NetScaler Gateway-Clients

Machine translated content

Disclaimer

Contents

NetScaler Gateway VPN-Clients und unterstützte Funktionen

March 27, 2024

> **Wichtig:**
>
> - Citrix SSO für iOS/Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.
> - Der alte VPN-Client wurde mit den privaten VPN-APIs von Apple erstellt, die jetzt veraltet sind. Die VPN-Unterstützung im Citrix Secure Access Client für macOS/iOS wurde mithilfe des öffentlichen Network Extension-Frameworks von Apple neu geschrieben. Das NetScaler Gateway-Plug-In und VPN für iOS und macOS werden nicht mehr unterstützt. Citrix Secure Access für iOS/macOS ist der empfohlene VPN-Client.
> - Die allgemeine Verfügbarkeit der nFactor-Authentifizierungsunterstützung für Android-Geräte wäre in einer der kommenden Versionen verfügbar.

In der folgenden Tabelle sind einige der am häufigsten verwendeten Funktionen aufgeführt, die für jeden VPN-Client unterstützt werden.

Feature	Citrix Secure Access für Windows	Citrix Secure Access für Linux	Citrix Secure Access für macOS	Citrix Secure Access für iOS	Citrix Secure Access für Android
Immer eingeschaltet (Benutzermodus)	Ja (11.1 und höher)	Nein	Nein	Nein	Ja (über MDM) Android 7.0+
PAC datei	Ja (12,0 und höher)	Nein	Ja	Ja	Nein
Client-Proxy-Unterstützung	Ja	Ja	Nein	Nein	Ja. *Siehe Anmerkung 1*
Maximale Grenze von Intranet-Anwendungen	512	128	Kein Limit	Kein Limit	Kein Limit
Unterstützung für Intranet-IP (IIP)	Ja	Ja	Ja	Ja	Ja

Feature	Citrix Secure Access für Windows	Citrix Secure Access für Linux	Citrix Secure Access für macOS	Citrix Secure Access für iOS	Citrix Secure Access für Android
Split-Tunnel EIN	Ja	Ja	Ja	Ja	Ja
Split-Tunnel rückwärts	Ja	Ja	Ja	Ja	Ja. *Siehe Anmerkung 5*
DNS-REMOTE aufgeteilt	Nein	Ja	Ja	Ja	Ja. *Siehe Hinweis 6*
Split DNS BOTH	Ja	Nein	Ja	Ja	Ja. *Siehe Hinweis 6*
FQDN-basierter Splittunnel	Yes-Only ON (13.0 and later)	Nein	Ja	Ja	Ja. *Siehe Anmerkung 5*
Timeout für Client im Leerlauf	Ja	Ja	Ja	Nein	Nein
Endpunktanalyse	Ja	Ja	Ja	Nein	Nein
Gerätezertifikat (klassisch)	Ja	Nein	Ja	Nein	Nein
nFactor-Authentifizierung	Ja (12.1 und höher)	Nein	Ja	Ja	Ja. *Siehe Anmerkung 3*
EPA (nFactor)	Ja (12.1 und höher)	Nein	Ja	Nein	Nein
Gerätezertifikat (nFactor)	Ja (12.1 und höher)	Nein	Ja	Nein	Nein
Push Benachrichti-gung	Ja (12.1 und höher)	Nein	Nein	Ja	Ja
OTP-Token-Autofill-Unterstützung. *Siehe Anmerkung 2*	Nein	Nein	Nein	Ja	Ja

Feature	Citrix Secure Access für Windows	Citrix Secure Access für Linux	Citrix Secure Access für macOS	Citrix Secure Access für iOS	Citrix Secure Access für Android
TLS 1.3-Unterstützung	Ja	Ja	Ja	Ja (Standard-mäßig deaktiviert. Auf Anfrage erhältlich.)	Ja (Standard-mäßig deaktiviert. Auf Anfrage erhältlich.)
DTLS-Unterstützung. *Siehe Anmerkung 4*	Ja (13,0 und höher)	Nein	Ja	Ja	Nein
Nur Http-Cookies	Ja	Ja	Ja	Ja	Ja
Globaler Serverlaste-nausgleich (GSLB)	Ja	Ja	Ja	Ja	Ja
Lokaler LAN-Zugriff	Ja	Nein	Immer aktiviert	Immer aktiviert	Nein

Hinweis:

1. Das Festlegen eines Proxys in der Clientkonfiguration auf dem virtuellen VPN-Server in der Gateway-Konfiguration für Android 10 und höher wird unterstützt. Es wird nur eine grundlegende HTTP-Proxy-Konfiguration mit IP-Adresse und Port unterstützt.
2. Nur mit QR-Code gescannte Tokens können automatisch ausgefüllt werden. Das automatische Ausfüllen wird im nFactor-Authentifizierungsablauf nicht unterstützt.
3. Die Unterstützung der nFactor-Authentifizierung für Android-Geräte ist in der Vorschau und die Funktion ist standardmäßig deaktiviert. Wenden Sie sich an den NetScaler-Support, um diese Funktion zu aktivieren. Kunden müssen den FQDN ihres NetScaler Gateway dem Support-Team zur Verfügung stellen, um die nFactor-Authentifizierung für Android-Geräte zu aktivieren.
4. Einzelheiten finden Sie unter Konfigurieren des virtuellen DTLS-VPN-Servers mithilfe des virtuellen SSL-VPN-Servers.
5. FQDN-basierte Split-Tunnelunterstützung und Reverse-Split-Tunnel für Android-Geräte sind in der Vorschau und die Funktion ist standardmäßig deaktiviert. Wenden Sie sich an den NetScaler-Support, um diese Funktion zu aktivieren. Kunden müssen den FQDN ihres

NetScaler Gateway dem Support-Team zur Verfügung stellen, um ihn für Android-Geräte zu aktivieren.

6. Für den Modus Split DNS BOTH müssen DNS-Suffixe auf dem Gateway konfiguriert werden, und nur DNS-A-Datensatzabfragen, die mit diesen Suffixen enden, werden an das Gateway gesendet. Der Rest der Abfragen wird lokal aufgelöst. Citrix Secure Access für Android unterstützt auch den Split-DNS-Modus "LOCAL".

Referenz

Hilfedokumentation für Endbenutzer

Citrix Secure Access für macOS/iOS

March 27, 2024

Der alte VPN-Client wurde mit den privaten VPN-APIs von Apple erstellt, die jetzt veraltet sind. Die VPN-Unterstützung in Citrix Secure Access für macOS und iOS wurde mithilfe des öffentlichen Network Extension-Frameworks von Apple von Grund auf neu geschrieben.

Hinweis

- Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.
- Citrix Secure Access für macOS wird auf 10.15 (Catalina), 11.x (Big Sur) und 12.x (Monterey) unterstützt. Es unterstützt Geräte mit Intel-Chips und M1-Chips.
- Benutzer mit Hardware, die nicht auf eine der zuvor genannten Versionen aktualisiert werden kann (macOS 10.15 und macOS 11.0), haben Zugriff auf die letzte kompatible Version im App Store, es gibt jedoch keine weiteren Updates für die älteren Versionen.
- Wenn ein macOS-Benutzer zwischen App Store-App und TestFlight-Vorschau-Build oder umgekehrt wechselt, müssen die Benutzer das Verbindungsprofil neu erstellen, indem sie die folgenden Schritte ausführen:

  1. Click the hamburger menu and then click **Configuration**.
  2. Delete the profile from the list and add the same profile again.

Hauptfunktionen des Citrix Secure Access Clients für macOS/iOS

- **Kennwort-Token:** Ein Kennwort-Token ist ein 6-stelliger Code, der eine Alternative zu sekundären Kennwortdiensten wie VIP, OKTA darstellt. Dieser Code verwendet das zeit-

basierte One Time Password (T-OTP) -Protokoll, um den OTP-Code ähnlich wie Dienste wie Google Authenticator und Microsoft Authenticator zu generieren. Benutzer werden bei der Authentifizierung bei NetScaler Gateway für einen bestimmten Active Directory-Benutzer zur Eingabe von zwei Kennwörtern aufgefordert. Der zweite Faktor ist ein sich ändernder sechsstelliger Code, den Benutzer von einem registrierten Drittanbieterdienst wie Google oder Microsoft Authenticator in den Desktop-Browser kopieren. Benutzer müssen sich zuerst auf der NetScaler-Appliance für T-OTP registrieren. Hinweise zur Registrierung finden Sie unter https://support.citrix.com/article/CTX228454. In der App können Benutzer die OTP-Funktion hinzufügen, indem sie den auf NetScaler generierten QR-Code scannen oder das TOTP-Geheimnis manuell eingeben. Einmal hinzugefügte OTP-Token werden im Segment Kennwort-Tokens auf der Benutzeroberfläche angezeigt.

Um das Erlebnis zu verbessern, fordert das Hinzufügen eines OTP den Benutzer auf, automatisch ein VPN-Profil zu erstellen. Benutzer können dieses VPN-Profil nutzen, um direkt von ihren iOS-Geräten aus eine Verbindung zum VPN herzustellen.

Der Citrix Secure Access Client für macOS/iOS kann verwendet werden, um den QR-Code zu scannen, während Sie sich für die native OTP-Unterstützung registrieren.
Die NetScaler Gateway-Push-Benachrichtigungsfunktion ist nur für Citrix Secure Access für macOS/iOS-Benutzer verfügbar.

- **Push-Benachrichtigung:** NetScaler Gateway sendet Push-Benachrichtigungen auf Ihrem registrierten Mobilgerät für eine vereinfachte Zwei-Faktor-Authentifizierung. Anstatt den Citrix Secure Access Client für macOS/iOS zu starten, um das Einmalpasswort für den zweiten Faktor auf der NetScaler-Anmeldeseite bereitzustellen, können Sie Ihre Identität überprüfen, indem Sie Ihre Geräte-PIN/Touch-ID/Gesichts-ID für das registrierte Gerät angeben.

Sobald Sie Ihr Gerät für die Push-Benachrichtigung registriert haben, können Sie das Gerät auch für native OTP-Unterstützung mit Citrix Secure Access für macOS/iOS verwenden. Die Registrierung für Push-Benachrichtigungen ist für den Benutzer transparent. Wenn Benutzer TOTP registrieren, wird das Gerät auch für Push-Benachrichtigungen registriert, wenn NetScaler dies unterstützt.

Versionshinweise

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS wurde jetzt in Citrix Secure Access umbenannt. Wir aktualisieren die UI-Screenshots in unserer Dokumentation, um diese Namensänderung widerzuspiegeln.

> Möglicherweise stellen Sie auch fest, dass Citrix SSO-Referenzen in der iOS-Dokumentation während dieser Übergangszeit verwendet wurden.

In den Versionshinweisen werden die neuen Funktionen, Verbesserungen vorhandener Funktionen, behobene Probleme und bekannte Probleme beschrieben, die in einer Service-Version verfügbar sind. Die Versionshinweise enthalten einen oder mehrere der folgenden Abschnitte:

Was ist neu: Die neuen Funktionen und Verbesserungen, die in der aktuellen Version verfügbar sind.

Behobene Probleme: Die Probleme, die in der aktuellen Version behoben wurden.

Bekannte Probleme: Die in der aktuellen Version vorhandenen Probleme und deren Problemumgehungen, sofern zutreffend.

> **Wichtige Hinweise zu EPA-Clients:**
>
> - EPA-Clients werden in den Versionen macOS 10.13, 10.14, 10.15, 11.x, 12.x und 13.x unterstützt.
> - EPA-Clients werden in den Versionen NetScaler 12.1, 13.0, 13.1 und 14.1 unterstützt.

V24.03.1 (14. März 2024)

Was ist neu

- Die EPA-Bibliotheken wurden auf 24.03.1.0 aktualisiert (OPSWAT OESIS-Bibliothek V 4.3.3460.0).
- **Automatisches einmaliges Anmelden (SSO) bei Citrix Secure Access über die Citrix Workspace-App —Vorschau**

  Citrix Secure Access für macOS unterstützt jetzt automatisches Single Sign-On (SSO) bei Citrix Secure Access, wenn Sie sich bei der Citrix Workspace-App anmelden. Stellen Sie sicher, dass Sie Citrix Secure Access für macOS 24.03.1/Citrix Workspace-App für Mac 2402 und höher verwenden, um diese Funktionalität nutzen zu können. Diese Funktion wird nur in Cloud-Stores und nicht in lokalen Stores unterstützt.

  Derzeit ist diese Funktion standardmäßig deaktiviert. Sie können sich für die Vorschau anmelden unter https://podio.com/webforms/29383411/2410629.

  Einzelheiten finden Sie in den Versionshinweisen zur Citrix Workspace-App 2402 für Mac.

  [CSACLIENTS-6321]

- **Allgemeine Leistungs- und Stabilitätsverbesserungen**

  Der Citrix Secure Access Client wurde um die folgenden Funktionen erweitert, um die Gesamtleistung und Stabilität zu verbessern:

- Eine Erhöhung der Anzahl gleichzeitiger Verbindungen, die über ein VPN getunnelt werden können. Dies gilt nur für iOS-Clients.
- Eine verbesserte Stabilität der VPN-Verbindung mit IPv6-Gateways. Dies gilt sowohl für macOS- als auch für iOS-Clients.

[NSHELP-36903]

V24.02.1 (15. Februar 2024)

Was ist neu

- **Unterstützung für EPA-Scanoperatoren auf Mac-Clients**

  Der Citrix Secure Access Client für macOS unterstützt jetzt alle Operatoren <, >, >=, <=, == und != im EPA-Editor. Außerdem ist die **Mac OS-Option** als separate Option im EPA-Editor verfügbar (**Mac > Mac OS**). Mit diesen Operatoren können Sie einen Produktversionsscan Ihrer macOS-Geräte durchführen.

  Einzelheiten finden Sie im Abschnitt **Hinweis** unter Erweiterte Endpoint Analysis-Scans.

  [CSACLIENTS-6462]

- Die EPA-Bibliotheken wurden auf 24.1.2.1 aktualisiert (OPSWAT OESIS-Bibliothek V 4.3.3405.0).

  [CSACLIENTS-8520]

- In dieser Version werden einige Probleme behoben, um die Gesamtleistung und Stabilität zu verbessern.

24.1.5 EPA-Client für macOS (12. Februar 2024)

Was ist neu

- **EPA-Unterstützung für Mac-Geräte mit Apple-Siliziumprozessor**

  Der Citrix EPA-Client unterstützt jetzt Mac-Geräte, die den Apple-Siliziumprozessor verwenden. Auf Mac-Geräten muss Rosetta nicht mehr installiert sein, um den Citrix EPA-Client auszuführen.

  [CSACLIENTS-8731]

- **Unterstützung für EPA-Scanoperatoren auf Mac-Clients**

  Der Citrix EPA-Client für Mac unterstützt jetzt die Operatoren (<, >, >= und <=) in den EPA-Ausdrücken. Administratoren können EPA-Scans so konfigurieren, dass sie eine Vielzahl von Betriebssystemversionen zulassen.

Um beispielsweise die Betriebssystemversionen von 12.4 bis 13.0 außer 12.8 zuzulassen, können Administratoren den Ausdruck konfigurieren. `version >= 12.4 && version <= 13.0 && version != 12.8` Das bedeutet, dass die macOS-Version von 12.4 bis 13.0 sein muss, aber nicht 12.8 sein kann.

Einzelheiten finden Sie unter Erweiterte Endpoint Analysis-Scans.

[CSACLIENTS-6462]

V23.12.2 (20. Dezember 2023)

Was ist neu

In dieser Version werden Probleme behoben, um die Gesamtleistung und Stabilität zu verbessern.

V23.12.1 (06. Dezember 2023)

Was ist neu

- Die EPA-Bibliotheken wurden auf 23.11.1.5 aktualisiert (OPSWAT OESIS-Bibliothek V 4.3.3318.0).

  [CSACLIENTS-8516]
- In dieser Version werden weitere Probleme behoben, um die Gesamtleistung und Stabilität zu verbessern.

V23.11.2 (01. November 2023)

Was ist neu

EPA-Bibliotheken wurden auf 23.11.1.1 aktualisiert (OPSWAT OESIS-Bibliothek V 4.3.3279.0).

[CSACLIENTS-8515]

V23.11.1 (27. Oktober 2023)

Was ist neu

- Citrix SSO für iOS wurde jetzt in Citrix Secure Access umbenannt. Wir aktualisieren die UI-Screenshots in unserer Dokumentation, um diese Namensänderung widerzuspiegeln.
- EPA-Bibliotheken wurden auf 23.10.1.1 aktualisiert (OPSWAT OESIS-Bibliothek V 4.3.3246.0).
- Diese Version befasst sich mit den folgenden Themen:

- Verbindungsprobleme mit der Citrix Secure Private Access-Umgebung.
- Andere Probleme zur Verbesserung der Gesamtleistung und Stabilität.

V23.10.2 (17. Oktober 2023)

Diese Version behebt die IPv6-Anmeldeprobleme.

V23.10.1 (09. Oktober 2023)

Was ist neu

- EPA-Bibliotheken wurden auf 23.9.1.2 aktualisiert (OPSWAT OESIS-Bibliothek V4.3.3221.0).
- **Unterstützung für lokalen LAN-Zugriff**

  Citrix Secure Access für macOS/ Citrix SSO für iOS unterstützt jetzt die lokale LAN-Zugriffsfunktion von NetScaler Gateway. Sie können den lokalen LAN-Zugriff so konfigurieren, dass Endbenutzer nach dem Aufbau einer VPN-Verbindung entweder Zugriff auf lokale LAN-Ressourcen auf ihren Client-Geräten haben oder nicht. Weitere Informationen:

  - NetScaler Gateway-Administratorkonfigurationen
  - Endbenutzerkonfigurationen —macOS
  - Endbenutzerkonfigurationen —iOS

V23.09.1 (07. September 2023)

> **Wichtig:**
>
> Wenn Sie die neuesten Apple OS-Versionen wie macOS 14/iOS 17 und höher verwenden, empfehlen wir Ihnen, auf Citrix Secure Access Client/Citrix SSO Version 23.09.1 oder höher zu aktualisieren. Weitere Informationen zu den Anforderungen der NetScaler Gateway-Clientsoftware finden Sie unter Systemanforderungen für den Citrix Secure Access Client.

Was ist neu

- EPA-Bibliotheken wurden auf 1.3.9.9 (OPSWAT OESIS v4.3.3160) aktualisiert.

  [CSACLIENTS-6547]

- **Einblicke in gesicherte Verbindungen auf der Benutzeroberfläche**

  Auf dem Bildschirm „Verbindungen“der Citrix Secure Access Client-Benutzeroberfläche können Sie die gesicherten Verbindungsdetails anzeigen. Zu den Details gehören die IP-Adresse, der

FQDN, der Zielport und die Dauer der Verbindung. Weitere Informationen finden Sie unter Einblicke in gesicherte Verbindungen.

[SPA-2364]

- **Authentifizieren Sie sich nach einem VPN-Verbindungsfehler erneut mit NetScaler Gateway**

  Der Citrix Secure Access Client für macOS und Citrix SSO für iOS fordern Sie jetzt auf, sich erneut bei NetScaler Gateway zu authentifizieren, wenn eine VPN-Verbindung unterbrochen wird. Sie werden auf der Benutzeroberfläche darüber informiert, dass die Verbindung zu NetScaler Gateway unterbrochen wurde und dass Sie sich erneut authentifizieren müssen, um die Verbindung wieder aufzunehmen. Weitere Informationen:

  - Stellen Sie nach einem VPN-Verbindungsfehler von macOS erneut eine Verbindung zu NetScaler Gateway her
  - Stellen Sie nach einem VPN-Verbindungsfehler erneut eine Verbindung von iOS zu NetScaler Gateway her.

  [CSACLIENTS-6071]

V23.08.1 (24. August 2023)

Was ist neu

- In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.
- EPA-Bibliotheken wurden auf 1.3.9.9 aktualisiert (OPSWAT OESIS v4.3.3122).

23.7.6 EPA-Client für macOS (10. August 2023)

In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V23.07.1 (17. Juli 2023)

Was ist neu

- **Verschiedene Optionen zum Teilen von Protokolldateien**

  Die Option “Protokolle per E-Mail senden”in Citrix SSO für iOS wurde jetzt durch die Option “Protokolle teilen”ersetzt. Die komprimierten Protokolldateien können jetzt über Optionen wie E-Mail, Chat, In Dateien speichern usw. freigegeben werden.

Weitere Informationen finden Sie unter Protokolle senden.

[CSACLIENTS-3834]

- **Verbesserungen an der Seite "Logs"**

  Die Protokollseite von Citrix Secure Access für macOS wurde um die folgenden Optionen erweitert:

  - Maximale Anzahl von Protokolldateien: Geben Sie die maximale Anzahl von Protokolldateien an, die Sie für die Protokollsammlung hinzufügen möchten.
  - Protokolle per E-Mail senden: Senden Sie die Protokolle per E-Mail.

  Weitere Informationen finden Sie unter Protokolle senden.

  [SPA-2365]

Behobene Probleme

Wenn Sie bei der Verbindung mit VPN aufgefordert werden, ein Zertifikat für die Authentifizierung auszuwählen, wird der Anmeldebildschirm für die Authentifizierung hinter der Homepage des Citrix Secure Access Clients angezeigt.

[CSACLIENTS-455]

V23.06.1 (07. Juni 2023)

Was ist neu

- **Hilfemenü in der Navigationsleiste**

  Der Navigationsleiste des Citrix Secure Access Clients wurde jetzt ein Hilfemenü hinzugefügt. Die Optionen (Protokolle öffnen, Protokolle exportieren, E-Mail-Protokolle und Protokolle löschen) im Hilfemenü können zum Debuggen von Protokollen verwendet werden.

  Im Hilfemenü wird eine Option E-Mail-Protokolle eingeführt. Es kann verwendet werden, um die Protokolle per E-Mail zu teilen. Weitere Informationen finden Sie unter Protokolle senden.

  [SPA-2361]

Behobene Probleme

In einigen Fällen schlägt die DNS-Kurznamenauflösung auf Citrix Secure Access für macOS und Citrix SSO für iOS fehl.

[NSHELP-34568]

Bekannte Probleme

In einigen Fällen werden die ausgeschlossenen Routen beim Reverse-Split-Tunneling getunnelt.

[CGOP-24575]

V23.05.2 (11. Mai 2023)

Behobene Probleme

Nach einem Upgrade können die Citrix SSO für iOS-Clientgeräte keine VPN-Verbindungen pro App herstellen.

[NSHELP-35224]

V23.05.1 (04. Mai 2023)

Was ist neu

- EPA-Bibliotheken wurden auf 1.3.9.3 und OPSWAT-Bibliotheken auf 4.3.2987 aktualisiert.
- **Unterstützung für das Senden von Ereignissen an Citrix Analytics**

  Citrix Secure Access für macOS unterstützt jetzt das Senden von Ereignissen wie Sitzungserstellung, Sitzungsbeendigung und App-Verbindung an den Citrix Analytics Service. Diese Ereignisse werden dann im Secure Private Access-Dienst-Dashboard protokolliert.

  [SPA-2197]

Behobene Probleme

- Wenn die Benutzer mit Citrix Secure Access oder Citrix SSO verbunden sind, zeigt das Feld „Verbindungsdauer“die Uhrzeit nicht im regionsspezifischen Format an.

  [CGOP-23587]

V23.04.1 (04. April 2023)

Was ist neu

- Die EPA-Bibliotheken wurden auf 1.3.9.1 und die OPSWAT-Bibliotheken auf 4.3.2923 aktualisiert.

V22.12.2 (27. Feb. 2023)

Was ist neu

- Die EPA-Bibliotheken wurden auf 1.3.8.9 aktualisiert (OPSWAT OESIS v4.3.2892.0).

V22.12.1 (07. Dez. 2022)

In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V22.11.1 (29. Nov. 2022)

Behobene Probleme

- Die Übertragungsanmeldung funktioniert nicht für die Nicht-nFactor-Authentifizierung mit on-premises Gateways.

  [CGOP-22729]

22.11.3 EPA-Plug-In für macOS (28.11.2022)

Behobene Probleme

- Das Citrix EPA-Plug-In für macOS stürzt ab, wenn GSLB auf NetScaler aktiviert ist.

  [CGOP-22722]

V22.10.1 (17. November 2022)

Was ist neu

- Das Citrix Endpoint Analysis-Plug-In unterstützt jetzt neue Ausdrücke zur MAC-Adressüberprüfung, mit denen Mustersätze für die Liste der zulässigen IP-Adressen erstellt werden können.

  [CGOP-22095]

Behobene Probleme

- Manchmal führen leere Proxyeinstellungen in NetScaler Gateway Version 13.0 oder 13.1 dazu, dass Citrix SSO falsche Proxyeinstellungen erstellt.

  [NSHELP-31970]

- Manchmal können VPN-Clients nach einem Netzwerkausfall oder nach dem Erwachen des Geräts aus dem Ruhemodus keine Verbindung herstellen.

  [NSHELP-32483]

- Manchmal schlagen Gateway-Verbindungen fehl, wenn IPv6-Literale als Ziel verwendet werden.

  [NSHELP-32876]

22.10.1 EPA-Plug-In für macOS (27.10.2022)

Was ist neu

- Das Citrix Endpoint Analysis-Plug-In unterstützt jetzt einen neuen Ausdruck zur MAC-Adressüberprüfung, mit dem Mustersätze für die Liste der zulässigen IP-Adressen erstellt werden können.

  [CGOP-22098]

- Das Citrix Endpoint Analysis-Plug-In sendet doppelte Einwilligungswarnungen und bearbeitet Preflight-Anfragen für privaten Netzwerkzugriff von Google Chrome.

  [CGOP-21751]

V22.06.1 (20-Sep-2022)

Was ist neu

- EPA-Bibliotheken wurden auf 4.3.2523.0 aktualisiert (1.3.7.5)

Behobene Probleme

- Die nFactor-Authentifizierung mit EPA-Scan funktioniert auf den macOS-Clients nicht.

  [NSHELP-32182 - macOS]

- Auf der Secure Access Agent-Startseite für macOS werden je nach ausgewähltem Thema (hell oder dunkel) links und oben im Hamburger-Menü zusätzliche Polster mit weißer oder schwarzer Farbe angezeigt.

[CGOP-19353 - macOS]

- Bei der Anmeldung beim VPN wird das WebView-Fenster beim ersten Versuch minimiert, wenn das Gerätezertifikat konfiguriert ist.

  [CGOP-19354 - macOS]

- Die Endpunktanalyse funktioniert nicht für die Citrix Secure Access-App auf dem macOS-Client, wenn GSLB auf der NetScaler Appliance aktiviert ist.

  [CGOP-21634 - macOS]

- Wenn der konfigurierte Anwendungsname ein Leerzeichen enthält und Sie versuchen, auf die App zuzugreifen, wird das Popup "Enhanced Security Enabled"auf macOS-Clients nicht angezeigt.

  [ACS-2632 - macOS]

- Die nFactor-Authentifizierung mit einem optionalen Client-Zertifikat schlägt fehl, wenn keine entsprechenden Client-Zertifikate auf dem Gerät vorhanden sind.

  [NSHELP-32127 - iOS]

- Auf einem Mac-Gerät, das Chrome verwendet, stürzt die VPN-Erweiterung beim Zugriff auf zwei FQDNs ab.

  [NSHELP-32144]

- Citrix Secure Access stürzt ab, wenn ein falscher Standortwert vom Gateway empfangen wird. Dies kann passieren, wenn der Administrator eine Responderrichtlinie definiert, um auf einen anderen Host umzuleiten.

  [NSHELP-32312]

- Direkte Verbindungen zu Ressourcen außerhalb des von Citrix Secure Access eingerichteten Tunnels schlagen möglicherweise fehl, wenn es zu einer erheblichen Verzögerung oder Überlastung kommt.

  [NSHELP-31598]

V3.2.4.9 - EPA-Plug-In für macOS (01-Aug-2022)

Behobene Probleme

- Das Citrix Endpoint Analysis-Plug-In verarbeitet keine Preflight-Anforderungen für den privaten Netzwerkzugriff von Google Chrome-Browser Version 104.

  [CGOP-20709]

- Das Citrix Endpoint Analysis Plug-In für macOS unterstützt GSLB nicht.

  [CGOP-21543]

Bekannte Probleme

- Das Citrix Endpoint Analysis Plug-In für macOS zeigt ein doppeltes Zustimmungsdialogfeld an, wenn es von Google Chrome-Browser Version 104 gestartet wird. Die Benutzer müssen beide Aufforderungen akzeptieren.

  [CGOP-21751]

V22.03.1 (14-Jun-2022)

Was ist neu

- EPA-Bibliotheken wurden auf 4.3.2393.0 aktualisiert.

Behobene Probleme

- Eine zusätzliche DNS-Domain wird der Suchliste hinzugefügt. Dies liegt daran, dass, wenn der Split-Tunnel auf "Split"oder "Both"gesetzt ist, nur die angegebenen Domänen und ihre Subdomains NICHT getunnelt werden. Wenn die angegebene Domain A.B.C ist, wird zusätzlich zu A.B.C und *.A.B.C auch B.C. abgeglichen.

  [CGOP-21657]

- HTTP/HTTPS-Proxyeinstellungen, die keine PAC-Datei verwenden, sind fehlerhaft.

  [CGOP-21660]

V22.02.3 (24-Mar-2022)

Was ist neu

- Citrix Secure Access für macOS löst den FQDN eines Dienstknotens bei jeder TCP-Datenverbindung vom Client für die Cloud-Workspace-Verbindungen auf. Das Auflösen des FQDN eines Dienstknotens bei jeder TCP-Datenverbindung ist für die on-premises Gateway-Verbindungen nicht anwendbar.

  [ACS-1068]

Behobene Probleme

- Manchmal unterbricht Citrix Secure Access für macOS Verbindungen aufgrund von Problemen mit einigen Nicht-DNS-Protokollen, die Port 53 verwenden, wie z. B. STUN.

  [NSHELP-31004]

- Die Citrix Secure Access-App unterbricht einige Protokolle, wenn der Server Daten vor dem Client sendet, unmittelbar nachdem die Verbindung hergestellt wurde.

  [NSHELP-29374]

- Wenn der Benutzer das Authentifizierungsfenster des Citrix Secure Access Clients für macOS schließt, ohne die Authentifizierung abzuschließen, schlagen nachfolgende Versuche, eine Verbindung zum Server herzustellen, fehl, bis die App neu gestartet wird.

  [ACS-2415]

- Der Citrix Secure Access Client für macOS ist jetzt mit der OPSWAT-Bibliotheksversion 4.3.2367.0 gebündelt

  [NSHELP-30802]

- Citrix Secure Access für macOS benötigt länger als erwartet, um die EPA-Prüfung nach der Authentifizierung auszuführen.

  [NSHELP-29118]

Bekannte Probleme

- Die Citrix Secure Access-App für macOS meldet sich eine Minute, nachdem die bereits verbundene Citrix Secure Private Access-Dienstregion nicht mehr erreichbar ist, ab. Dies wirkt sich jedoch nicht auf die on-premises Gateway-Verbindungen aus.

  [ACS-2715]

V22.02.2 (15-Feb-2022)

Behobene Probleme

- Wenn ein Benutzer versucht, über Citrix Secure Access für macOS auf eine nicht abonnierte Webanwendung zuzugreifen, werden mehrere Popups angezeigt.

  [ACS-2406]

V22.01.1 (08-Feb-2022)

Behobene Probleme

- Pro-App-VPN-Verbindungen mit Citrix SSO für iOS-Geräte können an anderen Ports als 443 keine Verbindung zu NetScaler Gateway herstellen.

  [NSHELP-30653]

V1.4.1 (28-Jan-2022)

Was ist neu

- Die Citrix SSO-App für macOS wurde jetzt in Citrix Secure Access umbenannt.

  [ACS-1092]

Behobene Probleme

- Die Authentifizierung des Clientzertifikats schlägt fehl, wenn der Authentifizierungsserver das Client-Zertifikat in derselben Webview-Sitzung mehrmals anfordert.

  [CGOP-20388]

- Citrix SSO kann keine VPN-Verbindung herstellen, wenn das Serverzertifikat aufgrund eines Proxys zwischen dem Client und dem ADC nur eine IP-Adresse für den allgemeinen Namen hat.

  [CGOP-20390]

- Der EPA-Scan zur Überprüfung des letzten vollständigen Systemscans des Virenschutzes schlägt unter macOS fehl.

  [NSHELP-29571]

- Manchmal stürzt die Citrix SSO-App ab, während große DNS-Pakete verarbeitet werden.

  [NSHELP-29133]

V1.4.0 (17-Nov-2021)

Behobene Probleme

- Manchmal schlägt der Servervalidierungscode fehl, wenn das Serverzertifikat vertrauenswürdig ist. Daher können Endbenutzer nicht auf das Gateway zugreifen.

  [NSHELP-28942]

- Citrix SSO kann die VPN-Verbindung nach einer Netzwerkunterbrechung nicht wieder herstellen.

  [CGOP-19988]

V1.3.13 (05-Nov-2021)

Behobene Probleme

- Beim Filtern von Sitzungen nach verwalteten und nicht verwalteten VPNs kann es zu Fehlern kommen. Bei den ersten Anforderungen zum Einrichten der Sitzung fehlen die "ManagedVpn" -Informationen im User-Agent-Header.

  [CGOP-19561]

V1.3.12 (21-Oct-2021)

Behobene Probleme

- Die Clientzertifikatauthentifizierung schlägt für Citrix SSO für macOS fehl, wenn der macOS-Schlüsselbund keine Clientzertifikate enthält.

  [NSHELP-28551]

- Die Citrix SSO-App stürzt beim Empfang von Benachrichtigungen zeitweise ab.

  [CGOP-19363]

- Die VPN-Erweiterung stürzt möglicherweise ab, wenn der Parameter "isFeatureEnabled" aufgerufen wird, um ein Feature-Flag zu überprüfen.

  [CGOP-19360]

- Die Gateway-VPN-Erweiterung stürzt ab, wenn das DTLS-Protokoll eine leere Nutzlast hat.

  [CGOP-19361]

- Die SSO-App stürzt zeitweise ab, wenn das Gerät aus dem Ruhemodus aufwacht und das VPN verbunden ist.

  [CGOP-19362]

V1.3.11 (17-Sep-2021)

Behobene Probleme

- Der EPA-Scan für die Firewall-Prüfung schlägt für macOS-Geräte mit Citrix SSO fehl.

[CGOP-19271]

- Citrix SSO stürzt auf einem iOS 12-Gerät ab, wenn die Legacy-Authentifizierung oder Intune Network Access Compliance (NAC) konfiguriert ist.

  [CGOP-19261]

V1.3.10 (31-Aug-2021)

Was ist neu

- Citrix SSO für macOS ist jetzt mit der OPSWAT-Bibliothek Version 4.3.1977.0 gebündelt.

  [NSHELP-28467]

V1.3.9 (13-Aug-2021)

Behobene Probleme

- Auf einigen Systemen mit installierter HTTP-Proxy-Software wird die NetScaler Gateway-IP-Adresse intern als 127.0.0.1 angezeigt, wodurch die Einrichtung eines Tunnels verhindert wird.

  [CGOP-18538]

- Die Einstellung "Nicht vertrauenswürdige Server blockieren"funktioniert nicht auf Systemen, die die nicht-englische Lokalisierung von Citrix SSO für iOS unterstützen.

  [CGOP-18539]

- Citrix SSO kann keine Verbindung zu Systemen herstellen, bei denen der DNS-Name nicht mit dem allgemeinen Namen im Serverzertifikat übereinstimmt. Citrix SSO sucht jetzt nach alternativen Namen des Betreffs und stellt eine korrekte Verbindung her.

  [NSHELP-28348]

V1.3.8 (07-Jul-2021)

Was ist neu

- Citrix SSO für macOS ist nur mit den Versionen 10.15 (Catalina) und höher kompatibel.

  [CGOP-12555]

- Ab Citrix SSO für macOS Version 1.3.8 sind die EPA-Bibliotheken in die App eingebettet und nicht vom NetScaler Gateway-Server heruntergeladen. Die aktuelle Version der eingebetteten EPA-Bibliothek ist 1.3.5.1.

  [NSHELP-26838]

Citrix Secure Access für iOS-Benutzer einrichten

March 27, 2024

> **Wichtig:**
>
> - Citrix SSO für iOS wurde jetzt in Citrix Secure Access umbenannt. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln. Möglicherweise stellen Sie fest, dass in der Übergangszeit in der Dokumentation Citrix SSO-Referenzen verwendet werden.
> - VPN kann unter iOS 12 und höher nicht verwendet werden. Verwenden Sie Citrix Secure Access, um weiterhin VPN zu nutzen.

Eine Liste einiger häufig verwendeter Funktionen, die von Citrix Secure Access für iOS unterstützt werden, finden Sie unter NetScaler Gateway VPN-Clients und unterstützte Funktionen.

Kompatibilität mit MDM-Produkten

Citrix Secure Access (macOS/iOS) ist mit den meisten MDM-Anbietern wie Citrix Endpoint Management (früher XenMobile), Microsoft Intune usw. kompatibel.

Citrix Secure Access (macOS/iOS) unterstützt auch eine Funktion namens Network Access Control (NAC). Weitere Informationen zu NAC finden Sie unter Konfigurieren des Geräts für die Netzwerkzugriffssteuerung. Überprüfen Sie den virtuellen NetScaler Gateway-Server für die Einzelfaktor-Anmeldung Mit NAC können MDM-Administratoren die Konformität von Endbenutzergeräten durchsetzen, bevor sie eine Verbindung zur NetScaler Appliance herstellen. NAC auf Citrix Secure Access (macOS/iOS) erfordert einen MDM-Server wie Citrix Endpoint Management oder Intune und NetScaler.

> **Hinweis:**
>
> Um den Citrix Secure Access Client unter macOS/iOS mit NetScaler Gateway VPN ohne MDM zu verwenden, müssen Sie eine VPN-Konfiguration hinzufügen. Sie können die VPN-Konfiguration auf iOS von der Citrix Secure Access (macOS/iOS) -Startseite hinzufügen.

Konfigurieren Sie ein MDM-verwaltetes VPN-Profil für den Citrix Secure Access Client (macOS/iOS)

Im folgenden Abschnitt finden Sie schrittweise Anweisungen zur Konfiguration von geräteweiten und appspezifischen VPN-Profilen für den Citrix Secure Access Client (macOS/iOS) am Beispiel von Citrix Endpoint Management (ehemals XenMobile). Andere MDM-Lösungen können dieses Dokument als Referenz verwenden, wenn sie mit Citrix Secure Access (macOS/iOS) arbeiten.

> **Hinweis:**
>
> In diesem Abschnitt werden die Konfigurationsschritte für ein grundlegendes geräteweites und pro-App-VPN-Profil erläutert. Sie können auch On-Demand-Proxys konfigurieren, indem Sie der Dokumentation zu Citrix Endpoint Management (ehemals XenMobile) oder der MDM-VPN-Payload-Konfigurationvon Apple folgen.

VPN-Profile auf Geräteebene

VPN-Profile auf Geräteebene werden verwendet, um ein systemweites VPN einzurichten. Der Datenverkehr von allen Apps und Diensten wird basierend auf den in NetScaler definierten VPN-Richtlinien (wie Full-Tunnel, Split-Tunnel, Reverse Split-Tunnel) an NetScaler Gateway getunnelt.

So konfigurieren Sie ein VPN auf Geräteebene in Citrix Endpoint Management Führen Sie die folgenden Schritte aus, um ein VPN auf Geräteebene in Citrix Endpoint Management zu konfigurieren.

1. Navigieren Sie auf der Citrix Endpoint Management MDM-Konsole zu **Konfigurieren** > **Geräterichtlinien** > **Neue Richtlinie hinzufügen**.
2. Wählen Sie **im linken Bereich Policy Platform iOS** aus. Wählen Sie im rechten Bereich **VPN** aus.
3. Geben Sie auf der Seite **Richtlinieninformationen** einen gültigen Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **VPN-Richtlinie** für iOS einen gültigen Verbindungsnamen ein und wählen Sie **Benutzerdefiniertes SSL** unter **Verbindungstyp**.

   In der MDM-VPN-Nutzlast entspricht der Verbindungsname dem **UserDefinedName-Schlüssel** und der **VPN-Typschlüssel** muss auf **VPN**eingestellt sein.
5. Geben Sie unter **Benutzerdefinierte SSL-Kennung (umgekehrtes DNS-Format)com.citrix.netscalergatew**
   Dies ist die Paket-ID für Citrix Secure Access auf iOS.

   In der MDM-VPN-Nutzlast entspricht der Custom SSL Identifier dem Schlüssel **VPNSubtype**.

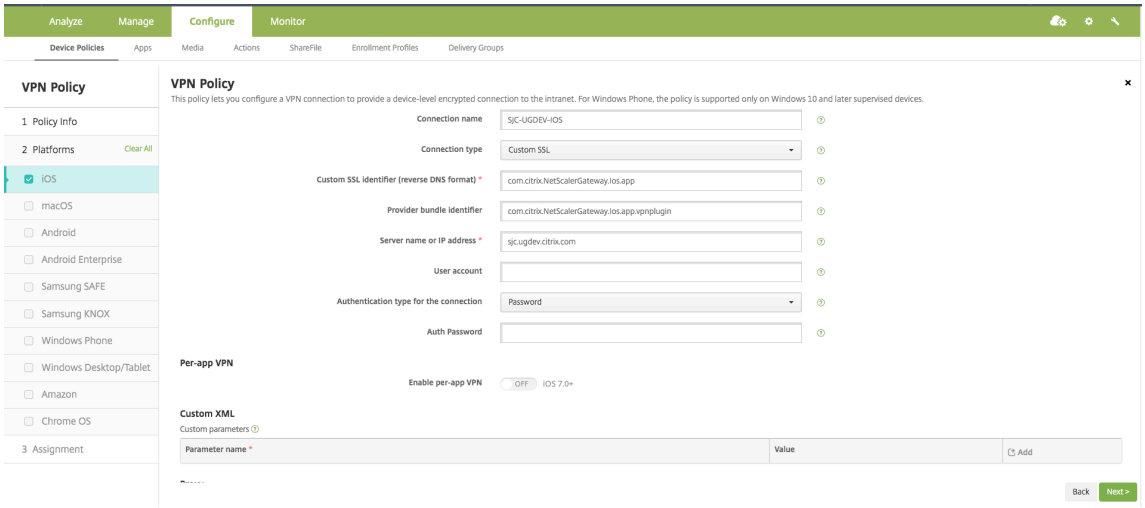
6. Geben Sie unter **Anbieter-Bundle-IDcom.citrix.netscalerGateway.ios.app.VPNPlugin**ein. Dies ist die Paket-ID der Netzwerkerweiterung, die in der Binärdatei der Citrix Secure Access iOS-App enthalten ist.

   In der MDM-VPN-Nutzlast entspricht die Anbieter-Bundle-ID dem **ProviderBundleIdentifier-Schlüssel**.

7. Geben Sie **unter Servername oder IP-Adresse** die IP-Adresse oder den FQDN (vollqualifizierter Domänenname) des NetScaler ein, der dieser Citrix Endpoint Management-Instanz zugeordnet ist.

   Die verbleibenden Felder auf der Konfigurationsseite sind optional. Konfigurationen für diese Felder finden Sie in der Dokumentation zu Citrix Endpoint Management (ehemals XenMobile).

8. Klicken Sie auf **Weiter**.



9. Klicken Sie auf **Speichern**.

Pro-App-VPN-Profile

Pro-App-VPN-Profile werden verwendet, um das VPN für eine bestimmte Anwendung einzurichten. Der Datenverkehr nur von der bestimmten App wird zu NetScaler Gateway getunnelt. Die **VPN-Nutzlast pro App** unterstützt alle Schlüssel für geräteweites VPN sowie einige andere Schlüssel.

So konfigurieren Sie ein VPN auf App-Ebene auf Citrix Endpoint Management Führen Sie die folgenden Schritte aus, um ein Per-App VPN zu konfigurieren:

1. Schließen Sie die VPN-Konfiguration auf Geräteebene in Citrix Endpoint Management ab.
2. Schalten Sie den Schalter **Pro-App-VPN** aktivieren im Abschnitt Pro-App-VPN ein.

3. Schalten Sie den **Schalter On-Demand Match App Enabled** EIN, wenn Citrix Secure Access (macOS/iOS) automatisch gestartet werden muss, wenn die Match App gestartet wird. Dies wird für die meisten Per-App-Fälle empfohlen.

   In der MDM-VPN-Nutzlast entspricht dieses Feld dem Schlüssel **onDemandMatchAppEnabled**.

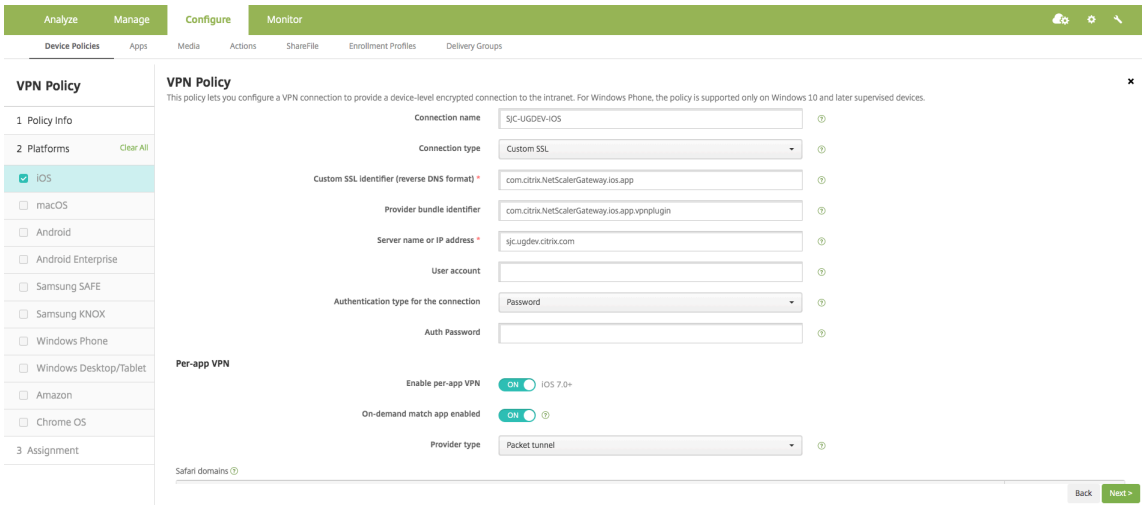
4. Wählen Sie unter **ProvidertypPacket Tunnel**aus.

   In der MDM-VPN-Nutzlast entspricht dieses Feld dem **Schlüsselanbietertyp**.

5. Die Konfiguration der Safari-Domain ist optional. Wenn eine Safari-Domäne konfiguriert ist, wird Citrix Secure Access (macOS/iOS) automatisch gestartet, wenn Benutzer Safari starten und zu einer URL navigieren, die der URL im Feld **Domain** entspricht. Dies wird nicht empfohlen, wenn Sie das VPN für eine bestimmte App einschränken möchten.

   In der MDM-VPN-Nutzlast entspricht dieses Feld den wichtigsten **SafariDomains**.

   Die verbleibenden Felder auf der Konfigurationsseite sind optional. Konfigurationen für diese Felder finden Sie in der Dokumentation zu Citrix Endpoint Management (ehemals XenMobile).



6. Klicken Sie auf **Weiter.**
7. Klicken Sie auf **Speichern**.

Um dieses VPN-Profil einer bestimmten App auf dem Gerät zuzuordnen, müssen Sie eine App-Inventarrichtlinie und eine Richtlinie für den Anbieter von Anmeldeinformationen erstellen, indem Sie diesem Handbuch folgen - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/.

Konfigurieren eines Split-Tunnels im Pro-App-VPN

MDM-Kunden können Split-Tunnel in Per-App VPN für Citrix Secure Access (macOS/iOS) konfigurieren. Das folgende Schlüssel/Wert-Paar muss dem Abschnitt zur Herstellerkonfiguration des auf dem MDM-

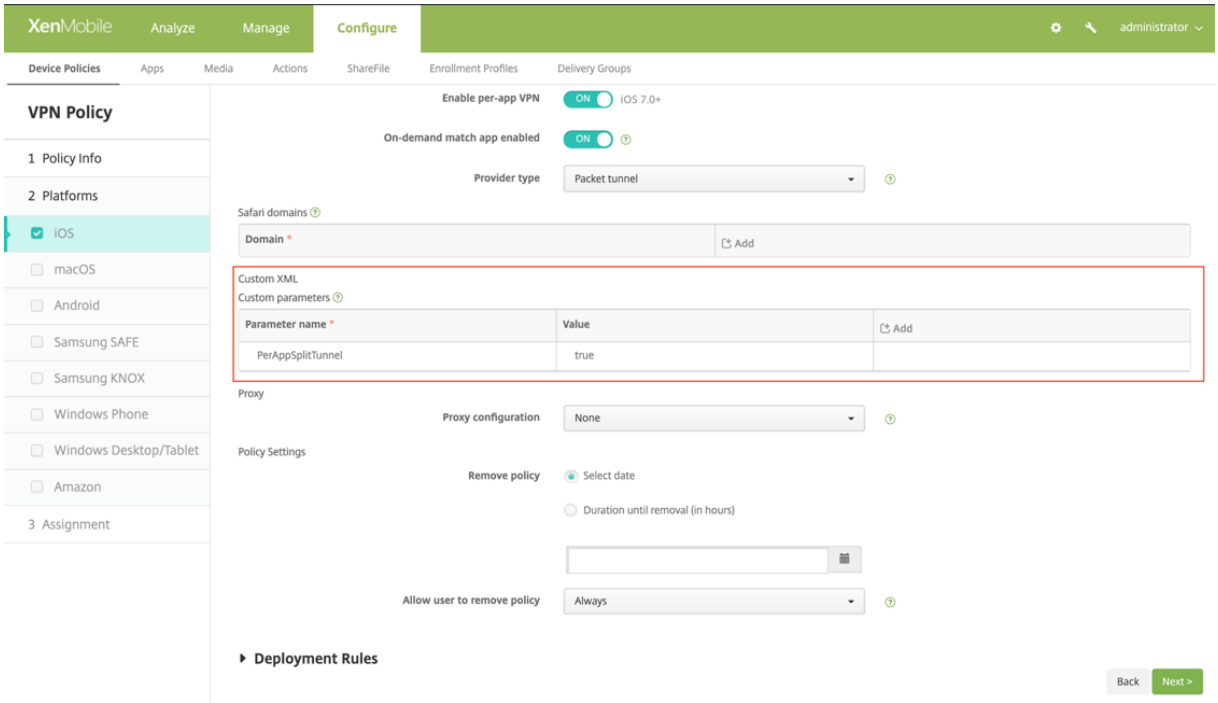
Server erstellten VPN-Profils hinzugefügt werden.

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

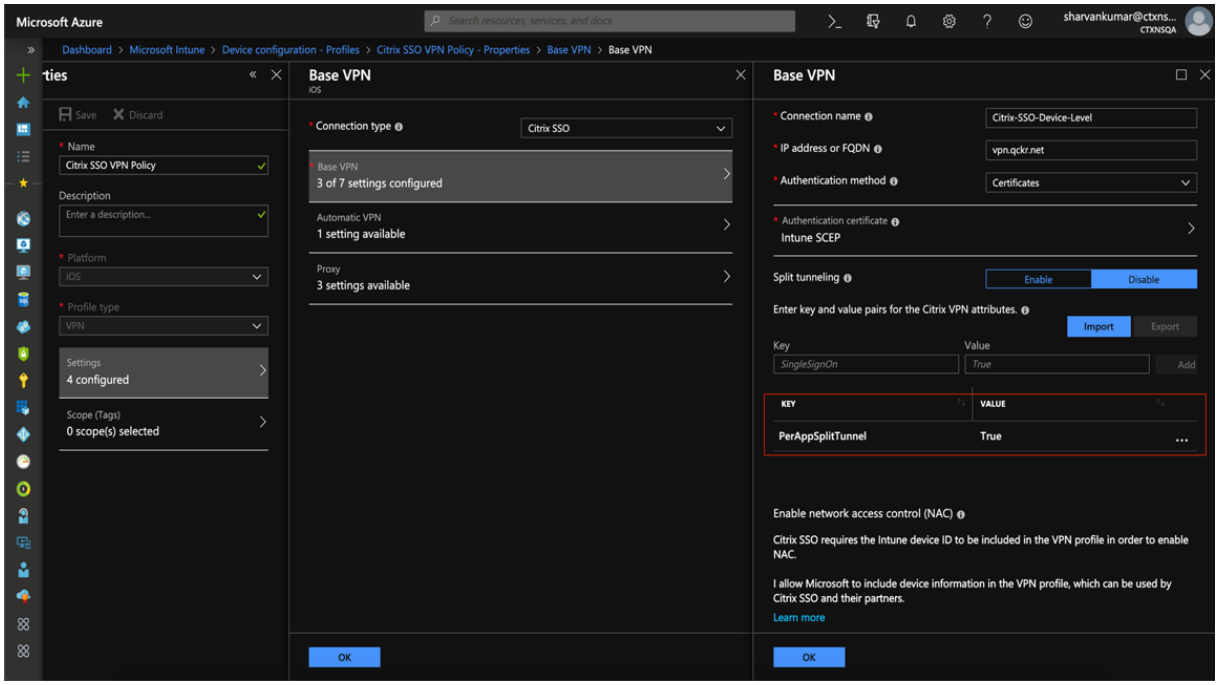
Der Schlüssel berücksichtigt die Groß-/Kleinschreibung und muss exakt übereinstimmen, während der Wert nicht zwischen Groß- und Kleinschreibung beachtet

> **Hinweis:**
>
> Die Benutzeroberfläche zum Konfigurieren der Anbieterkonfiguration ist bei allen MDM-Anbietern nicht Standard. Wenden Sie sich an den MDM-Anbieter, um den Abschnitt zur Anbieterkonfiguration auf Ihrer MDM-Benutzerkonsole zu finden.

Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Citrix Endpoint Management.



Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Microsoft Intune.



Deaktivieren von Benutzern erstellten VPN-Profilen

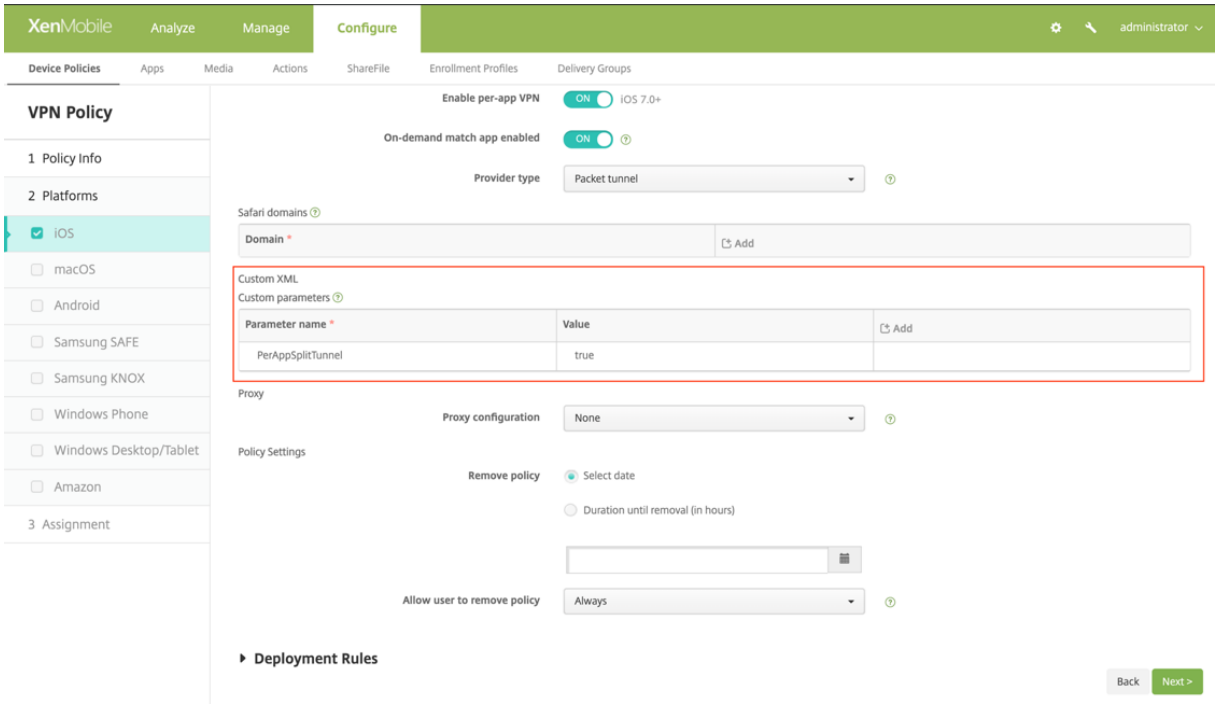
MDM-Kunden können verhindern, dass Benutzer manuell VPN-Profile in Citrix Secure Access (macOS/iOS) erstellen. Dazu muss das folgende Schlüssel/Wert-Paar zum Abschnitt Herstellerkonfiguration des auf dem MDM-Server erstellten VPN-Profils hinzugefügt werden.

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

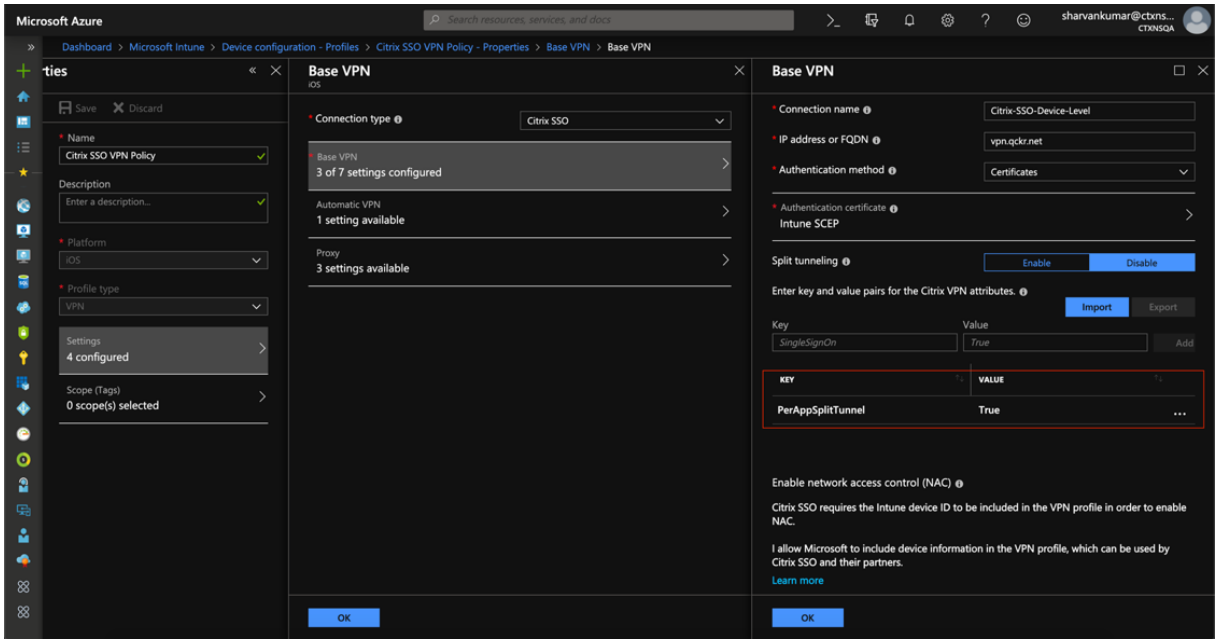
Der Schlüssel berücksichtigt die Groß-/Kleinschreibung und muss exakt übereinstimmen, während der Wert nicht zwischen Groß- und Kleinschreibung beachtet

> **Hinweis:**
>
> Die Benutzeroberfläche zum Konfigurieren der Anbieterkonfiguration ist bei allen MDM-Anbietern nicht Standard. Wenden Sie sich an den MDM-Anbieter, um den Abschnitt zur Anbieterkonfiguration auf Ihrer MDM-Benutzerkonsole zu finden.

Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Citrix Endpoint Management.



Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Microsoft Intune.



DNS-Handhabung

Die empfohlenen DNS-Einstellungen für den Citrix Secure Access Client lauten wie folgt:

- **DNS teilen > REMOTE**, wenn der geteilte Tunnel auf **AUS gestellt ist.**

- **DNS teilen > BEIDE**, wenn der geteilte Tunnel auf **ON**eingestellt ist. In diesem Fall müssen die Administratoren DNS-Suffixe für die Intranet-Domains hinzufügen. DNS-Abfragen für FQDNs, die zu DNS-Suffixen gehören, werden an die NetScaler Appliance getunnelt, und die verbleibenden Abfragen gehen an den lokalen Router.

> **Hinweis:**
>
> - Es wird empfohlen, dass das **DNS-Abkürzungsfix**-Flag immer **ON** ist. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX200243.
> - Wenn der Split-Tunnel auf **ON** eingestellt ist und Split-DNS auf **REMOTE**eingestellt ist, kann es zu Problemen bei der Lösung von DNS-Abfragen kommen, nachdem das VPN verbunden ist. Dies hängt damit zusammen, dass das Network Extension-Framework nicht alle DNS-Abfragen abfängt.

Bekannte Probleme

Problembeschreibung: Tunneln für FQDN-Adressen, die eine Domäne “ `.local`”in Pro-App-VPN- oder On-Demand-VPN-Konfigurationen enthalten. Es gibt einen Fehler im Network Extension Framework von Apple, der verhindert, dass FQDN-Adressen, die `.local` im Domänenteil enthalten (z. B. http://wwww.abc.local), über die TUN-Schnittstelle des Systems getunnelt werden. Stattdessen wird der Datenverkehr für die FQDN-Adressen über die physische Schnittstelle des Client-Geräts gesendet. Das Problem wird nur bei der Pro-App-VPN- oder On-Demand-VPN-Konfiguration beobachtet und tritt bei systemweiten VPN-Konfigurationen nicht auf. Citrix hat einen Radar-Fehlerbericht bei Apple eingereicht, und Apple hat festgestellt, dass laut RFC-6762: https://tools.ietf.org/html/rfc6762 “local” eine Multicast-DNS-Abfrage (mDNS) ist und somit kein Bug ist. Apple hat den Fehler jedoch noch nicht geschlossen und es ist nicht klar, ob das Problem in zukünftigen iOS-Versionen behoben wird.

Problemumgehung: Weisen Sie einen Domänennamen non `.local` für Adressen wie die Problemumgehung zu.

Einschränkungen

- Die Endpunktanalyse (EPA) wird unter iOS nicht unterstützt.
- Split-Tunneling basierend auf Ports/Protokollen wird nicht unterstützt.

Identität des Benutzerzertifikats als E-Mail-Anhang an iOS-Benutzer senden

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Citrix Secure Access unter iOS unterstützt die Clientzertifikatauthentifizierung mit NetScaler Gateway. Unter iOS können Zertifikate auf eine der folgenden Arten an Citrix Secure Access übermittelt werden:

- MDM-Server - Dies ist der bevorzugte Ansatz für MDM-Kunden. Zertifikate werden direkt im MDM-verwalteten VPN-Profil konfiguriert. Die VPN-Profile und die Zertifikate werden dann an registrierte Geräte übertragen, wenn sich ein Gerät beim MDM-Server registriert. Bitte befolgen Sie für diesen Ansatz die herstellerspezifischen MDM-Dokumente.
- E-Mail - Einzige Methode für Nicht-MDM-Kunden. Bei diesem Ansatz senden Administratoren eine E-Mail mit der Identität des Benutzerzertifikats (Zertifikat und privater Schlüssel), die als PCKS #12 -Datei angehängt ist, an Benutzer. Benutzer müssen ihre E-Mail-Konten auf ihrem iOS-Gerät konfiguriert haben, um die E-Mail mit Anhang zu erhalten. Die Datei kann dann in Citrix Secure Access auf dem iOS importiert werden. Im folgenden Abschnitt werden die Konfigurationsschritte für diesen Ansatz erläutert.

Voraussetzungen

- Benutzerzertifikat - Eine PKCS #12 -Identitätsdatei mit einer Erweiterung.pfx oder .p12 für einen bestimmten Benutzer. Diese Datei enthält sowohl das Zertifikat als auch den privaten Schlüssel.
- Auf dem iOS-Gerät konfiguriertes E-Mail-Konto.
- Citrix Secure Access ist auf dem iOS-Gerät installiert.

Konfigurationsschritte

1. Benennen Sie die Erweiterung/den MIME-Typ des Benutzerzertifikats um.

   Dateierweiterungen, die am häufigsten für Benutzerzertifikate verwendet werden, sind “.pfx” , “.p12”usw. Diese Dateierweiterungen sind im Gegensatz zu Formaten wie .pdf, .doc für die iOS-Plattform nicht standardmäßig. Sowohl „.pfx“als auch „.p12”werden vom iOS-System

beansprucht und können nicht von Drittanbieter-Apps wie Citrix Secure Access beansprucht werden. Daher hat Citrix Secure Access eine neue Erweiterung/einen neuen MIME-Typ namens „.citrixsso-pfx“und „.citrixsso-p12”definiert. Administratoren müssen den Erweiterungs-/MIME-Typ des Benutzerzertifikats von Standard “.pfx”oder “.p12”auf “.citrixsso-pfx” bzw. “.citrixsso-p12”ändern. Um die Erweiterung umzubenennen, können Administratoren den folgenden Befehl in der Eingabeaufforderung oder im Terminal ausführen.

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-->
```

2. Senden Sie die Datei als E-Mail-Anhang.

   Die Benutzerzertifikatdatei mit der neuen Erweiterung kann als E-Mail-Anhang an den Benutzer gesendet werden.

   Nach Erhalt der E-Mail müssen Benutzer das Zertifikat in Citrix Secure Access installieren.

Richten Sie die Proxy-PAC-Datei für die Citrix SSO-App für iOS-Benutzer oder den Citrix Secure Access-Client für macOS-Benutzer ein

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Die Citrix Secure App für iOS oder der Citrix Secure Access Client für macOS unterstützen Auto Proxy Config (Proxy-PAC-Datei) nach der Einrichtung des VPN-Tunnels. Administratoren können die Proxy-PAC-Datei verwenden, damit der gesamte HTTP-Verkehr des Clients einen Proxy durchlaufen kann, einschließlich der Auflösung von Hostnamen.

So richten Sie eine Proxy-PAC-Datei ein

Haben Sie einen internen Computer, der eine Proxy-Datei hosten kann. Bedenken Sie beispielsweise, dass die IP der Maschine 172.16.111.43 lautet und der Name der PAC-Datei proxy.pac lautet.

Wenn die IP-Adresse des eigentlichen Proxyservers 172.16.43.83 ist, der auf Port 8080 lauscht, lautet ein Beispiel für proxy.pac wie folgt:

```
function FindProxyForURL(url, host)
{
return “PROXY 172.16.43.83:8080”;
}
```

Die Proxy-PAC-URL lautet http://172.16.111.43/proxy.pac. Angenommen, die Datei wird auf Port HTTP-Port 80 gehostet.

Weitere Einzelheiten finden Sie unter https://support.citrix.com/article/CTX224235 oder Proxy-Autokonfiguration für Outbound-Proxy-Unterstützung für NetScaler Gateway.

Hinweis:

- Wenn Split Tunnel eingeschaltet ist, stellen Sie sicher, dass die IP-Adresse des Servers, der die PAC-Datei hostet, in die Liste der Intranet-Anwendungen aufgenommen wird, damit sie über VPN erreichbar ist.
- Nach der Anmeldung über Citrix Secure Access (macOS/iOS) beginnen die Browser, die Regeln aus der Proxy-PAC-Datei zu verwenden. Wenn wie im vorherigen Beispiel nur eine Proxy-Regel bereitgestellt wird, wird der gesamte HTTP- oder HTTPS-Verkehr an den internen Proxyserver weitergeleitet.

Citrix Secure Access für macOS-Benutzer einrichten

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Der Citrix Secure Access Client für macOS bietet eine erstklassige Lösung für Anwendungszugriff und Datenschutz, die von NetScaler Gateway angeboten wird. Sie können nun überall und jederzeit sicher auf wichtige Anwendungen, virtuelle Desktops und Unternehmensdaten zugreifen.
Citrix Secure Access ist der VPN-Client der nächsten Generation für NetScaler Gateway zum Erstellen und Verwalten von VPN-Verbindungen von macOS-Geräten aus. Citrix Secure Access wurde mit dem

Network Extension (NE) Framework von Apple erstellt. NE-Framework von Apple ist eine moderne Bibliothek, die APIs enthält, mit denen die Kernnetzwerkfunktionen von macOS angepasst und erweitert werden können. Die Netzwerkerweiterung mit Unterstützung für SSL VPN ist auf Geräten verfügbar, auf denen macOS 10.11+ ausgeführt wird.

Citrix Secure Access bietet vollständige Unterstützung für Mobile Device Management (MDM) unter macOS. Mit einem MDM-Server kann ein Administrator nun VPN-Profile auf Geräteebene und VPN-Profile per App konfigurieren und verwalten.
Citrix Secure Access für macOS kann von einem Mac App Store aus installiert werden.

Eine Liste der häufig verwendeten Funktionen, die vom Citrix Secure Access Client für macOS unterstützt werden, finden Sie unter NetScaler Gateway VPN-Clients und unterstützte Funktionen.

Kompatibilität mit MDM-Produkten

Citrix Secure Access für macOS ist mit den meisten MDM-Anbietern wie Citrix XenMobile, Microsoft Intune usw. kompatibel. Es unterstützt eine Funktion namens Network Access Control (NAC), mit der MDM-Administratoren die Konformität von Endbenutzergeräten erzwingen können, bevor sie eine Verbindung zu NetScaler Gateway herstellen. NAC auf Citrix Secure Access erfordert einen MDM-Server wie XenMobile und NetScaler Gateway. Weitere Informationen zu NAC finden Sie unter Konfigurieren des Geräts für die Netzwerkzugriffssteuerung. Überprüfen Sie den virtuellen NetScaler Gateway-Server für die Einzelfaktor-Anmeldung

> **Hinweis:**
>
> Um Citrix Secure Access mit NetScaler Gateway VPN ohne MDM zu verwenden, müssen Sie eine VPN-Konfiguration hinzufügen. Sie können die VPN-Konfiguration unter macOS von der Citrix Secure Access-Konfigurationsseite hinzufügen.

Konfigurieren eines von MDM verwalteten VPN-Profils für Citrix Secure Access

Im folgenden Abschnitt werden schrittweise Anweisungen zum Konfigurieren von geräteweiten und anwendungsspezifischen VPN-Profilen für Citrix Secure Access mit Citrix Endpoint Management (ehemals XenMobile) als Beispiel beschrieben. Andere MDM-Lösungen können dieses Dokument als Referenz für die Arbeit mit Citrix Secure Access verwenden.

> **Hinweis:**
>
> In diesem Abschnitt werden die Konfigurationsschritte für ein grundlegendes geräteweites und pro-App-VPN-Profil erläutert. Sie können auch On-Demand-Proxys konfigurieren, indem Sie der Dokumentation zu Citrix Endpoint Management (ehemals XenMobile) oder der MDM-VPN-Payload-Konfigurationvon Apple folgen.

VPN-Profile auf Geräteebene

VPN-Profile auf Geräteebene werden verwendet, um ein systemweites VPN einzurichten. Der Datenverkehr von allen Apps und Diensten wird basierend auf den in NetScaler definierten VPN-Richtlinien (wie Full-Tunnel, Split-Tunnel, Reverse Split-Tunnel) an NetScaler Gateway getunnelt.

So konfigurieren Sie ein VPN auf Geräteebene in Citrix Endpoint Management Führen Sie die folgenden Schritte aus, um ein VPN auf Geräteebene zu konfigurieren.

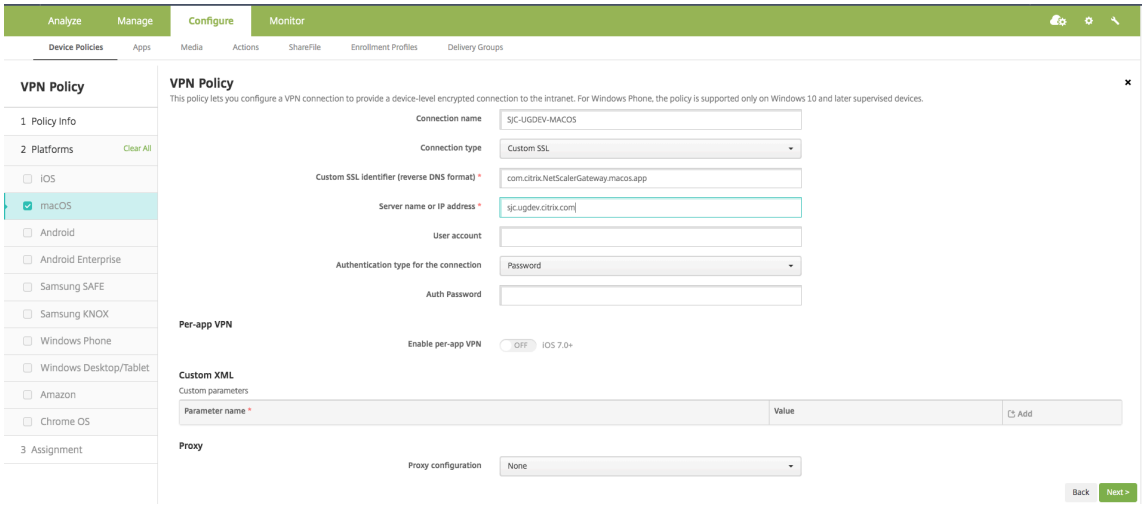
1. Navigieren Sie auf der Citrix Endpoint Management MDM-Konsole zu **Konfigurieren** > **Geräterichtlinien** > **Neue Richtlinie hinzufügen**.
2. Wählen Sie im linken Bereich Policy Platform **macOS** aus. Wählen Sie im rechten Bereich **VPN-Richtlinie** aus.
3. Geben Sie auf der Seite **Richtlinieninformationen** einen gültigen Richtliniennamen und eine Beschreibung ein und klicken Sie auf **Weiter**.
4. Geben Sie auf der **Richtliniendetailseite** für macOS einen gültigen Verbindungsnamen ein und wählen Sie **Benutzerdefiniertes SSL** unter **Verbindungstyp**.

   In der MDM-VPN-Nutzlast entspricht der Verbindungsname dem **UserDefinedName-Schlüssel** und der **VPN-Typschlüssel** muss auf **VPN**eingestellt sein.
5. Geben Sie unter **Benutzerdefinierte SSL-Kennung (umgekehrtes DNS-Format)com.citrix.netscalerGate** Dies ist die Bundle-ID für den Citrix Secure Access auf macOS.

   In der MDM-VPN-Nutzlast entspricht der Custom SSL Identifier dem Schlüssel **VPNSubtype**.
6. Geben Sie unter **Anbieter-Bundle-IDcom.citrix.netscalerGateway.macOS.App.VPNPlugin**ein. Dies ist die Paket-ID der Netzwerkerweiterung, die in der Binärdatei des Citrix Secure Access-Clients enthalten ist.

   In der MDM-VPN-Nutzlast entspricht die Anbieter-Bundle-ID dem **ProviderBundleIdentifier-Schlüssel**.
7. Geben Sie **unter Servername oder IP-Adresse** die IP-Adresse oder den FQDN des NetScaler ein, der dieser Citrix Endpoint Management-Instanz zugeordnet ist.

   Die verbleibenden Felder auf der Konfigurationsseite sind optional. Konfigurationen für diese Felder finden Sie in der Citrix Endpoint Management-Dokumentation.
8. Klicken Sie auf **Weiter**.



9. Klicken Sie auf **Speichern**.

Pro-App-VPN-Profile

Pro-App-VPN-Profile werden verwendet, um ein VPN für eine bestimmte Anwendung einzurichten. Der Datenverkehr nur von der bestimmten App wird zu NetScaler Gateway getunnelt. Die **VPN-Nutzlast pro App unterstützt alle** Schlüssel für geräteweites VPN sowie einige andere Schlüssel.

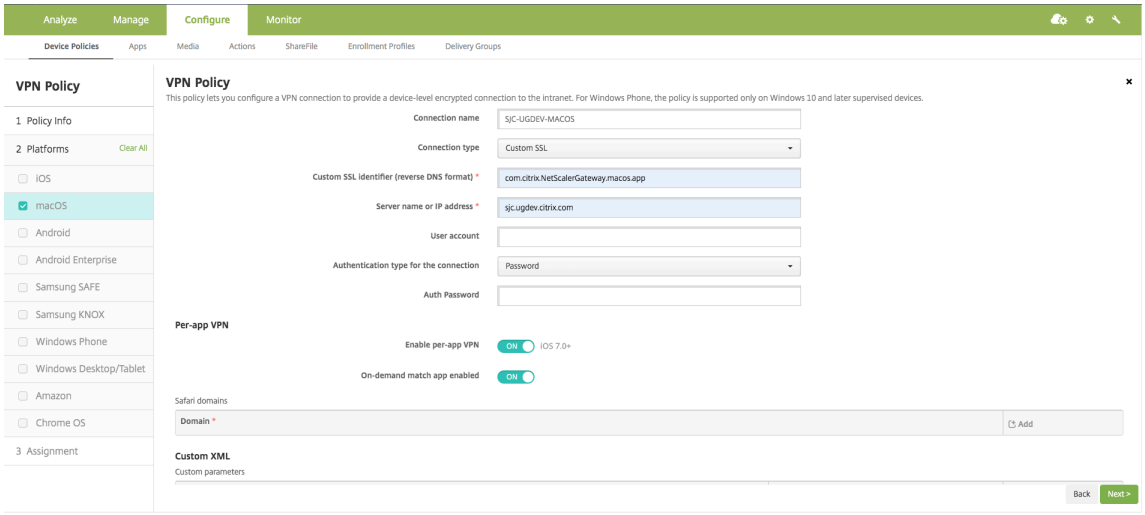
So konfigurieren Sie ein VPN auf App-Ebene auf Citrix Endpoint Management Führen Sie die folgenden Schritte aus, um ein Pro-App-VPN auf Citrix Endpoint Management zu konfigurieren:

1. Schließen Sie die VPN-Konfiguration auf Geräteebene in Citrix Endpoint Management ab.
2. Schalten Sie den Schalter **Pro-App-VPN aktivieren** im Abschnitt **Pro-App-VPN ein**.
3. Schalten Sie die **Option App für On-Demand-Match aktiviert** EIN, wenn Citrix Secure Access beim Start der Match-App automatisch gestartet werden muss. Dies wird für die meisten Per-App-Fälle empfohlen.

   In der MDM-VPN-Nutzlast entspricht dieses Feld dem Schlüssel **onDemandMatchAppEnabled**.
4. Die Konfiguration der Safari-Domain ist optional. Wenn eine Safari-Domäne konfiguriert ist, wird Citrix Secure Access automatisch gestartet, wenn Benutzer Safari starten und zu einer URL navigieren, die mit der URL im Feld **Domain** übereinstimmt. Dies wird nicht empfohlen, wenn Sie das VPN für eine bestimmte App einschränken möchten.

   In der MDM-VPN-Nutzlast entspricht dieses Feld den wichtigsten **SafariDomains**.

   Die verbleibenden Felder auf der Konfigurationsseite sind optional. Konfigurationen für diese Felder finden Sie in der Dokumentation zu Citrix Endpoint Management (ehemals XenMobile).



5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf **Speichern**.

   Um das VPN-Profil einer bestimmten App auf dem Gerät zuzuordnen, müssen Sie eine App-Inventarrichtlinie und eine Richtlinie für den Anbieter von Anmeldeinformationen erstellen, indem Sie diesem Handbuch folgen - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

Konfigurieren eines Split-Tunnels im Pro-App-VPN

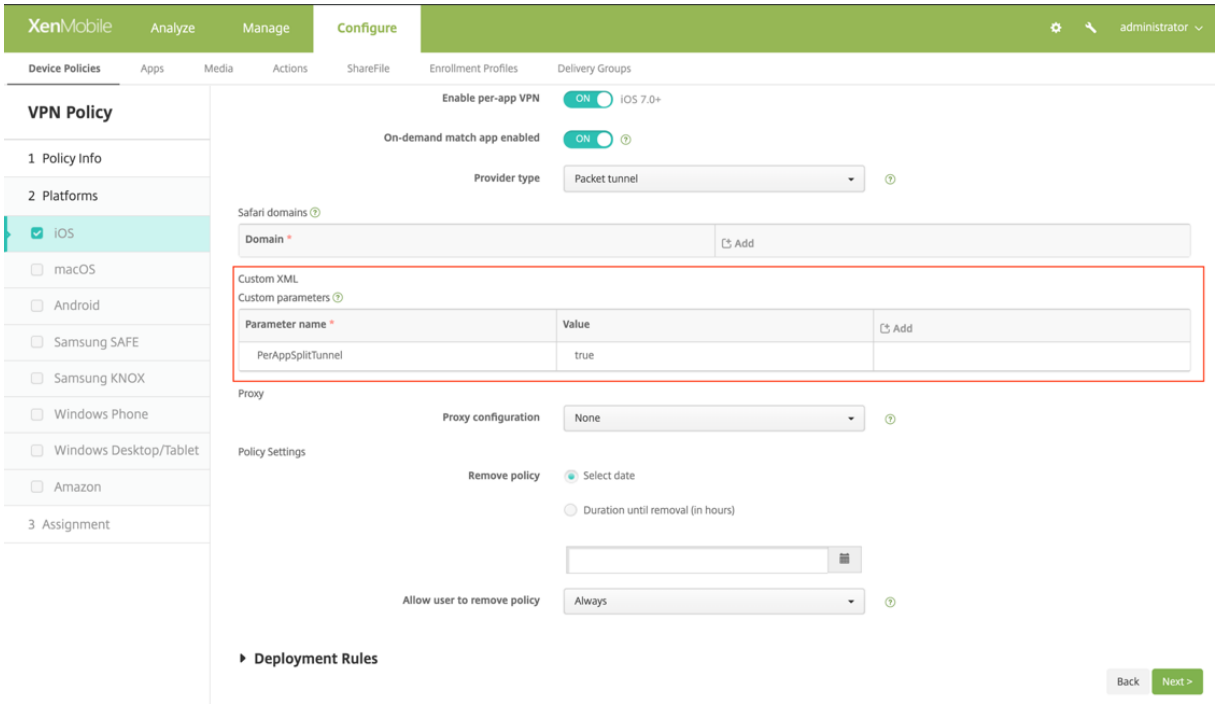
MDM-Kunden können den geteilten Tunnel in Pro-App-VPN für Citrix Secure Access konfigurieren. Das folgende Schlüssel/Wert-Paar muss dem Abschnitt zur Herstellerkonfiguration des auf dem MDM-Server erstellten VPN-Profils hinzugefügt werden.

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

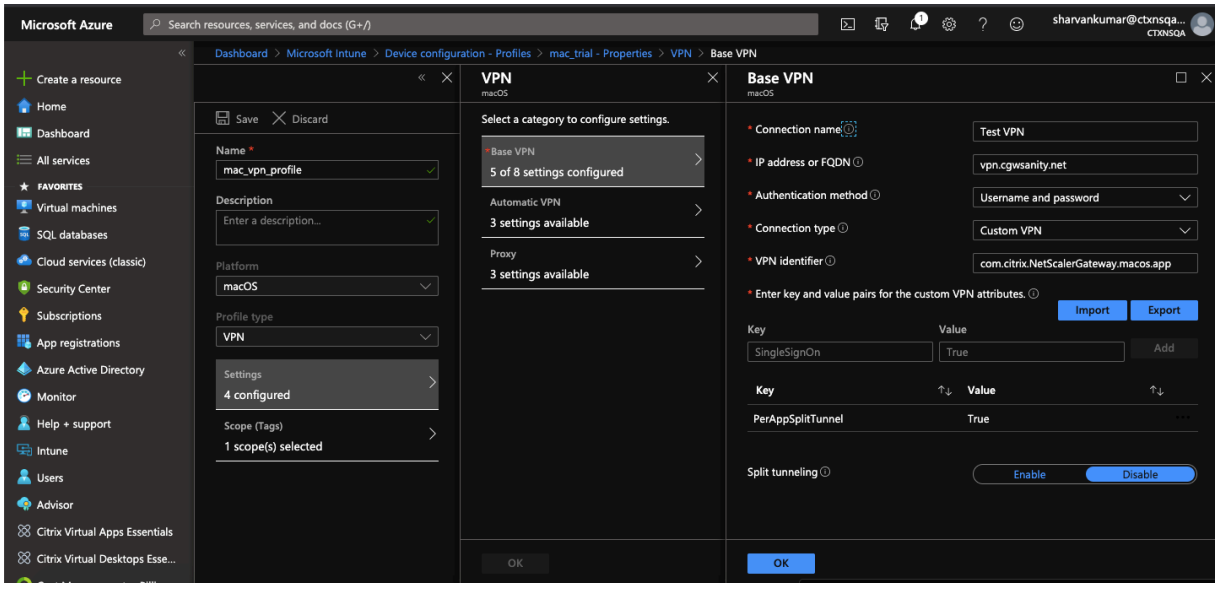
Der Schlüssel berücksichtigt die Groß-/Kleinschreibung und muss exakt übereinstimmen, während der Wert nicht zwischen Groß- und Kleinschreibung beachtet

> **Hinweis:**
>
> Die Benutzeroberfläche zum Konfigurieren der Anbieterkonfiguration ist bei den MDM-Anbietern nicht Standard. Wenden Sie sich an den MDM-Anbieter, um den Abschnitt zur Anbieterkonfiguration auf Ihrer MDM-Benutzerkonsole zu finden.

Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Citrix Endpoint Management.



Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Microsoft Intune.



Deaktivieren von Benutzern erstellten VPN-Profilen

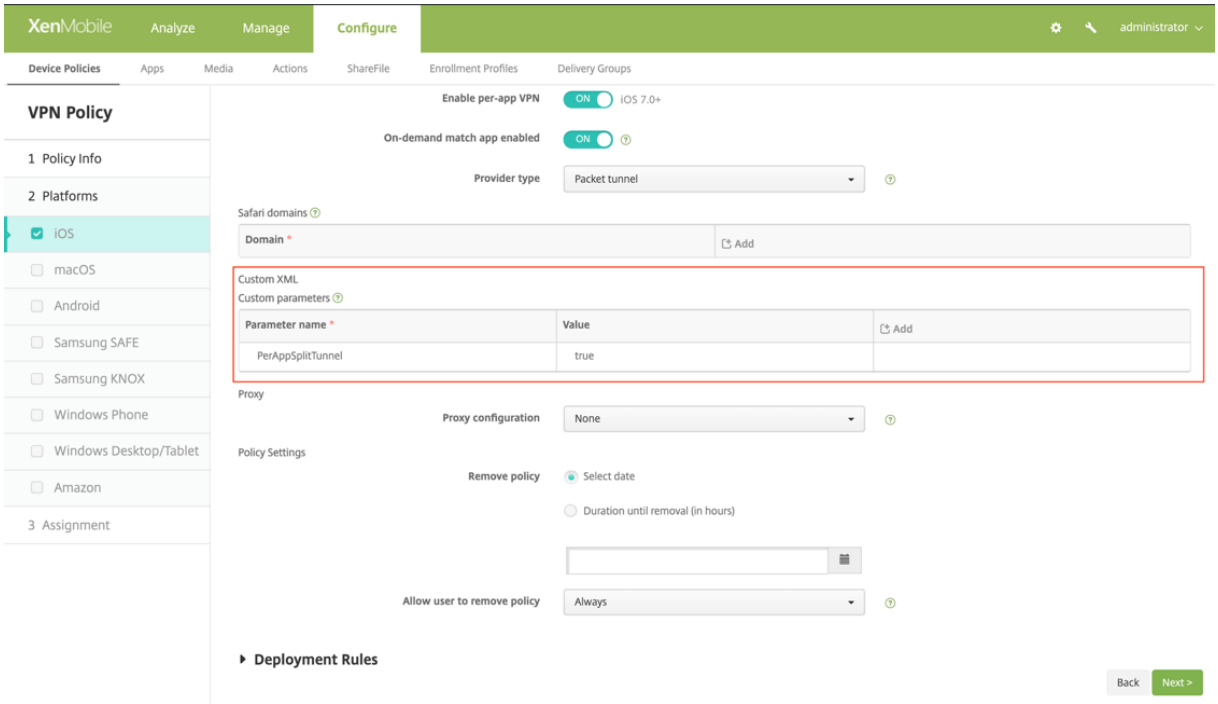
MDM-Kunden können verhindern, dass Benutzer VPN-Profile von Citrix Secure Access aus manuell erstellen. Dazu muss das folgende Schlüssel/Wert-Paar zum Abschnitt Herstellerkonfiguration des auf dem MDM-Server erstellten VPN-Profils hinzugefügt werden.


```
- Key = "disableUserProfiles"
- Value = "true or 1 or yes"
```

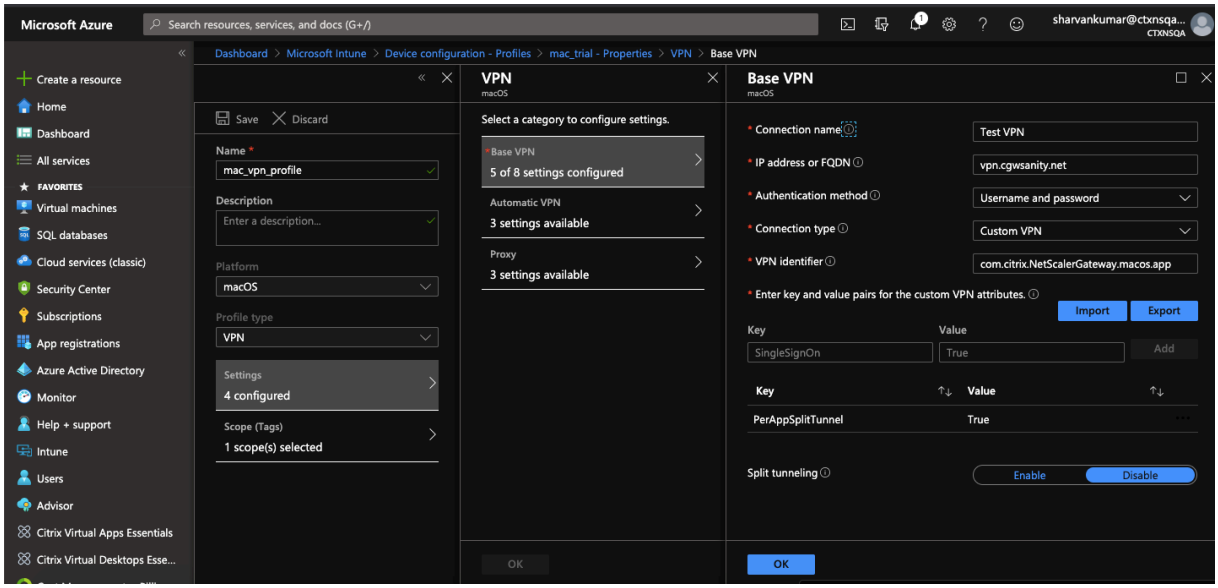
Der Schlüssel berücksichtigt die Groß-/Kleinschreibung und muss exakt übereinstimmen, während der Wert nicht zwischen Groß- und Kleinschreibung beachtet

> **Hinweis:**
>
> Die Benutzeroberfläche zum Konfigurieren der Anbieterkonfiguration ist bei allen MDM-Anbietern nicht Standard. Wenden Sie sich an den MDM-Anbieter, um den Abschnitt zur Anbieterkonfiguration auf Ihrer MDM-Benutzerkonsole zu finden.

Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Citrix Endpoint Management.



Das Folgende ist ein Beispiel für einen Screenshot der Konfiguration (herstellerspezifische Einstellungen) in Microsoft Intune.



DNS-Handhabung

Die empfohlenen DNS-Einstellungen für Citrix Secure Access lauten wie folgt:

- **DNS teilen > REMOTE**, wenn der geteilte Tunnel auf **AUS gestellt ist.**
- **DNS teilen > BEIDE**, wenn der geteilte Tunnel auf **ON**eingestellt ist. In diesem Fall müssen die Administratoren DNS-Suffixe für die Intranet-Domains hinzufügen. DNS-Abfragen für FQDNs, die zu DNS-Suffixen gehören, werden an die NetScaler Appliance getunnelt, und die verbleibenden Abfragen gehen an den lokalen Router.

> **Hinweis:**
>
> - Es wird empfohlen, dass das **DNS-Abkürzungsfix**-Flag immer **ON** ist. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX200243.
> - Wenn der Split-Tunnel auf **ON** eingestellt ist und Split-DNS auf **REMOTE**eingestellt ist, kann es zu Problemen bei der Lösung von DNS-Abfragen kommen, nachdem das VPN verbunden ist. Dies hängt damit zusammen, dass das Network Extension-Framework nicht alle DNS-Abfragen abfängt.

Unterstützte EPA-Scans

Eine vollständige Liste der unterstützten Scans finden Sie unter Neueste EPA-Bibliotheken.

1. Klicken Sie im Abschnitt **Unterstützte Scanmatrix von OPSWAT v4**unter der Spalte **MAC OS-spezifisch** auf **Liste der unterstützten Anwendungen**.

2. Klicken Sie in der Excel-Datei auf die Registerkarte **Klassische EPA-Scans**, um die Details anzuzeigen.

Bekannte Probleme

Im Folgenden sind die derzeit bekannten Probleme aufgeführt.

- Die EPA-Anmeldung schlägt fehl, wenn der Benutzer in die Quarantänegruppe aufgenommen wird.
- Warnmeldung für erzwungenes Timeout wird nicht angezeigt.
- Citrix Secure Access ermöglicht die Anmeldung, wenn der Split-Tunnel aktiviert ist und keine Intranet-Apps konfiguriert sind.

Einschränkungen

Im Folgenden sind die aktuellen Einschränkungen aufgeführt.

- Die folgenden EPA-Scans schlagen möglicherweise fehl, weil der Zugriff auf Secure Access aufgrund von Sandboxing eingeschränkt ist.
  - Festplattenverschlüsselung “Typ”und “Pfad”
  - Webbrowser “Standard”und “läuft”
  - Patch-Verwaltung “fehlende Patches”
  - Beenden Sie den Prozessbetrieb während EPA
- Split-Tunneling basierend auf Ports/Protokollen wird nicht unterstützt.
- Stellen Sie sicher, dass Sie nicht zwei Zertifikate mit demselben Namen und Ablaufdatum im Schlüsselbund haben, da der Client dadurch nur eines der Zertifikate anstelle von beiden anzeigt.

Problembehandlung

Wenn den Endbenutzern im Authentifizierungsfenster von Citrix Secure Access die Schaltfläche **EPA-Plug-in herunterladen** angezeigt wird, bedeutet dies, dass die Inhaltssicherheitsrichtlinie auf der NetScaler Appliance den Aufruf der URL `com.citrix.agmacepa://`blockiert. Die Administratoren müssen die Inhaltssicherheitsrichtlinie so ändern, dass `com.citrix.agmacepa://` zulässig ist.

nFactor-Unterstützung für den Citrix Secure Access-Client unter macOS/iOS

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Die Multi-Faktor-Authentifizierung (nFactor) erhöht die Sicherheit einer Anwendung, indem Benutzer mehrere Identifikationsnachweise vorlegen müssen, um Zugriff zu erhalten. Administratoren können verschiedene Authentifizierungsfaktoren konfigurieren, darunter Clientzertifikat, LDAP, RADIUS, OAuth, SAML usw. Diese Authentifizierungsfaktoren können in beliebiger Reihenfolge basierend auf den Anforderungen der Organisation konfiguriert werden.

Der Citrix Secure Access Client unter macOS/iOS unterstützt die folgenden Authentifizierungsprotokolle:

- **nFactor** —Das nFactor-Protokoll wird verwendet, wenn ein virtueller Authentifizierungsserver an den virtuellen VPN-Server auf dem Gateway gebunden ist. Da die Reihenfolge der Authentifizierungsfaktoren dynamisch ist, verwendet der Client eine Browserinstanz, die im Kontext der App gerendert wird, um die Authentifizierungs-GUI darzustellen.
- **Classic** —Classic-Protokoll ist das standardmäßige Fallback-Protokoll, das verwendet wird, wenn klassische Authentifizierungsrichtlinien auf dem virtuellen VPN-Server auf dem Gateway konfiguriert sind. Das klassische Protokoll ist das Fallback-Protokoll, wenn nFactor für bestimmte Authentifizierungsmethoden wie NAC ausfällt.
- **Citrix Identity Platform** —Das Citrix Identity Platform Protocol wird für die Authentifizierung bei CloudGateway oder Citrix Gateway Service verwendet und erfordert eine MDM-Registrierung bei Citrix Cloud.

In der folgenden Tabelle sind die verschiedenen Authentifizierungsmethoden zusammengefasst, die von jedem Protokoll unterstützt werden.

Authentifizierungsmethode	nFactor	Klassisch	Citrix IdP
Kunde Cert	Unterstützt	Unterstützt	Nicht unterstützt
LDAP	Unterstützt	Unterstützt	Nicht unterstützt
Lokal	Unterstützt	Unterstützt	Nicht unterstützt

Authentifizierungsmethode	nFactor	Klassisch	Citrix IdP
RADIUS	Unterstützt	Nicht unterstützt	Nicht unterstützt
SAML	Unterstützt	Nicht unterstützt	Nicht unterstützt
OAuth	Unterstützt	Nicht unterstützt	Nicht unterstützt
TACACS	Unterstützt	Nicht unterstützt	Nicht unterstützt
WebAuth	Unterstützt	Nicht unterstützt	Nicht unterstützt
Verhandeln	Unterstützt	Nicht unterstützt	Nicht unterstützt
EPA	Unterstützt	Unterstützt	Nicht unterstützt
NAC	Nicht unterstützt	Unterstützt	Nicht unterstützt
StoreFront	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
ADAL	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
DS-AUTH	Nicht unterstützt	Nicht unterstützt	Unterstützt

nFactor Konfiguration

Einzelheiten zur Konfiguration von nFactor finden Sie unter Konfigurieren der nFactor-Authentifizierung.

> **Wichtig:**
>
> Um das nFactor-Protokoll mit dem Citrix Secure Access-Client unter macOS/iOS zu verwenden, ist die empfohlene lokale NetScaler Gateway-Version 12.1.50.xx und höher.

Einschränkungen

- Mobilspezifische Authentifizierungsrichtlinien wie NAC (Network Access Control) erfordern, dass der Client im Rahmen der Authentifizierung mit NetScaler Gateway eine signierte Gerätekennung sendet. Die signierte Gerätekennung ist ein drehbarer geheimer Schlüssel, der ein mobiles Gerät eindeutig identifiziert, das in einer MDM-Umgebung registriert ist. Dieser Schlüssel ist in ein VPN-Profil eingebettet, das von einem MDM-Server verwaltet wird. Es ist möglicherweise nicht möglich, diesen Schlüssel in den WebView-Kontext zu injizieren. Wenn NAC in einem MDM-VPN-Profil aktiviert ist, greift der Citrix Secure Access Client unter macOS/iOS automatisch auf das klassische Authentifizierungsprotokoll zurück.
- Sie können NAC-Check nicht mit Intune für macOS konfigurieren, da Intune im Gegensatz zu iOS keine Option zur Aktivierung von NAC für macOS bietet.

Behebung häufiger Probleme mit Citrix Secure Access für macOS/iOS

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Probleme bei der DNS-Lösung

- Wenn das Gerät in den Ruhezustand geht oder längere Zeit inaktiv ist, kann es etwa 30—60 Sekunden dauern, bis das VPN wieder aufgenommen wird. Während dieser Zeit sehen Benutzer möglicherweise, dass einige DNS-Anfragen fehlschlagen. DNS-Anfragen werden nach kurzer Zeit automatisch aufgelöst.
  Wenn DNS-Abfragen nicht aufgelöst werden, ist es möglich, dass eine erweiterte Autorisierungsrichtlinie den DNS-Verkehr blockiert. Siehe https://support.citrix.com/article/CTX232237, um dieses Problem zu beheben.
- Überprüfen Sie immer die DNS-Auflösung von Browsern. DNS-Abfragen, die den `nslookup` Befehl vom Terminal verwenden, sind möglicherweise nicht korrekt. Wenn Sie den `nslookup` Befehl verwenden müssen, müssen Sie die Client-IP-Adresse in den Befehl aufnehmen. Zum Beispiel `nslookup website_name 172.16.255.1.`

EPA-Probleme

- Gatekeeper wird als Antivirenprogramm betrachtet. Wenn es einen Scan gibt, der nach "Antivirenprogrammen"sucht (MAC-ANTIVIR_0_0), wird der Scan immer erfolgreich, auch wenn der Benutzer kein Antivirenprogramm von anderen Anbietern installiert hat.

Hinweis:

- Aktivieren Sie die Client-Sicherheitsprotokolle, um Debug-Protokolle für EPA zu Sie können die Client-Sicherheitsprotokollierung aktivieren, indem Sie den VPN-Parameter `clientsecurityLog` auf ON setzen.
- Die integrierte Patch-Management-Software von Apple ist "Software-Update". Es entspricht der App "App Store"auf dem Gerät. Die Version des "Software-Updates"muss so sein `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- Halten Sie die EPA-Bibliotheken auf NetScaler immer auf dem neuesten Stand. Die neuesten Bibliotheken finden Sie unter https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html

nFactor Probleme

- Citrix Secure Access öffnet das **Citrix SSO**-Authentifizierungsfenster für die nFactor-Authentifizierung. Es ähnelt einem Browser. Wenn auf dieser Seite Fehler auftreten, kann dies durch die Authentifizierung in einem Webbrowser überprüft werden.
- Wenn die Übertragungsanmeldung fehlschlägt, wenn nFactor aktiviert ist, ändern Sie das Portal-Design auf "rfWebUI".
- Wenn Sie die Fehlermeldung "Eine sichere Verbindung zu NetScaler Gateway kann nicht hergestellt werden, da die Zertifikatskette keines der erforderlichen Zertifikate enthält. Bitte wenden Sie sich an Ihren Administrator"oder "Gateway nicht erreichbar", dann ist entweder das Gateway-Serverzertifikat abgelaufen oder das Serverzertifikat ist mit aktiviertem SNI gebunden. Citrix Secure Access unterstützt SNI noch nicht. Binden Sie das Serverzertifikat ohne aktiviertes SNI. Der Fehler kann auch auf das im MDM-VPN-Profil konfigurierte Zertifikat-Pinning und auf das von NetScaler Gateway vorgelegte Zertifikat zurückzuführen sein, das nicht mit dem angeheftete Zertifikat übereinstimmt.
- Wenn Sie versuchen, eine Verbindung zum Gateway herzustellen, wenn das **Citrix SSO Auth-Fenster** geöffnet wird, aber leer ist, prüfen Sie, ob die ECC-Kurve (ALL) an die Standardchiffergruppe gebunden ist. Die ECC-Kurve (ALL) muss an die Standard-Verschlüsselungsgruppe gebunden sein.

Überprüfung der Netzwerkzugriffssteuerung (NAC)

Die NAC-Authentifizierungsrichtlinie wird nur bei der klassischen Authentifizierung unterstützt. Es wird im Rahmen der nFactor-Authentifizierung nicht unterstützt.

Häufig gestellte Fragen

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für iOS heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

In diesem Abschnitt werden die häufig gestellten Fragen zu Citrix Secure Access für macOS/iOS zusammengefasst.

Wie unterscheidet sich der Citrix Secure Access Client für macOS/iOS von der VPN-App?
Der Citrix Secure Access Client für macOS und der Citrix Secure Access Client für iOS (früher bekannt

als Citrix SSO für iOS) sind der SSL-VPN-Client der nächsten Generation für NetScaler. Die App verwendet das Network Extension-Framework von Apple, um VPN-Verbindungen auf iOS- und macOS-Geräten herzustellen und zu verwalten. Citrix VPN ist der ältere VPN-Client, der die privaten VPN-APIs von Apple verwendet, die jetzt veraltet sind. Die Unterstützung für Citrix VPN ist im App Store nicht mehr verfügbar.

Was ist NE?
Das Network Extension (NE) -Framework von Apple ist eine moderne Bibliothek, die APIs enthält, mit denen die Kernnetzwerkfunktionen von iOS und macOS angepasst und erweitert werden können. Die Netzwerkerweiterung mit Unterstützung für SSL VPN ist auf Geräten mit iOS 9+ und macOS 10.11+ verfügbar.

Für welche Versionen von NetScaler ist der Citrix Secure Access Client für macOS/iOS kompatibel?
VPN-Funktionen im Citrix Secure Access Client für macOS/iOS werden in NetScaler Versionen 10.5 und höher unterstützt. Das TOTP ist auf NetScaler Version 12.0 und höher verfügbar. Push-Benachrichtigung auf NetScaler wurde noch nicht öffentlich angekündigt. Die App benötigt Versionen iOS 9+ und macOS 10.11+.

Wie funktioniert die CERT-basierte Authentifizierung für Nicht-MDM-Kunden?
Kunden, die zuvor Zertifikate per E-Mail oder Browser verteilt haben, um die Clientzertifikatauthentifizierung in VPN durchzuführen, müssen diese Änderung beachten, wenn sie den Citrix Secure Access Client für macOS/iOS verwenden. Dies gilt vor allem für Nicht-MDM-Kunden, die keinen MDM-Server zum Verteilen von Benutzerzertifikaten verwenden.

Was ist Network Access Control (NAC)? Wie konfiguriere ich NAC mit Citrix Secure Access für iOS und NetScaler Gateway?
MDM-Kunden von Microsoft Intune und Citrix Endpoint Management (ehemals XenMobile) können die Network Access Control (NAC) -Funktion in Citrix Secure Access für iOS nutzen. Mit NAC können Administratoren ihr internes Unternehmensnetzwerk sichern, indem sie eine zusätzliche Authentifizierungsebene für mobile Geräte hinzufügen, die von einem MDM-Server verwaltet werden. Administratoren können bei der Authentifizierung in Citrix Secure Access für iOS eine Gerätekompatibilitätsprüfung erzwingen.

Um NAC mit Citrix Secure Access für iOS zu verwenden, müssen Sie es sowohl auf dem NetScaler Gateway als auch auf dem MDM-Server aktivieren.

- Informationen zum Aktivieren von NAC auf NetScaler finden Sie unter Konfigurieren des Geräts für die Netzwerkzugriffssteuerung. Suchen Sie nach dem virtuellen NetScaler Gateway-Server für
- Wenn ein MDM-Anbieter Intune ist, lesen Sie Netzwerkzugriffssteuerung (NAC) -Integration mit Intune.

- Wenn ein MDM-Anbieter Citrix Endpoint Management (früher XenMobile) ist, lesen Sie Network Access Control.

  > **Hinweis:**
  >
  > Die unterstützte Mindestversion des Citrix Secure Access Clients für macOS/iOS ist 1.1.6 und höher.

Citrix Secure Access für Android

March 27, 2024

Citrix Secure Access (ehemals Citrix SSO) für Android bietet eine erstklassige Lösung für Anwendungszugriff und Datenschutz, die von NetScaler Gateway angeboten wird. Sie können nun überall und jederzeit sicher auf wichtige Anwendungen, virtuelle Desktops und Unternehmensdaten zugreifen.

> **Wichtig:**
>
> - Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.
> - Der Citrix Secure Access Client für Android funktioniert innerhalb des Android-Subsystems, das auf ChromeOS basiert. Es funktioniert mit ChromeOS, wenn es als Android-App aus dem Play Store installiert ist, und kann jede Anwendung innerhalb des Android-Subsystems tunneln.

Versionshinweise

March 27, 2024

> **Wichtig:**
>
> - Citrix SSO für Android wurde jetzt in Citrix Secure Access umbenannt. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln. Möglicherweise stellen Sie fest, dass in der Übergangszeit in der Dokumentation Citrix SSO-Referenzen verwendet werden.
> - FQDN-basiertes Split-Tunneling und nFactor-Authentifizierungsunterstützung befinden

> sich derzeit in der Vorschau
>
> - Citrix Secure Access wird für Android 6.x und niedrigere Versionen nach Juni 2020 nicht unterstützt.

In den Versionshinweisen zu Citrix Secure Access werden die neuen Funktionen, Verbesserungen vorhandener Funktionen, behobene Probleme und bekannte Probleme beschrieben, die in einem Service Release verfügbar sind. Die Versionshinweise enthalten einen oder mehrere der folgenden Abschnitte:

Was ist neu: Die neuen Funktionen und Verbesserungen, die in der aktuellen Version verfügbar sind.

Behobene Probleme: Die Probleme, die in der aktuellen Version behoben wurden.

Bekannte Probleme: Die in der aktuellen Version vorhandenen Probleme und deren Problemumgehungen, sofern zutreffend.

V23.12.2 (15. Dezember 2023)

> **Hinweis:**
>
> Citrix Secure Access für Android Version 23.12.2 enthält den Fix für CSACLIENTS-8799 und ersetzt Version 23.12.1.

[CSACLIENTS-8799]

Was ist neu

- **Citrix SSO für Android wurde in Citrix Secure Access umbenannt**

  Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

  [CSACLIENTS-6337]

- **Benachrichtigungen auf Geräten mit Android 13+ empfangen oder blockieren**

  Bei der Installation oder Neuinstallation des Citrix Secure Access Clients auf einem Android 13-Gerät werden Endbenutzer nun aufgefordert, Berechtigungen für den Empfang von Benachrichtigungen vom Citrix Secure Access Client anzugeben. Wenn Endbenutzer die Erlaubnis verweigern, erhalten sie weder VPN-Status- noch Pushbenachrichtigungen vom Citrix Secure Access Client auf ihren Android-Geräten. MDM-Administratoren wird empfohlen, Citrix Secure Access (Paket-ID: `com.citrix.CitrixVPN`) in ihrer Lösung die Benachrichtigungsberechtigung zu erteilen.

Endbenutzer können auf dem Android-Gerät zu **Einstellungen > Benachrichtigungen** navigieren, um die Benachrichtigungsberechtigung für
den Citrix Secure Access Client zu ändern. Einzelheiten finden Sie unter So verwenden Sie Citrix Secure Access von Ihrem Android-Gerät aus.

[CSACLIENTS-8252]

- **Unterstützung für Anmeldungsübertragung im Always-On-VPN-Modus**

  Citrix Secure Access für Android unterstützt jetzt die Funktion "Anmeldung übertragen"im Always-On-VPN-Modus. Einzelheiten zur Konfiguration der Anmeldungsübertragung finden Sie unter Seite "Anmeldung übertragen"konfigurieren.

  [CSACLIENTS-8305]

Behobene Probleme

Citrix Secure Access stürzt ab, wenn Benutzer den TOTP-Token (zeitbasiertes Einmalkennwort) auf das Gerät mit Android 13+ kopieren.

[CSACLIENTS-8799]

V23.10.2 (19. Dez. 2023)

Was ist neu

> **Hinweise:**
>
> - Citrix SSO für Android Version 23.10.2 enthält den Fix für CSACLIENTS-8314 und ersetzt Version 23.10.1.
> - Citrix SSO für Android 23.10.1 funktioniert mit Android 14.

- **Nach einem Ausfall der VPN-Verbindung erneut mit NetScaler Gateway authentifizieren —Vorschau**

  Citrix SSO für Android fordert Sie jetzt auf, sich erneut bei NetScaler Gateway zu authentifizieren, wenn eine VPN-Verbindung unterbrochen wird. Sie werden auf der Citrix SSO-Benutzeroberfläche und im Benachrichtigungsfeld Ihres Android-Geräts darüber informiert, dass die Verbindung zu NetScaler Gateway unterbrochen wurde und dass Sie sich erneut authentifizieren müssen, um die Verbindung wieder aufzunehmen. Dieses Feature ist als Preview verfügbar.

  Weitere Informationen finden Sie unter Wiederverbinden mit NetScaler Gateway nach einem VPN-Verbindungsfehler.

Behobene Probleme

Citrix SSO stürzt zeitweise ab, wenn der VPN-Dienst in bestimmten Always-On-VPN-Szenarien neu gestartet wird.

[CSACLIENTS-8314]

V23.8.1 (31. August 2023)

Was ist neu

- **Automatischer Neustart von Always On VPN**

  Die Citrix SSO-App startet das Always On VPN automatisch neu, wenn eine App, die Teil der Zulassungs- oder Blockierungsliste ist, in einem Arbeitsprofil oder einem Geräteprofil installiert wird. Der Datenverkehr dieser App wird automatisch über eine VPN-Verbindung getunnelt, ohne dass das Arbeitsprofil neu gestartet oder das Gerät neu gestartet werden muss. Um den automatischen Neustart von Always On VPN zu aktivieren, müssen Endbenutzer der Citrix SSO-App die Zustimmung „ Alle Pakete abfragen “erteilen. Weitere Informationen finden Sie unter Automatischer Neustart von Always On VPN.

  [CSACLIENTS-6158]

- **Debug-Protokollierung in einem verwalteten VPN-Profil aktivieren**

  MDM-Administratoren können jetzt die Debug-Protokollierung als benutzerdefinierten Parameter im verwalteten VPN-Profil der Endpoint Management-Konsole aktivieren. Um die Debug-Protokollierung zu aktivieren, `EnableDebugLogging` muss der Wert von auf True gesetzt werden. Wenn für eine der verwalteten VPN-Konfigurationen die Debug-Protokollierung aktiviert ist, wird die Debug-Protokollierungsfunktion wirksam, wenn die Konfigurationen analysiert werden. Weitere Informationen finden Sie unter Benutzerdefinierte Parameter für die Intune-Konfiguration.

  [CSACLIENTS-3746]

Behobene Probleme

- Manchmal kann die Citrix SSO-App den Datenverkehr zu einigen Ressourcen möglicherweise nicht tunneln. Dieses Problem tritt auf, wenn Split-Tunneling auf OFF gesetzt ist und einige nicht erreichbare Domänen oder IP-Adressen in ein Blackhole gesetzt sind.

  [NSHELP-35555]

V22.11.1 (30. November 2022)

Was ist neu

- **Citrix Secure Access wurde auf Android 12.1 (API-Level 32) aktualisiert**

  Citrix Secure Access wurde jetzt auf Android 12.1 (API-Level 32) aktualisiert. Bei einem Pro-App-VPN wird der VPN-Dienst möglicherweise nicht automatisch neu gestartet, wenn eines der Pakete in der Paketliste der Pro-App-VPNs nach der Einrichtung des VPN-Tunnels installiert wird. Dies ist auf die in Android 11 eingeführten Sichtbarkeitsbeschränkungen der App zurückzuführen. Einzelheiten finden Sie unter https://developer.android.com/training/package-visibility.

  [CGOP-21409]

V22.10.1 (21. Oktober 2022)

Was ist neu

- Die Anzeige der Versionsnummer der App wird auf das Format YY.MM.Point-Release aktualisiert, wobei YY die zweistellige Jahreszahl, MM der zweistellige Monat und Point-Release 1+ ist, abhängig von der Veröffentlichungsnummer innerhalb eines Monats.
- Die Datenerfassung von Google Analytics/Crashlytics aus der EU-Region ist für Android-Clients deaktiviert.

Behobene Probleme

- Fehlermeldungen, die für eine ungültige Eingabe in den Bildschirmen “Verbindung hinzufügen” und “Verbindung bearbeiten”angezeigt werden, sind nicht lokalisiert.

  [CGOP-22060]

V2.5.3 (05. Mai 2022)

Was ist neu

- Citrix SSO wurde auf das Android 11-Ziel-SDK aktualisiert (API 30)

  Die Citrix SSO-App wurde jetzt auf das Android 11-Ziel-SDK (API 30) aktualisiert. Diese Änderung erfordert, dass Microsoft Intune NAC v2-APIs von NetScaler Gateway für die Überprüfung der Gerätekonformität verwendet werden. Einzelheiten finden Sie im KB-Artikel https://support.citrix.com/article/CTX331615.

[CGOP-19774]

Behobene Probleme

- Manchmal verwendet Citrix SSO nach einer Netzwerkänderung möglicherweise keinen alternativen DNS-Server für die Hostnamensauflösung.

  [NSHELP-29378]

V2.5.2 (21. Oktober 2021)

Behobene Probleme

- Manchmal stürzt Citrix SSO ab, wenn ein Nichtkonformitätsfehler bei der NAC-Überprüfung behandelt wird.

  [CGOP-19198]

V2.5.1 (12. August 2021)

Behobene Probleme

- Die Citrix SSO-App kann den Host nicht auflösen, wenn die CNAME-Kette länger als 6 Hops ist.

  [CGOP-18475]

- Citrix SSO zeigt eine Authentifizierungsaufforderung an, wenn die Authentifizierung mit NAC-Prüfung von NetScaler Gateway erforderlich ist.

  [CGOP-18348]

- Citrix SSO kann bei der Verarbeitung ungewöhnlich großer ICMP-Pakete abstürzen.

  [CGOP-18286]

- Citrix SSO kann beim Hinzufügen eines VPN-Profils auf einigen Android 8.0-Geräten abstürzen.

  [CGOP-17607]

- Citrix SSO stürzt möglicherweise ab, wenn Sie das für Always On konfigurierte VPN neu starten.

  [CGOP-17580]

- Citrix SSO kann bei der Behandlung eines SSL-Fehlers im nFactor-Authentifizierungsablauf abstürzen.

  [CGOP-17577]

V2.5.0 (08-Juni-2021)

Was ist neu

- **Unterstützung für FQDN-basiertes Split-Tunneling**

  Citrix SSO für Android unterstützt jetzt FQDN-basiertes Split-Tunneling.

  [CGOP-12079]

Behobene Probleme

- Citrix SSO Preview Build 2.5.0 (110) kann keine Verbindung zu NetScaler Gateway-Versionen 12.1 und früher herstellen.

  [CGOP-17735]

- Die Einstellung "DisableUserProfiles"wird nach dem Neustart der SSO-App nicht angewendet.

  [CGOP-17454]

V2.4.16 (31-Mar-2021)

Behobene Probleme

- Die nFactor-Authentifizierung wird abgebrochen, wenn sicheres Surfen auf einigen Geräten nicht aktiviert ist.

  [CGOP-17514]

V2.4.15 (17-Mar-2021)

Behobene Probleme

- Manchmal verbindet Citrix SSO Always On VPN nicht erneut, wenn ein Sitzungstimeout auf der NetScaler Gateway-Appliance auftritt.

  [CGOP-16800]

V2.4.14 (23-Feb-2021)

Behobene Probleme

- Citrix SSO erfordert Benutzerinteraktion, wenn Always-On VPN mit Nur-Zertifikat-Authentifizierung zusammen mit nFactor-Authentifizierung verwendet wird.

[CGOP-16805]

- Manchmal kann Citrix SSO während des Neustarts oder Übergangs des VPN-Dienstes abstürzen.

  [CGOP-16766]

V2.4.13 (04-Feb-2021)

Behobene Probleme

- In einigen Fällen übertritt die Citrix SSO-Anmeldeanforderung ein Timeout, bevor NetScaler Gateway antwortet.

  [CGOP-16759]

V2.4.12 (15. Januar 2021)

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.4.11 (08-Jan-2021)

- Die klassische Authentifizierung schlägt fehl, da das Citrix SSO einen HTTP-Header (X-Citrix-Gateway) an das NetScaler Gateway sendet, der nur bei der nFactor-Authentifizierung verwendet wird.

  [CGOP-16449]

V2.4.10 (09-Dec-2020)

Behobene Probleme

- Manchmal schlägt die klassische Authentifizierung für Android-Geräte fehl.

  [CGOP-16219]

- Citrix SSO kann bei der Durchführung der klassischen Authentifizierung abstürzen.

  [CGOP-16012]

- Die Ausrichtung der Citrix SSO-App ändert sich nicht, wenn Sie das Gerät drehen.

  [CGOP-639]

V2.4.9 (20-Nov-2020)

Behobene Probleme

- Die Citrix SSO-App stürzt ab, wenn ein Benutzer auf den TOTP-Tokenwert auf dem Gerät tippt.

  [CGOP-15886]

V2.4.8 (04-Nov-2020)

Behobene Probleme

- Citrix SSO kann beim Trennen des VPN nach einem Sitzungstimeout auf dem Gateway abstürzen.

  [CGOP-15592]

V2.4.7 (12-Oct-2020)

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.4.6 (28-Sep-2020)

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.4.5 (16-Sep-2020)

Was ist neu

- Das neue NetScaler-Logo wird eingeführt.

  [CGOP-15327]

V2.4.4 (10-Sep-2020)

Behobene Probleme

- Manchmal stürzt Citrix SSO beim erneuten Verbinden der VPN-Sitzung ab.

  [CGOP-15215]

V2.4.3

Bekannte Probleme

- Citrix SSO kann keine VPN-Sitzung für NetScaler Gateway einrichten, wenn das Android-Gerät ressourcenbeschränkt ist.

  [NSHELP-24647]

V2.4.2

Behobene Probleme

- Die Citrix SSO-App stürzt ab, wenn zuvor gespeicherte beschädigte Token-Daten geladen werden. Mit diesem Fix wird der Token-Wert als "Token-Daten beschädigt"für beschädigte Token in der Token-Liste angezeigt. Entferne die beschädigten Token und füge sie erneut hinzu.

  [CGOP-14546]

V2.4.1

Behobene Probleme

- Die Citrix SSO-App wird für Android 6.x und niedrigere Versionen nach Juni 2020 nicht unterstützt.

  [CGOP-13853]

V2.3.19

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.3.18

Was ist neu

- Die Proxy-Konfiguration wird jetzt in der Android Citrix SSO-App für Android 10-Geräte unterstützt.

  [CGOP-12007]

V2.3.17

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.3.16

In diesem Release wurden verschiedene Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

V2.3.15

Was ist neu

- Die Citrix SSO-App unterstützt jetzt das Anheften von NetScaler Gateway-Zertifikaten für verwaltete VPN-Profile.

  [CGOP-12538]

- Die Citrix SSO-App für Android 10 erkennt jetzt Always On VPN aus den Systemeinstellungen.

  [CGOP-12656]

Behobene Probleme

- Die Citrix SSO-App stürzt beim Trennen der Verbindung zum VPN ab, wenn nur MDM-VPN-Profile definiert sind.

  [CGOP-13825]

V2.3.14

Was ist neu

- Die Citrix SSO-App kann jetzt die Benutzerauthentifizierung im Auftrag der Citrix Workspace-App für die native einmalige Anmeldung der App durchführen.

  [CGOP-12083]

- Der VPN-Dienst wird neu gestartet, wenn eines der Pakete in der Pro-App-VPN-Paketliste nach der Einrichtung des VPN-Tunnels installiert wird.

  [CGOP-11262]

Behobene Probleme

- Citrix SSO verarbeitet die endgültige Meldung zum Aufbau einer VPN-Sitzung jetzt korrekt.

  [CGOP-12488]

- Die NetScaler Gateway IP-Adresse wird jetzt nur einmal aufgelöst. Zuvor wurde die NetScaler Gateway-IP-Adresse mehrmals aufgelöst, was manchmal zu Verbindungsfehlern führte.

  [CGOP-12101]

Bekannte Probleme

- Der Always-On VPN-Status wird in der App-Benutzeroberfläche nicht immer korrekt aktualisiert.

  [NSHELP-21709]

V2.3.13

Behobene Probleme

- Die NetScaler Gateway IP-Adresse wird jetzt nur einmal aufgelöst.

  Zuvor wurde die NetScaler Gateway-IP-Adresse mehrmals aufgelöst, was manchmal zu Verbindungsfehlern führte.

  [CGOP-12101]

Bekannte Probleme

- Der Always-On VPN-Status wird in der App-Benutzeroberfläche nicht immer korrekt aktualisiert.

  [NSHELP-21709]

V2.3.12

Behobene Probleme

- Citrix SSO kann beim Speichern eines VPN-Profils abstürzen.

  [CGOP-12137]

V2.3.11

Behobene Probleme

- Citrix SSO kann beim Speichern eines VPN-Profils abstürzen.

  [CGOP-12137]

- Die Einstellung disableUserProfile wird in der Benutzeroberfläche nicht korrekt wiedergegeben, wenn ein neues VPN-Profil oder eine Aktualisierung eines vorhandenen Profils zur Änderung des disableUserProfile-Werts führt.

  [CGOP-11899]

- Citrix SSO für Android verarbeitet keine VPN-Profile im Modus Gerätebesitzer (DO).

  [CGOP-11981]

- Eine VPN-Verbindung wird nicht hergestellt, wenn es nur lokale IPv6-DNS-Server gibt.

  [CGOP-12053]

V2.3.10

Behobene Probleme

- Die VPN-Verbindung ging nach einiger Leerlaufzeit auf dem Gerät verloren.

  [CGOP-11381]

V2.3.8

Was ist neu

- **Einrichten der Citrix SSO-App in einer Intune Android Enterprise-Umgebung**

  Sie können jetzt die Citrix SSO-App in einer Intune Android Enterprise-Umgebung einrichten. Einzelheiten finden Sie unter Einrichten der Citrix SSO-App in einer Intune Android Enterprise-Umgebung.

  [CGOP-635]

- **Unterstützung für die Bereitstellung von VPN-Profilen über Android Enterprise**

  Die Bereitstellung von VPN-Profilen über Android Enterprise wird jetzt unterstützt.

  [CGOP-631]

Behobene Probleme

- Wenn Sie ein bereits gespeichertes Token speichern und dann versuchen, es zu öffnen, erscheinen verstümmelte Zeichen im Token-Namen.

  [CGOP-11696]

- Die Citrix SSO-App kann keine VPN-Sitzung einrichten, wenn auf NetScaler Gateway keine DNS-Suchdomänen konfiguriert sind.

  [CGOP-11259]

V2.3.6

Was ist neu

- **Always On Unterstützung für Citrix SSO**

  Die Always On Funktion von Citrix SSO stellt sicher, dass Benutzer immer mit dem Unternehmensnetzwerk verbunden sind. Diese dauerhafte VPN-Konnektivität wird durch die automatische Einrichtung eines VPN-Tunnels erreicht.

  [CGOP-10015]

- **Eine Benachrichtigung zur erneuten Anmeldung wird angezeigt, wenn der Ablauf des Athena-Tokens eine Abmeldung verursacht**

  Eine Benachrichtigung, in der die Benutzer aufgefordert werden, sich erneut bei Citrix Workspace anzumelden, wird angezeigt, wenn die folgenden Bedingungen erfüllt sind.

  - Die Funktion Always On ist im von Citrix Workspace bereitgestellten VPN-Profil aktiviert
  - Die Athena-Authentifizierung wird für SSO verwendet
  - Der Benutzer ist aufgrund des Ablaufs des Athena-Tokens von der Citrix Workspace-App abgemeldet

  [CGOP-10016]

- **Die Registrierung für den Push-Benachrichtigungsdienst erfolgt mit NetScaler Gateway**

  Sie können sich jetzt mit dem NetScaler Gateway-Gerät für den Push-Benachrichtigungsdienst registrieren. Früher erfolgte die Registrierung auf dem Clientgerät.

  [CGOP-10542]

Behobene Probleme

Manchmal stürzt Citrix SSO ab, wenn ein neues Token gescannt wird. Beispielsweise stürzt Citrix SSO ab, wenn ein vorhandenes Token gelöscht und ein anderes mit demselben Tokennamen gescannt wird.

[CGOP-10818]

V2.3.1

Was ist neu

- **Verwaltete Konfigurationen werden aktualisiert, um mehr Benutzereinstellungen einzuschließen**

  Verwaltete Konfigurationen werden aktualisiert, um die Einstellungen "BlockUntrusted-Servers", "DefaultProfileName"und "DisableUserProfiles"für Android Enterprise-Umgebungen einzuschließen.

  [CGOP-10033]

- **Verbesserte Unterstützung von Push-**

  Bei der Konfiguration von NetScaler Gateway für Push-Benachrichtigung mit dem Typ "OTP"wird PIN/Fingerprint nicht gefragt, nachdem der Benutzer als Antwort auf die Push-Benachrichtigung "Zulassen"ausgewählt hat, in der die Zustimmung des Benutzers zum Fortfahren der Authentifizierung angefordert wird.

  [CGOP-9843]

- **Unterstützung von Firebase Analytics**

  Unterstützung für grundlegende Firebase Analytics wurde hinzugefügt, um Nutzungsinformationen zur Citrix SSO-App bereitzustellen. Die Verbesserung gilt für grobe Geolokalisierungen, Bildschirmnutzung, verschiedene Versionen von Android, die verwendet werden und so weiter.

  [CGOP-7523]

- **Unterstützung für Android Managed Configurations basierte VPN-Profilkonfiguration**

  Die Citrix SSO-App kann in der Android Enterprise-Umgebung mit einem EMM/UEM-Anbieter wie Citrix Endpoint Management konfiguriert werden. Der Assistent für verwaltete Android Enterprise-Konfigurationen in CEM kann verwendet werden, um verwaltete VPN-Konfigurationen für die Citrix SSO-App bereitzustellen. Informationen zur Konfiguration der Citrix SSO-App mithilfe verwalteter Konfigurationen finden Sie unter VPN-Geräterichtlinie.

V2.2.9

Was ist neu

- **Unterstützung für Push-Benachrichtigungen**

  NetScaler Gateway sendet eine Push-Benachrichtigung auf Ihrem registrierten Mobilgerät für eine vereinfachte Zwei-Faktor-Authentifizierung.

  [CGOP-9592]

Behobene Probleme

- Nicht-URL-Zeichen sind im Feld Server unter dem Bildschirm Verbindung hinzufügen zulässig.

  [CGOP-588]

Citrix Secure Access in einer MDM-Umgebung einrichten

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Informationen zum Einrichten von Citrix Secure Access in einer MDM-Umgebung finden Sie unter Citrix Secure Access-Protokoll für Android konfigurieren.

> **Hinweise:**
>
> - In einer Nicht-MDM-Umgebung erstellen Benutzer VPN-Profile manuell.
> - Sie können auch eine von Android Enterprise verwaltete Konfiguration für Citrix Secure Access erstellen. Einzelheiten finden Sie unter Konfigurieren von VPN-Profilen für Android Enterprise.
> - Für Benutzer von Android 13+, die Citrix Secure Access 23.12.1 und höher verwenden, wird MDM-Administratoren empfohlen, Citrix Secure Access (Paket-ID: `com.citrix.CitrixVPN`) in ihrer Lösung die Benachrichtigungsberechtigung zu gewähren.

Citrix Secure Access in einer Intune Android Enterprise-Umgebung einrichten

March 27, 2024

> **Wichtig:**
>
> Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Das Thema enthält Details zur Bereitstellung und Konfiguration von Citrix Secure Access über Microsoft Intune. In diesem Dokument wird davon ausgegangen, dass Intune bereits für die Unterstützung von Android Enterprise konfiguriert ist und die Gerätereregistrierung bereits abgeschlossen ist.

Voraussetzungen

- Intune ist für Android Enterprise Support konfiguriert
- Die Gerätereregistrierung ist abgeschlossen

So richten Sie Citrix Secure Access in einer Intune Android Enterprise-Umgebung ein

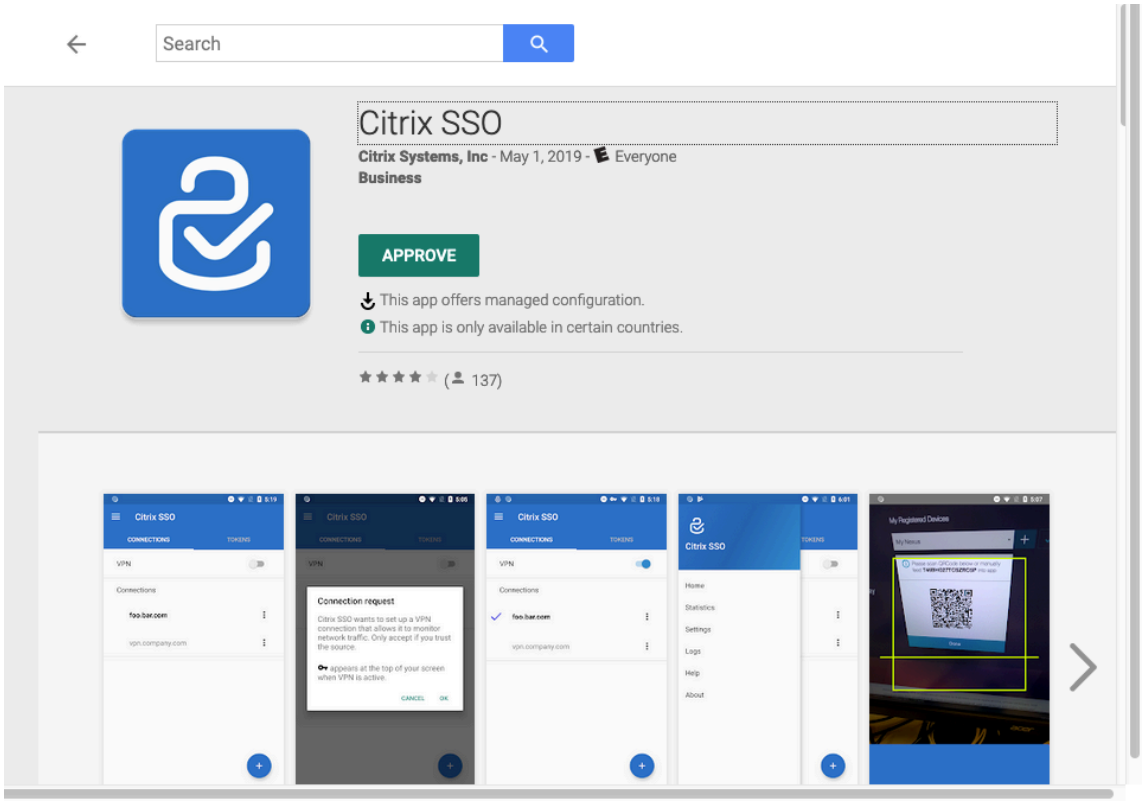
- Citrix Secure Access als verwaltete App hinzufügen
- Richtlinie für verwaltete Apps für Citrix Secure Access konfigurieren

Citrix Secure Access als verwaltete App hinzufügen

1. Melden Sie sich an Ihrem Azure-Portal an.
2. Klicken Sie im linken Navigationsblatt auf **Intune**.
3. Klicken Sie im Microsoft Intune-Blade auf **Client-Apps** und dann im Blade der Client-Apps auf Apps.
4. Klicken Sie in den Menüoptionen oben rechts auf **+Link hinzufügen**. Das Blade App-Konfiguration hinzufügen wird angezeigt.
5. Wählen Sie **Managed Google Play** für den App-Typ aus.

   Dadurch wird die Google Play-Suche verwalten und Blade genehmigen hinzugefügt, wenn Sie Android Enterprise konfiguriert haben.

6. Suchen Sie nach Citrix Secure Access und wählen Sie es aus der Liste der Apps aus.



Hinweis: Wenn Citrix Secure Access nicht in der Liste angezeigt wird, bedeutet dies, dass die App in Ihrem Land nicht verfügbar ist.

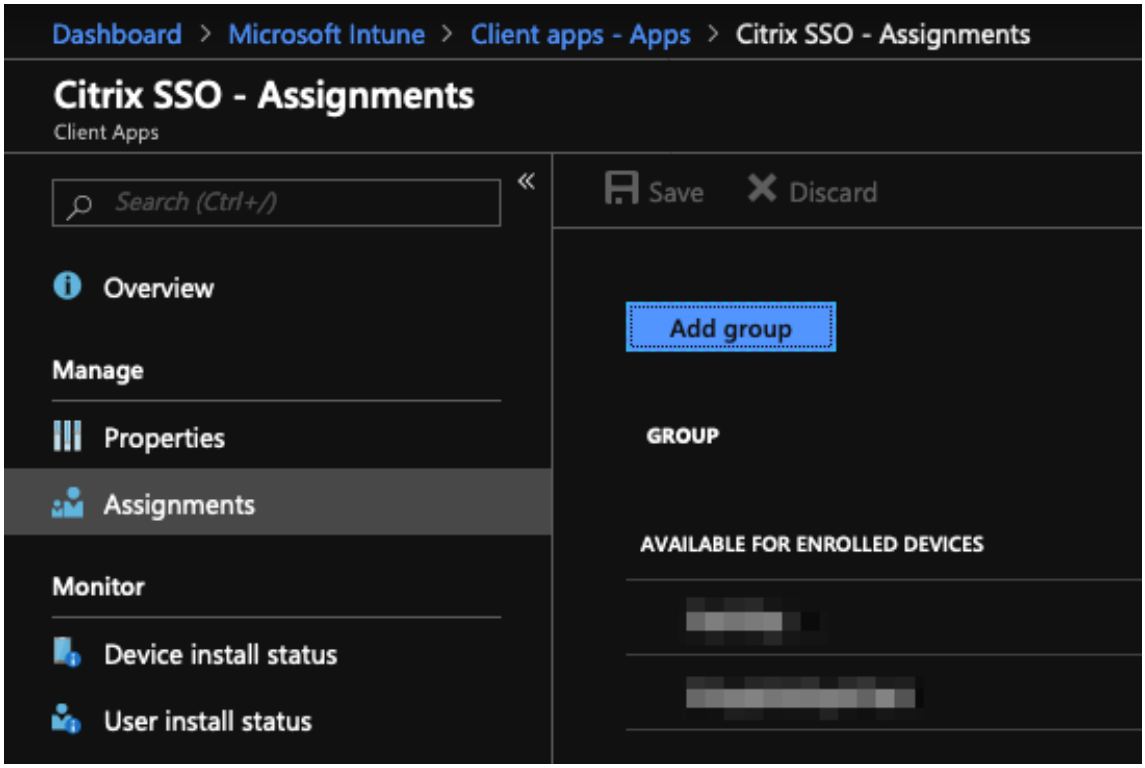
7. Klicken Sie auf **GENEHMIGEN**, um Citrix Secure Access für die Bereitstellung über den verwalteten Google Play Store zu genehmigen.

   Die Berechtigungen, die für Citrix Secure Access erforderlich sind, sind aufgeführt.

8. Klicken Sie auf **GENEHMIGEN**, um die App für die Bereitstellung zu genehmigen.
9. Klicken Sie auf **Sync**, um diese Auswahl mit Intune zu synchronisieren.

   Citrix Secure Access wird der Liste der Client-Apps hinzugefügt. Möglicherweise müssen Sie nach Citrix Secure Access suchen, wenn viele Apps hinzugefügt wurden.

10. Klicken Sie auf die App **Citrix Secure Access**, um das Blatt mit den App-Details zu öffnen.
11. Klicken Sie im Details-Blade auf **Zuweisungen**. Das Blatt **Citrix Secure Access —Assignments** wird angezeigt.



12. Klicken Sie auf **Gruppe hinzufügen**, um die Benutzergruppen zuzuweisen, denen Sie die Berechtigung zur Installation von Citrix Secure Access erteilen möchten, und klicken Sie auf **Speichern**.
13. Schließen Sie das Citrix Secure Access-Detailblatt.

Citrix Secure Access wird hinzugefügt und für die Bereitstellung für Ihre Benutzer aktiviert.

Richtlinie für verwaltete Apps für Citrix Secure Access konfigurieren

Nachdem Citrix Secure Access hinzugefügt wurde, müssen Sie eine verwaltete Konfigurationsrichtlinie für Citrix Secure Access erstellen, damit das VPN-Profil für Citrix Secure Access auf dem Gerät bereitgestellt werden kann.

1. Öffnen Sie das **Intune-Blade** in Ihrem Azure-Portal.
2. Öffnen Sie das **Client-Apps-Blade** vom Intune-Blade aus.
3. Wählen Sie im Blade für Client-Apps das Element **App-Konfigurationsrichtlinien** aus und klicken Sie auf **Hinzufügen**, um das Blade für **Konfigurationsrichtlinien** zu öffnen.
4. Geben Sie einen Namen für die Richtlinie ein und fügen Sie eine Beschreibung dafür hinzu.
5. Wählen Sie unter **Geräteregistrierungstyp** die Option **Verwaltete Geräte** aus.
6. Wählen Sie unter **Plattform** die Option **Android** aus.

Dadurch wird eine weitere Konfigurationsoption für die zugehörige App hinzugefügt.

7. Klicken Sie auf **Zugeordnete App** und wählen Sie die App **Citrix Secure Access** aus.

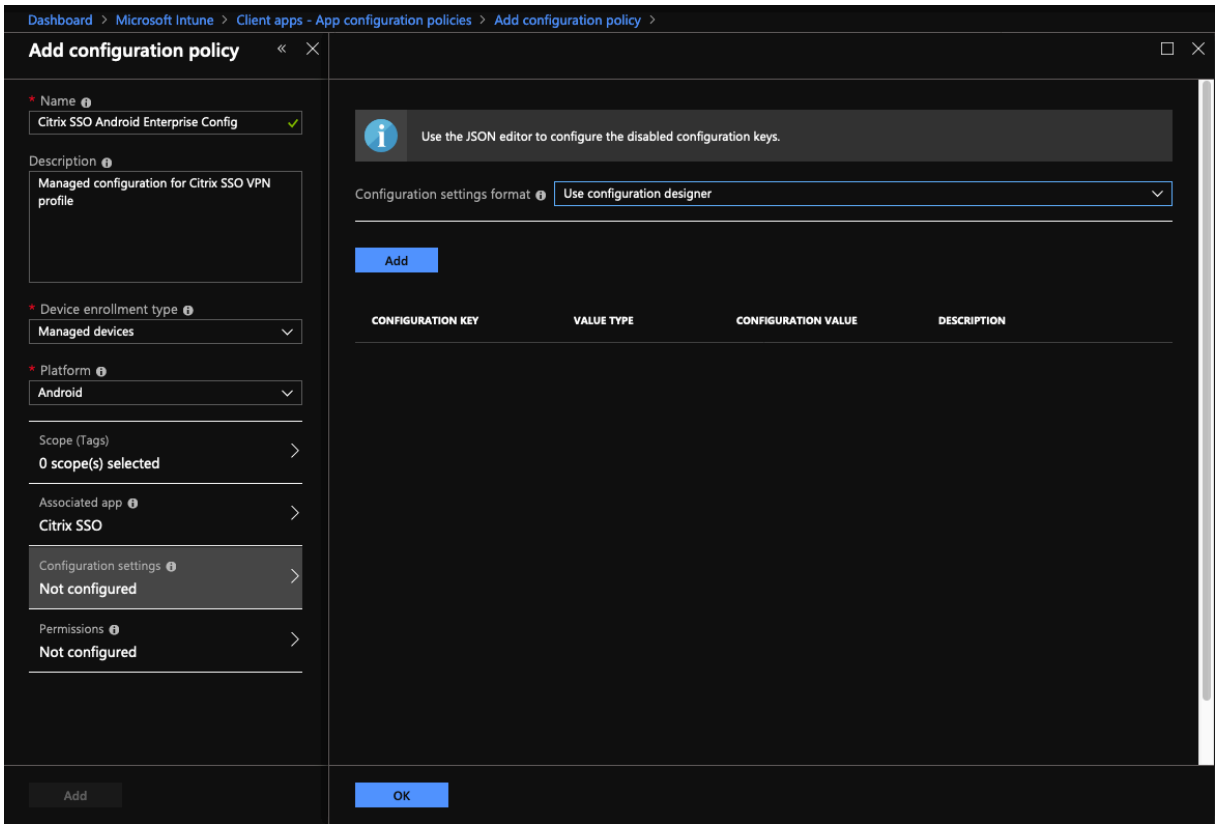
   Möglicherweise müssen Sie danach suchen, wenn Sie viele Apps haben.

8. Klicken Sie auf **OK**. Eine Option für Konfigurationseinstellungen wird im Blade für Konfigurationsrichtlinien hinzufügen hinzugefügt.

9. Klicken Sie auf **Konfigurationseinstellungen**.

   Ein Blatt zur Konfiguration von Citrix Secure Access wird angezeigt.

10. Wählen Sie in den **Konfigurationseinstellungen** entweder **Konfigurationsdesigner verwenden** oder **Geben Sie JSON-Daten** ein, um Citrix Secure Access zu konfigurieren.



> **Hinweis:**
>
> Für einfache VPN-Konfigurationen wird empfohlen, den Konfigurationsdesigner zu verwenden.

VPN-Konfiguration mit dem Konfigurationsdesigner

1. Wählen Sie in den **Konfigurationseinstellungen** die Option **Konfigurationsdesigner verwenden** aus und klicken Sie auf **Hinzufügen**.

Es wird ein Fenster zur Eingabe von Schlüsselwerten angezeigt, in dem Sie verschiedene Eigenschaften konfigurieren können, die von Citrix Secure Access unterstützt werden. Sie müssen mindestens die Eigenschaften **Serveradresse** und **VPN-Profilname** konfigurieren. Sie können den Mauszeiger über den Abschnitt **BESCHREIBUNG** bewegen, um weitere Informationen zu jeder Eigenschaft zu erhalten.

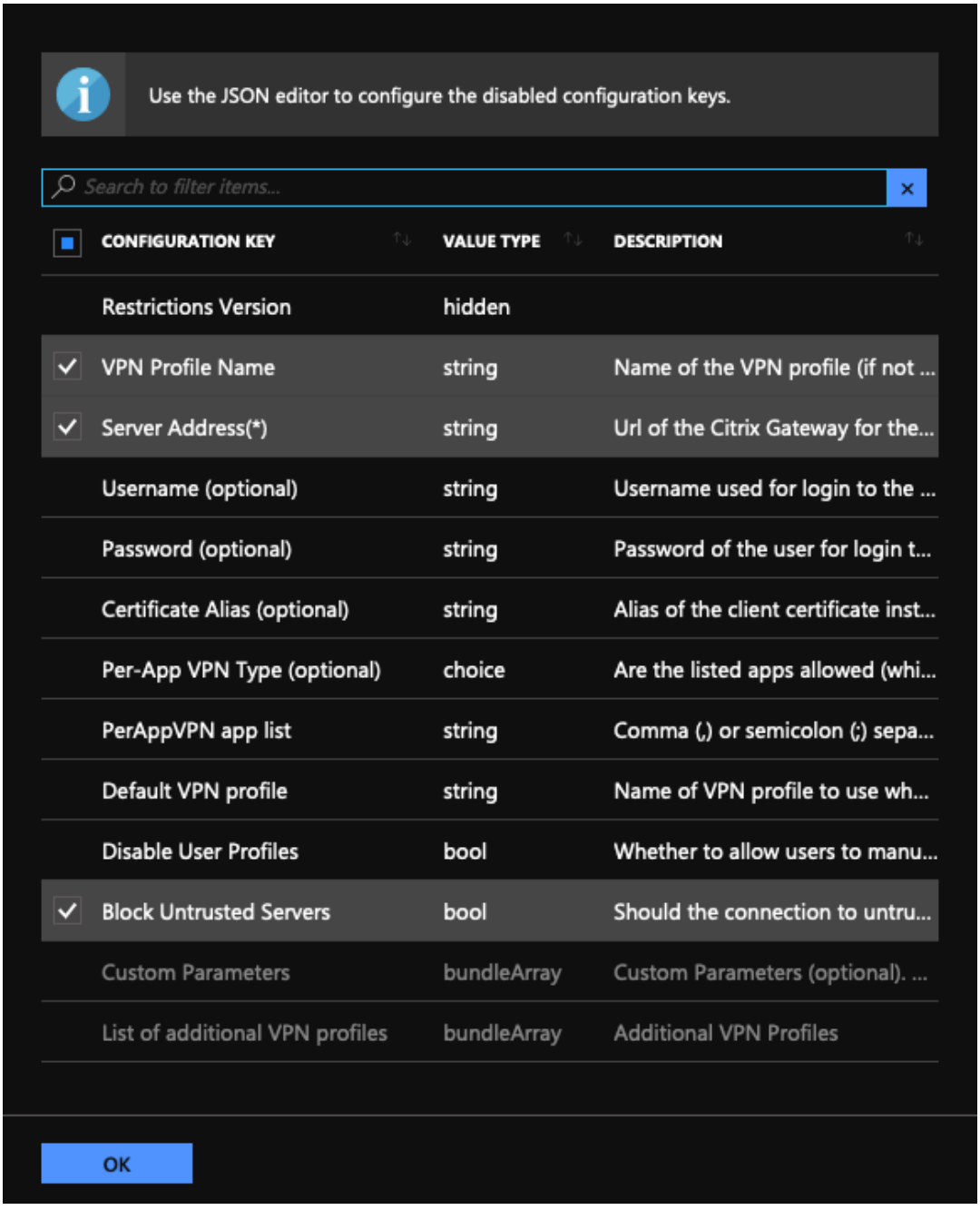
2. Wählen Sie beispielsweise Eigenschaften für **VPN-Profilname** und **Serveradresse (*)** aus und klicken Sie auf **OK**.

   Dadurch werden die Eigenschaften zum Konfigurationsdesigner hinzugefügt. Sie können die folgenden Eigenschaften konfigurieren.

   - **VPN-Profilname**. Geben Sie einen Namen für das VPN-Profil ein. Wenn Sie mehrere VPN-Profile erstellen, verwenden Sie für jedes Profil einen eindeutigen Namen. Wenn Sie keinen Namen angeben, wird die Adresse, die Sie in das Feld Serveradresse eingeben, als VPN-Profilname verwendet.
   - **Serveradresse (*)**. Geben Sie Ihren NetScaler Gateway Basis-FQDN ein. Geben Sie auch den NetScaler Gateway-Port ein, wenn Sie nicht Port 443 verwenden. Verwenden Sie das URL-Format. Beispiel: `https://vpn.mycompany.com:8443`.
   - **Benutzername (optional)**. Geben Sie den Benutzernamen ein, den die Endbenutzer zur Authentifizierung beim NetScaler Gateway verwenden. Sie können den Intune-Konfigurationswerttoken für dieses Feld verwenden, wenn das Gateway für die Verwendung konfiguriert ist (siehe Konfigurationswerttoken). Wenn Sie keinen Benutzernamen angeben, werden Benutzer aufgefordert, einen Benutzernamen anzugeben, wenn sie eine Verbindung zu NetScaler Gateway herstellen.
   - **Kennwort (optional)**. Geben Sie das Kennwort ein, mit dem Endbenutzer sich beim NetScaler Gateway authentifizieren. Wenn Sie kein Kennwort angeben, werden Benutzer aufgefordert, ein Kennwort anzugeben, wenn sie eine Verbindung zu NetScaler Gateway herstellen.
   - **Zertifikat-Alias (optional)**. Geben Sie im Android KeyStore einen Zertifikatsalias an, der für die Authentifizierung von Clientzertifikaten verwendet werden soll. Dieses Zertifikat ist für Benutzer vorausgewählt, wenn Sie zertifikatbasierte Authentifizierung verwenden.
   - **Gateway-Zertifikat-Pins (optional)**. JSON-Objekt, das für NetScaler Gateway verwendete Zertifikat-Pins beschreibt. Beispielwert: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Einzelheiten finden Sie unter NetScaler Gateway-Zertifikatpinning mit Android Citrix Secure Access.
   - **Pro-App-VPN-Typ (optional)**. Wenn Sie ein Pro-App-VPN verwenden, um einzuschränken, welche Apps dieses VPN verwenden, können Sie diese Einstellung konfigurieren.

  - Wenn Sie **Zulassen** auswählen, wird der Netzwerkverkehr für App-Paketnamen, die in der PerAppVPN-App-Liste aufgeführt sind, über das VPN geleitet. Der Netzwerkverkehr aller anderen Apps wird nicht über das VPN geleitet.
  - Wenn Sie **Verbieten** auswählen, wird der Netzwerkverkehr für App-Paketnamen, die in der PerAppVPN-App-Liste aufgeführt sind, außerhalb des VPN geleitet. Der Netzwerkverkehr aller anderen Apps wird über das VPN geleitet. Die Standardeinstellung ist Zulassen.

- **PerAppVPN app list**. Eine Liste aller Apps, deren Datenverkehr auf dem VPN zugelassen oder nicht zugelassen ist, festgelegt durch den Wert für Pro-App-VPN-Typ. Die App-Paketnamen sind durch Kommas oder Semikolons in der Liste getrennt. Die Groß- und Kleinschreibung wird berücksichtigt und die Schreibweise der App-Paketnamen in der Liste müssen mit dem Namen im Google Play Store identisch sein. Diese Liste ist optional. Beim Provisioning eines geräteweiten VPNs lassen Sie die Liste unausgefüllt.
- **Standard-VPN-Profil**. Der VPN-Profilname, der verwendet wird, wenn Always On VPN für Citrix Secure Access konfiguriert ist. Wenn dieses Feld leer ist, wird das Hauptprofil für die Verbindung verwendet. Wenn nur ein Profil konfiguriert ist, wird es als Standard-VPN-Profil markiert.



Hinweis:

- Um Citrix Secure Access als Always-On-VPN-App in Intune einzurichten, verwenden Sie den VPN-Anbieter als benutzerdefinierten und `com.citrix.CitrixVPN` als App-Paketnamen.
- Nur die zertifikatbasierte Clientauthentifizierung wird für Always On VPN von Citrix Secure Access unterstützt.

> • Administratoren müssen **Clientauthentifizierung** auswählen und **Clientzertifikat** im **SSL-Profil** oder in den **SSL-Eigenschaften** auf dem NetScaler Gateway auf **Obligatorisch** festlegen, damit Citrix Secure Access wie vorgesehen funktioniert.

- **Benutzerprofile deaktivieren**
  - Wenn Sie diesen Wert auf true festlegen, können Benutzer keine neuen VPN-Profile auf ihren Geräten hinzufügen.
  - Wenn Sie diesen Wert auf false setzen, können Benutzer ihre eigenen VPNs auf ihren Geräten hinzufügen.

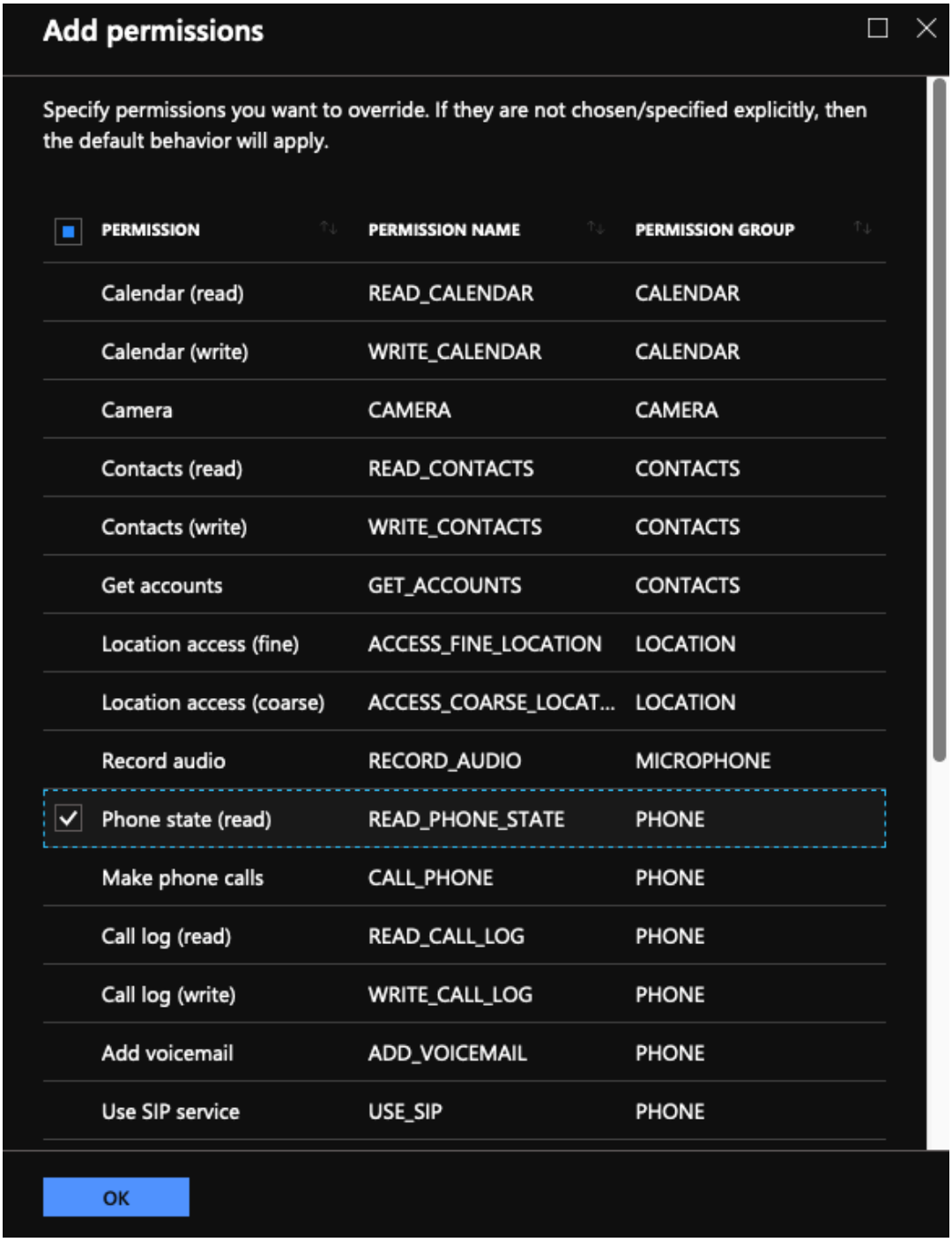
  Der Standardwert ist false.

- **Nicht vertrauenswürdige Server blockieren**
  - Legen Sie diesen Wert auf false fest, wenn Sie ein selbstsigniertes Zertifikat für NetScaler Gateway verwenden oder wenn das Stammzertifikat für die CA, die das NetScaler Gateway-Zertifikat ausstellt, nicht in der System-CA-Liste enthalten ist.
  - Setzen Sie diesen Wert auf true, damit das Android-Betriebssystem das NetScaler Gateway-Zertifikat validiert. Wenn die Validierung fehlschlägt, wird die Verbindung nicht zugelassen.

  Der Standardwert ist true.

3. Geben Sie für die Eigenschaft **Serveradresse (*)** Ihre VPN-Gateway-Basis-URL ein (z. B. `https://vpn.mycompany.com`).
4. Geben Sie unter **VPN-Profilname** einen Namen ein, der für den Endbenutzer auf dem Hauptbildschirm des Citrix Secure Access Clients sichtbar ist (z. B. My Corporate VPN).
5. Sie können andere Eigenschaften entsprechend Ihrer NetScaler Gateway-Bereitstellung hinzufügen und konfigurieren. Klicken Sie auf **OK**, wenn Sie mit der Konfiguration fertig sind.
6. Klicken Sie auf den Abschnitt **Berechtigungen**. Sie können die folgenden für Citrix Secure Access erforderlichen Berechtigungen gewähren:

   - Wenn Sie die Intune-NAC-Prüfung verwenden, erfordert Citrix Secure Access, dass Sie die Berechtigung **Phone state (read)** gewähren. Klicken Sie auf **Hinzufügen**, um das Berechtigungsblatt zu öffnen. Derzeit zeigt Intune eine umfangreiche Liste von Berechtigungen an, die für alle Apps verfügbar sind.
   - Wenn Sie Intune NAC Check verwenden, wählen Sie die Berechtigung **Telefonstatus (lesen)** und klicken Sie auf **OK**. Dadurch wird es zur Liste der Berechtigungen für die App hinzugefügt. Wählen Sie entweder **Aufforderung** oder **Auto Grant** aus, damit die Intune NAC-Prüfung funktionieren kann, und klicken Sie auf **OK**.



- Es wird empfohlen, Citrix Secure Access automatisch Benachrichtigungsberechtigungen zu gewähren.

> **Hinweis:**
>
> Für Benutzer von Android 13+, die Citrix Secure Access 23.12.1 und höher verwenden, wird MDM-Administratoren empfohlen, Citrix Secure Access (Paket-ID: `com.citrix.`

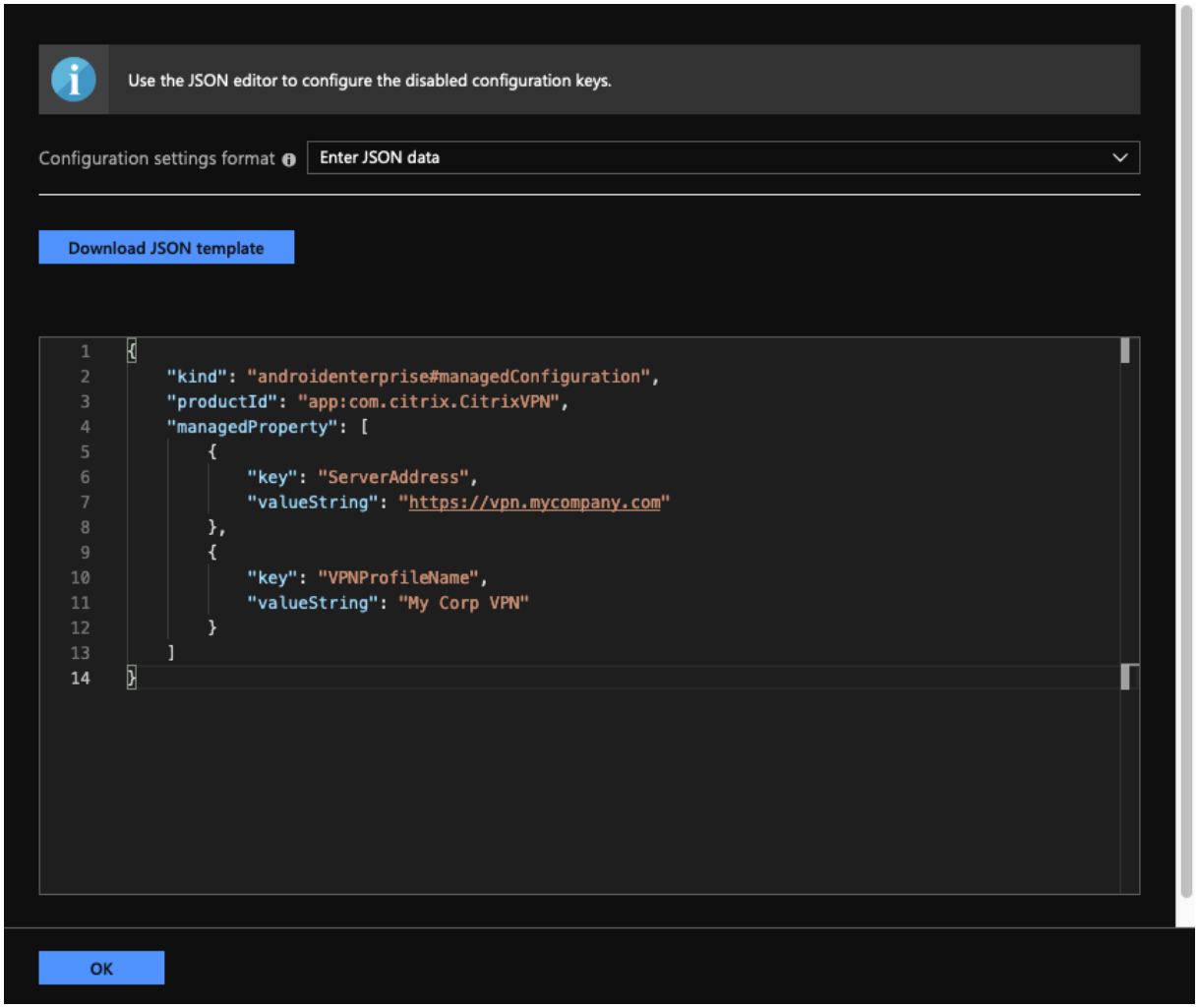
> `CitrixVPN`) in ihrer Lösung die Benachrichtigungsberechtigung zu gewähren.

7. Klicken Sie unten auf der Seite App-Konfigurationsrichtlinie auf **Hinzufügen**, um die verwaltete Konfiguration für Citrix Secure Access zu speichern.
8. Klicken Sie im Blatt für App-Konfigurationsrichtlinien auf **Zuweisungen**, um das Blatt **Zuweisungen** zu öffnen.
9. Wählen Sie die Benutzergruppen aus, für die diese Citrix Secure Access-Konfiguration bereitgestellt und angewendet werden soll.

VPN-Konfiguration durch Eingabe von JSON-Daten

1. Wählen Sie in **Konfigurationseinstellungen** die Option **JSON-Daten eingeben**, um Citrix Secure Access zu konfigurieren.
2. Verwenden Sie die Schaltfläche JSON-Vorlage herunterladen, um eine Vorlage herunterzuladen, die eine detailliertere oder komplexere Konfiguration für Citrix Secure Access ermöglicht. Diese Vorlage besteht aus einer Reihe von JSON-Schlüssel-Wert-Paaren zur Konfiguration aller möglichen Eigenschaften, die Citrix Secure Access versteht.

   Eine Liste aller verfügbaren Eigenschaften, die konfiguriert werden können, finden Sie unter Verfügbare Eigenschaften für die Konfiguration des VPN-Profils in der Citrix Secure Access-App.
3. Nachdem Sie eine JSON-Konfigurationsdatei erstellt haben, kopieren Sie den Inhalt und fügen Sie ihn in den Bearbeitungsbereich ein. Das Folgende ist beispielsweise die JSON-Vorlage für die Grundkonfiguration, die zuvor mit der Konfigurationsdesigner-Option erstellt wurde.



Damit ist das Verfahren zur Konfiguration und Bereitstellung von VPN-Profilen für Citrix Secure Access in der Microsoft Intune Android Enterprise-Umgebung abgeschlossen.

> **Wichtig:**
>
> Das für die clientzertifikatsbasierte Authentifizierung verwendete Zertifikat wird mit einem Intune-SCEP-Profil bereitgestellt. Der Alias für dieses Zertifikat muss in der Eigenschaft **Certificate Alias** der verwalteten Konfiguration für Citrix Secure Access konfiguriert werden.

Verfügbare Eigenschaften für die Konfiguration des VPN-Profils in Citrix Secure Access

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
VPN-Profilname	VPNProfileName	Text	Name des VPN-Profils (falls nicht standardmäßig auf Serveradresse festgelegt).
Serveradresse (*)	ServerAddress	URL	Basis-URL des NetScaler Gateway für die Verbindung (`https://host[:port]`). Dies ist ein Pflichtfeld.
`Username` (optional)	Benutzername	Text	Benutzername, der für die Authentifizierung mit dem NetScaler Gateway verwendet wird (optional).
Password (optional)	Kennwort	Text	Kennwort des Benutzers für die Authentifizierung mit dem NetScaler Gateway (optional).
Alias des Zertifikats (optional)	ClientCertAlias	Text	Alias des im Android-Anmeldeinformationsspeicher installierten Client-Zertifikats zur Verwendung bei der zertifikatsbasierten Clientauthen-tifizierung (optional). Der**Zertifikatalias** ist ein erforderliches Feld, wenn Sie die zertifikatbasierte Authentifizierung auf NetScaler Gateway verwenden.

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
Gateway-Zertifikat-Pins (optional)	ServerCertificatePins	JSON-Text	Eingebettetes JSON-Objekt, das die für NetScaler Gateway verwendeten Zertifikat-Pins beschreibt. Beispielwert: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`. Achten Sie darauf, diese eingebetteten JSON-Daten zu maskieren, wenn Sie den JSON-Konfigurator verwenden.

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
VPN-Typ pro App (optional)	PerAppVPN_Allow_Disallow_Setting	Enum (Allow, Disallow)	Ist es den aufgelisteten Apps erlaubt (Positivliste) oder nicht (Sperrliste), den VPN-Tunnel zu verwenden.Wenn auf **Zulassen** gesetzt, dürfen nur aufgelistete Apps (in der PerAppVPN App-Listeneigenschaft) durch das VPN tunneln. Wenn auf **Verbieten** gesetzt, dürfen alle Apps mit Ausnahme der aufgelisteten über das VPN tunneln. Wenn keine Apps aufgeführt sind, dürfen alle Apps das VPN tunneln.
PerAppVPN app list	PerAppName_Appnames	Text	Durch Komma (,) oder Semikolon (;) getrennte Liste von App-Paketnamen für VPN pro App. Die Paketnamen müssen mit denen übereinstimmen, die in der URL der Google Play Store-App-Auflistungsseite angezeigt werden. Bei Paketnamen wird zwischen Groß- und Kleinschreibung unterschieden.

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
Standard-VPN-Profil	DefaultProfileName	Text	Name des VPN-Profils, das verwendet werden soll, wenn das System den VPN-Dienst startet. Diese Einstellung wird verwendet, um das VPN-Profil zu identifizieren, das verwendet werden soll, wenn Always On VPN auf dem Gerät konfiguriert ist.
Benutzerprofile deaktivieren	DisableUserProfiles	Boolescher Wert	Eigenschaft, die es den Endbenutzern erlaubt oder nicht, VPN-Profile manuell zu erstellen. Setzen Sie diesen Wert auf**true**, um Benutzern das Erstellen von VPN-Profilen zu verbieten. Der Standardwert ist **falsch.**

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
Nicht vertrauenswürdige Server blockieren	BlockUntrustedServers	Boolescher Wert	Eigenschaft, um festzustellen, ob die Verbindung zu nicht vertrauenswürdigen Gateways (z. B. bei Verwendung selbstsignierter Zertifikate oder wenn die ausstellende Zertifizierungsstelle vom Android-Betriebssystem nicht als vertrauenswürdig eingestuft wird) blockiert werden soll? Der Standardwert ist true (Verbindungen zu nicht vertrauenswürdigen Gateways blockieren).
Benutzerdefinierte Parameter (optional)	CustomParameters	Liste	Liste der benutzerdefinierten Parameter (optional), die von Citrix Secure Access unterstützt werden. Einzelheiten finden Sie unter Benutzerdefinierte Parameter. Die verfügbaren Optionen finden Sie in der **NetScaler Gateway-Produktdokumentation**.

Konfigurationsschlüssel	JSON-Feldname	Werttyp	Beschreibung
Liste anderer VPN-Profile	bundle_profiles	Liste	Liste anderer VPN-Profile. Die meisten der zuvor genannten Werte für jedes Profil werden unterstützt. Einzelheiten finden Sie unter Unterstützte Eigenschaften für jedes VPN in der VPN-Profilliste.

Benutzerdefinierte Parameter Jeder benutzerdefinierte Parameter muss mit den folgenden Schlüssel-Wert-Namen definiert werden.

Schlüssel	Werttyp	Wert
ParameterName	Text	Name des benutzerdefinierten Parameters.
ParameterValue	Text	Wert des benutzerdefinierten Parameters.

Benutzerdefinierte Parameter für die Intune-Konfiguration

Parametername	Beschreibung	Wert
UserAgent	Citrix Secure Access hängt diesen Parameterwert an den User-Agent-HTTP-Header an, wenn es mit NetScaler Gateway kommuniziert, um NetScaler Gateway zusätzlich zu überprüfen.	Geben Sie den Text an, den Sie an den HTTP-Header des Benutzeragenten anhängen müssen. Der Text muss den HTTP-User-Agent-Spezifikationen entsprechen.

Parametername	Beschreibung	Wert
EnableDebugLogging	Aktivieren Sie die Debug-Protokollierung auf Citrix Secure Access, um VPN-Verbindungsprobleme bei Always On VPN zu beheben. Sie können es in einer beliebigen verwalteten VPN-Konfiguration aktivieren. Die Debug-Protokollierung wird wirksam, wenn die verwalteten Konfigurationen verarbeitet werden.	**True**: Aktiviert die Debug-Protokollierung. Standardwert: **False**.

Weitere Informationen zu den benutzerdefinierten Parametern finden Sie unter Erstellen einer verwalteten Android Enterprise-Konfiguration für Citrix Secure Access.

Unterstützte Eigenschaften für jedes VPN in der VPN-Profilliste Die folgenden Eigenschaften werden für jedes VPN-Profil unterstützt, wenn mehrere VPN-Profile mit der JSON-Vorlage konfiguriert werden.

Konfigurationsschlüssel	JSON-Feldname	Werttyp
VPN-Profilname	bundle_VPNProfileName	Text
Serveradresse (*)	bundle_ServerAddress	URL
Benutzername	bundle_Username	Text
Kennwort	bundle_Password	Text
Client-Cert-Alias	bundle_ClientCertAlias	Text
Gateway-Zertifikats-Pins	bundle_ServerCertificatePins	Text
Pro-App-VPN-Typ	bundle_PerAppVPN_Allow_Disallow_Setting	Enum (Allow, Disallow)
PerAppVPN app list	bundle_PerAppVPN_Appnames	Text
Benutzerdefinierte Parameter	bundle_CustomParameters	Liste

Citrix Secure Access in Intune als Always-On-VPN-Anbieter festlegen

In Ermangelung einer On-Demand-VPN-Unterstützung in einem Android-VPN-Subsystem kann das Always On VPN als Alternative verwendet werden, um eine nahtlose VPN-Konnektivitätsoption zusammen mit der Clientzertifikatsauthentifizierung mit Citrix Secure Access bereitzustellen. Das VPN wird vom Betriebssystem gestartet, wenn es hochfährt oder wenn das Arbeitsprofil aktiviert wird.

Um Citrix Secure Access in Intune zu einer Always-On-VPN-App zu machen, müssen Sie die folgenden Einstellungen verwenden.

- Wählen Sie die richtige Art der zu verwendenden verwalteten Konfiguration (in persönlichem Besitz mit Arbeitsprofil ODER vollständig verwaltetes, dediziertes und unternehmenseigenes Arbeitsprofil).
- Erstellen Sie ein Gerätekonfigurationsprofil, wählen Sie **Geräteeinschränkungen** aus und gehen Sie dann zum Abschnitt **Konnektivität**. Wählen Sie Aktivieren für Always On VPN Einstellung.
- Wählen Sie **Citrix Secure Access** als VPN-Client. Wenn Citrix Secure Access nicht als Option verfügbar ist, können Sie **Benutzerdefiniert** als VPN-Client wählen und **com.citrix.CitrixVPN** in das Feld “Paket-ID”eingeben (im Feld “Paket-ID”wird zwischen Groß- und Kleinschreibung unterschieden).
- Lassen Sie andere Optionen so wie sie sind. Es wird empfohlen, den Lockdown-Modus nicht zu aktivieren. Wenn diese Option aktiviert ist, verliert das Gerät möglicherweise die vollständige Netzwerkkonnektivität, wenn VPN nicht verfügbar ist.
- Zusätzlich zu diesen Einstellungen können Sie auch den **Pro-App-VPN**-Typ und die **Pro-App-VPN**-App-Liste auf der Seite **App-Konfigurationsrichtlinien** festlegen, um Pro-App-VPN für Android zu aktivieren, wie in den vorherigen Abschnitten beschrieben.

> **Hinweis:**
>
> Always On VPN wird nur mit der Clientzertifikatauthentifizierung in Citrix Secure Access unterstützt.

Referenzen

Weitere Informationen zum Einrichten von Konnektivitätsoptionen in Intune finden Sie in den folgenden Themen.

- Vollständig verwaltete dedizierte Unternehmensgeräte
- Geräte in persönlichem Besitz

Automatischer Neustart von Always On VPN

Ab Citrix SSO für Android 23.8.1 startet Citrix Secure Access das Always-On-VPN automatisch neu, wenn eine App, die Teil der Positiv- oder Sperrliste ist, in einem Arbeitsprofil oder einem Geräteprofil installiert wird. Der Datenverkehr von der neu installierten App wird automatisch über eine VPN-Verbindung getunnelt, ohne das Arbeitsprofil oder das Gerät neu zu starten.

Um den automatischen Neustart von Always-On-VPN zu aktivieren, müssen Endbenutzer der Option Alle Pakete abfragen die Zustimmung zu Citrix Secure Access erteilen. Sobald die Zustimmung erteilt wurde, kann Citrix Secure Access Folgendes:

- Empfängt die Benachrichtigung über die Paketinstallation vom Betriebssystem.
- Startet das Always-On-VPN neu.

Wenn ein Endbenutzer zum ersten Mal eine Verbindung zu einem VPN-Profil pro App herstellt, wird er aufgefordert, seine Zustimmung zur Erfassung von Informationen über das installierte Paket zu erteilen (gemäß den Google-Richtlinien erforderlich). Erteilt der Endbenutzer die Zustimmung, wird die VPN-Verbindung initiiert. Wenn der Benutzer die Zustimmung verweigert, wird die VPN-Verbindung abgebrochen. Die Seite zur Zustimmung wird nicht wieder angezeigt, wenn die Zustimmung erteilt wurde. Einzelheiten zu den Anweisungen für Endbenutzer finden Sie unter So verwenden Sie Citrix Secure Access von Ihrem Android-Gerät aus.

Einschränkungen

Die folgenden Einschränkungen gelten für Pro-App-VPNs auf Android 11+-Geräten in einer Android Enterprise-Umgebung verwenden, aufgrund von Paketsichtbarkeitsbeschränkungen, die in Android 11 eingeführt wurden:

- Wenn eine App, die Teil der Liste “Zulässig/Verweigert”ist, nach dem Start der VPN-Sitzung auf einem Gerät bereitgestellt wird, muss der Endbenutzer die VPN-Sitzung neu starten, damit die App ihren Datenverkehr durch die VPN-Sitzung weiterleiten kann.
- Wenn das Pro-App-VPN über eine Always-On-VPN-Sitzung verwendet wird, muss der Endbenutzer nach der Installation einer neuen App auf dem Gerät das Arbeitsprofil oder das Gerät neu starten, damit der Datenverkehr der App über die VPN-Sitzung weitergeleitet wird.

> **Hinweis:**
>
> Diese Einschränkungen gelten nicht bei Verwendung von Citrix SSO für Android 23.8.1 oder höher. Weitere Informationen finden Sie unter Automatischer Neustart von Always On VPN.

NetScaler Gateway-Zertifikatpinning mit Citrix Secure Access für Android

January 29, 2024

> **Wichtig:**
>
> Citrix SSO für Android heißt jetzt Citrix Secure Access. Wir aktualisieren unsere Dokumentation und die Screenshots der Benutzeroberfläche, um diese Namensänderung widerzuspiegeln.

Das Anheften von Zertifikaten hilft, Man-in-the-Middle-Angriffe zu verhindern. Citrix Secure Access unterstützt das Zertifikatpinning nur für verwaltete VPN-Konfigurationen im Android Enterprise-Modus und im Legacygeräteverwaltungsmodus. Es wird nicht für VPN-Profile unterstützt, die vom Endbenutzer hinzugefügt wurden.

NetScaler Gateway-Zertifikatpinning mit Android Citrix Secure Access konfigurieren

Einzelheiten zum Zertifikatpinning in der verwalteten Konfiguration (früher App-Einschränkungen) für Citrix Secure Access finden Sie unter Zertifikate und Authentifizierung.

Ein neues Schlüssel-Wert-Paar ist definiert, um die angeheftete NetScaler Gateway-Zertifikatshashes wie folgt zu tragen.

```
Key: ServerCertificatePins
Value: {

  "hash-alg": "sha256",
  "pinset": [
    "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
       (SPKI)",
    "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
    ...
  ]
 }

<!--NeedCopy-->
```

Der Schlüssel zur Angabe von Details zum Anheften von Zertifikaten in der verwalteten Konfiguration ist **ServerCertificatePins**. Der Wert ist eine JSON-Nutzlast, die die base64-codierten SHA-256-Hashes des angehefteten NetScaler Gateway-Zertifikats und des verwendeten Hashing-Algorithmus trägt. Das angeheftete Zertifikat kann jedes der vom Betriebssystem validierten Zertifikate in der Vertrauenskette sein. In diesem Fall ist es Android.

Das Anheften des Zertifikats erfolgt erst, nachdem das Betriebssystem die Zertifikatskette während des TLS-Handshakes validiert hat. Die Pin des Zertifikats wird berechnet, indem die öffentlichen Schlüsselinformationen (SPKI) des Zertifikats gehasht werden. Beide Felder ("**Hash-Alg**"und **"Pinset"**) müssen in der JSON-Nutzlast angegeben werden.

Das "**Hash-Alg**"gibt den Hashing-Algorithmus an, der zur Berechnung des SPKI-Hashs verwendet wird.
Das "**Pinset**"gibt das JSON-Array an, das den base64-codierten SHA-256-Hash der SPKI-Daten des NetScaler Gateway-Zertifikats enthält.
Für die Zertifikat-Pin muss mindestens ein Wert angegeben werden. Es können mehr Pinwerte angegeben werden, um eine Rotation oder einen Ablauf des Zertifikats zu ermöglichen.

Sie können den Wert für den Pin für eine Domäne (z. B. gw.yourdomain.com) mithilfe des folgenden openssl-Befehls berechnen.

```
1 openssl s_client -servername gw.yourdomain.com -connect gw.yourdomain.
     com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin -outform
      der | openssl dgst -sha256 -binary | openssl enc -base64
2 <!--NeedCopy-->
```

Der Befehl zeigt den base64-codierten SHA-256-Hash des Blatt-Zertifikats an, das von einem Gateway präsentiert wird. Jedes Zertifikat in der Kette kann für das Anheften von Zertifikaten verwendet werden. Wenn ein Unternehmen beispielsweise seine eigene zwischengeschaltete CA zum Generieren von Zertifikaten für mehrere Gateways verwendet, kann eine dem Zwischensignaturzertifikat entsprechende Pin verwendet werden. Wenn keiner der Pins mit den Zertifikaten in der validierten Zertifikatskette übereinstimmt, wird der TLS-Handshake abgebrochen und die Verbindung zum Gateway wird nicht fortgesetzt.

> **Hinweis:**
>
> Im Geräteadministratormodus wird das Anheften von Zertifikaten nur mit Citrix Endpoint Management- und Microsoft Endpoint Management-Lösungen unterstützt. Das Anheften von Zertifikaten muss in den benutzerdefinierten Parametern konfiguriert werden, die im Legacy-VPN-Profil (nicht verwaltete Konfiguration) mit dem benutzerdefinierten Parameter ServerCertificatePins mit derselben JSON-Nutzlast für das Anheften verwendet werden.

Citrix Secure Access für Windows —Versionshinweise

March 27, 2024

Der Citrix Secure Access Client für Windows ist jetzt eigenständig veröffentlicht und mit allen NetScaler-Versionen kompatibel. Die Citrix Secure Access Clientversion folgt dem Format JJ.MM Release.Build.

In den Versionshinweisen werden die neuen Funktionen, Verbesserungen der vorhandenen Funktionen und behobene Probleme beschrieben.

Was ist neu: Die neuen Funktionen und Verbesserungen, die in der aktuellen Version verfügbar sind.

Behobene Probleme: Die Probleme, die in der aktuellen Version behoben wurden.

Ausführliche Informationen zu den unterstützten Funktionen finden Sie in der NetScaler Gateway-Produktdokumentation.

> **Hinweis:**
>
> - Der Citrix Secure Access Client für Windows Builds 23.7.1.1 und höher enthält den Fix für. https://support.citrix.com/article/CTX564833
> - Der Citrix Secure Access Client (früher bekannt als NetScaler Gateway Plug-in für Windows) erstellt 21.9.1.2 und höher und enthält den Fix für. https://support.citrix.com/article/CTX341455

24.2.1.15 (04.03.2024)

Was ist neu

- **Unterstützung für SNI**

  In einer Citrix Secure Private Access-Bereitstellung unterstützt der Citrix Secure Access Client jetzt die SNI-Erweiterung (Server Name Indication) bei allen Vorauthentifizierungsanfragen.

  [SPAHELP-236]

- **Unterstützung für TLS 1.3**

  Der Citrix Secure Access Client unterstützt jetzt das TLS 1.3-Protokoll. TLS 1.3 wird auf den folgenden Plattformen unterstützt:

  - Windows 11 und höher
  - Windows Server 2022 und höher

  Einzelheiten zur Konfiguration von TLS 1.3 auf NetScaler finden Sie unter Unterstützung für das TLS 1.3-Protokoll.

  [CSACLIENTS-6106]

- **Unterstützung für Windows-Betriebssystemdetails im HTTP-Header**

  Der Citrix Secure Access Client enthält jetzt Details des Windows-Betriebssystems als Teil der HTTP-Header-Zeichenfolge (User-Agent).

  [NSHELP-36732]

Behobene Probleme

Die DNS-Auflösung schlägt zeitweise fehl, wenn IPv6 auf dem Client-Netzwerkadapter aktiviert ist.

[NSHELP-35708]

Benutzer können sich möglicherweise nicht am Citrix Secure Access Client anmelden, wenn gleichzeitig versucht wird, sich mit Autologon anzumelden.

[NSHELP-35768]

Die Installation von Citrix Secure Access schlägt fehl, wenn Smart App Control auf nicht englischen Clientcomputern aktiviert ist.

[NSHELP-36126], [NSHELP-36907]

Benutzer können nicht über VPN auf einige Anwendungen zugreifen, wenn der Citrix Secure Access Client mit dem WFP-Treiber konfiguriert ist. Dieses Problem tritt aufgrund von Änderungen an den Firewallrichtlinien auf.

[NSHELP-36254], [NSHELP-36312]

Während eines EPA-Scans erscheint ein Popup-Dialogfeld. Wenn der Benutzer jedoch auf OK klickt, funktioniert der EPA-Scan wie gewohnt. Dieses Problem tritt auf, wenn auf der Benutzeroberfläche des Citrix Secure Access Clients die schwedische**Sprache ausgewählt ist (Konfiguration > Sprache**).

[NSHELP-36408]

In einem Always-On-VPN-Modus kann der Tunnel auf Maschinenebene die Sitzung nicht übertragen, wenn die Benutzerzertifikatauthentifizierung auf NetScaler Gateway konfiguriert ist.

[NSHELP-36492]

Der Zugriff auf die Intranetressourcen schlägt zeitweise fehl, wenn der Windows Filtering Platform (WFP) -Treiber auf dem Citrix Secure Access Client aktiviert ist.

[NSHELP-36568]

Die Benutzeroberflächenseite des Citrix Secure Access Clients friert zeitweise ein, wenn Benutzer auf die Home-Schaltfläche klicken.

[NSHELP-37046]

Benutzer ohne Administratorrechte können keine Verbindung zum vollständigen VPN-Tunnel herstellen, wenn die folgenden Bedingungen erfüllt sind:

- EPA ist als Faktor in einem nFactor-Flow konfiguriert.
- Edge WebView ist aktiviert.

- Die Einstellung für das Control-Upgrade des Citrix EPA-Clients ist auf **Always** on NetScaler Gateway festgelegt, und die Citrix EPA-Clientversionen zwischen dem Clientgerät und NetScaler stimmen nicht überein.

[NSHELP-37340]

Der Scan von EPA-Gerätezertifikaten schlägt fehl, wenn der Systemzertifikatspeicher des Client-Computers nur ein Gerätezertifikat enthält.

[NSHELP-37371]

Die Anmeldeseite des Citrix Secure Access Clients wird zeitweise leer, wenn eine Verbindung zum Citrix Secure Private Access Service hergestellt wird.

[SPAHELP-202]

Endbenutzer können die Client-Computer möglicherweise nicht über VPN mit der Domäne verbinden, wenn Windows Server 2019 oder spätere Versionen verwendet werden.

[SPAHELP-219]

Wenn der Citrix Device Posture Service aktiviert ist, werden unerwünschte Einträge in der Dropdownliste **Verbindung** der Citrix Secure Access Client-Benutzeroberfläche angezeigt.

[SPAHELP-271]

Endbenutzer können nicht auf die Intranetressourcen zugreifen, wenn die Single Sign-On-Funktion auf dem Citrix Secure Access Client aktiviert ist.

[CSACLIENTS-9940]

23.10.1.7 (29. Nov. 2023)

Was ist neu

- **Privaten Portbereich für serverinitiierte Verbindungen konfigurieren**

  Sie können jetzt einen privaten Port zwischen 49152 und 64535 für serverinitiierte Verbindungen konfigurieren. Durch die Konfiguration privater Ports werden Konflikte vermieden, die auftreten können, wenn Sie Ports verwenden, um Sockets zwischen dem Citrix Secure Access Client und Apps von Drittanbietern auf den Client-Computern zu erstellen. Sie können die privaten Ports mit der Windows-VPN-Registrierung "SicBeginPort"konfigurieren. Alternativ können Sie den privaten Portbereich mithilfe einer JSON-Datei zur Anpassung des VPN-Plug-ins auf NetScaler konfigurieren.

  Weitere Informationen finden Sie unter Serverinitiierte Verbindungen konfigurieren und NetScaler Gateway Windows VPN-Client-Registrierungsschlüssel.

  [NSHELP-36627]

- **Unterstützung der Kerberos-Authentifizierung für eine nahtlose automatische Anmeldung**

  Der Citrix Secure Access Client verwendet jetzt die Kerberos-Authentifizierungsmethode für die automatische Anmeldung. Im Rahmen dieser Unterstützung wird ein VPN-Client-Registrierungsschlüssel "EnableKerberosAuth"eingeführt. Als Voraussetzung müssen Administratoren die Kerberos-Authentifizierung auf NetScaler und ihren Clientmaschinen konfigurieren. Endbenutzer müssen Microsoft Edge WebView auf ihren Maschinen installieren, um die Kerberos-Authentifizierungsmethode zu aktivieren. Weitere Informationen finden Sie unter Automatische Anmeldung mit Kerberos-Authentifizierung.

  [CSACLIENTS-3128]

- **Automatische Zuweisung eines Spoof-IP-Adressbereichs**

  Der Citrix Secure Access Client kann jetzt einen neuen Spoof-IP-Adressbereich erkennen und anwenden, wenn ein Konflikt zwischen dem vom Administrator konfigurierten Spoof-IP-Adressbereich und den IP-basierten Anwendungen oder dem Netzwerk des Endbenutzers besteht.

  [CSACLIENTS-6132]

- **Microsoft-Benachrichtigungen**

  Die Citrix Secure Access Clientbenachrichtigungen werden jetzt als Microsoft-Benachrichtigungen im Benachrichtigungsfeld Ihres Windows-Computers angezeigt.

  [CSACLIENTS-6136]

- **Verbesserte Protokollerfassung**

  Die Protokollebene "Ausführlich"wird jetzt als Debug-Standardprotokollierungsebene für eine erweiterte Protokollerfassung und Problembehandlung verwendet. Weitere Informationen zur Protokollierung finden Sie unter Protokollierung mit der Client-Benutzeroberfläche konfigurieren.

  [CSACLIENTS-8151]

Behobene Probleme

Der Citrix Secure Access Client bleibt im Status "Connecting", wenn der Maschinentunnel des Always-On-Dienstes den Standort des Clientgeräts nicht erkennt.

[CSACLIENTS-1174]

Die Funktion zum Übertragen der Anmeldung funktioniert nicht, wenn Microsoft Edge WebView im Citrix Secure Access Client aktiviert ist.

[CSACLIENTS-6655]

Im Always-On-Dienstmodus kann der Citrix Secure Access Client keinen Tunnel auf Maschinenebene mit NetScaler Gateway einrichten, wenn die auf Gerätezertifikaten basierenden klassischen Authentifizierungsrichtlinien an einen virtuellen VPN-Server gebunden sind.

[NSHELP-33766]

Eingehende und ausgehende Webex-Anrufe schlagen fehl, wenn Benutzer mit dem VPN verbunden sind. Dieses Problem tritt auf, wenn der Treiber für die Windows-Filterplattform (WFP) auf dem Citrix Secure Access Client anstelle des DNE-Treibers (Deterministic Network Enhancer) aktiviert ist.

[NSHELP-34651]

Der Citrix Secure Access Client stürzt ab, wenn die folgenden Bedingungen erfüllt sind:

- Verbindungen werden gewechselt, wenn SAML-Richtlinien an einen virtuellen VPN-Server gebunden sind.
- Die Internet Explorer WebView-Unterstützung ist aktiviert.

[NSHELP-35366]

Die Benutzeroberfläche des Citrix Secure Access Clients zeigt während der automatischen Anmeldung die Schaltfläche “Verbinden”an. Dieses Problem tritt auf, wenn die UserCert-Authentifizierungsmethode verwendet wird, um eine VPN-Verbindung herzustellen.

[NSHELP-36134]

Die lokale LAN-Zugriffsfunktion funktioniert nicht mit dem Citrix Secure Access Client, wenn ein Tunnel auf Maschinenebene konfiguriert ist.

In dieser Version kann die lokale LAN-Zugriffsfunktion mit einer Tunnelkonfiguration auf Maschinenebene eingerichtet werden. Um dies zu erreichen, müssen Sie den lokalen LAN-Zugriffsparameter auf FORCED konfigurieren, wenn Sie den Maschinentunnelmodus verwenden. Weitere Informationen finden Sie unter Erzwingen des lokalen LAN-Zugriffs für Endbenutzer basierend auf der ADC-Konfiguration.

[NSHELP-36214]

Wenn eine Clientmaschine mehrmals aus dem Ruhemodus aufwacht, kann der Citrix Secure Access Client keine VPN-Verbindung mit den Intranetanwendungen herstellen.

[NSHELP-36221]

23.8.1.11 (19. Oktober 2023)

Behobene Probleme

Die Datei epaPackage.exe kann möglicherweise nicht heruntergeladen werden, wenn die Forward-Proxyunterstützung auf NetScaler Gateway konfiguriert ist.

[CSACLIENTS-6917]

Die Installation des Citrix EPA-Clients schlägt für Benutzer ohne Administratorrechte mit eingeschränktem Zugriff auf Laufwerk C fehl.

[NSHELP-36590]

23.8.1.5 (09-Aug-2023)

Behobene Probleme

Kerberos SSO schlägt für Anwendungen fehl, wenn sie über den Citrix Secure Private Access-Dienst verbunden sind.

[CSACLIENTS-912]

Der Anwendungszugriff mit dem Citrix Secure Private Access-Dienst schlägt zeitweise fehl. Dieses Problem tritt auf, wenn der Citrix Secure Access Client eine falsche Ziel-IP-Adresse für TCP- oder UDP-Verkehr verwendet.

[CSACLIENTS-1151, CSACLIENTS-6326]

Der Citrix Secure Access Client kann aufgrund eines DNS-Caching-Problems zeitweise keine Anwendungen starten.

[CSACLIENTS-1170]

Der Citrix Secure Access Client kann kein DNS-Suffix auf Citrix Virtual Adapter anwenden. Dieses Problem tritt auf, wenn der Citrix Virtual Adapter sich nicht mit Active Directory authentifizieren kann.

[NSHELP-33817]

Der Citrix Secure Access Client stürzt ab, wenn die folgenden Bedingungen erfüllt sind:

- Der virtuelle NetScaler Gateway-Server enthält ein Client-Zertifikat als Faktor für die nFactor-Authentifizierung.
- Die Microsoft Edge WebView-Unterstützung ist aktiviert.

[CSACLIENTS-6171]

Wenn Sie mit einem VPN verbunden sind, können Sie möglicherweise nicht auf Back-End-Ressourcen zugreifen, nachdem Sie Microsoft KB5028166 installiert haben.

[NSHELP-35909]

Der Citrix Secure Access Client kann die Konfigurationen zeitweise nicht von NetScaler Gateway herunterladen, wenn die Portalanpassung den zulässigen Grenzwert überschreitet.

[NSHELP-35971]

Bekannte Probleme

Die Transfer-Logon-Funktion funktioniert nicht mit dem Citrix Secure Access Client. Dieses Problem tritt auf, wenn Microsoft Edge WebView aktiviert ist.

Umgehung: Melden Sie sich mit einem Webbrowser an, um die Sitzung zu übertragen.

23.7.1.1 (14. Juli 2023)

Behobene Probleme

In einigen Fällen kann der Datenverkehr nach einem Upgrade auf die Release-Version 23.x.x.x den VPN-Tunnel nicht passieren, was zur Blockierung des VPN-Zugriffs führt, wenn ein Intranet-IP-Bereich auf NetScaler konfiguriert ist. Dies passiert, wenn die profilübergreifende Firewallregel nicht auf VPN-Anwendungen angewendet wird.

[NSHELP-35766]

23.5.1.3 (02. Juni 2023)

Behobene Probleme

Der AlwaysOn-Dienst stürzt ab, wenn die verbesserte Protokollsammlung mithilfe der Registrierung "useNewLogger"unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client` aktiviert wird.

[CGOP-24462]

23.4.1.5 (14-Apr-2023)

Was ist neu

- **Unterstützung für Microsoft Edge WebView**

Die Unterstützung von Microsoft Edge WebView auf dem Citrix Secure Access Client für Windows führt zu einer verbesserten Endbenutzererfahrung. Diese Funktion ist standardmäßig deaktiviert. Einzelheiten finden Sie unter Microsoft Edge WebView-Unterstützung für Windows Citrix Secure Access.

[CGOP-22245]

- **Hinzufügen von DNS-Suffixen zur Auflösung von FQDNs zu IP-Adressen**

  Admins können den Anwendungen jetzt auf Betriebssystemebene Suffixe hinzufügen. Dies hilft Citrix Secure Access Clients, einen nicht vollständig qualifizierten Domänennamen während der Namensauflösung zu lösen.

  Administratoren können Anwendungen auch mithilfe der IP-Adressen (IP-CIDR/IP-Bereich) konfigurieren, sodass die Endbenutzer über die entsprechenden FQDNs auf die Anwendungen zugreifen können. Einzelheiten finden Sie unter DNS-Suffixe zur Auflösung von FQDNs in IP-Adressen.

  [ACS-2490]

- **Verbesserte Protokollerfassung**

  Die Protokollierungsfunktion für den Windows Secure Access Client wurde jetzt für die Protokollerfassung und das Debuggen verbessert. Die folgenden Änderungen wurden an der Protokollierungsfunktion vorgenommen.

  - Ermöglichen Sie Benutzern, die maximale Größe der Protokolldatei auf einen Wert unter 600 MB zu ändern.
  - Ermöglichen Sie Benutzern, die Anzahl der Protokolldateien auf weniger als 5 zu aktualisieren.
  - Erhöhen Sie die Protokollebenen für die neue Protokollierungsfunktion auf drei.

  Mit diesen Änderungen können Admins und Endbenutzer Protokolle der aktuellen Sitzung und früherer Sitzungen sammeln. Bisher war die Erfassung von Protokollen nur auf die aktuellen Sitzungen beschränkt. Einzelheiten finden Sie unter Verbesserte Protokollerfassung für den Windows-Client.

  > **Hinweis:**
  >
  > Um die Debug-Protokollierung zu aktivieren, wählen Sie **Logging > Verbose** aus der Dropdownliste **Select Log Level** aus. Vor der Veröffentlichung des Citrix Secure Access Client für Windows 23.4.1.5 konnte die Debug-Protokollierung über das Kontrollkästchen **Konfiguration > Debug-Protokollierung aktivieren** aktiviert werden.

  [CGOP-23537]

- **Unterstützung für das Senden von Ereignissen an den Citrix Analytics Service**

Der Citrix Secure Access Client für Windows unterstützt jetzt das Senden von Ereignissen wie Sitzungserstellung, Sitzungsbeendigung und App-Verbindung an den Citrix Analytics Service. Diese Ereignisse werden dann im Citrix Secure Private Access-Dashboard protokolliert.

[SPA-2197]

Behobene Probleme

- Die Single Sign-On-Authentifizierung des Citrix Secure Access Clients mit der Citrix Workspace-App für den Cloud-Endpunkt schlägt für Unicode-Benutzer fehl.

  [CGOP-22334]

- Der Zugriff auf die Ressourcen schlägt fehl, wenn auf Hostnamen basierende Anwendungen zusammen mit dem DNS-Suffix in Citrix Secure Private Access konfiguriert werden.

  [SPA-4430]

- Die Always-On-VPN-Verbindung schlägt beim Start zeitweise fehl, da der virtuelle Gateway-Server nicht erreichbar ist.

  [NSHELP-33500]

- Auf Intranetressourcen, die sich mit einem gefälschten IP-Adressbereich überschneiden, kann nicht zugegriffen werden, wenn der Split-Tunnel auf dem Citrix Secure Access Client auf OFF gesetzt ist.

  [NSHELP-34334]

- Der Citrix Secure Access Client kann das Authentifizierungsschema nicht laden, was zu einem Anmeldefehler im Citrix Secure Private Access-Dienst führt.

  [SPAHELP-98]

23.1.1.11 (20.02.2023)

In dieser Version werden Probleme behoben, die zur Verbesserung der Gesamtleistung und Stabilität des Citrix Secure Private Access-Dienstes beitragen.

23.1.1.8 (08-Feb-2023)

Behobene Probleme

- DNS-Auflösungsfehler treten auf, da Citrix Secure Access IPv4-Pakete nicht gegenüber IPv6-Paketen priorisiert.

  [NSHELP-33617]

- Die Betriebssystemfilterregeln werden erfasst, wenn der Citrix Secure Access Client im WFP-Modus (Windows Filtering Platform) ausgeführt wird.

  [NSHELP-33715]

- Eine gefälschte IP-Adresse wird für IP-basierte Intranetanwendungen verwendet, wenn der Citrix Secure Access Client im Citrix Deterministic Network Enhancer (DNE) -Modus ausgeführt wird.

  [NSHELP-33722]

- Wenn Sie den Windows Filtering Platform (WFP) -Treiber verwenden, funktioniert der Intranetzugriff manchmal nicht, nachdem das VPN erneut verbunden wurde.

  [NSHELP-32978]

- Der EPA-Scan (Endpoint Analysis) für die Betriebssystemversionsprüfung schlägt auf Windows 10- und Windows 11 Enterprise-Desktops mit mehreren Sitzungen fehl.

  [NSHELP-33534]

- Der Windows-Client unterstützt standardmäßig eine Konfigurationsdateigröße von 64 KB, wodurch die Benutzer daran gehindert werden, der Konfigurationsdatei weitere Einträge hinzuzufügen. Diese Größe kann erhöht werden, indem Sie den Registrierungswert `ConfigSize` in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client festlegen. Der Registrierungsschlüsseltyp `ConfigSize` ist `REG_DWORD` und die Schlüsseldaten sind <`Bytes size`>. Wenn die Größe der Konfigurationsdatei größer als der Standardwert (64 KB) ist, muss der ConfigSize-Registrierungswert für jede zusätzliche Anzahl von 64 KB auf 5 x 64 KB (nach der Konvertierung in Byte) gesetzt werden. Wenn Sie beispielsweise weitere 64 KB hinzufügen, müssen Sie den Registrierungswert auf 64 x 1024 x 5 = 327680 festlegen. Ebenso müssen Sie, wenn Sie 128 KB hinzufügen, den Registrierungswert auf 64 x 1024 x (5+5) = 655360 setzen.

  [SPA-2865]

- Bei der VPN-Abmeldung werden die Einträge der DNS-Suffixliste in der SearchList-Registrierung in umgekehrter Reihenfolge, getrennt durch ein oder mehrere Kommas, neu geschrieben.

  [NSHELP-33671]

- Die Proxyauthentifizierung schlägt fehl, wenn die NetScaler Appliance einen EPA-Scan nach Antivirenprogrammen abschließt.

  [NSHELP-30876]

- Wenn die Registrierungswerte für Citrix Secure Access mehr als 1500 Zeichen umfassen, kann der Log Collector die Fehlerprotokolle nicht erfassen.

  [NSHELP-33457]

22.10.1.9 (08-Nov-2022)

Was ist neu

- **EPA-Unterstützung für Site-Persistenz vom Verbindungsproxytyp in GSLB**

  Der Windows EPA-Scan unterstützt jetzt die Site-Persistenz vom Typ Verbindungsproxy in GSLB, wenn der Scan von einem Browser aus initiiert wird. Bisher unterstützte der EPA-Scan für Windows den Verbindungsproxy-Persistenztyp für den vom Browser initiierten EPA-Scan nicht.

  [CGOP-21545]

- **Nahtloses Single Sign-On für Workspace-URL (nur Cloud)**

  Der Citrix Secure Access Client unterstützt jetzt Single Sign-On für die Workspace-URL (nur Cloud), wenn sich der Benutzer bereits über die Citrix Workspace-App angemeldet hat. Weitere Informationen finden Sie unter Single Sign-On-Unterstützung für die Workspace-URL für Benutzer, die über die Citrix Workspace-App angemeldet sind.

  [ACS-2427]

- **Verwaltung der Citrix Secure Access Client- und/oder EPA-Plug-In-Version über die Citrix Workspace-App (nur Cloud)**

  Die Citrix Workspace-App kann jetzt die neueste Version des Citrix Secure Access- und/oder EPA-Plug-Ins über den Global App Configuration Service herunterladen und installieren. Weitere Informationen finden Sie unter Global App Configuration Service.

  [ACS-2426]

- **Verbesserung der Debug-Protokollierungssteuerung**

  Die Debug-Protokollierungssteuerung für den Citrix Secure Access Client ist jetzt unabhängig von NetScaler Gateway und kann über die Plugin-Benutzeroberfläche sowohl für den Computer als auch für den Benutzertunnel aktiviert oder deaktiviert werden.

  [NSHELP-31968]

- **Unterstützung für Preflight-Anfragen für privaten Netzwerkzugriff**

  Der Citrix Secure Access Client für Windows unterstützt jetzt Preflight-Anfragen für privaten Netzwerkzugriff, die vom Chrome-Browser beim Zugriff auf private Netzwerkressourcen von öffentlichen Websites aus gestellt werden.

  [CGOP-20544]

Behobene Probleme

- Der Citrix Secure Access Client, Version 21.7.1.1 und höher, kann für Benutzer ohne Administratorrechte nicht auf neuere Versionen aktualisiert werden.

  Dies gilt nur, wenn das Citrix Secure Access Client-Upgrade von einer NetScaler-Appliance aus durchgeführt wird. Einzelheiten finden Sie unter Upgrade-/Downgrade-Problem auf dem Citrix Secure Access Client.

  [NSHELP-32793]

- Benutzer können sich aufgrund intermittierender EPA-Fehler nicht bei VPN anmelden.

  [NSHELP-32138]

- Manchmal richtet der Citrix Secure Access Client im Modus "Nur Maschinentunnel"den Maschinentunnel nicht automatisch ein, nachdem der Computer aus dem Ruhemodus erwacht ist.

  [NSHELP-30110]

- Im Servicemodus "Immer aktiv"versucht der Benutzertunnel zu starten, auch wenn nur der Maschinentunnel konfiguriert ist.

  [NSHELP-31467]

- Der Link zur Startseite auf der Citrix Secure Access-Benutzeroberfläche funktioniert nicht, wenn Microsoft Edge der Standardbrowser ist.

  [NSHELP-31894]

- Eine benutzerdefinierte EPA-Fehlerprotokollmeldung wird nicht im NetScaler Gateway-Portal angezeigt, stattdessen wird die Meldung "interner Fehler"angezeigt.

  [NSHELP-31434]

- Wenn Benutzer auf dem Citrix Secure Access-Bildschirm für Windows auf die Registerkarte Startseite klicken, wird auf der Seite der Fehler "Verbindung verweigert"angezeigt.

  [NSHELP-32510]

- Auf einigen Client-Computern kann der Citrix Secure Access Client die Proxyeinstellung nicht erkennen, was zu einem Anmeldefehler führt.

  [SPAHELP-73]

Bekannte Probleme

- Der auf der Windows Update-Prüfung basierende EPA-Scan funktioniert unter der Windows 11 22H2-Version nicht. Weitere Informationen finden Sie unter EPA-Check schlägt für Windows11 22H2 fehl.

[NSHELP-33068]

22.6.1.5 (17-Juni-2022)

Was ist neu

- **Konfiguration des Anmelde- und Abmeldeskripts**

  Der Citrix Secure Access Client greift über die folgenden Registrierungen auf die Anmelde- und Abmeldeskriptkonfiguration zu, wenn der Citrix Secure Access Client eine Verbindung zum Citrix Secure Private Access-Clouddienst herstellt.

  Registrierungspfad: **HKEY_LOCAL_MACHINE>SOFTWARE>Citrix > Secure Access Client**

  Werte der Registrierung:

  - SecureAccessLogInScript - Typ REG_SZ - Pfad zum Anmeldeskript
  - SecureAccessLogOutScript - Typ REG_SZ - Pfad zum Abmeldeskript

  [ACS-2776]

- **Windows Citrix Secure Access Client mit der Windows-Filterplattform (WFP)**

  WFP ist eine Reihe von API- und Systemdiensten, die eine Plattform zum Erstellen von Netzwerkfilteranwendungen bieten. WFP wurde entwickelt, um frühere Paketfiltertechnologien zu ersetzen, den Network Driver Interface Specification (NDIS) -Filter, der mit dem DNE-Treiber verwendet wurde. Einzelheiten finden Sie unter Windows Citrix Secure Access Client mit der Windows-Filterplattform.

  [CGOP-19787]

- **FQDN-basierte Unterstützung für Reverse**

  Der WFP-Treiber unterstützt jetzt FQDN-basiertes REVERSE-Split-Tunneling. Es wird mit dem DNE-Treiber nicht unterstützt. Weitere Informationen zum Reverse-Split-Tunnel finden Sie unter Split-Tunneloptionen.

  [CGOP-16849]

Behobene Probleme

- Manchmal funktioniert die automatische Windows-Anmeldung nicht, wenn sich ein Benutzer im Always-On-Dienstmodus am Windows-Computer anmeldet. Der Maschinentunnel wechselt nicht zum Benutzertunnel und die Meldung **Verbinden** wird in der Benutzeroberfläche des VPN-Plug-ins angezeigt.

  [NSHELP-31357]

- Bei der VPN-Abmeldung werden die Einträge der DNS-Suffixliste in der Registrierung SearchList (Computer\ HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client) in umgekehrter Reihenfolge, getrennt durch ein oder mehrere Kommas, neu geschrieben.

  [NSHELP-31346]

- Die gefälschte IP-Adresse wird auch dann verwendet, wenn die Konfiguration der NetScaler Intranetanwendung von einer FQDN-basierten in eine IP-basierte Anwendung geändert wurde.

  [NSHELP-31236]

- Die Gateway-Startseite wird nicht sofort angezeigt, nachdem das Gateway-Plug-in den VPN-Tunnel erfolgreich eingerichtet hat

  Mit diesem Fix wird der folgende Registrierungswert eingeführt.

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

  Typ: DWORD

  Standardmäßig wird dieser Registrierungswert nicht festgelegt oder hinzugefügt. Wenn der Wert von "SecureChannelResetTimeoutSeconds"0 ist oder nicht hinzugefügt wird, funktioniert der Fix zur Behandlung der Verzögerung nicht. Dies ist das Standardverhalten. Der Administrator muss diese Registrierung auf dem Client einrichten, um das Update zu aktivieren (das heißt, die Homepage wird sofort angezeigt, nachdem das Gateway-Plug-in den VPN-Tunnel erfolgreich eingerichtet hat).

  [NSHELP-30189]

- Die AlwaysOnAllow-Listenregistrierung funktioniert nicht wie erwartet, wenn der Registrierungswert größer als 2000 Byte ist.

  [NSHELP-31836]

- Der Citrix Secure Access Client für Windows tunnelt keine neuen TCP-Verbindungen zum Back-End-TCP-Server, wenn die bereits verbundene Citrix Secure Private Access-Dienstregion nicht mehr erreichbar ist. Dies wirkt sich jedoch nicht auf die on-premises Gateway-Verbindungen aus.

  [ACS-2714]

22.3.1.5 (24-Mär-2022)

Behobene Probleme

- Der Name des Windows EPA-Plug-ins wird auf das NetScaler Gateway EPA-Plug-In

  [CGOP-21061]

Bekannte Probleme

- Der Citrix Secure Access Client für Windows tunnelt keine neuen TCP-Verbindungen zum Back-End-TCP-Server, wenn die bereits verbundene Citrix Secure Private Access-Dienstregion nicht mehr erreichbar ist. Dies wirkt sich jedoch nicht auf die on-premises Gateway-Verbindungen aus.

  [ACS-2714]

22.3.1.4 (10-Mär-2022)

Was ist neu

- **Erzwingen des lokalen LAN-Zugriffs für Endbenutzer basierend auf der ADC-Konfiguration**

  Administratoren können die Endbenutzer daran hindern, die lokale LAN-Zugriffsoption auf ihren Client-Computern zu deaktivieren. Eine neue Option, FORCED, wird zu den vorhandenen Parameterwerten für lokalen LAN-Zugriff hinzugefügt. Wenn der Wert Lokaler LAN-Zugriff auf FORCED gesetzt ist, ist der lokale LAN-Zugriff für Endbenutzer auf den Client-Computern immer aktiviert. Endbenutzer können die lokalen LAN-Einstellungen nicht über die Benutzeroberfläche des Citrix Secure Access Clients deaktivieren. Wenn Administratoren eine Option zum Aktivieren oder Deaktivieren des lokalen LAN-Zugriffs für den Endbenutzer bereitstellen möchten, müssen sie den lokalen LAN-Zugriffsparameter auf ON neu konfigurieren.

  Um die **FORCED-Option** mit der GUI zu aktivieren:

  1. Navigieren Sie zu **NetScaler Gateway > Globale Einstellungen > Globale Einstellungen ändern**.
  2. Klicken Sie auf die Registerkarte **Clienterfahrung** und dann auf **Erweiterte Einstellungen**.
  3. Wählen Sie unter **Lokaler LAN-Zugriff**die Option **FORCED**

  Führen Sie den folgenden Befehl aus, um die Option **FORCED** über die CLI zu aktivieren:

  ```
  set vpn parameter -localLanAccess FORCED
  <!--NeedCopy-->
  ```

  [CGOP-19935]

- **Unterstützung für Windows Server 2019 und 2022 beim EPA-Betriebssystemscan**

  Der EPA-Betriebssystemscan unterstützt jetzt Windows Server 2019 und 2022.

  Sie können die neuen Server über die GUI auswählen.

  1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Vorauthentifizierung**.

2. Erstellen Sie eine neue Vorauthentifizierungsrichtlinie oder bearbeiten Sie eine vorhandene Richtlinie.
3. Klicken Sie auf den Link **OPSWAT EPA Editor**.
4. Wählen Sie im **AusdruckseditorWindows > Windows Update**aus und klicken Sie auf das Symbol**+**.
5. Wählen Sie **unter Betriebssystemname**den Server gemäß Ihren Anforderungen aus.

Sie können auf die OPSWAT-Version 4.3.2744.0 aktualisieren, um die Windows Server 2019 und 2022 im EPA-Betriebssystemscan zu verwenden.

[CGOP-20061]

- **Neue EPA-Scan-Klassifikationstypen für fehlende**

  Die folgenden neuen Klassifikationstypen wurden zum EPA-Scan nach fehlenden Sicherheitspatches hinzugefügt. Der EPA-Scan schlägt fehl, wenn der Client über einen der folgenden fehlenden Sicherheitspatches verfügt.

  - Anwendung
  - Connectors
  - CriticalUpdates
  - DefinitionUpdates
  - DeveloperKits
  - FeaturePacks
  - Guidance
  - SecurityUpdates
  - ServicePacks
  - Tools
  - UpdateRollups
  - Updates

  Sie können die Klassifikationstypen über die GUI konfigurieren.

  1. Navigieren Sie zu **NetScaler Gateway > Richtlinien > Vorauthentifizierung**.
  2. Erstellen Sie eine neue Vorauthentifizierungsrichtlinie oder bearbeiten Sie eine vorhandene Richtlinie.
  3. Klicken Sie auf den Link ((OPSWAT EPA Editor)).
  4. Wählen Sie im Ausdruckseditor **Windows > Windows Update**aus.
  5. Wählen Sie unter **Sollte kein Patch mit folgendem Windows Update-Klassifizierungstyp fehlen**den Klassifizierungstyp für die fehlenden Sicherheitspatches aus
  6. Klicken Sie auf **OK**.

  Sie können auf die OPSWAT-Version 4.3.2744.0 aktualisieren, um diese Optionen zu verwenden.

  - Einzelheiten zu den GUIDs der Windows Server-Update-Dienste finden Sie unter https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)
  - Eine Beschreibung der Terminologie für Microsoft-Softwareupdates finden Sie unter https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates

  Zuvor wurden die EPA-Scans nach fehlenden Sicherheitspatches mit dem Schweregrad Kritisch, Wichtig, Moderat und Niedrig auf dem Windows-Client durchgeführt.

  [CGOP-19465]

- **Unterstützung für mehrere Gerätezertifikate für den EPA-Scan**

  Wenn in der Konfiguration Always on VPN mehrere Gerätezertifikate konfiguriert sind, wird das Zertifikat mit dem längsten Ablaufdatum für die VPN-Verbindung versucht. Wenn dieses Zertifikat den EPA-Scan erfolgreich ermöglicht, wird eine VPN-Verbindung hergestellt. Wenn dieses Zertifikat beim Scanvorgang fehlschlägt, wird das nächste Zertifikat verwendet. Dieser Vorgang wird solange fortgeführt, bis alle Zertifikate ausprobiert wurden.

  Wenn früher mehrere gültige Zertifikate konfiguriert wurden und der EPA-Scan für ein Zertifikat fehlgeschlagen war, wurde der Scan für die anderen Zertifikate nicht versucht.

  [CGOP-19782]

Behobene Probleme

- Wenn der clientCert-Parameter bei der Konfiguration des virtuellen VPN-Servers im SSL-Profil auf "Optional"festgelegt ist, werden Benutzer mehrmals aufgefordert, die Smartcard auszuwählen.

  [NSHELP-30070]

- Benutzer können keine Verbindung zur NetScaler Gateway-Appliance herstellen, nachdem sie den Profilparameter "networkAccessOnVPNFailure"von "fullAccess"auf "onlyToGateway"geändert haben.

  [NSHELP-30236]

- Wenn Always on konfiguriert ist, schlägt der Benutzertunnel aufgrund der falschen Versionsnummer (1.1.1.1) in der Datei aoservice.exe fehl.

  [NSHELP-30662]

- Die DNS-Auflösung für interne und externe Ressourcen funktioniert über eine längere VPN-Sitzung nicht mehr.

  [NSHELP-30458]

- Der Windows VPN-Client berücksichtigt die Warnung "SSL-Benachrichtigung zum Schließen" des Servers nicht und sendet die Anmeldeanforderung für die Übertragung über dieselbe Verbindung.

  [NSHELP-29675]

- Registrierung EPA-Prüfung für die "=="und "! ="-Operator schlägt für einige Registrierungseinträge fehl.

  [NSHELP-29582]

22.2.1.103 (17-Feb-2022)

Behobene Probleme

- Benutzer können das EPA-Plug-In oder das VPN-Plug-In nach einem Upgrade auf Chrome 98 oder Edge 98 nicht starten. Um dieses Problem zu beheben, führen Sie Folgendes aus:

  1. Für das VPN-Plug-In-Upgrade müssen Endbenutzer zum ersten Mal eine Verbindung über den VPN-Client herstellen, um das Update auf ihren Computern zu erhalten. Bei den nachfolgenden Anmeldeversuchen können Benutzer den Browser oder das Plug-In für die Verbindung auswählen.
  2. Für den einzigen Anwendungsfall der EPA verfügen die Endbenutzer nicht über den VPN-Client, um eine Verbindung zum Gateway herzustellen. Führen Sie in diesem Fall Folgendes aus:

     a) Stellen Sie mit einem Browser eine Verbindung zum Gateway her.
     b) Warten Sie, bis die Download-Seite angezeigt wird, und laden Sie die nsepa_setup.exe herunter.
     c) Schließen Sie nach dem Herunterladen den Browser und installieren Sie die Datei nsepa_setup.exe.
     d) Starten Sie den Client neu.

  [NSHELP-30641]

21.12.1.4 (17-Dez-2021)

Was ist neu

- **Änderungen beim Rebranding**

  NetScaler Gateway-Plug-in für Windows wird in Citrix Secure Access Client umbenannt.

  [ACS-2044]

- **Unterstützung für private TCP/HTTP (S) -Anwendungen**

  Der Citrix Secure Access Client unterstützt jetzt private TCP/HTTP (S) -Anwendungen für Remotebenutzer über den Citrix Workspace Secure Access Service.

  [ACS-870]

- **Unterstützung für weitere Sprachen**

  Windows VPN- und EPA-Plug-Ins für NetScaler Gateway unterstützen jetzt die folgenden Sprachen:

  - Koreanisch
  - Russisch
  - Chinesisch (traditionell)

  [CGOP-17721]

- **Citrix Secure Access-Unterstützung für Windows 11**

  Der Citrix Secure Access Client wird jetzt für Windows 11 unterstützt.

  [CGOP-18923]

- **Automatische Übertragungsanmeldung, wenn sich der Benutzer vom selben Computer aus anmeldet und Always on konfiguriert ist**

  Die automatische Anmeldeübertragung erfolgt jetzt ohne Benutzereingriff, wenn Always on konfiguriert ist und sich der Benutzer von demselben Computer aus anmeldet. Zuvor wurde eine Popup-Meldung angezeigt, als sich der Client (Benutzer) in Szenarien wie Systemneustart oder Netzwerkkonnektivitätsproblemen erneut anmelden musste. Der Benutzer musste das Transfer-Login bestätigen. Mit dieser Erweiterung ist das Popup-Fenster deaktiviert.

  [CGOP-14616]

- **Ableiten der Standard-Gateway-IP-Adresse des Citrix Virtual Adapters von der von NetScaler bereitgestellten Netzmaske**

  Die Standard-Gateway-IP-Adresse von Citrix Virtual Adapter wird jetzt von der von NetScaler bereitgestellten Netzmaske abgeleitet.

  [CGOP-18487]

Behobene Probleme

- Manchmal verlieren Benutzer den Internetzugriff, nachdem ein VPN-Tunnel im Modus “Split-Tunnel EIN”eingerichtet wurde. Die fehlerhafte Standardroute des Citrix Virtual Adapters verursacht dieses Netzwerkproblem.

  [NSHELP-26779]

- Wenn der geteilte Tunnel auf "Reverse"eingestellt ist, schlägt die DNS-Auflösung für die Intranetdomänen fehl.

  [NSHELP-29371]

21.9.100.1 (30-Dez-2021)

Was ist neu

- **Citrix Secure Access-Unterstützung für Windows 11**

  Der Citrix Secure Access Client wird jetzt für Windows 11 unterstützt.

  [CGOP-18923]

Behobene Probleme

- Manchmal verlieren Benutzer den Internetzugriff, nachdem ein VPN-Tunnel im Modus "Split-Tunnel EIN"eingerichtet wurde. Die fehlerhafte Standardroute des Citrix Virtual Adapters verursacht dieses Netzwerkproblem.

  [NSHELP-26779]

- Wenn der geteilte Tunnel auf "Reverse"eingestellt ist, schlägt die DNS-Auflösung für die Intranetdomänen fehl.

  [NSHELP-29371]

21.9.1.2 (04-Okt-2021)

Behobene Probleme

- Manchmal kann der DNS-Resolver nach dem Trennen des VPN die Hostnamen nicht auflösen, da die DNS-Suffixe während der VPN-Trennung entfernt werden.

  [NSHELP-28848]

- Manchmal wird ein Benutzer innerhalb weniger Sekunden bei NetScaler Gateway abgemeldet, wenn das Timeout im Leerlauf des Clients festgelegt ist.

  [NSHELP-28404]

- Das Windows-Plug-In kann während der Authentifizierung abstürzen.

  [NSHELP-28394]

- Im Dienstmodus Always On kann das VPN-Plug-In für Windows den Benutzertunnel nicht automatisch einrichten, nachdem sich die Benutzer an ihren Windows-Computern angemeldet haben.

  [NSHELP-27944]

- Nach dem Tunnelaufbau fügt das Windows-Plug-In die Routen mit der Standard-Gateway-Adresse hinzu, anstatt DNS-Serverrouten mit der vorherigen Gateway-IP-Adresse hinzuzufügen.

  [NSHELP-27850]

V21.7.1.1 (27-Aug-2021)

Was ist neu

- **Neuer MAC-Adressscan**

  Unterstützung für neuere MAC-Adressscans wurde hinzugefügt.

  [CGOP-16842]

- **EPA-Scan, um nach Windows OS und seiner Build-Version zu suchen**

  EPA-Scan hinzugefügt, um nach Windows OS und seiner Build-Version zu suchen.

  [CGOP-15770]

- **EPA-Scan zur Überprüfung der Existenz eines bestimmten Werts**

  Eine neue Methode im Registrierungs-EPA-Scan prüft jetzt, ob ein bestimmter Wert existiert.

  [CGOP-10123]

Behobene Probleme

- Wenn während der Anmeldung aufgrund eines Netzwerkfehlers ein JavaScript-Fehler auftritt, schlagen nachfolgende Anmeldeversuche mit demselben JavaScript-Fehler fehl.

  [NSHELP-27912]

- Der EPA-Scan schlägt für die Überprüfung der letzten Aktualisierung von McAfee Antivirus fehl.

  [NSHELP-26973]

- Manchmal verlieren Benutzer den Internetzugang, nachdem ein VPN-Tunnel eingerichtet wurde.

  [NSHELP-26779]

- Während der nFactor-Authentifizierung wird möglicherweise ein Skriptfehler für das VPN-Plug-In angezeigt.

  [NSHELP-26775]

- Bei einer Netzwerkunterbrechung fällt der UDP-Datenverkehr, der vor der Netzwerkunterbrechung begann, nicht für bis zu 5 Minuten ab.

  [NSHELP-26577]

- Es kann zu einer Verzögerung beim Start des VPN-Tunnels kommen, wenn die DNS-Registrierung länger als erwartet dauert.

  [NSHELP-26066]

V21.3.1.2 (31-Mar-2021)

Was ist neu

- **Aktualisierte EPA-Bibliotheken**

  Die EPA-Bibliotheken wurden aktualisiert, um die neueste Version der in EPA-Scans verwendeten Softwareanwendungen zu unterstützen.

  [NSHELP-26274]

- **Kompatibilität mit virtuellen NetScaler Gateway-Adaptern**

  Der virtuelle NetScaler Gateway-Adapter ist jetzt mit virtuellen Direktadaptern Hyper-V und Microsoft Wi-Fi kompatibel (wird mit Druckern verwendet).

  [NSHELP-26366]

Behobene Probleme

- Das Windows VPN-Gateway-Plug-In blockiert die Verwendung von “STRG + P”und “STRG + O” über den VPN-Tunnel.

  [NSHELP-26602]

- Das NetScaler Gateway Plug-In für Windows reagiert nur mit einer im Active Directory registrierten Intranet-IP-Adresse, wenn eine `"nslookup"`-Aktion für den Computernamen angefordert wird.

  [NSHELP-26563]

- Die IIP-Registrierung und -Abmeldung schlägt zeitweise fehl, wenn das geteilte DNS als “Lokal” oder “Beide”festgelegt ist.

  [NSHELP-26483]

- Die automatische Anmeldung am Windows VPN-Gateway-Plug-In schlägt fehl, wenn Always On konfiguriert ist.

  [NSHELP-26297]

- Das Windows VPN-Gateway-Plug-In kann IPv6-DNS-Pakete nicht löschen, was zu Problemen mit der DNS-Auflösung führt.

  [NSHELP-25684]

- Das Windows VPN-Gateway-Plug-In behält die vorhandene Proxy-Ausnahmeliste bei, auch wenn die Liste aufgrund der Browserbeschränkung in der Internet Explorer-Proxy-Ausnahmeliste

  [NSHELP-25578]

- Das Windows VPN-Gateway-Plug-In kann die Proxy-Einstellungen nicht wiederherstellen, wenn der VPN-Client im Always-Ein-Modus abgemeldet ist.

  [NSHELP-25537]

- Das VPN-Plug-In für Windows richtet den Tunnel nach der Anmeldung bei Windows nicht ein, wenn die folgenden Bedingungen erfüllt sind:

  - Das NetScaler Gateway-Gerät ist für die Funktion Always On konfiguriert.
  - Die Appliance ist für zertifikatbasierte Authentifizierung mit Zwei-Faktor-Authentifizierung “aus”konfiguriert.

  [NSHELP-23584]

Microsoft Edge WebView-Unterstützung für Windows Citrix Secure Access —Tech Preview

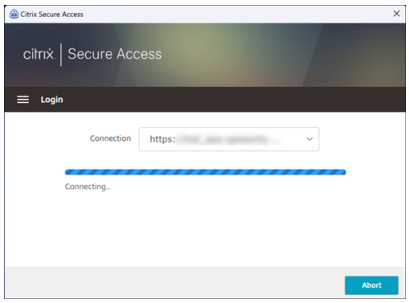
March 27, 2024

Microsoft Edge WebView ist jetzt das von Microsoft empfohlene WebView, da der Internet Explorer WebView veraltet ist. Wir empfehlen Ihnen, den Citrix Secure Access Client 23.8.1.5 oder neuere Versionen zu verwenden, um die Funktionen von Microsoft Edge WebView zu nutzen.

Derzeit ist Microsoft Edge WebView standardmäßig deaktiviert. Sie können sich für die Vorschau anmelden unter https://podio.com/webforms/28291989/2245437.

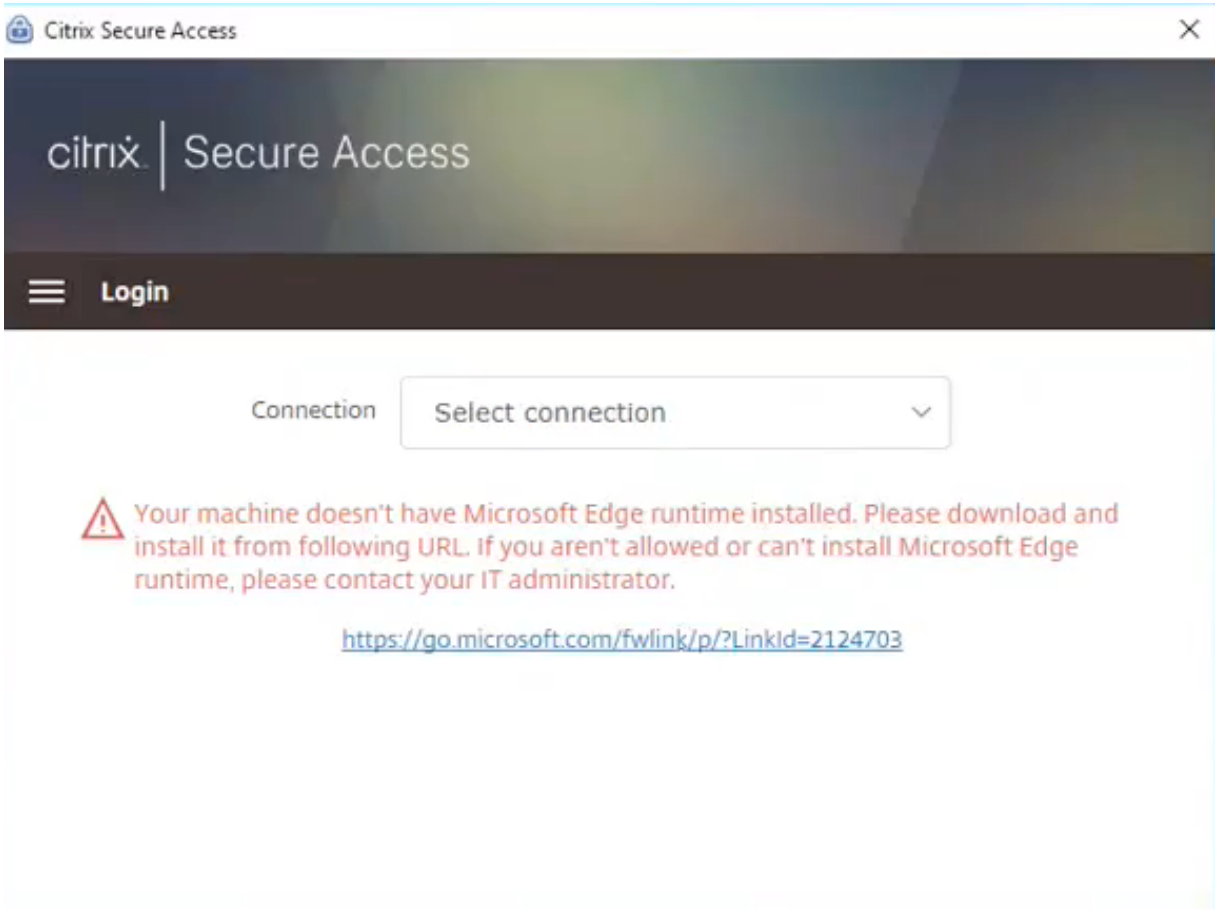
Änderungen für den Endbenutzer

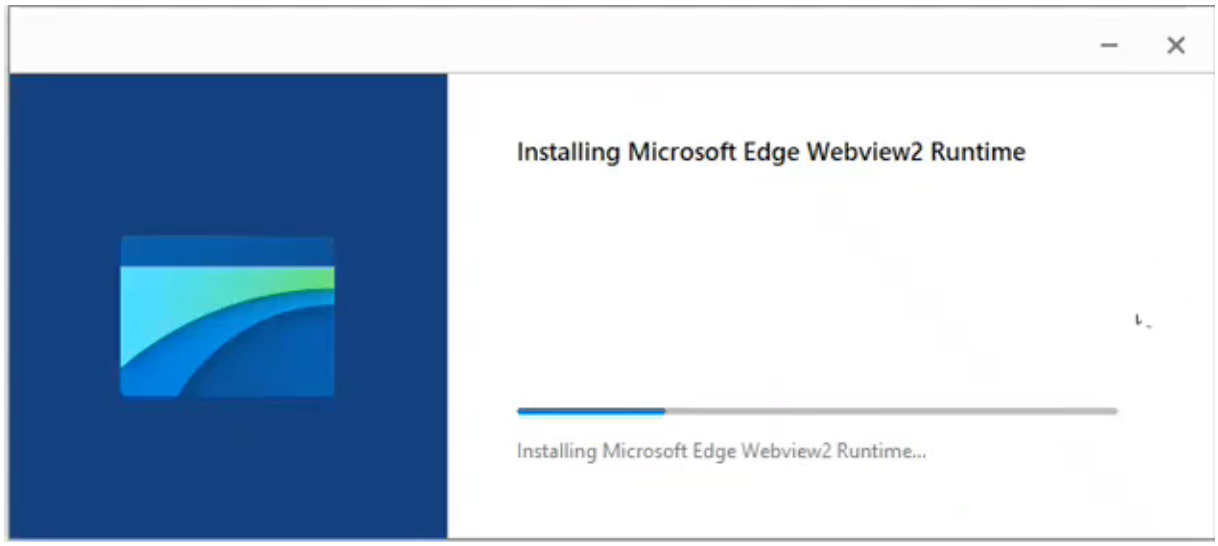
Die Authentifizierungsbildschirme der Citrix Secure Access Client-Benutzeroberfläche sehen wie folgt aus.



Sobald die Endbenutzer die URL ausgewählt haben, öffnet der Citrix Secure Access Client ein neues Fenster, in dem sie aufgefordert werden, sich mit ihren Anmeldeinformationen bei NetScaler Gateway anzumelden.

Wenn auf dem Windows-Client-Computer die Microsoft Edge WebView-Laufzeit nicht installiert ist, erhalten Endbenutzer auf der Benutzeroberfläche des Citrix Secure Access Clients einen Link, über den sie die Microsoft Edge WebView-Laufzeit herunterladen und installieren können. Endbenutzer können die Edge WebView-Laufzeit problemlos herunterladen und installieren, wenn sie mit dem VPN verbunden sind, und die Authentifizierung wird während dieses Vorgangs nicht unterbrochen.





Hinweise:

- Die Microsoft Edge WebView-Funktionalität hat keine Auswirkungen auf administratorspezifische Konfigurationen.
- Wir empfehlen, die HttpOnly-Cookiefunktion zu aktivieren, wenn Sie Edge WebView auf Cit-

> rix Secure Access verwenden. Dies verbessert die NetScaler Gateway-Anmeldedauer, wenn EPA als Faktor im nFactor-Flow verwendet wird.

Problembehandlung

- Wenn Sie Probleme mit dieser Funktion haben, wenden Sie sich an den Citrix Support.
- Sie können Ihr Feedback zur Edge WebView-Funktion über einreichen citrixgatewaybetafeedback@cloud.com.

Verbesserte Protokollerfassung für den Windows-Client

March 27, 2024

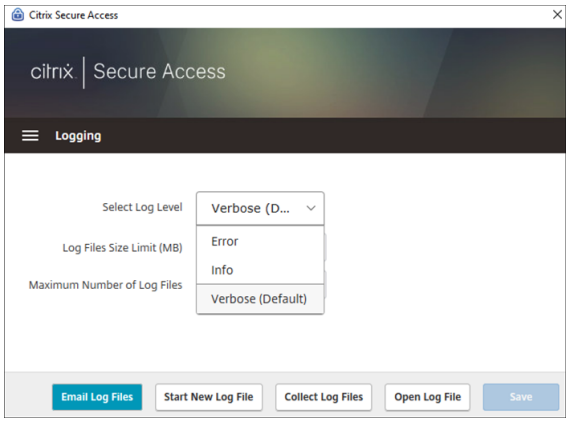
Die Protokollierungsfunktion für den Windows Secure Access Client wurde um eine verbesserte Protokollerfassung und ein verbessertes Debugging erweitert. Die neuen Logdateien haben das Präfix "csa_".

Ab Citrix Secure Access Client für Windows 23.10.1.7 ist die Standardprotokollebene für eine erweiterte Protokollerfassung und Problembehandlung auf "Ausführlich"festgelegt.

Mit diesen Änderungen können Administratoren und Endbenutzer Protokolle der aktuellen Sitzung sowie früherer Sitzungen sammeln. Bisher war die Erfassung von Protokollen nur auf die aktuellen Sitzungen beschränkt.

Protokollierung mit der Citrix Secure Access Client-Benutzeroberfläche konfigurieren

1. Installieren Sie den Secure Access Client für Windows.
2. Klicken Sie im Menü auf **Logging**. Alle Konfigurationen im Zusammenhang mit Protokollen können im Logging-Bildschirm vorgenommen werden.



- **Wählen Sie Log Level aus:**

  Wenn der neue Protokollierungsmechanismus aktiviert ist, sind die folgenden drei Protokollebenen verfügbar.

  - Fehler: Nur von der Anwendung gemeldete Ausnahmen oder Fehler werden protokolliert.
  - Information: Diese Ebene enthält Informationsmeldungen und Ereignisse, die für die Programmausführung relevant sind. Es enthält auch Fehler und Ausnahmen.
  - Ausführlich (Standard): Diese Stufe umfasst alle Protokollmeldungen, die von den Protokollebenen Error und Info gemeldet wurden, sowie zusätzliche Meldungen, die bei der Problembehandlung hilfreich sein könnten.

- **Größenbeschränkung für Protokolldateien:** (Obligatorisch) Geben Sie die Größe der Protokolldateien für jede Protokolldatei ein. Der Maximalwert beträgt 600 MB.
- **Maximale Anzahl von Protokolldateien:** (Obligatorisch) Geben Sie die Anzahl der Dateien ein, die Sie für die Protokollerfassung hinzufügen möchten. Der Maximalwert ist 5.
- **E-Mail-Protokolldateien** —Senden Sie die Protokolldateien per E-Mail an die registrierte E-Mail-ID.
- **Neue Protokolldatei starten** —Wenn Sie diese Option auswählen, wird eine neue Protokolldatei erstellt.
- **Protokolldateien sammeln** —Klicken Sie hier, um eine Zip-Datei mit allen Protokolldateien aus der Anwendung zu erstellen. Diese Zip-Datei wird auf dem Desktop des Clients gespeichert.
- **Protokolldateien öffnen** —Wenn Sie diese Option auswählen, wird die neueste Datei `csa_nssslvpn*.txt` geöffnet.

Citrix Secure Access-Client für Linux

March 27, 2024

Der Citrix Secure Access-Client für Linux ist eine von NetScaler Gateway verwaltete VPN-Clientsoftware, mit der Benutzer remote auf Unternehmensdaten und -anwendungen zugreifen können. Der Citrix Secure Access-Client schützt Anwendungen vor unbefugtem Zugriff, Bedrohungen auf Anwendungsebene und browserbasierten Angriffen.

Der Citrix End Point Analysis-Client (EPA-Client) ist eine Clientsoftware, die von NetScaler Gateway verwaltet wird. Er überprüft die Endpunktkriterien, bevor über NetScaler Gateway der Zugriff auf Unternehmensdaten gewährt wird. Der Citrix EPA-Client und der Citrix Secure Access-Client sind voneinander unabhängig.

> **Hinweis:**
>
> Auch wenn Sie EPA nicht verwenden, empfehlen wir, die EPA- und VPN-Plug-in-Binärdateien zusammen zu aktualisieren, falls Sie die EPA-Funktion später verwenden möchten.

Unterstützte Linux-Versionen

Der Citrix Secure Access-Client und der Citrix EPA-Client sind mit den Versionen Ubuntu 18.04, Ubuntu 20.04 und Ubuntu 22.04 kompatibel. Weitere Informationen zu den unterstützten Browsern finden Sie unter Anforderungen an die Clientsoftware.

> **Hinweis:**
>
> Damit Ubuntu 22.04 mit dem Citrix Secure Access Client und dem Citrix EPA-Client funktioniert, legen Sie den SSL-Parameter `denySSLReneg` auf der NetScaler CLI auf `NONSECURE` fest.

Unterstützte Features

Der Citrix Secure Access Client für Ubuntu unterstützt die folgenden Funktionen:

- Split-Tunneling und Reverse-Split-Tunneling
- Tunneling von TCP-, UDP- und ICMP-Anwendungen
- Serverinitiierte Verbindungen über Intranet-IP (IIP)
- Geteilte DNS-Fernbedienung
- Clientseitiger Proxy
- Klassische EPA-Scans
- Erweiterte Authentifizierung (nFactor) einschließlich erweiterter EPA-Scans (nur über den Browser)
- Nur Http-Cookies
- Globaler Serverlastenausgleich (GSLB)

> **Hinweis:**
>
> Split DNS BOTH wird vom Citrix Secure Access Client für Ubuntu nicht unterstützt.

Aktualisieren Sie Ubuntu-Clients auf NetScaler Gateway

Sie können den Citrix Secure Access Client und den Citrix EPA-Client für Ubuntu von der Download-Seite herunterladen.

Der Citrix Secure Access Client und der Citrix EPA-Client haben die Namen “nsgclient18_64.deb”bzw. “nsepa18.deb“. Die Clients sind sowohl mit Ubuntu 18.04 als auch mit 20.04 kompatibel.

Der Citrix Secure Access Client und der Citrix EPA-Client, die Ubuntu 22.04 unterstützen, heißen “nsginstaller64.deb”bzw. “nsepa.deb“.

Wenn Sie beispielsweise von Version 1.0.0.x auf Version 23.6.1 auf die neueste Version des Citrix Secure Access Clients aktualisieren möchten, gehen Sie wie folgt vor:

1. Ersetzen Sie die Dateien “nsgclient18_64.deb”und “nsginstaller64.deb”unter /var/netscaler/gui/vpn/scripts/linux/ mithilfe der Shell-Eingabeaufforderung.
2. Ersetzen Sie die Dateien “nsepa18.deb”und “nsepa.deb”unter /var/netscaler/gui/epa/scripts/linux/ mithilfe der Shell-Eingabeaufforderung.
3. Öffnen Sie die Datei /var/netscaler/gui/vpn/scripts/linux/clientversions.xml.

    a) Ersetzen Sie für den Citrix EPA-Client die aktuelle Version (1.0.0.x) in den folgenden XML-Tags durch die neueste Version (23.6.1). Wenn die XML-Tags nicht existieren, fügen Sie sie der XML-Datei hinzu. Beispiel:

    ersetzen

    ```
    <component pkgname="nsepa18"currentversion="1.0.0.x"minversion
    ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/
    nsepa18.deb"/>
    ```

    mit

    ```
    <component pkgname="nsepa18"currentversion="23.6.1"minversion
    ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/
    nsepa18.deb"/>
    ```

    und ersetzen

    ```
    <component pkgname="nsepa22"currentversion="1.0.0.x"minversion
    ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
    .deb"/>
    ```

    mit

    ```
    <component pkgname="nsepa22"currentversion="23.6.1"minversion
    ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
    ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
    .deb"/>
    ```


b) Ersetzen Sie für den Citrix Secure Access Client die aktuelle Version (1.0.0.x) in den folgenden XML-Tags durch die neueste Version (23.6.1). Wenn die XML-Tags nicht existieren, fügen Sie sie der XML-Datei hinzu. Beispiel:

ersetzen

```
<component pkgname="nsgclient18"currentversion="1.0.0.x"
minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
"maxkernelversion="5.16"updatetype="compatible"action="/vpn/
scripts/linux/nsgclient18_64.deb"/>
```

nach

```
<component pkgname="nsgclient18"currentversion="23.6.1"minversion
="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
="5.16"updatetype="compatible"action="/vpn/scripts/linux/
nsgclient18_64.deb"/>
```

und

```
<component pkgname="nsgclient22"currentversion="1.0.0.x"
minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
"maxkernelversion="5.20"updatetype="compatible"action="/vpn/
scripts/linux/nsginstaller64.deb"/>
```

nach

```
<component pkgname="nsgclient22"currentversion="23.6.1"minversion
="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
="5.20"updatetype="compatible"action="/vpn/scripts/linux/
nsginstaller64.deb"/>
```

4. Führen Sie an der NetScaler-Shell-Eingabeaufforderung die folgenden Befehle aus:

```
1 rm -rf /netscaler/ns_gui
2 ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. Führen Sie auf der NetScaler CLI die folgenden Befehle aus:

```
1 set vpn parameter -clientversions all
2 flush cache contentgroup loginstaticobjects
```

Referenzen

- NetScaler Gateway VPN-Clients und unterstützte Funktionen
- Endpunktanalyse-Scans, die für Ubuntu unterstützt werden
- Hilfedokumentation für Endbenutzer

Versionshinweise zu Citrix Secure Access für Linux

March 27, 2024

Der Citrix Secure Access Client und der Citrix End Point Analysis (EPA) -Client für Linux werden jetzt eigenständig veröffentlicht und sind mit allen NetScaler-Versionen kompatibel. Die Citrix Secure Access Clientversion folgt dem Format JJ.MM Release.Build.

In den Versionshinweisen werden die neuen Funktionen, Verbesserungen der vorhandenen Funktionen, behobene Probleme und bekannte Probleme beschrieben.

Was ist neu: Die neuen Funktionen und Verbesserungen, die in der aktuellen Version verfügbar sind.

Behobene Probleme: Die Probleme, die in der aktuellen Version behoben wurden.

Bekannte Probleme: Die in der aktuellen Version vorhandenen Probleme und deren Problemumgehungen, sofern zutreffend.

Ausführliche Informationen zu den unterstützten Funktionen finden Sie in der NetScaler Gateway-Produktdokumentation.

23.10.3 (16. Oktober 2023)

Behobene Probleme

Für französische Benutzer wird auf der Verbindungsseite der Benutzeroberfläche von Citrix Secure Access für Linux die Datenübertragungsrate in KB und MB statt in Ko bzw. Mo angezeigt.

[NSOSLX-177]

23,9,1 (08-Sep-2023)

Was ist neu

In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

[CGOP-25231]

23.6.2 (20. Juni 2023)

Was ist neu

- **Ubuntu 22.04-Unterstützung für den Citrix Secure Access-Client und den Citrix EPA-Client**

  Ubuntu 22.04 ist die neueste Version von Ubuntu mit langfristiger Unterstützung. Die Citrix Secure Access- und Citrix EPA-Clients sind mit Ubuntu 22.04 kompatibel. Weitere Informationen finden Sie unter Anforderungen an die Clientsoftware.

  [CGOP-24312]

- **GSLB-Unterstützung für Citrix Secure Access- und Citrix EPA-Clients**

  Der Citrix Secure Access Client und der Citrix EPA-Client für Ubuntu unterstützen die Funktion Global Server Load Balancing (GSLB) auf NetScaler Gateway. Durch die Konfiguration von GSLB für NetScaler Gateway können Administratoren sicherstellen, dass das Unternehmensnetzwerk (Intranetressourcen) Endbenutzern von jedem geografischen Standort aus immer zur Verfügung steht. GSLB behebt auch Katastrophensituationen oder Netzwerkausfälle, bei denen Benutzer eines Rechenzentrums zu einem anderen Rechenzentrum umgeleitet werden können. Weitere Informationen finden Sie unter Unterstützung für aktiv-aktive GSLB-Bereitstellungenauf NetScaler Gateway.

  [CGOP-23506]

- **HTTPOnly-Unterstützung für Citrix Secure Access- und Citrix EPA-Clients**

  Die Citrix Secure Access- und Citrix EPA-Clients unterstützen das HTTPOnly-Flag auf den Authentifizierungscookies. NetScaler Gateway-Administratoren konfigurieren die HTTPOnly-Funktion für die Authentifizierungscookies, die von Webanwendungen generiert werden. Diese Funktion hilft dabei, Cookie-Diebstahl aufgrund von Cross-Site Scripting zu verhindern. Weitere Informationen finden Sie unter Erzwingen des HTTPOnly-Flags für Authentifizierungscookies.

  [CGOP-23517]