

NetScaler Gatewayクライアント

Contents

NetScaler Gateway VPNクライアントとサポートされる機能	15
リファレンス	19
macOS/iOS向けCitrix Secure Access	20
macOS/iOS向けCitrix Secure Accessクライアントの主な機能	20
リリースノート	21
V24.07.1 (2024年7月15日)	22
新機能	22
V24.06.2 (2024年6月27日)	22
新機能	22
V24.06.1 (2024年6月24日)	22
新機能	22
解決された問題	23
24.6.1 macOS 用 EPA クライアント (18 Jun 2024)	23
新機能	23
V24.04.1 (2024年4月18日)	23
新機能	23
V24.03.1 (2024年3月14日)	23
新機能	23
V24.02.1 (2024年2月15日)	24
新機能	24
24.1.5 MacOS 用 EPA クライアント (2024 年 2 月 12 日)	25
新機能	25
V23.12.2 (2023年12月20日)	25
新機能	25
V23.12.1 (2023 年 12 月 6 日)	25
新機能	25

V23.11.2 (2023 年 11 月 1 日)	26
新機能	26
V23.11.1 (2023 年 10 月 27 日)	26
新機能	26
V23.10.2 (2023 年 10 月 17 日)	26
V23.10.1 (2023 年 10 月 9 日)	26
新機能	26
V23.09.1 (2023 年 9 月 7 日)	27
新機能	27
V23.08.1 (2023 年 8 月 24 日)	27
新機能	27
23.7.6 macOS 用 EPA クライアント (2023 年 8 月 10 日)	27
V23.07.1 (2023 年 7 月 17 日)	28
新機能	28
解決された問題	28
V23.06.1 (2023 年 6 月 7 日)	28
新機能	28
解決された問題	29
既知の問題	29
V23.05.2 (2023 年 5 月 11 日)	29
解決された問題	29
V23.05.1 (2023 年 5 月 4 日)	29
新機能	29
解決された問題	29
V23.04.1 (2023 年 4 月 4 日)	29
新機能	29
V22.12.2 (2023 年 2 月 27 日)	30
新機能	30

V22.12.1 (2022 年 12 月 7 日)	30
V22.11.1 (2022 年 11 月 29 日)	30
解決された問題	30
22.11.3 macOS 用 EPA プラグイン (2022年11月28日)	30
解決された問題	30
V22.10.1 (2022 年 11 月 17 日)	30
新機能	30
解決された問題	30
22.10.1 macOS 用 EPA プラグイン (2022 年 10 月 27 日)	31
新機能	31
V22.06.1 (2022 年 9 月 20 日)	31
新機能	31
解決された問題	31
V3.2.4.9-macOS 用 EPA プラグイン (2022 年 8 月 1 日)	32
解決された問題	32
既知の問題	32
V22.03.1 (14-Jun-2022)	32
新機能	32
解決された問題	32
V22.02.3 (24-Mar-2022)	33
新機能	33
解決された問題	33
既知の問題	33
V22.02.2 (15-Feb-2022)	33
解決された問題	33
V22.01.1 (08-Feb-2022)	34
解決された問題	34
V1.4.1 (28-Jan-2022)	34

新機能	34
解決された問題	34
V1.4.0 (17-Nov-2021)	34
解決された問題	34
V1.3.13 (05-Nov-2021)	35
解決された問題	35
V1.3.12 (21-Oct-2021)	35
解決された問題	35
V1.3.11 (17-Sep-2021)	35
解決された問題	35
V1.3.10 (31-Aug-2021)	36
新機能	36
V1.3.9 (13-Aug-2021)	36
解決された問題	36
V1.3.8 (07-Jul-2021)	36
新機能	36
iOSユーザー向けCitrix Secure Accessのセットアップ	37
MDM 製品との互換性	37
Citrix Secure Access クライアント (macOS/iOS) 用の MDM マネージド VPN プロファイル の設定	37
デバイスレベルの VPN プロファイル	38
アプリごとの VPN プロファイル	39
アプリ単位 VPN での分割トンネルの設定	40
ユーザー作成の VPN プロファイルの無効化	40
DNSハンドリング	41
既知の問題	42
制限事項	42

Mac向けCitrix Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン-プ レビュー	42
前提条件	43
注意事項	43
ユーザー証明書の ID を電子メールの添付ファイルとしてiOS ユーザーに送信する	44
前提条件	44
構成の手順	44
iOSユーザー用のCitrix SSOアプリ用またはmacOSユーザー用のCitrix Secure Accessクライア ント用のプロキシPACファイルのセットアップ	45
プロキシ PAC ファイルを設定する方法	46
macOS ユーザー向けCitrix Secure Accessのセットアップ	46
MDM 製品との互換性	47
Citrix Secure Accessの MDM 管理対象VPNプロファイルを構成する	47
デバイスレベルの VPN プロファイル	48
アプリごとの VPN プロファイル	49
アプリ単位 VPN での分割トンネルの設定	50
ユーザー作成の VPN プロファイルの無効化	50
DNSハンドリング	51
サポートされている EPA スキャン	52
既知の問題	52
制限事項	52
トラブルシューティング	53
macOS/iOS 上の Citrix Secure Accessクライアントの nFactor サポート	53
nFactor 構成	54
制限事項	54
macOS/iOS向けCitrix Secure Accessに関する一般的な問題のトラブルシューティング	54
DNS 解決の問題	55
EPA の問題	55

nFactor の問題	55
ネットワークアクセスコントロール (NAC) チェック	56
よくある質問	56
Android向けCitrix Secure Access	58
リリースノート	58
V25.03.3 (2025年6月30日)	59
修正された問題	59
V25.03.2 (2025年6月13日)	59
新機能	59
V25.03.1 (2025年5月28日)	59
新機能	59
修正された問題	59
V25.02.1 (2025年3月19日)	60
修正された問題	60
V24.11.1 (02-Dec-2024)	60
新機能	60
修正された問題	60
V24.10.1 (10-Oct-2024)	60
新機能	60
修正された問題	60
V24.08.2 (2024年9月26日)	61
新機能	61
V24.08.1 (2024年9月9日)	61
新機能	61
修正された問題	61
V24.04.1 (2024年5月3日)	61
V23.12.2 (2023年12月15日)	62
新機能	62

修正された問題	63
V23.10.2 (2023年12月19日)	63
新機能	63
修正された問題	64
V23.8.1 (31-Aug-2023)	64
新機能	64
修正された問題	64
V22.11.1 (30-Nov-2022)	64
新機能	64
V22.10.1 (2022年10月21日)	65
新機能	65
修正された問題	65
V2.5.3 (2022年5月5日)	65
新機能	65
修正された問題	65
V2.5.2 (21-Oct-2021)	66
修正された問題	66
V2.5.1 (12-Aug-2021)	66
修正された問題	66
V2.5.0 (08-Jun-2021)	66
新機能	66
修正された問題	66
V2.4.16 (2021年3月31日)	67
修正された問題	67
V2.4.15 (2021年3月17日)	67
修正された問題	67
V2.4.14 (2021年2月23日)	67
修正された問題	67

V2.4.13 (2021年2月4日)	67
修正された問題	67
V2.4.12 (2021年1月15日)	67
V2.4.11 (2021年1月8日)	67
V2.4.10 (2020年12月9日)	68
修正された問題	68
V2.4.9 (20-Nov-2020)	68
修正された問題	68
V2.4.8 (04-Nov-2020)	68
修正された問題	68
V2.4.7 (12-Oct-2020)	68
V2.4.6 (28-Sep-2020)	68
V2.4.5 (16-Sep-2020)	68
新機能	68
V2.4.4 (2020年9月10日)	69
修正された問題	69
V2.4.3	69
既知の問題	69
V2.4.2	69
修正された問題	69
V2.4.1	69
修正された問題	69
V2.3.19	69
V2.3.18	69
新機能	69
V2.3.17	70
V2.3.16	70
V2.3.15	70

新機能	70
修正された問題	70
V2.3.14	70
新機能	70
修正された問題	70
既知の問題	71
V2.3.13	71
修正された問題	71
既知の問題	71
V2.3.12	71
修正された問題	71
V2.3.11	71
修正された問題	71
V2.3.10	72
修正された問題	72
V2.3.8	72
新機能	72
修正された問題	72
V2.3.6	72
新機能	72
修正された問題	73
V2.3.1	73
新機能	73
V2.2.9	74
新機能	74
修正された問題	74
MDM環境でのCitrix Secure Accessのセットアップ	74
Intune Android Enterprise環境でCitrix Secure Accessをセットアップする	75

前提条件	75
Intune Android Enterprise環境でCitrix Secure Accessをセットアップするには	75
Citrix Secure Accessを管理対象アプリとして追加	75
Citrix Secure Accessの管理対象アプリケーションポリシーの設定	76
Intune 設定のカスタムパラメータ	86
Intune で Citrix Secure Accessを常時接続の VPN プロバイダーとして設定する	88
参照ドキュメント	88
常時接続 VPN の自動再起動	89
制限事項	89
Android向けCitrix Secure AccessによるNetScaler Gateway証明書ピン留め	90
Android Citrix Secure AccessによるNetScaler Gateway の証明書ピン留めの設定	90
Citrix Secure Access for Windows リリースノート	93
24.6.1.18 (2024年7月24日)	94
新機能	94
解決された問題	95
24.4.1.7 (2024年4月30日)	96
解決された問題	96
24.2.1.15 (2024年3月4日)	97
新機能	97
解決された問題	98
23.10.1.7 (2023年11月29日)	99
新機能	99
解決された問題	100
23.8.1.11 (2023年10月19日)	101
解決された問題	101
23.8.1.5 (2023年8月9日)	101
解決された問題	101
既知の問題	102

23.7.1.1 (2023 年 7 月 14 日)	102
解決された問題	102
23.5.1.3 (2023 年 6 月 2 日)	102
解決された問題	102
23.4.1.5 (2023 年 4 月 14 日)	102
新機能	102
解決された問題	104
23.1.11 (2023 年 2 月 20 日)	104
23.1.1.8 (2023 年 2 月 8 日)	104
解決された問題	104
22.10.1.9 (2022年11月8日)	105
新機能	105
解決された問題	106
既知の問題	107
22.6.1.5 (2022年6月17日)	107
新機能	107
解決された問題	108
22.3.1.5 (2022年3月24日)	109
解決された問題	109
既知の問題	109
22.3.1.4 (2022年3月10日)	109
新機能	109
解決された問題	112
22.1.103 (2022年2月17日)	112
解決された問題	112
21.12.1.4 (17-Dec-2021)	113
新機能	113
解決された問題	114

21.9.100.1 (2021年12月30日)	114
新機能	114
解決された問題	114
21.9.1.2 (04-Oct-2021)	115
解決された問題	115
V21.7.1.1 (27-Aug-2021)	115
新機能	115
解決された問題	115
V21.3.1.2 (31-Mar-2021)	116
新機能	116
解決された問題	116
Technical Previewの機能	117
Windows クライアントのログ収集が改善されました	117
Citrix Secure Accessクライアントユーザーインターフェイスを使用してログを構成する	118
Windows向けCitrix Workspaceアプリを介したCitrix Secure Access への自動シングルサインオン	118
機能	119
前提条件	119
構成	119
Citrix WorkspaceアプリによるCitrix Secure Access のインストールと自動アップデートを有効にする	119
Citrix Workspaceアプリ経由でCitrix Secure Access へのSSOを有効にする	119
制限事項	120
Windows Citrix Secure Accessの Microsoft Edge WebView サポート-プレビュー	120
エンドユーザーへの変更	120
トラブルシューティング	121
Linux向けCitrix Secure Accessクライアント	122
サポートされている Linux バージョン	122

サポートされる機能	122
NetScaler GatewayでのUbuntuクライアントのアップグレード	123
参照ドキュメント	125
Linux向けCitrix Secure Accessリリースノート	126
23.10.3 (2023年10月16日)	126
解決された問題	126
23.9.1 (2023年9月8日)	126
新機能	126
23.6.2 (2023年6月20日)	126
新機能	126

NetScaler Gateway VPNクライアントとサポートされる機能

重要：

- iOS/Android向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。
- レガシー VPN クライアントは Apple のプライベート VPN API を使用して構築されていましたが、現在は廃止されています。macOS/iOS向けCitrix Secure AccessクライアントのVPNサポートは、Appleのパブリックネットワーク拡張フレームワークを使用して書き直されました。iOSおよびmacOS用のNetScaler GatewayプラグインとVPNはサポートされなくなりました。iOS/macOS向けCitrix Secure Accessは、使用することをお勧めするVPNクライアントです。
- Android デバイス用の nFactor 認証サポートの一般提供は、今後のリリースの 1 つで利用可能になる予定です。

次の表に、各 VPN クライアントでサポートされる一般的に使用される機能の一部を示します。

機能	WINDOWS 向けCITRIX SECURE ACCESS	LINUX向け CITRIX SECURE ACCESS	CITRIX SECURE ACCESS FOR MACOS	IOS向け CITRIX SECURE ACCESS	ANDROID向 けCITRIX SECURE ACCESS
常時オン (ユーザー モード)	はい (11.1 以降)	いいえ	いいえ	いいえ	はい (MDM 経由) Android 7.0+
PAC ファイ ル	はい (12.0 以降)	いいえ	はい	はい	いいえ
クライアン トプロキシ のサポート	はい	はい	いいえ	いいえ	はい。注 1 を参照

機能	WINDOWS 向けCITRIX SECURE ACCESS	LINUX向け CITRIX SECURE ACCESS	CITRIX SECURE ACCESS FOR MACOS	IOS向け CITRIX SECURE ACCESS	ANDROID向 けCITRIX SECURE ACCESS
イントラ ネットアプ リケーショ ンの最大制 限	512	128	制限なし	制限なし	制限なし
イントラ ネット IP (IIP) のサ ポート	はい	はい	はい	はい	はい
分割トンネ ル ON	はい	はい	はい	はい	はい
分割トンネ ルのリバー ス	はい	はい	はい	はい	はい。注 5 を参照
スプリット DNS リモコ ン	いいえ	はい	はい	はい	はい。注 6 を参照
スプリット DNS 両方	はい	いいえ	はい	はい	はい。注 6 を参照
FQDN ベー スの分割ト ンネル	はいオン専 用 (13.0 以 降)	いいえ	はい	はい	はい。注 5 を参照
クライアントのアイドルタイムアウト	はい	はい	はい	いいえ	いいえ
エンドポイ ント分析	はい	はい	はい	いいえ	いいえ

機能	WINDOWS 向けCITRIX SECURE ACCESS	LINUX向け CITRIX SECURE ACCESS	CITRIX SECURE ACCESS FOR MACOS	IOS向け CITRIX SECURE ACCESS	ANDROID向 けCITRIX SECURE ACCESS
デバイス証 明書 (クラ シック)	はい	いいえ	はい	いいえ	いいえ
nFactor認証	はい (12.1 以降)	いいえ	はい	はい	はい。注3 を参照
EPA (nFactor)	はい (12.1 以降)	いいえ	はい	いいえ	いいえ
デバイス証 明書 (nFactor)	はい (12.1 以降)	いいえ	はい	いいえ	いいえ
プッシュ通 知	はい (12.1 以降)	いいえ	いいえ	はい	はい
OTP トーク ンの自動入 力のサポー ト。注2を 参照	いいえ	いいえ	いいえ	はい	はい
TLS 1.3のサ ポート	はい	はい	はい	はい (デフォ ルトでは無 効。ご要望 に応じてご 利用いただ けます。)	はい (デフォ ルトでは無 効。ご要望 に応じてご 利用いただ けます。)
DTLS サ ポート。注 4を参照	はい (13.0 以降)	いいえ	はい	はい	いいえ
HTTP のみ のクッキー	はい	はい	はい	はい	はい

機能	WINDOWS 向けCITRIX SECURE ACCESS	LINUX向け CITRIX SECURE ACCESS	CITRIX SECURE ACCESS FOR MACOS	IOS向け CITRIX SECURE ACCESS	ANDROID向 けCITRIX SECURE ACCESS
広域サー バー負荷分 散（Global Server Load Balancing： GSLB）	はい	はい	はい	はい	はい
ローカル LANアクセ ス	はい	いいえ	常に有効	常に有効	いいえ

注：

1. Android 10 以降のゲートウェイ構成の VPN 仮想サーバー上のクライアント構成でのプロキシの設定がサポートされています。IP アドレスとポートを持つ基本的な HTTP プロキシ設定のみがサポートされています。
2. QRコードをスキャンしたトークンのみが自動入力の対象となります。自動入力は nFactor 認証フローではサポートされていません。
3. Android デバイスの nFactor 認証サポートはプレビュー段階にあり、この機能はデフォルトで無効になっています。この機能を有効にするには、NetScalerサポートにお問い合わせください。Androidデバイス用のnFactor認証を有効にするには、NetScaler Gateway の FQDNをサポートチームに提供する必要があります。
4. 詳細については、[SSL VPN 仮想サーバーを使用した DTLS VPN 仮想サーバーの設定を参照してください](#)。
5. Android デバイスの FQDN ベースの分割トンネルのサポートとリバース分割トンネルはプレビュー中で、この機能はデフォルトで無効になっています。この機能を有効にするには、NetScalerサポートにお問い合わせください。Androidデバイスで有効にするには、NetScaler Gateway の FQDNをサポートチームに提供する必要があります。
6. Split DNS BOTH モードでは、DNS サフィックスをゲートウェイに設定する必要があり、そのサフィックスで終わる DNS A レコードクエリだけがゲートウェイに送信されます。残りのクエリはローカルで解決されます。Android向けCitrix Secure Accessは、スプリットDNSローカルモードもサポートしています。

リファレンス

[エンドユーザー向けヘルプドキュメント](#)

macOS/iOS向けCitrix Secure Access

レガシー VPN クライアントは Apple のプライベート VPN API を使用して構築されていましたが、現在は廃止されています。macOSおよびiOS向けCitrix Secure AccessのVPNサポートは、Appleのパブリックネットワーク拡張フレームワークを使用してゼロから書き直されました。

注

- iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。
- macOS向けCitrix Secure Accessは、10.15 (Catalina) 、11.x (Big Sur) 、12.x (Monterey) 、13.x (Ventura) 、14.x (Sonoma) でサポートされています。IntelチップとAppleチップを搭載したデバイスをサポートします。
- 前述のバージョン (macOS 10.15およびmacOS 11.0) のいずれかにアップグレードできないハードウェアを使用しているユーザーは、App Storeで最後に互換性のあるバージョンにアクセスできますが、古いバージョンへのアップデートはありません。
- macOS ユーザーが App Store アプリと TestFlight プレビュービルドを切り替えたり、その逆に切り替えたりした場合、ユーザーは次の手順を実行して接続プロファイルを再作成する必要があります：
 - a. Click the hamburger menu and then click **Configuration**.
 - b. Delete the profile from the list and add the same profile again.

macOS/iOS向けCitrix Secure Accessクライアントの主な機能

- **パスワードトークン**：パスワードトークンは、VIP、OKTAなどのセカンダリパスワードサービスの代替となる6桁のコードです。このコードは、時間ベースのワンタイムパスワード (T-OTP) プロトコルを使用して、Google Authenticatorや Microsoft Authenticator システムなどのサービスと同様の OTP コードを生成します。ユーザーは、特定のActive Directory ユーザーのNetScaler Gateway への認証中に2つのパスワードの入力を求められます。2 目目の要因は、ユーザーが Google や Microsoft Authenticator などの登録済みのサードパーティサービスからデスクトップブラウザにコピーする 6 桁のコードです。ユーザーは、まずNetScaler ADCア

プライアンスでT-OTPに登録する必要があります。登録手順については、[<https://support.citrix.com/article/CTX228454>](https://support.citrix.com/article/CTX228454) を参照してください。アプリでは、NetScaler ADCで生成されたQRコードをスキャンするか、TOTPシークレットを手動で入力して、OTP機能を追加できます。一度追加された OTP トークンは、ユーザーインターフェイスのパスワードトークンセグメントに表示されます。

エクスペリエンスを向上させるために、OTP を追加すると、VPN プロファイルを自動的に作成するようにユーザーに求められます。ユーザーは、この VPN プロファイルを利用して、iOS デバイスから直接 VPN に接続できます。

macOS/iOS向けCitrix Secure Accessクライアントを使用すると、ネイティブOTPサポートへの登録時にQRコードをスキャンできます。NetScaler Gatewayのプッシュ通知機能は、macOS/iOS向けCitrix のセキュアアクセスユーザーのみが使用できます。

- **プッシュ通知：** NetScaler Gateway は、登録されたモバイルデバイスでプッシュ通知を送信し、簡素化された2要素認証エクスペリエンスを実現します。macOS/iOS向けCitrix Secure Accessクライアントを起動してNetScalerのログオンページに第2ファクタのOTPを設定する代わりに、登録されたデバイスのデバイスPIN/Touch ID /フェイスIDを入力することで本人確認を行うことができます。

デバイスをプッシュ通知用に登録すると、そのデバイスをmacOS/iOS向けCitrix Secure Accessを使用してネイティブOTPサポートに使用することもできます。プッシュ通知の登録は、ユーザーに対して透過的に行われます。ユーザーがTOTPを登録すると、NetScaler ADCがサポートしている場合、デバイスはプッシュ通知用にも登録されます。

リリースノート

リリースノートでは、サービスリリースで利用できる新機能、既存機能の拡張、修正された問題、既知の問題について説明します。リリースノートには、次のセクションの1つまたは複数が含まれます：

新機能:現在のリリースで利用できる新機能と拡張機能。

修正された問題:現在のリリースで修正された問題。

既知の問題:現在のリリースに存在する問題とその回避策 (該当する場合)。

重要な情報:

- EPA クライアントは macOS 10.13、10.14、10.15、11.x、12.x、13.x の各バージョンでサポートされています。
- EPAクライアントは、NetScaler 12.1、13.0、13.1、および14.1のバージョンでサポートされています。
- Citrix Secure Access for macOS/iOS 24.06.1 以降のリリースでは、CVE-2024-3661 で説明されている TunnelVision の脆弱性が解決されています。

V24.07.1 (2024年7月15日)**新機能**

- EPA ライブラリが 24.06.1.0 (OPSWAT OESIS ライブラリ V 4.3.3612.0) に更新されました。
- このリリースでは、全体的なパフォーマンスと安定性を向上させるためのいくつかの問題が修正されています。

V24.06.2 (2024年6月27日)**新機能**

このリリースでは、IPv6 ログインの問題が解決されています。

V24.06.1 (2024年6月24日)**新機能**

- このリリースは、CVE-2024-3661 で説明されているトンネルビジョンの脆弱性に対処します。
- このリリースでは、全体的なパフォーマンスと安定性を向上させるためのいくつかの問題が修正されています。
- EPA ライブラリが 24.05.2.0 (OPSWAT OESIS ライブラリ V 4.3.3586.0) に更新されました。
- EPA スキャンによるCitrix Workspaceアプリのバージョンの確認

Citrix Secure Accessは、macOSマシン上のCitrix Workspaceのバージョンを検証する新しいEPAスキャン **CWA Version** をサポートしています。サポートされている EPA スキャンの詳細については、「[式文字列](#)」を参照してください。

- サードパーティのセキュア Web ゲートウェイとの相互運用性の強化

Citrix Secure Accessのユーザーエージェント文字列が更新され、サードパーティのセキュア Webゲートウェイとの相互運用性が強化されました。

解決された問題

- リバーススプリットトンネリングを使用するアプリごとのVPNが有効になっている場合、Citrix Secure Accessは除外されたアプリのVPNトンネルをバイパスできません。

24.6.1 macOS 用 EPA クライアント (18 Jun 2024)

新機能

- EPA スキャンによるCitrix Workspaceアプリのバージョンの確認

Citrix EPAクライアントは、macOSマシン上のCitrix Workspaceバージョンを検証する新しいスキャン「CWAバージョン」をサポートしています。サポートされている EPA スキャンの詳細については、「[式文字列](#)」を参照してください。

V24.04.1 (2024年4月18日)

新機能

- EPA ライブラリが 24.04.1.0 (OPSWAT OESIS ライブラリ V 4.3.3503.0) に更新されました。
- このリリースでは、全体的なパフォーマンスと安定性を向上させるためのいくつかの問題が修正されています。

V24.03.1 (2024年3月14日)

新機能

- EPA ライブラリが 24.03.1.0 (OPSWAT OESIS ライブラリ V 4.3.3460.0) に更新されました。
- Citrix Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン (SSO) -プレビュー

macOS向けCitrix Secure Accessは、Citrix WorkspaceアプリにログインしたときのCitrix Secure Accessへの自動シングルサインオン（SSO）をサポートするようになりました。この機能を利用するには、必ずmacOS 24.03.1向けのCitrix Secure AccessとMac 2402以降のCitrix Workspaceアプリを使用してください。この機能はクラウドストアでのみサポートされ、オンプレミスストアではサポートされません。

- 。現在、この機能はデフォルトで無効になっています。 <https://podio.com/webforms/29383411/2410629> を使用してプレビューにサインアップできます。
- 。管理者およびエンドユーザーの手順については、「Mac向けCitrix [Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン-プレビュー](#)」を参照してください。
- 。エンドユーザー向けの手順については、「Citrix [Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン](#)」を参照してください。

• 全体的なパフォーマンスと安定性の向上

Citrix Secure Accessクライアントは、全体的なパフォーマンスと安定性を向上させるために、次の機能で強化されています：

- 。VPN 経由でトンネリングできる同時接続数の増加。これは iOS クライアントにのみ適用されます。
- 。IPv6 ゲートウェイによる VPN 接続の耐障害性が向上しました。これは macOS クライアントと iOS クライアントの両方に適用されます。

V24.02.1 (2024年2月15日)

新機能

• Mac クライアントでの EPA スキャンオペレータのサポート

macOS向けCitrix Secure Accessクライアントは、EPAエディターのすべての演算子 **<**、**>**、**>=**、**<=**、**==** および **!=** をサポートするようになりました。また、**Mac OS** オプションはEPA エディタの個別のオプションとして使用できます (**Mac > Mac OS**)。これらのオペレータを使用して、macOS デバイスの製品バージョンスキャンを実行できます。

詳細については、「[高度なエンドポイント分析スキャン](#)」の「**注意**」セクションを参照してください。

- EPA ライブラリが 24.1.2.1 (OPSWAT OESIS ライブラリ V 4.3.3405.0) に更新されました。

- このリリースでは、全体的なパフォーマンスと安定性を向上させるためのいくつかの問題が修正されています。

24.1.5 MacOS 用 EPA クライアント (2024 年 2 月 12 日)

新機能

- **Apple シリコンプロセッサを搭載した Mac デバイスの EPA サポート**

Citrix EPAクライアントは、Appleシリコンプロセッサを使用するMacデバイスをサポートするようになりました。Macデバイスでは、Citrix EPAクライアントを実行するためにRosettaをインストールする必要がなくなりました。

- **Mac クライアントでの EPA スキャンオペレータのサポート**

Mac向けCitrix EPAクライアントは、EPA式の演算子（<、>、>= および <=）をサポートするようになりました。管理者は EPA スキャンを設定して、さまざまな OS バージョンを許可できます。

たとえば、12.8を除く12.4から13.0までのOSバージョンを許可するには、管理者が式 `version >= 12.4 && version <= 13.0 && version != 12.8` を設定できます。つまり、macOSのバージョンは12.4から13.0でなければなりませんが、12.8であってはなりません。

詳細については、[高度なエンドポイント分析スキャンを参照してください](#)。

V23.12.2 (2023年12月20日)

新機能

このリリースでは、全体的なパフォーマンスと安定性を向上させるための問題が修正されています。

V23.12.1 (2023 年 12 月 6 日)

新機能

- EPA ライブラリは 23.11.1.5 (OPSWAT OESIS ライブラリ V 4.3.3318.0) に更新されました。
- このリリースでは、その他の問題も解決され、全体的なパフォーマンスと安定性が向上しています。

V23.11.2 (2023 年 11 月 1 日)

新機能

EPA ライブラリは 23.11.1.1 (OPSWAT OESIS ライブラリ V 4.3.3279.0) に更新されました。

V23.11.1 (2023 年 10 月 27 日)

新機能

- iOS向けCitrix SSOの名前がCitrix Secure Accessに変更されました。この名前の変更を反映するために、ドキュメント内の UI スクリーンショットを更新しています。
- EPA ライブラリは 23.10.1.1 (OPSWAT OESIS ライブラリ V 4.3.3246.0) に更新されました。
- このリリースでは、次の内容が取り上げられています：
 - Citrix Secure Private Access 環境での接続の問題。
 - 全体的なパフォーマンスと安定性を向上させるためのその他の問題。

V23.10.2 (2023 年 10 月 17 日)

このリリースでは、IPv6 ログインの問題が解決されています。

V23.10.1 (2023 年 10 月 9 日)

新機能

- EPA ライブラリは 23.9.1.2 (OPSWAT OESIS ライブラリ V4.3.3221.0) に更新されました。
- ローカル LAN アクセスのサポート

Citrix Secure Access for macOS/Citrix SSO for iOSは、NetScaler GatewayのローカルLANアクセス機能をサポートするようになりました。VPN 接続が確立されたら、エンドユーザーがクライアントデバイス上のローカル LAN リソースにアクセスすることを許可またはブロックするように、ローカル LAN アクセスを設定できます。詳しくは、以下を参照してください：

- [NetScaler Gateway 管理者設定](#)
- [エンドユーザー設定-macOS](#)
- [エンドユーザー設定-iOS](#)

V23.09.1 (2023 年 9 月 7 日)

重要：

macOS 14/iOS 17以降などの最新のApple OSバージョンを使用している場合は、Citrix Secure Accessクライアント/Citrix SSOバージョン23.09.1以降にアップグレードすることをお勧めします。NetScaler Gatewayクライアントのソフトウェア要件について詳しくは、「[Citrix Secure Accessクライアントのシステム要件](#)」を参照してください。

新機能

- EPA ライブラリは 1.3.9.9 (OPSWAT OESIS v4.3.3160) にアップデートされました。
- セキュリティで保護された接続に関するインサイトを UI で確認

Citrix Secure Accessクライアントユーザーインターフェイスの「接続」画面では、セキュリティで保護された接続の詳細を表示できます。詳細には、IP アドレス、FQDN、宛先ポート、接続時間が含まれます。詳細については、「[安全な接続に関する洞察](#)」を参照してください。

- VPN接続障害後にNetScaler Gateway で再認証する

MacOS向けCitrix Secure AccessクライアントおよびiOS向けCitrix SSOは、VPN接続が失われたときにNetScaler Gatewayによる再認証を求めるメッセージを表示するようになりました。NetScaler Gatewayへの接続が失われ、接続を再開するには再認証が必要であることを示す通知がUIに表示されます。詳しくは、次のトピックを参照してください：

- [VPN接続が失敗した後に、macOSからNetScaler Gateway に再接続する](#)
- [VPN接続に障害が発生したら、iOSからNetScaler Gateway に再接続します。](#)

V23.08.1 (2023 年 8 月 24 日)

新機能

- このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。
- EPA ライブラリが 1.3.9.9 (OPSWAT OESIS v4.3.3122) にアップデートされました。

23.7.6 macOS 用 EPA クライアント (2023 年 8 月 10 日)

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V23.07.1 (2023 年 7 月 17 日)

新機能

- ログファイルを共有するためのさまざまなオプション

iOS向けCitrix SSOの「メールログ」オプションが「ログの共有」オプションに置き換えられました。圧縮されたログファイルは、電子メール、チャット、ファイルへの保存などのオプションで共有できるようになりました。

詳しくは、「[ログの送信](#)」を参照してください。

- 「ログ」ページの機能強化

macOS向けCitrix Secure Accessの「ログ」ページが拡張され、次のオプションが追加されました。

- ログファイルの最大数:ログ収集に追加するログファイルの最大数を指定します。
- メールログ:ログをメールで送信します。

詳しくは、「[ログの送信](#)」を参照してください。

解決された問題

VPNに接続するときに、認証用の証明書を選択するように求められた場合は、Citrix Secure Accessクライアントのホームページの背後に認証ログイン画面が表示されます。

V23.06.1 (2023 年 6 月 7 日)

新機能

- ナビゲーションバーのヘルプメニュー

Citrix Secure Access クライアントのナビゲーションバーにメニューが追加されました。メニューのオプション(、 、)は、ログのデバッグに使用できます。

「ヘルプ」メニューに「メールログ」オプションが導入されました。電子メールでログを共有するために使用できます。詳しくは、「[ログの送信](#)」を参照してください。

解決された問題

macOS向けCitrix Secure AccessおよびiOS向けCitrix SSOでは、DNSの短縮名解決が失敗する場合があります。

既知の問題

場合によっては、リバース分割トンネリングで除外されたルートがトンネリングされます。

V23.05.2 (2023 年 5 月 11 日)

解決された問題

アップグレード後、iOS向けCitrix SSOクライアントデバイスはアプリごとのVPN接続を確立できません。

V23.05.1 (2023 年 5 月 4 日)

新機能

- EPA ライブラリは 1.3.9.3 に更新され、OPSWAT ライブラリは 4.3.2987 に更新されました。
- Citrix Analytics へのイベント送信のサポート

macOS向けCitrix Secure Accessは、セッションの作成、セッションの終了、Citrix Analytics サービスへのアプリケーション接続などのイベントの送信をサポートするようになりました。その後、これらのイベントはSecure Private Accessサービスのダッシュボードに記録されます。

解決された問題

- ユーザーがCitrix Secure AccessまたはCitrix SSOに接続している場合、「接続時間」フィールドに地域固有の形式で時間が表示されません。

V23.04.1 (2023 年 4 月 4 日)

新機能

- EPA ライブラリは 1.3.9.1 にアップデートされ、OPSWAT ライブラリは 4.3.2923 にアップデートされました。

V22.12.2 (2023 年 2 月 27 日)

新機能

- EPA ライブラリが 1.3.8.9 (OPSWAT OESIS v4.3.2892.0) にアップデートされました。

V22.12.1 (2022 年 12 月 7 日)

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V22.11.1 (2022 年 11 月 29 日)

解決された問題

- 転送口グオンは、オンプレミスゲートウェイの nFactor 以外の認証では機能しません。

22.11.3 macOS 用 EPA プラグイン (2022年11月28日)

解決された問題

- NetScaler で GSLB が有効になっていると、macOS 用Citrix EPA プラグインがクラッシュします。

V22.10.1 (2022 年 11 月 17 日)

新機能

- Citrix Endpoint Analysisプラグインは、許可されるIPアドレスのリストに対してパターンセットを作成できる新しいMACアドレス検証式をサポートするようになりました。

解決された問題

- NetScaler Gateway リリース13.0または13.1のプロキシ設定が空の場合、Citrix SSOによって不適切なプロキシ設定が作成されることがあります。
- ネットワークが停止したり、デバイスがスリープモードから復帰したりすると、VPN クライアントは再接続に失敗することがあります。
- IPv6 リテラルを宛先として使用すると、ゲートウェイ接続が失敗することがあります。

22.10.1 macOS 用 EPA プラグイン (2022 年 10 月 27 日)

新機能

- Citrix Endpoint Analysisプラグインは、許可されたIPアドレスのリストに対してパターンセットを作成できる新しいMACアドレス検証式をサポートするようになりました。
- Citrix Endpoint Analysisプラグインは、Google Chromeからのプライベートネットワークアクセスプリフライトリクエストを処理する際に、重複する同意アラートを送信します。

V22.06.1 (2022 年 9 月 20 日)

新機能

- EPA ライブラリが 4.3.2523.0 (1.3.7.5) に更新されました

解決された問題

- EPA スキャンによる nFactor 認証は macOS クライアントでは機能しません。
- macOS用のSecure Access Agentのホームページでは、選択したテーマ（明るいままたは暗い）に応じて、ハンバーガーメニューの左と上部に白または黒の余分なパディングが表示されません。
- VPN にログインするときに、デバイス証明書が設定されていれば、WebView ウィンドウが最初の試行で最小化されます。
- NetScaler ADCアプライアンスでGSLBが有効になっていると、macOSクライアント上のCitrix Secure Accessアプリでエンドポイント分析が機能しません。
- 設定したアプリケーション名にスペースが含まれている場合にアプリケーションにアクセスしようとしても、macOS クライアントに「セキュリティ強化有効」ポップアップが表示されません。
- デバイスに適切なクライアント証明書がない場合、オプションのクライアント証明書による nFactor 認証は失敗します。
- Chrome を使用する Mac デバイスで、2 つの FQDN にアクセス中に VPN 拡張機能がクラッシュします。

- Citrix Secure Accessは、ゲートウェイから誤ったロケーション値を受信するとクラッシュします。これは、管理者が別のホストにリダイレクトするレスポnderポリシーを定義した場合に発生する可能性があります。
- Citrix Secure Accessによって確立されたトンネルの外部にあるリソースへの直接接続は、大幅な遅延または輻輳が発生すると失敗することがあります。

V3.2.4.9-macOS 用 EPA プラグイン (2022 年 8 月 1 日)

解決された問題

- Citrix Endpoint Analysisプラグインは、Google Chromeブラウザバージョン104からのプライベートネットワークアクセスのプリフライトリクエストを処理しません。
- macOS用Citrix Endpoint AnalysisプラグインはGSLBをサポートしていません。

既知の問題

- macOS用Citrix Endpoint AnalysisプラグインをGoogle Chromeブラウザバージョン104から起動すると、重複した同意ダイアログボックスが表示されます。ユーザーは両方のプロンプトを受け入れる必要があります。

V22.03.1 (14-Jun-2022)

新機能

- EPA ライブラリは 4.3.2393.0 に更新されました。

解決された問題

- 検索リストに追加の DNS ドメインが追加されます。これは、分割トンネルが「スプリット」または「両方」に設定されている場合、指定されたドメインとそのサブドメインのみがトンネリングされないためです。指定したドメインがA.B.C の場合、A.B.C と *.A.B.C に加えて B.C も一致します。
- PAC ファイルを使用しない HTTP/HTTPS プロキシ設定は壊れています。

V22.02.3 (24-Mar-2022)

新機能

- Citrix Secure Access for macOSは、クラウドワークスペース接続のクライアントからのすべてのTCPデータ接続でサービスノードのFQDNを解決します。すべてのTCPデータ接続でサービスノードのFQDNを解決することは、オンプレミスのゲートウェイ接続には適用されません。

解決された問題

- ポート53を使用する一部の非DNSプロトコル（STUNなど）の問題により、macOS向けCitrix Secure Accessが接続を切断することがあります。
- Citrix Secure Accessアプリは、接続が確立された直後にサーバーがクライアントの前にデータを送信すると、一部のプロトコルを中断します。
- ユーザーが認証を完了せずにmacOS向けCitrix Secure Accessクライアントの認証ウィンドウを閉じると、その後サーバーに接続しようとしても、アプリが再起動されるまで失敗します。
- macOS向けCitrix Secure Access クライアントがOPSWAT ライブラリバージョン4.3.2367.0にバンドルされるようになりました
- macOS向けCitrix Secure Accessは、認証後のEPAチェックの実行に予想よりも長い時間がかかります。

既知の問題

- macOS向けCitrix Secure Accessアプリは、すでに接続されているCitrix Secure Private Access サービスリージョンにアクセスできなくなった1分後にログアウトします。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

V22.02.2 (15-Feb-2022)

解決された問題

- ユーザーがCitrix Secure Access for macOSからサブスクライブ解除されたWebアプリにアクセスしようとする、複数のポップアップが表示されます。

V22.01.1 (08-Feb-2022)

解決された問題

- iOSデバイス向けCitrix SSOを使用したアプリごとのVPN接続では、443以外のポートでNetScaler Gateway に接続できません。

V1.4.1 (28-Jan-2022)

新機能

- macOS向けCitrix SSOアプリは、Citrix Secure Accessとしてブランド名が変更されました。

解決された問題

- 認証サーバが同じ Web ビューセッションでクライアント証明書を複数回要求すると、クライアント証明書認証は失敗します。
- クライアントとADCの間にプロキシが存在するため、サーバー証明書に共通名のIPアドレスしかない場合、Citrix SSOはVPN接続の確立に失敗します。
- macOS でアンチウイルスの最後のフルシステムスキャンを確認するための EPA スキャンが失敗します。
- サイズの大きいDNSパケットの処理中に、Citrix SSOアプリがクラッシュすることがあります。

V1.4.0 (17-Nov-2021)

解決された問題

- サーバー証明書が信頼されていると、サーバー検証コードが失敗することがあります。その結果、エンドユーザーはゲートウェイにアクセスできなくなります。
- ネットワークが中断された後、Citrix SSOがVPN接続の再確立に失敗します。

V1.3.13 (05-Nov-2021)

解決された問題

- 管理対象VPNと非管理対象VPNのセッションをフィルタリングすると、障害が発生することがあります。セッションを確立する最初の要求で、User-Agent ヘッダーに「ManagedVPN」情報が欠落しています。

V1.3.12 (21-Oct-2021)

解決された問題

- macOSキーチェーンにクライアント証明書がない場合、Citrix SSO for macOSのクライアント証明書認証が失敗します。
- 通知を受信すると、Citrix SSOアプリが断続的にクラッシュする。
- 機能フラグを確認するために「isFeatureEnabled」パラメーターが呼び出されると、VPN拡張機能がクラッシュすることがあります。
- DTLSプロトコルのペイロードが空の場合、ゲートウェイVPN拡張機能はクラッシュします。
- デバイスがスリープモードから復帰しVPNが接続されると、SSOアプリが断続的にクラッシュします。

V1.3.11 (17-Sep-2021)

解決された問題

- Citrix SSO を使用する macOS デバイスのファイアウォールチェックの EPA スキャンが失敗します。
- レガシー認証または Intune ネットワークアクセスコンプライアンス（NAC）が構成されていると、iOS 12 デバイスでCitrix SSOがクラッシュする。

V1.3.10 (31-Aug-2021)

新機能

- macOS用のCitrix SSOはOPSWAT ライブラリバージョン4.3.1977.0にバンドルされるようになった。

V1.3.9 (13-Aug-2021)

解決された問題

- HTTPプロキシソフトウェアがインストールされている一部のシステムでは、NetScaler Gateway IPアドレスが内部的に127.0.0.1として表示されるため、トンネルの確立が妨げられます。
- 「信頼できないサーバーをブロックする」設定は、Citrix SSO for iOSの英語以外のローカライズをサポートするシステムでは機能しません。
- Citrix SSOは、DNS名がサーバー証明書の共通名と一致しないシステムに接続できません。Citrix SSOはサブジェクトの別名をチェックし、正しく接続するようになりました。

V1.3.8 (07-Jul-2021)

新機能

- macOS向けCitrix SSOは、バージョン10.15（Catalina）以上とのみ互換性がある。
- macOSバージョン1.3.8用のCitrix SSO以降、EPAライブラリはアプリ内に埋め込まれ、NetScaler Gateway サーバーからはダウンロードされません。現在の組み込み EPA ライブラリのバージョンは 1.3.5.1 です。

iOSユーザー向けCitrix Secure Accessのセットアップ

重要：

- iOS向けCitrix SSOの名前がCitrix Secure Accessに変更されました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。この移行期間中に、ドキュメントでCitrix SSOのリファレンスが使用されていることに気付くかもしれません。
- VPN は iOS 12 以降では使用できません。VPNを引き続き使用するには、Citrix Secure Accessを使用してください。

iOS向けCitrix Secure Accessでサポートされている一般的に使用される機能の一覧については、「[NetScaler Gateway VPNクライアントとサポートされている機能](#)」を参照してください。

MDM 製品との互換性

Citrix Secure Access (macOS/iOS) は、Citrix Endpoint Management (旧XenMobile)、Microsoft Intune などのほとんどのMDMプロバイダーと互換性があります。

Citrix Secure Access (macOS/iOS) は、ネットワークアクセス制御 (NAC) と呼ばれる機能もサポートしています。NACについて詳しくは、「[単一要素ログイン用のNetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成](#)」を参照してください。NACを使用すると、MDM管理者はNetScaler ADCアプライアンスに接続する前にエンドユーザーデバイスのコンプライアンスを強制できます。Citrix Secure Access (macOS/iOS) 上の NAC には、Citrix Endpoint Management や Intune と NetScaler などの MDM サーバーが必要です。

注：

macOS/iOSでCitrix Secure AccessクライアントをMDMなしでNetScaler Gateway VPNで使用するには、VPN構成を追加する必要があります。iOSのVPN構成は、Citrix Secure Access (macOS/iOS) のホームページから追加できます。

Citrix Secure Access クライアント (macOS/iOS) 用の MDM マネージド VPN プロファイルの設定

次のセクションでは、例としてCitrix Endpoint Management (旧XenMobile) を使用して、Citrix Secure Accessクライアント (macOS/iOS) のデバイス全体のVPNプロファイルとアプリごとのVPNプロファイルの両方を構成する手順を段階的に説明します。他のMDMソリューションでは、

Citrix Secure Access (macOS/iOS) を使用する際の参考資料としてこのドキュメントを使用できます。

注:

このセクションでは、基本的なデバイス全体およびアプリごとの VPN プロファイルの設定手順について説明します。また、Citrix Endpoint Management (旧XenMobile) のマニュアルまたはAppleのMDMVPNペイロード構成に従って、オンデマンドプロキシを構成することもできます。

デバイスレベルの VPN プロファイル

デバイスレベルの VPN プロファイルは、システム全体の VPN を設定するために使用されます。すべてのアプリとサービスからのトラフィックは、NetScaler ADCで定義されたVPNポリシー（フルトンネル、分割トンネル、リバース分割トンネルなど）に基づいてNetScaler Gateway にトンネリングされます。

Citrix Endpoint ManagementでデバイスレベルのVPNを構成するには

Citrix Endpoint ManagementでデバイスレベルのVPNを構成するには、次の手順を実行します。

1. Citrix Endpoint Management MDMコンソールで、[構成] > [デバイスポリシー] > [新しいポリシーの追加] に移動します。
2. 左側の ペインで を選択します。右側のペインで を選択します。
3. ページで、有効なポリシー名と説明を入力し、 をクリックします。
4. **iOS** の ページで、有効な接続名を入力し、 で を選択します。

MDM VPN ペイロードでは、接続名は **UserDefinedName** キーに対応し、**VPN タイプキーは ****VPN**に設定する必要があります。

5. に **com.citrix.NetScalerGateway.ios.app**と入力します。これは、iOS上のCitrix Secure Accessのバンドル識別子です。

MDM VPN ペイロードでは、カスタム SSL 識別子は **VPNSubType** キーに対応します。

6. に **com.citrix.NetScalerGateway.ios.app.vpnplugin**と入力します。これは、Citrix Secure Access iOSアプリバイナリに含まれるネットワーク拡張のバンドル識別子です。

MDM VPN ペイロードでは、プロバイダーバンドル識別子は **ProviderBundleIdentifier** キーに対応します。

7. に、このCitrix Endpoint Managementインスタンスに関連付けられたNetScaler ADC IPアドレスまたはFQDN（完全修飾ドメイン名）を入力します。

設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧XenMobile）のドキュメントを参照してください。

8. **【次へ】** をクリックします。



9. **【保存】** をクリックします。

アプリごとの VPN プロファイル

アプリごとの VPN プロファイルは、特定のアプリケーションの VPN を設定するために使用されます。特定のアプリからのトラフィックのみが、NetScaler Gateway にトンネリングされます。

Per-App VPN ペイロードは、デバイス全体の VPN のすべてのキーに加えて、その他いくつかのキーをサポートします。

Citrix Endpoint ManagementでアプリごとのレベルのVPNを構成するには

アプリ単位 VPN を設定するには、次の手順を実行します。

1. Citrix Endpoint ManagementでデバイスレベルのVPN構成を完了します。
2. セクションの スイッチをオンにします。
3. マッチアプリの起動時にCitrix Secure Access（macOS/iOS）を自動的に起動する必要がある場合は、「オンデマンドマッチアプリを有効にする」スイッチをオンにしてください。これは、ほとんどのアプリごとのケースで推奨されます。

MDM VPN ペイロードでは、このフィールドは **onDemandMatchAppEnabled**キーに対応します。

4. **で** を選択します。

MDM VPN ペイロードでは、このフィールドはキー**プロバイダータイプ**に対応します。

5. Safari ドメインの設定はオプションです。Safariドメインを設定すると、ユーザーがSafariを起動し、「ドメイン」フィールドのURLと一致するURLに移動すると、Citrix Secure Access（macOS/iOS）が自動的に**起動**します。特定のアプリの VPN を制限する場合、これはお勧めできません。

MDM VPN ペイロードでは、このフィールドはキー **safariDomains**に対応します。

設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧XenMobile）のドキュメントを参照してください。



6. をクリックします。 **

7. **【保存】** をクリックします。

この VPN プロファイルをデバイス上の特定のアプリに関連付けるには、このガイド () に従って、アプリインベントリポリシーと認証情報プロバイダーポリシーを作成する必要があります。

`<https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/>`。

アプリ単位 VPN での分割トンネルの設定

MDMのお客様は、Citrix Secure Access (macOS/iOS) 用のアプリベースVPNで分割トンネルを構成できます。次のキーと値のペアは、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに追加する必要があります。

```
- Key = "PerAppSplitTunnel"

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

キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

注:

ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Managementの構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



ユーザー作成の VPN プロファイルの無効化

MDMのお客様は、ユーザーがCitrix Secure Access (macOS/iOS) 内から手動でVPNプロファイルを作成することを防ぐことができます。これを行うには、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに、次のキーと値のペアを追加する必要があります。

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

キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

注:

ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Managementの構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



DNSハンドリング

Citrix Secure Accessクライアントの推奨DNS設定は次のとおりです：

- 分割トンネルが **OFF** に設定されている場合は、**スプリット DNS > REMOTE****。 **
- **分割トンネルが **ON** に設定されている場合は、**スプリット DNS **BOTH**。この場合、管理者はイントラネットドメインの DNS サフィックスを追加する必要があります。DNSサフィックスに属するFQDNのDNSクエリはNetScaler ADCアプライアンスにトンネリングされ、残りのクエリはローカルルーターに送信されます。

注：

- DNS 切り捨て修正フラグは常に****ON にすることをお勧めします。詳しくは、「<<https://support.citrix.com/article/CTX200243>>」を参照してください。
- 分割トンネルが ON に設定され、スプリット DNS が REMOTE に設定されている場合、VPN の接続後に DNS クエリーを解決する際に問題が発生する可能性があります。これは、ネットワーク拡張フレームワークがすべての DNS クエリをインターセプトしない場合に関連しています。

既知の問題

問題の説明: アプリ単位 VPN またはオンデマンド VPN 構成の “.local” ドメインを含む FQDN アドレスのトンネリング。Apple の Network Extension フレームワークには、ドメイン部分（たとえば <<http://www.abc.local>>）.local に含まれる FQDN アドレスがシステムの TUN インターフェイスを介してトンネリングされないようにするバグがあります。代わりに、FQDN アドレスのトラフィックは、クライアントデバイスの物理インターフェイスを介して送信されます。この問題は、アプリ単位 VPN またはオンデマンド VPN の設定でのみ発生し、システム全体の VPN 設定では発生しません。Citrix は Apple にレーダーバグレポートを提出しており、Apple は、RFC-6762 によると <<https://tools.ietf.org/html/rfc6762>>、ローカルはマルチキャスト DNS（mDNS）クエリであり、したがってバグではないと述べています。しかし、Apple はまだバグをクローズしておらず、この問題が将来の iOS リリースで対処されるかどうかは明らかではありません。

回避策： 回避策として、このようなアドレスに non .local ドメイン名を割り当てます。

制限事項

- エンドポイント分析 (EPA) は iOS ではサポートされていません。
- ポート/プロトコルに基づく分割トンネリングはサポートされていません。

Mac向けCitrix Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン-プレビュー

Citrix Secure Access for macOS 24.03.1以降、Citrix Workspaceアプリにログインすることで、エンドユーザーがCitrix Secure Accessクライアントにシングルサインオン（SSO）し、ユーザートンネルを確立し、TCP/UDPアプリケーションへのシームレスなアクセスを提供できるようになりました。エンドユーザーがCitrix Workspaceアプリに接続している場合、macOS向けCitrix Secure

Accessが自動的に起動し、エンドユーザーはシングルサインオンを使用してシームレスにログオンできます。

エンドユーザーがCitrix Workspaceアプリからログアウトすると、Citrix Secure Accessはユーザーの介入なしに自動的にログアウトします。この機能により、エンドユーザーは1つのアプリケーションにのみログオンするだけで済むため、統一されたエクスペリエンスが提供され、時間を節約できます。

現在、この機能はデフォルトで無効になっています。 `<https://podio.com/webforms/29383411/2410629>` を使用してプレビューにサインアップできます。

前提条件

1. エンドユーザーは、 [Citrix Workspaceアプリ2402以降を使用している必要があります](#)。Mac向けCitrix Workspaceアプリのインストールについて詳しくは、「[Mac向けCitrix Workspaceアプリ](#)」を参照してください。
2. エンドユーザーは、 [macOS 24.03.1以降のCitrix Secure Accessを使用している必要があります](#)。
3. MDM を使用してこの機能を有効にするには、管理者は次の設定を使用する必要があります：
 - `<key>EnableSecureAccessAutoLogin</key><true/>`

注意事項

- この機能を有効にする前にエンドユーザーがすでにCitrix Workspaceアプリにログオンしている場合は、Citrix WorkspaceアプリがCitrix Secure AccessクライアントへのSSOをトリガーできるように再ログインする必要があります。
- タイムアウトやユーザーによる手動ログアウトなどの理由でCitrix Workspaceアプリからログオフすると、Citrix Secure Accessもログアウトされ、ユーザーセッションは切断されます（これは、Citrix Secure AccessがCitrix Workspaceアプリを介して自動的に起動された場合のみ）。
- Citrix WorkspaceアプリからCitrix Secure AccessへのSSOログインは、単一のプライマリドメインでのみサポートされています。複数ドメインでのSSOはサポートされていません。
- この機能を使用してCitrix Secure Accessにシングルサインオンした後に、Citrix Workspaceアプリ接続を別のURLに切り替えると、Citrix Workspaceアプリ接続URLを選択するように求められます。

ユーザー証明書の ID を電子メールの添付ファイルとして iOS ユーザーに送信する

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

iOS上のCitrix Secure Accessは、NetScaler Gatewayによるクライアント証明書認証をサポートしています。iOSでは、証明書は次のいずれかの方法でCitrix Secure Accessに配信できます：

- MDM サーバ-これは MDM のお客様にとって好ましいアプローチです。証明書はMDM管理のVPNプロファイルで直接構成されます。デバイスがMDMサーバーに登録されると、VPNプロファイルと証明書の両方が登録済みデバイスにプッシュされます。このアプローチについては、MDM ベンダー固有のドキュメントに従ってください。
- メール - MDM以外をご使用のお客様の唯一のアプローチです。この方法では、管理者は PKCS #12 ファイルとしてユーザー証明書 ID (証明書と秘密キー) を添付した電子メールをユーザーに送信します。ユーザーが添付ファイル付きのメールを受信するには、iOS デバイスでメールアカウントを設定する必要があります。その後、ファイルをiOSのCitrix Secure Accessにインポートできます。次のセクションでは、このアプローチの設定手順について説明します。

前提条件

- ユーザー証明書-特定のユーザーの拡張子が.pfx または.p12 の PKCS #12 識別ファイル。このファイルには、証明書と秘密キーの両方が含まれています。
- iOS デバイスで設定された電子メールアカウント。
- iOSデバイスにCitrix Secure Accessがインストールされています。

構成の手順

1. ユーザー証明書の拡張/MIME タイプの名前を変更します。

ユーザー証明書で最も一般的に使用されるファイル拡張子は、「.pfx」、「.p12」などです。これらのファイル拡張子は、.pdf、.doc などの形式とは異なり、iOS プラットフォームでは標準ではありません。「.pfx」と「.p12」はどちらもiOSシステムによって要求され、Citrix Secure Accessなどのサードパーティアプリでは要求できません。そのため、Citrix Secure Accessは「.citrixsso-pfx」と「.citrixsso-p12」という新しい拡張機能/MIMEタイプを定義しました。管理者は、ユーザー証明書の拡張子/MIME タイプを標準の「.pfx」または「.p12」から「.citrixsso-pfx」または「.citrixsso-p12」にそれぞれ変更する必要があります。拡張機能の名

前を変更するには、管理者はコマンドプロンプトまたはターミナルで次のコマンドを実行します。

Windows 10

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>

rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
pfx
```

macOS

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>

mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
```

2. ファイルを電子メールの添付ファイルとして送信します。

新しい拡張子を持つユーザー証明書ファイルは、電子メールの添付ファイルとしてユーザーに送信できます。

電子メールを受信したら、ユーザーはCitrix Secure Accessに証明書をインストールする必要があります。

iOSユーザー用のCitrix SSOアプリ用またはmacOSユーザー用のCitrix Secure Accessクライアント用のプロキシPACファイルのセットアップ

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

iOS向けCitrix Secure アプリまたはmacOS向けCitrix Secure Accessクライアントは、VPNトンネルの確立後に自動プロキシ構成（プロキシPACファイル）をサポートします。管理者はプロキシPACファイルを使用して、ホスト名の解決を含め、クライアントのすべてのHTTPトラフィックがプロキシを通過することを許可できます。

プロキシ PAC ファイルを設定する方法

プロキシファイルをホストできる内部マシンがある。たとえば、マシンの IP アドレスが 172.16.111.43 で、PAC ファイルの名前が proxy.pac であるとします。

実際のプロキシサーバの IP アドレスが、ポート 8080 でリッスンしている 172.16.43.83 である場合、proxy.pac のサンプルは次のようになります。関数 findProxyForUrl (url, host) {「PROXY 172.16.43. 83:8080」 を返す;}

プロキシ PAC URLは <http://172.16.111.43/proxy.pac> です。ファイルがポート HTTP ポート 80 でホストされていると仮定します。

詳細については、<<https://support.citrix.com/article/CTX224235>> または「[NetScaler Gatewayの送信プロキシサポートのプロキシ自動構成](#)」を参照してください。

注：

- 分割トンネルがオンの場合は、PAC ファイルをホストするサーバの IP アドレスがイントラネットアプリケーションリストに含まれていることを確認し、VPN 経由でアクセスできるようにします。
- Citrix Secure Access (macOS/iOS) からログインすると、ブラウザはプロキシPACファイルのルールを使用し始めます。前の例のようにプロキシルールを 1 つだけ指定すると、すべての HTTP または HTTPS トラフィックが内部プロキシサーバにルーティングされます。

macOS ユーザー向けCitrix Secure Accessのセットアップ

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

macOS向けCitrix Secure Accessクライアントは、NetScaler Gatewayが提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションを提供します。ビジネスクリティカルなアプリケーション、仮想デスクトップ、企業データにいつでもどこからでも安全にアクセスできるようになりました。Citrix Secure Accessは、macOSデバイスからのVPN接続を作成および管理するためのNetScaler Gateway用の次世代VPNクライアントです。Citrix Secure Accessは、Appleのネットワーク拡張（NE）フレームワークを使用して構築されています。Apple の NE フレームワークは、macOS のコアネットワーク機能をカスタマイズおよび拡張するために使用できる API

を含む最新のライブラリです。SSL VPN をサポートするネットワーク拡張は、macOS 10.11 以降を実行しているデバイスで利用できます。

Citrix Secure Accessは、macOSでモバイルデバイス管理（MDM）を完全にサポートします。管理者は、MDMサーバーを使用してデバイスレベルのVPNプロファイルやアプリごとのVPNプロファイルをリモートで構成して管理できるようになりました。 macOS向けCitrix Secure Accessは、Mac App Storeからインストールできます。

macOS向けCitrix Secure Accessクライアントでサポートされる一般的に使用される機能のリストについては、「[NetScaler Gateway VPNクライアントとサポートされている機能](#)」を参照してください。

MDM 製品との互換性

macOS向けCitrix Secure Accessは、Citrix XenMobile、Microsoft Intune などのほとんどのMDMプロバイダーと互換性があります。ネットワークアクセス制御（NAC）と呼ばれる機能をサポートしています。これを使用して、MDM管理者はNetScaler Gateway に接続する前にエンドユーザーデバイスのコンプライアンスを強制できます。Citrix Secure Access上のNACを使用するには、XenMobileやNetScaler GatewayなどのMDMサーバーが必要です。NACについて詳しくは、「[単一要素ログイン用のNetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成](#)」を参照してください。

注：

MDMなしでNetScaler Gateway VPNでCitrix Secure Accessを使用するには、VPN構成を追加する必要があります。macOSのVPN構成は、[\[Citrix Secure Access\] 構成ページ](#)から追加できます。

Citrix Secure Accessの MDM 管理対象VPNプロファイルを構成する

次のセクションでは、Citrix Endpoint Management（以前のXenMobile）を例として使用して、Citrix Secure Accessのデバイス全体のVPNプロファイルとアプリごとのVPNプロファイルの両方を構成する手順を説明します。他のMDMソリューションでは、Citrix Secure Accessを使用する際の参照としてこのドキュメントを使用できます。

注:

このセクションでは、基本的なデバイス全体およびアプリごとの VPN プロファイルの設定手順について説明します。また、Citrix Endpoint Management（旧XenMobile）[のマニュアル](#)または[AppleのMDM](#)VPNペイロード構成に従って、オンデマンドプロキシを構成することもできます。

デバイスレベルの VPN プロファイル

デバイスレベルの VPN プロファイルは、システム全体の VPN を設定するために使用されます。すべてのアプリとサービスからのトラフィックは、NetScaler ADCで定義されたVPNポリシー（フルトンネル、分割トンネル、リバース分割トンネルなど）に基づいてNetScaler Gateway にトンネリングされます。

Citrix Endpoint ManagementでデバイスレベルのVPNを構成するには

デバイスレベル VPN を設定するには、次の手順を実行します。

1. Citrix Endpoint Management MDMコンソールで、[構成] > [デバイスポリシー] > [新しいポリシーの追加] に移動します。
2. 左側の ペインで を選択します。右側のペインで を選択します。
3. ページで、有効なポリシー名と説明を入力し、 をクリックします。
4. **macOS** の ページで、有効な接続名を入力し、 で を選択します。

MDM VPN ペイロードでは、接続名は **UserDefinedName** キーに対応し、**VPN タイプキーは ****VPN**に設定する必要があります。

5. に **com.citrix.netscalergateway.macos.app**と入力します。macOS上のCitrix Secure Access のバンドル識別子です。

MDM VPN ペイロードでは、カスタム SSL 識別子は **VPNSubType** キーに対応します。

6. に **com.citrix.NetScalerGateway.macos.app.VPNPlugin**と入力します。これは、Citrix Secure Accessクライアントバイナリに含まれるネットワーク拡張のバンドル識別子です。

MDM VPN ペイロードでは、プロバイダーバンドル識別子は **ProviderBundleIdentifier** キーに対応します。

7. [**サーバー名またはIPアドレス**] に、このCitrix Endpoint Managementインスタンスに関連付けられているNetScaler ADC IPアドレスまたは完全修飾ドメイン名を入力します。

設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Managementのドキュメントを参照してください。

8. **【次へ】** をクリックします。



9. **【保存】** をクリックします。

アプリごとの VPN プロファイル

アプリごとの VPN プロファイルは、特定のアプリケーションの VPN を設定するために使用されます。特定のアプリからのトラフィックのみが、NetScaler Gateway にトンネリングされます。

Per-App VPN ペイロードは、デバイス全体の VPN のすべてのキーに加えて、その他いくつかのキーをサポートします。

Citrix Endpoint ManagementでアプリごとのレベルのVPNを構成するには

次の手順を実行して、Citrix Endpoint Managementでアプリ単位VPNを構成します。

1. Citrix Endpoint ManagementでデバイスレベルのVPN構成を完了します。
2. セクションの スイッチを**オンにします。
3. **マッチアプリの起動時にCitrix Secure Accessを自動的に起動する必要がある場合は、【オンデマンドマッチアプリ有効】** スイッチをオンにします。これは、ほとんどのアプリごとのケースで推奨されます。

MDM VPN ペイロードでは、このフィールドは **onDemandMatchAppEnabled** キーに対応します。

4. Safari ドメインの設定はオプションです。Safariドメインが構成されている場合、ユーザーがSafariを起動し、「ドメイン」フィールドのURLと一致するURLに移動すると、Citrix Secure Accessが自動的に**起動**します。特定のアプリの VPN を制限する場合、これはお勧めできません。

MDM VPN ペイロードでは、このフィールドはキー **safariDomains**に対応します。

設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧XenMobile）のドキュメントを参照してください。



5. **【次へ】** をクリックします。
6. **【保存】** をクリックします。

VPN プロファイルをデバイス上の特定のアプリに関連付けるには、このガイドに従って、アプリインベントリポリシーと認証情報プロバイダーポリシーを作成する必要があります。

```
<https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/>
```

アプリ単位 VPN での分割トンネルの設定

MDM のお客様は、Citrix Secure Access のアプリ単位VPNで分割トンネルを構成できます次のキーと値のペアは、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに追加する必要があります。

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

キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

注:

ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー全体で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Managementの構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



ユーザー作成の VPN プロファイルの無効化

MDMのお客様は、ユーザーがCitrix Secure Access内からVPNプロファイルを手動で作成できないようにすることができます。これを行うには、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに、次のキーと値のペアを追加する必要があります。

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

キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

注:

ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Managementの構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



DNSハンドリング

Citrix Secure Accessで推奨されるDNS設定は次のとおりです。

- 分割トンネルが **OFF** に設定されている場合は、**スプリット DNS > REMOTE****。 **
- **分割トンネルが **ON** に設定されている場合は、**スプリット DNS **BOTH**。この場合、管理者はイントラネットドメインの DNS サフィックスを追加する必要があります。DNSサフィックスに属するFQDNのDNSクエリはNetScaler ADCアプライアンスにトンネリングされ、残りのクエリはローカルルーターに送信されます。

注：

- DNS 切り捨て修正フラグは常に****ON にすることをお勧めします。詳しくは、「[<https://support.citrix.com/article/CTX200243>](https://support.citrix.com/article/CTX200243)」を参照してください。
- 分割トンネルが ON に設定され、スプリット DNS が REMOTE に設定されている場合、VPN の接続後に DNS クエリーを解決する際に問題が発生する可能性があります。これは、ネットワーク拡張フレームワークがすべての DNS クエリーをインターセプトしない場合に関連しています。

サポートされている EPA スキャン

サポートされているスキャンの完全なリストについては、[最新の EPA ライブラリを参照してください](#)。

1. セクションで**、列の をクリックします。
2. Excel ファイルで、タブをクリックして詳細を表示します。

既知の問題

以下は、現在の既知の問題です。

- ユーザーが検疫グループに配置されている場合、EPA ログインは失敗します。
- 強制タイムアウト警告メッセージは表示されません。
- Citrix Secure Accessでは、分割トンネルがオンで、イントラネットアプリが構成されていない場合にログインできます。

制限事項

以下は、現在の制限事項です。

- 次の EPA スキャンは、サンドボックス化によりセキュアアクセスへのアクセスが制限されているために失敗する可能性があります。
 - ハードディスク暗号化 'type' と 'path'
 - Web ブラウザの「デフォルト」と「実行中」
 - パッチ管理「見つからないパッチ」
 - EPA 中にプロセスの強制終了操作

- ポート/プロトコルに基づく分割トンネリングはサポートされていません。
- キーチェーンに同じ名前と有効期限を持つ証明書が 2 つ存在しないようにしてください。この場合、クライアントには両方の証明書ではなく 1 つの証明書のみが表示されます。

トラブルシューティング

Citrix Secure Accessの認証ウィンドウにエンドユーザーに「EPAプラグインのダウンロード」ボタンが表示される場合は、NetScalerアプライアンスのコンテンツセキュリティポリシーが URL `com.citrix.agmacepa://` の呼び出しをブロックしていることを意味します。管理者は、`com.citrix.agmacepa://` が許可されるようにコンテンツセキュリティポリシーを変更する必要があります。

macOS/iOS 上の Citrix Secure Accessクライアントの nFactor サポート

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

多要素 (nFactor) 認証は、アクセスするために複数の身元証明を提供することをユーザーに要求することにより、アプリケーションのセキュリティを強化します。管理者は、クライアント証明書、LDAP、RADIUS、OAuth、SAML など、さまざまな認証要素を設定できます。これらの認証要素は、組織のニーズに応じて任意の順序で構成できます。

macOS/iOS上のCitrix Secure Accessクライアントは、以下の認証プロトコルをサポートしています：

- **nFactor** — nFactor プロトコルは、認証仮想サーバーがゲートウェイ上の VPN 仮想サーバーにバインドされている場合に使用されます。認証要素の順序は動的であるため、クライアントはアプリケーションのコンテキスト内でレンダリングされるブラウザインスタンスを使用して認証 GUI を表示します。
- **Classic**：クラシックプロトコルは、ゲートウェイ上の VPN 仮想サーバでクラシック認証ポリシーが設定されている場合に使用されるデフォルトのフォールバックプロトコルです。クラシックプロトコルは、NAC などの特定の認証方式で nFactor が失敗した場合のフォールバックプロトコルです。
- **Citrix IDプラットフォーム** — Citrix IDプラットフォームプロトコルは、CloudGatewayまたはNetScaler Gatewayサービスへの認証に使用され、Citrix CloudへのMDM登録が必要です。

次の表は、各プロトコルでサポートされているさまざまな認証方法をまとめたものです。

認証方法	NFACTOR	クラシック	CITRIX IDP
クライアント証明書	サポート対象	サポート対象	未サポート
LDAP	サポート対象	サポート対象	未サポート

nFactor 構成

nFactor の設定の詳細については、[nFactor 認証の設定を参照してください](#)。

重要：

macOS/iOS上のCitrix Secure AccessクライアントでnFactorプロトコルを使用するには、NetScaler Gatewayのオンプレミスバージョンは12.1.50.xx以降が推奨されます。

制限事項

- NAC（ネットワークアクセス制御）などのモバイル固有の認証ポリシーでは、クライアントはNetScaler Gatewayでの認証の一部として署名付きデバイス識別子を送信する必要があります。署名付きデバイス識別子は、MDM環境に登録されているモバイルデバイスを一意に識別する回転可能な秘密キーです。このキーは、MDMサーバーによって管理されるVPNプロファイルに埋め込まれます。このキーをWebViewコンテキストに挿入できない場合があります。MDM VPNプロファイルでNACが有効になっている場合、macOS/iOS上のCitrix Secure Accessクライアントは自動的に従来の認証プロトコルにフォールバックします。
- macOS用のIntuneではNACチェックを設定できません。iOSの場合とは異なり、IntuneにはmacOS用のNACを有効にするオプションが用意されていないためです。

macOS/iOS向けCitrix Secure Accessに関する一般的な問題のトラブルシューティング

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

DNS 解決の問題

- デバイスがスリープ状態になったり、長時間非アクティブになった場合、VPN が再開するまで約 30 ～ 60 秒かかることがあります。この間、ユーザーには一部の DNS 要求が失敗することがあります。DNS 要求は、短期間で自動的に解決されます。DNS クエリが解決されない場合、高度な認可ポリシーが DNS トラフィックをブロックしている可能性があります。この問題を解決するには、[<https://support.citrix.com/article/CTX232237>](https://support.citrix.com/article/CTX232237) を参照してください。
- ブラウザから DNS 解決を常にチェックしてください。端末からの `nslookup` コマンドを使用した DNS クエリは、正確ではない場合があります。 `nslookup` コマンドを使用する必要がある場合は、クライアントの IP アドレスをコマンドに含める必要があります。例： `nslookup website_name 172.16.255.1.`

EPA の問題

- ゲートキーパーはアンチウィルスとみなされます。「任意のウィルス対策」（MAC-ANTIVIR_0_0）をチェックするスキャンがある場合、ユーザーが他のベンダーのウィルス対策ソフトウェアをインストールしていなくても、スキャンは常に成功します。

注：

- クライアントセキュリティログを有効にして、EPA のデバッグログを取得します。VPN パラメータ `clientsecurityLog` を ON に設定すると、クライアントセキュリティログを有効にできます。
- アップルの内蔵パッチ管理ソフトウェアは「ソフトウェアアップデート」です。端末の「App Store」アプリに相当します。「ソフトウェアアップデート」のバージョンは次のようになっている必要があります。 `"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- NetScaler ADC 上の EPA ライブラリを常に最新の状態に保ちます。最新のライブラリは [<https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html>](https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html) にあります

nFactor の問題

- Citrix Secure Access は、nFactor 認証の **Citrix SSO** 認証ウィンドウを開きます。これはブラウザに似ています。このページにエラーがある場合は、Web ブラウザで認証を試すことでクロス検証できます。
- nFactor が有効になっているときに転送ログオンが失敗した場合は、ポータルをテーマを「RfWebUI」に変更します。

- 「証明書チェーンに必要な証明書が含まれていないため、NetScaler Gateway への安全な接続を確立できません。管理者に連絡してください」または「ゲートウェイに到達できません」。その後、ゲートウェイサーバー証明書の有効期限が切れているか、サーバー証明書が SNI 対応でバインドされています。Citrix Secure AccessはSNIをまだサポートしていません。SNI を有効にせずにサーバー証明書をバインドします。このエラーは、MDM VPNプロファイルで構成された証明書ピン留めと、NetScaler Gateway によって提示された証明書がピン留めされた証明書と一致しないことが原因である可能性があります。
- ゲートウェイに接続しようとしたときに、**Citrix SSO認証ウィンドウが開くが空白の場合** は、ECC曲線（ALL）がデフォルトの暗号グループにバインドされているかどうかを確認します。ECC 曲線 (ALL) は、デフォルトの暗号グループにバインドする必要があります。

ネットワークアクセスコントロール (NAC) チェック

NAC 認証ポリシーは、クラシック認証でのみサポートされます。nFactor 認証の一部としてはサポートされていません。

よくある質問

重要：

iOS向けCitrix SSOは、Citrix Secure Accessと呼ばれるようになりました。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新しています。

このセクションでは、macOS/iOS向けCitrix Secure Accessに関するよくある質問について説明します。

macOS/iOS向けCitrix Secure AccessクライアントはVPNアプリとどう違うのですか？ macOS向けCitrix Secure AccessクライアントおよびiOS向けCitrix Secure Accessクライアント（以前はiOS向けCitrix SSOと呼ばれていました）は、NetScaler向けの次世代SSL VPNクライアントです。このアプリはAppleのネットワーク拡張フレームワークを使用して、iOS および macOS デバイスでVPN接続を作成および管理します。Citrix VPNは、現在廃止されているAppleのプライベートVPN APIを使用する従来のVPNクライアントです。Citrix VPNのサポートはアプリストアではご利用いただけなくなりました。

NEって何ですか Appleのネットワーク拡張 (NE) フレームワークは、iOS と macOS のコアネットワーク機能をカスタマイズおよび拡張するために使用できるAPIを含む最新のライブラリです。SSL VPNをサポートするネットワーク拡張は、iOS 9以降と macOS 10.11以降を実行しているデバイスで利用できます。

macOS/iOS向けCitrix Secure AccessクライアントはどのバージョンのNetScalerと互換性がありますか？ macOS/iOS向けCitrix Secure AccessクライアントのVPN機能は、NetScalerバージョン10.5以降でサポートされています。TOTPは、NetScaler ADCバージョン12.0以降で使用できます。NetScaler プッシュ通知はまだ公開されていません。このアプリにはiOS 9 以降のバージョンと macOS 10.11 以降のバージョンが必要です。

MDM 以外のお客様の証明書ベースの認証はどのように機能しますか。 以前にVPNでクライアント証明書認証を実行するために電子メールまたはブラウザ経由で証明書を配布したことがあるお客様は、macOS/iOS向けCitrix Secure Accessクライアントを使用する際に、この変更に注意する必要があります。これは主に、MDMサーバーを使用してユーザー証明書を配布しない非MDM顧客に当てはまります。

ネットワークアクセスコントロール (NAC) とは何ですか。iOS向けCitrix Secure AccessとNetScaler Gatewayを使用してNACを構成する方法を教えてください。 Microsoft Intune および Citrix Endpoint Management (旧XenMobile) MDMのお客様は、iOS向けCitrix Secure Accessのネットワークアクセス制御 (NAC) 機能を利用できます。NACを使用すると、管理者はMDMサーバーで管理されるモバイルデバイスの認証レイヤーを追加することで、企業の内部ネットワークを保護できます。管理者は、iOS向けCitrix Secure Accessの認証時にデバイスのコンプライアンスチェックを実施できます。

iOS向けCitrix Secure AccessでNACを使用するには、NetScaler GatewayとMDMサーバーの両方でNACを有効にする必要があります。

- NetScaler ADCでNACを有効にするには、「[単一要素ログイン用のNetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成](#)」を参照してください。
- MDM ベンダーが Intune の場合は、「[ネットワークアクセス制御 \(NAC\) と Intune の統合](#)」を参照してください。
- MDMベンダーがCitrix Endpoint Management (旧XenMobile) の場合は、「[ネットワークアクセス制御](#)」を参照してください。

注：

サポートされているmacOS/iOS向けCitrix Secure Accessクライアントの最小バージョンは1.1.6以上です。

Android向けCitrix Secure Access

Android向けCitrix Secure Access（旧Citrix SSO）は、NetScaler Gatewayが提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションを提供します。ビジネスクリティカルなアプリケーション、仮想デスクトップ、企業データにいつでもどこからでも安全にアクセスできるようになりました。

重要：

- Android向けCitrix SSOは、現在Citrix Secure Accessと呼ばれています。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。
- Android向けCitrix セキュアアクセスクライアントは、ChromeOS上に構築されたAndroidサブシステム内で動作します。PlayストアからAndroidアプリとしてインストールすればChromeOSで動作し、Androidサブシステム内の任意のアプリケーションをトンネリングできます。

リリースノート

重要:

- Android版Citrix® SSOはCitrix Secure Accessに名称変更されました。この名称変更を反映するため、ドキュメントとUIスクリーンショットを更新しています。この移行期間中、ドキュメント内でCitrix SSOの参照が使用されていることに気づく場合があります。
- FQDNベースの分割トンネリングおよびnFactor認証のサポートは現在プレビュー中です。
- 2025年5月以降、Citrix Secure AccessはAndroid 11およびそれ以前のバージョンではサポートされません。

Citrix Secure Accessのリリースノートでは、サービスリリースで利用可能な新機能、既存機能の強化、修正された問題、および既知の問題について説明しています。リリースノートには、以下のセクションのいずれか、または複数が含まれています。

新機能: 現在のリリースで利用可能な新機能と機能強化。

修正された問題: 現在のリリースで修正された問題。

既知の問題: 現在のリリースに存在する問題、および該当する場合の回避策。

V25.03.3 (2025年6月30日)

修正された問題

- バージョン25.03.1にアップグレードした後、Citrix Secure AccessクライアントがAlways On VPN接続を再確立できず、「Always-On VPNでは対話型ユーザー認証はサポートされていません」というエラーメッセージが表示される場合があります。

V25.03.2 (2025年6月13日)

新機能

- このリリースでは、全体的なパフォーマンスと安定性を向上させるために、いくつかの問題に対処しています。

V25.03.1 (2025年5月28日)

新機能

- Always On VPNモードの定期的な監視のサポート

Google Play開発者サービスによる更新によってCitrix Secure Accessクライアントが終了した場合に、クライアントが自動的に再起動するように、Always On VPNモードの定期的な監視がサポートされるようになりました。

修正された問題

- Always On VPNモードでは、ゲートウェイ名がラウンドロビンDNSロードバランシング方式を使用して複数のIPアドレスに解決される場合、Citrix Secure AccessアプリがVPNへの再接続を繰り返し試行する可能性があります。

V25.02.1 (2025年3月19日)

修正された問題

- DNS応答にCNAMEレコードが含まれている場合、ユーザーはCitrix Secure Accessアプリを介してFQDNを使用してイントラネットアプリケーションにアクセスできない可能性があります。
- Always On VPNモードでは、デバイスがアイドルモードまたは省電力モードになったときに、手動での介入なしにCitrix Secure AccessクライアントがVPNセッションを再開しない場合があります。

V24.11.1 (02-Dec-2024)

新機能

- **Android 14 SDK要件のサポート**

Citrix Secure Accessアプリは、Android 14 SDKの要件をサポートするようになりました。

- **アプリごとの言語設定のサポート**

Citrix Secure Accessアプリは、アプリごとの言語システム設定をサポートするようになりました。

修正された問題

- Always On VPNが有効になっている場合でも、Citrix Secure Accessアプリが転送ロゲインプロンプトを表示することがありました。

V24.10.1 (10-Oct-2024)

新機能

- このリリースでは、全体的なパフォーマンスと安定性を向上させるためにいくつかの問題に対処しています。

修正された問題

- Android版Citrix Secure Accessクライアントでプッシュ通知が機能しない場合があります。

- アイドルセッションのタイムアウト後、Always On機能がNetScaler Gatewayセッションを再開しない場合があります。

V24.08.2 (2024年9月26日)

新機能

- このリリースでは、全体的なパフォーマンスと安定性を向上させるためにいくつかの問題に対処しています。

V24.08.1 (2024年9月9日)

新機能

- サードパーティのセキュアWebゲートウェイとの相互運用性の強化

サードパーティのセキュアWebゲートウェイとの相互運用性を強化するため、Citrix Secure AccessのUser-Agent文字列が更新されました。詳細については、「[クライアントの定義](#)」を参照してください。

- Android版Citrix Secure Accessアプリのセキュリティ機能の強化

ログイン認証中に機密情報が表示されている場合、ユーザーのデバイス上のサードパーティ製アプリはCitrix Secure Accessアプリのスクリーンショットを撮ることができません。

修正された問題

- Citrix Secure Accessアプリが、SAML認証に適さない証明書を表示します。

V24.04.1 (2024年5月3日)

- Always On VPNプロファイルの機能強化

Citrix Secure Access は、VPN プロファイルで Always On VPN` (オプション) プロパティをサポートするようになりました。このプロパティは、VPN プロファイルが Always On VPN プロファイルであるかどうかを決定します。このプロパティが True に設定されている場合、VPN プロファイルは Always On VPN プロファイルであることを示します。

注:

このプロパティは、メインのVPNプロファイルでのみ設定できます。追加のVPNプロファイルには設定できません。

Always On VPNトンネルは、次のシナリオで再確立されます。

- MDMプロファイルの更新
- Androidデバイスの再起動
- ネットワーク接続障害発生時に、別のNetScaler Gatewayに再接続する
- Androidデバイスが省電力モードのときにNetScaler Gatewayセッションの有効期限が切れた後、再接続します。デバイスが省電力モードから復帰すると、接続が再確立されます。

詳細については、以下の記事を参照してください。

- [構成デザイナーを使用したVPN構成](#)
- [Android Enterprise 用の VPN プロファイルを構成する](#)
- [Android 用の Citrix SSO プロトコルを構成する](#)

V23.12.2 (2023年12月15日)

注:

Android 版 Citrix Secure Access バージョン 23.12.2 には、CSAClients-8799 の修正が含まれており、バージョン 23.12.1 を置き換えます。

新機能

- **Android 版 Citrix SSO が Citrix Secure Access に名称変更**

Android 版 Citrix SSO は、Citrix Secure Access に名称変更されました。この名称変更を反映するため、ドキュメントと UI スクリーンショットを更新しています。

- **Android 13 以降のデバイスで通知を受信またはブロックする**

Android 13 デバイスに Citrix Secure Access クライアントをインストールまたは再インストールする際、エンドユーザーは Citrix Secure Access クライアントからの通知を受信する権限を付与するよう求められるようになりました。エンドユーザーがこの権限を拒否した場合、

Android デバイスで Citrix Secure Access クライアントからの VPN ステータスやプッシュ通知は受信されません。MDM 管理者は、ソリューション内で Citrix Secure Access (パッケージ ID: `com.citrix.CitrixVPN`) に通知権限を付与することをお勧めします。

エンドユーザーは、Android デバイスで **設定 > 通知** に移動して、Citrix Secure Access クライアントの通知権限を変更できます。詳細については、「[Android デバイスから Citrix Secure Access を使用する方法](#)」を参照してください。

- **Always On VPNモードでの転送ログオンのサポート**

Android版Citrix Secure Accessは、Always On VPNモードでの転送ログオン機能をサポートするようになりました。転送ログオンの設定方法の詳細については、「[転送ログオンページの構成](#)」を参照してください。

修正された問題

- Android 13以降のデバイスで、ユーザーが時間ベースのOTP (TOTP) トークンをコピーすると、Citrix Secure Accessがクラッシュする。

V23.10.2 (2023年12月19日)

新機能

注：

- Android版Citrix SSOバージョン23.10.2には、CSAClients-8314の修正が含まれており、バージョン23.10.1を置き換えます。
- Android版Citrix SSO 23.10.1はAndroid 14で動作します。

- **VPN接続障害後にNetScaler Gatewayで再認証 - プレビュー**

VPN接続が失われた場合、Android版Citrix SSOはNetScaler Gatewayでの再認証を促すようになりました。Citrix SSO UIおよびAndroidデバイスの通知パネルに、NetScaler Gatewayへの接続が失われたこと、および接続を再開するには再認証が必要であることが通知されます。この機能はプレビュー版です。

詳細については、「[VPN接続障害後にNetScaler Gatewayに再接続](#)」を参照してください。

修正された問題

Citrix SSO が、特定のAlways On VPNシナリオでVPNサービスを再起動する際に、断続的にクラッシュする。

V23.8.1 (31-Aug-2023)

新機能

- **Always On VPNの自動再起動**

Citrix SSOアプリは、許可リストまたはブロックリストの一部であるアプリがワークプロファイルまたはデバイスプロファイルにインストールされると、Always On VPNを自動的に再起動します。このアプリからのトラフィックは、ワークプロファイルを再起動したりデバイスを再起動したりすることなく、VPN接続を介して自動的にトンネルされます。Always On VPNの自動再起動を有効にするには、エンドユーザーはCitrix SSOアプリに[Query all packages](#)の同意を付与する必要があります。詳細については、「[Always On VPNの自動再起動](#)」を参照してください。

- **管理対象VPNプロファイルでのデバッグログの有効化**

MDM管理者は、Endpoint Managementコンソールの管理対象VPNプロファイルで、カスタムパラメーターとしてデバッグログを有効にできるようになりました。デバッグログを有効にするには、`EnableDebugLogging` の値をTrueに設定する必要があります。管理対象VPN構成のいずれかでデバッグログが有効になっている場合、構成が解析されるとデバッグログ機能が有効になります。詳細については、「[Intune構成のカスタムパラメーター](#)」を参照してください。

修正された問題

- Citrix SSOアプリが、一部のリソースへのトラフィックをトンネルできない場合があります。この問題は、スプリットトンネリングがOFFに設定されており、到達不能なドメインまたはIPアドレスがブラックホール化されている場合に発生します。

V22.11.1 (30-Nov-2022)

新機能

- **Citrix Secure Access は Android 12.1 (API レベル 32) をターゲットとするように更新されました**

Citrix Secure Access は、Android 12.1 (API レベル 32) をターゲットとするように更新されました。アプリごとの VPN の場合、VPN トンネル設定後にアプリごとの VPN パッケージリスト内のいずれかのパッケージがインストールされると、VPN サービスが自動的に再起動しないことがあります。これは、Android 11 で導入されたアプリの可視性制限が原因です。詳細については、<https://developer.android.com/training/package-visibility> を参照してください。

V22.10.1 (2022年10月21日)

新機能

- アプリのバージョン番号の表示形式が YY.MM.point-release に更新されました。YY は2桁の年、MM は2桁の月、point-release は月内のリリース番号に応じて1以上となります。
- Android クライアントの場合、EU 地域からの Google Analytics/Crashlytics データ収集は無効になっています。

修正された問題

- 接続の追加画面と接続の編集画面で無効な入力に対して表示されるエラーメッセージがローカライズされていません。

V2.5.3 (2022年5月5日)

新機能

- Citrix SSO が Android 11 ターゲット SDK (API 30) に更新されました

Citrix SSO アプリは、Android 11 ターゲット SDK (API 30) に更新されました。この変更により、デバイスコンプライアンスチェックのために NetScaler Gateway で Microsoft Intune NAC v2 API を使用する必要があります。詳細については、KB 記事 <https://support.citrix.com/article/CTX331615> を参照してください。

修正された問題

- ネットワーク変更後、Citrix SSO がホスト名解決に代替 DNS サーバーを使用しない場合があります。

V2.5.2 (21-Oct-2021)

修正された問題

- NAC チェックで非標準エラーを処理する際に、Citrix SSO がクラッシュする場合があります。

V2.5.1 (12-Aug-2021)

修正された問題

- CNAME チェーンが 6 ホップを超えると、Citrix SSO アプリがホストを解決できません。
- NetScaler Gateway が NAC チェックのみの認証を要求する場合、Citrix SSO は認証プロンプトを表示します。
- 異常に大きな ICMP パケットを処理中に、Citrix SSO がクラッシュする場合があります。
- 一部のAndroid 8.0デバイスでVPNプロファイルを追加する際にCitrix SSOがクラッシュする可能性があります。
- Always On用に構成されたVPNを再起動すると、Citrix SSOがクラッシュする可能性があります。
- nFactor認証フローでSSLエラーを処理する際に、Citrix SSOがクラッシュする可能性があります。

V2.5.0 (08-Jun-2021)

新機能

- FQDNベースの分割トンネリングのサポート

Android版Citrix SSOは、FQDNベースの分割トンネリングをサポートするようになりました。

修正された問題

- Citrix SSOプレビュービルド2.5.0は、NetScaler Gatewayバージョン12.1以前への接続に失敗します (110)。
- SSOアプリの再起動後、「DisableUserProfiles」設定が適用されません。

V2.4.16 (2021年3月31日)

修正された問題

- 一部のデバイスでセーフブラウジングが有効になっていない場合、nFactor認証が中止されます。

V2.4.15 (2021年3月17日)

修正された問題

- NetScaler Gatewayアプライアンスでセッションタイムアウトが発生した場合、Citrix SSOがAlways On VPNに再接続しないことがあります。

V2.4.14 (2021年2月23日)

修正された問題

- nFactor認証と併用して証明書のための認証によるAlways-On VPNを使用する場合、Citrix SSOはユーザーの操作を必要とします。
- VPNサービスの再起動または移行中に、Citrix SSOがクラッシュすることがあります。

V2.4.13 (2021年2月4日)

修正された問題

- 場合によっては、NetScaler Gatewayが応答する前にCitrix SSOログイン要求がタイムアウトします。

V2.4.12 (2021年1月15日)

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ様々な問題に対処しています。

V2.4.11 (2021年1月8日)

- Citrix SSOがnFactor認証でのみ使用されるHTTPヘッダー (X-Citrix-Gateway) をNetScaler Gatewayに送信するため、従来の認証が失敗します。

V2.4.10 (2020年12月9日)

修正された問題

- Androidデバイスで従来の認証が失敗する場合があります。
- 従来の認証を実行すると、Citrix SSOがクラッシュする場合があります。
- デバイスを回転させても、Citrix SSOアプリの向きは変わりません。

V2.4.9 (20-Nov-2020)

修正された問題

- ユーザーがデバイス上でTOTPトークン値をタップすると、Citrix SSOアプリがクラッシュします。

V2.4.8 (04-Nov-2020)

修正された問題

- ゲートウェイでのセッションタイムアウト後にVPNを切断すると、Citrix SSOがクラッシュする可能性があります。

V2.4.7 (12-Oct-2020)

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ様々な問題に対処しています。

V2.4.6 (28-Sep-2020)

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つ様々な問題に対処しています。

V2.4.5 (16-Sep-2020)

新機能

- 新しいNetScaler®ロゴが導入されました。

V2.4.4 (2020年9月10日)

修正された問題

- VPNセッションを再接続する際に、Citrix SSOがクラッシュすることがあります。

V2.4.3

既知の問題

- Androidデバイスのリソースが制限されている場合、Citrix SSOはNetScaler GatewayへのVPNセッションを確立できません。

V2.4.2

修正された問題

- 以前に保存された破損したトークンデータを読み込む際に、Citrix SSOアプリがクラッシュします。この修正により、トークンリスト内の破損したトークンについては、トークン値が「Token data corrupted」と表示されます。破損したトークンを削除し、再度追加してください。

V2.4.1

修正された問題

- 2020年6月以降、Citrix SSOアプリはAndroid 6.x以前のバージョンではサポートされません。

V2.3.19

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題に対処しています。

V2.3.18

新機能

- Android 10デバイス向けAndroid版Citrix SSOアプリで、プロキシ構成がサポートされるようになりました。

V2.3.17

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題に対処しています。

V2.3.16

このリリースでは、全体的なパフォーマンスと安定性の向上に役立つさまざまな問題に対処しています。

V2.3.15

新機能

- Citrix SSOアプリは、管理対象VPNプロファイル向けのNetScaler Gateway証明書ピンニングをサポートするようになりました。
- Android 10向けCitrix SSOアプリは、システム設定からAlways On VPNを検出するようになりました。

修正された問題

- MDM VPNプロファイルのみが定義されている場合、VPNから切断するとCitrix SSOアプリがクラッシュします。

V2.3.14

新機能

- Citrix SSOアプリは、ネイティブアプリのシングルサインオンのためにCitrix Workspaceアプリの代わりにユーザー認証を実行できるようになりました。
- VPNトンネル設定後にアプリごとのVPNパッケージリスト内のいずれかのパッケージがインストールされた場合、VPNサービスが再起動します。

修正された問題

- Citrix SSO は、最終的な VPN セッション確立メッセージを正しく処理するようになりました。

- NetScaler Gateway の IP アドレスは、一度だけ解決されるようになりました。以前は、NetScaler Gateway の IP アドレスが複数回解決され、接続障害が発生することがありました。

既知の問題

- Always-On VPN のステータスが、アプリのユーザーインターフェイスで常に正しく更新されずとは限りません。

V2.3.13

修正された問題

- NetScaler Gateway の IP アドレスは、一度だけ解決されるようになりました。

以前は、NetScaler Gateway の IP アドレスが複数回解決され、接続障害が発生することがありました。

既知の問題

- Always-On VPN のステータスが、アプリのユーザーインターフェイスで常に正しく更新されずとは限りません。

V2.3.12

修正された問題

- VPNプロファイルを保存する際にCitrix SSOがクラッシュする場合があります。

V2.3.11

修正された問題

- VPNプロファイルを保存する際にCitrix SSOがクラッシュする場合があります。
- 新しいVPNプロファイルまたは既存のプロファイルの更新によってdisableUserProfile値が変更された場合、disableUserProfile設定がユーザーインターフェイスに正しく反映されません。
- Android版Citrix SSOは、Device Owner (DO) モードでVPNプロファイルを処理しません。

- IPv6のみのローカルDNSサーバーがある場合、VPN接続が確立されません。

V2.3.10

修正された問題

- デバイスが一定時間アイドル状態になった後、VPN接続が失われる。

V2.3.8

新機能

- **Intune Android Enterprise環境でCitrix SSOアプリをセットアップする**

Intune Android Enterprise環境でCitrix SSOアプリをセットアップできるようになりました。詳細については、「[Intune Android Enterprise環境でCitrix Secure Accessをセットアップする](#)」を参照してください。

- **Android Enterpriseを介したVPNプロファイルプロビジョニングのサポート**

Android Enterpriseを介したVPNプロファイルプロビジョニングがサポートされるようになりました。

修正された問題

- 既に保存されているトークンを保存し、その後開こうとすると、トークン名に文字化けが表示される。
- NetScaler GatewayでDNS検索ドメインが設定されていない場合、Citrix SSOアプリはVPNセッションを確立できない。

V2.3.6

新機能

- **Citrix SSO の Always On サポート**

Citrix SSO の Always On 機能により、ユーザーは常にエンタープライズネットワークに接続されます。この永続的な VPN 接続は、VPN トンネルの自動確立によって実現されます。

- **Athena トークンの有効期限切れによりログアウトした場合、再ログインの通知が表示される**

以下の条件が満たされた場合、Citrix Workspace に再ログインするようユーザーに促す通知が表示されます。

- Citrix Workspace でプロビジョニングされた VPN プロファイルで Always On 機能が有効になっている
- SSO に Athena 認証が使用されている
- Athena トークンの有効期限切れにより、ユーザーが Citrix Workspace アプリからサインアウトされた

- **プッシュ通知サービスの登録は NetScaler Gateway を使用して行われる**

NetScaler Gateway アプライアンスを使用して、プッシュ通知サービスに登録できるようになりました。以前は、登録はクライアントデバイスで行われていました。

修正された問題

新しいトークンがスキャンされると、Citrix SSOがクラッシュすることがあります。たとえば、既存のトークンが削除され、同じトークン名で別のトークンがスキャンされると、Citrix SSOがクラッシュします。

V2.3.1

新機能

- **管理対象構成が更新され、より多くのユーザー設定が含まれるようになりました**

管理対象構成が更新され、Android Enterprise環境向けに「BlockUntrustedServers」、「DefaultProfileName」、「DisableUserProfiles」の設定が含まれるようになりました。

- **強化されたプッシュ通知のサポート**

NetScaler Gatewayを「OTP」タイプのプッシュ通知用に構成すると、認証の続行を許可するユーザーの同意を求めるプッシュ通知に応答してユーザーが「許可」を選択した後、PIN/指紋は要求されません。

- **Firebase Analyticsのサポート**

Citrix SSOアプリの利用状況情報を提供するために、基本的なFirebase Analyticsのサポートが追加されました。この機能強化は、おおまかな地理的位置情報、画面の使用状況、使用中のAndroidの異なるバージョンなどに適用されます。

- **Android管理対象構成に基づくVPNプロファイル構成のサポート**

Citrix Endpoint ManagementのようなEMM/UEMベンダーを使用して、Android Enterprise環境でCitrix SSOアプリを設定できます。CEMのAndroid Enterpriseマネージド構成ウィザードを使用して、マネージドVPN構成をCitrix SSOアプリに展開できます。マネージド構成を使用してCitrix SSOアプリを設定する方法については、[VPNデバイスポリシー](#)を参照してください。

V2.2.9

新機能

- **プッシュ通知のサポート**

NetScaler Gatewayは、簡素化された2要素認証エクスペリエンスのために、登録済みのモバイルデバイスにプッシュ通知を送信します。

修正された問題

- 「接続の追加」画面の「サーバー」フィールドで、URL以外の文字が許可されています。

MDM環境でのCitrix Secure Accessのセットアップ

重要：

Android向けCitrix SSOは、現在Citrix Secure Accessと呼ばれています。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。

MDM環境でCitrix Secure Accessをセットアップするには、「[Android向けCitrix Secure Accessプロトコルの構成](#)」を参照してください。

メモ：

- MDM 以外の環境では、ユーザーは VPN プロファイルを手動で作成します。
- Citrix Secure Access用のAndroid Enterprise管理構成を作成することもできます。詳しくは、[Android Enterprise 用の VPN プロファイルの設定を参照してください](#)。
- Citrix Secure Access 23.12.1以降を使用しているAndroid 13以降のユーザーの場合、MDM管理者はソリューション内のCitrix Secure Access（パッケージID: `com.citrix.CitrixVPN`）に通知権限を付与することをお勧めします。

Intune Android Enterprise環境でCitrix Secure Accessをセットアップする

重要：

Android向けCitrix SSOは、現在Citrix Secure Accessと呼ばれています。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。

このトピックでは、Microsoft Intune による Citrix Secure Access の展開と構成について詳しく説明します。このドキュメントでは、Intune がすでに Android Enterprise サポート用に設定されており、デバイスの登録がすでに行われていることを前提としています。

前提条件

- Intune は Android Enterprise サポート用に設定されています
- デバイス登録が完了しました

Intune Android Enterprise環境でCitrix Secure Accessをセットアップするには

- Citrix Secure Accessを管理対象アプリとして追加
- Citrix Secure Accessの管理対象アプリケーションポリシーの設定

Citrix Secure Accessを管理対象アプリとして追加

1. Azure Portalにログインします。
2. 左側のナビゲーションブレードの **Intune** をクリックします。
3. Microsoft Intune ブレードで をクリックし、ブレードの をクリックします。

4. 右上のメニューオプションで をクリックします。ブレードが表示されます。
5. アプリの種類として を選択します。

これにより、Android Enterprise を設定している場合、Google Play の検索を管理してブレードを承認するが追加されます。

6. 「Citrix Secure Access」を検索し、アプリのリストから選択します。



****注：****Citrix Secure Accessがリストに表示されない場合は、そのアプリがお住まいの国では利用できないことを意味します。

7. 「承認」をクリックして、管理対象Google Play ストアを通じてCitrix Secure Accessを導入することを承認します。

Citrix Secure Accessに必要な権限が一覧表示されます。

8. をクリックして、アプリの展開を承認します。
9. をクリックして、この選択を Intune と同期します。

Citrix Secure Accessがクライアントアプリリストに追加されました。多くのアプリが追加されている場合は、Citrix Secure Accessを検索しなければならない場合があります。

10. **Citrix Secure Access**アプリをクリックして、アプリの詳細ブレードを開きます。
11. 詳細ブレードの をクリックします。**Citrix Secure Access-アサインメントブレード**が表示されます。



12. 「グループの追加」をクリックして、Citrix Secure Accessのインストール権限を付与するユーザーグループを割り当てて、「保存」をクリックします。
13. Citrix Secure Accessの詳細ブレードを閉じます。

Citrix Secure Accessが追加され、ユーザーへの展開が可能になりました。

Citrix Secure Accessの管理対象アプリケーションポリシーの設定

Citrix Secure Accessを追加したら、VPNプロファイルをデバイス上のCitrix Secure Accessに展開できるように、Citrix Secure Accessの管理対象構成ポリシーを作成する必要があります。

1. Azure Portalで **Intune** ブレードを開きます。
2. Intune ブレードから ブレードを開きます。
3. ブレードから 項目を選択し、 をクリックして ブレードを開きます。
4. ポリシーの名前を入力し、その説明を追加します。

5. で、 を選択します。
6. で、 を選択します。

これにより、関連付けられたアプリに別の構成オプションが追加されます。

7. 「**関連アプリ**」をクリックし、「**Citrix Secure Accessアプリ**」を選択します。

アプリが多いなら検索しなきゃいけないかも。

8. **[OK]** をクリックします。構成設定オプションが ブレードに追加されます。
9. をクリックします。

Citrix Secure Accessを構成するためのブレードが表示されます。

10. **[構成設定]** で、**[構成デザイナーを使用する]** または **[JSONデータを入力する]** を選択して、Citrix Secure Accessを構成します。



注:

単純な VPN 構成の場合は、構成デザイナーを使用することをお勧めします。

構成デザイナーを使用した VPN 構成

1. で、 を選択し、 をクリックします。

Citrix Secure Accessでサポートされているさまざまなプロパティを構成するためのキー値入力画面が表示されます。少なくとも、**サーバーアドレス**と**VPN プロファイル名**のプロパティを設定する必要があります。セクションにマウスポインターを合わせると、各プロパティの詳細が表示されます。

2. たとえば、**[VPN プロファイル名]** および **[サーバーアドレス (*)]** プロパティを選択し、**[**OK]**** をクリックします。

これにより、プロパティが構成デザイナーに追加されます。次のプロパティを設定できます。

- **VPN プロファイル名**。VPNプロファイルの名前を入力します。複数のVPNプロファイルを作成している場合は、それぞれに一意の名前を使用します。名前を指定しない場合、フィールドに入力したアドレスが VPN プロファイル名として使用されます。
- **サーバーアドレス (*)**。NetScaler Gatewayのベース完全修飾ドメイン名を入力します。NetScaler Gatewayのポートが443ではない場合は、ポートも入力します。URL形式を使用します。例： `https://vpn.mycompany.com:8443` 。

- **ユーザー名（オプション）**。エンドユーザーがNetScaler Gateway への認証に使用するユーザー名を入力します。ゲートウェイがそれを使用するように設定されている場合は、このフィールドに Intune設定値トークン{{userprincipalname}}を使用できます（設定値トークンを参照）。ユーザー名を指定しない場合、ユーザーはNetScaler Gateway に接続するときにユーザー名の入力を求められます。
- **パスワード（オプション）**。エンドユーザーがNetScaler Gateway への認証に使用するパスワードを入力します。パスワードを指定しない場合、ユーザーはNetScaler Gateway に接続するときにパスワードの入力を求められます。
- **証明書エイリアス（オプション）**。クライアント証明書認証に使用する証明書エイリアスを Android KeyStore に提供します。証明書ベースの認証を使用している場合、この証明書はユーザーに対して事前に選択されています。
- **ゲートウェイ証明書ピン (オプション)**。NetScaler Gateway で使用される証明書ピンを記述するJSONオブジェクト。値の例：

```
{"hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"]}
```

。詳しくは、「[Android Citrix Secure AccessによるNetScaler Gateway 証明書ピン留め](#)」を参照してください。
- **Per-App VPNの種類（オプション）**。アプリごとのVPNを使用してこのVPNを使用するアプリを制限している場合は、この設定を構成できます。
 - **[許可]** を選択すると、PerAppVPN アプリ一覧に表示されるアプリパッケージ名のネットワークトラフィックがVPN 経由でルーティングされます。ほかのアプリのネットワークトラフィックは、すべてVPN外でルーティングされます。
 - **[許可しない]** を選択した場合、[Per-App VPNアプリ一覧] に含まれるアプリパッケージ名のネットワークトラフィックがVPN外でルーティングされます。ほかのアプリのネットワークトラフィックは、すべてVPNを介してルーティングされます。デフォルトは [許可] です。
- **perAppVPN アプリリスト**。[Per-App VPNの種類] の値に応じ、トラフィックがVPNで許可されるか、または許可されないアプリの一覧。アプリパッケージ名がカンマまたはセミコロンで区切って一覧にされます。アプリパッケージ名は大文字と小文字が区別され、この一覧でもGoogle Playストアに表示されているのと同じように表示される必要があります。この一覧はオプションです。デバイス全体のVPNをプロビジョニングする場合は、この一覧を空のままにします。
- **デフォルトの VPN プロファイル**。常時接続VPNがCitrix Secure Access用に構成されている場合に使用されるVPNプロファイル名。このフィールドが空の場合、接続にはメインプロファイルが使用されます。プロファイルが 1 つだけ設定されている場合、そのプロファイルはデフォルトの VPN プロファイルとしてマークされます。

- **常時接続VPN (オプション):** True に設定すると、VPN プロファイルが常時接続 VPN プロファイルであることを示します。このプロパティは、メイン VPN プロファイルにのみ設定できます。追加の VPN プロファイルには設定できません。デフォルトでは、このプロパティは False に設定されています。

注：

`Always On VPN (optional)` プロパティは、Android 24.04.1以降のCitrix Secure Accessから入手できます。

**注：**

- Citrix Secure AccessをIntune で常時稼働VPNアプリとして作成するには、VPNプロバイダーをカスタムおよび `com.citrix.CitrixVPN` をアプリパッケージ名として使用します。
- Citrix Secure AccessによるAlways On VPNでは、証明書ベースのクライアント認証のみがサポートされています。
- Citrix Secure Accessが意図したとおりに動作するには、管理者がNetScaler GatewayのSSLプロファイルまたはSSL****プロパティで [クライアント認証] を選択し、[クライアント証明書] を [必須] に設定する必要があります。

• ユーザープロファイルの無効化

- この値を true に設定すると、ユーザーはデバイスに新しい VPN プロファイルを追加できません。
- この値を false に設定すると、ユーザーは自分のデバイスに独自の VPN を追加できます。

デフォルト値は false です。

• 信頼できないサーバーをブロックする

- NetScaler Gateway で自己署名証明書を使用する場合、またはNetScaler Gateway 証明書を発行するCAのルート証明書がシステムCAリストにない場合は、この値をfalseに設定します。

- 。AndroidオペレーティングシステムがNetScaler Gateway 証明書を検証できるようにするには、この値をtrueに設定します。検証に失敗した場合、接続は許可されません。

デフォルト値は、trueです。

3. プロパティに、VPN ゲートウェイのベース URL (`https://vpn.mycompany.com` など) を入力します。
4. 「**VPNプロファイル名**」には、Citrix Secure Accessクライアントのメイン画面でエンドユーザーに表示される名前 (「マイコーポレートVPN」など) を入力します。
5. NetScaler Gateway 展開環境には、必要に応じて他のプロパティを追加および構成できます。設定が完了したら、「**OK**」をクリックします。
6. 「**権限**」セクションをクリックします。Citrix Secure Accessに必要な次の権限を付与できます：

- Intune NACチェックを使用している場合、Citrix Secure Accessでは、**電話状態（読み取り）** 権限を付与する必要があります。ボタンをクリックして、ブレードを開きます。現在、Intune には、すべてのアプリで使用できるアクセス許可の重要なリストが表示されます。
- Intune NAC チェックを使用している場合は、**電話の状態（読み取り）** 権限を選択し、**OK**をクリックします。これにより、アプリの権限のリストに追加されます。Intune NAC チェックが機能するように または のいずれかを選択し、 をクリックします。



- Citrix Secure Accessに通知権限を自動付与することをお勧めします。

注：

Citrix Secure Access 23.12.1以降を使用しているAndroid 13以降のユーザーの場合、MDM管理者はソリューション内のCitrix Secure Access（パッケージID: `com.citrix.CitrixVPN`）に通知権限を付与することをお勧めします。

7. アプリ構成ポリシーブレードの下部にある「**追加**」をクリックして、Citrix Secure Accessの管理対象構成を保存します。
8. ブレードの をクリックして、** ブレードを開きます。
9. このCitrix Secure Access構成を配信して適用したいユーザーグループを選択します。

JSON データを入力することによる VPN の設定

1. [構成設定] で、[JSONデータを入力してCitrix Secure Accessを構成する] を選択します。
2. [JSONテンプレートのダウンロード] ボタンを使用して、Citrix Secure Accessのより詳細で複雑な構成を提供できるテンプレートをダウンロードします。このテンプレートは、Citrix Secure Accessが認識できるすべてのプロパティを構成するためのJSONキーと値のペアのセットです。

構成可能なすべてのプロパティの一覧については、「[Citrix Secure AccessアプリでVPNプロファイルを構成するために使用できるプロパティ](#)」を参照してください。

3. JSON 設定ファイルを作成したら、その内容をコピーして編集領域に貼り付けます。たとえば、構成デザイナーオプションを使用して以前に作成された基本設定の JSON テンプレートを次に示します。



これで、Microsoft Intune Android Enterprise環境で Citrix Secure Access の VPN プロファイルを構成および展開する手順は完了です。

重要:

クライアント証明書ベースの認証に使用される証明書は、Intune SCEP プロファイルを使用して展開されます。この証明書のエイリアスは、Citrix Secure Accessの管理対象構成の「**証明書エイリアス**」プロパティで構成する必要があります。

Citrix Secure AccessでVPNプロファイルを構成するために使用できるプロパティ

構成キー	JSON フィールド名	値の種類	説明
VPN プロファイル名	VPN プロファイル名	テキスト	VPN プロファイルの名前（デフォルトはサーバアドレスに設定されていない場合）。
サーバーアドレス (*)	サーバーアドレス	URL	接続のNetScaler Gateway のベース URL (<code>https://host[:port]</code>)。これは必須フィールドです。

構成キー	JSON フィールド名	値の種類	説明
Username (オプション)	ユーザー名	テキスト	NetScaler Gatewayでの認証に使用されるユーザー名 (オプション)。
パスワード (オプション)	パスワード	テキスト	NetScaler Gatewayでの認証に使用されるユーザーのパスワード (オプション)。
証明書エイリアス (オプション)	ClientCertAlias	テキスト	証明書ベースのクライアント認証に使用するためにAndroid資格情報ストアにインストールされているクライアント証明書のエイリアス (オプション)。NetScaler Gatewayで証明書ベースの認証を使用する場合、 証明書エイリアス は必須フィールドです。
ゲートウェイ証明書ピン (オプション)	ServerCertificatePins	JSONテキスト	NetScaler Gatewayに使用される証明書PINを記述する埋め込みJSONオブジェクト。値の例： <pre> {"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAA AAAAAAAAAAAA=", "BBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBB BBBBBBBBBBBBBBBB"] } </pre> JSONコンフィギュレーターを使用する

構成キー	JSON フィールド名	値の種類	説明
			ときは、この埋め込まれたJSONデータを必ずエスケープしてください。
Per-App VPNの種類 (オプション)	PerAppVPN_Allow_Disallow_Setting	列挙型 (許可、不許可)	リストにあるアプリでVPNトンネルを使用することを許可 (許可リスト) または拒否 (禁止リスト) していますか。 【許可】 に設定すると、リストされているアプリ (perAppVPN アプリリストプロパティ内) のみがVPN経由のトンネリングを許可されます。【許可しない】 に設定すると、一覧表示されているアプリを除くすべてのアプリがVPN経由のトンネリングを許可されます。アプリがリストに表示されない場合、すべてのアプリがVPN経由でトンネリングできます。
perAppVPN アプリリスト	PERAppName_appNames	テキスト	Per-App VPNのアプリパッケージ名をカンマ (,) またはセミコロン (;) で区切ったリスト。パッケージ名は、Google Play ストアのアプリ一覧ページの URL に表示されているものと同じである必要があ

構成キー	JSON フィールド名	値の種類	説明
			ります。パッケージ名では大文字と小文字が区別されます。
デフォルトのVPNプロファイル	DefaultProfileName	テキスト	システムがVPNサービスを開始するときに使用するVPNプロファイルの名前。この設定は、デバイスでVPN常時接続が構成されている場合に使用するVPNプロファイルを識別するために使用されます。
常時接続 VPN (オプション)	IsAlwaysOnVpn	ブーリアン型	VPN プロファイルが Always ON VPN プロファイルであるかどうかを判断します。True に設定すると、VPN プロファイルが常時接続 VPN プロファイルであることを示します。このプロパティは、メイン VPN プロファイルでのみ設定できます。追加の VPN プロファイルには設定できません。デフォルト値はFalseです。 このプロパティは、Citrix Secure Access for Android 24.04.1リリース以降から使用できます。

構成キー	JSON フィールド名	値の種類	説明
ユーザープロファイルの無効化	DisableUserProfiles	ブーリアン型	エンドユーザーが手動でVPNプロファイルを作成することを許可または禁止するプロパティ。ユーザーがVPNプロファイルを作成できないようにするには、この値を true に設定します。デフォルト値は false です。
信頼できないサーバーをブロックする	BlockUntrustedServers	ブーリアン型	信頼できないゲートウェイへの接続をブロックするかどうかを決定するプロパティ（たとえば、自己署名証明書を使用する場合や、発行したCAがAndroidオペレーティングシステムによって信頼されていない場合など）。デフォルト値はtrue（信頼できないゲートウェイへの接続をブロック）です。
カスタムパラメーター（オプション）	CustomParameters	一覧	Citrix Secure Accessでサポートされているカスタムパラメーター（オプション）のリスト。詳細については、「 カスタムパラメータ 」を参照してください。使用可能なオプションについては、 NetScaler Gateway製品ドキュ

構成キー	JSON フィールド名	値の種類	説明
			メントを確認してください。
その他のVPNプロファイルのリスト	bundle_profiles	一覧	その他のVPNプロファイルのリスト。各プロファイルの前述の値のほとんどがサポートされています。詳しくは、「 VPN プロファイルリストの各VPNでサポートされるプロパティ 」を参照してください。

カスタムパラメータ

各カスタムパラメータは、次のキーと値の名前を使用して定義する必要があります。

キー	値の種類	値
ParameterName	テキスト	カスタムパラメータの名前。
ParameterValue	テキスト	カスタムパラメータの値。

Intune 設定のカスタムパラメータ

パラメーター名	説明	値
UserAgent	Citrix Secure Accessは、NetScaler Gatewayと通信するときに、このパラメーター値をユーザーエージェントのHTTPヘッダーに追加して、NetScaler Gatewayで追加のチェックを実行します。	ユーザーエージェント HTTPヘッダーに追加する必要があるテキストを指定します。テキストは、HTTP ユーザーエージェント仕様に準拠している必要があります。
EnableDebugLogging	Citrix Secure Accessのデバッグログを有効にすると、常時接続VPNの場合にVPN接続の問題のトラブルシューティングに役立ちます。このオブ	True ：デバッグのログを有効にします。デフォルト値: False 。

パラメーター名	説明	値
	ションは、管理対象のVPN構成のいずれかで有効にすることができます。デバッグのログは、管理対象の構成を処理するときに有効になります。	

カスタムパラメータについて詳しくは、「[Citrix Secure Access用のAndroid Enterprise管理構成の作成](#)」を参照してください。

VPN プロファイルリストの各 VPN でサポートされるプロパティ

JSON テンプレートを使用して複数の VPN プロファイルを設定する場合、各 VPN プロファイルで次のプロパティがサポートされます。

構成キー	JSON フィールド名	値の種類
VPN プロファイル名	bundle_vpnProfileName	テキスト
サーバーアドレス (*)	bundle_serverAddress	URL
ユーザー名	bundle_username	テキスト
パスワード	bundle_password	テキスト
クライアント証明書エイリアス	bundle_clientCertalias	テキスト
ゲートウェイ証明書ピン	bundle_serverCertificatePins	テキスト
Per-App VPNの種類	bundle_perappVPN_allow_disallow_setting	列挙型 (許可、不許可)
perAppVPN アプリリスト	bundle_perappVPN_appnames	テキスト
カスタムパラメータ	bundle_customParameters	一覧

Intune で Citrix Secure Accessを常時接続の VPN プロバイダーとして設定する

Android VPNサブシステムにオンデマンドVPNサポートがない場合は、Always On VPNを代替手段として使用して、Citrix Secure Accessによるクライアント証明書認証とともにシームレスなVPN接続オプションを提供できます。VPN は、起動時または仕事用プロファイルが有効になったときに、オペレーティングシステムによって起動されます。

Citrix Secure AccessをIntune で常時稼働のVPNアプリにするには、次の設定を使用する必要があります。

- 使用する適切な管理対象設定の種類（仕事用プロファイルで個人所有または完全管理型、専用型、および企業所有の仕事用プロファイル）を選択します。
- デバイス構成プロファイルを作成し、を選択し、 セクションに移動します。VPN常時接続設定で を選択します。
- VPNクライアントとして**Citrix Secure Access**を選択します。Citrix Secure Accessがオプションとして利用できない場合は、「VPNクライアントとして**カスタム**」を選択し、「パッケージID」フィールドに「**com.citrix.CitrixVPN**」と入力します（パッケージIDフィールドは大文字と小文字が区別されます）
- 他のオプションはそのままにしておきます。ロックダウンモードを有効にしないことをお勧めします。有効にすると、VPN が利用できない場合、デバイスは完全なネットワーク接続を失う可能性があります。
- これらの設定に加えて、前のセクションで説明したように、 ページでPer-App VPNの種類と****PerAppVPN アプリリストを設定して**、AndroidのPer-App VPNを有効にすることもできます。

注：

常時接続VPNは、Citrix Secure Accessのクライアント証明書認証でのみサポートされます。

参照ドキュメント

Intune での接続オプションの設定の詳細については、次のトピックを参照してください。

- 完全に管理された企業所有の専用デバイス
- 個人所有のデバイス

常時接続 VPN の自動再起動

Citrix SSO for Android 23.8.1以降、許可リストまたは禁止リストに含まれるアプリが仕事用プロファイルまたはデバイスプロファイルにインストールされている場合、Citrix Secure AccessはAlways On VPNを自動的に再起動します。新しくインストールされたアプリからのトラフィックは、仕事用プロファイルを再起動したりデバイスを再起動したりすることなく、VPN接続を介して自動的にトンネリングされます。

Always On VPNの自動再起動を有効にするには、エンドユーザーがCitrix Secure Accessに「[すべてのパッケージを照会](#)」の許可を与える必要があります。同意が得られたら、Citrix Secure Access：

- オペレーティングシステムからパッケージインストール通知を受け取ります。
- 常時接続 VPN を再起動します。

エンドユーザーがアプリごとのVPNプロファイルに初めて接続すると、インストールされたパッケージの情報を収集するための同意を求めるメッセージが表示されます（Googleのポリシーで義務付けられています）。エンドユーザーが同意すると、VPN 接続が開始されます。ユーザーが同意を拒否した場合、VPN 接続は中止されます。同意した後は、同意画面は再表示されません。エンドユーザーの手順について詳しくは、「[AndroidデバイスからCitrix Secure Accessを使用する方法](#)」を参照してください。

制限事項

Android 11で導入された[パッケージの公開設定の制限](#)により、Android 11以降のデバイス上のAndroid Enterprise環境におけるPer-App VPNには、次の制限が適用されます。

- 許可/拒否リストに含まれるアプリが VPN セッションの開始後にデバイスに展開された場合、アプリがそのトラフィックを VPN セッション経由でルーティングできるようにするには、エンドユーザーが VPN セッションを再起動する必要があります。
- Per-App VPNをVPN常時接続セッションで使用する場合、デバイスに新しいアプリをインストールした後、エンドユーザーは仕事用プロファイルを再起動するか、デバイスを再起動して、アプリのトラフィックを VPN セッション経由でルーティングする必要があります。

注：

これらの制限は、Android向けCitrix SSO 23.8.1以降のバージョンを使用している場合には適用されません。詳細については、「[Always On VPN の自動再起動](#)」を参照してください。

Android向けCitrix Secure AccessによるNetScaler Gateway証明書ピン留め

重要：

Android向けCitrix SSOは、現在Citrix Secure Accessと呼ばれています。この名前の変更を反映するために、ドキュメントとUIスクリーンショットを更新中です。

証明書のピン留めは、中間者攻撃の防止に役立ちます。Citrix Secure Accessは、Android Enterpriseモードとレガシーデバイス管理者モードの管理対象VPN構成でのみ証明書ピン留めをサポートします。エンドユーザによって追加されたVPNプロファイルではサポートされません。

Android Citrix Secure AccessによるNetScaler Gateway の証明書ピン留めの設定

Citrix Secure Accessの管理対象構成（旧アプリ制限）における証明書ピン留めについて詳しくは、「[証明書と認証](#)」を参照してください。

固定されたNetScaler Gateway 証明書ハッシュを伝送するために、新しいキーと値のペアが次のように定義されます。

```
Key: ServerCertificatePins

Value: {

    "hash-alg": "sha256",

    "pinset": [

        "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo(SPKI)"
        ,

        "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",

        "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="

        ...

    ]
}
```

}

管理対象構成で証明書ピン留めの詳細を指定するためのキーは **ServerCertificatePins** です。この値は、固定された NetScaler Gateway 証明書の base64 でエンコードされた SHA-256 ハッシュと使用されるハッシュアルゴリズムを運ぶ JSON ペイロードです。固定証明書には、オペレーティングシステムによって検証された信頼チェーン内の任意の証明書を使用できます。この場合、それは Android です。

証明書のピン留めは、オペレーティングシステムが TLS ハンドシェイク中に証明書チェーンを検証した後にのみ実行されます。証明書の PIN は、証明書のサブジェクト公開キー情報 (SPKI) をハッシュすることによって計算されます。JSON ペイロードには、両方のフィールド (「**hash-alg**」と「**pinset**」) を指定する必要があります。

「**hash-alg**」は、SPKI ハッシュの計算に使用されるハッシュアルゴリズムを指定します。「**ピンセット**」は、NetScaler Gateway 証明書の SPKI データの base64 でエンコードされた SHA-256 ハッシュを含む JSON 配列を指定します。証明書の PIN には少なくとも 1 つの値を指定する必要があります。証明書のローテーションまたは有効期限を許可するために、PIN 値をさらに指定できます。

次の openssl コマンドを使用して、ドメイン（たとえば、gw.yourdomain.com）の暗証番号の値を計算できます。

```
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
```

このコマンドは、ゲートウェイによって提示されたリーフ証明書の base64 エンコードされた SHA-256 ハッシュを表示します。チェーン内の任意の証明書を証明書のピン留めに使用できます。たとえば、企業が独自の中間 CA を使用して複数のゲートウェイの証明書を生成している場合、中間署名証明書に対応する PIN を使用できます。検証済みの証明書チェーン内の証明書と一致する PIN がいない場合、TLS ハンドシェイクは中止され、ゲートウェイへの接続は続行されません。

注：

デバイス管理者モードでは、証明書のピン留めは、Citrix Endpoint Managementおよび Microsoft Endpoint Managementソリューションでのみサポートされます。証明書のピン留めは、レガシー VPN プロファイル（管理対象設定ではない）で使用されるカスタムパラメータで、固定用の同じ JSON ペイロードを持つカスタムパラメータ `serverCertificatePins` で設定する必要があります。

Citrix Secure Access for Windows リリースノート

Windows向けCitrix Secure Accessクライアントは現在スタンドアロンベースでリリースされており、すべてのNetScalerバージョンと互換性があります。最新の修正と拡張機能が含まれている最新バージョンのCitrix Secure Accessクライアントを使用することをお勧めします。

Citrix Secure Access クライアントのリリースは、YY.MM.Release.build という形式になっています。

リリースノートでは、新機能、既存機能の拡張、修正された問題について説明しています。

新機能:現在のリリースで利用可能な新機能と機能強化。

修正された問題:現在のリリースで修正された問題。

サポートされる機能について詳しくは、[NetScaler Gateway 製品ドキュメント](#)を参照してください。

メモ：

- Citrix Secure Access バージョン24.6.1.18が24.6.1.17に取って代わり、一般公開されました。
- Windows向けCitrix Secure Accessクライアントビルド23.7.1.1以降には、<https://support.citrix.com/article/CTX564833> の修正が含まれています。
- Citrix Secure Access for Windows 23.5.1.3以降のリリースでは、<https://support.citrix.com/article/CTX561480/citrix-secure-access-client-for-windows-security-bulletin-for-cve202324491> で説明されているセキュリティの脆弱性に対処しています。
- Citrix Secure Access クライアント（以前はWindows用NetScaler Gatewayプラグインとして知られていました）ビルド21.9.1.2以降には、<https://support.citrix.com/article/CTX341455> の修正が含まれています。

24.6.1.18 (2024年7月24日)

重要な更新：

Citrix Secure Access バージョン24.6.1.18は24.6.1.17に代わるもので、現在一般公開されています。

新機能

- **EPA スキャンによるCitrix Workspaceアプリのバージョンの確認**

Citrix Secure Access は、Windowsマシン上のCitrix Workspaceバージョンを検証する新しいEPAスキャン「CWAバージョン」をサポートしています。サポートされている EPA スキャンの詳細については、「[式文字列](#)」を参照してください。

- **Citrix Workspaceアプリを使用したCitrix Secure Accessへの自動シングルサインオン**

Citrix Workspaceアプリは、Citrix Secure Access 向けの統一されたクライアント管理エクスペリエンスを提供します。ユーザーがCitrix Workspaceアプリにログオンすると、Citrix Secure Accessに自動的にサインオンし、複数のクライアントアプリケーションを手動で構成してサインインしなくても、TCP/UDPアプリケーションにシームレスにアクセスできます。詳しくは、「[Windows向けCitrix Workspaceアプリを介したCitrix Secure Accessへの自動シングルサインオン-プレビュー](#)」を参照してください。

- **Secure Private Accessでのトンネル除外サポート**

Citrix Secure Accessは、レジストリ、`ExcludeDomainsFromTunnel` を使用して特定のアプリケーショントラフィックをトンネリングから除外できるようになりました。

`example.com` が複数のアプリケーションをホストするイントラネットドメインで、`sshhost.example.com`、`rdphost.example.com`、`*.ftphost.example.com` などの特定のアプリケーションを除外したい場合は、このレジストリを使用できます。

詳しくは、「[NetScaler Gateway Windows VPN クライアントレジストリキー](#)」を参照してください。

- **TCP ベースの DNS リクエストの IP アドレススプーフィング**

Citrix Secure Accessは、以下のシナリオでTCPベースのDNSリクエストのIPアドレススプーフィングをサポートします：

- FQDNベースのトンネリングルールはNetScaler Gatewayで構成されます。
- FQDNは、Citrix Secure Private Access 環境のDNSサフィックスと一致します。

- **サードパーティのセキュア Web ゲートウェイとの相互運用性の強化**

Citrix Secure Accessのユーザーエージェント文字列が更新され、サードパーティのセキュア Webゲートウェイとの相互運用性が強化されました。

- **オンプレミス向けCitrix Secure Private Access サポート**

Citrix Secure Accessは、オンプレミス向けのCitrix Secure Private Access サポートするようになりました。

- **EPA スキャン暗号化の強化**

EPA スキャンのセキュリティ暗号化は、楕円曲線ディフィー・ヘルマン (ECDH) キーによって強化されています。

- **署名作成用のハッシュキー**

管理者はSHA-384ハッシュキーを使用してデバイス証明書認証の署名を作成できるようになりました。

- **POP 障害時のシームレス接続**

Secure Private Access環境では、現在の POP への接続に障害が発生すると、VPN ユーザは手で操作しなくても自動的に別のポイントオブプレゼンス (POP) に再接続されます。

- **診断機能の強化**

Citrix Secure Accessの診断機能が強化され、TCP/UDPアプリでのアクセス問題のトラブルシューティングに役立つフィールドが追加されました。

解決された問題

- Windows 管理インストルメンテーションコマンドライン (WMIC) 機能が無効になっていると、Windows 11 デバイスで DNS 解決が失敗します。
- Citrix Secure Accessは、NetScaler GatewayでリバーススプリットトンネリングとイントラネットIPアドレスが構成されている場合、IPv6トラフィックがループバックインターフェイスを介してルーティングされないようにします。

- ,
- イン트라ネットアプリケーションのIPアドレス範囲がワイルドカードサブネットマスクで構成されている場合、Citrix Secure Accessがクラッシュします。
- NetScaler GatewayでリバーススプリットトンネリングとイントラネットIPアドレスが構成されている場合、アップグレード後にユーザーはMicrosoftアプリケーションに接続できません。
- Citrix Secure Access ClientがWFPを使用して構成されている場合、アクティブなセッション中、またはログインとログアウトが複数回発生すると、VPN接続が失われます。
- クライアントマシン上のアプリケーションが `A` および `AAAA` レコードタイプのDNS クエリを送信すると、DNS 解決が遅れます。
- Citrix Secure Private Access 環境では Kerberos 認証が失敗します。

24.4.1.7 (2024年4月30日)

解決された問題

Microsoft Edge WebViewモードで自動ログオンが失敗した場合、エンドユーザーはCitrix Secure Accessにログオンできません。

クライアントアプリケーションがAAAA レコードタイプの DNS クエリを送信すると、一部のバックエンドリソースの DNS 解決が失敗します。

,

Citrix Secure Accessは、クライアントを数時間実行すると、WFPドライバーモードで新しい接続を確立できないことがあります。

, ,

Citrix Secure Accessでは、言語が英語に設定されていても、デバイス証明書が失敗したことを示すEPAスキャンエラーメッセージが別の言語で表示されます。

WFP モードで Always On VPN が設定されている場合、VPN セッションが長引くと、インターネットとイントラネットの接続が失われる可能性があります。

「filetime」パラメータが設定されている場合、EPA スキャンは失敗します。

EPA スキャン中にファイルの MD5 チェックサム設定が失敗します。

VPNが常時接続VPNモードになっていない場合でも、Windowsの資格情報マネージャー画面にはCitrix Secure Accessアイコンが表示されます。

Citrix Secure Accessログには、IP アドレスが逆の順序で表示されます。たとえば、Microsoft EdgeブラウザーがNetScaler (IP: 192.20.4.5:24)に接続されている場合、ログメッセージは次のように表示されます。

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

アップグレード後、ユーザーがCitrix Secure Access GUIの **【ホーム】** ページボタンをクリックすると、ホームページのURLがデフォルトのブラウザーで起動しません。

Citrix Secure Private Access環境では、証明書がルートCAではなく中間CAによって署名されている場合、デバイス証明書のチェックは失敗します。

24.2.1.15 (2024年3月4日)

新機能

- **SNI のサポート**

Citrix Secure Private Access環境では、Citrix Secure Accessクライアントはすべての事前認証要求でサーバー名表示 (SNI) 拡張をサポートするようになりました。

- **TLS 1.3 のサポート**

Citrix Secure Accessクライアントは TLS 1.3 プロトコルをサポートするようになりました。TLS 1.3 は次のプラットフォームでサポートされています：

- Windows 11以降
- Windows Server 2022以降

NetScalerでTLS 1.3を構成する方法については、「[TLS 1.3プロトコルのサポート](#)」を参照してください。

- **HTTP ヘッダーの Windows OS 詳細のサポート**

Citrix Secure Accessクライアントには、Windows OSの詳細がHTTPヘッダー (ユーザーエージェント) 文字列の一部として含まれるようになりました。

解決された問題

クライアントネットワークアダプタで IPv6 が有効になっていると、DNS 解決が断続的に失敗します。

自動ログオンを使用して同時にログインしようとする、ユーザーはCitrix Secure Accessクライアントにログオンできないことがあります。

英語以外のクライアントマシンでスマートアプリコントロールが有効になっていると、Citrix Secure Accessのインストールが失敗します。

,

Citrix Secure AccessクライアントがWFPドライバーで構成されている場合、ユーザーはVPN経由で一部のアプリケーションにアクセスできません。この問題は、ファイアウォールポリシーの変更が原因で発生します。

,

EPA スキャン中にポップアップダイアログが表示されます。ただし、ユーザーが「OK」をクリックすると、EPA スキャンは通常どおり機能します。この問題は、Citrix Secure AccessクライアントUIでスウェーデン語を選択した場合（**構成** > **言語**）に発生します。

Always On VPNモードでは、NetScaler Gatewayでユーザー証明書認証が構成されていると、マシンレベルのトンネルがセッションを転送できません。

Citrix Secure Access クライアントで Windows フィルタリングプラットフォーム（WFP）ドライバーが有効になっていると、イントラネットリソースへのアクセスが断続的に失敗します。

ユーザーが **ホーム** ボタンをクリックすると、Citrix Secure AccessクライアントのUIページが断続的にフリーズします。

管理者以外のユーザーは、次の条件が満たされている場合、完全な VPN トンネルに接続できません：

- EPA は nFactor フローのファクターとして設定されます。
- Edge WebViewは有効になっています。
- Citrix EPAクライアントのコントロールアップグレード設定が **[NetScaler Gatewayの常時オン]** に設定されており、クライアントデバイスとNetScalerの間でCitrix EPAクライアントのバージョンが一致していません。

クライアントマシンのシステム証明書ストアにデバイス証明書が 1 つしか含まれていない場合、EPA デバイス証明書スキャンは失敗します。

Citrix Secure Private Access サービスに接続すると、Citrix Secure Access クライアントのログインページが断続的に空白になります。

Windows Server 2019 以降のバージョンを使用している場合、エンドユーザーは VPN 経由でクライアントマシンをドメインに接続できないことがあります。

Citrix Device Postureサービスが有効になっていると、Citrix Secure **Access**クライアントUIの接続ドロップダウンリストに不要なエントリが表示されます。

Citrix Secure Accessクライアントでシングルサインオン機能が有効になっている場合、エンドユーザーはイントラネットリソースにアクセスできません。

23.10.1.7 (2023年11月29日)

新機能

- **サーバーが開始する接続のプライベートポート範囲の設定**

サーバーが開始する接続用に、49152 ~ 64535 の範囲のプライベートポートを設定できるようになりました。プライベートポートを構成することで、ポートを使用してCitrix Secure Accessクライアントとクライアントマシン上のサードパーティアプリとの間でソケットを作成するときに発生する可能性のある競合を回避できます。プライベートポートは、「SicBeginPort」の Windows VPN レジストリを使用して設定できます。または、NetScalerのVPNプラグインカスタマイズJSONファイルを使用してプライベートポート範囲を構成することもできます。

詳しくは、「[サーバー起動接続の構成](#)」および「[NetScaler Gateway WindowsVPNクライアントのレジストリキー](#)」を参照してください。

- **シームレスな自動ログオンを実現する Kerberos 認証サポート**

Citrix Secure Accessクライアントは、自動ログオンにKerberos認証方法を使用するようになりました。このサポートの一環として、VPN クライアントのレジストリキー

「EnableKerberosAuth」が導入されました。前提条件として、管理者はNetScalerとクライアントマシンでKerberos認証を構成する必要があります。エンドユーザーは、自分のマシンにMicrosoft Edge WebView をインストールして、Kerberos 認証方法を有効にする必要があります。詳しくは、「[Kerberos 認証による自動ログオン](#)」を参照してください。

- **スプーフィング IP アドレス範囲の自動割り当て**

Citrix Secure Access Clientは、管理者が構成したスプーフィングIPアドレス範囲とIPベースのアプリケーションまたはエンドユーザーのネットワークとの間に競合がある場合に、新しいスプーフィングIPアドレス範囲を検出して適用できるようになりました。

- **Microsoft通知**

Citrix Secure Accessクライアントの通知が、Windowsマシンの通知パネルにMicrosoftの通知として表示されるようになりました。

- **ログ収集の改善**

ログ収集とトラブルシューティングを強化するため、Verbose ログレベルがデフォルトのデバッグログレベルとして使用されるようになりました。ログについて詳しくは、「クライアントユーザーインターフェイスを使用して[ログを構成する](#)」を参照してください。

解決された問題

Always Onサービスのマシントンネルがクライアントデバイスの場所を検出できない場合、Citrix Secure Accessクライアントは「接続中」状態のままになります。

Citrix Secure Access クライアントで Microsoft Edge WebView が有効になっていると、ログオン転送機能が動作しません。

Always Onサービスモードでは、デバイス証明書ベースの従来の認証ポリシーがVPN仮想サーバーにバインドされている場合、Citrix Secure AccessクライアントはNetScaler Gatewayとのマシンレベルのトンネルを確立できません。

ユーザがVPNに接続すると、着信および発信のWebex コールが失敗します。この問題は、Citrix Secure Accessクライアントで確定的ネットワークエンハンサー（DNE）ドライバーではなくWindowsフィルタープラットフォーム（WFP）ドライバーが有効になっている場合に発生します。

次の条件が満たされると、Citrix Secure Access クライアントがクラッシュします：

- SAML ポリシーが VPN 仮想サーバーにバインドされると、接続が切り替わります。
- Internet Explorer WebView サポートが有効になっています。

Citrix Secure Access クライアントのユーザーインターフェイスには、自動ログオン中に「接続」ボタンが表示されます。この問題は、UserCert 認証方法を使用してVPNに接続する場合に発生します。

マシンレベルのトンネルが構成されている場合、ローカルLANアクセス機能はCitrix Secure Accessクライアントでは機能しません。

今回のリリースでは、ローカルLANアクセス機能をマシンレベルのトンネル構成で設定できます。これを実現するには、マシントンネルモードを使用するときにローカル LAN アクセスパラメータを FORCESD に設定する必要があります。詳細については、「[ADC構成に基づいてエンドユーザーにローカルLANアクセスを強制する](#)」を参照してください。

クライアントマシンがスリープモードから複数回起動すると、Citrix Secure AccessクライアントはイントラネットアプリケーションとのVPN接続を確立できません。

23.8.1.11 (2023年10月19日)

解決された問題

NetScaler Gatewayでフォワードプロキシサポートが構成されている場合、epaPackage.exe ファイルのダウンロードに失敗することがあります。

Cドライブへのアクセスが制限されている管理者以外のユーザーでは、Citrix EPAクライアントのインストールが失敗します。

23.8.1.5 (2023年8月9日)

解決された問題

Citrix Secure Private Access・サービスを介してアプリケーションに接続すると、Kerberos SSOが失敗します。

Citrix Secure Private Accessサービスによるアプリケーションアクセスが断続的に失敗します。この問題は、Citrix Secure AccessクライアントがTCPまたはUDPトラフィックの誤った宛先IPアドレスを共有している場合に発生します。

DNSキャッシュの問題により、Citrix Secure Accessクライアントが断続的にアプリケーションを起動できなくなります。

Citrix Secure Access クライアントが Citrix 仮想アダプタに DNS サフィックスを適用できません。この問題は、Citrix 仮想アダプターが Active Directory による認証に失敗した場合に発生します。

次の条件が満たされると、Citrix Secure Access クライアントがクラッシュします：

- NetScaler Gateway仮想サーバーには、nFactor認証の要素としてクライアント証明書が含まれています。
- Microsoft Edge WebView サポートが有効になっています。

VPN に接続していると、Microsoft KB5028166 を適用した後にバックエンドリソースにアクセスできなくなる場合があります。

ポータルのカスタマイズが許可されている制限を超えると、Citrix Secure AccessクライアントはNetScaler Gatewayからの構成のダウンロードに断続的に失敗します。

既知の問題

転送ログオン機能はCitrix Secure Accessクライアントでは動作しません。この問題は、Microsoft Edge WebView が有効になっている場合に発生します。

回避策: Web ブラウザを使用してログオンし、セッションを転送します。

23.7.1.1 (2023 年 7 月 14 日)

解決された問題

リリースバージョン23.x.x.xにアップグレードした後、NetScalerでイントラネットIP範囲が構成されていると、トラフィックがVPNトンネルを通過できず、VPNアクセスがブロックされることがあります。これは、クロスプロファイルファイアウォールルールがVPNアプリケーションに適用されていない場合に発生します。

23.5.1.3 (2023 年 6 月 2 日)

解決された問題

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client` 下の「useNewLogger」レジストリを使用して改善されたログ収集を有効にすると、Always On サービスがクラッシュします。

23.4.1.5 (2023 年 4 月 14 日)

新機能

- Microsoft Edge WebView サポート

Windows 向けCitrix Secure Accessクライアントでの Microsoft Edge WebView サポートにより、エンドユーザーエクスペリエンスが強化されました。この機能はデフォルトでは無効になっています。詳細については、「[Windows Citrix Secure Access の Microsoft Edge WebView サポート](#)」を参照してください。

• IP アドレスに FQDN を解決するための DNS サフィックスの追加

管理者は、オペレーティングシステムレベルでアプリケーションにサフィックスを追加できるようになりました。これにより、Citrix Secure Accessクライアントは、名前解決時に完全修飾されていないドメイン名を解決できます。

管理者は、エンドユーザーが対応するFQDNを使用してアプリケーションにアクセスできるように、IPアドレス（IP CIDR/IP範囲）を使用してアプリケーションを設定することもできます。詳細については、「[FQDN を IP アドレスに変換するための DNS サフィックス](#)」を参照してください。

• ログ収集の改善

Windows Secure Access クライアントのログ機能が改善され、ログの収集とデバッグが可能になりました。ロギング機能に次の変更が加えられました。

- ユーザーがログファイルの最大サイズを 600 MB 未満の値に変更できるようにします。
- ユーザーがログファイルの数を 5 個未満に更新できるようにします。
- 新しいロギング機能のログレベルを 3 に増やしてください。

これらの変更により、管理者とエンドユーザーは現在のセッションと過去のセッションからログを収集できます。以前は、ログの収集は現在のセッションのみに制限されていました。詳細については、「[Windows クライアントのログ収集の改善](#)」を参照してください。

注：

デバッグログを有効にするには、「**ログレベルの選択**」ドロップダウンリストから「**Logging**」>「**Verbose**」を選択します。Citrix Secure Accessクライアントの Windows 23.4.1.5リリースより前のリリースでは、**[構成]** > **[デバッグログを有効にする]** チェックボックスを使用してデバッグログを有効にできました。

• Citrix Analytics サービスへのイベント送信のサポート

Windows向けCitrix Secure Accessクライアントは、セッションの作成、セッションの終了、Citrix Analyticsサービスへのアプリケーション接続などのイベントの送信をサポートするようになりました。その後、これらのイベントはCitrix Secure Private Accessダッシュボードに記録されます。

解決された問題

- Citrix WorkspaceアプリによるクラウドエンドポイントへのCitrix Secure Accessクライアントのシングルサインオン認証は、Unicodeユーザーでは失敗します。
- Citrix Secure Private Accessでホスト名ベースのアプリケーションをDNSサフィックスと一緒に構成すると、リソースへのアクセスが失敗します。
- ゲートウェイの仮想サーバーへの到達性の問題により、Always-On VPN 接続が起動時に断続的に失敗します。
- Citrix Secure Accessクライアントで分割トンネルがオフに設定されていると、なりすましIPアドレス範囲と重複するイントラネットリソースにアクセスできません。
- Citrix Secure Accessクライアントが認証スキーマの読み込みに失敗し、Citrix Secure Private Accessサービスへのログインが失敗します。

23.1.11 (2023 年 2 月 20 日)

このリリースでは、Citrix Secure Private Accessサービスの全体的なパフォーマンスと安定性の向上に役立つ問題が修正されています。

23.1.1.8 (2023 年 2 月 8 日)

解決された問題

- DNS解決の失敗は、Citrix Secure AccessがIPv4パケットをIPv6パケットよりも優先しない場合に発生します。
- OSのフィルタリングルールは、Citrix Secure AccessクライアントがWindowsフィルタリングプラットフォーム（WFP）モードで実行されているときにキャプチャされます。

- Citrix Secure AccessクライアントがCitrix Demonic Network Enhancer (DNE) モードで実行されている場合、スプーフィングされたIPアドレスがIPベースのイントラネットアプリケーションに使用されます。
- Windows フィルタリングプラットフォーム (WFP) ドライバーを使用する場合、VPN を再接続した後にイントラネットアクセスが機能しないことがあります。
- Windows 10 および Windows 11 Enterprise のマルチセッションデスクトップで、OS バージョンチェック用のエンドポイント分析 (EPA) スキャンが失敗します。
- Windows クライアントは、デフォルトで 64 KB の構成ファイルサイズをサポートしているため、ユーザーは構成ファイルにさらにエントリを追加することが制限されます。このサイズは、HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Clientのレジストリ値 `ConfigSize` を設定することで増やすことができます。 `ConfigSize` レジストリキータイプは `REG_DWORD` で、キーデータは `<Bytes size>` です。構成ファイルのサイズがデフォルト値 (64 KB) より大きい場合は、64 KB を追加するたびに `ConfigSize` レジストリ値を (バイトに変換後) $5 \times 64 \text{ KB}$ に設定する必要があります。たとえば、64 KB を追加する場合は、レジストリ値を $64 \times 1024 \times 5 = 327680$ に設定する必要があります。同様に、128 KB を追加する場合は、レジストリ値を $64 \times 1024 \times (5+5) = 655360$ に設定する必要があります。
- VPN ログオフ時に、SearchList レジストリの DNS サフィックスリストのエントリは、1 つ以上のカンマで区切られた逆の順序で書き換えられます。
- NetScaler ADCアプライアンスがウイルス対策のEPAスキャンを完了すると、プロキシ認証は失敗します。
- Citrix Secure Access関連のレジストリ値が1500文字を超える場合、ログコレクターはエラーログを収集できません。

22.10.1.9 (2022年11月8日)

新機能

- **GSLB での接続プロキシタイプのサイトパーシステンスに対する EPA サポート**

Windows EPA スキャンは、スキャンをブラウザーから開始するときの GSLB での接続プロキシタイプのサイトパーシステンスをサポートするようになりました。以前は、Windows 用

EPA スキャンは、ブラウザが開始する EPA スキャンの接続プロキシパーシステンスタイプをサポートしていませんでした。

- **ワークスペース URL のシームレスなシングルサインオン (クラウドのみ)**

Citrix Secure Accessクライアントは、ユーザーがCitrix Workspaceアプリですでにログオンしている場合、ワークスペースURLのシングルサインオン（クラウドのみ）をサポートするようになりました。詳しくは、「[Citrix Workspaceアプリを使用してログインしたユーザーのワークスペースURLのシングルサインオンサポート](#)」を参照してください。

- **Citrix Workspace アプリ（クラウドのみ）を使用してCitrix Secure Accessクライアントおよび/またはEPAプラグインバージョンを管理**

Citrix Workspaceアプリでは、Global App Configuration Serviceを介して最新バージョンのCitrix Secure AccessまたはEPAプラグインをダウンロードしてインストールできるようになりました。詳細については、「[Global App Configuration Service](#)」を参照してください。

- **デバッグロギング制御の強化**

Citrix Secure Accessクライアントのデバッグログ制御は、NetScaler Gateway に依存せず、マシントネルとユーザートンネルの両方のプラグインUIから有効または無効にできるようになりました。

- **プライベートネットワークアクセスのプリフライトリクエストのサポート**

Citrix Secure Access Client for Windowsは、公開WebサイトからプライベートネットワークリソースにアクセスするときにChromeブラウザによって発行されるプライベートネットワークアクセスのプリフライトリクエストをサポートするようになりました。

解決された問題

- Citrix Secure Accessクライアントのバージョン21.7.1.1以降では、管理者権限のないユーザーが新しいバージョンにアップグレードできません。

これは、Citrix Secure AccessクライアントのアップグレードがNetScaler ADCアプライアンスから行われた場合にのみ適用されます。詳しくは、「[Citrix Secure Access クライアントのアップグレード/ダウングレードの問題](#)」を参照してください。

- EPA の障害が断続的に発生するため、ユーザーは VPN にログオンできません。

- マシントネルのみモードのCitrix Secure Accessクライアントは、マシンがスリープモードから復帰した後に、自動的にマシントネルを確立しないことがあります。
- Always on service モードでは、マシントネルのみが構成されていても、ユーザートンネルは起動を試みます。
- Microsoft Edgeがデフォルトのブラウザの場合、Citrix Secure Access UIのホームページリンクは機能しません。
- カスタマイズされたEPA障害ログメッセージはNetScaler Gateway ポータルには表示されず、代わりに「内部エラー」というメッセージが表示されます。
- ユーザーがWindows向けCitrix Secure Access画面の [ホームページ] タブをクリックすると、ページに接続拒否エラーが表示されます。
- 一部のクライアントマシンでは、Citrix Secure Accessクライアントがプロキシ設定を検出できず、ログオンが失敗します。

既知の問題

- Windows Update チェックベースの EPA スキャンは、Windows 11 22H2 バージョンでは機能しません。詳細については、「[Windows11 22H2 の EPA チェックが失敗する](#)」を参照してください。

22.6.1.5 (2022年6月17日)

新機能

- ログインとログアウトのスクリプト設定

Citrix Secure Accessクライアントは、Citrix Secure AccessクライアントがCitrix Secure Private Accessクラウドサービスに接続するときに、次のレジストリからログインおよびログアウトスクリプト構成にアクセスします。

レジストリパス: **HKEY_LOCAL_MACHINE>ソフトウェア>Citrix>Secure Access Client**

レジストリ値:

- SecureAccessLoginScript タイプ REG_SZ-ログインスクリプトへのパス
- SecureAccessLogoutScript タイプ REG_SZ-ログアウトスクリプトへのパス

- **Windows フィルタリングプラットフォーム (WFP) を使用する Windows Citrix Secure Accessクライアント**

WFPは、ネットワークフィルタリングアプリケーションを作成するためのプラットフォームを提供する一連のAPIおよびシステムサービスです。WFP は、DNE ドライバーで使用されていたネットワークドライバインターフェイス仕様 (NDIS) フィルターという、以前のパケットフィルター技術を置き換えるように設計されています。詳しくは、「[Windows フィルタリングプラットフォームを使用する Windows Citrix Secure Accessクライアント](#)」を参照してください。

- **FQDN ベースの逆分割トンネルのサポート**

WFP ドライバーが FQDN ベースの REVERSE 分割トンネリングのサポートを有効にするようになりました。DNE ドライバーではサポートされていません。リバース分割トンネルの詳細については、[分割トンネリングオプションを参照してください](#)。

解決された問題

- ユーザーが Always On サービスモードで Windows マシンにログインすると、Windows 自動ログオンが機能しない場合があります。マシントンネルはユーザートンネルに移行せず、VPN ブラグインの UI に「**接続中**」というメッセージが表示されます。
- VPN ログオフ時に、SearchList (コンピューター\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client) レジストリ内の DNS サフィックスリストのエントリは、1 つ以上のカンマで区切られた逆の順序で書き換え
- なりすましIPアドレスは、NetScaler ADCイントラネットアプリケーションの構成がFQDN ベースからIPベースのアプリケーションに変更された後も使用されます。
- ゲートウェイのホームページは、ゲートウェイブラグインが VPN トンネルを正常に確立した直後には表示されません。

今回の修正により、次のレジストリ値が導入されました。

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

種類：DWORD

デフォルトでは、このレジストリ値は設定も追加もされません。

「SecureChannelResetTimeoutSeconds」の値が0または追加されていない場合、遅延を処理するための修正が機能しません。これはデフォルトの動作です。管理者は、このレジストリを

クライアントに設定して修正を有効にする必要があります (つまり、ゲートウェイプラグインが VPN トンネルを正常に確立した直後にホームページを表示する)。

- レジストリ値が 2000 バイトを超えると、AlwaysOnAllow リストレジストリが期待どおりに動作しません。
- Windows向けCitrix Secure Accessクライアントは、すでに接続されているCitrix Secure Private Accessサービスリージョンにアクセスできなくなった場合でも、新しいTCP接続をバックエンドTCPサーバーにトンネリングしません。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

22.3.1.5 (2022年3月24日)

解決された問題

- Windows EPAプラグイン名は、NetScaler Gateway EPAプラグインに戻されます。

既知の問題

- Windows向けCitrix Secure Accessクライアントは、すでに接続されているCitrix Secure Private Accessサービスリージョンにアクセスできなくなった場合でも、新しいTCP接続をバックエンドTCPサーバーにトンネリングしません。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

22.3.1.4 (2022年3月10日)

新機能

- **ADC 構成に基づいてエンドユーザーにローカル LAN アクセスを強制する**

管理者は、エンドユーザーがクライアントマシンのローカル LAN アクセスオプションを無効にすることを制限できます。既存のローカル LAN アクセスパラメータ値に、FORCED という新しいオプションが追加されました。ローカル LAN アクセス値が FORCED に設定されている場合、クライアントマシンのエンドユーザーはローカル LAN アクセスが常に有効になります。エンドユーザーは、Citrix Secure AccessクライアントUIを使用してローカルLAN設定を無効にすることはできません。管理者がエンドユーザーにローカルLANアクセスを有効または無

効にするオプションを提供したい場合は、ローカルLANアクセスパラメーターをONに再構成する必要があります。

GUI を使用して **FORCED** オプションを有効にするには、次の手順を実行します：

- a. [**NetScaler Gateway**] > [**グローバル設定**] > [**グローバル設定の変更**] に移動します。
- b. タブをクリックし、 をクリックします。
- c. で を選択します

CLI を使用して **FORCED** オプションを有効にするには、次のコマンドを実行します。

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

• EPA OS スキャンでの Windows サーバー 2019 および 2022 のサポート

EPA OS スキャンで、Windows サーバー 2019 および 2022 がサポートされるようになりました。

GUI を使用して新しいサーバを選択できます。

- a. **NetScaler Gateway** > **ポリシー** > **事前認証**に移動します。
- b. 新しい事前認証ポリシーを作成するか、既存のポリシーを編集します。
- c. ** リンクをクリックします。
- d. **式エディタ**で、 > を選択し、 アイコンをクリックします。
- e. で、要件に従ってサーバを選択します。

EPA OS スキャンで Windows サーバー 2019 および 2022 を使用するには、OPSWAT バージョン 4.3.2744.0 にアップグレードできます。

• 不足しているセキュリティパッチに対する新しい EPA スキャン分類タイプ

不足しているセキュリティパッチの EPA スキャンに、次の新しい分類タイプが追加されました。クライアントに次の不足しているセキュリティパッチのいずれかがある場合、EPA スキャンは失敗します。

- アプリケーション
- コネクタ
- クリティカルなアップデート
- 定義更新

- developerKits
- FeaturePack
- ガイダンス
- セキュリティアップデート
- ServicePack
- ツール
- UpdateRollUps
- アップデート

GUI を使用して分類タイプを設定できます。

- NetScaler Gateway > ポリシー > 事前認証に移動します。**
- 新しい事前認証ポリシーを作成するか、既存のポリシーを編集します。
- ((OPSWAT EPA エディタ)) リンクをクリックします。
- 式エディタで > を選択します。
- で、未適用のセキュリティパッチの分類タイプを選択します。
- [OK]** をクリックします。

OPSWAT バージョン 4.3.2744.0 にアップグレードして、これらのオプションを使用できます。

- Windows サーバ更新サービス分類 GUID の詳細については、[<https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803\(v=vs.85\)>](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)>) を参照してください。
- Microsoft のソフトウェア更新プログラムの用語については、「[<https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates>](https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates>)」を参照してください。

以前は、欠落しているセキュリティパッチの EPA スキャンは、Windows クライアントの重大度 (重大、重要、中、低) で行われていました。

• EPA スキャン用の複数デバイス証明書のサポート

Always on VPN 設定では、複数のデバイス証明書が設定されている場合、有効期限が最も長い証明書が VPN 接続で試行されます。この証明書で EPA スキャンが正常に許可されると、VPN

接続が確立されます。この証明書がスキャンプロセスで失敗すると、次の証明書が使用されません。このプロセスは、すべての証明書が試行されるまで続きます。

以前は、複数の有効な証明書が構成されていて、1つの証明書のEPAスキャンが失敗すると、他の証明書に対してスキャンは試行されませんでした。

解決された問題

- VPN 仮想サーバーを構成するときに SSL プロファイルで ClientCert パラメーターが「オプション」に設定されている場合、スマートカードを選択するように求めるメッセージが複数回表示されます。
- [NetworkAccessonVPNFailure] プロファイルパラメーターを [フルアクセス] から [OnlyToGateway] に変更すると、ユーザーはNetScaler Gateway アプライアンスに接続できなくなります。
- Always on が設定されている場合、aoservice.exe ファイルのバージョン番号 (1.1.1.1) が正しくないため、ユーザトンネルが失敗します。
- 内部リソースと外部リソースに対する DNS 解決は、長期間の VPN セッションでは機能しくなります。
- Windows VPN クライアントは、サーバからの「SSL close notify」アラートを尊重せず、同じ接続で転送ログイン要求を送信します。
- レジストリ EPA は「==」と「!=」演算子は一部のレジストリエントリで失敗します。

22.1.103 (2022年2月17日)

解決された問題

- Chrome 98 または Edge 98 ブラウザバージョンにアップグレードすると、ユーザーはEPAプラグインまたはVPNプラグインを起動できません。この問題を解決するには、次の手順に従います。
 - a. VPN プラグインをアップグレードする場合、エンドユーザーは最初にVPNクライアントを使用して接続し、各自のマシンで修正プログラムを取得する必要があります。それ以降のログイン試行では、接続するブラウザまたはプラグインを選択できます。

- b. EPA のみのユースケースでは、エンドユーザにはゲートウェイに接続するための VPN クライアントがありません。この場合は、次の操作を行います。
 - a. ブラウザを使用してゲートウェイに接続します。
 - b. ダウンロードページが表示されるのを待ち、nsepa_setup.exe をダウンロードします。
 - c. ダウンロード後、ブラウザを閉じて nsepa_setup.exe ファイルをインストールします。
 - d. クライアントを再起動します。

21.12.1.4 (17-Dec-2021)

新機能

- **リブランディングの変更**

Windows 用NetScaler Gatewayプラグインは、Citrix Secure Accessクライアントにリブランドされました。

- **TCP/HTTP (S) プライベートアプリケーションのサポート**

Citrix Secure Accessクライアントは、Citrix Workspace Secure Accessサービスを通じてリモートユーザー向けのTCP/HTTP (S) プライベートアプリケーションをサポートするようになりました。

- **追加言語のサポート**

NetScaler Gateway 用のWindows VPNおよびEPAプラグインで、次の言語がサポートされるようになりました。

- 韓国語
- ロシア語
- 繁体字中国語

- **Windows 11でのCitrix Secure Accessのサポート**

Citrix Secure AccessクライアントがWindows 11でサポートされるようになりました。

- **ユーザーが同じマシンからログインしていて、Always on が構成されている場合の自動転送ログオン**

Always on が構成され、ユーザーが同じマシンからログインしている場合に、ユーザーの介入なしに自動ログイン転送が行われるようになりました。以前は、システムの再起動やネットワーク接続の問題などのシナリオでクライアント (ユーザ) が再ログインすると、ポップアップメッセージが表示されていました。ユーザーは移管ログインを確認する必要がありました。この機能強化により、ポップアップウィンドウは無効になりました。

- **NetScaler ADCが提供するネットマスクからCitrix仮想アダプタのデフォルトゲートウェイIPアドレスを導出する**

Citrix仮想アダプタのデフォルトゲートウェイIPアドレスは、NetScaler ADCが提供するネットマスクから導出されるようになりました。

解決された問題

- 分割トンネル ON モードで VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。Citrix Virtualアダプタのデフォルトルートに誤りがあると、このネットワークの問題が発生します。
- 分割トンネルが「リバース」に設定されている場合、イントラネットドメインの DNS 解決は失敗します。

21.9.100.1 (2021年12月30日)

新機能

- **Windows 11でのCitrix Secure Accessのサポート**

Citrix Secure AccessクライアントがWindows 11でサポートされるようになりました。

解決された問題

- 分割トンネル ON モードで VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。Citrix Virtualアダプタのデフォルトルートに誤りがあると、このネットワークの問題が発生します。
- 分割トンネルが「リバース」に設定されている場合、イントラネットドメインの DNS 解決は失敗します。

21.9.1.2 (04-Oct-2021)

解決された問題

- VPN の切断後、DNS リゾルバがホスト名の解決に失敗することがあります。これは、VPN の切断中に DNS サフィックスが削除されるためです。
- クライアントのアイドルタイムアウトが設定されていると、ユーザーが数秒以内にNetScaler Gateway からログアウトすることがあります。
- Windows プラグインは、認証中にクラッシュすることがあります。
- Always On サービスモードでは、Windows 用 VPN プラグインは、ユーザーが Windows マシンにログオンした後、ユーザートンネルを自動的に確立できません。
- トンネルの確立後、以前のゲートウェイ IP アドレスで DNS サーブルートを追加する代わりに、Windows プラグインはデフォルトゲートウェイアドレスを持つルートを追加します。

V21.7.1.1 (27-Aug-2021)

新機能

- **新しい MAC アドレススキャン**

新しい MAC アドレススキャンのサポートが追加されました。

- **EPA スキャンで Windows OS とそのビルドバージョンを確認する**

Windows OS とそのビルドバージョンを確認するための EPA スキャンを追加しました。

- **EPA スキャンで特定の値の存在をチェックする**

レジストリ EPA スキャンの新しいメソッドは、特定の値の存在をチェックするようになりました。

解決された問題

- ネットワークエラーが原因でログイン中に JavaScript エラーが発生した場合、後続のログイン試行は同じ JavaScript エラーで失敗します。

- McAfee アンチウイルスの最終更新時刻のチェックで EPA スキャンが失敗する。
- VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。
- VPN プラグインのスクリプトエラーが nFactor 認証中に表示されることがあります。
- ネットワークの中断が発生した場合、ネットワークが中断する前に開始された UDP トラフィックフローは、最大 5 分間はドロップされません。
- DNS 登録に予想よりも長い時間がかかる場合、VPN トンネルの開始に遅延が生じることがあります。

V21.3.1.2 (31-Mar-2021)

新機能

- アップグレードされた EPA ライブラリ

EPA ライブラリは、EPA スキャンで使用するソフトウェアアプリケーションの最新バージョンをサポートするようにアップグレードされます。

- **NetScaler Gateway 仮想アダプタの互換性**

NetScaler Gateway 仮想アダプターは、Hyper-VおよびMicrosoft Wi-Fi Direct仮想アダプター（プリンターで使用）と互換性があります。

解決された問題

- Windows VPN ゲートウェイプラグインは、VPN トンネルでの「CTRL + P」と「CTRL + O」の使用をブロックします。
- Windows向けNetScaler Gateway プラグインは、マシン名の `"nslookup"` アクションが要求されたときに、Active Directory に登録されたイントラネットIPアドレスでのみ応答します。
- スプリット DNS が「ローカル」または「両方」に設定されている場合、IIP の登録および登録解除は断続的に失敗します。
- Always On が構成されている場合、Windows VPN ゲートウェイプラグインへの自動ログオンが失敗します。

- Windows VPN ゲートウェイプラグインが IPv6 DNS パケットのドロップに失敗し、DNS 解決に問題が生じます。
- Windows VPN ゲートウェイプラグインは、Internet Explorer のプロキシ除外リストのブラウザー制限のためにプロキシ除外リストがオーバーフローした場合でも、既存のプロキシ除外リストを維持します。
- Windows VPN ゲートウェイプラグインは、VPN クライアントが Always On モードでログオフすると、プロキシ設定を復元できません。
- Windows 用 VPN プラグインは、次の条件が満たされている場合、Windows へのログオン後にトンネルを確立しません。
 - NetScaler Gateway アプライアンスは、常時オン機能用に構成されています。
 - アプライアンスは、2 要素認証が「off」の証明書ベースの認証用に設定されています。

Technical Previewの機能

プレビュー版の機能は、非運用環境または限定的な実稼働環境で使用でき、お客様にフィードバックを共有する機会を提供します。プレビュー中の機能のサポートケースは受け付けていませんが、改善のためのフィードバックをお待ちしています。私たちは、その重要性、重要性、重要性に基づいて、フィードバックに基づいて行動することがあります。

次の機能は現在プレビュー中です：

- [Windows Citrix Secure Access のMicrosoft Edge WebView サポート](#)

Windows クライアントのログ収集が改善されました

Windows Secure Access クライアントのロギング機能が強化され、ログの収集とデバッグが強化されました。新しいログファイルの先頭には「csa_」が付きます。

Windows 23.10.1.7向けCitrix Secure Accessクライアント以降、ログ収集とトラブルシューティングを強化するため、デフォルトのログレベルはVerboseに設定されています。

これらの変更により、管理者とエンドユーザーは現在のセッションと過去のセッションからログを収集できます。以前は、ログの収集は現在のセッションのみに制限されていました。

Citrix Secure Accessクライアントユーザーインターフェイスを使用してログを構成する

1. Windows 用 Secure Access クライアントをインストールします。
2. メニューから をクリックします。ログに関するすべての設定は、ロギング画面で行うことができます。



• ログレベルの選択:

新しいロギングメカニズムを有効にすると、次の 3 つのログレベルを使用できます。

- エラー:アプリケーションによって報告された例外または障害のみがログに記録されます。
- 情報:このレベルには、プログラムの実行に関連する情報メッセージとイベントが含まれます。エラーや例外も含まれます。
- Verbose (デフォルト): このレベルには、Error および Info ログレベルで報告されたすべてのログメッセージと、トラブルシューティングに役立つ可能性のあるその他のメッセージが含まれます。

- **ログファイルのサイズ制限:** (必須) 各ログファイルのログファイルサイズを入力します。最大値は 600 MB です。
- **ログファイルの最大数:** (必須) ログ収集用に追加するファイルの数を入力します。最大値は 5 です。
- **メールログファイル** — 登録した電子メール ID にログファイルを電子メールで送信します。
- **新しいログファイルを開始** — このオプションを選択すると、新しいログファイルが作成されます。
- **ログファイルの収集** — クリックすると、アプリケーションのすべてのログファイルを含む zip ファイルが作成されます。この zip ファイルはクライアントのデスクトップに保存されます。
- **ログファイルを開く** — このオプションを選択すると、最新の `csa_nssslvpn*.txt` ファイルが開きます。

Windows向けCitrix Workspaceアプリを介したCitrix Secure Access への自動シングルサインオン

Citrix Workspaceアプリは、Citrix Secure Access 向けの統一されたクライアント管理エクスペリエンスを提供します。ユーザーがCitrix Workspaceアプリにログオンすると、Citrix Secure Access に自動的にサインオンし、複数のクライアントアプリケーションを手動で構成してサインインしなくても、TCP/UDPアプリケーションにシームレスにアクセスできます。

機能

Citrix Workspaceアプリは、Citrix Secure Accessクライアントのインストール、自動アップデート、およびシングルサインオン（SSO）を実行します。エンドユーザーは、手動で操作しなくても自動的にCitrix Secure Accessにログオンし、SSOが成功すると通知されます。

この機能により、エンドユーザーは1つのアプリケーションにログオンするだけで済むため、時間を節約でき、統一されたユーザーエクスペリエンスが提供されます。また、エンドユーザーとCitrix Secure Accessとの間にはやり取りはありません。

前提条件

エンドユーザーは、[Windows 2405以降のバージョン向けのCitrix Workspaceアプリを使用する必要があります](#)。

構成

Citrix WorkspaceアプリがCitrix Secure Accessへのインストール、自動更新、およびシングルサインオンを実行できるようにするには、管理者がCitrix CloudでGlobal App Configuration Service（GACS）設定を構成する必要があります。

Citrix WorkspaceアプリによるCitrix Secure Access のインストールと自動アップデートを有効にする

1. Citrix Cloudにログオンします。
2. ハンバーガーメニューをクリックし、> に移動します。
3. 「**アップデートとプラグイン**」セクションを選択し、「**Secure Access プラグイン**」に移動します。
4. **Windows** チェックボックスを有効にします。この手順により、Citrix Secure Access for Windowsがインストールされ、自動的に最新バージョンに更新されます。
5. をクリックして Windows プラグインの設定を行います。
6. ** ページで、オプションを有効にします。
7. をクリックします。
8. 表示される確認ウィンドウで、 をクリックします。



Citrix Workspaceアプリ経由でCitrix Secure Access へのSSOを有効にする

1. Citrix Cloudにログオンします。

- ハンバーガーメニューをクリックし、> に移動します。
- > に移動します。
- 「**セキュアアクセス自動ログイン**」セクションで、「**Windows**」チェックボックスを有効にします。



GACSについて詳しくは、「[Global App Configuration Serviceを使用してCitrix Workspaceアプリを構成する](#)」を参照してください。

または、ユーザー認証ポリシーを設定すれば、SSO を有効にできます。Citrix Secure Access 24.6.1.18以降とCitrix Workspaceアプリ2405以降を使用していることを確認してください。

ユーザー認証ポリシーを有効にするには：

- ローカルグループポリシーエディターで、[管理用テンプレート] > [Citrix Workspace] > [ユーザー認証] に移動します。
- Citrix Secure Accessクライアントポリシーへのシングルサインオンを有効にします。

制限事項

- Citrix WorkspaceアプリからCitrix Secure AccessへのSSOログインは、単一のプライマリドメインでのみサポートされます。複数ドメインでのSSOはサポートされていません。
- Citrix Workspaceアプリは、Citrix Secure Accessクライアントイベント（ログインの成功または失敗）を記録しません。

Windows Citrix Secure Accessの Microsoft Edge WebView サポート-プレビュー

Internet Explorer WebView は廃止されたため、Microsoft Edge WebView はマイクロソフトが推奨している WebView になりました。Microsoft Edge WebViewの機能を利用するには、Citrix Secure Accessクライアント23.8.1.5以降のバージョンを使用することをお勧めします。

現在、Microsoft Edge ウェブビューはデフォルトで無効になっています。 <https://podio.com/webforms/28291989/2245437> を使用してプレビューにサインアップできます。

エンドユーザーへの変更

Citrix Secure Accessクライアントユーザーインターフェイスの認証画面は次のように表示されます。



エンドユーザーがURLを選択すると、Citrix Secure Accessクライアントは新しいウィンドウを開き、資格情報を使用してNetScaler Gatewayにログオンするように求めます。



Windows クライアントマシンに Microsoft Edge WebView ランタイムがインストールされていない場合、エンドユーザーには、Microsoft Edge WebView ランタイムをダウンロードしてインストールするためのリンクが Citrix Secure Access クライアント UI に表示されます。エンドユーザーは VPN に接続すると、Edge WebView ランタイムをシームレスにダウンロードしてインストールでき、このプロセス中に認証が中断されることはありません。



メモ：

- Microsoft Edge WebView 機能は、管理者固有の構成には影響しません。
- Citrix Secure AccessでEdge WebView を使用する場合は、[HttpOnly Cookie](#) 機能を有効にすることをお勧めします。これにより、EPAをnfactorフローの要素として使用する場合のNetScaler Gatewayのログオン時間が短縮されます。

トラブルシューティング

- この機能で問題が発生した場合は、[Citrix サポート](#)にお問い合わせください。
- < citrixgatewaybetafeedback@cloud.com >Edge WebView 機能に関するフィードバックは、を通じて送信できます。

Linux向けCitrix Secure Accessクライアント

Linux向けCitrix Secure Accessクライアントは、NetScaler Gatewayが管理するVPNクライアントソフトウェアで、ユーザーは企業のデータやアプリケーションにリモートでアクセスできます。Citrix Secure Accessクライアントは、不正アクセス、アプリケーションレベルの脅威、およびブラウザベースの攻撃からアプリケーションを保護します。

Citrix End Point Analysis (EPA) クライアントは、NetScaler Gatewayによって管理されるクライアントソフトウェアです。NetScaler Gateway経由での企業データへのアクセスを許可する前に、エンドポイント基準をチェックします。Citrix EPAクライアントとCitrix Secure Accessクライアントは相互に独立しています。

注：

EPA を使用しない場合でも、後で EPA 機能を使用する場合に備えて、EPA と VPN の両方のプラグインバイナリを同時に更新することをお勧めします。

サポートされている Linux バージョン

Citrix Secure AccessクライアントとCitrix EPAクライアントは、Ubuntu 18.04、Ubuntu 20.04、およびUbuntu 22.04バージョンと互換性があります。サポートされているブラウザの詳細については、「[クライアントソフトウェア要件](#)」を参照してください。

注：

Ubuntu 22.04をCitrix Secure AccessクライアントおよびCitrix EPAクライアントと連携させるには、NetScaler CLIでSSLパラメータ `denySSLReneg` を `NONSECURE` に設定します。

サポートされる機能

Ubuntu向けCitrix Secure Access クライアントは、以下の機能をサポートしています。

- 分割トンネリングとリバース分割トンネリング
- TCP、UDP、および ICMP アプリケーションのトンネリング

- イントラネット IP (IIP) 経由のサーバー起動接続
- スプリット DNS リモート
- クライアント側のプロキシ
- 従来の EPA スキャン
- 高度な EPA スキャンを含む高度な認証 (nFactor) (ブラウザからのみ)
- HTTP のみのクッキー
- 広域サーバー負荷分散 (Global Server Load Balancing : GSLB)

注：

スプリット DNS BOTH は Ubuntu 用 Citrix Secure Access クライアントではサポートされていません。

NetScaler GatewayでのUbuntuクライアントのアップグレード

Ubuntu用のCitrix Secure AccessクライアントとCitrix EPAクライアントは、ダウンロードページからダウンロードできます。

Citrix Secure Access クライアントと Citrix EPA クライアントには、それぞれ「nsgclient18_64.deb」と「nsepa18.deb」という名前が付けられています。クライアントはUbuntu 18.04と20.04の両方に対応しています。

Ubuntu 22.04をサポートするCitrix Secure AccessクライアントとCitrix EPAクライアントには、それぞれ「nsginstaller64.deb」と「nsepa.deb」という名前が付けられています。

Citrix Secure Accessクライアントの最新バージョンをバージョン1.0.0.xからバージョン23.6.1にアップグレードする場合は、たとえば次のようにします。

1. シェルプロンプトを使用して、場所 `/var/netScaler/gui/vpn/scripts/linux/` にある「nsgclient18_64.deb」と「nsginstaller64.deb」ファイルを置き換えます。
2. シェルプロンプトを使用して、場所 `/var/netScaler/gui/epa/scripts/linux/` にある「nsepa18.deb」と「nsepa.deb」ファイルを置き換えます。
3. `/var/netScaler/gui/vpn/scripts/linux/clientversions.xml` ファイルを開きます。

- a. Citrix EPA クライアントの場合は、次の XML タグの現在のバージョン (1.0.0.x) を最新バージョン (23.6.1) に置き換えます。XML タグが存在しない場合は、それらを XML ファイルに追加します。例：

変更前

```
<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" />
```

変更後

```
<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" />
```

変更前

```
<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" />
```

変更後

```
<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. Citrix Secure Access クライアントの場合は、次の XML タグ内の現在のバージョン (1.0.0.x) を最新バージョン (23.6.1) に置き換えてください。XML タグが存在しない場合は、それらを XML ファイルに追加します。例：

変更前

```
<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" />
```

変更後

```
<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" />
```

および

```
<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" />
```

変更後

```
<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. NetScaler シェルプロンプトで、次のコマンドを実行します。

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

5. NetScaler CLIで、以下のコマンドを実行します。

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

参照ドキュメント

- [NetScaler Gateway VPNクライアントとサポートされる機能](#)
- [Ubuntu でサポートされるエンドポイント分析スキャン](#)
- [エンドユーザー向けヘルプドキュメント](#)

Linux向けCitrix Secure Accessリリースノート

Linux向けCitrix Secure AccessクライアントとCitrix End Point Analysis (EPA) クライアントは現在、スタンドアロンベースでリリースされており、すべてのNetScalerバージョンと互換性があります。Citrix Secure Accessクライアントバージョンは、YY.MM リリース.ビルドの形式に従います。

リリースノートには、新機能、既存機能の強化、解決された問題、既知の問題が記載されています。

新機能:現在のリリースで利用可能な新機能と機能強化。

修正された問題:現在のリリースで修正された問題。

既知の問題:現在のリリースに存在する問題とその回避策 (該当する場合)。

サポートされる機能について詳しくは、[NetScaler Gateway 製品ドキュメント](#)を参照してください。

23.10.3 (2023年10月16日)

解決された問題

フランスのユーザーの場合、Citrix Secure Access for Linuxユーザーインターフェイスの [接続] ページには、データ転送速度がそれぞれKB単位とMo単位ではなく、KB単位とMB単位で表示されます。

23.9.1 (2023年9月8日)

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

23.6.2 (2023年6月20日)

新機能

- **Ubuntu 22.04 のCitrix Secure Access クライアントとCitrix EPA クライアントのサポート**

Ubuntu 22.04は、Ubuntuの最新の長期サポートリリースです。Citrix Secure Access とCitrix EPAクライアントはUbuntu 22.04と互換性があります。詳しくは、「[クライアントソフトウェア要件](#)」を参照してください。

- **Citrix Secure Access およびCitrix EPAクライアントのGSLBサポート**

Ubuntu向けCitrix Secure AccessクライアントとCitrix EPAクライアントは、NetScaler Gatewayのグローバルサーバー負荷分散（GSLB）機能をサポートしています。NetScaler GatewayのGSLBを構成することで、管理者はエンドユーザーがどこからでもエンタープライズネットワーク（イントラネットリソース）を常にご利用できるようにすることができます。GSLBは、あるデータセンターのユーザーが別のデータセンターにリダイレクトされるような災害状況やネットワーク障害にも対処します。詳しくは、「[NetScaler Gatewayでのアクティブ-アクティブGSLB展開のサポート](#)」を参照してください。

- **Citrix Secure Access およびCitrix EPA クライアントの HTTP のみのサポート**

Citrix Secure Access クライアントと Citrix EPA クライアントは、認証クッキーの HttpOnly フラグをサポートしています。NetScaler Gatewayの管理者は、Webアプリケーションによって生成される認証クッキーにHTTPOnly機能を構成します。この機能は、クロスサイトスクリプティングによる Cookie の盗難を防ぐのに役立ちます。詳細については、「[認証クッキーに HttpOnly フラグを適用する](#)」を参照してください。