citrix

Secure Web

Contents

Secure Web の新機能

September 15, 2021

> 注:
>
> Android 6.x および iOS 11.x バージョンの Secure Hub、Secure Mail、Secure Web、Citrix Workspace アプリのサポートは、2020 年 6 月に廃止されます。

最新バージョンの新機能

Secure Web 21.9.0

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web for Android

このリリースには、バグの修正が含まれています。

以前のバージョンの新機能

Secure Web 21.8.5

Secure Web for Android

既に登録されているデバイスで **Android 12 Beta 4** を使用できます。Secure Web は Android 12 Beta 4 をサポートするようになりました。Android 12 Beta 4 へのアップグレードを検討している場合は、最初に Secure Hub をバージョン 21.7.1 に更新してください。Secure Hub 21.7.1 は、Android 12 Beta 4 にアップグレードするために必要な最小バージョンです。このリリースでは、既に登録されているユーザーが Android 11 から Android 12 Beta 4 にシームレスにアップグレードできるようになっています。

> 注:
>
> Citrix は、Android 12 について Day 1 サポートの提供を約束しており、Secure Web の後続のバージョンにさらに更新を追加していき、Android 12 を完全にサポートします。

Secure Web 21.8.0

> 注:
>
> このバージョンの Secure Web は、iOS 12.1 以降でのみサポートされています。iOS バージョン 12 以前のデバイスで実行されている Secure Web のアップデートは利用できません。

Secure Web for iOS

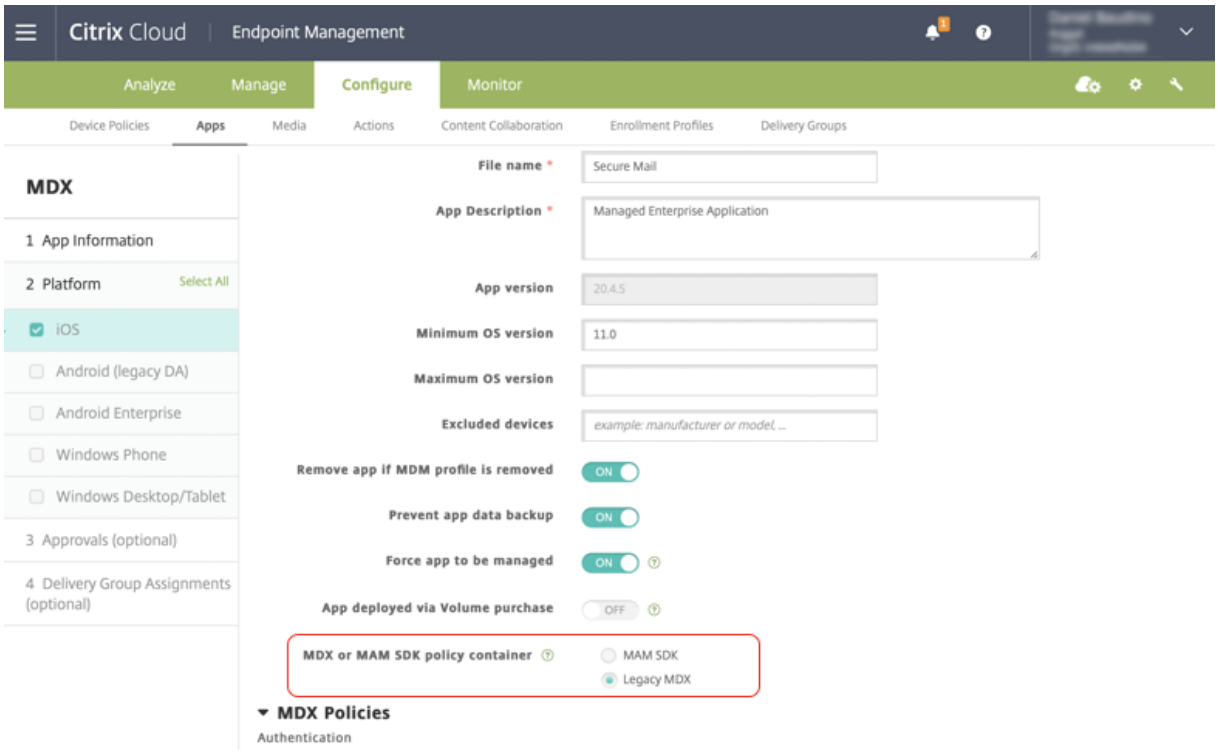
Secure Web のデュアルモード

モバイルアプリケーション管理（MAM：mobile application management）SDK は、iOS プラットフォームがカバーできない MDX 機能の領域で代わりに使用できます。MDX ラッピングテクノロジは、2022 年 3 月に製品終了（EOL）になる予定です。

Citrix Secure Web は、2022 年 3 月に予定されている MDX の EOL に備え、MDX フレームワークおよび MAM SDK フレームワークとともにリリースされます。エンタープライズアプリケーションの管理を続行するには、MAM SDK を使用する必要があります。**MAM SDK** に切り替えることをお勧めします。デュアルモード機能は、Secure Web アプリから新しい MAM SDK モデルへの移行手段を提供することを目的としています。

デュアルモード機能により、MDX（現在はレガシ **MDX**）を使用してアプリの管理を継続するか、新しい **MAM SDK** に切り替えることができます。［**MDX** または **MAM SDK** ポリシーコンテナ］内のポリシー設定で次のオプションが表示されます：

- **MAM SDK**
- レガシ **MDX**



［**MDX** または **MAM SDK** ポリシーコンテナ］ポリシーでは、オプションを ［レガシ **MDX**］から ［**MAM SDK**］に変更できます。

アプリを再インストールする必要があるため、［**MAM SDK**］から ［レガシ **MDX**］に切り替えないことをお勧めします。デフォルト値は ［レガシ **MDX**］です。デバイス上で実行されている Secure Mail と Secure Web の両方に同じポリシーモードを設定してください。同じデバイス上で 2 つの異なるモードを実行することはできません。

［**MAM SDK**］モードを選択すると、アプリは自動的に MAM SDK フレームワークに切り替わり、管理者が操作しなくてもデバイスポリシーが更新されます。

> 注:
>
> ［レガシ **MDX**］から ［**MAM SDK**］フレームワークに切り替える場合、［ネットワークアクセス］ポリシーを［トンネル **- Web SSO**］または ［制限なし］のいずれかに変更する必要があります。

前提条件

デュアルモード機能を正常に展開するために、次の要件を満たしていることを確認してください:

- Citrix Endpoint Management をバージョン 10.12 RP2 以降、または 10.11 RP5 以降に更新します。
- モバイルアプリをバージョン 21.8.0 以降に更新します。
- 組織でサードパーティ製アプリを使用している場合は、MAM SDK フレームワークに切り替える前に、必ずサードパーティ製アプリに MAM SDK を組み込むようにしてください。すべての管理対象アプリを、一度に MAM SDK に移動する必要があります。

制限事項

- MAM SDK はプラットフォームベースの暗号化のみをサポートし、MDX 暗号化はサポートしません。
- Citrix Endpoint Management をバージョン 10.12 RP2 以降または 10.11 RP5 以降に更新せずに、ポリシーファイルがバージョン 21.8.0 以降で実行されている場合、Secure Web に対してポリシーエントリが重複して作成されます。
- アプリ管理の MAM SDK モードに切り替えると、一部の機能がサポートされない、または使用できなくなります。また、異なるモードの 2 つのアプリを相互利用する場合、［このアプリケーションで開く］やコピー/貼り付けなどの操作がサポートされません。たとえば、レガシ **MDX** モードで管理されているアプリから **MAM SDK** モードで管理されているアプリにコンテンツをコピーすることはできません（その逆も同様にコピーできません）。MAM SDK モードで使用できない機能については、次の表を参照してください:

機能	レガシ MDX	MAM SDK
共有デバイス	はい	いいえ
Intune	はい	いいえ
SMIME 共有証明書コンテナ	はい	いいえ
派生資格情報	はい	いいえ
UIWebView トンネリング	はい	いいえ
完全 VPN	はい	いいえ

- 次のポリシーは廃止され、MAM SDK モードでは使用できません:
  - 許可する Secure Web ドメイン
  - 許可された Wi-Fi ネットワーク
  - 代替 Citrix Gateway
  - 証明書ラベル
  - Citrix レポート
  - 明示的なログオフ通知
  - マイクロ VPN セッションを必須とする
  - マイクロ VPN セッションを必須とするまでの猶予期間（分）
  - レポートファイルキャッシュの最大値
  - Wi-Fi を必須とする
  - Wi-Fi のみでレポートを送信
  - アップロードトークン

注:

> 内部サーバーへの認証にクライアント証明書を使用している場合、クライアント証明書は Access Gateway で使用されているものと同じである必要があります。

MAM SDK について詳しくは、次の記事を参照してください:

- MAM SDK の概要
- Mobile Application Integrationに関する Citrix 開発者向けドキュメント
- Citrix ブログの投稿
- Citrix ダウンロードページにサインオンするときの SDK ダウンロード

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web 21.7.0

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web 21.6.0

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web for iOS 21.5.0

このリリースには、バグの修正が含まれています。

Secure Web for Android 21.4.5

このリリースには、バグの修正が含まれています。

Secure Web 21.3.5

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web 21.3.0

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web 21.2.0

Secure Web for iOS

Secure Web の色の刷新。Secure Web は、シトリックスの最新のブランドカラーに準拠しています。

Secure Web for Android

- **Secure Web** の色の刷新。Secure Web は、シトリックスの最新のブランドカラーに準拠しています。
- 折りたたみ式デバイスでの安定した動作。Secure Web for Android には、折りたたみ式デバイスで安定して機能するための修正が含まれています。

Secure Web 21.1.5

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web 21.1.0

このリリースには、バグの修正が含まれています。

Secure Web 20.12.0

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web 20.11.0

このリリースには、バグの修正が含まれています。

Secure Web 20.10.5

Secure Web for Android

AndroidX ライブラリのサポート。Google の推奨事項に従って、Secure Web は **AndroidX** ライブラリをサポートします。これは、**android.support** としてパッケージ化されたライブラリに置き換わるものです。

Secure Web 20.10.0

Secure Web for Android

Secure Web は、Android 10 に関する Google Play の最新のターゲット API 要件をサポートしています。

Secure Web 20.9.5

Secure Web for iOS

このリリースには、バグの修正が含まれています。

Secure Web 20.9.0

Secure Web for Android

> 注:
>
> Android 6.x のサポートは 2020 年 9 月 15 日に終了しました。

Secure Web 20.8.5

Secure Web for Android

Secure Web for Android は、Android 11 をサポートしています。

Secure Web 20.8.0

Secure Web for Android

Secure Web for Android のデュアルモード。モバイルアプリケーション管理（MAM：mobile application management）SDK は、iOS および Android プラットフォームがカバーできない MDX 機能の領域で代わりに使用されます。MDX ラッピングテクノロジは、2021 年 9 月に製品終了（EOL）になる予定です。エンタープライズアプリケーションの管理を続行するには、MAM SDK を使用する必要があります。

バージョン 20.8.0 から、Android アプリが MDX および MAM SDK とともにリリースされ、前述の MDX の EOL に対応しています。MDX デュアルモードは、従来の MDX Toolkit から新しい MAM SDK に移行する方法を提供します。デュアルモード機能を使用すると、MDX Toolkit（現在はレガシ **MDX**）を使用してアプリを管理し続けるか、新しい MAM SDK に切り替えてアプリ管理を行うことができます。

アプリ管理のために MAM SDK に切り替えると、Citrix によりさらに変更が実装されます。管理者による操作は必要ありません。

MAM SDK について詳しくは、次の記事を参照してください:

- MAM SDK の概要
- デバイス管理についての Citrix Developer セクション
- Citrix ブログの投稿
- Citrix ダウンロードページにサインオンするときの SDK ダウンロード

前提条件

デュアルモード機能を正常に展開するには、次の点を確認してください:

- Citrix Endpoint Management をバージョン 10.12 RP2 以降、または 10.11 RP5 以降に更新します。
- モバイルアプリをバージョン 20.8.0 以降に更新します。
- ポリシーファイルをバージョン 20.8.0 以降に更新します。
- 組織でサードパーティ製アプリを使用している場合は、Citrix 業務用モバイルアプリの MAM SDK オプションに切り替える前に、必ずこれらのアプリに MAM SDK を組み込むようにしてください。すべての管理対象アプリを、一度に MAM SDK に移動する必要があります。

> 注:
>
> MAM SDK は、すべてのクラウドベースのお客様向けにサポートされています。

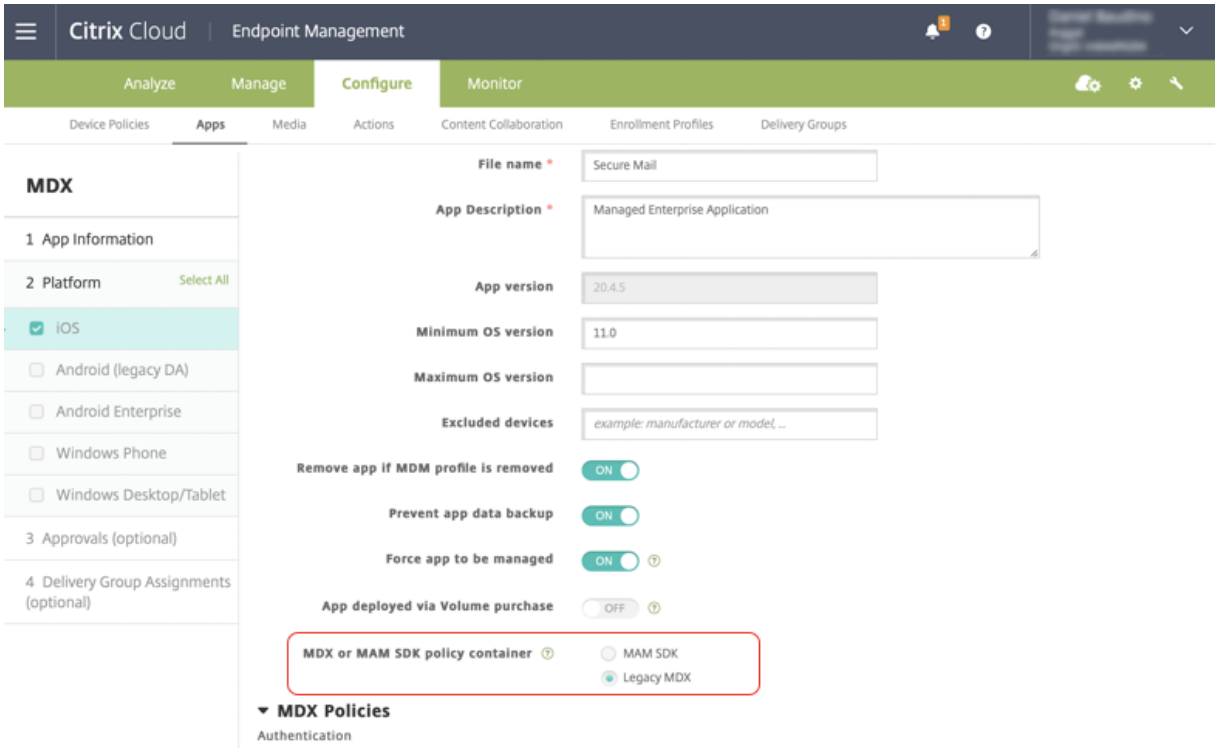
制限事項

- MAM SDK は、Citrix Endpoint Management 展開の Android Enterprise プラットフォームで公開されたアプリのみをサポートします。新しく公開されたアプリの場合、デフォルトの暗号化はプラットフォームベースの暗号化です。
- MAM SDK はプラットフォームベースの暗号化のみをサポートし、MDX 暗号化はサポートしません。
- Citrix Endpoint Management を更新せず、モバイルアプリのポリシーファイルがバージョン 20.8.0 以降で実行されている場合は、Secure Web 用にネットワークポリシーの重複エントリが作成されます。

Citrix Endpoint Management で Secure Web を構成する場合、デュアルモード機能を使用すると、MDX Toolkit（現在はレガシ **MDX**）を使用してアプリを管理し続けるか、新しい **MAM SDK** に切り替えてアプリ管理を行うことができます。**MAM SDK** はモジュール化されており、組織で使用している MDX 機能のサブセットのみを使用できるようにするため、MAM SDK に切り替えることを Citrix ではお勧めします。これによって、アプリの全体的なバイナリでランタイムのフットプリントを削減できます。

[**MDX** または **MAM SDK** ポリシーコンテナ] 内のポリシー設定で次のオプションが表示されます:

- **MAM SDK**
- レガシ **MDX**



[**MDX** または **MAM SDK** ポリシーコンテナ] ポリシーでは、オプションをレガシ **MDX** から MAM SDK に変更する

ことのみ可能です。MAM SDK からレガシ **MDX** に切り替えるオプションは許可されていないため、アプリを再公開する必要があります。デフォルト値は MDX レガシです。同じデバイス上で実行されている Secure Mail と Secure Web の両方に同じポリシーモードを設定してください。同じデバイス上で 2 つの異なるモードを実行することはできません。

Secure Web 20.7.5

このリリースには、バグの修正が含まれています。

Secure Web 20.7.0

マルチタスクのサポート。Secure Web for iOS では、マルチタスクにより、2 つのアプリを同時に使用します。この機能を有効にするには、1 つのアプリをドックの外にドラッグします。これを画面の右端または左端にスライドすると、画面が分割し 2 つのアプリを同時使用できるようになります。

業務用モバイルアプリの最新情報については、「最新の情報」を参照してください。

Secure Web 20.6.0

このリリースには、バグの修正が含まれています。

Secure Web 20.5.0

このリリースには、バグの修正が含まれています。

Secure Web 20.4.5

新しいタブでブックマークに移動します。Secure Web for iOS では、新しいタブを開いたときにブックマークを表示、編集、またはブックマークに移動できます。

Secure Web 19.10.5～20.4.0

これらのリリースには、バグの修正が含まれています。

Secure Web 19.10.0

Secure Web は **iOS** および **Android** バージョンとも、暗号化管理をサポートしています。暗号化管理を使用すると、最新のデバイスプラットフォームセキュリティを使用しながら、デバイスをプラットフォームセキュリティを効果的に使用するのに十分な状態に保つことができます。暗号化管理を使用すると、ファイルシステムの暗号化が iOS または Android の各プラットフォームによって提供されるため、ローカルデータの暗号化の冗長性がなくなります。

この機能を有効にするには、管理者は、Citrix Endpoint Management コンソールで、暗号化の種類 MDX ポリシーを ［コンプライアンス強制によるプラットフォームの暗号化］に設定する必要があります。

暗号化管理を使用すると、最新のデバイスプラットフォームセキュリティを使用しながら、デバイスをプラットフォームセキュリティを効果的に使用するのに十分な状態に保つことができます。暗号化管理を使用すると、ファイルシステムの暗号化が iOS または Android プラットフォームによって提供されるため、ローカルデータの暗号化の冗長性がなくなります。この機能を有効にするには、管理者は、Citrix Endpoint Management コンソールで、暗号化の種類 MDX ポリシーを ［コンプライアンス強制によるプラットフォームの暗号化］に設定する必要があります。

暗号化の種類

暗号化管理機能を使用するには、Citrix Endpoint Management コンソールで、暗号化の種類ポリシーを ［コンプライアンス強制によるプラットフォーム暗号化］に設定します。これにより、暗号化管理とユーザーのデバイス上の既存のすべての暗号化アプリケーションデータを、MDX ではなくデバイスによって暗号化された状態にシームレスに移行できます。この移行中、アプリはワンタイムデータ移行のために一時停止します。移行が成功すると、ローカルに保存されたデータの暗号化に対する責任が、MDX からデバイスプラットフォームに移ります。MDX は引き続き、アプリが起動されるたびにデバイスのコンプライアンスをチェックします。この機能は、MDM + MAM 環境と MAM のみの環境の両方で機能します。

暗号化の種類ポリシーを ［コンプライアンス強制によるプラットフォーム暗号化］に設定すると、新しいポリシーが既存の MDX 暗号化よりも優先されます。

Secure Web の暗号化管理 MDX ポリシーについて詳しくは、以下のページの「暗号化」セクションを参照してください：

- iOS 向け業務用モバイルアプリの MDX ポリシー
- Android 向け業務用モバイルアプリの MDX ポリシー

非準拠デバイスの動作

デバイスが最小コンプライアンス要件を下回ると、非準拠デバイスの動作ポリシーによって、実行する操作を次の中から選択することができます：

- アプリを許可 - アプリが正常に動作することを許可します。
- 警告後にアプリを許可する - アプリが最小コンプライアンス要件を満たしていないことをユーザーに警告してから、アプリの実行を許可します。これがデフォルト値です。
- アプリを許可しない – アプリの実行を許可しません。

デバイスが最小コンプライアンス要件を満たしているかどうかは、次の基準で決まります。

iOS を実行しているデバイスの場合：

- iOS 10：指定されたバージョン以上のバージョンのオペレーティングシステムをアプリで実行している。
- デバッガーアクセス：アプリでデバッグが有効になっていない。
- ジェイルブレイクされたデバイス：アプリがジェイルブレイクされたデバイスで実行されていない。

- デバイスのパスコード：デバイスのパスコードがオンになっている。
- データ共有：アプリに対してデータ共有が有効になっていない。

Android を実行しているデバイスの場合：

- Android SDK 24（Android 7 Nougat）：指定されたバージョン以上のバージョンのオペレーティングシステムをアプリで実行している。
- デバッガーアクセス：アプリでデバッグが有効になっていない。
- Root 化済みデバイス：Root 化済みデバイスでアプリが実行されていない。
- デバイスのロック：デバイスのパスコードがオンになっている。
- 暗号化されたデバイス：暗号化されたデバイスでアプリが実行されている。

Secure Web 19.9.5

このリリースには、バグの修正が含まれています。

Secure Web 19.9.0

Secure Web for iOS

Secure Web for iOS は iOS 13 をサポートしています。

Secure Web for Android

このリリースには、バグの修正が含まれています。

Secure Web for Android 19.8.5

Secure Web for Android は、Android Q をサポートしています。

Secure Web 19.8.0

このリリースには、バグの修正が含まれています。

Secure Web 19.7.5

Secure Web for iOS

このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

Secure Web for Android

このリリース以降、Secure Web for Android は Android 6 以降を実行するデバイスのみでサポートされます。

Secure Web 19.3.0～19.6.5

これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

Secure Web 19.2.0

Secure Web でリンクを開いてデータをセキュアな状態で保護する。Secure Web では、ユーザーは専用の VPN トンネルによって機密情報があるサイトに安全にアクセスできます。この機能は、Secure Web for iOS では既に利用できます。このリリースでは、Android のサポートが追加されています。詳しくは、「Secure Web の機能」を参照してください。

Secure Web バージョン 18.11.5～19.1.5

これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

Secure Web 18.11.0

Secure Web for iOS で、サイトのキャッシュサイズ一覧が報告されず、アプリ設定に表示されなくなります。デフォルトのキャッシュ機能に変更はありません。

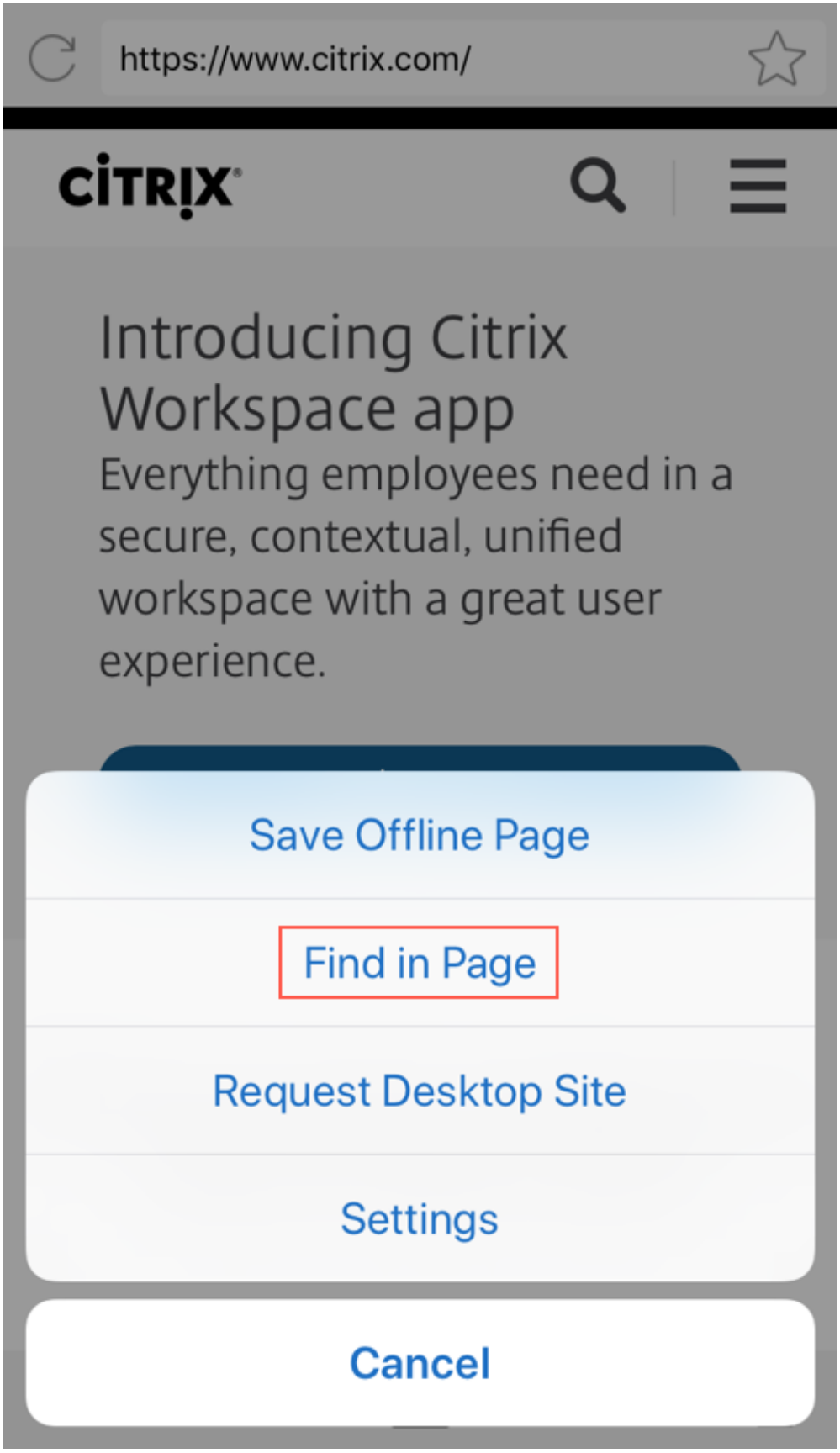
Secure Web 18.9.0～18.10.5

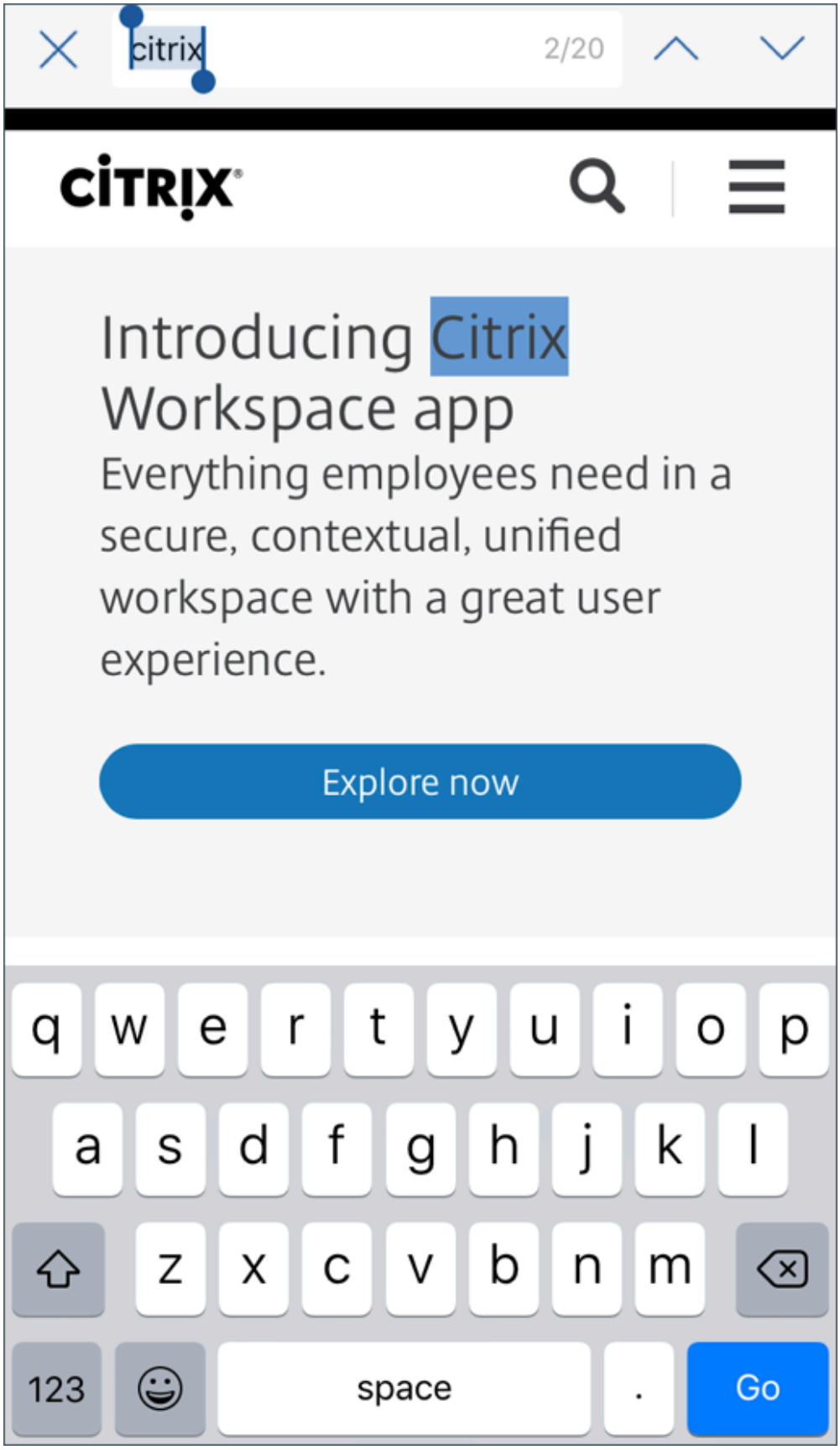
これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

Secure Web 10.8.65

以下の機能は Secure Web 10.8.65 の新機能です:

- プルして更新。Secure Web for iOS では、プルして更新する機能を使用して、画面に表示されるデータを更新することができます。
- [ページ内の検索] オプションを使用した検索。[ページ内の検索] オプションを使用すると、文字列をすぐに検索できます。このオプションでは、検索時にキーワードが強調表示され、ツールバーの右側に一致の合計数が表示されます。再起動した場合、最後に検索されたキーワードが保持されます。





- スクロールアップによるヘッダーバーとフッターバーの非表示。Secure Web for iOS では、スクロールアップするとヘッダーバーとフッターバーが非表示になります。これにより、Web ページを表示するときにモバイル画面にさらに多くの情報を表示することができます。

Secure Web 10.8.60

- ポーランド語のサポート

Secure Web 10.8.35

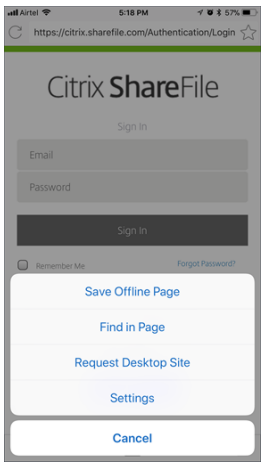
- プルして更新。Secure Web for Android では、プルして更新する機能を使用して、画面に表示されるデータを更新することができます。

Secure Web 10.8.15

- **Secure Web** は **Android Enterprise**（以前の **Android for Work**）をサポートします。Secure Mail で Android Enterprise アプリを使用することで、別の仕事用プロファイルを作成できます。詳しくは、「Secure Mail の Android Enterprise」を参照してください。
- **Secure Web for Android** は **Web** ページをデスクトップモードでレンダリングできます。オーバーフローメニューから、［デスクトップサイトの要求］を選択します。Secure Web は、Web サイトのデスクトップ版を表示します。

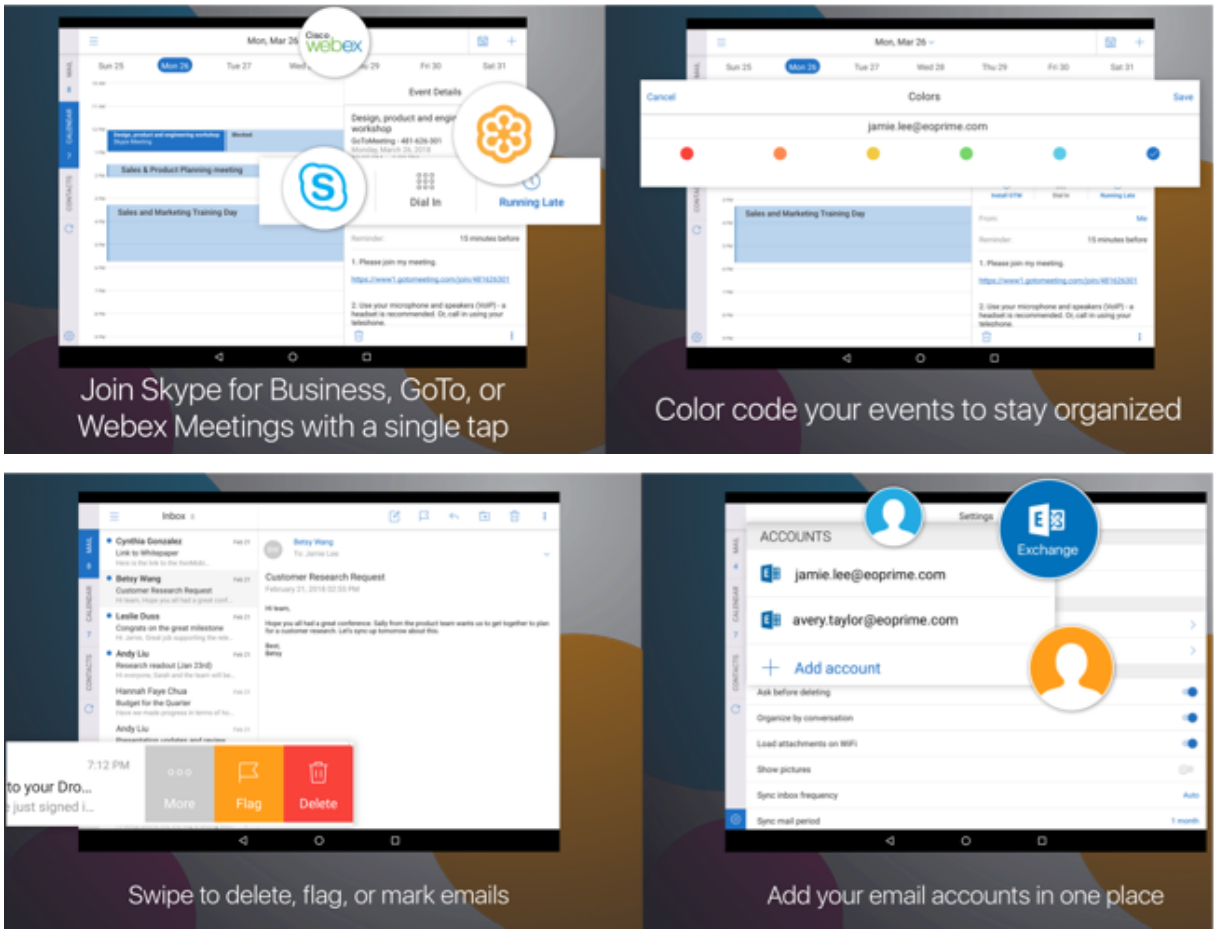
Secure Web 10.8.10

- **Secure Web for iOS** は **Web** ページをデスクトップモードでレンダリングできます。ハンバーガーメニューから、［デスクトップサイトの要求］を選択すると、Secure Web に Web サイトのデスクトップバージョンが表示されます。



Secure Web 10.8.5

Secure Mail と **Secure Web for iOS** および **Android** では、より適切なフォント、色、その他 **UI** の要素が導入されました。この変更は、Citrix アプリケーション全体により統一感を与え、ユーザーの操作性も向上しています。



既知の問題と解決された問題

September 15, 2021

Citrix では、業務用モバイルアプリの直近 2 つのバージョンからのアップグレードをサポートしています。

Secure Web 21.9.0

このリリースでは既知の問題および解決された問題はありません。

Secure Web 21.8.5

このリリースでは既知の問題および解決された問題はありません。

Secure Web 21.8.0

Secure Web 21.8.0 での既知の問題

このリリースで解決された問題はありません。

古いバージョンでの既知の問題と修正された問題

Secure Web の以前のバージョンでの既知の問題と解決された問題については、「古いバージョンでの既知の問題と修正された問題」を参照してください。

Secure Web の統合と提供

March 29, 2021

Secure Web を統合して提供するには、次の一般的な手順に従います:

1. 内部ネットワークで SSO を有効にするには、Citrix Gateway を構成します。

   HTTP トラフィックの場合、Citrix ADC は Citrix ADC がサポートするすべてのプロキシ認証タイプに対して SSO を提供できます。HTTPS トラフィックの場合、[Web パスワードのキャッシュを有効化] ポリシーにより、MDX を介するプロキシサーバーへの SSO を Secure Web が認証して提供するようにできます。MDX は、ベーシック、ダイジェスト、NTLM プロキシ認証のみをサポートします。パスワードは MDX を使ってキャッシュされ、機密アプリデータ用のセキュアなストレージ領域である Endpoint Management の共有コンテナに格納されます。Citrix Gateway の構成について詳しくは、「Citrix Gateway」を参照してください。

2. Secure Web をダウンロードします。
3. 内部ネットワークに対するユーザー接続をどのように構成するか決定します。
4. ほかの MDX アプリと同じ手順で Secure Web を Endpoint Management に追加し、MDX ポリシーを構成します。Secure Web に固有のポリシーについて詳しくは、「Secure Web ポリシーについて」を参照してください。

ユーザー接続の構成

Secure Web は、ユーザー接続について次の構成をサポートします:

- セキュアブラウズ: 内部ネットワークをトンネルする接続は、さまざまなクライアントレス VPN を使用できます。これはセキュアブラウズと呼ばれています。これは、[優先 **VPN** モード] ポリシーで指定されるデフォルト構成です。シングルサインオン (SSO) を必須とする接続に対しては、[セキュアブラウズ] を推奨します。
- 完全 **VPN** トンネル: 内部ネットワークへトンネルする接続は完全 VPN トンネルを使用でき、[優先 **VPN** モード] ポリシーにより構成されます。内部ネットワークのリソースにクライアント証明書またはエンドツーエンドの SSL を使用する接続に対しては、[完全 VPN トンネル] を推奨します。完全 VPN トンネルは、TCP 上

のあらゆるプロトコルを処理し、iOS や Android デバイスと同様に Windows や Mac コンピューターとともに使用できます。

> 注:
>
> MDX ラッピングテクノロジは、2021 年 9 月に製品終了（EOL）になる予定です。エンタープライズアプリケーションの管理を続行するには、MAM SDK を使用する必要があります。
> 完全 VPN トンネルは、レガシ MDX モードではサポートされていません。

- [**VPN** モードの切り替えを許可］ポリシーにより、完全 VPN トンネルモードとセキュアブラウズモードを必要に応じて切り替えることができます。デフォルトでは、このポリシーは無効になっています。このポリシーが有効な場合、優先 VPN モードで処理できない認証要求のために失敗するネットワーク要求は、代替モードで再試行されます。たとえば、クライアント証明書に対するサーバーチャレンジは完全 VPN トンネルモードでは処理できますが、セキュアブラウズモードでは処理できません。同様に、セキュアブラウズモードの使用時には、HTTP 認証チャレンジで SSO が実行される可能性が高くなります。
- **PAC** を使用した完全 **VPN** トンネル： Proxy Automatic Configuration（PAC）ファイルを iOS および Android デバイスの完全 VPN トンネル展開で使用できます。PAC ファイルには、指定の URL にアクセスするために Web ブラウザーがどのようにプロキシを選択するかを定義する規則が含まれます。PAC ファイル規則は、内部および外部の両サイトの処理を指定できます。Secure Web は PAC ファイル規則を解析し、プロキシサーバー情報を Citrix Gateway に送信します。
- PAC ファイルが使用される場合の完全 VPN トンネルのパフォーマンスは、セキュアブラウズモードと同等です。PAC 構成について詳しくは、「PAC を使用した完全 VPN トンネル」を参照してください。
- リバース分割トンネル：リバースモードでは、イントラネットアプリケーションのトラフィックは VPN トンネルをバイパスし、他のトラフィックは VPN トンネルを通過します。非ローカル LAN トラフィックをすべてログに記録するためにこのポリシーを使用できます。

リバース分割トンネリングの構成手順

Citrix Gateway に分割トンネリングリバースモードを構成するには、次の手順を実行します：

1. ［ポリシー］**>** ［セッション］ポリシーに移動します。
2. ［Secure Hub ポリシー］を選択し、［クライアントエクスペリエンス］**>** ［分割トンネル］に移動します。
3. ［リバース］を選択します。

リバース分割トンネルモードの除外対象一覧 **MDX** ポリシー

Citrix Endpoint Management のリバース分割トンネルモードポリシーで除外範囲を構成します。これは、DNS サフィックスと完全修飾ドメイン名のコンマ区切り一覧に基づいた範囲です。この一覧は、デバイスのローカルエリアネットワーク（LAN）で送信する必要があって Citrix ADC には送信しないトラフィックの URL を定義します。

次の表は、構成とサイトの種類に基づいて、Secure Web がユーザーに資格情報の入力を求めるかどうかを示しています。

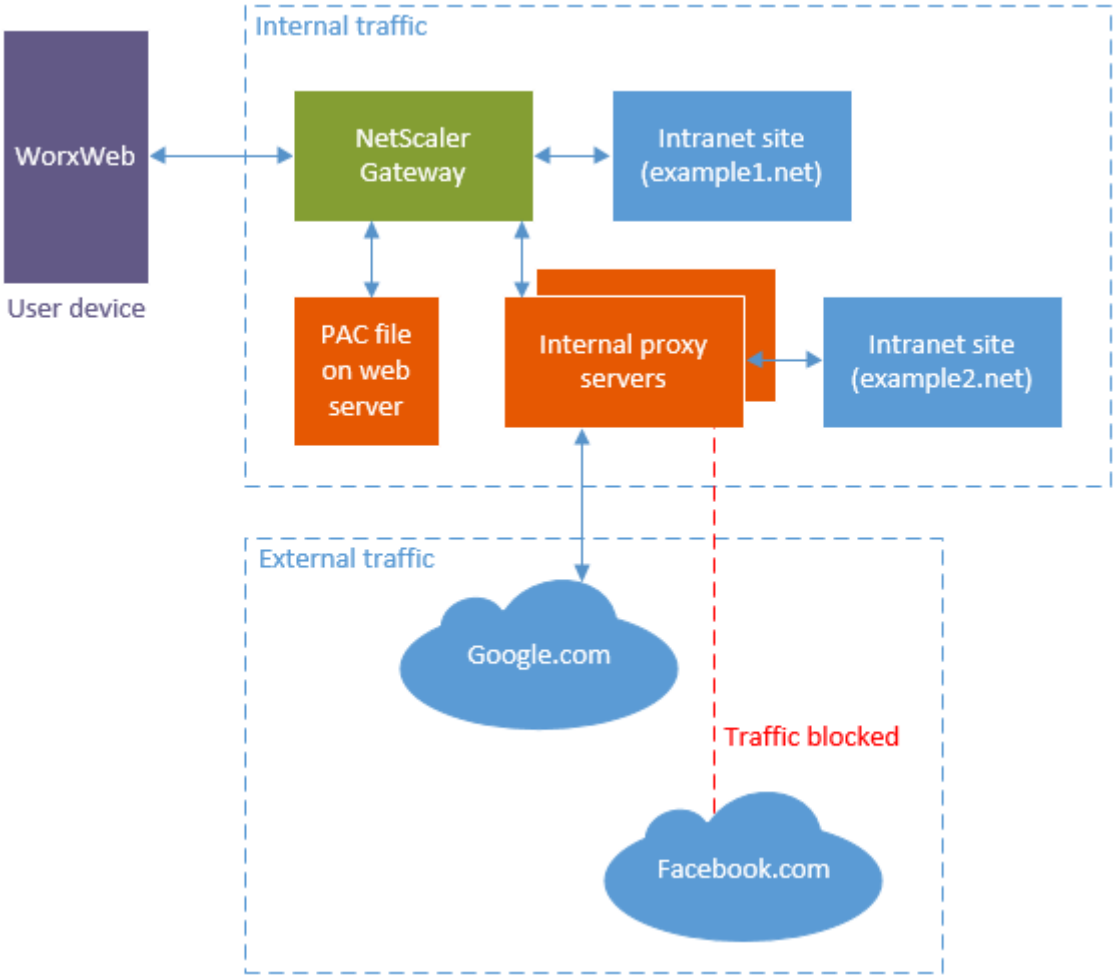
接続モード	サイトの種類	パスワードキャッシュ	Citrix Gateway 用に SSO が構成されています	Secure Web は、Web サイトへの最初のアクセス時に資格情報を要求します	Secure Web は、その Web サイトへの後続のアクセス時に資格情報を要求します	Secure Web は、パスワード変更後に資格情報を要求します
セキュアブラウズ	HTTP	いいえ	はい	いいえ	いいえ	いいえ
セキュアブラウズ	HTTPS	いいえ	はい	いいえ	いいえ	いいえ
完全 VPN	HTTP	いいえ	はい	いいえ	いいえ	いいえ
完全 VPN	HTTPS	はい。Secure Web の MDX ポリシー［Web パスワードのキャッシュを有効化］が［オン］の場合。	いいえ	はい。Secure Web で資格情報をキャッシュすることが必要。	いいえ	はい

PAC を使用した完全 **VPN** トンネル

> 重要:
>
> Secure Web が PAC ファイルで構成され、Citrix ADC がプロキシ操作用に構成されると、Secure Web がタイムアウトします。PAC を使用した完全 VPN トンネルを使用する前に、プロキシ用に構成された Citrix Gateway トラフィックポリシーを削除します。

PAC を使用した完全 VPN トンネルまたはプロキシサーバー用に Secure Web を構成すると、Secure Web は Citrix Gateway を介してすべてのトラフィックをプロキシに送信します。Citrix Gateway はその後、プロキシの構成規則に従ってトラフィックをルーティングします。この構成では、Citrix Gateway が PAC ファイルまたはプロキシサーバーを認識しません。トラフィックのフローは PAC がない完全 VPN トンネルと同じになります。

次の図は、Secure Web ユーザーが Web サイトにアクセスする場合のトラフィックフローを示しています:



この例では、トラフィック規則は次のようになっています:

- Citrix Gateway はイントラネットサイト`example1.net`に直接接続します。
- イントラネットサイト`example2.net`へのトラフィックは、内部プロキシサーバーを介してプロキシ接続されます。
- 外部トラフィックは内部プロキシサーバーを介してプロキシ接続されます。プロキシ規則によって、次の URL への外部トラフィックがブロックされます: `Facebook.com`.

PAC を使用した完全 **VPN** トンネルを構成するには

1. PAC ファイルの検証とテスト

   > 注:
   >
   > PAC ファイルの作成と使用について詳しくは、*findproxyforurl.com/*に移動してください。

   Pacparserなどの PAC 検証ツールを使って PAC ファイルを検証します。PAC ファイルを読み取る場合、Pacparser の結果が予想道理だったか確認します。PAC ファイルに構文エラーがある場合、モバイルデバイスは PAC ファイルを警告なしに無視します（PAC ファイルはモバイルデバイスのメモリ内にのみ格納されま

す)。

PAC ファイルは、上から順番に処理され、規則が現在のクエリと一致したら停止します。

Web ブラウザーで PAC ファイル URL をテストしてから、Endpoint Management の **PAC/Proxy** フィールドに入力します。PAC ファイルがあるネットワークにコンピューターがアクセスできるか確認します。

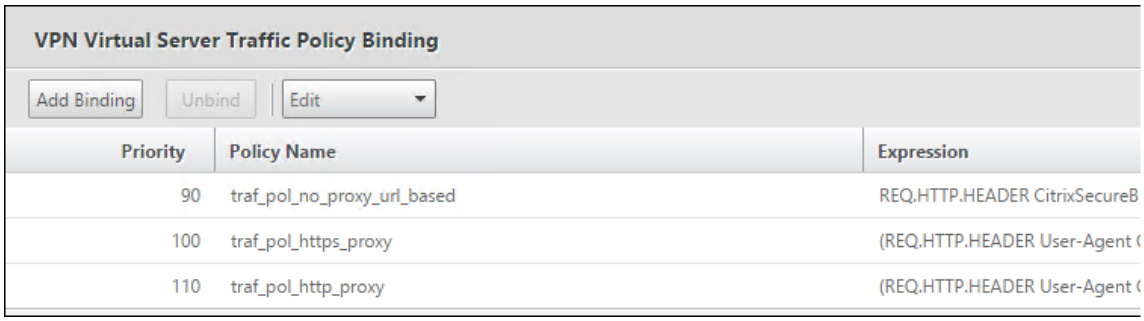
```
https://webserver.local/GenericPAC.pac
https://webserver.local/GenericPAC.pac
```

テストされた PAC ファイルの拡張子は.txt または.pac です。

PAC ファイルは Web ブラウザー内にコンテンツを表示する必要があります。

> 重要:
>
> Secure Web で使用される PAC ファイルを更新する度に、Secure Web をいったん閉じてから再度開く必要があることをユーザーに知らせます。

2. Citrix Gateway を構成します。
   - Citrix Gateway 分割トンネリングを無効にします。分割トンネリングが有効で PAC ファイルが構成されていると、PAC ファイル規則により Citrix ADC 分割トンネリング規則は無効になります。プロキシは Citrix ADC 分割トンネリング規則を上書きしません。
   - プロキシ用に構成した Citrix Gateway トラフィックポリシーを削除します。これは、Secure Web が正常に機能するために必要です。下の図は、削除するポリシー規則の例を示しています。



3. Secure Web ポリシーを構成します。
   - [優先 VPN モード] ポリシーを [完全 **VPN** トンネル] に設定します。
   - [VPN モードの切り替えを許可] ポリシーを [オフ] に設定します。
   - [PAC ファイルの URL、またはプロキシサーバー] ポリシーを構成します。Secure Web は、デフォルトおよび非デフォルトのポートに加えて、HTTP および HTTPS をサポートします。HTTPS については、証明書が自己署名または信頼されていない場合は、デバイスにルート証明機関をインストールする必要があります。

     ポリシーを構成する前に、Web ブラウザーで URL またはプロキシサーバーアドレスをテストしてください。

     PAC ファイル URL の例:


```
http[s]://example.com/proxy.pac
http[s]://10.10.0.100/proxy.txt
```

プロキシサーバーの例（ポートが必要）：

```
myhost.example.com:port
```

```
10.10.0.100:port
```

> 注：
>
> PAC ファイルまたはプロキシサーバーを構成する場合、Wi-Fi のシステムプロキシ設定で PAC を構成しないでください。

- ［Web パスワードのキャッシュを有効化］ポリシーを ［オン］に設定します。Web パスワードキャッシュが HTTPS サイトの SSO を処理します。

  プロキシが同じ認証インフラストラクチャをサポートする場合、Citrix ADC は内部プロキシに対して SSO を実行できます。

PAC ファイルサポートの制限

Secure Web は、次のことをサポートしません：

- あるプロキシサーバーから別のプロキシサーバーへのフェールオーバー。PAC ファイル検証は単一のホスト名に対して複数のプロキシサーバーを返すことができます。Secure Web は最初に返されたプロキシサーバーのみを使用します。
- PAC ファイルの FTP や gopher などのプロトコル。
- PAC ファイルの SOCKS プロキシサーバー。
- Web Proxy AutoDiscovery Protocol（WPAD）。

Secure Web は、PAC ファイル関数の alert を無視するため、Secure Web は呼び出しを含まない PAC ファイルを解析できます。

Secure Web のポリシー

Secure Web を追加する際には、Secure Web に固有の以下の MDX ポリシーに注意してください。サポートされているすべてのモバイルデバイスについて、以下の点に注意してください：

許可または禁止する **Web** サイト

Secure Web は、通常 Web リンクをフィルター処理しません。このポリシーを使って、許可されたサイトまたは禁止されたサイトの特定の一覧を構成できます。コンマ区切りの一覧形式で URL のパターンを入力して、Web ブラウザーでアクセスできる Web サイトを制限します。一覧内の各パターンには、プラス記号（+）またはマイナス記号（-）のプレフィックスが付いています。一致するものが見つかるまで、一覧の順序どおりに URL がパターンと比較されます。一致が見つかると、プレフィックスにより次のような処理が指示されます。

- マイナス（-）記号の場合、その URL へのアクセスが禁止されます。この場合、解決できない Web サーバーアドレスとして URL が処理されます。
- プラス（+）記号の場合、その URL へのアクセスが許可されます。
- パターンの最初の文字がプラス（+）またはマイナス（-）のどちらでもない場合は、+（許可）とみなされます。
- URL が一覧のパターンのいずれとも一致しない場合、その URL は許可されたものとなります。

いずれのパターンとも一致しない URL へのアクセスを禁止するには、一覧の最後にマイナス（-）の付いたアスタリスク（-*）を追加します。例:

- ポリシーの値が「+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*」の場合、mycorp.comドメイン内では HTTP URL を許可してほかの場所では HTTP URL をブロックし、すべての場所で HTTPS および FTP の URL を許可し、そのほかすべての URL をブロックします。
- このポリシー値+http://*.training.lab/*,+https://*.training.lab/*,-*により、ユーザーは、HTTP または HTTPS 経由で Training.lab ドメイン（イントラネット）内の任意のサイトを開くことができます。このポリシーの値では、ユーザーはプロトコルに関係なく Facebook、Google、Hotmail などのパブリック URL は開くことができません。

デフォルト値は空です（すべての URL が許可される）。

ポップアップをブロック

ポップアップは Web サイトがユーザーの権限なしに開く新しいタブです。このポリシーにより Secure Web がポップアップを許可するかどうかが決まります。［オン］にすると、Secure Web は Web サイトがポップアップを開くことを禁止します。デフォルト値は［オフ］です。

事前ロードするブックマーク

Secure Web ブラウザーに対して事前に読み込まれたブックマークのセットを定義します。ポリシーは、フォルダー名、フレンドリ名、および Web アドレスを含むタプルのコンマ区切りの一覧です。各組は「フォルダー、名前、URL」形式で入力します。フォルダーと名前は必要に応じて二重引用符（”）で囲みます。

たとえば、ポリシー値「,"Mycorp, Inc. home page",https://www.mycorp.com, "MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx」は 3 つのブックマークを定義します。1 つ目のブックマークは「Mycorp, Inc. home page」という名前のプライマリリンク (フォルダー名なし) です。2 つ目のブックマークは「MyCorp Links」という名前のフォルダーに「Account logon」という名前で追加されます。3 つ目のブックマークは「MyCorp Links」フォルダーの「Investor Relations」サブフォルダーに「Contact us」という名前で追加されます。

デフォルト値は空です。

ホームページの **URL**

Secure Web の起動時に読み込む Web サイトを定義します。デフォルト値は空です（デフォルトのスタートページ）。

サポートされている Android および iOS デバイスのみ:

Web ブラウザーのユーザーインターフェイス

このポリシーでは、Secure Web ブラウザーのユーザーインターフェイスコントロールの動作と表示を指定します。通常、ユーザーはすべてのコントロールを使用できます。Secure Web のユーザーインターフェイスには、次のページに進む、前のページに戻る、アドレスバー、更新または停止用などのコントロールがあります。このポリシーを構成して、一部のコントロールの使用および表示を制限できます。デフォルト値は［すべてのコントロールを表示］です。

以下のオプションがあります:

- すべてのコントロールを表示。すべてのコントロールが表示され、ユーザーはそのすべてを使用できます。
- 読み取り専用アドレスバー。すべてのコントロールが表示されますが、ユーザーはアドレスフィールドを編集できません。
- アドレスバーを隠す。アドレスバーが非表示になり、ほかのすべてのコントロールが表示されます。
- すべてのコントロールを隠す。ツールバー全体を非表示にして、フレームのないブラウジング環境を提供します。

Web パスワードのキャッシュを有効化

Web リソースへアクセスまたはそれを要求する場合に、Secure Web ユーザーが資格情報を入力すると、このポリシーによりデバイス上でパスワードが Secure Web によりサイレントキャッシュされるかどうかが決まります。このポリシーは、認証ダイアログに入力されたパスワードに適用され、Web フォームに入力されたパスワードには適用されません。

［オン］の場合、Web リソースの要求時にユーザーが入力するすべてのパスワードが Secure Web によりキャッシュされます。［オフ］の場合、Secure Web はパスワードをキャッシュせずに既存のキャッシュ済みパスワードを削除します。デフォルト値は ［オフ］です。

このポリシーは、このアプリで優先 VPN ポリシーを［完全 VPN トンネル］に設定した場合にのみ有効になります。

プロキシサーバー

また、セキュアブラウズモードで使用される場合に Secure Web に対してプロキシサーバーを構成できます。詳しくは、ブログ記事を参照してください。

DNS サフィックス

Android では、DNS サフィックスが構成されていない場合、VPN が失敗することがあります。DNS サフィックスの構成について詳しくは、「Android デバイスで DNS サフィックスを使用した DNS クエリのサポート」を参照してください。

Secure Web で使用するイントラネットサイトの準備

このセクションは、Android および iOS に対応した Secure Web で使用するイントラネットサイトの準備を担当する Web サイト開発者を対象にしています。デスクトップブラウザー用に設計されたイントラネットサイトを Android デバイスや iOS デバイスで適切に動作させるには変更が必要です。

Secure Web は Web 技術のサポートを提供するために、Android では WebView、iOS では WkWebView に依存しています。Secure Web でサポートされている Web 技術にはたとえば次のようなものがあります:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets（無制限モードのみ）

Secure Web でサポートされていない Web 技術にはたとえば次のようなものがあります:

- Flash
- Java

次の表は、Secure Web でサポートされている HTML レンダリング機能と技術をまとめたものです。○ は、その機能をプラットフォーム、ブラウザー、またはコンポーネントの組み合わせで利用できることを示しています。

技術	Secure Web for iOS	Secure Web for Android
JavaScript エンジン	JavaScriptCore	V8
ローカルストレージ	○	○
AppCache	○	○
IndexedDB		○
SPDY	○	
WebP		○
srcet	○	○
WebGL		○
requestAnimationFrame API		○

技術	Secure Web for iOS	Secure Web for Android
Navigation Timing API		○
Resource Timing API		○

さまざまなデバイスで同じ技術が機能しますが、Secure Web はデバイスごとに異なるユーザーエージェント文字列を返します。Secure Web で使用するブラウザーのバージョンを判断するには、ユーザーエージェント文字列を表示します。Secure Web から、https://whatsmyuseragent.com/にアクセスします。

イントラネットサイトのトラブルシューティング

イントラネットサイトを Secure Web で表示したときのレンダリングの問題を解決するには、その Web サイトが Secure Web と、互換性のあるサードパーティのブラウザーでどのようにレンダリングされるかを比較してください。

iOS の場合、テスト用に互換性のあるサードパーティのブラウザーは Chrome と Dolphin です。

Android の場合、テスト用に互換性のあるサードパーティのブラウザーは Dolphin です。

> 注:
>
> Chrome は Android のネイティブブラウザーです。これを比較には使用しないでください。

iOS では、ブラウザーがデバイスレベルでの VPN サポートが有効か確認してください。このサポートは、デバイスで ［設定］**>** ［**VPN**］**>** ［**VPN** 構成を追加］の順に選択して構成できます。

また App Store では、Citrix VPN、Cisco AnyConnect、またはPulse Secureなどの VPN クライアントアプリを利用できます。

- 2 つのブラウザーで Web ページのレンダリングが同じであれば、問題は Web サイトにあります。サイトを更新して、目的の OS で正しく動作することを確認してください。
- Secure Web でのみ Web ページに問題が現れる場合は、シトリックスサポートに連絡して、サポートチケットを開いてください。その際、トラブルシューティングの手順、およびテストに使用したブラウザーと OS の種類をお知らせください。Secure Web for iOS にレンダリングの問題がある場合は、以下で説明する手順に従ってページの Web アーカイブを含めてください。これは、シトリックスが問題をより早く解決するのに役立ちます。

SSL 接続の確認

SSL 証明書チェーンが適切に構成されていることを確認してください。SSL 証明書チェッカーを使用して、モバイルデバイスにリンクされていない、またはインストールされていないルート CA または中間 CA の欠落がないかどうかを確認できます。

多くのサーバー証明書は、複数の階層的な証明機関（CA）によって署名されています。つまり、証明書はチェーンを形成しています。これらの証明書をリンクする必要があります。証明書のインストールまたはリンクについては、「証明書のインストール、リンク、および更新」を参照してください。

Web アーカイブファイルを作成するには

macOS 10.9 以降で Safari を使用すると、（リーディングリストとして参照される）Web アーカイブファイルとして Web ページを保存できます。Web アーカイブファイルには画像、CSS、JavaScript などのすべてのリンク設定されたファイルが含まれます。

1. Safari から、リーディングリストのフォルダーを空にします：**Finder** でメニューバーの ［移動］メニューをクリックし、［フォルダへ移動］を選択してパス名「~/Library/Safari/ReadingListArchives/」を入力します。次にこの場所にあるフォルダーをすべて削除します。
2. メニューバーで ［**Safari**］**>** ［環境設定］**>** ［詳細］の順に選択し、［メニューバーに **“**開発**”** メニューを表示］チェックボックスをオンにします。
3. メニューバーで、［開発］**>** ［ユーザーエージェント］の順に選択し、Secure Web ユーザーエージェントを入力します：(Mozilla/5.0 (iPad; CPUOS 8_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25)。
4. Safari でリーディングリスト（Web アーカイブファイル）として保存する Web サイトを開きます。
5. メニューバーで、［ブックマーク］**>** ［リーディングリストに追加］の順に選択します。この処理には数分かかることがあります。バックグラウンドでアーカイブ化が実行されます。
6. アーカイブ化されたリーディングリストを検索します：メニューバーで、［表示］**>** ［リーディングリストサイドバーを表示］の順に選択します。
7. アーカイブファイルの確認：
   - Mac へのネットワーク接続を切断します。
   - リーディングリストから Web サイトを開きます。

     Web サイトは完全にレンダリングされます。
8. アーカイブファイルを圧縮します：**Finder** でメニューバーの ［移動］をクリックし、［フォルダへ移動］を選択してパス名「~/Library/Safari/ReadingListArchives/」を入力します。次に、ランダムな 16 進数文字列のファイル名を持つフォルダーを圧縮します。これは、サポートチケットを開く時にシトリックスサポートに送信できるファイルです。

Secure Web の機能

Secure Web では、モバイルデータ交換技術を使用した専用の VPN トンネルが作成され、内部サイトや外部の Web サイトにアクセスできるようになります。これらのサイトには、組織のセキュリティポリシーで保護された環境で機密情報を含むサイトがあります。

Secure Mail および Citrix Files との連携により、Secure Web ではセキュアな Endpoint Management コンテナ内のシームレスなユーザーエクスペリエンスが提供されます。連携機能の例をいくつか示します:

- ユーザーが **Mailto** リンクをタップすると、Secure Mail で新規メールメッセージ画面が開きます。資格情報を入力する必要はありません。
- **Secure Web** でリンクを開いてデータをセキュアな状態で保護する。Secure Web for iOS および Android では、ユーザーは専用の VPN トンネルによって機密情報があるサイトに安全にアクセスできます。Secure Mail から、Secure Web 内から、またはサードパーティ製アプリからリンクをクリックでき、Secure Web でリンクを開くため、データはセキュアな状態のままです。ユーザーは、Secure Web で ctxmobilebrowser スキームを使用した内部リンクを開きます。このとき、先頭の「`ctxmobilebrowser://`」が「`http://.`」に変換されて HTTPS リンクが開かれます。Secure Web により「`ctxmobilebrowsers://`」が「`https://`」に変換されます。

この機能は、受信ドキュメント交換と呼ばれるアプリと MDX ポリシーとの相互作用によるものです。デフォルトでは、このポリシーは［制限なし］に設定されています。この設定では、URL を Secure Web で開くことができます。許可リストに登録されたアプリのみが Secure Web と機能できるように、ポリシー設定を変更できます。

- また、メールメッセージ内のイントラネットリンクをクリックすると Secure Web がサイトに移動して、資格情報を入力せずにイントラネットサイトにアクセスできます。
- ユーザーは、Secure Web を使用して Web からダウンロードしたデータを Citrix Files にアップロードできます。

また、Secure Web ユーザーは以下の操作も実行できます:

- ポップアップをブロックする。

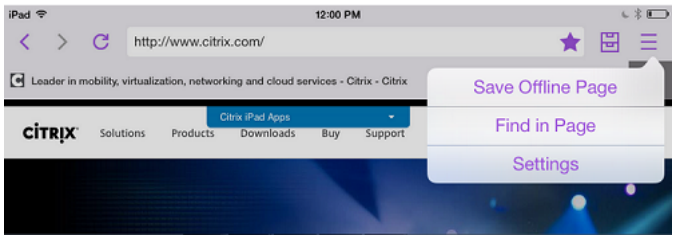
  > 注:
  >
  > Secure Web のメモリの大部分は、ポップアップのレンダリングで消費されます。そのため、通常、［設定］でポップアップをブロックすることで、パフォーマンスが向上します。

- お気に入りサイトをブックマークとして登録する。
- ファイルをダウンロードする。
- オフライン用にページを保存する。
- パスワードを自動保存する。
- キャッシュ、履歴、および Cookie を削除する。
- Cookie および HTML5 のローカルストレージの無効化。
- 他のユーザーとデバイスを安全に共有する。
- アドレスバー内で検索する。
- Secure Web で実行する Web アプリによる位置情報へのアクセスを許可します。
- 設定のエクスポートおよびインポート。

- ファイルをダウンロードすることなく Citrix Files でファイルを直接開く。この機能を有効にするには、Endpoint Management の「許可する URL」ポリシーに「**ctx-sf:**」を追加します。
- iOS で、3D タッチ操作でホーム画面から直接新しいタブを開いて、オフラインページ、お気に入りサイト、およびダウンロードにアクセスする。
- iOS で、あらゆるサイズのファイルをダウンロードし、Citrix Files やその他のアプリで開く。

  > 注:
  >
  > Secure Web をバックグラウンドに置くと、ダウンロードが停止します。

- 現在のページビュー内で ［ページ内の検索］を使用して用語を見つけます。



動的テキストサポートによって、デバイスで設定するフォント設定が Secure Web に表示されます。

iOS データ保護

July 17, 2020

ASD（Australian Signals Directorate：オーストラリア通信電子局）のデータ保護要件を満たす必要がある企業では、Secure Mail および Secure Web の ［**iOS** データ保護を有効化］ポリシーを使用できます。デフォルトでは、これらのポリシーは ［オフ］になっています。

Secure Web の ［**iOS** データ保護を有効化］ポリシーが ［オン］のとき、Secure Web ではサンドボックス内のすべてのファイルに対してクラス A の保護レベルが適用されます。Secure Mail のデータ保護について詳しくは、「オーストラリア通信電子局のデータ保護」を参照してください。このポリシーを有効にすると最高のデータ保護クラスが使用されるので、［最小データ保護クラス］ポリシーも指定する必要はありません。

［**iOS** データ保護を有効化］ポリシーを変更するには

1. Endpoint Management コンソールを使用して Secure Web および Secure Mail の MDX ファイルを Endpoint Management に読み込みます：新しいアプリの場合、［構成］**>** ［アプリ］**>** ［追加］の順に選択して ［**MDX**］をクリックします。アップグレードについては、「MDX またはエンタープライズアプリのアップグレード」を参照してください。
2. Endpoint Management コンソールを使用して MDX ファイルを Endpoint Management に読み込みます：新しいアプリの場合、［構成］**>** ［アプリ］**>** ［追加］の順に選択して ［**MDX**］をクリックします。アップグレードについては、「アプリの追加」を参照してください。

3. Secure Mail の場合、［アプリ］設定に移動して［**iOS** データ保護を有効化］ポリシーを見つけ、［オン］に設定します。古いバージョンのオペレーティングシステムが動作するデバイスは、このポリシーを有効にしても影響を受けません。
4. Secure Web の場合、［アプリ］設定に移動して［**iOS** データ保護を有効化］ポリシーを見つけ、［オン］に設定します。古いバージョンのオペレーティングシステムが動作するデバイスは、このポリシーを有効にしても影響を受けません。
5. 通常通りアプリのポリシーを構成して設定を保存し、Endpoint Management アプリストアにアプリを展開します。

Secure Web の機能

June 22, 2020

Secure Web では、モバイルデータ交換技術を使用した専用の VPN トンネルが作成され、内部サイトや外部の Web サイトにアクセスできるようになります。これらのサイトには、組織のセキュリティポリシーで保護された環境で機密情報を含むサイトがあります。

Secure Mail および Citrix Files との連携により、Secure Web ではセキュアな Endpoint Management コンテナ内のシームレスなユーザーエクスペリエンスが提供されます。連携機能の例をいくつか示します:

- ユーザーが mailto リンクをタップすると、Secure Mail で新規メールメッセージ画面が開きます。資格情報を入力する必要はありません。
- **Secure Web** でリンクを開いてデータをセキュアな状態で保護する。Secure Web for iOS および Android では、ユーザーは専用の VPN トンネルによって機密情報があるサイトに安全にアクセスできます。Secure Mail から、Secure Web 内から、またはサードパーティ製アプリからリンクをクリックでき、Secure Web でリンクを開くため、データはセキュアな状態のままです。ユーザーは、Secure Web で ctxmobilebrowser(s) スキームを使用した内部リンクを開きます。このとき、先頭の「`ctxmobilebrowser://`」が「`http://.`」に変換されて HTTPS リンクが開かれます。「`ctxmobilebrowsers://`」は「`https://`」に変換されます。

この機能は、受信ドキュメント交換と呼ばれるアプリと MDX ポリシーとの相互作用によるものです。デフォルトでは、このポリシーは［制限なし］に設定されています。この設定では、URL を Secure Web で開くことができます。許可リストに登録されたアプリのみが Secure Web と機能できるように、ポリシー設定を変更できます。

- また、メールメッセージ内のイントラネットリンクをクリックすると Secure Web がサイトに移動して、資格情報を入力せずにイントラネットサイトにアクセスできます。
- ユーザーは、Secure Web を使用して Web からダウンロードしたデータを Citrix Files にアップロードできます。

また、Secure Web ユーザーは以下の操作も実行できます:

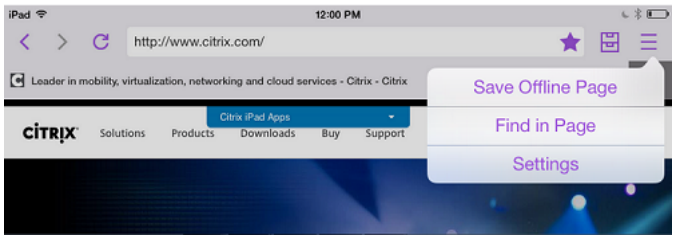
- ポップアップをブロックする。

> 注:
>
> Secure Web のメモリの大部分は、ポップアップのレンダリングで消費されます。そのため、通常、［設定］でポップアップをブロックすることで、パフォーマンスが向上します。

- お気に入りサイトをブックマークとして登録する。
- ファイルをダウンロードする。
- オフライン用にページを保存する。
- パスワードを自動保存する。
- キャッシュ、履歴、および Cookie を削除する。
- Cookie および HTML5 のローカルストレージの無効化。
- 他のユーザーとデバイスを安全に共有する。
- アドレスバー内で検索する。
- Secure Web で実行する Web アプリによる位置情報へのアクセスを許可します。
- 設定のエクスポートおよびインポート。
- ファイルをダウンロードすることなく Citrix Files でファイルを直接開く。この機能を有効にするには、Endpoint Management の「許可する URL」ポリシーに「**ctx-sf:**」を追加します。
- iOS で、3D タッチ操作でホーム画面から直接新しいタブを開いて、オフラインページ、お気に入りサイト、およびダウンロードにアクセスする。
- iOS で、あらゆるサイズのファイルをダウンロードし、Citrix Files やその他のアプリで開く。

  > 注:
  >
  > Secure Web をバックグラウンドに置くと、ダウンロードが停止します。

- 現在のページビュー内で ［ページ内の検索］を使用して用語を見つけます。



動的テキストサポートによって、デバイスで設定するフォント設定が Secure Web に表示されます。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States