Citrix Secure Access™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Install Citrix Secure Access 3

System requirements 7

Supported features 8

Client management 20

Feature management 25

Citrix Secure Access™ for Windows 25

Release notes 26

Features in preview 78

Improved log collection for Windows client 79

Integrated packet capture tool for Citrix Secure Access for connectivity troubleshooting 81

Citrix Secure Access™ auto log on for Windows Azure AD joined machines 84

Microsoft Edge WebView support for Windows Citrix Secure Access 88

Upgrade the Citrix Secure Access client and EPA client for Windows on NetScaler Gateway 91

Reverse split tunneling of non-configured domains 94

Troubleshooting failures in the Citrix Secure Access client for Windows 97

Citrix Secure Access for macOS/iOS 100

Release notes for the macOS clients 101

Release notes for the iOS clients 129

Set up Citrix Secure Access™ for iOS users 144

Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for Mac 152

Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for iOS 153

Send user certificate identity as an email attachment to iOS users 153

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Setup proxy PAC file for the Citrix SSO app for iOS users or the Citrix Secure Access™ client for macOS users 155

Set up Citrix Secure Access for macOS users 156

nFactor support for Citrix Secure Access client on macOS/iOS 164

Log collection for the macOS and iOS clients 166

Auto Update support for macOS 171

Troubleshooting common Citrix Secure Access for macOS/iOS issues 173

FAQs 175

Citrix Secure Access client for Linux 176

Release notes 180

Support for Microsoft Entra ID authentication with conditional access 186

Citrix Secure Access for Android 187

Release notes 188

Set up Citrix Citrix Secure Access in an MDM enviroment 207

Set up Citrix Secure Access in an Intune Android Enterprise environment 208

Single sign-on between Citrix Secure Access and Citrix Workspace app for Android 226

NetScaler Gateway certificate pinning with Citrix Secure Access for Android 227

Data governance 229

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install Citrix Secure Access

September 9, 2026

Install the Citrix Secure Access client for Windows

- For details on installing the Citrix Secure Access client for Windows, see Install Citrix Secure Access client for Windows.
- For details on how to use the Citrix Secure Access client for Windows, see How to use Citrix Secure Access client for Windows.

ARM64 support for the Citrix Secure Access client

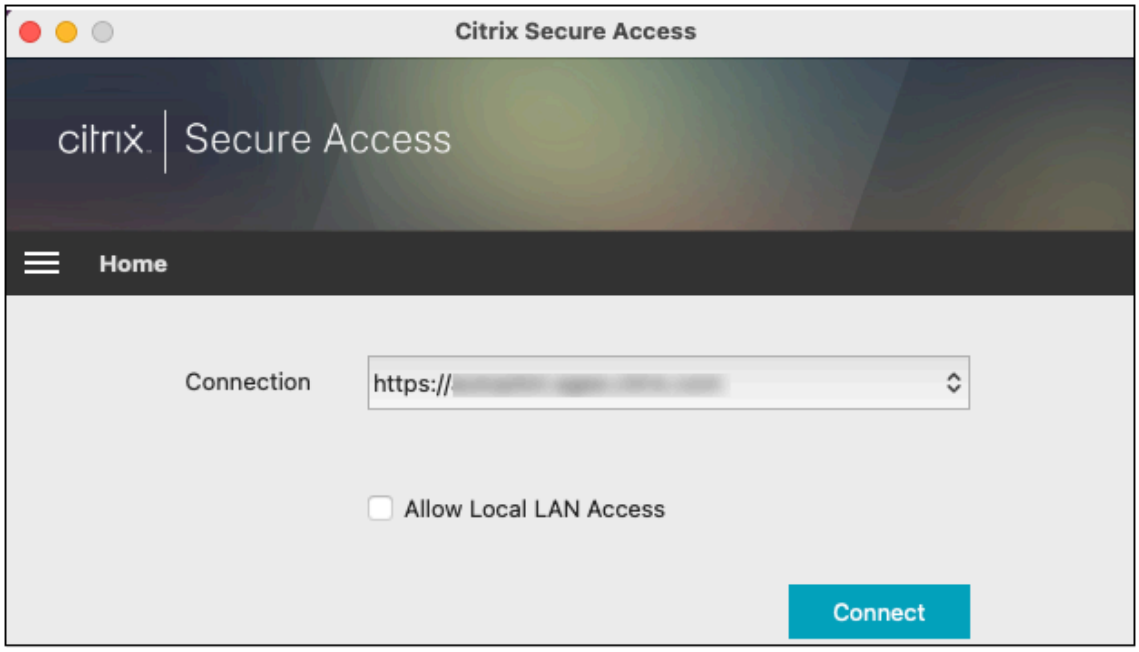
Starting from 25.7.1.11, the Citrix Secure Access application supports ARM64 Windows devices. The installer automatically detects the system architecture and installs the appropriate ARM64 version. This allows users on the ARM64 Windows devices to access NetScaler Gateway and Citrix Secure Private Access. Previously, the Citrix Secure Access client was not compatible with ARM64 Windows devices.

How to connect to the Citrix Secure Access client

End users must perform the following steps to launch the Citrix Secure Access client on their machines:

1. Launch the Citrix Secure Access client on the client device.
2. Enter the Workspace URL provided by the customer admin in the **URL** field in the Citrix Secure Access client and click **Connect**. It is a one-time activity and the URL is saved for subsequent use.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. The user is prompted for authentication based on the authentication method configured in Citrix Cloud.

Upon successful authentication, the user can access the configured private apps.

> **Note:**
>
> If the admin has configured SSO, then end users need not connect to Citrix Secure Access as they are automatically logged in.

Install the Citrix Secure Access client for macOS

- For details on installing the Citrix Secure Access client for macOS, see Install Citrix Secure Access client for macOS.
- For details on how to use Citrix Secure Access for macOS, see How to use Citrix Secure Access app from your macOS device.

> **Note:**
>
> - The Citrix Secure Access client for macOS is available from macOS 10.15 (Catalina) and later.
> - Preview builds are available in the TestFlight app.
> - If you are switching between the App Store app and the TestFlight preview app, you must recreate the profile you want to use with the Citrix Secure Access app. For example, if you have been using a connection profile with `blr.abc.company.com`, delete the VPN profile, and create the same profile again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install Citrix Secure Access client for iOS

1. Download the Citrix Secure Access app for iOS from the App Store.
2. Click **Open** once the download is complete.

For details on how to use Citrix Secure Access for iOS, see How to use Citrix Secure Access from your iOS device.

> **Note:**
>
> The Citrix Secure Access client for iOS supports client certificate authentication with NetScaler Gateway. For more information, see Import and install certificates in Citrix Secure Access app.

Install Citrix Secure Access client for Linux

- For details on installing Citrix Secure Access client on Linux, see Install Citrix Secure Access client.
- For details on how to use Citrix Secure Access for Linux, see Use Citrix Secure Access client for Linux.

Install Citrix Secure Access client for Android

Download the Citrix Secure Access app for Android from the Google Play store.

For details on how to use Citrix Secure Access for Android, see How to use Citrix Secure Access from your Android device.

User notification messages

A pop-up notification message appears in the following scenarios:

- The app is not authorized by the admin for the user.

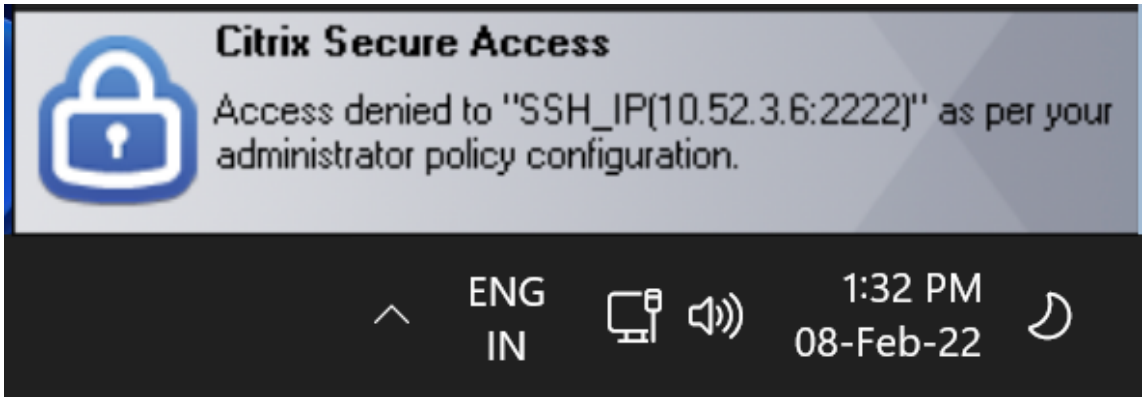
  Cause: The application configured for the accessed destination IP address or FQDN is not subscribed for the logged in user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The access policy evaluation results in denial of access.

  Cause: Access to the destination IP address or FQDN is denied because the policy bound to the application is evaluated to "Deny Access"to the logged in user.



- The enhanced security control is enabled for the app.

  Cause: The enhanced security control is enabled to the application for the accessed destination. The application can be launched using the Citrix Workspace™ App.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

System requirements

September 8, 2026

The Citrix Secure Access client as a desktop app is supported for the following operating systems and web browsers.

Supported operating systems	Supported versions	Supported browsers	Supported deployments
Windows	Windows 10 and Windows 11	Google Chrome Release 30 or later; Mozilla Firefox Release 24 or later; Edge Chromium	NetScaler Gateway and Citrix Secure Private Access
Windows Server	Windows Server 2016, Windows Server 1709, Windows Server 1803, and Windows Server 2019		
macOS	14.x (Sonoma) and 15.x (Sequoia)	Safari 7.1-18.1; Google Chrome Release 30 or later; Mozilla Firefox Release 30 or later	NetScaler Gateway and Citrix Secure Private Access
Ubuntu	22.04 and 24.04 eLux® and IGEL OS	Mozilla Firefox Release 44 and above; Google Chrome 50 and above	NetScaler Gateway and Citrix Secure Private Access

> **Note:**
>
> - Currently, Citrix Secure Access client and Citrix EPA client for Ubuntu only support the default GNOME display manager.
> - The Citrix Secure Access client for Linux version 24.11.4 and later supports eLux OS.

The Citrix Secure Access client as a mobile app is supported for the following operating systems.

VPN app	Supported versions	Supported deployments
iOS	iOS 16, 17, and 18	NetScaler Gateway and Citrix Secure Private Access
Android	Android 13, 14, 15, 16, and 17	NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If you are using the latest Apple OS versions such as macOS 26 (Tahoe)/iOS 26 and later, then we recommend that you upgrade to the Citrix Secure Access client version 25.08.1.1/25.08.1 or later.

Compatibility matrix for Citrix Secure Private Access

Platform	Supported client versions	Service deployments	On-premises deployments	Hybrid deployments
Windows	24.6.1.17 and later	Yes	Yes	Yes
macOS	24.06.2 and later	Yes	Yes	Yes
iOS	25.08.1 and later	Yes	No	Yes
Android	25.11.1 and later	Yes	No	Yes
Linux	24.10.1 and later	Yes	Yes	Yes

Supported features

September 25, 2026

> **Important:**
>
> - Citrix SSO for iOS/Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.
> - The legacy VPN client was built using Apple's private VPN APIs that are now deprecated. VPN support in Citrix Secure Access client for macOS/iOS is rewritten using Apple's public Network Extension framework. NetScaler Gateway plug-in and VPN for iOS and macOS are no longer supported. Citrix Secure Access for iOS/macOS is the recommended VPN client to be used.
> - General availability of nFactor authentication support for Android devices would be available in one of the upcoming releases.

The Citrix Secure Access clients support NetScaler Gateway and Citrix Secure Private Access deployments.

- Citrix Secure Access client features supported in NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Access client features supported in Citrix Secure Private Access

Citrix Secure Access client features supported in NetScaler Gateway

The following table lists some of the commonly used features supported for each VPN client in NetScaler Gateway.

Feature	Citrix Secure Access for Windows	Citrix Secure Access for macOS	Citrix Secure Access for iOS	Citrix Secure Access for Linux	Citrix Secure Access for Android
Always On (user mode)	Yes (11.1 and later)	No	No	No	Yes (via MDM)
PAC file	Yes (12.0 and later)	Yes	Yes	No	No
Client proxy support	Yes	No	No	No	Yes. *See note 1*
Max limit of Intranet Applications	512	No limit	No limit	128	No limit
Intranet IP (IIP) address support	Yes	Yes	Yes	Yes	Yes
Split tunnel ON	Yes	Yes	Yes	Yes	Yes
Split tunnel reverse	Yes	Yes	Yes	Yes	Yes. *See note 5*
Split DNS REMOTE	Yes	Yes	Yes	Yes	Yes. *See note 6*
Split DNS BOTH	Yes	Yes	Yes	Yes. *See note 8*	Yes. *See note 6*
FQDN based split tunnel	Yes-Only ON (13.0 and later)	Yes	Yes	Yes	Yes. *See note 5*
Client idle timeout	Yes	Yes	No	No	No
Endpoint analysis	Yes	Yes	No	Yes	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Access for Windows	Citrix Secure Access for macOS	Citrix Secure Access for iOS	Citrix Secure Access for Linux	Citrix Secure Access for Android
Device certificate (classic)	Yes	Yes	No	No	No
nFactor authentication	Yes (12.1 and later)	Yes	Yes	Yes	Yes. *See note 3*
EPA (nFactor)	Yes (12.1 and later)	Yes	No	Yes	No
Device certificate (nFactor)	Yes (12.1 and later)	Yes	No	No	No
Push notification	Yes (12.1 and later)	No	Yes	No	Yes
OTP token autofill support. *See note 2*	No	No	Yes	No	Yes
TLS 1.3 support	Yes	Yes. *See note 7*	Yes. *See note 7*	Yes	Yes
DTLS support. *See note 5*	Yes (13.0 and later)	Yes	Yes	No	No
HTTPOnly cookies	Yes	Yes	Yes	Yes	Yes
Global server load balancing (GSLB)	Yes	Yes	Yes	Yes	Yes
Local LAN access	Yes	Yes. *See note 7*	Yes. *See note 7*	No	No

Note:

1. Setting a proxy in the client configuration on the VPN virtual server in the gateway configuration for Android 10 and later is supported. Only basic HTTP proxy configuration with IP address and port is supported.
2. Only QR code-scanned tokens are eligible for auto filling. Auto filling is not supported in the nFactor authentication flow.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. nFactor authentication support for Android devices is under preview and the feature is disabled by default. Contact NetScaler support for enabling this feature. Customers must provide their NetScaler Gateway's FQDN to the support team for enabling nFactor authentication for Android devices.
4. For details, see Configure DTLS VPN virtual server using SSL VPN virtual server.
5. FQDN-based split tunnel support and reverse split tunnel for Android devices is under preview and the feature is disabled by default. Contact NetScaler support for enabling this feature. Customers must provide their NetScaler Gateway's FQDN to the support team for enabling it for Android devices.
6. For "Split DNS BOTH"mode, DNS suffixes must be configured on the gateway and only DNS A record queries ending in those suffixes are sent to the gateway. Rest of the queries are resolved locally. Citrix Secure Access for Android also supports "Split DNS LOCAL"mode.
7. TLS 1.3 and local LAN access are disabled by default in the Citrix Secure Access client for macOS and iOS. If required, contact Citrix Support.
8. The "Split DNS BOTH"mode functions the same as the "Split DNS LOCAL"mode in the Citrix Secure Access client for Linux.

Citrix Secure Access client features supported in Citrix Secure Private Access

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Always On (machine + user tunnel)	Yes	No	No	Yes	No	No	No	No	Yes. *See note 1*	No	No	No	No

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Always On (only user tunnel)	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No
Always On service (only machine tunnel)	Yes	No	No	Yes	No	No	No	No	Yes. *See note 1*	No	No	No	No
Client idle timeout	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes
SSO to Citrix Workspace™ app	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Datagram Transport Layer Security (DTLS)	Yes	Yes	No	No	No	No	No	No	Yes	Yes	Yes	No	No
EPA v2 or Device Posture service	Yes	Yes. *See note 4*	Yes	Yes	Yes. *See note 4*	No	No	Yes	Yes. *See note 3*	Yes. *See note 3* and 4	No	No	Yes. *See note 3*
Exclude domain DNS	Yes	Yes	No	Yes	Yes	Yes	No	No	Yes. *See note 7*	Yes. *See note 7*	Yes. *See note 7*	No	No
Forced time-out	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Global Server Load Balancing (GSLB)	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
HttpOnly cookie	Yes	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
Intranet IP address and Server Initiated Connection (SIC)	Yes	Yes	Yes	Yes. *See note 5*	Yes. *See note 5*	Yes. *See note 5*	Yes. *See note 9*	Yes. *See note 5*	Yes	Yes	Yes	Yes. *See note 9*	Yes
Local LAN access	Yes	Yes	No	No	No	No	No	No	Yes	Yes	Yes	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
nFactor authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes. *See note 11*	Yes
Device certificate authentication	Yes	Yes	No	Yes. *See note 2*	Yes. *See note 2*	No	No	No	Yes	Yes	No	No	No
Session timeout	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Smart spoofed IP address	Yes	No	No	Yes	No	No	Yes	No	Yes	No	No	Yes	No
Split tunnel OFF	No	No	No	No	No	No	No	No	No	No	No	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Split tunnel ON (hostname-based)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Split tunnel ON (IP address based)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Split tunnel REVERSE (hostname-based)	No	No	No	No	No	No	No	No	No	No	No	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Split tunnel REVERSE (IP address based)	No	No	No	No	No	No	No	No	No	No	No	No	No
Spoofed IP address support for both UDP and TCP DNS	Yes	Yes. *See note 8*	Yes	Yes	Yes. *See note 8*	Yes. *See note 8*	Yes. *See note 10*	Yes	Yes	Yes. *See note 8*	Yes. *See note 8*	Yes. *See note 10*	Yes
SSO using PRT token	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
SSO using Windows Hello	Yes	No	No	Yes	No	No	No	No	Yes	No	No	No	No
TCP split DNS support	Yes	No	Yes	Yes	No	No	No	Yes	Yes	No	No	No	Yes
Transmission Layer Security (TLS) 1.3	Yes	Yes. *See note 6*	Yes	Yes	Yes. *See note 6*	Yes. *See note 6*	Yes	Yes	Yes	Yes. *See note 6*	Yes. *See note 6*	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Citrix Secure Private Access - on-premises (Windows)	Citrix Secure Private Access - on-premises (macOS)	Citrix Secure Private Access on-premises (Linux)	Citrix Secure Private Access service (Windows)	Citrix Secure Private Access service (macOS)	Citrix Secure Private Access service (iOS)	Citrix Secure Private Access service (Android)	Citrix Secure Private Access service (Linux)	Citrix Secure Private Access hybrid (Windows)	Citrix Secure Private Access hybrid (macOS)	Citrix Secure Private Access hybrid (iOS)	Citrix Secure Private Access hybrid (Android)	Citrix Secure Private Access hybrid (Linux)
Plug-in upgrade through Gateway Appliance Configuration Service (GACS)	No	No	No	No	No	No	No	No	No	No	No	No	No
Observability	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No	Yes

Notes:

1. The hybrid deployments of Citrix Secure Private Access version 2502 and later supports Always On (machine and user tunnel) and Always On service (only machine tunnel) modes.
2. In the Citrix Secure Private Access service, device certificate authentication is not supported using third-party issued certificates.
3. The hybrid deployments of Citrix Secure Private Access version 2502 and later supports De-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vice Posture service.

4. The Device Posture service for macOS requires a standalone EPA client.
5. UDP is not supported in Citrix Secure Private Access service. So VoIP, SCCM, and GPO push from the server does not work in the Citrix Secure Private Access service.
6. For the macOS and iOS platforms, TLS 1.3 is behind a feature flag and is disabled by default. Contact Citrix Support to enable this feature.
7. The hybrid deployments of Citrix Secure Private Access version 2502 and later supports exclude domain DNS feature.
8. The spoofed IP address support for TCP DNS in Citrix Secure Private Access for macOS/iOS is behind a feature flag. Contact Citrix Support to enable this feature.
9. SIC is not supported for TCP/UDP connections in Adndroid devices.
10. Spoofed IP address is supported for UDP DNS but not for TCP DNS.
11. nFactor authentication is not supported if on-premises NetScaler Gateway is also using Network Access Control (NAC) check for Intune or CEM.

Client management

September 25, 2026

The Citrix Secure Access™ client can be managed using solutions like Microsoft Endpoint Configuration Manager, formerly System Center Configuration Manager (SCCM) and Citrix Global App Configuration service (GACS).

Single sign-on to Citrix Secure Access via Citrix Workspace app for Windows

Single sign-on to Citrix Secure Access through Citrix Workspace app for Mac - Preview

Single sign-on to Citrix Secure Access via Citrix Workspace™ app for Windows

Citrix Workspace app offers a unified client management experience for Citrix Secure Access. When users log on to Citrix Workspace app, they are automatically signed on to Citrix Secure Access and can access TCP/UDP applications seamlessly without the need to manually configure and sign in to multiple client applications.

How it works:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app installs, auto-updates, and signs on (SSO) to the Citrix Secure Access client. End users are automatically logged on to Citrix Secure Access without manual intervention and are notified upon a successful SSO.

This feature saves time as end users are expected to log on to just one application, providing a unified user experience. Also, there is no interaction between the end user and Citrix Secure Access.

Prerequisite:

End users must use Citrix Workspace app for Windows 2405 or later versions.

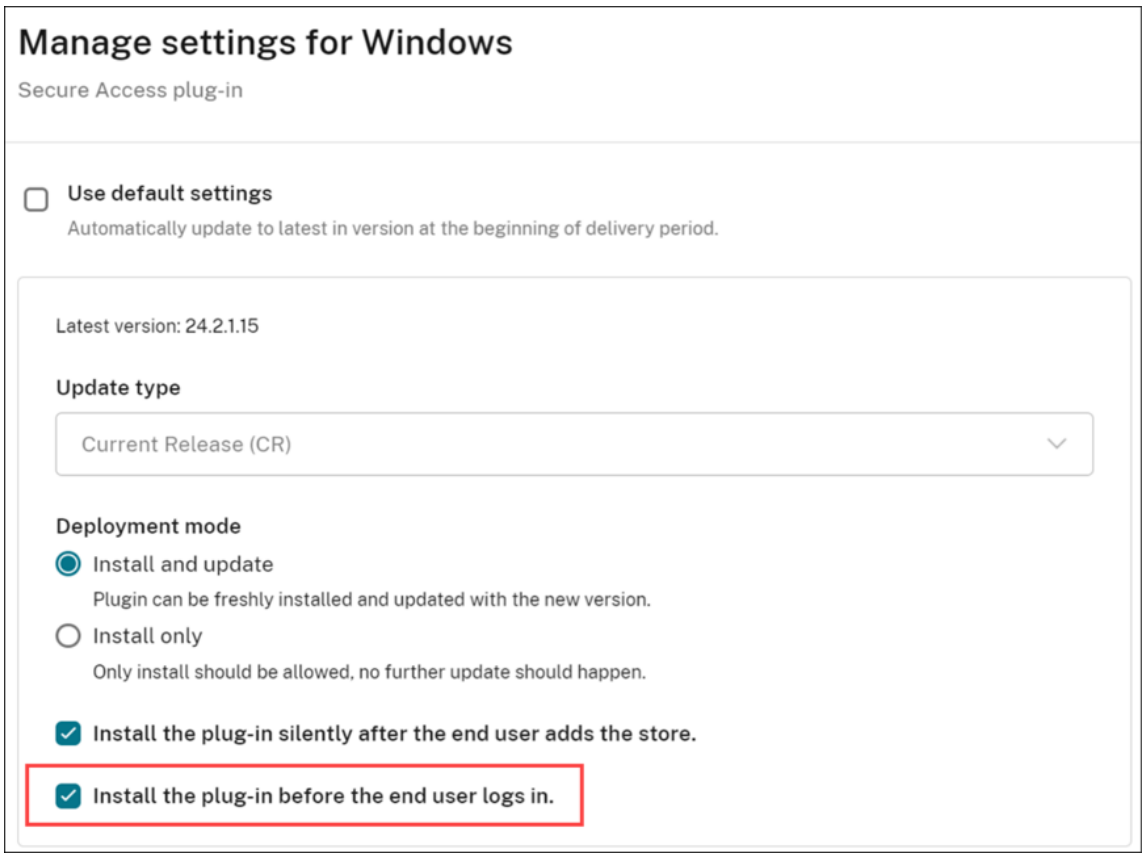
Configuration:

Admins must configure the Global App Configuration Service (GACS) settings on Citrix Cloud™ to enable Citrix Workspace app installs, auto-updates, and signs on (SSO) to the Citrix Secure Access client.

Enable installation and auto-update of Citrix Secure Access via Citrix Workspace app:

1. Log on to Citrix Cloud.
2. Click the hamburger menu and navigate to **Workspace Configuration > App Configuration**.
3. Select the **Updates and Plug-ins** section and navigate to **Secure Access Plug-in**.
4. Enable the **Windows** checkbox. This step installs Citrix Secure Access for Windows and automatically updates to the latest version.
5. Click **Edit** to configure the Windows plug-in settings.
6. On the **Manage settings for Windows** page, enable the **Install the plug-in before the end-user logs in** option.
7. Click **Save draft**.
8. On the confirmation window that appears, click **Yes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

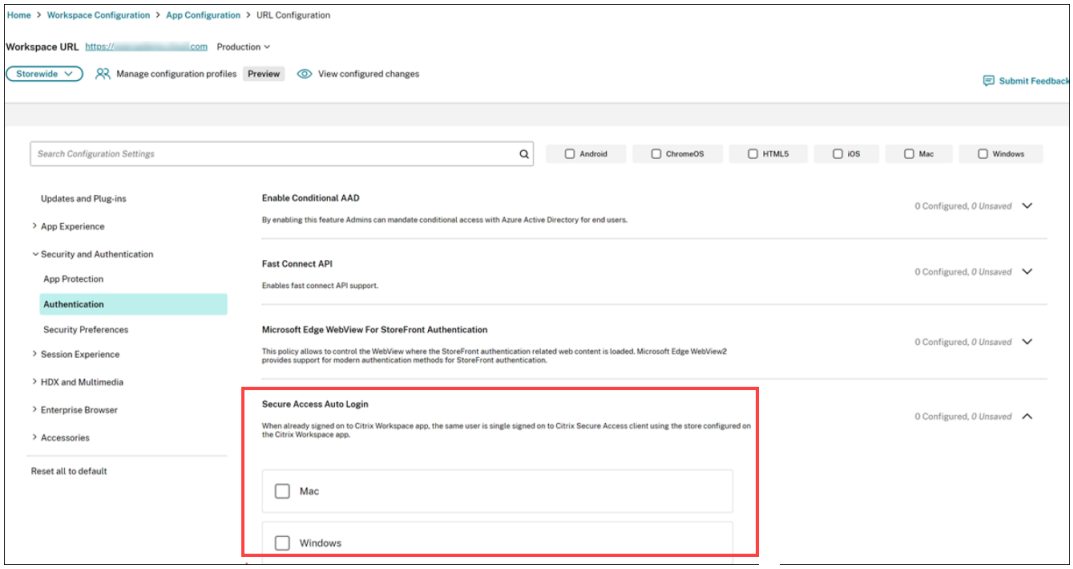


> **Note:**
>
> Auto-updation of the Citrix Secure Access client happens through the Beta channel. To subscribe to the Beta channel, refer to Installing Citrix Workspace app Beta program.

Enable SSO to Citrix Secure Access via Citrix Workspace app

1. Log on to Citrix Cloud.
2. Click the hamburger menu and navigate to **Workspace Configuration > App Configuration**.
3. Navigate to **Security and Authentication > Authentication**.
4. In the **Secure Access Auto Login** section, enable the **Windows** checkbox.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information about GACS, see Configure Citrix Workspace app using Global App Configuration service.

Limitations:

- 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.
- Citrix Workspace app does not log Citrix Secure Access client events (successful login or failure).

Enable SSO to Citrix Secure Access via Citrix Workspace app using the registry

The registry details used to enable SSO to Citrix Secure Access via Citrix Workspace app are as follows:

- Citrix Workspace Application version - **Citrix Workspace 22.10.5.14(2210.5) or above**
- Citrix Secure Access version - **22.10.1.9 or later**
- Citrix Secure Access Windows Registry - **EnableCWASSO**

The SSO feature is disabled by default. To enable this feature, add the following registry on the end-user machine.

- Registry Name - EnableCWASSO
- Registry Path - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Registry Type - REG_DWORD
- Registry Value - 1

> **Important:**
>
> Sometimes, the end user machines might need to reboot for successfully establishing single sign-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> on with Citrix Workspace app.

Single sign-on to Citrix Secure Access through Citrix Workspace app for Mac - Preview

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

When end-users log out of Citrix Workspace app, Citrix Secure Access automatically logs out without user intervention. This feature saves time as end-users are expected to log on to just one application, thereby providing a unified experience.

Pre-requisites:

1. End-users must be using 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 using Citrix Secure Access for macOS 24.03.1 or later.
3. To enable this feature through MDM, admins must use the following settings:
    - `<key>EnableSecureAccessAutoLogin</key><true/>`

Points to note:

- If end-users are already logged on to Citrix Workspace app before enabling this functionality, they must re-login so that Citrix Workspace app can trigger SSO to Citrix Secure Access client.
- When there is a logoff from Citrix Workspace app due to reasons such as a timeout or manual user logout, 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 single sign-on to Citrix Secure Access, you are prompted to select your Citrix Workspace app connection URL.

Client version control using Client app management

You can automatically update and manage the Citrix Secure Access client version for end users of the Secure Private Access service using the Client app management. For more information, see Citrix Secure Access - Client app management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported clients

The following table lists the platforms and the corresponding versions that support Client app management:

Platform	Version
Windows	25.11.1.12

Feature management

September 17, 2025

The Citrix Secure Access client provides access to preview features and allows dynamic management of features in production through Citrix-managed feature flags. To request a preview feature, customers must contact Citrix Support. The Citrix team will then enable and manage the feature from the back end for the gateway URLs of customers.

Feature management for the Citrix Secure Access client for Windows

To ensure optimal performance of preview features (features under feature flag) in the Citrix Secure Access client for Windows, you must enable traffic to `features.netscalergateway.net` and upgrade the clients to version 24.8.1.19 or later.

If an immediate upgrade isn't possible, use the registry settings for the preview features until end users update their client versions. Refer to NetScaler Gateway Windows VPN client registry keys for details on the registries.

> **Note:**
>
> No configuration is needed to enable traffic for feature management unless a firewall or proxy is blocking outbound traffic. In such cases, you must allow traffic to specific URLs or IP addresses according to your policy requirements.

Citrix Secure Access™ for Windows

September 25, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Starting from the Citrix Secure Access client for Windows release 25.2.1.18, you can ensure compatibility with the third-party software performing DLL injection from directories other than `C:\Windows` or `C:\Program Files`. Configure the third-party software to exclude the nsload.exe process. Alternatively, configure the `ExternalTrustedSigners` registry with the signer name of the injected DLL. For more information, see Login failure due to third-party software.

The Citrix Secure Access client for Windows enables you to access corporate data and applications remotely using NetScaler® Gateway and Secure Private Access.

The Citrix Secure Access client for Windows is now released on a standalone basis and is compatible with all NetScaler versions. We recommend that you use the latest version of Citrix Secure Access client as it contains the latest fixes and enhancements.

> **Notes:**
>
> - We recommend you to use Citrix Secure Access client for Windows version 24.6.1.18 or higher.
> - Citrix Secure Access for Windows 23.5.1.3 and later releases address the security vulnerabilities described in CTX561480. We do not support Citrix Secure Access for Windows versions below 23.5.1.3.

Release notes

September 25, 2026

> **Important:**
>
> Starting from the Citrix Secure Access client for Windows release 25.2.1.18, you can ensure compatibility with the third-party software performing DLL injection from directories other than `C:\Windows` or `C:\Program Files`. Configure the third-party software to exclude the nsload.exe process. Alternatively, configure the `ExternalTrustedSigners` registry with the signer name of the injected DLL. For more information, see Login failure due to third-party software.

The Citrix Secure Access client for Windows is now released on a standalone basis and is compatible with all NetScaler versions. We recommend that you use the latest version of the Citrix Secure Access client as it contains the latest fixes and enhancements.

The Citrix Secure Access client releases follow the format YY.MM.Release.Build.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The release notes describe the new features, enhancements to the existing features, and fixed issues.

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

For detailed information on the supported features, see NetScaler Gateway Product Documentation.

> **Note:**
>
> The Citrix Secure Access client for Windows release 26.6.1.20 or later addresses the security vulnerabilities described in CTX696734. We recommend you to use the Citrix Secure Access client for Windows version 26.6.1.20.

26.7.1.3 (Aug 14, 2026)

Fixed issues

- Citrix Secure Access fails to install on Windows 10 Enterprise LTSC 2019.

  [NSHELP-44881]

- The Citrix Secure Access client disconnects when NetScaler Gateway is explicitly configured to compress traffic inside the VPN tunnel.

  [NSHELP-44848]

- When location detection is enabled in Always On deployments, users might lose access to the local network while connecting to the corporate network.

  [NSHELP-44766]

- VPN logout might fail to restore the original automatic proxy settings when both manual and automatic proxy are configured.

  [NSHELP-44751]

- After upgrading to version 26.6.1.20, the Citrix Secure Access client fails to connect on ARM64 devices.

  [NSHELP-44719]

26.6.1.20 (Jul 14, 2026)

What's new

- **Support for multiple Entra profiles**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When a Windows device is registered with multiple Microsoft Entra tenants, including a primary Entra Join or Workplace Join, the Citrix Secure Access WebView authentication automatically selects the Entra account associated with the configured Workspace authentication, enabling a seamless sign-in experience.

[CSACLIENTS-16748]

Fixed issues

- When Citrix Secure Access is managed through Client App Management, it does not automatically update to the configured version after a system restart.

  [SPAHELP-700]

- Access to internal sites might fail when a large number of intranet applications are configured and ProxyOverride is applied on the client machine.

  [NSHELP-43489]

- On Windows 11, Citrix Secure Access fails to establish VPN connections with a configured auto-proxy URL due to proxy URL parsing limitations.

  [NSHELP-43386]

- Citrix Secure Access connection failures might occur when hostname-based applications are configured on an end-user machine with a network adapter that uses a 0.0.0.0 subnet mask.

  [NSHELP-43014]

- Windows 11 users with hardware smart card readers (CNG-backed certificates) might fail to authenticate through Citrix Secure Access when client certificate-based authentication is mandated on NetScaler.

  [NSHELP-42238]

- Secure Private Access diagnostic logs might be flooded with TCP DNS connection events.

  [CSACLIENTS-17199]

- When location detection is enabled in a machine tunnel setup, the Citrix Secure Access client fails to automatically reconnect if the user transitions from an intranet to an internet network.

  [CSACLIENTS-17091]

- Intranet application access might fail when you configure both Intranet IP address and location-detection together in Secure Private Access.

  [CSACLIENTS-17088]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Access to internal sites might fail if only machine tunnel is configured and Citrix Secure Access runs in DNE mode.

  [CSACLIENTS-17065]

- When ClientControl configuration is set to DENY under Always-On VPN profile, the Citrix Secure Access client UI still displays the Log Off button after the VPN tunnel is established, allowing users to disconnect manually.

  [CSACLIENTS-17020]

26.4.1.8 (May 06, 2026)

What's new

- **Integrated packet capture tool for troubleshooting**

  The Citrix Secure Access VPN client for Windows now includes an integrated network packet capture tool to help troubleshoot connectivity issues.

  From the Citrix Secure Access user interface, you can:

  - Start a live packet capture
  - Stop a live packet capture
  - View the status of an active packet capture

  Captured files are automatically saved to the `logs\captures\` directory under the Citrix Secure Access installation folder. Automatic file rotation is used to help limit disk usage.

  Packet capture files are also automatically included in the diagnostic log bundle when logs are collected for Citrix Support.

  To enable this feature, admins must configure the following registry:

  - **REG_PATH:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **REG_TYPE:** `REG_DWORD`
  - **REG_NAME:** `EnableNetworkTroubleshooting`
  - **REG_VALUE:** 1 (Enabled)

  > **Note:**
  >
  > The Citrix Secure Access installer includes the packet capture utility along with all required

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> dependencies, so no separate installation is needed. This capability is supported with Enhanced Citrix Secure Access UI. For details, see 25.11.1.12.

For details, see Integrated packet capture tool for troubleshooting.

[CSACLIENTS-11581]

- **Custom workspace domain support for accessing TCP and UDP applications**

  Custom workspace domain support allows organizations to provide users with access to TCP and UDP apps through a branded, organization-owned domain (for example, workspace.company.com) instead of the default *.cloud.com domain. Admins can configure a custom domain as the authentication and access endpoint for apps accessed via Citrix Secure Private Access. End users benefit from a seamless, branded experience while organizations gain greater control over access and security.

  For details, see Configure a custom domain.

  [CSACLIENTS-13337]

- **Server name indication support in Citrix Secure Access**

  Citrix Secure Access supports Server Name Indication (SNI) by including the SNI header in every TLS connection it initiates. This enables accurate server identification during each TLS handshake.

  > **Note:**
  >
  > In Always-On strict mode (AlwaysOn = 2) deployments where the gateway is behind a GSLB configuration, Citrix Secure Access might not always connect to the same resolved IP address because of SNI-driven routing behavior. This can lead to intermittent authentication failures. For a seamless experience, ensure that all GSLB-resolved IP addresses for the gateway are included in the Always-On allow list, so connectivity remains consistent across IP address changes. For more details, see Always On.

  [CSACLIENTS-15566]

- **Support for honoring SkipDNE changes during Citrix Secure Access upgrades**

  Citrix Secure Access now provides full support for WFP-only configurations during both upgrades and downgrades when the SkipDNE flag is enabled.

  To enable this behavior, admins must configure the following registry:

  - **REG_PATH:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **REG_TYPE:** `REG_DWORD`
  - **REG_NAME:** `SkipDNE`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **REG_VALUE:** 1 (Enabled)

[CSACLIENTS-16221]

- **Real-time control of application access on device posture change**

  The Citrix Secure Access client for Windows now enforces real-time application access updates when device posture changes during an active VPN session.

  When the Device Posture service detects a change in the endpoint security posture, Citrix Secure Access automatically refreshes its configuration, determines which applications are affected, notifies the user with a countdown timer, and then either gracefully revokes access to denied applications or disconnects the session if all applications are denied.

  To enable continuous device posture, follow the registry setting:

  - **REG_PATH:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
  - **REG_TYPE:** `REG_DWORD`
  - **REG_NAME:** `EnableContinousPosture`
  - **REG_VALUE:** 1 (Enabled)

  > **Note:**
  >
  > Recommended EPA version : 26.3.1.10

  [CSACLIENTS-16386]

- **Client version control using the client app management service for Secure Private Access hybrid deployments**

  Citrix Secure Access now supports versioning control via Global Application Configuration Service (GACS) integration for Secure Private Access hybrid deployments.

  For details, see Citrix Secure Access.

  [CSACLIENTS-16581]

- **Support for user logout and gateway switching in Always On VPN mode**

  Always On VPN mode with client control configuration in the Citrix Secure Access app now supports user logout while keeping the machine tunnel active for uninterrupted device connectivity. After logging out of the user tunnel, users can log in again to establish a new user tunnel and, if needed, switch gateways (Secure Private Access or on-premises) to connect to a different endpoint.

  To enable this feature, admins must configure the following registry entry:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **REG_PATH:** `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`
- **REG_TYPE:** `DWORD`
- **REG_NAME:** `ClientControl`
- **REG_VALUE:** `1`

> **Note:**
>
> If the machine tunnel and user tunnel connect to different gateways (for example, Endpoint A for the machine tunnel and Endpoint B for the user tunnel), ensure that Endpoint B is reachable through Endpoint A when DNS queries are routed over the machine tunnel. Additionally, make sure that Endpoint B is excluded from Endpoint A's tunnel range and application access list to prevent routing conflicts and allow the user tunnel to establish successfully.

[CSACLIENTS-16215]

Fixed issues

- During Wi-Fi transitions, such as switching from Wi-Fi A to Wi-Fi B, Citrix Secure Access UI remains in an "unreachable"state, though there is no impact on application access. The UI glitch is only applicable to the Enhanced Citrix Secure Access UI.

  [SPAHELP-681]

- Citrix Secure Access operating in non-Edge WebView mode (also known as IE WebView mode) fails to authenticate with gateway after upgrading NetScaler to version 13.1.62.x or 14.1.66.x, and throws JavaScript errors. This issue is not observed when Citrix Secure Access operates in Edge WebView mode.

  [NSHELP-42599]

- In a global server load balancing (GSLB) setup, establishing a Citrix Secure Access client session from the browser might fail if the HttpOnly cookie, CSP header, and HSTS features are enabled on NetScaler.

  [NSHELP-42881]

- The IPv6 loopback traffic is blocked, and applications that rely on IPv6 loopback may fail or behave unexpectedly when both of the following conditions are met:

  - Split Tunnel is set to Off
  - Citrix Secure Access is connected in WFP mode with IPv6 disabled (default behavior)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-40659]

- When Citrix Secure Access is configured to operate in the Windows Filtering Platform (WFP) mode, Windows Firewall inbound rules do not apply to the tunneled traffic.

  [NSHELP-42539]

- In Always-On machine tunnel deployments, the Citrix Secure Access client might fail to re-establish the tunnel after a session timeout or transient network disruption during re-authentication. This occurs particularly during or after sleep mode, or when connectivity is restored.

  [NSHELP-41657]

- The VPN traffic is dropped when Intranet IP address is configured on NetScaler and the Citrix Virtual Adapter is disabled or not installed.

  [NSHELP-42377]

- In the Windows Filtering Platform (WFP) mode, Citrix Secure Access blocks the injection of third-party signed DLLs into the Citrix Secure Access application, even if the signer is listed in the ExternalTrustedSigner registry. To troubleshoot the issue, see Troubleshooting failures in the Citrix Secure Access client for Windows.

  [NSHELP-42177]

- The Citrix Secure Access Cleanup Utility might fail to remove the Citrix Virtual Network Adapter, leaving a residual adapter on the endpoint. This leftover adapter can block the automated installation of the new Citrix Secure Access version, requiring manual intervention on affected devices. This issue is fixed in the Cleanup Utility version 25.11.1.1.

  [NSHELP-41610]

- Tunneling interruptions might be seen if the VPN session is active for several days depending on the volume and type of network traffic.

  [NSHELP-41648]

- On workgroup machines, the firewall profile on Citrix Virtual Adapter might be incorrectly classified as a Public Profile instead of the intended Domain Profile.

  [NSHELP-42223]

- Application access through Citrix Secure Access might fail if the local network subnet overlaps with the intranet application subnet and an Intranet IP address (IIP) is not configured.

  [NSHELP-40642]

- Installing Citrix Secure Access enables TLS 1.1, even if it was previously disabled on the system.

  [NSHELP-41990]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DNS resolution might fail intermittently when spoofed IP range overlaps with the Intranet IP range.

  [NSHELP-41603]

- Upgrading Citrix Secure Access via NetScaler from version 25.11.1.12 to a higher version prompts for administrator approval causing upgrade to fail for non-admin users.

  [CSACLIENTS-16569]

26.3.1.5 (Mar 26, 2026)

Fixed issues

- When the hide UI feature is enabled with an Always On deployment, Citrix Secure Access does not relaunch automatically after the user exits it manually.

  For information on the hide UI feature, see **Enhanced Always On mode user experience** in the 25.11.1.12 release notes.

  [SPAHELP-669]

- When installing the Citrix Secure Access client using the MSI installer, a "Files in use"warning might appear, which halts the installation process. This issue is observed only when enhanced UI (EnableWebModuleUI registry) is enabled on Citrix Secure Access.

  [SPAHELP-652]

- When authenticating with a smart card-backed key storage provider that is not supported by Citrix Secure Access, removal of the smart card might not trigger a user tunnel logout.

  With this fix, a new string registry key (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\smartCardProviders) is added that allows administrators to configure additional smart card providers via a semicolon-separated list.

  [NSHELP-42048]

- When Citrix Secure Access is configured to operate in the Windows Filtering Platform (WFP) mode with an Always On deployment over a machine tunnel, and strict mode is enabled, external (internet) access becomes unavailable.

  [NSHELP-40407]

26.1.1.9 (Feb 10, 2026)

What's new

- **Seamless gateway updates for hybrid data path**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access application enables the addition or removal of gateways within the Secure Private Access configuration without interrupting the active client sessions. For more information about hybrid data path, see Hybrid data path for Secure Private Access service.

[CSACLIENTS-16103]

- **User tunnel fallback for Always On VPN mode**

  The Citrix Secure Access client now includes a fallback mechanism for Always On VPN mode. If the machine tunnel fails to establish, the Citrix Secure Access client automatically attempts to form a user tunnel if the `UserTunnelFallbackEnabled` registry key is enabled.
  For more information, see NetScaler Gateway Windows VPN client registry keys.

  To enable this feature, admins must configure the following registry entry:

  - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** REG_DWORD
  - **REG_NAME:** UserTunnelFallbackEnabled
  - **REG_VALUE:** 1(Enabled)

  [CSACLIENTS-15978]

Fixed issues

- Citrix Secure Access displays the device posture screen to the end user during the single sign-on flow, even when the DisableWebViewForAutoLogon registry key is configured.

  [CSACLIENTS-16140]

- Users might experience failure in Avaya registration or delayed login when connected through the gateway.

  [SPAHELP-646]

- In rare cases, users might fail to access internal applications for Citrix Secure Access when application traffic is fragmented.

  [SPAHELP-607]

- In rare cases, when the Citrix Secure Access application is configured in Always On strict mode, users might experience delayed logins or login errors when the communication between the browser and the plug-in fails.

  [NSHELP-41787]

- When the Citrix Secure Access application is configured in Always On strict mode and if client control is enabled, users might fail to switch to other gateway URLs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-41703]

- DNS resolution failures might occur intermittently due to internal IP mapping overlaps between the spoofed range and the VPN adapter network.

  [NSHELP-41603]

- The Citrix Secure Access application might crash intermittently during frequent login or logout sequences in Secure Private Access hybrid deployment.

  [NSHELP-41681]

25.11.1.12 (Dec 08, 2025)

What's new

- **Enhanced user interface with Notification Center and integrated WebView**

  The Citrix Secure Access client now has an enhanced UI that introduces a **Notification Center** for streamlined alerts and an integrated WebView for improved client handling directly on their machine.

  To enable the new UI, admins must configure the following registry entry:

  - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** DWORD
  - **REG_NAME:** EnableWebModuleUI
  - **REG_VALUE:** 1

  [CSACLIENTS-14045]

- **Captive portal support within the Citrix Secure Access client**

  The Citrix Secure Access application now integrates captive portal login directly within the application. Users can complete authentication for captive portals without switching applications. This functionality is part of the new UI. To enable the new UI, admin must configure the `EnableWebModuleUI` registry. For more information, see NetScaler Gateway Windows VPN client registry keys.

  [CSACLIENTS-15230]

- **Enhanced security with anti-DLL protection**

  The anti-DLL protection helps protect the Citrix Secure Access client from unauthorized dynamic-link libraries (DLL) or untrusted modules. If such untrusted modules are injected, the Citrix Secure Access client detects these interventions and stops the modules from loading.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Also, if any untrusted or malicious DLL is detected during the Citrix secure access launch, it generates a notification and terminates the application launch.

To enable the anti-DLL injection security enhancement, admins must configure the following registry entry:

- **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- **REG_TYPE:** DWORD
- **REG_NAME:** EnableAntiDllProtection
- **REG_VALUE:** 1

[CSACLIENTS-14364]

- **Seamless login experience in the Citrix Secure Access client**
  - **Hidden login/logout script execution**

    The command prompt no longer flashes when login or logout scripts execute during Citrix Secure Access tunnel establishment or termination.

    To enable this behavior, admins must configure the following registry entry:

    - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **REG_TYPE:** DWORD
    - **REG_NAME:** HideLoginLogoutScriptsPrompt
    - **REG_VALUE:** 1
  - **Enhanced Always On mode user experience**

    The Citrix Secure Access client now completely hides the device posture or authentication screens when operating in Always On mode. This functionality is part of the new UI, which is enabled using the `EnableWebModuleUI` registry.

    In addition to the `EnableWebModuleUI` registry, admins must configure the following registry entry to enable this behavior:

    - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **REG_TYPE:** DWORD
    - **REG_NAME:** DisableWebViewForAutoLogon
    - **REG_VALUE:** 1

[SPAHELP-577]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Always On with only machine tunnel for Citrix Secure Private Access**

  The Citrix Secure Access client now supports an "only machine tunnel"configuration for Citrix Secure Private Access deployments.

  To enable only machine tunnel configuration, admins must configure the following registry:

  - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** DWORD
  - **REG_NAME:** AlwaysOnService
  - **REG_VALUE:** 1

  For more information, see Always On before Windows Logon.

  [CSACLIENTS-16046]

- **Client version control using Client app management**

  You can now automatically update and manage the Citrix Secure Access client version for end users of the Secure Private Access service using the Client app management.

  Prerequisites:

  - Admins must create the following registry entry in the Citrix Secure Access client:
    - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
    - **REG_TYPE:** DWORD
    - **REG_NAME:** EnableAdminConfigFetch
    - **REG_VALUE:** 1
  - Ensure that connectivity to the following endpoints is enabled for Citrix Secure Access:
    - https://gacs-discovery.cloud.com
    - https://gacs-config.cloud.com
    - https://downloadplugins.citrix.com [Auto-Update endpoint]
  - Verify that you have access to a Citrix Cloud account. If not, you can create an account from https://onboarding.cloud.com/. For more information, see Sign-up for Citrix Cloud.

  Configure Client app management for version control of the Citrix Secure Access client:

  1. Sign in to the Citrix Cloud portal and navigate to **Client app management > Citrix Secure Access**.
  2. From the list of configured store URLs, select the store for which you want to configure settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Navigate to **All Settings > Citrix Secure Access version**.
4. In the **Citrix Secure Access version** screen, select **Enabled** from the drop-down menu next to the required platform.
5. In the **Manage settings for Windows** screen, enable the following options:
    - **Update channel:**
        - **Release:** Select this option to control the client version of the production build.
        - **Beta:** Select this option to control the client version of the preview build.
    - **Choose how you want to update:**
        - **Update to latest version:** Select this option to update the client version for all the end users to the latest version. If you enable the **Beta** channel, only the latest version is available.
        - **Update to Specific Version:** Select this option to update the client version for all the end users to a specific version. When enabled, select the desired client version from the **Version** drop-down list, which displays the three latest client versions.
6. Click **Save draft > Yes > Save** to save your settings.
7. Click **Review unsaved setting(s)** to review the unsaved settings.
8. Review the changes and click **Publish Drafts > Publish** to publish your settings.

> **Note:**
>
> The settings are updated immediately to the Citrix Secure Access clients.

Related topics:

- Citrix Secure Access - Client app management
- NetScaler Gateway Windows VPN client registry keys
- Client management

[CSACLIENTS-14872]

Fixed issues

- Auto-login to the Citrix Secure Access client using Edge WebView fails if the user name or password contains UTF-8 encoded characters.

  [NSHELP-40865]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users might experience delay in connecting to NetScaler Gateway when the Citrix Secure Access client is operating in Always On strict mode.

  [NSHELP-40724]

- Administrators face challenges in troubleshooting Web Proxy AutoDiscovery (WPAD) issues due to unoptimized log and error reporting.

  [SPAHELP-597]

- Internet access fails when the Citrix Secure Access client has split tunneling enabled and the file-based proxy PAC is configured as the system proxy over the VPN tunnel. By default this feature is disabled.

  To enable this feature, admins must configure the following Windows registry:

  - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** REG_DWORD
  - **REG_VALUE:** 1
  - **REG_NAME:** DisableWpadProxyPacUsage

  [NSHELP-41128]

- Rarely, the Citrix Secure Access client in Always On mode fails to reestablish the VPN connection when a session timeout coincides with the machine resuming from sleep.

  [NSHELP-40822]

- When a machine tunnel is enabled, the login screen might briefly display an incorrect "connected"message while the tunnel is still being established.

  [NSHELP-40744]

- Active Directory users might be unable to log in to the Citrix Secure Access client when a machine tunnel with contextual access is enabled.

  [SPAHELP-614]

- Upgrade of the Citrix Secure Access client from versions 25.2.1.x or earlier to 25.7.1.x or later fails on older Windows operating systems prior to Windows 10 version 1709.

  [NSHELP-41054]

- The Citrix Secure Access icon intermittently fails to appear on the Windows credential screen when the Always On service mode is enabled.

  [SPAHELP-616]

- Ping to local DNS servers is blocked by the Citrix Secure Access client.

  [SPAHELP-605]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In rare cases, the Citrix Secure Access client might crash due to incorrect DNS handling.

  [NSHELP-41163]

25.9.1.5 (Sep 30, 2025)

> **Important update:**
>
> - Citrix Secure Access version 25.9.1.5 replaces 25.9.1.4 and is now generally available.

Fixed issues

- Connections to DNS servers and gateway IP addresses might fail if a non-standard DNS port (other than 53) is used.

  [CSACLIENTS-15404]

- In Citrix Secure Private Access hybrid deployments, Citrix Monitor overrides the update frequency configured by the administrator with default values.

  [CSACLIENTS-15441]

- In Citrix Secure Private Access hybrid deployments, Citrix Monitor shows incorrect immediate hop details.

  [CSACLIENTS-15100]

- The Citrix Secure Access client does not log out when the smart card is removed, even with the **Logout On Smart Card Removal** setting enabled on the VPN virtual server.

  [NSHELP-40615]

- The Citrix Secure Access client might crash while capturing diagnostic logs in Citrix Secure Private Access deployments.

  [CSACLIENTS-15376]

- The connection to the NetScaler Gateway virtual server might fail if a non-standard port (other than 443) is used. This issue occurs when the Citrix Secure Access client operates in Microsoft Edge WebView mode.

  [NSHELP-40594]

- After upgrading to version 25.5.1.15, the Citrix Secure Access client fails to launch. This issue occurs due to a failure in the initialization of dependent third-party libraries.

  [NSHELP-40516]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Secure Access client intermittently crashes during login while operating in Secure Private Access mode.

  [CSACLIENTS-15560]

- Users are repeatedly prompted for domain credentials after upgrading the Citrix Secure Access client to version 25.5.1.15 or later. This issue occurs when Windows domain join fails due to an error in DNS resolution.

  [NSHELP-40730]

- When connected in WFP mode, the Citrix Secure Access client crashes intermittently while tunneling TCP DNS traffic.

  [CSACLIENTS-15440]

- The Citrix Secure Access client fails to launch due to a case-sensitive path validation.

  [NSHELP-40819]

25.7.1.11 (Aug 13, 2025)

What's new

- **ARM64 support for the Citrix Secure Access client**

  The Citrix Secure Access application now supports ARM64 Windows devices. The installer automatically detects the system architecture and installs the appropriate ARM64 version. This allows users on the ARM64 Windows devices to access NetScaler Gateway and Citrix Secure Private Access.

  [CSACLIENTS-13377]

- **Enhanced DNS suffix handling for applications in Citrix Secure Private Access**

  Enhanced DNS suffix handling now ensures that only application domains that match the configured suffixes are securely tunneled through Citrix Secure Private Access, allowing other domains to access the internet directly.

  [CSACLIENTS-14669]

Fixed issues

- Users might experience intermittent auto-login failures in the Citrix Secure Access client when Windows Hello-based authentication is enabled on their devices. Users must manually launch the Citrix Secure Access client to establish connection to NetScaler Gateway.

  [SPAHELP-528]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Secure Access client fails to launch the login script intermittently when the IPv6 DNS server is active on the end-user device.

  [SPAHELP-521]

- Citrix Secure Access client users might experience connection delays of up to 30 seconds when accessing intranet applications. This issue occurs after a period of inactivity or hibernation.

  [SPAHELP-518]

- The Citrix Secure Access client might fail to auto-login on a Windows 11 version 24H2 machine when operating in Always On or Always On service mode.

  To fix this issue, admins must create the following registry entry:

  - **REG_PATH:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - **REG_TYPE:** DWORD
  - **REG_NAME:** EnableCsaAutoLaunch
  - **REG_VALUE:** 1

  [SPAHELP-511]

- The Citrix Secure Access client might fail to establish a VPN connection when a device resumes from standby. This issue occurs when a Hyper-V virtual switch is used as the primary external interface on the end-user device.

  [SPAHELP-451]

- The EPA periodic scan fails when the Citrix Secure Access client operates in WFP mode.

  [NSHELP-40557]

- Even with an active VPN connection, users might lose access to intranet applications due to DNS resolution failure. This failure occurs because the Citrix Secure Access client enforces the `nsapimgr -ys enable_vpn_dnstruncate_fix`=1 setting, even when it is disabled on NetScaler Gateway.

  [NSHELP-40413]

- When connected in WFP mode, the TCP connection download throughput over the tunnel is lower compared to DNE mode.

  [NSHELP-40363]

- The **Status** menu incorrectly displays that the VPN is connected, even when the end-user machine is already connected to the corporate network. This issue occurs when the Citrix Secure Access client operates in Always On service mode with location detection enabled.

  [NSHELP-40336]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Secure Access client fails to log in on a Windows 11 machine when the proxy server is configured using a script PAC file.

  [NSHELP-40331]

- The Citrix Secure Access client users experience intermittent login failures. This issue occurs in GSLB deployments when Always On strict mode is enabled.

  [NSHELP-40274]

- Auto-login might fail in the Citrix Secure Access client when Microsoft Edge WebView is enabled and a login schema other than "singleauth.xml"is configured on NetScaler Gateway.

  [NSHELP-40272]

- Auto-login for classic authentication fails in the Citrix Secure Access client versions 24.11.1.17 and later because the default Microsoft Edge WebView does not support classic authentication.

  With this fix, the Citrix Secure Access client allows reverting the default WebView to Internet Explorer WebView, which supports classic authentication. For more information, see Auto-login failure in the Citrix Secure Access client version 24.11.1.17 and above.

  [NSHELP-40164]

- The Citrix Secure Access client users might experience failed intranet application access due to DNS resolution errors. This issue occurs when both of the following conditions are met:

  - Local LAN access is enabled in the Citrix Secure Access client.
  - The DNS server's IP address is within the LAN subnet.

  [NSHELP-39741]

- The Citrix Secure Access client crashes intermittently when the tunnel is active.

  [SPAHELP-529]

25.5.1.15 (Jun 17, 2025)

Fixed issues

- Users might experience disruptions while accessing the applications if the DNS server is also used for other functionalities like Dynamic Host Configuration Protocol (DHCP) or traffic monitoring.

  [NSHELP-39427]

- The TLS handshake between the Citrix Secure Access client and NetScaler Gateway might fail, leading to VPN disconnection. This issue occurs when client certificate configuration on NetScaler Gateway is set to **Optional** and the client machine does not have a user certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-39865]

- The Citrix Secure Access client launches automatically upon Windows Hello login despite disabling the **Open homepage automatically** checkbox in the **Configuration** menu of the Citrix Secure Access client.

  [NSHELP-40033]

- Users experience a loss of access to both intranet and internet resources, with only the connection to the virtual server or NetScaler Gateway remaining intact. This issue occurs when both of the following conditions are met:

  - The user's device is connected to the intranet.
  - The Citrix Secure Access client is operating in Always On strict mode with WFP mode enabled.

  [NSHELP-39996]

- The Citrix Secure Access client crashes intermittently during the Dynamic DNS (DDNS) registration of the assigned IIP address.

  [NSHELP-40120]

- Intermittent DNS failures occur in the Citrix Secure Access client when reverse split tunneling is enabled. For more information, see Reverse split tunneling of non-configured domains.

  [NSHELP-40102]

25.4.1.9 (May 08, 2025)

What's new

- **Support for multi-workspace URLs**

  The Citrix Secure Access client now supports the multi-workspace URL feature for Secure Private Access service deployments.

  [CSACLIENTS-13276]

Fixed issues

- Auto-login to the Citrix Secure Access client might fail if the user name or password for LDAP authentication contains special characters.

  [NSHELP-39664]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Auto-login to the Citrix Secure Access client with Edge WebView fails when advanced authentication is configured using the default login schema that has the logon button ID set to "Logon" .

  [NSHELP-39607]

- Auto-login to the Citrix Secure Access client might fail when the end user's device is running in Always On strict mode, that is, Always On is set to 2.

  Include the loopback address `127.0.0.1; loopback` in the `AlwaysOnAllowlist` to enable auto-login in Always On strict mode.

  [NSHELP-39428]

- The device certificate scan might fail when the EPA client is installed and run in standalone mode.

  [NSHELP-39167]

- With the Device posture service enabled, users might be prompted to run the EPA client each time they connect to a Citrix Workspace™ URL using the Citrix Secure Access client.

  [CSACLIENTS-14191]

- The automatic update of the Citrix Secure Access client might not function without a system restart after configuring the EnableAutoUpdate registry to enable auto-update functionality.

  [CSACLIENTS-14127]

25.2.1.18 (Apr 09, 2025)

What's new

- **Single sign-on support with Windows Hello based login**

  The Citrix Secure Access client now supports single sign-on in Always On mode when Windows Hello-based login is enabled on the end user's device, in both Citrix Secure Private Access and NetScaler Gateway deployments.

  [CSACLIENTS-13223]

- **Support for hostname-based application access over UDP in Secure Private Access**

  The Citrix Secure Access client now supports hostname-based application access over UDP within a machine-level tunnel, when operating in Secure Private Access mode.

  [CSACLIENTS-13215]

- **Support for hostname-based application access with DTLS enabled**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access client now supports IP address spoofing for TCP and UDP-based DNS requests, enabling hostname-based application access when DTLS is configured in NetScaler Gateway.

[CSACLIENTS-9797]

- **Enhanced plug-in upgrade behavior in the EPA client**

  The EPA client now prevents prompts for downgrading to a lower version when a higher version of the EPA client is detected on the end-user device. This functionality is applicable irrespective of the **Windows EPA Plugin Upgrade** configuration (**Always**, **Essential**, or **Never**) in NetScaler Gateway. This enhancement ensures that the end-user device always runs the latest version of the EPA client, maintaining security and stability.

  [AAUTH-6718]

Fixed issues

- In an on-premises deployment, the Citrix Secure Access client might fail to establish a VPN connection when two-factor authentication is enabled.

  [NSHELP-39382]

- In an on-premises deployment, DNS resolution for hostname-based access might return a single IP address in response to the DNS query sent to NetScaler Gateway for resolution. This issue occurs even if the DNS can resolve to multiple IP addresses.

  [NSHELP-39332]

- When the machine-level tunnel is enabled on the Citrix Secure Access client, the connection to the NetScaler Gateway virtual server might fail if a non-standard port (other than 443) is used.

  [NSHELP-39331]

- DNS resolution might fail when the Citrix Secure Access client tries to connect to an intranet IP address. This issue occurs if the DNS server is not configured on the NetScaler Gateway virtual adapter.

  [NSHELP-39300]

- The Citrix Secure Access client in machine tunnel mode might fail to transfer the logon to another session when multiple sessions are available for transfer.

  [NSHELP-39279]

- Auto log in to the Citrix Secure Access client might fail when Local Security Authority is enabled.

  [NSHELP-39199]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The user tunnel establishment is delayed when Always On strict mode is enabled.

  [NSHELP-39033]

- The nglauncher of the EPA client might crash, and the device posture check might fail if the default language setting on the end-user machine includes non-English characters, such as å or ø.

  [AAUTHHELP-108]

- End users may lose access to intranet applications after a few hours of usage if the tunneling connection limit is reached, even though the actual number of connections is lower.

  [NSHELP-39814]

25.1.1.27 (Mar 21, 2025)

> **Important update:**
>
> - Citrix Secure Access version 25.1.1.27 replaces 25.1.1.11 and is now generally available.
> - Starting from the Citrix Secure Access version 25.1.1.27, Windows Filtering Platform (WFP) is enabled by default.

Fixed issues

- When a device resumes from standby, internet and intranet access through the Citrix Secure Access client might fail in Always On mode (when machine-level tunnel is in use).

  [NSHELP-39435]

- The Citrix Secure Access client might fail to establish a connection to a UDP application when multiple host names resolve to the same IP address in Secure Private Access mode.

  [SPAHELP-415]

- The Citrix Secure Access client does not automatically re-establish the VPN connection after a session is terminated due to inactivity. This issue occurs when the **Server Idle Session Timeout** is configured in Citrix Secure Private Access on Always On mode.

  [SPAHELP-413]

- The device certificate scan might fail when the EPA client is installed and run in standalone mode.

  [NSHELP-39167]

- The **Always On VPN before Windows Logon** configuration in the Citrix Secure Access client might fail to establish a VPN connection if client certificate-based authentication is configured.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-39141]

- The end users are prompted to download the plug-in even if the correct version of Citrix EPA is already installed. This issue occurs in the following conditions:
  - The HttpOnly cookie is enabled.
  - The **windowsEPAPluginUpgrade** parameter is set to **Always**.

  [AAUTH-6503]

24.11.1.17 (Dec 19, 2024)

> **Important update:**
>
> Starting from the Citrix Secure Access version 24.11.1.17, Microsoft Edge WebView is enabled by default. To disable the Microsoft Edge WebView, contact Citrix Support. For more information, see Microsoft Edge WebView support for Windows Citrix Secure Access.

What's new

- **Support for contextual access feature in Secure Private Access**

  The Citrix Secure Access client supports the contextual access feature that enables an admin to enforce ZTNA policies dynamically based on the user context like network location, geo location, and device posture. Admin can enable this feature using the `EnableContextualAccess` registry or by contacting Citrix Support. For more information, see NetScaler Gateway Windows VPN client registry keys.

  [CSACLIENTS-11429]

- **Citrix Secure Access client installer included in the VDA meta installer**

  The Citrix Secure Access client installer is now integrated with the VDA meta installer in Citrix Virtual Apps and Desktops 7 2411. This enhancement allows the admin to install the Citrix Secure Access client for Windows as part of the VDA installation process. For more information, see the Install VDA documentation.

  [CSACLIENTS-11234]

- **Enhanced Windows Last Update scan to support category-wise scans**

  The Windows Last Update scan output includes category-wise list of **Security updates**, **Critical updates**, **Definition updates**, and **Update rollups**. Previously, the Windows Last Update scan included only the generic updates. For more information, see Windows Last Update Scan.

  [AAUTH-5528]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enhanced troubleshooting with multi-session VDA**

  The Citrix Secure Access client now supports notifications for each user in a multi-session VDA environment. For admins, events from multi-session VDA are available in DaaS Monitor.

  [CSACLIENTS-11449]

- **Auto login support with Windows Hello based login**

  The Citrix Secure Access client now supports automatic launch and login when Windows Hello based login is enabled on the end user's device.

  [CSACLIENTS-12330]

- **Automatic update support for the Citrix Secure Access client**

  The Citrix Secure Access client can now automatically update the Windows client to the latest available version. This feature is not enabled by default. The admin can enable this feature and choose which machines must automatically get updates for either the early access build or the production build using the registries `EnableAutoUpdate` and `IsAutoUpdateControlledViaAdmin`. For more information, see NetScaler Gateway Windows VPN client registry keys.

  > **Note:**
  >
  > Because the automatic update feature is introduced in the Citrix Secure Access client for Windows version 24.11.1.17, administrators can use this feature in the subsequent releases.

Fixed issues

- The Microsoft Edge WebView might fail to load while logging in to the Citrix Secure Access client for Windows. The error message "Your machine doesn't have Microsoft Edge runtime installed" might appear even though it is already installed.

  [SPAHELP-352]

- The Citrix Secure Access client on Windows 11 machine fails to establish a DTLS connection to NetScaler Gateway.

  [NSHELP-38800]

24.10.1.5 (Nov 08, 2024)

Fixed issues

- In Secure Private Access mode, hostname-based application access might fail when a device resumes from standby.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[SPAHELP-355]

- When a device resumes from standby, the Citrix Secure Access client for Windows might occasionally take more than 60 seconds to activate and connect.

  [SPAHELP-350]

- The Citrix Secure Access client for Windows fail to establish a VPN connection to NetScaler Gateway when the Server Name Indication (SNI) is enabled.

  [NSHELP-38813]

- Users cannot establish a VPN connection due to SSL renegotiation failure when the session ticket parameter is enabled on NetScaler Gateway.

  [NSHELP-38793]

- Users cannot establish a VPN connection if there was a network failure during the previous logout process.

  [NSHELP-38791, NSHELP-38641]

- The `nsRmSac.exe` cleanup utility of the Citrix Secure Access client requires manual intervention to run on the end user's device. For more information, see Completely skip the DNE installation.

  [NSHELP-38711]

- After logging out of the VPN, localhost communication might fail if one of the network adapters on the machine is using the loopback address as the DNS server. As a result, when users attempt to log back into the VPN through the browser, they might be prompted to download the EPA plug-in again (if EPA is configured as an authentication factor), even if it is already installed.

  [NSHELP-38427]

- The custom redirection might fail when the user logs into the NetScaler® Gateway virtual server using the Citrix Secure Access client for Windows.

  [NSHELP-38382]

24.8.1.19 (Oct 10, 2024)

> **Important update:**
>
> Citrix Secure Access version 24.8.1.19 replaces 24.8.1.15 and is now generally available.

What's new

- **Secure Private Access support for cloud-hosted multi-session VDI**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access client now supports the use of Secure Private Access to achieve zero trust access to corporate resources from cloud-hosted multi-session VDIs. Admin can enable this feature using the `EnableMultiSessionFlow` registry. For domain-joined machines, use both `EnableMultiSessionFlow` and `AlwaysOnService` registries. For more information, see NetScaler Gateway Windows VPN client registry keys.

[CSACLIENTS-10642]

- **Continuous device posture assessment for active Secure Private Access applications**

  When you enable the **Periodic scan** setting in the Device Posture Service, EPA client scans the device every 30 minutes. If it detects a downgrade in posture status, it notifies the user and disconnects active Secure Private Access connections through the Citrix Secure Access client. For more information, see Periodic scanning of devices.

  [AAUTH-4910]

- **Support to exclude DNS traffic by Citrix Secure Access**

  You can now exclude DNS traffic from being intercepted by Citrix Secure Access client. For more information, see Exclude specific domain traffic from client interception.

  [CSACLIENTS-10347]

- **Always On location detection support for Secure Private Access**

  Citrix Secure Access for Windows supports the location detection feature for the Secure Private Access service. It connects the user's machine to the VPN session if it is not in the corporate network and disconnects the user's VPN session if the machine is in the corporate network. You must use the locationDetection registry and configure the DNS suffix on the Secure Private Access admin UI console to enable the location detection feature.

  For more information on using the registry, see NetScaler Gateway Windows VPN client registry keys.

  For more information on configuring the DNS suffix, see DNS suffixes to resolve FQDNs to IP addresses.

  [CSACLIENTS-8783]

- **Auto log on support for Azure Entra ID**

  Citrix Secure Access supports auto-logon for Azure AD joined machines and hybrid Azure AD joined machines using Primary Refresh Tokens (PRT) mechanism for both NetScaler Gateway and Secure Private Access. For more information, see Citrix Secure Access auto logon for Windows Azure AD joined machines.

  [CSACLIENTS-10595]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Support to triage and troubleshoot enumeration failures**

  Citrix Secure Access now supports triaging and troubleshooting enumeration failures using Citrix Monitor or Citrix Director, in Secure Private Access deployments. For more information, see Secure Private Access integration with Director (Preview).

  [CSACLIENTS-10751]

- **Enhanced Windows Last Update scan**

  The Windows Last Update scan now checks the Windows Updates installed through Windows Auto Upgrade service and also the updates installed via BigFix, Intune, and other third party tools. For more information, see Advanced Endpoint Analysis scans.

  [AAUTH-4876]

- **Split DNS support for TCP-based DNS requests**

  Citrix Secure Access supports split DNS for TCP based DNS requests, same as UDP based DNS requests. Admin can enable this feature using the `EnableTCPDNS` registry. For more information, see Session policies and NetScaler Gateway Windows VPN client registry keys.

  [CSACLIENTS-8142]

- **Enhanced client certificate authentication**

  During client certificate authentication, Citrix Secure Access automatically selects the client certificate based on the CA certificates configured on NetScaler Gateway. For more information, see Configuring Client Certificate Authentication.

  [CSACLIENTS-10592]

- **Support for Citrix Secure Private Access™ for on-premises**

  Citrix Secure Access now supports Citrix Secure Private Access for on-premises. For more information, see Citrix Secure Access client.

  [CSACLIENTS-10543]

Fixed issues

- Citrix Secure Access client does not display the correct error message on the Windows Credential Provider screen if the authentication fails due to an unreachable network.

  [SPAHELP-333]

- The Citrix Secure Access client UI fails to display the custom messages configured using the NetScaler Gateway RfWebUI portal theme.

  [NSHELP-38362]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DNS traffic is dropped if the DNS suffix applied to the Citrix Virtual Adapter (connected to Citrix Secure Access) is truncated after 15 characters. This issue occurs because NetScaler Gateway treats the DNS suffix as a NetBIOS name.

  [NSHELP-37990]

- Citrix Secure Access client generates high DNS traffic when an user accesses multiple applications over the VPN tunnel.

  [NSHELP-37822]

24.6.1.18 (Jul 24, 2024)

> **Important update:**
>
> Citrix Secure Access version 24.6.1.18 replaces 24.6.1.17 and is now generally available.

What's new

- **EPA scan to check Citrix Workspace app version**

  Citrix Secure Access supports a new EPA scan "CWA Version", that verifies the Citrix Workspace version on Windows machines. For details about the supported EPA scans, see Expression strings.

  [AAUTH-4870]

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

  Citrix Workspace app offers a unified client management experience for Citrix Secure Access. When users log on to Citrix Workspace app, they are automatically signed on to Citrix Secure Access and can access TCP/UDP applications seamlessly without the need to manually configure and sign in to multiple client applications. For details, see Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for Windows - Preview.

  [CSACLIENTS-6418]

- **Tunnel exclusion support in Secure Private Access**

  Citrix Secure Access can now exclude certain application traffic from being tunneled by using the registry, `ExcludeDomainsFromTunnel`.

  If `example.com` is an intranet domain that hosts multiple applications, and you want to exclude specific applications such as `sshhost.example.com`, `rdphost.example.com`, `*.ftphost.example.com`, you can use this registry.

  For details, see NetScaler Gateway Windows VPN client registry keys.

  [CSACLIENTS-8972]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **IP address spoofing for TCP-based DNS requests**

  Citrix Secure Access supports IP address spoofing of TCP-based DNS requests in the following scenarios:

  - FQDN-based tunneling rules are configured on NetScaler Gateway.
  - FQDNs match the DNS suffixes in a Citrix Secure Private Access deployment.

  [CSACLIENTS-8328]

- **Interoperability enhancements with third-party secure web gateway**

  The User-Agent strings for Citrix Secure Access have been updated for enhanced interoperability with third party secure web gateways.

  [CSACLIENTS-8593]

- **Support for Citrix Secure Private Access for on-premises**

  Citrix Secure Access now supports Citrix Secure Private Access for on-premises.

  [CSACLIENTS-10543]

- **Enhanced EPA scan encryption**

  The security encryption of EPA scans is enhanced by the Elliptic Curve Diffie-Hellman (ECDH) keys.

  [CSACLIENTS-8308]

- **Hash key for signature creation**

  Admins can now use the SHA-384 hash key to create signatures for device certificate authentication.

  [CSACLIENTS-8296]

- **Seamless connectivity during POP failure**

  In a Secure Private Access deployment, VPN users are automatically reconnected to a different Point of Presence (POP) without manual intervention, when connectivity to the current POP fails.

  [CSACLIENTS-6396]

- **Enhanced diagnostics**

  The Citrix Secure Access diagnostics are enhanced with additional fields that can help troubleshoot access issues with TCP/UDP apps.

  [CSACLIENTS-8335]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- DNS resolution fails on Windows 11 devices if the Windows Management Instrumentation Command-line (WMIC) feature is disabled.

  [NSHELP-37603]

- Citrix Secure Access blocks IPv6 traffic from being routed over a loopback interface if reverse split tunneling and intranet IP address are configured on NetScaler Gateway.

  [NSHELP-37096], [NSHELP-37534]

- Citrix Secure Access crashes if the IP address range of the intranet application is configured with a wildcard subnet mask.

  [NSHELP-37788]

- After an upgrade, users cannot connect to Microsoft applications if reverse split tunneling and intranet IP addresses are configured on NetScaler Gateway.

  [NSHELP-37876]

- When Citrix Secure Access client is configured with WFP, VPN connectivity is lost during an active session or when multiple logins and logouts happen.

  [NSHELP-37881]

- DNS resolution is delayed when applications on the client machine send A and AAAA record-type DNS queries.

  [NSHELP-38067]

- Kerberos authentication fails in a Citrix Secure Private Access deployment.

  [SPAHELP-286]

- In the Windows Filtering Platform (WFP) mode, application name of the intranet resource being accessed appears as **N/A** on the Secured Applications' connections tab on the Citrix Secure Access UI.

  [CSACLIENTS-9664]

- In a Citrix Secure Private Access deployment, Citrix Secure Access client fails to switch from machine-level tunnel to user-level tunnel if Always On is configured.

  [CSACLIENTS-9604]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

24.4.1.7 (Apr 30, 2024)

Fixed issues

End-users cannot log on to Citrix Secure Access when autologon fails in the Microsoft Edge WebView mode.

[CSACLIENTS-10005]

DNS resolution fails for some backend resources when the AAAA record-type DNS queries are sent by the client application.

[SPAHELP-288], [CSACLIENTS-10460]

Citrix Secure Access might fail to establish new connections in the WFP driver mode if the client runs for several hours.

[NSHELP-37427], [NSHELP-37124], [SPAHELP-280]

Citrix Secure Access displays an EPA scan error message of a device certificate failure in a different language, although the language set is English.

[NSHELP-37477]

Internet and intranet connections might be lost after a prolonged VPN session if Always On VPN is configured in the WFP mode.

[NSHELP-37283]

EPA scan fails when the "filetime"parameter is configured.

[NSHELP-37564]

The MD5 checksum configuration of a file fails during an EPA scan.

[NSHELP-37491]

The Windows credential manager screen displays the Citrix Secure Access icon even though VPN is not in the Always On VPN mode.

[NSHELP-37205]

The Citrix Secure Access logs display the IP addresses in reverse order. For example, if a Microsoft Edge browser is connected to NetScaler (IP: 192.20.4.5:24), the log message appears as,

```
"Application msedge.exe has opened a connection to 5.4.20.192:24 |
Making a connection to 5.4.20.192:24 by msedge.exe |"
```

[NSHELP-37314]

After an upgrade, when users click the **Home page** button on the Citrix Secure Access GUI, the home page URL fails to launch on the default browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-37659]

The device certificate check fails in a Citrix Secure Private Access deployment if the certificate is signed by an intermediate CA instead of the root CA.

[SPAHELP-287]

24.2.1.15 (Mar 04, 2024)

What's new

- **Support for SNI**

  In a Citrix Secure Private Access deployment, Citrix Secure Access client now supports the server name indication (SNI) extension on all the pre-authentication requests.

  [SPAHELP-236]

- **Support for TLS 1.3**

  Citrix Secure Access client now supports the TLS 1.3 protocol. TLS 1.3 is supported on the following platforms:

  - Windows 11 and later
  - Windows Server 2022 and later

  For details on how to configure TLS 1.3 on NetScaler, see Support for TLS 1.3 protocol.

  [CSACLIENTS-6106]

- **Support for Windows OS details in the HTTP header**

  Citrix Secure Access client now includes details of the Windows OS as part of the HTTP header (user-agent) string.

  [NSHELP-36732]

Fixed issues

- DNS resolution intermittently fails if IPv6 is enabled on the client network adapter.

  [NSHELP-35708]

- Users might not be able to log on to Citrix Secure Access client if there are simultaneous login attempts using autologon.

  [NSHELP-35768]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Secure Access installation fails when Smart App Control is enabled on non-English client machines.

  [NSHELP-36126], [NSHELP-36907]

- Users cannot access some applications through VPN if Citrix Secure Access client is configured with the WFP driver. This issue occurs because of modifications to the firewall policies.

  [NSHELP-36254], [NSHELP-36312]

- A popup dialog appears during an EPA scan. However, when the user clicks OK, EPA scan works as usual. This issue occurs when the Swedish language is selected (**Configuration > Language**) on the Citrix Secure Access client UI.

  [NSHELP-36408]

- In an Always On VPN mode, the machine level tunnel fails to transfer the session when the user certificate authentication is configured on NetScaler Gateway.

  [NSHELP-36492]

- Access to the intranet resources intermittently fails when the Windows Filtering Platform (WFP) driver is enabled on Citrix Secure Access client.

  [NSHELP-36568]

- The Citrix Secure Access client UI page intermittently freezes when users click the Home button.

  [NSHELP-37046]

- Non-admin users cannot connect to the full VPN tunnel if the following conditions are met:

  - EPA is configured as a factor in an nFactor flow.
  - Edge WebView is enabled.
  - The control upgrade setting of Citrix EPA client is set to **Always** on NetScaler Gateway and there's a mismatch in the Citrix EPA client versions between the client device and NetScaler.

  [NSHELP-37340]

- EPA device certificate scan fails if the client machine's system certificate store contains only one device certificate.

  [NSHELP-37371]

- The login page of Citrix Secure Access client intermittently goes blank when connecting to Citrix Secure Private Access service.

  [SPAHELP-202]

- End-users might not be able to connect the client machines to the domain through VPN if Windows Server 2019 or later versions are used.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[SPAHELP-219]

- When Citrix Device Posture service is enabled, unwanted entries appear in the **Connection** drop-down list of the Citrix Secure Access client UI.

  [SPAHELP-271]

- End-users cannot access the intranet resources if the single sign-on feature is enabled on Citrix Secure Access client.

  [CSACLIENTS-9940]

- Citrix Secure Access might crash due to memory corruption.

  [NSHELP-36993]

23.10.1.7 (29-Nov-2023)

What's new

- **Configure private port range for server initiated connections**

  You can now configure a private port ranging from 49152 to 64535 for server-initiated connections. Configuring private ports avoids conflicts that might arise when you use ports to create sockets between Citrix Secure Access client and third party apps on the client machines. You can configure the private ports by using the "SicBeginPort"Windows VPN registry. Alternatively, you can configure the private port range by using a VPN plug-in customization JSON file on NetScaler.

  For more information, see Configure server-initiated connections and NetScaler Gateway Windows VPN client registry keys.

  [NSHELP-36627]

- **Kerberos authentication support for seamless autologon**

  Citrix Secure Access client now uses the Kerberos authentication method for autologon. As part of this support, a VPN client registry key "EnableKerberosAuth"is introduced. As a pre-requisite, admins must configure Kerberos authentication on NetScaler and on their client machines. End users must install Microsoft Edge WebView on their machines to enable the Kerberos authentication method. For more information, see Autologon with Kerberos authentication.

  [CSACLIENTS-3128]

- **Auto assign of spoof IP address range**

  Citrix Secure Access client can now detect and apply a new spoof IP address range if there is a conflict between the admin-configured spoof IP address range and the IP-based applications or the end-user's network.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[CSACLIENTS-6132]

- **Microsoft notifications**

  The Citrix Secure Access client notifications now appear as Microsoft notifications on the Notifications panel of your Windows machine.

  [CSACLIENTS-6136]

- **Improved log collection**

  The Verbose log level is now used as the default debug logging level for an enhanced log collection and troubleshooting. For more information about logging, see Configure logging by using the Citrix Secure Access client UI.

  [CSACLIENTS-8151]

Fixed issues

Citrix Secure Access client remains in the "Connecting"state if the machine tunnel of the Always On service fails to detect the client device location.

[CSACLIENTS-1174]

The transfer logon feature fails to work when Microsoft Edge WebView is enabled in Citrix Secure Access client.

[CSACLIENTS-6655]

In the Always On service mode, Citrix Secure Access client fails to establish a machine-level tunnel with NetScaler Gateway if the device certificate-based classic authentication policies are bound to a VPN virtual server.

[NSHELP-33766]

Incoming and outgoing Webex calls fail when users are connected to the VPN. This issue occurs when the Windows filtering platform (WFP) driver is enabled on Citrix Secure Access client instead of the Deterministic network enhancer (DNE) driver.

[NSHELP-34651]

Citrix Secure Access client crashes if the following conditions are met:

- Connections are switched when SAML policies are bound to a VPN virtual server.
- Internet Explorer WebView support is enabled.

[NSHELP-35366]

The Citrix Secure Access client UI displays the Connect button during autologon. This issue occurs if the UserCert authentication method is used to connect to VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-36134]

The local LAN access feature fails to work with Citrix Secure Access client if a machine-level tunnel is configured.

With this release, the local LAN access feature can be set with a machine-level tunnel configuration. To achieve this, you must configure the local LAN access parameter to FORCED when using the machine tunnel mode. For more details, see Enforce local LAN access to end users based on ADC configuration.

[NSHELP-36214]

When a client machine wakes up from sleep mode multiple times, Citrix Secure Access client fails to establish a VPN connection with the intranet applications.

[NSHELP-36221]

23.8.1.11 (19-Oct-2023)

Fixed issues

The epaPackage.exe file might fail to download if forward proxy support is configured on NetScaler Gateway.

[CSACLIENTS-6917]

The Citrix EPA client installation fails for non-admin users with restricted access to C drive.

[NSHELP-36590]

23.8.1.5 (09-Aug-2023)

Fixed issues

Kerberos SSO fails for applications when connected over Citrix Secure Private Access service.

[CSACLIENTS-912]

Application access with Citrix Secure Private Access service fails intermittently. This issue occurs when Citrix Secure Access client shares an incorrect destination IP address for TCP or UDP traffic.

[CSACLIENTS-1151, CSACLIENTS-6326]

Citrix Secure Access client fails to launch applications intermittently because of a DNS caching issue.

[CSACLIENTS-1170]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access client fails to apply a DNS suffix to Citrix Virtual Adapter. This issue occurs when Citrix Virtual Adapter fails to authenticate with Active Directory.

[NSHELP-33817]

Citrix Secure Access client crashes if the following conditions are met:

- NetScaler Gateway virtual server contains a client certificate as a factor for nFactor authentication.
- Microsoft Edge WebView support is enabled.

[CSACLIENTS-6171]

When connected to VPN, you might not be able to access back-end resources after you apply Microsoft KB5028166.

[NSHELP-35909]

Citrix Secure Access client intermittently fails to download the configurations from NetScaler Gateway when the portal customization exceeds the allowed limit.

[NSHELP-35971]

Known issues

The transfer logon feature fails to work with Citrix Secure Access client. This issue occurs when Microsoft Edge WebView is enabled.

Workaround: Log on using a web browser to transfer the session.

23.7.1.1 (14-Jul-2023)

Fixed issues

In some cases, after an upgrade to the release version 23.x.x.x, traffic fails to pass through the VPN tunnel, resulting in blocking of VPN access when an Intranet IP range is configured on NetScaler. This happens when cross profile firewall rule is not applied to VPN applications.

[NSHELP-35766]

23.5.1.3 (02-Jun-2023)

Fixed issues

The Always On service crashes when the improved log collection is enabled using the "useNewLogger" registry under `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[CGOP-24462]

23.4.1.5 (14-Apr-2023)

What's new

- **Microsoft Edge WebView support**

  Microsoft Edge WebView support on Citrix Secure Access client for Windows introduces an enhanced end user experience. This feature is disabled, by default. For details, see Microsoft Edge WebView support for Windows Citrix Secure Access.

  [CGOP-22245]

- **Adding DNS suffixes to resolve FQDNs to IP addresses**

  Admins can now add suffixes to the applications at the operating system level. This helps Citrix Secure Access clients to resolve a non-fully qualified domain name during name resolution.

  Admins can also configure applications using the IP addresses (IP CIDR/IP range) so that the end users can access the applications using the corresponding FQDNs. For details see, DNS suffixes to resolve FQDNs to IP addresses.

  [ACS-2490]

- **Improved log collection**

  The logging feature for the Windows Secure Access client is now improved for log collection and debugging. The following changes are made to the logging feature.

  - Enable users to change the maximum log file size to a value less than 600 MB.
  - Enable users to update the number of log files to less than 5.
  - Increase the log levels to three for the new logging feature.

  With these changes, admins and end-users can collect logs from the current session and past sessions. Previously, collection of logs was limited to the current sessions only. For details see, Improved log collection for Windows client.

  > **Note:**
  >
  > To enable debug logging, select **Logging > Verbose** from the **Select Log Level** drop-down list. Prior to the Citrix Secure Access client for Windows 23.4.1.5 release, debug logging could be enabled using the **Configuration > Enable debug logging** check-box.

  [CGOP-23537]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Support for sending events to Citrix Analytics service**

  Citrix Secure Access client for Windows now supports sending events such as session creation, session termination, and app connection to Citrix Analytics service. These events are then logged in Citrix Secure Private Access dashboard.

  [SPA-2197]

Fixed issues

- Citrix Secure Access client single sign-on authentication with Citrix Workspace app to cloud endpoint fails for Unicode users.

  [CGOP-22334]

- Access to the resources fails when host name-based applications are configured along with DNS suffix in Citrix Secure Private Access.

  [SPA-4430]

- Always-On VPN connection fails intermittently on startup due to gateway virtual server reachability issue.

  [NSHELP-33500]

- Intranet resources overlapping with a spoofed IP address range cannot be accessed with split-tunnel set to OFF on the Citrix Secure Access client.

  [NSHELP-34334]

- Citrix Secure Access client fails to load the authentication schema leading to login failure in Citrix Secure Private Access service.

  [SPAHELP-98]

23.1.1.11 (20-Feb-2023)

This release addresses issues that help to improve the overall performance and stability of Citrix Secure Private Access service.

23.1.1.8 (08-Feb-2023)

Fixed issues

- DNS resolution failures occur as the Citrix Secure Access fails to prioritize IPv4 packets over IPv6 packets.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-33617]

- The OS filtering rules are captured when the Citrix Secure Access client is running in Windows Filtering Platform (WFP) mode.

  [NSHELP-33715]

- Spoofed IP address is used for IP-based intranet applications when the Citrix Secure Access client runs on Citrix Deterministic Network Enhancer (DNE) mode.

  [NSHELP-33722]

- When using the Windows Filtering Platform (WFP) driver, sometimes intranet access does not work after the VPN is reconnected.

  [NSHELP-32978]

- Endpoint analysis (EPA) scan for OS version check fails on Windows 10 and Windows 11 Enterprise multi-session desktops.

  [NSHELP-33534]

- Windows client supports 64 KB configuration file size, by default, and this restricts the users to add more entries in the configuration file. This size can be increased by setting the `ConfigSize` registry value in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client. The `ConfigSize` registry key type is `REG_DWORD` and key data is <`Bytes size`>. If the configuration file size is larger than the default value (64 KB), then the ConfigSize registry value must be set to 5 x 64 KB (after converting to bytes) for every addition of 64 KB. For example, if you are adding additional 64 KB, then you must set the registry value to 64 x 1024 x 5 = 327680. Similarly, if you are adding 128 KB, then you must set the registry value to 64 x 1024 x (5+5) = 655360.

  [SPA-2865]

- On VPN logoff, DNS suffix list entries in SearchList registry are rewritten in a reverse order separated by one or more commas.

  [NSHELP-33671]

- Proxy authentication fails when the NetScaler appliance completes an EPA scan for antivirus.

  [NSHELP-30876]

- If the Citrix Secure Access related registry values are greater than 1500 characters, then the log collector fails to gather the error logs.

  [NSHELP-33457]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

22.10.1.9 (08-Nov-2022)

What's new

- **EPA support for connection proxy type site persistence in GSLB**

  Windows EPA scan now supports connection proxy type site persistence in GSLB when the scan is initiated from a browser. Previously, EPA scan for Windows did not support connection proxy persistence type for browser initiated EPA scan.

  [CGOP-21545]

- **Seamless single sign-on for Workspace URL (Cloud only)**

  Citrix Secure Access client now supports single sign-on for Workspace URL (cloud only) if the user has already logged on via the Citrix Workspace app. For more details, see Single sign-on support for the Workspace URL for users logged in via Citrix Workspace app.

  [ACS-2427]

- **Manage Citrix Secure Access client and/or EPA plug-in version via Citrix Workspace App (Cloud only)**

  Citrix Workspace app now has the capability to download and install the latest version of Citrix Secure Access and/or EPA plug-in via the Global App Configuration Service. For more details, see Global App Configuration Service.

  [ACS-2426]

- **Debug logging control enhancement**

  Debug logging control for Citrix Secure Access client is now independent of NetScaler Gateway and it can be enabled or disabled from the plug-in UI for both machine and user tunnel.

  [NSHELP-31968]

- **Support for Private Network Access preflight requests**

  Citrix Secure Access Client for Windows now supports Private Network Access preflight requests issued by the Chrome browser when accessing private network resources from public websites.

  [CGOP-20544]

Fixed issues

- The Citrix Secure Access client, version 21.7.1.1 and later, fails to upgrade to later versions for users with no administrative privileges.

  This is applicable only if the Citrix Secure Access client upgrade is done from a NetScaler appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[NSHELP-32793]

- Users cannot log on to VPN because of intermittent EPA failures.

  [NSHELP-32138]

- Sometimes, the Citrix Secure Access client in machine tunnel only mode does not establish the machine tunnel automatically after the machine wakes up from sleep mode.

  [NSHELP-30110]

- In Always on service mode, user tunnel tries to start even if only machine tunnel is configured.

  [NSHELP-31467]

- The Home Page link on the Citrix Secure Access UI does not work if Microsoft Edge is the default browser.

  [NSHELP-31894]

- Customized EPA failure log message is not displayed on the NetScaler Gateway portal, instead the message "internal error"is displayed.

  [NSHELP-31434]

- When users click the Home Page tab on the Citrix Secure Access screen for Windows, the page displays the connection refused error.

  [NSHELP-32510]

- On some client machines, the Citrix Secure Access client fails to detect the proxy setting and this results in logon failure.

  [SPAHELP-73]

Known issues

- Windows Update check-based EPA scan does not work on the Windows 11 22H2 version.

  [NSHELP-33068]

22.6.1.5 (17-June-2022)

What's new

- **Login and logout script configuration**

  The Citrix Secure Access client accesses the login and logout script configuration from the following registries when the Citrix Secure Access client connects to the Citrix Secure Private Access cloud service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Registry path: **HKEY_LOCAL_MACHINE>SOFTWARE>Citrix > Secure Access Client**

Registry values:

- SecureAccessLogInScript type REG_SZ - path to login script
- SecureAccessLogOutScript type REG_SZ - path to logout script

[ACS-2776]

- **Windows Citrix Secure Access client using Windows Filtering Platform (WFP)**

  WFP is a set of API and system services that provide a platform for creating network filtering application. WFP is designed to replace previous packet filtering technologies, the Network Driver Interface Specification (NDIS) filter which was used with the DNE driver. For details, see Windows Citrix Secure Access client using Windows Filtering Platform.

  [CGOP-19787]

- **FQDN based reverse split tunnel support**

  WFP driver now enables support for FQDN based REVERSE split tunneling. It is not supported with the DNE driver. For more details on reverse split tunnel, see Split tunneling options.

  [CGOP-16849]

Fixed issues

- Sometimes, the Windows auto logon does not work when a user logs into the windows machine in an Always On service mode. The machine tunnel does not transition to the user tunnel and the message **Connecting** is displayed in the VPN plug-in UI.

  [NSHELP-31357]

- On VPN logoff, the DNS suffix list entries in SearchList (Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ Access Client) registry are rewritten in reverse order separated by one or more commas.

  [NSHELP-31346]

- Spoofed IP address is used even after the NetScaler intranet application configuration is changed from FQDN based to IP based application.

  [NSHELP-31236]

- The gateway home page is not displayed immediately after the gateway plug-in establishes the VPN tunnel successfully.

  With this fix, the following registry value is introduced.

  \HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds

  Type: DWORD

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, this registry value is not set or added. When the value of "SecureChannelResetTimeoutSeconds"is 0 or not added, the fix to handle the delay does not work, which is the default behavior. Admin has to set this registry on the client to enable the fix (that is to display the home page immediately after the gateway plug-in establishes the VPN tunnel successfully).

[NSHELP-30189]

- AlwaysOnAllow list registry does not work as expected if the registry value is greater than 2000 bytes.

  [NSHELP-31836]

- Citrix Secure Access client for Windows does not tunnel new TCP connections to the back-end TCP server if the already connected Citrix Secure Private Access service region becomes unreachable. However, this does not affect the on-premises gateway connections.

  [ACS-2714]

22.3.1.5 (24-Mar-2022)

Fixed issues

- The Windows EPA plug-in name is reverted to the NetScaler Gateway EPA plug-in.

  [CGOP-21061]

Known issues

- Citrix Secure Access client for Windows does not tunnel new TCP connections to the back-end TCP server if the already connected Citrix Secure Private Access service region becomes unreachable. However, this does not affect the on-premises gateway connections.

  [ACS-2714]

22.3.1.4 (10-Mar-2022)

What's new

- **Enforce local LAN access to end users based on ADC configuration**

  Admins can restrict the end users from disabling the local LAN access option on their client machines. A new option, FORCED is added to the existing Local LAN Access parameter values. When the Local LAN Access value is set to FORCED, the local LAN access is always enabled for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

end users on the client machines. End users cannot disable the local LAN settings using the Citrix Secure Access client UI. If admins want to provide an option to enable or disable local LAN access to the end user, they must re-configure the Local LAN access parameter to ON.

To enable the **FORCED** option by using the GUI:

1. Navigate to **NetScaler Gateway > Global Settings > Change Global Settings**.
2. Click the **Client Experience** tab and then click **Advanced Settings**.
3. In **Local LAN Access**, select **FORCED**.

To enable the **FORCED** option by using the CLI, run the following command:

```
set vpn parameter -localLanAccess FORCED
```

[CGOP-19935]

- **Support for Windows server 2019 and 2022 in the EPA OS scan**

  EPA OS scan now supports Windows server 2019 and 2022.

  You can select the new servers by using the GUI.

  1. Navigate to **NetScaler Gateway > Policies > Preauthentication**.
  2. Create a new preauthentication policy or edit an existing policy.
  3. Click the **OPSWAT EPA Editor** link.
  4. In **Expression Editor**, select **Windows > Windows Update** and click the **+** icon.
  5. In **OS Name**, select the server as per your requirement.

  You can upgrade to the OPSWAT version 4.3.2744.0 to use the Windows server 2019 and 2022 in the EPA OS scan.

  [CGOP-20061]

- **New EPA scan classification types for missing security patches**

  The following new classification types are added to the EPA scan for missing security patches. The EPA scan fails if the client has any of the following missing security patches.

  - Application
  - Connectors
  - CriticalUpdates
  - DefinitionUpdates
  - DeveloperKits
  - FeaturePacks
  - Guidance
  - SecurityUpdates
  - ServicePacks

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tools
- UpdateRollups
- Updates

You can configure the classification types by using the GUI.

1. Navigate to **NetScaler Gateway > Policies > Preauthentication**.
2. Create a new preauthentication policy or edit an existing policy.
3. Click the ((OPSWAT EPA Editor)) link.
4. In Expression Editor, select **Windows > Windows Update**.
5. In **Shouldn't have missing patch of following windows update classification type**, select the classification type for the missing security patches
6. Click **OK**.

You can upgrade to the OPSWAT version 4.3.2744.0 to use these options.

- For details about the Windows server update services classification GUIDs, see https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)
- For the description of the Microsoft software updates terminology, see https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates

Earlier, the EPA scans for missing security patches were done on the severity levels; Critical, Important, Moderate, and Low on the Windows client.

[CGOP-19465]

- **Support for multiple device certificates for EPA scan**

  In the Always on VPN configuration, if multiple device certificates are configured, the certificate with the longest expiry date is tried for the VPN connection. If this certificate allows EPA scan successfully, then VPN connection is established. If this certificate fails in the scan process, the next certificate is used. This process continues until all the certificates are tried.

  Earlier, if multiple valid certificates were configured, if the EPA scan failed for one certificate, the scan was not attempted on the other certificates.

  [CGOP-19782]

Fixed issues

- If the clientCert parameter is set to 'Optional' in the SSL profile when configuring the VPN virtual server, users are prompted multiple times to select the smart card.

  [NSHELP-30070]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users cannot connect to the NetScaler Gateway appliance after changing the ‘networkAccessOnVPNFailure’always on profile parameter from ‘fullAccess’to ‘onlyToGateway‘.

  [NSHELP-30236]

- When Always on is configured, the user tunnel fails because of the incorrect version number (1.1.1.1) in the aoservice.exe file.

  [NSHELP-30662]

- DNS resolution to internal and external resources stops working over a prolonged VPN session.

  [NSHELP-30458]

- The Windows VPN client does not honor the ‘SSL close notify’alert from the server and sends the transfer login request on the same connection.

  [NSHELP-29675]

- Registry EPA check for the “==”and “!=”operator fails for some registry entries.

  [NSHELP-29582]

22.2.1.103 (17-Feb-2022)

Fixed issues

- Users cannot launch the EPA plug-in or the VPN plug-in after an upgrade to Chrome 98 or Edge 98 browser versions. To fix this issue, perform the following:

  1. For the VPN plug-in upgrade, end users must connect using the VPN client for the first time to get the fix on their machines. In the subsequent login attempts, users can choose the browser or the plug-in to connect.
  2. For the EPA only use case, the end users will not have the VPN client to connect to the gateway. In this case, perform the following:

     a) Connect to the gateway using a browser.
     a. Wait for the download page to appear and download the nsepa_setup.exe.
     b. After downloading, close the browser and install the nsepa_setup.exe file.
     c. Restart the client.

  [NSHELP-30641]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

21.12.1.4 (17-Dec-2021)

What's new

- **Rebranding changes**

  NetScaler Gateway plug-in for Windows is rebranded to Citrix Secure Access client.

  [ACS-2044]

- **Support for TCP/HTTP(S) private applications**

  Citrix Secure Access client now supports TCP/HTTP(S) private applications for remote users through the Citrix Workspace Secure Access service.

  [ACS-870]

- **Additional language support**

  Windows VPN and EPA plug-ins for NetScaler Gateway now support the following languages:

  - Korean
  - Russian
  - Chinese (Traditional)

  [CGOP-17721]

- **Citrix Secure Access support for Windows 11**

  Citrix Secure Access client is now supported for Windows 11.

  [CGOP-18923]

- **Automatic transfer logon when the user is logging in from the same machine and Always on is configured**

  Automatic login transfer now occurs without any user intervention when Always on is configured and the user is logging in from the same machine. Previously, when the client (user) had to relogin in the scenarios such as system restart or network connectivity issues, a pop-up message appeared. The user had to confirm the transfer login. With this enhancement, the pop-up window is disabled.

  [CGOP-14616]

- **Deriving Citrix Virtual Adapter default gateway IP address from the NetScaler provided net mask**

  Citrix Virtual Adapter default gateway IP address is now derived from the NetScaler provided net mask.

  [CGOP-18487]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- Sometimes, users lose internet access after a VPN tunnel is established in split tunnel ON mode. Citrix Virtual adapter's erroneous default route causes this network issue.

  [NSHELP-26779]

- When split tunnel is set to "Reverse,"DNS resolution for the intranet domains fails.

  [NSHELP-29371]

21.9.100.1 (30-Dec-2021)

What's new

- **Citrix Secure Access support for Windows 11**

  Citrix Secure Access client is now supported for Windows 11.

  [CGOP-18923]

Fixed issues

- Sometimes, users lose internet access after a VPN tunnel is established in split tunnel ON mode. Citrix Virtual adapter's erroneous default route causes this network issue.

  [NSHELP-26779]

- When split tunnel is set to "Reverse,"DNS resolution for the intranet domains fails.

  [NSHELP-29371]

21.9.1.2 (04-Oct-2021)

Fixed issues

- Sometimes, after disconnecting the VPN, the DNS resolver fails to resolve the host names, because the DNS suffixes are removed during VPN disconnection.

  [NSHELP-28848]

- Sometimes, a user is logged out of NetScaler Gateway within a few seconds when the client idle timeout is set.

  [NSHELP-28404]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Windows plug-in might crash during authentication.

  [NSHELP-28394]

- In Always On service mode, the VPN plug-in for Windows fails to establish the user tunnel automatically after the users log on to their Windows machines.

  [NSHELP-27944]

- After the tunnel establishment, instead of adding DNS server routes with the previous gateway IP address, the Windows plug-in adds the routes with the default gateway address.

  [NSHELP-27850]

V21.7.1.1 (27-Aug-2021)

What's new

- **New MAC address scan**

  Support is added for newer MAC address scans.

  [CGOP-16842]

- **EPA scan to check for Windows OS and its build version**

  Added EPA scan to check for Windows OS and its build version.

  [CGOP-15770]

- **EPA scan to check for a particular value's existence**

  A new method in the registry EPA scan now checks for a particular value's existence.

  [CGOP-10123]

Fixed issues

- If there is a JavaScript error during login because of a network error, subsequent login attempts fail with the same JavaScript error.

  [NSHELP-27912]

- The EPA scan fails for McAfee antivirus last update time check.

  [NSHELP-26973]

- Sometimes, users lose internet access after a VPN tunnel is established.

  [NSHELP-26779]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A script error for the VPN plug-in might be displayed during nFactor authentication.

  [NSHELP-26775]

- If there is a network disruption, UDP traffic flow that started before the network disruption does not drop for up to 5 minutes.

  [NSHELP-26577]

- You might experience a delay in the starting of the VPN tunnel if the DNS registration takes a longer time than expected.

  [NSHELP-26066]

V21.3.1.2 (31-Mar-2021)

What's new

- **Upgraded EPA libraries**

  The EPA libraries are upgraded to support the latest version of the software applications used in EPA scans.

  [NSHELP-26274]

- **NetScaler Gateway virtual adapter comaptibility**

  The NetScaler Gateway virtual adapter is now compatible with Hyper-V and Microsoft Wi-Fi direct virtual adapters (used with printers).

  [NSHELP-26366]

Fixed issues

- The Windows VPN gateway plug-in blocks use of "CTRL + P"and "CTRL + O"over the VPN tunnel.

  [NSHELP-26602]

- The NetScaler Gateway plug-in for Windows responds only with an Intranet IP address registered in the Active Directory when a `"nslookup"` action is requested for the machine name.

  [NSHELP-26563]

- The IIP registration and deregistration fails intermittently if the split DNS is set as "Local"or "Both."

  [NSHELP-26483]

- Auto logon to Windows VPN gateway plug-in fails if Always On is configured.

  [NSHELP-26297]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Windows VPN gateway plug-in fails to drop IPv6 DNS packets resulting in issues with DNS resolution.

  [NSHELP-25684]

- The Windows VPN gateway plug-in maintains the existing proxy exception list even if the list overflows because of the browser limit on the Internet Explorer proxy exception list.

  [NSHELP-25578]

- The Windows VPN gateway plug-in fails to restore the proxy settings when the VPN client is logged off in Always On mode.

  [NSHELP-25537]

- The VPN plug-in for Windows does not establish the tunnel after logging on to Windows, if the following conditions are met:

  - NetScaler Gateway appliance is configured for the Always On feature.
  - The appliance is configured for certificate based authentication with two factor authentication "off."

  [NSHELP-23584]

Features in preview

September 7, 2025

Features in preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. We do not accept support cases for features in preview but welcome feedback for improving them. We might act on feedback based on its severity, criticality, and importance.

The following feature is currently in preview:

- Microsoft Edge WebView support for Windows Citrix Secure Access

> **Note:**
>
> - Starting from the Citrix Secure Access client for Windows version 24.11.1.17, Microsoft Edge WebView is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved log collection for Windows client

September 8, 2026

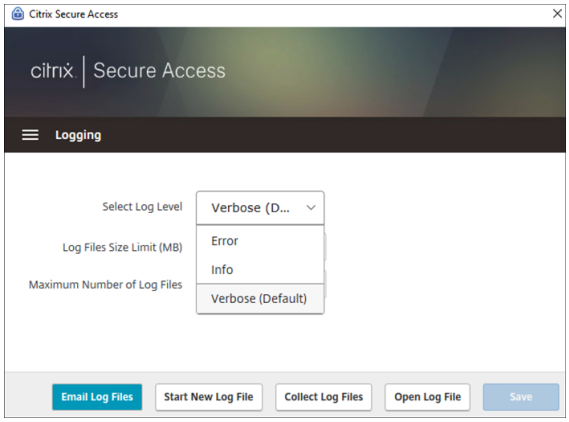
The logging feature for the Windows Secure Access client is enhanced with improved log collection and debugging. The new log files are prefixed with “csa_”.

Starting from the Citrix Secure Access client for Windows 23.10.1.7, the default log level is set to Verbose for an enhanced log collection and troubleshooting.

With these changes, admins and end-users can collect logs from the current session and past sessions. Previously, the collection of logs was limited to the current sessions only.

Configure logging by using the Citrix Secure Access™ client UI

1. Install the Secure Access client for Windows.
2. Click **Logging** from the menu. All configuration related to logs can be done in the Logging screen.



- **Select Log Level:**

  When the new logging mechanism is enabled, the following three log levels are available.

  - Error: Only exceptions or failures reported by the application are logged.
  - Info: This level includes informational messages and events relevant from program execution. It also includes errors and exceptions.
  - Verbose (default): This level includes all log messages reported by Error and Info log levels and additional messages that might help in troubleshooting.

- **Log File Size Limit:** (Mandatory) Enter the log file size of each log file. The maximum value is 600 MB.

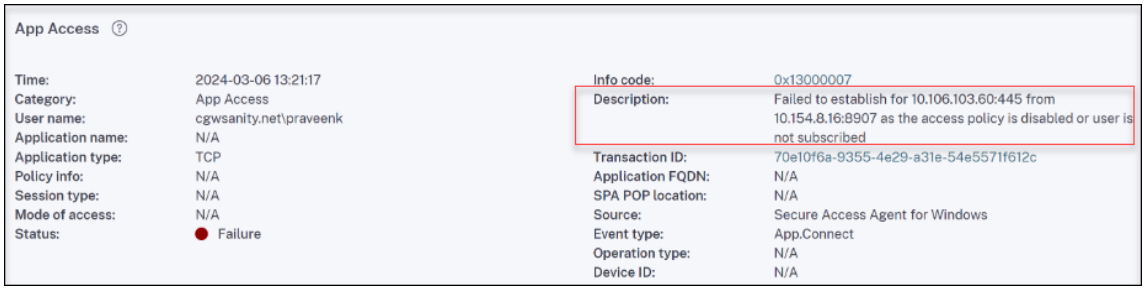
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Maximum Number of Log Files:** (Mandatory) Enter the number of files that you want to add for log collection. The maximum value is 5.
- **Email Log Files** –Email the log files to the registered email ID.
- **Start New Log File** –When you select this option, a new log file is created.
- **Collect Log Files** –Click to create a zip file with all log files from the application. This zip file is saved on the client's desktop.
- **Open Log Files** –When you select this option, the latest `csa_nssslvpn*.txt` file opens.

Improved Citrix Secure Access diagnostics for Windows client

Starting from the Citrix Secure Access client for Windows release 24.6.1.18, the Citrix Secure Access diagnostics are enhanced to include additional fields for troubleshooting access issues with TCP/UDP applications.

- **Description:** The destination IP, source port, and destination port are included in the **Description** field of the **App Access** log when access to the TCP/UDP apps from the Citrix Secure Access client for Windows fails.



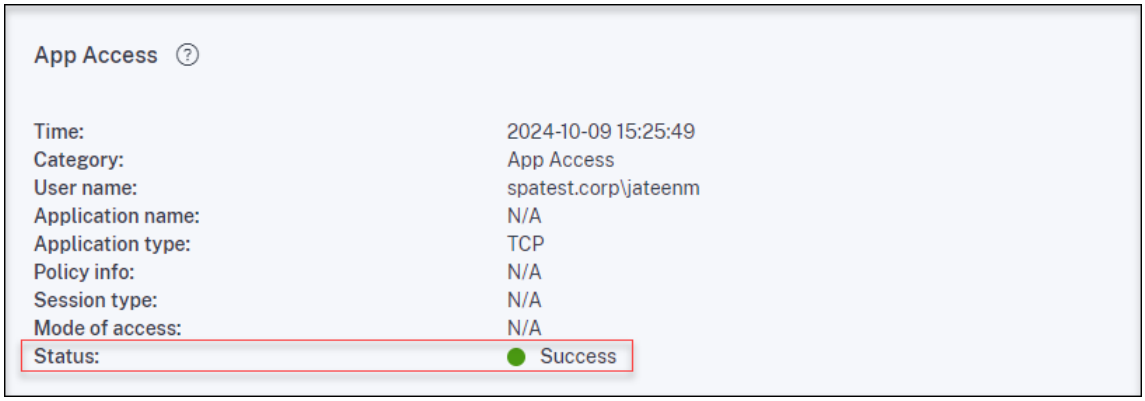
- **DNS failures:** TCP based DNS failures and UDP based DNS failures are reported explicitly in the **App Access** log.



- **Application name details:** The **App Access** log in the Citrix Secure Access client for Windows includes the application name with access failure or success status. This field allows the admin

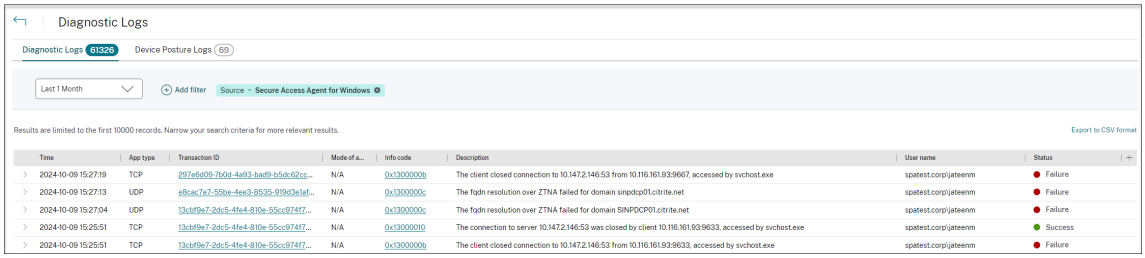
© 1997–2026 Citrix Systems, Inc. All rights reserved.

to understand which applications are accessing the TCP/UDP workflow and if the same is using a different port combination.



In addition to the **App Access** log, the CAS (Citrix Access Security) **Diagnostics Logs** is enhanced with the following:

- **Overview of CAS Diagnostics Logs:** The overview of the CAS **Diagnostics Logs** includes descriptions of what is failing in the Citrix Secure Access client for Windows and the cause of failure.
- **WPAD DNS failures:** By default, **WPAD DNS** failures of the Citrix Secure Access client for Windows are reported on CAS **Diagnostics Logs**. Administrators must configure the `DisableWpadDnsCasReporting` registry in the Citrix Secure Access client for Windows to prevent overloading of CAS **Diagnostics Logs** with WPAD DNS failures.



Integrated packet capture tool for Citrix Secure Access for connectivity troubleshooting

May 6, 2026

The Citrix Secure Access VPN client for Windows includes an integrated network packet capture tool to help troubleshoot connectivity issues. Captured files are automatically saved to the `logs\captures\` directory under the Citrix Secure Access installation folder. Automatic file rotation

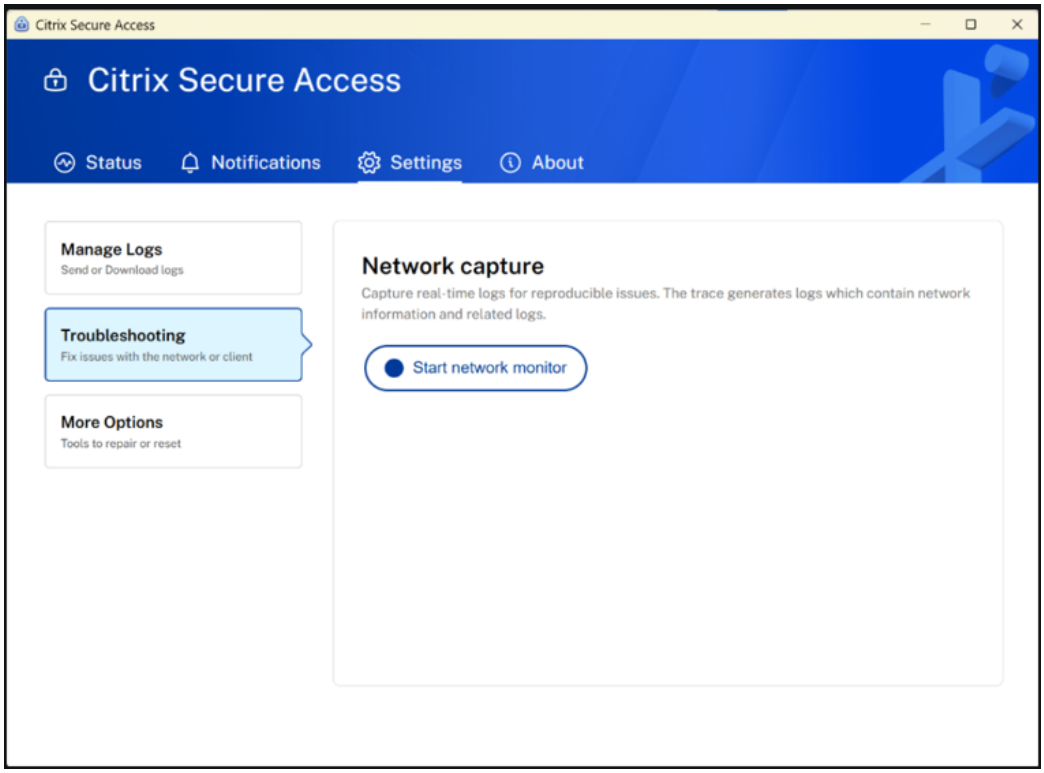
© 1997–2026 Citrix Systems, Inc. All rights reserved.

helps limit disk usage. The packet capture files are also automatically included in the diagnostic log bundle when logs are collected for Citrix Support.

> **Note:**
>
> - The network packet capture tool is available only in the new WebModule UI.
> - The Citrix Secure Access installer includes the packet capture utility and the required WinDivert kernel driver dependencies. No separate installation is required.

Start a packet capture

1. Open the **Citrix Secure Access** application.
2. Click the **Settings** tab.
3. In the left panel, select **Troubleshooting**.
4. In the right pane, go to the **Network capture** section.
5. Click **Start network monitor** to begin capturing network traffic.

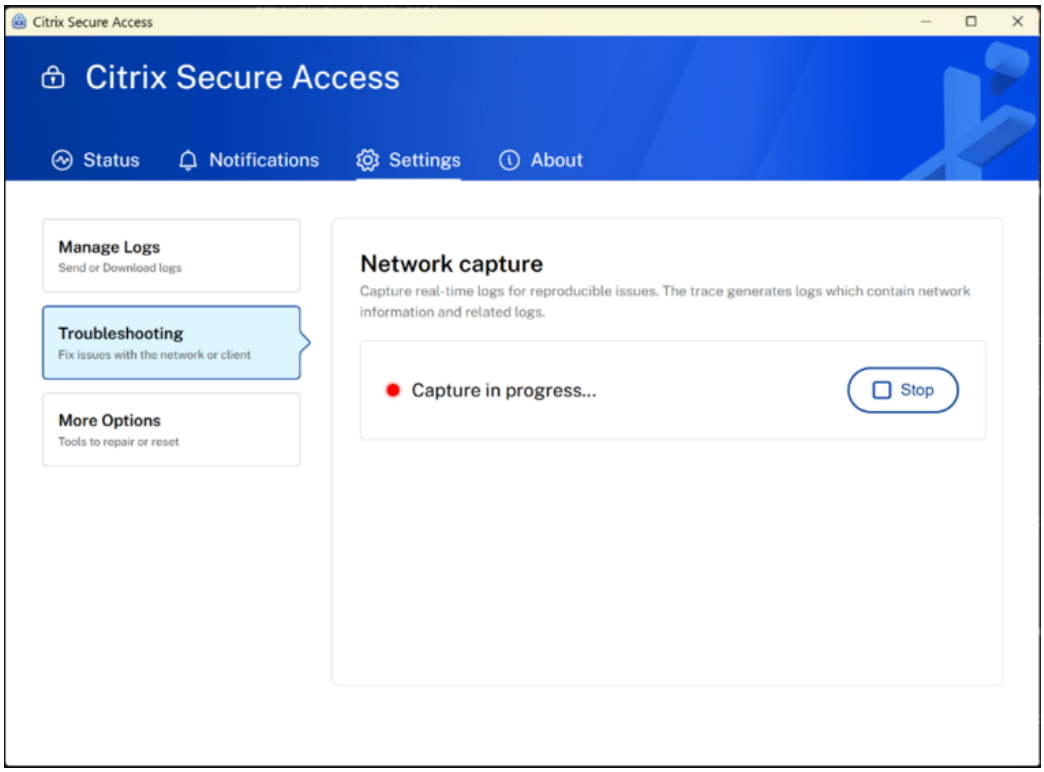


When capture starts, the status changes to **Capture in progress…** and the **Stop** button becomes available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Stop a packet capture

1. In the Citrix Secure Access application, navigate to **Settings** > **Troubleshooting**.
2. When capture is active, the **Network capture** panel shows **Capture in progress...** with a red indicator.
3. Click the **Stop** button to end the capture.



After capture stops: download or restart

Once the capture stops, the status changes to **Capture complete** (green indicator).

You can then choose one of the following options:

- **Download**: Saves the capture file to your local machine.
- **Restart**: Starts a new packet capture session immediately.

An information banner displays the full path where the capture file is saved. For example:

```
C:\Program Files\Citrix\Secure Access Client\logs\captures\csatrace_20260407_0
.pcap
```

The `.pcap` file can be opened in a packet analysis tool such as Wireshark for further investigation or shared with Citrix Support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access™ auto log on for Windows Azure AD joined machines

September 25, 2026

Auto log on to NetScaler Gateway virtual server

Citrix Secure Access client can perform SSO to NetScaler Gateway virtual server using PRT and auto-connect the user to the NetScaler Gateway URL mentioned in the `AlwaysOnURL` registry. For more information, see NetScaler Gateway Windows VPN client registry keys.

Admin must configure the following to enable SSO to NetScaler Gateway virtual server using PRT:

- Microsoft Entra ID must be configured as the SAML IdP.
- NetScaler Gateway must be configured as the SAML SP.
- Citrix Secure Access client must be configured in Always On or Always On service mode.

To configure Citrix Secure Access client to perform SSO using PRT, you must complete the following steps:

1. Join the windows machine to Azure Entra ID. Admin must visit the following url and join the windows machine:

   URL.

2. Configure NetScaler Gateway as SAML SP and Microsoft Entra ID as SAML IdP. For more information, see Configure Microsoft Entra ID as SAML IdP and NetScaler as SAML SP.
3. Configure Citrix Secure Access client in Always On and Always On service mode. For more information, see Always On VPN before Windows Logon (formally Always On service) and Always On.

Users must use their credentials and login for the first time. During subsequent system reboots, Citrix Secure Access client auto-connects the user to NetScaler Gateway virtual server using PRT.

Auto log on to the Secure Private Access service

Citrix Secure Access client can perform SSO to Secure Private Access service using PRT. This works when the client is configured in Always On or Always On service mode.

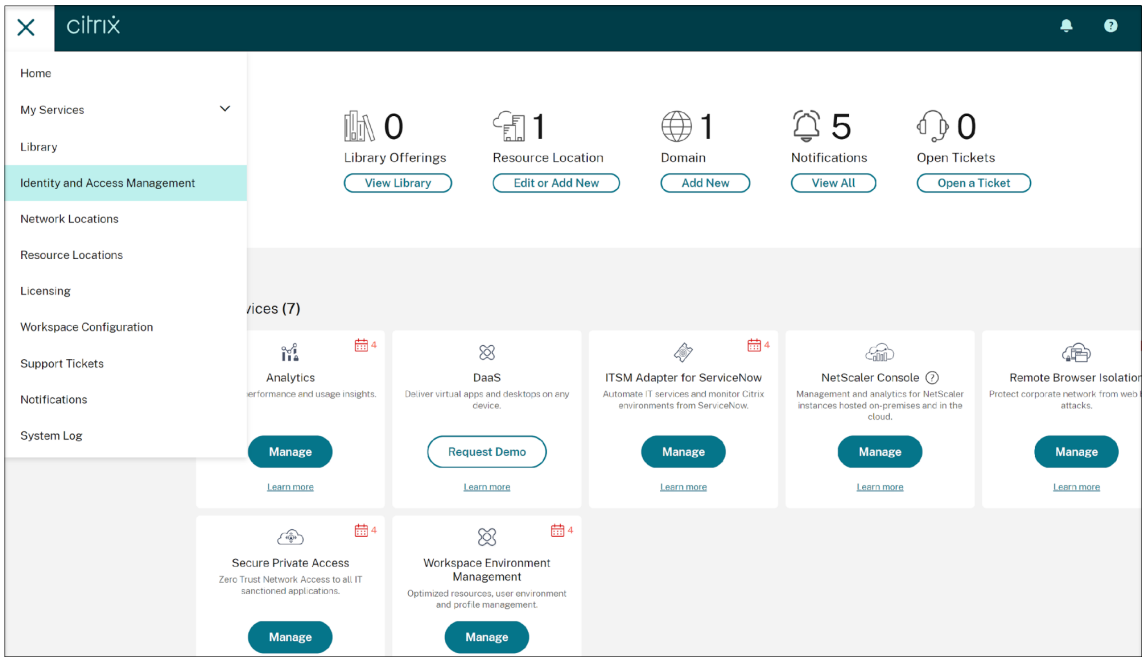
To configure Citrix Secure Access client to perform SSO using PRT, you must complete the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

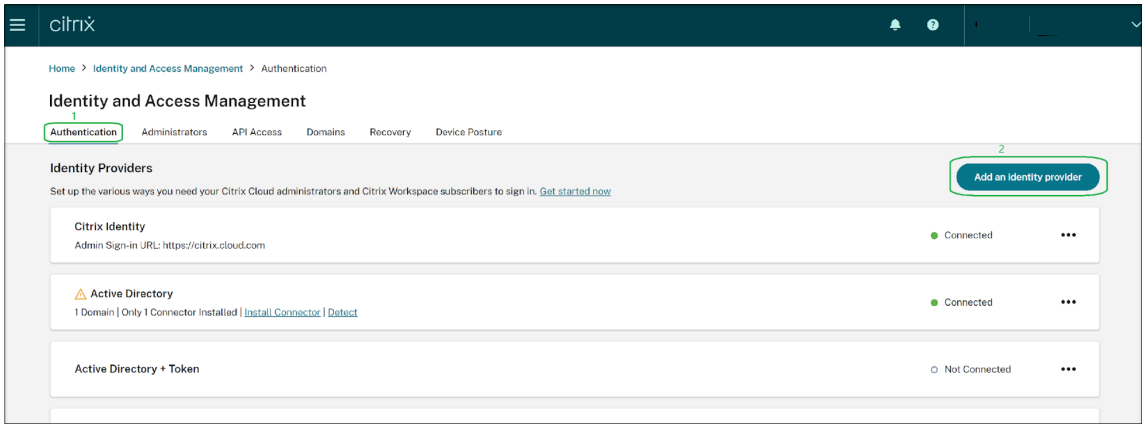
1. Join the windows machine to Azure Entra ID. Admin must visit the following url and join the windows machine:

   URL.

2. Log in to the Citrix Cloud™ account.
3. Click the hamburger icon and navigate to **Identity and Access Management**.

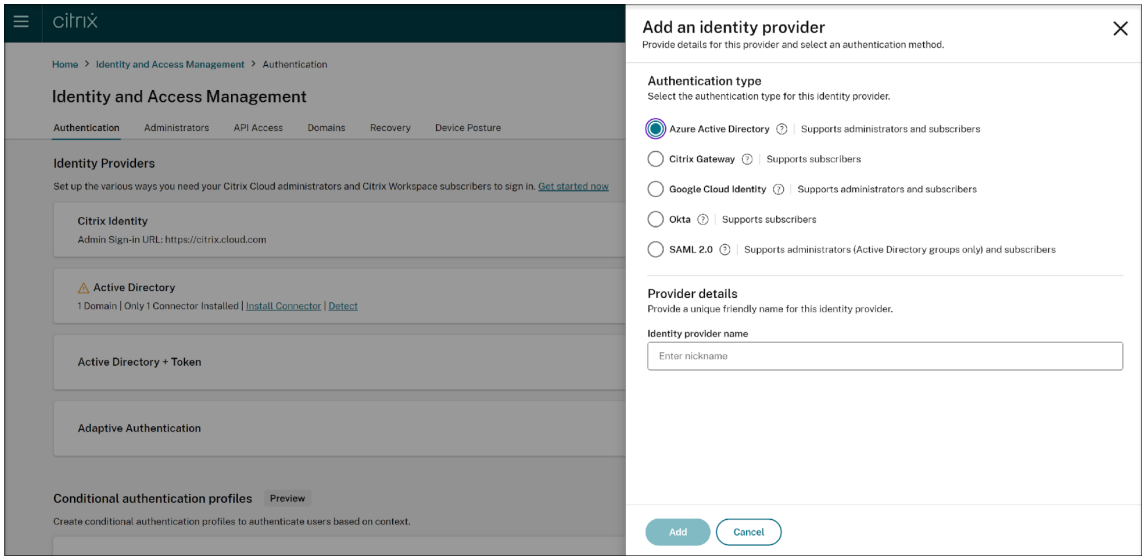


4. On the **Identity and Access Management** screen, click the **Authentication** tab and then click the **Add an Identity provider** button.

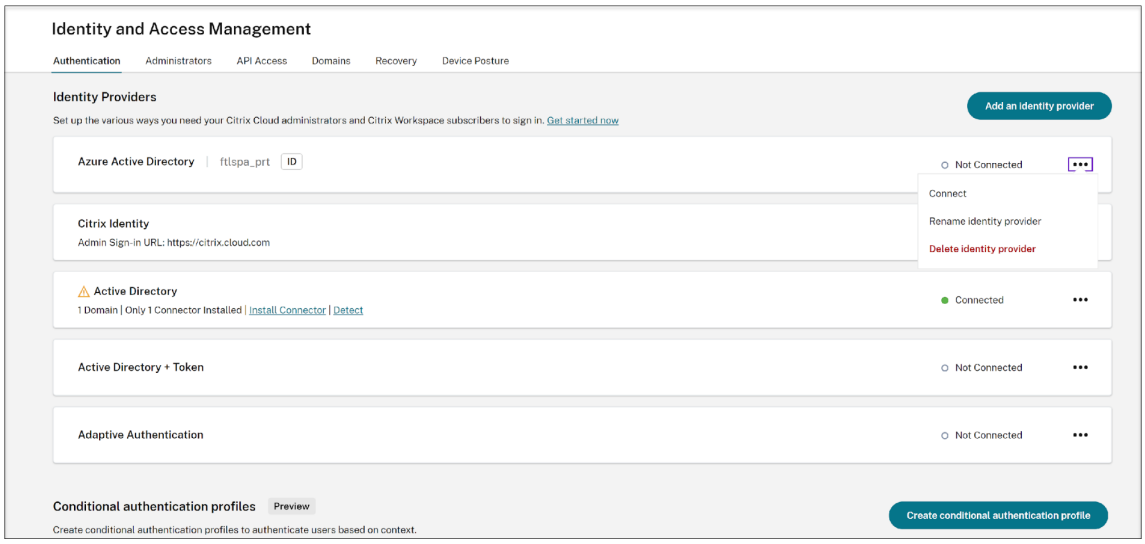


5. Select the authentication type as **Azure Active Directory**, provide a name to the identity provider in the **Identity Provider name** text box, and click the **Add** button.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

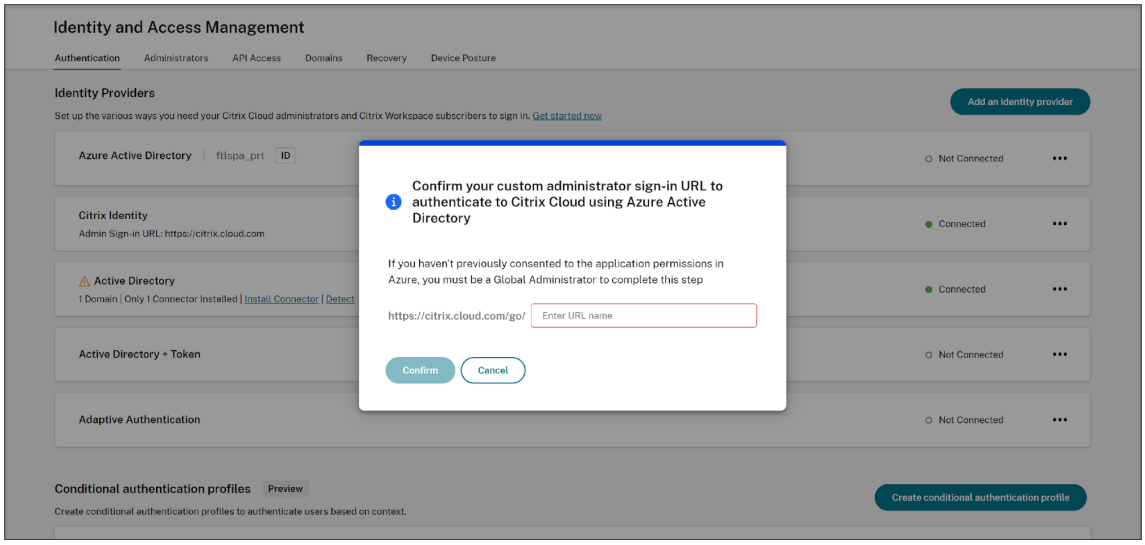


6. **Azure Active Directory** is listed on the identity providers list as shown below. Click **Connect**.

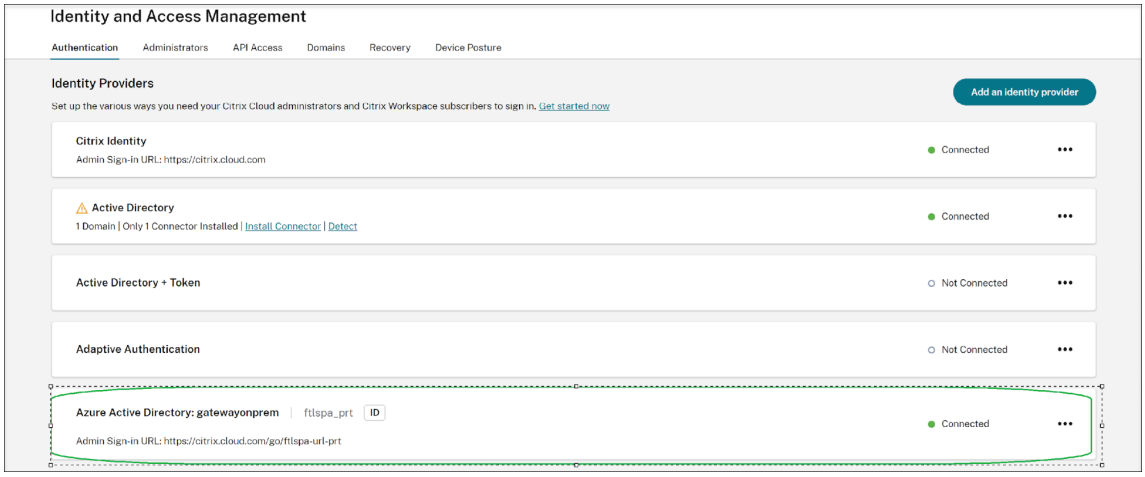


7. On the connect screen, enter the URL name and click the **Confirm** button.

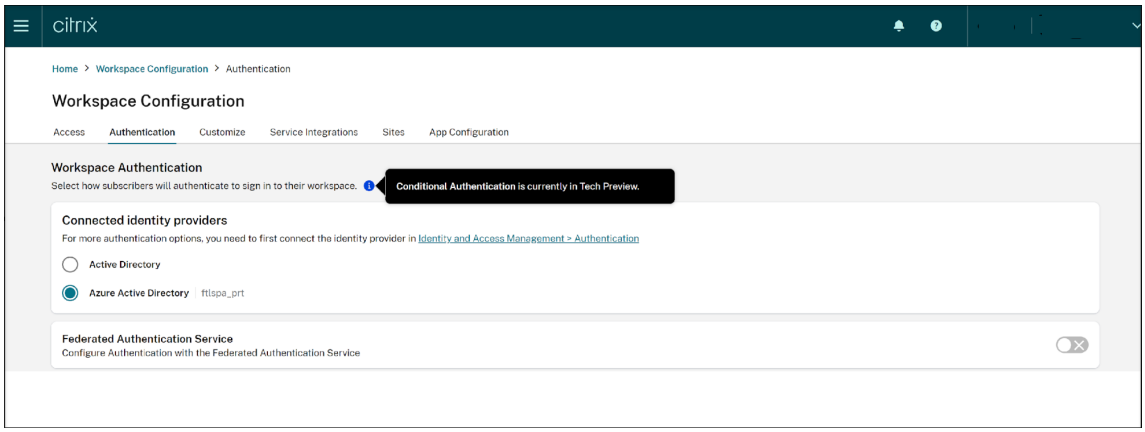
© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Admin is redirected to the Microsoft sign-in page. Sign in using an Azure Entra ID user account. Once login succeeds, Azure Active Directory shows as connected.

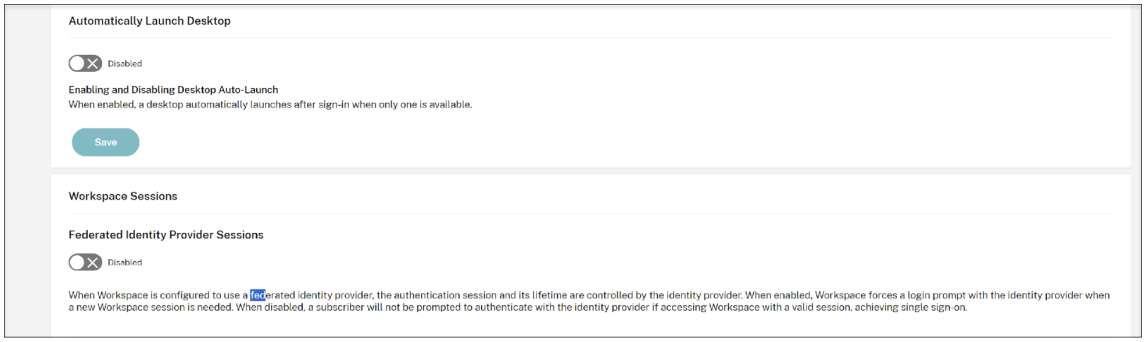


9. Go back to **Workspace Configuration**, click the **Authentication** tab, and select **Azure Active Directory**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Navigate to **Workspace Configuration** -> **customize** -> **preferences** and deselect the checkbox below **Federated Identity Provider Sessions** to disable Federated Authentication Service.



Users must use their credentials and login for the first time. During subsequent system reboots, the Citrix Secure Access client auto-connects the user to Secure Private Access using PRT.

Microsoft Edge WebView support for Windows Citrix Secure Access

September 8, 2026

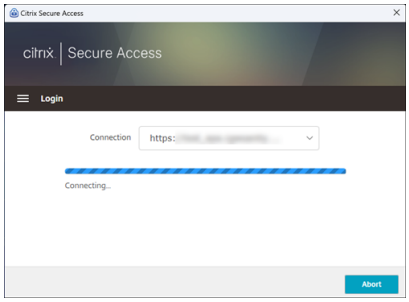
> **Important:**
>
> - Starting from the Citrix Secure Access client for Windows version 24.11.1.17, Microsoft Edge WebView is enabled by default.
> - Starting January 29, 2025, Citrix changes the method of enabling preview features in the Citrix Secure Access client for Windows. To ensure optimal performance of preview features (features under feature flag) in the Citrix Secure Access client for Windows, you must enable traffic to `features.netscalergateway.net` and upgrade the clients to version 24.8.1.19 or later. For more information, see Feature management for the Citrix Secure Access client for Windows.

Microsoft Edge WebView is now the recommended WebView by Microsoft because the Internet Explorer WebView is deprecated. We recommend you to use Citrix Secure Access client 23.8.1.5 or later versions to leverage the functionalities of Microsoft Edge WebView.

Changes to the end-user

The authentication screens of the Citrix Secure Access client UI appear as follows.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

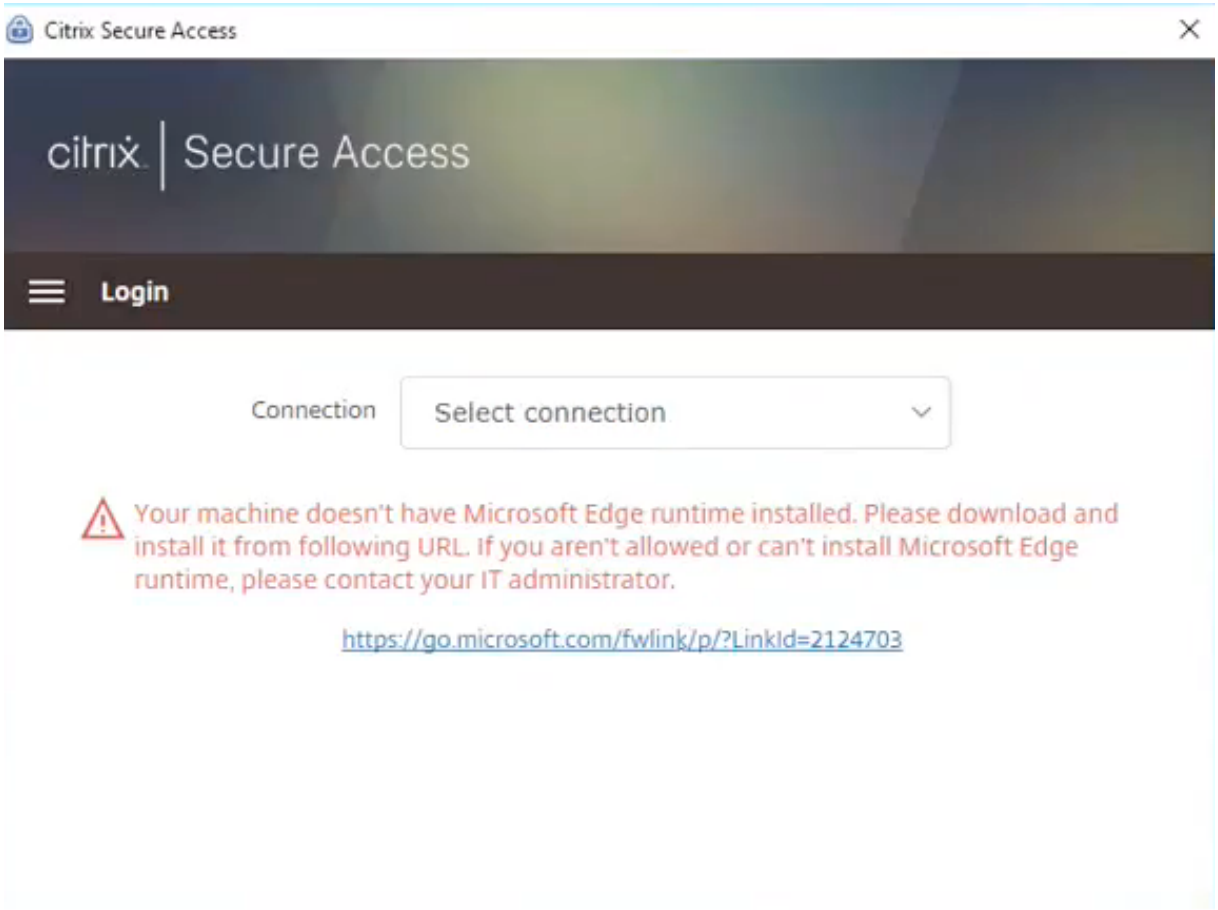


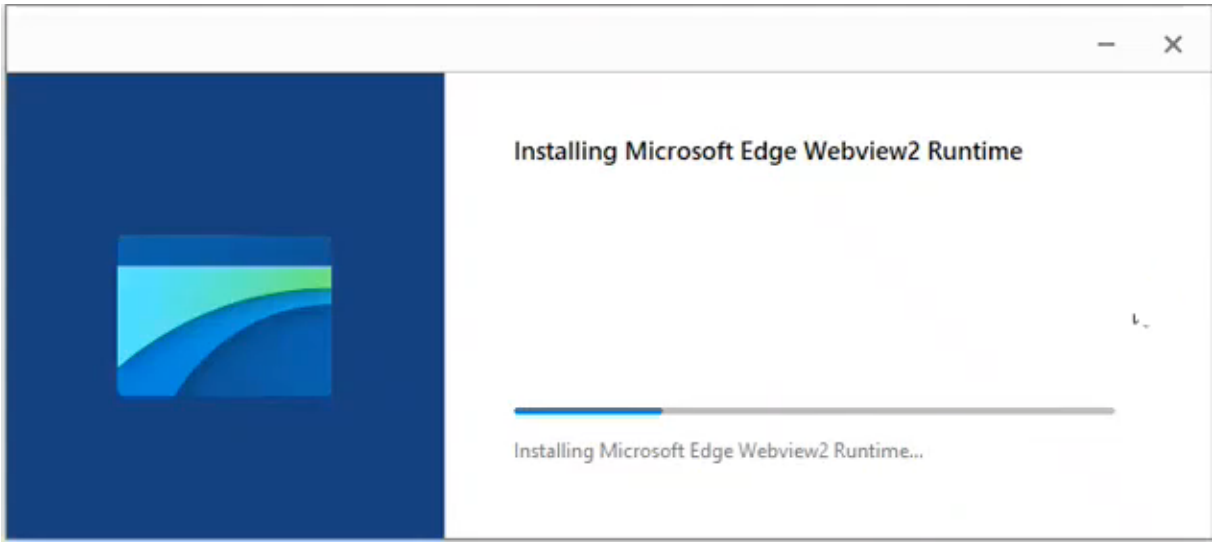
Once the end-users select the URL, Citrix Secure Access client opens a new window prompting them to log on to NetScaler Gateway using their credentials.



If the Windows client machine does not have the Microsoft Edge WebView runtime installed, end-users are provided with a link on the Citrix Secure Access client UI to download and install the Microsoft Edge WebView runtime. End-users can download and install the Edge WebView runtime seamlessly when connected to the VPN and the authentication isn't interrupted during this process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





Notes:

- The Microsoft Edge WebView functionality does not impact any admin-specific configurations.
- We recommend that you enable the HttpOnly cookie feature when using Edge WebView on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Citrix Secure Access. This improves the NetScaler Gateway logon duration when EPA is used as a factor in the nfactor flow.

Troubleshooting

- If you face any issues with this feature, contact Citrix support.
- You can submit your feedback about the Edge WebView feature through citrixgatewaybetafeedback@cloud.com.

Upgrade the Citrix Secure Access client and EPA client for Windows on NetScaler Gateway

September 25, 2026

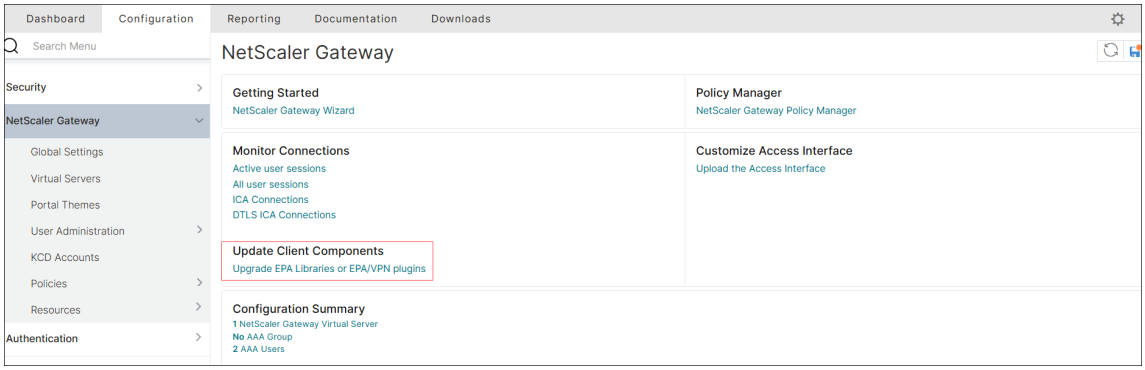
> **Important:**
>
> - You can upgrade the Citrix Secure Access client and EPA client for Windows on NetScaler Gateway to ensure that your appliance checks for the latest firewalls and antivirus.
> - Upgrading the Citrix Secure Access client and EPA client for Windows eliminates the need to upgrade NetScaler Gateway solely for client updates.
> - The upgrade of the Citrix Secure Access client and EPA client for Windows is facilitated through the NetScaler Gateway UI from the release build 13.0-76.31 and above.
> - In a high availability setup, the Citrix Secure Access™ client and EPA client for Windows must be upgraded on both the primary and secondary nodes.
> - Before upgrading, ensure the upgrade files (tar.zip format) are uploaded to your local machine or NetScaler Gateway.
> - Even if you do not use EPA, we recommend that you update both VPN and EPA plug-in binaries together in case you choose to use the EPA functionality later.

Upgrade the clients using the NetScaler Gateway GUI

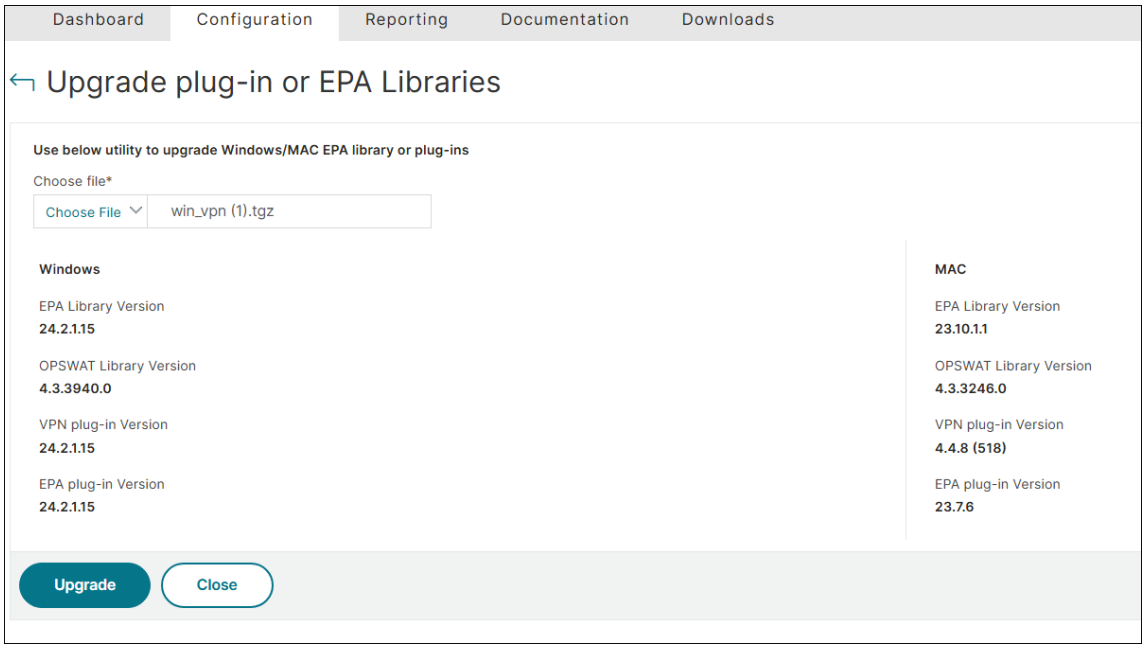
Perform the following steps on the NetScaler Gateway GUI to upgrade the clients:

1. Navigate to **NetScaler Gateway** > **Update Client Components**.
2. Under **Update Client Components**, click the **Upgrade EPA/Client Components** link.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

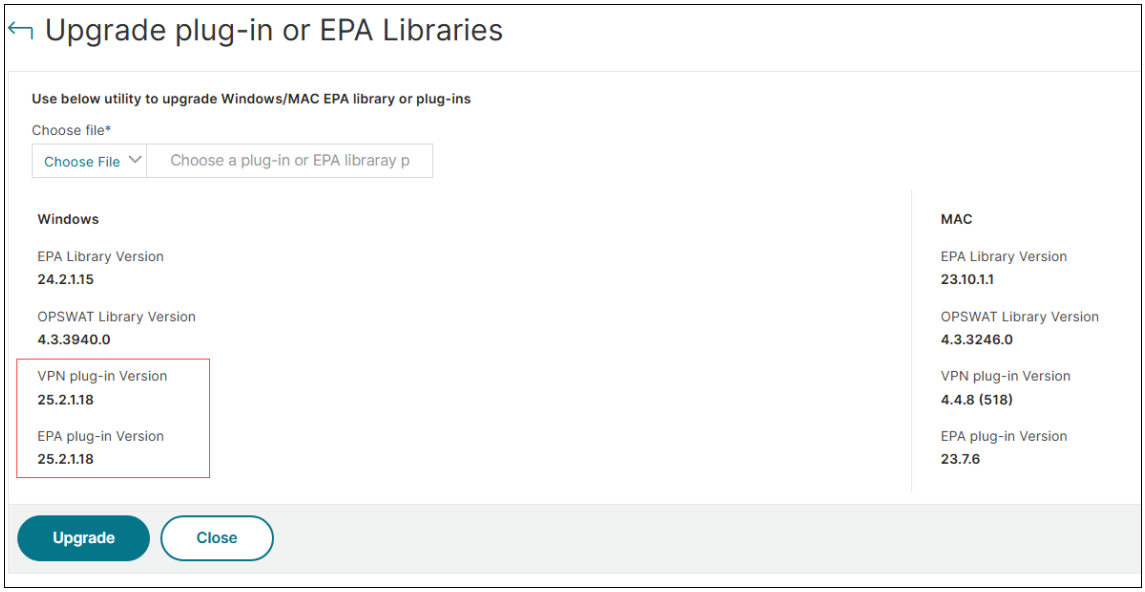


3. In **Choose File**, select the source for the upgrade file (local or NetScaler Gateway).
4. Navigate to the file to select the file and click **Upgrade**.



5. After the upgrade is completed, click the **Upgrade EPA/Client Components** link and verify if the upgrade is successful.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Upgrade the clients using the NetScaler® file system

Perform the following steps to upgrade the clients:

1. Download the latest version of the Citrix Secure Access client and EPA client for Windows.
2. Open the NetScaler file system using a Secure File Transfer Protocol (SFTP) or Secure Copy Protocol (SCP) application such as winscp.
3. For upgrading the Citrix Secure Access client:

   a. Select the file `/var/netscaler/gui/vpns/scripts/vista`.

   b. Replace the `AGEE_setup.exe` file with the downloaded client file.

   c. Go to `/netscaler/ns_gui/vpn/`.

   d. Open the `pluginlist.xml` file.

   e. Replace the current version with the latest version and set the plug-in type as “WIN-VPN”. See the following image for reference:

```
1 ![Set plug-in type](/en-us/citrix-secure-access/media/upgrade-win-
     vpn.png)
2
3 >**Note:**
4 >
5 >Ensure to set the upgrade type to “Always” on the XML file.
```

   f. Copy the updated XML file and replace it in the `/var/netscaler/gui/vpn/` directory.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. For upgrading the EPA client:

   a. Navigate to /var/netscaler/gui/epa/scripts/win/.

   b. Replace the nsepa_setup.exe file with the downloaded client file.

   c. Go to /netscaler/ns_gui/vpn/.

   d. Open the pluginlist.xml file.

   e. Replace the current version with the latest version and set the plug-in type as "WIN-EPA"or "WIN-EPA64"based on your requirement. See the following image for reference:

```
1 ![Set plug-in type for EPA](/en-us/citrix-secure-access/media/
    upgrade-win-epa.png)
```

   f. Copy the updated XML file and replace it in the /var/netscaler/gui/vpn/ directory.

Reverse split tunneling of non-configured domains

September 7, 2025

Starting with the Citrix Secure Access client for Windows release 25.5.1.15, DNS resolution for non-configured domains is performed remotely when reverse split tunneling is enabled, irrespective of the **Split DNS** setting. Previously, DNS resolution for non-configured domains worked as follows with reverse split tunneling:

- When **Split DNS** is set to **BOTH**, non-configured domains are resolved both locally and remotely, leading to redundancy and ambiguity.
- When **Split DNS** is set to **LOCAL**, non-configured domains are resolved locally, increasing the risk of DNS leakage and unintended routing.

DNS resolution matrix

The following table summarizes the DNS resolution behavior for different **Split DNS** settings when reverse split tunneling is enabled.

Split DNS setting	Host name is configured	DNS suffix is configured	Domains are not configured
LOCAL	LOCAL	REMOTE	REMOTE
REMOTE	REMOTE	REMOTE	REMOTE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Split DNS setting	Host name is configured	DNS suffix is configured	Domains are not configured
BOTH	BOTH	REMOTE	REMOTE

Example:

The following is a sample split tunnel configuration in the Citrix Secure Access™ client:

```
{

    "Version": 1,
    "Username": "xyz",
    "Tunnel": {

        "Split-Tunnel": "ON",
        "Split-DNS": "BOTH",
        "Tunnel-Rules": [
            {

                "Protocol": "ANY",
                "Type": "Hostname",
                "Hostnames": [
                    "login.microsoftonline.com"
                ]
             }
 ,
            {

                "Protocol": "ANY",
                "Type": "Hostname",
                "Hostnames": [
                    "*.spatest.corp"
                ]
             }
 ,
            {

                "Protocol": "ANY",
                "Type": "IPV4",
                "Start": "10.102.76.14",
                "Stop": "10.102.76.14"
             }

        ],
        "FQDN-SpoofedIP": {

            "IPv4": "172.16.0.0",
            "IPv4-Prefix": 16
         }
 ,
        "DNS-Truncate-Fix": true,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        "DNS-Suffix-List": [
            "cgwsanity.net"
        ]
    }
,
    "AlwaysON": {

        "Network-Access": true,
        "Client-Control": true
    }
,
    "EPA": {

    }
,
    "Proxy": {

    }
,
    "Client-Config": {

        "Local-Lan-Access": true,
        "Restart-NLA": true,
        "Allow-Logging": true,
        "Forced-Timeout": 0,
        "Forced-Timeout-Warning": 0,
        "Client-Idle-Timeout": 0
    }
,
    "Client-Cleanup": {

    }
,
    "Supported-Mux-Versions": "1,2"
}
```

For the preceding split tunnel configuration, the DNS resolution is performed as given in the table that follows:

Entity	Configuration	Split DNS Setting	DNS Resolution
login.microsoftonline.com	Host name login.microsoftonline.com is configured in Tunnel-Rules	BOTH	LOCAL+REMOTE
		LOCAL	LOCAL
*.spatest.corp	Host name *.spatest.corp is configured in Tunnel-Rules	BOTH	LOCAL+REMOTE
		LOCAL	LOCAL
dc.cgwsanity.net	DNS suffix cgwsanity.net is configured in Tunnel-Rules	BOTH	REMOTE
		LOCAL	REMOTE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Entity	Configuration	Split DNS Setting	DNS Resolution
citrite.net	Domain or host name is not configured in Tunnel-Rules	BOTH	REMOTE
		LOCAL	REMOTE
sf1.spatest.corp	Domain or host name is not configured in Tunnel-Rules	BOTH	REMOTE
		LOCAL	REMOTE

To restore older split DNS behavior

To restore the older split DNS behavior, where non-configured domains are resolved both locally and remotely when reverse split tunneling is enabled, configure the following registry:

Registry Name: DisableReverseTunChangeSplitDnsBehavior

Registry Type: REG_DWORD

Registry value: 1

Registry path: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

> **Note:**
>
> Use this registry only if legacy behavior is essential for compatibility or operational reasons.

Troubleshooting failures in the Citrix Secure Access client for Windows

September 25, 2026

Auto-login failure in the Citrix Secure Access client version 24.11.1.17 and above

Auto-login for classic authentication fails in the Citrix Secure Access client when Microsoft Edge WebView is enabled. Previously, versions prior to 24.11.1.17 supported auto-login for both classic and advanced authentication using Internet Explorer WebView.

Due to Microsoft's deprecation of Internet Explorer, Citrix Secure Access clients versions 24.11.1.17 and later default to Microsoft Edge WebView, which does not support classic authentication. We recommend migrating to advanced (nFactor) authentication. If you must continue using classic authentication, disable Microsoft Edge WebView until the migration is complete.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following table summarizes the compatibility matrix for different authentication modes and WebView components in various Citrix Secure Access client versions:

Citrix Secure Access client version	Default WebView	Authentication mode	Auto-login support	Workaround required
24.11.1.17 and lower	Internet Explorer WebView	Classic	Supported	Not required
24.11.1.17 and lower	Internet Explorer WebView	Advanced (nFactor)	Supported	Not required
24.11.1.17 and above	Microsoft Edge WebView	Advanced (nFactor)	Supported	Not required
24.11.1.17 and above	Microsoft Edge WebView	Classic	Not Supported	• Option 1: Contact Citrix Support • Option 2: Configure registry

To resolve auto-login failure

To enable auto-login for classic authentication in the Citrix Secure Access client version 24.11.1.17 and above, the default WebView in the Citrix Secure Access client must be reverted to Internet Explorer WebView using one of the following methods.

Option 1: Contact Citrix Support Contact Citrix Support to disable Microsoft Edge WebView for the customer environment.

Option 2: Configure registry To revert the default WebView to Internet Explorer WebView, apply the following registry configuration:

REG_NAME: EnableEdgeWebView

REG_PATH: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

REG_TYPE: REG_DWORD

REG_VALUE: 0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Login failure due to third-party software

You might encounter login failures in the Citrix Secure Access client if a third-party software performs Dynamic Link Library (DLL) injection from directories other than `C:\\Windows` or `C:\\Program Files`.

To troubleshoot the login failure, verify the log file at `C:\Program Files\Citrix\Secure Access Client\logs\csa_nsverctl.txt`. A "No External Signature matched"log suggests the problem lies with the third-party software. The following is an example of a failure log:

```
2025-05-27 14:15:24.398 | 17020 | DEBUG | D | NONE | Signer cert name to verify file: = ABC signername INC |
2025-05-27 14:15:24.398 | 17020 | ERROR | S | NONE | Verify file: No External Signature matched |
```

To resolve the login failure

The login failure due to a third-party software can be resolved using one of the following methods:

Option 1: Exclude the nsload.exe process Configure the third-party software to exclude the nsload.exe process. This configuration ensures optimal compatibility with the third-party software that performs DLL injection from directories other than `C:\Windows` or `C:\Program Files`.

Option 2: Configure registry Starting from the Citrix Secure Access client for Windows release 25.2.1.18, you can apply the following registry configuration if DLL injection is required:

REG_NAME: ExternalTrustedSigners

REG_PATH: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client

REG_TYPE: REG_MULTI_SZ

REG_VALUE: Signer name of the DLL being injected

You can get the signer name from the log file at `C:\Program Files\Citrix\Secure Access Client\logs\csa_nsverctl.txt`. In the following example log, "ABC signername INC"is the signer name to be configured in the `ExternalTrustedSigners` registry.

```
2025-05-27 14:15:24.398 | 17020 |   DEBUG | D | NONE | Signer cert name to verify file: = ABC signername INC  |
2025-05-27 14:15:24.398 | 17020 |   ERROR | S | NONE | Verify file: No External Signature matched |
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access for macOS/iOS

September 25, 2026

The legacy VPN client was built using Apple's private VPN APIs that are now deprecated. VPN support in Citrix Secure Access for macOS and iOS is rewritten from the ground up using Apple's public Network Extension framework.

> **Note**
>
> - Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.
> - Citrix Secure Access for macOS is supported on 12.x (Monterey), 13.x (Ventura), 14.x (Sonoma), and 15.x (Sequoia). It supports devices with Intel chips and Apple chips.
> - Users with hardware which cannot be upgraded to one of the earlier mentioned versions (macOS 10.15 and macOS 11.0) have access to the last compatible version on the App Store, but there are no further updates to the older versions.
> - If a macOS user switches between App Store app and TestFlight preview build or conversely, then the users must recreate the connection profile by performing the following steps:
>
>   1. Click the hamburger menu and then click **Configuration**.
>   2. Delete the profile from the list and add the same profile again.

Major features of Citrix Secure Access client for macOS/iOS

- **Password tokens:** A password token is a 6-digit code which is an alternative to Secondary Password Services such as VIP, OKTA. This code uses the Time-based One Time Password (T-OTP) protocol to generate the OTP code similar to services such as Google Authenticator and Microsoft Authenticator. Users are prompted for two passwords during authentication to NetScaler Gateway for a given Active Directory user. The second factor is a changing six-digit code that users copy from a registered third-party service such as Google or Microsoft Authenticator into the desktop browser. Users must first register for T-OTP on the NetScaler appliance. For registration steps, refer CTX228454. On the app, users can add the OTP feature by scanning the QR Code generated on NetScaler or manually entering the TOTP secret. OTP Tokens once added show up on the Password Tokens segment on the user interface.

To improve the experience, adding an OTP prompts the user to create a VPN profile automatically. Users can take advantage of this VPN profile to connect to the VPN directly from their iOS devices.

Citrix Secure Access client for macOS/iOS can be used to scan the QR code while registering for native OTP support.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway Push notification functionality is available only to the Citrix Secure Access for macOS/iOS users.

- **Push notification:** NetScaler Gateway sends push notification on your registered mobile device for a simplified two-factor authentication experience. Instead of launching Citrix Secure Access client for macOS/iOS to provide the second factor OTP on the NetScaler logon page, you can validate your identity by providing your Device PIN/Touch ID/ Face ID for the registered device.

Once you register your device for Push notification, you can also use the device for native OTP support using Citrix Secure Access for macOS/iOS. Registration for Push Notifications is transparent to the user. When users register TOTP, the device is also registered for Push Notifications if NetScaler supports it.

Release notes for the macOS clients

October 7, 2026

The release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes include one or more of the following sections:

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

Known issues: The issues that exist in the current release and their workarounds, wherever applicable.

> **Important information:**
>
> - EPA clients are supported on macOS 10.13, 10.14, 10.15, 11.x, 12.x, 13.x, 14.x, and 15.x versions.
> - EPA clients are supported on the NetScaler 12.1, 13.0, 13.1, and 14.1 versions.
> - Citrix Secure Access for macOS/iOS 24.06.1 and later releases address the TunnelVision vulnerabilities described in CVE-2024-3661.

V25.11.3 (Oct 05, 2026)

> **Important:**
>
> This build is only available in the App Store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

This release addresses issues to improve the overall performance, security, and stability.

V26.09.1.1 (Sep 24, 2026)

What's new

- This release introduces day-zero support for macOS 27, and includes performance and stability fixes.
- EPA libraries are updated to 26.8.1.0 (OPSWAT OESIS library version 4.3.5914.0).

V26.08.1.1 (Aug 24, 2026)

> **Important:**
>
> This build is only available in the Citrix Downloads page.

What's new

- This release addresses some issues to improve the overall performance and stability.
- EPA libraries are updated to 26.7.1.0 (OPSWAT OESIS library version 4.3.5733.0).

V26.06.1.1 (Jul 14, 2026)

> **Important:**
>
> This build is only available in the Citrix Downloads page.

What's new

- This release addresses some issues to improve the overall performance and stability.
- EPA libraries are updated to 26.5.1.0 (OPSWAT OESIS library version 4.3.5495.0).

Fixed issues

- SSH termination and direct traffic access issues might occur when Citrix Secure Access is connected and contextual routing is enabled.

  [NSHELP-40828]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Users might experience a failure to re-establish the connection when switching networks.

  [NSHELP-44311]

V26.04.1.1 (Apr 28, 2026)

> **Important:**
>
> The 26.04.1.1 build is available in the Citrix Downloads page.

What's new

- **Custom workspace domains for accessing applications**

  Citrix Secure Access client now supports custom workspace domains. This feature allows organizations to provide users with access to SaaS and private web applications through a branded, organization-owned domain (for example, `workspace.company.com`) instead of the default `*.cloud.com` domain. Admins can configure a custom domain as the authentication and access endpoint for browser-based applications delivered via Chrome Enterprise Premium and Citrix Secure Private Access. End users benefit from a seamless, branded experience while organizations gain greater control over access and security. For details, see Custom workspace domains for accessing apps.

  [CTXENG-65830]

- This release addresses issues to improve the overall performance and stability.

Fixed issues

- Mac devices disconnect from the Citrix Secure Access client when the `enable_vpn_dnstruncate_fix` configuration parameter is set to 0, resulting in VPN stability and user connectivity issues.

  [NSHELP-41139]

- EPA libraries are updated to 26.3.1.0 (OPSWAT OESIS library version 4.3.5186.0).

  [CSACLIENTS-16302]

V25.11.2 (Apr 08, 2026)

> **Important:**
>
> This build is only available in the App Store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

This release addresses issues to improve the overall performance, security, and stability.

V26.01.1.1 (Feb 09, 2026)

What's new

- **Auto Update feature support**

  The Citrix Secure Access application for macOS can now automatically update the client to the latest available version through an Auto Update feature that provides the following functionalities:

  - Periodically checks for updates.
  - Updates the app after notifying the user automatically.

  This feature is not enabled by default. To enable Auto Update support, contact Citrix Support. For more information, see the Auto Update support for macOS.

  > **Note:**
  >
  > Because the Auto Update feature is introduced in the version 26.01.1.1, the administrators can use this feature in the subsequent releases.

  [CSACLIENTS-16129]

- EPA libraries are updated to 26.1.1.0 (OPSWAT OESIS library version 4.3.4910.0).

  [CSACLIENTS-15816]

V25.11.1 (Dec 10, 2025)

> **Important:**
>
> The 25.11.1 build is available in the App store.

What's new

- EPA libraries are updated to 25.10.1.0 (OPSWAT OESIS library version 4.3.4523.0).

  [CSACLIENTS-15726]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The Citrix Secure Access client crashes intermittently due to incorrect DNS handling.

  [NSHELP-40828]

- Users might be unable to access intranet applications through the Citrix Secure Access app if the DNS response contains CNAME records. To enable CNAME record handling for the Citrix Secure Access client, contact Citrix Support.

  [SPAHELP-543]

Known issues

- On macOS 26 devices, the Citrix Secure Access application might repeatedly prompt for file system permissions after a first-time installation. Prompts can appear during operations such as establishing VPN connections or performing EPA checks. This behavior is due to a macOS issue and is not caused by the Citrix Secure Access application.

  [CSACLIENTS-16072]

V25.11.1.1 (Dec 05, 2025)

> **Important:**
>
> The 25.11.1.1 build is available in the Citrix Downloads page.

What's new

- **EPA client plug-in integration with the Citrix Secure Access application**

  The macOS Citrix Secure Access application, distributed as a .pkg file, now includes the EPA client plug-in. This means the plug-in is automatically installed when users install the application.

  [CSACLIENTS-15140]

- **Enhanced client certificate authentication**

  During client certificate authentication, Citrix Secure Access automatically selects the client certificate based on the CA certificates configured on NetScaler Gateway. For more information, see Configuring Client Certificate Authentication.

  [CSACLIENTS-15840]

- EPA libraries are updated to 25.10.1.0 (OPSWAT OESIS library version 4.3.4523.0).

  [CSACLIENTS-15726]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The Citrix Secure Access client crashes intermittently due to incorrect DNS handling.

  [NSHELP-40828]

- Users might be unable to access intranet applications through the Citrix Secure Access app if the DNS response contains CNAME records. To enable CNAME record handling for the Citrix Secure Access client, contact Citrix Support.

  [SPAHELP-543]

Known issues

- On macOS 26 devices, the Citrix Secure Access application might repeatedly prompt for file system permissions after a first-time installation. Prompts can appear during operations such as establishing VPN connections or performing EPA checks. This behavior is due to a macOS issue and is not caused by the Citrix Secure Access application.

  [CSACLIENTS-16072]

V25.08.1.2 (Oct 23, 2025)

> **Important:**
>
> The build 25.08.1.2 is available in the Citrix Downloads page.

What's new

- **PureAuth app support on the Citrix Secure Access client**

  The Citrix Secure Access client now supports PureAuth app launch on macOS devices when configured for authentication.

  [CSACLIENTS-15719]

V25.08.2 (Oct 22, 2025)

> **Important:**
>
> The build 25.08.2 is available in the App Store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

- **PureAuth app support on the Citrix Secure Access client**

  The Citrix Secure Access client now supports PureAuth app launch on macOS devices when configured for authentication.

  [CSACLIENTS-15719]

V25.08.1.1 and V25.08.1 (Sep 17, 2025)

> **Important:**
>
> - If you are using the latest Apple OS versions such as macOS 26 (Tahoe) and later, then we recommend that you upgrade to the Citrix Secure Access client version 25.08.1.1/25.08.1 or later. For more information about the NetScaler Gateway client software requirements, see System requirements.
> - The build 25.08.1.1 is available in the Citrix Downloads page and the build 25.08.1 is available in the App Store.

What's new

- **Route TCP DNS queries to the application-specific resource location**

  The TCP DNS queries for specific host names can now be routed directly to the resource location configured in the corresponding application. This routing improves application performance by ensuring that DNS queries reach the most relevant resource location. Previously, all TCP DNS queries were, by default, routed to the geographically closest resource location, regardless of the application's actual location.

  [CSACLIENTS-14336]

- **SNI support for the Citrix Secure Access client**

  The Citrix Secure Access client now sends the Server Name Indication (SNI) field as part of the TLS handshake. This feature is enabled by default. To disable SNI support, contact Citrix Support.

  [CSACLIENTS-15361]

- **Okta Verify app support on the Citrix Secure Access client**

  The Citrix Secure Access client now supports the Okta Verify app launch on macOS devices when configured for authentication.

  [CSACLIENTS-15359]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- EPA libraries are updated to 25.08.1.0 (OPSWAT OESIS library version 4.3.4253.0).

  [CSACLIENTS-15423]

V25.07.1 (Aug 12, 2025)

> **Important:**
>
> This build is only available in the App Store.

What's new

- **Support for multi-workspace URLs**

  The Citrix Secure Access client for macOS now supports multi-workspace URLs, allowing administrators to configure multiple access points within the Citrix Cloud environment. This feature is useful for enterprises that must provide different access URLs for various user groups, such as HR, IT, contractors, or vendors. For more information, see Configure Workspace URLs.

  [CSACLIENTS-13970]

- EPA libraries are updated to 25.07.1.0 (OPSWAT OESIS library version 4.3.4141.0).

  [CSACLIENTS-15064]

V25.07.1.1 (Aug 12, 2025)

> **Important:**
>
> This build is only available in the Citrix Downloads page.

What's new

- **Support for multi-workspace URLs**

  The Citrix Secure Access client now supports multi-workspace URLs, allowing administrators to configure multiple access points within the Citrix Cloud environment. This feature is useful for enterprises that must provide different access URLs for various user groups, such as HR, IT, contractors, or vendors. For more information, see Configure Workspace URLs.

  [CSACLIENTS-13970]

- EPA libraries are updated to 25.07.1.0 (OPSWAT OESIS library version 4.3.4141.0).

  [CSACLIENTS-15064]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V25.06.1.2 (Jul 16, 2025)

> **Important:**
>
> This build is only available in the Citrix Downloads page.

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.06.2 (Jul 10, 2025)

> **Important:**
>
> This build is only available in the App Store.

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.06.1.1 (Jul 09, 2025)

> **Important:**
>
> This build is released for the Citrix Secure Access client for macOS and is only available in the Citrix Downloads page.

What's new

- **Support for the Citrix Secure Access client for macOS**

  You can now download and install the application using either the package (`.pkg`) file available at Citrix Downloads or from the App Store. The `.pkg` file can be installed either manually or using management tools like Jamf and Intune.

  Prerequisites

  Before installing the `.pkg` file for the Citrix Secure Access app, ensure that the following prerequisites are fulfilled:

  - The Mac computer is running on macOS 13.0 or later.
  - The user has administrator privileges on the Mac computer. On managed machines, administrators must ensure that application installation permissions are enabled and the system extension with the identifier "com.citrix.NSG.macos.app.vpnplugin"is activated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Log out of the Citrix Secure Access app if it's currently running.
- Delete any previously installed App Store version of the Citrix Secure Access app.

How to install the Citrix Secure Access app on macOS:

> **Important**
>
> The Citrix Secure Access app's `.pkg` file uses the system extension with the identifier "com.citrix.NSG.macos.app.vpnplugin"for VPN connections. For client certificate authentication, certificates must be installed in the **System Keychain** because macOS system extensions cannot access certificates from the **login Keychain**.

1. Download the `.pkg` file from Citrix Downloads.
2. Install the application using the management tool (Jamf or Intune) or manually. To install the application manually, double-click the `.pkg` file and follow the on-screen instructions.

First-time setup:

After installing the Citrix Secure Access app, perform the following instructions to use the Citrix Secure Access app from your macOS device:

1. Open the **Applications** folder and double-click the Citrix Secure Access app icon to launch it.
2. On the first launch, the system prompts for permission to install the system extension. Click **OK** on the system prompt.

   If the system prompt does not appear, go to **System Settings** to enable the installation of the system extension with the identifier "com.citrix.NSG.macos.app.vpnplugin".

   - For macOS 14.x, the **System Settings** option is under the **Privacy & Security** tab.
   - For macOS 15.x and later, the **System Settings** option is under the **Login Items & Extensions** -> **Network Extensions**.

[CSACLIENTS-14826]

V25.06.1 (Jul 09, 2025)

> **Important:**
>
> This build is only available in the App Store.

- EPA libraries are updated to 25.06.1.0 (OPSWAT OESIS library version 4.3.4025.0).

  [CSACLIENTS-14646]
- This release addresses some issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V25.03.4 (May 14, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.3 (May 12, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.2 (May 08, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.1 (Apr 10, 2025)

What's new

- **Hybrid data path support for Secure Private Access service**

  The Citrix Secure Access client now supports a hybrid data path in the Secure Private Access service, using both on-premises and cloud infrastructures to provide secure access to applications. You can configure applications to be routed either through the Cloud Connector or the on-premises NetScaler Gateway. For more information, see Hybrid data path for Secure Private Access service.

  [CSACLIENTS-12469]

- EPA libraries are updated to 25.03.1.0 (OPSWAT OESIS library version 4.3.3980.0).

  [CSACLIENTS-13799]

- This release addresses some issues to improve the overall performance and stability.

V25.02.1 (Mar 14, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The Citrix Secure Access client might fail to function with third-party Secure Web Gateways if the User-Agent string in the WebView used during sign-on does not include the correct identifier.

  [NSHELP-39147]

V25.01.2 (Feb 18, 2025)

What's new

- This release addresses some security-related issues and enhances the overall performance of the application.

V25.01.1 (Jan 16, 2025)

What's new

- **Server-initiated connection support from Secure Private Access**

  The Citrix Secure Access client for macOS now supports a server-initiated connection from Citrix Secure Private Access. This feature enables users to configure a policy that allows an application to open a TCP connection to the endpoint. For more information, see Support for server-to-client connections - Preview.

  [CSACLIENTS-9626]

- EPA libraries are updated to 25.01.13.16 (OPSWAT OESIS library version 4.3.3910.0).

  [CSACLIENTS-12925]

Fixed issues

- The Citrix Secure Access client on devices running macOS 15.2 and above might fail to complete the configured OPSWAT scans.

  [CSACLIENTS-13099]

V24.11.1 (Nov 25, 2024)

What's new

- **Monitor TCP application session activity in Citrix Director**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access client for macOS now sends TCP application session activity to Citrix Director for both cloud and on-premises deployments of Citrix Secure Private Access.

[CSACLIENTS-11081]

- **Monitor session activity events in Citrix Director**

  The Citrix Secure Access client for macOS now sends summarized session activity events such as successful app launches, app launch failures, and DNS failures, to Citrix Director for both cloud and on-premises deployments of Citrix Secure Private Access.

  [CSACLIENTS-11959]

- **Support for contextual access feature in Secure Private Access**

  The Citrix Secure Access client supports the contextual access feature that enables an admin to enforce ZTNA policies dynamically based on the user context like network location, geo location, and device posture. For more information, see Context-based app routing and resource locations selection.

  [CSACLIENTS-11580]

- EPA libraries are updated to 24.11.1.0 (OPSWAT OESIS library version 4.3.3820.0).

  [CSACLIENTS-12523]

V24.10.1 (Oct 17, 2024)

What's new

- **Support to exclude DNS traffic by Citrix Secure Access client**

  You can now configure the Citrix Secure Access client to exclude DNS traffic from being intercepted. For more information, see Exclude specific domain traffic from client interception.

  [CSACLIENTS-10237]

- EPA libraries are updated to 24.09.1.0 (OPSWAT OESIS library version 4.3.3750.0).

  [CSACLIENTS-11371]

- This release addresses some issues to improve the overall performance and stability.

V24.09.1 (Sep 16, 2024)

> **Important:**
>
> If you are using the latest Apple OS versions such as macOS 15 and later, then we recommend that you upgrade to Citrix Secure Access client version 24.09.1 or later. For more information

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> about the NetScaler Gateway client software requirements, see Citrix Secure Access client system requirements.

What's new

- **System notifications support for Secure Private Access**

  The Citrix Secure Access client now supports system notifications for on-premises deployment of Secure Private Access.

  [CSACLIENTS-10726]

- EPA libraries are updated to 24.08.1.0 (OPSWAT OESIS library version 4.3.3709.0).

  [CSACLIENTS-11369]

- This release addresses some issues to improve the overall performance and stability.

V24.08.1 (Aug 14, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.07.1 (Jul 15, 2024)

What's new

- EPA libraries are updated to 24.06.1.0 (OPSWAT OESIS library version 4.3.3612.0).

  [CSACLIENTS-10605]

- This release addresses some issues to improve the overall performance and stability.

V24.06.2 (Jun 27, 2024)

What's new

This release addresses the IPv6 login issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V24.06.1 (Jun 24, 2024)

What's new

- This release addresses the TunnelVision vulnerabilities described in CVE-2024-3661.

  [CSACLIENTS-10918]

- This release addresses some issues to improve the overall performance and stability.
- EPA libraries are updated to 24.05.2.0 (OPSWAT OESIS library version 4.3.3586.0).

  [CSACLIENTS-10601]

- **EPA scan to check Citrix Workspace™ app version**

  Citrix Secure Access supports a new EPA scan `CWA Version`, that verifies the Citrix Workspace version on macOS machines. For details about the supported EPA scans, see Expression strings.

  [CGOP-6422]

- **Interoperability enhancements with third-party secure web gateway**

  The User-Agent strings for Citrix Secure Access have been updated for an enhanced interoperability with third party Secure Web Gateways.

  [CSACLIENTS-8501]

Fixed issues

- Citrix Secure Access fails to bypass the VPN tunnel for the excluded apps, if a per-app VPN with reverse split tunneling is enabled.

  [CSACLIENTS-10340]

24.6.1 EPA client for macOS (Jun 18, 2024)

What's new

- **EPA scan to check Citrix Workspace app version**

  Citrix EPA client supports a new scan, "CWA Version", that verifies the Citrix Workspace version on macOS machines. For details about the supported EPA scans, see Expression strings.

  [AAUTH-4918]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V24.04.1 (Apr 18, 2024)

What's new

- EPA libraries are updated to 24.04.1.0 (OPSWAT OESIS library version 4.3.3503.0).

  [CSACLIENTS-9559]

- This release addresses some issues to improve the overall performance and stability.

V24.03.1 (Mar 14, 2024)

What's new

- EPA libraries are updated to 24.03.1.0 (OPSWAT OESIS library version 4.3.3460.0).
- **Automatic single sign-on (SSO) to Citrix Secure Access through Citrix Workspace app - Preview**

  Citrix Secure Access for macOS now supports automatic single sign on (SSO) to Citrix Secure Access when you log on to Citrix Workspace app. Ensure that you use Citrix Secure Access for macOS 24.03.1 and Citrix Workspace app for Mac 2402 and above, to leverage this functionality. This feature is supported only on cloud stores and not for on-premises stores.

  - For admin and end-user instructions, refer to Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for Mac - Preview.
  - For end-user instructions, refer to Automatic single sign-on to Citrix Secure Access via Citrix Workspace app.

  [CSACLIENTS-6321]

- **Overall performance and stability improvements**

  Citrix Secure Access client is enhanced with the following capability to improve the overall performance and stability:

  - An improved VPN connection resiliency with IPv6 gateways.

  [NSHELP-36903]

V24.02.1 (Feb 15, 2024)

What's new

- **Support for EPA scan operators on Mac clients**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access client for macOS now supports all the operators <, >, >=, <=, ==, and != on the EPA editor. Also, the **Mac OS** option is available as a separate option on the EPA editor (**Mac > Mac OS**). You can perform a product version scan of your macOS devices using these operators.

For details, see the **Note** section in Advanced Endpoint Analysis scans.

[CSACLIENTS-6462]

- EPA libraries are updated to 24.1.2.1 (OPSWAT OESIS library version 4.3.3405.0).

  [CSACLIENTS-8520]

- This release addresses some issues to improve the overall performance and stability.

24.1.5 EPA client for macOS (Feb 12, 2024)

What's new

- **EPA support for Mac devices with Apple silicon processor**

  Citrix EPA client now supports Mac devices that use the Apple silicon processor. Mac devices no longer require Rosetta to be installed to run the Citrix EPA client.

  [CSACLIENTS-8731]

- **Support for EPA scan operators on Mac clients**

  Citrix EPA client for Mac now supports the operators (<, >, >=, and <=) in the EPA expressions. Admins can configure EPA scans to allow a wide range of OS versions.

  For example, to allow the OS versions from 12.4 to 13.0, except 12.8, admins can configure the expression `version >= 12.4 && version <= 13.0 && version != 12.8`. This means that the macOS version must be from 12.4 to 13.0 but cannot be 12.8.

  For details, see Advanced Endpoint Analysis scans.

  [CSACLIENTS-6462]

V23.12.2 (20 Dec 2023)

What's new

This release addresses issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V23.12.1 (06 Dec 2023)

What's new

- EPA libraries are updated to 23.11.1.5 (OPSWAT OESIS library version 4.3.3318.0).

  [CSACLIENTS-8516]
- This release addresses other issues to improve the overall performance and stability.

V23.11.2 (01 Nov 2023)

What's new

EPA libraries are updated to 23.11.1.1 (OPSWAT OESIS library version 4.3.3279.0).

[CSACLIENTS-8515]

V23.11.1 (27 Oct 2023)

What's new

- EPA libraries are updated to 23.10.1.1 (OPSWAT OESIS library version 4.3.3246.0).
- This release addresses the following:
  - Connection issues with the Citrix Secure Private Access™ environment.
  - Other issues to improve the overall performance and stability.

V23.10.2 (17 Oct 2023)

This release addresses the IPv6 login issues.

V23.10.1 (09 Oct 2023)

What's new

- EPA libraries are updated to 23.9.1.2 (OPSWAT OESIS library version4.3.3221.0).
- **Support for Local LAN access**

  Citrix Secure Access for macOS now support the Local LAN access functionality of NetScaler Gateway. You can configure local LAN access so that once a VPN connection is established, end

© 1997–2026 Citrix Systems, Inc. All rights reserved.

users are either allowed to or blocked from accessing local LAN resources on their client devices. For more information, see the following:

- NetScaler Gateway admin configurations
- End user configurations - macOS

V23.09.1 (07 Sep 2023)

> **Important:**
>
> If you are using the latest Apple OS versions such as macOS 14 and later, then we recommend that you upgrade to Citrix Secure Access client version 23.09.1 or later. For more information about the NetScaler Gateway client software requirements, see Citrix Secure Access client system requirements.

What's new

- EPA libraries are updated to 1.3.9.9 (OPSWAT OESIS v4.3.3160).

  [CSACLIENTS-6547]

- **Secured connection insights on the UI**

  On the "Connections"screen of the Citrix Secure Access client UI, you can view the secured connection details. The details include the IP address, FQDN, destination port, and the duration of the connection. For more information, see Secured connection insights.

  [SPA-2364]

- **Reauthenticate with NetScaler Gateway after a VPN connection failure**

  Citrix Secure Access client for macOS now prompt you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the UI indicating that the connection to NetScaler Gateway is lost and that you must reauthenticate to resume the connection. For more information, see Reconnect to NetScaler Gateway from macOS after a VPN connection failure.

  [CSACLIENTS-6071]

V23.08.1 (24 Aug 2023)

What's new

- This release addresses issues that help to improve overall performance and stability.
- EPA libraries are updated to 1.3.9.9 (OPSWAT OESIS v4.3.3122).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

23.7.6 EPA client for macOS (10 Aug 2023)

This release addresses issues that help to improve overall performance and stability.

V23.07.1 (17 Jul 2023)

What's new

- **Enhancements to Logs page**

  The Logs page of Citrix Secure Access for macOS is enhanced with the following options:

  - Maximum number of log files: Specify the maximum number of log files that you want to add for log collection.
  - Email logs: Send the logs over email.

  For more information, see Send logs.

  [SPA-2365]

Fixed issues

When connecting to VPN, if you are prompted to select a certificate for authentication, then the authentication login screen appears behind the Citrix Secure Access client's home page.

[CSACLIENTS-455]

V23.06.1 (07 Jun 2023)

What's new

- **Help menu on the navigation bar**

  A Help menu is now added to the navigation bar of the Citrix Secure Access client. The options (Open Logs, Export Logs, Email Logs, and Clear Logs) in the Help menu can be used for debugging logs.

  An Email Logs option is introduced under the Help menu. It can be used to share the logs over email. For more information, see Send logs.

  [SPA-2361]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

In some cases, the DNS short name resolution fails on Citrix Secure Access for macOS.

[NSHELP-34568]

Known issues

In some cases, the excluded routes in reverse split-tunneling are tunneled.

[CGOP-24575]

V23.05.2 (11 May 2023)

Fixed issues

After an upgrade, the Citrix SSO for iOS client devices cannot establish per-app VPN connections.

[NSHELP-35224]

V23.05.1 (04 May 2023)

What's new

- EPA libraries are updated to 1.3.9.3 and OPSWAT libraries are updated to 4.3.2987.
- **Support for sending events to Citrix Analytics**

  Citrix Secure Access for macOS now supports sending events such as session creation, session termination, and app connection to Citrix Analytics service. These events are then logged in the Secure Private Access service dashboard.

  [SPA-2197]

Fixed issues

- When the users are connected to Citrix Secure Access or Citrix SSO, the "Connection Duration" field fails to display the time in the region-specific format.

  [CGOP-23587]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V23.04.1 (04 Apr 2023)

What's new

- EPA libraries are updated to 1.3.9.1 and OPSWAT libraries are updated to 4.3.2923.

V22.12.2 (27-Feb-2023)

What's new

- EPA libraries are updated to 1.3.8.9 (OPSWAT OESIS v4.3.2892.0).

V22.12.1 (07-Dec-2022)

This release addresses issues that help to improve overall performance and stability.

V22.11.1 (29-Nov-2022)

Fixed issues

- Transfer logon does not work for non-nFactor authentication with on-premises gateways.

  [CGOP-22729]

22.11.3 EPA plug-in for macOS (28-Nov-2022)

Fixed issues

- Citrix EPA plug-in for macOS crashes when GSLB is enabled on NetScaler.

  [CGOP-22722]

V22.10.1 (17-Nov-2022)

What's new

- The Citrix Endpoint Analysis plug-in now supports new MAC address validation expression where pattern sets can be created for the list of allowed IP addresses.

  [CGOP-22095]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- Sometimes, empty proxy settings in NetScaler Gateway release 13.0 or 13.1 causes Citrix SSO to create improper proxy settings.

  [NSHELP-31970]

- Sometimes, VPN clients fail to reconnect after a network outage or after the device wakes up from sleep mode.

  [NSHELP-32483]

- Sometimes, gateway connections fail when using IPv6 literals as the destination.

  [NSHELP-32876]

22.10.1 EPA plug-in for macOS (27-Oct-2022)

What's new

- The Citrix Endpoint Analysis plug-in now a supports new MAC address validation expression where pattern sets can be created for the list of allowed IP addresses.

  [CGOP-22098]

- The Citrix Endpoint Analysis plug-in sends duplicate consent alerts while handling private network access preflight requests from Google Chrome.

  [CGOP-21751]

V22.06.1 (20-Sep-2022)

What's new

- EPA libraries are updated to 4.3.2523.0 (1.3.7.5)

Fixed issues

- nFactor authentication with EPA scan does not work on the macOS clients.

  [NSHELP-32182 - macOS]

- On the Secure Access Agent home page for macOS, extra padding with white or black color appears on the left and top of the hamburger menu depending on the selected theme (light or dark).

  [CGOP-19353 - macOS]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When logging into the VPN, the WebView window minimizes on the first try if the device certificate is configured.

  [CGOP-19354 - macOS]

- Endpoint analysis does not work for the Citrix Secure Access app on the macOS client when GSLB is enabled on the NetScaler appliance.

  [CGOP-21634 - macOS]

- If there is a space in the configured application name and you try to access the app, the Enhanced Security Enabled popup does not show up on the macOS clients.

  [ACS-2632 - macOS]

- On a Mac device using Chrome, the VPN extension crashes while accessing two FQDNs.

  [NSHELP-32144]

- Citrix Secure Access crashes when an incorrect location value is received from the gateway. This can happen if the administrator defines a responder policy to redirect to another host.

  [NSHELP-32312]

- Direct connections to the resources outside of the tunnel established by Citrix Secure Access might fail if there is a significant delay or congestion.

  [NSHELP-31598]

V3.2.4.9 - EPA plug-in for macOS (01-Aug-2022)

Fixed issues

- Citrix Endpoint Analysis plug-in does not handle private network access preflight requests from the Google Chrome browser version 104.

  [CGOP-20709]

- Citrix Endpoint Analysis plug-in for macOS does not support GSLB.

  [CGOP-21543]

Known issues

- Citrix Endpoint Analysis plug-in for macOS displays a duplicate consent dialog box when started from the Google Chrome browser version 104. The users have to accept both the prompts.

  [CGOP-21751]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V22.03.1 (14-Jun-2022)

What's new

- EPA libraries are updated to 4.3.2393.0.

Fixed issues

- An extra DNS domain is added to the search list. This is because, when the split tunnel is set to "Split"or "Both"only the specified domains and their subdomains are NOT tunneled. If the specified domain is A.B.C, then B.C is also matched in addition to A.B.C and *.A.B.C.

  [CGOP-21657]

- HTTP/HTTPS proxy settings that do not use a PAC file are broken.

  [CGOP-21660]

V22.02.3 (24-Mar-2022)

What's new

- Citrix Secure Access for macOS resolves the FQDN of a service node on every TCP data connection from the client for the cloud workspace connections. Resolving the FQDN of a service node on every TCP data connection is not applicable for the on-premises gateway connections.

  [ACS-1068]

Fixed issues

- Sometimes, the Citrix Secure Access for macOS drops connections because of issues with some non-DNS protocols using port 53, such as STUN.

  [NSHELP-31004]

- The Citrix Secure Access app breaks some protocols when the server sends data before the client, immediately after the connection is established.

  [NSHELP-29374]

- If the user closes the authentication window of the Citrix Secure Access client for macOS without completing the authentication, then subsequent attempts to connect to the server fail until the app is restarted.

  [ACS-2415]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Secure Access client for macOS is now bundled with OPSWAT library version 4.3.2367.0

  [NSHELP-30802]

- Citrix Secure Access for macOS takes a longer time than expected to run the post-authentication EPA check.

  [NSHELP-29118]

Known issues

- Citrix Secure Access app for macOS logs out one minute after the already connected Citrix Secure Private Access service region becomes unreachable. However, this does not affect the on-premises gateway connections.

  [ACS-2715]

V22.02.2 (15-Feb-2022)

Fixed issues

- Multiple pop-ups are displayed when a user tries to access an unsubscribed Web app from Citrix Secure Access for macOS.

  [ACS-2406]

V1.4.1 (28-Jan-2022)

what's new

- The Citrix SSO app for macOS is now rebranded as Citrix Secure Access.

  [ACS-1092]

Fixed issues

- Client certificate authentication fails if the authentication server requests for the client certificate multiple times in the same web view session.

  [CGOP-20388]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix SSO fails to establish a VPN connection if the server certificate has only an IP address for common name because of a proxy in between the client and the ADC.

  [CGOP-20390]

- EPA scan for checking the antivirus last full system scan fails on macOS.

  [NSHELP-29571]

- Sometimes, the Citrix SSO app crashes while handling large DNS packets.

  [NSHELP-29133]

V1.4.0 (17-Nov-2021)

Fixed issues

- Sometimes, the server validation code fails when the server certificate is trusted. As a result, end users cannot access the gateway.

  [NSHELP-28942]

- Citrix SSO fails to re-establish the VPN connection after network disruption.

  [CGOP-19988]

V1.3.13 (05-Nov-2021)

Fixed issues

- You might experience failures when filtering sessions for managed versus unmanaged VPNs. The initial requests to establish the session are missing the "ManagedVpn"information in the User-Agent header.

  [CGOP-19561]

V1.3.12 (21-Oct-2021)

Fixed issues

- Client certificate authentication fails for Citrix SSO for macOS if there are no client certificates in the macOS Keychain.

  [NSHELP-28551]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix SSO app crashes intermittently when receiving notifications.

  [CGOP-19363]

- The VPN extension might crash when the “isFeatureEnabled”parameter is called to check a feature flag.

  [CGOP-19360]

- The gateway VPN extension crashes if the DTLS protocol has an empty payload.

  [CGOP-19361]

- The SSO app crashes intermittently when the device wakes up from the sleep mode and the VPN is connected.

  [CGOP-19362]

V1.3.11 (17-Sep-2021)

Fixed issues

- EPA scan for firewall check fails for macOS devices using Citrix SSO.

  [CGOP-19271]

- Citrix SSO crashes in an iOS 12 device when legacy authentication or Intune Network Access Compliance (NAC) is configured.

  [CGOP-19261]

V1.3.10 (31-Aug-2021)

What’s new

- Citrix SSO for macOS is now bundled with OPSWAT library version 4.3.1977.0.

  [NSHELP-28467]

V1.3.9 (13-Aug-2021)

Fixed issues

- On some systems with HTTP proxy software installed, the NetScaler Gateway IP address shows up internally as 127.0.0.1 thus preventing tunnel establishment.

  [CGOP-18538]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix SSO cannot connect to systems where the DNS name does not match the common name in the server certificate. Citrix SSO now checks for the subject alternative names, and connects correctly.

  [NSHELP-28348]

V1.3.8 (07-Jul-2021)

What's new

- Citrix SSO for macOS is compatible with versions 10.15 (Catalina) and higher only.

  [CGOP-12555]

- Starting from Citrix SSO for macOS version 1.3.8, the EPA libraries are embedded within the app and are not downloaded from the NetScaler Gateway server. The current embedded EPA library version is 1.3.5.1.

  [NSHELP-26838]

Release notes for the iOS clients

October 7, 2026

The release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes include one or more of the following sections:

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

Known issues: The issues that exist in the current release and their workarounds, wherever applicable.

> **Important information:**
>
> - Citrix Secure Access for macOS/iOS 24.06.1 and later releases address the TunnelVision vulnerabilities described in CVE-2024-3661.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V26.09.1 (Oct 05, 2026)

What's new

- This release addresses issues to improve the overall performance, security, and stability.

V26.08.1 (Sep 02, 2026)

What's new

- This release addresses issues to improve the overall performance, security, and stability.

V26.06.1 (Jul 22, 2026)

Fixed issues

- Users might experience a failure to re-establish the connection when switching networks.

  [NSHELP-44311]

V26.05.2 (Jul 01, 2026)

What's new

- This release addresses some issues to improve the overall performance and stability.

V26.05.1 (Jun 30, 2026)

What's new

- This release addresses some issues to improve the overall performance and stability.

V26.04.1 (Apr 28, 2026)

What's new

- **Custom workspace domains for accessing applications**

  Citrix Secure Access client now supports custom workspace domains. This feature allows organizations to provide users with access to SaaS and private web applications through a branded,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

organization-owned domain (for example, workspace.company.com) instead of the default `*.cloud.com` domain. Admins can configure a custom domain as the authentication and access endpoint for browser-based applications delivered via Citrix Secure Private Access. End users benefit from a seamless, branded experience while organizations gain greater control over access and security. For details, see Custom workspace domains for accessing apps.

[CTXENG-65830]

- This release addresses some issues to improve the overall performance and stability.

V26.03.1 (Mar 24, 2026)

What's new

- **Single sign-on (SSO) support for Citrix Secure Access on iOS**

  Citrix Secure Access for iOS 26.03.1 and later supports Single Sign-On (SSO). When a user signs in to the Citrix Workspace app and then initiates a connection in the Citrix Secure Access app, they are logged in automatically without needing to re-enter credentials. This enables seamless access to Secure Private Access URLs and provides a unified experience.

  To enable this feature, contact Citrix Support.

  For more information see, Automatic single sign-on to Citrix Secure Access through Citrix Workspace app for iOS.

  [CTXENG-72243]

- Citrix Secure Access app for iOS now supports DNS suffixes. To enable this feature, contact Citrix Support.

  [CTXENG-72263]

Fixed issues

- Users might experience a packet drop when the device wakes up until the DTLS connection is re-established.

  [NSHELP-42287]

V25.11.1 (Dec 10, 2025)

What's new

- **Support for multi-workspace URLs**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access client for iOS now supports multi-workspace URLs, allowing administrators to configure multiple access points within the Citrix Cloud environment. This feature is useful for enterprises that must provide different access URLs for various user groups, such as HR, IT, contractors, or vendors. For more information, see Configure Workspace URLs.

[CSACLIENTS-15272]

- **Monitor session activity events in Citrix Director**

  The Citrix Secure Access client for iOS now sends summarized session activity events such as successful app launches, app launch failures, and DNS failures, to Citrix Director for both cloud and on-premises deployments of Citrix Secure Private Access.

  [CSACLIENTS-15369]

V25.08.1 (Sep 18, 2025)

> **Important:**
>
> If you are using the latest Apple OS versions such as iOS 26 and later, then we recommend that you upgrade to Citrix Secure Access client version 25.08.1 or later. For more information about the NetScaler Gateway client software requirements, see System requirements.

What's new

- **Support for Citrix Secure Private Access**

  The Citrix Secure Access client for iOS now supports Citrix Secure Private Access deployments. This enables administrators to enforce ZTNA policies, ensuring users securely access corporate applications and web resources from iOS devices. For more information, see Citrix Secure Private Access for mobile devices.

  [CSACLIENTS-15178]

- **Route TCP DNS queries to the application-specific resource location**

  The TCP DNS queries for specific host names can now be routed directly to the resource location configured in the corresponding application. This routing improves application performance by ensuring that DNS queries reach the most relevant resource location. Previously, all TCP DNS queries were, by default, routed to the geographically closest resource location, regardless of the application's actual location.

  [CSACLIENTS-14336]

- **SNI support for the Citrix Secure Access client**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access client now sends the Server Name Indication (SNI) field as part of the TLS handshake. This feature is enabled by default. To disable SNI support, contact Citrix Support.

[CSACLIENTS-15361]

V25.07.1 (Aug 12, 2025)

What's new

- **Dropping of QUIC handshake packets**

  The Citrix Secure Access client for iOS now drops Quick UDP Internet Connections (QUIC) handshake packets, enabling a faster switch to TCP connection establishment. To enable this feature, contact Citrix Support.

  [CSACLIENTS-14921]

V25.06.2 (Jul 11, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.06.1 (Jul 09, 2025)

- This release addresses some issues to improve the overall performance and stability.

V25.03.4 (Jun 02, 2025)

Fixed issues

- External applications might load slowly or fail to load when the per-app VPN is enabled in the Citrix Secure Access client for iOS.

  [NSHELP-39673]

- iOS device users might be prompted to transfer their login when both of the following conditions are met:

  - An Intranet IP address (IIP) is assigned to the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The previous session remains active during network transitions, such as switching between Wi-Fi and mobile data.

Contact Citrix Support to enable the auto-transfer login feature, which eliminates the need for manual prompts during session transfers.

[NSHELP-39727]

V25.03.3 (May 12, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.2 (May 08, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.1 (Apr 10, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.02.1 (Mar 14, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.01.1 (Jan 16, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- The Citrix Secure Access client on devices running macOS 15.2 and above might fail to complete the configured OPSWAT scans.

  [CSACLIENTS-13099]

V24.11.1 (Nov 25, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.10.1 (Oct 17, 2024)

What's new

- **Support to exclude DNS traffic by Citrix Secure Access client**

  You can now configure the Citrix Secure Access client to exclude DNS traffic from being intercepted. For more information, see Exclude specific domain traffic from client interception.

  [CSACLIENTS-10237]

- This release addresses some issues to improve the overall performance and stability.

V24.09.1 (Sep 16, 2024)

> **Important:**
>
> If you are using the latest Apple OS versions such as iOS 18 and later, then we recommend that you upgrade to Citrix Secure Access client version 24.09.1 or later. For more information about the NetScaler Gateway client software requirements, see Citrix Secure Access client system requirements.

What's new

- This release addresses some issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V24.08.1 (Aug 14, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.07.1 (Jul 15, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.06.2 (Jun 27, 2024)

What's new

This release addresses the IPv6 login issues.

V24.06.1 (Jun 24, 2024)

What's new

- This release addresses the TunnelVision vulnerabilities described in CVE-2024-3661.

  [CSACLIENTS-10918]

- This release addresses some issues to improve the overall performance and stability.
- **Interoperability enhancements with third-party secure web gateway**

  The User-Agent strings for Citrix Secure Access have been updated for an enhanced interoperability with third party secure web gateways.

  [CSACLIENTS-8501]

Fixed issues

- Citrix Secure Access fails to bypass the VPN tunnel for the excluded apps, if per-app VPN with reverse split tunneling is enabled.

  [CSACLIENTS-10340]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V24.04.1 (Apr 18, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.03.1 (Mar 14, 2024)

What's new

- **Overall performance and stability improvements**

  Citrix Secure Access client is enhanced with the following capabilities to improve the overall performance and stability:

  - An increase in the number of the simultaneous connections that can be tunneled through a VPN.
  - An improved VPN connection resiliency with IPv6 gateways.

  [NSHELP-36903]

V24.02.1 (Feb 15, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V23.12.2 (20 Dec 2023)

What's new

This release addresses issues to improve the overall performance and stability.

V23.12.1 (06 Dec 2023)

What's new

- This release addresses other issues to improve the overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V23.11.1 (27 Oct 2023)

What's new

- Citrix SSO for iOS is now renamed to Citrix Secure Access. We are updating the UI screenshots in our documentation to reflect this name change.
- This release addresses the following:
  - Connection issues with the Citrix Secure Private Access™ environment.
  - Other issues to improve the overall performance and stability.

V23.10.2 (17 Oct 2023)

This release addresses the IPv6 login issues.

V23.10.1 (09 Oct 2023)

What's new

- **Support for Local LAN access**

  Citrix SSO for iOS now support the Local LAN access functionality of NetScaler Gateway. You can configure local LAN access so that once a VPN connection is established, end users are either allowed to or blocked from accessing local LAN resources on their client devices. For more information, see the following:

  - NetScaler Gateway admin configurations
  - End user configurations - iOS

V23.09.1 (07 Sep 2023)

> **Important:**
>
> If you are using the latest Apple OS versions such as iOS 17 and later, then we recommend that you upgrade to Citrix SSO version 23.09.1 or later. For more information about the NetScaler Gateway client software requirements, see Citrix Secure Access client system requirements.

What's new

- **Secured connection insights on the UI**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On the "Connections"screen of the Citrix Secure Access client UI, you can view the secured connection details. The details include the IP address, FQDN, destination port, and the duration of the connection. For more information, see Secured connection insights.

[SPA-2364]

- **Reauthenticate with NetScaler Gateway after a VPN connection failure**

  Citrix SSO for iOS now prompt you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the UI indicating that the connection to NetScaler Gateway is lost and that you must reauthenticate to resume the connection. For more information, see Reconnect to NetScaler Gateway from iOS after a VPN connection failure.

  [CSACLIENTS-6071]

V23.07.1 (17 Jul 2023)

What's new

- **Various options to share log files**

  The "Email Logs"option in Citrix SSO for iOS is now replaced with the "Share Logs"option. The compressed log files can now be shared through options such as email, chat, save to files, and so on.

  For more information, see Send logs.

  [CSACLIENTS-3834]

V23.06.1 (07 Jun 2023)

What's new

- **Help menu on the navigation bar**

  A Help menu is now added to the navigation bar of the Citrix Secure Access client. The options (Open Logs, Export Logs, Email Logs, and Clear Logs) in the Help menu can be used for debugging logs.

  An Email Logs option is introduced under the Help menu. It can be used to share the logs over email. For more information, see Send logs.

  [SPA-2361]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

In some cases, the DNS short name resolution fails on Citrix SSO for iOS.

[NSHELP-34568]

Known issues

In some cases, the excluded routes in reverse split-tunneling are tunneled.

[CGOP-24575]

V23.05.2 (11 May 2023)

Fixed issues

After an upgrade, the Citrix SSO for iOS client devices cannot establish per-app VPN connections.

[NSHELP-35224]

V23.05.1 (04 May 2023)

What's new

- **Support for sending events to Citrix Analytics**

  Citrix Secure Access for macOS now supports sending events such as session creation, session termination, and app connection to Citrix Analytics service. These events are then logged in the Secure Private Access service dashboard.

  [SPA-2197]

Fixed issues

- When the users are connected to Citrix Secure Access or Citrix SSO, the "Connection Duration" field fails to display the time in the region-specific format.

  [CGOP-23587]

V22.12.1 (07-Dec-2022)

This release addresses issues that help to improve overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V22.11.1 (29-Nov-2022)

Fixed issues

- Transfer logon does not work for non-nFactor authentication with on-premises gateways.

  [CGOP-22729]

V22.10.1 (17-Nov-2022)

What's new

- The Citrix Endpoint Analysis plug-in now supports new MAC address validation expression where pattern sets can be created for the list of allowed IP addresses.

  [CGOP-22095]

Fixed issues

- Sometimes, empty proxy settings in NetScaler Gateway release 13.0 or 13.1 causes Citrix SSO to create improper proxy settings.

  [NSHELP-31970]

- Sometimes, VPN clients fail to reconnect after a network outage or after the device wakes up from sleep mode.

  [NSHELP-32483]

- Sometimes, gateway connections fail when using IPv6 literals as the destination.

  [NSHELP-32876]

V22.06.1 (20-Sep-2022)

Fixed issues

- nFactor authentication with an optional client certificate fails when there are no appropriate client certificates on the device.

  [NSHELP-32127 - iOS]

- Citrix Secure Access crashes when an incorrect location value is received from the gateway. This can happen if the administrator defines a responder policy to redirect to another host.

  [NSHELP-32312]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Direct connections to the resources outside of the tunnel established by Citrix Secure Access might fail if there is a significant delay or congestion.

  [NSHELP-31598]

V22.03.1 (14-Jun-2022)

Fixed issues

- An extra DNS domain is added to the search list. This is because, when the split tunnel is set to "Split"or "Both"only the specified domains and their subdomains are NOT tunneled. If the specified domain is A.B.C, then B.C is also matched in addition to A.B.C and *.A.B.C.

  [CGOP-21657]

- HTTP/HTTPS proxy settings that do not use a PAC file are broken.

  [CGOP-21660]

V22.02.3 (24-Mar-2022)

Fixed issues

- The Citrix Secure Access app breaks some protocols when the server sends data before the client, immediately after the connection is established.

  [NSHELP-29374]

V22.01.1 (08-Feb-2022)

Fixed issues

- Per-App VPN connections with Citrix SSO for iOS devices fail to connect to NetScaler Gateway on ports other than 443.

  [NSHELP-30653]

Fixed issues

- Client certificate authentication fails if the authentication server requests for the client certificate multiple times in the same web view session.

  [CGOP-20388]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix SSO fails to establish a VPN connection if the server certificate has only an IP address for common name because of a proxy in between the client and the ADC.

  [CGOP-20390]

- EPA scan for checking the antivirus last full system scan fails on macOS.

  [NSHELP-29571]

- Sometimes, the Citrix SSO app crashes while handling large DNS packets.

  [NSHELP-29133]

V1.4.0 (17-Nov-2021)

Fixed issues

- Sometimes, the server validation code fails when the server certificate is trusted. As a result, end users cannot access the gateway.

  [NSHELP-28942]

- Citrix SSO fails to re-establish the VPN connection after network disruption.

  [CGOP-19988]

V1.3.13 (05-Nov-2021)

Fixed issues

- You might experience failures when filtering sessions for managed versus unmanaged VPNs. The initial requests to establish the session are missing the "ManagedVpn"information in the User-Agent header.

  [CGOP-19561]

V1.3.12 (21-Oct-2021)

Fixed issues

- The Citrix SSO app crashes intermittently when receiving notifications.

  [CGOP-19363]

- The VPN extension might crash when the "isFeatureEnabled"parameter is called to check a feature flag.

  [CGOP-19360]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The gateway VPN extension crashes if the DTLS protocol has an empty payload.

  [CGOP-19361]

- The SSO app crashes intermittently when the device wakes up from the sleep mode and the VPN is connected.

  [CGOP-19362]

V1.3.11 (17-Sep-2021)

Fixed issues

- Citrix SSO crashes in an iOS 12 device when legacy authentication or Intune Network Access Compliance (NAC) is configured.

  [CGOP-19261]

V1.3.9 (13-Aug-2021)

Fixed issues

- On some systems with HTTP proxy software installed, the NetScaler Gateway IP address shows up internally as 127.0.0.1 thus preventing tunnel establishment.

  [CGOP-18538]

- The setting "Block Untrusted Servers"does not work on systems that support non-English localization of Citrix SSO for iOS.

  [CGOP-18539]

- Citrix SSO cannot connect to systems where the DNS name does not match the common name in the server certificate. Citrix SSO now checks for the subject alternative names, and connects correctly.

  [NSHELP-28348]

Set up Citrix Secure Access™ for iOS users

September 25, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> - Citrix SSO for iOS is now renamed to Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change. You might notice Citrix SSO references used in the documentation during this transition period.
> - VPN cannot be used on iOS 12 and later. To continue to VPN, use Citrix Secure Access.

For the list of some commonly used features supported by the Citrix Secure Access for iOS, see Citrix Secure Access client features supported in NetScaler Gateway.

Compatibility with MDM products

Citrix Secure Access (macOS/iOS) are compatible with most MDM providers such as Citrix Endpoint Management (formerly XenMobile), Microsoft Intune and so on.

Citrix Secure Access (macOS/iOS) also support a feature called Network Access Control (NAC). For more information on NAC, see Configure Network Access Control device check for NetScaler Gateway virtual server for single factor login. With NAC, MDM administrators can enforce end user device compliance before connecting to the NetScaler appliance. NAC on Citrix Secure Access (macOS/iOS) requires an MDM server such as Citrix Endpoint Management or Intune and NetScaler.

> **Note:**
>
> To use Citrix Secure Access client on macOS/iOS with NetScaler Gateway VPN without MDM, you must add a VPN configuration. You can add the VPN configuration on iOS from Citrix Secure Access (macOS/iOS) home page.

Configure an MDM managed VPN profile for Citrix Secure Access client (macOS/iOS)

The following section captures step-by-step instructions to configure both device-wide and per-app VPN profiles for the Citrix Secure Access client (macOS/iOS) using Citrix Endpoint Management (formerly XenMobile) as an example. Other MDM solutions can use this document as reference when working with Citrix Secure Access (macOS/iOS).

> **Note:**
>
> This section explains the configuration steps for a basic Device-wide and Per-App VPN profile. Also you can configure On-Demand, Proxies by following the Citrix Endpoint Management™ (formerly XenMobile) documentation or Apple's MDM VPN payload configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Device level VPN profiles

Device level VPN profiles are used to set up a system wide VPN. Traffic from all apps and services is tunneled to NetScaler Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split tunnel) defined in NetScaler.

To configure a device level VPN on Citrix Endpoint Management Perform the following steps to configure a device level VPN on Citrix Endpoint Management.

1. On the Citrix Endpoint Management MDM console, navigate to **Configure** > **Device Policies** > **Add New Policy**.
2. Select **iOS** on the left Policy Platform pane. Select **VPN** on the right pane.
3. On the **Policy Info** page, enter a valid policy name and description and click **Next**.
4. On the **VPN Policy** page for iOS, type a valid connection name and choose **Custom SSL** in **Connection Type**.

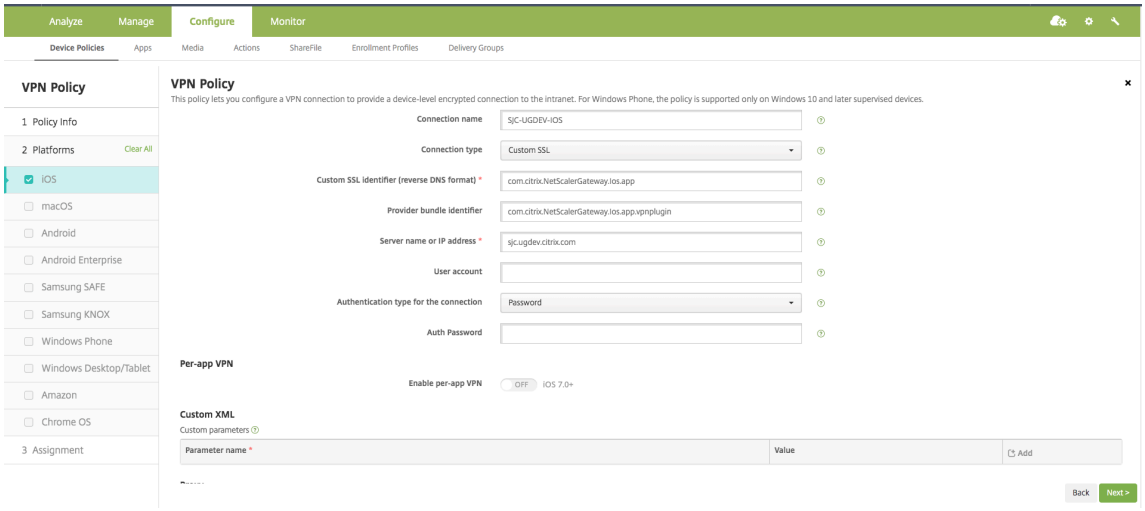
   In the MDM VPN payload, the connection name corresponds to the **UserDefinedName** key and **VPN Type Key** must be set to **VPN**.
5. In **Custom SSL identifier (reverse DNS format)**, enter **com.citrix.NetScalerGateway.ios.app**. This is the bundle identifier for the Citrix Secure Access on iOS.

   In the MDM VPN payload, the Custom SSL identifier corresponds to the **VPNSubType** key.
6. In **Provider bundle identifier** enter **com.citrix.NetScalerGateway.ios.app.vpnplugin**. This is the bundle identifier of the network extension contained in the Citrix Secure Access iOS app binary.

   In the MDM VPN payload, the provider bundle identifier corresponds to the **ProviderBundleIdentifier** key.
7. In **Server name or IP address** enter the IP address or FQDN (fully qualified domain name) of the NetScaler associated with this Citrix Endpoint Management instance.

   The remaining fields in the configuration page are optional. Configurations for these fields can be found in the Citrix Endpoint Management (formerly XenMobile®) documentation.
8. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Click **Save**.

Per-App VPN profiles

Per-App VPN profiles are used to set up the VPN for a specific application. Traffic from only the specific app is tunneled to NetScaler Gateway. The **Per-App VPN payload** supports all keys for Device-wide VPN plus a few other keys.

To configure a per-App level VPN on Citrix Endpoint Management Perform the following steps to configure a Per-App VPN:

1. Complete the device level VPN configuration on Citrix Endpoint Management.
2. Turn the **Enable Per-App VPN** switch ON in the Per-App VPN section.
3. Turn the **On-Demand Match App Enabled switch ON** if Citrix Secure Access (macOS/iOS) must be started automatically when the Match App is launched. This is recommended for most Per-App cases.

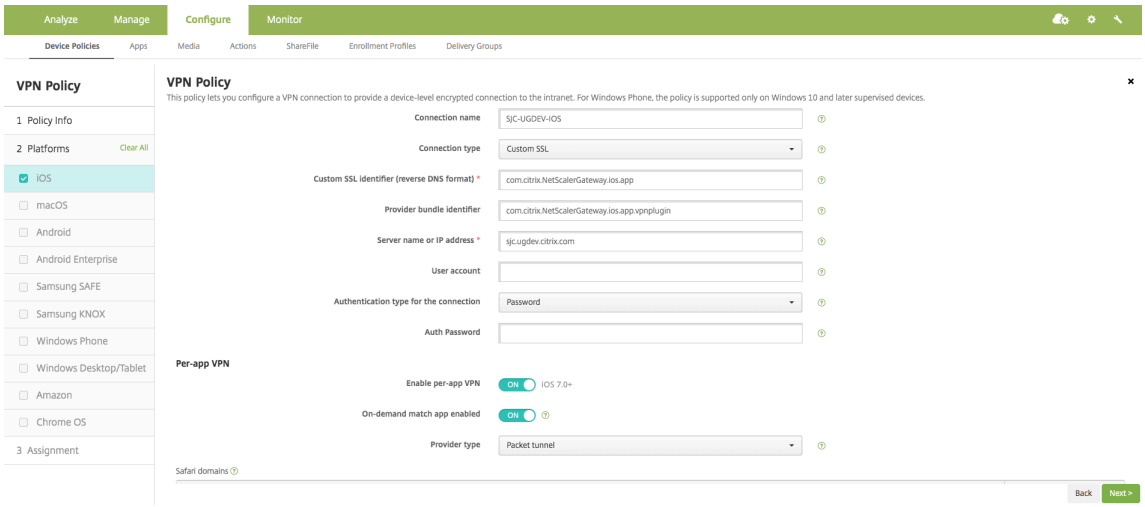
   In the MDM VPN payload, this field corresponds to the key **OnDemandMatchAppEnabled**.
4. In **Provider Type**, select **Packet Tunnel**.

   In the MDM VPN payload, this field corresponds to the key **Provider Type**.
5. Safari Domain configuration is optional. When a Safari domain is configured, Citrix Secure Access (macOS/iOS) starts automatically when users launch Safari and navigate to a URL that matches the one in the **Domain** field. This is not recommended if you want to restrict the VPN for a specific app.

   In the MDM VPN payload, this field corresponds to the key **SafariDomains**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The remaining fields in the configuration page are optional. Configurations for these fields can be found in the Citrix Endpoint Management (formerly XenMobile) documentation.



6. Click **Next.**
7. Click **Save**.

To associate this VPN profile to a specific App on the device, you must create an App Inventory policy and a credentials provider policy.

Configuring split tunnel in Per-App VPN

MDM customers can configure split tunnel in Per-App VPN for Citrix Secure Access (macOS/iOS). The following key/value pair must be added to the vendor configuration section of the VPN profile created on the MDM server.

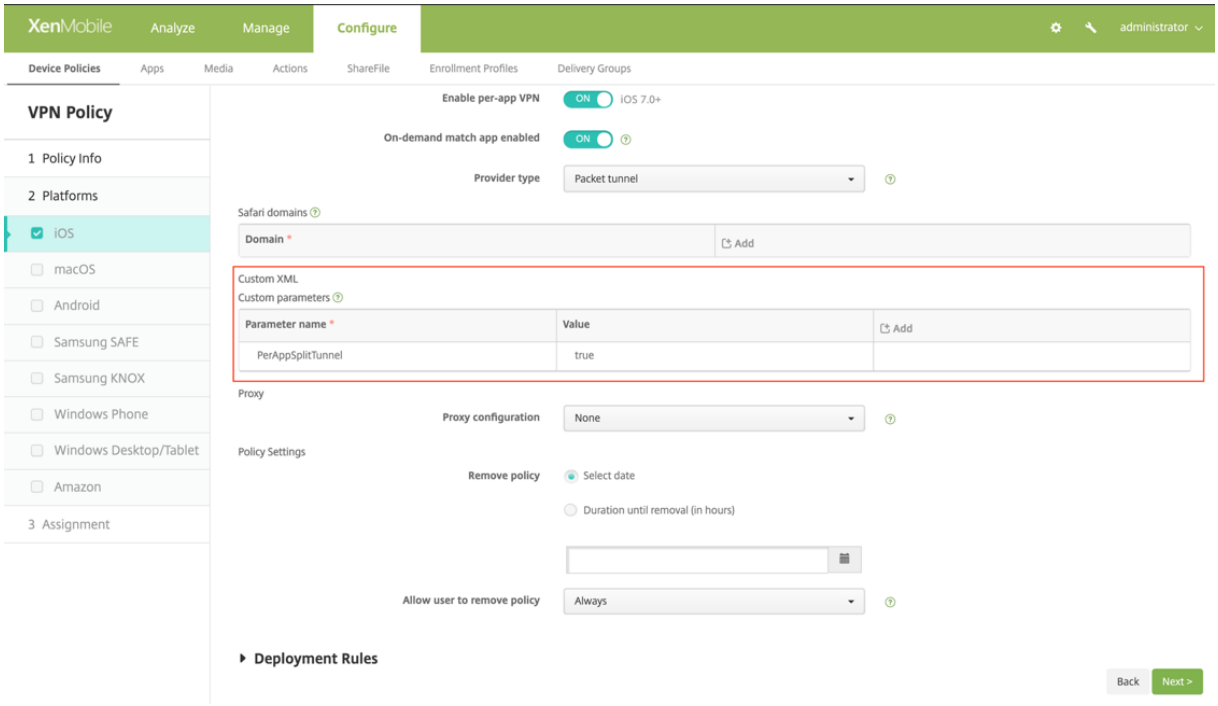
```
1  -  Key = "PerAppSplitTunnel"
2  -  Value = "true or 1 or yes"
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

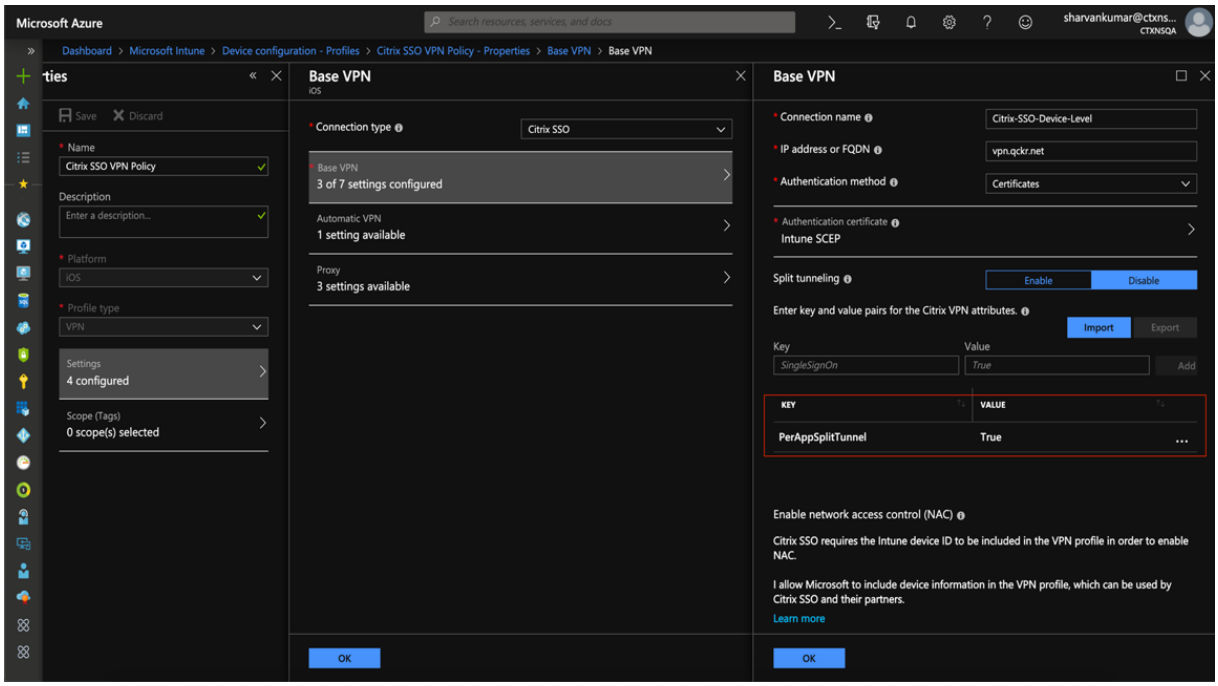
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.



Disabling user created VPN profiles

MDM customers can prevent users from manually creating VPN profiles from within Citrix Secure Access (macOS/iOS). To do this, the following key/value pair must be added to the vendor configuration

© 1997–2026 Citrix Systems, Inc. All rights reserved.

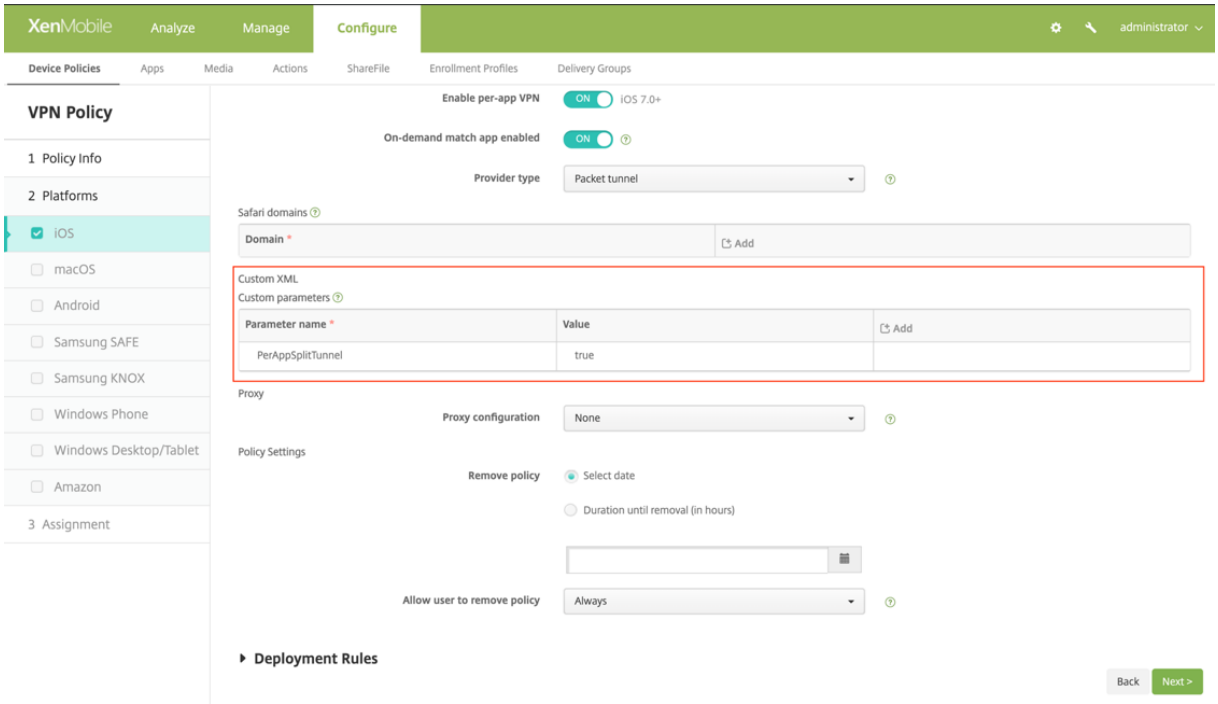
section of the VPN profile created on the MDM server.

```
- Key = "disableUserProfiles"
- Value = "true or 1 or yes"
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

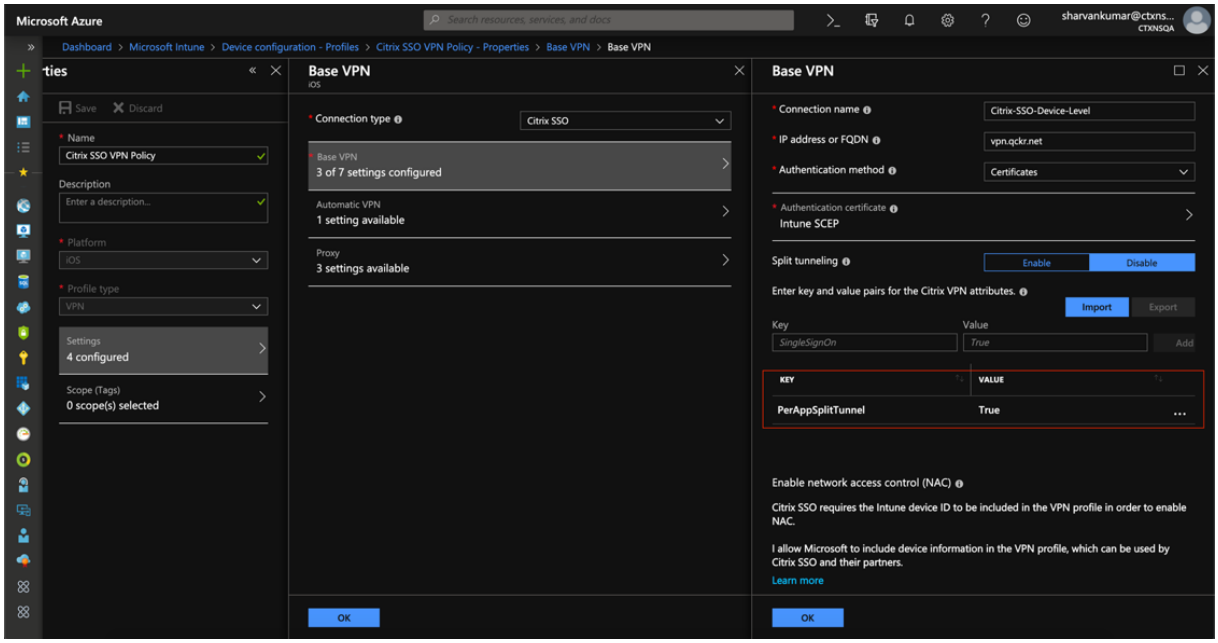
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.



The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



DNS handling

The recommended DNS settings for Citrix Secure Access client are as follows:

- **Split DNS > REMOTE** if the split tunnel is set to **OFF.**
- **Split DNS > BOTH** if the split tunnel is set to **ON**. In this case, the admins have to add DNS suffixes for the intranet domains. DNS queries for FQDNs belonging to DNS suffixes are tunneled to the NetScaler appliance and the remaining queries go to the local router.

> **Note:**
>
> - It is recommended that the **DNS truncate fix** flag is always **ON**. For more details, see CTX200243.
> - When split tunnel is set to **ON** and split DNS is set to **REMOTE**, there might be issues resolving DNS queries after the VPN is connected. This is related to the Network Extension framework not intercepting all the DNS queries.

Known issues

Issue description: Tunneling for FQDN addresses that contain a "`.local`" domain in Per-App VPN or On-Demand VPN configurations. There is a bug at Apple's Network Extension framework which stops FQDN addresses containing `.local` in the domain part (for example, http://wwww.abc.local) from being tunneled over the system's TUN interface. Instead, the traffic for the FQDN addresses is sent through the physical interface of the client device. The issue is observed only with Per-App VPN or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On-Demand VPN config and is not seen with system-wide VPN configurations. Citrix has filed a radar bug report with Apple, and Apple noted that according to RFC-6762. For more details, see RFC-6762, local is a multicast DNS (mDNS) query and is hence not a bug. However, Apple has not closed the bug yet and it is not clear if the issue will be addressed in future iOS releases.

Workaround: Assign a `non .local` domain name for such addresses as the workaround.

Limitations

- End Point Analysis (EPA) is not supported on iOS.
- Split tunneling based on ports/protocols is not supported.

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

September 7, 2025

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

When end-users log out of Citrix Workspace app, Citrix Secure Access automatically logs out without user intervention. This feature saves time as end-users are expected to log on to just one application, thereby providing a unified experience.

Currently, this functionality is disabled, by default.

Pre-requisites

1. End-users must be using 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 using Citrix Secure Access for macOS 24.03.1 or later.
3. To enable this feature through MDM, admins must use the following settings:
    - `<key>EnableSecureAccessAutoLogin</key><true/>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Points to note

- If end-users are already logged on to Citrix Workspace app before enabling this functionality, they must re-login so that Citrix Workspace app can trigger SSO to Citrix Secure Access client.
- When there is a logoff from Citrix Workspace app due to reasons such as a timeout or manual user logout, 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.

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

March 4, 2026

Starting from Citrix Secure Access for iOS 26.03.1, a login to Citrix Workspace app can single sign-on (SSO) end users to Citrix Secure Access client, establish a user tunnel, and seamlessly provide access to TCP/UDP applications. If the end users are connected to Citrix Workspace app, they need not provide credentials while logging in to the same URL on Citrix Secure Access for iOS.

End users with an active connection to the Citrix Workspace app can seamlessly log on to the same URL in the Citrix Secure Access app for iOS without being prompted for credentials. This feature saves time and provides a unified experience, as end users only need to log on to one application.

To get this feature enabled, contact Citrix Support.

> **Note:**
>
> Logging out of the Citrix Workspace app does not trigger a logout from the Citrix Secure Access app.

Send user certificate identity as an email attachment to iOS users

September 8, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

Citrix Secure Access on iOS supports client certificate authentication with NetScaler Gateway. On iOS, certificates can be delivered to Citrix Secure Access in one of following ways:

- MDM server - This is the 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. Please follow MDM vendor specific documents for this approach.
- Email - Only approach for non-MDM customers. In this approach, administrators send an email with the User Certificate identity (Certificate and private key) attached as a PCKS#12 file to users. Users need to have their email accounts configured on their iOS device to receive the email with attachment. The file may then be imported to Citrix Secure Access on the iOS. The following section explains the configuration steps for this approach.

Prerequisites

- User Certificate - A PKCS#12 identity file with a .pfx or .p12 extension for a given user. This file contains both the certificate and the private key.
- Email account configured on the iOS device.
- Citrix Secure Access installed on the iOS device.

Configuration steps

1. Rename the Extension/MIME type of the User Certificate.

   File extensions most commonly used for user certificate are “.pfx,”*“.p12,”and so forth. These file extensions are non-standard to the iOS platform unlike formats such as .pdf, .doc. Both “.pfx” and “.p12”are claimed by the iOS System and cannot be claimed by third-party apps such as Citrix Secure Access. Hence Citrix Secure Access has defined a new Extension/MIME type called “.citrixsso-pfx”and “.citrixsso-p12”. Administrators must change the Extension/MIME type of the User Certificate, from standard “.pfx”or “.p12”to “.citrixsso-pfx”or “.citrixsso-p12” respectively. To rename the extension, admins can run the following command on Command prompt or terminal.

   Windows 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
   citrixsso-pfx
```

macOS

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
   pfx
```

2. Send the file as an email attachment.

   The User Certificate file with the new extension can be sent as an email attachment to the user.

   On receipt of the email, users must install the certificate in Citrix Secure Access.

Setup proxy PAC file for the Citrix SSO app for iOS users or the Citrix Secure Access™ client for macOS users

September 25, 2026

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

Citrix Secure app for iOS or the Citrix Secure Access client for macOS support Auto Proxy Config(proxy PAC file) after the VPN tunnel establishment. Admins can use the proxy PAC file to allow all the client's HTTP traffic to go through a proxy, including resolving host names.

How to set up a proxy PAC file

Have an internal machine that can host a proxy file. For example, consider that the IP of the machine is 172.16.111.43 and the name of the PAC file is proxy.pac.

If the IP address of the actual proxy server is 172.16.43.83 which is listening on port 8080, then a sample of proxy.pac is as follows:
function FindProxyForURL(url, host)
{
return "PROXY 172.16.43.83:8080";
}

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The proxy PAC URL is http://172.16.111.43/proxy.pac. Assuming that the file is hosted on port HTTP port 80.

For more details, see CTX224235 or Proxy Auto Configuration for Outbound Proxy support for NetScaler Gateway.

Note:

- If Split Tunnel is ON, then make sure that the IP address of the server hosting the PAC file is included in the intranet applications list so that it is reachable through VPN.
- After logging in from Citrix Secure Access (macOS/iOS), the browsers start to use the rules from the proxy PAC file. If only one proxy rule is provided as in the previous example, then all HTTP or HTTPS traffic is routed to the internal proxy server.

Set up Citrix Secure Access for macOS users

September 25, 2026

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

The Citrix Secure Access client for macOS provides a 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 is the next generation VPN client for NetScaler Gateway to create and manage VPN connections from macOS devices. Citrix Secure Access is built using Apple's Network Extension (NE) framework. NE framework from Apple is a modern library which contains APIs that can be used to customize and extend the core networking features of macOS. Network Extension with support for SSL VPN is available on devices running macOS 10.11+.

Citrix Secure Access 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.
Citrix Secure Access for macOS can be installed from a Mac App store.

For the list of some commonly used features supported by the Citrix Secure Access client for macOS, see Citrix Secure Access client features supported in NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Compatibility with MDM products

Citrix Secure Access for macOS is compatible with most MDM providers such as Citrix XenMobile, Microsoft Intune and so on. It supports a feature called Network Access Control (NAC) using which, MDM administrators can enforce end user device compliance before connecting to NetScaler Gateway. NAC on Citrix Secure Access requires an MDM server such as XenMobile and NetScaler Gateway. For more information on NAC, see Configure Network Access Control device check for NetScaler Gateway virtual server for single factor login.

> **Note:**
>
> To use the Citrix Secure Access with NetScaler Gateway VPN without MDM, you must add a VPN configuration. You can add the VPN configuration on macOS from the Citrix Secure Access configuration page.

Configure an MDM managed VPN profile for Citrix Secure Access

The following section captures step-by-step instructions to configure both device-wide and per-app VPN profiles for Citrix Secure Access using Citrix Endpoint Management™ (formerly XenMobile) as an example. Other MDM solutions can use this document as reference when working with Citrix Secure Access.

> **Note:**
>
> This section explains the configuration steps for a basic Device-wide and Per-App VPN profile. Also you can configure On-Demand, Proxies by following the Citrix Endpoint Management (formerly XenMobile) documentation or Apple's MDM VPN payload configuration.

Device level VPN profiles

Device level VPN profiles are used to set up a system wide VPN. Traffic from all apps and services is tunneled to NetScaler Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split tunnel) defined in NetScaler.

To configure a device level VPN on Citrix Endpoint Management Perform the following steps to configure a device level VPN.

1. On the Citrix Endpoint Management MDM console, navigate to **Configure** > **Device Policies** > **Add New Policy**.
2. Select **macOS** on the left Policy Platform pane. Select **VPN Policy** on the right pane.
3. On the **Policy Info** page, enter a valid policy name and description and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the **Policy detail** page for macOS, type a valid connection name and choose **Custom SSL** in **Connection Type**.

   In the MDM VPN payload, the connection name corresponds to the **UserDefinedName** key and **VPN Type Key** must be set to **VPN**.

5. In **Custom SSL identifier (reverse DNS format)**, enter **com.citrix.NetScalerGateway.macos.app**. This is the bundle identifier for the Citrix Secure Access on macOS.

   In the MDM VPN payload, the Custom SSL identifier corresponds to the **VPNSubType** key.

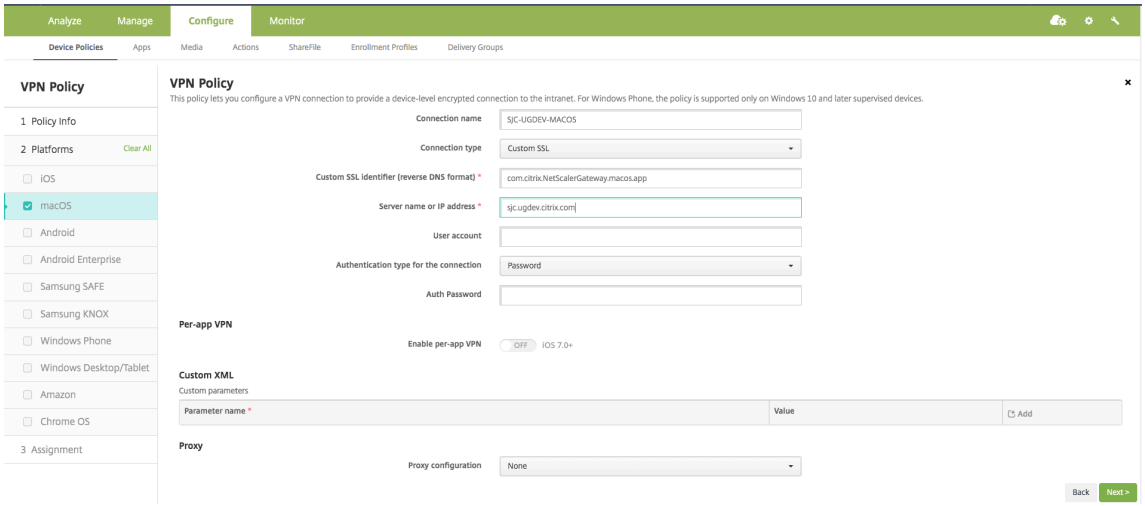
6. In **Provider bundle identifier** enter **com.citrix.NetScalerGateway.macos.app.vpnplugin**. This is the bundle identifier of the network extension contained in the Citrix Secure Access client binary.

   In the MDM VPN payload, the provider bundle identifier corresponds to the **ProviderBundleIdentifier** key.

7. In **Server name or IP address** enter the IP address or FQDN of the NetScaler associated with this Citrix Endpoint Management instance.

   The remaining fields in the configuration page are optional. Configurations for these fields can be found in the Citrix Endpoint Management documentation.

8. Click **Next**.



9. Click **Save**.

Per-App VPN profiles

Per-App VPN profiles are used to set up a VPN for a specific application. Traffic from only the specific app is tunneled to NetScaler Gateway. The **Per-App VPN payload supports all** keys for Device-wide VPN plus a few other keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

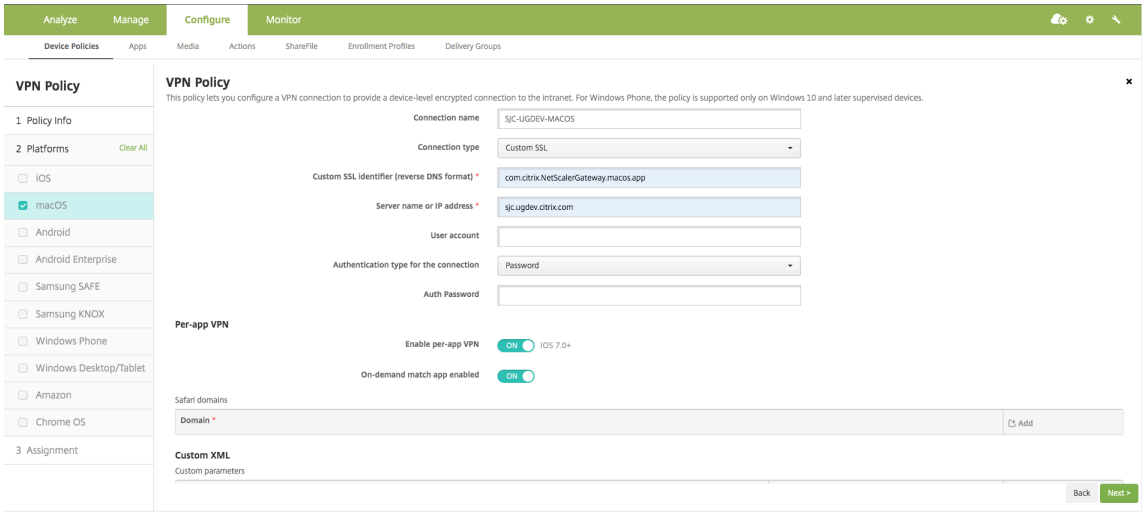
To configure a per-App level VPN on Citrix Endpoint Management Perform the following steps to configure a Per-App VPN on Citrix Endpoint Management:

1. Complete the device level VPN configuration on Citrix Endpoint Management.
2. Turn the **Enable Per-App VPN** switch ON in the **Per-App VPN** section.
3. Turn the **On-Demand Match App Enabled switch ON** if Citrix Secure Access must be started automatically when the Match App is launched. This is recommended for most Per-App cases.

   In the MDM VPN payload, this field corresponds to the key **OnDemandMatchAppEnabled**.
4. Safari Domain configuration is optional. When a Safari domain is configured, Citrix Secure Access starts automatically when users launch Safari and navigate to a URL that matches the one in the **Domain** field. This is not recommended if you want to restrict the VPN for a specific app.

   In the MDM VPN payload, this field corresponds to the key **SafariDomains**.

   The remaining fields in the configuration page are optional. Configurations for these fields can be found in the Citrix Endpoint Management (formerly XenMobile®) documentation.



5. Click **Next**.
6. Click **Save**.

   To associate the VPN profile to a specific App on the device, you must create an App Inventory policy and a credentials provider policy.

Configuring split tunnel in Per-App VPN

MDM customers can configure split tunnel in Per-App VPN for Citrix Secure Access. The following key/-value pair must be added to the vendor configuration section of the VPN profile created on the MDM server.

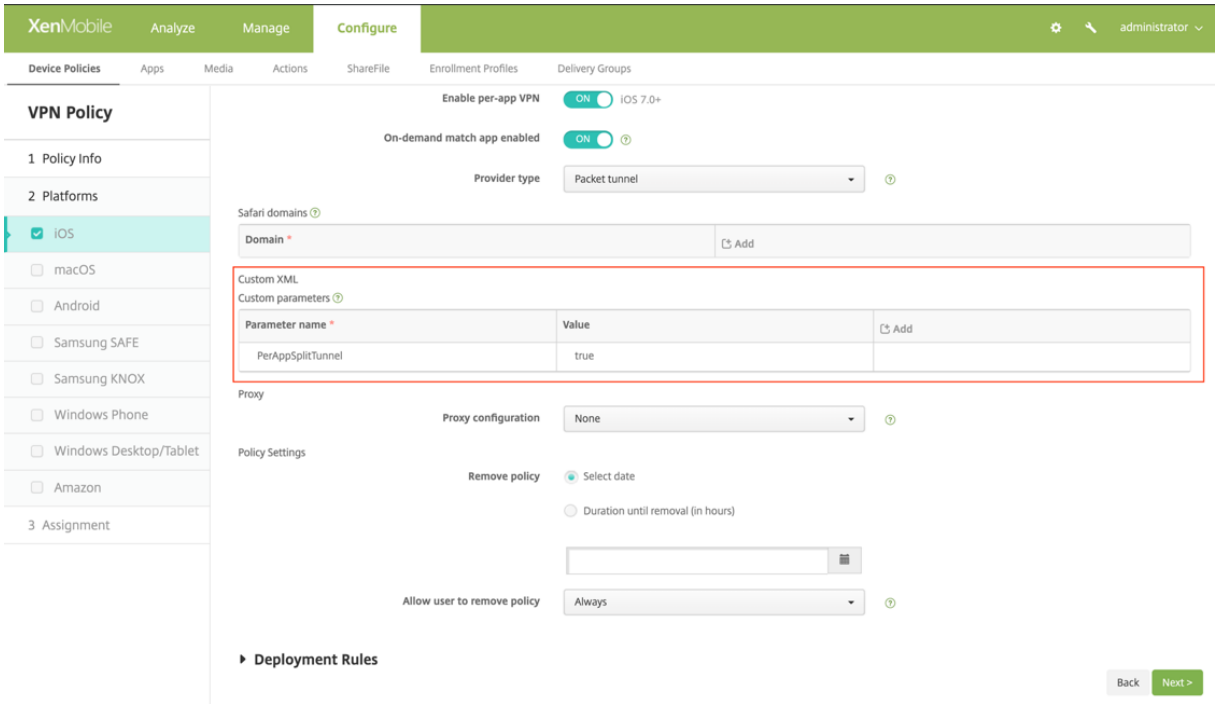
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
- Key = "PerAppSplitTunnel"
- Value = "true or 1 or yes"
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

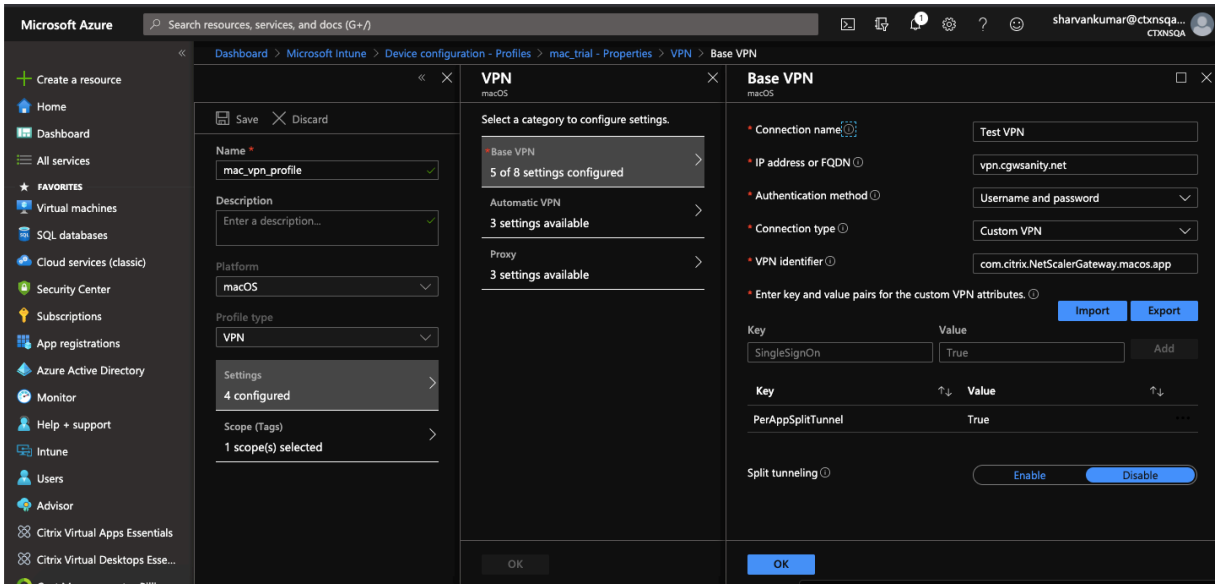
> **Note:**
>
> The user interface to configure vendor configuration is not standard across the MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.



The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Disabling user created VPN profiles

MDM customers can prevent users from manually creating VPN profiles from within the Citrix Secure Access. To do this, the following key/value pair must be added to the vendor configuration section of the VPN profile created on the MDM server.

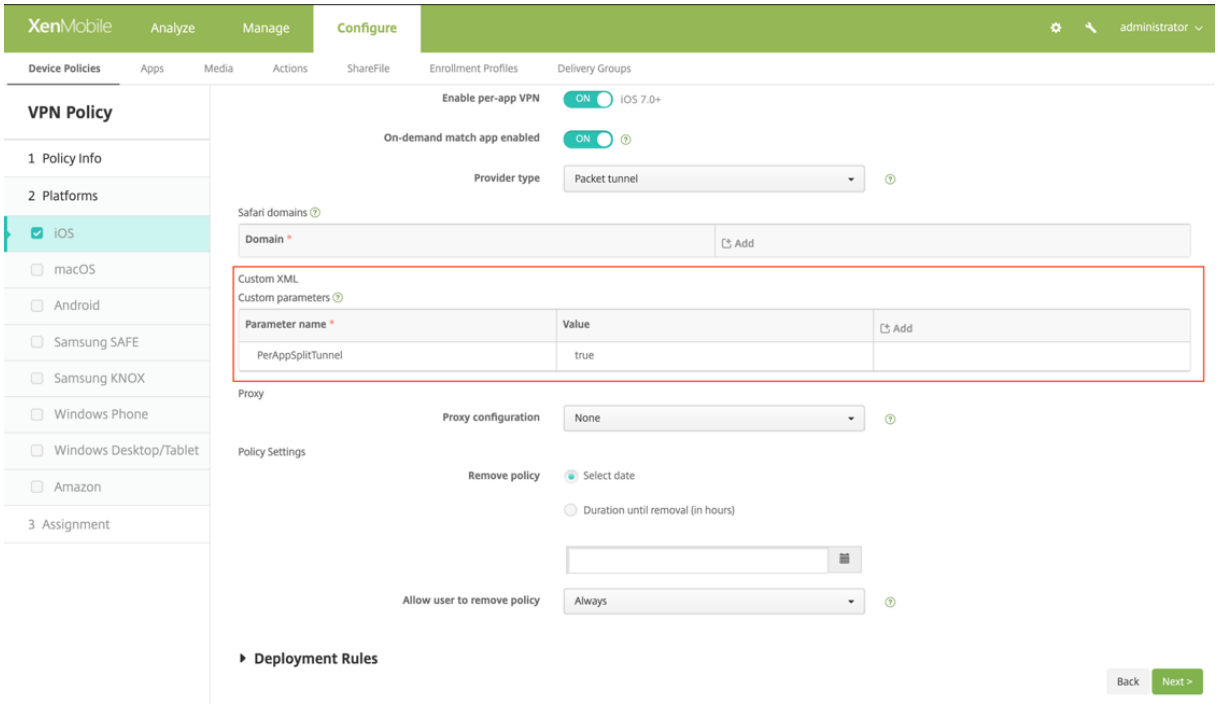
```
- Key = "disableUserProfiles"
- Value = "true or 1 or yes"
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

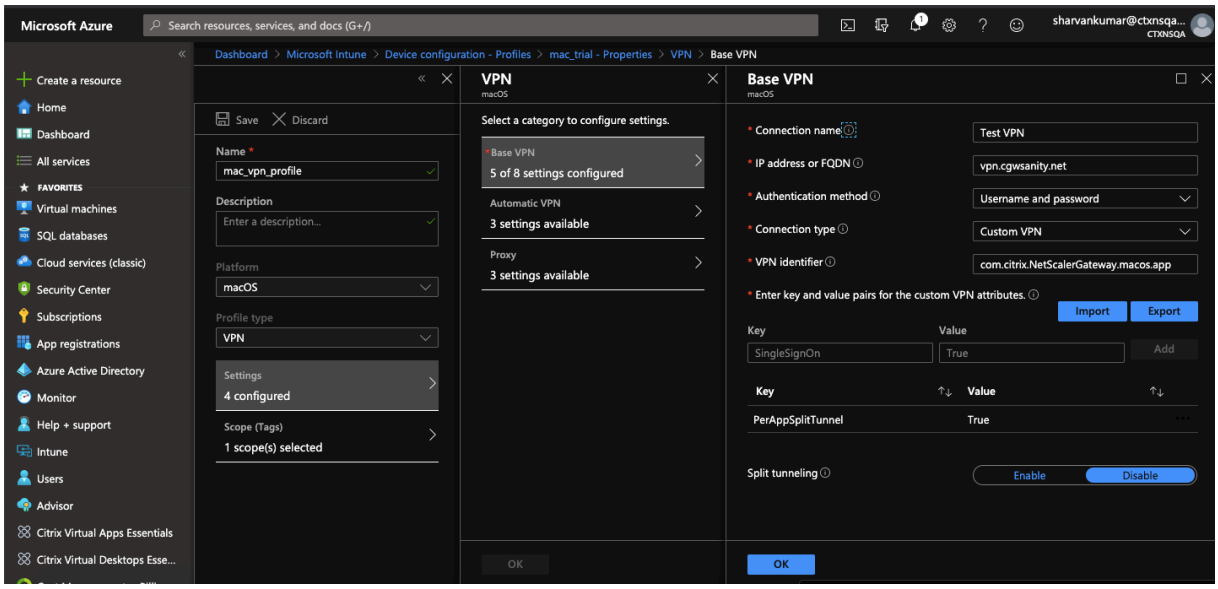
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.



DNS handling

The recommended DNS settings for Citrix Secure Access are as follows:

- **Split DNS > REMOTE** if the split tunnel is set to **OFF.**
- **Split DNS > BOTH** if the split tunnel is set to **ON**. In this case, the admins have to add DNS suffixes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

for the intranet domains. DNS queries for FQDNs belonging to DNS suffixes are tunneled to the NetScaler appliance and the remaining queries go to the local router.

> **Note:**
>
> - It is recommended that the **DNS truncate fix** flag is always **ON**. For more details, see CTX200243.
> - When split tunnel is set to **ON** and split DNS is set to **REMOTE**, there might be issues resolving DNS queries after the VPN is connected. This is related to the Network Extension framework not intercepting all the DNS queries.

Supported EPA scans

For the complete list of scans supported, see Latest EPA Libraries.

1. In the section **Supported Scan Matrix by OPSWAT v4**, click **Supported Application List** under the column **MAC OS Specific**.
2. In the Excel file, click the **Classic EPA scans** tab to view the details.

Known issues

The following are the known issues currently.

- EPA login fails if the user is placed in the quarantine group.
- Forced timeout warning message is not displayed.
- Citrix Secure Access allows login if the split tunnel is ON and no intranet apps are configured.

Limitations

The following are the limitations currently.

- The following EPA scans might fail because of restricted access to Secure Access due to sandboxing.
  - Hard Disk encryption ‘type’and ‘path’
  - Web Browser ‘default’and ‘running’
  - Patch management ‘missing patches’
  - Kill process operation during EPA
- Split tunneling based on ports/protocols is not supported.
- Ensure that you do not have two certificates with the same name and expiry date in the keychain as this causes the client to display only one of the certificates instead of both.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

If the end users are presented with the **Download EPA plug-in** button in the authentication window of Citrix Secure Access, it means that the content security policy on the NetScaler appliance is blocking invocation of the URL `com.citrix.agmacepa://`. The admins have to modify the content security policy such that `com.citrix.agmacepa://` is allowed.

nFactor support for Citrix Secure Access client on macOS/iOS

September 25, 2026

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

Multi-factor (nFactor) authentication enhances the security of an application by requiring users to provide multiple proofs of identity to gain access. Admins can configure different authentication factors that include client cert, LDAP, RADIUS, OAuth, SAML, and so on. These authentication factors can be configured in any order based on the organization's needs.

Citrix Secure Access client on macOS/iOS supports the following authentication protocols:

- **nFactor** –The nFactor protocol is used when an authentication virtual server is bound to the VPN virtual server on the gateway. Because the order of the authentication factors is dynamic, the client uses a browser instance (WebView) that is rendered within the app's context to present the authentication GUI.
- **Classic** –Classic protocol is the default fall-back protocol used if classic authentication policies are configured on the VPN virtual server on the gateway. Classic protocol is also used by the client for nFactor authentication if NAC check is required.
- **Citrix identity platform** –The Citrix identity platform protocol is used when authenticating to CloudGateway or Citrix Gateway service and requires MDM enrollment with Citrix Cloud.

The following table summarizes the various authentication methods supported by each protocol.

Authentication method	nFactor	Classic	Citrix IdP
Client Cert	Supported	Supported	Not supported
LDAP	Supported	Supported	Not supported

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication method	nFactor	Classic	Citrix IdP
Local	Supported	Supported	Not supported
RADIUS	Supported	Not supported	Not supported
SAML	Supported	Not supported	Not supported
OAuth	Supported	Not supported	Not supported
TACACS	Supported	Not supported	Not supported
WebAuth	Supported	Not supported	Not supported
Negotiate	Supported	Not supported	Not supported
EPA	Supported	Supported	Not supported
NAC	Supported*	Supported	Not supported
StoreFront™	Not supported	Not supported	Not supported
ADAL	Not supported	Not supported	Not supported
DS-AUTH	Not supported	Not supported	Supported

> **Note:**
>
> *nFactor authentication with Network Access Control (NAC) check operates under the following conditions:
>
> - When an nFactor authentication policy includes a NAC check, the Citrix Secure Access client for iOS uses the classic authentication protocol instead of WebView-based authentication.
> - Authentication policies requiring credential collection via WebView are not supported. Instead, the Citrix Secure Access client for iOS displays a legacy dialog box to collect user credentials.
> - For Intune NAC checks, ensure all required authentication factors (such as one or two passwords) are collected in a single step. Configure the login schema policy to prompt for and gather all necessary factors during the initial authentication prompt.

nFactor configuration

For details about configuring nFactor, see Configuring nFactor authentication.

> **Important:**
>
> To use the nFactor protocol with Citrix Secure Access client on macOS/iOS, the recommended

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> NetScaler Gateway on-premises version is 12.1.50.xx and later.

Limitations

- Mobile specific authentication policies such as NAC (network access control) require the client to send a signed device identifier as part of the authentication with NetScaler Gateway. The signed device identifier is a rotatable secret key that uniquely identifies a mobile device, which is enrolled in an MDM environment. This key is embedded in a VPN profile that is managed by an MDM server. It might not be possible to inject this key into the WebView context. If NAC is enabled in an MDM VPN profile, the Citrix Secure Access client for iOS automatically falls back to the classic authentication protocol.
- You cannot configure NAC check with Intune for macOS as Intune does not provide an option to enable NAC for macOS unlike for iOS.

Log collection for the macOS and iOS clients

December 5, 2025

Log collection for the macOS clients

The Citrix Secure Access client for macOS provides end-users with several options, including inspecting client logs and sharing them with the development team. These options allow end-users to:

- View and inspect live logs
- Email logs to the development team
- Compress and share logs with the development team
- Clear previously stored logs

The collection of logs is supported across multiple sessions and is not limited to the current session only.

For the macOS clients, since the application and VPN extensions are running separately, the logs are collected in 2 types of files:

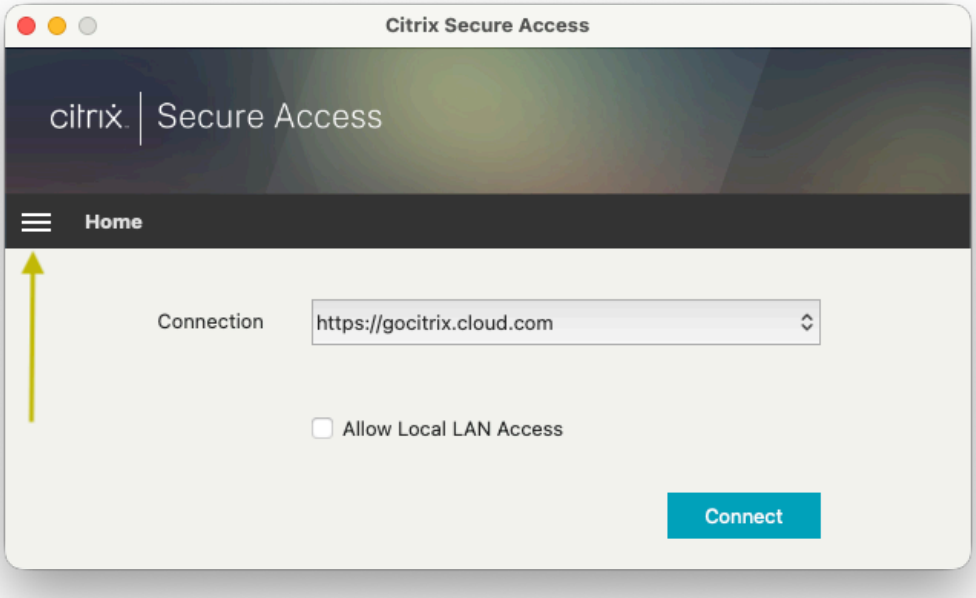
- **nsgControllerApp.log:** Collects all logs for the Citrix Secure Access application workflow.
- **nsg_vpnextension_process-pid_Date-time_file_number.log:** Collects all logs for the network extension. The `file_number` increases by 1 for new file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure logging by using the GUI

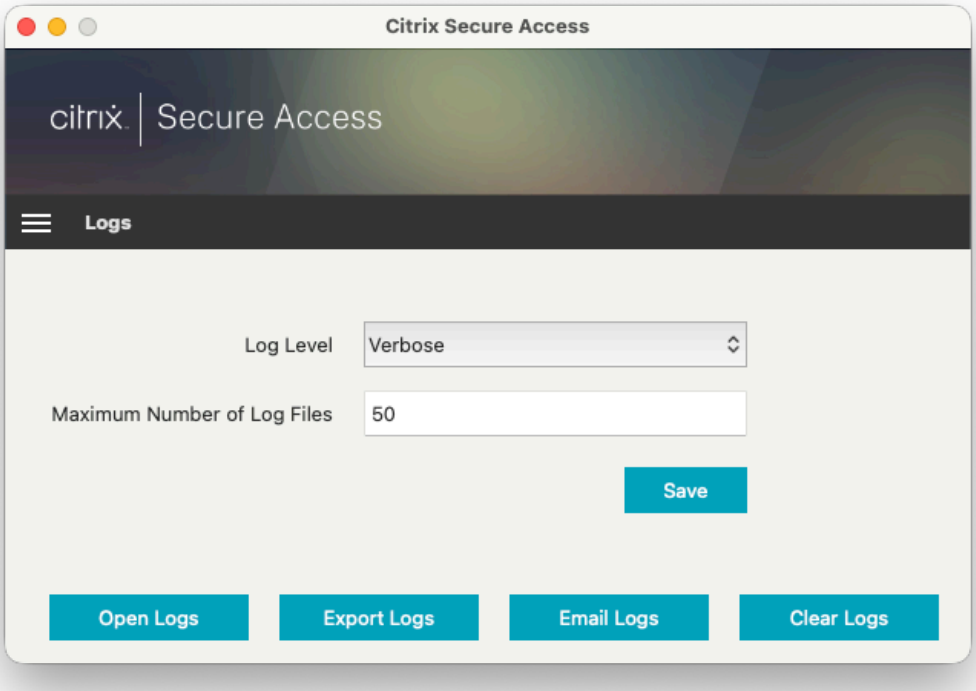
1. Click the hamburger icon on the **Home** screen and select the **Logs** menu to access the log screen.

   > **Note:**
   >
   > The hamburger icon is not available until the user adds at least one configuration or server URL.



2. All configuration related to logs can be done in the **Logs** screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **Log Level:** The following three log levels are available to select:
  - **Error**: Only exceptions or failures reported by the application are logged.
  - **Debug Messages**: This level includes debug messages and events relevant from program execution.
  - **Verbose**: This level includes all log messages reported by **Error** and **Info** log levels and other messages that might help in troubleshooting.
- **Maximum Number of Log Files:** Enter the number of files that you want to add for log collection. This option is mandatory.
- **Open Logs:** When you select this option, the latest application and extension log files open in console.
- **Email Logs:** Email the log files to the registered email ID using the mail app. A new mail opens with an attached `ta.gz` file.
- **Export Logs:** When you select this option, all the log files created so far are zipped and saved in the `Downloads` folder for the current user. The zip file name looks like `citrixsso-20251127-120843-logs.tar.gz`.
- **Clear Logs:** When you select this option, the log files created so far are cleared except the latest `nsgControllerApp.log` file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log collection for the iOS clients

The Citrix Secure Access client for iOS offers end-users different logging options such as:

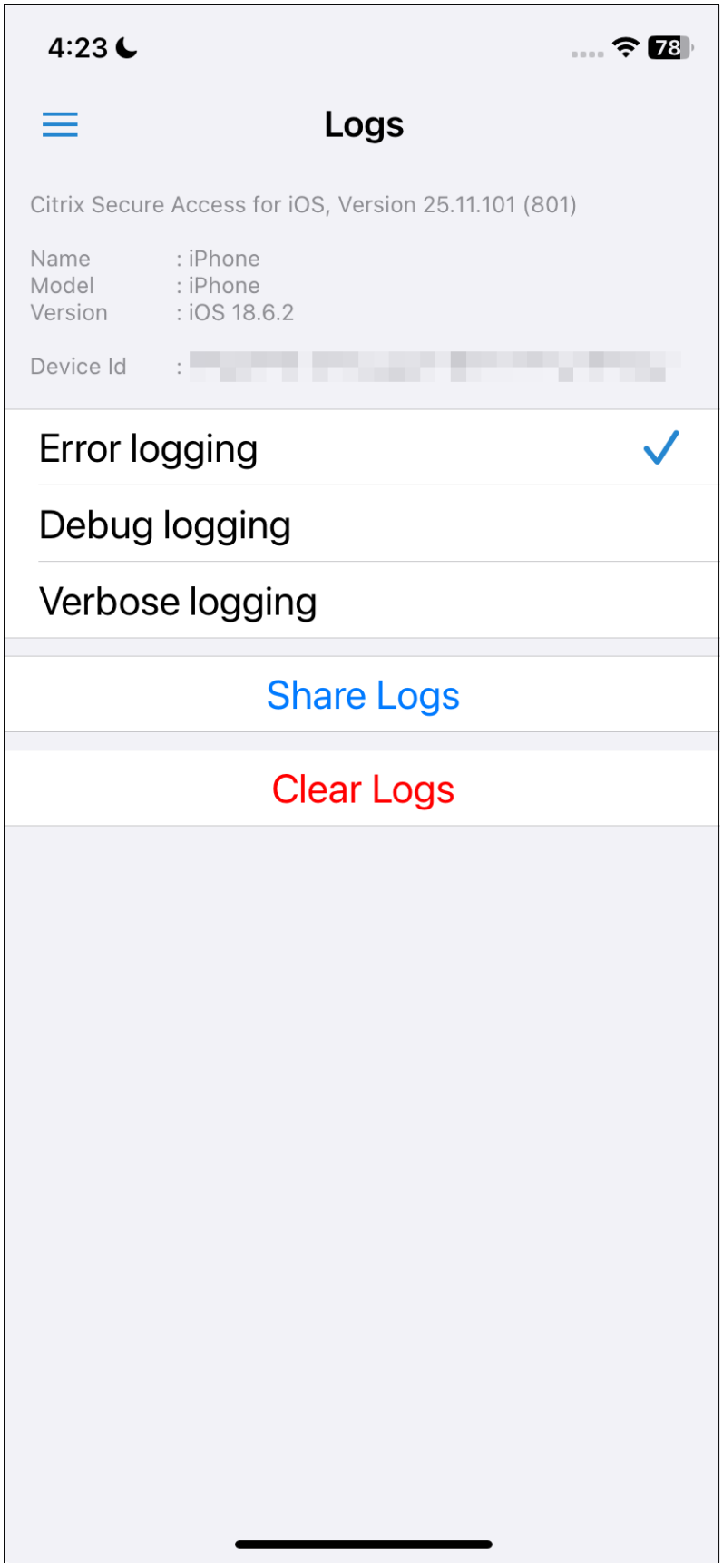
- Share logs
- Clear logs

For the iOS clients, the Log folder contains separate logs for application and extension:

- **nsgControllerApp.log:** Collects all logs for the Citrix Secure Access application workflow.
- **nsg_vpnextension_process-pid_Date-time_file_number.log:** Collects all logs for network extension. The file_number increases by 1 for new file.

Tap on the hamburger icon and select **Logs** to see the options available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

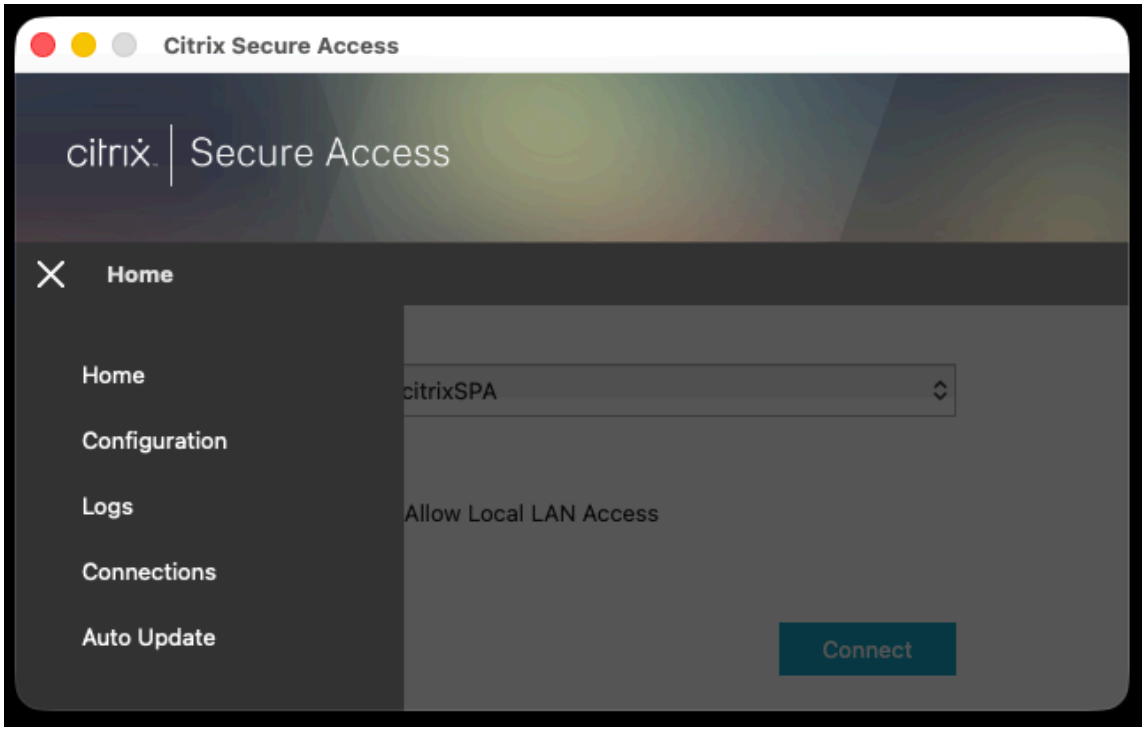
- **Select Log Level:** The following three log levels are available to select:
  - **Error logging**: Only exceptions or failures reported by the application are logged.
  - **Debug logging**: This level includes debug messages and events relevant from program execution.
  - **Verbose logging**: This level includes all log messages reported by **Error** and **Info** log levels and other messages that might help in troubleshooting.
- **Share Logs:** On tapping this menu, the device opens up multiple options to share the logs like AirDrop and Mail. Along with this option, the log zip file can be saved to `Files` or copied. If the **Mail** option is selected, the log zip file is attached to a new mail and can be sent.
- **Clear Logs:** On tapping this menu, the existing log files are cleared.

Auto Update support for macOS

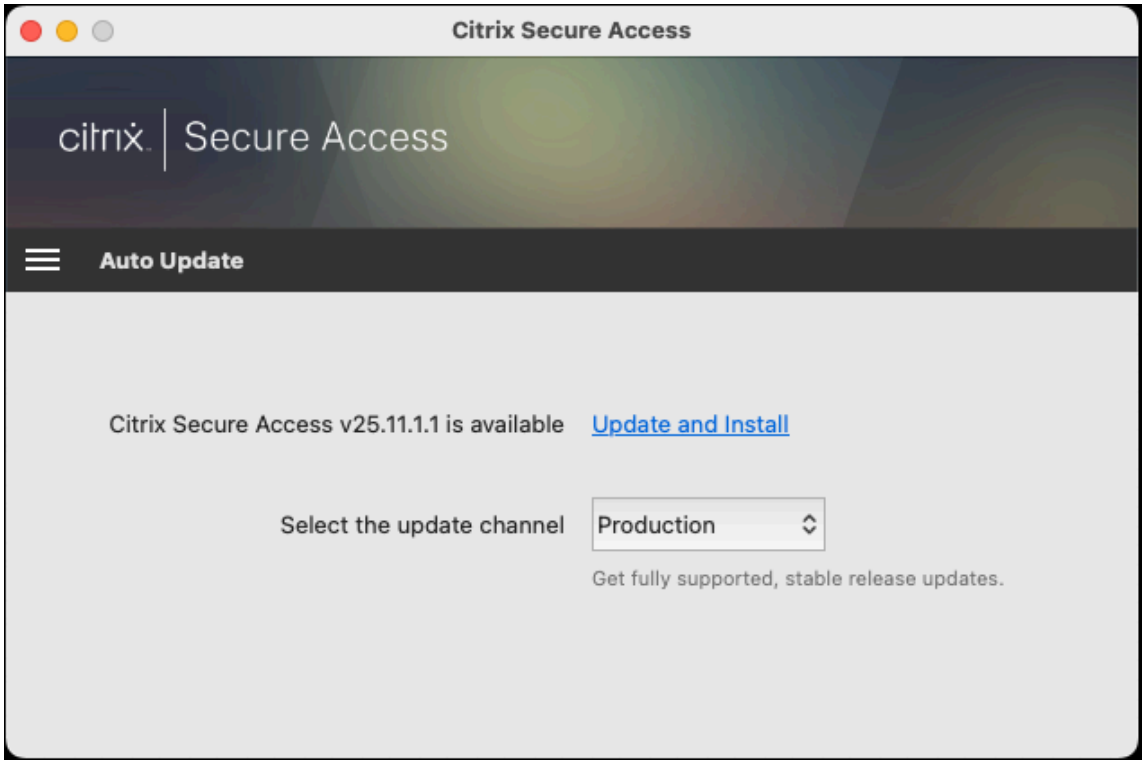
February 2, 2026

Starting from release 26.01.1.1, the Citrix Secure Access application for macOS includes an Auto Update feature that provides the following functionalities:

- Periodically checks if any update is available.
- Updates the app automatically after notifying the user.



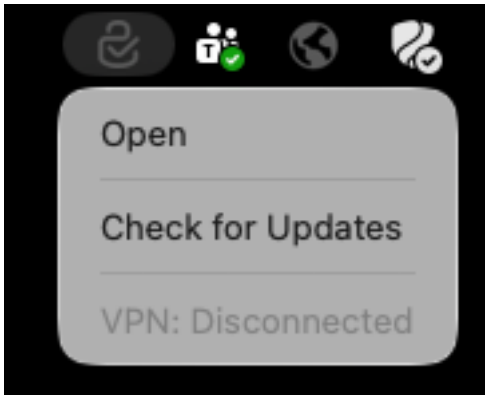
© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> The Auto update feature is available only in the Production channel.

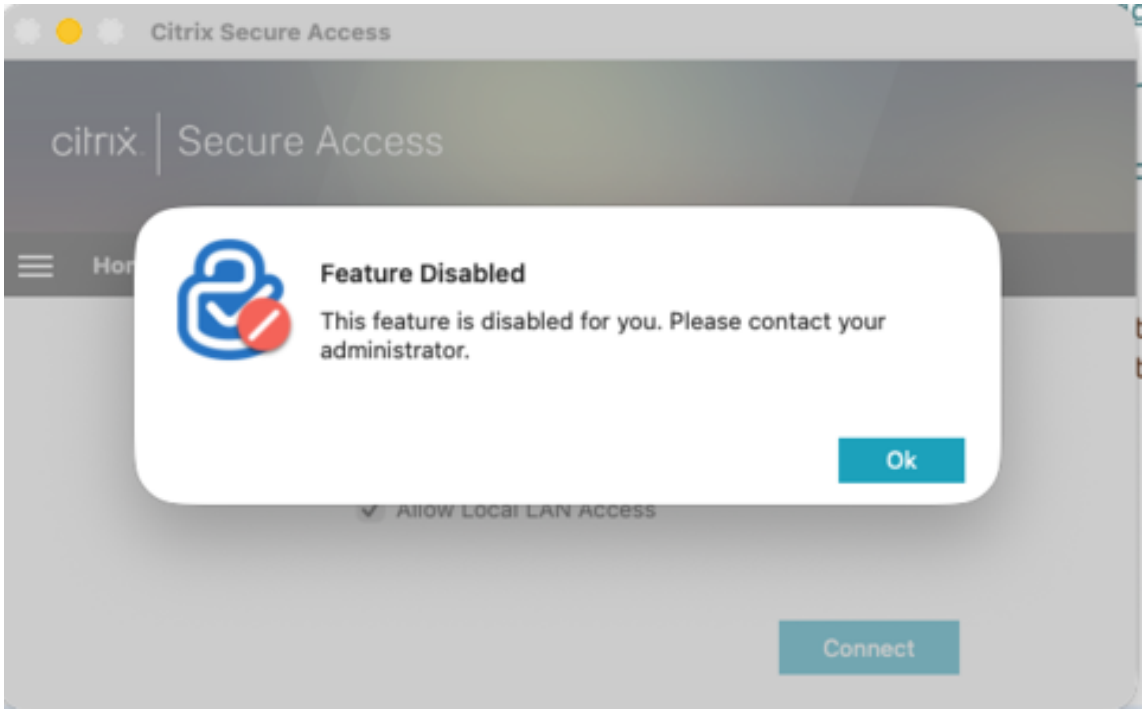
Option for end users

- End users can also check for the updates and install the updates manually by using the **Check for Updates** option from the menu bar.



- The **Auto Update** option in the hamburger menu is disabled for the end users. When end users click the option, the message **Feature Disabled** appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting common Citrix Secure Access for macOS/iOS issues

September 25, 2026

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

DNS resolution issues

- If the device goes to sleep or is inactive for long, then it might take around 30–60 seconds for the VPN to resume. During this time, users might see some DNS requests failing. DNS requests automatically resolve after a short period.
  If DNS queries are not resolving, it is possible that an advanced authorization policy is blocking the DNS traffic. See CTX232237 to fix this issue.
- Always check the DNS resolution from browsers. DNS queries using the `nslookup` command from the terminal might not be accurate. If you have to use the `nslookup` command, then you have to include the client IP address in the command. For example, `nslookup website_name 172.16.255.1.`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA issues

- Gatekeeper is considered as an antivirus. If there is a scan that checks for "any antivirus"(MAC-ANTIVIR_0_0), the scan always passes even if the user has not installed any antivirus from other vendors.

Note:

- Enable client security logging to get debug logs for EPA. You can enable client security logging by setting the VPN parameter `clientsecurityLog` to ON.
- The built-in patch management software from Apple is "Software Update". It corresponds to the "App Store"app on the device. The version of the "Software Update"must be like `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- Always keep the EPA libraries on NetScaler up to date. The latest libraries can be found at EPA libraries

nFactor issues

- Citrix Secure Access opens the **Citrix SSO auth** window for nFactor authentication. It is similar to a browser. If there are errors on this page, it can be cross verified by trying authentication on a web browser.
- If the transfer logon fails when nFactor is enabled, then change the portal theme to "RFWebUI".
- If you get an error "Secure connection to NetScaler Gateway cannot be established because the certificate chain does not contain any of the required certificates. Please contact your administrator", or "Gateway not reachable", then either the gateway server certificate has expired or the server certificate is bound with SNI enabled. Citrix Secure Access does not support SNI yet. Bind the server certificate without SNI enabled. The error can also be due to certificate pinning configured in the MDM VPN profile and the certificate presented by NetScaler Gateway not matching the pinned certificate.
- When trying to connect to the gateway, if the **Citrix SSO auth window** opens but is blank, then check if the ECC curve (ALL) is bound to the default cipher group. The ECC curve (ALL) must be bound to the default cipher group.

Network Access Control (NAC) check

NAC authentication policy is supported only in classic authentication. It is not supported as part of nFactor authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQs

September 25, 2026

> **Important:**
>
> Citrix SSO for iOS is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

This section captures the FAQ on Citrix Secure Access for macOS/iOS.

How is Citrix Secure Access client for macOS/iOS different from VPN app?
Citrix Secure Access client for macOS and Citrix Secure Access client for iOS (formerly known as Citrix SSO for iOS) is the next generation SSL VPN client for NetScaler. The App uses Apple's Network Extension framework to create and manage VPN connections on iOS and macOS devices. Citrix VPN is the legacy VPN client that uses Apple's private VPN APIs which are now deprecated. Support for Citrix VPN is no longer available on the App store.

What is NE?
The Network Extension (NE) framework from Apple is a modern library which contains APIs that can be used to customize and extend the core networking features of iOS and macOS. Network Extension with support for SSL VPN is available on devices running iOS 9+ and macOS 10.11+.

For which versions of NetScaler is the Citrix Secure Access client for macOS/iOS compatible?
VPN features in Citrix Secure Access client for macOS/iOS are supported on NetScaler versions 10.5 and above. The TOTP is available on NetScaler version 12.0 and above. Push Notification on NetScaler has not been publicly announced yet. The App requires iOS 9+ and macOS 10.11+ versions.

How does Cert-based authentication for non-MDM customers work?
Customers who previously distributed Certificates via Email or Browser to perform Client Certificate Authentication in VPN must note this change when using Citrix Secure Access client for macOS/iOS. This is mostly true for non-MDM customers who do not use an MDM Server to distribute User Certificates.

What is Network Access Control (NAC)? How do I configure NAC with Citrix Secure Access for iOS and NetScaler Gateway?
Microsoft Intune and Citrix Endpoint Management™ (formerly XenMobile) MDM customers can take advantage of the Network Access Control (NAC) feature in the Citrix Secure Access for iOS. With NAC, administrators can secure their enterprise internal network by adding an extra layer of authentication for mobile devices that are managed by an MDM server. Administrators can enforce a device compliancy check at the time of authentication in the Citrix Secure Access for iOS.

To use NAC with the Citrix Secure Access for iOS, you must enable it on both the NetScaler Gateway and the MDM server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To enable NAC on NetScaler, see Configure Network Access Control device check for NetScaler Gateway virtual server for single factor login.
- If an MDM vendor is Intune, see "Network access control (NAC) integration with Intune"in Microsoft Learn Challenge page.
- If an MDM vendor is Citrix Endpoint Management (formerly XenMobile), see Network Access Control.

  > **Note:**
  >
  > The minimum supported Citrix Secure Access client for macOS/iOS version are 1.1.6 and above.

Citrix Secure Access client for Linux

October 6, 2026

Citrix Secure Access client for Linux is a VPN client software that enables users to access corporate data and applications remotely. Citrix Secure Access client protects applications from unauthorized access, application-level threats, and browser-based attacks.

Citrix End Point Analysis (EPA) client is a client software that 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.

> **Note:**
>
> Even if you do not use EPA, we recommend that you update both EPA and VPN plug-in binaries together in case you choose to use the EPA functionality later.

Supported Linux versions

The Citrix Secure Access client and Citrix EPA client are compatible with Ubuntu versions 22.04 and 24.04, and eLux and IGEL OS. For more information about the supported browsers, see System requirements.

> **Notes:**
>
> - We recommend you to use the Citrix Secure Access client for Linux version 24.8.5 or later.
> - The Citrix Secure Access client for Linux version 24.11.4 and later supports eLux OS.
> - For Ubuntu 22 and higher to work with Citrix Secure Access client and Citrix EPA client, en-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

able TLS 1.3 on the VPN virtual server. If you have enabled only TLS 1.2, then set the SSL parameter denySSLReneg to NONSECURE on the CLI.

- Starting from the Citrix Secure Access client release 25.8.1, support for Ubuntu 20.04 is deprecated.
- The **Linux Plugin Upgrade** and **EPA Linux Upgrade** settings on NetScaler Gateway do not support the option **Essential** when used with the Citrix Secure Access client for Linux. For more information, see How users connect with the Citrix Secure Access client and Create a virtual server.
- For eLux and IGEL OS, the following are the recommended configurations in NetScaler Gateway:
  - **Global Configuration:** Set **Linux Plugin Upgrade** to **Never**. For more information, see How users connect with the Citrix Secure Access client.
  - **Session Profile:** Set **Linux Plugin Upgrade** to **Never**. For more information, see To configure the session profile for the Citrix Secure Access client.
  - **Virtual Server: Set EPA Plugin Upgrade** to **Never**. For more information, see Create a virtual server.
- For deployments using classic authentication, the **Linux Plugin Upgrade** setting within the session profile in NetScaler Gateway is not supported. For more information, see To configure the session profile for the Citrix Secure Access client.

Supported features

Citrix Secure Access client for Ubuntu supports the following features:

- Split tunneling and reverse split tunneling
- Tunneling TCP, UDP, and ICMP applications
- Server-initiated connections via Intranet IP (IIP)
- Split DNS remote
- Client side proxy
- Classic EPA scans
- Advanced authentication (nFactor) including advanced EPA scans
- HTTPOnly cookies
- Global server load balancing (GSLB)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network configurations for the Citrix Secure Access client

The Citrix Secure Access client for Linux uses specific network configurations that administrators must be aware of:

- Firewall marks: `0xc5a00001` and `0xc5a00002`
- Custom routing table: ID `221` with name `csa`

> **Important:**
>
> If these firewall marks and routing table ID are used in other applications, it might lead to conflicts with the Citrix Secure Access client.

Upgrade Ubuntu clients on NetScaler Gateway

You can download the Citrix Secure Access client and Citrix EPA client for Ubuntu from the Downloads page.

The Citrix Secure Access client and Citrix EPA client are named "nsgclient18_64.deb"and "nsepa18.deb", respectively. The clients are compatible with Ubuntu 20.04.

The Citrix Secure Access client and Citrix EPA client that support Ubuntu 22.04 and 24.04 are named "nsginstaller64.deb"and "nsepa.deb", respectively.

If you want to upgrade to the latest version of Citrix Secure Access client from version 1.0.0.x to version 23.6.1, for example:

1. Replace the files "nsgclient18_64.deb"and "nsginstaller64.deb"at the location `/var/netscaler/gui/vpn/scripts/linux/` by using the shell prompt.
2. Replace the files "nsepa18.deb"and "nsepa.deb"at the location `/var/netscaler/gui/epa/scripts/linux/` by using the shell prompt.
3. Open the `/var/netscaler/gui/vpn/scripts/linux/clientversions.xml` file.

```
a.  For the Citrix EPA client, replace the current version (1.0.0.x) in the following XML tags with the latest version (23.6.1). If the XML tags do not exist, add them to the XML file. For example,

replace

`<component pkgname="nsepa18" currentversion="1.0.0.x" minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="0" maxkernelversion="100" updatetype="compatible" action="/epa/scripts/linux/nsepa18.deb" />`

with
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
8
9  `<component pkgname="nsepa18" currentversion="23.6.1" minversion="
      23.6.1" ostype="ubuntu64" minkernelversion="0" maxkernelversion
      ="100" updatetype="compatible" action="/epa/scripts/linux/
      nsepa18.deb" />`
10
11 and replace
12
13 `<component pkgname="nsepa22" currentversion="1.0.0.x" minversion=
      "1.0.0.x" ostype="ubuntu64" minkernelversion="0"
      maxkernelversion="100" updatetype="compatible" action="/epa/
      scripts/linux/nsepa.deb" />`
14
15 with
16
17 `<component pkgname="nsepa22" currentversion="23.6.1" minversion="
      23.6.1" ostype="ubuntu64" minkernelversion="0" maxkernelversion
      ="100" updatetype="compatible" action="/epa/scripts/linux/nsepa
      .deb" />`
18
19 b.  For the Citrix Secure Access client, replace the current
      version (1.0.0.x) in the following XML tags with the latest
      version (23.6.1). If the XML tags do not exist, add them to the
       XML file. For example,
20
21 replace
22
23 `<component pkgname="nsgclient18" currentversion="1.0.0.x"
      minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="3.0"
      maxkernelversion="5.16" updatetype="compatible" action="/vpn/
      scripts/linux/nsgclient18_64.deb" />`
24
25 to
26
27 `<component pkgname="nsgclient18" currentversion="23.6.1"
      minversion="23.6.1" ostype="ubuntu64" minkernelversion="3.0"
      maxkernelversion="5.16" updatetype="compatible" action="/vpn/
      scripts/linux/nsgclient18_64.deb" />`
28
29 and
30
31 `<component pkgname="nsgclient22" currentversion="1.0.0.x"
      minversion="1.0.0.x" ostype="ubuntu64" minkernelversion="3.0"
      maxkernelversion="5.20" updatetype="compatible" action="/vpn/
      scripts/linux/nsginstaller64.deb" />`
32
33 to
34
35 `<component pkgname="nsgclient22" currentversion="23.6.1"
      minversion="23.6.1" ostype="ubuntu64" minkernelversion="3.0"
      maxkernelversion="5.20" updatetype="compatible" action="/vpn/
      scripts/linux/nsginstaller64.deb" />`
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On the NetScaler shell prompt, run the following commands:

```
rm -rf /netscaler/ns_gui
ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. On the NetScaler CLI, run the following commands:

```
set vpn parameter -clientversions all
flush cache contentgroup loginstaticobjects
```

References

- Supported features.
- Endpoint Analysis scans supported for Ubuntu.
- End-user help documentation.

Release notes

September 8, 2026

The Citrix Secure Access client and Citrix End Point Analysis (EPA) client for Linux are now released on a standalone basis and are compatible with all NetScaler versions. The Citrix Secure Access client version follows the format YY.MM Release.Build.

The release notes describe the new features, enhancements to the existing features, fixed issues, and known issues.

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

Known issues: The issues that exist in the current release and their workarounds, wherever applicable.

For detailed information on the supported features, see Supported features.

25.8.2 (Sep 15, 2025)

> **Important update:**
>
> - Citrix Secure Access version 25.8.2 replaces 25.8.1 and is now generally available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

- **Timeout setting support**

  The Citrix Secure Access client for Linux now supports the timeout settings configured in NetScaler Gateway and Citrix Secure Private Access deployments. For more information, see Configure time-out settings and Timeouts for user sessions.

  [CSACLIENTS-14250]

- **Support for multi-workspace URLs**

  The Citrix Secure Access client for Linux now supports multi-workspace URLs. This feature is useful for enterprises that must provide different access URLs for various user groups, such as HR, IT, contractors, or vendors. For more information, see Configure Workspace URLs.

  [CSACLIENTS-14170]

Fixed issues

- Users are unable to log in to the Citrix Secure Access client if classic authentication is configured in NetScaler Gateway.

  [CSACLIENTS-15609]

25.5.3 (May 19, 2025)

> **Important update:**
>
> - Citrix Secure Access version 25.5.3 replaces 25.5.1 and is now generally available.

What's new

- **Seamless connectivity during PoP failure**

  In a Citrix Secure Private Access deployment, if the Citrix Secure Access client users lose connectivity to the current Point of Presence (PoP), they are automatically reconnected to an alternate PoP. This failover occurs seamlessly without requiring any user action.

  [CSACLIENTS-12437]

- **Ubuntu 24.04 support for the Citrix Secure Access client and Citrix EPA client**

  The Citrix Secure Access and the Citrix EPA clients are now compatible with Ubuntu 24.04.

  [CSACLIENTS-12712]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Support for Microsoft Entra ID authentication with conditional access**

  Microsoft Entra ID authentication with conditional access is supported with the Microsoft Edge browser in the Citrix Secure Access client.

  Perform the following steps to configure the Citrix Secure Access client to use the Microsoft Edge browser for Microsoft Entra ID authentication:

  Prerequisites:

  Microsoft Edge browser must be installed on the end user's device.

  > **Note:**
  >
  > The following configuration changes must be done only if the authentication has **Entra ID with conditional access** set to **Allow only registered devices**.

  1. Open the file `/opt/Citrix/NSGClient/globalConfiguration.json` using administrator permissions.
  2. Change the value of `enable_edge_browser_auth` to **`true`**.
  3. For the changes in `globalConfiguration.json` to take effect, restart the Citrix Secure Access client.
  4. Close all the windows of the Microsoft Edge browser.

  [CSACLIENTS-13360]

Known issues

- Automatic upgrade of the Citrix Secure Access client from version 25.5.3 to a newer version through NetScaler might fail if the EPA client is not installed, resulting in a "bad signature" error.

  Workaround: Download and install the Citrix Secure Access client version 25.8.1 or later directly from the Citrix Downloads page.

  [CSACLIENTS-14788]

25.2.2 (Feb 24, 2025)

What's new

- **Support for persistent and consistent connections in Citrix Secure Private Access**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix Secure Access client supports both connector stickiness and client IP address stickiness to ensure persistent and consistent connections for applications requiring session continuity in Citrix Secure Private Access deployments. For more information, see Maintain consistent connections.

[CSACLIENTS-12438]

- **Split DNS support in Citrix Secure Private Access and NetScaler Gateway deployments**

  The Citrix Secure Access client supports split DNS in Citrix Secure Private Access and NetScaler Gateway on-premises deployments.

  [CSACLIENTS-12207]

- **Server-initiated connection support from Citrix Secure Private Access**

  The Citrix Secure Access client for Linux now supports server-initiated connections from Citrix Secure Private Access. This feature enables the admin to create an application that allows the server to initiate a TCP connection to a remote endpoint. For more information, see Support for server-to-client connections.

  [CSACLIENTS-10503]

- **Support troubleshooting in Citrix Secure Private Access deployments**

  The Citrix Secure Access client now supports troubleshooting, by using Citrix Monitor or Citrix Director, in Citrix Secure Private Access deployments.

  [CSACLIENTS-12436]

24.11.4 (Dec 03, 2024)

What's new

- **Interoperability enhancements with third-party secure web gateway**

  The Citrix Secure Access user-agent strings are updated for enhanced interoperability with the third-party secure web gateways.

  [CSACLIENTS-8595]

- **Support to triage and troubleshoot enumeration failures**

  Citrix Secure Access now supports triaging and troubleshooting enumeration failures using Citrix Monitor or Citrix Director, in Secure Private Access deployments. For more information, see Secure Private Access integration with Director (Preview).

  [CSACLIENTS-10502]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **IP address spoofing for TCP-based DNS requests**

  Citrix Secure Access supports IP address spoofing of TCP-based DNS requests in the following scenarios:

  - FQDN-based tunneling rules are configured on NetScaler Gateway.
  - FQDNs match DNS suffixes or host names configured in the applications in Citrix Secure Private Access deployment.

  [CSACLIENTS-12551]

24.10.1 (Oct 07, 2024)

What's new

- **Support for FQDN-based tunneling**

  Citrix Secure Access client for Linux supports FQDN-based tunneling for TCP and UDP applications in Secure Private Access and NetScaler Gateway on-premises deployment. For more information, see Configure connection settings in a session profile.

  > **Note:**
  >
  > - FQDN-based tunneling is supported with split tunnel **ON** and split tunnel **OFF** settings and is not supported with split tunnel **REVERSE** setting.
  > - DNS resolution is supported only with split DNS **Remote** setting and is performed over the tunnel regardless of the NetScaler® Gateway's split DNS setting.

  [CSACLIENTS-10500]

Fixed issues

- Client sessions might remain active on NetScaler Gateway and service node even after the user logs out of the Citrix Secure Access client.

  [NSHELP-38259]

24.8.5 (Sep 02, 2024)

What's new

- **Support for Secure Private Access deployments**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access for Linux supports IP address-based TCP/UDP applications in both on-premises and cloud deployments of Citrix Secure Private Access. To configure TCP/UDP apps for on-premises, see Configure TCP/UDP apps. To configure TCP/UDP apps for cloud, see Configure TCP/UDP server-client apps.

> **Note:**
>
> IP address-based TCP/UDP apps are supported in Ubuntu 18.04, Ubuntu 20.04. They are not supported in Ubuntu 22.04.

[CTXENG-341]

- **Support for nFactor authentication**

  Citrix Secure Access for Linux now supports nFactor authentication directly through the VPN client. When users log on to Citrix Secure Access for Linux, a webview window appears, prompting them to authenticate based on the admin-configured nFactor flow. For details about nFactor authentication, see nFactor authentication.

  [CTXENG-338]

Fixed issues

- EPA scan fails if the length of EPA expressions configured on NetScaler Gateway exceeds 1024 characters.

  [NSHELP-38149]

- In the Citrix Secure Access client UI, the "Choose session to transfer"section fails to display the list of transfer logon sessions when the maximum limit of the NetScaler Gateway sessions is reached.

  [CSACLIENTS-352]

23.10.3 (16-Oct-2023)

Fixed issues

For French users, the Connections page of the Citrix Secure Access for Linux UI displays the data transfer rate in KB and MB instead of Ko and Mo, respectively.

[NSOSLX-177]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

23.9.1 (08-Sep-2023)

What's new

This release addresses issues that help to improve overall performance and stability.

[CGOP-25231]

23.6.2 (20-Jun-2023)

What's new

- **Ubuntu 22.04 support for Citrix Secure Access client and Citrix EPA client**

  Ubuntu 22.04 is the latest long-term support release of Ubuntu. The Citrix Secure Access and Citrix EPA clients are compatible with Ubuntu 22.04. For more information, see Client software requirements.

  [CGOP-24312]

- **GSLB support for Citrix Secure Access and Citrix EPA clients**

  The Citrix Secure Access client and Citrix EPA client for Ubuntu support the Global Server Load Balancing (GSLB) feature on NetScaler Gateway. By configuring GSLB for NetScaler Gateway, admins can ensure that the enterprise network (intranet resources) is always available to end-users from any geographic location. GSLB also addresses disaster situations or network outages wherein users of one data center can be redirected to another data center. For more information, see Support for active-active GSLB deployments on NetScaler Gateway.

  [CGOP-23506]

- **HTTPOnly support for Citrix Secure Access and Citrix EPA clients**

  The Citrix Secure Access and Citrix EPA clients support the HTTPOnly flag on the authentication cookies. NetScaler Gateway admins configure the HTTPOnly feature on the authentication cookies that are generated by web applications. This feature helps in preventing cookie theft due to cross-site scripting. For more information, see Enforce the HttpOnly flag on authentication cookies.

  [CGOP-23517]

Support for Microsoft Entra ID authentication with conditional access

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting from the Citrix Secure Access client for Linux release 25.5.1, Microsoft Entra ID authentication with conditional access is supported with the Microsoft Edge browser.

Perform the following steps to configure the Citrix Secure Access™ client to use the Microsoft Edge browser for Microsoft Entra ID authentication:

Prerequisites:

Microsoft Edge browser must be installed on the end user's device.

> **Note:**
>
> The following configuration changes must be done only if the authentication has **Entra ID with conditional access** set to **Allow only registered devices**.

1. Open the file `/opt/Citrix/NSGClient/globalConfiguration.json` using administrator permissions.
2. Change the value of `enable_edge_browser_auth` to **`true`**.
3. For the changes in `globalConfiguration.json` to take effect, restart the Citrix Secure Access client.
4. Close all the windows of the Microsoft Edge browser.

Citrix Secure Access for Android

September 8, 2026

Citrix Secure Access (formerly Citrix SSO) for Android provides 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.

> **Important:**
>
> - Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.
> - Citrix Secure Access client for Android works within the Android subsystem built on ChromeOS. It works with ChromeOS if installed as an Android app from the Play Store and can tunnel any application within the Android subsystem.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release notes

September 29, 2026

> **Important:**
>
> - Citrix SSO for Android is now renamed to Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change. You might notice Citrix SSO references used in the documentation during this transition period.
> - FQDN based split tunneling and nFactor authentication support are currently in preview.
> - Citrix Secure Access is not supported for Android 11 and lower versions after May 2025.

The Citrix Secure Access release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes include one or more of the following sections:

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

Known issues: The issues that exist in the current release and their workarounds, wherever applicable.

V26.08.1 (Sep 08, 2026)

What's new

- **Removed support for Android 12 and older versions**

  The Citrix Secure Access application no longer supports Android 12 and older versions.

  [CTXENG-17872]

- **Support for Android 16/17 SDK requirements**

  The Citrix Secure Access application now supports Android 16/17 SDK requirements.

  [CTXENG-17219]

- **Allow local network access on Android 17 and later**

  When users install, reinstall, or update Citrix Secure Access application on Android 17 and later, they are prompted to allow local network access. If access is denied, certain local network services, such as Wi-Fi printers, might be unavailable when a VPN session begins.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

MDM administrators are advised to pre-grant this permission to the Citrix Secure Access application.
For details, see How to use Citrix Secure Access from your Android device.

[CTXENG-17213]

V26.06.1 (Jun 23, 2026)

What's new

- This release addresses some issues to improve the overall performance and stability.

V26.04.1 (Apr 28, 2026)

What's new

- **Single sign-on between Citrix Secure Access and Citrix Workspace app for Android**

  Starting from Citrix Secure Access for Android version 26.04.1, single sign-on (SSO) is supported with Citrix Workspace app (CWA). If a user is already signed in to the Citrix Workspace app, they do not need to enter credentials again when signing in to the same URL in Citrix Secure Access for Android, and vice versa.

  Also, if a user signs out of the Citrix Secure Access app, the user is also logged out of the Citrix Workspace app, and vice versa. This behavior enables seamless access to TCP/UDP applications and provides a unified Secure Private Access experience. This signout synchronization is enabled by default. To disable it, contact Citrix Support. For details, see Single sign-on to Citrix Secure Access through Citrix Workspace app for Android.

  [CTXENG-72640]

V26.01.1 (Feb 02, 2026)

Fixed issues

- Always On VPN with Intranet IP assignment to devices might intermittently enter a continuous reconnection loop.

  [NSHELP-41567]

- The Citrix Secure Access app does not remember the last used tab across app restarts.

  [CSACLIENTS-8804]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Secure Access app might crash when processing fragmented UDP traffic.

  [NSHELP-41931]

- The Citrix Secure Access app fails to establish a VPN session if the home page in the VPN session profile on NetScaler Gateway is set to none.

  [NSHELP-42016]

V25.11.1 (Dec 08, 2025)

What's new

- **Support for forced timeout notification**

  The Citrix Secure Access application now displays notifications for forced timeout warnings, if configured on NetScaler Gateway. For more information, see Configure time-out settings.

  [CSACLIENTS-14865]

- **Support for Android 15 SDK requirements**

  The Citrix Secure Access app now supports Android 15 SDK requirements. Support for TLS 1.0 and TLS 1.1 is removed for the devices running Android 15 and later versions.

  [CSACLIENTS-12949]

- **Support for Secure Private Access**

  The Citrix Secure Access client for Android now supports Secure Private Access deployments. It provides basic tunneling for TCP/UDP applications. If access to any TCP/UDP application is not allowed through the client's session, the application notifies you, provided notification permissions are enabled for the Citrix Secure Access application.

  When adding a connection in the Citrix Secure Access application, you must use the StoreFront base URL. For more information about adding a connection, see How to use Citrix Secure Access from your Android device.

  Related topics

  - Citrix Secure Access client features supported in Citrix Secure Private Access
  - Citrix Secure Private Access for mobile devices

  [CSACLIENTS-14743]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V25.07.1 (Oct 14, 2025)

What's new

- **Removed support for Android 11 and older versions**

  The Citrix Secure Access application no longer supports Android 11 and older versions.

  [CSACLIENTS-14340]

- **Enhanced signature verification with Google Play app signing**

  The Citrix Secure Access client application now uses Google Play app signing for enhanced signature verification.

  [CSACLIENTS-12738]

V25.03.3 (Jun 30, 2025)

Fixed issues

- After upgrading to version 25.03.1, the Citrix Secure Access client might fail to re-establish the Always On VPN connection and an error message "Interactive user authentication not supported for Always-On VPN"is displayed.

  [NSHELP-40268]

V25.03.2 (Jun 13, 2025)

What's new

- This release addresses some issues to improve the overall performance and stability.

V25.03.1 (May 28, 2025)

What's new

- **Support for periodic monitoring of Always On VPN mode**

  Support is now added for periodic monitoring of Always On VPN mode to ensure that the Citrix Secure Access client automatically restarts if it is terminated by a Google Play Services update.

  [CSACLIENTS-13203]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- In Always On VPN mode, the Citrix Secure Access app might repeatedly attempt to reconnect to the VPN if the gateway name resolves to multiple IP addresses using round robin DNS load balancing method.

  [NSHELP-39872]

V25.02.1 (Mar 19, 2025)

Fixed issues

- Users might be unable to access intranet applications using FQDN through the Citrix Secure Access app if the DNS response contains CNAME records.

  [NSHELP-39375]

- In Always On VPN mode, the Citrix Secure Access client might not restart the VPN session without manual intervention when the device goes into idle or power save modes.

  [CSACLIENTS-12477]

V24.11.1 (Dec 02, 2024)

What's new

- **Support for Android 14 SDK requirements**

  The Citrix Secure Access app now supports Android 14 SDK requirements.

  [CSACLIENTS-9577]

- **Support for per-app language setting**

  The Citrix Secure Access app now supports per-app language system setting.

  [CSACLIENTS-6250]

Fixed issues

- The Citrix Secure Access app might show a transfer login prompt even when Always On VPN is enabled.

  [NSHELP-38858]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V24.10.1 (Oct 10, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

Fixed issues

- Push notification might not work on the Citrix Secure Access client for Android.

  [NSHELP-38679]

- The Always On feature might not restart the NetScaler Gateway session after an idle session time-out.

  [NSHELP-38354]

V24.08.2 (Sep 26, 2024)

What's new

- This release addresses some issues to improve the overall performance and stability.

V24.08.1 (Sep 09, 2024)

What's new

- **Interoperability enhancements with third-party secure web gateway**

  The User-Agent strings for Citrix Secure Access have been updated for an enhanced interoperability with third-party secure web gateways. For more information, see Defining Clients.

  [CSACLIENTS-10798]

- **Enhanced security feature in Citrix Secure Access app for Android**

  Third-party apps in the user's device can not take screenshots of the Citrix Secure Access app when sensitive information is displayed during login authentication.

  [CSACLIENTS-11671]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- Citrix Secure Access app displays certificates, which are not appropriate for SAML authentication.

  [NSHELP-38431]

V24.04.1 (May 03, 2024)

- **Enhancements to the Always On VPN profile**

  Citrix Secure Access now supports the 'Always On VPN'(optional) property in the VPN profiles. This property determines whether a VPN profile is an Always On VPN profile or not. When this property is set to True, it indicates that the VPN profile is an Always On VPN profile.

  > **Note:**
  >
  > This property can be set only on the main VPN profiles. It cannot be set for the additional VPN profiles.

  The Always On VPN tunnel is re-established in the following scenarios:

  - MDM profile update
  - Reboot of the Android device
  - Reconnect to a different NetScaler Gateway during a network connection failure
  - Reconnect after a NetScaler Gateway session expires when the Android device is in power saving mode. The connection is re-established when the device comes out of the power saving mode.

  For details, refer to the following articles:

  - VPN configuration using configuration designer
  - Configure VPN profiles for Android Enterprise
  - Configure the Citrix SSO protocol for Android

  [CSACLIENTS-9668]

V23.12.2 (15-Dec-2023)

> **Note:**
>
> Citrix Secure Access for Android version 23.12.2 includes the fix for CSACLIENTS-8799 and replaces version 23.12.1.

[CSACLIENTS-8799]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

- **Citrix SSO for Android renamed to Citrix Secure Access**

  Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

  [CSACLIENTS-6337]

- **Receive or block notifications on an Android 13+ devices**

  When installing or reinstalling Citrix Secure Access client on an Android 13 device, end-users are now prompted to provide permissions to receive notifications from Citrix Secure Access client. If end-users deny the permission, they will not receive any VPN status or push notifications from Citrix Secure Access client on their Android devices. MDM admins are advised to grant the notification permission to Citrix Secure Access (Package ID: `com.citrix.CitrixVPN`) in their solution.

  End-users can navigate to **Settings > Notifications** on the Android device to change the notification permission for
  Citrix Secure Access client. For details, see How to use Citrix Secure Access from your Android device.

  [CSACLIENTS-8252]

- **Support for Transfer Logon in Always On VPN mode**

  Citrix Secure Access for Android now supports the Transfer Logon functionality in the Always On VPN mode. For details about how to configure Transfer Logon, see Configure the Transfer Logon page.

  [CSACLIENTS-8305]

Fixed issues

- Citrix Secure Access crashes when users copy the Time-based OTP (TOTP) token on the Android 13+ device.

  [CSACLIENTS-8799]

V23.10.2 (19-Dec-2023)

What's new

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Notes:**
>
> - Citrix SSO for Android version 23.10.2 includes the fix for CSACLIENTS-8314 and replaces version 23.10.1.
> - Citrix SSO for Android 23.10.1 works with Android 14.

- **Reauthenticate with NetScaler Gateway after a VPN connection failure - Preview**

  Citrix SSO for Android now prompts you to reauthenticate with NetScaler Gateway when a VPN connection is lost. You are notified on the Citrix SSO 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. This feature is in preview.

  For more information, see Reconnect to NetScaler Gateway after a VPN connection failure.

Fixed issues

Citrix SSO crashes intermittently when restarting the VPN service in certain Always On VPN scenarios.

[CSACLIENTS-8314]

V23.8.1 (31-Aug-2023)

What's new

- **Automatic restart of Always On VPN**

  The Citrix SSO app automatically restarts the Always On VPN when an app that is part of the allow or block list is installed in a work profile or a device profile. Traffic from this app is automatically tunneled over a VPN connection without restarting the work profile or rebooting the device. To enable the automatic restart of Always On VPN, end users must grant the Query all packages consent to the Citrix SSO app. For more information, see Automatic restart of Always On VPN.

  [CSACLIENTS-6158]

- **Enable debug logging in a managed VPN profile**

  MDM admins can now enable debug logging as a custom parameter in the managed VPN profile of the Endpoint Management console. To enable debug logging, the value of `EnableDebugLogging` must be set to True. If any of the managed VPN configurations has debug logging enabled, the debug logging functionality takes effect when the configurations are parsed. For more details, see Custom parameters for Intune configuration.

  [CSACLIENTS-3746]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- Sometimes, the Citrix SSO app might fail to tunnel the traffic to some resources. This issue occurs when split tunneling is set to OFF and some unreachable domains or IP addresses are blackholed.

  [NSHELP-35555]

V22.11.1 (30-Nov-2022)

What's new

- **Citrix Secure Access is updated to target Android 12.1 (API level 32)**

  Citrix Secure Access is now updated to target Android 12.1 (API level 32). In case of per-app VPN, the VPN service might not restart automatically, if one of the packages in the per-app VPN package list is installed after the VPN tunnel setup. This is due to the app visibility restrictions introduced in Android 11. For details, see Package visibility.

  [CGOP-21409]

V22.10.1 (21-Oct-2022)

What's new

- Display of the app's version number is updated to the format YY.MM.point-release, where YY is the 2-digit year, MM is the 2-digit month, and point-release that is 1+ depending on the release number within a month.
- Google Analytics/Crashlytics data collection from EU region is disabled for Android clients.

Fixed issues

- Error messages that appear for an invalid input in the Add Connection and Edit connection screens are not localized.

  [CGOP-22060]

V2.5.3 (05-May-2022)

What's new

- Citrix SSO updated to Android 11 target SDK (API 30)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Citrix SSO app is now updated to Android 11 target SDK (API 30). This change requires that Microsoft Intune NAC v2 APIs are used by NetScaler Gateway for device compliance check. For details, refer to the KB article CTX331615.

[CGOP-19774]

Fixed issues

- Sometimes, Citrix SSO might not use an alternate DNS server for host name resolution after a network change.

  [NSHELP-29378]

V2.5.2 (21-Oct-2021)

Fixed issues

- Sometimes, Citrix SSO crashes when handling a non-compliance error in NAC check.

  [CGOP-19198]

V2.5.1 (12-Aug-2021)

Fixed issues

- Citrix SSO app fails to resolve host when the CNAME chain is longer than 6 hops.

  [CGOP-18475]

- Citrix SSO displays an authentication prompt when NAC check only authentication is required by NetScaler Gateway.

  [CGOP-18348]

- Citrix SSO might crash while processing unusually large ICMP packets.

  [CGOP-18286]

- Citrix SSO might crash when adding a VPN profile on some Android 8.0 devices.

  [CGOP-17607]

- Citrix SSO might crash when you restart the VPN configured for Always On.

  [CGOP-17580]

- Citrix SSO might crash when handling an SSL error in the nFactor authentication flow.

  [CGOP-17577]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2.5.0 (08-Jun-2021)

What's new

- **Support for FQDN based split tunneling**

  Citrix SSO for Android now supports FQDN based split tunneling.

  [CGOP-12079]

Fixed issues

- Citrix SSO preview build 2.5.0 fails (110) to connect to NetScaler Gateway versions 12.1 and earlier.

  [CGOP-17735]

- The "DisableUserProfiles"setting is not applied after the SSO app is restarted.

  [CGOP-17454]

V2.4.16 (31-Mar-2021)

Fixed issues

- The nFactor authentication is aborted if safe browsing is not be enabled on some devices.

  [CGOP-17514]

V2.4.15 (17-Mar-2021)

Fixed issues

- Sometimes, Citrix SSO does not reconnect Always On VPN when session timeout happens on the NetScaler Gateway appliance.

  [CGOP-16800]

V2.4.14 (23-Feb-2021)

Fixed issues

- Citrix SSO requires user interaction when Always-On VPN with certificate only authentication is used along with nFactor authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[CGOP-16805]

- Sometimes, Citrix SSO might crash during VPN service restart or transition.

  [CGOP-16766]

V2.4.13 (04-Feb-2021)

Fixed issues

- In some cases, the Citrix SSO login request times out before NetScaler Gateway responds.

  [CGOP-16759]

V2.4.12 (15-Jan-2021)

This release addresses various issues that help to improve overall performance and stability.

V2.4.11 (08-Jan-2021)

- Classic authentication fails because the Citrix SSO sends an HTTP header (X-Citrix-Gateway) to the NetScaler Gateway which is used only in nFactor authentication.

  [CGOP-16449]

V2.4.10 (09-Dec-2020)

Fixed issues

- Sometimes, classic authentication might fail for Android devices.

  [CGOP-16219]

- Citrix SSO might crash when performing classic authentication.

  [CGOP-16012]

- The orientation of the Citrix SSO app does not change when you rotate the device.

  [CGOP-639]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2.4.9 (20-Nov-2020)

Fixed issues

- Citrix SSO app crashes when a user taps the TOTP token value on the device.

  [CGOP-15886]

V2.4.8 (04-Nov-2020)

Fixed issues

- Citrix SSO might crash when disconnecting the VPN after a session timeout on the gateway.

  [CGOP-15592]

V2.4.7 (12-Oct-2020)

This release addresses various issues that help to improve overall performance and stability.

V2.4.6 (28-Sep-2020)

This release addresses various issues that help to improve overall performance and stability.

V2.4.5 (16-Sep-2020)

What's new

- New NetScaler® logo is introduced.

  [CGOP-15327]

V2.4.4 (10-Sep-2020)

Fixed issues

- Sometimes, Citrix SSO crashes when reconnecting the VPN session.

  [CGOP-15215]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2.4.3

Known issues

- Citrix SSO fails to establish a VPN session to NetScaler Gateway when the Android device is resource constrained.

  [NSHELP-24647]

V2.4.2

Fixed issues

- Citrix SSO app crashes when loading previously saved corrupt token data. With this fix, the token value is displayed as "Token data corrupted"for corrupt tokens in the token list. Remove the corrupt tokens and add it again.

  [CGOP-14546]

V2.4.1

Fixed issues

- Citrix SSO app is not supported for Android 6.x and lower versions after June 2020.

  [CGOP-13853]

V2.3.19

This release addresses various issues that help to improve overall performance and stability.

V2.3.18

What's New

- Proxy configuration is now supported in the Android Citrix SSO app for Android 10 devices.

  [CGOP-12007]

V2.3.17

This release addresses various issues that help to improve overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2.3.16

This release addresses various issues that help to improve overall performance and stability.

V2.3.15

What's New

- Citrix SSO app now supports NetScaler Gateway certificate pinning for managed VPN profiles.

  [CGOP-12538]
- Citrix SSO app for Android 10 now detects Always On VPN from the system settings.

  [CGOP-12656]

Fixed issues

- Citrix SSO app crashes when disconnecting from VPN if there are only MDM VPN profiles defined.

  [CGOP-13825]

V2.3.14

What's New

- Citrix SSO app can now perform user authentication on behalf of Citrix Workspace app for native app single sign-on.

  [CGOP-12083]
- VPN service restarts if one of the packages in the per-app VPN package list is installed after the VPN tunnel setup.

  [CGOP-11262]

Fixed issues

- Citrix SSO now correctly handles the final VPN session establishment message.

  [CGOP-12488]
- The NetScaler Gateway IP address is now resolved only once. Earlier, the NetScaler Gateway IP address was resolved multiple times that resulted in connection failures sometimes.

  [CGOP-12101]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues

- Always-On VPN status is not always updated correctly in the app user interface.

  [NSHELP-21709]

V2.3.13

Fixed issues

- The NetScaler Gateway IP address is now resolved only once.

  Earlier, the NetScaler Gateway IP address was resolved multiple times that resulted in connection failures sometimes.

  [CGOP-12101]

Known issues

- Always-On VPN status is not always updated correctly in the app user interface.

  [NSHELP-21709]

V2.3.12

Fixed issues

- Citrix SSO might crash when saving a VPN profile.

  [CGOP-12137]

V2.3.11

Fixed issues

- Citrix SSO might crash when saving a VPN profile.

  [CGOP-12137]

- The disableUserProfile setting is not correctly reflected in the user interface when a new VPN profile or update to an existing profile results in the change of the disableUserProfile value.

  [CGOP-11899]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix SSO for Android does not process VPN profiles in Device Owner (DO) mode.

  [CGOP-11981]

- VPN connection is not established when there are IPv6 only local DNS servers.

  [CGOP-12053]

V2.3.10

Fixed issues

- VPN connection lost after some idle time on the device.

  [CGOP-11381]

V2.3.8

What's new

- **Set up Citrix SSO app in an Intune Android Enterprise environment**

  You can now set up the Citrix SSO app in an Intune Android Enterprise environment. For details, see Set up Citrix Secure Access in an Intune Android Enterprise environment.

  [CGOP-635]

- **Support for VPN profile provisioning via Android Enterprise**

  VPN profile provisioning via Android Enterprise is now supported.

  [CGOP-631]

Fixed issues

- If you save a token that is already saved and then try to open it, garbled characters appear in the token name.

  [CGOP-11696]

- Citrix SSO app fails to establish a VPN session if no DNS search domains are configured on NetScaler Gateway.

  [CGOP-11259]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

V2.3.6

What's new

- **Always On support for Citrix SSO**

  The Always On feature of Citrix SSO ensures that users are always connected to the enterprise network. This persistent VPN connectivity is achieved by an automatic establishment of a VPN tunnel.

  [CGOP-10015]

- **Notification to relogin is displayed if Athena token expiry causes a logout**

  A notification prompting the users to relogin to Citrix Workspace is displayed if the following conditions are met.

  - Always On feature is enabled in the Citrix Workspace provisioned VPN profile
  - Athena authentication is used for SSO
  - User is signed out of the Citrix Workspace app because of Athena token expiry

  [CGOP-10016]

- **Registration for Push notification service is done using NetScaler Gateway**

  You can now register for push notification service using the NetScaler Gateway appliance. Earlier the registration was done on the client device.

  [CGOP-10542]

Fixed issues

Sometimes, Citrix SSO crashes when a new token is scanned. For example, Citrix SSO crashes when an existing token is deleted and another one is scanned with the same token name.

[CGOP-10818]

V2.3.1

What's new

- **Managed configurations are updated to include more user settings**

  Managed configurations are updated to include "BlockUntrustedServers," "DefaultProfileName," and "DisableUserProfiles" settings for Android Enterprise environments.

  [CGOP-10033]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Enhanced Push notification support**

  Upon configuring NetScaler Gateway for Push Notification with type "OTP," PIN/fingerprint is not asked after the user selects "Allow" in response to the Push Notification requesting the user's consent for allowing the authentication to proceed.

  [CGOP-9843]

- **Firebase Analytics support**

  Support for basic Firebase Analytics is added to provide usage information about the Citrix SSO app. The enhancement is applicable to coarse geolocations, screen usage, different versions of Android in use and so on.

  [CGOP-7523]

- **Support for Android Managed Configurations based VPN profile configuration**

  Citrix SSO app can be configured in the Android Enterprise environment using an EMM/UEM vendor like Citrix Endpoint Management. The Android Enterprise Managed Configurations wizard in CEM can be used to deploy managed VPN configurations to the Citrix SSO app. For information on how to configure the Citrix SSO app using Managed Configurations, refer VPN device policy.

V2.2.9

What's new

- **Push Notification support**

  NetScaler Gateway sends a push notification on your registered mobile device for a simplified two-factor authentication experience.

  [CGOP-9592]

Fixed issues

- Non-URL characters are allowed in the Server field under the Add Connection screen.

  [CGOP-588]

Set up Citrix Citrix Secure Access in an MDM enviroment

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

To set up Citrix Secure Access in an MDM environment, see Configure Citrix Secure Access protocol for Android.

> **Notes:**
>
> - In a Non-MDM environment, users create VPN profiles manually.
> - You can also create an Android Enterprise managed configuration for Citrix Secure Access. For details, see Configure VPN profiles for Android Enterprise.
> - For Android 13+ users using Citrix Secure Access 23.12.1 and above, MDM admins are advised to grant the notification permission to Citrix Secure Access (Package ID: `com.citrix.CitrixVPN`) in their solution.

Set up Citrix Secure Access in an Intune Android Enterprise environment

September 29, 2026

> **Important:**
>
> Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

The topic captures details about deploying and configuring Citrix Secure Access through Microsoft Intune. This document assumes that Intune is already configured for Android Enterprise support and device enrollment is already done.

Prerequisites

- Intune is configured for Android Enterprise Support
- Device enrollment is complete

To set up Citrix Secure Access in an Intune Android Enterprise environment

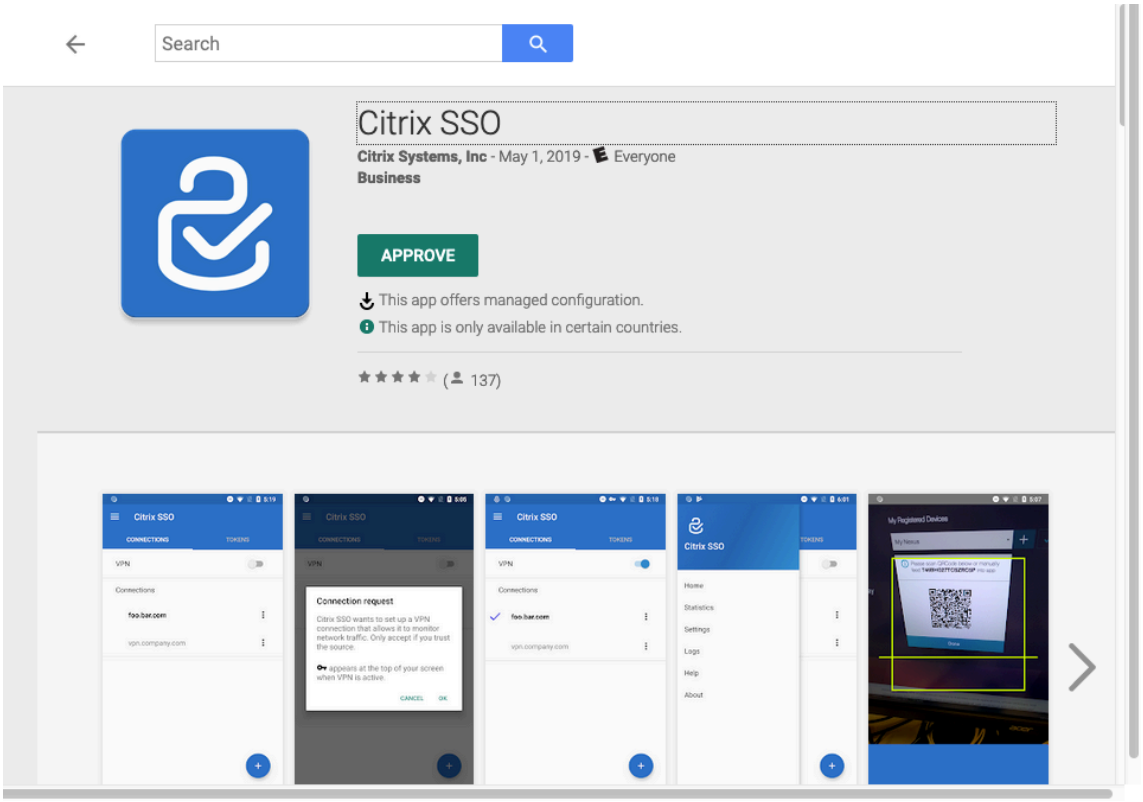
- Add Citrix Secure Access as a managed app
- Configure managed app policy for Citrix Secure Access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add Citrix Secure Access as a managed app

1. Log in to your Azure portal.
2. Click **Intune** on the left navigation blade.
3. Click **Client Apps** in the Microsoft Intune blade and then click Apps in the Client apps blade.
4. Click **+Add link** in the top right menu options. The Add app configuration blade appears.
5. Select **Managed Google Play** for the app type.

   This adds Manage Google Play search and approve blade if you have configured Android Enterprise.
6. Search for Citrix Secure Access and select it from the list of apps.



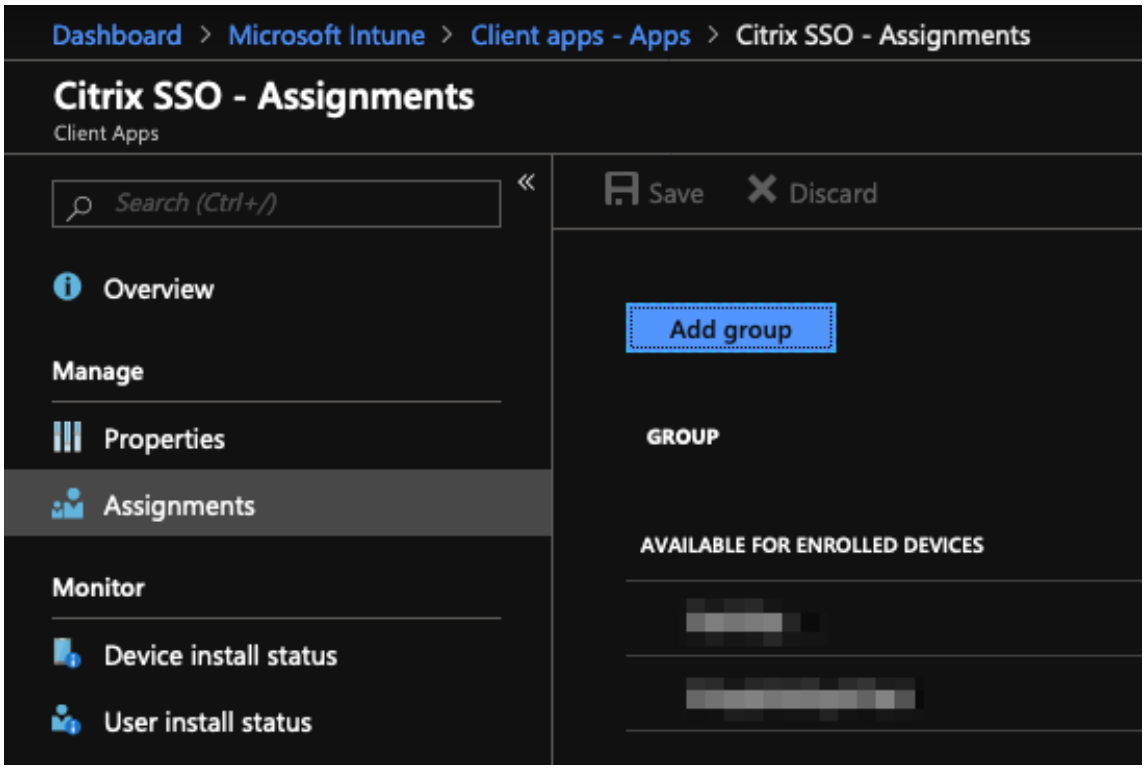
   Note: If Citrix Secure Access does not appear in the list, it means that the app is not available in your country.
7. Click **APPROVE** to approve Citrix Secure Access for deployment through Managed Google Play store.

   The permissions that are required by the Citrix Secure Access are listed.
8. Click **APPROVE** to approve the app for deployment.
9. Click **Sync** to sync this selection with Intune.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Access is added to the Client apps list. You might have to search for the Citrix Secure Access if there are many apps added.

10. Click **Citrix Secure Access** app to open the app details blade.
11. Click **Assignments** in the details blade. **Citrix Secure Access - Assignments** blade appears.



12. Click **Add group** to assign the user groups to which you want to give permission to install Citrix Secure Access, and click **Save**.
13. Close the Citrix Secure Access details blade.

Citrix Secure Access is added and enabled for deployment to your users.

Configure managed app policy for Citrix Secure Access

After Citrix Secure Access is added, you must create a managed configuration policy for Citrix Secure Access so that the VPN profile can be deployed to Citrix Secure Access on the device.

1. Open the **Intune** blade in your Azure portal.
2. Open **Client Apps** blade from the Intune blade.
3. Select **App configuration policies** item from the Client apps blade and click **Add** to open the **Add configuration policy** blade.
4. Enter a name for the policy and add a description for it.

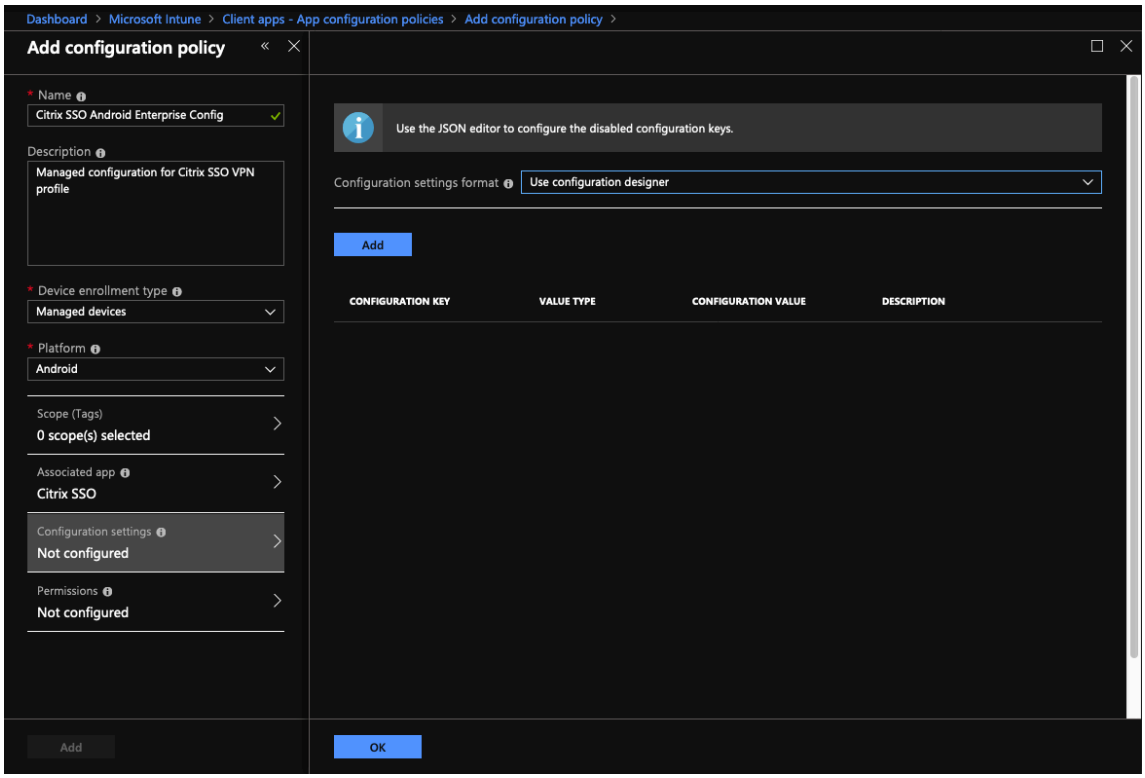
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. In **Device enrollment type**, select **Managed devices**.
6. In **Platform**, select **Android**.

   This adds another configuration option for the associated app.
7. Click **Associated app** and select **Citrix Secure Access** app.

   You might have to search for it if you have many apps.
8. Click **OK**. A configuration settings option is added in the Add configuration policy blade.
9. Click **Configuration** settings.

   A blade to configure Citrix Secure Access appears.
10. In **Configuration Settings**, select either **Use configuration designer**or **Enter JSON data** to configure the Citrix Secure Access.



> **Note:**
>
> For simple VPN configurations it is recommended to use the configuration designer.

VPN configuration using configuration designer

1. In **Configuration Settings**, select **Use configuration designer** and Click **Add**.

   You are presented with a key value entry screen for configuring various properties that are supported by Citrix Secure Access. At a minimum you must configure the **Server Address** and **VPN**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Profile Name properties. You can hover over the **DESCRIPTION** section to get more information about each property.

2. For example, select **VPN Profile Name** and **Server Address(*)** properties and click **OK**.

   This adds the properties to the configuration designer. You can configure the following properties.

   - **VPN Profile Name**. Type a name for the VPN profile. If you are creating more than one VPN profile, use a unique name for each. If you do not provide a name, the address you enter in the Server Address field is used as the VPN profile name.
   - **Server Address(*)**. Type your NetScaler Gateway base FQDN. If your NetScaler Gateway port is not 443, also type your port. Use URL format. For example, `https://vpn.mycompany.com:8443`.
   - **Username (optional)**. Enter the user name that the end users use to authenticate to the NetScaler Gateway. You can use the Intune config value token for this field if the gateway is configured to use it (see config value tokens.) If you do not provide a user name, users are prompted to provide a user name when they connect to NetScaler Gateway.
   - **Password (optional)**. Enter the password that end users use to authenticate to the NetScaler Gateway. If you do not provide a password, users are prompted to provide a password when they connect to NetScaler Gateway.
   - **Certificate Alias (optional)**. Provide a certificate alias in the Android KeyStore to be used for client certificate authentication. This certificate is pre-selected for users if you are using certificate-based authentication.
   - **Gateway Certificate Pins (optional)**. JSON object describing certificate pins used for NetScaler Gateway. Example value: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. For details, see NetScaler Gateway certificate pinning with Android Citrix Secure Access.
   - **Per-App VPN Type (optional)**. If you are using a per-app VPN to restrict which apps use this VPN, you can configure this setting.
     - If you select **Allow**, network traffic for app package names listed in the PerAppVPN app list is routed through the VPN. The network traffic of all other apps is routed outside the VPN.
     - If you select **Disallow**, network traffic for app package names listed in the PerAppVPN app list are routed outside the VPN. The network traffic of all other apps is routed through the VPN. Default is Allow.
   - **PerAppVPN app list**. A list of apps whose traffic is allowed or disallowed on the VPN, depending on the value of Per-App VPN Type. List the app package names separated by com-

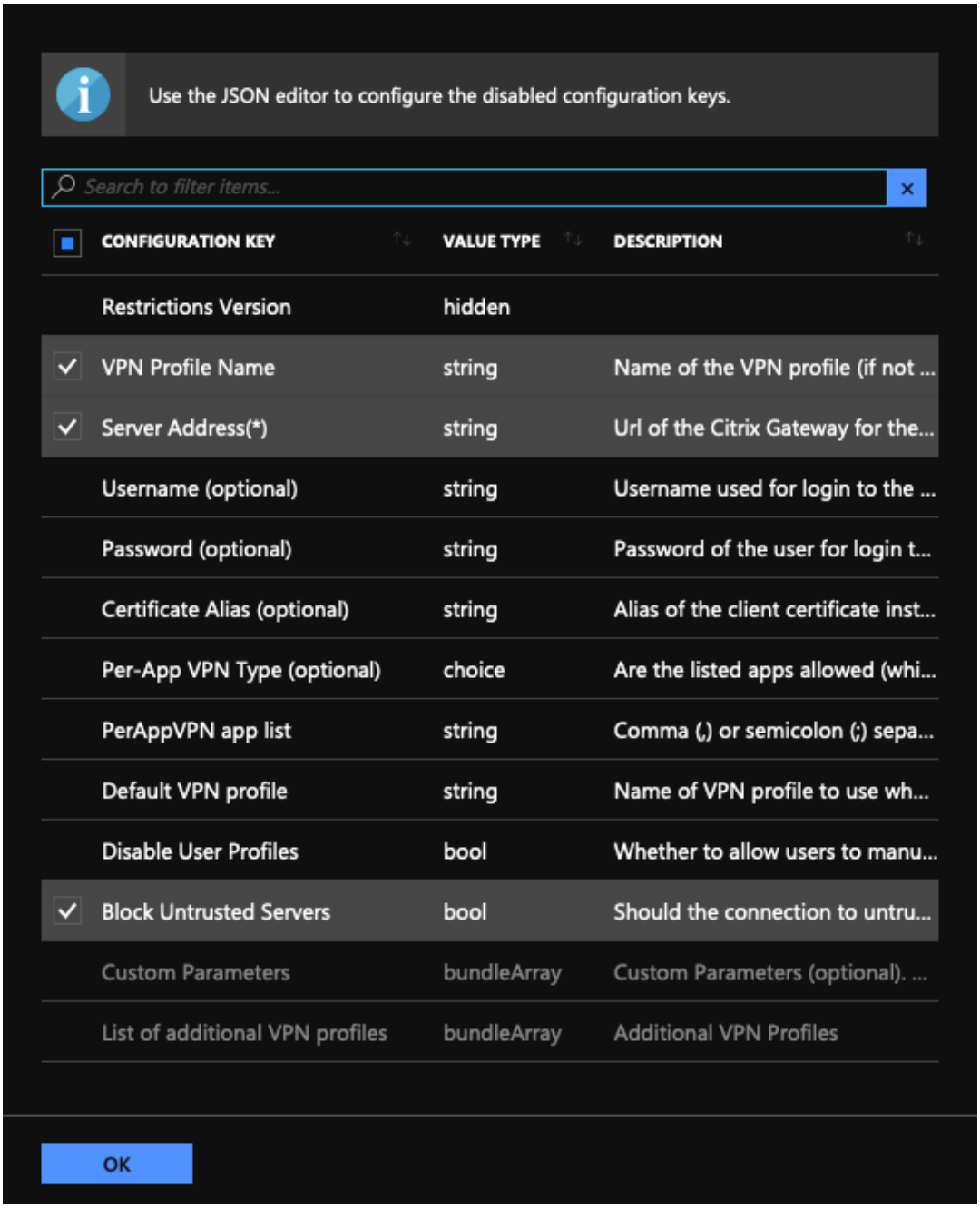
© 1997–2026 Citrix Systems, Inc. All rights reserved.

mas or semicolons. App package names are case sensitive and must appear on this list exactly as they appear in the Google Play store. This list is optional. Keep this list empty for provisioning device-wide VPN.

- **Default VPN profile**. The VPN profile name used when Always On VPN is configured for Citrix Secure Access. If this field is empty, the main profile is used for the connection. If only one profile is configured, it is marked as the default VPN profile.
- **Always On VPN (optional):** When set to True, it indicates that the VPN profile is an Always On VPN profile. This property can be set only for the main VPN profile. It cannot be set for the additional VPN profiles. By default, this property is set to False.

  > **Note:**
  >
  > The `Always On VPN (optional)` property is available from Citrix Secure Access for Android 24.04.1 onwards.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note:

- For making Citrix Secure Access as an Always On VPN app in Intune, use VPN provider as custom and `com.citrix.CitrixVPN` as the app package name.
- Only certificate-based client authentication is supported for Always On VPN by Citrix Secure Access.
- Admins must select **Client Authentication** and set **Client Certificate** to **Mandatory**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> in the **SSL Profile** or **SSL Properties** on the NetScaler Gateway for Citrix Secure Access to work as intended.

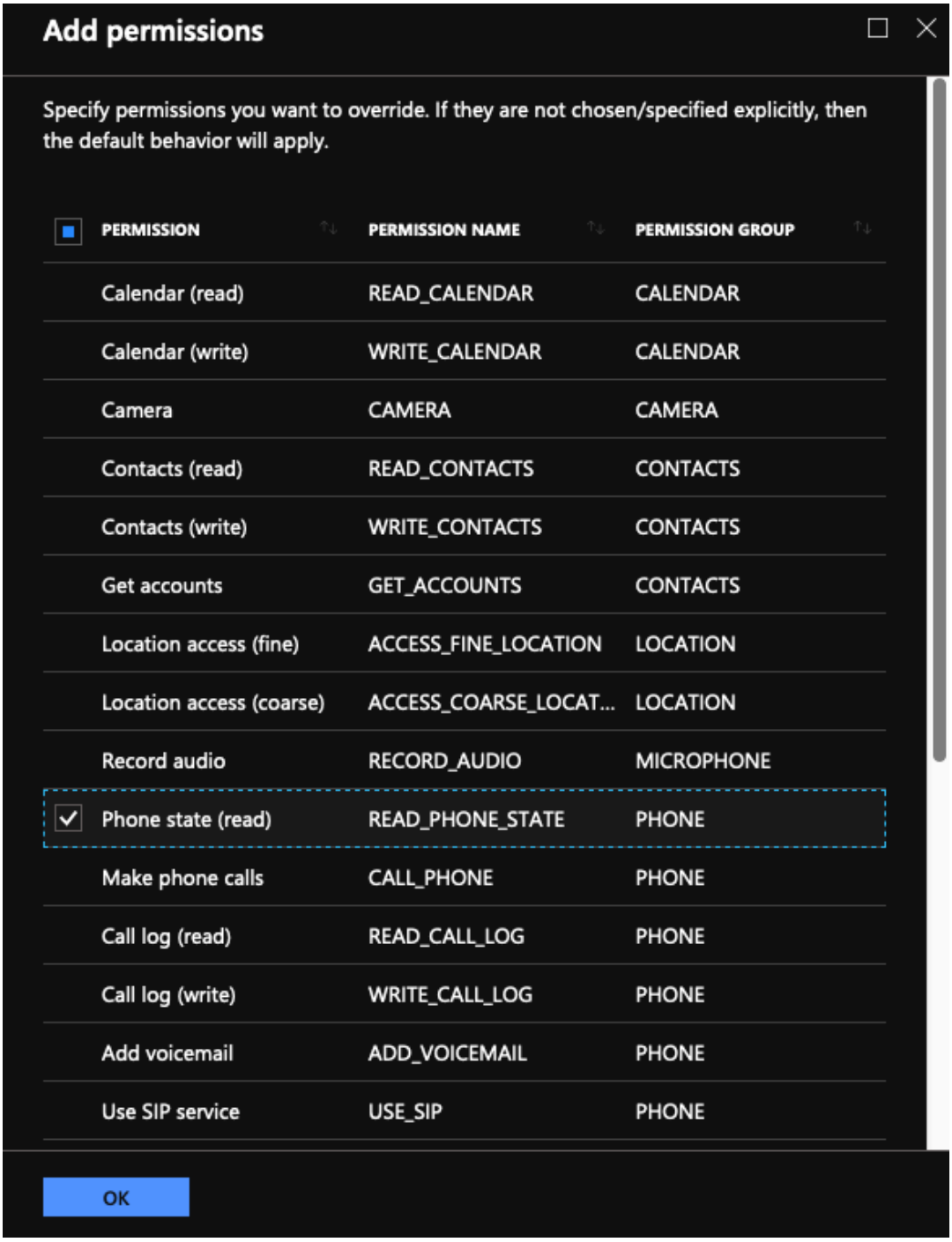
- **Disable User Profiles**
  - If you set this value to true, users cannot add new VPN profiles on their devices.
  - If you set this value to false, users can add their own VPNs on their devices.

  The default value is false.
- **Block Untrusted Servers**
  - Set this value to false when using a self-signed certificate for NetScaler Gateway or when the root certificate for the CA issuing the NetScaler Gateway certificate is not in the system CA list.
  - Set this value to true to enable the Android operating system validate the NetScaler Gateway certificate. If the validation fails, the connection is not allowed.

  The default value is true.

3. For the **Server Address(*)** property, enter your VPN gateway base URL (for example, `https://vpn.mycompany.com`).
4. For **VPN Profile Name**, enter a name that is visible to the end user in the Citrix Secure Access client's main screen (for example, My Corporate VPN).
5. You can add and configure other properties as appropriate to your NetScaler Gateway deployment. Click **OK** when you are done with configuration.
6. Click the **Permissions** section. You can grant the following permissions required by Citrix Secure Access:
   - If you are using the Intune NAC check, Citrix Secure Access requires that you grant **Phone state (read)** permission. Click **Add** button to open permissions blade. Currently, Intune displays a significant list of permissions that are available to all the apps.
   - If you are using Intune NAC check, select **Phone state (read)** permission and click **OK**. This adds it to the list of permissions for the app. Select either **Prompt** or **Auto grant** so that the Intune NAC check can work and click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- You are advised to autogrant notifications permissions to Citrix Secure Access.

> **Note:**
>
> For Android 13+ users using Citrix Secure Access 23.12.1 and above, MDM admins are advised to grant the notification permission to Citrix Secure Access (package ID: `com.citrix.CitrixVPN`) in their solution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

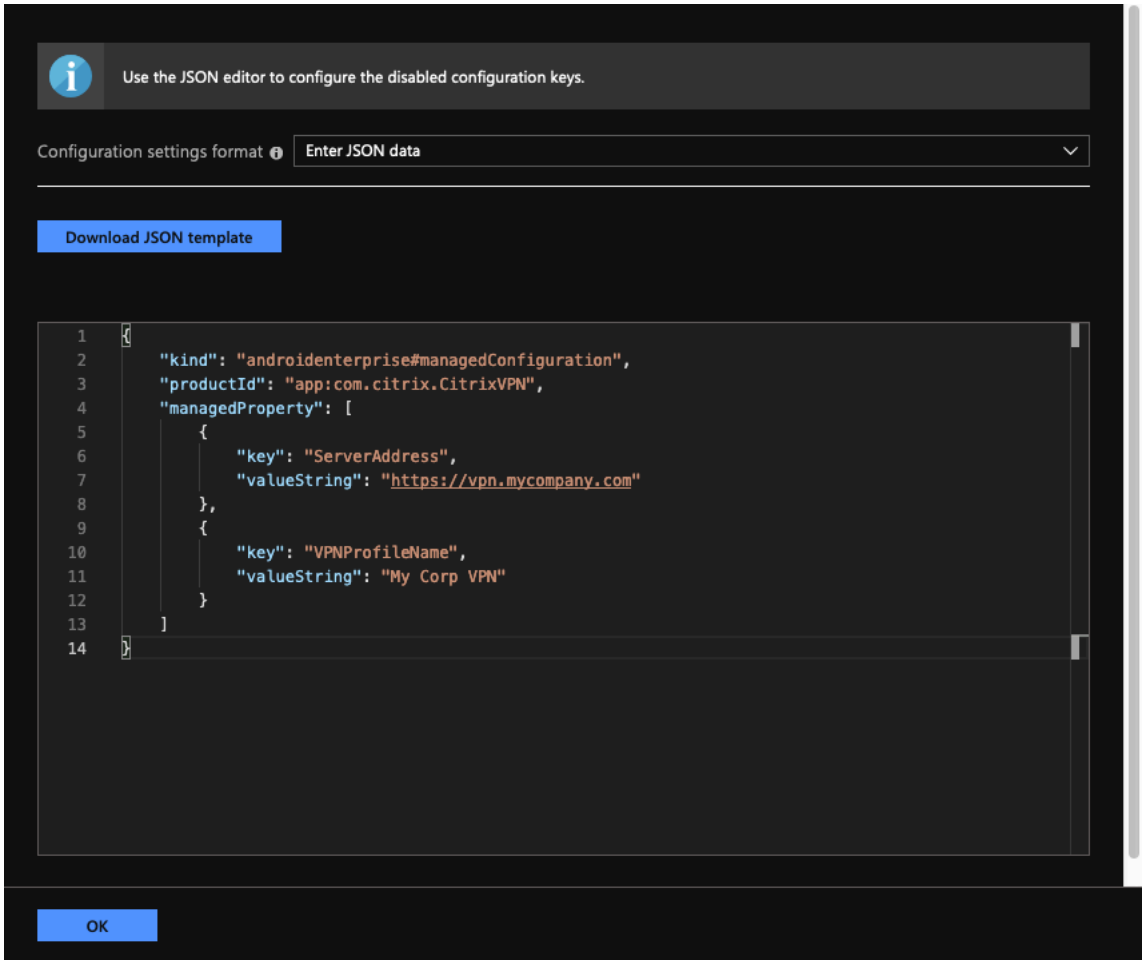
7. Click **Add** at the bottom of the App configuration policy blade to save the managed configuration for Citrix Secure Access.
8. Click **Assignments** in the App configuration policy blade to open the **Assignments** blade.
9. Select the user groups for which you want this Citrix Secure Access configuration to be delivered and applied.

VPN configuration by entering JSON data

1. In **Configuration Settings**, select **Enter JSON data** for configuring the Citrix Secure Access.
2. Use the Download JSON template button to download a template that allows for providing more detailed/complex configuration for Citrix Secure Access. This template is a set of JSON key-value pairs to configure all the possible properties that Citrix Secure Access understands.

   For a list of all the available properties that can be configured, see Available properties for configuring VPN profile in Citrix Secure Access app.
3. Once you have created a JSON configuration file, copy and paste its contents in the editing area. For example, the following is the JSON template for basic configuration created previously using the configuration designer option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This completes the procedure for configuring and deploying VPN profiles for Citrix Secure Access in the Microsoft Intune Android Enterprise environment.

> **Important:**
>
> The certificate used for client certificate-based authentication is deployed using an Intune SCEP profile. The alias for this certificate must be configured in the **Certificate Alias** property of the managed configuration for Citrix Secure Access.

Available properties for configuring VPN profile in Citrix Secure Access

Configuration Key	JSON Field Name	Value Type	Description
VPN Profile Name	VPNProfileName	Text	Name of the VPN profile (if not set defaults to the server address).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
Server Address(*)	ServerAddress	URL	Base URL of the NetScaler Gateway for the connection (`https://host[:port]`). This is a required field.
`Username` (optional)	Username	Text	User name used for authenticating with the NetScaler Gateway (optional).
Password (optional)	Password	Text	Password of the user for authenticating with the NetScaler Gateway (optional).
Certificate Alias (optional)	ClientCertAlias	Text	Alias of the client certificate installed in the Android credential store for use in certificate-based client authentication (optional). **Certificate alias** is a required field when using certificate-based authentication on NetScaler Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
Gateway Certificate Pins (optional)	ServerCertificatePins	JSON Text	Embedded JSON object describing certificate pins used for NetScaler Gateway. Example value: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Make sure to escape this embedded JSON data when using the JSON configurator.
Per-App VPN Type (optional)	PerAppVPN_Allow_Disallow_Setting	Enum (Allow, Disallow)	Are the listed apps allowed (allow list) or disallowed (block list) to use the VPN tunnel. If set to **Allow**, only listed apps (in the PerAppVPN app list property) are allowed to tunnel through the VPN. If set to **Disallow**, all apps except the listed ones are allowed to tunnel through the VPN. If no apps are listed the all apps are allowed to tunnel through the VPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
PerAppVPN app list	PerAppName_Appnames	Text	Comma (,) or semicolon (;) separated list of app package names for per-app VPN. The package names must be the same as they appear in the Google Play store app listing page URL. Package names are case sensitive.
Default VPN profile	DefaultProfileName	Text	The name of the VPN profile to use when the system starts the VPN service. This setting is used for identifying the VPN profile to use when Always On VPN is configured on the device.
Always On VPN (optional)	IsAlwaysOnVpn	Boolean	Determines whether the VPN profile is an Always ON VPN profile or not. When set to True, it indicates that the VPN profile is an Always On VPN profile. This property can be set only on the main VPN profile. It cannot be set for the additional VPN profiles. Default value is False.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
			This property is available from starting from Citrix Secure Access for Android 24.04.1 release onwards.
Disable User Profiles	DisableUserProfiles	Boolean	Property to allow or not allow the end users to manually create VPN profiles. Set this value to **true** to disable users from creating VPN profiles. Default value is **false.**
Block Untrusted Servers	BlockUntrustedServers	Boolean	Property to determine if the connection to untrusted gateways (for example, using self-signed certificates or when issuing CA is not trusted by the Android operating system) be blocked? Default value is true (block connections to untrusted gateways).
Custom Parameters (optional)	CustomParameters	List	List of custom parameters (optional) that are supported by Citrix Secure Access. For details, see Custom Parameters. Check the **NetScaler Gateway product documentation** for available options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
List of other VPN profiles	bundle_profiles	List	List of other VPN profiles. Most of the previously mentioned values for each profile are supported. For details, see Properties supported for each VPN in VPN Profile List.

Custom Parameters Each custom parameter must be defined using the following key-value names.

Key	Value Type	Value
ParameterName	Text	Name of the custom parameter.
ParameterValue	Text	Value of the custom parameter.

Custom Parameters for Intune configuration

Parameter name	Description	Value
UserAgent	Citrix Secure Access appends this parameter value to the user-agent HTTP header, when communicating with NetScaler Gateway, to perform an additional check on NetScaler Gateway.	Specify the text that you need to append to the user-agent HTTP header. The text must conform to the HTTP user-agent specifications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Parameter name	Description	Value
EnableDebugLogging	Enables debug logging on Citrix Secure Access to help troubleshoot VPN connectivity issues in case of Always On VPN. You can enable it in any one of the managed VPN configurations. The debug logging takes effect when the managed configurations are processed.	**True**: Enables debug logging. Default value: **False**.
DisableLogoutFromStoreOnExplicitDisconnect	Controls logout from the store when the end user explicitly disconnects the VPN session from the app UI. Applicable to Citrix Secure Private Access deployments only.	**True**: Disables logout from Secure Private Access store and leaves the Secure Private Access session intact, just disconnects the Citrix Secure Access app session. Default value: **False**.

For more information about the custom parameters, see Create an Android Enterprise managed configuration for Citrix Secure Access.

Properties supported for each VPN in VPN Profile List Following properties are supported for each of the VPN profile when configuring multiple VPN profiles using the JSON template.

Configuration Key	JSON Field Name	Value Type
VPN Profile Name	bundle_VPNProfileName	Text
Server Address(*)	bundle_ServerAddress	URL
User name	bundle_Username	Text
Password	bundle_Password	Text
Client Cert Alias	bundle_ClientCertAlias	Text
Gateway Certificate Pins	bundle_ServerCertificatePins	Text
Per-App VPN Type	bundle_PerAppVPN_Allow_Disallow_Set	Enum(Allow, Disallow)
PerAppVPN app list	bundle_PerAppVPN_Appnames	Text

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type
Custom Parameters	bundle_CustomParameters	List

Set Citrix Secure Access as Always On VPN provider in Intune

In the absence of an on-demand VPN support in an Android VPN subsystem, the Always On VPN can be used as an alternative to provide seamless VPN connectivity option along with client certificate authentication with Citrix Secure Access. The VPN is started by the operating system when it starts up or when the work profile is turned on.

For making Citrix Secure Access an Always On VPN app in Intune, you must use the following settings.

- Choose the correct type of managed configuration to use (personally owned with work profile OR fully managed, dedicated, and corporate owned work profile).
- Create a device configuration profile and select **Device restrictions** and then go to **Connectivity** section. Select enable for Always On VPN setting.
- Choose **Citrix Secure Access** as VPN client. If Citrix Secure Access is not available as an option, you can choose **Custom** as VPN Client and enter **com.citrix.CitrixVPN** in the Package ID field (the Package ID field is case sensitive)
- Leave other options as is. It is recommended not to enable Lockdown mode. When enabled, the device might lose complete network connectivity if VPN is not available.
- In addition to these settings, you can also set **Per-App VPN type** and **PerAppVPN app list** in the **App configuration policies** page to enable per-app VPN for Android as described in the preceding sections.

> **Note:**
>
> Always On VPN is supported only with client certificate authentication in Citrix Secure Access.

References

Refer to the following topics for more details about setting up connectivity options in Intune.

- Fully managed dedicated corporate owned devices
- Personally owned devices

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Automatic restart of Always On VPN

Starting from Citrix SSO for Android 23.8.1, Citrix Secure Access automatically restarts the Always On VPN when an app that is a part of the allow or block list is installed in a work profile or a device profile.Traffic from the newly installed app is automatically tunneled over a VPN connection without restarting the work profile or rebooting the device.

To enable automatic restart of Always On VPN, end users must grant the Query all packages consent to Citrix Secure Access. Once the consent is granted, Citrix Secure Access:

- Receives the package install notification from the operating system.
- Restarts the Always On VPN.

When an end user connects to a per-app VPN profile for the first time, the user is prompted to provide consent (required by Google policies) to collect information of the installed package. If the end user grants the consent, the VPN connection is initiated. If the user denies the consent, the VPN connection is aborted. The consent screen does not reappear once the consent has been granted. For details about the end user instructions, see How to use Citrix Secure Access from your Android device.

Limitations

The following are the limitations for per-app VPN in Android Enterprise environment on Android 11+ devices due to package visibility restrictions introduced in Android 11:

- If an app that is part of the allowed/denied list is deployed to a device after the VPN session has started, the end user must restart the VPN session for the app to be able to route its traffic through the VPN session.
- If per-app VPN is used via an Always On VPN session, then after installing a new app on the device, the end user must restart the work profile or reboot the device for the app's traffic to be routed via the VPN session.

> **Note:**
>
> These limitations are not applicable if you are using Citrix SSO for Android 23.8.1 or later versions. See Automatic restart of Always On VPN for more details.

Single sign-on between Citrix Secure Access and Citrix Workspace app for Android

September 7, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Starting from Citrix Secure Access for Android version 26.04.1, single sign-on (SSO) is supported with Citrix Workspace app (CWA). If a user is already signed in to the Citrix Workspace app, they do not need to enter credentials again when signing in to the same URL in Citrix Secure Access for Android, and vice versa.

Also, if a user signs out of the Citrix Secure Access app, the user is also logged out of the Citrix Workspace app, and vice versa. This behavior enables seamless access to TCP/UDP applications and provides a unified Secure Private Access experience. This signout synchronization is enabled by default. To disable it, contact Citrix Support.

Customers who use an MDM provider to configure a VPN profile in the Citrix Secure Access app for Android can also disable this feature by adding the custom parameter, `DisableLogoutFromStoreOnExplicit` to the managed app configuration. For details about this parameter, see Custom Parameters for Intune configuration.

Previously, users of Secure Private Access service had to authenticate twice, once in the Android Citrix Workspace app to access SaaS and published apps, and again in the Android Citrix Secure Access app to access TCP/UDP apps.

NetScaler Gateway certificate pinning with Citrix Secure Access for Android

September 8, 2026

> **Important:**
>
> Citrix SSO for Android is now called Citrix Secure Access. We are updating our documentation and the UI screenshots to reflect this name change.

Certificate pinning helps in preventing man-in-the-middle attacks. Citrix Secure Access supports certificate pinning only for managed VPN configurations in Android Enterprise mode and legacy device administrator mode. It is not supported for VPN profiles added by end user.

Configure NetScaler Gateway certificate pinning with Android Citrix Secure Access

For details on certificate pinning in the managed configuration (formerly app restrictions) for Citrix Secure Access, see Certificates and authentication.

A new key-value pair is defined to carry the pinned NetScaler Gateway certificate hashes as follows.

```
Key: ServerCertificatePins
Value: {
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
3
4   "hash-alg": "sha256",
5   "pinset": [
6     "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
        (SPKI)",
7     "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
8     "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
9     ...
10   ]
11  }
```

The key for specifying certificate pinning details in the managed configuration is **ServerCertificatePins**. The value is a JSON payload carrying the base64 encoded SHA-256 hashes of the pinned NetScaler Gateway certificate and the hashing algorithm used. The pinned certificate can be any of the certificates in the chain of trust validated by the operating system. In this case, it is Android.

The certificate pinning is done only after the operating system has validated the certificate chain during TLS handshake. The pin of the certificate is computed by hashing the certificate's subject public key information (SPKI). Both the fields ("**hash-alg**"and **"pinset"**) must be specified in the JSON payload.

The "**hash-alg**"specifies the hashing algorithm used to compute the SPKI hash.
The "**pinset**"specifies the JSON array containing base64 encoded SHA-256 hash of the NetScaler Gateway certificate's SPKI data.
At least one value must be specified for the certificate pin. More pin values can be specified to allow for certificate rotation or expiry.

You can compute the value for the pin for a domain (for example, gw.yourdomain.com) by using the following openssl command.

```
1  openssl s_client -servername gw.yourdomain.com -connect gw.yourdomain.
       com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin -outform
        der | openssl dgst -sha256 -binary | openssl enc -base64
```

The command displays the base64 encoded SHA-256 hash of the leaf certificate presented by a gateway. Any certificate in the chain can be used for certificate pinning. For example, if an enterprise is using their own intermediate CA for generating certificates for multiple gateways, pin corresponding to the intermediate signing certificate can be used. If none of the pins match the certificates in the validated certificate chain, the TLS handshake is aborted and connection to the gateway does not proceed.

> **Note:**
>
> In device administrator mode, certificate pinning is supported only with Citrix Endpoint Management™ and Microsoft Endpoint Management solutions. Certificate pinning must be configured in the custom parameters used in the legacy VPN profile (not managed configuration) with the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> custom parameter ServerCertificatePins with the same JSON payload for pinning.

Data governance

September 9, 2026

Citrix Secure Access sends application events and metrics to the Telemetry Analytics Platform (TAP) server. TAP is a Citrix-proprietary server platform that collects and stores events and metrics, for product improvement.

> **Points to note:**
>
> - Telemetry sent by Citrix Secure Access is sent only to TAP, and not with any third-party vendor. Also, Citrix Secure Access does not share any personal information of the user to TAP.
> - To prevent the telemetry from being sent to TAP, contact Citrix Support.
> - Upon installation of Citrix Secure Access on the Windows client, the files are added to the Windows Firewall allow list. Citrix Secure Access collects product configuration and usage data to improve client experience.

Data collection

TAP collects and stores the telemetry sent from Citrix Secure Access based on the following categories:

- **Geo location:** Country, continent and by state in larger countries.
- **Client version and client type:** Windows, Linux
- **VPN URLs accessed:** URLs accessed, MAC address pattern.

TAP collects metadata and telemetry logs whenever the following features are enabled or disabled:

- Edge WebView
- Domain-joined machines
- WFP
- Microsoft Intune
- Always On
- Always On service
- Split tunneling
- DNS / split DNS
- Intranet IP addresses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Local LAN access
- SSO
- GSLB
- HTTPOnly cookie
- NetScaler Gateway and Secure Private Access deployments
- DNS truncation fix

© 2025 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.