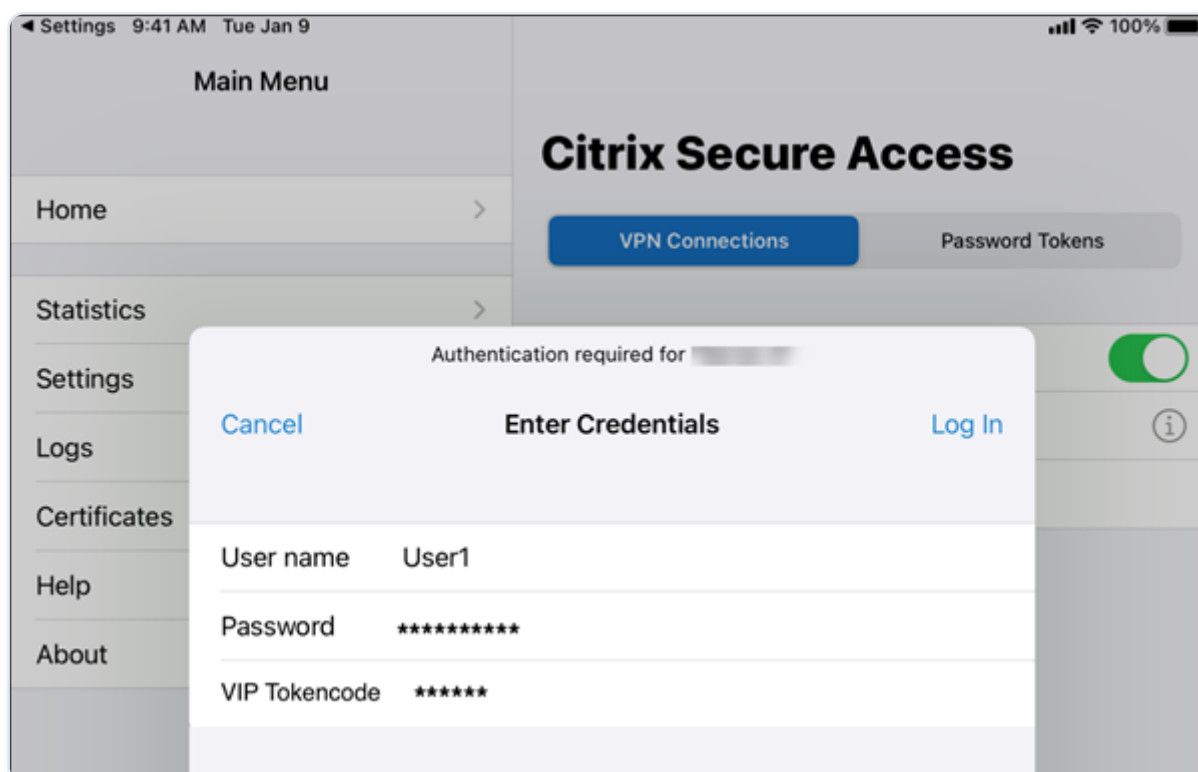
1. Tocca **Aggiungi configurazione VPN** per aggiungere una nuova connessione.
2. Inserisci i dettagli del server.

Puoi anche aggiungere facoltativamente il nome utente.

3. Tocca **Salva** e poi tocca **Salva e connetti** o **Salva**, a seconda dei casi.



4. Fornisci le credenziali di autenticazione per il tuo server e tocca **Accedi**.



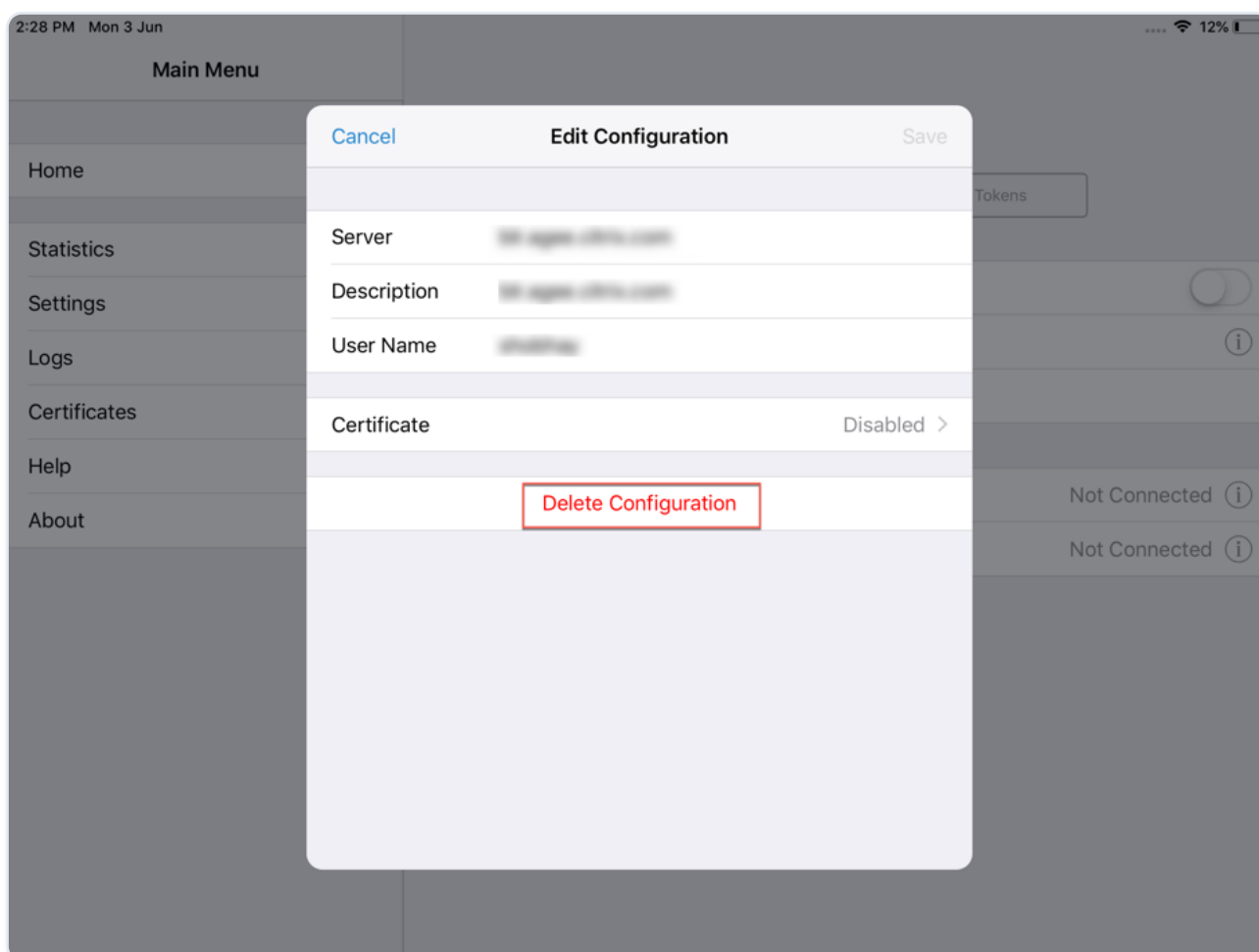
Nota: Per disconnettersi da Citrix Secure Access, disattiva la VPN.

Riconnettersi a NetScaler Gateway dopo un errore di connessione VPN

L'app Citrix Secure Access per iOS richiede di eseguire nuovamente l'autenticazione con NetScaler Gateway quando una connessione VPN viene persa. Viene visualizzata una notifica nell'interfaccia utente che la connessione a NetScaler Gateway è stata persa e che è necessario eseguire nuovamente l'autenticazione per riprendere la connessione.

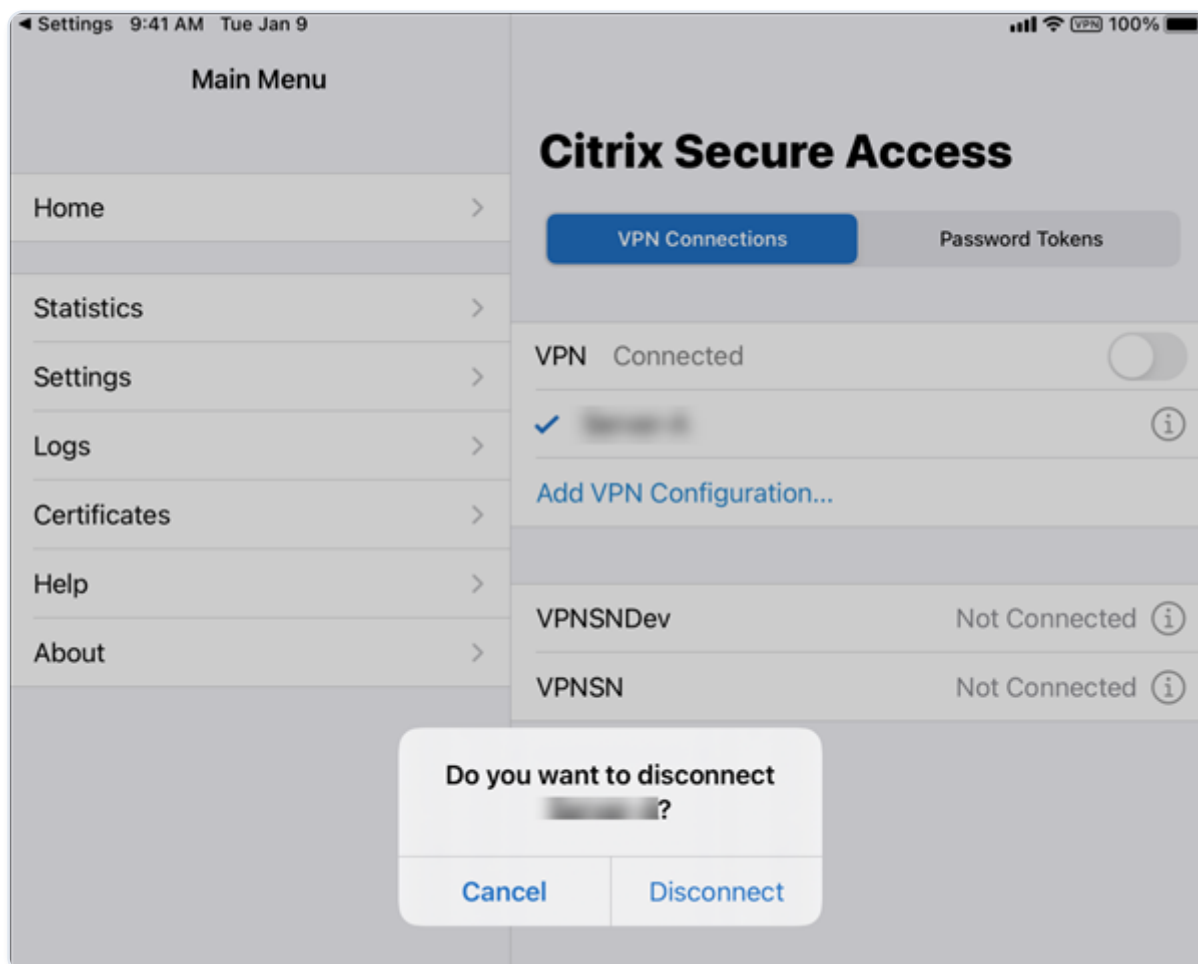
Eliminare una connessione esistente

Toccare l'icona accanto alla connessione e quindi toccare Elimina configurazione.



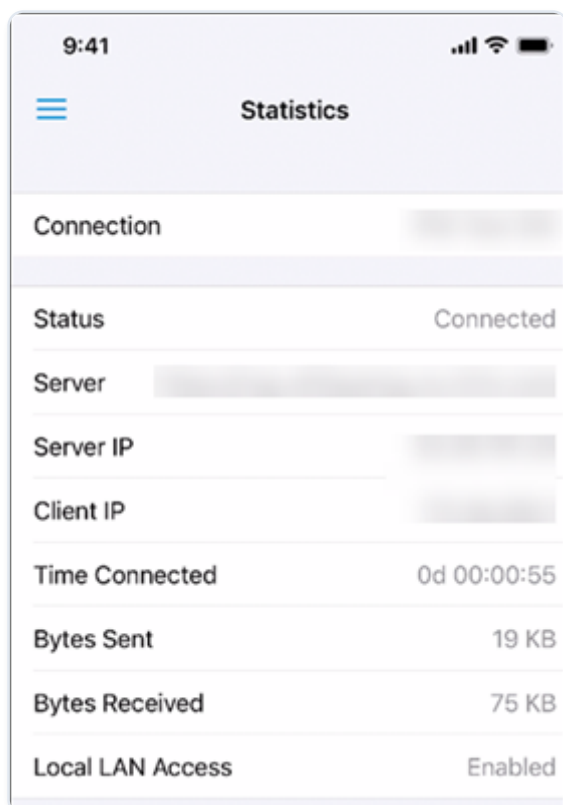
Disconnettere una connessione

Impostare l'interruttore VPN su OFF e quindi toccare Disconnetti.



Visualizzare le statistiche

È possibile visualizzare le statistiche di connessione quando la VPN è connessa.



Bloccare i server non attendibili

Citrix SSO non si connette ai server non attendibili (server che utilizzano certificati autofirmati o che non dispongono di un certificato radice attendibile per il gateway), per impostazione predefinita. Per consentire questi tipi di connessioni, è possibile disattivare l'interruttore Blocca server non attendibili.

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

Accesso LAN locale

Citrix SSO per iOS 23.10.1 supporta la funzionalità di accesso LAN locale in cui è possibile determinare se si desidera accedere alle risorse LAN locali sul dispositivo client una volta stabilita una connessione VPN. È possibile utilizzare questa funzionalità solo se l'amministratore ha configurato l'impostazione di accesso LAN locale su NetScaler Gateway.

Per configurare l'accesso LAN locale nell'interfaccia utente di Citrix Secure Access:

1. Accedere al menu principale e fare clic su **Impostazioni**.
2. Abilitare **Consenti accesso LAN locale**.

È possibile verificare lo stato dell'accesso LAN locale nella pagina **Statistiche**.

Invia log

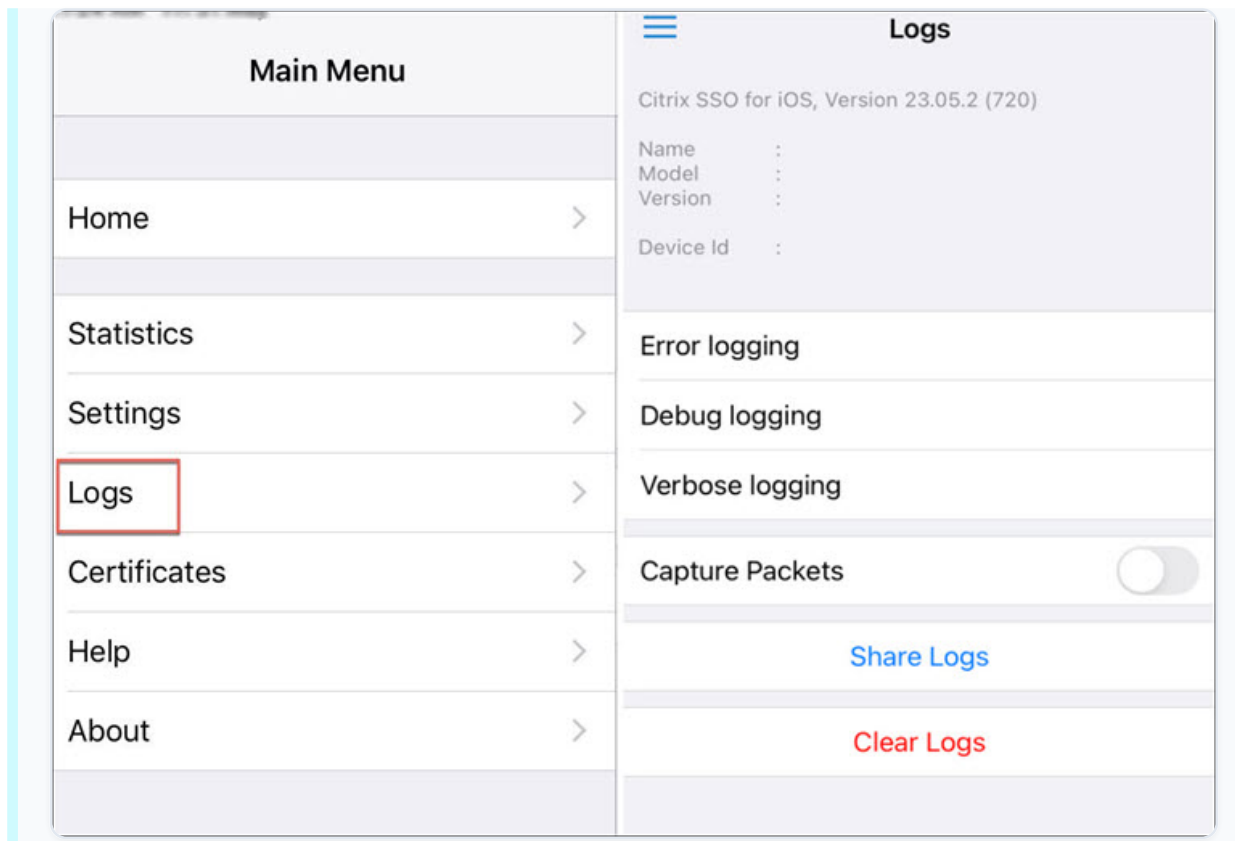
L'acquisizione dei log di debug è una parte fondamentale della risoluzione dei problemi o della segnalazione di problemi al supporto Citrix.

Di seguito sono riportati i passaggi per acquisire e condividere i log di debug:

1. Impostare l'interruttore **Registrazione debug** su ON.
2. Condividere i log utilizzando opzioni quali e-mail, chat, salvataggio su file e così via.

Nota:

- Per generare un nuovo set di log, eliminare prima i log precedenti utilizzando **Cancella log**.
- A partire dalla versione 23.07.1, l'opzione **Log e-mail** è stata sostituita con l'opzione **Condividi log**. Condividi log offre varie opzioni per condividere i file di log compressi.



Visualizza i certificati client

È possibile visualizzare i certificati client importati in Citrix Secure Access. I certificati importati vengono visualizzati nella sezione **Certificati**. È possibile eliminare i certificati in uno dei seguenti modi.

- Sulla cella del certificato, eseguire un gesto di scorrimento da destra a sinistra per rivelare il pulsante **Elimina**. Quindi toccare **Elimina**.
- Toccare **Modifica** per rivelare il pulsante **Elimina** e quindi toccare **Elimina**.

Visualizzare o eliminare un certificato(/en-us/citrix-sso/media/sso-ios-certificates.png)

Argomenti della guida

Per assistenza su vari elementi, vedere **Guida**.

Visualizzare gli argomenti della guida(/en-us/citrix-sso/media/sso-ios-help.png)

Client Citrix Secure Access per dispositivi macOS

L'app Citrix Secure Access offre la migliore soluzione di accesso alle applicazioni e protezione dei dati fornita da NetScaler Gateway. Ora è possibile accedere in modo sicuro ad applicazioni aziendali critiche, desktop virtuali e dati aziendali da qualsiasi luogo e in qualsiasi momento. L'app Citrix Secure Access è il client VPN di nuova generazione per NetScaler Gateway, basato sul framework Network Extension di Apple. Sostituisce il client VPN Citrix legacy sull'App Store.

L'app Citrix Secure Access offre il supporto completo per la gestione dei dispositivi mobili (MDM) su macOS. Con un server MDM, un amministratore può ora configurare e gestire da remoto profili VPN a livello di dispositivo e profili VPN per app.

Importante:

- L'app Citrix Secure Access supporta l'accesso alla rete Zero-trust. Oltre all'URL di NetScaler Gateway, è possibile connettersi anche all'URL di Workspace.
- Per istruzioni specifiche per l'amministratore su Citrix Secure Access per macOS, vedere [Citrix SSO per iOS](#) e [Citrix Secure Access per macOS](#).

Installare il client Citrix Secure Access per macOS

A partire dalla versione 25.06.1.1 del client Citrix Secure Access per macOS, è possibile scaricare e installare l'applicazione utilizzando il file del pacchetto (`.pkg`) disponibile in [Citrix Secure Access per macOS](#) o dall'App Store. Il file `.pkg` può essere installato manualmente o utilizzando strumenti di gestione come Jamf e Intune. In precedenza, gli utenti potevano installare il client Citrix Secure Access per macOS solo dall'App Store.

Installare l'app Citrix Secure Access su macOS utilizzando il file .pkg

Prerequisiti

Prima di installare il file `.pkg` per l'app Citrix Secure Access, assicurarsi che siano soddisfatti i seguenti prerequisiti:

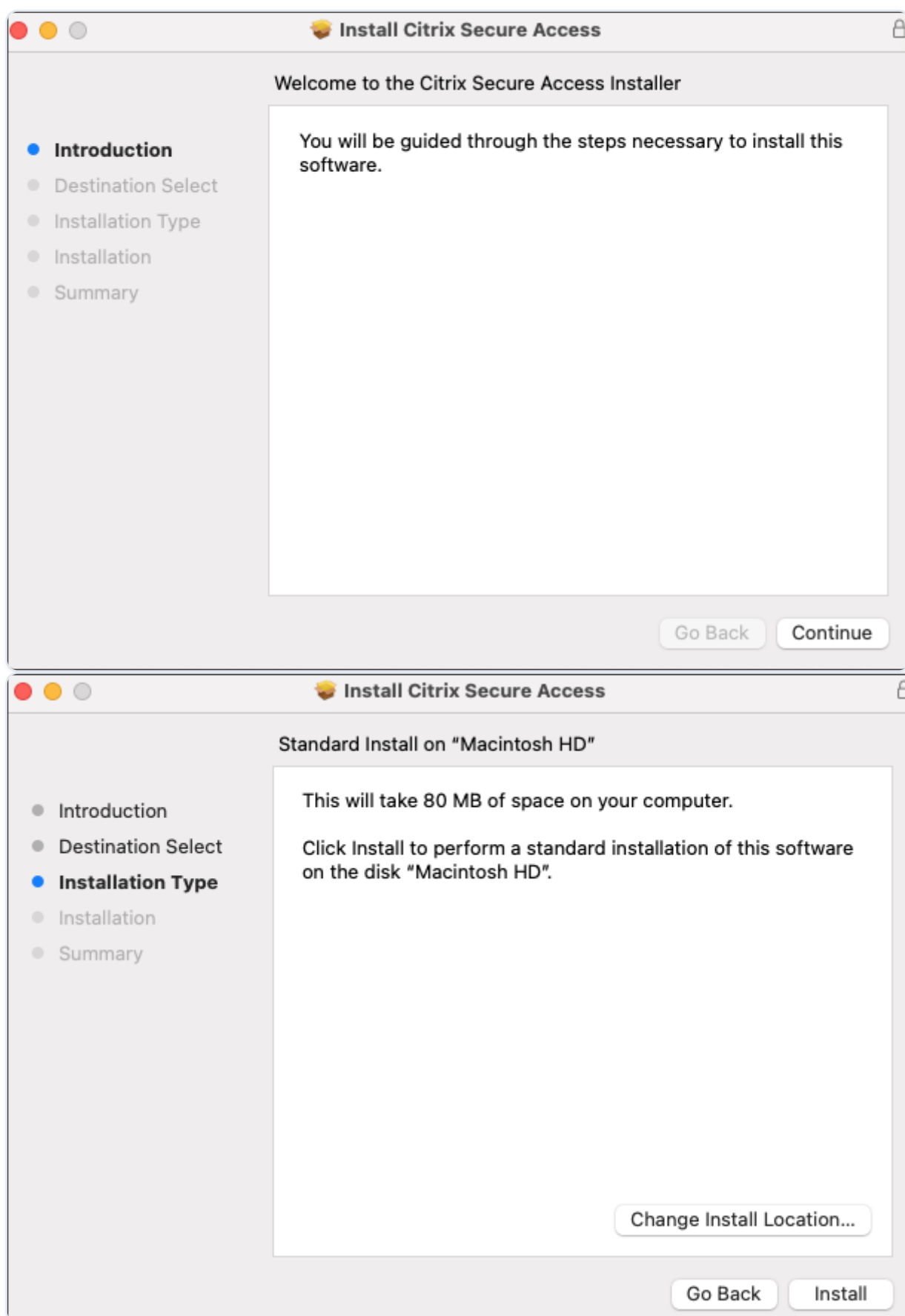
- Il computer Mac esegue macOS 13.0 o versioni successive.
- L'utente dispone di privilegi di amministratore sul computer Mac. Sulle macchine gestite, gli amministratori devono assicurarsi che le autorizzazioni di installazione delle applicazioni siano abilitate e che l'estensione di sistema con l'identificatore "com.citrix.NSG.macos.app.vpnplugin" sia attivata.
- Disconnettersi dall'app Citrix Secure Access se è attualmente in esecuzione.
- Eliminare qualsiasi versione dell'app Citrix Secure Access precedentemente installata dall'App Store.

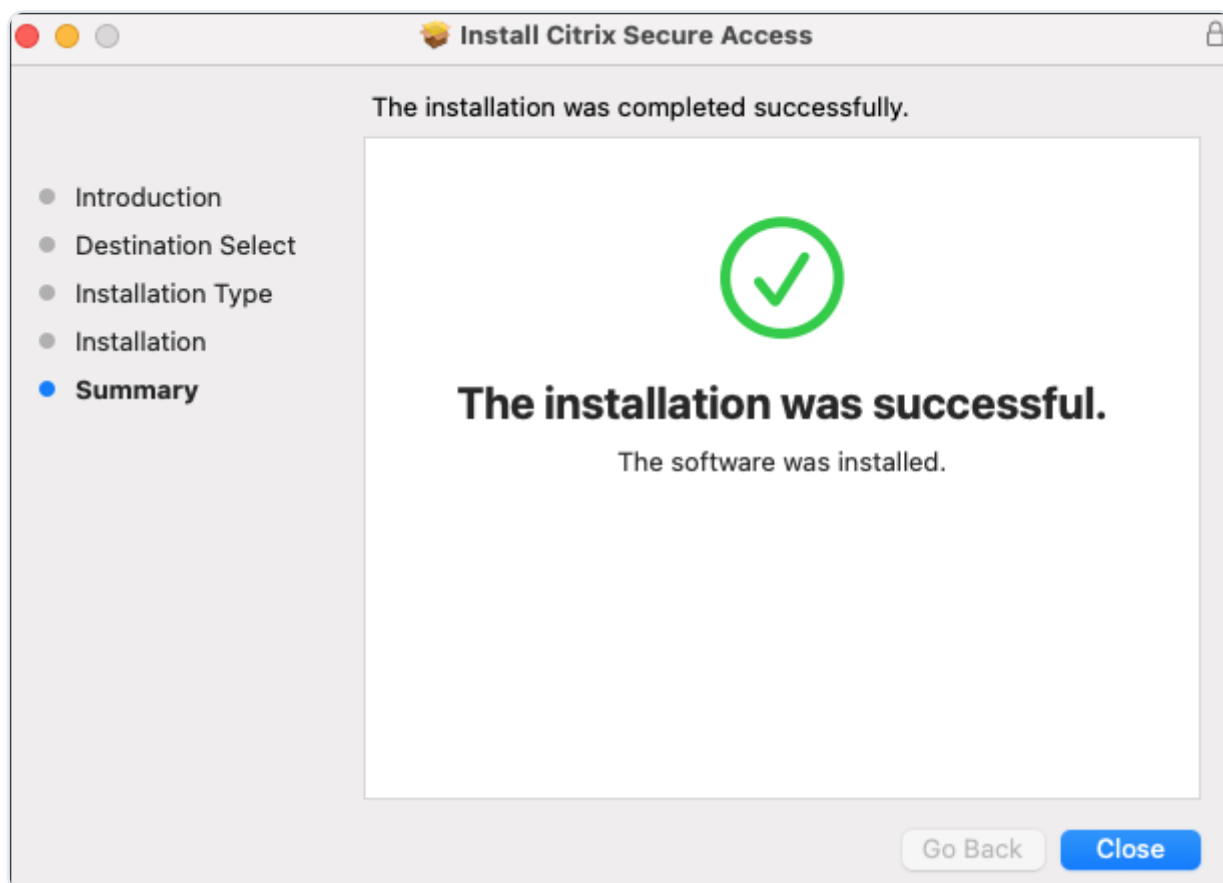
Come installare l'app Citrix Secure Access su macOS

Importante:

- Il file `.pkg` dell'app Citrix Secure Access utilizza l'estensione di sistema con l'identificatore "com.citrix.NSG.macos.app.vpnplugin" per le connessioni VPN.
- Per l'autenticazione del certificato client, i certificati devono essere installati nel **Portachiavi di sistema** perché le estensioni di sistema di macOS non possono accedere ai certificati dal **Portachiavi di login**.
- Se lo stesso certificato è installato sia nel **Portachiavi di sistema** che nel **Portachiavi di login**, eliminare il certificato insieme alla sua chiave dal **Portachiavi di login**.

1. Scaricare il file `.pkg` da [Citrix Secure Access per macOS](#).
2. Installare l'applicazione utilizzando lo strumento di gestione (Jamf o Intune) o manualmente. Per installare l'applicazione manualmente, fare doppio clic sul file `.pkg` e seguire le istruzioni visualizzate.

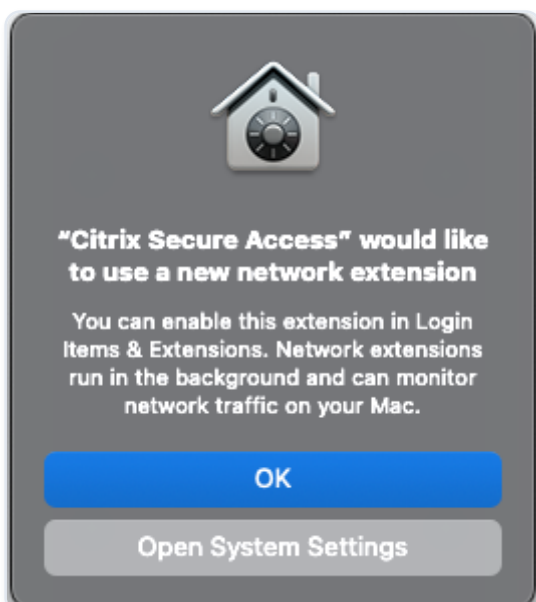




Configurazione iniziale

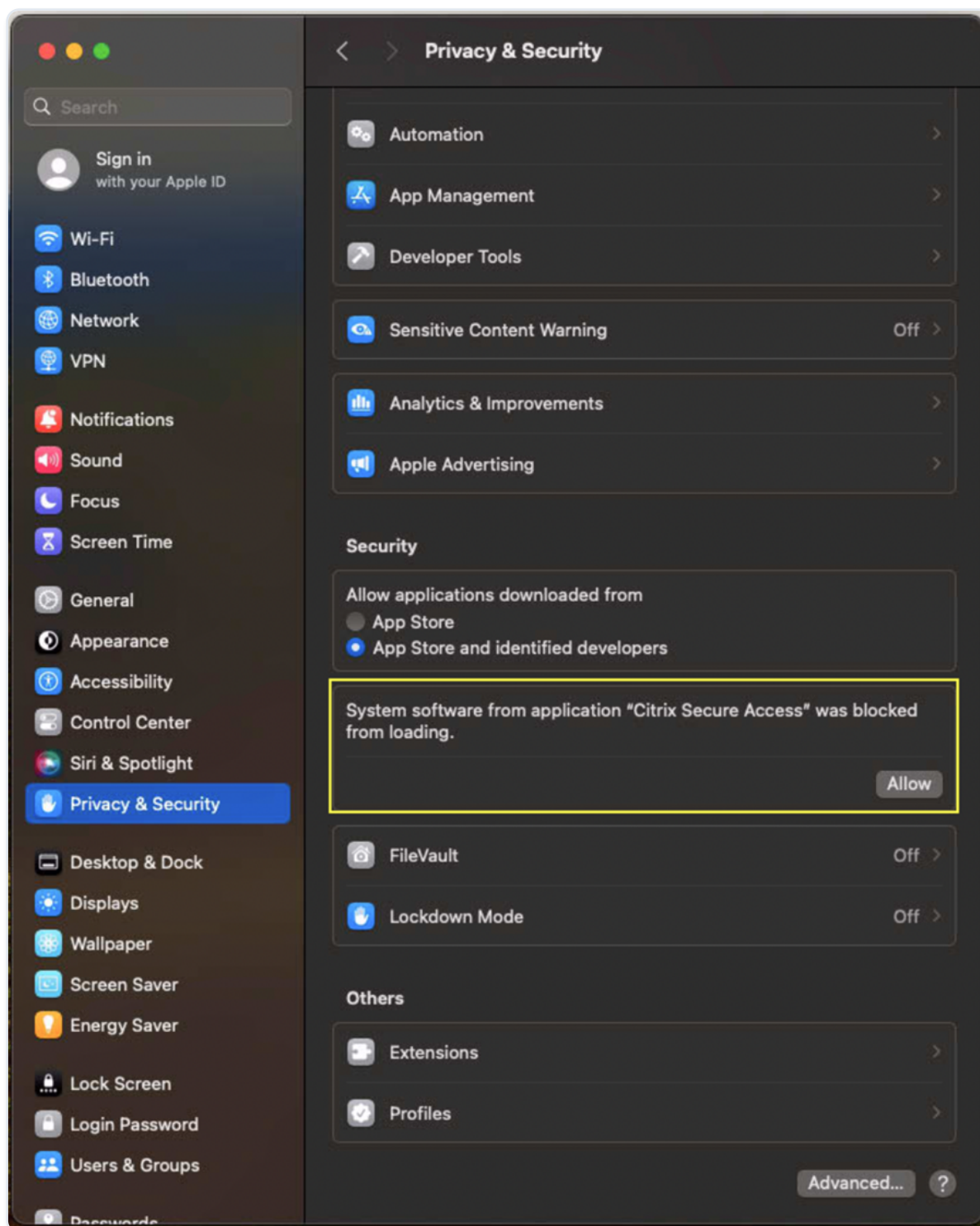
Dopo aver installato l'app Citrix Secure Access, seguire le istruzioni seguenti per utilizzare l'app Citrix Secure Access dal dispositivo macOS:

1. Aprire la cartella **Applicazioni** e fare doppio clic sull'icona dell'app Citrix Secure Access per avviarla.
2. Al primo avvio, il sistema richiede l'autorizzazione per installare l'estensione di sistema. Fare clic su **OK** nella richiesta di sistema.

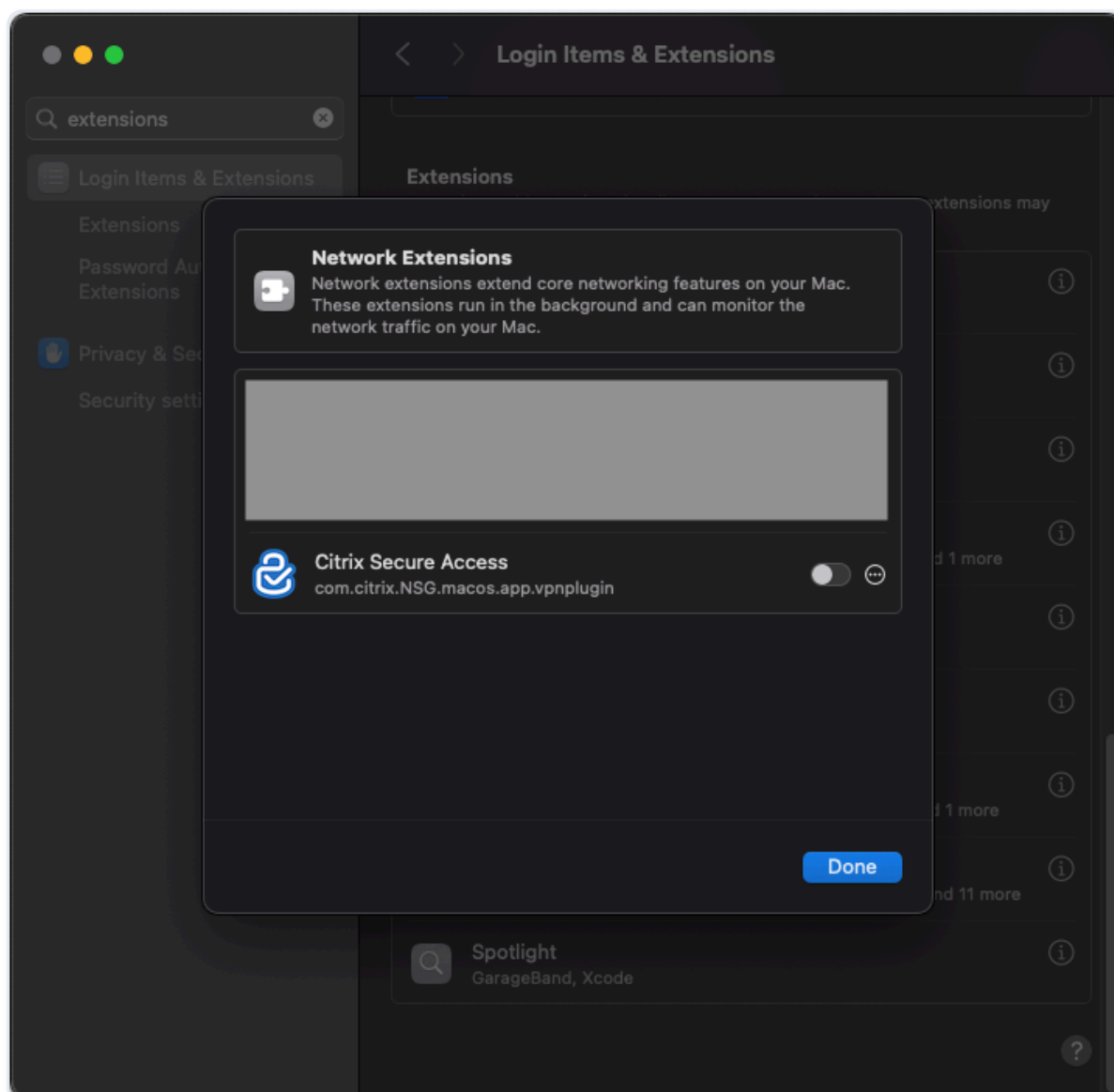


Se il prompt di sistema non appare, vai a **Impostazioni di Sistema** per abilitare l'installazione dell'estensione di sistema con l'identificatore "com.citrix.NSG.macos.app.vpnplugin".

- Per macOS 14.x, l'opzione **Impostazioni di Sistema** si trova sotto la scheda **Privacy e Sicurezza**.



- Per macOS 15.x e versioni successive, l'opzione **Impostazioni di Sistema** si trova sotto **Elementi di accesso ed estensioni** -> **Estensioni di rete**.



Supporto per l'installazione automatica del plug-in Endpoint Analysis™ con l'applicazione Citrix Secure Access

A partire dalla versione 25.11.1.1, l'applicazione Citrix Secure Access include l'installazione automatica del plug-in Endpoint Analysis (EPA). Il plug-in EPA è ora incluso per impostazione predefinita in tutte le installazioni e gli aggiornamenti, eliminando la necessità di un'installazione separata e semplificando il processo di configurazione. Questa funzionalità non è disponibile per la versione dell'applicazione dell'App Store.

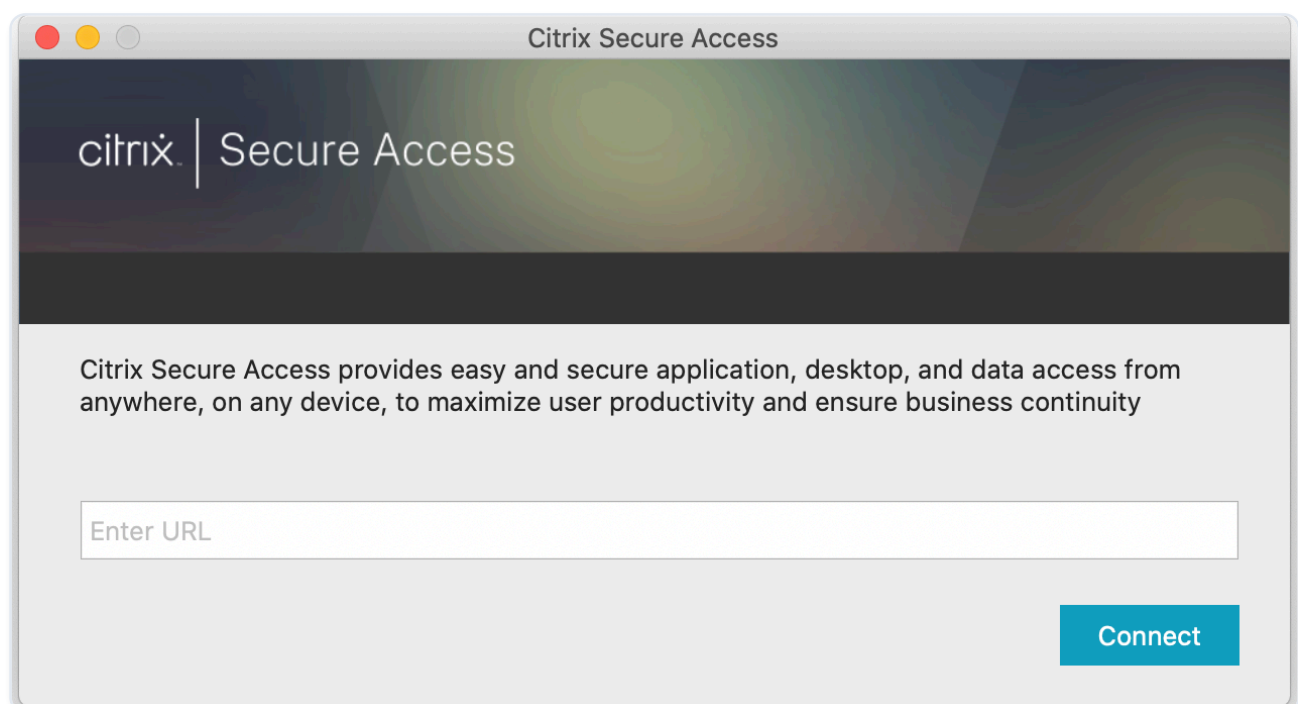
In precedenza, gli utenti dovevano scaricare e installare manualmente il plug-in EPA durante l'accesso all'applicazione Citrix Secure Access.

Come usare l'app Citrix Secure Access dal tuo dispositivo macOS

Gli utenti per la prima volta devono creare una connessione a NetScaler Gateway aggiungendo il server. Gli utenti esistenti possono connettersi a una connessione esistente o aggiungerne una nuova, e anche modificare le connessioni esistenti. È inoltre possibile visualizzare i log e intraprendere le azioni appropriate di conseguenza.

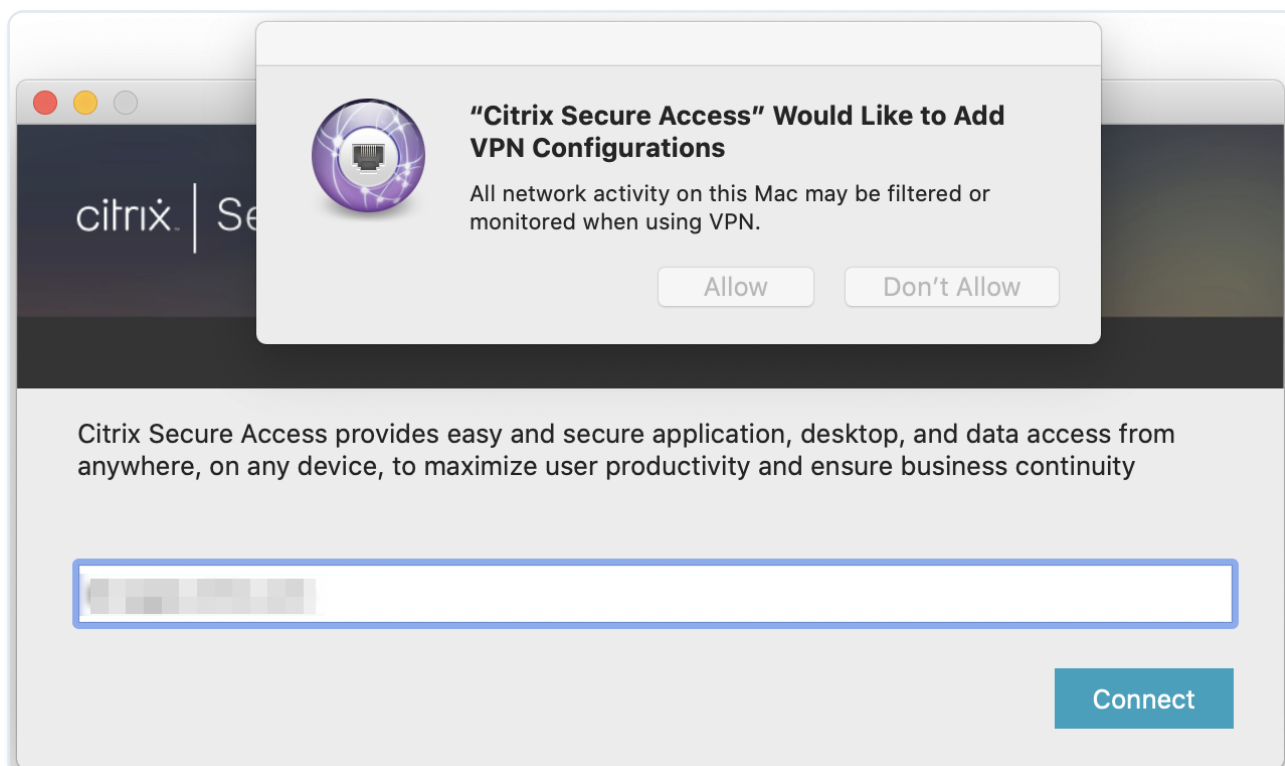
Esperienza utente per la prima volta

Dopo aver installato l'app Citrix Secure Access e averla aperta per la prima volta, viene visualizzata la seguente schermata.

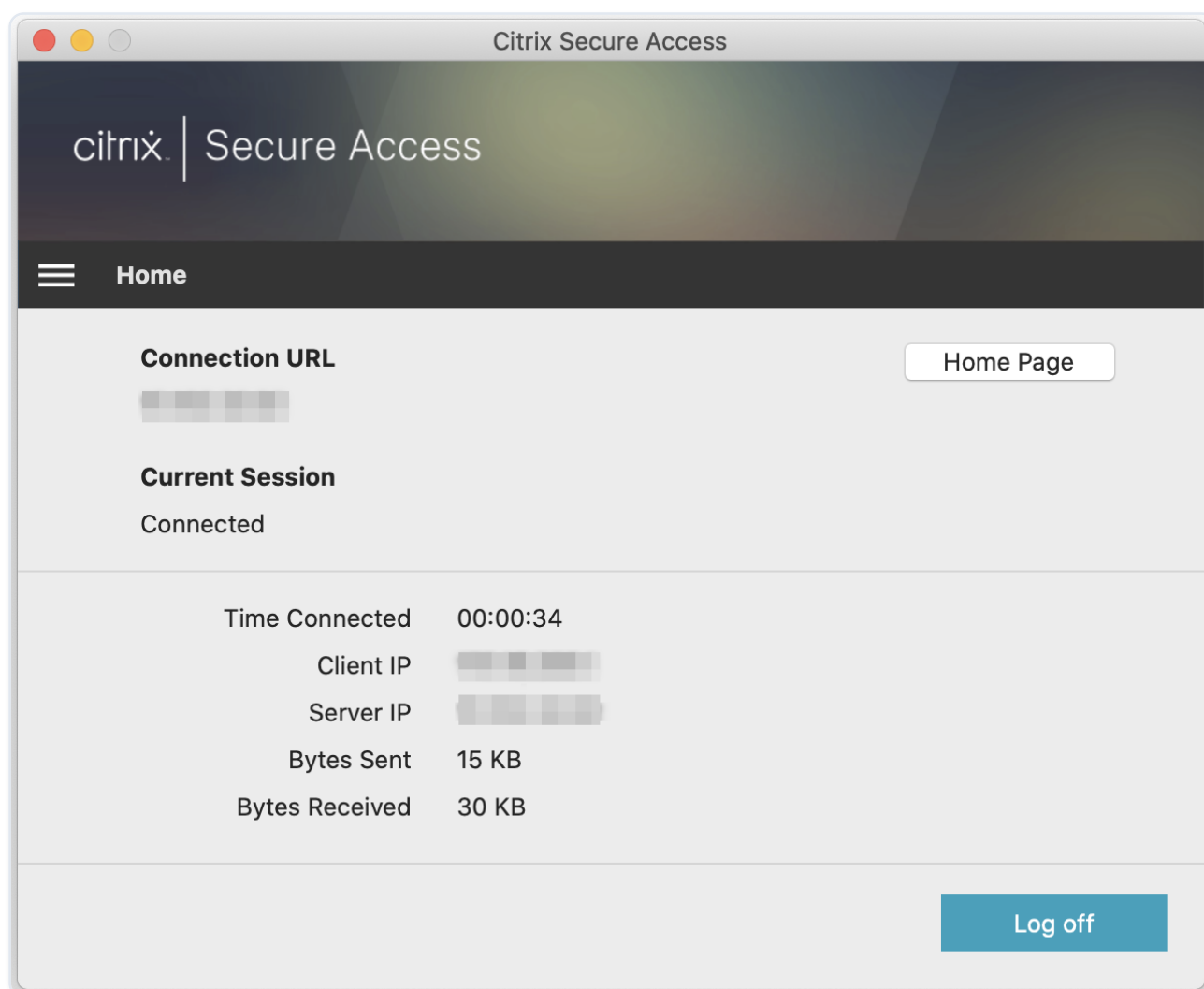


Inserisci l'URL di base di NetScaler Gateway o l'URL di Citrix Workspace e fai clic su **Connetti**.

Viene visualizzato un messaggio popup. Fai clic su **Consenti** per abilitare l'aggiunta di una connessione. Questo messaggio appare solo la prima volta. Per le nuove connessioni successive, questo messaggio non appare.



Nota: Per disconnettersi da Citrix Secure Access, si consiglia di fare prima clic su **Disconnetti** nell'app e quindi di chiudere l'app dal dock. Non utilizzare l'opzione **Esci** dal dock.

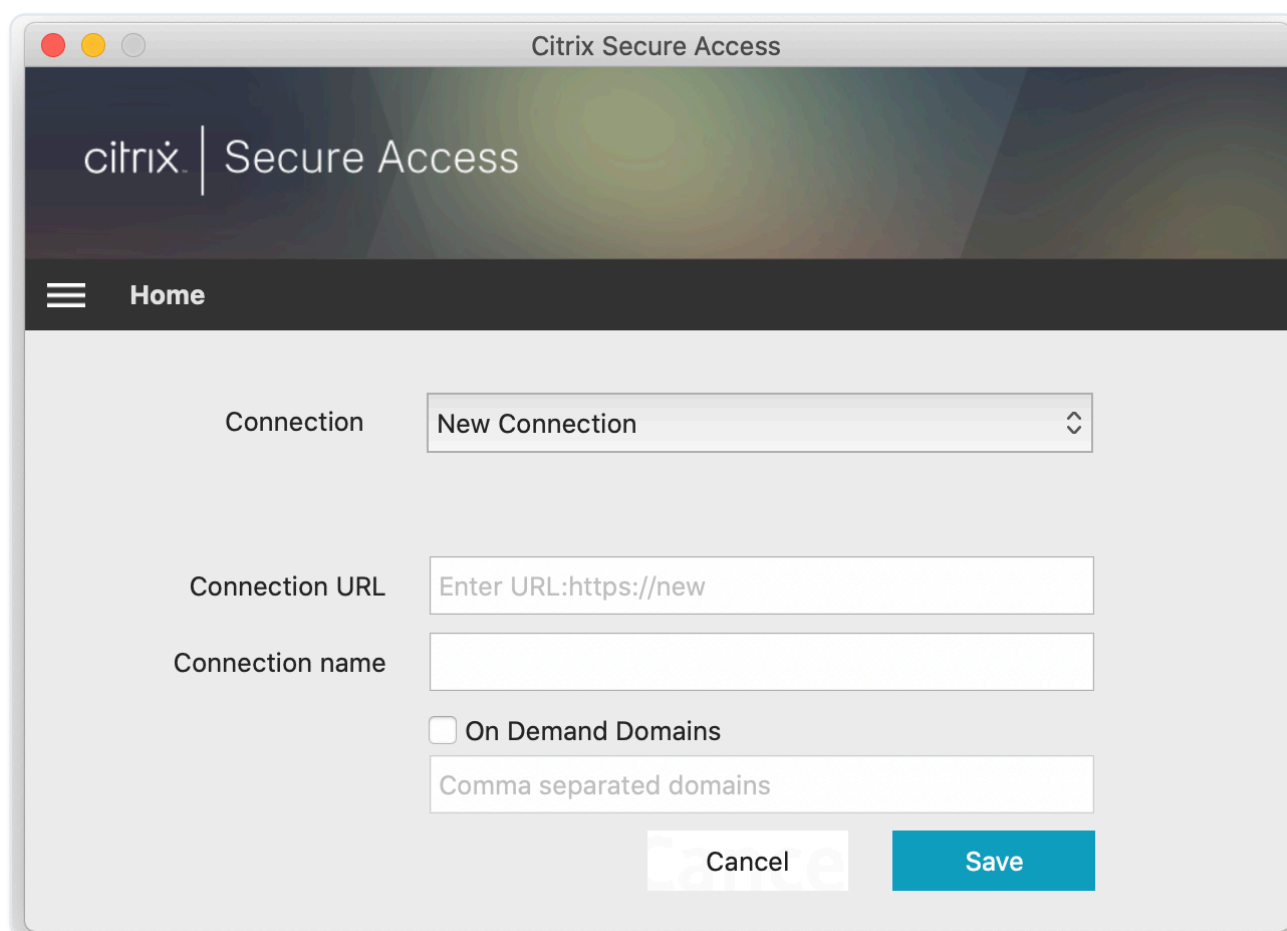


Connettersi a NetScaler Gateway

Dopo aver aggiunto la prima connessione, per le connessioni successive, è possibile connettersi a un NetScaler Gateway o a un Citrix Workspace esistente oppure aggiungere una connessione.

Aggiungere una connessione

Inserisci l'URL di base (ad esempio, [La mia azienda <https://gateway.mycompany.com>](https://gateway.mycompany.com)) e il nome per la connessione VPN.



The screenshot shows a web browser window titled "Citrix Secure Access". The header features the Citrix logo and the text "Secure Access". Below the header is a navigation bar with a hamburger menu icon and the word "Home". The main content area is a form for creating a new connection. It includes a "Connection" dropdown menu currently set to "New Connection". Below this are input fields for "Connection URL" (with placeholder text "Enter URL:https://new"), "Connection name", and a checkbox for "On Demand Domains". A text input field for "Comma separated domains" is also present. At the bottom right of the form are "Cancel" and "Save" buttons.

Citrix Secure Access

citrix | Secure Access

Home

Connection New Connection

Connection URL Enter URL:https://new

Connection name

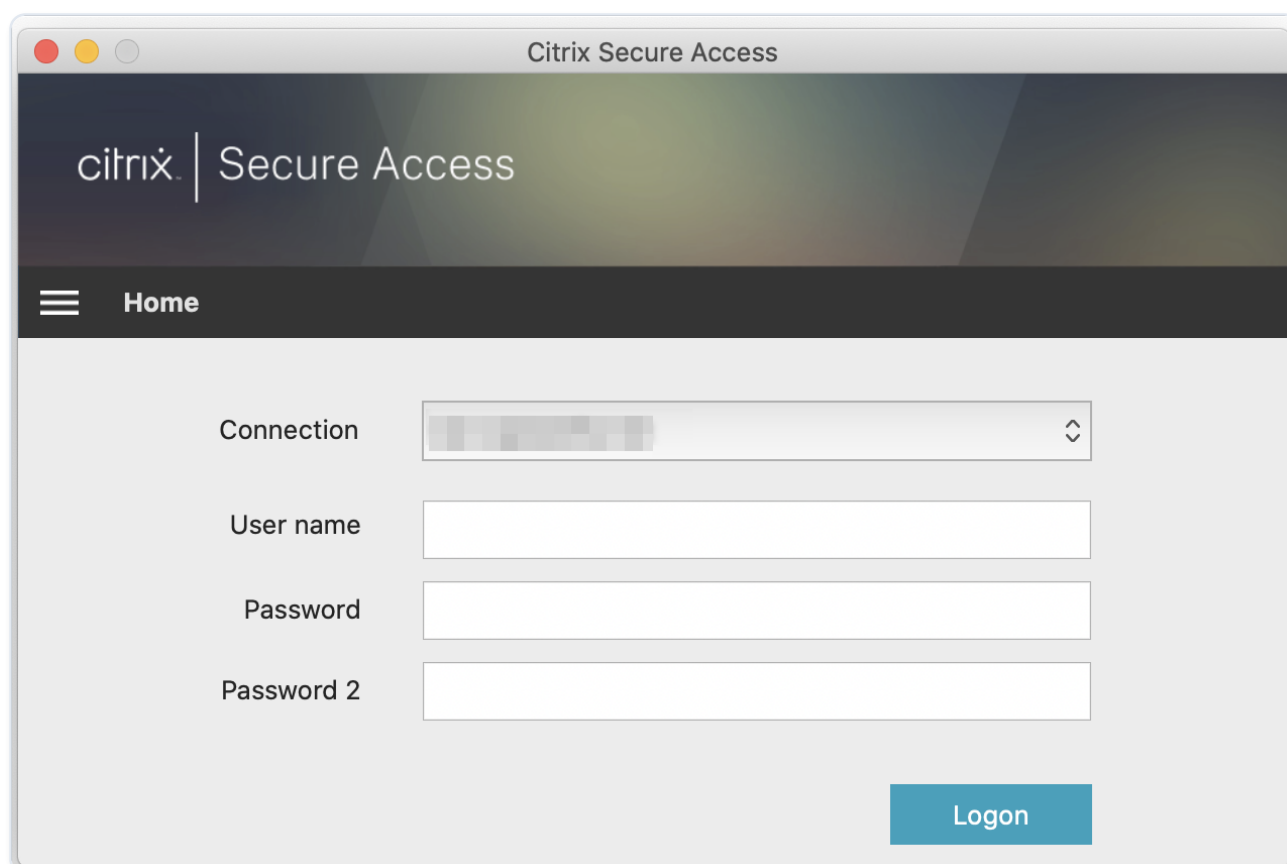
☐ On Demand Domains

Comma separated domains

Cancel Save

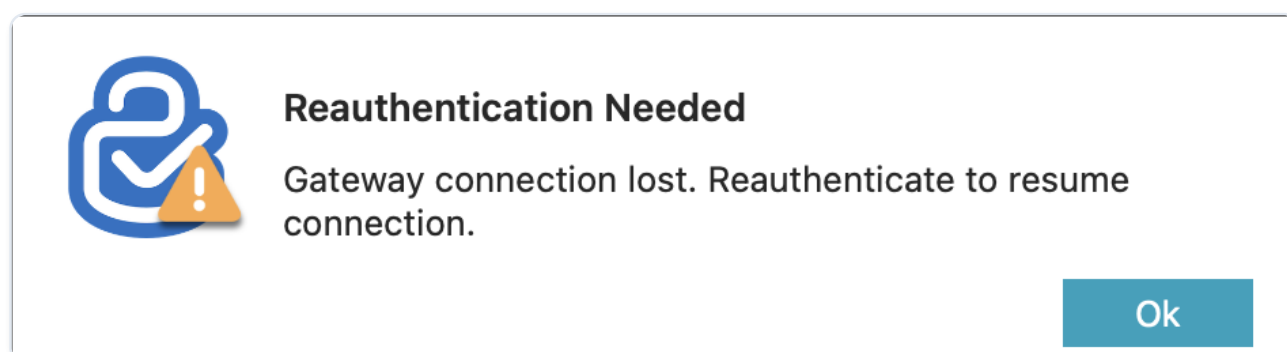
Connettersi a un NetScaler Gateway esistente

Selezionare una connessione esistente, fornire le credenziali di autenticazione per il server e selezionare **Logon**.



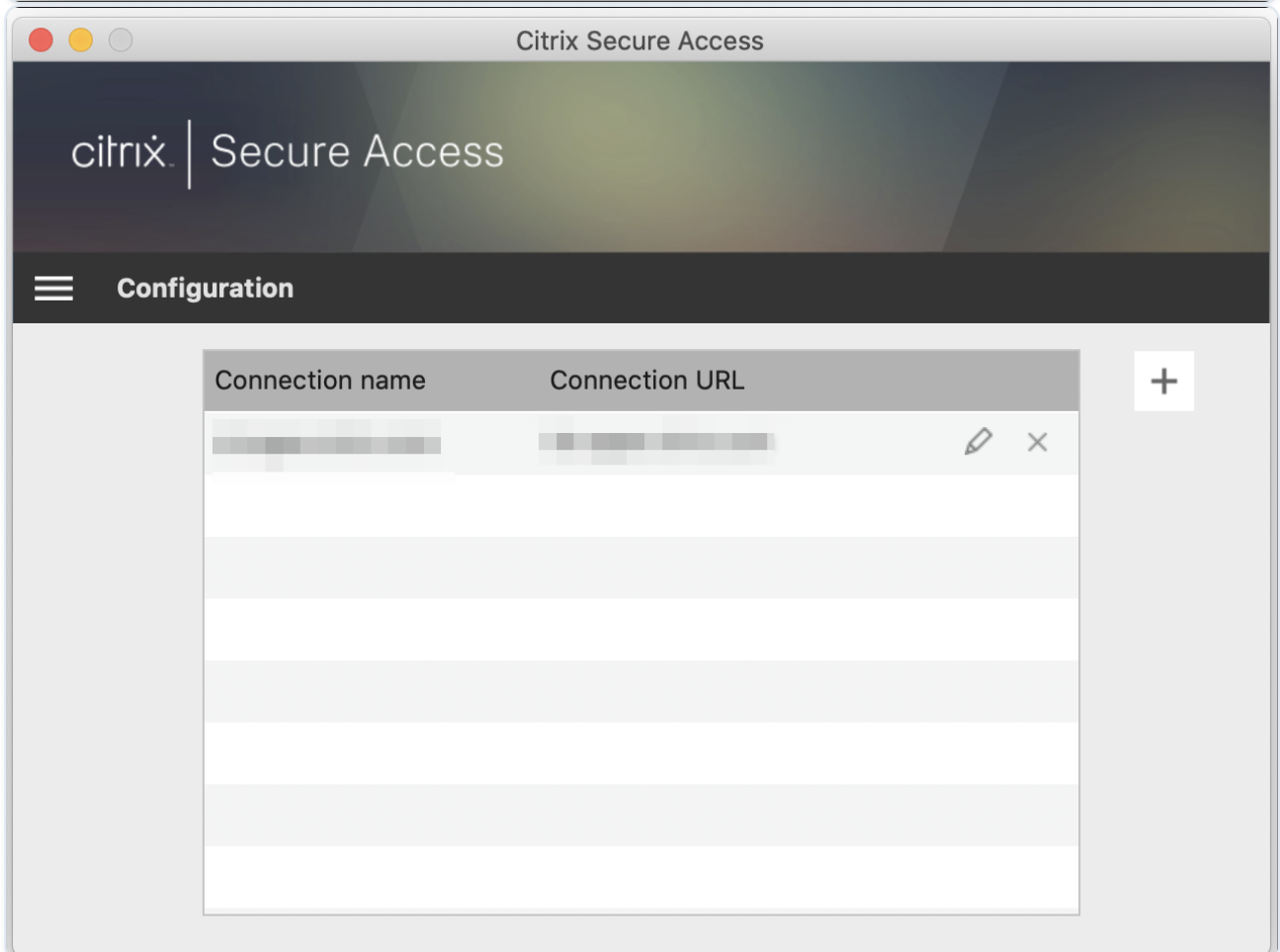
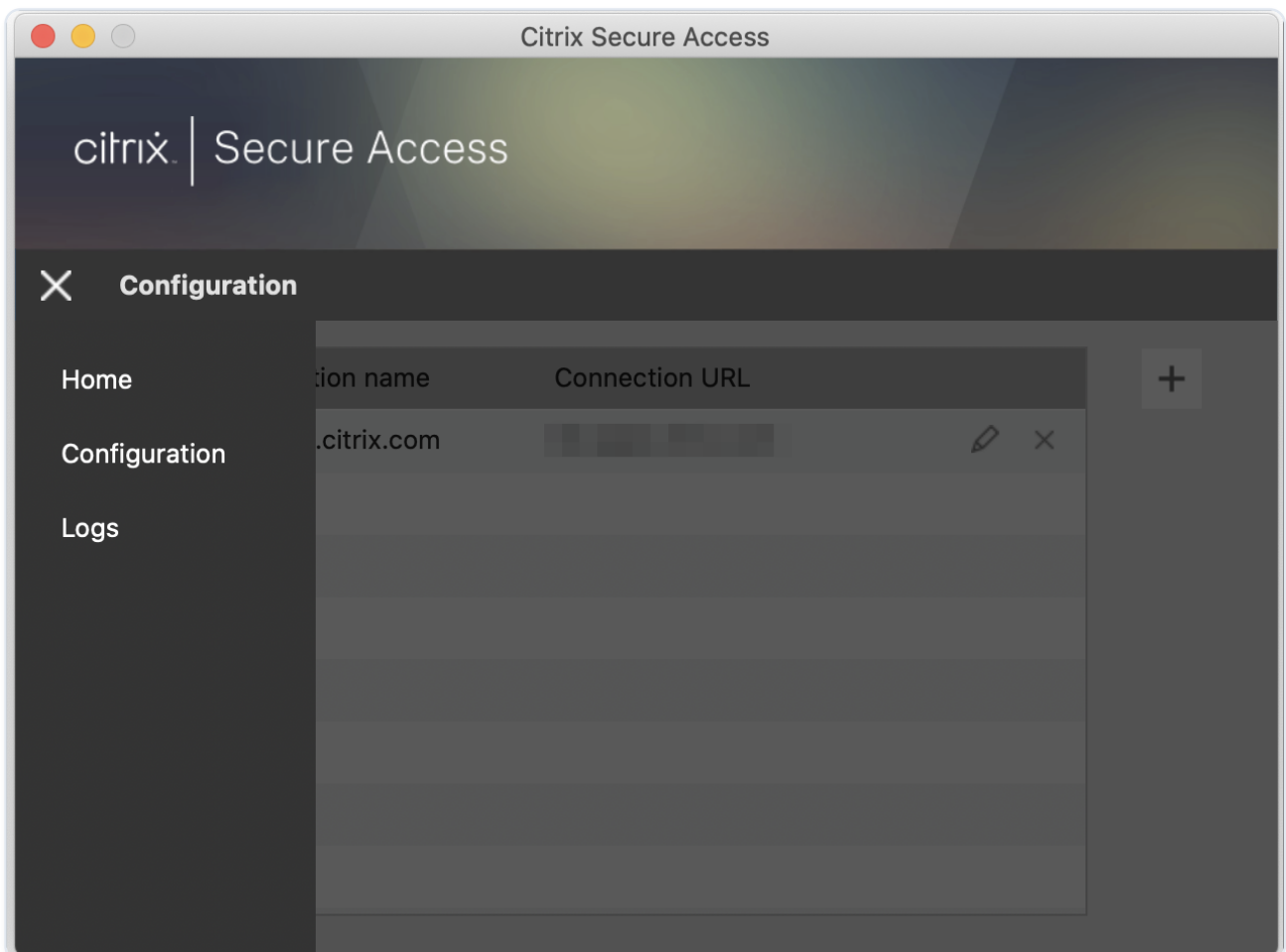
Riconnettersi a NetScaler Gateway dopo un errore di connessione VPN

A partire dalla versione 23.09.1, il client Citrix Secure Access per macOS richiede di eseguire nuovamente l'autenticazione con NetScaler Gateway quando una connessione VPN viene persa. Si riceve una notifica sull'interfaccia utente del client Citrix Secure Access che indica che la connessione a NetScaler Gateway è stata persa e che è necessario eseguire nuovamente l'autenticazione per riprendere la connessione.

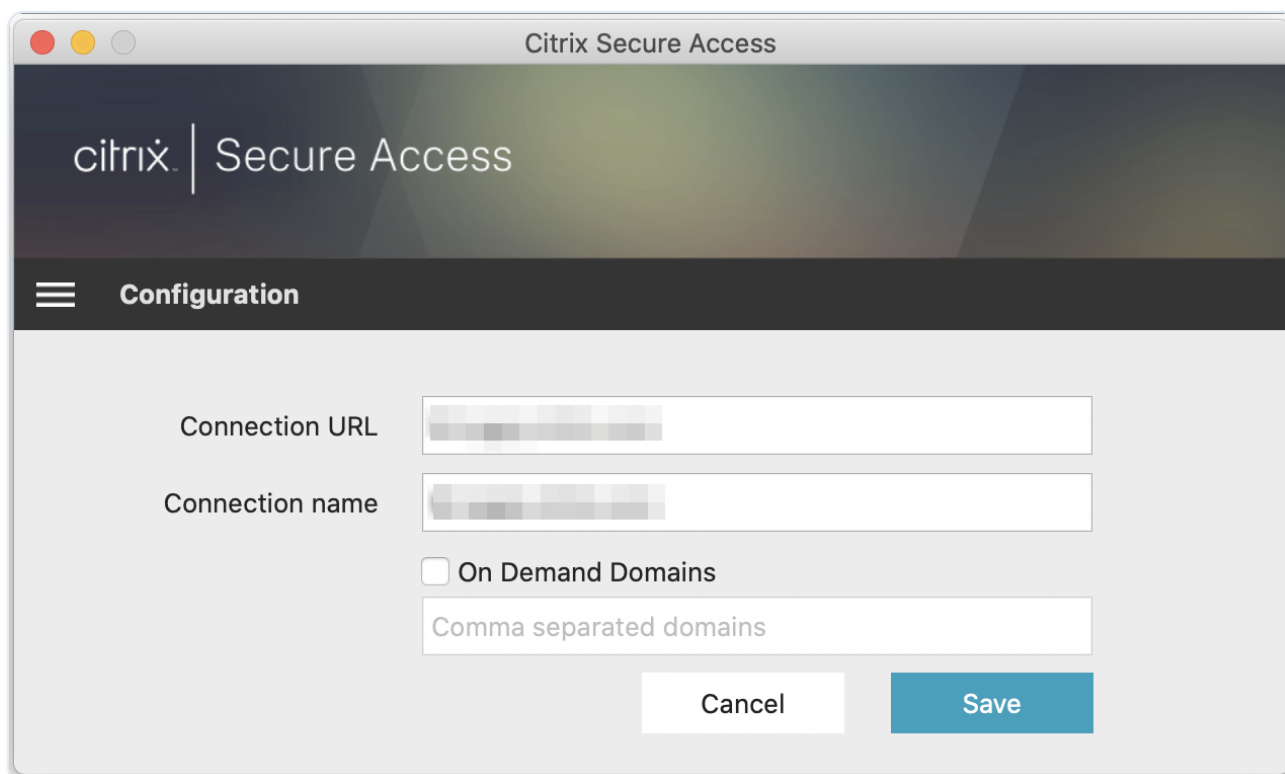


Modificare una connessione esistente

È possibile modificare o eliminare una connessione esistente.



Modificare i dettagli della connessione come richiesto.

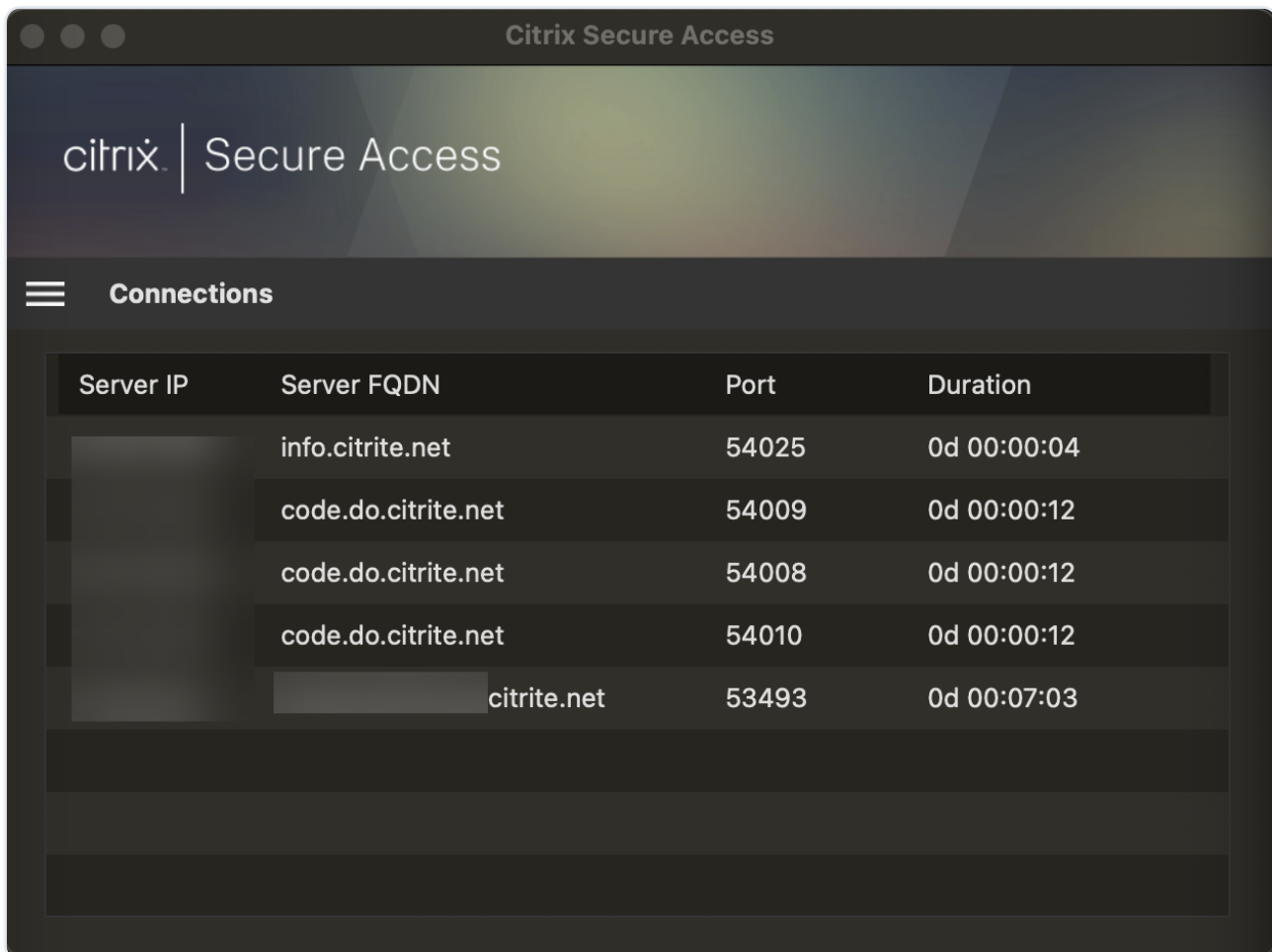


The screenshot shows a macOS-style window titled "Citrix Secure Access". The window has a dark header bar with the Citrix logo and the text "Secure Access". Below the header, there is a dark navigation bar with a hamburger menu icon and the word "Configuration". The main content area is light gray and 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 below the checkbox with the placeholder text "Comma separated domains".
- At the bottom right, there are two buttons: "Cancel" (white with gray text) and "Save" (blue with white text).

Informazioni sulle connessioni protette

A partire dalla versione 23.09.1, è possibile visualizzare i dettagli della connessione protetta che includono l'indirizzo IP, il FQDN, la porta di destinazione e la durata della connessione. Per visualizzare questi dettagli, fare clic sul menu hamburger nell'interfaccia utente e accedere a **Connections**.



The screenshot shows the Citrix Secure Access application window. At the top, the title bar reads 'Citrix Secure Access'. Below it, the header area contains the 'citrix | Secure Access' logo. A sidebar menu on the left has a hamburger icon and the label 'Connections'. 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

Accesso LAN locale

Il client Citrix Secure Access per macOS 23.10.1 supporta la funzionalità di accesso LAN locale, che consente di determinare se si desidera accedere alle risorse LAN locali sul computer client una volta stabilita una connessione VPN. È possibile utilizzare questa funzionalità solo se l'amministratore ha configurato l'impostazione di accesso LAN locale su NetScaler Gateway.

Per abilitare l'accesso LAN locale sull'interfaccia utente del client Citrix Secure Access, accedere alla home page e abilitare la casella di controllo **Consenti accesso LAN locale**.

Dopo aver stabilito una connessione, è possibile verificare lo stato dell'accesso LAN locale nella stessa pagina.

Single sign-on automatico a Citrix Secure Access tramite l'app Citrix Workspace

Importante:

Questa funzionalità è disabilitata per impostazione predefinita. Per utilizzarla, contattare l'amministratore.

A partire da Citrix Secure Access per macOS 24.03.1, un accesso all'app Citrix Workspace può eseguire il single sign-on (SSO) degli utenti finali a Citrix Secure Access, stabilire un tunnel utente e fornire un accesso trasparente alle applicazioni TCP/UDP. Se si è connessi all'app Citrix Workspace, Citrix Secure Access per macOS può essere avviato automaticamente ed è possibile accedere senza problemi utilizzando il single sign-on.

Quando si accede all'app Citrix Workspace, il client Citrix Secure Access viene avviato automaticamente e si esegue il single sign-on al client. Quando si esce dall'app Citrix Workspace, Citrix Secure Access disconnette automaticamente l'utente dall'applicazione senza alcun intervento manuale. Questa funzionalità consente di risparmiare tempo poiché gli utenti finali devono accedere a una sola applicazione, fornendo così un'esperienza unificata.

Nota:

Affinché questa funzionalità funzioni, l'URL primario a cui si accede tramite l'app Citrix Workspace e il client Citrix Secure Access deve essere lo stesso.

Prerequisiti

1. Gli utenti finali devono utilizzare [Citrix Workspace app 2402](#) o versioni successive. Per i dettagli sull'installazione dell'app Citrix Workspace per Mac, vedere [Citrix Workspace app per Mac](#).
2. Gli utenti finali devono utilizzare [Citrix Secure Access per macOS 24.03.1](#) o versioni successive.

Punti da notare:

- Se gli utenti finali sono già connessi all'app Citrix Workspace prima di utilizzare questa funzionalità, devono effettuare nuovamente l'accesso all'app Citrix Workspace in modo che l'app possa attivare un single sign-on al client Citrix Secure Access.
- Quando un utente si disconnette dall'app Citrix Workspace a causa di un timeout, disconnessione manuale dell'utente e così via, anche Citrix Secure Access viene

disconnesso e la sessione utente viene interrotta (questo solo se Citrix Secure Access è stato avviato automaticamente tramite l'app Citrix Workspace).

- L'accesso SSO dall'app Citrix Workspace a Citrix Secure Access è supportato solo su un singolo dominio primario. L'SSO su più domini non è supportato.
- Se si cambia la connessione dell'app Citrix Workspace a un URL diverso dopo aver effettuato l'accesso singolo a Citrix Secure Access tramite questa funzionalità, viene richiesto di scegliere l'URL di connessione dell'app Citrix Workspace.

App Citrix Workspace(/en-us/citrix-ssso/media/switch-cwa-connection.png)

Invia log

L'acquisizione dei log di debug è una parte fondamentale della risoluzione dei problemi o della segnalazione di problemi al supporto Citrix. Per risolvere i problemi relativi ai log, accedere a **Home > Log**.

Fare clic sulla scheda Log(/en-us/citrix-ssso/media/ssso-macos-logs1.png)

Selezionare uno dei seguenti livelli di log della sessione:

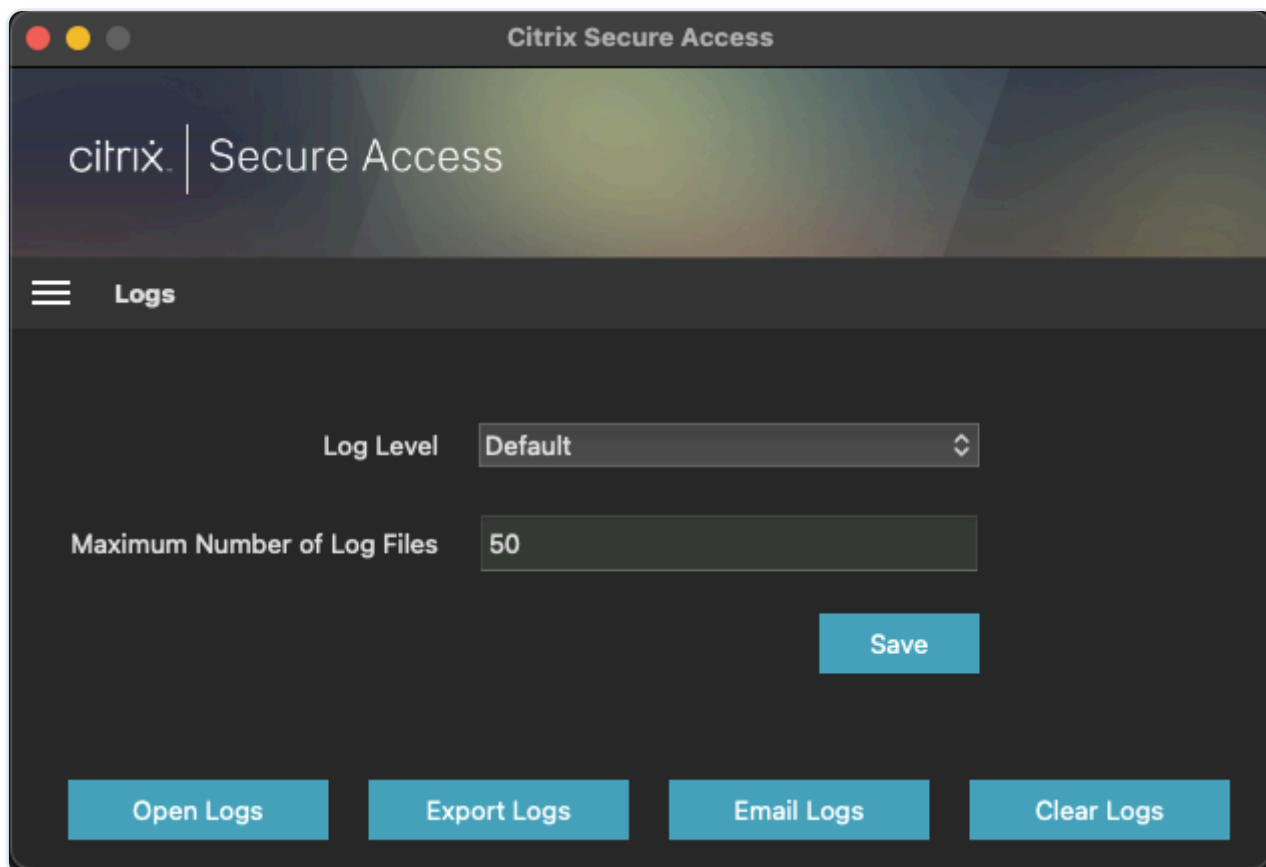
- **Predefinito**: Stampa i log minimi per la risoluzione dei problemi di base.
- **Messaggi di debug**: Stampa tutti i log.
- **Dettagliato**: Stampa i log dettagliati, inclusi i messaggi del tunnel e le informazioni di configurazione.

A partire dalla versione 23.07.1, è possibile utilizzare il campo **Numero massimo di file di log** per specificare il numero di file che si desidera aggiungere per la raccolta dei log. È possibile aggiungere fino a 50 file di log.

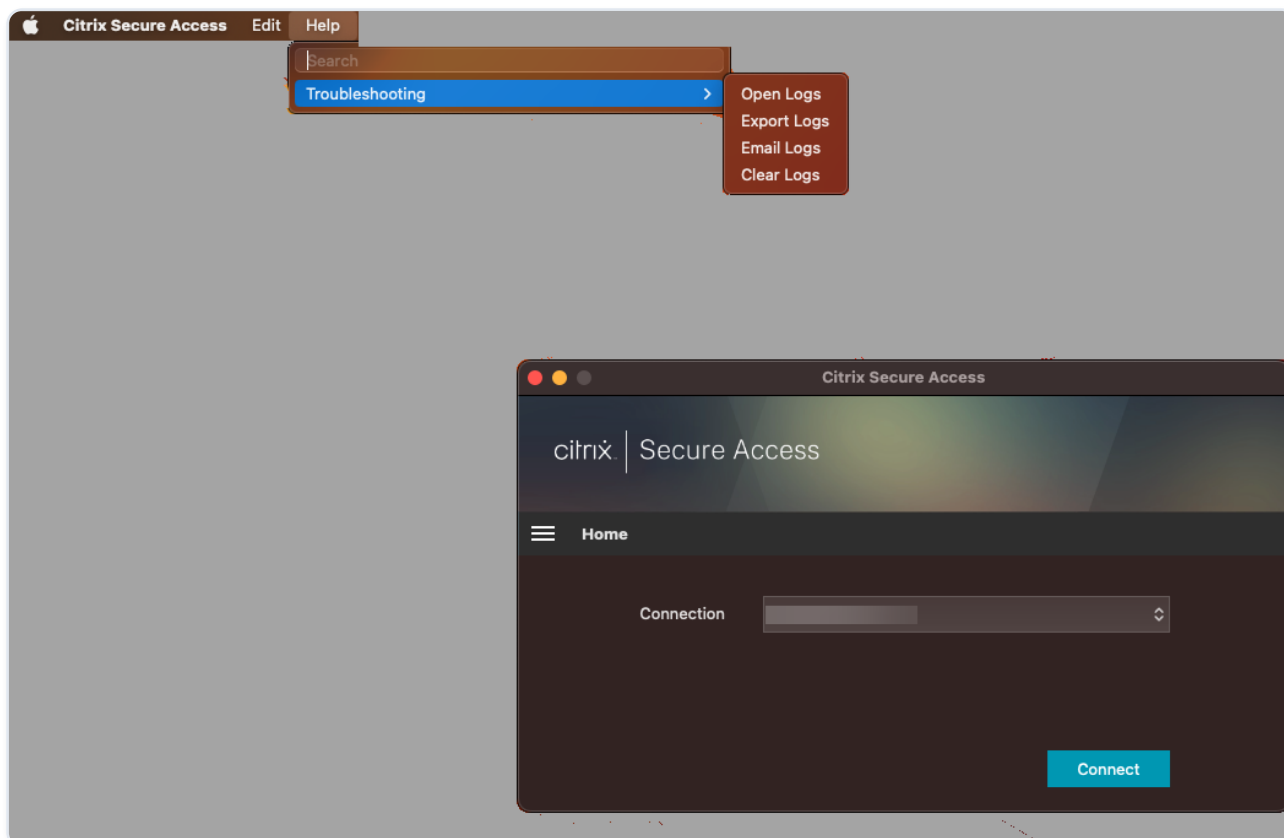
- Fare clic su **Apri log** per visualizzare i log.
- Fare clic su **Esporta log** per esportare i log nella directory locale.
- Fare clic su **Email Logs** per inviare i log via e-mail.
- Fare clic su **Clear Logs** per eliminare i log meno recenti.

Nota:

A partire dalla versione 23.07.1 di Citrix Secure Access per macOS, l'opzione **Email Logs** è disponibile nella pagina **Logs**.



A partire da Citrix Secure Access per macOS 23.06.1, è stato introdotto un menu Guida nella barra di navigazione del client Citrix Secure Access. Questo menu può essere utilizzato come posizione alternativa per acquisire e inviare i log di debug.



Riferimento

Per istruzioni specifiche per l'amministratore su Citrix SSO per iOS, vedere [Citrix SSO per iOS](#) e [Citrix Secure Access per macOS](#).

Client Citrix Secure Access per Linux

Il client Citrix Secure Access per Linux è un software client VPN gestito da NetScaler Gateway che consente di accedere a dati e applicazioni aziendali da remoto.

Il client Citrix End Point Analysis (EPA) è un software client gestito da NetScaler Gateway. Verifica i criteri dell'endpoint prima di concedere l'accesso ai dati aziendali tramite NetScaler Gateway. Il client Citrix EPA e il client Citrix Secure Access sono indipendenti l'uno dall'altro.

È possibile installare il client Citrix EPA solo se l'amministratore lo ha configurato. Per istruzioni specifiche per l'amministratore, vedere [Client Citrix Secure Access per Linux](#).

Aggiornamento importante:

Stiamo aggiornando la nostra interfaccia utente e la documentazione del prodotto al nuovo marchio NetScaler. Potreste vedere riferimenti a Citrix e NetScaler usati in modo intercambiabile durante questo periodo di transizione.

Installa il client Citrix Secure Access e il client Citrix EPA

Note:

- Quando si installano il client Citrix Secure Access e il client Citrix EPA dal Software Center, è necessario disinstallare le versioni esistenti se non sono aggiornate prima di eseguire l'aggiornamento alla versione più recente. Ciò è necessario perché, a differenza di Ubuntu 18.04, le versioni attuali non possono essere sostituite con le versioni più recenti.
- Su Ubuntu 20.x, se si scarica il client Citrix Secure Access da un browser Firefox e poi lo si apre usando l'opzione **Apri con**, l'installazione potrebbe fallire. Questo perché Firefox scarica il client in una posizione temporanea e l'installazione del client Citrix Secure Access fallisce da questa posizione.

Come soluzione alternativa, si consiglia di selezionare l'opzione **Salva file**. Questa opzione scarica il client Citrix Secure Access nella cartella **Download**. È quindi possibile fare doppio clic sul file scaricato e installare il client Citrix Secure Access.

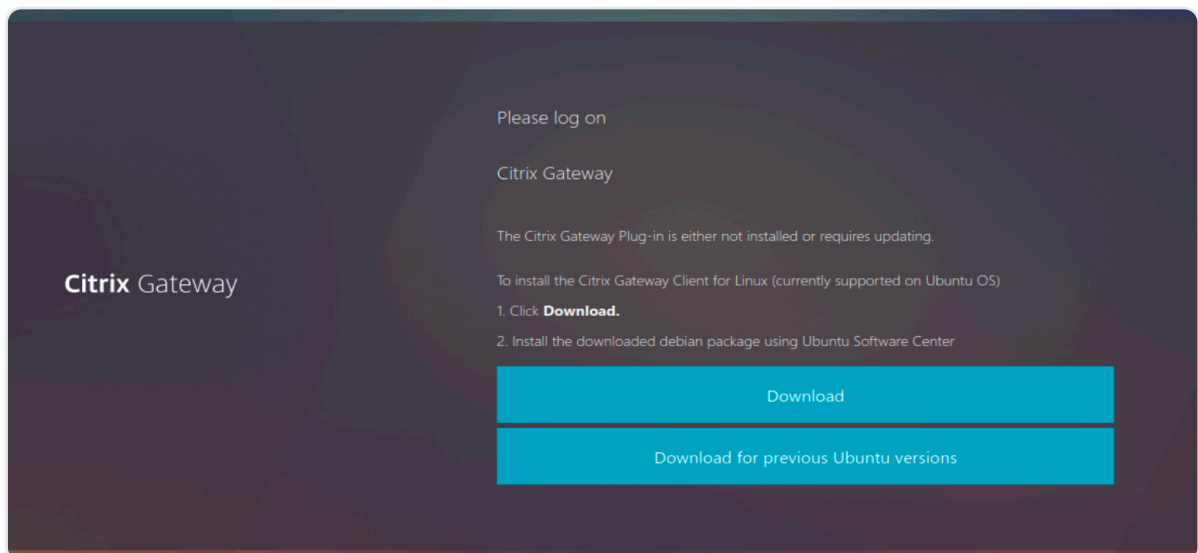
- Nei client Linux sottili come eLux e IGEL OS, il client Citrix Secure Access e il client Citrix EPA sono gestiti dall'amministratore. Gli utenti non possono installare direttamente il client Citrix Secure Access e il client Citrix EPA.

Installa il client Citrix Secure Access e il client Citrix EPA per Ubuntu 20.04

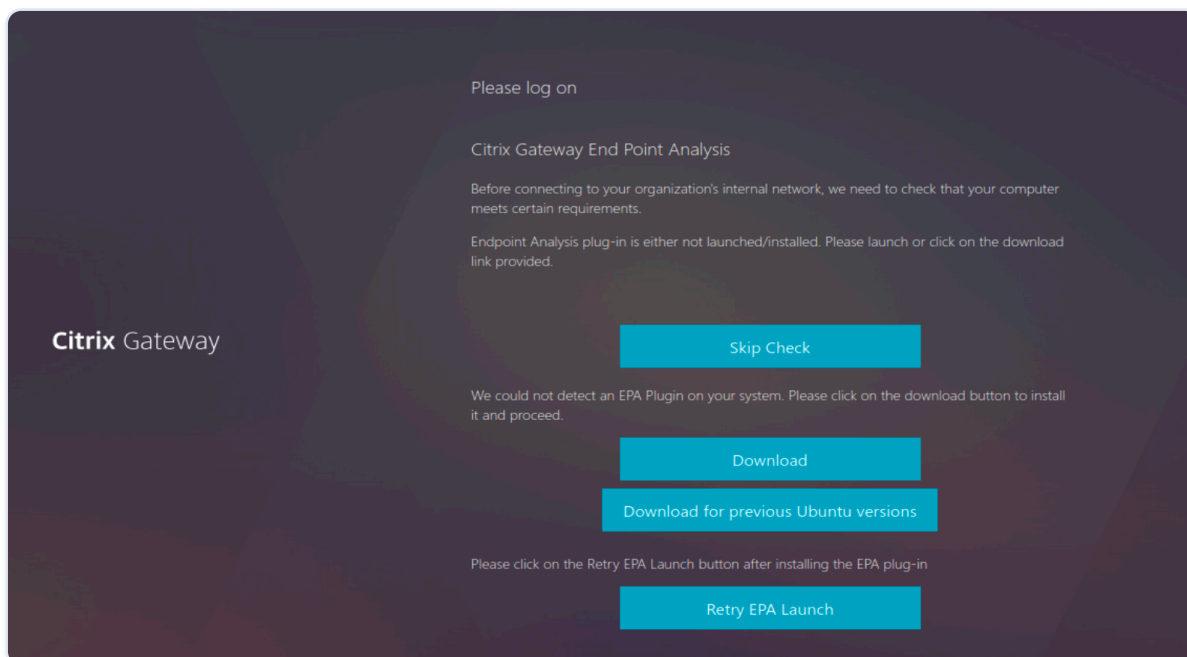
È possibile installare il client Citrix Secure Access e il client Citrix EPA utilizzando le seguenti istruzioni:

1. Scarica il client Citrix Secure Access e il client Citrix EPA utilizzando una delle seguenti opzioni:
 - **Opzione 1:** Aprire un browser web e inserire l'URL di NetScaler Gateway fornito dall'amministratore. Fare clic sul pulsante **Download per le versioni precedenti di Ubuntu** nella schermata di download che appare dopo pochi secondi.

La seguente schermata appare per il download del client Citrix Secure Access:



La seguente schermata appare per il download del client Citrix EPA:



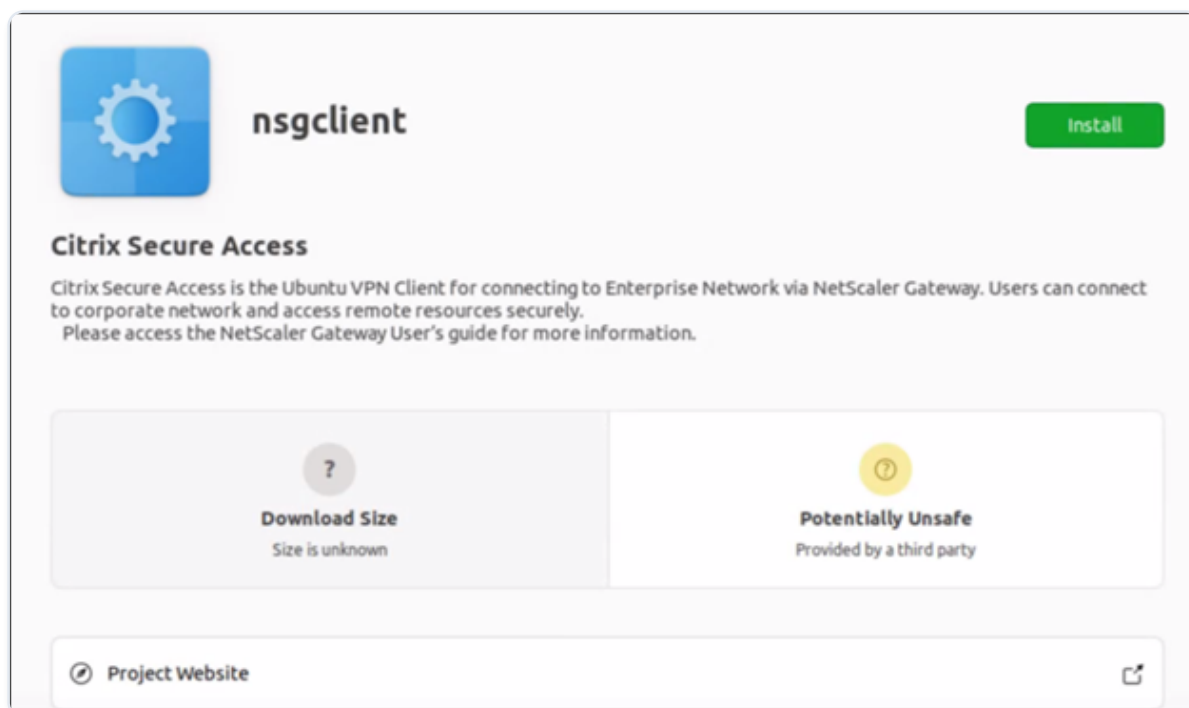
- **Opzione 2:** Andare a [Client Citrix Secure Access per Ubuntu](#) e fare clic sul pulsante **Download** sotto la sezione Ubuntu 20 per scaricare il client Citrix Secure Access e il client Citrix EPA.

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

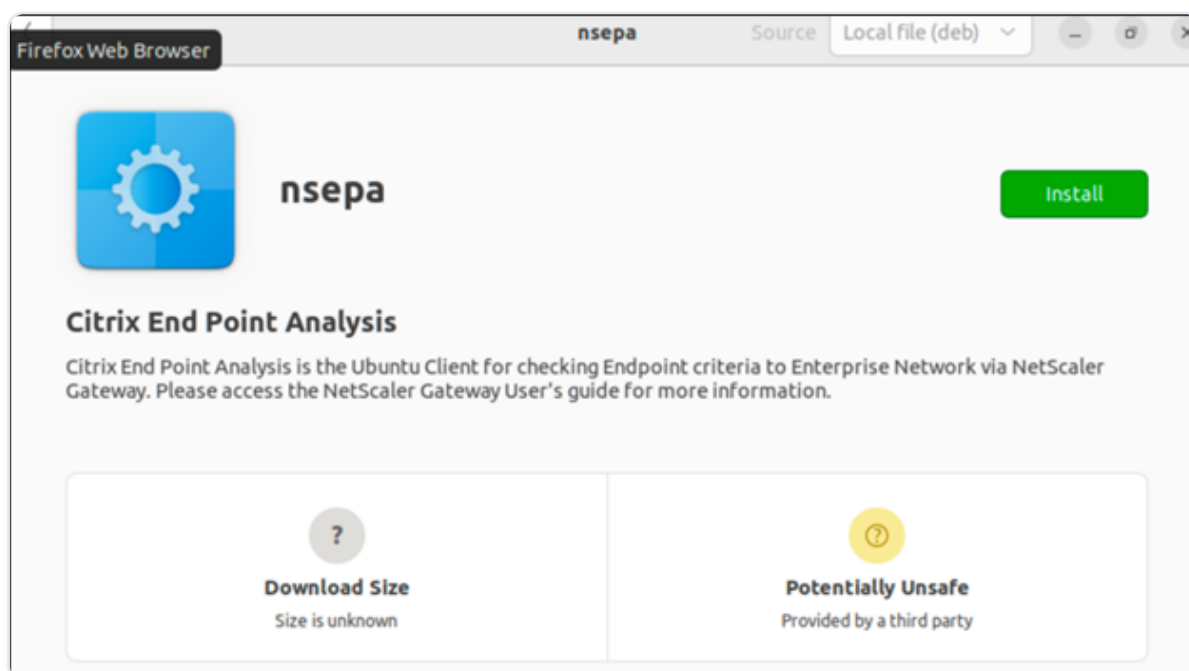
2. Installare il client Citrix Secure Access e il client Citrix EPA dall'interfaccia grafica o utilizzando il terminale Ubuntu.

- Fare doppio clic sul file scaricato e installare il client Citrix Secure Access e il client Citrix EPA.

Viene visualizzata la seguente schermata quando si fa doppio clic sul client Citrix Secure Access scaricato:

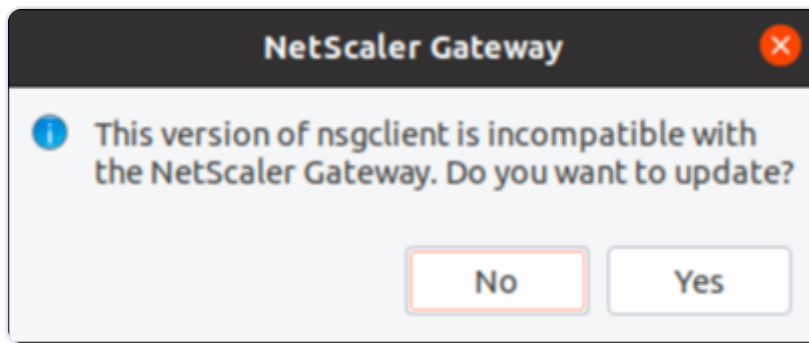


Viene visualizzata la seguente schermata quando si fa doppio clic sul client Citrix EPA scaricato:



Se il client Citrix Secure Access è già installato ma non aggiornato, viene richiesto di eseguire l'aggiornamento alla versione più recente. Fare clic su **Sì** per eseguire l'aggiornamento alla versione più recente, come mostrato nella schermata seguente:

Questo aggiornamento non è applicabile al client Citrix EPA.



- Installare il client Citrix Secure Access e il client Citrix EPA utilizzando il terminale Ubuntu.

Per installare il client Citrix Secure Access, nel terminale, digitare:

```
sudo apt install ./nsgclient18_64.deb

sudo apt install -f
```

Per installare il client Citrix EPA, nel terminale, digitare:

```
sudo apt install ./nsepa18.deb

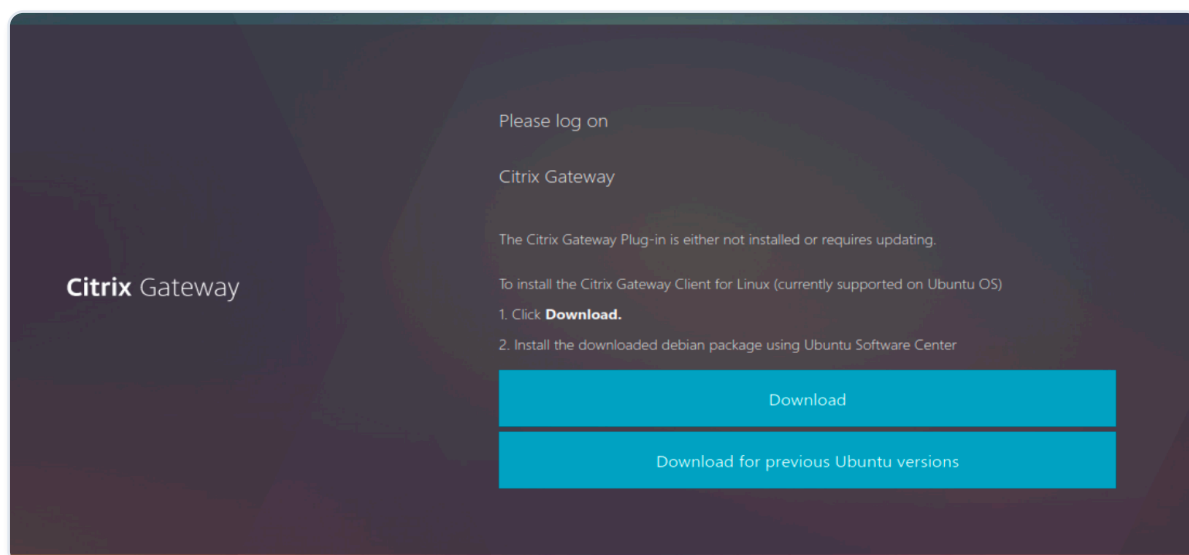
sudo apt install -f
```

Installare il client Citrix Secure Access e il client Citrix EPA per Ubuntu 22.04 e versioni successive

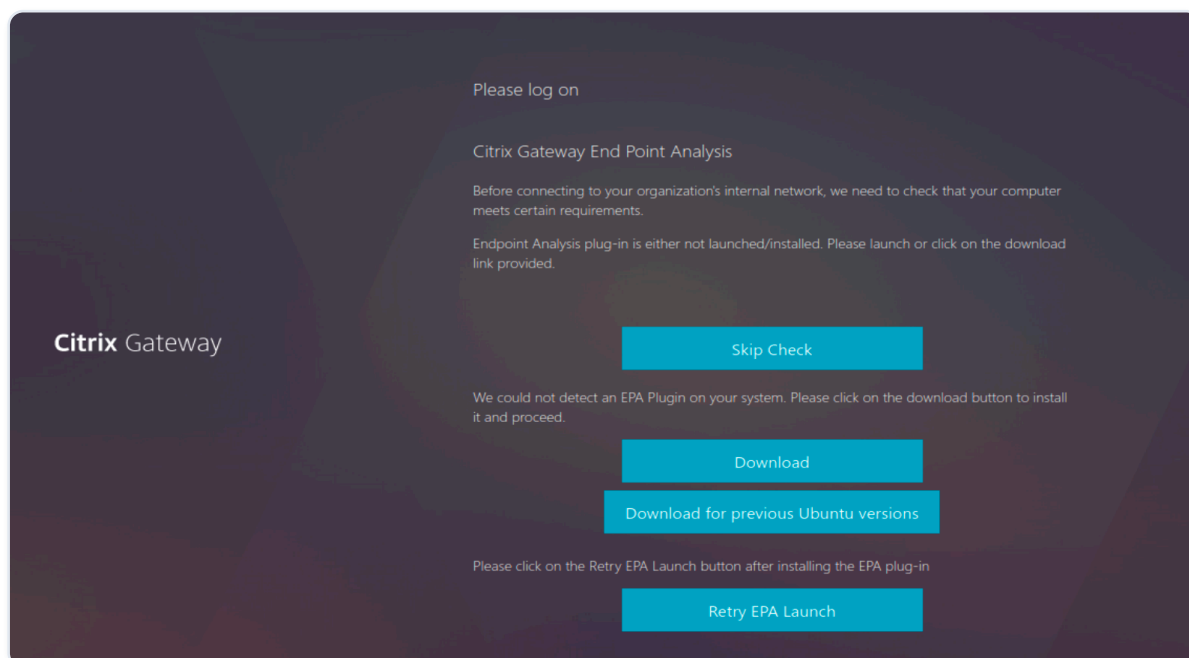
È possibile installare il client Citrix Secure Access e il client Citrix EPA utilizzando le seguenti istruzioni:

1. Scaricare il client Citrix Secure Access e il client Citrix EPA utilizzando una delle seguenti opzioni:
 - **Opzione 1:** Aprire un browser web e inserire l'URL di NetScaler Gateway fornito dall'amministratore. Fare clic sul pulsante **Download** nella schermata di download che appare dopo alcuni secondi

La seguente schermata appare per il download del client Citrix Secure Access:



La seguente schermata appare per il download del client Citrix EPA:



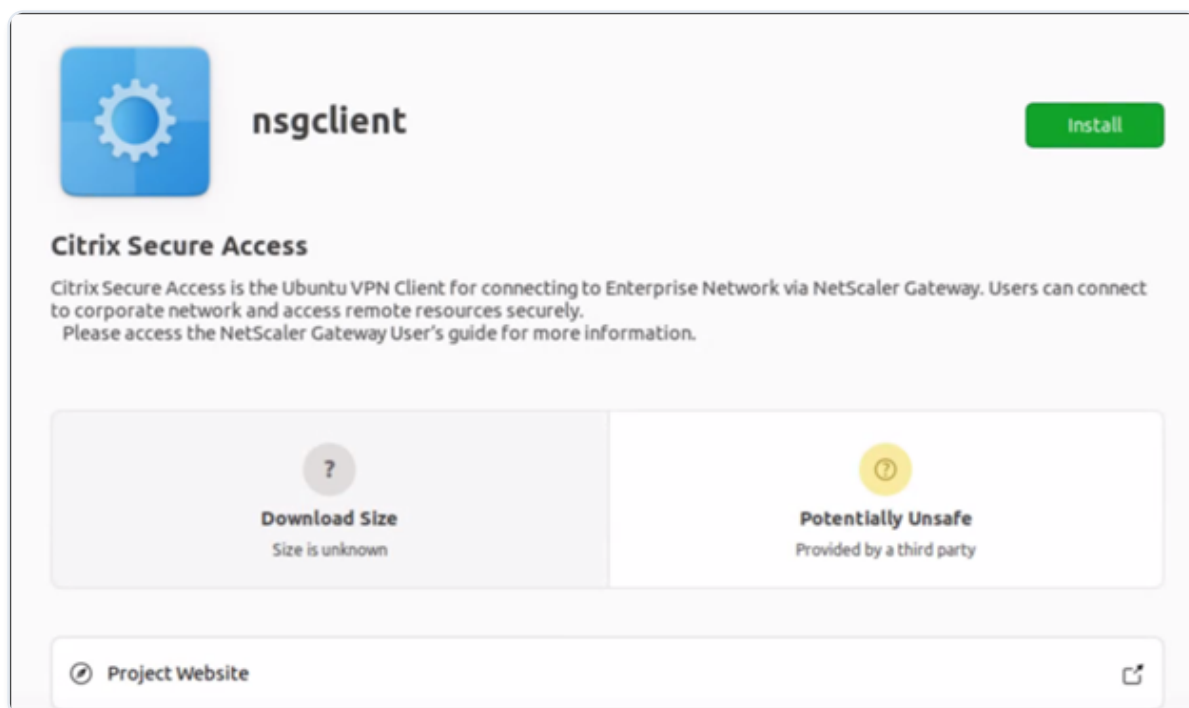
- **Opzione 2:** Andare a [Client Citrix Secure Access per Ubuntu](#) e fare clic sul pulsante **Download** sotto la sezione Ubuntu 22/24 per scaricare il client Citrix Secure Access e il client Citrix EPA.

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

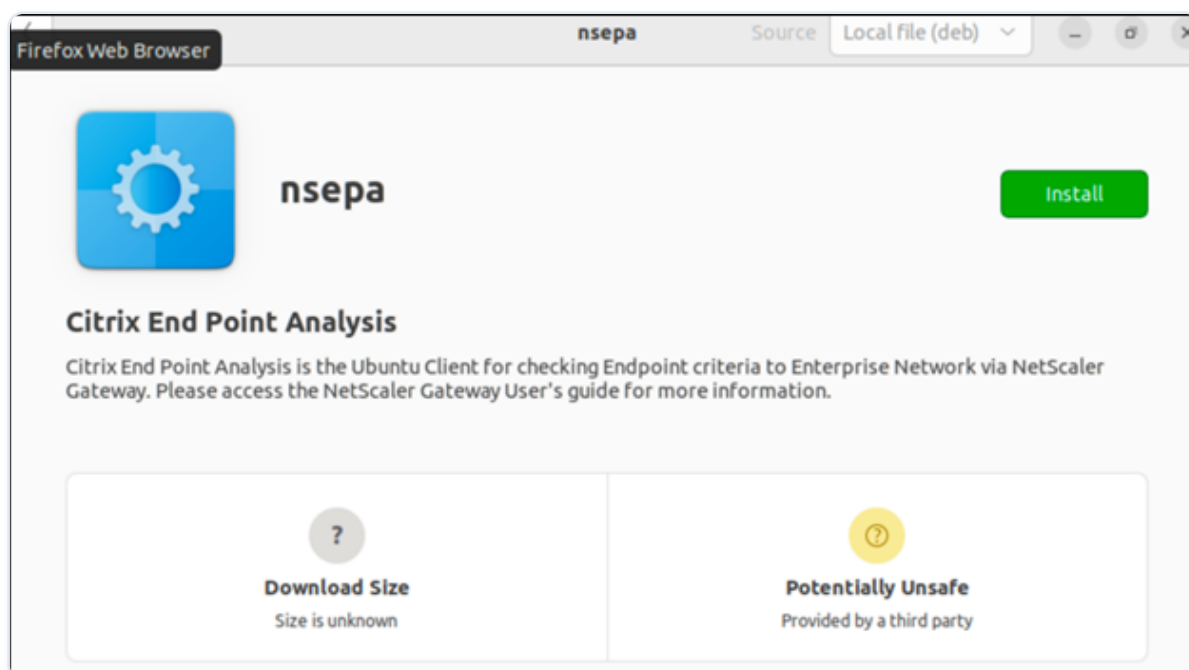
2. Installare il client Citrix Secure Access e il client Citrix EPA dalla GUI o utilizzando il terminale Ubuntu.

- Fare doppio clic sul file scaricato e installare il client Citrix Secure Access e il client Citrix EPA.

La seguente schermata appare quando si fa doppio clic sul client Citrix Secure Access scaricato:

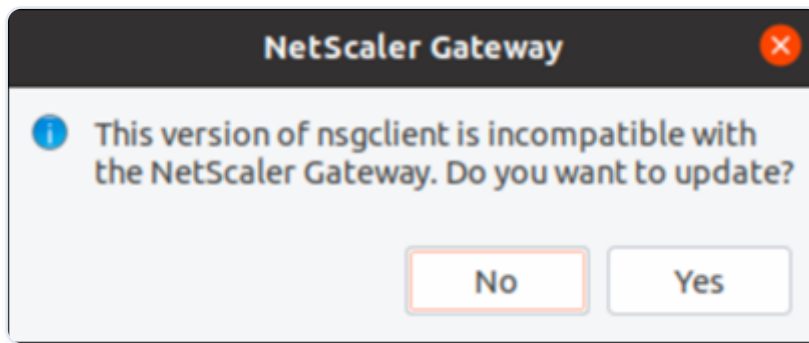


La seguente schermata appare quando si fa doppio clic sul client Citrix EPA scaricato:



Se il client Citrix Secure Access è già installato ma non aggiornato, viene richiesto di eseguire l'aggiornamento all'ultima versione. Fare clic su **Sì** per aggiornare all'ultima versione come mostrato nella schermata seguente:

Questo aggiornamento non è applicabile al client Citrix EPA.



- Installare il client Citrix Secure Access e il client Citrix EPA utilizzando il terminale Ubuntu.

Per installare il client Citrix Secure Access, nel terminale, digitare:

```
sudo apt install ./nsginstaller64.deb

sudo apt install -f
```

Per installare il client Citrix EPA, nel terminale, digitare:

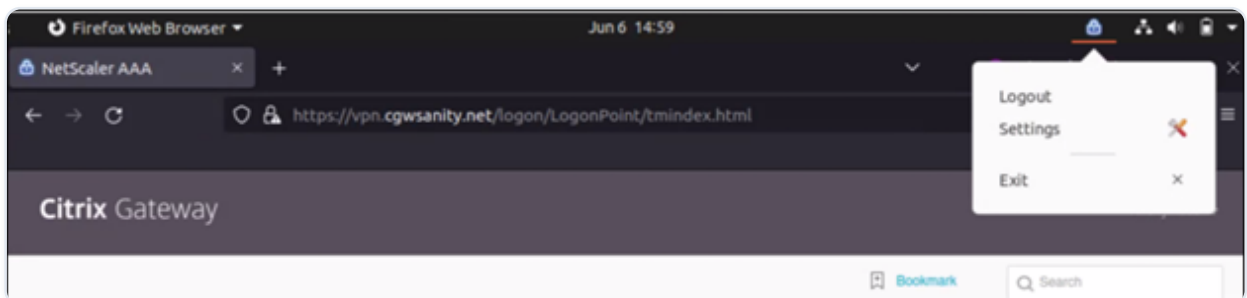
```
sudo apt install ./nsepa.deb

sudo apt install -f
```

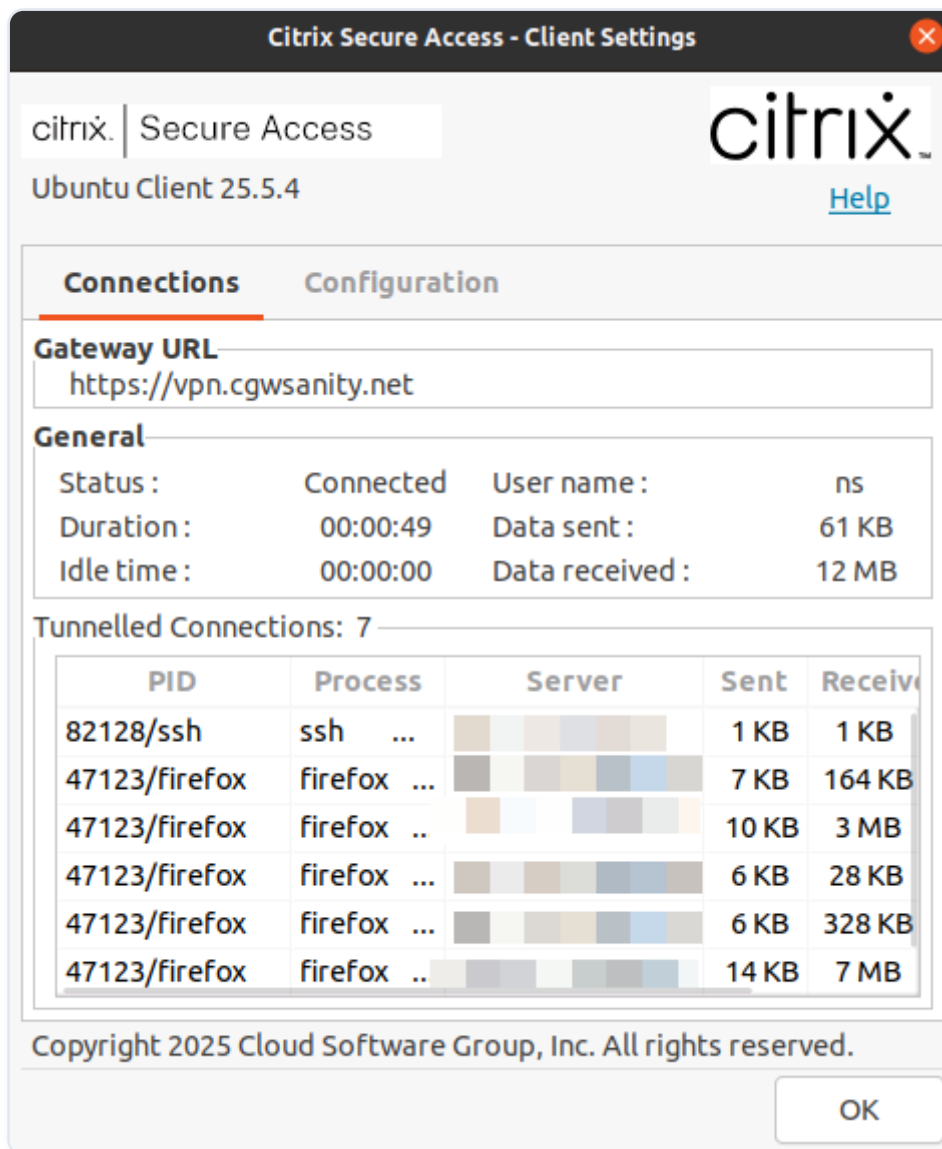
Come usare il client Citrix Secure Access per Linux

Inserisci l'URL di NetScaler Gateway nel tuo browser per autenticarti con il client Citrix Secure Access. Una volta che l'autenticazione è riuscita, il browser ti chiederà di avviare il client Citrix Secure Access.

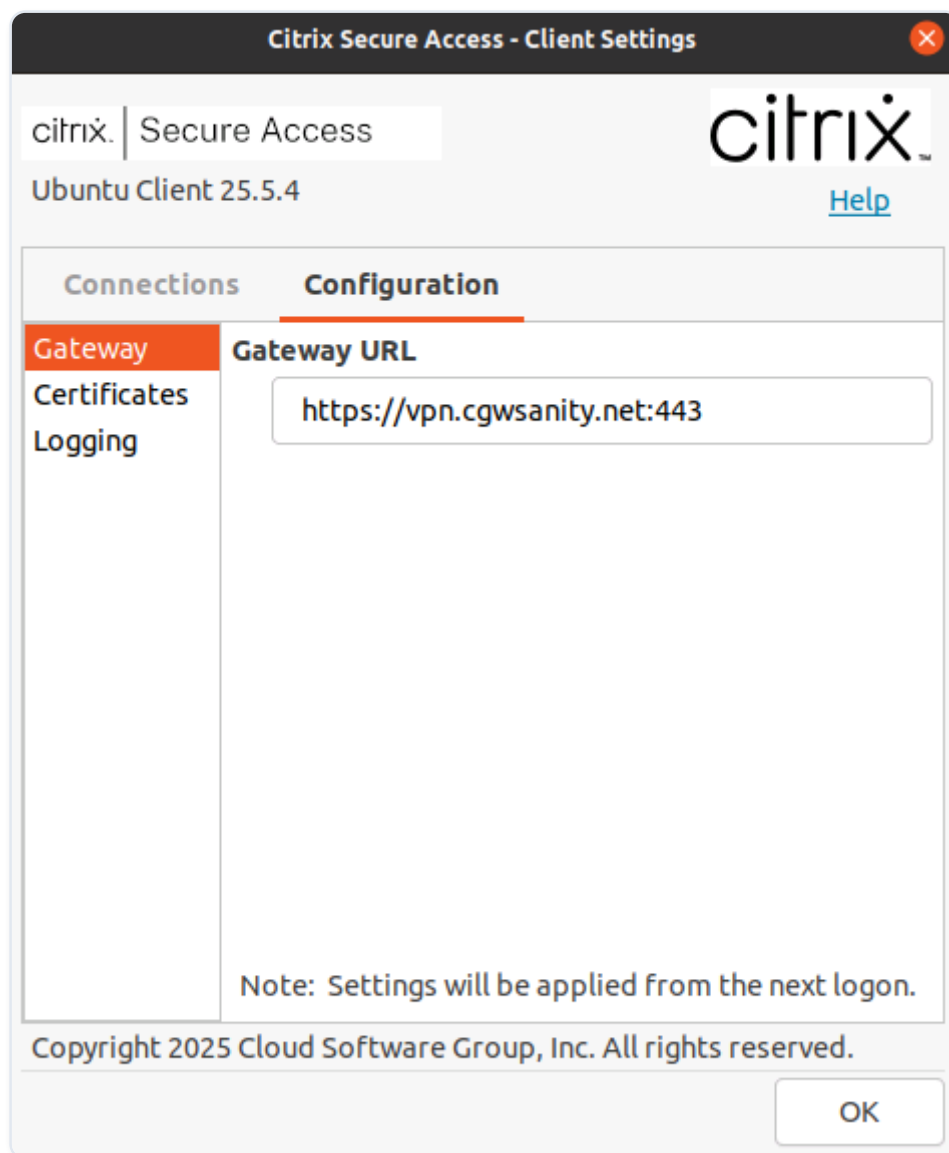
- Seleziona l'icona del client Citrix Secure Access sulla barra delle applicazioni e fai clic su **Impostazioni**.



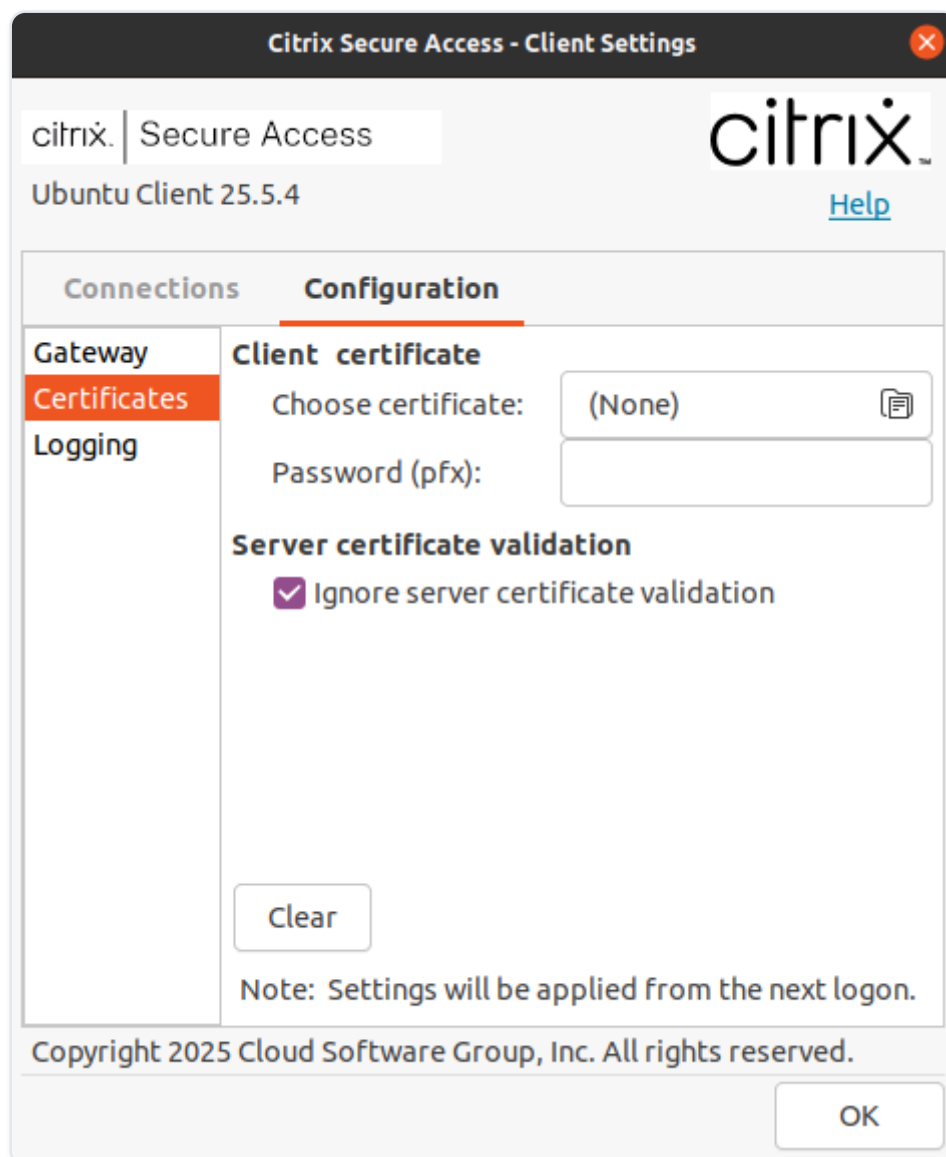
- La scheda **Connessioni** visualizza dettagli come lo stato della connessione, le informazioni utente, le connessioni tunnel e l'utilizzo dei dati.



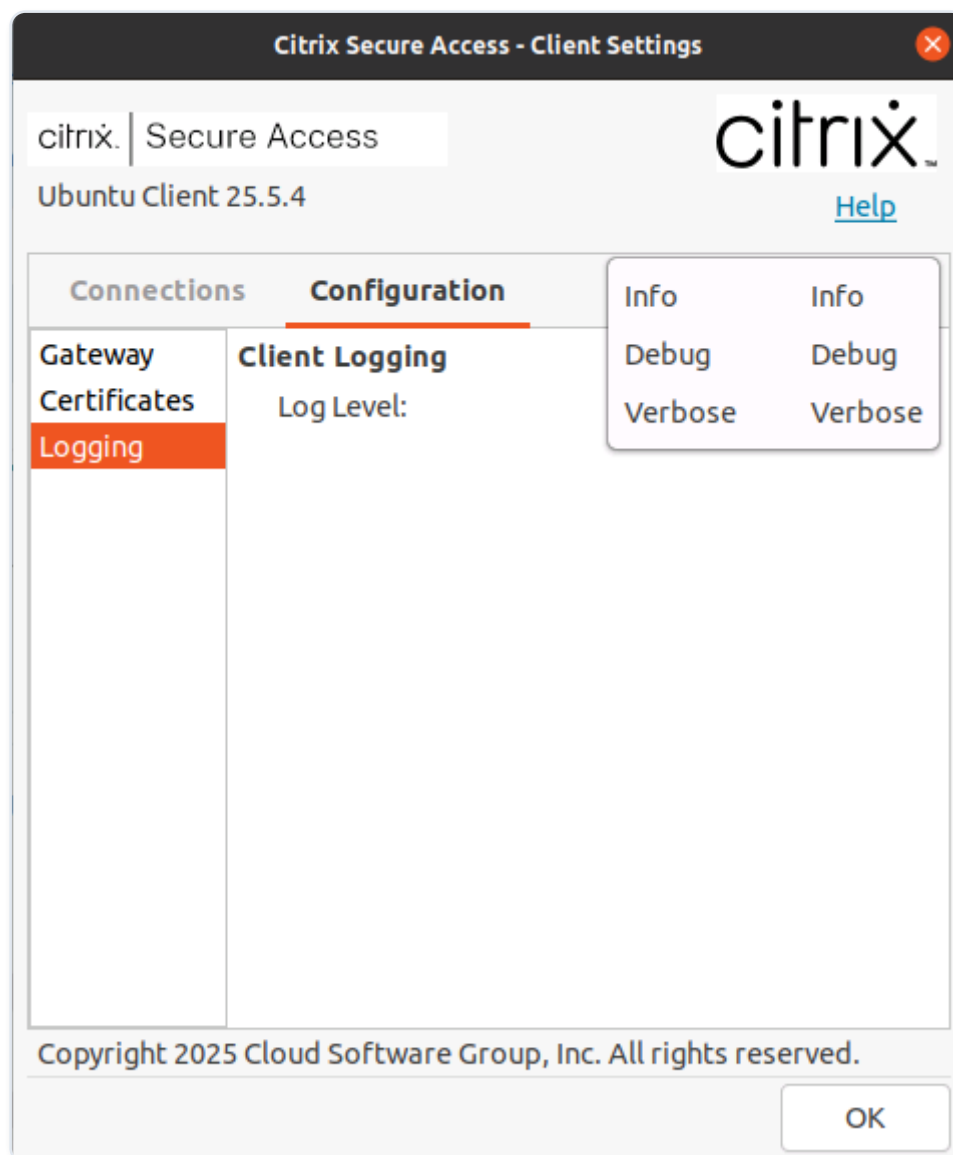
- La scheda **Configurazione** visualizza le informazioni di NetScaler Gateway, un'opzione per caricare un certificato client e le opzioni di registrazione.



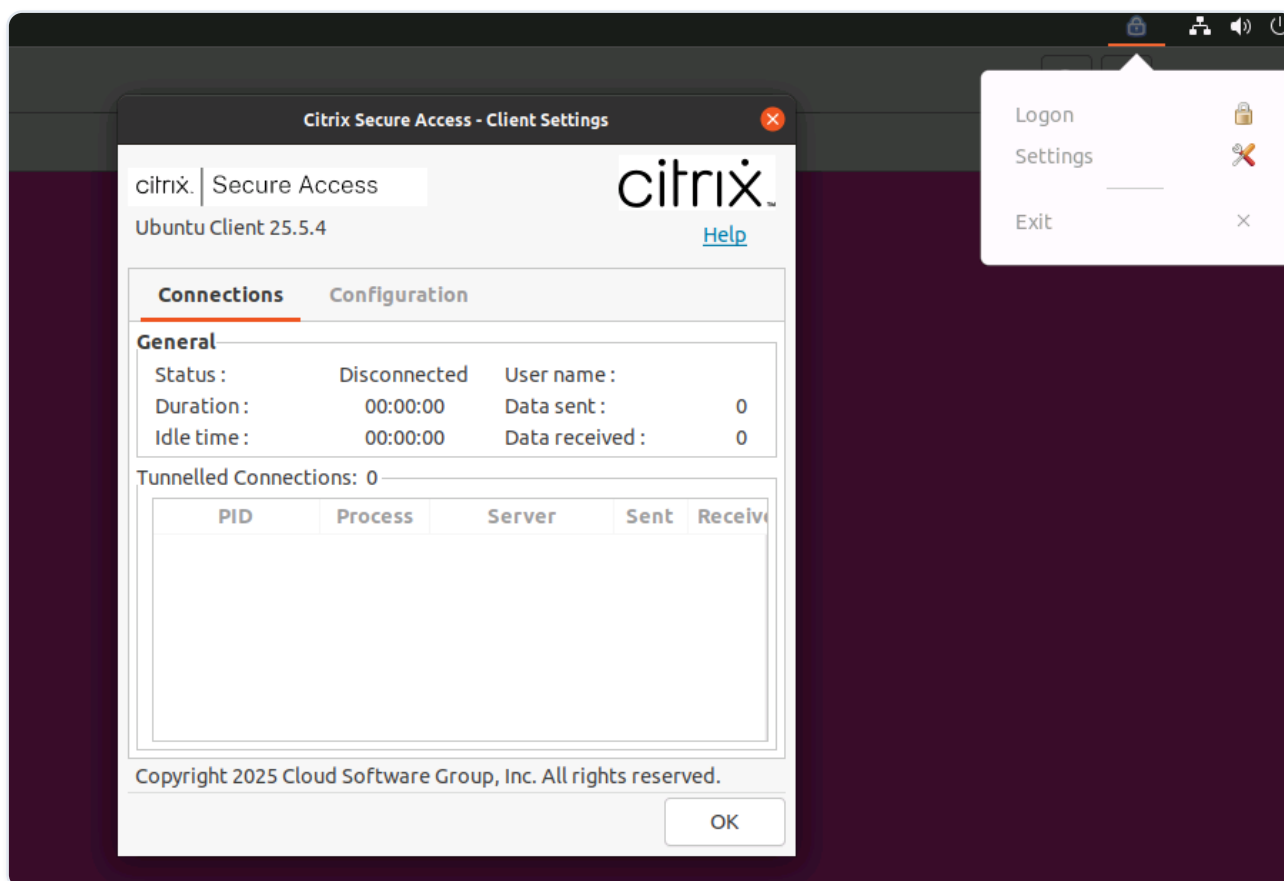
- **Certificati:** Naviga in questa sezione per configurare un certificato client. Questo passaggio è richiesto solo se l'amministratore ti ha fornito un certificato client per l'autenticazione con NetScaler Gateway.



- **Registrazione:** Naviga in questa sezione per acquisire i log di debug. L'acquisizione dei log di debug è una parte fondamentale della risoluzione dei problemi o della segnalazione di problemi al supporto Citrix.



In alternativa, puoi avviare il client Citrix Secure Access e fare clic su **Accesso**. Se sei un utente per la prima volta, ti verrà chiesto di fornire l'URL di NetScaler Gateway o l'URL del tuo spazio di lavoro.



Invia log

I file di log che invii all'amministratore sono nel formato `nsgcepa.txt`, `nsepa.txt`, `nssslvpn.txt` e `epalibv2.log`. Questi file si trovano nella directory `~/.citrix/`.

Acquisiscono i seguenti dettagli:

- **Info:** Stampa i log di base e di errore.
- **Debug:** Stampa tutti i log. Si consiglia di selezionare questa opzione per raccogliere i log e condividerli con l'amministratore.
- **Verbose:** Stampa i log dettagliati, inclusi i messaggi del tunnel e le informazioni di configurazione.

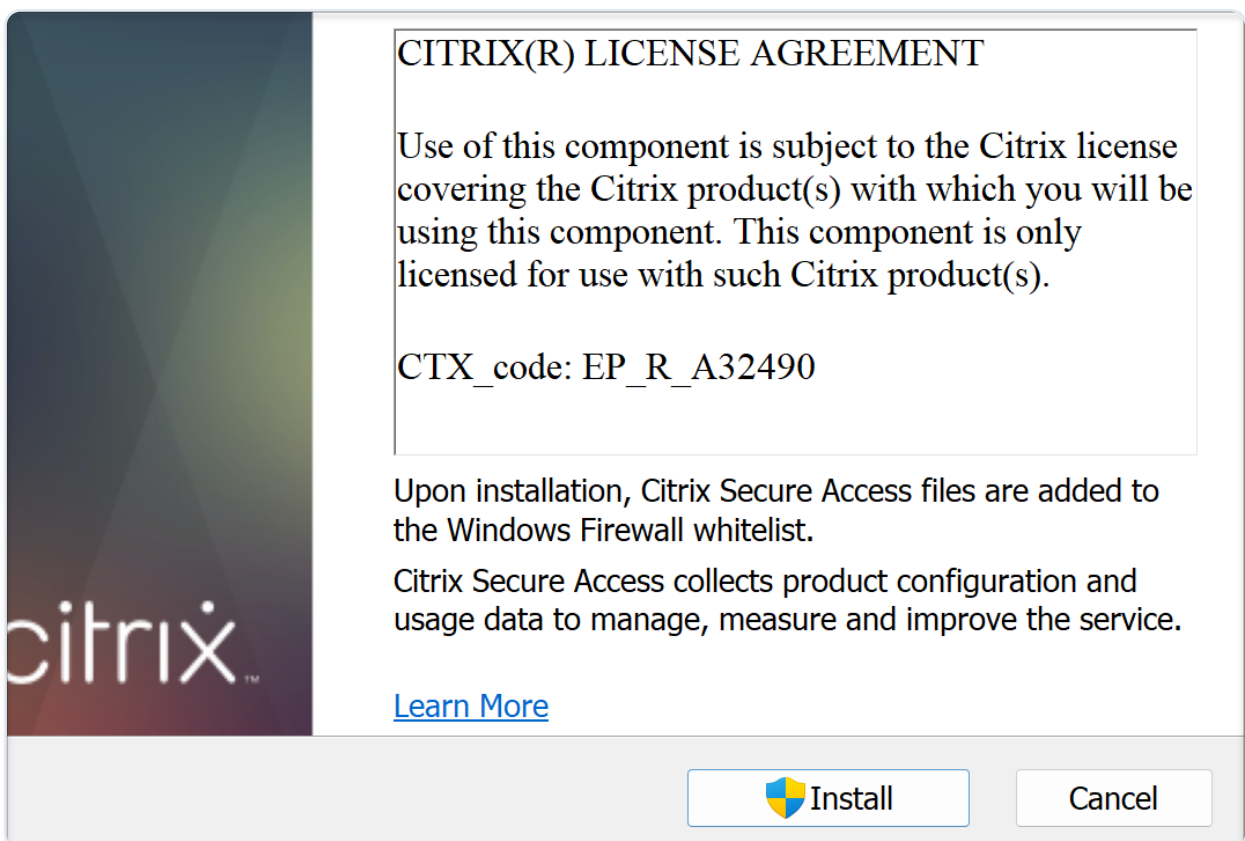
Client Citrix Secure Access per Windows

Il client Citrix Secure Access per Windows è un software client VPN che consente di accedere a dati e applicazioni aziendali in remoto utilizzando NetScaler Gateway e Secure Private Access.

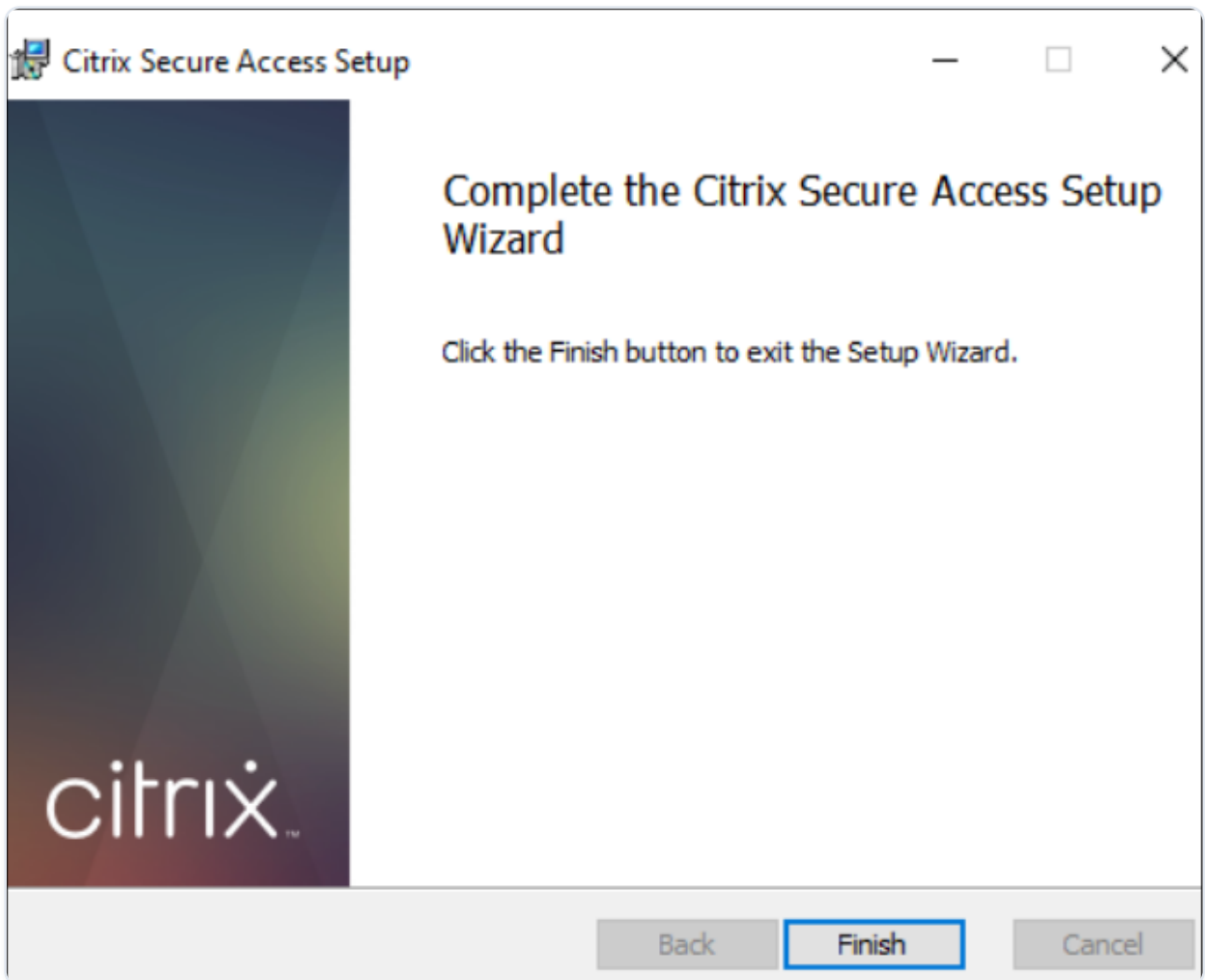
Installare il client Citrix Secure Access per Windows

È possibile installare il client Citrix Secure Access seguendo le istruzioni riportate di seguito, che richiedono i diritti di amministratore:

1. Scaricare il client Citrix Secure Access da [Client Citrix Secure Access per Windows](#).
2. Fare clic su **Installa** per installare il client sul computer Windows. Se si dispone di un client Citrix Secure Access esistente, questo verrà aggiornato.



3. Fare clic su **Fine** per completare l'installazione.



Come usare il client Citrix Secure Access per Windows

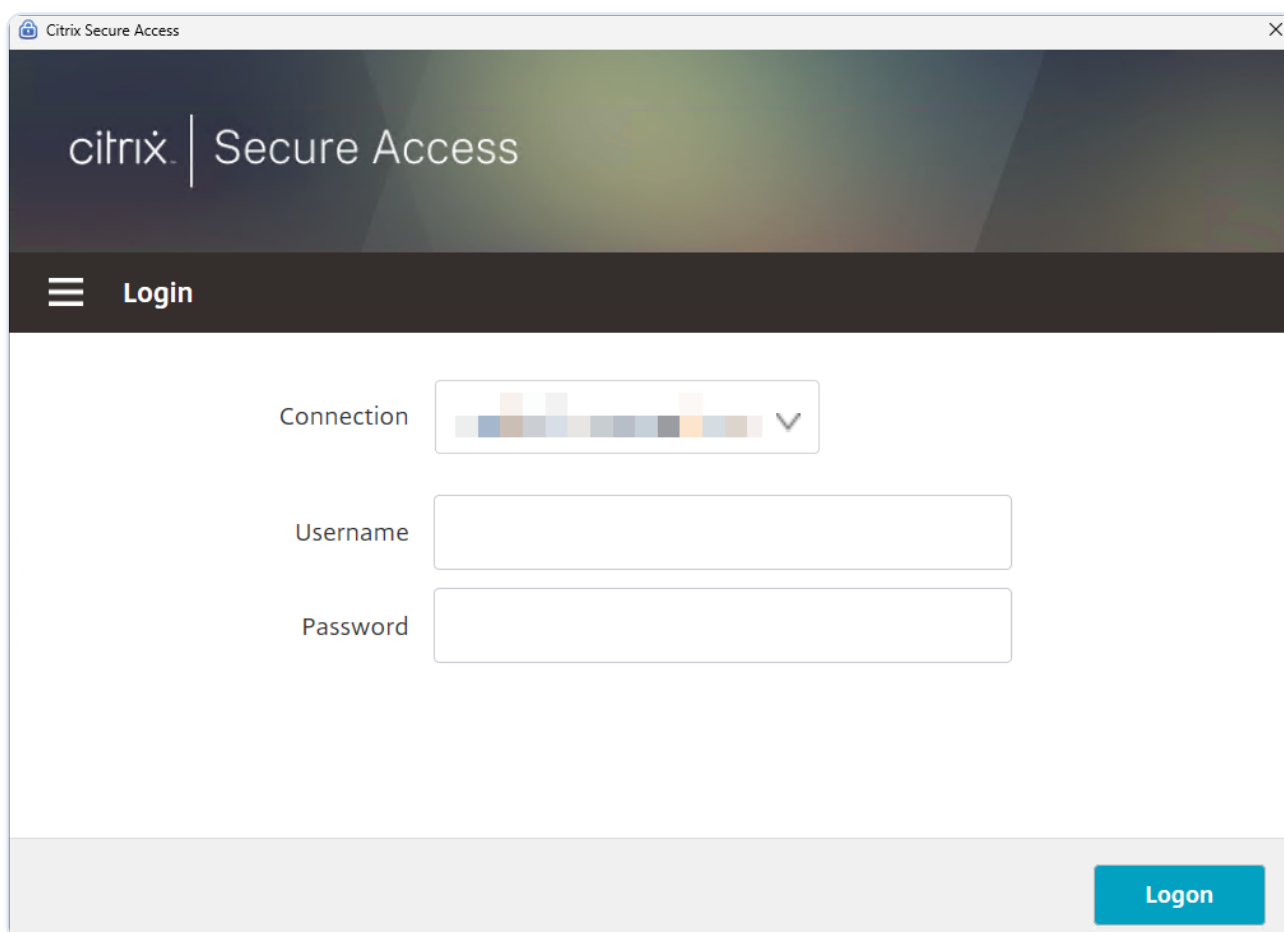
Gli utenti che accedono per la prima volta devono creare una connessione a NetScaler Gateway o Secure Private Access aggiungendo l'URL di connessione, se l'amministratore non ha già aggiunto l'URL di connessione per l'applicazione. Per gli utilizzi successivi, è possibile connettersi a una connessione esistente, aggiungere una connessione e modificare anche le connessioni esistenti. È inoltre possibile visualizzare i log e intraprendere le azioni appropriate di conseguenza.

Aggiungere una connessione

Importante:

Dopo aver aggiunto la connessione, il client Citrix Secure Access richiede l'autenticazione. La richiesta dipende dal metodo di autenticazione configurato in NetScaler Gateway o Secure Private Access. Potrebbe essere necessario inserire una password o una password monouso. In alternativa, potresti essere reindirizzato a un URL di autenticazione SAML.

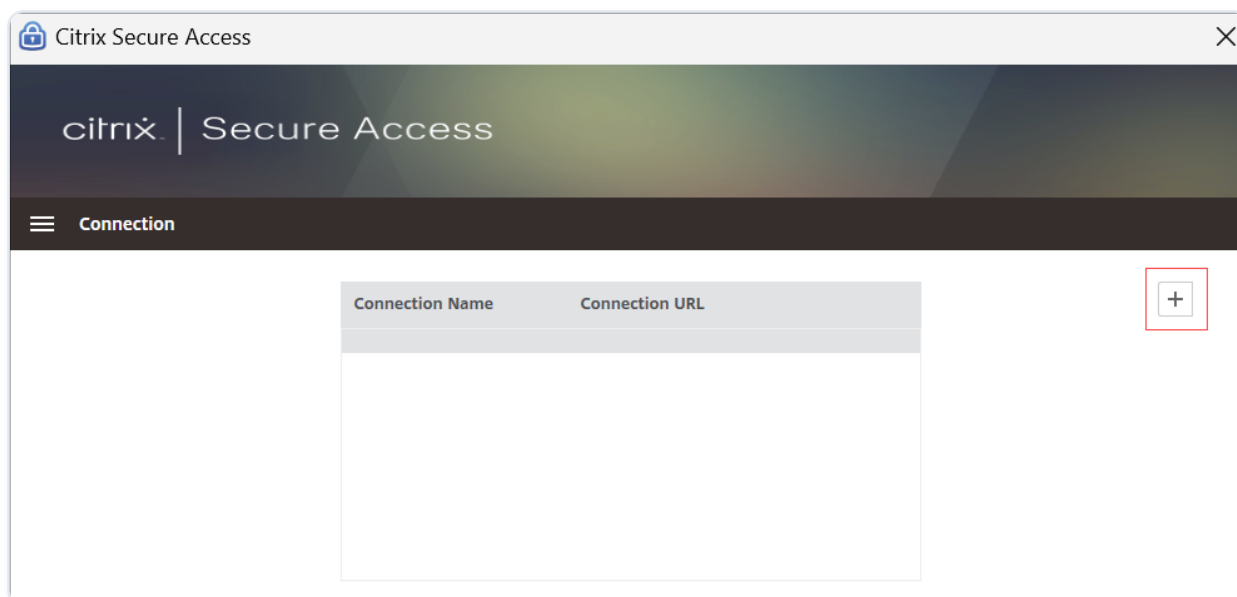
Se l'amministratore ha già aggiunto una connessione all'applicazione, selezionare la connessione dall'elenco a discesa nella pagina **Home**, inserire il nome utente e la password (o la password monouso) e fare clic su **Logon**.



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

Se l'amministratore non ha aggiunto l'URL di connessione, è necessario aggiungere una connessione seguendo i passaggi seguenti:

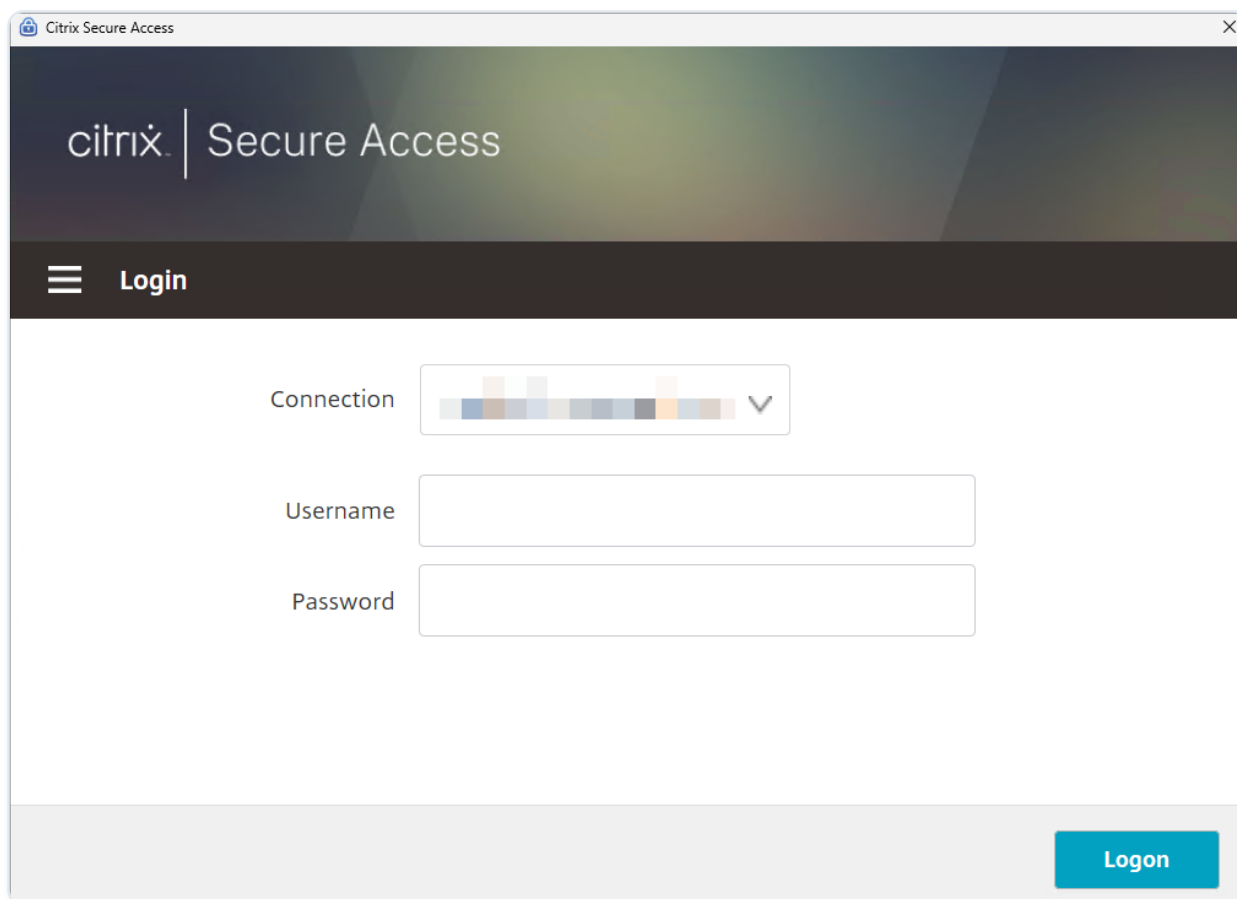
1. Dopo aver installato il client Citrix Secure Access per Windows, aprire l'applicazione nel computer Windows.
2. Passare alla scheda **Connessione** e fare clic su **+** per aggiungere una connessione.



3. Immettere l'URL fornito dall'amministratore nella casella di testo **URL di connessione**, assegnare un nome alla connessione e fare clic su **Salva**.

This screenshot shows the same Citrix Secure Access interface, but now with input fields. The 'Connection URL' label is followed by a text input field. Below it, the 'Connection Name' label is followed by another text input field. At the bottom right of the page, there is a blue button with the text 'Save' in white.

4. Una volta aggiunta la connessione, passare alla scheda **Home**, selezionare la connessione dall'elenco a discesa, inserire il nome utente e la password (o la password monouso) e fare clic su **Logon**.

The image shows a web browser window titled "Citrix Secure Access". The page has a dark header 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 "Login". The main content area is white and 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 of the form is a blue "Logon" button.

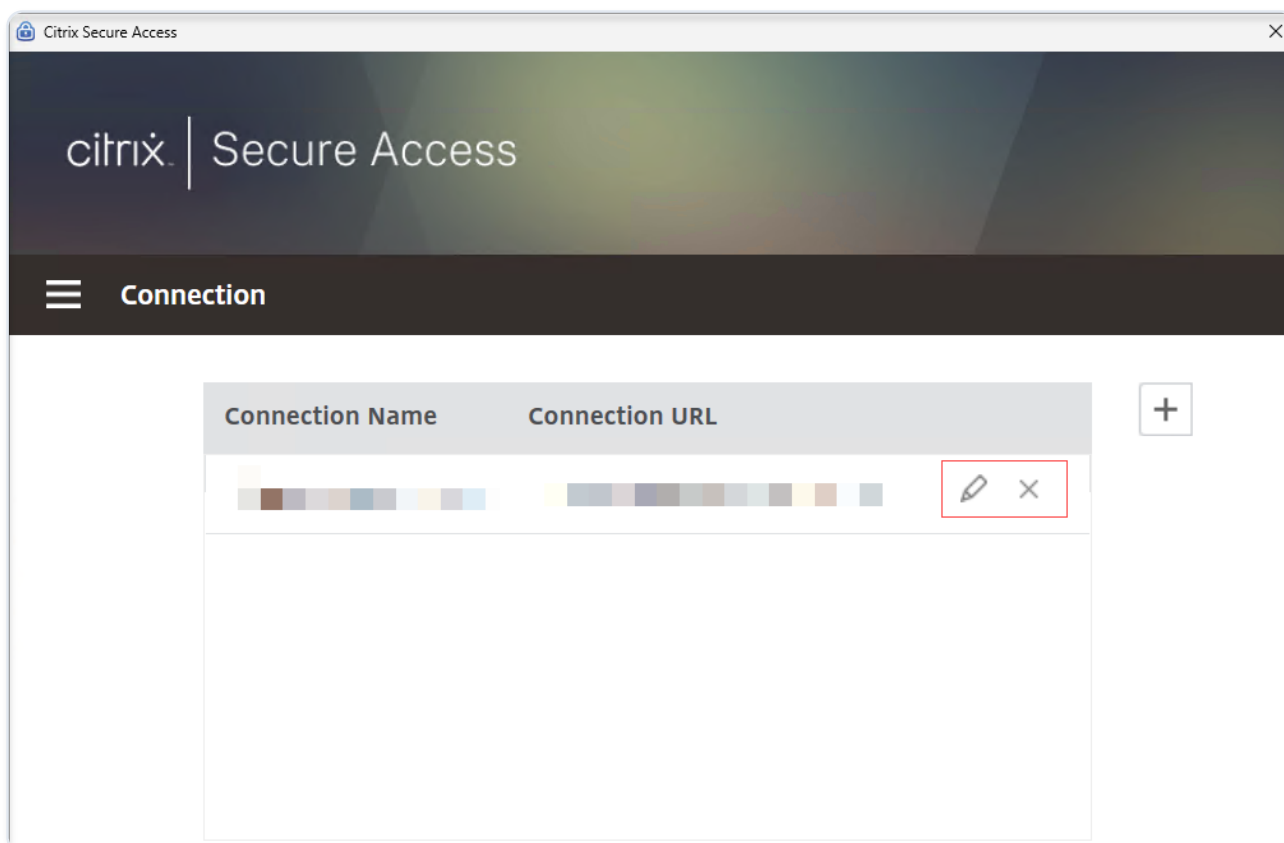
Quando l'autenticazione ha esito positivo, è possibile accedere alle applicazioni intranet.

Nota:

Dopo il login iniziale, non è possibile connettere o disconnettere manualmente la VPN se l'amministratore ha abilitato il profilo [Always On](#) o [Always On before Windows Logon](#) su NetScaler Gateway o Secure Private Access.

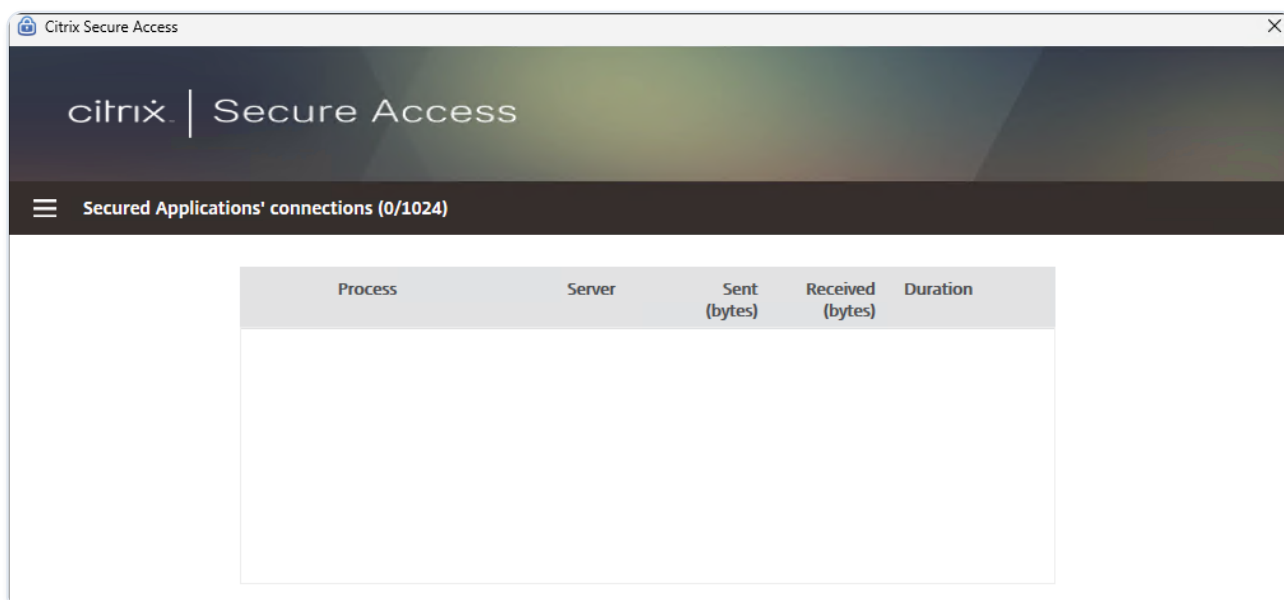
Modificare o eliminare una connessione esistente

Nella scheda **Connessione**, fare clic sull'icona di modifica o sull'icona di annullamento per modificare o eliminare la connessione esistente.



Visualizzare le applicazioni protette

È possibile visualizzare le applicazioni connesse al server, l'IP del server, i dati inviati e ricevuti e la durata della connessione nella scheda **Applicazioni protette**.



Configurare la registrazione

È possibile configurare il livello di log, la dimensione del file e il numero massimo di file di log nella scheda **Registrazione**.

1. **Seleziona livello di log:** Il client Citrix Secure Access per Windows ha due livelli di registrazione:
 - **Info:** Questo livello include messaggi informativi ed eventi rilevanti per l'esecuzione del programma. Include anche errori ed eccezioni.
 - **Dettagliato:** Questo livello include tutti i messaggi di log riportati dal livello **Info** e altri messaggi che potrebbero aiutare nella risoluzione dei problemi.
2. **Limite dimensione file di log:** Immettere la dimensione di ciascun file di log. Il valore massimo è 600 MB.
3. **Numero massimo di file di log:** Immettere il numero di file che si desidera aggiungere per la raccolta dei log. Il valore massimo è 5.
4. Fare clic su **Salva** per salvare le configurazioni di registrazione aggiunte.

La scheda **Registrazione** include le seguenti opzioni:

- **Invia file di log tramite e-mail:** Invia i file di log all'amministratore nel formato nssslvpn.txt.
- **Avvia nuovo file di log:** Crea un nuovo file di log, in genere per avviare una nuova registrazione per una nuova sessione o dopo un evento specifico per la risoluzione dei problemi.
- **Raccogli file di log:** Crea un file zip con tutti i file di log dell'applicazione. Questo file zip viene salvato sul desktop.
- **Apri file di log:** Apre l'ultimo file csa_nssslvpn*.txt.

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 'Info' and 'Verbose (Default)' visible in the expanded list. Below the dropdown 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.