Citrix Gateway Clients

Contents

Citrix Gateway VPN clients and supported features 3

Citrix SSO for iOS and Citrix Secure Access for macOS 5

Release Notes 6

Set up Citrix SSO for iOS users 23

Send user certificate identity as an email attachment to iOS users 30

Setup proxy PAC file for the Citrix SSO app for iOS users or the Citrix Secure Access agent for macOS users 32

Set up Citrix Secure Access for macOS users 33

nFactor support for the Citrix SSO app on iOS and the Citrix Secure Access agent on macOS 40

Troubleshooting common Citrix SSO issues 42

FAQs 43

Citrix SSO for Android devices 45

Release Notes 45

Set up Citrix SSO app in an MDM environment 55

Set up the Citrix SSO app in an Intune Android Enterprise environment 56

Citrix Gateway certificate pinning with Android Citrix SSO 71

Citrix Secure Access for Windows release notes 73

Microsoft Edge WebView support for Windows Citrix Secure Access – Preview 85

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix Gateway VPN clients and supported features

March 27, 2023

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

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

Feature	Citrix Secure Access for Windows	Linux	Citrix Secure Access for macOS	SSO for iOS	SSO for Android
Always On (user mode)	Yes (11.1 and later)	No	No	No	Yes (via MDM) Android 7.0+
PAC file push	Yes (12.0 and later)	No	Yes	Yes	No
Client proxy support	Yes	Yes	No	No	Yes. *See note 1*
Max limit of Intranet Applications	512	128	No limit	No limit	No limit
Intranet IP (IIP) 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	No	Yes	Yes	Yes	Yes. *See note 6*
Split DNS BOTH	Yes	No	Yes	Yes	Yes. *See note 6*

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Feature	Citrix Secure Access for Windows	Linux	Citrix Secure Access for macOS	SSO for iOS	SSO for Android
FQDN based split tunnel	Yes-Only ON (13.0 and later)	No	Yes	Yes	Yes. *See note 5*
Client idle timeout	Yes	Yes	Yes	No	No
Endpoint analysis	Yes	Yes	Yes	No	No
Device certificate (classic)	Yes	No	Yes	No	No
nFactor authentication	Yes (12.1 and later)	No	Yes	Yes	Yes. *See note 3*
EPA (nFactor)	Yes (12.1 and later)	No	Yes	No	No
Device certificate (nFactor)	Yes (12.1 and later)	No	Yes	No	No
Push notification	Yes (12.1 and later)	No	No	Yes	Yes (device registration only)
OTP token autofill support. *See note 2*	No	No	No	Yes	Yes
DTLS support. *See note 4*	Yes (13.0 and later)	No	Yes	Yes	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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

2. Only QR code-scanned tokens are eligible for auto filling. Auto filling is not supported in the nFactor authentication flow.
3. nFactor authentication support for Android devices is under preview and the feature is disabled, by default. Contact Citrix Support for enabling this feature. Customers must provide their Citrix 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 Citrix Support for enabling this feature. Customers must provide their Citrix 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. Android Citrix SSO app also supports Split DNS LOCAL mode.

Citrix SSO for iOS and Citrix Secure Access for macOS

July 25, 2022

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

Note

- Citrix Secure Access for macOS is supported on 10.15 (Catalina), 11.x (Big Sur) and 12.x (Monterey). It supports devices with Intel chips and M1 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 vice versa, 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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Major features of the Citrix SSO app for iOS and the Citrix Secure Access agent for macOS

- **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 Citrix 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 Citrix ADC appliance. For registration steps, refer https://support.citrix.com/article/CTX228454. On the app, users can add the OTP feature by scanning the QR Code generated on Citrix ADC 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.

The Citrix SSO app for iOS or the Citrix Secure Access agent for macOS can be used to scan the QR code while registering for native OTP support.
Citrix Gateway Push notification functionality is available only to the Citrix SSO for iOS and Citrix Secure Access for macOS users.

- **Push notification:** Citrix Gateway sends push notification on your registered mobile device for a simplified two-factor authentication experience. Instead of opening the Citrix SSO for iOS app or Citrix Secure Access agent for macOS to type in the second factor OTP on the Citrix ADC 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 the Citrix SSO app for iOS or the Citrix Secure Agent for macOS. Registration for Push Notifications is transparent to the user. When users register TOTP, the device is also registered for Push Notifications if Citrix ADC supports it.

Release Notes

February 27, 2023

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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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.

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 Citrix ADC.

  [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]

Fixed issues

- Sometimes, empty proxy settings in Citrix Gateway release 13.0 or 13.1 causes Citrix SSO to create improper proxy settings.

  [NSHELP-31970]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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]

- 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 Citrix ADC appliance.

  [CGOP-21634 - macOS]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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]

- nFactor authentication with an optional client certificate fails when there are no appropriate client certificates on the device.

  [NSHELP-32127 - iOS]

- 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]

V22.03.1 (14-Jun-2022)

What's new

- EPA libraries are updated to 4.3.2393.0.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 agent for macOS without completing the authentication, then subsequent attempts to connect to the server fail until the app is restarted.

  [ACS-2415]

- The Citrix Secure Access agent 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Known issues

- Citrix Secure Access app for macOS logs out one minute after the already connected 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]

V22.01.1 (08-Feb-2022)

Fixed issues

- Per-App VPN connections with Citrix SSO for iOS devices fail to connect to Citrix Gateway on ports other than 443.

  [NSHELP-30653]

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]

- 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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]

- 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]

© 1999–2023 Cloud Software Group, 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

- 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 Citrix 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Citrix Gateway server. The current embedded EPA library version is 1.3.5.1.

  [NSHELP-26838]

V1.3.7 (17-Mar-2021)

Fixed issues

- Citrix SSO for macOS shows expired certificates in the list of device and client certificates.

  [CGOP-17337 - macOS]

- UDP and ICMP traffic does not work if FQDN split tunneling is configured.

  [CGOP-15691 - macOS]

V1.3.6 (04-Feb-2021)

Fixed issues

- The endpoint analysis scan fails in Citrix SSO for macOS if the gateway server is configured on an SSL port other than the default port 443.

  [CGOP-14661 - macOS]

V1.3.5 (08-Jan-2021)

Fixed issues

- TOTP push notification during nFactor authentication stops the nFactor authentication process.

  [NSHELP-24592 - iOS]

- Sometimes, Citrix SSO crashes while connecting to Citrix Gateway because of indexing errors in VPN profiles.

  [CGOP-16415]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.3.4 (09-Dec-2020)

This release addresses various issues that help to improve overall performance and stability.

V1.3.3 (20-Nov-2020)

Fixed issues

- EPA scan for file check is not supported with Citrix SSO for macOS if it has the special character ~ (tilde) in the file path.

  [CGOP-15721 - macOS]

V1.3.2 (04-Nov-2020)

Fixed issues

- Citrix SSO for macOS does not prompt users to select a new device certificate in case it expires or the Certificate Authority on the ADC has changed.

  [CGOP-15653 - macOS]

V1.3.1 (15-Oct-2020)

What's new

- The Error, Debug, and Verbose logging levels are now available in Citrix SSO for iOS.

  [CGOP-15234 - iOS]

- The packet header information is displayed in Verbose level logging and the old log files are deleted if their number exceeds 50.

  [CGOP-13987]

Fixed issues

- Users cannot select a new device certificate in Citrix SSO for macOS if the current certificate expires.

  [NSHELP-24481]

V1.3.0 (16-Sep-2020)

What's new

- New Citrix logo is introduced.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[CGOP-15327]

V1.2.18 (10-Sep-2020)

What's new

- Verbose logging level is now added for Citrix SSO for macOS.

  [CGOP-13985]

Fixed issues

- Citrix SSO for macOS prompts for user permission to access the root directory when the device certificate check is added as part of the nFactor scan.

  [CGOP-14722]

- After the macOS wakes up from sleep mode, Citrix SSO takes more than 30 seconds to re-establish the VPN connection.

  [CGOP-14723]

- Citrix SSO for iOS and macOS fails to transfer logon if classic authentication is enabled.

  [NSHELP-24577]

V1.2.17

Fixed issues

- Transfer Logon does not happen with Citrix Gateway version 13.0, build 61.48 if nFactor authentication is enabled.

  [CGOP-14619]

- Citrix SSO for iOS and macOS does not connect to Citrix Gateway if it is hosted on a port other than port 443.

  [NSHELP-24079]

Known issues

- Citrix SSO for iOS and macOS fails to transfer logon if classic authentication is enabled.

  [NSHELP-24491]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.16

Fixed issues

- Citrix SSO for macOS does not support the idle timeout feature.

  [CGOP-237]

- Citrix SSO for macOS does not display the forced timeout warning message.

  [CGOP-246]

Known issues

- Transfer Logon does not happen with Citrix Gateway version 13.0, build 61.48 if nFactor authentication is enabled.

  [CGOP-14619]

V1.2.15

Fixed issues

- Citrix SSO 1.2.14 does not work as intended on the client if the following two conditions are met:
  - Split tunnel is set to ON.
  - Citrix ADC appliance version is 12.1 or earlier.

  [NSHELP-24038]

- Transfer Logon does not work if the following two conditions are met:
  - nFactor authentication is configured.
  - Citrix ADC theme is set to Default.

[CGOP-14092]

V1.2.14

Fixed issues

- In a rare case, Citrix SSO crashes repeatedly.

  [NSHELP-24009]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.13

Fixed issues

- Citrix SSO is not supported on iOS versions 11 and earlier. Only iOS versions 12.0 and later are supported.

  [CGOP-14034 - iOS]

- Citrix SSO does not reconnect after a high availability failover if post authentication EPA is configured.

  [NSHELP-23574 - macOS]

- Citrix SSO does not open certain apps after connecting over the tunnel when the compression mode is set to “mixed”.

  [NSHELP-23489]

V1.2.12

This release addresses various issues that help to improve overall performance and stability.

V1.2.11

Fixed issues

- TOTP token load fails and a user sees no TOTP tokens. If a user tries to add a token, the earlier tokens are lost. With this fix, you can create and save the tokens again.

  [NSHELP-23351]

V1.2.10

This release addresses various issues that help to improve overall performance and stability.

V1.2.9

Known issues

- TOTP token load fails and a user sees no TOTP tokens. If a user tries to add a token, the earlier tokens are lost.

  [NSHELP-23351]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.8

What's new

- nFactor authentication is now supported for all customers using the Citrix SSO app.

  [CGOP-12728]

Fixed issues

- Citrix SSO app for iOS crashes if per app-VPN tunnel feature is enabled.

  [CGOP-13133 - iOS]

- The Accept Connection dialog box displays content in the English language irrespective of the language selected.

  [CGOP-13050 - macOS]

- The text "Home Page" in the **Citrix SSO app > Home** page is truncated for some languages.

  [CGOP-13049 - macOS]

- Citrix SSO app does not connect to Citrix Gateway if the device's language is set to "Simplified Chinese".

  [CGOP-12919 - macOS]

V1.2.7

Fixed issues

- Sometimes, Citrix SSO might fall back to classic authentication even if nFactor authentication is configured.

  [CGOP-12611]

- Citrix SSO might crash on iOS devices when per-app VPN is configured.

  [CGOP-10702 - iOS]

Known issues

- VPN is sometimes frozen after macOS wakes from sleep.

  [NSHELP-20656 - macOS]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.6

Known issues

- VPN is sometimes frozen after macOS wakes from sleep.

  [NSHELP-20656 - macOS]

V1.2.5

Known issues

- VPN is sometimes frozen after macOS wakes from sleep.

  [NSHELP-20656 - macOS]

V1.2.4

Known issues

- Sometimes, the VPN session does not respond after the Mac device wakes up from sleep mode.

  [NSHELP-20656 - macOS]

V1.2.3

What's new

- Citrix SSO URL scheme – Citrix SSO now registers a URL scheme so that other applications can determine if Citrix SSO is installed on an iOS device. The URL scheme is "`citrixsso`."

  [CGOP-11979 - iOS]

Fixed issues

- Citrix SSO app crashes when sending heavy UDP traffic.

  [CGOP-11603 - macOS]

- Citrix SSO for the iPad crashes when the app is started from a notification on iOS 13.

  [NSHELP-21087 - iOS]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.2

Fixed issues

- In some GSLB deployments, Citrix SSO resolves the gateway name multiple times resulting in connection failures.

  [CGOP-12013]

- Citrix SSO for iOS fails to scan `OTPSecret` greater than 16 bytes.

  [CGOP-11978 - iOS]

- Users with profiles configured for certificate only authentication and a NAC check are prompted to enter the logon credentials and are unable to create the VPN connections.

  [CGOP-11925 - iOS]

- Though the per-app Split Tunnel flag is checked only for TCP traffic, ICMP traffic is tunneled even in cases where the ICMP traffic must be sent directly.

  [CGOP-11614 - iOS]

Known issues

- The Citrix Gateway plug-in for macOS does not support the feature that opens the landing page on the Citrix Workspace app.

  [NSHELP-7047]

V1.2.0

What's new

- **nFactor authentication support.** nFactor authentication is now supported on both, iOS, and macOS.

  [CGOP-11251]

- **Citrix SSO app support.** Citrix SSO app is now supported on iOS 13 and macOS Catalina.

  [CGOP-11714]

Fixed issues

- The client IP address is displayed backwards in the Connections page of the SSO app.

  [CGOP-11596]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Citrix SSO does not honor the DNS truncated bit in the DNS flag in Citrix ADC release 13.0.

  [CGOP-11777]

- Per-app split tunnel is not compatible with Citrix ADC release 13.0.

  [CGOP-11464]

- Citrix SSO ignores some of the timeout messages from Citrix Gateway.

  [CGOP-11310]

- When users log in to the app for the first time, the last line of the app description does not appear on the user screen.

  [CGOP-11595 - macOS]

- The Citrix SSO app logon window size keeps increasing when you repeatedly click the Logon button.

  [CGOP-11594 - macOS]

- When the maximum number of licensed users limit is exceeded, an error message is displayed at the system level and not within the app window.

  [CGOP-11600 - macOS]

V1.1.12

What's new

- **Telemetry data collection for macOS.** Citrix SSO collects custom analytics events related to VPN usage in the app.

  [CGOP-9789 - macOS]

- **Per-app split tunnel support.** Administrators can configure the per-app split tunnel. Per-app traffic that matches the intranet routes for Citrix Gateway is tunneled to the Citrix Gateway appliance.

  [CGOP-657]

- **FQDN Split Tunnel tunnels traffic based on the FQDN of the system.** FQDN Split Tunnel tunnels traffic based on the FQDN of the system rather than the IP resolved by the DNS servers.

  [CGOP-316]

Fixed issues

- User interface elements such as buttons, text fields, labels and so forth are misaligned across iPad screens.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[CGOP-10141 - iOS]

- Users are not notified for a remote login if they do not have a VPN profile added.

  [CGOP-9731 - iOS]

V1.1.10

Fixed issues

- Citrix SSO app does not display the proper error message upon reaching the maximum number of users.

  [CGOP-231]

- EULA check box is not cleared by default.

  [CGOP-245]

- Add functionality is not supported for antiphishing “enabled” scan in EndPoint Analysis.

  [CGOP-249]

- Automatic selection of the client or device certificate for authentication does not happen even if only one client/device is present in the keychain.

  [CGOP-251]

- Unable to add a ‘connection record’ after editing one in the Citrix SSO app.

  [CGOP-7256]

Set up Citrix SSO for iOS users

March 8, 2023

> **IMPORTANT:**
>
> Citrix VPN cannot be used on iOS 12 and later. To continue to VPN, use the Citrix SSO app.

For the list of some commonly used features supported by the Citrix SSO for iOS, see Citrix Gateway VPN clients and supported features.

Compatibility with MDM products

Citrix SSO (iOS) and Citrix Secure Access (macOS) are compatible with most MDM providers such as Citrix Endpoint Management (formerly XenMobile), Microsoft Intune and so on.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix SSO (iOS) and Citrix Secure Access (macOS) also support a feature called Network Access Control (NAC). For more information on NAC, see Configure Network Access Control device check for Citrix Gateway virtual server for single factor login. With NAC, MDM administrators can enforce end user device compliance before connecting to the Citrix ADC appliance. NAC on Citrix SSO (iOS) and Citrix Secure Access (macOS) requires an MDM server such as Citrix Endpoint Management or Intune and Citrix ADC.

> **Note:**
>
> To use the Citrix SSO app on iOS or the Citrix Secure Access agent on macOS with Citrix Gateway VPN without MDM, you must add a VPN configuration. You can add the VPN configuration on iOS from the Citrix SSO (iOS) and the Citrix Secure Access (macOS) home page.

Configure an MDM managed VPN profile for Citrix SSO app (iOS) or Citrix Secure Access agent (macOS)

The following section captures step-by-step instructions to configure both device-wide and per-app VPN profiles for the Citrix SSO app (iOS) or the Citrix Secure Access agent (macOS) using Citrix Endpoint Management (formerly XenMobile) as an example. Other MDM solutions can use this document as reference when working with Citrix SSO (iOS) and Citrix Secure Access (macOS).

> **Note:**
>
> This section explains the configuration steps for a basic Device-wide and Per-App VPN profile. Also you can configure On-Demand, Always-On, 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 Citrix Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split tunnel) defined in Citrix ADC.

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**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 SSO App on iOS.

   In the MDM VPN payload, the Custom SSL identifier corresponds to the **VPNSubType** key.

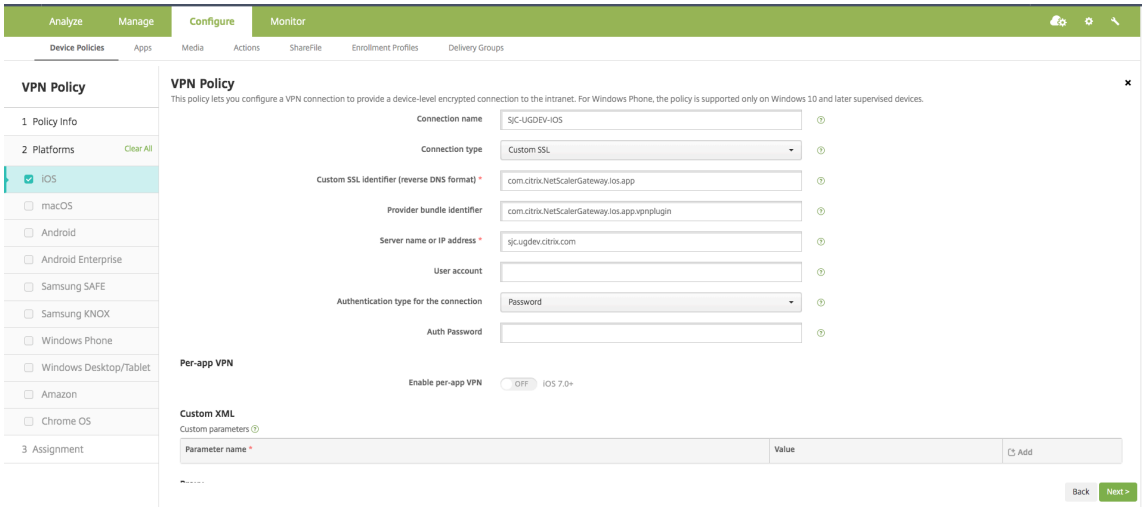
6. In **Provider bundle identifier** enter **com.citrix.NetScalerGateway.ios.app.vpnplugin**. This is the bundle identifier of the network extension contained in the Citrix SSO iOS app binary.

   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 Citrix ADC 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**.



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 Citrix Gateway. The **Per-App VPN payload** supports all keys for Device-wide VPN plus a few other keys.

© 1999–2023 Cloud Software Group, 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:

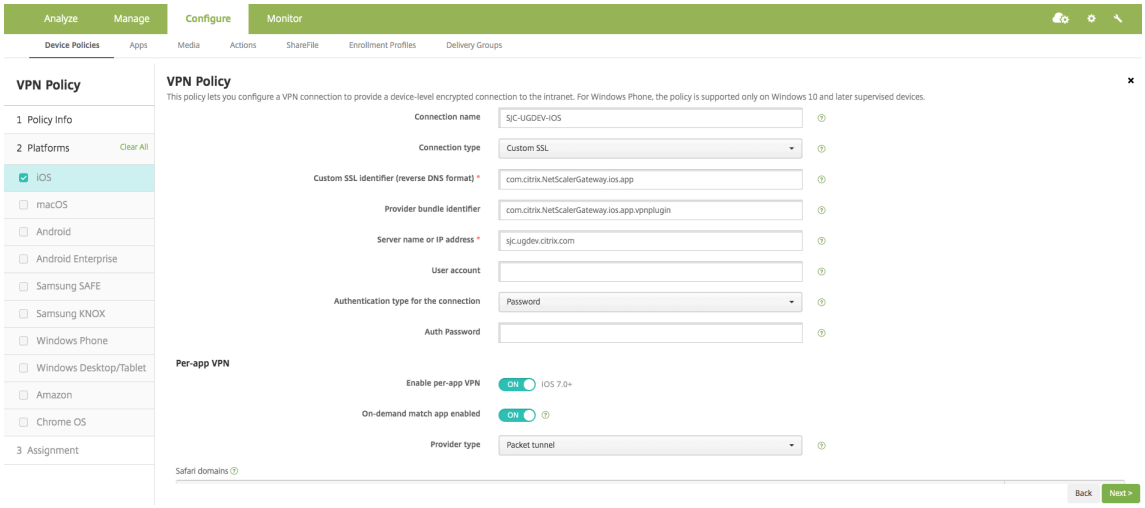
1. Complete the device level VPN configuration on Citrix Endpoint Management.
2. Turn the **Enable Per-App VPN** switch ON in the Per-App VPN section.
3. Turn the **On-Demand Match App Enabled switch ON** if Citrix SSO (iOS) and Citrix Secure Access (macOS) must be started automatically when the Match 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 SSO (iOS) and Citrix Secure Access (macOS) 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.



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 by following this guide - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configuring split tunnel in Per-App VPN

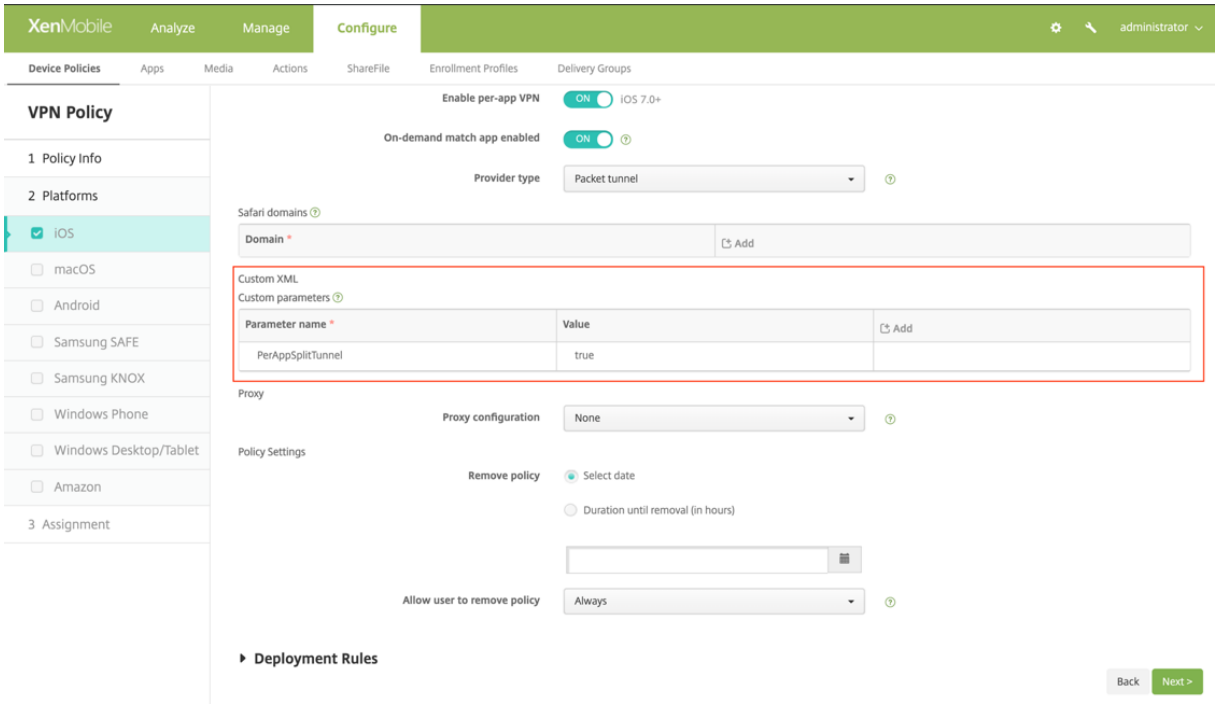
MDM customers can configure split tunnel in Per-App VPN for Citrix SSO (iOS) and Citrix Secure Access (macOS). The following key/value pair must be added to the vendor configuration section of the VPN profile created on the MDM server.

```
1  -  Key = "PerAppSplitTunnel"
2  -  Value = "true or 1 or yes"
3  <!--NeedCopy-->
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

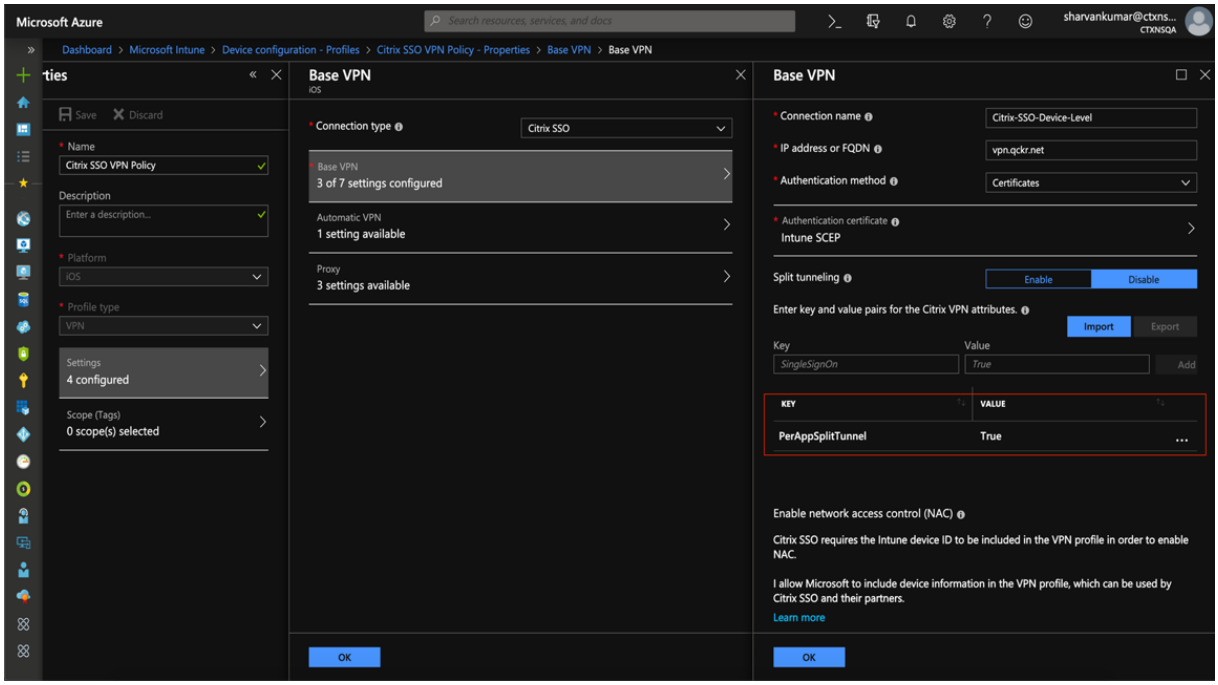
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Disabling user created VPN profiles

MDM customers can prevent users from manually creating VPN profiles from within the Citrix SSO (iOS) app and Citrix Secure Access (macOS) agent. 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.

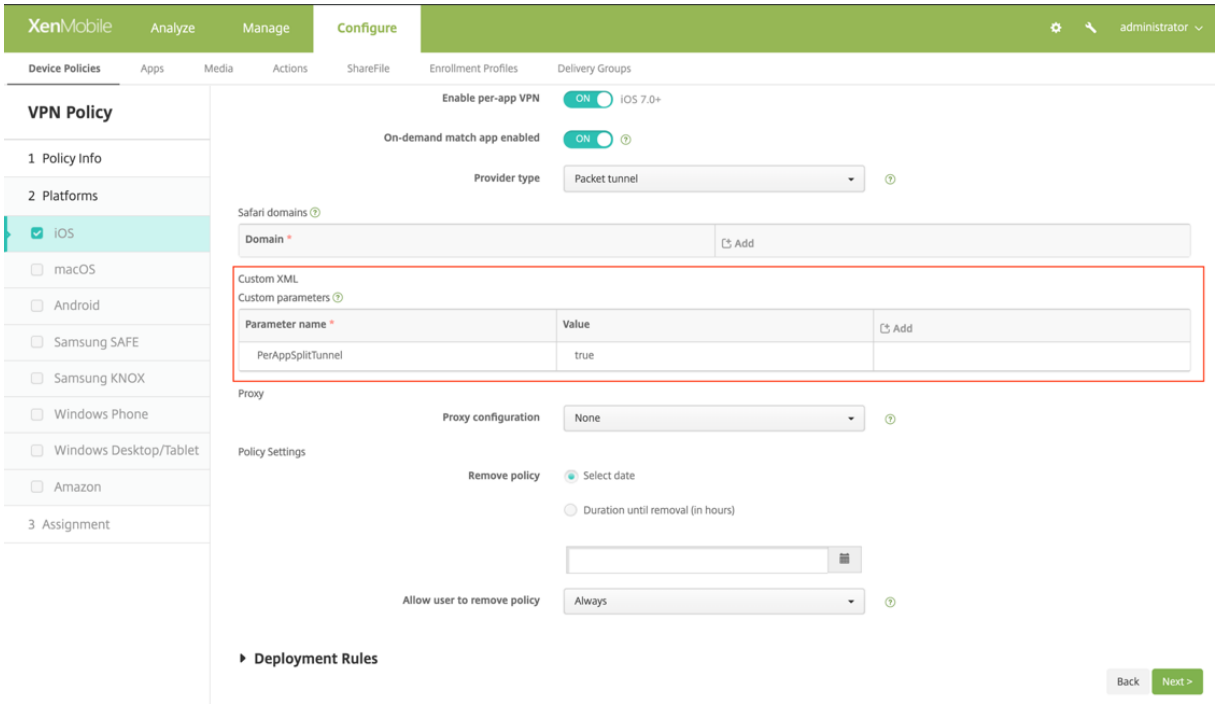
```
-  Key = "disableUserProfiles"
-  Value = "true or 1 or yes"
<!--NeedCopy-->
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

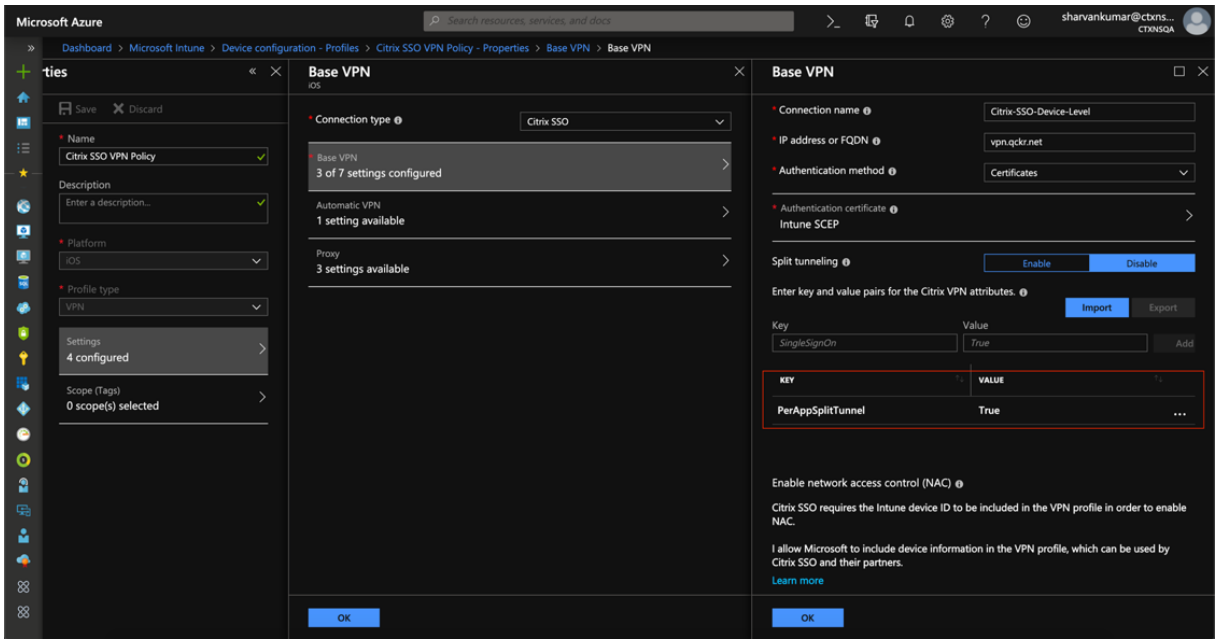
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

© 1999–2023 Cloud Software Group, 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 the Citrix SSO app or the Citrix Secure Access agent are as follows:

- **Split DNS > REMOTE** if split tunnel is set to **OFF.**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **Split DNS > BOTH** if 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 Citrix ADC 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 https://support.citrix.com/article/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 in 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. The traffic for this address is sent out via the device's physical interface instead. The issue is observed only with Per-App VPN or On-Demand VPN config and is not seen with system-wide VPN configurations. Citrix has filed a radar bug report with Apple, and Apple had noted that according to RFC-6762: https://tools.ietf.org/html/rfc6762, 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.

Send user certificate identity as an email attachment to iOS users

November 12, 2020

Citrix SSO on iOS supports client certificate authentication with Citrix Gateway. On iOS, certificates can be delivered to the Citrix SSO app 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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 the Citrix SSO app 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 SSO app 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 SSO. Hence Citrix SSO 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

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
   rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
      citrixsso-pfx
   <!--NeedCopy-->
   ```

   macOS

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
   mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
      pfx
   <!--NeedCopy-->
   ```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 SSO app.

Setup proxy PAC file for the Citrix SSO app for iOS users or the Citrix Secure Access agent for macOS users

October 25, 2021

Citrix SSO app for iOS or the Citrix Secure Access agent 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”;
}
```

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 https://support.citrix.com/article/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 SSO (iOS) or Citrix Secure Access (macOS), 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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Set up Citrix Secure Access for macOS users

March 8, 2023

The Citrix Secure Access client for macOS provides a best-in-class application access and data protection solution offered by Citrix 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 Citrix 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 Gateway VPN clients and supported features.

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 Citrix Gateway. NAC on Citrix Secure Access requires an MDM server such as XenMobile and Citrix Gateway. For more information on NAC, see Configure Network Access Control device check for Citrix Gateway virtual server for single factor login.

> **Note:**
>
> To use the Citrix Secure Access with Citrix 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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> This section explains the configuration steps for a basic Device-wide and Per-App VPN profile. Also you can configure On-Demand, Always-On, 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 Citrix Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split tunnel) defined in Citrix ADC.

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**.
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.

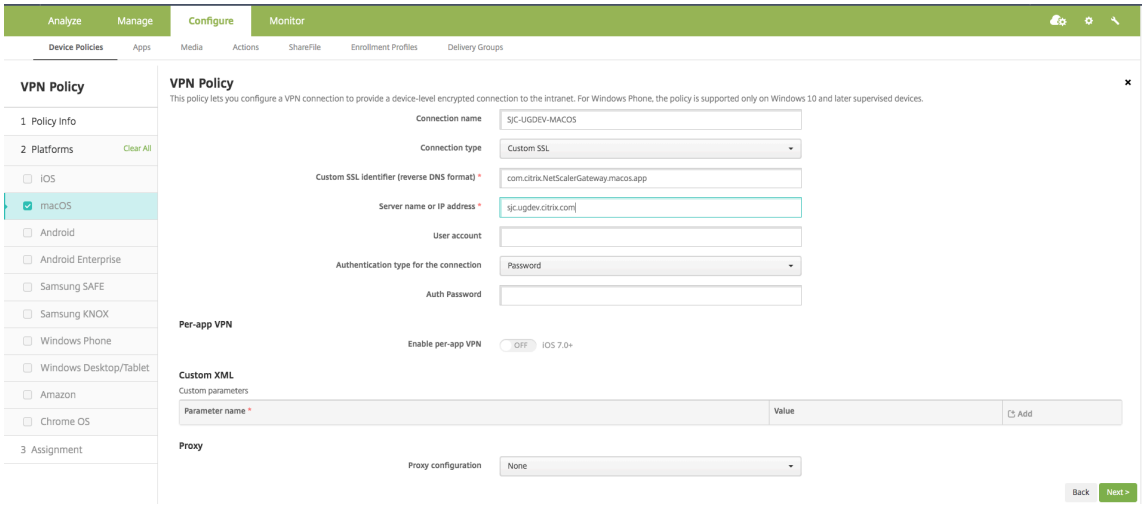
   In the MDM VPN payload, the Custom SSL identifier corresponds to the **VPNSubType** key.
6. In **Provider bundle identifier** enter **com.citrix.NetScalerGateway.macos.app.vpnplugin**. This is the bundle identifier of the network extension contained in the Citrix Secure Access app binary.

   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 of the Citrix ADC 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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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 on Citrix Endpoint Management:

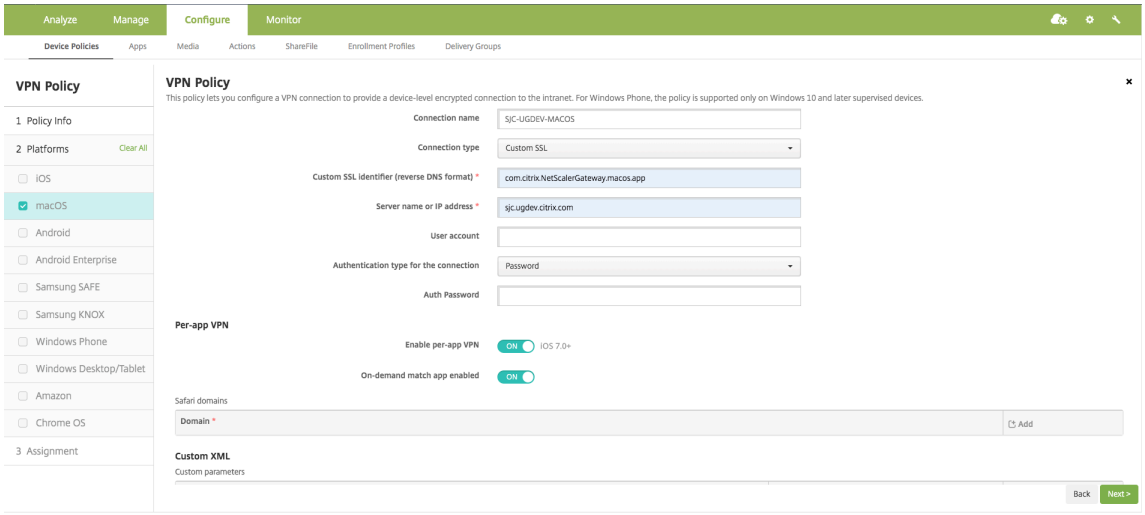
1. Complete the device level VPN configuration on Citrix Endpoint Management.
2. Turn the **Enable Per-App VPN** switch ON in the **Per-App VPN** section.
3. Turn the **On-Demand Match App Enabled switch ON** if Citrix Secure Access must be started automatically when the Match App is launched. This is 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 SSO 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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



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 by following this guide - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

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.

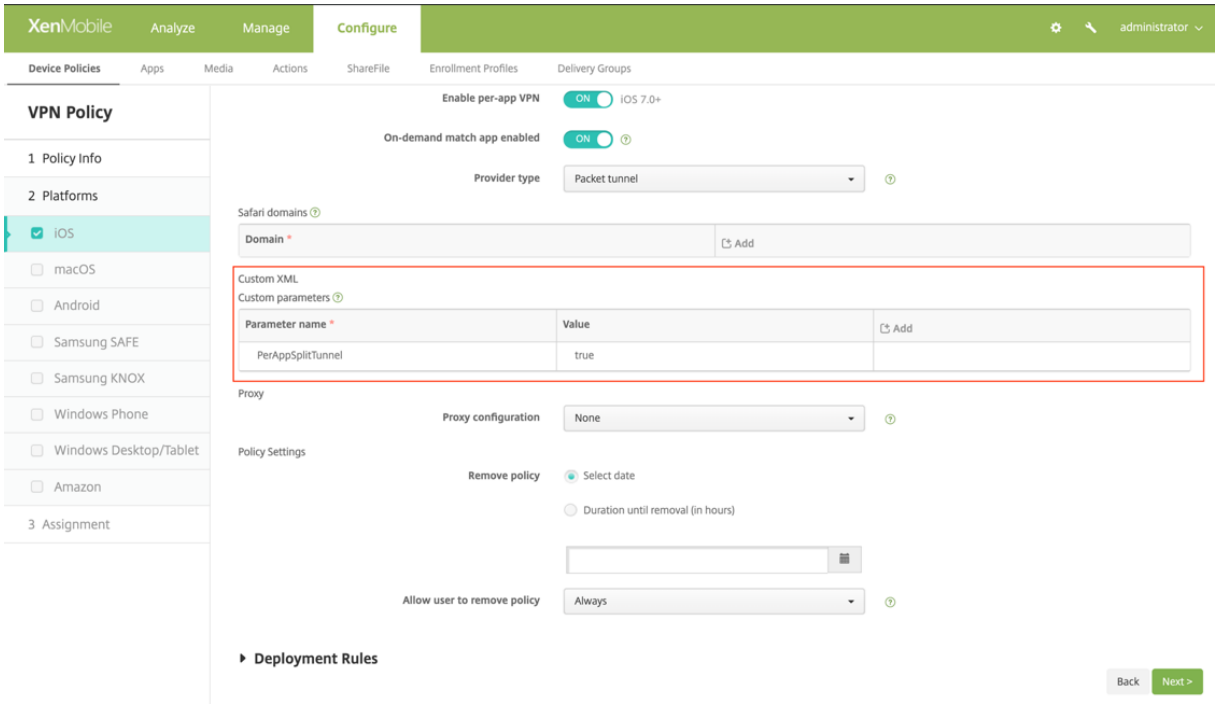
```
1  -  Key = "PerAppSplitTunnel"
2  -  Value = "true or 1 or yes"
```

The key is case sensitive and must be an exact match while the value is not case sensitive.

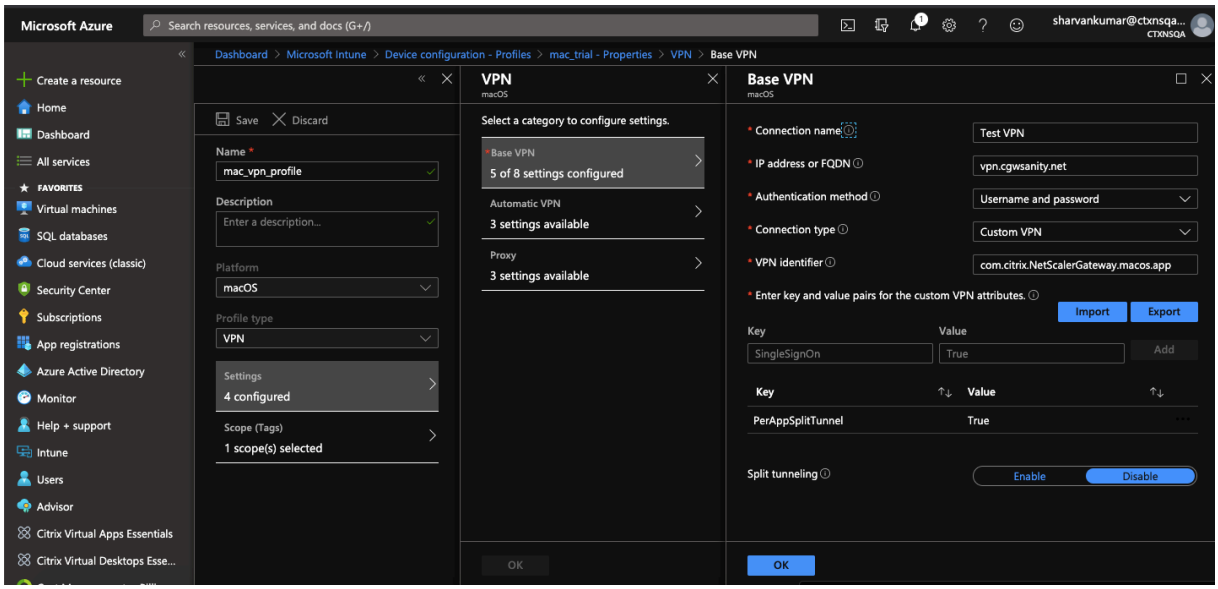
> **Note:**
>
> The user interface to configure vendor configuration is not standard across the MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

© 1999–2023 Cloud Software Group, 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 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.

```
1  -  Key = "disableUserProfiles"
```

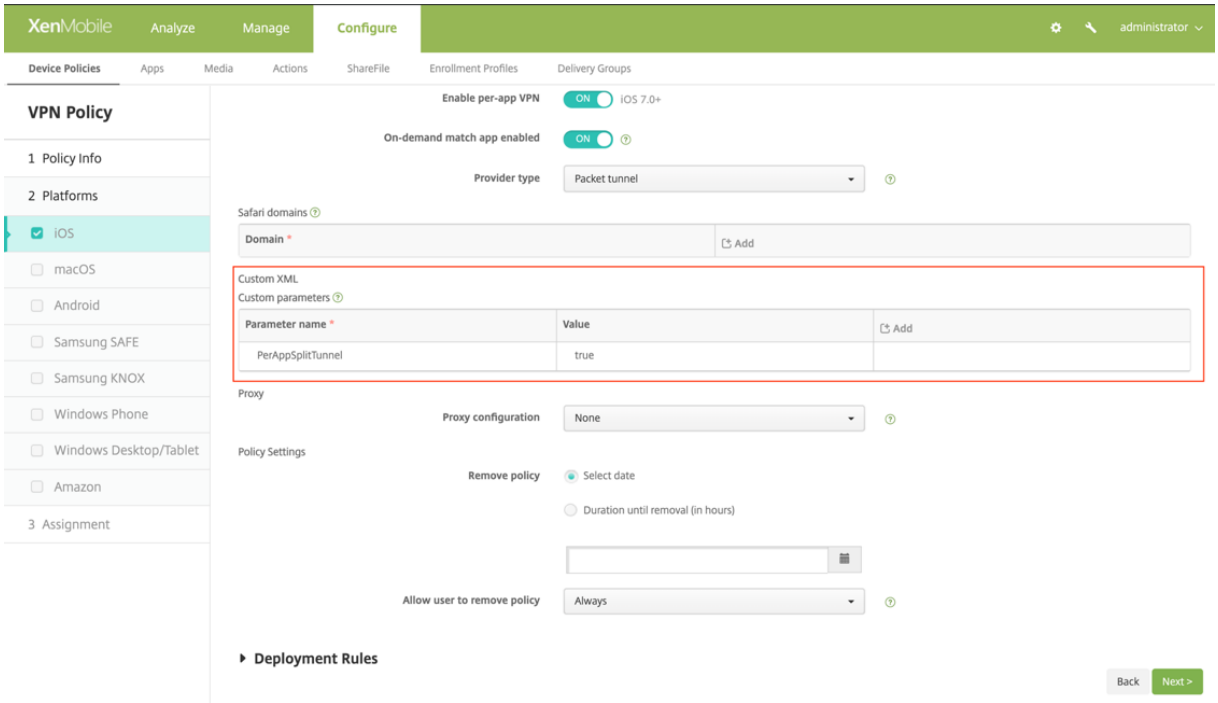
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
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.

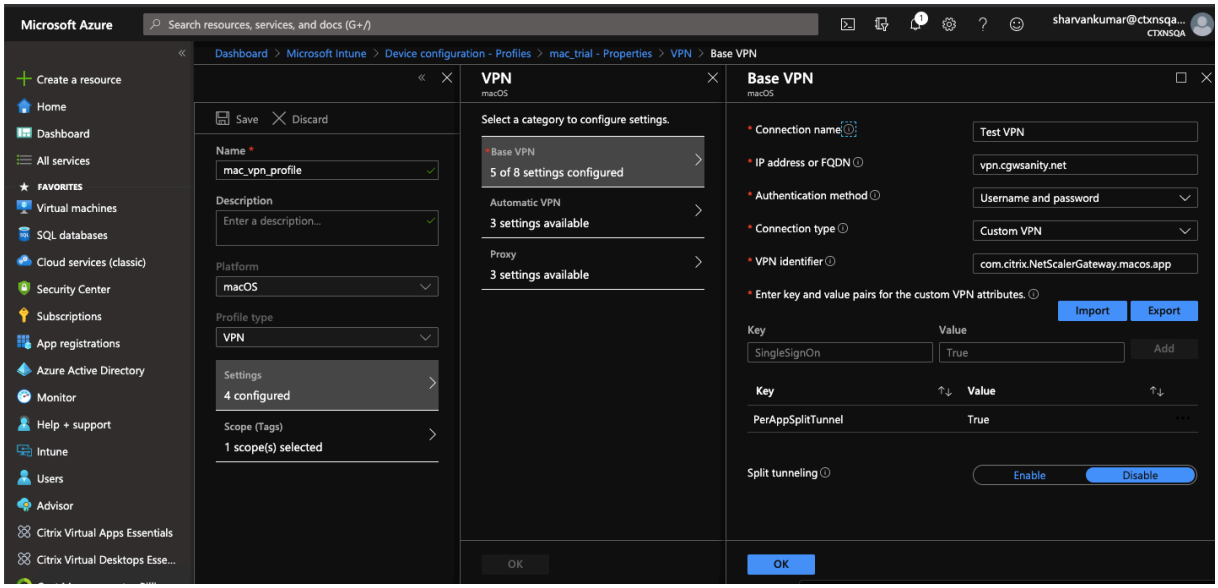
> **Note:**
>
> The user interface to configure vendor configuration is not standard across MDM vendors. Contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.



The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



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 for the intranet domains. DNS queries for FQDNs belonging to DNS suffixes are tunneled to the Citrix ADC 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 https://support.citrix.com/article/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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- EPA login fails if the user is placed in the quarantine group.
- Forced timeout warning message is not displayed.
- SSO app 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 the SSO app 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.

Troubleshooting

If the end users are presented with the **Download EPA plug-in** button in the authentication window of the Citrix SSO app, it means that the content security policy on the Citrix ADC 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 the Citrix SSO app on iOS and the Citrix Secure Access agent on macOS

January 19, 2022

Multi-factor (nFactor) authentication enhances the security of an application by requiring users to provide multiple proofs of identify 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.

The Citrix SSO app on iOS and the Citrix Secure Access agent on macOS 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,

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

the client uses a browser instance 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 the fall-back protocol if nFactor fails for specific authentication methods such as NAC.
- **Citrix identity platform** – The Citrix identity platform protocol is used when authenticating to CloudGateway or 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
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	Not 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

nFactor configuration

For details about configuring nFactor, see Configuring nFactor authentication.

> **Important:**
>
> To use the nFactor protocol with the Citrix SSO app on iOS and the Citrix Secure Access agent on macOS, the recommended Citrix Gateway on-premises version is 12.1.50.xx and later.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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 on an MDM VPN profile, the Citrix SSO app on iOS and the Citrix Secure Access agent on macOS automatically fall 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.

Troubleshooting common Citrix SSO issues

February 2, 2021

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 https://support.citrix.com/article/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.`

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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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 `"MACPATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- Always keep the EPA libraries on Citrix ADC up to date. The latest libraries can be found at https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html

nFactor issues

- Citrix SSO app 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 Citrix 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 SSO 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 Citrix 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.

FAQs

October 25, 2021

This section captures the FAQ on the Citrix SSO app for iOS and Citrix Secure Access agent for macOS.

How is Citrix SSO app for iOS or the Citrix Secure Access agent for macOS different from Citrix VPN app?

Citrix SSO is the next generation SSL VPN client for Citrix ADC. The App uses Apple’s Network Extension framework to create and manage VPN connections on iOS and macOS devices. Citrix

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

VPN is the legacy VPN client that uses Apple's private VPN APIs which are now deprecated. Support for Citrix VPN will be removed from the App Store in the months to come.

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 Citrix ADC is the Citrix SSO app for iOS and Citrix Secure Access agent for macOS compatible?

VPN features in the Citrix SSO app for iOS and the Citrix Secure Access agent for macOS are supported on Citrix ADC versions 10.5 and above. The TOTP is available on Citrix ADC version 12.0 and above. Push Notification on Citrix ADC 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 Citrix VPN must note this change when using the Citrix SSO app for iOS or the Citrix Secure Access agent for macOS. This is
mostly true for non-MDM customers who do not use an MDM Server to distribute User Certificates. For details, see "Importing Certificates into Citrix SSO app for iOS and Citrix Secure Access agent for macOS via Email" to be able to distribute Certificates.

What is Network Access Control (NAC)? How do I configure NAC with Citrix SSO app for iOS or Citrix Secure Access agent for macOS and Citrix Gateway?

Microsoft Intune and Citrix Endpoint Management (formerly XenMobile) MDM customers can take advantage of the Network Access Control (NAC) feature in the Citrix SSO app for iOS and the Citrix Secure Access agent for macOS. 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 SSO app for iOS and the Citrix Secure Access agent for macOS.

To use NAC with the Citrix SSO app for iOS or the Citrix Secure Access agent for macOS, you must enable it on both the Citrix Gateway and the MDM server.

- To enable NAC on Citrix ADC, see Configure Network Access Control device check for Citrix Gateway virtual server for single factor login.
- If an MDM vendor is Intune, see Network access control (NAC) integration with Intune.
- If an MDM vendor is Citrix Endpoint Management (formerly XenMobile), see Network Access Control.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> The minimum supported Citrix SSO app for iOS and Citrix Secure Access agent for macOS version are 1.1.6 and above.

Citrix SSO for Android devices

October 9, 2020

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

Release Notes

December 19, 2022

> **Important:**
>
> - FQDN based split tunneling and nFactor authentication support are currently in preview.
> - Citrix SSO app is not supported for Android 6.x and lower versions after June 2020.

The Citrix SSO 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.

V 22.11.1 (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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

introduced in Android 11. For details, see https://developer.android.com/training/package-visibility.

[CGOP-21409]

V 22.10.1 (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]

V 2.5.3 (05-May-2022)

What's new

- Citrix SSO updated to Android 11 target SDK (API 30)

  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 Citrix Gateway for device compliance check. For details, refer to the KB article https://support.citrix.com/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]

V 2.5.2 (21-Oct-2021)

Fixed issues

- Sometimes, Citrix SSO crashes when handling a non-compliance error in NAC check.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[CGOP-19198]

V 2.5.1 (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 Citrix 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]

V 2.5.0 (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 Citrix Gateway versions 12.1 and earlier.

  [CGOP-17735]

- The "DisableUserProfiles" setting is not applied after the SSO app is restarted.

  [CGOP-17454]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Citrix 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.

  [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 Citrix 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 Citrix Gateway which is used only in nFactor authentication.

  [CGOP-16449]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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]

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 Citrix logo is introduced.

  [CGOP-15327]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V2.4.4 (10-Sep-2020)

Fixed issues

- Sometimes, Citrix SSO crashes when reconnecting the VPN session.

  [CGOP-15215]

V2.4.3

Known issues

- Citrix SSO fails to establish a VPN session to Citrix 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V2.3.17

This release addresses various issues that help to improve overall performance and stability.

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 Citrix 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- The Citrix Gateway IP address is now resolved only once. Earlier, the Citrix 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]

V2.3.13

Fixed issues

- The Citrix Gateway IP address is now resolved only once.

  Earlier, the Citrix 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]

© 1999–2023 Cloud Software Group, 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 SSO app 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 Citrix Gateway.

  [CGOP-11259]

© 1999–2023 Cloud Software Group, 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 Citrix Gateway**

  You can now register for push notification service using the Citrix 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," "DefaultProfile-Name," and "DisableUserProfiles" settings for Android Enterprise environments.

  [CGOP-10033]

- **Enhanced Push notification support**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Upon configuring Citrix 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 https://info.citrite.net/x/8TIFTw

V2.2.9

What’s new

- **Push Notification support**

  Citrix 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 SSO app in an MDM environment

March 17, 2021

To set up Citrix SSO app in an MDM environment, see Configure Citrix SSO protocol for Android.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> - In a Non-MDM environment, users create VPN profiles manually.
> - You can also create an Android Enterprise managed configuration for Citrix SSO. For details, see Configure VPN profiles for Android Enterprise.

Set up the Citrix SSO app in an Intune Android Enterprise environment

December 20, 2022

The topic captures details about deploying and configuring the Citrix SSO app via 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 the Citrix SSO app in an Intune Android Enterprise environment

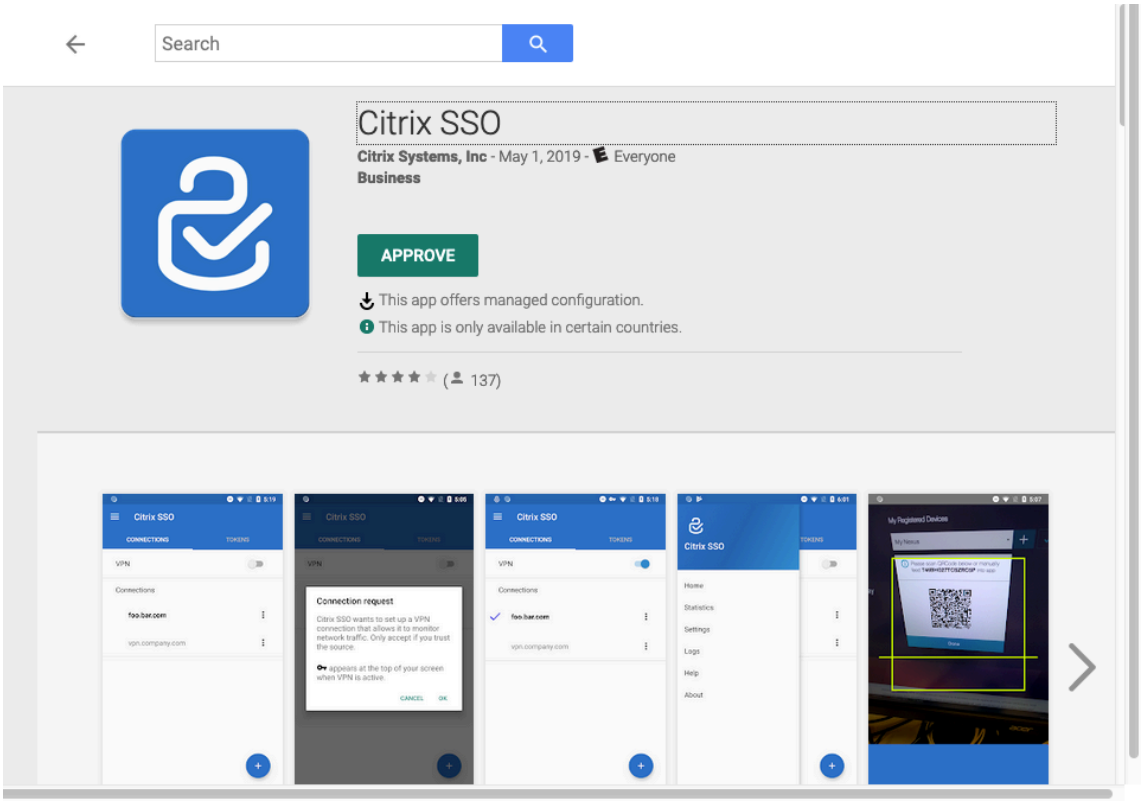
- Add Citrix SSO app as a managed app
- Configure managed app policy for Citrix SSO app

Add Citrix SSO app 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 the Citrix SSO app and select it from the list of apps.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Note: If Citrix SSO does not appear in the list, it means that the app is not available in your country.

7. Click **APPROVE** to approve Citrix SSO for deployment through Managed Google Play store.

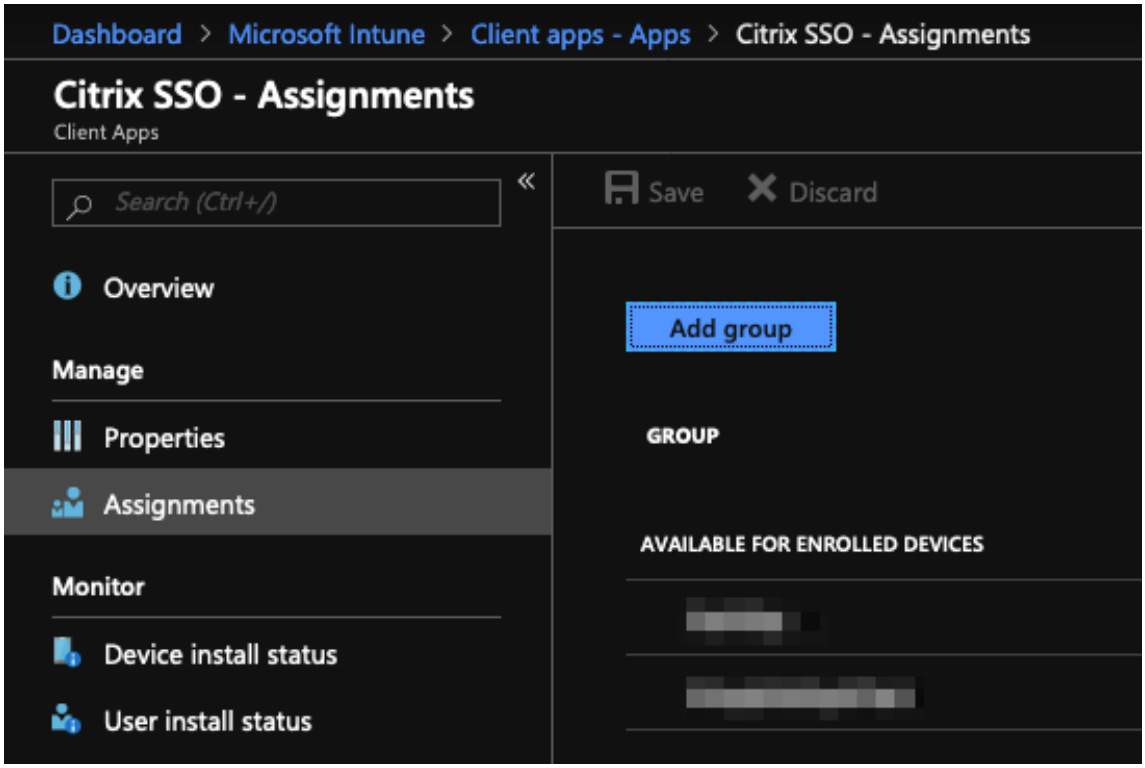
   The permissions that are required by the Citrix SSO app are listed.

8. Click **APPROVE** to approve the app for deployment.
9. Click **Sync** to sync this selection with Intune.

   Citrix SSO app is added to the Client apps list. You might have to search for the Citrix SSO app if there are many apps added.

10. Click **Citrix SSO** app to open the app details blade.
11. Click **Assignments** in the details blade. **Citrix SSO - Assignments** blade appears.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



12. Click **Add group** to assign the user groups to which you want to give permissions to install the Citrix SSO app, and click **Save**.
13. Close the Citrix SSO app details blade.

Citrix SSO app is added and enabled for deployment to your users.

Configure managed app policy for Citrix SSO app

After the Citrix SSO app is added, you must create a managed configuration policy for the Citrix SSO app so that the VPN profile can be deployed to the Citrix SSO app on the device.

1. Open **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.
5. In **Device enrollment type**, select **Managed devices**.
6. In **Platform**, select **Android**.

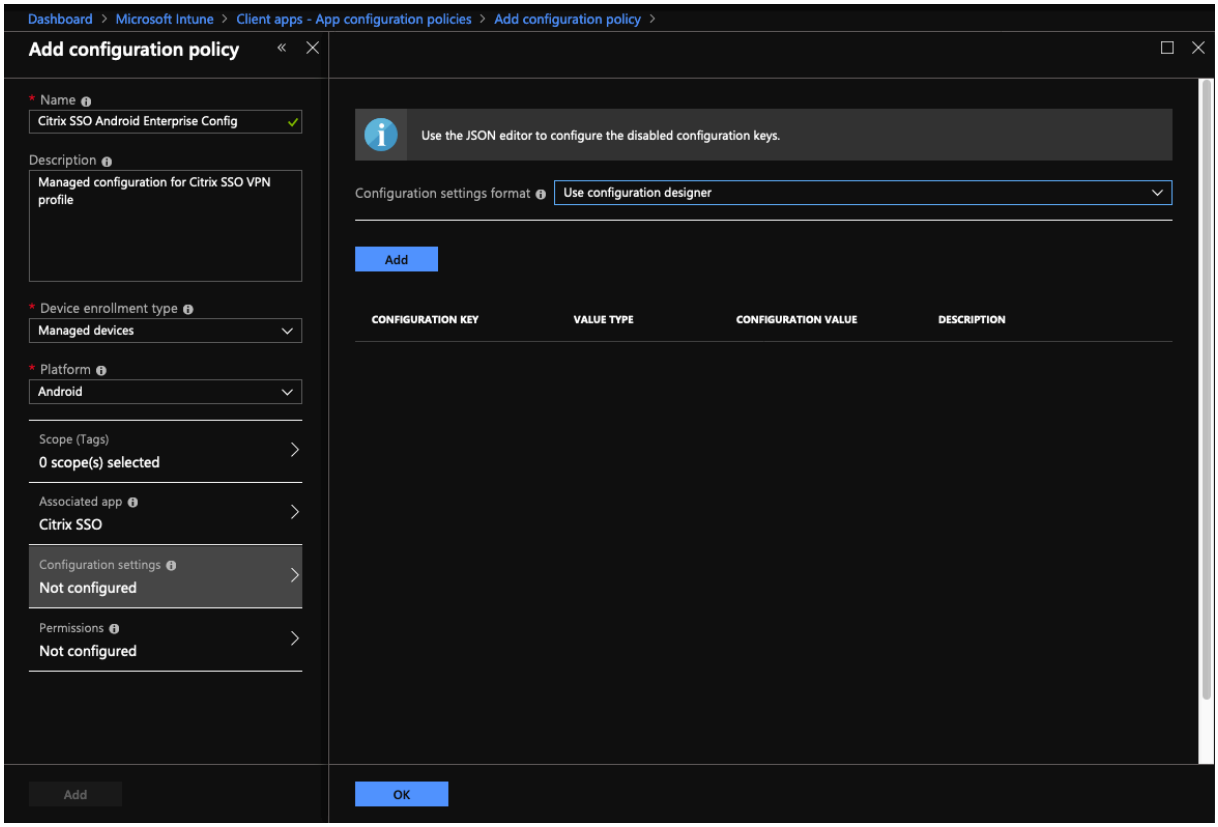
   This adds another configuration option for the associated app.
7. Click **Associated app** and select **Citrix SSO** app.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 the Citrix SSO app appears.
10. In **Configuration Settings**, select either **Use configuration designer**or **Enter JSON data** to configure the Citrix SSO app.



> **Note:**
>
> For simple VPN configurations it is recommended to use the configuration designer.

VPN configuration using user 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 the Citrix SSO app. At a minimum you must configure the **Server Address** and **VPN 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**.

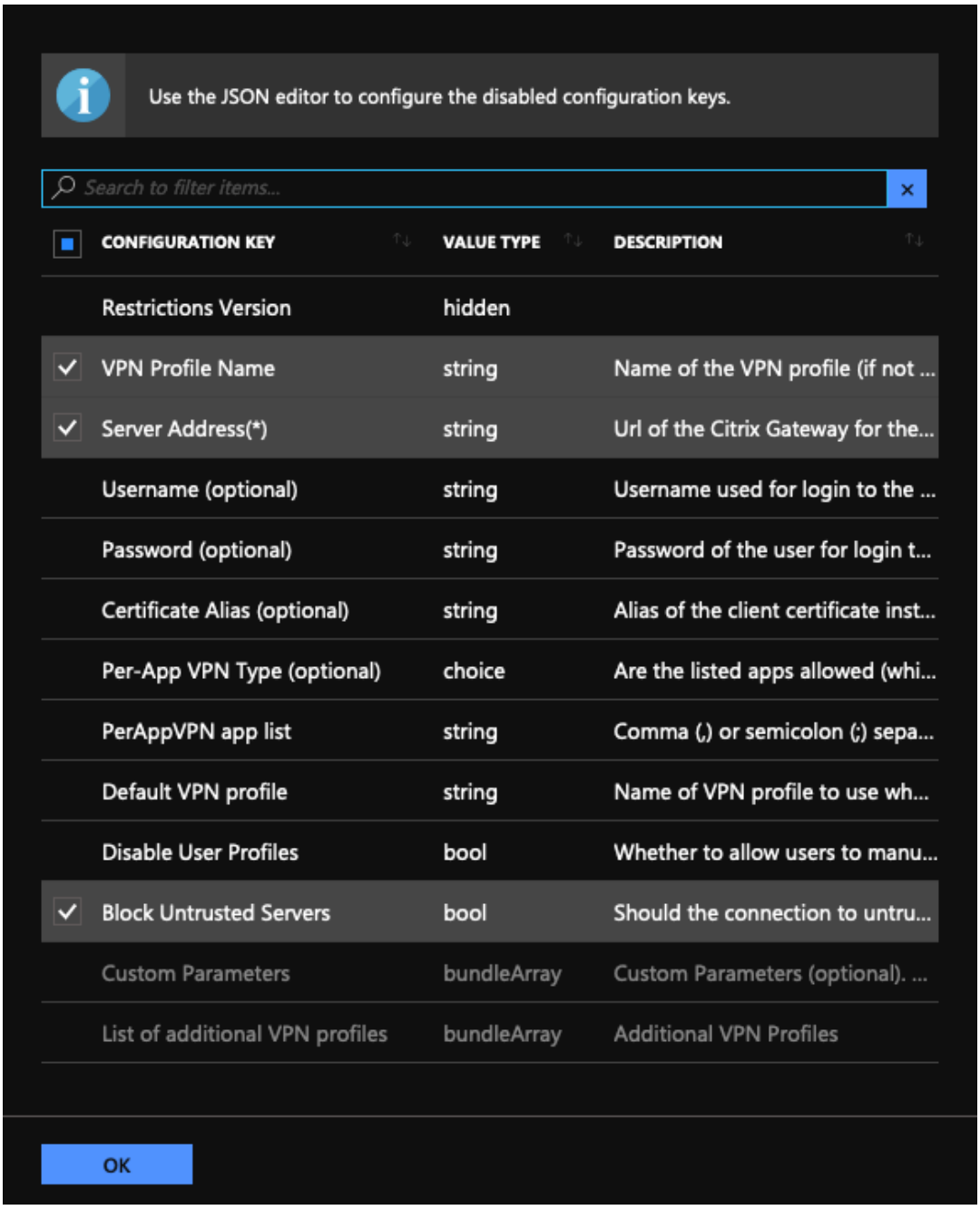
© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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 Citrix Gateway base FQDN. If your Citrix 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 Citrix 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 Citrix Gateway.
- **Password (optional)**. Enter the password that end users use to authenticate to the Citrix Gateway. If you do not provide a password, users are prompted to provide a password when they connect to Citrix 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.
- **ServerCertificatePins (optional)**. JSON object describing certificate pins used for Citrix Gateway. Example value: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBB=="] }`. For details, see Citrix Gateway certificate pinning with Android Citrix SSO.
- **Per-App VPN Type (optional)**. If you are using 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 commas 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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

the Citrix SSO app. If this field is empty, the main profile is used for connection. If only one profile is configured, it is marked as the default VPN profile.



Note:

- For making Citrix SSO app as Always On VPN app in Intune, use VPN provider as custom and com.citrix.CitrixVPN as app package name.
- Only certificate-based client authentication is supported for Always On VPN by the Citrix SSO app.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> - Admins must select **Client Authentication** and set **Client Certificate** to **Mandatory** in the **SSL Profile** or **SSL Properties** on the Citrix Gateway for the SSO app to work as intended.

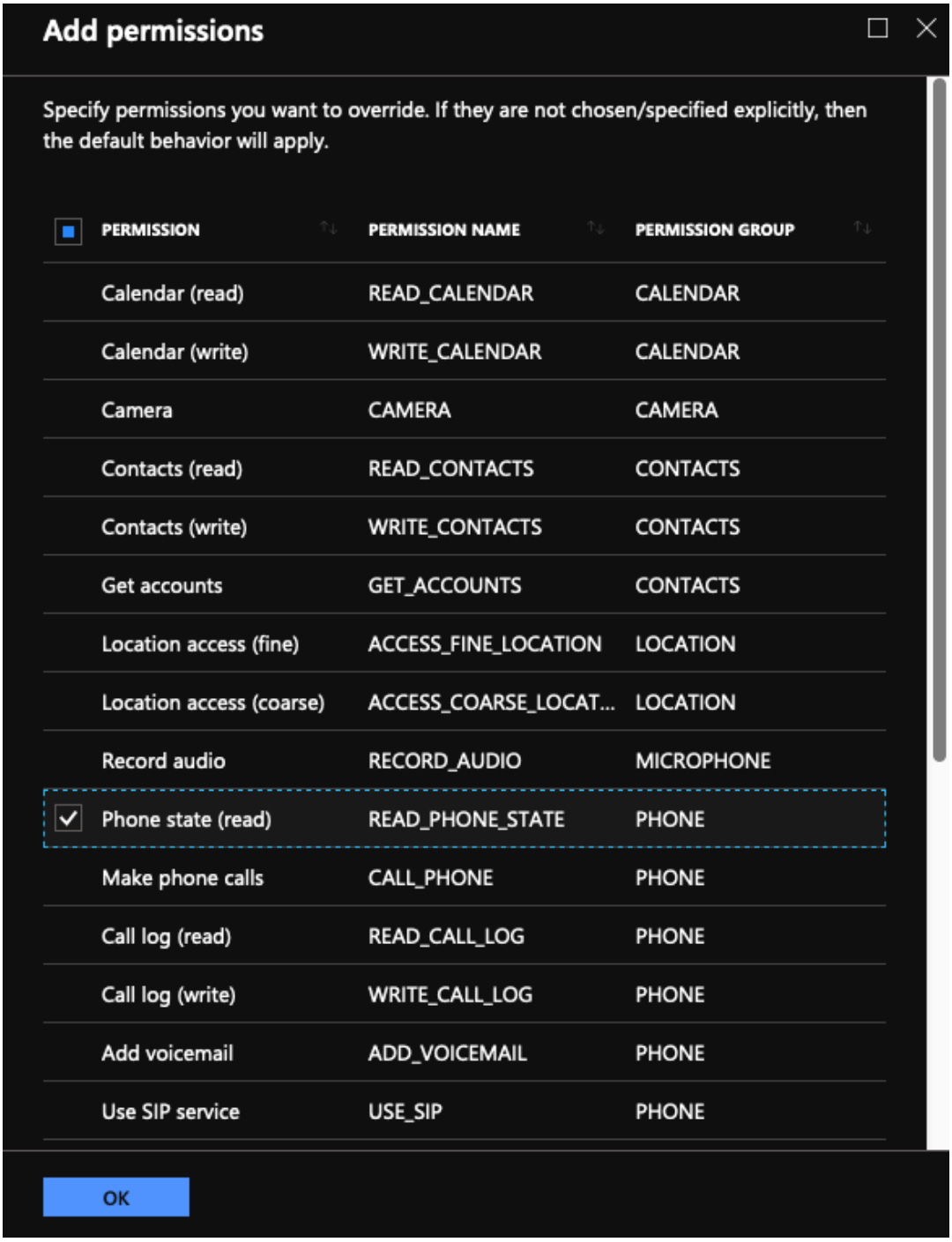
- **Disable User Profiles**
  - If you set this value to true, users cannot add new VPN profiles on their devices.
  - If you set this value to false, users can add their own VPNs on their devices.

  Default value is false.
- **Block Untrusted Servers**
  - Set this value to false when using a self-signed certificate for Citrix Gateway or when the root certificate for the CA issuing the Citrix Gateway certificate is not in the system CA list.
  - Set this value to true to enable the Android operating system validate the Citrix Gateway certificate. If the validation fails, the connection is not allowed.

  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 SSO app's main screen (for example, My Corporate VPN).
5. You can add and configure other properties as appropriate to your Citrix Gateway deployment. Click **OK** when you are done with configuration.
6. Click **Permissions** section. In this section, you can grant the permissions required by the Citrix SSO app.
   - If you are using the Intune NAC check, the Citrix SSO app 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**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



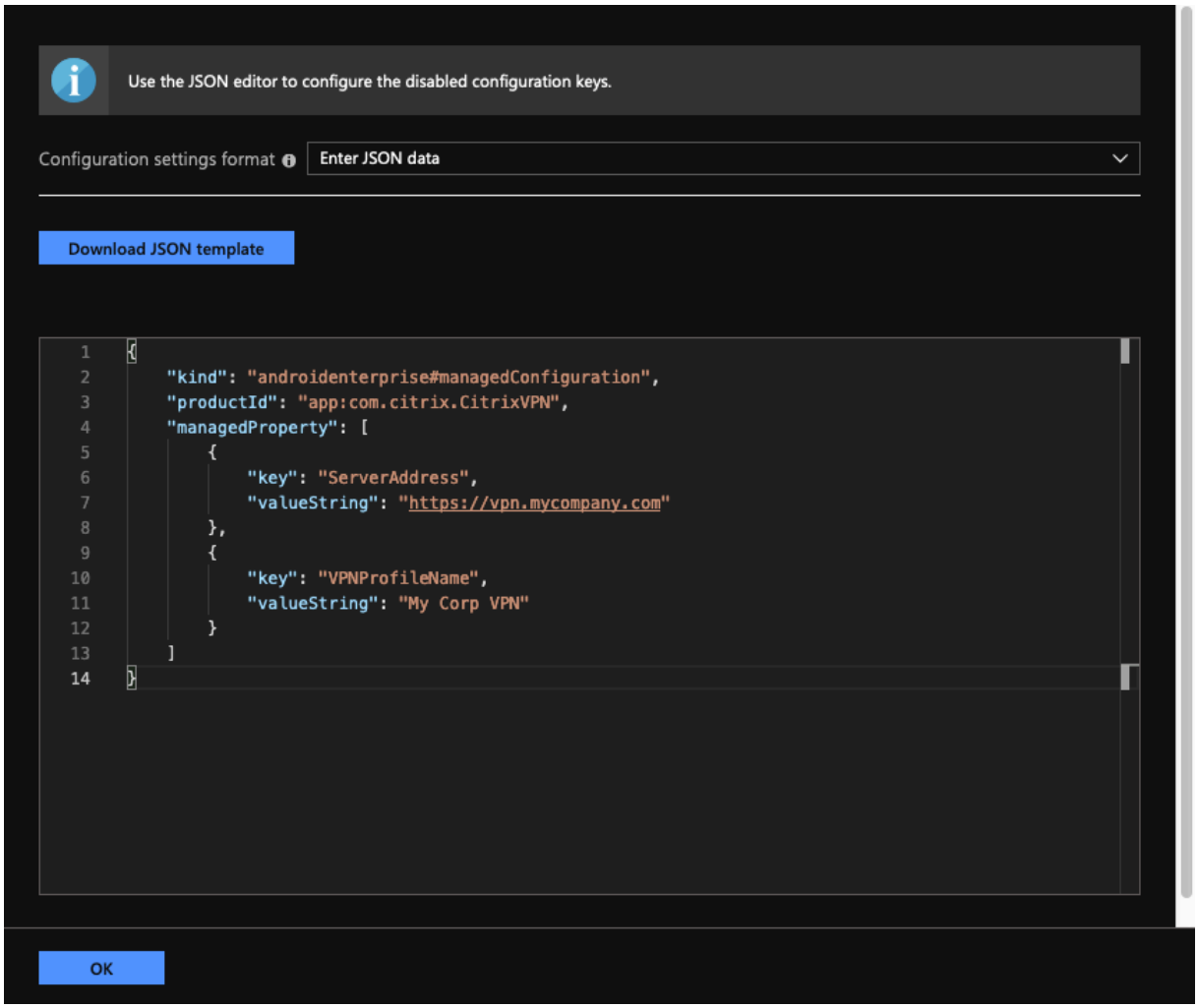
7. Click **Add** at the bottom of the App configuration policy blade to save the managed configuration for the Citrix SSO app.
8. Click **Assignments** in the App configuration policy blade to open the **Assignments** blade.
9. Select the user groups for which you want this Citrix SSO configuration to be delivered and applied.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

VPN configuration by entering JSON data

1. In **Configuration Settings**, select **Enter JSON data** for configuring the Citrix SSO app.
2. Use the Download JSON template button to download a template that allows for providing more detailed/complex configuration for the Citrix SSO app. This template is a set of JSON key-value pairs to configure all the possible properties that the Citrix SSO app understands.

   For a list of all the available properties that can be configured, see Available properties for configuring VPN profile in Citrix SSO 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.



This completes the procedure for configuring and deploying VPN profiles for the Citrix SSO app in the Microsoft Intune Android Enterprise environment.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> 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 the Citrix SSO app.

Available properties for configuring VPN profile in Citrix SSO app

Configuration Key	JSON Field Name	Value Type	Description
VPN Profile Name	VPNProfileName	Text	Name of the VPN profile (if not set defaults to server address).
Server Address(*)	ServerAddress	URL	Base URL of the Citrix Gateway for the connection (`https://host[:port]`). This is a required field.
`Username` (optional)	Username	Text	User name used for authenticating with the Citrix Gateway (optional).
Password (optional)	Password	Text	Password of the user for authenticating with the Citrix Gateway (optional).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
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 Citrix Gateway.
Server Certificate Pins (optional)	ServerCertificatePins	JSON Text	Embedded JSON object describing certificate pins used for Citrix Gateway. Example value: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Make sure to escape this embedded JSON data when using the JSON configurator.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
Per-App VPN Type (optional)	PerAppVPN_Allow_Disa	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.
PerAppVPN app list	PerAppName_Appnames	Text	Comma (,) or semicolon (;) separated list of app package names for per-app VPN. The package names must be exactly the same as they appear in the Google Play store app listing page URL. Package names are case sensitive.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
Default VPN profile	DefaultProfileName	Text	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.
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).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configuration Key	JSON Field Name	Value Type	Description
Custom Parameters (optional)	CustomParameters	List	List of custom parameters (optional) that are supported by Citrix SSO app. For details, see Custom Parameters. Check the **Citrix Gateway product documentation** for available options.
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.

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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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
Server Certificate Pins	bundle_ServerCertificatePins	Text
Per-App VPN Type	bundle_PerAppVPN_Allow_Disa	Enum (Allow, Disallow)
PerAppVPN app list	bundle_PerAppVPN_Appnames	Text
Custom Parameters	bundle_CustomParameters	List

Set Citrix SSO app 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 the Citrix SSO app. The VPN is started by the operating system when it starts up or when the work profile is turned on.

For making the Citrix SSO app 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 SSO app** as VPN client. If Citrix SSO is not available as an option, you can choose **Custom** as VPN Client and enter **com.citrix.CitrixVPN** in the Package ID field (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 the Citrix SSO app.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

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.

Citrix Gateway certificate pinning with Android Citrix SSO

November 12, 2020

Certificate pinning helps in preventing man-in-the-middle attacks. Citrix SSO 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 Citrix Gateway certificate pinning with Android Citrix SSO

For details on certificate pinning in the managed configuration (formerly app restrictions) for Citrix SSO, see Certificates and authentication.

A new key-value pair is defined to carry the pinned Citrix Gateway certificate hashes as follows.

```
Key: ServerCertificatePins
Value: {

  "hash-alg": "sha256",
  "pinset": [
    "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
       (SPKI)",
    "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
```

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

```
    "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
    ...
  ]
 }

<!--NeedCopy-->
```

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 Citrix 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 Citrix 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.

```
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
<!--NeedCopy-->
```

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 custom parameter ServerCertificatePins with the same JSON payload for pinning.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Access for Windows release notes

February 20, 2023

The Citrix Secure Access agent for Windows is now released on a standalone basis and is compatible with all Citrix ADC versions. The Citrix Secure Access agent version follows the format YY.MM Release.Build.

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 Citrix Gateway Product Documentation.

> **Note:**
>
> Citrix Secure Access agent (formerly known as Citrix Gateway plug-in for Windows) build 21.9.1.2 and later contains the fix for https://support.citrix.com/article/CTX341455.

23.1.1.11 (20-Feb-2023)

This release addresses issues that help to improve the overall performance and stability of 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.

  [NSHELP-33617]

- The OS filtering rules are captured when the Citrix Secure Access agent 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 agent 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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 Citrix ADC 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]

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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **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 Citrix 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 Citrix ADC appliance. For details, see Upgrade/downgrade issue on Citrix Secure Access agent.

  [NSHELP-32793]

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

  [NSHELP-32138]

- Sometimes, the Citrix Secure Access agent 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- Customized EPA failure log message is not displayed on the Citrix 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. For details, see EPA Check failing for Windows11 22H2.

  [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.

  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 agent 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 agent using Windows Filtering Platform.

  [CGOP-19787]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- **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 Citrix ADC 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

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

  [ACS-2714]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

22.3.1.5 (24-Mar-2022)

Fixed issues

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

  [CGOP-21061]

Known issues

- Citrix Secure Access Agent for Windows does not tunnel new TCP connections to the back-end TCP server if the already connected 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 now restrict the end users to enable or disable 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, end users are restricted from using the local LAN access option on their client machines. If the end users must enable or disable the local LAN access, the admins must reconfigure the Local LAN Access option in the Citrix ADC appliance accordingly.

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

  1. Navigate to **Citrix 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
  <!--NeedCopy-->
  ```

  [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.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

1. Navigate to **Citrix 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
  - Tools
  - UpdateRollups
  - Updates

  You can configure the classification types by using the GUI.

  1. Navigate to **Citrix 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

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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]

- Users cannot connect to the Citrix 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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

  [NSHELP-30641]

21.12.1.4 (17-Dec-2021)

What's new

- **Rebranding changes**

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

  [ACS-2044]

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

  Citrix Secure Access agent 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 Citrix Gateway now support the following languages:

  - Korean
  - Russian
  - Chinese (Traditional)

  [CGOP-17721]

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

  Citrix Secure Access agent is now supported for Windows 11.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

[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 Citrix ADC provided net mask**

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

  [CGOP-18487]

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 agent 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- 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 Citrix Gateway within a few seconds when the client idle timeout is set.

  [NSHELP-28404]

- 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

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]

- 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]

- **Citrix Gateway virtual adapter comaptibility**

  The Citrix 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]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- The Citrix 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]

- 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:

  - Citrix Gateway appliance is configured for the Always On feature.
  - The appliance is configured for certificate based authentication with two factor authentication “off.”

  [NSHELP-23584]

Microsoft Edge WebView support for Windows Citrix Secure Access – Preview

February 6, 2023

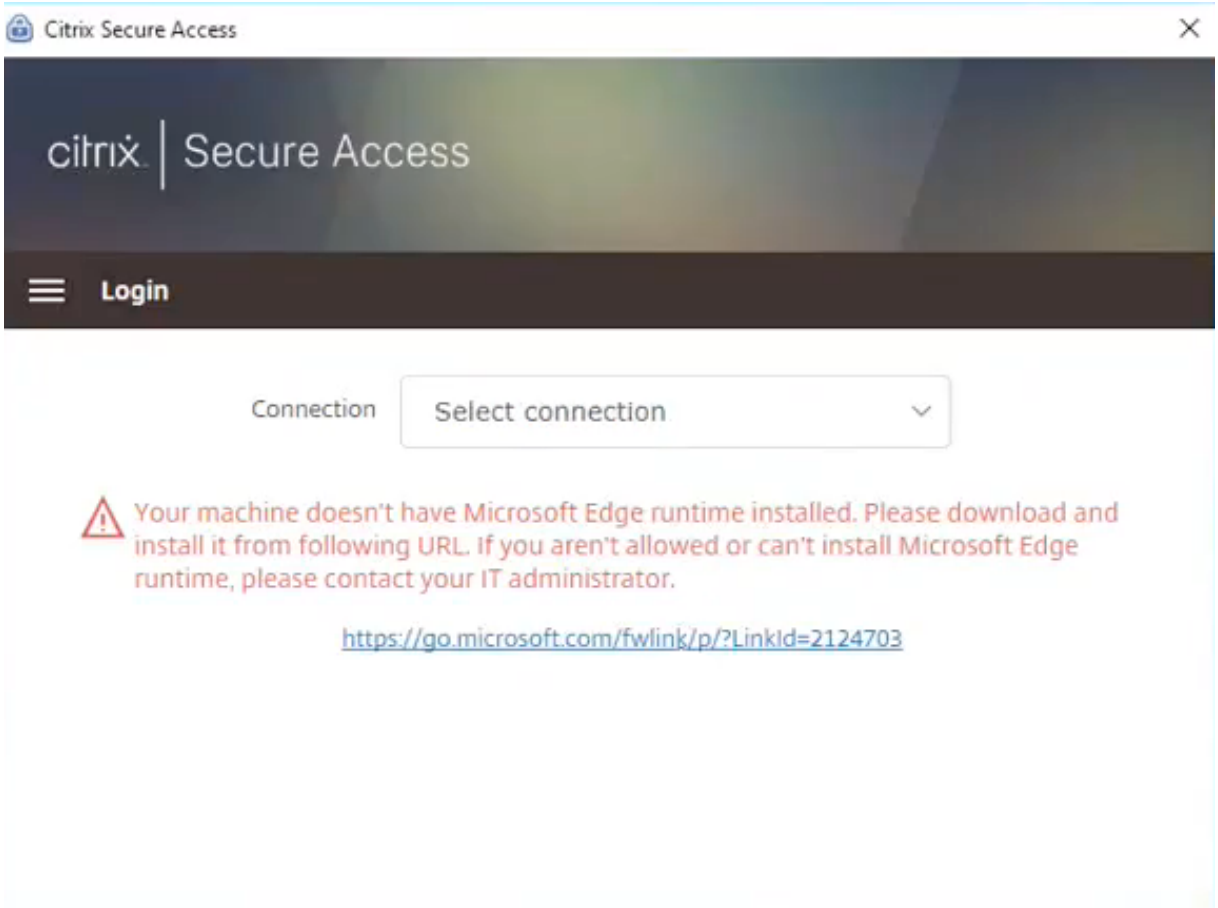
Microsoft Edge WebView support on Citrix Secure Access Agent for Windows introduces an enhanced end user experience. With the Citrix Secure Access client, the end user can use advanced authentication methods on the client browser window itself, which was supported via the web browser in legacy versions. Furthermore, the legacy Citrix Secure Access client is built on Internet Explorer WebView, the

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

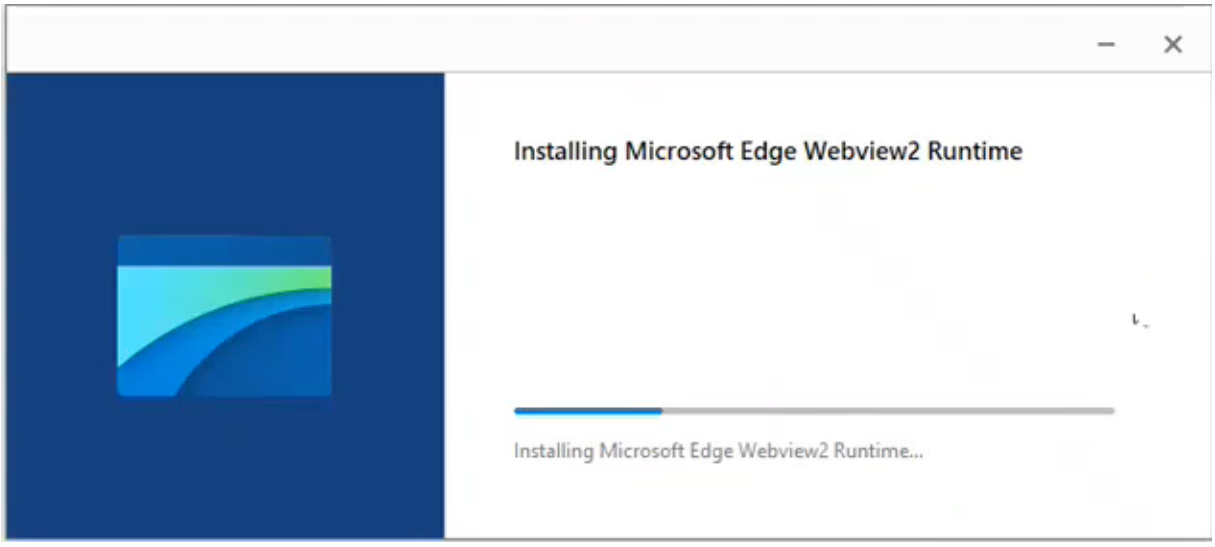
APIs for which are planned for deprecation. Therefore, it is recommended to use the Microsoft Edge WebView for Citrix Secure Access Client for Windows, as it supports the latest APIs.

How to move to Microsoft Edge WebView

As moving to Microsoft Edge WebView affects every nFactor authentication request, the Internet Explorer based web-view is enabled by default for the Secure Access for Windows. However, the end users are provided with a link on the Secure Access for Windows login page to download and install Microsoft Edge WebView. End users can download and install Edge WebView seamlessly while connecting to the VPN and the authentication is not interrupted.



© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Enable Microsoft Edge-based WebView

Customers can raise a request to enable the EnableEdgeWebView feature flag by filling in the form https://podio.com/webforms/28291989/2245437.

> **Note:**
>
> The preview build does not support multiple client-certificate authentications.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).