iOS 用 Citrix Workspace™ アプリ

iOS 用 Citrix Workspace アプリは、Apple Store からダウンロードできるクライアントソフトウェアです。Citrix Virtual Apps and Desktops によって提供される仮想デスクトップやホスト型アプリケーションにアクセスして実行できます。

iOS は、iPad や iPhone などの Apple モバイルデバイス用のオペレーティングシステムです。iOS 用 Citrix Workspace アプリは、iPhone X、iPad mini、iPad Pro など、iOS オペレーティングシステムを使用するデバイスで動作します。

機能、修正された問題、既知の問題に関する詳細については、このリリースについてのページを参照してください。

非推奨の項目については、非推奨のページを参照してください。

言語サポート

iOS 用 Citrix Workspace アプリは、英語以外の言語での使用に対応しています。iOS 用 Citrix Workspace アプリがサポートする言語のリストについては、言語サポート を参照してください。

参照記事

- 技術概要: Citrix Workspace
- グローバルアプリ構成サービス
- Workspace ユーザーインターフェイス (UI)
- Citrix Virtual Apps and Desktops 環境での Microsoft Teams の最適化
- Citrix Workspace アプリのリリーススケジュール

関連製品の新機能

- Citrix Workspace (シトリックス ワークスペース)
- シトリックス DaaS
- StoreFront
- セキュアプライベートアクセス

- Mac 用 Citrix Workspace アプリ

レガシー ドキュメント

ライフサイクル終了 (EOL) に達した製品リリースについては、レガシー ドキュメント を参照してください。

このリリースについて

新機能、機能強化、修正された問題、既知の問題について説明します。

注:

- このバージョンに関する貴重なフィードバックをお待ちしております。フィードバックは、**設定** > **問題の報告** に移動して提供できます。詳細ログとスクリーンショットの両方をここから共有できます。
- テクニカルプレビューをお探しですか？それらを1か所で見つけられるようにリストをまとめました。テクニカルプレビューの機能ページをご覧ください。

26.9.0 の新機能

OS 27 のサポート

iOS 版 Citrix Workspace アプリは、iOS/iPadOS 27 をサポートするようになりました。

マルチウィンドウレイアウトでの画面キャプチャ防止機能の強化

アプリ保護が有効なセッションでの画面キャプチャ防止機能が、フローティングウィンドウモードにも拡張されました。保護は、保護されたセッションが表示される場所（全画面表示、Split View、Slide Over、フローティングウィンドウ、Stage Manager）で適用され、Citrix Workspace アプリから切り替えた場合でも、バックグラウンドおよびアプリスイッチャーのスナップショットで保持されます。

26.9.0 で修正された問題

- iPad で Citrix Workspace アプリバージョン 25.9.0.36 にアップグレードした後、Novatek アプリケーションでバーコードスキャンが断続的に不正確または不完全なデータを返す。
- Citrix Workspace アプリがバックグラウンド/全画面表示で、Safari 経由で起動された場合、公開されたアプリが表示されない。

- Web Interface モードでストアが追加された場合、iOS 版 Citrix Workspace アプリ 2511 でアプリ保護されたリソースが起動しないことがある。

26.7.0 の新機能

EDT Lossy 経由でのオーディオパフォーマンス（再生）の向上

バージョン 2607 以降、iOS 版 Citrix Workspace アプリは、リアルタイムオーディオストリーミングに最適化された UDP ベースのトランスポートである EDT Lossy を活用することで、セッション内オーディオ再生を改善します。

標準のEDTおよびTransmission Control Protocol (TCP)と比較して、EDTロッシーモードは、高遅延、可変帯域幅、またはパケット損失のあるモバイルネットワークでよりスムーズなオーディオを提供します。このアップデートにより、オーディオの途切れやドロップアウトが減少し、仮想セッション、メディア再生、オンライン会議中に、より一貫性のある高品質なリスニング体験が提供されます。

マウス、トラックパッド、タッチのスクロールサポート

この機能は、以下の入力方法で水平および斜めスクロールをサポートします。

- **マウスホイールスクロール:** 物理マウスホイールを使用して、垂直および水平にスクロールします。
- **トラックパッド2本指パン（Appleおよびサードパーティ製）:** 2本指パンジェスチャを使用して、垂直および水平にスクロールします。
- **画面タッチ（1本指スクロール）:** iPhoneまたはiPadの画面で1本の指を使用して、垂直および水平にスクロールします。

VDA OS検出とキーボードショートカットのサポート

バージョン2607以降、iOS版Citrix Workspace™アプリは、接続されているVDAのオペレーティングシステムを検出し、適切なキーボードショートカットを送信するようになりました。

- **VDAオペレーティングシステム検出:** 接続されているVDAがWindows、Linux、macOSのいずれを実行しているかを検出します。
- **macOS VDAの自動入力モード:** macOS VDAに接続すると、アプリは入力モードを**スキャンコード**に切り替えます。アプリは診断データも送信し、この設定のテレメトリデータポイントを記録します。
- **拡張キーボードツールバーショートカット:** 一般的なショートカットをChromeOS版Citrix Workspaceアプリのモデルに合わせてマッピングします。

- コピー (Ctrl+C または Command+C)
- 貼り付け (Ctrl+V または Command+V)
- 切り取り (Ctrl+X または Command+X)
- すべて選択 (Ctrl+A または Command+A)
- 元に戻す (Ctrl+Z または Command+Z)
- 検索 (Ctrl+F または Command+F)
- 保存 (Ctrl+S または Command+S)

セッション内ツールバーの改善

セッションツールバーは、iPhoneとiPadで統一されたデザインに刷新され、更新されたノッチとキーパッドのアセットが含まれています。ツールバーはiPadの向きに関わらず一貫して動作するようになり、セッション内キーボードとツールバー間のインタラクションが改善され、よりスムーズなユーザーエクスペリエンスが提供されます。

グラフィック設定のネイティブiOS設定との自動同期

Citrix Workspaceアプリ for iOS 2607以降、**［設定］>［表示オプション］>［解像度］**にあった従来の解像度ピッカーは、ネイティブiOS設定と表示スケーリングを連携させる、簡素化された意図ベースのオプションに置き換えられます。これにより、仮想デスクトップセッションを接続されたディスプレイの解像度（最大4K）に動的に調整することで、外部モニターでのDPIマッチングが容易になり、最適な鮮明さと読みやすさが実現されます。詳しくは、「グラフィック設定のネイティブiOS設定との自動同期」を参照してください。

EDTとTCP接続の並行試行による、より高速で回復力のあるセッション起動

Citrix Workspaceアプリ for iOSは、EDTとTCP接続を並行して試行することで、セッション起動を改善しました。以前は、セッション確立は一度に1つのトランスポートパスに依存しており、優先パスの応答が遅い場合や利用できない場合に接続設定時間が増加する可能性がありました。この機能強化により、アプリは最初に利用可能になったトランスポートで続行できるため、起動の遅延を減らし、さまざまなネットワーク条件下での接続の信頼性を向上させることができます。

廃止予定の通知

- バージョン27.3.0以降、**［EDTを許可］設定**はアプリUIでは利用できなくなりました。以前は、この設定は**［設定］>［詳細］>［アダプティブトランスポート設定］>［EDTを許可］**で利用可能でした。

EDTは、管理者制御の設定として引き続き利用可能です。この更新により、アプリのエクスペリエンスが簡素化され、管理ポリシーを通じて一貫したEDT構成が提供されます。

- バージョン26.11.0以降、**［自動構成］**、**［XenApp Services］**、および**［Access Gateway］**のストア追加方法は非推奨になります。**［手動セットアップ］**オプションは削除されます。**［Webインターフェイス］**オプションは、ウェルカム画面に移動され、**［カスタムWebストアとして追加］**に名称変更されます。

非推奨の項目については、非推奨のページを参照してください。

26.7.0で修正された問題

- 一定期間操作がないと、Citrix Workspaceアプリに**［開始］**画面が表示されることがあります。これは、ユーザーがすでにストアにログインしている場合でも発生します。
- Citrix Workspaceアプリ for iOSバージョン2509を使用すると、セッションの起動が**「セッションの起動が終了しました。セッションがユーザーに表示されなかったか、ICAエンジンが正しくロードされませんでした」**というエラーメッセージで失敗することがあります。
- Citrix Workspaceアプリを介して公開アプリを起動しようとしたときに、起動方法がWebブラウザに設定されている場合、**Failed to retrieve ICA**というエラーメッセージが表示されて起動に失敗することがあります。
- iOS版Citrix Workspaceアプリを使用している場合、VDAセッションで2バイト文字を貼り付けられないことがあります。
- iOS版Citrix Workspaceアプリ26.3.0を搭載したiPadで、ストアの資格情報を入力するとアプリがフリーズし、列挙画面が表示されないことがあります。
- プレゼンテーションモードで外部ディスプレイを使用している場合、iPadでローカル操作を行った後、カーソルが応答しなくなり、外部画面に戻らないことがあります。
- iOS版Citrix Workspaceアプリ25.11でWebインターフェースモードで追加されたストアから保護されたリソースを起動すると、**Session Error, Failed to Retrieve ICA**というエラーメッセージが表示されることがあります。

26.7.0の既知の問題

iPhoneで保護されたセッションを起動すると、画面上部に白い領域が表示され、Windowsタスクバーが消えることがあります。この問題を回避するには、デバイスの向きを横向きに変更してください。

26.3.10の新機能

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領域に対処しています。

26.3.10で修正された問題

- Citrix Gatewayが*http*経由でStoreFrontに接続されている場合、ストアの追加に失敗することがあります。

26.3.10の既知の問題

新しい既知の問題はありません。

26.3.0の新機能

オーディオユニット管理の改善

バージョン26.3.0以降、ステレオオーディオ処理がiOS 26との互換性向上のために改良されました。これにより、安定性、明瞭度、および高品質なサウンドパフォーマンスが向上します。

セッション再接続エクスペリエンスの改善（テクニカルプレビュー）

バージョン26.3.0以降、25.11.0リリースで発表された「セッションタイムアウトエクスペリエンスの改善（テクニカルプレビュー）」機能に以下の機能強化が加えられました。

- セッションタイムアウトの具体的な理由（**デバイスロック**、**アプリのバックグラウンド**、**ネットワークの中断**など）を表示します。
- セッション再接続設定は、GACSで**セッションエクスペリエンス > 接続**にある**手動セッション再接続**オプションを有効にするか、MDMを介して構成できます。

WSP非アクティブタイムアウト時のIdPログアウト

バージョン26.3.0以降、Citrix WorkspaceアプリはWorkspaceポータルに**非アクティブタイムアウト後にIDプロバイダーからログオフする**という設定を導入しました。この設定により、管理者はユーザーがCitrix Workspaceアプリからサインアウトしたときに、IDプロバイダー（Microsoft Entra IDなど）からユーザーをログアウトさせることができます。この機能は、多要素認証（MFA）が構成されているストアで動作します。

SecureHDX接続におけるEDTロッシーモードのサポート

バージョン26.3.0以降、EDT (Enlightened Data Transport) ロッシーモード（信頼性の低いサブチャネル）はSecureHDX (SecureICA 2.0) 接続でも動作します。以前は、EDTロッシーはDTLS暗

号化接続でのみ動作していました。この機能強化により、信頼性の低いサブチャネルのサポートがSecureHDX接続に拡張されます。SecureICA 2.0が有効な場合、オーディオやビデオなどの遅延に敏感なプロトコルのリアルタイムパフォーマンスが向上します。詳細については、EDTロッシーモードがSecureHDXをサポートするようになりましたを参照してください。

アクティブなHDXセッション中の動的なキーボード設定のサポート

バージョン26.3.0以降、アクティブなHDXセッション中に変更されたキーボード設定はすぐに有効になります。これにより、これまで必要だった既存のセッションを切断して再接続する必要がなくなります。

常時オンのトレース (AOT)

バージョン26.3.0以降、iOS版Citrix Workspaceアプリは、Citrixの最新の診断フレームワークである常時オンのトレース (AOT) を導入しました。AOTは、Citrix Virtual Apps and Desktops (CVAD) 環境全体で関連するログデータを継続的に収集します。これはCitrix Diagnostic Facility (CDF) トレースに基づいており、VDA登録の失敗やアプリまたはデスクトップの起動問題などの一般的な問題のトラブルシューティングに役立つコンポーネントログを追加します。AOTはバックグラウンドで自動的に実行され、問題を再現できない場合でも、問題発生時に重要な診断データが利用可能であることを保証します。

AOTは、以下の方法でIT管理者とCitrixサポートチームのトラブルシューティングを簡素化します。

- 手動の手順を必要とせずに、セッションログとシステムログを自動的にキャプチャします。
- アクセスしやすく、読みやすいログを提供します。
- セルフサービス診断を可能にします。
- Citrixサポートへの依存を軽減し、平均解決時間 (MTTR) の短縮を保証します。
- 完全な診断コンテキストにより、エスカレーションを容易にします。
- 機密データの編集により、ログを安全に処理します。

前提条件と詳細な構成情報については、Citrix Always On Tracingのドキュメントを参照してください。

メニューバーとソフトウェアキーボード機能の安定性の向上

リリース26.3.0には、iPadOS 26のプラットフォーム変更に合わせて、以下の機能強化が含まれています。

- デバイスの向きを変更すると、アプリは拡張キーボードを非表示にします。

- **デバイス設定 > ディスプレイと明るさ**で**拡張ディスプレイ**を有効にし、その後**Citrix Workspaceアプリの設定**で無効にした場合、マルチモニター設定でキーボードとマウスが機能しない場合があります。

2603で修正された問題

- Citrix Workspaceアプリを使用してLinux VDAに接続すると、Windows VDAでは機能するにもかかわらず、クライアントカメラが検出されないか、使用できない場合があります。
- セカンダリストアページでCitrix Workspaceアプリを終了し、再起動すると、プライマリストアの列挙ページが開きます。
- Citrix Workspaceアプリ for iOSバージョン25.7.0でストアURLを追加しようとすると、「エラーコード: 403」が表示される場合があります。
- フローティングウィンドウが有効になっている場合、別のアプリに切り替えてCitrix Workspaceアプリに戻った後、カスタム解像度設定が保持されない場合があります。
- Citrix Workspaceアプリを再起動すると、Webインターフェースモードの表示オプションに加えた変更はデフォルト値に戻ります。
- Citrix Workspaceアプリをバージョン25.11.0にアップグレードした後、セッション起動の失敗が発生する場合があります。
- Citrix Workspaceアプリバージョン25.9.0でVDAセッションを起動すると、「*The session launch ended; either the session was not visible to the user, or the ICA engine did not load properly*」というエラーが表示されることがあります。

2603の既知の問題

新しい既知の問題はありません。

25.11.0の新機能

deviceTRUST®とCitrix Workspace™アプリ for iOSのシームレスな統合

バージョン25.11.0以降、Citrix Workspaceアプリ for iOSにはdeviceTRUSTが搭載され、セッション内での継続的なデバイスポスチャチェックを通じてセキュリティが強化されます。
deviceTRUSTは、統合展開のためにCitrix Workspaceアプリと統合されています。詳細については、deviceTRUSTを参照してください。

主な詳細:

- **統合された機能:** リリース25.11.0以降、deviceTRUSTクライアント拡張機能はCitrix Workspaceアプリ for iOSの一部としてデフォルトでインストールされ、展開と管理が簡素化されます。
- **継続的なポスチャチェック:** この機能は、セッション内でエンドポイントデバイスのコンテキストとセキュリティポスチャを継続的にチェックすることでセキュリティを強化し、ゼロトラストセキュリティモデルの実装を支援します。
- **互換性:** この統合は、iOS 17、18、および26のバージョンでサポートされています。
- **管理:** 管理者はdeviceTRUSTコンソールを使用して、ポリシーを構成し、デバイス信頼設定を管理できます。構成方法の詳細については、Getting Started for Localを参照してください。

強化されたオンスクリーンキーボードエクスペリエンス

バージョン25.11.0以降、CitrixはWindows Virtual Desktop Agent (VDA) 25.11.0デスクトップに接続する際の自動キーボード表示動作の改善により、タッチキーボードエクスペリエンスを強化しました。

これらの機能強化により、オンスクリーンタッチキーボードを使用中に、デスクトップセッションの下部に表示される入力フィールドやタスクバー要素を操作する際の使いやすさが向上します。

改善されたセッションタイムアウトエクスペリエンス（テクニカルプレビュー）

この取り組みは、非アクティブまたはネットワーク中断によって引き起こされるセッションタイムアウト中のエンドユーザーエクスペリエンスを向上させることを目的としています。クラウドとオンプレミスの両方のストアのユーザーは、タイムアウト画面から直接再接続するオプションが提供され、クライアントUIからセッションを再起動する必要がなくなります。

主な機能:

- タイムアウト画面には、**デバイスがスリープ状態になりました** や **ネットワークの中断** など、セッションタイムアウトの具体的な理由が表示されます。
- 管理者の構成に基づいて、ユーザーは新しいセッションであるか、以前のセッションの継続であるかにかかわらず、セッションにシームレスに再接続できます。
- このソリューションは、ネットワークの切り替え（例: Wi-FiからLAN）など、自動再接続が失敗する可能性のある再接続シナリオをサポートします。

> **注：**

> この機能は現在、ブラウザから起動されたセッションや、Webインターフェイスとして追加されたストアではサポートされていません。

> この管理者制御機能を有効にする方法の詳細については、Citrix Virtual Apps and DesktopsのHDXドキュメントを参照してください。

カスタムWebストアでのアンチスクリーンキャプチャおよびアンチキーロギングのサポート

バージョン25.11.0以降、App Protectionの**アンチスクリーンキャプチャ**と**アンチキーロギング**がカスタムWebストアでサポートされるようになりました。

Webインターフェイスのユーザーエージェント

バージョン25.11.0以降、Webインターフェイスを介して開始される一部のネットワーク要求中に使用されるユーザーエージェント文字列には、デフォルトでCitrix Workspaceアプリの識別子が含まれるようになりました。

変更前のユーザーエージェントは次のとおりでした。 `Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148`

変更後のユーザーエージェントは次のとおりです。

`Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148`

`CWA/25.11.0 iOS/26.2 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad`

iOS上のEntra ID参加済みVDAに対するシームレスなシングルサインオン

バージョン25.11.0以降、iOS版Citrix Workspaceアプリは、クラウド展開におけるMicrosoft Entra ID参加済みVDAとのシームレスなシングルサインオン（SSO）をサポートします。以前は、このシナリオではSSOが利用できなかったため、Microsoft Entra ID参加済みVDAでHDXセッションを起動する際に、ユーザーは資格情報の入力を求められていました。この変更により、管理者はSSOを構成するオプションが提供され、セッション起動時の資格情報入力の必要性を省略できるため、Entra IDを主要なIDプロバイダーとして使用する組織の認証が効率化されます。

この機能により、Active DirectoryからEntra IDに移行するユーザーは、手動で資格情報を入力することなくセッションを起動でき、改善された簡素化された認証エクスペリエンスが提供されます。

システムの互換性とエンドツーエンドの構成手順については、Microsoft Entraシングルサインオンを参照してください。

25.11.0で修正された問題

- USB-C - 3.5mmヘッドホンジャックアダプターがデバイスに接続されているときにTeams通話中にCitrix Workspaceアプリがクラッシュする場合があります。
- SPAから展開されたVisma Webアプリにアクセスすると、Citrix Workspaceアプリがクラッシュする場合があります。
- ストアの資格情報を入力した後、iOS向けCitrix Workspaceアプリが「サービスの取得中」ダイアログで停止する場合があります。
- GACSで構成されたオンプレミスストアで、システム認証ブラウザを使用してFIDO2で認証する際に問題が発生した可能性があります。
- 派生資格情報を使用してiOS 24.9.0向けCitrix Workspaceアプリにアカウントを追加しようとすると、問題が発生する場合があります。
- バージョン25.3.1からアップグレードした後、Citrix Workspaceアプリ25.7.2でピンチ＆ズーム機能に一貫性のない動作が発生する場合があります。
- 以前のバージョンのiOS向けCitrix Workspaceアプリでは、ネットワーク障害後にEDTセッションを再接続する際に、転送に一貫性のない動作が発生した可能性があります。更新されたバージョンでは、最後に成功したプロトコルが維持され、利用可能な場合はEDTを使用し、EDTが利用できない場合にのみTCPにフォールバックします。

25.11.0の既知の問題

新しい既知の問題はありません。

25.9.0の新機能

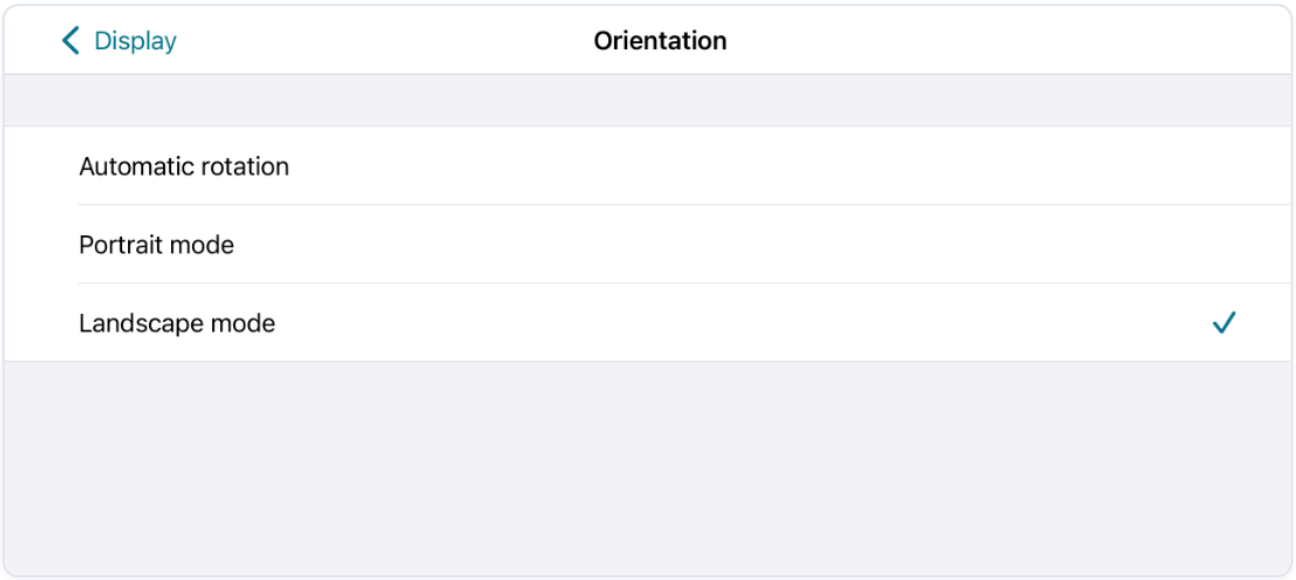
Citrix Troubleshoot Connectionによるトラブルシューティングの強化

以前は、仮想アプリまたはデスクトップの起動に関する問題の解決には、ITサポートが必要でした。強化されたCitrix Troubleshoot Connection機能では、刷新されたUIを通じて、Citrix Workspaceアプリが明確なエラーメッセージと段階的な推奨事項を提供することで、ユーザーが起動に関する問題を自己修復および修正できるようにします。ユーザーは詳細なエラーと問題を修正するためのボタンを確認できます。ネットワークの問題や利用できないリソースなどの一般的な問題は、ワンクリックの回復アクションで解決できます。これにより、ITサポートの必要性が減

り、より迅速に作業に戻ることができます。詳細については、Citrix Troubleshoot Connectionを参照してください。

iPhoneでの横向きモードのサポート

この機能には、デバイスでのトラブルシューティングエクスペリエンスを向上させるためのiPhoneでの横向きモードのサポートも含まれています。この設定により、デスクトップコンテンツやデータ集約型画面を最適に表示するために、アプリの向きを選択できます。バージョン2509では、デフォルトの向きは**自動回転**です。



デスクトップ起動エクスペリエンスの強化

バージョン2509以降、iOS向けCitrix Workspaceアプリは、強化されたデスクトップ起動エクスペリエンスを提供します。ユーザーは、中間画面なしで、シームレスでちらつきのないデスクトップへの移行を体験できます。また、アプリはサイズ変更や拡大時の黒い画面やちらつきをなくし、安定した最新のインターフェイスを提供します。この機能はデフォルトで有効になっています。

外部キーボードのCaps Lock同期の改善

バージョン2509以降、iOS向けCitrix Workspaceアプリは、外部キーボードを使用する際のCaps Lock同期の処理を改善します。このアプリは、iOSクライアントとVirtual Delivery Agent (VDA)の間でCaps Lockの状態が一貫していることを保証し、シームレスな入力動作を提供します。ローカルのiOSアプリとCitrixセッションを切り替えても、大文字と小文字の入力が一致しない問題は発生しなくなりました。

オーディオデバイスと音量同期の改善

仮想セッションでのオーディオデバイスと音量の管理方法を強化しました。

オーディオデバイス同期の改善: 現在選択されているシステムオーディオデバイスのみがVirtual Delivery Agent (VDA)にマッピングされるようになり、不要なデバイスマッピングが防止されます。デバイスの実際の名前は保持されるため、セッション内で識別しやすくなります。

オーディオ音量同期の強化: スピーカーの音量は、システムからVDAへ一方向で同期されるようになりました。また、VDA内でマイクゲインを直接調整できるようになり、Citrix Workspaceアプリはこの設定を保存し、今後のセッションで使用します。

レガシー機能の非推奨通知

バージョン26.3.0以降、iOS向けCitrix Workspaceアプリは以下のレガシー機能をサポートしなくなりました。以下の機能のサポートは終了しました。

- Citrix X1 マウス
- シトリックス キャスティング

詳細については、「Citrix Workspace app for iOS deprecation」を参照してください。

25.9.0で修正された問題

- セッションがウィンドウモードに切り替わったときに、iOS 26デバイスで拡張ツールバーUIが表示される場合があります。
- Citrix Workspaceアプリのウィンドウのサイズを変更したときに、iOS 26デバイスでソフトキーボードが消える場合があります。
- セッションを起動する際、Citrix Workspaceアプリがセッション起動画面でYubikeyに存在する証明書を検出しない場合があります。
- iPhoneデバイスでCitrix Workspaceアプリ for iOSを使用している場合、ストアにログインできないことがあります。
- iPadデバイスでCitrix Workspaceアプリ for iOSを使用している場合、オーディオが2203 VDAにリダイレクトされないことがあります。
- Citrix Workspaceアプリ for iOSでAirPodsを使用している場合、セッション中に呼び出し音が聞こえないことがあります。
- USB-Cハブを介して接続されたオーディオデバイスは、Citrix Workspaceアプリ for iOSのSkypeで動作しない場合があります。
- セッション内でWindows Media Playerで再生されているオーディオファイルの音量を、デバイスの音量アップ/ダウンボタンで増減できない場合があります。
- Audacityを介して録音を再開した後、オーディオ再生が停止する場合があります。

- ネットワーク接続がオフの状態でストアからサインアウトしようとすると、Citrix Workspaceアプリがクラッシュする場合があります。
- iPadデバイスで、セッション起動中に外部モニターに接続されている場合、Citrix Workspaceアプリがクラッシュする場合があります。

25.9.0の既知の問題

- USB-C - 3.5mmヘッドホンジャックアダプターがデバイスに接続されている状態でTeams通話中にCitrix Workspaceアプリがクラッシュする場合があります。
- デバイスがしばらくロックされた後、ロックを解除すると、セッション画像の切り捨てが発生する場合があります。

以前のリリース

このセクションでは、サポート対象の以前のリリースにおける新機能と修正された問題に関する情報を提供します。これらのリリースのライフサイクルに関する詳細については、Lifecycle Milestones for Citrix Workspace app and Citrix Receiverを参照してください。

25.7.2

新機能

iOS 26のサポート

Citrix Workspace app for iOS は現在 iOS 26 をサポートしています。iOS 26 の詳細については、ブログ iOS26 を参照してください。

強化された接続強度インジケーター

接続強度インジケーターは、接続品質に関するリアルタイムの洞察を提供し、接続の問題を自己解決するのに役立ちます。この機能はツールバーからアクセスでき、デフォルトで有効になっています。バージョン 25.7.2 から、インジケーターが強化され、以下の情報が表示されるようになりました。

- ローカルデバイスでの**リアルタイムのCPU、メモリ、ディスク**使用量。パフォーマンスの低下がエンドポイントコンピューティングの負荷によるものかどうかをユーザーに可視化します。
- 過去15分間のアクティビティを可視化する**接続履歴**。接続が常に安定していたか、断続的な切断が発生していたかを示します。

- **リアルタイムの推奨事項** - 接続強度インジケーターは、サポートチケットを発行する前にユーザーが接続の問題を解決するのに役立つ可能性のある推奨事項をユーザーに提供しようとします。

詳細については、「強化された接続強度インジケーター」を参照してください。

デスクトップとアプリの自動起動

バージョン 25.7.2 以降、Citrix Workspace app for iOS は、Citrix Studio で管理者が `KEYWORDS:AutoStartPrimaryApp` とタグ付けしたデスクトップまたはアプリを自動的に起動します。この機能は、クラウドストアとオンプレミスストアの両方で動作します。詳細については、「デスクトップとアプリの自動起動」を参照してください。

ロックダウンモードでのiPadおよびiPhoneのサポート

バージョン 25.7.2 以降、Citrix Workspace app for iOS は iPad および iPhone のロックダウンモードをサポートします。ロックダウンモードが有効になっている場合、特定のデバイス機能は意図的に制限されます。

25.7.2 で修正された問題

新しい修正された問題はありません。

25.5.10

新機能

このリリースにはマイナーなバグ修正が含まれており、Citrix Workspace app for iOS は現在 iOS 26 をサポートしています。

修正された問題

このリリースには修正された問題はありません。

25.5.0

新機能

ポインターモードのエクスペリエンスを強化

バージョン25.5.0以降、iOS向けCitrix Workspaceアプリは、ポインターモード使用時にセッション内でのスクロールとズームをサポートします。ポインターモードでは、ユーザーは次のことができるようになりました。

- 2本指でスワイプ（垂直または水平）して、それぞれの方向にスクロールします。
- 2本指でタップしてホールドし、その後ピンチジェスチャを使用してセッションコンテンツをズームします。

> **注：**
>
> デフォルトでは、2本指のピンチでローカルズームが実行されます。リモートズームを実行するには、「Remote zoom enabled」というメッセージが表示されるまで2本指で数秒間タップしてホールドし、その後ズーム操作に進みます。

キーボード設定の表示に関する更新

iOS向けCitrix Workspaceアプリバージョン25.5.0以降、ストアが構成されていない場合でもキーボード設定が表示されるようになりました。以前は、Citrix Workspaceアプリのキーボードオプションはストアを追加した後にのみ表示されていました。お客様の環境では、この機能は期待どおりに動作し、ストアの追加後に同期は成功していました。しかし、お客様はセキュリティ上の制限により、ストアをCitrix Workspaceアプリに追加できないと報告しています。

この更新により、セキュリティポリシーのためにストアを追加できないユーザーでも、必要に応じてキーボード設定にアクセスして変更できるようになります。

デスクトップのリサイズエクスペリエンスをスムーズに

画面のサイズ変更やウィンドウモードの変更中に、黒い画面やちらつきが発生する場合があります。この機能は、これらの問題を解消し、画面のサイズ変更や引き伸ばし時にスムーズでシームレスな移行を提供することで、ユーザーエクスペリエンスを向上させます。

フローティングセッションウィンドウのサポート

モバイルデバイスのVDAセッションでアプリを切り替える際に、中断や切断が発生する場合があります。この問題は、会議への参加やMFA認証の実行などのマルチタスク中に頻繁に発生しま

す。この機能は、アプリがバックグラウンドで実行されている場合でも、オーディオやグラフィックなどのセッションパフォーマンスを中断することなく維持することで、ユーザーエクスペリエンスを向上させます。これにより、ユーザーはセッションのタイムアウトや視認性の喪失を心配することなく、シームレスにマルチタスクを実行できます。この機能は、Stage Managerをサポートしないデバイスに対して、より信頼性が高く効率的なワークフローを提供します。

制限事項

この機能はiOS 18.0以降で動作します

- デバイスのチップ機能が異なるため、マルチタスクカメラはサポートされない場合があります。
- マルチモニターシナリオはサポートされていません。

修正された問題

- Azure Multi-Factor認証を使用して認証できない場合があります。
- iOS上のCitrix Workspace™アプリ構成がIntune経由で展開されている場合、オンプレミスストアが1つしか表示されるように構成されていないにもかかわらず、複数のストアが表示されることがあります。

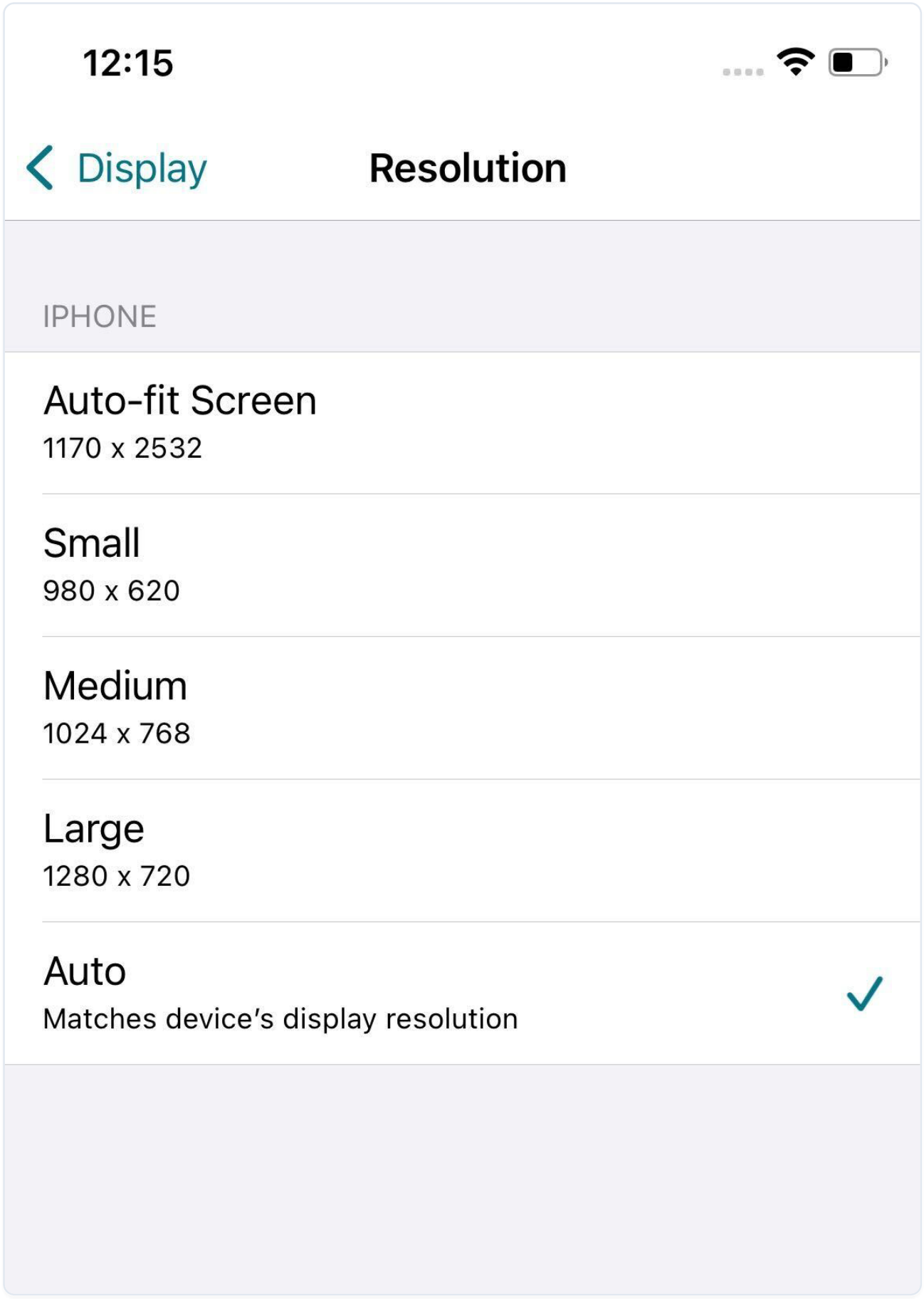
25.3.4

新機能

セッション解像度の強化

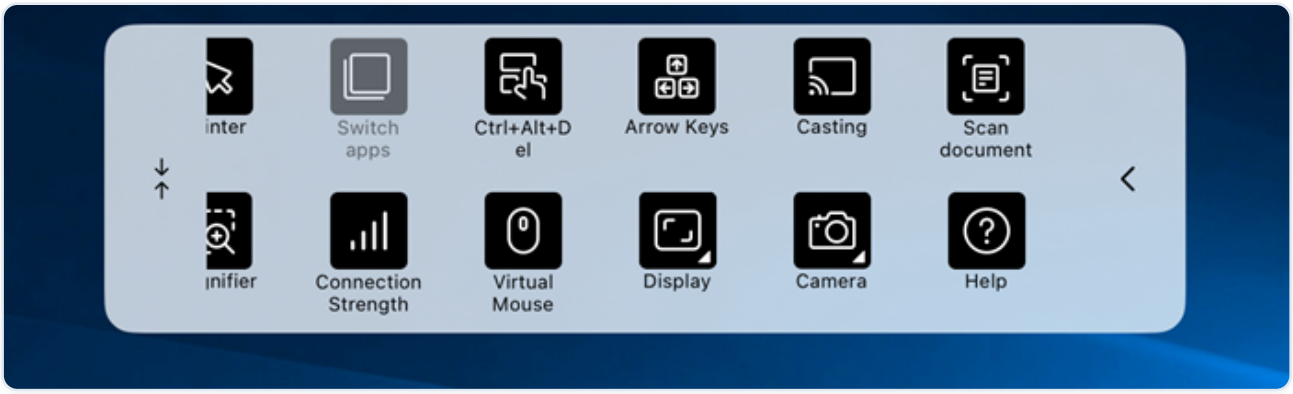
バージョン25.3.4以降、iOS版Citrix Workspaceアプリは、よりシームレスなユーザーエクスペリエンスのために、セッション解像度の強化を導入します。デフォルトで「自動」に設定されており、ユーザーがセッションを起動するたびに**DPI**設定が自動的に調整され、全体的なエクスペリエンスが向上します。

一貫性のある使いやすいエクスペリエンスを確保するため、仮想デスクトップはデフォルトで横向きモードで起動するようになりました。これにより、ワイドスクリーンアプリケーションやマルチタスクのニーズに対応します。この機能はデフォルトで有効になっています。


12:15
Display
Resolution
IPHONE
Auto-fit Screen
1170 x 2532
Small
980 x 620
Medium
1024 x 768
Large
1280 x 720
Auto
Matches device's display resolution

新しいセッション内ツールバー

バージョン25.3.4以降、Global App Configurationサービス (GACS) およびモバイルデバイス管理 (MDM) を介して管理者設定が構成されていない場合、新しいツールバーはデフォルトで有効になります。



修正された問題

- iOS版Citrix Workspaceアプリバージョン25.3.4にアップグレードした後、一部のユーザーはセッションを起動しようとすると、次のエラーに遭遇する可能性があります。 操作を完了できませんでした (HDXSDKErrorDomain_Session Error 8)。
- VDA 2402および2402 CU1を使用している一部のiPadユーザーは、SkypeやWebexなどのアプリでの通話中に相手の声を聞くことができません。影響を受けるユーザーはセッションからのメディア再生は聞くことができますが、相手の声は聞こえません。オーディオを一度切断して再接続すると、一時的な回避策となる場合があります。
- Windows VDAでタスクバーのバッテリーアイコンをクリックすると、ツールバーのポインターが有効になることがあります。
- iPadデバイスに物理マウスが接続されている場合、拡大鏡とポインターのアイコンが自動的にオフにならないことがあります。
- アイパッドオーエス: Firebase-Foundation _userInfoForFileAndLine-AppSwitcher.

25.1.2

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領域に対処しています。

修正された問題

ユーザーが指定されたVPNに接続している場合、iOS版Citrix Workspaceアプリはセッションを確立できないことがあります。

25.1.1

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領域に対処しています。

> **重要:**
>
> バージョン25.1.0は安定性の問題によりロールバックされました。利用可能な新しいバージョンは25.1.1です。これは、最新ビルド25.1.1にはバージョン25.1.0の機能が含まれていないことを意味します。現在、バージョン25.1.0のすべての機能と必要な修正を含む新しい安定版ビルドに取り組んでいます。

修正された問題

以前の安定版ビルドと同様です。

25.1.0

新機能

- 事前入力されたユーザー名によるCitrixセキュリティの強化
- GACS認証済みマイクロサービス（オンプレミス）をサポート
- クロス・マルチスクリーンエクスペリエンスの強化
- DPIマッチング
- 仮想デスクトップのデフォルト横向き表示
- 強化されたセキュアICA
- 改善されたマウスポインターモード

改善されたマウスポインターモード

バージョン25.1.0以降、iOS版Citrix Workspaceアプリはマウスポインターモードの改善を導入します。この機能により、よりスムーズで一貫したエクスペリエンスを提供するための以下の機能強化が導入されます。

- マウスポインターがスワイプ速度を使用して、より自然に動くようになりました。
- マウスポインターモードが、iPadと同様にiPhoneでも利用可能になりました。

注：

このリリースから、iPhoneでのセッションはデフォルトでマルチタッチモードで起動し、ピンチジェスチャでセッション内ズームを実行できるようになります。クライアント側（ビューポート）ズームを使用するには、ポインターモードを有効にする必要があります。

事前入力されたユーザー名によるCitrix®セキュリティの強化

バージョン25.1.0以降、Unified Endpoint Management (UEM) を使用して、特定の形式でユーザー名をプッシュし、デバイスを管理できます。iOSでは、Citrix Workspaceアプリがこの構成を読み取り、ユーザー名を取得し、認証プロンプトに事前入力して読み取り専用にします。詳細については、「事前入力されたユーザー名によるCitrixセキュリティの強化」(/ja-jp/citrix-workspace-app-for-ios/authenticate.html#enhanced-citrix-security-with-pre-populated-user-name)を参照してください。

GACS認証済みマイクロサービス（オンプレミス）をサポート

バージョン25.1.0以降、iOS版Citrix Workspaceアプリは認証済みマイクロサービスをサポートし、GACSがユーザーグループを管理できるようになります。この機能により、管理者はオンプレミス環境で強化された制御を行うことができます。詳細については、「GACS認証済みマイクロサービス（オンプレミス）をサポート」(/ja-jp/citrix-workspace-app-for-ios/configure.html#supports-gacs-authenticated-microservices-on-premises)を参照してください。

クロス複数画面エクスペリエンスの強化

バージョン25.1.0以降、iOS版Citrix Workspaceアプリは、外部モニターまたはドックに接続されたiPadのユーザーエクスペリエンスを向上させます。これらの更新には、マルチタスクを改善するために複数の画面にアプリケーションを分散する機能が含まれます。この機能はデフォルトで有効になっています。詳細については、「クロス複数画面エクスペリエンスの強化」(/ja-jp/citrix-workspace-app-for-ios/configure/user-experience.html#enhance-cross-multi-screen-experience)を参照してください。

DPIマッチング

DPIマッチング機能により、仮想セッションがデバイスのDPIに従ってレンダリングされることが保証されます。バージョン25.1.0以降、新しい表示設定によりDPIマッチング機能が強化されます。詳細については、「DPIマッチング」(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#dpi-matching)を参照してください。

仮想デスクトップのデフォルトの横向き表示

バージョン25.1.0以降、Citrix WorkspaceアプリはiPhoneデバイスで仮想デスクトップを起動する際に、デフォルトで横向き表示を適用します。これにより、ワイドスクリーンアプリケーションとマルチタスクにおいて、最適で一貫性のあるユーザーエクスペリエンスが保証されます。詳細については、「仮想デスクトップのデフォルトの横向き表示」(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#default-landscape-orientation-for-virtual-desktops)を参照してください。

強化されたセキュアなICA®

バージョン25.1.0以降、新しいICA暗号化機能は、最新の暗号化アルゴリズムを使用することでセキュリティを向上させます。これにより、当社の製品のセキュリティ体制が強化され、お客様はシンプルかつ信頼性の高い方法で環境のセキュリティ体制を強化できるようになります。詳細については、「強化されたセキュアなICA」(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#enhanced-secured-ica)を参照してください。

25.1.0で修正された問題

このリリースには、新たに修正された問題はありません。

24.12.0

新機能

- インメモリICAソリューションの起動
- 高速スマートカード(#fast-smart-card)
- ゲートウェイを使用したオンプレミスWSUIのサポート
- Citrix Workspaceアプリを使用したCitrixアクセス強制
- 地理的位置に基づくマルチサイトストアフェールオーバーのサポート
- Altキーの右オプションキーマッピング
- 接続強度インジケーター
- 強化された新しいカスタマイズ可能なツールバー
- オペレーティングシステムiOS 15の非推奨化

インメモリICAソリューションの起動

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、Citrix Workspaceランチャーを使用したインメモリハイブリッド起動のサポートを強化します。この改善により、ICAファイルをダウ

ンロードする必要がなくなり、より効率的で安全なユーザーエクスペリエンスが可能になります。詳細については、「インメモリICAソリューションの起動」を参照してください。

高速スマートカード

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、認証パフォーマンスと使いやすさを向上させるスマートカードの機能強化を導入します。このアップデートにより、スマートカードのサポートが大幅に改善され、ユーザーエクスペリエンスがよりスムーズで効率的になります。詳細については、「高速スマートカード」を参照してください。

ゲートウェイを使用したオンプレミスWSUIのサポート

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、ゲートウェイの背後にあるオンプレミスストアのWeb UIもサポートします。この機能はデフォルトでは有効になっていないため、管理者が構成する必要があります。詳細については、「ゲートウェイを使用したオンプレミスWSUIのサポート」を参照してください。

Citrix Workspaceアプリを使用したCitrixアクセス強制

バージョン24.12.0以降、管理者はiOSデバイスのユーザーに対し、Citrix Workspaceへのアクセスをネイティブアプリ経由のみに義務付けることができます。この機能が有効になっている場合、ストアURLやサードパーティ製ブラウザにアクセスしようとするユーザーは、自動的にCitrix Workspaceアプリにリダイレクトされます。これにより、ユーザーはネイティブアプリのすべての機能を活用し、シームレスなユーザーエクスペリエンスを享受できます。詳しくは、「Citrix Workspaceアプリを使用したCitrixアクセス強制」を参照してください。

地理的位置に基づくマルチサイトストアフェイルオーバーのサポート

バージョン24.12.0以降、マルチストアフェイルオーバー処理機能は、ストアアドレスチェックを非同期で実行し、新しいフェイルオーバーストアアドレスが検出されたときに古いストアエントリを削除することで、マルチストアフェイルオーバー処理を改善します。詳しくは、「地理的位置に基づくマルチサイトストアフェイルオーバーのサポート」を参照してください。

Altキーの右Optionキーマッピング

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリでは、セッション内で右OptionキーをAltキーにマッピングできる機能強化が導入されました。詳しくは、「Altキーの右Optionキーマッピング」を参照してください。

接続強度インジケーター

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、**Desktop Viewer**ツールバーで接続強度インジケーターをサポートします。この機能は、ネットワークの問題を警告するネットワーク強度アイコンを表示します。詳しくは、「接続強度インジケーター」を参照してください。

強化された新しいカスタマイズ可能なツールバー

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、新しいカスタマイズ可能なツールバーを導入します。刷新されたDesktop Viewerツールバーは、より高い柔軟性を提供することで、ユーザーエクスペリエンスとサポートを強化します。管理者は、組織のニーズに合わせてセッション内ツールバーをカスタマイズできるようになりました。新しいツールバーで外部Webカメラの選択が可能になりました。詳しくは、「強化された新しいカスタマイズ可能なツールバー」を参照してください。

オペレーティングシステムiOS 15の非推奨化

24.12.0リリース以降、オペレーティングシステムiOS 15のサポートは非推奨になりました。代替として、利用可能な最新バージョンのiOSにアップグレードできます。詳しくは、「非推奨」を参照してください。

24.12.0で修正された問題

- 削除されたストア設定にインストールされていたクライアント証明書を削除できない場合があります。
- ユーザーがサイドバーからセッションを切断しても、セッションがセカンダリモニターでアクティブなままになる場合があります。
- iPadでCitrix Workspaceアプリを開き、StoreFront™ 2402 LTSRの次世代UIを使用しているときに、「**サーバーに接続できません**」というエラーメッセージが表示されることがあります。

24.10.0

新機能

機能フラグの管理

Citrixは、機能フラグの管理方法を変更し、プレビュー機能へのアクセスを許可し、本番環境での機能の動的な管理を可能にしています。機能フラグの下にある機能が最適に機能するようにするには、URL `features.netscalergateway.net` へのトラフィックを有効にする必要があります。詳細については、「機能フラグの管理」を参照してください。

修正された問題

同じVDAから公開された複数のアプリが開いている場合、セッションツールバーの**「切り替え」**ボタンをクリックしても、ユーザーがこれらのアプリを切り替えることができず、応答がない場合があります。

24.9.0

新機能

- iOS 18のサポート
- ラピッドスキャンのサポート
- サステナビリティへの取り組みのサポート
- 強化されたマルチアプリウィンドウ管理
- 生体認証有効化プロンプトのスキップ
- メール、ストアURL、またはドメインベースの検出APIによるGACSエンドポイントの取得
- GACS認証済みマイクロサービス（クラウド）のサポート
- App Protectionのサポート

iOS 18のサポート

Citrix Workspaceアプリ for iOSは、iOS 18をサポートするようになりました。

Rapid Scanのサポート

バージョン24.9.0以降、iOS向けCitrix WorkspaceアプリはRapid Scan機能をサポートしています。この機能を使用すると、iOSデバイスで複数のドキュメントをスキャンし、スキャンしたドキュメントをMacおよびiOS向けCitrix Workspaceアプリを使用してMacデバイスに転送できます。

詳細については、「Rapid Scanのサポート」を参照してください。(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#support-for-rapid-scan)

サステナビリティへの取り組みのサポート

バージョン24.9.0以降、ユーザーは仮想デスクトップを閉じると、デスクトップセッションからサインアウトするよう促されます。この機能は、不要なときにVMからサインアウトすることで、エネルギーの節約に役立ちます。以前は、これらのセッションは切断された状態のままであり、不必要なエネルギー消費につながっていました。

詳細については、「サステナビリティへの取り組みのサポート」を参照してください。(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#support-for-sustainability-initiative)

強化されたマルチアプリウィンドウ管理

バージョン24.9.0以降、iOS向けCitrix Workspaceアプリは、外部モニターに接続されたiPad向けのシームレスなマルチアプリウィンドウ管理をサポートしています。この機能は、ネイティブのマルチアプリエクスペリエンスを可能にすることで、マルチタスクと生産性を向上させます。iPadデバイスが外部モニターに接続されていない場合でも、この機能を有効にできます。

詳細については、「強化されたマルチアプリウィンドウ管理」を参照してください。(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#enhanced-multi-app-window-management)

生体認証有効化プロンプトをスキップ

以前は、エンドユーザーはCitrix Workspaceアプリでの認証に生体認証（Touch IDまたはFace ID）を使用するかどうかを選択するよう促されていました。バージョン24.9.0以降、管理者はこのプロンプトをスキップできるようになり、ユーザーのログインプロセスが効率化されます。

生体認証が有効になっている場合、ユーザーパスワードはキーチェーンに安全に保存され、生体認証によって保護されます。認証トークンの有効期限が切れると、ユーザーは自動的に生体認証の確認を求められます。デバイスで生体認証が構成されていない場合、トークンの有効期限が切れたときにユーザーは手動で資格情報を入力する必要があります。

この機能は現在、LDAP認証を使用するオンプレミスストアでのみサポートされています。

詳細については、「生体認証有効化プロンプトをスキップ」を参照してください。(/ja-jp/citrix-workspace-app-for-ios/authenticate.html#skip-enable-biometrics-prompt)

メール、ストアURL、またはドメインベースの検出APIによるGACSエンドポイントの取得

バージョン24.9.0以降、管理者はメールアドレス、ドメイン、ストアURLに基づいてWebストアを構成できるようになり、Global App Configuration Service (GACS) がユーザーを適切なカスタムWeb URLに識別して誘導できるようになります。Citrix WorkspaceアプリのiOSデバイスは、この検出APIを使用してGACSエンドポイントを取得できるようになり、ハードコードされたエンドポイントが不要になり、構成されていない場合の不要な呼び出しが削減されます。

詳しくは、「メール、ストアURL、またはドメインベースの検出APIによるGACSエンドポイントの取得」を参照してください。

GACS認証済みマイクロサービス（クラウド）をサポート

24.9.0リリース以降、iOS版Citrix Workspaceアプリは認証済みマイクロサービスをサポートし、GACSがお客様のユーザーグループを管理できるようになりました。これにより、柔軟性と制御が向上し、現在はクラウドストアのみでサポートされています。

詳しくは、「GACS認証済みマイクロサービス（クラウド）のサポート」を参照してください。

アプリ保護のサポート

バージョン24.9.0以降、iOS版Citrix Workspaceアプリはアプリ保護機能をサポートしています。

アプリ保護は、Citrix Workspaceアプリの機能で、Citrix Virtual Apps and Desktops™公開リソースを使用する際にセキュリティを強化します。この機能は、クライアントがキーロギングや画面キャプチャマルウェアによって侵害される可能性を制限します。アプリ保護は、ユーザー資格情報や画面に表示される機密情報などの機密情報の持ち出しを防ぎます。この機能により、ユーザーや攻撃者がスクリーンショットを撮ったり、キーロガーを使用して機密情報を収集したり悪用したりすることを防ぎます。

詳しくは、「アプリ保護のサポート」を参照してください。

24.9.0で修正された問題

新しい修正された問題はありません。

24.8.1

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領域に対処しています。

24.8.1で修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

24.8.0

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領域に対処しています。

24.8.0 で修正された問題

- スマートカードが有効な設定で、VDAセッションを起動し、仮想デスクトップに正常にログインできない場合があります。

24.7.0

新機能

DTLS 1.2 のサポート

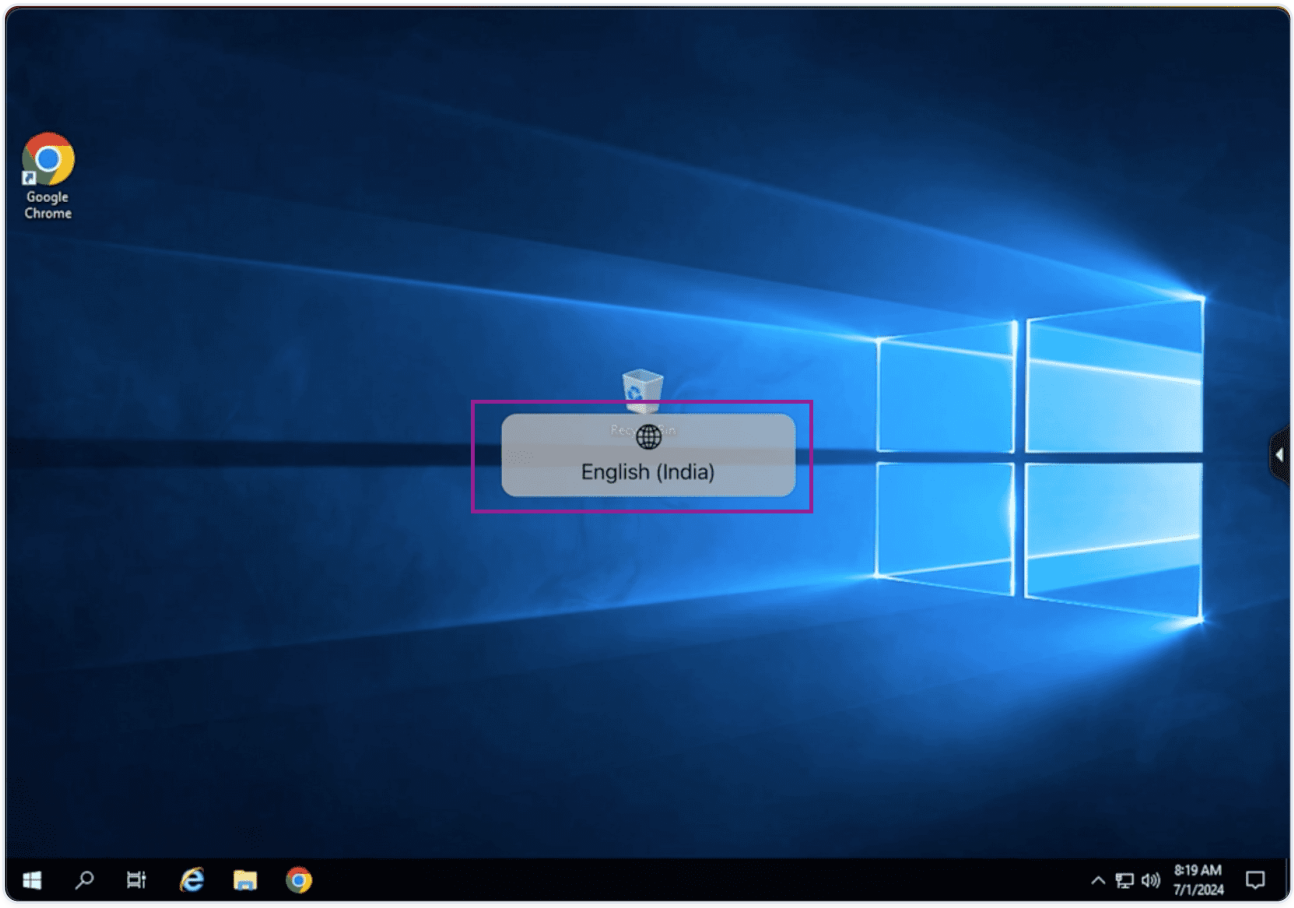
バージョン24.7.0以降、iOS向けCitrix WorkspaceアプリはDTLSプロトコルバージョン1.2をサポートします。DTLS 1.2は、堅牢な暗号化アルゴリズム、より優れたハンドシェイクプロトコル、さまざまな攻撃からの保護など、以前のバージョンに比べて機能強化と改善を提供します。このプロトコルは全体的なセキュリティを向上させます。

> **注：**
>
> DTLSプロトコルバージョン1.2に問題がある場合、iOS向けCitrix Workspaceアプリはシームレスに以前のサポートバージョンにフォールバックします。

> 詳細については、「DTLS 1.2 のサポート」を参照してください。

仮想セッションでのキーボード言語変更の検出と表示

バージョン24.7.0以降、iOS向けCitrix Workspaceアプリは、ユーザーがキーボード言語を切り替えると、仮想セッション内でメッセージを自動的に検出し表示するようになりました。デバイスのキーボードまたは外部キーボードの地球儀キーを使用してキーボード言語を切り替えると、現在のキーボード言語を通知するメッセージが画面に表示されます。この機能により、仮想セッション内で現在のキーボード言語を把握できます。



詳細については、「仮想セッションでのキーボード言語変更の検出と表示」を参照してください。

アダプティブオーディオのサポート

バージョン24.7.0以降、iOS向けCitrix WorkspaceアプリはHDXアダプティブオーディオをサポートします。この機能は、オーディオ品質の向上と低遅延を提供することで、ユーザーエクスペリエンスを向上させます。

詳細については、Citrix Virtual Apps and Desktopsドキュメントの「オーディオポリシー設定」の記事を参照してください。

UEMを介したCitrix Workspaceアプリ設定の構成のサポート

以前は、Citrix WorkspaceアプリでストアURLを構成できるのは、Unified Endpoint Management (UEM) を使用した場合のみでした。

バージョン24.7.0以降、インフラストラクチャに展開されている任意のUEMソリューションを使用して、管理対象デバイス上のCitrix Workspaceアプリ設定を構成することもできます。

> **注：**

> 管理者として、UEMとGlobal App Configurationサービス (GACS) を使用してCitrix Workspaceアプリ設定を構成するオプションがある場合、UEM設定がGACSよりも優先されます。

> 詳細については、「UEMを介したCitrix Workspaceアプリ設定の構成のサポート」を参照してください。

テクニカルプレビュー

- オンプレミスストアへの接続時のFIDO2を使用した認証のサポート
- 複数のオーディオデバイスのサポート
- アプリ保護のサポート

テクニカルプレビュー機能の完全なリストについては、「テクニカルプレビューの機能」ページを参照してください。

24.7.0で修正された問題

- Secure Private Accessがクライアントレスvpn (cVPN) ポリシーで有効になっている場合、iOS版Citrix WorkspaceアプリのNetScaler®ストアユーザーは新しいUIにサインインできないことがあります。(RFIOS-13733)

24.6.0

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領域に対処しています。

24.6.0で修正された問題

- iPad Pro M4デバイスの仮想セッションで、Magic Keyboardのトラックパッドが正常に機能しない場合があります。詳細については、「Citrix Knowledge Centerの記事 - CTX677048」を参照してください。
- 仮想アプリセッションからデバイスカメラを使用して画像をキャプチャすると、キャプチャされた画像が逆さまに表示されることがあります。
- 仮想セッションでSkypeを使用しているときに、Citrix Workspaceアプリを閉じてセッションに再接続すると、画面がフリーズすることがあります。

24.5.0

新機能

クラウドストアへの接続時のFIDO2を使用した認証のサポート

バージョン24.5.0以降、ユーザーはクラウドストアに接続する際に、FIDO2ベースのパスワードレス認証を使用してCitrix Workspaceアプリに認証できるようになりました。FIDO2はシームレスな認証方法を提供し、企業従業員がユーザー名やパスワードを入力することなく、仮想セッション内のアプリやデスクトップにアクセスできるようにします。この機能は、ローミング認証器（USBのみ）とプラットフォーム認証器（PINコード、Touch ID、Face IDのみ）の両方をサポートしています。この機能はデフォルトで有効になっています。詳細については、「FIDO2を使用したクラウドストア接続時の認証のサポート」を参照してください。

> **注：**
>
> FIDO2認証は、デフォルトでChromeカスタムタブでサポートされています。WebViewでFIDO2認証を使用することに関心がある場合は、<ios_ear_support@cloud.com>までメールでご連絡ください。

ドキュメントスキャナーのサポート

バージョン2405以降、iOS向けCitrix Workspaceアプリはドキュメントスキャナー機能をサポートしています。この機能により、デスクトップセッション内で複数のドキュメントをスキャンして保存できるようになりました。この機能はデフォルトで有効になっています。詳細については、「ドキュメントスキャナーのサポート」を参照してください。

テクニカルプレビュー

- Microsoft Entra IDに参加しているVMのシングルサインオンのサポート
- Citrix Workspaceアプリへのアクセスに生体認証を強制するサポート

テクニカルプレビュー機能の完全なリストについては、「テクニカルプレビューの機能」ページを参照してください。

修正された問題

- 仮想セッションでバーコードスキャナーを使用すると、テキストが正しくスキャンされない場合があります。

24.4.0

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領域に対処しています。

TLS 1.0およびTLS 1.1プロトコルの非推奨に関するお知らせ

Citrixは、今後のリリースでTLS 1.0およびTLS 1.1プロトコルのサポートを非推奨にする予定です。代替プロトコルはTLS 1.2またはTLS 1.3です。詳細については、「非推奨」を参照してください。

修正された問題

- 仮想アプリセッションからデバイスカメラを開くと、iOS向けCitrix Workspaceアプリが予期せず終了する場合があります。

24.3.5

新機能

Twocanoesスマートカードユーティリティリーダーのサポート

バージョン24.3.5以降、iOS向けCitrix WorkspaceアプリはTwocanoesスマートカードユーティリティリーダーをサポートしています。サポートされているスマートカードリーダーと構成の詳細については、「スマートカード」を参照してください。

> **注：**
>
> TwocanoesスマートカードユーティリティUSB-Cリーダーは、Citrix Workspaceアプリのログインと仮想セッションのログインの両方でサポートされています。ただし、TwocanoesスマートカードユーティリティBluetoothリーダーは、Citrix Workspaceアプリのログインのみをサポートしており、仮想セッションのログインはサポートしていません。

UEM を介したデバイス名の構成のサポート

バージョン 24.3.5 以降、iOS 向け Citrix Workspace アプリでは、管理者が Unified Endpoint Management (UEM) を介してユーザーグループに基づいてデバイス名を割り当て、識別できるようになります。詳細については、「UEM を介したデバイス名の構成のサポート」を参照してください。

テクニカルプレビュー

- UEM を介した Citrix Workspace アプリ設定の構成のサポート

このテクニカルプレビューの詳細については、「テクニカルプレビューの機能」を参照してください。

修正された問題

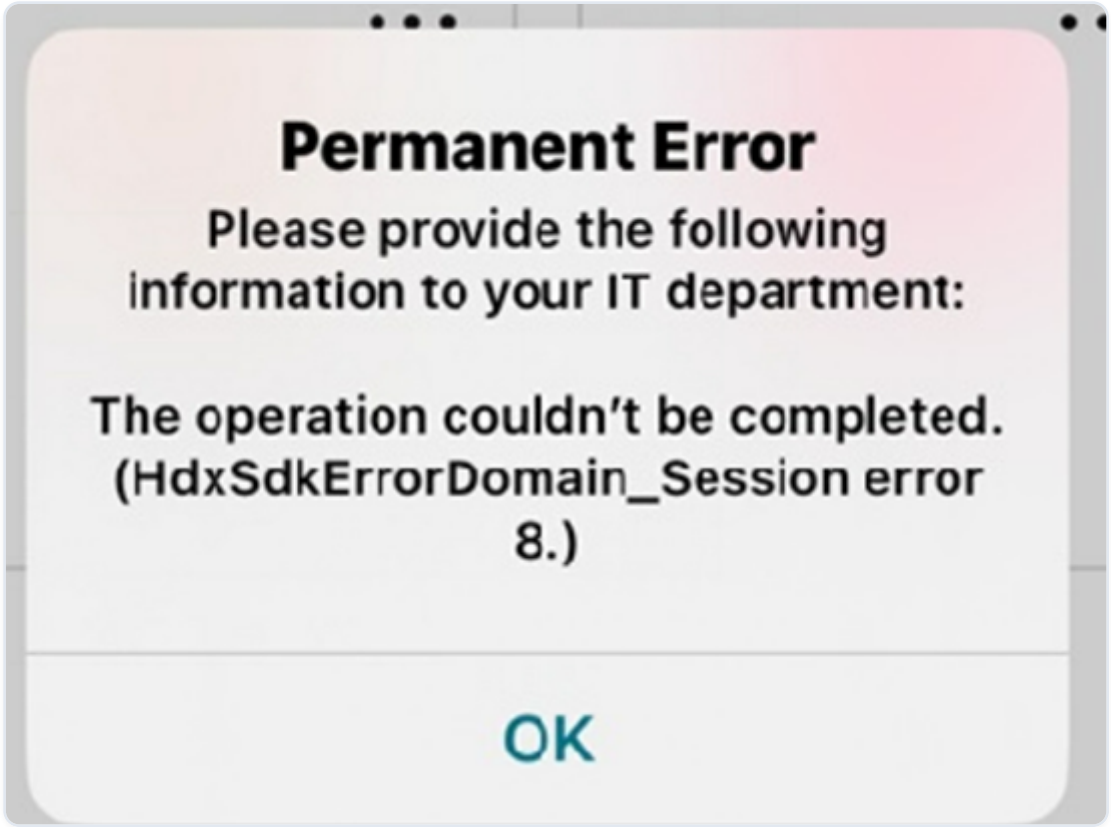
このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

25.7.2 の既知の問題

- iOS デバイスがドックに接続されている場合、セッションの起動が次のエラーで失敗することがあります。

  「永続的なエラーです。以下の情報を IT 部門に提供してください。操作を完了できませんでした。(HdxSdkErrorDomain_session error 8.)」



  この問題は、デバイスがすでにドックに接続されている状態で Citrix Workspace アプリを起動した場合に発生します。回避策として、まず Citrix Workspace アプリを起動し、次にドックを

デバイスに接続してセッションを起動します。修正はリリースバージョン 25.9.0 (10月末予定) で計画されています。

- iOS バージョン 26 はウィンドウモードをサポートしますが、このリリース以降、iOS 向け Citrix Workspace アプリは単一ウィンドウに制限されます。つまり、一度にアクティブにできるセッションは 1 つだけであり、ユーザーが別のウィンドウを開こうとすると、現在アクティブなセッションに切り替わります。
- ロックダウンモードは、以下に示すように、iPad または iPhone で有効にすると、特定の Web ベースの機能を制限します。
  - ロックダウンモードは、リッチメディアコンテンツの表示を簡素化します。
  - 認証フローが制限されたり、ネットワーク操作が制限されたりする場合もあります。

25.5.0 の既知の問題

新しい既知の問題はありません。

25.1.0 の既知の問題

外部モニターで新しいツールバーのノッチをクリックしても、ツールバーメニューが展開されません。

24.12.0 の既知の問題

Fast Smart Card は現在、楕円曲線暗号 (ECC) スマートカードをサポートしていません。

24.9.0 の既知の問題

新しい既知の問題はありません。

24.8.1 の既知の問題

新しい既知の問題はありません。

24.8.0 の既知の問題

新しい既知の問題はありません。

24.7.0 の既知の問題

新しい既知の問題はありません。

24.5.0 の既知の問題

iPad Pro M4 デバイス上の仮想セッションで、Magic Keyboard のトラックパッドが正常に機能しないことに気付くかもしれません。回避策として、仮想セッションで画面を操作するために外部マウス (有線 USB Type-C コネクタまたは Bluetooth) を使用できます。

24.1.0 の既知の問題

Citrix Workspace アプリ for iOS をバージョン 24.1.0 にアップグレードした後、Oracle Java Web Start ソフトウェアに基づくアプリケーションでは、セッション内の仮想キーボードを使用したキーボード入力が失敗する可能性があります。

24.10.0 の既知の問題

新しい既知の問題はありません。

制限事項

- コピーアンドペーストするには、デバイスのソフトキーボードで **Control + C** および **Control + V** キーを使用することをお勧めします。外部キーボードの **Command + C** および **Command + V** キーは機能しない場合があります。
- Safari Web ブラウザを使用している場合、ダウンロードマネージャーで ICA ファイルをタップしてアプリを起動しようとすると失敗します。 Safari からアプリを正常に起動するには、Citrix Workspace アプリまたは Citrix Receiver for iOS の最新バージョン (両方ではなくいずれか一方) がデバイスにインストールされていることを確認してください。
- StoreFrontからCitrix Workspaceに移行した後、Pendoガイドの**次へ**ボタンをタップすると、画面が一時的にちらつきます。
- Citrix Workspaceアプリ内からWebアプリおよびSaaSアプリを起動する際、アプリがGoogle IdPを使用し、ユーザーのサインインを要求する場合、認証は「Access Denied」というエラーメッセージで失敗します。

非推奨

非推奨の項目については、非推奨ページを参照してください。

テクニカルプレビューの機能

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様がフィードバックを共有する機会を提供します。Citrix®はテクニカルプレビューの機能に対するサ

ポートケースを受け付けていませんが、改善のためのフィードバックを歓迎します。Citrixは、フィードバックの重大度、重要度、および優先度に基づいて対応する場合があります。

テクニカルプレビュー機能を試してみたいですか？mailto:citrixappios@citrix.comにメールを送信し、評価したい機能をお知らせください。

テクニカルプレビューの機能一覧

タイトル	提供バージョン
派生資格情報とAppleトークン拡張機能のサポート(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#derived-credentials-and-apple-token-extension-support)	26.7.0
改善されたセッション再接続エクスペリエンス	26.3.0
Microsoft Entra IDに参加しているVMのシングルサインオンのサポート(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#support-for-single-sign-on-for-microsoft-entra-id-joined-vms)	24.5.0
UEMを介したCitrix Workspaceアプリ設定の構成のサポート(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#support-for-configuring-citrix-workspace-app-settings-through-uem)	24.3.5
Unified Endpoint Management (UEM) を使用して複数のストアを追加する(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#add-multiple-stores-using-unified-endpoint-management-uem)	23.9.0
Unified Endpoint Management (UEM) を使用して複数のストアを削除する(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#delete-	23.9.0

タイトル	提供バージョン
multiple-stores-using-unified-endpoint-management-uem)	
強化されたWebストアエクスペリエンス(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#enhanced-web-store-experience)	23.8.0
webおよびSaaSアプリ向けの強化されたシングルサインオン (SSO) エクスペリエンスのサポート(/ja-jp/citrix-workspace-app-for-ios/about-this-release/features-in-technical-preview.html#support-for-an-enhanced-single-sign-on-sso-experience-for-web-and-saas-apps)	23.3.0

派生資格情報とApple Token Extensionのサポート

Citrix Workspaceアプリ for iOS 26.7.0は、アプリとアクティブなHDXセッションの両方でApple Token Extension (CryptoTokenKit) をサポートしています。これにより、デバイス上のサードパーティの派生資格情報アプリケーションが、以下のユースケースにデジタル証明書を提供できるようになります。

- **Citrix GatewayまたはStoreFront認証**: 物理的なスマートカードリーダーなしで、派生証明書を使用してCitrix環境にユーザーを認証します。
- **仮想アプリおよびデスクトップへのログオン**: ユーザープリンシパル名は証明書から読み取られ、起動時にVDAに渡されるため、セッションは再度プロンプトを表示することなくサインオンします。
- **セッション内暗号化リダイレクト**: 資格情報をHDXセッションに拡張することで、仮想化されたアプリ（ブラウザ、メールクライアント、PDF署名ツール、エンタープライズアプリなど）がクライアントトークン拡張機能を通じて暗号化要求を行うことができます。

派生資格情報とは、登録時に既存のPIVまたはCACカードで本人確認を行った後、モバイルデバイスに発行されるクライアント証明書です。これにより、カードリーダーのないデバイスでもスマートカードと同等の保証が提供されます。

改善されたセッション再接続エクスペリエンス

バージョン26.3.0以降、25.11.0リリースで発表された「改善されたセッションタイムアウトエクスペリエンス (テクニカルプレビュー)」機能に以下の機能強化が加えられました。

- セッションタイムアウトの具体的な理由（**デバイスロック、アプリのバックグラウンド化、ネットワークの中断**など）を表示します。
- セッション再接続設定は、GACSで**セッションエクスペリエンス > 接続**にある**手動セッション再接続**オプションを有効にするか、MDMを介して構成できます。

システムおよびインフラストラクチャ要件

コンポーネント	要件
クライアントOS	iOSまたはiPadOS 17.0以降
Citrixクライアント	Citrix Workspaceアプリ for iOS 26.7.0以降
バーチャル デリバリー エージェント	Citrix VDA for Windows、スマートカードリダイレクトポリシーが有効な場合
サードパーティプロバイダー	iOS CryptoTokenKitトークン拡張機能を実装する登録済み資格情報アプリ
インフラストラクチャ	クライアント証明書認証用に構成されたCitrix GatewayまたはStoreFront
証明書	セッションログオンおよびセッション内使用のために、サブジェクト代替名（SAN）にUPNを含める必要があります

この機能は顧客ごとに有効になります。Citrixサポートに連絡して、ストアで有効にしてください。

構成手順

1. 派生資格情報プロバイダーアプリをインストールし、登録を完了します。
2. Citrix Workspaceアプリで、**設定** > **派生資格情報** に移動し、**派生資格情報を使用** を有効にします。
3. ストアを追加します。クライアント証明書認証が構成されている場合、Citrix Workspaceアプリは利用可能な資格情報を提示します。
4. デスクトップまたはアプリを起動し、プロンプトが表示されたら認証します。

管理者は、MDMの高度な設定ポリシーを通じてこの設定をロックできます。

Microsoft Entra IDに参加しているVMのシングルサインオンのサポート

|バージョン24.5.0からのテクニカルプレビュー|有効化フォーム|フィードバックフォーム|

バージョン24.5.0以降、iOS版Citrix Workspaceアプリは、シングルサインオン認証を使用してAzure AD参加済みVMデバイスにサインインするユーザーをサポートします。Azure AD参加済みVMデバイスに初めてサインインする際には、Microsoftの資格情報を提供する必要があります。それ以降のサインインでは、トークンの有効期限が切れるまで資格情報は不要です。

注：

- ユーザーが認証に**WKwebview**を使用しない場合、資格情報は初回に手動で入力する必要があります。
- この機能はクラウドストアにのみ適用されます。

Unified Endpoint Management (UEM) を使用して複数のストアを追加する

23.12.0バージョンからのテクニカルプレビュー|有効化フォーム|フィードバックフォーム|

管理者は、Unified Endpoint Management ソリューションを使用して、管理対象の iOS デバイスに複数のストアを構成および追加できます。各ストアの詳細は XML ファイルに追加できます。この XML ファイルは、アプリ構成ポリシーの構成時にアップロードできます。

注：

XML ファイルはキーと値の形式である必要があります。

構成キー	値のタイプ	説明
URL	文字列	ストアのURL。例: example.cloud.com
storeType (オプション)	整数	**1** に設定すると、ユーザーはネイティブまたはデフォルトのストアの読み込みを表示できます。**2** に設定すると、ユーザーはWebイン

構成キー	値のタイプ	説明
		ターフェイス内でストアを表示できます。
displayName (オプション)	文字列	ストアの名前。
restrict_user_store_modification (オプション)	ブール値	**true**に設定されている場合、ユーザーはストアを変更（追加、削除、編集）できません。**false**に設定されている場合、ユーザーはストアを変更（追加、削除、編集）できます。

重要

- **restrict_user_store_modification**フラグが**true**に設定されている場合、新しいUEM構成ストアを追加する前に、既存のすべてのストアが削除されます。
- storeTypeが指定されていない場合、デフォルトのインターフェイスはネイティブとして扱われます。

ストアを追加するためのXML構成のサンプル

詳細については、このXMLサンプルファイルを参照してください。

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>test.cloud.com</string>
            <key>storeType</key>
```

```
                <integer>1</integer>

                <key>displayName</key>

                <string>Cloud Store </string>

            </dict>

            <dict>

                <key>url</key>

                <string>test.citrix.com</string>

                <key>storeType</key>

                <integer>2</integer>

                <key>displayName</key>

                <string>StoreFront</string>

            </dict>

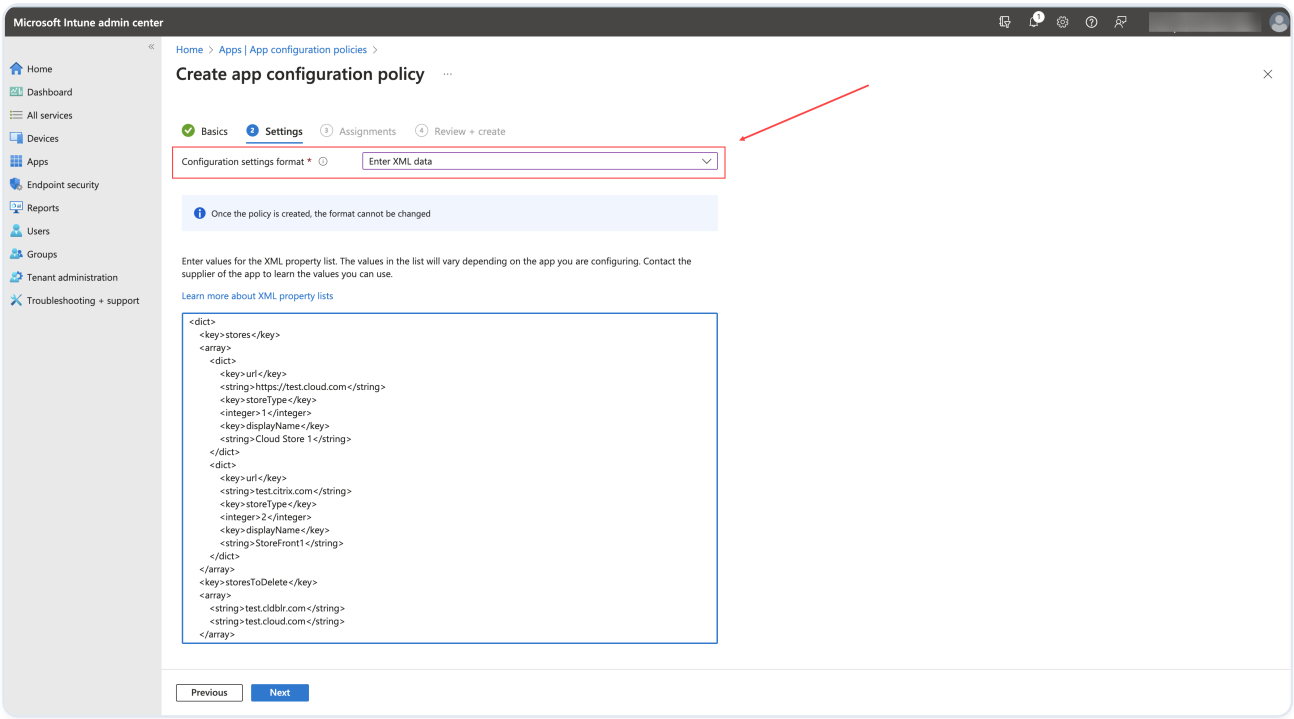
        </array>

            <key>restrict_user_store_modification</key>

        <true/>

    </dict>
```

ストア構成を含むXMLファイルが準備できたら、管理者はそのファイルを**アプリ構成ポリシーの作成**ページにアップロードできます。たとえば、Microsoft Intuneでは、管理者は**構成設定形式**ドロップダウンから**XMLデータの入力**オプションを選択する必要があります。



Unified Endpoint Management (UEM) を使用して複数のストアを削除する

|バージョン23.12.0からのテクニカルプレビュー|有効化フォーム|フィードバックフォーム|

管理者は、1つ以上のストアを削除するために、キー名**storesToDelete**を使用して削除するストアのリストをXMLファイルに追加する必要があります。

ストアを削除するためのXML構成のサンプル

詳細については、このXMLサンプルファイルを参照してください。

```
<dict>
    <key>storesToDelete</key>
<array>
    <string>test.cldblr.com</string>
    <string>test.onprem.com</string>
</array>
</dict>
```

以下は、ストアの追加と削除の構成が含まれているXML構成ファイルのサンプルです。

```
<dict>
<key>stores</key>
<array>
    <dict>
        <key>url</key>
        <string>test.cloud.com</string>
        <key>storeType</key>
        <integer>1</integer>
        <key>displayName</key>
        <string>Cloud Store </string>
    </dict>
    <dict>
        <key>url</key>
        <string>test.citrix.com</string>
        <key>storeType</key>
        <integer>2</integer>
        <key>displayName</key>
        <string>StoreFront</string>
    </dict>
</array>
<key>storesToDelete</key>
<array>
```

```
            <string>test.cldblr.com</string>
            <string>test.onprem.com</string>
        </array>
        <key>restrict_user_store_modification</key>
        <true/>
    </dict>
```

強化されたWebストアエクスペリエンス

|バージョン23.8.0からのテクニカルプレビュー|有効化フォーム|フィードバックフォーム|

エンドユーザーは、サインアウトするかセッションがタイムアウトするまで、Webインターフェイスストアにサインインしたままにできるようになりました。エンドユーザーは、現在のストアからサインアウトせずに設定オプションにアクセスすることもできます。省略記号アイコンをクリックして、次のオプションにアクセスします。

- **設定**: このオプションを使用して、ストアを追加および管理します。
- **サインアウト**: このオプションを使用して、現在のWebインターフェイスストアからサインアウトします。

WebアプリおよびSaaSアプリ向けの強化されたシングルサインオン（SSO）エクスペリエンスのサポート

22.3.5バージョンからのテクニカルプレビュー|有効化フォーム|フィードバックフォーム|

この機能により、サードパーティのIDプロバイダー（IdP）を使用しながら、社内WebアプリおよびSaaSアプリのSSO構成が簡素化されます。強化されたSSOエクスペリエンスにより、プロセス全体が数個のコマンドに短縮されます。SSOをセットアップするために、IdPチェーンでCitrix Secure Private Access™を構成するという必須の前提条件が不要になります。また、Workspaceアプリと起動される特定のWebアプリまたはSaaSアプリの両方で認証に同じIdPが使用されている場合、ユーザーエクスペリエンスも向上します。

テクニカルプレビューから一般提供 (GA) へ

サービスまたは機能	一般提供バージョン
Citrix Workspaceアプリへのアクセスに生体認証を強制するサポート	24.9.0
高速スキャンをサポート	24.9.0
アプリ保護のサポート	24.9.0
オンプレミスストアに接続する際のFIDO2を使用した認証のサポート	24.9.0
複数のオーディオデバイスのサポート	24.9.0
アダプティブオーディオのサポート	24.5.0
アクセシビリティとVoiceOverのサポート	24.9.0
外部Webカメラのサポート	24.9.0
UEMを介したCitrix Workspaceアプリ設定の構成のサポート(/ja-jp/citrix-workspace-app-for-ios/configure/configure-workspace-app.html#support-for-configuring-citrix-workspace-app-settings-through-uem)	24.7.0
ドキュメントスキャナーのサポート(/ja-jp/citrix-workspace-app-for-ios/configure/peripheral-devices.html#support-for-document-scanner)	24.5.0
FIDO2ベースの認証のサポート(/ja-jp/citrix-workspace-app-for-ios/authenticate.html#support-for-fido2-based-authentication-when-connecting-to-hdx-session)	23.9.0
Appleのネイティブ非ミラーモードのサポート(/ja-jp/citrix-workspace-app-for-ios/session-experience.html#support-for-apples-native-non-mirror-mode)	23.3.0

システム要件と互換性

カスタマーサポートを利用するには、Citrix Workspace™ app for iOS を Apple Store で入手可能な最新バージョンにアップデートする必要があります。

サポートされているオペレーティングシステム

Citrix Workspace app for iOS は、以下のオペレーティングシステムをサポートしています。

- iOS 26 および iPadOS 26。
- iOS 18 および iPadOS 18。
- iOS 17 および iPadOS 17。

Citrix® は、常に最新の iOS オペレーティングシステムと、その前の2つのバージョン (N、N-1、N-2) のみをサポートしています。

サーバー要件

サーバーに最新のホットフィックスがすべてインストールされていることを確認してください。

- 仮想デスクトップおよびアプリへの接続の場合、Citrix Workspace app は Citrix StoreFront および Web Interface をサポートしています。

  StoreFront:

  - StoreFront 3.6 以降 (推奨)。Citrix Workspace app は StoreFront の最新バージョンで検証済みです。以前にサポートされていたバージョンには、StoreFront 2.6 以降が含まれます。

    StoreFront ストアへの直接アクセスを提供します。Citrix Workspace app は、以前のバージョンの StoreFront もサポートしています。

    > **注：**
    >
    > XenApp および XenDesktop 7.8 では、Citrix は Framehawk 仮想チャネルと 3D Pro のサポートを導入しました。この機能は Citrix Workspace app にも拡張されました。

- Web サイト用の Workspace で構成された StoreFront。

  Safari Web ブラウザーから StoreFront ストアへのアクセスを提供します。ユーザーはブラウザーを使用して ICA ファイルを手動で開く必要があります。この展開の制限事項については、StoreFront ドキュメントを参照してください。

Webインターフェース:

- Web Interface 5.4 (Web Interface サイトを含む)
- Web Interface 5.4 と XenApp および XenDesktop サイト
- Citrix Gateway 上の Web Interface (Safari を使用したブラウザベースのアクセスのみ)

  Citrix Gateway が提供する書き換えポリシーを有効にします。

- **Citrix Virtual Apps and Desktops™**、**XenApp**、および **XenDesktop** (以下のいずれかの製品):
  - Citrix Virtual Apps and Desktops 7 1808 以降
  - Citrix XenDesktop 7.x 以降
  - Citrix XenApp 7.5 以降

接続、証明書、および認証

StoreFront への接続の場合、Citrix Workspace アプリは以下の認証方法をサポートしています。

	ブラウザを使用した WORKSPACE FOR WEB	STOREFRONT SERVICES サイト (ネイティブ)	STOREFRONT XENAPP および XENDESKTOP サイト (ネイティブ)	CITRIX GATEWAY から WORKSPACE FOR WEB (ブラウザ)	CITRIX GATEWAY から STOREFRONT SERVICES サイト (ネイティブ)
匿名	はい	はい			
ドメイン	はい	はい	はい	はい*	はい*
ドメインパススルー	はい	はい	はい		

	ブラウザを使用した WORKSPACE FOR WEB	STOREFRONT SERVICES サイト (ネイティブ)	STOREFRONT XENAPP および XENDESKTOP サイト (ネイティブ)	CITRIX GATEWAY から WORKSPACE FOR WEB (ブラウザ)	CITRIX GATEWAY から STOREFRONT SERVICES サイト (ネイティブ)
セキュリティトークン				はい*	はい*
2要素認証 (セキュリティトークン付きドメイン)				はい*	はい*
SMS				はい*	いいえ
スマートカード		はい		はい*	はい*
ユーザー証明書				はい (Citrix Gatewayプラグイン)	はい (Citrix Gatewayプラグイン)

*以下の場合にのみ利用可能:

- Webサイト用ワークスペース。
- Citrix Gateway を含む展開で、関連するプラグインをデバイスにインストールしているか否かに関わらず.

Web Interface 5.4 への接続の場合、Citrix Workspace アプリは、以下の認証方法をサポートしています。

> **注：**

> Web Interface では、ドメインおよびセキュリティトークン認証を表すために「明示的」という用語を使用します。

	WEB INTERFACE (ブラウザー)	WEB INTERFACE XENAPP および XENDESKTOP ® サイト	CITRIX GATEWAY から WEB INTERFACE (ブラウザー)	CITRIX GATEWAY から WEB INTERFACE XENAPP および XENDESKTOP サイト
匿名	はい			
ドメイン	はい	はい	はい*	
ドメインパススルー	はい			
セキュリティトークン			はい*	
2要素認証 (セキュリティトークン付きドメイン)			はい*	
SMS			はい*	
スマートカード				
ユーザー証明書			はい (Citrix Gateway プラグインが必要)	

証明書

プライベート (自己署名) 証明書

Citrix Workspaceアプリを使用して、Citrixリソースに正常にアクセスできます。

- リモートゲートウェイにプライベート証明書がインストールされている場合。
- 組織の証明機関のルート証明書がデバイスにインストールされている場合。

> **注：**
>
> 接続時にリモートゲートウェイの証明書を検証できない場合、信頼されていない証明書の警告が表示されます。この問題は、ルート証明書がローカルキーストアに含まれていないために発生します。ユーザーが警告を無視して続行することを選択した場合、アプリケーションのリストが表示されますが、アプリケーションは起動に失敗します。

手動でインストールされた証明書

iOS 10.3以降では、手動でインストールしたプロファイルに含まれる証明書は、SSLに対して自動的に信頼されません。iOSで手動でインストールされた証明書プロファイルを信頼するには：

1. デバイスに証明書プロファイルがインストールされていることを確認してください。
2. **設定** > **一般** > **情報** > **証明書信頼設定** に移動します。

   プロファイルを通じてインストールされた各ルートは、**ルート証明書の完全な信頼を有効にする** の下に表示されます。
3. 各ルートの信頼をオンまたはオフに切り替えることができます。

iPadおよびiPhoneデバイスでルート証明書をインポートする

証明書発行者のルート証明書を取得し、デバイスに設定されているメールアカウントにメールで送信します。添付ファイルをクリックすると、ルート証明書のインポートを求められます。

ワイルドカード証明書

ワイルドカード証明書は、同じドメイン内の任意のサーバーに対して個々のサーバー証明書の代わりに使用されます。Citrix Workspaceアプリはワイルドカード証明書をサポートしています。

中間証明書とCitrix Gateway

証明書チェーンに中間証明書が含まれている場合、中間証明書はCitrix Gateway（またはAccess Gateway）サーバー証明書に追加する必要があります。また、Access Gatewayのインストールについては、Citrix ADCドキュメントで要件に一致する証明書のインストール、リンク、および更新を参照してください。

RSA SecurID 認証は、Secure Gateway 構成 (Web Interface 経由のみ) およびサポートされているすべての Access Gateway 構成でサポートされています。

Citrix Workspace アプリは、Access Gateway がサポートするすべての認証方法をサポートしています。

統合サーバー証明書検証ポリシー

Citrix Workspace アプリのリリースでは、サーバー証明書に対してより厳格な検証ポリシーが適用されます。

重要

Citrix Workspace アプリをインストールする前に、サーバーまたはゲートウェイの証明書がここに記載されているとおりに正しく構成されていることを確認してください。次の場合、接続が失敗する可能性があります。

- サーバーまたはゲートウェイの構成に誤ったルート証明書が含まれている場合
- サーバーまたはゲートウェイの構成にすべての中間証明書が含まれていない場合
- サーバーまたはゲートウェイの構成に、期限切れまたはその他の無効な中間証明書が含まれている場合
- サーバーまたはゲートウェイの構成に、クロス署名された中間証明書が含まれている場合

サーバー証明書を検証する際、Citrix Workspace アプリは、サーバー証明書の検証時にサーバー（またはゲートウェイ）から提供される**すべて**の証明書を使用するようになりました。以前のリリースと同様に、Citrix Workspace アプリは、証明書が信頼されているかどうかも確認します。証明書が信頼されていない場合、接続は失敗します。

このポリシーは、Webブラウザーの証明書ポリシーよりも厳格です。多くのWebブラウザーは、信頼する多数のルート証明書を含んでいます。

サーバー（またはゲートウェイ）は、正しい証明書のセットで構成されている必要があります。誤った証明書のセットは、Citrix Workspace アプリの接続を失敗させる可能性があります。

ゲートウェイがこれらの有効な証明書で構成されているとします。この構成は、Citrix Workspace アプリがどのルート証明書を使用するかを正確に判断することで、より厳格な検証を必要とするお客様に推奨されます。

- サーバー証明書の例
- 中間証明書の例
- 例のルート証明書

その後、Citrix Workspace アプリはこれらの証明書がすべて有効であるかを確認します。Citrix Workspace アプリは、**Example Root Certificate** がすでに信頼されているかどうかも検証します。

> **注記:**
>
> - Citrix Workspace アプリが **Example Root Certificate** を信頼しない場合、接続は失敗します。
> - 一部の認証局は複数のルート証明書を持っています。より厳格な検証が必要な場合は、構成が適切なルート証明書を使用していることを確認してください。

> 例えば、現在2つの証明書があります。

- DigiCert または GTE CyberTrust Global Root
- DigiCert Baltimore ルート または Baltimore CyberTrust ルート

これらの証明書は、同じサーバー証明書を検証できます。一部のユーザーデバイスでは両方のルート証明書が利用可能ですが、他のデバイスではいずれか一方のみが利用可能です（**DigiCert Baltimore Root** または **Baltimore CyberTrust Root**）。

ゲートウェイで**GTE CyberTrust Global Root**を構成すると、それらのユーザーデバイスでのCitrix Workspaceアプリの接続は失敗します。どのルート証明書を使用する必要があるかを判断するには、認証局のドキュメントを参照してください。また、すべての証明書と同様に、ルート証明書も最終的には期限切れになることに注意してください。

すると、Citrix Workspaceアプリはこれら2つの証明書を使用します。アプリはユーザーデバイス上でルート証明書を検索します。アプリが正しく検証され、かつ信頼されている証明書（**Example Root Certificate**など）を見つけた場合、接続は成功します。そうでない場合、接続は失敗します。

この構成により、Citrix Workspaceアプリが必要とする中間証明書が提供されますが、Citrix Workspaceアプリが有効で信頼された任意のルート証明書を選択することも可能になります。

ここで、ゲートウェイが次の証明書で構成されていると仮定します。

- サーバー証明書の例
- 中間証明書の例
- 誤ったルート証明書

Webブラウザーは誤ったルート証明書を無視する可能性があります。しかし、Citrix Workspaceアプリは誤ったルート証明書を無視しないため、接続は失敗します。

一部の認証局は複数の中間証明書を使用します。この場合、ゲートウェイは通常、すべての中間証明書（ただしルート証明書は除く）で構成されます。例：

- サーバー証明書の例
- 例の中間証明書 1
- 中間証明書2の例

重要

一部の認証局は、クロス署名された中間証明書を使用します。このような証明書は、複数のルート証明書があり、以前のルート証明書がより新しいルート証明書と同時にまだ使用されている状況を想定しています。そのような場合、少なくとも2つの中間証明書が存在します。

例えば、以前のルート証明書 **Class 3 Public Primary Certification Authority** には、対応するクロス署名された中間証明書 **Verisign Class 3 Public Primary Certification Authority - G5** があります。しかし、**Class 3 Public Primary Certification Authority** を置き換える、対応する新しいルート証明書 **Verisign Class 3 Public Primary Certification Authority - G5** も利用可能です。この新しいルート証明書は、クロス署名された中間証明書を使用しません。

注：

クロス署名された中間証明書とルート証明書は同じSubject name（Issued To）を持ちますが、クロス署名された中間証明書は異なるIssuer name（Issued By）を持ちます。Issuer nameは、クロス署名された中間証明書を通常の一般的な中間証明書（**Example Intermediate Certificate 2**など）と区別します。

ルート証明書とクロス署名された中間証明書を省略するこの構成が、通常推奨されます。

- サーバー証明書の例
- 中間証明書の例

Citrix Workspaceアプリが以前のルート証明書を選択するため、ゲートウェイをクロス署名された中間証明書を使用するように構成することは避けてください。

- サーバー証明書の例
- 中間証明書の例
- クロス署名された中間証明書の例 \[非推奨\]

ゲートウェイをサーバー証明書のみで構成することは推奨されません。

- サーバー証明書の例

そのような場合、Citrix Workspaceアプリがすべての中間証明書を見つけられない場合、接続は失敗します。

Microsoft Entra SSOのシステム要件

Microsoft Entra SSOを使用するためのシステム要件は次のとおりです。

- コントロールプレーン: Citrix DaaS
  - Citrix Cloud Commercial (米国、EU、およびAPS)
  - Citrix クラウド ジャパン
- ユーザーポータル: Citrix Workspace
- 仮想配信エージェント (VDA)
  - Windows: バージョン2507以降
- シトリックス ワークスペース アプリ
  - iOS: バージョン 2511 以降
- セッションホストOS:
  - Windows 11 バージョン 24H2、2025年9月 Windows 11 用累積更新プログラム (KB5065789) 以降がインストールされていること (ビルド 26100.6725)

考慮事項

- Microsoft Entraシングルサインオンは、Citrix Workspaceアプリを介してCitrix Workspaceにアクセスする場合にのみサポートされます。ユーザーがWebブラウザを介してCitrix Workspaceにアクセスする場合、シングルサインオンは機能しません。

- Microsoft Entra シングルサインオンを使用してセッションにログオンする場合、自動クライアント再接続はサポートされていません。このログオン方法が使用されると、この機能は自動的に無効になります。ネットワーク障害が発生した場合でも、セッションの信頼性は自動再接続に利用できます。
- 仮想デスクトップがロックされている場合、デフォルトの動作はWindowsロック画面を表示することです。認証要件によっては、セッションロックの動作を変更する必要がある場合があります。詳細については、「セッションロックの動作」を参照してください。

インストールとアップグレード

Citrix Workspaceアプリの最新バージョンをApple Storeからダウンロードまたはアップグレードできます。

- 初めてのユーザーは、Apple StoreからCitrix Workspaceアプリをダウンロードし、デバイスにインストールできます。
- 既存のユーザーは、Apple StoreからCitrix Workspaceアプリの最新バージョンにアップグレードできます。

Citrix Workspaceアプリの構成については、構成セクションを参照してください。

iOS向けCitrix Workspaceアプリで利用可能な機能については、Citrix Workspaceアプリの機能マトリックスを参照してください。

はじめに

セットアップ

Citrix Workspaceアプリ for iOSは、Citrix Virtual Apps展開環境向けのWeb Interfaceの構成をサポートしています。Web Interfaceサイトには2種類あります。

- XenAppおよびXenDesktop®サイト
- シトリックス Virtual Apps and Desktops™ および シトリックス DaaS（旧シトリックス Virtual Apps and Desktopsサービス）サイト。

Web Interfaceサイトを使用すると、クライアントデバイスをサーバーファームに接続できます。Citrix Workspaceアプリ for iOSとWeb Interfaceサイト間の認証は、Citrix Secure Web Gatewayを含むさまざまなソリューションを使用して処理できます。

また、StoreFrontを構成して、Citrix Workspaceアプリの認証およびリソース配信サービスを提供することもできます。この構成により、デスクトップ、アプリケーション、およびその他のリソースをユーザーに配信するための一元化されたエンタープライズストアを作成できます。

接続の構成に関する詳細情報（ビデオ、ブログ、サポートフォーラムを含む）については、`<http://community.citrix.com>`を参照してください。

ユーザーがCitrix Virtual Apps and DesktopsおよびCitrix DaaS展開環境でホストされているアプリケーションにアクセスする前に、ここに記載されているように、展開環境で次のコンポーネントを構成してください。

- ファームまたはサイトでアプリケーションを公開する際は、StoreFrontストアを介してそれらのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションを検討してください。
    - 公開アプリケーションには意味のある説明を含めるようにしてください。これらの説明はCitrix Workspaceアプリでユーザーに表示されるためです。
    - モバイルデバイスユーザー向けに、公開アプリケーションを強調表示できます。アプリケーションを「おすすめ」リストに表示できます。Citrix Workspaceアプリでこのリストに表示するには、サーバーで公開されているアプリケーションのプロパティを編集します。**

［アプリケーションの説明］**フィールドの値に「KEYWORDS: Featured」という文字列を追加できるようになりました。

- 画面サイズに合わせるモードでは、アプリケーションがモバイルデバイスの画面サイズに合わせて調整されます。このモードを有効にするには、サーバーで公開されているアプリケーションのプロパティを編集し、［アプリケーションの説明］フィールドの値に「KEYWORDS: mobile」という文字列を追加します。このキーワードは、アプリケーションの自動スクロール機能もアクティブにします。
- ストアのすべてのユーザーをアプリケーションに自動的にサブスクライブするには、Citrix Virtual Appsでアプリケーションを公開するときに、説明に「KEYWORDS: Auto」という文字列を追加します。ユーザーがストアにログオンすると、ユーザーが手動でアプリケーションをサブスクライブする必要なく、アプリケーションが自動的にプロビジョニングされます。

- Citrix Virtual Apps and DesktopsおよびCitrix DaaS™展開環境のWeb Interfaceにサイトがない場合は、サイトを作成します。サイトの名前と作成方法は、インストールされているWeb Interfaceのバージョンによって異なります。

手動セットアップ

一般的に、Citrix WorkspaceアプリがCitrix Gatewayに接続すると、認証後にXenAppおよびXenDesktopサイトまたはCitrix Virtual Apps Webサイトを検索しようとします。サイトが検出されない場合、Citrix Workspaceアプリ for iOSはエラーを表示します。この状況を回避するには、Citrix Workspaceアプリ for iOSがCitrix Gatewayに接続できるように、アカウントを手動で構成できます。

1. **アカウント**アイコン > **アカウント画面** > **プラス記号（+）**をタップします。新しいアカウント画面が表示されます。
2. 画面の右上隅で、**オプション**の左側にあるアイコンをタップし、**手動セットアップ**をタップします。他のフィールドが画面に表示されます。
3. **アドレス**フィールドに、サイトまたはCitrix GatewayのセキュアなURLを入力します（例：`agee.mycompany.com`）。
4. 次の接続オプションのいずれかを選択します。画面上の他のフィールドは、選択内容に応じて変化します。

   - **Webインターフェイス** - Citrix WorkspaceアプリがWebブラウザと同様にCitrix Virtual Apps Webサイトを表示するように選択します。このUIはWebビューとも呼ばれます。

- **XenAppサービス** - Citrix Gatewayを介した認証が構成されていない特定のXenAppおよびXenDesktopサイトをCitrix Workspaceアプリ for iOSが検索するように選択します。この画面に表示される追加オプションで、サイトのログオン資格情報を入力します。
  - \<StoreFront FQDN\>: 多数のストアがある場合、リストが表示され、ユーザーは追加するストアを選択できます。
  - \<StoreFront FQDN\>/citrix/\<Store Name\>: このオプションは、StoreFrontストア\<Store Name\>を追加します。
  - \<StoreFront FQDN\>/citrix/PnAgent/config.xml: このオプションは、デフォルトのレガシーPNAgentストアを追加します。
  - \<StoreFront FQDN\>/citrix/\<Store Name\>/PnAgent/config.xml: このオプションは、\<Store Name\>に関連付けられたレガシーPNAgentストアを追加します。
- Citrix Gateway - Citrix Workspaceアプリ for iOSが特定のCitrix Gatewayを介してXenAppおよびXenDesktopサイトに接続するように選択します。この画面の追加オプションで、サーバーエディションとそのログオン資格情報（認証にセキュリティトークンが必要かどうかを含む）を選択します。

5. 証明書のセキュリティについては、「証明書の警告を無視」フィールドの設定を使用して、無効な、自己署名された、または期限切れの証明書を持つサーバーであっても接続するかどうかを決定します。デフォルト設定はオフです。 重要：このオプションを有効にする場合は、正しいサーバーに接続していることを確認してください。Citrix®は、オンラインセキュリティ攻撃からユーザーデバイスを保護するために、すべてのサーバーが有効な証明書を持つことを強く推奨します。セキュアなサーバーは、認証局から発行されたSSL証明書を使用します。Citrixは自己署名証明書をサポートしておらず、証明書のセキュリティをバイパスすることを推奨しません。
6. 保存をタップします。
7. ユーザー名とパスワード（または、2要素認証を選択した場合はトークン）を入力し、「ログオン」をタップします。Citrix Workspaceアプリ for iOS画面が表示され、デスクトップにアクセスしたり、アプリを追加して開いたりできます。

StoreFront

> **重要:**

- StoreFrontを使用する場合、iOS向けCitrix Workspaceアプリは、Citrix Access Gateway Enterprise Editionバージョン9.3以降、およびCitrix Gatewayバージョン13までをサポートします。
- iOS向けCitrix Workspaceアプリは、Web Interface上のXenAppおよびXenDesktopサイトのみをサポートします。
- iOS向けCitrix Workspaceアプリは、Webブラウザ がWorkspace for Webで動作する限り、Workspace for Webからのセッション起動をサポートします。起動しない場合は、iOS向けCitrix Workspaceアプリから直接アカウントを設定してください。ユーザーは、ブラウザの「Open in Workspace」機能を使用してICAファイルを手動で開く必要があります。この展開の制限事項については、StoreFrontのドキュメントを参照してください。

StoreFrontを使用すると、作成するストアは、iOS向けCitrix Workspaceアプリの認証およびリソース配信インフラストラクチャを提供するサービスで構成されます。以下のデスクトップおよびアプリケーションをカウントおよび集計するストアを作成します。

- シトリックス バーチャルアプリおよびデスクトップ および シトリックス DaaS サイト
- Citrix Virtual Appsファーム

1. StoreFrontをインストールして構成します。詳細については、StoreFront製品ドキュメントを参照してください。より詳細な制御が必要な管理者向けに、CitrixはiOS向けCitrix Workspaceアプリのダウンロードサイトを作成するために使用できるテンプレートを提供しています。
2. 他のCitrix Virtual Apps and DesktopsおよびCitrix DaaSアプリケーションと同様に、StoreFrontのストアを構成します。モバイルデバイスに特別な構成は必要ありません。詳細については、製品ドキュメントのStoreFrontセクションにある「ユーザーアクセスオプション」を参照してください。モバイルデバイスの場合は、次のいずれかの方法を使用します。
    - プロビジョニングファイル。ユーザーに、ストアの接続詳細を含むプロビジョニングファイル（.cr）を提供できます。インストール後、ユーザーはデバイスでファイルを開き、iOS向けCitrix Workspaceアプリを自動的に構成します。デフォルトでは、Workspace for websitesは、サイトが構成されている単一のストアのプロビジョニングファイルをユーザーに提供します。または、Citrix StoreFront管理コンソールを使用して、単一または複数のストアのプロビジョニングファイルを生成し、手動でユーザーに配布することもできます。
    - 手動構成。ユーザーにCitrix GatewayまたはストアのURLを直接通知して、デスクトップおよびアプリケーションにアクセスさせることができます。Citrix Gatewayを介した接続の場合、ユーザーは製品エディションと必要な認証方法も知っている必要があります。インス

トール後、ユーザーはこれらの詳細をCitrix Workspaceアプリに入力します。アプリは接続の検証を試み、成功した場合はユーザーにサインインを促します。

- 自動構成。ようこそ画面で**［アカウントの追加］**をタップし、アドレスフィールドにStoreFrontサーバーのURLを入力します。アカウントの追加中に、アカウントの構成が自動的に行われます。

Citrix Gatewayを構成するには

内部ネットワークの外部から接続するユーザーがいる場合は、Citrix Gatewayを介した認証を構成します。たとえば、リモートロケーションからインターネットを使用して接続するユーザーなどです。

- StoreFrontを使用する場合、iOS向けCitrix Workspaceアプリは、Citrix Access Gateway Enterprise Editionバージョン9.3以降、およびCitrix Gatewayバージョン13までをサポートします。

ウェブインターフェース

Web Interfaceサイトを構成するには、iPhoneおよびiPadデバイスのユーザーは、Web Interfaceサイトとモバイルデバイスに組み込まれているSafariブラウザを介してアプリケーションを起動できます。Web Interfaceサイトは、他のCitrix Virtual Appsアプリケーションの場合と同様に構成します。モバイルデバイス用にXenAppおよびXenDesktopサイトが構成されていない場合、Citrix Workspaceアプリ for iOSは自動的にWeb Interfaceサイトを使用します。モバイルデバイスに特別な構成は必要ありません。

組み込みのSafariブラウザはWeb Interface 5.xをサポートしています。

iOSデバイスでアプリケーションを起動するには

モバイルデバイスでは、ユーザーは通常のログオンとパスワードを使用してWeb Interfaceサイトにログオンできます。

モバイルデバイスの自動プロビジョニング

StoreFrontで、**複数ストアのプロビジョニングファイルのエクスポート**および**プロビジョニングファイルのエクスポート**タスクを使用して、ストア用に構成されたCitrix Gateway展開やビーコンを含む、ストアの接続詳細を含むファイルを生成します。これらのファイルをユーザーが利用できるようにして、Citrix Workspaceアプリ for iOSをストアの詳細で自動的に構成できるようにしま

す。ユーザーは、WebサイトWorkspaceからCitrix Workspaceアプリ for iOSのプロビジョニングファイルを取得することもできます。

> **重要:**
>
> 多くのサーバー展開では、サーバーグループの構成を変更するために一度に1つのサーバーのみを使用します。展開内の他のどのサーバーでもCitrix StoreFront管理コンソールが実行されていないことを確認します。完了したら、構成変更をサーバーグループに伝播して、展開内の他のサーバーが更新されるようにします。

1. Windowsのスタート画面またはアプリ画面で、Citrix StoreFrontタイルを見つけてクリックします。Citrix StoreFront管理コンソールの左ペインで、ノードを選択します。
2. 複数のストアの詳細を含むプロビジョニングファイルを生成するには、ペインでをクリックし、ファイルに含めるストアを選択します。
3. をクリックし、プロビジョニングファイルを`.cr`拡張子でネットワーク上の適切な場所に保存します。

ユーザーアクセス情報

ユーザーがホストされているアプリケーション、デスクトップ、およびデータにアクセスするために必要なCitrix Workspaceアプリ for iOSのアカウント情報をユーザーに提供する必要があります。この情報は、次の方法で提供できます。

- メールベースのアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- ユーザーに手動で入力するアカウント情報を提供する

メールベースのアカウント検出を構成する

Citrix Workspaceアプリ for iOS をメールベースのアカウント検出を使用するように構成できます。構成すると、ユーザーはCitrix Workspaceアプリ for iOS の初回インストールおよび構成時に、サーバーURLではなくメールアドレスを入力します。Citrix Workspaceアプリは、ドメインネームシステム (DNS) サービス (SRV) レコードに基づいてメールアドレスに関連付けられているAccess GatewayまたはStoreFrontサーバー、あるいはEndpoint Management仮想アプライアンスを特定し、ホストされているアプリケーション、デスクトップ、データにアクセスするためにログオンするようユーザーに促します。

> **注：**
>
> Citrix Workspaceアプリ for iOS がWeb Interface展開に接続している場合、メールベースのアカウント検出はサポートされません。

メールベースの検出を有効にするためにDNSサービスロケーション (SRV) レコードを追加する

初回構成時に、Citrix WorkspaceアプリはActive Directoryドメインネームシステム (DNS) サーバーに接続して、ユーザーが利用できるストアの詳細を取得できます。これにより、ユーザーはCitrix Workspaceアプリ for iOS をインストールおよび構成する際に、ストアのアクセス詳細を知る必要がなくなります。代わりに、ユーザーはメールアドレスを入力し、Citrix WorkspaceアプリがDNSサーバーに接続します。メールアドレスからドメインの詳細を収集できます。

Citrix Workspaceアプリがユーザーのメールアドレスに基づいて利用可能なストアを特定できるようにするには、次の手順を実行します。

- Access Gatewayのサービスロケーション (SRV) ロケーターリソースレコードを構成します。
- DNSサーバーでStoreFrontまたはAppControllerの接続を構成します。

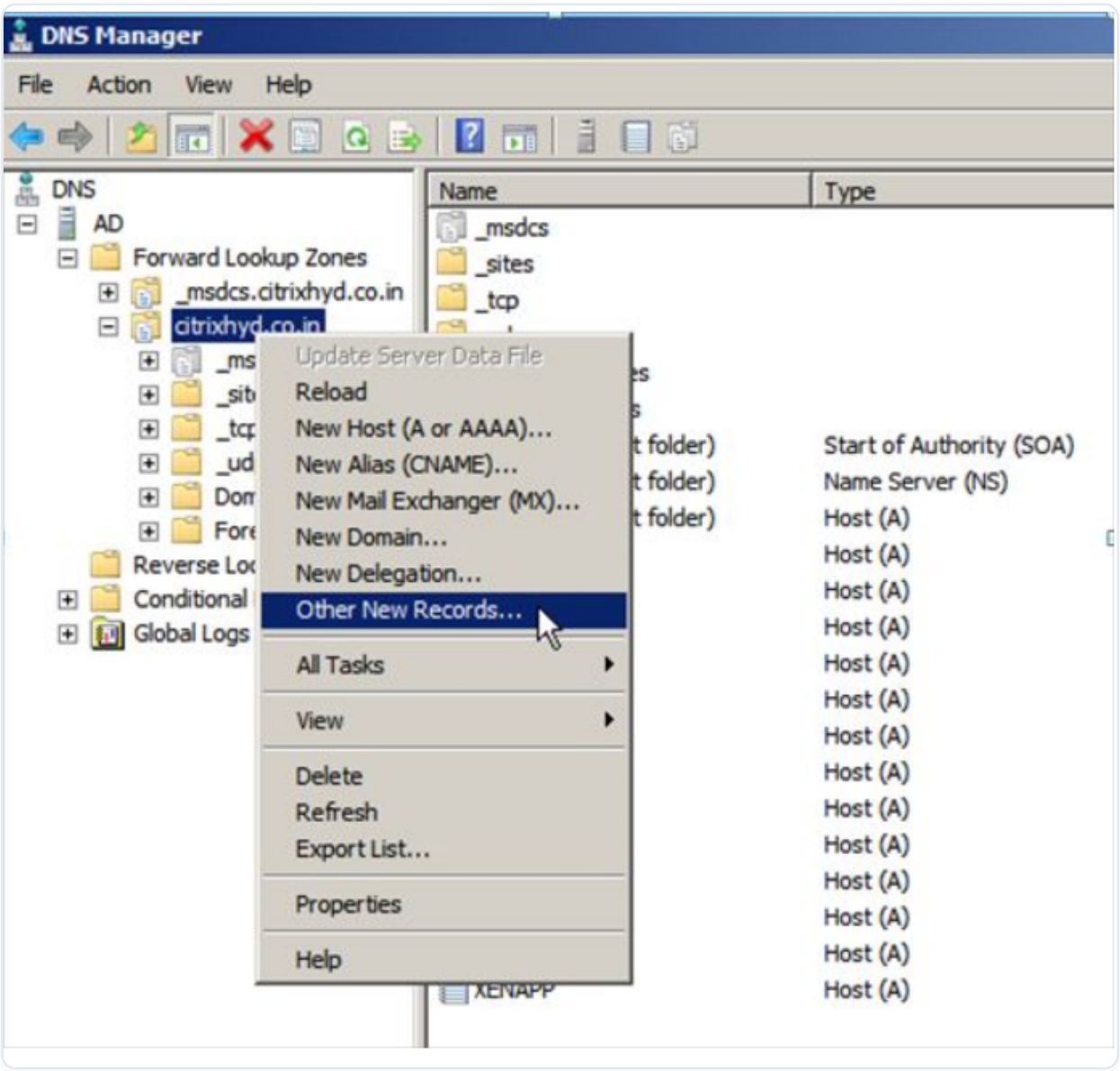
メールベースのアカウント検出を有効にするには、Access GatewayアプライアンスおよびStoreFrontまたはAppControllerサーバーに有効なサーバー証明書をインストールする必要があります。ルート証明書への完全なチェーンも有効である必要があります。最高のユーザーエクスペリエンスのために、次のいずれかの証明書をインストールしてください。

- サブジェクト
- *discoverReceiver.domain* のサブジェクトの別名エントリ。
- ユーザーのメールアカウントを含むドメインのワイルドカード証明書。

ユーザーがメールアドレスを使用してCitrix Workspaceアプリ for iOS を構成できるようにするには、次のようにDNSゾーンにSRVレコードを追加します。

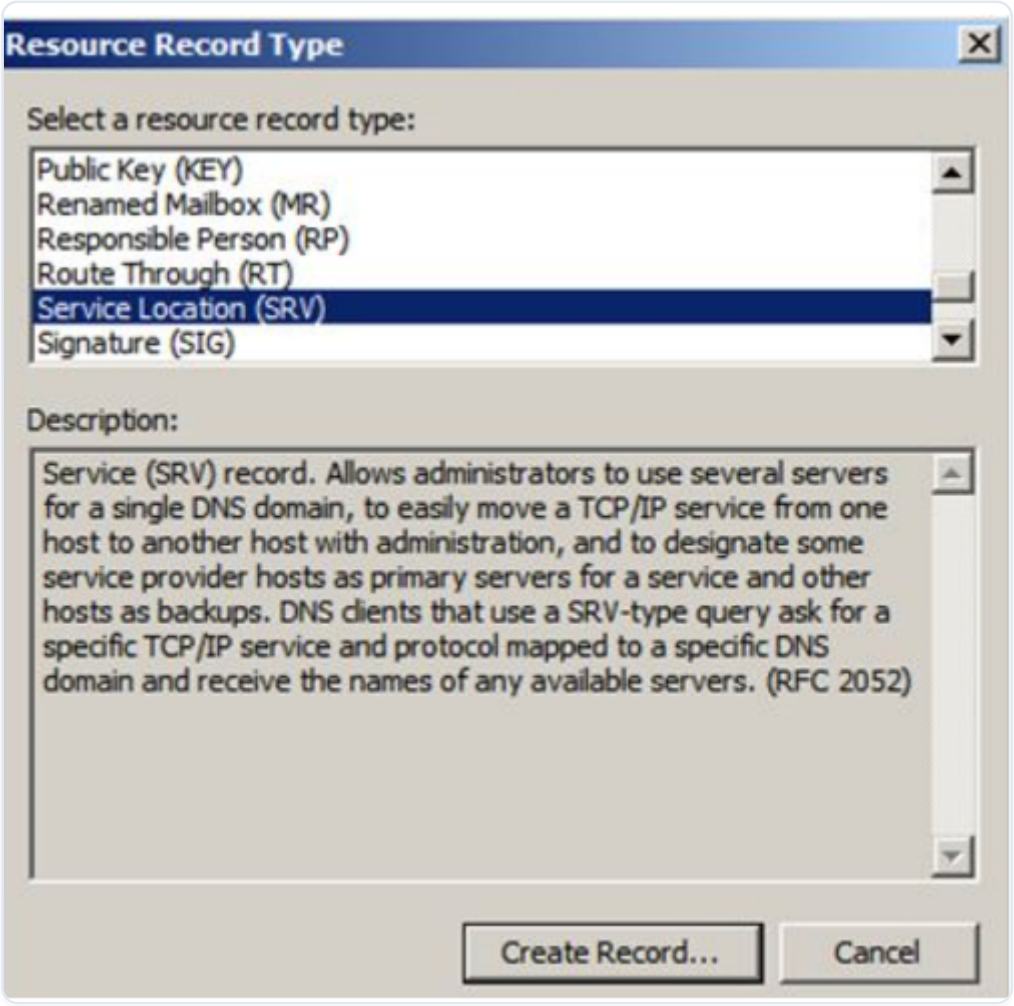
1. DNSサーバーにログオンします。
2. DNSで、前方参照ゾーンを右クリックします。

3. **その他の新しいレコード** をクリックします。



4. 「**リソースレコードの種類**」ダイアログボックスが表示されます。
5. 「**リソースレコードの種類を選択してください**」で、「**サービスロケーション (SRV)**」を選択します。

6. 「**レコードの作成**」を選択します。



7. 「プロパティ」ダイアログボックスが表示されます。
8. 「**サービスロケーション**」タブを選択します。
9. 「**サービス**」で、ホスト値 _citrixreceiver を入力します。
10. 「**プロトコル**」で、値 _tcp を入力します。
11. 「**このサービスを提供するホスト**」で、Access Gatewayアプライアンスの完全修飾ドメイン名 (FQDN) とポート (ローカルユーザーとリモートユーザーの両方をサポートするため)、またはStoreFrontまたはAppControllerサーバー (ローカルネットワーク上のユーザーのみをサポートするため) を指定します。
12. OKをクリックします。

注：

StoreFrontのFQDNは、Access Gateway仮想サーバーのFQDNとは異なり、一意である必要があります。StoreFrontとAccess Gateway仮想サーバーで同じFQDNを使用することはサポートされていません。Citrix Workspaceアプリは、内部ネットワークに接続されている

> ユーザーデバイスからのみ解決可能な、一意のStoreFront FQDNアドレスを必要とします。そうでない場合、Citrix Workspaceアプリのユーザーはメールベースのアカウント検出を使用できません。

ユーザーにプロビジョニングファイルを提供する

StoreFrontを使用して、アカウントの接続詳細を含むプロビジョニングファイルを作成できます。これらのファイルをユーザーに提供することで、Citrix Workspaceアプリ for iOSを自動的に構成できるようになります。Citrix Workspaceアプリ for iOSをインストールした後、ユーザーはデバイスで`.cr`ファイルを開くだけで、Citrix Workspaceアプリ for iOSを構成できます。Webサイト向けにWorkspaceを構成している場合、ユーザーはそれらのサイトからCitrix Workspaceアプリ for iOSのプロビジョニングファイルを取得することもできます。

詳しくは、StoreFrontのドキュメントを参照してください。

ユーザーに手動で入力するアカウント情報を提供する

ユーザーに手動で入力するアカウント詳細を提供する場合、ホストされたデスクトップに正常に接続できるように、以下の情報を配布してください。

- リソースをホストするStoreFront URLまたはXenAppおよびXenDesktopサイト。例: `servername.company.com`。
- Citrix Gatewayを使用してアクセスする場合、Citrix Gatewayのアドレスと必要な認証方法を提供します。

ユーザーが新しいアカウントの詳細を入力すると、Citrix Workspaceアプリは接続の検証を試みます。成功した場合、Citrix Workspaceアプリ for iOSは、ユーザーにアカウントへのログオンを促します。

Citrix Workspaceアプリの構成

この記事では、iOS 版 Citrix Workspace アプリを構成するのに役立つタスクを一覧表示します。

デスクトップとアプリの自動起動

バージョン 25.7.2 以降、デスクトップまたはアプリケーションの自動起動を体験できるようになりました。

> **注：**
>
> モバイルプラットフォームは、一度に1つのリソースの起動のみをサポートしています。複数のリソースを自動起動としてマークすると、予期しない動作につながる可能性があります。

構成方法

Citrix Workspace でコアアプリケーションが自動的に起動するようにするには、管理者はアプリケーションの説明に文字列 `KEYWORDS: AutoStartPrimaryApp` を追加する必要があります。構成後、アプリケーションはすべてのユーザーに対して自動的に起動します。

次の手順は管理者向けです。

1. **管理コンソールを開く:**

   Citrix Studio または組織の Citrix 管理ポータルを起動します。公開されているアプリケーションを編集する権限を持つアカウントでサインインします。

2. **アプリケーションを見つける:**

   アプリケーションに移動し、自動起動用に構成するアプリケーション（例: メモ帳）を選択します。

3. **アプリケーションのプロパティを編集する:**

   アプリケーションを選択し、**編集**または**プロパティ**を選択します。**説明**フィールドを見つけます。

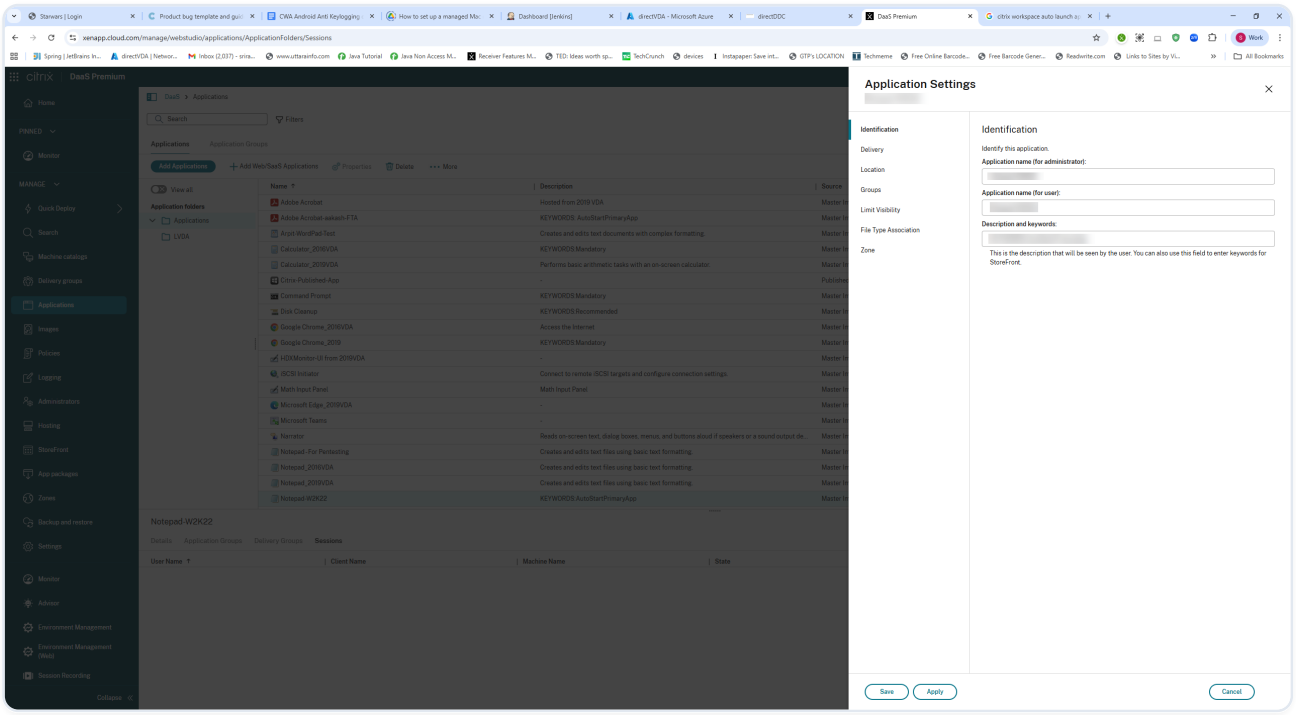
4. **自動起動キーワードを追加する:**

   説明の末尾にスペースを追加し、次のキーワードを追加します。

   ```
   KEYWORDS:AutoStartPrimaryApp
   ```

5. **変更を保存する:**

   OK、**保存**、または**更新**をクリックして変更を適用します。



リアルタイムエコーキャンセレーションによるオーディオ品質の向上

バージョン 25.3.0 以降、iOS 版 Citrix Workspace アプリにエコーキャンセレーション機能が導入され、モバイルデバイスで非常にクリアなオーディオを提供します。この機能は、リアルタイムでエコーを積極的に除去し、仮想会議や通話中のスムーズで中断のない通信を保証します。これにより、生産性が向上し、中断が減り、困難なモバイルネットワーク条件下でも優れたユーザーエクスペリエンスが提供されます。

GACS認証済みマイクロサービス（オンプレミス）をサポート

バージョン25.1.0以降、iOS向けCitrix Workspaceアプリは認証済みマイクロサービスをサポートし、GACSがユーザーグループを管理できるようにします。この機能は、オンプレミス環境の管理

者により強化された制御を提供します。詳細については、構成プロファイルを使用したユーザーグループの設定の管理を参照してください。

メール、ストアURL、またはドメインベースの検出APIによるGACSエンドポイントの取得

24.9.0リリース以降、管理者はメールアドレス、ドメイン、ストアURLに基づいてWebストアを構成できるようになり、Global App Configuration service (GACS) がユーザーを適切なカスタムWeb URLに識別して誘導できるようになります。Citrix WorkspaceアプリのiOSデバイスは、この検出APIを使用してGACSエンドポイントを取得できるようになり、ハードコードされたエンドポイントの必要性を排除し、構成されていない場合の不要な呼び出しを削減します。この更新はクラウドとオンプレミスの両方のストアに利益をもたらし、ユーザーはストアURLを介して直接Webストアを構成でき、GACSを使用してカスタムWebストアを追加するオプションもあります。詳細については、Global App Configuration serviceチャネルサポートを参照してください。

GACS認証済みマイクロサービスをサポート（クラウド）

24.9.0リリース以降、iOS向けCitrix Workspaceアプリは認証済みマイクロサービスをサポートし、GACSがお客様のユーザーグループを管理できるようにします。これにより、柔軟性と制御が向上し、現在はクラウドストアのみでサポートされています。詳細については、構成プロファイルを使用したユーザーグループの設定の管理（プレビュー）を参照してください。

機能フラグ管理

機能フラグは、機能を動的に有効または無効にするために使用されます。Citrix Workspaceアプリで本番環境で問題が発生した場合、その機能が出荷された後でも、影響を受ける機能を無効にできます。

ファイアウォールまたはプロキシがアウトバウンドトラフィックをブロックしている場合を除き、機能管理のためにトラフィックを有効にするための構成は不要です。そのような場合は、ポリシー要件に基づいて特定のURLまたはIPアドレスへのトラフィックを有効にする必要があります。

機能フラグ管理のためのトラフィックを有効にする

Citrix Workspaceアプリバージョン24.10.0以降:

最適な機能とプレビュー機能へのアクセスを確保するには、以下のURLへのトラフィックを有効にする必要があります。

- `features.netscalergateway.net`

> **注：**
>
> 2025年1月以降、Citrix Workspaceアプリのバージョン24.10.0未満では、以前の機能はサポートされなくなります。この日付以降、バージョン24.10.0以降ではこれらの機能が有効になっているため、このセクションは関係なくなります。問題を回避するには、Citrix Workspaceアプリバージョン24.10.0以降にアップグレードしてください。さらに、`features.netscalergateway.net`設定が有効になっていることを確認してください。そうしないと、バージョン24.10.0以降で問題が発生する可能性があります。

Citrix Workspaceアプリの非アクティブタイムアウト

管理者は、許可されるアイドル時間を指定できます。タイムアウト値を超えると、認証プロンプトが表示されます。

非アクティブタイムアウト値は、1分から24時間まで設定できます。デフォルトでは、非アクティブタイムアウトは構成されていません。管理者は、PowerShellモジュールを使用してinactivityTimeoutInMinutesMobileプロパティを構成できます。Citrix Workspaceアプリ構成用のPowerShellモジュールをダウンロードするには、Citrix Workspaceアプリ構成用のPowerShellモジュールをダウンロードをクリックしてください。

指定されたタイムアウト値に達すると、構成されている認証タイプに応じて、エンドユーザーエクスペリエンスは次のようになります。

- 非アクティビティタイムアウト後、Citrix Workspaceアプリに再度アクセスするために生体認証を提供するようプロンプトが表示されます。
- 生体認証プロンプトをキャンセルできる場合、次のメッセージが表示されます。

  Citrix Workspaceアプリはロックされています。

  Workspaceアプリを継続して使用するには、認証が必要です。

iOSでパスコードが設定されていない場合、非アクティビティタイムアウト後に資格情報でサインインする必要があります。

> **注：**
>
> この機能は、Workspace (Cloud) をご利用のお客様にのみ適用されます。

カスタマーエクスペリエンス向上プログラム (CEIP)

Citrix WorkspaceアプリのCitrixカスタマーエクスペリエンス向上プログラム (CEIP) とは何ですか?

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) は、Citrix Workspaceアプリから構成データと使用状況データを収集し、Citrix Analyticsに自動的に送信します。このデータにより、CitrixはCitrix Workspaceアプリのパフォーマンスを分析し、品質、機能、パフォーマンスを向上させ、製品開発のためのリソース割り当てを最適化し、効果的な人員配置とインフラ投資を通じてサービスレベルをサポートすることができます。

すべてのデータは集計形式でのみ使用および分析され、個々のユーザーやデバイスが特定されたり、個別に分析されたりすることはありません。CitrixはCEIPを通じて個人を特定できる情報 (PII) を収集することはなく、すべてのデータ収集は関連する業界のデータプライバシーおよびセキュリティ基準に準拠しています。

CEIPデータを収集するために使用されるツール

iOS版Citrix Workspaceアプリは、Citrix AnalyticsとGoogle Firebaseを使用してCEIPデータを収集します。

収集されるデータ

Citrix AnalyticsとGoogle Firebaseによって収集される特定のCEIPデータ要素は次のとおりです。

セッション情報とセッション起動方法	Citrixストアとストア構成	認証タイプと認証構成	ICA® 接続
HDX™ セッション起動	Storeアプリセッション	WebViewアクション開く	WebViewアクションコピー
WebViewアクション共有	Workspaceアプリレビュー	接続ステータス、接続エラー、接続センターの使用状況	外部ディスプレイ
ソケットステータス	セッション期間	UDP経由のHDX	セッション起動時間
デバイス情報	デバイスモデル情報	利用状況統計を送信	アプリ言語、Workspaceアプリ言語

キーボード言語	Citrixストアの種類	Citrixストアの組み合わせ	ストアプロトコルタイプ
ストア数	HDX UDPステータス	RSAトークンのインストール	

CEIPデータはどのユーザーから収集されますか?

Citrix Workspaceアプリは、すべての地域のユーザーを含むように構成されたCitrix Analyticsを介してCEIPデータを収集します。ただし、Citrix Analyticsを介して収集されたCEIPデータには、欧州連合（EU）、欧州経済領域（EEA）、スイス、および英国（UK）のユーザーデータが含まれますが、Google Firebaseはこれらの地域にいるユーザーを除外します。この機能が有効であることを確認するには、最新バージョンに更新してください。

ユーザーと管理者はCEIPデータ収集を無効にできますか?

CEIPデータ収集は、以下の構成に従って、すべての法域で完全に無効にできます。

バージョン2205以降、以下の手順に従ってCEIPデータの送信を停止できます（ただし、以下の注記に記載されている2つのデータ要素は除きます）。

1. iOS版Citrix Workspaceアプリを開きます。
2. **ホーム** > **設定** をタップします。
3. **一般** セクションに移動し、**使用状況統計を送信** をオフにします。

追加情報

Citrix は、お客様と Citrix との契約条件に従ってお客様のデータを処理します。データは、Citrix Services Security Exhibit に指定されているとおりに保護されます。詳細については、Citrix Trust Center を参照してください。

Citrix は、CEIP の一部として、Citrix Workspace アプリから特定のデータを収集するために Google Firebase を使用します。Google が Google Firebase 向けに収集されたデータを処理する方法 を確認してください。

> **注：**
>
> Google Firebase は、欧州連合（EU）、欧州経済領域（EEA）、スイス、および英国（UK）のユーザーに対するデータ収集を除外します。

既知の制限事項

- VDA 7.18 以前では、ワークスペースハブへのキャスティングには、使用しているデスクトップまたはその他のリソースで h.264 全画面表示ポリシーが有効になっており、レガシーグラフィックポリシーが無効になっている必要があります。

セッション共有

ユーザーが Citrix Workspace アプリのアカウントからログオフしても、リモートセッションから切断またはログオフすることは可能です。

- **切断**: このデバイスでの接続を終了しますが、セッションはサーバー上で実行され続けます。後で再接続して、中断したところから作業を再開できます。その後、ユーザーは別のデバイスを起動し、iOS 用 Citrix Workspace アプリを起動して、iOS デバイスから切断する前の最後の状態に再接続できます。このオプションを使用すると、ユーザーはデバイス間で再接続し、実行中のアプリケーションでの作業を再開できます。
- **ログオフ**: アカウントからログオフし、Windows アプリケーションを閉じます。また、Citrix Virtual Apps and Desktops および Citrix DaaS サーバーからもログオフします。このオプションを使用すると、ユーザーはサーバーから切断し、アカウントからログオフできます。iOS 用 Citrix Workspace アプリを再度起動すると、デフォルトの状態が開きます。

クラウドストア

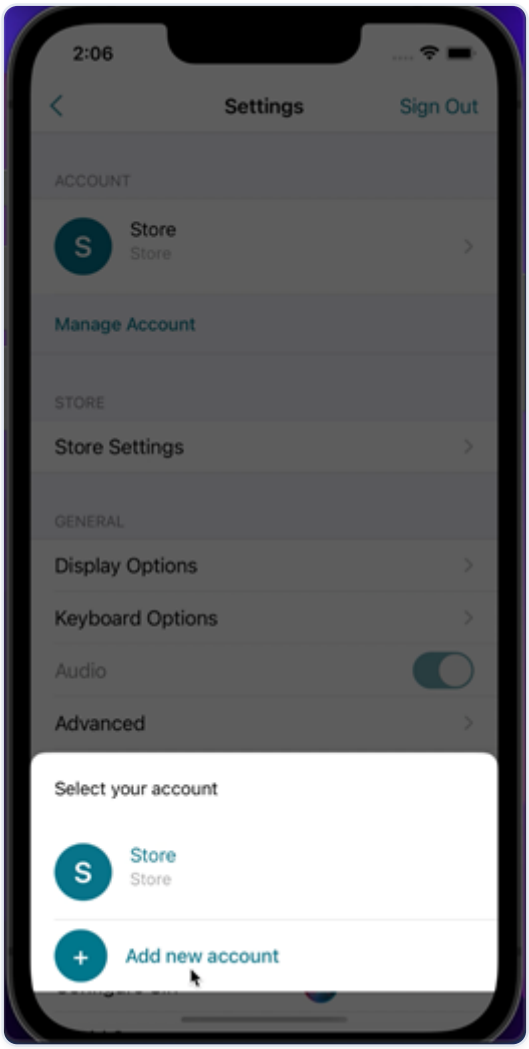
アクセス場所に関係なく、Web、SaaS アプリ、および組織がホストする Web サイトにアクセスできます。この機能は、クラウドストアを利用しているお客様のみが利用できます。

複数のクラウドストアのサポート

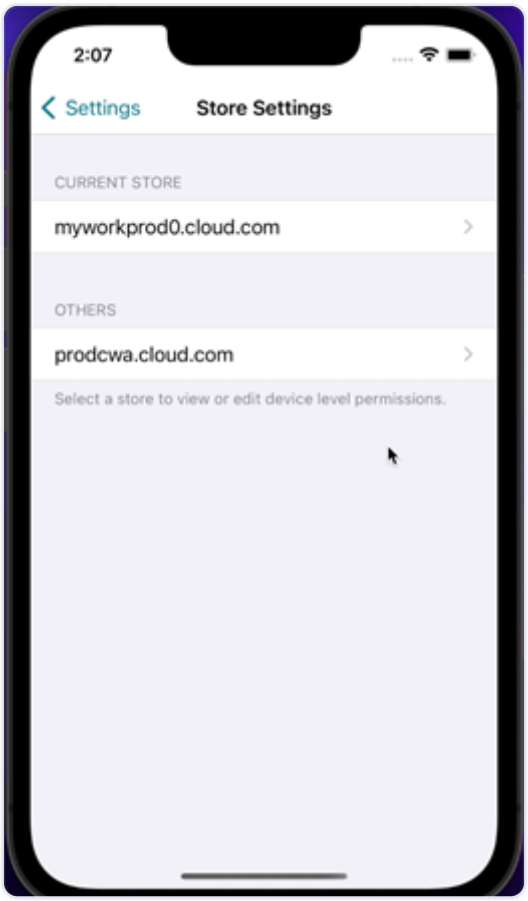
リリース 24.1.0 以降、iOS および iPadOS 用 Citrix Workspace アプリに複数のクラウドストアアカウントを追加できます。これにより、エンドユーザーは複数のストアを簡単に追加および切り替えることができます。この機能により、複数のストアにアクセスする際のユーザーエクスペリエンスが向上します。

別のアカウントを追加するには、次の手順を実行します。

1. **設定 > アカウントの管理**に移動します。画面の下部に、アカウントのリストを含むダイアログが表示されます。
2. **新しいアカウントを追加**をタップします。



3. IT管理者から提供されたURLまたはメールアドレスを入力します。必要に応じてスマートカードを使用してログオンするには、**スマートカードを使用**をタップします。
4. **続行**をタップします。ユーザー名、パスワード、ドメイン、パスコードの各フィールドがある**サインイン**ダイアログが表示されます。
5. 情報を入力します。フィールドの詳細については、IT管理者にお問い合わせください。
6. **サインイン**をタップします。新しいアカウントが設定されました。



ストアURLの自動入力

バージョン23.2.0以降、リブランドされたCitrix Workspaceアプリfor iOSにアクセスする際に、ストアURLを自動入力することを選択できます。この機能により、手動での介入が減り、アプリへの迅速なアクセスが提供されます。アプリのパーソナライズの詳細については、「アプリのパーソナライズ」を参照してください。

複数のストアの一括削除のサポート

バージョン24.2.0以降、Citrix Workspaceアプリfor iOSは、複数のストアの選択と削除をサポートしています。この機能により、複数のストアを操作する際のユーザーエクスペリエンスが向上します。この機能はデフォルトで有効になっています。

ストア画面から複数のストアを一括削除するには、次の手順を実行します。

1. **ストア**画面で、**選択**をタップします。



2. 削除するストアを選択します。すべてのストアを削除するには、**すべて選択**をタップします。
3. 「**削除**」をタップします。

ストアを削除(/en-us/citrix-workspace-app-for-ios/media/delete-stores-screen.png)

管理者によるストア名の変更制限のサポート

以前は、ユーザーは**アカウントの編集**オプションを使用してストア名を変更できました。

バージョン24.2.0以降、iOS向けCitrix Workspaceアプリは、管理者がユーザーによるストア名の変更を無効にするオプションを提供します。この機能により、管理者はストア名を簡単に識別し、一貫性を維持できます。

エンドユーザーがストア名を変更できるようにするには、次の手順を実行します。

1. 資格情報を使用してCitrix Cloudにサインインします。
2. **Workspace Configuration > Access**に移動します。**Workspace URL**の下に、既存のストアURLのリストが表示されます。

   ワークスペース構成(/en-us/citrix-workspace-app-for-ios/media/gacs-workspace.png)
3. エンドユーザーがストア名を変更できるようにしたいストアの省略記号メニューをクリックします。
4. 「**編集**」を選択します。

   編集オプション(/en-us/citrix-workspace-app-for-ios/media/edit-option.png)
5. 「**Workspace URLの編集**」ダイアログボックスで、「**エンドユーザーがWorkspaceでこのストア名を変更することを許可する（デフォルトでは許可されていません）**」を選択します。

   ストア名を無効にする(/en-us/citrix-workspace-app-for-ios/media/allow-admin-store.png)
6. をクリックします。

ストア名の自動入力

バージョン24.2.0以降、iOS向けCitrix Workspaceアプリは、管理者によるストア名の更新をサポートし、更新されたストア名をユーザーに自動的にプッシュします。この機能により、ストア名の更新時に手動での介入が不要になり、ユーザーエクスペリエンスが向上します。

> **注：**
>
> この機能は、管理者がユーザーによるストア名の変更を無効にしている場合にのみ有効になります。

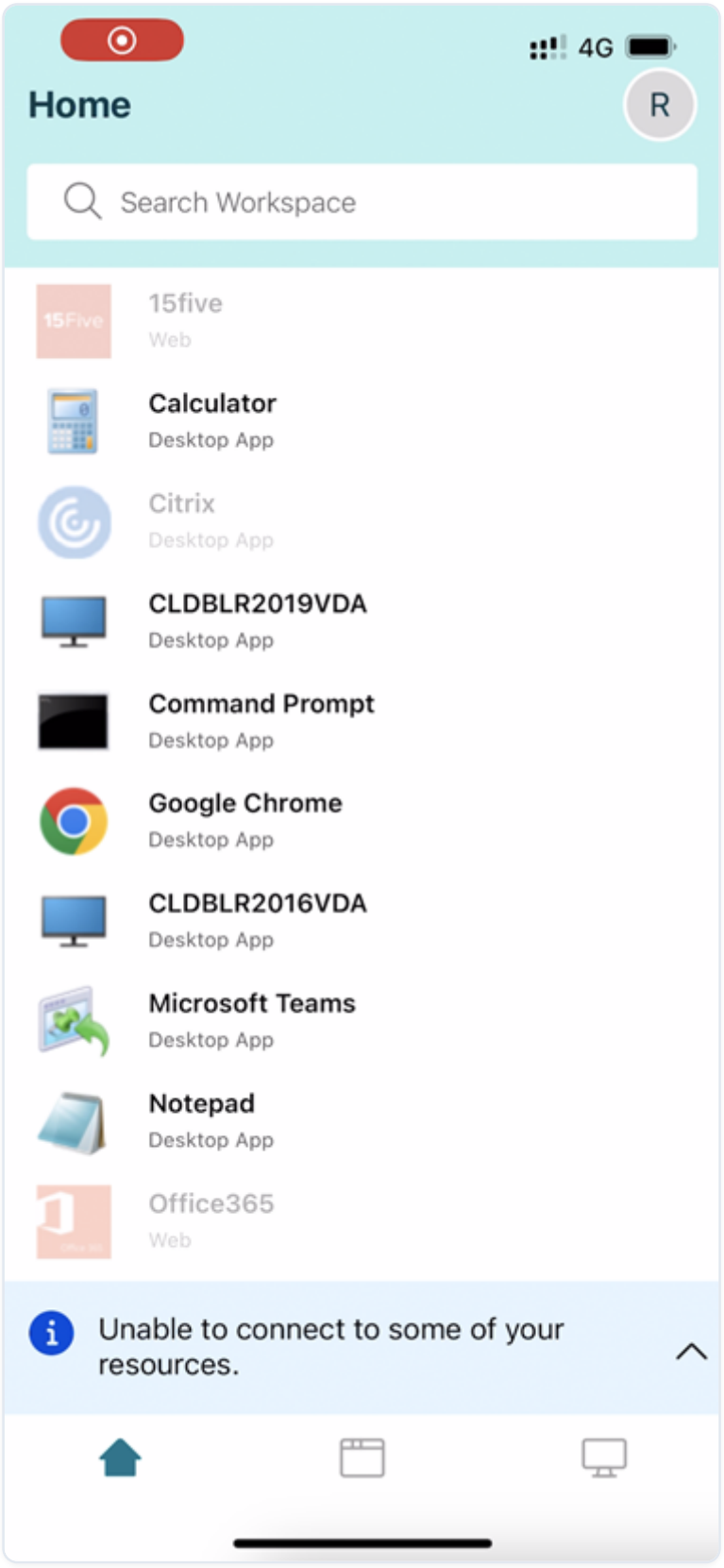
エンドユーザーエクスペリエンス監視の強化

EUEM (エンドユーザーエクスペリエンス監視) クライアントの起動メトリックをサポートするようになりました。EUEM は、非常に詳細なセッションエクスペリエンス監視データをリアルタイムで収集するのに役立ちます。このデータは Director ダッシュボードに送信され、管理者がユーザーエクスペリエンスを監視できるようになります。データは VDA 上のセッションエクスペリエンス監視サービス (SEMS) を介して収集されます。ダッシュボードで監視できるクライアント起動メトリックデータには、次のものが含まれます。

- ICA ファイルのダウンロード時間。
- セッション作成クライアントの期間。セッション作成クライアントの期間は、セッションの作成にかかる時間を表します。これは、ICA ファイルが起動されてから接続が確立されるまでの時間で計算されます。
- セッションルックアップクライアントの期間。セッションルックアップクライアントの期間は、要求された公開アプリケーションをホストするためにすべてのセッションを照会するのにかかる時間を表します。既存のセッションがアプリケーション起動要求を処理できるかどうかを判断するために、クライアントでチェックが実行されます。
- ICA ラウンドトリップタイム (ICA RTT とも呼ばれる) の Citrix リアルタイム記録。ICA RTT は、ユーザーがキーを押してから、応答がエンドポイントに表示されるまでの経過時間です。

サービス継続性オフラインモードのユーザーインターフェイスを強化

24.1.0 リリース以降、iOS 版 Citrix Workspace アプリのユーザーインターフェイスが改善され、Citrix Workspace の停止中に、より情報量が多く、モダンで、ユーザーフレンドリーなエクスペリエンスを提供するようになりました。オフラインモードでは、あいまい検索機能も含まれています。この機能を使用すると、テキストが近似しているアプリやデスクトップ、スペルミスのある検索語句の結果を見つけることができます。サービス継続性の詳細については、「サービス継続性」を参照してください。



Global App Configuration サービスチャネルのサポート

23.4.5 リリース以降、管理者は Global App Configuration サービスを使用して設定を定義し、すべてのエンドユーザーに構成を展開する前にテストできるようになりました。このプロセスにより、機能が本番環境に導入される前に十分にテストされることが保証されます。

注：

- iOS 版 Citrix Workspace アプリは、**Default** および **Test channel** の構成をサポートしています。デフォルトでは、すべてのユーザーが **Default** チャネルを使用します。

詳細については、「Global App Configuration サービス」のドキュメントを参照してください。

構成方法の詳細については、「Global App Configuration サービスチャネルのサポート」を参照してください。

Global App Configurationサービスが有効なWebストアへのアクセス

バージョン23.7.5以降、管理者は、メールベースのストア検出のためにWebストア（Webインターフェイス）を構成できるようになりました。エンドユーザーがストアを追加する際（ようこそ画面で）に入力したメールアドレスに基づいて、Global App Configurationサービスは、管理者が定義したカスタムWeb（Webインターフェイス）URLの特定を支援します。その後、エンドユーザーは管理者が構成したWebストアに自動的に誘導されます。エンドユーザー向けのWebストアURLの構成について詳しくは、「許可されたカスタムWebポータル」を参照してください。

Unified Endpoint Managementソリューションを使用したWorkspaceアプリの構成

バージョン23.3.0以降、iOS向けCitrix Workspaceアプリは、Unified Endpoint Management (UEM)ソリューションを使用して、AppConfigベースのキーと値のペアによるWorkspaceアプリの管理者構成をサポートします。

構成方法

Unified Endpoint Managementソリューションを使用してWorkspace StoreのURLを構成するには、次の手順に従います。

注：

説明のために、この例ではMicrosoft IntuneをUEMソリューションとして使用しています。以下の手順と表示されるUIは、UEMプロバイダーによって異なります。

1. Unified Endpoint Management (UEM) プロバイダーにサインインします。
2. UEMプロバイダーで管理したいCitrix Workspaceアプリを追加します。UEMプロバイダーのポータルを使用してアプリをアップロードし、UEMプロバイダーによる管理を有効にできます。または、App Storeのアプリにリンクすることもできます。
3. アプリの構成ポリシーを作成します。
4. XMLプロパティリストにキーと値のペアを追加し、以下の値を入力します。

    - **キー**: `url`
    - **値のタイプ**: `String`
    - **値**: ストアのURL（例: `prodcwa.cloud.com`）


Settings Edit

Configuration key	Value type	Configuration value
url	String	prodcwa.cloud.com

制限事項

- クラウドストアがすでに設定されており、管理者が新しいクラウドストアを構成した場合、既存のクラウドストアは削除されます。また、既存のクラウドストアに関連付けられているデータや設定もすべて削除されます。Citrix Workspaceで通知を受け取ります。その後、新しいクラウドストアがCitrix Workspaceに追加されるように、再度サインインする必要があります。
    - 上記の記述は、既存のクラウドストアにのみ適用されます。オンプレミスストアがすでに構成されており、管理者が新しいクラウドストアまたはオンプレミスストアを構成した場合、新しいストアが追加され、削除は行われません。
- 新しい構成を適用するには、Citrix Workspaceアプリを強制終了して再起動する必要があります。

統合エンドポイント管理ソリューションの機能強化

バージョン23.4.5以降、iOS向けCitrix Workspaceアプリは、AppConfigベースのキーと値のペアを使用してCitrix Workspaceアプリを構成するためのいくつかの追加構成をサポートしています。以前は、管理者はストアURLを構成できました。現在、管理者はエンドユーザーがストアURLを変更することを制限し、アプリの表示方法を制御できます。

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

詳細は次のとおりです。

構成キー	値の型	構成値
`url`	`String`	ストアURL。例: `prodcwa.cloud.com`
`storeType`	`Integer`	• (デフォルト) 1に設定すると、ユーザーはネイティブまたはデフォルトのストアの読み込みを表示できます。- 2に設定すると、ユーザーはWebインターフェイス内でストアを表示できます。
`restrict_user_store_modification`	`Boolean`	• **true**に設定すると、ユーザーはストアを変更できません (追加/削除/編集)。- **false**に設定すると、ユーザーはストアを変更できます。**注:** フラグがtrueに設定されている場合、UEMで構成されたストアを追加する前に、既存のすべてのストアが削除されます。

UEMを介したデバイス名の構成のサポート

バージョン24.3.5以降、iOS向けCitrix Workspaceアプリでは、管理者がUnified Endpoint Management (UEM) を介してユーザーグループに基づいてデバイス名を割り当て、識別できるようになります。

UEMを使用してデバイス名を構成するには、次の手順を実行します。

> **注：**
>
> この例では、説明のためにMicrosoft IntuneがUEMソリューションとして使用されています。以下の手順と表示されるUIは、UEMプロバイダーによって異なります。

1. UEMプロバイダーにサインインします。
2. UEMプロバイダーによって管理したいCitrix Workspaceアプリを追加します。UEMプロバイダーのポータルを使用してアプリをアップロードし、UEMプロバイダーによる管理を有効にできます。または、App Storeのアプリにリンクすることもできます。
3. アプリのアプリ構成ポリシーを作成します。
4. XMLプロパティリストにキーと値のペアを追加し、以下の値を入力します。
    - キー: deviceName
    - 値の型: String
    - 値: デバイス名（例: MY_IPHONE_Device）

デバイス名(/en-us/citrix-workspace-app-for-ios/media/device-name.png)

UEMを介したCitrix Workspaceアプリ設定の構成のサポート

以前は、Unified Endpoint Management (UEM) を使用して、Citrix Workspaceアプリでストアの URLのみを構成できました。

バージョン24.7.0以降、インフラストラクチャに展開されている任意のUEMソリューションを使用して、管理対象デバイス上のCitrix Workspaceアプリ設定も構成できます。

> **注：**
>
> 管理者として、UEMとGlobal App Configuration service (GACS) を使用してCitrix Workspaceアプリ設定を構成するオプションがある場合、UEM設定がGACSよりも優先されます。

> 以下は、Citrix Workspaceアプリ設定を構成するためのJSONファイルのサンプルです。

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store 1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
```

```
                        <key>value</key>
                        <true/>
                    </dict>
                </array>
            </dict>
            <dict>
                <key>category</key>
                <string>authentication</string>
                <key>userOverride</key>
                <false/>
                <key>settings</key>
                <array>
                    <dict>
                        <key>name</key>
                        <string>settings_auth_web_browser</string>
                        <key>value</key>
                        <string>embedded</string>
                    </dict>
                </array>
            </dict>
        </array>
    </dict>
```

```
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>StoreFront1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_audio_stream</string>
                            <key>value</key>
                            <false/>
                        </dict>
```

```
                </array>
            </dict>
            <dict>
                <key>category</key>
                <string>authentication</string>
                <key>userOverride</key>
                <false/>
                <key>settings</key>
                <array>
                    <dict>
                        <key>name</key>
                        <string>settings_auth_web_browser</string>
                        <key>value</key>
                        <string>system</string>
                    </dict>
                </array>
            </dict>
        </array>
    </dict>
</array>
<key>storesToDelete</key>
<array>
```

```
        <string>test.cldblr.com</string>
        <string>test.cloud.com</string>
    </array>
    <key>restrict_user_store_modification</key>
    <false/>
</dict>
```

注：

`userOverride`フラグを使用すると、ユーザーはCitrix Workspaceアプリの設定を変更できます。`userOverride`フラグがtrueに設定されている場合、ユーザーは設定を変更できます。`userOverride`フラグが任意の設定に対してfalseに設定されている場合、ユーザーはCitrix Workspaceアプリの設定でそれを変更できません。

Workspaceアプリ設定のキーと値のペアの表

次の表に、キーと値のペアの情報を示します。

注：

カテゴリ固有の設定は、そのカテゴリの下の1つのブロックに追加する必要があります。

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
認証	生体認証プロンプトの使用をスキップ	生体認証を有効または無効にします。	settings_skip_consent_for_biometric_protected_pass	true/false	ブール値	FALSE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
			word_saving 値			
オーディオ	オーディオ	ユーザーが仮想アプリまたはデスクトップからオーディオをオンまたはオフにできるようにします。	settings_audio_stream	true/false	ブール値	TRUE
キーボード	Unicode キーボードを使用	ユーザーが標準の Unicode キーボードを使用できるようにします。	settings_use_unicode_keyboard	true/false	ブール値	TRUE
キーボード	自動キーボード	セッション内キーボードを有効または無効にします。	settings_automatic_keyboard	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
キーボード	キーボードレイアウト同期	ユーザーがデバイスで優先するキーボードレイアウトに切り替えることを許可します。	settings_keyboard_layout_sync	true/false	ブール値	FALSE
キーボード	カスタムキーボードを使用	ユーザーが仮想セッションでダウンロードされたサードパーティ製キーボードを使用することを許可します。	settings_allow_keyboard_extensions	true/false	ブール値	FALSE
ディスプレイ	セッション解像度	ユーザーが画面解像度を選択できるようにします。	settings_resolution	0–9	整数	5 (iPad) 3 (iPhone)
表示	プレゼンテーションモード	外部ディスプレイを使用中に、iOS デバイスをトラッ	settings_presentation_mode	true/false	ブール値	FALSE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
		クパッドとして使用してセッションを制御できるようにします。				
表示	外部ディスプレイ	外部ディスプレイをデバイスに接続します。	settings_external_display	true/false	ブール値	TRUE
詳細設定	厳格な証明書検証	サーバー証明書の検証をより厳格に制御します。	settings_strictCertValidation	true/false	ブール値	FALSE
詳細設定	TLSバージョン	トラブルシューティングのために、ユーザーがTLS設定を変更できるようにします。	settings_tlsVersion	0〜3	整数	0
詳細設定	ネイティブコンボボックスを使用	iOSのネイティブ選択機能の使用を	settings_native_combobox	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
		有効にします。				
詳細設定	タッチ有効化 (iPadのみ)	タッチオプションがネイティブで有効になっていないアプリやデスクトップを含め、すべてのアプリとデスクトップでタッチを有効にします。	settings_multitouch_on	true/false	ブール値	真 (iPad) 偽 (iPhone)
詳細設定	全画面表示	アプリとデスクトップを全画面で表示できます。	settings_mobile_window_fullscreen	true/false	ブール値	真 (iPad) 偽 (iPhone)

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
詳細設定	ログイン時に再接続	新しいアカウントが追加されたとき、またはサインイン中に、セッションが自動的に再接続されるようにします。	settings_reconnect_logon	true/false	ブール値	FALSE
詳細	更新時に再接続	2台目のデバイスでアプリまたはデスクトップを更新すると、別のデバイスから起動されたセッションに自動的に再接続します。	settings_reconnect_refresh	true/false	ブール値	FALSE
詳細	HTTPプロキシを有効にする	セッションでHTTPプロキシを使用できるようにします。	settings_use_local_proxy	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
詳細	派生資格情報を使用する	派生資格情報を使用できるようにします。	setting_useDerivedCredentials	true/false	ブール値	FALSE
詳細	セッション内のスマートカード	セッション内でスマートカードデバイスの使用を許可します。この設定では、ユーザーはセッションに認証できません。	settings_usesSmartCardInsideSession	true/false	ブール値	FALSE
詳細	EDTを許可	アダプティブトランスポートのサポートを有効にします。	settings_allowUdp	true/false	ブール値	TRUE
詳細	自動タブレットモード	外部キーボードまたはマウスが検出されない場合に、仮想セッションをタブレッ	settings_enableTabModeSwitch	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
		トモードで起動できるようにします。				
詳細設定	ディスプレイをオンのままにする	画面をオンのままにします。	settings_stay_awake	true/false	ブール値	FALSE
詳細設定	iPadストレージを使用	デバイス上のローカルドライブにアクセスできます。	settings_client_drive	true/false	ブール値	無効
X1マウス	X1マウスを許可	Citrix X1 マウスへのアクセスを切り替えることができます。	settings_allow_X1_mouse	true/false	ブール値	FALSE
X1 マウス	Citrix® X1 マウス速度	ユーザーが仮想セッション内でマウスカーソルの速度を制御できるようにします。	settings_x1MouseSpeed	1,2	整数	200 (iPadPro) 100 (その他すべてのデバイス)
X1 マウス	Citrix X1 マウスにリモート	セッション内でカーソル	settings_X1_mouse_serve	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
	カーソル画像を使用	をアプリまたはデスクトップに合わせます。たとえば、カーソルがテキストボックス上にある場合、テキストボックスに合わせて変化します。	r_side_cursor			
認証	認証用Webブラウザ	デバイス上でWKWebの代わりにSafariViewControllerの使用状況を特定できます。	settings_auth_web_browser	system/embedded	文字列	埋め込み
thirdPartyServices	LaunchDarkly	Citrix Workspaceアプリの機能でLaunchDarklyフラグを有効にします。	enableLaunchDarkly	true/false	ブール値	true (EU圏外)

新しいツールバーメニューオプションのキーと値のペアの表

次の表は、新しいツールバーのキーと値のペアの情報を示しています。

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
ツールバー	新しいツールバー	新しいツールバーを有効にするキー。	enableNewToolbar	true/false	ブール値	TRUE
ツールバー	切断	セッションからのログアウト、セッションの切断、またはアクションのキャンセルを行うオプションを提供します。	enableCloseToolbarOption	true/false	ブール値	TRUE
ツールバー	キーボード	セッション内キーボードを有効または無効にします。	enableKeyboardToolbarOption	true/false	ブール値	TRUE
ツールバー	ポインター	セッション内のポインターを有効または無効にします。	enablePointerToolbarOption	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
ツールバー	拡大鏡	セッションの選択した部分を拡大します。	enableMagnifierToolbarOption	true/false	ブール値	TRUE
ツールバー	アプリの切り替え	開いているアプリ間の切り替えを有効にします。	enableSwitchAppsToolbarOption	true/false	ブール値	TRUE
ツールバー	接続強度	セッションのネットワーク接続強度を表示します。	enableConnectionStrengthToolbarOption	true/false	ブール値	TRUE
ツールバー	コントロール+オルト+デル	セッションを閉じる、ロックする、またはログアウトするオプションを提供します。	enableCtrlAltDelToolbarOption	true/false	ブール値	TRUE
ツールバー	デバイス	外部デバイスへの接続を有効にします	enableDevicesToolbarOption.	true/false	ブール値	TRUE
ツールバー	デバイスのペアリング	外部周辺機器とのペアリン	enablePairToolbarOption	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
		グオプションを有効にします。				
ツールバー	仮想マウス	セッションで仮想マウスを有効にします。	enableSoftMouseToolbarOption	true/false	ブール値	TRUE
ツールバー	矢印キー	ユーザーがセッション内を移動できる4つの矢印キーを有効にします。	enableArrowKeysToolbarOption	true/false	ブール値	TRUE
ツールバー	表示	ユーザーをCWAアプリの表示設定に移動させます。	enableDisplaySettingsToolbarOption.	true/false	ブール値	TRUE
ツールバー	キャスト	キャスト機能を有効または無効にします	enableCastingToolbarOption.	true/false	ブール値	TRUE
ツールバー	カメラ	ユーザーが前面、背面、または外部カメラをアクティブにでき	enableCameraToolbarOption	true/false	ブール値	TRUE

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
		るようにします。				
ツールバー	ドキュメントをスキャン	ユーザーがデスクトップセッション内からドキュメントをスキャンできるようにします。	enableScanDocumentToolbarOption	true/false	ブール値	TRUE
ツールバー	ヘルプ	初めてのユーザーがツールバーメニューを操作するのに役立つヘルプメニューをアクティブにします。	enableHelpToolbarOption	true/false	ブール値	TRUE

セッション再接続設定のキーと値のペアの表

以下の表は、新しいツールバーのキーと値のペアの情報を提供します。

カテゴリ	設定	説明	キー	値	値の型	デフォルト値
詳細設定	セッション再接続	セッション再接続を有効にする	settings_manual_reconnect	true/false	ブール値	TRUE

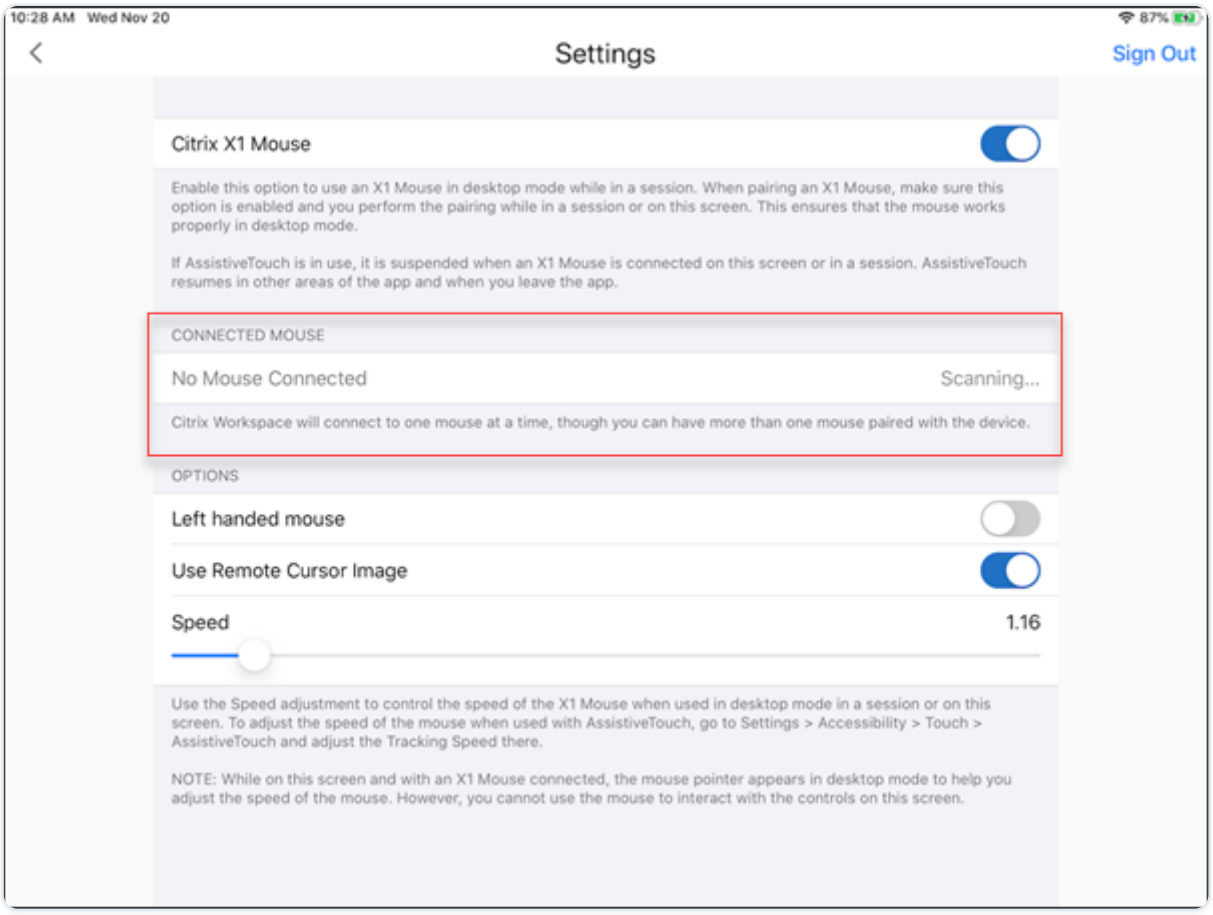
周辺機器

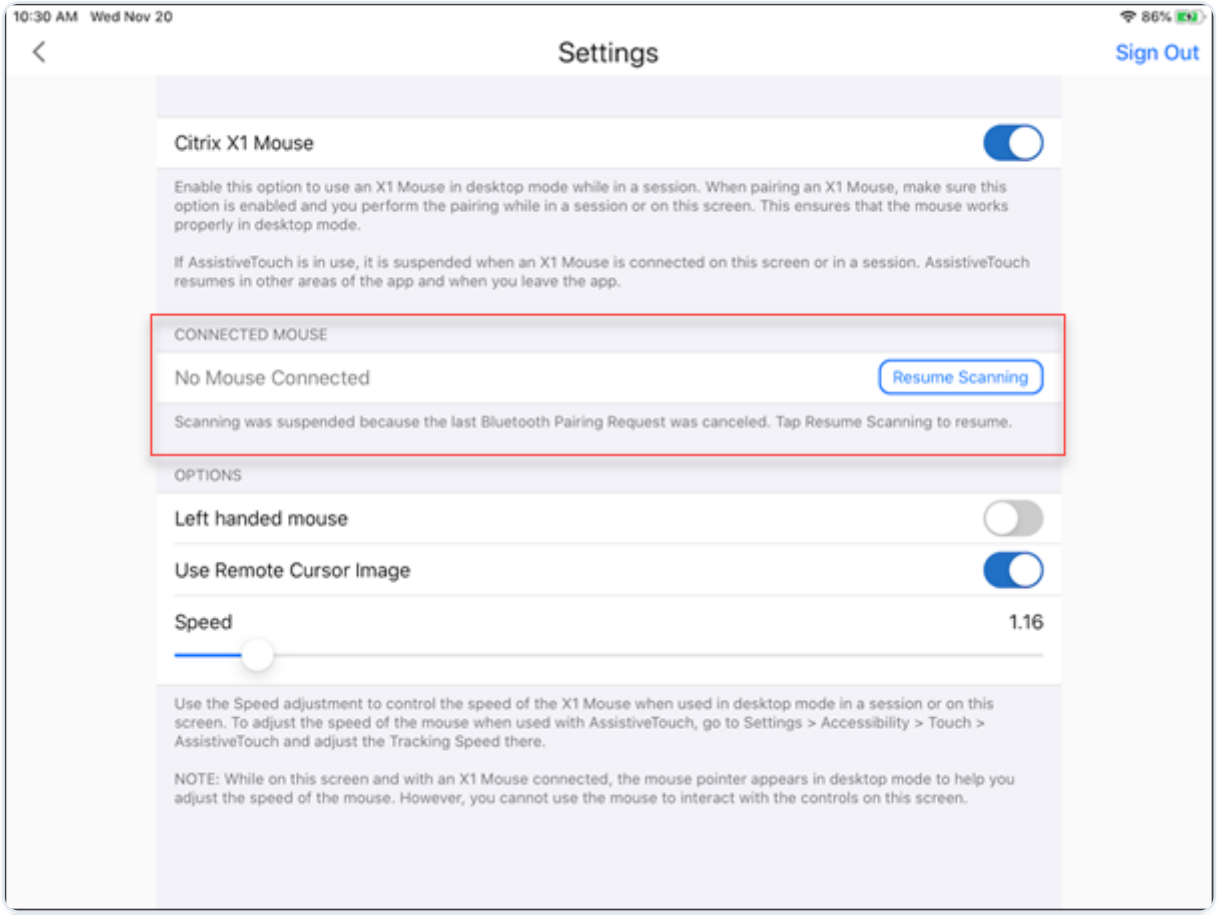
Citrix® X1 マウス

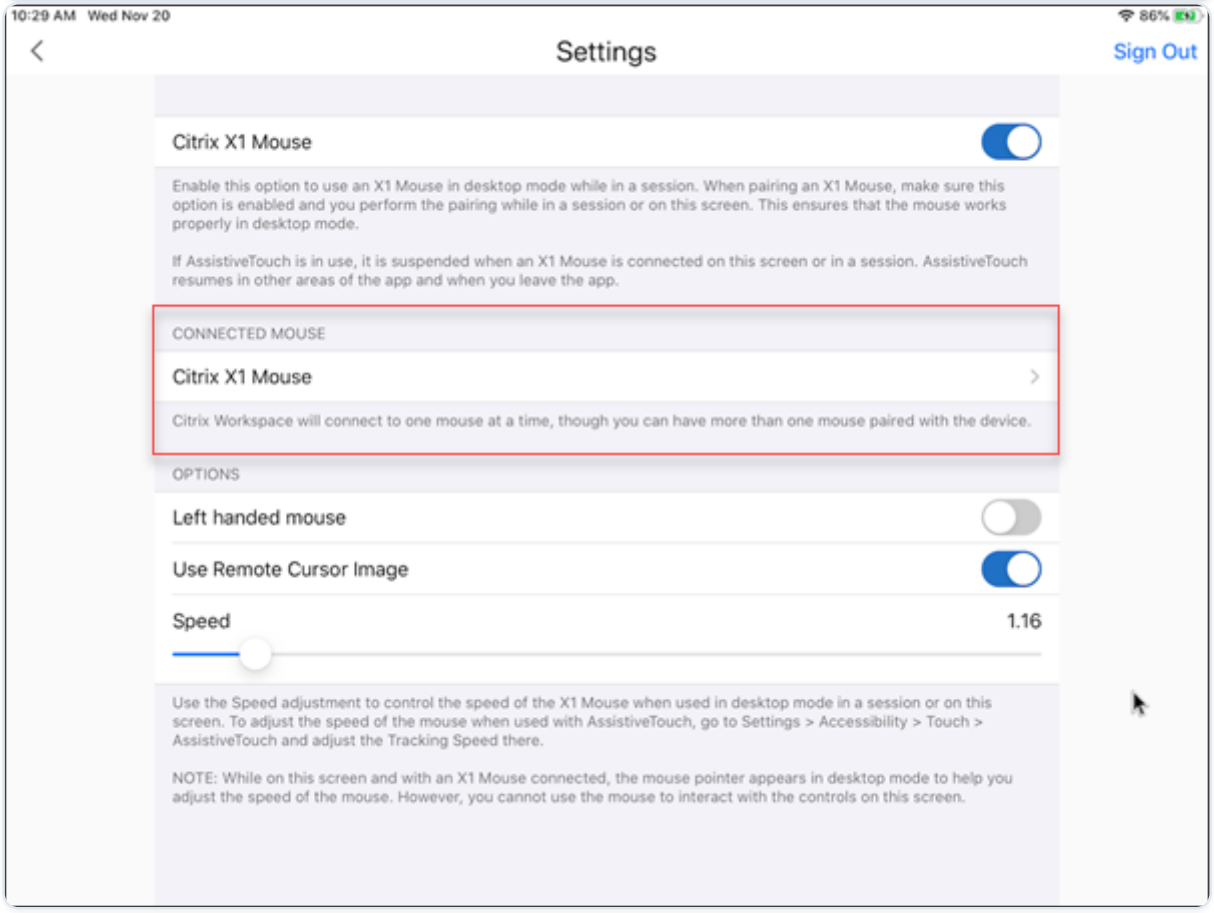
Citrix X1 マウスのペアリングと接続ステータス

この機能により、Citrix X1 マウスのペアリングプロセスをより詳細に制御できます。**設定**画面で、次のことができます。

- Citrix X1 マウスをペアリングします。セッション中にX1 マウスをペアリングすることもできます。
- 接続ステータスを表示します。



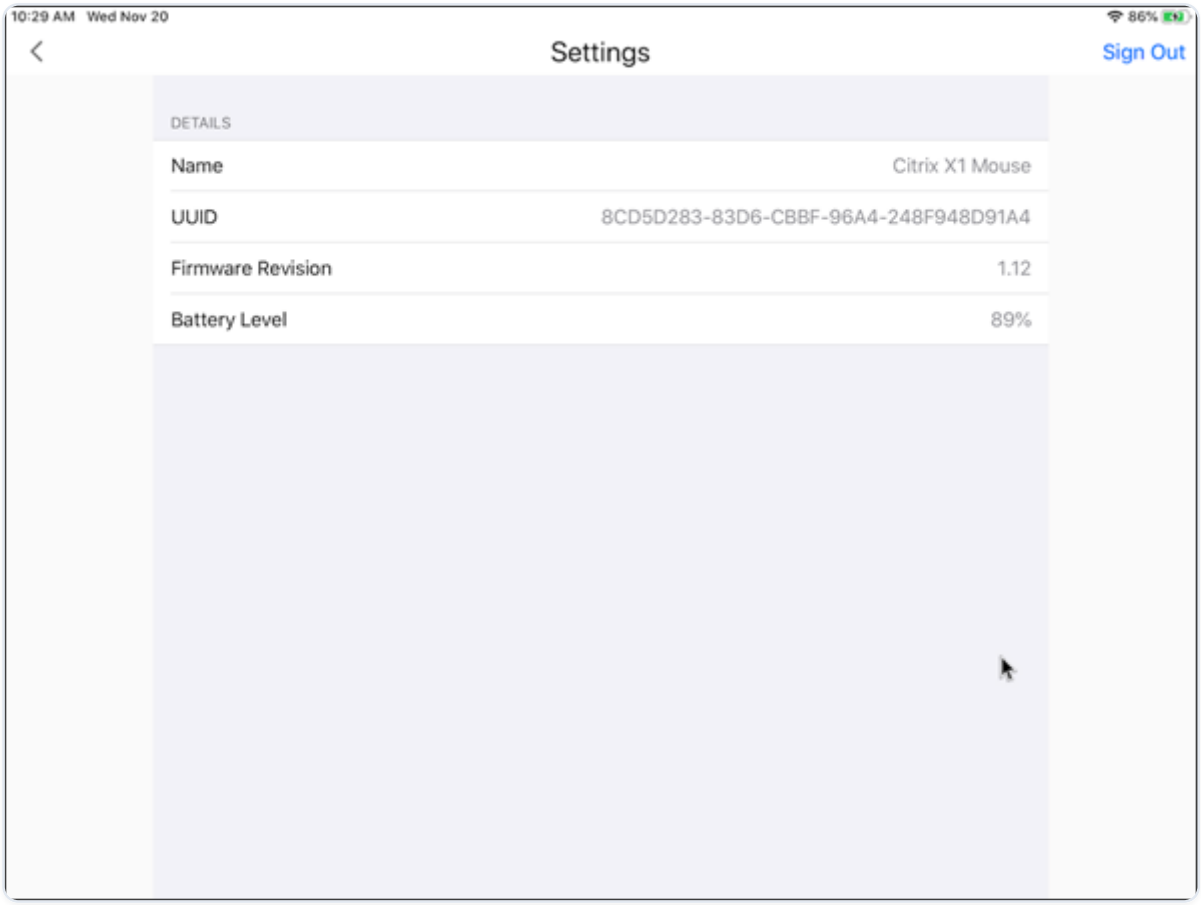

10:30 AM Wed Nov 20
86%
Settings
Sign Out
Citrix X1 Mouse
Enable this option to use an X1 Mouse in desktop mode while in a session. When pairing an X1 Mouse, make sure this option is enabled and you perform the pairing while in a session or on this screen. This ensures that the mouse works properly in desktop mode.
If AssistiveTouch is in use, it is suspended when an X1 Mouse is connected on this screen or in a session. AssistiveTouch resumes in other areas of the app and when you leave the app.
CONNECTED MOUSE
No Mouse Connected
Resume Scanning
Scanning was suspended because the last Bluetooth Pairing Request was canceled. Tap Resume Scanning to resume.
OPTIONS
Left handed mouse
Use Remote Cursor Image
Speed
1.16
Use the Speed adjustment to control the speed of the X1 Mouse when used in desktop mode in a session or on this screen. To adjust the speed of the mouse when used with AssistiveTouch, go to Settings > Accessibility > Touch > AssistiveTouch and adjust the Tracking Speed there.
NOTE: While on this screen and with an X1 Mouse connected, the mouse pointer appears in desktop mode to help you adjust the speed of the mouse. However, you cannot use the mouse to interact with the controls on this screen.


10:29 AM Wed Nov 20
86%
Settings
Sign Out
Citrix X1 Mouse
Enable this option to use an X1 Mouse in desktop mode while in a session. When pairing an X1 Mouse, make sure this option is enabled and you perform the pairing while in a session or on this screen. This ensures that the mouse works properly in desktop mode.
If AssistiveTouch is in use, it is suspended when an X1 Mouse is connected on this screen or in a session. AssistiveTouch resumes in other areas of the app and when you leave the app.
CONNECTED MOUSE
Citrix X1 Mouse
Citrix Workspace will connect to one mouse at a time, though you can have more than one mouse paired with the device.
OPTIONS
Left handed mouse
Use Remote Cursor Image
Speed
1.16
Use the Speed adjustment to control the speed of the X1 Mouse when used in desktop mode in a session or on this screen. To adjust the speed of the mouse when used with AssistiveTouch, go to Settings > Accessibility > Touch > AssistiveTouch and adjust the Tracking Speed there.
NOTE: While on this screen and with an X1 Mouse connected, the mouse pointer appears in desktop mode to help you adjust the speed of the mouse. However, you cannot use the mouse to interact with the controls on this screen.

- Citrix X1 マウスのプロパティ（例：**名前**、**UUID**、**ファームウェアリビジョン**、**バッテリーレベル**）を表示します。これを行うには、**接続済みマウス**の下にあるCitrix X1 マウスのエントリをタップします。



接続済みマウスのプロパティ:



AssistiveTouch

iOS 13以降でAssistiveTouch機能が有効になっている場合、デスクトップマウスモードとAssistiveTouchモードを切り替えると、AssistiveTouchカーソルが表示されます。

> **注：**

> デスクトップマウスモードでは、ポインターカーソルが表示されます。AssistiveTouchモードでは、丸いカーソルが表示されます。

> AssistiveTouchカーソルは、次の場合に表示されます。

- セッションを終了する
- iOSアプリスイッチャー画面に移動する
- iOSホーム画面または別のアプリに移動する

Citrix Workspaceアプリに戻り、セッション中にいると、デスクトップモードが再開されます。

外部モニターとツールバーのサポート

Citrix X1 Mouseを使用して、外部モニター上のツールバーを操作できます。ツールバーが閉じている間は、ツールバーのノッチを水平方向に移動できます。iOSデバイスを外部モニターに接続すると、Citrix Workspaceアプリは外部モニターの画面解像度を自動的に検出します。ツールバーの**表示**ボタンを使用して、特定の画面解像度を選択できます。アカウントを追加したり、最初にサインインしたりすることなく、**表示**オプションにアクセスできます。

一般的なマウス

一般的なマウスとトラックパッドのサポート

HDX™セッションで、一般的なマウスまたはトラックパッドを使用して、右クリック、スクロール、およびホバーを実行できます。これらの操作はCitrix X1 Mouseと同様です。ローカルマウスカーソルのスタイルは、リモートカーソルのスタイルと一致するように変更されます。

> **注記:**
>
> - この機能はiPadOS 13.4以降で利用できます。
> - この機能はiPhoneではサポートされていません。

制限事項

セッション中に外部モニターが接続されている場合、iOSの制限により、一般的なマウスカーソルはネイティブデバイスに残ります。

外部モニターでの一般的なマウスのサポート

iPadに接続された外部モニターで一般的なマウスを使用できます。一般的なマウスは、iOS 13.4以降を実行しているデバイスでサポートされています。

> **重要:**

外部モニターで汎用マウスを使用するには、Citrix Workspaceアプリで**設定** > **ディスプレイオプション**に移動して、**プレゼンテーション**モードがオフになっていることを確認してください。

汎用マウスを使用すると、外部モニターのツールバーは非表示になります。また、マウスポインターは外部モニターにミラーリングされ、iPad画面と外部モニターの両方に同時に表示されます。

iPad用汎用マウスによる拡張マルチモニターサポート

iPadを汎用マウスに接続すると、デスクトップセッションを外部モニターに拡張できます。この機能はiPadOSバージョン14.0以降をサポートしています。

注：

- この機能は以前のバージョンでも部分的に利用できる場合があります。完全な機能を使用するには、バージョン22.1.0にアップグレードしてください。
- Citrix Workspaceアプリがプライマリマウスクリックを受信できるように、iOSの**設定** > **アクセシビリティ** > **タッチ** > **AssistiveTouch**でAssistiveTouchを無効にしてください。

拡張モードの構成

拡張モードを有効にするには：

1. HDMIケーブルと必要なアダプターを使用して、外部モニターをiPadに接続します。

   注：

   この設定は、AppleのUSB-C Digital AV MultiportアダプタまたはLightning Digital AVアダプタを使用すると最適に機能します。

2. アプリケーションの**設定** > **ディスプレイオプション**に移動し、**外部ディスプレイ**を**オン**に切り替えます。異なる表示モードが表示されます。iPadOSのバージョンが14.0以降の場合、ミラーモードとプレゼンテーションモードも汎用マウスを使用します。

3. **拡張**オプションを選択します。

次のいずれかの表示モードを選択できます。

- Mirror: iPadに接続された外部モニターにディスプレイをミラーリングできます。
- Presentation: 外部モニターをトラックパッドに変更できます。
- Extend: 各ディスプレイに異なるビューまたは画面を表示できます。

注：

- デスクトップセッションを起動して拡張する前に、「**Extend**」モードを設定します。
- 「**Extend**」モードは、発表されるまでiPhoneではサポートされていません。

ディスプレイの配置を構成する

ディスプレイの配置を構成するには：

1. 「**Extend**」モードを選択すると、「**Display arrangement**」オプションが表示されます。
2. 「**External display**」タイルを、iPadディスプレイの左、上、右、または下に再配置します。

注：

セッション中に、セッション内ツールバー > 「**Display**」設定アイコンを使用して、ディスプレイの配置を調整できます。

ディスプレイの拡張(/en-us/citrix-workspace-app-for-ios/media/extend-display.png)

注：

外部ディスプレイの解像度は、以下によって異なります。

- アダプター
- iPad
- 使用されているその他のハードウェア

汎用マウスモードとCitrix X1 マウスモード

汎用マウスモードは、Citrix X1 マウスモードよりも自動的に優先されます。X1 マウスが接続されている場合、代わりに汎用マウスとして使用されます。そのため、汎用マウス機能フラグが有効になっている場合、X1 マウスの設定ページにはアクセスできません。

> **注：**
>
> iPadOSバージョン14.0以降では、iPadに接続されているすべてのX1マウスはBluetoothマウスとして動作します。

マウスは利用できません(/en-us/citrix-workspace-app-for-ios/media/mouse-not-available.png)

汎用マウスアイコン

マウス設定アイコンは、セッション内ツールバーの**ディスプレイ**設定アイコンの隣に追加されます。セッション中に汎用マウスのトラッキング速度を調整するには、**マウス**設定を使用します。リモートカーソル画像の使用を切り替えることもできます。

> **注：**
>
> ネイティブマウスのトラッキング速度は、iOSの設定から調整できます。

マウス設定(/en-us/citrix-workspace-app-for-ios/media/mouse-settings.png)

機能の制限事項

- Citrix Workspaceアプリがプライマリマウスクリックを受信するようにするには、iOSの**設定** > **アクセシビリティ** > **タッチ** > **AssistiveTouch**でAssistiveTouchを無効にします。
- iOS設定のトラッキング速度とナチュラルスクロールオプションは、セッション内の汎用マウスには影響しません。ただし、スクロール速度はiOSの**設定**から制御できます。 トラッキング速度とナチュラルスクロールオプションは、セッションツールバー内の**マウス設定**画面からアクセスできます。
- iPadが分割モードで使用され、モニターが接続されている場合、汎用マウスはデスクトップセッション内のミラーモードでのみ機能します。

- アプリがポインターロックを取得する前、つまりセッション起動前にネイティブカーソルがマルチタスクメニュー上にある場合、マウスイベントは受信されません。 回避策として、通知センターをプルダウンし、ネイティブポインターを別の場所に移動してから通知センターを閉じます。
- iPadを外部モニターに接続すると、オーディオリダイレクトが失敗します。音声はiPadのスピーカーから再生されます。

機能の既知の問題

- セッションがアクティブな間、iPadまたは外部モニターに表示されるデスクトップイメージは、以下を変更すると乱れます。
  - 表示配置
  - 解決策
  - 向き、または
  - 表示モード

  回避策として、モニターを一度切断し、再接続してください。問題が解決しない場合は、切断してセッションを再起動してください。 。
- まれに、外部モニターでビデオを再生すると、音声に数秒の遅延が発生することがあります。
- まれに、iPadおよび外部モニターでVDA表示が切り詰められることがあります。回避策として、モニターを一度切断し、再接続してください。問題が解決しない場合は、切断してセッションを再起動してください。
- 外部モニターでビデオを全画面表示に最大化すると、ビデオ品質の問題が発生する場合があります。
- まれに、デスクトップセッション内で、iPadから外部モニターにアプリを移動しようとすると失敗することがあります。回避策として、モニターを一度切断し、再接続してください。問題が解決しない場合は、切断してセッションを再起動してください。
- まれに、サードパーティ製アダプターを使用してiPadを外部モニターに接続すると、表示オプションの下に表示モードが表示されないことがあります。
- VDAセッション内で、マウスポインターの下に線が表示されることがあります。

キーボードのサポート

Altキーの右Optionキーマッピング

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリでは、ユーザーがセッション内で右Optionキーを**Alt**キーにマッピングできる機能強化が導入されました。この新しいオプションは、既存のマッピング（左Optionキー、**Command**または**Windows**キー、両方のOptionキー）を補完し、キーボード構成においてユーザーにより大きな柔軟性を提供します。

右Optionキー(/en-us/citrix-workspace-app-for-ios/media/right-alt-key.png)

キーボードレイアウトの同期

キーボードレイアウトの同期により、ユーザーはクライアントデバイスで優先するキーボードレイアウトを切り替えることができます。この機能はデフォルトで無効になっています。

キーボードレイアウトの同期を有効にするには、［**設定**］ > ［**キーボードオプション**］ に移動し、［**キーボードレイアウトの同期**］ オプションを有効にします。

> **注：**
>
> ローカルキーボードレイアウトオプションを使用すると、クライアントIME（入力方式エディター）がアクティブになります。日本語、中国語、韓国語で作業していて、サーバーIMEを使用したい場合は、［**環境設定**］ > ［**キーボード**］ でオプションをオフにして、ローカルキーボードレイアウトオプションを無効にしてください。

前提条件

- Linux VDAの場合、クライアントキーボードレイアウトの同期とIME改善ポリシーを有効にします。
- Windows VDAの場合、Unicodeキーボードレイアウトマッピング、クライアントキーボードレイアウトの同期、およびIME改善ポリシーを有効にします。
- VDAはバージョン7.16以降である必要があります。

Windows VDAおよびLinux VDAのキーボードレイアウトのサポート

IOSのキーボードレイアウト	キーボード言語	WINDOWSのキーボードレイアウト	LINUXのキーボードレイアウト
ベラルーシ語（ベラルーシ）	ベラルーシ語（ベラルーシ）	ベラルーシ語（ベラルーシ）キーボード	by

IOSのキーボードレイアウト	キーボード言語	WINDOWSのキーボードレイアウト	LINUXのキーボードレイアウト
ブルガリア語	ブルガリア語	ブルガリア語 (タイプライター) キーボード	bg
中国語 (簡体字)	中国語 (簡体字、中国)	Citrix IME - 中国語 (簡体字、中国)	zh
中国語 (繁体字)	中国語 (繁体字、台湾)	Citrix IME - 中国語 (繁体字、台湾)	tw
クロアチア語	クロアチア語 (クロアチア)	クロアチア語キーボード	hr
チェコ語	チェコ語	チェコ語キーボード	cz
デンマーク語	デンマーク語	デンマーク語キーボード	df
オランダ語	オランダ語 (オランダ)	米国-インターナショナルキーボード	us
オランダ語 (ベルギー)	オランダ語	ベルギー (ピリオド) キーボード	be
英語 (オーストラリア)	英語 (オーストラリア)	USキーボード	us
英語 (カナダ)	英語 (カナダ)	USキーボード	us
英語 (英国)	英語 (英国)	英国キーボード	gb
英語(米国)	英語 (米国)	米国キーボード	米国
エストニア語	エストニア語	エストニア語キーボード	エストニア
フィンランド語	フィンランド語	フィンランド語キーボード	フィンランド
フランス語 (カナダ)	フランス語 (カナダ)	フランス語キーボード	fr

IOSのキーボードレイアウト	キーボード言語	WINDOWSのキーボードレイアウト	LINUXのキーボードレイアウト
フランス語 (スイス)	フランス語 (フランス)	スイスフランス語キーボード	スイス
フランス語(フランス)	フランス語 (フランス)	フランス語キーボード	fr
ドイツ語 (オーストリア)	ドイツ語 (オーストリア)	ドイツ語キーボード	at
ドイツ語 (スイス)	ドイツ語 (スイス)	スイスドイツ語キーボード	ch
ドイツ語 (ドイツ)	ドイツ語 (ドイツ)	ドイツ語キーボード	at
ギリシャ語	ギリシャ語	ギリシャ語キーボード	gr
ハンガリー語	ハンガリー語	ハンガリー語キーボード	hu
アイスランド	アイスランド	アイスランド語キーボード	is
アイルランド語	アイルランド語		ie
イタリア語	イタリア語 (イタリア)	イタリア語キーボード	it
日本語	日本語	Citrix IME - 日本語	jp
韓国語	韓国語	Citrix IME - 韓国語	kr
ラトビア語	ラトビア語	ラトビア語キーボード	lv
ノルウェー語	ノルウェー語 (ブークモール)	ノルウェー語キーボード	いいえ
ポーランド語	ポーランド語	ポーランド語 (プログラマー用) キーボード	pl

IOSのキーボードレイアウト	キーボード言語	WINDOWSのキーボードレイアウト	LINUXのキーボードレイアウト
ポルトガル語 (ブラジル)	ポルトガル語 (ブラジル)	ポルトガル語 (ブラジル ABNT) キーボード	br
ポルトガル語 (ポルトガル)	ポルトガル語 (ポルトガル)	ポルトガル語キーボード	pt
ルーマニア語	ルーマニア語 (ルーマニア)	ルーマニア語 (レガシー) キーボード	ro
ロシア語 (ロシア)	ロシア語	ロシア語キーボード	ru
スロバキア語	スロバキア語	スロバキア語キーボード	sk
スロベニア語	スロベニア語	スロベニア語キーボード	si
スペイン語 (メキシコ)	スペイン語 (メキシコ)	ラテンアメリカキーボード	ラテンアメリカ
スペイン語 (スペイン)	スペイン語 (スペイン)	スペイン語キーボード	es
スウェーデン語 (スウェーデン)	スウェーデン語 (スウェーデン)	スウェーデン語キーボード	se
トルコ語	トルコ語	トルコ語Fキーボード	tr
ウクライナ語	ウクライナ語	ウクライナ語キーボード	ua

特殊キーのサポート

iOS 13.4以降の外部キーボードにおける、以下の単一キーのサポート：

- PageUp
- PageDown
- ホーム

- End
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

特殊なキーの組み合わせのサポート

このリリースでは、iOS外部キーボードで以下のキーの組み合わせがサポートされます。

- ウィンドウズ + R
- ウィンドウズ + D
- ウィンドウズ + E
- ウィンドウズ + L
- ウィンドウズ + M
- ウィンドウズ + S
- ウィンドウズ + CTRL + S
- ウィンドウズ + T
- ウィンドウズ + U
- Windows + 数字
- Windows + アップ
- Windows + ダウン
- Windows + レフト
- Windows + ライト

- ウィンドウズ + X
- ウィンドウズ + K
- CTRL + ESC

拡張キーボードの機能強化

バージョン23.5.0以降、拡張キーボード機能が強化され、より良いユーザーエクスペリエンスが提供されるようになりました。以下にその機能強化を示します。

- 拡張ツールバーUIをピン留めまたはピン留め解除する。
- 画面の回転に合わせて拡張ツールバーを回転させる。
- Windowsアイコンキーと3キーの組み合わせショートカットをサポート。
- マルチモニター使用シナリオでのエクスペリエンスを向上。
- 拡張ツールバーUIを自動的に開くまたは折りたたむ。
- Stage Managerモード（M1チップ搭載iPadの場合）でのエクスペリエンスを向上。

IMEユーザーインターフェイス

一般的に、IMEは候補ウィンドウや変換ウィンドウなどのUIコンポーネントを提供します。変換ウィンドウには、変換中の文字や、下線や背景色などの変換UI要素が含まれます。候補ウィンドウには、候補リストが表示されます。

IME UI(/en-us/citrix-workspace-app-for-ios/media/ime-ui.png)

変換ウィンドウを使用すると、確定された文字と変換中の文字を区別できます。変換ウィンドウと候補ウィンドウは、入力カーソルに合わせて移動します。

その結果、この機能は以下を提供します。

- 変換ウィンドウのカーソル位置での文字入力の強化。
- 変換ウィンドウと候補ウィンドウでの表示の強化。

現在、この機能はWindows VDAでホストされているセッションで使用でき、ソフトウェアキーボードと外部物理キーボードの両方をサポートしています。

東アジア言語用汎用クライアントIME

汎用クライアント入力方式エディター（IME）機能は、iOSデバイスでの中国語、日本語、韓国語（CJK）の文字入力と表示エクスペリエンスを向上させます。この機能により、クライアントIMEを使用してセッション中にカーソル位置でCJK文字を構成できます。この機能はWindows VDA環

境で利用できます。より良いユーザーエクスペリエンスのために、VDA側のIMEではなくクライアントIMEを使用することをお勧めします。

前提条件

- グループポリシーを使用して、Windows VDAで「クライアントキーボードレイアウトの同期とIMEの改善を有効にする」および「Unicodeキーボードレイアウトマッピングを有効にする」を有効にします。

  キーボードIME(/en-us/citrix-workspace-app-for-ios/media/keyboard-ime.png)

詳細については、Knowledge Centerの記事CTX312404を参照してください。

Windows VDAで以下のレジストリを使用してオプションを有効にすることもできます。

```
-   HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0

-   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value = DWORD 1

-   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value =
DWORD 1
```

- Citrix Workspaceアプリから、**設定** > **キーボードオプション** > **キーボードレイアウトの同期**オプションを有効にします。

スキャンコード入力モードのサポート

24.1.0リリース以降、外部物理キーボードを使用する際に、キーボード入力モードとして**スキャンコード**を選択できるようになりました。この機能は、iOSデバイスを外部Windows PCの標準キーボードと組み合わせて使用する場合に役立ちます。**スキャンコード**を使用すると、iOSのキーボードではなくVDAのキーボードレイアウトを使用できます。この方法により、iOSではなく外部Windowsキーボードの入力スタイルに完全に従うことができます。東アジア言語で入力する場合に特に有効で、全体的なユーザーエクスペリエンスが大幅に向上します。エンドユーザーは、クライアントではなくサーバーのキーボードレイアウトを使用していることに気づくかもしれません。詳細については、この記事のユースケースセクションを参照してください。

スキャンコード機能を使用するには、次の手順を実行します。

1. iOS向けCitrix Workspaceアプリを開き、**設定 > キーボードオプション**に移動します。
2. **外部キーボードの入力モード**をタップします。 

3. 次のいずれかのオプションを選択します。

   - **スキャンコード:** クライアント側のキーボードからVDAにキー位置を送信し、VDAが対応する文字を生成します。サーバー側のキーボードレイアウトが適用されます。
   - **Unicode:** クライアント側のキーボードからVDAにキーを送信し、VDAがVDA内で同じ文字を生成します。クライアント側のキーボードレイアウトが適用されます。

   デフォルトでは、ソフトウェアキーボードまたはタッチキーボードと外部キーボードの両方で、入力モードとして**Unicode**が選択されています。

4. **スキャンコード**をタップします。

   セッション中に、リモート、サーバー、またはVDAのキーボードレイアウトを切り替え、リモート、サーバー、またはVDAのキーボードレイアウトで入力できます。

ユースケース

たとえば、iOSデバイスに接続されたUSインターナショナルキーボードレイアウトを使用しているシナリオを考えてみましょう。 **スキャンコード**を選択し、外部キーボードのCapsLockの隣にあるキーを入力すると、**スキャンコード 1E**がVDAに送信されます。その後、VDAは**1E**を使用して文字**a**を表示します。 **Unicode**を選択し、外部キーボードのCapsLockの隣にあるキーを入力すると、文字**a**がVDAに送信されます。そのため、VDAが同じ位置に異なる文字を持つ別のキーボードレイアウトを使用している場合でも、文字**a**が画面に表示されます。

> **注：**
>
> モバイルデバイスでタッチキーボードを使用する場合、**Unicode**が推奨される入力モードです。タッチキーボードのキーは通常、スキャンコードを生成しないためです。

外部キーボードショートカットのサポートの機能強化

バージョン24.1.0以降、iOS向けCitrix Workspaceアプリでは、リモートデスクトップまたはアプリセッション中に外部キーボードからより多くのショートカットを使用できるようになりました。外部キーボードショートカットに加えられた重要な改善点は次のとおりです。

- **Insert**、**Delete**、テンキーなど、Windowsキーボード固有のキーのサポート。
- キーを押し続けて離さない場合、リモートデスクトップ/アプリは正しく応答します。
- 3つ以上のキーを使用するショートカットをサポートします。

さらに、**設定 > キーボードオプション > Altに特定のキーを割り当てる** を介して、以下のオプションを使用して **Alt** の特定のキーを設定できるようになりました。

- **OptionまたはAlt (左)**: **Option (左) またはAlt (左)** を使用して **Alt** を送信します。
- **CommandまたはWindows (左)**: **Command (左) またはWindows (左)** キーを使用して **Alt** を送信します。
- **OptionまたはAlt (左右)**: **OptionまたはAlt (左右)** キーを使用して **Alt** を送信します。

Altに特定のキーを割り当てる オプションは、macOSの **Option** キーとWindowsの **Alt** キー間の競合を回避するのに役立ちます。

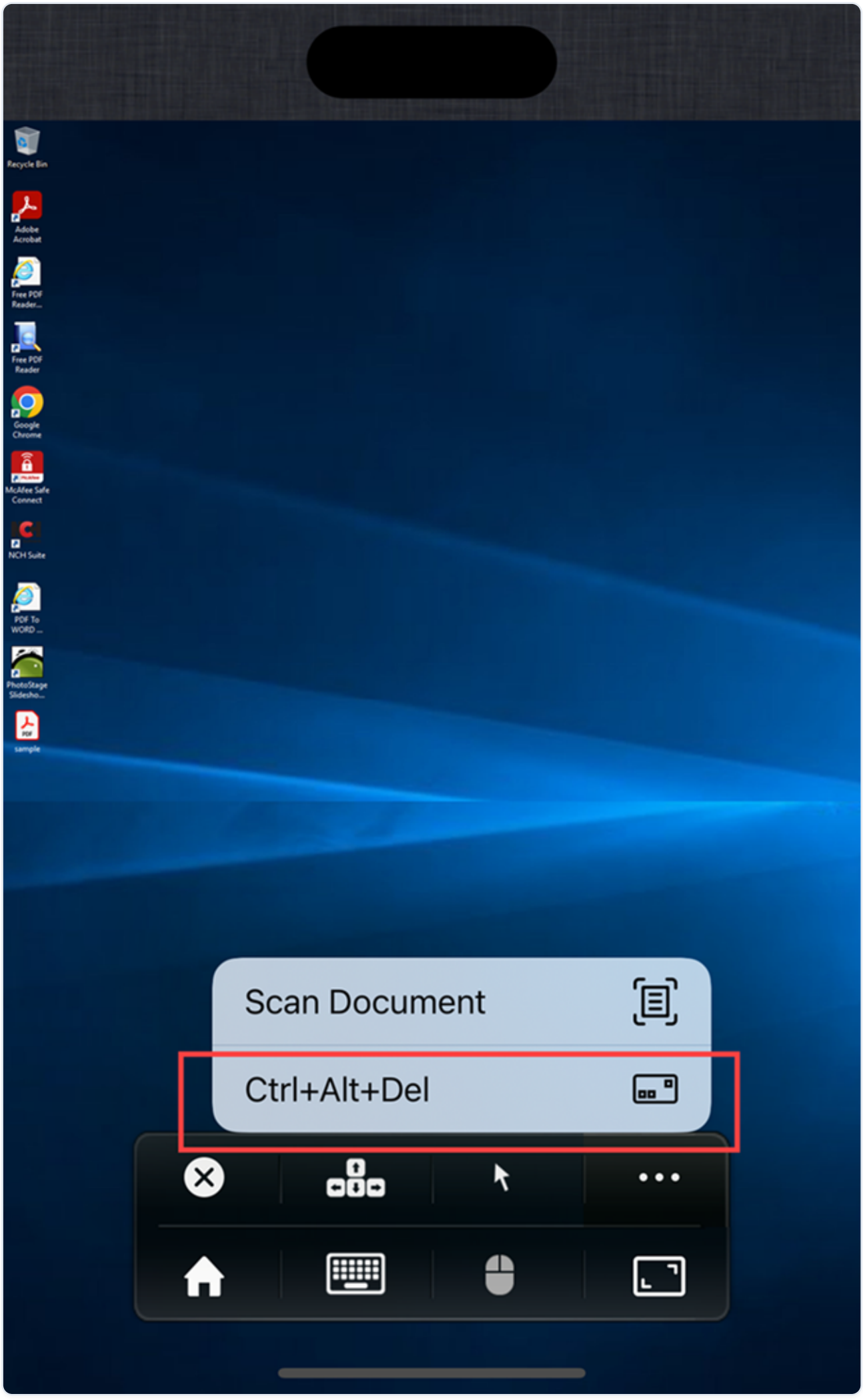
制限事項

現在、以下のiOSシステムショートカットはサポートされていません。

- **Command (Windows)-H**: ホーム画面に移動します。
- **Command (Windows)-Space bar**: 検索フィールドを表示または非表示にします。
- **Command (Windows)-Tab**: 開いているアプリの中から、次に最も最近使用したアプリに切り替えます。
- **Command (Windows)-Shift-3**: スクリーンショットを撮ります。
- **Command (Windows)-Shift-4**: スクリーンショットを撮り、すぐにマークアップを開いて表示または編集します。
- **Command (Windows)-Option (Alt)-D**: Dockを表示または非表示にします。
- **Command (Windows)-Ctrl-Q**: デバイスをロックします。
- ヨーロッパキーボードの **AltGr** はサポートされていません。**AltGr** を使用して特殊文字を入力したい場合は、代わりに以下のショートカットを使用してください。
  - macOS の **Option+*** ショートカット、または
  - Windows OS の **Alt + 数字パッドショートカット**。

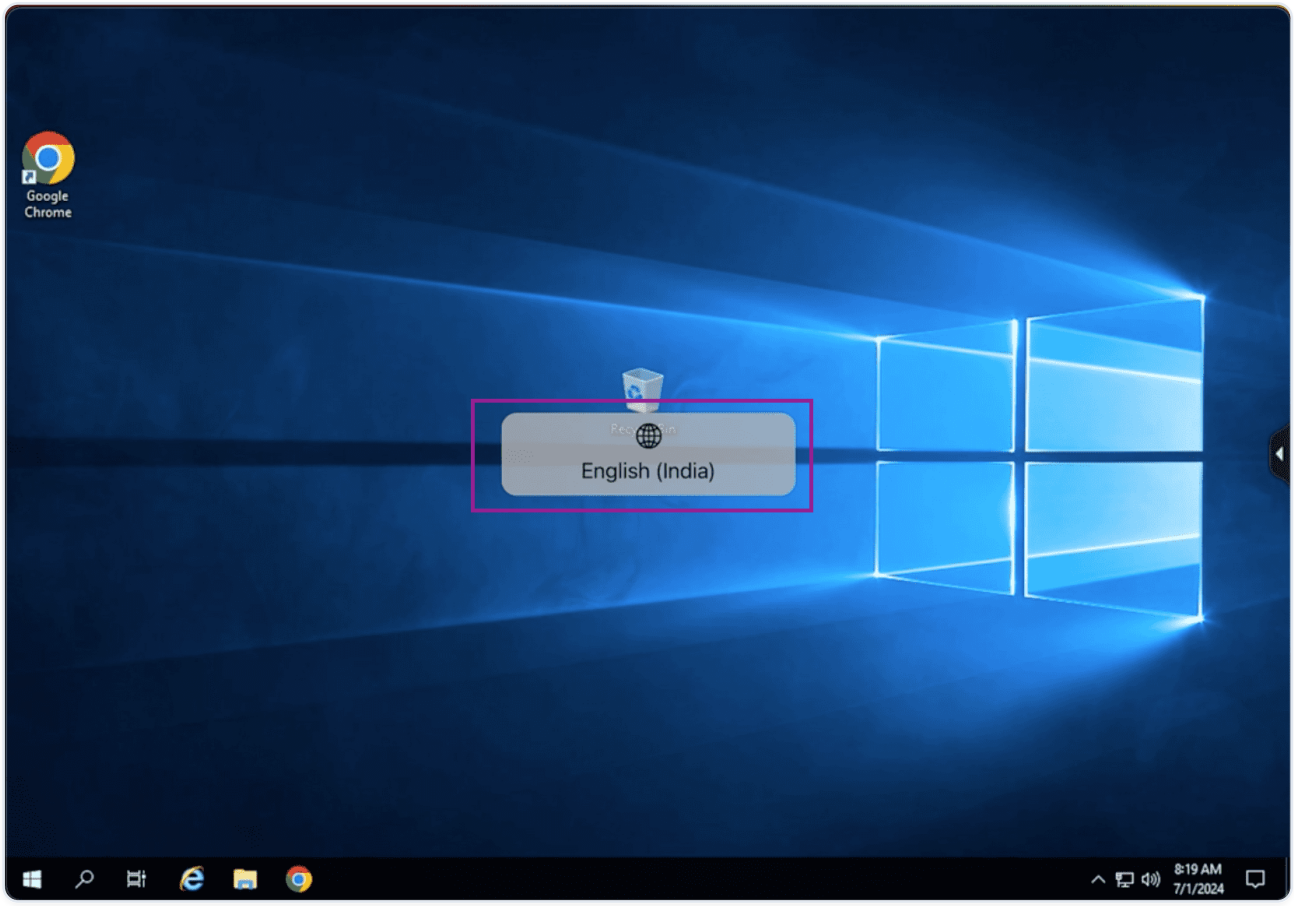
セッションツールバーへの Ctrl+Alt+Del ショートカットの追加

このバージョン以降、セッションツールバーに、ボタンをタップするだけで **Ctrl+Alt+Del** 機能を実行できるオプションが追加されました。このオプションにより、ユーザーはサインアウト、ユーザー切り替え、システムのロック、またはタスクマネージャーへのアクセスが容易になります。


Recycle Bin
Adobe Acrobat
Free PDF Reader...
Free PDF Reader
Google Chrome
McAfee Safe Connect
NCH Suite
PDF To WORD ...
PhotoStage Slidesho...
sample
Scan Document
Ctrl+Alt+Del

仮想セッションでのキーボード言語変更の検出と表示

バージョン24.7.0以降、Citrix Workspaceアプリ for iOSは、ユーザーがキーボード言語を切り替えると、仮想セッション内でメッセージを自動的に検出して表示するようになりました。デバイスキーボードまたは外部キーボードの地球儀キーを使用してキーボード言語を切り替えると、現在のキーボード言語を通知するメッセージが画面に表示されます。この機能により、仮想セッション内で現在のキーボード言語を確実に把握できます。



マイクとカメラへのアクセス

VDAセッションを介して、オーディオビデオ会議のためにマイクとカメラにアクセスできるようになりました。Citrix Workspaceアプリは、マイクまたはカメラにアクセスするために許可を必要とします。これは、デバイスの に移動し、カメラまたはマイクを有効にすることで提供できます。

また、クライアント選択的信頼セキュリティ機能の一部として、ストアごとのマイクとカメラへのアクセスが含まれており、Citrix WorkspaceアプリがVDAセッションからのアクセスを信頼できるようにしています。

Citrix Workspaceアプリは、マイクまたはカメラにアクセスするためにユーザーの許可を必要とします。

> に移動して、アクセスレベルを設定できます。 メニューで、ストアをクリックして、必要なマイクまたはカメラへのアクセスを有効にします。マイクまたはカメラへのアクセスの選択された設定は、ストアごとに適用されます。

外部Webカメラのサポート

Citrix Workspace app for iOS は、DaaS セッション内で外部接続されたウェブカメラをサポートするようになりました。USB 経由でウェブカメラを接続し、カメラアイコンをクリックして「**External Webcam**」オプションを選択することで、ビデオ会議に利用できます。これにより、エンドユーザーが利用できるリソースを使用してセッションエクスペリエンスが向上します。

> **注：**
>
> - External Webcam は、USB-C コネクタを搭載し、iOS 17 以降を実行している iPad でのみサポートされています。
> - External Webcam オプションは、外部カメラが検出された後にのみ表示されます。
> - クライアントアプリの設定は、HDX セッション内のカメラには影響しません。カメラの位置を切り替えるには、Citrix によって有効化されたカメラフローティングボタンを使用する必要があります。

> 外部ウェブカメラ(/en-us/citrix-workspace-app-for-ios/media/external-webcam.png)

次回ビデオ会議アプリを使用する際、システムはユーザーの設定を記憶し、それに応じてカメラ設定を使用します。たとえば、前回のビデオ通話を **External Webcam** の設定で終了した場合、次回は External Webcam がデフォルトで選択されます。

画面上のカメラアイコンをタップすることで、カメラ設定を変更できます。通話中にカメラ設定を変更することも可能です。

この機能は、クラウドおよびオンプレミスストアの両方の顧客が利用できます。

アクセシビリティと VoiceOver のサポート

バージョン 24.9.0 以降、Citrix Workspace app for iOS はアクセシビリティと VoiceOver 機能をサポートしています。この機能は、画面が見えにくいエンドユーザーを支援します。Citrix Workspace および仮想セッション UI を使用する際、ナレーターが画面要素を読み上げます。

VoiceOver 機能を有効にするには、iOS の **設定 > アクセシビリティ > VoiceOver** に移動してオンにします。

Citrix Workspace アプリを操作するには、iOS が提供するアクセシビリティ標準ジェスチャを使用する必要があります。たとえば、画面を左右にスワイプしてメニュー間を移動すると、各項目のボイスオーバーが再生されます。詳細については、Apple サポートドキュメントの iPhone のアクセシビリティ機能の概要 および iPad のアクセシビリティ機能の概要 を参照してください。

複数のオーディオデバイスのサポート

バージョン 24.7.0 以降、Citrix Workspace app for iOS は、仮想デスクトップセッションにローカルで接続されているすべての利用可能なオーディオデバイスの表示をサポートしています。この機能により、仮想デスクトップセッション内でオーディオデバイスを切り替えることができます。デバイス設定でローカルにオーディオデバイスを切り替えると、変更は仮想デスクトップセッションに自動的に適用されます。この機能は、プラグアンドプレイデバイスでもサポートされています。

複数のオーディオデバイス(/en-us/citrix-workspace-app-for-ios/media/multiple-audio-devices.png)

制限事項

- スピーカーのみ、マイクのみのデバイスはサポートされていません。
- AppleのAirPlayデバイスはサポートされていません。
- この機能は、仮想セッションでBluetoothデバイスまたは有線ヘッドセットデバイスのいずれかを一度にサポートします。

アダプティブオーディオのサポート

24.5.0以降、iOS向けCitrix WorkspaceアプリはHDXアダプティブオーディオをサポートしています。この機能は、オーディオ品質の向上と低遅延により、ユーザーエクスペリエンスを向上させます。

詳細については、Citrix Virtual Apps and Desktopsのドキュメントにあるオーディオポリシー設定の記事を参照してください。

背面カメラのサポート

バージョン23.2.0以降、iOS向けCitrix Workspaceアプリは、HDXセッション内でカメラの位置を前面から背面へ、またはその逆に切り替えることをサポートするようになりました。

仮想セッションでカメラを起動すると、カメラの位置を切り替えるためのカメラフローティングボタンが画面に表示されます。フローティングボタンは画面上で自由に移動させ、どこにでも配置できます。

仮想セッションでカメラの位置を前面と背面の間で切り替えるには、次の手順を実行します。

1. ビデオをキャプチャするクライアントアプリを開きます。
2. ビデオ録画を開始します。
3. 画面に表示されるカメラフローティングボタンをタップして、前面カメラと背面カメラを切り替えます。

> **注：**
>
> クライアントアプリの設定は、HDXセッション内のカメラには影響しません。カメラの位置を切り替えるには、Citrixによって有効化されたカメラフローティングボタンを使用する必要があります。

既知の問題

キャスティング機能またはドキュメントスキャン機能が有効になっている場合、フローティングボタンは部分的にまたは完全に遮られます。

グラフィックとディスプレイ

グラフィックパフォーマンスの向上

バージョン24.1.0以降、Citrix Workspaceアプリ for iOSは、ハードウェアアクセラレーションによるH.264ビデオのエンコードまたはデコードをサポートしています。Citrix HDXのマルチメディアエンジンは、AppleのVideo Toolboxフレームワークを使用してエンコードとデコードを行うようになりました。このフレームワークは、ビデオをより高速かつリアルタイムで圧縮および解凍します。この機能強化により、マルチメディア使用時のCPUへの負荷が軽減されます。

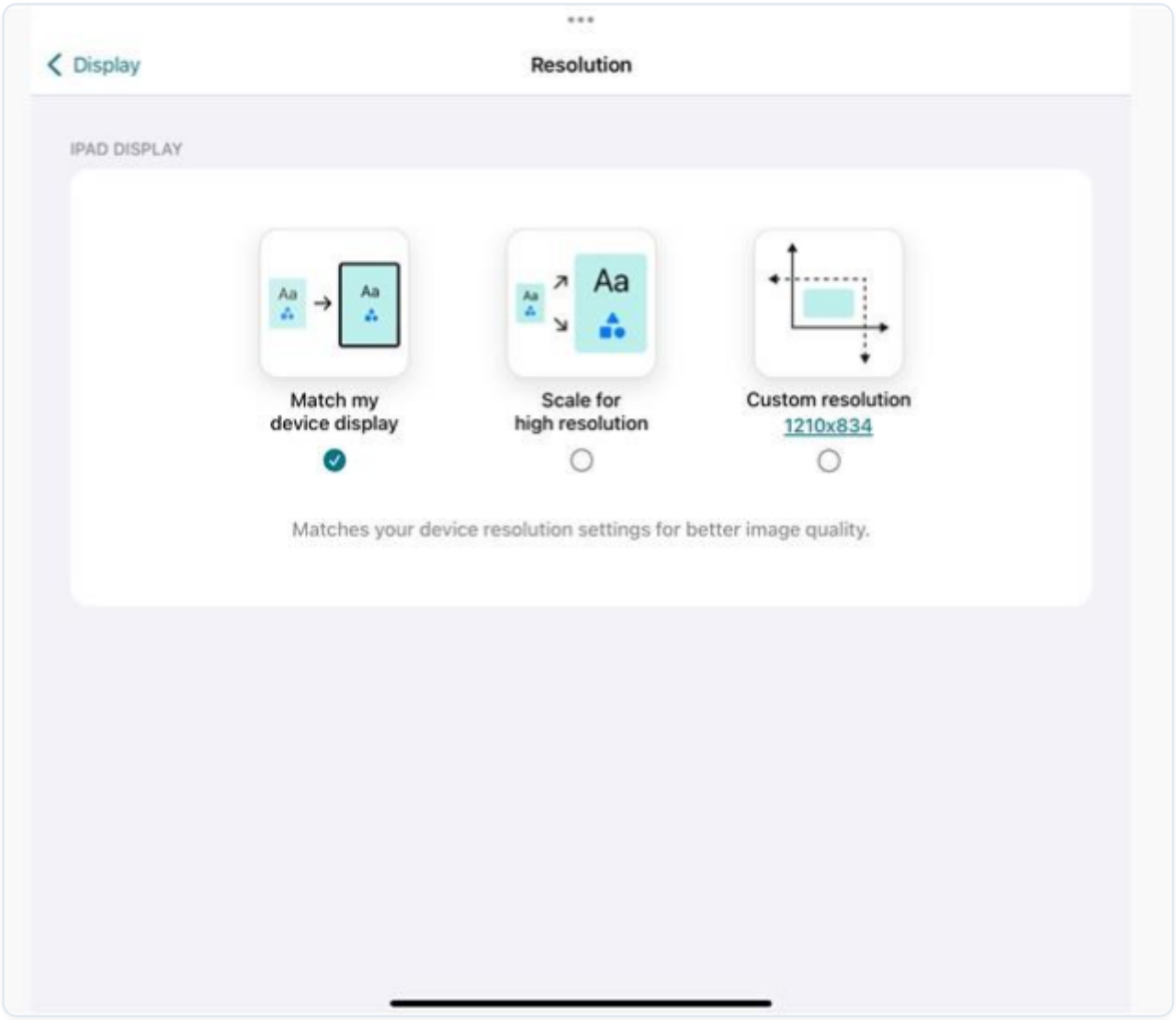
グラフィック設定のネイティブiOS設定との自動同期

新しく追加された**デバイスのディスプレイに合わせる**オプションは、iOS設定からDPIスケールを自動的に読み取るため、解像度を手動で設定する必要はありません。外部ディスプレイの場合、アプリは解像度リストを5つの統合されたオプションに置き換えます。この更新により、構成の複雑さが軽減され、よりネイティブなディスプレイエクスペリエンスが提供されます。

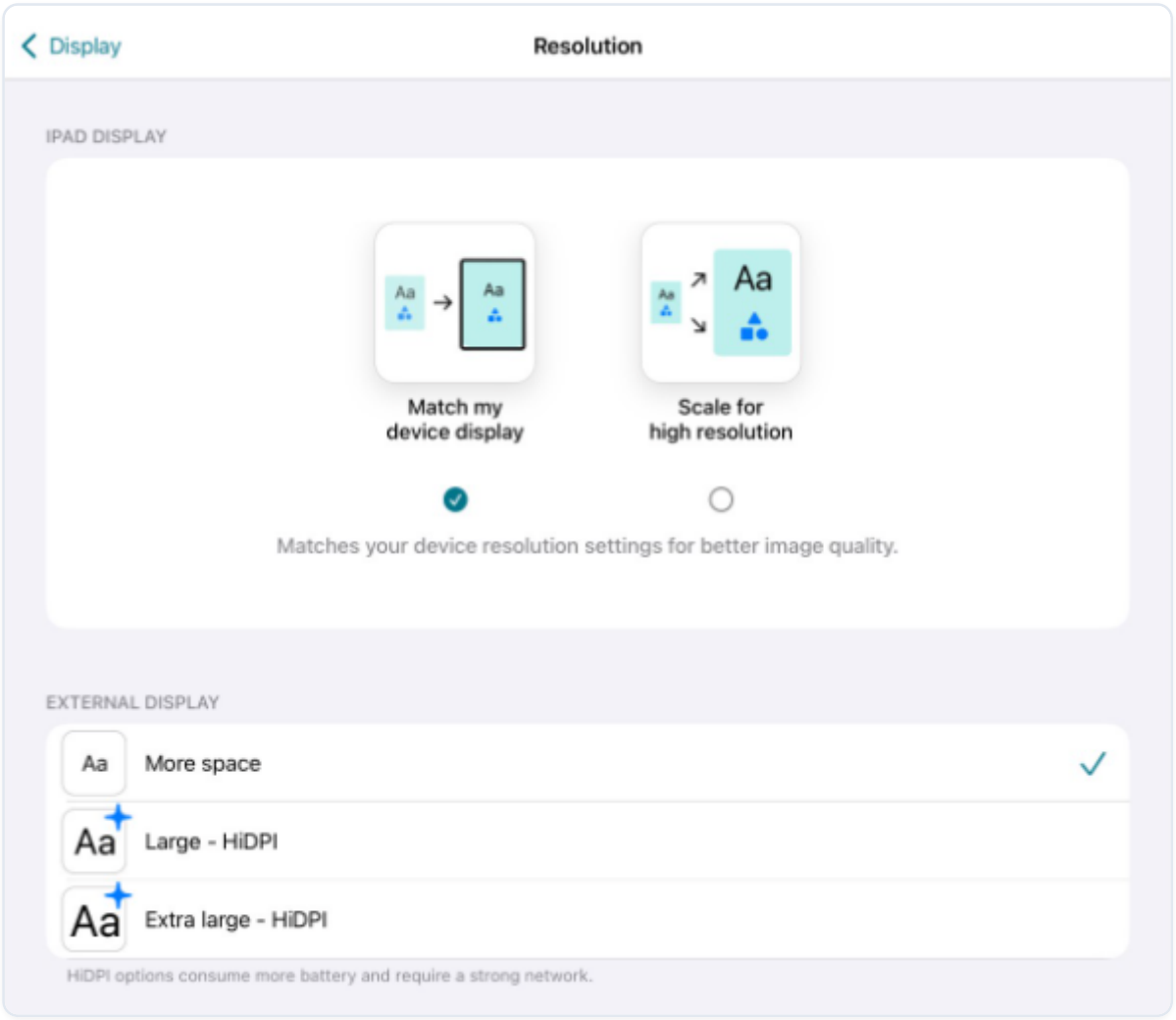
この機能を使用するには、**設定** > **表示オプション** > **解像度**に移動します。

以下のスクリーンショットは、iPhoneとiPadの表示オプションを示しています。

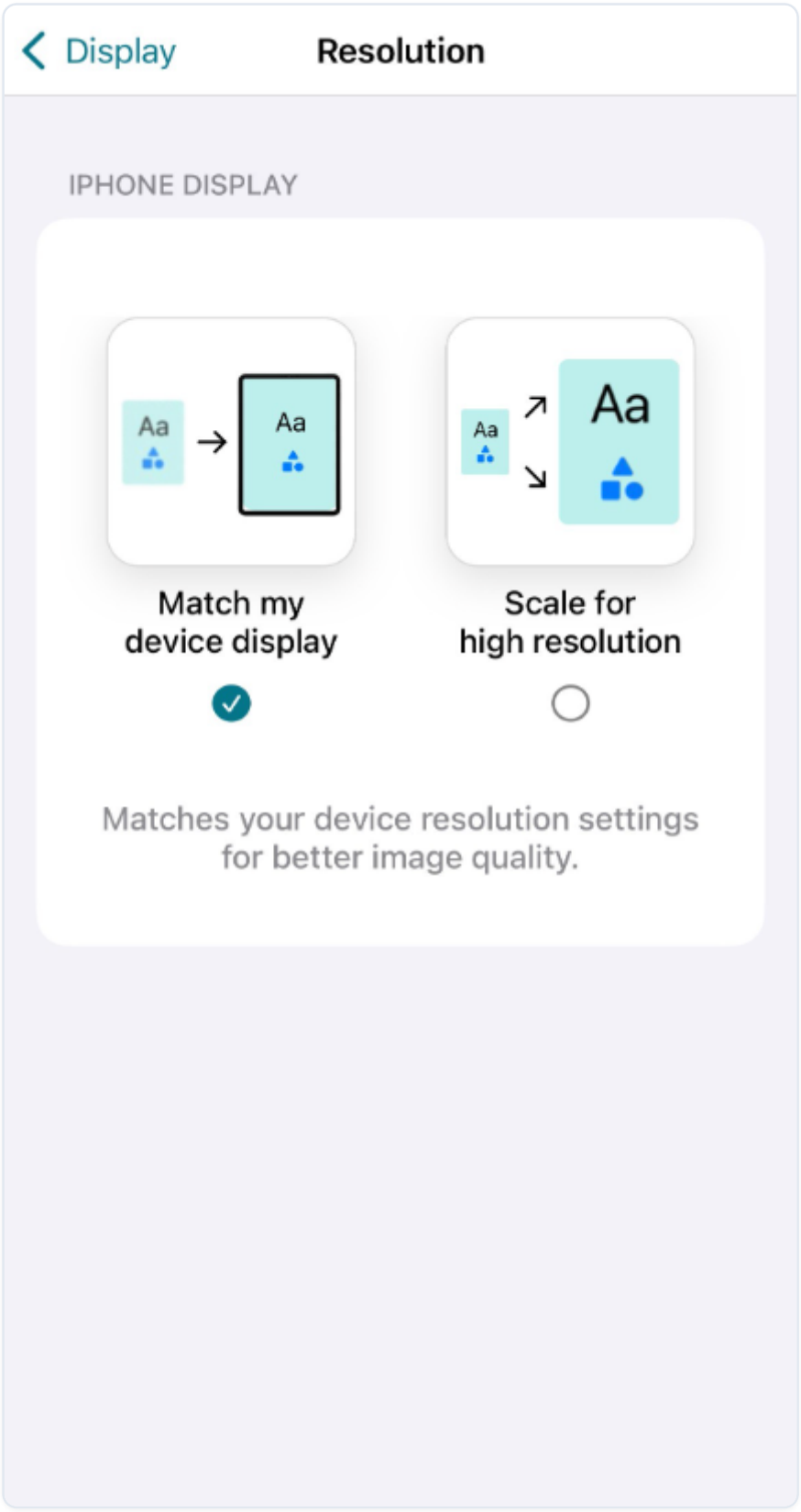
- メインディスプレイの解像度オプション。



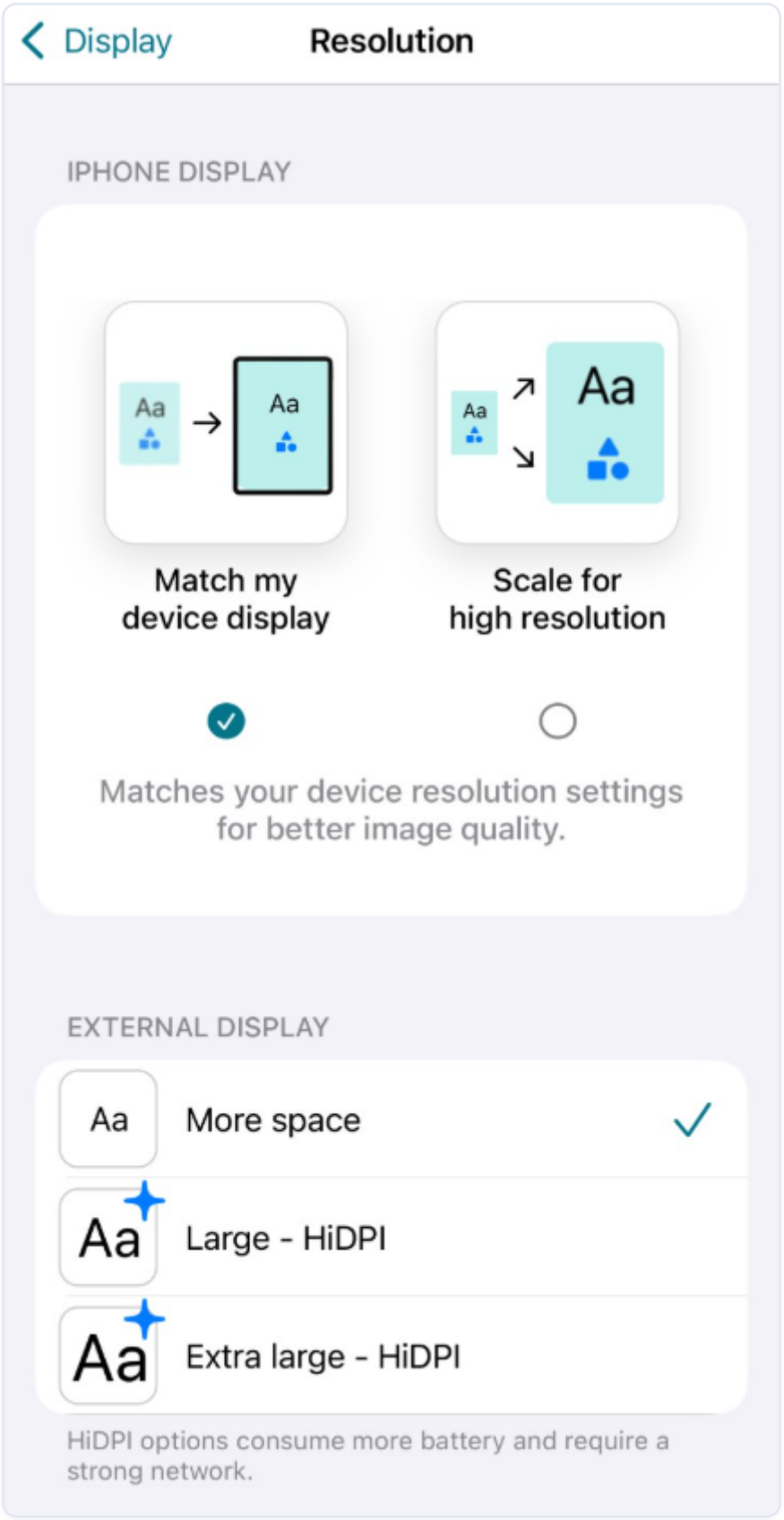
- 外部ディスプレイの解像度オプション。



- メインディスプレイの解像度オプション。



- 外部ディスプレイの解像度オプション。



クライアントドライブマッピング (CDM)

設定されたストアごとに、特定のデバイスストレージアクセスを選択できます。デバイスストレージアクセスには、次のオプションがあります。

- アクセスなし
- 読み取り専用アクセス
- 読み取りおよび書き込みアクセス
- 毎回確認する

毎回確認するを選択すると、起動するたびにデバイスストレージアクセスの種類を選択するよう求めるプロンプトが表示されます。デフォルトでは、**アクセスなし**オプションが選択されています。

> **注：**
>
> この機能は、直接ICA®起動およびCitrix Gatewayで構成されたストアにのみ適用されます。エンドツーエンドのSSL設定がないストアはサポートされていません。

> **デバイスストレージ**設定は、設定内の新しいセクションである**ストア設定**の下にあります。**デバイスストレージ**を表示するには、**設定** > **ストア設定**に移動します。

Citrix Ready® ワークスペースハブ

Citrix Ready workspace hubは、デジタル環境と物理環境を組み合わせて、安全なスマートスペース内でアプリとデータを提供します。この完全なシステムは、モバイルアプリやセンサーなどのデバイス（またはモノ）を接続し、インテリジェントで応答性の高い環境を作り出します。

Citrix Ready workspace hubは、Raspberry Pi 3プラットフォーム上に構築されています。Citrix Workspaceアプリを実行しているデバイスは、Citrix Ready workspace hubに接続し、アプリまたはデスクトップをより大きなディスプレイにキャストします。

Citrix Ready workspace hubの詳細については、Citrix Ready workspace hubのドキュメントを参照してください。

Citrix Ready workspace hubは、セキュリティ目的でモバイルデバイスとハブ間のSecure Sockets Layer (SSL) 接続をサポートしています。各デバイスを一意に識別するために、手動または自動で完全修飾ドメイン名 (FQDN) を設定します。詳細については、Citrix Ready workspace hubドキュメントのセキュリティ接続を参照してください。

Citrix Ready workspace hubは、以下のすべてのシステム要件が満たされている場合にCitrix Workspaceアプリで有効になります。

- Citrix Workspaceアプリ 1810.1 for iOS以降

- Bluetoothが有効になっている
- モバイルデバイスとワークスペースハブが同じWi-Fiネットワークを使用している

Citrix Ready workspace hubを構成する

Citrix Ready workspace hub機能を有効にするには、**設定**に移動し、**Citrix Casting**をタップしてデバイスで機能を有効にします。詳細については、iOSデバイスのヘルプドキュメントを参照してください。

Citrix Workspaceアプリは、iOSデバイスの信頼済みリストからワークスペースハブを追加または削除するための新しい手順を統合しています。詳細については、Security Connectionを参照してください。

ドキュメントスキャナーのサポート

バージョン24.5.0以降、iOS版Citrix Workspaceアプリはドキュメントスキャナー機能をサポートしています。この機能を使用すると、デスクトップセッション内で複数のドキュメントをスキャンして保存できます。この機能はデフォルトで有効になっています。

前提条件

- ストアに対してクライアントドライブマッピング (CDM) を有効にする必要があります。
- ドキュメントスキャナー機能には、デバイスへの読み取り/書き込みアクセスが必要です。アクセスを有効にするには、次の手順に従います。

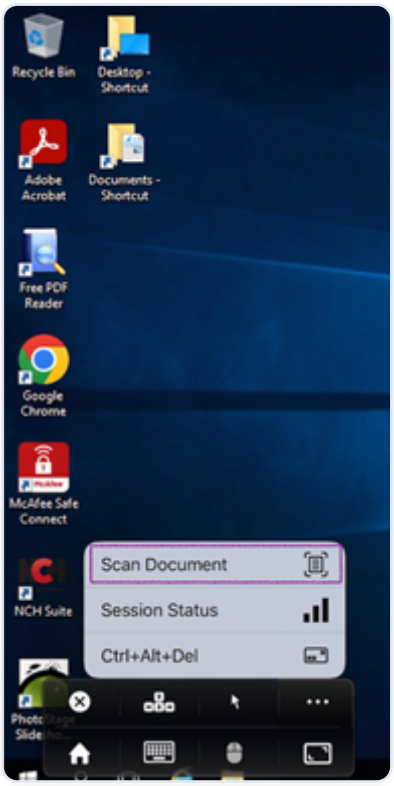
  a. プロファイルから、**アプリケーション設定 > ストア設定**をタップします。

  b. 現在のストアをタップします。

  c. **デバイスストレージ**をタップし、**フルアクセス**を選択します。

ドキュメントスキャナーを使用してドキュメントをスキャンするには、次の手順を実行します。

1. セッション内ツールバーから、省略記号メニューをタップし、**ドキュメントのスキャン**を選択します。カメラアプリが開きます。



2. シャッターボタンをタップして写真をキャプチャします。もう一度キャプチャする場合は、**再撮影**をタップします。

   画像をキャプチャ(/en-us/citrix-workspace-app-for-ios/media/capture-image.png)

3. オプション：スキャンしたドキュメントをトリミングします。必要なサイズにトリミングしたら、**スキャンを保持**をタップします。カメラアプリが再度開き、さらに画像をキャプチャできます。

   スキャンを保持(/en-us/citrix-workspace-app-for-ios/media/keep-scan.png)

4. 必要な画像をキャプチャしたら、**保存**をタップします。

   画像を保存(/en-us/citrix-workspace-app-for-ios/media/save-image.png)

5. スキャンしたドキュメントを必要な形式で保存するには、ファイル形式オプションを選択します。

   ファイル形式を選択(/en-us/citrix-workspace-app-for-ios/media/select-file-format.png)

6. **OK**をタップします。

   スキャンされたドキュメント(/en-us/citrix-workspace-app-for-ios/media/scanned-document.png)

すべてのスキャンされたドキュメントは、デバイスのローカルストレージにある**CitrixScannedDocuments**フォルダー内でアクセスできます。セッションファイルマネージャーからも**CitrixScannedDocuments**にアクセスできます。

セッションファイルマネージャー(/en-us/citrix-workspace-app-for-ios/media/session-file-manager.png)

AirPrint対応プリンターのサポート

バージョン23.9.0以降、エンドユーザーはAirPrintテクノロジー対応プリンターを使用して、iOSデバイスのアクティブなセッションからドキュメントを印刷できるようになりました。これにより、ケーブルやネットワーク経由でプリンターを接続する必要がなくなります。ユーザーが印刷コマンドを開始すると、AirPrint対応プリンターが他の利用可能なプリンターとともに一覧表示されます。

AirPrint対応プリンターを使用して印刷するには、ユーザーは以下を確認する必要があります。

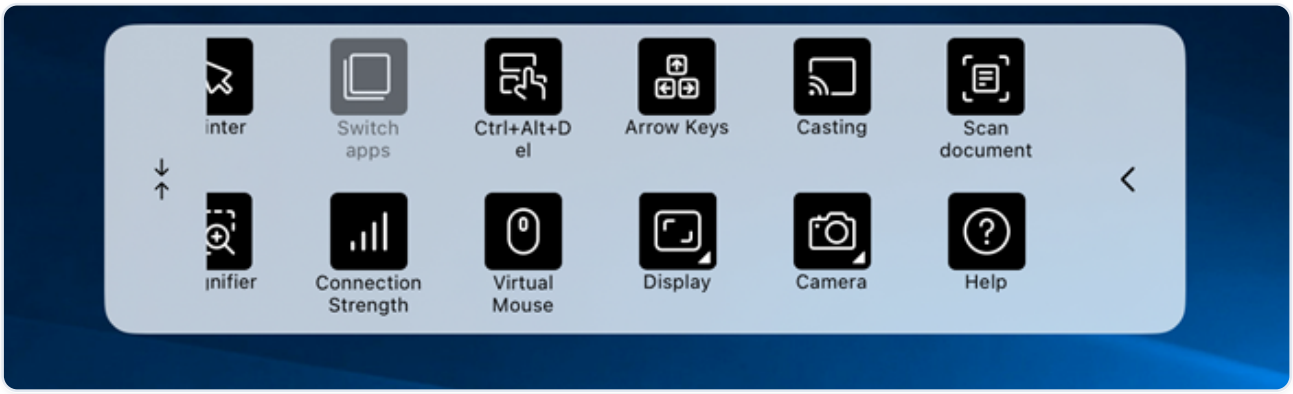
- 必要なプリンターはAirPrint互換で、AirPrintに対応している必要があります。
- ユーザーのデバイスは、AirPrint対応プリンターと同じWi-Fiネットワークに接続されている必要があります。

この機能は、クラウド環境とオンプレミス環境の両方で、iOSプラットフォームで利用できます。

ユーザーエクスペリエンス

新しいセッション内ツールバー

バージョン25.3.0以降、Global App Configurationサービス（GACS）およびモバイルデバイス管理（MDM）を介して管理者設定が構成されていない場合、新しいツールバーはデフォルトで有効になります。



クロス複数画面エクスペリエンスの強化

バージョン25.1.0以降、iOS向けCitrix Workspaceアプリは、外部モニターまたはドックに接続されたiPadのユーザーエクスペリエンスを向上させます。これらの更新には、マルチタスクを改善するために複数の画面にアプリケーションを分散する機能が含まれます。この機能はデフォルトで有効になっています。

ユーザーは、外部モニターとiPadのネイティブ画面の両方で利用可能なさまざまな解像度から選択でき、多様な好みに対応できます。複数の画面構成は、ローカルアプリとセッションを切り替える際にも保持され、継続性と生産性を確保します。この機能は、Stage Managerによって引き起こされるマウスロックの問題も解決します。

前提条件:

iPadでStage Managerを有効にする必要があります。

制限事項:

ユーザーがCitrix Workspace™アプリを外部ディスプレイで直接起動すると、フルスクリーンモードに切り替えたときに解像度リストが空になります。これはiOSシステムの欠陥が原因で発生し、Citrix Workspaceアプリはスクリーンショットに示すように、**外部ディスプレイを検出できません**という警告を表示します。

外部ディスプレイの警告(/en-us/citrix-workspace-app-for-ios/media/external-display-warning.png)

フルスクリーンモードでサポートされている外部ディスプレイ解像度の一覧：

外部ディスプレイの解像度(/en-us/citrix-workspace-app-for-ios/media/external-display-resolution.png)

セッションが外部ディスプレイでフルスクリーンモードに入ると、トーストメッセージが表示され、以下の画像に示すように、マルチモニター機能を使用したい場合はCitrix Workspaceアプリのウィンドウをiパッド画面に戻すようユーザーに促します。

トーストメッセージ(/en-us/citrix-workspace-app-for-ios/media/toast-message.png)

Spotlight検索の強化

アプリのアイコンが対応するアプリ検索と一致するようになりました。以前は、すべての検索でCitrix Workspaceアプリのアイコンが表示されていました。

Spotlight検索(/en-us/citrix-workspace-app-for-ios/media/spotlight-search.png)

3D Touchジェスチャによる最近使用したアプリへのアクセス

Citrix Workspaceアプリのアイコンで3D Touch (長押し) ジェスチャを使用すると、最近起動したアプリのリストにすばやくアクセスできます。

バッテリーステータスインジケーター

仮想デスクトップセッション内の通知領域に、デバイスのバッテリー状態が表示されるようになりました。

この機能は、VDAバージョン7.18以降でのみサポートされています。

> **注：**
>
> Microsoft Windows 10 VDAで実行されているセッションでは、バッテリー状態インジケーターが表示されるまでに約1〜2分かかる場合があります。

リソースにアクセスするための長押し機能

Citrix Workspaceアプリのアイコンを長押しして、最近起動したリソースにアクセスできるようになりました。Citrix Workspaceアプリを終了して、最近起動したリソースにアクセスできるようになりました。

ページ内検索機能の強化

ページ内検索機能の強化により、単語や語句を検索できます。このユーザビリティ強化は、WebアプリおよびSoftware-as-a-Service (SaaS) アプリ内で適用されます。

検索するには：

1. iPadで、右上隅にある省略記号 (...) ボタンをタップし、 を選択します。

iPadのページ内検索(/en-us/citrix-workspace-app-for-ios/media/ipadpage.png)

iPhoneで、右下隅にある省略記号 (...) ボタンをタップし、 を選択します。

iPhoneのページ内検索(/en-us/citrix-workspace-app-for-ios/media/iphonepage.png)

画面キーボードが表示されます。

キーボード(/en-us/citrix-workspace-app-for-ios/media/keyboard.png)

1. 検索したいテキストをテキストボックスに入力します (例: 「Citrix®」と入力します)。検索結果が表示されます。

検索結果(/en-us/citrix-workspace-app-for-ios/media/searchresult.png)

セッション内ツールバーを再配置する

セッション内ツールバーは、画面の上部または右側に再配置できます。ツールバーのノッチをツールバーの端からドラッグすると、長方形のドラッグインジケーターとドロップターゲットが表示されます。ドラッグインジケーターをドロップターゲットの上にドロップして、ツールバーを再配置します。

> **注記:**
>
> - この機能はiPadユーザーのみに適用されます。
> - この機能はタッチまたはマウスで動作します。
> - この機能はiPadまたは外部ディスプレイで動作します。
> - 最後のツールバーの位置は、次のセッションまたはアプリケーションの起動時まで保持されます。

SaaSアプリとWebアプリを切り替える

このユーザビリティの強化により、WebアプリとSoftware-as-a-Service (SaaS) アプリ内で前後に移動できます。

ナビゲーションボタンは、iPhoneのWorkspace WebおよびSaaSアプリセッションの左下隅に表示されます。

ナビゲーション(/en-us/citrix-workspace-app-for-ios/media/navigationb.png)

ナビゲーションボタンは、iPadのWorkspace WebおよびSaaSアプリセッションの左上隅に表示されます。

ナビゲーション(/en-us/citrix-workspace-app-for-ios/media/navigationa.png)

オンプレミスからクラウドアカウントへの移行

管理者は、オンプレミスのStoreFrontストアURLからWorkspace URLにエンドユーザーをシームレスに移行できます。管理者は、グローバルアプリ構成サービス を使用して、エンドユーザーの操作を最小限に抑えて移行を実行できます。

設定するには：

1. (https://developer.cloud.com/citrixworkspace/server-integration/global-app-configuration-service/docs/getting-started) URLに移動し、クラウドストアのURLを入力します。 例：`https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`。
2. **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** に移動し、**POST** をクリックします。
3. **INVOKE API** をクリックします。
4. ペイロードの詳細を入力してアップロードします。StoreFrontストアの有効期限をエポックタイムスタンプのミリ秒形式で入力します。

   例:

   ```
   "migrationUrl": [

   {



   "url": "<cloud store url>"

   "StoreFrontValidUntil": "<epoch timestamp in milliseconds>",

   }

   ]   ,
   ```

5. サービスをプッシュするには、**EXECUTE** をクリックします。

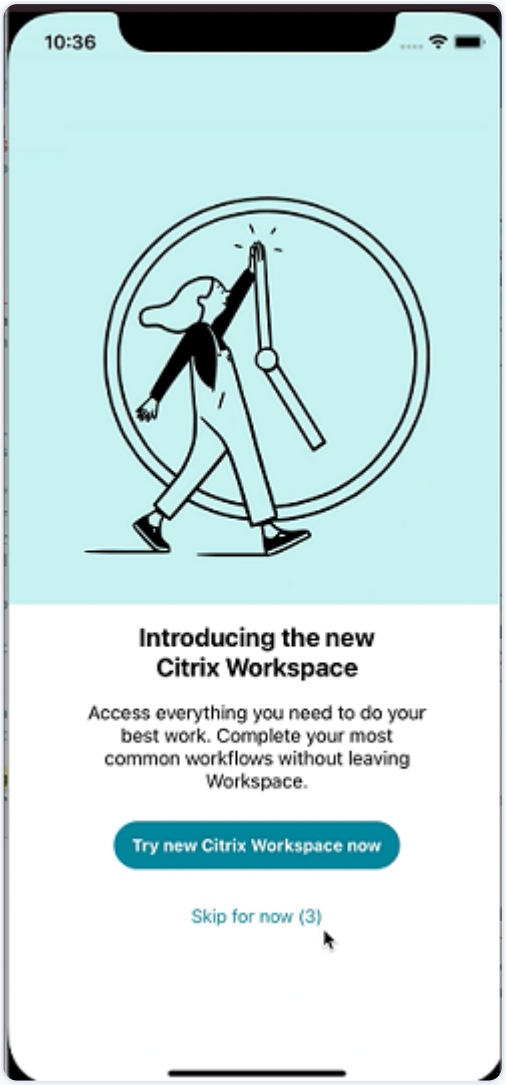
エンドユーザーエクスペリエンス

エンドユーザーとして、Citrix Workspaceアプリを初めて使用する場合、認証が成功すると、**新しいCitrix Workspaceの紹介** 移行画面が表示されます（対象の場合）。**今すぐ新しいCitrix**

Workspaceを試す オプションをタップすると、移行が開始されます。移行が成功すると、Workspaceストア（クラウドストア）にアクセスできます。

注：

移行を3回スキップできます。その後、スキップするオプションなしで移行が強制されます。



Workspace（クラウド）ストアに移行した後、**設定** でStoreFrontストアとWorkspaceストアの両方を表示できます。クラウドストアからオンプレミスのStoreFrontストアに切り替えると、フィードバック画面が表示され、回答を収集します。

注：

StoreFrontストアには有効期限があります。有効期限が過ぎると、ストアは削除されます。

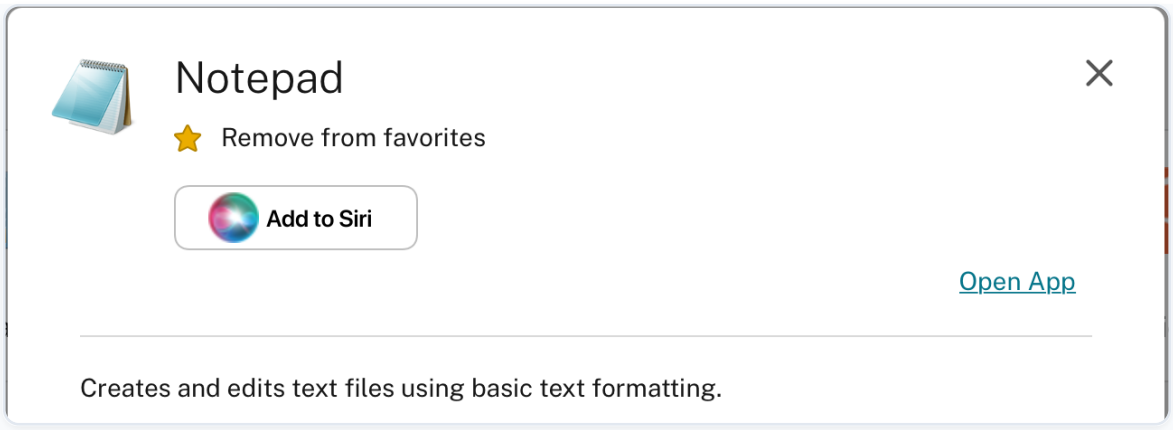
Siri連携

Siriと連携して、毎回Citrix Workspaceアプリを起動することなく、アプリやデスクトップなどのリソースを起動できます。

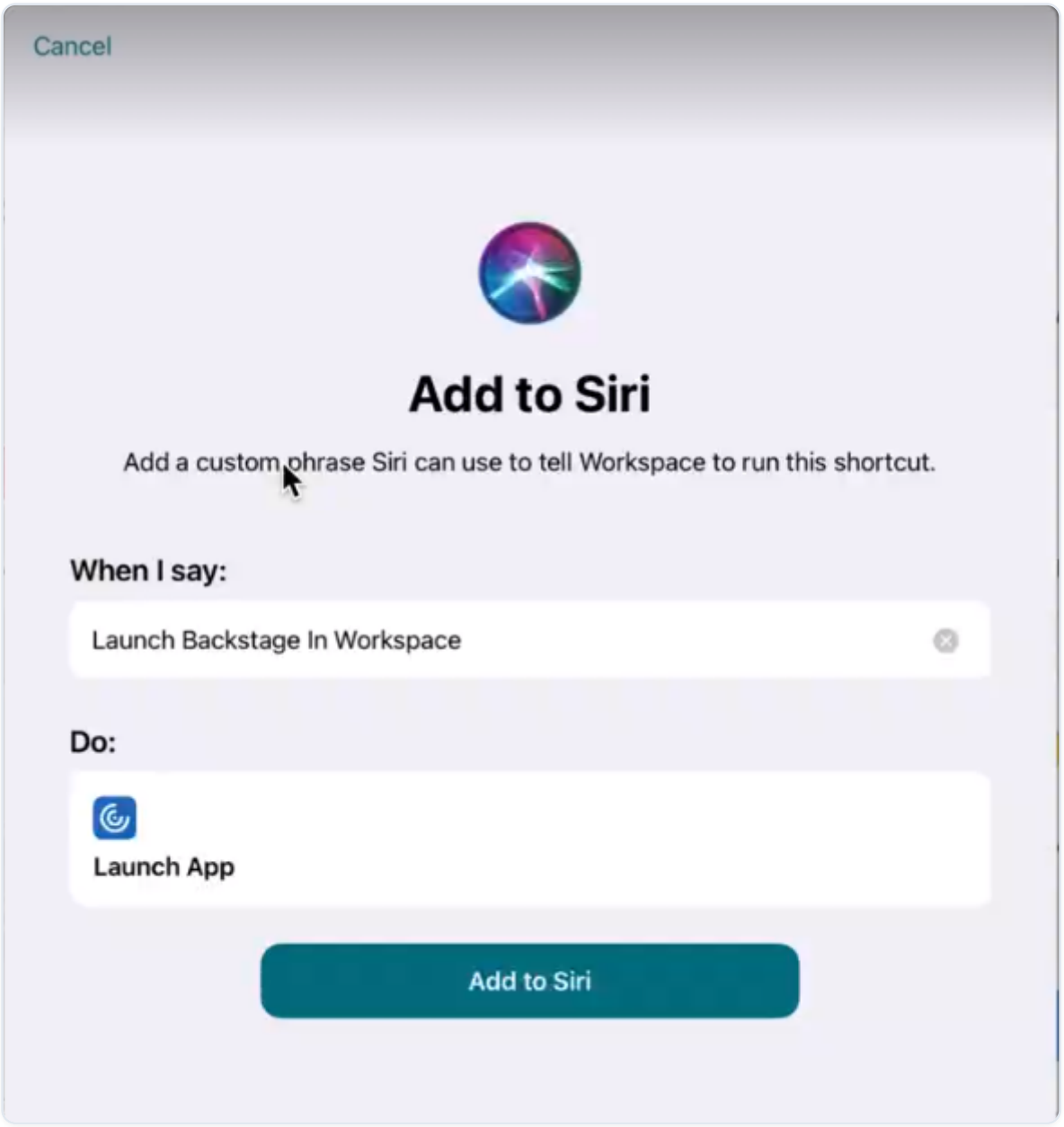
設定するには

1. Citrix Workspaceアプリを起動し、**アプリ**または**デスクトップ**をタップします。Siriショートカットに追加するリソースを選択します。
2. 省略記号（…）をタップします。ダイアログボックスが表示されます。

> **注：**
>
> iPhoneまたはiPadデスクトップユーザーの場合は、**省略記号**（…）> **アプリの詳細**画面 > **詳細を表示**をタップします。ダイアログボックスが表示されます。手順3に進みます。

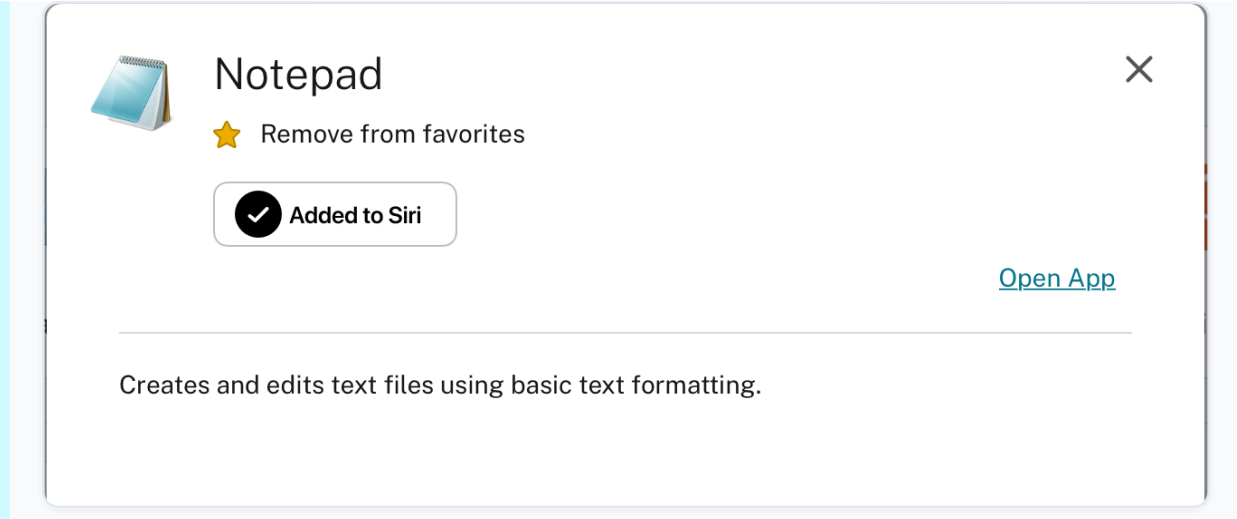


3. **Siriに追加**をタップします。**Siriに追加**ダイアログボックスが表示されます。



4. （オプション）Siriを呼び出すためのカスタムフレーズを編集します。**Siriに追加**をタップします。リソースがSiriショートカットに追加されました。ダイアログボックスを閉じます。

> **注：**
>
> 一部のデバイスでは、Siriを呼び出すためのカスタムフレーズの録音をサポートしています。



アプリケーション設定

Citrix Workspaceアプリを起動し、プロファイルアイコン > **アプリケーション設定** > **Siri構成**をタップします。この機能を有効にするには、**Siriに追加**をタップします。

これで、音声を使ってリソースを起動できます。

ショートカットを編集または削除するには

1. リソースを選択します。
2. 省略記号 (...) をタップします。ダイアログボックスが表示されます。
3. **Siriに追加**をタップします。**ショートカットを編集**ダイアログボックスが表示されます。

Citrix Workspaceアプリからのセッションウィンドウの分離のサポート

バージョン24.1.0以降、iOS向けCitrix Workspaceアプリは、マルチタスクをより効率的でユーザーフレンドリーにするためのセッションウィンドウの分離を導入しました。この機能により、デスクトップのようなエクスペリエンスを得ることができます。「セッションウィンドウの分離」機能が有効になっている場合、接続された外部モニターにセッションをドラッグ＆ドロップするだけで済みます。その結果、iPadのメインモニターを他のアプリとのマルチタスクに使用できます。

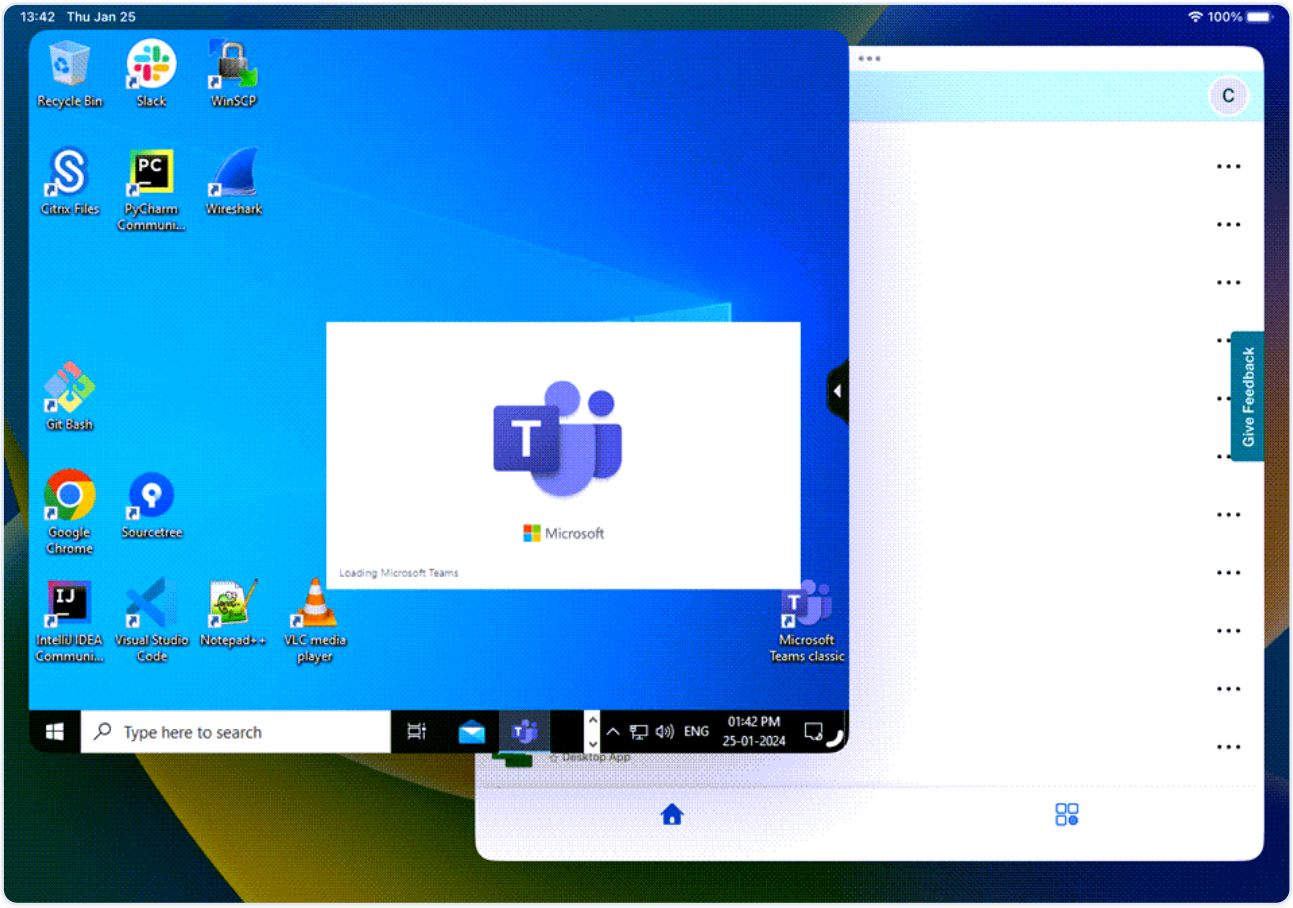
この機能には、以下の改善が含まれています。

- セッションメニューバーの**ホーム**ボタンをクリックすると、HDX™セッションウィンドウを閉じる代わりに、Citrix Workspace UIウィンドウが開きます。この機能強化により、Citrix Workspace UIとHDXセッションを同時に使用できます。Citrix Workspace UIから新しいセッションを開始すると、既存のセッションは自動的に切断されます。

- セッションメニューバーの**表示オプション**ボタンをクリックすると、HDXセッションの上に設定ウィンドウが表示されます。このウィンドウでは、Citrix Workspace UIの設定ではなく、セッションの解像度を調整できます。

> **注：**
>
> この機能は、Stage Manager機能をサポートするデバイスでのみサポートされています。すべてのiPhoneデバイスと一部のiPadデバイスは、この機能をサポートしていません。Stage Manager機能の詳細については、AppleサポートドキュメントのiPadでStage Managerをオンまたはオフにするを参照してください。

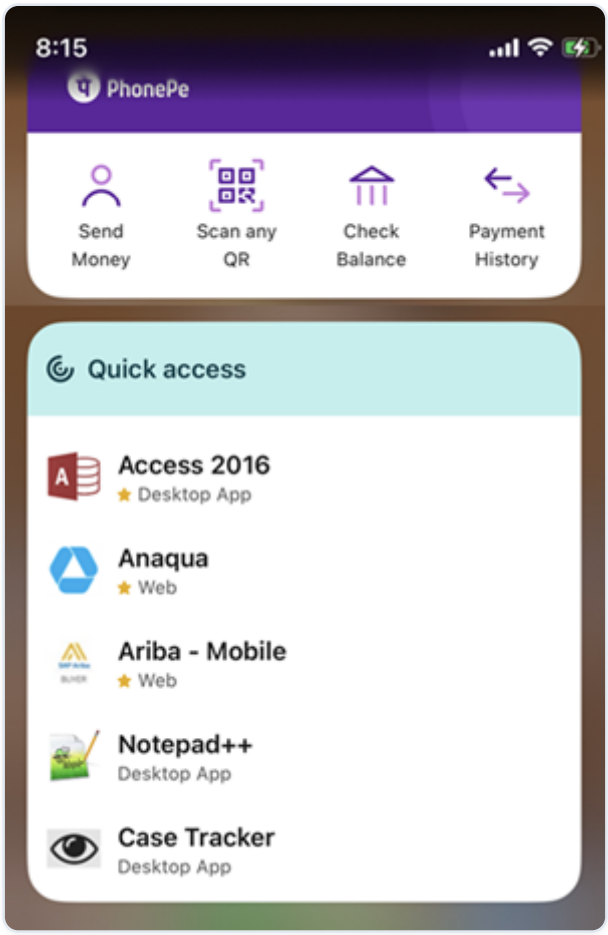
セッションウィンドウの分離機能を構成するには、**設定 -> 詳細 -> マルチタスク**に移動し、**セッションウィンドウの分離**を選択します。



アプリとデスクトップをウィジェットとして表示する

バージョン23.11.0以降、エンドユーザーはiPhoneおよびiPadから仮想アプリとデスクトップを直接起動できるようになりました。アプリまたはデスクトップセッションを開始するためにCitrix

Workspaceアプリを開く必要はありません。ユーザーは最大5つの仮想アプリとデスクトップをウィジェットとして持つことができます。



ウィジェットは、以下の基準に従って自動的に作成されます。

- お気に入り3つと最近開いた2つのアプリまたはデスクトップがウィジェットとして表示されます。
- お気に入りのアプリまたはデスクトップがない場合、最大5つの最近開いたアプリとデスクトップがウィジェットとして表示されます。
- 最近開いたアプリまたはデスクトップがない場合、最大5つのお気に入りのアプリまたはデスクトップがウィジェットとして表示されます。
- まだお気に入りにアプリまたはデスクトップが追加されておらず、最近開いたアプリまたはデスクトップもない場合、ユーザーはCitrix Workspaceアプリ for iOSを開くように促されます。その後、特定のアプリまたはデスクトップをお気に入りとしてマークできます。

ウィジェットなし(/en-us/citrix-workspace-app-for-ios/media/ios-without-widget.png)

WebおよびSaaSアプリ用Webview

Webページ

Webページの外部共有

Citrix Workspaceアプリから開いたWebページを他のユーザーと共有できます。次のことができます。

- Webview内からリンクをコピーする
- WebページをSafariで直接開く
- リンクをユーザーまたはアプリに直接送信する

共有するには、Webviewの右上にある**...**アイコンをタップするか、Webview内の任意のリンクを長押しし、必要なオプションをタップします。

ウェブビュー

SaaSアプリ用のネイティブコントロールを備えた強化されたWebview

SaaSアプリ用のネイティブコントロールを備えた強化されたWebviewを使用できます。この機能強化により、次のことが可能になります。

- アプリのURLを表示する。
- アプリのセキュリティ情報を表示する。
- アプリを共有する。

また、アプリを左右にスワイプして、それぞれ進む、戻る操作ができるようになりました。

Citrix Workspace モバイルアプリのWebビューア

Webビューアは、Citrix Workspaceアプリ内で動作するアプリ内ブラウジングソリューションです。これにより、ユーザーはCitrix WorkspaceアプリからWebアプリやSaaSアプリを安全に開くことができます。Webビューアは、さまざまなWebアプリやSaaSアプリにアクセスする際に一貫したユーザーインターフェイスを保証します。これにより、生産性が向上し、アプリのレンダリングパフォーマンスが向上します。

ユーザーエクスペリエンスの向上に継続的に注力し、新しいWebビューアは、以下の機能を備えた、より強化されたネイティブなブラウザのようなエクスペリエンスを提供します。

- VPNなしで内部Webページにアクセス

- アダプティブアクセスポリシーによるWebおよびSaaSのSSO
- プレビュー付きファイルダウンロード
- ページ間およびサイト間のシームレスなナビゲーション
- URL共有機能
- ページ内検索
- アクティビティフィードを介してリンクにアクセスする際の一貫した表示

管理者は、ダウンロード、クリップボード、ナビゲーション制限、ファイルアップロード、および透かしを含むSecure Private Access (SPA) を、URLごとにさまざまな組み合わせで有効にできます。

パスワード管理

パスワードの保存

Citrix Web Interface Managementコンソールを使用して、ユーザーがパスワードを保存できるように認証方法を構成できます。ユーザーアカウントを構成すると、暗号化されたパスワードはユーザーが初めて接続するまで保存されます。以下を考慮してください:

- パスワードの保存を有効にすると、Citrix Workspaceアプリ for iOSは、今後のログオンのためにデバイスにパスワードを保存し、ユーザーがアプリケーションに接続するときにパスワードの入力を求めません。

  > **注：**
  >
  > パスワードは、ユーザーがアカウント作成時に入力した場合にのみ保存されます。アカウントにパスワードが入力されていない場合、サーバー設定に関係なくパスワードは保存されません。

- パスワードの保存を無効にすると（デフォルト設定）、Citrix Workspaceアプリ for iOSは、ユーザーが接続するたびにパスワードの入力を求めます。

> **注：**
>
> StoreFrontへの直接接続の場合、パスワードの保存は利用できません。

パスワードの保存を上書きするには

サーバーをパスワード保存用に構成した場合でも、ログオン時にパスワードを要求することを好むユーザーは、パスワードの保存を上書きできます:

- アカウント作成時、パスワードフィールドを空白のままにします。
- アカウントを編集する際、パスワードを削除してアカウントを保存します。

使用方法

Citrix Workspaceアプリには、パスワードを保存できるようにすることで接続プロセスを効率化する機能があり、Citrix Workspaceアプリを開くたびにセッションを認証するという余分な手順が不要になります。

> **注：**
>
> **パスワードの保存**機能は現在、PNAプロトコルをサポートしています。StoreFrontの*ネイティブ*モードはサポートしていません。ただし、StoreFrontがPNA *レガシー*モードを有効にしている場合は、この機能は動作します。

StoreFrontでパスワードを保存するように構成する

StoreFront を構成して **パスワードを保存** 機能を有効にするには:

1. 既存のストアを構成する場合は、手順 3 に進みます。
2. 新しい StoreFront 展開を構成するには、インストール、セットアップ、アップグレード、およびアンインストール に記載されているベストプラクティスに従ってください。
3. Citrix StoreFront 管理コンソールを開きます。ベース URL が HTTPS を使用しており、SSL 証明書の生成時に指定された共通名と同じであることを確認してください。
4. 構成するストアを選択します。
5. **XenApp® Service Support の構成** をクリックします。
6. **XenApp Service support** を有効にし、**Default store** (オプション) を選択して、**OK** をクリックします。
7. c:\\inetpub\\wwwroot\\Citrix\\\<store name\>\\Views\\PnaConfig\\. にあるテンプレート構成ファイルに移動します。
8. Config.aspx のバックアップを作成します。
9. 元の Config.aspx ファイルを開きます。

10. 行 \<EnableSavePassword\>**false**\</EnableSavePassword\> を編集して、**false** の値を **true** に変更します。
11. 編集した Config.aspx ファイルを保存します。
12. StoreFront サーバーで、管理者権限で PowerShell を実行します。
13. PowerShell コンソールで:

    a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`

    b. 「Set-ExecutionPolicy RemoteSigned」と入力します

    c. 「.\\ImportModules.ps1」と入力します

    d. 「Set-DSServiceMonitorFeature –ServiceUrl」と入力します `https://localhost:443/StoreFrontMonitor`
14. StoreFrontグループがある場合は、グループ内のすべてのメンバーで同じコマンドを実行します。

Citrix Gatewayでパスワードを保存するように設定する

> **注：**

> この構成では、Citrix Gatewayロードバランスサーバーを使用します。

> 保存されたパスワード機能に対応するようにCitrix Gatewayを設定するには：

1. Citrix Gateway管理コンソールにログオンします。
2. Citrixのベストプラクティスに従って、ロードバランス仮想サーバー用の証明書を作成します。
3. 構成タブで、**Traffic Management** > **Load Balancing** > **Servers**に移動し、**Add**をクリックします。
4. StoreFrontサーバーのサーバー名とIPアドレスを入力します。
5. **Create**をクリックします。StoreFrontグループがある場合は、グループ内のすべてのサーバーに対して手順5を繰り返します。
6. 構成タブで、**Traffic Management** > **Load Balancing** > **Monitor**に移動し、**Add**をクリックします。
7. モニターの名前を入力します。種類として**StoreFront**を選択します。ページの下部で、**Secure**を選択します（StoreFrontサーバーがHTTPSを使用しているため必須）。

8. **Special Parameters**タブをクリックします。以前に構成したStoreFront名を入力し、**Check Backed Services**を選択して**Create**をクリックします。
9. 「**Configuration**」タブで、「**Traffic Management**」>「**Load Balancing**」>「**Service Group**s」の順に移動し、「**Add**」をクリックします。
10. サービスグループの名前を入力し、プロトコルを「**SSL**」に設定して、「**Ok**」をクリックします。
11. 画面右側の「Advanced Settings」の下にある「**Settings**」を選択します。
12. 「Client IP」を有効にし、ヘッダー値に「**X-Forwarded-For**」と入力して、「**OK**」をクリックします。
13. 画面右側の「Advanced Settings」の下にある「**Monitors**」を選択します。矢印をクリックして新しいモニターを追加します。
14. 「**Add**」ボタンをクリックし、「**Select Monitor**」ドロップダウンメニューを選択します。（Citrix Gatewayで構成された）モニターのリストが表示されます。
15. 以前に作成したモニターの横にあるラジオボタンをクリックし、「**Select**」をクリックしてから「**Bind**」をクリックします。
16. 画面右側（「Advanced Settings」の下）にある「**Members**」を選択します。矢印をクリックして新しいサービスグループメンバーを追加します。
17. 「**Add**」ボタンをクリックし、「**Select Member**」ドロップダウンメニューを選択します。
18. 「**Server Based**」ラジオボタンを選択します。（Citrix Gatewayで構成された）サーバーメンバーのリストが表示されます。以前に作成したStoreFrontサーバーの横にあるラジオボタンをクリックします。
19. ポート番号に「443」を入力し、ハッシュIDに一意の番号を指定して、「**Create**」をクリックし、次に「**Done**」をクリックします。すべてが適切に構成されている場合、「**Effective State**」は緑色のライトを表示し、監視が正常に機能していることを示します。
20. **Traffic Management -\> Load Balancing -\ > Virtual Servers** に移動し、**Add** をクリックします。サーバーの名前を入力し、プロトコルとして **SSL** を選択します。
21. StoreFrontロードバランスサーバーのIPアドレスを入力し、「**OK**」をクリックします。
22. 「**Load Balancing Virtual Server Service Group**」バインディングを選択し、矢印をクリックして、以前に作成したサービスグループを追加します。「**OK**」を2回クリックします。
23. ロードバランス仮想サーバー用に作成されたSSL証明書を割り当てます。「**No Server Certificate**」を選択します。
24. リストからロードバランサーサーバー証明書を選択し、**バインド**をクリックします。

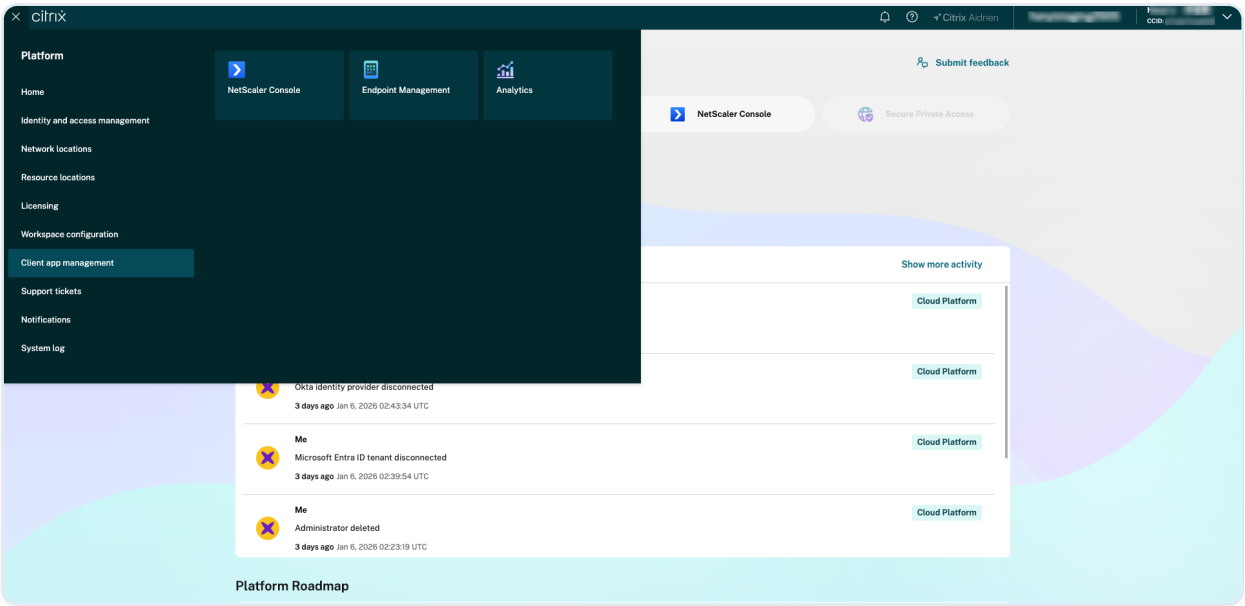
25. ドメイン証明書をロードバランサーサーバーに追加します。**CA証明書なし**をクリックします。
26. ドメイン証明書を選択し、**バインド**をクリックします。
27. 画面の右側で、**永続性**を選択します。
28. 永続性を**SOURCEIP**に変更し、タイムアウトを**20**に設定します。**保存**をクリックし、次に**完了**をクリックします。
29. ドメインDNSサーバーで、ロードバランサーサーバーを追加します (まだ作成されていない場合)。
30. iOSデバイスでCitrix Workspaceアプリ for iOSを起動し、完全なXenApp URLを入力します。

GACS & MDM のセッションツールバー構成のサポート

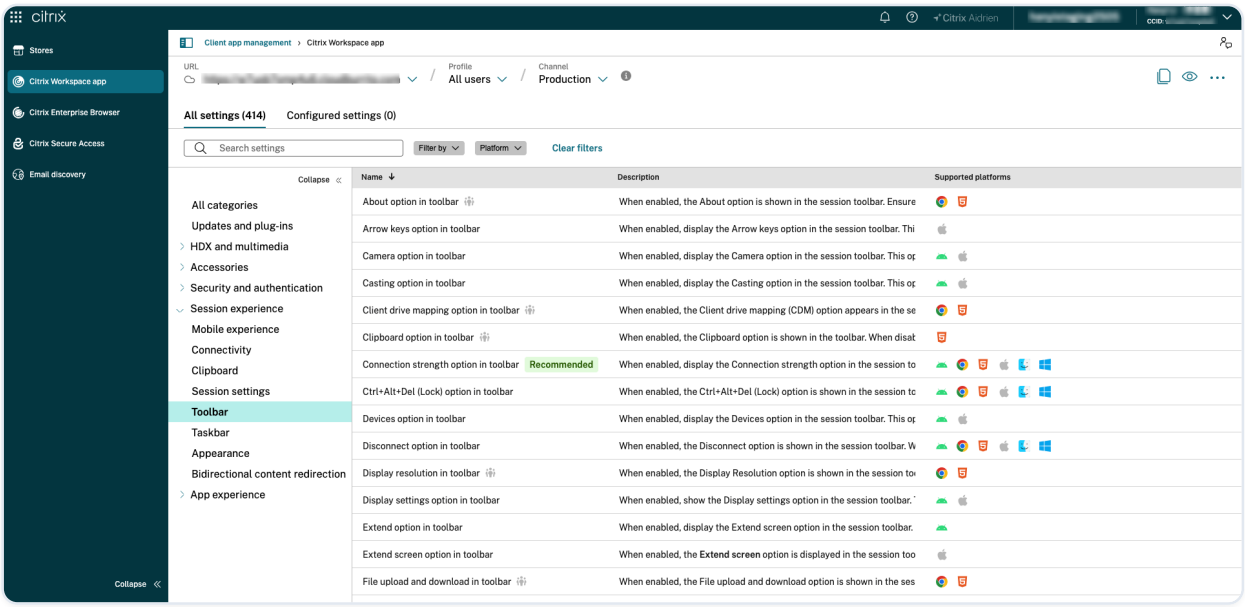
この機能は、Global App Configuration Service (GACS) および Mobile Device Management (MDM) を使用して構成できます。

GACS の使用

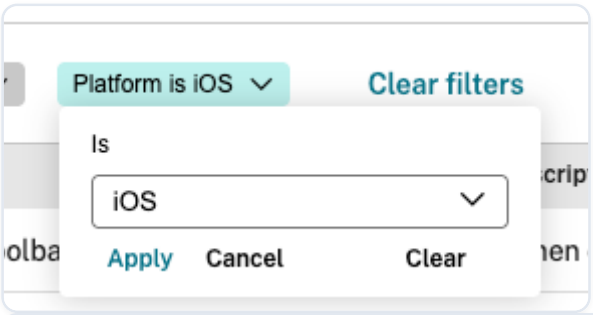
1. **Citrix Cloud™** アカウントにサインインし、**Client App Management** に移動します。

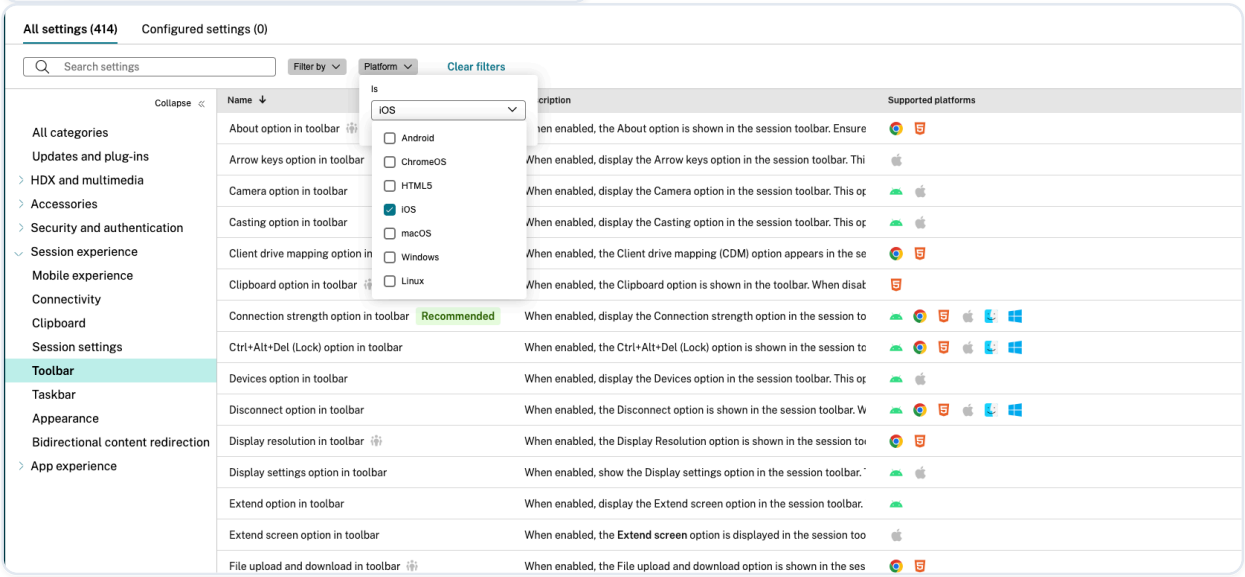


2. **Citrix Workspace app > Session Experience > Session Toolbar** をクリックします。

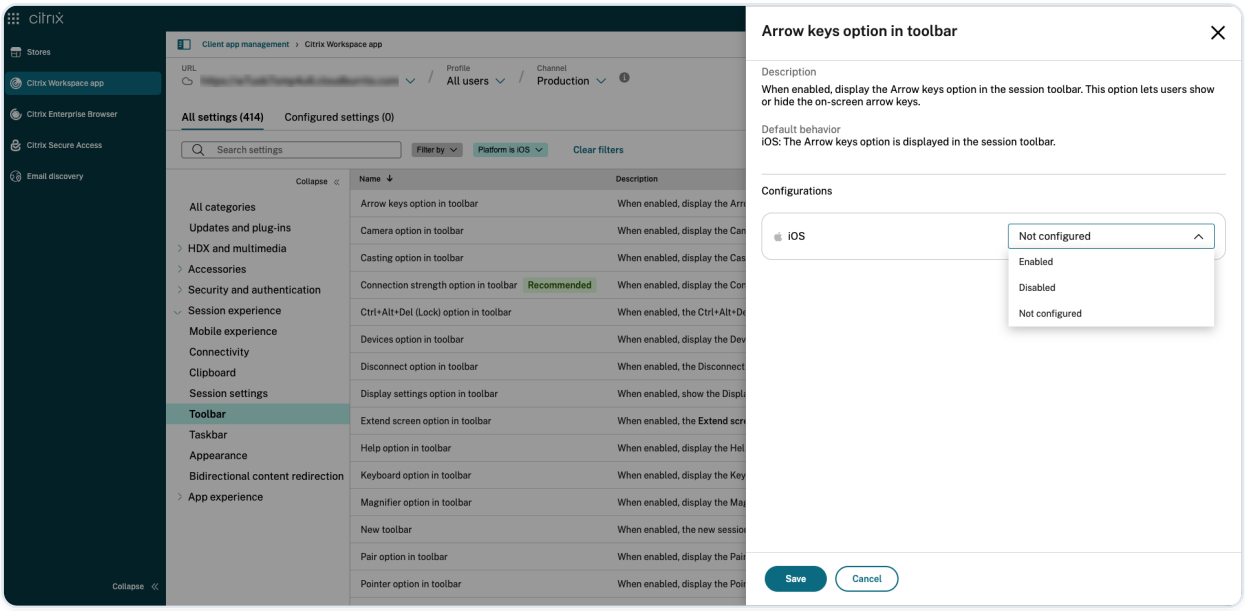


3. **Toolbar** セクションで、ツールバーの必要なオプションに移動し、編集する列をクリックします。プラットフォーム（iOS やその他のプラットフォームなど）でフィルタリングしてから、**Apply** をクリックすることもできます。



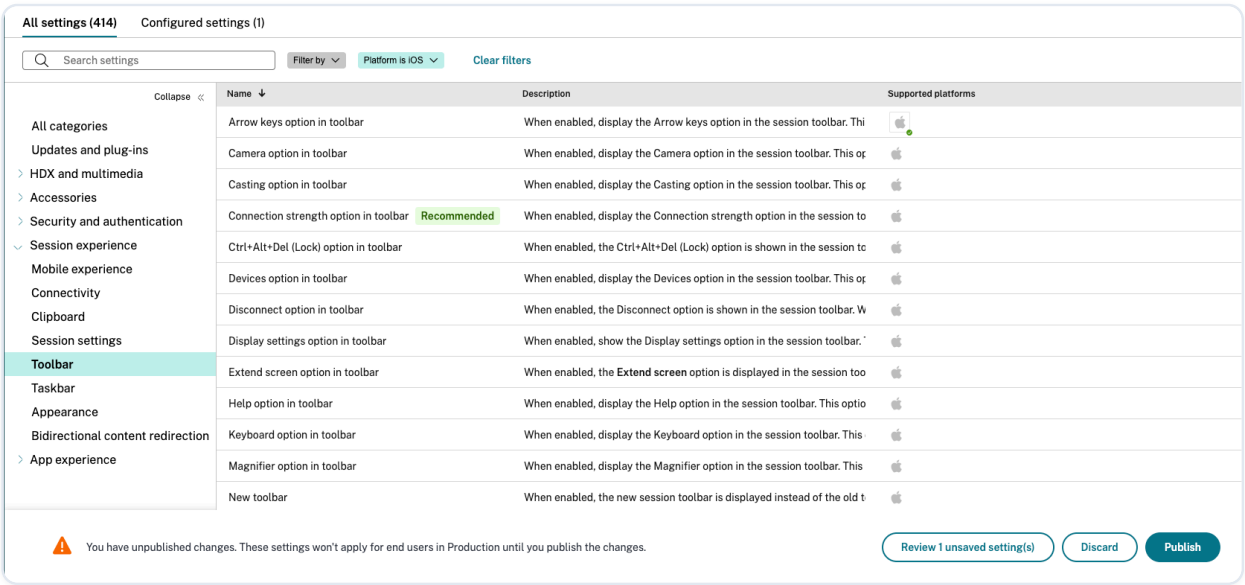


4. 構成チェックボックスを選択し、クリックします。これで、ツールバーオプションを *非表示* または *表示* にカスタマイズできます。



5. 構成を変更したら、**Save** をクリックします。

6. 設定を保存するには、**Publish** をクリックします。



注：

Citrix Cloud のキャッシュのため、変更が反映されるまでに最大 6 時間かかる場合があります。

MDM の使用

この構成は、Citrix Workspace アプリのバンドル ID の **Managed App Configuration** として、MDM ソリューションを通じて展開されます。MDM 構成は GACS 設定よりも優先されます。設定は、Apple の Managed App Configuration の一部として `XML/plist` 形式で保存されます。

ツールバーのMDM構成の例

```
<dict>

    <key>category</key>

    <string>toolbar</string>

    <key>userOverride</key>

    <false/>

    <key>settings</key>

    <array>

        <dict>

            <key>name</key>

            <string>enableKeyboardToolbarOption</string>

            <key>value</key>

            <true/>

        </dict>

        <dict>

            <key>name</key>

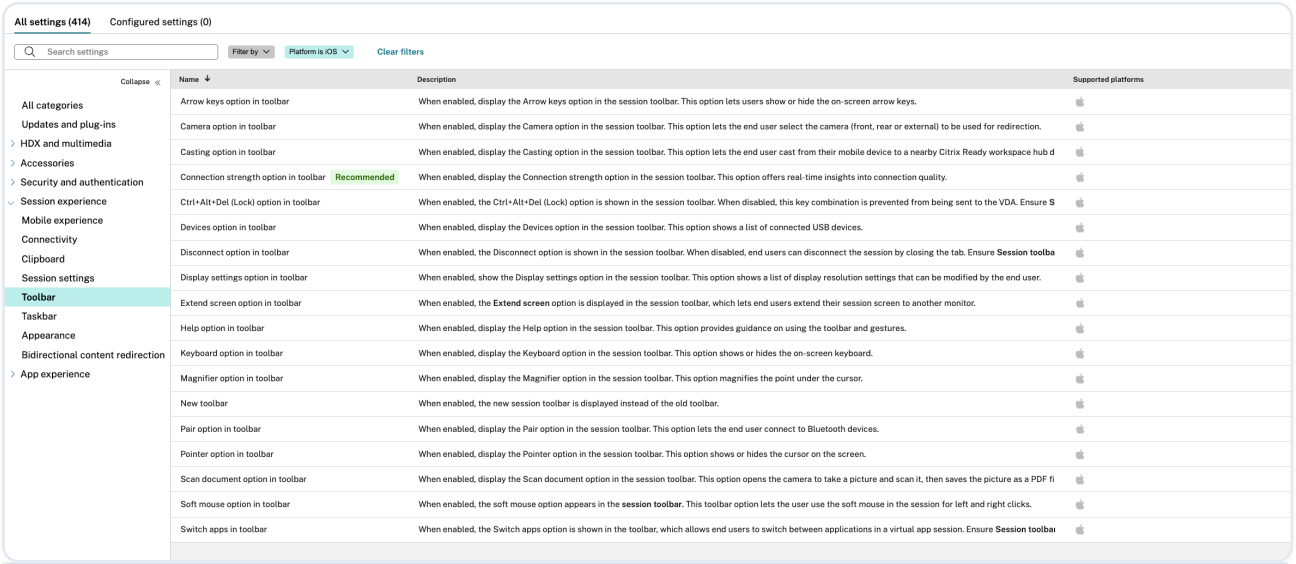
            <string>enableCloseToolbarOption</string>

            <key>value</key>

            <false/>
```

```
        </dict>
        <dict>
            <key>name</key>
            <string>enableCameraToolbarOption</string>
            <key>value</key>
            <true/>
        </dict>
    </array>
</dict>
```

iOSツールバーアイコンの構成



名前	説明	MDM設定キー
ツールバーの矢印キーオプション	有効にすると、セッションツールバーに矢印キーオプションが表示されます。このオプションを使用すると、ユーザーは画面上の矢印キーを表示または非表示にできます。	`enableArrowKeysToolbarOption`

名前	説明	MDM設定キー
ツールバーのカメラオプション	有効にすると、セッションツールバーにカメラオプションが表示されます。このオプションを使用すると、エンドユーザーはリダイレクトに使用するカメラ（前面、背面、または外部）を選択できます。	`enableCameraToolbarOption`
ツールバーのキャスティングオプション	有効にすると、セッションツールバーにキャスティングオプションが表示されます。このオプションを使用すると、エンドユーザーはモバイルデバイスから近くのCitrix Readyワークスペースハブデバイスにキャストできます。	`enableCastingToolbarOption`
ツールバーの接続強度オプション	有効にすると、セッションツールバーに接続強度オプションが表示されます。このオプションは、接続品質に関するリアルタイムの洞察を提供します。	`enableConnectionStrengthToolbarOption`
ツールバーのCtrl+Alt+Del (ロック) オプション	有効にすると、セッションツールバーにCtrl+Alt+Del (ロック) オプションが表示されます。無効にすると、このキーの組み合わせがVDAに送信されなくなります。この設定を有効にするには、セッションツールバーが有効になっていることを確認してください。	`enableCtrlAltDelToolbarOption`
ツールバーのデバイスオプション	有効にすると、セッションツールバーにデバイスオプションが表示されます。このオプションには、接続されて	`enableDevicesToolbarOption`

名前	説明	MDM設定キー
	いるUSBデバイスのリストが表示されます。	
ツールバーの切断オプション	有効にすると、セッションツールバーに切断オプションが表示されます。無効にすると、エンドユーザーはタブを閉じることでセッションを切断できます。この設定を有効にするには、セッションツールバーが有効になっていることを確認してください。	`enableCloseToolbarOption`
ツールバーの表示設定オプション	有効にすると、セッションツールバーに表示設定オプションが表示されます。このオプションには、エンドユーザーが変更できるディスプレイ解像度設定のリストが表示されます。	`enableDisplaySettingsToolbarOption`
ツールバーのヘルプオプション	有効にすると、セッションツールバーにヘルプオプションが表示されます。このオプションは、ツールバーとジェスチャの使用方法に関するガイダンスを提供します。	`enableHelpToolbarOption`
ツールバーのキーボードオプション	有効にすると、セッションツールバーにキーボードオプションが表示されます。このオプションは、オンスクリーンキーボードの表示/非表示を切り替えます。	`enableKeyboardToolbarOption`
ツールバーの拡大鏡オプション	有効にすると、セッションツールバーに拡大鏡オプションが表示されます。このオプションは、カーソル下のポイントを拡大します。	`enableMagnifierToolbarOption`

名前	説明	MDM設定キー
新しいツールバー	有効にすると、古いツールバーの代わりに新しいセッションツールバーが表示されます。	`enableNewToolbar`
ツールバーのペアオプション	有効にすると、セッションツールバーにペアオプションが表示されます。このオプションを使用すると、エンドユーザーはBluetoothデバイスに接続できます。	`enablePairToolbarOption`
ツールバーのポインターオプション	有効にすると、セッションツールバーにポインターオプションが表示されます。このオプションは、画面上のカーソルを表示または非表示にします。	`enablePointerToolbarOption`
ツールバーのドキュメントスキャンオプション	有効にすると、セッションツールバーにドキュメントスキャンオプションが表示されます。このオプションは、カメラを起動して写真を撮り、スキャンした後、その写真をPDFファイルとして保存します。	`enableScanDocumentToolbarOption`
ツールバーのソフトマウスオプション	有効にすると、セッションツールバーにソフトマウスオプションが表示されます。このツールバーオプションを使用すると、ユーザーはセッション内でソフトマウスを左右クリックに使用できます。	`enableSoftMouseToolbarOption`
ツールバーのアプリケーションの切り替え	有効にすると、ツールバーにアプリケーションの切り替えオプションが表示され、これによりエンドユーザーは仮想アプリセッションでアプリ	`enableSwitchAppsToolbarOption`

名前	説明	MDM設定キー
	ケーションを切り替えることができます。この設定を有効にするには、セッションツールバーが有効になっていることを確認してください。	

ストア構成

強化された新しいカスタマイズ可能なツールバー

バージョン24.12.0以降、iOS版Citrix Workspaceアプリに新しいカスタマイズ可能なツールバーが導入されました。刷新されたデスクトップビューアツールバーは、より高い柔軟性を提供することで、ユーザーエクスペリエンスとサポートを向上させます。管理者は、組織のニーズに合わせてセッション内ツールバーを調整できるようになりました。

機能	説明
管理者による制御	管理者は、エンドユーザーに表示されるオプションを選択して、ツールバーをカスタマイズできます。
UIとスキニング	**Desktop Viewer**ツールバーは、新しいユーザーインターフェイスとスキニングオプションで刷新されました。
切り替え可能なレイアウト	ツールバーは、単一列レイアウトと二重列レイアウトを切り替えることができます。
カスタマイズ可能なツールバー	管理者は、古いツールバーまたは新しいツールバーのいずれかをユーザーにプッシュすることを選択できます。
ドラッグ機能	横向きモードでは、ツールバーのノッチは画面の上端に沿ってのみ移動できます。縦向きモードでは、ノッチは左右に水平にドラッグできるほか、画面の端に沿って垂直にもドラッグできます。
クイックアクセスアイコン	よく使用する機能にすばやくアクセスするための新しいアイコンが導入されました。
ジェスチャーガイド	シングルクリック、右クリック、ドラッグ、ズーム、ポインターの切り替え、キーボードの使用方法に関するガイダンスを提供します。

機能	説明
ツールバーガイド	デバイス、キーボード、ポインター、拡大鏡、ソフトマウス、ディスプレイ、カメラ、スイッチ、スクロールなどのオプションが含まれます。

標準メニューオプション:

メニューオプション	説明
矢印キー	セッションナビゲーション用のナビゲーション矢印キーパッドを表示します。
キーボード	iOSシステムソフトキーボードと、コントロールキー付きの拡張キーボードアクセサリを表示します。
ポインター	セッションウィンドウ内にWindowsのようなマウスポインターを表示します。
拡大鏡	拡大レンズとともに、ウィンドウのようなマウスポインターを表示します。
仮想マウス	このオプションは、画面上にソフトマウスを表示します。
切り替え	アプリの切り替えは、1つのVirtual Desktop Agentで同時に開かれている複数の仮想アプリを切り替えるために使用されます。
表示	全画面表示設定のモーダルビューを表示します。
コントロール+オルト+デリート	Ctrl+Alt+Delキーの組み合わせをVirtual Desktop Agentに送信します。
ペアリング	セカンダリのiPhoneまたはiPadデバイスとペアリングして、トラックパッドとして機能させることができます。
切断	サステナビリティ機能が有効になっている場合、サインアウトと切断のどちらかを選択す

メニューオプション	説明
	るオプションが表示されます。そうでない場合は、セッションを切断します。
外部マウス設定	セッションマウス設定のモーダルビューを表示します。
カメラ	使用するカメラの種類（前面、背面、外部）を選択できます。カメラを開いてドキュメントをPDFにスキャンし、Virtual Desktop Agentにアップロードします。
ヘルプガイド	セッションのナビゲートと操作のために、ツールバー機能、ジェスチャ、およびメニューオプションの使用に関するガイダンスを提供します。

「カスタマイズ可能なツールバーオプション」(/en-us/citrix-workspace-app-for-ios/media/customizable-toolbar-1.png)

可変メニューオプション:

メニューオプション	説明
スキャン	ドキュメントをスキャンするための全画面カメラを表示します。
キャスト	画面をキャストするためのオプションを表示します。

「カスタマイズ可能なツールバーの可変オプション」(/en-us/citrix-workspace-app-for-ios/media/customizable-toolbar-2.png)

Global App Configuration service (GACS) を通じてこの機能を有効にし、機能フラグがオンになっていることを確認できます。

GACS を通じてこの機能を有効にするには、管理者は次の手順に従う必要があります。

1. Citrix Cloud で **Workspace Configuration** > **App Configuration** > **構成** に移動します。
2. **Citrix Workspace™ app** の下で、**Session Experience** を選択します。
3. **Toolbar** をクリックし、必要なオプションを有効にします。

「カスタマイズ可能なツールバー - GACS」(/en-us/citrix-workspace-app-for-ios/media/toolbar-gacs.png)

認証

事前入力されたユーザー名によるCitrix®セキュリティの強化

バージョン25.1.0以降、Unified Endpoint Management (UEM) を使用して、特定の形式でユーザー名を管理対象デバイスにプッシュできます。iOSでは、Citrix Workspaceアプリがこの構成を読み取り、ユーザー名を取得し、認証プロンプト内に読み取り専用として事前入力します。これにより、登録済みのデバイス所有者のみがその特定のデバイスでアプリを認証してアクセスできるようになります。

管理者は、複数のiOSデバイスにわたるユーザー認証を中央の場所から効率的に管理できると同時に、承認されたユーザーのみがサインインできるようにします。

この機能は、ユーザーが手動で資格情報を入力する必要をなくすことでログインプロセスを簡素化し、エラーのリスクを軽減し、全体的なユーザーエクスペリエンスを向上させます。堅牢なアクセス制御とシームレスなログインフローを組み合わせることで、iOS版Citrix Workspace™アプリは、セキュリティの強化と使いやすさの向上を両立させます。

この機能は、UEMを介して以下の設定を使用して構成できます。

> **注：**
>
> この例では、デモンストレーションのためにMicrosoft IntuneをUEMソリューションとして使用しています。手順とUIは、UEMプロバイダーによって異なる場合があります。

1. UEMプロバイダーにサインインします。
2. 管理のためにCitrix WorkspaceアプリをUEMプロバイダーに追加します。UEMポータルからアップロードするか、App Storeにリンクします。
3. アプリのアプリ構成ポリシーを作成します。
4. XMLプロパティリストにキーと値のペアを追加し、以下の値を入力します。
    - **キー:** `username`
    - **値の型:** `String`

- **値:** Microsoft Intuneポータルに記載されているペイロード変数。

マイクロソフト Intune:

```
<key>username</key>
<string>{{UserName}}</string>
```

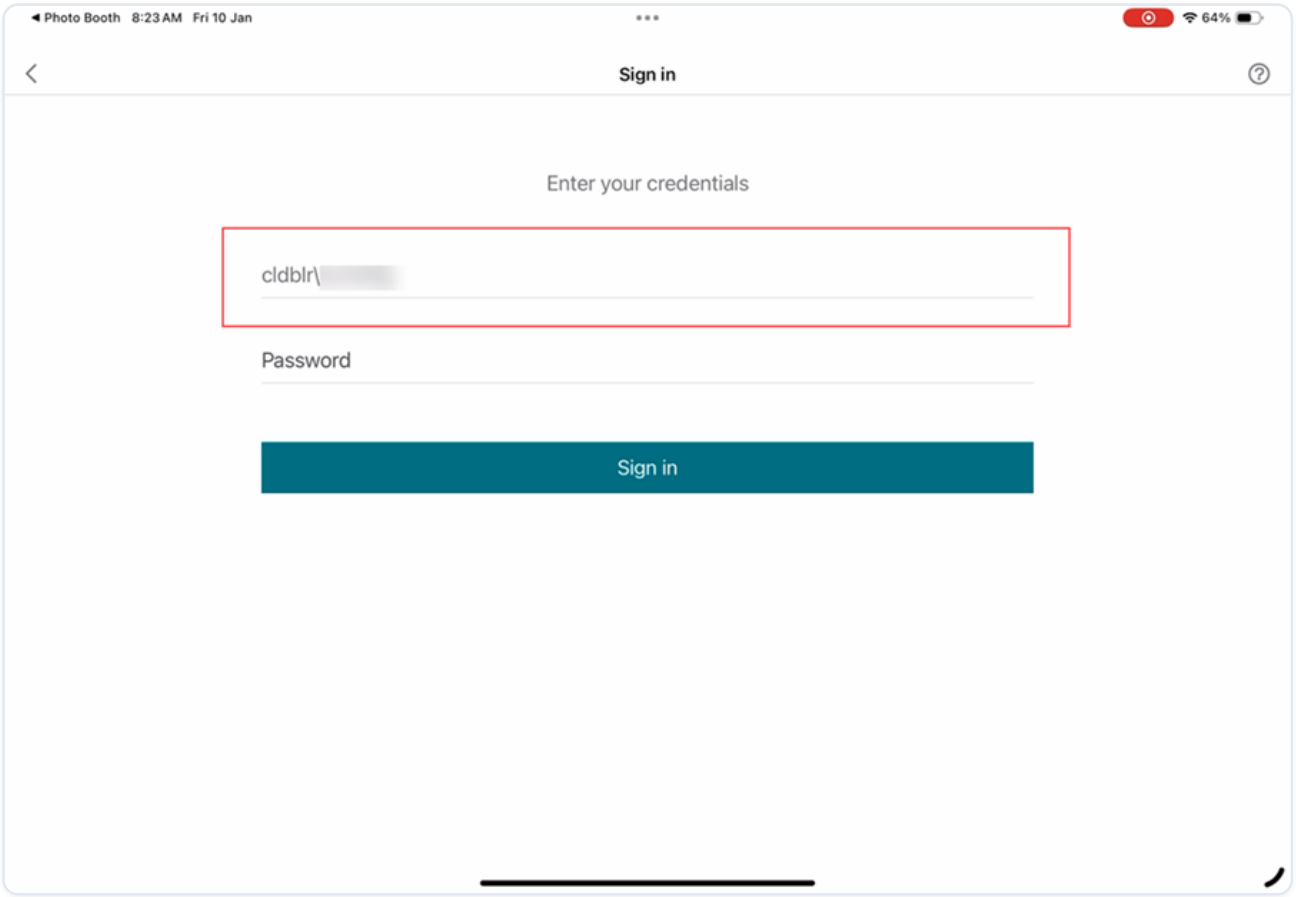
詳細については、「Intuneで一般的なiOS/iPadOS機能を使用するためのiOSおよびiPadOSデバイス設定」を参照してください。

ジャムフ:

```
<key>username</key>

    <string>$USERNAME</string>
```

詳細については、「構成プロファイルのペイロード変数」を参照してください。



制限事項:

システムはネイティブログインページのみをサポートしています。Webベースのログインでは、ユーザー名の事前入力はサポートされていません。

高速スマートカード

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、認証パフォーマンスと使いやすさを向上させるスマートカードの機能強化を導入しました。このアップデートにより、スマートカードのサポートが大幅に改善され、ユーザーエクスペリエンスがよりスムーズで効率的になります。同時プロトコルサポートと高速スマートカードプロトコルの統合により、ユーザーはより高速な認証とスマートカードリーダーのシームレスな使用を期待できます。高速スマートカードは、WindowsデスクトップのCNG（Crypto Next Generation）APIと互換性があります。

> **注：**
>
> この機能を有効にするには、Citrixヘルプデスクにお問い合わせください。

> **制限事項:**

- Citrix WorkspaceアプリiOSでは、同時実行は完全にサポートされていません。
- プラグアンドプレイはサポートされていません。

Citrix Workspaceアプリを使用したCitrixアクセスを強制する

バージョン24.12.0以降、管理者はiOSデバイスのユーザーに対し、Citrix Workspaceへのアクセスをネイティブアプリ経由のみに義務付けることができます。この機能が有効になっている場合、ストアURLやサードパーティ製ブラウザにアクセスしようとするユーザーは、自動的にCitrix Workspaceアプリにリダイレクトされます。これにより、ネイティブアプリのすべての機能を活用し、シームレスなユーザーエクスペリエンスを享受できます。さらに、この機能により、管理者はユーザー環境をより詳細に制御できるようになり、認証プロセスをネイティブアプリ内に保持することでセキュリティが強化され、ICAファイルをダウンロードする必要がなくなります。

管理者は、Citrix Cloudアカウントを使用してこの機能を有効にできます。この機能は現在、Cloudストアのみでサポートされています。詳細については、「エンドユーザーにネイティブアプリを介したアプリとデスクトップの認証とアクセスを義務付ける」を参照してください。

生体認証プロンプトをスキップする

以前は、エンドユーザーはCitrix Workspaceアプリでの認証に生体認証（Touch IDまたはFace ID）を使用するかどうかを選択するよう求められていました。バージョン24.9.0以降、管理者はこのプロンプトをスキップできるようになり、ユーザーのログインプロセスが効率化されます。

生体認証が有効になっている場合、ユーザーのパスワードはキーチェーンに安全に保存され、生体認証によって保護されます。認証トークンの有効期限が切れると、ユーザーは自動的に生体認証の確認を求められます。デバイスで生体認証が構成されていない場合、トークンの有効期限が切れると、ユーザーは手動で資格情報を入力する必要があります。

この機能は現在、Lightweight Directory Access Protocol (LDAP) 認証を使用するオンプレミスストアでのみサポートされています。

構成

生体認証を有効にするには、次の方法を使用できます。

- モバイルデバイス管理 (MDM)
- グローバルアプリ構成サービス (GACS)

MDMを介して生体認証を有効にするには、管理者は次の設定を使用する必要があります。

- キー: `settings_skip_consent_for_biometric_protected_password_saving`
- 値: `true/false`
- デフォルト値: `false`
  - `true`に設定されている場合、生体認証による再ログイン機能は、エンドユーザーに選択または拒否するオプションを提供することなく、自動的に適用されます。
  - `false`に設定されている場合、生体認証による再ログイン機能はオプションであり、ユーザーはそれを受け入れるか拒否するかを選択できます。

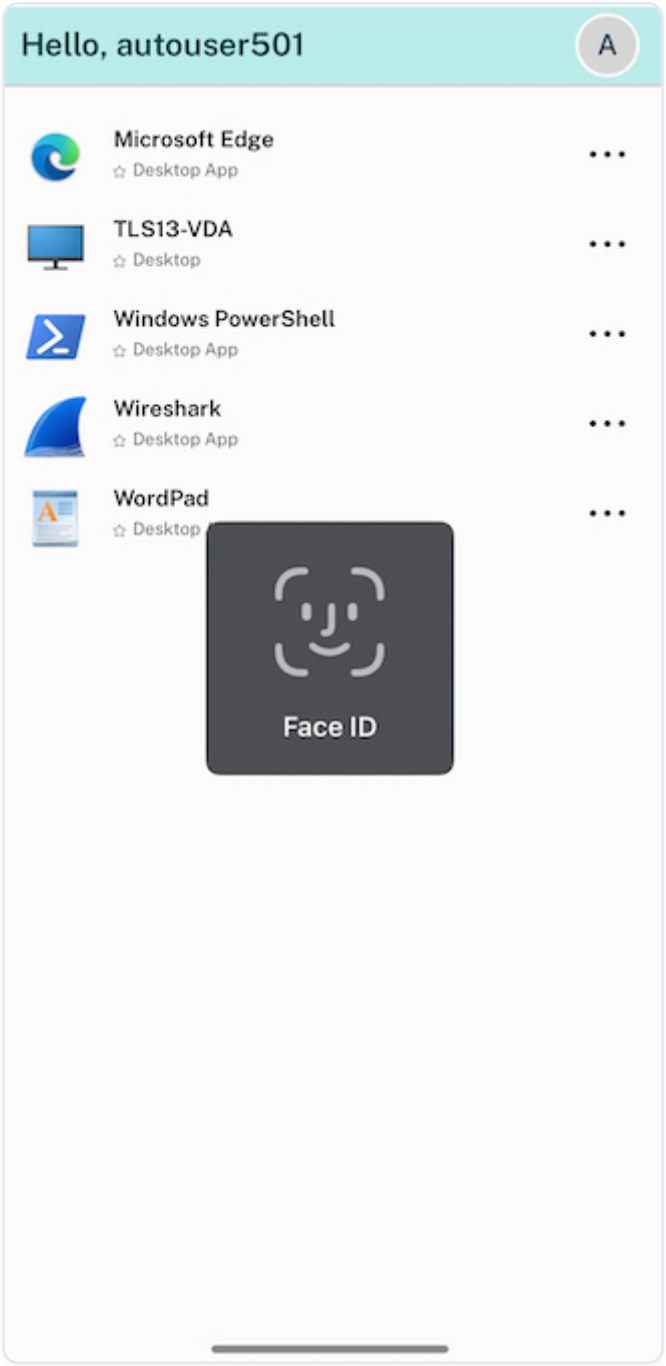
GACSを介して生体認証を有効にするには、管理者は次の手順を使用する必要があります。

1. Citrix Cloudで、**ワークスペース構成** > **アプリ構成** > **構成** に移動します。
2. **Citrix Workspaceアプリ**で、**Security and Authentication**を選択します。
3. **Authentication**で、**Skip use biometrics prompt**を有効にします。

詳細については、「UEMを介したCitrix Workspaceアプリ設定の構成のサポート」を参照してください。

Citrix Workspaceアプリへのアクセスに生体認証を強制するサポート

管理者は、ユーザーがCitrix Workspaceアプリにアクセスするためにデバイスの生体認証を強制できるようになりました。この機能により、Citrix Workspaceアプリを閉じた後に再度開くか、最小化した後に前面に表示すると、ロック解除してサインインするためにFace IDまたはTouch IDの確認プロンプトが表示されます。デバイスが生体認証をサポートしていない場合、アプリにアクセスするにはパスワードまたはパスコード認証方法が使用されます。デバイスでパスコードが有効になっていない場合、アカウントはサインアウトされ、ユーザーはCitrix Workspaceアプリケーションにアクセスするために再度サインインする必要があります。



管理者は、統合エンドポイント管理ソリューションを使用して、以下のキーと値のペアでこの機能を構成できます。

- **キー**: verify_biometric_on_app_foreground_transition
- **値の型**: Boolean
- **値**: true または false
  - **true** に設定されている場合、エンドユーザーがCitrix Workspaceアプリにアクセスするには生体認証が必要です。
  - **false** に設定されている場合、Citrix Workspaceアプリへのアクセスに生体認証は強制されません。ユーザーは生体認証を無効にするオプションがあります。

生体認証サインイン(/en-us/citrix-workspace-app-for-ios/media/biometric-signin.png)

オンプレミスストアに接続する際のFIDO2を使用した認証のサポート

バージョン24.7.0以降、ユーザーはオンプレミスストアに接続する際に、FIDO2ベースのパスワードレス認証を使用してCitrix Workspaceアプリ for iOSに認証できます。FIDO2はシームレスな認証方法を提供し、企業従業員がユーザー名やパスワードを入力することなくCitrix Workspaceアプリ for iOSにアクセスできるようにします。この機能は、ローミング認証器（USBのみ）とプラットフォーム認証器（PINコード、Touch ID、Face IDのみ）の両方をサポートしています。

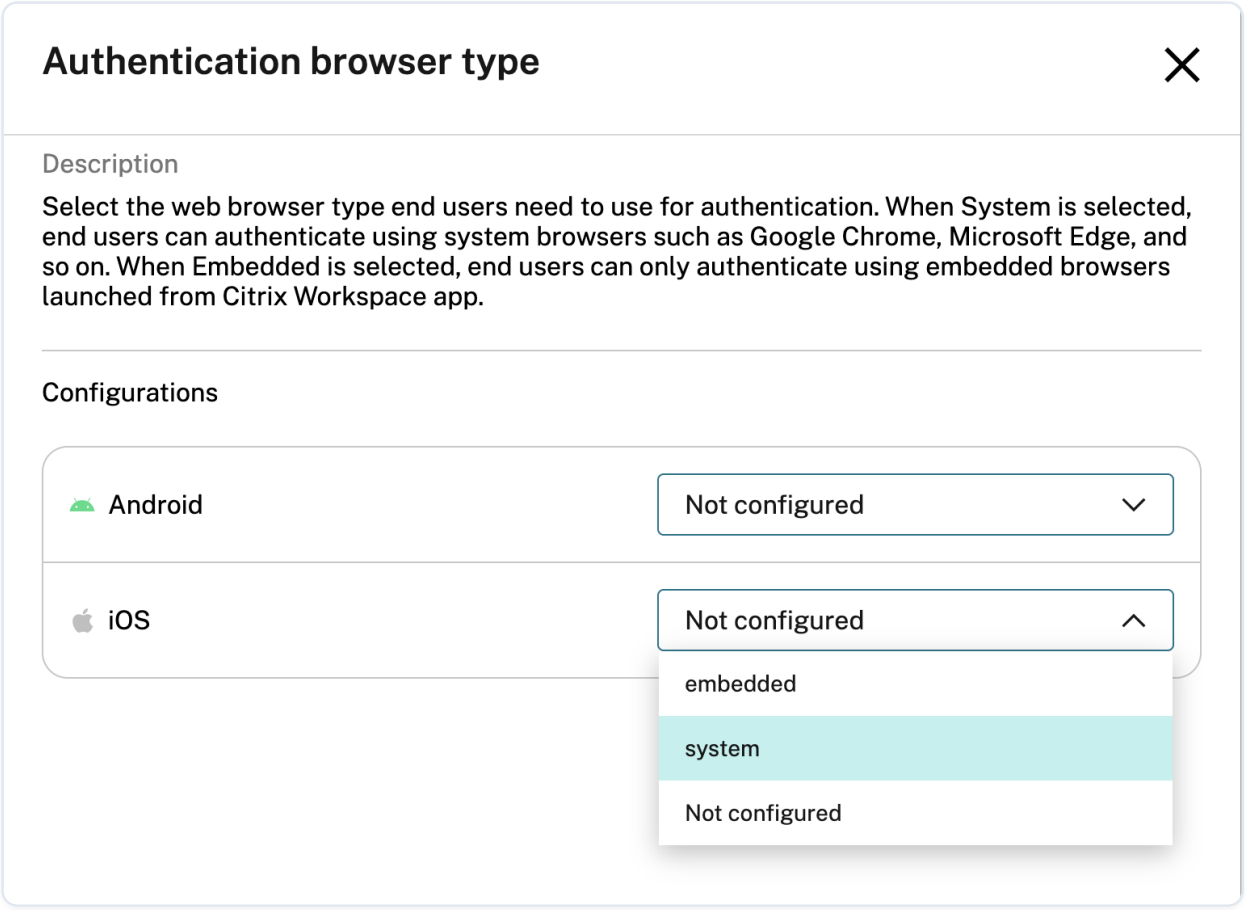
この機能は、グローバルアプリ構成サービスと統合エンドポイント管理を使用して構成できます。

> **注：**
>
> この機能はシステムブラウザでのみサポートされています。

グローバルアプリ構成サービスの使用

グローバルアプリ構成サービスを使用して構成するには、次の手順を実行します。

1. 資格情報を使用してCitrix Cloudにサインインします。
2. **Workspace構成** > **アプリ構成** に移動します。
3. 「**アプリ構成**」ページでストアを選択し、「**構成**」をタップします。
4. 「**Workspace URL**」ページで、「**セキュリティと認証**」>「**認証**」に移動します。
5. 「**認証ブラウザの種類**」で「**iOS**」を選択し、ドロップダウンメニューから「**system**」を選択します。



6. 選択したストアの設定を公開するには、「**ドラフトの公開**」をタップします。

Global App Configurationサービスの詳細については、Global App Configurationサービスのドキュメントにあるオンプレミスストアの設定を構成するを参照してください。

統合エンドポイント管理ソリューションの使用

統合エンドポイント管理を使用して構成するには、次の手順を実行します。

1. Unified Endpoint Management (UEM) プロバイダーにサインインします。
2. UEMプロバイダーで管理するCitrix Workspaceアプリを追加します。UEMプロバイダーのポータルを使用してアプリをアップロードし、UEMプロバイダーによる管理を有効にできます。または、App Storeのアプリにリンクすることもできます。
3. アプリのアプリ構成ポリシーを作成します。
4. XMLプロパティリストにキーと値のペアを追加し、次の値を入力します。

```
<dict>

                <key>category</key>

                <string>authentication</string>
```

```
                <key>userOverride</key>
                <false/>
                <key>settings</key>
                <array>
                    <dict>
                        <key>name</key>
                        <string>settings_auth_web_browser</string>
                        <key>value</key>
                        <string>system</string>
                    </dict>
                </array>
</dict>
```

詳細については、Unified Endpoint Managementソリューションを使用してWorkspaceアプリを構成するを参照してください。

クライアント証明書認証

重要:

- StoreFrontを使用する場合、Citrix Workspaceアプリは以下をサポートします。
  - Citrix Access Gateway Enterprise Editionバージョン9.3
  - NetScaler Gatewayバージョン10.xからバージョン11.0
  - Citrix Gatewayバージョン11.1以降
- iOS向けCitrix Workspaceアプリは、クライアント証明書認証をサポートしています。

- Access Gateway Enterprise Edition 9.xおよび10.x（およびそれ以降のリリース）のみがクライアント証明書認証をサポートしています。
- 二重ソース認証タイプはCERTとLDAPである必要があります。
- Citrix Workspaceアプリは、オプションのクライアント証明書認証もサポートしています。
- P12形式の証明書のみがサポートされています。

Citrix Gateway仮想サーバーにサインインするユーザーは、仮想サーバーに提示されるクライアント証明書の属性に基づいて認証することもできます。クライアント証明書認証は、別の認証タイプであるLDAPと組み合わせて使用することで、二重ソース認証を提供することもできます。

管理者は、クライアント側の証明書属性に基づいてエンドユーザーを次のように認証できます。

- 仮想サーバーでクライアント認証が有効になっていること。
- 仮想サーバーがクライアント証明書を要求すること。
- Citrix Gateway上の仮想サーバーにルート証明書をバインドすること。

ユーザーがCitrix Gateway仮想サーバーにサインインすると、認証後、証明書の**SubjectAltName:OtherName:MicrosoftUniversalPrincipalName**フィールドからユーザー名とドメイン情報を抽出できます。これは`username@domain`の形式です。

ユーザーがユーザー名とドメインを抽出し、必要な情報（パスワードなど）を提供すると、認証が完了します。ユーザーが有効な証明書と資格情報を提供しない場合、またはユーザー名/ドメインの抽出に失敗した場合、認証は失敗します。

デフォルトの認証タイプをクライアント証明書を使用するように設定することで、クライアント証明書に基づいてユーザーを認証できます。また、クライアントSSL証明書に基づく認証中に何を行うかを定義する証明書アクションを作成することもできます。

XenApp®ファームを構成するには

Citrix Virtual Apps™コンソールまたはWeb Interfaceコンソールで、モバイルデバイス用のXenAppファームを作成します。使用するコンソールは、インストールされているCitrix Virtual Appsのバージョンによって異なります。

Citrix Workspaceアプリは、XenAppファームを使用して、ユーザーが権限を持つアプリケーションに関する情報を取得します。同じ情報は、デバイスで実行されているアプリと共有されます。こ

の方法は、従来のSSLベースのCitrix Virtual Apps接続でWeb Interfaceを使用する方法と似ており、Citrix Gatewayを構成できます。

モバイルデバイス用Citrix WorkspaceアプリがCitrix Gatewayからの接続をサポートするように、XenAppファームを次のように構成します。

1. XenAppファームで、**セキュアクライアントアクセスを管理** > **セキュアクライアントアクセス設定を編集** を選択します。
2. アクセス方法をGateway Directに変更します。
3. Citrix GatewayアプライアンスのFQDNを入力します。
4. Secure Ticket Authority (STA)情報を入力します。

Citrix Gatewayアプライアンスを構成するには

クライアント証明書認証の場合、CertおよびLDAP認証ポリシーを使用して、Citrix Gatewayを2要素認証で構成します。Citrix Gatewayアプライアンスを構成するには:

1. Citrix WorkspaceアプリからのCitrix Virtual Apps接続を許可するように、Citrix Gatewayでセッションポリシーを作成します。新しく作成したXenAppファームの場所を指定します。

    - 接続がCitrix Workspaceアプリからのものであることを識別するセッションポリシーを作成します。セッションポリシーを作成する際に、次の式を構成し、式の演算子として「すべての式に一致」を選択します:

      ```
      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
      ```

    - セッションポリシーの関連プロファイル構成で、**セキュリティ**タブの**デフォルトの承認**を**許可**に設定します。

      公開アプリケーションタブで、設定がグローバル設定でない場合（「グローバルを上書き」チェックボックスを選択した場合）、**ICA®プロキシ**フィールドが**ON**に設定されていることを確認します。

      Web Interfaceの**アドレス**フィールドに、デバイスユーザーが使用するXenAppファームのconfig.xmlを含むURLを入力します。例:

        - /XenAppServerName/Citrix/PNAgent/config.xml または
        - /XenAppServerName/CustomPath/config.xml。

    - セッションポリシーを仮想サーバーにバインドします。
    - CertおよびLDAPの認証ポリシーを作成します。

- 認証ポリシーを仮想サーバーにバインドします。
- TLSハンドシェイクでクライアント証明書を要求するように仮想サーバーを構成します。これを行うには、**Certificate** > **open SSL Parameters** > **Client Authentication** に移動し、**Client Certificate** を **Mandatory** に設定します。

> **重要:**
>
> - Citrix Gatewayで使用されるサーバー証明書が証明書チェーンの一部である場合。たとえば、それが中間証明書である場合は、Citrix Gatewayに証明書をインストールします。証明書のインストールについては、Citrix Gatewayのドキュメントを参照してください。
> - 認証が実行される前にクライアント証明書が必須に設定されている場合、ユーザーは証明書を手動でインポートする必要があります。

モバイルデバイスを構成するには

Citrix Gatewayでクライアント証明書認証が有効になっている場合、ユーザーはクライアント証明書の特定の属性に基づいて認証されます。認証後、証明書からユーザー名とドメインを抽出できます。各ユーザーに特定のポリシーを適用できます。

1. Citrix Workspaceアプリから、**Account** を開き、サーバーフィールドにCitrix Gatewayサーバーの一致するFQDNを入力します。たとえば、GatewayClientCertificateServer.organization.com。Citrix Workspaceアプリは、クライアント証明書が必要であることを自動的に検出します。
2. ユーザーは新しい証明書をインストールするか、すでにインストールされている証明書リストから選択できます。iOSクライアント証明書認証の場合、Citrix Workspaceアプリからのみ証明書をダウンロードしてインストールしてください。
3. 有効な証明書を選択すると、サインイン画面のユーザー名とドメインフィールドには、証明書からのユーザー名が事前に入力されます。エンドユーザーは、パスワードを含む他の詳細を入力できます。
4. クライアント証明書認証がオプションに設定されている場合、ユーザーは証明書ページで「戻る」を押して証明書の選択をスキップできます。この場合、Citrix Workspaceアプリは接続を続行し、ユーザーにログオン画面を提供します。

5. ユーザーが最初のサインインを完了すると、証明書を再度提供することなくアプリケーションを開始できます。Citrix Workspaceアプリは、アカウントの証明書を保存し、将来のログオン要求に自動的に使用します。

認証用のWebブラウザを切り替えるサポート

23.2.0以降、オンプレミスのCitrix GatewayおよびStoreFront展開で高度な認証ポリシーが構成されている場合、管理者はiOSまたはiPadデバイスで認証プロセスに使用されるブラウザを埋め込みブラウザからシステムブラウザに切り替えることができます。

認証プロセスのリライトポリシーを構成する

管理者は、認証プロセスで使用されるブラウザを埋め込みブラウザからシステムブラウザに切り替えることができます。これは、オンプレミスのCitrix GatewayおよびStoreFront展開で高度な認証ポリシーが構成されている場合にのみ可能です。高度な認証ポリシーを構成するには、NetScalerコマンドラインを使用してNetScalerリライトポリシーを構成します。

1. `enable ns feature REWRITE`
2. `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
3. `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ(\"/cgi/authenticate\")" insert_auth_browser_type_hdr_act`
4. `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_pol -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

システムブラウザに移行すると、次のようなより多くの機能が提供されます。

- 証明書ベースの認証でより良いエクスペリエンス。
- 認証プロセス中にデバイスのキーストアから既存のユーザー証明書を使用する機能。
- SITHS eIDのような一部のサードパーティ認証システムをサポート。

管理者が上記のリライトポリシーを構成していない場合、埋め込みブラウザが認証のデフォルトブラウザとして使用されます。

この表は、NetScaler® GatewayおよびGlobal App Config Serviceの設定に基づいて認証に使用されるブラウザを示しています。

ネットスケーラー ゲートウェイ	グローバルアプリ構成サービス	認証に使用されるブラウザ
システム	システム	システム

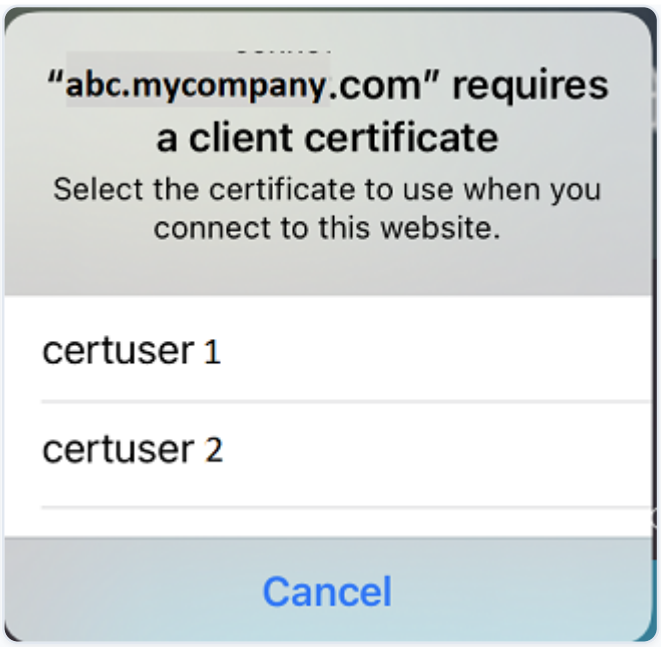
ネットスケーラー ゲートウェイ	グローバルアプリ構成サービス	認証に使用されるブラウザ
システム	埋め込み	システム
埋め込み	システム	システム
埋め込み	埋め込み	埋め込み
設定なし	システム	システム
設定なし	埋め込み	埋め込み

オンプレミスストアの証明書ベースの認証をサポート

エンドユーザーは、証明書がデバイスのキーチェーンに保存されている場合、証明書ベースの認証を処理できるようになりました。サインイン時に、Citrix Workspaceアプリはデバイス上の証明書のリストを検出し、認証用の証明書を選択できます。

重要:

証明書を選択すると、その選択は次回のCitrix Workspaceアプリ起動時にも保持されます。別の証明書を選択するには、iOSデバイスの設定から「Safariをリセット」するか、Citrix Workspaceアプリを再インストールします。



> **注：**
>
> この機能はオンプレミス展開をサポートしています。
>
> 構成するには：

1. Global App Configuration Store Settings API URLに移動し、クラウドストアのURLを入力します。 例: `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`。
2. **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** に移動し、**POST**をクリックします。
3. **INVOKE API**をクリックします。
4. ペイロードの詳細を入力してアップロードします。次のいずれかの値を選択します。

   - "Embedded": WKWebViewを使用できます。このオプションはデフォルトで設定されています。
   - "system": Safariビューコントローラーを使用できます。

   例:

   ```
   "category": "Authentication",

   "userOverride": false,

   "settings": [

   { "name": "Web Browser to use for Authentication", "value":
   "*Embedded*/*System*" },
   ```

   iOSまたはiPadデバイスでは、管理者は認証プロセスに使用されるブラウザを切り替えることができます。オンプレミスのCitrix GatewayおよびStoreFront展開で高度な認証ポリシーが構成されている場合、埋め込みブラウザからシステムブラウザに切り替えることができます。詳細については、「認証プロセスの書き換えポリシーを構成する」を参照してください。
5. サービスをプッシュするには、**EXECUTE** をクリックします。

スマートカード

Citrix Workspaceアプリは、セッション内接続のみSITHSスマートカードをサポートしています。

FIPS Citrix Gatewayデバイスを使用している場合は、SSL再ネゴシエーションを拒否するようにシステムを構成してください。詳細については、Knowledge Centerの記事CTX123680を参照してください。

以下の製品と構成がサポートされています。

- サポートされているリーダー：
  - Precise Biometrics Tactivo for iPad Mini ファームウェアバージョン 3.8.0
  - Precise Biometrics Tactivo for iPad（第4世代）およびTactivo for iPad（第3世代）およびiPad 2 ファームウェアバージョン 3.8.0
  - BaiMobile® 301MPおよび301MP-L スマートカードリーダー
  - サースビー PKard USB リーダー
  - Feitian iR301 USBリーダー
  - Type-C CCID準拠リーダー
  - Twocanoes スマートカードユーティリティリーダー
- サポートされているVDAスマートカードミドルウェア
  - ActiveIdentity
- サポートされているスマートカード：
  - PIVカード
  - 共通アクセスカード (CAC)
- サポートされる構成:
  - StoreFront 2.xおよびXenDesktop 7.x以降またはXenApp 6.5以降を使用したCitrix Gatewayへのスマートカード認証

Citrix Workspaceアプリを構成してアプリにアクセスするには

1. アカウント作成時にCitrix Workspaceアプリを自動的に構成してアプリにアクセスする場合は、アドレスフィールドにストアの一致するURLを入力します。例:
   - StoreFront.organization.com
   - netscalervserver.organization.com
2. スマートカードを使用して認証する場合は、**［Use Smartcard］**オプションを選択します。

注：

ストアへのログオンは約1時間有効です。その時間を過ぎると、ユーザーは他のアプリケーションを更新または起動するために再度ログオンする必要があります。

Type-Cベースの汎用リーダーのサポート

バージョン23.12.0以降、iOS向けCitrix Workspaceアプリは、スマートカード認証用のType-C CCID準拠リーダーをサポートするようになりました。以前は、Lightningポートベースのリーダーのみがサポートされていました。Citrix WorkspaceアプリにType-Cスマートカードリーダーが組み込まれたことで、ユーザーはCitrix Workspaceアプリを介して認証し、仮想デスクトップセッション内でスマートカードをシームレスに使用できるという2つの利点が得られます。

Twocanoesスマートカードユーティリティリーダーのサポート

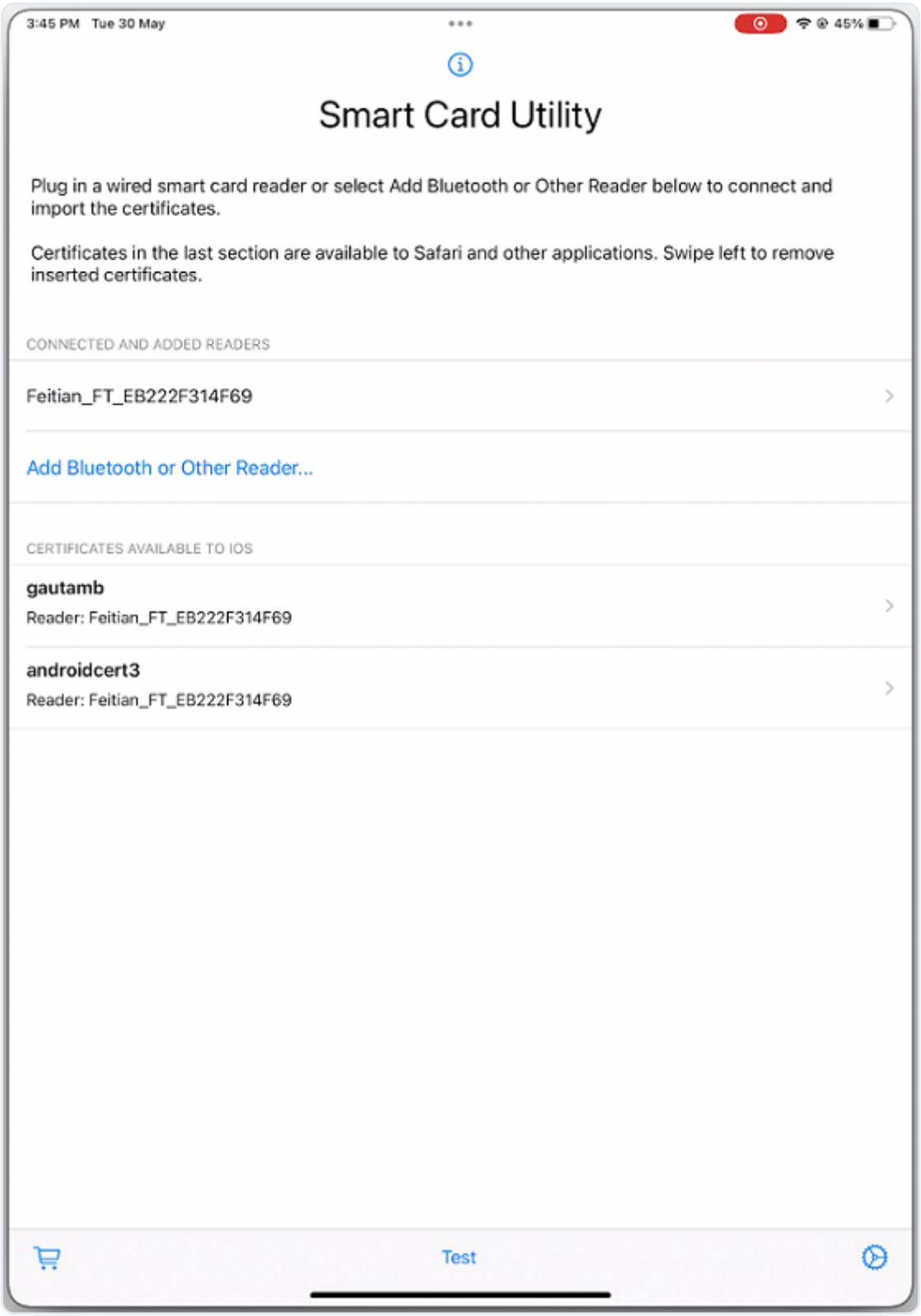
バージョン24.3.5以降、iOS向けCitrix WorkspaceアプリはTwocanoesスマートカードユーティリティリーダーをサポートしています。サポートされているスマートカードリーダーについて詳しくは、「スマートカード」を参照してください。

注：

TwocanoesスマートカードユーティリティUSB-Cリーダーは、Citrix Workspaceアプリのログインと仮想セッションのログインの両方でサポートされています。ただし、TwocanoesスマートカードユーティリティBluetoothリーダーは、Citrix Workspaceアプリのログインのみをサポートしており、仮想セッションのログインはサポートしていません。

TwocanoesスマートカードユーティリティBluetoothリーダーを構成するには、次の手順を実行します。

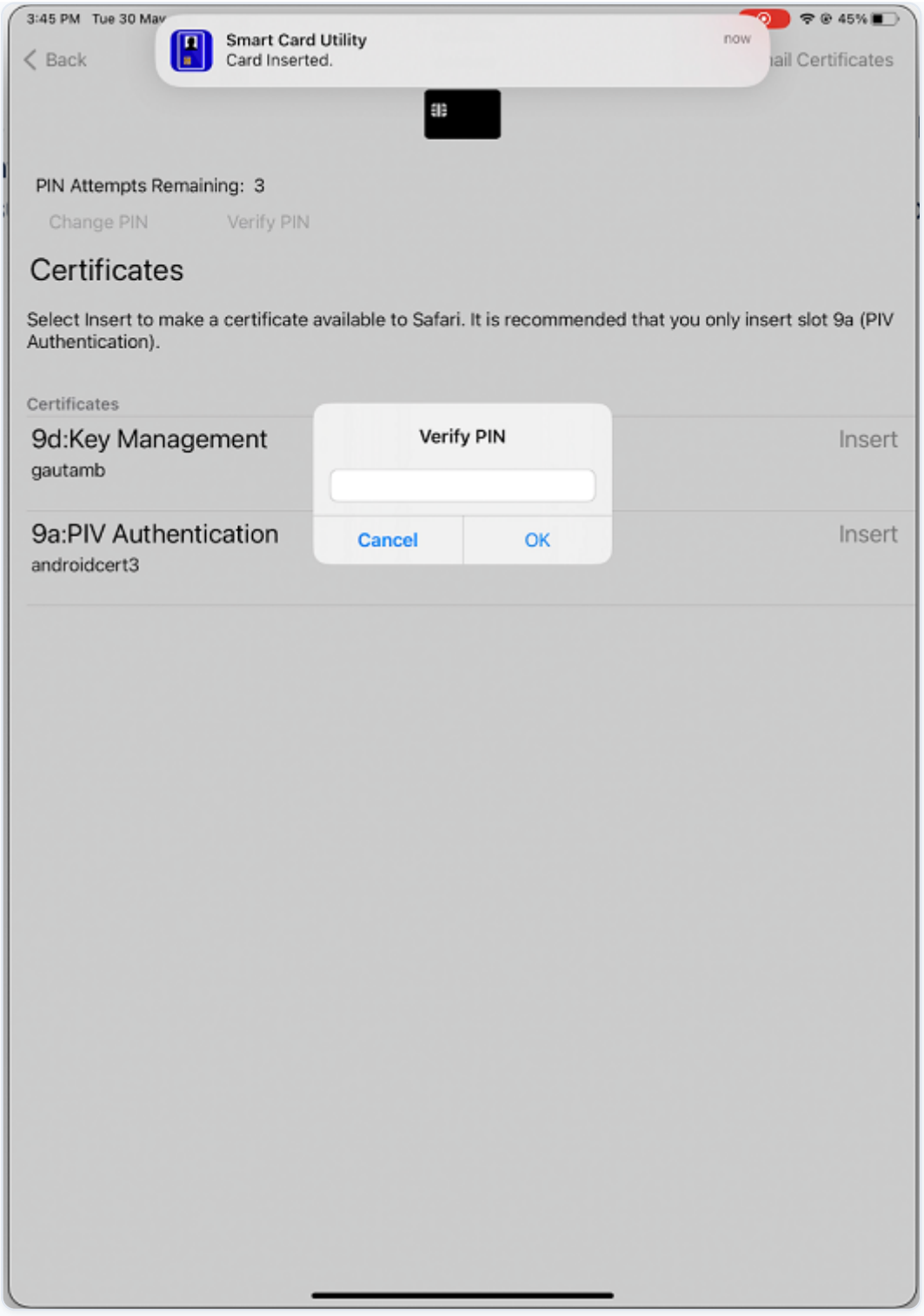
1. App StoreからSmart Card Utilityアプリをダウンロードしてインストールします。詳細については、TwocanoesナレッジベースのSmart Card Utility Bluetooth Reader Quick Startを参照してください。
2. デバイスのBluetoothがオンになっていて、スマートカードがリーダーに挿入されていることを確認します。
3. Smart Card Utilityアプリを開きます。



4. Bluetoothリーダーを使用している場合は、**Add Bluetooth or Other Reader…**をタップし、接続するリーダーを選択します。

> **注：**

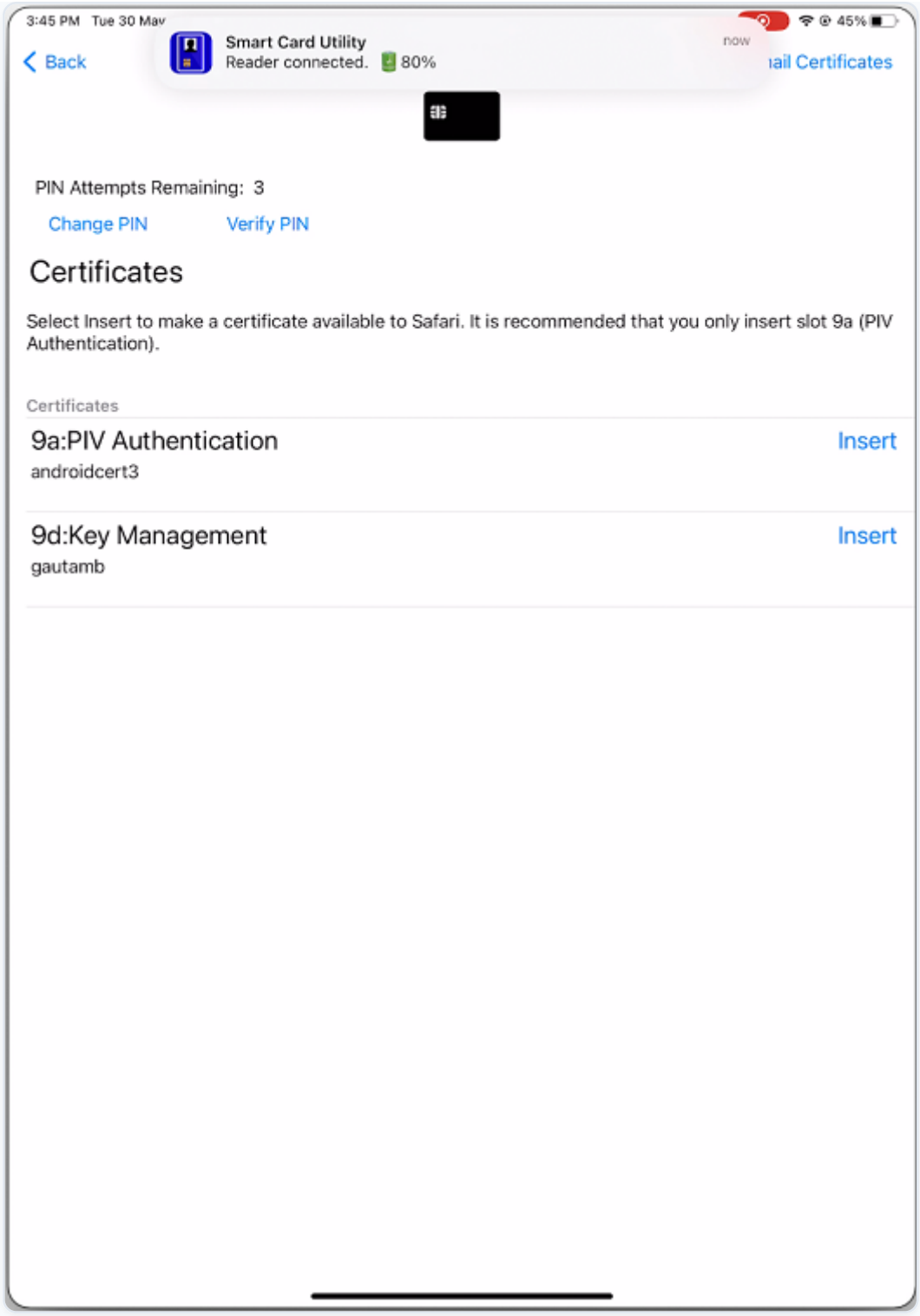
> リーダーでPINペアリングが有効になっている場合は、プロンプトが表示されたら**PIN**を入力する必要があります。**PIN**はリーダーの裏面に記載されています。



5. 必要な証明書で**Insert**をタップして、キーチェーンインターフェイスにコピーします。

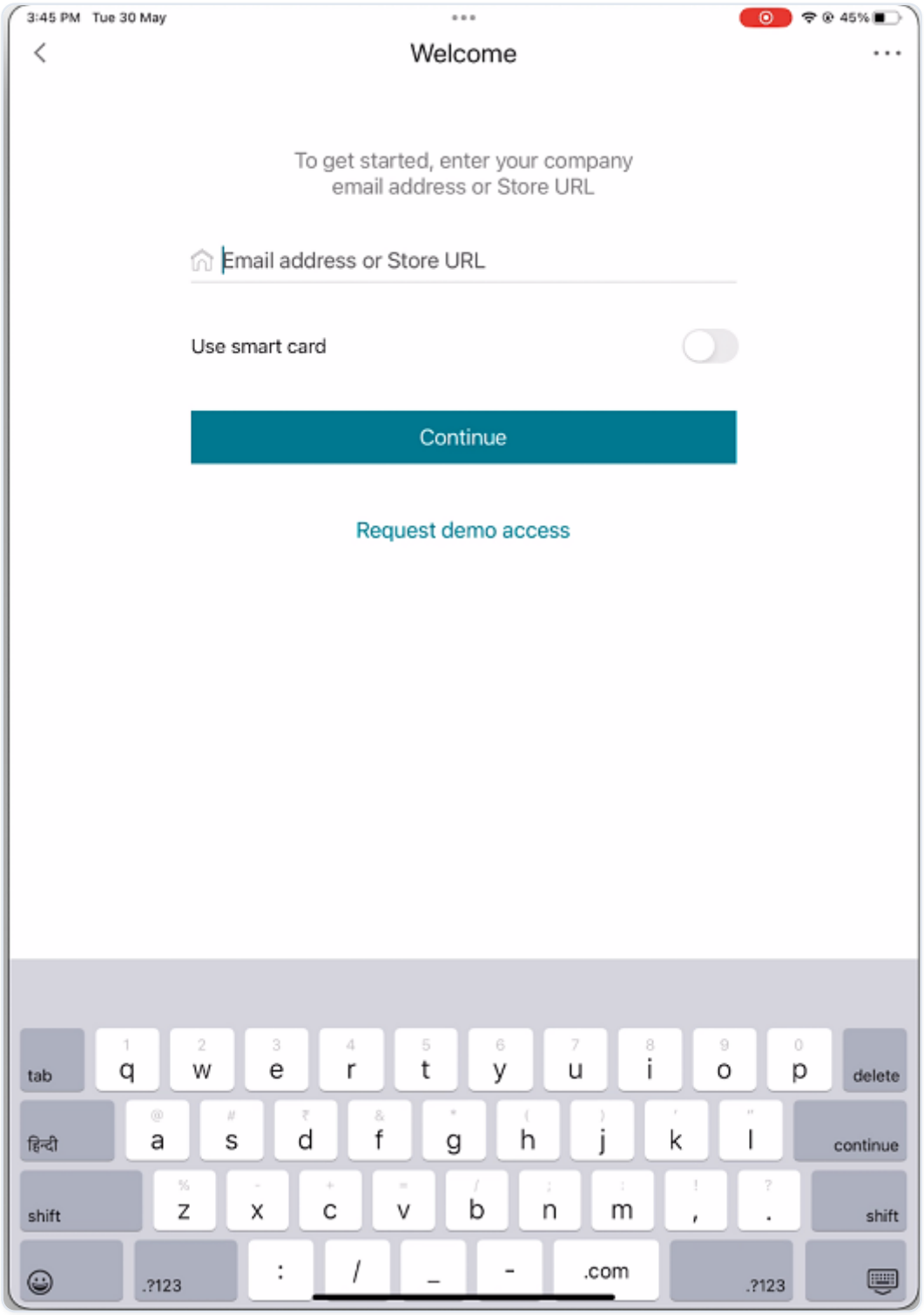
> **注：**

Smart Card Utilityアプリは、Appleが提供するcryptokit拡張機能を実装しており、証明書をトークンの形式でキーチェーンインターフェイスに書き込みます。詳細については、Apple開発者向けドキュメントのConfigure Smart Card Authenticationを参照してください。



6. リーダーがデバイスに接続されたままであることを確認します。

7. Citrix Workspaceアプリを開き、スマートカード認証で構成されているストアURLを入力します。



8. 証明書画面で、必要な証明書を選択し、IT管理者が提供したスマートカードPINを入力してサインインします。

   スマートカードソフトピン(/en-us/citrix-workspace-app-for-ios/media/smart-card-soft-pin.png)

9. 複数のストアにアクセスできる場合は、必要なストアを選択し、**続行**をタップします。

スマートカードの複数ストア(/en-us/citrix-workspace-app-for-ios/media/smart-card-multiple-stores.png)

10. 認証が成功すると、Citrix Workspaceアプリにサインインします。

スマートカード認証におけるYubiKeyのサポート

バージョン23.12.0以降、YubiKeyを使用してスマートカード認証を実行できるようになりました。この機能は、Citrix Workspaceアプリ、およびVDAセッション内の仮想セッションと公開アプリに対して、単一デバイスでの認証エクスペリエンスを提供します。スマートカードリーダーやその他の外部認証デバイスを接続する必要がなくなります。YubiKeyはOTP、FIDOなど、幅広いプロトコルをサポートしているため、エンドユーザーエクスペリエンスが簡素化されます。

Citrix WorkspaceアプリにサインインするにはエンドユーザーはYubiKeyをiPhoneまたはiPadに挿入し、スマートカードトグルをオンにして、ストアURLを提供する必要があります。

> **注：**
>
> この機能は、StoreFront展開におけるCitrix Workspaceアプリへの直接接続のみをサポートしており、Citrix Gateway経由ではサポートしていません。Citrix Gateway経由のスマートカード認証におけるYubiKeyのサポートは、将来のリリースで利用可能になる予定です。 Citrix Workspaceアプリ for iOSは、YubiKey 5シリーズのみをサポートしています。YubiKeyの詳細については、YubiKey 5シリーズを参照してください。

スマートカード認証における複数証明書のサポート

以前は、Citrix Workspaceアプリ for iOSは、接続されたスマートカードの最初のスロットで利用可能な証明書を表示していました。

バージョン24.1.0以降、Citrix Workspaceアプリ for iOSは、スマートカードで利用可能なすべての証明書を表示します。この機能により、スマートカード認証時に必要な証明書を選択できます。

証明書の選択(/en-us/citrix-workspace-app-for-ios/media/smart-card-certificate.png)

スマートカードで利用可能なすべての証明書を表示

バージョン23.7.5以降、Citrix Workspaceアプリ for iOSは、スマートカードで利用可能な複数の証明書を表示し、スマートカードベースの認証に使用する証明書を選択できるようになりました。スマートカードトグルが有効になると、**証明書の選択**ページから必要な証明書を選択できます。

複数のスマートカードを表示(/en-us/citrix-workspace-app-for-ios/media/multiple-certificate.png)

RSA SecurID認証

Citrix Workspaceアプリは、Secure Web Gateway構成用のRSA SecurID認証をサポートしています。これらの構成は、Web Interfaceを介して、およびすべてのCitrix Gateway構成に対して行われます。

iOS版Citrix Workspaceアプリのソフトウェアトークンに必要なURLスキーム: Citrix Workspaceアプリで使用されるRSA SecurIDソフトウェアトークンは、URLスキームcom.citrix.securidのみを登録します。

エンドユーザーがiOSデバイスにCitrix WorkspaceアプリとRSA SecurIDアプリの両方をインストールしている場合、ユーザーはRSA SecurIDソフトウェアオーセンティケーター（ソフトウェアトークン）をデバイス上のCitrix Workspaceアプリにインポートするために、URLスキーム**com.citrix.securid**を選択する必要があります。

RSA SecurIDソフトトークンをインポートするには

Citrix WorkspaceアプリでRSAソフトトークンを使用するには、管理者として、エンドユーザーが以下に従うことを確認してください。

- PINの長さに関するポリシー
- PINの種類（数字のみ、英数字）
- PINの再利用に関する制限

エンドユーザーがRSAサーバーに正常に認証された後、エンドユーザーはPINを一度だけ設定する必要があります。PINの検証後、StoreFrontサーバーでも認証されます。すべての検証が完了すると、Workspaceアプリは利用可能な公開アプリケーションとデスクトップを表示します。

RSAソフトトークンを使用するには

1. 組織から提供されたRSAソフトトークンをインポートします。
2. SecurIDファイルが添付されたメールから、インポート先として**Open in Workspace**を選択します。ソフトトークンがインポートされると、Citrix Workspaceアプリが自動的に開きます。
3. 組織からインポートを完了するためのパスワードが提供された場合は、組織から提供されたパスワードを入力し、**OK**をクリックします。**OK**をクリックすると、トークンが正常にインポートされたことを示すメッセージが表示されます。
4. インポートメッセージを閉じ、Citrix Workspaceアプリで**アカウントの追加**をタップします。

5. 組織から提供されたストアのURLを入力し、**次へ**をクリックします。
6. ログオン画面で、ユーザー名、パスワード、ドメインなどの資格情報を入力します。PINフィールドには、組織から別のデフォルトPINが提供されていない限り、**0000**を入力します。PIN 0000はRSAのデフォルトですが、組織のセキュリティポリシーに従って変更されている場合があります。
7. 左上隅にある**ログオン**をクリックします。PINを作成するためのメッセージが表示されます。
8. 4〜8桁のPINを入力し、**OK**をクリックします。新しいPINを確認するためのメッセージが表示されます。
9. もう一度PINを入力し、**OK**をクリックします。これでアプリとデスクトップにアクセスできます。

次のトークンコード

Citrix Workspaceアプリは、RSA SecurID認証でCitrix Gatewayを構成する際に、次のトークンコード機能をサポートします。3回誤ったパスワードを入力すると、Citrix Gatewayプラグインにエラーメッセージが表示されます。サインインするには、次のトークンを待ちます。RSAサーバーは、ユーザーが誤ったパスワードで何度もログオンした場合に、ユーザーのアカウントを無効にするように構成できます。

派生資格情報

Citrix Workspaceアプリ内でPurebred派生資格情報のサポートが利用可能です。派生資格情報を許可するストアに接続する場合、ユーザーは仮想スマートカードを使用してCitrix Workspaceアプリにログオンできます。この機能は、オンプレミス展開でのみサポートされています。

> **注：**
>
> この機能を使用するには、Citrix Virtual Apps and Desktops™ 7 1808以降が必要です。

> Citrix Workspaceアプリで派生資格情報を有効にするには：

1. **設定** > **詳細** > **派生資格情報**に移動します。
2. **派生資格情報を使用**をタップします。

派生資格情報で使用する仮想スマートカードを作成するには：

1. **設定** > **詳細** > **派生資格情報**で、**新しい仮想スマートカードを追加**をタップします。

2. 仮想スマートカードの名前を編集します。
3. 8桁の数字のみのPINを入力し、確認します。
4. **次へ**をタップします。
5. 認証証明書の下で、**証明書のインポート…**をタップします。
6. ドキュメントピッカーが表示されます。**参照**をタップします。
7. 場所の下で、**Purebred Key Chain**を選択します。
8. リストから適切な認証証明書を選択します。
9. **キーのインポート**をタップします。
10. 必要に応じて、デジタル署名証明書と暗号化証明書について、手順5〜9を繰り返します。
11. **保存**をタップします。

仮想スマートカードには、3つ以下の証明書をインポートできます。仮想スマートカードが正しく機能するには、認証証明書が必要です。暗号化証明書とデジタル署名証明書は、VDAセッションでの使用のために追加できます。

> **注：**
>
> HDX™セッションに接続すると、作成された仮想スマートカードがセッションにリダイレクトされます。

既知の制限事項

- ユーザーは一度に1枚のアクティブなカードしか持つことができません。
- 仮想スマートカードは一度作成すると編集できません。カードを削除して再作成してください。
- PINは最大10回まで無効にできます。10回試行しても無効な場合、仮想スマートカードは削除されます。
- 派生資格情報を選択すると、仮想スマートカードが物理スマートカードを上書きします。

ユーザーエージェント

Citrix Workspaceアプリは、ネットワークリクエストでUser-Agent文字列を送信します。これは、他のIDプロバイダー (IdP) への認証のリダイレクトを含む認証ポリシーを設定するために使用できます。

注

以下の表のUser-Agentの一部として記載されているバージョン番号は例であり、使用しているバージョンに基づいて自動的に更新されます。

シナリオ	IOS (WKWEBVIEW)	IOS (サファリビューコントローラ)	IPADOS (WKWEBVIEW)	IPADOS (サファリビューコントローラ)
クラウドストア	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone AuthManager/24.7.0.1	デフォルトのSafari User-Agent文字列。	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1.	デフォルトのSafari User-Agent文字列。
クラウドストア - SaaSおよびWebアプリ	デフォルトのWKWebview User-Agent文字列。	デフォルトのSafari User-Agent文字列。	`isFeatureUseSafariUserAgentForSaasWebviewEnabled`が有効な場合、以下のUser-Agentが送信されます	デフォルトのSafari User-Agent文字列。

シナリオ	IOS (WKWEBVIEW)	IOS (サファリビューコントローラ)	IPADOS (WKWEBVIEW)	IPADOS (サファリビューコントローラ)
同上	同上	同上	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15) AppleWebKit/605.1.15 (KHTML, like Gecko) / Version/13.4	同上
同上	同上	同上	`Safari/605.1.15` `shouldTunnelWebViewTraffic` がTrueに設定されている場合、以下のUser-Agentが送信されます Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15) AppleWebKit/605.1.15 (KHTML, like Gecko) / Version/13.4 Safari/605.1.15/ CitrixReceiver/24.5.0/ X1Class CWACapable	同上
同上	同上	同上		同上

シナリオ	IOS (WKWEBVIEW)	IOS (サファリビューコントローラ)	IPADOS (WKWEBVIEW)	IPADOS (サファリビューコントローラ)
オンプレミスストア	デフォルトのWKWebview User-Agent文字列。	デフォルトのSafari User-Agent文字列。	---	デフォルトのSafari User-Agent文字列。
NetScaler Gatewayを使用したオンプレミスストア	デフォルトのWKWebview User-Agent文字列。	デフォルトのSafari User-Agent文字列。	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1	デフォルトのSafari User-Agent文字列。
NetScaler GatewayとnFactor認証を使用したオンプレミスストア	Mozilla/5.0 (マッキントッシュ; インテル Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) モバイル/15E148 CWA/24.7.0 iOS/18.0	デフォルトのSafariユーザーエージェント文字列。	Mozilla/5.0 (マッキントッシュ; インテル Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) モバイル/15E148 CWA/24.7.0 iOS/18.0	デフォルトのSafariユーザーエージェント文字列。

シナリオ	IOS (WKWEBVIEW)	IOS (サファリビューコントローラ)	IPADOS (WKWEBVIEW)	IPADOS (サファリビューコントローラ)
	X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-アイフォーン AuthManager/24.7.0.1		X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-アイパッド AuthManager/24.7.0.1	

WKWebViewのユーザーエージェント文字列

バージョン23.3.5以降、WKWebViewを介して開始される一部のネットワーク要求中に使用されるユーザーエージェント文字列には、デフォルトでCitrix Workspaceアプリの識別子が含まれるようになりました。

そのため、次のように変更されました。 `Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0`

次のいずれかに変更されます。

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone` (iPhoneの例)

または

`Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad` (iPadの例)

nFactor認証

多要素（nFactor）認証のサポート

多要素認証は、ユーザーがアクセスするために複数の身元証明を提供することを要求することで、アプリケーションのセキュリティを強化します。多要素認証により、認証手順と関連する資格情報収集フォームを管理者が構成できるようになります。

ネイティブのCitrix Workspaceアプリは、StoreFrontにすでに実装されているフォームログオンサポートに基づいて、このプロトコルをサポートできます。Citrix GatewayおよびTraffic Manager仮想サーバーのWebログオンページもこのプロトコルを使用します。

詳細については、SAML認証、および多要素（nFactor）認証を参照してください。

制限事項:

- nFactorサポートが有効になっている場合、Touch IDやFace IDなどの生体認証は使用できません。

nFactor高度認証ポリシーのサポート

Citrix GatewayでnFactor Advanced認証ポリシーを通じて構成された場合、Citrix Workspaceアプリで証明書ベースの認証をサポートするようになりました。nFactor認証は、柔軟で機敏な多要素スキーマの構成に役立ちます。

ユーザーエージェント文字列:

Citrix WorkspaceアプリのiPhoneまたはiPadで高度な（nFactor）認証を実行すると、認証プロセスは埋め込みWebViewにリダイレクトされます。結果として得られるユーザーエージェント文字列は、OSバージョン、CWAビルドバージョン、デバイスモデル、およびAuthManagerバージョンによって若干異なる場合があります。たとえば、iPhoneおよびiPadの次のユーザーエージェント文字列を考慮してください。

iPhoneの場合：

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/16.2 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone AuthManager/3.3.0.0
```

iPadの場合：

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0
```

注：

- バージョンまたはデバイスモデルの情報は、環境によって異なる場合があります。
- 認証中にiOS版Citrix Workspaceアプリ固有のユーザーエージェントベースのポリシーを適用するには、次のキーワードを使用します。
  - iOS
  - CWA
  - CWA対応

HDXセッションへの接続時のFIDO2ベース認証のサポート

23.9.0バージョン以降、iOS版Citrix Workspaceアプリは、FIDO2ベースの認証方法を使用してCitrix Virtual Apps and Desktopsセッション内でパスワードレス認証をサポートするようになりました。この機能により、ユーザーはFIDO2対応のYubicoセキュリティキーを使用して、Google ChromeやMicrosoft Edgeなどのブラウザで WebAuthn対応のWebサイトにサインインできます。WebAuthn対応のWebサイトを開くだけで、パスワードレス認証がトリガーされます。 Lightningポートベースのデバイスのみがサポートされています（USB-CまたはUSB 4ポートを備えたデバイスはサポートされていません）。パスワードレス認証を使用したCitrix Workspaceアプリまたはデスクトップセッションへのサインインはサポートされていません。

前提条件の詳細については、Citrix Virtual Apps and DesktopsドキュメントのFIDO2を使用したローカル認証と仮想認証を参照してください。

クラウドストアへの接続時のFIDO2を使用した認証のサポート

24.5.0バージョン以降、ユーザーはクラウドストアに接続する際に、FIDO2ベースのパスワードレス認証を使用してCitrix Workspaceアプリに認証できます。FIDO2はシームレスな認証方法を提供し、企業従業員がユーザー名やパスワードを入力することなく、仮想セッション内のアプリやデスクトップにアクセスできるようにします。この機能は、ローミング認証器（USBのみ）とプ

ラットフォーム認証器（PINコード、Touch ID、Face IDのみ）の両方をサポートしています。この機能はデフォルトで有効になっています。

> **注：**
>
> FIDO2認証は、デフォルトでChromeカスタムタブでサポートされています。WebViewでFIDO2認証を使用することに関心がある場合は、このPodioフォームを使用して関心を登録してください。

オンプレミス展開での認証トークンのストレージ構成のサポート

Citrix Workspace アプリ for iOS は、オンプレミスストアの認証トークンをローカルディスクに保存するオプションを提供するようになりました。この機能により、セキュリティ強化のために認証トークンの保存を無効にできます。無効にした後、システムまたはセッションが再起動すると、セッションにアクセスするために再度認証する必要があります。

管理設定ファイルを使用してオンプレミス展開での認証トークンの保存を無効にするには、次の手順を実行します。

1. テキストエディターを使用して、通常 `C:\inetpub\wwwroot\Citrix\Roaming directory` にある web.config ファイルを開きます。
2. ファイル内でユーザーアカウント要素を見つけます (store は展開のアカウント名です)。 例: `<account id=... name="Store">`
3. `</account>` タグの前に、そのユーザーアカウントのプロパティに移動して、以下を追加します。

```
<properties>

    <property name="TokenPersistence" value="false" />

</properties>
```

web.config ファイルの例を次に示します。

```
<account id="########################################" name="Store
Service"

    description="" published="true" updaterType="None"
remoteAccessType="StoresOnly">

    <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_Store">

            <metadata>

                <plugins>

                    <clear />

                </plugins>

                <trustSettings>

                    <clear />

                </trustSettings>

                <properties>

                    <clear />

                    <property name="TokenPersistence" value="false" />

                 </properties>

            </metadata>

        </annotatedServiceRecord>

    </annotatedServices>

    <metadata>

    <plugins>
```

```
      <clear />
    </plugins>
    <trustSettings>
      <clear />
    </trustSettings>
    <properties>
    </properties>
  </metadata>
</account>
```

セッションタイムアウト後の再認証

バージョン 23.3.0 以降、前回のサインイン以降にセッションの有効期限が切れている場合、Citrix Workspace アプリへの再認証を求められるようになりました。Web またはネイティブクライアントから Citrix Workspace アプリに接続する際、2 要素認証またはユーザー名とパスワードの入力を求められます。

セキュリティ

サーバーファームとCitrix Workspaceアプリ間の通信を保護するには、Citrix Gatewayを含むさまざまなセキュリティ技術を使用して、サーバーファームへの接続を統合します。

> **注：**
>
> Citrixでは、StoreFrontサーバーとユーザーデバイス間の通信を保護するためにCitrix Gatewayを使用することをお勧めします。

- SOCKSプロキシサーバーまたはセキュアプロキシサーバー（セキュリティプロキシサーバー、HTTPSプロキシサーバーとも呼ばれます）。

  プロキシサーバーを使用して、ネットワークへのアクセスを制限したり、Citrix Workspaceアプリとサーバー間の接続を処理したりできます。Citrix WorkspaceアプリはSOCKSおよびセキュアプロキシプロトコルをサポートしています。
- セキュアWebゲートウェイ。

  Secure Web GatewayをWeb Interfaceと組み合わせて使用すると、インターネットを介して社内ネットワーク上のサーバーへの単一で安全な暗号化されたアクセスポイントを提供できます。

  Secure Web GatewayをWeb Interfaceと組み合わせて使用すると、単一で安全な暗号化されたデータを提供できます。社内ネットワーク上のサーバーは、インターネットを介して保護されたデータにアクセスできます。
- Transport Layer Security（TLS）プロトコルを使用したSSLリレーソリューション。
- ファイアウォール。

  ネットワークファイアウォールは、宛先アドレスとポートに基づいてパケットを許可またはブロックできます。

  サーバーの内部ネットワークIPアドレスを外部インターネットアドレスにマッピングする（つまり、ネットワークアドレス変換、またはNAT）ネットワークファイアウォールを介してCitrix Workspaceアプリを使用している場合は、外部アドレスを構成してください。

地理的位置に基づくマルチサイトストアフェイルオーバーのサポート

バージョン24.12.0以降、マルチストアフェイルオーバー処理機能は、ストアアドレスチェックを非同期で実行し、新しいフェイルオーバーストアアドレスが検出されたときに古いストアエントリを削除することで、マルチストアフェイルオーバー処理を改善します。障害によるフェイルオーバーが発生した場合、Global Server Load Balancer（GSLB）はクライアントを新しいサイトにリダイレクトします。この機能により、以前追加したストアを起動する際に、Gateway検出器がユーザーの地理的位置に基づいてストアアドレスが変更されたかどうかを確認します。新しいアドレスが見つかった場合、クライアントは自動的に古いストアエントリを削除し、新しいエントリを追加します。このプロセスはバックグラウンドで実行され、手動での介入なしに新しいストアへのシームレスな移行を可能にします。 この機能はオンプレミスストアにのみ適用されることに注意してください。

前提条件：

ユーザーはストアにログインする必要があります。

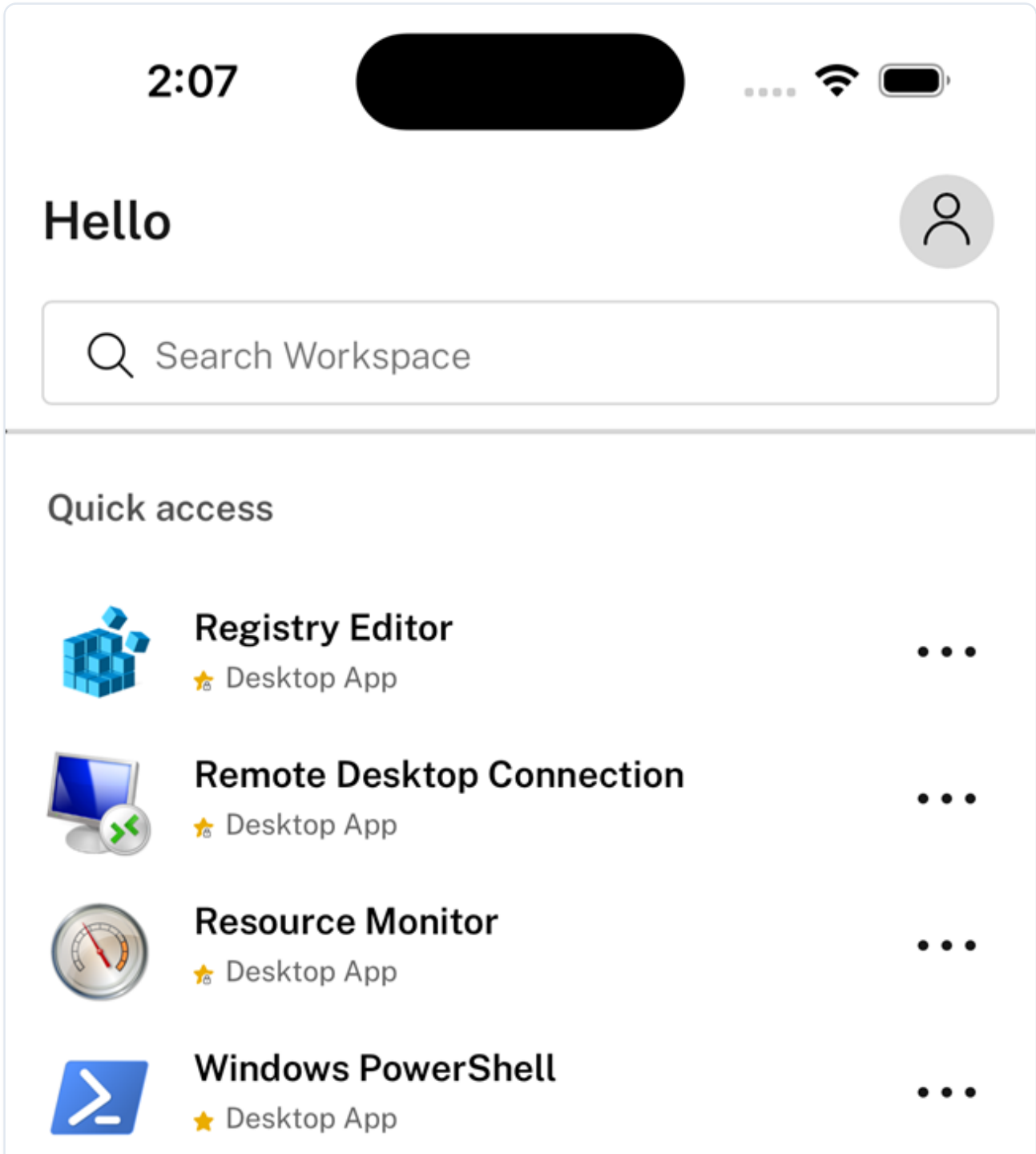
制限事項:

ログインセッションクッキーの有効期限が切れると、URL取得用のAPIが失敗するため、マルチストアフェイルオーバーは自動的に発生しません。この場合、ログインページが表示されます。

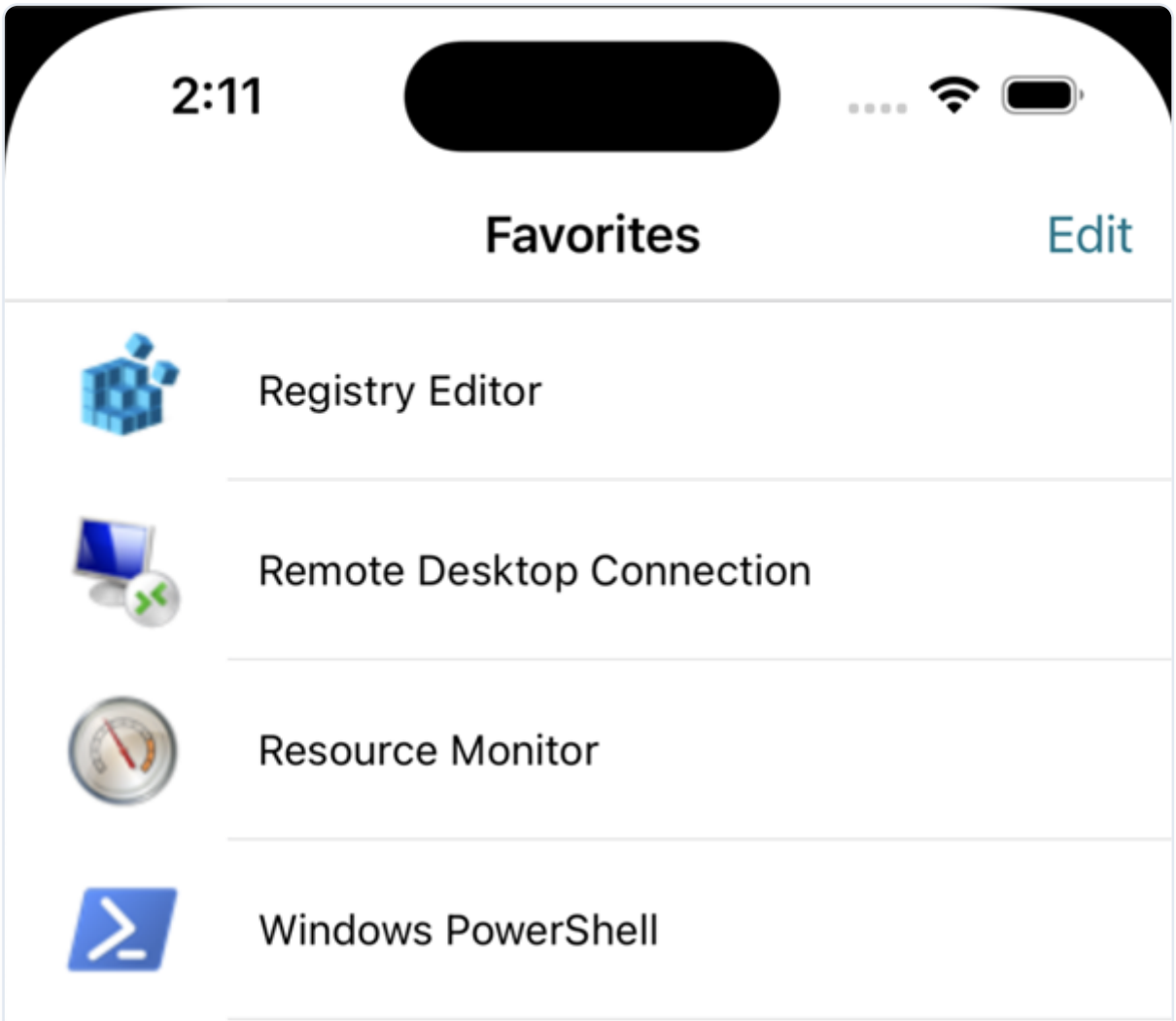
ゲートウェイを使用したオンプレミスWSUIのサポート

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、ゲートウェイの背後にあるオンプレミスストアのWeb UIもサポートします。この機能はデフォルトでは有効になっていないため、管理者が構成する必要があります。構成の詳細については、「オンプレミスストアの新しいUI（テクニカルプレビュー）」を参照してください。

次の画像は現在のUIを示しています。


2:07
Hello
Search Workspace
Quick access
Registry Editor
Desktop App
Remote Desktop Connection
Desktop App
Resource Monitor
Desktop App
Windows PowerShell
Desktop App

次の画像は新しいUIを示しています。


2:11
Favorites
Edit
Registry Editor
Remote Desktop Connection
Resource Monitor
Windows PowerShell

Citrix ゲートウェイ

リモートユーザーがCitrix Gatewayを介してCitrix Endpoint Management展開に接続できるようにするには、StoreFrontで動作するように証明書を構成できます。アクセスを有効にする方法は、展開におけるCitrix Endpoint Managementのエディションによって異なります。

ネットワークにCitrix Endpoint Managementを展開する場合、Citrix GatewayとStoreFrontを統合することで、内部ユーザーまたはリモートユーザーがCitrix Gatewayを介してStoreFrontに接続できるようにします。この展開により、ユーザーはStoreFrontに接続して、XenAppから公開されたアプリケーションやXenDesktopから仮想デスクトップにアクセスできます。ユーザーはCitrix Workspaceアプリを介して接続します。

セキュアWebゲートウェイ

このトピックは、Web Interfaceを使用する展開にのみ適用されます。

Secure Web Gatewayを通常モードまたはリレーモードで使用して、Citrix Workspaceアプリとサーバー間の通信にセキュアなチャネルを提供できます。Secure Web Gatewayを**通常**モードで使用している場合、Citrix Workspaceアプリには構成は不要です。エンドユーザーがWeb Interfaceを介して接続していることを確認してください。

Citrix Workspaceアプリは、Secure Web Gatewayを実行しているサーバーに接続するために、Web Interfaceサーバーでリモートで構成された設定を使用します。

Secure Web Gatewayプロキシがセキュアネットワーク内のサーバーにインストールされている場合、Secure Web Gatewayプロキシをリレーモードで使用できます。リレーモードを使用している場合、Secure Web Gatewayサーバーはプロキシとして機能するため、Citrix Workspaceアプリを次のように構成する必要があります。

- Secure Web Gatewayサーバーの完全修飾ドメイン名（FQDN）。
- Secure Web Gatewayサーバーのポート番号。

> **注：**

> Secure Web Gatewayバージョン2.0はリレーモードをサポートしていません。

> FQDNは、次の3つのコンポーネントを順番にリストする必要があります。

- ホスト名

- 中間ドメイン
- トップレベルドメイン

例えば、`my_computer.example.com` はFQDNです。これは、ホスト名 (`my_computer`)、中間ドメイン (example)、トップレベルドメイン (`com`) を順にリストしているためです。中間ドメインとトップレベルドメインの組み合わせ (`example. com`) は、ドメイン名と呼ばれます。

プロキシサーバー

プロキシサーバーは、ネットワークへのアクセスを制限し、Citrix Workspaceアプリとサーバー間の接続を処理するために使用されます。Citrix Workspaceアプリは、SOCKSとセキュアプロキシプロトコルの両方をサポートしています。

Citrix Workspaceアプリは、Citrix Virtual Apps and Desktopsサーバーと通信するためにプロキシサーバー設定を使用します。プロキシサーバー設定は、Web Interfaceサーバーでリモートから構成されます。

Citrix WorkspaceアプリがWebサーバーと通信する場合、アプリはプロキシサーバー設定を使用します。ユーザーデバイスのデフォルトWebブラウザーのプロキシサーバー設定を適切に構成してください。

ファイアウォール

ネットワークファイアウォールは、宛先アドレスとポートに基づいてパケットを許可またはブロックできます。展開でファイアウォールを使用している場合、Citrix Workspaceアプリはファイアウォールを介してWebサーバーとCitrixサーバーの両方と通信できる必要があります。ファイアウォールは、ユーザーデバイスからWebサーバーへの通信のためにHTTPトラフィックを許可する必要があります。通常、セキュアなWebサーバーが使用されている場合、HTTPトラフィックは標準のHTTPポート80または443を介して行われます。Citrixサーバー通信の場合、ファイアウォールはポート1494および2598でインバウンドICAトラフィックを許可する必要があります。

ファイアウォールがネットワークアドレス変換 (NAT) 用に構成されている場合、Web Interfaceを使用して、内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。たとえば、Citrix Virtual Apps and DesktopsおよびCitrix DaaS (旧称 Citrix Virtual Apps and Desktops service) サーバーが代替アドレスで構成されていない場合、Web Interfaceを構成して、Citrix Workspaceアプリ for iOSに代替アドレスを提供できます。Citrix Workspaceアプリ for iOSは、その後、外部アドレスとポート番号を使用してサーバーに接続します。

TLS

Citrix Workspaceアプリは、XenAppおよびXenDesktopへのTLS接続に対して、以下の暗号スイートでTLS 1.2および1.3をサポートしています。

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **注：**

> iOS 9以降またはバージョン21.2.0で実行されているCitrix Workspaceアプリは、以下のTLS暗号スイートをサポートしていません。

> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

> Transport Layer Security (TLS) は、TLSプロトコルの最新の標準化されたバージョンです。Internet Engineering Taskforce (IETF) は、TLSをオープン標準として開発する責任を引き継いだ際に、その名称をTLSに変更しました。

TLSは、サーバー認証、データストリームの暗号化、およびメッセージ整合性チェックを提供することにより、データ通信を保護します。米国政府機関を含む一部の組織では、データ通信を保護するためにTLSの使用を義務付けています。これらの組織は、Federal Information Processing Standard (FIPS) 140などの検証済み暗号化の使用も要求する場合があります。FIPS 140は暗号化の標準です。

Citrix Workspaceアプリは、1024、2048、3072ビット長のRSAキーをサポートしています。4096ビット長のRSAキーを持つルート証明書もサポートされています。

> **注：**

- Citrix Workspaceアプリは、Citrix WorkspaceアプリとStoreFront間の接続にiOSプラットフォームの暗号化を使用します。

TLSの構成と有効化

TLSのセットアップには、主に2つの手順があります。

1. Citrix Virtual Apps and Desktops™サーバーとWeb InterfaceサーバーでSSLリレーをセットアップし、必要なサーバー証明書を取得してインストールします。
2. ユーザーデバイスに同等のルート証明書をインストールします。

ユーザーデバイスにルート証明書をインストールする

TLSが有効なCitrix WorkspaceアプリとCitrix Virtual Apps and Desktops間の通信を保護するには、ユーザーデバイスにルート証明書が必要です。この証明書は、サーバー証明書上の認証局の署名を検証できます。

iOSには、約100種類の商用ルート証明書がプリインストールされています。別の証明書を使用したい場合は、認証局から証明書を受け取り、各ユーザーデバイスにインストールできます。

組織のポリシーと手順に応じて、ユーザーにインストールを指示する代わりに、各ユーザーデバイスにルート証明書をインストールできます。最も簡単で安全な方法は、ルート証明書をiOSキーチェーンに追加することです。

ルート証明書をキーチェーンに追加するには

1. 証明書ファイルを添付したメールを自分宛に送信します。
2. デバイスで証明書ファイルを開きます。この操作により、キーチェーンアクセスアプリケーションが自動的に起動します。
3. プロンプトに従って証明書を追加します。
4. iOS 10以降では、iOSの **設定** > **一般** > **証明書信頼設定** に移動して、証明書が信頼されていることを確認します。

   証明書信頼設定の下にある「ルート証明書の完全な信頼を有効にする」セクションを参照してください。証明書が完全な信頼のために選択されていることを確認してください。

ルート証明書がインストールされます。TLS対応クライアントおよびその他のアプリケーションは、TLSを使用してルート証明書を使用できます。

Transport Layer Security 1.3のサポート

23.9.0以降、iOS向けCitrix Workspaceアプリは、パフォーマンスと効率を向上させるTransport Layer Security (TLS) 1.3をサポートするようになりました。TLS 1.3は、強力な暗号スイートとワンタイムセッションキーにより、堅牢なセキュリティを提供します。

エンドユーザーは、iOS向けCitrix Workspaceアプリで次のように有効にできます。

1. ［**Advanced settings**］ > ［**TLS Versions**］ の順に移動します。
2. ［**TLS 1.3 version**］ を選択します。

TLS 1.3(/en-us/citrix-workspace-app-for-ios/media/tls-setting.png)

DTLS 1.2のサポート

バージョン24.7.0以降、iOS向けCitrix WorkspaceアプリはDTLSプロトコルバージョン1.2をサポートします。DTLS 1.2は、堅牢な暗号化アルゴリズム、より優れたハンドシェイクプロトコル、さまざまな攻撃に対する保護など、以前のバージョンよりも機能強化と改善を提供します。このプロトコルは、全体的なセキュリティを向上させます。

> **注：**
>
> DTLSプロトコルバージョン1.2に問題がある場合、iOS向けCitrix Workspaceアプリは、以前にサポートされていたバージョンにシームレスにフォールバックします。

Citrix Device Postureサービスのサポート

バージョン2402以降、iOS向けCitrix Workspace™アプリはCitrix Device Postureサービスをサポートします。Citrix Device Postureサービスは、管理者がCitrix DaaS（仮想アプリとデスクトップ）またはCitrix Secure Private Access™リソースへのアクセスを得るためにエンドデバイスが満たす必要のある特定の要件を適用するのに役立つクラウドベースのソリューションです。

iOS向けCitrix Workspaceアプリの場合、デバイスポスチャは、Citrix WorkspaceアプリのバージョンとiOSデバイスのオペレーティングシステムバージョンのスキャンのみをサポートします。

詳しくは、Device Postureのドキュメントを参照してください。

> **注**
>
> この機能はクラウドストアでのみサポートされています。

XenApp and XenDesktop®サイト

XenApp®およびXenDesktopサイトを構成するには：

重要:

- Citrix Workspaceアプリは、Citrix Secure Gateway 3.xをサポートするXenAppおよびXenDesktopサイトを使用します。
- Citrix Workspaceアプリは、Citrix Secure Gateway 3.xをサポートするCitrix Virtual Apps Webサイトを使用します。
- XenAppおよびXenDesktopサイトは、シングルファクター認証のみをサポートします。
- Citrix Virtual Apps™ Webサイトは、シングルファクター認証とデュアルファクター認証の両方をサポートします。
- すべての組み込みブラウザーはWeb Interface 5.4をサポートしています。

この構成を開始する前に、Citrix Gatewayをインストールして、Web Interfaceと連携するように構成してください。これらの手順は、特定の環境に合わせて調整できます。

Citrix Secure Gateway接続を使用している場合は、Citrix WorkspaceアプリでCitrix Gateway設定を構成しないでください。

Citrix Workspaceアプリは、XenAppおよびXenDesktopサイトを使用して、エンドユーザーがアクセス権を持つアプリケーションに関する情報を取得します。このプロセスで、情報はデバイスで実行されているCitrix Workspaceアプリに表示されます。同様に、従来のSSLベースのCitrix Virtual Apps接続にはWeb Interfaceを使用できます。同じSSLベースの接続に対して、Citrix Gatewayを構成できます。Web Interface 5.xで実行されているXenAppおよびXenDesktopサイトには、この構成機能が組み込まれています。

Citrix Secure Gateway接続からの接続をサポートするようにXenAppおよびXenDesktopサイトを構成します。

1. XenAppおよびXenDesktopサイトで、［**Manage secure client access**］ > ［**Edit secure client access settings**］ の順に選択します。
2. アクセス方法を**［Gateway Direct］**に変更します。
3. Secure Web GatewayのFQDNを入力します。

4. Secure Ticket Authority（STA）情報を入力します。

> **注：**
>
> Citrix Secure Gateway の場合、Citrix は Citrix のデフォルトパス (//XenAppServerName/Citrix/PNAgent) を使用することを推奨します。デフォルトパスを使用すると、エンドユーザーは接続先の Secure Web Gateway の FQDN を指定できます。XenApp および XenDesktop サイトにある config.xml ファイルへのフルパスは使用しないでください。例: (//XenAppServerName/CustomPath/config.xml)。

Citrix Secure Gateway を構成するには

1. Citrix Secure Gateway 構成ウィザードを使用してゲートウェイを構成します。

   Citrix Secure Gateway は、XenApp Service サイトをホストするセキュアネットワーク内のサーバーをサポートします。

   「**Indirect**」オプションを選択した後、Secure Web Gateway サーバーの FQDN パスを入力し、ウィザードの手順を続行します。
2. ユーザーデバイスから接続をテストし、Secure Web Gateway がネットワークと証明書の割り当てに関して正しく構成されていることを確認します。

モバイルデバイスを構成するには

1. Citrix Secure Gateway アカウントを追加するときは、**アドレス**フィールドに Citrix Secure Gateway サーバーの一致する FQDN を入力します。

   - デフォルトパス (/Citrix/PNAgent) を使用して XenApp および XenDesktop サイトを作成した場合は、Secure Web Gateway の FQDN を入力します: FQDNofSecureGateway.companyName.com
   - XenApp および XenDesktop サイトのパスをカスタマイズした場合は、config.xml ファイルのフルパスを入力します。例: FQDNofSecureGateway.companyName.com/CustomPath/config.xml
2. アカウントを手動で構成する場合は、**新しいアカウント**ダイアログで Citrix Gateway オプションのチェックを外します。

セッションエクスペリエンス

EDT LossyモードがSecureHDX (SecureICA 2.0) 接続をサポートするようになりました

以前は:

- EDT Lossy (信頼性の低いサブチャネル) はDTLS暗号化のみで動作します。
- SecureHDX接続は、信頼性の高いトランスポートのみに限定されます。
- SecureHDX接続では、オーディオおよびビデオのパフォーマンスが低下する可能性がありました。

現在:

- EDT Lossyは現在、DTLSおよびSecureHDX接続の両方で動作します。
- SecureICA 2.0を使用すると、オーディオ、ビデオ、およびその他の遅延に敏感なチャネルのリアルタイムパフォーマンスが向上します。
- SecureHDX接続での遅延の削減により、ユーザーエクスペリエンスが向上します。

技術概要

この機能強化により、SecureHDX (SecureICA 2.0) 暗号化を使用する際に、信頼性の低いUDPサブチャネルを許可するようにネットワークトランスポート層が変更されます。信頼性の低いサブチャネルは、オーディオやビデオフレームなどの遅延に敏感なデータを伝送し、偶発的なパケット損失が許容されます。このアプローチでは、失われたパケットを再送信するのではなく、リアルタイム配信を優先します。

前提条件

- サーバーとクライアントの両方でSecureICA 2.0を有効にします。詳細については、Secure HDX™ Citrix Virtual Apps and Desktops™ 7 2511を参照してください。
- サーバーとクライアントの両方でEDT Lossyを有効にします。詳細については、Adaptive transport Citrix Virtual Apps and Desktops™ 7 2511を参照してください。

強化された接続強度インジケーター

25.7.2以降、接続強度インジケーターを強化しました。この機能強化により、接続品質に関するリアルタイムの洞察が得られ、接続の問題を自己解決するのに役立ちます。この機能はツールバーからアクセスでき、デフォルトで有効になっています。

前提条件:

- この機能を使用するには、強化されたDesktop Viewerツールバーを有効にします。管理者は、Global App Configurationサービスを通じて新しいツールバー機能を有効にする必要があります。この機能は、VDA 2407以降でのみ利用可能です。
- クライアント側でSupportability Virtual Channelを有効にする必要があります。これはCitrix WorkspaceアプリiOS 24.12.0でデフォルトで有効になっています。

接続強度インジケーター(/en-us/citrix-workspace-app-for-ios/media/connection-strength-indicator1.png)

接続強度インジケーター(/en-us/citrix-workspace-app-for-ios/media/connection-strength-indicator2.png)

利点:

- **即時フィードバック:** ネットワークの問題が検出されると、ネットワーク強度アイコンがユーザーに通知します。
- **強化されたトラブルシューティング:** リアルタイムの統計と診断により、ユーザーとITチームは接続の問題を特定し、解決できます。

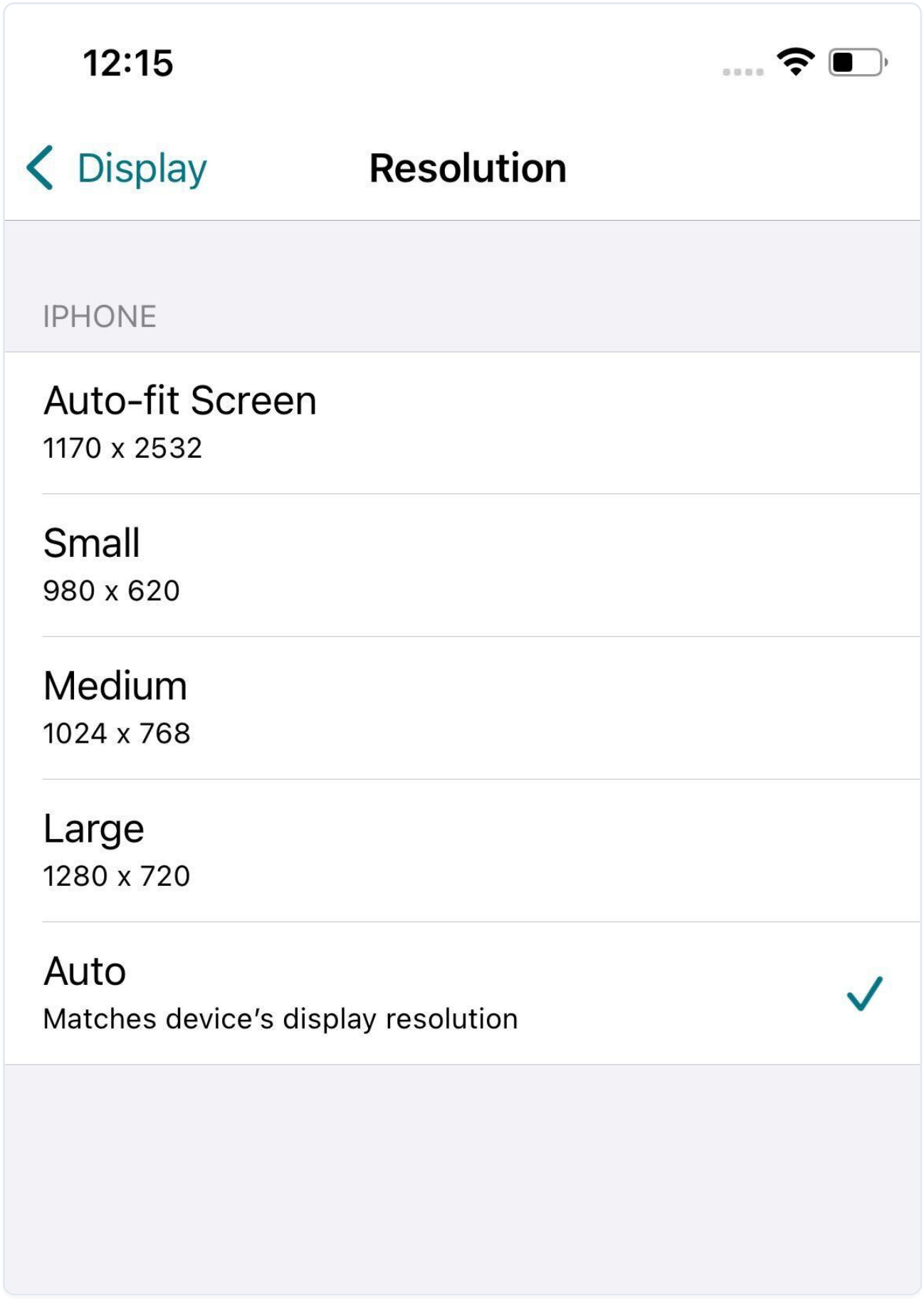
接続強度インジケーターの機能強化

- **まったく新しいUI:** ユーザーインターフェイスは、明瞭度の向上とより良いユーザーエクスペリエンスのために再設計されました。
- **追加の接続詳細:** インジケーターは、現在のデバイスのCPUとメモリの使用状況を表示するようになりました。
- **スコア化されたメトリックと推奨事項:** 遅延と帯域幅のスコアが計算され、表示されます。スコアが「Fair」または「Poor」の場合、問題に対処するための推奨事項が表示されます。
- **接続履歴:** 過去15分間の接続スコアが記録され、レイアウトの下部にあるグラフに表示されます。この複合スコアは帯域幅と遅延に基づいており、履歴データはコピーまたはダウンロード時にログに含まれます。
- **詳細のダウンロード:** 遅延、帯域幅、CPU、メモリ使用量を含むすべての接続メトリックが記録されます。過去15分間の接続履歴もダウンロード可能なログに含まれます。

強化されたセッション解像度

バージョン25.3.0以降、iOS版Citrix Workspaceアプリは、よりシームレスなユーザーエクスペリエンスのために、セッション解像度の機能強化を導入しています。デフォルトで自動に設定されている**DPI**設定は、ユーザーがセッションを起動するたびに自動的に調整され、全体的なエクスペリエンスが向上します。

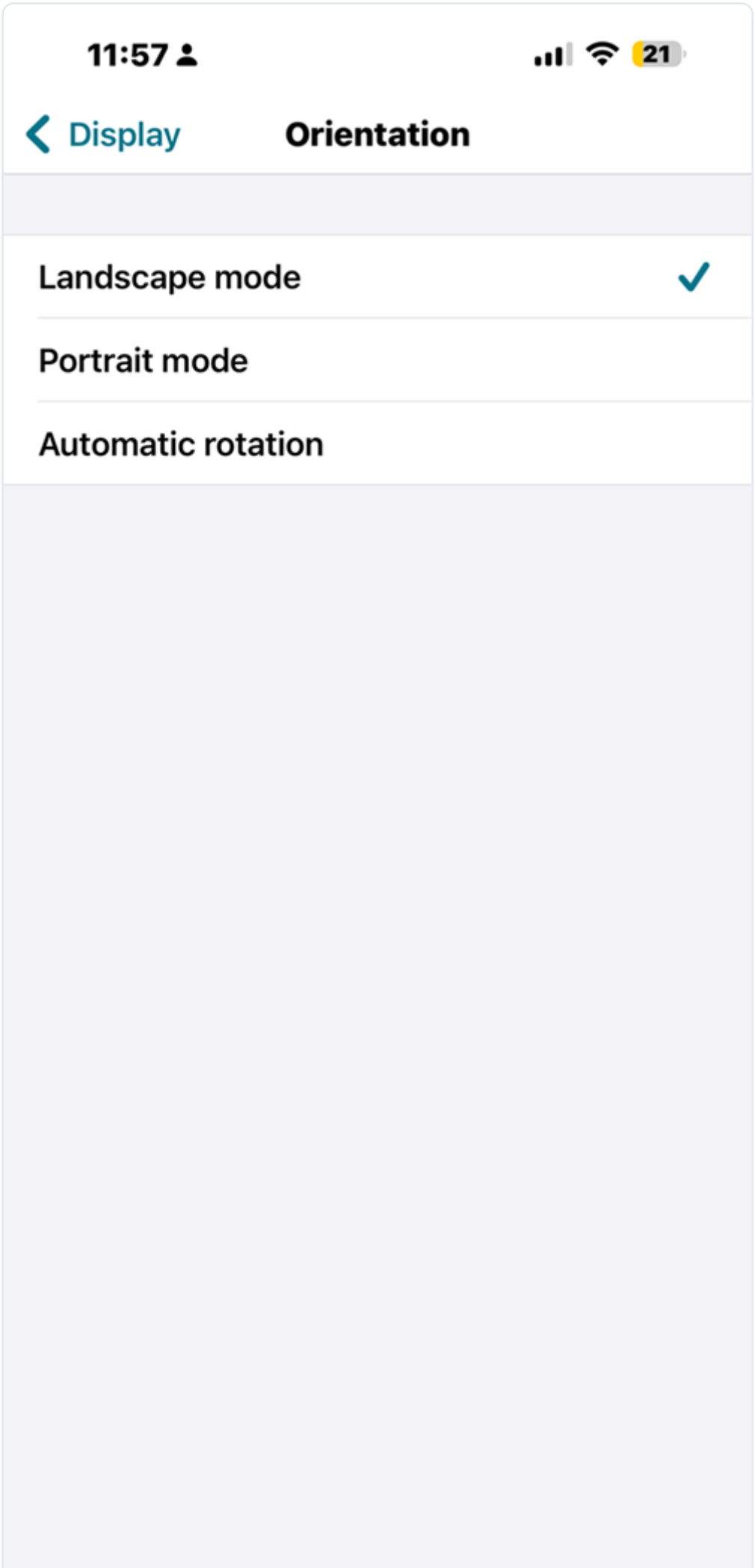
一貫性のあるユーザーフレンドリーなエクスペリエンスを確保するため、仮想デスクトップはデフォルトで横向きモードで起動するようになりました。これにより、ワイドスクリーンアプリケーションとマルチタスクのニーズに対応します。この機能はデフォルトで有効になっています。


12:15
Display
Resolution
IPHONE
Auto-fit Screen
1170 x 2532
Small
980 x 620
Medium
1024 x 768
Large
1280 x 720
Auto
Matches device's display resolution

仮想デスクトップのデフォルトの横向き

バージョン25.1.0以降、Citrix Workspaceアプリは、iPhoneデバイスで仮想デスクトップを起動する際に、デフォルトで横向きを強制します。これにより、ワイドスクリーンアプリケーションとマルチタスクに最適な一貫したユーザーエクスペリエンスが保証されます。ユーザーは、アプリまたはHDX-Toolbarを介して、横向きにロック、縦向きにロック、アプリケーションメタデータに基づいて自動調整、またはデバイスの画面向きに従うように向き設定を構成できます。この柔軟性により、縦向きモード用に設計されたアプリを含むさまざまなワークフローに対応しつつ、シームレスでユーザーフレンドリーなエクスペリエンスを維持します。

デフォルトの向きを構成するには、**Settings** > **Display** > **Orientation** > **Landscape mode**に移動します。


11:57
21
Display
Orientation
Landscape mode
Portrait mode
Automatic rotation

強化されたセキュアなICA®

バージョン25.1.0以降、新しいICA暗号化機能は、最新の暗号化アルゴリズムを使用することでセキュリティを向上させます。これにより、製品のセキュリティ体制が強化され、お客様はシンプルかつ信頼性の高い方法で環境のセキュリティ体制を向上させることができます。複雑な証明書管理を不要にすることでセットアップを簡素化し、Citrixポリシー設定を通じて簡単に構成できるようにします。この機能は、サポートされているすべてのプラットフォームでシームレスに動作します。

前提条件:

- 展開がCVAD Serviceまたはオンプレミスでの使用向けに構成されていることを確認します。
- サポートされているプラットフォームには、Windows、Linux、Mac、Android、iOS、HTML5、Chrome OSが含まれます。
- Citrix Studioへの管理者アクセスが必要です。

構成

この機能は、単一のポリシーまたはデリバリーグループのプロパティを使用して有効または無効にできます。Delivery Controller™ (DDC) にアクセスし、次の変更を行います。

1. 必要なポリシーを構成するには、**設定** > **コンピューター設定 - ICA** に移動します。
2. グループポリシーを更新するには、次のコマンドを実行します。 `gpupdate/force`
3. 変更を適用するには、セッションを再起動します。

DPIマッチング

DPIマッチング機能により、仮想セッションがデバイスのDPIに従ってレンダリングされるようになります。バージョン25.1.0のリリース以降、新しい表示設定によりDPIマッチング機能が強化されました。

- 自動解像度検出：アプリがデバイスの画面解像度を自動的に識別します。
- 動的DPI調整：仮想デスクトップセッションのDPIが、検出されたディスプレイの解像度に合わせて動的に調整されます。これにより、それぞれのディスプレイで最適な鮮明度、読みやすさ、および使いやすさが保証されます。
- スムーズなスケーリング：DPIが調整されると、UI要素、フォント、および画像が歪みやピクセル化なしでスムーズにスケーリングされます。
- 最大4Kの解像度をサポートします。

自動 (DPIマッチング) オプションにより、シームレスな表示エクスペリエンスのためにDPIが自動調整されます。DPI設定は、アプリ内で**設定** > **表示** > **解像度**に移動してアクセスできます。

DPIマッチング(/en-us/citrix-workspace-app-for-ios/media/dpi-matching.png)

接続強度インジケーター

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、**Desktop Viewer**ツールバーで接続強度インジケーターをサポートします。この機能は、ネットワークの問題を警告するネットワーク強度アイコンを表示します。アイコンをクリックすると、クライアント、ゲートウェイ、VDAのリアルタイム接続統計を表示し、高度なトラブルシューティングのために診断情報をIT部門と共有するためにコピーできます。

前提条件:

- この機能を使用するには、拡張Desktop Viewerツールバーを有効にします。管理者は、Global App Configurationサービスを通じて新しいツールバー機能を有効にする必要があります。この機能は、VDA 2405以降でのみ利用可能です。
- サポート性仮想チャネルはクライアント側で有効にする必要がありますが、これはCitrix WorkspaceアプリiOS 24.12.0でデフォルトで有効になっています。

接続強度インジケーター(/en-us/citrix-workspace-app-for-ios/media/connection-strength-indicator.png)

インメモリICAソリューションの起動

バージョン24.12.0以降、iOS向けCitrix Workspaceアプリは、Citrix Workspaceランチャーを使用したインメモリハイブリッド起動のサポートを強化します。この改善により、ICAファイルをダウンロードする必要がなくなり、より効率的で安全なユーザーエクスペリエンスが可能になります。

前提条件:

iOS向けCitrix Workspaceアプリ24.12.0以降。

構成

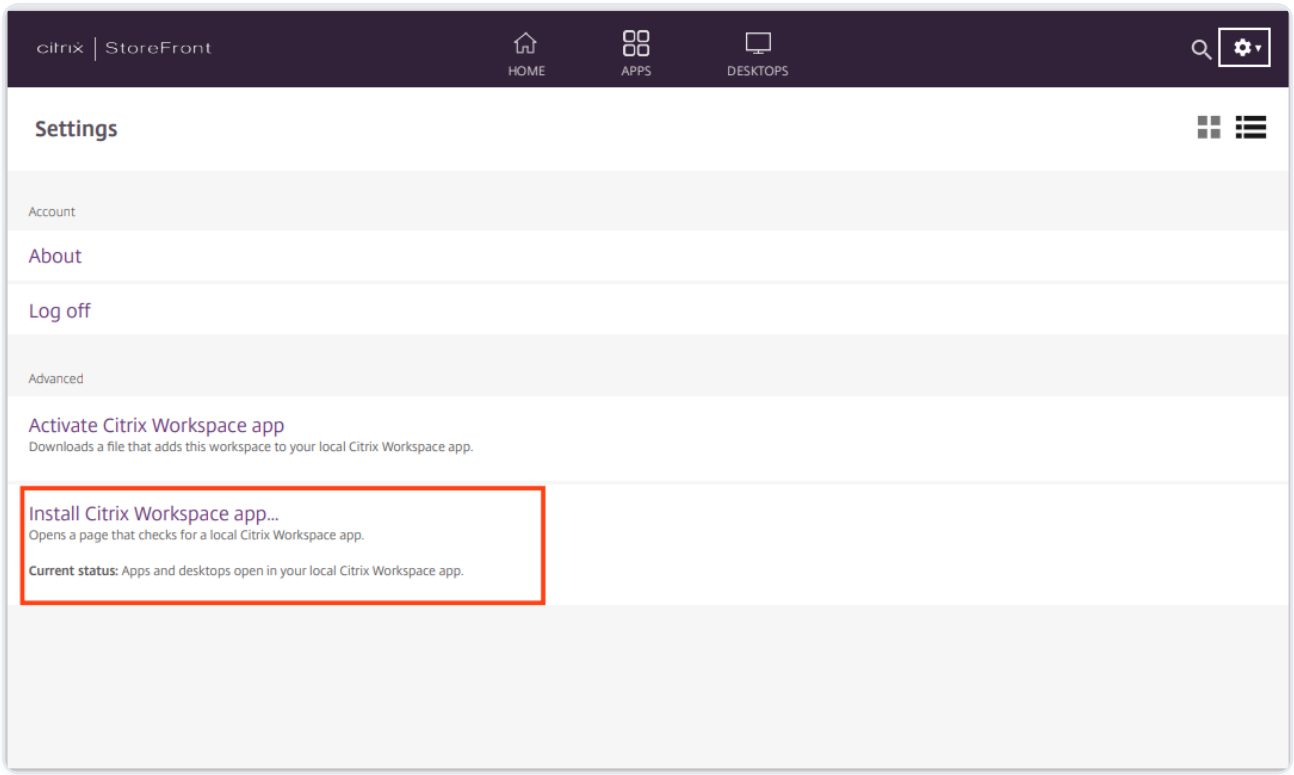
ICAファイルをダウンロードせずにCitrix Workspaceアプリを起動するには、iOSデバイスで次の手順を実行します。

1. サポートされているWebブラウザ（Safari、Chrome、またはFirefox）を開きます。
2. 組織のストアURLにアクセスし、資格情報を使用してサインインします。

3. ようこそ画面で、**Citrix Workspaceアプリを検出**を見つけてタップします。これにより、クライアント検出プロセスが開始され、Citrix Workspaceアプリが開きます。 Citrix Workspaceアプリを検出(/en-us/citrix-workspace-app-for-ios/media/detect-cwa.png)
4. 検出後、ブラウザに戻ります。組織ストアのホーム画面が表示されます。

ICAファイルをダウンロードすることなく、組織ストアのインターフェイスからアプリやデスクトップに直接アクセスして開くことができるようになりました。

初回ログイン時にクライアント検出をスキップした場合、 **> >** から移動できます。



制限事項:

クライアント検出に失敗した場合、システムは自動的にICAファイルをダウンロードし、ダウンロードされたファイルからセッションが起動します。

Rapid Scanのサポート

バージョン24.9.0以降、iOS向けCitrix WorkspaceアプリはRapid Scan機能をサポートしています。この機能を使用すると、iOSデバイスで複数のドキュメントをスキャンし、スキャンしたドキュメントをMac向けCitrix WorkspaceアプリとiOS向けCitrix Workspaceアプリを使用してMacデバイスに転送できます。

MacとiOSデバイスの両方でCitrix Workspaceにサインインしている場合、Rapid Scanを使用してiPhoneまたはiPadでドキュメントをスキャンできます。スキャンされたファイルはMacに保存さ

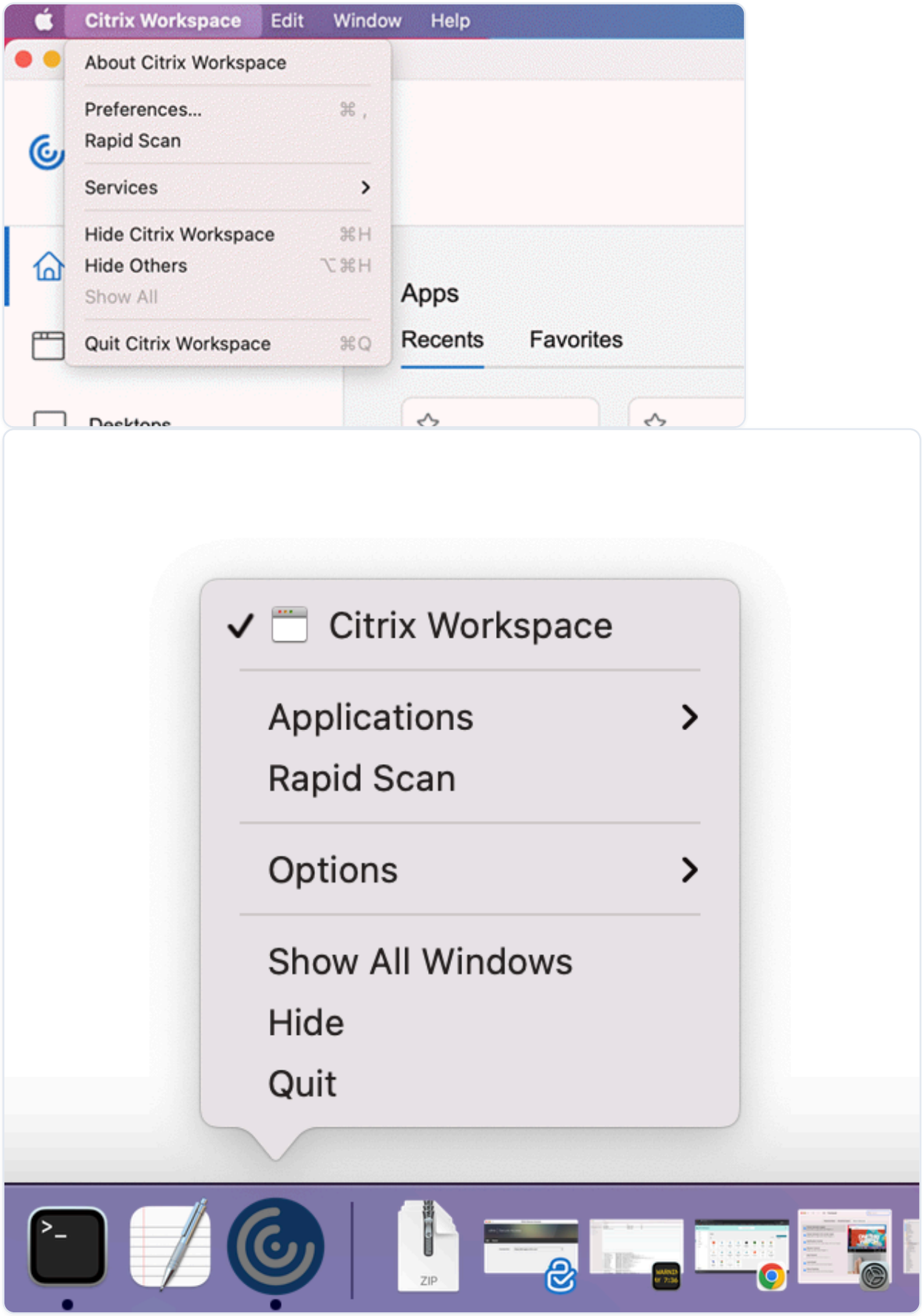
れ、クライアントドライブマッピングを使用して仮想デスクトップからリモートでアクセスすることもできます。この機能は、クラウドストアとオンプレミスストアの両方で機能します。

前提条件:

- 両方のデバイスが同じCitrix Workspaceアカウントにログインしていることを確認してください。
- 両方のデバイスが同じWi-Fiネットワークに接続されている必要があります。
- Mac向けCitrix Workspaceアプリはバージョン24.9.0以降である必要があります。

Rapid Scanの使用方法:

1. MacでCitrix Workspaceアプリを開きます。
2. DockまたはメニューバーのCitrix Workspaceアイコンを長押し（または右クリック）します。



3. メニューから****を選択します。Macの画面にQRコードが表示されます。
4. iOSデバイスで、**設定**に移動し、**Rapid Scan**をタップします。

5. iOSデバイスを使用して、Macに表示されているQRコードをスキャンします。
6. Macに確認ウィンドウが表示されたら、**はい**をクリックして接続を確立します。 これで、iOSデバイスを使用してドキュメントをスキャンできます。
7. スキャンしたファイルをPDFまたはJPEG形式で保存することを選択します。
8. デフォルトでは、スキャンされたドキュメントはMacの**ダウンロード**フォルダーに保存されます。
9. ダウンロードが完了したら、Macで**Finderで開く**をクリックして、スキャンされたドキュメントを見つけます。

仮想デスクトップからスキャンされたドキュメントにアクセスする:

1. 仮想デスクトップ内でMacのストレージドライブにアクセスするには、クライアントドライブマッピング (CDM) を有効にする必要があります。これにより、Macと仮想デスクトップ間でファイルを転送できます。この機能を有効にするには、管理者にお問い合わせください。
2. CDMが有効になると、ローカルドライブが仮想デスクトップに表示されます。
3. プロンプトが表示されたら、仮想デスクトップからローカルディスクにアクセスするための**読み取りと書き込み**のアクセス許可を許可します。
4. スキャンされたドキュメントが保存されているフォルダー（デフォルトでは**ダウンロード**フォルダー）に移動し、ファイルを仮想デスクトップのストレージにコピーします。

Appleネイティブの非ミラーモードのサポート

iPad OS 16.2で利用可能なAppleの非ミラーモードを使用して、ディスプレイを拡張できるようになりました。外部モニターでCitrix Workspaceアプリ、仮想アプリ、仮想デスクトップを実行し、iPad画面を他のネイティブアプリの実行に自由に使えるようにすることで、マルチタスクを実行できます。

> **注：**
>
> Appleの非ミラーモード拡張ディスプレイのサポートは、一部のiPadモデルでのみ利用可能です。詳細については、Appleのドキュメントを参照してください。

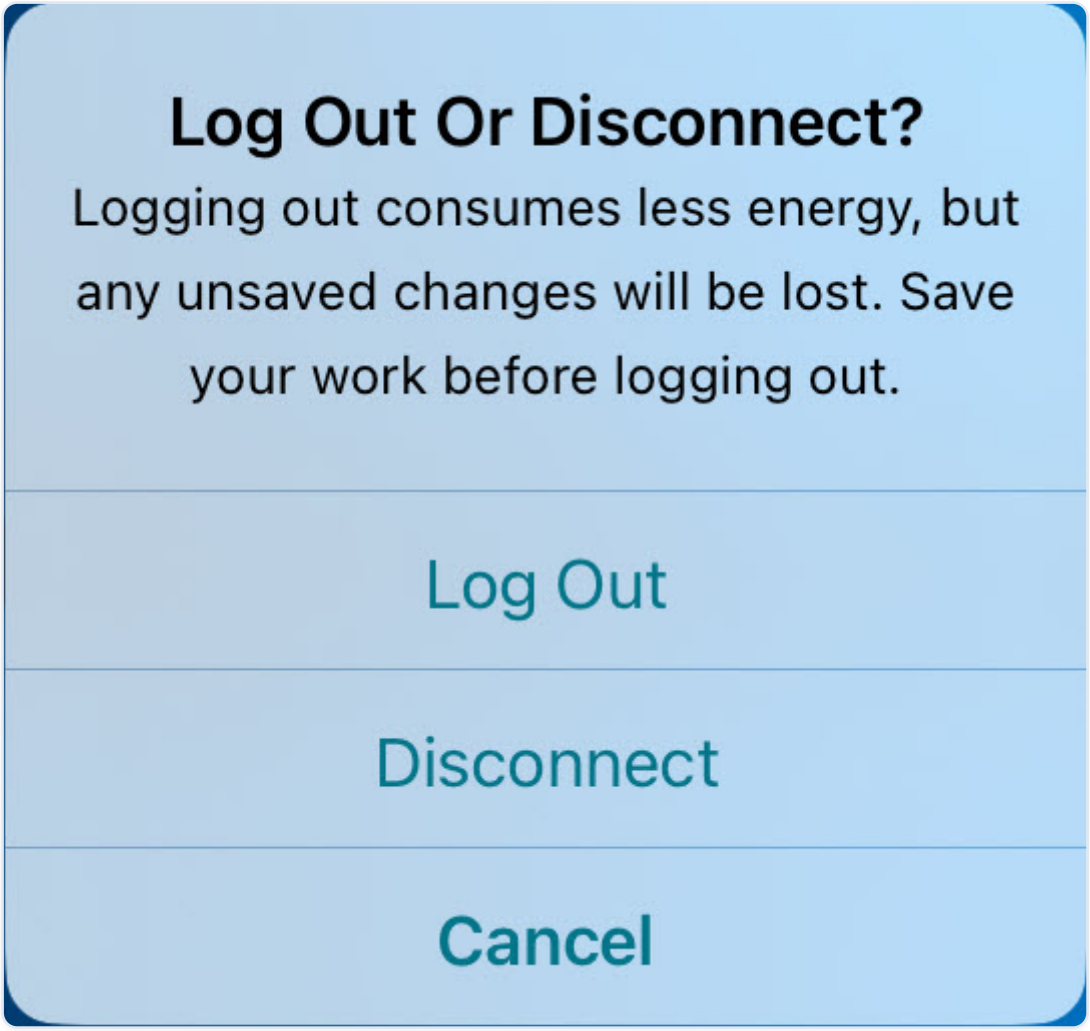
> このテクニカルプレビュー機能を使用しない場合は、常にCitrix Workspaceアプリを全画面モードで使用できます。

サステナビリティイニシアチブのサポート

バージョン24.9.0以降、ユーザーは仮想デスクトップを閉じると、デスクトップセッションからサインアウトするよう促されます。この機能は、不要なときにVMからサインアウトすることで、エネルギーの節約に役立ちます。以前は、これらのセッションは切断された状態のままであり、不必要なエネルギー消費につながっていました。

サステナビリティが有効になっていないセッションから切断する場合、ユーザーには、将来の自動切断のために「**切断して次回から表示しない**」オプションを含むプロンプトが表示されます。このデフォルトのテキストはローカライズされています。

ユーザーがサステナビリティを有効にして切断する場合、システムはエネルギー節約のために「**ログアウト**」するよう促します。管理者として、サステナビリティメッセージをカスタマイズできます。



管理者は、葉のアイコンを含むサステナビリティアラートを表示し、タイトルとプロンプトメッセージをカスタマイズできます。管理者がタイトルまたはプロンプトメッセージを提供せず、サステナビリティ機能を有効にしながら葉のアイコンをオフにした場合、デフォルトメッセージ「**デスクトップを切断しますか？ 次回マネージド%@デスクトップに接続するときも、作業は中断し**

たところから再開されます」が表示されます。%@ は仮想デスクトップアプリ名に置き換えられます。これらのデフォルトメッセージはローカライズされています。

管理者が設定したメッセージはローカライズされないため、管理者はテキストの明確さと正確性を確保する必要があります。

この機能を有効にしてカスタマイズする方法の詳細については、Windows向けCitrix Workspaceアプリのドキュメントにある「Citrix Workspaceアプリのサステナビリティイニシアチブ」を参照してください。

強化されたマルチアプリウィンドウ管理

バージョン24.9.0以降、iOS向けCitrix Workspaceアプリは、外部モニターに接続されたiPad向けのシームレスなマルチアプリウィンドウ管理をサポートするようになりました。この機能は、ネイティブのマルチアプリエクスペリエンスを可能にすることで、マルチタスクと生産性を向上させます。iPadデバイスが外部モニターに接続されていない場合でも有効にできます。

この機能を使用すると、次のことができます。

- アプリケーション間を切り替え、単一のアプリを別々のウィンドウで開くことで、ワークフローと生産性を向上させます。
- 外部モニターに接続中に、1つのセッションで複数のアプリを使用します。

シームレスなマルチアプリを有効にするには、次の手順に従います。

1. **アプリケーション設定** > **詳細** > **マルチタスク** に移動します。
2. **セッションウィンドウを分離** を有効にします。
3. 「**Multi Windows for Seamless App Session**」を有効にします。

制限事項:

- Stage Manager はデバイスで有効にする必要があり、使用中は有効にしておく必要があります。
- 起動後、灰色のオーバーレイと HDX セッションウィンドウが表示される場合があります。これは、サーバーの起動中に発生します。数秒から数分後、ユーザーはアプリの画面を確認し、通常どおり使用できます。
- この機能は、Apple Silicon チップ搭載 iPad など、Stage Manager をサポートするデバイスでのみ利用可能です。

トラブルシューティング

アプリのバージョンを確認する方法

Citrix Workspaceアプリのバージョンを確認するには、アプリを開きます。「**設定**」>「**バージョン情報**」をタップします。バージョン情報が画面に表示されます。

アプリのバージョン(/en-us/citrix-workspace-app-for-ios/media/check-appversion.png)

Citrix Workspaceアプリを最新バージョンにアップグレードする方法

App StoreからCitrix Workspaceアプリの最新バージョンにアップグレードできます。Citrix Workspaceアプリを検索し、「**アップグレード**」ボタンをタップします。

Citrix Workspaceアプリをリセットする方法

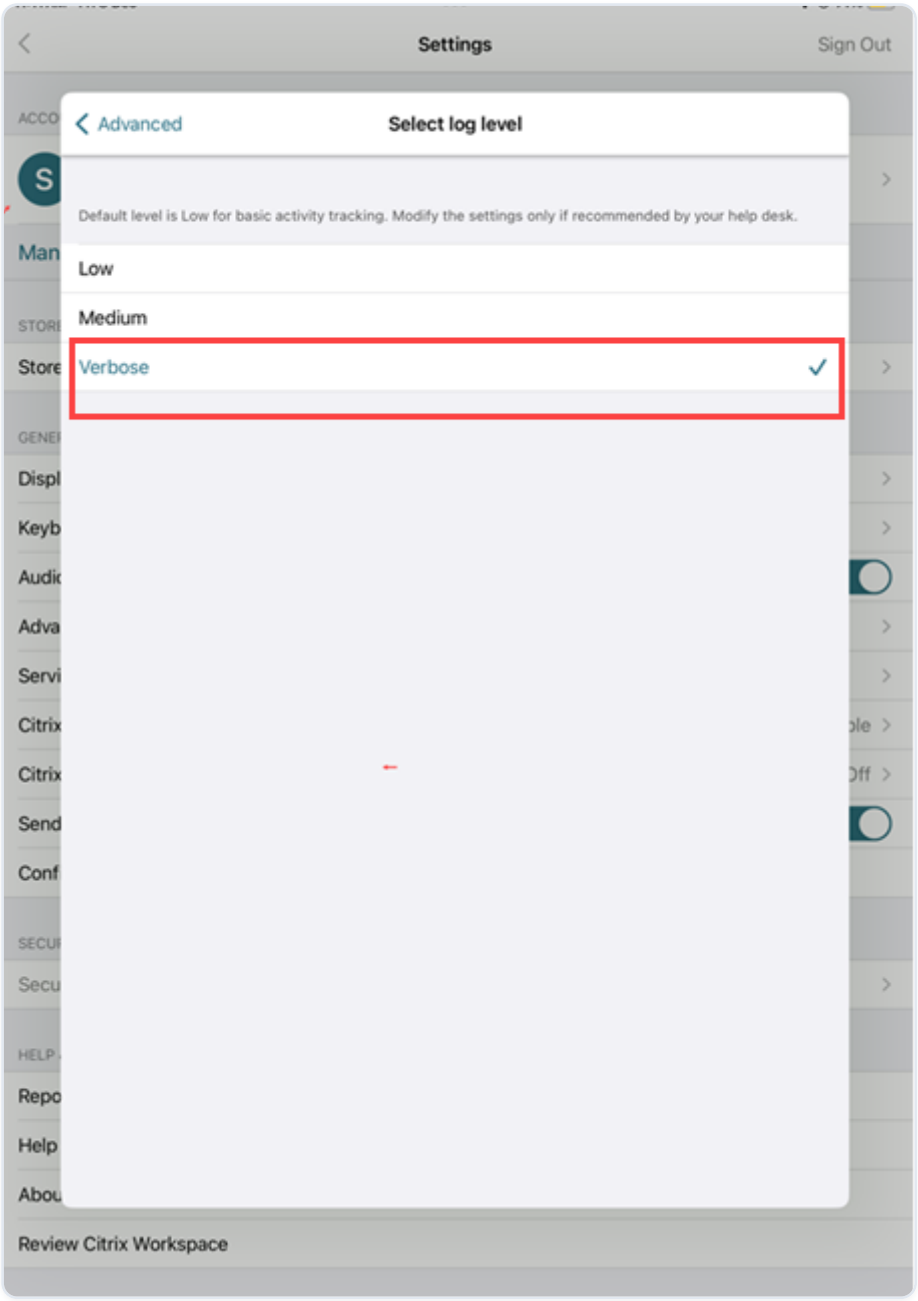
次のいずれかの方法でCitrix Workspaceアプリをリセットできます。

- Citrix Workspaceアプリから既存のアカウントをすべて削除する
- Citrix Workspaceアプリのストレージデータをクリアする
- Citrix Workspaceアプリをアンインストールし、最新の修正が適用されたiOS版Citrix Workspaceアプリの最新バージョンをインストールします。

ログを収集する方法

1. Citrix Workspaceアプリを開き、「**設定**」に移動します。
2. 「**ヘルプとサポート**」で、「**問題の報告**」を選択します。

   問題の報告(/en-us/citrix-workspace-app-for-ios/media/report-issue.png)
3. 問題を再現します。
4. 「ログレベルの選択」ページで、「**Verbose**」を選択します。



5. 「**ログ保存場所の選択**」ページで、「**コンソールとファイルの両方**」を選択します。
6. zipファイルをCitrixと共有します。

「ログファイル」(/en-us/citrix-workspace-app-for-ios/media/logs-share.png)

機能強化をリクエストする方法

機能強化のリクエストは、<ios_ear_support@citrix.com>までメールでお送りいただけます。

テクニカルプレビュー機能にアクセスする方法

テクニカルプレビュー機能は、各機能に固有の<ios_ear_support@citrix.com>までメールでリクエストできます。このフォームは、製品ドキュメントのテクニカルプレビュー発表に添付されています。

EARに関するフィードバックを提供する方法

EARに関するフィードバックは、<ios_ear_support@citrix.com>までメールで提供できます。

一般的な問題とトラブルシューティングのヒント

切断されたセッション

ユーザーは、以下の方法でCitrix Workspaceアプリfor iOSセッションから切断（ログオフではない）できます。

- セッションで公開アプリケーションまたはデスクトップを表示中に：
  - 画面上部にある矢印をタップして、セッション内ドロップダウンメニューを表示します。
  - **ホーム**ボタンをタップして、起動パッドに戻ります。
  - アクティブなセッションがまだ続いている公開済みアプリのアイコンの下に白い影があることに注意し、そのアイコンをタップします。
  - 切断をタップします。
- Citrix Workspaceアプリ for iOSを閉じるには：
  - デバイスの**ホーム**ボタンをダブルタップします。
  - iOSアプリスイッチャービューでCitrix Workspaceアプリ for iOSを見つけます。
  - 表示されるダイアログで切断をタップします。
- モバイルデバイスのホームボタンを押す。
- アプリのドロップダウンメニューで「ホーム」または「切り替え」をタップする。

セッションは切断された状態のままになります。ユーザーは後で再接続できますが、切断されたセッションが特定の時間間隔後に非アクティブとして表示されることを確認できます。

アプリを非アクティブモードで表示するには、リモートデスクトップセッションホストの構成（以前は「ターミナルサービス構成」として知られていました）で、ICA-TCP接続のセッションタイムアウトを構成します。

リモートデスクトップサービス（以前は「ターミナルサービス」として知られていました）の構成の詳細については、Microsoft Windows Serverの製品ドキュメントを参照してください。

期限切れのパスワード

Citrix Workspaceアプリ for iOSは、ユーザーが期限切れのパスワードを変更する機能をサポートしています。ユーザーには、必要な情報を入力するためのプロンプトが表示されます。

脱獄デバイス

ユーザーは、脱獄されたiOSデバイスで接続することにより、展開のセキュリティを侵害する可能性があります。脱獄デバイスとは、通常、特定のセキュリティ保護をバイパスする目的で所有者によって改造されたデバイスです。

Citrix Workspaceアプリ for iOSが脱獄されたiOSデバイスを検出すると、Citrix Workspaceアプリ for iOSはユーザーに警告を表示します。

環境のセキュリティをさらに強化するために、検出された脱獄デバイスがアプリを実行するのを防ぐために、StoreFrontまたはWeb Interfaceを構成できます。

要件

- シトリックス レシーバー for iOS 6.1以降
- StoreFront 3.0またはWeb Interface 5.4以降
- 管理者アカウントを介したStoreFrontまたはWeb Interfaceへのアクセス

> **注：**
>
> Citrix Workspace™アプリは、脱獄デバイスを検出すると、データ保護とセキュリティ維持のために自身を非アクティブ化します。これにより、不正な変更が加えられたデバイスでアプリが使用されることがなくなります。

HDX™オーディオ品質の低下

Citrix Virtual Apps and DesktopsおよびCitrix DaaS（旧Citrix Virtual Apps and Desktopsサービス）から、Citrix Workspaceアプリ for iOSへのHDXオーディオの品質が低下する場合があります。この問題は、オーディオとビデオを同時に使用するときに発生します。

この問題は、Citrix Virtual Apps and Desktops™およびCitrix DaaSのHDXポリシーが、ビデオデータと同時に大量のオーディオデータを処理できない場合に発生します。

オーディオ品質を向上させるポリシーの作成方法に関する提案については、Knowledge Centerの記事CTX123543を参照してください。

カスタマイズされたストアエクスペリエンスのデスクトップおよびアプリセッションの起動に失敗しました

カスタマイズされたストアエクスペリエンスがある場合、Citrix Workspaceアプリからデスクトップおよびアプリセッションを起動できないことがあります。ストアタイプの自動検出は、メールアドレスのみがサポートされており、ストアURLはサポートされていません。カスタマイズされたストアがある場合は、メールアドレスまたはWebインターフェースログインモードを使用することをお勧めします。詳細については、手動セットアップおよびメールベースのアカウント検出の構成を参照してください。

Webインターフェースログインモードを介してアカウントを手動で構成するには、次の手順を実行します。

1. 「**アカウントアイコン > アカウント画面 > プラス記号 (+)**」をタップします。「**新しいアカウント**」画面が表示されます。
2. 画面の左下隅にある**オプション**の左側のアイコンをタップし、**手動セットアップ**をタップします。他のフィールドが画面に表示されます。
3. **アドレス**フィールドに、サイトまたはCitrix GatewayのセキュアなURL（例: agee.mycompany.com）を入力します。
4. **Webインターフェイス**接続を選択します。この接続モードでは、Webブラウザに似たCitrix Virtual Apps™のWebサイトが表示されます。このUIはWebビューとも呼ばれます。

   Webインターフェイス(/en-us/citrix-workspace-app-for-ios/media/web-interface.png)
5. 証明書のセキュリティについては、**証明書の警告を無視**フィールドの設定を使用して、無効な証明書、自己署名証明書、または期限切れの証明書を持つサーバーであっても接続するかどうかを決定します。デフォルト設定はオフです。

   > **重要:**
   >
   > このオプションを有効にする場合は、正しいサーバーに接続していることを確認してください。Citrixは、ユーザーデバイスをオンラインセキュリティ攻撃から保護するために、すべてのサーバーが有効な証明書を持つことを強く推奨します。セキュアなサーバーは、認証局によって発行されたSSL証明書を使用します。Citrixは自己署名証明書をサポートしておらず、証明書のセキュリティをバイパスすることを推奨していません。

6. **保存**をタップします。
7. ユーザー名とパスワード（2要素認証を選択した場合はトークン）を入力し、ログオンをタップします。Citrix Workspaceアプリ for iOSの画面が表示され、デスクトップにアクセスしたり、アプリを追加して開いたりできます。

> **注：**
>
> Webインターフェイスのログインモードではユーザー資格情報は保存されないため、接続ごとにユーザー資格情報を入力する必要があります。

Citrixトラブルシューティング接続

Citrixトラブルシューティング接続機能は、エンドユーザーがデスクトップまたはアプリケーションの起動失敗の可能性を効果的に自己トラブルシューティングできるように設計されています。この機能強化は、ユーザーに明確な診断、潜在的な推奨事項、および簡単なクリックで修正を実行する機能を提供することを目的としています。

仕組み

この機能は、より詳細で強化されたエラーメッセージを提供し、ユーザーが起動失敗の根本原因を明確に理解できるようにします。トラブルシューティング接続機能は、起動プロセス中にVirtual Delivery Agent (VDA) への接続問題をリアルタイムで分析します。その後、ユーザーフレンドリーなエラーメッセージと推奨事項を提示し、ユーザーが問題を直接解決するか、必要に応じてサポートチケットのためにログを収集できるようにします。

分析される接続パス

この機能は、以下を含む重要な接続ポイント全体で、仮想アプリとデスクトップの起動に関する潜在的な問題を診断します。

- クライアントからゲートウェイへのネットワーク接続。
- ゲートウェイからStoreFrontサーバーへの接続。
- StoreFrontサーバーからBrokerへの接続。
- BrokerからVDAへの接続。

強化されたエラーメッセージと診断

起動に失敗した場合、Citrixは、ネットワークエラー、サーバーの利用不可、VDA障害など、特定の接続問題を特定する明確でユーザーフレンドリーなエラーメッセージを表示するようになりました。管理者向けには、詳細なエラーコードがログに提供され、サーバー側とクライアント側のエラーに分類されており、詳細な調査のための貴重な参照情報として役立ちます。

トラブルシューティングのエラーメッセージ(/en-us/citrix-workspace-app-for-ios/media/troubleshooting_error_message.png)

トラブルシューティングのエラーメッセージと修正(/en-us/citrix-workspace-app-for-ios/media/troubleshooting_error_fix.png)

自己回復と修復アクション

Citrix Troubleshoot Connection機能には、ユーザーが一般的な問題から自動的に回復するための手順が含まれており、サポート介入の必要性を最小限に抑えます。ガイド付き修復で解決できる潜在的な問題は次のとおりです。

- VDAの再起動
- Citrix Workspaceアプリ (CWA) の再起動 - CWAへの再ログイン
- リソースリストの更新
- アプリを更新して再試行
- ストアを再構成する
- CWAをアップグレードする
- CWAを再インストールする
- ネットワークを確認する
- 待機して再試行する

システム要件

接続トラブルシューティング機能を使用するには、以下のCitrix Workspaceアプリのバージョンが必要です。

- **iOS向けCitrix Workspaceアプリ:** バージョン2509以降

> **注：**

エラーメッセージにはサーバーエラーコードも含まれており、オンプレミスとクラウドの両方に関する詳細は、エラーコードセクションで確認できます。

接続トラブルシューティング機能は、DaaS環境でデフォルトで有効になっています。ブラウザで起動されたセッションとCitrix Workspaceアプリで開始されたセッションの両方で、詳細なエラーメッセージと推奨事項が利用可能です。エラーコードとトランザクションIDは、管理者参照用にログに記録されます。エラーコードは、サーバー側またはクライアント側に分類されます。特定のエラーについては、Virtual Delivery Agent (VDA) を再起動する修復オプションが提供されます。この機能はハイブリッドモードのセッションをサポートしていません。たとえば、ブラウザでICAファイルをダウンロードし、そのファイルをCitrix Workspaceアプリで開く場合には使用できません。

よくある質問

低電力デバイスまたはモバイルデバイスでの仮想アプリおよび仮想デスクトップのビデオパフォーマンスを向上させる方法

Citrix Virtual Apps and Desktopsのバージョンに応じて、MaxFramesPerSecondレジストリ値またはHDXポリシーを使用して仮想デスクトップのビデオパフォーマンスを向上および構成する方法については、Knowledge Centerの記事CTX123543を参照してください。

Citrix Workspaceアプリにサインオンした後、アプリやデスクトップが表示されません

詳細については、会社のヘルプデスクまたはITサポートチームの管理者に問い合わせてください。

低速接続のトラブルシューティング方法

以下のいずれかの問題が発生した場合は、以下の**回避策**セクションに記載されている手順に従ってください。

- Citrix Virtual Apps and Desktopsサイトへの接続が遅い
- アプリケーションアイコンの欠落
- 繰り返し発生するプロトコルドライバーエラーメッセージ

回避策

Citrix Virtual Appsサーバー、Citrix Secure Web Gateway™、およびWeb Interfaceサーバーのネットワークインターフェイスで、Citrix PV Ethernet Adapterのプロパティを無効にします。 Citrix PV

Ethernet Adapterのプロパティには、デフォルトで有効になっている以下のプロパティが含まれています。これらのプロパティはすべて無効にする必要があります。

- ラージセンドオフロード
- IPチェックサムオフロード
- TCPチェックサムオフロード
- UDPチェックサムオフロード

> **注：**
>
> サーバーの再起動は不要です。この回避策は、Windows Server 2003および2008の32ビット版に適用されます。この問題はWindows Server 2008 R2には影響しません。

数字キーと特殊文字に関する問題のトラブルシューティング

数字キーまたは中国語IME文字が期待どおりに機能しない場合は、Unicodeキーボードオプションを無効にする必要があります。 Unicodeキーボードオプションを無効にするには：

1. **設定** > **キーボードオプション** に移動します。
2. **Unicodeキーボードの使用** を **オフ** に設定します。

iOS向けCitrix Workspaceアプリ

iOS向けCitrix Workspaceアプリは、App Storeからダウンロードできるクライアントソフトウェアです。これにより、Citrix Virtual Apps and Desktopsによって提供される仮想デスクトップとホスト型アプリケーションにアクセスして実行できます。

iOSは、iPadやiPhoneなどのAppleモバイルデバイス用のオペレーティングシステムです。iOS向けCitrix Workspaceアプリは、iPhone X、iPad mini、iPad Proなど、iOSオペレーティングシステムを使用するデバイスで動作します。

言語サポート

iOS向けCitrix Workspaceアプリは、英語以外の言語での使用に適応しています。iOS向けCitrix Workspaceアプリでサポートされている言語のリストについては、「言語サポート」を参照してください。

非推奨

この記事の発表は、段階的に廃止されるプラットフォーム、Citrix®製品、および機能について事前に通知し、お客様がタイムリーなビジネス上の意思決定を行えるようにするものです。Citrixは、お客様の使用状況とフィードバックを監視して、いつ廃止するかを決定します。発表は、その後のリリースで変更される可能性があり、廃止されたすべての機能や特性が含まれるとは限りません。

非推奨の項目はすぐに削除されません。Citrix はこのリリースでは引き続きサポートしますが、将来的に削除されます。

項目	非推奨が発表されたバージョン	削除日	代替
iOSオペレーティングシステムバージョン17	iOS向けCitrix Workspaceアプリバージョン26.9.0	iOS向けCitrix Workspaceアプリバージョン26.9.0	利用可能な最新バージョンのiOSにアップグレード

CITRIX WORKSPACE™ アプリ FOR IOS

項目	非推奨が発表されたバージョン	削除日	代替
自動構成、XenApp Services、および Access Gateway	iOS向けCitrix Workspaceアプリ バージョン26.7.0	iOS向けCitrix Workspaceアプリ 26.11.0	-
EDT設定を許可	iOS向けCitrix Workspaceアプリ バージョン26.7.0	iOS向けCitrix Workspaceアプリ 27.3.0	管理者設定として利用可能
Citrix X1 マウス	iOS 版 Citrix Workspace アプリ バージョン 25.9.0	iOS 版 Citrix Workspace アプリ 26.3.0	-
Citrix キャスティング	iOS 版 Citrix Workspace アプリ バージョン 25.9.0	iOS 版 Citrix Workspace アプリ 26.3.0	-
iOS オペレーティングシステム バージョン 16	iOS 版 Citrix Workspace アプリ バージョン 25.7.2	iOS 版 Citrix Workspace アプリ 25.7.2	最新の iOS バージョンにアップグレードしてください
iOS オペレーティングシステム バージョン 15	iOS 版 Citrix Workspace アプリ バージョン 24.7.0	iOS 版 Citrix Workspace アプリ 24.12.0	最新の iOS バージョンにアップグレードしてください
DTLS 1.0プロトコルのサポート	Citrix Workspaceアプリ for iOS バージョン 24.5.0	-	DTLS 1.2プロトコル
TLS 1.0およびTLS 1.1プロトコルのサポート	Citrix Workspaceアプリ for iOS バージョン 24.4.0	Citrix Workspaceアプリ for iOS バージョン 25.3.0	TLS 1.2またはTLS 1.3プロトコル
XenApp Services（PNAgentとも呼ばれる）	Citrix Workspaceアプリ for iOS バージョン 23.7.5	-	Citrix Workspaceアプリ内で、XenApp Services URLではなくストアURLを使用してストアに接続します。

CITRIX WORKSPACE™ アプリ FOR IOS

項目	非推奨が発表されたバージョン	削除日	代替
iOSオペレーティングシステム バージョン 14	Citrix Workspaceアプリ for iOS バージョン 23.10.0	対象: Citrix Workspaceアプリ for iOS 23.12.0	最新の利用可能なiOSバージョンにアップグレードしてください
iOSオペレーティングシステム バージョン 13.x	Citrix Workspaceアプリ for iOS バージョン 22.9.5	ターゲット: 2022年12月およびバージョン22.12.0	iOSの最新の利用可能なバージョンにアップグレードしてください
iOSオペレーティングシステムバージョン11.xおよび12.x	Citrix Workspace app for iOS バージョン21.12.0	ターゲット: 2022年8月およびバージョン22.8.0	iOSの最新の利用可能なバージョンにアップグレードしてください
iOSオペレーティングシステムバージョン10.x	Citrix Workspace app for iOS バージョン21.1.5	21.1.5に続くリリース	Citrix Workspace app for iOS バージョン21.1.5またはそれ以前を使用してください

注記:

- 非推奨のプラットフォームバージョンを使用している既存のCitrix Workspace™ appユーザーは、Citrix Workspace appの最新リリース（App Storeから）にアップグレードできません。
- 非推奨のプラットフォームバージョンを使用している新規のCitrix Workspace appユーザーは、App Storeから以前の互換性のあるバージョンのみをダウンロードできます。
- 非推奨のプラットフォームバージョンを使用しているユーザーは、Citrix Workspace appの新しいリリースごとに提供される新機能やセキュリティパッチを受け取れません。