



Citrix SSO per iOS

Contents

Citrix Secure Access per dispositivi iOS	2
Importare e installare certificati nell'app Citrix Secure Access	2
Come utilizzare Citrix Secure Access dal proprio dispositivo iOS	5

Citrix Secure Access per dispositivi iOS

March 16, 2024

Citrix Secure Access per iOS offre la migliore soluzione di accesso alle applicazioni e di protezione dei dati offerta da NetScaler Gateway. Consente di accedere in modo sicuro alle applicazioni business-critical, ai desktop virtuali e ai dati aziendali da qualsiasi luogo e in qualsiasi momento.

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

Importante:

- a partire dalla versione 23.11.1, Citrix SSO per iOS verrà rinominato Citrix Secure Access. Stiamo aggiornando la nostra documentazione e le schermate dell'interfaccia utente per rispecchiare tale modifica del nome.
- Per istruzioni specifiche per l'amministratore su Citrix SSO per iOS, vedere [Citrix SSO per iOS](#) e [Citrix Secure Access per macOS](#).

Importare e installare certificati nell'app Citrix Secure Access

March 16, 2024

Importante:

- a partire dalla versione 23.11.1, Citrix SSO per iOS verrà rinominato Citrix Secure Access. Stiamo aggiornando la nostra documentazione e le schermate dell'interfaccia utente per rispecchiare tale modifica del nome.
- Per istruzioni specifiche per l'amministratore su Citrix Secure Access per iOS, vedere [Citrix Secure Access per iOS](#) e [Citrix Secure Access per macOS](#).

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

- **Server MDM** - Approccio preferito per i clienti MDM. I certificati vengono configurati direttamente nel 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. Seguire i documenti specifici del fornitore MDM per questo approccio.

- **E-mail** - Approccio solo per i clienti non MDM. Gli amministratori inviano un messaggio di posta elettronica con l'identità del certificato utente (certificato e chiave privata) allegato come file PKCS#12 agli utenti. Gli utenti devono avere i propri account di posta elettronica 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 l'estensione/il tipo MIME del certificato utente, da standard `.pfx` o `.p12` rispettivamente a `.citrixsso-pfx` o `.citrixsso-p12`.

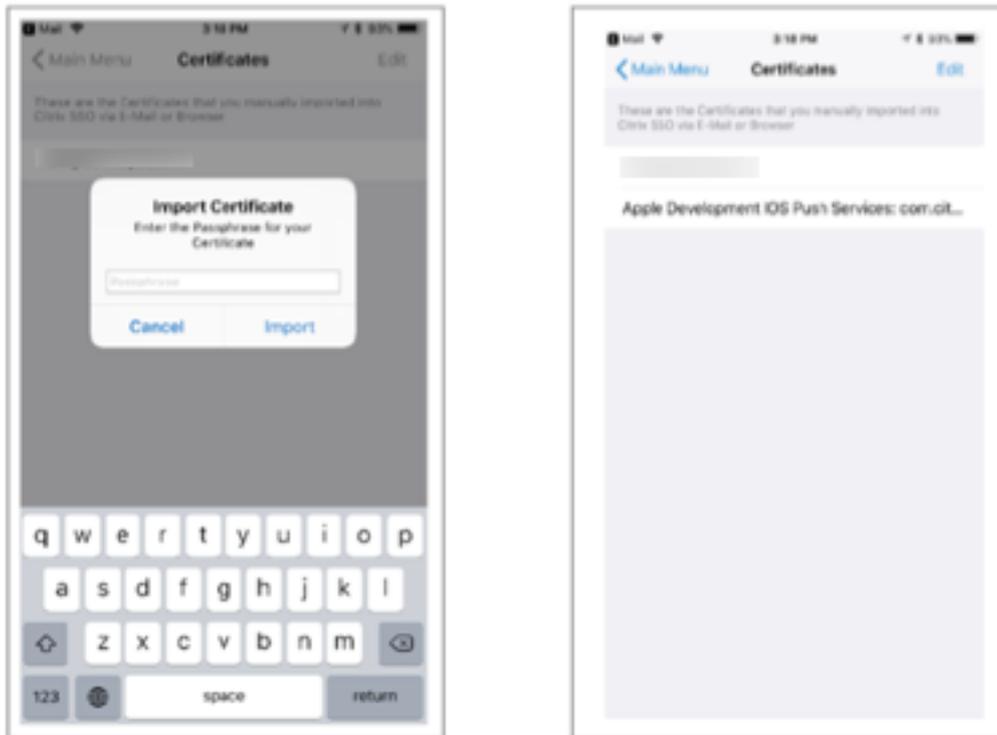
1. Aprire il messaggio di posta elettronica con l'identità del certificato utente (certificato e chiave privata) allegato come file PKCS#12.
 - Toccare l'allegato per visualizzare il menu **OpenIn** del sistema.
 - Toccare **Copy on Citrix SSO**.



2. Installare il certificato in Citrix Secure Access.

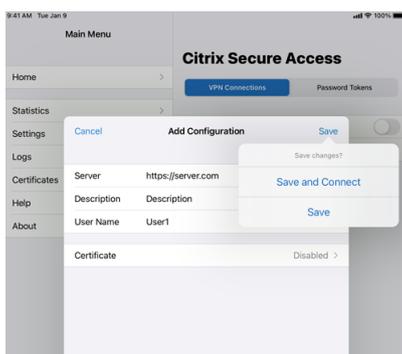
L'app viene avviata e viene visualizzata una richiesta per la passphrase del certificato. Immettere la passphrase corretta per il certificato da installare nel portachiavi dell'app e fare clic su **Import**.

Al completamento della convalida, il certificato viene importato.

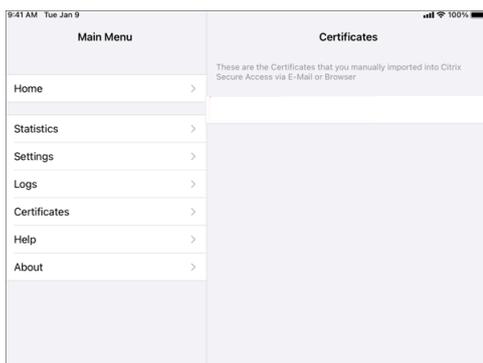


3. Utilizzare l'autenticazione basata su certificati con VPN.

- Per utilizzare il certificato per l'autenticazione VPN, è necessario innanzitutto creare una configurazione VPN o un profilo su Citrix Secure Access.
 - Passare alla vista **VPN Connections** e toccare **Add VPN Configuration** (Aggiungi configurazione VPN).
 - Nella vista di configurazione del profilo VPN, è possibile selezionare il certificato importato nella sezione **Certificates**.



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



4. Gestire i certificati.

Per gestire i certificati importati in Citrix Secure Access, passare alla scheda **Certificates** (Certificati) del **menu principale**.

Come utilizzare Citrix Secure Access dal proprio dispositivo iOS

March 16, 2024

Importante:

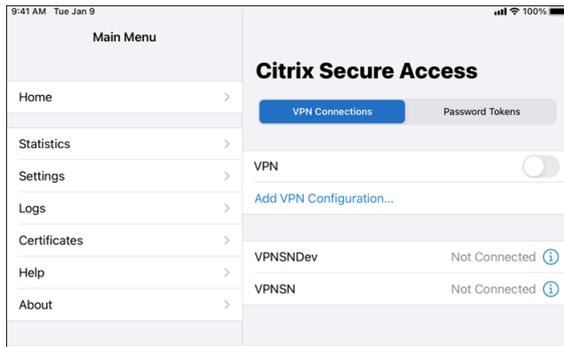
- a partire dalla versione 23.11.1, Citrix SSO per iOS verrà rinominato Citrix Secure Access. Stiamo aggiornando la nostra documentazione e le schermate dell'interfaccia utente per rispecchiare tale modifica del nome.
- Per istruzioni specifiche per l'amministratore su Citrix Secure Access per iOS, vedere [Citrix Secure Access per macOS/iOS](#).

Installare l'app Citrix Secure Access dall'App Store. Dopo aver installato l'app, al primo uso è necessario creare una connessione a NetScaler Gateway aggiungendo il server. Per gli usi successivi, è possibile connettersi a una connessione esistente o aggiungere una nuova connessione e modificare anche le connessioni esistenti. È inoltre possibile visualizzare i registri e intraprendere le azioni appropriate di conseguenza.

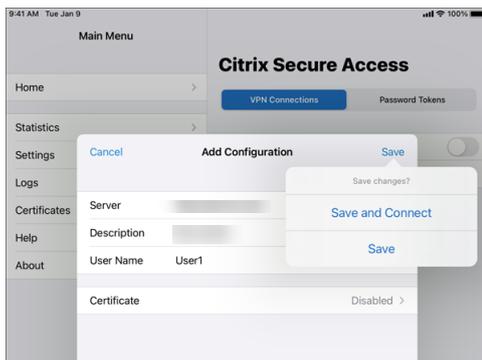
Per i clienti MDM, l'amministratore potrebbe avere connessioni VPN preconfigurate che vengono visualizzate automaticamente al momento della registrazione del dispositivo. È possibile avviare le connessioni direttamente selezionando la connessione e attivando lo switch VPN. Queste connessioni VPN non sono modificabili dagli utenti.

Aggiungere una connessione

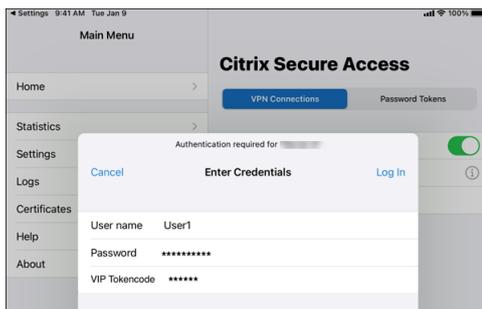
Dopo aver installato Citrix Secure Access e aperto l'app, viene visualizzata la seguente schermata.



1. Toccare **Add VPN Configuration** (Aggiungi configurazione VPN) per aggiungere una nuova connessione.
2. Immettere i dettagli del server.
È inoltre possibile aggiungere un nome utente se si desidera.
3. Toccare **Save**, quindi toccare **Save and Connect** o **Save**, a seconda delle esigenze.



4. Fornire le credenziali di autenticazione per il server e toccare **Log In** (Accedi).



Nota: per disconnettersi da Citrix Secure Access, disattivare la VPN.

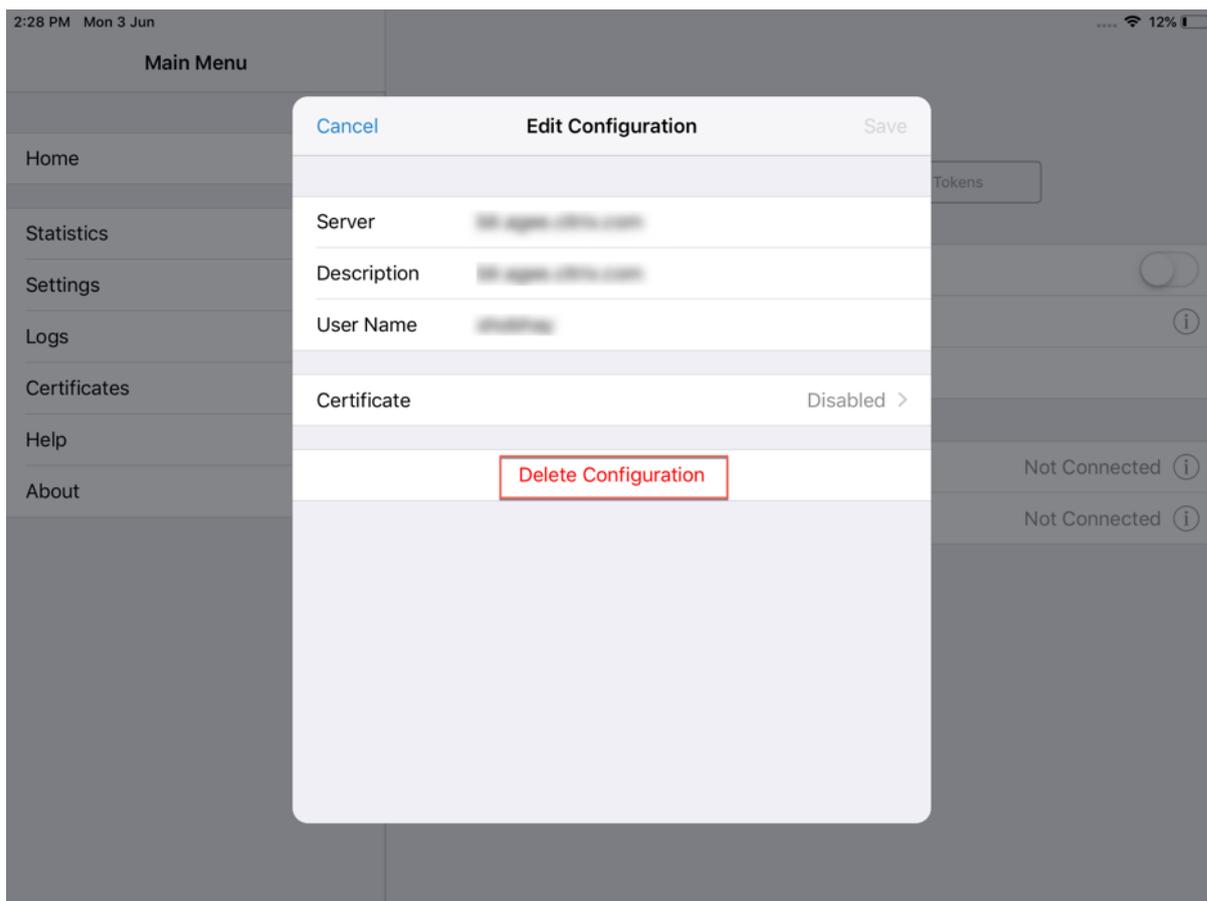
Riconnettersi a NetScaler Gateway dopo un errore di connessione alla VPN

A partire dalla versione 23.09.1, l'app Citrix SSO per iOS richiede di riautenticarsi con NetScaler Gateway quando si perde una connessione VPN. Nell'interfaccia utente si riceverà una notifica che indica

che la connessione a NetScaler Gateway è stata interrotta e che è necessario eseguire nuovamente l'autenticazione per riprendere la connessione.

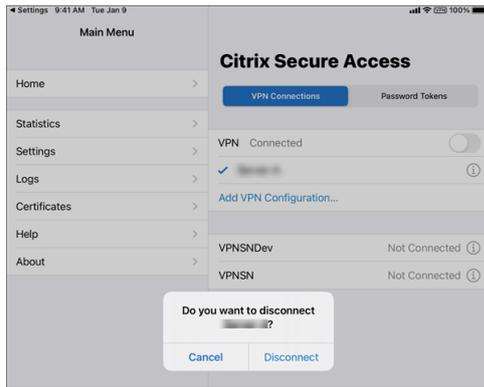
Eliminare una connessione esistente

Toccare l'icona accanto alla connessione, quindi toccare Delete Configuration (Elimina configurazione).



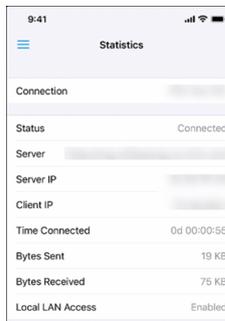
Disconnettere una connessione

Impostare lo switch VPN su OFF, quindi toccare Disconnect.



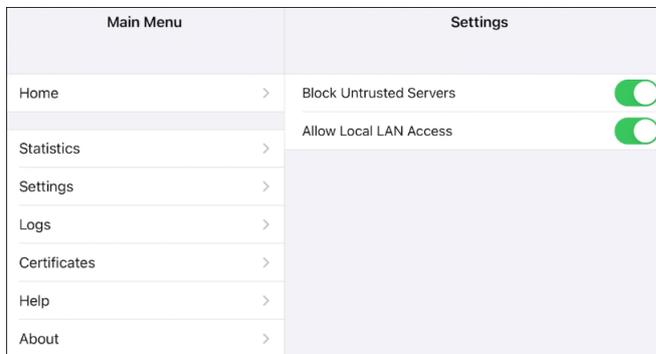
Visualizzare le statistiche

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



Bloccare i server non attendibili

Citrix SSO non si connette a server non attendibili (server che utilizzano certificati autofirmati o non dotati di certificato radice attendibile per il gateway) per impostazione predefinita. Per consentire questi tipi di connessione, mettere lo switch Block Untrusted Servers (Blocca server non attendibili) in posizione OFF.



Accesso alla 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 alla LAN locale nell'interfaccia utente di Citrix Secure Access:

1. Vai al menu principale e fai clic su **Settings** (Impostazioni).
2. Abilita **Allow Local LAN Access** (Consenti accesso LAN locale).

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

Inviare i registri

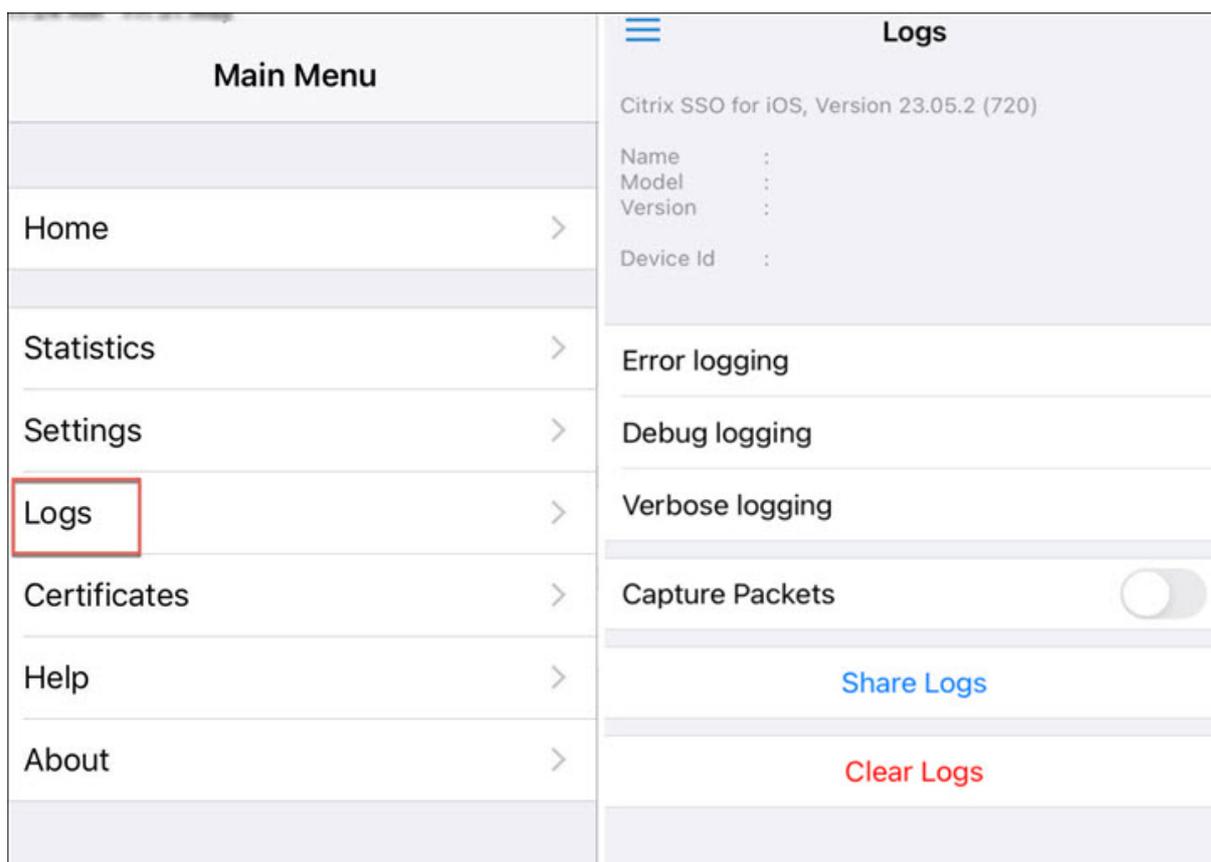
L'acquisizione dei registri di debug è una parte fondamentale della risoluzione dei problemi o della segnalazione di problemi al supporto Citrix.

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

1. Impostare lo switch **Debug Logging** su ON.
2. Condividere i log utilizzando opzioni come e-mail, chat, salvataggio su file e così via.

Nota:

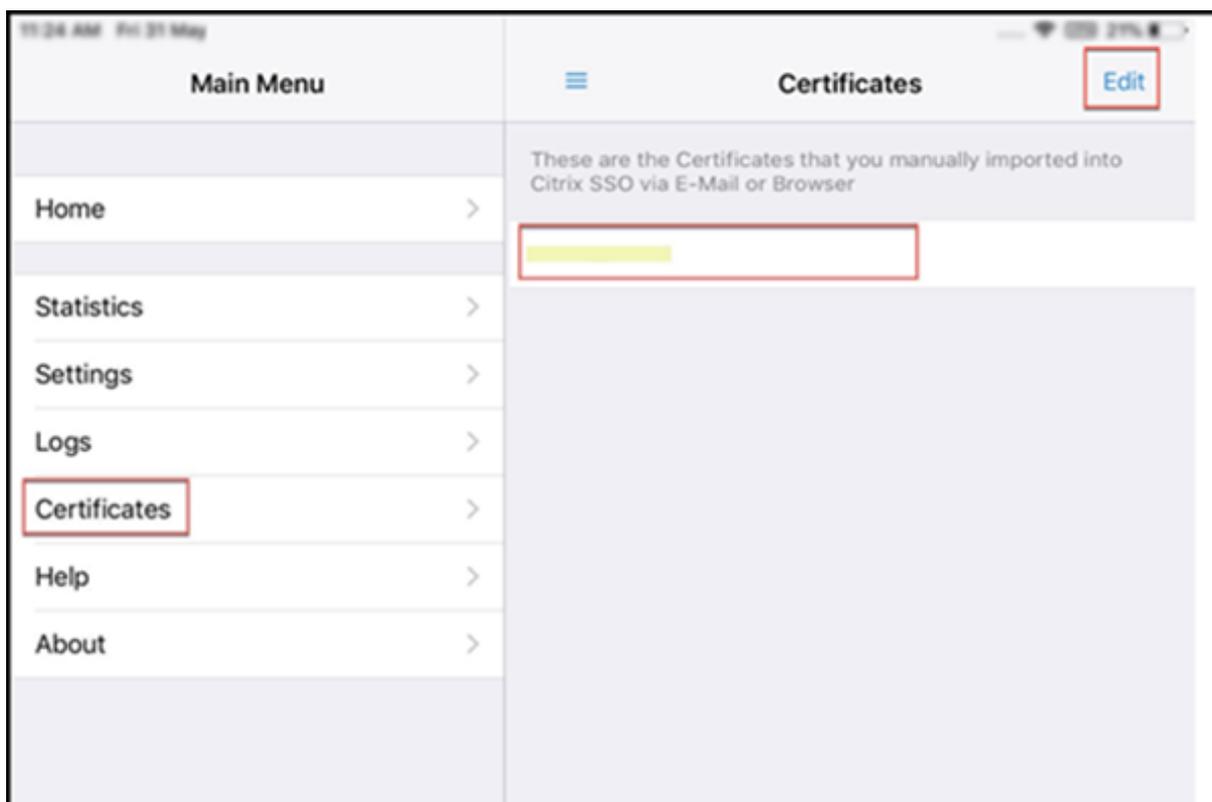
- Per generare un nuovo insieme di registri, eliminare prima i registri più vecchi utilizzando **Clear Logs**.
- A partire dalla versione 23.07.1, l'opzione **Email Logs** viene sostituita dall'opzione **Share Logs**. Share Logs offre varie opzioni per condividere i file di registro compressi.



Visualizzare i certificati client

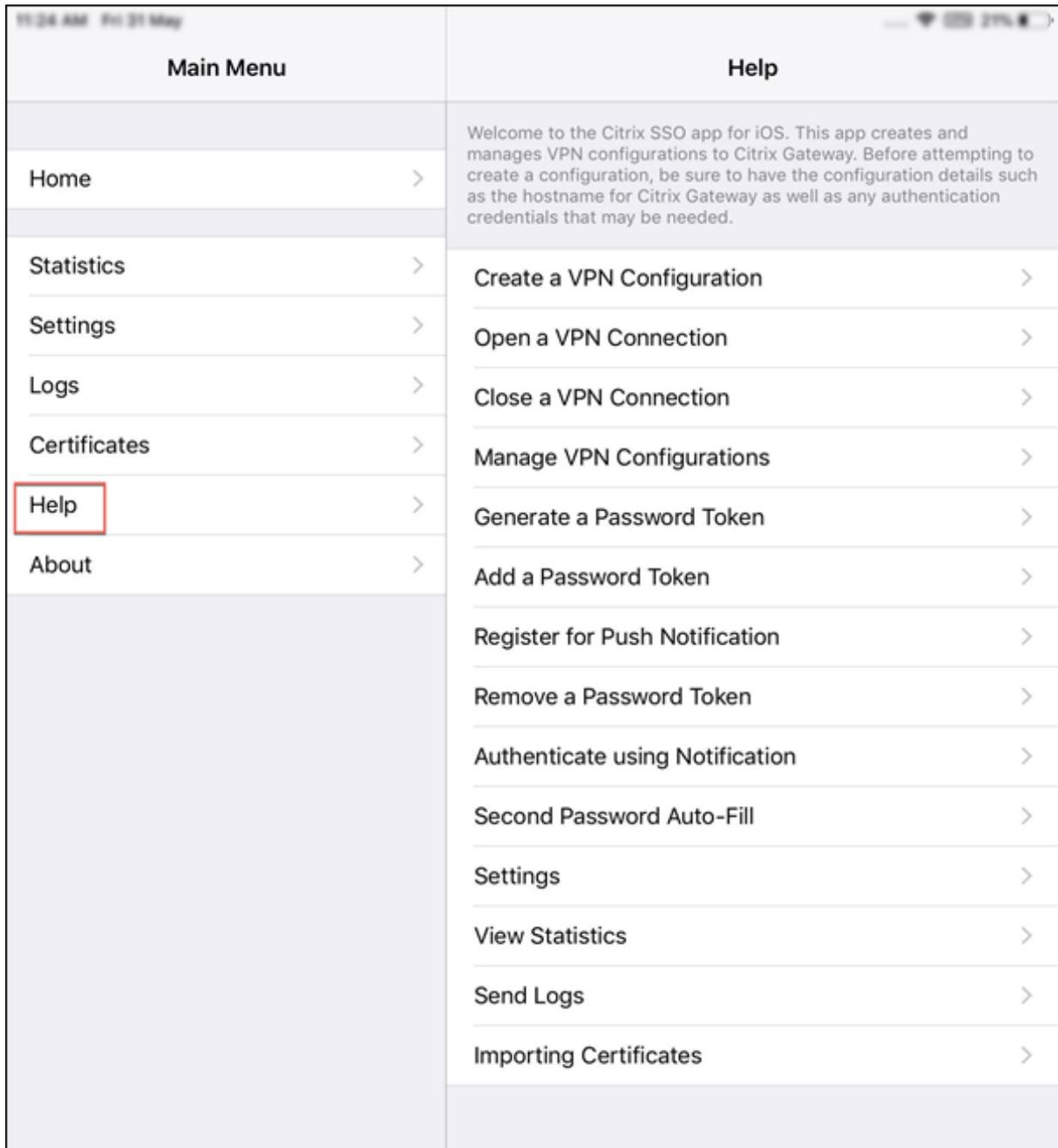
È possibile visualizzare i certificati client importati in Citrix Secure Access. I certificati importati vengono visualizzati nella sezione **Certificates** (Certificati). È possibile eliminare i certificati in uno dei modi seguenti.

- Nella cella del certificato, eseguire un movimento di scivolamento da destra a sinistra per visualizzare il pulsante **Delete**. Quindi toccare **Delete**.
- Toccare **Edit** per visualizzare il pulsante **Delete**, quindi toccare **Delete**.



Argomenti della Guida

Per informazioni sui vari elementi, vedere la **Guida in linea**.





© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.