業務用モバイルアプリ

Contents

業務用モバイルアプリのリリーススケジュール **2**

業務用モバイルアプリのサポート **3**

管理者のタスクと注意事項 **5**

プラットフォームごとの機能 **17**

Citrix Secure Hub **27**

Secure Mail の概要 **61**

Citrix Secure Web **62**

業務用モバイルアプリ向け **Citrix QuickEdit** **71**

ShareConnect **75**

Citrix ShareFile Workflows **87**

Citrix Content Collaboration for Endpoint Management **87**

EOL と廃止予定のアプリ **94**

Office 365 アプリとのセキュアな対話式操作の許可 **96**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

業務用モバイルアプリのリリーススケジュール

December 16, 2021

Citrix 業務用モバイルアプリのリリース間隔は 2 週間です。正確なリリース日は変更される可能性がありますが、このリリース間隔を意識することで、お客様が今後の計画を立てやすくなります。また、アプリの展開と更新もより管理しやすくする予定です。

Secure Mail と **Secure Web** の段階的なリリースプロセスについて

Secure Mail と Secure Web の新しいバージョンが利用可能になると、次のように段階的にリリースのロールアウトが行われます:

- iOS および Android ユーザーは、App Store および Google Play Store で Secure Mail と Secure Web の更新プログラムを入手します。ここで、更新プログラムを公開するユーザーの割合を 1 週間（7 日間）の間に増やしていきます。
- Secure Mail for iOS と Secure Web for iOS の新しいダウンロードファイルでは、この週の間に新しいバージョンが展開されます。Secure Mail for Android と Secure Web for Android の新しいダウンロードファイルでは、新しいリリースを受け取るユーザーの割合が 100%に達するまで、1 つ前のバージョンが実行されます。
- ユーザーに対して、一部の機能は段階的にリリースされます。

機能フラグ管理の前提条件

実稼働で Secure Hub または Secure Mail に問題が発生した場合、影響を受ける機能をアプリのコード内で無効化できます。無効化するには、機能フラグと、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。業務用モバイルアプリ 10.6.15 以降で MDX がドメインをトンネリングから除外する機能について詳しくは、MDX Toolkit のドキュメントを参照してください。機能フラグおよび LaunchDarkly に関する FAQ について詳しくは、Support Knowledge Centerの記事を参照してください。

> 注:
> 段階的に廃止される Citrix Endpoint Management の機能に関する事前の通知については、「廃止」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

業務用モバイルアプリのサポート

February 27, 2024

自動更新を有効にしているユーザーは、アプリストアから最新バージョンを受け取ります。業務用モバイルアプリの最新バージョンは、次のとおりです:

- 23.10.0（Secure Web for Android）
- 23.9.0（Secure Mail および Secure Web for iOS）
- 23.8.2（Secure Mail for Android）

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。業務用モバイルアプリの直近の 2 バージョンは、次のとおりです:

- 23.8.1（Secure Mail for Android）
- 23.8.0（Secure Web for Android）
- 23.7.0（Secure Mail for Android、Secure Mail for iOS）
- 23.5.0（Secure Mail for iOS および Secure Web for Android）
- 23.2.0（Secure Web for iOS）
- 22.9.1（Secure Web for iOS）

> 重要:
>
> MDX 暗号化は 2020 年 9 月 1 日に製品終了（EOL）に達しました。従来のデバイス管理（DA）に登録されているデバイスの場合:
>
> - MDX 暗号化を使用していない場合、対応は不要です。
> - MDX 暗号化を使用している場合は、Android デバイスを Android Enterprise に移行してください。Android 10 を実行しているデバイスは、Android Enterprise を使用して登録または再登録する必要があります。これには、MAM-only モードの Android デバイスが含まれます。詳しくは、「Device Administration から Android Enterprise への移行」を参照してください。

サポートされるオペレーティングシステム

業務用モバイルアプリは以下のいずれかのオペレーティングシステムをサポートします:

製品名	オペレーティングシステム	展開の最小バージョン	利用可能な最新バージョン
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x
Secure Mail	Android	8.x	14.x

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

製品名	オペレーティングシステム	展開の最小バージョン	利用可能な最新バージョン
Secure Web	iOS	13.x	17.x
	Android	8.x	14.x
	iOS	13.x	17.x

最新バージョンの業務用モバイルアプリは、最新バージョンと 2 つ前までのバージョンの Citrix Endpoint Management と互換性があります。Citrix Endpoint Management でサポートされるオペレーティングシステムについて詳しくは、「サポートされるデバイスオペレーティングシステム」を参照してください。

最新バージョンの業務用モバイルアプリには、最新バージョンの Secure Hub が必要です。Secure Hub を最新の状態に保つようにしてください。

> 注:
>
> Citrix は常に、最新および直近の 2 つの Android および iOS オペレーティングシステム（N、N-1、および N-2）のみをサポートします。

その他の考慮事項と制限事項

段階的に廃止される Citrix Endpoint Management の機能に関する事前の通知については、「廃止」を参照してください。

Secure Mail

- Secure Ticket Authority（STA）および Secure Mail の問題により、Endpoint Management では現在 NetScaler 12.0.41.16 はサポートされていません。この問題は、NetScaler 12.0 ビルド 41.22 で解決されています。
- Exchange 2007 および Lotus Notes 8.5.3 用の Secure Mail のサポートは、2017 年 9 月 30 日に終了（EOL：End of Life）しました。
- Citrix Files の添付ファイルを送信するときのパフォーマンスを向上させるため、最新バージョンの Citrix Files を使用してください。Citrix Files は Windows ではサポートされていません。
- IBM Notes 環境では、IBM Domino Traveler サーバーのバージョン 9.0 が構成されている必要があります。詳しくは、「Exchange Server または IBM Notes Traveler Server の統合」を参照してください。

> 注:
>
> - Citrix Files for XenMobile は、2023 年 7 月 1 日に製品終了（EOL）になりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Web

デバイスに Android WebView の最新バージョンをインストールします。Android WebView は Google Play ストアからダウンロードできます。

QuickEdit

QuickEdit は業務用モバイルアプリとして継続します。以前お知らせしていましたが、2018 年 9 月 1 日に製品終了（EOL）ステータスは適用されません。

Citrix Content Collaboration for Endpoint Management

また Citrix Content Collaboration for Endpoint Management については、バージョン 6.5 以降は、パブリックアプリストアからアクセスします。

ShareConnect

ShareConnect は、2020 年 6 月 30 日に製品終了（EOL）になりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

Citrix Secure Notes および Citrix Secure Tasks

Citrix Secure Notes および Citrix Secure Tasks は 2018 年 12 月 31 日に製品終了（EOL）となりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

管理者のタスクと注意事項

October 31, 2022

ここでは、業務用モバイルアプリの管理者に関連するタスクと注意事項について説明します。

フィーチャーフラグ管理

実稼働で業務用モバイルアプリに問題が発生した場合、影響を受ける機能をアプリのコード内で無効にできます。iOS および Android 用の Secure Hub、Secure Mail、Secure Web で機能を無効にできます。無効化するには、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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。MDX がドメインをトンネリングから除外する機能について詳しくは、MDX Toolkit のドキュメントを参照してください。

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

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

ドメインごとの許可リストを作成する

以前は、内部ポリシーが IP アドレスの一覧のみを必要とする場合に使用できる IP アドレス一覧を提供していました。インフラストラクチャの機能向上に伴い、2018 年 7 月 16 日以降、Citrix ではパブリック IP アドレスの使用を段階的に停止しています。そのため、可能な場合はドメインごとの許可リストを作成することをお勧めします。

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。

> 注:
>
> パブリックアプリストアのアプリを初めて展開する場合は、新しくインストールする必要があります。現在のラッピングされたエンタープライズバージョンのアプリをパブリックストアバージョンにアップグレードすることはできません。
>
> パブリックアプリストアでの配信では、Citrix が開発したアプリを MDX Toolkit で署名およびラッピングしません。MDX Toolkit を使って、サードパーティ製アプリまたはエンタープライズアプリをラッピングできます。

LaunchDarkly のシステム要件

- Endpoint Management 10.7 以降。
- Citrix ADC の分割トンネリングが ［オフ］ に設定されている場合、アプリが以下のサービスと通信できることを確認してください:
  - LaunchDarkly サービス

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- APNs リスナーサービス

サポートされるアプリストア

業務用モバイルアプリは、Apple App Store や Google Play で入手できます。

中国では、Google Play を使用できないため、Secure Hub for Android は以下のアプリストアで入手できます:

- https://shouji.baidu.com
- https://apk.hiapk.com
- https://apk.91.com

パブリックアプリストアでの配信の有効化

1. Endpoint Management のダウンロードページから、iOS と Android の両方のパブリックストア向け.mdx ファイルをダウンロードします。
2. Endpoint Management コンソールに.mdx ファイルをアップロードします。パブリックストアバージョンの業務用モバイルアプリは今までどおり MDX アプリケーションとしてアップロードします。パブリックストアアプリとしてサーバーにアップロードしないでください。手順については、「アプリの追加」を参照してください。
3. セキュリティポリシーに基づくデフォルト設定からポリシーを変更します（オプション）。
4. 必須アプリとしてプッシュ配信します（オプション）。この手順は、お使いの環境でモバイルデバイス管理が有効になっている必要があります。
5. App Store、Google Play、または Endpoint Management アプリストアからデバイスにアプリをインストールします。
   - Android では、アプリをインストールするときに Play Store に移動されます。iOS では、MDM による展開で、ユーザーは App Store に移動することなくアプリがインストールされます。
   - App Store または Play ストアからアプリをインストールすると、次のアクションが発生します。対応する.mdx ファイルがサーバーにアップロードされていれば、アプリは管理対象アプリケーションになります。管理対象アプリに移行すると、アプリは Citrix PIN の入力を要求します。Citrix PIN を入力すると、Secure Mail でアカウント構成画面が表示されます。
6. アプリにアクセスできるのは、デバイスを Secure Hub に登録し、対応する.mdx ファイルがサーバーにある場合のみです。いずれかの条件が満たされていない場合、アプリをインストールすることはできますが、アプリの使用がブロックされます。

パブリックアプリストアにある Citrix Ready Marketplace のアプリを現在利用中であれば、展開プロセスについてはすでに精通しているはずです。業務用モバイルアプリでは、多くの独立系ソフトウェアベンダーが現在使用しているアプローチを採用しています。アプリ内に MDX SDK を埋め込み、アプリをパブリックストア対応にします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> iOS および Android 対応の Citrix Files アプリのパブリックストアバージョンは、ユニバーサルアプリになりました。Citrix Files アプリは、スマートフォンとタブレットで同じです。

Apple プッシュ通知サービス

プッシュ通知の構成について詳しくは、「プッシュ通知用 Secure Mail の構成」を参照してください。

パブリックアプリストアのよくある質問

- パブリックストアアプリの複数のコピーを複数のユーザーグループに展開できますか。たとえば、複数のポリシーを複数のユーザーグループに展開する場合があります。

  ユーザーグループごとに異なる.mdx ファイルをアップロードします。ただし、この場合、1 人のユーザーが複数のグループに属することはできません。ユーザーが複数のグループに属していた場合、そのユーザーには同じアプリの複数のコピーが割り当てられます。パブリックストアアプリの複数のコピーを同じデバイスに展開することはできません。アプリの ID を変更できないからです。

- 必須アプリとしてパブリックストアアプリをプッシュ配信できますか。

  はい。アプリをデバイスにプッシュ配信するには MDM が必要です。MAM-only 展開をサポートしていません。

- トラフィックポリシーまたはユーザーエージェントに基づく Exchange Server のルールの更新は必要ですか。

  ユーザーエージェントベースポリシーやルールに対するプラットフォームごとの文字列は以下のとおりです。

  > 注:
  >
  > Secure Notes および Secure Tasks は 2018 年 12 月 31 日に製品終了（EOL）となりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

Android

アプリ	サーバー	ユーザーエージェント文字列
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

アプリ	サーバー	ユーザーエージェント文字列
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

アプリ	サーバー	ユーザーエージェント文字列
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- アプリのアップグレードはしなくてもいいですか。

  いいえ。更新プログラムがパブリックアプリストアにポストされると、自動更新を有効にしているユーザーはすべてこの更新プログラムを受信します。

- アプリのアップグレードを強制することはできますか。

  はい、アップグレードはアップグレード猶予期間ポリシーによって強制できます。更新バージョンのアプリに対応する新しい.mdx ファイルが Endpoint Management にアップロードされると、このポリシーは設定されます。

- 更新スケジュールを調整できない場合、更新を受信する前にアプリをテストする方法はありますか。

  Secure Hub の手順と同様に、EAR 期間中に TestFlight for iOS でアプリのテストができます。Android の場合、アプリは Google Play ベータプログラムによって EAR 期間中に利用できます。この期間中はすべてのアプリの更新プログラムをテストできます。

- 自動更新プログラムがユーザーデバイスに送信される前に新しい.mdx ファイルに更新しないとどうなりますか。

  更新されたアプリは、古い.mdx ファイルとの互換性を維持します。新しいポリシーに依存した新機能は使えません。

- Secure Hub がインストールされていればアプリを管理対象に移行できますか、それともアプリの登録が必要ですか。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

パブリックストアアプリを管理対象アプリ（MDX で保護）としてアクティブ化して使用できるようにするには、Secure Hub へのユーザー登録が必要です。Secure Hub がインストールされていても登録していなければ、ユーザーはパブリックストアアプリを利用できません。

- パブリックストアアプリに Apple Enterprise デベロッパーアカウントは必要ですか。

  いいえ。現在は Citrix が証明書を管理し、業務用モバイルアプリ用のプロファイルをプロビジョニングしているため、アプリをユーザーに展開するために Apple Enterprise デベロッパーアカウントは不要です。

- エンタープライズ配信の終了はこれまで展開したラップされたアプリケーションにも適用されますか。

  いいえ、次の業務用モバイルアプリにのみ適用されます：Secure Mail、Secure Web、Citrix Content Collaboration for Endpoint Management、QuickEdit、ShareConnect。展開したラップ済みエンタープライズアプリ（社内開発またはサードパーティ製）はエンタープライズラッピングを使い続けることができます。MDX Toolkit はアプリ開発者向けにエンタープライズラッピングのサポートを継続します。

- Google Play からアプリをインストールすると、Android エラー（エラーコード「505」）が発生します。

  > 注：
  >
  > Android 5.x のサポートは、2018 年 12 月 31 日に終了しました。

  これは、Google Play と Android 5.x バージョンで発生する既知の問題です。このエラーが発生した場合、以下の手順に従って、アプリのインストールを妨げているデバイス上の古いデータをすべて除去できます：

1. デバイスを再起動します。
2. デバイス設定で Google Play のキャッシュとデータをクリアします。
3. 最終手段として、デバイスの Google アカウントを削除してからもう一度追加します。

詳しくは、「Fix Google Play Store Error 505 in Android: Unknown Error Code」というキーワードを使用してこのサイトを検索してください。

- Google Play でアプリが実稼働環境向けにリリースされ、新しいベータリリースがない場合でも、Google Play のアプリタイトルに「Beta」が表示され続けるのはなぜですか。

  アーリーアクセスリリース（EAR）プログラムに参加している場合、必ずアプリタイトルの横に「Beta」と表示されます。これは単純に、特定のアプリへのユーザーのアクセスレベルを示しています。「Beta」がついている名前は、ユーザーが利用可能なアプリの最新バージョンを受け取っていることを示しています。最新バージョンとは、実稼働トラックまたはベータトラックに公開されている最も新しいバージョンとなります。

- .mdx ファイルが Endpoint Management コンソールにある場合でもアプリをインストールして開くと、「承認されていないアプリ」というメッセージが表示されます。

  この問題は、App Store または Google Play からアプリを直接インストールして Secure Hub を更新していない場合に発生する可能性があります。Secure Hub は、Inactivity Timer が期限切れしたときに更新する必要があります。ポリシーは、ユーザーが Secure Hub を開いて再認証したときに更新されます。アプリは、ユーザーが次回アプリを開いたときに認証されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- アプリを利用するためにアクセスコードは必要ですか。App Store や Play Store からアプリをインストールするとき、アクセスコードの入力を促す画面が表示されます。

  アクセスコードの要求画面が表示される場合、Secure Hub で Endpoint Management に登録されていません。Secure Hub で登録してアプリ用の.mdx ファイルが確実にサーバーに展開されていることを確認してください。また、アプリを使用できることも確認してください。アクセスコードは、Citrix 内部使用のみに制限されています。アプリを有効化するには Endpoint Management の展開が必要です。

- VPP または DEP 経由で iOS パブリックストアアプリを展開できますか。

  Endpoint Management は、MDX 対応ではないパブリックストアアプリの VPP ディストリビューション用に最適化されています。Endpoint Management パブリックストアアプリを VPP で配布することはできますが、Endpoint Management および Secure Hub ストアに追加の拡張を行って制限に対応しない限り、展開は最適ではありません。VPP 経由の Endpoint Management パブリックストアアプリの展開に関する既知の問題と想定される解決策の一覧は、Citrix Knowledge Centerのトピックを参照してください。

業務用モバイルアプリに対する **MDX** ポリシー

MDX ポリシーでは、Endpoint Management で適用される設定を構成できます。ポリシーは認証、デバイスセキュリティ、ネットワーク要件およびアクセス、暗号化、アプリ相互作用、アプリ制限などに対応します。多くの MDX ポリシーがすべての業務用モバイルアプリに適用されます。一部のポリシーはアプリ固有のものです。

ポリシーファイルは、業務用モバイルアプリのパブリックストアバージョンの MDX ファイルとして提供されます。アプリを追加する場合は、Endpoint Management コンソールでポリシーを構成することもできます。

MDX ポリシーについて詳しくは、このセクションの次の記事を参照してください:

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

次のセクションでは、ユーザー接続に関連する MDX ポリシーについて説明します。

Secure Mail 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）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、現在の MDX Toolkit から新しい MAM SDK に移行する方法を提供します。デュアルモードにより、次のいずれかの方法を利用できます。

- MDX Toolkit（Endpoint Management コンソールでの現在の名前は「レガシ MDX」）を使用するアプリを引き続き管理する

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 新しい MAM SDK を組み込んだアプリを管理する

  > 注:
  >
  > MAM SDK を使用する場合、アプリをラップする必要はありません。

MAM SDK に切り替えた後は、追加の手順は必要ありません。

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。

> 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

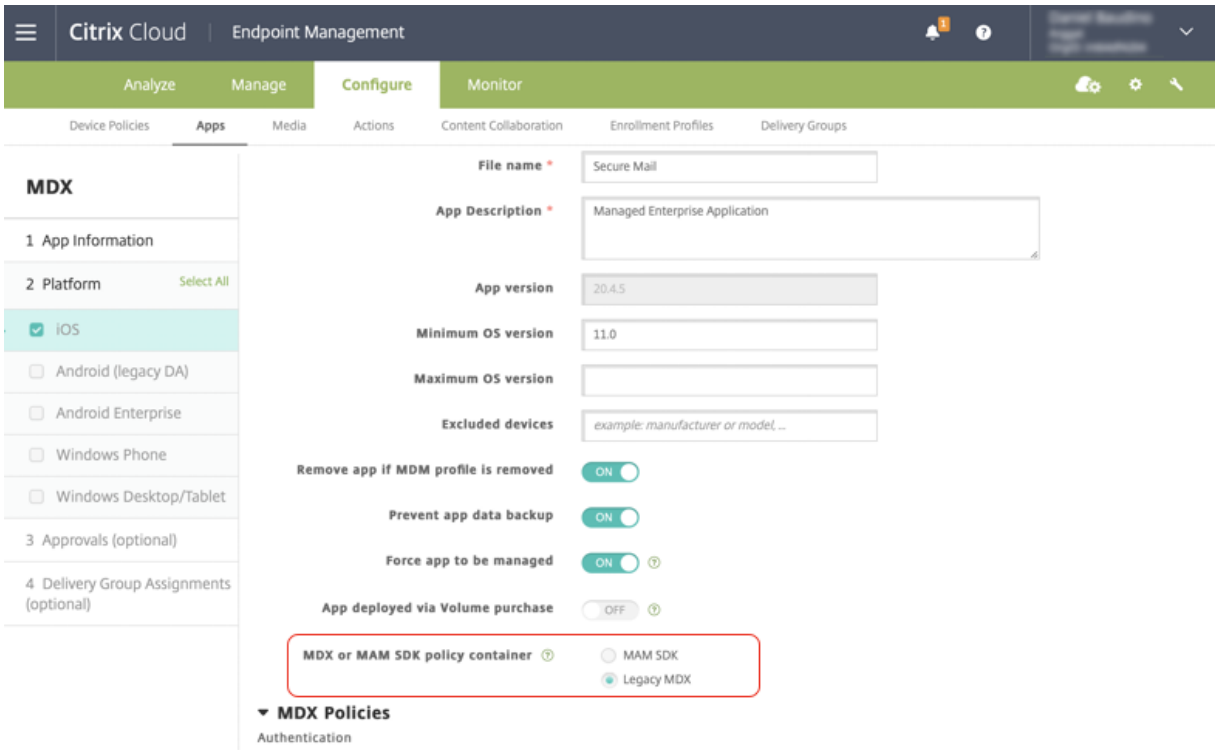
- MAM SDK は、Citrix Endpoint Management 展開の Android Enterprise プラットフォームで公開されたアプリのみをサポートします。新しく公開されたアプリの場合、デフォルトの暗号化はプラットフォームベースの暗号化です。
- MAM SDK はプラットフォームベースの暗号化のみをサポートし、MDX 暗号化はサポートしません。
- Citrix Endpoint Management を更新せず、モバイルアプリのポリシーファイルがバージョン 20.8.0 以降で実行されている場合は、Secure Mail 用にネットワークポリシーの重複エントリが作成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

Citrix Endpoint Management で Secure Mail 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。

［**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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **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 ［レガシ **MDX**］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。

内部ネットワークへのユーザー接続

内部ネットワークをトンネルする接続は、完全 VPN トンネルまたはクライアントレス VPN の一種である「トンネル - Web SSO」を使用できます。優先 VPN モードポリシーがこれを制御します。デフォルトでは、SSO が必要な接続にはトンネル - Web SSO が推奨されます。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 トンネル設定を推奨します。この設定は、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。

[VPN モードの切り替えを許可］ポリシーにより、完全 VPN トンネルモードとトンネル-Web SSO モードを必要に応じて自動的に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、トンネル- Web SSO モードでは処理できません。同様に、[トンネル Web SSO］モードの使用時には、HTTP 認証チャレンジが SSO で実行される可能性が高くなります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ネットワークアクセス制限

ネットワークアクセスポリシーは、ネットワークアクセスを制限するかしないかを指定します。デフォルトでは、Secure Mail のアクセスは無制限で、ネットワークアクセスに制限はありません。アプリはデバイスが接続されるネットワークに無制限にアクセスします。デフォルトでは、Secure Web アクセスは内部ネットワークにトンネルされ、内部ネットワークに戻るアプリケーションごとの VPN トンネルは、すべてのネットワークアクセスに使用されて、Citrix ADC 分割トンネル設定が使用されます。またブロックされるアクセスを指定して、デバイスがネットワークに接続していないようにアプリを操作できます。

AirPrint、iCloud、Facebook および Twitter の API といった機能を有効にする場合は、ネットワークアクセスポリシーをブロックしないでください。

また、ネットワークアクセスポリシーはバックグラウンドネットワークサービスポリシーと相互に作用します。詳しくは、「Exchange Server または IBM Notes Traveler Server の統合」を参照してください。

Endpoint Management クライアントプロパティ

クライアントプロパティには、ユーザーのデバイスの Secure Hub に直接提供される情報が含まれています。クライアントのプロパティは Endpoint Management コンソールの ［設定］**>**［クライアント］**>**［クライアントプロパティ］にあります。

クライアントのプロパティは次のような設定を構成するために使用されます:

ユーザーパスワードのキャッシュ

ユーザーパスワードキャッシュにより、ユーザーの Active Directory パスワードをモバイルでバス上にローカルでキャッシュできます。ユーザーパスワードのキャッシュを有効にすると、ユーザーは Citrix PIN またはパスコードを設定するよう求められます。

Inactivity Timer

ユーザーがデバイスを非アクティブにした後で、Citrix PIN またはパスコードの入力を求められずにアプリにアクセスできる時間（分単位）を定義します。MDX アプリでこの設定を有効にするには、［アプリのパスコードポリシー］を ［オン］にする必要があります。［アプリのパスコードポリシー］が ［オフ］である場合、ユーザーは完全認証を実行するよう Secure Hub へリダイレクトされます。この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。

Citrix PIN 認証

Citrix PIN は、ユーザー認証工程を簡素化します。PIN は、クライアント証明書をセキュリティで保護するため、または Active Directory 資格情報をデバイス上にローカルに保存するために使用されます。PIN 設定を構成すると、

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ユーザーのサインオン工程は次のようになります。

1. ユーザーが初めて Secure Hub を起動したときに PIN の入力が求められ、Active Directory 資格情報がキャッシュされます。
2. それ以降は、Secure Mail などの業務用モバイルアプリを起動する場合に PIN を入力してサインインします。

クライアントのプロパティを使って PIN 認証を有効にし、PIN の種類を指定し、また PIN の強さや長さも指定して、要件を変更します。

指紋認証または **Touch ID** 認証

iOS デバイスの指紋認証（Touch ID 認証）は、Citrix PIN の代わりに使用できます。この機能は、Inactivity timer がタイムアウトした場合など、Secure Hub 以外のラップされたアプリでオフライン認証が必要なときに便利です。この機能は、次の認証シナリオで有効化できます。

- Citrix PIN+ クライアント証明書構成
- Citrix PIN+ キャッシュされた AD パスワード構成
- Citrix PIN+ クライアント証明書構成およびキャッシュされた AD パスワード構成
- Citrix PIN がオフ

指紋認証が失敗した場合、またはユーザーが指紋認証プロンプトをキャンセルした場合は、ラップされたアプリは Citrix PIN または AD パスワード認証にフォールバックします。

指紋認証の要件

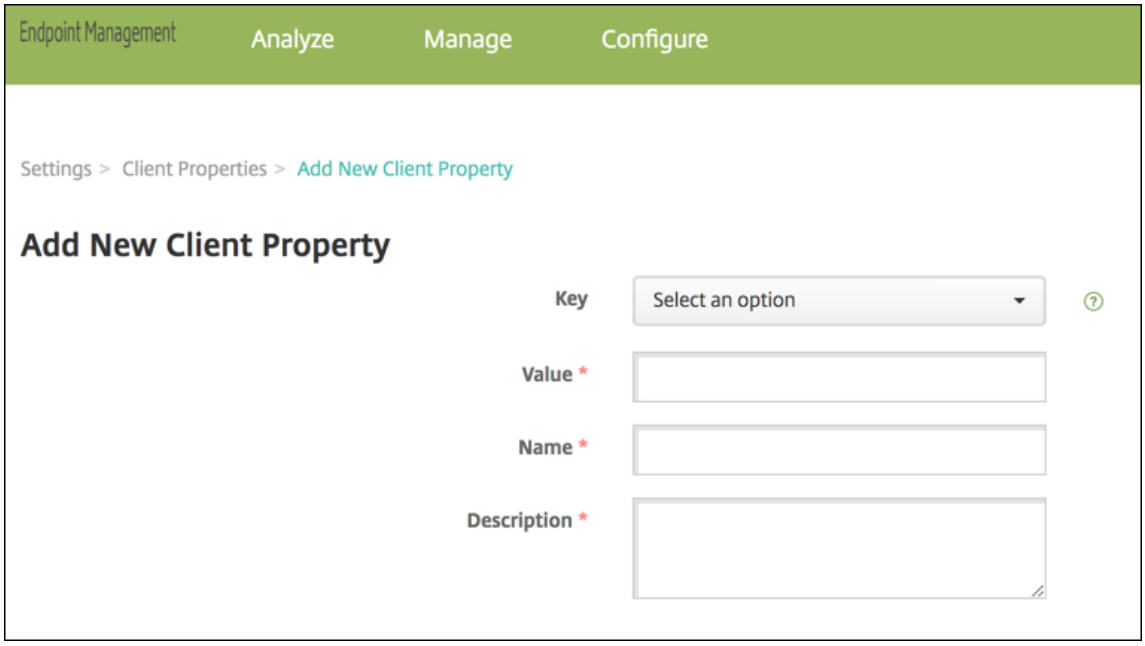
- 指紋認証をサポートし、1 つ以上の指紋が構成されている iOS デバイス（バージョン 8.1 以上）
- ユーザーエントロピーがオフである

指紋認証を設定するには

> 重要:
>
> ユーザーエントロピーがオンの場合、Enable Touch ID Authentication プロパティは無視されます。ユーザーエントロピーは、Encrypt secrets using the Passcode キーによって有効化されます。

1. Endpoint Management コンソールで、［設定］**>**［クライアント］**>**［クライアントプロパティ］の順に選択します。
2. ［追加］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. **ENABLE_TOUCH_ID_AUTH** キーを追加し、その ［値］を ［**True**］、ポリシー名を ［指紋認証機能を有効にする］に設定します。

指紋認証を設定した後、デバイスを再登録する必要はありません。

パスコードキーおよびクライアントプロパティを使用したシークレットの暗号化全般についてについて詳しくは、「クライアントプロパティ」を参照してください。

Google Analytics

Citrix Secure Mail は、Google Analytics を使用してアプリ統計情報と使用状況情報の分析データを収集し、製品の質を向上させます。Citrix は、その他の個人ユーザー情報を収集または保存しません。

Google Analytics を無効にする

管理者は、**DISABLE_GA** という名前のカスタムクライアントプロパティを構成することで Google Analytics を無効にできます。Google Analytics を無効にするには、以下を実行します:

1. Citrix Endpoint Management コンソールにサインインし、［設定］ > ［クライアント プロパティ］ > ［新しいクライアント プロパティの追加］の順に移動します。
2. 値 **DISABLE_GA** を ［キー］フィールドに追加します。
3. クライアントプロパティの値を **true** に設定します。

> 注:
>
> Citrix Endpoint Management コンソールで値 **DISABLE_GA** を構成しない場合、Google Analytics のデ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ータはアクティブです。

プラットフォームごとの機能

September 12, 2023

以下の表は、Citrix 業務用モバイルアプリの機能の概要です。プロットフォームごとに使用可能な機能について O で示しています。QuickEdit の機能について詳しくは、Citrix QuickEdit の記事を参照してください。

Citrix Secure Hub

機能	iOS	Android
サインオンして認証	X	X
ポリシー遵守の監視	X	X
アプリやデスクトップへアクセス	X	X
HDX アプリとデスクトップ	X	X
エラーログの作成と送信	X	X
ログにスクリーンショットを添付	X	X
アプリ内でヘルプデスクへ連絡	X	X
アプリ内で Citrix サポートへの連絡	X	X
クラッシュ発生時の情報収集と分析	X	X
オフライン認証	X	X
Citrix Secure Mail でのログ送信	X	X
Google Analytics	X	X
縦長および横長モード	X	X
アプリを信頼するためのアプリ内ガイド	X	X
メールで登録した場合の、Secure Mail での自動登録（MAM only）	X	X
Touch ID オフライン認証	X	X
派生資格情報を使用した登録	X	
生体認証		X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
Workspace アプリストアの使用	X	X

Citrix Secure Mail

機能	iOS	Android
電子メールの生産性		
ドラフトの最小化	X	X
送信したメールを元に戻す		X
暗号化管理	X	X
カレンダーの予定リストウィジェット		X
Secure Mail の連絡先の写真	X	X
応答性メールのサポート	X	X
下書きフォルダーの自動同期	X	X
下書きフォルダーでの添付ファイルの同期		X
メールの送信、受信、返信、全員へ返信、転送	X	X
下書きの作成、編集、削除	X	X
メールにフラグ設定	X	X
未読にする	X	X
すべてのフォルダーおよびサブフォルダーの表示	X	X
アプリがバックグラウンドにある場合に下書きを自動保存	X	X
Citrix Secure Notes でのメモへのメール。重要：Secure Notes は 2018 年 12 月 31 日に製品終了（EOL）となりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
メールの検索（ローカルおよびサーバー）	X	X
メールの同期間隔の選択（最大 1 か月またはすべてのメール）	X	X
未読メッセージの表示	X	X
セキュアな添付ファイル表示/画像、動画、および音声の再生	X	X
複数の添付ファイル	X	X
添付ファイルの返信および転送	X	X
Citrix Files からのファイル添付	X	X
Citrix Files Restricted Zones およびコネクタからのファイル添付	X	X
添付ファイルリポジトリ	X	X
リッチテキスト編集	X	X
件名によるメール通知、ロック画面でのプレビュー	X	X
通知画面からのメールおよび出席依頼への返信と削除	X	
写真の添付または撮影	X	X
複数のメッセージの選択	X	X
添付ファイルのダウンロード	X	X
画像インラインの読み込み	X	X
高速並べ替え	X	X
添付された ZIP ファイルの送信、受信、展開、および保存	X	X
画面の縦向きおよび横向き	○：メール一覧、メール読み取り、作成、カレンダー、および連絡先ビュー	○：メール読み取りおよび作成ビューのみ
貼り付け文字列で書式設定を維持	X	X
連絡先からの SMS	X	X
連絡先からの FaceTime	X	
接続の問題または送信トレイがいっぱいなことによるメッセージの未送信	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
最近使ったフォルダーのバブルアップ		X
プルダウンメール更新	X	X
最終更新タイムスタンプ	X	X
メッセージ操作のための左スワイプ	X	X
Microsoft Exchange および IBM Notes Traveler のサポート	X	X
メール、カレンダー、連絡先をタップして更新	X	X
メールビューでのデバイスのアクセシビリティ/フォントサイズの設定の許可	X	X
S/MIME 署名と暗号化	X	X
メールを介した S/MIME cert インポート	X	X
S/MIME、Intercede 統合	X	
S/MIME、Entrust 統合	X	
メッセージ本文の Microsoft IRM 保護	X	X
プッシュ通知	X	X
受信トレイへのプッシュ通知による、カレンダーを含む全フォルダーの自動更新	X	
Office 365 ドキュメントを開く	X	X
3D タッチ操作	X	
ロック画面上のコンテキストアイコン	X	X
フォルダーの検索	X	X
VIP メールフォルダー	X	X
動的な入力のサポート	X	X
拡張フォルダーの維持	X	X
メッセージ分類マーカー	X	X
スペルチェック	X	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
最後に撮影した写真の添付	X	X
URL のプレビュー	X	X
Citrix Files での Citrix Files リンクのオープン	X	X
`.pass`ファイルのサポート	X	
検索モードでの複数のメールの選択	X	X
インラインイメージの挿入	X	X
Exchange ActiveSync（EAS）バージョン 16 へのアップグレード	X	X
ユーザーによる不明ドメインや個人用ドメイン使用の制限	X	
スーパーワイドデバイス画面のサポート		X
複数の Exchange アカウントの構成	X	X
左または右へのスワイプによる他の操作の実行	X	X
暗号化されたメールの返信メールや転送メールの暗号化	X	
メールとインラインイメージの印刷	X	
設定で［行のプレビュー］を使用して、メールボックスのプレビュー表示にメール本文を何行表示するかを構成	X	
応答性メールのサポート	X	X
添付ファイルのアプリ内プレビュー（MS Office ファイルまたは画像）	X	X
個人用連絡先グループ	X	X
ユーザー名をメールアドレス（UPN）に移行	X	X
フィッシングメールの報告	X	X
先進認証（OAuth）	X	X
添付ファイルの印刷	X	
Android Enterprise（Android for Work）	X	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
リッチテキスト署名	X	
リッチプッシュ通知	X	
フィード	X	X
写真の添付の機能強化	X	X
グループ通知	X	
Slack 統合（プレビュー）	X	X
フィードを管理	X	
内部ドメイン	X	X
フィードの管理	X	X
MS Teams との統合	X	X
自己診断（トラブルシューティング）オプション		X
デュアルモード（MAM SDK）	X	X
自己診断ツール		X
カレンダー		
ICS ファイルをカレンダーイベントとしてプレビューおよびインポート		X
カレンダーイベントをドラッグアンドドロップ	X	X
日、週、月、および予定一覧の表示	X	X
ロック画面上の詳細なアラーム	X	X
6 か月間の同期	X	X
イベントをプライベートとして設定	X	X
最初のイベントの前の時間にスクロール	X	
手動更新オプション	X	X
アラームの設定	X	X
タップによる住所の地図表示	X	X
週番号	X	X
動的な入力のサポート	X	X
セキュリティ分類マーカー	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
住所をロングタップ	X	
稼働週の開始日の設定	X	X
選択した日付の週のフォーカス表示	X	
現在の日付は常に強調表示	X	X
添付リポジトリからのカレンダー添付ファイル	X	X
個人用カレンダーのサポート	X	X
個人用カレンダーイベントの競合を表示		X
カレンダーイベントの印刷	X	
カレンダーの件名で電話番号とWeb アドレスをタップ	X	
カレンダーを検索	X	
会議		
会議を返信、全員に返信、転送	X	X
招待への返信についての主催者のビュー	X	X
提案した時間に対する招待者の空き時間についての主催者のビュー	X	X
タップしてオンライン会議へ参加。注：WebEx および Lync の場合、アプリを有効にするためには Citrix Endpoint Management でポリシーを設定する必要があります。	X	X
タップして音声会議へ参加	X	X
新しい出席依頼のオンライン会議、音声、電話会議のスケジュール	X	X
新しい出席依頼への ShareFile リンクの追加	X	X
添付ファイルの付いた出席依頼の転送	X	X
タップして「遅刻」メールの送信	X	X
タップして会議主催者へ返信	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
タップしてすべての会議への招待に返信	X	X
タップして会議の全招待者へ返信	X	X
タップして会議の全招待者へ添付ファイル付で返信	X	X
GoToMeeting へのダイヤルイン	X	X
ロック画面または通知画面からの出席依頼への返信	X	X
WebEx または Lync 会議へのダイヤルイン	X	X
拒否されたイベントを隠す	X	X
3 つ以上の同時進行イベントの表示	X	X
出席依頼状況のクイックビュー	X	X
キャンセルされたイベントの削除、返信、全員に返信、コメントの追加	X	X
転送された招待での主催者名の表示	X	X
共有デバイス	X	X
Skype for Business 会議への参加	X	X
会議通知への応答（承諾、辞退、仮承諾など）	X	X
メッセージ通知への応答（返信、削除）	X	
連絡先		
［連絡先］でのフォルダーの作成		X
連絡先の双方向同期	X	X
詳細な連絡先情報（GAL 検索）	X	X
ローカルの連絡先への Secure Mail 連絡先のエクスポートと同期	X	X
連絡先：お気に入りおよびカテゴリ		X
エクスポートを許可する連絡先フィールドの制御	X	X
Secure Mail で管理していない連絡先の詳細	X	X
動的な入力のサポート	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
連絡先を VIP としてマーク	X	X
.vcardsとの連絡先の共有	X	X
長押しで連絡先を表示		X
ネイティブメールアカウントが存在する場合の連絡先のエクスポート	X	X
フォルダーおよびサブフォルダーの表示	X	
デバイス上で構成される設定		
iMessage のサポート	X	
通知を制御するための詳細オプション	X	X
ロック画面での通知	X	X
メールとカレンダーの通知音	X	X
フォルダーの自動更新	X	X
所属組織内および所属組織外への不在通知の設定	X	X
削除の前に確認する	X	X
スレッド形式の会話または時系列ビュー	X	X
Wi-Fi での添付ファイルのロード	X	X
Wi-Fi での添付ファイルのロードのデフォルト設定	X	X
メールを同期する期間の設定	X	X
無制限同期/すべてのメールの同期		X
メール署名の設定	X	X
名または姓による連絡先の一覧	X	X
自動表示	X	X
ホームタイムゾーンを使用する		X
迅速な応答のテンプレート		X
メール構成頻度のプッシュ		X
設定のエクスポート/インポート	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
デバイスの戻るボタンをタップしてフローティング動作設定ボタンオプションを閉じる		X
Microsoft Teams	X	X

Citrix Secure Web

機能	iOS	Android
マルチタスクによる 2 つのアプリの同時使用	X	
ファイルのダウンロード	X	X
お気に入りに追加	X	X
保存されたユーザー名とパスワードのクリア	X	X
キャッシュ、履歴、および Cookie の削除	X	X
ポップアップをブロック	X	X
オフラインページで保存	X	X
アドレスバーでの検索	X	X
通知からダウンロードされた項目を開く	X	X
パスワードの自動保存	X	X
プロキシサポート		
エンタープライズプロキシ	X	X
URL の禁止リストと許可リスト	X	X
履歴	X	X
既定のホームページ	X	X
タブ	X	X
ブックマークのプッシュ	X	X
画面キャプチャのブロック		X
現在のページを検索	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

機能	iOS	Android
3D タッチ操作	X	
共有デバイス	X	X
ファイル改ざん防止（共有デバイスの場合）	X	
設定のエクスポート/インポート	X	X
縦長および横長モード	X	X
Android Enterprise（Android for Work）		X
画面上のコンテンツをプルして更新	X	X
デフォルトブラウザーとしての Secure Web		X

Citrix Secure Hub

February 27, 2024

Citrix Secure Hub は、業務用モバイルアプリへの入り口です。ユーザーは Secure Hub にデバイスを登録して、アプリストアにアクセスします。アプリストアから、Citrix の業務用モバイルアプリとサードパーティ製アプリを追加できます。

Secure Hub およびその他のコンポーネントは、Citrix Endpoint Management のダウンロードページからダウンロードできます。

Secure Hub および業務用モバイルアプリの他のシステム要件については、「システム要件」を参照してください。

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。

次のセクションでは、Secure Hub の最新リリースおよび以前のリリースの新機能について説明します。

> 注:
>
> Secure Hub の Android 6.x および iOS 11.x バージョンのサポートは、2023 年 10 月に終了しました。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

最新バージョンの新機能

Secure Hub for Android 23.12.0

サインインページに認証 **PIN** に関するヒントを追加する　23.12.0 リリース以降、サインインページに認証 PIN に関するヒントを追加できるようになりました。この機能はオプションであり、2 要素認証に登録されたデバイスに適用されます。ヒントにより、PIN にアクセスする方法がわかります。

ヒントはテキストまたはリンクとして構成できます。ヒントのテキストでは PIN に関する簡単な情報が提供され、リンクでは PIN へのアクセス方法に関する詳細情報が提供されます。ヒントの構成方法について詳しくは、「Citrix Endpoint Management コンソールを使用したヒントの構成」を参照してください。

nFactor 認証によるシングルサインオン機能のサポート　Secure Hub for Android バージョン 23.12.0 以降、nFactor のモバイルアプリケーション管理（MAM：Mobile Application Management）登録またはログインはシングルサインオン（SSO）機能をサポートします。この機能により、以前に入力したサインイン資格情報が MAM 登録またはログインプロセスを通過できるため、ユーザーが再度手動でサインイン資格情報を入力する必要がなくなります。nFactor SSO プロパティについて詳しくは、Citrix Endpoint Management ドキュメントの「クライアントプロパティリファレンス」を参照してください。

直接起動モードでの完全なワイプのサポート　以前は、再起動したデバイスで完全なワイプコマンドを実行するには、デバイスのロックを解除する必要がありました。今回、デバイスがロックされている場合でも、直接起動モードで完全なワイプコマンドを実行できるようになりました。この機能は、特にデバイスが権限のない個人によって所有されている場合に、セキュリティの観点から役立ちます。完全なワイプコマンドについて詳しくは、Citrix Endpoint Management のドキュメントの「セキュリティ操作」を参照してください。

Secure Hub の **App Store** の読み込み速度を最適化　Secure Hub の App Store の読み込みが以前より速くなり、ユーザーはより迅速にアクセスできるようになりました。

以前のバージョンの新機能

Secure Hub for iOS 23.11.0

サインインページに認証 **PIN** に関するヒントを追加する　23.11.0 リリース以降、サインインページに認証 PIN に関するヒントを追加できるようになりました。この機能はオプションであり、2 要素認証に登録されたデバイスに適用されます。ヒントにより、PIN にアクセスする方法がわかります。

ヒントはテキストまたはリンクとして構成できます。ヒントのテキストでは PIN に関する簡単な情報が提供され、リンクでは PIN へのアクセス方法に関する詳細情報が提供されます。ヒントの構成方法について詳しくは、「Citrix Endpoint Management コンソールを使用したヒントの構成」の記事を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

nFactor 認証によるシングルサインオン機能のサポート　Secure Hub for iOS バージョン 23.11.0 以降、nFactor のモバイルアプリケーション管理（MAM：Mobile Application Management）登録またはサインインはシングルサインオン（SSO）機能をサポートします。この機能により、以前に入力したサインイン資格情報が MAM 登録またはサインインプロセスを通過できるため、ユーザーが再度手動でサインイン資格情報を入力する必要がなくなります。

nFactor SSO プロパティについて詳しくは、Citrix Endpoint Management ドキュメントの「クライアントプロパティリファレンス」を参照してください。

Secure Hub 23.10.0

Secure Hub for Android

Secure Hub for Android 23.10.0 は Android 14 をサポートしています。Secure Hub バージョン 23.10.0 にアップグレードすると、Android 14 に更新されたデバイスが引き続きサポートされます。

Secure Hub 23.9.0

Secure Hub for Android

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。

Secure Hub 23.8.1

Secure Hub for iOS　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。

Secure Hub 23.8.0

Secure Hub for iOS　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。

Secure Hub 23.7.0

Secure Hub for Android

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Play Integrity API　SafetyNet Attestation API は、廃止予定のタイムラインに従って Google によって間もなく廃止され、推奨されている Play Integrity API に移行します。

詳しくは、Citrix Endpoint Management のドキュメントの「Play Integrity API」を参照してください。

廃止予定のタイムラインについて詳しくは、Citrix Endpoint Management のドキュメントの「廃止と削除」を参照してください。

Android の SafetyNet 機能については、「SafetyNet」を参照してください。

Secure Hub 23.4.0

Secure Hub for iOS

ユーザーエクスペリエンスの向上　バージョン 23.4.0 以降、Secure Hub for iOS では次のユーザーエクスペリエンスが向上しています:

- ストアエクスペリエンス

  以前は、［マイアプリ］ページが最初に表示されていました。バージョン 23.4.0 では、［ストア］ページが最初に表示されます。

  以前は、ユーザーが［ストア］オプションをクリックするたびに、Secure Hub ストアは再読み込み操作を実行していました。

  バージョン 23.4.0 では、ユーザーエクスペリエンスが向上しています。今後は、ユーザーが初めてアプリを起動したとき、アプリを再起動したとき、または画面を下にスワイプしたときに、アプリが再読み込みされるようになりました。

- ユーザーインターフェイス：以前は、［サインオフ］オプションは画面の左下に配置されていました。23.4.0 バージョンでは、［サインオフ］オプションはメインメニューの一部で、［バージョン］オプションの上にあります。
- ハイパーリンク：以前は、アプリの詳細ページのハイパーリンクはプレーンテキストとして表示されていました。バージョン 23.4.0 では、ハイパーリンクをクリックできるようになり、リンクを示す下線の書式が設定されています。

MDX から **MAM SDK** への移行エクスペリエンス　バージョン 23.4.0 以降、レガシ MDX から MAM SDK への移行エクスペリエンスが iOS デュアルモードアプリ向けに強化されています。この機能は、通知メッセージの数を減らし、Secure Hub に切り替えることで、業務用モバイルアプリを使用するときのユーザーエクスペリエンスを向上させます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix PIN を使用したアプリのロックの解除　以前は、エンドユーザーはデバイスのパスコードを入力して、モバイルアプリ管理（MAM）に基づいてアプリのロックを解除していました。

バージョン 23.4.0 以降、エンドユーザーはパスコードとして Citrix PIN を入力して、MAM ベースのアプリのロックを解除できるようになります。管理者は、CEM サーバー上のクライアントプロパティを使用してパスコードの複雑さを設定できます。

アプリが許可された時間を超えて非アクティブな場合、エンドユーザーは管理者が設定した構成に応じて Citrix PIN を入力し、アプリのロックを解除できます。

Android 向け Secure Hub の場合、MAM アプリケーションで非アクティブタイマーに対応する方法を構成するための別のクライアントプロパティがあります。詳しくは、「Android 向けの個別の非アクティブタイマー」を参照してください。

Secure Hub 23.4.1

Secure Hub for Android　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。

Secure Hub 23.4.0

Secure Hub for Android　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。

Secure Hub 23.2.0

Secure Hub for Android

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

MDX 完全トンネルモード **VPN**　MDX マイクロ VPN（完全トンネルモード）は廃止されました。

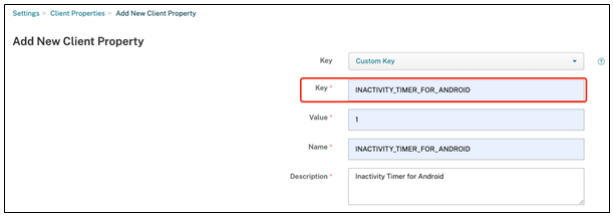
詳しくは、Citrix Endpoint Management のドキュメントの「廃止」を参照してください。

Android 用の個別の非アクティブタイマー　以前は、非アクティブタイマーのクライアントプロパティは Android および iOS の Secure Hub で共通でした。

バージョン 23.2.0 以降、IT 管理者は新しいクライアントプロパティ **Inactivity_Timer_For_Android** を使用して、非アクティブタイマーを iOS から分離できます。IT 管理者は、**Inactivity_Timer_For_Android** の値を 0 に

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

設定して、Android の非アクティブタイマーを個別に無効にできます。この場合、Secure Hub を含む仕事用プロファイル内のすべてのアプリは、PIN のみで機能します。



クライアントプロパティの追加および変更について詳しくは、XenMobile のドキュメントの「クライアントプロパティ」を参照してください。

Secure Hub 22.11.0

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 22.9.0

Secure Hub for Android　このリリースには、次の内容が含まれています:

- デバイスのパスコードにおけるパスコードの複雑さ（Android 12 以降）
- SDK 31 のサポート
- バグ修正

デバイスのパスコードにおけるパスコードの複雑さ（**Android 12** 以降）　パスコードの複雑さは、カスタムのパスワード要件よりも優先されます。パスコードの複雑さのレベルは、事前定義されたレベルの 1 つです。したがって、エンドユーザーは複雑さのレベルが低いパスワードを設定できません。

Android 12 以降のデバイスのパスコードの複雑さは次のとおりです:

- パスコードの複雑さを適用する：カスタムのパスワード要件ではなく、プラットフォームによって定義された複雑さのレベルのパスワードが必要です。Android 12 以降で Secure Hub 22.9 以降を使用しているデバイスのみ対象。
- 複雑さのレベル：事前定義されたパスワードの複雑さのレベル。
  - なし：パスワードは必要ありません。
  - 低：パスワードは次の場合があります:
    - パターン
    - PIN（4 つ以上の数字）
  - 中：パスワードは次の場合があります:
    - 繰り返しの文字（4444）または順番どおりの文字（1234）ではない PIN と、最低 4 つの数字
    - 4 文字以上のアルファベット

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    - 4 文字以上の英数字
  - 高：パスワードは次の場合があります：
    - 繰り返しの文字（4444）または順番どおりの文字（1234）ではない PIN と、最低 8 つの数字
    - 6 文字以上のアルファベット
    - 6 文字以上の英数字

> メモ：
>
> - BYOD デバイスの場合、最小文字数、必須文字、生体認証、詳細規則などのパスコード設定は、Android 12 以降では適用できません。代わりにパスコードの複雑さを使用してください。
> - 仕事用プロファイルのパスコードの複雑さが有効になっている場合は、デバイス側のパスコードの複雑さも有効にする必要があります。

詳しくは、Citrix Endpoint Management のドキュメントの「Android Enterprise の設定」を参照してください。

Secure Hub 22.7.0

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 22.6.0

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 22.5.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub 22.4.0

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 22.2.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　このリリースには、バグの修正が含まれています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 21.11.0

Secure Hub for Android

会社所有のデバイスでの仕事用プロファイルのサポート　Android Enterprise デバイスで、会社所有のデバイスモードでの仕事用プロファイルに Secure Hub を登録できるようになりました。この機能は、Android 11 以降を実行しているデバイスで使用できます。以前に個人使用可能なコーポレート所有（COPE）モードで登録されていたデバイスは、デバイスが Android 10 から Android 11 以降にアップグレードされると、会社所有のデバイスモードでの仕事用プロファイルに自動的に移行します。

Secure Hub 21.10.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　**Android 12** のサポート。このリリース以降、Secure Hub は Android 12 を実行するデバイスでサポートされます。

Secure Hub 21.8.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub 21.7.1

Secure Hub for Android　既に登録されているデバイスで **Android 12** を使用できます。Android 12 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 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 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:
>
> Android 12 にアップグレードする前に Secure Hub がバージョン 21.7.1 に更新されていない場合、以前の機能を回復するために、デバイスの再登録または工場出荷時状態へのリセットが必要になる場合があります。
>
> 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 Hub 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 Hub 21.7.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 21.6.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 21.5.1

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 21.5.0

Secure Hub for iOS　このリリースでは、MDX Toolkit バージョン 19.8.0 以前でラッピングされたアプリは機能しなくなります。機能を適切に再開するには、アプリを最新の MDX Toolkit でラッピングしてください。

Secure Hub 21.4.0

Secure Hub の色の刷新。Secure Hub は、Citrix の最新のブランドカラーに準拠しています。

Secure Hub 21.3.2

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub 21.3.0

このリリースには、バグの修正が含まれています。

Secure Hub 21.2.0

Secure Hub for Android　このリリースには、バグの修正が含まれています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 21.1.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 20.12.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub for Android　Secure Hub for Android は、直接起動モードをサポートしています。直接起動モードについて詳しくは、*Developer.android.com* で、Android ドキュメントを参照してください。

Secure Hub 20.11.0

Secure Hub for Android　Secure Hub 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 Hub 20.10.5

このリリースには、バグの修正が含まれています。

Secure Hub 20.9.0

Secure Hub for iOS　Secure Hub for iOS は iOS 14 をサポートしています。

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub 20.7.5

Secure Hub for Android

- Secure Hub for Android は Android 11 をサポートしています。
- **Secure Hub** のアプリが **32** ビットから **64** ビット版へ移行。Secure Hub バージョン 20.7.5 では、32 ビットアーキテクチャのサポートが終了し、64 ビット版に更新されました。Citrix ではバージョン 20.6.5 から 20.7.5 にアップグレードすることをお勧めます。ユーザーが Secure Hub バージョン 20.6.5 へのアップグレードをスキップし、代わりに 20.1.5 から直接 20.7.5 に更新する場合、再認証が必要です。再認証には、資

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

格情報の入力と Secure Hub の PIN のリセットが含まれます。Secure Hub バージョン 20.6.5 は、Google Play ストアで入手できます。

- **App Store** から更新をインストールします。Secure Hub for Android では、利用可能な更新があるアプリが強調表示され、［更新可能］機能が App Store 画面に表示されます。

  ［更新可能］をタップすると、保留中の更新があるアプリの一覧を表示するストアに移動します。アプリの ［詳細］をタップして、更新をインストールします。アプリが更新されると、［詳細］の下向き矢印がチェックマークに変わります。

Secure Hub 20.6.5

Secure Hub for Android　アプリが **32** ビット版から **64** ビット版へ移行。Secure Hub 20.6.5 リリースは、Android モバイルアプリの 32 ビットアーキテクチャをサポートする最後のリリースです。以降のリリースでは、Secure Hub は 64 ビットアーキテクチャをサポートします。再認証なしで以降のバージョンにアップグレードできるように、ユーザーが Secure Hub バージョン 20.6.5 にアップグレードすることを Citrix ではお勧めします。ユーザーが Secure Hub バージョン 20.6.5 へのアップグレードをスキップし、代わりに直接 20.7.5 に更新する場合、再認証が必要です。再認証には、資格情報の入力と Secure Hub の PIN のリセットが含まれます。

> 注:
>
> 20.6.5 リリースは、デバイス管理者モードで Android 10 を実行しているデバイスの登録をブロックしません。

Secure Hub for iOS　**iOS** デバイスで構成されたプロキシを有効にします。Secure Hub for iOS では、ユーザーが ［設定］**>** ［**W-Fi**］で構成するプロキシサーバーを使用できるようにする場合、新しいクライアントプロパティ`ALLOW_CLIENTSIDE_PROXY`を有効にする必要があります。詳しくは、「クライアントプロパティリファレンス」の「`ALLOW_CLIENTSIDE_PROXY`」を参照してください。

Secure Hub 20.3.0

> 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。

Secure Hub for iOS

- ネットワーク拡張が無効になりました。最近の App Store レビューガイドラインの変更により、Secure Hub リリース 20.3.0 以降では、iOS を実行しているデバイスでネットワーク拡張（NE）をサポートしていません。NE は、Citrix の業務用モバイルアプリには影響を与えません。ただし NE の削除は、展開済みの、MDX でラップされたエンタープライズアプリに多少の影響を与えます。認証トークン、タイマー、PIN の再試行などによるコンポーネントの同期で、Secure Hub への必要のない切り替えが発生することがあります。詳しくは、https://support.citrix.com/article/CTX270296を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> 新規ユーザーには、VPN のインストールを求めるメッセージは表示されません。

- 登録プロファイルの拡張機能のサポート。Secure Hub は、「登録プロファイルサポート」で説明している Citrix Endpoint Management の登録プロファイルの拡張機能をサポートしています。

Secure Hub 20.2.0

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

Secure Hub 20.1.5

このリリースには、次の内容が含まれています:

- ユーザープライバシーポリシーの形式と表示の更新。この機能の更新により、Secure Hub の登録フローが変更されます。
- バグ修正。

Secure Hub 19.12.5

このリリースには、バグの修正が含まれています。

Secure Hub 19.11.5

このリリースには、バグの修正が含まれています。

Secure Hub 19.10.5

Secure Hub for Android　**COPE** モードで **Secure Hub** を登録する。Android Enterprise デバイスでは、個人使用可能なコーポレート所有端末（COPE）登録プロファイルで Citrix Endpoint Management が構成されている場合、COPE モードで Secure Hub を登録します。

Secure Hub 19.10.0

このリリースには、バグの修正が含まれています。

Secure Hub 19.9.5

Secure Hub for iOS　このリリースには、バグの修正が含まれています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub for Android　**Android Enterprise** の仕事用プロファイルおよび完全に管理されているデバイスの **Keyguard** 管理機能のサポート。Android の Keyguard は、デバイスのロック画面および仕事用チャレンジのロック画面を管理します。Citrix Endpoint Management の Keyguard 管理デバイスポリシーを使用して、仕事用プロファイルデバイスの keyguard 管理と、完全に管理された専用デバイスの keyguard 管理を制御します。keyguard 管理を使用すると、Keyguard 画面のロックを解除する前に、ユーザーが使用できる機能（信頼できるエージェントやセキュアカメラなど）を指定できます。または、すべての Keyguard 機能を無効にできます。

機能の設定とデバイスポリシーの構成方法について詳しくは、「Keyguard 管理デバイスポリシー」を参照してください。

Secure Hub 19.9.0

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

Secure Hub for Android　このリリースには、バグの修正が含まれています。

Secure Hub for Android 19.8.5

このリリースには、バグの修正が含まれています。

Secure Hub 19.8.0

Secure Hub 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 Hub for Android　**Android Q** のサポート。このリリースには、Android Q のサポートが含まれます。Android Q プラットフォームにアップグレードする前に、Google Device Administration API の廃止が Android Q を実行するデバイスに与える影響について、「Device Administration から Android Enterprise への移行」を参照してください。また、ブログ（Citrix Endpoint Management および Android Enterprise - 変革）も参照してください。

Secure Hub 19.7.5

Secure Hub 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 Hub for Android　**Samsung Knox SDK 3.x** のサポート。Secure Hub for Android は Samsung Knox SDK 3.x をサポートしています。Samsung Knox 3.x の移行について詳しくは、Samsung Knox の開発者向けドキュメントを参照してください。このリリースでは、新しい Samsung Knox 名前空間もサポートしています。以前の Samsung Knox 名前空間からの変更について詳しくは、「古い Samsung Knox 名前空間の変更」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Secure Hub for Android は、Android 5 を実行しているデバイスで Samsung Knox 3.x をサポートしていません。

Secure Hub 19.3.5 〰 19.6.6

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 Hub 19.3.0

Samsung Knox Platform for Enterprise のサポート。Secure Hub for Android は、Android Enterprise デバイスで Knox Platform for Enterprise（KPE）をサポートします。

Secure Hub 19.2.0

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 Hub 19.1.5

Secure Hub for Android Enterprise は、次のポリシーをサポートするようになりました:

- **WiFi** デバイスポリシー Wi-Fi デバイスポリシーは、Android Enterprise をサポートするようになりました。このポリシーについて詳しくは、「Wi-Fi デバイスポリシー」を参照してください。
- カスタム **XML** デバイスポリシーカスタム XML デバイスポリシーは、Android Enterprise をサポートするようになりました。このポリシーについて詳しくは、「カスタム XML デバイスポリシー」を参照してください。
- ファイルデバイスポリシー Citrix Endpoint Management にスクリプトファイルを追加して、Android Enterprise デバイスで機能を実行できます。このポリシーについて詳しくは、「ファイルデバイスポリシー」を参照してください。

Secure Hub 19.1.0

Secure Hub のフォント、色、そのほかの **UI** の要素が刷新されました。この変更は、Citrix の業務用モバイルアプリ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。

Secure Hub 18.12.0

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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 18.11.5

- **Android Enterprise** の制限デバイスポリシー設定。制限デバイスポリシーの新しい設定により、ユーザーは Android Enterprise デバイスでステータスバー、ロック画面の Keyguard、アカウント管理、位置情報の共有、デバイス画面の表示を維持する機能にアクセスできます。詳しくは、「制限デバイスポリシー」を参照してください。

Secure Hub 18.10.5～18.11.0 には、パフォーマンスの強化機能とバグの修正が含まれています。

Secure Hub 18.10.0

- **Samsung DeX** モードのサポート： Samsung DeX を使用すると、ユーザーは KNOX 対応デバイスを外部ディスプレイに接続して、PC のようなインターフェイスでアプリを使用したり、ドキュメントを確認したり、ビデオを見ることができます。Samsung DeX のデバイス要件と Samsung DeX の設定については、「Samsung DeX の機能」を参照してください。

  Citrix Endpoint Management で Samsung DeX モードの機能を設定するには、Samsung Knox の制限デバイスポリシーを更新します。詳しくは、「制限デバイスポリシー」の「**Samsung KNOX** の設定」を参照してください。

- **Android SafetyNet** のサポート： **Android SafetyNet** 機能を使用して、Secure Hub がインストールされている Android デバイスの互換性とセキュリティを評価するように Endpoint Management を設定できます。結果は、デバイス上で自動化された操作をトリガーするために使用できます。詳しくは、「Android SafetyNet」を参照してください。

- **Android Enterprise** デバイスのカメラ使用を禁止する：制限デバイスポリシーの新しい設定である ［カメラの使用を許可］を設定することで、ユーザーが Android Enterprise デバイスでカメラを使用できないようにすることができます。詳しくは、「制限デバイスポリシー」を参照してください。

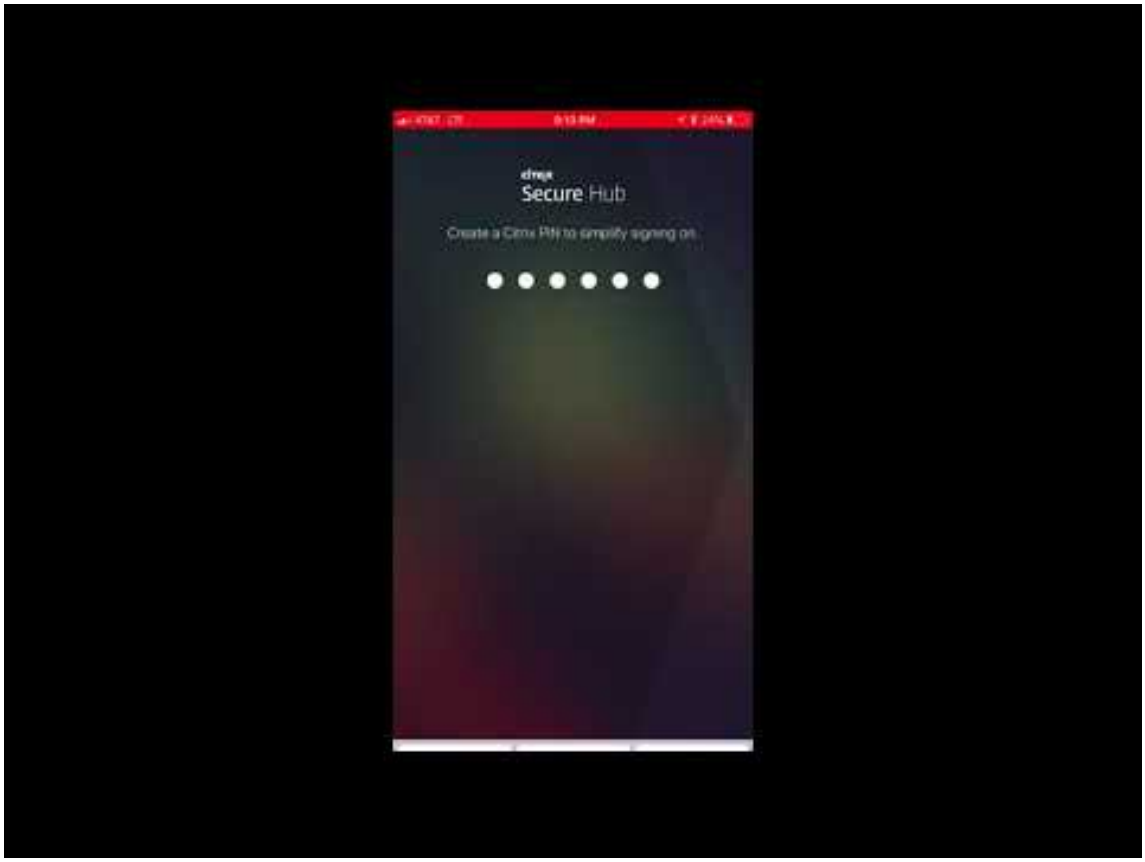
Secure Hub 10.8.60～18.9.0

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 Hub 10.8.60

- ポーランド語のサポート。
- Android P のサポート。
- ワークスペースアプリストアの使用のサポート。
  Secure Hub を開いても、Secure Hub ストアは表示されません。［アプリを追加］ボタンを押すと、ワークスペースアプリストアに移動します。次のビデオでは、iOS デバイスで Citrix Workspace アプリを使用して、Citrix Endpoint Management への登録を行う様子を示します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 重要:
>
> この機能は新規顧客にのみ提供されます。現在のところ、既存の顧客の移行はサポートされていません。

この機能を使用するには、以下を設定します:

- パスワードのキャッシュポリシーおよびパスワード認証ポリシーを有効にします。これらのポリシーの構成について詳しくは、「業務用モバイルアプリの MDX ポリシーの概要」を参照してください。
- Active Directory 認証を AD または AD+Cert として構成します。これら 2 つのモードをサポートしています。認証の構成について詳しくは、「ドメインまたはドメイン + セキュリティトークン認証」を参照してください。
- Endpoint Management のワークスペース統合を有効にします。ワークスペース統合について詳しくは、「ワークスペースの構成」を参照してください。

> 重要:
>
> この機能を有効にすると、Citrix Files SSO は Endpoint Management（旧 XenMobile）ではなく、ワークスペースを通して実行されます。ワークスペースの統合を有効にする前に、Endpoint Management コンソールで Citrix Files の統合を無効にすることをお勧めします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Hub 10.8.55

- JSON 構成を使用して、Google のゼロタッチ登録と Samsung Knox Mobile Environment（KME）ポータルにユーザー名とパスワードを渡す機能です。詳しくは、「Samsung Knox の一括登録」を参照してください。
- 証明書のピン留めを有効にすると、ユーザーは自己署名証明書を使用して Endpoint Management に登録することはできません。ユーザーが自己署名証明書を使用して Endpoint Management に登録しようとすると、証明書が信頼されていないという警告が表示されます。

Secure Hub 10.8.25: Secure Hub for Android では Android P デバイスがサポートされています。

> 注:
>
> Android P プラットフォームにアップグレードする前に: サーバーインフラストラクチャが、subjectAltName（SAN）拡張で一致するホスト名を持つセキュリティ証明書に準拠していることを確認します。ホスト名を検証するには、サーバーは一致する SAN を含む証明書を提示する必要があります。ホスト名に一致する SAN を含まない証明書は信頼されません。詳しくは、Android 開発者ドキュメントを参照してください。

Secure Hub for iOS の更新（**2018** 年 **3** 月 **19** 日）: Secure Hub for iOS バージョン 10.8.6 では、VPP アプリポリシーの問題を修正できます。詳しくは、Citrix Knowledge Center の記事を参照してください。

Secure Hub 10.8.5: Android Work（Android for Work）の COSU モード対応 Secure Hub for Android でサポート。詳しくは、Citrix Endpoint Management のドキュメントを参照してください。

Secure Hub の管理

Secure Hub に関連する大部分の管理タスクは、Endpoint Management の初期構成時に実行します。ユーザーが iOS や Android で Secure Hub を利用できるようにするために、Secure Hub を iOS App Store、または Google Play ストアにアップロードします。

Secure Hub は、Citrix Gateway を使用した認証後にユーザーの Citrix Gateway セッションが更新されたときに、インストールされているアプリの、Endpoint Management に格納されている MDX ポリシーのほとんどを更新します。

> 重要:
>
> これらのポリシーのうちのいずれかを変更する場合は、ユーザーはアプリを削除してから再インストールし、更新されたポリシーを適用する必要があります: セキュリティグループ、暗号化を有効化、Secure Mail の Exchange Server

Citrix PIN

Citrix PIN を使用するように、Secure Hub を構成できます。このセキュリティ機能は、Endpoint Management コンソールで ［設定］ > ［クライアントプロパティ］を選択して有効にします。この設定では、登録されているモバ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

イルデバイスユーザーが Secure Hub にサインオンし、ラップされた MDX アプリを暗証番号（PIN）の使用によりアクティブ化する必要があります。

Citrix PIN 機能で、セキュリティで保護されたラップアプリにログオンするときのユーザー認証が簡単になります。Active Directory のユーザー名やパスワードなど、別の資格情報を繰り返し入力する必要はありません。

Secure Hub に初めてサインオンするユーザーは、Active Directory ユーザー名とパスワードを入力する必要があります。サインオン時に、Secure Hub は Active Directory 資格情報またはクライアント証明書をユーザーデバイスに保存し、ユーザーに対して PIN を入力するよう要求します。ユーザーは再度のサインオン時に PIN を入力することにより、アクティブなユーザーセッションの次回アイドルタイムアウトが終了するまで、Citrix アプリおよび Store にセキュアにアクセスできます。関連するクライアントのプロパティでは、PIN を使用したシークレットの暗号化、PIN のパスコードの種類の指定、および PIN の強度と長さの要件の指定を実行できます。詳しくは、「クライアントプロパティ」を参照してください。

指紋認証（Touch ID）が有効なときに、アプリが無効なためにオフライン認証が求められた場合、ユーザーは指紋を使用してサインインできます。ただし、初めて Secure Hub にサインインしたり、デバイスを再起動したりする場合、および非アクティブタイマーの有効期限が切れた後には、PIN を入力する必要があります。指紋認証の有効化について詳しくは、「指紋認証または Touch ID 認証」を参照してください。

証明書ピン留め

Secure Hub for iOS および Secure Hub for Android は、SSL 証明書のピン留めをサポートしています。これにより、Citrix クライアントが Endpoint Management と通信する際に、企業が署名した証明書が使用されます。したがって、デバイス上のルート証明書のインストールにより SSL セッションに危害が及ぶ場合に、クライアントから Endpoint Management への接続が阻止されます。Secure Hub がサーバー公開キーに対する何らかの変更を検出すると、接続が拒否されます。

Android N 以降、ユーザーが追加した認証機関（CA）はオペレーティングシステムで許可されなくなります。Citrix ではユーザーが追加した CA の代わりに、パブリックルート CA を使用することをお勧めします。

Android N にアップグレードするユーザーは、プライベートまたは自己署名 CA を使用すると問題が発生する可能性があります。次の状況では、Android N デバイス上の接続が切断されます:

- Endpoint Management オプションのプライベート/自己署名 CA と必須の信頼済み CA が ［オン］ に設定されている。詳しくは、「デバイス管理」を参照してください。
- プライベート/自己署名 CA と Endpoint Management AutoDiscovery サービス（ADS）は到達可能ではありません。セキュリティ上の問題により ADS に到達できない場合、必須の信頼済み CA は、最初は ［オフ］ に設定されていた場合でも ［オン］ になります。

デバイスの登録または Secure Hub のアップグレード前に、証明書のピン留めを有効にすることを検討してください。デフォルトで、このオプションは ［オフ］ になっており、ADS によって管理されます。証明書のピン留めを有効にすると、ユーザーは自己署名証明書を使用して Endpoint Management に登録することはできません。ユーザーが自己署名証明書を使用して登録しようとすると、証明書が信頼されていないという警告が表示されます。ユーザーが証明書を承認しない場合、登録は失敗します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

証明書ピン留めを使用するには、Citrix ADS サーバーに Citrix が証明書をアップロードするように依頼する必要があります。Citrix サポートポータルでテクニカルサポートケースを開きます。秘密キーを Citrix に送信しないでください。次に、以下の情報を入力します:

- ユーザーが登録時に使用するアカウントを含むドメイン。
- Endpoint Management の完全修飾ドメイン名（FQDN）。
- Endpoint Management のインスタンス名。デフォルトでは、インスタンス名は zdm であり、大文字と小文字が区別されます。
- ユーザー ID のタイプ。UPN またはメールのいずれかにできます。デフォルトでは、タイプは UPN です。
- デフォルトポート 8443 からポート番号を変更した場合は、iOS 登録に使用されるポート。
- デフォルトポート 443 からポート番号を変更した場合は、Endpoint Management が接続を受け入れるポート。
- Citrix Gateway の完全な URL。
- 管理者のメールアドレス（オプション）。
- ドメインに追加する PEM 形式の証明書。これは、秘密キーではなく公開証明書である必要があります。
- 既存のサーバー証明書の制御方法。古いサーバー証明書を（危険にさらされているため）直ちに削除するか、失効するまでサポートを継続するか。

詳細情報および証明書が Citrix サーバーに追加されると、テクニカルサポートケースが更新されます。

証明書 + ワンタイムパスワード認証

Citrix ADC を構成して、証明書とセキュリティトークンを使用して Secure Hub で認証を行うようにすることができます。セキュリティトークンはワンタイムパスワードとして機能します。この構成により、Active Directory のフットプリントをデバイスに残さない強力なセキュリティオプションが提供されます。

Secure Hub で証明書 + ワンタイムパスワードタイプの認証を使用できるようにするには：Citrix ADC の書き換えアクションと書き換えポリシーを追加する必要があります。これにより、Citrix Gateway ログオンタイプを示す「**X-Citrix-AM-GatewayAuthType: CertAndRSA**」形式のカスタム応答ヘッダーが挿入されます。

通常 Secure Hub では、Endpoint Management コンソールで構成された Citrix Gateway ログオンタイプが使用されます。ただしこの情報は、Secure Hub が初回のログオンを完了するまで、Secure Hub では使用できません。そのため、カスタムヘッダーが必要となります。

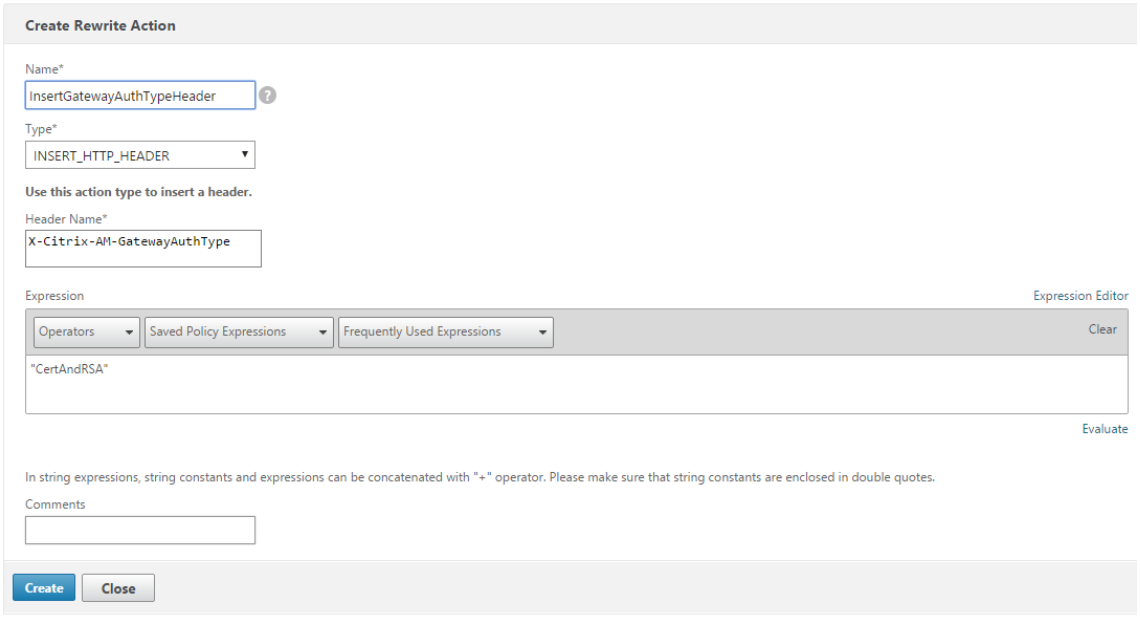
> 注:
>
> Endpoint Management と Citrix ADC で異なるログオンタイプが設定されている場合は、Citrix ADC の構成で上書きされます。詳しくは、「Citrix Gateway と Endpoint Management」を参照してください。

1. Citrix ADC で、［構成］**>**［**AppExpert**］**>**［書き換え］**>**［アクション］の順に選択します。
2. ［追加］をクリックします。

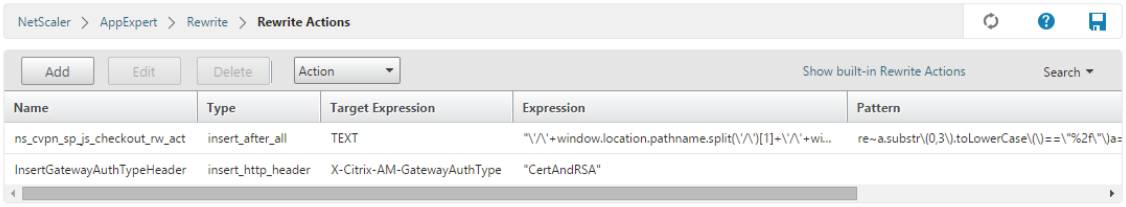
   ［書き換えアクションの作成］画面が開きます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 以下のとおりに各フィールドを入力して、［作成］をクリックします。

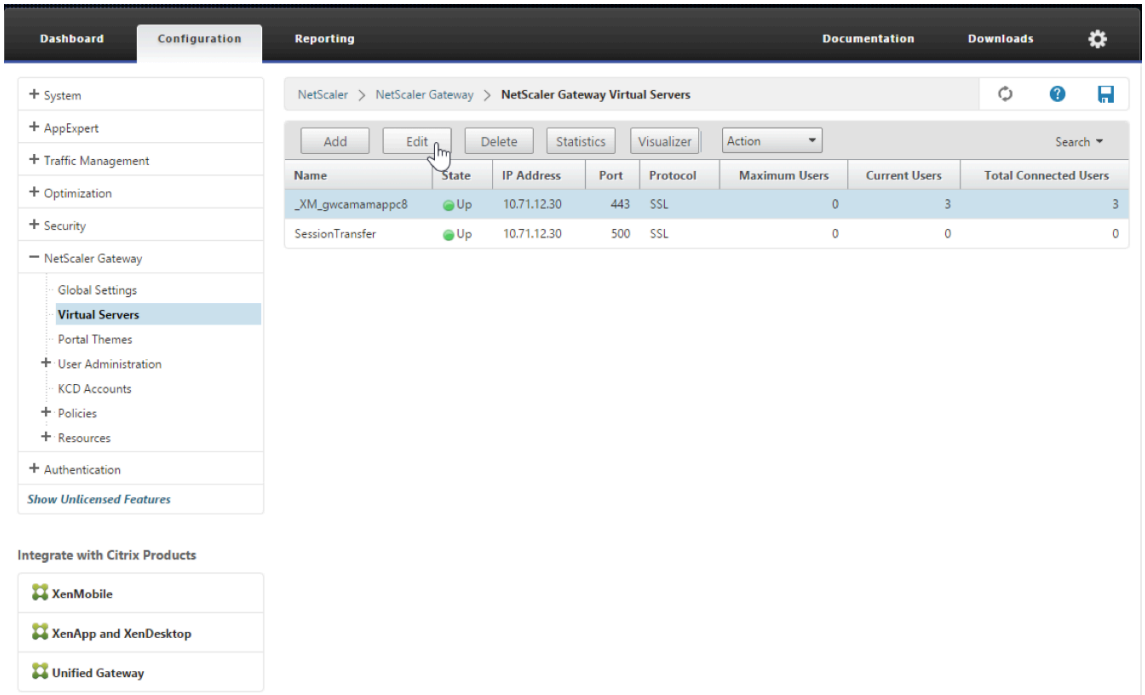


メインの ［書き換えアクション］画面に次の結果が表示されます。

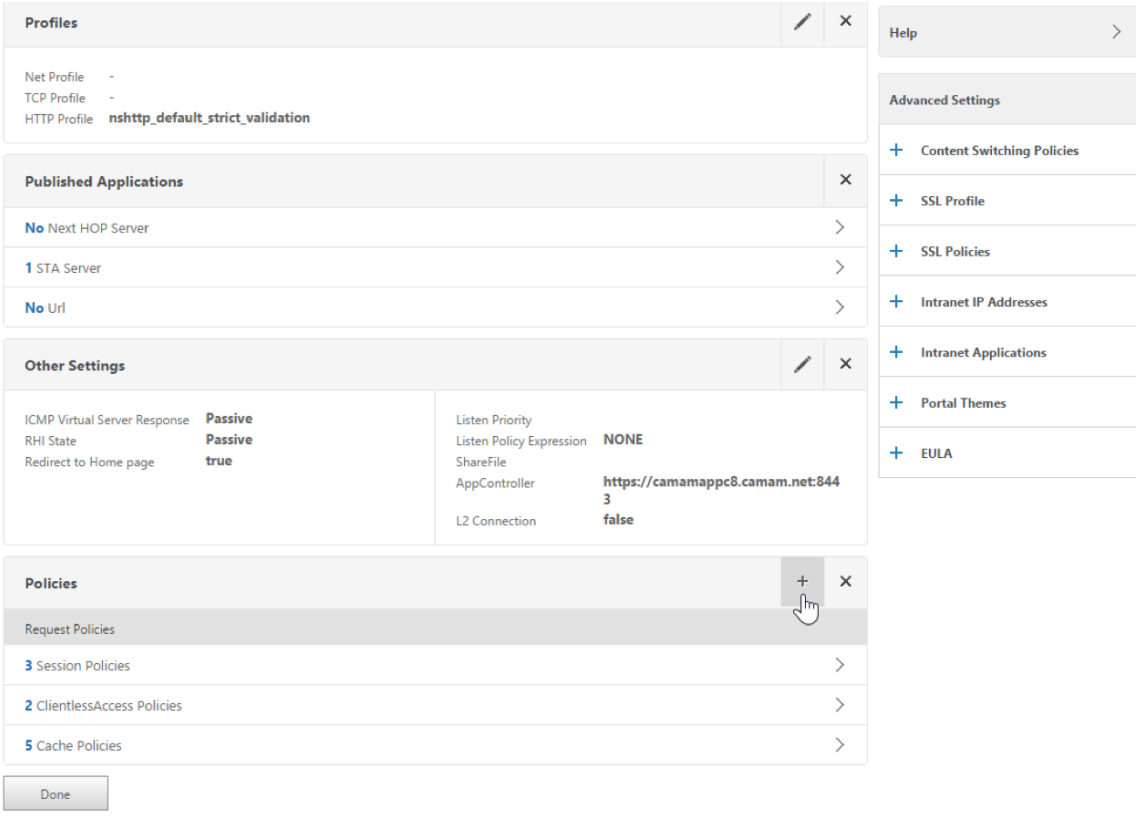


4. 書き換えアクションを書き換えポリシーとして仮想サーバーにバインドします。［構成］**>** ［**NetScaler Gateway**］**>** ［仮想サーバー］の順に選択して、仮想サーバーを選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

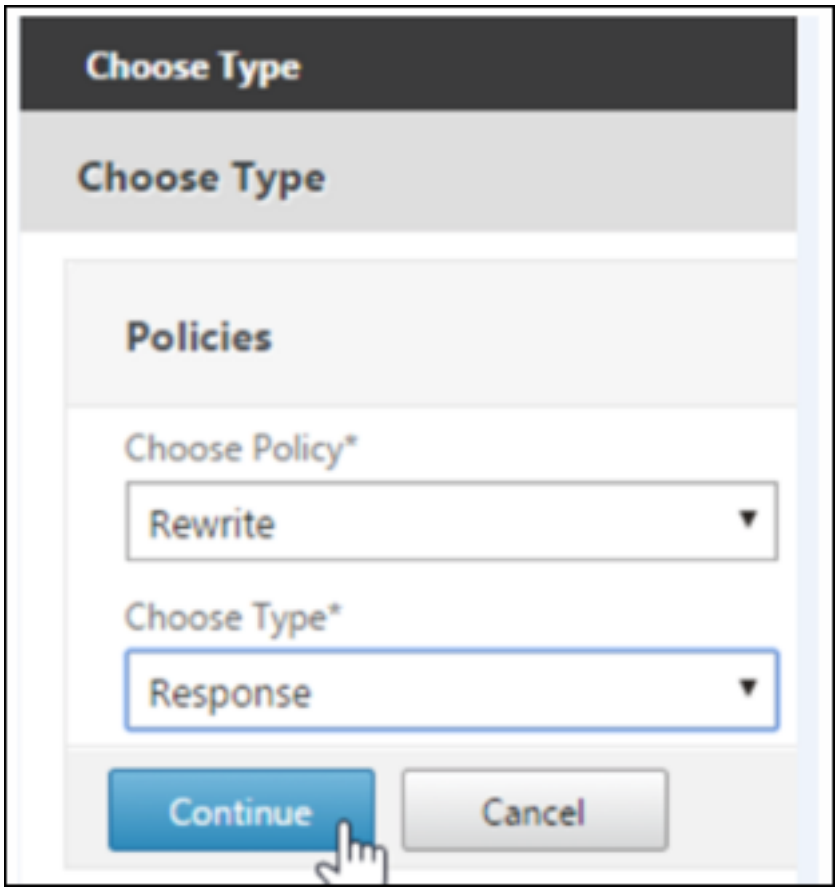


5. [編集] をクリックします。
6. [仮想サーバーの構成] 画面で、[ポリシー] までスクロールします。
7. **+** をクリックして、ポリシーを追加します。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

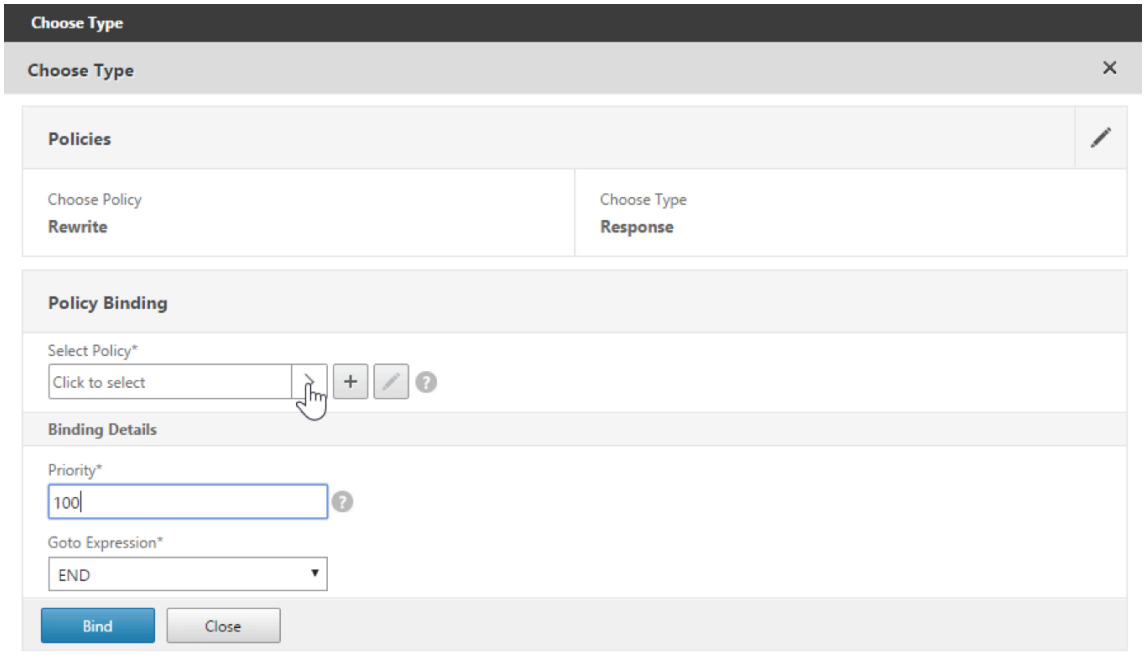
8. ［ポリシーの選択］フィールドで ［書き換え］を選択します。
9. ［種類の選択］フィールドで ［応答］を選択します。



10. ［続行］をクリックします。

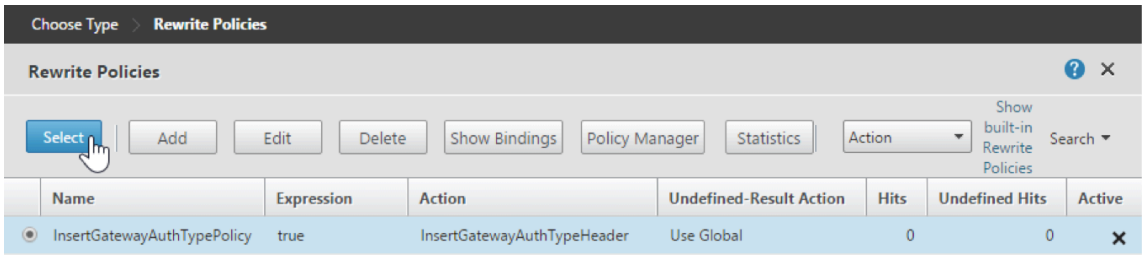
    ［ポリシーバインディング］セクションが展開されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



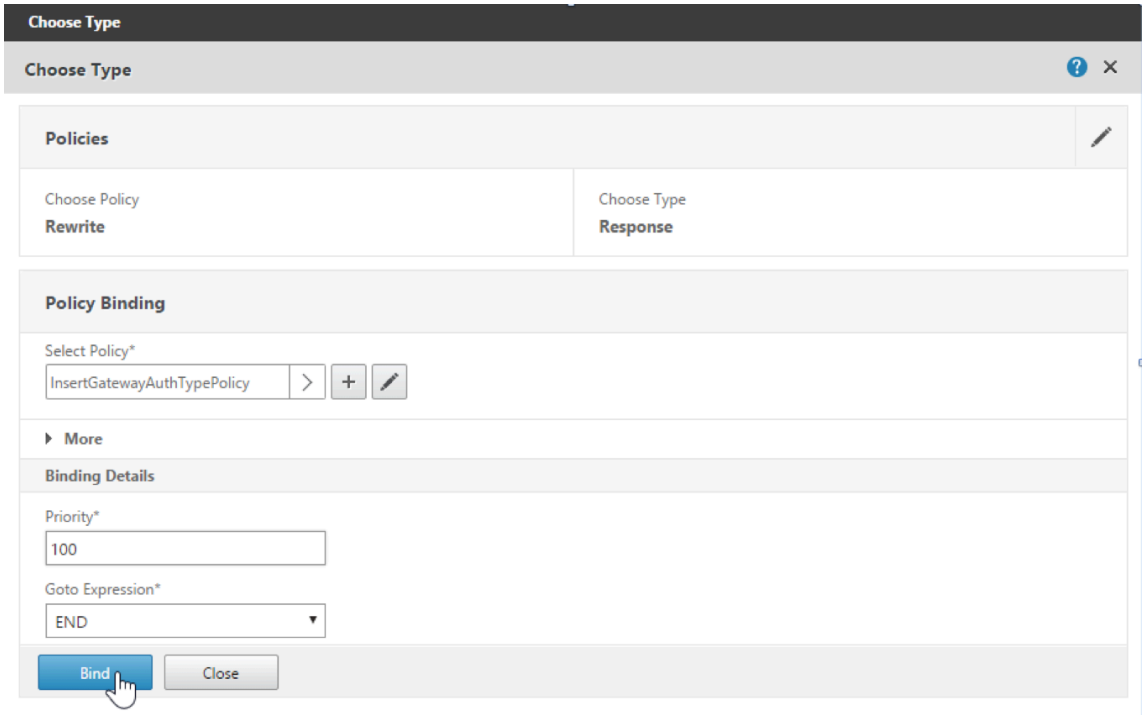
11. ［ポリシーの選択］をクリックします。

    使用可能なポリシーの画面が表示されます。



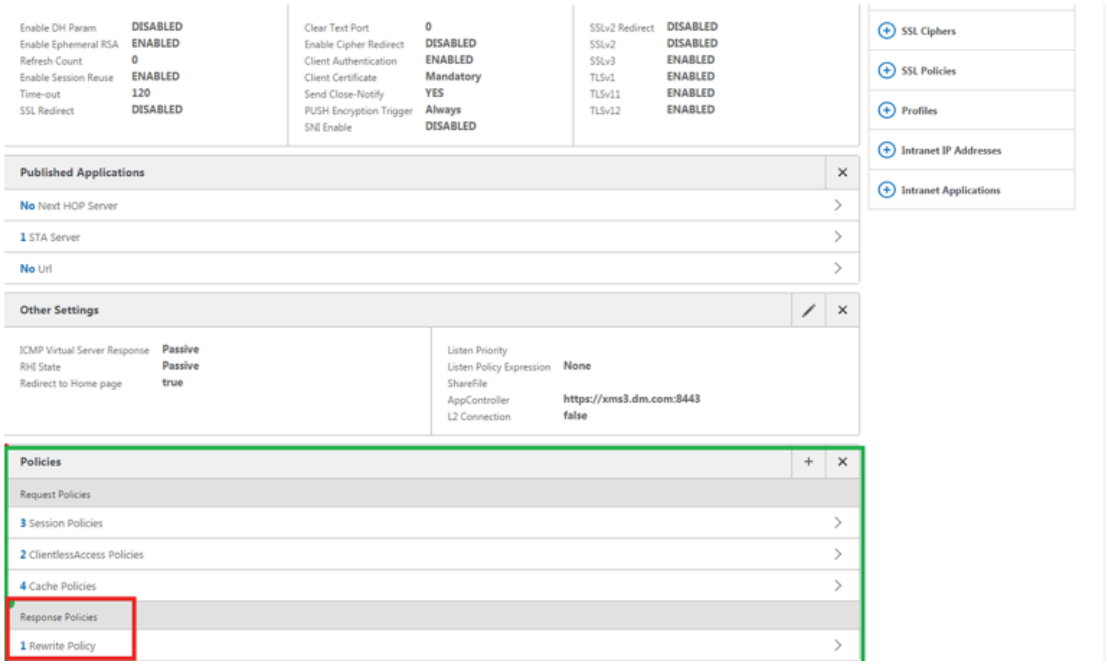
12. 作成したポリシーの行をクリックして、［選択］をクリックします。選択したポリシーが入力された ［ポリシーバインディング］画面に戻ります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



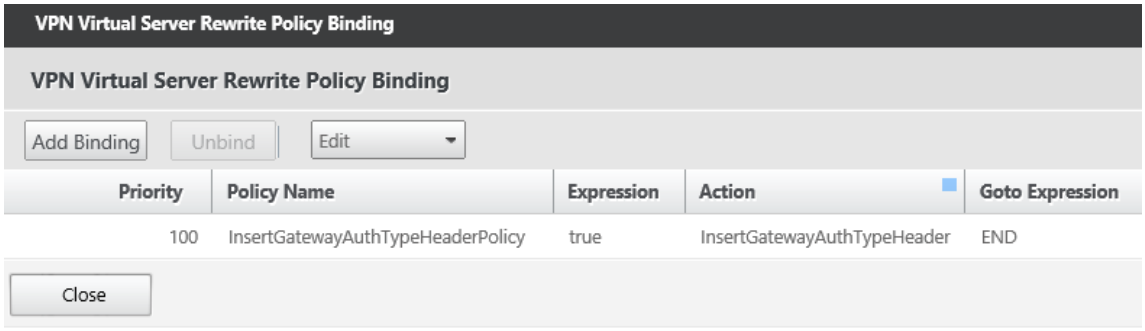
13. [**Bind**] をクリックします。

    正常にバインドされると、メインの構成画面に戻り、完成した書き換えポリシーが表示されます。



14. ポリシーの詳細を表示するには、[書き換えポリシー] をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Android デバイスの **ADS** 接続のためのポート要件　ポート構成により、Secure Hub から接続する Android デバイスで社内ネットワークから Citrix ADS にアクセスできることを保証します。ADS を介して利用可能なセキュリティ更新プログラムをダウンロードする時、ADS にアクセスする能力は重要です。ADS 接続はプロキシサーバーと互換性がない可能性があります。このシナリオでは、ADS 接続がプロキシサーバーをバイパスすることを可能にします。

> 重要:
>
> Secure Hub for Android および iOS では、Android デバイスから ADS にアクセスできる必要があります。詳しくは、Citrix Endpoint Management のドキュメントの「ポート要件」を参照してください。この通信は送信ポート 443 で実行されます。大半の場合で、既存の環境ではこれを許可するよう設計されています。この通信を保証できない場合は、Secure Hub 10.2 にアップグレードしないでください。不明の点があれば、Citrix サポートに問い合わせてください。

前提条件:

- Endpoint Management と Citrix ADC の証明書を収集します。証明書は PEM 形式で、秘密キーではなく公開証明書である必要があります。
- Citrix サポートに証明書ピン留めの有効化を依頼します。このプロセスで、証明書の提出を求められます。

証明書ピン留めに追加された機能向上のため、デバイスは登録前に ADS に接続する必要があります。この前提条件により、デバイスを登録する環境の最新のセキュリティ情報が Secure Hub で利用できることが保証されます。デバイスが ADS に接続できない場合は、Secure Hub はデバイスの登録を許可しません。したがって、内部ネットワーク内で ADS アクセスを可能にすることは、デバイスの登録を有効にするために重要です。

Secure Hub for Android に ADS へのアクセスを許可するには、以下の IP アドレスおよび FQDN のポート 443 を開放します:

FQDN	IP アドレス	ポート	IP とポートの使用
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - ADS 通信

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

FQDN	IP アドレス	ポート	IP とポートの使用
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - ADS 通信
ads.xm.cloud.com: Secure Hub バージョン 10.6.15 以降ではads.xm.cloud.comが使用されることに注意してください。	34.194.83.188	443	Secure Hub - ADS 通信
ads.xm.cloud.com: Secure Hub バージョン 10.6.15 以降ではads.xm.cloud.comが使用されることに注意してください。	34.193.202.23	443	Secure Hub - ADS 通信

証明書ピン留めが有効な場合、次の処理が実行されます:

- Secure Hub は、デバイス登録時に企業の証明書を固定します。
- Secure Hub は、アップグレード時に現在固定されている証明書を破棄し、登録済みユーザーに対して最初の接続でサーバー証明書を固定します。

  > 注:
  >
  > アップグレード後に証明書ピン留めを有効にする場合は、再登録する必要があります。

- 証明書公開キーを変更しなかった場合、証明書の更新時に再登録する必要はありません。

証明書ピン留めではリーフ証明書がサポートされますが、中間証明書および発行者証明書はサポートされません。証明書ピン留めは、Endpoint Management、Citrix Gateway などの Citrix サーバーには適用されますが、サードパーティ製のサーバーには適用されません。

[アカウントの削除] の無効化

Auto Discovery Services（ADS）が有効になっている環境では、Secure Hub で ［アカウントの削除］を無効にできます。

［アカウントの削除］を無効にするには、次の手順を実行します:

1. ドメインの ADS を構成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Citrix Endpoint Management で [**AutoDiscovery** サービス情報]を開き、`displayReenrollLink` の値を **False** に設定します。
   デフォルトでは、この値は **True** です。
3. デバイスが MDM+MAM（ENT）モードで登録されている場合、ログオフしてから再度ログインすると、変更が有効になります。
   デバイスが他のモードで登録されている場合は、デバイスを再登録する必要があります。

Secure Hub の使用

ユーザーは、最初に Apple または Android のストアから自分のデバイス上に Secure Hub をダウンロードします。

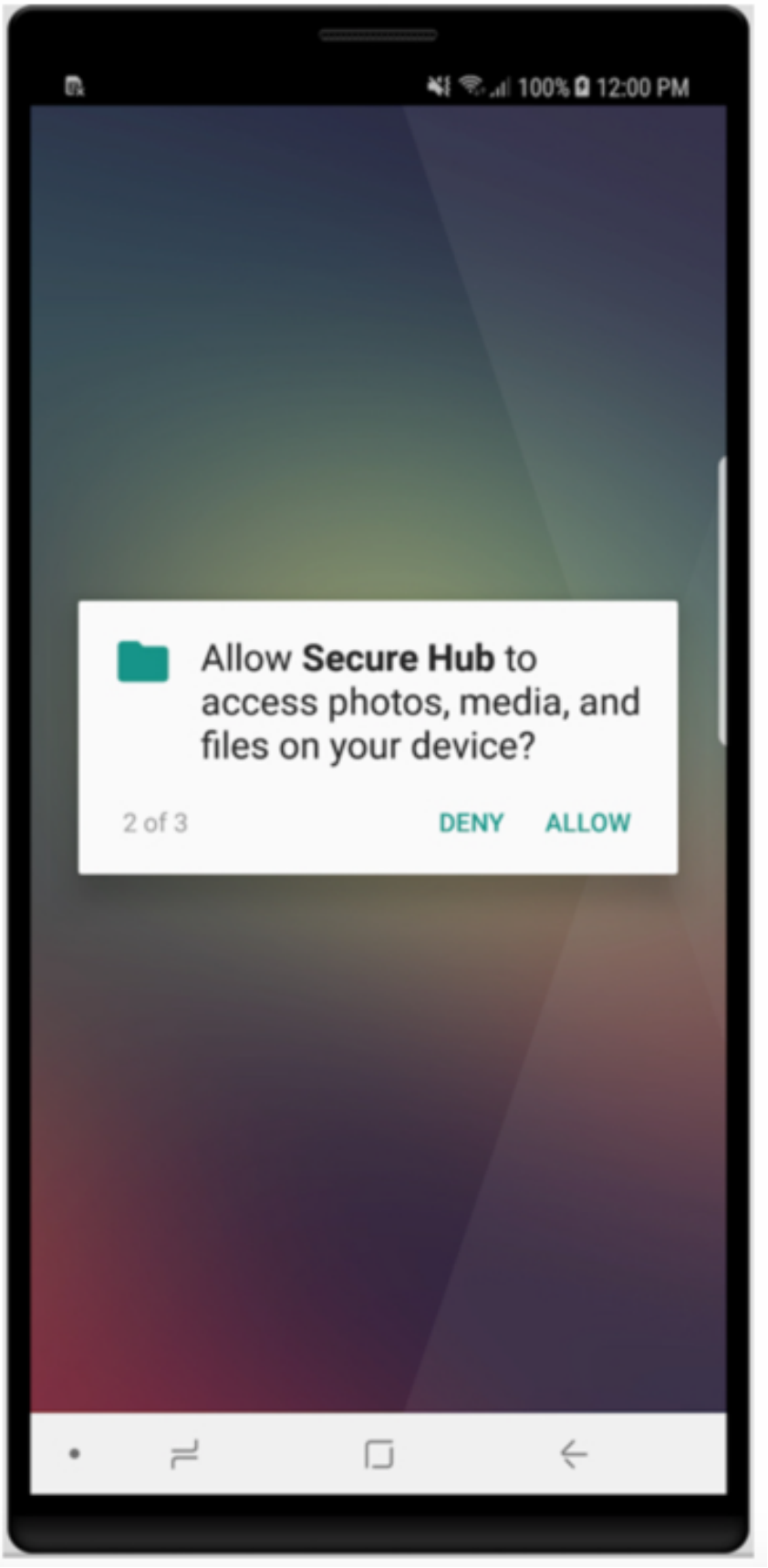
Secure Hub を起動すると、勤務先や組織から提供された資格情報を入力してデバイスを登録するための画面が開きます。デバイス登録の詳細については、「ユーザーアカウント、役割、および登録」を参照してください。

Secure Hub for Android では、初期インストールおよび登録時に、次のメッセージが表示されます。「Secure Hub がデバイス上の写真、メディア、ファイルにアクセスできるようにしますか?」

このメッセージは、Android オペレーティングシステムによるものであり、Citrix からのものではありません。［許可］をタップしても、Secure Hub を管理する管理者および Citrix には、個人データは表示されません。ただし、管理者とのリモートサポートセッションを行っている場合、管理者はセッション内で個人ファイルを表示できます。

登録が完了すると、ユーザーの ［マイアプリ］タブに指定したアプリとデスクトップが表示されます。ユーザーは Store からアプリを追加できます。スマートフォン上の左上隅のハンバーガーアイコンの ［設定］の下に Store へのリンクがあります。

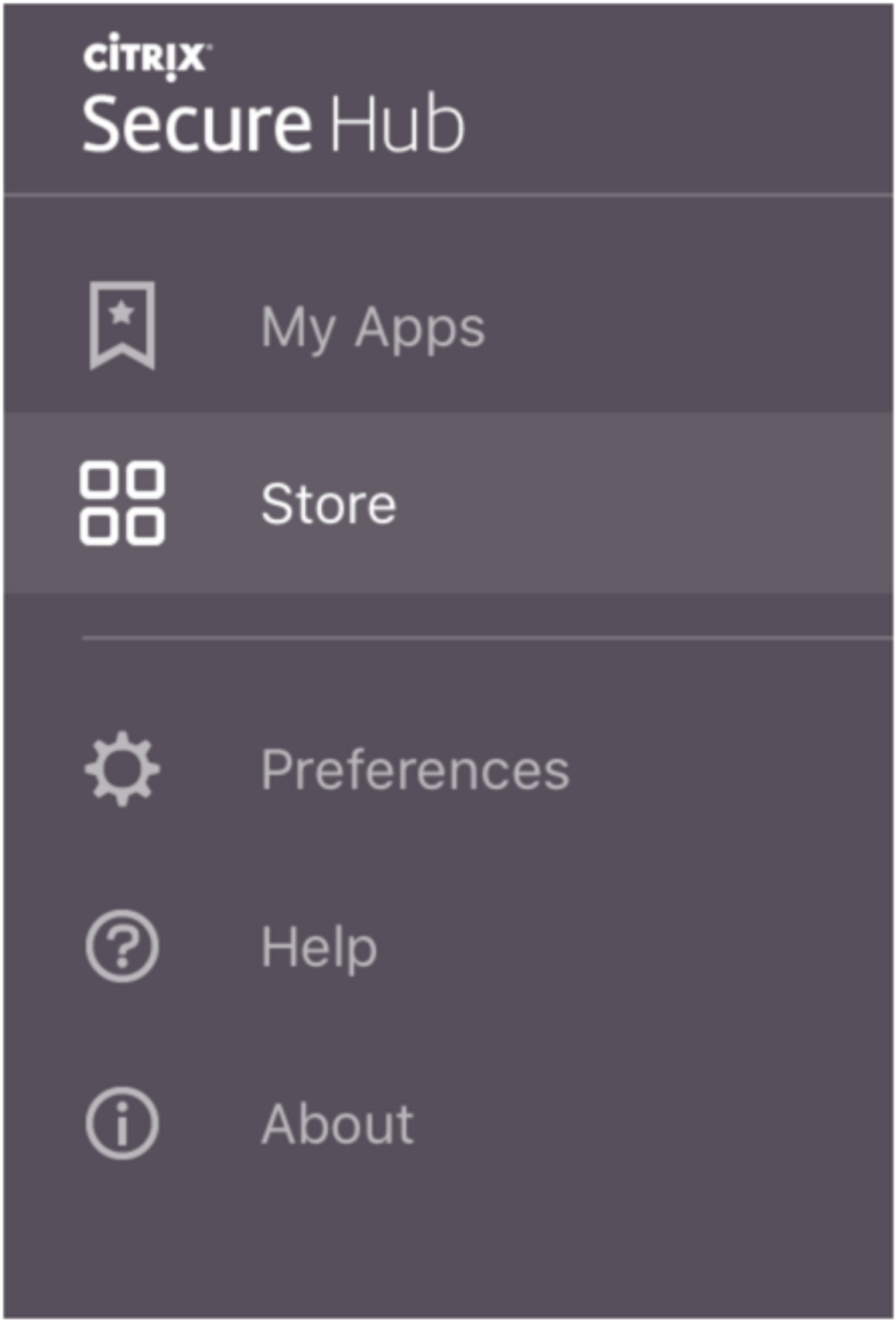
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

タブレットでは、Store は別のタブとなります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

iOS 9 以降の iPhone を使用するユーザーがストアから業務用モバイルアプリをインストールすると、メッセージが表示されます。そのメッセージでは、エンタープライズデベロッパーである Citrix がその iPhone で信頼されていないことが示されます。このメッセージは、デベロッパーが信頼できる状態になるまで、アプリを使用できないことを説明しています。このメッセージが表示された場合、Secure Hub はユーザーに、iPhone で Citrix エンタープライズアプリが信頼されるようにする手順を示すガイドを表示するよう求めます。

Secure Mail での自動登録

MAM-only 展開の場合、Endpoint Management を、Android または iOS デバイスを持ち、メール資格情報で Secure Hub に登録したユーザーが Secure Mail に自動的に登録されるように構成できます。これは、ユーザーが追加情報を入力する必要がないか、Secure Mail に登録する追加手順を実行する必要がないことを意味します。

Secure Mail を初めて使用する場合、Secure Mail は Secure Hub からユーザーの電子メールアドレス、ドメインおよびユーザー ID を取得します。Secure Mail は、Autodiscovery に電子メールアドレスを使用します。ドメインとユーザー ID を使用して Exchange Server が識別されます。Exchange Server によって、Secure Mail のユーザー自動認証が行われます。パスワードをパススルーしないようにポリシーが設定されている場合、ユーザーはパスワードの入力を求められます。ただし、ユーザーはさらに情報を入力する必要はありません。

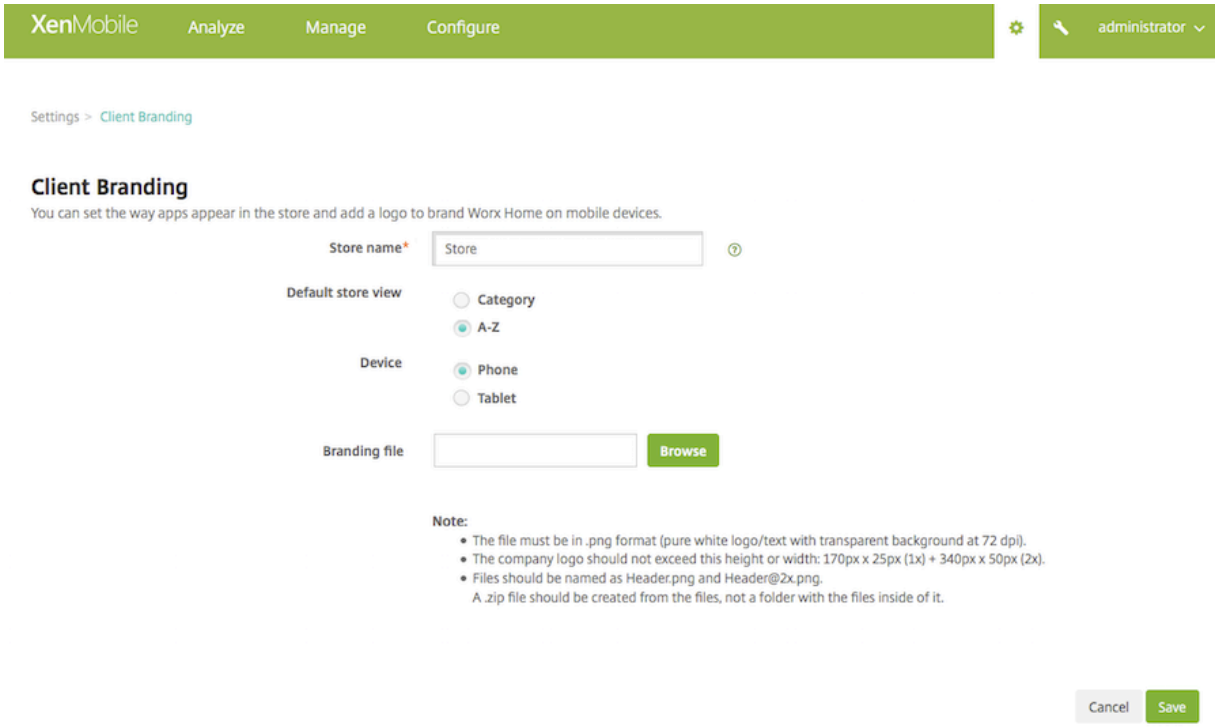
この機能を有効にするには、3 つのプロパティを作成する必要があります:

- サーバープロパティ MAM_MACRO_SUPPORT。手順については、「サーバープロパティ」を参照してください。
- クライアントプロパティ ENABLE_CREDENTIAL_STORE および SEND_LDAP_ATTRIBUTES。手順については、「クライアントプロパティ」を参照してください。

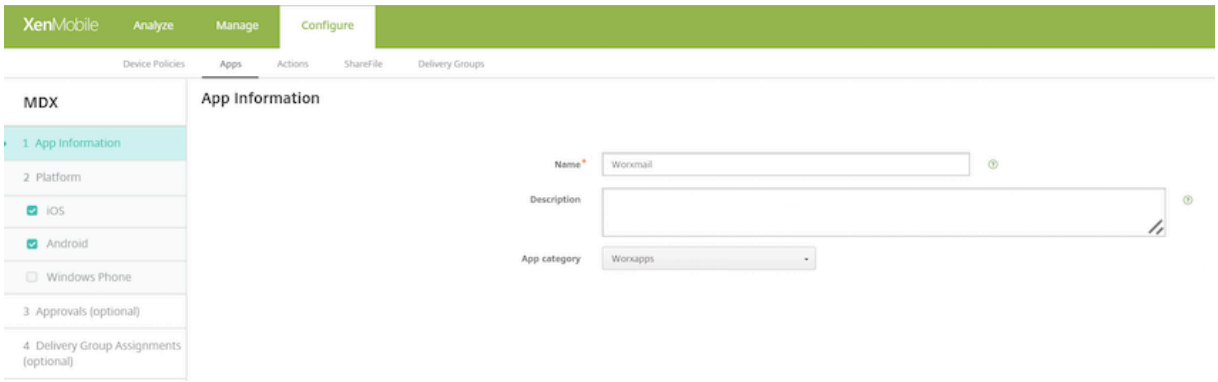
カスタマイズされたストア

ストアをカスタマイズする場合は、［設定］**>**［クライアントのブランド設定］の順に選択して、名前を変更し、ロゴを追加して、アプリの外観を指定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Endpoint Management コンソールでアプリの説明を編集できます。［構成］をクリックして、［アプリ］を選択します。表からアプリを選択して ［編集］をクリックします。編集する説明があるアプリのプラットフォームを選択し、［説明］ボックスに文字列を入力します。

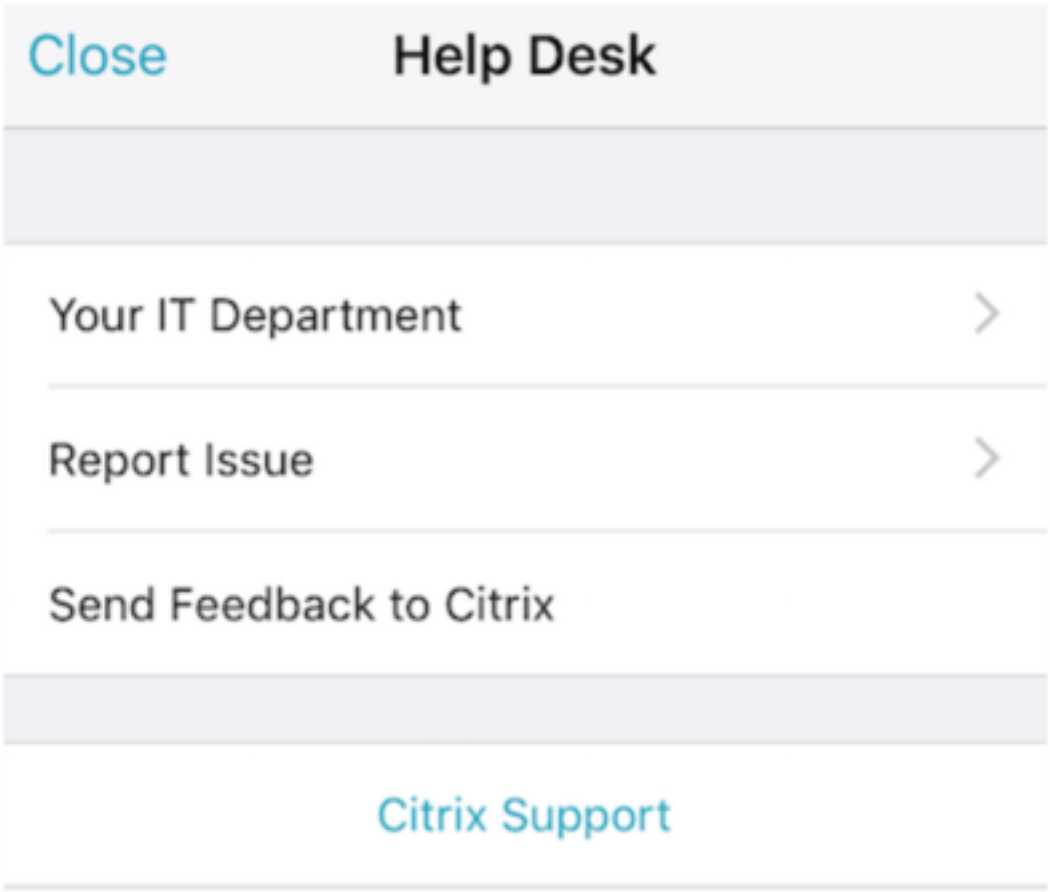


Store では、ユーザーは Endpoint Management で構成および保護されたアプリおよびデスクトップのみを参照できます。アプリを追加するには、［詳細］をタップしてから、［追加］をタップします。

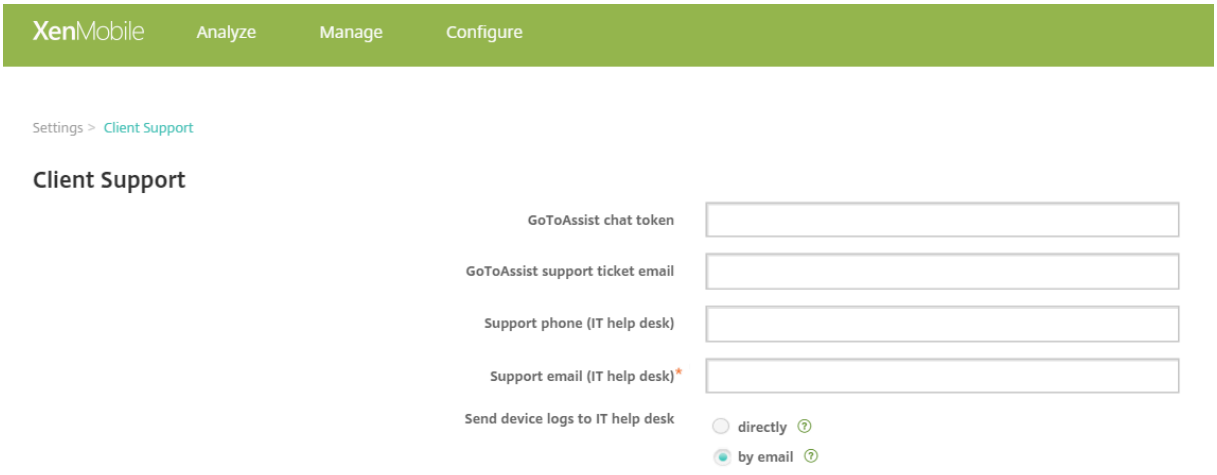
構成済みのヘルプオプション

また、Secure Hub では、ユーザーがヘルプを得られるさまざまな方法も提供しています。タブレットでは、右上隅にあるクエスチョンマークをタップするとヘルプオプションが表示されます。スマートフォンで、左上隅にあるハンバーガーメニューアイコンをタップしてから、［ヘルプ］をタップします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



[**IT** 部門］には会社のヘルプデスクの電話番号とメールアドレスが表示され、ユーザーがアプリから直接アクセスできます。Endpoint Management コンソールで電話番号とメールアドレスを入力します。右上隅にある歯車のアイコンをクリックします。［設定］ページが開きます。［詳細］をクリックして ［クライアントサポート］をクリックします。情報を入力する画面が表示されます。



［問題の報告］にユーザーのアプリの一覧が表示されます。ユーザーは、問題のあるアプリを選択します。Secure

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Hub で自動的にログが生成され、Secure Mail に、zip ファイルとしてログが添付されたメッセージが開かれます。ユーザーは、件名の行と問題の説明を追加します。スクリーンショットを添付することもできます。

[**Citrix** へのフィードバックの送信] をクリックすると、Citrix サポートのアドレスが入力された Secure Mail のメッセージが開きます。メッセージの本文で、Secure Mail の改善点についてのメッセージを入力することができます。デバイスに Secure Mail がインストールされていない場合は、ネイティブのメールプログラムが開きます。

またユーザーは [**Citrix** サポート] をタップして、Citrix Knowledge Centerを開くこともできます。ここでは、すべての Citrix 製品のサポート文書を検索できます。

[環境設定] で、ユーザーのアカウントとデバイスに関する情報を確認できます。

位置情報ポリシー

また、Secure Hub は位置情報ポリシーや地理追跡ポリシーを提供します。これにより、たとえば、会社所有のデバイスが特定の地理的境界の外側に出ていないかどうかを確認できます。詳しくは、「位置情報デバイスポリシー」を参照してください。

クラッシュ発生時の情報収集と分析

Secure Hub では障害の原因を確認できるように、障害の情報を自動的に収集し分析します。Crashyltics ソフトウェアがこの機能をサポートします。

iOS および Android で利用できる機能については、「Citrix Secure Hub」のプラットフォームごとの機能を参照してください。

Secure Hub のデバイスログの生成

このセクションでは、Secure Hub のデバイスログを生成するとともに、ログに正しいデバッグレベルを設定する方法について説明します。

Secure Mail のログを取得するには、以下を実行します。

1. [**Secure Hub**] **>** [ヘルプ] **>** [問題の報告] の順に選択します。アプリの一覧から [Secure Mail] を選択します。
   組織のヘルプデスク宛の電子メールが開きます。
2. ログの設定は、サポートチームからそうするように指示があった場合にのみ、変更します。設定が正しく行われていることを常に確認してください。
3. Secure Mail に戻り、問題を再現します。問題の再現を開始した時刻と、問題が発生した時刻またはエラー メッセージが表示された時刻に注目してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. ［**Secure Hub**］**>**［ヘルプ］**>**［問題の報告］の順に戻ります。アプリの一覧から［Secure Mail］を選択します。
   組織のヘルプデスク宛の電子メールが開きます。
5. 件名行と、問題を簡単に説明する本文を入力します。手順 3 で収集したタイムスタンプも追加して、［送信］をクリックします。
   完成したメッセージが開きます。圧縮されたログファイルが添付されています。
6. ［送信］をもう一度クリックします。

   送信される圧縮ファイルには、次のログが含まれています:

   - CtxLog_AppInfo.txt（iOS）、Device_And_AppInfo.txt（Android）、logx.txt and WH_logx.txt（Windows Phone）

   アプリケーション情報ログには、デバイスとアプリケーションに関する情報が含まれています。

Secure Mail の概要

November 1, 2023

Citrix Secure Mail では、スマートフォンまたはタブレット上でメール、カレンダー、および連絡先を管理できます。Microsoft Outlook または IBM Notes アカウントからの連続性を維持するため、Secure Mail は Microsoft Exchange Server および IBM Notes Traveler Server と同期します。

Citrix 製品ファミリのアプリである Secure Mail には、Citrix Secure Hub とのシングルサインオン（SSO）互換性があります。ユーザーが Secure Hub にサインオンした後は、ユーザー名とパスワードを再入力する必要なく、シームレスに Secure Mail に移動できます。デバイスが Secure Hub に登録されるとユーザーデバイスに自動的に公開されるように Secure Mail を構成できます。または、ユーザーが Store からアプリを追加できます。

> 注:
>
> Exchange Server 2010 のサポートは、2020 年 10 月 13 日に終了しました。

Secure Mail は次のものと互換性があります。

- Exchange Server 2019 累積更新プログラム 13
- Exchange Server 2019 累積更新プログラム 12
- Exchange Server 2019 累積更新プログラム 11
- Exchange Server 2019 累積更新プログラム 10
- Exchange Server 2019 累積更新プログラム 9
- Exchange Server 2019 累積更新プログラム 8
- Exchange Server 2019 累積更新プログラム 7

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Exchange Server 2019 累積更新プログラム 6
- Exchange Server 2016 累積更新プログラム 23
- Exchange Server 2016 累積更新プログラム 22
- Exchange Server 2016 累積更新プログラム 21
- Exchange Server 2016 累積更新プログラム 20
- Exchange Server 2016 累積更新プログラム 19
- Exchange Server 2016 累積更新プログラム 18
- Exchange Server 2016 累積更新プログラム 17
- Exchange Server 2013 累積更新プログラム 23
- Exchange Server 2013 累積更新プログラム 22
- Exchange Server 2013 累積更新プログラム 21
- HCL Domino バージョン 12.0.2 FP2
- HCL Traveler バージョン 12.0.2.1 ビルド 202302010413_30
- HCL Domino 11（旧称 Lotus Notes）
- HCL Domino 10.0.1（旧称 Lotus Notes）
- HCL Domino 9.0.1 FP10 HF197（旧称 Lotus Notes）
- HCL Domino 10.0.1.0 ビルド 201811191126_20（旧称 Lotus Notes）
- HCL Domino 9.0.1.21（旧称 Lotus Notes）
- Microsoft Office 365（Exchange Online）

まず、Secure Mail とその他の Endpoint Management コンポーネントをCitrix Endpoint Management のダウンロードからダウンロードします。

Secure Mail および他のモバイルアプリのシステム要件については、「システム要件」を参照してください。

アプリがバックグラウンドで実行されている時、または閉じている時の Secure Mail for iOS および Android の通知については、「Secure Mail のプッシュ通知」を参照してください。

Secure Mail でサポートされている iOS 機能については、「Secure Mail の iOS 機能」を参照してください。

Secure Mail でサポートされている Android 機能については、「Secure Mail の Android 機能」を参照してください。

Secure Mail でサポートされている iOS 機能と Android 機能については、「Secure Mail の iOS 機能と Android 機能」を参照してください。

ユーザー向けヘルプドキュメントについては、Citrix ユーザーヘルプセンターの「Citrix Secure Mail」のページを参照してください。

Citrix Secure Web

July 27, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Secure Web は、内部サイトおよび外部サイトへのセキュアなアクセスを提供する HTML5 互換のモバイル Web ブラウザーです。デバイスが Secure Hub に登録されるとユーザーデバイスに自動的に公開されるように Secure Web を構成できます。または、Endpoint Management アプリストアからアプリを追加することもできます。

Secure Web および他の業務用モバイルアプリのシステム要件については、「業務用モバイルアプリのサポート」を参照してください。

Secure Web の統合と提供

> 注:
>
> MDX Toolkit 10.7.10 は、業務用モバイルアプリのラッピングをサポートする最終リリースです。業務用モバイルアプリバージョン 10.7.5 以降には、パブリックアプリストアからアクセスします。

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シングルサインオン（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、この資料の後半にある「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:

- トンネル **- Web SSO**：内部ネットワークをトンネルする接続は、クライアントレス VPN の一種である「トンネル - Web SSO」を使用できます。これは、［優先 **VPN** モード］ポリシーに指定されるデフォルトの構成です。トンネル–Web SSO は、シングルサインオン（SSO）を必要とする接続に対して推奨されます。
- 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。ただし Secure Web は、モバ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

イルデバイスに保存されているクライアント証明書を読み取ることができません。この機能を提供できる、ラッピングされたサードパーティ製のエンタープライズアプリがインストールされている場合があります。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。

- [**VPN** モードの切り替えを許可] ポリシーにより、完全 VPN トンネルモードとトンネル-Web SSO モードを必要に応じて自動的に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、トンネル-Web SSO モードでは処理できません。同様に、[トンネル Web SSO] モードの使用時には、HTTP 認証チャレンジが SSO で実行される可能性が高くなります。

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
トンネル-Web SSO	HTTP	いいえ	はい	いいえ	いいえ	いいえ
トンネル-Web SSO	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

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:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。ただし、プロトコルに関係なく Facebook、Google、Hotmail などのパブリック URL を開くことはできません。

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。デフォルトの値は、［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/`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

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。

オプション

- 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。デフォルトの値は、［オフ］です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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、トンネル-Web SSO 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、このブログ投稿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、NetScaler Gateway ドキュメントの「Supporting DNS Queries by Using DNS Suffixes for Android Devices」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

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	iOS Secure Web	Android 6.x/7.x Secure Web
JavaScript エンジン	JavaScriptCore	V8
ローカルストレージ	X	X
AppCache	X	X

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

技術	iOS Secure Web	Android 6.x/7.x Secure Web
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

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。VPN 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、Citrix VPN、Cisco AnyConnect、Pulse Secureなどの App Store で入手可能な VPN クライアントアプリを使用することもできます。

- 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、Citrix 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 の種類を報告します。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 アーカイブを含めます。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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/」を入力してから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。バックグラウンドでアーカイブ化が実行されます。これには数分かかることがあります。
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。サポートチケットを開くときに、このファイルを Citrix サポートに送信できます。

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：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ユーザーが **Mailto** リンクをタップすると、Citrix 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。
- iOS では、URL の前に **ctxmobilebrowser://** を付けることで、ユーザーはネイティブのメールアプリから Secure Web 内のリンクを開くことができます。たとえば、ネイティブのメールアプリで`example.com`を開くには、ctxmobilebrowser://example.com という URL を使用します。
- 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。

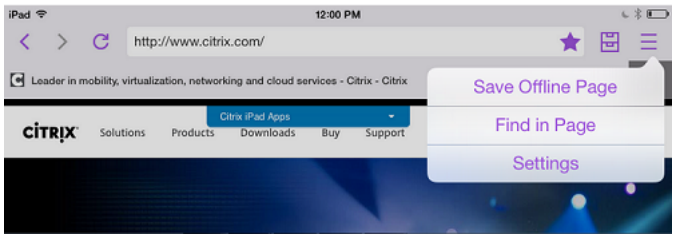
  > 注:
  >
  > Secure Web のメモリの大部分は、ポップアップのレンダリングで消費されます。そのため、通常、[設定] でポップアップをブロックすることで、パフォーマンスが向上します。

- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 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。



Secure Web の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。

> 注:
>
> - Citrix Files for XenMobile は、2023 年 7 月 1 日に製品終了（EOL）になりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

業務用モバイルアプリ向け **Citrix QuickEdit**

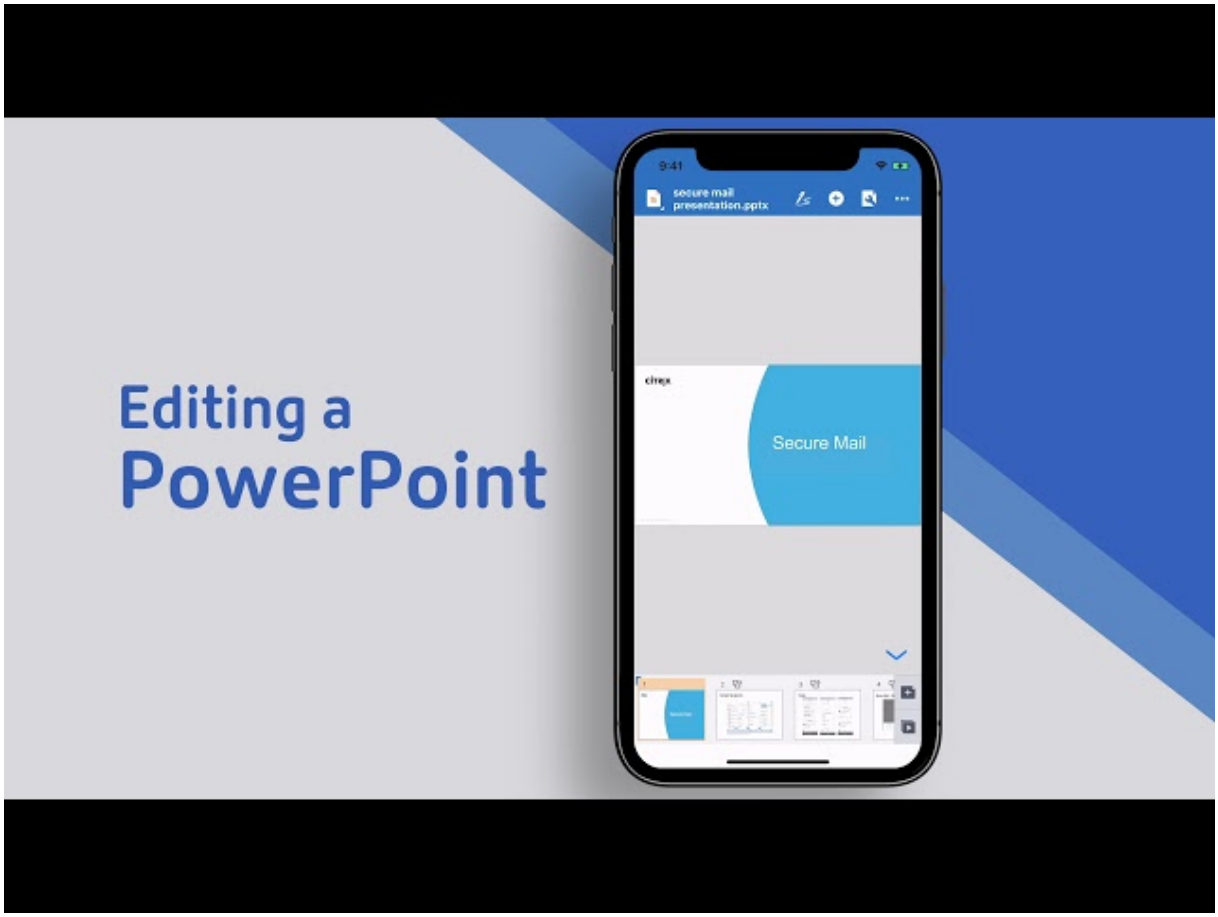
December 16, 2021

Citrix QuickEdit は、業務用モバイルアプリの編集ツールです。Citrix Secure Mail と Citrix Content Collaboration for Endpoint Management との連携により、セキュアな Endpoint Management 環境内でシームレスなワークフローが提供されます。

> 更新:
>
> - **2020** 年 **6** 月 **19** 日更新： MDX 暗号化は 2020 年 9 月 1 日に製品終了（EOL）に達します。そのため、2020 年 7 月までに MDX 暗号化からの移行をテストし、計画する必要があります。
> - **2018** 年 **7** 月 **2** 日更新： QuickEdit は業務用モバイルアプリとして継続します。2018 年 9 月 1 日に製品終了（EOL）とお知らせしていましたが、このステータスは適用されないことになりました。代わりに、QuickEdit のコンテンツ管理コンポーネントの更新が予定されています。

Citrix QuickEdit 機能のビデオについては、Citrix YouTube チャンネルで次のビデオを参照してください:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



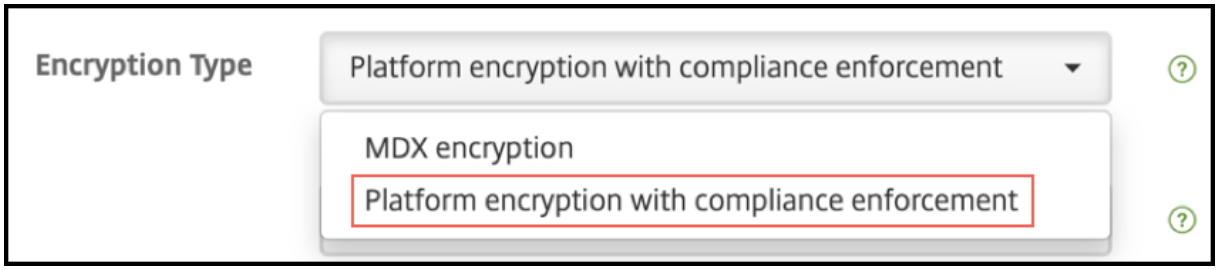
QuickEdit および他の業務用モバイルアプリのシステム要件については、「システム要件」を参照してください。

デバイスが Secure Hub に登録されるとユーザーデバイスに自動的に公開されるように QuickEdit を構成できます。または、ユーザーがアプリストアからアプリを追加できます。

QuickEdit はネイティブのメールプログラムとも互換性があるため、添付ファイルまたは Citrix Files リンクとしてファイルを簡単に共有したり転送したりできます。

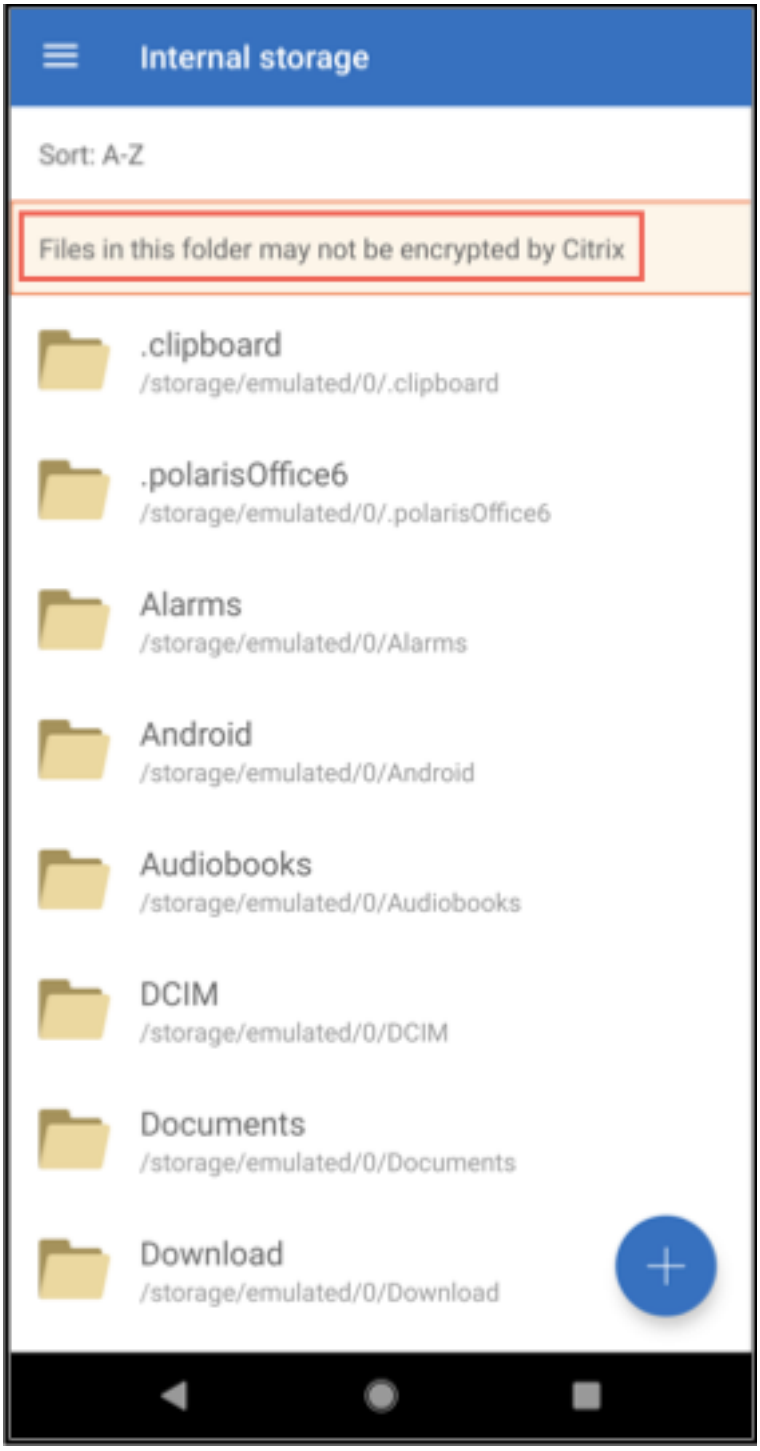
暗号化

QuickEdit バージョン 20.5.0 以降では、データ暗号化の種類を選択できます。暗号化の種類に ［コンプライアンス強制によるプラットフォーム暗号化］を選択すると、データはデバイスプラットフォームによって暗号化されます。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

暗号化の種類に ［コンプライアンス強制によるプラットフォーム暗号化］を選択すると、データはデバイスの SD カードに残りますが、カード内のファイルは暗号化されません。デバイスに次の警告が表示されます:



クラウドリポジトリに保存されているファイルへの影響は、データ暗号化の種類が変更されることのみです。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

サポートされているファイルタイプ

- Microsoft Word –DOC および DOCX
- Microsoft Excel –.xls および.xlsx
- Microsoft PowerPoint –PPT および PPTX
- .csv、.txt
- .jpeg、.png、.png、.svg、.bmp

最新のリリースでは次のファイルタイプは推奨されていません：.docm、.xlsm、.pptm、.rft

QuickEdit の統合と提供

QuickEdit と Endpoint Management を統合して提供するには、以下の一般的な手順に従います：

1. オプションとして、Secure Hub から SSO を有効にできます。これを行うには、Endpoint Management で Citrix Files アカウント情報を設定して、Citrix Files の SAML ID プロバイダとして Endpoint Management を有効にします。

   Endpoint Management での Citrix Files アカウント情報の設定は、すべての Endpoint Management クライアント、Citrix Files クライアント、および非 MDX Citrix Files クライアントで使用される 1 回だけの設定です。詳しくは、「Citrix Files クライアントの統合と提供」を参照してください。

2. QuickEdit をダウンロードします。

   - QuickEdit はEndpoint Management のダウンロードページからダウンロードできます。
   - 新規ユーザーの場合、QuickEdit は Citrix Workspace プラットフォームでも使用できます。詳しくは、「Citrix Workspace プラットフォーム」を参照してください。

3. ほかの MDX アプリの場合と同じ手順を使用して、QuickEdit を Endpoint Management に追加します。詳しくは、「アプリの追加」を参照してください。

ファイルのアップロード

デバイスから ShareFile などのクラウドリポジトリにファイルをアップロードし、ほかのデバイス上でそれらにアクセスできます。QuickEdit は現在、iOS と Android でのみサポートされています。ただし、ファイルがクラウドリポジトリに移行されている場合は、デバイス上の任意のツールを使用して編集できます。

現在のリリースの解決された問題と既知の問題

以下は、最新リリースでの既知の問題または解決された問題です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

解決された問題

- QuickEdit for iOS または ScanDirect から Secure Mail にファイルを送信しようとすると、転送できません。回避策として、これらのアプリのポリシー設定で次のファイル暗号化の除外を追加します:「/tmp/.com.apple.Pasteboard」（バージョン 6.14 にあります）

既知の問題

- ページサイズが 10,000 ポイント（幅または高さ）を超えると、潜在的なメモリエラーを防ぐためにドキュメントが開きません。
- QuickEdit でデジタル署名とインライン画像がサポートされていません。
- iOS 12 デバイス上の QuickEdit でファイルを作成すると、「メモリ不足のため」の問題が表示されます。
- 編集モードでファイルを開いて［注釈］オプションを選択した場合のみ、PDF ファイルへの注釈を表示できます。
- 150MB を超える PDF ファイルを開くと、「サポートされていないファイル」のエラーメッセージが表示されます。
- iPad 上の QuickEdit では、編集モードでキーボードが想定通りに表示されません。
- 複数の写真を含む PowerPoint（.ppt）ファイルを作成できません。

制限事項

- QuickEdit は共有デバイスではサポートされていません。
- 共有デバイスをサポートする古いバージョンの QuickEdit を実行していて、iOS バージョン 7.4.0 以降の QuickEdit にアップグレードすると、ローカルで管理されているすべてのファイルとフォルダーが失われます。ただし、Citrix Files データは影響を受けず、アクセス可能です。

ShareConnect

August 8, 2022

> 重要:
>
> ShareConnect は、2020 年 6 月 30 日に製品終了（EOL）になりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

ShareConnect を使用すると、ユーザーは iPad、Android タブレット、Android スマートフォンから自分のコンピューターに安全に接続して、ファイルやアプリケーションにアクセスできます。次のことを実行できます:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ユーザーのコンピューター上のファイルだけでなく、そのコンピューターで接続済みのネットワークドライブ上のファイルを操作する
- ShareConnect 内で、ターゲットマシンからアプリを実行する
- ほかの業務用モバイルアプリをラップせずに、モバイルアプリにアクセスする
- モバイルに最適化したアクセスのため、ShareConnect を Citrix Virtual Desktops で実行する

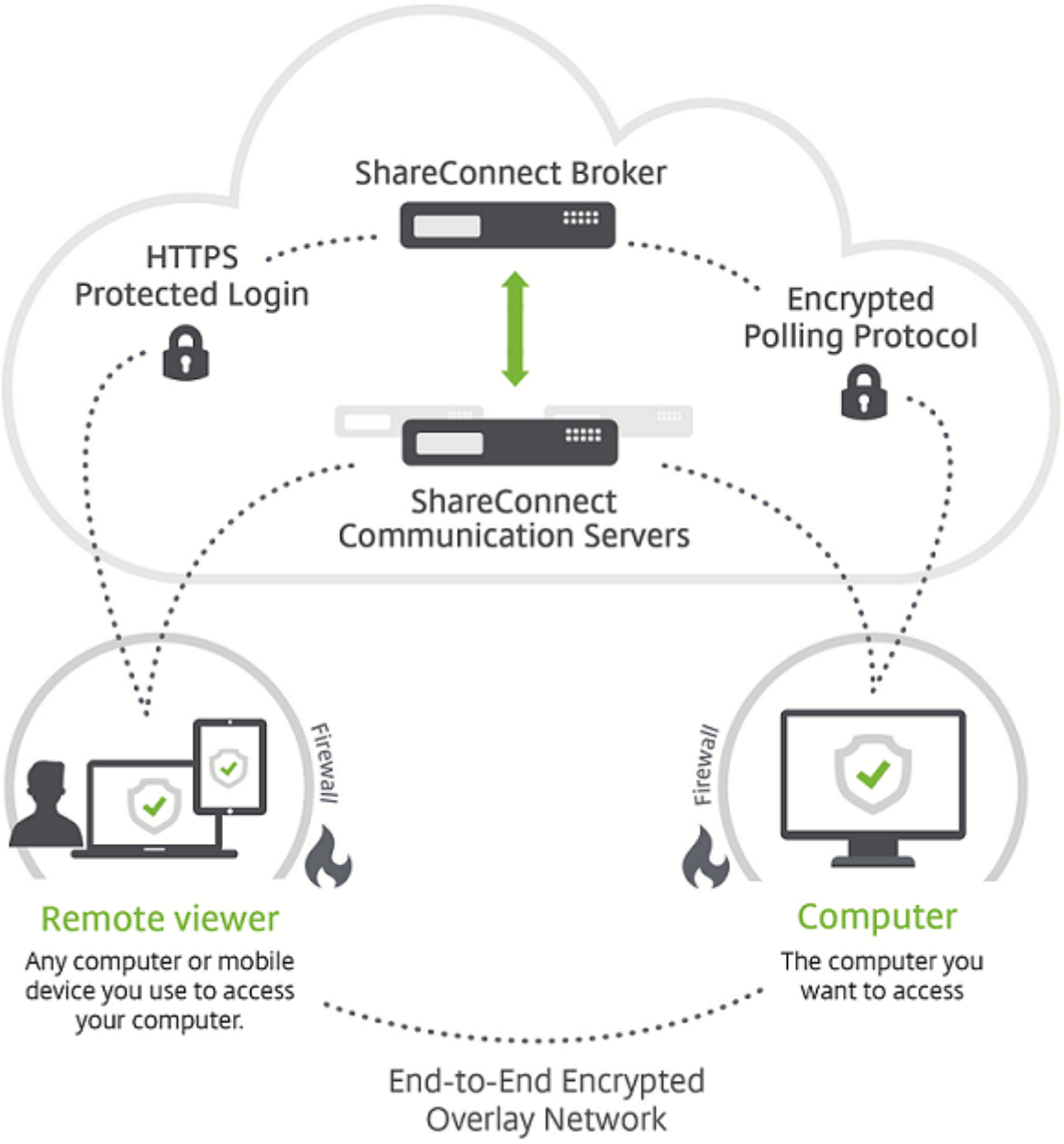
ShareConnect の MDX バージョンはEndpoint Management のダウンロードページからダウンロードできます。

ShareConnect のインストール方法および使い方については、Citrix Knowledge Centerを参照してください。

アーキテクチャの概要

ShareConnect コンポーネントには、次の図で示すようにシトリックス所有の ShareConnect Broker や ShareConnect Communication Servers があります。ShareConnect Broker は、ユーザーをコンピューターにマップするアプリケーションサーバーおよびデスクトップです。その後、アプリケーションは、ホストコンピュータがオンラインかオフラインかをユーザーに知らせます。ShareConnect Communication Servers は、ホストコンピューターとクライアントコンピューター間でデータを交換するために使用されます。データは、**Endpoint Management** 設定をベースとしたホストコンピューターとクライアントコンピューター間でセキュアなマイクロ VPN トンネルを介してやり取りできます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



また Citrix Files は、Endpoint Management または Active Directory Federation Services（ADFS）などの SAML ID プロバイダー（IdP）でシングルサインオン（SSO）を介したユーザー認証を提供できます。Endpoint Management での展開においては、Citrix Gateway を介してネットワーク外のリソースへアクセスします。

ShareConnect での接続

ShareConnect では、直接または間接のいずれかによる接続が確立されます。

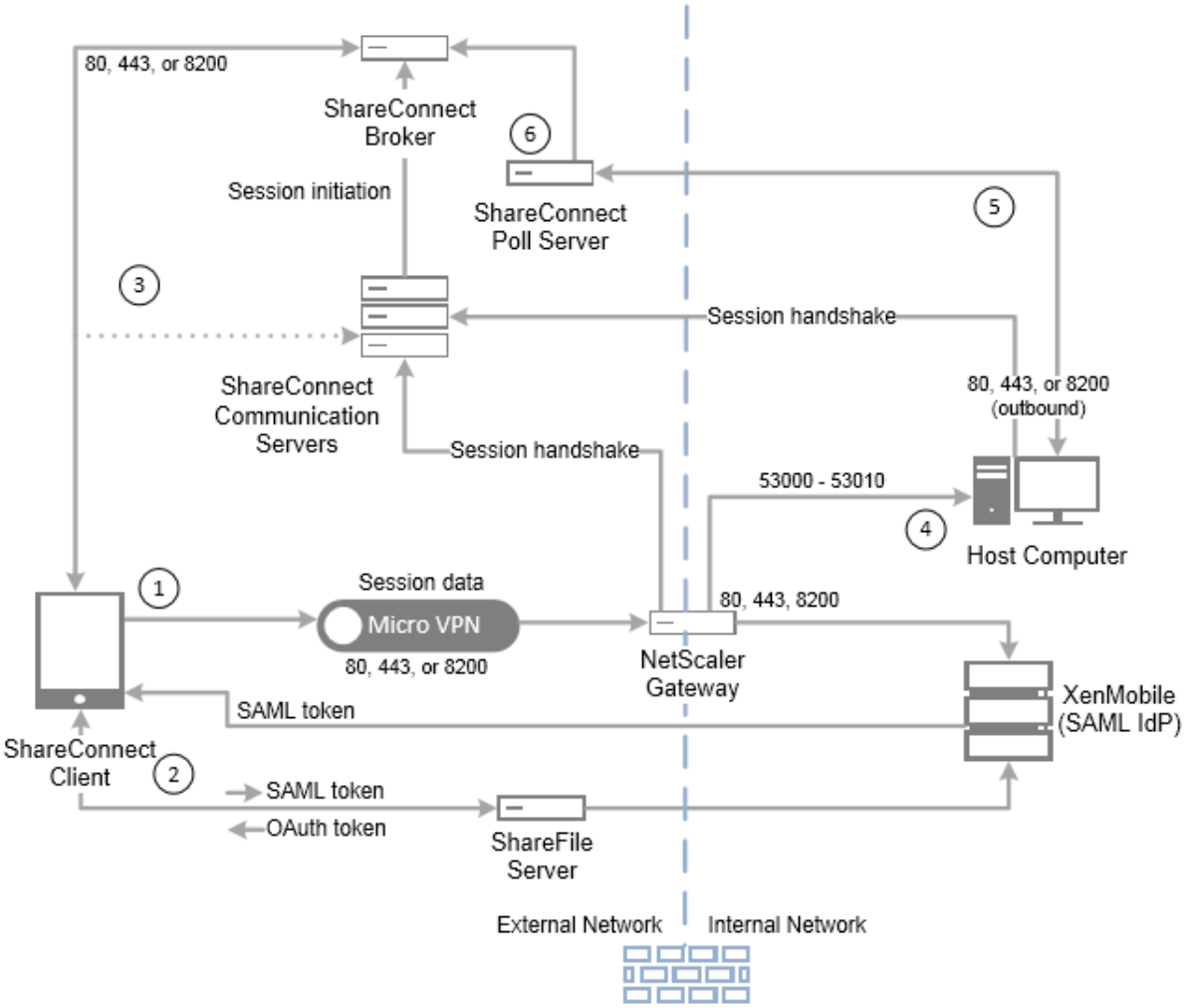
- 直接接続。ShareConnect は、クライアントコンピューターとホストコンピューターが同じ LAN または Wi-Fi ネットワークにある場合、その間に直接接続を確立します。この場合、クライアントコンピューターま

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

たはモバイルデバイスとホストコンピューター間のアクセスにおいてデータが直接やり取りされます。パフォーマンスを最適化した結果、データは ShareConnect Communication Servers を通ってはフローしません。直接接続の場合、Endpoint Management は Citrix Gateway を使ってローカルネットワークの外にあるリソースへの安全なアクセスを提供します。

- 間接接続。ShareConnect は、クライアントコンピューターとホストコンピューターに直接到達できない場合、関節接続を確立します。この場合、データは ShareConnect Communication Servers を通ってフローします。

次の図は、ユーザーが直接接続を使って ShareConnect が動作するコンピューターまたはモバイルデバイスからホストコンピューターにアクセスする場合に使用される接続を示しています。接続手順については、別の図で説明しています。



• このシナリオでは、Endpoint Management が Citrix Files の SAML IdP として機能し、Secure Hub から SSO を提供するように構成します。ShareConnect が Secure Hub に SAML トークンを要求し、次に Citrix Gateway を介して要求が Endpoint Management に渡されます。その後、Endpoint Management は SAML トークンを ShareConnect に送信します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ShareConnect は SAML トークンを検証し、SAML トークンと OAuth トークンを取り換えるために Citrix Files に送信します。
- ShareConnect は OAuth トークンを ShareConnect Broker に送信し、これによりセッショントークンが ShareConnect に送信されます。
- ShareConnect は ShareConnect Broker からホストコンピューターの一覧を取得し、ホストコンピューターの資格情報が要求されます。その後、ShareConnect は ShareConnect Communication Server との直接接続を確立します。ホストコンピューターが資格情報を検証した後、ShareConnect はそのホストコンピューターからファイルとアプリの一覧を取得します。ユーザーがファイルまたはアプリを開いた後、ShareConnect とホストコンピューター間での直接接続が実行されます。
- ホストコンピューター上の ShareConnect エージェントは、状態メッセージを ShareConnect Poll Server に送信して、それがオンラインかオフラインかを示します。
- ShareConnect Poll Server は、ShareConnect エージェントからの負荷分散された要求を ShareConnect Broker に送信し、またホスト状態の更新を ShareConnect Broker に送信します。

ShareConnect のセキュリティ

ShareConnect では組み込みの 128 ビット AES 暗号化が使用され、ShareConnect クライアントと ShareConnect エージェントを実行するホストコンピューター間で送信されるすべてのデータはエンドツーエンドで完全に暗号化されます。暗号化キーは各接続に一意なものです。最高性能の装置でも、重要データを傍受して暗号を解読することは不可能です。

通常は ShareConnect を構成して、データが ShareConnect クライアントとホストコンピューター間で直接やり取りされるようにします。無制限アクセスに対するネットワークアクセスポリシーを構成しない限り、データは ShareConnect Communication Server を経由しません。ポリシーについて詳しくは、「Endpoint Management に ShareConnect を追加するには」を参照してください。

直接または間接接続の場合、接続の確立に必要な IP アドレスやポートといった暗号化されたメタデータは、ShareConnect サーバーに送信されます。

また、ShareConnect の MDX ラッピングでは、MDX Vault を介したデータ暗号化を提供します。iOS（iOS 9 より前）および Android の両方のデバイスで MDX ラップアプリと関連する保存データが暗号化されます。暗号化には、OpenSSL により提供された FIPS 認定済み暗号化モジュールが使用されます。

セキュリティ設定および管理コントロールに関する情報については、以下のセキュリティホワイトペーパーを参照してください。

ShareConnect セキュリティホワイトペーパー

ShareConnect 管理ガイド

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ShareConnect のポート要件

ShareConnect 通信を許可するには、次のポートを開きます。ポート要件は接続の種類により異なります。同じ LAN または Wi-Fi ネットワーク上にあるコンピューター同士の接続は、直接接続の場合があります。また、クライアントおよびホストコンピューターが直接接続できない場合は、間接接続の場合もあります。

直接接続の場合

TCP ポート 80 - Citrix Gateway から app.shareconnect.com への発信接続のために使用されます。

接続元 - Citrix Gateway

接続先 - app.shareconnect.com

TCP ポート 80、443、8200 - Citrix Gateway から ShareConnect Communication Server への発信接続のため、これらの 1 つ以上のポートが必要です。

接続元 - Citrix Gateway

接続先 - ShareConnect Communication Server

TCP ポート 80、443、8200 - ShareConnect ホストコンピューターから Citrix サーバーへの発信接続のため使用されます。

接続元 - ShareConnect ホストコンピューター

接続先 - poll.shareconnect.com、ShareConnect Communication Server

TCP ポート 443 - Citrix Gateway から必要なサイトへの発信接続のために使用されます。

接続元 - Citrix Gateway

接続先 - crashlytics.com、secure.sharefile.com、ShareFile_sub-domain.sharefile.com

TCP ポート 53000～53010 - Citrix Gateway から ShareConnect ホストコンピューターへの発信接続のために使用されます。

接続元 - Citrix Gateway

接続先 - LAN ベースの ShareConnect ホストコンピューター

TCP ポート 53000～53010 - Citrix Gateway から ShareConnect ホストコンピューターへの受信接続のために使用されます。

接続元 - Citrix Gateway

接続先 - LAN ベースの ShareConnect ホストコンピューター

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

間接接続の場合

TCP ポート 80 - ShareConnect エージェントから app.shareconnect.com への発信接続のために使用されます。

接続元 - ShareConnect エージェント

接続先 - app.shareconnect.com

TCP ポート 80、443、8200 - ShareConnect エージェントから ShareConnect Communication Server への発信接続のため、これらの 1 つ以上のポートが必要です。

接続元 - ShareConnect エージェント

接続先 - ShareConnect Communication Server

TCP ポート 80、443、8200 - ShareConnect ホストコンピューターから Citrix サーバーへの発信接続のため使用されます。

接続元 - ShareConnect ホストコンピューター

接続先 - poll.shareconnect.com、ShareConnect Communication Server

TCP ポート 443 - ShareConnect エージェントから必要なサイトへの発信接続のために使用されます。

接続元 - ShareConnect エージェント

接続先 - crashlytics.com、secure.sharefile.com、ShareFile_sub-domain.sharefile.com

ShareConnect の統合と提供

ShareConnect を Endpoint Management と統合して提供するには、次の一般的な手順に従います:

1. オプションとして、Secure Hub から SSO を有効にできます。これを行うには、Endpoint Management で Citrix Files アカウント情報を設定して、Citrix Files の SAML IdP として Endpoint Management を有効にします。

   Endpoint Management での Citrix Files アカウント情報の設定は、1 回だけの設定です。1 回だけの設定は、すべての業務用モバイルアプリクライアント、Citrix Files Worx クライアント、および非 MDX Citrix Files クライアントで使用されます。

2. ShareConnect をダウンロードしてラップします。詳しくは、「MDX Toolkit について」を参照してください。
3. ShareConnect を Endpoint Management に追加して、MDX ポリシーを構成します。
4. ホストコンピューターへの ShareConnect エージェントのインストール。ShareConnect エージェントは MSI パッケージなので、既存のソフトウェア展開方式により配信およびインストールできます。インストールしてから 1 時間以内に、ユーザーは Citrix Files 資格情報を使ってエージェントに署名してホストコンピューターを登録する必要があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

または、ShareConnect で接続するコンピューターに ShareConnect エージェントをインストールできます。詳しくは、「コンピューターに ShareConnect エージェントをインストールするには」を参照してください。

Endpoint Management に ShareConnect を追加する

ほかの MDX アプリの場合と同じ手順を使用して、ShareConnect を Endpoint Management に追加します。詳しくは、「MDX アプリの追加」を参照してください。ShareConnect を追加する場合、MDX ポリシーを次の表で示すように構成します。

ポリシー	値	結果
ネットワークアクセス	内部ネットワークへトンネルまたは制限なし	[内部ネットワークへトンネル] は、すべてのネットワークアクセスに内部ネットワークへのアプリケーションごとの VPN トンネルを使用します。この構成により、ShareConnect とホストコンピューター間に直接接続が提供されます。[制限なし] は、シトリックス所有の Communication Server を使ってホストコンピューターと ShareConnect 間で暗号化されたデータをやり取りします。ネットワークアクセスに [内部ネットワークへトンネル] を使おうとする場合でも、制限されていないアクセスでセットアップをテストしてすべてが機能するか確認してください。
優先 VPN モード	トンネル-Web SSO	SSO を必要とする接続に対して初期接続モードを適切に設定します。
暗号化を有効化	オン	タブレットに格納されているデータが暗号化されます。
切り取りおよびコピー	制限なし	ShareConnect で切り取りとコピー操作が有効になります。
貼り付け	制限なし	ShareConnect で貼り付け操作が有効になります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ポリシー	値	結果
ドキュメント交換（このアプリケーションで開く）	制限なし	ユーザーは、ShareConnect から接続しているコンピューターまたは接続しているネットワークドライブ上のファイルを開くことができます。
パスワードの保存	オフ	ユーザーは、ShareConnect にサインオンするたびに、コンピューターのユーザー名とパスワードを入力するよう要求されます。

コンピューターに **ShareConnect** エージェントをインストールするには

次の手順では、ユーザーがサポートされているモバイルデバイスから接続する物理または仮想コンピューターごとに、ShareConnect エージェントをインストールする方法について説明します。

これらの手順を実行する前に、まず Secure Hub をインストールする必要があります。次に、プロンプトに従ってサポートされているモバイルデバイスに業務用モバイルアプリをインストールするのを許可する必要があります。

1. タブレットで Secure Hub にサインオンします。
2. ShareConnect を開き、
3. [Email download link] をタップします。

   Citrix の no-reply@shareconnect.com からメールが送信されます。
4. ShareConnect からアクセスするホストコンピューターで、このメールを開きます。
5. メール内の［Set up this computer］をクリックします。
6. **ShareConnect_Installer.exe** をダブルクリックしてインストールを開始します。

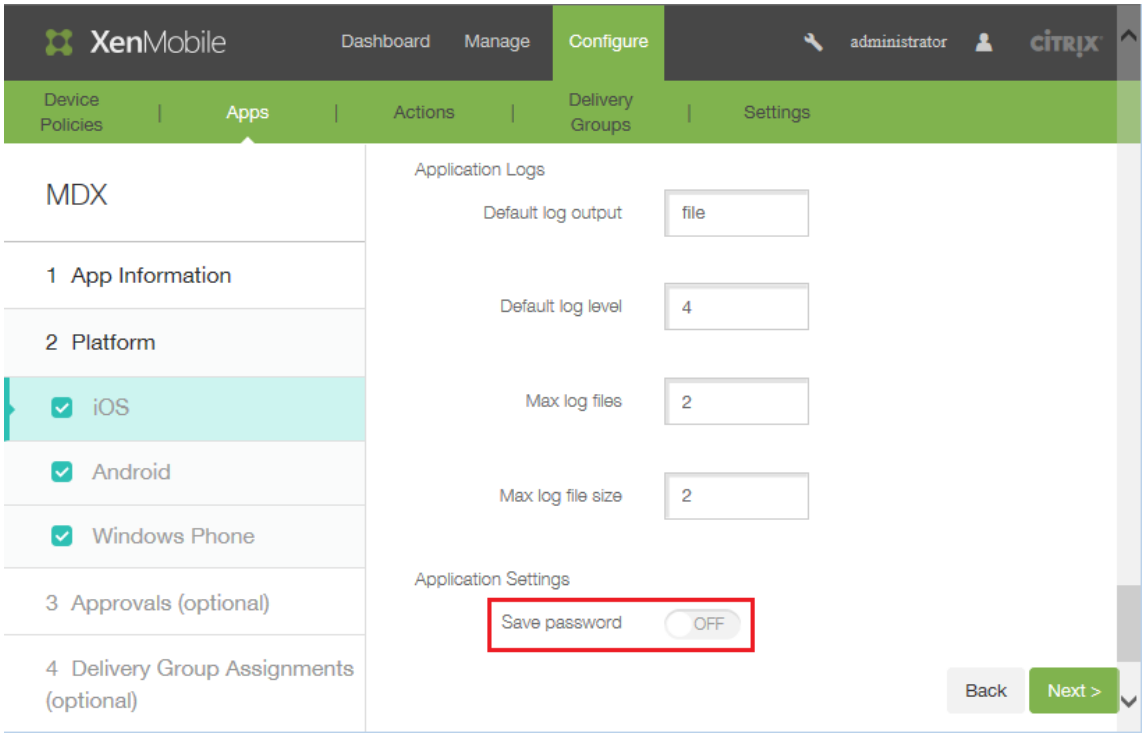
   ホストコンピューターに ShareConnect エージェントがインストールされます。インストール時、Citrix Files SSO が構成されている場合は、ShareConnect によってメールアドレスが求められます。Citrix Files SSO が構成されていない場合は、Citrix Files 資格情報が要求されます。
7. 表示される手順に従って処理を実行します。

次に、ShareConnect エージェントがホストコンピューターを登録します。これにより、電源がオンになっていて 1 つ以上の公開ポート（80、443、または 8200）で poll.shareconnect.com に到達できるホストコンピューターであれば、ShareConnect クライアントから接続できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

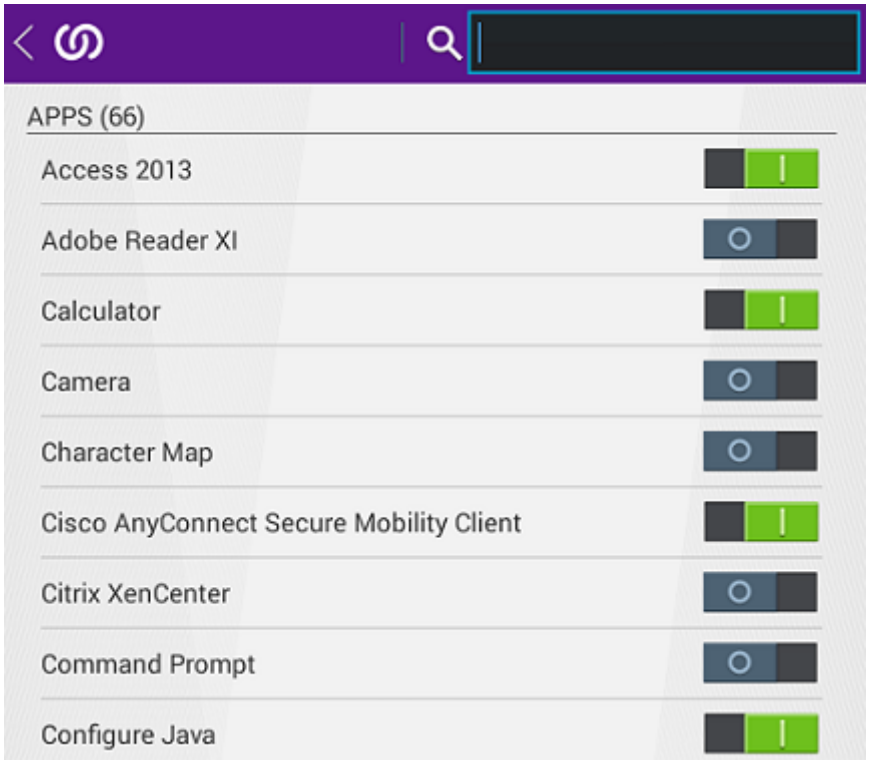
ShareConnect 機能

- ホストコンピューターの追加。ユーザーは ShareConnect を使ってサポートされているモバイルデバイスからリモートホストコンピューターを追加して接続できます。
- ファイルのアクセス。ユーザーが最近使用したファイルの一覧が表示されるので、ホストコンピューターおよび接続されているドライブ上のファイルに簡単にアクセスできます。
- ファイルの編集。ユーザーは、タブレットから自分のコンピューター上のデスクトップアプリケーションを使用してファイルを編集できます。また、ユーザーは、アプリケーションを全画面表示で使用できます。
- 画面共有。単一のファイルやアプリを表示する代わりに画面共有機能を使って、ホストコンピューターのデスクトップを表示できます。
- **Citrix Files** の統合。ユーザーは、ホストコンピューターと Citrix Files の間で、ファイルを移動または共有できます。
- キーボードとマウス。ShareConnect では、Bluetooth キーボードと Citrix XI Prototype Mouse を同時に使用できます。
- ポート制限。ShareConnect で使用されるポートは 53000 から 53010 のみです。
- 各サインオン時のパスワード入力の強制。セキュリティを強化するため、ShareConnect への各サインオン時にコンピューターパスワードの入力を必須にすることができます。次の図に示しているように、Save password ポリシーが無効の場合は、接続するたびにサインオン資格情報の入力が必要となります。



- アプリの追加と削除。ユーザーは、各アプリの横のスイッチをオンまたはオフにして、ShareConnect 内のアプリトレイからアプリを追加または削除できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- プレビュー済みファイルのキャッシュ。ShareConnect では、ユーザーがアクセスしたファイルがキャッシュされます。ユーザーがほかのファイルをプレビューした後で元のファイルにアクセスしたときに再ダウンロードは行われません。これにより、ファイルのロード時間が改善されます。

ShareConnect のトラブルシューティング

ShareConnect エージェントのインストールの問題

問題	説明と解決策
ユーザーが ShareConnect エージェントをダウンロードしてから 1 時間以上インストールを開始しない場合は、Citrix Files アカウント名とパスワードを入力して ShareConnect エージェントを登録する必要があります。	ShareConnect エージェントのインストーラーには、ダウンロード後 1 時間有効なトークンが含まれています。このトークンの有効期限が切れる前にインストールを開始しない場合、Citrix Files アカウントに 2 回サインオンする必要があります。最初に ShareConnect エージェントを登録するためにサインオンし、次にインストールが完了した後にエージェントにサインオンします。ShareConnect エージェントをダウンロードして 1 時間以内にインストールする場合は、サインオンは 1 度だけで済みます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

問題	説明と解決策
ShareConnect エージェントを登録する間、エージェントは接続を実行せず、「接続を確認してからもう一度実行してください。」といったエラーメッセージが表示されます。	poll.shareconnect.com へのポートがブロックされていないか確認します。詳しくは、このアーティクルの「システム要件」を参照してください。

ShareConnect の接続の問題

> 重要:
>
> ShareConnect をテストするため、ネットワークアクセスポリシーを ［制限なし］ に設定してポートとネットワーク設定の問題を除外することをお勧めします。無制限アクセスでは ShareConnect が ShareConnect Communication Server を介して接続し、通常はこれによって、ShareConnect モバイルデバイスおよびホストコンピューターでインターネットアクセスが有効な場合に接続をテストできるようになります。

問題	説明と解決策
ShareConnect が開始するが、ホストコンピューターに接続せず、資格情報を求めるプロンプトが表示されない。	このアーティクルの「システム要件」で説明しているポート要件を満たしているか確認してください。
Citrix Files アカウントの資格情報を使って ShareConnect にサインオンできない。	ShareConnect へのシングルサインオン（SSO）では、Citrix Files アカウントを SAML IdP で構成する必要があります。Endpoint Management を SAML IdP として使用する方法について詳しくは、「Citrix Content Collaboration for Endpoint Management」を参照してください。その他の IdP の構成について詳しくは、Knowledge Center の記事を参照してください。アカウントで SSO が構成されていない場合は、ShareConnect for iOS によりユーザーの Citrix Files ユーザー名とパスワードを求めるプロンプトが表示されます。
ユーザーが ShareConnect にサインオンした後、ShareConnect がホストコンピューターに接続できない。	ShareConnect を直接接続用に構成する（つまり、ネットワークアクセスポリシーを［内部ネットワークへトンネル］に設定する）と、ファイアウォールブロックやプロキシサーバー構成のようなネットワーク設定に制限があると、接続障害が起こります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix ShareFile Workflows

December 16, 2021

> 注:
>
> Secure Forms は 2018 年 3 月 31 日に製品終了（EOL）となりました。Citrix Files Platinum および Premium アカウントに含まれる ShareFile WorkFlow を使用することをお勧めします。

ShareFile Workflows は、Citrix Files カスタムワークフロー機能のモバイルコンポーネントです。この機能により、ユーザーは複数のトリガーや操作が含まれるカスタマイズされたワークフローを作成できます。カスタマイズされたフォームはワークフローテンプレートに追加し、ユーザーに割り当てることができます。

フォームが割り当てられたユーザーは、このフォームを ShareFile Workflows モバイルアプリで完了して送信できます。フォームデータのストレージは Citrix Files と安全に統合され、ワークフローファイルはレビュー、参照、および取得用に保存されます。

ワークフローおよびフォームのテンプレートは Citrix Files Web アプリケーション内で作成および管理されます。

ユーザードキュメント

ワークフローおよびフォームテンプレートの作成および管理に関連するユーザードキュメントは、以下の Citrix Knowledge Center にあります:

- ワークフローテンプレートの作成
- フォームテンプレートの作成
- ワークフローモバイルアプリからのフォームの送信

Citrix Content Collaboration for Endpoint Management

July 27, 2023

Citrix Content Collaboration for Endpoint Management クライアントは、Citrix Files モバイルクライアントの MDX 対応バージョンです。これらのクライアントでは、ほかの MDX ラップしたアプリのデータに、安全かつ統合的にアクセスできます。Citrix Content Collaboration for Endpoint Management クライアントでは、マイクロ VPN、Secure Hub を使用したシングルサインオン（SSO）、2 要素認証などの MDX 機能も使用できます。

Citrix Files は、エンタープライズクラスのファイル同期および共有サービスで、ユーザーは簡単かつ安全にドキュメントを共有できます。また、Citrix Files for Android Phone および Citrix Files for iPad などの Citrix Files モバイルクライアントを含む、さまざまなアクセスオプションが用意されています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Files と Endpoint Management を統合すると、Citrix Files の全機能セットを提供することも、ストレージゾーンコネクタへのアクセスのみを提供することもできます。デフォルトでは、Citrix Endpoint Management コンソールでは Citrix Files の構成のみが可能です。Endpoint Management でストレージゾーンコネクタを使用するように構成するには、Citrix Endpoint Management ドキュメントの「Endpoint Management で Citrix Content Collaboration を使用する」を参照してください。

Endpoint Management、Citrix Files、ストレージゾーンコントローラー、Citrix ADC を次のように使用して、Citrix Content Collaboration for Endpoint Management クライアントを展開および管理します:

- Endpoint Management が Citrix Files を含めて構成されている場合、Endpoint Management は SAML ID プロバイダ（IdP）として機能し、Citrix Content Collaboration for Endpoint Management クライアントを展開します。Citrix Files が Citrix Files データを管理します。Citrix Files データは Endpoint Management を経由しません。
- Endpoint Management が Citrix Files またはストレージゾーンコネクタを含めて構成されている場合、ストレージゾーンコントローラーがネットワーク共有と SharePoint のデータへの接続を提供します。ユーザーは、Citrix Files 業務用モバイルアプリ経由で保存されたデータにアクセスします。モバイルデバイスから Microsoft Office ドキュメントの編集、および Adobe PDF ファイルのプレビューと注釈付けができます。
- Citrix ADC は、接続のセキュリティを保護して外部ユーザーからの要求を管理し、要求を負荷分散して、ストレージゾーンコネクタのコンテンツスイッチを処理します。

Citrix Content Collaboration for Endpoint Management クライアントをダウンロードするには、Citrix.com のダウンロードページにアクセスします。

Citrix Content Collaboration for Endpoint Management および他の業務用モバイルアプリのシステム要件については、「業務用モバイルアプリのサポート」を参照してください。

Citrix Content Collaboration for Endpoint Management クライアントと **Citrix Files** モバイルクライアントとの違い

以下に、Citrix Content Collaboration for Endpoint Management クライアントと Citrix Files モバイルクライアントの違いについて説明します。

ユーザーアクセス

Citrix Content Collaboration for Endpoint Management クライアント:

ユーザーは、Citrix Content Collaboration for Endpoint Management クライアントを Secure Hub から取得して起動します。

Citrix Files モバイルクライアント:

ユーザーは、アプリストアから Citrix Files モバイルクライアントを取得します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SSO

Citrix Content Collaboration for Endpoint Management クライアント:

Endpoint Management と Citrix Files の統合の場合: Endpoint Management を Citrix Files 用の SAML IdP として構成できます。この構成では、Secure Hub は Endpoint Management を SAML IdP として使用して、Citrix Content Collaboration for Endpoint Management クライアント用の SAML トークンを取得します。Citrix Content Collaboration for Endpoint Management クライアントを起動した後、Secure Hub にサインオンしていないユーザーは、Secure Hub にサインオンするよう求められます。ユーザーは、自分の Citrix Files ドメインやアカウント情報を知っておく必要はありません。

Citrix Files モバイルクライアント:

Endpoint Management と Citrix Gateway を Citrix Files 用の SAML IdP として構成できます。この構成では、ユーザーが、Web ブラウザーまたはほかの Citrix Files クライアントを使用して Citrix Files にログオンしている場合、ユーザー認証のため Endpoint Management 環境にリダイレクトされます。Endpoint Management で認証された後、ユーザーは Citrix Files アカウントへのログオンに有効な SAML トークンを受信します。

マイクロ **VPN**

Citrix Content Collaboration for Endpoint Management クライアント:

リモートユーザーの場合、Citrix Gateway を介した VPN またはマイクロ VPN 接続を使用して接続し、内部ネットワークのアプリやデスクトップにアクセスすることができます。この機能は、Endpoint Management と統合された Citrix ADC を介して使用することができ、ユーザーには透過的です。

Citrix Files モバイルクライアント:

該当なし

2 要素認証

Citrix Content Collaboration for Endpoint Management クライアント:

Endpoint Management と統合された Citrix ADC では、クライアント証明書認証と別の種類の認証を組み合わせた認証もサポートされています（LDAP、RADIUS など）。

Citrix Files モバイルクライアント:

該当なし

フォルダーのアクセス許可

Citrix Content Collaboration for Endpoint Management クライアントと *Citrix Files* モバイルクライアント:

Endpoint Management と Citrix Files の統合の場合: Citrix Files によって決定されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ドキュメントアクセスの保護

Citrix Content Collaboration for Endpoint Management クライアント:

Secure Mail で受信した添付ファイルを開いたり、MDX ラップしたアプリでダウンロードできます。［このアプリケーションで開く］操作を実行すると、MDX ラップしたアプリのみが表示されます。Citrix Content Collaboration for Endpoint Management クライアントでは、ラップされていないアプリから取得したデータは使用できません。Secure Mail ユーザーは、Citrix Files リポジトリのファイルをデバイスにダウンロードしなくても添付できます。ラップされた Citrix Files とラップされていない Citrix Files がデバイス上に存在する場合、ラップされた Citrix Files クライアントは、ユーザーのパーソナル Citrix Files アカウント内のファイルにはアクセスできません。ラップされた Citrix Files クライアントは、Endpoint Management に構成されている Citrix Files サブドメインにのみアクセスできます。

Citrix Files モバイルクライアント:

ユーザーは、任意のアプリから添付ファイルを開くことができます。

Citrix Files アカウントへのアクセス

Citrix Content Collaboration for Endpoint Management クライアント:

Endpoint Management と Citrix Files の統合の場合: 個人用の Citrix Files アカウントまたはサードパーティの Citrix Files アカウントにアクセスするには、デバイス上で非 MDX バージョンの Citrix Files を使用する必要があります。

Citrix Files モバイルクライアント:

Endpoint Management と Citrix Files の統合の場合: Citrix Files クライアントから利用できます。

デバイスポリシー

Citrix Content Collaboration for Endpoint Management クライアントと *Citrix Files* モバイルクライアント:

Endpoint Management と Citrix Files の両方のデバイスポリシーが、Citrix Content Collaboration for Endpoint Management クライアントに適用されます。たとえば、Endpoint Management コンソールから、デバイスのワイプを実行できます。また、Citrix Files コンソールから、リモートで Citrix Files アプリをワイプできます。

MDX ポリシー

Citrix Content Collaboration for Endpoint Management クライアント:

MDX ポリシーでは、Citrix Endpoint Management アプリストアで適用される設定を構成できます。MDX でのみ使用できるポリシーには、カメラのブロック、マイク、メールの作成、画面キャプチャ、クリップボードの切り取り、コピー、貼り付けの各操作などがあります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Files モバイルクライアント:

該当なし

データの暗号化

Citrix Content Collaboration for Endpoint Management クライアントと *Citrix Files* モバイルクライアント:

AES-256 を使用してすべての格納データが暗号化され、SSL 3.0 と最低 128 ビットの暗号化を通して転送データが保護されます。

可用性

Citrix Content Collaboration for Endpoint Management クライアント:

Citrix Content Collaboration for Endpoint Management クライアントは、Endpoint Management の Advanced Edition および Enterprise Edition に含まれています。

Citrix Files モバイルクライアント:

Endpoint Management のすべてのエディションに、Citrix Files の機能がすべて含まれています。Endpoint Management と Citrix Files の全機能セットを統合することも、ストレージゾーンコネクタのみを統合することもできます。

Citrix Content Collaboration for Endpoint Management クライアントの統合と提供

Citrix Content Collaboration for Endpoint Management クライアントを統合して提供するには、以下の一般的な手順を実行します:

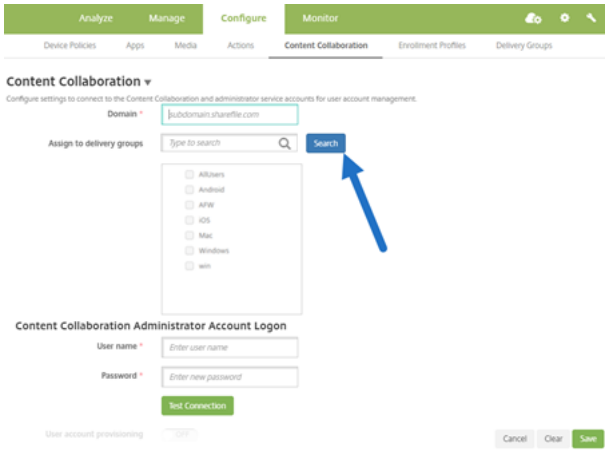
1. Endpoint Management を Citrix Files 用の SAML IdP として有効にし、Citrix Files クライアントから Citrix Files に SSO を提供する。そのためには、Endpoint Management で Citrix Files アカウント情報を設定する必要があります。詳しくは、「Endpoint Management で SSO 用の Citrix Files アカウント情報を設定するには」を参照してください。

   > 重要:
   >
   > Endpoint Management を、Citrix Files Web アプリや Citrix Files 同期クライアントなどの非 MDX Citrix Files クライアント用 SAML IdP として使用するには、追加の構成が必要です。詳しくは、Citrix Files サポートサイトの記事「
   >
   > Citrix Files（ShareFile）へのシングルサインオン（SSO）」を参照してください。この記事には、Endpoint Management 構成ガイドのダウンロードリンクが記載されています。

2. Citrix Files クライアントをダウンロードします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. Citrix Files クライアントを Endpoint Management に追加します。詳しくは、後述の「Citrix Files を Endpoint Management に追加するには」を参照してください。
4. 構成を検証します。詳しくは、後述の「Citrix Files クライアントを検証するには」を参照してください。



設定については、次の点に注意してください。

- ドメインは、クライアントに使用される Citrix Files サブドメインです。
- クライアントから Citrix Files に SSO でアクセスできるのは、選択したデリバリーグループ内のユーザーのみです。

  デリバリーグループのユーザーが Citrix Files のアカウントを保有していない場合、Endpoint Management に Citrix Files クライアントを追加すると、Endpoint Management によって Citrix Files にユーザーがプロビジョニングされます。
- Endpoint Management は、Citrix Files 管理者アカウントログオン情報を使用して、Citrix Files コントロールプレーンに SAML 設定を保存します。

> 重要:
>
> 構成で、Citrix Files クライアントから Citrix Files への SSO を有効にしても、ネットワーク共有または SharePoint のドキュメントライブラリに対してユーザーは認証されません。これらのコネクタデータソースにアクセスするには、ネットワーク共有または SharePoint サーバーが存在する Active Directory ドメインへの認証が必要になります。

Endpoint Management で **SSO** 用の **Citrix Files** アカウント情報を設定するには

Secure Hub から業務用モバイルアプリへの SSO を有効にするには、Endpoint Management コンソールで Citrix Files アカウントと Citrix Files 管理者サービスアカウント情報を指定します。この構成では、Endpoint Management は Citrix Files 用、業務用モバイルアプリクライアント用、Citrix Files クライアント用、および非 MDX Citrix Files クライアント用の SAML IdP として機能します。ユーザーが業務用モバイルアプリクライアントを起動すると、Secure Hub が Endpoint Management からユーザーの SAML トークンを取得し、Citrix Files クライアントに送信します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Endpoint Management コンソールで、［構成］> ［**Content Collaboration**］（**Citrix Files** の新しい名称）の順にクリックします。

Citrix Content Collaboration for Endpoint Management クライアントを **Endpoint Management** に追加するには

Citrix Content Collaboration for Endpoint Management クライアントを Endpoint Management に追加すると、Citrix Content Collaboration for Endpoint Management クライアントからコネクタデータソースへの SSO アクセスを有効にできます。これを実行するには、このセクションの説明に従って、ネットワークポリシーと優先 VPN モードポリシーを構成します。

前提条件

- Endpoint Management は、Citrix Files サブドメインに接続できる必要があります。接続をテストするには、Endpoint Management サーバーから Citrix Files サブドメインに ping を実行します。
- Citrix Files アカウントで構成したタイムゾーンと、Endpoint Management を実行するハイパーバイザーで構成したタイムゾーンが一致している必要があります。タイムゾーンが異なる場合、想定時間内に SAML トークンが Citrix Files に到達せず、SSO 要求が失敗することがあります。Endpoint Management 用 NTP サーバーを構成するには、Endpoint Management コマンドラインインターフェイスを使用します。

  > 注:
  >
  > Hyper-V ホストは、Linux VM 上の時刻を、UTC ではなく、ローカルタイムゾーンに設定します。

- 管理者として ShareFile アカウントにログオンし、［設定］>［管理設定］>［セキュリティ］>［ログインおよびセキュリティポリシー］>［シングルサインオン**/SAML 2.0** 構成］で SAML SSO 設定を確認します。
- Citrix Content Collaboration for Endpoint Management クライアントをダウンロードします。

手順:

1. Endpoint Management コンソールで、［構成］**>**［アプリ］に移動し、［追加］をクリックします。
2. ［**MDX**］をクリックします。
3. ［名前］を入力し、必要に応じて、アプリの ［説明］と ［アプリケーションカテゴリ］を入力します。
4. ［次へ］をクリックして、Citrix Content Collaboration for Endpoint Management クライアントの.mdx ファイルをアップロードします。
5. ［次へ］をクリックして、アプリの情報とポリシーを構成します。

   構成で、Citrix Content Collaboration for Endpoint Management クライアントから Citrix Files への SSO を有効にしても、ネットワーク共有または SharePoint のドキュメントライブラリに対してユーザーは認証されません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. Secure Hub のマイクロ VPN とストレージゾーンコントローラーの間で SSO を有効にするには、次のポリシー構成を実行します:

   - ネットワークアクセスポリシーを ［内部ネットワークへトンネル］に設定します。

     このモードでは、Citrix Content Collaboration for Endpoint Management クライアントからのネットワークトラフィックがすべて MDX フレームワークによりインターセプトされます。インターセプトされたネットワークトラフィックは、アプリ固有のマイクロ VPN により Citrix Gateway 経由でリダイレクトされます。

   - ［優先 VPN モード］ポリシーを ［トンネル**-Web SSO**］に設定します。

     このトンネルモードでは、MDX アプリからの SSL/HTTP トラフィックが MDX フレームワークによって終了され、ユーザーの内部接続に対して新しい接続が開始されます。このポリシー設定では、MDX フレームワークが、Web サーバーから発行された認証チャレンジを検出してそれに応答できます。

7. 必要に応じて、［承認］および［デリバリーグループ（DG）割り当て］に入力します。

Citrix Content Collaboration for Endpoint Management クライアントから Citrix Files に SSO でアクセスできるのは、選択したデリバリーグループ内のユーザーのみです。デリバリーグループのユーザーが Citrix Files のアカウントを保有していない場合、Endpoint Management に Citrix Content Collaboration for Endpoint Management クライアントを追加すると、Endpoint Management によって Citrix Files にユーザーがプロビジョニングされます。

Citrix Content Collaboration for Endpoint Management クライアントを検証するには

1. この記事で説明する構成を完了したら、Citrix Content Collaboration for Endpoint Management クライアントを起動します。Citrix Files がサインオンを要求することはありません。
2. Secure Mail で、メールを作成して Citrix Files から添付ファイルを追加します。Citrix Files ホームページが開きますが、サインオンを要求されることはありません。

> 注:
>
> - Citrix Files for XenMobile は、2023 年 7 月 1 日に製品終了（EOL）になりました。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

EOL と廃止予定のアプリ

July 27, 2023

以下のアプリは、製品終了（EOL）になったか、EOL ステータスに達する予定です。製品リリースが EOL に到達すると、製品のライセンス契約書の条件内で製品を使用できますが、利用できるサポートオプションは限られます。履

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

歴情報が Knowledge Center またはほかのオンラインリソースに表示されます。この文書は今後更新されず、そのままの状態で提供されます。製品のライフサイクルマイルストーンについて詳しくは、「製品マトリクス」を参照してください。

> 注:
>
> 段階的に廃止される Citrix Endpoint Management の機能に関する事前の通知については、「廃止」を参照してください。

Citrix Files for XenMobile（**MDX**）: Citrix Files for XenMobile は、2023 年 7 月 1 日に製品終了（EOL）になりました。

Apple App Store および Google Play で入手可能な Citrix Files を使用することをお勧めします。MAM SDK 対応です。

Secure Mail for Intune SDK（**iOS** および **Android**）: Secure Mail は 2023 年 4 月 30 日に EOL になりました。

Citrix Files for Intune: 2020 年 12 月 31 日に廃止対象になりました。

プラットフォーム機能を活用して、Android Enterprise（仕事用プロファイル使用）および iOS ユーザー登録を介して通常の Citrix Files アプリ（アプリストアで入手可能なもの）をコンテナ化するオプションを検討することをお勧めします。

ShareConnect: ShareConnect は、2020 年 6 月 30 日に EOL になりました。

Secure Notes: Secure Notes は 2018 年 12 月 31 日に EOL となりました。

Secure Notes と Secure Tasks の機能が必要な場合は、MDX ポリシーで保護できるサードパーティアプリである Notate for Citrix をお勧めします。

Outlook に Secure Notes と Secure Tasks の保存データがある場合、Notate でそのデータにアクセスできます。ShareFile（現 Citrix Files）に保存データがある場合、データは移行されません。

ユーザーは、使用中のプラットフォームのオペレーティングシステムが Secure Notes ユーザーインターフェイスのサポートを停止するまで、EOL 到達日以降も引き続き Secure Notes を実行できます。ただし、サポートされていない製品を使用することはお勧めしません。

Secure Tasks: Secure Tasks は 2018 年 12 月 31 日に EOL となりました。

Secure Forms: Secure Forms は 2018 年 3 月 31 日に EOL となりました。Citrix Files Platinum および Premium アカウントに含まれる Citrix ShareFile Workflows への移行をお勧めします。詳しくは、「Citrix ShareFile Workflows」を参照してください。

ScanDirect: ScanDirect は 2018 年 9 月 1 日に EOL となりました。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Office 365 アプリとのセキュアな対話式操作の許可

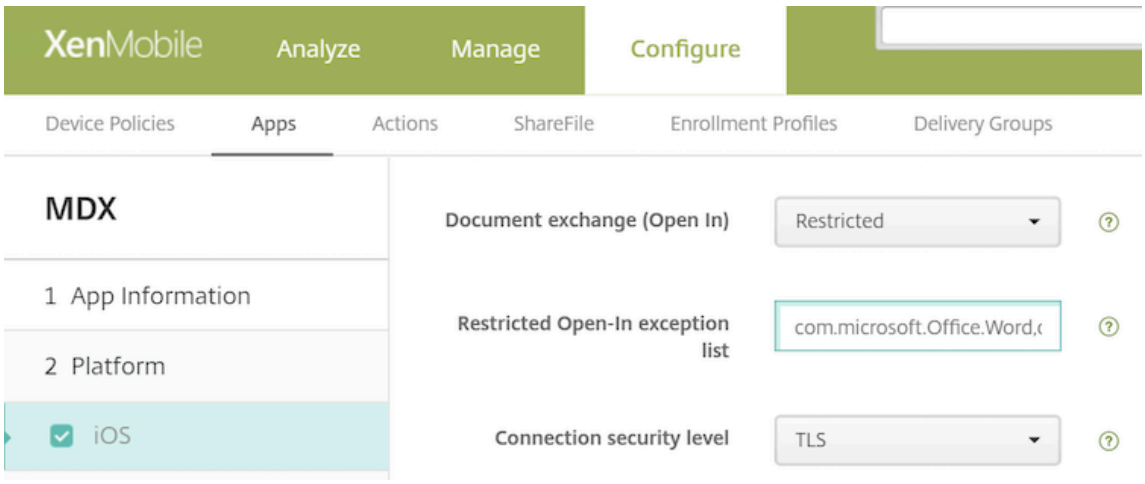
August 21, 2020

Citrix Secure Mail、Citrix Secure Web、および Citrix Files には、MDX コンテナを開放して Microsoft Office 365 アプリへドキュメントとデータを転送できるようにするオプションがあります。この機能は iOS および Android プラットフォーム向けであり、Endpoint Management コンソール上で Open-in ポリシーを介して管理します。

データを Microsoft アプリで開くと、MDX コンテナでの保護および暗号化が解除されます。この機能を有効化する前に、セキュリティ対する影響を検討してください。特に、データ損失の防止を重視する場合や、HIPAA やその他の厳格なコンプライアンス要件に従う必要がある場合は、コンテナを開放することの得失を検討する必要があります。

iOS で Office 365 を有効にする

1. Endpoint Management のダウンロードページから、Secure Mail アプリ、Secure Web アプリ、または Citrix Files アプリの最新バージョンをダウンロードします。
2. Endpoint Management コンソールにファイルをアップロードします。
3. ［ドキュメント交換（このアプリケーションで開く）］ポリシーに移動して、［制限］に設定します。［このアプリケーションで開く制限の例外 一覧］に、Microsoft Word、Excel、PowerPoint、OneNote、および Outlook が自動的に一覧表示されます。例: com.microsoft.Office.Word、com.microsoft.Office.Excel、com.microsoft.Office.Powerpoint、com.microsoft.onenote、com.microsoft.onenoteiPad、com.microsoft.Office.Outlook



MDM 登録では、iOS デバイス用の追加の制御機能を利用できます。

iTunes アプリを Endpoint Management コンソールにアップロードし、アプリをデバイスにプッシュすることができます。このオプションを使用する場合は、次のポリシーを ［オン］に設定します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- MDM プロファイルが削除されたらアプリを削除します
- アプリデータのバックアップを阻止します
- アプリを管理対象にする（選択的なワイプでは、アプリとすべてのデータが削除されることに注意してください）

Microsoft アプリからデバイス上の管理されていないアプリにドキュメントやデータが移動しないようにするには、Endpoint Management コンソールで ［構成］**>**［デバイス］**>**［制限］**>**［**iOS**］にアクセスして、［管理対象アプリから非管理対象アプリへのドキュメントの移動］と ［非管理対象アプリから管理対象アプリへのドキュメントの移動］を ［オフ］に設定します。

Android で **Office 365** を有効にする

1. Endpoint Management のダウンロードページから、Secure Mail アプリ、Secure Web アプリ、または Citrix Files アプリの最新バージョンをダウンロードします。
2. Endpoint Management コンソールにファイルをアップロードします。
3. ［ドキュメント交換（このアプリケーションで開く）］ポリシーにスクロールダウンして、［制限］を選択します。
4. このアプリケーションで開く制限の例外一覧 に、次のパッケージ ID を追加します。

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }
   ```

5. 他のアプリポリシーを通常どおりに構成し、アプリを保存します。

ユーザーは Secure Mail、Secure Web、または Citrix Files から自分のデバイスにファイルを保存して、そのファイルを Office 365 アプリで開く必要があります。

iOS と Android の両方で、ユーザーがデバイス上で開いて編集することができるファイルの種類は次のとおりです。

サポートされるファイル形式

サポートされるファイル形式については、Microsoft Office ドキュメント を参照してください。

© 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).