



# iOS 向け Citrix Workspace アプリ

## Contents

<b>iOS 向け Citrix Workspace アプリ</b>	<b>2</b>
このリリースについて	3
<b>Technical Preview</b> の機能	<b>29</b>
システム要件と互換性	48
インストールとアップグレード	55
開始	55
<b>Citrix Workspace</b> アプリの構成	<b>63</b>
統合エンドポイント管理ソリューションを使用した <b>Citrix Workspace</b> アプリの構成	75
周辺機器	77
ユーザーエクスペリエンス	98
<b>Web</b> アプリおよび <b>SaaS</b> アプリの <b>Webview</b>	<b>109</b>
パスワード管理	110
認証	114
セキュリティ	136
トラブルシューティング	142
<b>iOS 向け Citrix Workspace アプリ</b>	<b>153</b>

## iOS 向け Citrix Workspace アプリ

July 1, 2024

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。これによって、Citrix Virtual Apps and Desktops が配信する仮想デスクトップおよびホストされるアプリケーションにアクセスし、これらを実行できるようになります。

iOS は、iPad や iPhone などの Apple モバイルデバイス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 などの、iOS オペレーティングシステムを使ったデバイスで実行することができます。

機能、修正された問題、既知の問題の詳細については、「[このリリースについて](#)」ページを参照してください。

廃止済みの項目については、「[廃止済み](#)」ページを参照してください。

### 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。

### 参考記事

- [技術概要: Citrix Workspace](#)
- [Global App Configuration Service](#)
- [ワークスペースユーザーインターフェイス \(user interface: UI\)](#)
- [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](#)
- [開発者用のドキュメント](#)

### 関連製品の到着情報

- [Citrix Workspace](#)
- [Citrix DaaS](#)
- [StoreFront](#)
- [Secure Private Access](#)
- [Mac 向け Citrix Workspace アプリ](#)

### 古いドキュメント

保守終了 (EOL) に達した製品リリースについては、[古いドキュメント](#)を参照してください。

## このリリースについて

July 1, 2024

新機能、機能強化、解決された問題、既知の問題について説明します。

注:

Technical Preview をお探しですか? 1 か所で見つけられるように厳選した一覧を作成しました。「[Technical Preview の機能](#)」ページをご覧ください、記載されている Podio フォームリンクを使用してフィードバックを共有してください。

### 24.5.0 の新機能

クラウドストアへの接続で **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 Citrix Workspace アプリに認証するときに、FIDO2 ベースのパスワードなしの認証を利用してクラウドストアに接続できます。FIDO2 はシームレスな認証方法を提供し、企業の従業員がユーザー名やパスワードを入力しなくても、仮想セッション内で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、ローミング認証システム (USB のみ) とプラットフォーム認証システム (PIN コード、Touch ID、Face ID のみ) の両方をサポートします。この機能はデフォルトで有効になっています。詳しくは、「[クラウドストアへの接続で FIDO2 を使用した認証のサポート](#)」を参照してください。

注:

FIDO2 認証は、Chrome のカスタムタブでデフォルトでサポートされています。WebView で FIDO2 認証を使用することの詳細について興味を持たれた場合は、この [Podio フォーム](#) を使用して登録していただくようお願いいたします。

ドキュメントスキャナーのサポート

24.5.0 バージョン以降、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ます。この機能を使用することで、デスクトップセッション内で複数のドキュメントをすべて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。詳しくは、「[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。

**DTLS 1.0** プロトコル廃止のお知らせ Citrix は、将来のリリースで DTLS 1.0 プロトコルのサポートを廃止する予定です。代替プロトコルは DTLS 1.2 です。詳しくは、「[廃止](#)」を参照してください。

## Technical Preview

- Microsoft Entra ID 参加済み仮想マシンのシングルサインオンをサポート
- Citrix Workspace アプリへのアクセスで生体認証の強制をサポート

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 24.5.0 で解決された問題

- 仮想セッションでバーコードスキャナーを使用すると、テキストを正しくスキャンできない場合があります。  
[HDX-63675]

### 24.5.0 の既知の問題

iPad Pro M4 デバイスの仮想セッションでは、Magic Keyboard のトラックパッドが正しく機能しないことがあります。この問題を回避するために、外付けマウス（有線 USB タイプ C コネクタまたは Bluetooth）を使用して仮想セッションの画面を操作することができます。[HDX-66083]

### 以前のリリース

このセクションでは、サポートされている以前のリリースでの新機能と解決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ついては、「[Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#)」を参照してください。

## 24.4.0

### 新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

**TLS 1.0** および **TLS 1.1** プロトコル廃止のお知らせ Citrix は、将来のリリースで TLS 1.0 および TLS 1.1 プロトコルのサポートを廃止する予定です。代替プロトコルは TLS 1.2 または TLS 1.3 です。詳しくは、「[廃止](#)」を参照してください。

### 解決された問題

- 仮想アプリセッションからデバイスのカメラを開くと、iOS 向け Citrix Workspace アプリが予期せず終了することがあります。[CVADHELP-24825]

#### 既知の問題

新しい既知の問題はありません。

### 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 24.3.5 バージョン以降、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 USB-C リーダーは、Citrix Workspace アプリのログインでのみサポートされ、仮想セッションのログインではサポートされていません。

**UEM** を介したデバイス名の構成をサポート 24.3.5 バージョン以降、iOS 向け Citrix Workspace アプリでは、管理者が統合エンドポイント管理 (UEM) 経由で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した。詳しくは、「[UEM を介したデバイス名の構成をサポート](#)」を参照してください。

#### Technical Preview

- UEM 経由による Citrix Workspace アプリ設定の構成をサポート

この Technical Preview については、「[Technical Preview の機能](#)」を参照してください。

#### 解決された問題

このバージョンでは、パフォーマンスや安定性が総合的に向上する部分に対処しています。

#### 既知の問題

新しい既知の問題はありません。

### 24.3.0

#### 新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## Technical Preview

- アダプティブオーディオのサポート

この Technical Preview について詳しくは、「[Technical Preview の機能](#)」を参照してください。

### 解決された問題

iOS 向け Citrix Workspace アプリをバージョン 24.1.0 にアップグレードした後、Oracle Java Web Start ソフトウェアベースのアプリケーションで、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に失敗する場合があります。[CVADHELP-24645]

### 既知の問題

新しい既知の問題はありません。

## 24.2.0

### 新機能

**複数のストアを一度に削除するためのサポート** バージョン 24.2.0 以降、iOS 向け Citrix Workspace アプリでは、複数のストアの選択と削除がサポートされています。この機能により、複数のストアで作業する場合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。詳しくは、「[複数のストアを一度に削除するためのサポート](#)」を参照してください。

**ユーザーのストア名の変更に関する管理者による制限をサポート** 以前は、ユーザーは **[Edit Account]** オプションを使用してストア名を変更できました。

24.2.0 以降、iOS 向け Citrix Workspace アプリでは、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が管理者に提供されます。この機能を使用すると、管理者はストア名の一貫性を簡単に確認して維持できます。詳しくは、「[ユーザーのストア名の変更に関する管理者による制限をサポート](#)」を参照してください。

**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、ストア名を更新するときに手動での操作の必要がなくなり、ユーザーエクスペリエンスが向上します。詳しくは、「[ストア名の自動入力](#)」を参照してください。

#### 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。

## Technical Preview

- アクセシビリティと VoiceOver のサポート

この Technical Preview について詳しくは、「[Technical Preview の機能](#)」を参照してください。

### 解決された問題

このバージョンでは、パフォーマンスや安定性が総合的に向上する部分に対処しています。

### 既知の問題

新しい既知の問題はありません。

## 24.1.0

### 新機能

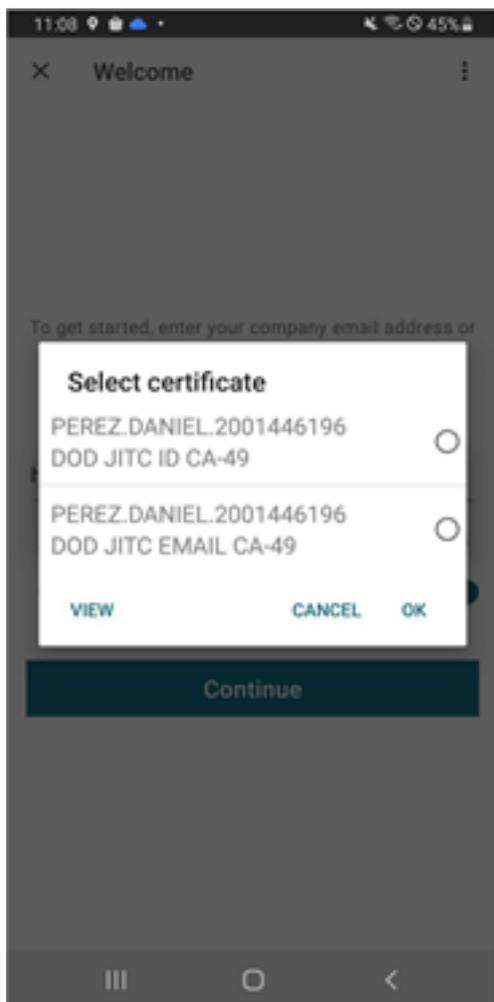
**セキュリティの更新** このリリースには、重要なセキュリティ更新プログラムとセキュリティ問題の修正が含まれています。

**オンプレミス展開での認証トークンの保存の構成をサポート** iOS 向け Citrix Workspace アプリは、ローカルディスクでオンプレミスストアの認証トークンの保存を構成するオプションを提供するようになりました。この機能を使用すると、認証トークンの保存を無効にして、セキュリティを強化することができます。無効にした後、システムまたはセッションが再起動されると、セッションにアクセスするには再度認証が必要になります。詳しくは、「[オンプレミス展開での認証トークンの保存の構成をサポート](#)」を参照してください。

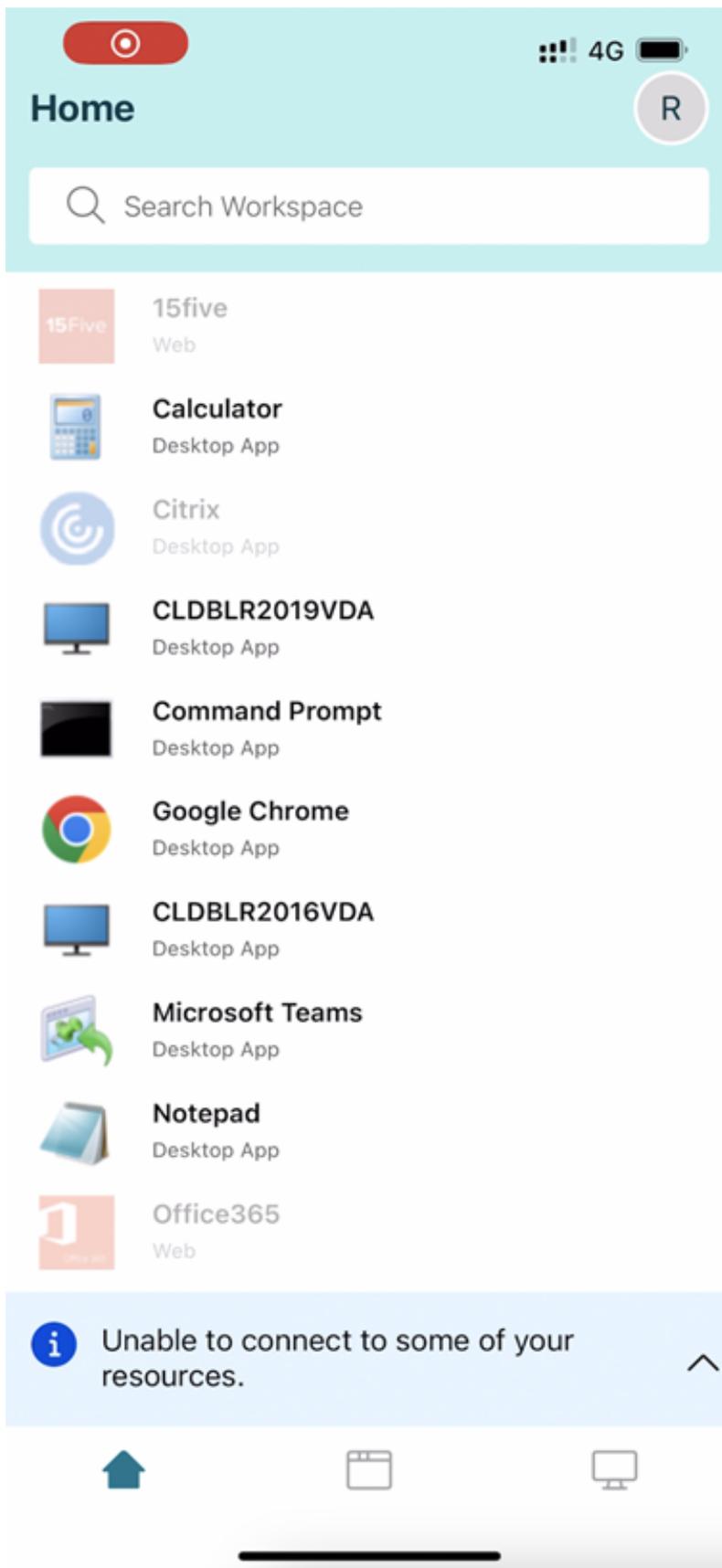
**複数のクラウドストアをサポート** 24.1.0 リリース以降、iOS および iPadOS 向け Citrix Workspace アプリに複数のクラウドストアアカウントを追加できます。エンドユーザーが簡単に複数のストアを追加したり、切り替えたりできるようになりました。この機能により、複数のストアにアクセスするときのユーザー エクスペリエンスが向上します。詳しくは、「[複数のクラウドストアをサポート](#)」を参照してください。

**スマートカード認証での複数の証明書のサポート** 以前は、iOS 向け Citrix Workspace アプリでは、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が表示されていました。

24.1.0 リリース以降、iOS 向け Citrix Workspace アプリでは、スマートカードで利用可能なすべての証明書が表示され、スマートカード認証での認証時に必要な証明書を選択できるようになりました。詳しくは、「[スマートカード認証での複数の証明書のサポート](#)」を参照してください。



強化された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 24.1.0 リリース以降、iOS 向け Citrix Workspace アプリのユーザーインターフェイスが強化され、洗練され、さらに詳細な情報を表示するようになり、Citrix Workspace の停止時にユーザーフレンドリーなエクスペリエンスを提供します。オフラインモードに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、アプリやデスクトップの結果で一致に近いテキストや、検索語のスペルミスを見つけることができます。サービス継続性機能について詳しくは、「[サービス継続性](#)」を参照してください。

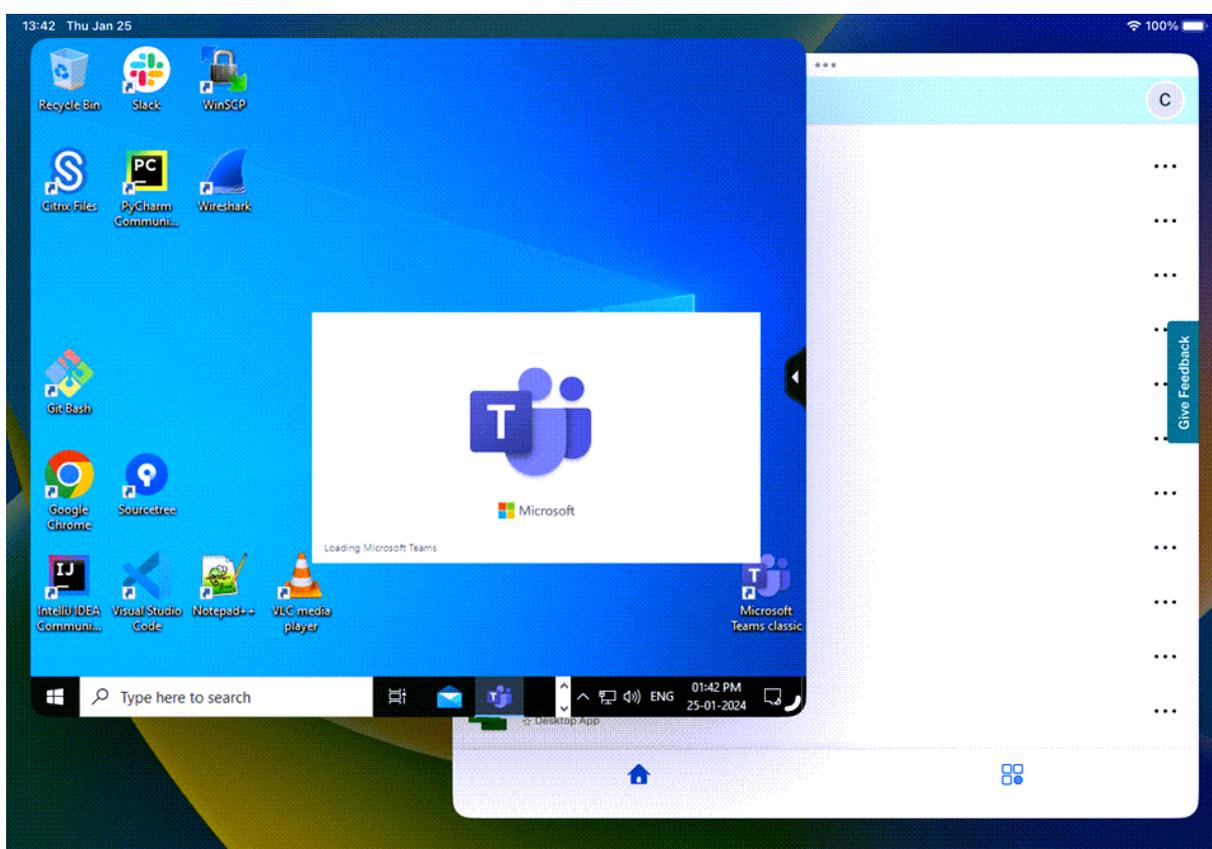


**Citrix Workspace** アプリからの個別のセッションウィンドウのサポート バージョン 24.1.0 以降、iOS 向け Citrix Workspace アプリには、マルチタスクをより効率的で使いやすい個別のセッションウィンドウが導入されています。この機能を使用すると、デスクトップのようなエクスペリエンスを実現できます。個別のセッションウィンドウ機能が有効になっている場合は、単に接続されている外部モニターにセッションをドラッグアンドドロップするだけです。その結果、iPad のメインモニターを他のアプリとのマルチタスクに使用できるようになります。

注:

この機能は、ステージマネージャ機能をサポートするデバイスでのみサポートされます。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。ステージマネージャ機能について詳しくは、Apple サポートドキュメントの「iPad でステージマネージャのオン/オフを切り替える」を参照してください。

詳しくは、「Citrix Workspace アプリからの個別のセッションウィンドウのサポート」を参照してください。



**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、外付けの物理キーボードの使用時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 デバイスを外付けの Windows PC の標準キーボードで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 のソフトキーボードの代わりに VDA のキーボードレイアウトを使用できます。これによって、iOS ではなく外付けの Windows キーボードの入力スタイルを完全に再現することができます。全体的なユーザーエクスペリエンスが大幅に向上するため、東アジア言

語で入力する場合に役立ちます。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することになる可能性があります。詳しくは、「[スキャンコード入力モードのサポート](#)」を参照してください。

外部キーボードのショートカットのサポートを強化 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ショートカットをより多く使用できるようになりました。以下は、外部キーボードのショートカットで強化された重要な変更点です：

- **Insert**、**Delete**、テンキーなどの Windows キーボード固有のキーのサポート。
- キーを押したままにすると、リモートデスクトップ/アプリが正しく応答します。
- 3つを超える数のキーを使用した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] で、次のオプションによって **Alt** に特定のキーを構成できるようになりました：

- **Option or Alt (left)**: **Option (left) or Alt (left)** を使用して **Alt** を送信します。
- **Command or Windows (left)**: **Command (left) or Windows (left)** キーを使用して **Alt** を送信します。
- **Option or Alt (left and right)**: **Option or Alt (left and right)** キーを使用して **Alt** を送信します。

**Alt** オプションに特定のキーを割り当てると、macOS の **Option** キーと Windows の **Alt** キーの間の競合を回避できます。

詳しくは、「[外部キーボードのショートカットのサポートを強化](#)」を参照してください。

グラフィックパフォーマンスの向上 24.1.0 バージョン以降、iOS 向け Citrix Workspace アプリは、ハードウェアアクセラレーションによる H.264 ビデオエンコードまたはデコードをサポートします。Citrix HDX のマルチメディアエンジンは、エンコーディングとデコーディングに Apple の Video Toolbox フレームワークを使用するようになりました。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。この機能拡張により、マルチメディアの使用中の CPU の負荷が軽減されます。詳しくは、「[グラフィックパフォーマンスの向上](#)」を参照してください。

### 解決された問題

このバージョンでは、パフォーマンスや安定性が総合的に向上する部分に対処しています。

### 既知の問題

- iOS 向け Citrix Workspace アプリをバージョン 24.1.0 にアップグレードした後、Oracle Java Web Start ソフトウェアベースのアプリケーションで、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場合があります。[CVADHELP-24645]

## 23.12.1

### 新機能

**YubiKey** によるスマートカード認証のサポート 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 アプリと、VDA セッションの仮想セッションおよび公開アプリに、単一デバイス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システムを接続する必要がなくなります。YubiKey は OTP、FIDO などの多様なプロトコルをサポートしており、エンドユーザーのエクスペリエンスを簡素化します。

Citrix Workspace アプリにサインインするには、iPhone または iPad に YubiKey を挿入し、スマートカードの切り替えをオンにして、ストア URL を指定します。

#### 注:

iOS 向け Citrix Workspace アプリは YubiKey 5 シリーズのみをサポートします。YubiKey について詳しくは、「[YubiKey 5 シリーズ](#)」を参照してください。

**Type C** ベースの一般的なリーダーのサポート iOS 向け Citrix Workspace アプリは、スマートカード認証で Type-C CCID 準拠リーダーをサポートでき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をサポートしていました。Citrix Workspace アプリに Type-C スマートカードリーダーを搭載すると、ユーザーは Citrix Workspace アプリを通じて認証できる上に、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 つの利点を得られます。

**UEM** を介したデバイス名の構成 このリリースでは、Unified Endpoint Management (UEM) を通じて、deviceName という新規パラメーターを構成できるようになりました。この属性は、管理者がユーザーグループに基づいてデバイス名を割り当て、識別するのに役立ちます。

構成キー	値の種類	構成値
deviceName	文字列	name_of_the_device

**iOS** バージョン **14** のサポートは廃止されました iOS 向け Citrix Workspace アプリは、23.12.0 より、iOS バージョン 14 以前のサポートを停止します。iOS の最新バージョンへは、App Store からアップグレードできます。詳しくは、[廃止の表](#)を参照してください。

### Technical Preview

- 外部 Web カメラのサポート

この Technical Preview について詳しくは、「[Technical Preview の機能](#)」を参照してください。

#### 解決された問題

- Citrix Workspace アプリの言語がイタリア語に設定されている場合に、デスクトップセッションの起動が失敗します。

## 23.12.0

#### 新機能

**YubiKey** によるスマートカード認証のサポート 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 アプリと、VDA セッションの仮想セッションおよび公開アプリに、単一デバイス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システムを接続する必要がなくなります。YubiKey は OTP、FIDO などの多様なプロトコルをサポートしており、エンドユーザーのエクスペリエンスを簡素化します。

Citrix Workspace アプリにサインインするには、iPhone または iPad に YubiKey を挿入し、スマートカードの切り替えをオンにして、ストア URL を指定します。

注:

iOS 向け Citrix Workspace アプリは YubiKey 5 シリーズのみをサポートします。YubiKey について詳しくは、「[YubiKey 5 シリーズ](#)」を参照してください。

**Type C** ベースの一般的なリーダーのサポート iOS 向け Citrix Workspace アプリは、スマートカード認証で 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をサポートしていました。Citrix Workspace アプリに Type-C スマートカードリーダーを搭載すると、ユーザーは Citrix Workspace アプリを通じて認証できる上に、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 つの利点を得られます。

**UEM** を介したデバイス名の構成 このリリースでは、Unified Endpoint Management (UEM) を通じて、deviceName という新規パラメーターを構成できるようになりました。この属性は、管理者がユーザーグループに基づいてデバイス名を割り当て、識別するのに役立ちます。

---

構成キー	値の種類	構成値
deviceName	文字列	name_of_the_device

---

**iOS バージョン 14** のサポートは廃止されました iOS 向け Citrix Workspace アプリは、23.12.0 より、iOS バージョン 14 以前のサポートを停止します。iOS の最新バージョンへは、App Store からアップグレードできます。詳しくは、[廃止の表](#)を参照してください。

## Technical Preview

- 外部 Web カメラのサポート

この Technical Preview について詳しくは、「[Technical Preview の機能](#)」を参照してください。

### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## 23.12.0

### 新機能

**YubiKey** によるスマートカード認証のサポート 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。これにより、Web アプリや SaaS アプリ、および仮想セッションに対する単一デバイス認証エクスペリエンスが提供され、スマートカードリーダーやその他の外部認証システムに接続する必要がなくなります。YubiKey は OTP、FIDO などの多様なプロトコルをサポートしており、エンドユーザーのエクスペリエンスを簡素化します。

Citrix Workspace アプリにサインインするには、iPhone または iPad に YubiKey を挿入し、スマートカードの切り替えをオンにして、ストア URL を指定します。

注:

iOS 向け Citrix Workspace アプリは YubiKey 5 シリーズのみをサポートします。YubiKey について詳しくは、「[YubiKey 5 シリーズ](#)」を参照してください。

**Type C** ベースの一般的なリーダーのサポート iOS 向け Citrix Workspace アプリは、スマートカード認証で 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をサポートしていました。Citrix Workspace アプリに Type-C スマートカードリーダーを搭載すると、ユーザーは Citrix Workspace アプリを通じて認証できる上に、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 つの利点を得られます。

**UEM** を介したデバイス名の構成 このリリースでは、Unified Endpoint Management (UEM) を通じて、deviceName という新規パラメーターを構成できるようになりました。この属性は、管理者がユーザーグループに基づいてデバイス名を割り当て、識別するのに役立ちます。

---

構成キー	値の種類	構成値
deviceName	文字列	name_of_the_device

---

**iOS** バージョン **14** のサポートは廃止されました。iOS 向け Citrix Workspace アプリは、23.12.0 より、iOS バージョン 14 以前のサポートを停止します。iOS の最新バージョンへは、App Store からアップグレードできます。詳しくは、[廃止の表](#)を参照してください。

## Technical Preview

- 外部 Web カメラのサポート

この Technical Preview について詳しくは、「[Technical Preview の機能](#)」を参照してください。

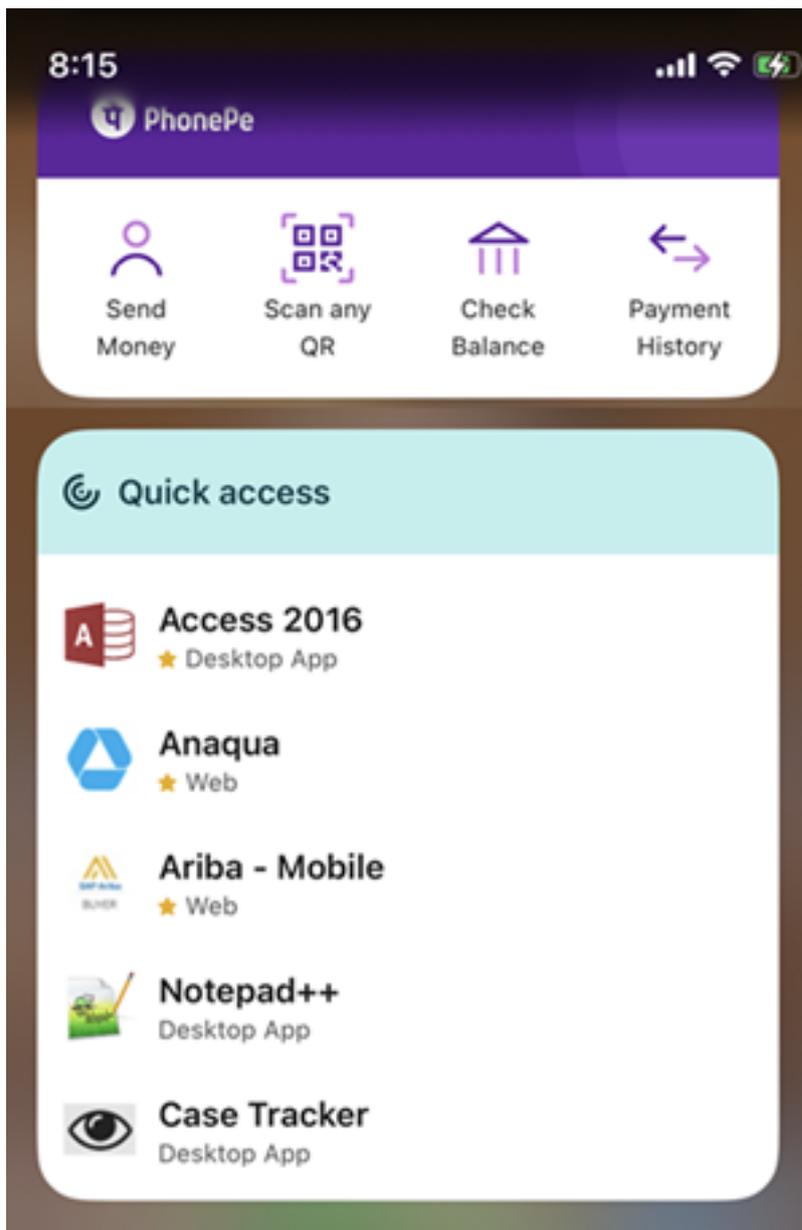
### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## 23.11.0

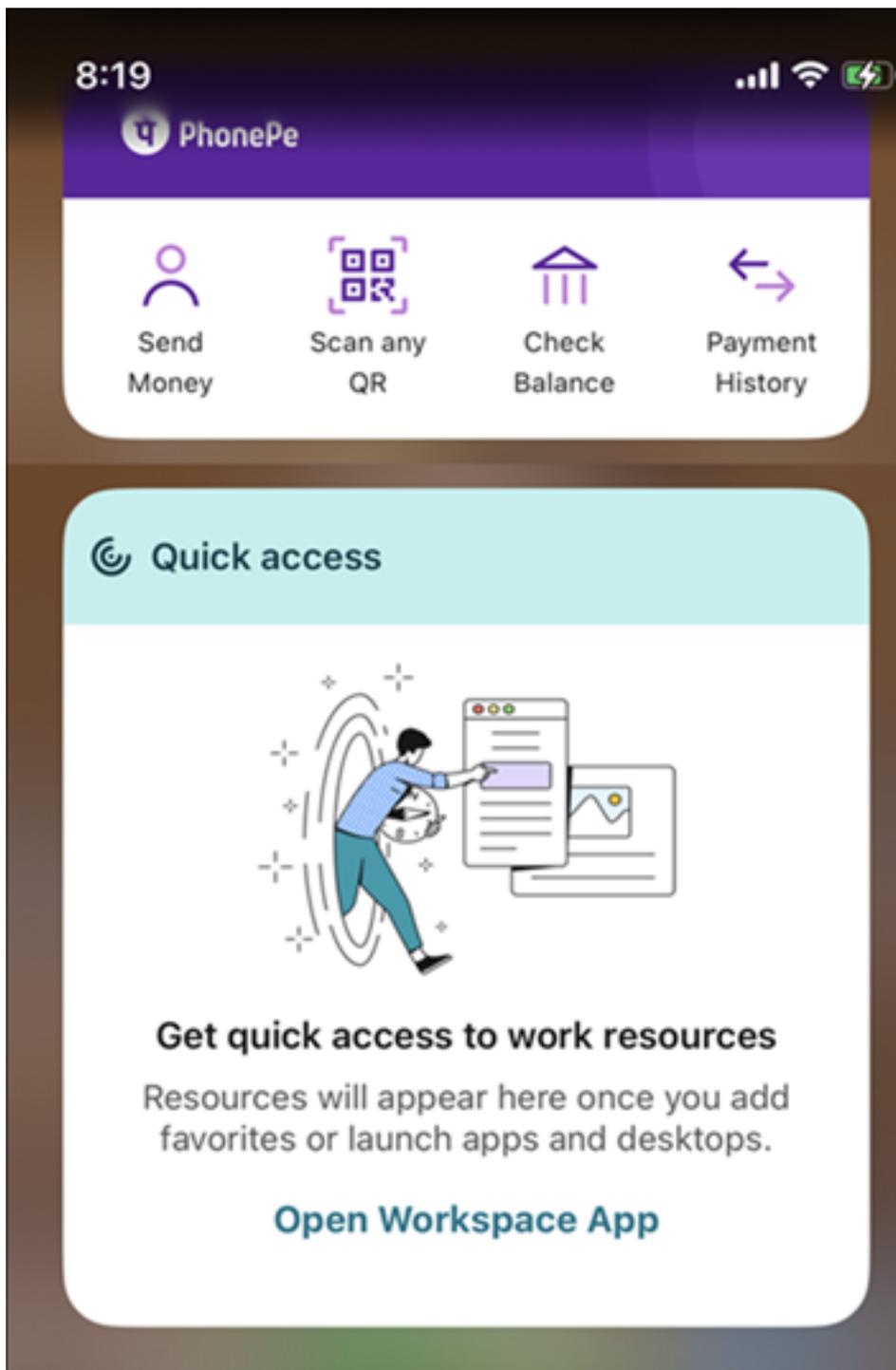
アプリとデスクトップをウィジェットとして表示

エンドユーザーは、iPhone や iPad から直接仮想アプリやデスクトップを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使うことができます。



ウィジェットは、次の基準に従って自動的に作成されます：

- 3つのお気に入りと2つの最近開いた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は、最大5つの最近開いた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
- 最近開いたアプリまたはデスクトップがない場合は、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
- アプリまたはデスクトップがまだお気に入りとして追加されておらず、最近アプリまたはデスクトップを開いていない場合、ユーザーはiOS向けCitrix Workspaceアプリを開くように求められます。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。



#### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 23.10.1

#### 新機能

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

#### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 23.10.0

#### 新機能

**iOS バージョン 14** のサポートの廃止に関する情報 Citrix Workspace アプリでは、のバージョン 23.12.0 以降、iOS バージョン 14 以前のサポートを停止します。iOS の最新バージョンへは、App Store からアップグレードできます。詳しくは、「[廃止](#)」の表を参照してください。

#### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 23.9.0

#### 新機能

**Transport Layer Security 1.3** のサポート iOS 向け Citrix Workspace アプリが Transport Layer Security (TLS) 1.3 をサポートするようになり、パフォーマンスと効率が向上しました。TLS 1.3 は、強力な暗号の組み合わせと 1 回限りのセッションキーによる堅牢なセキュリティを提供します。

エンドユーザーが iOS 向け Citrix Workspace アプリでこの機能を有効にするには、次の手順を実行します。

1. [詳細設定] > [TLS バージョン] に移動します。
2. [TLS バージョン] を選択します。

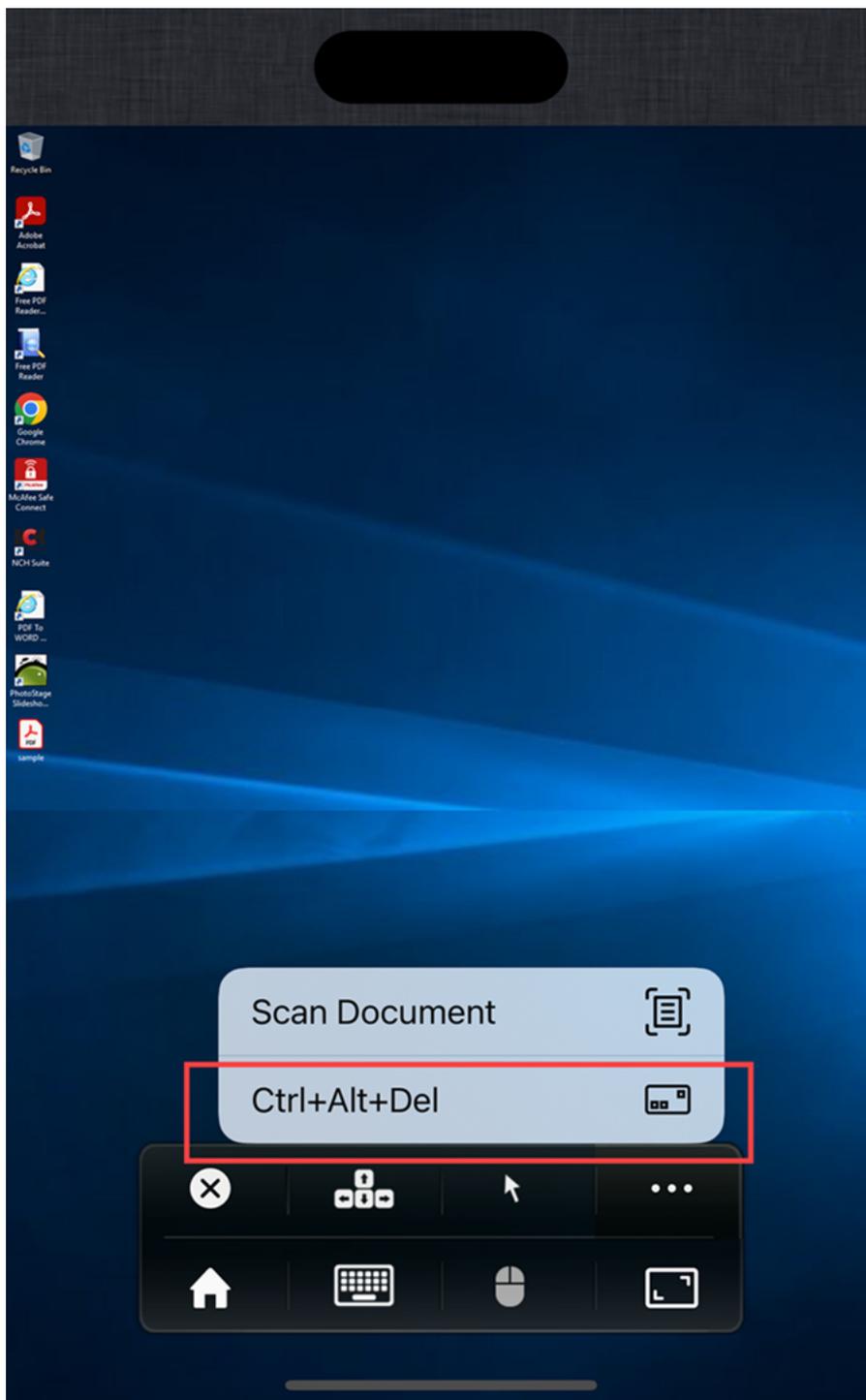
**AirPrint** 対応プリンターのサポート AirPrint テクノロジー対応プリンターを使用すると、エンドユーザーは iOS デバイス上のアクティブなセッションからドキュメントを印刷できるようになります。これにより、ケーブルまたはネットワーク経由でプリンターを接続する必要がなくなります。ユーザーが印刷コマンドを開始すると、AirPrint 対応プリンターが他の利用可能なプリンターとともに一覧に表示されます。

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

- 該当するプリンターは AirPrint と互換性があり、AirPrint が有効になっ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する必要があります。

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

**Ctrl+Alt+Del** ショートカットをセッションツールバーに追加 セッションツールバーには、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、ユーザーの切り替え、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。



**FIDO2** ベースの認証 iOS 向け 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なしの認証をサポートするようになりました。これにより、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

ドなしの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 ポートがあるデバイスはサポートされていません)。パスワードなしの認証を使用した 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。

この機能の前提条件については、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。

### Technical Preview

- 統合エンドポイント管理 (UEM) を使用して複数のストアを追加する
- 統合エンドポイント管理 (UEM) を使用して複数のストアを削除する

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## 23.7.5

### 新機能

スマートカードで利用可能なすべての証明書を表示する

iOS 向け Citrix Workspace アプリでは、スマートカードで利用可能な複数の証明書が表示され、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。スマートカードの切り替えを有効にすると、必要な証明書を [証明書の選択] ページから選択できます。



## **Global App Configuration** サービス対応 **Web** ストアにアクセスする

管理者は、メールアドレスによるストア検出用に Web ストア (Web Interface) を構成できるようになりました。Global App Configuration Service によって、ストアを追加するときに (ようこそ画面上で) エンドユーザーが入力したメールアドレスに基づき、管理者が定義したカスタム Web (Web Interface) URL を識別できます。エンドユーザーは、管理者が構成した Web ストアに自動的に移動します。エンドユーザー向けの Web ストア URL の構成については、「[Allowed custom web portal](#)」を参照してください。

## **PNAgent** 廃止のお知らせ

iOS 向け Citrix Workspace アプリで、23.7.5 リリースでの PNA ストアの廃止が発表されました。Citrix は、23.7.5 リリース以降、PNA ストア機能のバグ修正やセキュリティ パッチをサポートしません。

### 解決された問題

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

## **23.6.5**

### 新機能

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

### 解決された問題

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

## **23.6.0**

### 新機能

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

### 解決された問題

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

## 23.5.0

### 新機能

**拡張キーボードの機能強化** 23.5.0 バージョン以降、拡張キーボード機能が強化され、より優れたユーザーエクスペリエンスが提供されます。以下のような機能強化です：

- 拡張ツールバー UI を固定または固定解除します。
- 画面の回転に合わせて拡張ツールバーを回転させます。
- Windows アイコンキーと 3 キーの組み合わせによるショートカットをサポートします。
- 複数モニターのユースケースシナリオにおけるエクスペリエンスが向上します。
- 拡張ツールバー UI を自動的に開くか閉じます。
- ステージマネージャーモードのエクスペリエンスが向上します (M1 チップを搭載した iPad 上)。

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

## 23.4.5

### 新機能

**Global App Configuration Service** チャンネルのサポート 23.4.5 リリース以降、管理者は Global App Configuration Service 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ロールアウトする前にそれらをテストできるようになりました。このプロセスにより、実稼働前に機能を十分にテストすることができます。

#### 注：

- iOS 向け Citrix Workspace アプリは、デフォルトおよびテストチャンネル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デフォルトチャンネルを使用しています。

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

構成方法について詳しくは、[Global App Configuration Service Channel のサポート](#)を参照してください。

**MDM** ソリューションを使用したストア構成のサポート iOS 向け Citrix Workspace アプリは、モバイルデバイス管理 (MDM) ソリューションを使用した Workspace ストア URL のリモート構成をサポートするようになりました。詳しくは、「[MDM ソリューションを使用した Workspace アプリの構成](#)」を参照してください。

**MDM** ソリューションの機能強化 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 アプリを構成するいくつかの構成をサポートしています。以前は、管理者がストア 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 を変更し、アプリの表示方法を制御することを制限できるようになりました。

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	値の種類	構成値
url	String	ストア URL。例： <code>prodcwa.cloud.com</code>
storeType	Integer	- (既定値) 1 に設定すると、ユーザーはネイティブの、またはデフォルトのストアの読み込み内容を表示できます。- 2 に設定すると、ユーザーは Web Interface 内でストアを表示できます。
restrict_user_store_modification	Boolean	<ul style="list-style-type: none"> <li>• <b>true</b> に設定すると、ユーザーはストアを変更（追加、削除、または編集）できません。</li> <li>- <b>false</b> に設定すると、ユーザーはストアを変更できます。</li> </ul> 注：フラグが true に設定されている場合、新しい MDM 構成ストアを追加する前に、すべての既存のストアが削除されます。

## Technical Preview

- FIDO2 ベースの認証のサポート

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 23.4.5 で解決された問題

- ナチュラルスクロールモードを有効にして、指を iPad の上から下に移動すると、ページが下に移動します。ナチュラルスクロールを無効にしても、同じ動作が実行されます。また、この現象は Magic Mouse でも発生

します。[HDX-49267]

- 拡張モードでは、解像度が [自動調整-中] または [自動調整 - 高] の場合、画面の解像度が自動スケーリングされ、表示が切り捨てられます。この問題は、Citrix Workspace アプリがバックグラウンドから前面に移動したときに発生します。[CVADHELP-19169]

## 23.3.5

### 新機能

ユーザーエージェント文字列 WKWebView を介して開始された一部のネットワーク要求で使用される user-agent 文字列に、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。

したがって、次のように変更されました。変更前:

```
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
```

変更後 (以下のいずれか):

```
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)
```

### Technical Preview

- 高速スキャン

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 23.3.5 で解決された問題

iOS 向け Citrix Workspace アプリをバージョン 23.3.0 にアップグレードした後、ストアが MDM ソリューションによって完全なストアアドレスを使用して構成されている場合、ストアで認証できません。

## 23.3.0

### 新機能

#### MDM ソリューションを使用したストア構成のサポート **[Technical Preview]**

注:

この機能は公開プレビュー段階です。

iOS 向け Citrix Workspace アプリは、モバイルデバイス管理 (MDM) ソリューションを使用した Workspace ストア URL のリモート構成をサポートするようになりました。詳しくは、「[MDM ソリューションを使用した Workspace アプリの構成](#)」を参照してください。

**セッションのタイムアウト後の再認証** このリリースでは、前回のサインイン以降にセッションの有効期限が切れた場合、Citrix Workspace アプリへの再認証を求めるメッセージが表示さ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 アプリに接続するときに、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。

### Technical Preview

- ドキュメントスキャナー
- PiP のサポート

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 解決された問題

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

## 23.2.1

### 新機能

**背面カメラのサポート** iOS 向け Citrix Workspace アプリでは、VDA セッション内でカメラを前面から背面に、またはその逆に切り替えることができるようになりました。

仮想セッションでカメラを呼び出すと、画面にカメラのフローティングボタンが表示され、カメラの位置を切り替えることができます。また、フローティングボタンを画面上で自由に動かして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の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 によって有効になっているカメラの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:

キャスト機能またはドキュメントのスキャン機能が有効になっていると、フローティングボタンが部分的または完全に遮られます。

**ストア URL の自動入力**のサポート 名称変更された iOS 向け Citrix Workspace アプリにアクセスする場合、ストア URL の自動入力を選択できます。この機能により、手動による介入が減り、アプリへの迅速なアクセスが提供されます。アプリの個人設定について詳しくは、「[App Personalization](#)」を参照してください。

**認証でのブラウザ切り替え**のサポート iOS または iPad デバイスでは、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、管理者は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るようになりました。詳しくは、「[認証プロセスの書き換えポリシーの構成](#)」を参照してください。

解決された問題

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

## 23.2.0

### 新機能

**背面カメラのサポート** iOS 向け Citrix Workspace アプリでは、VDA セッション内でカメラを前面から背面に、またはその逆に切り替えることができるようになりました。

仮想セッションでカメラを呼び出すと、画面にカメラのフローティングボタンが表示され、カメラの位置を切り替えることができます。また、フローティングボタンを画面上で自由に動かして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の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 によって有効になっているカメラの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:

キャスト機能またはドキュメントのスキャン機能が有効になっていると、フローティングボタンが部分的または完全に遮られます。

**ストア URL の自動入力**のサポート 名称変更された iOS 向け Citrix Workspace アプリにアクセスする場合、ストア URL の自動入力を選択できます。この機能により、手動による介入が減り、アプリへの迅速なアクセスが提供されます。アプリの個人設定について詳しくは、「[App Personalization](#)」を参照してください。

**認証でのブラウザ切り替え**のサポート iOS または iPad デバイスでは、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、管理者は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るようになりました。詳しくは、「[認証プロセスの書き換えポリシーの構成](#)」を参照してください。

### 解決された問題

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

### 制限事項

- コピー/貼り付けには、デバイスのソフトキーボードの **Control+C** キーと **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** キーと **Command+V** キーは機能しない場合があります。[HDX-32431]
- Safari Web ブラウザー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できません。  
Safari からアプリを起動するためには、デバイス上に iOS 向け Citrix Workspace アプリまたは Citrix Receiver for iOS のいずれか一方のみの最新バージョンがインストールされていることを確認してください。[RFIOS-5502]
- StoreFront から Citrix Workspace に移行した後、Pendo ガイドの [次へ] ボタンをタップしている間、画面が一瞬点滅します。
- Citrix Workspace アプリ内から Web および SaaS アプリを起動中、Google IdP を使用しているアプリでユーザーによるサインインが必要な場合は、認証が失敗し、「アクセスが拒否されました」というエラーメッセージが表示されます。[RFIOS-11904]

## 廃止

廃止済みの項目については、「[廃止済み](#)」ページを参照してください。

## Technical Preview の機能

July 1, 2024

Technical Preview の機能は、非実稼働環境または制限のある稼働環境で使用でき、お客様がフィードバックを共有する機会を提供します。Technical Preview の機能のサポートは行っていませんが、改善に関するフィードバックをお待ちしております。重要度と重大度により、フィードバックに対応する場合があります。

### Technical Preview の機能の一覧

次の表に、Technical Preview の機能を示します。これらの機能は、リクエストベースで提供される Preview 機能です。これらの機能についてフィードバックを提供する場合は、対応するフォームにご記入ください。

タイトル	利用できる最小バージョン	有効化フォーム（アイコンをクリック）	フィードバックフォーム（アイコンをクリック）
<a href="#">Citrix Workspace アプリへのアクセスで生体認証の強制をサポート</a>	2405		
<a href="#">Microsoft Entra ID 参加済み仮想マシンのシングルサインオンをサポート</a>	2405		
<a href="#">UEM 経由による Citrix Workspace アプリ設定の構成をサポート</a>	24.3.5		
<a href="#">アダプティブオーディオのサポート</a>	24.3.0		
<a href="#">アクセシビリティと VoiceOver のサポート</a>	24.2.0		

タイトル	利用できる最小バージョン	有効化フォーム（アイコンをクリック）	フィードバックフォーム（アイコンをクリック）
外部 Web カメラのサポート	23.12.0		
統合エンドポイント管理 (UEM) を使用して複数のストアを追加する	23.9.0		
統合エンドポイント管理 (UEM) を使用して複数のストアを削除する	23.9.0		
高速スキャン	23.3.5		
ピクチャインピクチャ (PiP) のサポート	23.3.0		
Apple ネイティブの非ミラーリングモードのサポート	23.3.0		
Web アプリおよび SaaS アプリ向けに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	23.3.0		

### Citrix Workspace アプリへのアクセスで生体認証の強制をサポート

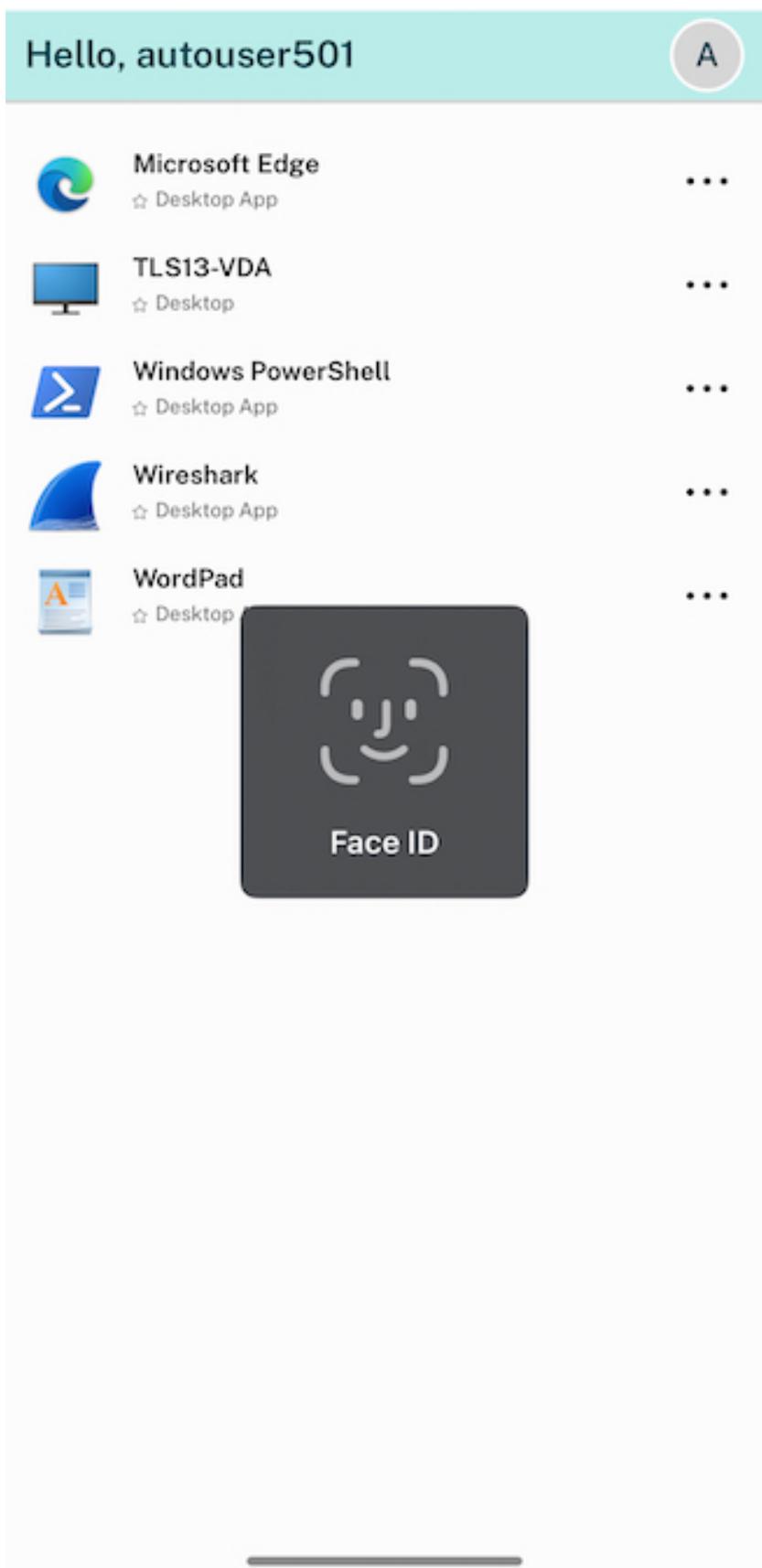
2405 バージョン以降の Technical Preview

[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 以降では、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使用することを強制できるようになりました。この機能を使用すると、Citrix Workspace アプリを閉じた後に開くか、最小化した後に最前面に表示すると、ロック解除してサインインするための Face ID または Touch ID の検証の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、アプリへのアクセスにはパス

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になり、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、次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`
- 値の種類: ブール値
- 値: `true` または `false`
  - **true** に設定すると、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になります。
  - **false** に設定すると、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ことができます。

## Microsoft Entra ID 参加済み仮想マシンのシングルサインオンをサポート

---

2405 バージョン以降の Technical

[有効化フォーム](#)

[フィードバックフォーム](#)

---

Preview

24.5.0 バージョン以降、iOS 向け Citrix Workspace アプリは、シングルサインオン認証を使用して Azure AD に参加している仮想マシンデバイスに、ユーザーがサインインできるようにします。Azure AD 参加済み仮想マシンデバイスに初めてサインインするときは、Microsoft 資格情報を提供する必要があります。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必要ありません。

注：

- ユーザーが認証に **WKwebview** を使用しない場合は、最初に資格情報を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。

## UEM 経由による Citrix Workspace アプリ設定の構成をサポート

---

24.3.5 バージョンからの

[有効化フォーム](#)

[フィードバックフォーム](#)

---

Technical Preview

以前は、統合エンドポイント管理 (UEM) を使用してのみ、Citrix Workspace アプリでストア URL を構成できました。

24.3.5 バージョン以降は、インフラストラクチャに展開されている UEM ソリューションを使用して、管理対象デバイス上で 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 および Global App Configuration Service (GACS) を使用して Citrix Workspace ア

アプリ設定を構成するオプションがある場合、UEM は常に GACS よりも優先されます。

以下は、Citrix Workspace アプリの設定を構成するためのサンプル json ファイルです:

```
1 <dict>
2   <key>stores</key>
3   <array>
4     <dict>
5       <key>url</key>
6       <string>https://teststore.cloud.com</string>
7       <key>storeType</key>
8       <integer>1</integer>
9       <key>displayName</key>
10      <string>Cloud Store 1</string>
11      <key>appSettings</key>
12      <array>
13        <dict>
14          <key>category</key>
15          <string>audio</string>
16          <key>userOverride</key>
17          <false/>
18          <key>settings</key>
19          <array>
20            <dict>
21              <key>name</key>
22              <string>settings_audio_stream</string>
23              <key>value</key>
24              <true/>
25            </dict>
26          </array>
27        </dict>
28      <dict>
29        <key>category</key>
30        <string>authentication</string>
31        <key>userOverride</key>
32        <false/>
33        <key>settings</key>
34        <array>
35          <dict>
36            <key>name</key>
37            <string>settings_auth_web_browser</string>
38            <key>value</key>
39            <string>embedded</string>
40          </dict>
41        </array>
42      </dict>
43    </array>
44  </dict>
45  <dict>
46    <key>url</key>
47    <string>https://teststore.cloud.com</string>
48    <key>storeType</key>
49    <integer>1</integer>
50    <key>displayName</key>
```

```
51     <string>StoreFront1</string>
52     <key>appSettings</key>
53     <array>
54         <dict>
55             <key>category</key>
56             <string>audio</string>
57             <key>userOverride</key>
58             <false/>
59             <key>settings</key>
60             <array>
61                 <dict>
62                     <key>name</key>
63                     <string>settings_audio_stream</string>
64                     <key>value</key>
65                     <false/>
66                 </dict>
67             </array>
68         </dict>
69         <dict>
70             <key>category</key>
71             <string>authentication</string>
72             <key>userOverride</key>
73             <false/>
74             <key>settings</key>
75             <array>
76                 <dict>
77                     <key>name</key>
78                     <string>settings_auth_web_browser</string>
79                     <key>value</key>
80                     <string>system</string>
81                 </dict>
82             </array>
83         </dict>
84     </array>
85 </dict>
86 </array>
87 <key>storesToDelete</key>
88 <array>
89     <string>test.cldblr.com</string>
90     <string>test.cloud.com</string>
91 </array>
92 <key>restrict_user_store_modification</key>
93 <false/>
94 </dict>
95 <!--NeedCopy-->
```

## 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。いずれかの設定で `userOverride` フラグが `false` に設定されている場合、ユーザーは Citrix Workspace アプリの設定でその設定を変更できません。

キーと値のペアの表

次の表に、キーと値のペアに関する情報を示します：

注：  
 カテゴリに固有の設定は、そのカテゴリの 1 つ下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	値の種類	デフォルト値
オーディオ	オーディオ	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するためのアクセスをユーザーに提供します。	settings_audio	true/false	ブーリアン型	TRUE
keyboard	Unicode キーボードを使用する	ユーザーは標準の Unicode キーボードを使用できます。	settings_use_unicode_keyboard	true/false	ブーリアン型	TRUE
keyboard	自動キーボード	セッション内のキーボードの自動表示を有効または無効にします。	settings_automate_keyboard	true/false	ブーリアン型	TRUE
keyboard	キーボードレイアウトの同期	ユーザーはデバイスの優先キーボードレイアウトに切り替えることができます。	settings_keyboard_layout_sync	true/false	ブーリアン型	FALSE

カテゴリ	設定	説明	キー	値	値の種類	デフォルト値
keyboard	カスタムキーボードを使用する	ユーザーは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できません。	settings_allow_third_party_extensions	true/false	ブーリアン型	FALSE
display	セッション解像度	ユーザーは画面の解像度を選択できません。	settings_resolution	0/1/2/3/4/5	整数	5 (iPad) 3 (iPhone)
display	プレゼンテーションモード	外部ディスプレイを使用している間、iOS デバイスをトラックパッドとして使用してセッションを制御できます。	settings_present_mode	true/false	ブーリアン型	FALSE
display	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	ブーリアン型	TRUE
advanced	厳密な証明書の検証	サーバー証明書の検証をより厳密に制御します。	settings_strict_certificate_validation	true/false	ブーリアン型	FALSE
advanced	TLS バージョン	ユーザーは、トラブルシューティングの目的で TLS 設定を変更できます。	settings_tlsVersion	0/1/2/3	整数	0

カテゴリ	設定	説明	キー	値	値の種類	デフォルト値
advanced	ネイティブのコンボボックスを使用する	iOS のネイティブ選択機能の使用を有効にします。	settings_native_checkbox	true/false	ブーリアン型	TRUE
advanced	タッチ有効 (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と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	true/false	ブーリアン型	true (iPad) false (iPhone)
advanced	全画面表示	アプリとデスクトップを全画面で表示できるようにします。	settings_mobile_fullscreen	true/false	ブーリアン型	true (iPad) false (iPhone)
advanced	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ます。	settings_reconnect_on_login	true/false	ブーリアン型	FALSE
advanced	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_on_refresh	true/false	ブーリアン型	FALSE

カテゴリ	設定	説明	キー	値	値の種類	デフォルト値
advanced	HTTP プロキシを有効にする	セッションに HTTP プロキシを使用できるようにします。	settings_use_proxy	true/false	ブーリアン型	TRUE
advanced	派生資格情報を使用します	派生資格情報を使用できるようにします。	setting_useDerivedCredentials	true/false	ブーリアン型	FALSE
advanced	セッションでスマートカード使用	セッション内でスマートカードデバイスを使用できるようにします。この設定では、ユーザーはセッションに対して認証できません。	settings_usesSmartCardInsideSession	true/false	ブーリアン型	FALSE
advanced	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_allow_tdp	true/false	ブーリアン型	TRUE
advanced	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、タブレットモードで仮想セッションを起動できます。	settings_enableTabletModeSwitch	true/false	ブーリアン型	TRUE
advanced	表示したままにする	画面をオンのままにします。	settings_stay Awake	true/false	ブーリアン型	FALSE

カテゴリ	設定	説明	キー	値	値の種類	デフォルト値
advanced	iPad ストレージの使用	デバイス上のローカルドライブにアクセスできるようにします。	settings_client_storage	true/false	ブーリアン型	false
X1 Mouse	X1 マウスを許可	Citrix X1 Mouse へのアクセスを切り替えることができるようにします。	settings_allow_x1_mouse	true/false	ブーリアン型	FALSE
X1 Mouse	Citrix X1 マウスの速度	ユーザーは、仮想セッション内でマウスカーソルの速度を制御できます。	settings_x1_mouse_speed	整数	整数	200 (iPadPro) 100 (その他のすべてのデバイス)
X1 Mouse	Citrix X1 マウスのリモートカーソルイメージを使用する	セッション内でカーソルをアプリまたはデスクトップに一致させます。たとえば、カーソルがテキストボックス上にある場合は、テキストボックスに対応した形になります。	settings_x1_mouse_always_side_cursor	true/false	ブーリアン型	TRUE
authentication	認証用の Web ブラウザー	デバイス上で WKWeb ではなく SafariView-Controller を使用していることを識別できます。	settings_auth_system_embedding	true/false	ブーリアン型	埋め込み

## iOS 向け Citrix Workspace アプリ

カテゴリ	設定	説明	キー	値	値の種類	デフォルト値
thirdPartyServices	LaunchDarkly	Citrix Workspace アプリの機能で LaunchDarkly フラグを有効にします。	enableLaunchDarkly	false	ブーリアン型	true (EU 以外の地域)

### アダプティブオーディオのサポート

24.3.0 バージョンからの  
Technical Preview

[有効化フォーム](#)

[フィードバックフォーム](#)

24.3.0 以降、iOS 向け Citrix Workspace アプリでは HDX アダプティブオーディオがサポートされます。この機能は、音質の向上と低遅延を提供することにより、ユーザーエクスペリエンスを向上させます。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[オーディオポリシー設定](#)」を参照してください。

### アクセシビリティと **VoiceOver** のサポート

24.2.0 バージョンからの  
Technical Preview

[有効化フォーム](#)

[フィードバックフォーム](#)

バージョン 24.2.0 以降、iOS 向け Citrix Workspace アプリはアクセシビリティと VoiceOver 機能をサポートします。この機能は、画面を見ることが困難なエンドユーザーをサポートします。Citrix Workspace と仮想セッションの UI の使用時に、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。

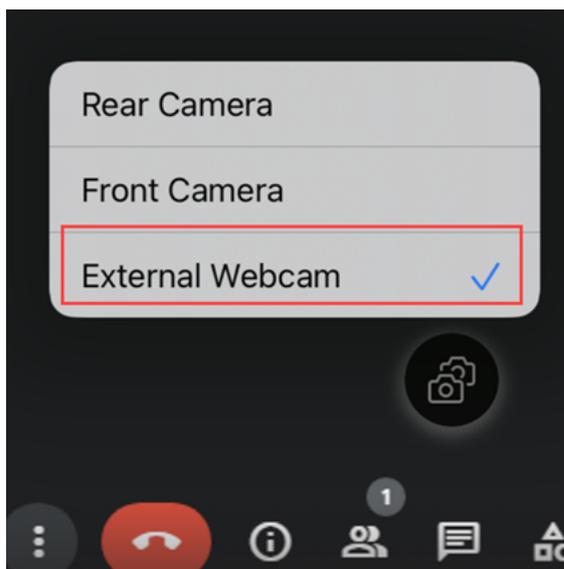
Citrix Workspace アプリを操作するには、iOS が提供するアクセシビリティの標準ジェスチャを使用する必要があります。たとえば、画面を左右にスワイプすると、各項目の voiceover を再生しながらメニュー間を移動できます。詳しくは、Apple サポートドキュメントの「[iPhone のアクセシビリティ機能を使ってみる](#)」および「[iPad のアクセシビリティ機能を使ってみる](#)」を参照してください。

### 外部 **Web** カメラのサポート

iOS 向け Citrix Workspace アプリが、DaaS セッション内で外部接続された Web カメラをサポートするようになりました。Web カメラを USB で接続してビデオ会議に使用する場合は、[カメラ] アイコンをクリックして [外部 **Web** カメラ] オプションを選択します。エンドユーザーが利用できるリソースを使用することで、セッションエクスペリエンスを強化できます。

注:

- 外部 Web カメラは、USB-C コネクタを備えた iOS 17 以降を実行している iPad でのみサポートされません。
- [外部 Web カメラ] オプションは、外部カメラが検出された後に表示されます。
- 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 によって有効になっているカメラのフローティングボタンを使用する必要があります。



次回ビデオ会議アプリを使用するとき、システムは前回のユーザーの環境設定に応じたカメラの設定を使用します。たとえば、最後のビデオ通話を [外部 **Web** カメラ] 設定で終了した場合、次回からは外部 Web カメラ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と、カメラの環境設定を変更できます。通話中にカメラの設定を変更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両方のお客様が使用できます。

統合エンドポイント管理 (**UEM**) を使用して複数のストアを追加する

## Technical Preview

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、管理対象の iOS デバイス用に複数のストアを追加して構成できるようになりました。各ストアの詳細を 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中にアップロードできます。

## 注:

XML ファイルはキーと値で構成される形式である必要があります。

構成キー	値の種類	説明
url	文字列	ストア URL。たとえば、 example.cloud.com
storeType (オプション)	整数	<b>1</b> に設定すると、ユーザーはネイティブの、またはデフォルトのストアの読み込み内容を表示できます。 <b>2</b> に設定すると、ユーザーは Web Interface 内でストアを表示できます。
displayName (オプション)	文字列	ストアの名前です。
restrict_user_store_modification (オプション)	ブーリアン型	<b>true</b> に設定すると、ユーザーはストアを変更（追加、削除、または編集）できません。 <b>false</b> に設定すると、ユーザーはストアを変更（追加、削除、または編集）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、既存のストアがすべて削除されます。
- 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がネイティブと見なされます。

ストアを追加するためのサンプル **XML** 構成

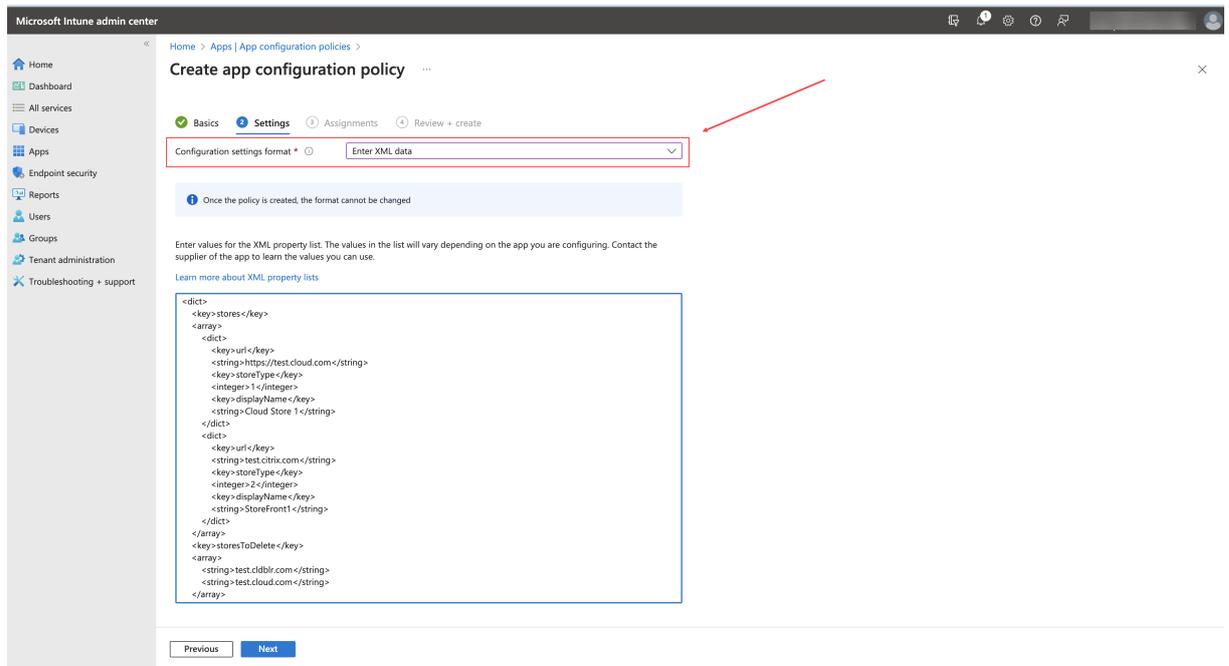
詳しくは、このサンプル XML ファイルを参照してください。

```

1      <dict>
2          <key>stores</key>
3          <array>
4              <dict>
5                  <key>url</key>
6                  <string>test.cloud.com</string>
7                  <key>storeType</key>
8                  <integer>1</integer>
9                  <key>displayName</key>
10                 <string>Cloud Store </string>
11             </dict>
12             <dict>
13                 <key>url</key>
14                 <string>test.citrix.com</string>
15                 <key>storeType</key>
16                 <integer>2</integer>
17                 <key>displayName</key>
18                 <string>StoreFront</string>
19             </dict>
20         </array>
21         <key>restrict_user_store_modification</key>
22         <true/>
23     </dict>
24
25 <!--NeedCopy-->

```

ストア構成を含む XML ファイルの準備ができたなら、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。



統合エンドポイント管理 (UEM) を使用して複数のストアを削除する

23.12.0 バージョンからの

[有効化フォーム](#)

[フィードバックフォーム](#)

Technical Preview

1 つまたは複数のストアを削除するには、管理者は、キー名 **storesToDelete** を使用して、削除するストアの一覧を 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サンプル XML 構成

詳しくは、このサンプル XML ファイルを参照してください。

```
1 <dict>
2   <key>storesToDelete</key>
3   <array>
4     <string>test.cldblr.com</string>
5     <string>test.onprem.com</string>
6   </array>
7 </dict>
8
9 <!--NeedCopy-->
```

以下は、ストアの追加と削除の構成を含むサンプル XML 構成ファイルです。

```
1 <dict>
2   <key>stores</key>
3   <array>
4     <dict>
5       <key>url</key>
6       <string>test.cloud.com</string>
7       <key>storeType</key>
8       <integer>1</integer>
9       <key>displayName</key>
10      <string>Cloud Store </string>
11    </dict>
12    <dict>
13      <key>url</key>
14      <string>test.citrix.com</string>
15      <key>storeType</key>
16      <integer>2</integer>
17      <key>displayName</key>
18      <string>StoreFront</string>
19    </dict>
20  </array>
21  <key>storesToDelete</key>
22  <array>
23    <string>test.cldblr.com</string>
24    <string>test.onprem.com</string>
25  </array>
```

```
26     <key>restrict_user_store_modification</key>
27     <true/>
28 </dict>
29
30 <!--NeedCopy-->
```

## 高速スキャン

---

23.3.5 バージョンからの

[有効化フォーム](#)

[フィードバックフォーム](#)

Technical Preview

---

複数のデバイスで Citrix Workspace アプリにサインインしている場合は、高速スキャン機能を使用して iOS デバイスの多数のドキュメントをスキャンできます。その後、スキャンしたドキュメントを iOS デバイ스에 転送します。

高速スキャン機能を使用してドキュメントをスキャンする方法については、次の手順に従ってください：

1. Mac デバイスで、デスクトップセッションの Citrix Workspace アプリのアイコンを右クリックし、[高速スキャン] をクリックします。QR コードが表示されます。
2. iOS デバイスで、[設定] > [高速スキャン] をクリックします。
3. Mac デバイスに表示された QR コードをスキャンして、Mac と iOS デバイス間の接続を確立します。
4. ドキュメントをスキャンして、Mac デバイスに送信します。
5. Mac デバイスのデスクトップセッションでは、Finder でスキャンしたドキュメントを見つけることができます。

## 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。
- iOS デバイスと Mac デバイスの両方で、Citrix Workspace アプリの同じアカウントにサインインする必要があります。
- 同じ Wi-Fi に接続している必要があります。
- 必要な Mac 向け Citrix Workspace アプリの最小バージョンは 2304 です。
- 高速スキャンには、デバイスでの読み取りおよび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：
  1. プロファイルから、[アプリケーション設定] > [ストアの設定] をクリックします。
  2. 現在のストアをクリックします。
  3. [デバイスストレージ] をクリックし、[読み取り/書き込みアクセス] を選択します。

## ピクチャインピクチャ (PiP) のサポート

---

**Technical Preview**

---

iOS 向け Citrix Workspace アプリは、ピクチャインピクチャ (PiP) モードをサポートするようになりました。これにより、デスクトップセッション、SaaS アプリ、または Web アプリを浮動ウィンドウへと縮小できます。このウィンドウは画面上で自由に動かして、どこにでも配置できます。PiP モードでは、Citrix Workspace アプリのホーム画面が解放され、他のタスクを実行できるようになります。デスクトップセッションのセッションツールバーの [ホーム] ボタンをクリックするか、SaaS アプリまたは Web アプリの省略記号メニュー (…) > [最小化] をクリックして画面を最小化します。浮動ウィンドウをクリックしてアプリを全画面表示し、浮動ウィンドウの [X] アイコンをクリックしてアプリを閉じます。別のアプリを最小化すると、浮動ウィンドウが自動的に全画面表示されます。

この機能は、オンプレミス展開とクラウド展開の両方でサポートされます。ただし、クラウド展開の場合、Web アプリを PiP に最小化できます。浮動ウィンドウをクリックして、デスクトップセッションと Web アプリを切り替えることもできます。

**注:**

一度にアクティブにできるアプリは 2 つだけです。1 つは全画面表示モードで、もう 1 つは PiP として最小化されます。

- 2 つの Web アプリまたは SaaS アプリ
- 1 つの Web アプリまたは SaaS アプリと 1 つの仮想アプリまたはデスクトップセッション

**既知の制限事項:**

- マウスやキーボード、外部モニターなどの外付け周辺機器が接続されている場合、PiP モードは使用できません。
- PiP モードが有効で、デバイスが外部モニターに接続されている場合、Citrix Workspace アプリが応答しなくなり、デスクトップセッション内のディスプレイ設定で戻るボタンが使用できなくなります。

**Apple** ネイティブの非ミラーリングモードのサポート

---

**Technical Preview**

---

iPad OS 16.2 で利用できる Apple の非ミラーリングモードを使用して、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、および仮想デスクトップを実行し、iPad 画面で他のネイティブアプリを実行できるようにして、マルチタスクを実現できます。

注:

Apple の非ミラーリングモードによる拡張ディスプレイのサポートは、一部の iPad モデルでのみ利用できません。詳しくは、[Apple のドキュメント](#)を参照してください。

この Technical Preview 機能を使用しない場合は、いつでも Citrix Workspace アプリを全画面モードで使用できます。

**Web** アプリおよび **SaaS** アプリ向けに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

[有効化フォーム](#)

[フィードバックフォーム](#)

---

Technical Preview

---

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、内部 Web アプリおよび SaaS アプリ向けの SSO の構成を簡素化できます。強化された SSO エクスペリエンスにより、プロセス全体がいくつかのコマンドに集約されます。SSO をセットアップするために ID プロバイダーチェーンで Citrix Secure Private Access を構成するという、必須の前提条件がなくなります。また、Workspace アプリと起動中の特定の Web または SaaS アプリの両方の認証に同じ ID プロバイダーが使用される場合、ユーザーエクスペリエンスも向上します。

**Technical Preview** から一般提供 (**GA**)

---

サービスまたは機能	一般提供バージョン
-----------	-----------

---

<a href="#">ドキュメントスキャナーのサポート</a>	24.5.0
----------------------------------	--------

<a href="#">FIDO2 ベースの認証のサポート</a>	23.9.0
-----------------------------------	--------

---

システム要件と互換性

March 27, 2024

デバイスの要件

- iOS 向け Citrix Workspace アプリバージョン 23.9.0 以降は、iOS 17 および iPadOS 17 でサポートされません。

- iOS 向け Citrix Workspace アプリバージョン 22.9.0 以降は、iOS 16 および iPadOS 16 でサポートされません。
- iOS 向け Citrix Workspace アプリバージョン 21.9.1 以降は、iOS 15 および iPadOS 15 でサポートされません。
- iOS 向け Citrix Workspace アプリバージョン 20.9.0 以降は、iOS 14 および iPadOS 14 でサポートされません。
- このソフトウェアアップデートは、以下のデバイスで検証済みです：
  - iPhone 7x 各モデル、iPhone 8x 各モデル、iPhone X のみ。
  - iPad Pro を含めたすべての iPad モデル (iPad 1 と iPad 2 はサポートされていません)
- 外部ディスプレイのサポートは次のとおりです。
  - iPhone - iOS でサポートされるデバイス。
  - iPad - iOS でサポートされるデバイス (ディスプレイ全体には表示されません)。

### サーバーの要件

各サーバーに最新の Hotfix 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。

- Citrix Workspace アプリで仮想デスクトップやアプリに接続する場合、Citrix StoreFront、および Web Interface がサポートされます。

#### StoreFront:

- StoreFront 3.6 以降 (推奨)。Citrix Workspace アプリは StoreFront の最新バージョンで検証済みです。サポートされる前バージョンは、StoreFront 2.6 以降です。

StoreFront ストアへの直接アクセスを提供します。Citrix Workspace アプリでは、前バージョンの StoreFront もサポートされます。

#### 注:

XenApp および XenDesktop 7.8 で、Framehawk 仮想チャネルおよび 3D Pro が Citrix でサポートされるようになりました。この機能は、Citrix Workspace アプリに拡張されました。

- Workspace for Web サイトが構成された StoreFront。

StoreFront ストアへの Safari Web ブラウザーからのアクセスを提供します。ユーザーはブラウザーを使って手動で ICA ファイルを開く必要があります。この展開方法で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。

#### Web Interface:

- Web Interface サイトに Web Interface 5.4 使用
- XenApp および XenDesktop サイトに Web Interface 5.4 使用

- Citrix Gateway 上の Web Interface (Safari のみを使うブラウザーベースのアクセス)  
Citrix Gateway で提供されるリライトポリシーを有効にします。

• **Citrix Virtual Apps and Desktops、XenApp および XenDesktop** の以下のバージョン:

- 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、認証

StoreFront への接続では、Citrix Workspace アプリで以下の認証方法がサポートされます:

	Web 向け Workspace (ブラウザー)	StoreFront サ ービスサイト (ネイティブ)	StoreFront XenApp および XenDesktop サ イト (ネイティ ブ)	Citrix Gateway から Web 向け Workspace (ブラウザー)	Citrix Gateway から StoreFront サ ービスサイト (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		
セキュリティト ークン				はい *	はい *
2 要素認証 (ド メイン + セキュ リティトークン)				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 Plug-in)	はい (Citrix Gateway Plug-in)

\* 以下の環境でのみ利用可能:

- Workspace for Web サイト。
- Citrix Gateway が動作する環境 (デバイスへのゲートウェイプラグインソフトウェアのインストールは不要)。

注:

Citrix Gateway End-Point Analysis Plugin (EPA) は Citrix Workspace でサポートされています。ネイティブの Citrix Workspace アプリでは、nFactor 認証を使用する場合にのみサポートされます。詳しくは、Citrix ADC ドキュメントの「[nFactor 認証の要素として認証前および認証後の EPA スキャンを構成](#)」を参照してください。

Web Interface 5.4 への接続では、Citrix Workspace アプリで以下の認証方法がサポートされます:

注:

Web Interface では、「指定ユーザー」による認証がドメインおよびセキュリティトークン認証に相当します。

	Web Interface (ブラウザ)	Web Interface XenApp および XenDesktop サイト	Citrix Gateway から Web Interface (ブラウザ)	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 (ドメイン + セキュリティトークン)			はい *	
SMS			はい *	
スマートカード				
ユーザー証明書			はい (Citrix Gateway Plug-in が必要)	

#### 証明書

プライベート (自己署名) 証明書 以下の場合、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:

- プライベート証明書がリモートゲートウェイにインストールされている。
- 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。

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ことが原因で発生します。ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

手動でインストールした証明書 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 通信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した証明書プロファイルを信頼するには:

1. 証明書プロファイルがデバイス上にインストールされていることを確認します。
2. [設定] > [一般] > [情報] > [証明書信頼設定] の順に選択します。

プロファイルを介してインストールされた各ルート証明書は、[ルート証明書を全面的に信頼する] の下に表示されます。

3. 各ルート証明書に対して、信頼設定を切り替えることができます。

**iPad** および **iPhone** へのルート証明書のインポート 証明書の発行者のルート証明書を取得して、デバイスに構成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、ルート証明書をインポートするかどうかを確認するメッセージが表示されます。

ワイルドカード証明書 ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。Citrix Workspace アプリでは、ワイルドカード証明書がサポートされています。

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る場合は、中間証明書を Citrix Gateway (または Access Gateway) の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 のドキュメントの「[証明書のインストール、リンク、および更新](#)」で必要なセクションを参照してください。

RSA SecurID 認証は、Secure Gateway 構成 (Web Interface を使用する環境のみ) と、すべての Access Gateway 構成でサポートされています。

Citrix Workspace アプリでは、Access Gateway でサポートされるすべての認証方法がサポートされています。

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、サーバー証明書に関する厳格な検証ポリシーがあります。

### 重要

このバージョンの 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、ここで説明されているように正しく構成されていることを確認してください。以下の場合、接続できないことがあります：

- サーバーまたはゲートウェイの構成に間違ったルート証明書が含まれている
- サーバーまたはゲートウェイ構成にすべての中間証明書が含まれていない
- サーバーまたはゲートウェイ構成に期限切れまたは無効な中間証明書が含まれている
- サーバーまたはゲートウェイ構成にクロスルート用中間証明書が含まれていない

Citrix Workspace アプリは、サーバー証明書を検証するときにサーバー（またはゲートウェイ）が提供するすべての証明書を使用するようになりました。以前のリリース同様、Citrix Workspace アプリは、証明書が信頼済みかについても確認します。証明書が信頼済みでない場合、接続に失敗します。

このポリシーは、Web ブラウザーの証明書ポリシーより厳格です。多くの Web ブラウザーには、多数の信頼済みのルート証明書セットが含まれます。

サーバー（またはゲートウェイ）は、正しい証明書セットで構成する必要があります。不正な証明書のセットを使用すると、Citrix Workspace アプリの接続に失敗することがあります。

以下は、ゲートウェイがこのような有効な証明書で構成されていることを前提としています。この構成は、Citrix Workspace アプリで使用されるルート証明書を正確に確認するために、より厳格な検証が必要なユーザーにお勧めします：

- サーバー証明書サンプル
- 中間証明書サンプル
- ルート証明書サンプル

次に、Citrix Workspace アプリはこれらすべての証明書が有効であるかを確認します。Citrix Workspace アプリは、ルート証明書サンプルが既に信頼されているかどうかを検証します。

### メモ：

- Citrix Workspace アプリがルート証明書サンプルを信頼していない場合、接続に失敗します。
- 証明機関によっては、複数のルート証明書があります。より厳格な検証が必要な場合、構成で適切なルート証明書が使用されていることを確認してください。

たとえば、現在以下の 2 つの証明書があります：

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

これらの証明書は、同じサーバー証明書を検証できます。ユーザーデバイスによっては、両方のルート証明書が使用できます。その他のデバイスでは、1 つの証明書のみを使用できます (**DigiCert Baltimore Root/Baltimore CyberTrust Root**)。

ゲートウェイで **GTE CyberTrust Global Root** を構成すると、これらのユーザーデバイスで Citrix Workspace アプリの接続に失敗します。どのルート証明書を使用すべきかについては、証明機関のドキュメントを参照してください。また、ルート証明書の有効期限についても注意してください。

次に、Citrix Workspace アプリはこれら 2 つの証明書を使用します。アプリがユーザーデバイスでルート証明書を検索します。正しく検証できる証明書が見つかり、信頼済みである場合（ルート証明書サンプルなど）、接続は成功します。信頼済みの証明書が見つからない場合は、失敗します。

この構成では、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 アプリは任意の有効な、信頼済みのルート証明書を選択できます。

以下は、ゲートウェイがこのような証明書で構成されていることを前提としています：

- サーバー証明書サンプル
- 中間証明書サンプル
- 間違ったルート証明書

Web ブラウザーは、不正なルート証明書を無視することがありますが、Citrix Workspace アプリは不正なルート証明書を無視しないため、接続は失敗します。

証明機関によっては、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、以下のようにすべて中間証明書（ルート証明書ではない）で構成されます：

- サーバー証明書サンプル
- 中間証明書サンプル 1
- 中間証明書サンプル 2

#### 重要

証明機関によっては、クロスルート用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最新のルート証明書と同時に使用中の状況を想定しています。この場合、少なくとも 2 つの中間証明書が存在します。

たとえば、以前のルート証明書 **Class 3 Public Primary Certification Authority** には、関連するクロスルート用中間証明書 **Verisign Class 3 Public Primary Certification Authority - G5** があります。ただし、ルート証明書 **Verisign Class 3 Public Primary Certification Authority - G5** も利用可能であり、**Class 3 Public Primary Certification Authority** に置き換わります。最新のルート証明書はクロスルート用中間証明書を使用しません。

#### 注：

クロスルート用中間証明書とルート証明書のサブジェクト名（Issued To）は同じですが、クロスルート用中間証明書の発行者名（Issued By）は異なります。発行者名によって、クロスルート用中間証明書と通常の中間証明書（中間証明書サンプル 2 など）を区別できます。

通常は、このルート証明書およびクロスルート用中間証明書を省略した構成が推奨されます：

- サーバー証明書サンプル
- 中間証明書サンプル

クロスルート用中間証明書をゲートウェイで構成しないでください。これは、Citrix Workspace アプリによって以前のルート証明書が選択されるようになるのを避けるためです:

- サーバー証明書サンプル
- 中間証明書サンプル
- クロスルート用中間証明書サンプル (非推奨)

ゲートウェイでサーバー証明書のみを構成しないでください:

- サーバー証明書サンプル

このような場合、Citrix Workspace アプリはすべての中間証明書を検出できないため、接続に失敗します。

## インストールとアップグレード

November 8, 2023

Apple Store で Citrix Workspace アプリの最新バージョンをダウンロード、または最新バージョンに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て、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](#)で 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。

Citrix Workspace アプリで使用できる機能について詳しくは、[Citrix Workspace アプリの機能マトリックス](#)を参照してください。

## 開始

March 27, 2024

### セットアップ

iOS 向け Citrix Workspace アプリは Citrix Virtual Apps 環境向けの Web Interface の構成をサポートします。Web Interface サイトには 2 つの種類があります:

- XenApp および XenDesktop サイト
- Citrix Virtual Apps and Desktops および Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) サイト。

これらの Web Interface サイトにより、クライアントデバイスがサーバーファームに接続できるようになります。iOS 向け Citrix Workspace アプリと Web Interface サイト間での認証は、Citrix Secure Web Gateway など、さまざまな方法で実装できます。

また、StoreFront が Citrix Workspace アプリへの認証およびリソース配信を提供するように構成できます。この構成では、デスクトップ、アプリケーション、およびそのほかのリソースをユーザーに配信する一拠点のエンタープライズリソースストアを作成することもできます。

接続の構成については、<http://community.citrix.com>を参照してください。ビデオ、ブログ、サポートフォーラムなどを利用できます。

Citrix Virtual Apps and Desktops および Citrix DaaS の展開環境で公開されているアプリケーションにユーザーがアクセスできるようにするには、以下のコンポーネントを構成する必要があります。

- アプリケーションを公開するときは、StoreFront のストアを経由して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、次のオプションについて検討します。
  - 公開アプリケーションを簡単に識別できるように、わかりやすい説明を入力したことを確認します。この説明は、ユーザーの Citrix Workspace アプリに表示されます。
  - 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できます。[おすすめ] 一覧の下にアプリケーションを一覧表示できます。この一覧を Citrix Workspace アプリに追加するには、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。「KEYWORDS: Featured」という文字列を **Application description** フィールドの値に追加できるようになりました。
  - アプリケーションの表示サイズをモバイルデバイスの画面サイズに合わせる機能を有効にするには、サーバー上でその公開アプリケーションのプロパティを編集し、[説明] ボックスに文字列「KEYWORDS:mobile」を追加します。このキーワードの追加により、そのアプリケーションでの自動スクロール機能も有効になります。
  - アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、Citrix Virtual Apps でその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、そのアプリケーションを手動でサブスクライブしなくても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、作成します。サイト名およびその作成方法は、インストールしている Web Interface のバージョンにより異なります。

### 手動セットアップ

通常、Citrix Workspace アプリで Citrix Gateway に接続すると、認証の後で XenApp および XenDesktop サイトまたは Citrix Virtual Apps Web サイトが検出されます。サイトが検出されない場合、iOS 向け Citrix Workspace

アプリはエラーを表示します。この問題を避けるには、iOS 向け Citrix Workspace アプリが正しく Citrix Gateway に接続されるように、手作業でアカウントを構成します。

1. アカウントアイコン > アカウント画面 > プラス記号 (+) の順にタップします。[新規アカウント] 画面が開きます。
2. 画面左下の [オプション] の左側のアイコンをタップして、[手動セットアップ] をタップします。画面に他のフィールドが表示されます。
3. [アドレス] フィールドに、サイトまたは Citrix Gateway の URL (`agee.mycompany.com`など) を入力します。
4. 次のいずれかの接続オプションを選択します。選択するオプションにより、画面に表示されるフィールドが変わります。
  - **Web Interface** - Citrix Workspace アプリで Citrix Virtual Apps Web サイトを表示する場合は、このオプションを選択します。この UI は、「Web ビュー」とも呼ばれます。
  - **XenApp Services** - Citrix Gateway 経由の認証が構成されていない特定の XenApp および XenDesktop サイトを指定する場合、iOS 向け Citrix Workspace アプリにはこのオプションを選択します。追加されるフィールドに、ログオン用の資格情報を入力します。
    - <StoreFront FQDN>: 複数のストアがある場合は一覧が表示され、追加するストアをユーザーが選択できます。
    - <StoreFront FQDN>/citrix/<Store Name>: <Store Name> に指定する StoreFront のストアが追加されます。
    - <StoreFront FQDN>/citrix/PnAgent/config.xml: 従来の既定の PNAgent ストアが追加されます。
    - <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: <Store Name> に関連付けられている従来の PNAgent ストアが追加されます。
  - Citrix Gateway - 特定の Citrix Gateway 経由で XenApp および XenDesktop サイトに接続する場合、iOS 向け Citrix Workspace アプリにはこのオプションを選択します。追加されるオプションでサーバーのエディションを選択し、ログオン用の資格情報、セキュリティトークンを使用するかどうかなどを指定します。
5. [証明書の警告を無視] で、無効、自己署名、または期限切れの証明書を無視してサーバーに接続するかどうかを指定します。デフォルトでは、[オフ] になっています。

重要: このオプションをオンにする場合は、常に接続先のサーバーが正しいかどうかを確認してください。ユーザーのデバイスを不正な攻撃から守るため、Citrix ではすべてのサーバー上に有効な証明書をインストールしておくことを強くお勧めします。証明機関から入手した SSL 証明書を使用すると、サーバーのセキュリティが向上します。自己署名入りの証明書を使用したり、証明書を使用しなかったりすることは Citrix では推奨されません。
6. [保存] をタップします。
7. ユーザー名およびパスワード (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。iOS 向け Citrix Workspace アプリの画面が開き、デスクトップにアクセスしたり、アプリを追加および実行したりできます。

## StoreFront

**重要:**

- StoreFront を使用すると、iOS 向け Citrix Workspace アプリは Citrix Access Gateway Enterprise Edition 9.3 以降および Citrix Gateway 13 以前をサポートします。
- iOS 向け Citrix Workspace アプリでは、Web Interface の XenApp および XenDesktop サイトがサポートされます。
- iOS 向け Citrix Workspace アプリは、Web ブラウザーが Workspace for Web と連携している限り、セッションの開始をサポートします。セッションが開始しない場合、iOS 向け Citrix Workspace アプリを介して直接アカウントを構成します。ユーザーは Citrix Workspace のブラウザを開く機能を使って手動で ICA ファイルを開く必要があります。この展開方法で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 で作成するストアは、iOS 向け Citrix Workspace アプリのリソース配信インフラストラクチャと認証を提供するサービスにより構成されます。以下からデスクトップとアプリケーションを集計するストアを作成します。

- Citrix Virtual Apps and Desktops および Citrix 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。詳しくは、[StoreFront](#)の製品ドキュメントを参照してください。iOS 向け Citrix Workspace アプリダウンロードサイトを独自に作成する管理者用に、テンプレートが提供されています。
  2. Citrix Virtual Apps and Desktops および Citrix DaaS のアプリケーションと同様の手順で、StoreFront 用にストアを構成します。ユーザーのモバイルデバイス側で特別な構成を行う必要はありません。詳しくは、製品ドキュメントの「StoreFront」のセクションで、「ユーザーアクセスオプション」を参照してください。以下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。管理者は、ストアに接続するための詳細が定義されたプロビジョニングファイル (.cr) をユーザーに提供します。デバイスにインストールした後で、提供されたファイルをユーザーが開くと iOS 向け Citrix Workspace アプリが自動的に構成されます。Web 向け Workspace のサイトは、デフォルトではそのサイトの単一ストア用のプロビジョニングファイルがユーザーに提供されます。または、管理者が Citrix StoreFront 管理コンソールで単一の、または複数のストア用のプロビジョニングファイルを生成して、それらをユーザーにメールなどで配布することもできます。
    - 手動構成。デスクトップやアプリケーションにアクセスするには、Citrix Gateway またはストア URL が必要であることをユーザーに直接知らせることができます。Citrix Gateway を経由する接続の場合、ユーザーは製品のエディションと必要な認証方法についても把握する必要があります。インストール後、Citrix Workspace アプリにこれらの詳細を入力し、接続が検証され成功すると、サインインを求められます。
    - 自動構成。ようこそ画面で [アカウントの追加] をタップして、アドレスフィールドに StoreFront サーバーの URL を入力します。追加中、アカウントは自動的に構成されます。

## 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は、Citrix Gateway を使用して認証を構成します。たとえば、リモートの場所からインターネットで接続するユーザーです。

- StoreFront を使用すると、iOS 向け Citrix Workspace アプリは Citrix Access Gateway Enterprise Edition 9.3 以降および Citrix Gateway 13 以前をサポートします。

## Web Interface

Web Interface サイトを設定する場合、iPhone および iPad のユーザーは、デバイスの Safari ブラウザーで Web Interface サイトに接続してアプリケーションを起動します。管理者は、ほかの Citrix Virtual Apps アプリケーションと同じ方法で Web Interface サイトを設定できます。モバイルデバイス用に XenApp および XenDesktop サイトが設定されていない場合、iOS 向け Citrix Workspace アプリは自動的に Web Interface サイトに接続されます。ユーザーのモバイルデバイス側で特別な構成を行う必要はありません。

デバイスの Safari ブラウザーでは、Web Interface 5.x がサポートされています。

## iOS デバイス上でアプリケーションを起動するには

ユーザーデバイスで、通常の資格情報を入力して Web Interface サイトにログオンします。

## モバイルデバイスの自動プロビジョニング

StoreFront で、ストアで使用される Citrix Gateway 環境やビーコンポイントなどの詳細情報が定義されたプロビジョニングファイルを生成するには、[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] タスクを使用します。ユーザーにプロビジョニングファイルを提供すると、ユーザーが iOS 向け Citrix Workspace アプリを簡単に構成できるようになります。iOS 向け Citrix Workspace アプリのプロビジョニングファイルは、Workspace for Web サイトから入手できるようにすることもできます。

### 重要:

複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上で Citrix StoreFront 管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windows の [スタート] 画面または [アプリ] 画面で、[Citrix StoreFront] タイルをクリックします。Citrix StoreFront 管理コンソールの左ペインで [ストア] ノードを選択します。
2. 複数のストアの詳細情報が定義されたプロビジョニングファイルを生成するには、[操作] ペインの [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] をクリックして、対象のサイトを選択します。
3. [エクスポート] をクリックして、拡張子が `.cr` のプロビジョニングファイルをネットワーク上の適切な場所に保存します。

### ユーザーのアクセス情報

管理者は、ユーザーに iOS 向け Citrix Workspace アプリアカウントの情報を提供します。ユーザーは、この情報を使用してアプリケーション、デスクトップ、およびデータにアクセスします。次の方法でユーザーに情報を提供できます：

- メールアドレスによるアカウント検出の構成
- ユーザーにプロビジョニングファイルを提供する
- アカウント情報をユーザーに手入力させる

### メールアドレスによるアカウント検出を構成する

管理者は、メールアドレスによる iOS 向け Citrix Workspace アプリアカウントの検出機能を構成できます。この機能を有効にした場合、ユーザーは iOS 向け Citrix Workspace アプリの初期設定時にサーバーの URL の代わりに自分のメールアドレスを入力できます。DNS (Domain Name System) サービス (SRV) レコードにより、そのメールアドレスに関連付けられている Access Gateway または StoreFront のサーバー、または Endpoint Management 仮想アプライアンスが Citrix Workspace アプリにより自動的に検出され、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のログオンを求めるメッセージが表示されます。

#### 注：

iOS 向け Citrix Workspace アプリで Web Interface に接続する環境では、メールアドレスによるアカウント検出がサポートされません。

**DNS** サービスの場所 (**SRV**) レコードを追加して、メールアドレスによる検出を有効にする 初期構成時に、Citrix Workspace アプリは Active Directory DNS (Domain Name System: ドメイン名システム) 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。つまり、ユーザーが iOS 向け Citrix Workspace アプリをインストールして構成するときに、ストアのアクセスの詳細を知っている必要はありません。代わりに、ユーザーがメールアドレスを入力すると、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。

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検索するために、Citrix Workspace アプリを有効にするには：

- Access Gateway のサービスローケーション (SRV) ロケーターリソースレコードを構成する。
- DNS サーバーで StoreFront または App Controller 接続を構成する。

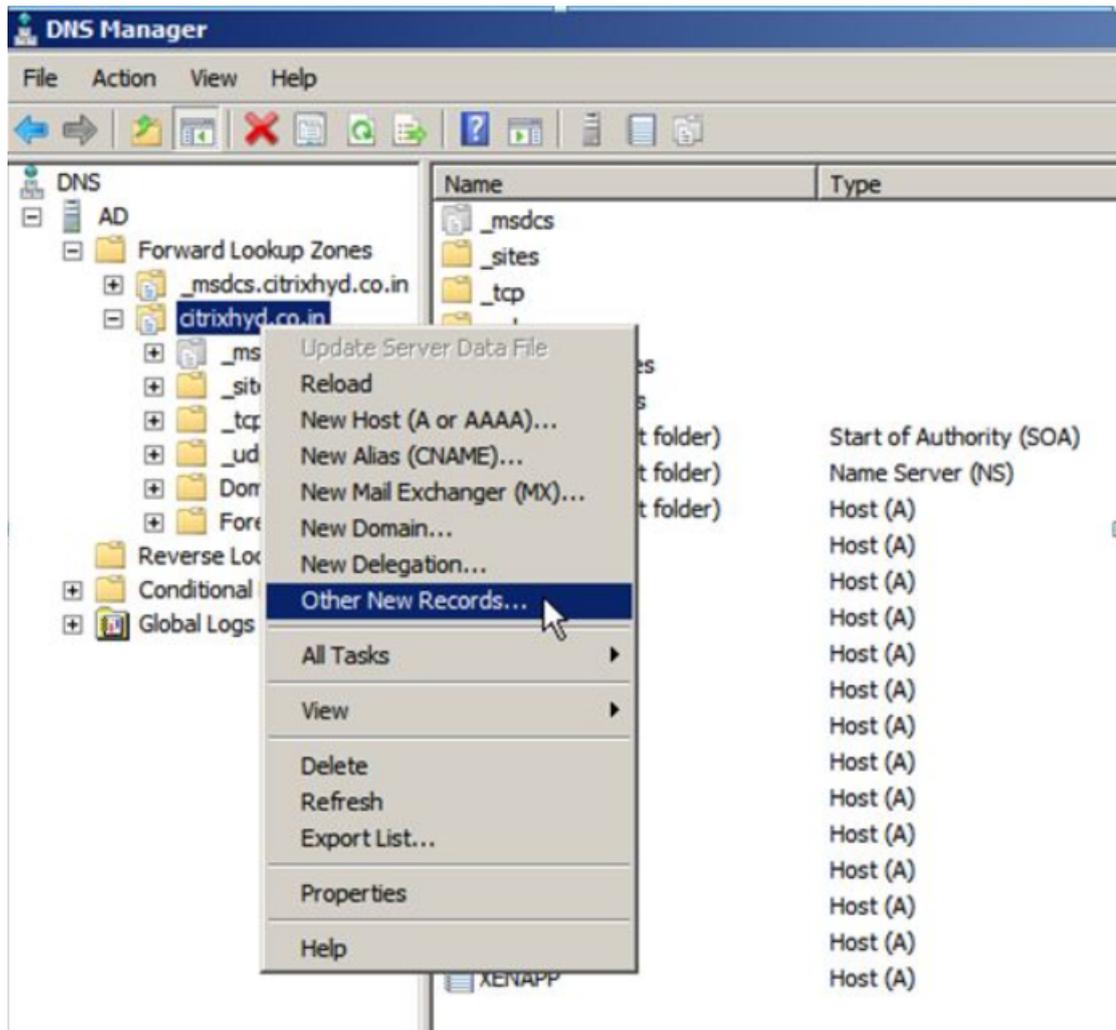
メールアドレスによるアカウント検出を有効にするには、Access Gateway アプライアンスおよび StoreFront または AppController サーバー上に有効なサーバー証明書をインストールする必要があります。また、ルート証明書へのチェーンのすべてが有効である必要があります。最高のユーザーエクスペリエンスのためには、次のいずれかの証明書をインストールします：

- Subject

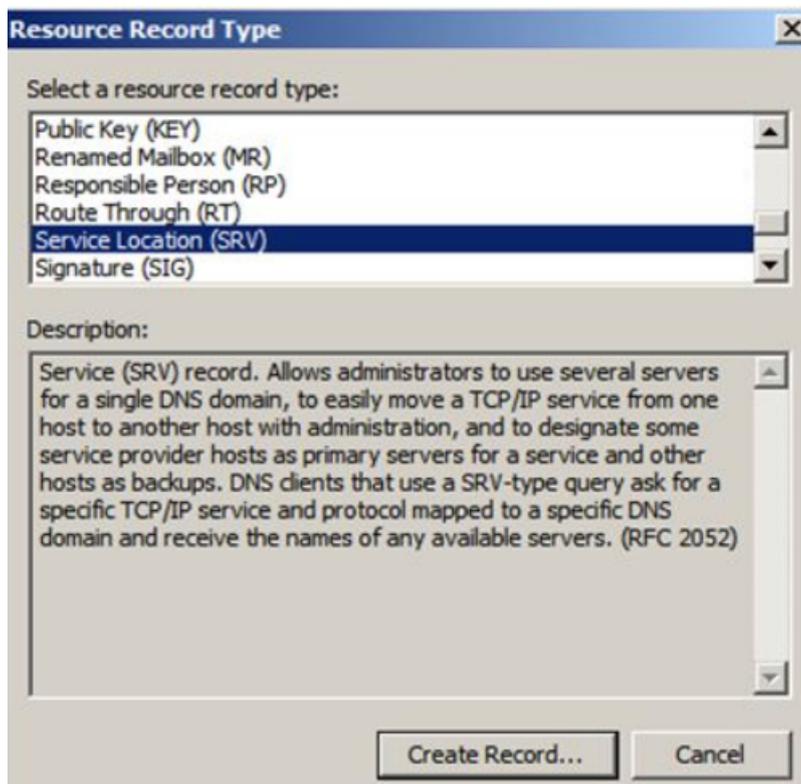
- *discoverReceiver.domain* の Subject Alternative Name エントリ。
- ユーザーのメールアカウントを含むドメインのワイルドカード証明書。

ユーザーがメールアドレスを使用して iOS 向け Citrix Workspace アプリ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 サーバーにログインします。
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] 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しているホスト] で、Access Gateway アプライアンス（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場合）、または StoreFront か AppController のサーバー（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場合）の完全修飾ドメイン名（FQDN）とポートを指定します。
12. [OK] をクリックします。

注:

StoreFront FQDN は一意で、Access Gateway の仮想サーバーの FQDN とは異なる必要があります。StoreFront と Access Gateway 仮想サーバーに同じ FQDN を使用することはサポートされていません。Citrix Workspace アプリでは、内部ネットワークに接続されたユーザーデバイスからのみ解決できる一意の StoreFront FQDN アドレスである必要があります。それ以外の場合、Citrix Workspace アプリのユーザーは、メールアドレスによるアカウントの検出機能を使用できません。

#### ユーザーにプロビジョニングファイルを提供する

管理者は、StoreFront を使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、iOS 向け Citrix Workspace アプリを自動的に構成できるようにします。デバイスに iOS 向け Citrix Workspace アプリをインストールした後で、提供された .cr ファイルをユ

ユーザーが開くと iOS 向け Citrix Workspace アプリが自動的に構成されます。Workspace for Web サイトを構成する場合は、そのサイトからユーザーに iOS 向け Citrix Workspace アプリのプロビジョニングファイルを提供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。

### アカウント情報をユーザーに手入力させる

ユーザーにアカウント情報を入力させる場合は、ホストされるデスクトップに接続できるように以下の情報を提供する必要があります：

- StoreFront URL またはリソースをホストしている XenApp および XenDesktop サイト (`servername.company.com`など)。
- Citrix Gateway を使用する場合は、そのアドレスと認証方法。

ユーザーが新しいアカウントの詳細を入力すると、Citrix Workspace アプリにより接続が検証されます。検証に成功すると、そのアカウントにログオンするための画面が iOS 向け Citrix Workspace アプリで開きます。

## Citrix Workspace アプリの構成

March 27, 2024

この記事では、iOS 向け Citrix Workspace アプリの構成に役立つタスクについて説明します。

### フィーチャーフラグ管理

実稼働環境の Citrix Workspace アプリで問題が発生した場合、影響を受ける機能を Citrix Workspace アプリで動的に無効にすることができます。機能が出荷された後でも、無効にできます。この場合、フィーチャーフラグと、LaunchDarkly と呼ばれるサードパーティ製サービスを使用します。ファイアウォールまたはプロキシが送信トラフィックをブロックしている場合を除いて、LaunchDarkly へのトラフィックを有効にするために構成する必要はありません。送信トラフィックがブロックされている場合、ポリシー要件に応じて、特定の URL または IP アドレス経由の LaunchDarkly へのトラフィックを有効にします。

LaunchDarkly へのトラフィックと通信は、次の方法で有効化できます：

次の **URL** へのトラフィックを有効にする

- [app.launchdarkly.com](https://app.launchdarkly.com)
- [events.launchdarkly.com](https://events.launchdarkly.com)

- [stream.launchdarkly.com](https://stream.launchdarkly.com)
- [clientstream.launchdarkly.com](https://clientstream.launchdarkly.com)
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- [mobile.launchdarkly.com](https://mobile.launchdarkly.com)

#### IP アドレスの許可リストを作成する

IP アドレスの許可リストを作成する必要がある場合、現在のすべての IP アドレス範囲については、「[LaunchDarkly のパブリック IP 一覧](#)」を参照してください。この一覧を使用すると、インフラストラクチャの更新に合わせてファイアウォールの構成が自動的に更新されます。インフラストラクチャの変更の状態について詳しくは、[LaunchDarkly Statuspage](#)を参照してください。

#### LaunchDarkly のシステム要件

Citrix ADC の分割トンネリングが以下のサービスに対して [オフ] に設定されている場合、アプリがこれらのサービスと通信できることを確認する必要があります：

- LaunchDarkly サービス
- APNs リスナーサービス

#### LaunchDarkly サービスを無効にするプロビジョニング：

オンプレミスストアとクラウドストアの両方で LaunchDarkly サービスを無効にすることができます。

クラウド環境では、enableLaunchDarkly 属性を False に設定することにより、LaunchDarkly サービスを無効にすることができます。これは、Global App Configuration Service の UI で実行できます。

```
1 {
2
3     "assignedTo": [
4         "AllUsersNoAuthentication"
5     ],
6     "category": "Third Party Services",
7     "settings": [
8         {
9
10            "name": "Enable Launch Darkly",
11            "value": "true"
12        }
13    ],
14    "userOverride": false
15 }
16 }
17
18 <!--NeedCopy-->
```

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

オンプレミスの展開で、次の手順を実行します：

1. テキストエディターを使って web.config ファイルを開きます。このファイルは通常、`C:\inetpub\wwwroot\Citrix\Roaming`ディレクトリにあります。
2. このファイルで、ユーザーアカウント要素の場所を見つけます（「Store」は使用環境のアカウント名です）。

例: `<account id=... name="Store">`

タグの前に、ユーザーアカウントのプロパティに移動します：

```
1 <properties>
2 <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. enableLaunchDarkly タグを追加し、値を false に指定します。
4. enableLaunchDarkly タグを追加し、値を false に指定します。

```
<property name="enableLaunchDarkly" value="false"/>
```

注：

ほとんどの機能は、LaunchDarkly によって制御される機能フラグの背後にあります。この機能が無効になっている環境では、少なくとも 90 日間待つ必要があります。

## 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。タイムアウト値に達した後、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 アプリ構成のための PowerShell モジュールをダウンロードするには、[こちら](#)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の種類に応じて、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：

- 非アクティブタイムアウトの後、Citrix Workspace アプリに再度アクセスするための生体認証を行うよう求める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は、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 アプリを引き続き使用するには、認証する必要があります。

パスコードが iOS で構成されていない場合は、非アクティブタイムアウト後に資格情報を使用してサインインする必要があります。

注:

この機能は、Workspace (Cloud) の顧客のみに適用されます。

### カスタマーエクスペリエンス向上プログラム (CEIP)

収集データ	説明	使用目的
構成および使用状況データ	Citrix カスタマーエクスペリエンス向上プログラム (CEIP) では、iOS 向け Citrix Workspace アプリの構成および使用状況データが収集され、Google Firebase に自動的に送信されます。	このデータは、Workspace アプリの品質、信頼性、およびパフォーマンスを向上させる目的で Citrix によって使用させていただきます。

#### 追加情報

Citrix は、お客様のデータを Citrix との契約条件に従って処理します。データは、[Citrix サービスのセキュリティに関する別紙](#)での指定に従って保護されています。詳しくは、「[Citrix Hypervisor Center](#)」を参照してください。

Citrix は、CEIP の一環として、Google Firebase を使用して Citrix Workspace アプリから特定のデータを収集します。[Google Firebase のために収集されたデータの Google の取り扱い方法](#)について確認してください。

Citrix および Google Firebase への CEIP データの送信を停止するには:

1. iOS 向け 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ます。
4. [使用統計の送信] オプションを無効にします。

注:

欧州連合 (EU)、欧州経済領域 (EEA)、スイス、および英国 (UK) のユーザーのデータは収集されません。

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	認証の種類と認証構成	ICA 接続
-------------------	------------------	------------	--------

HDX セッションの起動	ストアアプリセッション	WebView アクションを開く	WebView アクションのコピー
WebView アクションの共有	Workspace アプリのレビュー	接続の状態、接続エラー、コネクションセンターの使用	外部ディスプレイ
ソケットの状態	セッションの実行時間	HDX over UDP	セッションの起動時間
デバイス情報	デバイスモデル情報	使用統計の送信	アプリ言語、ワークスペースアプリ言語
キーボード言語	Citrix ストアの種類	Citrix ストアの組み合わせ	ストアプロトコルの種類
ストア数	HDX UDP の状態	RSA トークンのインストール	

#### 既知の制限事項

- VDA 7.18 以前の場合、ワークスペースハブにキャストするには、使用するデスクトップまたはその他のリソースで H.264 の全画面ポリシーが有効、および従来のグラフィックモード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 アプリアカウントからログオフした場合でも、リモートセッションから切断またはログオフできます。

- 切断: アカウントからログオフされますが、Windows アプリケーションやデスクトップはサーバー上で実行されたままになります。ほかのデバイス上の iOS 向け Citrix Workspace アプリからこのセッションに再接続すると、切断時の状態から作業を続行できます。このオプションにより、ユーザーがほかのデバイスに移動して、作業を続行できるようになります。
- 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終了します。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て、アカウントからログオフできます。iOS 向け 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

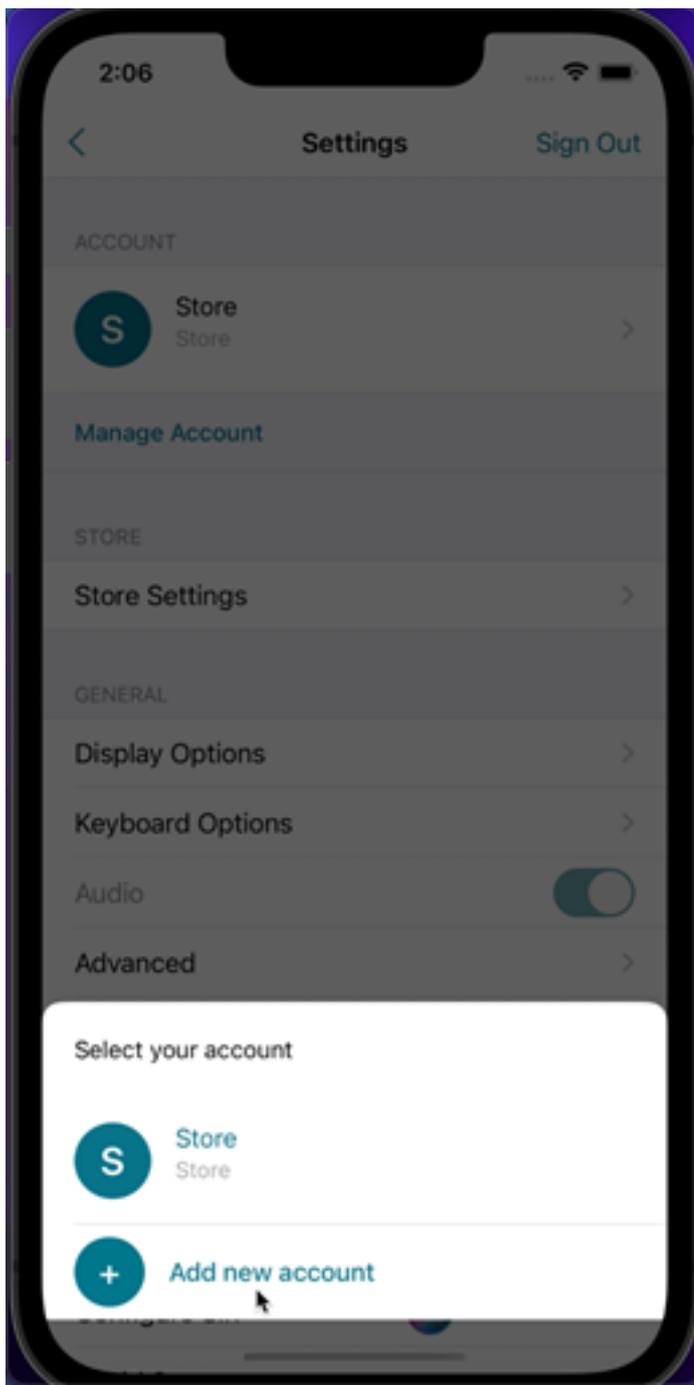
アクセス場所に関係なく、組織がホストする Web、SaaS アプリ、および Web サイトにアクセスできます。この機能は、クラウドストアのお客様のみが使用できます。

## 複数のクラウドストアをサポート

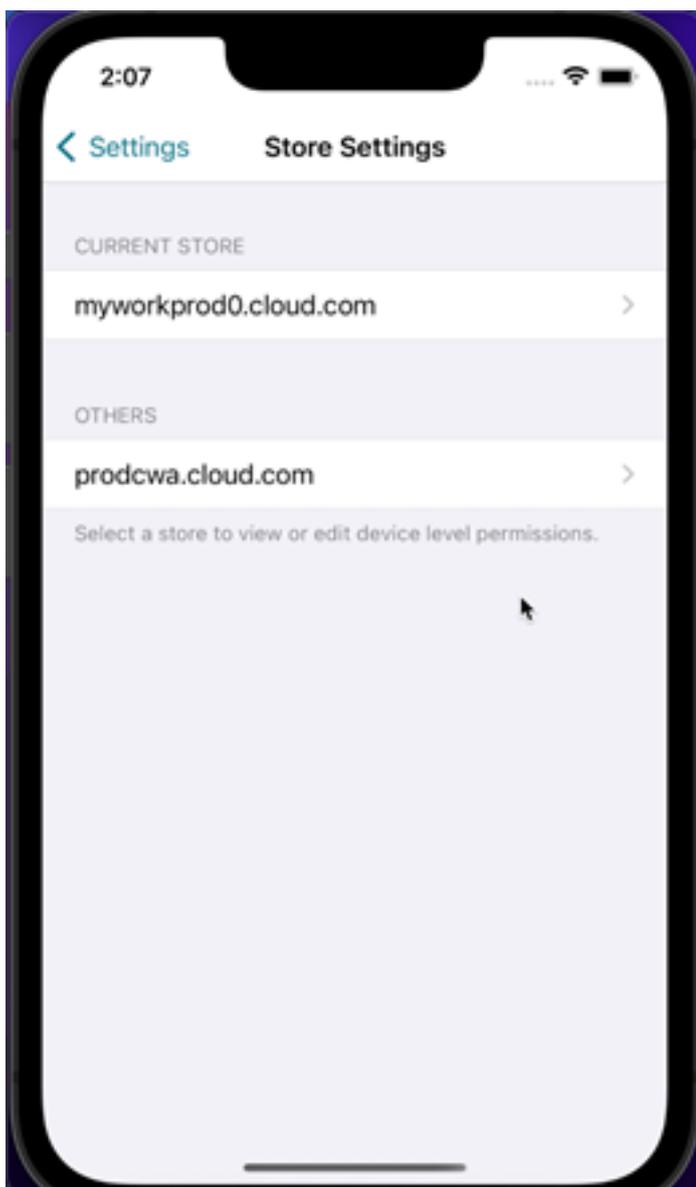
24.1.0 リリース以降、iOS および iPadOS 向け Citrix Workspace アプリに複数のクラウドストアアカウントを追加できます。エンドユーザーが簡単に複数のストアを追加したり、切り替えたりできるようになりました。この機能により、複数のストアにアクセスするときのユーザー エクスペリエンスが向上します。

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一覧のダイアログが開きます。
2. [新しいアカウントの追加] 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。スマートカードを使ってログオンする場合は、[スマートカードの使用] をタップします。
4. [続行] をタップします。[サインイン] ダイアログボックスに、ユーザー名、パスワード、パスコードのフィールドが表示されます。
5. 情報を入力します。フィールドについて詳しくは、IT 管理者に連絡してください。
6. [サインイン] をタップします。これで新しいアカウントがセットアップされました。



### ストア **URL** の自動入力

名称変更された iOS 向け Citrix Workspace アプリにアクセスする場合、ストア URL の自動入力を選択できます。この機能により、手動による介入が減り、アプリへの迅速なアクセスが提供されます。アプリの個人設定について詳しくは、「[App Personalization](#)」を参照してください。

### 複数のストアを一度に削除するためのサポート

バージョン 24.2.0 以降、iOS 向け Citrix Workspace アプリでは、複数のストアの選択と削除がサポートされています。この機能により、複数のストアで作業する場合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。

[Stores] 画面から複数のストアを一度に削除するには、次の手順を実行します：

1. [Stores] 画面で、[Select] 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、[Select All] をタップします。
3. [Delete] をタップします。

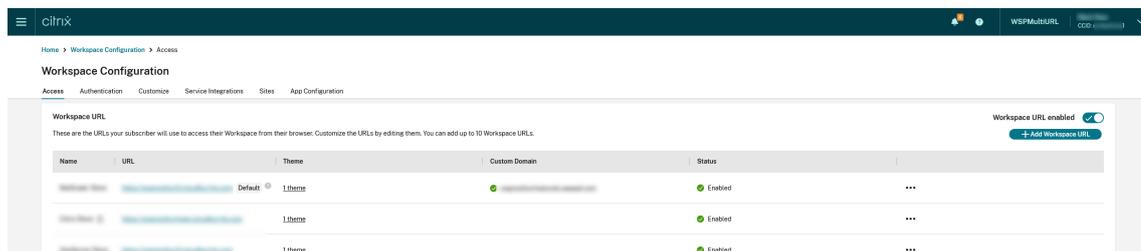
ユーザーのストア名の変更に関する管理者による制限をサポート

以前は、ユーザーは [Edit Account] オプションを使用してストア名を変更できました。

24.2.0 以降、iOS 向け Citrix Workspace アプリでは、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が管理者に提供されます。この機能を使用すると、管理者はストア名の一貫性を簡単に確認して維持できます。

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：

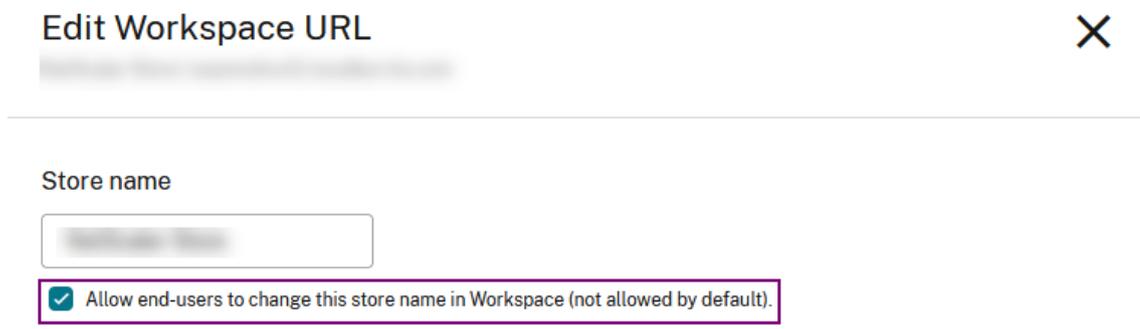
1. 資格情報でCitrix Cloudにサインインします。
2. [ワークスペース構成] > [アクセス] に移動します。[ワークスペース URL] の下に、既存のストア URL の一覧が表示されます。



3. エンドユーザーにストア名の変更を許可する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。



5. [ワークスペース 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できるようにする (デフォルトでは許可されていません)] を選択します。



Store name

Allow end-users to change this store name in Workspace (not allowed by default).

6. [保存] 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、ストア名を更新するときに手動での操作の必要がなくなり、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。

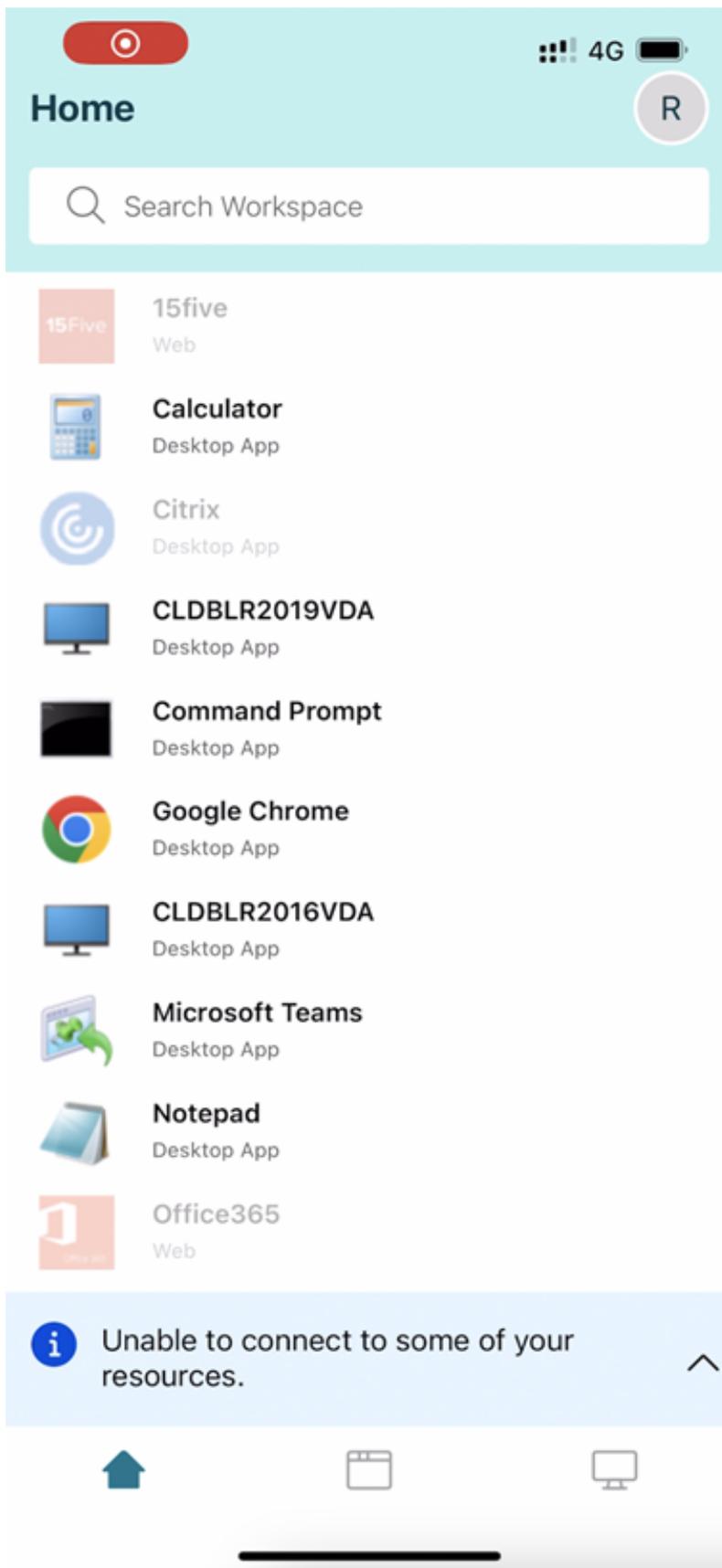
#### エンドユーザー状況監視の機能強化

EUEM (End User Experience Monitoring: エンドユーザー状況監視) のクライアント開始メトリックがサポートされるようになりました。EUEM は、非常に詳細なセッション状況監視データをリアルタイムで収集するのに役立ちます。データが Director ダッシュボードに送信されるため、管理者はユーザーエクスペリエンスを監視できます。データは、VDA 上のセッション状況監視サービス (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開始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実行時間。
- セッション作成時のクライアントの実行時間。セッション作成時のクライアントの実行時間は、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た瞬間から接続が確立されるまでの時間です。
- セッション検索時のクライアントの実行時間。セッション検索時のクライアントの実行時間は、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。この照会処理は既存のセッションでアプリケーションの起動要求を処理できるかどうかを判断するために、クライアント上で実行されます。
- ICA 往復時間の Citrix によるリアルタイム記録。ICA RTT と呼ばれる。ICA RTT は、ユーザーがキーを押してからエンドポイントに応答が表示されるまでの経過時間です。

### 強化された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

24.1.0 リリース以降、iOS 向け Citrix Workspace アプリのユーザーインターフェイスが強化され、洗練され、さらに詳細な情報を表示するようになり、Citrix Workspace の停止時にユーザーフレンドリーなエクスペリエンスを提供します。オフラインモードに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、アプリやデスクトップの結果で一致に近いテキストや、検索語のスペルミスを見つけることができます。サービス継続性機能について詳しくは、「[サービス継続性](#)」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を使用した **Citrix Workspace** アプリの構成

April 17, 2024

iOS 向け Citrix Workspace アプリは、統合エンドポイント管理 (UEM) ソリューションを使用した AppConfig ベースのキー値ペアによる Workspace アプリの管理者構成をサポートするようになりました。

### 構成方法

統合エンドポイント管理ソリューションを使用して Workspace ストア 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 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. 統合エンドポイント管理 (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することができます。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. キーと値のペアを XML プロパティ一覧に追加し、次の値を入力します：
  - キー: `url`
  - 値の種類: `String`
  - 値: ストア URL (例: `prodcwa.cloud.com`)

#### Settings [Edit](#)

Configuration key	Value type	Configuration value
<code>url</code>	<code>String</code>	<code>prodcwa.cloud.com</code>

### 制限事項

- クラウドストアが既に設定されていて、管理者が新しいクラウドストアを構成する場合、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の関連するデータや設定も削除されます。Citrix Workspace で通知を受け取ります。その場合、再度サインインして、新しいクラウドストアが Citrix Workspace に追加されるようにする必要があります。

- 上記の説明は、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既に構成されていて、管理者が新しいクラウドまたはオンプレミスストアを構成する場合、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

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 アプリを構成するいくつかの構成をサポートしています。以前は、管理者がストア 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 を変更し、アプリの表示方法を制御することを制限できるようになりました。

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	値の種類	構成値
<code>url</code>	<code>String</code>	ストア URL。例： <code>prodcwa.cloud.com</code>
<code>storeType</code>	<code>Integer</code>	- (既定値) 1 に設定すると、ユーザーはネイティブの、またはデフォルトのストアの読み込み内容を表示できます。-2 に設定すると、ユーザーは Web Interface 内でストアを表示できます。
<code>restrict_user_store_modification</code>	<code>Boolean</code>	<ul style="list-style-type: none"> <li>• <b>true</b> に設定すると、ユーザーはストアを変更（追加、削除、または編集）できません。</li> <li>- <b>false</b> に設定すると、ユーザーはストアを変更できます。</li> </ul> 注：フラグが true に設定されている場合、UEM 構成ストアを追加する前に、すべての既存のストアが削除されます。

## UEM を介したデバイス名の構成をサポート

24.3.5 バージョン以降、iOS 向け Citrix Workspace アプリでは、管理者が統合エンドポイント管理 (UEM) 経由で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した。

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：

説明のために、この例では 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することができます。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. キーと値のペアを XML プロパティ一覧に追加し、次の値を入力します：

- キー： deviceName
- 値の種類： 文字列
- 値： デバイスの名前（例： MY\_IPHONE\_Device）

Configuration key	Value type	Configuration value
url	String	prodca.cloud.com ...
deviceName ✓	String ▼	MY_IPHONE_DVICE ✓ ...
	Select one ▼	

## 周辺機器

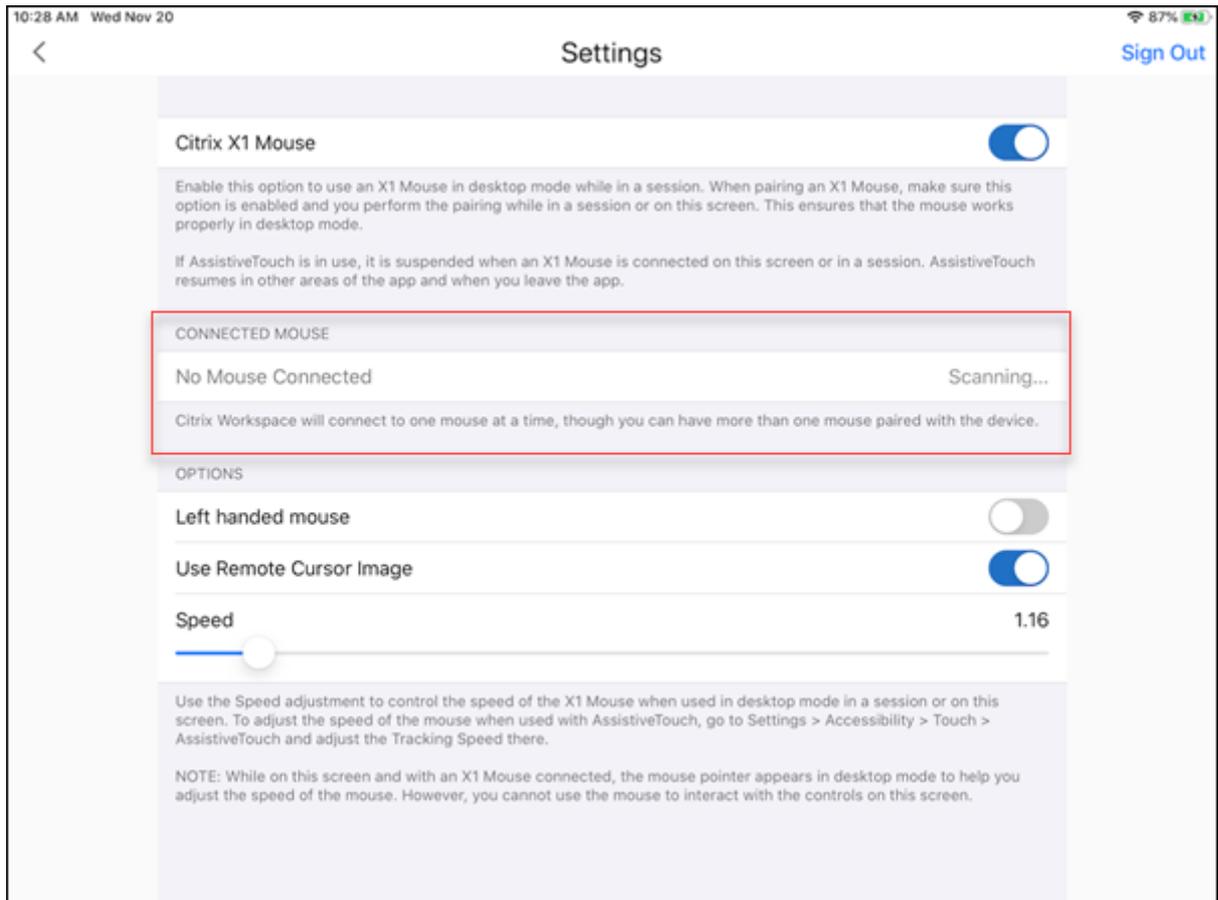
July 1, 2024

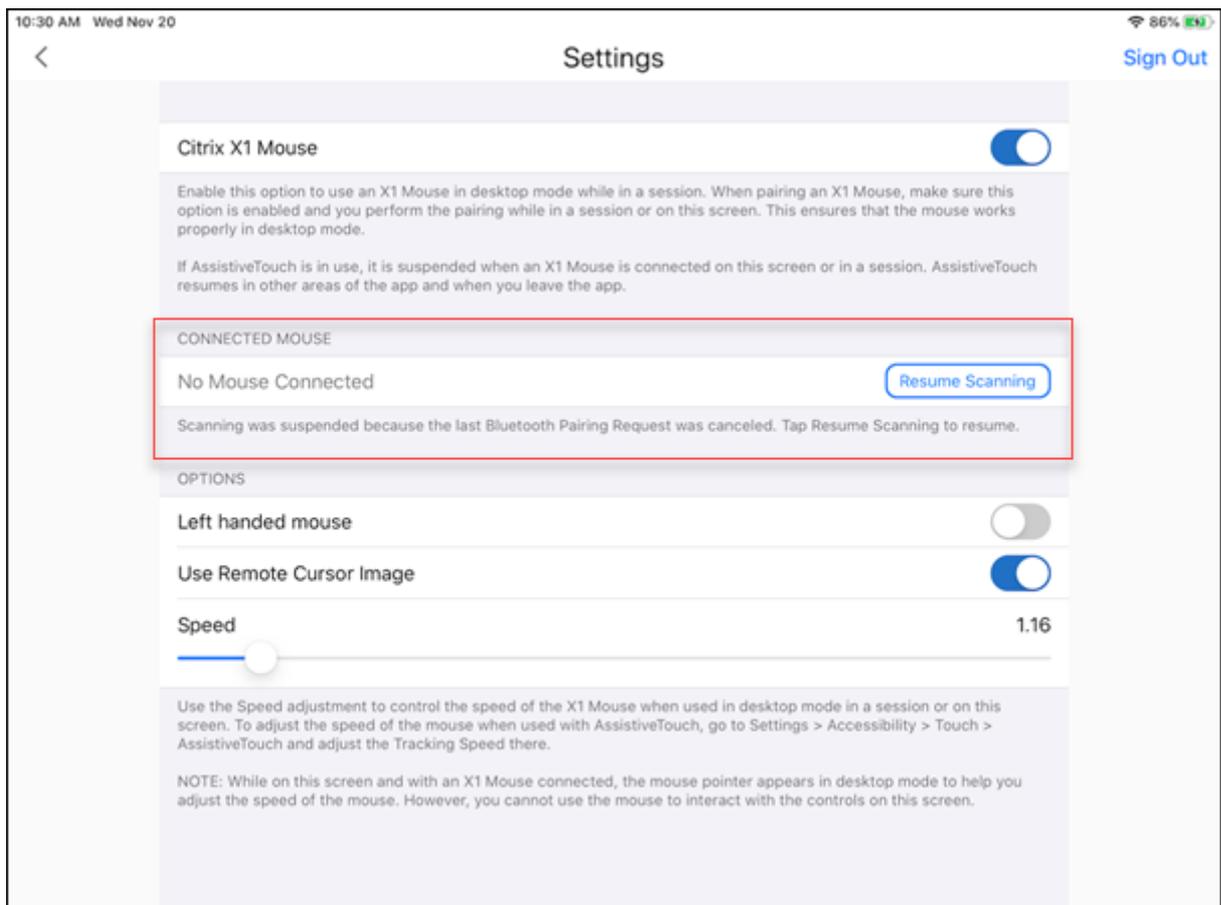
## Citrix X1 Mouse

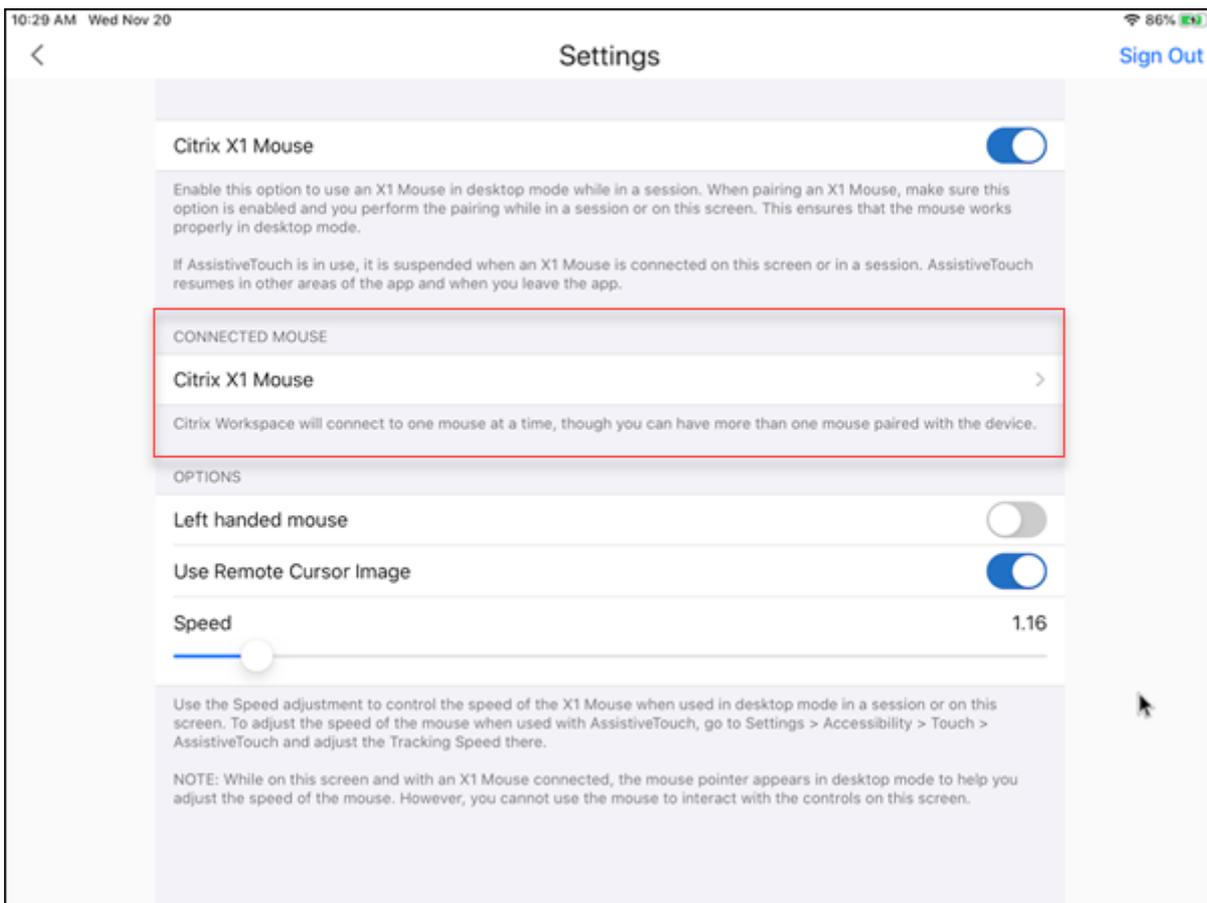
### Citrix X1 Mouse のペアリングと接続の状態

この機能を使用すると、Citrix X1 Mouse のペアリングプロセスをより細かく制御できます。[設定] 画面では、次の操作を実行できます：

- Citrix X1 Mouse のペアリング。セッション中に Citrix X1 Mouse をペアリングすることもできます。
- 接続状態の表示。



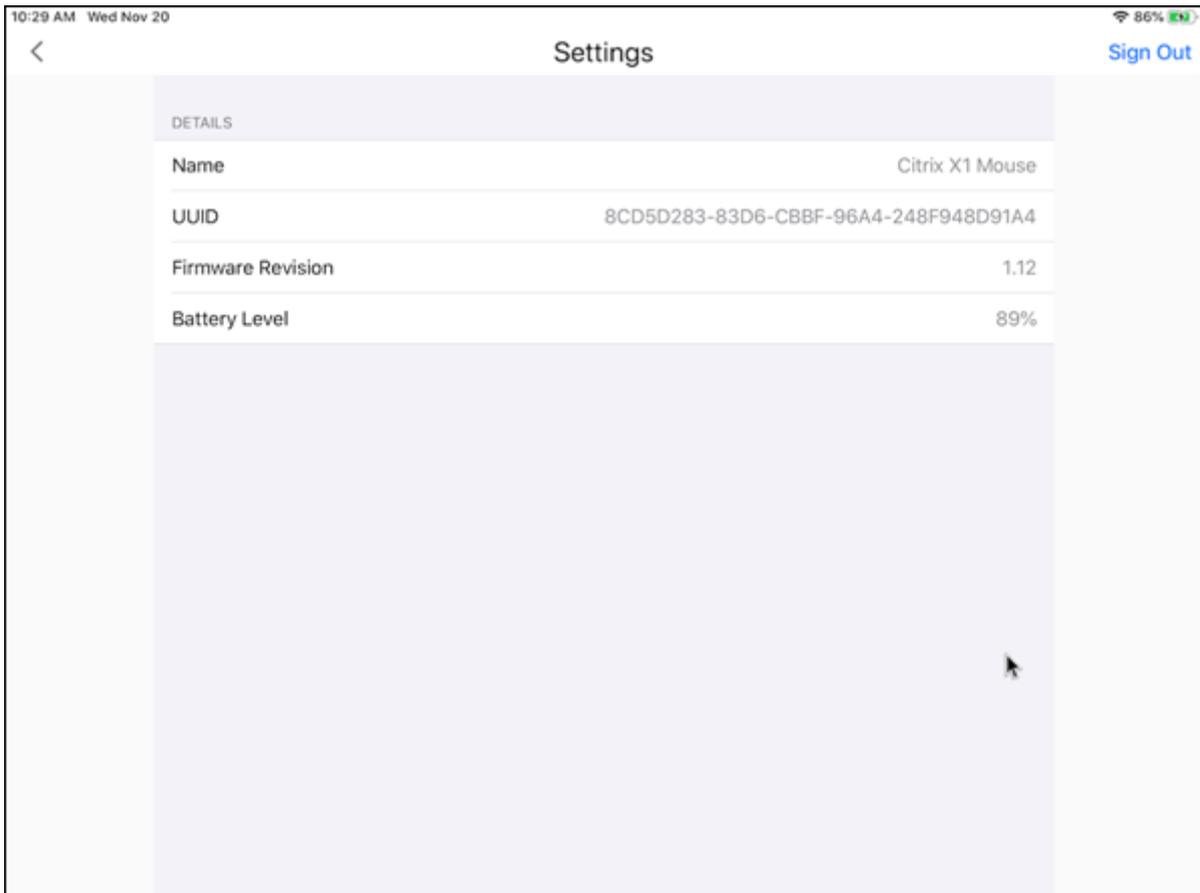




- [名前]、[UUID]、[ファームウェアのリビジョン]、[バッテリー残量] などの Citrix X1 Mouse のプロパティを表示する。そのためには、[接続されたマウス] で、Citrix X1 Mouse エントリをタップします。



接続されたマウスのプロパティ:



**AssistiveTouch** iOS 13 以降のデバイスで AssistiveTouch 機能を有効にすると、デスクトップマウスモードと AssistiveTouch モードの切り替えで、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 App Switcher 画面に移動する
- iOS のホーム画面または別のアプリに移動する

Citrix Workspace アプリに戻ったとき、およびセッション中は、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でツールバーを操作できます。ツールバーを閉じている間は、ツールバーのノッチを水平に移動することができます。iOS デバイスを外部モニターに接続すると、Citrix Workspace アプリ

によって外部モニターの画面解像度が自動的に検出されます。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。表示オプションにアクセスするには、アカウントを追加したりサインインしたりする必要はありません。

### 汎用マウス

#### 汎用マウスとトラックパッドのサポート

汎用マウスまたはトラックパッドを使用して、HDX セッションで右クリック、スクロール、ホバーが可能です。これらの操作は、Citrix X1 Mouse の操作と同様です。ローカルの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。

#### メモ:

- 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た場合、iOS の制限事項により、汎用マウスカーソルはネイティブデバイスに残ります。

#### 外部モニターでの汎用マウスのサポート

iPad に接続された外部モニターで汎用マウスを使用できます。汎用マウスは、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、[設定] > [表示オプション] に移動して、Citrix Workspace アプリで [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ます。

汎用マウスを使用すると、外部モニターでツールバーが非表示になります。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** で汎用マウスを使用したマルチモニター拡張サポート

iPad と汎用マウスを接続すると、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 以降で利用できます。

#### 注:

- この機能は、以前のバージョンでも一部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 アプリのマウスクリックを優先させるには、iOS 設定で [設定] > [アクセシビリティ] > [タッチ] > [AssistiveTouch] で AssistiveTouch を無効にします。

拡張モードの構成 拡張モードを有効にするには、以下の手順を実行します：

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：

このセットアップでは、Apple の USB-C to Digital AV Multiport アダプターまたは Lightning Digital AV アダプターが最適に機能します。

2. [設定] > [表示オプション] に移動して [外部ディスプレイ] をオンに切り替えます。さまざまな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、ミラーリングモードとプレゼンテーションモードでも汎用マウスが使用されます。
3. [拡張] オプションを選択します。

次の表示モードのいずれかを選択できます。

- ミラーリング：iPad に接続された外部モニターのディスプレイをミラーリングできます。
- プレゼンテーション：外部モニターをトラックパッドに変更できます。
- 拡張：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、拡張モードを設定します。
- 拡張モードのサポートは、iPhone ではまだ発表されていません。

ディスプレイ配置の構成 ディスプレイ配置を構成するには、以下を実行します：

1. [拡張] を選択すると、[ディスプレイの配置] オプションが表示されます。
2. 外部ディスプレイタイルを iPad ディスプレイの左、上、右、または下に再配置します。

注：

セッション内ツールバーで [表示] 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。

注：

外部ディスプレイの解像度は、以下に応じて異なります：

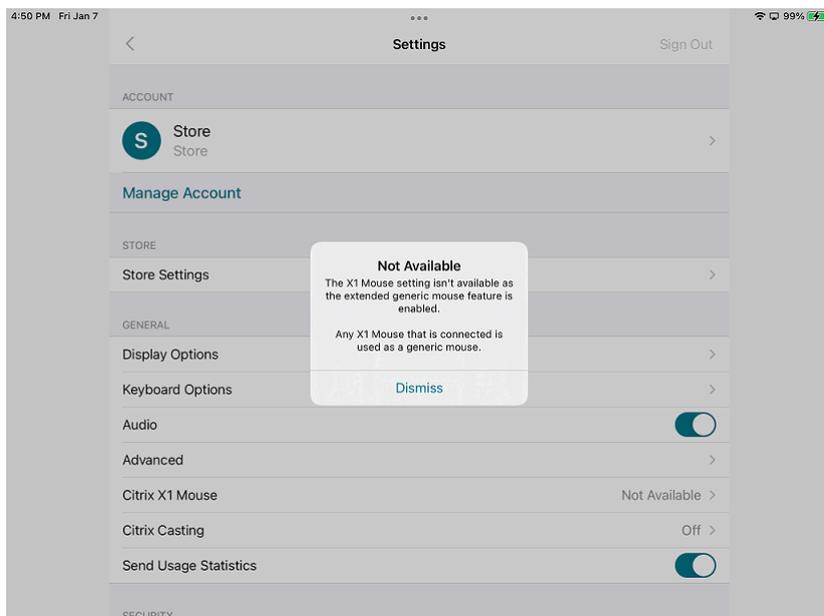
- アダプター
- iPad
- 使用される他のハードウェア

## 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、自動的に Citrix X1 マウスモードよりも優先されます。X1 マウスを接続している場合は、汎用マウスの代わりとして使用されます。そのため、汎用マウスのフィーチャーフラグが有効になっている場合、X1 マウス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 以降の場合、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。

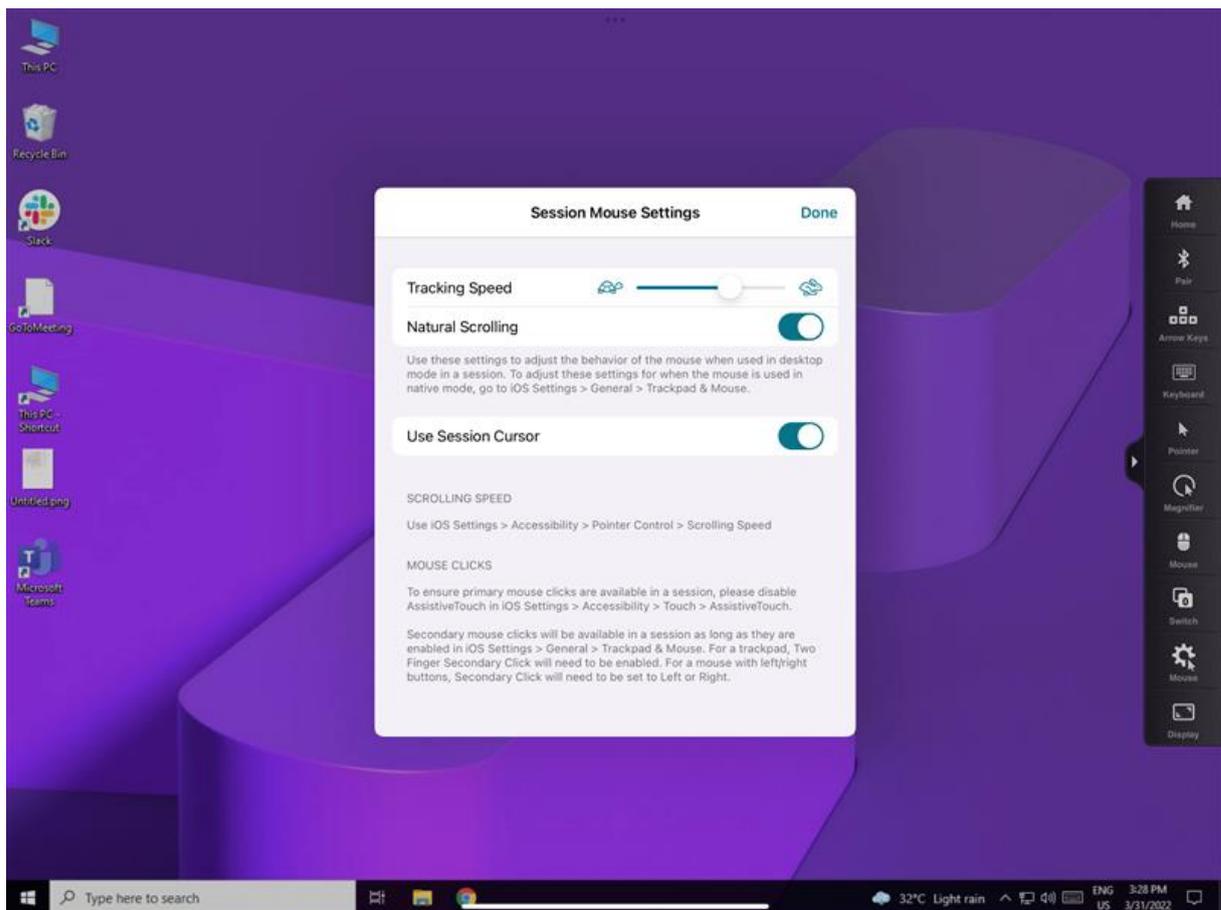


## 汎用マウスアイコン

[マウス] 設定アイコンは、セッション内ツールバーの [表示] 設定アイコンの横に追加されます。[マウス] 設定を使用して、セッション中の汎用マウスの追跡速度を調整します。リモートカーソルイメージを使用して切り替えることもできます。

注:

iOS の設定からネイティブマウスの追跡速度を調整できます。



#### 機能の制限事項

- Citrix Workspace アプリのマウスクリックを優先させるようにするには、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 設定の軌跡の速さ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。セッションツールバー内のマウス設定画面から、軌跡の速さとナチュラルスクロールオプションにアクセスできます。
- 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、つまりセッションの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、マウスイベントが受信されません。この問題を回避するには、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、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。オーディオは iPad スピーカーから再生されます。[HDX-39159]

#### この機能の既知の問題

- セッションがアクティブな間に以下を変更すると、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が乱れます：
    - ディスプレイの配置
    - 解像度
    - 方向または
    - 表示モード
- この問題を回避するには、モニターを切断してから再接続します。問題が解決しない場合は、セッションを切断して再起動します。[HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924]
- まれに、ビデオが外部モニターで再生されるときに、オーディオに数秒の遅れが発生する場合があります。[HDX-39159]
  - まれに、iPad および外部モニターで VDA ディスプレイが一部欠けることがあります。この問題を回避するには、モニターを切断してから再接続します。問題が解決しない場合は、セッションを切断して再起動します。[HDX-37100]
  - 外部モニターでビデオを全画面に最大化すると、ビデオ品質の問題が発生する場合があります。[HDX-39159]
  - まれに、デスクトップセッション内で、アプリを iPad から外部モニターに移動しようとして失敗することがあります。この問題を回避するには、モニターを切断してから再接続します。問題が解決しない場合は、セッションを切断して再起動します。[HDX-36981]
  - まれに、サードパーティの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。[HDX-39713]
  - VDA セッション内の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。[RFIOS-9569]

#### キーボードのサポート

##### 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って、クライアントデバイスの優先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は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で、クライアント IME (Input Method Editor) を有効にします。日本語、中国語、または韓国語でサーバー IME を使用する場合は、[環境設定] > [キーボード] のチェックボックスをオフにして、ローカルキーボードレイアウトオプションを無効にします。

## 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 の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のマッピングポリシー、クライアントキーボードレイアウトの同期および IME の改善ポリシーを有効にします。
- VDA はバージョン 7.16 以降が必要です。

**Windows VDA** および **Linux VDA** で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 でのキーボードレイアウト	Linux で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
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
繁体字中国語	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	ベルギー語 (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 (アメリカ)	英語 (米国)	US キーボード	us
エストニア語	エストニア語	エストニア語キーボード	ee
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	fi
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
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	ch
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

iOS のキーボードレイアウト	キーボード言語	Windows でのキーボードレイアウト	Linux でのキーボードレイアウト
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
アイスランド語	アイスランド語	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) キーボード	pl
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) 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	latam
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 以降で外部キーボードの次の単一キーがサポートされます：

- PageUp
- PageDown
- ホーム
- End
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

#### 特殊キーの組み合わせのサポート

このリリースでは、iOS 対応の外部キーボードで次のキーの組み合わせのサポートが追加されています：

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + CTRL+ S
- Windows + T
- Windows + U
- Windows + 数字
- Windows + 上方向
- Windows + 下方向
- Windows + 左方向
- Windows + 右方向
- Windows + X

- Windows + K
- CTRL + ESC

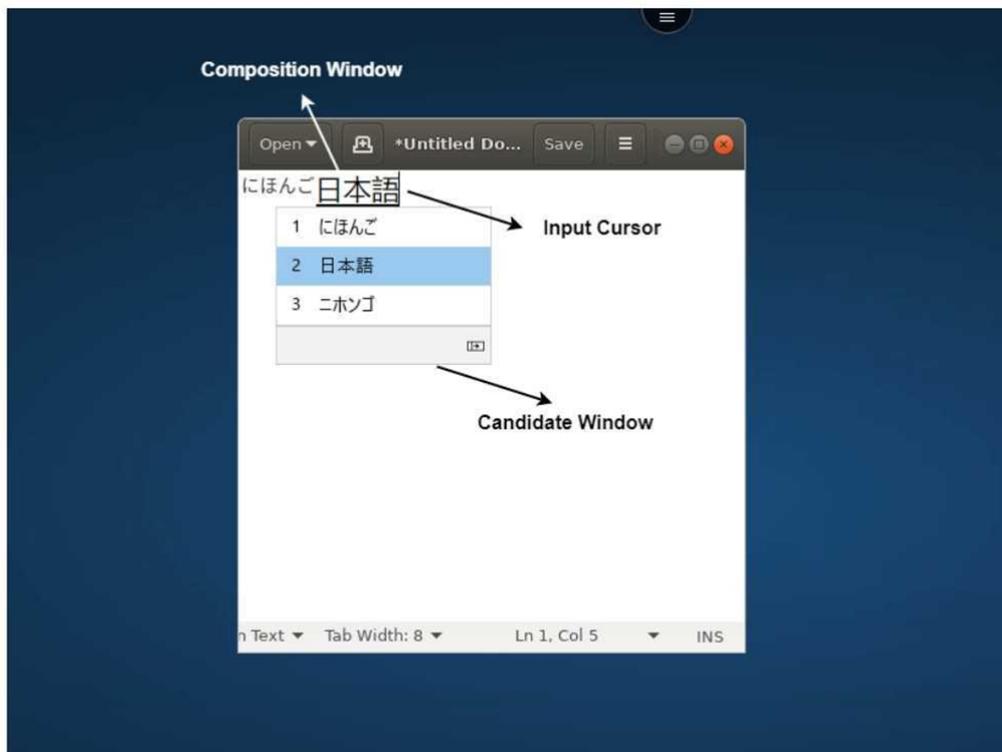
#### 拡張キーボードの機能強化

23.5.0 バージョン以降、拡張キーボード機能が強化され、より優れたユーザーエクスペリエンスが提供されます。以下のような機能強化です：

- 拡張ツールバー UI を固定または固定解除します。
- 画面の回転に合わせて拡張ツールバーを回転させます。
- Windows アイコンキーと 3 キーの組み合わせによるショートカットをサポートします。
- 複数モニターのユースケースシナリオにおけるエクスペリエンスが向上します。
- 拡張ツールバー UI を自動的に開くか閉じます。
- ステージマネージャーモードのエクスペリエンスが向上します（M1 チップを搭載した iPad 上）。

#### IME ユーザーインターフェイス

IME は通常、候補ウィンドウ、テキスト作成ウィンドウなどの UI コンポーネントを備えています。テキスト作成ウィンドウには、作成する文字および下線、背景色などのテキスト作成 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。



テキスト作成ウィンドウでは、確定済みの文字と作成中の文字を区別できます。作成ウィンドウと候補ウィンドウは、入力カーソルに沿って移動します。

そのため、次のように機能が強化されています：

- テキスト作成ウィンドウでのカーソル位置での文字入力機能の強化。
- テキスト作成ウィンドウと候補ウィンドウでの表示機能の強化。

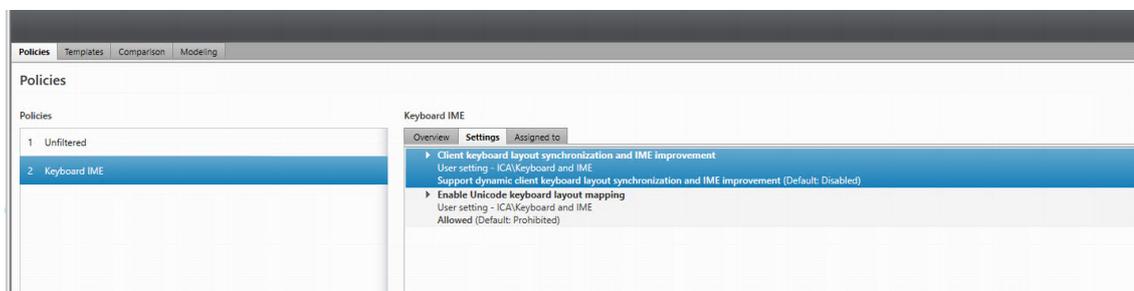
現在、この機能は Windows VDA でホストされているセッションで使用可能で、ソフトキーボードと外付けの物理キーボードの両方をサポートしています。

### 東アジア言語の汎用クライアント IME

汎用クライアント IME 機能は、iOS デバイスでの中国語、日本語、および韓国語 (CJK) 言語の文字の入力および表示エクスペリエンスを強化します。クライアント IME を使用したセッション中にこの機能を使用すると、カーソル位置に CJK 文字を入力できます。この機能は、Windows VDA 環境で使用できます。ユーザーエクスペリエンスを向上させるために、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

- Windows VDA でグループポリシー [クライアントキーボードレイアウトの同期と IME の改善] と [Unicode キーボードレイアウトのマッピングを有効にする] を有効にします。



詳しくは、Knowledge Center の [CTX312404](#) を参照してください。

Windows VDA で次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：

- 1 - HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0
- 2 - HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value = DWORD 1
- 3 - HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value = DWORD 1

- Citrix Workspace アプリで [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、外付けの物理キーボードの使用時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 デバイスを外付けの Windows PC の標準キーボードで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 のソフトキーボードの代わりに VDA のキーボードレイアウトを使用できます。これによって、iOS ではなく外付けの Windows キーボードの入力スタイルを完全に再現することができます。全体的なユーザーエクスペリエンスが大幅に向上するため、東アジア言語で入力する場合に役立ちます。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することになる可能性があります。さらに詳しい内容については、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を適用します。
  - **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 は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を適用します。

デフォルトでは、ソフトウェアまたはタッチキーボード、および外部キーボードの両方の入力モードとして **[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て、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。

**使用例** たとえば、iOS デバイ스에 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場合のシナリオを想定してみましょう。

**[Scancode]** を選択して外部キーボードの Caps Lock の隣のキーを入力すると、スキャンコード「**1E**」が VDA に送信されます。次に、VDA は「**1E**」を使用して文字「**a**」を表示します。

**[Unicode]** を選択して外部キーボードの CapsLock の隣のキーを入力すると、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含む別のキーボードレイアウトを使用している場合でも、「**a**」という文字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は、**Unicode** が優先される入力モードです。これは、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。

外部キーボードのショートカットのサポートを強化

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ショートカットをより多く使用できるようになりました。以下は、外部キーボードのショートカットで強化された重要な変更点です：

- **Insert** キー、**Delete** キー、テンキーなどの Windows キーボード固有のキーのサポート。
- キーを押したままにすると、リモートデスクトップ/アプリが正しく応答します。
- 3つを超える数のキーを使用した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] で、次のオプションによって **Alt** に特定のキーを構成できるようになりました：

- **Option** または **Alt** (左)：[**Option** または **Alt** (左)] を **Alt** キーの代わりに使用します。
- **Command** または **Windows** (左)：[**Command** または **Windows** (左)] を **Alt** キーの代わりに使用します。
- **Option** または **Alt** (左右)：[**Option** または **Alt** (左右)] を **Alt** キーの代わりに使用します。

**Alt** オプションに特定のキーを割り当てると、macOS の **Option** キーと Windows の **Alt** キーの間の競合を回避できます。

制限事項 次の iOS システムのショートカットは現在サポートされていません：

- コマンド (**Windows**) - **H** キー：ホーム画面に移動します。
- コマンド (**Windows**) - スペースキー：検索フィールドを表示または非表示にします。
- コマンド (**Windows**) - **Tab** キー：開いているアプリの中で、2 番目に最近使用したアプリに切り替えます。
- コマンド (**Windows**) - **Shift - 3** キー：スクリーンショットを撮ります。
- コマンド (**Windows**) - **Shift - 4** キー：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。
- コマンド (**Windows**) - オプション (**Alt**) - **D** キー：ドックを表示または非表示にします。
- コマンド (**Windows**) - **Ctrl - Q** キー：デバイスをロックします。
- ヨーロッパのキーボードで **AltGr** はサポートされていません。 **AltGr** を含む特殊文字を入力する場合は、代わりに次のショートカットを使用します：
  - macOS での **Option +\*** ショートカット、または
  - Windows OS での **Alt +** テンキーのショートカット。

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/ビデオ会議で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 アプリがマイクやカメラにアクセスすることを許可する必要があります。デバイスの [設定] に移動し、カメラやマイクを有効にします。

また、Client Selective Trust 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いるため、Citrix Workspace アプリは VDA セッションからのアクセスを信頼できます。

Citrix Workspace アプリでは、マイクまたはカメラにアクセスするためにはユーザーの許可が必要です。

[設定] > [ストアの設定] に移動して、アクセスレベルを構成できます。[ストアの設定] メニューで、必要なマイクまたはカメラへのアクセスを有効にするストアをクリックします。選択したマイクアクセス設定またはカメラアクセス設定は、ストアごとに適用されます。

### 背面カメラのサポート

iOS 向け Citrix Workspace アプリでは、VDA セッション内でカメラを前面から背面に、またはその逆に切り替えることができるようになりました。

カメラを呼び出すと、フローティングボタンが表示されます。フローティングボタンを 1 回タップして、前面カメラと背面カメラの間で切り替えます。

また、フローティングボタンを画面上で自由に動かしてどこにでも配置できます。

既知の問題:

キャスト機能またはドキュメントのスキャン機能が有効になっていると、フローティングボタンが部分的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

24.1.0 バージョン以降、iOS 向け Citrix Workspace アプリは、ハードウェアアクセラレーションによる H.264 ビデオエンコードまたはデコードをサポートします。Citrix HDX のマルチメディアエンジンは、エンコーディングとデコーディングに Apple の Video Toolbox フレームワークを使用するようになりました。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。この機能拡張により、マルチメディアの使用中の CPU の負荷が軽減されます。

### クライアントドライブマッピング (CDM)

構成されたすべてのストアで特定のデバイスストレージへのアクセスを選択できます。デバイスストレージへのアクセスには、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/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へのアクセスの種類を選択するように求められます。デフォルトでは、[アクセスなし] が選択されています。

注:

この機能は、ICA の直接起動と Citrix Gateway 構成ストアにのみ適用されます。エンドツーエンド SSL がセットアップされてい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] に新設された [ストアの設定] セクションで使用できます。[デバイスストレージ] を表示するには、[設定] > [ストアの設定] にアクセスします。

### Citrix Ready ワークスペースハブ

Citrix Ready ワークスペースハブは、デジタル環境と物理環境を組み合わせ、セキュアなスマートスペース内にアプリやデータを配信します。このシステム全体が、モバイルアプリやセンサーなどのデバイス（「モノ」）を接続して、インテリジェントで応答性の高い環境を作ります。

Citrix Ready ワークスペースハブは Raspberry Pi 3 プラットフォーム上に構築されます。Citrix Workspace アプリを実行しているデバイスは Citrix Ready ワークスペースハブに接続し、デスクトップまたはアプリをより大きなディスプレイにキャストします。

Citrix Ready ワークスペースハブについて詳しくは、[Citrix Ready ワークスペースハブドキュメント](#)を参照してください。

セキュリティ上の理由から、Citrix Ready ワークスペースハブでは、モバイルデバイスとハブ間の SSL (Secure Sockets Layer) 接続がサポートされます。各デバイスを一意に特定するため、完全修飾ドメイン名 (FQDN) を設定します。詳しくは、Citrix Ready ワークスペースハブドキュメントの「[セキュリティ接続](#)」を参照してください。

次のシステム要件がすべて満たされている場合、Citrix Workspace アプリで Citrix Ready ワークスペースハブが有効になります:

- iOS 向け Citrix Workspace アプリ 1810.1 以降
- Bluetooth に対応している
- 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 ワークスペースハブの構成

Citrix Ready ワークスペースハブの各機能を有効にするには、デバイス上で [設定] に移動し、[**Citrix Casting**] をタップして機能を有効化します。詳しくは、[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 アプリに、iOS デバイス上の信頼できるデバイス一覧に対してワークスペースハブを追加または削除する新しい手順が統合されました。詳しくは、「[セキュリティ接続](#)」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

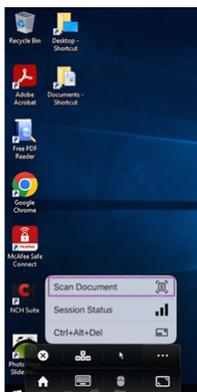
24.5.0 バージョン以降、iOS 向け Citrix Workspace アプリはドキュメントスキャナー機能をサポートします。この機能を使用することで、デスクトップセッション内で複数のドキュメントをすべてスキャンして保存できるようになりました。この機能はデフォルトで有効になっています。

### 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、デバイスでの読み取りおよび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：
  1. プロフィールから、アプリケーションの [設定] > [ストアの設定] をタップします。
  2. 現在のストアをタップします。
  3. デバイスの [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：

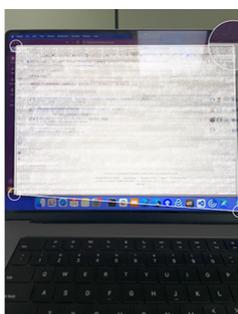
1. セッション中のツールバーから省略記号メニューをタップし、[書類をスキャン] を選択します。カメラアプリが開きます。



2. シャッターボタンをタップして写真を撮影します。再度撮影する場合は、[再撮影] をタップします。



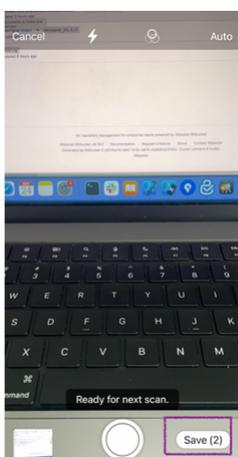
3. オプション: スキャンしたドキュメントをトリミングします。必要なサイズにトリミングしたら、[スキャンを保持] をタップします。カメラアプリが再び開き、さらに画像を撮影できるようになります。



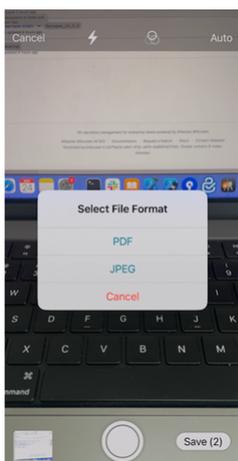
Retake

Keep Scan

4. 必要な画像をキャプチャしたら、[保存] をタップします。



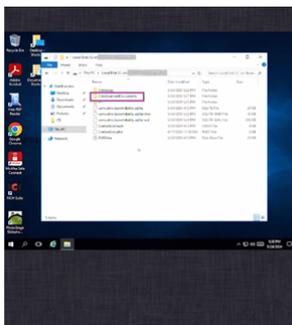
5. スキャンした書類を必要な形式で保存するには、ファイル形式オプションを選択します。



6. [OK] をタップします。



スキャンされたすべてのドキュメントは、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で **CitrixScannedDocuments** にアクセスすることもできます。

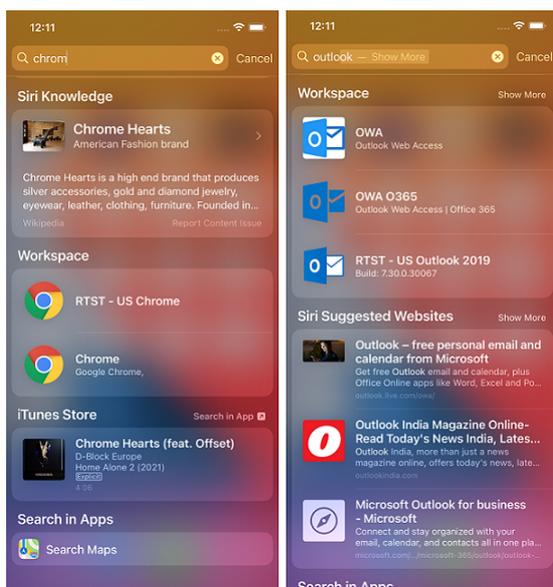


## ユーザーエクスペリエンス

March 27, 2024

### **Spotlight** 検索の機能強化

アプリアイコンは、対応するアプリ検索と一致しています。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。



### 3D Touch ジェスチャによる最近のアプリへのアクセス

**Citrix Workspace** アプリアイコンで 3D Touch（長押し）ジェスチャを使用すると、最近起動した一覧からすばやくアプリにアクセスできます。

### バッテリー状態インジケータ

デバイスのバッテリー状態が、仮想デスクトップセッションのシステムトレイに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 上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が表示されるまでに約 1~2 分かかる場合があります。

### 長押し機能によるリソースへのアクセス

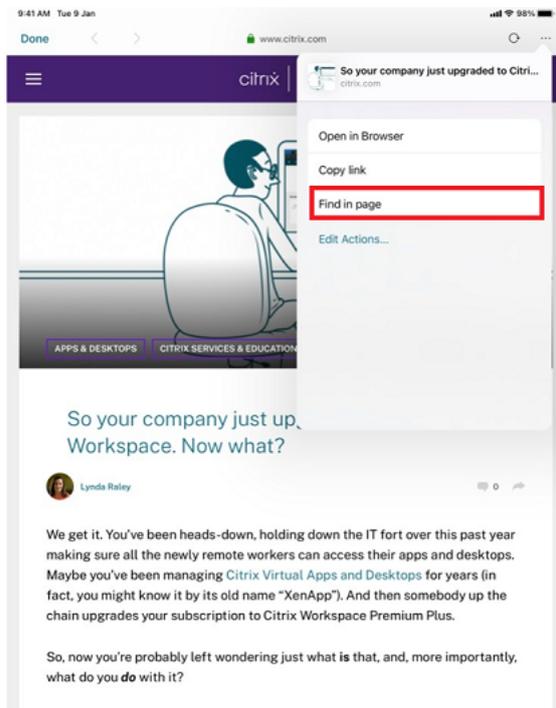
Citrix Workspace アプリのアイコンを長押しして、最後に起動したリソースにアクセスできるようになりました。Citrix Workspace アプリを終了しても、最後に起動したリソースにアクセスできるようになりました。

### ページ内の検索機能の強化

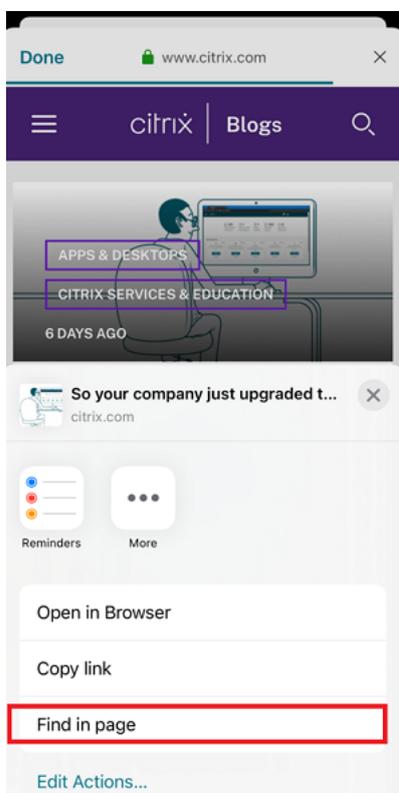
ページ内の検索機能の強化では、単語や語句を検索できます。このユーザビリティの向上は、Web や Software-as-a-Service (SaaS) アプリ内に適用できます。

検索するには、以下を実行します：

1. iPad では、右上隅の省略記号 (⋮) ボタンをタップし、[ページ内を検索] を選択します。

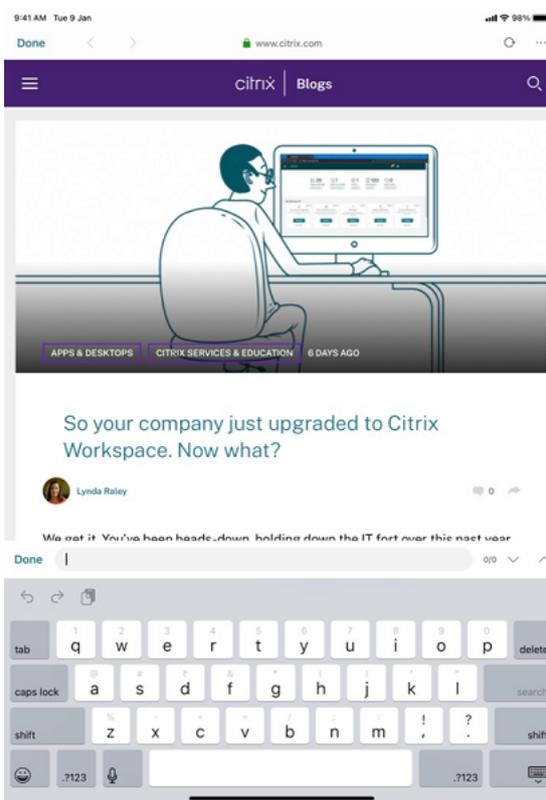


- iPhone では、右下隅の省略記号 (⋮) ボタンをタップし、[ページ内を検索] を選択します。

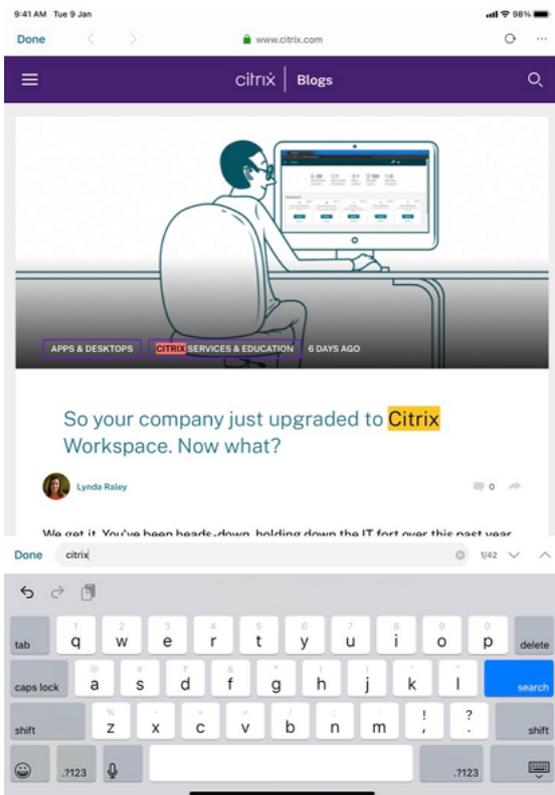


スクリーンキーボードが表示されます。

## iOS 向け Citrix Workspace アプリ



1. 検索するテキスト（たとえば、「Citrix」）をテキストボックスに入力します。検索結果が表示されます。



## セッション内ツールバーの位置を変更

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とドロップ先が表示されます。ドロップ先の上でドラッグインジケータをドロップして、ツールバーの位置を変更します。

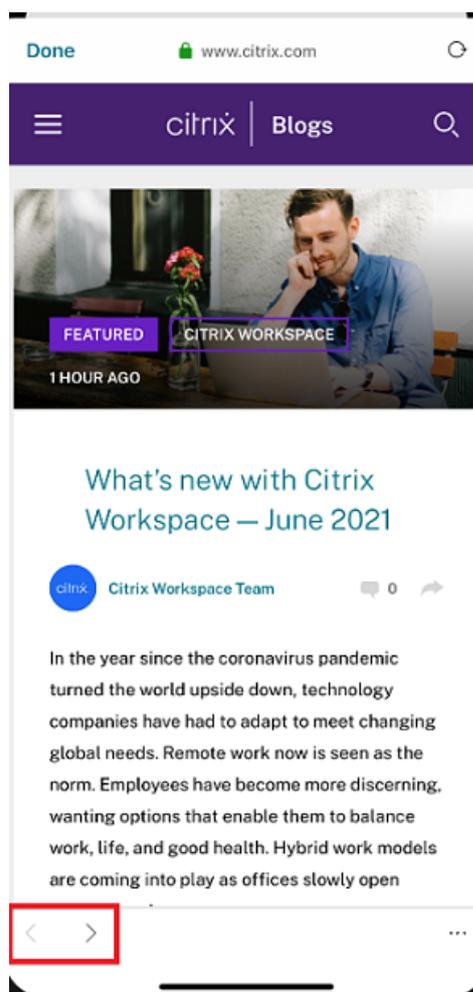
### メモ:

- この機能は iPad ユーザーにのみ適用されます。
- この機能は、タッチパッド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まで保持されます。

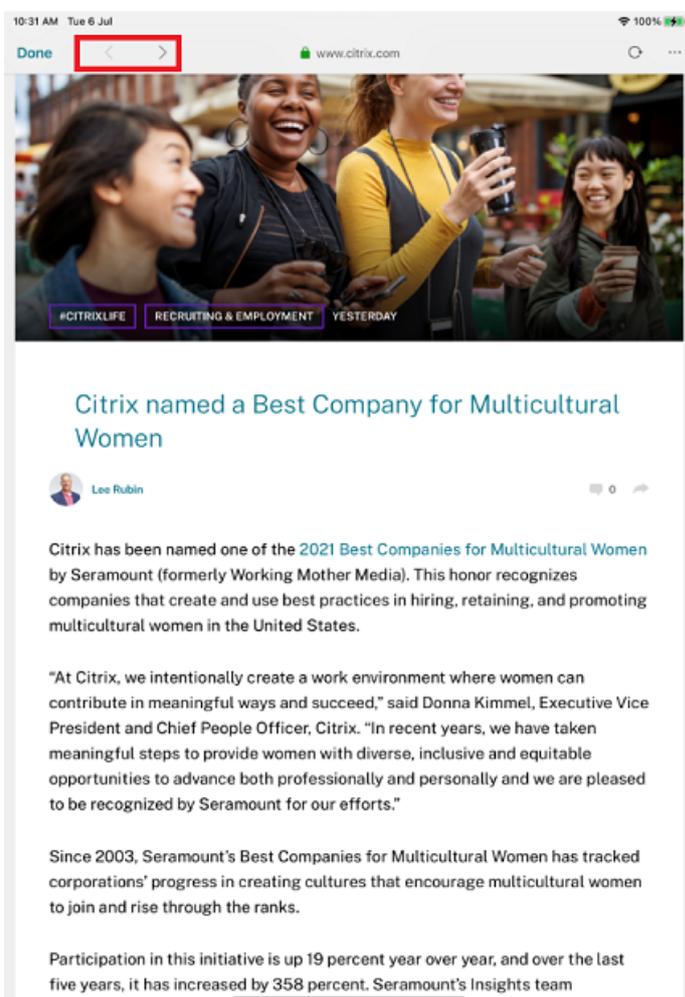
## SaaS アプリと Web アプリ間で切り替え

ユーザビリティの向上により、Web アプリ内や Software-as-a-Service (SaaS) アプリ間でも自在に移動できるようになりました。

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



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



## 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、エンドユーザーをオンプレミスの StoreFront ストアの URL から Workspace URL にシームレスに移行できます。管理者は、[Global App Configuration Service](#)を使用して、最小限のエンドユーザー操作で移行を実行できます。

構成するには、以下を実行します：

1. [Global App Configuration Store Settings API](#)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** に移動して、**[POST]** をクリックします。
3. **[INVOKE API]** をクリックします。

4. パ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ミリ秒形式のエポックタイムスタンプで入力します。

例:

```
1  "migrationUrl": [  
2  {  
3  
4  
5  "url": "<cloud store url>"  
6  "StoreFrontValidUntil": "<epoch timestamp in milliseconds>",  
7  }  
8  
9  ] ,  
10 <!--NeedCopy-->
```

5. [EXECUTE] をクリックして、サービスをプッシュします。

## 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** ができること] 移行画面が表示されます（資格がある場合）。[新しい **Citrix Workspace** を今すぐ試す] 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:

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



Workspace（クラウド）ストアに移行すると、[設定] で StoreFront 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、応答を収集するフィードバック画面が表示されます。

注:

StoreFront ストアには有効期限があります。有効期限を指定すると、ストアは削除されます。

## Siri の統合

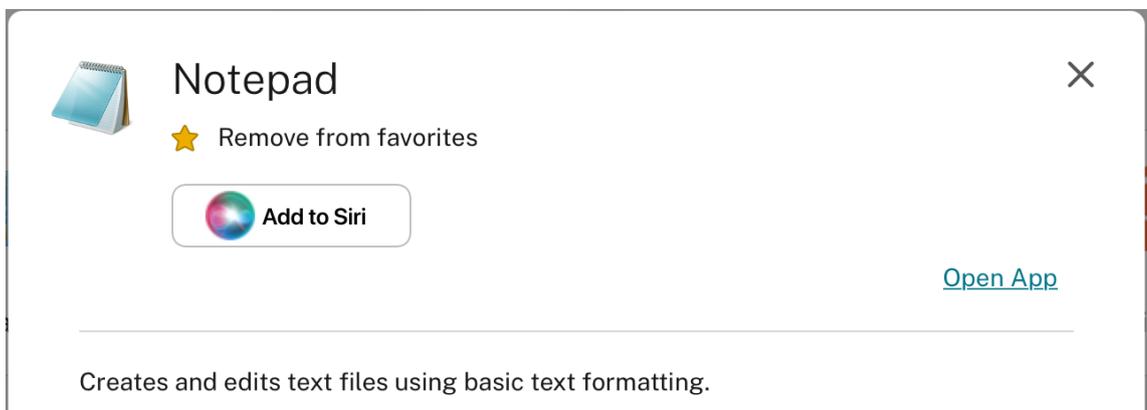
毎回 Citrix Workspace アプリを起動しなくても、Siri を操作して、アプリやデスクトップなどのリソースを起動できます。

構成するには

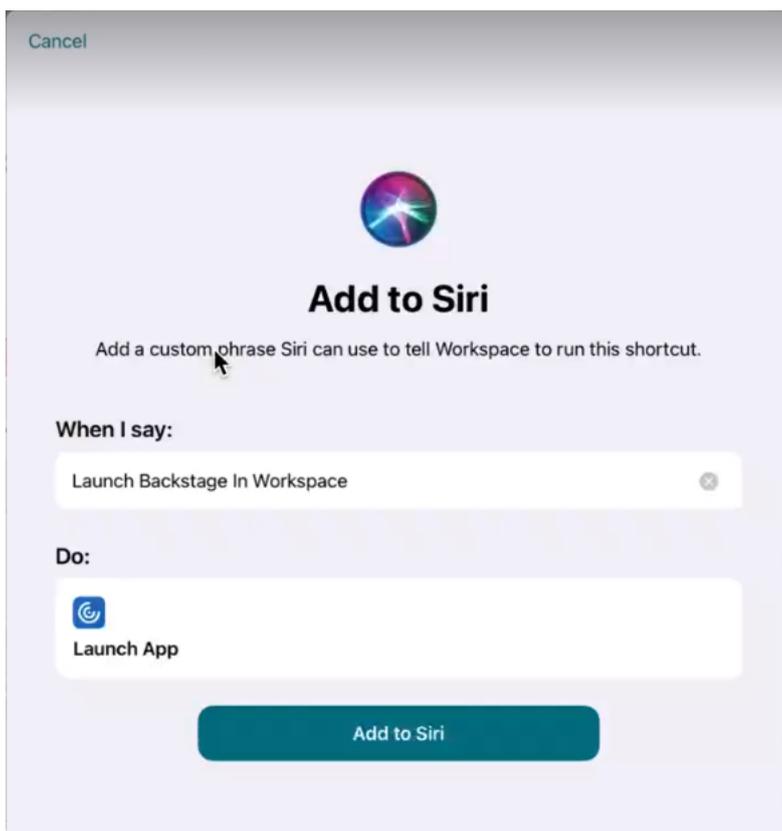
1. Citrix Workspace アプリを起動し、[アプリ] または [デスクトップ] をタップします。Siri ショートカットに追加するリソースを選択します。
2. 省略記号 (…) をタップします。ダイアログボックスが開きます。

注:

iPhone または iPad デスクトップユーザーの場合は、省略記号 (…) をタップし、アプリの詳細画面で [詳細の表示] をタップします。ダイアログボックスが開きます。手順 3 に進みます。



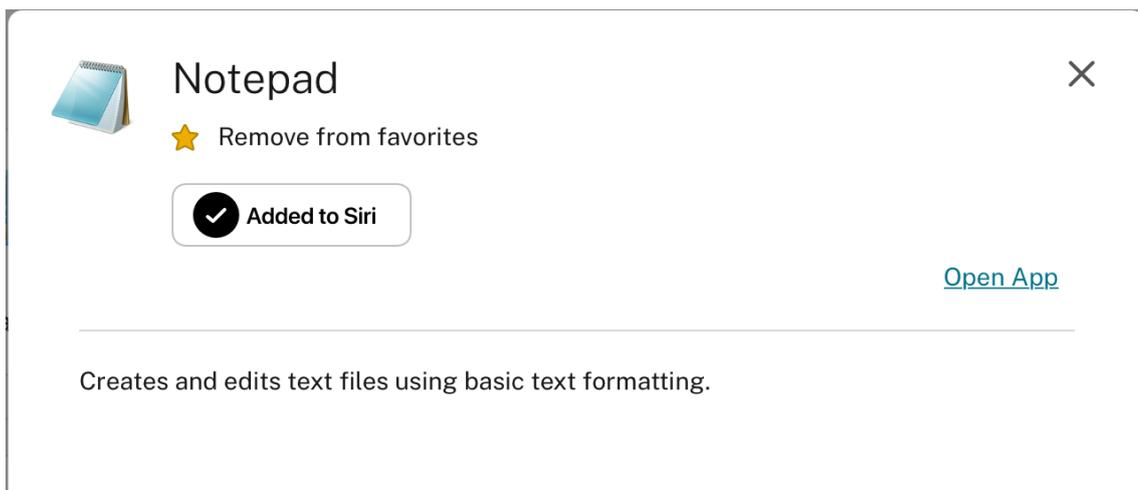
3. **[Siri に追加]** をタップします。**[Siri に追加]** ダイアログボックスが開きます。



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。これで、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:

Siri を呼び出すための、カスタムフレーズの記録に対応しているデバイスもあります。



### 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をタップして、[アプリケーション設定] > [**Siri**の構成]の順にタップします。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、音声を使用してこの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開きます。
3. [**Siri**に追加されました] をタップします。ショートカットを編集するためのダイアログボックスが開きます。

### Citrix Workspace アプリからの個別のセッションウィンドウのサポート

バージョン 24.1.0 以降、iOS 向け Citrix Workspace アプリには、マルチタスクをより効率的で使いやすくする個別のセッションウィンドウが導入されています。この機能を使用すると、デスクトップのようなエクスペリエンスを実現できます。個別のセッションウィンドウ機能が有効になっている場合は、単に接続されている外部モニターにセッションをドラッグアンドドロップするだけです。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るようになります。

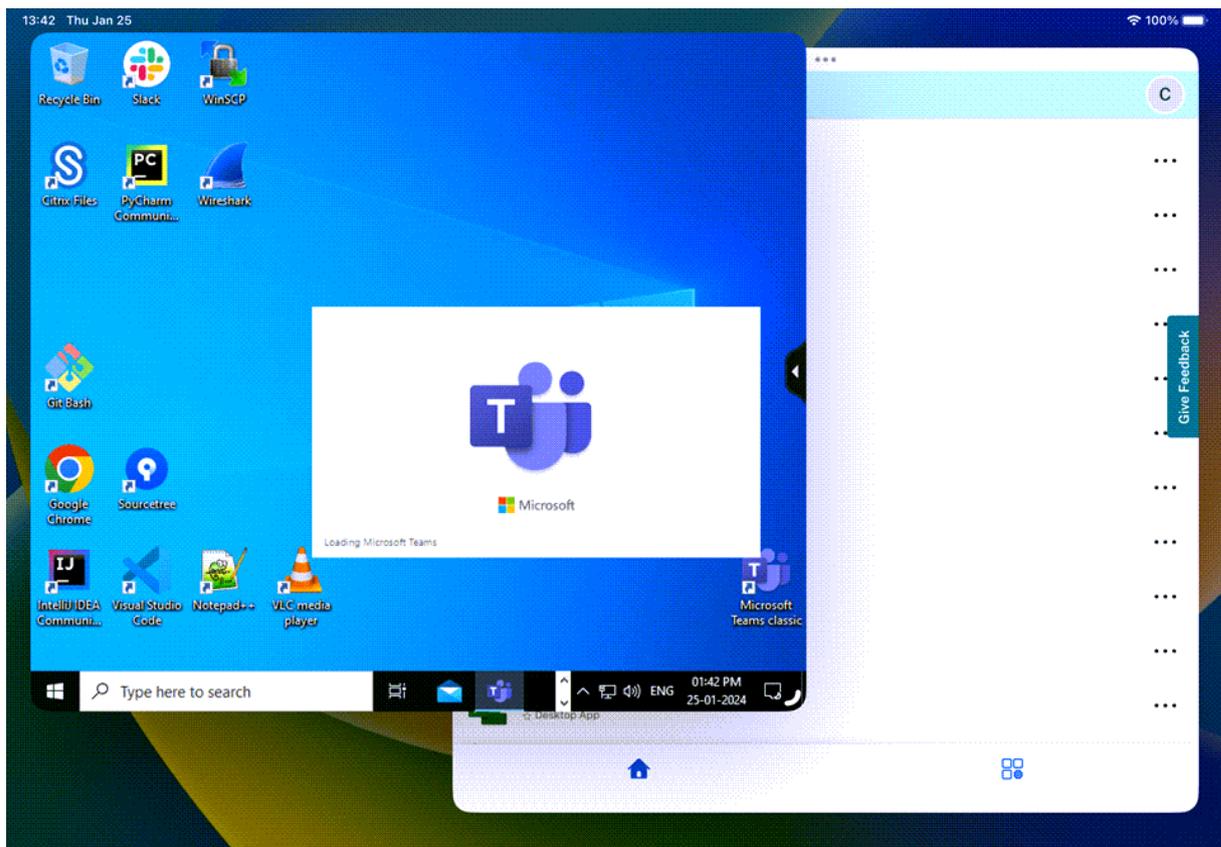
この機能には次の改善が含まれています：

- 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るようになります。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 セッションの上部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 設定の代わりにセッション解像度を調整できます。

#### 注：

この機能は、ステージマネージャ機能をサポートするデバイスでのみサポートされます。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。ステージマネージャ機能について詳しくは、Apple サポートドキュメントの「[iPad でステージマネージャのオン/オフを切り替える](#)」を参照してください。

個別のセッションウィンドウ機能を設定するには、[設定] > [詳細] > [**Multitasking**] に移動し、[**Separate Session Window**] を選択します。



## Web アプリおよび SaaS アプリの Webview

December 12, 2023

### 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。次の操作を実行できます：

- Web ビュー内からリンクをコピーする
- Safari で Web ページを直接開く
- 相手やアプリにリンクを直接送信する

共有するには、Web ビューの右上にある [...] アイコンをタップするか、Web ビュー内の任意のリンクを長押ししてから、必要なオプションをタップします。

## Web ビュー

### SaaS アプリのネイティブコントロールによる Web ビュー機能強化

SaaS アプリのネイティブコントロールを備えた Web ビューを使用できます。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、それぞれ前後に移動できるようになりました。

### Citrix Workspace モバイルアプリ Web ビューアー

Web ビューアーは、Citrix Workspace アプリ内で実行され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 アプリから安全な方法で Web または SaaS アプリを開くことができます。Web ビューアーでは、さまざまな Web または SaaS アプリにアクセスする場合に、一貫したユーザーインターフェイスを使用できます。これによって生産性や、アプリのレンダリングのパフォーマンスが向上します。

この新しい Web ビューアーは、ユーザーエクスペリエンスの向上に引き続き重点を置いており、次の機能を備えた、強化された、よりネイティブブラウザのようなエクスペリエンスを提供します：

- 内部 Web ページへの VPN レスアクセス
- アダプティブアクセスポリシーを使用した Web および SaaS への SSO
- プレビューがあるファイルダウンロード
- ページとサイト間のシームレスなナビゲーション
- URL を共有する機能
- ページ内を検索
- 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ときと同じビュー

管理者は、URL ごとにさまざまな組み合わせで、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、透かしなどの Secure Private Access (SPA) を有効にできます。

## パスワード管理

March 27, 2024

## パスワードの保存

Citrix Web Interface 管理コンソールでは、認証時にユーザーがパスワードを保存することを許可できます。管理者がユーザーのアカウントを設定すると、パスワードが暗号化され、そのユーザーの初回接続時まで保存されます。以下に注意してください：

- ユーザーによるパスワードの保存を許可すると、iOS 向け Citrix Workspace アプリでパスワードがデバイス上に格納され、アプリケーションへの接続時にパスワードの再入力が不要になります。

注：

パスワードが保存されるのは、ユーザーがアカウントを作成するときにパスワードを入力した場合のみです。アカウントのパスワードが入力されていない場合は、サーバー側の設定にかかわらずパスワードは保存されません。

- 管理者がパスワードの保存を無効（デフォルト設定）にすると、ユーザーが iOS 向け Citrix Workspace アプリに接続するときにパスワードの入力が常に必要になります。

注：

StoreFront 直接接続では、パスワードを保存することはできません。

## パスワード保存設定を上書きするには

サーバー側でパスワードの保存を有効にしても、ユーザーは以下の方法でパスワードの入力が毎回要求されるように設定できます：

- アカウント作成時に、パスワードフィールドを空白のままにする。
- アカウント編集時に、パスワードを削除して設定を保存する。

## 使用方法

Citrix Workspace アプリでパスワードを保存することができるため、接続プロセスが効率的に処理されます。これにより、Citrix Workspace アプリを開くたびにセッションを認証する追加手順が省かれます。

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 ネイティブモードはサポートしていません。ただし、StoreFront で PNA レガシモードを有効にすると、この機能が有効になります。

## パスワードを保存するように **StoreFront** を構成

StoreFront を構成してパスワードの保存機能を有効にするには：

1. 既存のストアを構成している場合は、手順 3 に移動します。
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」で説明されているベストプラクティスの説明に従ってください。
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、SSL 証明書の生成時に指定したのと同じ共通名にする必要があります。
4. 構成するストアを選択します。
5. [XenApp Services サポートの構成] をクリックします。
6. [XenApp Services サポートを有効にする] をオンにし、任意で [デフォルトストア] を選択し、[OK] をクリックします。
7. 「c:\inetpub\wwwroot\Citrix\<ストア名>\Views\PnaConfig\」にあるテンプレート構成ファイルにアクセスします。
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>」の「**false**」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、管理者権限を使って PowerShell を実行します。
13. PowerShell コンソールで、次のように実行します：
  - a. `cd "c:\Program Files\Citrix\Receiver StoreFront\Scripts"`
  - b. 次のように入力します。「Set-ExecutionPolicy RemoteSigned」
  - c. 次のように入力します。「.\ImportModules.ps1」
  - d. 次のように入力します。「Set-DSServiceMonitorFeature -ServiceUrl https://localhost:443/StoreFrontMonitor
14. StoreFront グループがある場合は、グループのすべてのメンバーで同じコマンドを実行します。

#### パスワードを保存する **Citrix Gateway** の構成

注:

この構成は、Citrix Gateway 負荷分散サーバーを使用します。

Citrix Gateway を構成してパスワードの保存機能をサポートするには:

1. Citrix Gateway 管理コンソールにログインします。
2. Citrix ベストプラクティスに従って負荷分散仮想サーバー用の証明書を作成します。

3. [Configuration] タブで、[Traffic Management] > [Load Balancing] > [Servers] の順に移動し、[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で手順 5. を繰り返します。
6. [Configuration] タブで、[Traffic Management] > [Load Balancing] > [Monitor] の順に移動し、[Add] をクリックします。
7. モニター名を入力します。[Type] として [StoreFront] を選択します。ページ下部で、[Secure] を選択します (StoreFront サーバーでは HTTPS を使用するため必要です)。
8. [Special Parameters] タブをクリックします。前の手順で構成した StoreFront 名を入力し、[Check Backed Services] を選択してから [Create] をクリックします。
9. [Configuration] タブで、[Traffic Management] > [Load Balancing] > [Service Groups] に移動し、[Add] をクリックします。
10. サービスグループ名を入力し、プロトコルを [SSL] に設定し、[OK] をクリックします。
11. 画面の右側の [Advanced Settings] で [Settings] を選択します。
12. クライアント IP を有効にして、Header 値を **X-Forwarded-For** にして [OK] をクリックします。
13. 画面右側で ([Advanced Settings] の下) [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て、[Select Monitor] ドロップダウンメニューを選択します。(Citrix Gateway で構成されている) モニターのリストが表示されます。
15. 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て、[Select]、[Bind] の順にクリックします。
16. 画面右側で ([Advanced Settings] の下) [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て、[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 で構成されている) サーバーメンバーの一覧が表示されます。作成済みの 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. ポート番号として「443」と入力し、Hash ID に一意の番号を指定してから [Create]、[Done] の順にクリックします。すべてが適切に構成されたら、[Effective State] が緑となってモニターが適正に機能していることが示されます。
20. [Traffic Management] > [Load Balancing] > [Virtual Server] の順にクリックし、[Add] をクリックします。サーバー名を入力してプロトコルに [SSL] を選択します。
21. StoreFront 負荷分散サーバーの 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 Binding]** 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. 負荷分散仮想サーバーに対して作成された SSL 証明書を割り当てます。**[No Server Certificate]** を選択します。
24. 一覧から負荷分散サーバー証明書を選択し **[Bind]** をクリックします。
25. ドメイン証明書を負荷分散サーバーに追加します。**[No CA certificate]** をクリックします。
26. ドメイン証明書をクリックし、**[Bind]** をクリックします。
27. 画面右側で **[Persistence]** を選択します。
28. **[Persistence]** を **[SOURCEIP]** に変更して、タイムアウト値を **[20]** に設定します。**[Save]**、**[Done]** の順にクリックします。
29. ドメイン DNS サーバーで負荷分散サーバー（未作成の場合）を追加します。
30. iOS デバイスで iOS 向け Citrix Workspace アプリを起動して、完全な XenApp URL を入力します。

## 認証

July 1, 2024

### クライアント証明書認証

**重要:**

- StoreFront を使用する場合、Citrix Workspace アプリでは以下がサポートされます。
  - 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 まで
  - Citrix Gateway バージョン 11.1 以降
- iOS 向け Citrix Workspace アプリでは、クライアント証明書による認証をサポートしています。
- クライアント証明書による認証は、Access Gateway Enterprise Edition 9.x および 10.x 以降でのみサポートされます。
- 2 要素認証の種類は、Cert と LDAP である必要があります。
- Citrix Workspace アプリでは、クライアント証明書による認証をオプション（選択自由）として設定することもできます。
- この認証では、P12 形式の証明書のみがサポートされます。

Citrix Gateway 仮想サーバーにサインインするユーザーを、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による認証は、LDAP を使用した 2 要素認証でも使用できます。

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

- 仮想サーバーでクライアント認証が有効になっている。
- 仮想サーバーがクライアント証明書を要求している。
- Citrix Gateway 上でルート証明書をその仮想サーバーにバインドする。

ユーザーは Citrix Gateway 仮想サーバーにサインインし、認証された後、ユーザー名およびドメインの情報を証明書の **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** フィールドから抽出できます。  
`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、そのほかの必須情報（パスワードなど）を提供すると、認証が完了します。有効な証明書や資格情報が提供されなかったり、ユーザー名とドメインの抽出に失敗したりすると、認証に失敗します。

クライアント証明書に基づいて認証するには、既定の認証の種類としてクライアント証明書を指定します。また、「証明書アクション」を作成して、クライアントの SSL 証明書に基づいた認証時の動作を定義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。コンソールは、インストールした 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。同じ情報が、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 接続のために、Web Interface を使用して、Citrix Gateway を構成する方法に似ています。

Citrix Workspace アプリのために、モバイルデバイス用の XenApp ファームを構成して、以下のように Citrix Gateway からの接続をサポートします：

1. XenApp ファームで **[Manage secure client access]** > **[Edit secure client access]** の順に選択します。
2. [Access Method] を [Gateway Direct] に変更します。
3. Citrix Gateway アプライアンスの完全修飾ドメイン名 (FQDN) を入力します。
4. Secure Ticket Authority (STA) の情報を入力します。

### **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による認証を使用するには、Citrix Gateway で Cert と LDAP 認証ポリシーによる 2 要素認証を構成する必要があります。Citrix Gateway アプライアンスを構成するには

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

- Citrix Workspace アプリからの接続であることを特定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したら、次の式を設定し、式の演算子として [Match All Expressions] を選択します:

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

- セッションポリシーのプロファイル設定で、[Security] タブの [Default Authorization] を [Allow] に設定します。

[Published Applications] タブで、これがグローバル設定でない ([Override Global] チェックボックスをオンにする) 場合は [ICA Proxy] が [ON] であ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。次に例を示します:

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

- この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 と LDAP 用の認証ポリシーを作成します。
- これらの認証ポリシーを、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。このためには、[Certificate] で [SSL Parameters] を開き、[Client Authentication] の [Client Certificate] で [Mandatory] を設定します。

**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、中間証明書の場合は、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。

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による認証を有効にすると、クライアント証明書の属性に基づいてユーザーが認証されます。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。ユーザーごとに特定のポリシーを適用できます。

1. Citrix Workspace アプリで、[アカウント] の [サーバー] ボックスに、一致する Citrix Gateway サーバーの FQDN を入力します。たとえば、「GatewayClientCertificateServer.organization.com」などです。Citrix Workspace アプリにより、クライアント証明書が必要であることが自動的に検出されます。
2. ユーザーは、新しい証明書をインストールするか、インストール済みのものを一覧から選択できます。iOS のクライアント証明書認証では、Citrix Workspace アプリのみから証明書をダウンロードしてインストールします。

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のフィールドに、証明書のユーザー名が事前に入力されます。エンドユーザーは、パスワードなどの他の詳細を入力できます。
4. クライアント証明書による認証をオプションとして設定した場合、ユーザーは証明書ページの [戻る] をクリックすることで証明書の選択をスキップすることができます。この場合、Citrix Workspace アプリはそのまま接続を続行し、ユーザーにログイン画面を表示します。
5. ユーザーが初回サインインを完了すると、証明書を提示しなくてもアプリケーションを起動できるようになります。ユーザーのアカウントで使用された証明書は Citrix Workspace アプリに格納され、次回以降のログイン時に自動的に使用されるようになります。

#### 認証プロセスの書き換えポリシーの構成

管理者は、認証プロセスに使用するブラウザーを埋め込みブラウザーからシステムブラウザーに切り替えることができます。これは、高度な認証ポリシーがオンプレミスの Citrix Gateway および StoreFront 展開で構成されている場合のみ可能です。高度な認証ポリシーを構成するには、次のように NetScaler コマンドラインを使用して NetScaler 書き換え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`

システムブラウザーに移行すると、次のような追加機能が提供されます：

- 証明書ベースの認証のエクスペリエンスが向上。
- 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 などのいくつかのサードパーティ認証システムをサポート。

管理者が上記の書き換えポリシーを構成していない場合、埋め込みブラウザーが認証のデフォルトブラウザーとして使用されます。

この表は、NetScaler Gateway および Global App Config Service での構成に基づき、認証に使用されるブラウザーを示しています：

	Global App Configuration	
NetScaler Gateway	Service	認証に使用されるブラウザー
システム	システム	システム
システム	埋め込み	システム
埋め込み	システム	システム

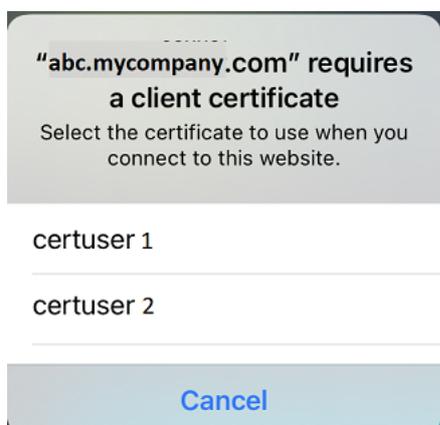
NetScaler Gateway	Global App Configuration Service	認証に使用されるブラウザ
埋め込み	埋め込み	埋め込み
構成なし	システム	システム
構成なし	埋め込み	埋め込み

オンプレミスストアで証明書ベースの認証をサポート

エンドユーザーは、証明書ベースの認証を処理できるようになりました。証明書はデバイスのキーチェーンに保存されます。サインイン中に、Citrix Workspace アプリはデバイス上の証明書の一覧を検出し、認証用の証明書を選択できます。

**重要:**

証明書を選択した後、その選択は次回の Citrix Workspace アプリの起動まで保持されます。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、オンプレミス展開でサポートされます。

構成するには、以下を実行します:

1. [Global App Configuration Store Settings API](#)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** に移動して、**[POST]** をクリックします。

3. **[INVOKE API]** をクリックします。
4. パ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ます。
  - “system”：Safari View Controller を使用できます。

例：

```
1 "category": "Authentication",
2 "userOverride": false,
3 "settings": [
4 {
5   "name": "Web Browser to use for Authentication", "value": "*
   Embedded*/*System*" }
6 ,
7 <!--NeedCopy-->
```

iOS または iPad デバイスでは、管理者は認証プロセスに使用す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。詳しくは、「認証プロセスの書き換えポリシーの構成」を参照してください。

5. **[EXECUTE]** をクリックして、サービスをプッシュします。

## スマートカード

Citrix Workspace アプリは、SITHS スマートカードのセッション中の接続のみ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 の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ます。詳しくは、Knowledge Center の記事[CTX123680](#)を参照してください。

サポートされる製品および構成は以下のとおりです：

- サポートされるスマートカードリーダー：
  - 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）、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 Smart Card Reader
  - Thursby 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
- サポートされる VDA スマートカードミドルウェア
  - ActiveIdentity

- サポートされるスマートカード：
  - PIV カード
  - Common Access Card (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 以降と統合された Citrix Gateway でのスマートカード認証

**Citrix Workspace** アプリでのアプリへのアクセスを構成するには

1. 新しいアカウントを作成するときに Citrix Workspace アプリに自動的にアクセスするよう構成する場合、[アドレス] フィールドにストアの URL を入力します。例：
  - StoreFront.organization.com
  - netscalervserver.organization.com
2. スマートカードを使って認証している場合は、[スマートカードの使用] 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。これを超過した場合、再ログオンするまでアプリケーション一覧を更新したりほかのアプリケーションを起動したりできなくなります。

**twocanoes** スマートカードユーティリティリーダーのサポート

24.3.5 バージョン以降、iOS 向け Citrix Workspace アプリは twocanoes スマートカード ユティリティリーダーをサポートします。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。

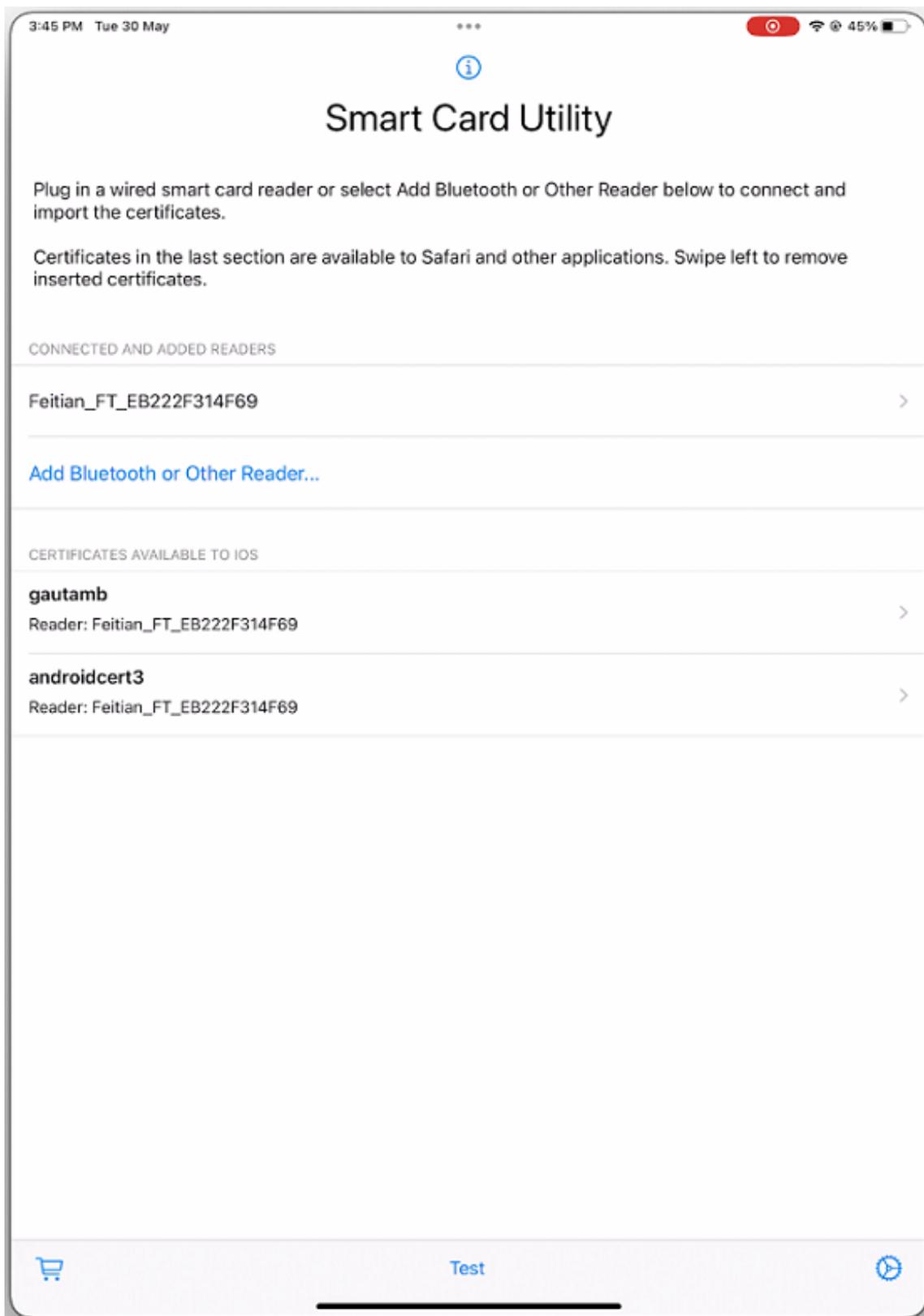
注:

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 USB-C リーダーは、Citrix Workspace アプリのログインでのみサポートされ、仮想セッションのログインではサポートされていません。

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。詳しくは、twocanoes のナレッジベースで「[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てください。

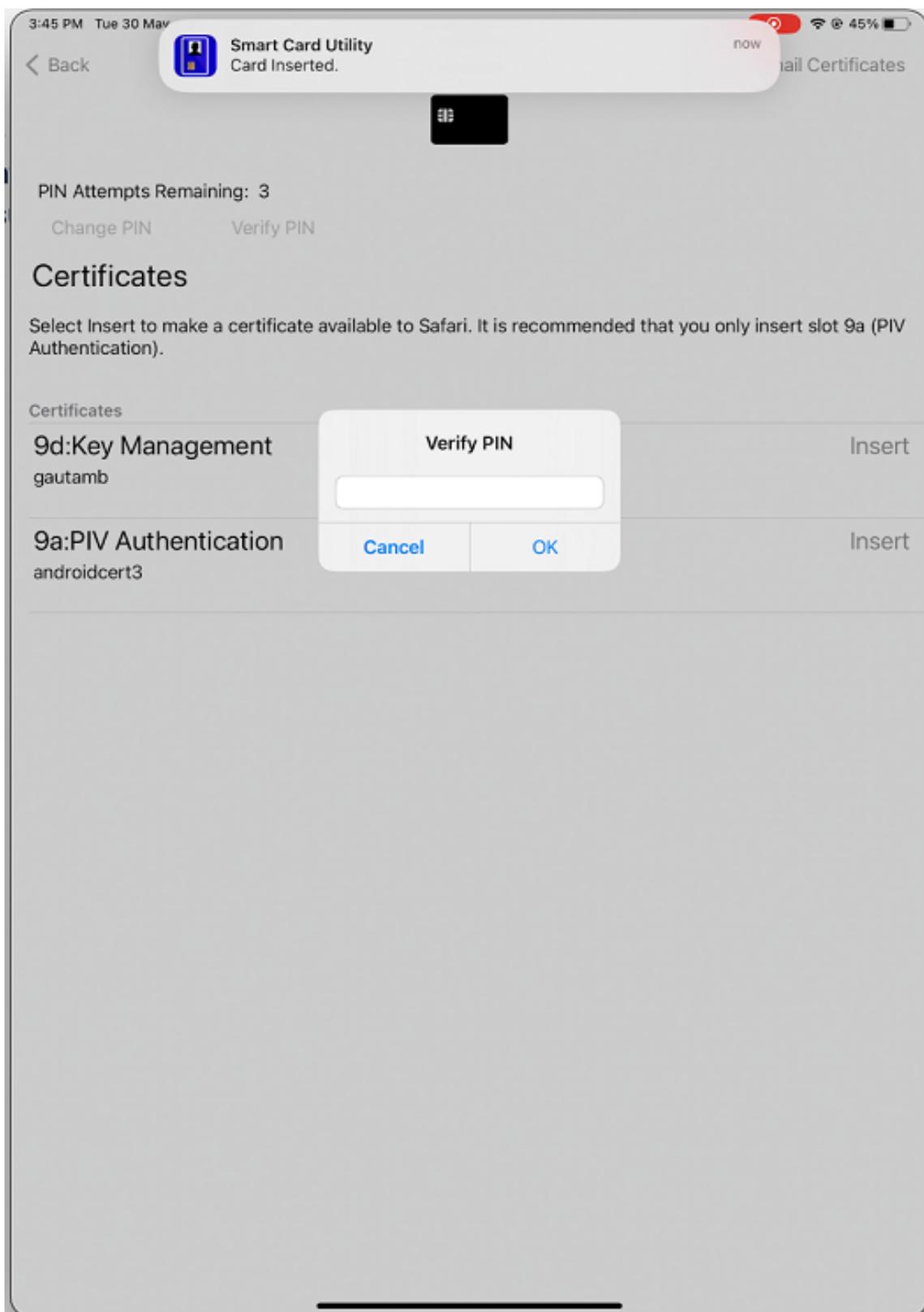
3. Smart Card Utility アプリを開きます。



- 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:

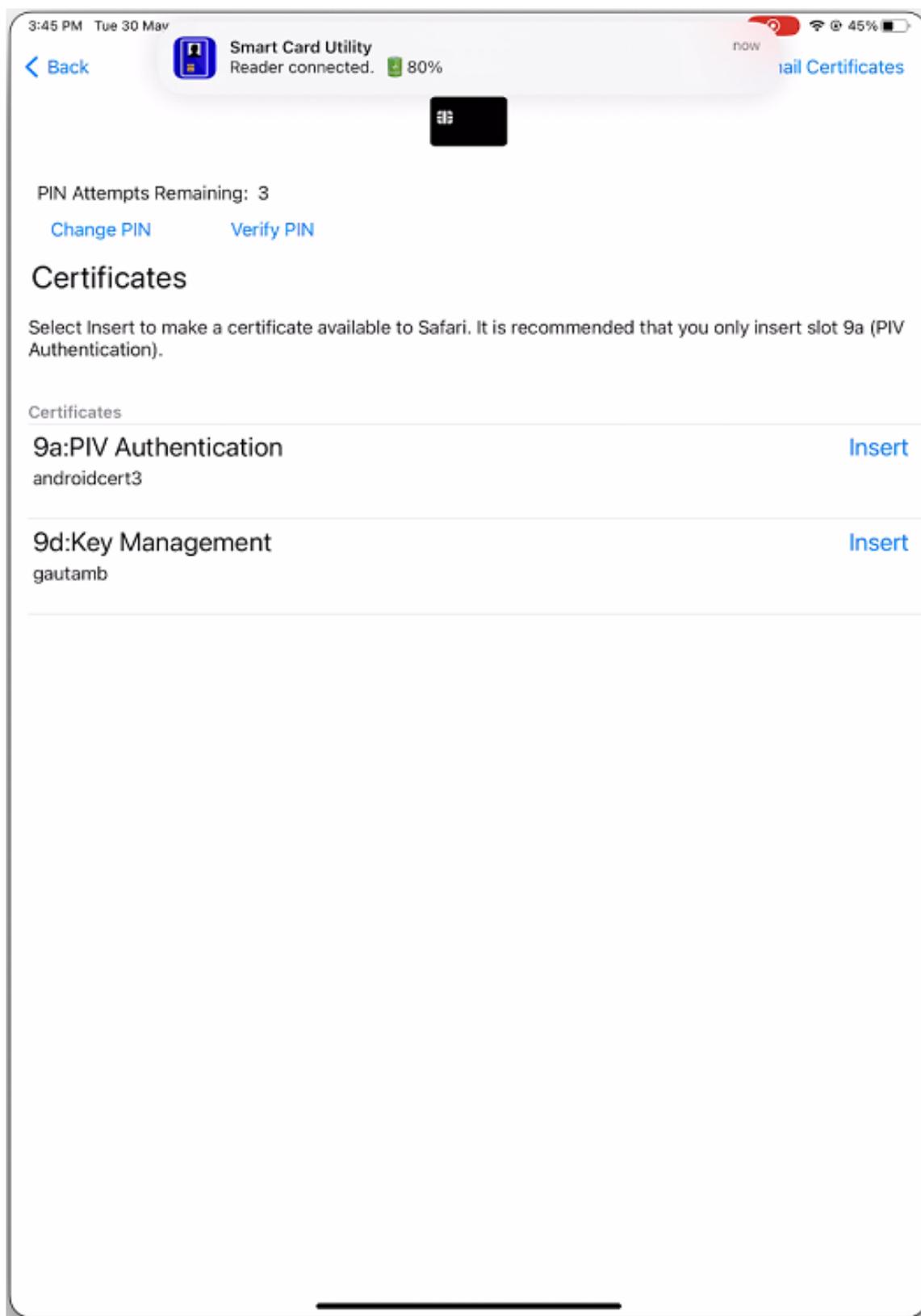
リーダーで PIN のペアリングが有効になっている場合は、プロンプトが表示されたら **PIN** を入力する必要があります。**PIN** はリーダーの背面にあります。



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

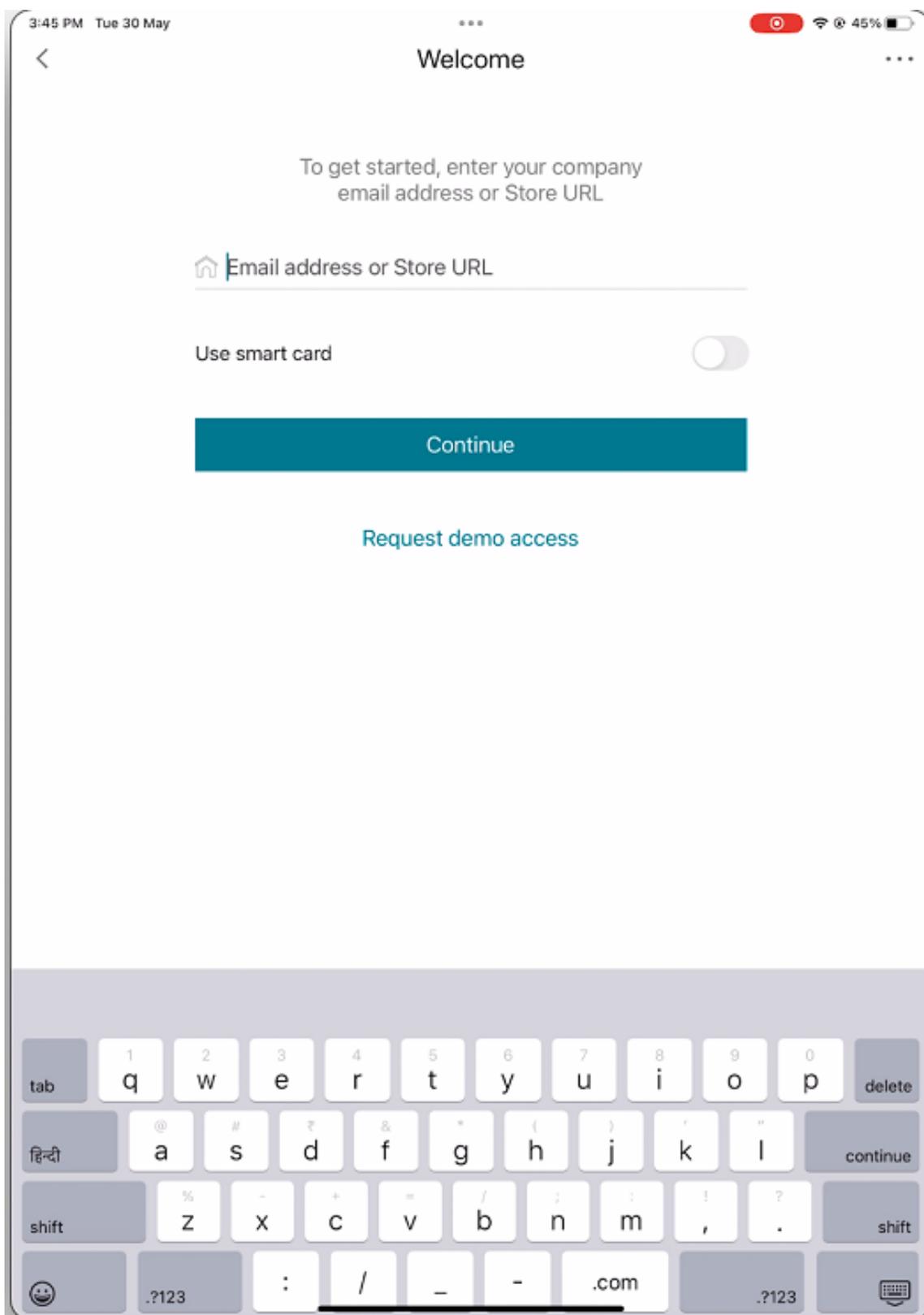
注:

Smart Card Utility アプリは、トークンの形式でキーチェーンのインターフェイスに証明書を書き込むために、Apple が提供する cryptokit 拡張機能を実装しています。詳しくは、Apple Developer ドキュメントの「[スマートカード認証の構成](#)」を参照してください。

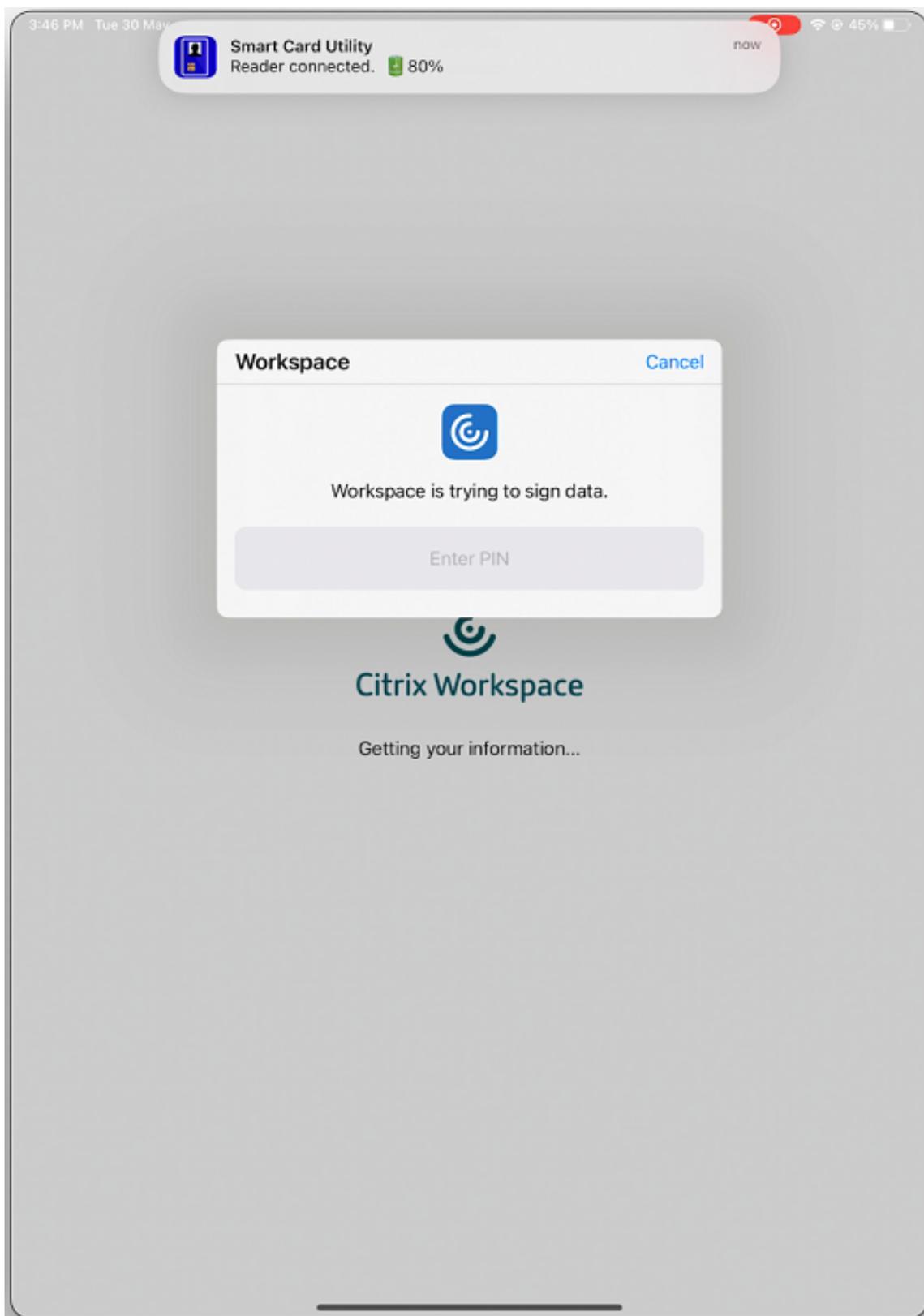


6. リーダーがデバイスに接続されたままであることを確認してください。

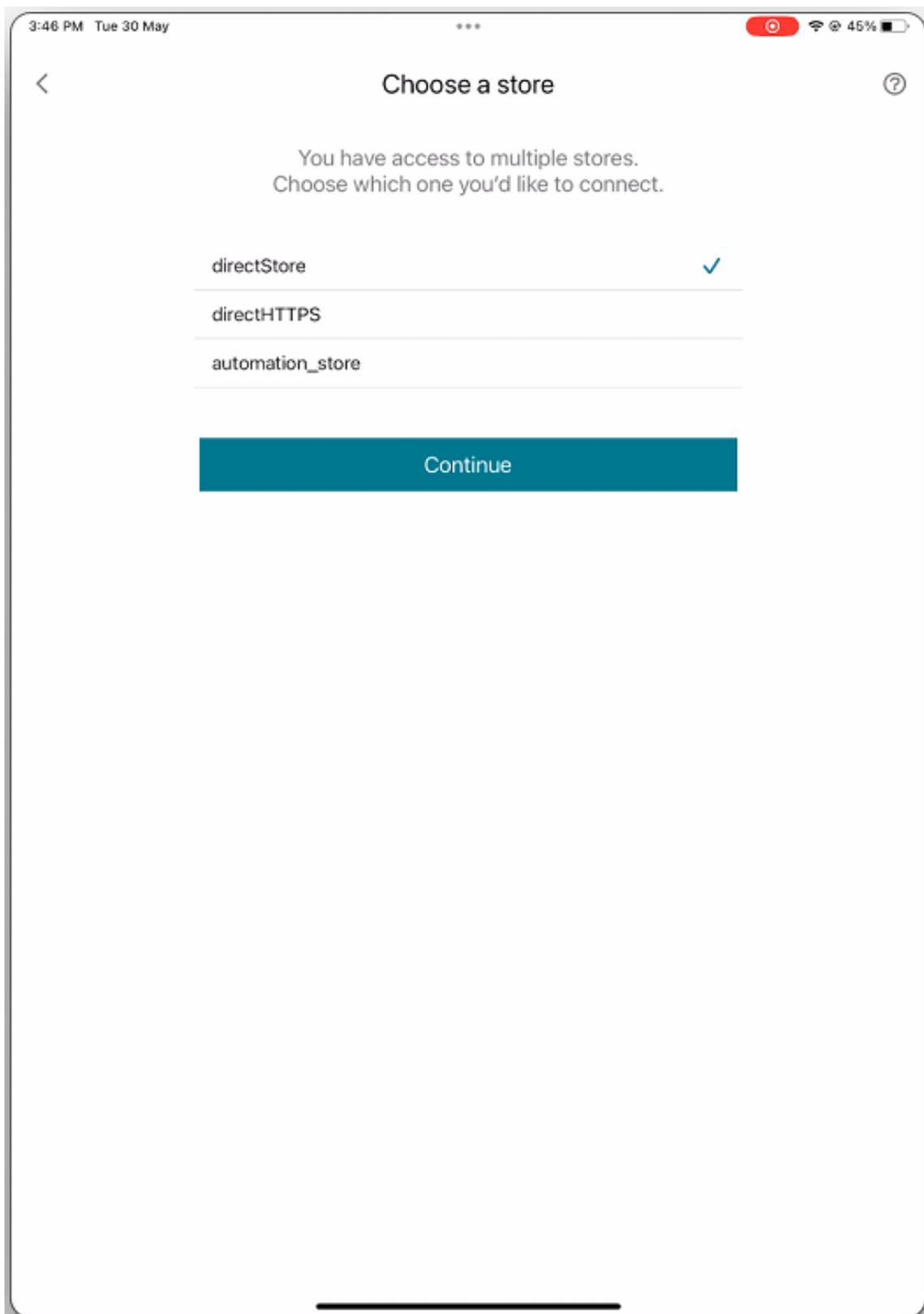
7. Citrix Workspace アプリを開き、スマートカード認証が構成されているストアの URL を入力します。



8. [Certificates] 画面で必要な証明書を選択し、IT 管理者から提供されたスマートカードの PIN を入力してサインインします。



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、[Continue] をタップします。



10. 認証が成功した後、Citrix Workspace アプリにサインインします。

### YubiKey によるスマートカード認証のサポート

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 アプリと、VDA セッションの仮想セッションおよび公開アプリに、単一デバイス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システムを接続する必要がなくなります。YubiKey は OTP、FIDO などの多様なプロトコルをサポートしており、エンドユーザーのエクスペリエンスを簡素化します。

Citrix Workspace アプリにサインインするために、エンドユーザーは iPhone または iPad に YubiKey を挿入し、スマートカードの切り替えをオンにして、ストア URL を指定する必要があります。

注:

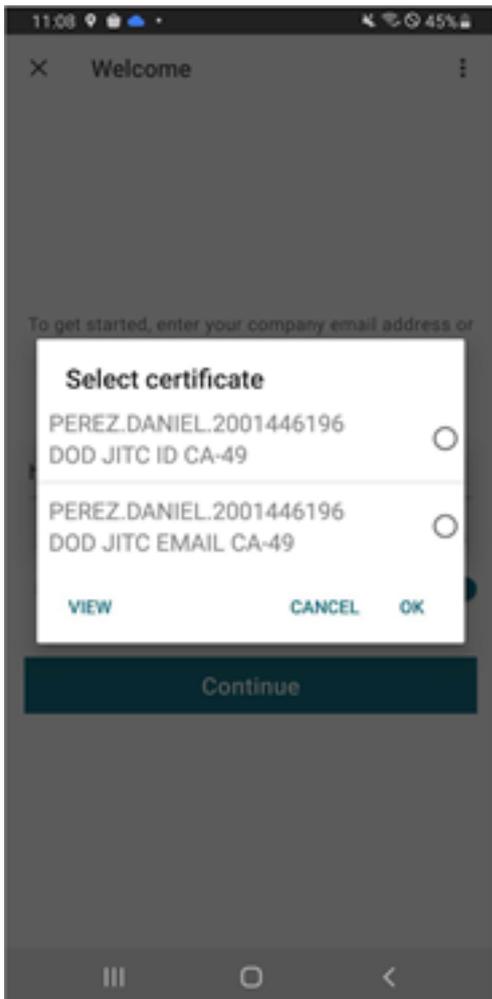
この機能は、StoreFront 展開上の Citrix Workspace アプリへの直接接続のみをサポートし、Citrix Gateway 経由ではサポートしません。Citrix Gateway 経由のスマートカード認証に対する YubiKey のサポートは、将来のリリースで利用可能になる予定です。

iOS 向け Citrix Workspace アプリは YubiKey 5 シリーズのみをサポートします。YubiKey について詳しくは、「[YubiKey 5 シリーズ](#)」を参照してください。

### スマートカード認証での複数の証明書のサポート

以前は、iOS 向け Citrix Workspace アプリでは、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が表示されていました。

バージョン 24.1.0 以降、iOS 向け Citrix Workspace アプリには、スマートカードで利用可能なすべての証明書が表示されます。この機能を使用すると、スマートカード認証による認証中に必要な証明書を選択できます。



## RSA SecurID 認証

Citrix Workspace アプリは、Citrix Secure Web Gateway の構成で RSA SecurID 認証をサポートします。構成は、Web Interface を介して行われ、すべての Citrix Gateway 構成に適用されます。

**iOS** 向け **Citrix Workspace** アプリのソフトウェアトークン用の **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により、URL スキーム「com.citrix.securid」のみが登録されます。

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たエンドユーザーは、URL スキーム「**com.citrix.securid**」を選択して Citrix Workspace アプリに RSA SecurID Software Authenticator (ソフトウェアトークン) をインポートする必要があります。

### RSA SecurID ソフトウェアトークンをインポートするには

Citrix Workspace アプリで RSA ソフトウェアトークンを管理者として使用するには、エンドユーザーが以下に従っていることを確認してください:

- PIN 長のポリシー
- PIN の種類（数字のみおよび英数字）
- PIN 再使用の制限

エンドユーザーが RSA サーバーに対して正常に認証された後、エンドユーザーは PIN を 1 回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。すべての検証後、Workspace アプリは、利用可能な公開アプリケーションと公開デスクトップを表示します。

#### **RSA** ソフトウェアトークンを使用するには

1. 組織から提供された RSA ソフトウェア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で、インポート先として [**Workspace** で開く] を選択します。ソフトウェアトークンがインポートされたら、Citrix Workspace アプリが自動的に開きます。
3. インポートを完了させるために組織によりパスワードが提供されている場合は、そのパスワードを入力して [**OK**] をクリックします。[**OK**] をクリックした後、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、資格情報を入力します：ユーザー名、パスワード、ドメイン。組織によって別のデフォルト PIN が指定されていない場合は、[PIN] に「0000」と入力します PIN 0000 は RSA のデフォルトですが、セキュリティポリシーに準拠させるため組織によって変更されていることがあります。
7. 左上の [ログオン] をクリックします。PIN の作成を促すメッセージが表示されます。
8. 4~8 文字の PIN を入力し [**OK**] をクリックします。新しい PIN を確認するメッセージが表示されます。
9. PIN をもう一度入力し、[**OK**] をクリックします。アプリやデスクトップにアクセスできるようになりました。

#### **Next Tokencode**

Citrix Gateway に RSA SecurID 認証を設定すると、Citrix Workspace アプリで Next Tokencode 機能がサポートされます。不正なパスワードを 3 回入力すると、Citrix Gateway Plug-in 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。ユーザーが不正なパスワードで何度もログオンしようとした場合に、そのユーザーのアカウントが無効になるように RSA サーバーを設定できます。

#### 派生資格情報

Citrix Workspace アプリでは、Purebred による派生資格情報がサポートされています。派生資格情報を使用できるストアに接続するときに、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、オンプレミス展開のみでサポートされます。

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。

派生資格情報とともに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. 表示された仮想スマートカードの名前を編集します。
3. 数字のみ 8 桁の PIN を入力し、確定します。
4. [次へ] をタップします。
5. [認証証明書] 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] で、[Purebred Key Chain] を選択します。
8. 一覧から、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. 手順 5~9 を繰り返して、デジタル署名証明書と暗号化証明書をインポートします (必要な場合)。
11. [保存] をタップします。

証明書は、仮想スマートカードに最大 3 つまでインポートできます。仮想スマートカードが正しく動作するには、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 セッション内で使用するために追加することができます。

注:

HDX セッションに接続する場合は、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、有効なカードを一度に 1 つだけ保持することができます。
- 仮想スマートカードは、いったん作成すると編集することができません。削除してからカードを作成します。
- 無効な PIN は、10 回まで入力できます。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。

**WKWebView** のユーザーエージェント文字列

WKWebView を介して開始された一部のネットワーク要求で使用される user-agent 文字列に、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。

したがって、次のように変更されました。変更前:

```
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
```

変更後 (以下のいずれか):

```
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、アクセス権を付与するために複数の ID をユーザーに要求することで、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、管理者が認証手順および関連する資格情報コレクションフォームを構成できます。

ネイティブの Citrix Workspace アプリは、既に StoreFront に実装されているフォームによるログオンのサポートを構築することで、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 ログオンページでも、このプロトコルを使用します。

詳しくは、「[SAML 認証](#)」および「[nFactor 認証](#)」を参照してください。

制限事項:

- nFactor サポートを有効にすると、Touch ID や Face ID などの生体認証を使用できなくなります。

### nFactor 高度認証ポリシーのサポート

Citrix Gateway で nFactor 高度認証ポリシーを使用して構成する場合、Citrix Workspace アプリで証明書ベースの認証がサポートされるようになりました。nFactor 認証により、柔軟でアジャイルな多要素スキーマを構成できます。

**user-agent** 文字列:

iPhone または iPad で Citrix Workspace アプリに対して高度な (nFactor) 認証を実行すると、認証プロセスは埋め込まれた WebView にリダイレクトされます。表示さ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 バージョンに基づいて若干異なる場合があります。たとえば、iPhone と iPad のユーザーエージェント文字列は、以下のように異なります。

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
```

この機能はプレビュー段階です。[Podio リンク](#)を使用するか、Citrix テクニカルサポートに連絡して、リクエストすることで有効にできます。ただし最終的には、プレビュー段階が終了した後にすべてのお客様にロールアウトされます。

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 向け 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、次のキーワードを利用します:
  - iOS
  - CWA
  - CWA 対応

## HDX セッションへの接続時に FIDO2 ベースの認証をサポート

iOS 向け 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なしの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、パスワードなしの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)。パスワードなしの認証を使用した 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。

前提条件について詳しくは、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で **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 Citrix Workspace アプリに認証するときに、FIDO2 ベースのパスワードなしの認証を利用してクラウドストアに接続できます。FIDO2 はシームレスな認証方法を提供し、企業の従業員がユーザー名やパスワードを入力しなくても、仮想セッション内で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、ローミング認証システム（USB のみ）とプラットフォーム認証システム（PIN コード、Touch ID、Face ID のみ）の両方をサポートします。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、Chrome のカスタムタブでデフォルトでサポートされています。WebView で FIDO2 認証を使用することの詳細について興味を持たれた場合は、この [Podio フォーム](#) を使用して登録していただくようお願いいたします。

## オンプレミス展開での認証トークンの保存の構成をサポート

iOS 向け Citrix Workspace アプリは、ローカルディスクでオンプレミスストアの認証トークンの保存を構成するオプションを提供するようになりました。この機能を使用すると、認証トークンの保存を無効にして、セキュリティを強化することができます。無効にした後、システムまたはセッションが再起動されると、セッションにアクセスするには再度認証が必要になります。

管理構成ファイルを使用してオンプレミス展開で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って `web.config` ファイルを開きます。このファイルは通常、`C:\inetpub\wwwroot\Citrix\Roaming directory` にあります。
2. このファイルで、ユーザーアカウント要素の場所を見つめます（「Store」は使用環境のアカウント名です）。  
例: `<account id=... name="Store">`
3. `</account>` タグの前にあるユーザーアカウントのプロパティに移動し、次の内容を追加します:

```
1 <properties>
2   <property name="TokenPersistence" value="false" />
3 </properties>
4 <!--NeedCopy-->
```

次に示すのは、`web.config` ファイルの例です:

```
1 <account id="#####" name="Store
2   Service"
3   description="" published="true" updatertype="None"
4   remoteAccessType="StoresOnly">
5   <annotatedServices>
6     <clear />
7     <annotatedServiceRecord serviceRef="1__Citrix_Store">
8       <metadata>
9         <plugins>
10          <clear />
11        </plugins>
```

```
10         <trustSettings>
11             <clear />
12         </trustSettings>
13         <properties>
14             <clear />
15             <property name="TokenPersistence" value="false"
16                 />
17         </properties>
18     </annotatedServiceRecord>
19 </annotatedServices>
20 <metadata>
21 <plugins>
22     <clear />
23 </plugins>
24 <trustSettings>
25     <clear />
26 </trustSettings>
27 <properties>
28 </properties>
29 </metadata>
30 </account>
31 <!--NeedCopy-->
```

## セキュリティ

January 9, 2024

サーバーファームと Citrix Workspace アプリ間の通信をセキュリティ保護するには、使用している接続を、Citrix Gateway などの一連のセキュリティ技術と統合します。

注:

StoreFront サーバーとユーザーデバイス間の通信を保護するには、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）。

プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Citrix Workspace アプリとサーバー間の接続を制御できます。Citrix Workspace アプリは、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。

- Secure Web Gateway。

Secure Web Gateway を Web Interface と一緒に使うと、社内ネットワーク上のサーバーにインターネットを介して接続できる、暗号化されたセキュアな単一のアクセスポイントをユーザーに提供できます。

Secure Web Gateway と Web Interface を使用して、単一のセキュアな暗号化されたデータを提供できます。企業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セキュリティ保護されたデータにアクセスできます。

- Transport Layer Security (TLS) プロトコルによる SSL Relay 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、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。

サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（ネットワークアドレス変換））を介して Citrix Workspace アプリを使用する場合は、外部アドレスを構成します。

## Citrix Gateway

リモートのユーザーが Citrix Gateway を介して Citrix Endpoint Management 環境に接続できるようにするには、StoreFront と通信するように証明書を構成します。このアクセスを有効にする方法は、Citrix Endpoint Management のエディションによって異なります。

ネットワークで Citrix Endpoint Management を展開する場合、Citrix Gateway と StoreFront を統合することで Citrix Gateway を経由して内部ユーザーやリモートユーザーが StoreFront に接続できます。ユーザーは、StoreFront に接続して XenApp の公開アプリケーションや XenDesktop の仮想デスクトップにアクセスします。ユーザーは、Citrix Workspace アプリを使用して接続を行います。

## Secure Web Gateway

このトピックの内容は、Web Interface 環境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のどちらかで使用して、Citrix Workspace アプリとサーバーの間に保護された通信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は、Citrix Workspace アプリ側での構成は不要です。エンドユーザーが Web Interface を使用して接続していることを確認します。

Citrix Workspace アプリが Secure Web Gateway サーバーに接続するときは、リモートの Web Interface サーバーで構成されている設定が使用されます。

Secure Web Gateway Proxy がセキュリティで保護された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は、Secure Web Gateway Proxy をリレーモードで使用できます。ただし、リレーモードで使用する場合、Secure Web Gateway サーバーはプロキシサーバーとして機能するため、Citrix Workspace アプリで次の項目を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 では、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の 3 つの要素を順に指定する必要があります:

- ホスト名
- サブドメイン名
- 最上位ドメイン名

たとえば、`my_computer.example.com` は完全修飾ドメイン名です。ホスト名 (`my_computer`)、サブドメイン名 (`example`)、最上位ドメイン名 (`com`) が順に指定されています。サブドメイン名と最上位ドメイン名の組み合わせ (`example.com`) をドメイン名といいます。

### プロキシサーバー

プロキシサーバーは、ネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Citrix Workspace アプリとサーバー間の接続を制御するために使います。Citrix Workspace アプリは、SOCKS プロトコル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 アプリで Citrix Virtual Apps and Desktops サーバーと通信する場合、プロキシサーバー設定が使用されます。プロキシサーバー設定は、Web Interface サーバーでリモートで構成されます。

Citrix Workspace アプリが Web サーバーと通信する場合、プロキシサーバー設定を使用します。各ユーザーデバイス上のデフォルトの Web ブラウザーで、プロキシサーバー設定を構成します。

### ファイアウォール

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。ファイアウォールが使用されている環境では、Citrix Workspace アプリと Web サーバーおよび Citrix 製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。ユーザーデバイスから Web サーバーへの通信のため、ファイアウォールで 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 を経由します。また、Citrix 製品サーバーの通信では、ポート 1494 とポート 2598 の受信 ICA トラフィックがファイアウォールを通過できるように設定します。

ファイアウォールによるネットワークアドレス変換 (NAT: Network Address Translation) を使用している場合は、Web Interface を使っ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 (Citrix Virtual Apps and Desktops サービスの新名称) のサーバーに代替アドレスが設定されていない場合は、Web Interface から iOS 向け Citrix Workspace アプリに代替アドレスが提供されるように設定できます。これにより、iOS 向け Citrix Workspace アプリでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。

## TLS

Citrix Workspace アプリは XenApp および XenDesktop との TLS 接続に、以下の暗号の組み合わせを使用した TLS 1.0、1.1、1.2 をサポートします：

- 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 以降で実行されている Citrix Workspace アプリまたはバージョン 21.2.0 は、以下の暗号の組み合わせをサポートしません：

- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5

Transport Layer Security (TLS) は、SSL プロトコルの最新の標準化バージョンです。IETF (Internet Engineering TaskForce) が、TLS の公開標準規格の開発を Netscape Communications から引き継いだときに、SSL という名前を TLS に変更しました。

TLS は、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信をセキュアに保護します。米国政府機関をはじめとする組織の中には、データ通信を保護するために TLS の使用を義務付けているところもあります。このような組織では、さらに FIPS 140 (Federal Information Processing Standard) などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140 は、暗号化の情報処理規格です。

Citrix Workspace アプリは、ビット長 1024、2048 および、3072 の RSA キーをサポートします。さらに、ビット長 4096 の RSA キーを持つルート証明書がサポートされます。

注：

- Citrix Workspace アプリは、プラットフォーム (iOS) の暗号化機能を Citrix Workspace アプリと StoreFront の接続に使用します。

### TLS の構成および有効化

TLS のセットアップは、以下の 2 つの手順で行います：

1. Citrix Virtual Apps and Desktops サーバーおよび Web Interface サーバー上で SSL Relay をセットアップし、必要なサーバー証明書を入手してインストールします。
2. ユーザーデバイス上で、ルート証明書をインストールします。

ユーザーデバイスへのルート証明書のインストール TLS 機能が有効になっている Citrix Workspace アプリと Citrix Virtual Apps and Desktops 間の通信をセキュアに保護するには、ルート証明書がユーザーデバイスにインストールされている必要があります。このルート証明書は、サーバー証明書上の証明機関の署名を検証できます。

iOS には、何百もの商用ルート証明書がプリインストールされています。それ以外の証明書を使用する場合は、該当する証明機関からルート証明書を購入して、各ユーザーデバイスにインストールする必要があります。

組織の方針によっては、デバイスへのルート証明書のインストールはエンドユーザーではなく管理者が行うことができる場合があります。ルート証明書を簡単および確実にインストールするには、iOS のキーチェーンにその証明書を追加します。

ルート証明書をキーチェーンに追加するには

1. 証明書ファイルをメール添付で自分に送信します。
2. 証明書ファイルをデバイスで開きます。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 を起動して iOS の [設定] > [情報] > [証明書信頼設定] から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] で、[ルート証明書の完全な信頼を有効にする] のセクションを参照します。証明書が完全に信頼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 が有効なクライアントおよび他のアプリケーションは、TLS でルート証明書を使用できます。

## XenApp および 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、1 要素認証のみをサポートします。
- Citrix Virtual Apps Web サイトは、1 要素認証と 2 要素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 をサポートします。

この構成を実行する前に、Citrix Gateway をインストールして Web Interface と連動するように構成します。これらの手順は運用環境に合わせて適宜変更できます。

Citrix Secure Gateway 接続を使用する環境では、Citrix Workspace アプリ上で Citrix Gateway オプションを構成しないでください。

Citrix Workspace アプリでは、そのユーザーがアクセスできるアプリケーションの情報を XenApp および XenDesktop サイトから取得します。その過程で、デバイス上で実行中の Citrix Workspace アプリに情報が表示されます。同様に、従来の SSL ベースの Citrix Virtual Apps 接続に 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 上で動作する 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 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]** の順に選択します。
2. [Access Method] を **[Gateway Direct]** に変更します。
3. Secure Web Gateway の完全修飾ドメイン名 (FQDN) を入力します。
4. Secure Ticket Authority (STA) の情報を入力します。

注：

Citrix Secure Gateway の場合、Citrix 定義のデフォルトのパス (`//XenAppServerName/Citrix/PNAgent`) を使用することをお勧めします。デフォルトのパスを使用すると、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を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に対応します。

間接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、ウィザードを進めます。

2. ユーザーデバイスからの接続をテストして、Secure Web Gateway のネットワークと証明書の割り当てが正しく設定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場合、[アドレス] フィールドに一致する Citrix Secure Gateway サーバーの FQDN を入力します：
  - 既定のパス (`/Citrix/PNAgent`) を使って XenApp および XenDesktop サイトを作成した場合は、Secure Web Gateway の FQDN を次のように入力します。 `FQDNofSecureGateway.companyName.com`

- 既定のパスを使わず 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 ファイルへのパスを、次のように入力します。FQDNofSecureGateway.companyName.com/CustomPath/config.xml
2. アカウントを手動で構成する場合は、Citrix Gateway オプションの [新規アカウント] ダイアログをオフにします。

## トラブルシューティング

March 27, 2024

### 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。



24.1.0.10 (2401)

© 1990-2024 Cloud Software Group, Inc.  
All Rights Reserved.

[Third Party Notices](#)

[User Agreements](#)



## **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 で 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。

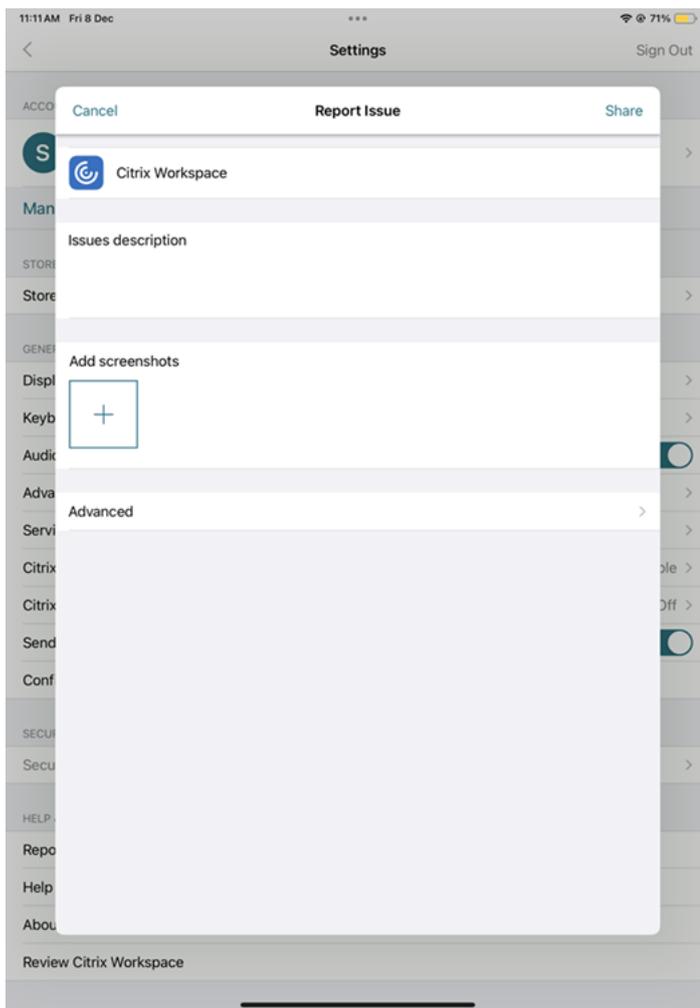
## **Citrix Workspace** アプリをリセットする方法

次のいずれかの方法で Citrix Workspace アプリをリセットできます。

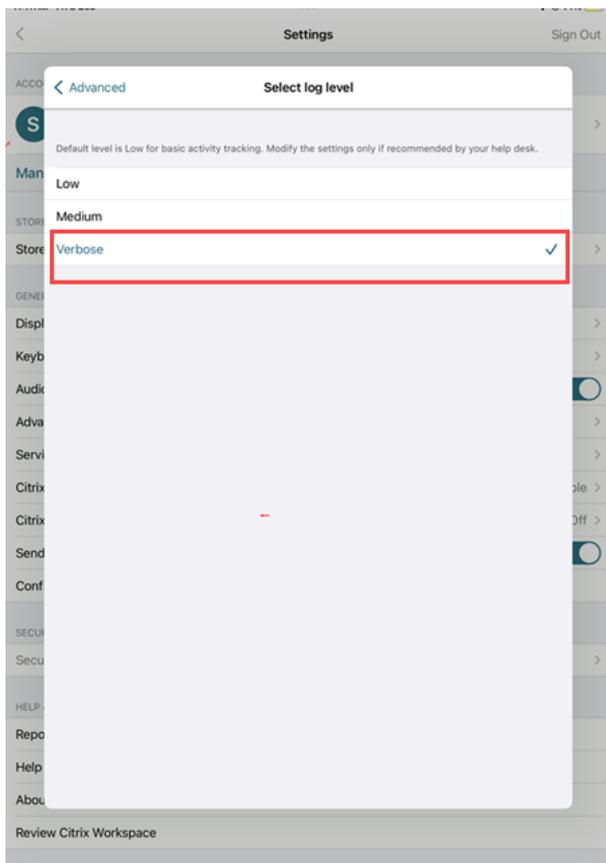
- Citrix Workspace アプリから既存のアカウントを削除します
- Citrix Workspace アプリのストレージデータをクリアします。
- Citrix Workspace アプリをアンインストールし、最新の修正が適用された最新の iOS 向け Citrix Workspace アプリをインストールします。

## ログを収集する方法

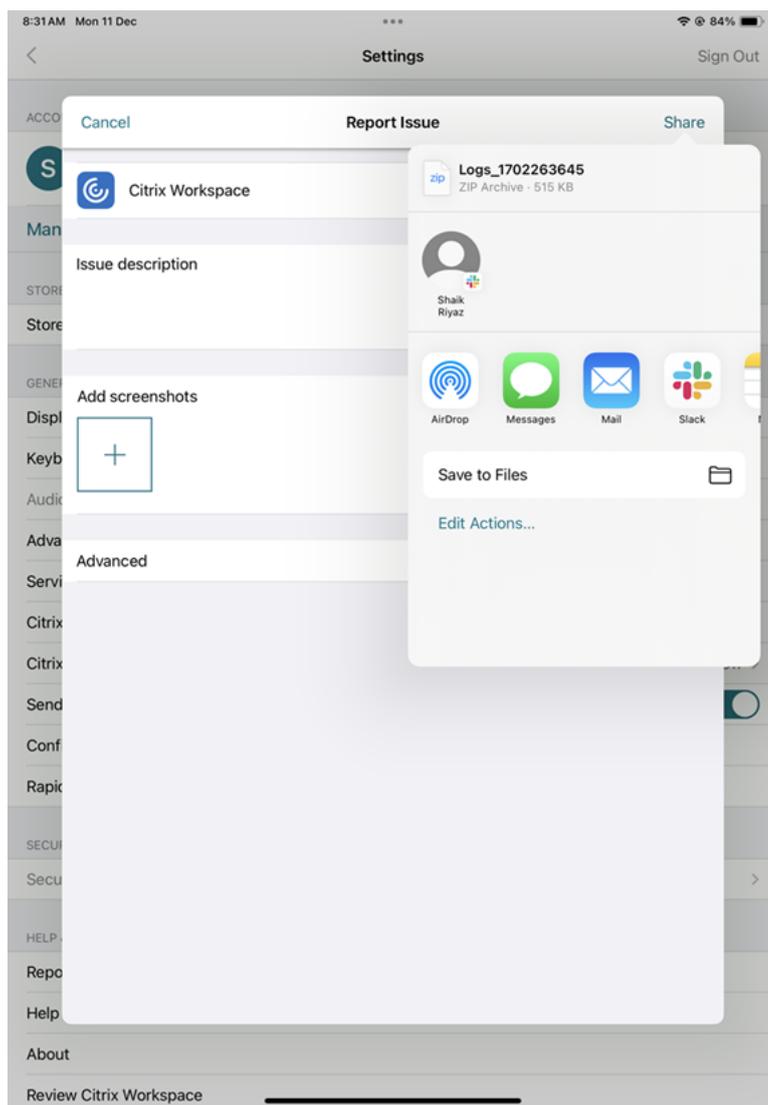
1. Citrix Workspace アプリを開き、[設定] に移動します。
2. [ヘルプとサポート] で、[問題の報告] を選択します。



3. 問題を再現します。
4. [ログレベルの選択] ページで [詳細] を選択します。



5. [ログの場所の選択] 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。



### 機能拡張のリクエスト方法

[このフォーム](#)に記入して機能拡張のリクエストを送信できます。

### Technical Preview 機能にアクセスする方法

各機能に固有の Podio フォームを使用して、Technical Preview 機能を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 Technical Preview の情報に添付されています。

### EAR のフィードバックを提供する方法

EAR バージョンに関するフィードバックを提供するには、[こちら](#)をタップしてください。

### よくある問題とトラブルシューティングのヒント

#### セッションの切断

ユーザーが以下の操作を行うと、iOS 向け Citrix Workspace アプリセッションを終了せずに切断できます：

- セッションで公開アプリまたはデスクトップを表示している間に次のことを実行する：
  - 画面を上部で矢印をタップして、セッションのドロップダウンメニューを表示させる。
  - [ホーム] ボタンをタップして、起動パッドに戻る。
  - アクティブなセッションに残っている公開アプリのいずれかのアイコンの下にある白い影をタップする。
  - 切断をタップする。
- iOS 向け Citrix Workspace アプリを終了する：
  - デバイスの [ホーム] ボタンをダブルタップする。
  - iOS App Switcher ビューで、iOS 向け Citrix Workspace アプリを探す。
  - 表示されるダイアログで切断をタップする。
- 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内の [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。ユーザーは切断セッションに再接続できますが、管理者は特定の時間が経過した後に切断セッションが非アクティブとして表示されてい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サーバーの構成（「ターミナルサービス構成」の新名称）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（「ターミナルサービス」の新名称）の設定について詳しくは、Microsoft Windows Server の製品ドキュメントを参照してください。

#### 有効期限が切れたパスワード

iOS 向け Citrix Workspace アプリでは、有効期限が切れたパスワードをユーザーが変更することができます。パスワードの有効期限が切れると、必要な情報を入力するためのメッセージが表示されます。

#### ジェイルブレイクされたデバイス

ユーザーがジェイルブレイクされた iOS デバイスで接続することにより、展開環境のセキュリティを侵害する可能性があります。ジェイルブレイクしたデバイスとは、所有者によりセキュリティ権限が変更され、一般的には特定のセキュリティ保護機能をバイパスするようになっているデバイスです。

iOS 向け Citrix Workspace アプリでジェイルブレイクされた iOS が検出されると、ユーザーに通知が表示されません。

環境のセキュリティをさらに保護する野に役立てるため、StoreFront または Web Interface を構成して、検出したジェイルブレイクされたデバイスでアプリを実行できないようにすることができます。

#### 要件

- Citrix Receiver for iOS 6.1 以降
- StoreFront 3.0 または Web Interface 5.4 以降
- StoreFront または Web Interface への管理者アカウントによるアクセス

検出したジェイルブレイクされたデバイスでアプリを実行できないようにするには

1. StoreFront または Web Interface サーバーに管理者特権を持つユーザーとしてログオンします。
2. ファイル **default.ica** を見つけます。このファイルは以下のいずれかの場所にあります：
  - `C:\inetpub\wwwroot\Citrix\*storename*\conf` (Microsoft インターネットインフォメーションサービス)
  - `C:\inetpub\wwwroot\Citrix\*storename*\App\_Data` (Microsoft インターネットインフォメーションサービス)
  - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. **[Application]** セクションに以下の行を追加します。 **AllowJailBrokenDevices=OFF**
4. ファイルを保存して StoreFront または Web Interface サーバーを再起動します。

StoreFront サーバーを再起動した後は、ジェイルブレイクされたデバイスについての通知を受け取ったユーザーは StoreFront または Web Interface サーバーからアプリを起動できません。

検出したジェイルブレイクされたデバイスでアプリを実行できるようにするには `AllowJailBrokenDevices` を設定しなければ、デフォルトの動作ではジェイルブレイクされたデバイスについてユーザーに通知が表示されますが、依然としてアプリケーションを起動が許可されます。

ジェイルブレイクされたデバイスでのアプリの実行をユーザーに明確に許可するには、次の手順に従います：

1. StoreFront または Web Interface サーバーに管理者特権を持つユーザーとしてログオンします。
2. `default.ica` ファイルを見つけてみます。このファイルは以下のいずれかの場所にあります：
  - `C:\inetpub\wwwroot\Citrix\*storename*\conf` (Microsoft インターネットインフォメーションサービス)
  - `C:\inetpub\wwwroot\Citrix\*storename*\App\_Data` (Microsoft インターネットインフォメーションサービス)
  - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. **[Application]** セクションに以下の行を追加します。 **AllowJailBrokenDevices=ON**

4. ファイルを保存して StoreFront または Web Interface サーバーを再起動します。

AllowJailBrokenDevices を ON に設定すると、ユーザーはジェイルブレイクされたデバイスについて通知を受け取りますが、StoreFront または Web Interface サーバー経由でアプリケーションを実行できます。

#### **HDX** の音質の低下

iOS 向け Citrix Workspace アプリを使用した Citrix Virtual Apps and Desktops および Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) のセッションで、音質が低下することがあります。この問題は、音声と動画を同時に使用すると発生します。

この問題は、Citrix Virtual Apps and Desktops および Citrix DaaS の HDX に関連するポリシーが音声と動画のデータ量に対応できない場合に発生します。

音質を改善するためのポリシー作成については、Knowledge Center の[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で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

ストアエクスペリエンスをカスタマイズしている場合、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場合があります。ストアの種類の自動検出は、メールアドレスでのみサポートされており、ストア URL で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 Interface のログインモードを使用することをお勧めします。詳しくは、「[手動セットアップ](#)」および「[メールアドレスによるアカウント検出を構成する](#)」を参照してください。

Web Interface のログインモード経由でアカウントを手動で設定するには、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 (+) の順にタップします。[新規アカウント] 画面が開きます。
2. 画面左下の [オプション] の左側のアイコンをタップして、[手動セットアップ] をタップします。画面に他のフィールドが表示されます。
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 (agee.mycompany.com など) を入力します。
4. **Web Interface** 接続を選択します。この接続モードでは、Web ブラウザーに似た Citrix Virtual Apps 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。

1:50 PM Tue 19 Mar 37%

[Cancel](#) **New Account** [Save](#)

---

**Address** `https://ag.cldblr.com`

---

**Description** WI Store

---

**Auto-Configure**

---

**Web Interface**

---

**XenApp Services**

---

**Access Gateway**

---

**Ignore certificate warnings**

---

[Help & Support](#)

5. [証明書の警告を無視] で、無効、自己署名、または期限切れの証明書を無視してサーバーに接続するかどうかを指定します。デフォルトでは、[オフ] になっています。

**重要:**

このオプションをオンにする場合は、常に接続先のサーバーが正しいかどうかを確認してください。ユ

ユーザーのデバイスを不正な攻撃から守るため、Citrix ではすべてのサーバー上に有効な証明書をインストールしておくことを強くお勧めします。証明機関から入手した SSL 証明書を使用すると、サーバーのセキュリティが向上します。自己署名入りの証明書を使用したり、証明書を使用しなかったりすることは Citrix では推奨されません。

6. [保存] をタップします。

7. ユーザー名およびパスワード（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。iOS 向け Citrix Workspace アプリの画面が開き、デスクトップにアクセスしたり、アプリを追加および実行したりできます。

注:

ユーザーの資格情報は Web Interface のログインモードでは保存されないため、接続ごとに入力する必要があります。

### よくある質問

低電力またはモバイルデバイスの仮想アプリと仮想デスクトップで、ビデオのパフォーマンスを向上させるにはどうすればよいですか？

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改善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** アプリにサインインした後、アプリまたはデスクトップが表示されません

さらにサポートが必要な場合は、会社のヘルプデスクまたは IT サポートチーム管理者にお問い合わせください。

### 接続の遅さをトラブルシューティングする方法

次の問題のいずれかが発生した場合は、次の「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
- アプリアイコンが見つからない
- プロトコルドライバのエラーメッセージが繰り返し表示される

回避方法 Citrix Virtual Apps サーバー、Citrix Secure Web Gateway、および Web Interface サーバー上のネットワークインターフェイスの Citrix PV イーサネットアダプターのプロパティを無効にします。

Citrix PV イーサネット アダプターのプロパティには、デフォルトで有効になっている次のプロパティが含まれています。これらのプロパティをすべて無効にする必要があります。

- 大量送信オフロード
- 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

注:

サーバーの再起動は必要ありません。この回避策は、Windows Server 2003 および Windows Server 2008 (32 ビット) で使用できます。Windows Server 2008 R2 では、この問題は発生しません。

### 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 IME での中国語の文字入力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] > [キーボードのオプション] 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

July 1, 2024

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。これによって、Citrix Virtual Apps and Desktops が配信する仮想デスクトップおよびホストされるアプリケーションにアクセスし、これらを実行できるようになります。

iOS は、iPad や iPhone などの Apple モバイルデバイス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 などの、iOS オペレーティングシステムを使ったデバイスで実行することができます。

### 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。

### 廃止

この記事の告知は、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止されるプラットフォーム、Citrix 製品、機能について前もってお知らせするためのものです。Citrix ではお客様の使用状況とフィードバックをチェッ

くして、各プラットフォーム、Citrix 製品、機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。

廃止となったアイテムはすぐには削除されません。このリリースでは引き続きサポートされますが、今後削除される予定です。

アイテム	廃止が発表されたリリース	削除されたリリース	代替手段
DTLS 1.0 プロトコルのサポート	iOS 向け Citrix Workspace アプリバージョン 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	iOS 向け Citrix Workspace アプリバージョン 24.4.0	-	TLS 1.2 または TLS 1.3 プロトコル
XenApp Services (PNAgent と呼ばれる)	iOS 向け Citrix Workspace アプリバージョン 23.7.5	-	Citrix Workspace アプリ内で、XenApp Services の URL ではなくストア URL を使用してストアに接続します。
iOS オペレーティングシステムバージョン 14	iOS 向け Citrix Workspace アプリバージョン 23.10.0	予定: iOS 向け Citrix Workspace アプリバージョン 23.12.0	iOS の利用可能な最新バージョンにアップグレードする
iOS オペレーティングシステムバージョン 13.x	iOS 向け Citrix Workspace アプリバージョン 22.9.5	予定: 2022 年 12 月、バージョン 22.12.0	iOS の利用可能な最新バージョンにアップグレードする
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	iOS 向け Citrix Workspace アプリバージョン 21.12.0	予定: 2022 年 8 月、バージョン 22.8.0	iOS の利用可能な最新バージョンにアップグレードする
iOS オペレーティングシステムバージョン 10.x	iOS 向け Citrix Workspace アプリバージョン 21.1.5	21.1.5 以降のリリース	iOS 向け Citrix Workspace アプリバージョン 21.1.5 以前を使用する

メモ:

- 廃止プラットフォームバージョンで Citrix Workspace アプリを使用している既存ユーザーは、Citrix Workspace アプリを (App Store から) 最新リリースにアップグレードできません。
- 廃止プラットフォームバージョンで Citrix Workspace アプリを使用している新規ユーザーは、App Store から互換性のある古いバージョンのみをダウンロードできます。
- 廃止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 アプリのすべての新しいリリースに含まれる新機能やセキュリティパッチを入手できません。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).