Citrix Secure Access

Contents

Citrix Secure Access client for Android devices

December 5, 2024

Citrix Secure Access client for Android provides the best-in-class application access and data protection solution offered by NetScaler Gateway. You can now securely access business critical applications, virtual desktops, and corporate data from anywhere at any time.

> **Notes:**
>
> - Starting from release 23.12.1, Citrix SSO for Android is renamed to Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.
> - For administrator-specific instructions on Citrix Secure Access for Android, see Citrix Secure Access for Android devices.

How to use Citrix Secure Access from your Android device

December 5, 2024

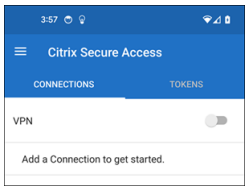
Install Citrix Secure Access from your Play Store. First-time users must create a connection to NetScaler Gateway by adding the server in non-MDM case. For subsequent uses, you can connect to an existing connection or add a connection, and edit existing connections as well, if allowed by your administrator in an MDM deployment. You can also view the logs and take appropriate actions accordingly.

> **Notes:**
>
> - Connections deployed via MDM cannot be edited.
> - You might be prompted to grant the Query all packages consent to the Citrix Secure Access app. Once the consent is granted, the Citrix Secure Access app:
>   - Receives the package install notification from the operating system.
>   - Restarts the Always On VPN.
>
>   When you connect to your VPN profile for the first time, you are prompted to provide consent (required by Google policies) to collect information of the installed package. If the you grant the consent, the VPN connection is initiated. If you deny the consent, the VPN connection is aborted. The consent screen does not reappear once the consent has been granted.

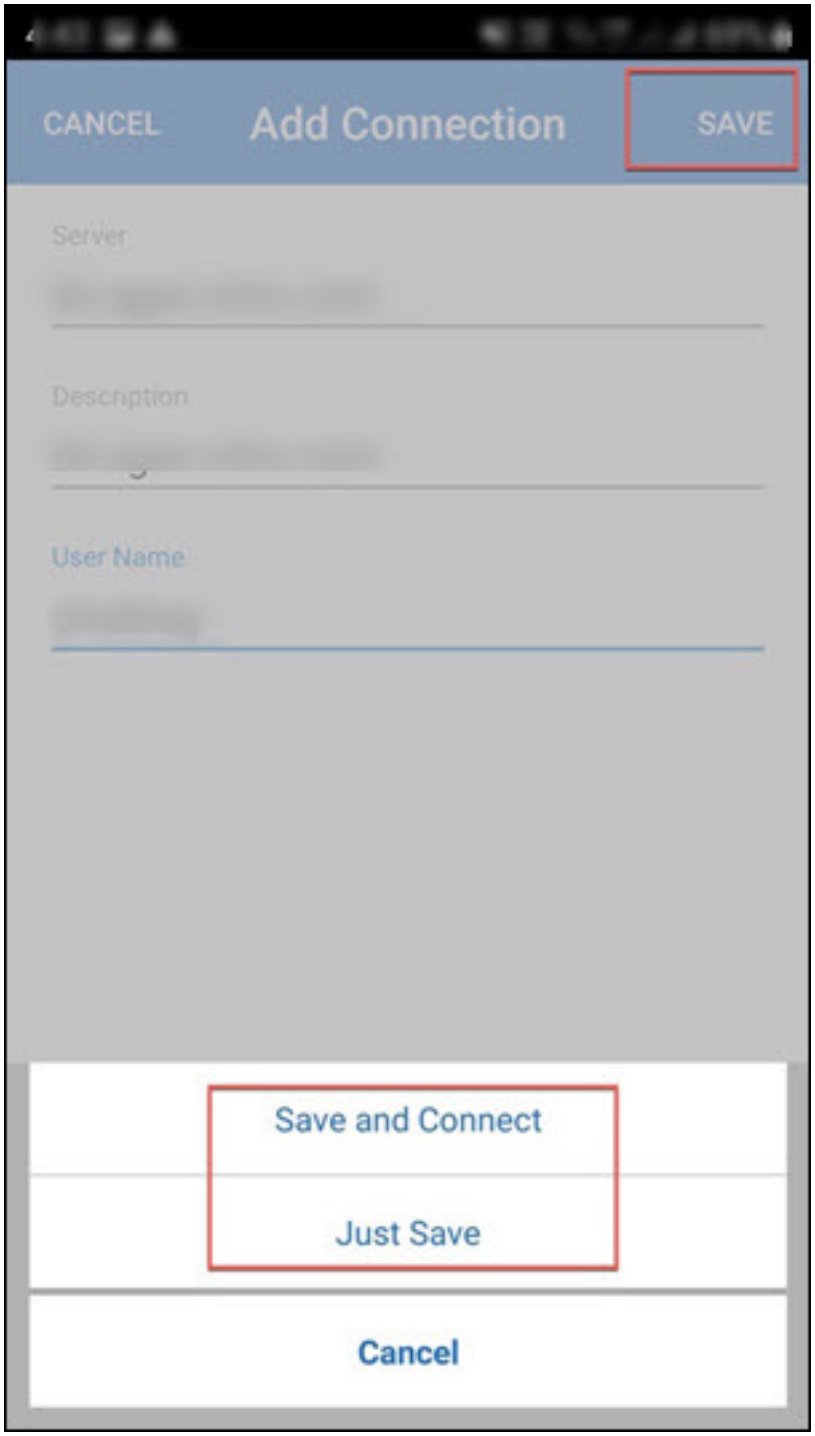
Add a connection

Note: This step is required only in a non-MDM case.

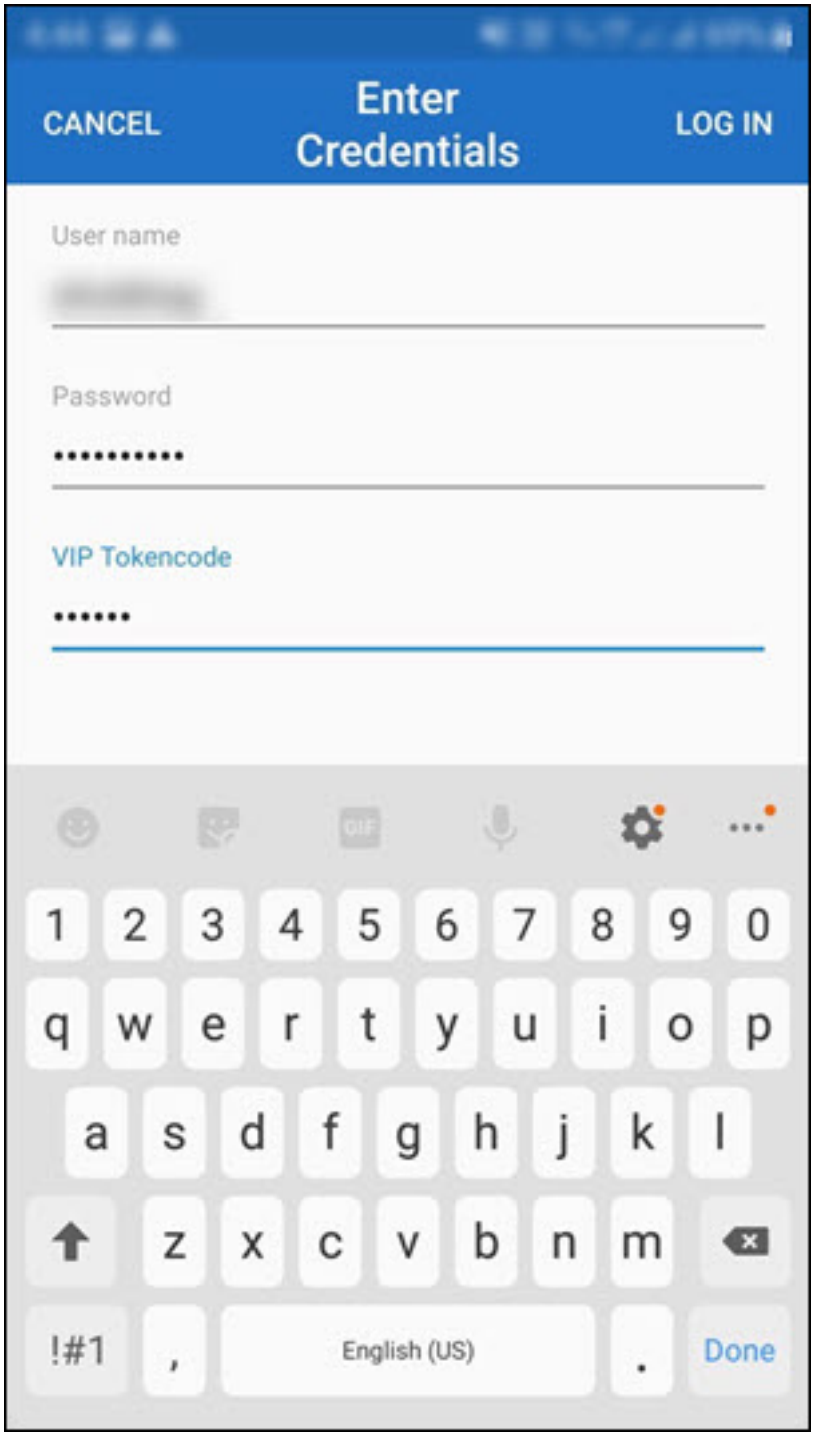
After you install Citrix Secure Access and open the app on your Android device, the following screen appears.



1. Click **+** to add a connection.
2. Enter the base URL (for example, https://gateway.mycompany.com) and the name for the VPN connection. Optionally, you can enter the user name.
3. Click **Save** and then click **Save and Connect** or **Just Save** as appropriate.

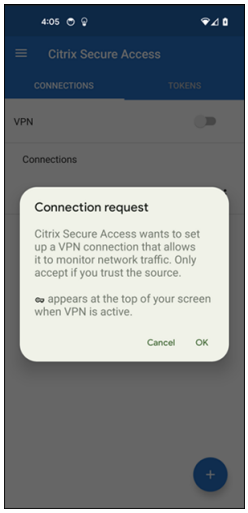


4. Provide authentication credentials for your server and tap **LOG IN** or **Done** on the keypad.

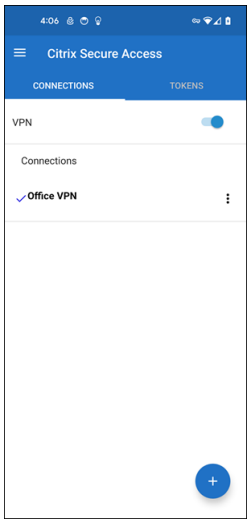


The connection request message appears. Click **OK**.

Note: This message appears only the first time that any VPN connection is established by Citrix Secure Access. If user allows the connection first time, this message is not shown again until the user uninstalls and reinstalls the app.



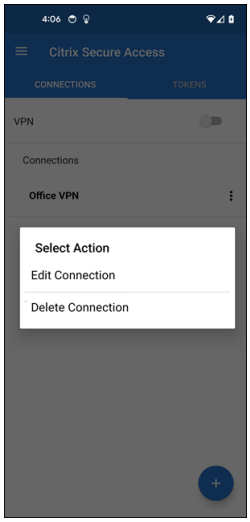
Note: To log out from Citrix Secure Access, turn the **VPN switch** OFF.



Modify or delete an existing connection

You can edit or delete a connection after you log out from Citrix Secure Access.

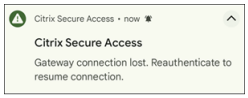
Tap and hold the server name and select **Edit Connection** or **Delete Connection**.



Reconnect to NetScaler Gateway after a VPN connection failure - Preview

The Citrix Secure Access client for Android prompts you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the UI and the notification panel of your Android device indicating that the connection to NetScaler Gateway is lost and that you must reauthenticate to resume the connection.

> **Note:**
>
> This feature is in preview.

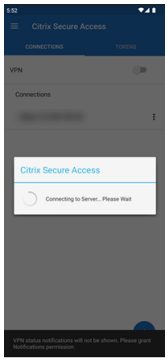


Receive or block notifications on Android 13+ devices

Starting from the Citrix Secure Access client for Android release 23.12.1, when you install or reinstall Citrix Secure Access client on Android 13+ devices, you are prompted to provide permissions to receive notifications from Citrix Secure Access client. If you deny the permission, you do not receive any VPN status or push notifications from Citrix Secure Access client on your Android device.

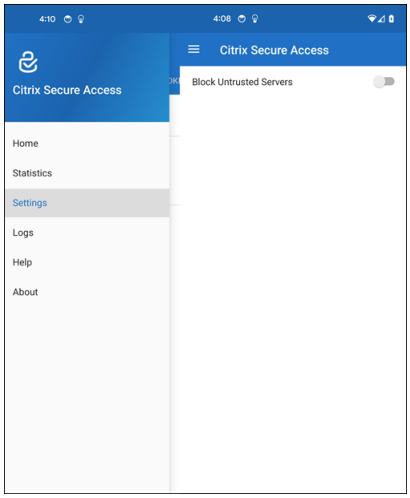
You can navigate to **Settings > Notifications** on your Android device to change the notification permissions.

In the following example, the VPN status notifications have been disabled.



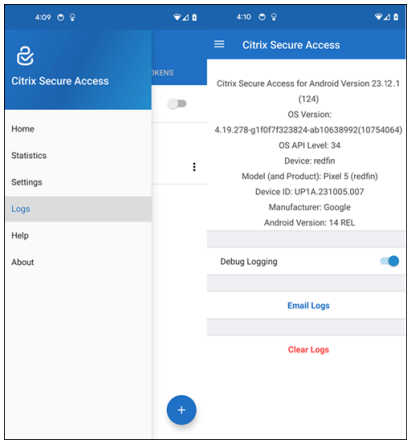
Block untrusted servers

Citrix Secure Access does not connect to untrusted servers, by default. Untrusted servers refer to servers using self-signed certificates or not having trusted root certificate for the gateway. To allow these types of connections, you can turn **Block Untrusted Servers** switch **OFF**.



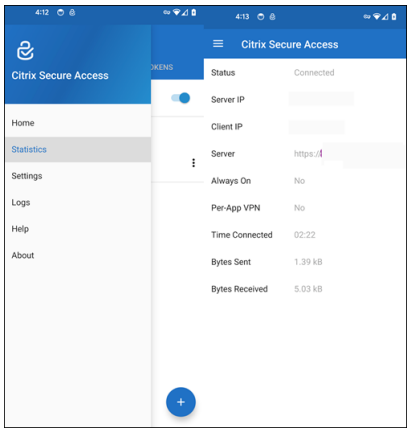
Enable debug logs

Capturing debug logs is a critical part of troubleshooting or reporting issues to Citrix Support.
Tap the **Debug Logging** switch **ON** to turn on debug logging for Citrix Secure Access. You can email the logs when troubleshooting connection issues using the **Email Logs** link.



View statistics

You can view the connection statistics when VPN is connected.



Password tokens

You can add a 6-digit password token as a second factor authentication. This code uses the time-based one time password protocol to generate the OTP code.

You can add a password token manually or register a password token using the QR code scan method. Second factor authentication using push notifications is not be enabled if you choose to enter the token manually.

Register a password token

1. Log in to your organization's manage one-time PIN page in your web browser on a desktop or a laptop.
2. Click **Add Device**.

3. Enter a name for your device, then click **Go**.

   A QR code is generated.

Add a password token by scanning the QR code on the browser

1. Navigate to **Tokens** tab on the **Home** view.
2. Tap **+** and tap **Scan QR Code**.
3. Focus the camera on the QR code on your browser.

Citrix Secure Access auto-populates the device name and secret key.

Alternatively, you can manually enter the secret key that appears above the QR code.

Citrix Secure Access validates the QR code and then registers with gateway for push notifications. If there are no errors in the registration process, the token is successfully added to the tokens tab.

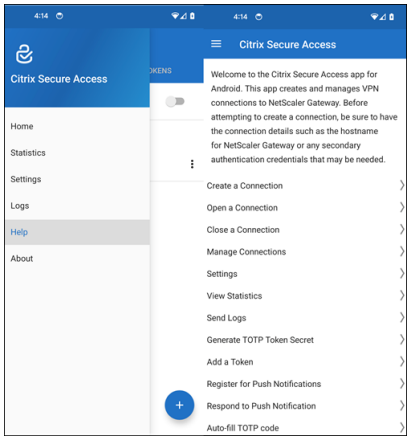
> **Note:**
>
> - You must allow camera permissions for Citrix Secure Access to capture the QR code.
> - You must enable the device PIN/password on your device.

Add a password token manually

1. Navigate to **Tokens** tab on the **Home** view.
2. Tap + and tap **Enter Manually**.
3. Enter the device name and the secret key as it appears on the password token generated on the browser.

Help topics

For more information about how to use Citrix Secure Access, see **Help**.



Connect to your corporate network using Citrix Secure Access configured in an Intune environment

December 5, 2024

> **Note:**
>
> For administrator-specific instructions on Citrix Secure Access for Android, see Citrix Secure Access for Android devices.

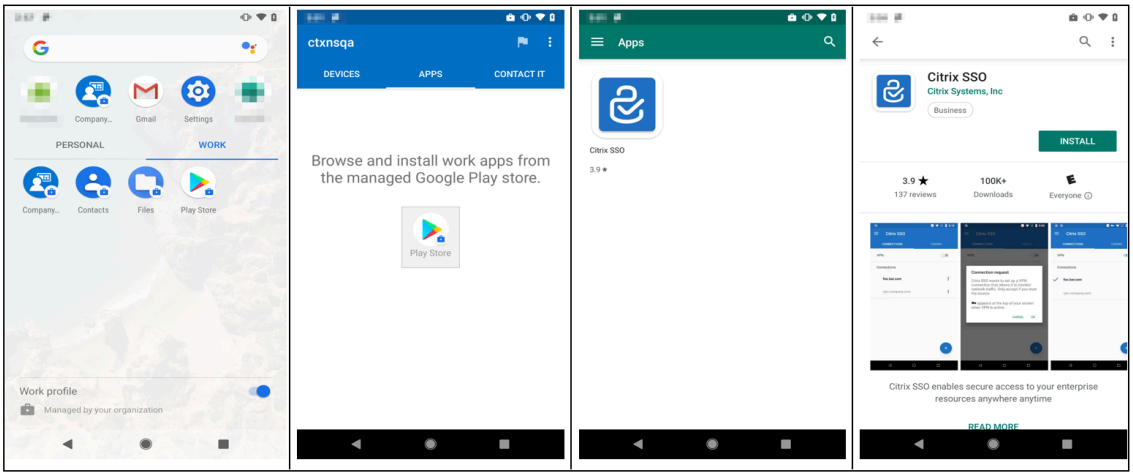
This topic captures details about connecting to your corporate network using Citrix Secure Access client configured in the Microsoft Intune Android Enterprise environment.

Assumptions:

- You have enrolled the device in Intune using Intune Company Portal app.
- Work profile for the user is set up on the device.

1. Open **Intune Company Portal** app on the device from the work profile.
2. Click the three dots menu to open settings for the app and scroll to the bottom of the screen. Tap **SYNC** to sync with the Intune server and then navigate to the main app screen.
3. Tap on the **APPS** tab and tap on the **Managed Google Play Store** link.

   The list of approved apps for the user appears.



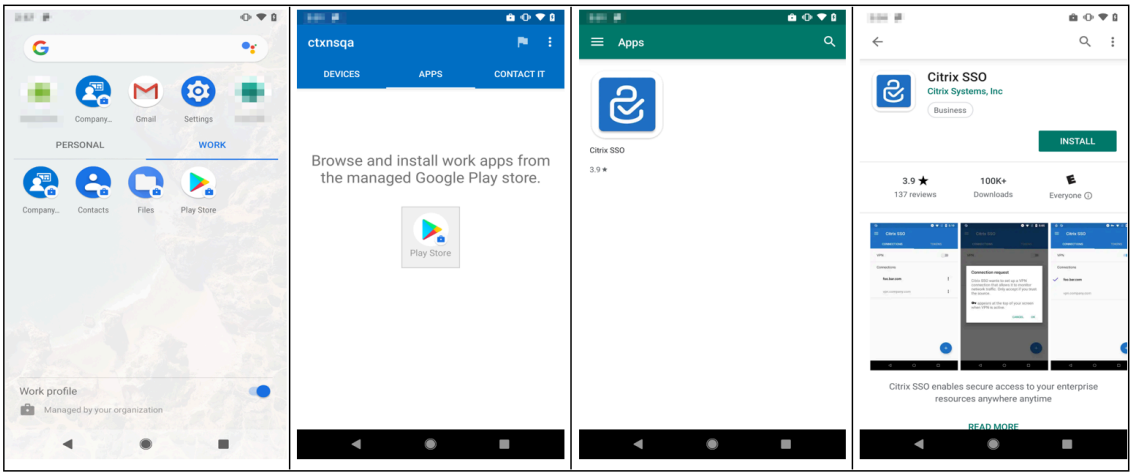
4. Tap **Citrix Secure Access**.

   The Citrix Secure Access client appears in the Managed Google Play store.

5. Tap **INSTALL**.

6. Navigate back to the work profile apps list. The Citrix Secure Access is added to the installed app list.

7. Tap the Citrix Secure Access icon in the **WORK** profile app list to open it.



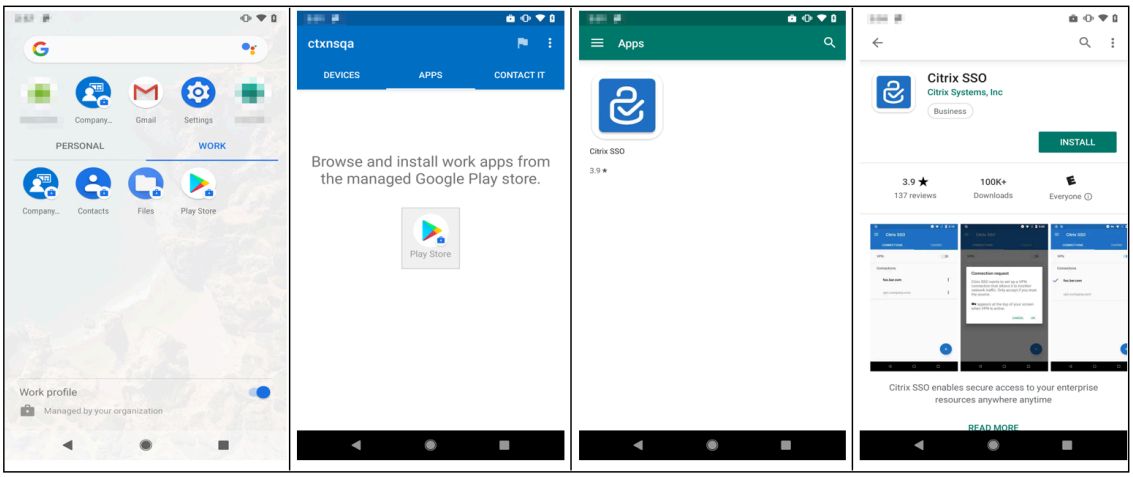
   Citrix Secure Access opens. You are prompted to allow or disallow permission to communicate securely with your company's internal network.

8. Tap **ALLOW** to grant the permission. Citrix Secure Access closes if you choose **DON'T ALLOW** and you cannot use the Citrix Secure Access client.

   > **Note:**
   >
   > You might be prompted to allow or deny **permission to manage and make phone calls** (if not already granted via Intune). Tap **Allow** to grant permission. You may deny this permis-

> sion but if Intune NAC check is required for device authentication on NetScaler Gateway, you cannot connect to your company's internal network until you grant this permission.

9. The **My Corporate VPN** (or the name you chose in the Citrix Secure Access configuration in Intune) is listed in the Managed Connections section of the **CONNECTIONS** tab. Tap on this connection, you are prompted for the credentials to authenticate with NetScaler Gateway.
10. Provide credentials for authentication with NetScaler Gateway and tap **LOG IN**.



You may be prompted to select a certificate if client certificate authentication is configured on NetScaler Gateway. You can provide access to the certificate.

11. You are prompted by Android system to allow **Connection request** for VPN tunnel setup. Tap **OK** to grant Citrix Secure Access permission to establish secure connection with your internal company network.

    Note: This prompt is only displayed when you establish a secure connection to NetScaler Gateway for the first time. It is not displayed for subsequent connection attempts until Citrix Secure Access is uninstalled and then installed again on the device.

You are connected to your internal company network. A key icon appears in the device status bar notifying you that VPN connection is active. Citrix Secure Access client's VPN service notification icon also appears on the status bar. The connect switch changes its state to connected and a check mark icon appears next to the VPN profile name.

Citrix Secure Access client for iOS devices

December 5, 2024

The Citrix Secure Access client for iOS provides the best in-class application access and data protection solution offered by NetScaler Gateway. You can now securely access business critical applications, virtual desktops, and corporate data from anywhere at any time.

Citrix Secure Access app provides complete Mobile Device Management (MDM) support on iOS. With an MDM server, an admin can now remotely configure and manage device level VPN profiles and per-app VPN profiles.

> **Important:**
>
> - Starting from release 23.11.1, Citrix SSO for iOS is renamed to Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.
> - For administrator-specific instructions on Citrix Secure Access for iOS, see Citrix SSO for iOS and Citrix Secure Access for macOS.

Import and install certificates in Citrix Secure Access app

December 5, 2024

Citrix Secure Access on iOS supports client certificate authentication with NetScaler Gateway. Certificates can be delivered to the Citrix Secure Access in the following ways:

- **MDM server** - Preferred approach for MDM customers. Certificates are configured directly on the MDM-managed VPN profile. Both VPN profiles and certificates are then pushed to enrolled devices when the device enrolls into the MDM server. Follow MDM vendor-specific documents for this approach.
- **Email** - Only approach for non-MDM customers. Administrators send an email with the User Certificate identity (Certificate and private key) attached as a PKCS#12 file to users. Users must have their email accounts configured on their iOS device to receive the email with an attachment. The file can then be imported to the Citrix Secure Access on the iOS.

  > **Note:**
  >
  > File name extensions `.pfx` and `.p12` are claimed by the iOS system and cannot be claimed by third-party apps such as Citrix Secure Access. Therefore, administrators must change the Extension/MIME type of the user certificate, from standard `.pfx` or `.p12` to `.citrixsso-pfx` or `.citrixsso-p12` respectively.

1. Open the email with the user certificate identity (certificate and private key) attached as a PKCS#12 file.
   - Tap on the attachment to reveal the system **OpenIn** menu.

- Tap **Copy to Citrix SSO**.

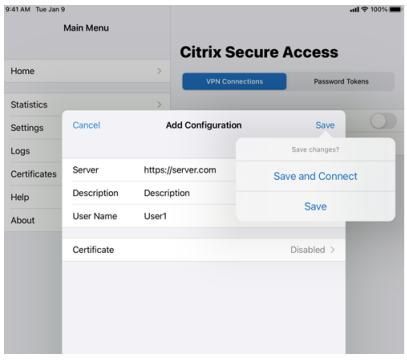
2. Install certificate in Citrix Secure Access.

   The app is now launched and a prompt for the certificate passphrase is displayed. Enter the correct passphrase for the certificate to be installed into the app's keychain and click **Import**.

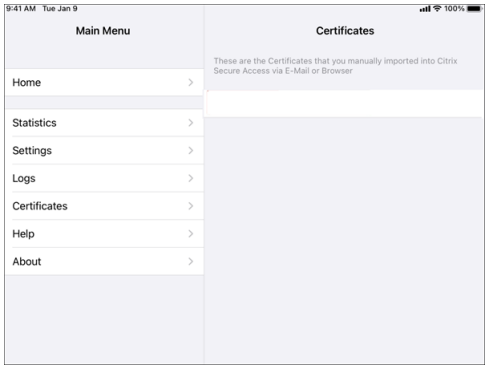
   Upon successful validation, the certificate is imported.

3. Use certificate-based authentication with VPN.

   - To use the certificate for VPN authentication, you must first create a VPN configuration or a profile on Citrix Secure Access.
     - Navigate to the **VPN Connections** view and tap **Add VPN Configuration**.
     - On the configuration view of the VPN profile, you can select the imported certificate in the **Certificates** section.



   - Tap **Save** to import the certificate.



4. Manage certificates.

To manage the certificates imported into Citrix Secure Access navigate to the **Certificates** tab in **Main Menu**.

How to use Citrix Secure Access from your iOS device

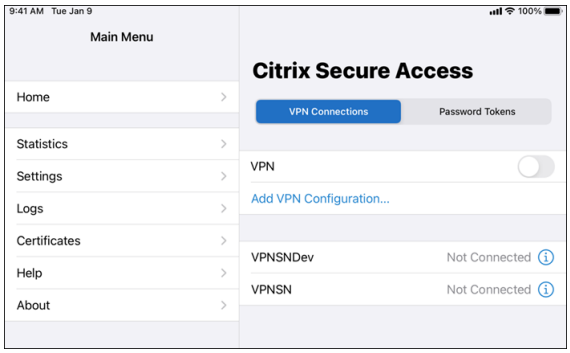
December 5, 2024

Install the Citrix Secure Access app from App Store. After installing the app, first time you must create a connection to NetScaler Gateway by adding the server. For subsequent uses, you can connect to an existing connection or add a new connection, and edit existing connections as well. You can also view the logs and take appropriate actions accordingly.

For MDM customers, your admin might have pre-configured VPN connections that appear automatically when you enroll your device. You can start the connections directly by selecting the connection and turning the VPN switch ON. These VPN connections are non-editable by users.

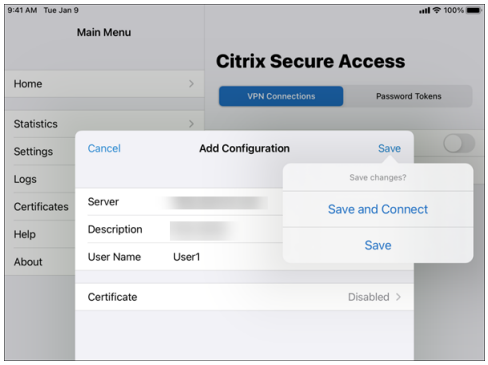
Add a connection

After you install Citrix Secure Access and open the app, the following screen appears.

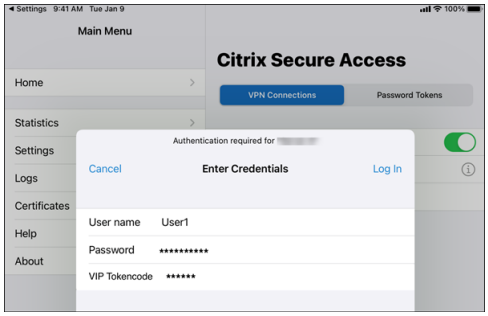


1. Tap **Add VPN Configuration** to add a new connection.
2. Enter the server details.

   You can also optionally add user name.
3. Tap **Save** and then tap **Save and Connect** or **Save**, as appropriate.



4. Provide authentication credentials for your server and tap **Log In**.



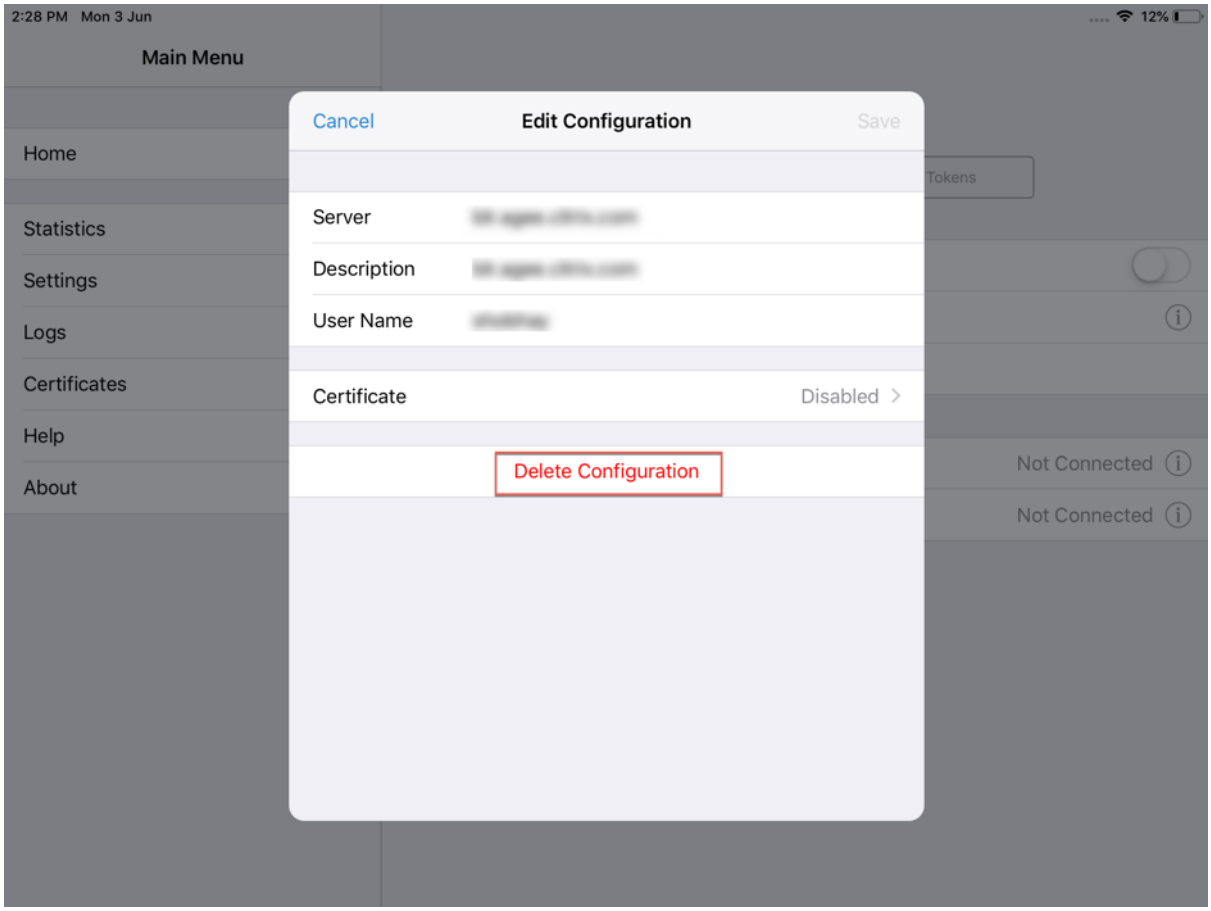
Note: To log out from Citrix Secure Access, turn the VPN OFF.

Reconnect to NetScaler Gateway after a VPN connection failure

The Citrix Secure Access app for iOS prompts you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the UI that the connection to NetScaler Gateway is lost and that you must reauthenticate to resume the connection.

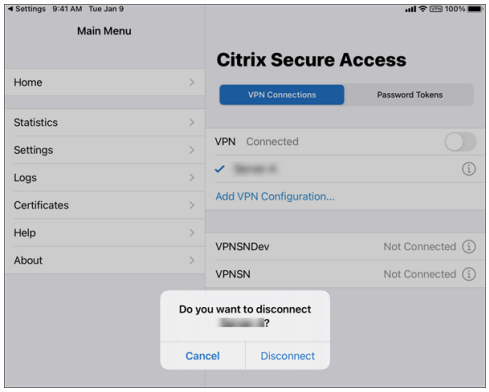
Delete an existing connection

Tap the icon next to the connection and then tap Delete Configuration.



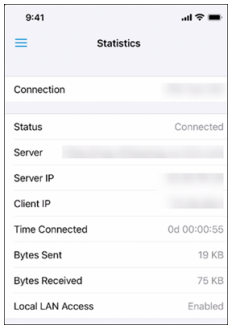
Disconnect a connection

Toggle the VPN switch to OFF and then tap Disconnect.



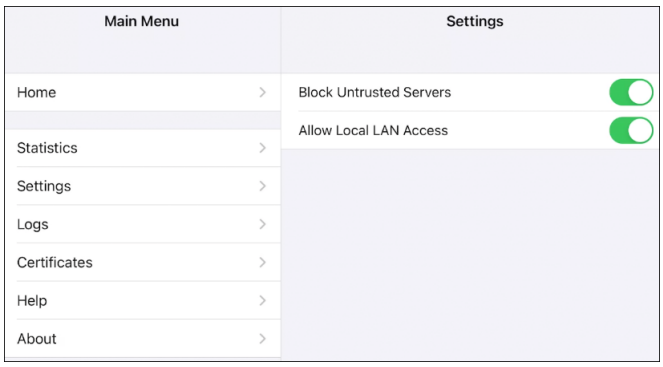
View statistics

You can view the connection statistics when the VPN is connected.



Block untrusted servers

Citrix SSO does not connect to untrusted servers (servers using self-signed certificates or not having trusted root certificate for the gateway), by default. To allow these types of connections, you can turn Block Untrusted Servers switch OFF.



Local LAN access

Citrix SSO for iOS 23.10.1 supports the Local LAN access feature wherein you can determine whether you want to access the local LAN resources on your client device once a VPN connection is established. You can use this feature only if your administrator has configured the local LAN access setting on NetScaler Gateway.

To configure local LAN access on the Citrix Secure Access UI:

1. Navigate to the main menu and click **Settings**.
2. Enable **Allow Local LAN Access**.

You can verify the status of local LAN access on the **Statistics** page.

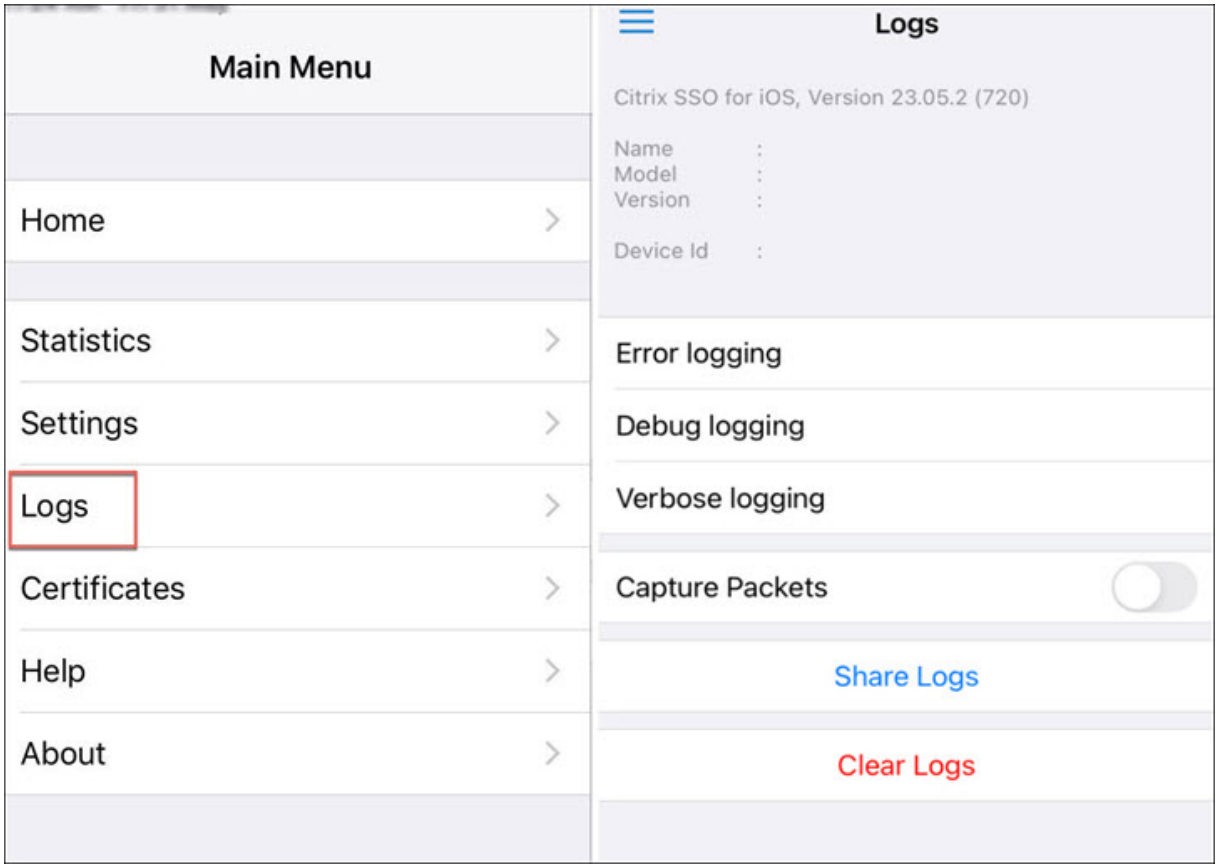
Send logs

Capturing debug logs is a critical part of troubleshooting or reporting issues to Citrix Support.

Following are the steps to capture and share the debug logs:

1. Set the **Debug Logging** switch to ON.
2. Share the logs using options such as email, chat, save to files, and so on.

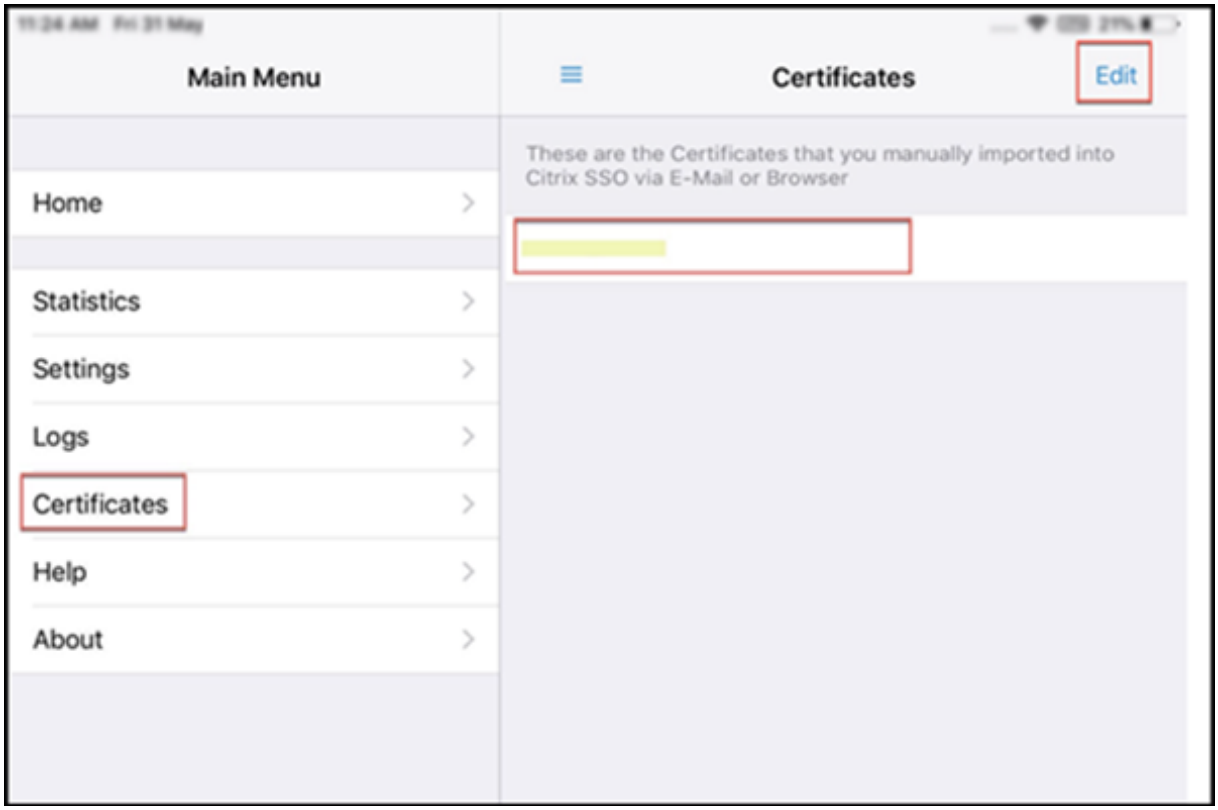
> **Note:**
>
> - To generate a new set of logs, delete older logs first by using **Clear Logs**.
> - Starting from release 23.07.1, the **Email Logs** option is replaced with the **Share Logs** option. Share Logs provides various options to share the compressed log files.



View client certificates

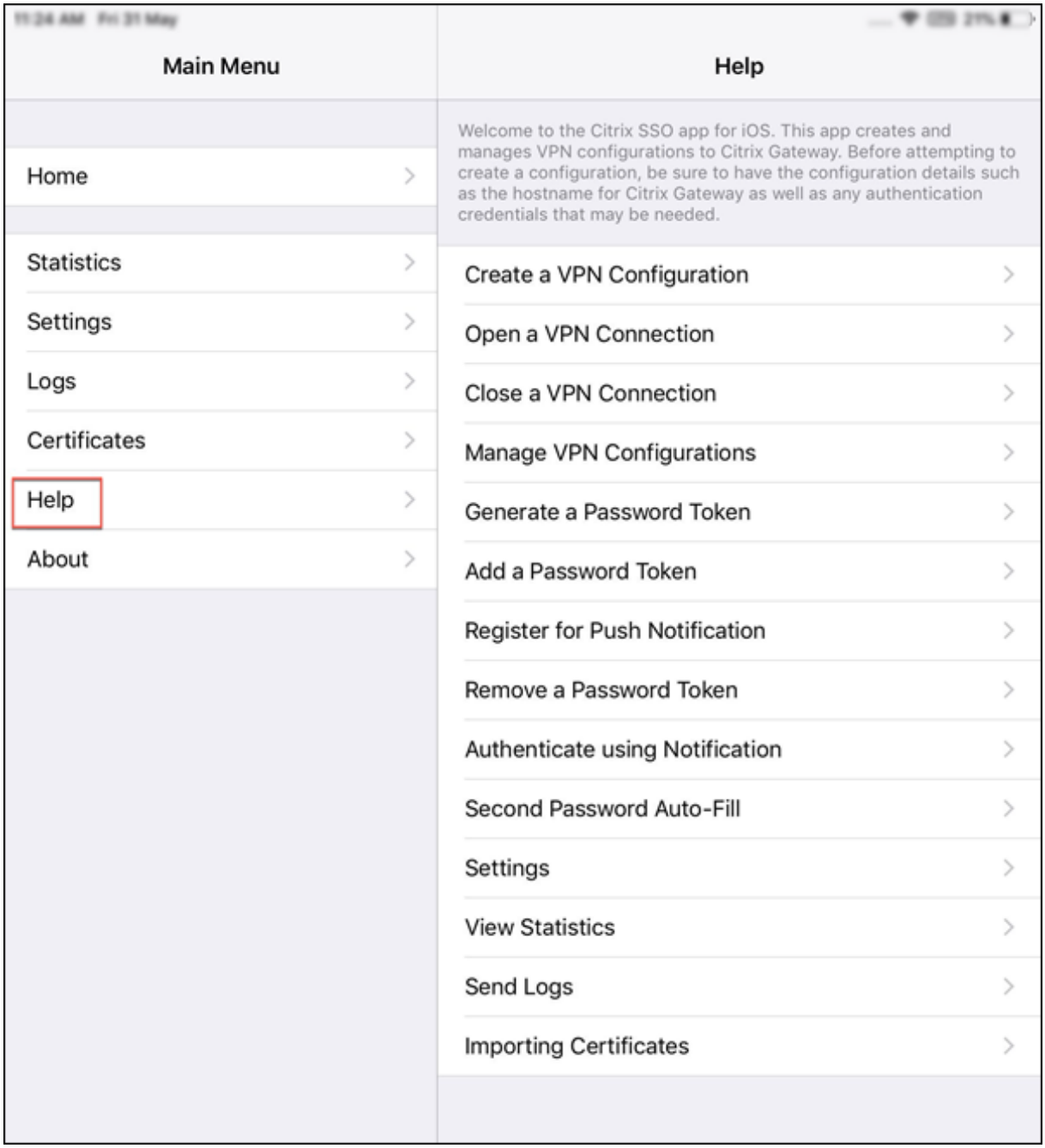
You can view the client certificates that are imported into Citrix Secure Access. The imported certificates appear in the **Certificates** section. You can delete the certificates by one of the following ways.

- On the certificate cell, perform a slide gesture from right to left to reveal the **Delete** button. Then tap **Delete.**
- Tap **Edit** to reveal the **Delete** button and then tap **Delete.**



Help topics

For help on various items, see **Help**.



Citrix Secure Access client for macOS devices

December 5, 2024

Citrix Secure Access app provides the best-in-class application access and data protection solution offered by NetScaler Gateway. You can now securely access business critical applications, virtual desk-

tops, and corporate data from anywhere at any time. Citrix Secure Access app is the next generation VPN client for NetScaler Gateway built using Apple's Network Extension framework. It replaces the legacy Citrix VPN client on the App Store.

Citrix Secure Access app provides complete Mobile Device Management (MDM) support on macOS. With an MDM server, an admin can now remotely configure and manage device level VPN profiles and per-app VPN profiles.

> **Important:**
>
> - Citrix Secure Access app supports Zero-trust network access. In addition to the NetScaler Gateway URL, you can also connect to the Workspace URL.
> - For administrator-specific instructions on Citrix Secure Access for macOS, see Citrix SSO for iOS and Citrix Secure Access for macOS.

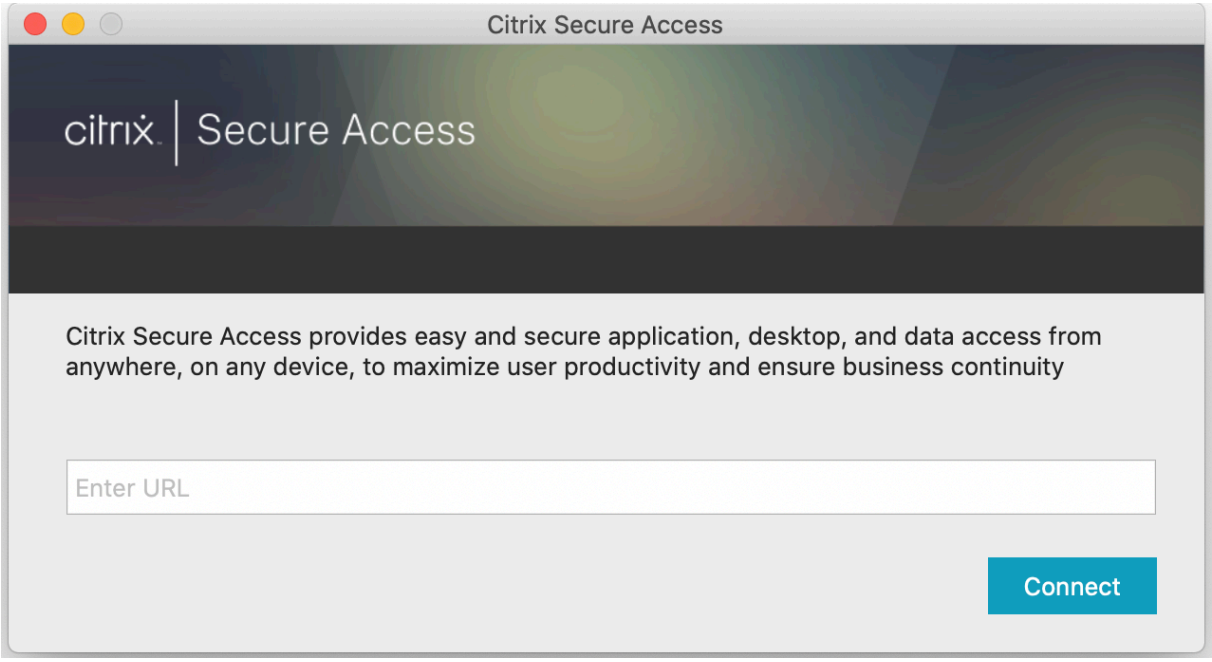
How to use Citrix Secure Access app from your macOS device

December 5, 2024

Install the Citrix Secure Access app from your App Store. First-time users must create a connection to NetScaler Gateway by adding the server. Existing users can connect to an existing connection or add a new connection, and edit existing connections as well. You can also view the logs and take appropriate actions accordingly.

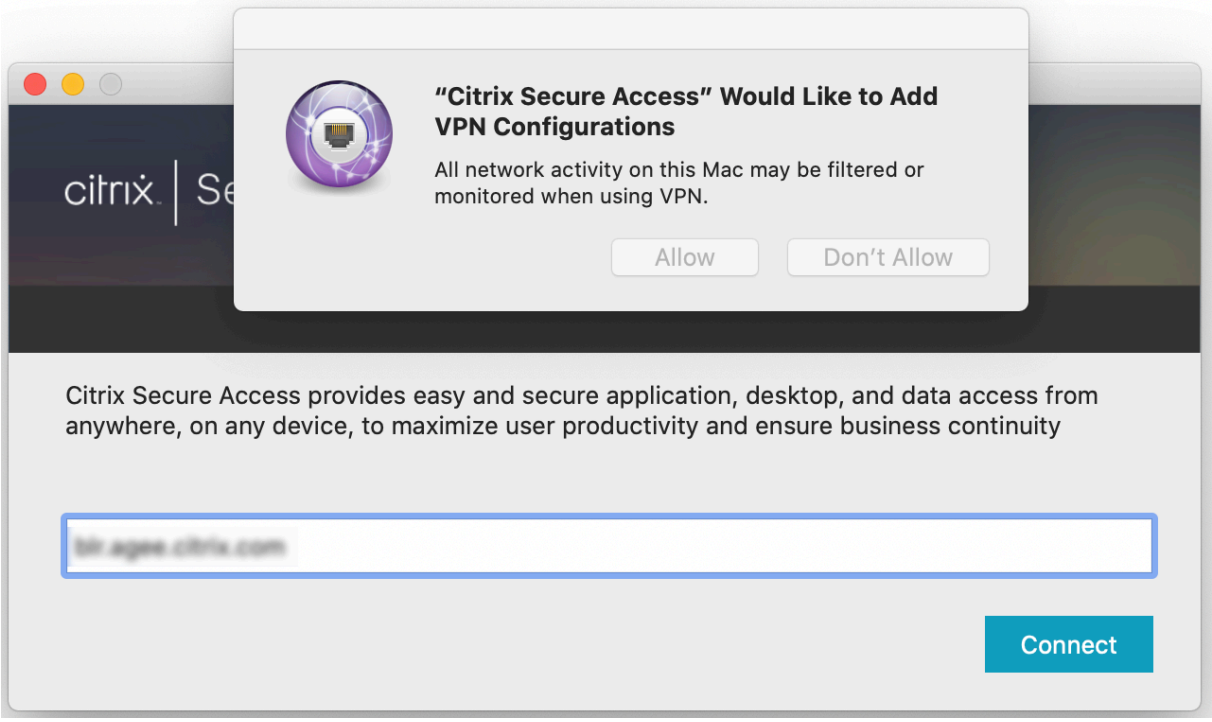
First time user experience

After you install the Citrix Secure Access app and open the app for the first time, the following screen appears.

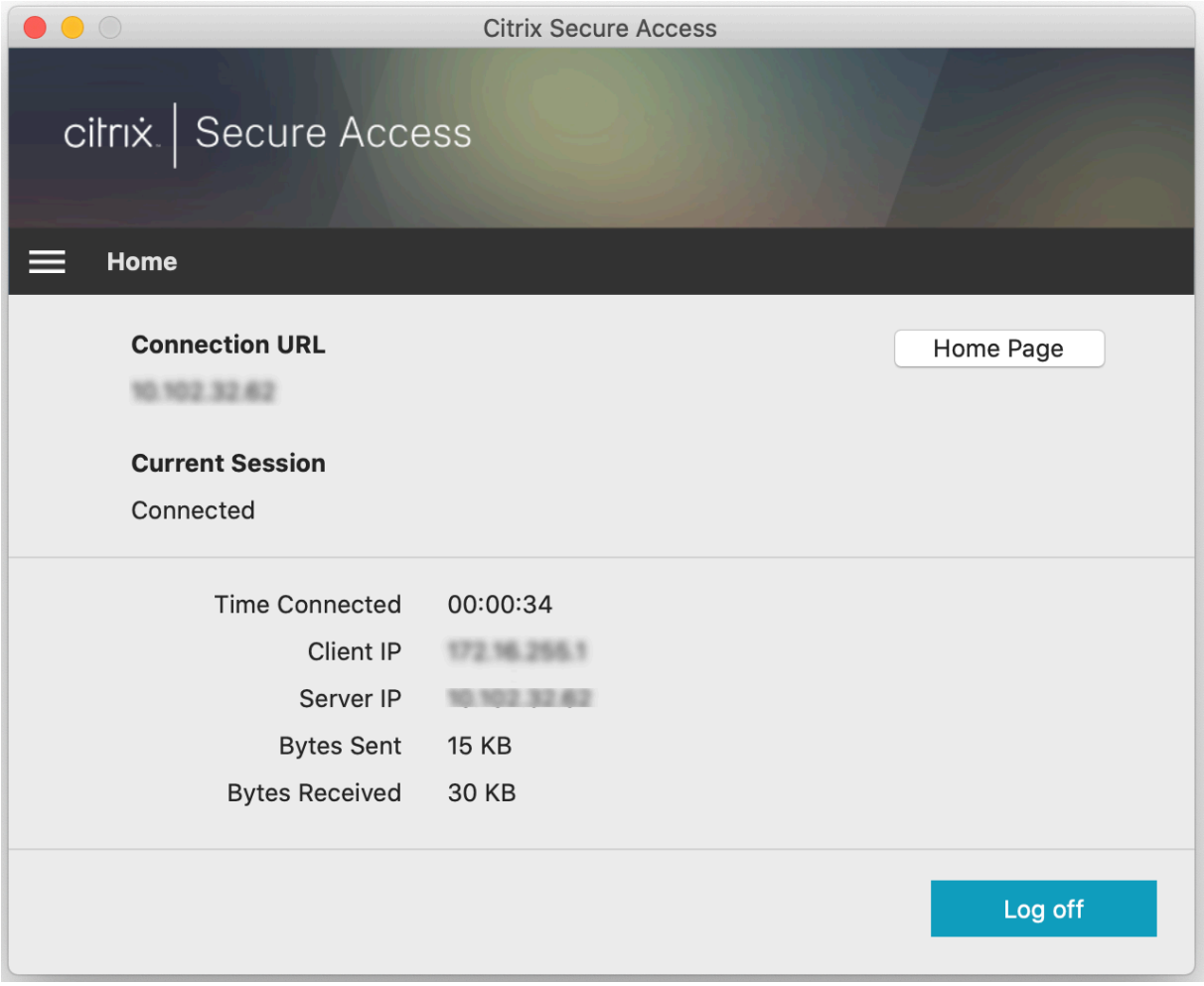


Enter the NetScaler Gateway base URL or the Citrix Workspace URL and click **Connect**.

A popup message appears. Click **Allow** to enable adding a connection. This message appears only the first time. For subsequent new connections, this message does not appear.



Note: To log out from Citrix Secure Access, it is recommended that you first click **Log Off** in the app and then quit the app from the dock. Do not use the **Quit** option from the dock.

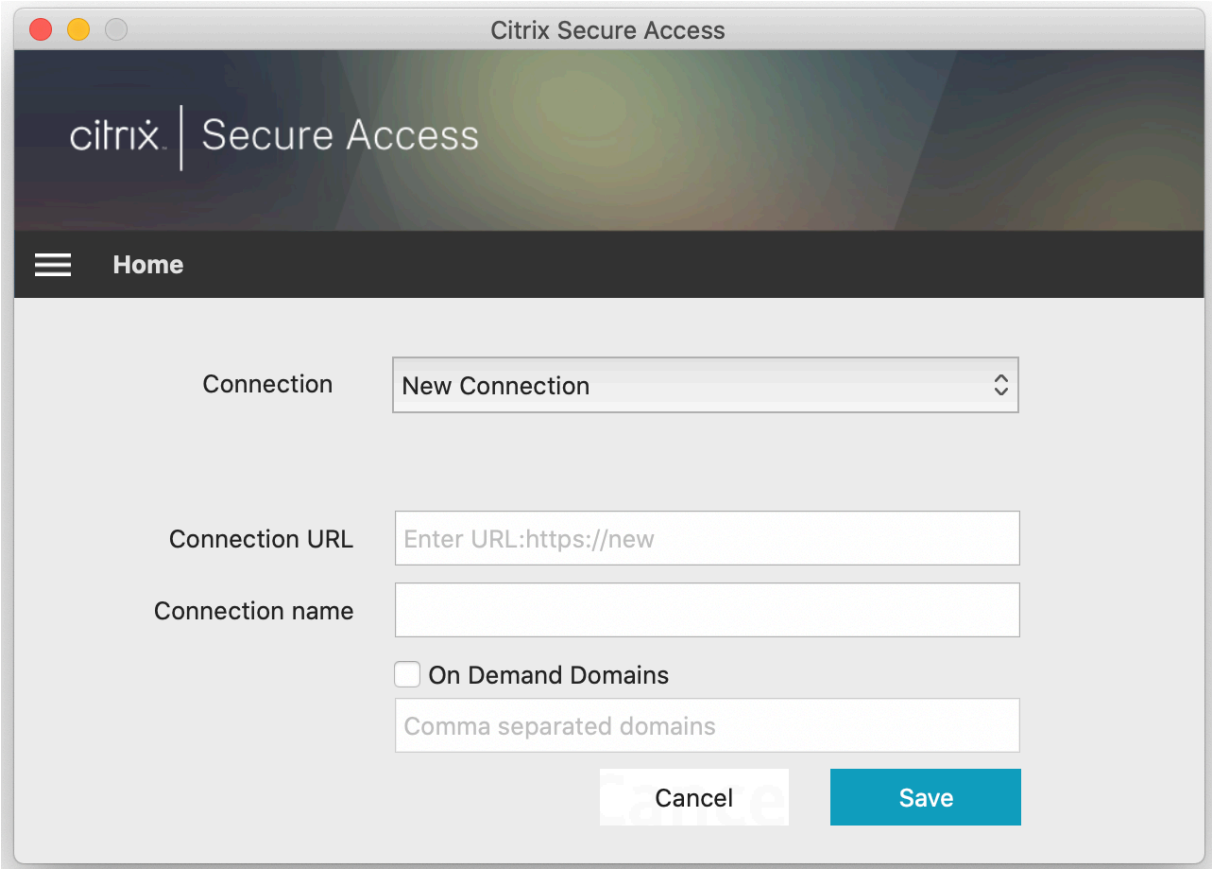


Connect to NetScaler Gateway

After adding the first connection, for subsequent connections, you can either connect to an existing NetScaler Gateway or the Citrix Workspace or add a connection.

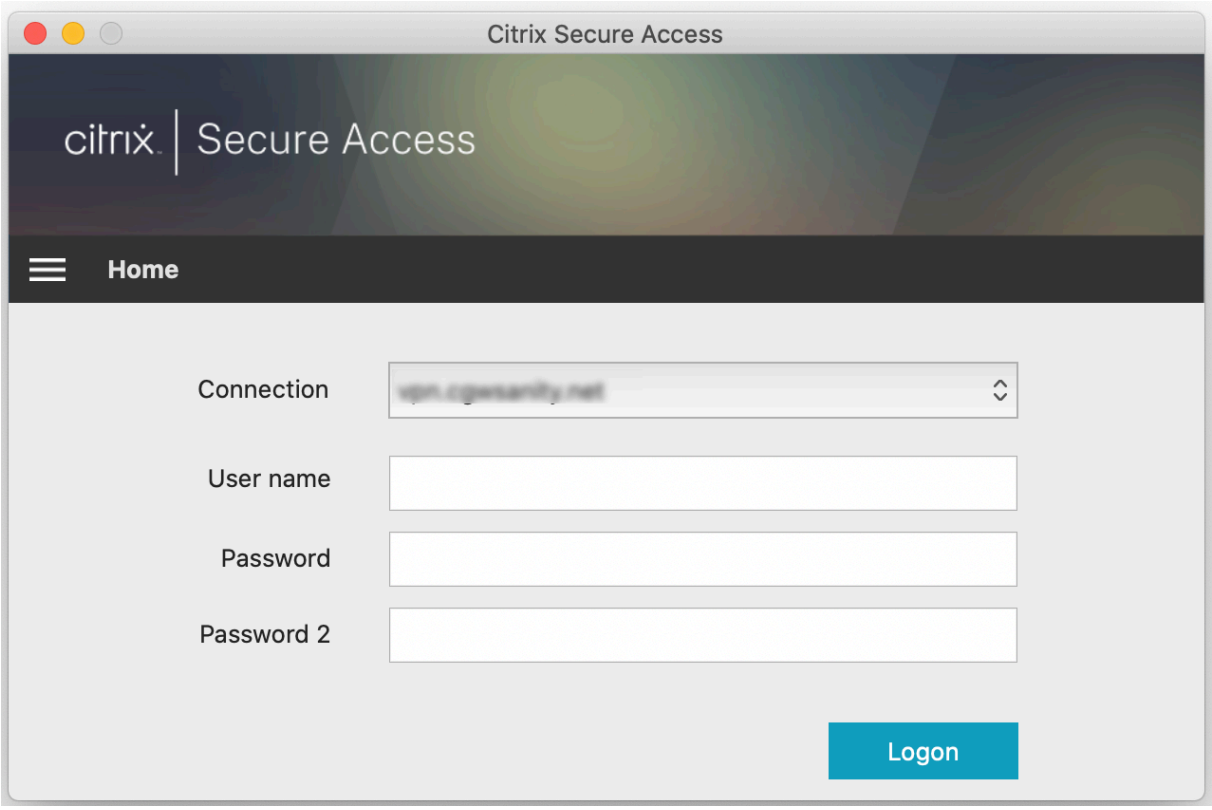
Add a connection

Enter the base URL (for example, https://gateway.mycompany.com) and the name for the VPN connection.



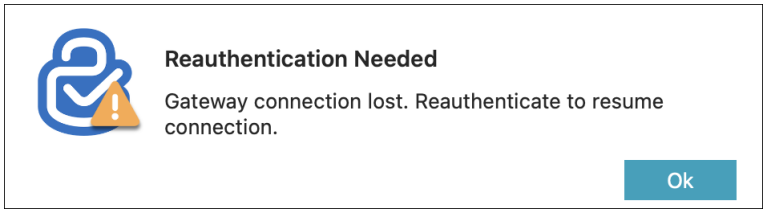
Connect to existing NetScaler Gateway

Select an existing connection and provide authentication credentials for your server and select **Logon**.



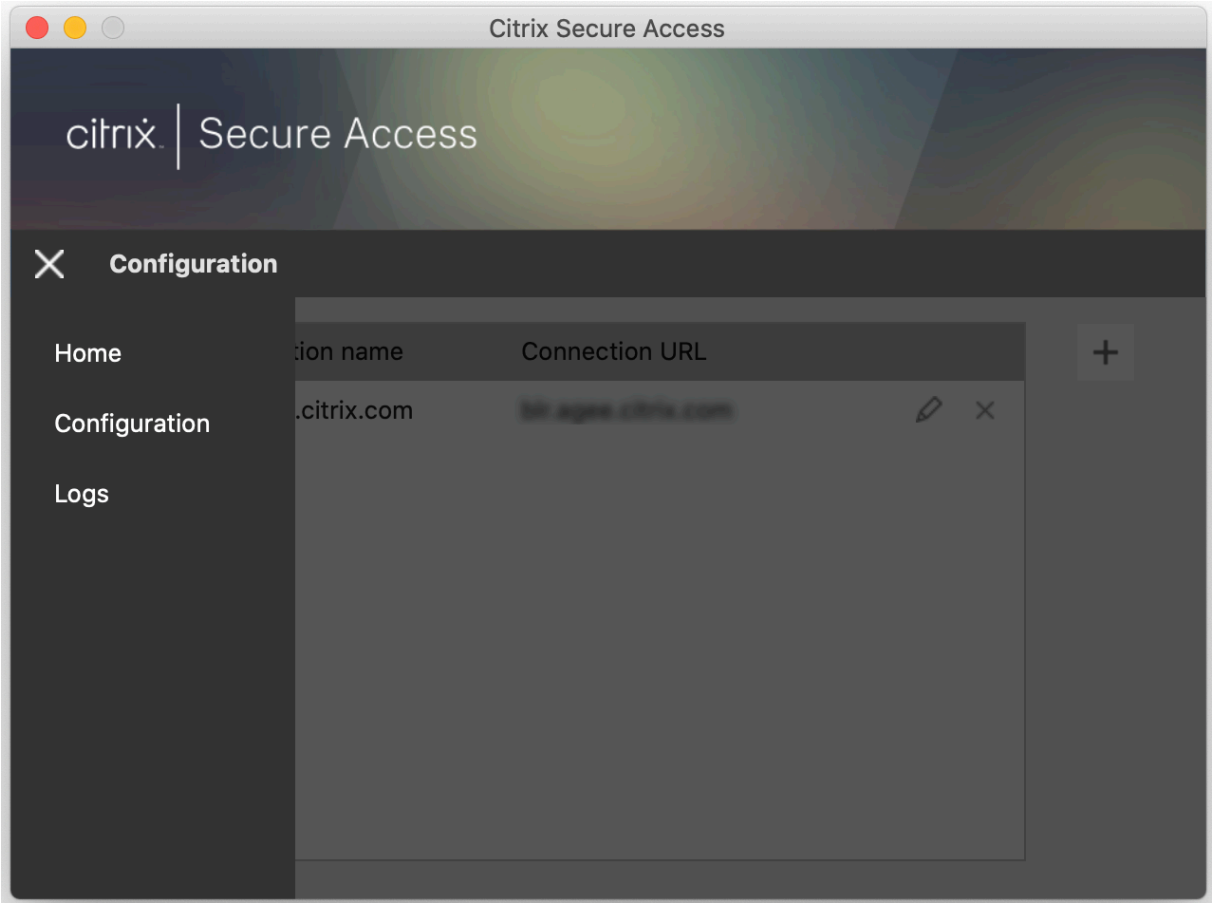
Reconnect to NetScaler Gateway after a VPN connection failure

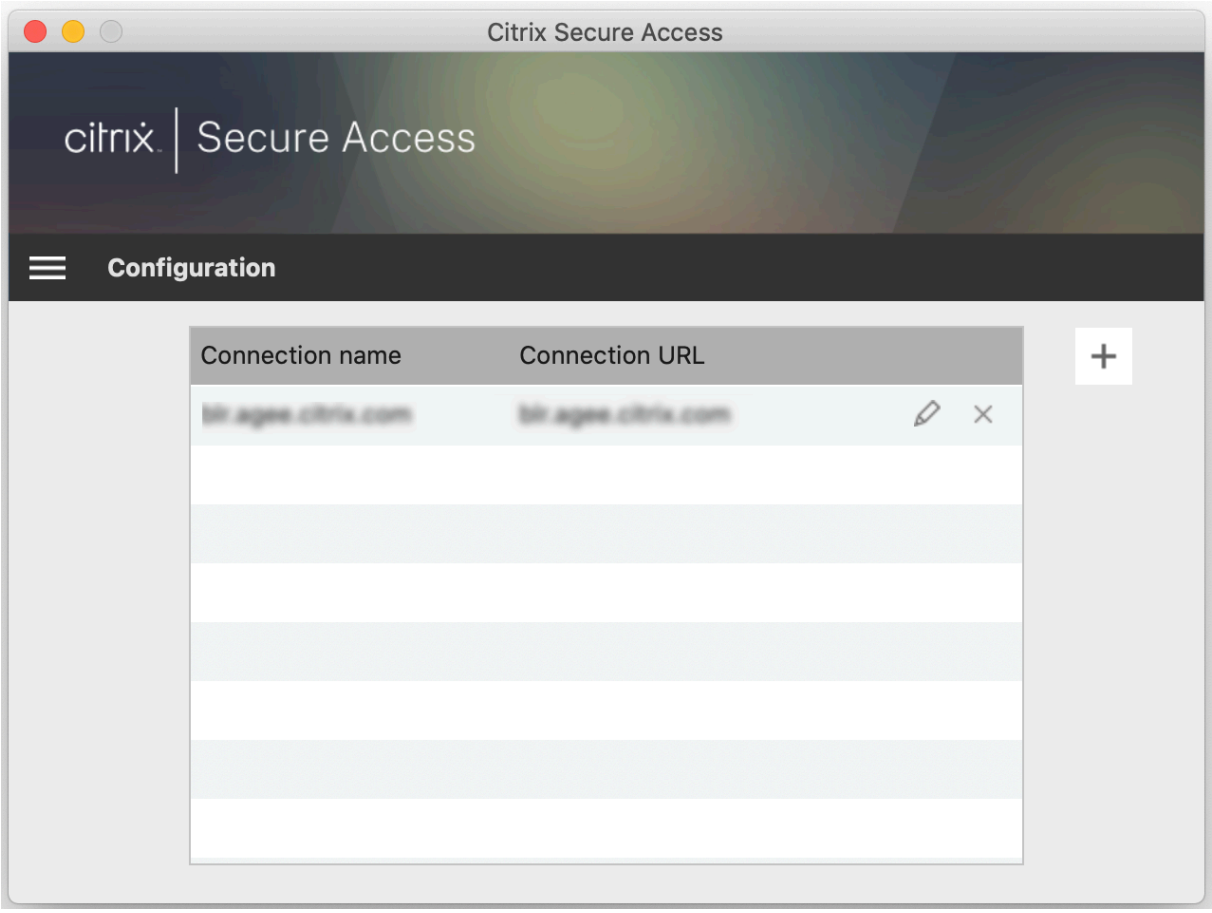
Starting from release 23.09.1, Citrix Secure Access client for macOS prompts you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the Citrix Secure Access client UI indicating that the connection to NetScaler Gateway is lost and that you must reauthenticate to resume the connection.



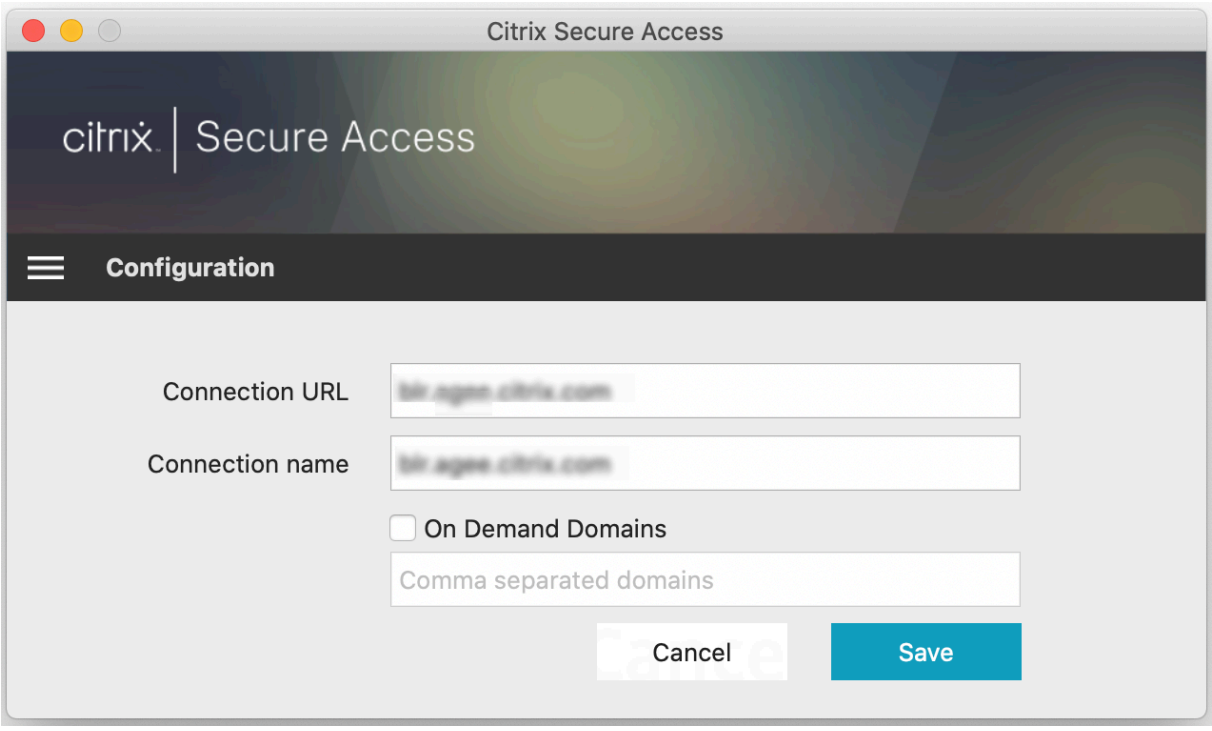
Modify an existing connection

You can modify or delete an existing connection.



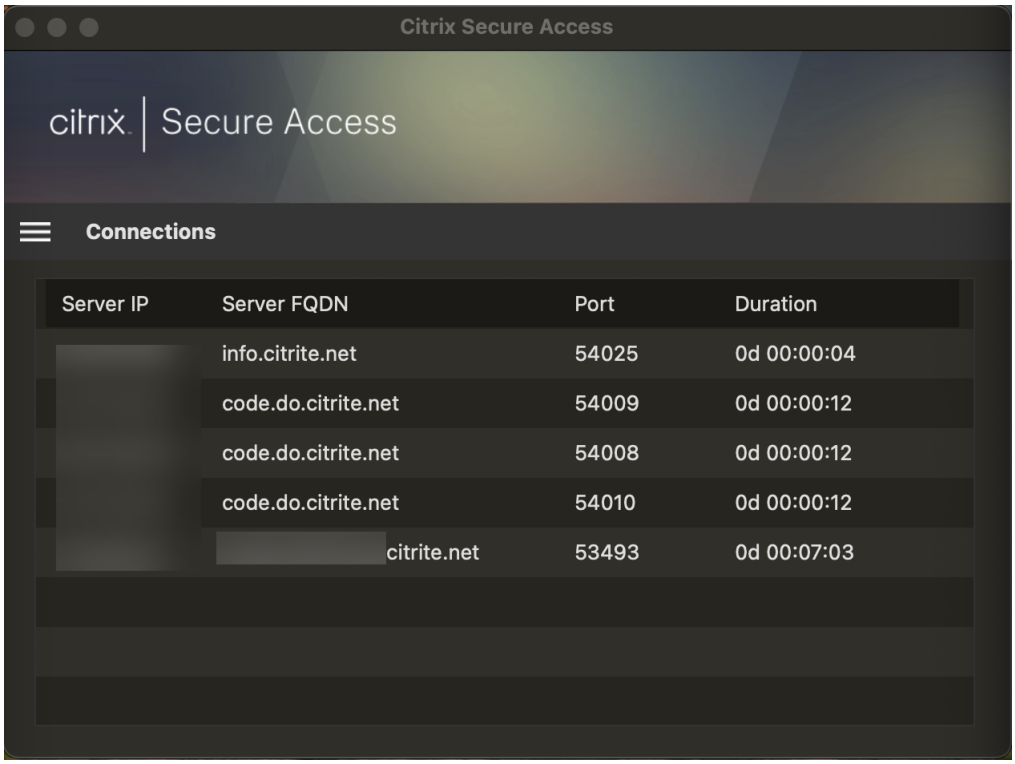


Modify the connection details as required.



Secured connection insights

Starting from release 23.09.1, you can view the secured connection details that include the IP address, FQDN, destination port, and duration of the connection. To view these details, click the hamburger menu on the UI and navigate to **Connections**.



Local LAN access

Citrix Secure Access client for macOS 23.10.1 supports the Local LAN access feature wherein you can determine whether you want to access the local LAN resources on your client machine once a VPN connection is established. You can use this feature only if your administrator has configured the local LAN access setting on NetScaler Gateway.

To enable the local LAN access on the Citrix Secure Access client UI, navigate to the home page and enable the **Allow Local LAN Access** checkbox.

After a connection has been established, you can verify the status of local LAN access on the same page.

Automatic single sign-on to Citrix Secure Access through Citrix Workspace app

> **Important:**
>
> This functionality is disabled, by default. To leverage this functionality, contact your administrator.

Starting from Citrix Secure Access for macOS 24.03.1, a login to Citrix Workspace app can single sign-on (SSO) the end-users to Citrix Secure Access, establish a user tunnel, and seamlessly provide access to TCP/UDP applications. If you are connected to Citrix Workspace app, Citrix Secure Access for macOS can be automatically launched and you can seamlessly log in using single sign-on.

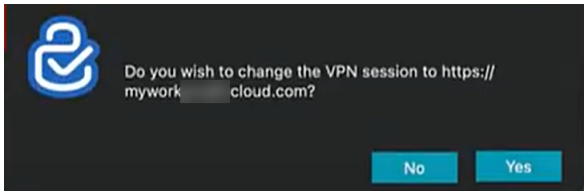
When you log on to Citrix Workspace App, Citrix Secure Access client is automatically launched and you are single signed on to the client. When you log out of Citrix Workspace app, Citrix Secure Access automatically logs you out of the application without your manual intervention. This feature saves time as end-users are expected to log on to just one application, thereby providing a unified experience.

> **Note:**
>
> For this feature to work, the primary URL that is accessed via Citrix Workspace app and Citrix Secure Access client must be the same.

Pre-requisites

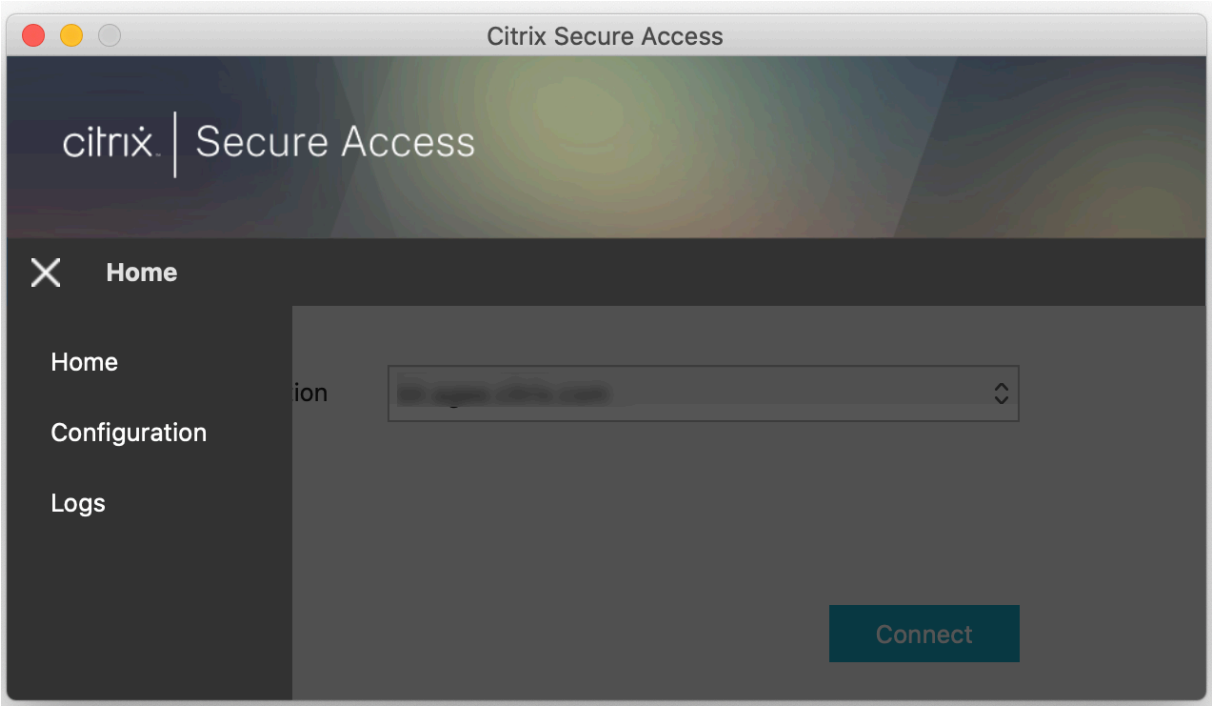
1. End-users must be on Citrix Workspace app 2402 or later. For details about installation of Citrix Workspace app for Mac, see Citrix Workspace app for Mac.
2. End-users must be on Citrix Secure Access for macOS 24.03.1 or later.

> **Points to note:**
>
> - If end-users are already logged on to Citrix Workspace app prior to using this functionality, they must re-login to Citrix Workspace app so that the app can trigger a single sign on to Citrix Secure Access client.
> - When a user logs out of Citrix Workspace app due to a timeout, manual user logout, and so on, Citrix Secure Access is also logged out and the user session is disconnected (this is only if Citrix Secure Access was automatically launched via Citrix Workspace app).
> - SSO login from Citrix Workspace app to Citrix Secure Access is supported only on a single primary domain. SSO on multiple domains is not supported.
> - If you switch your Citrix Workspace app connection to a different URL after being single signed on to Citrix Secure Access through this feature, you are prompted to choose your Citrix Workspace app connection URL.



Send logs

Capturing debug logs is a critical part of troubleshooting or reporting issues to Citrix Support. To troubleshoot the logs, navigate to **Home > Logs**.



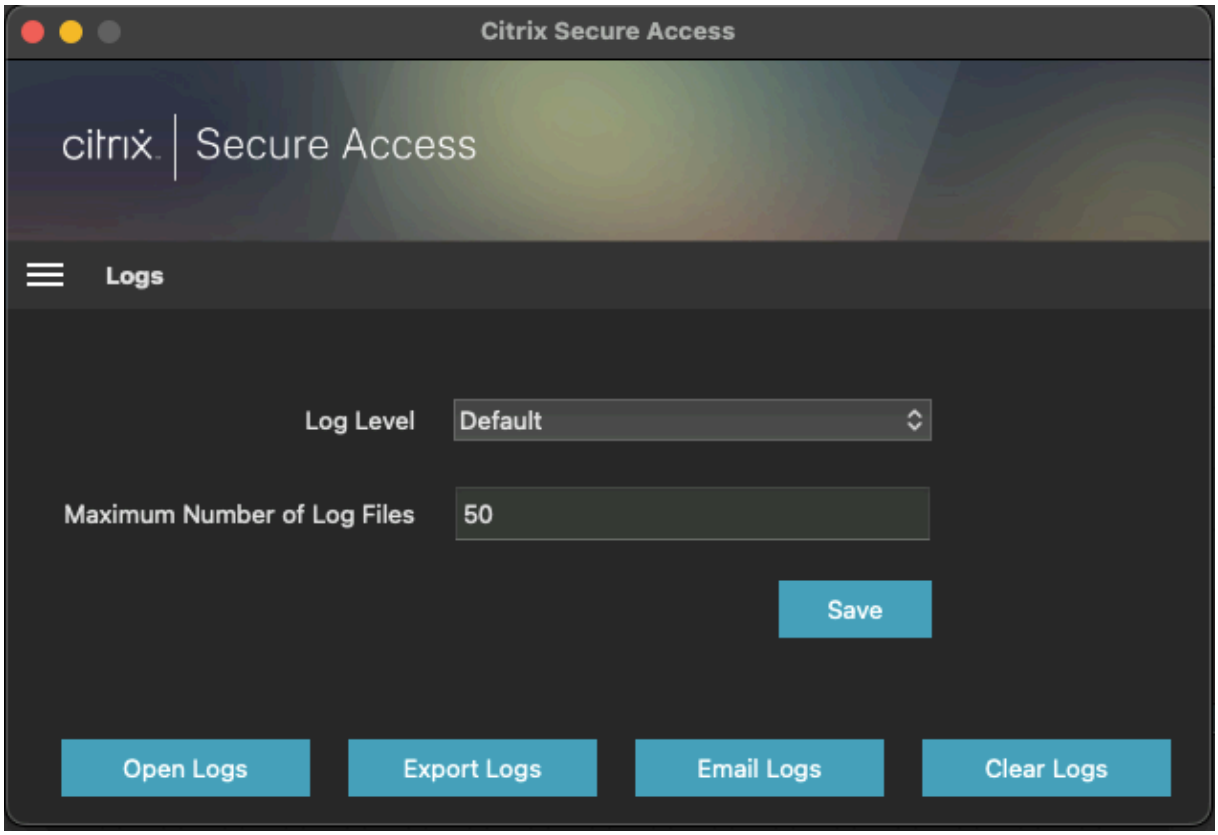
Select one of the following session log levels:

- **Default**: Prints the minimum logs for basic troubleshooting.
- **Debug Messages**: Prints all the logs.
- **Verbose**: Prints the verbose logs including tunnel messages and configuration information.

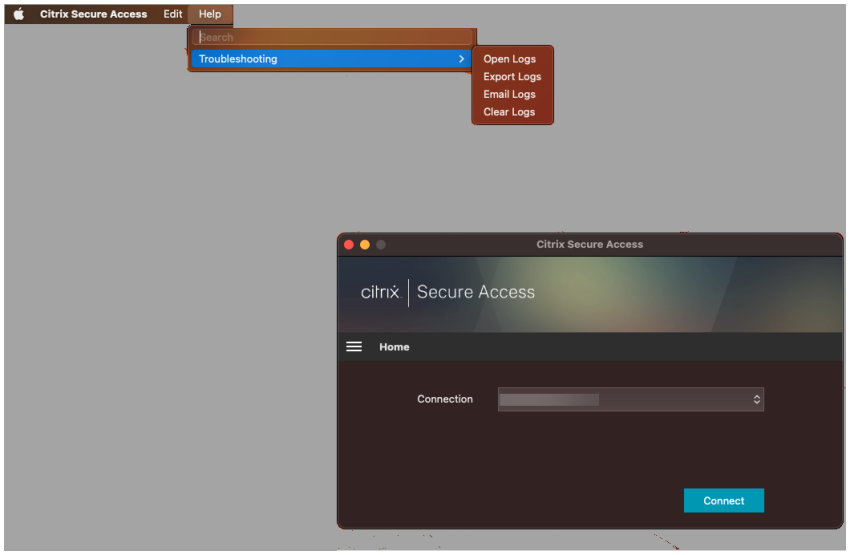
Starting from release 23.07.1, you can use the **Maximum Number of Log Files** field to specify the number of files that you want to add for log collection. You can add up to 50 log files.

- Click **Open Logs** to view logs.
- Click **Export Logs** to export the logs to your local directory.
- Click **Email Logs** to send the logs over email.
- Click **Clear Logs** to delete older logs.

> **Note:**
>
> Starting from Citrix Secure Access for macOS release 23.07.1, the **Email Logs** option is available on the **Logs** page.



Starting from Citrix Secure Access for macOS 23.06.1, a Help menu is introduced on the navigation bar of the Citrix Secure Access client. This menu can be used as an alternate location to capture and send the debug logs.



Reference

For administrator-specific instructions on Citrix SSO for iOS, see Citrix SSO for iOS and Citrix Secure Access for macOS.

Citrix Secure Access client for Linux

December 5, 2024

Citrix Secure Access client for Linux is a VPN client software managed by NetScaler Gateway that enables you to access corporate data and applications remotely.

Citrix End Point Analysis (EPA) client is a client software managed by NetScaler Gateway. It checks the endpoint criteria before granting access to corporate data through NetScaler Gateway. The Citrix EPA client and Citrix Secure Access client are independent from each other.

You can install the Citrix EPA client only if your administrator has configured it. For administrator specific instructions, see Citrix Secure Access client for Linux.

> **Important update:**
>
> We are updating our user interface and product documentation to the new NetScaler brand. You might see Citrix and NetScaler references used interchangeably during this transition period.

Install Citrix Secure Access client and Citrix EPA client

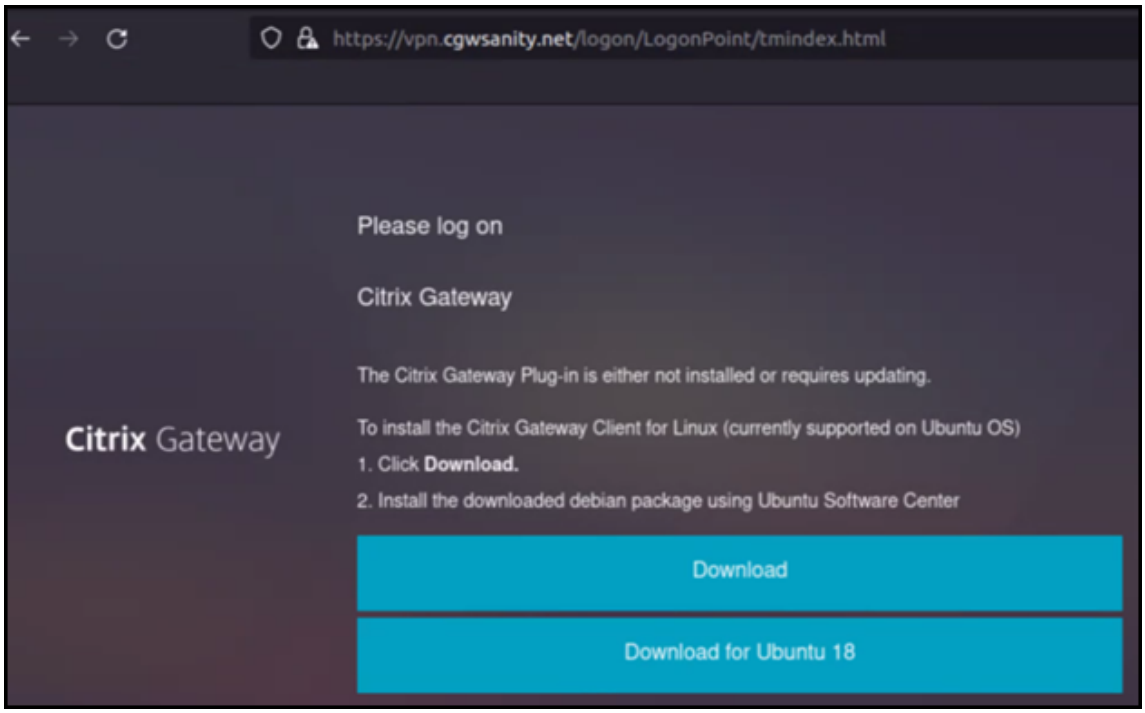
December 5, 2024

You can install the Citrix Secure Access client and the Citrix EPA client using the following instructions:

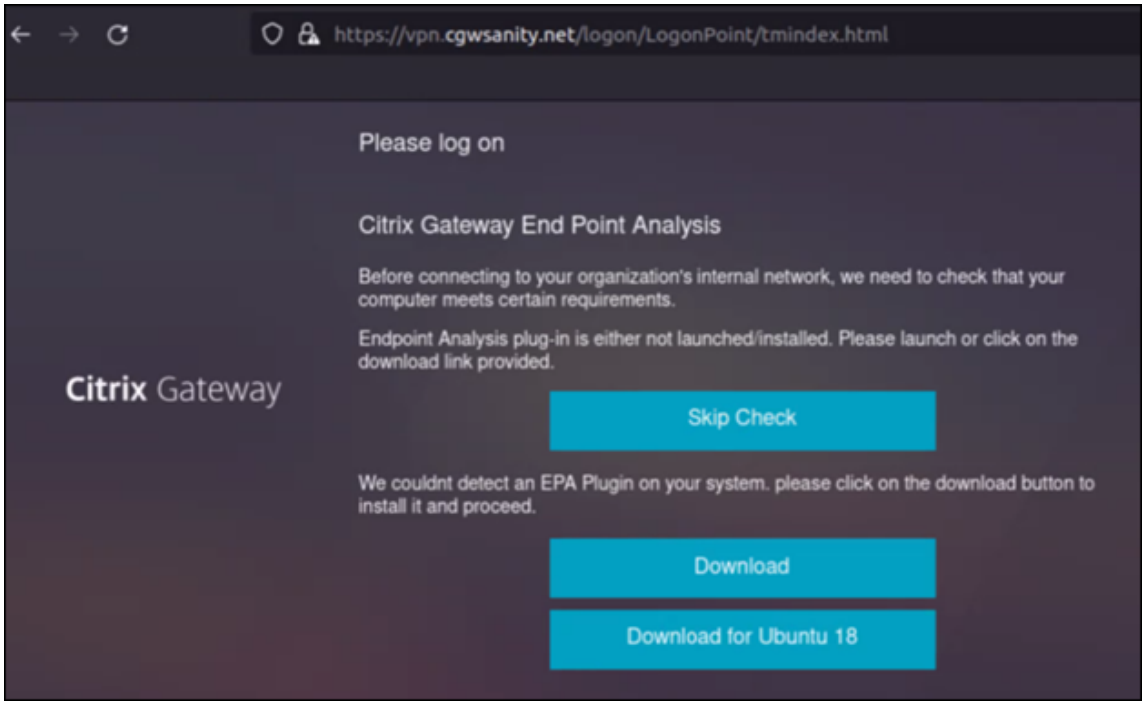
1. Open a web browser and enter the NetScaler Gateway URL provided by your administrator. After a few seconds, a download screen appears:

   - Click the **Download** button to download the Citrix Secure Access client for Ubuntu 22.04.
   - Click the **Download for Ubuntu 18** button to download the Citrix Secure Access client for Ubuntu 18.04 or Ubuntu 20.04.

   The following screen appears for the Citrix Secure Access client download:

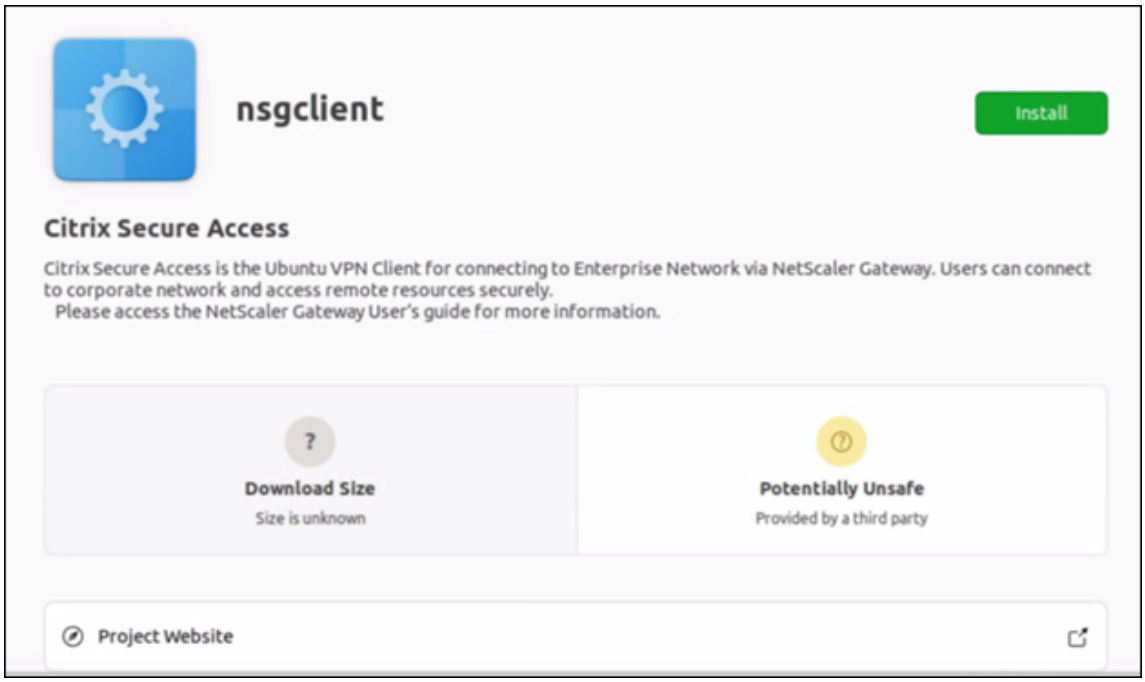


   The following screen appears for the Citrix EPA client download:

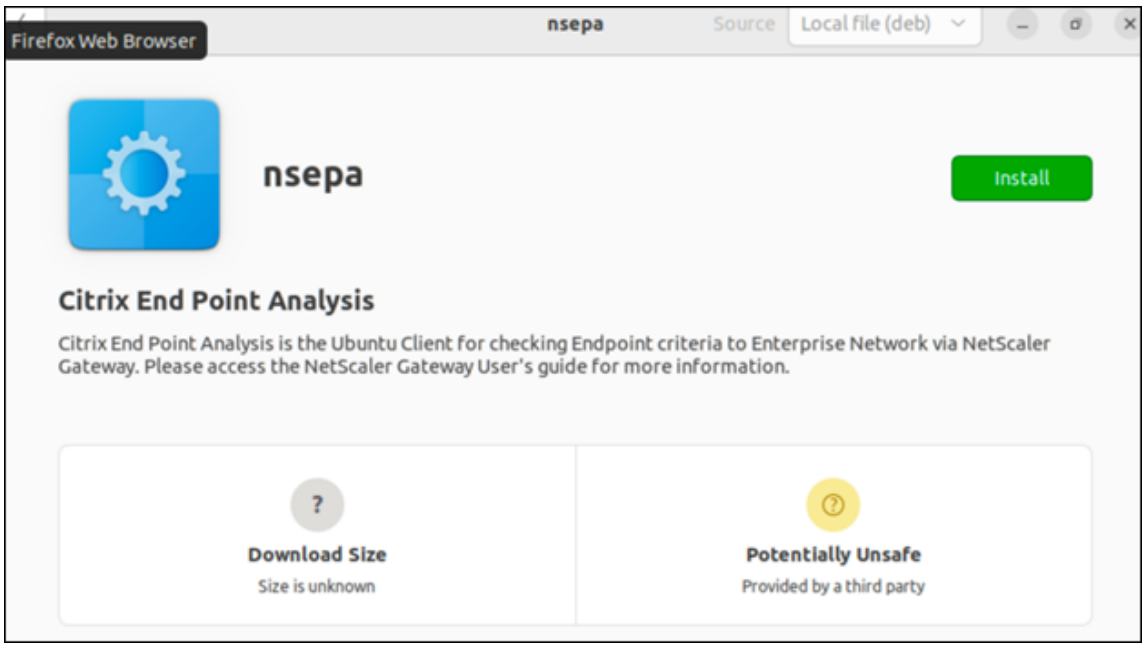


2. Once the download is complete, double-click the file and install the Citrix Secure Access client and Citrix EPA client.

   The following screen appears when you double-click the downloaded Citrix Secure Access client:

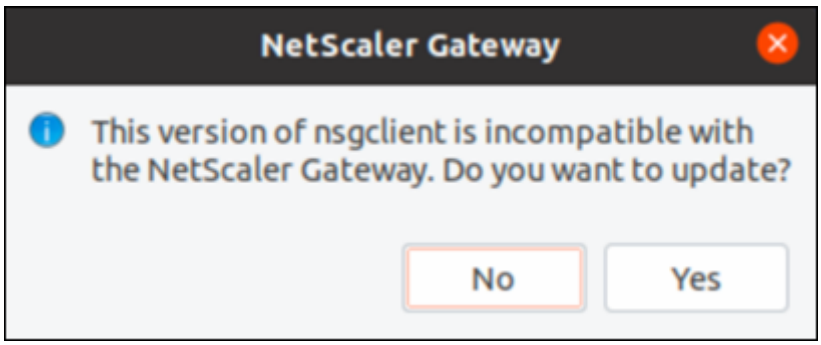


   The following screen appears when you double-click the downloaded Citrix EPA client:



If the Citrix secure Access client is already installed but not upgraded, you are prompted to upgrade to the latest version. Click **Yes** to upgrade to the latest version as shown in the following screen:

This upgrade is not applicable to the Citrix EPA client.



Notes:

- **Ubuntu 20.04 or 22.04 users**: If Citrix Secure Access client and Citrix EPA client are already installed but not up to date, you must uninstall the current version of the clients before upgrading to the latest version. This is because, unlike Ubuntu 18.04, you cannot replace the current version of the clients with the latest version.
- On Ubuntu 20.x, if you download the Citrix Secure Access client from a Firefox browser and then open it using the Open With option, then the installation might fail. This is because Firefox downloads the client at a temporary location and the Citrix Secure Access client installation fails from this location.

  As a workaround, we recommend that you select the Save File option. This option down-

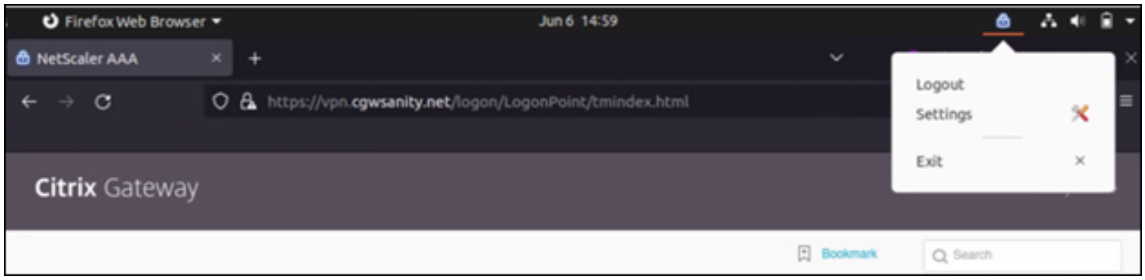
> loads the Citrix Secure Access client in the Downloads folder. You can then double-click the downloaded file and install the Citrix Secure Access client.

How to use Citrix Secure Access client for Linux

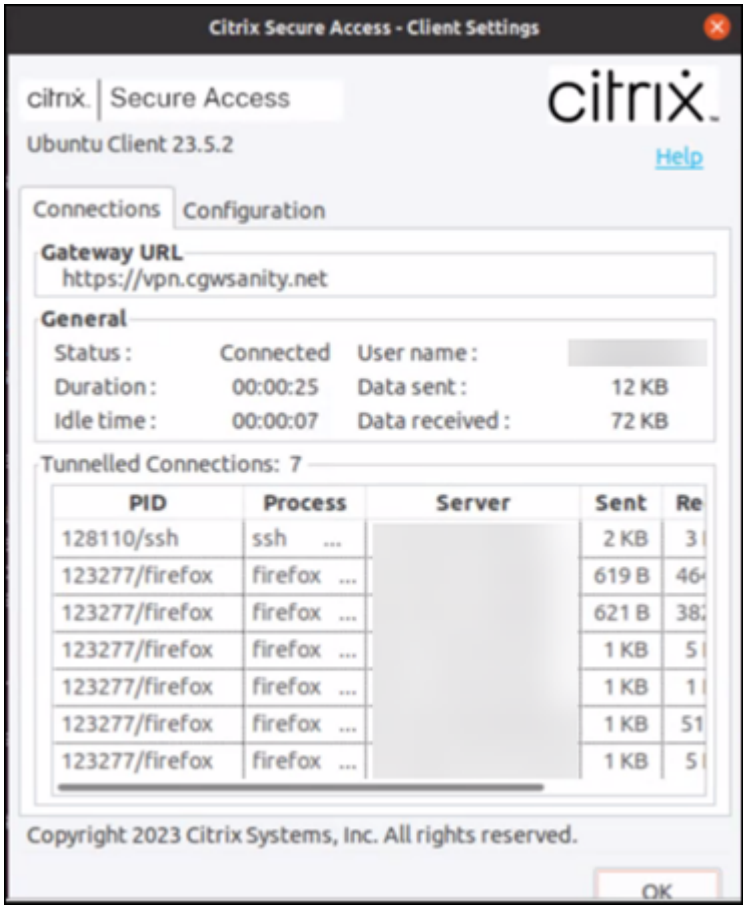
December 5, 2024

Enter the NetScaler Gateway URL on your browser to authenticate with the Citrix Secure Access client. Once the authentication is successful, the browser prompts you to launch the Citrix Secure Access client.

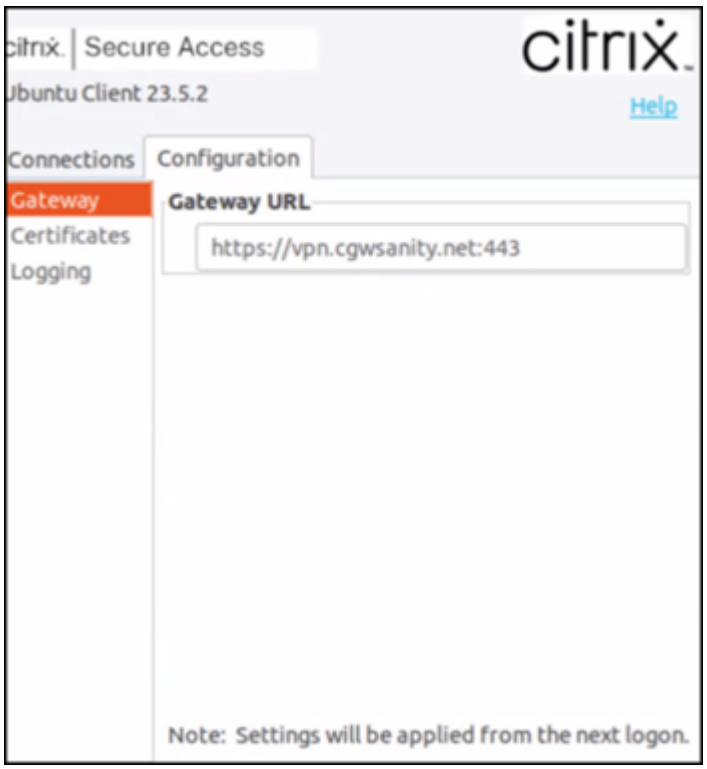
- Select the Citrix Secure Access client icon on the taskbar and click **Settings**.



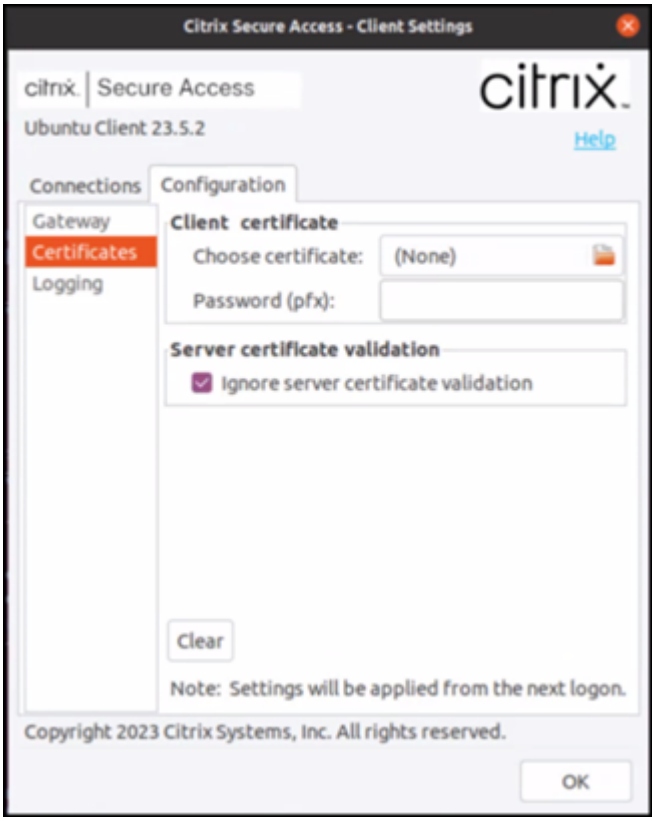
- The **Connections** tab displays details such as connection status, user information, tunneled connections, and data usage.



- The **Configuration** tab displays the NetScaler Gateway information, an option to upload a client certificate, and logging options.

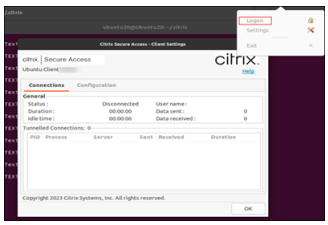


- Certificates: Navigate to this section to configure a client certificate. This step is required only if your administrator has provided a client certificate to you to authenticate with NetScaler Gateway.



- Logging: Navigate to this section to capture the debug logs. Capturing debug logs is a critical part of troubleshooting or reporting issues to Citrix Support.

Alternatively, you can launch Citrix Secure Access client and click **Logon**. If you are a first time user, you are prompted to provide either the NetScaler Gateway URL or your workspace URL.



Send logs

The log files that you send to your administrator are of the format `nsgcepa.txt`, `nsepa.txt`, and `nssslvpn.txt`. These files are in the ~/`.citrix`/ directory. They capture the following details:

- Info: Prints the basic and error logs.
- Debug: Prints all the logs. We recommend that you select this option to collect the logs and share with your administrator.
- Verbose: Prints the verbose logs including tunnel messages and configuration information.

Citrix Secure Access client for Windows

January 8, 2025

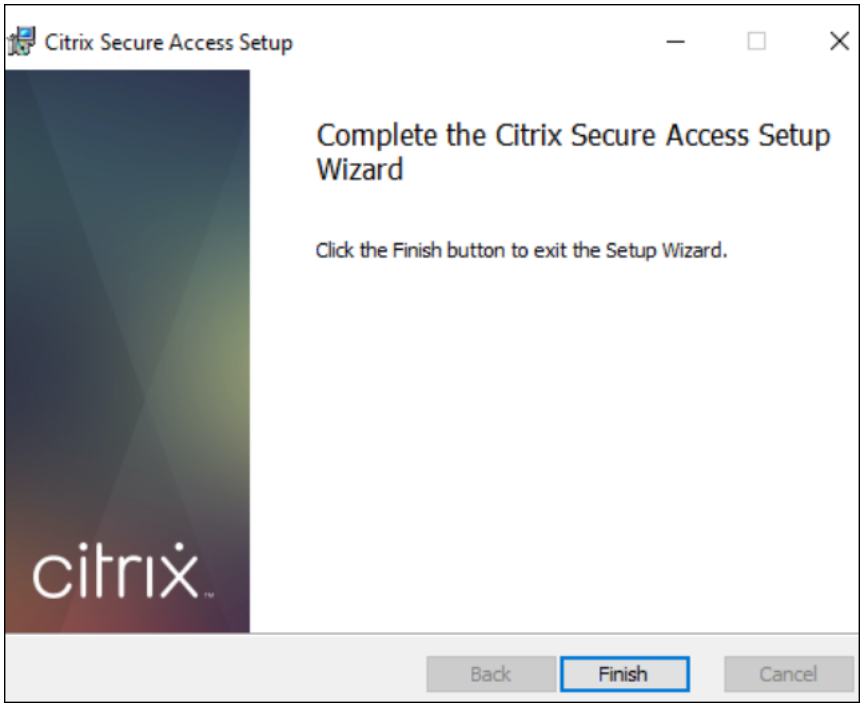
The Citrix Secure Access client for Windows is a VPN client software that enables you to access corporate data and applications remotely using NetScaler Gateway and Secure Private Access.

Install Citrix Secure Access client for Windows

You can install the Citrix Secure Access client using the following instructions:

1. Download the Citrix Secure Access client from https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
2. Click **Install** to install the client on your Windows machine. If you have an existing Citrix Secure Access client, the same gets upgraded.

3. Click **Finish** to complete the installation.



How to use Citrix Secure Access client for Windows

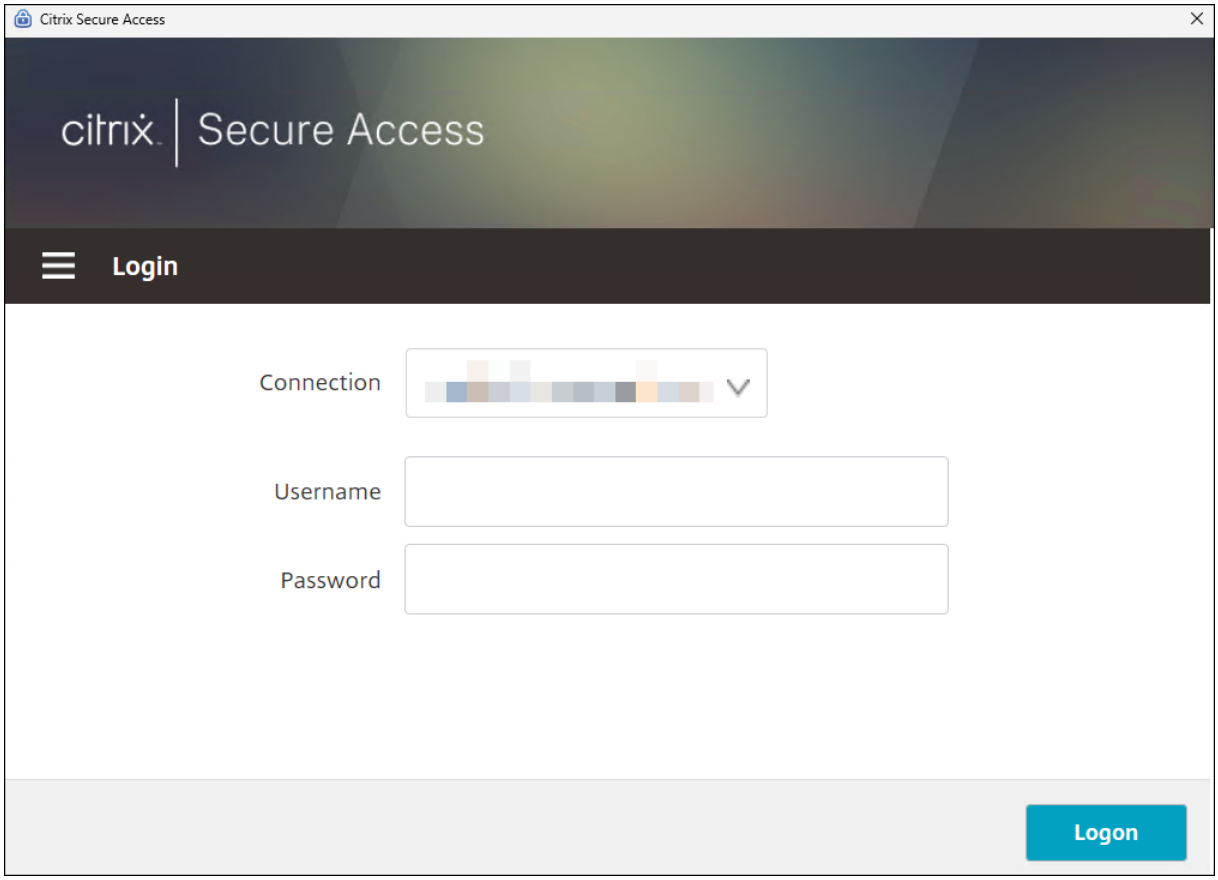
March 18, 2025

First-time users must create a connection to NetScaler Gateway or Secure Private Access by adding the connection URL, if your administrator has not added the connection URL for your application. For subsequent uses, you can connect to an existing connection, add a connection, and edit existing connections as well. You can also view the logs and take appropriate actions accordingly.

Add a connection

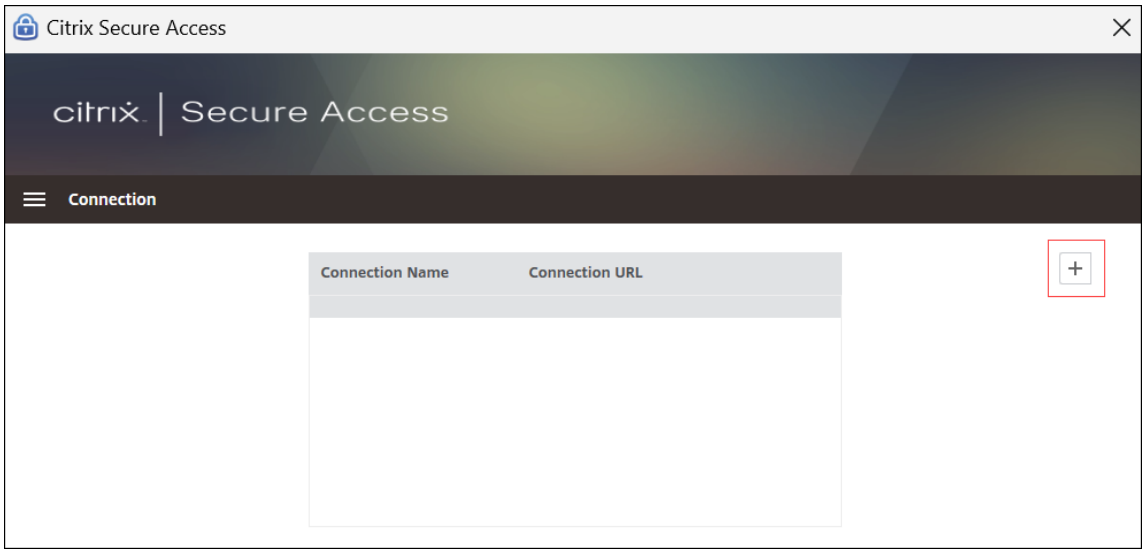
> **Important:**
>
> After the connection is added, the Citrix Secure Access client prompts for authentication. The prompt depends on the authentication method configured in NetScaler Gateway or Secure Private Access. You might need to enter a password or a one-time password. Alternatively, you might be redirected to a SAML authentication URL.

If your administrator has already added a connection to your application, select the connection from the drop-down list in the **Home** page, enter your user name and password (or one-time password), and click **Logon**.

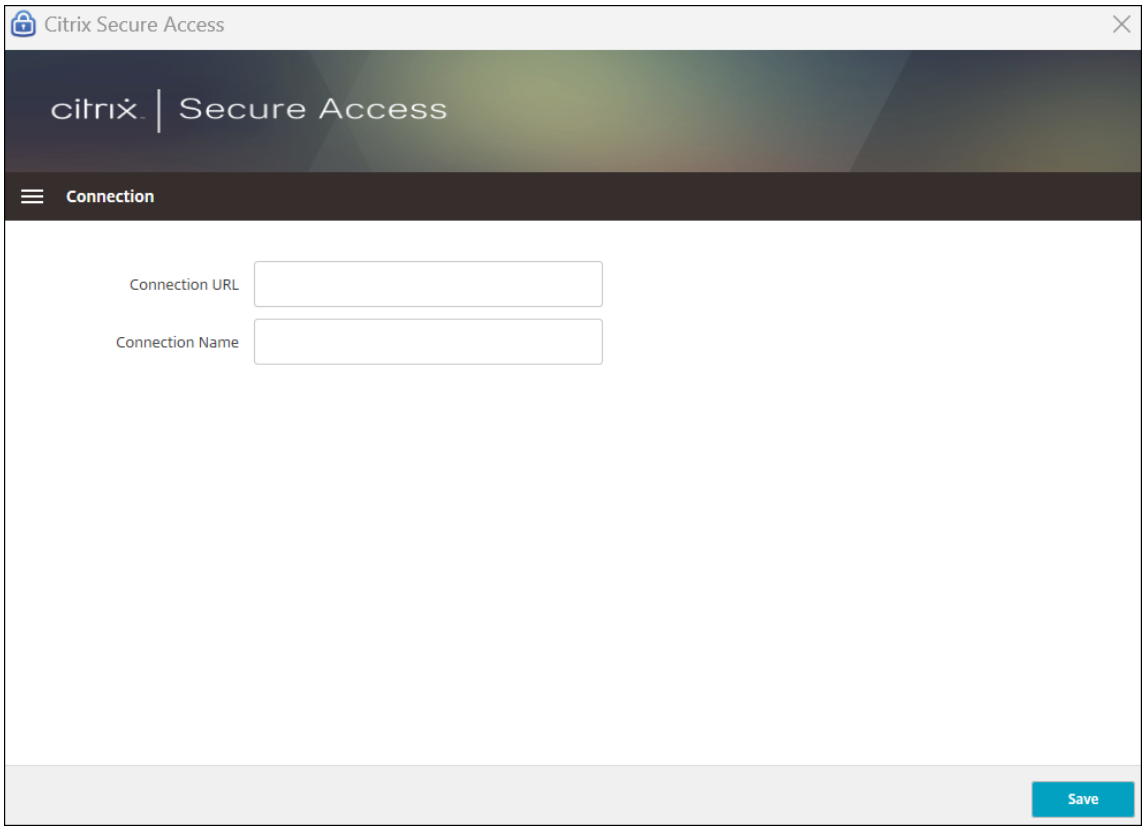


If your administrator has not added the connection URL, you must add a connection using the following steps:

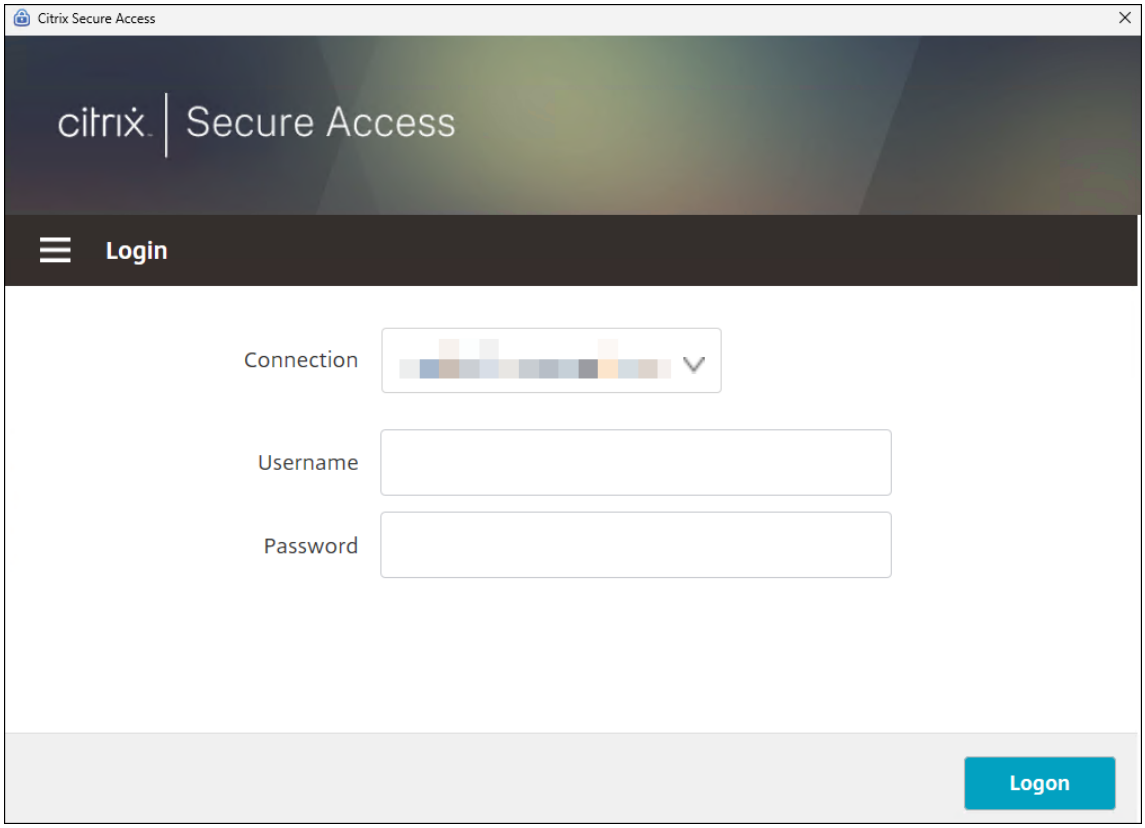
1. After you install the Citrix Secure Access client for Windows, open the application in your Windows machine.
2. Navigate to the **Connection** tab and click **+** to add a connection.



3. Enter the URL provided by your administrator in the **Connection URL** textbox, provide a name for the connection, and click **Save**.



4. Once the connection is added, navigate to the **Home** tab, select the connection from the drop-down list, enter your user name and password (or one-time password), and click **Logon**.

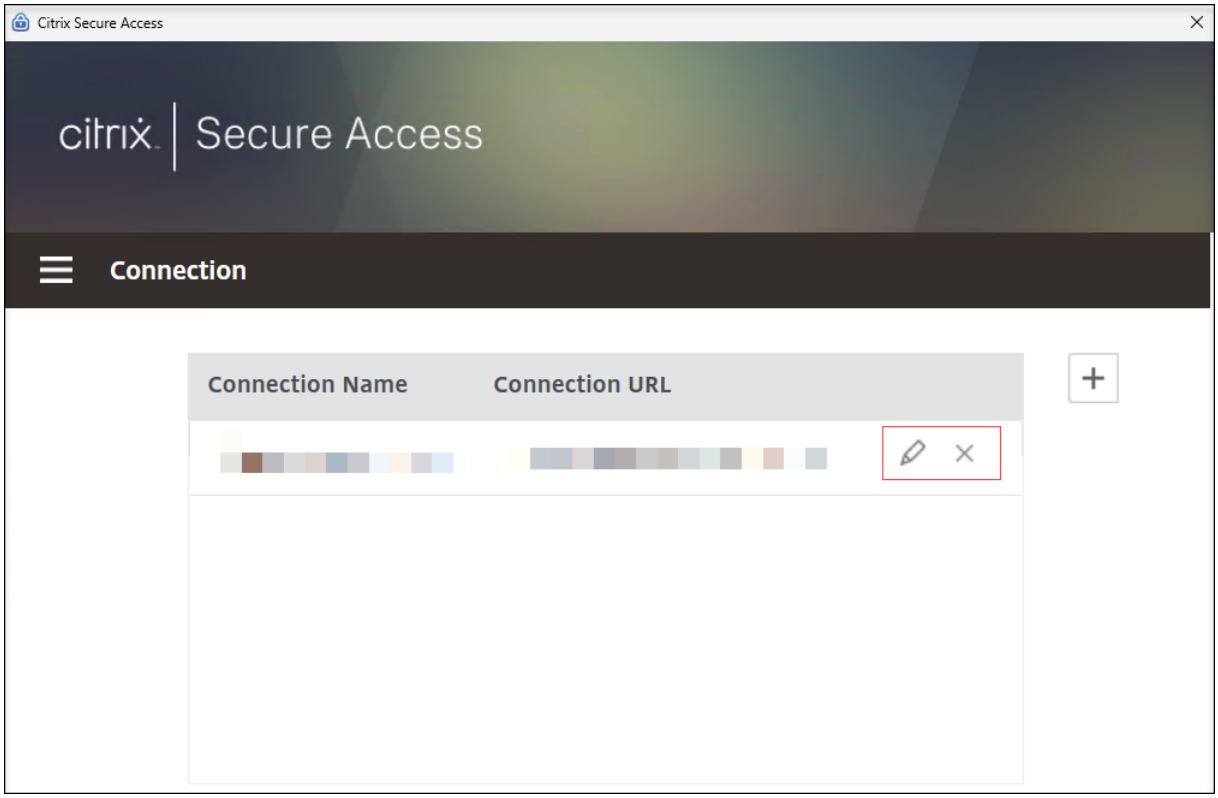


When the authentication is successful, you can access the intranet applications.

> **Note:**
>
> After the initial login, you cannot manually connect or disconnect the VPN if the administrator has enabled the Always On or Always On before Windows Logon profile on NetScaler Gateway or Secure Private Access.

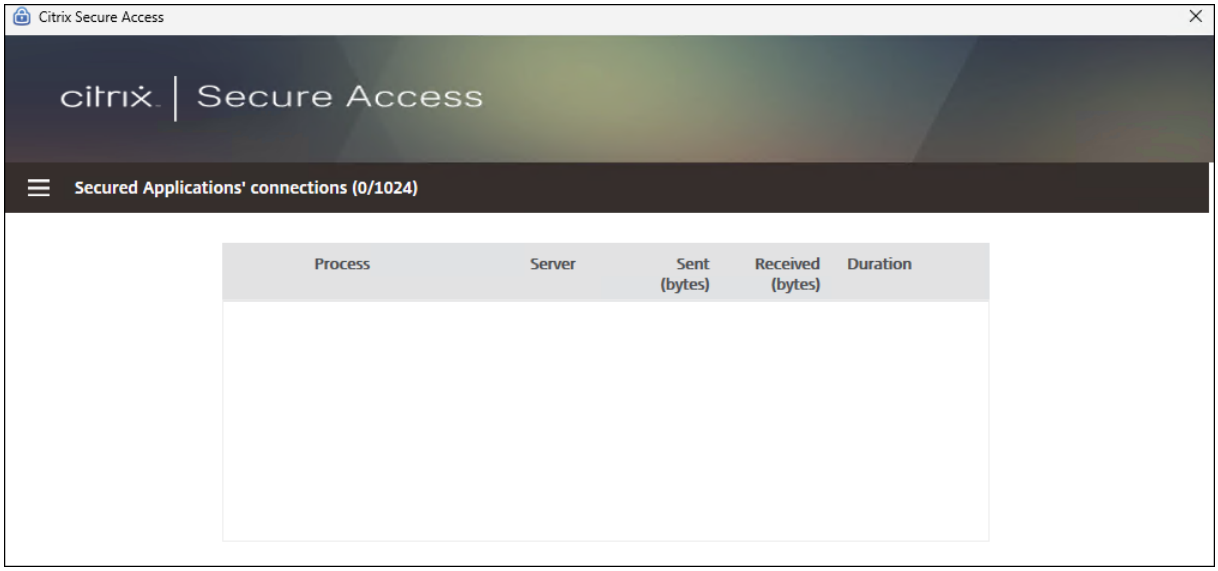
Modify or delete an existing connection

On the **Connection** tab, either click the edit icon or cancel icon to modify or delete the existing connection.



View secured applications

You can view the applications connected to the server, server IP, data sent and received, and duration of connection in the **Secured Applications** tab.



Configure logging

You can configure the log level, file size, and maximum number of log files in the **Logging** tab.

1. **Select Log Level:** The Citrix Secure Access client for Windows has two levels of logging:
    - **Info:** This level includes informational messages and events relevant to program execution. It also includes errors and exceptions.
    - **Verbose:** This level includes all log messages reported by **Info** level and other messages that might help in troubleshooting.
2. **Log File Size Limit:** Enter the file size of each log file. The maximum value is 600 MB.
3. **Maximum Number of Log Files:** Enter the number of files that you want to add for the log collection. The maximum value is 5.
4. Click **Save** to save the added logging configurations.

The **Logging** tab includes the following options:

- **Email Log Files:** Sends the log files to your administrator in the format nssslvpn.txt.
- **Start New Log File:** Creates a new log file, typically to start fresh logging for a new session or after a specific event for troubleshooting.
- **Collect Log Files:** Creates a zip file with all log files from the application. This zip file is saved on your desktop.
- **Open Log File:** Opens the latest csa_nssslvpn*.txt file.