Citrix Endpoint Management

Contents

Citrix Endpoint Management

March 15, 2024

Citrix Endpoint Management は、モバイルデバイス管理（MDM）機能とモバイルアプリケーション管理（MAM）機能を提供する、エンドポイント管理ソリューションです。Citrix Endpoint Management では、デバイスポリシーとアプリポリシーを管理し、アプリをユーザーに配信します。ID、デバイス、アプリ、データ、ネットワークに厳重なセキュリティを用いて、ビジネス情報が保護された状態を保ちます。

Citrix とお客様が管理する分野

Citrix Cloud Operations が、さまざまなインフラストラクチャおよび監視タスクを処理します。そのため、管理者はユーザーエクスペリエンスやデバイス、アプリ、ポリシーの管理に集中できます。

Citrix が管理する分野:

- Citrix Endpoint Management サーバーノード
- NetScaler Gateway（サービスまたはオンプレミス）の初期の統合と構成
- NetScaler Gateway ロードバランサー
- データベース
- Cloud Connector ソフトウェアの構成
- ShareFile との SAML 認証の統合
- Citrix Endpoint Management のサイト監視: インスタンス、データベース、エンタープライズ接続（LDAP）、VPN トンネル（該当する場合）、パブリック SSL 証明書、Citrix Endpoint Management ライセンス管理

顧客が管理する分野:

- NetScaler Gateway（オンプレミス）の管理と更新
- Cloud Connector と Gateway Connector（Citrix Gateway サービス用）がインストールされているマシン
- LDAP/Active Directory
- DNS
- ShareFile: ShareFile の初期構成、オンプレミス Storage Zone Controller のインストール、Citrix Files の更新
- Citrix Endpoint Management の構成: デバイス、ポリシー、アプリ、デリバリーグループ、操作、クライアント証明書

Microsoft Endpoint Manager との統合

Citrix Endpoint Management と Microsoft Endpoint Manager（MEM）が統合されました。この統合により、Citrix Endpoint Management マイクロ VPN の価値が Microsoft Edge ブラウザーなどの Microsoft Intune 対

応アプリに追加されます。統合により、次のことが可能になります

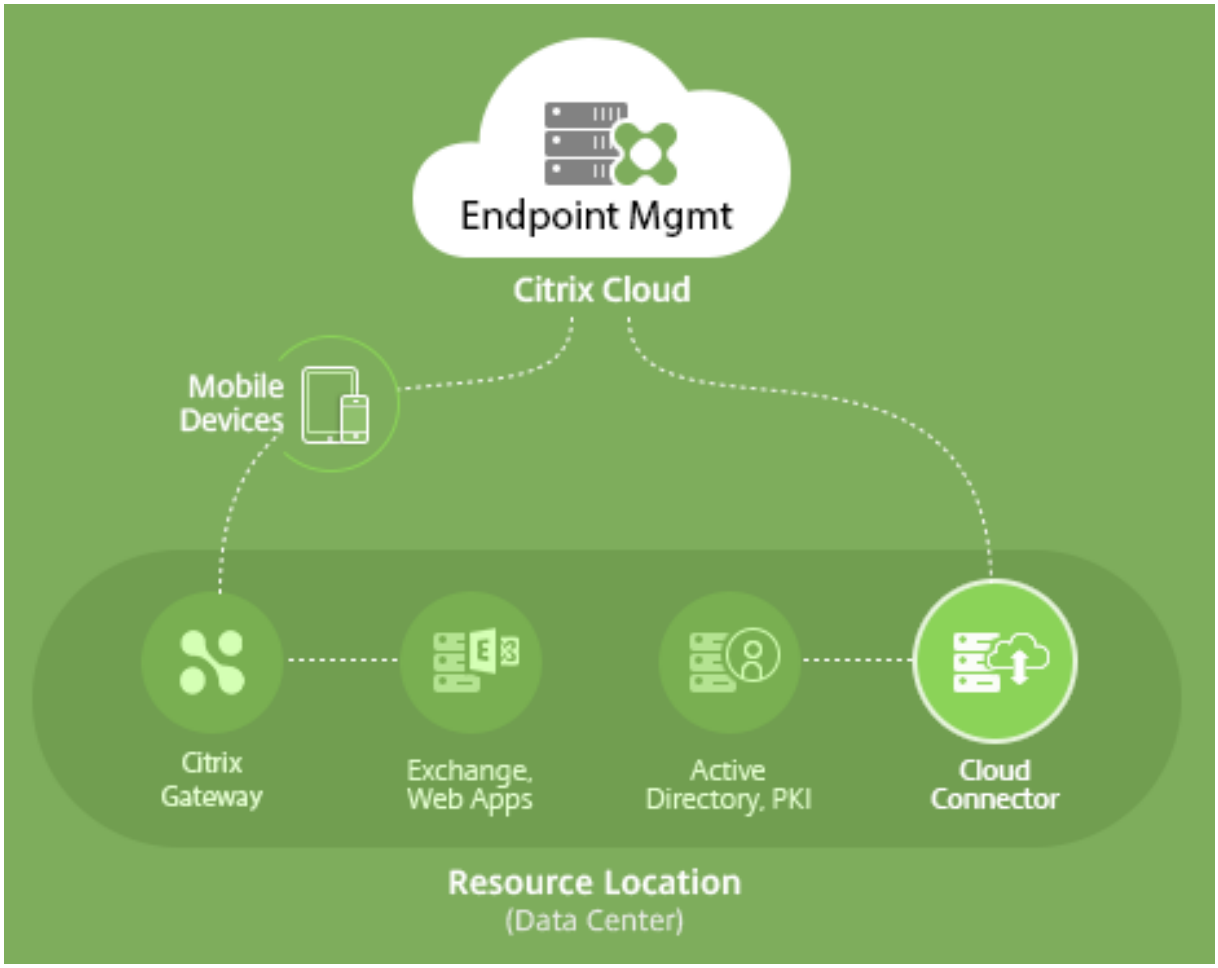
- Azure AD を使用した条件付きアクセスで Office 365 アプリケーションを保護します。詳しくは、「Azure AD 条件付きアクセスとの統合」を参照してください。
- Intune と Citrix で顧客独自のビジネスアプリをラップし、Intune のモバイルアプリ管理（MAM）コンテナ内でマイクロ VPN 機能を利用できます。
- Office 365 アプリ、基幹業務アプリ、Citrix Secure Mail を 1 つのコンテナで管理し配信します。この管理方法は、究極のセキュリティと生産性を提供します。たとえば、次の作業を行えます。
  - 個別のデバイスまたはオペレーティングシステムのブロック
  - デバイス、ユーザー、またはユーザーグループに基づいた ActiveSync ポリシーのカスタマイズ
  - デバイスレベルでの検疫
  - 個別の接続またはデバイスの監視
  - 資格情報およびデータキャッシュのセキュリティ上のリスクの回避

デバイスを管理するには、Citrix Endpoint Management MDM+MAM または Intune MDM を使用します。詳しくは、「Citrix Endpoint Management と Microsoft Endpoint Manager との統合」を参照してください。

Cloud Connector とリソースの場所

Citrix Endpoint Management には、Cloud Connector で接続します。Cloud Connector は、Citrix Cloud とリソースの場所の間で通信チャネルとして機能します。Cloud Connector によって、VPN や IPsec トンネルなどの複雑なネットワークやインフラストラクチャを構成せずにクラウドを管理できます。

リソースの場所には、利用者にサービスを提供するために必要なリソースが含まれます。Citrix Endpoint Management の場合、リソースの場所は顧客の NetScaler Gateway、LDAP、DNS、PKI サーバーです。



Cloud Connector とリソースの場所について詳しくは、「Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management を開始する

> ヒント:
>
> XenMobile Migration Service
>
> XenMobile Server をオンプレミスで使用している場合、XenMobile Migration Service によって Citrix Endpoint Management の使用を開始することができます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。
>
> 詳しくは、地域の Citrix 営業担当者、システムエンジニア、または Citrix パートナーにお問い合わせください。
>
> 移行サービスについて詳しくは、「Citrix Endpoint Management サービスに移行すべき 3 つの理由」を参照してください。
>
> Citrix Endpoint Management に移行する理由、方法、メリットについては、CEM 移行サービスコースカタ

> ログ（英語）にアクセスするか、『Citrix Endpoint Management（CEM）移行サービス（英語）』ガイドを参照してください。

Citrix Endpoint Management の評価または購入時には、Citrix Endpoint Management 運用チームが継続的に導入支援を提供します。運用チームはまた、コアの Citrix Endpoint Management サービスが正しく実行され、正しく構成されていることを確認するためにお客様とのコミュニケーションを実施します。この図は、オンボードの手順を示しています。

Citrix アカウントを新規登録して Citrix Endpoint Management のトライアルをリクエストするには、Citrix の営業担当者にお問い合わせください。準備が整い次第、https://onboarding.cloud.comにアクセスします。

Citrix Endpoint Management のオンボードと構成の概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

使用開始前に、さらに詳しい内容を知りたい場合、以下のリソースを参照してください。

Citrix Endpoint Management のドキュメント：オンボードから初期構成、高度な構成まで、Citrix Endpoint Management に関するドキュメントを提供しています。「新機能」のページでは、新しい機能や修正について説明しています。新しいリリースに関する内容が利用可能になり次第、Citrix からお知らせします。

『**Citrix Endpoint Management Onboarding Handbook**』：Citrix Endpoint Management に関して入手できる情報がすべて集約されているため、Citrix Endpoint Management の有効化とオンボードをスムーズに進めることができます。このドキュメントを使用して、内部プロセスの変更を記録し、高度な機能設計を文書化することができます。

「**Citrix Endpoint Management** の展開」：Citrix Endpoint Management の展開を計画する場合、多くの検討事項があります。ここには、Citrix Endpoint Management 環境の推奨事項、よくある質問、ユースケースが記載されています。

SalesIQ：Citrix パートナー向けのその他のリソース。

次の手順

Citrix Endpoint Management のオンボード処理について詳しくは、「オンボードとリソースのセットアップ」を参照してください。

オンボードを完了したら、「デバイス登録およびリソース提供の準備」を参照してください。

廃止される項目の情報

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 Endpoint Management サポート

Citrix Endpoint Management コンソールでサポートされるアクセス方法の関連情報およびツールについて詳しくは、「モニターとサポート」を参照してください。

Citrix Endpoint Management リリースのローリング更新は、約 2 週間間隔で提供されます。このプロセスは、お客様向けのわかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々にお客様の環境に適用されます。更新を段階的に配信することで、製品の品質を確保し、可用性を最大化しています。

Citrix Endpoint Management Cloud 運用チームから Citrix Endpoint Management の更新やメールなどを直接受け取ることができます。これらの更新は、新機能、既知の問題、解決された問題などを最新の状態に保ちます。

Citrix Cloud 運用チームは、Cloud Operations チームによる最新の Citrix Endpoint Management Rolling Patch を使用して、Citrix Endpoint Management 環境を維持します。Rolling Patch の前に必要な特定のパッチまたは修正プログラムを入手するには、Citrix テクニカルサポートにお問い合わせください。

お使いの環境に問題がある場合は、Citrix テクニカルサポートまたは Citrix アカウントチームにお問い合わせください。モバイルデバイスの登録、Citrix Endpoint Management コンソールアクセス、または Citrix Secure Mail の問題なども含まれます。

クラウドまたは Citrix Endpoint Management で NetScaler Gateway を統合または変更する必要がある場合は、Citrix テクニカルサポート経由でリクエストを送信してください。

以下は、変更のリクエスト例です:

- クラウドで Citrix Files と NetScaler Gateway を統合する
- NetScaler Gateway の認証の種類を変更する
- 顧客のデータセンターのリソースに対する接続を検証する
- マイクロ VPN の分割トンネル構成を変更する
- サーバー構成の一部変更により Citrix Endpoint Management コンポーネントを再起動する

サービスレベルアグリーメント

Citrix Endpoint Management は、業界のベストプラクティスを使用して、クラウドの規模と高度なサービス可用性を実現するように設計されています。

Citrix Cloud サービスの可用性に関する Citrix の目標について詳しくは、「サービスレベルアグリーメント」を参照してください。

新機能

March 15, 2024

Citrix は、Citrix Endpoint Management をご使用のお客様に、新機能と製品の更新をいち早くお届けするよう取り組んでいます。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。

- Citrix Endpoint Management のローリング更新は、約 2 週間間隔で提供されます。
- これらの更新によって、インスタンスまたはデバイスユーザーのダウンタイムが発生することはありません。
- すべてのリリースに新機能があるわけではなく、一部の更新に修正とパフォーマンスの強化が含まれています。

このプロセスは、お客様向けのわかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々にお客様の環境に適用されます。段階的に更新することによって、製品の品質を確認し、最大限の可用性を提供しています。

Citrix Endpoint Management Cloud 運用チームから Citrix Endpoint Management の更新やメールなどを直接受け取ることができます。これらの更新は、新機能、既知の問題、解決された問題などを最新の状態に保ちます。

クラウドの規模とサービスの可用性などについて詳しくは、Citrix Endpoint Management の「サービスレベルアグリーメント」を参照してください。サービスの中断および定期メンテナンスを監視するには、Service Health Dashboardを参照してください。

Citrix ADC で廃止のクラシックポリシーの継続的なサポート

Citrix は最近、Citrix ADC 12.0 ビルド 56.20 以降の一部のクラシックポリシーベースの機能が廃止されたことを発表しました。この Citrix ADC の機能廃止は、既存の Citrix Endpoint Management と NetScaler Gateway の統合には影響しません。Citrix Endpoint Management は引き続きクラシックポリシーをサポートしており、アクションは不要です。

エンドポイントの **iOS 14.5** へのアップグレード準備

エンドポイントを iOS 14.5 にアップグレードする前に、Citrix ではアプリのクラッシュを軽減するために以下を実行することをお勧めします:

- Citrix Secure Mail および Citrix Secure Web を 21.2.X 以降にアップグレードします。「MDX またはエンタープライズアプリのアップグレード」を参照してください。
- MDX Toolkit を使用する場合は、すべてのサードパーティ iOS アプリケーションを MDX Toolkit 21.3.X 以降でラップし、Citrix Endpoint Management コンソールでそれらのアプリケーションをアップグレードします。MDX Toolkit のダウンロードページで最新バージョンを確認してください。

オンプレミスの **Citrix ADC** を **13.0-64.35** 以降にアップグレードする前に

オンプレミスバージョンの Citrix ADC を使用し、バージョン 13.0-64.35 以降にアップグレードする場合：「Citrix Endpoint Management 20.10.1 の既知の問題」で説明されている回避策を実行します。

Citrix Endpoint Management 24.1.0

また、複数の問題にも対応しているため、パフォーマンスや安定性が総合的に向上しています。新機能は追加されていません。

Citrix Endpoint Management 23.12.0

Android の **802.1x** 設定に新しい必須フィールド「ドメイン」を追加：認証の種類が［**802.1x EAP**］の **Android Enterprise** プラットフォームのネットワークポリシー設定ページに、新しい［ドメイン］フィールドが追加されました。詳しくは、「Android の 802.1x 設定」を参照してください。

Citrix Endpoint Management 23.9.0

> 注：
>
> Citrix Endpoint Management 23.9.0 のドキュメントの更新は、製品リリースのロールバックとともにロールバックされました。

現在の既知の問題

Citrix Endpoint Management 22.6.0 の既知の問題

3 つのログタイプ（[デバッグ]、[管理者監査]、[ユーザー監査]）を ［トラブルシューティングとサポート］**>** ［ログ］ですべて選択してダウンロードすることが、断続的にできなくなっています。デバッグログのみがダウンロードされています。回避策として、各ログを個別にダウンロードするか、シークレットモードで Web ブラウザーを開いて、3 つのチェックボックスすべてにマークを付けてすべてのログをダウンロードしてください。[CXM-105334]

Android Enterprise で Web リンクを作成するときに、アイコンを使用してアプリを保存しようとするとエラーが発生します。これは Google サービスの問題です。回避策として、アイコンをアップロードせずにアプリを保存してください。[CXM-105395]

Samsung Knox/SAFE ポリシーは廃止後も登録済みデバイスでアクティブのままであり、無効にしたり構成したりすることはできません。この問題を回避するには、デバイスの登録を解除してから再登録します。[CXM-104303]

Citrix Endpoint Management 22.4.0 の既知の問題

［監視］タブで登録済みの Active Directory ユーザーを検索すると、そのユーザーの登録済みデバイスが表示されません。［管理］**>**［デバイス］でユーザーに割り当てられているポリシーとアプリを表示して、すべてのセキュリティ操作を実行することはできます。iOS と Android の両方の登録済みデバイスが影響を受けます。[CXM-104283]

Google サービスの問題により、Android Enterprise を使用してプライベートアプリを公開できません。問題が解決したら、ドキュメントを更新します。[CXM-103690]

Citrix Endpoint Management 21.12.0 の既知の問題

Citrix Cloud でフルアクセス権限を持つ管理ユーザーは、Citrix Cloud ベースの RBAC に移行した後、移行前にカスタム権限を持っていた場合でも、CEM でフルアクセス権限を取得します。回避策として、Citrix Cloud の［ID およびアクセス管理］ページで、目的のアクセス権限で管理者権限を更新できます。[CXM-102765]

2018 年より前に使用を開始したお客様には、コンソールへのローカル管理者アクセス権があります。ローカルユーザーを追加または編集する権限を持つ CEM 管理者ユーザーは、Citrix Cloud でローカルユーザーを追加または編集することができます。これには、ローカルユーザーのパスワードの変更が含まれます。この問題を解決するには、サポートに連絡して、コンソールへの直接のローカル管理者アクセスをブロックし、Citrix Cloud 管理者アクセスのみを許可するようにできます。[CXM-102780]

Citrix Endpoint Management 21.11.0 の既知の問題

MAM にのみ登録されている iOS デバイスでは、エンタープライズアプリのインストールに失敗します。[CXM-101852]

Citrix Endpoint Management サーバーが 21.11.0 にアップグレードされると、Android Enterprise の管理対象アプリの自動更新ポリシーをデバイスに適用できません。ポリシーの失敗は、デバイスのアプリの更新に影響します。回避策として、管理者はポリシーを編集および保存して、デフォルト値を更新できます。[CXM-102446]

Citrix Endpoint Management 21.10.0 の既知の問題

VPN デバイスポリシーは、管理対象の Windows 11 デバイスでは正しく機能しません。Citrix はこの問題を Microsoft 社に報告し、Microsoft 社と協力して解決に取り組んでいます。進捗状況については、随時最新情報を提供します。

Citrix Endpoint Management 21.9.1 の既知の問題

企業所有のデバイスモードで仕事用プロファイルに登録されている Android デバイスの場合：個人プロファイルでアプリをインストールまたは検索できないというエラーがユーザーの画面に表示されることがあります。これらのエラーが表示された場合は、Google Play ストアアプリを更新して再試行します。[CXM-100678]

Citrix Endpoint Management 21.5.0 の既知の問題

次の場合、ユーザーは Azure Active Directory（Azure AD）に対して認証できません：

1. Azure AD 資格情報を使用して、デバイスを Citrix Endpoint Management に登録する。
2. Office 365 アプリを起動して、Azure AD 登録を完了する。
3. Microsoft Authenticator アプリからアカウントを削除する。
4. Office 365 アプリを起動し、サインアウトする。

この問題を回避するには、Citrix Endpoint Management からデバイスの登録を解除し、再登録します。[CXM-90235]

Citrix Endpoint Management 21.4.0 の既知の問題

再登録しようとしているユーザーが、デバイスに最初に登録したユーザーとは異なる Azure Active Directory ユーザーである場合、iOS デバイスでの再登録は失敗します。この問題を回避するには、再登録する前に、デバイスの Microsoft Authenticator アプリから元のユーザーの登録を解除してください。[CXM-90218]

Citrix Endpoint Management 21.2.0 の既知の問題

Android Enterprise の MDX アプリとして Citrix Secure Web を追加すると、管理対象 Google Play はアプリ識別子を使用してアプリを見つけることができません。アプリ識別子の代わりに「Citrix Secure Web」を検索すると、管理対象 Google Play はアプリを見つけることができます。この問題は Google のバグです。[CXM-91991]

SSL リスナー証明書のインポートが失敗する可能性があります。CTX-297153の手順を実行して、証明書キーストアを再パッケージ化します。[XMHELP-3346]

Citrix Endpoint Management 20.10.1 の既知の問題

オンプレミスの Citrix ADC を 13.0-64.35 以降にアップグレードし、Citrix Endpoint Management がワークスペースに対応していない場合：Citrix Files または ShareFile ドメイン URL にシングルサインオンすると、エラーが発生します。ユーザーはサインインできません。このエラーは、［会社の従業員のサインイン］オプションが設定されたブラウザーでのみ発生します。

この問題を回避するには、NetScaler Gateway の ADC CLI から次のコマンドを実行して（まだ実行していない場合）、グローバル SSO を有効にします：

```
set vpn parameter SSO ON

bind vpn vs <vsName> -portalTheme X1
```

詳しくは、次のトピックを参照してください：

- Citrix ADC リリース

- 影響を受ける SSO 構成

この回避策を完了すると、ユーザーは、［会社の従業員のサインイン］オプションを備えた Web ブラウザーで、SSO を使用して Citrix Files または ShareFile ドメイン URL の認証を実行できます。[CXM-88400]

Citrix Endpoint Management 20.2.1 の既知の問題

Citrix Endpoint Management コンソールで ShareFile URL を使用して ShareFile を設定した後、［接続のテスト］ボタンをクリックすると、エラーになります。この問題を解決するには、ShareFile の多要素認証を無効にしてください。この問題とその回避策について詳しくは、このサポートページを参照してください。[CXM-79240]

Citrix Endpoint Management 20.1.0 の既知の問題

Citrix Cloud のライブラリにユーザーを追加すると、Citrix Endpoint Management は成功を報告しますが、ユーザーは追加されません。[CXM-73726]

Citrix Endpoint Management 19.11.0 の既知の問題

MDX アプリとパブリックアプリはコンソールから削除できません。この問題を回避するには、削除するアプリを選択して ［編集］をクリックします。［**Android Enterprise**］の選択を解除して、プラットフォーム一覧から他のプラットフォームを選択します。アプリを保存した後、アプリを削除できます。[CXM-74468]

Citrix Endpoint Management 19.5.0 の既知の問題

Citrix Ready ワークスペースハブデバイスを登録するときには、登録の失敗を避けるために、Ethernet（eth0）MAC アドレスを許可リストに定義します。[CXM-43141]

Citrix Endpoint Management 19.4.1 の既知の問題

Windows GPO デバイスポリシーのオプションをタブ移動すると、ラジオボタンとチェックボックスはスキップされます。[CXM-58277]

Citrix Endpoint Management 19.2.1 の既知の問題

Google 管理コンソールで Android Enterprise エンタープライズを削除して登録を解除すると、再登録できないことがあります。Android Enterprise エンタープライズの登録を解除する場合、「[Android Enterprise エンタープ

ライズの登録を解除する]」(/en-us/citrix-endpoint-management/device-management/android/android-enterprise.html#unenroll-an-android-enterprise-enterprise) の手順に従って、常に Citrix Endpoint Management コンソールを使用してください。Google Workspace ユーザーは、「Android Enterprise エンタープライズの登録解除」の手順に従ってください。[CXM-62709] [CXM-62950]

Citrix Endpoint Management 19.2.0 の既知の問題

Citrix Endpoint Management 10.18.3 でパブリックストアアプリを作成した場合：iPad アプリ設定ページでアプリを検索せずに ［戻る］をクリックしてから ［次へ］をクリックすると、次の問題が発生します。ナビゲーションボタンが反応せず、アプリを検索できません。この問題は、iOS または Android の両方でパブリックストアアプリを作成するときに発生します。[CXM-46820]

Citrix Endpoint Management 10.19.1 の既知の問題

［設定］**>** ［**Android Enterprise**］ページで登録プロセスを完了すると、次のエラーメッセージが表示されます：`A configuration error occurred. Please try again`。エラーメッセージを閉じると、Android Enterprise 構成は保存されますが、［**Android Enterprise** の有効化］は ［オフ］になります。この問題を回避するには、アプリのカテゴリの数を 30 以下に減らします。[CXM-60899]

Citrix Endpoint Management 10.18.5 の既知の問題

Chrome アプリを Chrome OS デバイスの必須アプリとして構成した場合：ユーザーはログオフしてから再度ログインしないとこのアプリをインストールできなくなる場合があります。このサードパーティの問題は、Google バグ ID #76022819 です。[CXM-48060]

Citrix Endpoint Management 10.18.3 の既知の問題

デバイスが登録されている Citrix Cloud 管理者を削除した後：管理者が Citrix Secure Hub アプリまたは Self-Help Portal から再度ログインするまで、Citrix Endpoint Management は Citrix Endpoint Management コンソールのユーザー役割を更新しません。[CXM-45730]

Citrix Endpoint Management 10.7.4 の既知の問題

Azure Active Directory へのシングルサインオン（SSO）に Citrix ID プロバイダーを使用するように Citrix Endpoint Management を構成した場合：Citrix Endpoint Management 管理者またはユーザーが **Azure Active Directory** のサインイン画面にリダイレクトされると、画面に「Citrix Secure Hub のサインインページ」というメッセージが表示されます。正しいメッセージは、「Citrix Endpoint Management コンソールのサインインページ」です。[CXM-42309]

サードパーティ製品についての通知

April 27, 2020

Citrix Endpoint Management には、次のドキュメントで定義された条件の下でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

Citrix Endpoint Management のサードパーティ製品についての通知

廃止

November 29, 2023

以下の告知は、お客様が適宜ビジネス上の決定を下せるように、段階的に廃止される Citrix Endpoint Management の機能について前もってお知らせするためのものです。Citrix ではお客様の使用状況とフィードバックをチェックして、各プラットフォーム、Citrix 製品、機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。製品ライフサイクルサポートについて詳しくは、「製品ライフサイクルサポートポリシー」の記事を参照してください。

> 重要:
>
> Citrix Endpoint Management Analyzer ツールをご利用いただきありがとうございます。Citrix が提供する製品のリリース間隔は、頻度が高く、安定しているため、このツールを使用する必要がなくなりました。そのため、このサービスの提供を 2023 年 3 月 31 日をもって停止することを決定しました。代わりに、Citrix Endpoint Management コンソールまたは Citrix NetScaler Gateway で利用できる接続性チェックを使用することをお勧めします。詳しくは、「接続確認」を参照してください。

廃止と削除

廃止または削除される Citrix Endpoint Management の機能を以下の一覧に示します。

廃止されたアイテムはすぐには削除されません。Citrix は今後のリリースで、廃止が発表されたアイテムが削除されるまではサポートを継続します。

削除アイテムは、Citrix Endpoint Management で削除されたか、サポートされなくなりました。

製品終了となった業務用モバイルアプリについては、「EOL と廃止予定のアプリ」を参照してください。

アイテム	説明	廃止の発表	削除	代替手段
Citrix Endpoint Management Government 製品	Citrix Endpoint Management Government 製品で廃止されたサポート。	2022 年 1 月	2022 年 7 月	Citrix Endpoint Management Standard Edition
SafetyNet Attestation API	Google の発表によると、Android SafetyNet Attestation のサポートは廃止されました。	2023 年 7 月	2023 年 11 月	Play Integrity API
Chrome OS	Chrome OS のサポートは廃止されました。	2022 年 7 月	2023 年 5 月	代替はありません
tvOS	tvOS のサポートは廃止されました。	2022 年 7 月	2023 年 5 月	代替はありません
Windows Information Protection（WIP）	Microsoft の発表によると、Windows Information Protection のサポートは廃止されました。	2022 年 8 月	2022 年 10 月	代替はありません
Citrix Endpoint Management アナライザー	Citrix Endpoint Management Analyzer ツールのサポートは廃止されました。	2022 年 7 月	予定：2023 年 3 月 31 日	代替はありません
ワークスペースハブのデバイス管理	Citrix Ready ワークスペースハブのサポートは廃止されました。	2022 年 1 月	2022 年 6 月	代替はありません

アイテム	説明	廃止の発表	削除	代替手段
ビジネス向け Microsoft ストア	ビジネス向け Microsoft Store のサポートは廃止されました。Microsoft は、このプラットフォームをサポートしなくなりました。詳しくは、Microsoft 社のドキュメントを参照してください。	2021 年 7 月	予定：2023 年 3 月	代替はありません
Samsung SAFE	Samsung SAFE のサポートは廃止されました。	2022 年 1 月	2022 年 6 月	Android Enterprise を使用してください。
Zebra のカスタム XML	Zebra デバイスでのカスタム XML のサポートは廃止されました。	2022 年 1 月	2022 年 6 月	Android Enterprise 管理対象の構成を使用してください。
PKI ID：汎用、Symantec PKI、DigiCert、および Entrust	汎用、DigiCert 管理、および Entrust アダプターの PKI エンティティのサポート廃止。	2021 年 6 月	2022 年 1 月	代替はありません
Android for Workspace	Android for Workspace のサポート廃止	2022 年 1 月	2022 年 4 月	代替はありません
キャリア SMS ゲートウェイ	Nexmo SMS ゲートウェイ通知のサポートは廃止されました	2022 年 1 月	2022 年 4 月	SMTP サーバー通知を使用する
モバイルサービスプロバイダー（MSP）	Blackberry およびその他の Exchange ActiveSync デバイスにクエリを実行して操作を発行する MSP インターフェイスのサポートは廃止されました	2022 年 1 月	2022 年 4 月	代替はありません

アイテム	説明	廃止の発表	削除	代替手段
MDX Toolkit	MDX Toolkit のサポートが廃止され、モバイルアプリケーション管理（MAM）SDK に置き換えられます。移行期間中、MDX でラップされたアプリと MAM SDK で開発したアプリの両方を使用できます。	2020 年 3 月	2023 年 7 月	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 を使用してください。
RBAC の役割 - 共有デバイスの登録者と COSU（特定業務専用コーポレート所有端末）デバイスの登録者	共有デバイス登録者と COSU デバイス登録者の事前定義された RBAC（役割ベースのアクセス制御）設定のサポートを終了	2021 年 7 月	2021 年 12 月	Apple Business Manager または Apple School Managerを使用して iOS デバイスを構成します。登録プロファイルを使用して、Android COSU（専用）デバイスを構成します。
[Wi-Fi センサーホットスポットへの自動接続を許可］の Windows デバイスでの制限	Windows 10 デバイスで［Wi-Fi センサーホットスポットへの自動接続を許可］に関するサポートを削除します。Windows 10 はこの機能をサポートしなくなりました。詳しくは、Microsoft 社のドキュメントを参照してください。	2021 年 10 月	2022 年 2 月	代替はありません
MDX：代替ゲートウェイサーバー	iOS および Android デバイスの拡張認証を終了します。	2020 年 3 月	2021 年 9 月	代替はありません

アイテム	説明	廃止の発表	削除	代替手段
MDX：マイクロ VPN（完全トンネルモード）	iOS および Android デバイス向けの完全仮想プライベートネットワーク（VPN）トンネルが廃止されます。	2020 年 3 月	2021 年 9 月	MAM SDK の Web SSO モードを使用するか、Citrix SSO の接続の種類で Per-App VPN ポリシーを作成します。
MDX：PAC ファイルのサポート	を iOS および Android デバイスの完全 VPN トンネル展開で、Proxy Automatic Configuration（PAC）ファイルのサポートが廃止されます。	2020 年 3 月	2021 年 9 月	Citrix Gateway を使用してプロキシサーバー経由で接続し、内部ネットワークにアクセスします。
MDX 共有デバイスのサポート	MDX アプリ向けの共有デバイスのサポートが廃止されます。	2020 年 3 月	2021 年 9 月	Android Enterprise の場合、専用デバイスとして登録された共有デバイスを使用します。iOS の場合は、Apple School Manager または GroundControl を使用します。
Android - Sony	Android Sony デバイスおよび Sony 固有のポリシーに対するサポートは廃止されました。	2021 年 1 月	2022 年 2 月	Android Enterprise を使用してください
Android - HTC	Android HTC デバイスおよび HTC 固有のポリシーに対するサポートは廃止されました。	2021 年 1 月	2022 年 2 月	Android Enterprise を使用してください

アイテム	説明	廃止の発表	削除	代替手段
Android - Amazon	Android Amazon デバイスのポリシー、および Amazon 固有のポリシーのサポートは廃止されました。	2021 年 1 月	2022 年 2 月	Android Enterprise を使用してください
Knox Mobile Enrollment（従来の DA）	すべての Android バージョンで、従来のデバイス管理モードでの Knox Mobile Enrollment（KME）のサポートが終了しました。	2021 年 5 月 4 日	2021 年 9 月	KME を使用して Android Enterprise モードに登録します。Android 8、9、10、11 は Android Enterprise をサポートしています。
高セキュリティ登録モード	高セキュリティ登録セキュリティモードで登録招待を生成するためのサポートが終了しました。	2021 年 7 月	2022 年 2 月	サポートされている登録セキュリティモードの一覧については、「登録招待」を参照してください。
派生資格情報	派生資格情報および Citrix Derived Credential Manager アプリのサポートの廃止。	2021 年 3 月	2021 年 12 月	iOS でサポートされている認証の種類の一覧については、「iOS」を参照してください。

アイテム	説明	廃止の発表	削除	代替手段
APNs 送信ポート	APNs の従来のバイナリプロトコルに対する Apple のサポートは、2021 年 3 月 31 日で終了します。代わりに HTTP/2 ベースの APN プロバイダー API の使用をお勧めします。この変更の一部として、`*.push.apple.com`に APNs 通知を送信するために使用されるポート 2195 および 2196 のサポートが廃止されます。	2020 年 10 月	2021 年 3 月	代わりにポート 443 を使用してください。「ネットワークとファイアウォールの要件」を参照してください。
MDX Service	MDX Service のサポートが廃止され、モバイルアプリケーション管理（MAM）SDK に置き換えられます。移行期間中、MDX Toolkit を使用して MDX でラップしたアプリと、MAM SDK で開発したアプリの両方を使用できます。	2020 年 3 月	2021 年 9 月	エンタープライズアプリケーションのラップを続行するには、MDX Toolkit を使用してください。
Self Help Portal での登録招待の設定	Self Help Portal から登録招待を生成するためのユーザーのサポートが終了しました。	2021 年 7 月	2021 年 7 月	管理者に連絡して、Citrix Endpoint Management コンソールで登録招待を生成してください。

アイテム	説明	廃止の発表	削除	代替手段
登録招待の設定	デバイスの IMEI、シリアル番号、および UDID を使用した登録招待の作成のサポート廃止。	2021 年 4 月	2021 年 7 月	登録招待状を作成するときは、Citrix Endpoint Management コンソールの ［管理］ > ［登録招待］ で使用可能な設定を構成します。
証明書ベースの認証署名アルゴリズム（非 FIPS および弱い暗号）	次の署名アルゴリズムのサポートが終了しました: SHA1withRSA、SHA224withRSA、SHA1withECDSA、SHA224withECDSA、SHA1withDSA、RIPEMD160withRSA、RIPEMD128withRSA、RIPEMD256withRSA。	2020 年 5 月	2021 年 6 月	Citrix Endpoint Management コンソール（［設定］ > ［資格情報プロバイダー］ > ［証明書署名要求］）で資格情報プロバイダーの CSR（証明書の署名要求）を作成するときは、より強い暗号を選択します。
Android 7.x および iOS 12.x 向けの Citrix モバイルアプリおよび Workspace アプリ	Android 7.x および iOS 12.x バージョンの Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web、Citrix Workspace アプリのサポートは廃止されました。	2021 年 4 月	2021 年 6 月	最低限、主要オペレーティングシステムプラットフォームの最新バージョンおよび 1 つ前のバージョンを使用してください。古いデバイスは登録されたまま残ります。ただし、Citrix は従来のデバイスをテストまたはサポートしません。

アイテム	説明	廃止の発表	削除	代替手段
Android の RSA ソフトウェアトークンのサポート	Citrix Secure Hub for Android への RSA ソフトウェアトークンの直接インポートのサポートは廃止されました。	2021 年 1 月	2021 年 2 月	Google Play で利用可能な RSA セキュア ID アプリ内に RSA ソフトウェアトークンをインポートした後、Citrix Gateway 認証にトークンを使用できます。
Internet Explorer 11	Citrix Endpoint Management コンソールでの Internet Explorer 使用サポートは廃止されました。	2021 年 1 月	2021 年 1 月	次の Web ブラウザーの最新バージョンを使用してください: Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
Citrix Endpoint Management アナライザーでのゲートウェイ構成チェック	ゲートウェイ構成チェックオプションのサポートは廃止されました。	2020 年 11 月	2020 年 11 月	アナライザーの Citrix Insight Services チェックを使用して、Citrix ADC 構成で Citrix Endpoint Management の展開の準備ができているかどうかを確認します。

アイテム	説明	廃止の発表	削除	代替手段
Android Enterprise デバイスの従来のデバイス管理モード用に公開されたアプリ	従来の DA プラットフォーム用に公開されたアプリの Android Enterprise 登録済みデバイスへの配信は終了しました。	2020 年 10 月	2020 年 11 月	Android Enterprise デバイスの場合、Android Enterprise プラットフォーム用のアプリを公開します。従来の DA アプリを DA モードのデバイスに引き続き公開するには、それらのアプリ用に別のデリバリーグループを作成します。
Android 10 デバイスのレガシデバイス管理者モード	Google は一部の Device Administrator API を廃止しました。Android API レベル 29 をターゲットにした Citrix Secure Hub のアップグレード以降、Citrix はデバイス管理者モードに登録された Android 10 デバイスをサポートしません。	2020 年 2 月	2020 年 11 月	Android 10 デバイスを Android Enterprise に移行します。
Android TouchDown	DigiCert は Android TouchDown のサポートを停止しました。Citrix では、Exchange デバイスポリシーから Android TouchDown プラットフォームページを削除しました。	2018 年 7 月	2020 年 11 月	推奨事項: Citrix Secure Mail を使用してください。

アイテム	説明	廃止の発表	削除	代替手段
Android 10 の新しいデバイス管理者の登録	Android 10 デバイスでレガシデバイス管理者モードへの新しい登録または再登録のサポートが終了しました。既に登録されているデバイスは引き続き機能します。	2020 年 2 月	2020 年 9 月	新しい Android 10 以降のデバイスを Android Enterprise に登録します。
MDX 暗号化	Citrix Endpoint Management コンソールで MDX 暗号化および MDX 暗号化機能が廃止されます。	2019 年 10 月	2020 年 9 月	コンプライアンスチェックを追加した暗号化管理機能を使用して、iOS または Android プラットフォームの暗号化を有効にします。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、計画してください。
Windows Mobile/CE	Windows Mobile/CE デバイスのサポートが終了しました。	2018 年 4 月	2020 年 9 月	Windows 10 デスクトップおよびノートブックを使用します。
Samsung SEAMS コンテナ	Samsung SEAMS コンテナのサポートは廃止されました。	2020 年 6 月	2020 年 8 月	Android Enterprise を使用してください。
リモート サポート	リモートサポートクライアントは廃止されました。	2019 年 1 月	2020 年 8 月	代替はありません

アイテム	説明	廃止の発表	削除	代替手段
Android 6.x および iOS 11.x 向けの Citrix モバイルアプリおよび Workspace アプリ	Android 6.x および iOS 11.x バージョンの Citrix Secure Hub、Citrix Secure Mail、Citrix Secure Web、Citrix Workspace アプリのサポートは廃止されました。	2020 年 4 月	2020 年 6 月	最低限、主要オペレーティングシステムプラットフォームの最新バージョンおよび 1 つ前のバージョンを使用してください。古いデバイスは登録されたまま残ります。ただし、Citrix は従来のデバイスをテストまたはサポートしません。
Citrix Secure Hub for iOS のネットワーク拡張機能	iOS デバイス用のネットワーキング機能をカスタマイズできる、ネットワーク拡張フレームワークは廃止されました。Citrix Secure Hub リリース 20.3.0	2018 年 10 月	2020 年 3 月	代替はありません
ローカルアカウントを使用した API サインイン	管理者は、ローカルアカウントを使用して REST API にサインインできなくなります。	2020 年 10 月		管理者は、Citrix Cloud アカウントを使用してログインできます。「REST API」を参照してください。
自己署名の Secure Sockets Layer（SSL）証明書	すべてのデバイスプラットフォームに対する自己署名 SSL 証明書のサポートが終了しました。	2020 年 5 月		既存の自己署名 L 証明書を、既知の CA（Certificate Authority：証明機関）からの信頼される SSL 証明書に置き換えます。

システム要件

March 15, 2024

Citrix が Citrix Endpoint Management をプロビジョニングしている間、Cloud Connector をインストールして Citrix Endpoint Management の展開を準備してください。Citrix Endpoint Management ソリューションは Citrix がホストしていますが、一部の通信とポートの設定が必要です。これによって、Citrix Endpoint Management インフラストラクチャを Active Directory などの企業サービスに接続できます。

Cloud Connector の要件

Citrix では、Cloud Connector を使用して Citrix Endpoint Management アーキテクチャを既存のインフラストラクチャに統合します。Cloud Connector は、ポート 443 を介して Citrix Endpoint Management に次のリソースの場所を安全に統合します：LDAP、PKI サーバー、内部 DNS クエリ、および Citrix Workspace の列挙。

- Active Directory ドメインに参加している少なくとも 2 台の専用 Windows Server マシン。マシンは仮想マシンでも物理マシンでもかまいません。適切なインストールおよび操作のために、Cloud Connector をインストールするマシンは、UTC 時間と同期している必要があります。最新の要件の完全な一覧については、Citrix アカウントチームが提供する展開資料を参照してください。

  オンボードウィザードでは、これらのマシンに Cloud Connector をインストールする方法について順を追って説明します。

- プラットフォームのシステム要件について詳しくは、「Citrix Cloud Connector」を参照してください。

サポートされる **Active Directory** の機能レベル

Citrix Endpoint Management と合わせて使用することで、Citrix Cloud Connector は、Active Directory フォレストとドメインの以下の機能レベルをサポートします。

フォレスト機能レベル	ドメイン機能レベル	サポートされるドメインコントローラー
Windows Server 2016	Windows Server 2016	Windows Server 2016、Windows Server 2019
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

> 注:
>
> Windows Server 2012 R2、2012、および 2008 R2 は製品終了（EOL）となったため、サポートされなくなりました。詳しくは、Microsoft 社の製品に関するライフサイクルドキュメントを参照してください。

NetScaler Gateway Gateway の要件

Citrix Endpoint Management では、次のシナリオに対応するためにリソースの場所に NetScaler Gateway がインストールされている必要があります:

- 基幹業務アプリのために内部ネットワークリソースにアクセスするには、マイクロ VPN が必要。これらのアプリは、Citrix の MDX テクノロジでラップされています。Micro VPN は、内部バックエンドインフラストラクチャに接続するために NetScaler Gateway が必要です。
- Citrix 業務用モバイルアプリ（Citrix Secure Mail など）を使用する予定。
- Citrix Endpoint Management と Microsoft Endpoint Manager を統合する予定である。

以下は要件です:

- ドメイン（LDAP）認証
- NetScaler Gateway 12.1 以降。プラットフォームライセンスまたはユニバーサルライセンスが必要

詳しくは、「ライセンス」を参照してください。

- パブリック SSL 証明書。

詳しくは、「Citrix ADC アプライアンスでの SSL 証明書の作成と使用」を参照してください。

- NetScaler Gateway Gateway 仮想サーバーの未使用のパブリック IP アドレス。
- NetScaler Gateway Gateway 仮想サーバーのパブリックに解決可能な完全修飾ドメイン名（FQDN）
- クラウドでホストされた Citrix Endpoint Management の中間証明書とルート証明書（スクリプトバンドルで提供）
- プロキシロードバランサー IP 用の未使用の内部プライベート IP アドレス
- ポート要件については、後述の「NetScaler Gateway のポート要件」を参照してください。
- Citrix Endpoint Management と Microsoft Endpoint Manager との統合
- Microsoft Azure で Citrix ADC VPX インスタンスを展開する

NetScaler Gateway の要件については、Citrix アカウントチームが提供する展開資料を参照してください。

Android Enterprise の要件について詳しくは、「Android Enterprise」セクションを参照してください。

Citrix Files の要件

Citrix Endpoint Management Premium Service オファリングでは、Citrix Files のファイル同期と共有サービスを利用できます。Storage Zone Controller を使用すると、Citrix Files アカウントでプライベートデータストレ

ージを使用できるようになり、Citrix Files SaaS（Software as a Service）のクラウドストレージが拡張されます。

Storage Zone Controller の要件:

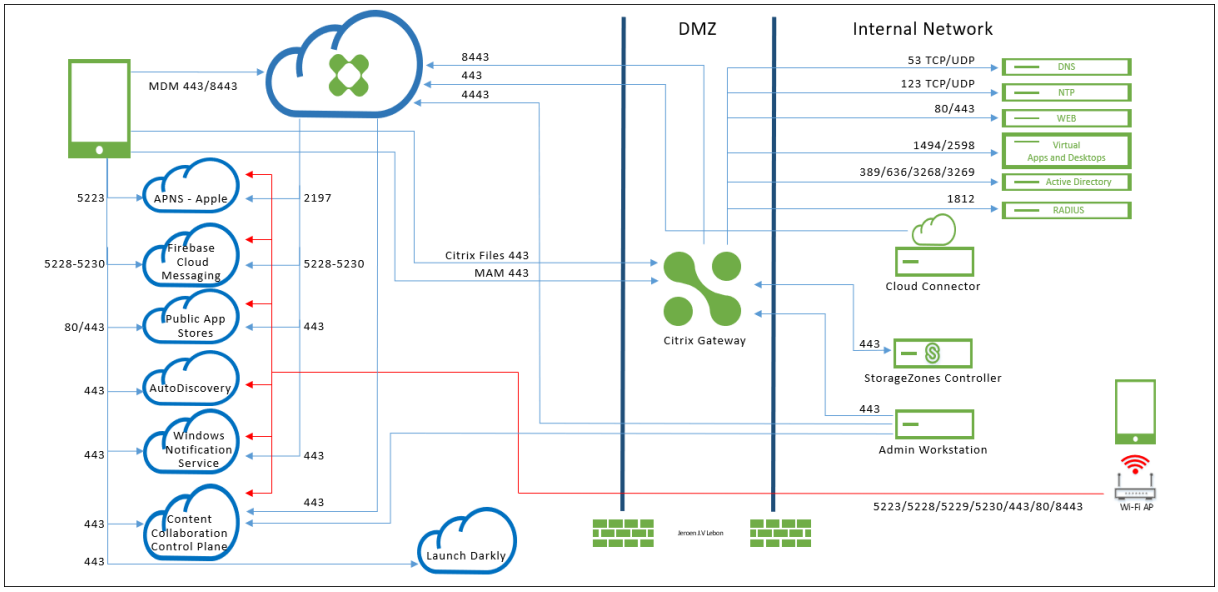
- 専用の物理マシンまたは仮想マシン
- Windows Server 2012 R2（Datacenter、Standard、または Essentials）、Windows Server 2016、Windows Server 2019、または Windows Server 2022
- 2 つの vCPU
- 4GB の RAM
- 50GB のハードディスクスペース
- Web サーバー（IIS）のサーバーの役割:
  - アプリケーション展開: ASP. NET 4.5.2
  - セキュリティ: 基本認証
  - セキュリティ: Windows 認証

Citrix Files のプラットフォーム要件:

- Citrix Files インストーラーには、Windows Server の管理者権限が必要です
- Citrix Files 管理ユーザー名

ポート要件

デバイスとアプリが Citrix Endpoint Management と通信できるようにするには、ファイアウォールの特定のポートを開きます。次の図は、Citrix Endpoint Management のトラフィックフローです。



次のセクションに、開く必要があるポートを一覧で示します。業務用モバイルアプリで使用する URL について詳しくは、「機能フラグ管理」を参照してください。

NetScaler Gateway Gateway のポート要件

Citrix Secure Hub および Citrix Workspace から NetScaler Gateway 経由でユーザーが接続できるようにするポートを開きます:

- Citrix Endpoint Management
- StoreFront
- イントラネット Web サイトなどのその他の内部ネットワークリソース

NetScaler Gateway について詳しくは、NetScaler Gateway ドキュメントの「Citrix Endpoint Management 環境の設定の構成」を参照してください。IP アドレスについては、NetScaler Gateway のドキュメントで「NetScaler Gateway が IP アドレスを使用する方法」を参照してください。

TCP ポート	説明	接続元	接続先
53（TCP と UDP）	DNS 接続に使用されます。	NetScaler Gateway SNIP	DNS サーバー
80/443	NetScaler Gateway Gateway は、2 番目のファイアウォールを介して Micro VPN 接続を内部ネットワークリソースに渡します。	NetScaler Gateway SNIP	イントラネット Web サイト
123（TCP と UDP）	ネットワークタイムプロトコル（Network Time Protocol：NTP）サービスに使用されます。	NetScaler Gateway SNIP	NTP サーバー
389	セキュリティで保護されない LDAP 接続に使用されます。	NetScaler Gateway NSIP（ロードバランサーを使用する場合は SNIP）	LDAP 認証サーバーまたは Microsoft Active Directory
443	Citrix Workspace から StoreFront への接続、Citrix Virtual Apps and Desktops への接続に使用されます。	インターネット	NetScaler Gateway

TCP ポート	説明	接続元	接続先
443	Web、モバイル、および SaaS アプリの配信のための Citrix Endpoint Management への接続に使用されます。	インターネット	NetScaler Gateway
443	Cloud Connector 通信に使用 - LDAP、DNS、PKI、Citrix Workspace の列挙	Cloud Connector サーバー	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.blob.core.windows.net/, https://*.servicebus.windows.net
443	Citrix Endpoint Management Self Help Portal が有効な場合に、Web ブラウザーからアクセスするために使用されます。	アクセスポイント（ブラウザー）	Citrix Endpoint Management（https://<sitename>/zdm/shp）
636	セキュリティで保護される LDAP 接続に使用されます。	NetScaler Gateway NSIP（ロードバランサーを使用する場合は SNIP）	LDAP 認証サーバーまたは Active Directory
1494	内部ネットワーク内の Windows ベースのアプリケーションへの ICA コネクションに使用されます。このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway SNIP	Citrix Virtual Apps and Desktops
1812	RADIUS 接続に使用されます。	NetScaler Gateway NSIP	RADIUS 認証サーバー

TCP ポート	説明	接続元	接続先
2598	セッション画面の保持を使用した内部ネットワーク内の Windows ベースのアプリケーションへの接続に使用されます。このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway SNIP	Citrix Virtual Apps and Desktops
3269	Microsoft Global Catalog のセキュリティで保護される LDAP 接続に使用されます。	NetScaler Gateway NSIP（ロードバランサーを使用する場合は SNIP）	LDAP 認証サーバーまたは Active Directory
4443	管理者がブラウザーを使用して Citrix Endpoint Management コンソールにアクセスする場合に使用されます。	アクセスポイント（ブラウザー）	Citrix Endpoint Management
8443	登録、アプリストア、モバイルアプリケーション管理（MAM）に使用されます。	NetScaler Gateway SNIP	Citrix Endpoint Management
8443	Citrix Secure Mail 認証トークンに使用される Citrix Secure Ticket Authority（STA）ポート	NetScaler Gateway SNIP	Citrix Endpoint Management

ネットワークとファイアウォールの要件

デバイスとアプリが Citrix Endpoint Management と通信できるようにするには、ファイアウォールの特定のポートを開きます。次の表に、これらのポートの一覧を示します。

内部ネットワークから Citrix Cloud へのポートを開く：

TCP ポート	接続元 IP	説明	接続先	接続先 IP
443		Cloud Connector	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.sharefile.com, https://cwsproduction.blob.core.windows.net/downloads, https://*.servicebus.windows.net	
443		管理コンソール	https://*.citrixworkspacesapi.net, https://*.cloud.com (commercial), https://*.citrix.com, https://cwsproduction.blob.core.windows.net/downloads	
443		Web ブラウザー経由の Citrix Endpoint Management Self Help Portal アクセス（ポータルが有効な場合）	Citrix Endpoint Management	

TCP ポート	接続元 IP	説明	接続先	接続先 IP
4443		Web ブラウザーからの Citrix Endpoint Management コンソールへのアクセス	Citrix Endpoint Management	

インターネットから DMZ へのポートを開く：

TCP ポート	説明	接続元 IP	接続先	接続先 IP
443	Citrix Endpoint Management クライアントデバイス		NetScaler Gateway IP	
443	Citrix Endpoint Management クライアントデバイス		NetScaler Gateway VIP	
443	Citrix Files パブリック IP	CTX208318	NetScaler Gateway VIP	

DMZ から内部ネットワークへのポートを開く：

TCP ポート	説明	接続元 IP	接続先	接続先 IP
389 または 636	NetScaler Gateway NSIP		Active Directory IP	
53（UDP）	NetScaler Gateway NSIP		DNS サーバー IP	
443	NetScaler Gateway SNIP		Exchange（EAS）サーバー IP	
443	NetScaler Gateway SNIP		内部 Web アプリ/サービス	
443	NetScaler Gateway SNIP		Storage Zone Controller IP	

内部ネットワークから DMZ へのポートを開く：

TCP ポート	説明	接続元 IP	接続先	接続先 IP
443	管理クライアント		NetScaler Gateway NSIP	

内部ネットワークからインターネットへのポートを開く：

TCP ポート	説明	接続元 IP	接続先	接続先 IP
443	Exchange（EAS）サーバー IP		Citrix Endpoint Management プッシュ通知リスナー (1)	
443	Storage Zone Controller IP		Citrix Files コントロールプレーン	CTX208318

(1)us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com

企業 Wi-Fi からインターネットへのポートを開く：

TCP ポート	説明	接続元 IP	接続先	接続先 IP
8443 / 443	Citrix Endpoint Management クライアントデバイス		Citrix Endpoint Management	
5223	Citrix Endpoint Management クライアントデバイス		Apple APNS サーバー	17.0.0.0/8
5228	Citrix Endpoint Management クライアントデバイス		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
5229	Citrix Endpoint Management クライアントデバイス		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com

TCP ポート	説明	接続元 IP	接続先	接続先 IP
5230	Citrix Endpoint Management クライアントデバイス		Firebase Cloud Messaging	android.apis.google.com, fcm.googleapis.com
443	Citrix Endpoint Management クライアントデバイス		Firebase Cloud Messaging	fcm.googleapis.com
443	Citrix Endpoint Management クライアントデバイス		Windows プッシュ通知サービス	*.notify.windows.com
443 / 80	Citrix Endpoint Management クライアントデバイス		Apple iTunes App Store	ax.apps.apple.com, *.mzstatic.com, vpp.itunes.apple.com
443 / 80	Citrix Endpoint Management クライアントデバイス		Google Play	play.google.com, android.clients.google.com, android.l.google.com, android.com, google-analytics.com
443 / 80	Citrix Endpoint Management クライアントデバイス		Microsoft アプリストア	login.live.com, *.notify.windows.com

TCP ポート	説明	接続元 IP	接続先	接続先 IP
443	Citrix Endpoint Management クライアントデバイス		iOS および Android 向け Citrix Endpoint Management AutoDiscovery サービス	discovery.cem.cloud.us
443	Citrix Endpoint Management クライアントデバイス		Windows 向け Citrix Endpoint Management AutoDiscovery サービス	enterpriseenrollment.mycompany.com, discovery.cem.cloud.us
443	Storage Zone Controller IP		Citrix Files コントロールプレーン	CTX208318
443	Citrix Endpoint Management クライアントデバイス		Google Mobile Management、Google API、Google Play ストア API	*.googleapis.com
443	Citrix Endpoint Management クライアントデバイス		CloudDPC v470 より前の接続性チェック。N MR1 以降の Android 接続性チェックでは、https://www.google.com/generate_204 にアクセスできるか、指定された Wi-Fi ネットワークでアクセス可能な PAC ファイルが指定されている必要があります。	connectivitycheck.android.com, www.google.com

AutoDiscovery サービスの接続のポート要件

このポート構成では、Citrix Secure Hub for Android から接続する Android デバイスで内部ネットワークから Citrix Endpoint Management AutoDiscovery サービス（ADS）にアクセスできるようにします。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とき、ADS にアクセスする能力は重要です。

> 注:
>
> ADS 接続ではプロキシサーバーがサポートされ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。

証明書ピン留めを有効にする場合は、次の前提条件を完了します。

- **Citrix Endpoint Management** サーバーと **NetScaler Gateway** の証明書を収集する：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する：このプロセスで、証明書の提出を求められます。

証明書ピン留めでは、デバイスを登録前に ADS に接続する必要があります。この要件により、最新のセキュリティ情報が Citrix Secure Hub で利用できることが保証されます。Citrix Secure Hub でデバイスを登録する場合、デバイスが ADS にアクセスできる必要があります。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。

Citrix Secure Hub for Android/iOS に ADS へのアクセスを許可するには、以下の FQDN のポート 443 を開放します:

FQDN	ポート	IP とポートの使用
`discovery.cem.cloud.us`	443	Citrix Secure Hub - CloudFront 経由の ADS 通信

サポートされている IP アドレスについては、AWS のクラウドベースのストレージセンターを参照してください。

Android Enterprise のネットワーク要件

Android Enterprise のネットワーク環境設定時に考慮すべき発信接続については、Google のサポート記事Android Enterprise Network Requirementsを参照してください。

アプリの要件

Citrix Endpoint Management は、最大 300 個のアプリの追加と維持に対応しています。この制限を超えると、システムが不安定になります。

Citrix Endpoint Management の互換性

March 15, 2024

新しい機能や修正された機能、およびポリシーの更新を利用するには、Citrix では以下の項目の最新バージョンをインストールすることをお勧めします:

- Citrix ではモバイルアプリケーション管理（MAM）SDK をエンタープライズ iOS アプリや Android アプリと統合して、MDX 機能をアプリに適用することをお勧めします。

  MDX Toolkit は、2023 年 7 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の管理を継続するには、MAM SDK を使用する必要があります。

- 業務用モバイルアプリ

このトピックでは、連係可能な Citrix Endpoint Management コンポーネントのサポートされているバージョンを示しています。

最新バージョンの Citrix Secure Hub、MDX Toolkit、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。

業務用モバイルアプリ

業務用モバイルアプリには、パブリックアプリストアからアクセスします。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 Citrix Secure Hub が必要です。2 つ前までのバージョンのアプリは、最新の Citrix Secure Hub と互換性があります。

業務用モバイルアプリの 2 週間ごとのリリースの流れについて詳しくは、「リリーススケジュール」を参照してください。詳しくは、「業務用モバイルアプリのサポート」を参照してください。

MAM SDK

MAM SDK は、iOS および Android プラットフォームではカバーされない MDX 機能を提供します。これらのアプリを、内部ストアまたはパブリックアプリストアのいずれかで利用できるようにします。「MDX アプリ SDK」を参照してください。

MDX Toolkit

MDX Toolkit は、2023 年 7 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。

Citrix では、最新の 3 つのリリース（n.n.n）の MDX Toolkit をサポートしています。「MDX Toolkit の新機能」を参照してください。

ブラウザーサポート

Citrix Endpoint Management コンソールには、サポートされている次の Web ブラウザーのいずれかが必要です:

- 最新バージョンの Google Chrome
- 最新バージョンの Mozilla Firefox
- 最新バージョンの Microsoft Edge
- 最新バージョンの Apple Safari

サポートされるデバイスオペレーティングシステム

March 15, 2024

この記事では、Citrix Endpoint Management によるエンタープライズモビリティ管理に関してサポートされているデバイスについて説明します。プラットフォームには固有の制限事項やセキュリティ機能があるため、すべてのプラットフォームで Citrix Endpoint Management のすべての機能がサポートされるわけではありません。

業務用モバイルアプリの最新バージョンについては、「業務用モバイルアプリのサポート」を参照してください。

> 注:
>
> Citrix は、主要オペレーティングシステムプラットフォームの最新バージョンおよび 1 つ前のバージョンをサポートします。Citrix Endpoint Management の一部の機能は、以前のプラットフォームリリースでは使用できません。
>
> 廃止される項目の情報については、「廃止」を参照してください。

オペレーティングシステムのサポートリスト

Citrix Endpoint Management は、以下のオペレーティングシステムをサポートします:

- **Android**: 10.x、11.x、12.x、13.x、14.x

  Citrix は、Android 10 以降にアップグレードしてから Android Enterprise デバイスを使用することをお勧めします。詳しくは、「Android に関する注意事項」を参照してください。

- **iOS**: 13.x、14.x、15.x、16.x、17.x

  Citrix Endpoint Management と Citrix モバイルアプリでは、現在 iOS 14.x、iOS 15.x、iOS 16.x、および iOS 17.x で使用できるすべての新機能がサポートされているわけではありません。

- **iPadOS**: 13.x、14.x、15.x、16.x、17.x

Citrix Endpoint Management と Citrix モバイルアプリでは、現在 iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x で使用できるすべての新機能がサポートされているわけではありません。

- **macOS:** 11.x、12.x、13.x、14.x

  Citrix Endpoint Management と Citrix モバイルアプリでは、現在 macOS 11、macOS 12、macOS 13 および macOS 14 で使用できるすべての新機能がサポートされているわけではありません。

- **Windows 10** および **Windows 11** デスクトップおよびタブレット：（MDM のみ）

  - Windows 10 Professional および Windows 11 Professional
  - Windows 10 Enterprise および Windows 11 Enterprise
  - Windows 10 Education および Windows 11 Education
  - Windows IoT Enterprise

  特定のオペレーティングシステムのサポートのレベルについては、Microsoft のドキュメントを参照してください。

Android に関する注意事項

Android 10 以降にアップグレードする前に、Google の Device Administration API のサポート終了が Android 10 以降を実行してい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。こちらのCitrix ブログも参照してください。

- Google は Device Administration API のサポートを終了しており、このことは Android 10 以降を実行しているデバイスに影響します。デバイス管理モード（レガシ）で Android 10 以降のデバイスを登録しようとすると失敗します。Citrix は、デバイス管理モードでの Android デバイスの登録をサポートしていません。
- Android デバイスでは Android Enterprise を使用することをお勧めします。詳しくは、「Device Administration から Android Enterprise への移行」を参照してください。
- Google API の変更は、MAM のみモードで登録されているデバイスには影響しません。
- こちらのCitrix ブログも参照してください。

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。Citrix では、ホスト名に一致する SAN が含まれている証明書のみを信頼します。

言語サポート

November 29, 2023

Citrix 業務用モバイルアプリおよび Citrix Endpoint Management コンソールは英語以外の言語での使用にも適応しています。サポートには、アプリがユーザーの優先言語にローカライズされていない場合でも、英語以外の文字およびキーボード入力が含まれます。全 Citrix 製品のグローバル化サポートについて詳しくは、「https://support.citrix.com/article/CTX119253」を参照してください。

ここでは、最新リリースの Citrix Endpoint Management でサポートされる言語を示します。

Citrix Endpoint Management コンソールと **Self Help Portal**

- フランス語
- ドイツ語
- スペイン語
- 日本語
- 韓国語
- ポルトガル語
- 簡体字中国語

Citrix 業務用モバイルアプリ

X は、その言語でアプリを使用できることを示しています。

iOS または **Android**

言語	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
日本語	X	X	X	X	X	X
簡体字中国語	X	X	X	X	X	X
繁体字中国語	X	X	X	X	X	X
フランス語	X	X	X	X	X	X
ドイツ語	X	X	X	X	X	X
スペイン語	X	X	X	X	X	X
韓国語	X	X	X	X	X	X
ポルトガル語	X	X	X	X	X	X
オランダ語	X	X	X	X	X	X
イタリア語	X	X	X	X	X	X

言語	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
デンマーク語	X	X	X	X	X	X
スウェーデン語	X	X	X	X	X	X
ヘブライ語	X	X	X	X	X	iOS のみ
アラビア語	X	X	X	X	X	X
ロシア語	X	X	X	X	X	X
トルコ語	X	X	Android のみ	-	-	-
ポーランド語	X	X	X	-	-	-

右書きの言語のサポート

次の表は、XenMobile アプリの機能の概要です。○ は、プラットフォームごとに利用可能な機能です。Windows デバイスでは、右から左へと記述する言語のサポートは使用できません。

アプリ	iOS	Android
Citrix Secure Hub	X	X
Citrix Secure Mail	X	X
Citrix Secure Web	X	X
QuickEdit	X	X

FIPS 140-2 への準拠

October 18, 2021

米国立標準技術研究所（National Institute of Standards and Technologies：NIST）が発行している FIPS（Federal Information Processing Standard：米国の情報処理標準）は、セキュリティシステムで使用される暗号化モジュールのセキュリティ要件を規定しています。FIPS 140-2 はこの標準の 2 つ目のバージョンです。NIST 検証済み FIPS 140 モジュールについて詳しくは、NIST Computer Security Resource Centerを参照してください。

iOS では、すべての保存データおよび転送中データの暗号化操作で、FIPS 検証済み暗号モジュールが使用されます。Android では、すべての保存データ暗号化操作は Citrix が提供する FIPS 検証済み暗号化モジュール、またはデバイス製造元が提供するプラットフォームの暗号モジュールを使用します。デバイス製造元のモジュールについて詳しくは、シトリックス担当者にお問い合わせください。

サポートされる Windows デバイスでは、モバイルデバイス管理（MDM）のためのすべての保存データおよび転送中データの暗号化操作で、FIPS 検証済み暗号モジュールが使用されます。

Citrix Endpoint Management MDM のためのすべての保存データおよび転送中データの暗号化操作で、FIPS 検証済み暗号モジュールが使用されます。MDM フローのすべての保存データおよび転送中データは、FIPS 準拠の暗号化モジュールをエンドツーエンドで使用します。そのセキュリティには、モバイルデバイス用の上記の暗号化操作と、モバイルデバイスと Citrix Gateway 間の暗号化操作が含まれます。

MDX Vault は、FIPS 検証済み暗号化モジュールを使って、iOS デバイスおよび Android デバイス上の、MDX でラップされたアプリおよび割り当てられた保存データを暗号化します。

Citrix Endpoint Management

March 15, 2024

Citrix Endpoint Management は、すべてのアプリとエンドポイントを 1 つの統合ビューにまとめて、セキュリティを強化し、生産性を向上させる統合エンドポイント管理（UEM）ソリューションです。UEM の概要については、Citrix Tech Zone テクニカルブリーフの「Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management は、モバイルデバイス管理（MDM）とモバイルアプリケーション管理（MAM）を提供します。

Citrix Endpoint Management の MDM 機能により、次の操作が可能になります:

- デバイスポリシーやアプリを展開する
- アセットインベントリを取得する
- デバイスのワイプなどのアクションをデバイスで実行する

Citrix Endpoint Management の MAM 機能により、次の操作が可能になります:

- BYO モバイルデバイスのアプリとデータのセキュリティを保護する。
- エンタープライズモバイルアプリを配信する。
- アプリのロックおよびデータのワイプを実行する。

MDM と MAM の機能を組み合わせることにより、次の操作が可能になります:

- MDM を使用してコーポレート発行のデバイスを管理する
- デバイスポリシーやアプリを展開する
- アセットインベントリを取得する

- デバイスのワイプ
- エンタープライズモバイルアプリを配信する
- アプリをロックしてデバイス上のデータをワイプする

次の表は、MDM、MAM、または MDM+MAM でサポートされている Citrix Endpoint Management 機能の概要です。

機能（プラットフォーム別）	MDM（1）	MAM（2）	MDM + MAM
Android Enterprise:			
デバイス登録のサポート	はい	はい	はい
ドメイン認証のサポート	はい	いいえ	はい
ドメインおよびセキュリティトークン認証のサポート	いいえ	いいえ	はい
クライアント証明書認証のサポート	いいえ	はい	はい
クライアント証明書 + ドメイン認証のサポート	いいえ	いいえ	はい
クライアント証明書 + セキュリティトークンのサポート	いいえ	いいえ	はい
Azure AD ID プロバイダーのサポート	はい	いいえ	はい
Okta ID プロバイダーのサポート	はい	いいえ	はい
ネイティブ SaaS アプリへのシングルサインオン	はい	いいえ	はい
CDN を使用したエンタープライズアプリ配信のサポート	はい	はい	はい
CDN を使用した MDX アプリ配信のサポート	はい	はい	はい
Android Enterprise 専用（COSU）デバイスのプロビジョニングによる共有デバイスのサポート	はい	いいえ	はい
Android（レガシー）:			
デバイス登録のサポート	はい	はい	はい

機能（プラットフォーム別）	MDM（1）	MAM（2）	MDM + MAM
ドメインまたはドメイン + セキュリティトークン認証のサポート	いいえ	いいえ	はい
クライアント証明書認証のサポート	いいえ	はい	はい
クライアント証明書 + ドメイン認証のサポート	いいえ	いいえ	はい
クライアント証明書 + セキュリティトークンのサポート	いいえ	いいえ	はい
Azure AD および Citrix ID プロバイダーのサポート	はい	いいえ	はい
Okta ID プロバイダーのサポート	はい	いいえ	はい
ネイティブ SaaS アプリへのシングルサインオン	はい	いいえ	はい
CDN を使用したエンタープライズアプリ配信のサポート	はい	はい	はい
CDN を使用した MDX アプリ配信のサポート	はい	はい	はい
Chrome:			
デバイス登録のサポート	はい	いいえ	はい
ユーザー名とパスワード認証のサポート	はい	いいえ	はい
iOS:			
デバイス登録のサポート	はい	はい	はい
ドメインまたはドメイン + セキュリティトークン認証のサポート	いいえ	いいえ	はい
クライアント証明書認証のサポート	いいえ	はい	はい
クライアント証明書 + ドメイン認証のサポート	いいえ	いいえ	はい

機能（プラットフォーム別）	MDM（1）	MAM（2）	MDM + MAM
Azure AD および Citrix ID プロバイダーのサポート	はい	いいえ	はい
Okta ID プロバイダーのサポート	はい	いいえ	はい
ネイティブ SaaS アプリへのシングルサインオン	はい	いいえ	はい
CDN を使用したエンタープライズアプリ配信のサポート	はい	はい	はい
CDN を使用した MDX アプリ配信のサポート	はい	はい	はい
Apple Education の統合	はい	いいえ	はい
macOS:			
デバイス登録のサポート	はい	いいえ	いいえ
ドメイン、またはドメインおよびワンタイムパスワードのサポート	はい	いいえ	いいえ
招待 URL およびワンタイムパスワードのサポート	はい	いいえ	いいえ
Windows:			
デバイス登録のサポート	はい	いいえ	いいえ
Citrix Workspace アプリを使用した Windows 10 および Windows 11 デバイスの自動登録	はい	いいえ	いいえ
ドメインまたはドメイン + セキュリティトークン認証のサポート	はい	いいえ	いいえ
クライアント証明書認証のサポート	はい	いいえ	いいえ
クライアント証明書 + ドメイン認証のサポート	はい	いいえ	いいえ
Azure AD または Citrix ID プロバイダー経由のフェデレーション認証	はい	いいえ	いいえ

機能（プラットフォーム別）	MDM（1）	MAM（2）	MDM + MAM
CDN を使用したエンタープライズアプリ配信のサポート	はい	いいえ	いいえ
Workspace Environment Management の統合（3）	はい	いいえ	いいえ

> 注：
>
> （1）展開順は、MDM 用に構成された登録プロファイルを持つデリバリーグループ内のデバイスにのみ適用されます。
>
> （2）MAM 登録には、NetScaler Gateway が必要です。
>
> （3）Workspace Environment Management（WEM）の統合により、広範囲な Windows オペレーティングシステム上の MDM 機能にアクセスできます。

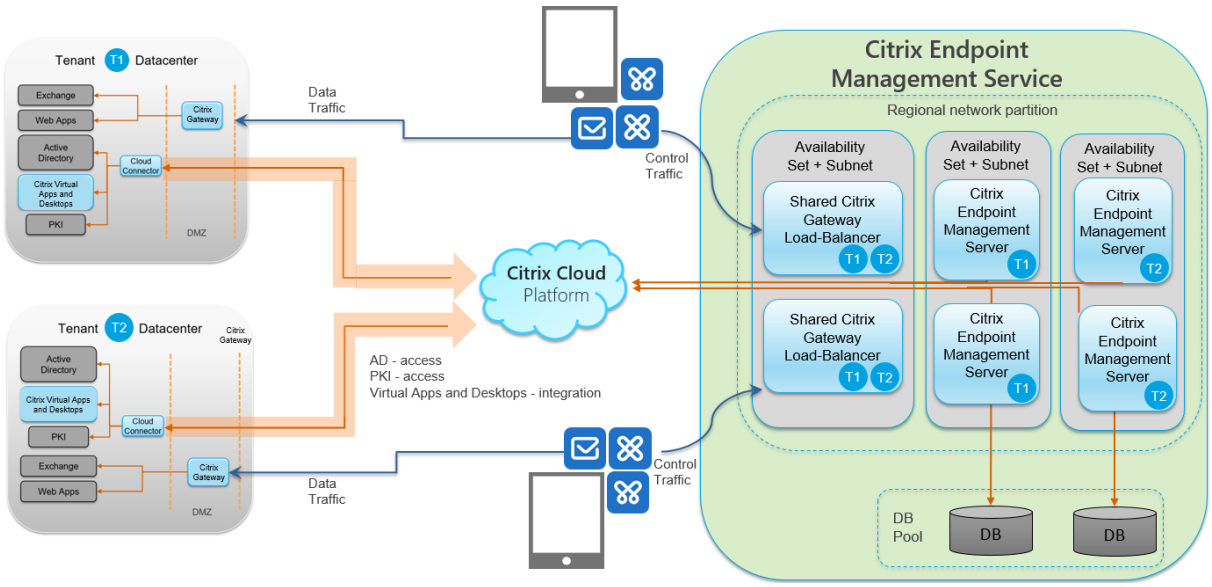
詳しくは、「管理モード」を参照してください。

アーキテクチャ

Citrix Endpoint Management アーキテクチャの必要な Citrix Endpoint Management コンポーネントは、組織のデバイスまたはアプリの管理要件によって異なります。Citrix Endpoint Management のコンポーネントはモジュール形式で、相互に依存しています。たとえば、環境には NetScaler Gateway が含まれています：

- NetScaler Gateway では、ユーザーはモバイルアプリにリモートアクセスして、ユーザーデバイスの種類を追跡できます。
- Citrix Endpoint Management でこれらのアプリとデバイスを管理します。

次の図は、Citrix Endpoint Management クラウド展開とデータセンターとの統合に関する一般的なアーキテクチャの概要です。



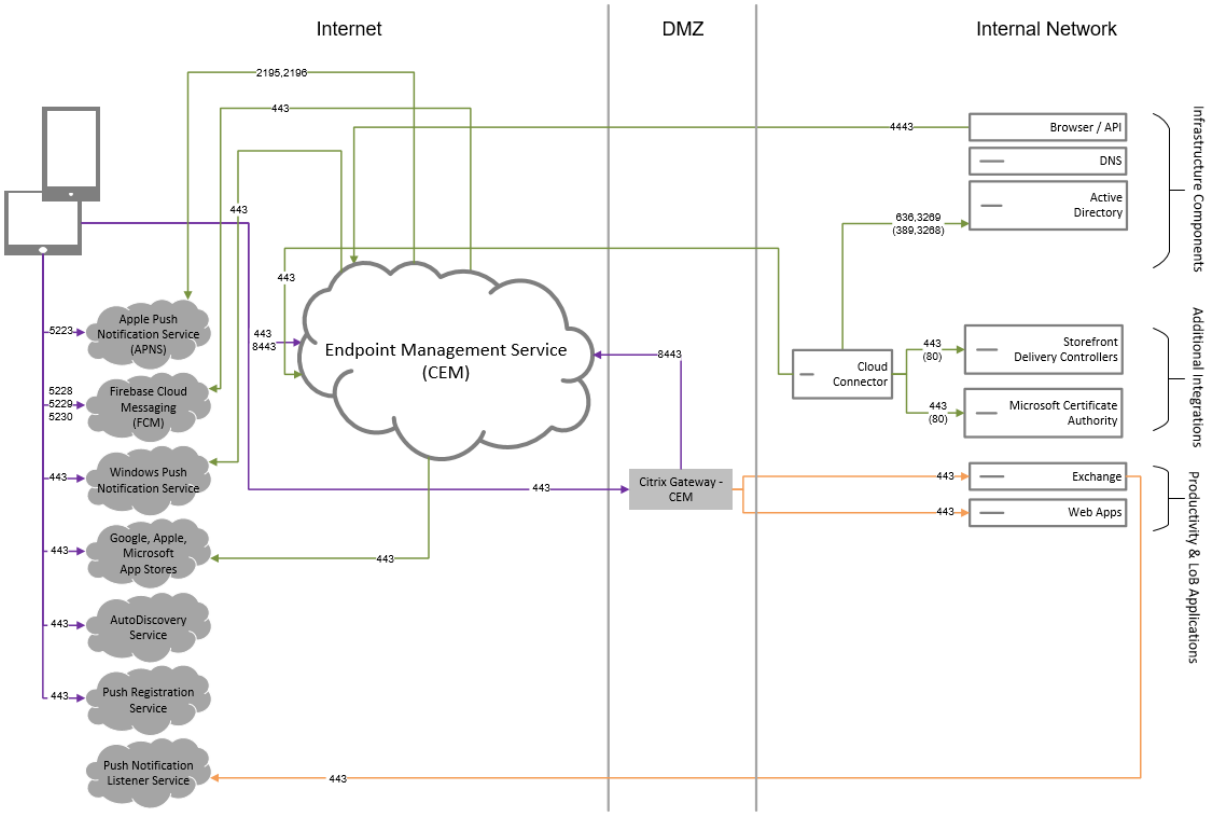
以下のサブセクションには、次に関するリファレンスアーキテクチャ図が含まれています:

- Citrix Endpoint Management
- 外部認証機関および Citrix Endpoint Management コネクタ: Exchange ActiveSync 用、および Citrix Endpoint Management MDM+MAM と Intune MAM のトラフィックフローなどのオプションコンポーネント。

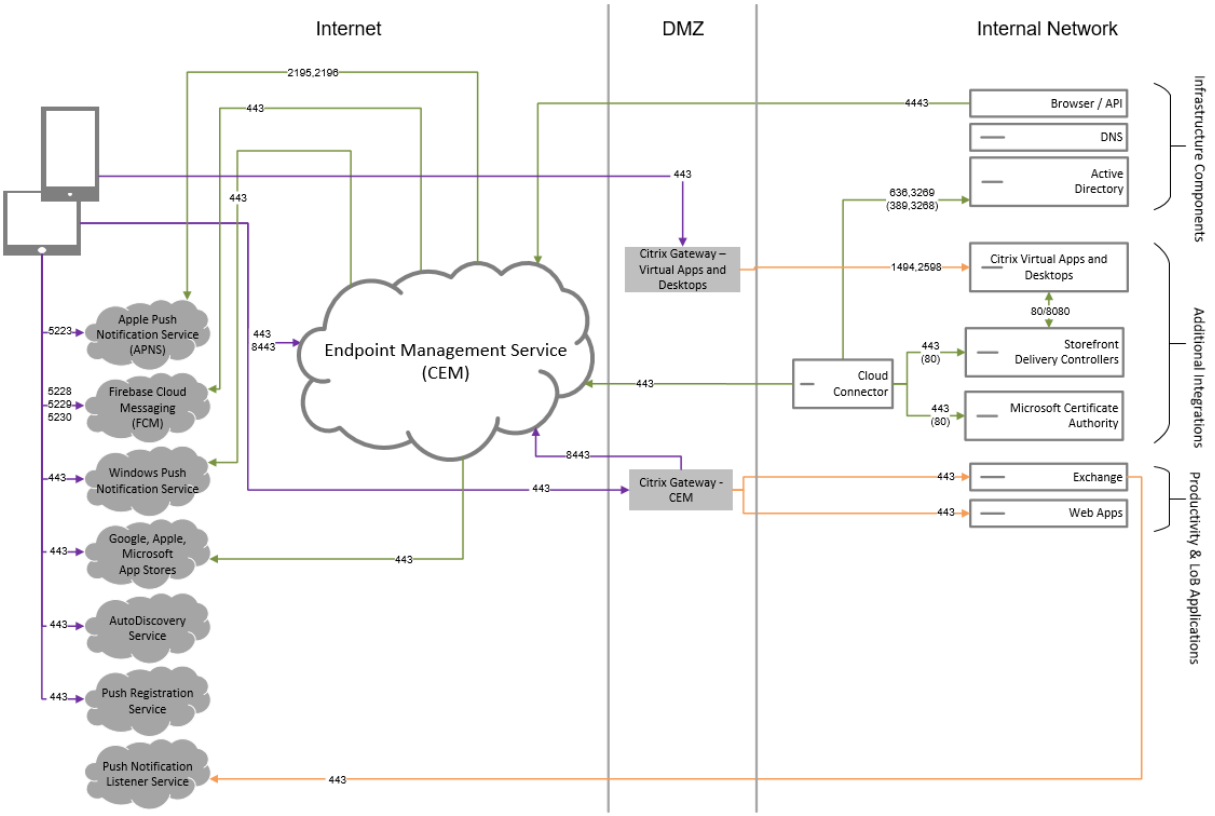
Citrix ADC および NetScaler Gateway の要件について詳しくは、Citrix の製品ドキュメント（https://docs.citrix.com/）を参照してください。

コアリファレンスアーキテクチャ

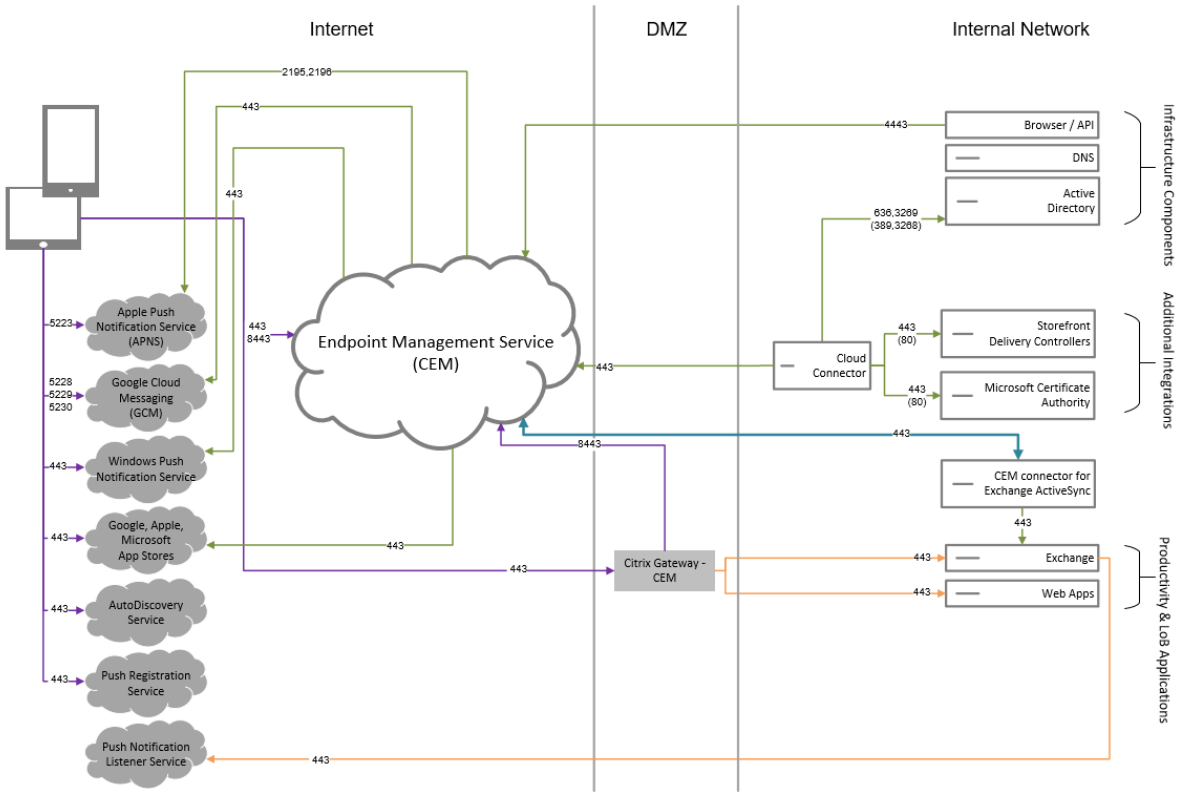
ポートの要件について詳しくは、「システム要件」を参照してください。



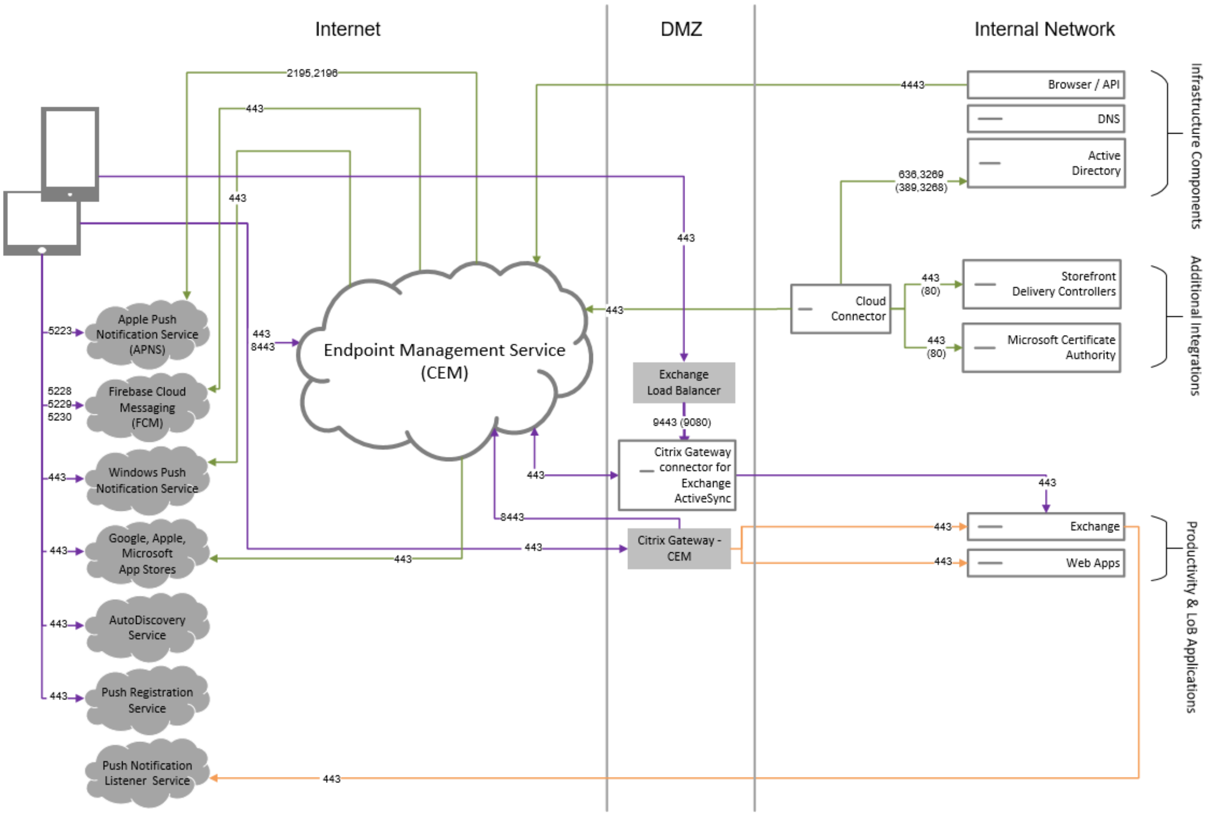
Citrix Virtual Apps and Desktops を含むリファレンスアーキテクチャ



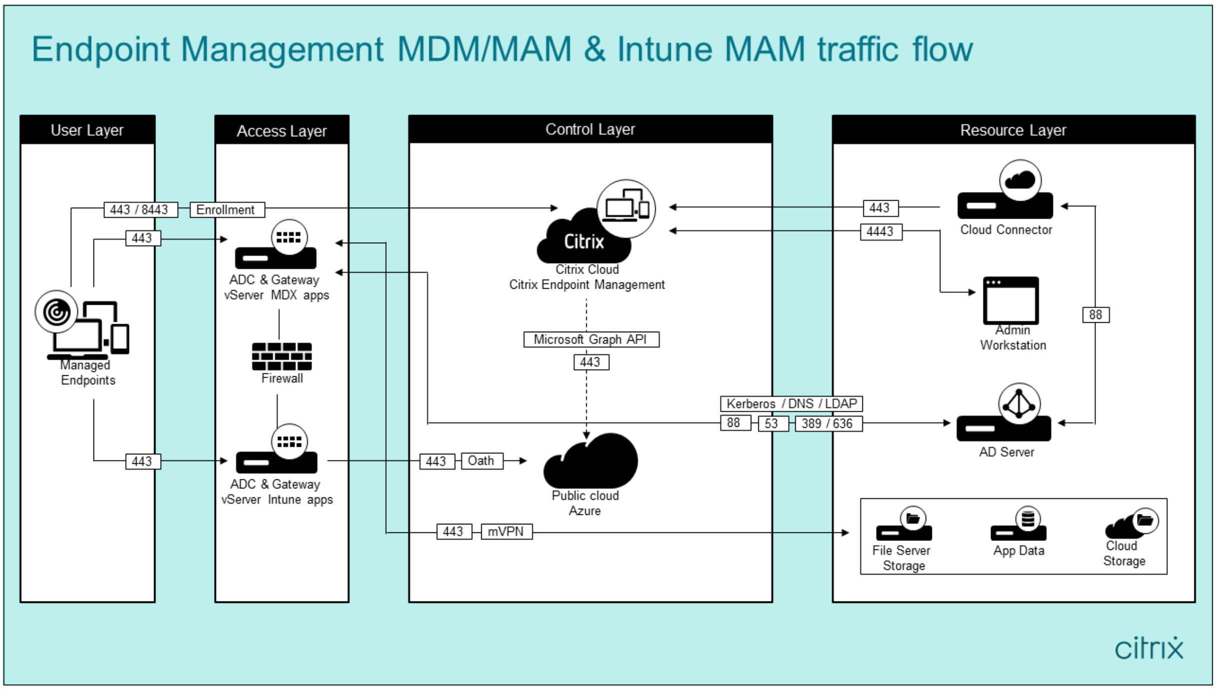
Citrix Endpoint Management コネクタ：**Exchange ActiveSync** 用を含むリファレンスアーキテクチャ



NetScaler Gateway コネクタ：**Exchange ActiveSync** 用を含むリファレンスアーキテクチャ



Citrix Endpoint Management MDM+MAM と **Intune MAM** を使用するリファレンスアーキテクチャ



リソースの場所

リソースの場所は、業務上の必要性に応じた最適な場所を選択してください。パブリッククラウド、ブランチオフィス、プライベートクラウド、データセンターなどさまざまな場所をリソースの場所にできます。以下は、場所の選択を決定する要素の例です:

- 利用者との距離
- データとの距離
- 拡張の必要性
- セキュリティ属性

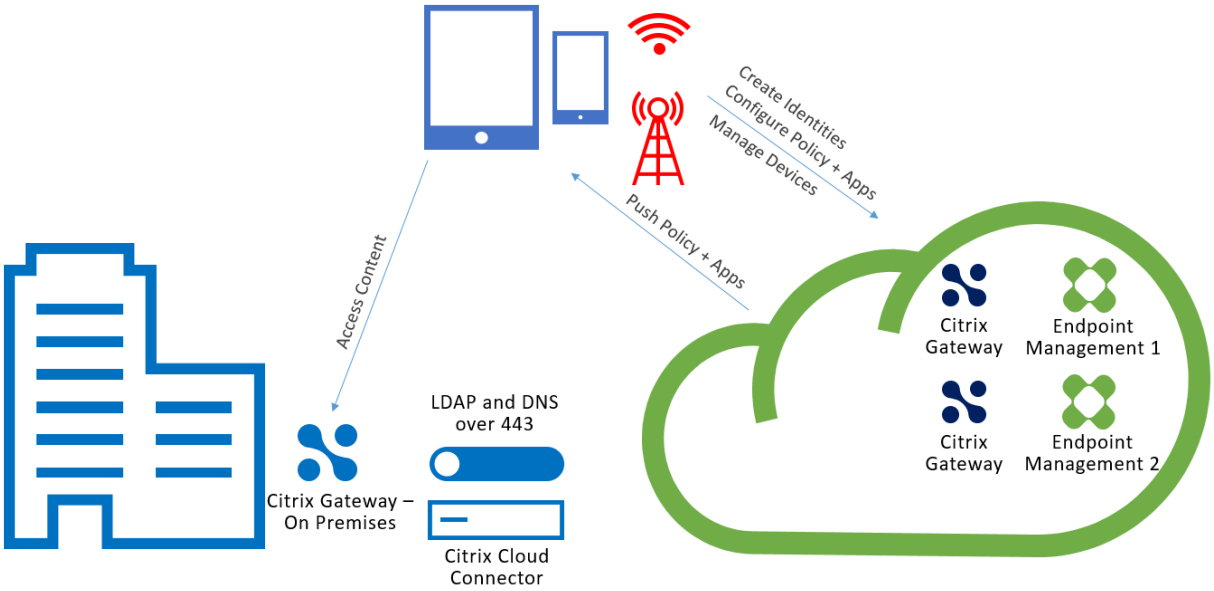
必要な数のリソースの場所を構築できます。以下はいくつかの例です:

- データとの距離が近い方が望ましい利用者やアプリケーションのために、本社のデータセンターにリソースの場所を構築する。
- グローバルユーザーのために、パブリッククラウドに別のリソースの場所を追加する。または、ブランチオフィスで別のリソースの場所を構築して、ブランチワーカーが最適に利用できるアプリケーションを提供する。
- 別のネットワークにさらにリソースの場所を追加して、限定されたアプリケーションを提供する。これ以外のリソースの場所を調整する必要なく、他のリソースや利用者に表示される内容を制限できます。

Cloud Connector

Cloud Connector は、Citrix Cloud とリソースの場所の間ですべての通信を認証および暗号化します。次のサービスにアクセスするには、Cloud Connector が必要です：LDAP、ID プロバイダー、PKI（公開キー基盤）サーバー、内部 DNS クエリ、Citrix Virtual Apps、NetScaler Gateway、Citrix Workspace、および Microsoft Endpoint Manager。

次の図は、Cloud Connector のトラフィックフローです。



Cloud Connector は、Citrix Cloud への接続を確立し、受信接続を受け入れません。

Cloud Connector には、デバイスの登録中にのみ負荷がかかります。詳しくは、「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

モバイルアプリケーション管理（MAM）を含むソリューションには、オンプレミスの NetScaler Gateway によって提供される Micro VPN が必要です。このシナリオの内容は以下のとおりです。

- データセンターには、次のコンポーネントが存在します：
  - Cloud Connector
  - NetScaler Gateway
  - Exchange、Web アプリ、Active Directory、PKI 用のサーバー
- モバイルデバイスは、Citrix Endpoint Management およびオンプレミスの NetScaler Gateway と通信します。

Citrix Endpoint Management コンポーネント

Citrix Endpoint Management コンソール。Citrix Endpoint Management 管理コンソールは、Citrix Endpoint Management の構成に使用します。Citrix Endpoint Management コンソールの使用について詳しくは、「Citrix Endpoint Management」の記事を参照してください。Citrix Endpoint Management が最新リリースに更新されると同時に、Citrix から新機能に関する記事の通知をお送りします。

Citrix Endpoint Management サービスとオンプレミス版の違いは次のとおりです：

- Remote Support クライアントは、Citrix Endpoint Management では使用できません。
- Citrix では、Citrix Endpoint Management の syslog とオンプレミスの syslog サーバーとの統合はサポートされません。代わりに、Citrix Endpoint Management コンソールの［トラブルシューティングとサポート］ページからログをダウンロードできます。これを行う場合は、［すべてダウンロード］をクリックする必要があります。

MAM SDK。MDX Toolkit は、2023 年 7 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。

- モバイルアプリケーション管理（MAM）SDK は、iOS および Android プラットフォームではカバーされない MDX 機能を提供します。iOS アプリや Android アプリを MDX 対応にして保護できます。これらのアプリを、内部ストアまたはパブリックアプリストアのいずれかで利用できるようにします。「MDX アプリ SDK」を参照してください。

業務用モバイルアプリ。Citrix が開発した業務用モバイルアプリにより、Citrix Endpoint Management 環境に生産性と通信のためのツールスイートが提供されます。所属する組織のポリシーは、それらのアプリを保護します。詳しくは、「業務用モバイルアプリ」を参照してください。

Citrix Endpoint Management コネクタ：**Exchange ActiveSync** 用 Citrix Endpoint Management コネクタ：Exchange ActiveSync 用によって、ネイティブモバイルメールアプリを使用するユーザーはメールに安全にア

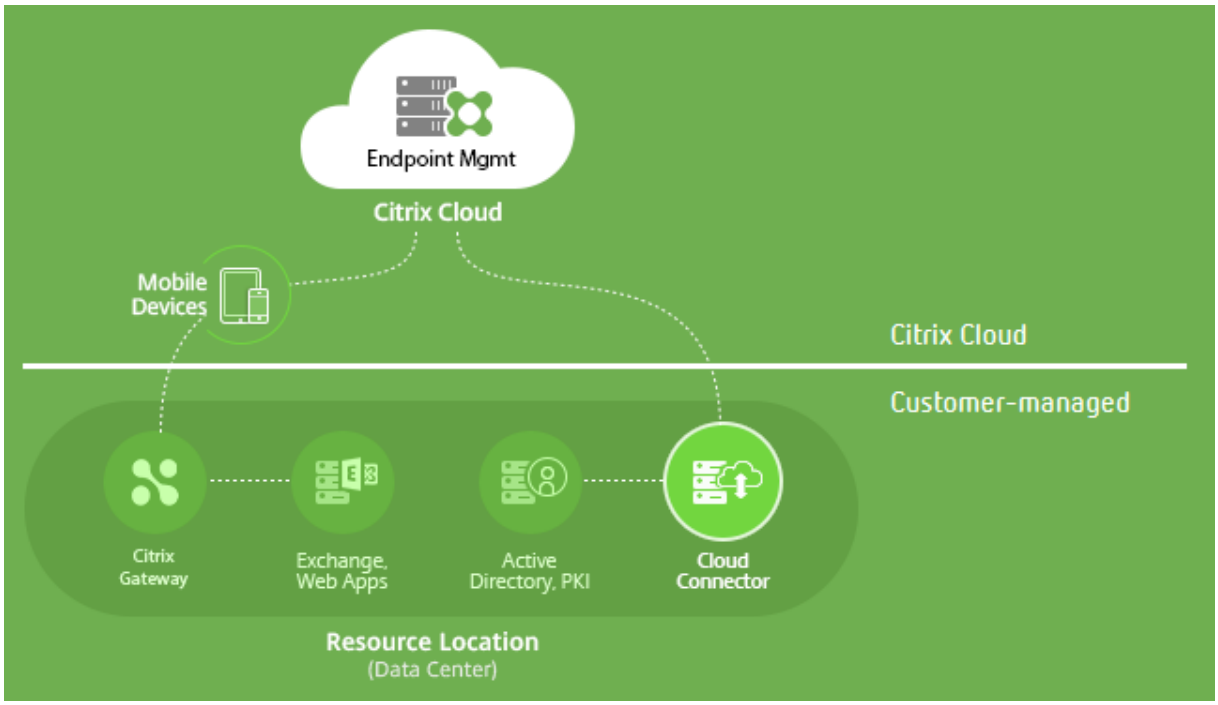
クセスできます。Exchange ActiveSync 用コネクタは、Exchange サービスレベルで ActiveSync フィルターを提供します。つまり、メールが Citrix Endpoint Management 環境に到達した時ではなく、Exchange サービスに到達した後にのみフィルタリングが行われます。コネクタで NetScaler Gateway を使用する必要はありません。既存の ActiveSync トラフィックのルーティングに変更を加えることなく、コネクタを展開できます。詳しくは、「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」を参照してください。

NetScaler Gateway コネクタ：**Exchange ActiveSync** 用。NetScaler Gateway コネクタ：Exchange ActiveSync 用によって、ネイティブモバイルメールアプリを使用するユーザーはメールに安全にアクセスできます。Exchange ActiveSync 用コネクタは、境界に ActiveSync フィルターを提供します。このフィルタリングでは、NetScaler Gateway を ActiveSync トラフィックのプロキシとして使用します。その結果、フィルタリングコンポーネントはメールトラフィックフローのパスの一部として、メールが環境に出入りするときにインターセプトします。Exchange ActiveSync 用コネクタは、NetScaler Gateway と Citrix Endpoint Management の間の仲介役を果たします。詳しくは、「NetScaler Gateway コネクタ：Exchange ActiveSync 用」を参照してください。

Citrix Endpoint Management のセキュリティの技術概要

Citrix Cloud は、Citrix Endpoint Management 環境のコントロールプレーンを管理します。このコントロールプレーンには、Citrix Endpoint Management サーバー、Citrix ADC ロードバランサー、シングルテナントデータベースなどが含まれます。クラウドサービスは、Citrix Cloud Connector を使用して顧客データセンターと統合します。Cloud Connector を使用している Citrix Endpoint Management のユーザーは、通常、自社データセンターで NetScaler Gateway を管理します。

次の図は、サービスとそのセキュリティ境界です。



このセクションには、次の情報が記載されています：

- Citrix Cloud のセキュリティ機能を紹介します。
- Citrix Cloud のセキュリティを確保するために、Citrix と顧客の責任範囲を定義します。
- Citrix Cloud、またはそのコンポーネントやサービスの構成および管理に関するガイダンスは提供しません。

包括的なエンドツーエンドのセキュリティを実現するために Citrix Endpoint Management が使用するテクノロジについては、Security and Productivity for the Mobile Enterpriseを参照してください。

データフロー

コントロールプレーンは、ユーザーオブジェクトおよびグループオブジェクトへの読み取りアクセスが制限されています。これらのオブジェクトは、ディレクトリ、DNS、および同様のサービスに格納されています。コントロールプレーンは、セキュリティ保護された HTTPS 接続を使用して Citrix Cloud Connector 経由でこれらのサービスにアクセスします。

メール、イントラネット、Web アプリのトラフィックなどの企業データは、NetScaler Gateway を介して直接デバイスとアプリケーションサーバー間を移動します。NetScaler Gateway は、顧客のデータセンターに導入されています。

データ分離

コントロールプレーンは、ユーザーデバイスおよびそのモバイルアプリケーションを管理するために必要なメタデータを保存します。サービス自体は、マルチテナントコンポーネントとシングルテナントコンポーネントを組み合わせて構成されています。ただし、サービスアーキテクチャごとに、顧客のメタデータは常に各テナントに個別に保存され、固有の資格情報で保護されます。

資格情報の処理

このサービスは、次の種類の資格情報を処理します:

- ユーザーの資格情報：ユーザーの資格情報は、HTTPS 接続経由でデバイスからコントロールプレーンに送信されます。コントロールプレーンは、セキュリティで保護された接続を介して顧客ディレクトリ内のディレクトリでこれらの資格情報を検証します。
- 管理者資格情報：管理者は、Citrix Online のサインオンシステムを使用する Citrix Cloud に対して認証を行います。このプロセスでは、ワンタイム署名された JSON Web Token（JWT）が生成され、管理者はそのサービスにアクセスできます。
- **Active Directory** 資格情報：コントロールプレーンには、Active Directory からユーザーのメタデータを読み取るためにバインド資格情報が必要です。これらの資格は、AES-256 暗号化で暗号化され、テナントごとのデータベースに保存されます。

展開に関する考慮事項

ご使用の環境内に NetScaler Gateway を導入する場合、公開されているベストプラクティスのドキュメントを参照することをお勧めします。

その他のリソース

Citrix 製品に関連するセキュリティ情報を確認することをお勧めします。新しいセキュリティ情報、および更新されたセキュリティ情報については、「Citrix Security Bulletins」を参照してください。また、サインアップして ［通知設定］ でアラートを受信することを検討してください。

セキュリティ情報について詳しくは、次のリソースを参照してください:

- Citrix セキュリティサイト: https://www.citrix.com/security
- Citrix Cloud ドキュメント: セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド
- Secure Deployment Guide for Citrix ADC（英語）

Mobile Threat Defense ソフトウェアとの統合

Mobile Threat Defense（MTD）は、エンタープライズモバイルデバイスに対する高度なサイバー攻撃の検出、分析、および阻止するための支援を行います。MTD と Unified Citrix Endpoint Management（UEM）を組み合わせることによって、組織のセキュリティと可視性を向上させます。

MTD ソフトウェアは、Citrix Endpoint Management が以下の目的で使用する脅威データを提供します:

- マルウェア、フィッシング、ネットワーク攻撃、および中間者攻撃に対して保護する。
- デバイスのコンプライアンスステータスを定義する。
- リスクレベルを定義する。
- アプリ、データ、デバイス、およびモバイルネットワークを保護するために、ポリシーベースの措置を講じる。

Citrix Endpoint Management は、以下の MTD ベンダーと統合されています:

- Check Point
- Lookout
- Wandera
- Zimperium

詳細およびデモのリクエストについては、当社の MTD パートナーまたは Citrix の営業担当者にお問い合わせください。

Citrix Endpoint Management と Microsoft Endpoint Manager との統合

March 15, 2024

Citrix Endpoint Management と Microsoft Endpoint Manager（MEM）との統合により、Citrix Endpoint Management マイクロ VPN の価値が Microsoft Edge ブラウザーなどの Microsoft Intune 対応アプリに追加されます。

統合をアクティブ化するには、Citrix Cloud 運用チームに連絡してください。

このリリースでは、次のユースケースがサポートされます：

- Intune MAM と Citrix Endpoint Management MDM+MAM。

  この資料では、Intune MAM と Citrix Endpoint Management MDM+MAM のユースケースについて説明します。Citrix を MDM プロバイダーとして追加したら、デバイスに配信する Intune 管理対象アプリを構成します。

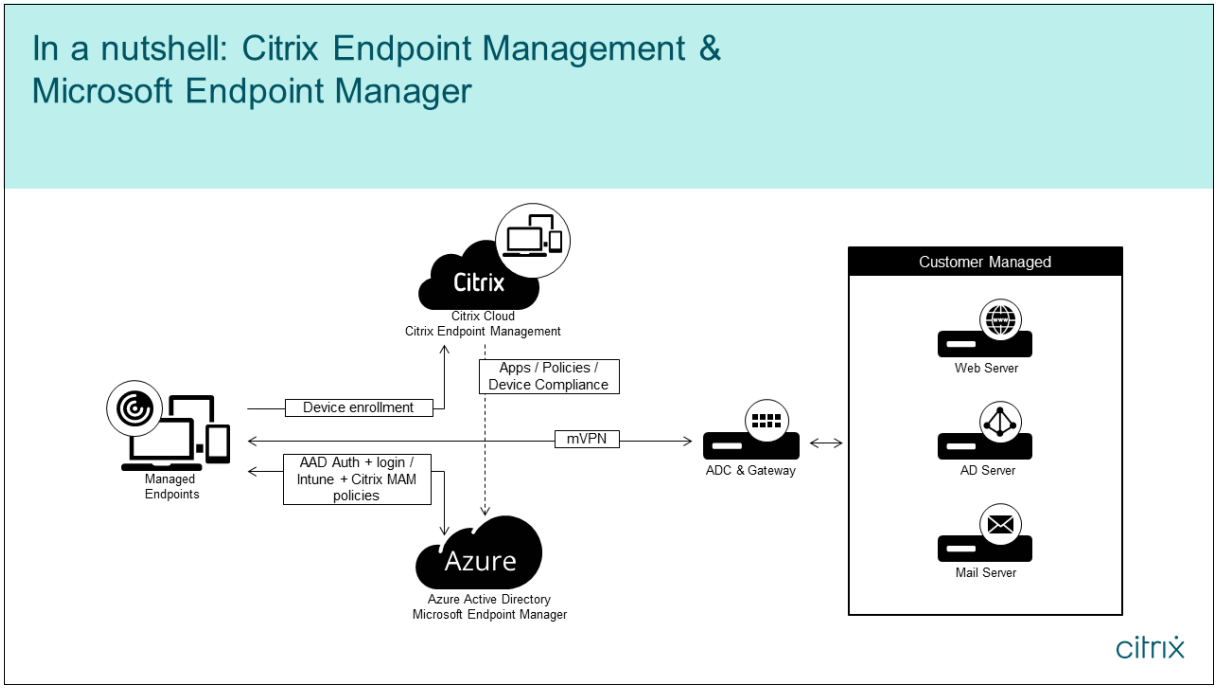
  > 重要：
  >
  > このユースケースでは、Citrix Secure Mail は Intune との統合をサポートしていません。Citrix Secure Mail は MDX モードで登録されているデバイスでのみ動作します。

- Intune MAM および Citrix Endpoint Management MDM。
- Intune MAM。
- Intune MAM および Intune MDM。Citrix Secure Mail for iOS は、このユースケースでのシングルサインオンをサポートしています。

MEM と Citrix Endpoint Management との統合を設定する方法については、入門ガイド（英語）で画像付きの分かりやすいガイドを参照してください。

Azure AD 条件付きアクセスとの統合について詳しくは、「Azure AD 条件付きアクセスとの統合」を参照してください。

次の図は、Citrix Endpoint Management と Microsoft Endpoint Manager との統合に関する概要です。



システム要件

MDX 対応

- MAM SDK

  または

- MDX Toolkit

Microsoft

- Azure Active Directory（AD）アクセス（テナントの管理者特権あり）
- Intune 対応のテナント

ファイアウォールのルール

- ファイアウォールのルールを有効にして、NetScaler Gateway のサブネット IP から`*.manage.microsoft.com`、`https://login.microsoftonline.com`、および`https://graph.windows.net`（ポート 53 および 443）に対する DNS および SSL のトラフィックを許可します。

前提条件

- **Microsoft Edge** ブラウザー： Mobile Apps SDK は、iOS および Android 用の Microsoft Edge ブラウザーアプリに統合されています。Microsoft Edge について詳しくは、Microsoft Edge のドキュメントを参照してください。
- **Citrix Cloud** アカウント： Citrix アカウントを新規登録して Citrix Endpoint Management のトライアルをリクエストするには、Citrix の営業担当者にお問い合わせください。準備が整い次第、https://onboarding.cloud.comにアクセスします。Citrix Cloud アカウントのリクエストについて詳しくは、「Citrix Cloud へのサインアップ」を参照してください。

  > 注:
  >
  > 指定するメールは、Azure AD に関連付けられていないアドレスにする必要があります。任意のフリーメールのサービスを利用できます。

- **iOS** の **APNs** 証明書： iOS の APNs 証明書を構成していることを確認します。この証明書の構成に関する詳細は、Citrix ブログ：APN 証明書の作成とインポートに関する記事を参照してください。
- **Azure AD** との同期： Azure AD とオンプレミスの Active Directory の間で同期を設定します。AD 同期ツールはドメインコントローラーマシンにはインストールしないでください。この同期の設定について詳しくは、Azure Active Directoryに関する Microsoft 社のドキュメントを参照してください。

NetScaler Gateway の構成

新しい Citrix Endpoint Management の展開を設定している場合、次の NetScaler Gateway アプライアンスのいずれかをインストールします：

- NetScaler Gateway VPX 3000 シリーズ以上
- NetScaler Gateway MPX または専用 SDX インスタンス

Citrix Endpoint Management と MEM との統合で NetScaler Gateway を使用するには：

- 管理インターフェイスとサブネット IP で NetScaler Gateway を構成します。
- すべてのクライアントからサーバーへの通信で TLS 1.2 を使用します。NetScaler Gateway での TLS 1.2 の構成について詳しくは、CTX247095を参照してください。

Citrix Endpoint Management MDM+MAM 展開で Citrix Endpoint Management と MEM との統合を使用している場合は、Citrix Gateway を 2 つ構成します。一方の NetScaler Gateway を経由して MDX アプリのトラフィックがルーティングされます。もう一方の NetScaler Gateway を経由して Intune アプリのトラフィックがルーティングされます。構成：

- 2 つのパブリック IP アドレス。
- 必要に応じて、ネットワークアドレス変換された IP を 1 つ。
- 2 つの DNS 名。例：`https://mam.company.com`。

- 2 つのパブリック SSL 証明書。予約済みのパブリック DNS 名と一致する証明書を構成するか、ワイルドカード証明書を使用します。
- 内部でルーティング不可能な RFC 1918 IP アドレスを使用する MAM ロードバランサー。
- LDAP Active Directory サービスアカウント。

委任権限の要求に同意する

ユーザーの認証が必要な管理対象アプリの場合、アプリは Microsoft Graph によって公開されているアプリの権限を要求します。これらの権限要求に同意することにより、アプリは必要なリソースと API にアクセスできます。Microsoft Azure AD のグローバル管理者の同意が必要となるアプリもあります。これらの委任権限については、グローバル管理者は Citrix Cloud にトークンを要求する権限を与える必要があります。このトークンにより、以下の権限が有効になります。詳細については、「Microsoft Graph のアクセス許可のリファレンス」を参照してください。

- サインインとユーザープロファイルの読み取り：この権限により、ユーザーは Azure AD にサインインして接続できるようになります。Citrix にはユーザーの資格情報を表示する権限はありません。
- すべてのユーザーの基本プロファイルの読み取り：アプリが組織のユーザーに関するプロファイルのプロパティを読み取ります。プロパティには、組織のユーザーの表示名、姓名、メールアドレス、写真が含まれます。
- すべてのグループの読み取り：この権限により、Azure AD グループでアプリとポリシーの割り当てを指定することができます。
- ディレクトリに対するサインインしたユーザーと同じアクセス：この権限により、Intune サブスクリプションを検証し、NetScaler Gateway と VPN を設定できます。
- **Microsoft Intune** アプリの読み取りと書き込み：アプリは次の読み取りと書き込みを行うことができます：
  - マイクロソフトが管理するプロパティ
  - グループの割り当てとアプリのステータス
  - アプリ構成
  - アプリ保護ポリシー

また、NetScaler Gateway の構成中に、Azure AD のグローバル管理者には次の要件が適用されます：

- マイクロ VPN 用に選択された Active Directory を承認する必要があります。また、NetScaler Gateway が Azure AD および Intune との通信に使用するクライアントシークレットも生成する必要があります。
- Citrix 管理者の役割を持つことはできません。代わりに、Citrix 管理者は適切な Intune アプリの管理者権限を持つユーザーに Azure AD アカウントを割り当てます。そうすることで Intune 管理者は、Citrix Cloud 管理者として Citrix Cloud 内から Intune を管理します。

> 注：
>
> Citrix はセットアップ時にのみ Intune グローバル管理者のパスワードを使用して、認証を Microsoft にリダイレクトします。Citrix にはパスワードにアクセスする権限はありません。

Citrix Endpoint Management と **MEM** との統合を構成する

1. Citrix Cloud のサイトにログオンし、Citrix Endpoint Management のトライアルをリクエストします。
2. セールスエンジニアがオンボードに関する打ち合わせを調整します。当社のエンジニアに、Citrix Endpoint Management と MEM との統合が必要であることを伝えます。リクエストが承認されたら、［管理］をクリックします。
3. サイトの右上の歯車をクリックして、［**Configure Site**］を選択できます。
4. 最初の手順にあった ［**ID** およびアクセス管理］ページへのリンクを使って移動します。
5. ［接続］をクリックして、Azure AD のインストール環境に接続します。
6. Azure AD 管理者がログオンに使用する一意のログオン URL を入力し、［確認］をクリックします。
7. Azure AD グローバル管理者アカウントを追加し、権限要求を承諾します。
8. Azure AD インスタンスが正常に接続されていることを確認します。接続が成功したことは、［接続されていません］ボタンの表示が ［有効］に変わることで分かります。
9. ［管理者］タブをクリックし、Azure AD Intune 管理者を Citrix Cloud 管理者として追加します。ドロップダウンメニューから［Azure AD］または［Citrix ID］を選択し、追加するユーザー名を検索します。［招待］選択してユーザーに ［フルアクセス］または ［カスタムアクセス］を許可してから ［招待を送信する］をクリックします。

   > 注:
   >
   > Citrix Endpoint Management では、カスタムアクセスに関する次の規則が必要です：ライブラリおよび Citrix Endpoint Management。

   追加すると Azure AD Intune 管理者にメールで招待状が送られます。招待状経由でパスワードを作成して、Citrix Cloud にサインインできます。管理者がサインインする前に、他のすべてのアカウントからサインアウトします。

   この手順の残りの作業は、Azure AD Intune 管理者が続ける必要があります。
10. 新しいアカウントでサインインした後、［**Citrix Endpoint Management**］の ［管理］をクリックします。すべてを正しく構成すれば、ページには Azure AD 管理者がサインインしていること、および Intune サブスクリプションが有効であることが表示されます。

NetScaler Gateway でマイクロ **VPN** が利用できるように設定する

Intune でマイクロ VPN を使用するには、NetScaler Gateway で Azure Active Directory が認証されるように設定する必要があります。このユースケースでは、既存の NetScaler Gateway 仮想サーバーは利用できません。

まず、Azure AD がオンプレミスの Active Directory と同期するように設定します。この手順は、Intune と NetScaler Gateway との間の認証を適切に行うために必要です。

1. Citrix Cloud コンソールの ［**Citrix Endpoint Management**］タイルで、［管理］をクリックします。
2. ［マイクロ **VPN**］の横にある ［マイクロ **VPN** を設定］をクリックします。
3. マイクロ VPN サービスの名前と NetScaler Gateway の外部 URL を入力し、［次へ］をクリックします。

   このスクリプトにより、NetScaler Gateway が Azure AD と Intune アプリをサポートするように設定されます。
4. ［スクリプトのダウンロード］をクリックします。.zip ファイルには、スクリプトの実行に関する説明付きの readme が同梱されています。保存してここで終了することもできますが、NetScaler Gateway のインストール環境でスクリプトを実行するまで、マイクロ VPN の設定は完了しません。

   > 注:
   >
   > NetScaler Gateway の設定プロセスが終了した後に COMPLETE 以外の OAuth ステータスが表示されている場合は、「トラブルシューティング」のセクションを参照してください。

デバイス管理を設定する

アプリだけでなくデバイスも管理する場合は、デバイス管理の方法を選択します。Citrix Endpoint Management MDM+MAM または Intune MDM を使用できます。

> 注:
>
> コンソールのデフォルトは Intune MDM です。Intune を MDM プロバイダーとして使用するには、Microsoft Intune のドキュメントを参照してください。

1. Citrix Cloud コンソールの［Citrix Endpoint Management と MEM との統合］で、［管理］をクリックします。［デバイス管理 **-** オプション］の横にある ［**MDM** の構成］をクリックします。
2. 一意のサイト名を入力し、最も近い場所のクラウドリージョンを選択してから ［**Request a Site**］をクリックします。サイトの準備が完了次第、メールが届きます。
3. ［**OK**］をクリックしてページを閉じます。Active Directory の場所を選択してサイトに関連付けるか、リソースの場所を作成してから ［次へ］をクリックします。
4. ［**Cloud Connector** をダウンロード］をクリックし、画面の指示に従って Cloud Connector をインストールします。インストールが終わったら、［接続のテスト］をクリックして、Citrix Cloud と Cloud Connector との間の接続を確認します。
5. ［保存して終了］をクリックして終了します。リソースの場所が表示されます。［完了］をクリックすると、設定画面に戻ります。
6. これで、サイトのタイルから Citrix Endpoint Management コンソールにアクセスできるようになりました。ここから、MDM 管理タスクを実行してデバイスポリシーを割り当てることができます。デバイスポリシーについて詳しくは、「デバイスポリシー」を参照してください。

Intune 管理対象アプリをデバイスへの配信用に構成する

Intune 管理対象アプリを配信用に構成するには:

- アプリを Citrix Cloud ライブラリに追加する
- データのフローを制御するための Citrix Endpoint Management デバイスポリシーを作成する
- アプリとポリシーのデリバリーグループを作成する

Microsoft Intune アプリを **Citrix Cloud** ライブラリに追加する

追加するアプリごとに:

1. Citrix Cloud コンソールでメニューアイコンをクリックし、［ライブラリ］をクリックします。
2. 右上にあるプラス記号のアイコンをクリックし、［モバイルアプリを追加］をクリックします。
3. Citrix Endpoint Management コンソールで Android Enterprise を構成している場合は、［アプリケーションを選択］で［**Microsoft Intune** アプリ］を選択します。カスタマイズするアプリテンプレートを選択するか、［独自のアプリをアップロードする］をクリックします。

   Citrix では既製のアプリテンプレートを提供しており、それぞれのテンプレートには事前に設定済みの、デフォルトのポリシーセットが付属します。ユーザーがアップロードするアプリの場合は、次のポリシーが適用されます:

   - **MDX** ファイル: 以下のような、MAM SDK 対応アプリまたは MDX でラップされたアプリが含まれます:
     - Intune アプリ保護ポリシーとパッケージのデフォルトの MDX ポリシー
     - パブリックストアアプリ。Intune アプリ保護ポリシーやバンドル ID またはパッケージ ID に一致するデフォルトの MDX ポリシーなど
   - **IPA** ファイル: Intune アプリ保護ポリシー。
   - **APK** ファイル: Intune アプリ保護ポリシー。

   > 注:
   >
   > アプリが Intune でラップされていない場合、Intune アプリ保護ポリシーは適用されません。

4. ［独自のアプリをアップロードする］をクリックして、.mdx ファイルまたは Intune でラップされたファイルをアップロードします。
5. アプリの名前と説明を入力し、そのアプリを任意にするか必須にするかを選択して［次へ］をクリックします。
6. アプリケーション設定を構成します。次の構成により、Citrix Endpoint Management と Intune コンテナが互いにデータを転送できるようになります。

   - アプリが他のアプリからのデータを受信することを許可する:［ポリシー管理対象アプリ］を選択します。
   - アプリが他のアプリにデータを転送することを許可する:［すべてのアプリ］を選択します。

- 他のアプリとの切り取り、コピー、貼り付けを制限する：［ポリシー管理対象アプリ］を選択します。

7. 保存データ用のストレージリポジトリを構成します。［企業データを保存できるストレージサービスを選択してください］で、［**LocalStorage**］を選択します。
8. 任意：アプリのデータの再配置、アクセス、および PIN ポリシーを設定します。［次へ］をクリックします。
9. アプリの概要を確認し、［完了］をクリックします。

   このアプリ設定には数分かかる場合があります。処理が完了すると、アプリがライブラリに公開されたことを示すメッセージが表示されます。
10. ユーザーグループをアプリに割り当てるには、［ユーザーを割り当てる］をクリックします。
11. 検索ボックスでユーザーグループを検索し、クリックで追加します。ユーザーを個別に追加することはできません。
12. すべてのグループを追加したら、［X］をクリックしてウィンドウを閉じます。

    ユーザーグループを追加するときにエラーが発生することがあります。このエラーは、ユーザーグループがローカル環境の Active Directory に同期されていない場合に発生します。

Android Enterprise アプリを **Citrix Cloud** ライブラリに追加する

Android Enterprise アプリを Citrix Cloud ライブラリに追加し、Intune アプリ保護ポリシーを設定するには、次のようにクラウド環境を構成します：

- Azure Active Directory（AAD）アカウントを使用して Citrix Cloud のフェデレーションを行います。「Azure Active Directory を Citrix Cloud に接続する」を参照してください。
- Citrix Endpoint Management で LDAP と Cloud Connector を構成します。
- Citrix Endpoint Management で Android Enterprise をセットアップします。MDM および MAM で Android Enterprise デバイスが登録されていることを確認します。Android Enterprise をセットアップするには、「Android Enterprise」を参照してください。

この手順を実行すると、Android Enterprise アプリが Citrix Endpoint Management コンソールと Intune コンソールに同時に追加されます。追加する Android Enterprise アプリごとに、次を実行します：

1. Citrix Cloud コンソールでメニューアイコンをクリックし、［ライブラリ］をクリックします。
2. 右上にあるプラス記号のアイコンをクリックし、［モバイルアプリを追加］をクリックします。
3. ［アプリケーションを選択］で、［**Android Enterprise** アプリ］を選択します。
4. 管理対象 Google Play ストアウィンドウでアプリを検索し、承認します。Google ウィンドウを閉じた後、［次へ］をクリックします。
5. アプリケーションの詳細を追加し、［次へ］をクリックします。

6. Citrix 業務用モバイルアプリを検索して選択した場合は、マイクロ VPN ポリシーを構成できます。これらのポリシーを構成したら、［次へ］をクリックします。
7. Intune アプリ保護ポリシーを構成します。［次へ］をクリックします。
8. アプリケーション設定を構成します。次の構成により、Citrix Endpoint Management と Intune コンテナが互いにデータを転送できるようになります。

    - アプリが他のアプリからのデータを受信することを許可する：［ポリシー管理対象アプリ］を選択します。
    - アプリが他のアプリにデータを転送することを許可する：［すべてのアプリ］を選択します。
    - 他のアプリとの切り取り、コピー、貼り付けを制限する：［ポリシー管理対象アプリ］を選択します。

9. 保存データ用のストレージリポジトリを構成します。［企業データを保存できるストレージサービスを選択してください］で、［**LocalStorage**］を選択します。
10. 任意：アプリのデータの再配置、アクセス、および PIN ポリシーを設定します。［次へ］をクリックします。
11. アプリの概要を確認し、［完了］をクリックします。

    このアプリ設定には数分かかる場合があります。処理が完了すると、アプリがライブラリに公開されたことを示すメッセージが表示されます。このアプリは、Citrix Endpoint Management コンソールと Intune コンソールで利用できます。Citrix Endpoint Management コンソールでは、このアプリは新しいデリバリーグループの一部であり、パブリックアプリストアのアプリとして識別されます。

12. ユーザーグループをアプリに割り当てるには、［ユーザーを割り当てる］をクリックします。
13. 検索ボックスでユーザーグループを検索し、クリックで追加します。ユーザーを個別に追加することはできません。
14. すべてのグループを追加したら、［X］をクリックしてウィンドウを閉じます。

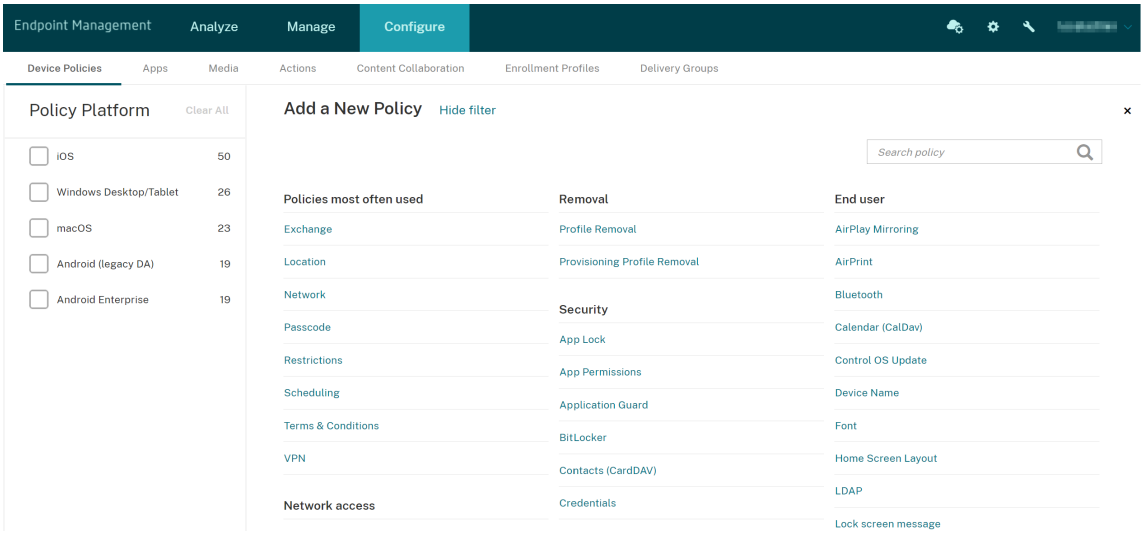
    ユーザーグループを追加するときにエラーが発生することがあります。このエラーは、ユーザーグループがローカル環境の Active Directory に同期されていない場合に発生します。

管理対象アプリ間で転送されるデータの種類を制御する

Citrix Endpoint Management デバイスポリシーを使用して、Citrix Endpoint Management または Intune コンテナ内の管理対象アプリ間で転送できるデータの種類を制御します。「企業」というタグが付けられたデータのみを許可するよう制限ポリシーを構成できます。データにタグを付けるようアプリ構成ポリシーを構成します。

制限デバイスポリシーを構成するには：

1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］の順にクリックします。
2. ［デバイスポリシー］ページで、［追加］をクリックします。［新しいポリシーの追加］ページが開きます。



3. ポリシーのリストから ［制限］をクリックします。
4. ［ポリシー情報］ページで、ポリシーの名前と（任意で）説明を入力します。［次へ］をクリックします。
5. iOS アプリのデバイスポリシーを作成するには、［プラットフォーム］ペインで ［**iOS**］を選択します。
6. ［セキュリティ - 許可］で、［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］を ［オフ］に設定します。これを ［オフ］に設定すると、［非管理対象アプリによる管理対象アカウント連絡先の読み取り］と［管理対象アプリによる非管理対象アカウント連絡先への書き込み］も ［オフ］に設定されます。［次へ］をクリックします。
7. ［保存］ボタンが表示されるまで ［次へ］をクリックします。［保存］をクリックします。

各アプリのアプリ構成デバイスポリシーを構成する：

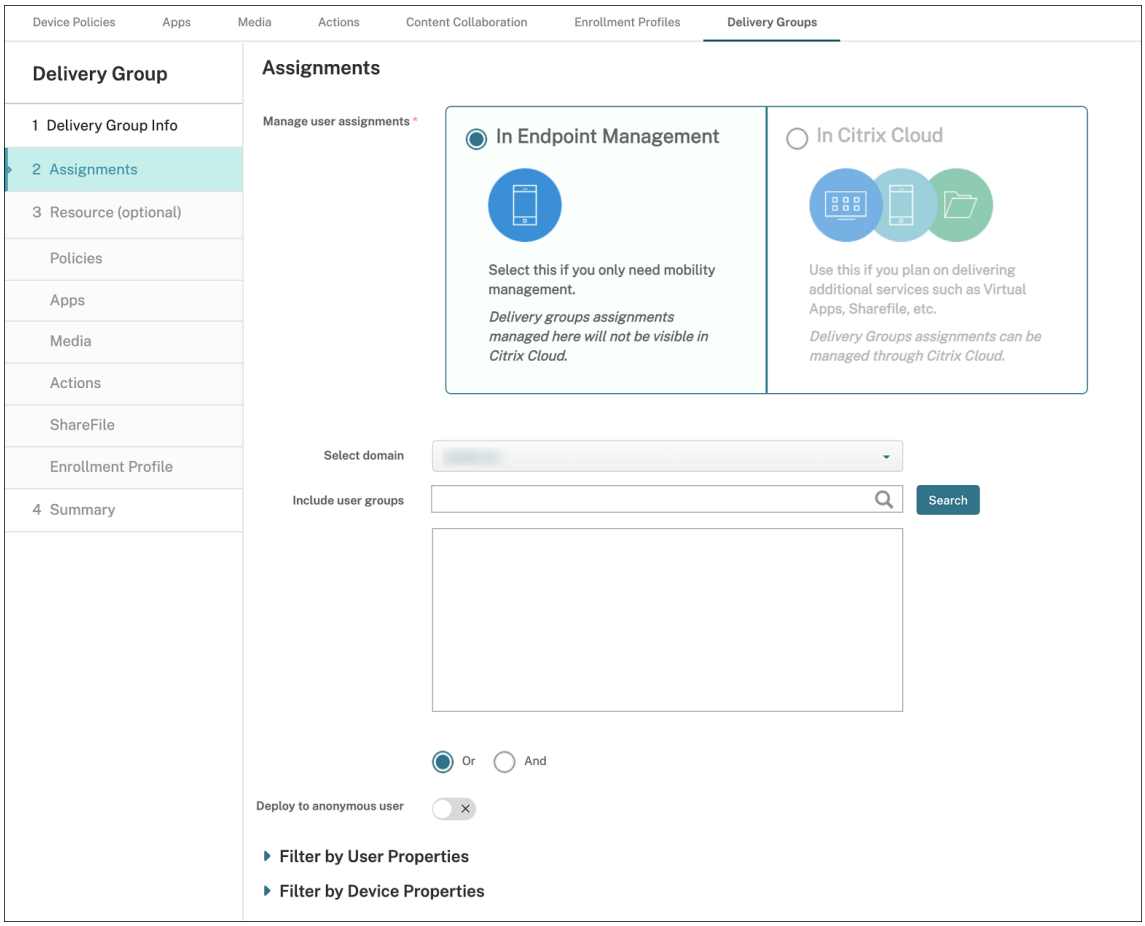
1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］の順にクリックします。
2. ［追加］をクリックします。［新しいポリシーの追加］ページが開きます。
3. ポリシーのリストから ［アプリ構成］をクリックします。
4. ［ポリシー情報］ページで、ポリシーの名前と（任意で）説明を入力します。［次へ］をクリックします。
5. iOS アプリのデバイスポリシーを作成するには、［プラットフォーム］ペインで ［**iOS**］を選択します。
6. 構成するアプリの識別子を選択します。
7. iOS アプリの場合、次のテキストを ［辞書コンテンツ］に追加します：

```
<dict>
    <key>IntuneMAMUPN</key>
    <string>${
 user.userprincipalname }
 </string>
</dict>
<!--NeedCopy-->
```


8. ［ディクショナリをチェック］をクリックします。
9. ［次へ］をクリックします。
10. ［保存］をクリックします。

アプリとデバイスポリシーのデリバリーグループを構成する

1. Citrix Endpoint Management コンソールで、［構成］**>**［デリバリーグループ］の順にクリックします。
2. ［デリバリーグループ］ページで、［追加］をクリックします。［デリバリーグループ情報］ページが開きます。
3. ［デリバリーグループ情報］ページで、デリバリーグループの名前と（任意で）説明を入力します。［次へ］をクリックします。
4. ［割り当て］ページで、デリバリーグループの展開方法を指定します：［**Citrix Endpoint Management** 使用］または ［**Citrix Cloud** 使用］を選択します。



5. ［**Citrix Endpoint Management** 使用］を選択した場合：
   - ドメインを選択：一覧から、ユーザーを選択するドメインを選択します。
   - ユーザーグループを含める：次のいずれかを行います：

- ユーザーグループの一覧で、追加するグループを選択します。選択したグループが ［選択したユーザーグループ］一覧に表示されます。
- ［検索］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
- グループ名の全体または一部を検索ボックスに入力して ［検索］をクリックし、ユーザーグループの一覧を絞り込みます。

［選択したユーザーグループ］の一覧からユーザーグループを削除するには、次のいずれかを行います:

- ［選択したユーザーグループ］の一覧で、削除する各グループの横にある ［**X**］をクリックします。
- ［検索］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
- グループ名の全体または一部を検索ボックスに入力して ［検索］をクリックし、ユーザーグループの一覧を絞り込みます。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。

6. ［次へ］をクリックします。
7. ［ポリシー］ページで、作成した制限ポリシーとアプリ構成ポリシーを左から右にドラッグします。［次へ］をクリックします。
8. ［アプリ］ページで、配信するアプリをページの左側から ［必須アプリ］または ［任意アプリ］にドラッグします。［次へ］をクリックします。
9. 任意で、［メディア］ページ、［操作］ページ、［登録］ページの設定を構成します。または、各ページをデフォルトのままにして、［次へ］をクリックします。
10. ［概要］ページで、デリバリーグループの設定を確認し、［保存］をクリックしてデリバリーグループを作成します。

Intune コンソールでアプリを公開する場合は、［アプリを管理対象にする］を選択します。監視されていないデバイスのユーザーは、アプリの管理を許可するよう求められます。ユーザーが要求を受け入れると、アプリはそのデバイスで管理対象となります。ユーザーが要求を拒否した場合、アプリはそのデバイスで利用できません。

Citrix Secure Mail を構成する

Citrix Secure Mail ではさまざまな構成がサポートされます。オンプレミスの Exchange Server に接続している Citrix Secure Mail は、Intune MAM コンテナにラップすることができます。Citrix Secure Mail は、ホストされている Exchange または Office 365 アカウントに接続できます。ただし、このリリースでは証明書ベースの認証はサポートされていないため、代わりに LDAP を使用してください。

> 重要:
>
> Citrix Secure Mail を MDX モードで使用するには、Citrix Endpoint Management MDM+MAM モードを使用する必要があります。

また、Citrix Secure Mail ではユーザー名が自動的に入力されます。この機能を有効にするには、まず以下のカスタムポリシーを構成する必要があります。

1. Citrix Endpoint Management コンソールから、［設定］**>** ［サーバープロパティ］の順に移動し、［追加］をクリックします。
2. リストから［カスタムキー］をクリックし、［キー］フィールドに「`xms.store.idpuser_attrs`」を入力します。
3. 値を **true** に設定し、［表示名］に「`xms.store.idpuser_attrs`」を入力します。［保存］をクリックします。
4. ［クライアントプロパティ］をクリックし、［追加］をクリックします。
5. ［カスタムキー］を選択し、［キー］フィールドに「**SEND_LDAP_ATTRIBUTES**」を入力します。
6. ［値］フィールドに「`userPrincipalName=${ user.userprincipalname } ,email=${ user.mail } ,displayname=${ user.displayname } ,sAMAccountName=${ user.samaccountname } ,aadupn=${ user.id_token.upn } ,aadtid=${ user.id_token.tid }`」を入力します。説明を入力し、［保存］をクリックします。

   以下の手順は、iOS デバイスにのみ適用されます。
7. ［構成］**>** ［デバイスポリシー］に移動して［追加］をクリックし、次に ［アプリ構成］ポリシーを選択します。
8. ポリシー名を入力し、［次へ］をクリックします。

   識別子リストで、［新規追加］をクリックします。表示されたテキストボックスに、Citrix Secure Mail アプリのバンドル ID を入力します。
9. ［ディクショナリ］の内容ボックスに、次のテキストを入力します。

```
<dict>

<key>XenMobileUserAttributes</key>

<dict>

<key>userPrincipalName</key>

<string>${
 user.userprincipalname }
 </string>

<key>email</key>

<string>${
 user.mail }
 </string>

<key>displayname</key>

```



```
<string>${
 user.displayname }
 </string>

<key>sAMAccountName</key>

<string>${
 user.samaccountname }
 </string>

<key>aadupn</key>

<string>${
 user.id_token.upn }
 </string>

<key>aadtid</key>

<string>${
 user.id_token.tid }
 </string>

</dict>

<key>IntuneMAMUPN</key>

<string>${
 user.id_token.upn }
 </string>

</dict>
```

10. [**Windows** デスクトップ**/**タブレット] チェックボックスをオフにして、[次へ] をクリックします。
11. ポリシーを展開するユーザーグループを選択し、[保存] をクリックします。

トラブルシューティング

一般的な問題

問題：アプリを開くと、次のエラーメッセージが表示される：アプリのポリシーが必要です。

解決策： Microsoft Graph API にポリシーを追加します。

問題：ポリシーの競合が発生する。

解決策：アプリに対して許可されるポリシーは、1 つだけです。

問題：アプリが内部リソースに接続できない。

解決策：ファイアウォールで正しいポートが開いていることや、正しいテナント ID を使用していることなどを確認してください。

NetScaler Gateway の問題

次の表は、NetScaler Gateway の構成における一般的な問題とその解決方法の一覧です。トラブルシューティングのために、取得するログの量を増やし、以下のことを行ってログを確認してください:

1. コマンドラインインターフェイスから、次のコマンドを実行します: `set audit syslogParams -logLevel ALL`
2. シェルから、次を使用してログを確認します: `tail -f /var/log/ns.log`

問題	解決策
Azure のゲートウェイアプリ用に設定する必要のある権限を使用できない。	適切な Intune ライセンスが利用可能かどうかを確認します。manage.windowsazure.com ポータルを利用して、権限を追加できるかどうかを試してください。問題が解決しない場合は、Microsoft のサポートにお問い合わせください。
NetScaler Gateway が`login.microsoftonline.com`および`graph.windows.net`に到達できない。	NS シェルから、次の Microsoft の Web サイトにアクセスできるかどうかを確認します: `curl -v -k https://login.microsoftonline.com`。次に、NetScaler Gateway で DNS が設定されているか、およびファイアウォールが正しく設定されているかを確認します（DNS 要求がファイアウォールによってブロックされている可能性があるため）。
OAuthAction を設定すると、ns.log にエラーが記録される。	Intune のライセンスが有効であること、および Azure のゲートウェイアプリに適切な権限のセットが設定されているかを確認します。
Sh OAuthAction コマンドで OAuth のステータスが完了と表示されない。	DNS 設定と Azure のゲートウェイアプリに設定されている権限を確認します。
Android または iOS デバイスで 2 要素認証のプロンプトが表示されない。	2 要素デバイス ID ログオンスキーマが認証仮想サーバーにバインドされているかを確認します。

OAuth のエラーの状態とステータス

状態	エラーの状態
COMPLETE	成功
AADFORGRAPH	シークレットが無効、URL が未解決、接続タイムアウト
MDMINFO	*manage.microsoft.com がダウンしている、または到達不能

状態	エラーの状態
GRAPH	グラフエンドポイントがダウンしており到達不能
CERTFETCH	DNS エラーのため「トークンエンドポイント: https://login.microsoftonline.com」と通信できない。この設定を検証するには、シェルを起動して「curl https://login.microsoftonline.com」を入力します。このコマンドは検証が必要です。

制限事項

以下は、Citrix Endpoint Management で MEM を使用する場合の制限事項に関する項目です。

- Citrix と Intune の組み合わせで、マイクロ VPN をサポートするアプリを展開する場合：ユーザーがダイジェストサイトにアクセスするためにユーザー名とパスワードを入力すると、資格情報が有効であってもエラーが表示される。[CXM-25227]
- ［分割トンネル］を［オン］から［オフ］に変更した後で、その時点のゲートウェイセッションが期限切れになるのを待った場合：ユーザーが完全 VPN モードで内部サイトを起動するまで、外部トラフィックが NetScaler Gateway を経由せずに直接通過する。[CXM-34922]
- ［このアプリで開く］ポリシーの設定を、［管理対象アプリ］から ［すべてのアプリ］に変更すると、Citrix Secure Mail を閉じて再起動するまで、非管理対象アプリでドキュメントを開けない。[CXM-34990]
- 完全 VPN モードで分割トンネルが ［オン］のときに、分割 DNS をローカルからリモートに変更すると、内部サイトが読み込めない。[CXM-35168]

既知の問題

mVPN ポリシー「**http/https** リダイレクト（**SSO** 使用）を有効化」がオフの場合、Citrix Secure Mail が機能しない。[CXM-58886]

サードパーティの既知の問題

Citrix Secure Mail for Android で、ユーザーが ［イベントの新規作成］をタップしても新しいイベントの作成ページが表示されない。[CXM-23917]

Citrix と Intune の組み合わせで Citrix Secure Mail for iOS を配布して、マイクロ VPN をサポートする場合：ユーザーがアプリをバックグラウンドに移動した際に Citrix Secure Mail の画面を不鮮明にするアプリポリシーが適用されない。[CXM-25032]

オンボードとリソースのセットアップ

March 15, 2024

Citrix、Citrix Cloud、または Citrix Endpoint Management を初めて使用する場合は、この記事でオンボードについて説明します。開始に必要なワークフローとその詳細について説明します。

- 最初のステップ
  - Citrix Endpoint Management サブスクリプションを購入していない場合は、「初めて Citrix 製品を利用する場合」を参照してください。
  - Citrix Endpoint Management サブスクリプションを購入済みの場合は、「［管理］ボタンが使用可能な場合」に進みます。
  - Citrix Endpoint Management サイトがプロビジョニング済みの場合は、「認証の構成」を参照してください。
- 構成の順序は重要ですか? ここでは、推奨される構成手順を記載しています。手順は入れ替えることもできます。Citrix Endpoint Management コンソールの「プロビジョニング後にセットアップする」などのメッセージで、前提条件があればお知らせします。
- オンボード後にどうすればよいですか? ここで説明したオンボードとリソースの構成が完了したら、Citrix Endpoint Management コンソールで構成を続行します。次の手順については、「デバイス登録とリソース配信の準備」を参照してください。

初めて **Citrix** 製品を利用する場合

Citrix Endpoint Management を初めて利用する Citrix Cloud のお客様:

Citrix Endpoint Management サブスクリプションを購入済みの場合は、「［管理］ボタンが使用可能な場合」に進みます。

Citrix Cloud アカウントを設定していない場合は、「Citrix Cloud への登録」を参照してください。

Citrix Cloud アカウントをセットアップ済みで、Citrix Endpoint Management を購入していない場合は、サービスデモをリクエストしてください。

1. Citrix Cloud 管理者の資格情報を使用して Citrix Cloud アカウントにサインインします。[Citrix Cloud] のホームページが開きます。

   すべての Citrix Cloud 管理者アカウントが、以下のように作成されます:

   - デフォルトでは、Citrix Cloud の管理者が Citrix Endpoint Management の管理者になります。
   - 顧客アクセスで作成された Citrix Cloud 管理者が Citrix Endpoint Management を管理するには、「Citrix Endpoint Management」を選択する必要があります。

2. Citrix Cloud のホームページで、Citrix Endpoint Management サービスのタイルを探し、［**Request Demo**］をクリックします。
3. デモのリクエストフォームに記入して送信します。Citrix Endpoint Management サービスタイルのボタンが［**Demo Requested**］に変化します。

リクエストが処理される前に Citrix Endpoint Management サービスタイルをクリックすると、担当者またはパートナーに連絡するように勧める画面が表示されます。Citrix の営業担当者は、サービスに関する情報と詳細を提供できます。

トライアルの準備中に、「システム要件」を確認して Citrix Endpoint Management の展開を準備してください。Citrix Endpoint Management ソリューションは Citrix がホストしていますが、一部の通信とポートの要件を準備する必要があります。

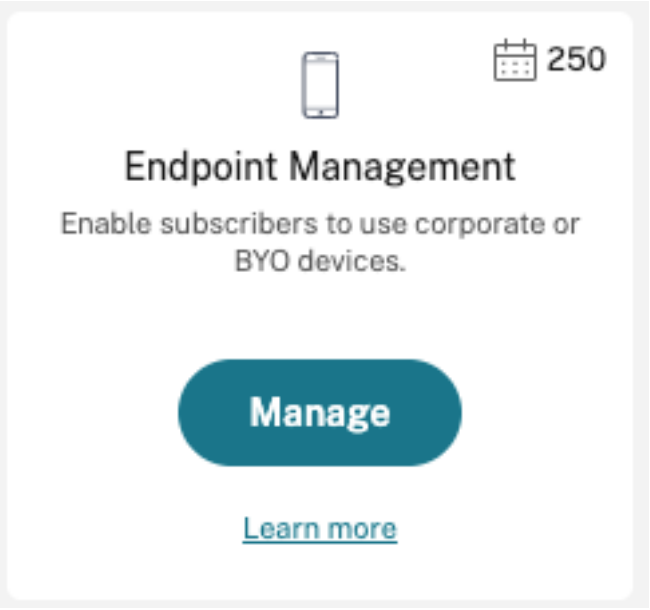
次のセクションに進みます。

［管理］ボタンが使用可能な場合

このビデオでは、オンボードについて説明します：

これは埋め込みビデオです。リンクをクリックしてビデオを見る

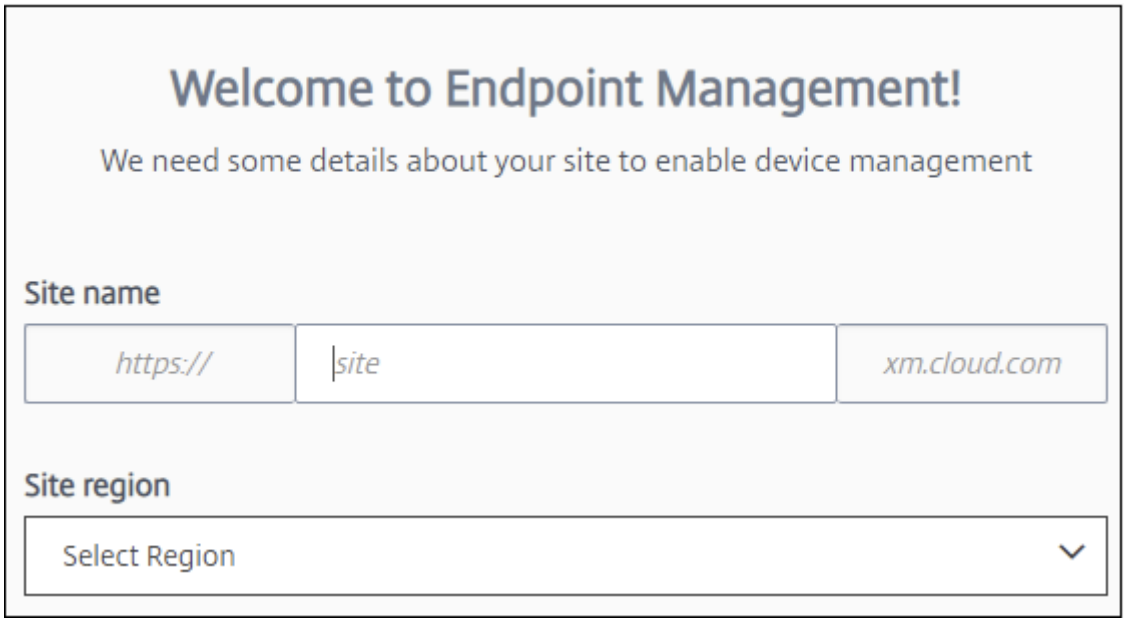
Citrix Endpoint Management サービスが利用可能な場合、Citrix Endpoint Management サービスタイトルのボタンが［管理］に変化します。



セットアップを開始するには、次の手順を実行します：

1. Citrix Cloud 管理者の資格情報を使用して Citrix Cloud アカウントにサインインします。
2. ［Citrix Endpoint Management］タイルの ［管理］をクリックして、Citrix Endpoint Management コンソールにアクセスします。

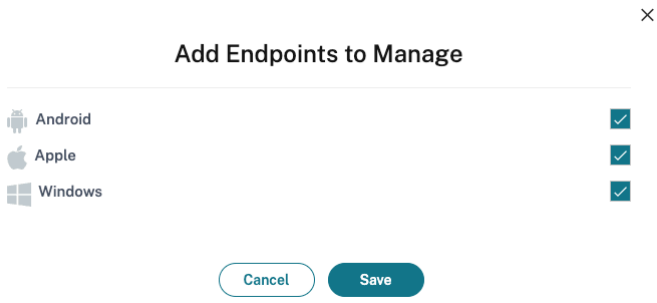
3. サイト名を入力し、地域を選択します。次に、［保存して続行］を選択します。



> 注:
>
> IP の許可を要求する場合、Citrix のサポート担当者に連絡してください。

次に、Citrix Endpoint Management コンソールが開き、スイートをプロビジョニングしていること、およびプロビジョニング中に一部の Citrix Endpoint Management 機能がロックされたことを示すメッセージが表示されます。

1. ［ようこそ］画面で［セットアップの開始］をクリックします。
2. 管理するエンドポイントを選択し、［保存］をクリックします。エンドポイントはいつでも追加または削除して、コンソールで表示または非表示にすることができます。エンドポイントの表示や非表示によって構成が影響を受けることはありません。



プロビジョニングが完了すると、Citrix からのメールを受信します。

リソースセンター


リソースセンターアイコンをクリックすると、コンソールを離れることなくハウツービデオを視聴できます。

プロビジョニング中

Citrix Endpoint Management をプロビジョニングしている間に、構成を開始できます。

リソースの場所の構成

Citrix Endpoint Management でライトウェイトディレクトリアクセスプロトコル（LDAP）接続を構成する前に、リソースの場所が必要です。リソースの場所には、利用者にクラウドサービスを提供するために必要なリソースが含まれます。ドメインごとに 1 つのリソースの場所が必要です。不明な点がある場合は、Citrix Cloud の記事「リソースの場所」を参照してください。

トライアルの準備中に、「システム要件」を確認して Citrix Endpoint Management の展開を準備してください。Citrix Endpoint Management ソリューションは Citrix がホストしていますが、一部の通信とポートの要件を準備する必要があります。これによって、Citrix Endpoint Management インフラストラクチャを Active Directory などの企業サービスに接続できます。提供する必要のある情報は、『Onboarding Handbook』（英語）の「Citrix Endpoint Management Trial Sales Engineer engagement」に記載されています。

トライアルへのアクセスが承認された後、**Citrix Endpoint Management** のボタンが［管理］に変化します。［管理］をクリックして Citrix Endpoint Management コンソールを開きます。

認証の構成

サイトのプロビジョニングを完了後、構成を続行できます。グループ、ユーザーアカウント、および関連するプロパティをインポートするには、クラウドでホストされる ID プロバイダー（IdP）、またはライトウェイトディレクトリアクセスプロトコル（LDAP）を設定することをお勧めします。

ID プロバイダーを構成するには

Citrix Endpoint Management は、Azure Active Directory、Okta、オンプレミスの NetScaler Gateway などの ID プロバイダーによる認証をサポートしています。

Citrix Cloud で ID プロバイダーを構成し、Citrix Endpoint Management 用に設定するには：

- Citrix Cloud を介した Azure Active Directory での認証
- Citrix Cloud を介した Okta での認証

- Citrix Cloud を介したオンプレミスの NetScaler Gateway での認証

LDAP を構成するには

ドメインベースの認証のために、Citrix Endpoint Management で 1 つまたは複数の LDAP 準拠ディレクトリへの接続を構成できます。Citrix Endpoint Management は、LDAP にネストされたグループをサポートします。ネストされたグループは、ローカル時間の午前 12 時に毎日同期します。

LDAP の構成の一部として、1 つ以上の Cloud Connector をインストールする必要があります。

概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

LDAP をセットアップするには、次の手順に従います:

1. ［設定］ページで **LDAP** タイルまでスクロールして ［セットアップ］をクリックします。
2. 画面に表示されるガイダンスに従って、Cloud Connector をダウンロードしてインストールします。Cloud Connector は、Citrix Cloud とリソースの間で通信するために必要です。不明な点がある場合は、「Citrix Cloud Connector」を参照してください。

LDAP を設定し、ID プロバイダーとして Azure AD や Okta を追加すると、Citrix Endpoint Management は ID プロバイダー固有の情報を Citrix Endpoint Management データベースの Active Directory グループに同期します。この構成は、既存のデリバリーグループとユーザー登録には影響しません。ただし、後で Citrix Endpoint Management に LDAP 設定を追加することはできません。詳しくは、「ID プロバイダー認証」を参照してください。

登録後に ［ドメインエイリアス］または ［ユーザー検索基準］を変更すると、ユーザーは再登録する必要があります。LDAP 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。

LDAP のセットアップ後、認証構成を続行するか特定のプラットフォームをセットアップできます。

NetScaler Gateway Gateway の構成

Citrix Endpoint Management と統合すると、NetScaler Gateway を経由して内部ネットワークとリソースにリモートデバイスでアクセスできるようになります。

Citrix Endpoint Management では、次のシナリオに対応するために NetScaler Gateway が必要です:

- 基幹業務アプリのために内部ネットワークリソースにアクセスするには、マイクロ VPN が必要。これらのアプリは、Citrix の MDX テクノロジでラップされています。Micro VPN は、内部バックエンドインフラストラクチャに接続するために NetScaler Gateway が必要です。
- Citrix Endpoint Management を使用してアプリを管理する予定である（MAM または MDM+MAM）。デバイスのみを管理する場合（MDM）、NetScaler Gateway は必要ありません。

- Citrix Endpoint Management と Microsoft Endpoint Manager を統合する予定である。（オンプレミスの NetScaler Gateway が必要です）

概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

次の表では、オンプレミスの NetScaler Gateway ソリューションでサポートされている機能がまとめられています。

サポートされる機能	NetScaler Gateway オンプレミス
Citrix Secure Mail（STA）*	はい
トンネル - Web SSO（Web シングルサインオン）	はい
完全 VPN（iOS 向け Citrix 業務用モバイルアプリでは使用できません）	はい
Per-App VPN	はい
モバイルシングルサインオン（アクセス制御）	いいえ
高可用性	はい **
マルチ POP 展開	はい ***
プロキシサポート	はい
分割トンネリング	はい
分割 DNS	はい

* Citrix Cloud Secure Ticket Authority（STA）サービスの構成

** オンプレミスの構成

*** グローバルサーバー負荷分散の構成

オンプレミスの **NetScaler Gateway** のユースケース

以下の場合には、1 つまたは複数のオンプレミスの NetScaler Gateway アプライアンスを、Citrix Endpoint Management と組み合わせて使用します:

- Per-App VPN の機能が必要である。
- 完全トンネリング、分割トンネリング、リバース分割トンネリング、または分割 DNS が必要である。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 を使用する接続には、［完全 VPN トンネル］を推奨します。
- Citrix Endpoint Management と Microsoft Endpoint Manager との統合を使用する。

オンプレミスの NetScaler Gateway を使用するには、大掛かりな構成とメンテナンスが必要です。Citrix Endpoint Management コンソールで LDAP と NetScaler Gateway を構成後、そのコンソールからスクリプトをエクスポートします。次に、NetScaler Gateway でスクリプトを実行します。

1. ［設定］ページで ［**NetScaler Gateway**］タイルまでスクロールして ［セットアップの開始］をクリックします。
2. 種類として ［**NetScaler Gateway**（オンプレミス）］を選択します。
3. 画面上のガイダンスに従います。詳しくは、「Citrix Endpoint Management で使用するオンプレミスの NetScaler Gateway を構成する」を参照してください。

通知サーバーの構成

通知を送信するには、ゲートウェイおよび通知サーバーを構成する必要があります。通知サーバーは接続性と、エンドユーザーおよび管理者間の通信の可能性を確保します。Citrix Endpoint Management で通知サーバーをセットアップするには、「通知」を参照してください。

Apple デバイス用の **Apple** プッシュ通知サービス（**APNs**）証明書の構成

Citrix Endpoint Management で Apple デバイスを登録して管理するには、Apple プッシュ通知サービス（APNs）証明書が必要です。Citrix Secure Mail for Apple でプッシュ通知を使用する場合も、Citrix Endpoint Management で APNs 証明書が必要です。Citrix Endpoint Management と APNs について詳しくは、「Citrix Secure Mail for iOS のプッシュ通知」を参照してください。

Apple から証明書を取得するには、Apple ID と開発者アカウントが必要です。詳しくは、Apple Developer Programの Web サイトを参照してください。

概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

APNs で Citrix 証明書署名要求を構成するには:

1. ［設定］ページで **Apple** タイルを展開します。
2. **APNs** 証明書タイルで ［セットアップ］をクリックして画面上のガイダンスに従います。

詳しくは、「証明書および認証」を参照してください。

Android Enterprise の構成

デリバリーグループを作成してユーザーをクラウドライブラリでデリバリーグループに割り当てると、Citrix Endpoint Management は完全に構成されます。この時点から、Citrix Endpoint Management の管理は Citrix Cloud 内で行われます。インターフェイスが統合されているため、Citrix Cloud と Citrix Endpoint Management の間の切り替えが簡単になります。

Google Play または Google Workspace を使用して、Citrix Endpoint Management 用に Android Enterprise をセットアップできます。

1. 組織が **Google Workspace** を使用しない場合：管理対象 Google Play を使用して Citrix を EMM プロバイダーとして登録できます。ビジネス向け Google Play を使用する場合、デバイスおよびエンドユーザーにビジネス向け Google Play アカウントをプロビジョニングします。ビジネス向け Google Play アカウントは、ビジネス向け Google Play へのアクセスを提供し、管理者が利用可能にしたワークアプリをユーザーがインストールし、使用できるようにします。組織がサードパーティの ID サービスを使用する場合、ビジネス向け Google Play アカウントと既存の ID アカウントを関連付けることができます。

   この種類のエンタープライズはドメインに関連付けられていないため、1 つの組織用に 1 つまたは複数のエンタープライズを作成できます。たとえば、組織の各部門または各地域は異なるエンタープライズとして登録できます。このセットアップにより、デバイスおよびアプリをさまざまなエンタープライズの個別セットとして管理できます。

2. 組織が既に **Google Workspace** を使用してユーザーに **Google** アプリのアクセスを提供している場合：Google Workspace を使用して Citrix を EMM として使用できます。組織が Google Workspace を使用している場合、既存のエンタープライズ ID および既存のユーザー用 Google アカウントが存在します。Citrix Endpoint Management で Google Workspace を使用するには、使用している LDAP ディレクトリと同期し、Google Directory API を使用して Google アカウント情報を Google から取得します。

   この種類のエンタープライズは、既存のドメインに関連付けられています。したがって、各ドメインで作成できるエンタープライズは 1 つだけです。Citrix Endpoint Management にデバイスを登録するには、各ユーザーが既存の Google アカウントで手動でサインインする必要があります。このアカウントでは、Google Workspace プランで管理対象 Google Play および他の Google サービスにアクセスできるようになります。

概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

開始するには、次の手順を実行します：

1. ［設定］ページで **Android** タイルを展開します。
2. **Android Enterprise** タイルで ［セットアップ］をクリックします。
3. Google アプリケーションへのユーザーアクセス方法によって **Google Play** または **G Suite** を選択します。Android Enterprise プラットフォームで既に Google Play が構成されている場合、Google Play ストアに移動する UI が表示され再登録できます。［再登録］をクリックして CEM コンソールに戻り、ページを更新します。
4. 画面上のガイダンスに従います。

次を参照してください：

- Android Enterprise アカウントの作成

Firebase Cloud Messaging の構成

Firebase Cloud Messaging（FCM）を使用して Android デバイスが Citrix Endpoint Management に接続するタイミングと方法を制御することを Citrix ではお勧めします。Citrix Endpoint Management は、FCM を有効にした Android デバイスへの接続通知を送信します。セキュリティ操作や展開コマンドによって、ユーザーに Citrix Endpoint Management サーバーへの再接続を求めるプッシュ通知が送信されます。詳しくは、「Firebase Cloud Messaging」を参照してください。

Microsoft Endpoint Manager との統合

Citrix Endpoint Management と Microsoft Endpoint Manager との統合により、Citrix Endpoint Management マイクロ VPN の価値が Microsoft Edge ブラウザーなどの Microsoft Intune 対応アプリに追加されます。

また、Citrix Endpoint Management と MEM との統合により、企業では Intune と Citrix の組み合わせで独自の LOB アプリをラップすることが可能になり、Intune のモバイルアプリ管理（MAM：Mobile Application Management）コンテナ内でマイクロ VPN 機能を利用することができます。Citrix Endpoint Management でマイクロ VPN を利用すると、ご利用のアプリでオンプレミスリソースにアクセスできるようになります。Office 365 アプリ、基幹業務アプリ、Citrix Secure Mail を 1 つのコンテナで管理し配信できます。単一のコンテナにより、究極のセキュリティと生産性が実現します。

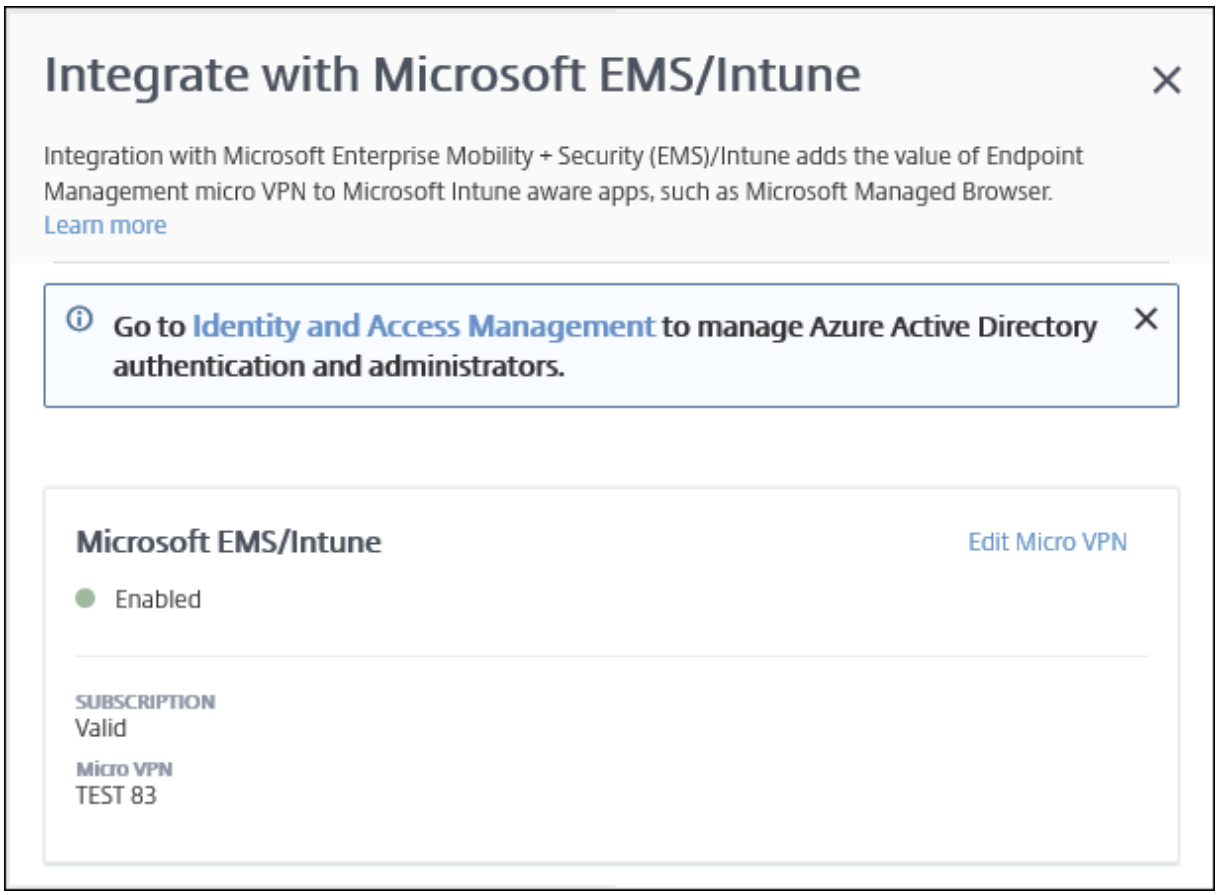
- デフォルトでは、Citrix Cloud の管理者が Citrix Endpoint Management の管理者になります。
- 顧客アクセスで作成された Citrix Cloud 管理者が Citrix Endpoint Management を管理するには、「Citrix Endpoint Management」を選択する必要があります。

Citrix Endpoint Management コンソールでは、ユーザーの役割とメンバーシップのみを変更できます。必要なときに役割を変更するには、Citrix Cloud ダッシュボードから Citrix Endpoint Management コンソールにアクセスします。［管理］タブに移動して ［ユーザー］をクリックします。特定のユーザーを選択し、［編集］をクリックして役割を変更します。詳しくは、「RBAC を使用した役割の構成」を参照してください。

MEM との統合については、「Citrix Endpoint Management と Microsoft Endpoint Manager との統合」を参照してください。

Citrix Cloud での構成の完了後、次の手順で Citrix Endpoint Management コンソールに戻ります：Citrix Cloud の ［ホーム］ページに移動して **Citrix Endpoint Management** タイルで ［管理］をクリックします。これによって、Azure Active Directory アカウントで Citrix Endpoint Management にサインインした場合に検証できます。

1. ［設定］ページで **Microsoft EMS/Intune** との統合タイルまでスクロールします。
2. ［詳細を表示］をクリックします。UI に、接続が正常に有効になったかが示されます。

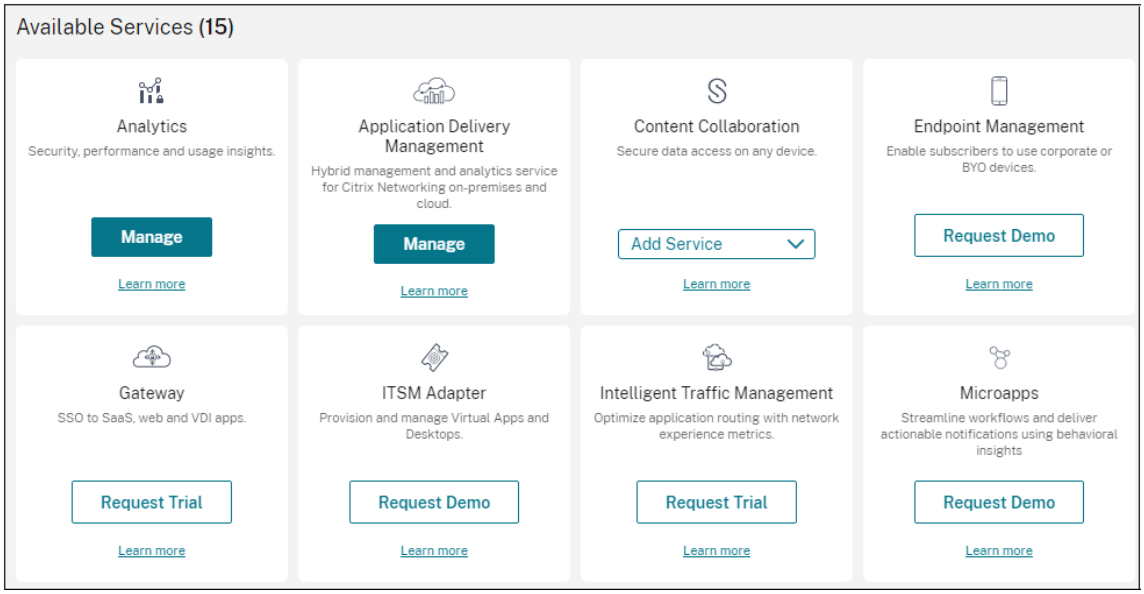


Citrix Cloud コンソールで、ユーザー名やパスワードの変更、およびローカルユーザーの削除や編集を実行することもできます。「ID およびアクセス管理」を参照してください。

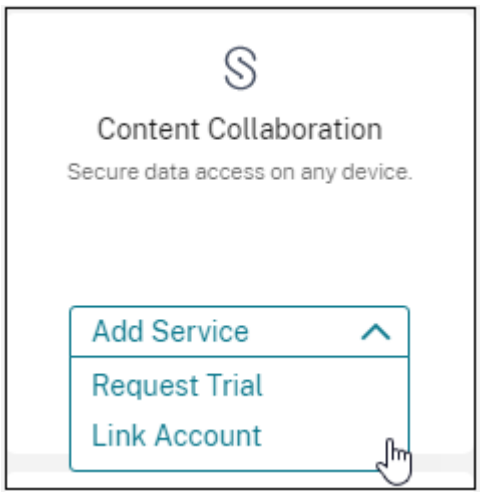
既存の **ShareFile** アカウントを **Citrix Cloud** にリンクする

Citrix Cloud にサインアップする前に ShareFile アカウントを持っていた場合は、そのアカウントを Citrix Cloud にリンクする必要があります。アカウントをリンクするには、ShareFile アカウントの管理者のメールアドレスを使用する必要があります。準備が整ったら、https://onboarding.cloud.comにアクセスします。

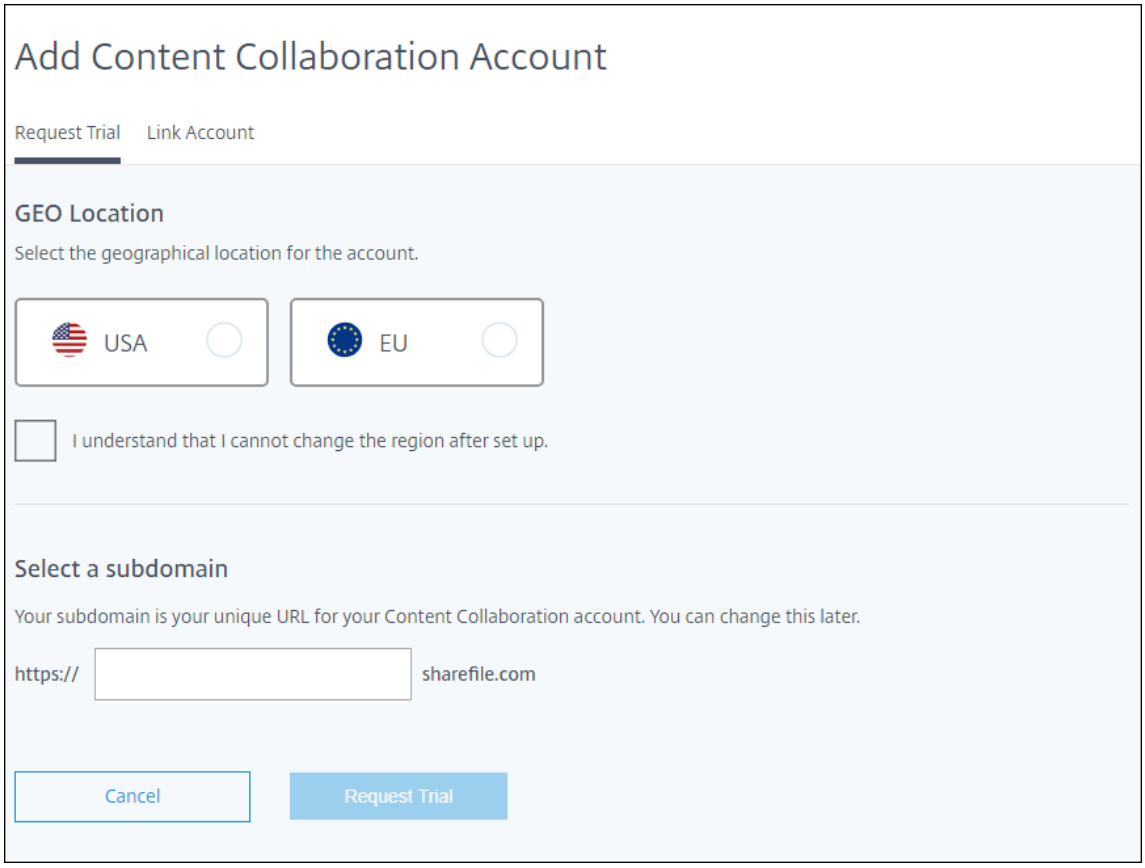
1. ログイン後、次のような画面が開きます。



2. [**ShareFile**] タイルで、[アカウントをリンクする] を選択します。



3. ShareFile アカウントを確認すると、次のページが開きます。



4. ［アカウントをリンクする］タブをクリックして処理を完了します。Citrix Cloud から ShareFile アカウントをすぐに管理できます。

Cloud Connector のサイズおよびスケールの考慮事項

November 29, 2023

Citrix Endpoint Management サービスのサイズとスケーラビリティを評価する場合は、特定の要件に合わせて Cloud Connector の構成を調べてテストします。Cloud Connector には、デバイスの登録中にのみ負荷がかかります。マシンのサイズを縮小すると、システムのパフォーマンスに悪影響を与える可能性があります。

Citrix では、リソースの場所ごとに 2 つの Cloud Connector が必要です。Cloud Connector は、他のコンポーネントや製品の責任を共有しない専用サーバーにインストールします。テストでは、Cloud Connector は（負荷分散されていない）高可用性セットに展開されています。

構成のテスト

- 専用の Windows Server 2019×2 台、vCPU×2、メモリ 4GB

- Android および iOS デバイスが MDM+MAM に登録、8 時間にわたって均等に分割
- 1,000 台のデバイスごとに、1 時間あたり 125 台のデバイスを登録するように Citrix Endpoint Management を構成
  - 1,000 台のデバイス（1 時間あたり 125 台のデバイス登録）
  - 5,000 台のデバイス（1 時間あたり 625 台のデバイス登録）
  - 10,000 台のデバイス（1 時間あたり 1250 台のデバイス登録）
  - 20,000 台のデバイス（1 時間あたり 2500 台のデバイス登録）

テスト結果

Cloud Connector	1,000 台のデバイス	5,000 台のデバイス	10,000 台のデバイス	20,000 台のデバイス
CPU 平均	2%	2%	4%	4%
CPU 最大	8%	8%	10%	11%
メモリ平均	73%	73%	75%	75%
メモリ最大	76%	76%	76%	79%

デバイス登録とリソース配信の準備

March 15, 2024

> 重要:
>
> 先に進む前に、「オンボードとリソースのセットアップ」で説明したすべてのタスクを完了してください。
>
> 今後の変更についてユーザーに通知します。Welcome to your Citrix User Adoption Kitを参照してください。

Citrix Endpoint Management では、さまざまな登録オプションがあります。この記事では、サポートされているすべてのデバイスの登録に必要な基本的なセットアップについて説明します。次の図に、基本的なセットアップの概要を示します。

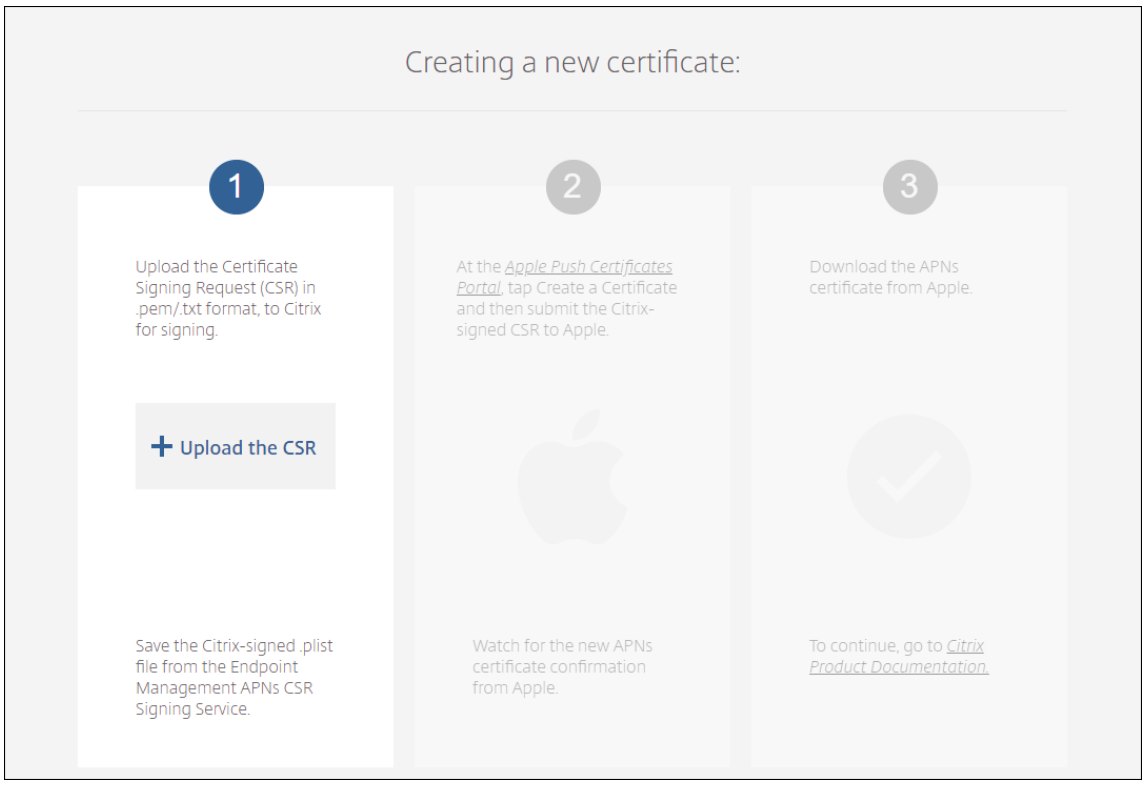
サポートされているデバイスのリストについては、「サポート対象のデバイスオペレーティングシステム」を参照してください。

iOS デバイス用の Apple プッシュ通知サービス（APNs）証明書のセットアップ

> 重要:
>
> APNs の従来のバイナリプロトコルに対する Apple のサポートは、2021 年 3 月 31 日で終了します。代わりに HTTP/2 ベースの APN プロバイダー API の使用をお勧めします。リリース 20.1.0 以降、Citrix Endpoint Management は HTTP/2 ベースの API をサポートしています。詳しくは、https://developer.apple.com/のニュースとアップデートで「Apple Push Notification Service のアップデート」を参照してください。APNs への接続を確認する方法については、「接続確認」を参照してください。

Citrix Endpoint Management で iOS デバイスを登録して管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書が必要です。Citrix Secure Mail for iOS のプッシュ通知の場合も、Citrix Endpoint Management で APNs 証明書が必要です。

- Apple から証明書を取得するには、Apple ID と開発者アカウントが必要です。詳しくは、Apple Developer Programの Web サイトを参照してください。
- APNs 証明書を取得して Citrix Endpoint Management にインポートするには、「APNs 証明書」を参照してください。



- Citrix Endpoint Management と APNs について詳しくは、「Citrix Secure Mail for iOS のプッシュ通知」を参照してください。

Android デバイス用の **Firebase Cloud Messaging**（**FCM**）のセットアップ

Firebase Cloud Messaging（FCM）は、Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御します。セキュリティ操作や展開コマンドを実行しようとすると、プッシュ通知が送信されます。この通知は、ユーザーに Citrix Endpoint Management への再接続を求めます。

- FCM をセットアップするには、Google アカウントの設定が必要です。Google Play 資格情報を作成するには、「デベロッパーアカウント情報の管理」を参照してください。Google Play は、アプリを追加、購入、および承認し、デバイスの Android Enterprise ワークスペースに展開するためにも使用します。Google Play を使用してプライベートな Android アプリ、パブリックアプリ、およびサードパーティアプリを展開できます。
- FCM をセットアップするには、「Firebase Cloud Messaging」を参照してください。

Citrix Endpoint Management AutoDiscovery サービスのセットアップ

AutoDiscovery サービスでは、メールベースの URL 検出によってユーザー登録処理が簡単になります。また、AutoDiscovery サービスは、登録確認や証明書のピン留めなどの機能を Citrix Workspace のお客様に提供します。

Citrix Cloud にホストされているこのサービスは、多くの Citrix Endpoint Management 環境で重要な要素となります。

AutoDiscovery サービスでは、ユーザーに次のメリットがあります:

- 社内ネットワークの資格情報を使用して、デバイスを登録できます。
- Citrix Endpoint Management のサーバーアドレスの詳細を入力する必要がありません。
- ユーザーは、ユーザー名をユーザープリンシパル名（UPN）形式で入力します。例: `user@mycompany.com`。

高セキュリティ環境では、AutoDiscovery サービスを使用することをお勧めします。AutoDiscovery サービスは、中間者攻撃を防ぐ公開キー証明書ピン留めをサポートしています。証明書ピン留めにより、Citrix クライアントが Citrix Endpoint Management と通信するときに所属組織が署名した証明書が使用されます。Citrix Endpoint Management サイトの証明書ピン留めを構成する方法については、Citrix サポートにお問い合わせください。証明書のピン留めについて詳しくは、「証明書ピン留め」を参照してください。

AutoDiscovery サービスにアクセスするには、https://adsui.cloud.com（商用）に移動します。

前提条件

- Citrix Cloud の新しい AutoDiscovery サービスには、最新バージョンの Citrix Secure Hub が必要です:
  - iOS の場合、Citrix Secure Hub バージョン 21.6.0 以降
  - Android の場合、Citrix Secure Hub バージョン 21.8.5 以降

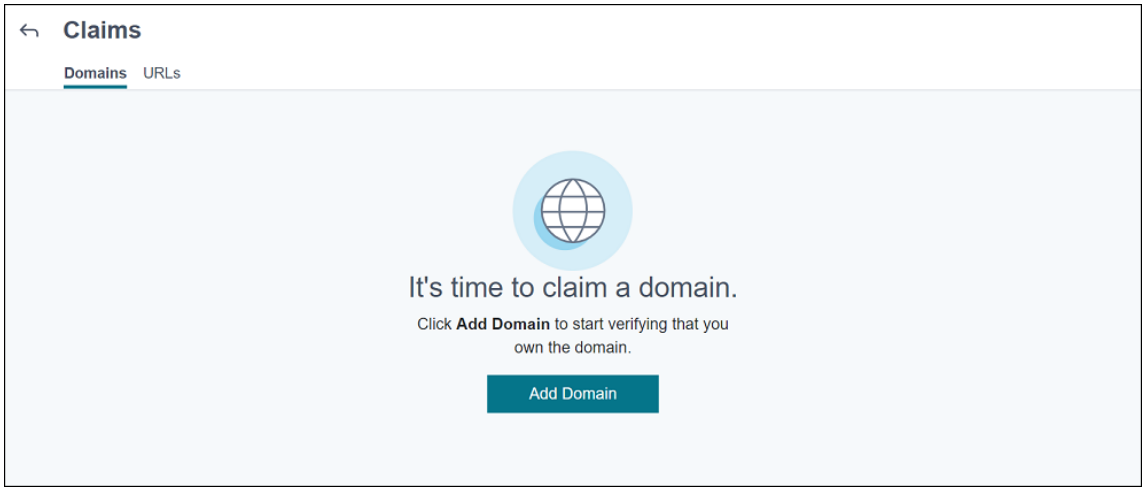
    以前のバージョンの Citrix Secure Hub で実行されているデバイスでは、サービスが中断する可能性があります。
- 新しい AutoDiscovery サービスにアクセスするには、フルアクセス権を持つ Citrix Cloud 管理者アカウントが必要です。AutoDiscovery サービスは、カスタムアクセス権を持つ管理者アカウントをサポートしていません。アカウントをお持ちでない場合は、「Citrix Cloud への登録」を参照してください。

  Citrix は、サービスを中断することなく、既存のすべての AutoDiscovery レコードを Citrix Cloud に移行しました。移行されたレコードは、新しいコンソールに自動的に表示されません。所有権を証明するには、新しい AutoDiscovery サービスでドメインを解放する必要があります。詳しくは、CTX312339を参照してください。
- Citrix Endpoint Management 環境で AutoDiscovery サービスの使用を開始する前に、ドメインを確認して要求してください。最大 10 個のドメインを要求できます。要求により、確認済みドメインが AutoDiscovery サービスに関連付けられます。10 を超えるドメインを申請するには、SRE チケットを開くか、Citrix テクニカルサポートにお問い合わせください。
- MAM トラフィックをデータセンターに転送するには、［NetScaler Gateway FQDN］の代わりに［MAM ポート］設定を使用します。NetScaler Gateway のポートと共に完全修飾ドメイン名を入力すると、クライアントデバイスは ［**MAM** ポート］設定の構成を使用します。

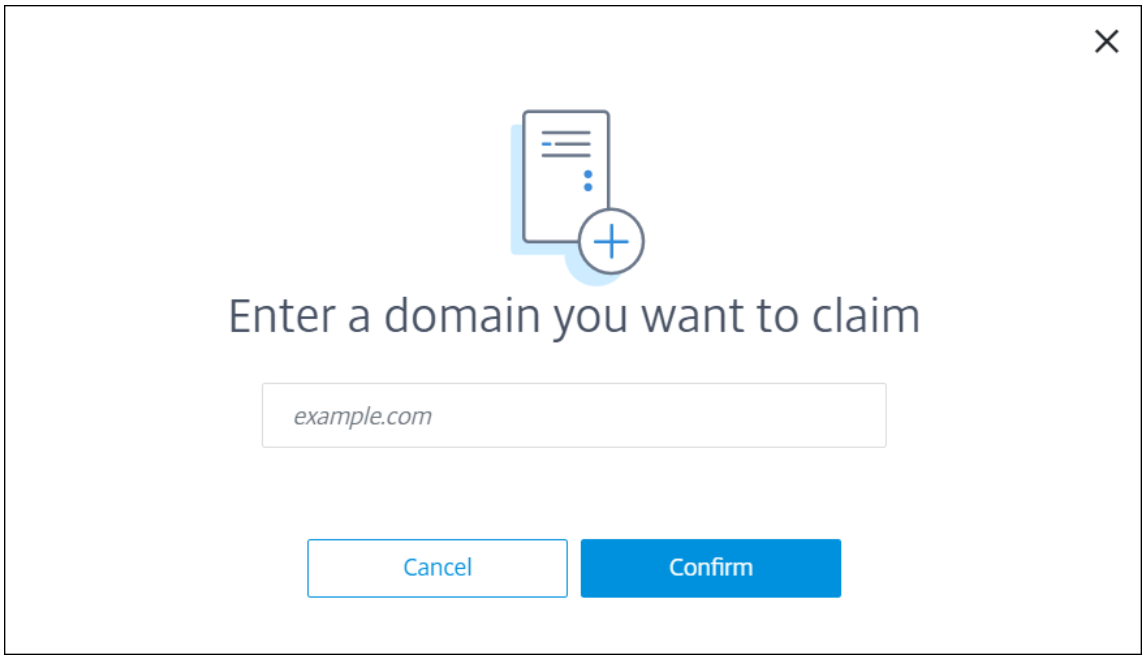
- 広告ブロッカーによって Web サイトが開かない場合は、Web サイト全体で広告ブロッカーを無効にしてください。

ドメインの要求

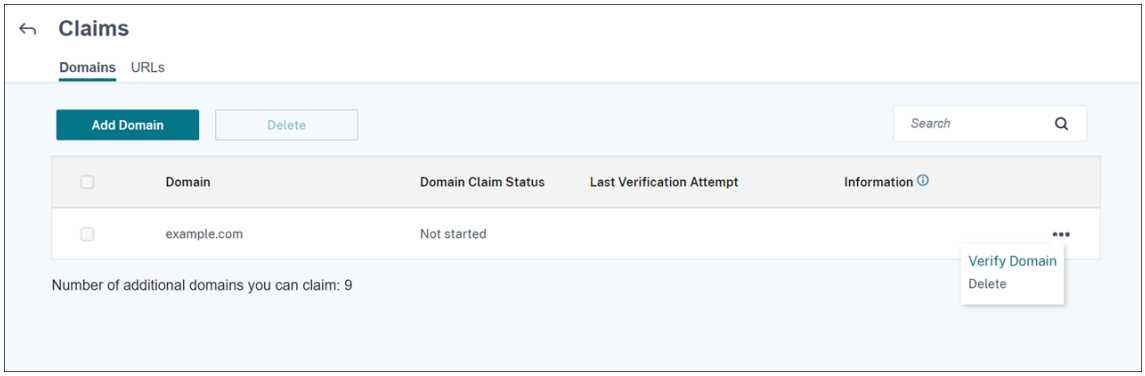
1. ［要求］ > ［ドメイン］タブで、［ドメインの追加］をクリックします。



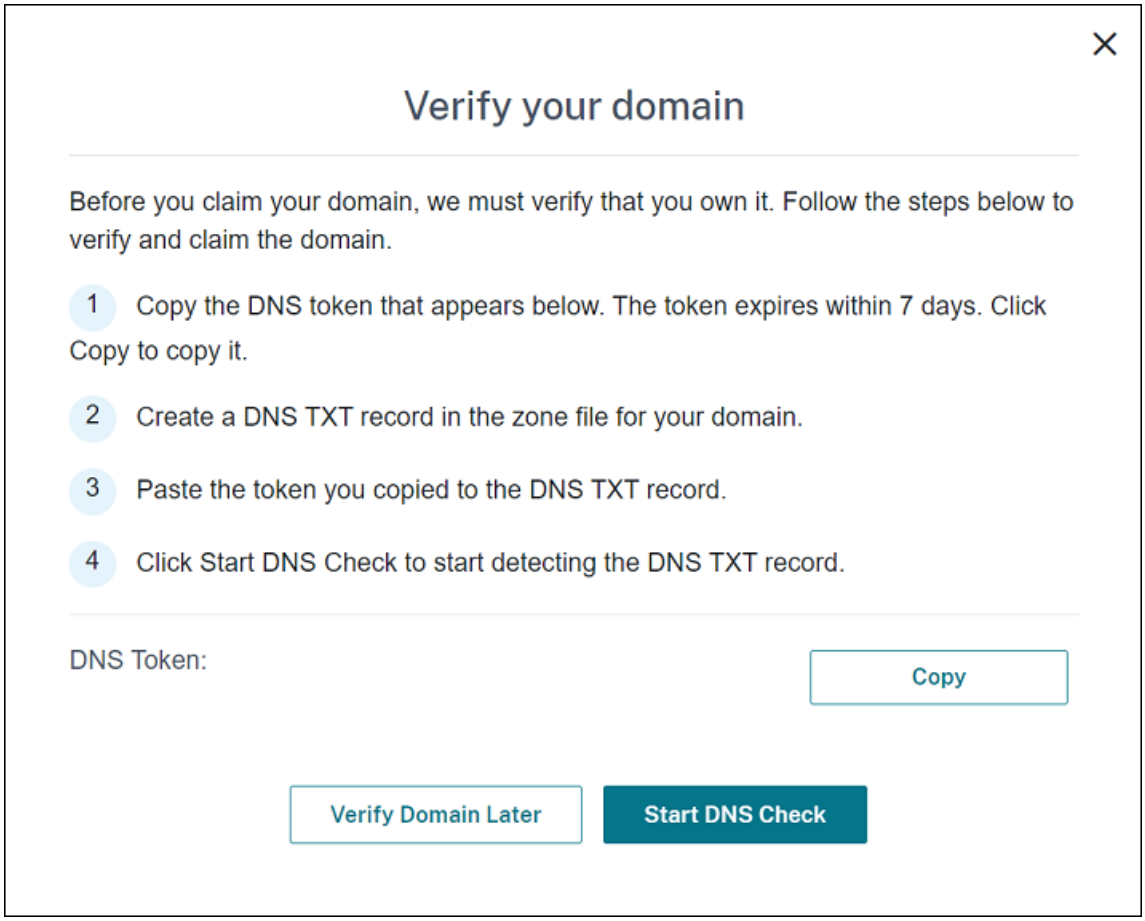
2. 表示されたダイアログボックスで、Citrix Endpoint Management 環境のドメイン名を入力してから ［確認］をクリックします。ドメインは ［要求］ > ［ドメイン］に表示されます。



3. 追加したドメイン上で、省略記号メニューをクリックし、［ドメインの確認］を選択して確認プロセスを開始します。［ドメインの確認］ページが開きます。



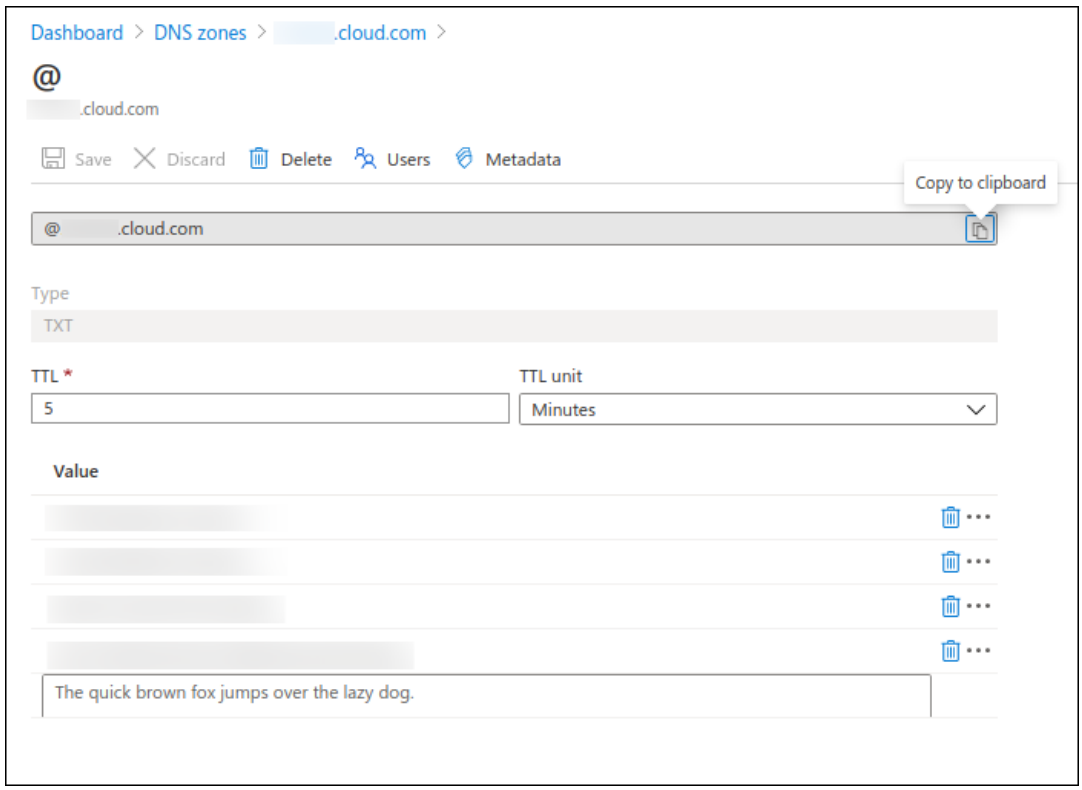
4. [ドメインの確認] ページで、指示に従ってドメインを所有していることを確認します。



a) [コピー] をクリックして、DNS トークンをクリップボードにコピーします。

b) ドメインのゾーンファイルで DNS TXT レコードを作成します。これを行うには、ドメインホスティングプロバイダーポータルに移動し、コピーした DNS トークンを追加します。

次のスクリーンショットは、ドメインホスティングプロバイダーポータルを示しています。ポータルの内容は異なる場合があります。



c) Citrix Cloud の ［ドメインの確認］ページで、［**DNS** チェックの開始］をクリックして、DNS TXT レコードの検出を開始します。後でドメインを確認する場合は、［後でドメインを確認する］をクリックします。

確認プロセスには通常、約 1 時間かかります。ただし、回答が返されるまでに最大で 2 日かかる場合があります。状態チェック中に、ログアウトしてから再度ログインしても問題ありません。

構成が完了すると、ドメインの状態が ［保留中］ > ［確認済］に変わります。

5. ドメインを要求した後に、AutoDiscovery サービス情報を提供します。追加したドメインの省略記号メニューをクリックしてから、[**Citrix Endpoint Management** 情報の追加] をクリックします。[**AutoDiscovery** サービス情報］ページが表示されます。
6. 次の情報を入力してから、［保存］をクリックします。

- **Citrix Endpoint Management** サーバー **FQDN**： Citrix Endpoint Management サーバーの完全修飾ドメイン名を入力します。例: `example.xm.cloud.com`。この設定は、MDM および MAM 制御トラフィックに使用されます。
- **NetScaler Gateway FQDN**： NetScaler Gateway の完全修飾ドメイン名を FQDN 形式または FQDN:port で入力します。例: `example.com`。この設定は、MAM トラフィックをデータセンターに転送するために使用されます。MDM のみの環境の場合、このフィールドは空白のままにします。

> 注:
>
> MAM トラフィックを制御するには、［**NetScaler Gateway FQDN**］の代わりに ［**MAM** ポート］設定を使用することをお勧めします。NetScaler Gateway のポートと共に完全修飾ドメイン名を入力すると、クライアントデバイスは ［**MAM** ポート］設定の構成を使用します。

- インスタンス名: 上記で構成した Citrix Endpoint Management サーバーのインスタンス名を入力します。インスタンス名がわからない場合は、デフォルト値の **zdm** のままにします。
- **MDM** ポート: MDM 制御トラフィックと MDM 登録に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは 443 です。
- **MAM** ポート: MAM 制御トラフィック、MAM 登録、iOS 登録、アプリの列挙に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは 8443 です。

Windows デバイスの **AutoDiscovery** の要請

Windows デバイスを登録する場合は、以下を実行します。

1. Citrix サポートに連絡して、Windows AutoDiscovery の有効化を要求するサポートリクエストを作成します。
2. `enterpriseenrollment.mycompany.com`の公式に署名された、非ワイルドカード SSL 証明書を取得します。ここで、`mycompany.com`部分はユーザーが登録に使用するアカウントが含まれるドメインです。サポートリクエストに前述の手順で作成した.pfx 形式の SSL 証明書とパスワードを添付します。

   複数のドメインを使用して Windows デバイスを登録する場合、以下の構造のマルチドメイン証明書を使用することもできます:

   - 対応するプライマリドメインを指定する、SubjectDN および CN（たとえば、enterpriseenrollment.mycompany1.com）。
   - 残りのドメインの適切な SAN（たとえば、enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.com など）。
3. DNS で正規名（CNAME）レコードを作成し、SSL 証明書のアドレス（enterpriseenrollment.mycompany.com）を autodisc.xm.cloud.com にマップします。

   ユーザーが Windows デバイスの登録時に UPN を使用する場合、Citrix 登録サーバーは以下を行います:

   - Citrix Endpoint Management サーバーの詳細を入力します。
   - デバイスに対して Citrix Endpoint Management の有効な証明書を要求するよう指示します。

この時点で、サポートされているすべてのデバイスを登録できます。次のセクションの手順に従って、リソースをデバイスに配信する準備をします。

Azure AD 条件付きアクセスとの統合

Azure AD 条件付きアクセスサポートを Office 365 アプリケーションに適用するように Citrix Endpoint Management を構成できます。この機能は、Office 365 アプリケーションを展開するときにデバイスユーザーにゼロトラスト手法を展開できます。デバイスの状態、リスクスコア、位置情報、およびデバイス保護を使用して、自動化されたアクションを適用し、管理対象の Android Enterprise および iOS デバイス上の Office 365 アプリケーションへのアクセスを定義できます。

Azure AD デバイスのコンプライアンスを適用するには、個々の Office 365 アプリケーションの条件付きアクセスポリシーを構成する必要があります。管理対象外および非準拠デバイス上の特定の Office 365 アプリケーションへのユーザーアクセスを制限し、管理対象および準拠デバイス上でのみ個々のアプリケーションへのアクセスを許可できます。

前提条件

- この統合には、Intune および Microsoft Office 365 ライセンスなど、有効な Azure AD Premium サブスクリプションが必要です。
- Citrix Secure Hub バージョン 21.4.0 以降
- Azure AD を Citrix Cloud の ID プロバイダー（IDP）として構成してから、Citrix ID を Citrix Endpoint Management の IDP の種類として設定します。詳しくは、「Citrix Cloud を介した Azure Active Directory での認証」を参照してください。
- モバイルアプリケーションが AAD クライアントアプリで認証できるようにするための Citrix マルチテナント AAD アプリケーションへの同意。Azure グローバル管理者が ［ユーザーはアプリケーションを登録できます］の値を ［いいえ］に設定した場合にのみ必要です。この設定は、［**Azure Active Directory**］**>**［ユーザー］**>**［ユーザー設定］の Azure Portal で構成します。同意の提供方法については、「Azure AD コンプライアンス管理用の Citrix Endpoint Management を構成する」を参照してください。
- Azure AD デバイスの登録プロセスを開始する前に、Microsoft Authenticator アプリケーションをデバイスにインストールします。
- Android Enterprise プラットフォームの場合、Web ブラウザーアプリを必要なパブリックストアアプリとして構成します。
- Azure AD コンソールで ［セキュリティの既定値］設定を無効にします。Azure AD 構成を開始すると、セキュリティのデフォルトを、より詳細な Azure AD 条件付きアクセスポリシーに置き換えることができます。セキュリティのデフォルトについて詳しくは、Microsoft のドキュメントを参照してください。

Azure AD 条件付きアクセスポリシーを使用してデバイスコンプライアンスを構成する

Azure AD 条件付きアクセスポリシーを使用してデバイスコンプライアンスを構成する一般的な手順は次のとおりです：

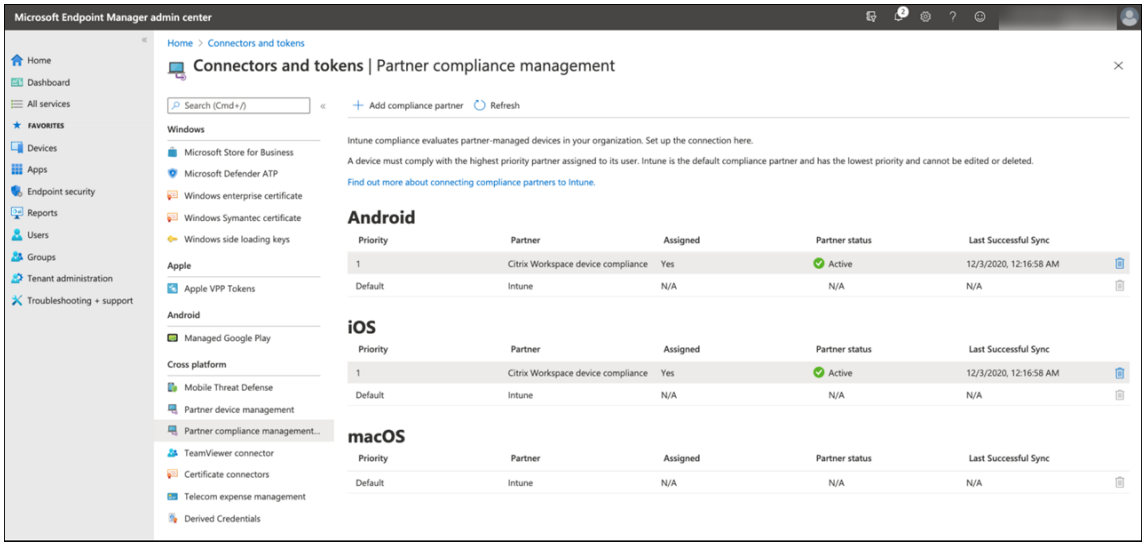
1. **Citrix Endpoint Management** 構成：

- Microsoft Endpoint Manager 管理センターで、**Citrix Workspace** デバイスコンプライアンスを各デバイスプラットフォームのコンプライアンスパートナーとして追加し、ユーザーグループを割り当てます。
- Citrix Endpoint Management で、Microsoft Endpoint Manager 管理センターからの情報を同期します。

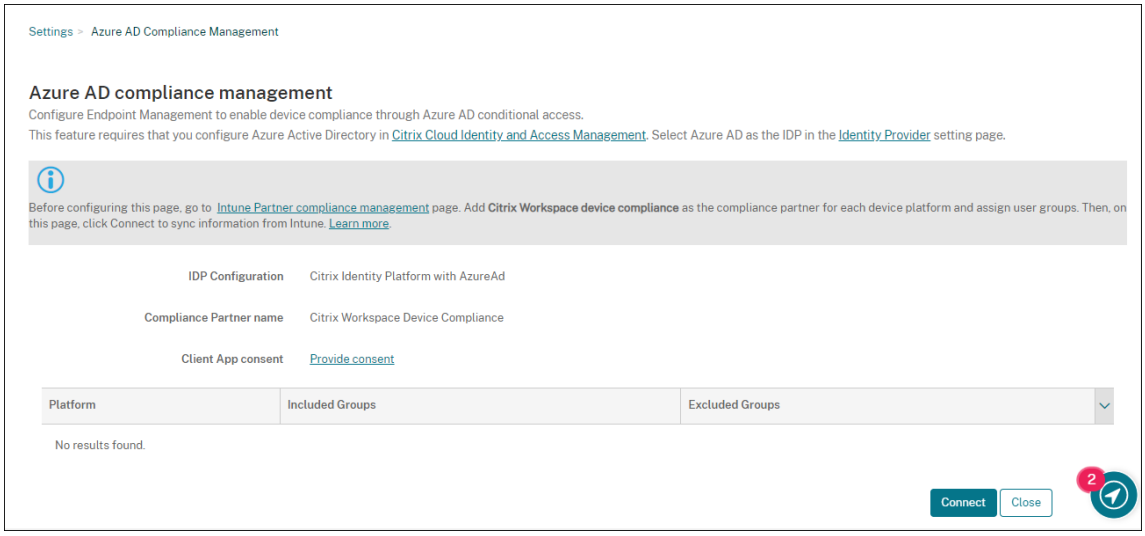
2. **Azure AD** 構成：Azure AD ポータルで、個々の Offic 365 アプリの条件付きアクセスポリシーを設定します。
3. **Citrix Endpoint Management** 構成： Office 365 アプリの条件付きアクセスポリシーを構成した後、Microsoft Authenticator アプリと Office 365 アプリを Citrix Endpoint Management のパブリックアプリストアのアプリとして追加します。これらのパブリックアプリをデリバリーグループに割り当て、必要なアプリとして設定します。

Azure AD コンプライアンス管理用の **Citrix Endpoint Management** を構成する

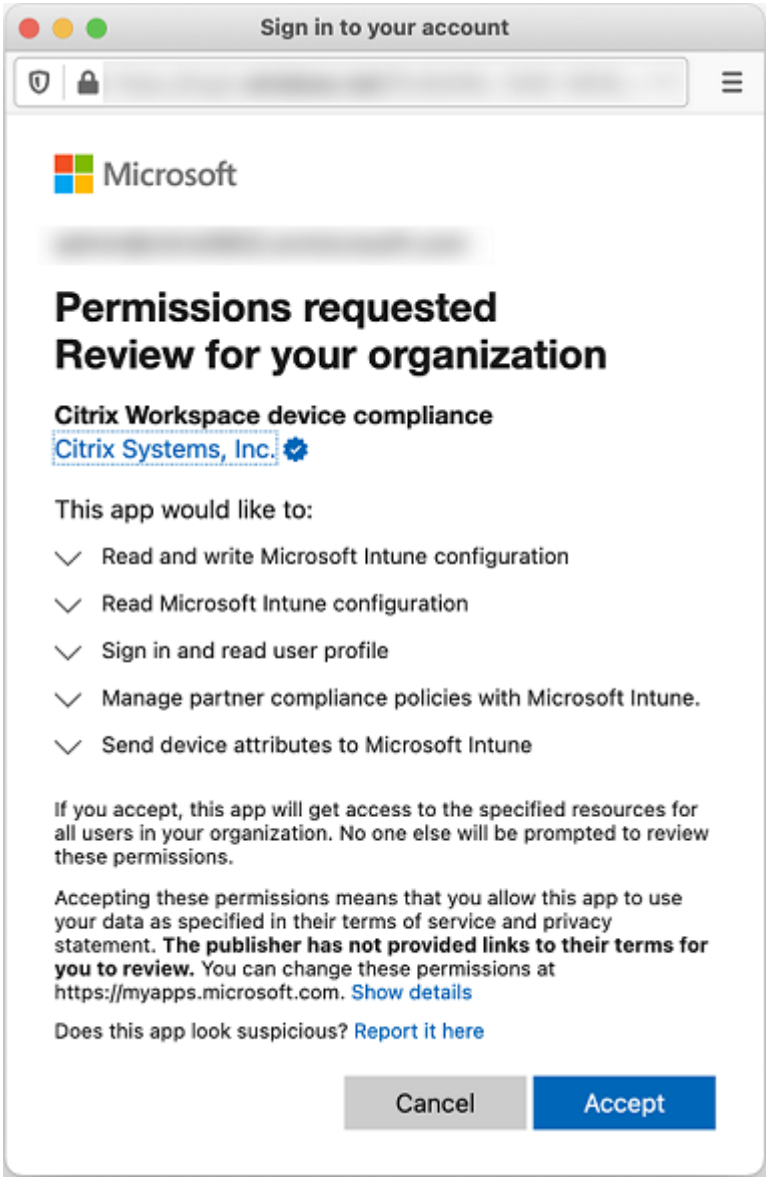
1. Microsoft Endpoint Manager 管理センターにサインインして、［テナント管理］**>**［コネクタとトークン］**>**［デバイスコンプライアンス管理］に移動します。［コンプライアンスパートナーの追加］をクリックし、各デバイスプラットフォームのコンプライアンスパートナーとして **Citrix Workspace** デバイスコンプライアンスを選択します。次に、ユーザーグループを割り当てます。



2. Citrix Endpoint Management で、［設定］**>**［**Azure AD** コンプライアンス管理］に移動します。
3. オプションで、ユーザーが各デバイスで同意する必要がないように、グローバルの同意を設定します。［クライアントアプリの同意］の横にある ［同意する］をクリックします。グローバル管理者の Azure AD 資格情報を入力し、プロンプトに従ってそのクライアントアプリについてグローバルの同意を行います。
4. ［接続］をクリックして、Microsoft Endpoint Manager 管理センターからの情報を同期します。



この構成のアクセス許可を承認するよう求めるダイアログボックスが表示されます。［同意する］をクリックします。構成が完了すると、同期されたデバイスプラットフォームがリストに表示されます。



Azure AD で条件付きアクセスポリシーを構成する

Azure AD ポータルで、Office 365 アプリの条件付きアクセスポリシーを構成して、デバイスコンプライアンスを適用します。[デバイス] **>** [条件付きアクセス] **>** [ポリシー] **>** [新しいポリシー] に移動します。詳しくは、Microsoft 社のドキュメントを参照してください。

Intune 管理対象アプリのデバイスコンプライアンスを構成するには:

- Intune 管理対象アプリをデバイスへの配信用に構成する
- 必要な承認済みクライアントアプリ
- クラウドアプリへのアクセスには、App Protection ポリシーと承認済みクライアントアプリが必要です

Citrix Endpoint Management でアプリを構成する

Office 365 アプリの条件付きアクセスポリシーを構成した後、Microsoft Authenticator アプリと Office 365 アプリを Citrix Endpoint Management のパブリックアプリストアのアプリとして追加します。これらのパブリックアプリをデリバリーグループに割り当て、必要なアプリとして設定します。詳しくは、「パブリックアプリケーションストアのアプリケーションの追加」を参照してください。

ユーザー認証ワークフロー

1. 新しいユーザーは、Azure AD 資格情報を使用してデバイスを Citrix Endpoint Management に登録する必要があります。以前 Azure AD 資格情報で登録したユーザーは、デバイスを再登録する必要はありません。
2. Citrix Endpoint Management は、Microsoft Authenticator と構成済みの Office 365 アプリを必要なアプリとしてデバイスにプッシュします。Android プラットフォームに必要なパブリックストアアプリとして Web ブラウザーアプリを構成した場合、Citrix Endpoint Management はそれをユーザーデバイスにもプッシュします。
3. Citrix Secure Hub は、Citrix Endpoint Management で管理されているすべてのアプリを自動的にインストールして表示します。
4. 利用可能な Office 365 アプリにユーザーがサインインしようとすると、デバイスはユーザーに **Azure AD** 登録リンクをタップして登録プロセスを開始するように求めます。
5. ユーザーが登録リンクをタップすると、Microsoft Authenticator アプリが開きます。ユーザーは Azure AD 資格情報を入力し、デバイスの登録条件に同意します。次に、Microsoft Authenticator アプリが閉じ、Citrix Secure Hub が再び開きます。
6. Citrix Secure Hub は、Azure AD デバイスの登録が完了したことを示すメッセージを表示します。これで、ユーザーは Microsoft アプリを使用してクラウドリソースにアクセスできます。

   登録が完了すると、Azure AD は、コンソールでデバイスを管理対象および準拠としてマークします。

デフォルトのデバイスポリシーおよび業務用モバイルアプリ

Citrix Endpoint Management 19.5.0 以降を使用してオンボードを開始する場合、いくつかのデバイスポリシーと業務用モバイルアプリが事前に構成されています。この構成により、以下を実行できます:

- デバイスに基本機能をすぐに導入できます
- セキュアな Workspace の推奨ベースライン構成を使用して開始できます

Android、Android Enterprise、iOS、macOS、Windows デスクトップ/タブレットプラットフォームの場合、サイトでは次のデバイスポリシーが事前に構成されています:

- パスコードデバイスポリシー: パスコードデバイスポリシーが ［オン］になっていて、すべてのデフォルトのパスコード設定が有効になっています。

- アプリインベントリデバイスポリシー：アプリインベントリデバイスポリシー ［オン］になっています。
- 制限デバイスポリシー：制限デバイスポリシーが ［オン］になっていて、すべてのデフォルトの制限設定が有効になっています。

これらのポリシーは、すべての Active Directory およびローカルユーザーを含む **AllUsers** デリバリーグループに含まれています。AllUsers デリバリーグループは、初期テストにのみ使用することをお勧めします。次に、デリバリーグループを作成し、AllUsers デリバリーグループを無効にします。デリバリーグループで事前構成されたデバイスポリシーやアプリは再利用できます。

すべての Citrix Endpoint Management デバイスポリシーは、「デバイスポリシー」に記載されています。ここでは、コンソールを使用してデバイスポリシーを編集する方法について説明します。すべてのデバイスに共通の一部のデバイスポリシーについて、「デバイスポリシーとユースケースの動作」を参照してください。

サイトには次の事前構成された iOS および Android プラットフォームの業務用モバイルアプリが含まれています：

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

これらのアプリは、**AllUsers** デリバリーグループに含まれています。

詳しくは、「業務用モバイルアプリについて」を参照してください。

Citrix Endpoint Management の構成（続き）

デバイス登録の基本的なセットアップの完了後に Citrix Endpoint Management を構成する方法は、ユースケースにより大きく異なります。例：

- セキュリティ要件は何ですか？ また、セキュリティ要件とユーザーエクスペリエンスとをどのように両立させたいですか？
- どのデバイスプラットフォームをサポートしていますか？
- ユーザー所有のデバイスとコーポレート所有端末のどちらを使用していますか？
- どのデバイスポリシーをデバイスにプッシュしますか？
- ユーザーにどのような種類のアプリを提供していますか？

このセクションでは、製品ドキュメントの各記事にリンクして、多様な構成オプションについて説明します。

サードパーティのサイトでの設定を完了したら、情報とその場所を書き留めて、Citrix Endpoint Management コンソール設定を構成するときに参照してください。

- セキュリティと認証。Citrix Endpoint Management では証明書を使用して、セキュアな接続を作成してユーザーを認証します。Citrix では、Citrix Endpoint Management インスタンスで使用できるワイルドカード証明書を提供しています。

  - 認証コンポーネントセキュリティレベル別に推奨される構成については、「高度な概念」の記事「認証」を参照してください。また、「セキュリティとユーザーエクスペリエンス」も参照してください。
  - Citrix Endpoint Management の運用で使用される認証コンポーネントの概要については、「証明書と認証」を参照してください。
  - 次の種類の認証から選択できます。認証の構成には、Citrix Endpoint Management コンソールおよび NetScaler Gateway コンソールのタスクが含まれます。
    * ドメインまたはドメイン + セキュリティトークン認証
    * クライアント証明書、または証明書とドメイン認証の組み合わせ
  - 証明書をユーザーに配信するには、以下を構成します:
    * PKI エンティティ
    * 資格情報プロバイダー
  - デバイス登録セキュリティモード。デバイス登録セキュリティモードは、資格情報の種類を指定し、ユーザーが Citrix Endpoint Management にデバイスを登録するために必要な登録手順を使用します。詳しくは、「登録セキュリティモードを構成する」を参照してください。
  - ユーザーが Azure Active Directory の資格情報を使用して認証できるようにするには、「Citrix Cloud を介した Azure Active Directory での認証」を参照してください。

- デバイス登録
  - 多数のデバイスを登録するためのプログラムを利用できます:
    * Apple Deployment Program でのデバイスの展開
    * Apple デバイスの一括登録
    * Windows デバイスの一括登録
  - Android デバイスを登録するには、Android Enterprise 管理者アカウントを作成します。「Android Enterprise」を参照してください。または、「Google Workspace ユーザー向けの従来の Android Enterprise」を参照してください。
  - 登録招待状を使用するか、登録の通知を送信できます。
    * 登録招待状。
    * 通知。
  - 登録について詳しくは、「デバイス管理」の記事を参照してください。

- デバイスポリシーと管理
  - デバイス（MDM）ポリシー。すべての Citrix Endpoint Management デバイスポリシーは、「デバイスポリシー」に記載されています。すべてのデバイスに共通の一部のデバイスポリシーについて、「デバイスポリシーとユースケースの動作」を参照してください。

  - 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 Citrix Secure Hub に直接提供される情報が含まれています。「クライアントプロパティ」および「Citrix Endpoint Management クライアントプロパティ」を参照してください。
  - デリバリーグループ。デリバリーグループに関連するサンプルユースケースは、「ユーザーコミュニティ」および「デリバリーグループの追加」を参照してください。

- アプリの展開準備
  - Citrix Endpoint Management でサポートされているアプリについては、「アプリの追加」を参照してください。
  - Apple の一括購入を使用すると、iOS アプリのライセンスを管理することができます。詳しくは、「Apple の一括購入」を参照してください。
  - Citrix Endpoint Management を使用して、Apple の一括購入を介して取得した iBooks を展開することができます。「メディアの追加」を参照してください。
  - Citrix では、Citrix Secure Mail や Citrix Secure Web などの業務用モバイルアプリを提供しています。「業務用モバイルアプリについて」を参照してください。
  - Citrix Secure Mail の代わりに、ネイティブメールをデバイスに配信することができます。次を参照してください:
    * メール戦略
    * Citrix Endpoint Management コネクタ：Exchange ActiveSync 用
    * NetScaler Gateway コネクタ：Exchange ActiveSync 用
  - ユーザーがドキュメントとデータを Microsoft Office 365 アプリにセキュアに転送できるようにするには、「Office 365 アプリとのセキュアな対話式操作の許可」および「Office デバイスポリシー」を参照してください。
  - アプリポリシーについては、「アプリポリシーとユースケースのシナリオ」を参照してください。
  - MDX Toolkit は、Citrix Endpoint Management を使用する安全な展開環境でエンタープライズアプリを準備するためのアプリラッピングテクノロジです。MAM SDK は、MDX Toolkit に代わるものです。MDX Toolkit は、2023 年 7 月に製品終了（EOL）になる予定です。

    MAM SDK について詳しくは、「MAM SDK の概要」を参照してください。
  - アプリについて詳しくは、「アプリの追加」の他の記事を参照してください。

- Citrix Endpoint Management の役割ベースのアクセス制御（Role-Based Access Control：RBAC）機能では、権限の定義済みセットである役割をユーザーとグループに割り当てることができます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。詳しくは、「RBAC を使用した役割の構成」を参照してください。
- Citrix Endpoint Management で自動化された操作を作成して、イベント、特定の設定、またはユーザーデバイスでのアプリの存在に対する対応を指定します。詳しくは、「自動化された操作」を参照してください。

証明書と認証

March 15, 2024

Citrix Endpoint Management の動作では、複数のコンポーネントが認証に関与します:

- **Citrix Endpoint Management**: Citrix Endpoint Management サーバーでは、登録に関するセキュリティと登録の動作を定義します。導入するユーザーの選択肢には次が含まれます:
  - 登録を全員にオープンにするか、または招待のみにするか。
  - 2 要素認証または 3 要素認証を必須にするかどうか。Citrix Endpoint Management のクライアントプロパティを介して、Citrix PIN 認証を有効化して、PIN の複雑度や有効期限を構成できます。
- **NetScaler Gateway**: NetScaler Gateway はマイクロ VPN SSL セッションを終了させます。NetScaler Gateway はネットワーク転送中セキュリティも提供し、ユーザーがアプリにアクセスするたびに使用される認証エクスペリエンスを定義できるようにします。
- **Citrix Secure Hub**: Citrix Secure Hub と Citrix Endpoint Management は、登録操作で連携します。Citrix Secure Hub は NetScaler Gateway と通信するデバイス上のエンティティです。セッションが期限切れになると、Citrix Secure Hub は NetScaler Gateway から認証チケットを取得して、MDX アプリにチケットを渡します。Citrix では中間者攻撃を防げる証明書ピン留めの使用をお勧めします。詳しくは、「Citrix Secure Hub」にある次のセクションを参照してください:「証明書ピンニング」。

  Citrix Secure Hub では MDX セキュリティコンテナも容易になります。Citrix Secure Hub は、ポリシーをプッシュし、アプリがタイムアウトすると NetScaler Gateway でセッションを作成し、MDX タイムアウトおよび認証エクスペリエンスを定義します。Citrix Secure Hub は、ジェイルブレイク検出、地理位置情報チェック、および適用するすべてのポリシーを担当します。
- **MDX** ポリシー: MDX ポリシーは、デバイス上にデータ格納場所を作成します。MDX ポリシーは、マイクロ VPN 接続に NetScaler Gateway を参照させ、オフラインモード制限を強制し、タイムアウトなどのクライアントポリシーを強制します。

Citrix Endpoint Management は、次の認証方法を使用して、リソースに対してユーザーを認証します:

- モバイルデバイス管理（MDM）
  - クラウドでホストされる ID プロバイダー（IdP）
  - ライトウェイトディレクトリアクセスプロトコル（LDAP）
    - 招待 URL および PIN
    - 2 要素認証
- モバイルアプリケーション管理（MAM）
  - LDAP
  - 証明書

- セキュリティトークン
  MAM 認証には NetScaler Gateway が必要です。

そのほかの構成について詳しくは、以下の記事を参照してください。

- 証明書のアップロード、アップデート、および更新
- NetScaler Gateway と Citrix Endpoint Management
- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- PKI エンティティ
- 資格情報プロバイダー
- APNs 証明書
- Citrix Files での SAML によるシングルサインオン
- Citrix Cloud を介した Azure Active Directory での認証
- Citrix Cloud を介した Okta での認証
- Citrix Cloud を介したオンプレミスの NetScaler Gateway での認証
- Wi-Fi サーバーを認証するには、証明書をデバイスに送信します：ネットワークデバイスポリシー
- 内部ルート証明機関（CA）証明書などのような認証や、特定のポリシーに使用されない一意の証明書をプッシュする場合：資格情報デバイスポリシー

証明書

Citrix Endpoint Management では、サーバーへの通信フローを保護するため、インストール中に自己署名 SSL（Secure Sockets Layer）証明書が生成されます。この SSL 証明書を、既知の CA（Certificate Authority：証明機関）からの信頼される SSL 証明書に置き換えます。

Citrix Endpoint Management はまた、独自の PKI（Public Key Infrastructure：公開キー基盤）サービスを使用するか、CA からクライアント証明書を取得します。すべての Citrix 製品でワイルドカード証明書と SAN（Subject Alternative Name：サブジェクトの別名）証明書がサポートされます。ほとんどの展開では、2 つのワイルドカード認証または SAN 認証のみが必要です。

クライアント証明書認証を使用するとモバイルアプリのセキュリティが強化され、ユーザーはシームレスに HDX アプリにアクセスできます。クライアント証明書認証が構成されている場合、ユーザーは Citrix Endpoint Management 準拠アプリへのシングルサインオン（SSO）アクセスには Citrix PIN を入力します。また Citrix PIN により、ユーザー認証工程が簡素化されます。Citrix 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。

Citrix Endpoint Management で iOS デバイスを登録して管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書を設定および作成します。手順については、「APNs 証明書」を参照してください。

次の表は、各 Citrix Endpoint Management コンポーネントの証明書の形式と種類を示しています：

Citrix Endpoint Management コンポーネント	証明書の形式	必要な証明書の種類
NetScaler Gateway	PEM（BASE64）、PFX（PKCS # 12）	SSL、ルート（NetScaler Gateway によって自動的に PFX が PEM に変換されます）。
Citrix Endpoint Management	.p12（Windows ベースのコンピューターの.pfx）	SSL、SAML、APN（Citrix Endpoint Management はインストール処理中に完全な PKI も生成します）重要： Citrix Endpoint Management では、拡張子「.pem」の証明書はサポートされません。.pem 証明書を使用するには、.pem ファイルを証明書とキーに分割し、それぞれを Citrix Endpoint Management にインポートします。
StoreFront	PFX（PKCS#12）	SSL、ルート

Citrix Endpoint Management はクライアント証明書をサポートします。ビット長は 4096 および 2048 です。

NetScaler Gateway および Citrix Endpoint Management の場合は、Verisign、DigiCert、Thawte などの商用 CA からサーバー証明書を取得することをお勧めします。NetScaler Gateway または Citrix Endpoint Management 構成ユーティリティから証明書署名要求（Certificate Signing Request：CSR）を作成できます。CSR の作成後、CA へ署名のために送信します。CA から署名入り証明書を受け取ったら、NetScaler Gateway または Citrix Endpoint Management に証明書をインストールできます。

> 重要：
>
> iOS、iPadOS、および macOS での信頼された証明書の要件
>
> Apple は、TLS サーバー証明書の新しい要件を設定しています。すべての証明書が Apple の要件に準拠していることを確認します。アップルの出版物である「https://support.apple.com/en-us/HT210176」を参照してください。
>
> Apple は TLS サーバー証明書の最大許容有効期間を短縮しています。この変更は、2020 年 9 月以降に発行されたサーバー証明書にのみ影響します。アップルの出版物である「https://support.apple.com/en-us/HT211025」を参照してください。

LDAP 認証

Citrix Endpoint Management は、LDAP（Lightweight Directory Access Protocol）に準拠している 1 つまたは複数のディレクトリに対するドメインベースの認証をサポートしています。LDAP は、グループ、ユーザーアカウ

ント、および関連するプロパティに関する情報へのアクセスを提供するソフトウェアプロトコルです。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。

ID プロバイダー認証

Citrix Cloud を介して ID プロバイダー（IdP）を構成し、ユーザーデバイスを登録および管理できます。

IdP でサポートされるユースケース:

- Citrix Cloud を介した Azure Active Directory
  - Workspace 統合はオプションです
  - 証明書ベースの認証で構成された NetScaler Gateway
  - Android Enterprise（プレビュー。BYOD（Bring Your Own Device）、完全管理対象デバイス、拡張された登録プロファイルをサポートします）
  - MDM+MAM 登録および MDM 登録用の iOS
  - Apple Business Manager 登録用の iOS および macOS
  - 従来の Android（DA）

  Apple School Manager などの自動登録機能は、現在サポートされていません。
- Citrix Cloud を介した Okta
  - Workspace 統合はオプションです
  - 証明書ベースの認証で構成された NetScaler Gateway
  - Android Enterprise（プレビュー。BYOD（Bring Your Own Device）、完全管理対象デバイス、拡張された登録プロファイルをサポートします）
  - MDM+MAM 登録および MDM 登録用の iOS
  - Apple Business Manager 登録用の iOS および macOS
  - 従来の Android（DA）

  Apple School Manager などの自動登録機能は、現在サポートされていません。
- Citrix Cloud を介したオンプレミスの NetScaler Gateway
  - 証明書ベースの認証で構成された NetScaler Gateway
  - Android Enterprise（プレビュー。BYOD（Bring Your Own Device）、完全管理対象デバイス、拡張された登録プロファイルをサポートします）
  - MDM+MAM 登録および MDM 登録用の iOS
  - 従来の Android（DA）

    Apple Deployment Program などの自動登録機能は、現在サポートされていません。

証明書のアップロード、アップデート、および更新

March 15, 2024

Citrix Endpoint Management の展開に必要な証明書を一覧化することをお勧めします。一覧を使用して、証明書の有効期限とパスワードを追跡します。この記事は、証明書の存続期間を通じて証明書を管理するのに役立ちます。

ご使用の環境には以下の証明書が含まれている可能性があります:

- Citrix Endpoint Management サーバー
  - MDM FQDN の SSL 証明書（XenMobile Server から Citrix Endpoint Management に移行した場合に必要です。それ以外の場合は、Citrix がこの証明書を管理します）
  - SAML 証明書（Citrix Files 用）
  - 上記証明書およびその他の内部リソース（StoreFront やプロキシなど）用のルート CA 証明書と中間 CA 証明書
  - iOS デバイス管理用の APNs 証明書
  - PKI に接続するための PKI ユーザー証明書（ご使用の環境で証明書ベースの認証が必要な場合に必須）
- MDX Toolkit
  - Apple Developer 証明書
  - Apple プロビジョニングプロファイル（アプリケーションごと）
  - Apple APNS 証明書（Citrix Secure Mail で使用）
  - Android キーストアファイル

  MAM SDK はアプリをラップしないため、証明書は必要ありません。
- Citrix Gateway
  - MDM FQDN の SSL 証明書
  - Gateway FQDN の SSL 証明書
  - ShareFile SZC FQDN の SSL 証明書
  - Exchange 負荷分散用の SSL 証明書（オフロード構成）
  - StoreFront 負荷分散用の SSL 証明書
  - 上記証明書のルート証明書および中間 CA 証明書

> 注:
>
> クライアントデバイスには、サーバー証明書を発行した証明機関との信頼を確立するために必須のルート証明書または中間証明書が必要です。これらがない場合、SSL エラー 61 が発生することがあります。この問題を解決するには、次の手順に従います。
>
> 1. SSL 証明書プロバイダーが発行した SSL ルート/中間証明書ファイル（.crt または.cer）をダウンロードまたは取得します。通常、ルート証明書、中間証明書、またはサーバー証明書は、SSL サービスプロバイ

> ダーによって提供される証明書バンドルに存在します。
> 2. クライアントデバイスにルート証明書または中間証明書をインストールします。
> 3. クライアントデバイスにウイルス対策ソフトウェアがインストールされている場合は、このソフトウェアが証明書を信頼していることを確認します。

証明書のアップロード

アップロードする各証明書は、［証明書］の表で 1 つのエントリを持ち、その内容がまとめられています。証明書が必要な PKI 統合コンポーネントを構成するときは、条件を満たすサーバー証明書を選択します。たとえば、Citrix Endpoint Management を Microsoft 証明機関（CA）と統合するように構成する場合があります。Microsoft CA への接続はクライアント証明書を使用して認証されます。

Citrix Endpoint Management は、特定の証明書に対して秘密キーを所有しない場合があります。同様に、Citrix Endpoint Management は、アップロードされた証明書に対して秘密キーを要求しない場合があります。

このセクションでは、証明書をアップロードする一般的な手順について説明します。クライアント証明書の作成、アップロード、構成について詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。

証明書をアップロードするには、次の 2 つの方法があります：

- コンソールに証明書を個別にアップロードする。
- REST API を使用して証明書を一括でアップロードする。このオプションは iOS デバイスでのみ使用できます。

コンソールに証明書をアップロードする場合、次のことができます：

- キーストアをインポートします。次にインストールするキーストアリポジトリのエントリを識別します（PKCS#12 形式をアップロードする場合を除く）。
- 証明書をインポートします。

CA がリクエストに署名するときに使用する（秘密キーなしの）CA 証明書をアップロードすることができます。クライアント認証用の（秘密キー付きの）SSL クライアント証明書をアップロードすることもできます。

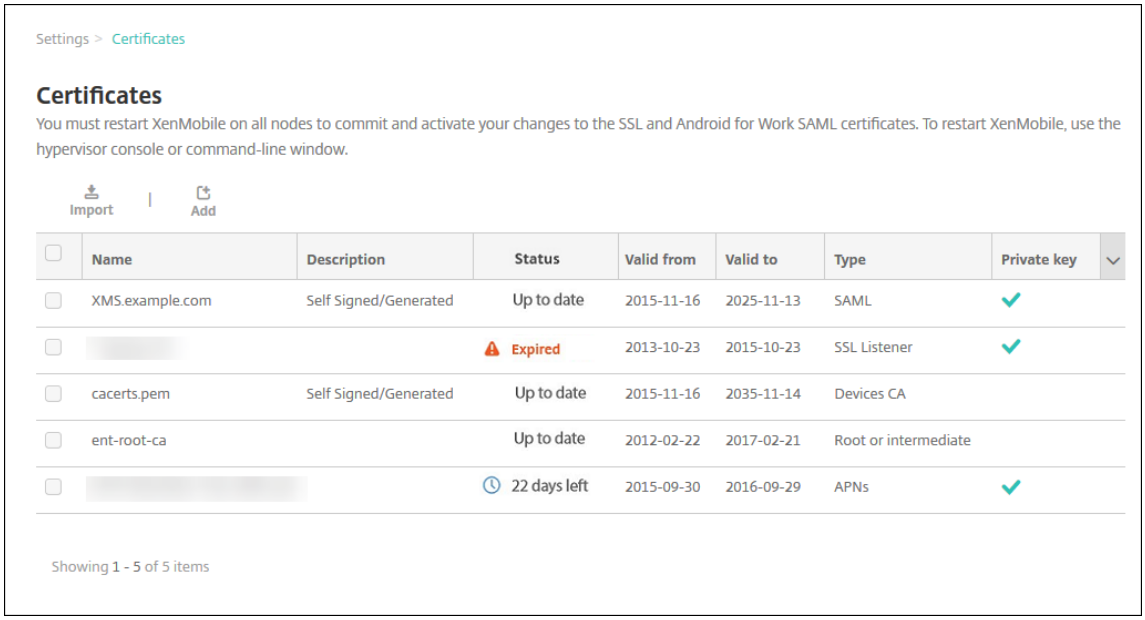
Microsoft CA エンティティを構成する場合は、CA 証明書を指定します。CA 証明書であるすべてのサーバー証明書の一覧から CA 証明書を選択します。同様に、クライアント認証を構成する場合は、Citrix Endpoint Management が秘密キーを持っているすべてのサーバー証明書の一覧から選択できます。

キーストアをインポートするには

キーストアは、セキュリティ証明書のリポジトリです。設計上、キーストアには複数のエントリを含めることができます。このため、キーストアから読み込むときに、読み込むエントリを識別するエントリのエイリアスを指定する必要があります。エイリアスを指定しない場合、ストアの最初のエントリが読み込まれます。PKCS#12 ファイルに含

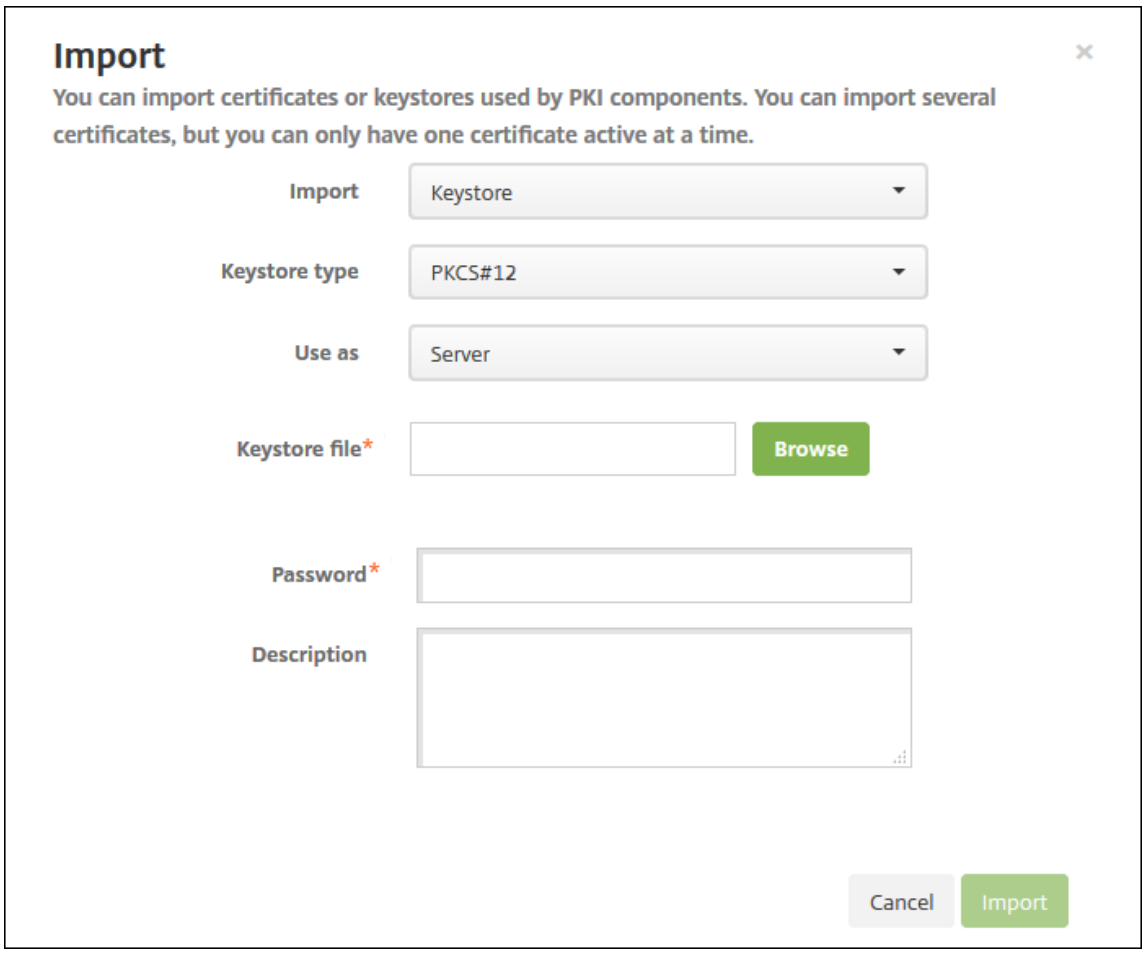
まれるエントリは通常 1 つだけであるため、キーストアの種類として PKCS#12 を選択した場合、エイリアスフィールドは表示されません。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。検索バーを使用して、［証明書］設定を見つけて開きます。



2. ［インポート］をクリックします。［インポート］ダイアログボックスが開きます。
3. 次の設定を構成します：

   - インポート：［キーストア］を選択します。



- キーストアの種類：ボックスの一覧から、［**PKCS#12**］を選択します。
- 使用目的：一覧から、証明書の使用方法を選択します。以下の種類から選択できます。
  - サーバー：サーバー証明書は Citrix Endpoint Management で機能上使用される証明書です。サーバー証明書を Citrix Endpoint Management Web コンソールにアップロードします。これらの証明書には、CA 証明書、RA 証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。これは特に、デバイスで信頼性を確立するために使用される CA に適用されます。
  - **SAML**：セキュリティアサーションマークアップランゲージ（Security Assertion Markup Language：SAML）証明書を使用すると、サーバー、Web サイト、およびアプリへの SSO アクセスを提供できます。
  - **APN**： Apple の APNs 証明書を使用すると、Apple Push Network を使用してモバイルデバイスを管理できます。
  - **SSL** リスナー： SSL（Secure Sockets Layer）リスナーは、Citrix Endpoint Management に SSL 暗号化アクティビティを通知します。
- キーストアファイル：インポートするキーストアを参照して見つけます。キーストアは.p12 または.pfx ファイルです。ファイルを選択して、［**Open**］をクリックします。

- パスワード：証明書に割り当てられたパスワードを入力します。
- 説明：任意で、キーストアの説明を入力します。この説明は、ほかのキーストアと区別するときに役立ちます。

4. ［インポート］をクリックします。キーストアが［証明書］の表に追加されます。

証明書をインポートするには

証明書をインポートするときに、Citrix Endpoint Management は入力から証明書チェーンの作成を試行します。Citrix Endpoint Management はそのチェーンのすべての証明書をインポートして、各証明書のサーバー証明書エントリを作成します。この操作は、ファイルまたはキーストアエントリの証明書がチェーンを形成する場合にのみ機能します。チェーン内の連続する各証明書は、前の証明書の発行者である必要があります。

インポートされた証明書にオプションで説明を追加できます。説明はチェーンの 1 つ目の証明書にのみ追加されます。ほかの証明書の説明は後から更新できます。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。検索バーを使用して、［証明書］設定を見つけて開きます。
2. ［証明書］ページで ［インポート］をクリックします。［インポート］ダイアログボックスが開きます。次のオプションを構成します：

   - インポート：［証明書］をクリックします。
   - 使用目的：証明書の使用方法を選択します。以下の種類から選択できます。
     - サーバー：サーバー証明書は Citrix Endpoint Management で機能上使用される証明書です。サーバー証明書を Citrix Endpoint Management Web コンソールにアップロードします。これらの証明書には、CA 証明書、RA 証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。このオプションは特に、デバイスで信頼性を確立するために使用される CA に適用されます。
     - **SAML**：セキュリティアサーションマークアップランゲージ（SAML）証明書を使用すると、サーバー、Web サイト、およびアプリへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
     - **SSL** リスナー： SSL（Secure Sockets Layer）リスナーは、Citrix Endpoint Management に SSL 暗号化アクティビティを通知します。
   - 証明書のインポート：インポートする証明書を参照して指定します。ファイルを選択して、［**Open**］をクリックします。
   - 秘密キーファイル：任意で、証明書の秘密キーファイルを参照して指定します。秘密キーは、証明書と共に暗号化と復号化で使用されます。ファイルを選択して、［**Open**］をクリックします。
   - 説明：任意で、証明書の説明を入力します。この説明は、ほかの証明書と区別するときに役立ちます。

3. ［インポート］をクリックします。証明書が［証明書］の表に追加されます。

REST API を使用した証明書の一括アップロード　証明書を一度に 1 つずつアップロードすることが合理的ではない場合もあります。そのような場合は、REST API を使用して証明書の一括アップロードを実行します。この方法は、.p12 形式の証明書をサポートします。REST API について詳しくは、「REST API」を参照してください。

1. 各証明書ファイルの名前を、device_identity_value.p12の形式に変更します。device_identity_valueは、各デバイスの IMEI、シリアル番号、または MEID です。

   例として、識別方法としてシリアル番号を使用するとします。あるデバイスのシリアル番号がA12BC3D4EFGHであれば、そのデバイスにインストールする証明書ファイルにA12BC3D4EFGH.p12という名前を付けます。

2. .p12 証明書のパスワードを保存するテキストファイルを作成します。そのファイルで、新しい行に各デバイスのデバイス識別子とパスワードを入力します。device_identity_value=passwordの形式を使用します。以下を参照してください:

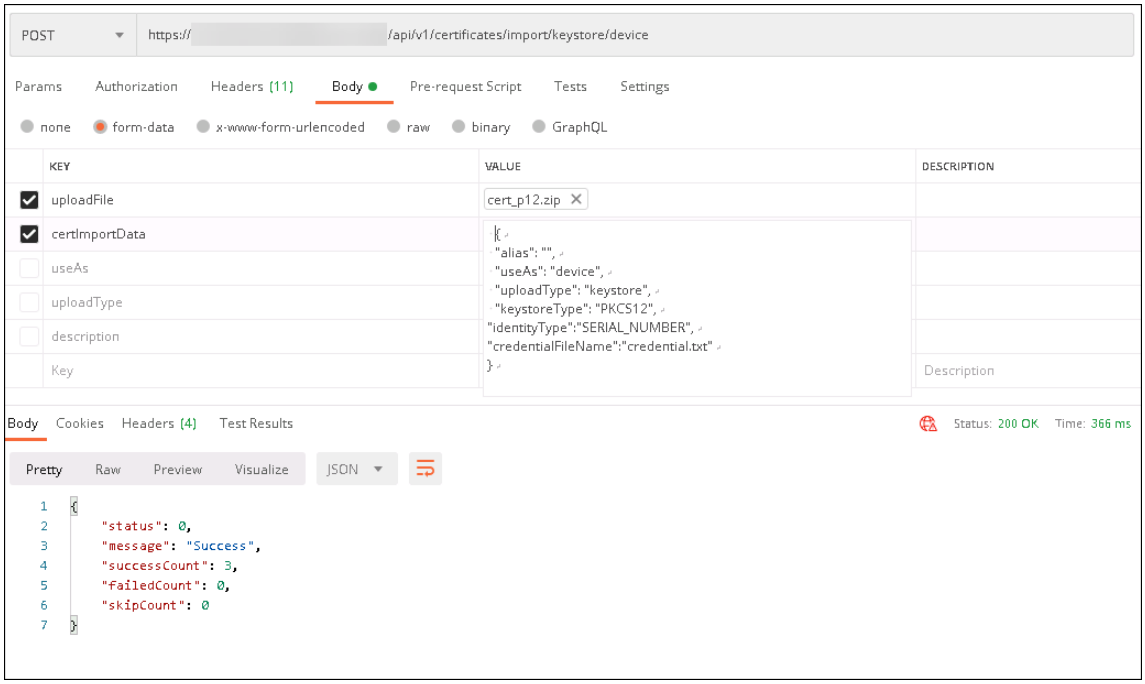
   ```
   A12BC3D4EFGH.p12=password1!
   A12BC3D4EFIJ.p12=password2@
   A12BC3D4EFKL.p12=password3#
   <!--NeedCopy-->
   ```

3. 作成したすべての証明書とテキストファイルを.zip ファイルに入れます。

4. REST API クライアントを起動し、Citrix Endpoint Management にログインして、認証トークンを取得します。

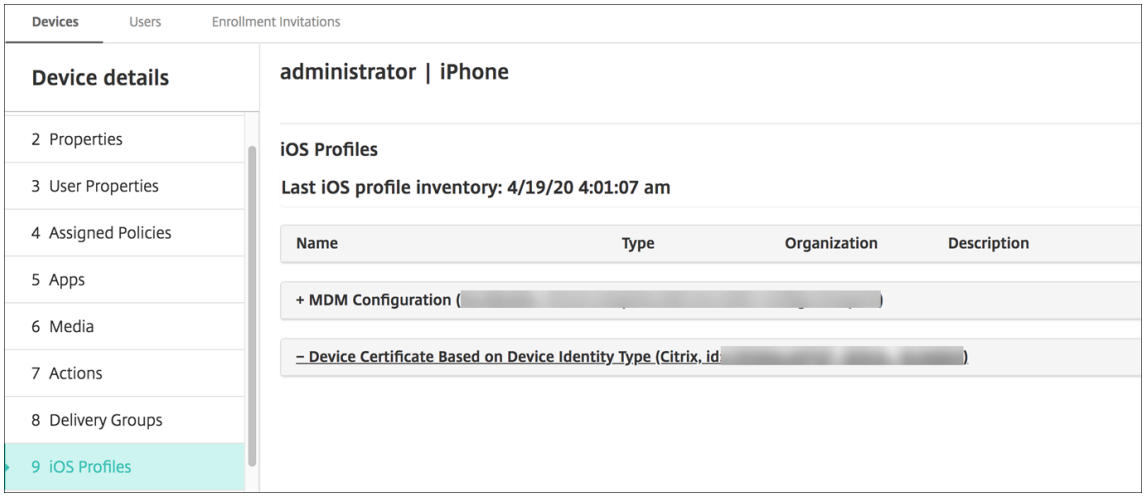
5. 証明書をインポートし、メッセージ本文に次の情報を入力してください:

   ```
   {

       "alias": "",
       "useAs": "device",
       "uploadType": "keystore",
       "keystoreType": "PKCS12",
       "identityType":"SERIAL_NUMBER",         # identity type can be
          "SERIAL_NUMBER","IMEI","MEID"
       "credentialFileName":"credential.txt"    # The credential file
          name in .zip
    }

   <!--NeedCopy-->
   ```

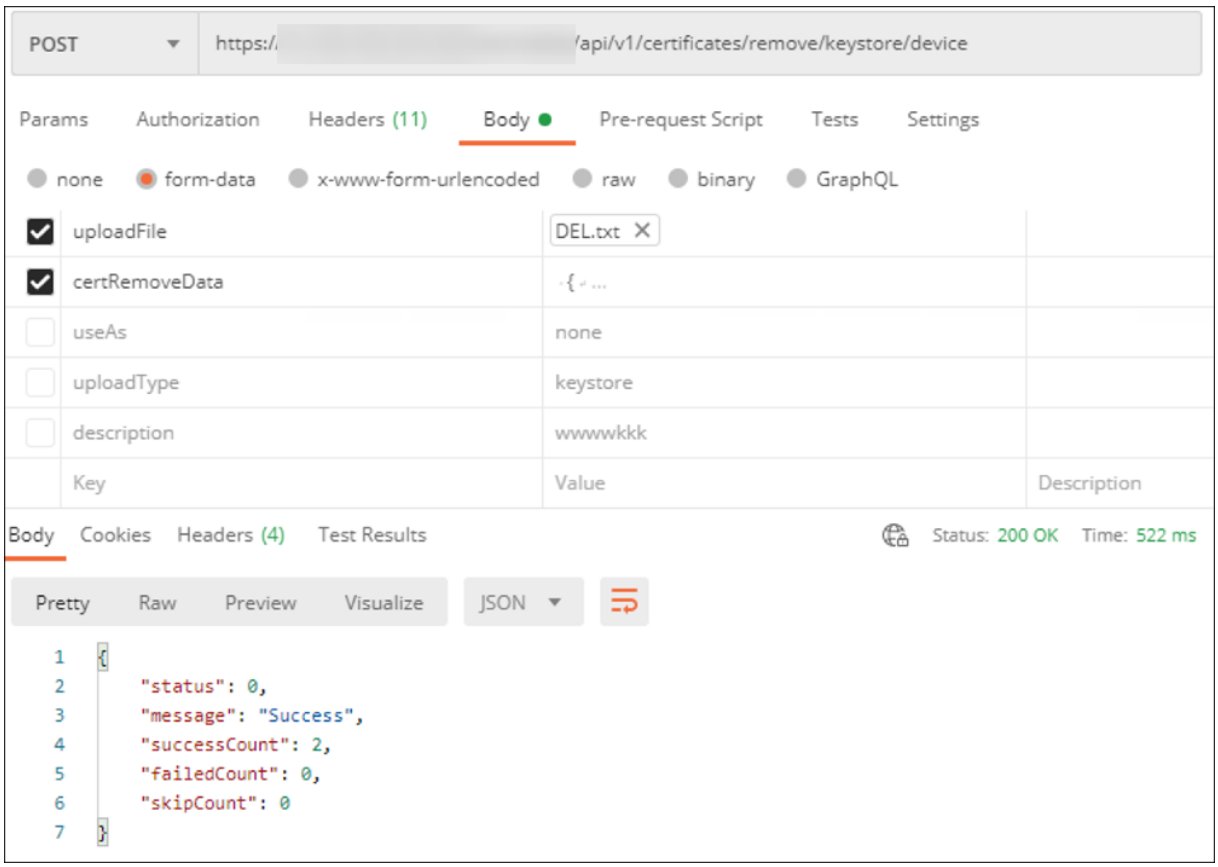
6. 資格情報タイプに ［**Always on IKEv2**］、およびデバイス認証方法に ［デバイス **ID** ベースのデバイス証明書］を使用して VPN ポリシーを作成します。証明書ファイル名で使用した ［デバイス **ID** の種類］を選択します。「VPN デバイスポリシー」を参照してください。

7. iOS デバイスを登録し、VPN ポリシーが展開されるのを待ちます。デバイスの MDM 構成をチェックして、証明書のインストールを確認します。Citrix Endpoint Management コンソールでデバイスの詳細を確認することもできます。



削除する証明書ごとにdevice_identity_valueが一覧表示されたテキストファイルを作成して、証明書を一括で削除することもできます。REST API で削除 API を呼び出し、次のリクエストを使用して、device_identity_valueを適切な識別子に置き換えます:

```
1 ```
2 {
3
4     "identityType"="device_identity_value"
5  }
6
7 <!--NeedCopy--> ```
```

証明書の更新

Citrix Endpoint Management で同時に存在できるのは 1 つの公開キーにつき 1 つの証明書のみです。既にインポートされている証明書と同じキーペアの証明書をインポートしようとする場合、以下を実行できます:

- 既存のエントリを置き換える。
- エントリを削除する。

新しい証明書をアップロードして古い証明書を置き換えた後、古い証明書を削除することはできません。PKI エンティティ設定を構成すると、[**SSL** クライアント証明書] メニューに両方の証明書が表示されます。新しい証明書は、古い証明書よりも一覧の下に表示されます。

証明書を更新するには

1. 「クライアント証明書、または証明書とドメイン認証の組み合わせ」の手順に従って、代わりの証明書を作成します。

   > 重要:
   >
   > 既存の秘密キーを使用して証明書を作成するために、このオプションを使用しないでください。有効期

> 限が切れる証明書を更新するために証明書を作成する場合、秘密キーも新しくする必要があります。

2. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。検索バーを使用して、［証明書］設定を見つけて開きます。
3. ［インポート］ダイアログボックスで、新しい証明書をインポートします。

サーバー証明書を更新すると、以前の証明書を使用していたコンポーネントが新しい証明書を使用するように自動的に切り替わります。同様に、デバイスにサーバー証明書を展開している場合、証明書は次回展開するときに自動的に更新されます。

APNs 証明書を更新するには、証明書を作成する手順を実行してから、Apple Push Certificates Portal にアクセスします。詳しくは、「APN 証明書の更新」を参照してください。

Citrix Gateway で SSL オフロードが設定されている場合は、必ず新しい cacert.pem を使ってロードバランサーを更新してください。

> 注:
>
> オンプレミスの XenMobile から Citrix Endpoint Management に移行し、証明書を更新する場合は、ここまでの手順を完了した後、Citrix サポートに連絡してください。証明書のパスワードを含む新しい証明書（PFX 形式）のコピーを提供する必要があります。Citrix サポートは、クラウドの NetScaler を更新し、テナントノードを再起動して、証明書の更新プロセスを完了します。

PKI サービス証明機関（**CA**）を更新するには

Citrix Endpoint Management 展開で内部的に PKI のための証明機関（CA）を更新または再生成するように Citrix Cloud Operations に要求できます。この要求については、テクニカルサポートケースを開いてください。

```
When the new CAs are available, Cloud Operations lets you know that you
    can proceed with renewing the device certificates for your users.
```

デバイス証明書の更新

デバイスで証明書の有効期限が切れると、証明書が無効になります。環境で安全なトランザクションを実行することや、Citrix Endpoint Management リソースにアクセスすることができなくなります。有効期限前に、証明機関（CA）から SSL 証明書を更新するよう求められます。前述の手順を実行して証明書を更新してから、登録済みのデバイスで証明書の更新を開始します。

サポートされている iOS、macOS、および Android デバイスの場合、［セキュリティ操作］から［証明書の書き換え］を使用して証明書の書き換えを開始することができます。Citrix Endpoint Management コンソールまたはパブリック REST API からデバイス証明書を書き換えます。登録済み Windows デバイスの場合、ユーザーは新しいデバイス証明機関（CA）を受信するためにデバイスを再登録する必要があります。

次回デバイスが Citrix Endpoint Management に接続すると、Citrix Endpoint Management サーバーは新しい CA に基づいて新しいデバイス証明書を発行します。

コンソールを使用してデバイス証明書を書き換えるには

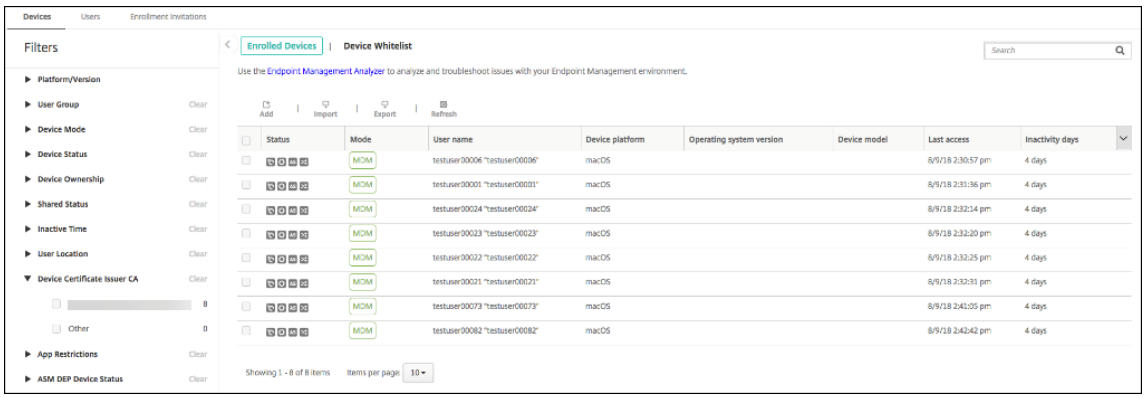
1. ［管理］ **>** ［デバイス］に移動して、証明書を書き換えるデバイスを選択します。
2. ［保護］をクリックし、［証明書の書き換え］をクリックします。

登録済みのデバイスは、中断することなく動作し続けます。Citrix Endpoint Management は、デバイスがサーバーに再度接続するときにデバイス証明書を発行します。

特定のデバイス証明書発行者 CA グループ内にあるデバイスのクエリを実行するには:

1. ［管理］ **>** ［デバイス］で、フィルターペインを展開します。
2. フィルターペインで、［デバイス証明書発行者 **CA**］を展開し、書き換える発行元 CA を選択します。

   デバイステーブルに、選択した発行元 CA のデバイスが表示されます。



REST API を使用してデバイス証明書を書き換えるには

Citrix Endpoint Management は、内部的に PKI のために次の認証機関を使用します: ルート CA、デバイス CA、およびサーバー CA。これらの CA は論理グループであり、グループ名を持っています。Citrix Endpoint Management のプロビジョニング中、サーバーは 3 つの CA を生成し、グループ名を「デフォルト」にします。

CA は以下の API を発行して、デバイス証明書の管理および書き換えを行います。既に登録済みのデバイスは、中断することなく動作し続けます。Citrix Endpoint Management は、デバイスがサーバーに再度接続するときにデバイス証明書を発行します。詳しくは、『Public API for REST Services』（PDF）をダウンロードしてください。

- 古い CA をまだ使用しているデバイスのリストを返す（『Public API for REST Services』（PDF）のセクション 3.16.2 を参照）
- デバイス証明書を書き換える（セクション 3.16.58 を参照）
- すべての CA グループを取得する（セクション 3.23.1 を参照）

Citrix Secure Mail の **APNs** 証明書

Apple プッシュ通知サービス（APNs）証明書は毎年有効期限が切れます。証明書の有効期限が切れる前に、APNs SSL 証明書を作成し、Citrix ポータルで証明書を更新してください。証明書の期限が切れた場合、Citrix Secure Mail プッシュ通知に一貫性がなくなります。また、アプリのプッシュ通知を送信することもできなくなります。

iOS デバイス管理用の **APNs** 証明書

Citrix Endpoint Management で iOS デバイスを登録して管理するには、Apple の APNs 証明書を設定および作成します。証明書の期限が切れた場合、Citrix Endpoint Management に登録したり、iOS デバイスを管理したりできなくなります。詳しくは、「APNs 証明書」を参照してください。

Apple Push Certificates Portal にログオンして、APNs 証明書のステータスと有効期限を表示できます。証明書を作成した時と同じユーザー名でログオンするようにしてください。

また、有効期限の 30 日前と 10 日前に、Apple からメール通知を受信します。この通知には、次の情報が含まれます:

```
The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR),
    then visit https://identity.apple.com/pushcert to renew your Apple
    Push Notification Service certificate.

Thank You,

Apple Push Notification Service
<!--NeedCopy-->
```

MDX Toolkit（**iOS** 配布証明書）

物理的な iOS デバイス（Apple App Store のアプリ以外）上で実行するアプリの署名要件は次のとおりです:

- プロビジョニングプロファイルでアプリに署名します。
- 対応する配布用証明書でアプリに署名します。

有効な iOS 配布証明書があるかを確認するには、以下の操作を行います:

1. Apple Enterprise Developer ポータルから、MDX でラップする各アプリで新しいプロビジョニングプロファイルと一意で明示的な App ID を作成します。有効な App ID の例: `com.CompanyName.ProductName`
2. Apple Enterprise Developer ポータルから、[**Provisioning Profiles**] > [**Distribution**] に移動して、社内プロビジョニングプロファイルを作成します。前述の手順で作成された App ID ごとに、この手順を繰り返します。
3. すべてのプロビジョニングプロファイルをダウンロードします。詳しくは、「iOS モバイルアプリのラップ」を参照してください。

すべての Citrix Endpoint Management サーバー証明書が有効であることを確認するには、以下の操作を行います:

1. Citrix Endpoint Management コンソールで、[設定] > [証明書] の順にクリックします。
2. APNs 証明書、SSL 証明書、リスナー証明書、ルート証明書、中間証明書を含むすべての証明書が有効であることを確認してください。

Android キーストア

キーストアは Android アプリに署名するために使用する証明書を含むファイルです。キーの有効期間が切れると、アプリの新しいバージョンにシームレスにアップグレードできなくなります。

Citrix Gateway

Citrix Gateway の証明書の有効期限について詳しくは、Citrix Support Knowledge Center で「How to handle certificate expiry on NetScaler」を参照してください。

Citrix Gateway 証明書の有効期限が切れると、ユーザーはストアに登録したり、アクセスすることができなくなります。Citrix Gateway 証明書の有効期限が切れると、ユーザーは Citrix Secure Mail を使用するときに Exchange Server に接続することもできなくなります。また、ユーザーは（証明書の有効期限切れによって）HDX アプリを一覧にしたり起動することもできなくなります。

Expiry Monitor および Command Center によって、Citrix Gateway 証明書の記録を確認できます。証明書の有効期限が切れると Command Center から通知が送信されます。これらのツールは、以下の Citrix Gateway 証明書の監視に役立ちます:

- MDM FQDN の SSL 証明書
- Gateway FQDN の SSL 証明書
- ShareFile SZC FQDN の SSL 証明書

- Exchange 負荷分散用の SSL 証明書（オフロード構成）
- StoreFront 負荷分散用の SSL 証明書
- 上記証明書のルート証明書および中間 CA 証明書

Citrix Gateway と Citrix Endpoint Management

November 29, 2023

Citrix Endpoint Management と統合すると、Citrix Gateway を経由して内部ネットワークとリソースにリモートデバイスでアクセスできるようになります。Citrix Endpoint Management により、デバイス上のアプリから Citrix Gateway へのマイクロ VPN が作成されます。

Citrix Gateway サービス（プレビュー）か、オンプレミスの Citrix Gateway（NetScaler Gateway とも呼ばれる）を使用できます。2 つの Citrix Gateway ソリューションの概要については、「Citrix Endpoint Management で使用する Citrix Gateway の構成」を参照してください。

内部ネットワークへのリモートデバイスアクセスに対する認証の構成

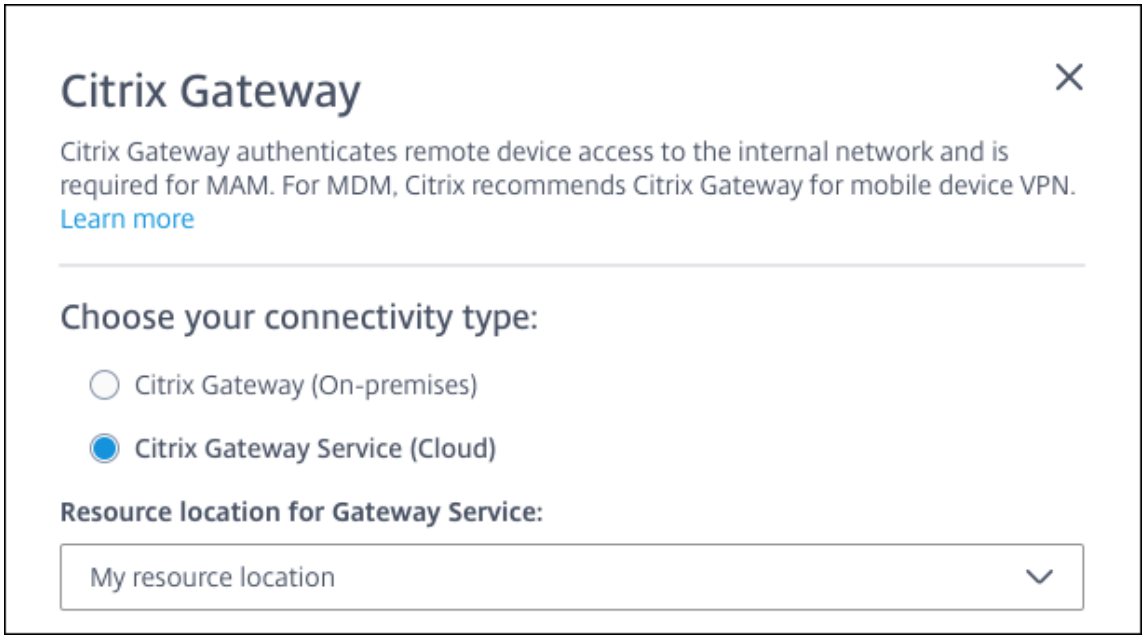
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［サーバー］の下の ［**Citrix Gateway**］をクリックします。［**Citrix Gateway**］ページが開きます。次の例では、Citrix Gateway インスタンスが 1 つ存在しています。

3. 次の設定を構成します:
   - 認証: 認証を有効にするかどうかを選択します。デフォルトは ［オン］です。
   - 認証用のユーザー証明書を配信: Citrix Endpoint Management で Citrix Secure Hub と認証証明書を共有するかを選択します。証明書を共有すると、Citrix Gateway でクライアント証明書認証を処理できるようになります。デフォルトは ［オフ］です。
   - 資格情報プロバイダー: ボックスの一覧で、使用する資格情報プロバイダーを選択します。詳しくは、「資格情報プロバイダー」を参照してください。
4. ［保存］をクリックします。

Citrix Gateway サービスインスタンスの追加（プレビュー）

認証設定の保存後、Citrix Gateway インスタンスを Citrix Endpoint Management に追加します。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで［Citrix Gateway］タイルまでスクロールして ［セットアップの開始］をクリックします。［**Citrix Gateway**］ページが開きます。
3. ［**Citrix Gateway** サービス（クラウド）］を選択し、Gateway サービスのリソースの場所を指定します。



   - **Gateway** サービスのリソースの場所： Citrix Secure Mail を使用する場合は必須です。STA サービスのリソースの場所を指定します。リソースの場所には、構成済みの Citrix Gateway が含まれている必要があります。Gateway サービス用に構成されているリソースの場所を後で削除する必要がある場合は、この設定を更新してください。

   これらの設定を完了したら、［接続］をクリックして接続を確立します。新しい Citrix Gateway が追加されます。［設定］ページに **Citrix Gateway** サービス（クラウド）タイルが表示されます。インスタンスを編集するには、［詳細を表示］をクリックします。選択したリソースの場所で Gateway Connector を使用できない場合は、［**Gateway Connector** の追加］をクリックします。画面に表示されるガイダンスに従って、Cloud Connector をインストールします。Gateway Connector は、後で追加することもできます。

4. ［スクリプトの保存とエクスポート］をクリックします。

   - ［スクリプトの保存とエクスポート］。ボタンをクリックして設定を保存し、構成バンドルをエクスポートします。バンドルのスクリプトを Citrix Gateway にアップロードし、Citrix Endpoint Management の設定を使用して構成できます。詳しくは、これらの手順の後で「Citrix Endpoint Management で使用するオンプレミスの Citrix Gateway の構成」を参照してください。

   新しい Citrix Gateway を追加しました。［設定］ページに **Citrix Gateway** タイルが表示されます。インスタンスを編集するには、［詳細を表示］をクリックします。

Citrix Endpoint Management で使用するオンプレミスの **Citrix Gateway** を構成する

Citrix Endpoint Management で使用するオンプレミスの Citrix Gateway を構成するには、以下で説明する一般的な手順を実行します。

1. 環境が前提条件を満たしていることを確認します。
2. Citrix Endpoint Management コンソールからスクリプトバンドルをエクスポートします。
3. バンドルからファイルを抽出します。Citrix Gateway でクラシックポリシーのみを使用し、Citrix ADC 13.0 以前を実行している場合は、ファイル名に「クラシック」が付いているスクリプトを使用します。拡張ポリシーを使用している場合や、Citrix ADC 13.1 以降を実行している場合は、ファイル名に「拡張」が付いているスクリプトを使用します。
4. Citrix Gateway で適切なスクリプトを実行します。最新の手順について詳しくは、スクリプトに付属する readme ファイルを参照してください。
5. 構成をテストします。

スクリプトにより、Citrix Endpoint Management に必要な以下の Citrix Gateway の設定が構成されます:

- MDM と MAM に必要な Citrix Gateway 仮想サーバー
- Citrix Gateway 仮想サーバー用セッションポリシー
- Citrix Endpoint Management サーバーの詳細
- 証明書検証用プロキシロードバランサー
- Citrix Gateway 仮想サーバーの認証ポリシーとアクション。スクリプトによって LDAP の構成設定が説明されます。
- プロキシサーバーのトラフィックアクションとポリシー
- クライアントレスアクセスプロファイル
- Citrix Gateway の静的ローカル DNS レコード
- 他のバインディング: サービスポリシー、CA 証明書

このスクリプトは以下の構成には対応していません:

- Exchange 負荷分散
- Citrix Files 負荷分散
- ICA プロキシ構成
- SSL オフロード

Citrix Gateway 構成スクリプトを使用するための前提条件

Citrix Endpoint Management の要件:

- スクリプトバンドルをエクスポートする前に、Citrix Endpoint Management で LDAP と Citrix Gateway の設定を完了します。設定を変更した場合は、スクリプトバンドルを再度エクスポートします。

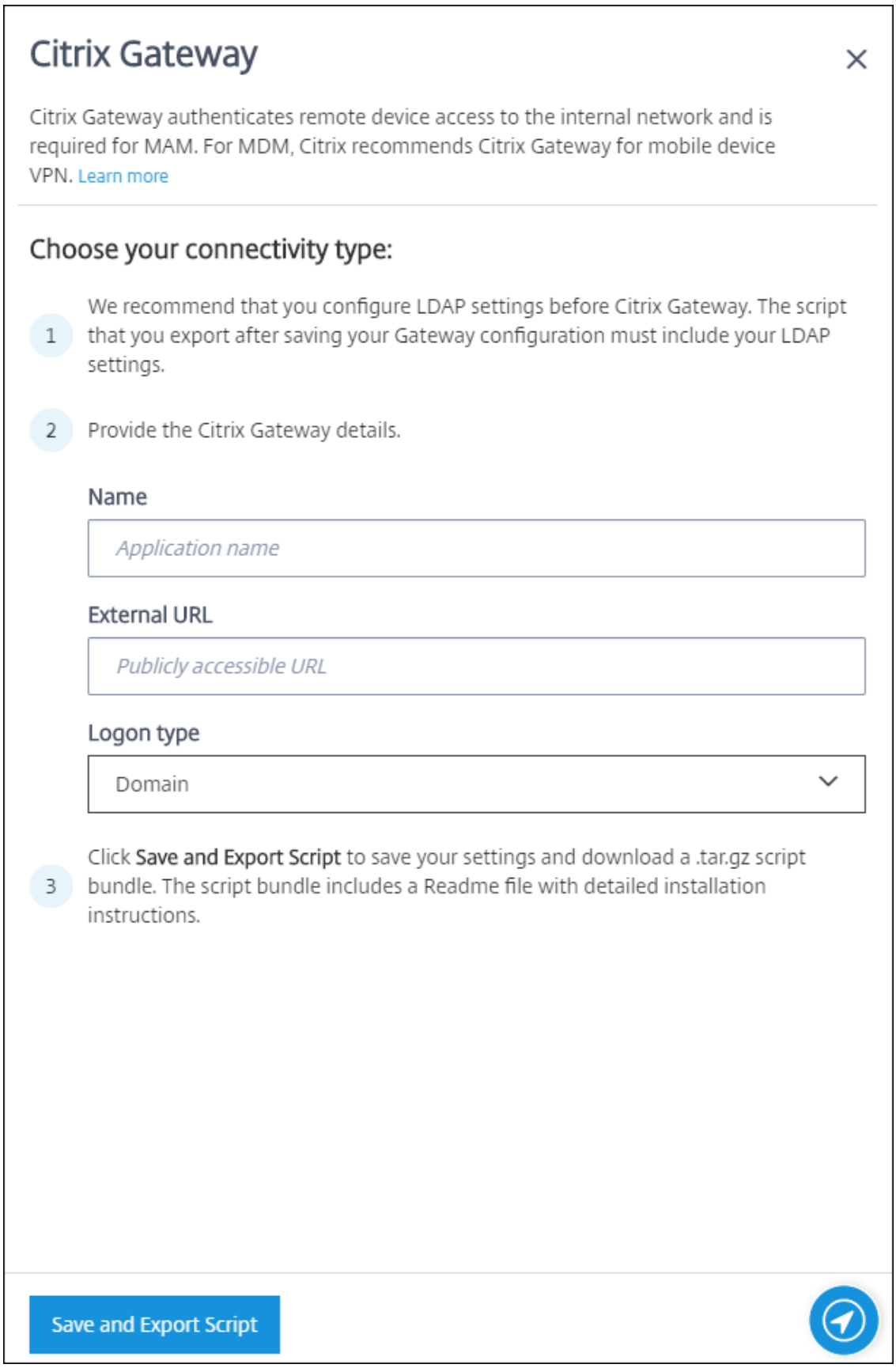
Citrix Gateway の要件:

- Citrix Gateway で証明書ベースの認証を使用する場合は、Citrix ADC アプライアンスで SSL 証明書を作成する必要があります。「Citrix ADC アプライアンスでの SSL 証明書の作成と使用」を参照してください。
- Citrix Gateway（最小バージョン 11.0、ビルド 70.12）
- Citrix Gateway の IP アドレスが構成済みであり、LDAP サーバーに接続できる（LDAP が負荷分散されていない場合）
- Citrix Gateway のサブネット IP（SNIP：Subnet IP）アドレスが構成済みであり、必要なバックエンドサーバーに接続でき、ポート 8443/TCP 経由でパブリックネットワークにアクセスできる
- DNS でパブリックドメインを解決できる
- Citrix Gateway にプラットフォーム/ユニバーサルライセンスまたはトライアルライセンスが付与されている。詳しくは、「https://support.citrix.com/article/CTX126049」を参照してください。

Citrix Endpoint Management からのスクリプトバンドルのエクスポート

認証設定の保存後、Citrix Gateway インスタンスを Citrix Endpoint Management に追加します。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで［Citrix Gateway］タイルまでスクロールして ［セットアップの開始］をクリックします。［**Citrix Gateway**］ページが開きます。
3. ［**Citrix Gateway**（オンプレミス）］を選択し、次の設定を構成します:



- 名前： Citrix Gateway インスタンスの名前を入力します。
- 外部 **URL**： Citrix Gateway の、パブリックにアクセスできる URL を入力します。例：`https://receiver.com`。
- ログオンの種類：ログオンの種類を選択します。種類には、［ドメイン］、［セキュリティトークンのみ］、［ドメインおよびセキュリティトークン］、［証明書］、［証明書およびドメイン］、［証明書およびセキュリティトークン］があります。デフォルトは ［ドメイン］です。

ドメインが複数ある場合は、［証明書およびドメイン］を使用します。詳しくは、「複数ドメイン認証の構成」を参照してください。

Citrix Gateway での証明書ベースの認証には追加の構成が必要です。たとえば、ルート CA 証明書を Citrix ADC アプライアンスにアップロードする必要があります。「Citrix ADC アプライアンスでの SSL 証明書の作成と使用」を参照してください。

詳しくは、展開ハンドブックの「認証」を参照してください。

4. ［スクリプトの保存とエクスポート］をクリックします。

   - ［スクリプトの保存とエクスポート］。ボタンをクリックして設定を保存し、構成バンドルをエクスポートします。バンドルのスクリプトを Citrix Gateway にアップロードし、Citrix Endpoint Management の設定を使用して構成できます。詳しくは、これらの手順の後で「Citrix Endpoint Management で使用するオンプレミスの Citrix Gateway の構成」を参照してください。

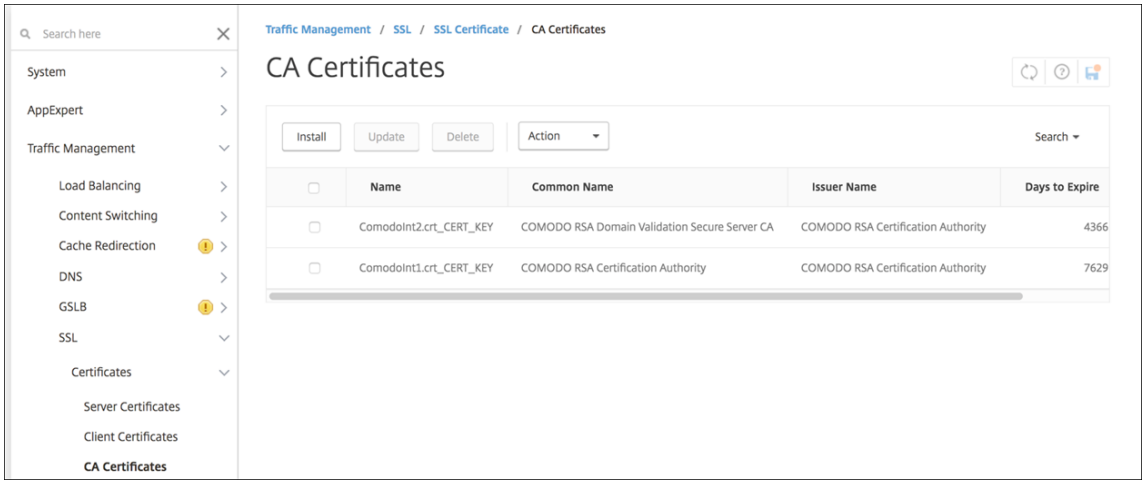
   新しい Citrix Gateway を追加しました。［設定］ページに **Citrix Gateway** タイルが表示されます。インスタンスを編集するには、［詳細を表示］をクリックします。

環境でのスクリプトのインストール

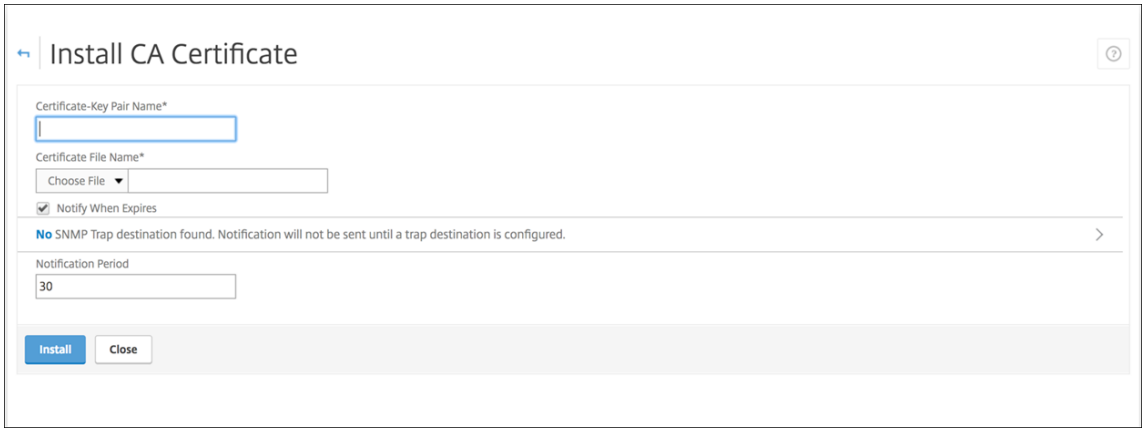
スクリプトバンドルの内容は次のとおりです。

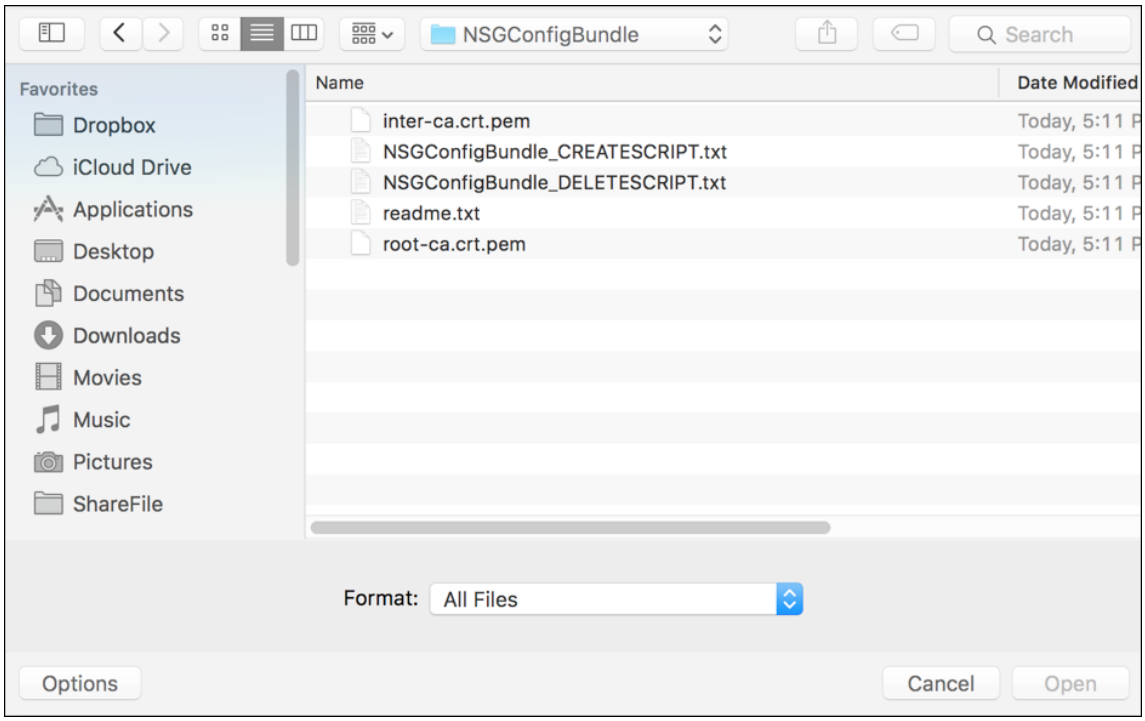
- 詳細説明付きの readme ファイル
- NetScaler の必須コンポーネントの構成に使用する NetScaler CLI コマンドを含むスクリプト
- パブリックルート CA 証明書と中間 CA 証明書
- NetScaler の構成の削除に使用する NetScaler CLI コマンドを含むスクリプト

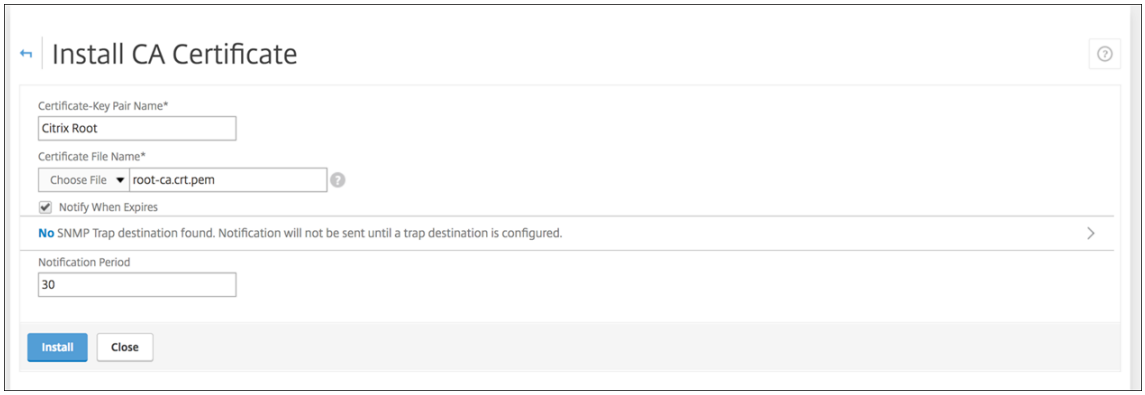
1. 証明書ファイル（スクリプトバンドルで提供）を Citrix ADC アプライアンスの/nsconfig/ssl/ディレクトリにアップロードしてインストールします。「Citrix ADC アプライアンスでの SSL 証明書の作成と使用」を参照してください。

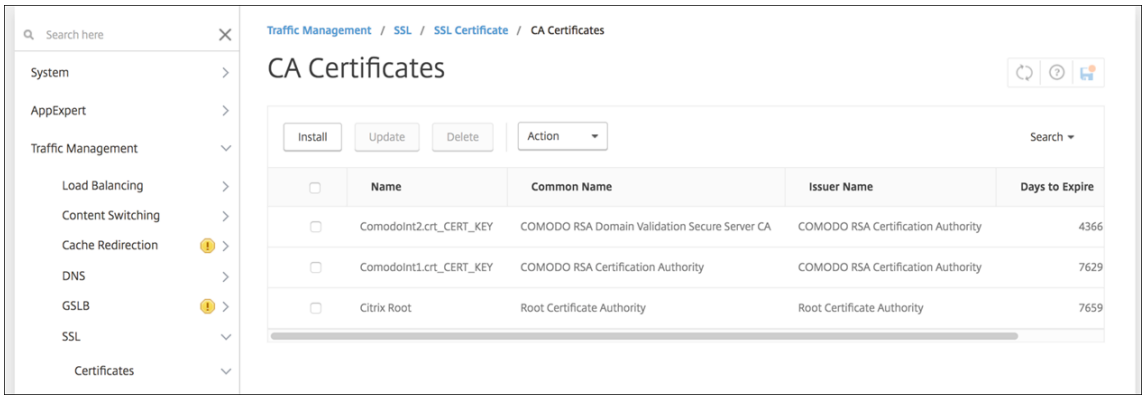


次の例は、ルート証明書をインストールする方法を示しています。









ルート証明書と中間証明書の両方をインストールしてください。

2. スクリプト(ConfigureCitrixGatewayScript_Classic.txt or ConfigureCitrixGatewayScript_Advanced.txt)を編集して、すべてのプレースホルダーをユーザー環境の詳細情報と置き換えます。

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. スクリプトバンドルに含まれる readme ファイルの説明に従って、編集済みのスクリプトを NetScaler の bash シェルで実行します。例:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```



```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

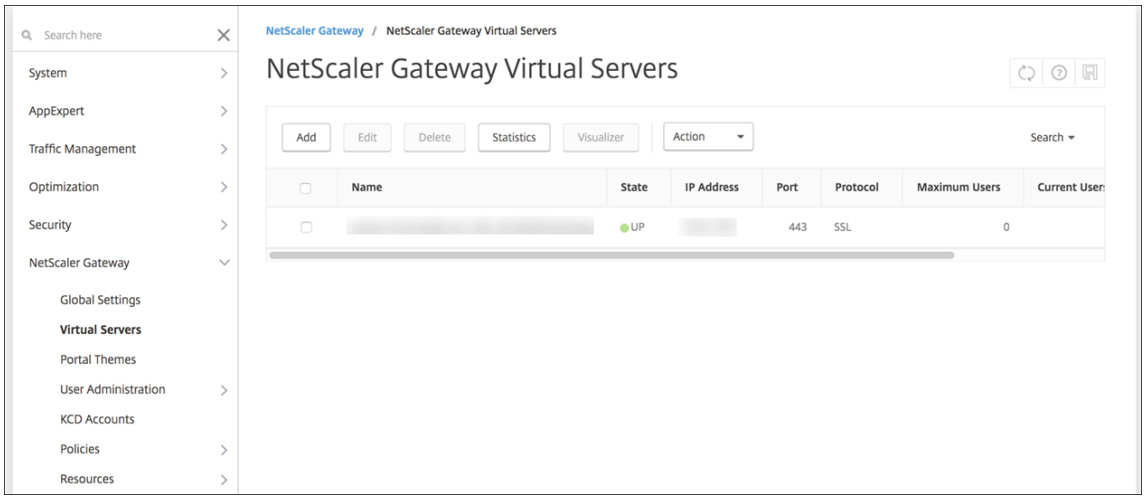
スクリプトが完了すると、次の行が表示されます。

```
exec: save ns config
 Done
 Done
root@ns#
```

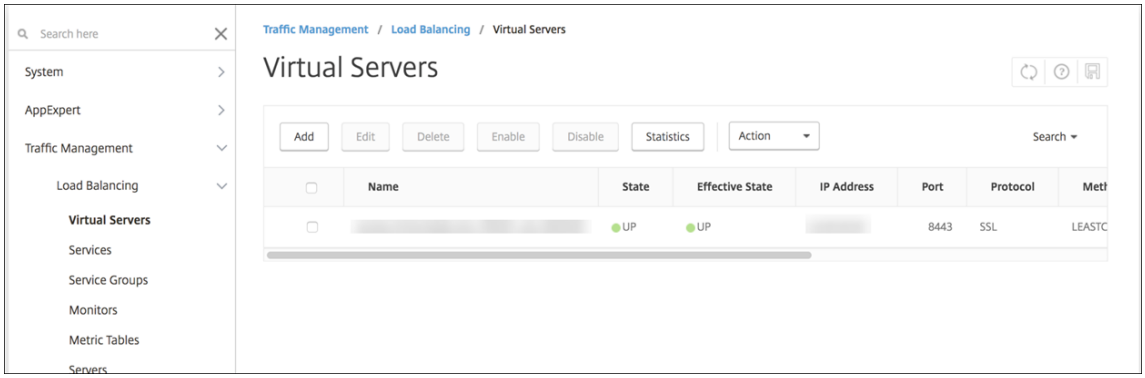
構成のテスト

構成を検証するには:

1. Citrix Gateway 仮想サーバーの状態表示が ［**UP**］であることを確認します。



2. Proxy 負荷分散仮想サーバーの状態表示が ［**UP**］であることを確認します。



3. Web ブラウザーを開いて Citrix Gateway の URL に接続し、認証を試みます。認証が成功すれば、HTTP ステータス 404 の「見つかりません」メッセージにリダイレクトされます。
4. デバイスを登録して、MDM と MAM の両方に登録されたことを確認します。

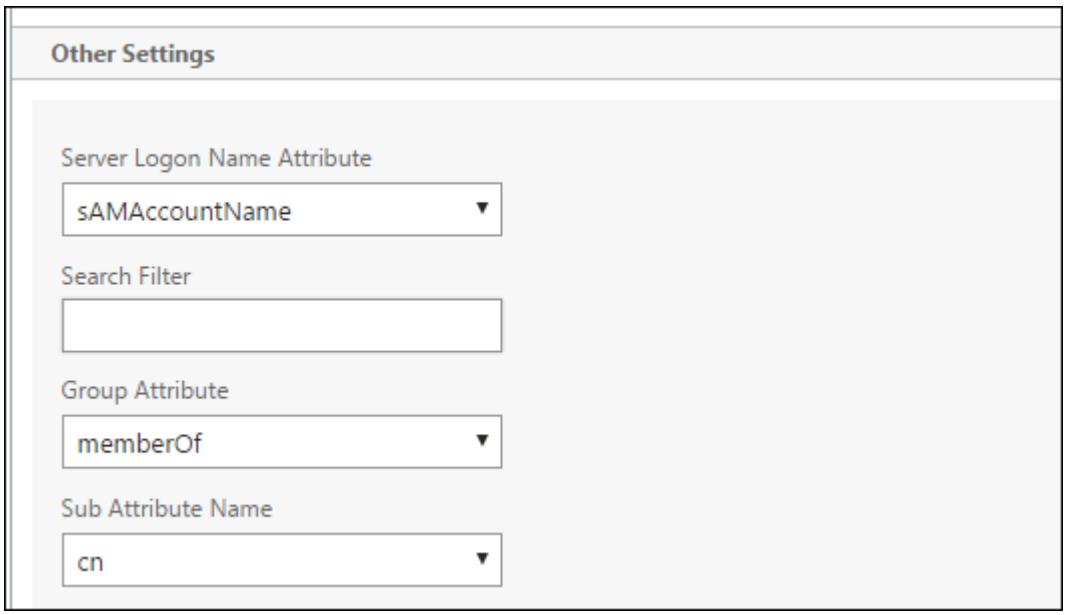
複数ドメイン認証の構成

テスト環境、開発環境、および実稼働環境などの複数の Citrix Endpoint Management インスタンスがある場合は、追加の環境用に手動で Citrix Gateway を構成します（NetScaler for XenMobile ウィザードは 1 回のみ使用できます）。

Citrix Gateway 構成

複数ドメイン環境で Citrix Gateway 認証ポリシーとセッションポリシーを構成するには:

1. Citrix Gateway 構成ユーティリティの ［構成］タブで ［**Citrix Gateway**］**>** ［ポリシー］**>** ［認証］を展開します。
2. ナビゲーションペインで ［**LDAP**］をクリックします。
3. クリックして LDAP プロファイルを編集します。［サーバーログオン名の属性］を **userPrincipalName**、または検索に使用する属性に変更します。指定した属性を記録します。この属性は、Citrix Endpoint Management コンソールで LDAP 設定を構成するときに使用します。

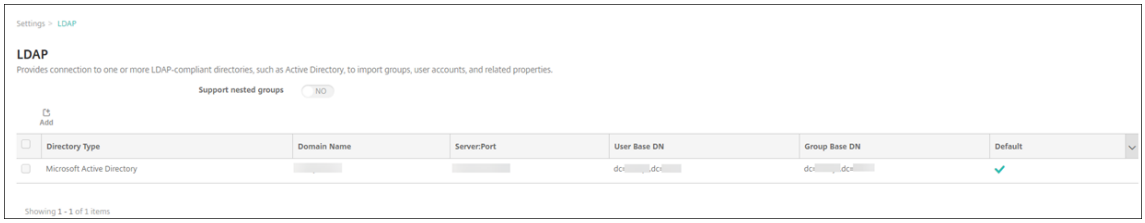


4. 各 LDAP ポリシーに対してこれらの手順を繰り返します。ドメインごとに個別の LDAP ポリシーが必要です。
5. Citrix Gateway 仮想サーバーにバインドされたセッションポリシーで、［**Edit session profile**］**>** ［**Published Applications**］に移動します。［**Single Sign-On Domain**］は空白にしてください。

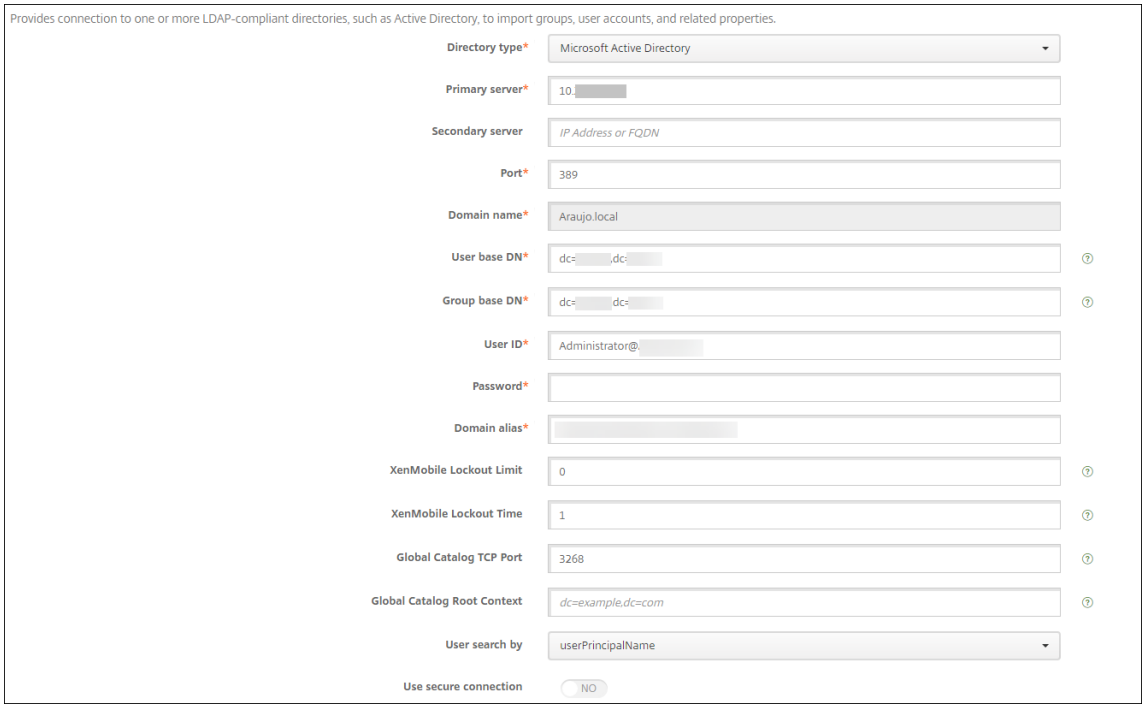
Citrix Endpoint Management 構成

Citrix Endpoint Management の LDAP を複数ドメイン環境に構成するには:

1. Citrix Endpoint Management コンソールで、［設定］**>** ［**LDAP**］に移動し、ディレクトリを追加または編集します。



2. 情報を指定します。
   - ［ドメインエイリアス］でユーザー認証に使用する各ドメインを指定します。ドメインはコンマで区切り、ドメイン間にはスペースを入れないでください。例: domain1.com,domain2.com,domain3.com
   - ［ユーザー検索基準］フィールドが Citrix Gateway LDAP ポリシーで指定された［サーバーログオン名の属性］と一致するようにしてください。



特定の **URL** への受信接続要求を破棄

ご使用の環境の Citrix Gateway が SSL オフロード用に構成されている場合は、ゲートウェイで特定の URL への受信接続要求が破棄されるようにすることができます。この方法でセキュリティを強化する必要がある場合は、Citrix Cloud Operations に連絡し、使用している IP アドレスをオンプレミスデータセンターで許可するよう依頼してください。

ドメインまたはドメイン + セキュリティトークン認証

November 29, 2023

Citrix Endpoint Management は、LDAP（Lightweight Directory Access Protocol）に準拠している 1 つまたは複数のディレクトリに対するドメインベースの認証をサポートしています。Citrix Endpoint Management で 1 つまたは複数のディレクトリへの接続を構成します。Citrix Endpoint Management は、LDAP 構成を使用して、グループ、ユーザーアカウント、および関連するプロパティをインポートします。

> 重要:
>
> Citrix Endpoint Management では、ユーザーが Citrix Endpoint Management にデバイスを登録した後に、認証モードを 1 つのタイプの認証モードから他の認証モードに変更することはサポートされていません。たとえば、ユーザー登録後に、認証モードをドメイン認証からドメイン + 証明書に変更することはできません。

LDAP について

LDAP は、オープンソースで特定のベンダーに依存しないアプリケーションプロトコルであり、インターネットプロトコル（IP）ネットワーク経由で分散ディレクトリ情報サービスへのアクセスや管理を行うためのものです。ディレクトリ情報サービスは、ネットワークで使用可能な、ユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。

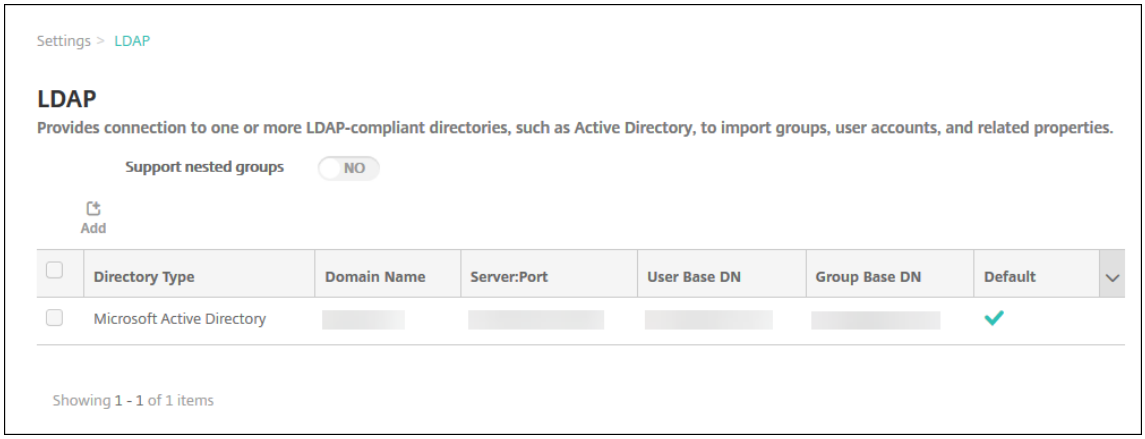
LDAP は一般的に、シングルサインオン（SSO）をユーザーに提供するために利用されます。SSO では（ユーザーごとに）1 つのパスワードを複数のサービス間で共有します。シングルサインオンにより、ユーザーは会社の Web サイトに一度ログオンすると、社内イントラネットへのアクセスが認証されます。

クライアントが、ディレクトリシステムエージェント（DSA）と呼ばれる LDAP サーバーに接続して、LDAP セッションを開始します。次に、クライアントは操作要求をサーバーに送信し、サーバーは適切な認証で応答します。

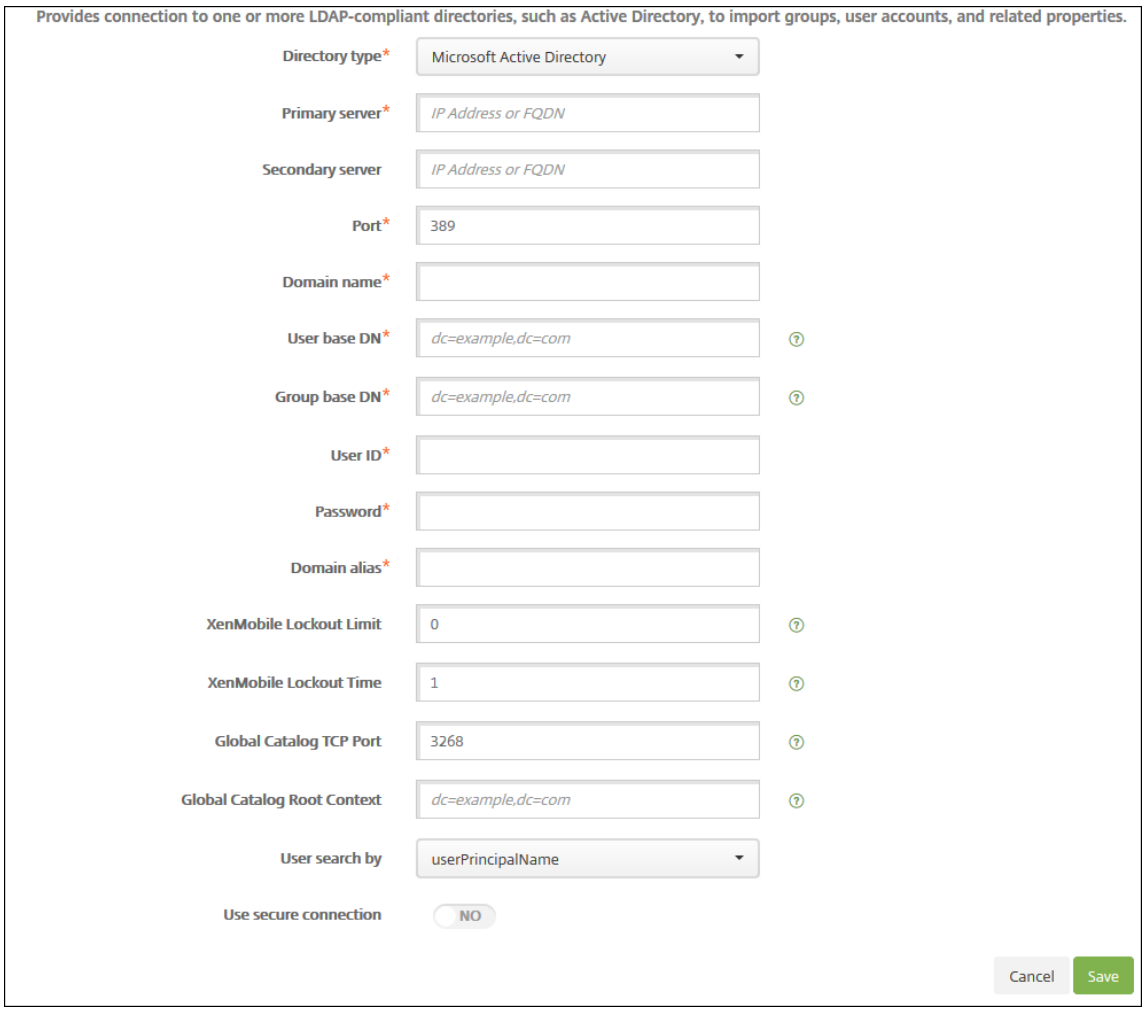
Citrix Endpoint Management で LDAP 接続を編集または追加するには

「LDAP の構成」で説明されているように、通常は、Citrix Endpoint Management にオンボーディングするときに LDAP 接続を構成します。そのセクションに示されている画面が使用可能になる前にオンボーディングした場合は、このセクションの情報を使用して LDAP 接続を追加します。

1. Citrix Endpoint Management コンソールで、［設定］**>**［**LDAP**］の順に選択します。
2. ［サーバー］の下の ［**LDAP**］をクリックします。［**LDAP**］ページが開きます。



3. ［**LDAP**］ページで、［追加］または ［編集］をクリックします。［**LDAP** の追加］または ［**LDAP** の編集］ページが開きます。



4. 次の設定を構成します:

   - ディレクトリの種類: 一覧から、適切なディレクトリの種類を選択します。デフォルトは ［**Microsoft Active Directory**］です。
   - プライマリサーバー: LDAP で使用するプライマリサーバーを入力します。IP アドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
   - セカンダリサーバー: セカンダリサーバーが構成されている場合、任意でセカンダリサーバーの IP アドレスまたは FQDN を入力します。このサーバーは、プライマリサーバーが使用できない場合に使用するフェイルオーバーサーバーです。
   - ポート: LDAP サーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていない LDAP 接続用のポート番号 **389** に設定されています。セキュリティ保護された LDAP 接続ではポート番号 **636**、Microsoft のセキュリティ保護されていない LDAP 接続では **3268**、Microsoft のセキュリティ保護された LDAP 接続では **3269** を使用します。
   - ドメイン名: ドメイン名を入力します。

- ユーザーベース **DN**: Active Directory 内でのユーザーの位置を一意の識別子で入力します。構文例には次が含まれます: `ou=users`、`dc=example`、`dc=com`
- グループベース **DN**: Active Directory のグループの場所を入力します。たとえば、`cn=users`, `dc=domain`, `dc=net`の場合、`cn=users`はグループのコンテナ名で`dc`は Active Directory のドメインコンポーネントです。
- ユーザー **ID**: Active Directory アカウントに関連付けられたユーザー ID を入力します。
- パスワード: ユーザーに関連付けられたパスワードを入力します。
- ドメインエイリアス: ドメイン名のエイリアスを入力します。登録後に ［ドメインエイリアス］設定を変更すると、ユーザーは再登録する必要があります。
- **Citrix Endpoint Management** ロックアウト制限: ログオンの試行失敗回数として、**0**～**999** の数値を入力します。「**0**」の値に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。デフォルトは ［**0**］です。

  このロックアウト制限は、LDAP ロックアウトポリシーよりも低い値に設定することを検討してください。そうすることで、Citrix Endpoint Management が LDAP サーバーに対して認証できない場合のユーザーのロックアウトを防ぐことができます。たとえば、LDAP ロックアウトポリシーが 5 回の試行である場合、このロックアウト制限は **4** 以下に構成します。
- **Citrix Endpoint Management** ロックアウト時間: ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、**0**～**99999** の数値を入力します。「**0**」の値に設定すると、ユーザーがロックアウト後に強制的に待機させられることはなくなります。デフォルトは **1** です。
- グローバルカタログ **TCP** ポート: グローバルカタログサーバーの TCP ポート番号を入力します。デフォルトでは、TCP ポート番号は **3268** に設定されています。SSL 接続では、ポート番号 **3269** を使用します。
- グローバルカタログルートコンテキスト: 任意で、Active Directory でのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準の LDAP 検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- ユーザー検索基準: Citrix Endpoint Management でこのディレクトリ内のユーザーを検索するのに使用するユーザー名またはユーザー ID の形式を選択します。ユーザーは、登録時にユーザー名またはユーザー ID をこの形式で入力します。登録後に ［ユーザー検索基準］を変更すると、ユーザーは再登録する必要があります。

  ［**userPrincipalName**］を選択した場合、ユーザーは次の形式でユーザープリンシパル名（UPN）を入力します:

  - ユーザー名 @ ドメイン

  ［**sAMAccountName**］を選択した場合、ユーザーは次のいずれかの形式でセキュアアカウントマネージャー（SAM）名を入力します:

  - ユーザー名 @ ドメイン

  - ドメイン\ユーザー名

- セキュリティで保護された接続を使用：セキュリティ保護された接続を使用するかどうかを選択します。デフォルトは ［いいえ］ です。

5. ［保存］ をクリックします。

LDAP 準拠のディレクトリを削除するには

1. ［**LDAP**］ の表で、削除するディレクトリを選択します。

   各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。

2. ［削除］ をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］ をクリックします。

ドメイン + セキュリティトークン認証の構成

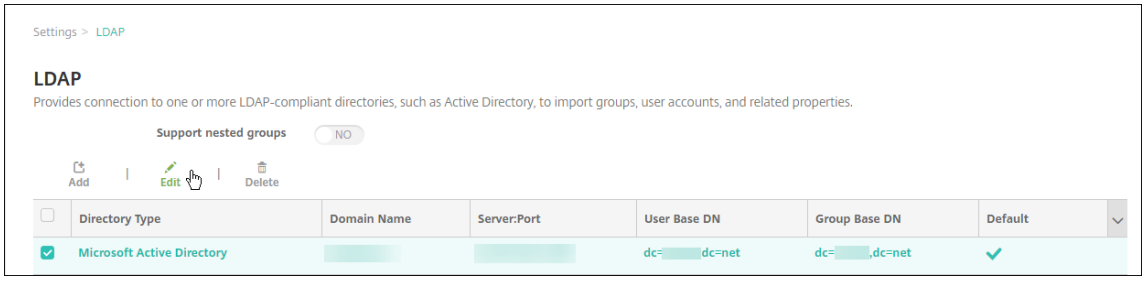
RADIUS プロトコルを使用して、LDAP 資格情報とワンタイムパスワードによる認証をユーザーに要求するように Citrix Endpoint Management を構成できます。

ユーザービリティを最適にするために、この構成を Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。この構成により、ユーザーは LDAP ユーザー名とパスワードを繰り返し入力する必要がなくなります。ただし、登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力します。

LDAP 設定の構成

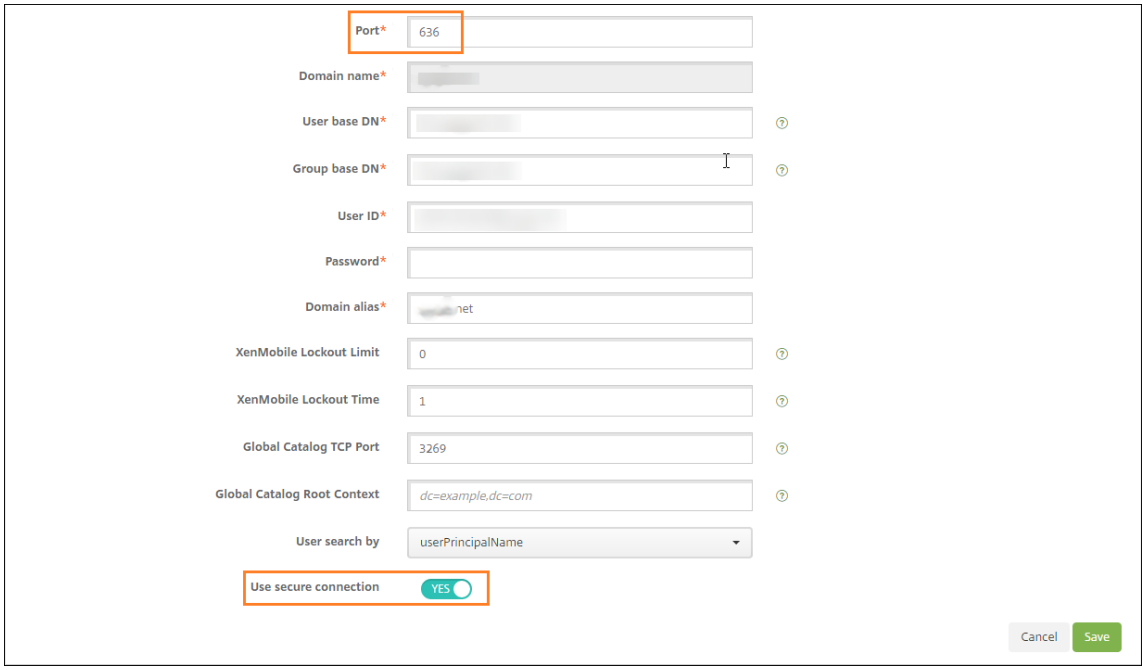
認証に LDAP を使用する場合、証明機関から Citrix Endpoint Management に SSL 証明書をインストールする必要があります。詳しくは、「証明書のアップロード」を参照してください。

1. ［設定］ で ［**LDAP**］ をクリックします。
2. ［**Microsoft Active Directory**］ を選択して ［編集］ をクリックします。



3. ［ポート］ が **636** であることを確認します（セキュリティで保護された LDAP 接続の場合）。セキュリティで保護された Microsoft LDAP 接続の場合は **3269** です。

4. ［セキュリティで保護された接続を使用］を ［はい］に変更します。



Citrix Gateway 設定の構成

次の手順では、Citrix Gateway インスタンスを既に Citrix Endpoint Management に追加してあると想定しています。Citrix Gateway インスタンスを追加するには、「Citrix Gateway と Citrix Endpoint Management」を参照してください。

1. ［設定］で ［**Citrix Gateway**］をクリックします。
2. ［Citrix Gateway］を選択して ［編集］をクリックします。
3. ［ログオンの種類］で ［ドメインおよびセキュリティトークン］を選択します。

Citrix PIN とユーザーパスワードキャッシュの有効化

Citrix PIN とユーザーパスワードキャッシュを有効化するには、［設定］**>**［クライアントプロパティ］に移動し、チェックボックス ［**Citrix PIN** 認証の有効化］および ［ユーザーパスワードキャッシュの有効化］をオンにします。詳しくは、「クライアントプロパティ」を参照してください。

ドメインおよびセキュリティトークン認証のための **Citrix Gateway** の構成

Citrix Gateway セッションのプロファイルおよびポリシーを、Citrix Endpoint Management で使用される仮想サーバー用に構成します。詳しくは、Citrix Gateway のドキュメントを参照してください。

クライアント証明書、または証明書とドメイン認証の組み合わせ

November 29, 2023

Citrix Endpoint Management のデフォルト構成は、ユーザー名とパスワードによる認証です。登録および Citrix Endpoint Management 環境へのアクセスのセキュリティを強化するには、証明書ベースの認証の使用を考慮してください。Citrix Endpoint Management 環境では、この構成はセキュリティとユーザーエクスペリエンスの最適な組み合わせです。証明書とドメイン認証を利用すれば、Citrix Gateway の 2 要素認証で提供されるセキュリティとと共に SSO の最高の可能性を引き出します。

ユーザービリティを最適にするために、この証明書とドメイン認証を Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。その結果、ユーザーは LDAP ユーザー名とパスワードを繰り返し入力する必要がなくなります。ただし、登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力します。

> 重要:
>
> Citrix Endpoint Management では、ユーザーが Citrix Endpoint Management にデバイスを登録した後に、認証モードをドメイン認証から他の認証モードに変更することはサポートされていません。

LDAP やスマートカードの使用または同様の方法を許可しない場合、証明書を構成すると Citrix Endpoint Management にスマートカードを提示できます。ユーザーはそれにより、Citrix Endpoint Management が生成する一意の PIN を使用して登録できます。ユーザーがアクセス権を獲得すると、Citrix Endpoint Management は、Citrix Endpoint Management 環境に認証するために使用される証明書を作成して展開します。

NetScaler for XenMobile ウィザードを使用すると、Citrix Gateway 証明書のみの認証または証明書とドメイン認証の組み合わせを使用する場合、Citrix Endpoint Management に必要な構成を実行できます。NetScaler for XenMobile ウィザードは 1 回のみ実行できます。

高セキュリティの環境では、パブリックネットワークまたは保護されていないネットワークで組織外の LDAP 資格情報を使用することは、組織に対する最大のセキュリティ脅威とみなされます。高セキュリティの環境では、クライアント証明書とセキュリティトークンを使用する 2 要素認証がオプションとなります。詳しくは、「Configuring Citrix Endpoint Management for Certificate and Security Token Authentication」を参照してください。

クライアント証明書認証は、MAM および MDM+MAM で登録しているデバイスで使用できます。これらのデバイスでクライアント証明書認証を使用するには、Microsoft サーバー、Citrix Endpoint Management を構成してから、Citrix Gateway を構成する必要があります。この記事に説明されているとおり、次の手順に従ってください。

Microsoft サーバーの場合:

1. 証明書のスナップインを Microsoft 管理コンソールに追加します。
2. テンプレートを証明機関（CA）に追加します。
3. CA サーバーから PFX 証明書を作成します。

Citrix Endpoint Management の場合:

1. 証明書を Citrix Endpoint Management にアップロードします。
2. 証明書に基づいた認証のために PKI エンティティを作成します。
3. 資格情報プロバイダーを構成します。
4. Citrix Gateway を構成して、認証用のユーザー証明書を配信します。

Citrix Gateway の構成について詳しくは、次の Citrix ADC ドキュメントの記事を参照してください:

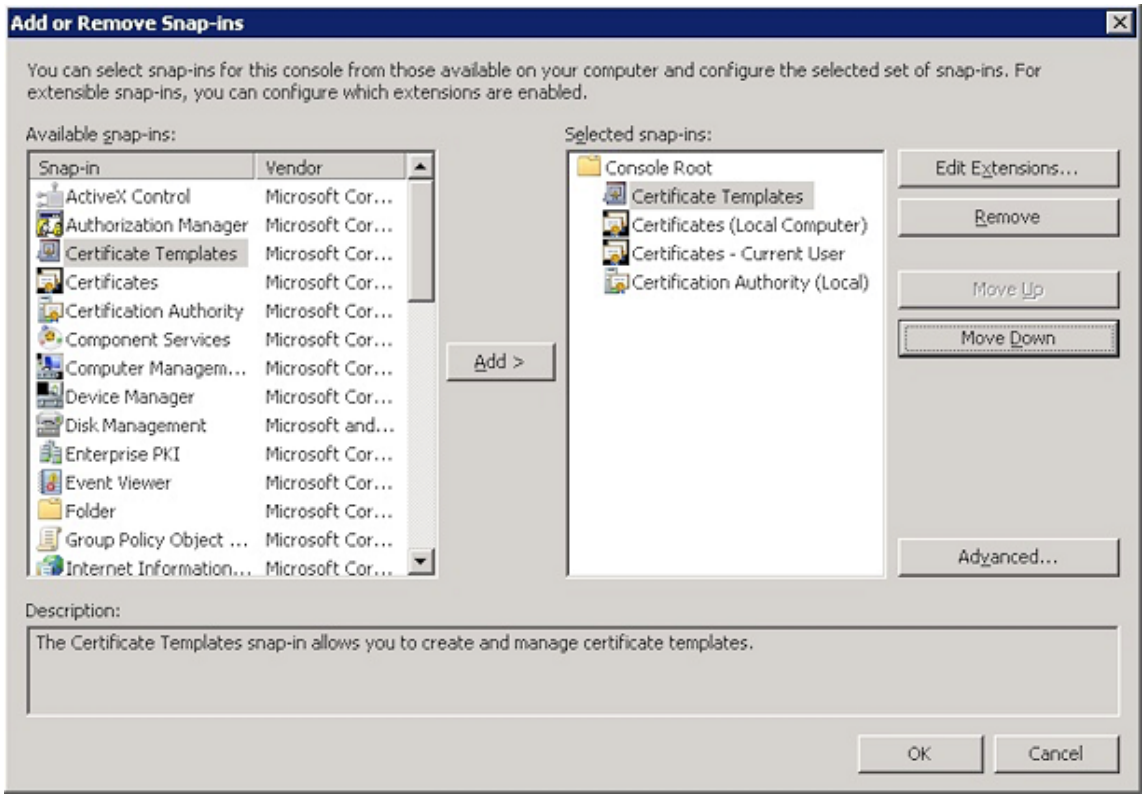
- クライアント認証
- SSL プロファイルインフラストラクチャ
- クライアント証明書認証ポリシーの構成およびバインド。

前提条件

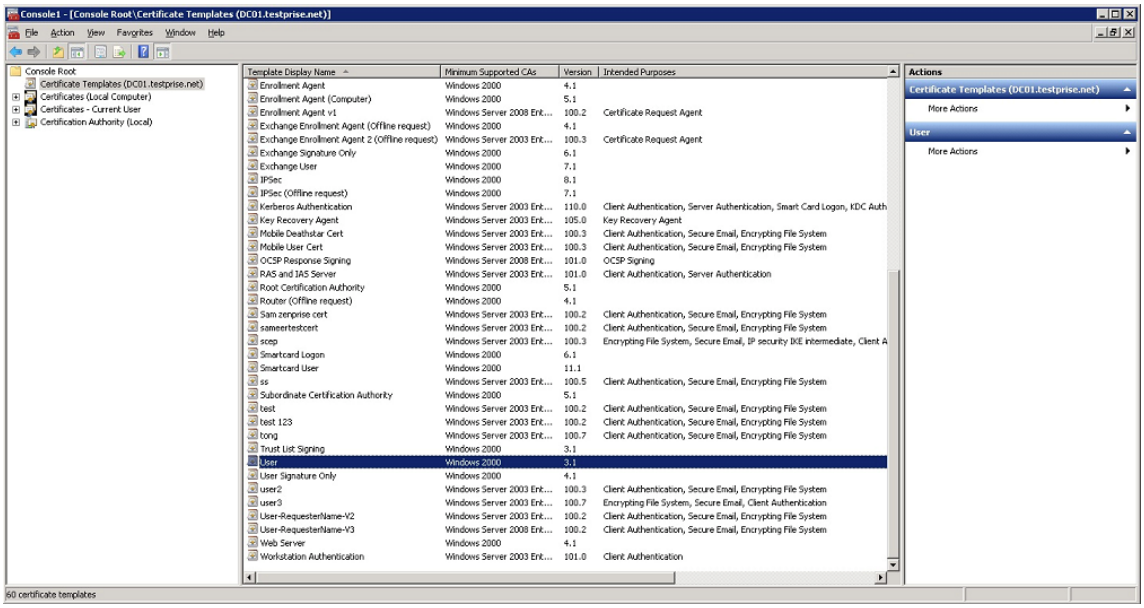
- Microsoft 証明書サービスのエンティティテンプレートを作成する場合は、登録済みデバイスの認証に関する問題を避けるため、特殊文字を使用しないでください。たとえば、テンプレート名には以下の文字を使用しないでください: : ! $ ()# % + * ~ ? | { } []
- Exchange ActiveSync に対して証明書ベースの認証を構成するには、Exchange Server に関する Microsoft ドキュメントを参照してください。Exchange ActiceSync の証明機関（CA）サーバーサイトを構成して、クライアント証明書を要求します。
- プライベートサーバー証明書を使用して Exchange Server への ActiveSync トラフィックを保護する場合は、モバイルデバイスにすべてのルート証明書および中間証明書があることを確認してください。これらの証明書がない場合、Citrix Secure Mail でのメールボックス設定時に、証明書ベースの認証が失敗します。Exchange IIS コンソールでは、次のことが必要です:
  - Citrix Endpoint Management を Exchange と使用するための Web サイトを追加し、Web サーバー証明書をバインドします。
  - ポート 9443 を使用します。
  - その Web サイトに対して、Microsoft-Server-ActiveSync 用と EWS 用に、2 つのアプリケーションを追加する必要があります。それらの両方のアプリケーションに対して、[**SSL Settings**] で [**Require SSL**] を選択します。

証明書のスナップインを **Microsoft** 管理コンソールに追加する

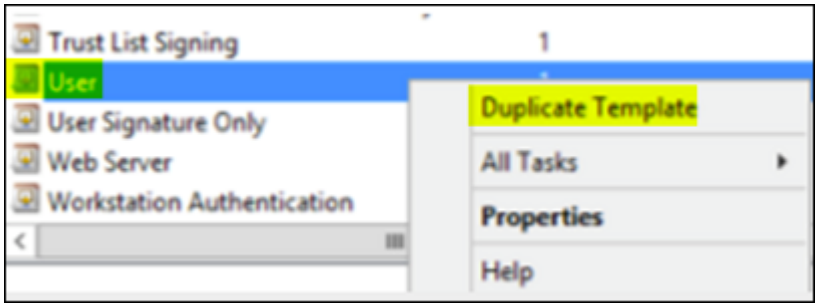
1. コンソールを開いて、[スナップインの追加と削除] をクリックします。
2. 次のスナップインを追加します:
   - 証明書テンプレート
   - 証明書（ローカルコンピューター）
   - 証明書 - 現在のユーザー
   - 証明機関（CA）（ローカル）



3. [証明書テンプレート] を展開します。



4. [ユーザー] テンプレートと [テンプレートの複製] を選択します。



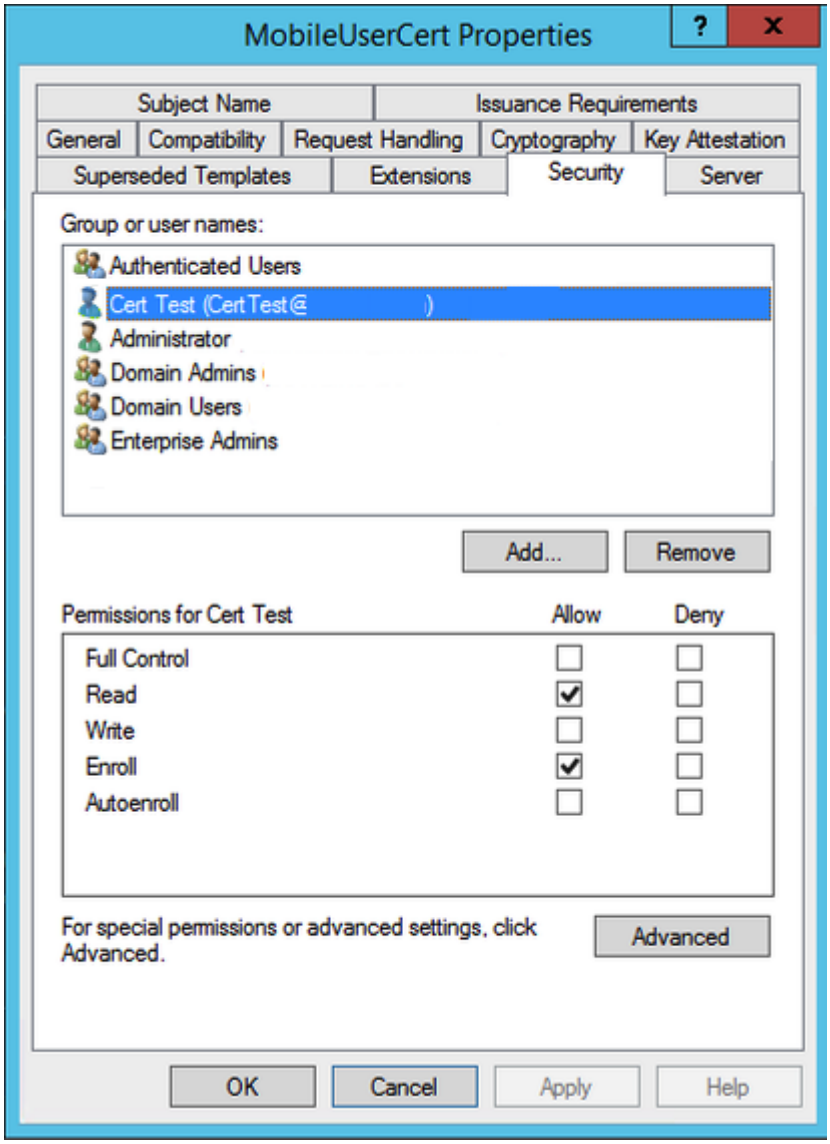
5. ［テンプレート］の表示名を入力します。

   > 重要:
   >
   > 必要な場合のみ、［**Active Directory** の証明書を発行する］チェックボックスをオンにします。このオプションがオンの場合、すべてのユーザークライアント証明書が Active Directory で作成され、Active Directory データベースを圧迫する可能性があります。

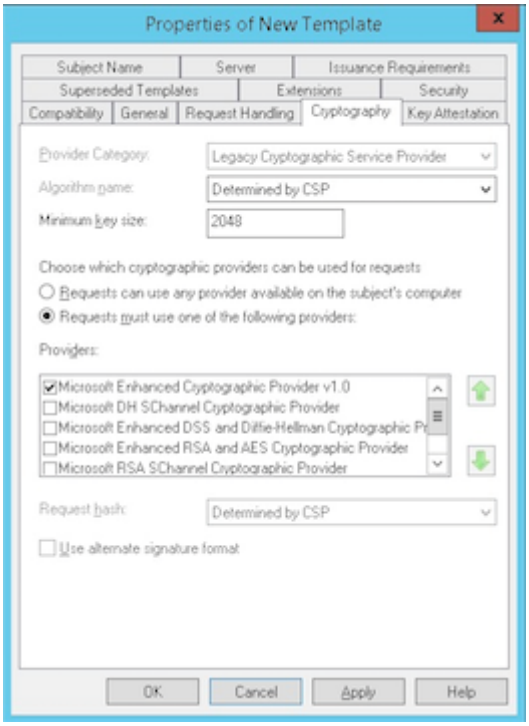
6. テンプレートの種類として［**Windows 2003 Server**］を選択します。Windows 2012 R2 サーバーの［互換性］で、［証明機関］を選択して **Windows 2003** を受信者として設定します。
7. ［セキュリティ］で ［追加］をクリックし、Citrix Endpoint Management が証明書の生成に使用する AD ユーザーアカウントを選択します。

   > 重要:
   >
   > サービスアカウントユーザーのみを追加してください。この AD ユーザーアカウントには、［登録］権限のみを追加します。

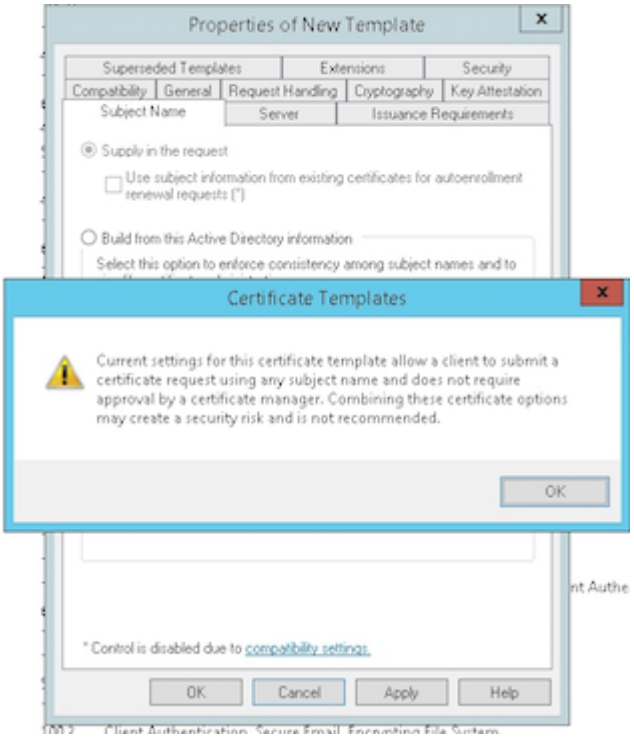
   この記事の後半で説明するように、サービスアカウントを使用してユーザー.pfx 証明書を作成します。詳しくは、「CA サーバーから PFX 証明書を作成する」を参照してください。



8. ［暗号化］に、必ずキーのサイズを指定してください。あとで、Citrix Endpoint Management の構成中にキーのサイズを入力します。



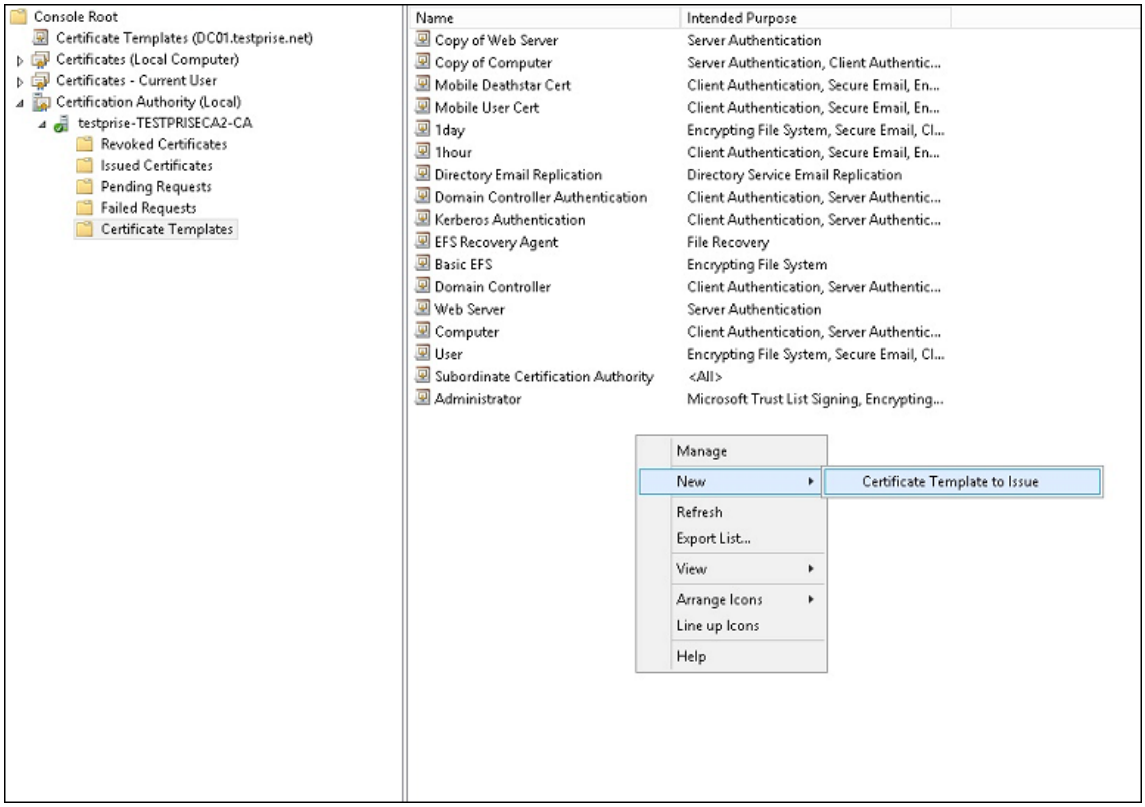
9. ［サブジェクト名］で、［要求に含まれる］を選択します。変更を適用して、保存します。



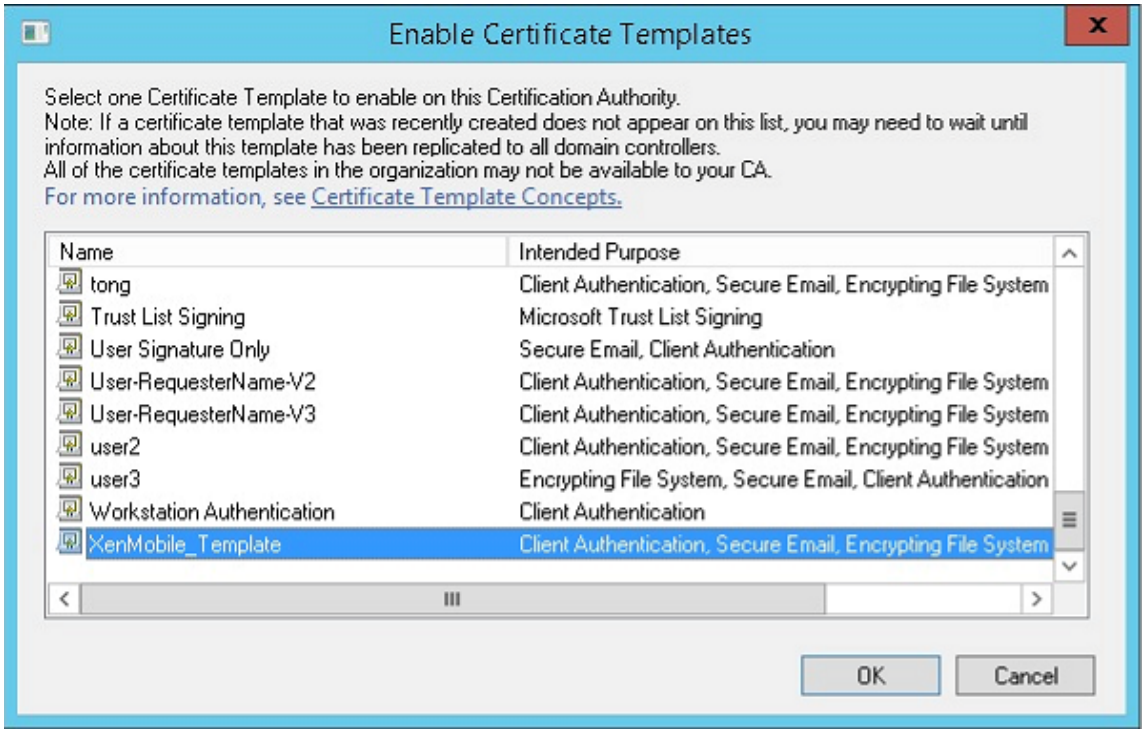
テンプレートを証明機関（**CA**）に追加する

1. ［証明機関］に移動して、［証明書テンプレート］を選択します。

2. 右ペインを右クリックして、［新規］、［発行する証明書テンプレート］の順に選択します。

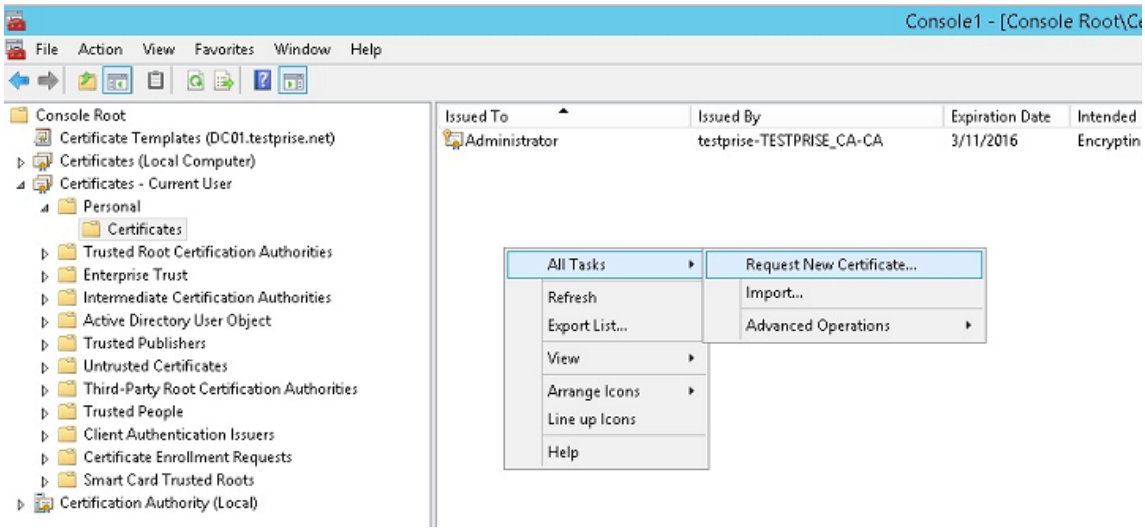


3. 前の手順で作成したテンプレートを選択し、［**OK**］をクリックして ［証明機関］ に追加します。

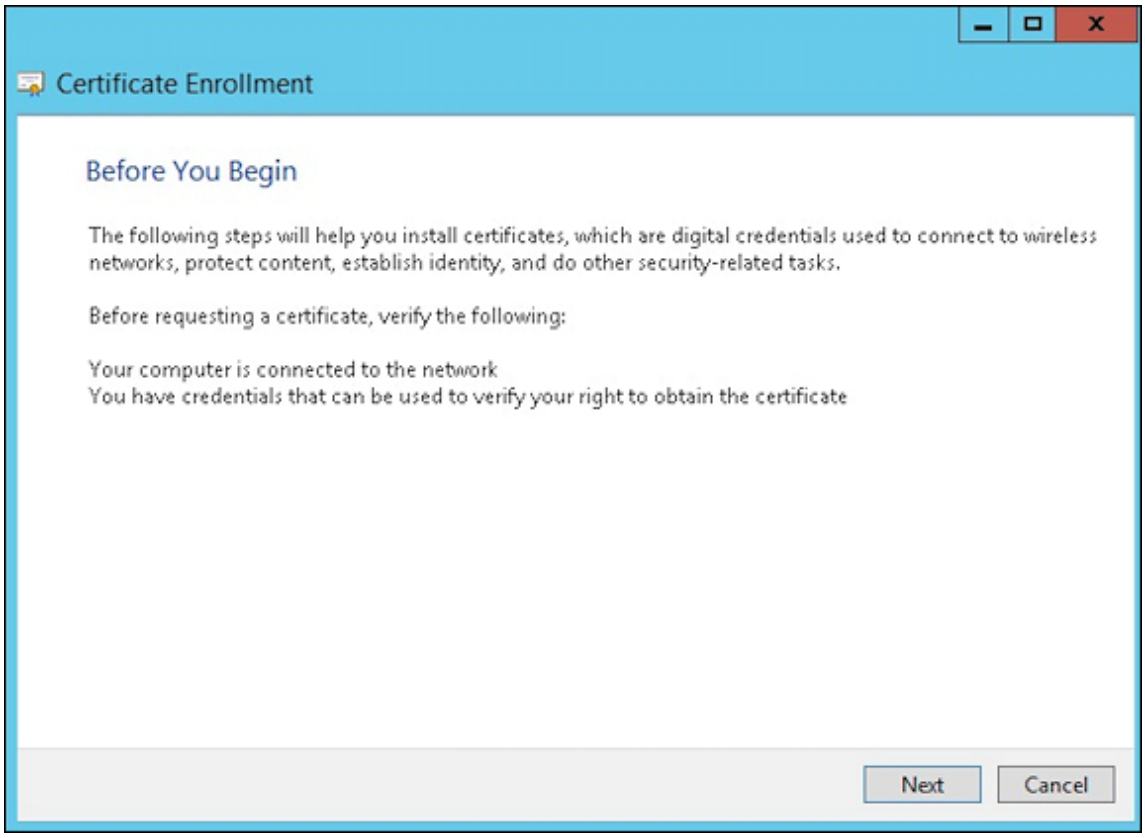


CA サーバーから **PFX** 証明書を作成する

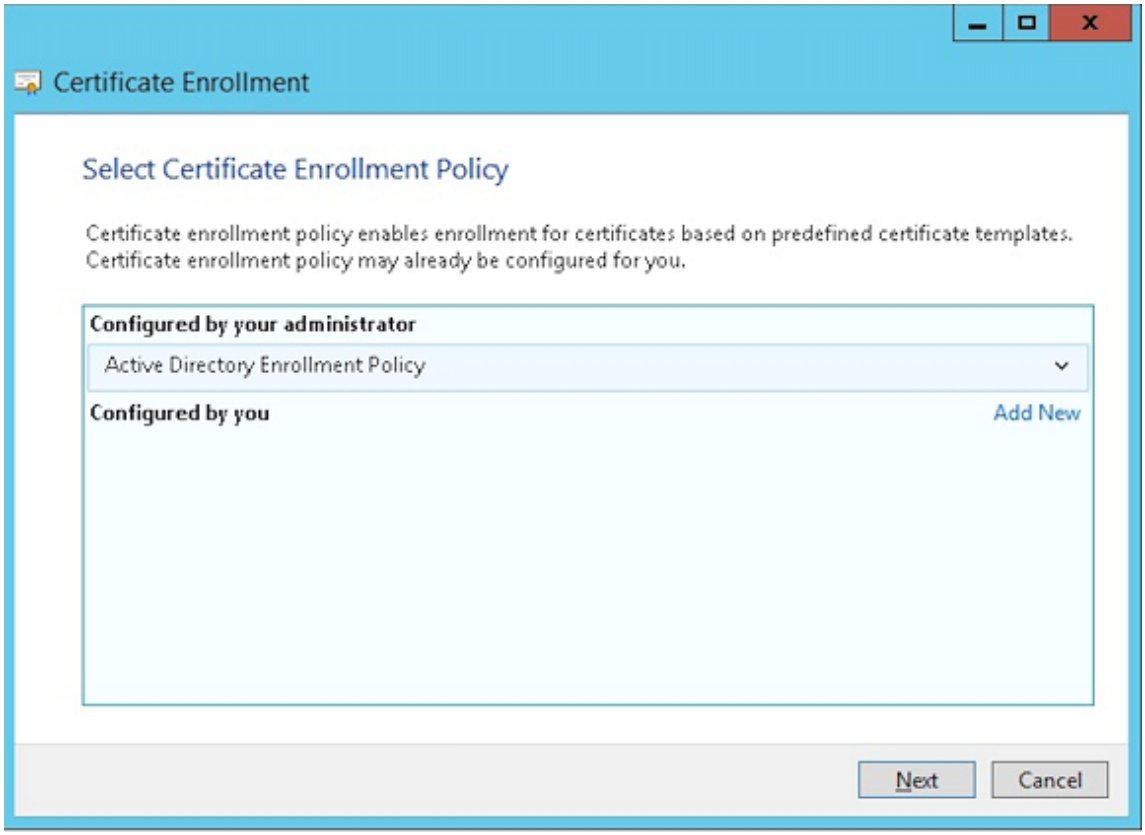
1. ログインしたサービスアカウントで、ユーザー.pfx cert を作成します。この.pfx ファイルは Citrix Endpoint Management にアップロードされ、デバイスを登録するユーザーのためにユーザー証明書を要求します。
2. ［現在のユーザー］で、［証明書］を展開します。
3. 右ペインで右クリックし、［新しい証明書の要求］をクリックします。



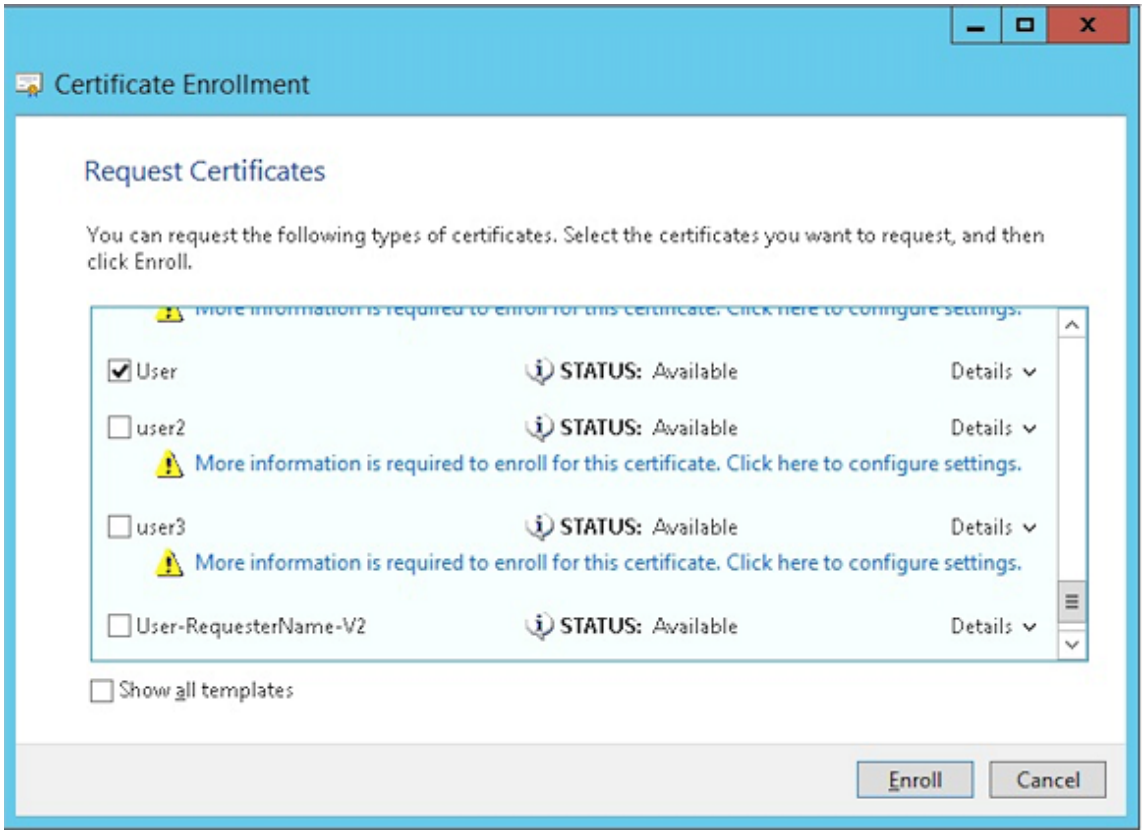
4. ［証明書の登録］画面が開きます。［次へ］をクリックします。



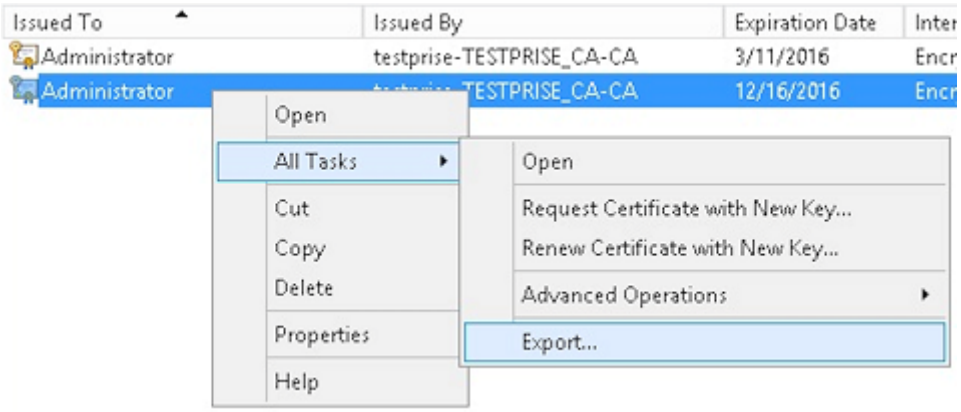
5. [**Active Directory** 登録ポリシー] を選択して [次へ] をクリックします。



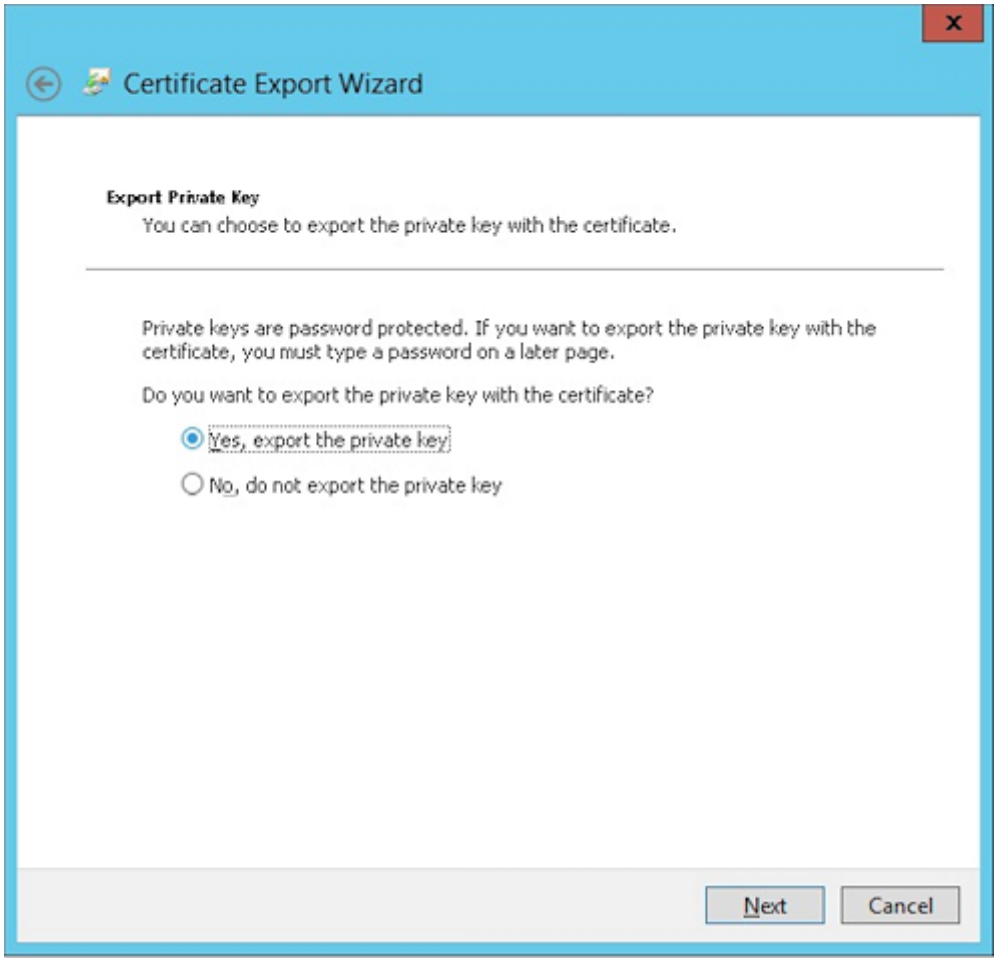
6. [ユーザー] テンプレートを選択し、[登録] をクリックします。



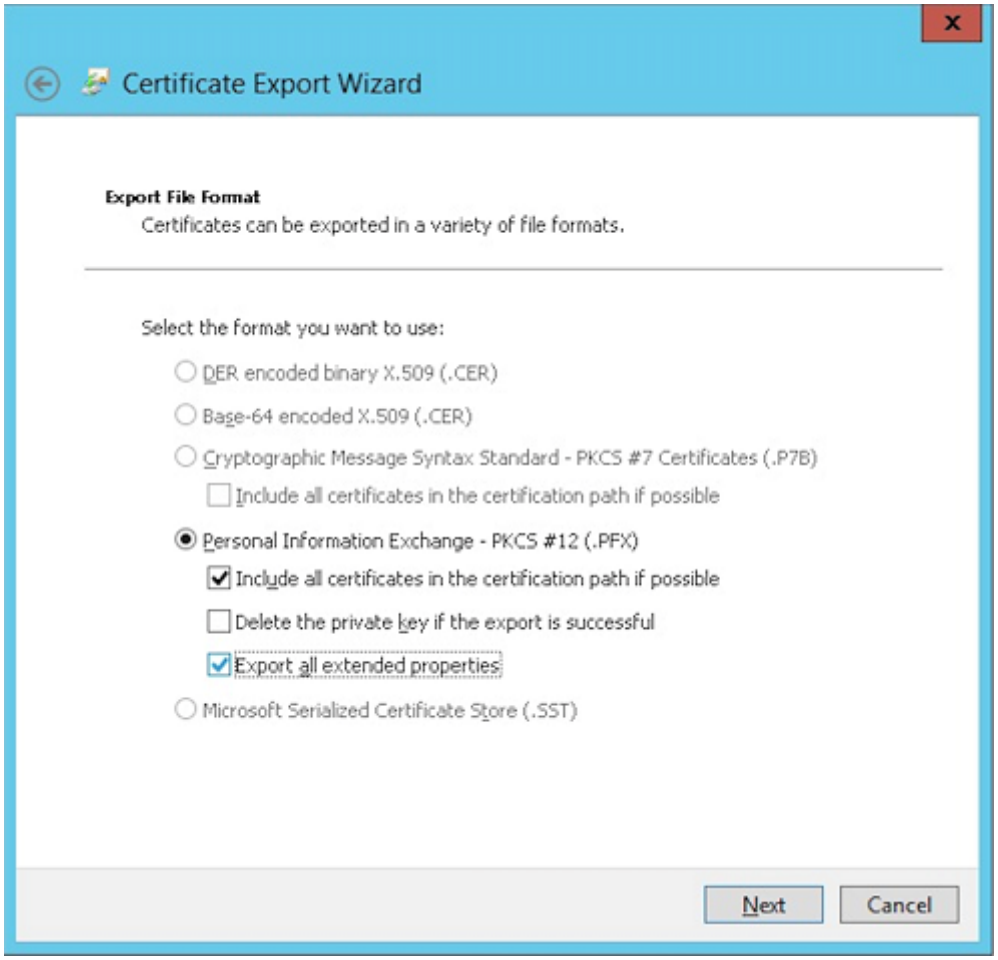
7. 前の手順で作成した.pfx ファイルをエクスポートします。



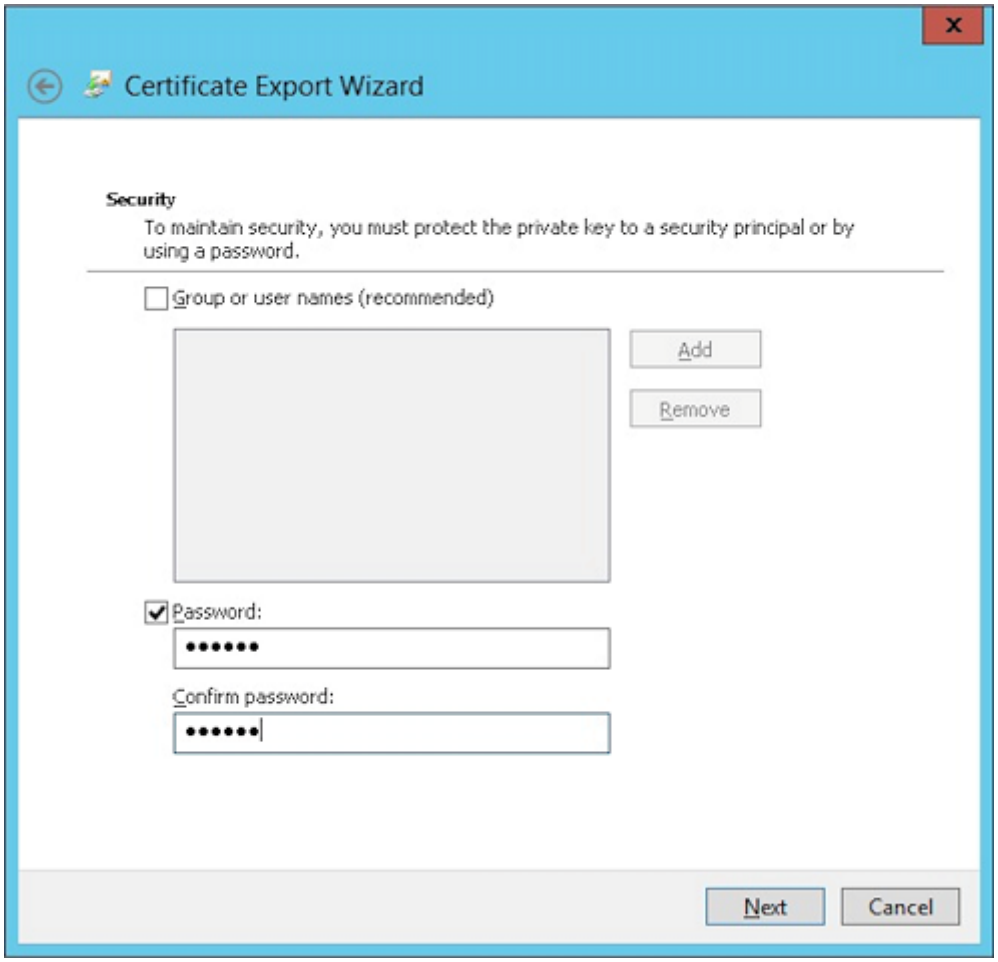
8. [はい、秘密キーをエクスポートします] をクリックします。



9. ［証明のパスにある証明書を可能であればすべて含む］を選択し、［すべての拡張プロパティをエクスポートする］チェックボックスをオンにします。



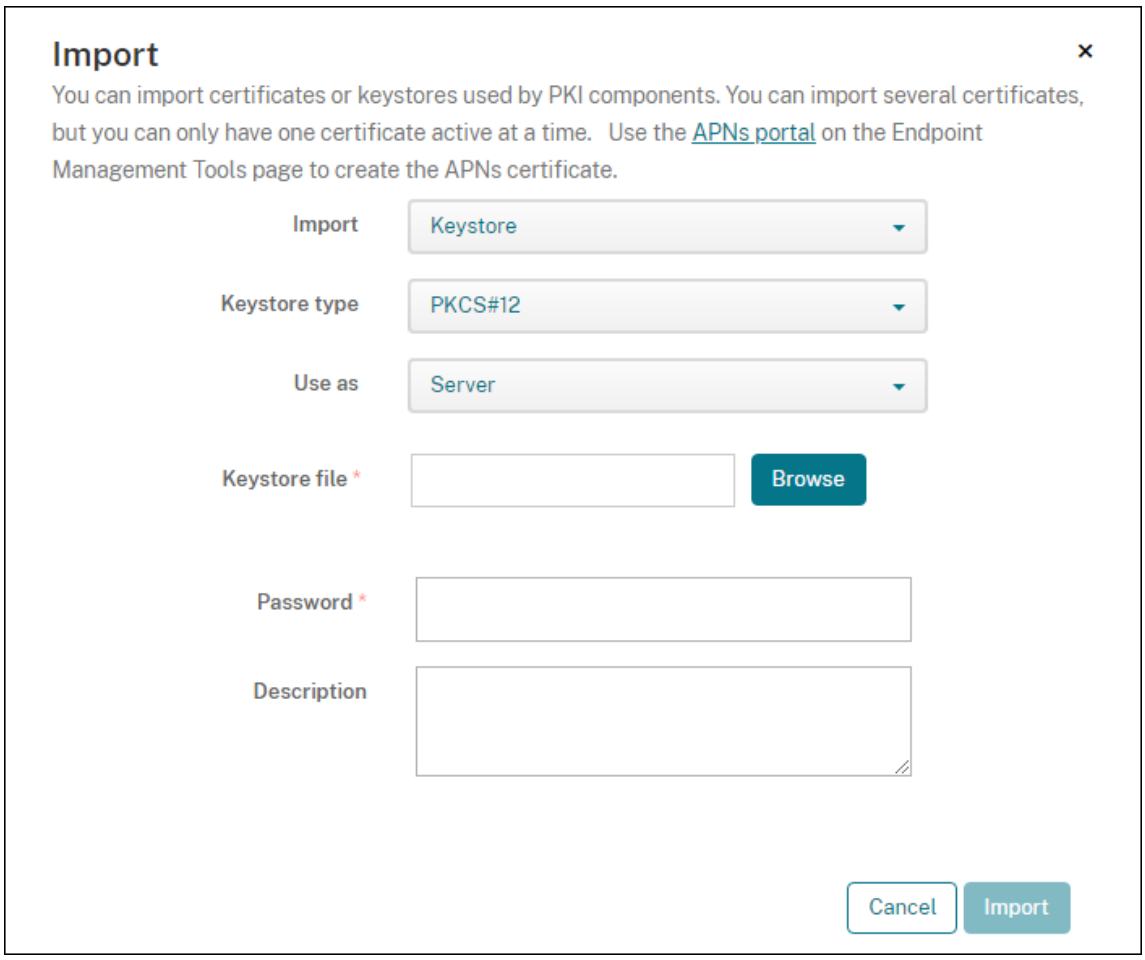
10. Citrix Endpoint Management にこの証明書をアップロードするときに使用するパスワードを設定します。



11. 証明書をローカルのハードドライブに保存します。

Citrix Endpoint Management への証明書のアップロード

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］画面が表示されます。
2. ［証明書］をクリックしてから、［インポート］をクリックします。
3. 以下のパラメーターを入力します。
   - インポート：キーストア
   - キーストアの種類： PKCS#12
   - 使用目的：サーバー
   - キーストアファイル：［参照］をクリックして、前の手順で作成した.pfx 証明書を選択します。
   - パスワード：この証明書用に作成したパスワードを入力します。

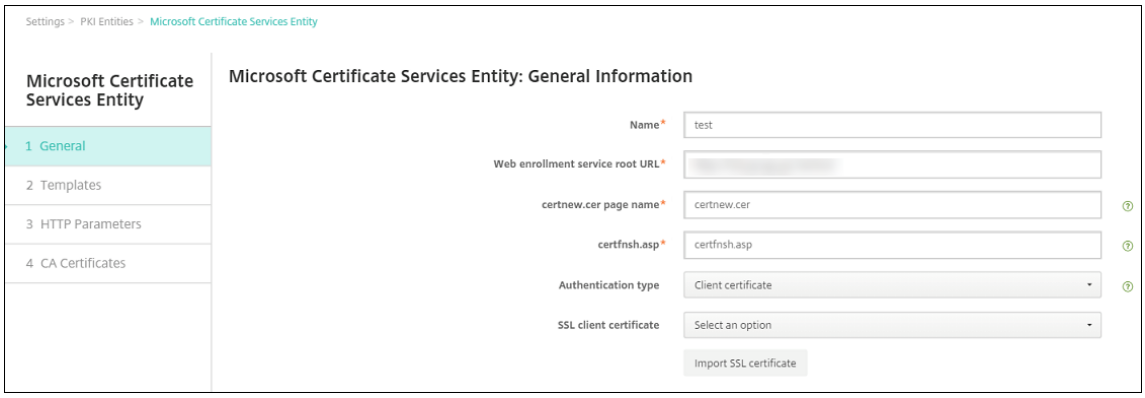


4. ［インポート］をクリックします。
5. 証明書が正常にインストールされているか確認します。正常にインストールされた証明書がユーザー証明書として表示されます。

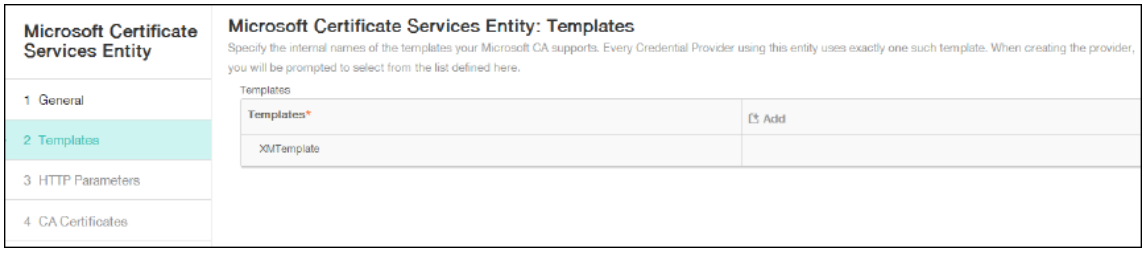
証明書に基づいた認証のための **PKI** エンティティの作成

1. ［設定］で、［詳細］**>**［証明書管理］**>**［**PKI** エンティティ］の順に移動します。
2. ［追加］をクリックしてから、［**Microsoft** 証明書サービスエンティティ］をクリックします。［**Microsoft** 証明書サービスエンティティ：一般的な情報］画面が開きます。
3. 以下のパラメーターを入力します。
   - 名前：任意の名前を入力します。
   - **Web** 登録サービスルート **URL**： `https://RootCA-URL/certsrv/`（URL パスの最後にスラッシュ（/）があることを確認してください。）
   - **certnew.cer** ページ名： certnew.cer（デフォルト値）
   - **certfnsh.asp**： certfnsh.asp（デフォルト値）

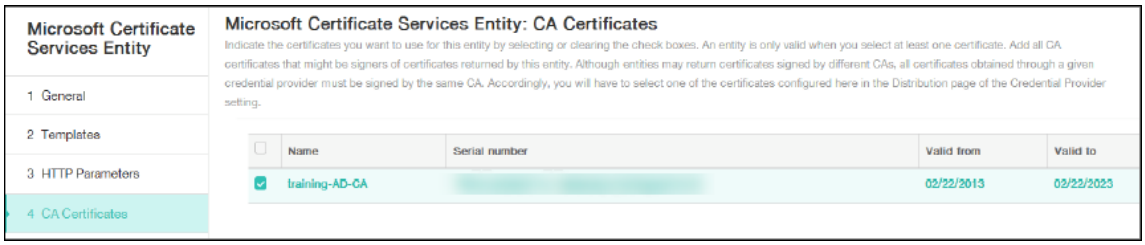
- 認証の種類：クライアント証明書
- **SSL** クライアント証明書： Citrix Endpoint Management クライアント証明書を発行するために使用するユーザー証明書を選択します。証明書が存在しない場合は、前のセクションの手順に従って証明書をアップロードします。



4. ［テンプレート］で、Microsoft 証明書を構成したときに作成したテンプレートを追加します。スペースを追加しないでください。



5. HTTP パラメーターをスキップし、［**CA** 証明書］をクリックします。
6. 環境内で関連するルート CA 証明書の名前を選択します。このルート CA 証明書は、Citrix Endpoint Management クライアント証明書からインポートされたチェーンの一部です。

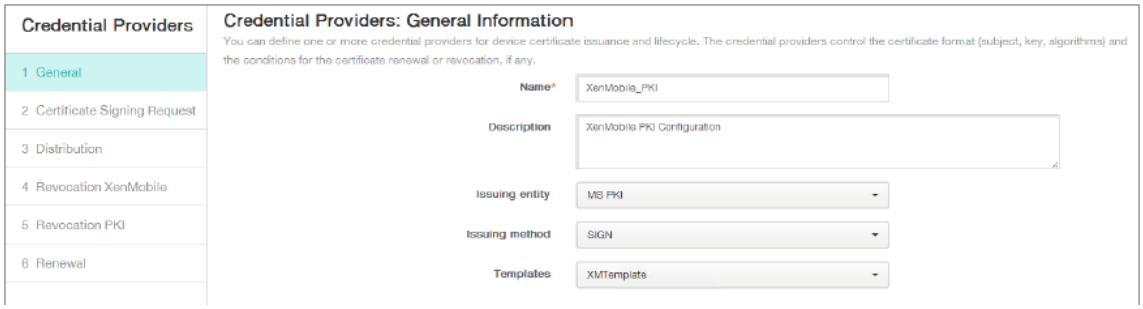


7. ［保存］をクリックします。

資格情報プロバイダーの構成

1. ［設定］で、［詳細］**>**［証明書管理］**>**［資格情報プロバイダー］の順に移動します。
2. ［追加］をクリックします。
3. ［全般］で、次のパラメーターを入力します：

- 名前：任意の名前を入力します。
- 説明：任意の説明を入力します。
- 発行エンティティ：前に作成した PKI エンティティを選択します。
- 発行方式： SIGN
- テンプレート： PKI エンティティに追加されたテンプレートを選択します。



4. ［証明書署名要求］をクリックしてから、次のパラメーターを入力します：

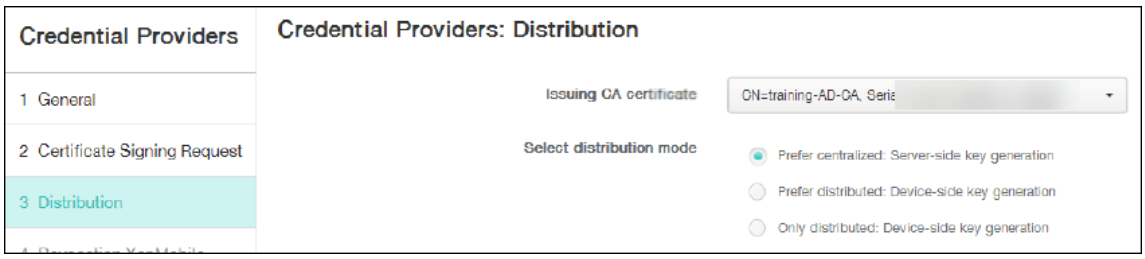
   - キーアルゴリズム： RSA
   - キーサイズ： 2048
   - 署名アルゴリズム： SHA256withRSA
   - サブジェクト名： `cn=$user.username`

   ［サブジェクトの別名］の ［追加］をクリックしてから、次のパラメーターを入力します：

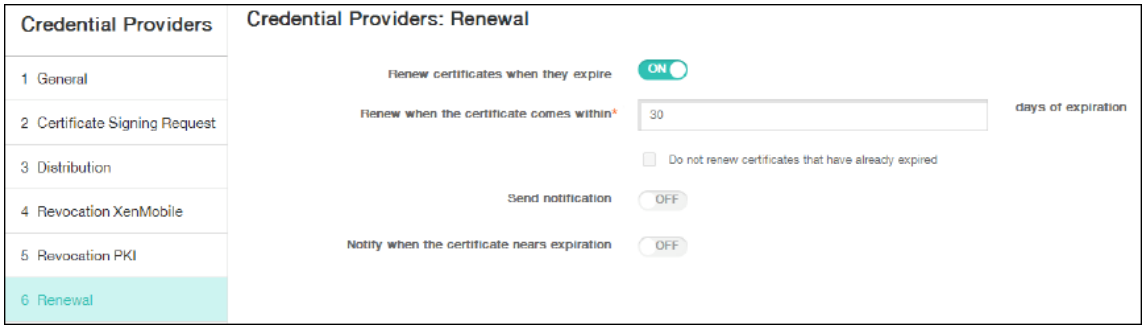
   - 種類：ユーザープリンシパル名
   - 値： `$user.userprincipalname`

5. ［説明］をクリックし、次のパラメーターを入力します：

   - 発行 **CA** 証明書：署名済みの Citrix Endpoint Management クライアント証明書の発行 CA を選択します。
   - ディストリビューションモードの選択：［集中を優先：サーバー側のキー生成］を選択します。



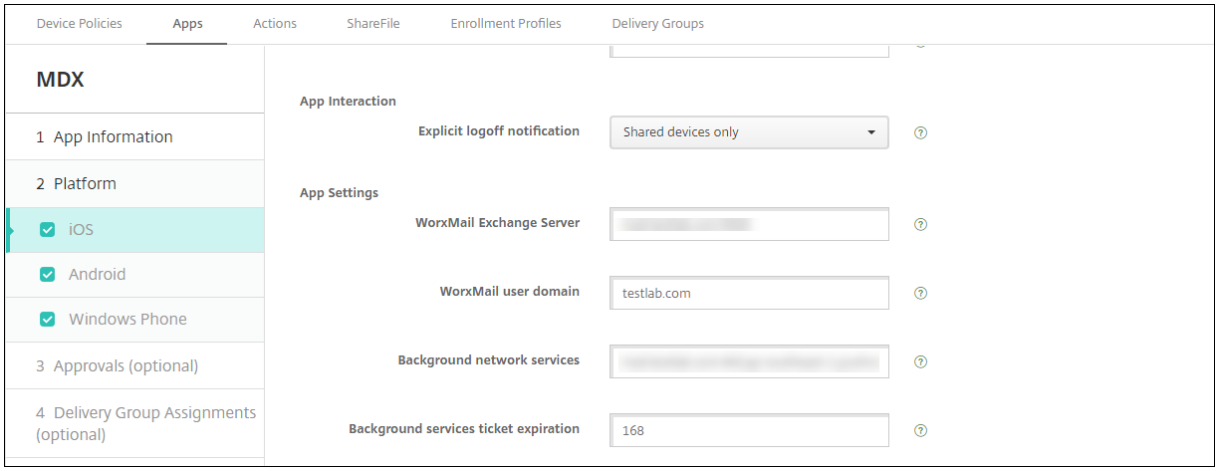
6. 次の 2 つのセクション（失効 **Citrix Endpoint Management** と失効 **PKI**）で必要なパラメーターを設定します。この例では、どちらのオプションもスキップします。
7. ［更新］をクリックします。
8. ［有効期限が切れたら証明書を書き換える］を有効にします。
9. そのほかの設定はすべてそのままにするか、必要な変更を加えます。



10. ［保存］をクリックします。

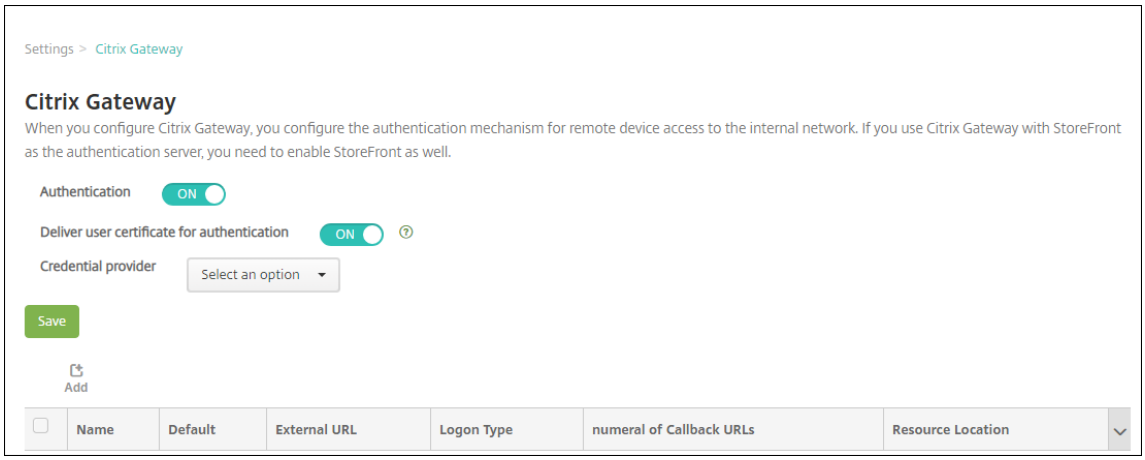
証明書ベースの認証を使用するように **Citrix Secure Mail** を構成する

Citrix Endpoint Management に Citrix Secure Mail を追加する場合、必ず ［アプリ設定］で Exchange の設定を構成してください。

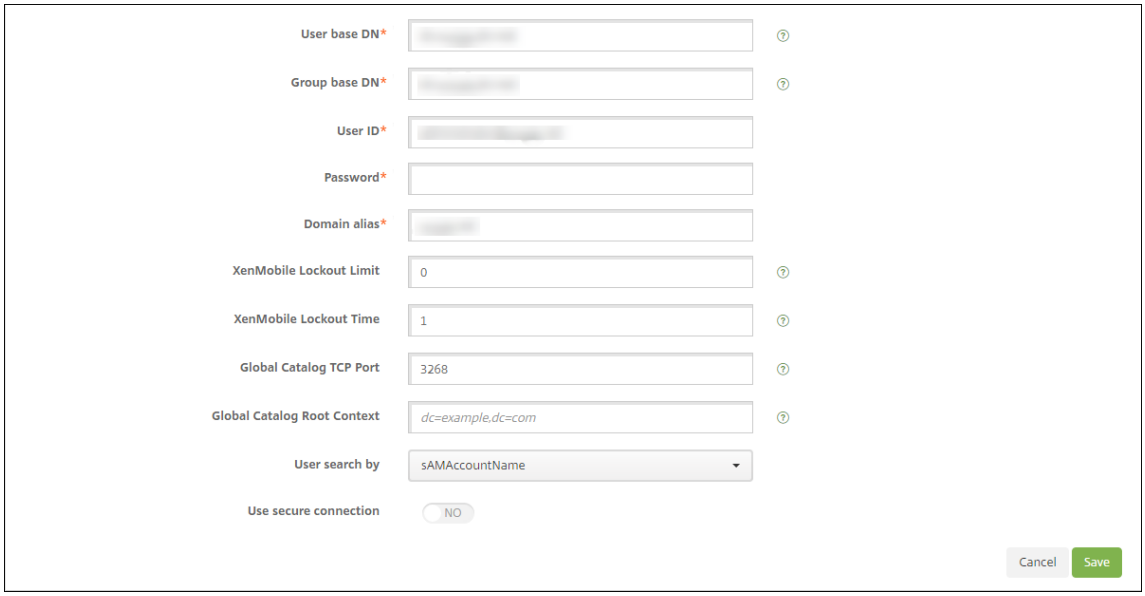


Citrix Endpoint Management での **Citrix Gateway** 証明書の配信の構成

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］画面が表示されます。
2. ［サーバー］の下の ［**Citrix Gateway**］をクリックします。
3. Citrix Gateway がまだ追加されていない場合、［追加］をクリックして、次のように設定を指定します:
   - 名前: アプライアンスの説明的な名前を入力します。
   - エイリアス: アプライアンスのオプションのエイリアスを入力します。
   - 外部 **URL**: `https://YourCitrixGatewayURL`
   - ログオンの種類: ［証明書およびドメイン］を選択します。
   - パスワードが必要: オフ
   - デフォルトとして設定: オン
4. ［認証］および ［認証用のユーザー証明書を配信］で ［オン］を選択します。



5. ［資格情報プロバイダー］でプロバイダーを選択し、［保存］をクリックします。
6. ユーザープリンシパル名（UPN）の代替としてユーザー証明書の sAMAccount 属性を使用するには、Citrix Endpoint Management の LDAP コネクタを次のように構成します:［設定］**>** ［**LDAP**］に移動し、ディレクトリを選択して ［編集］をクリックし、［ユーザー検索基準］で ［**sAMAccountName**］を選択します。



Citrix PIN とユーザーパスワードキャッシュの有効化

Citrix PIN とユーザーパスワードキャッシュを有効化するには、［設定］**>**［クライアントプロパティ］に移動し、チェックボックス ［**Citrix PIN** 認証の有効化］および ［ユーザーパスワードキャッシュの有効化］をオンにします。詳しくは、「クライアントプロパティ」を参照してください。

クライアント証明書構成のトラブルシューティング

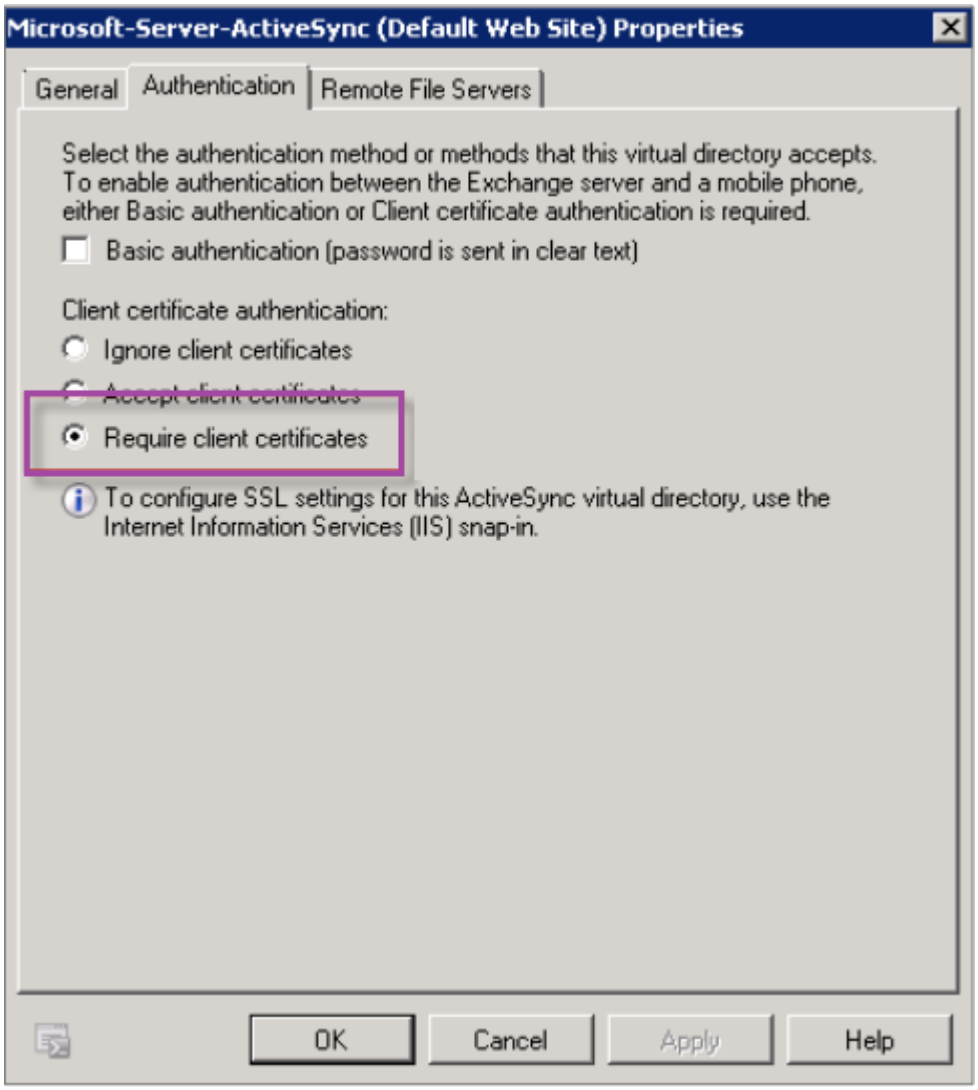
先行する構成と Citrix Gateway の構成が成功すると、ユーザーワークフローは次のようになります:

1. ユーザーがモバイルデバイスを登録します。
2. Citrix Endpoint Management がユーザーに Citrix PIN を作成するよう求めます。
3. ユーザーがアプリストアにリダイレクトされます。
4. Citrix Secure Mail の起動時、Citrix Endpoint Management はメールボックスの構成でユーザー資格情報を要求しません。その代わりに、Citrix Secure Mail は Citrix Secure Hub からのクライアント証明書を要求し、認証のために Microsoft Exchange Server に送信します。ユーザーが Citrix Secure Mail を起動したときに Citrix Endpoint Management で資格情報を求められた場合は、構成を確認してください。

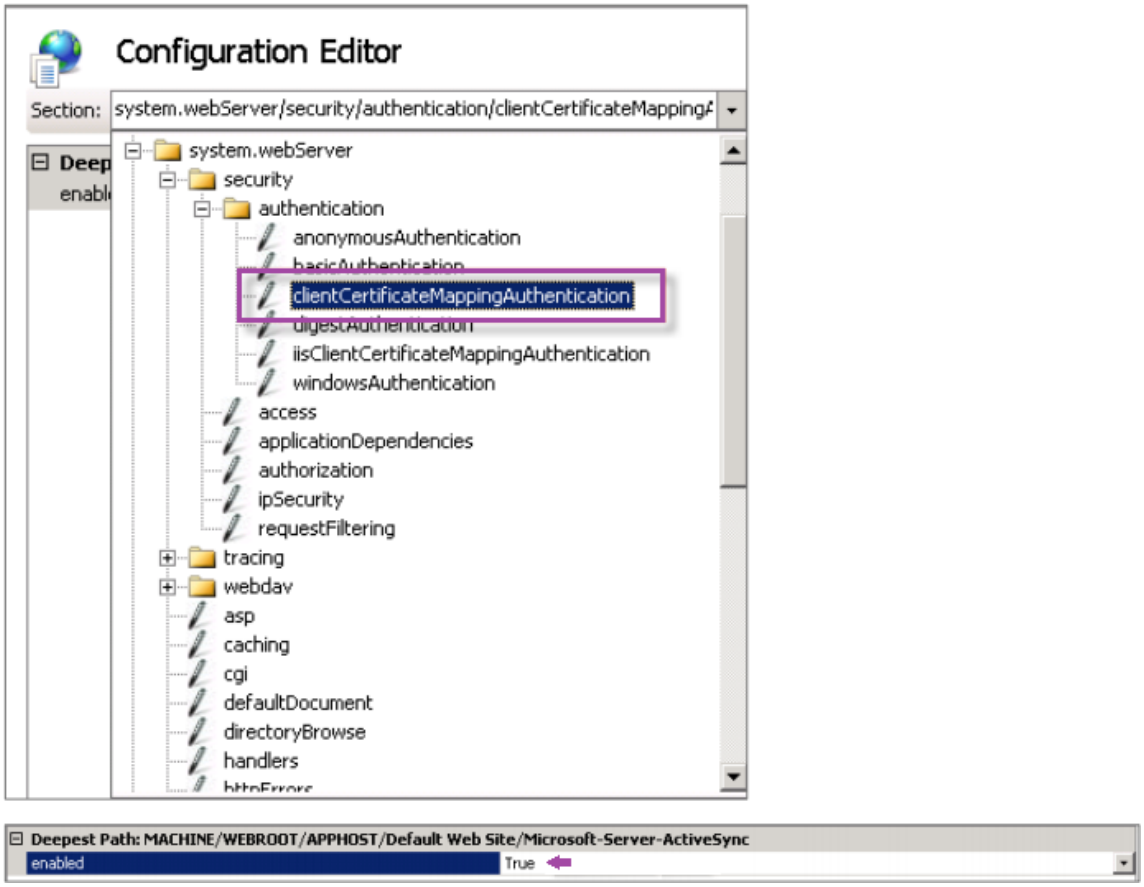
ユーザーは Citrix Secure Mail をダウンロードしてインストールできるが、Citrix Secure Mail でメールボックス構成時に構成を完了できない場合:

1. Microsoft Exchange Server ActiveSync がプライベート SSL サーバー証明書を使用してトラフィックを保護している場合、ルート証明書または中間証明書がモバイルデバイスにインストールされていることを確認してください。

2. ActiveSync に対して選択された認証の種類が ［クライアント証明書を要求する］であることを確認します。



3. Microsoft Exchange Server で、**Microsoft-Server-ActiveSync** サイトのクライアント証明書マッピング認証が有効になっていることを確認します。デフォルトでは、クライアント証明書マッピング認証は無効になっています。オプションは、［**Configuration Editor**］**>** ［**Security**］**>** ［**Authentication**］にあります。



［**True**］を選択したら、必ず ［適用］をクリックして変更を反映してください。

4. Citrix Endpoint Management コンソールで Citrix Gateway 設定を確認します：［認証用のユーザー証明書を配信］が ［オン］で、［資格情報プロバイダー］で適切なプロファイルが選択されていることを確認してください。

クライアント証明書がモバイルデバイスに配信されたかどうかを判定するには

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］と移動して、デバイスを選択します。
2. ［編集］または ［詳細表示］をクリックします。
3. ［デリバリーグループ］セクションに移動し、以下のエントリを検索します：

   Citrix Gateway 資格情報：必要な資格情報、**CertId=**

クライアント証明書ネゴシエーションが有効かどうか確認するには

1. この`netsh`コマンドを実行して、IIS Web サイトにバインドされた SSL 証明書構成を表示します。

   ```
   netsh http show sslcert
   ```


2. ［クライアント証明書のネゴシエート］の値が ［無効］の場合、次のコマンドを実行して有効化します：

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash
appid={ app_id } certstorename=store_name verifyclientcertrevocation
=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck
=Enable clientcertnegotiation=Enable
```

例：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf98
 appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=
ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

Citrix Endpoint Management を介して Windows Phone 8.1 デバイスにルート証明書または中間証明書を配信できない場合：

- 電子メールを介して Windows Phone 8.1 デバイスにルート証明書または中間証明書（.cer）ファイルを送信し、直接インストールします。

Citrix Secure Mail が Windows Phone 8.1 に正常にインストールされない場合は、以下を確認してください：

- Enterprise ハブデバイスポリシーを使用して、Citrix Endpoint Management 経由でアプリケーション登録トークン（.AETX ファイル）が配信されている。
- アプリケーション登録トークンが、Citrix Secure Mail のラップおよび Citrix Secure Hub アプリの署名に使用された証明書プロバイダーからのエンタープライズ証明書と同じものを使用して作成されている。
- Citrix Secure Hub、Citrix Secure Mail、アプリケーション登録トークンのラップと署名に同一の発行者 ID が使用されている。

PKI エンティティ

December 8, 2023

Citrix Endpoint Management の PKI（Public Key Infrastructure：公開キー基盤）エンティティ構成とは、実際の PKI 処理（発行、失効、状態情報）を実行するコンポーネントのことです。これらのコンポーネントには、Citrix Endpoint Management 内部のものと外部のものがあります。内部コンポーネントは、任意として参照されます。外部コンポーネントは企業インフラストラクチャの一部です。

Citrix Endpoint Management は、次の種類の PKI エンティティをサポートします：

- Microsoft 証明書サービス

- 任意 CA（Certificate Authority：証明機関）

Citrix Endpoint Management では、以下の CA サーバーがサポートされます：

- Windows Server 2016
- Windows Server 2019

> 注：
>
> Windows Server 2012 R2、2012、および 2008 R2 は製品終了（EOL）となったため、サポートされなくなりました。詳しくは、Microsoft 社の製品に関するライフサイクルドキュメントを参照してください。

共通の **PKI** 概念

種類に関係なく、すべての PKI エンティティには以下の機能のサブセットがあります。

- 署名：証明書署名要求（CSR）に基づく新しい証明書の発行
- フェッチ：既存の証明書とキーペアの回収
- 失効：クライアント証明書の失効

CA 証明書

PKI エンティティの構成時には、そのエンティティにより発行される（またはそのエンティティから回収される）証明書の署名者である CA 証明書を Citrix Endpoint Management に指定します。その PKI エンティティから、複数の異なる CA が署名した、（フェッチされたか、または新たに署名された）証明書が返されることがあります。

これらの証明機関それぞれの証明書を、PKI エンティティ構成の一部として提供します。これを行うには、証明書を Citrix Endpoint Management にアップロードして、PKI エンティティでそれらを参照します。任意 CA の場合、証明書は暗黙的に署名 CA 証明書です。外部エンティティの場合は、証明書を手動で指定する必要があります。

> 重要：
>
> Microsoft 証明書サービスのエンティティテンプレートを作成する場合は、登録済みデバイスの認証に関する問題を避けるため、テンプレート名に特殊文字を使用しないでください。たとえば、以下は使用しないでください：`! : $ ( )# % + * ~ ? | { } [ ]`

Microsoft 証明書サービス

Citrix Endpoint Management は、Web 登録インターフェイスを通じて Microsoft 証明書サービスと連携します。Citrix Endpoint Management は、このインターフェイスを使用した新しい証明書の発行のみをサポートします。Microsoft CA が Citrix Gateway ユーザー証明書を生成する場合、Citrix Gateway はこれらの証明書の更新と失効をサポートします。

Citrix Endpoint Management で Microsoft CA PKI エンティティを作成するには、証明書サービスの Web インターフェイスのベース URL を指定する必要があります。必要に応じて、SSL クライアント認証で Citrix Endpoint Management と証明書サービスの Web インターフェイス間の接続を保護できます。

Microsoft Certificate Services エンティティを追加する

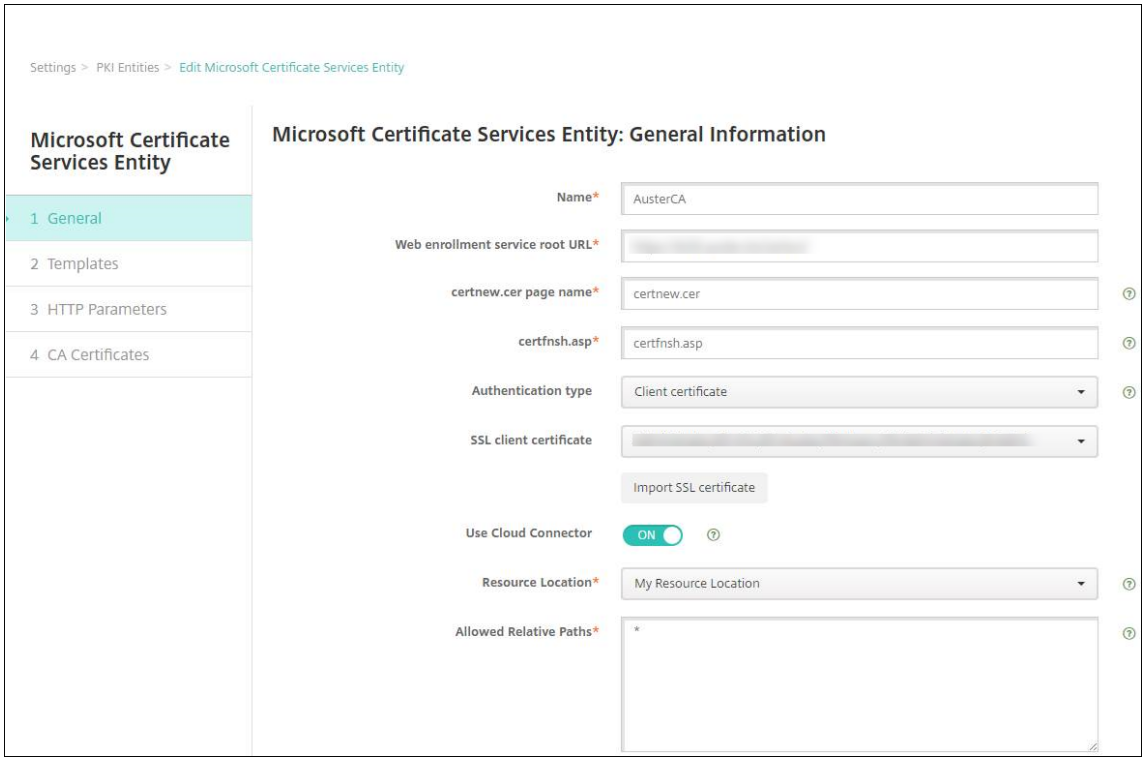
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックし、[**PKI** エンティティ] をクリックします。
2. [**PKI** エンティティ] ページで、[追加] をクリックします。

   PKI エンティティタイプのメニューが表示されます。
3. [**Microsoft** 証明書サービスエンティティ] をクリックします。

   [**Microsoft** 証明書サービスエンティティ**:** 一般的な情報] ページが開きます。
4. [**Microsoft** 証明書サービスエンティティ**:** 一般的な情報] ページで次の設定を構成します。

   - 名前: 新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意の名前にする必要があります。
   - **Web** 登録サービスルート **URL**: Microsoft CA Web 登録サービスのベース URL を入力します。例: `https://192.0.0.1/certsrv/`。URL には、HTTP または HTTP-over-SSL を使用します。
   - **certnew.cer** ページ名: certnew.cer ページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
   - **certfnsh.asp**: certfnsh.asp ページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
   - 認証の種類: 使用する認証方法を選択します。
     - なし
     - **HTTP** 基本: 接続に必要なユーザー名とパスワードを指定します。
     - クライアント証明書: 適切な SSL クライアント証明書を選択します。
   - **Cloud Connector** を使用します: [オン] を選択して Cloud Connector を使用して PKI サーバーに接続します。次に、[リソースの場所] と接続を [許可する相対パス] を指定します。
     - リソースの場所: Citrix Cloud Connectorで定義されているリソースの場所から選択します。
     - 許可する相対パス: 指定したリソースの場所に対して許可する相対パス。1 行に 1 つのパスを指定します。ワイルドカード文字としてアスタリスク (*) を使用できます。

       リソースの場所が`https://www.ServiceRoot/certsrv`である場合。そのパス内のすべての URL にアクセスできるようにするには、[許可する相対パス] に`/*`と入力します。



5. [接続のテスト] をクリックして、サーバーにアクセスできることを確認します。アクセスできない場合は、接続が失敗したことを示すメッセージが表示されます。構成設定を確認してください。
6. [次へ] をクリックします。

   [**Microsoft** 証明書サービスエンティティ: テンプレート] ページが開きます。このページで、Microsoft CA がサポートするテンプレートの内部名を指定します。資格情報プロバイダーを作成するとき、ここで定義したテンプレートを一覧で選択します。このエンティティを使用するすべての資格情報プロバイダーが、このようなテンプレートを 1 つだけ使用します。

   Microsoft Certificate Services テンプレートの要件については、お使いの Microsoft Server バージョンの Microsoft ドキュメントを参照してください。Citrix Endpoint Management には、「証明書」で説明している証明書形式以外、配布する証明書についての要件はありません。
7. [**Microsoft** 証明書サービスエンティティ: テンプレート] ページで [追加] をクリックし、テンプレートの名前を入力して、[保存] をクリックします。追加する各テンプレートについて、この手順を繰り返します。
8. [次へ] をクリックします。

   [**Microsoft** 証明書サービスエンティティ: **HTTP** パラメーター] ページが開きます。このページで、Microsoft Web 登録インターフェイスに対する HTTP 要求に Citrix Endpoint Management が追加するカスタムパラメーターを指定します。カスタムパラメーターは、CA で実行されているカスタマイズされたスクリプトでのみ有効です。
9. [**Microsoft** 証明書サービスエンティティ: **HTTP** パラメーター] ページで [追加] をクリックし、追加する HTTP パラメーターの名前と値を入力して、[次へ] をクリックします。

［**Microsoft** 証明書サービスエンティティ：**CA** 証明書］ページが開きます。このページでは、このエンティティを通じてシステムが取得する証明書の署名者を Citrix Endpoint Management に通知する必要があります。CA 証明書が更新された場合は、Citrix Endpoint Management の証明書も更新してください。変更内容は、Citrix Endpoint Management からエンティティに透過的に適用されます。

10. ［**Microsoft** 証明書サービスエンティティ：**CA** 証明書］ページで、このエンティティで使用する証明書を選択します。
11. ［保存］をクリックします。

    ［PKI エンティティ］の表にエンティティが表示されます。

Citrix Gateway 証明書失効一覧（**CRL**）

Citrix Endpoint Management は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートしています。Microsoft CA を構成済みの場合、Citrix Endpoint Management は Citrix Gateway を使用して失効を管理します。

クライアント証明書ベースの認証を構成する場合、［**Enable CRL Auto Refresh**］で Citrix Gateway 証明書失効一覧（CRL）設定を構成するかどうか検討します。この手順を使用すると、MAM のみモードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できなくなります。

ユーザー証明書は失効後もユーザーが自由に生成できるため、Citrix Endpoint Management は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

任意 **CA**

CA 証明書と関連の秘密キーを Citrix Endpoint Management に提供すると、任意 CA が作成されます。Citrix Endpoint Management は、管理者が指定したパラメーターに従って、証明書の発行、失効、および状態情報を内部で処理します。

任意 CA を構成するときに、その CA に対して OCSP（Online Certificate Status Protocol）サポートをアクティブにできます。OCSP サポートを有効にした場合、CA は発行する証明書に`id-pe-authorityInfoAccess`拡張を追加します。この拡張は、次の場所にある Citrix Endpoint Management の内部 OCSP レスポンダーを参照します：

```
https://<server>/<instance>/ocsp
```

OCSP サービスを構成するときに、該当の任意エンティティの OCSP 署名証明書を指定する必要があります。CA 証明書そのものを署名者として使用できます。CA 秘密キーの不必要な漏えいを防ぐには（推奨）：CA 証明書で署名された、委任 OCSP 署名証明書を作成し、`id-kp-OCSPSigning extendedKeyUsage`拡張を含めます。

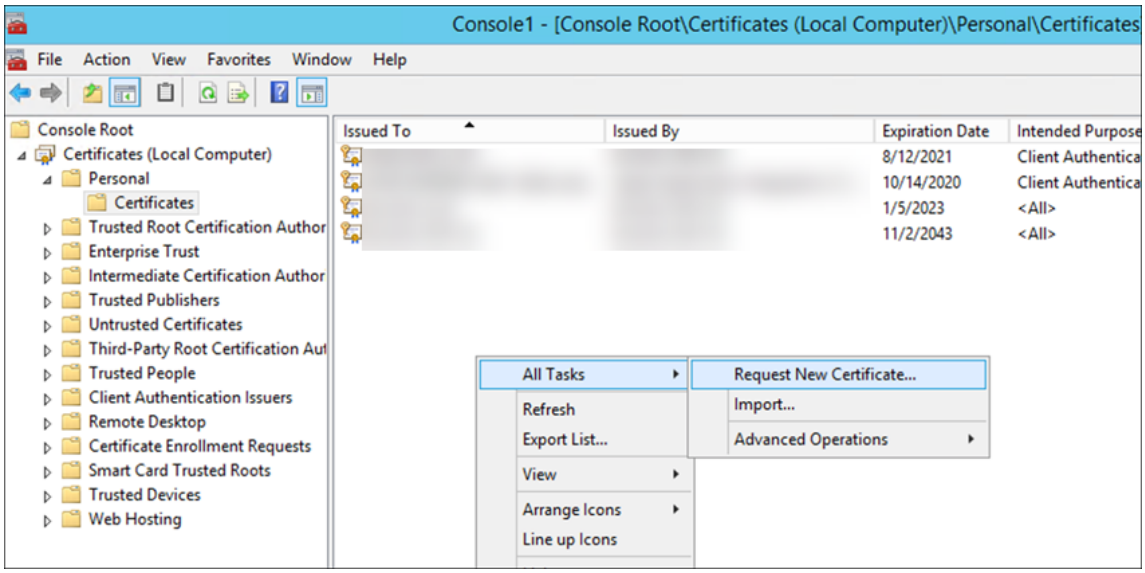
Citrix Endpoint Management OCSP レスポンダーサービスは、基本の OCSP 応答に加え、要求で以下のハッシュアルゴリズムをサポートします：

- SHA-256
- SHA-384
- SHA-512

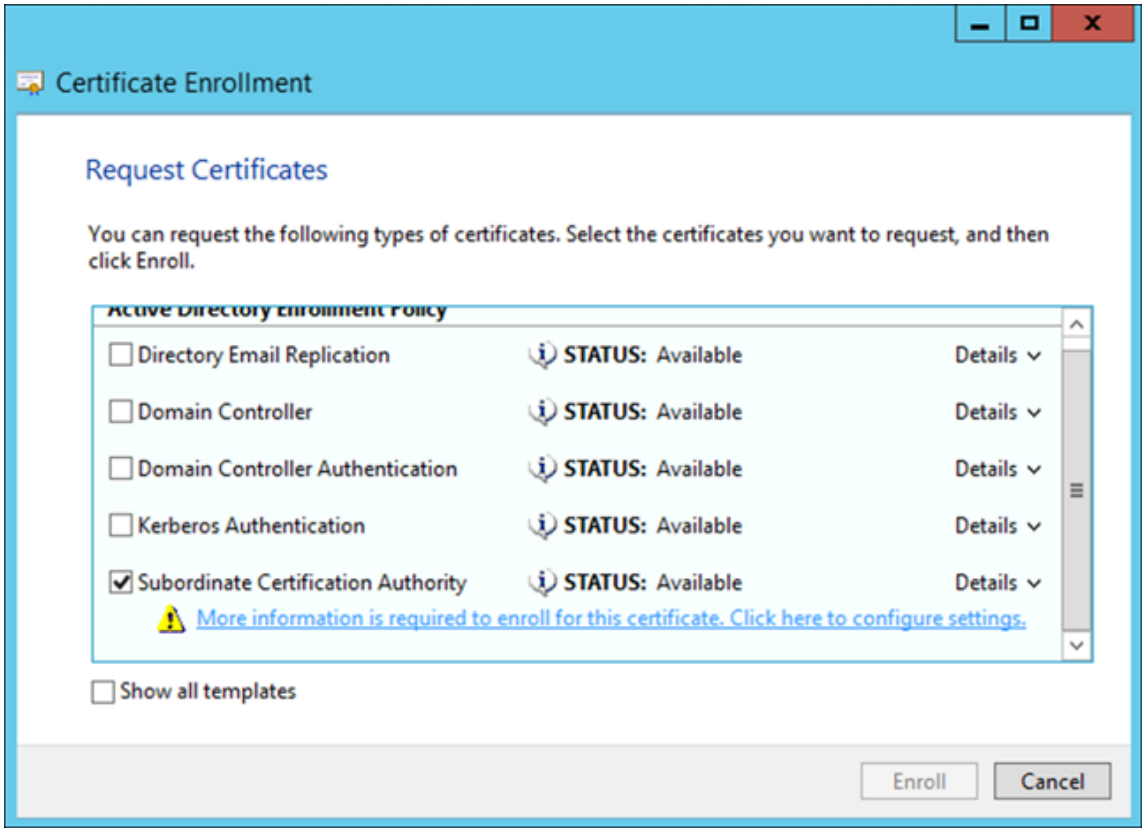
応答は SHA-256 および署名証明書キーアルゴリズム（DSA、RSA または ECDSA）で署名されます。

証明機関の証明書を生成してインポートする

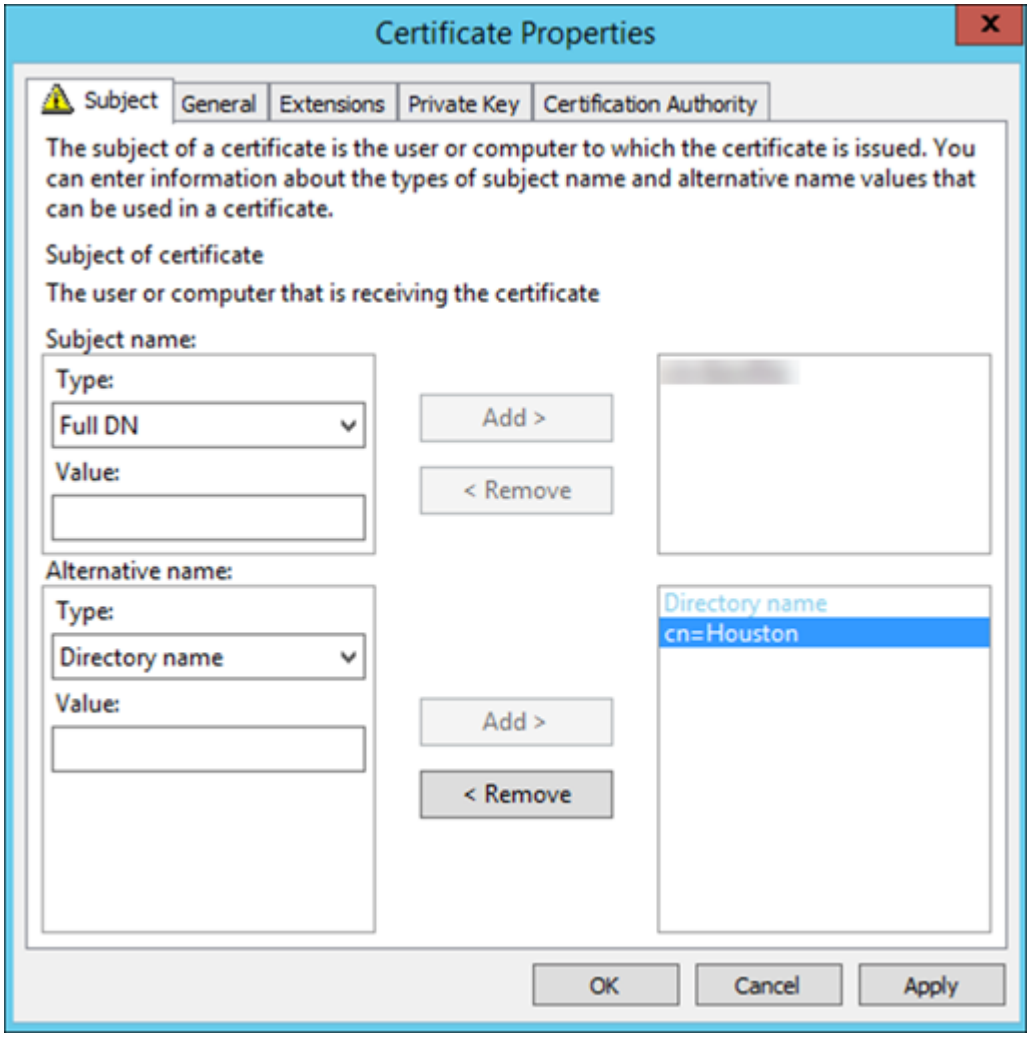
1. サーバーで、Local System アカウントを使用して Microsoft 管理コンソール（MMC）を開き、証明書スナップインを開きます。右ペインで右クリックし、［すべてのタスク］**>**［新しい証明書の要求］をクリックします。



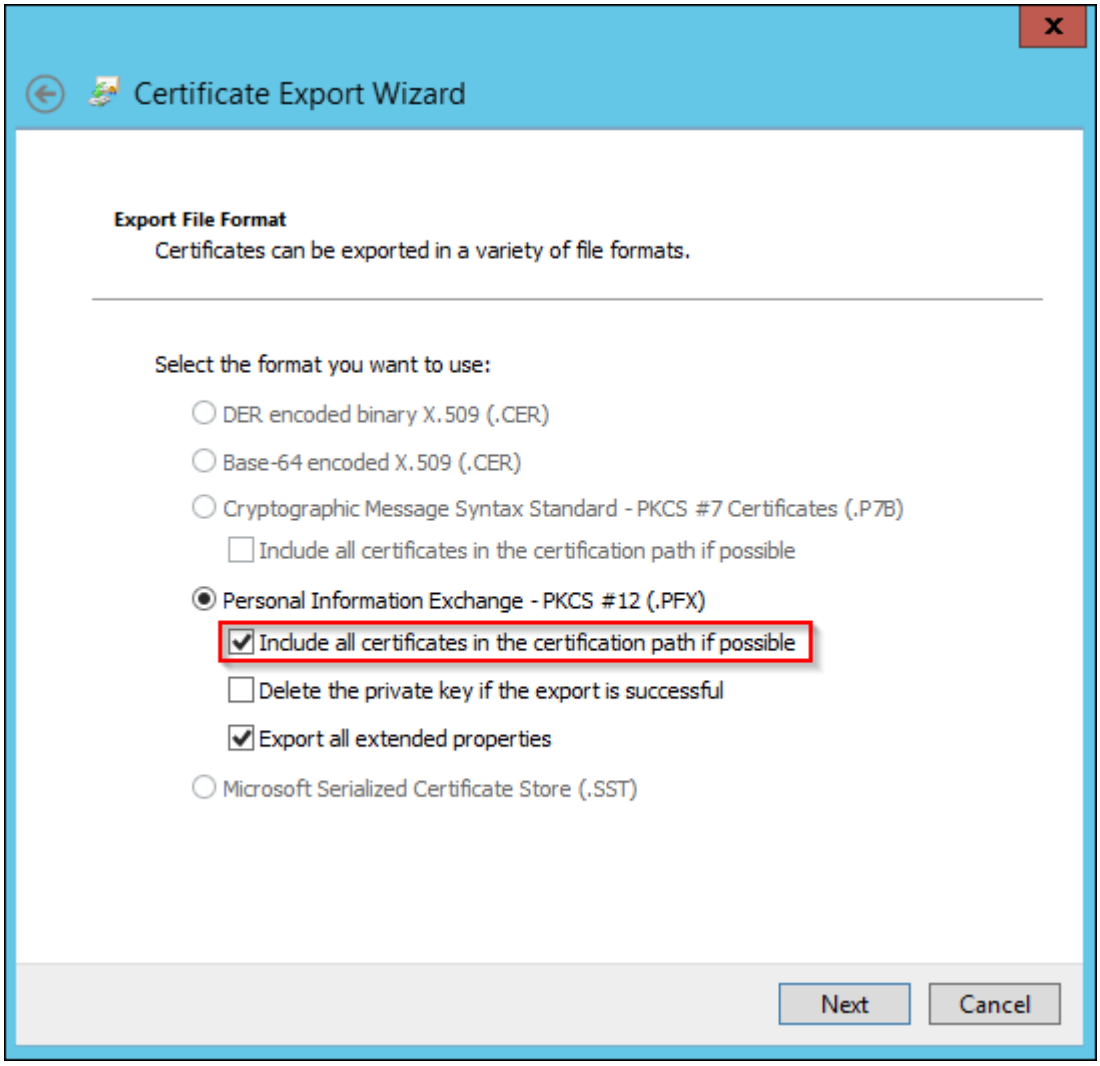
2. 開いたウィザードで、［次へ］を 2 回クリックします。［証明書の要求］一覧で、［下位証明機関］を選択し、［詳細情報］リンクをクリックします。



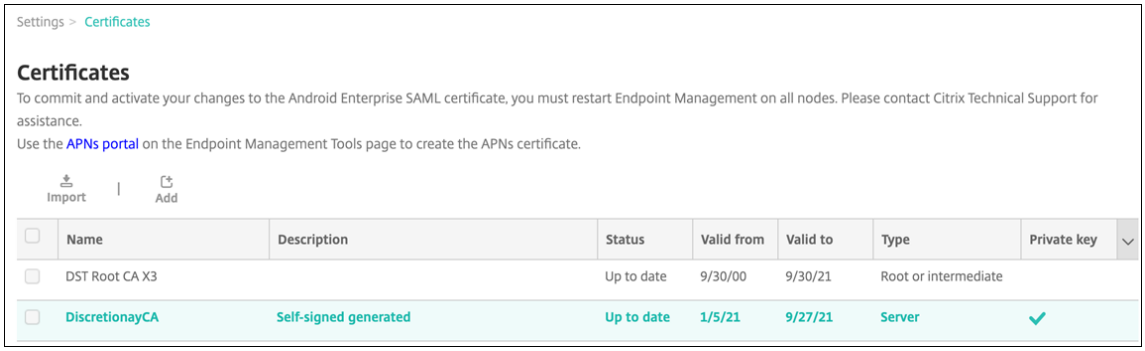
3. ウィンドウに、サブジェクト名と代替名を入力します。[**OK**] をクリックします。



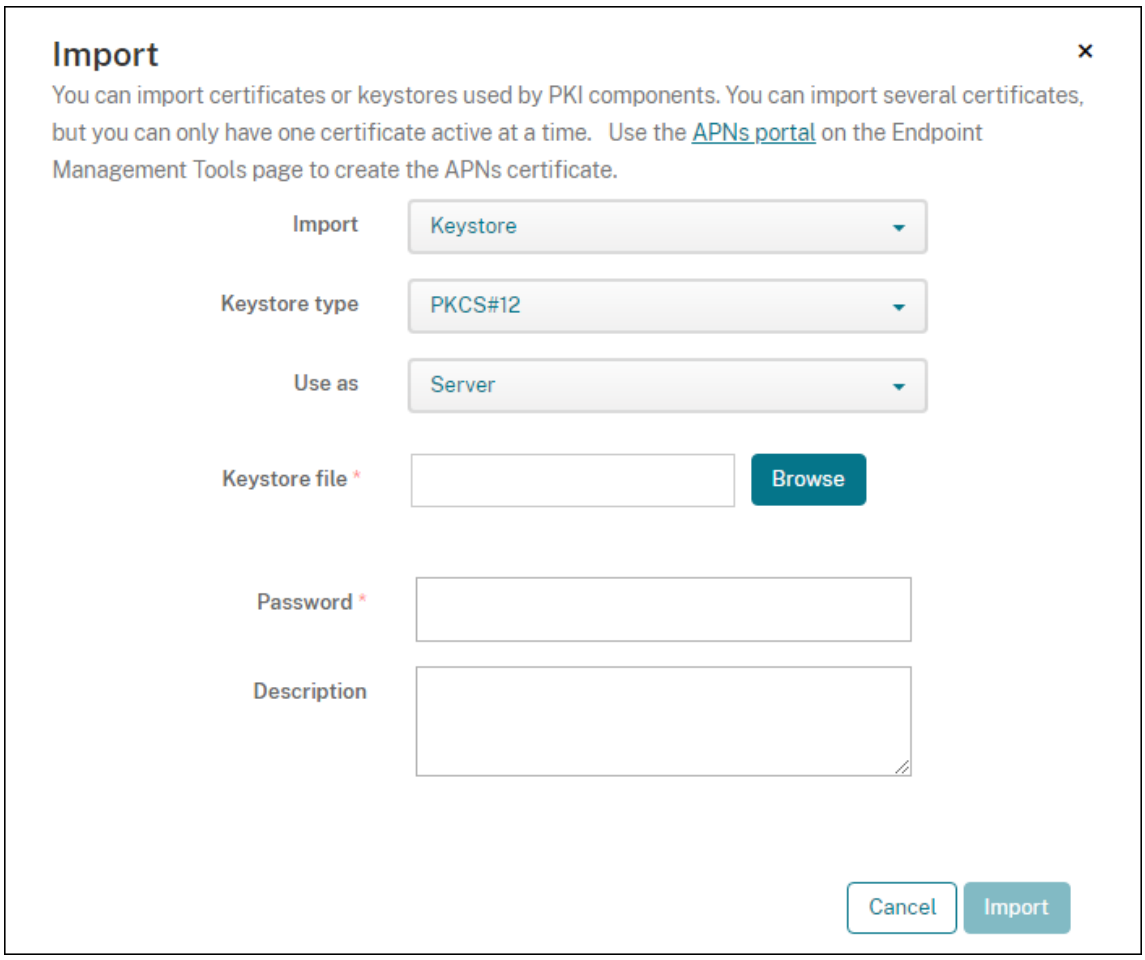
4. ［登録］をクリックしてから ［完了］をクリックします。
5. MMC で、作成した証明書を右クリックします。［すべてのタスク］**>**［エクスポート］の順にクリックします。証明書を.pfx ファイルとして秘密キーと一緒にエクスポートします。［証明のパスにある証明書を可能であればすべて含む］オプションを選択します。



6. Citrix Endpoint Management コンソールで、［設定］**>**［証明書］の順に選択します。



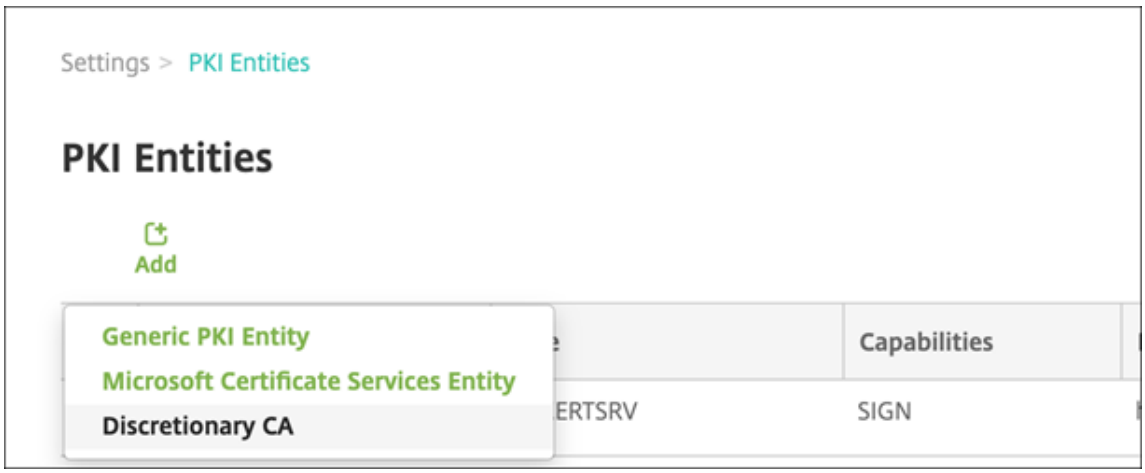
7. ［インポート］をクリックします。開いたウィンドウで、以前にエクスポートした証明書と秘密キーのファイルを参照します。



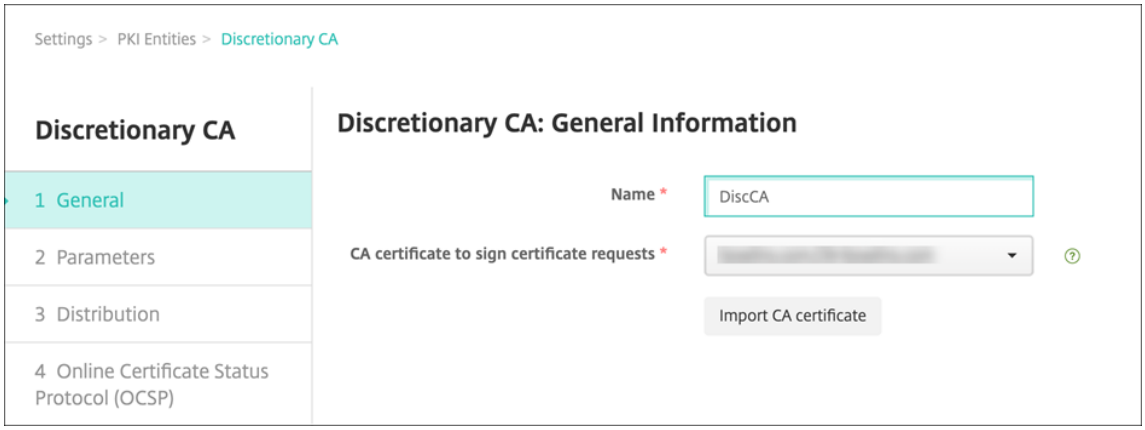
8. ［インポート］をクリックします。証明書が表に追加されます。

任意 **CA** を追加する

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックし、［詳細］**>**［**PKI** エンティティ］の順にクリックします。
2. ［**PKI** エンティティ］ページで、［追加］をクリックします。



3. ［任意 **CA**］をクリックします。

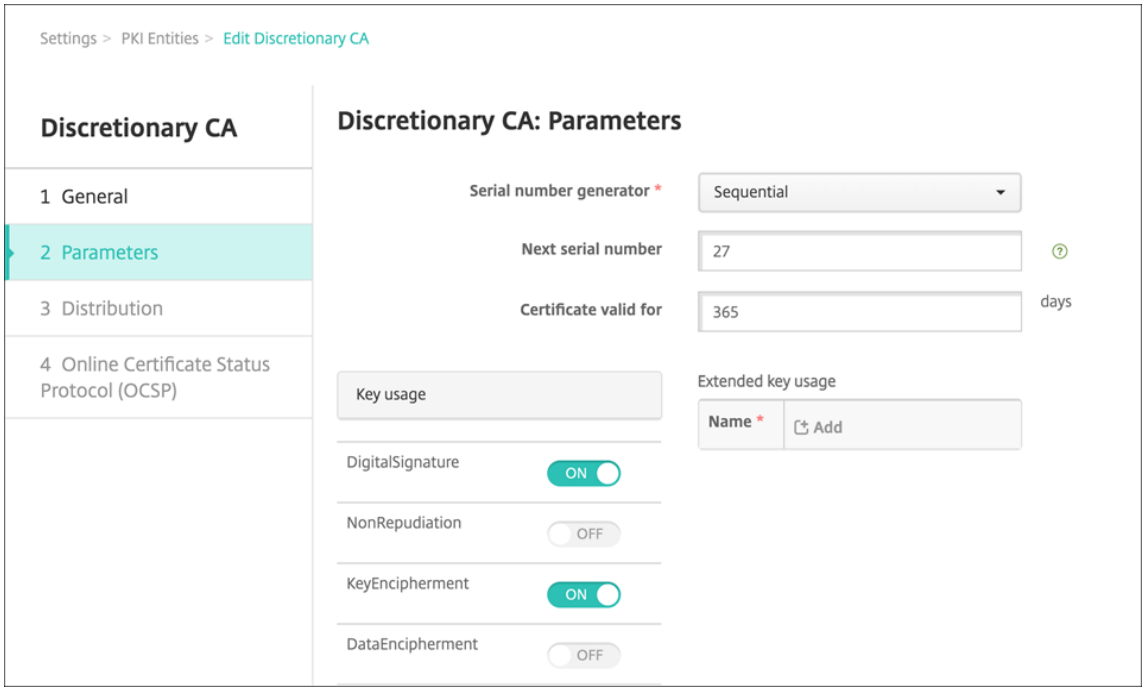


4. ［任意 **CA**：一般情報］ページで、以下を行います：

   - 名前：任意 CA の説明的な名前を入力します。
   - 証明書要求に署名するための **CA** 証明書：一覧から、証明書要求に署名するために使用する任意 CA の証明書を選択します。

     この証明書の一覧は、［構成］**>**［設定］**>**［証明書］で Citrix Endpoint Management にアップロードした、秘密キー付きの CA 証明書から生成されます。

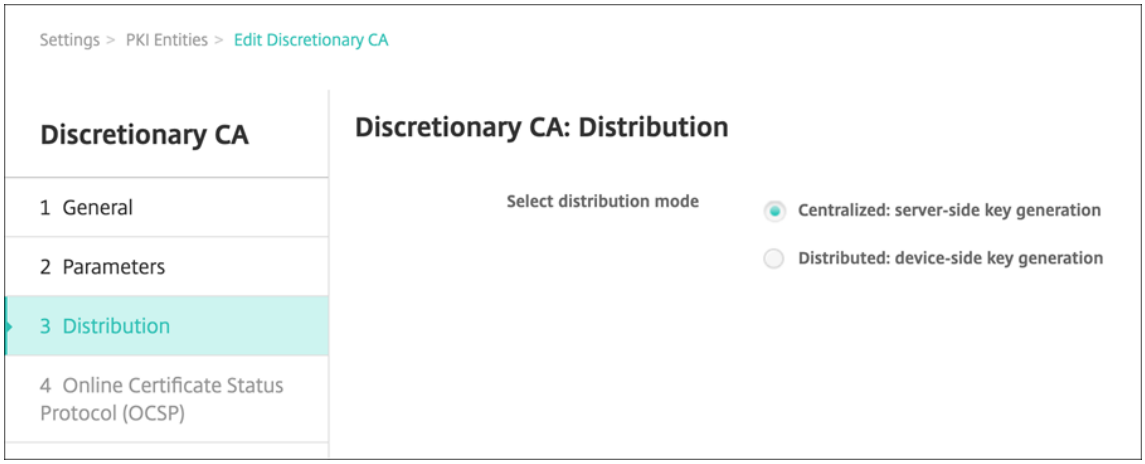
5. ［次へ］をクリックします。



6. [任意 **CA**：パラメーター] ページで、以下を行います：

   - シリアル番号ジェネレーター：任意 CA は発行する証明書のシリアル番号を生成します。一覧で ［シーケンシャル］ または ［非シーケンシャル］ を選択して、番号の生成方法を指定します。
   - 次のシリアル番号：値を入力して、次に発行される番号を指定します。
   - 証明書の有効期限：証明書の有効期間（日数）を入力します。
   - キー使用法：適切なキーを ［オン］ に設定して、任意 CA が発行する証明書の目的を指定します。設定すると、その CA（証明機関）による証明書の発行がそれらの目的に限定されます。
   - 拡張キー使用法：さらにパラメーターを追加するには、［追加］ をクリックし、キー名を入力して ［保存］ をクリックします。

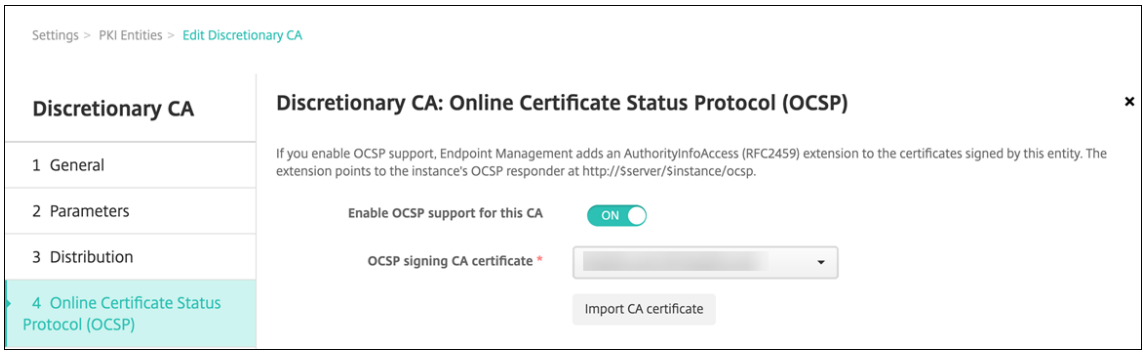
7. [次へ] をクリックします。



8. [任意 **CA**：ディストリビューション] ページで、配布モードを選択します：

- 集中：サーバー側のキー生成。Citrix ではこの集中管理オプションをお勧めします。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
- 分散：デバイス側のキー生成。ユーザーデバイス上で秘密キーが生成されます。この分散モードは SCEP を使用し、**keyUsage keyEncryption** 拡張による RA 暗号化証明書と **keyUsage digitalSignature** 拡張による RA 署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。

9. ［次へ］をクリックします。



10. ［任意 **CA**：**Online Certificate Status Protocol (OCSP)**］ページで、以下を行います：

    - この CA が署名する証明書に`AuthorityInfoAccess`（RFC2459）拡張を追加する場合は、［この **CA** の **OCSP** サポートを有効にする］を ［オン］に設定します。この拡張は、CA の OCSP レスポンダー（`https://<server>/<instance>/ocsp`）を参照します。
    - OCSP サポートを有効にした場合は、OSCP 署名 CA 証明書を選択します。この証明書一覧は、Citrix Endpoint Management にアップロードした CA 証明書から生成されます。

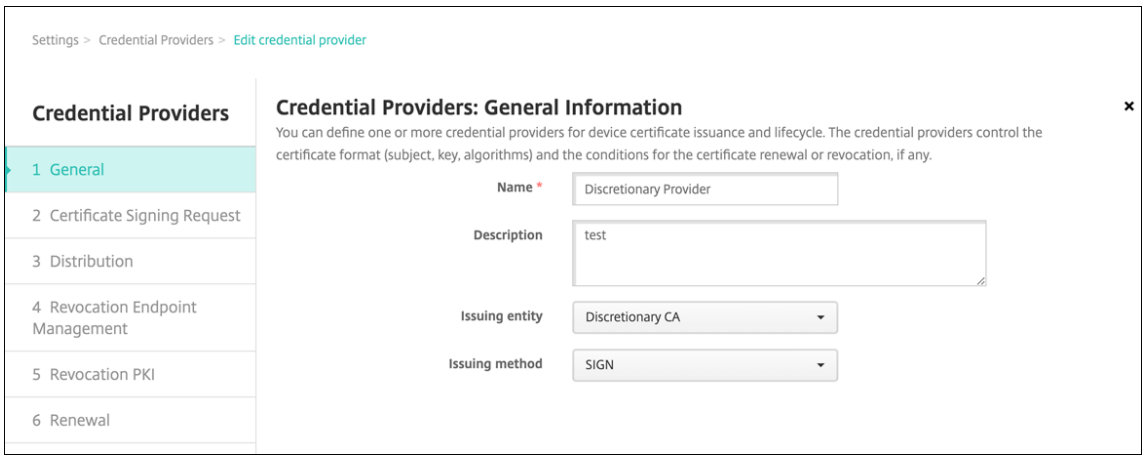
    この機能を有効にすると、証明書のステータスを確認する機会が Citrix ADC に与えられます。この機能を有効にすることをお勧めします。

11. ［保存］をクリックします。

    ［PKI エンティティ］の表に任意 CA が表示されます。

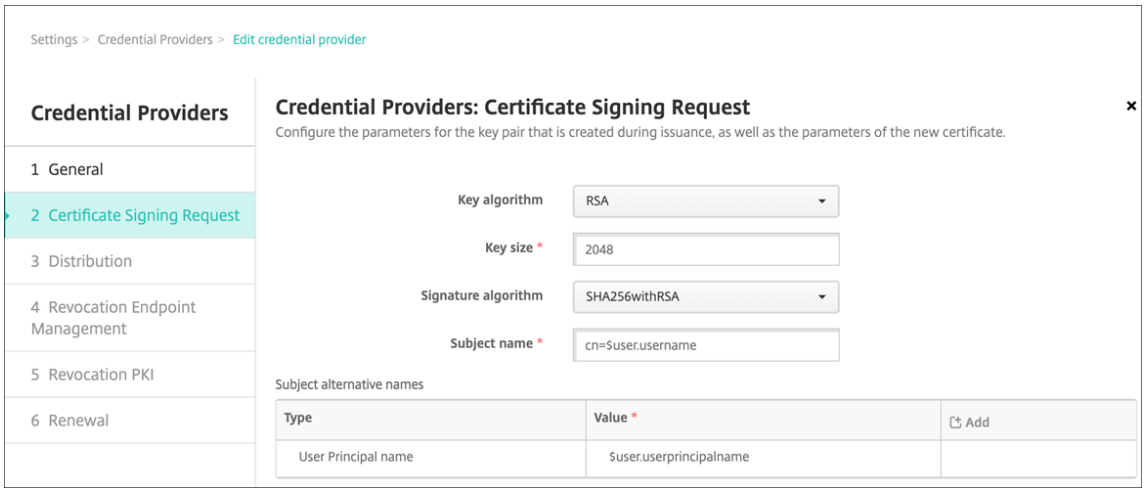
資格情報プロバイダーの構成

1. Citrix Endpoint Management コンソールで、［設定］**>**［資格情報プロバイダー］の順に選択し、［追加］をクリックします。
2. ［資格情報プロバイダー：一般情報］ページで、以下を行います：



- 名前：新しいプロバイダー構成の一意の名前を入力します。この名前は、Citrix Endpoint Management コンソールのほかの部分で構成を特定するために後で使用されます。
- 説明：資格情報プロバイダーの説明です。このフィールドはオプションですが、この資格情報プロバイダーの詳細が必要なときに説明が役立ちます。
- 発行エンティティ：［任意 **CA**］を選択します。
- 発行方式：［署名］または ［取得］をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。クライアント証明書認証の場合は、［署名］を使用します。

3. ［次へ］をクリックします。［資格情報プロバイダー：証明書署名要求］ページで、証明書の構成に応じて以下を構成します：



- キーアルゴリズム：新しいキーペアのキーアルゴリズムを選択します。使用可能な値は ［**RSA**］、［**DSA**］、および ［**ECDSA**］です。
- キーサイズ：キーペアのサイズ（ビット単位）を入力します。このフィールドは必須です。**2048** ビットの使用をお勧めします。
- 署名アルゴリズム：新しい証明書の値を選択します。値はキーアルゴリズムによって異なります。**SHA256withRSA** をお勧めします。

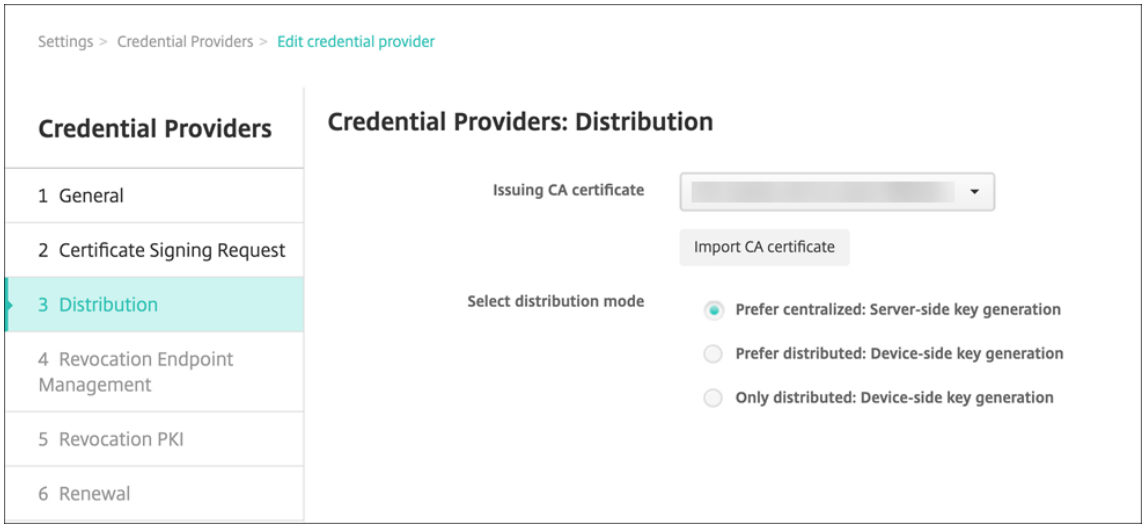
- サブジェクト名：必須です。新しい証明書のサブジェクトの識別名（Distinguished Name：DN）を入力します。ユーザー名に「`CN=${ user.username }`」、または sAMAccountName を使用する「`CN=${ user.samaccountname }`」を使用します。
- ［サブジェクトの別名］の表に新しいエントリを追加するには、［追加］をクリックします。別名の種類を選択して、2 つ目の列に値を入力します。

  以下を追加します：

  - 種類：ユーザープリンシパル名
  - 値：`$user.userprincipalname`

  サブジェクト名と同様に、値フィールドで Citrix Endpoint Management マクロを使用できます。

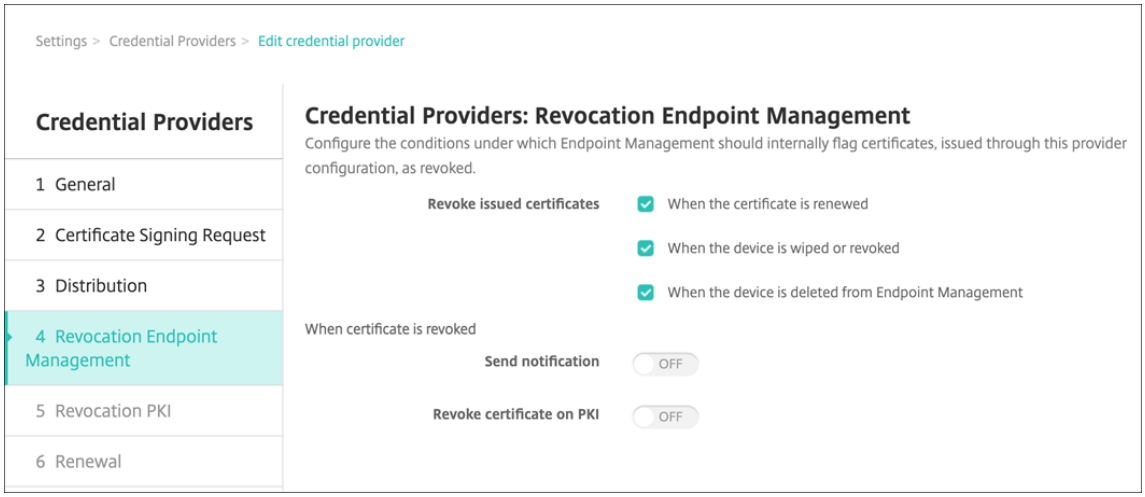
4. ［次へ］をクリックします。［資格情報プロバイダー：ディストリビューション］ページで、以下を行います：



- **CA** 証明書の発行：以前に追加した任意 CA 証明書を選択します。
- ［ディストリビューションモードの選択］：キーを生成し、配布する方法として以下のいずれかの方法を選択します：
  - 集中を優先：サーバー側のキー生成： Citrix ではこの集中オプションを推奨しています。このオプションは Citrix Endpoint Management でサポートされるすべてのプラットフォームをサポートし、Citrix Gateway 認証を使用する場合は必須です。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
  - 分散を優先：デバイス側のキー生成：秘密キーはユーザーデバイス上で生成され、保存されます。この分散モードは SCEP を使用し、keyUsage keyEncryption による RA 暗号化証明書と KeyUsage digitalSignature による RA 署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。
  - 分散のみ：デバイス側のキー生成：このオプションは ［分散を優先**:** デバイス側のキー生成］と同じように動作しますが、デバイス側でのキー生成が失敗した場合、または使用できない場合にはオプションを使用できない点が異なります。

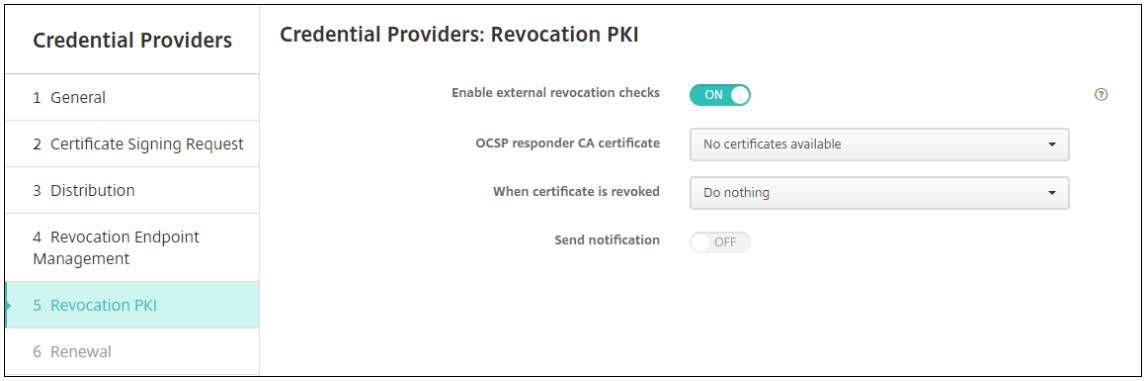
［優先分散**:** デバイス側のキー生成］または ［分散のみ**:** デバイス側のキー生成］を選択した場合は、［RA 署名証明］の一覧から RA 署名証明書を選択し、［RA 暗号化証明書］の一覧から RA 暗号化証明書を選択します。両方に同じ証明書を使用できます。これらの証明書のための新しいフィールドが表示されます。

5. ［次へ］をクリックします。［資格情報プロバイダー：失効 **Citrix Endpoint Management**］ページで、Citrix Endpoint Management がこのプロバイダー構成により発行された証明書に内部で失効のフラグを設定する条件を構成します。次のオプションを構成します:



   - ［発行された証明書の失効］で、証明書がいつ失効するかを示すいずれかのオプションを選択します。
   - 証明書が失効したときに Citrix Endpoint Management から通知を送信する場合は、［通知の送信］の値を ［オン］に設定して、通知テンプレートを選択します。
   - Citrix Endpoint Management を随意 PKI として使用している場合、［**PKI** 上の証明書の失効］は機能しません。

6. ［次へ］をクリックします。［資格情報プロバイダー：失効 **PKI**］ページで、証明書が失効した場合に PKI で行うアクションを特定します。また、通知メッセージを作成するオプションもあります。次のオプションを構成します:



   - 外部失効チェックの有効化：この設定を ［オン］に変更します。失効 PKI に関連する詳細フィールドが表示されます。

- [**OCSP** レスポンダー **CA** 証明書] の一覧から、証明書のサブジェクトの識別名（Distinguished Name: DN）を選択します。

  DN フィールドの値には、Citrix Endpoint Management マクロを使用できます。たとえば、次のようになります: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

- [証明書が失効した場合] の一覧から、証明書が失効したときに PKI エンティティで行う次のいずれかのアクションを選択します。

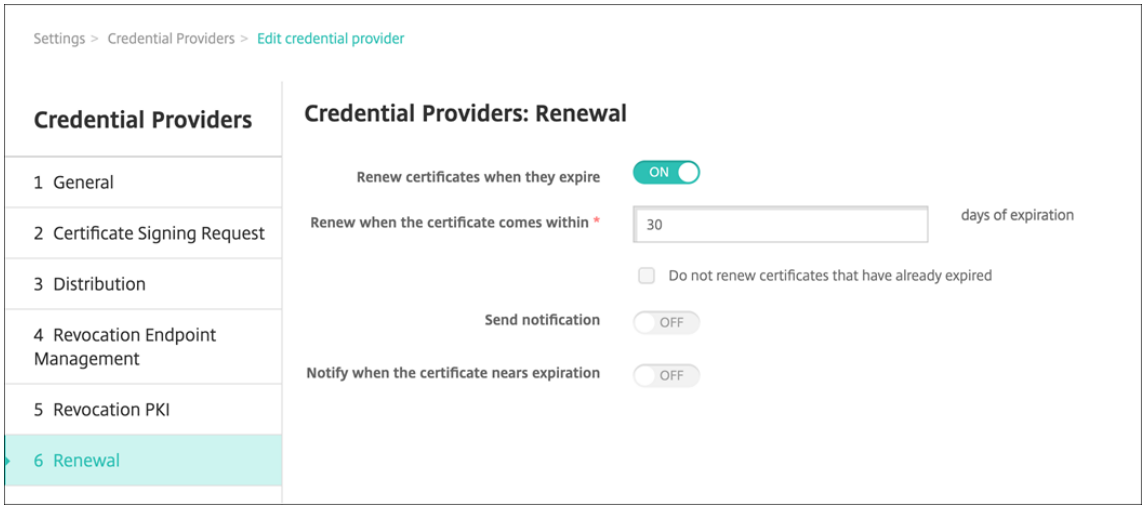
  - 何もしない。
  - 証明書の書き換え。
  - デバイスの失効とワイプ。

- 証明書が失効したときに Citrix Endpoint Management から通知を送信する場合: [通知の送信] の値を [オン] に設定します。

  2 つの通知オプションから選択できます。

  - [通知テンプレートを選択] を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、[通知テンプレート] の一覧にあります。
  - [通知の詳細を入力] を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

7. [次へ] をクリックします。[資格情報プロバイダー: 更新] ページで、以下を行います:



[有効期限が切れたら証明書を更新] を [オン] に設定します。詳細フィールドが表示されます。

- [更新が必要な有効期限までの日数] フィールドに、期限の何日前に証明書を更新するかを入力します。
- 必要に応じて、[既に有効期限が切れている証明書は更新しない] チェックボックスをオンにします。この場合の「既に有効期限が切れている」とは、`NotAfter`が過去の日付であることを意味し、証明書が失効しているという意味ではありません。Citrix Endpoint Management では、内部失効した証明書は更新しません。

証明書が更新されたときに Citrix Endpoint Management から通知を送信する場合：［通知の送信］を ［オン］に設定します。証明書の期限が近いときに Citrix Endpoint Management から通知を送信する場合：［証明書の有効期限が近づいたら通知］を ［オン］に設定します。
どちらの選択肢についても、以下の 2 つの通知オプションからいずれかを選択できます：

- 通知テンプレートを選択：カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［通知テンプレート］の一覧にあります。
- 通知の詳細を入力：独自の通知メッセージを作成できます。受信者の電子メールアドレス、メッセージ、および通知の送信頻度を指定します。

8. ［保存］をクリックします。

資格情報プロバイダー

November 29, 2023

資格情報プロバイダーは、Citrix Endpoint Management システムのさまざまな部分で使用する実際の証明書の構成です。資格情報プロバイダーは、証明書のソース、パラメーター、およびライフサイクルを定義します。これらの操作は、証明書がデバイス構成の一部であるかスタンドアロン（つまり、デバイスにそのままプッシュされる）であるかに関わらず発生します。

デバイス登録によって証明書のライフサイクルは制約されます。つまり、登録前に証明書は発行されませんが、登録の一部として一部の証明書が Citrix Endpoint Management から発行される場合があります。また、1 回の登録のコンテキスト内で内部 PKI から発行された証明書は、登録が失効すると失効します。管理関係が終了すると、証明書の有効性は維持されません。

1 つの資格情報プロバイダーの構成を複数の場所で使用し、1 つの構成によって任意の数の証明書を同時に管理することができます。この場合、この全体は展開リソースおよび展開上にあります。たとえば、資格情報プロバイダー P が構成 C の一部としてデバイス D に展開された場合、D に展開される証明書は P の発行設定によって決まります。同様に、C が更新された場合は D の更新設定が適用されます。また、C が削除された、または D が失効した場合には、D の失効設定も適用されます。

この規則に従って、Citrix Endpoint Management の資格情報プロバイダー構成により以下が決まります：

- 証明書のソース。
- 証明書の取得方法：新しい証明書に署名するか、既存の証明書とキーペアをフェッチ（回復）します。
- 発行または回復のパラメーター。キーサイズ、キーアルゴリズム、証明書拡張などの証明書署名要求（Certificate Signing Request：CSR）パラメーターがあります。
- 証明書をデバイスに配信する方法。
- 失効条件。管理関係が失われると Citrix Endpoint Management のすべての証明書が失効しますが、構成によっては、早期の失効を指定する場合もあります。たとえば、関連するデバイス構成が削除されたときに証明書が失効するように指定できます。また、条件によっては、Citrix Endpoint Management で関連付けられ

た証明書の失効がバックエンドの PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）に送信されることがあります。つまり、Citrix Endpoint Management の証明書失効により、PKI で証明書失効が発生する場合があります。

- リニューアル設定。特定の資格プロバイダーを通して取得された証明書は、有効期限が近づくと自動的に更新されます。または、そのような状況とは別に、有効期限が近づくと通知を出すこともできます。

任意エンティティの発行方法は常に署名です。

証明書の発行方法

任意エンティティの発行方法は常に署名です。

この方法では、新しい秘密キーを作成し、CSR を作成して CA（Certificate Authority：証明機関）に送信し、署名してもらいます。Citrix Endpoint Management では、MS 証明書サービスエンティティおよび任意 CA エンティティの両方の署名方法がサポートされています。

資格情報プロバイダーは署名の発行方法を使用します。

証明書の配信

Citrix Endpoint Management での証明書の配信には、集中と分散の 2 つのモードがあります。分散モードは SCEP（Simple Certificate Enrollment Protocol）を使い、クライアントがこのプロトコルをサポートする状況でのみ使用できます（iOS のみ）。場合によっては分散モードが必須となります。

資格情報プロバイダーで分散（SCEP を使用した）配信をサポートするには、特別な構成手順として、RA（Registration Authority：登録機関）証明書の設定が必要です。RA 証明書が必要なのは、SCEP プロトコルを使用する場合、Citrix Endpoint Management が実際の証明機関に対する代理（登録機関）と同様に機能するためです。Citrix Endpoint Management は、そのように行動する権限を持っていることをクライアントに証明する必要があります。その権限は、Citrix Endpoint Management に前述の証明書をアップロードすることにより確立されます。

RA 署名と RA 暗号化の 2 つの異なる証明書の役割が必要です（1 つの証明書で両方の要件を満たすことができます）。これらの役割には以下の制約があります。

- RA 署名証明書には、X.509 キー使用法デジタル署名が必要です。
- RA 暗号化証明書には、X.509 キー使用法キーの暗号化が必要です。

資格情報プロバイダーの RA 証明書を構成するには、それらの証明書を Citrix Endpoint Management にアップロードし、資格情報プロバイダーでそれらの証明書にリンクします。

資格情報プロバイダーに証明書の役割について構成されている証明書がある場合、分散配信のみをサポートするとみなされます。各資格情報プロバイダーは、集中モードを優先するか、分散モードを優先するか、または分散モードを必須とするように構成できます。実際の結果はコンテキストに応じて異なります。コンテキストが分散モードをサポートしないにもかかわらず、資格情報プロバイダーに分散モードが必要な場合、展開は失敗します。同様に、コンテ

キストに分散モードが必要な場合でも、資格情報プロバイダーが分散モードをサポートしていなければ、展開は失敗します。ほかのすべての場合、優先設定が適用されます。

次の表は、Citrix Endpoint Management 全体における SCEP 分散を示しています:

コンテキスト	SCEP のサポート	SCEP の必要
iOS プロファイルサービス	はい	はい
iOS モバイルデバイス管理登録	はい	番号
iOS 構成プロファイル	はい	番号
SHTP 登録	番号	番号
SHTP の構成	番号	番号
Windows タブレットの登録	番号	番号
Windows タブレットの構成	いいえ。ただし、Windows 10 および Windows 11 リリースでサポートされるネットワークデバイスポリシーを除く。	番号

証明書の失効

失効には以下の 3 つの種類があります。

- 内部失効: Citrix Endpoint Management で維持されている証明書の状態に影響します。Citrix Endpoint Management は、提示された証明書を評価するとき、または証明書の OCSP ステータス情報を提供するときに、このステータスを考慮します。資格情報プロバイダー構成により、さまざまな条件下でこの状態がどのように影響を受けるかが決まります。たとえば、資格情報プロバイダーは、証明書がデバイスから削除されたときに失効済みのフラグを立てるよう指定する場合があります。
- 外部に伝達される失効: 失効 Citrix Endpoint Management とも呼ばれるこの種類の失効は、外部の PKI から取得した証明書に適用されます。資格情報プロバイダー構成で定義された条件下で、Citrix Endpoint Management で証明書が内部失効すると、その証明書は PKI でも失効します。
- 外部で誘導される失効: 失効 PKI とも呼ばれるこの種類の失効も、外部の PKI から取得した証明書のみに適用されます。Citrix Endpoint Management で特定の証明書の状態が評価されるたびに、その状態について PKI に照会されます。PKI で証明書が失効している場合、Citrix Endpoint Management で証明書が内部失効します。このメカニズムでは OCSP プロトコルが使用されます。

これらの 3 つのタイプは排他的ではなく、むしろ同時に適用されます。外部失効または個別の調査により、内部失効が発生する場合もあります。内部失効は、外部失効に影響する可能性があります。

証明書の書き換え

証明書の書き換えとは、既存の証明書の失効と別の証明書の発行を両方行うことです。

Citrix Endpoint Management では、発行が失敗した場合にサービスが中断されないように、以前の証明書が失効する前にまず新しい証明書の取得を試行します。分散型（SCEP 対応）配信の場合、証明書がデバイスに正常にインストールされた後にのみ失効が行われます。それ以外の場合は、新しい証明書がデバイスに送信される前に失効が発生します。そのような失効は、証明書のインストールの成功や失敗とは無関係です。

失効の構成では、特定の期間を日単位で指定する必要があります。デバイスが接続されると、証明書の`NotAfter`の日付からこの指定した期間を引いて、現在の日付より後になっているかどうかがサーバーによって検証されます。証明書がこの条件を満たしている場合、Citrix Endpoint Management は証明書の更新を試行します。

資格情報プロバイダーの作成

資格情報プロバイダーの構成は、主に、資格情報プロバイダーに対して選択した発行エンティティや発行方法により異なります。内部エンティティを使用する資格情報プロバイダーと外部エンティティを使用する資格情報プロバイダーを区別できます。

- Citrix Endpoint Management に対して内部である任意エンティティは、内部エンティティです。任意エンティティの発行方法は常に署名です。署名とは、各発行操作で、Citrix Endpoint Management がエンティティに対して選択された CA 証明書で新しいキーペアに署名する方法です。キーペアがデバイスまたはサーバーのどちらで生成されるかは、選択した分散方法によって異なります。
- 企業インフラストラクチャの一部である外部エンティティには、Microsoft CA が含まれます。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックした後、［設定］の［資格情報プロバイダー］をクリックします。
2. ［資格情報プロバイダー］ページで、［追加］をクリックします。

   ［資格情報プロバイダー：一般情報］ページが開きます。
3. ［資格情報プロバイダー：一般情報］ページで、以下を指定します：

   - 名前：新しいプロバイダー構成の一意の名前を入力します。この名前は、Citrix Endpoint Management コンソールのほかの部分で構成を特定するために後で使用されます。
   - 説明：資格情報プロバイダーの説明です。このフィールドはオプションですが、この資格情報プロバイダーの詳細が必要なときに説明が役立ちます。
   - 発行エンティティ：証明書発行エンティティを選択します。
   - 発行方式：［署名］または ［取得］をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。クライアント証明書認証の場合は、［署名］を使用します。

- テンプレート一覧が使用できる場合は、資格情報プロバイダーの PKI エンティティで追加したテンプレートを選択します。

  これらのテンプレートは、[設定]、[**PKI** エンティティ] の順にクリックすると開くページで、Microsoft 証明書サービスエンティティが追加されている場合に使用可能になります。

4. [次へ] をクリックします。

   [資格情報プロバイダー: 証明書署名要求] ページが表示されます。

5. [資格情報プロバイダー: 証明書署名要求] ページで、証明書の構成に応じて以下を構成します:

   - キーアルゴリズム: 新しいキーペアのキーアルゴリズムを選択します。使用可能な値は [**RSA**]、[**DSA**]、および [**ECDSA**] です。
   - キーサイズ: キーペアのサイズ（ビット単位）を入力します。このフィールドは必須です。

     許容値はキータイプによって異なります。たとえば、DSA キーの最大サイズは 2048 ビットです。基になるハードウェアおよびソフトウェアに依存する偽陰性を回避するため、Citrix Endpoint Management ではキーサイズが強制されません。資格情報プロバイダーの構成を実稼働環境でアクティブにする前に、必ずテスト環境でテストしてください。
   - 署名アルゴリズム: 新しい証明書の値を選択します。値はキーアルゴリズムによって異なります。
   - サブジェクト名: 必須です。新しい証明書のサブジェクトの識別名（Distinguished Name: DN）を入力します。例:
     `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

     For example, for client certificate authentication, use these settings:

     - **Key algorithm:** RSA
     - **Key size:** 2048
     - **Signature algorithm:** SHA256withRSA
     - **Subject name:** `cn=$user.username`
   - [サブジェクトの別名] の表に新しいエントリを追加するには、[追加] をクリックします。別名の種類を選択して、2 つ目の列に値を入力します。

     クライアント証明書認証では、次のように指定します:

     - 種類: ユーザープリンシパル名
     - 値: `$user.userprincipalname`

       サブジェクト名と同様に、値フィールドで Citrix Endpoint Management マクロを使用できます。

6. [次へ] をクリックします。

   [資格情報プロバイダー: ディストリビューション] ページが開きます。

7. ［資格情報プロバイダー：ディストリビューション］ページで、以下を行います：

    - ［発行 **CA** 証明書］の一覧から、提供された CA 証明書を選択します。資格情報プロバイダーは任意 CA エンティティを使用するため、資格情報プロバイダーの CA 証明書は常にエンティティそのものに構成されている CA 証明書になります。ここでは、外部エンティティを使用する構成との整合性のために CA 証明書を示します。
    - ［ディストリビューションモードの選択］で、キーを生成し、配布する方法として以下のいずれかの方法をクリックします：
        - 集中を優先：サーバー側のキー生成： Citrix ではこの集中オプションを推奨しています。このオプションは Citrix Endpoint Management でサポートされるすべてのプラットフォームをサポートし、Citrix Gateway 認証を使用する場合は必須です。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
        - 分散を優先：デバイス側のキー生成：秘密キーはユーザーデバイス上で生成され、保存されます。この分散モードは SCEP を使用し、keyUsage keyEncryption による RA 暗号化証明書と KeyUsage digitalSignature による RA 署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。
        - 分散のみ：デバイス側のキー生成：このオプションは［分散を優先: デバイス側のキー生成］と同じように動作しますが、「優先」ではなく「のみ」であるため、デバイス側でのキー生成が失敗した場合、または使用できない場合にはオプションを使用できない点が異なります。

    ［優先分散**:** デバイス側のキー生成］または ［分散のみ**:** デバイス側のキー生成］を選択した場合は、［RA 署名証明］の一覧から RA 署名証明書を選択し、［RA 暗号化証明書］の一覧から RA 暗号化証明書を選択します。両方に同じ証明書を使用できます。これらの証明書のための新しいフィールドが表示されます。

8. ［次へ］をクリックします。

    ［資格情報プロバイダー：失効 **Citrix Endpoint Management**］ページが開きます。このページで、Citrix Endpoint Management がこのプロバイダー構成により発行された証明書に内部で失効のフラグを設定する条件を構成します。

9. ［資格情報プロバイダー：失効 **Citrix Endpoint Management**］ページで、以下を行います：

    - ［発行された証明書の失効］で、証明書がいつ失効するかを示すいずれかのオプションを選択します。
    - 証明書が失効したときに Citrix Endpoint Management から通知を送信する場合は、［通知の送信］の値を ［オン］に設定して、通知テンプレートを選択します。
    - Citrix Endpoint Management で証明書が失効したときに、PKI でも証明書を失効させる場合：［**PKI** 上の証明書の失効］を ［オン］に設定し、［エンティティー覧］からテンプレートを選択します。エンティティー覧には、失効機能で使用できるすべてのエンティティが表示されます。Citrix Endpoint Management で証明書が失効すると、［エンティティー覧］から選択した PKI に、失効呼び出しが送信されます。

10. ［次へ］をクリックします。

［資格情報プロバイダー：失効 **PKI**］ページが開きます。このページで、証明書が失効したときに PKI で行うアクションを特定します。また、通知メッセージを作成するオプションもあります。

11. PKI で証明書を失効させる場合、［資格情報プロバイダー：失効 **PKI**］ページで以下を行います。

    - ［外部失効チェックの有効化］の設定を ［オン］に変更します。失効 PKI に関連する詳細フィールドが表示されます。
    - ［**OCSP** レスポンダー **CA** 証明書］の一覧から、証明書のサブジェクトの識別名（Distinguished Name: DN）を選択します。

      DN フィールドの値には、Citrix Endpoint Management マクロを使用できます。例: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`
    - ［証明書が失効した場合］の一覧から、証明書が失効したときに PKI エンティティで行う次のいずれかのアクションを選択します。

      - 何もしない。
      - 証明書の書き換え。
      - デバイスの失効とワイプ。
    - 証明書が失効したときに Citrix Endpoint Management から通知を送信する場合：［通知の送信］の値を ［オン］に設定します。

      2 つの通知オプションから選択できます。
    - ［通知テンプレートを選択］を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［通知テンプレート］の一覧にあります。
    - ［通知の詳細を入力］を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

12. ［次へ］をクリックします。

    ［資格情報プロバイダー：更新］ページが開きます。このページで、Citrix Endpoint Management を構成して次のことを実行できます：

    - 証明書の書き換え。必要に応じて、更新時に通知を送信したり、期限切れの証明書を操作から除外したりすることもできます。
    - 期限が近い証明書に関する通知の発行（更新前の通知）。

13. 証明書が失効したら更新する場合は、［資格情報プロバイダー：更新］ページで以下を行います：

    ［有効期限が切れたら証明書を更新］を ［オン］に設定します。詳細フィールドが表示されます。

    - ［更新が必要な有効期限までの日数］フィールドに、期限の何日前に証明書を更新するかを入力します。
    - 必要に応じて、［既に有効期限が切れている証明書は更新しない］チェックボックスをオンにします。この場合の「既に有効期限が切れている」とは、`NotAfter`が過去の日付であることを意味し、証明書

が失効しているという意味ではありません。Citrix Endpoint Management では、内部失効した証明書は更新しません。

証明書が更新されたときに Citrix Endpoint Management から通知を送信する場合：［通知の送信］を ［オン］に設定します。証明書の期限が近いときに Citrix Endpoint Management から通知を送信する場合：［証明書の有効期限が近づいたら通知］を ［オン］に設定します。
どちらの選択肢についても、以下の 2 つの通知オプションからいずれかを選択できます：

- 通知テンプレートを選択：カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［通知テンプレート］の一覧にあります。
- 通知の詳細を入力：独自の通知メッセージを作成できます。受信者の電子メールアドレス、メッセージ、および通知の送信頻度を指定します。

［通知が必要な証明書の有効期限までの日数］フィールドで、証明書の期限の何日前に通知を送信するかを入力します。

14. ［保存］をクリックします。

［資格情報プロバイダー］の表に資格情報プロバイダーが追加されます。

APNs 証明書

December 8, 2023

Citrix Endpoint Management で Apple デバイスを登録して管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書を設定します。証明書を使用すると、Apple Push Network を使用してモバイルデバイスを管理できます。

ワークフローの概要：

手順 **1**：次のいずれかの方法で証明書署名要求（CSR）を作成：

- macOS でキーチェーンアクセスを使用する CSR の作成（Citrix 推奨）
- Microsoft IIS を使用する CSR の作成
- OpenSSL を使用する CSR の作成

手順 **2**： Citrix Endpoint Management ツールで CSR に署名

手順 **3**：署名済み CSR を Apple に送信し APNs 証明書を取得

手順 **4**：手順 1 で使用したのと同じコンピューターを使用して、CSR を完了し、PKCS #12 ファイルをエクスポート：

- macOS でキーチェーンアクセスを使用する PKCS #12 ファイルの作成
- Microsoft IIS を使用する PKCS #12 ファイルの作成

- OpenSSL を使用する PKCS #12 ファイルの作成

手順 **5**: APNs 証明書の Citrix Endpoint Management へのインポート

手順 **6**: APNs 証明書の更新

証明書署名要求の作成

macOS でキーチェーンアクセスを使用して CSR を作成することをお勧めします。Microsoft IIS または OpenSSL を使用して CSR を作成することもできます。

> 重要:
>
> - 証明書の作成に使用された Apple ID について:
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.
> - 証明書を失効させると、過失であっても故意であっても、デバイスを管理できなくなります。
> - iOS Developer Enterprise Program を使用して Mobile Device Manager プッシュ証明書を作成した場合: Apple Push Certificates Portal に移行した証明書に必要なアクションを実行してください。

macOS でキーチェーンアクセスを使用する **CSR** の作成

1. macOS を実行するコンピューターの ［アプリケーション］**>**［ユーティリティ］で、キーチェーンアクセスアプリを起動します。
2. ［キーチェーンアクセス］メニューで、［証明書アシスタント］**>**［認証局に証明書を要求］の順に選択します。
3. 証明書アシスタントにより、次の情報の入力を求められます:
   - メールアドレス: 証明書を管理する個人または役割アカウントのメールアドレス。
   - 共通名: 証明書を管理する個人または役割アカウントの通称。
   - **CA** のメールアドレス: 認証局のメールアドレス。
4. ［ディスクに保存］をクリックし、［鍵ペア情報を指定］チェックボックスをオンにして、［続ける］をクリックします。
5. CSR ファイルの名前を入力してコンピューターにファイルを保存し、［保存］を選択します。
6. 鍵ペア情報を指定:［鍵のサイズ］で［2048 ビット］を選択し、アルゴリズムに ［**RSA**］を選択してから ［続ける］をクリックします。APNs 証明書プロセスの一環として CSR ファイルをアップロードする準備ができました。
7. 証明書アシスタンスによる CSR プロセスが完了してから ［完了］をクリックします。
8. 続行するには、CSR に署名します。

Microsoft IIS を使用する **CSR** の作成

APNs 証明書要求を生成するには、まず CSR（証明書署名要求）を作成します。Windows の場合は、Microsoft IIS を使用して CSR を生成します。

1. Microsoft IIS を開きます。
2. IIS のサーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ウィンドウで、［証明書の要求の作成］をクリックします。
4. 適切な識別名（DN）情報を入力します。たとえば、www.domain.comなどの Citrix Endpoint Management サーバーの完全修飾ドメイン名（FQDN）を入力できます。［次へ］をクリックします。
5. ［暗号化サービスプロバイダー］で ［**Microsoft RSA SChannel Cryptographic Provider**］を選択して、ビット長として ［**2048**］を選択し、［次へ］をクリックします。
6. ファイル名を入力して CSR を保存する場所を指定し、［完了］をクリックします。
7. 続行するには、CSR に署名します。

OpenSSL を使用する **CSR** の作成

macOS デバイスまたは Microsoft IIS を使用して CSR を生成できない場合は、OpenSSL を使用します。OpenSSL は、OpenSSL の Web サイトからダウンロードしてインストールできます。

1. OpenSSL をインストールしたコンピューターで、コマンドプロンプトまたはシェルから次のコマンドを実行します。

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate
   .csr -newkey rsa:2048
   ```

2. 証明書の名前に関する次のメッセージが表示されます。要求された情報を入力します。

   ```
   1  You are about to be asked to enter information that will be
         incorporated into your certificate request.
   2  What you are about to enter is what is called a Distinguished Name
       or a DN.
   3  There are quite a few fields but you can leave some blank
   4  For some fields there will be a default value,
   5  If you enter '.', the field will be left blank.
   6  -----
   7  Country Name (2 letter code) [AU]:US
   8  State or Province Name (full name) [Some-State]:CA
   9  Locality Name (eg, city) []:RWC
   10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
         Customer
   11 Organizational Unit Name (eg, section) [:Marketing
   12 Common Name (eg, YOUR name) []:John Doe
   13 Email Address []:john.doe@customer.com
   14 <!--NeedCopy-->
   ```

3. 次のメッセージが表示されたら、CSR の秘密キーのパスワードを入力します。

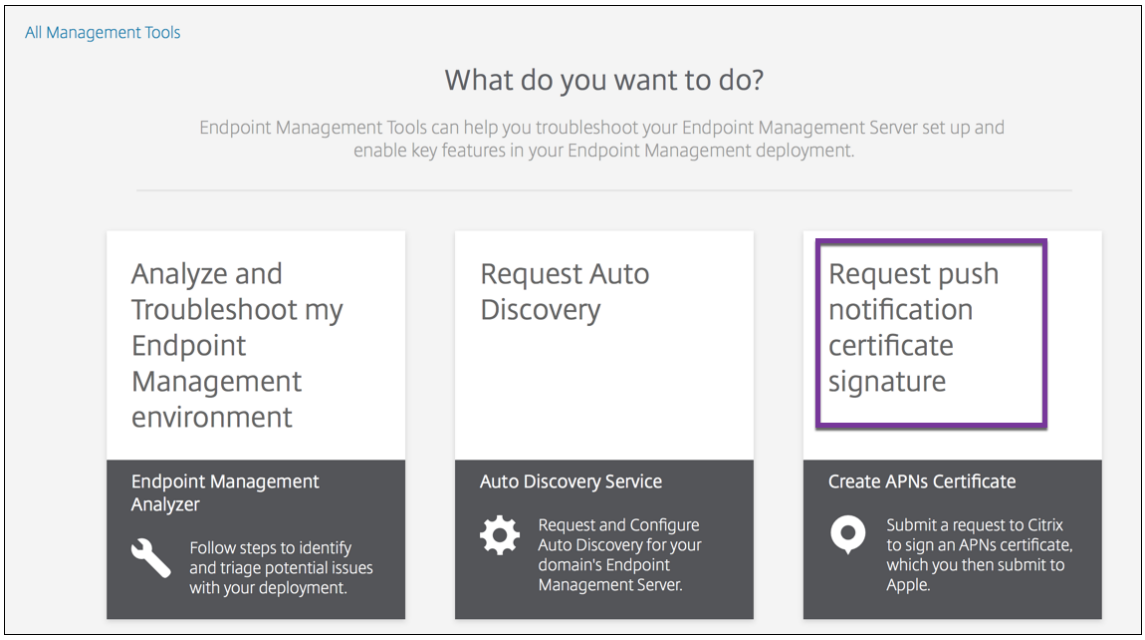

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
<!--NeedCopy-->
```

4. 続行するには、次のセクションの説明に従って、CSR に署名します。

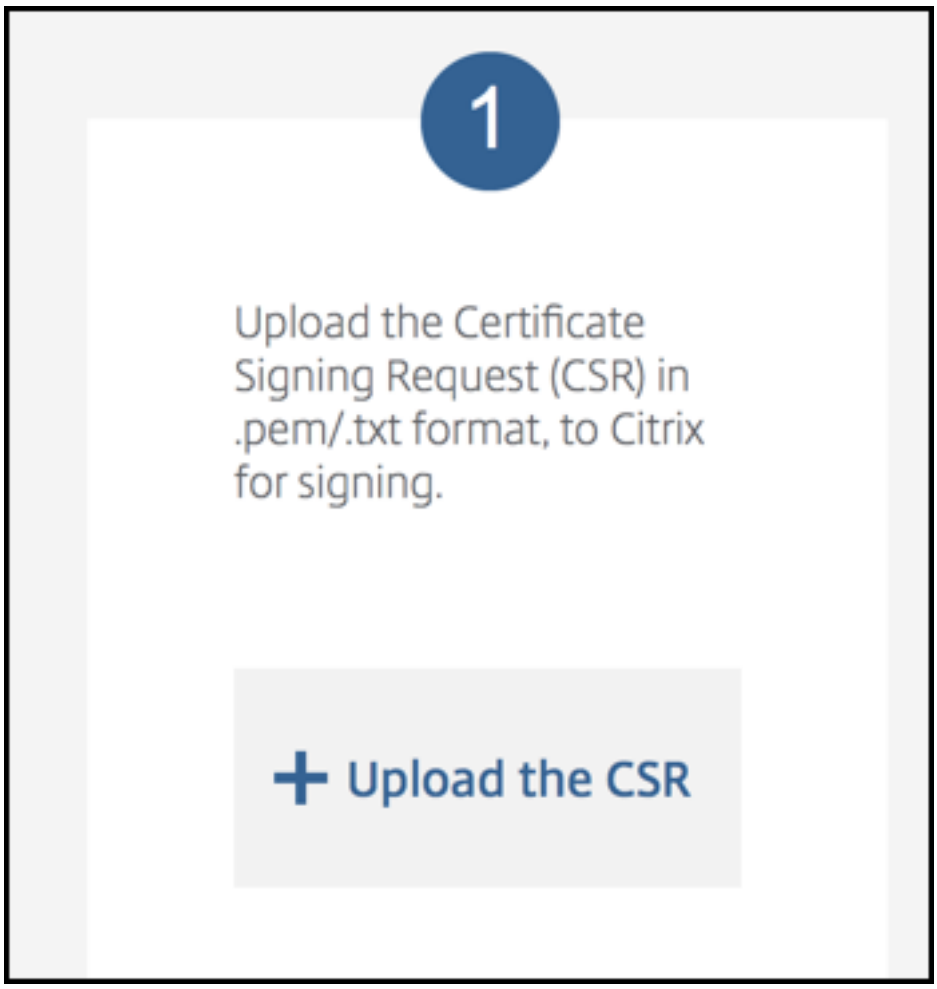
CSR への署名

Citrix Endpoint Management で証明書を使用するには、証明書を Citrix に送信して署名を求める必要があります。Citrix はモバイルデバイス管理の署名証明書を使用して CSR に署名し、`.plist`形式の署名ファイルを返送します。

1. 使用しているブラウザーでCitrix Endpoint Management ツールWeb サイトに移動し、[**Request push notificationcertificate signature**] を選択します。



2. 新しい証明書の作成ページで、[**Upload the CSR**] を選択します。



3. 証明書に移動して選択します。

> 重要:
>
> 証明書は.pem または.txt 形式である必要があります。必要に応じて、ファイル名を右クリックして名前を変更し、証明書のファイル拡張子を.pem または.txt に変更します。

4. **Citrix Endpoint Management APNs CSR** 署名ページで、［署名］をクリックします。CSR が署名されて、構成されているダウンロードフォルダーに自動的に保存されます。
5. 続行するには、次のセクションの説明に従って、署名入り CSR を送信します。

署名入り **CSR** の **Apple** への送信と **APNs** 証明書の取得

署名入り CSR（Certificate Signing Request：証明書署名要求）を Citrix から受け取ったら、その CSR を Apple に送信して、Citrix Endpoint Management へのインポートに必要な APNs 証明書を取得します。

> 注:
>
> 一部のユーザーから、Apple Push Portal へのログイン時の問題が報告されています。代わりに、Apple Developer Portalにログオンすることもできます。その後、次の手順を実行できます。

1. ブラウザーでApple Push Certificates Portalに移動します。
2. ［証明書識別情報を作成］をクリックします。
3. Apple で初めて証明書を作成する場合：［利用規約を読みました。内容に同意します。］チェックボックスをオンにして、［同意します］をクリックします。
4. ［ファイルの選択］をクリックし、コンピューター上の署名入り CSR を指定して ［アップロード］をクリックします。アップロードが成功したことを示す確認メッセージが表示されます。
5. ［ダウンロード］をクリックして、.pem 証明書を取得します。
6. 続行するには、CSR を完了し、次のセクションの説明に従って、PKCS #12 ファイルをエクスポートします。

CSR の完了と **PKCS #12** ファイルのエクスポート

Apple から APNs 証明書を受け取ったら、キーチェーンアクセス、Microsoft IIS、または OpenSSL に戻り、証明書を PCKS #12 ファイルにエクスポートします。

PKCS #12 ファイルには、APNs 証明書ファイルと秘密キーが含まれています。通常、PFX ファイルの拡張子は.pfx または.p12 です。.pfx ファイルと.p12 ファイルは、交換して使用できます。

> 重要:
>
> Citrix は、個人キーと公開キーを保存するか、ローカルシステムからエクスポートすることをお勧めします。これらのキーは、再利用するために APNs 証明書にアクセスするときに必要です。同じキーがないと、証明書は無効になり、CSR と APNs のプロセス全体を繰り返す必要があります。

macOS でキーチェーンアクセスを使用する **PKCS #12** ファイルの作成

> 重要:
>
> このタスクには、CSR を生成するために使用したのと同じ macOS デバイスを使用します。

1. このデバイスで、Apple から受け取った Production identity（.pem）証明書を検索します。
2. キーチェーンアクセスアプリケーションを起動し、［ログイン］**>** ［自分の証明書］タブに移動します。Product identity 証明書をドラッグして、開いているウィンドウにドロップします。
3. 証明書をクリックし、左矢印を展開して、証明書に関連する秘密キーが含まれていることを確認します。
4. PCKS #12（.pfx）証明書への証明書のエクスポートを開始するには、証明書と秘密キーを選択して右クリックし、［**2** 項目を書き出す］を選択します。

5. Citrix Endpoint Management で使用するには、証明書ファイルに一意の名前を付けるようにします。名前に空白や特殊文字は含めないでください。次に、保存する証明書のフォルダーの場所を選び、.pfx ファイル形式を選択して ［保存］をクリックします。
6. パスワードを入力して証明書をエクスポートします。Citrix では一意で強力なパスワードを使用することをお勧めします。また、後で使用および参照するために証明書とパスワードを安全に保管するようにします。
7. キーチェーンアクセスアプリによって、ログインパスワードまたは選択したキーチェーンを確認するメッセージが表示されます。パスワードを入力し、［**OK**］をクリックします。Citrix Endpoint Management サーバーで保存された証明書を使用する準備ができました。
8. 続行するには、「APNs 証明書の Citrix Endpoint Management へのインポート」を参照してください。

Microsoft IIS を使用する **PKCS #12** ファイルの作成

> 重要:
>
> このタスクには、CSR を生成するために使用したのと同じ IIS サーバーを使用します。

1. Microsoft IIS を開きます。
2. サーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ウィンドウで、［証明書の要求の完了］をクリックします。
4. Apple の Certificate.pem ファイルを指定します。フレンドリ名または証明書名を入力して ［**OK**］をクリックします。名前に空白や特殊文字は含めないでください。
5. 手順 4 で指定した証明書を選択して ［エクスポート］をクリックします。
6. .pfx 証明書の場所とファイル名およびパスワードを指定して ［**OK**］をクリックします。

   Citrix Endpoint Management にインポートするには、証明書のパスワードが必要です。
7. .pfx 証明書を Citrix Endpoint Management をインストールするサーバーにコピーします。
8. 続行するには、「APNs 証明書の Citrix Endpoint Management へのインポート」を参照してください。

OpenSSL を使用する **PKCS #12** ファイルの作成

OpenSSL を使用して CSR を作成する場合、OpenSSL を使用して.pfx APNs 証明書を作成することもできます。

1. コマンドプロンプトまたはシェルで、次のコマンドを実行します。`Customer.privatekey.pem`は CSR からの秘密キー、`APNs_Certificate.pem`は Apple から受け取った証明書です。

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.
   privatekey.pem -out apns_identity.pfx
   ```
2. .pfx 証明書ファイルのパスワードを入力します。このパスワードは、証明書を Citrix Endpoint Management にアップロードするときに再び使用するので覚えておいてください。

3. .pfx 証明書ファイルの場所を確認します。次に、Citrix Endpoint Management コンソールからアップロードできるように、このファイルを Citrix Endpoint Management サーバーにコピーします。
4. 続行するには、次のセクションの説明に従って、APNs 証明書を Citrix Endpoint Management にインポートします。

APNs 証明書の Citrix Endpoint Management へのインポート

新しい APNs 証明書を受け取ったら：その APNs 証明書を Citrix Endpoint Management にインポートして、最初の証明書として追加するか、既存の証明書を置き換えます。

1. Citrix Endpoint Management コンソールで、［設定］**>**［証明書］の順に選択します。
2. ［インポート］**>**［キーストア］の順にクリックします。
3. ［使用目的］から、［**APNs**］を選択します。
4. コンピューターの.pfx ファイルまたは.p12 ファイルを指定します。
5. パスワードを入力して、［インポート］をクリックします。

Citrix Endpoint Management の証明書について詳しくは、「証明書と認証」を参照してください。

APNs 証明書の更新

> 重要：
>
> 更新処理に別の Apple ID を使用する場合、ユーザーのデバイスを再登録する必要があります。

APNs 証明書を更新するには、証明書を作成する手順を実行してから、Apple Push Certificates Portalにアクセスします。このポータルを使用して、新しい証明書をアップロードします。ログオンすると、既存の証明書（または、前の Apple Developers アカウントからインポートされた証明書）が表示されます。

証明書を更新する場合は、証明書を作成する場合との唯一の違いとして、Certificates Portal で ［更新］をクリックします。Certificates Portal にアクセスするには、このサイトの開発者アカウントが必要です。証明書を更新するには、同じ組織名と Apple ID を使用します。

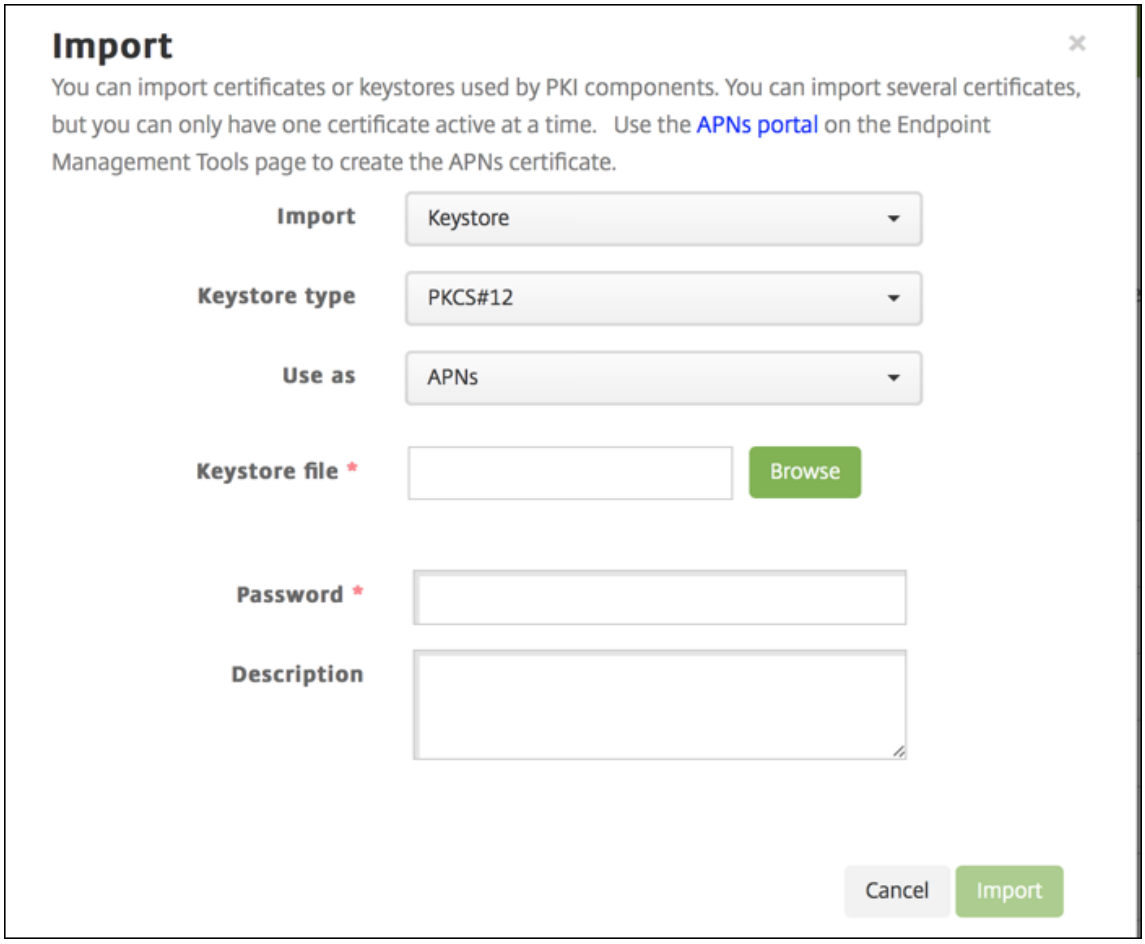
APNs 証明書の有効期限を調べるには、Citrix Endpoint Management コンソールで ［設定］**>**［証明書］の順に選択します。証明書の有効期限が切れた場合、その証明書を取り消さないでください。

1. Microsoft IIS、キーチェーンアクセス（macOS）、または OpenSSL を使用して CSR を生成します。CSR の生成について詳しくは、「証明書署名要求の作成」を参照してください。
2. ブラウザーで、Citrix Endpoint Management ツールに移動します。次に、［プッシュ通知証明書の署名要求］を選択します。
3. ［**+ Upload the CSR**］をクリックします。

4. ダイアログボックスで CSR に移動し、［開く］、［署名］の順にクリックします。
5. `.plist`ファイルを受信したら保存します。
6. 手順 3 のページで、**Apple Push Certificates Portal** をクリックしてサインオンします。
7. 更新する証明書を選択して ［更新］をクリックします。
8. `.plist`ファイルをアップロードします。出力として.pem ファイルを受信します。.pem ファイルを保存します。
9. この.pem ファイルを使用し、（手順 1 で CSR を作成するために使用した方法に従って）CSR を完了します。
10. 証明書を.pfx ファイルとしてエクスポートします。

Citrix Endpoint Management コンソールで.pfx ファイルをインポートし、以下の手順を実行して構成を完了します:

1. ［設定］**>**［証明書］**>**［インポート］の順に選択します。
2. ［インポート］メニューから、［キーストア］を選択します。
3. ［キーストアの種類］メニューから、［**PKCS** # **12**］を選択します。
4. ［使用目的］から、［**APNs**］を選択します。



5. ［キーストアファイル］では、［ブラウザー］をクリックしてファイルに移動します。
6. ［パスワード］ボックスに、証明書のパスワードを入力します。
7. 必要に応じて ［説明］に入力します。
8. ［インポート］をクリックします。

Citrix Endpoint Management で ［証明書］ページにリダイレクトされます。［名前］、［状態］、［有効期限開始］、および ［有効期限終了］フィールドが更新されます。

Citrix Files での SAML によるシングルサインオン

March 15, 2024

Citrix Endpoint Management と ShareFile を構成して、SAML（Security Assertion Markup Language：セキュリティアサーションマークアップランゲージ）を使用した Citrix Files モバイルアプリへのシングルサインオン（SSO：Single Sign-On）アクセスを提供することができます。この機能には次のものが含まれます：

- MAM SDK 対応か、MDX Toolkit を使用してラップされた Citrix Files アプリ
- ラップされていない Citrix Files クライアント（Web サイト、Outlook Plug-in、同期クライアントなど）
- ラップされた **Citrix Files** アプリの場合： Citrix Files にログオンするユーザーは、ユーザー認証および SAML トークンを取得するために Citrix Secure Hub にリダイレクトされます。認証が成功した後で、Citrix Files Mobile アプリから ShareFile に SAML トークンが送信されます。最初のログオンの後、ユーザーは SSO を介して Citrix Files モバイルアプリにアクセスできます。また、毎回ログオンしなくても、Citrix Secure Mail のメールに ShareFile からドキュメントを添付できます。
- ラップされていない **Citrix Files** クライアントの場合： Web ブラウザーまたはほかの Citrix Files クライアントを介して Citrix Files にログオンするユーザーは、Citrix Endpoint Management にリダイレクトされます。Citrix Endpoint Management で認証されると、ユーザーは ShareFile に送信された SAML トークンを取得します。最初のログオンの後は、毎回ログオンしなくてもユーザーは SSO を介して Citrix Files クライアントにアクセスできます。

Citrix Endpoint Management を ShareFile の SAML ID プロバイダー（IdP）として使用するには、この記事で説明するように、Enterprise アカウントを使用するように Citrix Endpoint Management を構成する必要があります。または、ストレージゾーンコネクタでのみ動作するように Citrix Endpoint Management を構成することもできます。詳しくは、「ShareFile を Citrix Endpoint Management と使用する」を参照してください。

詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。

前提条件

Citrix Endpoint Management および Citrix Files アプリに SSO を構成する前に、以下の前提条件を満たしている必要があります:

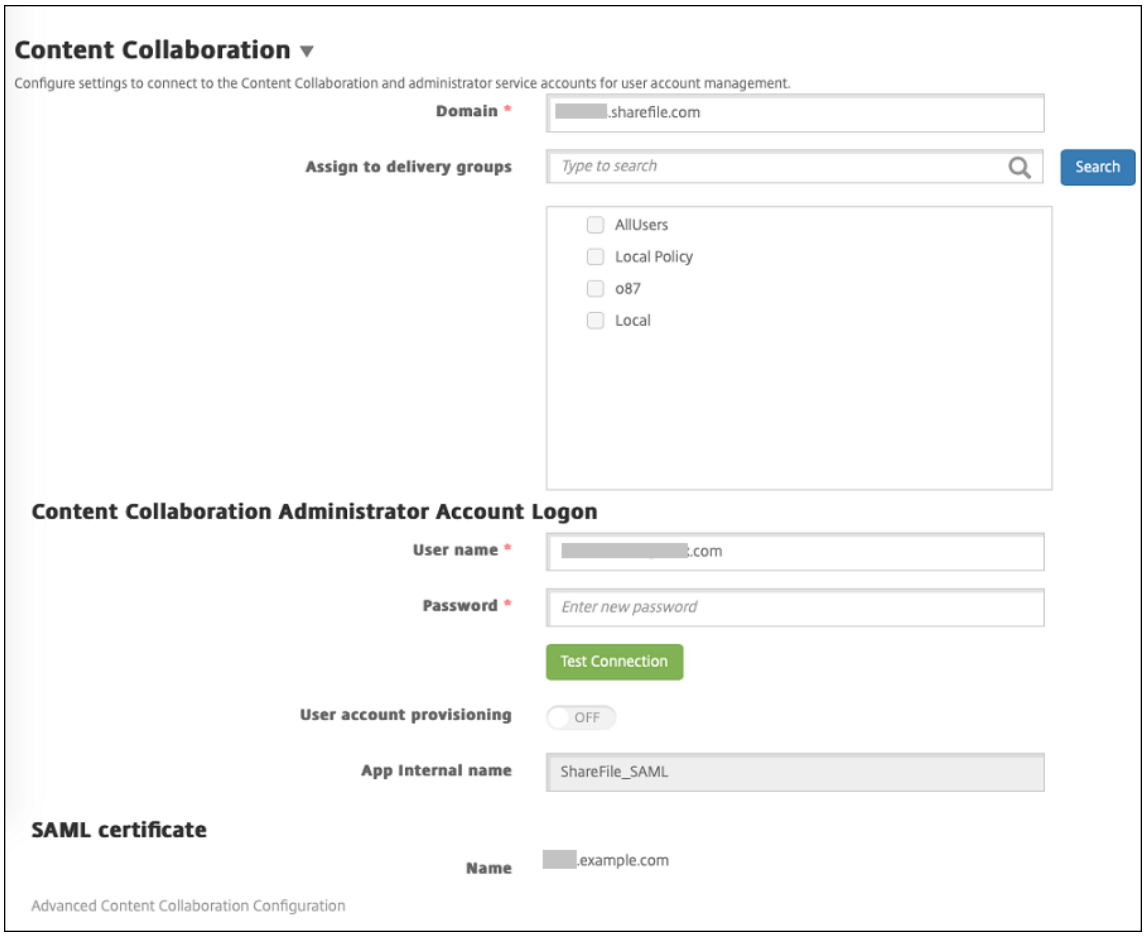
- MAM SDK または互換性があるバージョンの MDX Toolkit（Citrix Files モバイルアプリ用）。

  詳しくは、「Citrix Endpoint Management の互換性」を参照してください。
- 互換性があるバージョンの Citrix Files モバイルアプリと Citrix Secure Hub。
- ShareFile 管理者アカウント
- Citrix Endpoint Management と ShareFile 間の確認された接続。

ShareFile アクセスを構成する

ShareFile のために SAML を設定する前に、以下のように ShareFile アクセス情報を入力します。

1. Citrix Endpoint Management Web コンソールで、［**Configure**］の［**ShareFile**］をクリックします。［**ShareFile**］構成ページが開きます。



2. 次の設定を構成します:

    - ドメイン: ShareFile サブドメイン名を入力します。例: `example.sharefile.com`。
    - デリバリーグループに割り当て: ShareFile と共に SSO を使用するデリバリーグループを選択または検索します。
    - **ShareFile** 管理者アカウントログオン
    - ユーザー名: ShareFile 管理者のユーザー名を入力します。このユーザーには管理特権が必要です。
    - パスワード: ShareFile 管理者のパスワードを入力します。
    - ユーザーアカウントのプロビジョニング: この設定は無効のままにします。ユーザープロビジョニングに ShareFile User Management Tool を使用します。「ユーザーアカウントと配布グループのプロビジョニング」を参照してください。

3. [接続のテスト] をクリックして、ShareFile 管理者アカウントのユーザー名とパスワードが特定の ShareFile アカウントに対して認証されることを検証します。

4. [保存] をクリックします。

    - Citrix Endpoint Management が ShareFile と同期して、ShareFile の [**ShareFile** 発行者/エンティティ **ID**] と [ログイン **URL**] の設定が更新されます。
    - [構成] **>** [**ShareFile**] ページにアプリの内部名が表示されます。アプリの内部名は、後述の「Citrix Files.com の SSO 設定を変更する」で説明する手順を完了するために必要になります。

ラップされた **Citrix Files MDX** アプリ用の **SAML** の設定

MAM SDK で準備された Citrix Files アプリを使用したシングルサインオン構成に NetScaler Gateway を使用する必要はありません。Web サイト、Outlook Plug-in、同期クライアントなど、ラップされていない Citrix Files クライアントのアクセスを構成するには、「ほかの Citrix Files クライアントのために NetScaler Gateway を構成する」を参照してください。

ラップされた Citrix Files MDX アプリ用に SAML を構成するには:

1. Citrix Endpoint Management クライアントの ShareFile をダウンロードします。Citrix.com のダウンロードページを参照してください。
2. MAM SDK を使用して Citrix Files モバイルアプリを準備します。詳しくは、「MAM SDK の概要」を参照してください。
3. Citrix Endpoint Management コンソールで、準備された Citrix Files モバイルアプリをアップロードします。MDX アプリをアップロードする方法について詳しくは、「MDX アプリを Citrix Endpoint Management に追加するには」を参照してください。
4. SAML 設定の検証: 上記の手順で構成した管理者のユーザー名とパスワードで ShareFile にログオンします。

5. ShareFile および Citrix Endpoint Management が同じタイムゾーンで構成されていることを確認します。構成したタイムゾーンに関して、Citrix Endpoint Management に正しい時刻が表示されていることを確認します。そうでない場合、SSO が失敗する可能性があります。

Citrix Files モバイルアプリの検証

1. ユーザーデバイスに Citrix Secure Hub をインストールして構成します。
2. アプリストアから Citrix Files モバイルアプリをダウンロードしてインストールします。
3. ユーザー名やパスワードの入力を求められずに Citrix Files が開始されます。

Citrix Secure Mail による検証

1. まだ行っていない場合は、ユーザーデバイスに Citrix Secure Hub をインストールして構成します。
2. アプリストアから Citrix Secure Mail をダウンロード、インストール、および設定します。
3. 新規メールを開いて［**ShareFile** から添付］をタップします。メールに添付できるファイルがユーザー名とパスワードを入力しなくても表示されます。

ほかの **Citrix Files** クライアントのために **NetScaler Gateway** を構成する

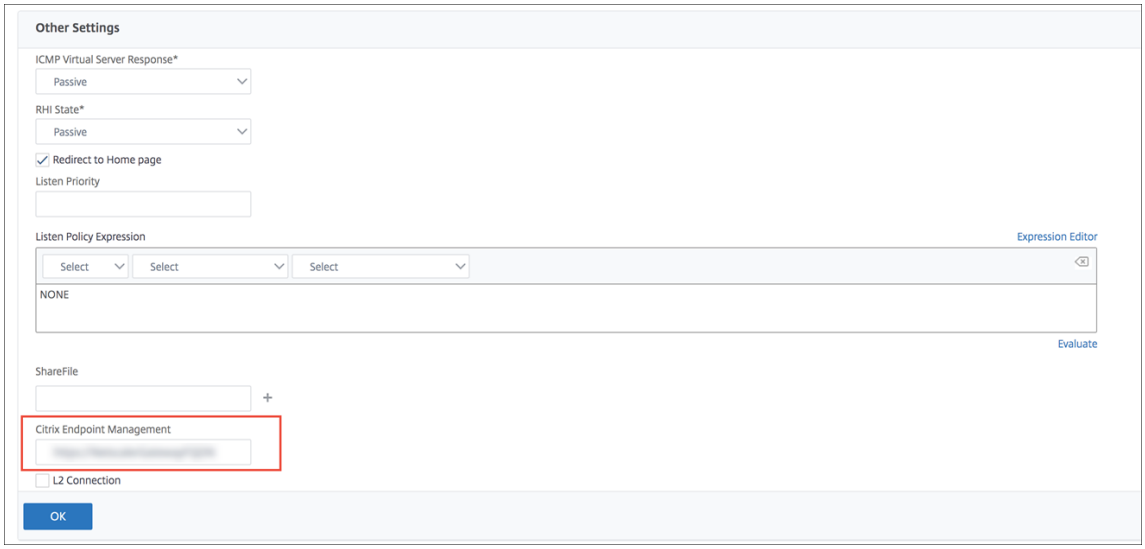
Web サイト、Outlook Plug-in、Sync クライアントなどのラップされていない Citrix Files クライアントへのアクセスを構成するには、以下のように NetScaler Gateway を構成して、SAML ID プロバイダーとしての Citrix Endpoint Management の使用をサポートする必要があります。

- ホームページのリダイレクトを無効にする。
- Citrix Files のセッションポリシーとプロファイルを作成する。
- NetScaler Gateway Gateway 仮想サーバーにポリシーを構成する。

ホームページのリダイレクトを無効にする

/cginfra パスから送られる要求に対するデフォルトの動作を無効にします。この操作により、ユーザーは、構成されたホームページの代わりに本来要求された内部 URL を見ることができるようになります。

1. Citrix Endpoint Management のログオンに使用される NetScaler Gateway 仮想サーバーの設定を編集します。NetScaler Gateway で、［**Other Settings**］に移動して［**Redirect to Home Page**］チェックボックスをオフにします。



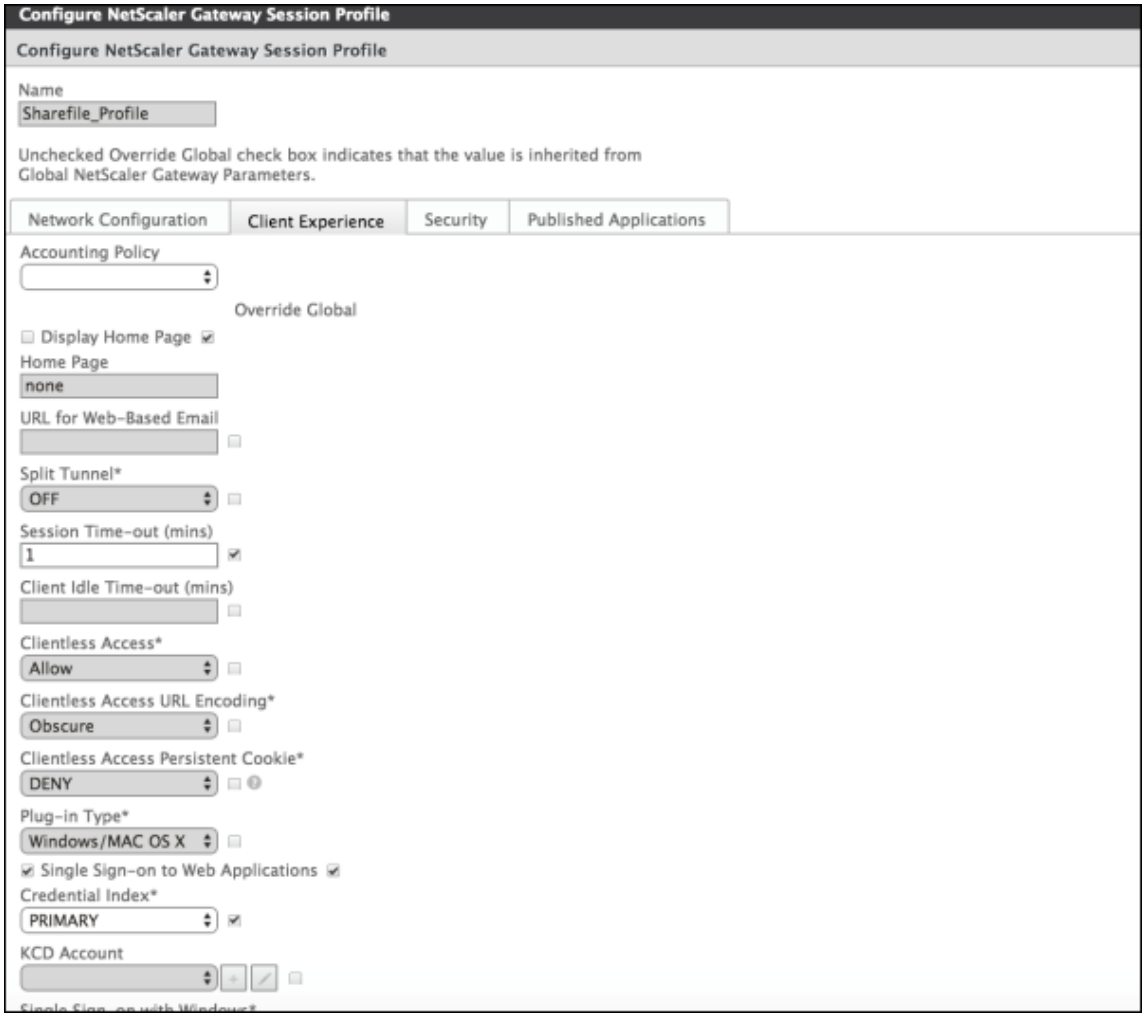
2. [**ShareFile**] の下に Citrix Endpoint Management の内部サーバー名およびポート番号を入力します。
3. **Citrix Endpoint Management** で、Citrix Endpoint Management URL を入力します。

   この構成により、/cginfra パスを介して入力した URL に対する要求が承認されます。

Citrix Files のセッションポリシーと要求プロファイルを作成する

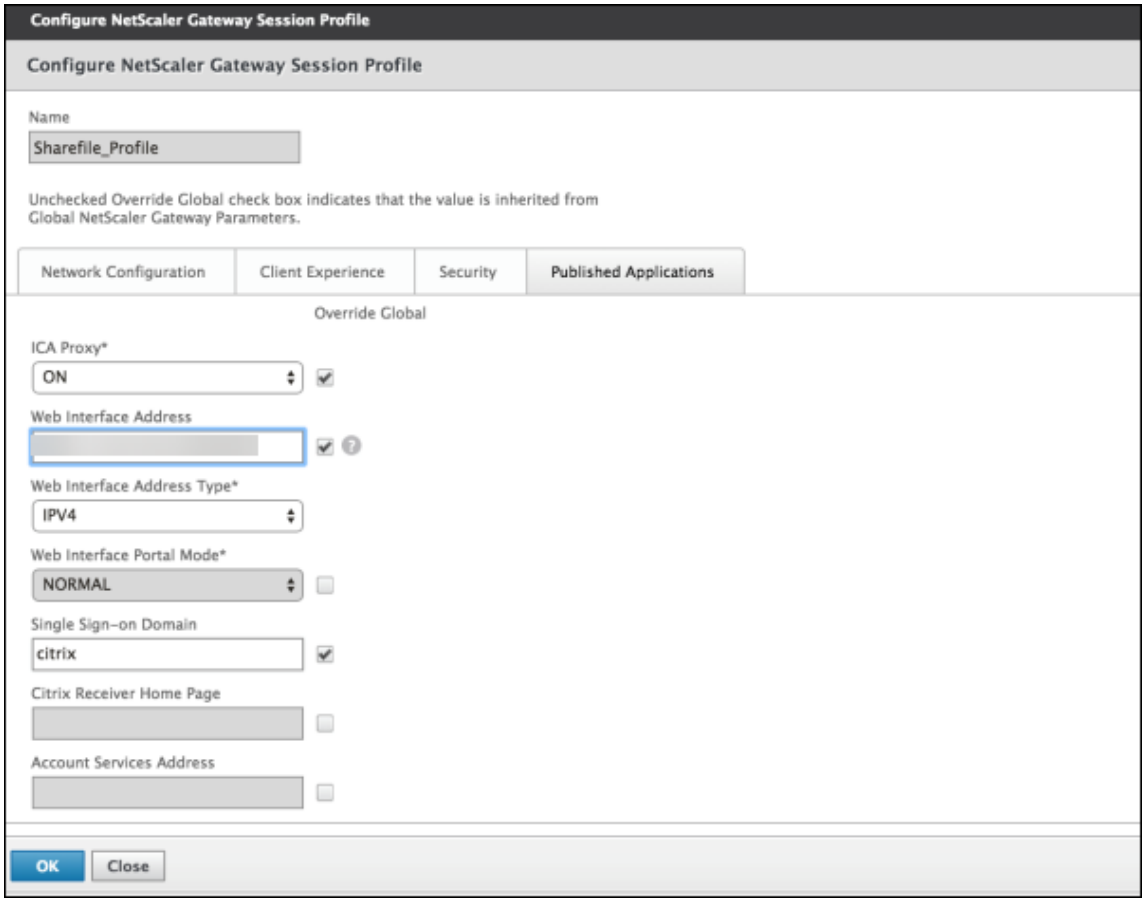
以下の設定を構成して Citrix Files セッションポリシーと要求プロファイルを作成します:

1. NetScaler Gateway Gateway 構成ユーティリティの左側のナビゲーションペインで、[**NetScaler Gateway**]、[**Policies**]、[**Session**] の順にクリックします。
2. セッションポリシーを作成します。[**Policies**] タブで [**Add**] をクリックします。
3. [**Name**] ボックスに「**ShareFile_Policy**」と入力します。
4. [**+**] をクリックして操作を作成します。[**Create NetScaler Gateway Session Profile**] ページが開きます。



次の設定を構成します:

- **Name**:「**ShareFile_Profile**」と入力します。
- [**Client Experience**] タブをクリックし、以下の設定を構成します:
  - **Home Page**:「**none**」と入力します。
  - **Session Time-out (mins)**:「**1**」と入力します。
  - **Single Sign-on to Web Applications**:この設定をクリックします。
  - **Credential Index**:[**PRIMARY**] をクリックします。
- [**Published Applications**] タブをクリックします。

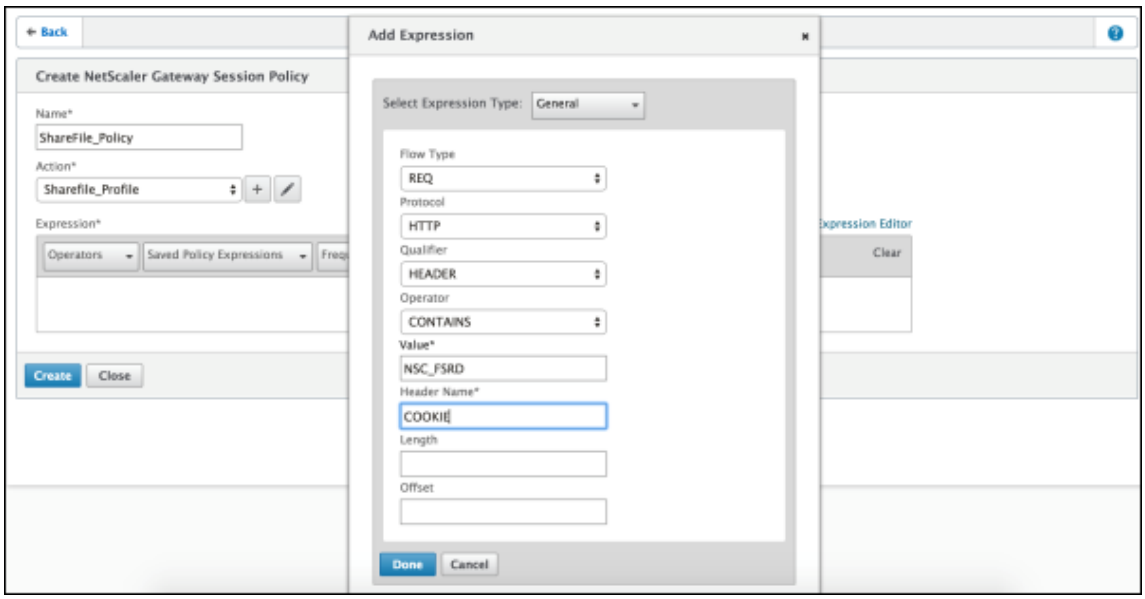


次の設定を構成します:

- **ICA Proxy**:［**ON**］を選択します。
- **Web Interface Address**: Citrix Endpoint Management サーバーの URL を入力します。
- **Single Sign-on Domain**: Active Directory ドメイン名を入力します。

  NetScaler Gateway セッションプロファイルを構成するとき、［**Single Sign-on Domain**］に入力するドメインサフィックスを LDAP に定義する Citrix Endpoint Management ドメインエイリアスと一致させる必要があります。

5. ［**Create**］をクリックしてセッションプロファイルを定義します。
6. ［**Expression Editor**］をクリックします。



次の設定を構成します:

- **Value**:「**NSC_FSRD**」と入力します。
- **Header Name**:「**COOKIE**」と入力します。

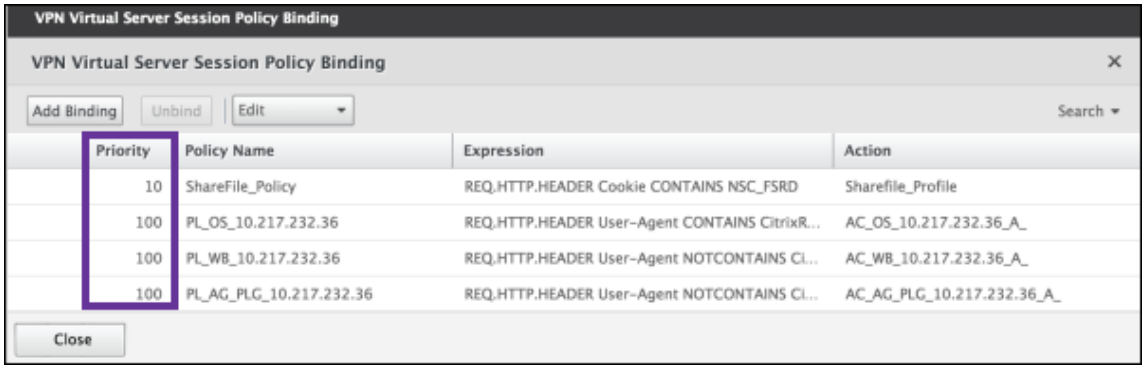
7. [**Create**] をクリックしてから、[**Close**] をクリックします。

NetScaler Gateway 仮想サーバーにポリシーを構成する

以下の設定を NetScaler Gateway 仮想サーバーに構成します。

1. NetScaler Gateway 構成ユーティリティの左側のナビゲーションペインで、[**NetScaler Gateway**] の [**Virtual Servers**] をクリックします。
2. [**Details**] ペインで NetScaler Gateway 仮想サーバーをクリックします。
3. [編集] をクリックします。
4. [**Configured policies**] の [**Session policies**] をクリックし、[**Add binding**] をクリックします。

5. [**ShareFile_Policy**] を選択します。
6. このポリシーの優先順位が一覧表示されるほかのポリシーよりも高くなるように、選択したポリシーに対して自動生成される [**Priority**] の番号を最も小さい数に変更します。例:



7. [**Done**] をクリックして、NetScaler Gateway 構成を保存します。

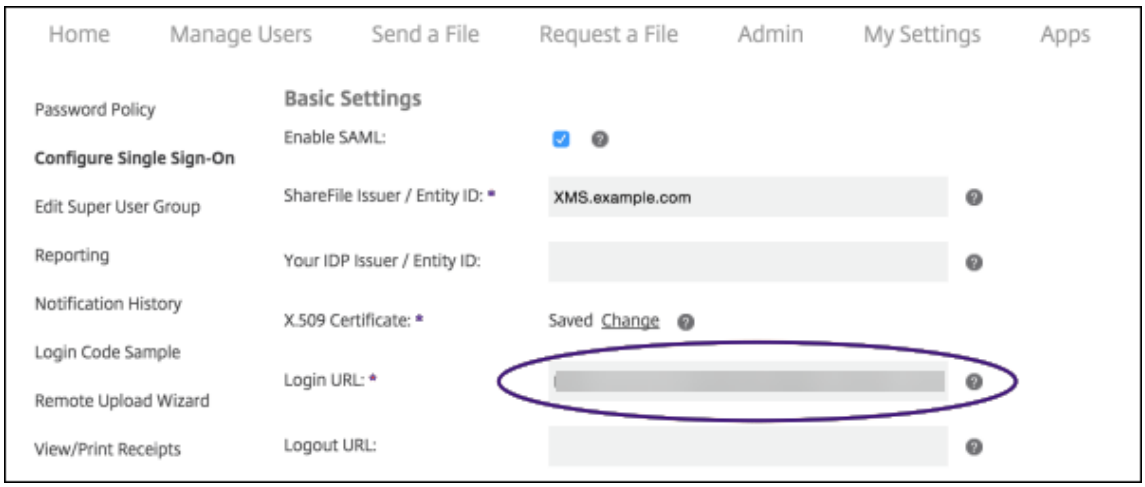
Citrix Files.com の SSO 設定を変更する

MDX および非 MDX Citrix Files アプリの両方に対して以下の変更を行います。

> 重要:
>
> 内部アプリケーション名に新しい番号が追加されます:
>
> - Citrix Files アプリの編集または再作成の都度
> - Citrix Endpoint Management での ShareFile 設定の変更の都度
>
> このため、Citrix Files Web サイトでログイン URL も更新して、更新されたアプリ名を反映する必要があります。

1. ShareFile アカウント (`https://<subdomain>.sharefile.com`) に ShareFile 管理者としてログオンします。
2. ShareFile Web インターフェイスで [管理] をクリックし、[シングルサインオンの構成] を選択します。
3. [ログイン **URL**] を以下のように編集します:

   編集前の [ログイン **URL**] の例は次のとおりです: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`



- Citrix Endpoint Management サーバーの FQDN の前に NetScaler Gateway 仮想サーバーの外部 FQDN および「**/cginfra/https/**」を挿入し、Citrix Endpoint Management の FQDN の後に「**8443**」を追加します。

  編集した URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

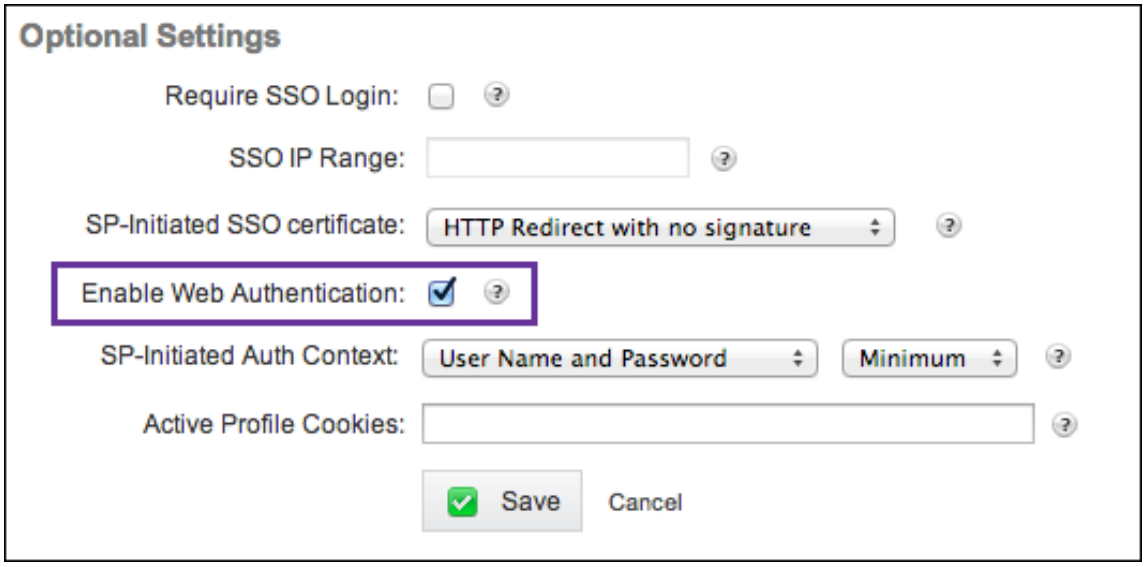
- パラメーター`&app=ShareFile_SAML_SP`を、Citrix Files 内部アプリ名に変更します。内部名はデフォルトで「`ShareFile_SAML`」です。ただし、構成を変更するたびに、内部名に数字が付加されます（例: `ShareFile_SAML_2`、`ShareFile_SAML_3`)。アプリの内部名は、［構成］**>** ［**ShareFile**］ページで調べることができます。

  編集した URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 「`&nssso=true`」を URL の最後に追加します。

  最終的な URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`

4. ［オプション設定］の下の ［**Web** 認証の有効化］チェックボックスをオンにします。



構成を検証する

以下の操作を実行して構成を検証します。

1. ブラウザーで`https://<subdomain>sharefile.com/saml/login`にアクセスします。

   NetScaler Gateway Gateway のログオンフォームにリダイレクトされます。リダイレクトされない場合は前の構成設定を検証します。

2. NetScaler Gateway および構成した Citrix Endpoint Management 環境のユーザー名とパスワードを入力します。

   `<subdomain>.sharefile.com`の Citrix Files フォルダーが表示されます。Citrix Files フォルダーが表示されない場合は、正しいログオン資格情報を入力したかどうか確認します。

Citrix Cloud を介した Azure Active Directory での認証

March 15, 2024

Citrix Endpoint Management では、Citrix Cloud を介した Azure Active Directory（Azure AD）の資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub 経由で MDM に登録するユーザーが利用できます。

Citrix Secure Hub を MDM+MAM で使用するには、Citrix Endpoint Management で MAM 登録に NetScaler Gateway を使用するよう構成します。詳しくは、「NetScaler Gateway と Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management は、Citrix Cloud サービスである Citrix ID を使用して、Azure Active Directory へのフェデレーションを行います。Azure Active Directory に直接接続するのではなく、Citrix ID プロバイダーを使用することをお勧めします。

Citrix Endpoint Management は、次のプラットフォームで Azure AD による認証をサポートしています:

- Apple Business Manager または Apple School Manager に登録されていない iOS および macOS デバイス
- Apple Business Manager に登録されている iOS および macOS デバイス
- Android Enterprise デバイス（プレビュー）、BYOD（Bring Your Own Device）および完全管理モード用

Citrix Cloud を介した Azure AD による認証には、次の制限があります:

- Citrix Endpoint Management ローカルアカウントでは使用できません。
- 登録招待状の Azure AD による認証をサポートしていません。登録 URL を含む登録招待状をユーザーに送信する場合は、ユーザーは Azure AD の代わりに LDAP を使用して認証します。

前提条件

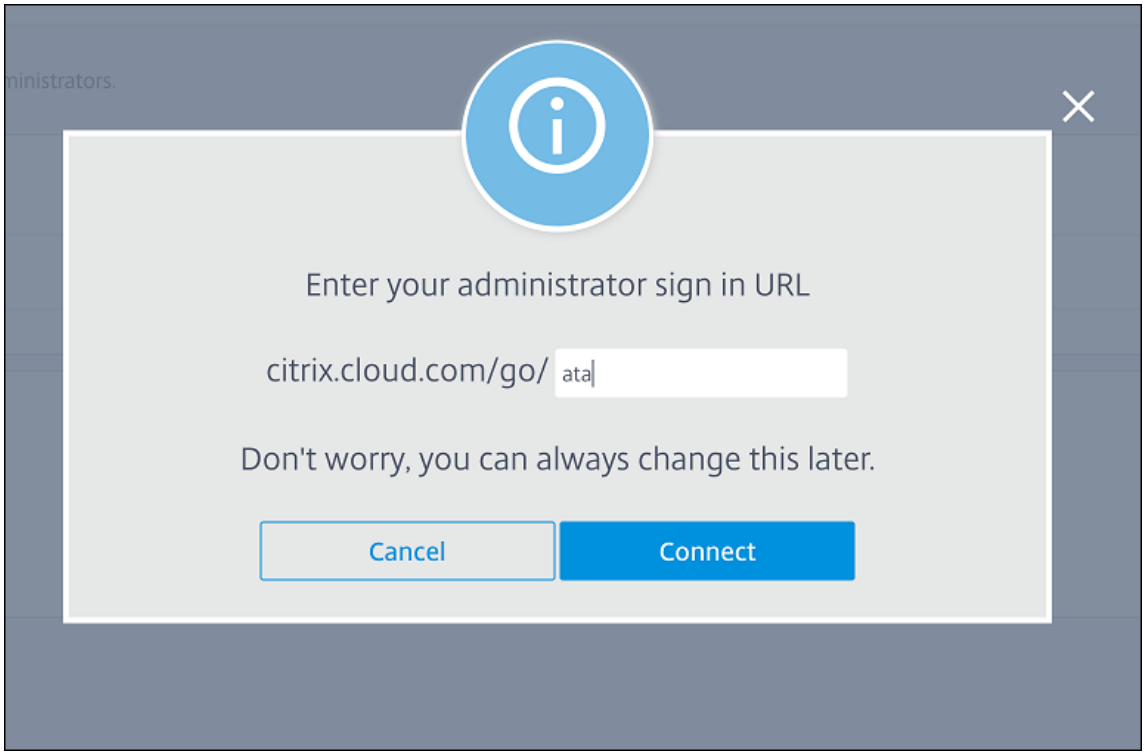
- Azure Active Directory ユーザーの資格情報
- Active Directory のユーザーグループは、Azure Active Directory のユーザーグループと一致する必要があります。
- Active Directory のユーザー名とメールアドレスは、Azure Active Directory のものと一致する必要があります。
- ディレクトリサービスの同期のために Citrix Cloud Connector がインストールされた Citrix Cloud アカウント
- で接続する必要があります。完全なシングルサインオンエクスペリエンスを実現するには、証明書ベースの認証か Azure AD のいずれかを有効にすることを Citrix ではお勧めします。モバイルアプリケーション管理（MAM：Mobile Application Management）登録のために、NetScaler Gateway で LDAP 認証を使用する場合、登録中にエンドユーザーには二重認証プロンプトが表示されます。詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。
- Android Enterprise の登録プロファイルで、［ユーザーにデバイス管理の許否を許可］を ［オフ］にする必要があります。ユーザーがデバイス管理を拒否した場合、登録の際に ID プロバイダーを使用して認証することができなくなります。詳しくは、「登録セキュリティ」を参照してください。

Azure Active Directory を **ID** プロバイダーとして使用するように **Citrix Cloud** を構成する

Citrix Secure Hub で使用するためにこのサービスをセットアップするには、Citrix Cloud で Azure Active Directory を構成します。

1. https://citrix.cloud.comで Citrix Cloud アカウントにサインインします。

2. Citrix Cloud メニューから ［**ID** およびアクセス管理］ページに移動し、Azure Active Directory に接続します。
3. 管理者のサインイン URL を入力し、［接続］をクリックします。



4. サインインすると、Azure Active Directory アカウントが Citrix Cloud に接続されます。［**ID** およびアクセス管理］**>**［認証］ページに、Citrix Cloud アカウントと Azure AD アカウントへのサインインに使用するアカウントが表示されます。
5. Citrix Secure Hub を介して登録するユーザーの Azure AD による認証を有効にするには、［ワークスペース構成］**>**［認証］で、［**Azure Active Directory**］を選択します。構成が完了したら、Citrix Secure Hub からユーザーデバイスを登録できます。

Citrix ID を **Citrix Endpoint Management** の **IDP** タイプとして構成する

この構成は、Citrix Secure Hub を介して登録するユーザーにのみ適用されます。Citrix Cloud で Azure Active Directory を構成したら、次のように Citrix Endpoint Management を構成します。

1. Citrix Endpoint Management コンソールで ［設定］**>**［**ID** プロバイダー（**IDP**）］に移動し、［追加］をクリックします。
2. ［**ID** プロバイダー（**IDP**）］ページで、次の項目を構成します：
   - **IDP** 名：作成する IDP 接続を識別できる一意の名前を入力します。
   - **IDP** の種類：［**Citrix ID** プラットフォーム］を選択します。

- 認証ドメイン：［**Azure Active Directory**］を選択します。このドメインは、Citrix Cloud の ［ワークスペース構成］**>**［認証］ページの ID プロバイダードメインに対応しています。

3. ［次へ］をクリックします。［**IDP** クレームの使用状況］ページで、次の項目を構成します：

   - ユーザー識別子の種類：このフィールドは、デフォルトでは［**userPrincipalName**］に設定されています。オンプレミスの Active Directory と Azure Active Directory の両方で、すべてのユーザーが同じ識別子で構成されていることを確認してください。Citrix Endpoint Management は、この識別子を使用して、ID プロバイダーのユーザーをオンプレミスの Active Directory ユーザーにマップします。
   - ユーザー識別子の文字列：このフィールドは自動入力されます。

4. ［次へ］を選択して ［概要］ページを確認し、［保存］をクリックします。

   これで、Citrix Secure Hub ユーザー、Citrix Endpoint Management コンソール、Self Help Portal ユーザーが Azure Active Directory の資格情報を使用してサインインできるようになります。ドメインに参加している Citrix Secure Hub ユーザーは、Citrix Secure Hub を使用して Azure AD 資格情報でサインオンできます。Citrix Secure Hub では、MAM デバイスのクライアント証明書認証を使用します。

Citrix Secure Hub の認証フロー

Citrix Endpoint Management は次のフローにより、Citrix Secure Hub を介して登録されたデバイス上の ID プロバイダーとして Azure AD を使用してユーザーを認証します：

1. Citrix Secure Hub を起動します。
2. Citrix Secure Hub が認証要求を Citrix ID に渡し、Citrix ID がこの要求を Azure Active Directory に渡します。
3. ユーザーは、Azure Active Directory のユーザー名とパスワードを入力します。
4. Azure Active Directory がユーザーを検証し、Citrix ID にコードを送信します。
5. Citrix ID がコードを Citrix Secure Hub に送信し、Citrix Secure Hub がコードを Citrix Endpoint Management サーバーに送信します。
6. Citrix Endpoint Management がコードとシークレットを使用して ID トークンを取得し、ID トークンに含まれるユーザー情報を検証します。Citrix Endpoint Management はセッション ID を返送します。

MAM 登録に **Citrix Gateway** を使用した **Azure Active Directory** での認証

December 8, 2023

Citrix Endpoint Management では、Gateway を介した Azure Active Directory（Azure AD）の資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub 経由で MAM に登録するユーザーのみが利用できます。

前提条件

Citrix Endpoint Management を構成し、MAM に登録されたデバイスで Azure AD を ID プロバイダー（IdP）として Citrix Gateway 経由で使用するには、次の前提条件が満たされていることを確認してください：

- Citrix Endpoint Management を構成し、MDM に登録されたデバイスの ID プロバイダーを Citrix Cloud 経由で Azure Active Directory に設定する。AAD で MDM を構成する方法について詳しくは、「Citrix Cloud を介した Azure Active Directory での認証」を参照してください。
- Citrix Cloud を Azure AD に接続する。詳しくは、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。
- プラットフォームに応じて、次の関連するフィーチャーフラグを有効にしてください：
  - iOS：
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android：
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

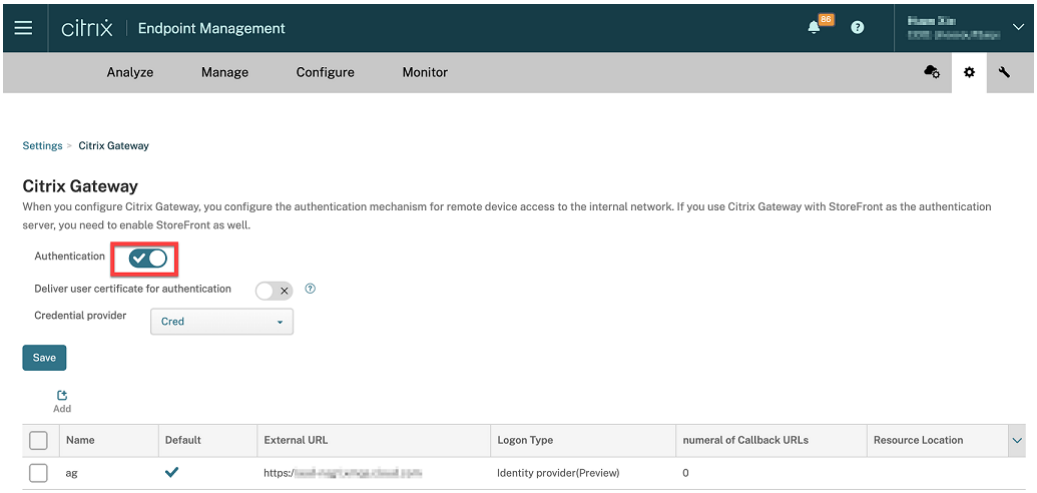
> 注：
>
> ご使用の環境でフィーチャーフラグを有効にするには、Podio フォームに記入してください。

- Android の場合、**Android Enterprise** を有効にします。

> 注：
>
> この機能は、従来の Android デバイス管理者（DA）モードではテストや検証がされていません。このモードはサポートされていません。

Azure AD を **MAM** で **ID** プロバイダーとして構成

1. Citrix Endpoint Management で Citrix Gateway を次のように構成します：
   a) Citrix Endpoint Management コンソールにサインインして、設定 アイコンをクリックします。
   b) ［サーバー］の下の ［**Citrix Gateway**］をクリックします。
   c) ［認証］トグルボタンを有効にします。



d) ゲートウェイの ［ログオンの種類］が ［*ID* プロバイダー］であることを確認します。

e) ［保存］をクリックします。

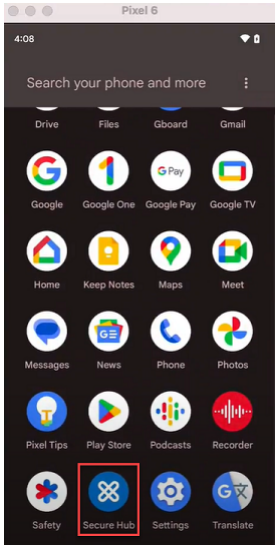
2. 「Azure AD を SAML IdP として構成」を参照して、Azure AD を SAML IdP として構成します。
3. 「NetScaler ADC を SAML サービス プロバイダー（SP）として構成」を参照して、高度なポリシーによって NetScaler ADC を SAML SP として構成します。
4. 「GUI を使用して認証仮想サーバーをセットアップするには」を参照して、AAA 仮想サーバーを作成します。
5. 「認証仮想サーバーの構成」を参照して、AAA 仮想サーバーを構成します。
6. 「認証プロファイル」を参照して、認証プロファイルを作成し、構成します。
7. 認証プロファイルを Gateway 仮想サーバーにバインドし、すべての構成を保存します。

Azure AD は、MAM に登録したデバイスの ID プロバイダーとして追加され、Azure AD を使用した認証が可能になりました。

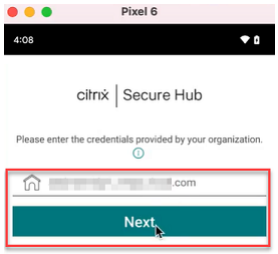
正常な動作

以下は、Android デバイスを使用した例です:

1. モバイルデバイスで、Citrix Secure Hub アプリを開きます。

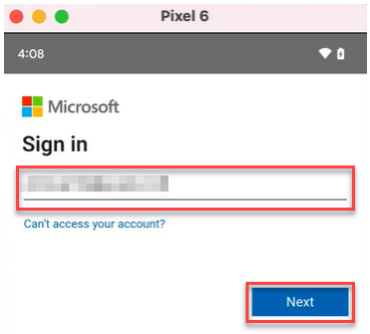


2. 必要な権限を許可します。
3. サインインページで、組織から提供された資格情報を入力し、［次へ］をタップします。

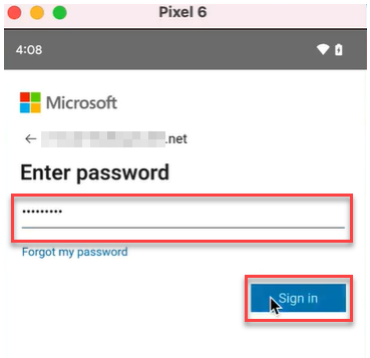


Microsoft のサインインページにリダイレクトされます。

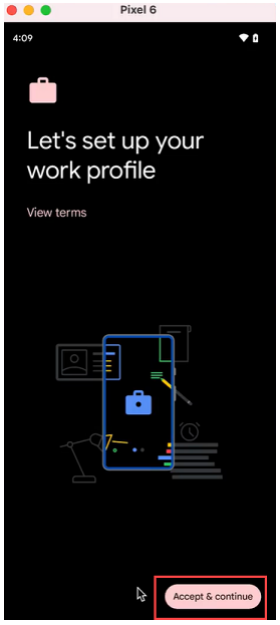
4. Microsoft のサインインページで、メール ID を入力し、［次へ］をタップします。



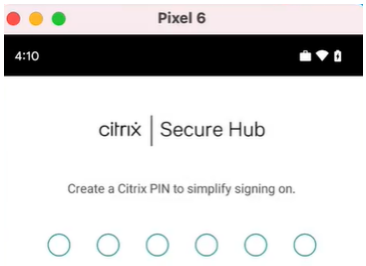
5. パスワードを入力し、［サインオン］をタップします。



6. 仕事用プロファイルの設定ページで、［同意して続行］をタップします。



7. Citrix Secure Hub アプリの PIN を作成して、確定します。



Citrix Secure Hub のホームページにリダイレクトされます。

Citrix Cloud を介した Okta での認証

March 15, 2024

Citrix Endpoint Management では、Citrix Cloud を介した Okta 資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub 経由で MDM に登録するユーザーが利用できます。

MAM に登録しているデバイスは、Okta 資格情報を使用して Citrix Cloud 経由で認証できません。Citrix Secure Hub を MDM+MAM で使用するには、Citrix Endpoint Management で MAM 登録に NetScaler Gateway を使用するよう構成します。詳しくは、「NetScaler Gateway と Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management は、Citrix Cloud サービスである Citrix ID を使用して、Okta へのフェデレーションを行います。Okta に直接接続するのではなく、Citrix ID プロバイダーを使用することをお勧めします。

Citrix Endpoint Management では、次のプラットフォームで Okta による認証をサポートしています:

- Apple Business Manager または Apple School Manager に登録されていない iOS および macOS デバイス
- Apple Business Manager に登録されている iOS および macOS デバイス
- Android Enterprise デバイス（プレビュー）、BYOD（Bring Your Own Device）および完全管理モード用

Citrix Cloud を介した Okta による認証には、次の制限があります:

- Citrix Endpoint Management ローカルアカウントでは使用できません。
- 登録招待状の Okta による認証はサポートしていません。登録 URL を含む登録招待状をユーザーに送信する場合は、ユーザーは Okta ではなく LDAP を使用して認証します。

前提条件

- Okta ユーザー資格情報
- Active Directory のユーザーグループは、Okta のユーザーグループと一致する必要があります。
- Active Directory のユーザー名とメールアドレスは、Okta のものと一致する必要があります。
- ディレクトリサービスの同期のために Citrix Cloud Connector がインストールされた Citrix Cloud アカウント
- で接続する必要があります。完全なシングルサインオンエクスペリエンスを実現するには、証明書ベースの認証を有効にすることを Citrix ではお勧めします。モバイルアプリケーション管理（MAM: Mobile Application Management）登録のために、NetScaler Gateway で LDAP 認証を使用する場合、登録中にエンドユーザーには二重認証プロンプトが表示されます。詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。
- Android Enterprise の登録プロファイルで、［ユーザーにデバイス管理の許否を許可］を ［オフ］にする必要があります。ユーザーがデバイス管理を拒否した場合、登録の際に ID プロバイダーを使用して認証することができなくなります。詳しくは、「登録セキュリティ」を参照してください。

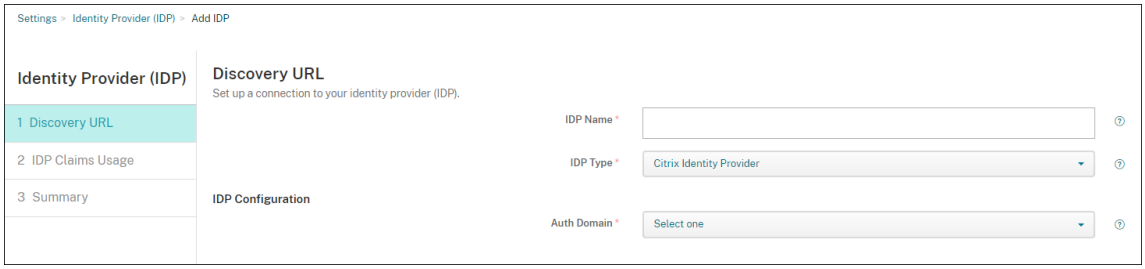
Okta を ID プロバイダーとして使用するように Citrix Cloud を構成する

Citrix Cloud で Okta を構成する方法については、「Okta を ID プロバイダーとして Citrix Cloud に接続する」を参照してください。

Citrix ID を Citrix Endpoint Management の IDP タイプとして構成する

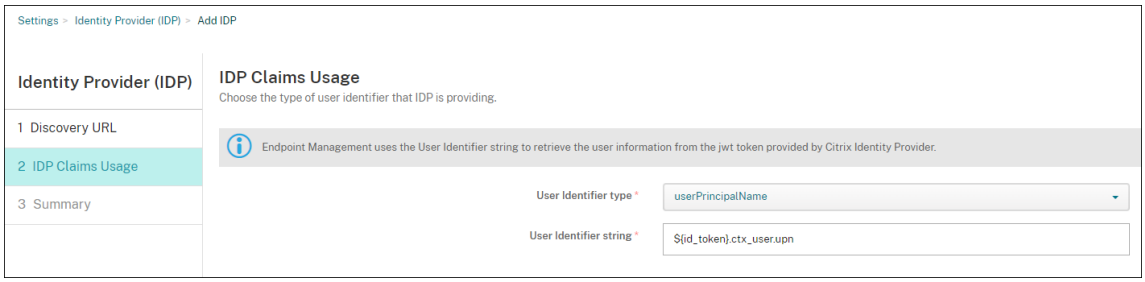
この構成は、Citrix Secure Hub を介して登録するユーザーにのみ適用されます。Citrix Cloud で Azure Active Directory を構成したら、次のように Citrix Endpoint Management を構成します:

1. Citrix Endpoint Management コンソールで ［設定］**>**［**ID** プロバイダー（**IDP**)］に移動し、［追加］をクリックします。
2. ［**ID** プロバイダー（**IDP**)］ページで、次の項目を構成します:



- **IDP** 名：作成する IdP 接続が識別できる一意の名前を入力します。
- **IDP** の種類：［**Citrix ID** プロバイダー］を選択します。
- 認証ドメイン：該当する Citrix Cloud ドメインを選択します。Citrix Cloud の ［**ID** およびアクセス管理］**>**［認証］ページに表示されるドメインを選択してください。

3. ［次へ］をクリックします。［**IDP** クレームの使用状況］ページで、次の項目を構成します:



- ユーザー識別子の種類：このフィールドは ［**userPrincipalName**］に設定します。オンプレミスの Active Directory と Okta で、すべてのユーザーが同じ識別子で構成されていることを確認してください。Citrix Endpoint Management は、この識別子を使用して、ID プロバイダーのユーザーをオンプレミスの Active Directory ユーザーにマップします。
- ユーザー識別子の文字列：このフィールドは自動入力されます。

この構成後、ドメインに参加している Citrix Secure Hub ユーザーは、Citrix Secure Hub を使用して Okta 資格情報でサインオンできます。Citrix Secure Hub では、MAM デバイスのクライアント証明書認証を使用します。

Citrix Secure Hub の認証フロー

Citrix Endpoint Management は次のフローにより、Citrix Secure Hub を介して登録されたデバイス上の ID プロバイダーとして Okta を使用してユーザーを認証します:

1. Citrix Secure Hub を起動します。
2. Citrix Secure Hub が認証要求を Citrix ID に渡し、Citrix ID がこの要求を Okta に渡します。
3. ユーザーはユーザー名とパスワードを入力します。
4. Okta がユーザーを検証し、Citrix ID にコードを送信します。
5. Citrix ID がコードを Citrix Secure Hub に送信し、Citrix Secure Hub がコードを Citrix Endpoint Management サーバーに送信します。
6. Citrix Endpoint Management がコードとシークレットを使用して ID トークンを取得し、ID トークンに含まれるユーザー情報を検証します。Citrix Endpoint Management はセッション ID を返送します。

MAM 登録に **Citrix Gateway** を使用した **Okta** での認証

November 29, 2023

Citrix Endpoint Management では、Citrix Gateway を介した Okta 資格情報による認証をサポートしています。この認証方法は、Citrix Secure Hub 経由で MAM に登録するユーザーのみが利用できます。

前提条件

Citrix Endpoint Management を構成し、MAM に登録されたデバイスで Okta を ID プロバイダー（IdP）として Citrix Gateway 経由で使用するには、次の前提条件が満たされていることを確認してください:

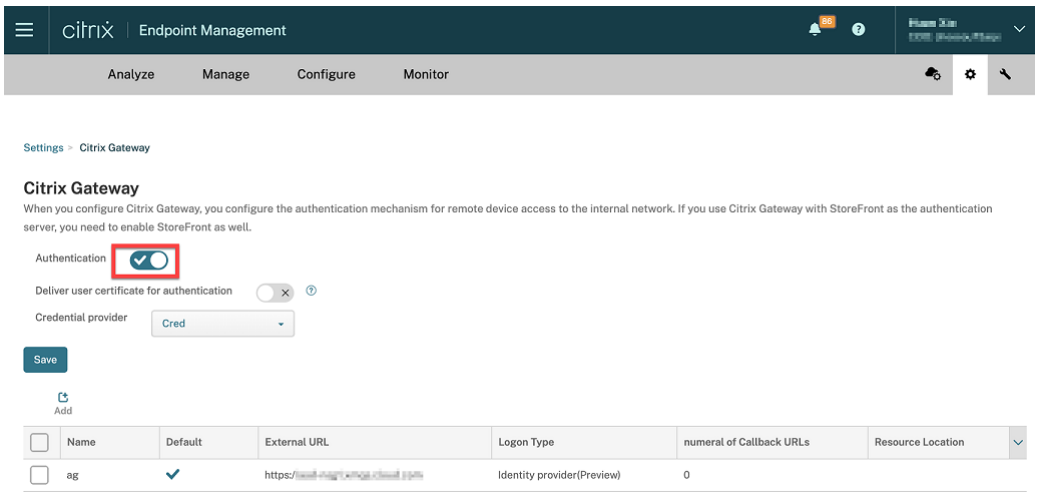
- Citrix Endpoint Management を構成し、MDM に登録されたデバイスの ID プロバイダーを Citrix Cloud 経由で Okta に設定する。MDM で Okta を構成する方法について詳しくは、「Citrix Cloud を介した Okta での認証」を参照してください。
- プラットフォームに応じて、次の関連するフィーチャーフラグを有効にしてください:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

> 注:
>
> ご使用の環境でフィーチャーフラグを有効にするには、Podio フォームに記入してください。

- Citrix Secure Hub の最新バージョンをダウンロードしてインストールします。
- 所属組織で Okta サービスが利用可能で、関連ユーザーおよびグループが Okta で作成されているか、インポートされていることを確認します。

Citrix Endpoint Management で使用する **Citrix Gateway** の構成

1. Citrix Endpoint Management コンソールにサインインして、設定 アイコンをクリックします。
2. ［サーバー］の下の ［**Citrix Gateway**］をクリックします。
3. ［認証］トグルボタンを有効にします。



4. ゲートウェイの ［ログオンの種類］が ［*ID* プロバイダー］であることを確認します。
5. ［保存］をクリックします。

オンプレミスの **Citrix Gateway** の準備

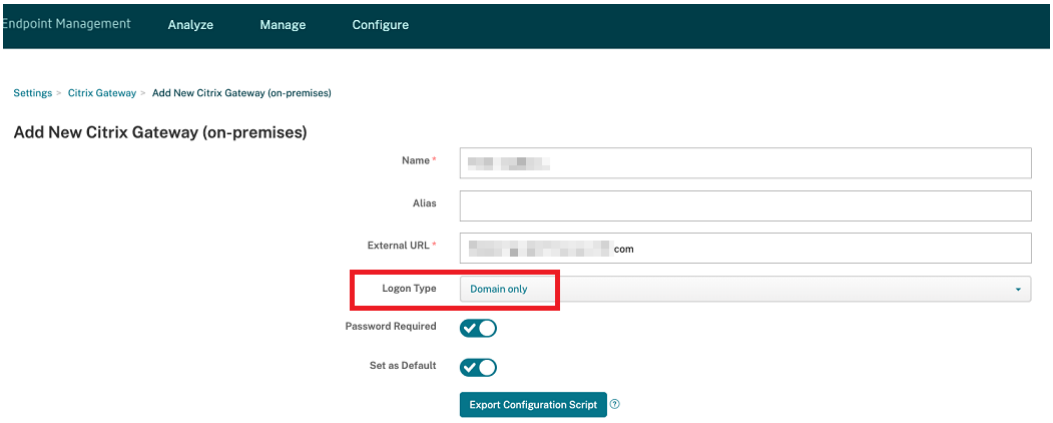
1. Citrix Endpoint Management でオンプレミスの Citrix Gateway が構成されていない場合、以下の手順を実行します:

   a) Citrix Endpoint Management コンソールにサインインして、設定 アイコンをクリックします。

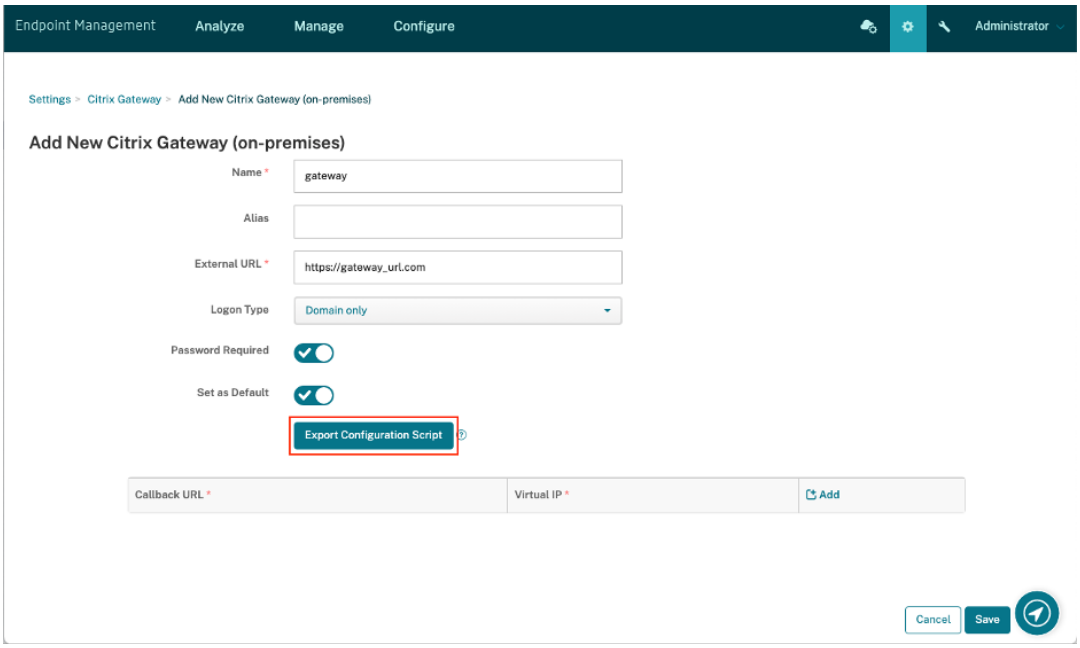
   b) ［サーバー］の下の ［**Citrix Gateway**］をクリックします。

   c) ［編集］をクリックします。

d) ［ログオンの種類］ドロップダウンメニューをクリックして、［ドメインのみ］を選択します。

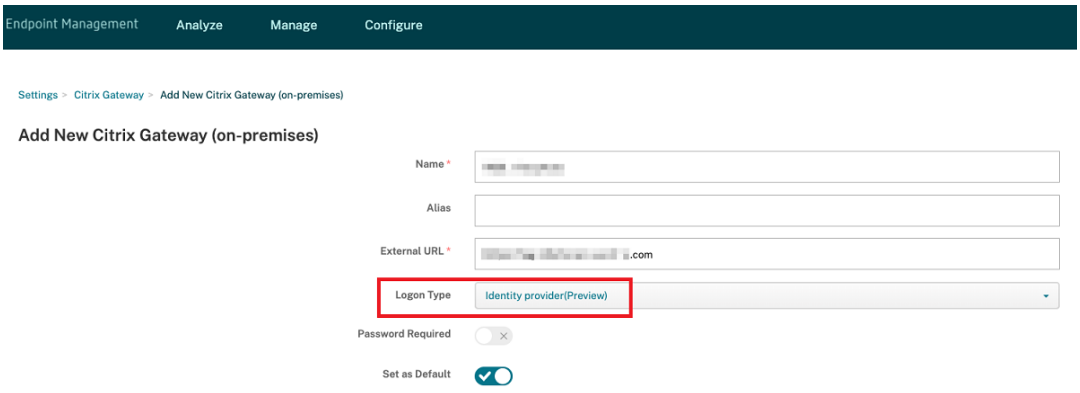


e) ［構成スクリプトのエクスポート］をクリックします。



［構成スクリプトのエクスポート］がダウンロードされます。

f) ［ログオンの種類］ドロップダウンメニューをクリックして ［*ID* プロバイダー］を選択します。



g) ［保存］をクリックします。

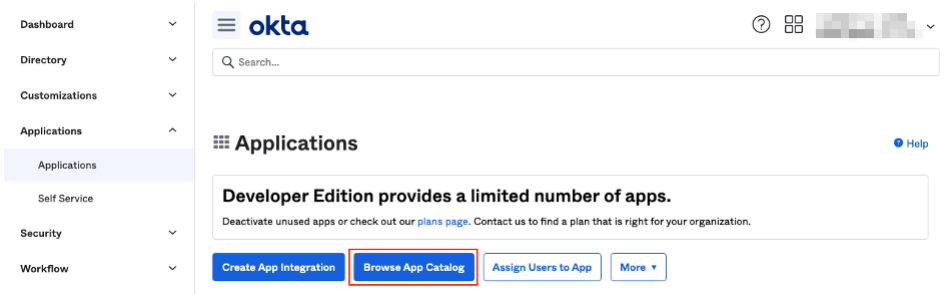
h) ダウンロードされた zip ファイルを開いて、ファイルを抽出します。

i) 抽出されたテキストファイルのスクリプトを実行して、オンプレミスの Citrix Gateway の準備をします。

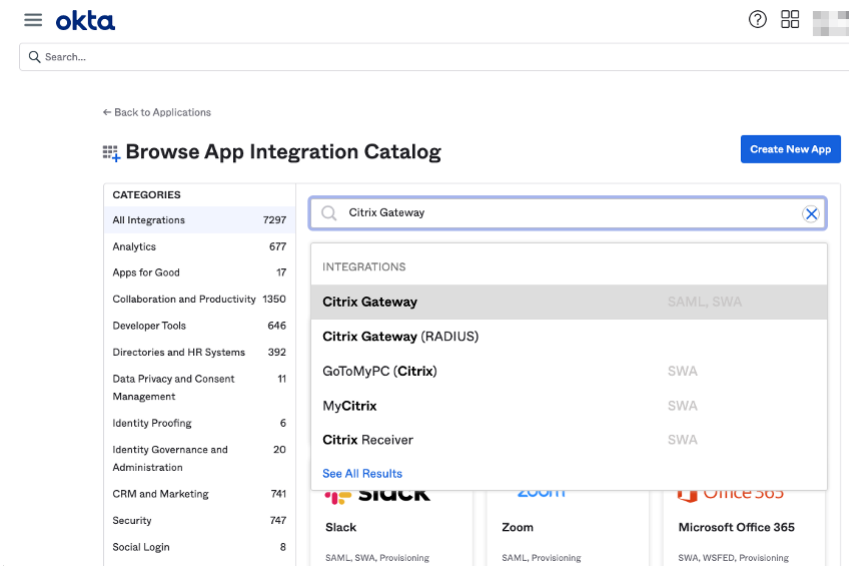
2. Citrix ADC 管理コンソールにサインインして、［**Citrix Gateway**］>［**Virtual Servers**］に移動します。
3. Citrix Endpoint Management のセットアップに関連したゲートウェイをクリックします。
4. オンプレミスの Citrix Gateway で既存の認証ポリシーのバインドを解除します。

Okta を構成する

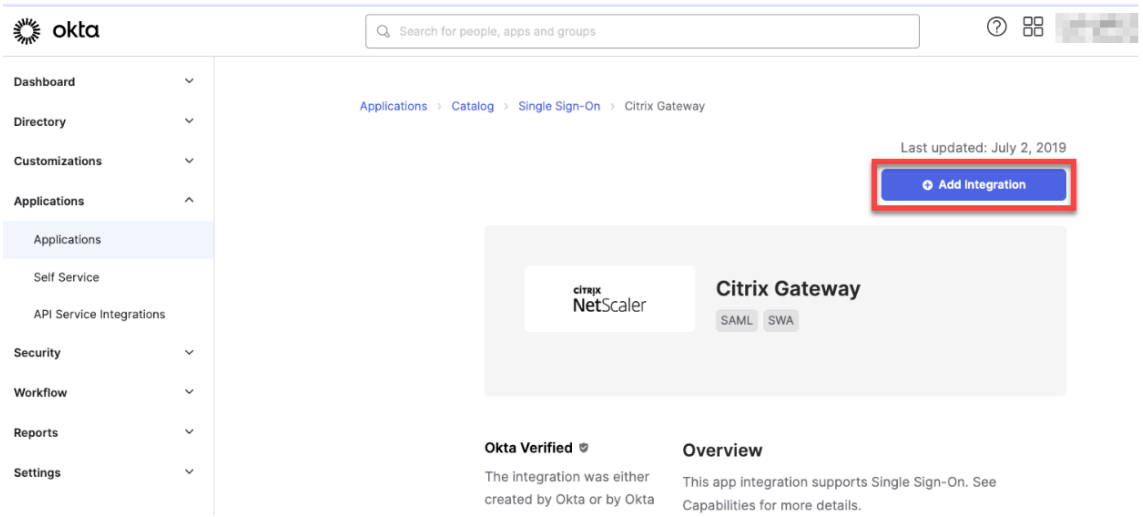
1. 管理者として Okta にサインインします。
2. ［**Applications**］>［**Applications**］>［**Browse App Catalog**］の順にクリックします。



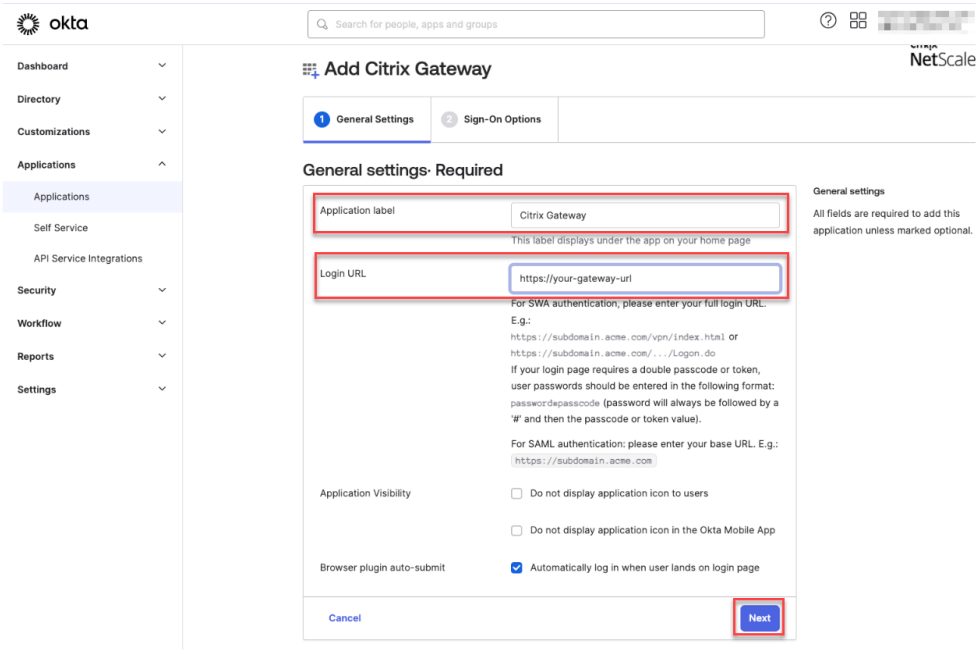
3. ［**Browse App Integration Catalog**］の下の検索バーに「**Citrix Gateway**」と入力して、**Citrix Gateway**（**SAML**、**SWA**）を選択します。



4. [**Add Integration**] をクリックします。

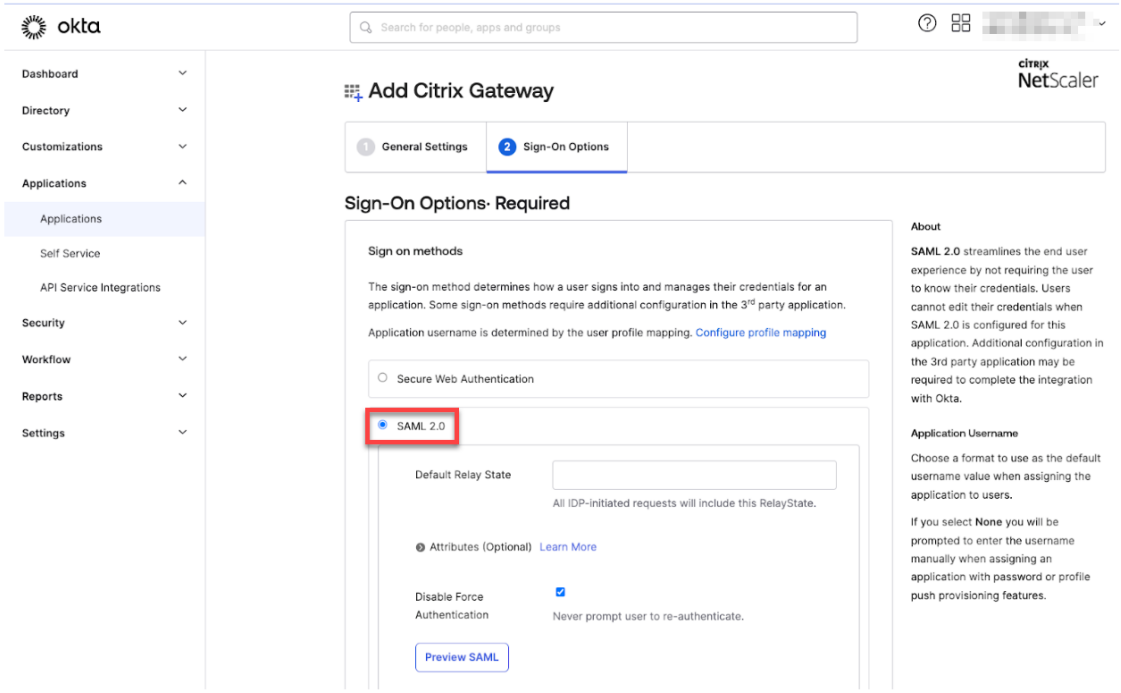


5. [**Application label**] フィールドに関連する名前を入力します。
6. [**Login URL**] フィールドにゲートウェイ仮想サーバー URL を入力して [**Next**] をクリックします。

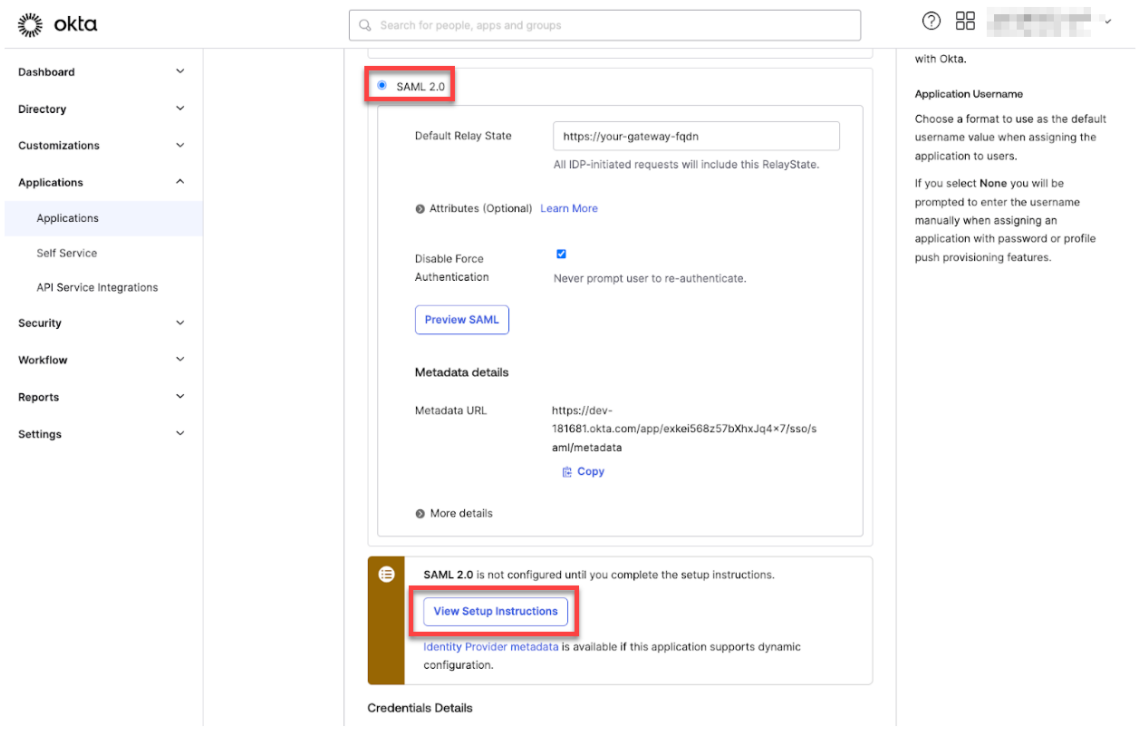


> 注:
>
> [**Login URL**] フィールドに入力した URL は、Citrix Endpoint Management 設定の Citrix Gateway URL と同じものにする必要があります。

7. [**Sign-On Options Required**] > [**Sign on methods**] の順に移動して、[**SAML 2.0**] を選択します。



8. [**View Setup Instructions**] をクリックしてページの指示に従い、Citrix オンプレミスゲートウェイの管理コンソールで SAML ポリシーを作成します。



> 注:
>
> - NetScaler Gateway バージョン 11.1 以降の構成中、CA 証明書をインストールしてから SAML アクションを作成します。SAML アクションを作成するには、[**Securit**] > [**AAA - Application Traffic**] > [**Policies**] > [**Authentication**] > [**Advanced Policies**] > [**Actions**] > [**SAML Actions**] に移動します。[**Add**] をクリックして、前のページで提供した情報を入力します。ページに表示される次のナビゲーションには従わないでください。[**NetScaler Gateway**] > [**Policies**] > [**Authentication**] > [**SAML**] > [**Servers**]。
> - また、SAML ポリシーを作成する手順にも従わないでください。これは古いポリシーを使用する手順です。現在は、より高度なポリシーを使用しています。高度なポリシーを使用して SAML ポリシーを作成するために、必ず手順 9 を実行してください。

9. SAML アクションに対応する SAML ポリシーを作成し、次のようにポリシーを認証仮想サーバーにバインドします:

   a) [Security] > [AAA-Application Traffic] > [Policies] > [Authentication] > [Advanced Policies] に移動して、[Add] をクリックします。

   b) [Create Authentication Policy] ページで、次の詳細を入力します:

   - **Name** - SAML ポリシーの名前を指定します。
   - **Action Type** - *SAML* を認証アクションの種類として選択します。
   - **Action** - SAML ポリシーをバインドする SAML サーバープロファイルを選択します。
   - **Expression** - ユーザーが SAML サーバーに認証すべきかを判断するために、SAML ポリシーが使用する規則や式の名前を表示します。有効にして、対応する SAML アクションが実行されるよ

うにするには、テキストボックスで、SAML ポリシーに **rule** = `true`の値を設定します。

c) SAML ポリシーを VPN 仮想サーバーにバインドして、認証プロファイル経由で VPN 仮想サーバーを認証仮想サーバーにリンクします。バインドの手順について詳しくは、「認証ポリシーのバインド」を参照してください。

10. 「GUI を使用して認証仮想サーバーをセットアップするには」を参照して、AAA 仮想サーバーを作成します。
11. 「認証仮想サーバーの構成」を参照して、AAA 仮想サーバーを構成します。
12. 「認証プロファイル」を参照して、認証プロファイルを作成し、構成します。
13. 認証プロファイルを Gateway 仮想サーバーにバインドし、すべての構成を保存します。
14. Citrix オンプレミスゲートウェイの管理コンソールで、SAML ポリシーの作成後、[Done] をクリックします。

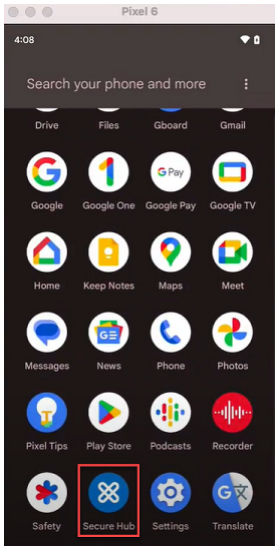
    Citrix Endpoint Management の統合で、Citrix Cloud の Web アプリケーションおよび Citrix Endpoint Management の MAM 認証の SAML アプリケーションという、2 つのアプリケーションが表示できるようになりました。
15. 関連ユーザーおよびグループを、作成したばかりの SAML アプリケーションに割り当てます。

Okta は、MAM に登録したデバイスの ID プロバイダーとして追加され、Okta を使用した認証が可能になりました。

正常な動作

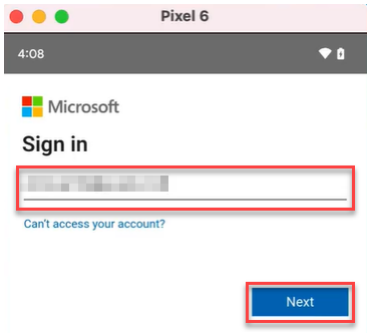
以下は、Android デバイスを使用した例です:

1. モバイルデバイスで、Citrix Secure Hub アプリを開きます。



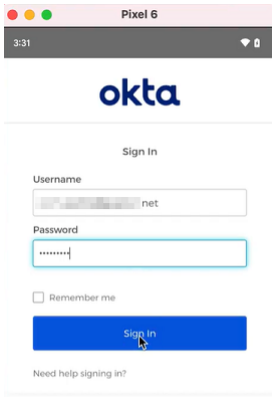
2. 必要な権限を許可します。

3. サインインページで、組織から提供された資格情報を入力し、［次へ］をタップします。

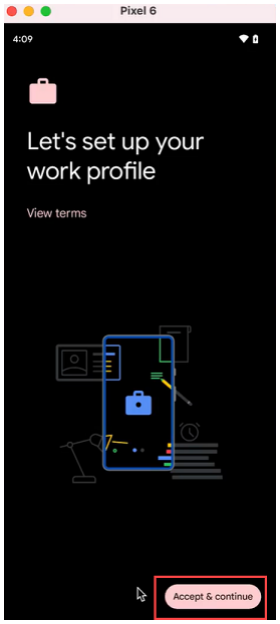


Okta のサインインページにリダイレクトされます。

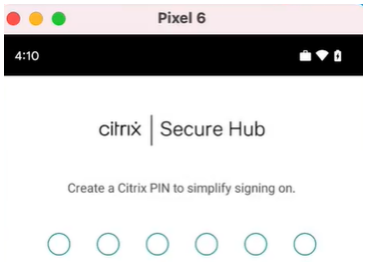
4. Okta のサインインページで資格情報を入力し、［**Sign in**］をタップします。



5. 仕事用プロファイルの設定ページで、［同意して続行］をタップします。



6. Citrix Secure Hub アプリの PIN を作成して、確定します。



Citrix Secure Hub のホームページにリダイレクトされます。

Citrix Cloud を介したオンプレミスの NetScaler Gateway での認証

March 15, 2024

Citrix Endpoint Management では、Citrix Cloud を介したオンプレミスの NetScaler Gateway による認証をサポートしています。この認証方法は、Citrix Secure Hub 経由で MDM に登録するユーザーが利用できます。

MAM に登録しているデバイスは、オンプレミスの NetScaler Gateway 資格情報を使用して Citrix Cloud 経由で認証することはできません。Citrix Secure Hub を MDM+MAM で使用するには、Citrix Endpoint Management で MAM 登録に NetScaler Gateway を使用するよう構成します。詳しくは、「NetScaler Gateway と Citrix Endpoint Management」を参照してください。

Citrix Endpoint Management では、次のプラットフォームに対して Citrix Cloud を介したオンプレミスの NetScaler Gateway による認証をサポートしています:

- iOS デバイス
- Android Enterprise デバイス、BYOD（Bring Your Own Device）および完全管理モード用

> 注:
>
> Citrix Endpoint Management は、登録招待状の Citrix Cloud を介したオンプレミスの NetScaler Gateway による認証をサポートしていません。登録 URL を含む登録招待状をユーザーに送信する場合は、ユーザーはオンプレミスの NetScaler Gateway ではなく LDAP を使用して、ID プロバイダーとして認証します。

完全なシングルサインオンエクスペリエンスを実現するには、証明書ベースの認証を有効にすることを Citrix ではお勧めします。モバイルアプリケーション管理（MAM：Mobile Application Management）登録のために、NetScaler Gateway で LDAP 認証を使用する場合、登録中にエンドユーザーには二重認証プロンプトが表示されます。詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。

前提条件

- で接続する必要があります。完全なシングルサインオンエクスペリエンスを実現するには、証明書ベースの認証を有効にすることを Citrix ではお勧めします。モバイルアプリケーション管理（MAM：Mobile Application Management）登録のために、NetScaler Gateway で LDAP 認証を使用する場合、登録中にエンドユーザーには二重認証プロンプトが表示されます。詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。
- ディレクトリサービスの同期のために Citrix Cloud Connector がインストールされた Citrix Cloud アカウント
- Citrix Secure Hub 20.5.0 以降。

NetScaler Gateway を **ID** プロバイダーとして使用するように **Citrix Cloud** を構成する

Citrix Cloud で NetScaler Gateway 認証をセットアップするには、「オンプレミスの NetScaler Gateway を ID プロバイダーとして Citrix Cloud に接続する」を参照してください。

Citrix ID プロバイダーを **Citrix Endpoint Management** の **IDP** タイプとして構成する

この構成は、Citrix Secure Hub を介して登録するユーザーにのみ適用されます。Citrix Cloud で NetScaler Gateway を構成したら、次のように Citrix Endpoint Management を構成します。

1. Citrix Endpoint Management コンソールで ［設定］**>**［**ID** プロバイダー（**IDP**）］に移動し、［追加］をクリックします。
2. ［**ID** プロバイダー（**IDP**）］ページで、次の項目を構成します：
   - **IDP** 名：作成する IDP 接続を識別できる一意の名前を入力します。
   - **IDP** の種類：［**Citrix ID** プロバイダー］を選択します。
   - 認証ドメイン：［**NetScaler Gateway**］を選択します。このドメインは、Citrix Cloud の ［ワークスペース構成］**>**［認証］ページの ID プロバイダードメインに対応しています。
3. ［次へ］をクリックします。［**IDP** クレームの使用状況］ページで、次の項目を構成します：
   - ユーザー識別子の種類：このフィールドは、デフォルトでは ［**userPrincipalName**］に設定されています。
   - ユーザー識別子の文字列：このフィールドは自動入力されます。
4. ［次へ］を選択して ［概要］ページを確認し、［保存］をクリックします。

   オンプレミスの NetScaler Gateway を ID プロバイダーとして使用し、Citrix Secure Hub を介してユーザーデバイスを登録できるようになりました。

Citrix Secure Hub の認証フロー

Citrix Endpoint Management は次のフローにより、Citrix Secure Hub を介して登録されたデバイス上の ID プロバイダーとしてオンプレミスの NetScaler Gateway を使用してユーザーを認証します:

1. Citrix Secure Hub を起動します。
2. Citrix Secure Hub が認証要求を Citrix ID に渡し、Citrix ID がこの要求をオンプレミスの NetScaler Gateway に渡します。
3. ユーザーはユーザー名とパスワードを入力します。
4. オンプレミスの NetScaler Gateway はユーザーを検証し、Citrix ID にコードを送信します。
5. Citrix ID がコードを Citrix Secure Hub に送信し、Citrix Secure Hub がコードを Citrix Endpoint Management サーバーに送信します。
6. Citrix Endpoint Management がコードとシークレットを使用して ID トークンを取得し、ID トークンに含まれるユーザー情報を検証します。Citrix Endpoint Management はセッション ID を返送します。

nFactor 認証

March 15, 2024

nFactor 認証では、Citrix Secure Hub を使用しているときに NetScaler で現在可能なすべての認証モードを使用できます。多要素認証は、アクセス権を付与するために複数の ID をユーザーに要求することで、アプリケーションのセキュリティを強化します。詳しくは、「nFactor 認証」を参照してください。

また、さまざまな認証および承認方法、およびそれらの構成方法について詳しくは、「認証と承認」を参照してください。

Citrix Endpoint Management では、次のプラットフォームで Okta による認証をサポートしています:

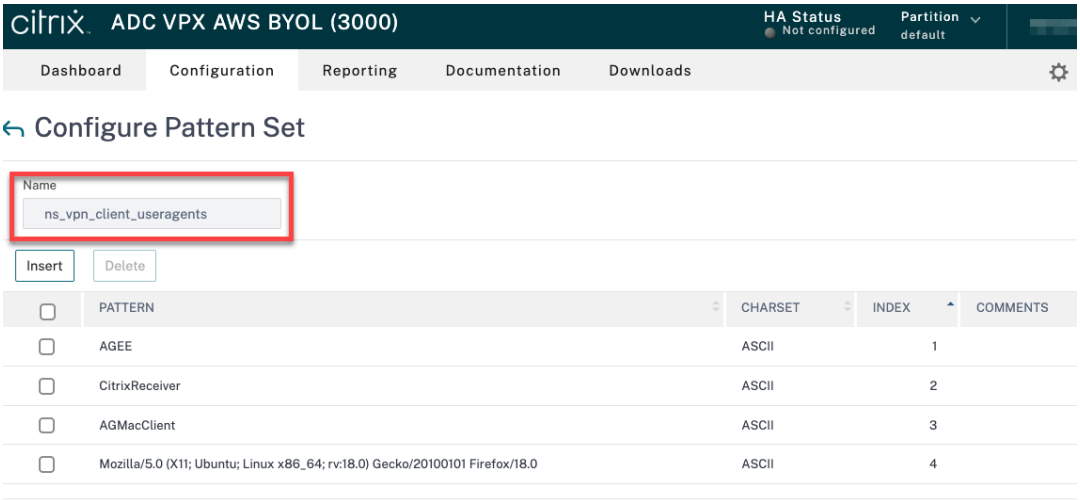
- ローカル
- ライトウェイトディレクトリアクセスプロトコル（LDAP）
- RADIUS
- SAML
- クライアント証明書認証

前提条件

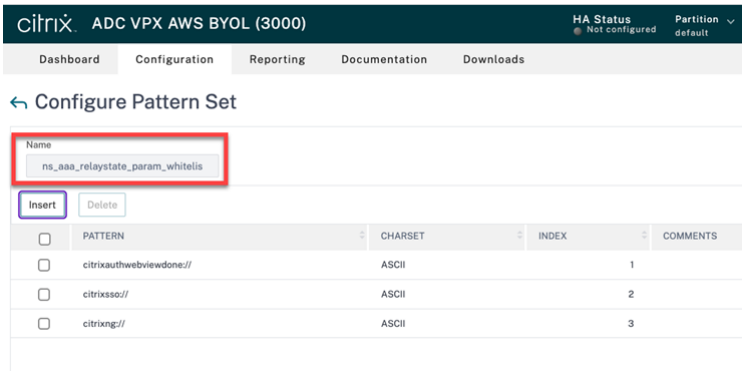
nFactor 認証を使用するように Citrix Endpoint Management を構成するには、次の前提条件が満たされていることを確認してください:

- NetScaler 13.0 以降を使用していることを確認する。

- Android および iOS デバイスの NetScaler で、次のパターンセット設定を構成していることを確認する:
  - Ns_vpn_client_useragents



  - NS_AAA_RelayState_Param_Whitelist



- Apple または Google Play から最新バージョンの Citrix Secure Hub がインストールされていることを確認する。
- NetScaler Gateway で高度な認証ポリシーを使用していることを確認する。
- オンプレミスとクラウドの両方で、クライアントプロパティ **ENABLE_MAM_NFACTOR_SSO** が **True** に設定されていることを確認する。**ENABLE_MAM_NFACTOR_SSO** プロパティについて詳しくは、「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。

> 注:
>
> クライアントプロパティ **Enable nFactor SSO** が **False** に設定されている場合は、従来の認証ポリシーが NetScaler Gateway にバインドされていることを確認する必要があります。

多要素（**nFactor**）認証の構成

NetScaler Gateway の設定方法に応じて、Citrix Endpoint Management の nFactor 認証を次のように構成します：

- Citrix Endpoint Management は、従来の認証ポリシーを使用して NetScaler Gateway で既に設定されています。詳しくは、「既存の NetScaler Gateway の従来のポリシーを高度な認証ポリシーに更新する」を参照してください。
- NetScaler Gateway で従来の認証ポリシーを使用した Citrix Endpoint Management の設定。詳しくは、「高度なポリシーを使用して NetScaler Gateway の設定を構成する」を参照してください。

既存の **NetScaler Gateway** の従来のポリシーを高度な認証ポリシーに更新する

Citrix Endpoint Management が NetScaler Gateway の従来の認証ポリシーを使用して既に設定されている場合は、次のいずれかの方法を使用して従来の認証ポリシーを高度な認証ポリシーに更新する必要があります：

- 新しい高度な認証ポリシーを作成し、高度な認証ポリシーを使用するようにゲートウェイ構成を変更します。詳しくは、「認証ポリシー」を参照してください。
- 従来の認証ポリシーを高度な認証ポリシーに更新します。詳しくは、「NSPEPI ツールを使用したポリシー式の変換」を参照してください。

高度なポリシーを使用して **NetScaler Gateway** の設定を構成する

高度な認証ポリシーを使用して NetScaler Gateway で Citrix Endpoint Management の nFactor 認証を構成するには、「多要素（nFactor）認証の構成」を参照してください。

> 注：
>
> - サポートされている認証の種類から関連した認証の種類を選択できます。
> - SAML 認証の種類を使用している場合は、次のいずれかの方法で MAM ID プロバイダーを使用して SAML を構成できます：
>   - Azure Active Directory を使用して構成するには、「MAM 登録に NetScaler Gateway を使用した Azure Active Directory での認証」を参照してください。
>   - Okta を使用して構成するには、「MAM 登録に NetScaler Gateway を使用した Okta での認証」を参照してください。

ユーザーアカウント、役割、および登録

March 15, 2024

Citrix Endpoint Management コンソールの ［管理］タブおよび ［設定］ページで、ユーザー構成タスクを実行します。別途記載されていない限り、ここでは以下のタスクの手順を説明します。

- 登録セキュリティモードおよび招待状
  - ［設定］**>**［登録］で、最大 7 つの登録セキュリティモードの構成と登録招待の送信を行います。それぞれの登録セキュリティモードに独自のセキュリティレベルと、ユーザーがデバイス登録時に実行する必要のある手順があります。
- ユーザーアカウントおよびグループの役割
  - ［設定］**>**［役割ベースのアクセス制御］で、権限の定義済みセットである役割をユーザーとグループに割り当てます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。詳しくは、「RBAC を使用した役割の構成」を参照してください。
  - ［設定］**>**［通知テンプレート］で通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Citrix Secure Hub または SMTP の 2 つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。詳しくは、「通知テンプレートの作成および更新」を参照してください。
- ユーザーアカウントおよびグループ:
  - ［管理］**>**［ユーザー］で、ローカルユーザーアカウントを手動で追加するか、.csv プロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理できます。ただし、ほとんどの Citrix Endpoint Management 展開はユーザーおよびグループ情報のために LDAP に接続します。次のようなユースケースでは、ローカルにユーザーアカウントを作成することをお勧めします。
    * リテールなど、デバイスが個別のユーザー専用にするよりも共有される環境の場合。
    * サポートされていないディレクトリ（Novell eDirectory など）を使用する場合。
  - ［設定］**>**［ワークフロー］で、ワークフローを使用して、ユーザーアカウントの作成および削除を管理します。

ユーザーアカウントについて

Citrix Endpoint Management のユーザーアカウントはローカルユーザー、Active Directory ユーザー、またはクラウドユーザーのいずれかです。

- クラウドユーザー：クラウドユーザーは、管理者が Citrix Cloud 顧客アカウントに追加されるときに Citrix Cloud によって作成される、特別なユーザーアカウントです。クラウドユーザーアカウントは、Citrix Cloud の管理者アカウントと同じユーザー名が使用され、デフォルトで Admin の役割になります。クラウドユーザーアカウントはシングルサインオンを提供し、その他の管理機能を実行します。

  Citrix Cloud アカウントに管理者を追加するには、「新しい管理者を招待する」を参照してください。

クラウドユーザーの場合:

- クラウドユーザーの役割とユーザープロパティは、Citrix Cloud コンソールから変更できます。「Citrix Cloud 管理者を管理する」を参照してください。
- パスワードを変更するには、「管理者」を参照してください。
- クラウドユーザーを削除するには、Citrix Cloud で［**ID** およびアクセス管理］**>**［管理者］に移動します。ユーザーの行の最後にある省略記号（…）をクリックして、［管理者の削除］を選択します。
- クラウドユーザーをローカルグループに追加することはできません。

登録セキュリティモードを構成する

デバイスの登録セキュリティモードを構成して、Citrix Endpoint Management へのデバイスの登録に使用するセキュリティレベルと通知テンプレートを指定します。

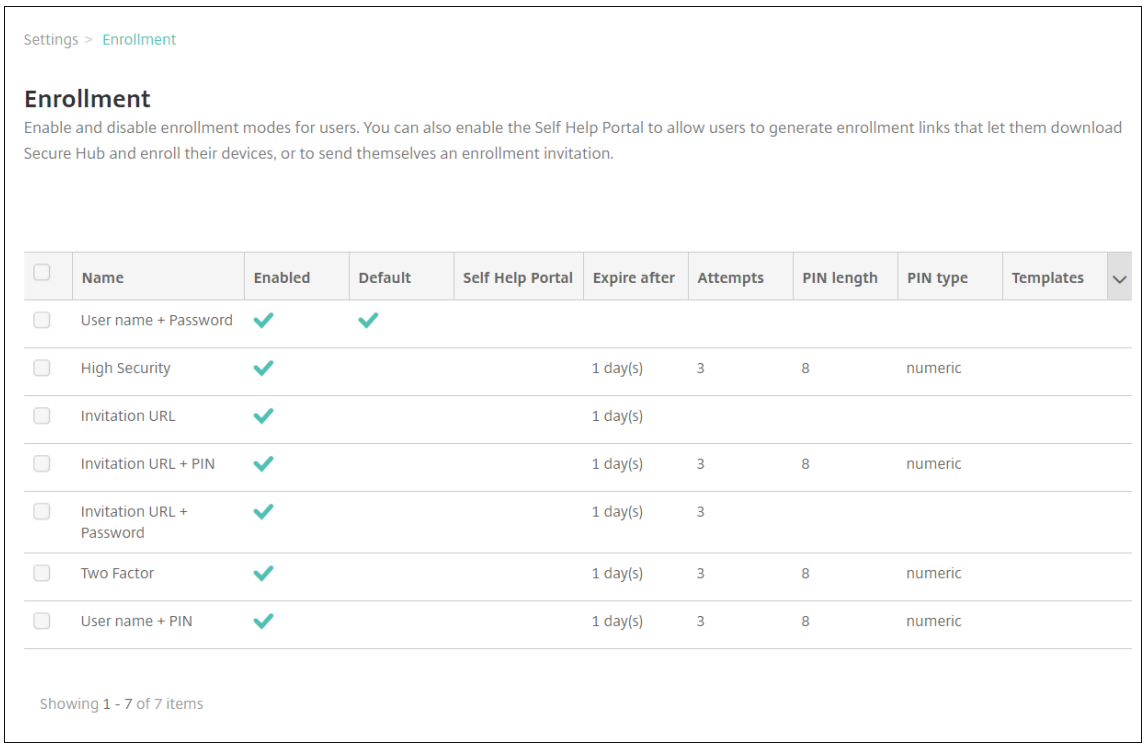
Citrix Endpoint Management には 6 つの登録セキュリティモードがあり、それぞれに独自のセキュリティレベルと、ユーザーがデバイスを登録するときに行う必要がある手順があります。登録セキュリティモードの構成は、Citrix Endpoint Management コンソールの ［管理］**>**［登録招待］ページから行います。詳しくは、「登録招待」を参照してください。

> 注:
>
> カスタム通知テンプレートを使用する予定の場合は、登録セキュリティモードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［登録］をクリックします。［登録］ページが開きます。使用可能なすべての登録セキュリティモードの表が表示されます。デフォルトでは、すべての登録セキュリティモードが有効です。
3. 一覧から登録セキュリティモードを選択して編集します。次に、モードをデフォルトとして設定するか、モードを無効にします。

   登録セキュリティモードの横にあるチェックボックスをオンにして、オプションメニューを表示します。または、一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

   > ヒント:
   >
   > 登録セキュリティモードを編集するときに、ユーザーがデバイスを登録できなくなる有効期限を指定できます。詳しくは、この記事の「登録セキュリティモードを編集するには」を参照してください。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。



プラットフォームごとに、以下の登録セキュリティモードがあります:

- ユーザー名およびパスワード
- 招待 URL
- 招待 URL および PIN
- 招待 URL およびパスワード
- 2 要素
- ユーザー名および PIN

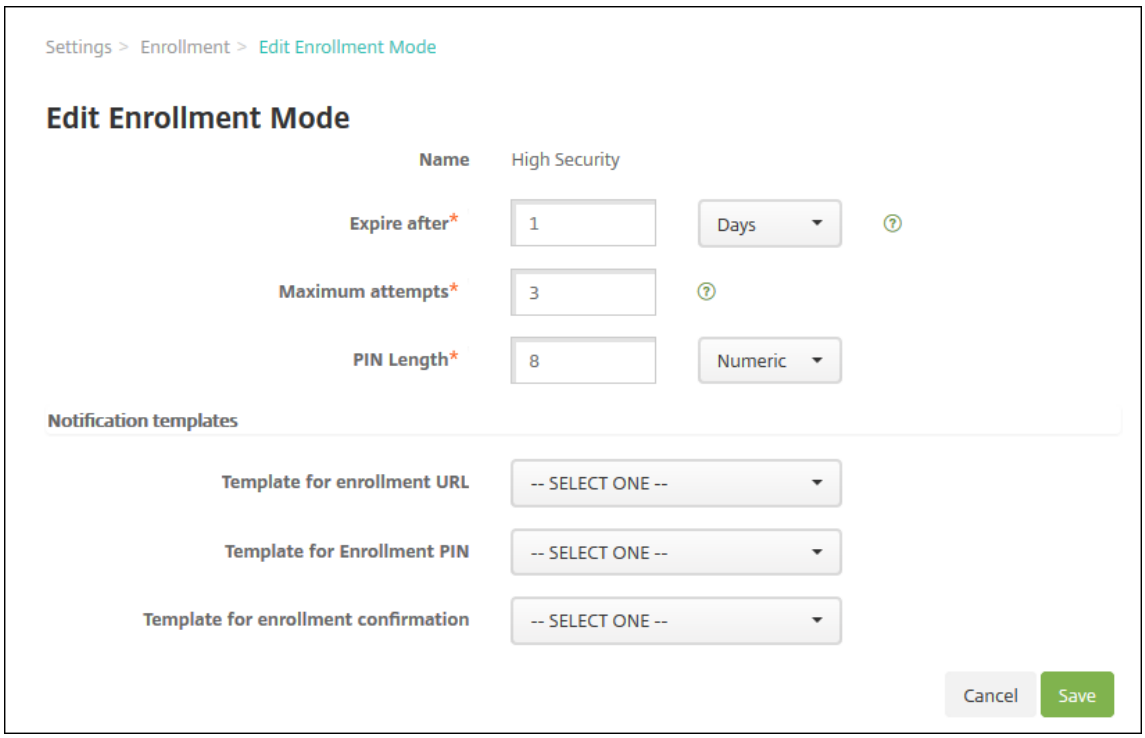
プラットフォーム固有の登録セキュリティモードについては、「プラットフォームごとの登録セキュリティモード」を参照してください。

登録招待状は、登録を特定のユーザーやグループに限定する場合に役立ちます。登録招待状を送信するには、登録セキュリティモードとして、[招待 **URL**]、[招待 **URL** および **PIN**]、または [招待 **URL** およびパスワード] のいずれかのみを使用できます。[ユーザー名およびパスワード]、[**2** 要素認証]、[ユーザー名および **PIN**] のいずれかで登録するデバイスの場合、Citrix Secure Hub に資格情報を手動で入力する必要があります。

ワンタイム PIN（OTP：One-Time PIN）登録招待状は、2 要素認証ソリューションとして使用できます。ワンタイム PIN 登録招待状では、ユーザーが登録可能なデバイスの数を制限できます。OTP の招待状は Windows デバイスでは利用できません。

登録セキュリティモードを編集するには

1. ［登録］の一覧で登録セキュリティモードを選択し、［編集］をクリックします。［登録モードの編集］ページが開きます。選択したモードによって、異なるオプションが表示される場合があります。



2. 必要に応じて以下の情報を変更します。

   - 有効期限：ユーザーがデバイスを登録できなくなる、有効期限を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。

     招待の有効期限が切れないようにするには **0** を入力します。

   - 日：ドロップダウンリストから、［有効期限］ボックスに入力した有効期限に応じて、［日］または ［時間］を選択します。

   - 最大試行数：登録処理からロックアウトされるまでにユーザーが実行できる登録の試行回数を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。

     無制限に試行できるようにするには **0** を入力します。

   - **PIN** 長：生成される PIN の長さを設定する数字を入力します。

   - **Numeric**：ドロップダウンリストから、PIN の種類として、［**Numeric**］または［**Alphanumeric**］を選択します。

   - 通知テンプレート：

     – 登録 **URL** 用テンプレート：ドロップダウンリストから、登録 URL に使用するテンプレートを選択します。たとえば、登録招待テンプレートでは、ユーザーにメールが送信されます。通知テンプ

レートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。
- 登録 **PIN** 用テンプレート：ドロップダウンリストから、登録 PIN に使用するテンプレートを選択します。
- 登録確認用テンプレート：ドロップダウンリストから、登録が成功したことをユーザーに通知するときに使用するテンプレートを選択します。

3. ［保存］をクリックします。

登録セキュリティモードをデフォルトとして設定するには

デフォルトの登録セキュリティモードは、別の登録セキュリティモードを選択しない限り、そのモードがすべてのデバイス登録要求に対して使用されます。デフォルトとして設定されている登録セキュリティモードがない場合は、デバイス登録ごとに登録要求を作成する必要があります。

1. デフォルトとして使用する登録セキュリティモードが有効になっていない場合は、それを選択して ［有効］をクリックします。デフォルトの登録セキュリティモードとして使用できるのは、［ユーザー名およびパスワード］、［**2** 要素］、［ユーザー名および **PIN**］のいずれかのみです。
2. 登録セキュリティモードを選択し、［デフォルト］をクリックします。これにより、選択したモードがデフォルトになります。ほかの登録セキュリティモードがデフォルトとして設定されていた場合、そのモードはデフォルトでなくなります。

登録セキュリティモードを無効化するには

登録セキュリティモードを無効化すると、その登録セキュリティモードは、グループ登録招待状でも Self Help Portal でも使用できなくなります。ある登録セキュリティモードを無効化して別の登録セキュリティモードを有効化することで、ユーザーがデバイスを登録できる方法を変更できます。

1. 登録セキュリティモードを選択します。

   デフォルトの登録セキュリティモードは無効化できません。デフォルトの登録セキュリティモードを無効化するには、登録モードのデフォルト状態をまず解除する必要があります。
2. ［無効化］をクリックします。登録セキュリティモードが有効でなくなります。

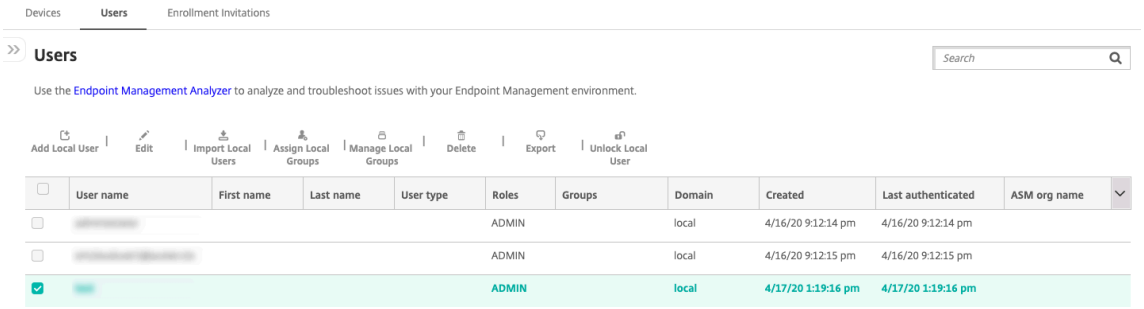
ローカルユーザーアカウントの追加、編集、ロック解除、または削除

ローカルユーザーアカウントを Citrix Endpoint Management に手動で追加したり、プロビジョニングファイルを使用してアカウントをインポートしたりすることができます。プロビジョニングファイルからユーザーをインポートする手順については、「ユーザーアカウントをインポートするには」を参照してください。

すべての Citrix Cloud 管理者が Citrix Endpoint Management 管理者として作成されます。カスタムアクセス権を持つ Citrix Cloud 管理者を作成する場合、Citrix Endpoint Management へのアクセスを含めるように注意し

ます。Citrix Cloud 管理者の追加について詳しくは、「Citrix Cloud アカウントに管理者を追加する」を参照してください。

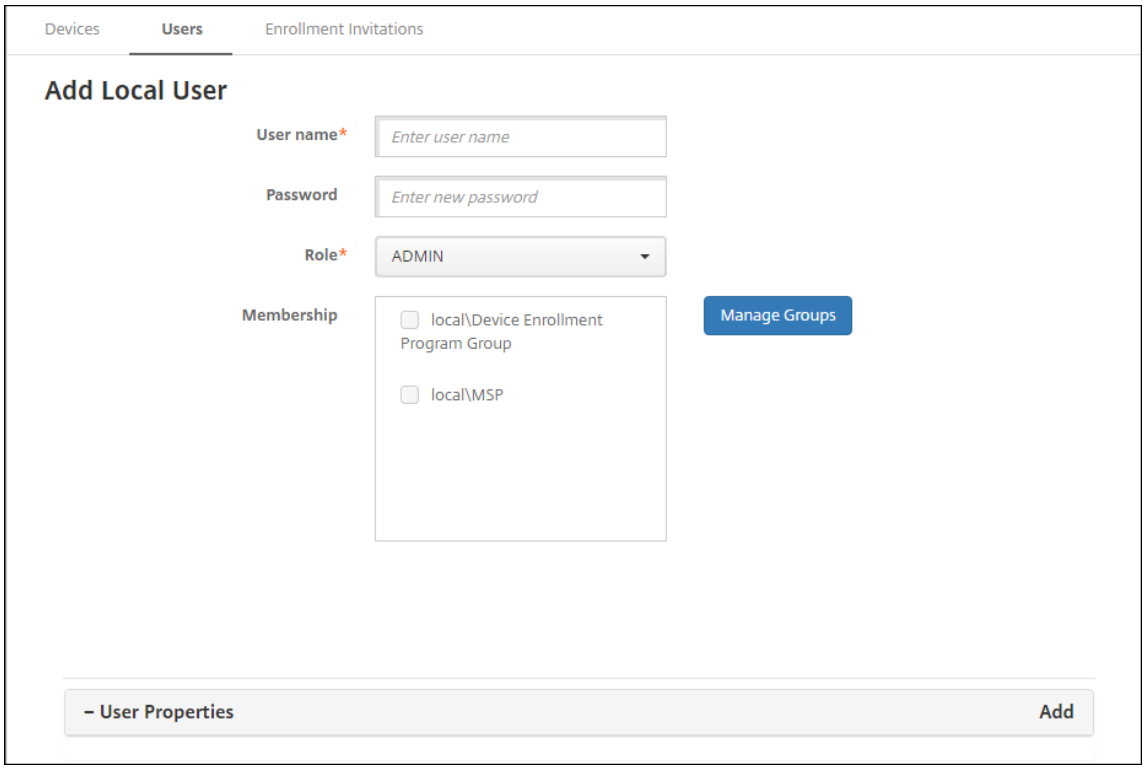
1. Citrix Endpoint Management コンソールで、[管理] > [ユーザー] の順にクリックします。[ユーザー] ページが開きます。



2. [フィルターを表示] をクリックして一覧をフィルターします。

ローカルユーザーアカウントを追加するには

1. [ユーザー] ページで、[ローカルユーザーの追加] をクリックします。[ローカルユーザーの追加] ページが開きます。



2. 次の設定を構成します:

- ユーザー名：名前を入力します。このフィールドは必須です。名前には、スペース、大文字、小文字を使用できます。
- パスワード：任意で、ユーザーのパスワードを入力します。パスワードは 14 文字以上にして、以下の条件のすべてを満たす必要があります：
  - 数字を 2 つ以上含む
  - 大文字と小文字をそれぞれ 1 つ以上含む
  - 特殊文字を 1 つ以上含む
  - 辞書の単語や制限された単語（Citrix ユーザー名やメールアドレスなど）は含めないでください。
  - 1111、1234、asdf など、3 文字以上の連続する文字や繰り返し文字、またはキーボードパターンを含めないでください。
- 役割：ドロップダウンリストから、ユーザーの役割を選択します。役割について詳しくは、「RBAC を使用した役割の構成」を参照してください。選択できるオプションは以下のとおりです：
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- メンバーシップ：ドロップダウンリストから、ユーザーを追加するグループを選択します。
- ユーザープロパティ：任意でユーザープロパティを追加します。追加するユーザープロパティごとに、［追加］をクリックして以下の操作を行います：
  - ユーザープロパティ：ドロップダウンリストからプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
  - ［完了］をクリックしてユーザープロパティを保存するか、［キャンセル］をクリックします。

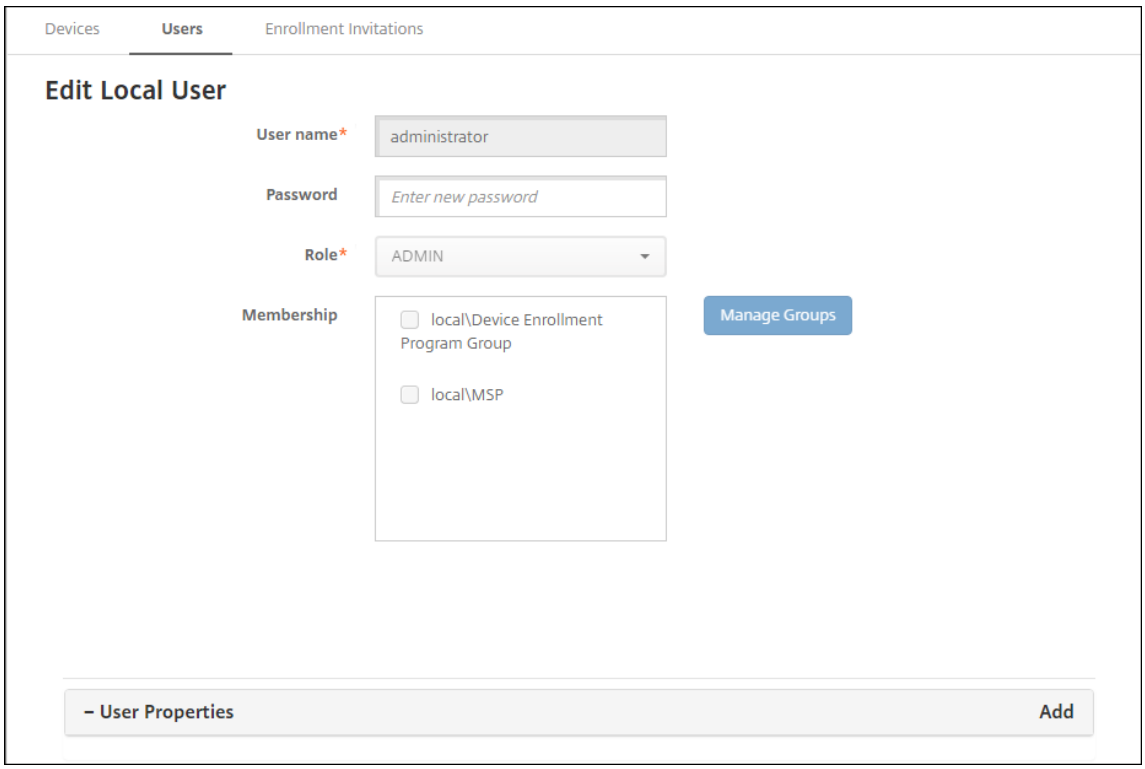
既存のユーザープロパティを削除するには、プロパティが含まれる行の上にマウスポインターを置き、右側の［**X**］をクリックします。プロパティがすぐに削除されます。

既存のユーザープロパティを編集するには、プロパティを選択して変更を加えます。［完了］をクリックして変更した項目を保存するか、［キャンセル］をクリックして項目を変更せずそのままにします。

3. ［保存］をクリックします。ユーザー作成後は、ローカルユーザーアカウントの ［ユーザーの種類］フィールドは空のままです。

ローカルユーザーアカウントを編集するには

1. ［ユーザー］ページのユーザー一覧で、ユーザーをクリックして選択してから ［編集］をクリックします。［ローカルユーザーの編集］ページが開きます。



2. 必要に応じて以下の情報を変更します。

   - ユーザー名：ユーザー名は変更できません。
   - パスワード：ユーザーパスワードを変更または追加します。
   - 役割：ドロップダウンリストから、ユーザーの役割を選択します。
   - メンバーシップ：ドロップダウンリストから、ユーザーアカウントを追加または編集するグループを選択します。ユーザーアカウントをグループから削除するには、グループ名の横にあるチェックボックスをオフにします。
   - ユーザープロパティ：次のいずれかを行います：
     - 変更するユーザープロパティごとに、プロパティを選択して変更を加えます。［完了］をクリックして変更した項目を保存するか、［キャンセル］をクリックして項目を変更せずそのままにします。
     - 追加するユーザープロパティごとに、［追加］をクリックして以下の操作を行います：
       * ユーザープロパティ：ドロップダウンリストからプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
       * ［完了］をクリックしてユーザープロパティを保存するか、［キャンセル］をクリックします。
     - 削除する既存のユーザープロパティごとに、プロパティが含まれる行の上にマウスポインターを置き、右側の ［**X**］をクリックします。プロパティがすぐに削除されます。

3. ［保存］をクリックして変更を保存するか、［キャンセル］をクリックしてユーザーを変更せずそのままにします。

ローカルユーザーアカウントのロックを解除するには

ローカルユーザーアカウントは、次のサーバープロパティに従ってロックされます:

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  詳しくは、「サーバープロパティ定義」を参照してください。

ローカルユーザーアカウントがロックされた場合、Citrix Endpoint Management コンソールからアカウントのロックを解除できます。

1. [ユーザー] ページのユーザーアカウント一覧で、ユーザーアカウントをクリックして選択します。
2. [ユーザーのロック解除] をクリックします。確認ダイアログボックスが開きます。
3. [ロック解除] をクリックしてユーザーアカウントのロックを解除するか、[キャンセル] をクリックしてユーザーを変更しないままにします。

Citrix Endpoint Management コンソールから Active Directory ユーザーのロックを解除することはできません。ロックされた Active Directory ユーザーは、パスワードのリセットについて Active Directory ヘルプデスクに連絡する必要があります。

ローカルユーザーアカウントを削除するには

1. [ユーザー] ページのユーザーアカウント一覧で、ユーザーアカウントをクリックして選択します。

   各ユーザーアカウントの横のチェックボックスをオンにして、削除するユーザーアカウントを複数選択できます。
2. [削除] をクリックします。確認ダイアログボックスが開きます。
3. [削除] をクリックしてユーザーアカウントを削除するか、[キャンセル] をクリックします。

Active Directory ユーザーを削除するには

一度に 1 人または複数の Active Directory ユーザーを削除するには、該当するユーザーを選択して [削除] をクリックします。

削除したユーザーがデバイスを登録していて、これらのデバイスを再登録する必要がある場合、再登録前に対象のデバイスを削除してください。デバイスを削除するには、[管理] **>** [デバイス] の順に選択し、対象のデバイスを選択して [削除] をクリックします。

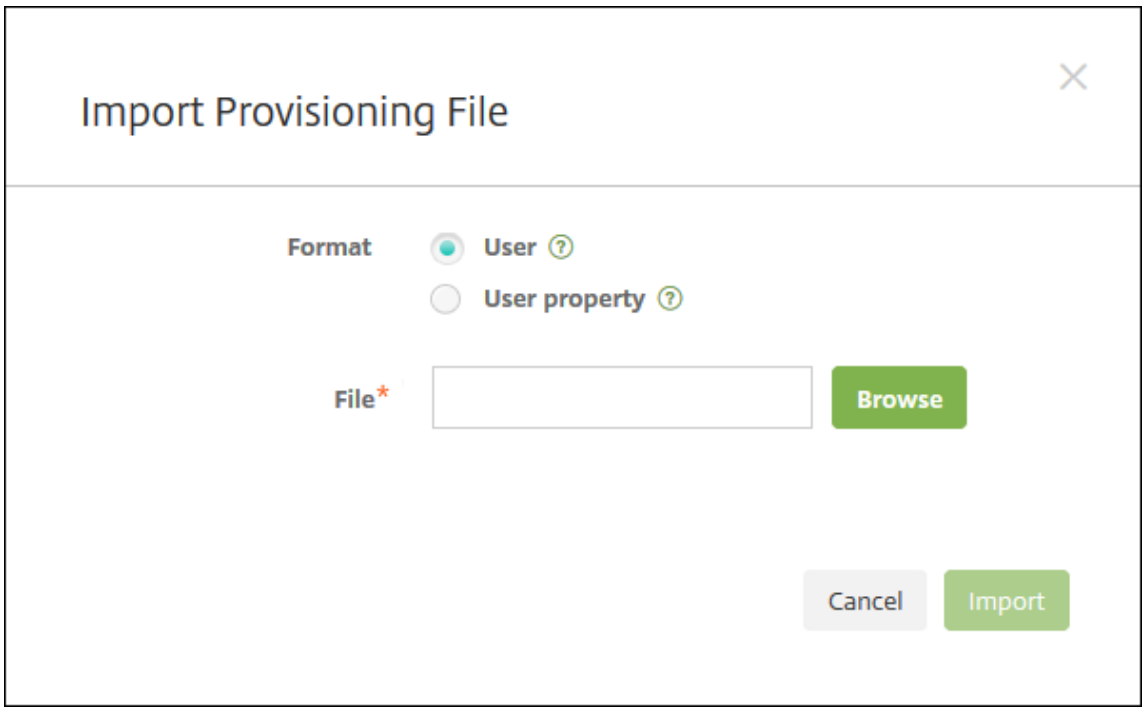
ユーザーアカウントのインポート

ローカルユーザーアカウントやプロパティを、プロビジョニングファイルと呼ばれる.csv ファイルからインポートできます。このファイルは手動で作成できます。プロビジョニングファイルの形式について詳しくは、「プロビジョニングファイル形式」を参照してください。

> 注:
>
> - ローカルユーザーの場合は、インポートファイル内のユーザー名とともにドメイン名を使用します。たとえば、`username@domain`を指定します。作成またはインポートしたローカルユーザーが Citrix Endpoint Management の管理対象ドメイン用である場合、このユーザーは対応する LDAP 資格情報を使って登録することはできません。
> - Citrix Endpoint Management の内部ユーザーディレクトリにユーザーアカウントをインポートする場合は、インポートプロセスの速度を上げるため、デフォルトのドメインを無効にします。ドメインを無効にすると登録にも影響があることに注意してください。内部ユーザーのインポートが完了した後で、デフォルトドメインを再び有効にします。
> - ローカルユーザーはユーザープリンシパル名（UPN：User Principal Name）形式で指定できます。ただし、管理対象ドメインは使用しないことをお勧めします。たとえば、example.com が管理対象である場合、「user@example.com」という UPN 形式のローカルユーザーは作成しないでください。

プロビジョニングファイルを準備した後、以下の手順に従ってファイルを Citrix Endpoint Management にインポートします。

1. Citrix Endpoint Management コンソールで、[管理] **>** [ユーザー] の順にクリックします。[ユーザー] ページが開きます。
2. [ローカルユーザーのインポート] をクリックします。[プロビジョニングファイルのインポート] ダイアログボックスが開きます。



3. インポートするプロビジョニングファイルの形式として、［ユーザー］または ［プロパティ］を選択します。
4. ［参照］をクリックして使用するプロビジョニングファイルの場所へ移動し、そのファイルを選択します。
5. ［インポート］をクリックします。

プロビジョニングファイル形式

プロビジョニングファイルを作成して、Citrix Endpoint Management へのユーザーアカウントとプロパティのインポートに使用できます。プロビジョニングファイルでは、次のいずれかの形式を使用します:

- ユーザープロビジョニングファイルのフィールド: `user;password;role;group1;group2`
- ユーザー属性プロビジョニングファイルのフィールド: `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> 注:
>
> - プロビジョニングファイル内のフィールドはセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。たとえば、プロパティ **propertyV; test;1;2** は、プロビジョニングファイルでは「**propertyV;test;1;2**」と入力します。
> - 役割として有効な値は、定義済みの役割である USER、ADMIN、SUPPORT、DEVICE_PROVISIONING のほか、ユーザーが定義した役割です。
> - グループの階層構造を作成するための区切り文字としてピリオド（.）を使用します。グループ名にピリオドは使用しないでください。

> - 属性プロビジョニングファイル内のプロパティ属性には小文字を使用してください。データベースの大文字と小文字は区別されます。

ユーザープロビジョニングファイルの内容例　エントリ「`user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01`」の意味:

- ユーザー: user01
- パスワード: pwd; 01
- 役割: USER
- グループ:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

別の例「`AUser0;1.password;USER;ActiveDirectory.test.net`」の意味:

- ユーザー: AUser0
- パスワード: 1.password
- 役割: USER
- グループ: ActiveDirectory.test.net

ユーザー属性プロビジョニングファイルの内容例　エントリ「`user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value`」の意味:

- ユーザー: user01
- プロパティ **1**:
  - 名前: propertyN
  - 値: propertyV;test;1;2
- プロパティ **2**:
  - 名前: prop 2
  - 値: prop2 value

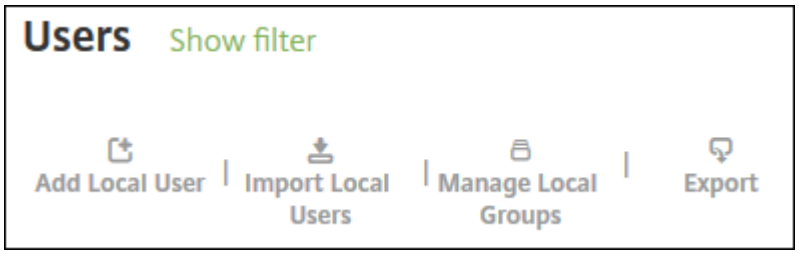
グループの追加または削除

グループの管理は、Citrix Endpoint Management コンソールの ［グループ管理］ダイアログボックスで行います: このダイアログボックスは、［ユーザー］ページ、［ローカルユーザーの追加］ページ、または ［ローカルユーザーの編集］ページからアクセスできます。グループ編集コマンドはありません。

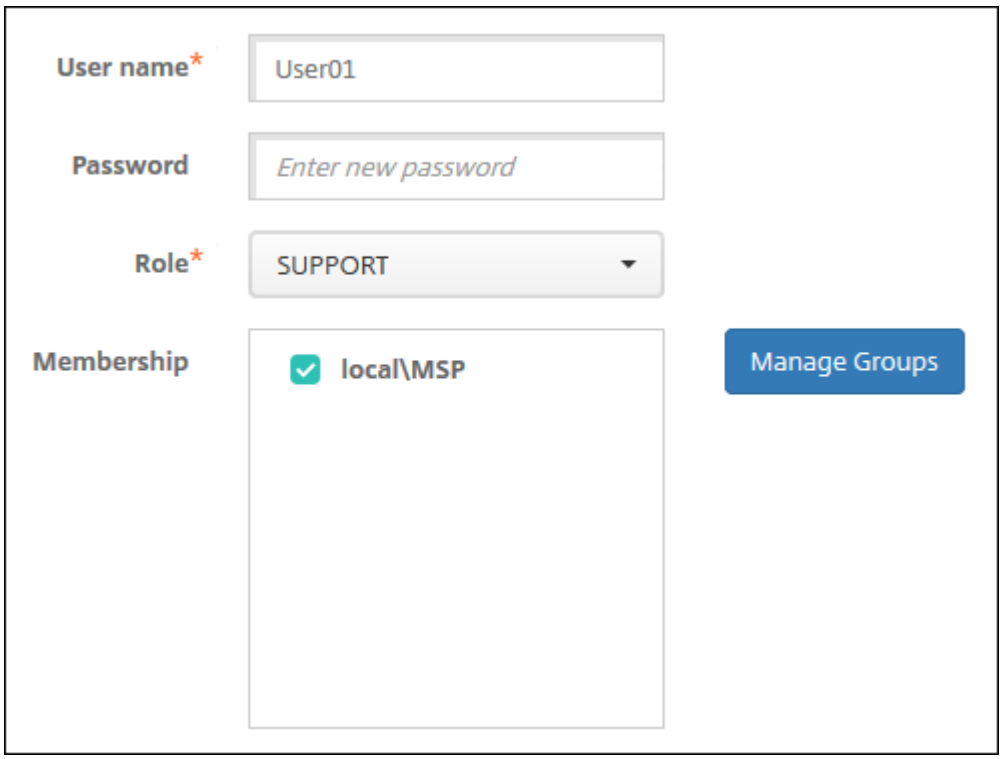
ローカルグループを追加するには

1. 次のいずれかを行います：

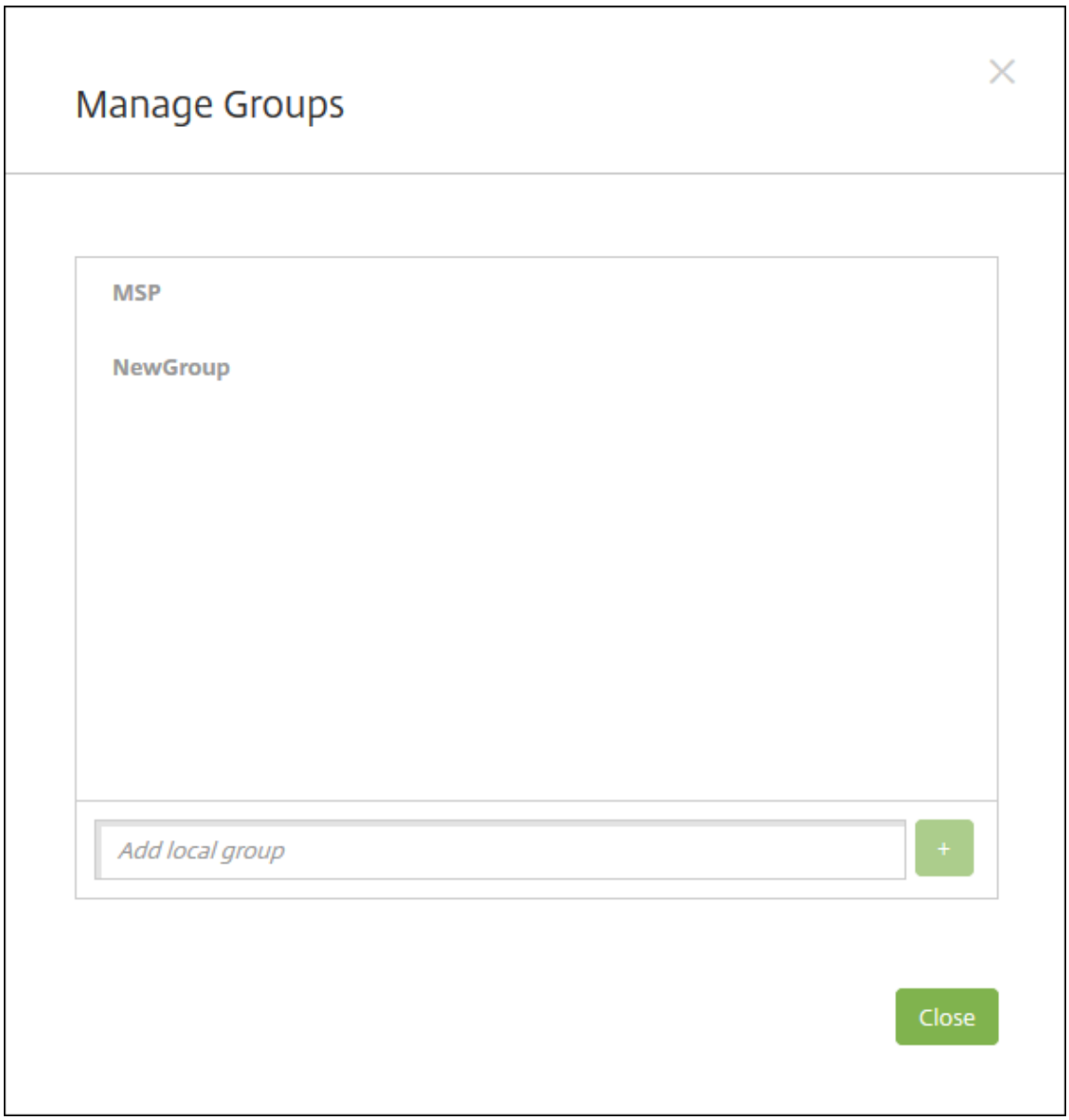
   - ［ユーザー］ページで、［ローカルグループの管理］をクリックします。



   - ［ローカルユーザーの追加］ページまたは［ローカルユーザーの編集］ページで、［グループの管理］をクリックします。



［グループ管理］ダイアログボックスが開きます。



2. グループの一覧の下で、新しいグループ名を入力してプラス記号（**+**）をクリックします。ユーザーグループが一覧に追加されます。
3. ［閉じる］をクリックします。

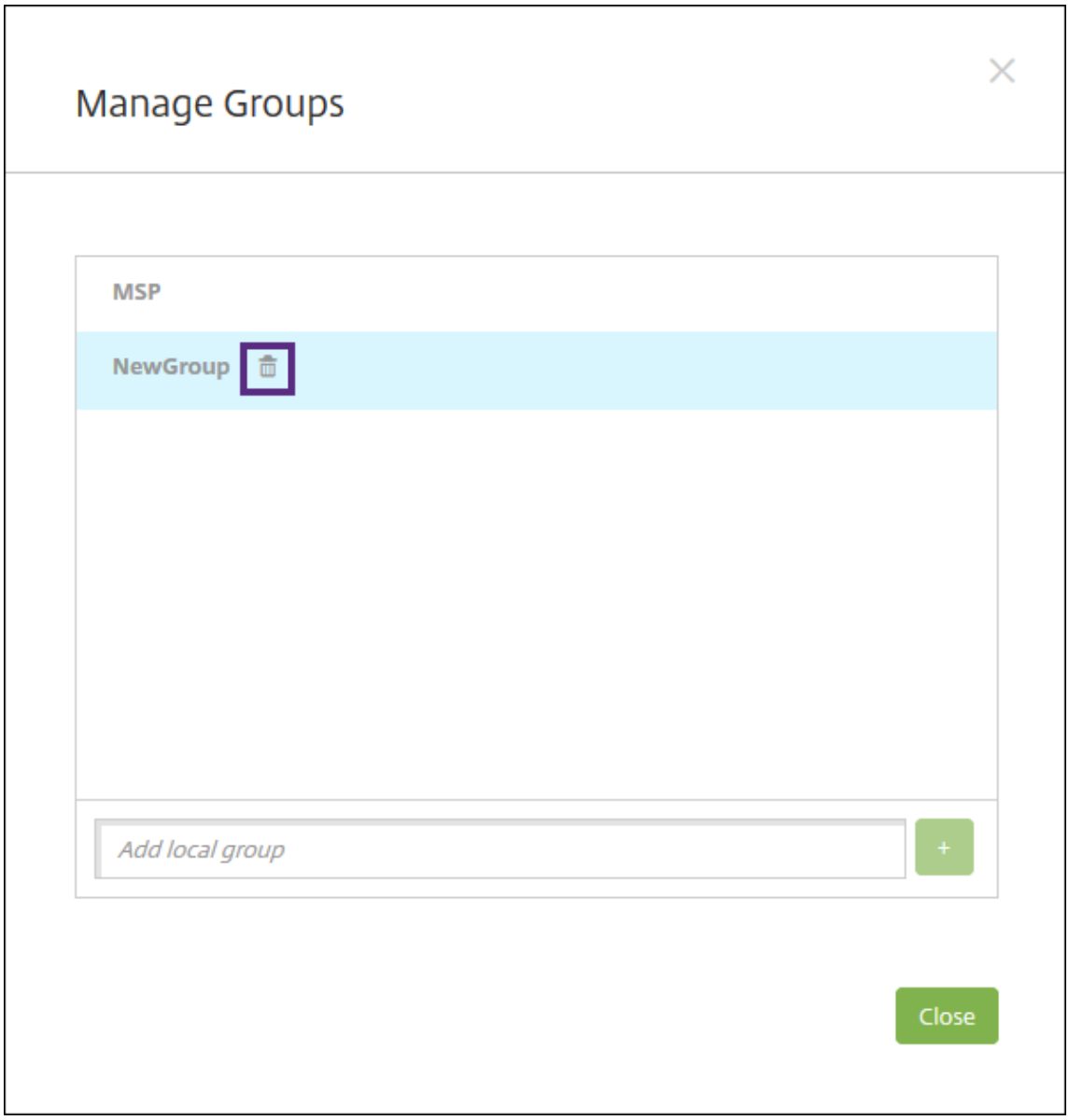
グループを削除するには

グループを削除してもユーザーアカウントには影響ありません。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

1. 次のいずれかを行います：

- ［ユーザー］ページで、［ローカルグループの管理］をクリックします。
- ［ローカルユーザーの追加］ページまたは［ローカルユーザーの編集］ページで、［グループの管理］をクリックします。

［グループ管理］ダイアログボックスが開きます。



2. ［グループ管理］ダイアログボックスで、削除するグループを選択します。
3. グループ名の右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。
4. ［削除］をクリックして操作を確認し、グループを削除します。

> 重要：
>
> この操作を元に戻すことはできません。

5. ［グループ管理］ダイアログボックスで、［閉じる］をクリックします。

ワークフローの作成および管理

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを作成する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認します。

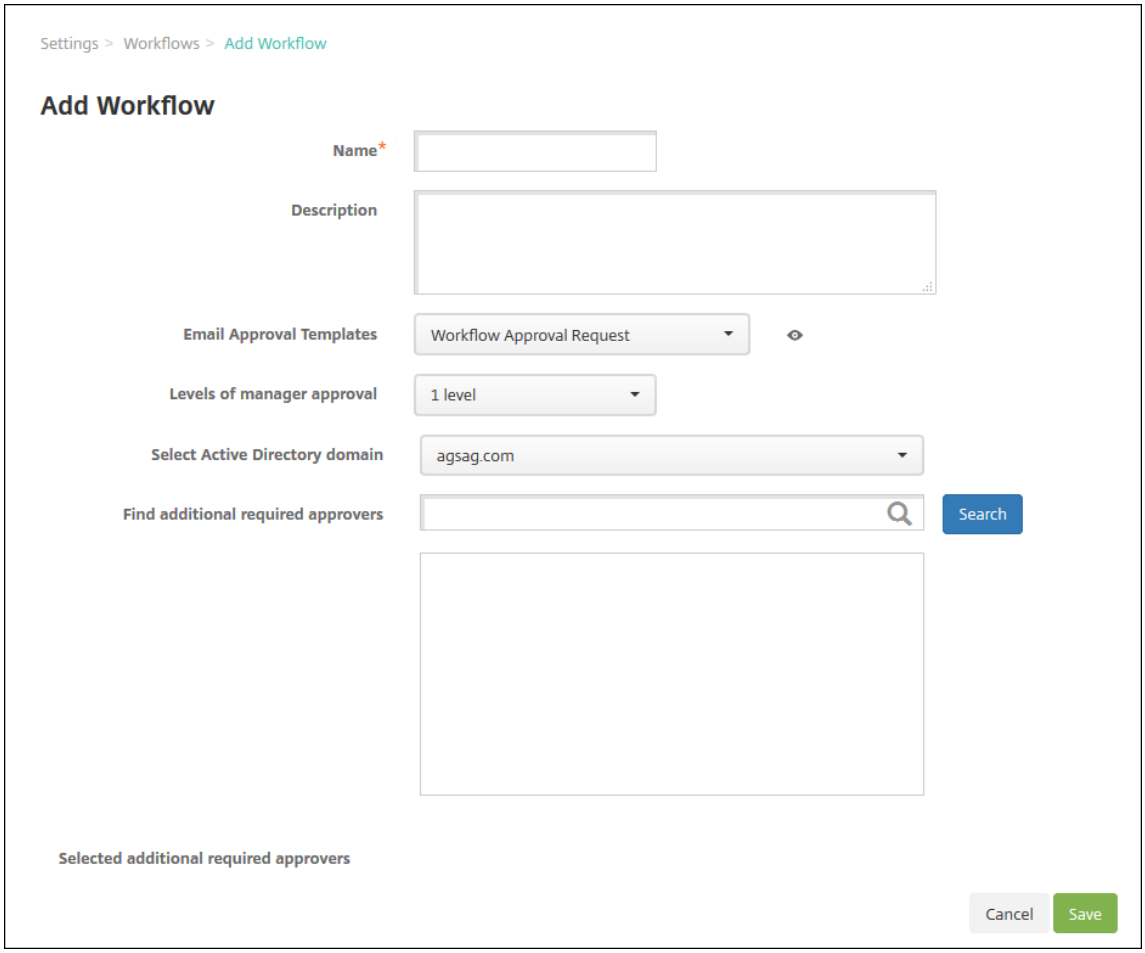
Citrix Endpoint Management を初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

Citrix Endpoint Management の次の 2 つの方法でワークフローを構成できます:

- Citrix Endpoint Management コンソールの ［設定］**>** ［ワークフロー］ページ。［ワークフロー］ページでは、アプリの構成で使用する複数のワークフローを構成できます。［ワークフロー］ページでワークフローを構成するとき、アプリを構成するときのワークフローを選択できます。
- アプリケーションコネクタを構成するとき、アプリで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。「アプリの追加」を参照してください。

ユーザーアカウントの管理者承認を最大 3 レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、名前またはメールアドレスでユーザーを検索して選択します。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［ワークフロー］をクリックします。［ワークフロー］ページが開きます。
3. ［追加］をクリックします。［ワークフローの追加］ページが開きます。



4. 次の設定を構成します:

   - 名前: ワークフローの固有の名前を入力します。
   - 説明: 任意で、ワークフローの説明を入力します。
   - メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。メールテンプレートの作成は、Citrix Endpoint Management コンソールの ［設定］の ［通知テンプレート］セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、構成中のテンプレートのプレビューが表示されます。
   - マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［**1** つのレベル］です。選択できるオプションは以下のとおりです:
     - 不必要
     - 1 つのレベル
     - 2 つのレベル
     - 3 つのレベル
   - **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
   - 追加の必須承認者を検索: 検索フィールドにユーザー名を入力して、［検索］をクリックします。名前は

Active Directory で取得されます。

- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］の一覧に表示されます。
  - 一覧からユーザー名を削除するには、次のいずれかの操作を行います：
    - ［検索］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して ［検索］をクリックし、検索結果を絞り込みます。
    - ［選択した追加の必須承認者］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

5. ［保存］をクリックします。作成したワークフローが ［ワークフロー］ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリを表示したり、ワークフローを削除したりできます。ワークフローを作成した後でワークフローを編集することはできません。承認レベルまたは承認者が異なるワークフローが必要な場合は、別のワークフローを作成します。

ワークフローの詳細の表示および削除を行うには

1. ［ワークフロー］ページの既存のワークフロー一覧で特定のワークフローを選択します。この選択を行うには、表の列をクリックするか、ワークフローの横にあるチェックボックスをオンにします。
2. ワークフローを削除するには、［削除］をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］をクリックします。

   > 重要：
   >
   > この操作を元に戻すことはできません。

登録プロファイル

November 29, 2023

各登録プロファイルで、次の項目が指定されます：

- Android、iOS、および Windows デバイスの場合、デバイス管理の登録オプション。
- Android および iOS デバイスの場合、アプリ管理の登録オプション。
- その他の登録オプション：
  - ユーザーが登録できるデバイスの数を制限するかどうか。

    デバイス数の上限に達すると、デバイス登録の上限を超えたことを知らせるエラーメッセージがユーザーに通知されます。

  - ユーザーにデバイス管理の拒否を許可するかどうか。

登録プロファイルを使用すると、1 つの Citrix Endpoint Management コンソール内で複数のユースケースとデバイス移行パスを組み合わせることができます。次のようなユースケースがあります:

- モバイルデバイス管理（MDM のみ）
- MDM+ モバイルアプリケーション管理（MAM）
- MAM のみ
- コーポレート所有端末の登録
- BYOD デバイスの登録（MDM 登録をオプトアウトできる）
- Android デバイス管理者の登録の、Android Enterprise 登録への移行（完全管理、仕事用プロファイル、専用デバイス）
- Windows 用 Citrix Workspace アプリを使用した Windows 10 および Windows 11 デバイスの自動登録（プレビュー）

現在のサイトが MDM のみで、MAM を追加する必要がある場合は、Citrix Gateway を構成する必要があります。詳しくは、「Citrix Gateway の要件」を参照してください。

デリバリーグループを作成すると、Global という名前のデフォルトの登録プロファイルを使用するか、別の登録プロファイルを指定することができます。

プラットフォームごとに、次の登録プロファイル機能があります。

- **Android** デバイスの場合：管理およびデバイス所有者モードを指定します。例：会社所有のデバイス、仕事用プロファイルで完全に管理、BYOD/仕事用プロファイル。

  新しいデバイスは、デフォルトで Android Enterprise に登録されます。従来の Android デバイス管理者（DA）モードを使用したデバイス管理を選択できます。また新しいデバイスは、デフォルトでアプリ管理に登録されます。

  セキュリティレベルの指定および必要な登録手順については、「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。

- **iOS** デバイスの場合：デバイスの管理の種類（**Apple** ユーザー登録、**Apple** デバイスの登録、またはデバイスを管理しない）を指定します。この **Apple** ユーザー登録モードは、公開プレビューとして使用できます。この機能を有効にするには、サポートチームにお問い合わせください。

  Apple ユーザー登録を選択した場合、管理対象 Apple ID にカスタムドメインを使用してそのドメインを構成することを選択できます。

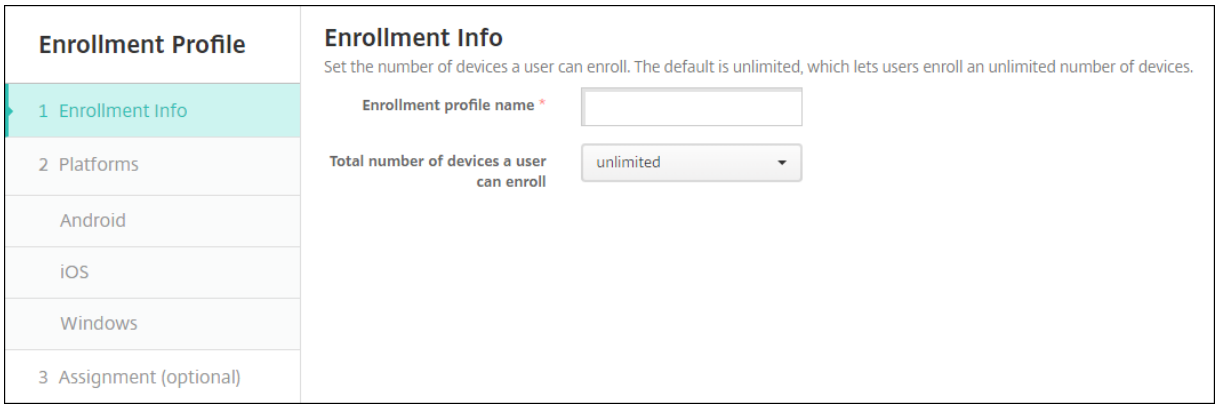
  新しいデバイスは、デフォルトで Apple デバイス管理に登録されます。また新しいデバイスは、デフォルトでアプリ管理に登録されます。

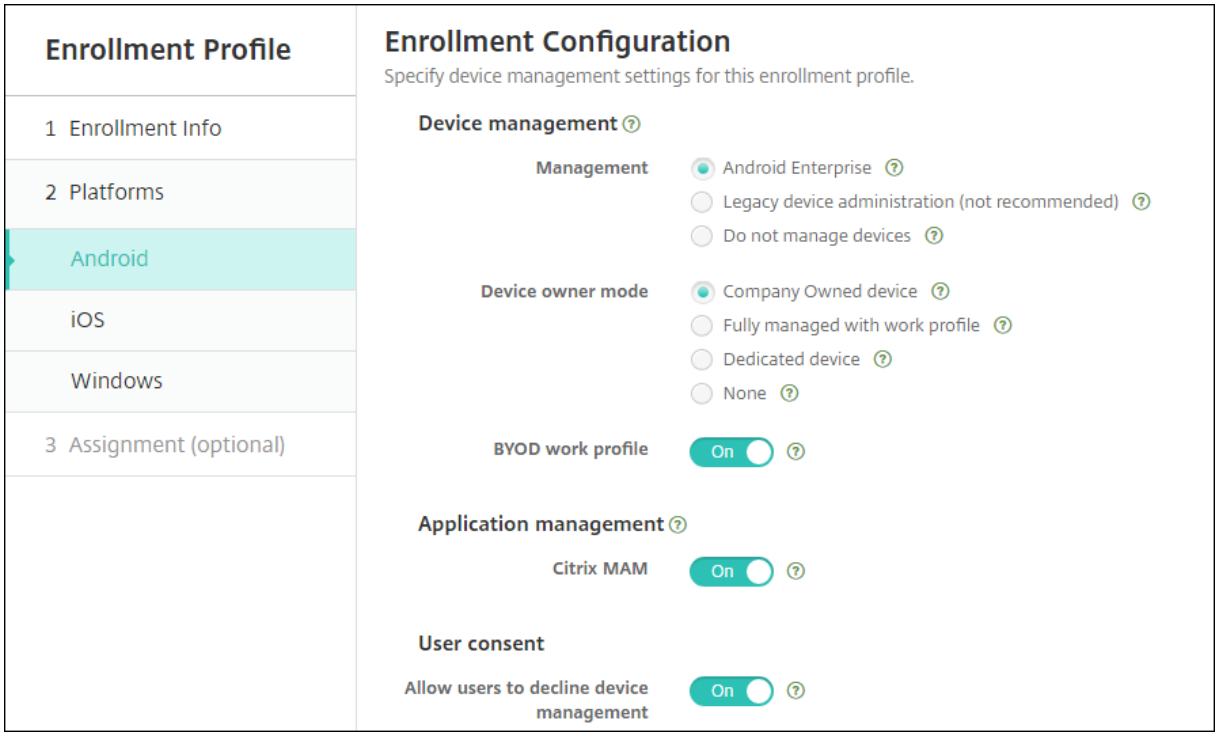
- **Windows 10** および **Windows 11** デバイスの場合： Citrix デバイス管理（Windows）を使用するかどうかを指定します。新しいデバイスは、デフォルトでデバイス管理に登録されます。

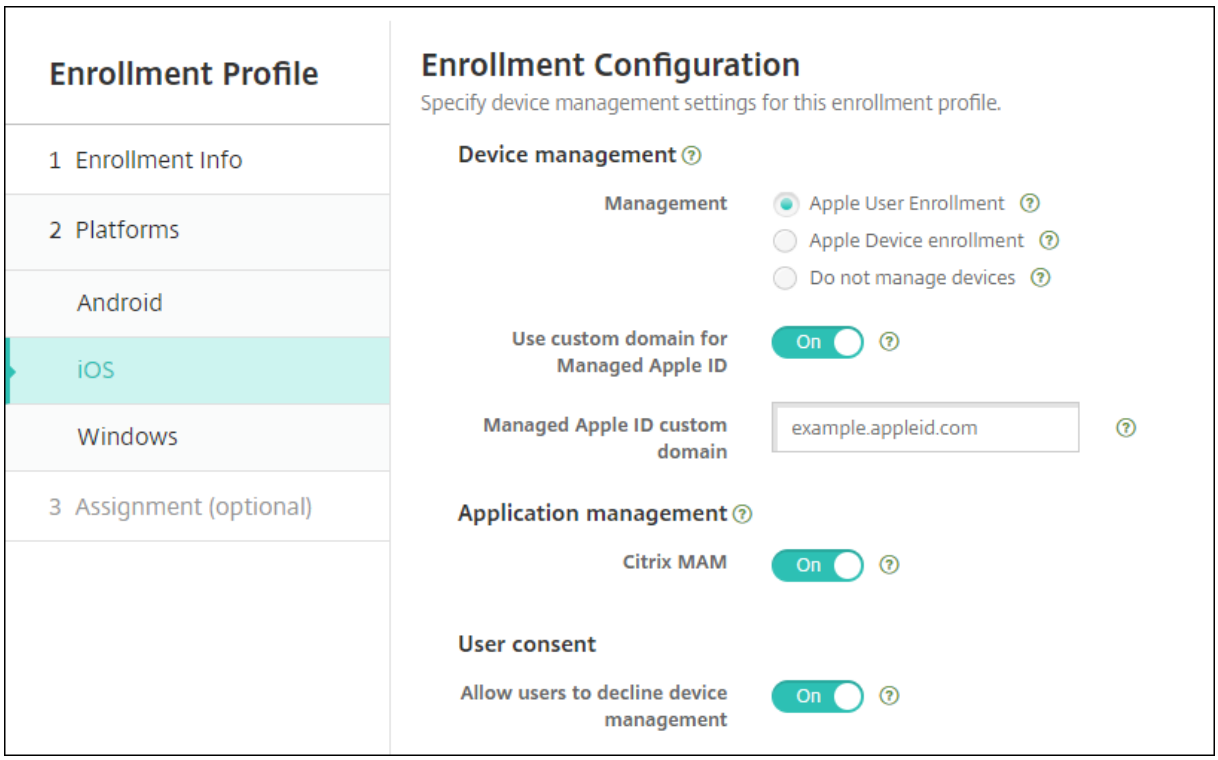
グローバル登録プロファイル

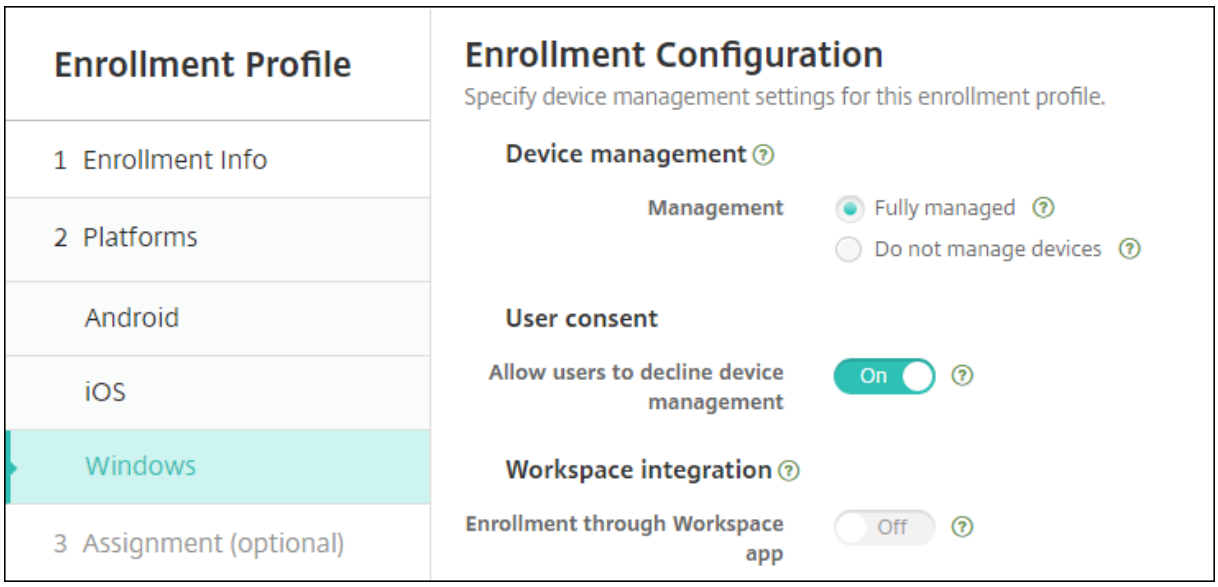
デフォルトの登録プロファイル名は Global です。グローバルプロファイルは、登録プロファイルを作成するまでテストに使用できます。

Citrix Endpoint Management 20.2.1 以降にオンボードした場合、グローバル登録プロファイルは事前に定義されています。次のスクリーンショットは、グローバル登録プロファイルのデフォルト設定を示しています。MAM のみの展開では、これらのオプションのサブセットが表示されます。









登録プロファイル、デリバリーグループ、登録

登録プロファイルとデリバリーグループは、次のように相互に作用します:

- 登録プロファイルは、1 つまたは複数のデリバリーグループに添付できます。
- 異なる登録プロファイルを持つ複数のデリバリーグループにユーザーが属している場合、デリバリーグループの名前によって、使用される登録プロファイルが決まります。Citrix Endpoint Management は、デリバリ

ーグループのアルファベット順一覧の最後に表示されるデリバリーグループを選択します。たとえば、次のような場合を想定します:

- 「EP1」と「EP2」という名前の、2 つの登録プロファイルがあります。
- 「DG1」と「DG2」という名前の、2 つのデリバリーグループがあります。
- 「DG1」は「EP1」に関連付けられています。
- 「DG2」は「EP2」に関連付けられています。

登録するユーザーが「DG1」と「DG2」の両方のデリバリーグループに属する場合、Citrix Endpoint Management は、「EP2」の登録プロファイルを使用してこのユーザーの登録の種類を決定します。

- 展開順は、MDM（デバイス管理）用に構成された登録プロファイルを持つデリバリーグループ内のデバイスにのみ適用されます。
- デバイス登録後、登録プロファイルに対して次の変更を行った場合は、再登録が必要になります:
  - デバイスを「MDM+MAM」から「MAM」または「MDM」登録にダウングレードするように設定を変更した場合。ダウングレードは、登録プロファイルを更新した場合や、デバイスを別のデリバリーグループに移動した場合に発生することがあります。
  - MDM 用に構成された登録プロファイルに MAM を追加した場合。
  - MAM 用に構成された登録プロファイルに MDM を追加した場合。
- 別の登録プロファイルに切り替えても、既存の登録済みデバイスには影響しません。ただし、変更を有効にするには、ユーザーはそれらのデバイスの登録を解除してから再登録する必要があります。

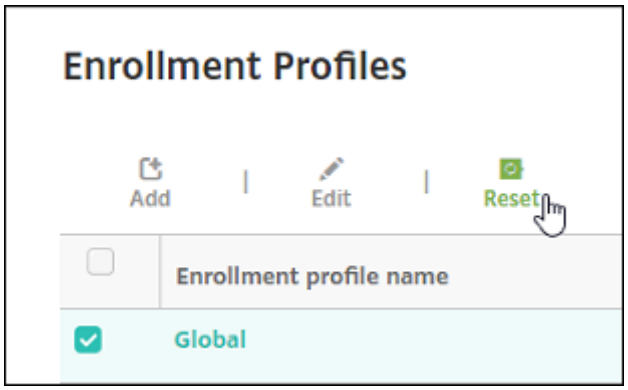
登録プロファイルの作成

1. Citrix Endpoint Management コンソールで、［構成］**>**［登録プロファイル］の順に移動します。
2. ［登録情報］ページで、プロファイルのわかりやすい名前を入力します。デフォルトでは、1 人のユーザーは無数のデバイスを登録できます。ユーザーごとのデバイスの数を制限するには、値を選択します。この制限は、ユーザーが登録する MAM または MDM 管理対象の Android、iOS、および Windows デバイスの合計数に適用されます。
3. プラットフォームページの入力を完了します。各プラットフォーム固有の登録設定については、以下を参照してください:
   - Android Enterprise: 登録プロファイルの作成
   - iOS: サポートされている登録方法
   - Windows デスクトップとタブレット: サポートされている登録方法
4. ［割り当て］ページで、1 つまたは複数のデリバリーグループを登録プロファイルに添付します。

   1 人のユーザーが、異なる登録プロファイルを持つ複数のデリバリーグループに属する場合があります。そのような場合には、デリバリーグループの名前によって使用する登録プロファイルが決まります。Citrix

Endpoint Management は、デリバリーグループのアルファベット順一覧の最後に表示されるデリバリーグループを選択します。デリバリーグループを作成するには、［構成］**>**［デリバリーグループ］の順に移動します。

登録プロファイルの一覧を表示するには、［構成］**>**［登録プロファイル］ページに移動します。Global プロファイルを編集する場合、または Global プロファイルを元のデフォルトの状態にリセットする場合は、Global プロファイルの行を選択して ［リセット］をクリックします。Global プロファイルを削除することはできません。



通知

November 29, 2023

Citrix Endpoint Management での通知は以下の目的で利用できます:

- 多くのシステム関連機能に関して、選択したグループのユーザーに連絡します。また、これらの通知の対象を特定のユーザーにすることもできます。たとえば、iOS デバイスを持つすべてのユーザー、コンプライアンスを満たしていないデバイスのユーザー、個人所有のデバイスを持つユーザーなどです。
- ユーザーとデバイスを登録します。
- 特定の条件が満たされたときに（自動化された操作を使用して）ユーザーに自動的に通知します。例:
  - コンプライアンスの問題により、ユーザーデバイスが企業ドメインからブロックされようとしているとき
  - デバイスがジェイルブレイクされたり Roote 化されたりした場合

自動化された操作について詳しくは、「自動化された操作」を参照してください。

Citrix Endpoint Management で通知を送信するには、ゲートウェイおよび通知サーバーを構成する必要があります。Citrix Endpoint Management で通知サーバーをセットアップして SMTP サーバーを構成できます。これらのサーバーは、ユーザーにメール通知を送信します。通知では、SMTP 経由でメッセージを送信できます。

- SMTP は、メール送信者がメール受信者と通信する、コネクション型のテキストベースプロトコルです。メール送信者は、通常 TCP 接続によってコマンド文字列を発行し、必要なデータを提供します。SMTP セッショ

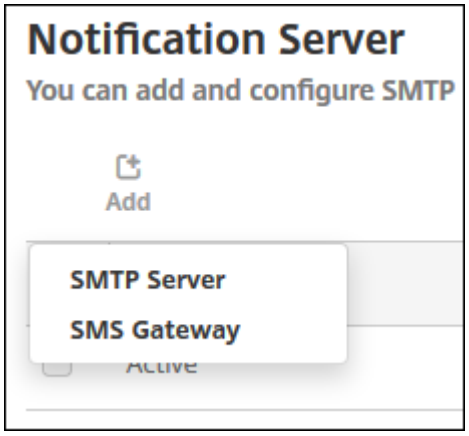
ンは、SMTP クライアント（メッセージの送信者）から送信されたコマンドと、コマンドに対応する、SMTP サーバーからの応答によって構成されます。

前提条件

- メッセージをユーザーに送信するための SMTP 通知サーバーを構成してください。サーバーが社内サーバーでホストされている場合は、システム管理者に構成情報を問い合わせてください。サーバーが、ホストされている電子メールサービスの場合は、サービスプロバイダーの Web サイトで適切な構成情報を確認してください。
- アクティブな SMTP サーバーは 1 つだけ使用できます。この通信チャネルでは、アクティブな構成が 1 つだけ可能です。
- ネットワークの DMZ 内の Citrix Endpoint Management からポート 25 を開き、内部ネットワークの SMTP サーバーにポイントバックしてください。これにより、Citrix Endpoint Management は通知を正常に送信できます。

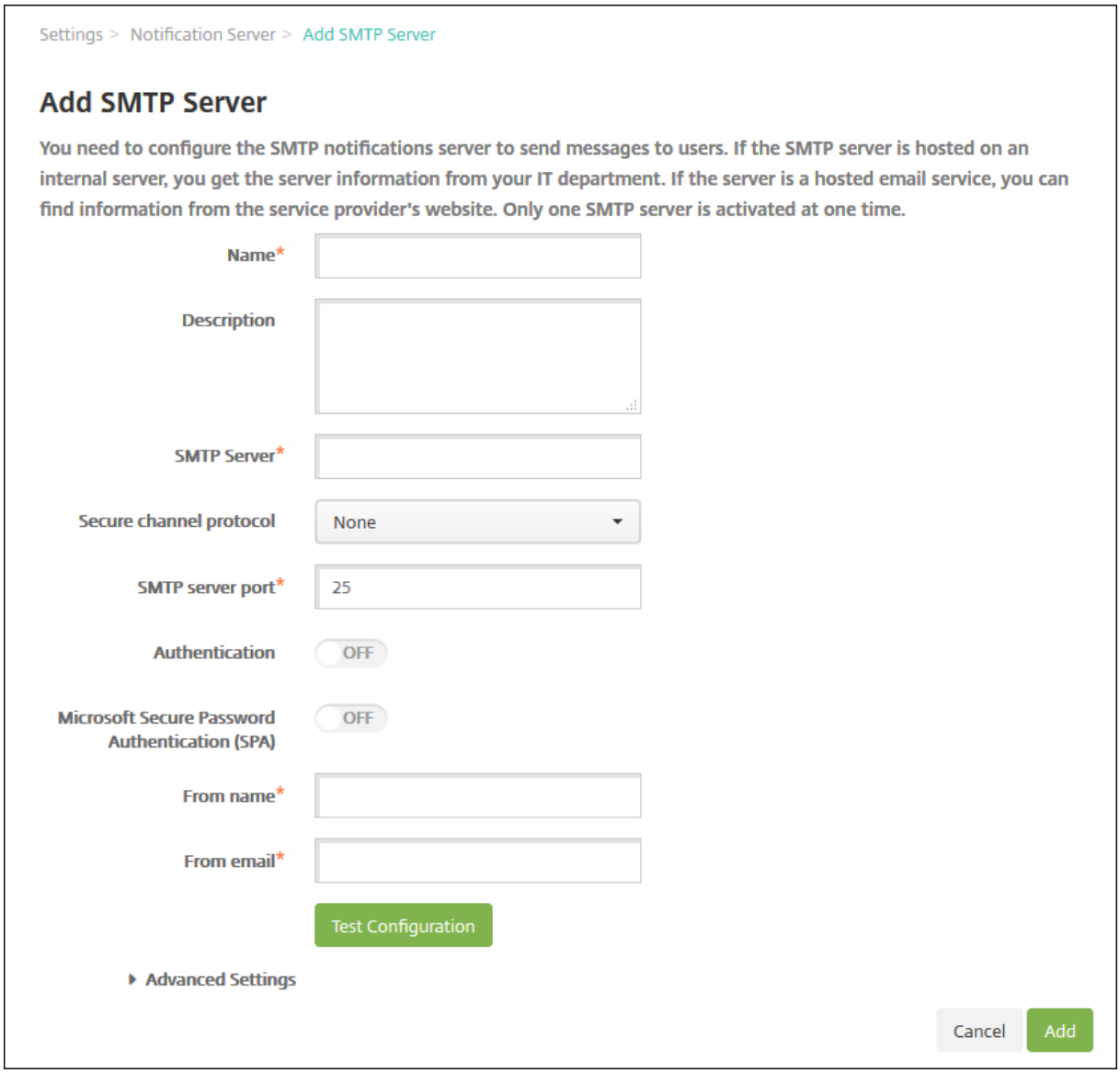
SMTP サーバーの構成

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［通知］の下の ［通知サーバー］をクリックします。［通知サーバー］ページが開きます。
3. ［追加］をクリックします。SMTP サーバーを構成するためのオプションが含まれたメニューが開きます。



   - SMTP サーバーを追加するには、［**SMTP** サーバー］を選択します。この設定を構成する手順については、「SMTP サーバーの追加」を参照してください。

SMTP サーバーの追加



1. 次の設定を構成します:

   - 名前: この SMTP サーバーアカウントに関連付ける名前を入力します。
   - 説明: 任意で、サーバーの説明を入力します。
   - **SMTP** サーバー: サーバーのホスト名を入力します。完全修飾ドメイン名（FQDN）または IP を指定します。
   - セキュアチャネルプロトコル:（サーバーが安全な認証を使用するよう構成されている場合）一覧から、サーバーが使用する適切なセキュアチャネルプロトコルとして［**SSL**］、［**TLS**］、または［なし］を選択します。デフォルトは［なし］です。
   - **SMTP** サーバーポート: SMTP サーバーが使用するポートを入力します。デフォルトでは、ポートは 25 に設定されています。SMTP 接続で SSL セキュアチャネルプロトコルを使用する場合、ポートを

465 に設定します。
- 認証：［オン］または ［オフ］を選択します。デフォルトは ［オフ］です。
- ［認証］を有効にした場合は、次の設定を構成します。
  - ユーザー名：認証に使用するユーザー名を入力します。
  - パスワード：認証に使用するユーザーのパスワードを入力します。
- **Microsoft** セキュリティで保護されたパスワード認証（**SPA**）： SMTP サーバーが SPA を使用している場合は、［オン］をクリックします。デフォルトは ［オフ］です。
- 送信名：クライアントがこのサーバーから通知メールを受信したとき、メールの送信者として表示される名前を入力します。たとえば、「Corporate IT」です。
- 送信メールアドレス： SMTP サーバーによって送信された通知に、メール受信者が返信する場合に使用されるメールアドレスを入力します。

2. ［構成のテスト］をクリックして、テストのメール通知を送信します。
3. ［詳細設定］を展開して以下の設定を構成します。
   - **SMTP** 再試行数： SMTP サーバーからのメッセージの送信が失敗した場合に再試行する回数を入力します。デフォルトは 5 です。
   - **SMTP** タイムアウト： SMTP 要求送信時に待機する時間（秒）を入力します。送信しているメッセージが、タイムアウトで失敗し続ける場合には、この値を大きくします。この値を小さくするとタイムアウト回数が多くなり、配信されないメッセージが増える場合があるため、注意してください。デフォルトは 30 秒です。
   - 最大 **SMTP** 受信者数： SMTP サーバーによって送信される各電子メールメッセージの最大受信者数を入力します。デフォルトは 100 です。
4. ［追加］をクリックします。

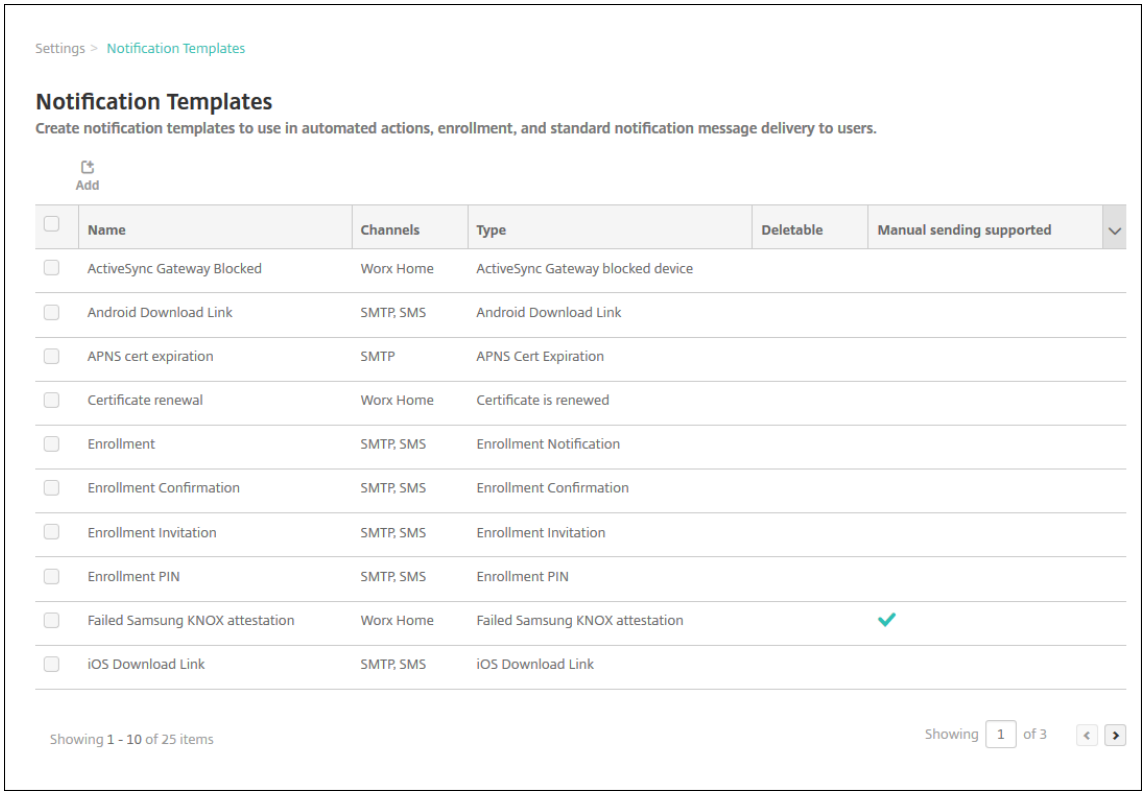
通知テンプレートの作成および更新

Citrix Endpoint Management で通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Citrix Secure Hub または SMTP の 2 つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。

Citrix Endpoint Management には定義済みの通知テンプレートが多数用意されています。このテンプレートには、システム内のすべてのデバイスに対して Citrix Endpoint Management が自動的に応答する個別の種類のイベントが反映されています。

> 注：
>
> SMTP チャネルを使用してユーザーに通知を送信する場合は、アクティブ化する前にチャネルを設定する必要があります。通知テンプレートを追加するときにチャネルがまだ設定されていないと、チャネルを設定するよう求めるメッセージが表示されます。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［通知テンプレート］をクリックします。［通知テンプレート］ページが開きます。



通知テンプレートの追加

1. ［追加］をクリックします。SMTP サーバーが設定されていない場合、SMTP 通知に関するメッセージが表示されます。SMTP サーバーを今すぐ設定するか後で設定するかを選択できます。

   SMTP サーバーを今すぐ設定することを選択した場合は、［設定］ページの ［通知サーバー］ページにリダイレクトされます。使用するチャネルを設定した後、［通知テンプレート］ページに戻って、通知テンプレートの追加または変更を続けることができます。

   > 重要：
   >
   > SMTP サーバーの設定をあとからセットアップすることを選択した場合、通知テンプレートを追加または編集するときにこれらのチャネルをアクティブ化することができません。つまり、これらのチャネルをユーザー通知の送信に利用することができません。

2. 次の設定を構成します：

   - 名前：テンプレートの説明的な名前を入力します。
   - 説明：テンプレートの説明を入力します。

- 種類：一覧から、通知の種類を選択します。選択した種類でサポートされるチャネルのみが表示されます。定義済みテンプレートである［APNs 証明書の有効期限］テンプレートは 1 つだけ使用できます。この種類のテンプレートは追加できません。

> 注：
>
> 一部のテンプレートの種類では、種類の下に［マニュアル送信がサポートされています］が表示されます。これらのテンプレートの種類は、［ダッシュボード］および［デバイス］ページの［通知］一覧で選択できます。これらの場所から、手動でユーザーに通知を送信できます。いずれのチャネルの場合も、［件名］フィールドまたは［メッセージ］フィールドに以下のマクロが使われているテンプレートでは、手動送信は使用できません。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

> 注：
>
> Citrix Endpoint Management コンソールには、「ブラックリスト」、「ホワイトリスト」という用語が含まれています。これらの用語は、今後のリリースで「禁止リスト」、「許可リスト」に変更されます。

3. ［チャネル］で、この通知で使用される各チャネルの情報を構成します。一部またはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。

   - ［**Citrix Secure Hub**］を選択した場合、iOS デバイスおよび Android デバイスのみが通知を受信し、通知はデバイスの通知トレイに表示されます。
   - ［**SMTP**］を選択した場合、メールアドレスを使って登録したユーザーがメッセージを受信します。

   Citrix Secure Hub:

   - アクティブ化：クリックして通知チャネルを有効にします。
   - メッセージ：ユーザーに送信されるメッセージを入力します。Citrix Secure Hub を使用する場合、このフィールドは必須です。メッセージでのマクロの使用について詳しくは、「マクロ」を参照してください。
   - 音声ファイル：一覧から、ユーザーが通知を受信したときに再生される通知音を選択します。

   SMTP:

   - アクティブ化：クリックして通知チャネルを有効にします。

     SMTP サーバーをセットアップした後でのみ、SMTP 通知をアクティブ化できます。

   - 差出人：任意で、通知の送信者（名前、メールアドレス、またはその両方）を入力します。
   - 受信者：このフィールドには、アドホック通知を除くすべての通知で、通知が正しい SMTP 受信者アドレスに送信されるようにするためのマクロが事前設定されています。テンプレートのマクロは変更しないでください。このフィールドにアドレスを追加することで、さらに受信者（社内の管理者など）を追

加することができます。マクロとアドレスは、セミコロン（;）で区切ります。アドホック通知を送信するには、個別に受信者を入力するか、［管理］**>**［デバイス］ページでデバイスを選択して、そこから通知を送信します。詳しくは、「デバイス」を参照してください。

- 件名：通知の説明的な件名を入力します。このフィールドは必須です。
- メッセージ：ユーザーに送信されるメッセージを入力します。メッセージでのマクロの使用について詳しくは、「マクロ」を参照してください。

4. ［追加］をクリックします。すべてのチャネルが正しく構成されている場合、［通知テンプレート］ページに、SMTP、Citrix Secure Hub の順に表示されます。正しく構成されていないチャネルがあれば、正しく構成されているチャネルの後に表示されます。

通知テンプレートの編集

1. 通知テンプレートを選択します。そのテンプレートの編集ページが表示されます。テンプレートで ［種類］フィールド以外を編集したり、チャネルをアクティブまたは非アクティブにしたりできます。
2. ［保存］をクリックします。

通知テンプレートの削除

追加した通知テンプレートのみを削除できます。事前定義済みの通知テンプレートは削除できません。

1. 既存の通知テンプレートを選択します。
2. ［削除］をクリックします。確認ダイアログボックスが開きます。
3. ［削除］をクリックして通知テンプレートを削除するか、［キャンセル］をクリックして通知テンプレートの削除を取り消します。

RBAC を使用した役割の構成

March 15, 2024

Citrix Endpoint Management の役割ベースのアクセス制御（Role-Based Access Control：RBAC）機能を使用して、役割をユーザーとグループに割り当てることができます。役割は、システム機能に対するユーザーのアクセスレベルを制御する権限のセットです。

Citrix Endpoint Management には、デフォルトで次のユーザー役割があります。自身のユーザー役割を作成するためにカスタマイズして使うテンプレートとして、デフォルトの役割を使用できます。

- 管理者：システムへのフルアクセスが許可されます。

- ユーザー：デバイスの登録と、Self Help Portal へのアクセスをユーザーに許可します。

Citrix Endpoint Management の RBAC 機能を使用すると、次のことを実行できます：

- ユーザー役割を作成および編集する。
- 役割をローカルユーザーグループと Active Directory（AD）グループに割り当てる。
- Citrix Cloud の［**ID** およびアクセス管理］**>**［管理者］で役割を管理者に割り当てる。「Citrix Cloud 管理者に役割を追加する」を参照してください。

RBAC 機能の使用

ローカルユーザー、クラウド管理者（Citrix Cloud 内）、およびローカルユーザーグループと Active Directory グループに、役割を割り当てることができます。

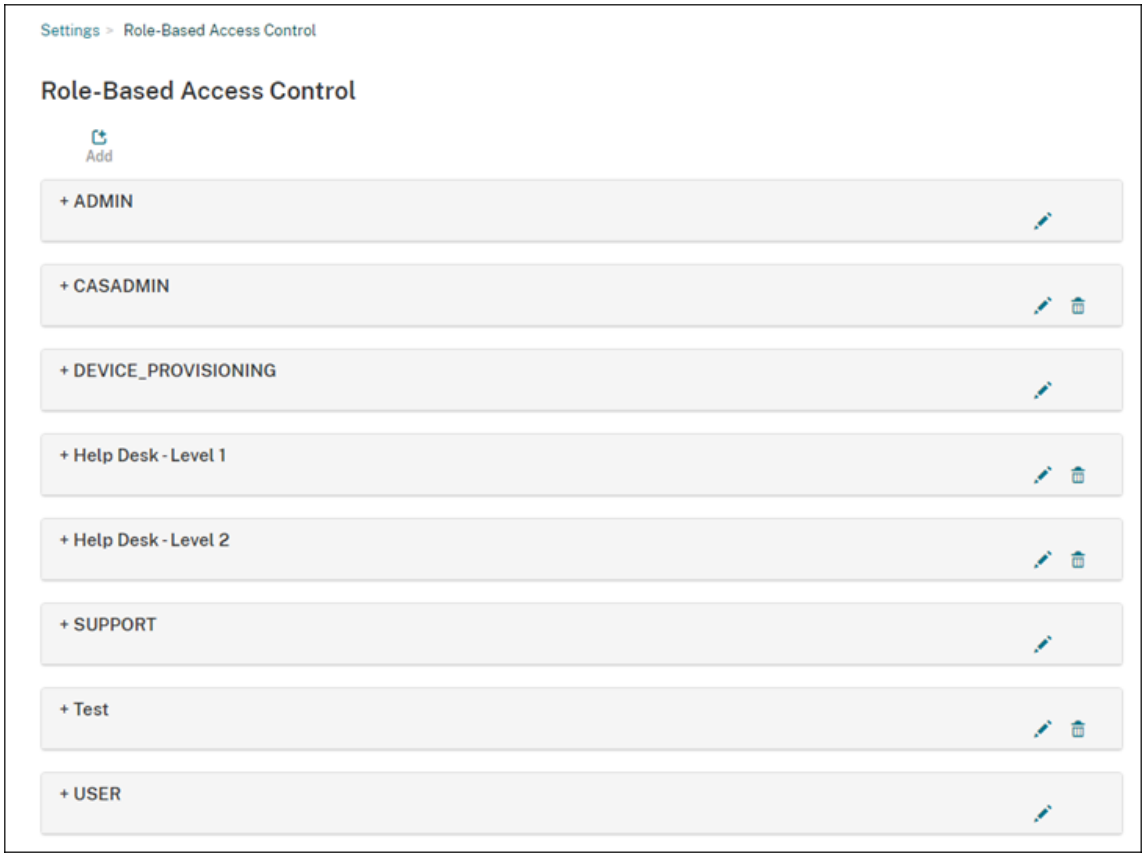
- ローカルユーザー：［管理］**>**［ユーザー］を使用して、ローカルユーザーに役割を割り当てます。ローカルユーザーに割り当てることができる役割は 1 つだけです。役割を変更するため、手作業でユーザーアカウントを編集できます。または、ローカルユーザー用のグループを作成し、そのグループに役割を割り当てることができます。
- クラウド管理者：クラウド管理者は、管理者が Citrix Cloud 顧客アカウントに追加されるときに Citrix Cloud によって作成される、特別なユーザーアカウントです。クラウド管理者アカウントは、Citrix Cloud の管理者アカウントと同じユーザー名を使用します。Citrix Endpoint Management コンソールで RBAC の役割を作成し、Citrix Cloud の［**ID** およびアクセス管理］**>**［管理者］でこれらのユーザーに役割を割り当てます。
- **Active Directory** グループ： Active Directory グループのすべてのユーザーは同じ権限を持っています。ユーザーが複数の Active Directory グループに属している場合は、すべての権限がマージされてそのユーザーの権限が定義されます。たとえば、ADGroupA ユーザーはマネージャーのデバイスを見つけることができ、ADGroupB ユーザーは従業員のデバイスをワイプできるとします。両方のグループに属するユーザーは、マネージャーのデバイスと従業員のデバイスを見つけてワイプできます。ユーザーが競合する権限を持つグループに属している場合、許可されたアクセス権限が優先されます。

詳しくは、「ユーザーアカウントについて」を参照してください。

役割を作成または編集する

1. Citrix Endpoint Management コンソールで、［設定］ページにアクセスし、右上隅の歯車アイコンをクリックします。
2. ［役割ベースのアクセス制御］をクリックします。［役割ベースのアクセス制御］ページには、デフォルトのユーザー役割と、追加した役割が表示されます。

   役割の横にあるプラス記号（+）をクリックすると、その役割のすべての権限を表示できます。



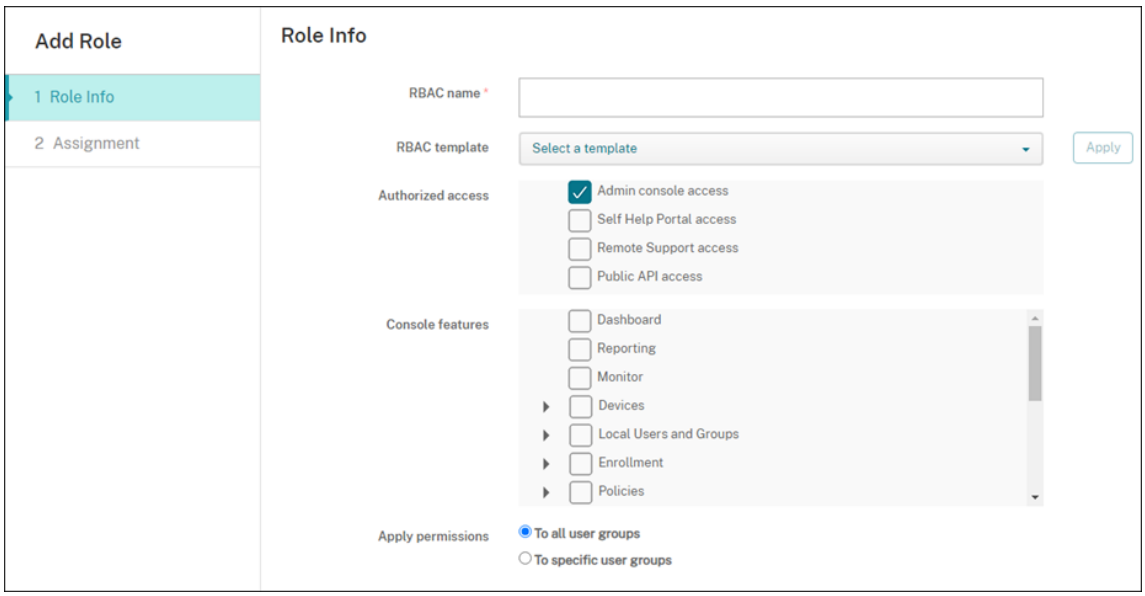
3. 役割を追加するには、[追加] をクリックします。または、役割を編集するには、既存の役割の右側にあるペンをクリックします。

   > 注:
   >
   > 定義した役割の右側にあるゴミ箱アイコンをクリックすると、役割を削除できます。デフォルトのユーザー役割を削除することはできません。

4. [役割の追加] ページで、次の情報を入力します:

   - **RBAC** 名: 新しいユーザー役割の説明的な名前を入力します。既存の役割の名前は変更できません。
   - **RBAC** テンプレート: 任意で、新しい役割の開始点とするテンプレートを選択します (役割を編集するときに、テンプレートを選択または変更することはできません)。RBAC テンプレートは、システム機能へのアクセスを定義するデフォルトのユーザー役割です。

   [適用] ボタンをクリックして、[承認済みアクセス] および [コンソールの機能] にあるチェックボックスに反映させます。Citrix Endpoint Management はこれらのフィールドに、選択したテンプレートで事前定義されているアクセス権と機能権限を設定します。



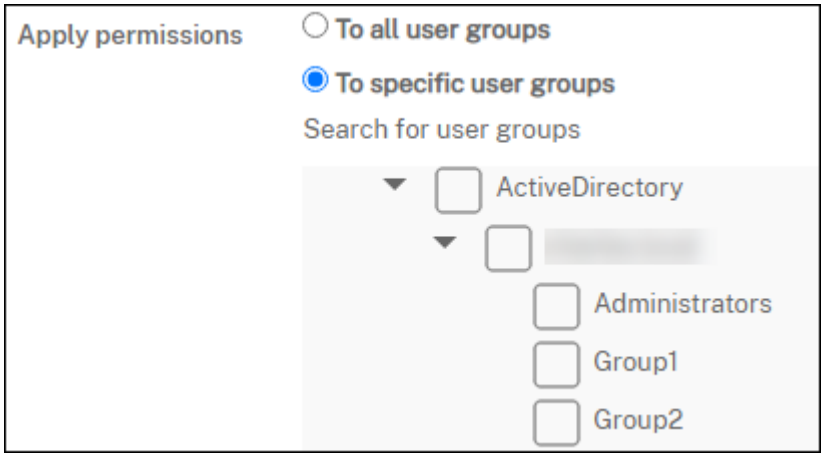
5. 役割をカスタマイズするには、［承認済みアクセス］および ［コンソールの機能］のチェックボックスをオンまたはオフにします。

   ［コンソールの機能］の横にある三角をクリックして表示された、その機能に固有の権限をオンにします。最上位レベルのチェックボックスをクリックしても、個々の権限はオンになりません。最上位レベルの権限を展開した後、個々のオプションを選択します。

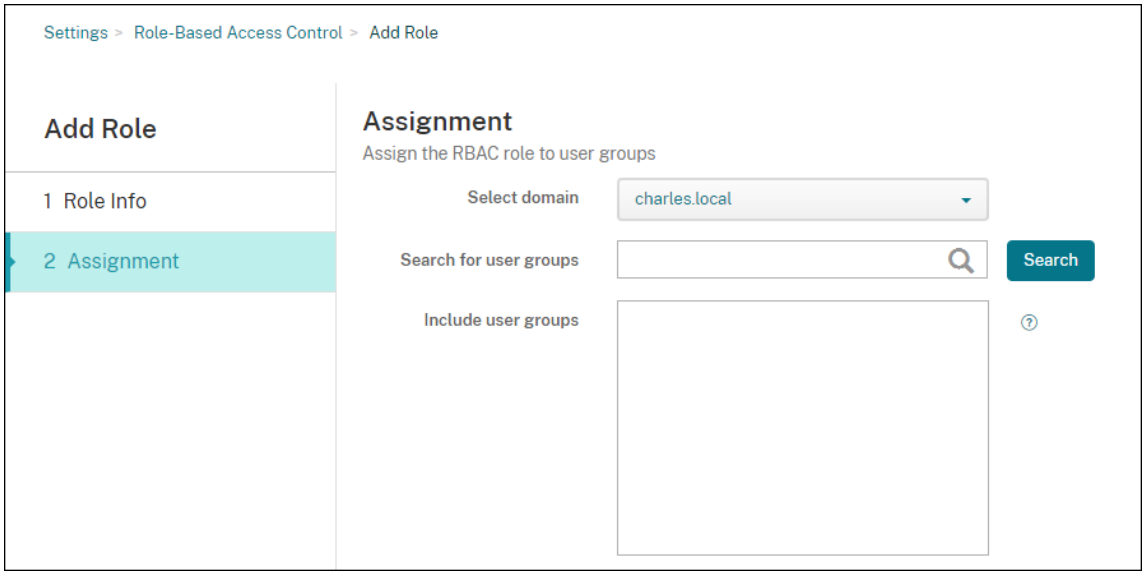
6. 権限を適用：［特定のユーザーグループ］をクリックして、選択したグループに権限を適用します。

   たとえば、RBAC 管理者が ActiveDirectory ユーザーグループに対するアクセス権限を持っている場合：

   - 管理者は、ActiveDirectory グループに属するユーザーの情報にのみアクセスできます。
   - 管理者は、他のローカルユーザーまたは AD ユーザーを表示することはできません。管理者が表示できるのは、いずれかのグループの子グループのメンバーであるユーザーです。
   - 管理者は次のグループに招待状を送ることができます：
     - 権限グループとその子グループ
     - 権限グループのメンバーであるユーザーとその子グループ



7. ［次へ］をクリックして、ユーザーグループに役割を割り当てるための次の情報を入力します。



- ドメインを選択：一覧からドメインを選択します。
- ユーザー グループで検索：使用可能なすべてのグループ一覧を表示するには、［検索］をクリックします。グループ名の全部または一部を入力して、検索を絞り込みます。
- ユーザー グループを含める：表示された一覧で、役割を割り当てるユーザーグループを選択します。

8. ［保存］をクリックします。

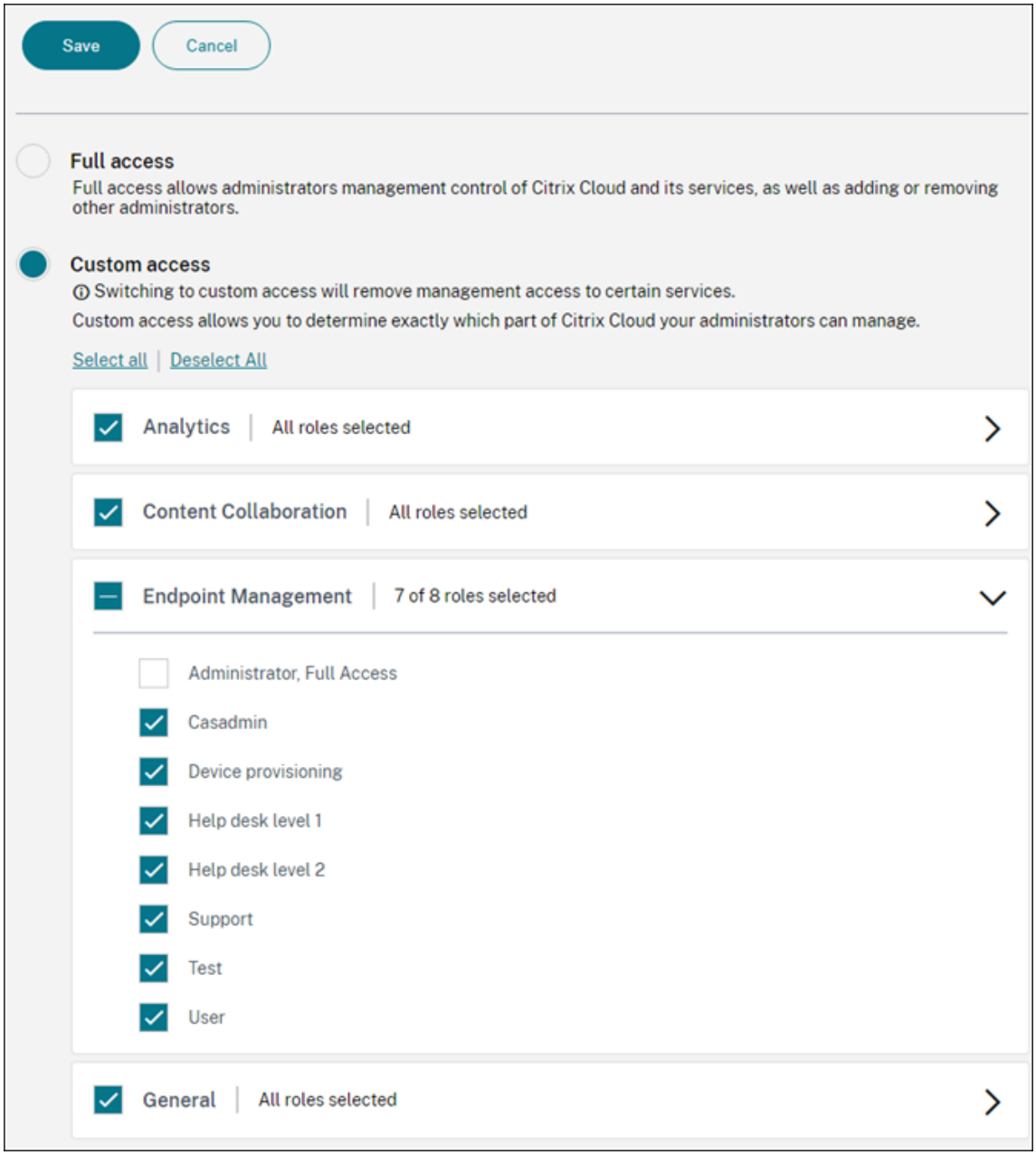
Citrix Cloud 管理者に役割を追加する

Citrix Endpoint Management コンソールを介して Citrix Cloud 管理者に RBAC の役割を割り当てる代わりに、Citrix Cloud コンソールから役割を割り当てます。

1. Citrix Cloud コンソールで ［**ID** およびアクセス管理］**>**［管理者］に移動します。
2. ID プロバイダーを選択し、メールアドレスを入力して管理者を追加します。［招待］をクリックします。

既存の管理者行の最後にある ［…］ をクリックしてこれらの権限を編集します。

3. ［カスタムアクセス］ をクリックします。管理者に権限を割り当てるときに、Citrix Endpoint Management コンソールで作成された RBAC の役割を選択できます。



4. ［招待を送信する］ をクリックして招待状を新しい管理者に送信するか、［保存］ をクリックして管理者の編集を終了します。

事前定義された役割

定義済みの RBAC の各役割には、一定のアクセス権と機能権限が関連付けられています。以下の表では、Admin の役割とユーザー役割の各権限について説明します。事前定義された役割を削除または編集することはできません。

- 組み込みの役割ごとのデフォルト権限に関する完全な一覧は、『Role-Based Access Control Defaults』（英文）をダウンロードしてください。
- Citrix Endpoint Management のユーザーアカウントについては、「ユーザーアカウントについて」を参照してください。

> 重要：
>
> 権限の［設定］で、RBAC 権限は、独自の権限を割り当てる機能を含むフルアクセス権を Admin ユーザーに許可します。このアクセス権は、Citrix Endpoint Management システムのすべてを操作する機能を許可するユーザーにのみ付与してください。

Admin の役割

事前定義された Admin の役割には、Citrix Endpoint Management での特定のアクセス権があります。デフォルトでは、［承認済みアクセス］（Self Help Portal を除く）、［コンソールの機能］、および ［適用権限］が有効になります。

［管理］**>**［ユーザー］を使用して、Admin の役割を割り当てられたローカルユーザーの役割を変更できます。Admin の役割が割り当てられたクラウドユーザーの場合は、Citrix Cloud コンソールを使用してアクセス権を変更します。デフォルトでは、Admin の役割が割り当てられたクラウドユーザーとローカルユーザーにフルアクセス権があります。

管理者用の承認済みアクセス

管理コンソールへのアクセス	管理者は Citrix Endpoint Management コンソールのすべての機能にアクセスできます。
Self-Help Portal へのアクセス	デフォルトでは、管理者は Self Help Portal にアクセスできません。（User の役割が割り当てられたユーザーは、Self Help Portal にのみアクセスできます。）
リモートサポートアクセス	管理者はリモートサポート機能にアクセスできます。

パブリック API へのアクセス	管理者はパブリック API にアクセスして、Citrix Endpoint Management コンソールで利用可能な処理をプログラム的に実行できます。これらの処理には証明書、アプリ、デバイス、デリバリーグループ、ローカルユーザーの管理が含まれます。

管理者用のコンソール機能　管理者は Citrix Endpoint Management コンソールに無制限にアクセスできます。

ダッシュボード	ダッシュボードは、管理者が Citrix Endpoint Management コンソールにログオンした後に表示される最初のページです。ダッシュボードには通知とデバイスに関する基本情報が表示されます。
レポート	［分析］**>**［レポート］ページでは事前定義されたレポートが提供され、アプリおよびデバイスの展開を分析できます。
デバイス	［管理］**>**［デバイス］ページは、管理者がユーザーデバイスを管理するためのページです。ページに個々のデバイスを追加したり、デバイスプロビジョニングファイルをインポートして一度に複数のデバイスを追加したりすることができます。
ローカルユーザーおよびグループ	［管理］**>**［ユーザー］ページでは、ローカルユーザーおよびローカルユーザーグループの追加、編集、または削除を行うことができます。
登録	［管理］**>**［登録招待］ページは、管理者がユーザーを招待してデバイスを Citrix Endpoint Management に登録する方法を管理するためのページです。
ポリシー	［構成］**>**［デバイスポリシー］ページでは、管理者が VPN やネットワークのようなデバイスポリシーを管理します。
アプリ	［構成］**>**［アプリ］ページは、管理者が、ユーザーがデバイスにインストールできる各種アプリを管理するためのページです。

メディア	［構成］**>**［メディア］ページは、管理者が、ユーザーがデバイスにインストールできる各種メディアを管理するためのページです。
操作	［構成］**>**［アクション］ページは、管理者が、イベントをトリガーする応答を管理するためのページです。
デリバリーグループ	［構成］**>**［デリバリーグループ］ページは、管理者がデリバリーグループ、およびデリバリーグループに関連付けられているリソースを管理するためのページです。
登録プロファイル	［構成］**>**［登録プロファイル］ページは、ユーザーがデバイスを登録する方法を指定するためのページです。
Alexa for Business	［設定］ページで、Alexa for Business のプロファイルを管理します。
設定	［設定］ページは、管理者がシステムの設定（クライアントおよびサーバープロパティ、証明書、資格情報プロバイダーなど）を管理するためのページです。重要：これらの設定には、RBAC 権限が含まれています。RBAC 権限は、独自の権限を割り当てる機能を含むフルアクセス権を Admin ユーザーに許可します。このアクセス権は、Citrix Endpoint Management システムのすべてを操作する機能を許可するユーザーにのみ付与してください。
サポート	［トラブルシューティングとサポート］ページは、管理者がトラブルシューティングアクティビティ（診断の実行やログの生成など）を実行するためのページです。

管理者用のデバイス制限　管理者はコンソール全体のデバイス機能にアクセスするため、デバイスの制限を設定したり、デバイスへの通知を設定して送信したり、デバイス上のアプリを管理したりします。

デバイスの完全なワイプ	デバイスからすべてのデータやアプリを消去します。デバイスに設置されている場合、メモリカードもその対象となります。
制限の削除	1 つまたは複数のデバイスの制限を削除します。
デバイスの選択的なワイプ	個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。

場所の表示	デバイスの場所を表示し、デバイスの地理的制約を設定します。関連機能：デバイスの検索、デバイスの追跡
デバイスのロック	ユーザーがデバイスを使用できないように、リモートでデバイスをロックします。
デバイスのロック解除	ユーザーがデバイスを使用できるように、リモートでデバイスのロックを解除します。
コンテナのロック	リモートでデバイス上の企業のコンテナをロックします。
コンテナのロック解除	リモートでデバイス上の企業のコンテナのロックを解除します。
コンテナのパスワードのリセット	企業のコンテナのパスワードをリセットします。
ASM/バイパスアクティベーションロックを有効化	アクティベーションロックが有効な場合、監視対象の iOS デバイスにバイパスコードを格納します。デバイスを消去するには、このコードを使用するとアクティベーションロックが自動的に解除されます。
常駐ユーザーの取得	現在のデバイスで有効なアカウントを持つユーザーの一覧を表示します。この操作により、デバイスと Citrix Endpoint Management コンソール間で強制的に同期が行われます。
常駐ユーザーのログアウト	現在のユーザーを強制的にログアウトします。
常駐ユーザーの削除	指定したユーザーの現在のセッションを削除します。ユーザーは再びサインインできます。
デバイスを呼び出します	リモートで、Windows のデバイスの警報をフルボリュームで 5 分間鳴らします。
デバイスを再起動	Citrix Endpoint Management コンソールから Windows デバイスを再起動します。
デバイスに展開	デバイスにアプリ、通知、制限、その他のリソースを送信します。
デバイスの編集	デバイスの設定を変更します。
デバイスへの通知	デバイスに通知を送信します。
デバイスの追加/削除	Citrix Endpoint Management のデバイスの追加または削除を行います。
デバイスのインポート	ファイルから Citrix Endpoint Management にデバイスのグループをインポートします。
デバイステーブルのエクスポート	［デバイス］ページからデバイス情報を収集し、.csv ファイルにエクスポートします。
デバイスの取り消し	デバイスから Citrix Endpoint Management への接続を禁止します。

アプリのロック	デバイスのすべてのアプリへのアクセスを拒否します。Android では、この制限により、ユーザーが Citrix Endpoint Management にサインインできなくなります。iOS では、ユーザーはサインインできますが、アプリにアクセスすることはできません。
アプリのワイプ	Android では、この制限により、ユーザーの Citrix Endpoint Management アカウントが削除されます。iOS では、この制限により、ユーザーが Citrix Endpoint Management 機能にアクセスするために必要な暗号キーが削除されます。
ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを表示します。
AirPlay ミラーリングの要求	AirPlay ストリーミング開始の要求
AirPlay ミラーリングの停止	AirPlay ストリーミングの停止
紛失モードを有効化	［管理］**>**［デバイス］ページで、監視対象デバイスを紛失モードにして、ロック画面で監視対象デバイスへのアクセスをブロックできます。デバイスを紛失した、または盗難にあった場合、この操作の後にデバイスの位置を特定します。
紛失モードを無効化	［管理］**>**［デバイス］ページで、紛失モードが設定されたデバイスの紛失モードを無効化できます。
OS 更新デバイス	OS アップデートデバイスポリシーをデバイスに展開できます。
デバイスのシャットダウン	Citrix Endpoint Management コンソールから iOS デバイスをシャットダウンします。
デバイスの再起動	Citrix Endpoint Management コンソールから iOS デバイスを再起動します。
デバイス登録証明書の書き換え	デバイス CA 証明書を書き換えます。

ローカルユーザーおよびグループ　管理者は、Citrix Endpoint Management の ［管理］**>**［ユーザー］ページで、ローカルユーザーおよびローカルユーザーグループを管理します。

ローカルユーザーの追加

ローカルユーザーの削除
ローカルユーザーの編集
ローカルユーザーのインポート
ローカルユーザーのエクスポート
ローカルユーザーグループ
ローカルユーザーのロック ID を取得
ローカルユーザーのロックを削除

登録　管理者は登録招待の追加および削除、ユーザーへの通知の送信、.csv ファイルへの登録テーブルのエクスポートを行うことができます。

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待状を追加または削除します。
ユーザーに通知	ユーザーまたはユーザーグループに登録招待状を送信します。
登録招待状テーブルのエクスポート	［登録］ページから登録情報を収集し、.csv ファイルにエクスポートします。

ポリシー

ポリシーの追加/削除	デバイスまたはアプリポリシーを追加または削除します。
ポリシーの編集	デバイスまたはアプリポリシーを変更します。
ポリシーのアップロード	デバイスまたはアプリポリシーをアップロードします。
ポリシーの複製	デバイスまたはアプリポリシーをコピーします。
ポリシーの無効化	既存のアプリポリシーを無効にします。
ポリシーのエクスポート	［デバイスポリシー］ページからデバイスポリシーの情報を収集し、.csv ファイルにエクスポートします。
ポリシーの割り当て	デバイスポリシーを 1 つまたは複数のグループに割り当てます。

アプリ　管理者は Citrix Endpoint Management の ［構成］**>**［アプリ］ページで各種アプリを管理します。

アプリストアまたはエンタープライズアプリの追加/削除	パブリックアプリストアのアプリまたはエンタープライズアプリ（MDX 対応ではない）を追加または削除します。
アプリストアまたはエンタープライズアプリの編集	パブリックアプリストアのアプリまたはエンタープライズアプリ（MDX 対応ではない）を変更します。
MDX、Web、SaaS アプリの追加/削除	MDX 対応アプリ、内部ネットワークからのアプリ（Web アプリ）、またはパブリックネットワークからのアプリ（SaaS）を Citrix Endpoint Management に追加または削除します。
MDX、Web、SaaS アプリの編集	MDX 対応アプリ、内部ネットワークからのアプリ（Web アプリ）、またはパブリックネットワークからのアプリ（SaaS）を Citrix Endpoint Management に対して変更します。
カテゴリの追加/削除	アプリストアでアプリの表示に使用できるカテゴリを追加または削除します。
パブリック/エンタープライズアプリのデリバリーグループへの割り当て	パブリックアプリストアのアプリ、または MDX 対応アプリを、展開のためにデリバリーグループに割り当てます。
デリバリーグループへの MDX/WebLink/SaaS アプリの割り当て	シングルサインオン（WebLink）を必要としない MDX 対応アプリ、またはパブリックネットワーク（SaaS）からのアプリをデリバリーグループに割り当てます。
アプリテーブルのエクスポート	［アプリ］ページからアプリ情報を収集し、.csv ファイルにエクスポートします。

メディア　パブリックアプリストアから、または一括購入ライセンスからメディアを管理します。

アプリストアまたはエンタープライズブックの追加/削除
パブリック/エンタープライズブックのデリバリーグループへの割り当て
アプリストアまたはエンタープライズブックの編集

操作

アクションの追加/削除	トリガーおよび関連する応答によって定義されたアクションを追加または削除します。トリガーは、イベント、デバイスまたはユーザーのプロパティ、またはインストールされているアプリ名です。
アクションの編集	トリガーと関連する応答によって定義されたアクションを変更します。トリガーは、イベント、デバイスまたはユーザーのプロパティ、またはインストールされているアプリ名です。
アクションのデリバリー グループへの割り当て	ユーザーデバイスへの展開のために、デリバリーグループに操作を割り当てます。
アクションのエクスポート	［アクション］ページから操作の情報を収集し、.csv ファイルにエクスポートします。

デリバリー グループ　管理者は ［構成］**>** ［デリバリーグループ］ページからデリバリーグループを管理します。

デリバリーグループの追加/削除	デリバリーグループを作成または削除します。このグループには、指定のユーザーおよびオプションのポリシー、アプリ、操作が追加されています。
デリバリーグループの編集	既存のデリバリーグループを変更します。このグループでは、ユーザーおよびオプションのポリシー、アプリ、操作の変更が行われます。
デリバリーグループの展開	デリバリーグループが使用できる状態にします。
デリバリーグループのエクスポート	［デリバリーグループ］ページからデリバリーグループの情報を収集し、.csv ファイルにエクスポートします。

登録プロファイル　登録プロファイルを管理します。

登録プロファイルの追加/削除
登録プロファイルの編集
登録プロファイルのデリバリーグループへの割り当て

Alexa for Business　Alexa for Business のプロファイルを管理します。

ルームの追加/削除/編集	
ルームプロファイルの追加/削除/編集	
スキルグループの追加/削除/編集	

管理者用の設定　管理者は ［設定］ページで各種設定を構成します。

RBAC	RBAC 割り当て。重要：この権限は、独自の権限を割り当てる機能を含むフルアクセス権を Admin ユーザーに許可します。このアクセス権は、Citrix Endpoint Management システムのすべてを操作する機能を許可するユーザーにのみ付与してください。
LDAP	グループ、ユーザーアカウント、関連のプロパティをインポートする Active Directory のような 1 つまたは複数の LDAP 準拠のディレクトリを管理します。
登録	ユーザーと Self-Help Portal の登録セキュリティモードを有効にします。
リリース管理	現在インストールされてるリリースの情報を表示します。含まれるもの：リリース管理の更新
証明書	APNs 証明書の編集
通知テンプレート	自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを作成します。
ワークフロー	アプリの構成で使用するユーザーアカウントの作成、承認、削除を管理します。
資格情報プロバイダー	デバイスの証明書の発行を許可されている 1 つまたは複数の資格情報プロバイダーを追加します。資格情報プロバイダーは、証明書の形式および証明書の更新または失効の条件を管理します。
PKI エンティティ	公開キーのインフラストラクチャエンティティ（通常は Microsoft Certificate Services、または随意 CA）を管理します。

PKI 接続のテスト	［設定］**>**［**PKI** エンティティ］ページの ［接続のテスト］ボタンを使用して、サーバーがアクセス可能であることを確認します。
クライアントプロパティ	パスコードの種類、強度、有効期限など、ユーザーデバイスの各種プロパティを管理します。
クライアントサポート	ユーザーがサポートサービスに連絡する方法を設定します（メール、電話、またはサポートチケットメール）。
クライアントのブランド設定	アプリストアのカスタムストア名とデフォルトストア表示を作成します。アプリストアや Citrix Secure Hub に表示されるカスタムロゴを追加します。
キャリア SMS ゲートウェイ	キャリア SMS ゲートウェイを設定して、電話会社の SMS ゲートウェイ経由で Citrix Endpoint Management から送信される通知を構成します。
通知サーバー	メールをユーザーに送信するための SMTP ゲートウェイサーバーを設定します。
ActiveSync ゲートウェイ	規則およびプロパティを通してユーザーおよびデバイスへのユーザーアクセスを管理します。
Google Chrome	Google Workspace アカウントと通信できるように Citrix Endpoint Management を構成します。
Apple Deployment Programs	Citrix Endpoint Management に Apple Deployment Program アカウントを追加します。
Apple Configurator デバイス登録	Citrix Endpoint Management コンソールで Apple Configurator 設定を構成します。
iOS/一括購入設定	Apple の一括購入アカウントを追加します。
NetScaler Gateway	Citrix Endpoint Management で NetScaler Gateway（新名称：NetScaler Gateway）の設定を構成します。
ネットワークアクセス制御	デバイスが非準拠であるためネットワークへのアクセスを許可しないと判断する条件を設定します。
サーバープロパティ	サーバープロパティを追加または変更します。すべてのノードで Citrix Endpoint Management の再起動が必要になります。
Virtual Apps and Desktops	Citrix Workspace アプリを通してユーザーが Citrix Virtual Apps and Desktops を追加できるようにします。

Citrix Files	Citrix Endpoint Management と Enterprise アカウントを組み合わせる場合：ShareFile アカウントと、ユーザーアカウント管理用の管理者サービスアカウントに接続するための設定を構成します。既存の Citrix Files ドメインと管理者の資格情報が必要です。Citrix Endpoint Management とストレージゾーンコネクタを組み合わせる場合：ストレージゾーンコネクタで定義されたネットワーク共有と SharePoint の場所を指すように Citrix Endpoint Management を構成します。
Android Enterprise	Android Enterprise サーバー設定を構成します。
ID プロバイダー（IdP）	ID プロバイダーを構成します。
Citrix Endpoint Management ツール	［Citrix Endpoint Management ツール］ページにアクセスします。
Windows 一括登録	Windows 一括登録設定を構成します。

サポート　管理者は各種サポートタスクを実行できます。

NetScaler Gateway 接続性チェック	IP アドレスによる NetScaler Gateway の各種接続確認を実行します。ユーザー名とパスワードが必要です。
Citrix Endpoint Management 接続性チェック	選択した Citrix Endpoint Management の機能（データベース、DNS、Google Plan など）の接続確認を実行します。
Citrix 製品ドキュメント	Citrix Endpoint Management ドキュメントの公開サイトにアクセスします。
Citrix Knowledge Center	ナレッジベースの文書を検索するために Citrix Support サイトにアクセスします。
ログ	ログファイルを表示およびダウンロードします。
マクロ	プロファイル、ポリシー、通知、または登録テンプレートのテキストフィールドにユーザーまたはデバイスのプロパティデータを設定します。単一のポリシーを構成して大きなユーザーベースに展開し、各対象ユーザーに固有の値を表示させることができます。
PKI 構成	PKI 構成情報をインポートおよびエクスポートします。

APNs 署名ユーティリティ	Apple 社の Push Network signing（APNs）証明書の要求を提出するか、iOS 用の Citrix Secure Mail APNs 証明書をアップロードします。
Citrix Insight Services	さまざまな問題に対する支援が得られるように、Citrix Insight Services（CIS）にログをアップロードします。
NetScaler Gateway コネクタ：Exchange ActiveSync 用のデバイスの状態	Exchange ActiveSync 用コネクタに送信されたデバイスの状態について、Citrix Endpoint Management に対するクエリを実行します。クエリは、デバイスの ActiveSync ID に基づいています。

グループアクセスの制限　Admin ユーザーはすべてのユーザーグループに権限を適用することができます。

デバイスプロビジョニングのコンソール機能　Citrix Endpoint Management コンソールに対して、デバイスプロビジョニングユーザーは以下の制限付きアクセスが行えます。デフォルトでは、以下の機能がそれぞれ有効になっています。

デバイスの制限

デバイスの編集	デバイスの設定を変更します。
デバイスの追加/削除	Citrix Endpoint Management のデバイスの追加または削除を行います。

デバイスプロビジョニングの設定　デバイスプロビジョニングのユーザーは ［設定］ページにアクセスできますが、機能を構成する権限はありません。

User の役割

ユーザー役割を持つユーザーは、Citrix Endpoint Management に対して以下の制限付きアクセスが行えます。

ユーザー用の承認済みアクセス

Self-Help Portal	ユーザーは Citrix Endpoint Management の Self Help Portal にのみアクセスできます。

ユーザー用のコンソール機能　Citrix Endpoint Management コンソールに対して、ユーザーは以下の制限付きアクセスが行えます。

ユーザー用のデバイス制限アクセス

デバイスの完全なワイプ	デバイスからすべてのデータやアプリを消去します。デバイスに設置されている場合、メモリカードもその対象となります。
デバイスの選択的なワイプ	個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。
場所の表示	デバイスの場所を表示し、デバイスの地理的制約を設定します。含まれるもの：デバイスの検索、デバイスの場所の表示、デバイスの追跡、時間の経過によるデバイスの位置の追跡。
デバイスのロック	デバイスが使用できないように、リモートでロックします。
デバイスのロック解除	デバイスが使用できるように、リモートでロックを解除します。
コンテナのロック	リモートでデバイス上の企業のコンテナをロックします。
コンテナのロック解除	リモートでデバイス上の企業のコンテナのロックを解除します。
コンテナのパスワードのリセット	企業のコンテナのパスワードをリセットします。
ASM/バイパスアクティベーションロックを有効化	アクティベーションロックが有効な場合、監視対象の iOS デバイスにバイパスコードを格納します。デバイスを消去するには、このコードを使用するとアクティベーションロックが自動的に解除されます。
常駐ユーザーの取得	現在のデバイスで有効なアカウントを持つユーザーの一覧を表示します。この操作により、デバイスと Citrix Endpoint Management コンソール間で強制的に同期が行われます。
常駐ユーザーのログアウト	現在のユーザーを強制的にログアウトします。

常駐ユーザーの削除	指定したユーザーの現在のセッションを削除します。ユーザーは再びサインインできます。
デバイスを呼び出します	リモートで、Windows のデバイスの警報をフルボリュームで 5 分間鳴らします。
デバイスを再起動	Windows デバイスを再起動します。
アプリのロック	デバイスのすべてのアプリへのアクセスを拒否します。Android では、ユーザーが Citrix Endpoint Management にサインインできなくなります。iOS では、ユーザーはサインインできますが、アプリにアクセスすることはできません。
アプリのワイプ	Android では、この制限により、ユーザーの Citrix Endpoint Management アカウントが削除されます。iOS では、この制限により、ユーザーが Citrix Endpoint Management 機能にアクセスするために必要な暗号キーが削除されます。
ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを表示します。

ユーザー用の登録制限

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待状を追加または削除します。
ユーザーに通知	ユーザーまたはユーザーグループに登録招待状を送信します。

すべての役割用のグループアクセスの制限　デフォルトの役割の場合、この権限がデフォルトで設定され、すべてのユーザーグループに適用できます。役割を編集することはできません。

ライセンス

November 29, 2023

ライセンスの使用状況に関する情報については、以下を参照してください:

- クラウドサービスのライセンスおよびアクティブな使用状況の監視
- Citrix Endpoint Management のライセンスとアクティブな使用状況の監視

デバイス管理

March 15, 2024

Citrix Endpoint Management では、単一の管理コンソール内で、幅広いタイプのデバイスのプロビジョニング、管理、セキュリティ保護、インベントリを行うことができます。

- デバイスポリシーの共通セットを使用して、サポートされているデバイスを管理します。プラットフォームで利用可能なデバイスポリシーを簡単に確認するには、次の手順に従います:

  1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］に移動します。
  2. ［追加］をクリックし、表示するプラットフォームを選択します。

     詳細については、「追加されたデバイスポリシーの一覧のフィルター」を参照してください。

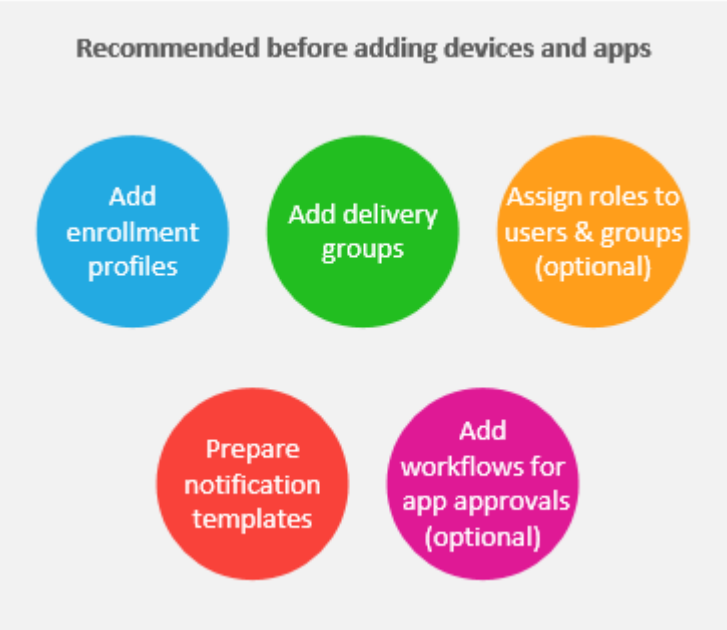
- ID、コーポレート所有のデバイス、BYO デバイス、アプリ、データ、ネットワークに厳重なセキュリティを用いて、ビジネス情報を保護します。デバイスへの認証に使用するユーザー ID を指定します。デバイス上で企業データと個人データを分離したままにする方法を設定します。
- デバイスやオペレーティングシステムに関係なく、あらゆるアプリをエンドユーザーに配信します。アプリレベルで情報を保護し、エンタープライズクラスのモバイルアプリケーション管理を提供します。
- プロビジョニングと構成制御を使用してデバイスを設定します。これらのコントロールには、デバイスの登録、ポリシーの適用、アクセス権限が含まれます。
- セキュリティおよびコンプライアンスの制御を使用して、カスタマイズされたセキュリティベースラインを実行可能なトリガーで作成します。たとえば、定められたコンプライアンス基準に違反した際には、デバイスをロック、ワイプ、またはデバイスに通知します。
- OS 更新制御を使用して、オペレーティングシステムの更新を禁止または強制します。この機能は、対象となるオペレーティングシステムの脆弱性に対するデータ損失防止のために不可欠です。

サポートされている各プラットフォームに関する記事にアクセスするには、コンテンツ一覧の［デバイス管理］セクションを展開します。これらの記事にはデバイスの各プラットフォーム固有の詳細が記載されています。本記事のこれより先は、一般的なデバイス管理タスクを実行する方法について説明します。

デバイス管理ワークフロー

このセクションのワークフロー図は、デバイス管理タスクの推奨手順を示しています。

1. デバイスとアプリの追加において推奨される前提条件：次のセットアップを事前に実行すると、中断することなくデバイスとアプリを構成できます。



次を参照してください：

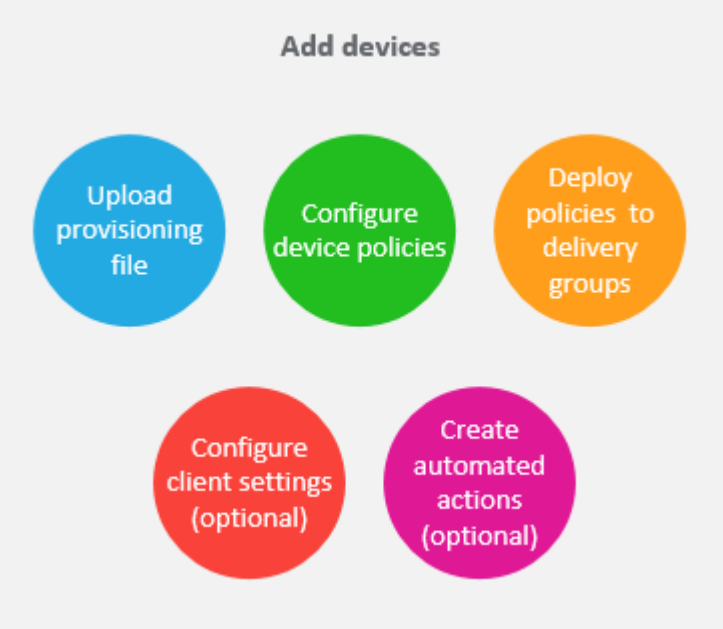
リソースの展開

RBAC を使用した役割の構成

通知テンプレートの作成および更新

ワークフローの作成および管理

2. 追加するデバイス：



次を参照してください:

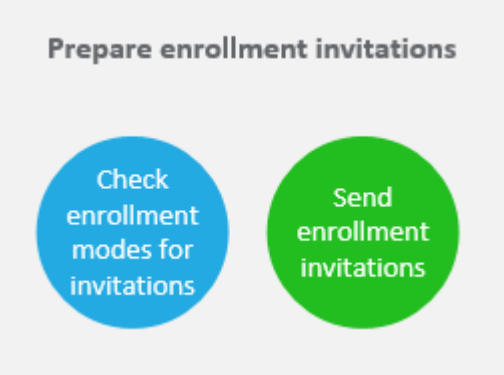
デバイス登録とリソース配信の準備

デバイスポリシー

デリバリーグループへの展開

自動化された操作

3. 登録招待状の準備: iOS、iPadOS、macOS、Android Enterprise、従来の Android デバイスを使用するユーザーに登録招待状メールを送信できます。登録招待状を使用する場合は、次の手順を実行してください。



次を参照してください:

登録セキュリティモードを構成する

デバイスに通知を送信する

4. アプリの追加:

次を参照してください:

MAM SDK

アプリの追加

アプリのカテゴリについて

ワークフローの適用

デリバリーグループへの展開

5. デバイスおよびアプリの管理を継続的に実行する： Citrix Endpoint Management ダッシュボードの使用に加えて、各リリースの「新機能」のコンテンツを確認することもお勧めします。「新機能」では、新しいデバイスポリシーの設定など、必要な操作に関する情報を提供します。

次を参照してください：

モニターとサポート

レポート

セキュリティ操作

新機能

デバイスポリシー

登録招待

ユーザーデバイスをリモートで安全に管理するため、ユーザーデバイスを Citrix Endpoint Management に登録します。Citrix Endpoint Management クライアントソフトウェアがユーザーデバイスにインストールされ、ユーザーの ID が認証されます。認証後、Citrix Endpoint Management とユーザープロファイルがインストールされ

ます。サポートされているデバイスプラットフォームの登録の詳細については、このセクションのデバイスに関する記述を参照してください。

Citrix Endpoint Management コンソールの場合:

- iOS、iPadOS、macOS、Android Enterprise、従来の Android デバイスを使用するユーザーに登録招待状メールを送信できます。登録招待状は、Windows デバイスでは利用できません。
- iOS、iPadOS、Android Enterprise、または従来の Android デバイスを使用しているユーザーにインストール URL を送信することができます。招待 URL は Windows デバイスでは使用できません。

登録招待は次のように送信されます。

- Active Directory ユーザーのメールアドレスが Active Directory に登録されている場合、ユーザーは招待を受信します。ローカルユーザーは、ユーザープロパティで指定されたメールアドレスで招待を受信します。

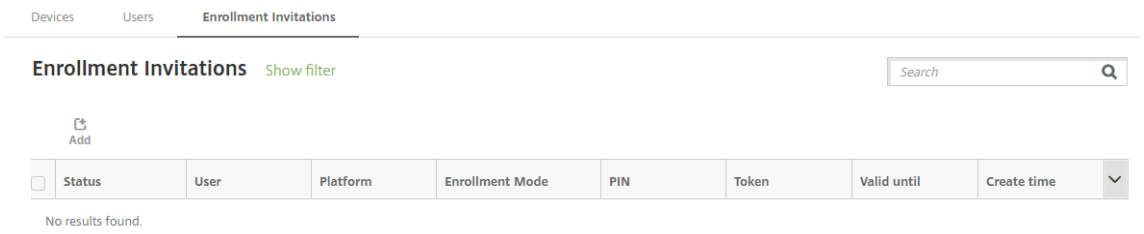
ユーザーが登録すると、そのデバイスは ［管理］ > ［デバイス］で管理対象として表示されます。招待 URL の状態は［再開］と表示されます。

前提条件

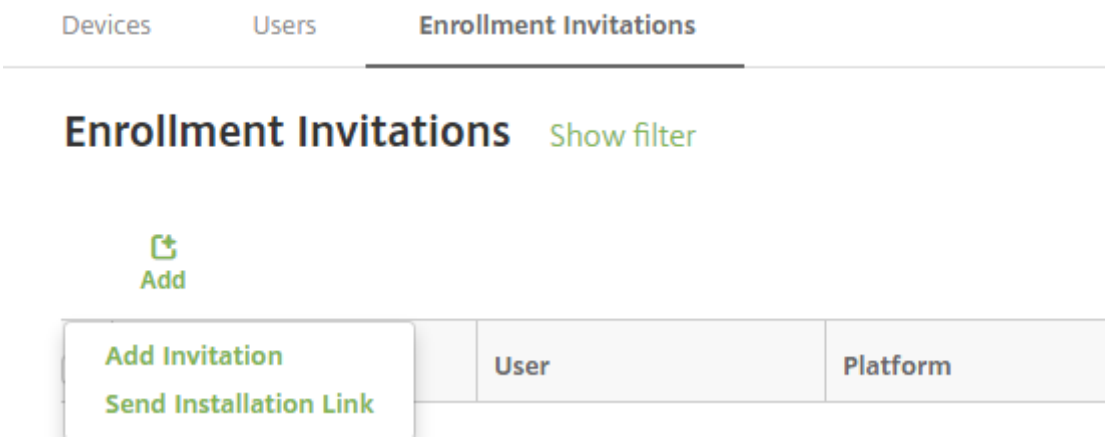
- 構成された LDAP
- ローカルグループおよびローカルユーザーを使用する場合:
  - 1 つまたは複数のローカルグループ。
  - ローカルグループに割り当てられたローカルユーザー。
  - デリバリーグループはローカルグループと関連付けられます。
- Active Directory を使用する場合:
  - デリバリーグループは Active Directory グループと関連付けられます。

登録招待の作成

1. Citrix Endpoint Management コンソールで、［管理］ > ［登録］の順にクリックします。［登録招待］ページが開きます。



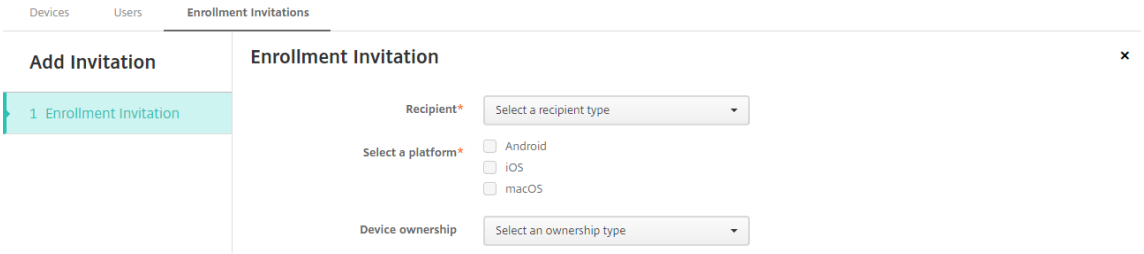
2. ［追加］をクリックします。登録オプションのメニューが表示されます。



- 1 人のユーザーまたは 1 つのグループに登録招待を送信するには、［招待の追加］をクリックします。
- SMTP 経由で登録インストールリンクを受信者の一覧に送信するには、［インストールリンクの送信］を選択します。

登録招待およびインストールリンクの送信は、次の手順の後に説明します。

3. ［招待の追加］をクリックします。［登録招待］画面が開きます。



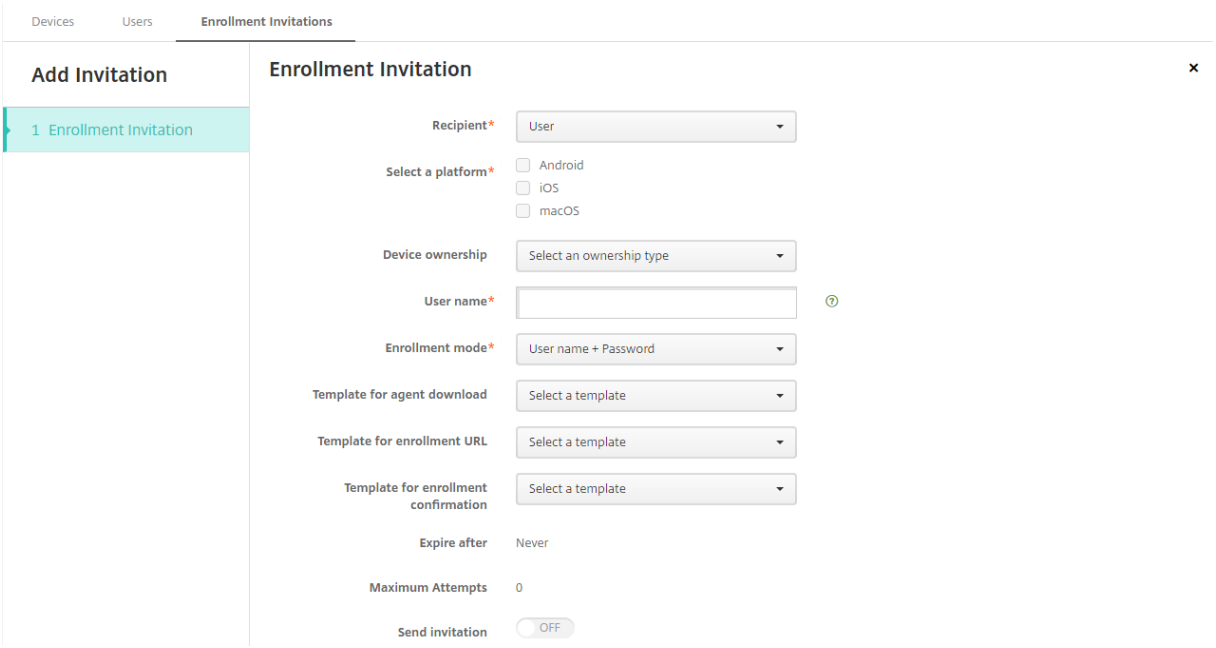
4. 次の設定を構成します:

- 宛先:［グループ］または ［ユーザー］を選択します。
- プラットフォームを選択:［宛先］が ［グループ］の場合はすべてのプラットフォームが選択されます。プラットフォームの選択は変更可能です。［宛先］が ［ユーザー］の場合はいずれのプラットフォームも選択されません。プラットフォームを選択します。

  Android Enterprise デバイスの登録招待状を作成するには、［**Android**］を選択します。
- デバイス所有権:［コーポレート］または ［従業員］を選択します。

次のセクションで説明するように、ユーザーまたはグループの設定が表示されます。

登録招待をユーザーに送信するには



1. ［ユーザー］について、次の設定を構成します。

   - ユーザー名：ユーザー名を入力します。このユーザーは、Citrix Endpoint Management サーバーのローカルユーザー、または Active Directory ユーザーとして存在している必要があります。ローカルユーザーの場合、通知を送信できるようにユーザーのメールプロパティを設定します。Active Directory ユーザーの場合、LDAP が構成されていることを確認します。
   - 電話番号：複数のプラットフォームを選択した場合、または macOS のみを選択した場合は、この設定は表示されません。任意で、ユーザーの電話番号を入力します。
   - キャリア：複数のプラットフォームを選択した場合、または macOS のみを選択した場合は、この設定は表示されません。ユーザーの電話番号に関連付けるキャリアを選択します。
   - 登録モード：ユーザーの登録セキュリティモードを選択します。デフォルトは ［ユーザー名およびパスワード］です。次のオプションの中には、すべてのプラットフォームでは使用できないものもあります：
     - ユーザー名およびパスワード
     - 招待 **URL**
     - 招待 **URL** および **PIN**
     - 招待 **URL** およびパスワード
     - **2** 要素
     - ユーザー名および **PIN**

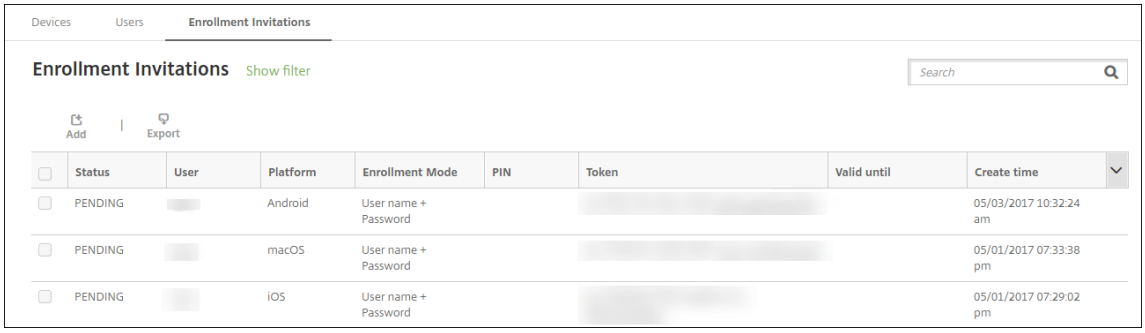
   高セキュリティ登録モードのサポートは廃止されました。登録招待状を送信するには、登録セキュリティモードとして、［招待 **URL**］、［招待 **URL** および **PIN**］、または ［招待 **URL** およびパスワード］のいずれかのみを使用できます。［ユーザー名およびパスワード］、［**2** 要素］、［ユーザー名および **PIN**］のいずれかで登録するデバイスの場合、Citrix Secure Hub をダウンロードして資格情報を手動で入力する必要があります。

詳しくは、「プラットフォームごとの登録セキュリティモード」を参照してください。登録用の PIN はワンタイム PIN とも呼ばれます。このような PIN は、ユーザーの登録時にのみ有効です。

> 注:
>
> PIN を含む登録セキュリティモードを選択すると、［登録 **PIN** 用テンプレート］フィールドが表示されます。［登録 **PIN**］をクリックします。

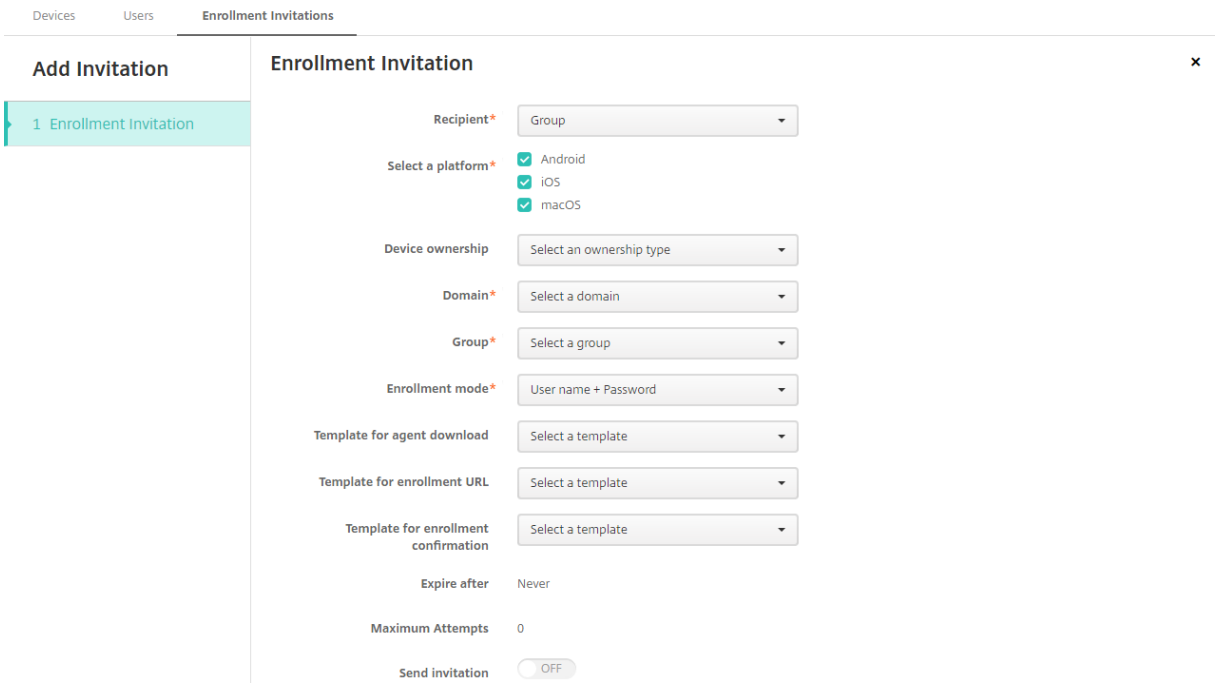
- エージェントダウンロード用テンプレート：ダウンロードリンクという名称のダウンロードリンクのテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォームで使用できます。
- 登録 **URL** 用テンプレート：［登録招待］を選択します。
- 登録確認用テンプレート：［登録確認］を選択します。
- 有効期限：このフィールドは登録の期限を示すものであり、登録セキュリティモードを構成するときに設定します。登録セキュリティモードの構成について詳しくは、「登録セキュリティモードを構成する」を参照してください。
- 最大試行数：このフィールドは登録処理を行う上限回数を示すものであり、登録セキュリティモードを構成するときに設定します。
- 招待を送信：招待を直ちに送信するには、［オン］を選択します。［登録招待］ページの表に招待を追加するが送信しないという場合は、［オフ］を選択します。

2. ［招待を送信］を有効にした場合は ［保存］および［送信］をクリックします。それ以外の場合は ［保存］をクリックします。［登録招待］ページの表に招待が追加されます。



登録招待をグループに送信するには

以下は、グループへの登録招待を構成するための設定画面です。



1. 次の設定を構成します:

   - ドメイン: 招待の宛先グループのドメインを選択します。
   - グループ: 招待の宛先グループを選択します。Citrix Endpoint Management は、Active Directory からユーザー一覧を取得します。この一覧には、名前に特殊文字が含まれているユーザーが含まれます。
   - 登録モード: ユーザーに求める登録の方法を選択します。デフォルトは ［ユーザー名およびパスワード］です。次のオプションの中には、すべてのプラットフォームでは使用できないものもあります:
     - ユーザー名およびパスワード
     - 招待 **URL**
     - 招待 **URL** および **PIN**
     - 招待 **URL** およびパスワード
     - **2** 要素
     - ユーザー名および **PIN**

   高セキュリティ登録モードのサポートは廃止されました。登録招待状を送信するには、登録セキュリティモードとして、[招待 **URL**]、[招待 **URL** および **PIN**]、または ［招待 **URL** およびパスワード］のいずれかのみを使用できます。[ユーザー名およびパスワード]、[**2** 要素]、[ユーザー名および **PIN**］のいずれかで登録するデバイスの場合、Citrix Secure Hub をダウンロードして資格情報を手動で入力する必要があります。

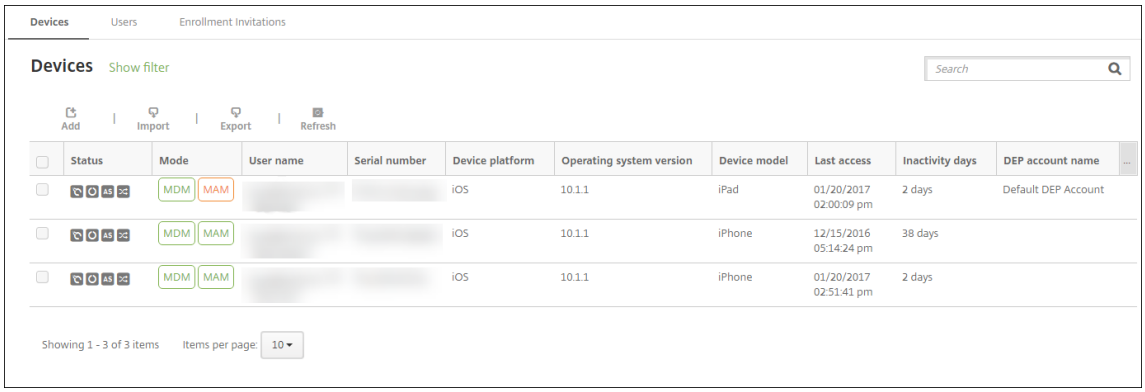
   選択した各プラットフォームに有効な登録セキュリティモードのみが表示されます。詳しくは、「プラットフォームごとの登録セキュリティモード」を参照してください。

   > 注:
   >
   > PIN を含む登録セキュリティモードを選択すると、［登録 **PIN** 用テンプレート］フィールドが表示され

> ます。[登録 **PIN**] をクリックします。

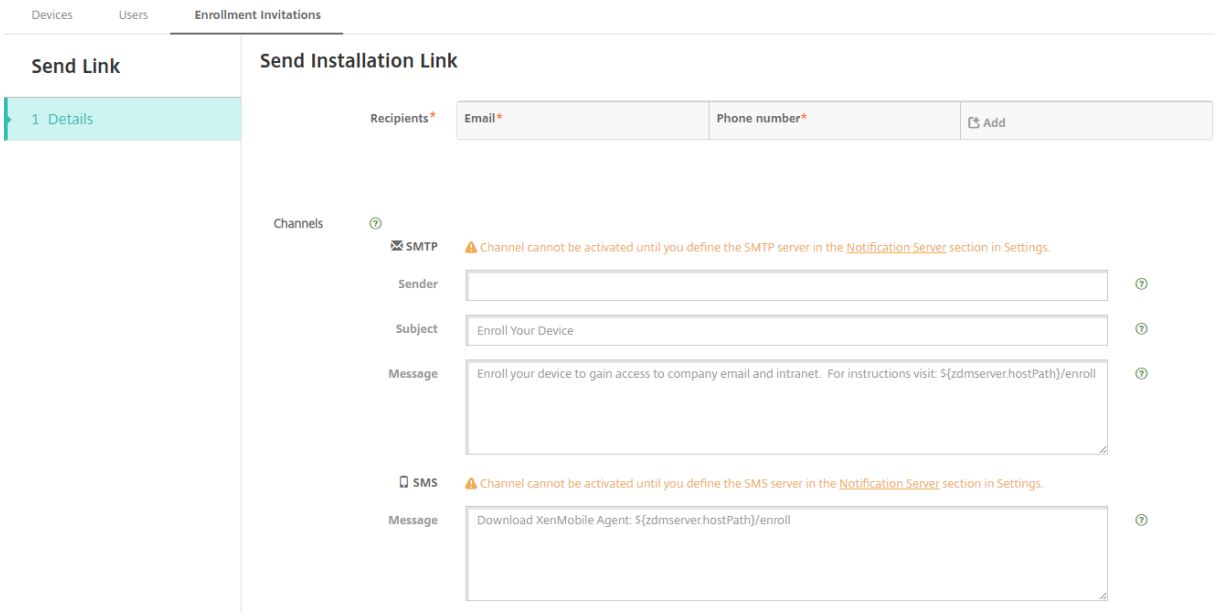
- エージェントダウンロード用テンプレート：ダウンロードリンクという名称のダウンロードリンクのテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォームで使用できます。
- 登録 **URL** 用テンプレート：[登録招待] を選択します。
- 登録確認用テンプレート：[登録確認] を選択します。
- 有効期限：このフィールドは登録の期限を示すものであり、登録セキュリティモードを構成するときに設定します。登録セキュリティモードの構成について詳しくは、「登録セキュリティモードを構成する」を参照してください。
- 最大試行数：このフィールドは登録処理を行う上限回数を示すものであり、登録セキュリティモードを構成するときに設定します。
- 招待を送信：招待を直ちに送信するには、[オン] を選択します。[登録招待] ページの表に招待を追加するが送信しないという場合は、[オフ] を選択します。

2. [招待を送信] を有効にした場合は [保存] および [送信] をクリックします。それ以外の場合は [保存] をクリックします。[登録招待] ページの表に招待が表示されます。



インストールリンクを送信するには

登録インストールリンクを送信する前に、[設定] ページでチャネル（SMTP）を構成する必要があります。詳しくは、「通知」を参照してください。



1. これらの設定を構成し、［保存］をクリックします。

   - 宛先：追加する宛先ごとに、［追加］をクリックして以下の操作を行います：
     - メール：送信先のメールアドレスを入力します。このフィールドは必須です。
     - 電話番号：送信先の電話番号を入力します。このフィールドは必須です。

     > 注：
     >
     > 送信先を削除するには、項目の行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには ［削除］をクリックし、項目をそのままにするには ［キャンセル］をクリックします。
     >
     > 送信先を編集するには、項目の行の上にマウスポインターを置きます。次に、右側のペンアイコンをクリックします。項目を変更し、［保存］をクリックして変更した項目を保存するか、［キャンセル］をクリックして項目を変更せずそのままにします。

   - チャネル：登録インストールリンクの送信に使用するチャネルを選択します。通知は **SMTP** で送信することができます。［通知サーバー］の ［設定］ページでサーバー設定を構成するまでは、これらのチャネルをアクティブ化できません。詳しくは、「通知」を参照してください。
   - **SMTP**：次の設定を任意で構成します。これらのフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
     - 差出人：オプションで送信者を入力します。
     - 件名：任意でメッセージの件名を入力します。たとえば、「Enroll your device」などです。
     - メッセージ：任意で、送信先に送信されるメッセージを入力します。たとえば、「Enroll your device to gain access to organizational apps and email.」などです。

2. ［送信］をクリックします。

> 注:
>
> 環境が sAMAccountName を使用している場合、ユーザーが招待を受け取ってリンクをクリックした後、認証を完了するには、ユーザー名を編集する必要があります。ユーザー名はsAMAccountName@domainname.comの形式で表示されます。ユーザーは「@domainname.com」の部分を削除する必要があります。

プラットフォームごとの登録セキュリティモード

次の表に、ユーザーデバイスの登録に使用できるセキュリティモードを示します。表の「はい」は、どのデバイスプラットフォームが、登録プロファイルが異なる特定の登録および管理モードをサポートしているかを示しています。

MDM 登録セキュリティモード	NetScaler Gateway の MAM 登録セキュリティモード	管理モード	異なる登録プロファイルをサポートするか	Android（レガシ）	Android Enterprise	iOS（ユーザー登録モード）	iOS	macOS	Windows
Citrix Cloud を介した ID プロバイダーとしての Azure Active Directory と Okta	クライアント証明書	MDM+MAMまたは MDM	はい	はい	はい	はい	はい	いいえ	いいえ

MDM 登録セキュリティモード	NetScaler Gateway の MAM 登録セキュリティモード	管理モード	異なる登録プロファイルをサポートするか	Android（レガシ）	Android Enterprise	iOS（ユーザー登録モード）	iOS	macOS	Windows
ユーザー名およびパスワード	LDAP、LDAP + クライアント証明書、およびクライアント証明書のみ	MDM+MAM、または MAM（MAM のみのモードは NetScaler Gateway のクライアント証明書をサポートしていません）	はい	はい	はい	はい	はい	はい	はい
招待 URL	クライアント証明書	MDM+MAM または MDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
招待 URL および PIN	クライアント証明書	MDM+MAM または MDM	はい	はい	はい	いいえ	はい	いいえ	いいえ

MDM 登録セキュリティモード	NetScaler Gateway の MAM 登録セキュリティモード	管理モード	異なる登録プロファイルをサポートするか	Android（レガシ）	Android Enterprise	iOS（ユーザー登録モード）	iOS	macOS	Windows
招待 URL およびパスワード	LDAP、LDAP + クライアント証明書、およびクライアント証明書のみ	MDM+MAM または MDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
2 要素認証（ユーザー名 + パスワード + PIN）	LDAP、LDAP + クライアント証明書、およびクライアント証明書のみ	MDM+MAM または MDM	はい	はい	はい	いいえ	はい	はい	いいえ
ユーザー名および PIN	クライアント証明書	MDM+MAM または MDM	はい	はい	はい	いいえ	はい	はい	いいえ

ここでは、iOS、Android、Android Enterprise デバイスでの登録セキュリティモードの動作について説明します:

- ユーザー名およびパスワード（デフォルト）
  - 登録 URL が記載された 1 つの通知をユーザーに送信します。ユーザーがこの URL をクリックすると、Citrix Secure Hub が開きます。ユーザーは、ユーザー名とパスワードを入力して Citrix Endpoint

Management にデバイスを登録します。

- 招待 **URL**
  - 登録 URL が記載された 1 つの通知をユーザーに送信します。ユーザーがこの URL をクリックすると、Citrix Secure Hub が開きます。Citrix Endpoint Management サーバー名と ［はい、登録します］ボタンが表示されます。ユーザーは ［はい、登録します］をタップして、デバイスを Citrix Endpoint Management に登録します。
- 招待 **URL** および **PIN**
  - ユーザーに次のメールを送信します:
    * ユーザーが Citrix Secure Hub 経由で Citrix Endpoint Management でデバイスを登録できる登録 URL が記載されたメール。
    * デバイスの登録時に、ユーザーの Active Directory（またはローカル）のパスワードとともにユーザーが入力する必要があるワンタイム PIN 付きのメール。
  - このモードでは、ユーザーは通知の登録 URL を使用してのみ登録します。ユーザーが登録招待状を紛失した場合、ユーザーは登録できなくなります。ただし、新たに招待状を送信することはできます。
- 招待 **URL** およびパスワード
  - 登録 URL が記載された 1 つの通知をユーザーに送信します。ユーザーがこの URL をクリックすると、Citrix Secure Hub が開きます。Citrix Endpoint Management サーバー名と、ユーザーがパスワードを入力できるフィールドが表示されます。
- **2** 要素
  - 登録 URL とワンタイム PIN が記載された 1 つの通知をユーザーに送信します。ユーザーがこの URL をクリックすると、Citrix Secure Hub が開きます。Citrix Endpoint Management サーバー名と、ユーザーがパスワードと PIN をそれぞれ入力できる 2 つのフィールドが表示されます。
- ユーザー名および **PIN**
  - ユーザーに次のメールを送信します:
    * ユーザーが Citrix Secure Hub をダウンロードしてインストールできる登録リンクが記載されたメール。Citrix Secure Hub の起動後、ユーザーは、ユーザー名とパスワードを入力して Citrix Endpoint Management にデバイスを登録するよう求められます。
    * デバイスの登録時に、ユーザーの Active Directory（またはローカル）のパスワードとともにユーザーが入力する必要があるワンタイム PIN 付きのメール。
  - ユーザーが登録招待状を紛失した場合、ユーザーは登録できなくなります。ただし、新たに招待状を送信することはできます。

ここでは、macOS デバイスでの登録セキュリティモードの動作について説明します:

- ユーザー名およびパスワード

  - 登録 URL が記載された 1 つの通知をユーザーに送信します。ユーザーが URL をクリックすると、Safari ブラウザーが開きます。サインインページが開き、ユーザーはユーザー名とパスワードを入力して Citrix Endpoint Management にデバイスを登録するよう求められます。

- **2** 要素
  - 登録 URL とワンタイム PIN が記載された 1 つの通知をユーザーに送信します。ユーザーが URL をクリックすると、Safari ブラウザーが開きます。サインインページが開き、ユーザーがパスワードと PIN をそれぞれ入力できる 2 つのフィールドが表示されます。

- ユーザー名および **PIN**
  - ユーザーに次のメールを送信します:
    * 登録 URL が記載されたメール。ユーザーが URL をクリックすると、Safari ブラウザーが開きます。サインインページが開き、ユーザーはユーザー名とパスワードを入力して Citrix Endpoint Management にデバイスを登録するよう求められます。
    * デバイスの登録時に、ユーザーの Active Directory（またはローカル）のパスワードとともにユーザーが入力する必要があるワンタイム PIN 付きのメール。
  - ユーザーが登録招待状を紛失した場合、ユーザーは登録できなくなります。ただし、新たに招待状を送信することはできます。

Windows デバイスに登録招待を送信することはできません。Windows ユーザーはデバイスから直接登録します。Windows デバイスの登録手順については、「Windows デバイス」を参照してください。

セキュリティ操作

［管理］**>**［デバイス］ページでデバイスやアプリのセキュリティの操作を実行できます。デバイスの操作には、取り消し、ロック、ロック解除、ワイプがあります。アプリのセキュリティの操作には、アプリのロック、アプリのワイプが含まれます。

- アクティベーションロックバイパス：デバイスのライセンス認証の前に、監視対象の iOS デバイスからアクティベーションロックを解除します。このコマンドでは、Apple の個人 ID やユーザーのパスワードが要求されることはありません。
- アプリのロック：デバイスのすべてのアプリへのアクセスを拒否します。Android では、アプリのロックが行われるとユーザーは Citrix Endpoint Management にサインインできなくなります。iOS では、ユーザーはサインインできますが、アプリにアクセスすることはできません。
- アプリのワイプ： Citrix Secure Hub からユーザーアカウントを削除し、デバイスの登録を解除します。管理者がアプリのワイプ解除アクションを使用するまで、ユーザーは再登録できません。
- **ASM Deployment Program** アクティベーションロック： Apple School Manager に登録されている iOS デバイスのアクティベーションロックバイパスコードを作成します。

- 証明書の書き換え：サポートされている iOS デバイス、macOS デバイス、および Android デバイスの場合、セキュリティ操作［証明書の書き換え］により証明書の書き換えが開始されます。次回デバイスが Citrix Endpoint Management に接続すると、Citrix Endpoint Management サーバーは新しい証明機関に基づいて新しいデバイス証明書を発行します。
- 制限の解除：監視対象の iOS デバイスでこのコマンドを使用すると、ユーザーによって構成された制限パスワードと制限設定を Citrix Endpoint Management で解除できるようになります。
- 紛失モードを有効化/無効化：監視対象の iOS デバイスを紛失モードにして、デバイスに表示されるメッセージ、電話番号、補足説明を送信します。2 回目にこのコマンドを送信すると、デバイスの紛失モードは無効になります。
- 追跡を有効にする： Android または iOS デバイスでは、このコマンドによって Citrix Endpoint Management が指定された頻度で特定のデバイスの場所をポーリングできます。デバイスの座標と位置をマップ上に表示するには、［管理］**>**［デバイス］に移動し、デバイスを選択して ［編集］をクリックします。デバイス情報は、［全般］タブの ［セキュリティ］にあります。デバイスを継続的に追跡するには、［追跡を有効にする］を使用します。Citrix Secure Hub は、デバイスの実行中にデバイスの場所を定期的に報告します。
- フルワイプ：デバイスからメモリカードを含むすべてのデータとアプリを直ちに消去します。ワイプされたデバイスは、監査目的で ［管理］**>**［デバイス］ページのデバイスリストに残ります。ワイプされたデバイスは、デバイスリストから削除できます。
  - Android デバイスの場合、メモリカードをワイプするオプションをこの要求に含めることができます。
  - 仕事用プロファイルで完全に管理された Android Enterprise デバイス（COPE デバイス）の場合、選択的なワイプにより仕事用プロファイルが削除された後、完全ワイプを実行できます。
  - iOS デバイスと macOS デバイスの場合、デバイスがロックされていても直ちにワイプが実行されます。

    iOS 11 デバイスおよび iPadOS 12 デバイス（最小バージョン）の場合：フルワイプを確認したら、携帯データネットワークプランをデバイスに保存することができます。

    iOS 11.3 デバイス（最小バージョン）の場合：フルワイプを確認したら、iOS デバイスが近接セットアップを実行するのを禁止できます。新しい iOS デバイスを設定する場合、通常ユーザーは既に構成済みの iOS デバイスを使用して自分のデバイスを設定できます。ワイプ済みの Citrix Endpoint Management 管理対象デバイスについて、近接セットアップを禁止することができます。
  - メモリカードの内容が削除される前にユーザーがデバイスの電源をオフにした場合、ユーザーはデバイスのデータにまだアクセスできる場合があります。
  - ワイプの要求がデバイスに送信されるまでは、要求をキャンセルできます。
- 検索：［管理］**>**［デバイス］ページの、［デバイス詳細］**>**［一般］で、デバイスを検索してデバイスの場所（マップなど）を報告します。検索は 1 回限りの操作です。［検索］を使用すると、操作を実行した時点のデバイスの場所が表示されます。一定期間にわたってデバイスを継続的に追跡するには、［追跡を有効にする］を使用します。

  - この操作を Android（Android Enterprise を除く）デバイス、または Android Enterprise（企業所有または BYOD）デバイスに適用する場合は、次の動作に注意してください：
    * ［検索］を使用するには、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しないことを選択できます。登録時にユーザーによって権限が付与されないと、Citrix Endpoint Management は **Locate** コマンドの送信時に検索の権限を再度要求します。
  - この機能を iOS または Android Enterprise デバイスに適用する場合は、次の制限に注意してください：
    * Android Enterprise デバイスの場合、位置情報デバイスポリシーでデバイスの位置情報モードが［高精度］または［バッテリー節約］に設定されていない限り、この要求は失敗します。
    * iOS デバイスの場合、このコマンドは、デバイスが MDM の紛失モードである場合にのみ成功します。

- ロック：デバイスをリモートでロックします。ロックは、デバイスの盗難に備えてデバイスをロックする必要がある場合に便利です。その後、Citrix Endpoint Management によって PIN コードが生成されてデバイスに設定されます。デバイスにアクセスするには、PIN コードを入力します。Citrix Endpoint Management コンソールからロックを解除するには ［ロックのキャンセル］を使用します。
- ロックおよびパスワードのリセット：デバイスをリモートロックしてパスコードをリセットします。
  - 以下のデバイスではサポートされません：
    * Android Enterprise に仕事用プロファイルモードで登録済みデバイス、および
    * Android 7.0 より前のバージョンを実行しているデバイス
  - Android 7.0 以降を実行する、仕事用プロファイルモードで Android Enterprise に登録されている端末の場合：
    * パスコードによって、仕事用プロファイルがロックされます。デバイスはロックされません。
    * パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしておらず、仕事用プロファイルにパスコードが設定されていない場合：デバイスはロックされます。
    * パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていないが、仕事用プロファイルにパスコードが設定済みの場合：仕事用プロファイルはロックされますが、デバイスはロックされません。
- 通知（通知音）： Android デバイスで通知音を鳴らします。
- 再起動： Windows 10 および Windows 11 デバイスを再起動します。Windows タブレットおよび PC の場合、保留中の再起動に関するメッセージが表示されます。再起動は 5 分で行われます。
- **AirPlay** ミラーリングの要求/停止：監視対象の iOS デバイスで、AirPlay ミラーリングを開始および停止します。
- 再起動/シャットダウン：監視対象の iOS デバイスを直ちに再起動またはシャットダウンします。
- 取り消し：デバイスから Citrix Endpoint Management への接続を禁止します。

- 取り消し/認証：選択的なワイプと同じ操作を実行します。取り消し後に、デバイスを再承認して再登録できます。
- 警報：監視対象の iOS デバイスが紛失モードの場合に、デバイスで警告音を鳴らします。警告音は、デバイスの紛失モードが解除されるか、ユーザーがサウンドを無効にするまで鳴り続けます。
- 個人用回復キーの交換： FileVault デバイスポリシーを有効にしている場合、このアクションにより新しい個人用回復キーが生成され、古いキーがこの新しいキーに置き換えられます。この要求が保留中である間は、要求をキャンセルできます。キャンセルするには、［個人用回復キーの交換をキャンセルする］をクリックします。
- 選択的なワイプ：個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。選択的なワイプの後、［認証］操作でデバイスを再認証すると、ユーザーは再度デバイスに登録できます。ワイプされたデバイスは、監査目的で ［管理］**>**［デバイス］ページのデバイスリストに残ります。ワイプされたデバイスは、デバイスリストから削除できます。
  - Android デバイスを選択的にワイプしても、Device Manager や社内ネットワークから切断されることはありません。デバイスが Device Manager にアクセスしないようにするには、デバイス証明書を失効させる必要もあります。
  - Android デバイスを選択的にワイプしてもデバイスが取り消されます。デバイスの再登録は、デバイスを再認証するか、コンソールから削除した場合にのみ行えます。
  - 仕事用プロファイルで完全に管理された Android Enterprise デバイス（COPE デバイス）の場合、選択的なワイプにより仕事用プロファイルが削除された後、完全ワイプを実行できます。または、同じユーザー名でデバイスを再登録できます。デバイスを再登録すると、仕事用プロファイルが再作成されます。
  - iOS デバイスおよび macOS デバイスでは、このコマンドにより、MDM を通じてインストールされたすべてのプロファイルが削除されます。
  - Windows デバイスに対して選択的ワイプを実行した場合、その時点でサインオンしているすべてのユーザーのプロファイルフォルダーの内容も削除されます。選択的なワイプでは、構成を介してユーザーに配信した Web クリップは削除されません。Web クリップを削除するには、ユーザーはデバイスを手動で登録解除します。選択的にワイプされたデバイスを再登録することはできません。
- ロック解除：デバイスがロックされたときに送信されたパスコードをクリアします。このコマンドによってデバイスがロック解除されることはありません。

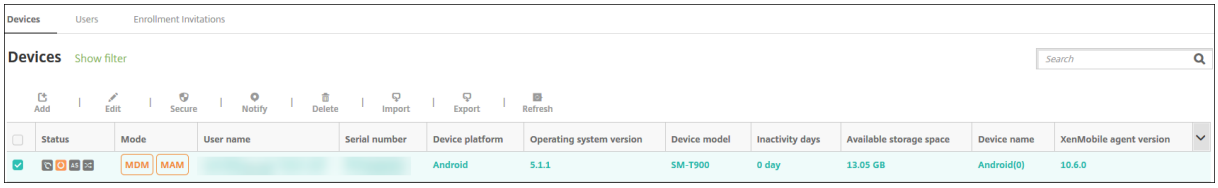
［管理］**>**［デバイス］の ［デバイス詳細］ページには、デバイスの［セキュリティ］プロパティも表示されます。これらのプロパティには、[Strong ID]、[デバイスのロック]、[アクティベーションロックバイパス]、およびプラットフォームの種類に関するその他の情報などが含まれます。［デバイスの完全なワイプ］フィールドには、ユーザーの PIN コードが含まれます。デバイスがワイプされた後、ユーザーはこのコードを入力する必要があります。ユーザーがコードを忘れた場合は、こちらで確認できます。

一部の操作を自動化することができます。詳しくは、「自動化された操作」を参照してください。

Citrix Endpoint Management コンソールからのデバイスの削除

> 重要:
>
> Citrix Endpoint Management コンソールからデバイスを削除しても、管理対象アプリとデータはそのデバイスに残ります。デバイスから管理対象アプリとデータを削除するには、この記事で後述する「デバイスの削除」を参照してください。

Citrix Endpoint Management コンソールからデバイスを削除するには、［管理］**>**［デバイス］の順に選択し、管理対象デバイスを選択して ［削除］をクリックします。



デバイスの選択的なワイプ

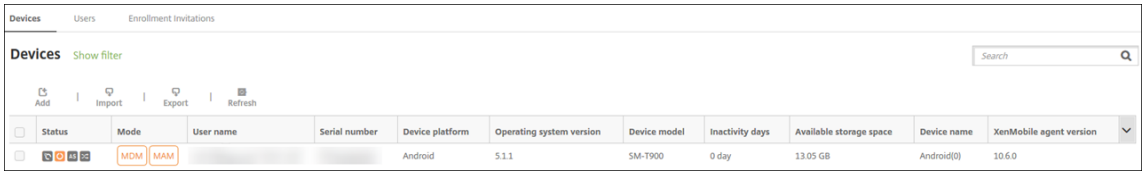
1. ［管理］**>**［デバイス］の順に選択し、管理対象デバイスを選択して ［保護］をクリックします。
2. ［セキュリティ操作］で、［選択的なワイプ］をクリックします。
3. Android デバイスのみ、デバイスをワイプした後、［セキュリティ操作］で ［取り消し］をクリックして、社内ネットワークからデバイスを切断します。

   選択的ワイプ要求が実行される前にその要求を取り消すには、［セキュリティ操作］で、［選択的なワイプのキャンセル］をクリックします。

デバイスの削除

この手順では、管理対象アプリとデータをデバイスから削除し、Citrix Endpoint Management コンソールの［デバイス］一覧からデバイスを削除します。Citrix Endpoint Management Public REST API を使用して、デバイスを一括で削除できます。

1. ［管理］**>**［デバイス］の順に選択し、管理対象デバイスを選択して ［保護］をクリックします。
2. ［選択的なワイプ］をクリックします。プロンプトが表示されたら、［選択的なワイプの実行］をクリックします。
3. ワイプコマンドが成功したことを確認するには、［管理］**>**［デバイス］を更新します。［モード］列で MDM と MAM が黄色の場合は、ワイプコマンドが成功したことを示します。

4. ［管理］**>**［デバイス］に移動し、デバイスを選択して ［削除］をクリックします。プロンプトが表示されたら、再び ［削除］をクリックします。

アプリのロック、ロック解除、ワイプ、ワイプ解除

1. ［管理］**>**［デバイス］の順に選択し、管理対象デバイスを選択して ［保護］をクリックします。
2. ［セキュリティ操作］で、アプリの操作をクリックします。

   ［セキュリティ操作］ボックスは、アカウントが無効になっているか、Active Directory から削除されているユーザーのデバイスの状態を確認するために使用することもできます。アプリロック解除またはアプリワイプ解除アクションが存在する場合、アプリがロックまたはワイプされていることを意味します。

アプリのワイプとワイプ解除

1. ［管理］**>**［デバイス］に移動します。デバイスを選択します。
2. アプリのワイプ
   - ［保護］**>**［アプリのワイプ］をクリックします。次のメッセージのダイアログボックスが表示されます：このデバイスのアプリをワイプしてもよろしいですか**?**［アプリのワイプ］をクリックします。
3. アプリのワイプ解除
   - ［保護］**>**［アプリのワイプ解除］をクリックします。次のメッセージのダイアログボックスが表示されます：このデバイスのアプリワイプを解除してもよろしいですか**?**［デバイスのアプリのワイプ解除］をクリックします。
4. 同じユーザーとして、同じモードでデバイスを再登録します。
5. MDX アプリを ［マイアプリ］ページから起動します。
6. Citrix Secure Hub を起動します。

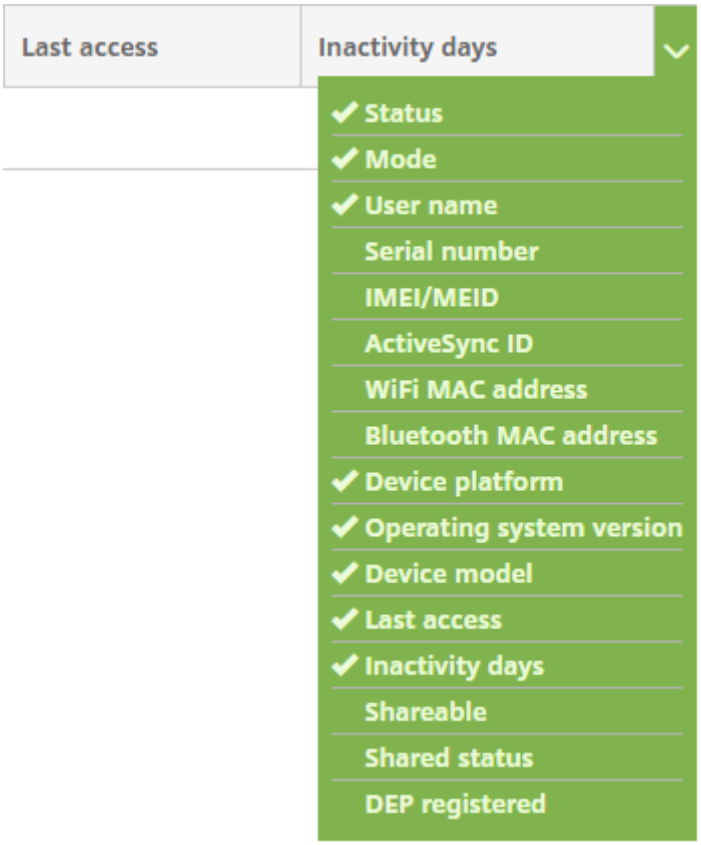
デバイス情報の取得

Citrix Endpoint Management のデータベースには、モバイルデバイスの一覧が保存されます。Citrix Endpoint Management コンソールにデバイスを追加するには、手動でデバイスを追加するか、ファイルからデバイスの一覧をインポートします。デバイスプロビジョニングファイル形式について詳しくは、「デバイスプロビジョニングファイル形式」を参照してください。

Citrix Endpoint Management コンソールの ［管理］**>**［デバイス］ページには、各デバイスと以下の情報が表示されます：

- 状態：デバイスがジェイルブレイクされているか、管理されているか、ActiveSync Gateway が使用可能か、およびデバイスの展開環境の状態などを示すアイコンです。
- モード： MDM や MDM+MAM などのデバイスモードを示します。
- ほかに、次のようなデバイスの情報を表示できます：ユーザー名、デバイスプラットフォーム、最終アクセス日時、非アクティブ日数。これらの見出しは、デフォルトで表示されます。

［デバイス］の表をカスタマイズするには、見出しの右端の下向き矢印をクリックします。次に、その表に表示する追加の見出しをオンにするか、または削除する見出しをオフにします。

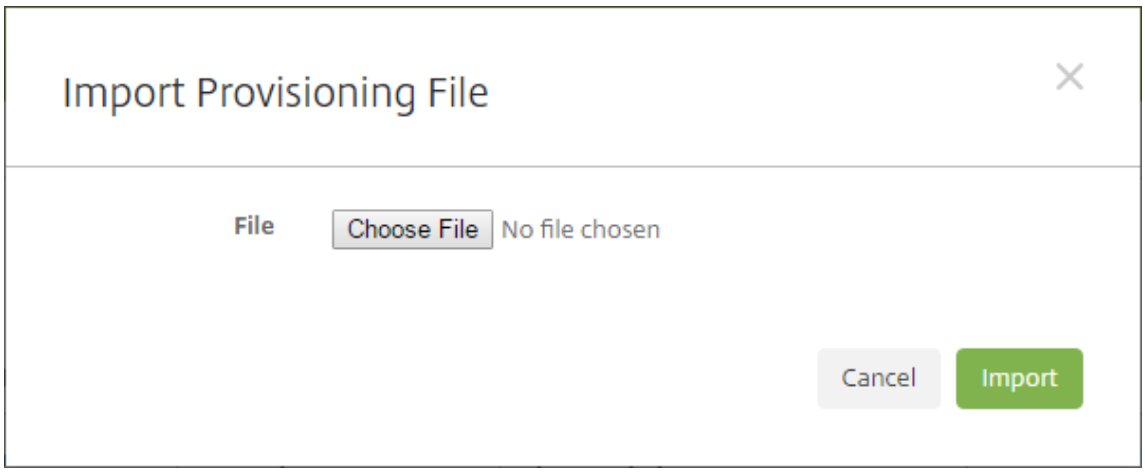


手動によるデバイスの追加、デバイスプロビジョニングファイルからのデバイスのインポート、デバイスの詳細の編集、Active Directory ユーザープロパティのカスタマイズ、セキュリティの操作の実行、デバイスへの通知の送信を行うことができます。デバイス表のデータ全体を.csv ファイルにエクスポートして、このファイルからカスタムレポートを作成することもできます。サーバーはすべてのデバイス属性をエクスポートします。フィルターを適用している場合、Citrix Endpoint Management は.csv ファイルの作成時にそのフィルターを使用します。

デバイスプロビジョニングファイルからのデバイスのインポート

モバイル事業者やデバイス製造元が提供するファイルをインポートしたり、独自のデバイスプロビジョニングファイルを作成したりすることができます。詳しくは、「デバイスプロビジョニングファイル形式」を参照してください。

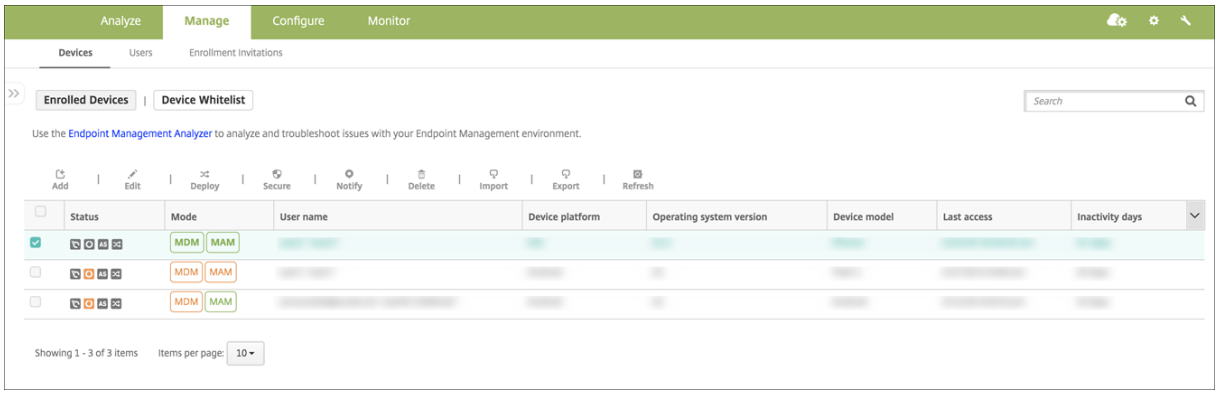
1. ［管理］**>**［デバイス］に移動して、［インポート］を選択します。［プロビジョニングファイルのインポート］ダイアログボックスが開きます。



2. ［ファイルの選択］を選択して、インポートするファイルまで移動します。
3. ［インポート］をクリックします。インポートされたファイルが ［デバイス］の表に追加されます。
4. デバイスの情報を編集するには、［デバイス詳細］を選択して ［編集］をクリックします。［デバイス詳細］ページについて詳しくは、「デバイス情報の取得」を参照してください。

デバイスに展開

1 つまたは複数のデバイスを Citrix Endpoint Management に強制的に接続できます。選択されたデバイスは、スケジュールされた次のチェックインを待たずに即座にリソースを受信できます。



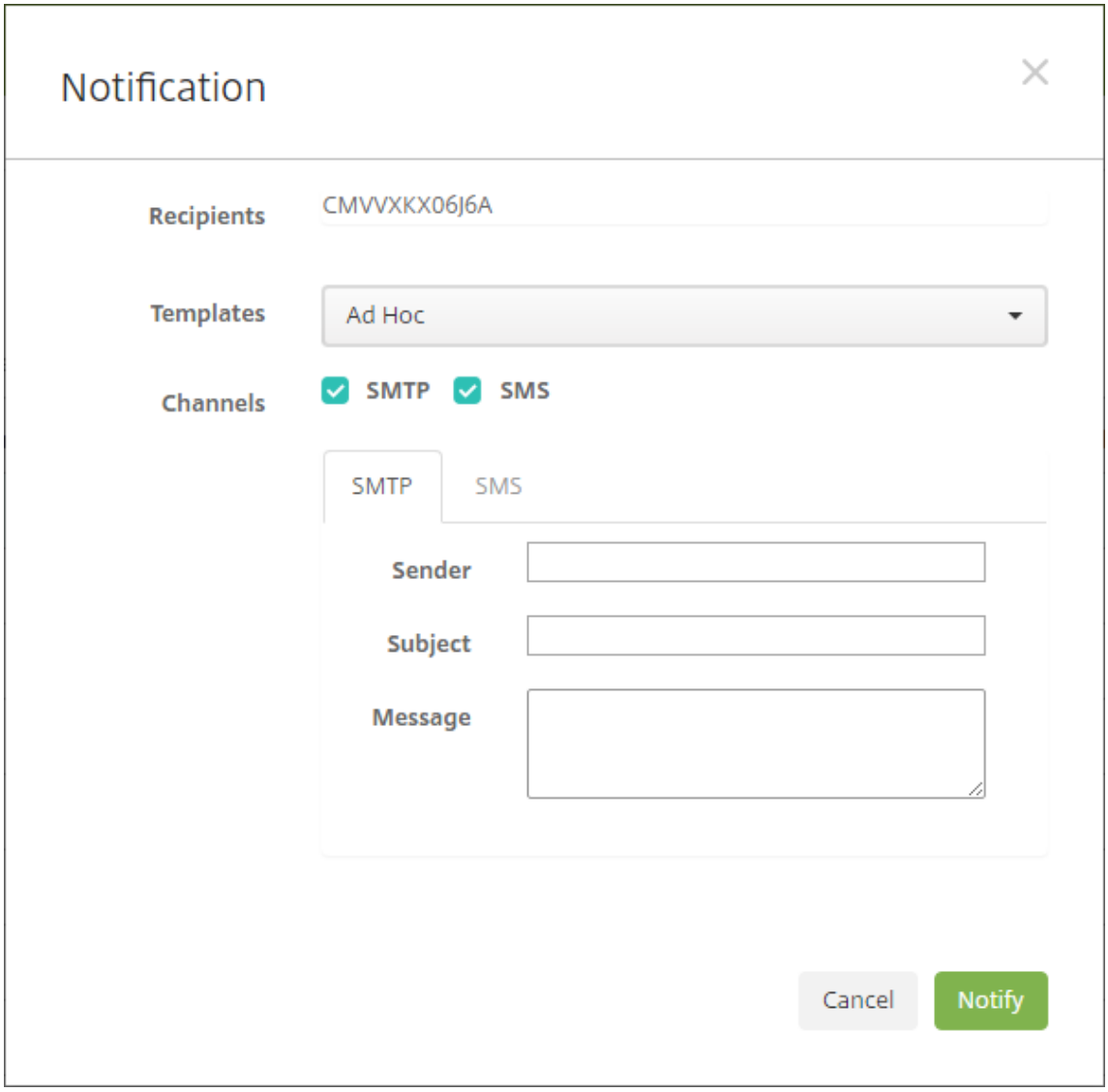
1. ［管理］**>**［デバイス］に移動し、MDM または MDM+MAM 管理対象デバイスを選択して ［展開］をクリックします。
2. ダイアログボックスで ［展開］をクリックして操作を確定します。

デバイスに通知を送信する

［デバイス］ページで、デバイスに通知を送信できます。通知について詳しくは、「通知」を参照してください。

1. ［管理］**>**［デバイス］ページで、通知を送信するデバイスを選択します。

2. ［通知］をクリックします。［通知］ダイアログボックスが開きます。［受信者］フィールドに、通知を受信するすべてのデバイスの一覧が表示されます。



3. 次の設定を構成します：

   - テンプレート：ドロップダウンリストから、送信する通知の種類を選択します。［アドホック］を選択した場合を除き、［件名］フィールドおよび ［メッセージ］フィールドには、選択したテンプレートで構成済みのテキストが入力されます。
   - チャネル：メッセージの送信方法を選択します。デフォルトは ［**SMTP**］です。各チャネルのメッセージの形式を表示するには、タブをクリックします。
   - 差出人：オプションで送信者を入力します。
   - 件名：［アドホック］メッセージの場合、件名を入力します。
   - メッセージ：［アドホック］メッセージの場合、メッセージを入力します。

4. ［通知］をクリックします。

［デバイス］の表のエクスポート

1. エクスポートファイルで表示する内容によって、［デバイス］の表にフィルターを適用します。
2. ［デバイス］の表の上にある ［エクスポート］をクリックします。Citrix Endpoint Management によって［デバイス］表の情報が抽出され、.csv ファイルに変換されます。
3. .csv ファイルを開くか、保存します。

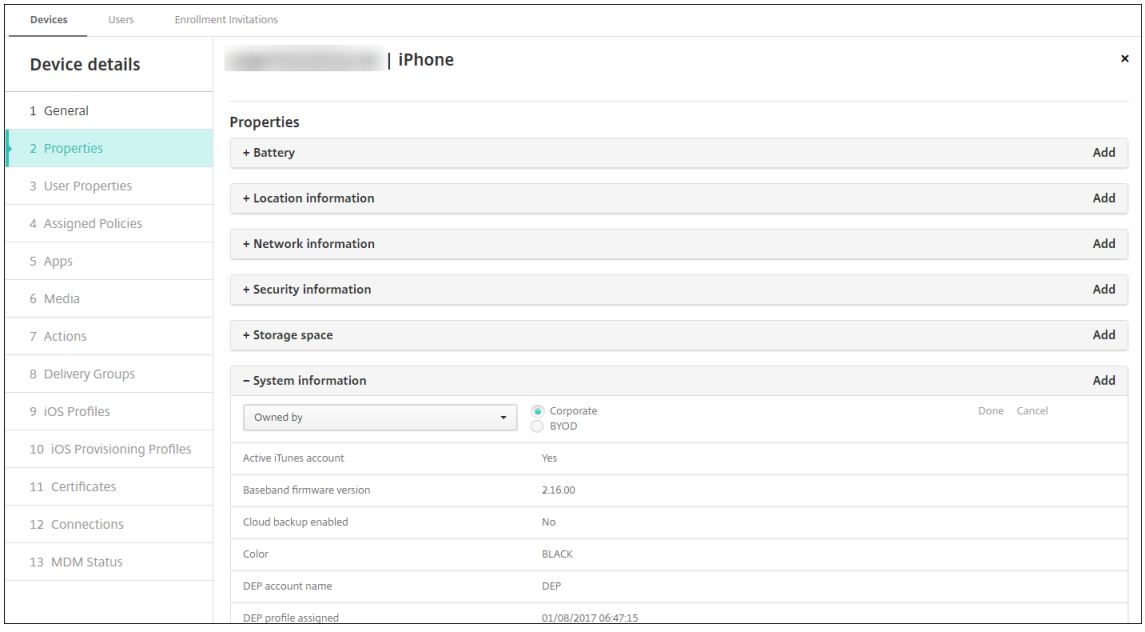
ユーザーデバイスの手動タグ付け

Citrix Endpoint Management では、次のいずれかの方法でデバイスに手動でタグ付けすることができます:

- 招待状に基づく登録処理中
- Self Help Portal 登録処理中
- デバイスの所有権をデバイスプロパティとして追加する

組織または個人所有のいずれかとして、デバイスにタグ付けするオプションが用意されています。Self Help Portal を使ってデバイスを自動登録するときに、組織または個人所有のいずれかとして、デバイスにタグを付けることができます。以下のように手動でデバイスにタグを付けることもできます。

1. Citrix Endpoint Management コンソールの ［デバイス］タブで、プロパティをデバイスに追加します。
2. ［所有者］という名前のプロパティを追加し、［コーポレート］か ［**BYOD**］（個人所有）のいずれかを選択します。



Active Directory ユーザー属性のカスタマイズ

特定の Active Directory ユーザー属性をカスタマイズして、Citrix Endpoint Management がユーザーアカウントを作成するためにアクセスできる属性を定義できます。

属性のリストを表示するには、［設定］**>**［サーバープロパティ］で、サーバープロパティ`optional.user.identity.attributes`をカスタムキーとして追加します。［値］フィールドでは、Citrix Endpoint Management がデフォルトで提供するオプションの Active Directory ユーザー属性を削除したり、後で復元したりできます。詳しくは、「サーバープロパティ」を参照してください。

デフォルト値のリストを編集して変更を保存したら、［管理］**>**［デバイス］**>**［ユーザープロパティ］に、更新された Active Directory ユーザー属性を表示できます。Citrix Endpoint Management は、ユーザーがデバイスにサインインした後、または次にスケジュールされているデバイスのチェックイン中にコンソールを更新します。スペルミスをしたり、サポートされていない値を追加したりすると、Citrix Endpoint Management は変更を無視します。

オプションの Active Directory ユーザー属性を削除すると、次の機能に影響を与える可能性があります:

- ユーザーアカウントのプロビジョニング: 姓名の値を削除すると、Citrix Endpoint Management は ShareFile および Salesforce のユーザーアカウントをプロビジョニングできません。
- 登録招待状: ユーザーのメールまたは携帯電話の詳細を削除すると、ユーザーは登録招待状を受け取ることができません。
- デバイス通知アクション: ユーザーのメールの詳細を削除すると、ユーザーは SMTP 経由で通知を受信できません。
- **Citrix Secure Mail** へのシングルサインオン: 表示名の値を削除すると、ユーザーはシングルサインオンを使用して Citrix Secure Mail にサインインできません。
- ユーザープロパティと展開規則: ユーザープロパティと展開規則の構成で使用するオプション属性のいずれかを削除すると、既存の構成に影響が及ぶ場合があります。
- アクション:［構成］**>**［アクション］で自動化された操作の設定で使用するオプション属性のいずれかを削除すると、既存の構成に影響が及ぶ場合があります。
- カスタムレポート: カスタムレポートで使用するオプション属性のいずれかを削除すると、既存の構成に影響が及ぶ場合があります。

デバイスの検索

高速検索の場合、デフォルト検索のスコープには、次のデバイスプロパティのみが含まれています:

- シリアル番号
- IMEI
- Wi-Fi MAC アドレス
- Bluetooth MAC アドレス
- Active Sync ID
- ユーザー名

新しいサーバープロパティ **include.device.properties.during.search** を使用して検索スコープを構成できます。デフォルトは **false** です。デバイス検索にすべてのデバイスプロパティを含めるには、［設定］**>**［サーバープロパティ］に移動し、設定を **true** に変更します。

デバイスプロビジョニングファイル形式

携帯電話会社またはデバイス製造業者の多くが公認のモバイルデバイスの一覧を提供しています。この一覧を使用することで、モバイルデバイスの長い一覧を手動で入力することを避けることができます。Citrix Endpoint Management は、次のサポート対象デバイスに共通のインポートファイル形式をサポートしています：Android、iOS、Windows。

手動で作成したプロビジョニングファイルは次の形式にする必要があります：

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

次のことに注意してください：

- 各プロパティの有効な値に関しては、デバイスのプロパティ名と値に関する PDF を参照してください。
- UTF-8 形式の文字セットを使用します。
- プロビジョニングファイル内では、フィールドをセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。

  たとえば、このプロパティの場合は次のようになります：

  ```
  propertyV;test;1;2
  ```

  以下のようにエスケープします：

  ```
  propertyV\;test\;1\;2
  ```

- シリアル番号は iOS デバイスの識別子であるため、iOS デバイスにはシリアル番号が必須です。
- その他のデバイスプラットフォームの場合、シリアル番号または IMEI が必要です。
- **OperatingSystemFamily** の有効な値は、**WINDOWS**、**ANDROID**、**iOS** のいずれかです。

デバイスプロビジョニングファイルの例：

```
1 `1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;
     propertyV\;test\;1\;2;prop 2
2 2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;
     propertyV$*&&éééétest
3 3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;
4 4050BF3F5173010816100655105903 93;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

ファイルの各行にデバイスの説明が含まれています。そのサンプルの最初のエントリは以下を意味しています：

- シリアル番号: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- オペレーティングシステムファミリ: `WINDOWS`
- プロパティ名: `propertyN`
- プロパティ値: `propertyV\;test\;1\;2;prop 2`

Alexa for Business

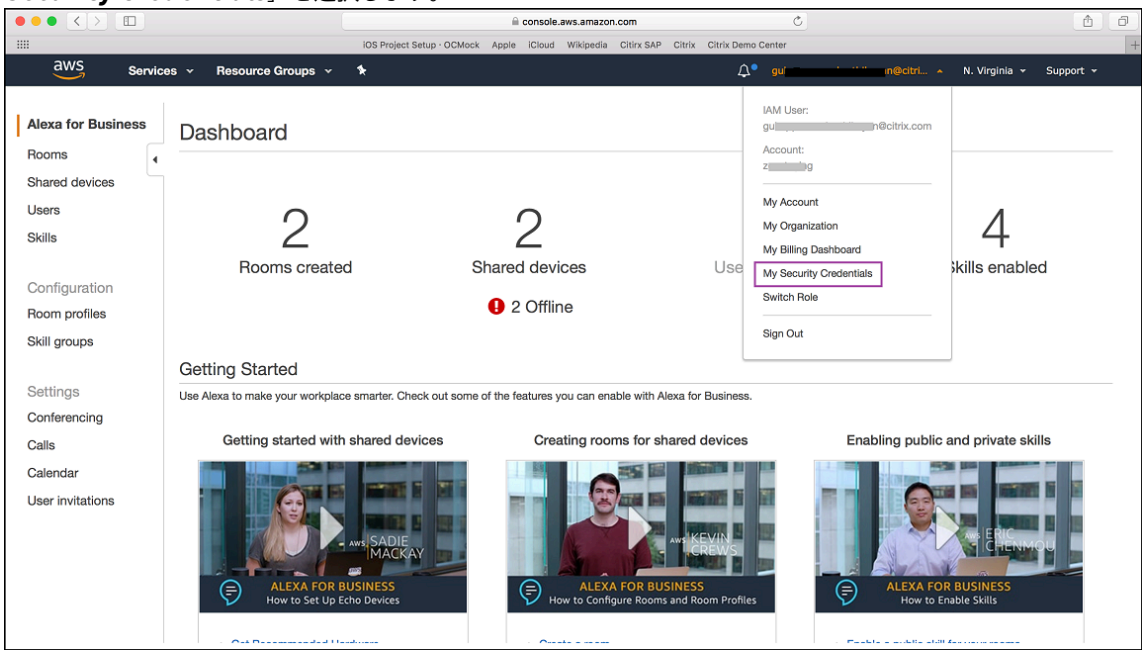
November 29, 2023

アマゾンウェブサービス（AWS：Amazon Web Services）の Alexa for Business サービスを使用すると、会議室でのサポートなどのビジネス用途向けに多数の Alexa 対応デバイスを管理することができます。Citrix Endpoint Management では、これらのデバイスを Citrix Endpoint Management コンソールで構成および管理できます。Citrix Endpoint Management では、Alexa デバイスにポリシーを直接展開しません。代わりに、Citrix Endpoint Management は AWS サービスを更新し、AWS は設定を Alexa デバイスに伝達します。

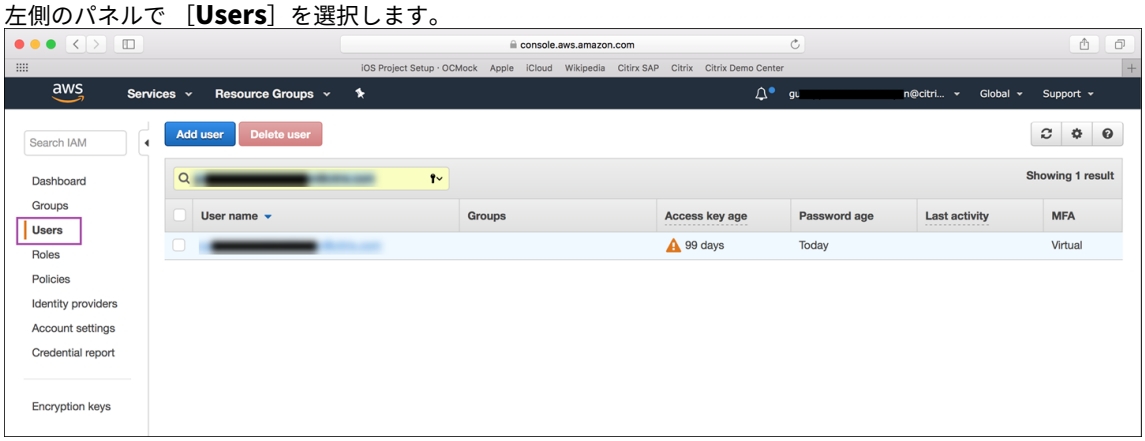
Alexa for Business の使用方法については、「Alexa for Business Administration Guide」を参照してください。

Citrix Endpoint Management で AWS アカウントを認証する

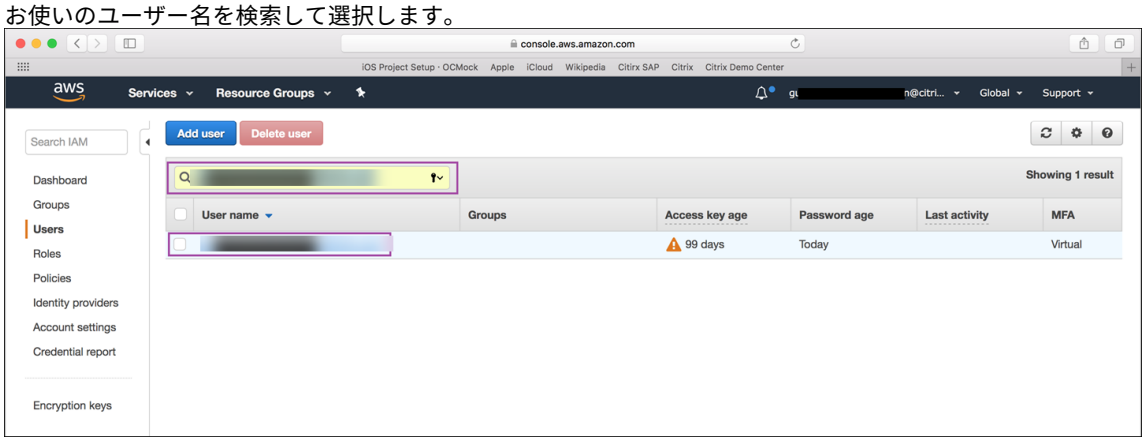
1. AWS アカウントの認証情報を取得するため、AWS コンソールにログインし、ユーザーメニューで ［**My Security Credentials**］を選択します。



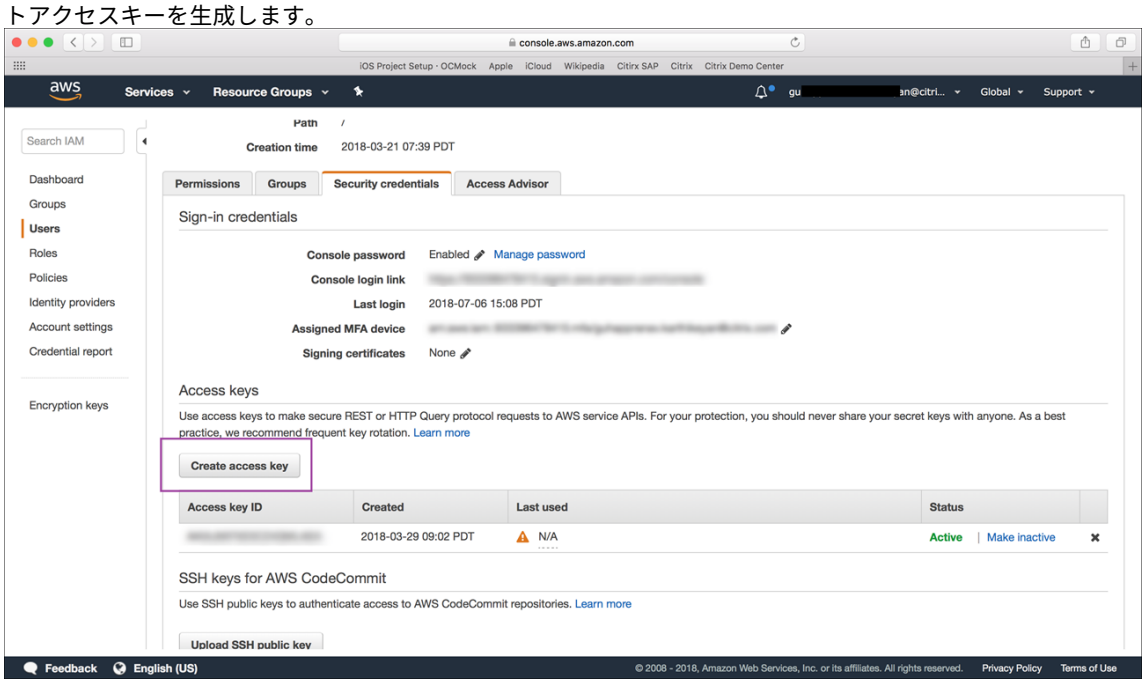
2. 左側のパネルで ［**Users**］を選択します。



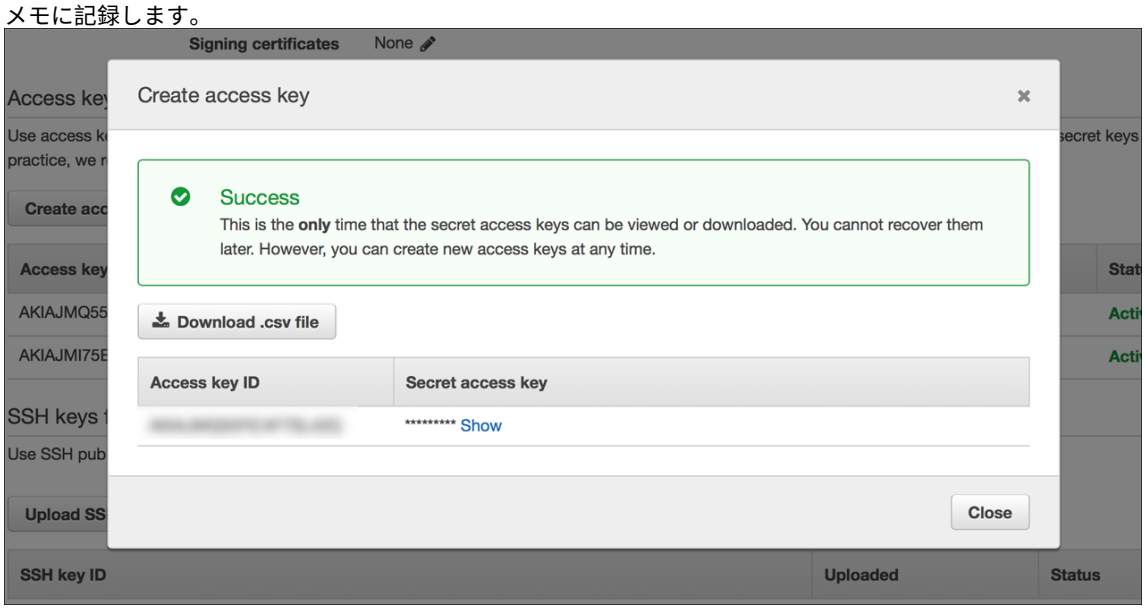
3. お使いのユーザー名を検索して選択します。



4. ［**Security Credentials**］タブで ［**Create access key**］をクリックして、アクセスキー ID とシークレットアクセスキーを生成します。

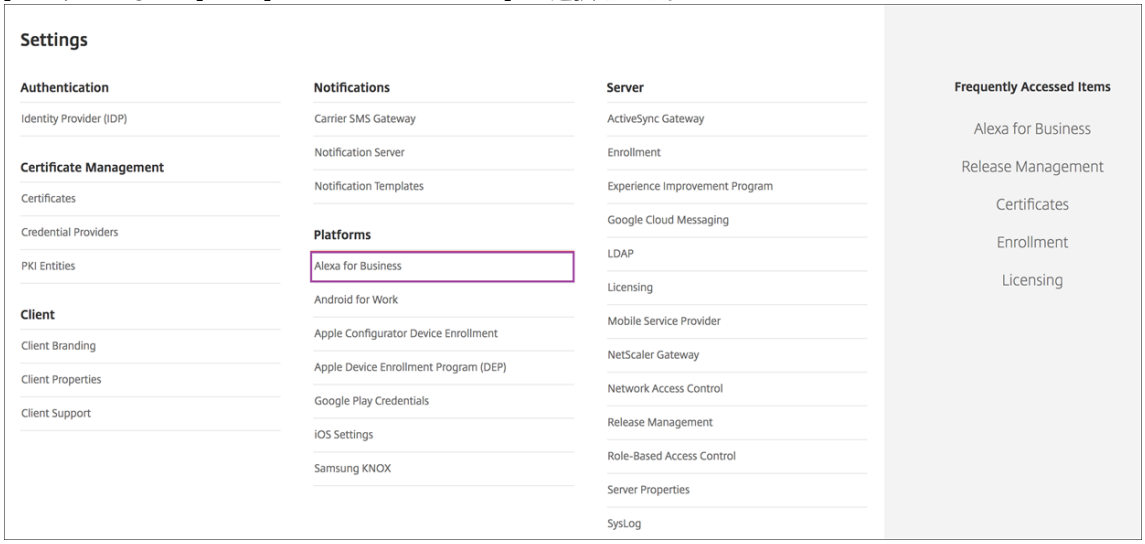


5. アクセスキー ID とシークレットアクセスキーをダウンロードします。ダウンロードしたキーを保存するか、メモに記録します。



6. Citrix Endpoint Management コンソールで、歯車アイコンをクリックして ［設定］に移動します。

7. ［プラットフォーム］で ［**Alexa for Business**］を選択します。



8. アクセスキー ID とシークレットアクセスキーを入力します。［保存］をクリックします。

Citrix Endpoint Management で **Alexa for Business** を構成する

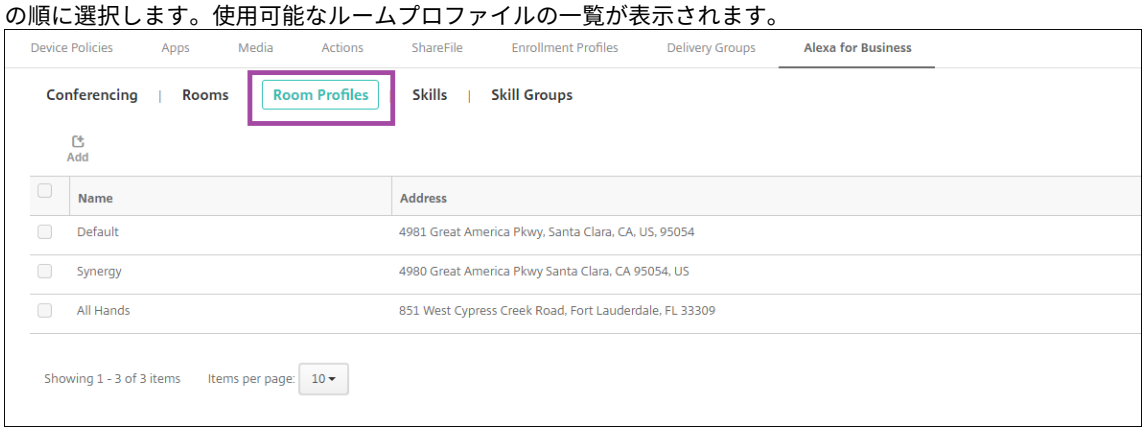
Citrix Endpoint Management では次のものを構成できます:

- Alexa デバイスが置かれた部屋に適用する設定で構成されるルームプロファイル
- デバイスが置かれた現実の部屋を表すルーム
- ルームまたはデバイスに割り当てるスキルグループ
- スキルグループに追加できる Alexa スキルストアの Alexa スキル
- 会議機能を使用すると、会議プロバイダーを選択し、ルームで会議のスケジュールや会議への参加を制御することができます。

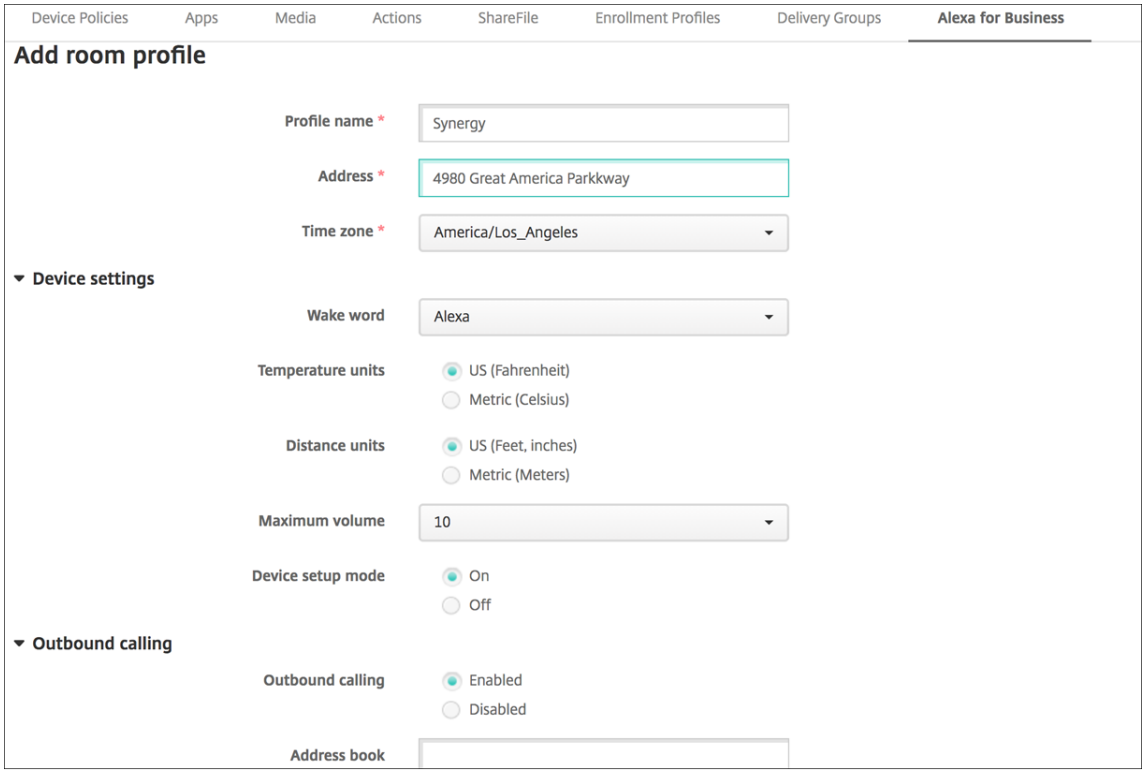
ルームプロファイルを構成する

ルームプロファイルは、Alexa デバイスが設置されたルームグループに適用できる一般的な構成をまとめたものです。ルームプロファイルは追加、編集、削除できます。

1. Citrix Endpoint Management コンソールで、[構成] **>** [**Alexa for Business**] **>** [ルームプロファイル] の順に選択します。使用可能なルームプロファイルの一覧が表示されます。



2. ルームプロファイルを追加するには、[追加] をクリックします。ルームプロファイルを編集するには、対象のプロファイルを選択して [編集] をクリックします。
3. 次のルームプロファイルの設定を入力します:



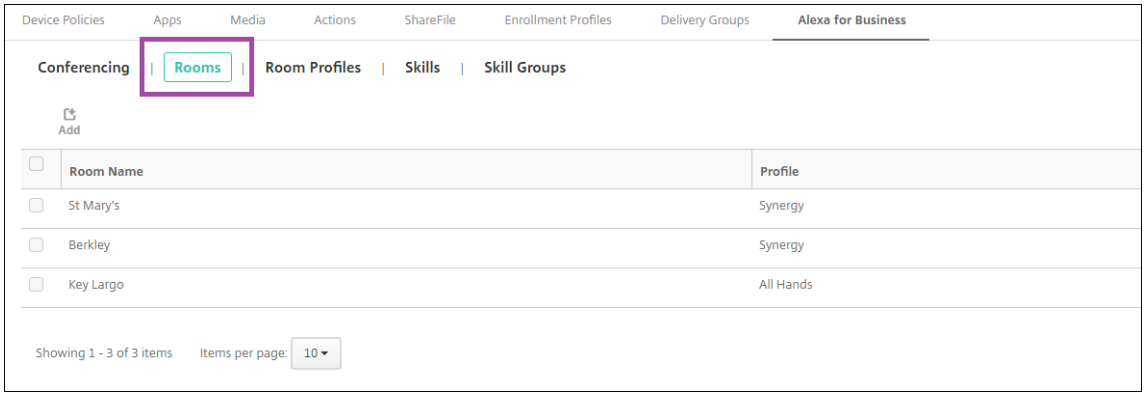
- プロファイル名：プロファイルの名前を入力します。
- 住所： Alexa デバイスを設置する部屋がある建物の住所を入力します。
- タイムゾーン：デバイスを設置する場所のタイムゾーンを選択します。
- ウェイクワード： Alexa デバイスが応答するウェイクワードを選択します。
- 温度単位： Alexa デバイスが温度を報告する際の単位を選択します。
- 距離単位： Alexa デバイスが距離を報告する際の単位を選択します。
- 最大音量： Alexa の最大音量を選択します。
- デバイス設定モード： Alexa デバイスを強制的にデバイスセットアップモードにして再構成できるようにするかどうかを指定します。
- アウトバウンドコール： Alexa デバイスのアウトバウンドコール機能を有効または無効にします。
- アドレス帳： Alexa デバイスのアドレス帳構成を設定します。

4. ［保存］をクリックします。

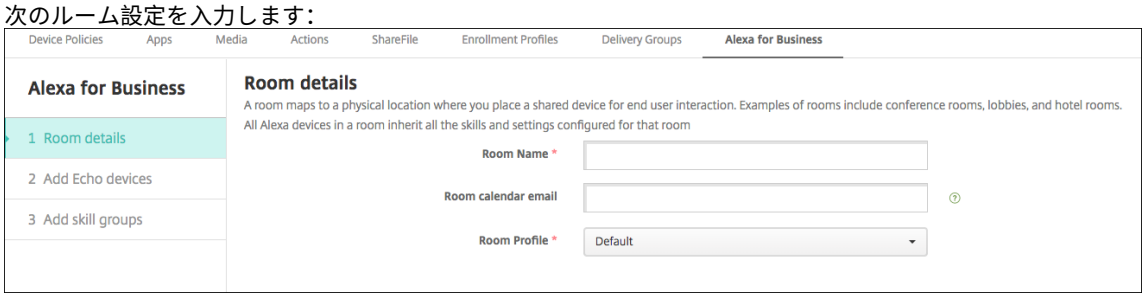
ルームを構成する

Citrix Endpoint Management コンソールで構成するルームは、建物内の会議室や面会室などの実際の部屋を表すものです。ルームの構成では、そのルームに Alexa デバイスを関連付け、デバイスにスキルグループを追加します。ルームは追加、編集、削除できます。

1. Citrix Endpoint Management コンソールで、［構成］ **>** ［**Alexa for Business**］ **>** ［ルーム］の順に選択します。使用可能なルームの一覧が表示されます。

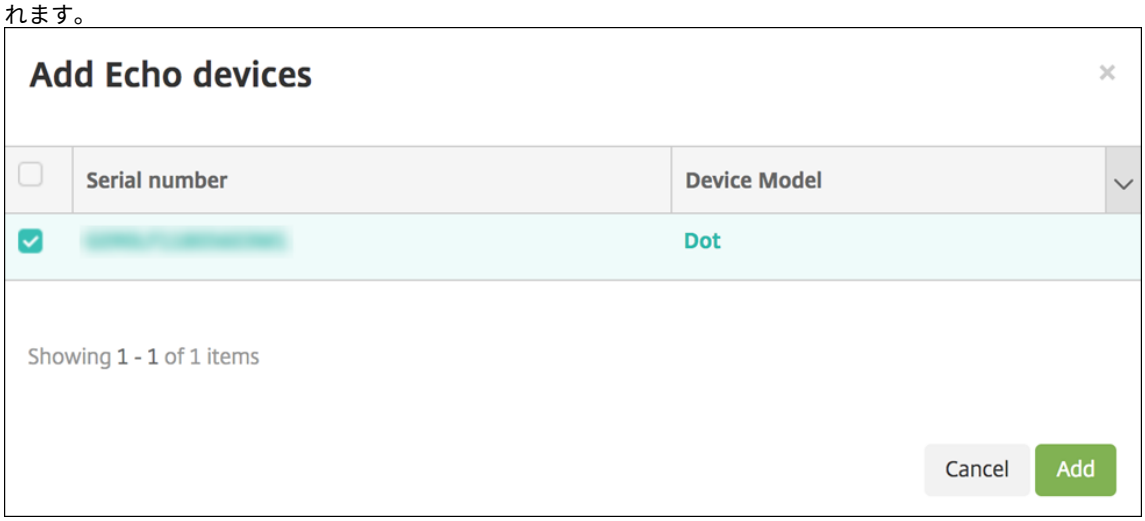


2. ルームを追加するには、［追加］をクリックします。ルームを編集するには、対象のルームを選択して ［編集］をクリックします。
3. 次のルーム設定を入力します：

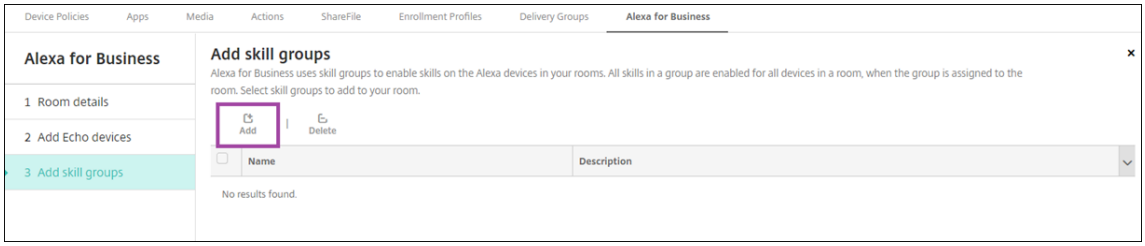


- ルーム名：会議室や面会室などの部屋の名前を入力します。
- ルームのカレンダーメール：ルームのカレンダーメールのアドレスを入力します。
- ルームプロファイル：このルームに使用するルームプロファイル構成の名前を選択します。

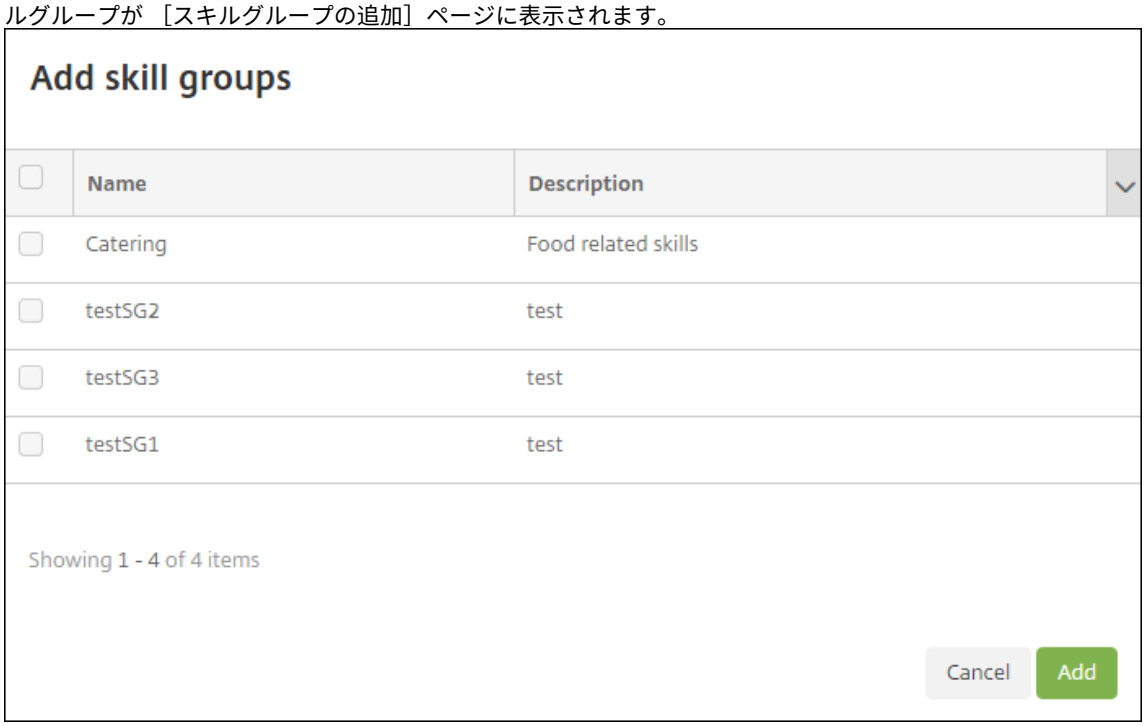
4. ［次へ］をクリックします。
5. ルームに Alexa デバイスを関連付けるには、［追加］をクリックします。
6. デバイスを選択し、［追加］をクリックします。選択したデバイスが ［**Echo** デバイスの追加］ページに表示されます。



7. ［次へ］をクリックします。
8. ルームの Alexa デバイスにスキルグループを追加するには、［追加］をクリックします。



9. ルームの Alexa デバイスに追加するスキルグループを選択します。［追加］をクリックします。選択したスキルグループが ［スキルグループの追加］ページに表示されます。

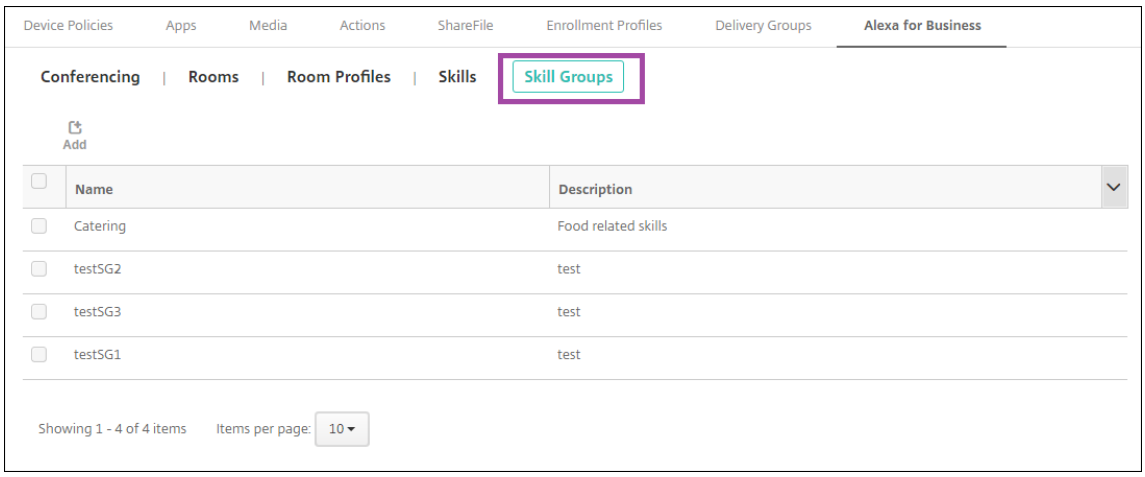


10. ［保存］をクリックします。

スキルグループを構成する

スキルグループは、ルームに適用するスキルをまとめたものです。スキルグループを作成して、ルームに割り当てることができます。スキルを使用することで、Alexa デバイスでオンライン会議の開始や終了、予定項目の一覧の確認などを行えます。スキルグループは追加、編集、削除できます。

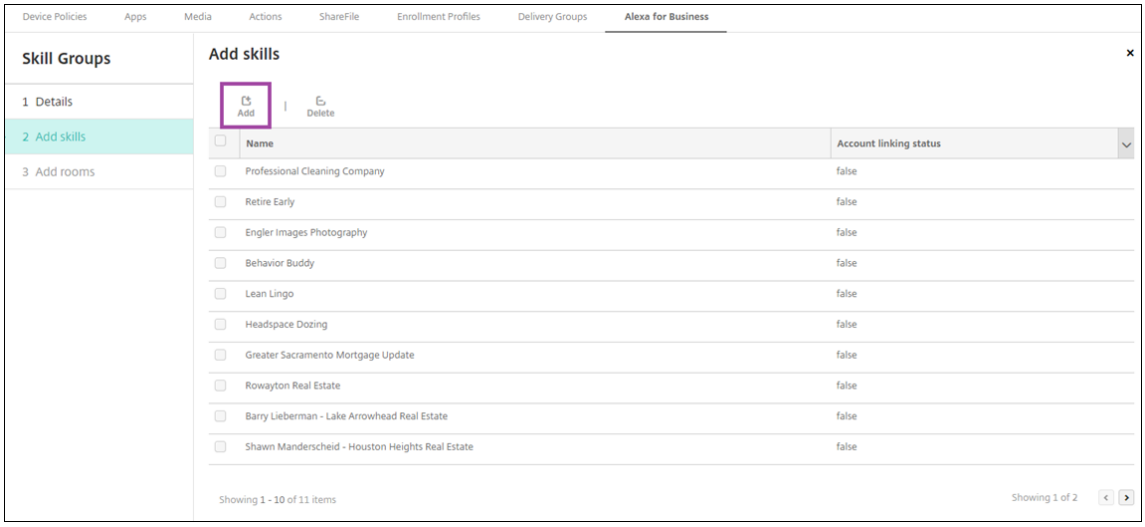
1. Citrix Endpoint Management コンソールで、［構成］**>** ［**Alexa for Business**］**>** ［スキルグループ］の順に選択します。使用可能なスキルグループの一覧が表示されます。



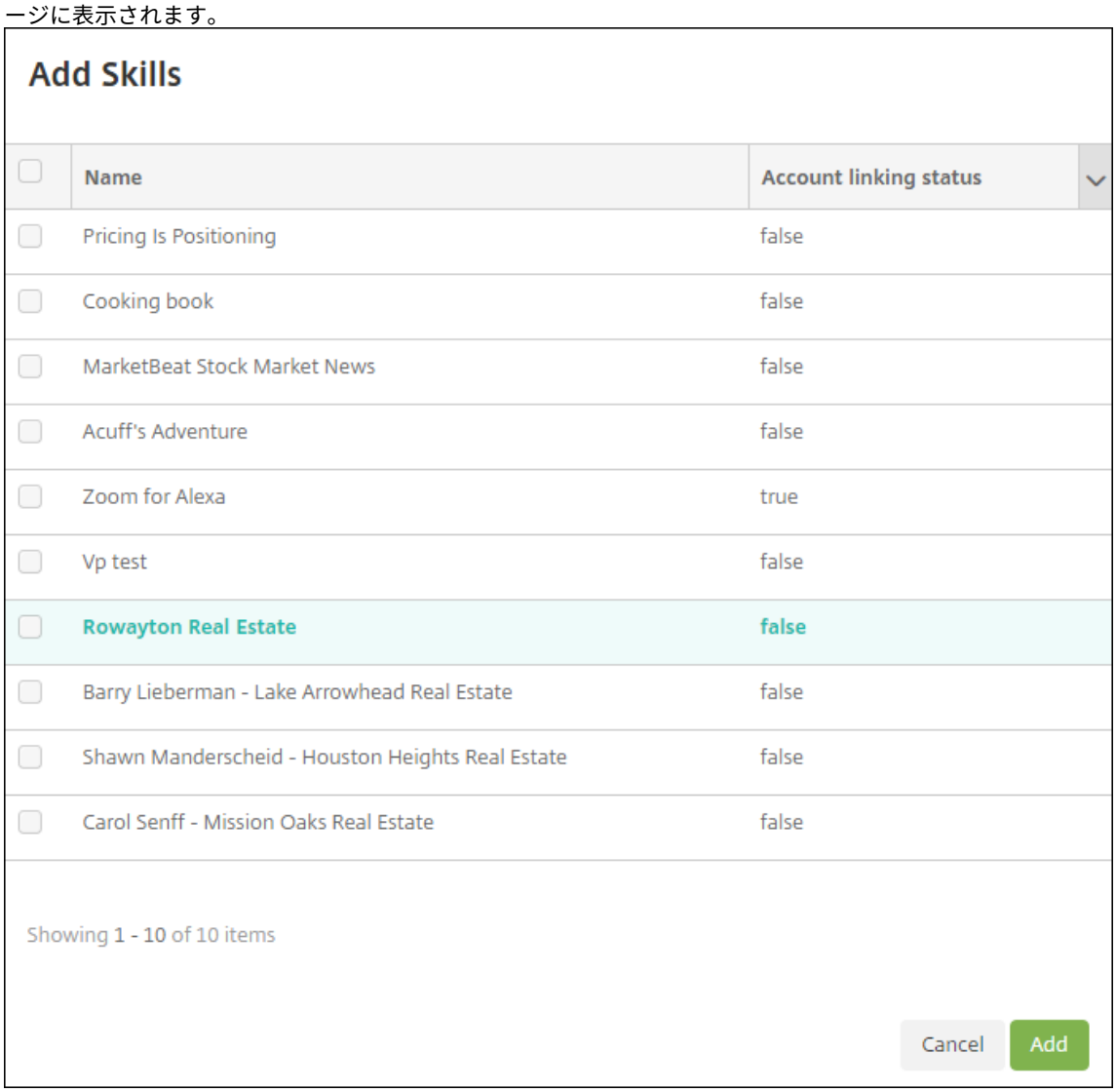
2. スキルグループを追加するには、［追加］をクリックします。スキルグループを編集するには、対象のスキルグループを選択して ［編集］をクリックします。
3. 次のスキルグループの設定を入力します：

   - 名前：スキルグループの名前を入力します。
   - 説明：スキルグループの簡単な説明を入力します。

4. ［次へ］をクリックします。
5. スキルグループにスキルを追加するには、［追加］をクリックします。

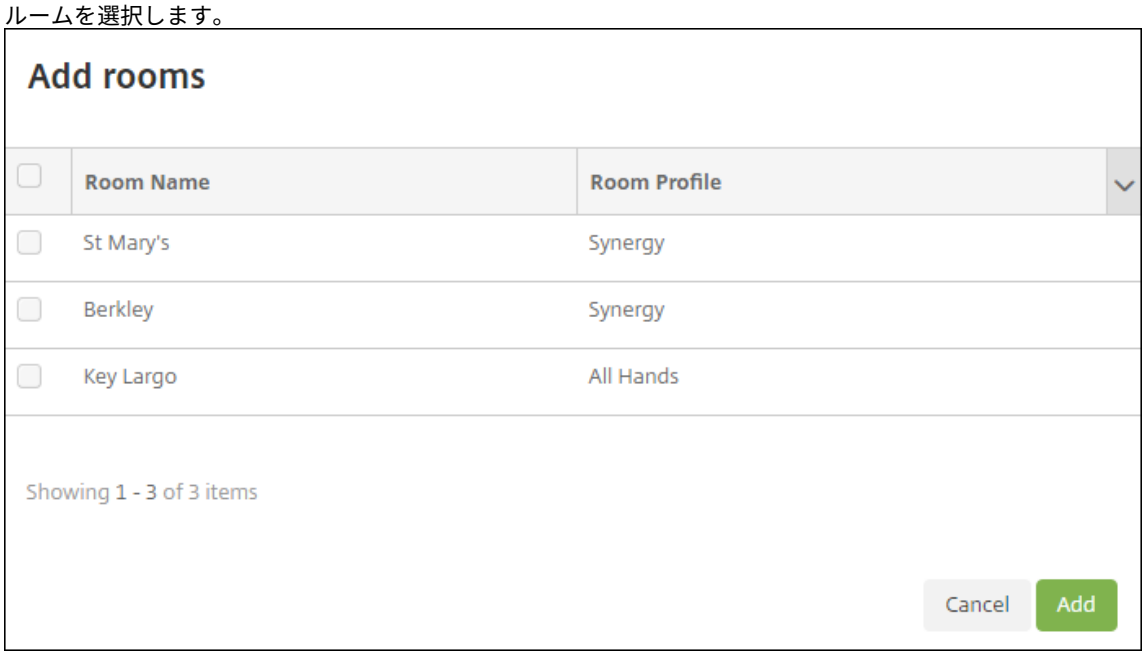


6. スキルグループに含めるスキルを選択して ［追加］をクリックします。選択したスキルが ［スキルの追加］ページに表示されます。



7. 特定のルームの Alexa デバイスにスキルグループを追加するには、［追加］をクリックします。

8. ルームを選択します。



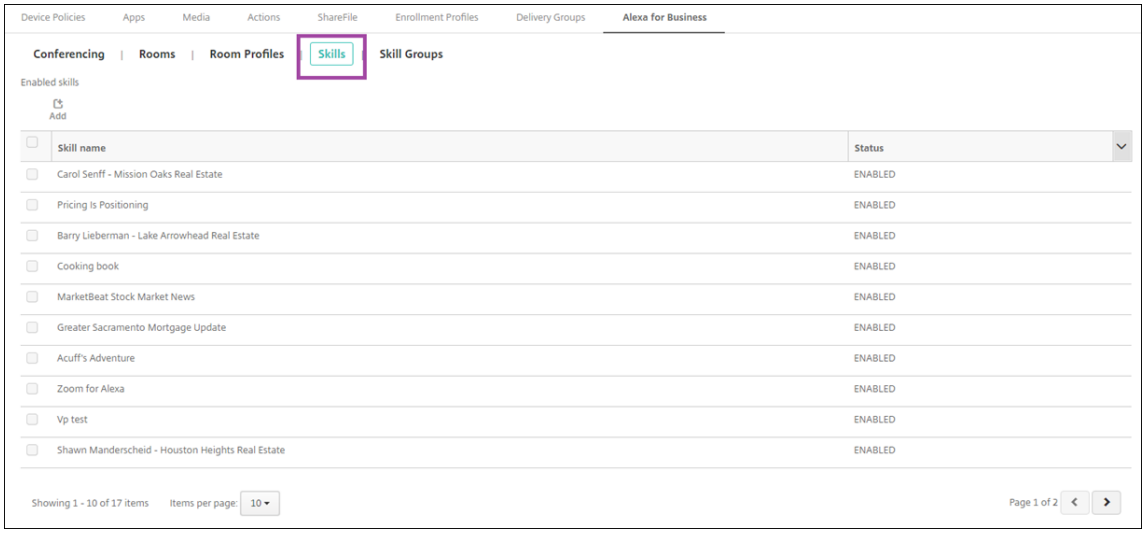
9. ［保存］をクリックします。

スキルグループでスキルを使用可能にする

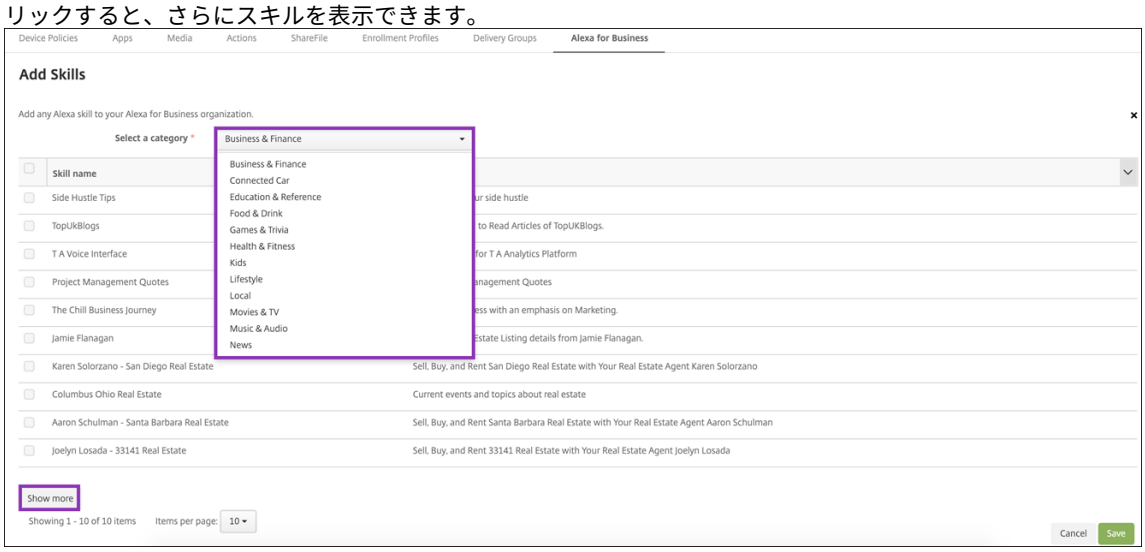
所属している Alexa for Business 組織のスキルグループに追加する使用可能な Alexa スキル一覧を構成します。これらのスキルはパブリックな Alexa スキルストアで利用可能なものか、対象組織専用のプライベートスキルです。

組織にスキルを追加

1. Citrix Endpoint Management コンソールで、［構成］**>** ［**Alexa for Business**］**>** ［スキル］の順に選択します。有効なスキルの一覧が表示されます。



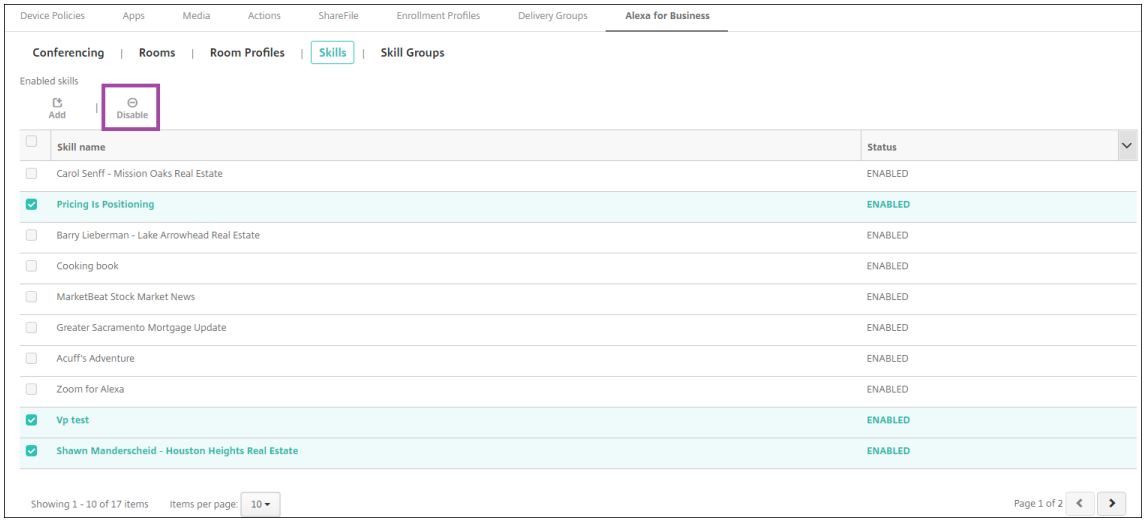
2. スキルを追加するには、［追加］をクリックします。
3. さらに Alexa スキルを表示するには、カテゴリを選択して ［詳細表示］をクリックします。［詳細表示］をクリックすると、組織で利用できるスキル一覧に最大 10 の追加スキルを表示できます。再度 ［詳細表示］をクリックすると、さらにスキルを表示できます。



4. 組織に追加するスキルを選択します。
5. ［保存］をクリックします。

組織からスキルを削除

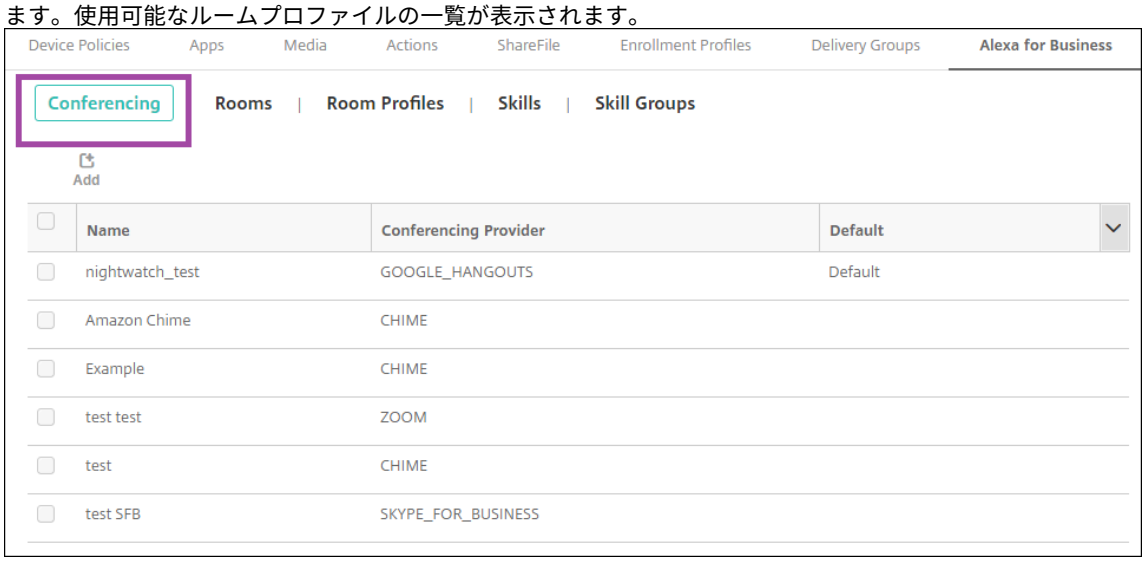
1. Citrix Endpoint Management コンソールで、［構成］**>** ［**Alexa for Business**］**>** ［スキル］の順に選択します。有効なスキルの一覧が表示されます。
2. 組織から削除するスキルを選択します。
3. ［無効化］をクリックします。



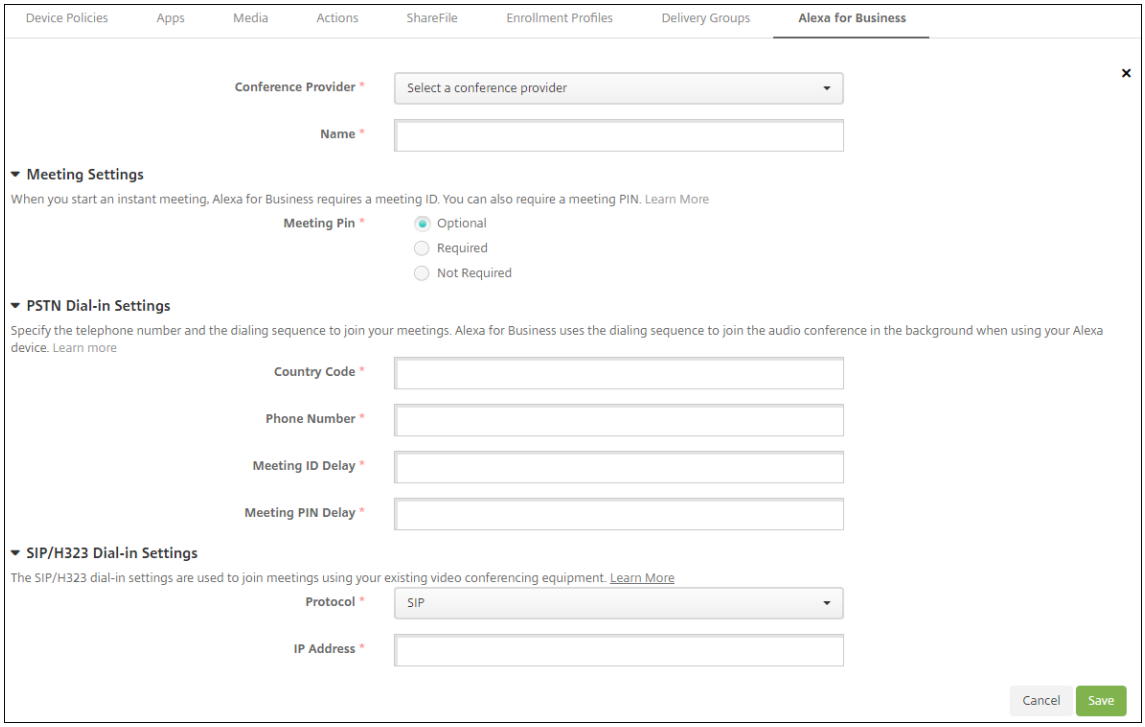
会議を構成

会議機能では、Alexa デバイスが含まれるルームの会議への参加方法を制御する Google Hangout や Amazon Chime のような会議プロバイダーを構成できます。会議プロバイダーは追加、編集、削除できます。デフォルトの会議プロバイダーを設定することもできます。

1. Citrix Endpoint Management コンソールで、［構成］**>**［**Alexa for Business**］**>**［会議］の順に選択します。使用可能なルームプロファイルの一覧が表示されます。



2. 会議プロバイダーを追加するには、［追加］をクリックします。会議プロバイダーを編集するには、対象のルームプロファイルを選択して ［編集］をクリックします。
3. 次のルームプロファイルの設定を入力します:



- 会議プロバイダー：一覧から会議プロバイダーを選択します。
- 名前：会議プロバイダーに指定する名前を入力します。
- 会議 **PIN**：会議に参加するために PIN が必要かを指定します。
- **PSTN** ダイヤルイン設定
  - 国コード：国コードを入力します。
  - 電話番号：電話番号を入力します。
  - 会議 **ID** の遅延：会議 ID が送信されるまでの秒数を指定します。
  - 会議 **PIN** の遅延： PIN が送信されるまでの秒数を指定します。
- **SIP/H323** ダイヤルイン設定 SIP/H323 ダイヤルイン設定は、既存のビデオ会議機器から会議に参加する場合に使用します。
  - **Protocol**：プロトコルを選択します
  - **IP** アドレス： IP アドレスを入力します。

4. ［保存］をクリックします。

複数の会議プロバイダーを構成する場合は、デフォルトのプロバイダーを設定します。

1. Citrix Endpoint Management コンソールで、［構成］**>** ［**Alexa for Business**］**>** ［会議］の順に選択します。使用可能なルームプロファイルの一覧が表示されます。
2. デフォルトとして設定する会議プロバイダーを選択します。
3. ［デフォルトを設定］をクリックします。

Device Administration から **Android Enterprise** への移行

November 29, 2023

この記事では、従来の Android デバイス管理から Android Enterprise への移行に関する考慮事項と推奨事項について説明します。Google は Android Device Administration API を廃止します。この API は、Android デバイス上のエンタープライズアプリをサポートしていました。Android Enterprise は、Google と Citrix が推奨する最新の管理ソリューションです。

Citrix Endpoint Management は Android Enterprise に変更され、これが Android デバイスのデフォルトの登録方法となります。Google がこの API を廃止した後は、Android Q デバイスはデバイス管理モードで登録できなくなります。

Android Enterprise では、完全管理デバイスモードと仕事用プロファイルデバイスモードがサポートされます。Google のドキュメント『Android Enterprise Migration Bluebook』で、従来のデバイス管理と Android Enterprise の違いについて詳しく説明しています。Google が提供する移行に関する情報を参照していただくことをお勧めします。

Citrix Tech Zone の記事「Citrix Endpoint Management を使用した Android Device Administrator から Android Enterprise への移行」も参照することをお勧めします。

デバイス管理の廃止の影響

Google は Device Administrator API を廃止し、2020 年 11 月 2 日をもってサポートを停止します。これらの API は、Citrix Secure Hub をターゲット Android API レベル 29 にアップグレードした後、Android 10 以降を実行しているデバイスでは機能しません。

- カメラの無効化：デバイスのカメラへのアクセスを制御します。
- **Keyguard** 機能：生体認証やパターンなど、デバイスのロックに関連する機能を制御します。
- パスワードの有効期限切れ：構成した期間が過ぎると、ユーザーはパスワードの変更を強制されます。
- パスワードの制限：パスワードの制限の要件を設定します。

要件と推奨事項

- デバイスを Android 10 以降にアップグレードできる場合、そのデバイスを Android Enterprise に登録する必要があります。
  - Android 11 デバイスを Android Enterprise に登録する必要があります。
  - 2020 年 9 月時点での Android 10 デバイスの場合：デバイス管理モードへの新規登録またはデバイスの再登録は Citrix ではサポートされていません。前のセクションで説明したように、既に登録されているデバイスは 2020 年 11 月 2 日まで引き続き機能します。

- Android 9 以前を実行しているデバイスの場合、従来のデバイス管理モードをサポートします。ただし、これらのデバイスをできるだけ早く Android Enterprise に移行することをお勧めします。
- Citrix MAM-only モードで登録された新規または既存のデバイスの場合、対応は不要です。この Google API の廃止は、MAM-only モードのデバイスには影響ありません。ただし、プラットフォーム暗号化への移行に伴い、MAM-only モードから Android Enterprise 仕事用プロファイルモード（BYOD）に移行することを強くお勧めします。仕事用プロファイルモードは MAM 機能を提供します。ただし、デバイスのコンテナにおいてです。

分析

移行の分析フェーズでは以下を行います：

- 従来の Android 設定を把握する
- 従来の機能と Android Enterprise の機能をマッピングできるように、従来の設定を文書化する

推奨される分析

1. Citrix Endpoint Management 上で Android Enterprise を評価します：完全管理、仕事用プロファイルでの完全管理、専用デバイス、仕事用プロファイル（BYOD）。
2. 現在のデバイス管理機能を Android Enterprise と比較して分析します。
3. デバイス管理のユースケースを文書化します。

デバイス管理のユースケースを文書化するには：

1. スプレッドシートを作成し、Citrix Endpoint Management コンソールに現在のポリシーグループを表示します。
2. 既存のポリシーグループに基づいて個別のユースケースを作成します。
3. ユースケースごとに、以下を文書化します：
    - Name
    - ビジネス責任者
    - ユーザー ID モデル
    - デバイスの要件
        - セキュリティ
        - 管理
        - 使いやすさ
    - デバイスインベントリ
        - 製造元とモデル

    - OS のバージョン
  - アプリ

4. アプリごとに、以下を示します:

   - アプリ名
   - パッケージ名
   - ホスティング方法
   - アプリがパブリックかプライベートか
   - アプリが必須かどうか（真/偽）

要件マッピング

分析結果に基づいて、Android Enterprise の機能要件を決定します。

推奨される要件マッピング

1. 管理モードと登録方法を決定します:

   - 仕事用プロファイル（BYOD）: 再登録が必要です。工場出荷時リセットは不要です。
   - 完全管理: 工場出荷時リセットが必要です。QR コード、近距離無線通信（NFC）バンプ、デバイスポリシーコントローラー（DPC）ID、ゼロタッチを使用してデバイスを登録します。

2. アプリの移行戦略を作成します。
3. ユースケース要件を Android Enterprise 機能にマッピングします。要件とそれに対応する Android バージョンに最も一致するデバイス要件ごとに機能を文書化します。
4. 機能要件に基づいて Android の最小 OS を決定します（7.0、8.0、9.0）。
5. ID モデルを選択します:

   - 推奨: managed Google Play アカウント
   - Google Cloud Identity のお客様の場合のみ、Google Workspace アカウントを使用します。

6. デバイス戦略を作成します:

   - アクションなし: デバイスが最小 OS レベル要件を満たしている場合
   - アップグレード: デバイスがサポート対象 OS をサポートしており、それに更新できる場合
   - 置換: デバイスをサポート対象 OS レベルに更新できない場合

推奨されるアプリ移行戦略

要件のマッピングが完了したら、アプリを Android プラットフォームから Android Enterprise プラットフォームに移行します。アプリの公開の詳細については、「アプリの追加」を参照してください。

- パブリックストアアプリ

  1. 移行するアプリを選択し、アプリを編集して Google Play 設定をクリアし、プラットフォームとして［**Android Enterprise**］を選択します。
  2. デリバリーグループを選択します。アプリが必須の場合、デリバリーグループの ［必須アプリ］リストにアプリを移行します。

  アプリを保存すると、Google Play ストアに表示されます。仕事用プロファイルがある場合、アプリは仕事用プロファイルの Google Play ストアに表示されます。

- プライベート（エンタープライズ）アプリ

  プライベートアプリは、社内で開発されるか、サードパーティの開発者によって開発されます。Google Play を使用してプライベートアプリを公開することをお勧めします。

  1. 移行するアプリを選択し、アプリを編集して、プラットフォームとして ［**Android Enterprise**］を選択します。
  2. APK ファイルをアップロードし、アプリの設定を構成します。
  3. 必要なデリバリーグループにアプリを公開します。

- MDX アプリ

  1. 移行するアプリを選択し、アプリを編集して、プラットフォームとして ［**Android Enterprise**］を選択します。
  2. MDX ファイルをアップロードします。アプリの承認プロセスを実行します。
  3. MDX ポリシーを選択します。

  エンタープライズ MDX アプリの場合、MDX に変更することをお勧めします。SDK モードのラップされたアプリ:

  - オプション 1: 組織に非公開で割り当てられた開発者アカウントを使用して、Google Play で APK をホストする。Citrix Endpoint Management で MDX ファイルを公開します。
  - オプション 2: Citrix Endpoint Management からエンタープライズアプリとしてアプリを公開する。Citrix Endpoint Management で APK を公開し、MDX ファイルのプラットフォームに ［**Android Enterprise**］を選択します。

Citrix デバイスポリシーの移行

Android（従来のデバイス管理者）プラットフォームと **Android Enterprise** プラットフォームの両方で使用可能なポリシーの場合：ポリシーを編集してプラットフォーム ［**Android Enterprise**］を選択します。

- Android Enterprise の場合、デバイスの登録方法を検討してください。一部のポリシーオプションは、仕事用プロファイルモードまたは完全管理モードのデバイスでのみ使用できます。「Android Enterprise デバイスポリシーとアプリポリシーの構成」を参照してください。
- 従来のデバイス管理者（DA）デバイスに Exchange デバイスポリシーを使用する場合は、代わりに［管理対象の構成］デバイスポリシーを作成して、メール設定を構成します。
- ポリシーで目的のデバイス（Android Enterprise か従来のデバイス管理者）を確実に対象にするには、ポリシーに展開規則を追加します。たとえば、従来のデバイス管理者プラットフォームの場合、次の展開規則を使用します：

  ```
  1  Limit by known device property name Android Enterprise
  2  Enabled Device? Isn' t equal to true
  3  <!--NeedCopy-->
  ```

  この展開規則は、デバイスが Android Enterprise に対して有効になっていないことを確認し、従来のデバイス管理者が有効になっているデバイスにアプリとともにポリシーを配信します。

概念実証

アプリを Android Enterprise に移行したら、意図したとおりに機能することを確認するための移行テストを設定できます。

推奨の概念実証設定

1. 展開インフラストラクチャを設定します：
   - Android Enterprise テスト用のデリバリーグループを作成します。
   - Citrix Endpoint Management で Android Enterprise を構成します。
2. ユーザーアプリを設定します。
3. Android Enterprise 機能を構成します。
4. ポリシーを Android Enterprise デリバリーグループに割り当てます。
5. 機能をテストして確認します。
6. ユースケースごとにデバイスセットアップウォークスルーを実行します。
7. ユーザーのセットアップ手順を文書化します。

展開

これで、Android Enterprise セットアップを展開し、ユーザーの移行準備ができました。

推奨される展開戦略

Citrix は展開戦略として、Android Enterprise の実稼働システムをすべてテストした後で、デバイスを移行することを推奨します。

- このシナリオでは、ユーザーは従来のデバイスを最新の構成で使い続けることができます。Android Enterprise 管理用に新しいデバイスをセットアップします。
- アップグレードまたは交換が必要な場合にのみ、既存のデバイスを移行します。
- 通常のライフサイクルの最後に、既存のデバイスを Android Enterprise 管理に移行します。または、紛失や破損のために交換が必要な場合にデバイスを移行します。

Android Enterprise

March 15, 2024

Android Enterprise は、Google が Android デバイス用のエンタープライズ管理ソリューションとして提供するツールとサービスのセットです。Android Enterprise では:

- Citrix Endpoint Management を使用して、会社所有の Android デバイスとユーザー所有の（BYOD）Android デバイスを管理します。
- デバイス全体を管理することも、デバイス上の個別のプロファイルを管理することもできます。この個別のプロファイルでは、ビジネス用のアカウント、アプリ、データが個人のアカウント、アプリ、データと分離されています。
- 在庫管理など、特定目的専用のデバイスを管理することもできます。Google による Android Enterprise で実行できることの概要については、「Android Enterprise 管理」を参照してください。

リソース:

- Android Enterprise に関連する用語と定義の一覧については、「Google Android Enterprise 開発者ガイド」の記事のAndroid Enterprise terminologyを参照してください。Google はこれらの用語を頻繁に更新します。
- Citrix Endpoint Management でサポートされている Android のオペレーティングシステムについては、「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。
- Android Enterprise のネットワーク環境設定時に考慮すべき発信接続については、Google のサポート記事Android Enterprise Network Requirementsを参照してください。

- Android Enterprise の展開については、「リソースの展開」を参照してください。

Android Enterprise の使用開始

> 重要:
>
> デバイス管理モードはサポートされなくなりました。ユーザーがデバイス管理モードのデバイスを使用している場合は、「デバイス管理から Android Enterprise への移行」を参照してください。デバイスを Android Enterprise に移行した後、次の手順で Android Enterprise デバイスをセットアップします。

ワンタイムセットアップ

1. 管理対象の Google Play アカウントを作成します。

   「Citrix Endpoint Management で管理対象 Google Play を使用する」および「要件」を参照してください。

2. Google Play アカウントを Citrix Endpoint Management にバインドします。

   「Citrix Endpoint Management を Google Play に接続する」を参照してください。

3. デバイスの管理方法を計画します。

   「デバイス展開シナリオとプロファイル」を参照してください。

4. ユーザーデバイスの登録セキュリティを計画します。

   「登録セキュリティ」を参照してください。

5. MDX 対応アプリを提供する準備をします。

   MAM SDK を使用してアプリを開発します。または、新しい SDK に移行する準備ができていない場合は、コマンドラインベースの MDX Toolkit を使用してアプリをラップします。

   「MAM SDK の概要」を参照してください。

この時点で、Android Enterprise デバイスをアプリとデバイスのポリシー、登録プロファイル、およびアプリで構成する準備が整いました。ガイダンスについては、次のセクションを参照してください。

デバイスの構成

1. デリバリーグループを作成します。

   誰がどのリソースをいつ取得するかを制御します。「リソースの展開」を参照してください。

   従来の DA プラットフォーム用に公開されたアプリの Android Enterprise 登録済みデバイスへの配信を停止します。Android Enterprise デバイスの場合、Android Enterprise プラットフォーム用のアプリを公開します。従来の DA アプリを DA モードのデバイスに引き続き公開するには、それらのアプリ用に別のデリバリーグループを作成します。「廃止」を参照してください。

2. アプリの追加 Google Play アプリは Citrix Endpoint Management コンソールから直接承認できます。

   Google のサポート記事、Manage apps in your organizationを参照してください。

3. 登録プロファイルを作成します。

   デバイスとアプリの管理登録オプションを指定します。「デバイス展開シナリオとプロファイル」および「登録プロファイルの作成」を参照してください。

   - Android Enterprise パブリックアプリストアのアプリを Android デバイスユーザーに展開すると、そのユーザーは自動的に Android Enterprise に登録されます。
   - ゼロタッチ登録でデバイスを構成し、最初に電源をオンにしたときに自動で登録できるようにします。「ゼロタッチ登録」を参照してください。

4. デバイスとアプリのポリシーを構成します。

   エンタープライズセキュリティとユーザープライバシーおよびユーザーエクスペリエンスのバランスを取ります。「Android Enterprise デバイスポリシーとアプリポリシーの構成」を参照してください。

5. Apple アプリを配布します。

   ビジネス向け Google Play を使用して、アプリを追加、購入、および承認し、デバイスの Android Enterprise ワークスペースに展開します。ユーザーは管理者が利用可能にした管理対象 Google Play のみからアプリをインストールできます。

   参照:

   - Android Enterprise アプリの配布
   - 管理対象の構成ポリシー
   - アプリの権限ポリシー

6. コンプライアンスを監視および確認するためのセキュリティアクションを構成します。

   「セキュリティ操作」を参照してください。

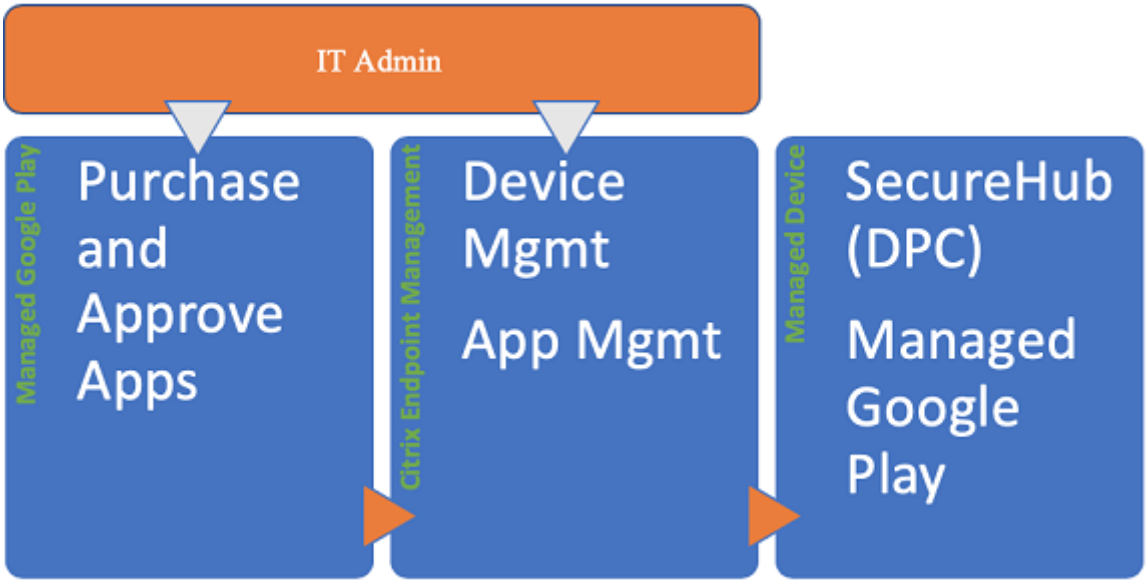
Citrix Endpoint Management で管理対象 Google Play を使用する

Citrix Endpoint Management を管理対象 Google Play と統合して Android Enterprise を使用する場合、エンタープライズを作成します。Google はエンタープライズを、組織とエンタープライズモバイル管理（EMM）ソリューションとの間のバインディングと定義しています。組織がソリューションを通して管理するすべてのユーザーとデバイスは、そのエンタープライズに属します。

Android Enterprise のエンタープライズには、EMM ソリューション、デバイスポリシーコントローラー（DPC）アプリ、および Google エンタープライズアプリプラットフォームの 3 つのコンポーネントがあります。Citrix Endpoint Management を Android Enterprise と統合すると、完成されたソリューションには次のコンポーネントが含まれます:

- **Citrix Endpoint Management**: Citrix EMM。Citrix Endpoint Management は、安全なデジタルワークスペースのための統合された Citrix Endpoint Management です。Citrix Endpoint Management は、IT 管理者が組織のデバイスとアプリを管理する手段を提供します。
- **Citrix Secure Hub**: Citrix DPC アプリ。Citrix Secure Hub は、Citrix Endpoint Management のランチパッドです。Citrix Secure Hub はデバイスにポリシーを適用します。
- 管理対象 **Google Play**: Citrix Endpoint Management と統合する Google エンタープライズアプリプラットフォーム。Google Play EMM API がアプリポリシーを設定し、アプリを配布します。

次の図に、管理者がこれらのコンポーネントとやり取りする方法と、コンポーネントが互いにやり取りする方法を示します:



> 注:
>
> 管理対象 Google Play または Google Workspace（旧称：G Suite）を使用して、Citrix を EMM プロバイダーとして Google Play に登録できます。この記事では、管理対象 Google Play で Android Enterprise を使用する方法について説明します。組織が Google Workspace を使用してアプリへのアクセスを提供している場合、Android Enterprise で使用できます。「Google Workspace ユーザー向けの従来の Android Enterprise」を参照してください。

管理対象 Google Play を使用する場合、デバイスおよびエンドユーザーに管理対象 Google Play アカウントをプロビジョニングします。管理対象 Google Play アカウントは、管理対象 Google Play へのアクセスを提供し、管理者が利用可能にしたアプリをユーザーがインストールし、使用できるようにします。組織がサードパーティの ID サービスを使用する場合、ビジネス向け Google Play アカウントと既存の ID アカウントを関連付けることができます。

この種類のエンタープライズはドメインに関連付けられていないため、1 つの組織用に 1 つまたは複数のエンタープライズを作成できます。たとえば、組織の各部門または各地域は異なるエンタープライズとして登録できます。さまざまなエンタープライズを使用すると、デバイスおよびアプリを個別セットとして管理できます。

Citrix Endpoint Management の管理者のために、管理対象 Google Play では、使い慣れた Google Play のユーザーエクスペリエンスとアプリストアの機能が、エンタープライズ向けに設計された管理機能セットと組み合わされています。ビジネス向け Google Play を使用して、アプリを追加、購入、および承認し、デバイスの Android Enterprise ワークスペースに展開します。Google Play を使用してパブリックアプリ、プライベートアプリ、およびサードパーティアプリを展開できます。

管理対象デバイスのユーザーの場合、管理対象 Google Play がエンタープライズアプリストアです。ユーザーは、アプリの閲覧、アプリの詳細の表示、アプリのインストールを実行できます。Google Play のパブリックバージョンとは異なり、ユーザーは管理者が利用可能にしたアプリのみをビジネス向け Google Play からインストールできます。

デバイス展開シナリオとプロファイル

デバイス展開シナリオは、展開するデバイスの所有者とデバイスの管理方法を示します。デバイスプロファイルは、DPC がデバイスのポリシーを管理および適用する方法を示します。

この仕事用プロファイルでは、ビジネス用のアカウント、アプリ、データが個人のアカウント、アプリ、データと分離されています。仕事用プロファイルと個人用プロファイルは、OS レベルで分離されています。仕事用プロファイルについて詳しくは、「仕事用プロファイルとは」を参照してください。

> 重要:
>
> Android Enterprise デバイスを Android 11 に更新すると、Google は［仕事用プロファイルで完全に管理］に設定された管理対象デバイスを、セキュリティが強化された新しい仕事用プロファイルエクスペリエンスに移行します。新しい登録モードは、「会社所有のデバイスの仕事用プロファイル」と呼ばれます。詳しくは、Android Enterprise の［仕事用プロファイルで完全に管理］への変更を参照してください。
> Android 12 デバイスの場合、仕事用プロファイルのセキュリティとプライバシーの強化を参照してください。

デバイス管理	使用例	仕事用プロファイル	個人プロファイル	メモ
会社所有のデバイス（完全管理対象）	仕事での使用のみを目的とした会社所有のデバイス	番号	番号	新規または出荷時設定のデバイスのみ。「Android Enterprise の完全に管理されたデバイスのプロビジョニング」を参照してください。
仕事用プロファイルで完全に管理/会社所有のデバイスの仕事用プロファイル	仕事と個人での使用を目的とした会社所有のデバイス	はい	はい。これらのデバイスで実行される DPC の 2 つのコピー：1 つはデバイス所有者モードでデバイスを管理し、もう 1 つはプロファイル所有者モードで仕事用プロファイルを管理します。デバイスと仕事用プロファイルに個別のポリシーを適用できます。	「Android Enterprise の完全に管理された仕事用プロファイルデバイスまたは会社所有のデバイスの仕事用プロファイルのプロビジョニング」を参照してください。

デバイス管理	使用例	仕事用プロファイル	個人プロファイル	メモ
専用デバイス *	デジタルサイネージやチケット印刷など、単一のユースケース用に構成された会社所有のデバイス	番号	番号	「Android Enterprise 専用デバイスのプロビジョニング」を参照してください。
BYOD/仕事用プロファイル **	仕事用プロファイル管理に登録されている個人用デバイス（プロファイル所有者モードとも呼ばれます）	はい	はい。DPC は、デバイス全体ではなく、仕事用プロファイルのみを管理します。	これらのデバイスは、新品または工場出荷時の設定にリセットする必要がありません。「Android Enterprise の仕事用プロファイルデバイスのプロビジョニング」を参照してください。

* ユーザーは専用デバイスを共有できます。ユーザーが専用デバイス上のアプリにサインオンすると、作業の状態はデバイスではなくアプリと連携します。

** Citrix Endpoint Management では、BYOD/仕事用プロファイルモードの Zebra デバイスはサポートされません。Citrix Endpoint Management は、Android Enterprise を使用して完全に管理された Zebra デバイスをサポートします。

登録セキュリティ

登録プロファイルで、Android デバイスを MAM、MDM、または MDM+MAM のいずれで登録するか、およびユーザーが MDM をオプトアウトするオプションを決定します。

セキュリティレベルの指定および必要な登録手順については、「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。

Citrix Endpoint Management は、MDM または MDM+MAM で登録した Android デバイスに対して、次の認証方法をサポートします。詳しくは、次の記事を参照してください：

- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- ID プロバイダー：
  - Citrix Cloud を介した Azure Active Directory での認証（プレビュー）
  - Citrix Cloud を介した Okta での認証（プレビュー）

使用頻度が少ない認証方法には、クライアント証明書とセキュリティトークンの組み合わせがあります。詳しくは、「https://support.citrix.com/article/CTX215200」を参照してください。

要件

Android Enterprise の使用を開始するには、以下が必要となります:

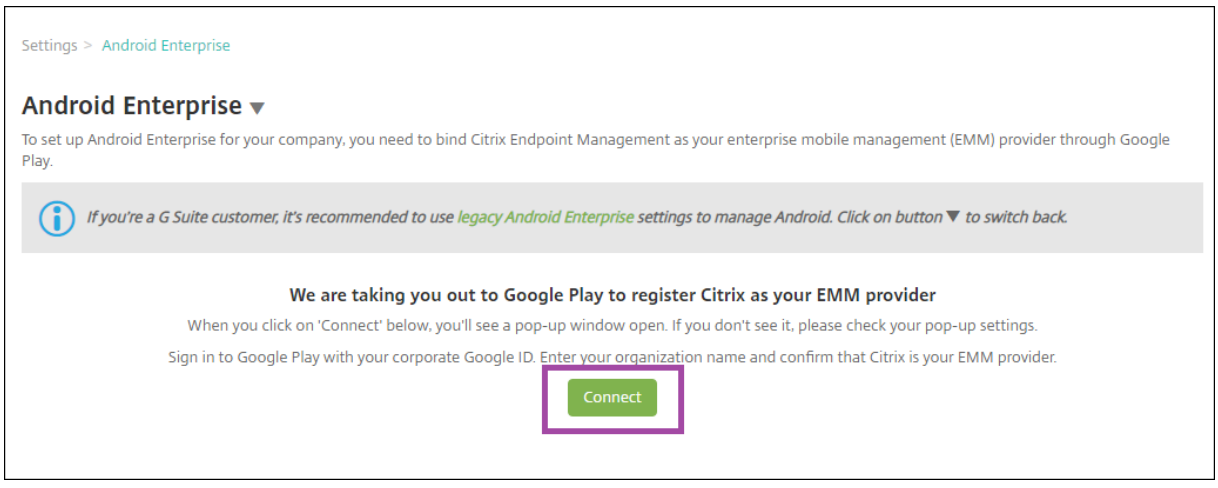
- アカウントと資格情報:
  - 管理対象 Google Play で Android Enterprise をセットアップする場合、企業 Google アカウント
  - 最新の MDX ファイルをダウンロードする場合、Citrix カスタマーアカウント
- Citrix Endpoint Management 用に構成された Firebase Cloud Messaging（FCM）および接続のスケジューリングデバイスポリシー。「Firebase Cloud Messaging」および「接続スケジューリングデバイスポリシー」を参照してください。

Citrix Endpoint Management を **Google Play** に接続する

組織の Android Enterprise をセットアップするには、管理対象 Google Play から Citrix を EMM プロバイダーとして登録します。これにより、管理対象 Google Play と Citrix Endpoint Management が接続され、Citrix Endpoint Management で Android Enterprise のエンタープライズが作成されます。

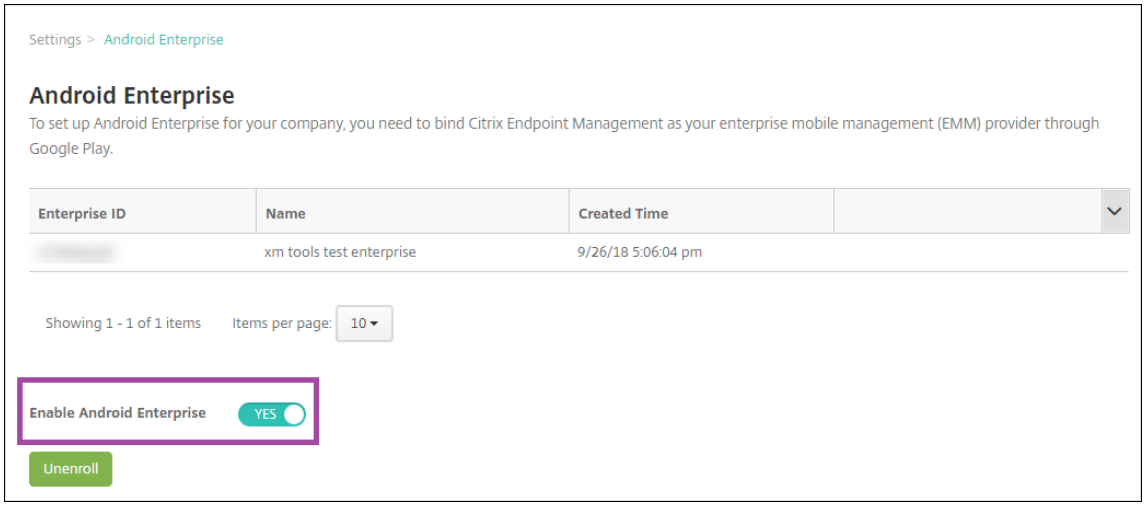
Google Play にサインインするための企業 Google アカウントが必要です。

1. Citrix Endpoint Management コンソールで、［設定］**>**［**Android Enterprise**］の順に移動します。
2. ［接続］をクリックします。Google Play が開きます。

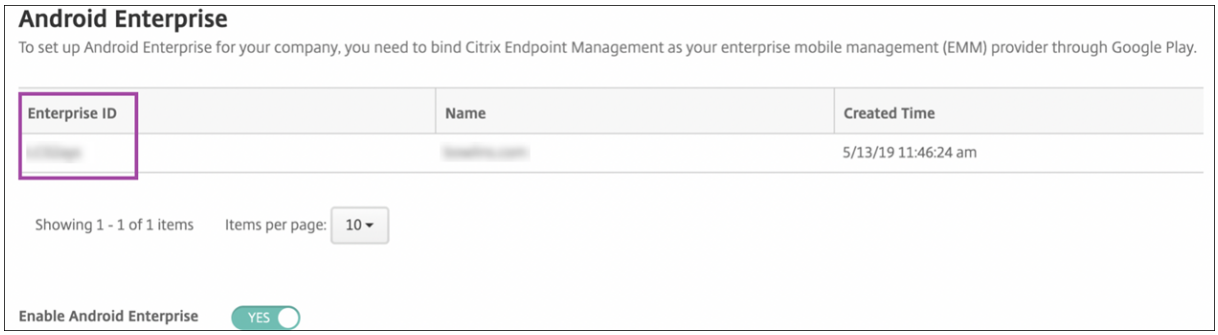


1. 企業 Google アカウントの資格情報で Google Play にサインインします。組織名を入力し、Citrix が EMM プロバイダーであることを確認します。

2. Android Enterprise にエンタープライズ ID が追加されます。Android Enterprise を有効にするには、［**Android Enterprise** の有効化］を ［はい］に切り替えます。



Citrix Endpoint Management コンソールにエンタープライズ ID が表示されます。



使用する環境が Google に接続され、デバイスを管理する準備ができます。これで、ユーザーにアプリを提供できるようになりました。

Citrix Endpoint Management を使用して、ユーザーに Citrix 業務用モバイルアプリ、MDX アプリ、パブリックアプリストアアプリ、Web および SaaS アプリ、エンタープライズアプリ、Web リンクを提供できます。これらの種類のアプリをユーザーに提供する方法について詳しくは、「Android Enterprise アプリの配布」を参照してください。

次のセクションでは、業務用モバイルアプリを提供する方法を示します。

Android Enterprise ユーザーに **Citrix** 業務用モバイルアプリを提供する

Android Enterprise ユーザーに Citrix 業務用モバイルアプリを提供するには、以下の手順を実行する必要があります。

1. アプリを MDX アプリとして公開します。「アプリを MDX アプリとして構成する」を参照してください。

2. ユーザーがデバイス上の仕事用プロファイルにアクセスするために使用するセキュリティ確認のルールを構成します。「セキュリティ確認ポリシーを構成する」を参照してください。

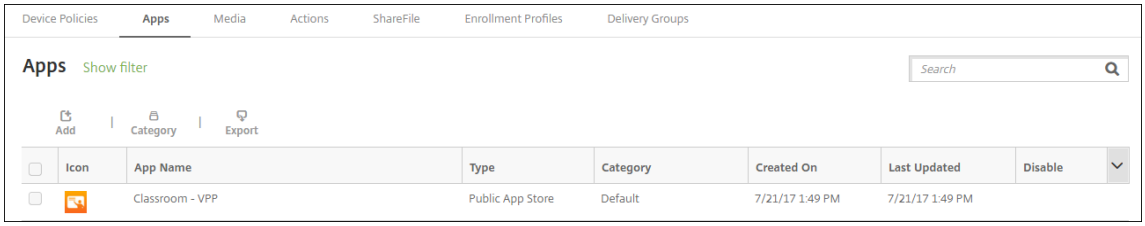
公開するアプリは、Android Enterprise エンタープライズに登録されているデバイスで利用できます。

> 注:
>
> Android Enterprise パブリックアプリストアのアプリを Android ユーザーに展開すると、そのユーザーは自動的に Android Enterprise に登録されます。

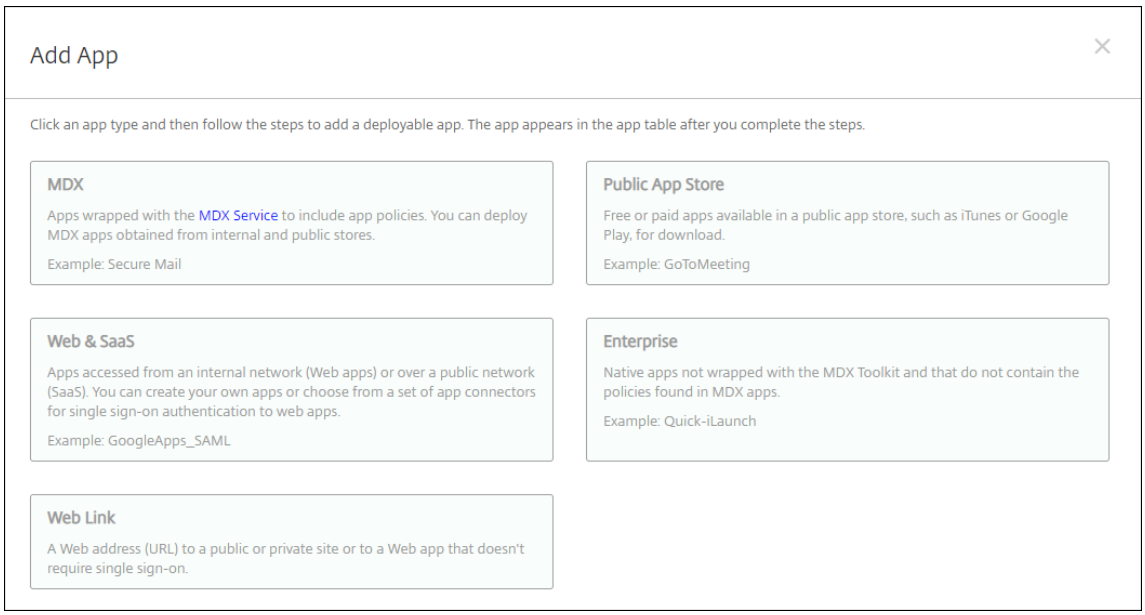
アプリを **MDX** アプリとして構成する

Citrix 業務用アプリを Android Enterprise 用の MDX アプリとして構成するには、次の手順を実行します:

1. Citrix Endpoint Management コンソールで、[構成] > [アプリ] の順にクリックします。[アプリ] ページが開きます。



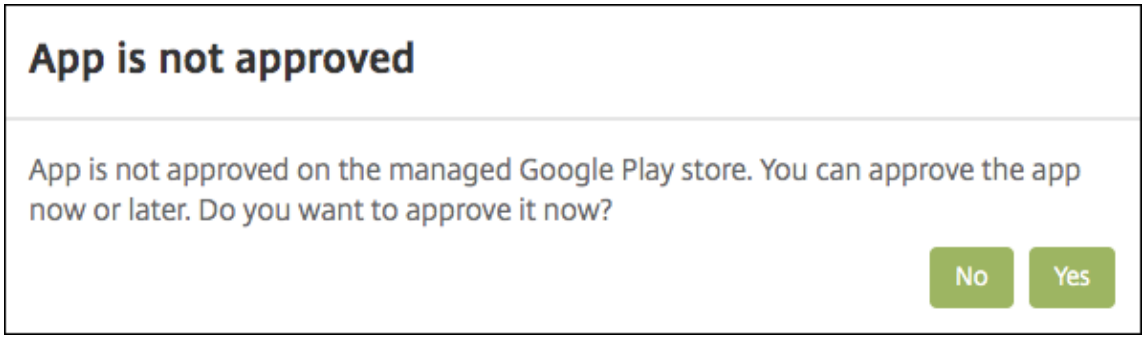
2. [追加] をクリックします。[アプリの追加] ダイアログボックスが開きます。



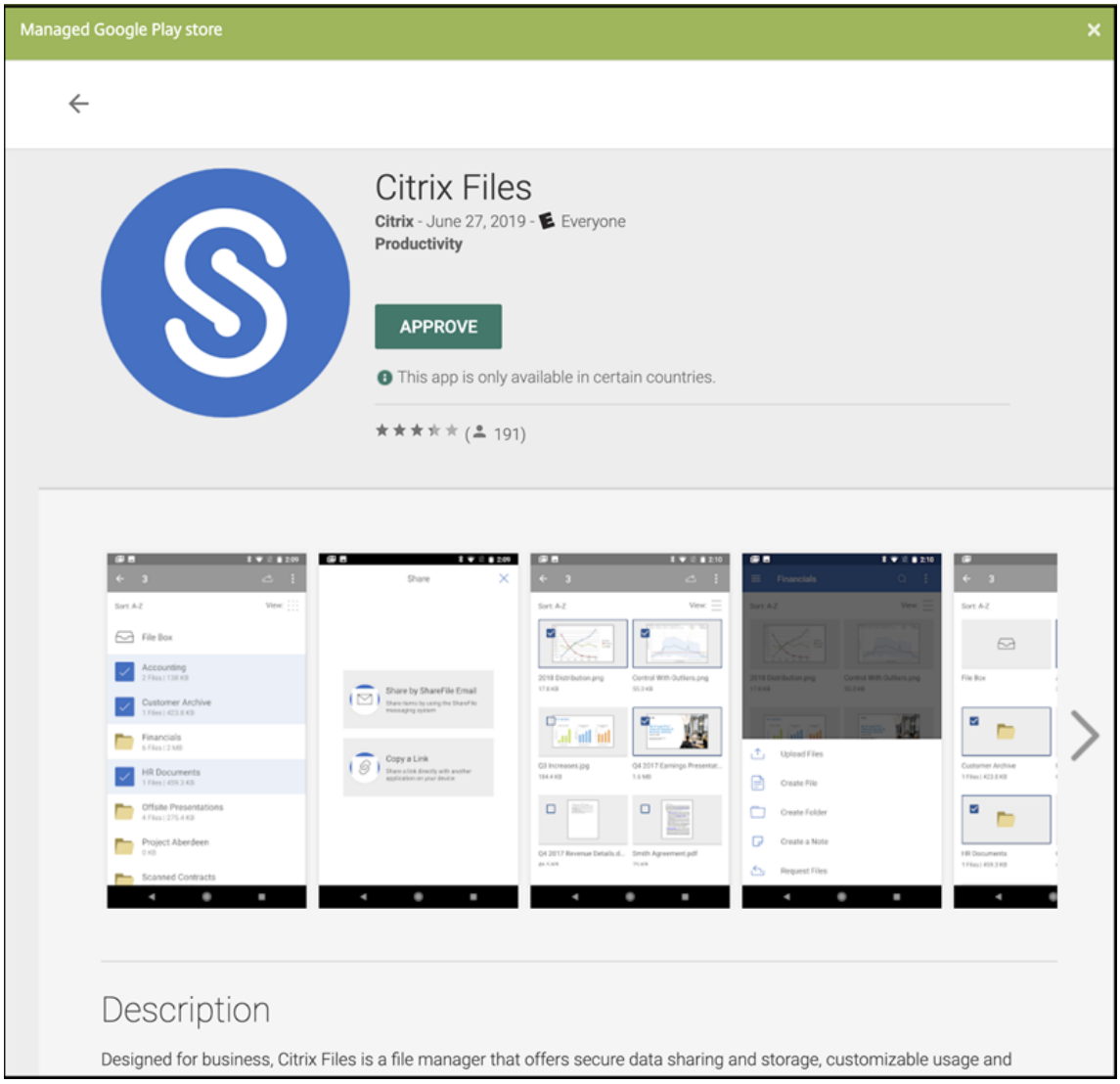
3. [**MDX**] をクリックします。[アプリ情報] ページが開きます。
4. ページの左側で、プラットフォームとして [**Android Enterprise**] を選択します。
5. [アプリケーション情報] ページで、以下の情報を入力します:

- 名前：アプリの説明的な名前を入力します。この名前は、［アプリ］の表の ［アプリ名］の下に表示されます。
- 説明：任意で、アプリの説明を入力します。
- アプリカテゴリ：任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリのカテゴリについて」を参照してください。

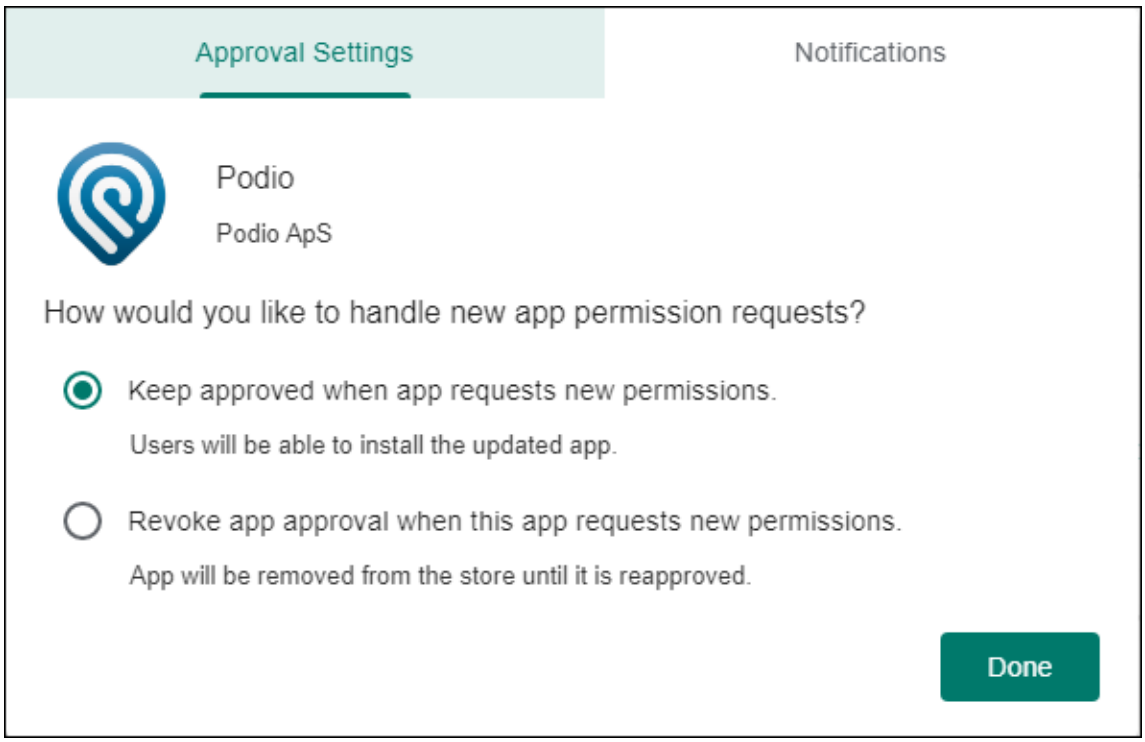
6. ［次へ］をクリックします。［**Android Enterprise MDX** アプリ］ページが開きます。
7. ［アップロード］をクリックしてアプリの.mdx ファイルの場所に移動し、ファイル選択して ［開く］をクリックします。
8. 追加されたアプリケーションが、管理対象 Google Play ストアからの承認を必要としているかどうかが UI によって通知されます。Citrix Endpoint Management コンソールを終了せずにアプリケーションを承認するには、［はい］をクリックします。



9. 管理対象 Google Play ストアのページが開いたら、［承認］をクリックします。



10. ［承認］を再度クリックします。
11. ［アプリが新しい権限を要求したときには承認を維持する］を選択します。［保存］をクリックします。



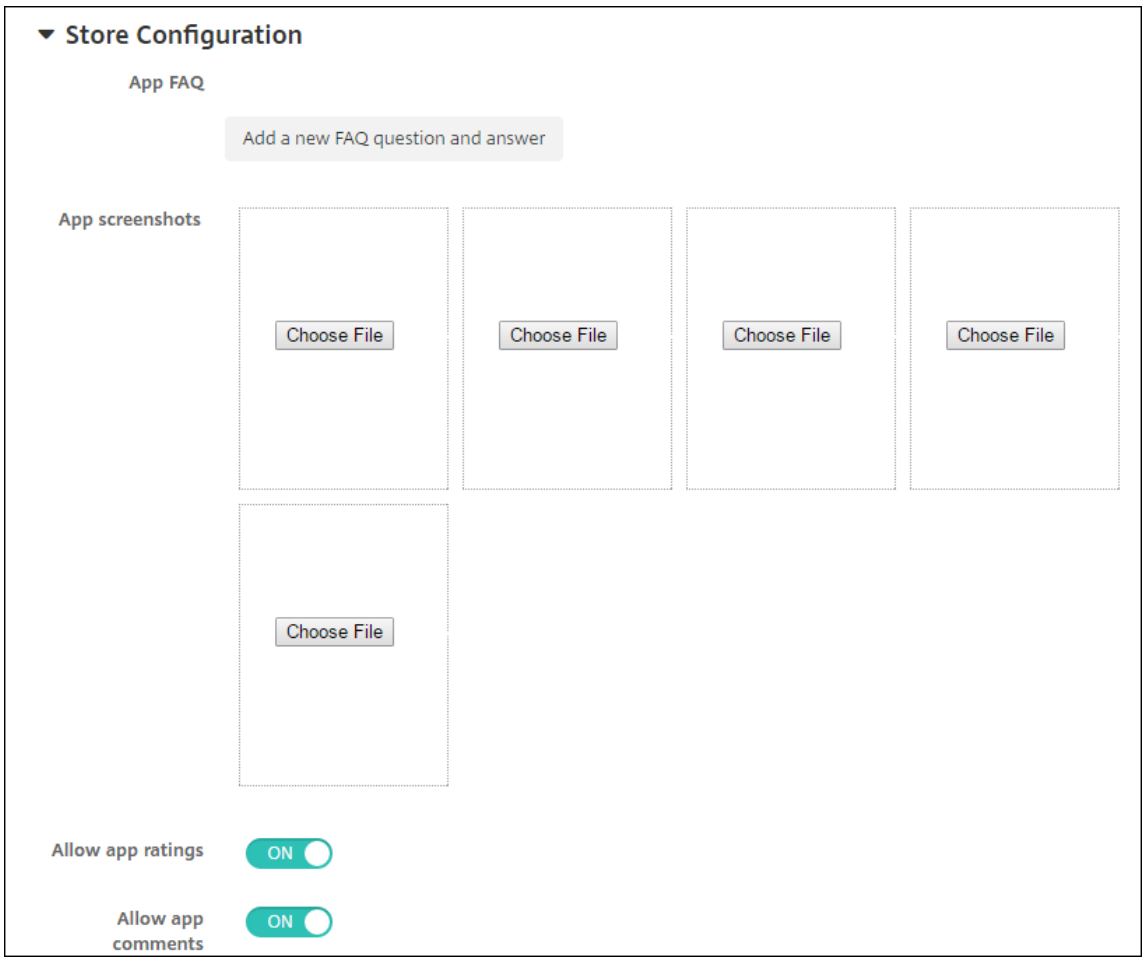
12. アプリを承認して保存すると、詳細な設定がページに表示されます。次の設定を構成します:

    - ファイル名: アプリに関連付けられているファイル名を入力します。
    - アプリの説明: アプリの説明を入力します。
    - 製品トラック: ユーザーデバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、そのトラックを選択してユーザーに割り当てることができます。デフォルトは［実稼働］です。
    - アプリのバージョン: 任意で、アプリのバージョン番号を入力します。
    - パッケージ **ID**: Google Play ストアでのアプリの URL。
    - 最小 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
    - 最大 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
    - 除外するデバイス: 任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。

13. **MDX** ポリシーを構成します。MDX アプリのアプリポリシーについて詳しくは、「MDX ポリシーの概要」および「MAM SDK の概要」を参照してください。

14. 展開規則を構成します。詳しくは、「リソースの展開」を参照してください。

15. ［ストア構成］を展開します。この設定は、管理対象 Google Play にのみ表示される Android Enterprise アプリには適用されません。

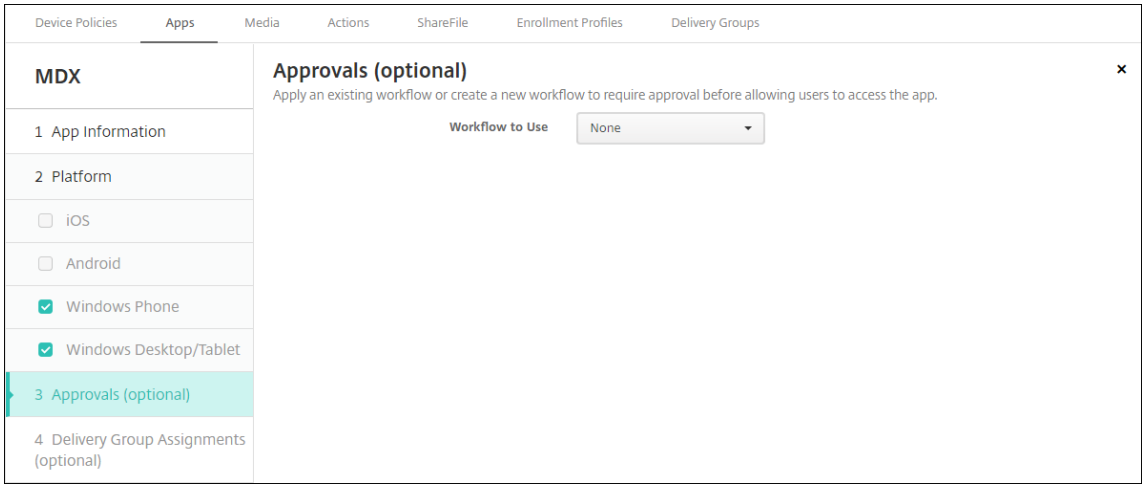


任意で、アプリに関する FAQ や、アプリストアに表示されるスクリーンショットを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します:
  - アプリの **FAQ**: アプリに関する FAQ の質問および回答を追加します。
  - アプリのスクリーンショット: アプリをアプリストアで分類しやすくするためのスクリーンショットを追加します。アップロードするグラフィックは PNG である必要があります。GIF 画像や JPEG 画像はアップロードできません。
  - アプリ評価を許可: ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは ［オン］です。

    アプリコメントを許可: 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは ［オン］です。

16. ［次へ］をクリックします。［承認］ページが開きます。



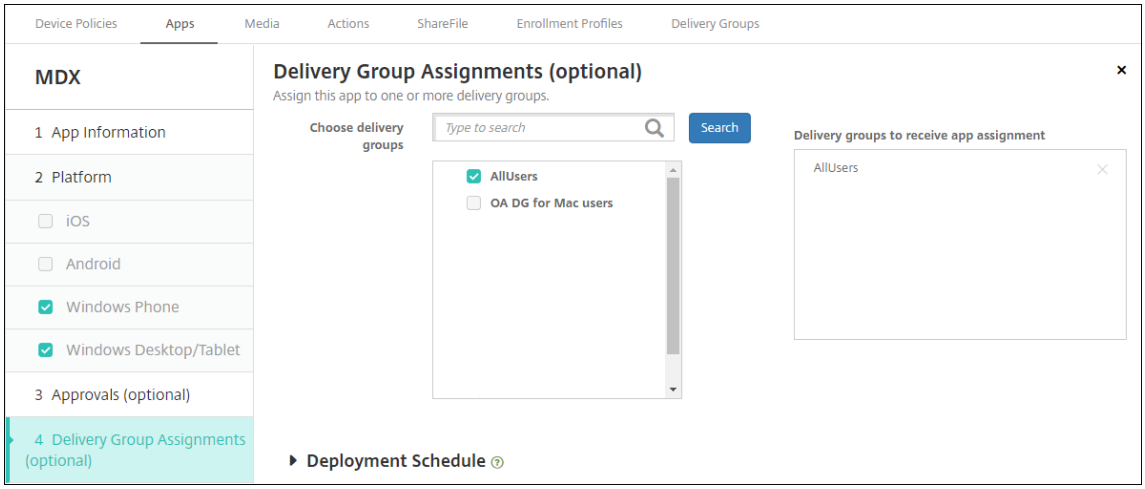
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定しない場合は、手順 15 に進みます。

ワークフローを割り当てるか作成するには、次の設定を構成します:

- 使用するワークフロー: 一覧から既存のワークフローを選択するか、[新しいワークフローの作成] をクリックします。デフォルトは [なし] です。
- [新しいワークフローの作成] を選択した場合は、次の設定を構成します。詳しくは、「ワークフローの作成および管理」を参照してください。
- 名前: ワークフローの固有の名前を入力します。
- 説明: 任意で、ワークフローの説明を入力します。
- メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
- マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは [1 つのレベル] です。選択できるオプションは以下のとおりです:
  - 不必要
  - 1 つのレベル
  - 2 つのレベル
  - 3 つのレベル
- **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
- 追加の必須承認者を検索: 検索フィールドに、追加で必要なユーザーの名前を入力して、[検索] をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが [選択した追加の必須承認者] の一覧に表示されます。
  - [選択した追加の必須承認者] の一覧からユーザーを削除するには、次のいずれかを行います:
    * [検索] をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。

* 名前の全体または一部を検索ボックスに入力して ［検索］をクリックし、検索結果を絞り込みます。
* ［選択した追加の必須承認者］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

17. ［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。



18. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

19. ［展開スケジュール］を展開して以下の設定を構成します：

- ［展開］の横の ［オン］をクリックすると展開がスケジュールされ、［オフ］をクリックすると展開が行われません。デフォルトのオプションは ［オン］です。
- ［展開スケジュール］の横の ［すぐに］または ［後で］をクリックします。デフォルトのオプションは［すぐに］です。
- ［あとで］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［展開状態］の横の ［接続するたび］をクリックするか、［以前の展開が失敗した場合のみ］をクリックします。デフォルトのオプションは、［接続するたび］です。
- ［常時接続に対する展開］の横で、［オフ］が選択されていることを確認します。デフォルトのオプションは ［オフ］です。Citrix Endpoint Management の使用を 10.18.19 以降のバージョンで始めたユーザーは、Android Enterprise で常時接続を使用できません。バージョン 10.18.19 より前に Citrix Endpoint Management を使い始めたユーザーには、この接続は推奨されません。

  このオプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

  構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

20. ［保存］をクリックします。

業務用モバイルアプリごとにこの手順を繰り返します。

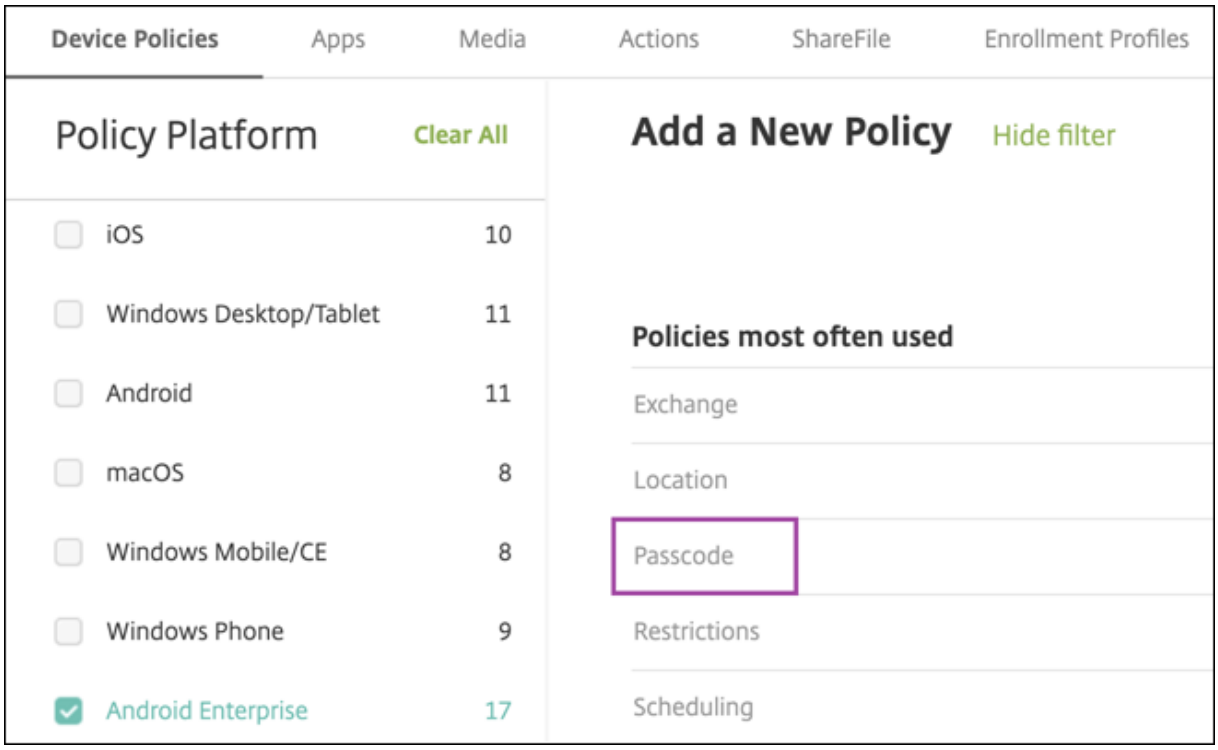
セキュリティ確認ポリシーを構成する

Citrix Endpoint Management パスコードデバイスポリシーでは、セキュリティ確認の規則を構成します。セキュリティ確認は、ユーザーが自分のデバイスまたは Android Enterprise の仕事用プロファイルにアクセスしたときに表示されます。セキュリティ確認はパスコードか生体認証です。パスコードポリシーについて詳しくは、「パスコードデバイスポリシー」を参照してください。

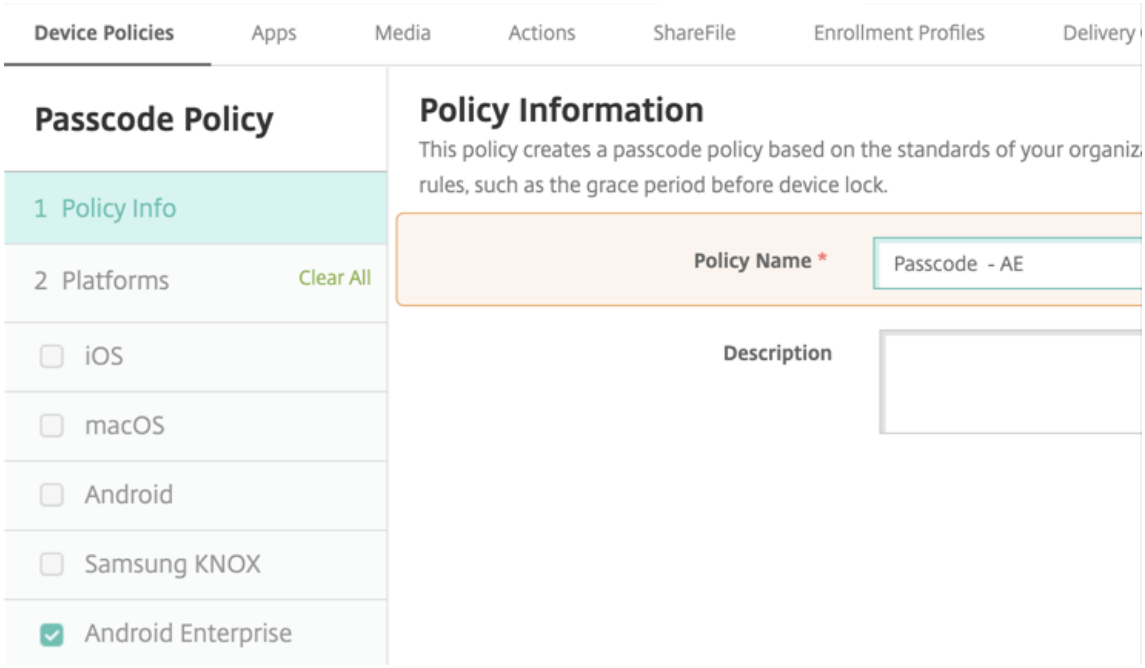
- Android Enterprise の展開に BYOD デバイスが含まれる場合、仕事用プロファイルのパスコードポリシーを構成します。
- 展開に会社所有の完全管理デバイスが含まれる場合、デバイス自体のパスコードポリシーを構成します。
- 展開に両方のタイプのデバイスが含まれる場合、両方のタイプのパスコードポリシーを構成します。

パスコードポリシーを構成するには:

1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］に移動します。
2. ［追加］をクリックします。
3. ［フィルターを表示］をクリックして、［ポリシープラットフォーム］ペインを開きます。［ポリシープラットフォーム］ペインで、［**Android Enterprise**］を選択します。
4. 右ペインで ［パスコード］をクリックします。



1. ［ポリシー名］を入力します。［次へ］をクリックします。



2. パスコードポリシー設定を構成します。

   - デバイス自体のセキュリティ確認に使用できる設定を確認するには、［デバイスのパスコードを要求］を［オン］に設定します。
   - 仕事用プロファイルのセキュリティ確認に使用できる設定を確認するには、［仕事用プロファイルのセキュリティ確認］を ［オン］に設定します。

3. ［次へ］をクリックします。
4. このポリシーを 1 つ以上のデリバリーグループに割り当てます。
5. ［保存］をクリックします。

登録プロファイルの作成

Citrix Endpoint Management 展開で Android Enterprise が有効になっている場合、登録プロファイルによって Android デバイスの登録方法が制御されます。登録プロファイルを作成して Android Enterprise デバイスを登録する場合は、登録プロファイルを構成して、新しいデバイスおよび工場出荷時リセットデバイスを以下のデバイスとして登録できます:

- 完全に管理されているデバイス
- 専用デバイス
- 仕事用プロファイルで完全に管理/会社所有のデバイスの仕事用プロファイル

これらの Android Enterprise の登録プロファイルをそれぞれ構成して、BYOD の Android デバイスを仕事用プロファイルデバイスとして登録することもできます。

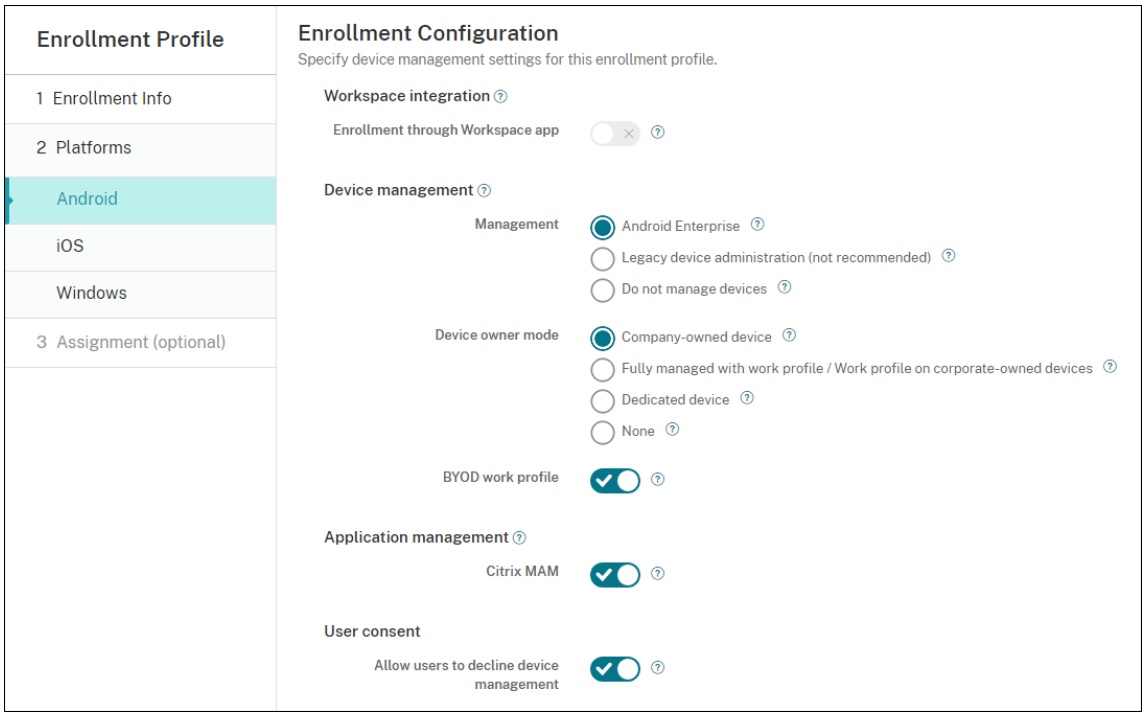
Citrix Endpoint Management 展開で Android Enterprise が有効になっている場合、新しく登録または再登録したすべての Android デバイスが Android Enterprise デバイスとして登録されます。デフォルトでは、Global 登録プロファイルは、新規および工場出荷時にリセットされた Android デバイスを完全に管理されたデバイスとして登録し、BYOD Android デバイスを会社所有のデバイスの仕事用プロファイルとして登録します。

登録プロファイルを作成したら、デリバリーグループを登録プロファイルに割り当てます。異なる登録プロファイルを持つ複数のデリバリーグループにユーザーが属している場合、デリバリーグループの名前によって、使用される登録プロファイルが決まります。Citrix Endpoint Management は、デリバリーグループのアルファベット順一覧の最後に表示されるデリバリーグループを選択します。詳しくは、「登録プロファイル」を参照してください。

完全に管理されたデバイスの登録プロファイルの追加

グローバル登録プロファイルは、デフォルトで完全に管理されたデバイスを登録しますが、完全に管理されたデバイスを登録するための登録プロファイルをさらに作成できます。

1. Citrix Endpoint Management コンソールで、［構成］**>**［登録プロファイル］の順に移動します。
2. 登録プロファイルを追加するには、［追加］をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. このプロファイルのメンバーが登録できるデバイスの数を設定します。
4. ［プラットフォーム］の［**Android**］を選択するか、［次へ］をクリックします。［登録構成］ページが開きます。
5. ［管理］を ［**Android Enterprise**］に設定します。
6. ［デバイス所有者モード］を ［会社所有のデバイス］に設定します。



7. ［**BYOD/**仕事用プロファイル］を使用すると、BYOD デバイスを仕事用プロファイルデバイスとして登録するように登録プロファイルを構成できます。新しいデバイスおよび工場出荷時リセットデバイスは、完全に管理されたデバイスとして登録されます。［**BYOD/**仕事用プロファイル］を ［オン］に設定すると、BYOD デバイスを仕事用プロファイルデバイスとして登録できます。［**BYOD/**仕事用プロファイル］を ［オフ］に設定して、登録を完全に管理されたデバイスに制限します。デフォルトは ［オン］です。
8. Citrix MAM にデバイスを登録するかどうかを選択します。
9. ［**BYOD/**仕事用プロファイル］を ［オン］に設定している場合は、ユーザーの同意を構成します。BYOD/仕事用プロファイルデバイスのユーザーがデバイスの登録時にデバイス管理を拒否することを許可するには、［ユーザーにデバイス管理の許否を許可］を ［オン］に設定します。

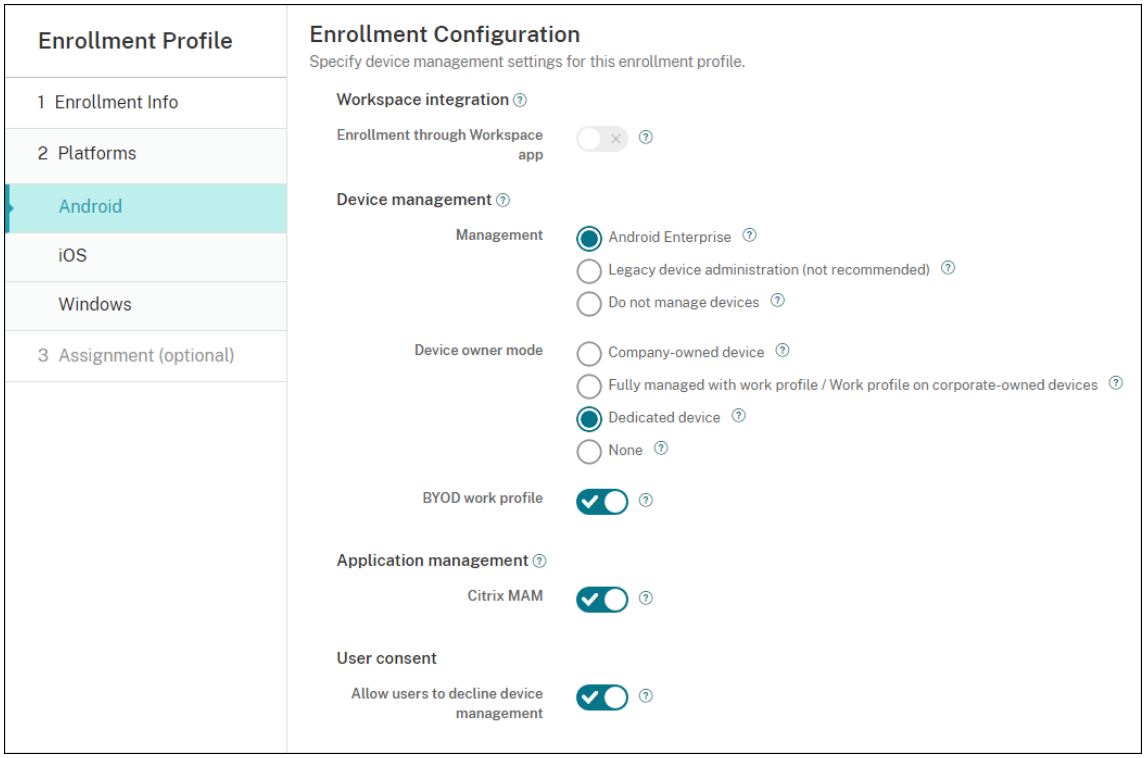
   ［**BYOD/**仕事用プロファイル］が ［オン］に設定されている場合、［ユーザーにデバイス管理の許否を許可］のデフォルト値は ［オン］です。［**BYOD/**仕事用プロファイル］が ［オフ］に設定されている場合、［ユーザーにデバイス管理の許否を許可］は無効になっています。
10. ［割り当て］を選択します（オプション）。［デリバリーグループ割り当て］ページが開きます。
11. 完全に管理されたデバイスを登録した管理者を含む、1 つまたは複数のデリバリーグループを選択します。次に、［保存］をクリックします。

    ［登録プロファイル］ページに、追加したプロファイルが表示されます。

専用デバイス登録プロファイルの追加

Citrix Endpoint Management 展開に専用デバイスを含める場合、1 人の Citrix Endpoint Management 管理者、または数人の管理者グループが専用デバイスを多数登録することがあります。こうした管理者が必要なすべてのデバイスを登録できるようにするには、ユーザーごとに無制限のデバイスを許可した状態で登録プロファイルを作成します。

1. Citrix Endpoint Management コンソールで、［構成］**>**［登録プロファイル］の順に移動します。
2. 登録プロファイルを追加するには、［追加］をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。このプロファイルのメンバーが登録できるデバイスの数を ［無制限］に設定します。
3. ［プラットフォーム］の［**Android**］を選択するか、［次へ］をクリックします。［登録構成］ページが開きます。
4. ［管理］を ［**Android Enterprise**］に設定します。
5. ［デバイス所有者モード］を ［専用デバイス］に設定します。



6. [**BYOD**/仕事用プロファイル］を使用すると、BYOD デバイスを仕事用プロファイルデバイスとして登録するように登録プロファイルを構成できます。新しいデバイスおよび工場出荷時リセットデバイスは、専用デバイスとして登録されます。[**BYOD**/仕事用プロファイル］を ［オン］に設定すると、BYOD デバイスを仕事用プロファイルデバイスとして登録できます。[**BYOD**/仕事用プロファイル］を ［オフ］に設定して、登録を会社所有のデバイスに制限します。デフォルトは ［オン］です。
7. Citrix MAM にデバイスを登録するかどうかを選択します。
8. [**BYOD**/仕事用プロファイル］を ［オン］に設定している場合は、ユーザーの同意を構成します。BYOD/仕事用プロファイルデバイスのユーザーがデバイスの登録時にデバイス管理を拒否することを許可するには、［ユーザーにデバイス管理の許否を許可］を ［オン］に設定します。

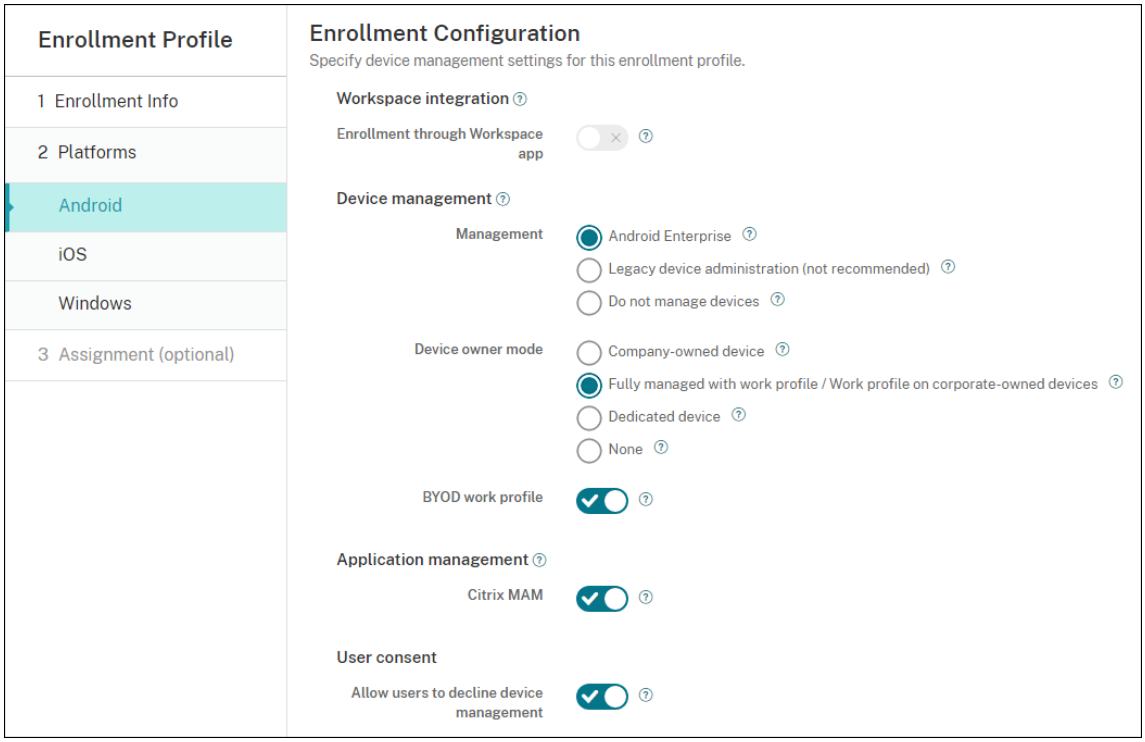
   [**BYOD**/仕事用プロファイル］が ［オン］に設定されている場合、［ユーザーにデバイス管理の許否を許可］のデフォルト値は ［オン］です。[**BYOD**/仕事用プロファイル］が ［オフ］に設定されている場合、［ユーザーにデバイス管理の許否を許可］は無効になっています。
9. ［割り当て］を選択します（オプション）。［デリバリーグループ割り当て］ページが開きます。
10. 専用デバイスを登録した管理者を含む、1 つまたは複数のデリバリーグループを選択します。次に、［保存］をクリックします。

    ［登録プロファイル］ページに、追加したプロファイルが表示されます。

仕事用プロファイルで完全に管理/会社所有のデバイスの仕事用プロファイルの登録プロファイルを追加

1. Citrix Endpoint Management コンソールで、［構成］**>** ［登録プロファイル］の順に移動します。

2. 登録プロファイルを追加するには、［追加］をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. このプロファイルのメンバーが登録できるデバイスの数を設定します。
4. ［プラットフォーム］の［**Android**］を選択するか、［次へ］をクリックします。［登録構成］ページが開きます。
5. ［管理］を［**Android Enterprise**］に設定します。［デバイス所有者モード］を［仕事用プロファイルで完全に管理/会社所有のデバイスの仕事用プロファイル］に設定します。



6. ［**BYOD/**仕事用プロファイル］を使用すると、BYOD デバイスを仕事用プロファイルデバイスとして登録するように登録プロファイルを構成できます。新しいデバイスおよび工場出荷時リセットデバイスは、仕事用プロファイルで完全に管理されたデバイスとして登録されます。［**BYOD/**仕事用プロファイル］を［オン］に設定すると、BYOD デバイスを仕事用プロファイルデバイスとして登録できます。［**BYOD/**仕事用プロファイル］を［オフ］に設定して、登録を専用デバイスに制限します。デフォルトは［オフ］です。
7. Citrix MAM にデバイスを登録するかどうかを選択します。
8. ［**BYOD/**仕事用プロファイル］を［オン］に設定している場合は、ユーザーの同意を構成します。BYOD/仕事用プロファイルデバイスのユーザーがデバイスの登録時にデバイス管理を拒否することを許可するには、［ユーザーにデバイス管理の許否を許可］を［オン］に設定します。

   ［**BYOD/**仕事用プロファイル］が［オン］に設定されている場合、［ユーザーにデバイス管理の許否を許可］のデフォルト値は［オン］です。［**BYOD/**仕事用プロファイル］が［オフ］に設定されている場合、［ユーザーにデバイス管理の許否を許可］は無効になっています。
9. ［割り当て］を選択します（オプション）。［デリバリーグループ割り当て］ページが開きます。

10. 仕事用プロファイルで完全に管理されたデバイスを登録した管理者を含む、1 つまたは複数のデリバリーグループを選択します。次に、［保存］をクリックします。

    ［登録プロファイル］ページに、追加したプロファイルが表示されます。

従来デバイスの登録プロファイルの追加

Google は、デバイス管理のデバイス管理者モードを廃止しました。デバイス所有者モードまたはプロファイル所有者モードで、すべての Android デバイスを管理することが推奨されています。（Google Android Enterprise 開発者ガイドのDevice admin deprecationを参照してください。）

この変更を利用するには、以下の設定が必要です：

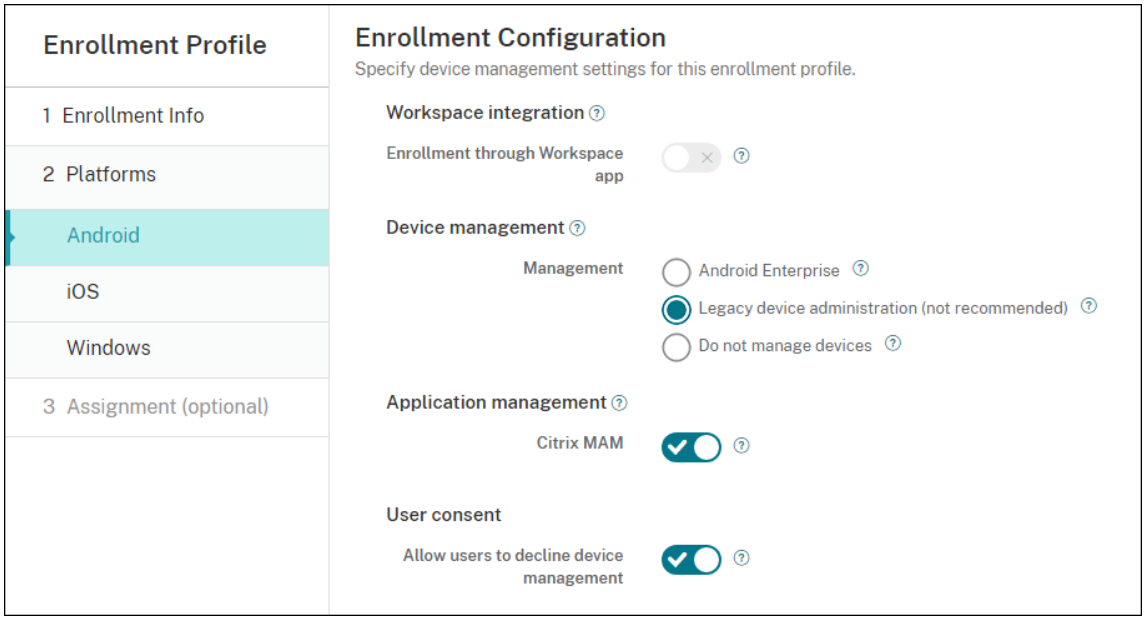
- Citrix では、Android Enterprise を Android デバイスのデフォルトの登録オプションにしました。
- Citrix Endpoint Management 展開で Android Enterprise が有効になっている場合、新しく登録または再登録したすべての Android デバイスが Android Enterprise デバイスとして登録されます。

組織では、従来の Android デバイスを、Android Enterprise を使用して管理する準備ができていない可能性があります。その場合は、デバイス管理者モードで引き続き管理できます。既にデバイス管理者モードで登録されているデバイスの場合、Citrix Endpoint Management はデバイス管理者モードでそれらを管理し続けます。

新しい Android デバイスの登録でデバイス管理者モードを使用できるように、従来のデバイスの登録プロファイルを作成します。

従来デバイスの登録プロファイルを作成するには、次の手順を実行します：

1. Citrix Endpoint Management コンソールで、［構成］**>**［登録プロファイル］の順に移動します。
2. 登録プロファイルを追加するには、［追加］をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。
3. このプロファイルのメンバーが登録できるデバイスの数を設定します。
4. ［プラットフォーム］の［**Android**］を選択するか、［次へ］をクリックします。［登録構成］ページが開きます。
5. ［管理］を ［従来のデバイス管理 **(**非推奨**)**］に設定します。［次へ］をクリックします。



6. Citrix MAM にデバイスを登録するかどうかを選択します。
7. ユーザーがデバイスの登録時にデバイス管理を拒否することを許可するには、［ユーザーにデバイス管理の許否を許可］を ［オン］に設定します。デフォルトは ［オン］です。
8. ［割り当て］を選択します（オプション）。［デリバリーグループ割り当て］ページが開きます。
9. 専用デバイスを登録した管理者を含む、1 つまたは複数のデリバリーグループを選択します。次に、［保存］をクリックします。

［登録プロファイル］ページに、追加したプロファイルが表示されます。

引き続きデバイス管理者モードで従来デバイスを管理するには、このプロファイルを使用して従来デバイスを登録または再登録します。仕事用プロファイルデバイスと同様のデバイス管理者デバイスを登録するには、ユーザーに Citrix Secure Hub をダウンロードさせ、登録サーバーの URL を指定します。

Android Enterprise の仕事用プロファイルデバイスのプロビジョニング

Android Enterprise 仕事用プロファイルデバイスは、プロファイル所有者モードで登録されます。これらのデバイスは、新品または工場出荷時の設定にリセットする必要がありません。BYOD デバイスは、仕事用プロファイルデバイスとして登録されます。登録手順は、Citrix Endpoint Management で Android を登録する場合と同様です。ユーザーは Google Play から Citrix Secure Hub をダウンロードし、デバイスを登録します。

デバイスを Android Enterprise で仕事用プロファイルデバイスとして登録している場合、デフォルトでは ［**USB** デバッグおよび不明なソース］の設定は無効になっています。

Android Enterprise のデバイスを仕事用プロファイルデバイスとして登録する場合は、必ず Google Play にアクセスしてください。そこから、ユーザーの個人プロファイルでの Citrix Secure Hub の表示を有効にします。

Android Enterprise の完全に管理されたデバイスのプロビジョニング

前のセクションで設定した展開に、完全に管理されたデバイスを登録できます。完全に管理されたデバイスは会社所有のデバイスで、デバイス所有者モードで登録されます。デバイス所有者モードで登録できるのは、新しいデバイスまたは工場出荷時の状態にリセットされたデバイスのみです。

デバイス所有者モードでデバイスを登録するには、次の登録方法のいずれかを使用します:

- **DPC ID** トークン: この登録方法では、ユーザーがデバイスの設定時に「`afw#xenmobile`」という文字を入力します。`afw#xenmobile`は Citrix DPC ID トークンです。このトークンにより、デバイスが Citrix Endpoint Management の管理対象であると識別され、Google Play ストアから Citrix Secure Hub がダウンロードされます。「Citrix DPC 識別子トークンを使用したデバイスの登録」を参照してください。
- 近距離無線通信（**NFC**）バンプ: NFC バンプの登録方法では、近距離無線通信を使用して 2 つのデバイス間でデータを転送します。新しいデバイスまたは工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびそのほかの通信モードは無効になっています。この状態のデバイスが使用する通信プロトコルは NFC のみです。「NFC バンプを使用してデバイスを登録する」を参照してください。
- **QR** コード: QR コード登録は、NFC をサポートしていないタブレットなどの分散型端末を登録するのに使用できます。QR コードによる登録方法では、セットアップウィザードから QR コードをスキャンすることによって、デバイスプロファイルモードを設定および構成します。「QR コードを使用してデバイスを登録する」を参照してください。
- ゼロタッチ: ゼロタッチ登録では、最初に電源をオンにしたときに自動で登録されるようにデバイスを構成できます。ゼロタッチ登録は、Android 9.0 以降が動作する一部の Android デバイスでサポートされています。「ゼロタッチ登録」を参照してください。
- **Google** アカウント: ユーザーは、Google アカウントの資格情報を入力して、プロビジョニングプロセスを開始します。このオプションは、Google Workspace を使用している企業向けです。

Citrix DPC 識別子トークンを使用したデバイスの登録

初期セットアップで新しいデバイスまたは工場出荷時の状態にリセットされたデバイスの電源を入れた後、Google アカウントの入力を求められたら「`afw#xenmobile`」と入力します。この操作により、Citrix Secure Hub がダウンロードされインストールされます。インストール後、Citrix Secure Hub の設定プロンプトに従って登録を完了します。

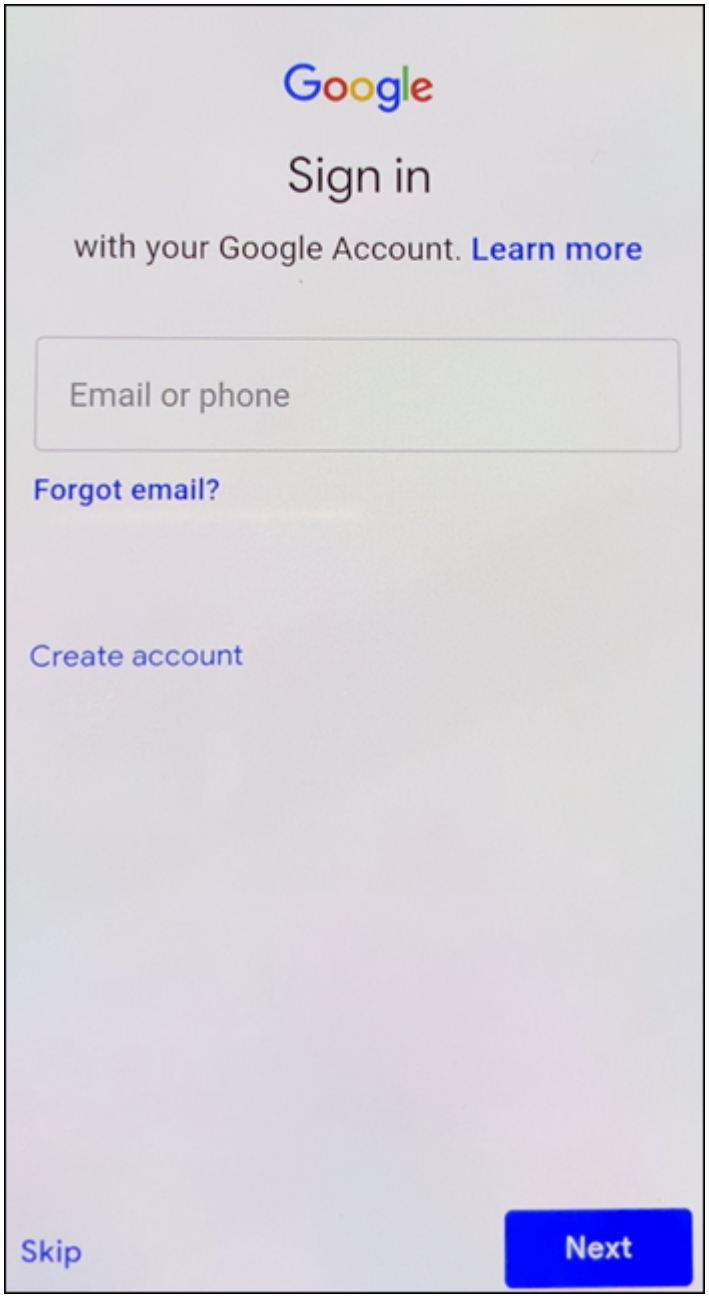
システム要件

- Android OS を実行するすべての Android デバイスでサポートされます。

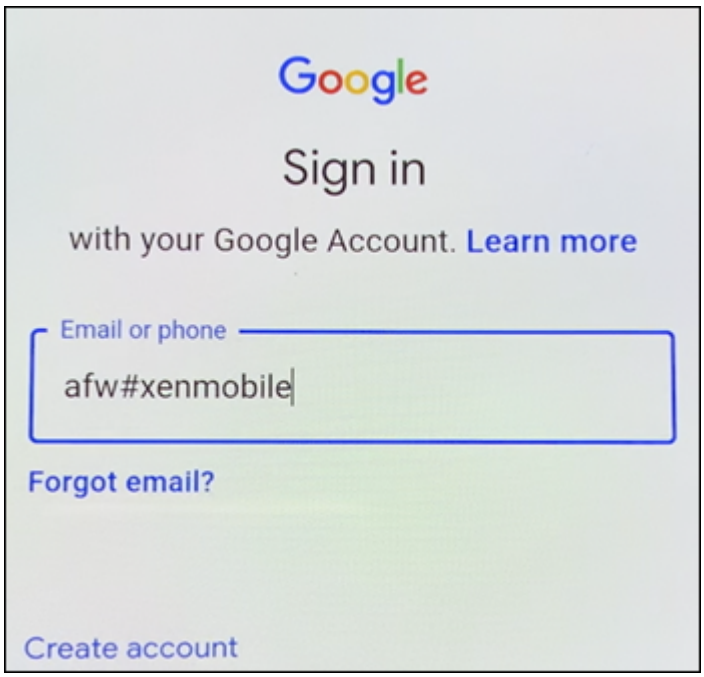
デバイスを登録するには

1. 新しいデバイスまたは工場出荷時の設定にリセットされたデバイスの電源を入れます。

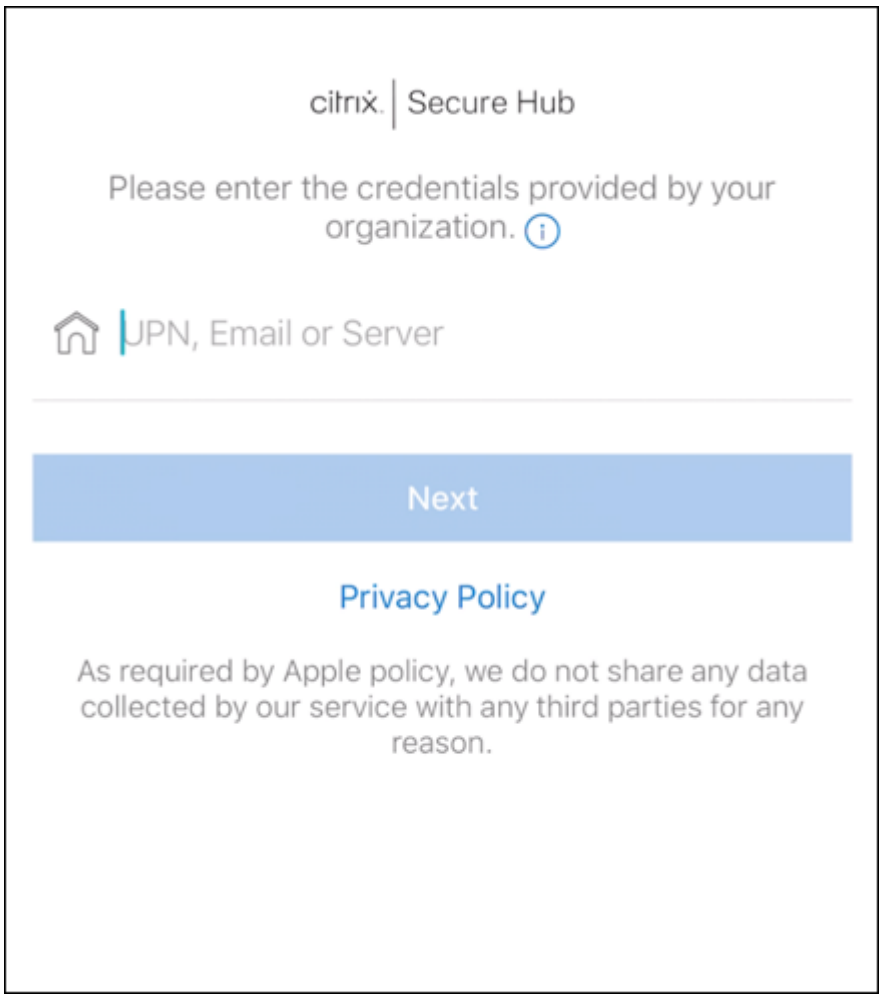
2. デバイスの初期セットアップが読み込まれ、Google アカウントの入力が求められます。デバイスのホーム画面が読み込まれたら、通知バーのセットアップ完了通知を確認します。



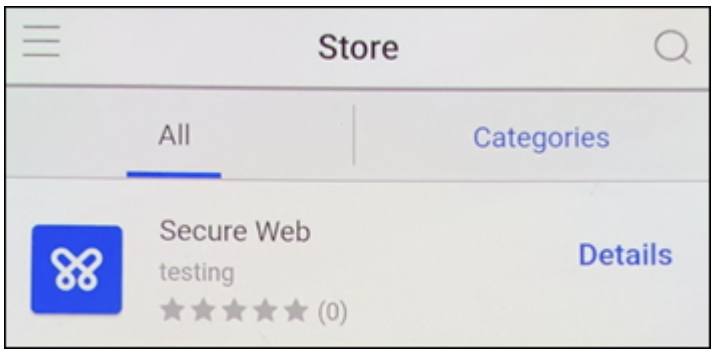
3. メールまたは電話フィールドに「`afw#xenmobile`」と入力します。



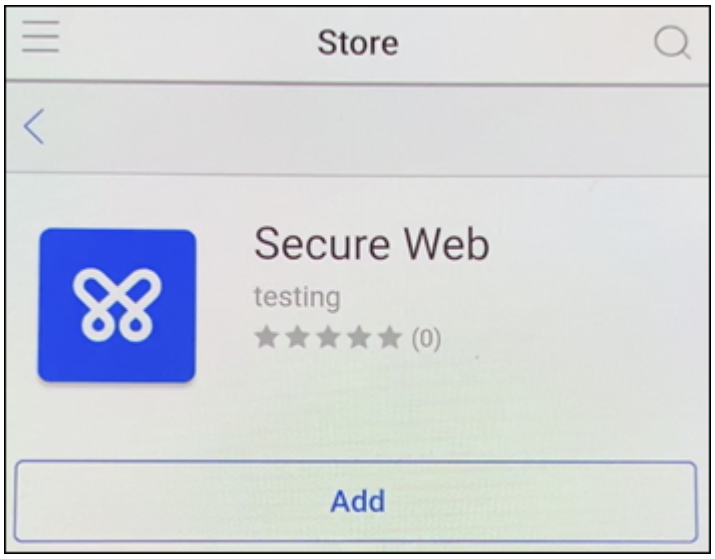
4. Citrix Secure Hub のインストールを求める Android Enterprise 画面で ［インストール］をタップします。
5. Citrix Secure Hub インストーラー画面で ［インストール］をタップします。
6. すべてのアプリの許可リクエストに対して ［許可する］をタップします。
7. ［同意して続行］をタップして Citrix Secure Hub をインストールし、デバイスを管理できるようにします。
8. これで、Citrix Secure Hub がインストールされ、デフォルトの登録画面に表示されます。この例では、AutoDiscovery は設定されていません。自動検出が設定されている場合、ユーザーはユーザー名/メールアドレスを入力可能で、それに対応するサーバーが検出されます。自動検出が設定されていない場合、環境の登録 URL を入力して ［次へ］をタップします。



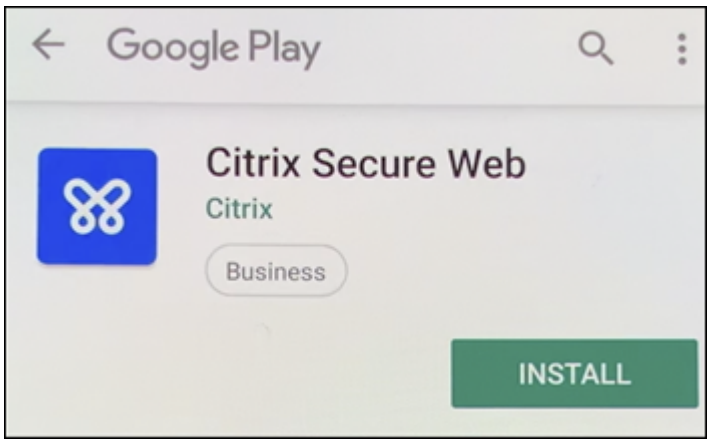
9. Citrix Endpoint Management のデフォルト設定では、MAM を使用するか、MDM+MAM を使用するかを選択できます。このようにプロンプトが表示されたら、［はい、登録します］をタップして MDM+MAM を選択します。
10. ユーザーのメールアドレスとパスワードを入力し、［次へ］をタップします。
11. デバイスのパスコードを設定するように求められます。［設定］をタップしてパスコードを入力します。
12. 仕事用プロファイルのロック解除方法を設定するよう求められます。この例では ［パスワード］、［**PIN**］をタップして PIN を入力します。
13. デバイスに Citrix Secure Hub の ［マイアプリ］ランディング画面が表示されます。［ストアからアプリを追加］をタップします。
14. Citrix Secure Web を追加するには、［**Citrix Secure Web**］をタップします。



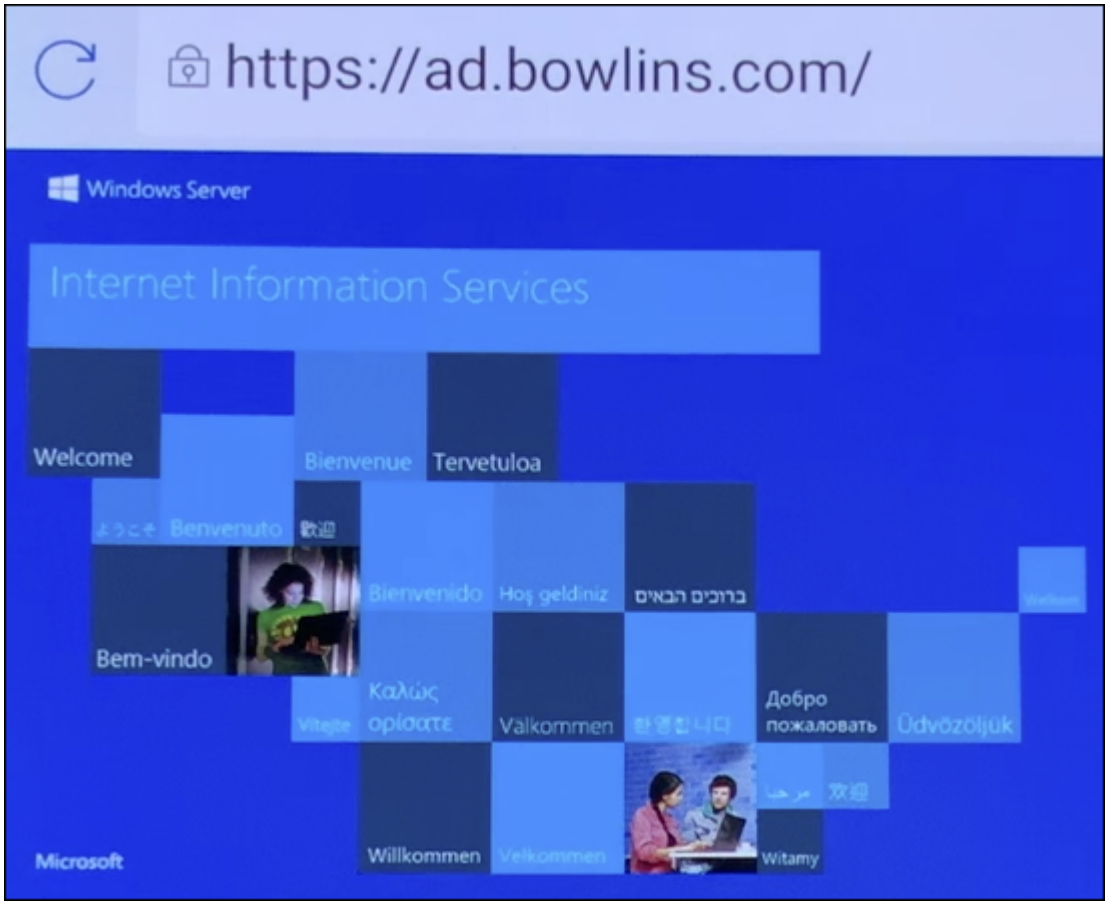
15. ［追加］をタップします。



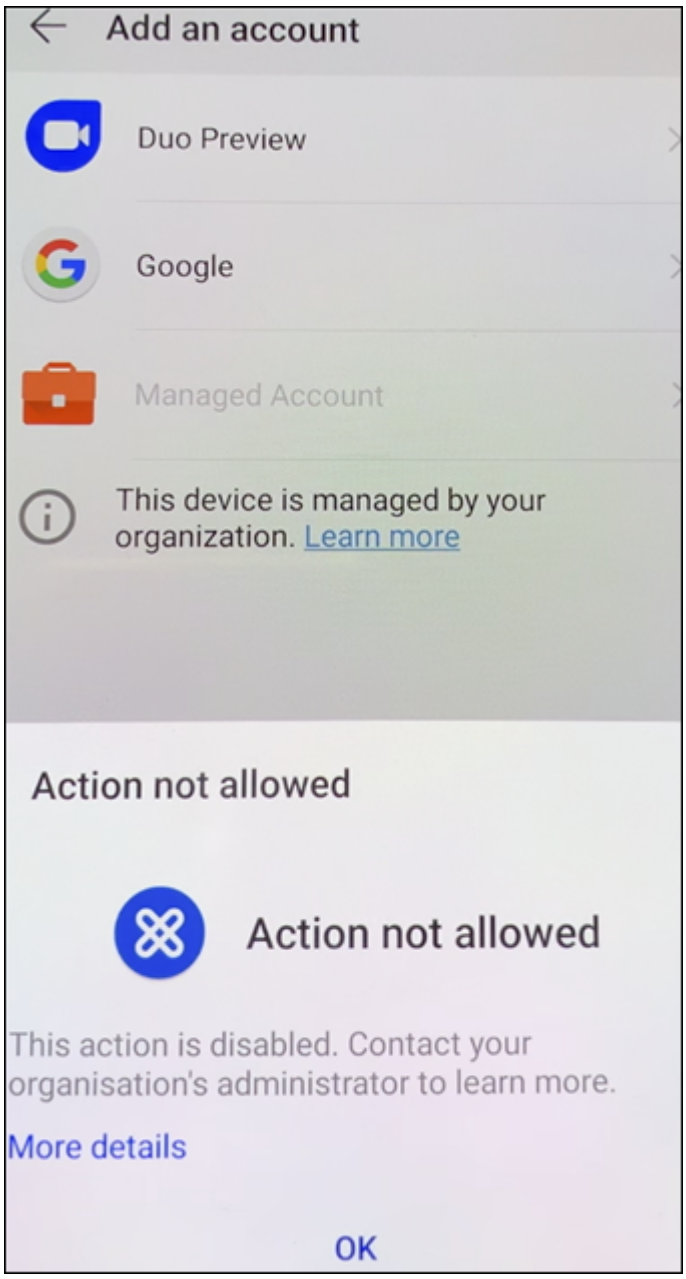
16. Citrix Secure Hub で、Citrix Secure Web をインストールするために Google Play ストアに移動します。［インストール］をタップします。



17. Citrix Secure Web がインストールされたら、［開く］をタップします。アドレスバーに内部サイトの URL を入力し、ページが読み込まれることを確認します。



18. デバイスで ［設定］ **>** ［アカウント］ に移動します。管理対象アカウントが変更できないことを確認します。画面の共有またはリモートデバッグのための開発者オプションもブロックされます。



NFC バンプを使用してデバイスを登録する

NFC バンプを使用して完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットされたデバイスと、Citrix Endpoint Management プロビジョニングツールを実行するデバイスの 2 台のデバイスが必要です。

システム要件および前提条件

- サポートされる Android デバイス

- 完全に管理されたデバイスとして Android Enterprise 向けにプロビジョニングされた新規デバイス、または近距離無線通信機能で工場出荷時設定にリセットされたデバイス。「Android Enterprise の完全に管理されたデバイスのプロビジョニング」のセクションを参照してください。
- 構成済みの Provisioning Tool を実行している、近距離無線通信機能を有効にした別のデバイス。Provisioning Tool は、Citrix Secure Hub またはCitrix ダウンロードページから入手できます。

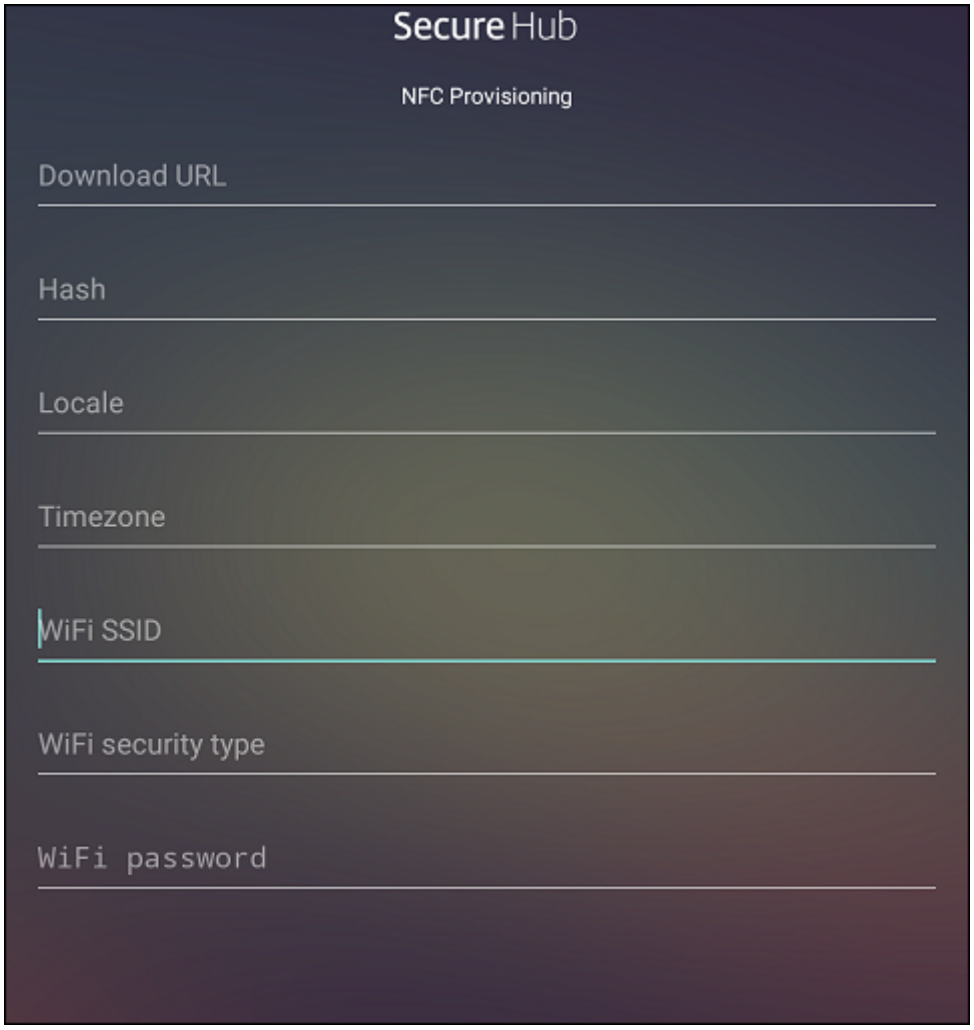
各デバイスでは、Android Enterprise プロファイルを 1 つのみ保有できます。この場合、プロファイルは管理対象 Citrix Secure Hub 用です。2 つ目の DPC アプリを追加しようとすると、インストール済みの Citrix Secure Hub が削除されます。

NFC バンプを介して転送されるデータ　工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータを NFC バンプ経由で送信して Android Enterprise を初期化する必要があります:

- デバイス所有者として機能する DPC アプリ（この場合は Citrix Secure Hub）のパッケージ名。
- デバイスが DPC アプリをダウンロードできるイントラネット/インターネット上の場所。
- ダウンロードが正常に完了したかどうかを確認する DPC アプリの SHA-256 ハッシュ。
- 工場出荷時の設定にリセットされたデバイスが DPC アプリに接続してダウンロードできるようにする Wi-Fi 接続の詳細。注：現時点では、Android はこの手順での 802.1x Wi-Fi をサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、プロビジョニングツールのデータが工場出荷時の設定にリセットされたデバイスに送信されます。このデータはその後、管理者設定での Citrix Secure Hub のダウンロードに使用されます。タイムゾーンと場所の値を入力しない場合、新しいデバイスでは Android によって自動的にこれらの値が構成されます。

Citrix Endpoint Management プロビジョニングツールの構成　NFC バンプを行う前に、プロビジョニングツールを構成する必要があります。この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFC バンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルを使用して入力することもできます。次の手順では、テキストファイルを構成する方法と、各フィールドを説明します。入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

テキストファイルを使用してプロビジョニングツールを構成するには　ファイルの名前を nfcprovisioning.txt にして、/sdcard/フォルダーにあるデバイスの SD カードに格納します。アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには次のデータが必要です:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=<download_location>
```

この行は、EMM プロバイダーアプリのイントラネット/インターネットの場所です。工場出荷時設定のデバイスが NFC バンプの後に Wi-Fi に接続した場合、デバイスはダウンロードのためにこの場所にアクセスする必要があります。URL は通常の URL で、特別な形式にする必要はありません。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>

この行は、EMM プロバイダーアプリのチェックサムです。このチェックサムはダウンロードが成功したかを検証するために使用されます。チェックサムを取得する手順については、後述します。

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

この行は、プロビジョニングツールを実行しているデバイスが接続されている Wi-Fi の SSID です。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

サポートされる値は WEP および WPA2 です。Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_LOCALE=<locale>

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

デバイスが実行されるタイムゾーンです。エリア/場所のデータベース名を入力します。たとえば、米国太平洋標準時の場合は「アメリカ/ロサンジェルス」と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

このデータは Citrix Secure Hub としてアプリにハードコードされるため、必須ではありません。ここでは、情報の完全性を守るためだけに記載しています。

WPA2 を使用して保護された Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

保護されていない Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Citrix Secure Hub のチェックサムを取得するには　Citrix Secure Hub のチェックサムは次の定数値です: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM。Citrix Secure Hub の APK ファイルをダウンロードするには、次の Google Play ストアのリンクを使用します: https://play.google.com/managed/downloadManagingApp?identifier=xenmobile。

アプリのチェックサムを取得するには　前提条件:

- Android SDK ビルドツールの **apksigner** ツール
- OpenSSL コマンドライン

アプリのチェックサムを取得するには、次の手順に従います:

1. Google Play ストアからアプリの APK ファイルをダウンロードします。
2. OpenSSL コマンドラインで、**apksigner** ツールandroid-sdk/build-tools/<version>/apksignerに移動して、以下を入力します:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

   コマンドから有効なチェックサムが返されます。

3. QR コードを生成するには、PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUMフィールドにチェックサムを入力します。例:


```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
     zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"
     qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.
     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

使用するライブラリ　プロビジョニングツールでは、以下のライブラリがソースコードに使用されています。

- v7 `appcompat` library、Design support library、および v7 Palette support library by Google（Apache license 2.0）

  詳しくは、「Support Library の機能」を参照してください。

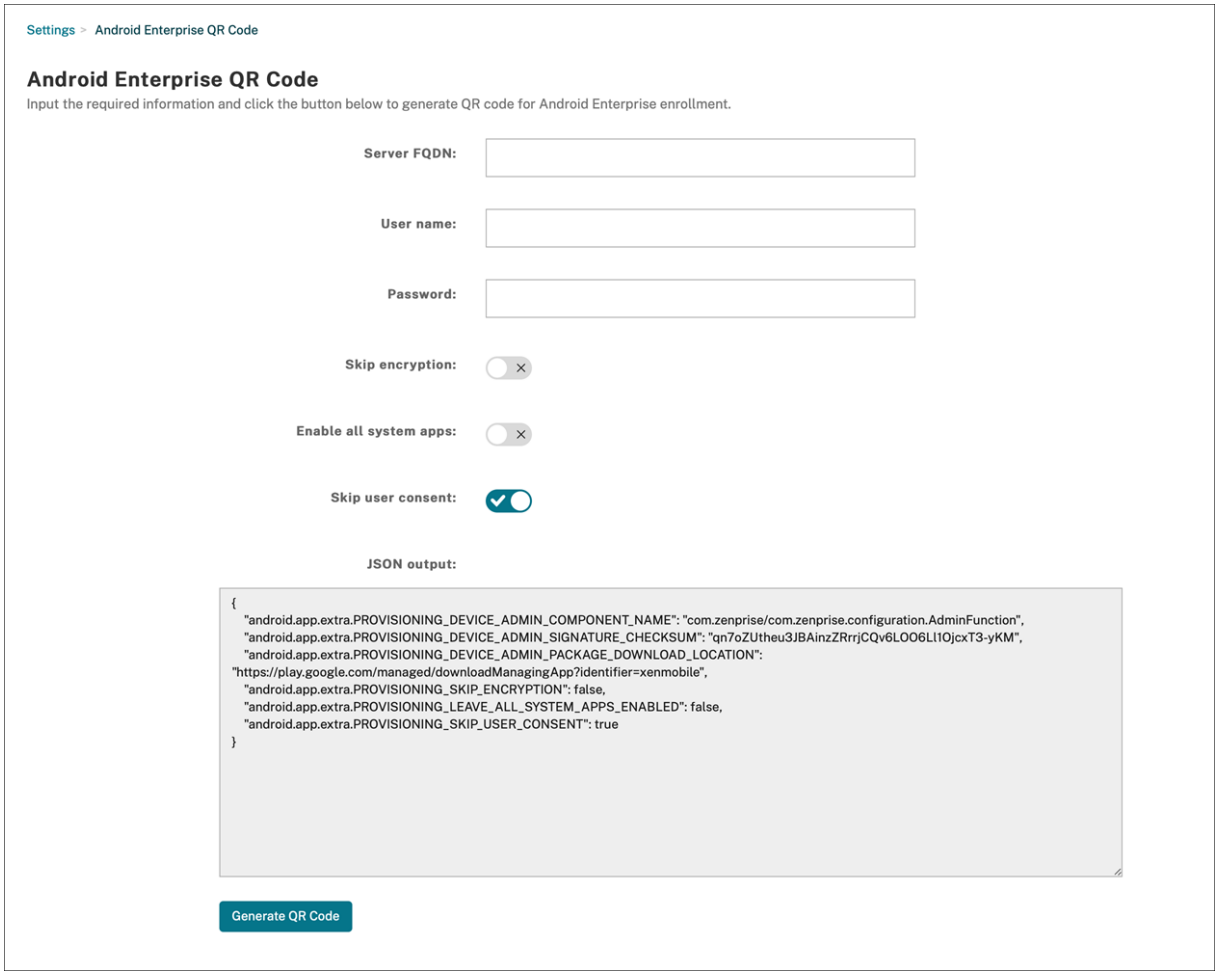
- Butter Knife by Jake Wharton（Apache license 2.0）

QR コードを使用してデバイスを登録する

ユーザーは、完全に管理されたデバイス用に生成した QR コードを使用してデバイスを登録できます。

システム要件　Android 7.0 以降を実行する Android デバイス。

QR コードの作成　必要に応じて登録情報を指定して QR コードを生成します。QR コードを生成したら、QR コードをローカルに保存します。Citrix Endpoint Management はこれを保存しません。



1. ［設定］**>**［**Android Enterprise QR** コード］に移動します。
2. 必要に応じて、次の登録情報を指定します：

   - サーバー **FQDN**： Citrix Endpoint Management サーバーの FQDN を入力します（例：`example.cem.cloud.com`）。この情報は入力しなくても構いません。空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - ユーザー名：登録に使用するユーザーの名前を入力します。QR コードを複数のユーザーに配布する予定がある場合は、このフィールドを空のままにしておくことをお勧めします。ユーザー名とパスワードを使用して QR コードを構成すると、キオスクデバイスを登録するのに役立ちます。フィールドを空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - パスワード：入力したユーザー名に関連付けられているパスワードを入力します。フィールドを空のままにした場合、ユーザーは登録時にこの情報を入力する必要があります。
   - 暗号化をスキップする：［オン］の場合、デバイスは登録中に暗号化されません。デフォルトは ［オフ］です。
   - すべてのシステムアプリを有効にする：［オン］の場合、デバイス上のすべてのシステムアプリへのアクセスを許可します。デフォルトは ［オフ］です。
   - ユーザー承認をスキップする：［オフ］の場合、ユーザーはデバイス管理をオプトアウトできます。デフ

ォルトは ［オフ］です。

［**JSON** 出力］ボックスには、指定した情報に対応する JSON コンテンツが表示されます。

3. 登録情報をさらに追加するには、［**JSON** 出力］ボックスの JSON コンテンツを編集します。
4. ［**QR** コードを生成］をクリックします。QR コードは JSON 出力の右側に表示されます。
5. QR コード画像を右クリックして保存します。
6. デバイス登録のために画像をユーザーに送信します。

工場出荷時の設定にリセットされたデバイスでこの QR コードをスキャンすると、デバイスは完全管理対象デバイスとして登録されます。

デバイスを登録するには　新しいデバイスまたは工場出荷時の設定にリセットされたデバイスの電源を入れた後、以下を行います：

1. ようこそ画面で画面を 6 回タップすると、QR コードの登録フローが開始されます。
2. プロンプトが表示されたら、Wi-Fi に接続します。QR コードにある Citrix Secure Hub のダウンロード場所には、この Wi-Fi ネットワーク経由でアクセスできます。

   端末が Wi-Fi に接続されると、Google から QR コードリーダーをダウンロードしてカメラを起動します。
3. カメラを QR コードに合わせて、コードをスキャンします。

   Android は、QR コードのダウンロード場所から Citrix Secure Hub をダウンロードし、署名証明書の署名を検証し、Citrix Secure Hub をインストールし、デバイス所有者として設定します。

詳しくは、Android EMM 開発者向け Google ガイド（https://developers.google.com/android/work/prov-devices#qr_code_method）を参照してください。

ゼロタッチ登録

ゼロタッチ登録を使用すると、初めてデバイスの電源をオンにしたときに完全に管理されているデバイスとしてプロビジョニングするようにセットアップできます。

デバイスのリセラーは、Android のゼロタッチポータルにアカウントを作成します。このポータルは、デバイスに構成を適用できるオンラインツールです。Android のゼロタッチポータルを使用して、1 つまたは複数のゼロタッチ登録構成を作成し、アカウントに割り当てられたデバイスにこの構成を適用します。ユーザーがこれらのデバイスの電源をオンにすると、デバイスは自動的に Citrix Endpoint Management に登録されます。デバイスに割り当てられた構成によって、自動登録プロセスが定義されます。

システム要件

- ゼロタッチ登録は、Android 9.0 以降でサポートされます。

リセラーからのデバイスとアカウントの情報

- ゼロタッチ登録の対象となるデバイスは、エンタープライズリセラーまたは Google パートナーから購入します。Android Enterprise のセロタッチパートナー一覧については、Android Web サイトを参照してください。
- リセラーによって作成された Android Enterprise のゼロタッチポータルアカウント。
- リセラーから提供された Android Enterprise のゼロタッチポータルアカウントのログイン情報。

ゼロタッチ構成の作成　ゼロタッチ構成を作成する場合は、カスタム JSON を含めて構成の詳細を指定します。

この JSON を使用して、指定した Citrix Endpoint Management サーバーに登録するようにデバイスを構成します。この例では、サーバーの URL を「URL」に置き換えます。

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL"
7            }
8
9         }
10
11  <!--NeedCopy-->
```

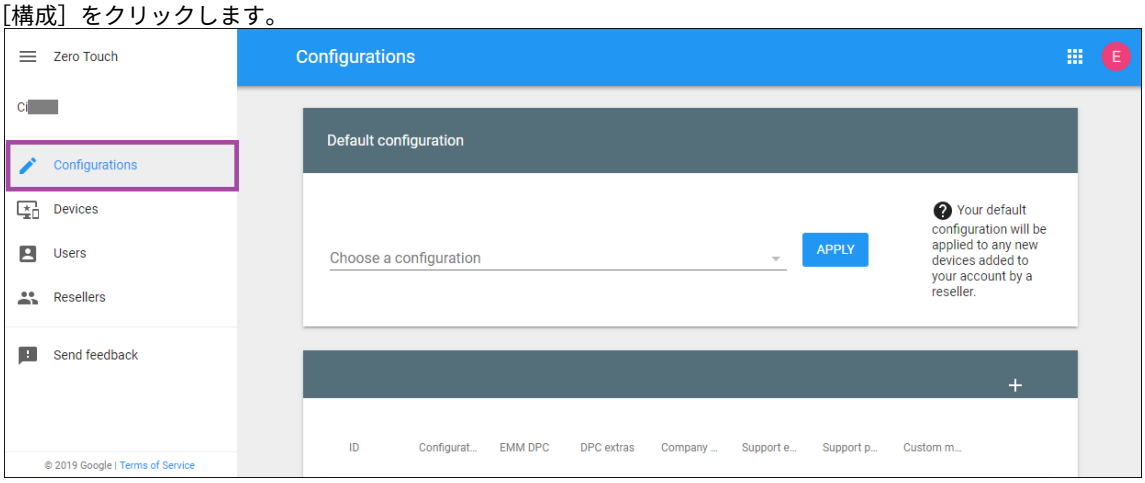
オプションでより多くのパラメーターを持つ JSON を使用して、構成をさらにカスタマイズできます。この例では、Citrix Endpoint Management サーバーと、この構成を使用するデバイスがそのサーバーにログオンするために使用するユーザー名とパスワードを指定します。

```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
11              }
12
13    <!--NeedCopy-->
```

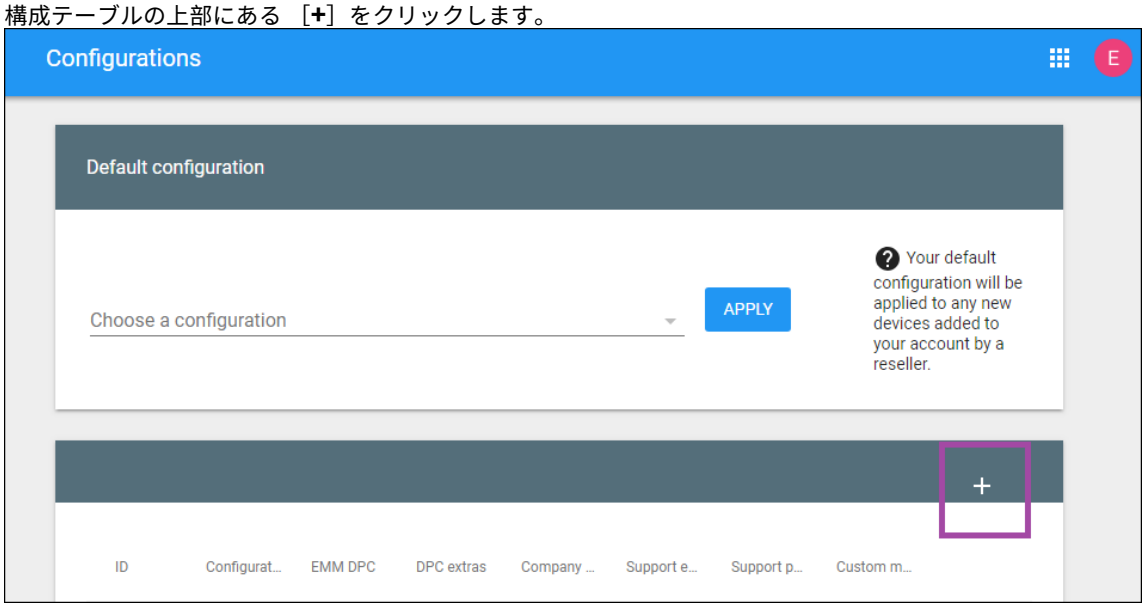
> 重要:
>
> 企業所有デバイスのモードで仕事用プロファイルにデバイスを登録するには、PROVISIONING_ADMIN_EXTRAS_BUNDL

> にあるカスタム JSON に`{ "desiredProvisioningMode": "managedProfile"}`を追加します。

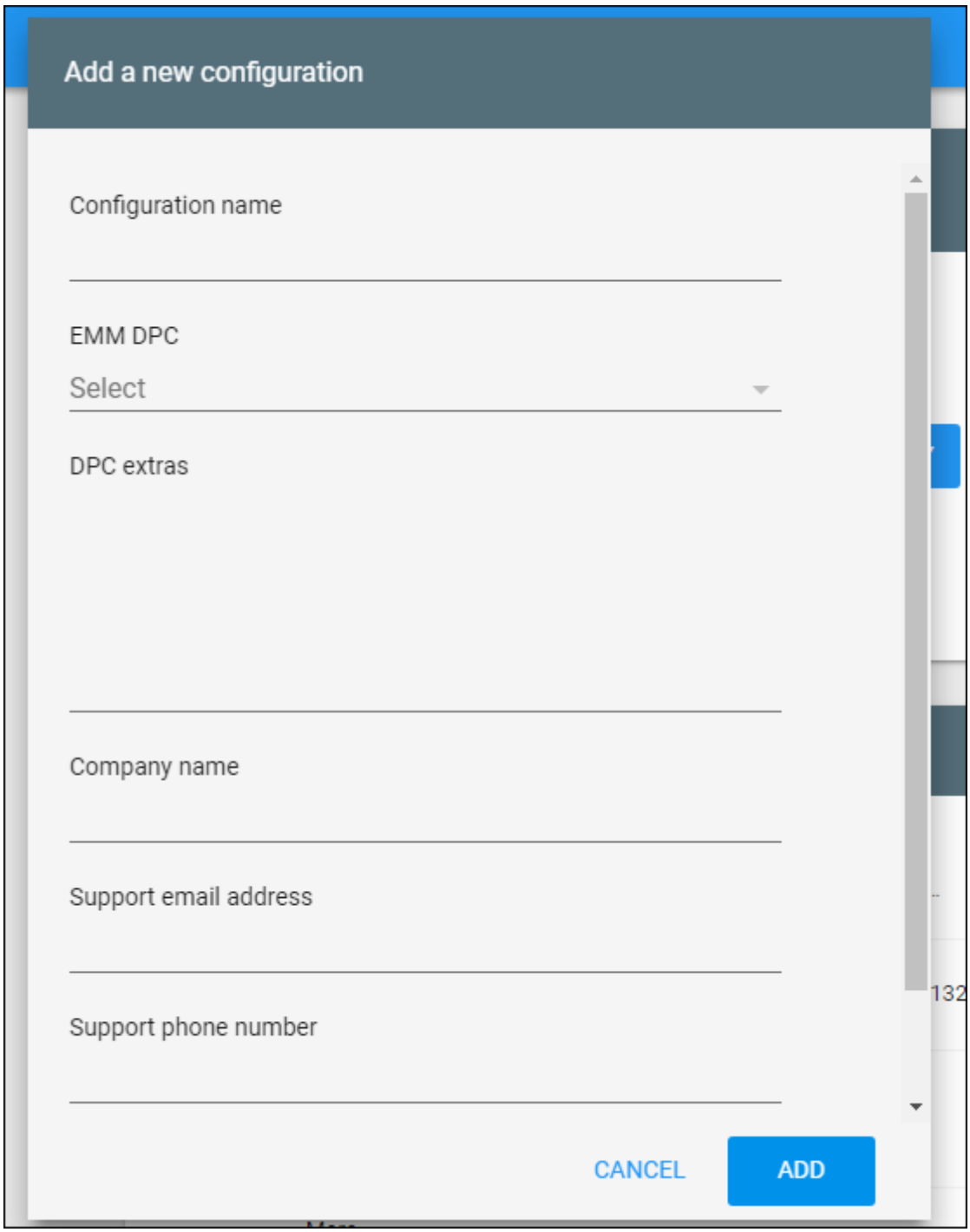
1. Android のゼロタッチポータル（https://partner.android.com/zerotouch）にアクセスします。ゼロタッチデバイスのリセラーのアカウント情報を使用してログインします。
2. ［構成］をクリックします。



3. 構成テーブルの上部にある ［+］をクリックします。



4. 開いた構成ウィンドウに構成情報を入力します。



- **Configuration name**：この構成の名前を入力します。
- **EMM DPC**：［**Citrix Secure Hub**］を選択します。
- **DPC extras**：カスタム JSON テキストをフィールドに貼り付けます。
- **Company name**：デバイスのプロビジョニング中、Android Enterprise のゼロタッチデバイスに表示させる名前を入力します。
- **Support email address**：サポートが必要なときにユーザーが連絡するメールアドレスを入力しま

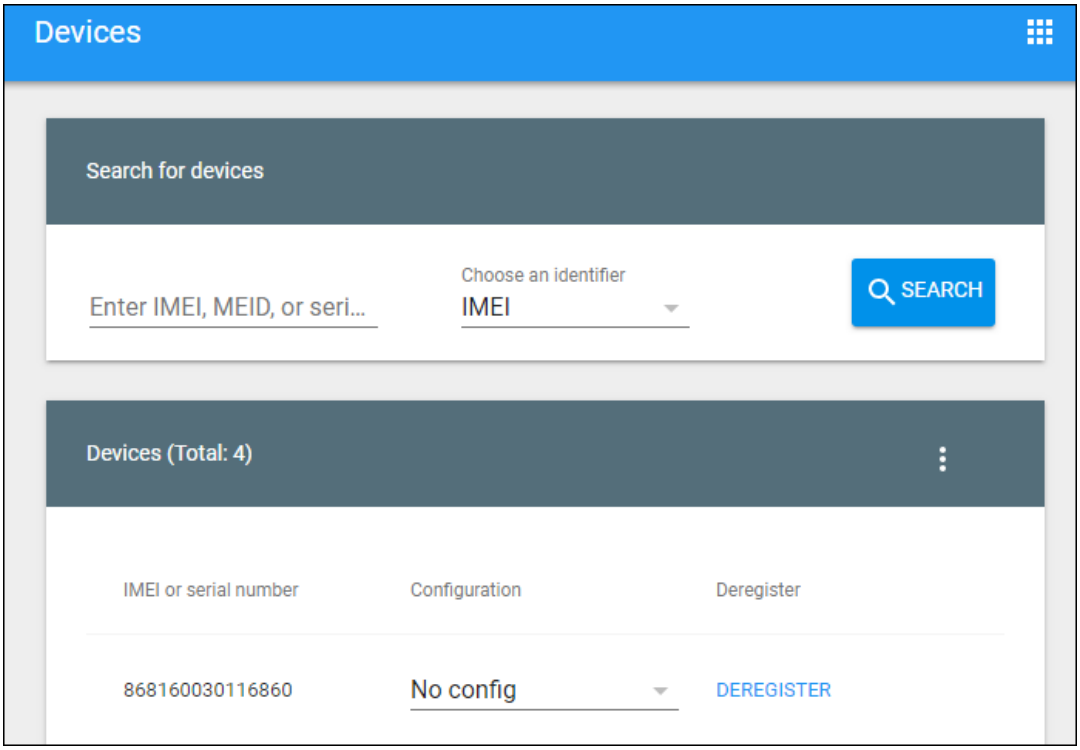
す。このアドレスは、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。

- **Support phone number**：ユーザーがサポートが必要なときに連絡する電話番号を入力します。この電話番号は、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。
- **Custom Message**：オプション。ユーザーが管理者にサポートを求めるように促す、またはデバイスで発生している状況をユーザーに説明するための、1、2 行程度の文章を追加します。このカスタムメッセージは、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。

5. ［追加］をクリックします。
6. さらに構成を作成するには、手順 2～4 を繰り返します。
7. デバイスに構成を適用するには、以下の手順を実行します：

   a) Android のゼロタッチポータルで［**Devices**］をクリックします。

   b) デバイスの一覧でデバイスを探し、割り当てる構成を選択します。



   c) ［**Update**］をクリックします。

CSV ファイルを使用して、多数のデバイスに構成を適用できます。

多数のデバイスに構成を適用する方法については、「ゼロタッチ登録：IT 管理者向け」を参照してください。この Android Enterprise のトピックには、構成を管理してデバイスに適用する方法の詳細が記載されています。

Android Enterprise 専用デバイスのプロビジョニング

Android Enterprise 専用デバイスは、単一のユースケース専用の完全に管理されたデバイスです。これらのデバイスを、このユースケースに必要なタスクを実行する 1 つのアプリまたはアプリの小セットのみに限定します。また、ユーザーがこれらのデバイスで他のアプリを有効にしたり、他の操作を実行したりすることを禁止することもできます。

専用デバイスは、「Android Enterprise の完全に管理されたデバイスのプロビジョニング」の説明のとおり、他の完全に管理されたデバイスで使用されている登録方法のいずれかを使用して登録します。専用デバイスをプロビジョニングするには、登録前に追加のセットアップが必要です。

専用デバイスをプロビジョニングするには:

- Citrix Endpoint Management 管理者が専用デバイスを Citrix Endpoint Management 展開に登録できるように、この管理者の登録プロファイルを追加します。「登録プロファイルの作成」を参照してください。
- 専用デバイスがアプリにアクセスできるようにするには、アプリを許可リストに追加します。
- 必要に応じて、許可されたアプリがロックタスクモードを許可するように設定します。アプリがロックタスクモードになると、ユーザーがアプリを開いたときにデバイス画面にアプリが固定されます。ホームボタンは表示されず、［戻る］ボタンは無効になります。ユーザーは、サインアウトなど、アプリでプログラムされた操作を使用してアプリを終了します。
- 追加した登録プロファイルに各デバイスを登録します。

システム要件

- 専用デバイスの登録は、Android 6.0 以降でサポートされます。

アプリの許可とロックタスクモードの設定

キオスクデバイスポリシーを使用すると、アプリを許可し、ロックタスクモードを設定できます。デフォルトでは、Citrix Secure Hub と Google Play サービスは許可リストに登録されています。

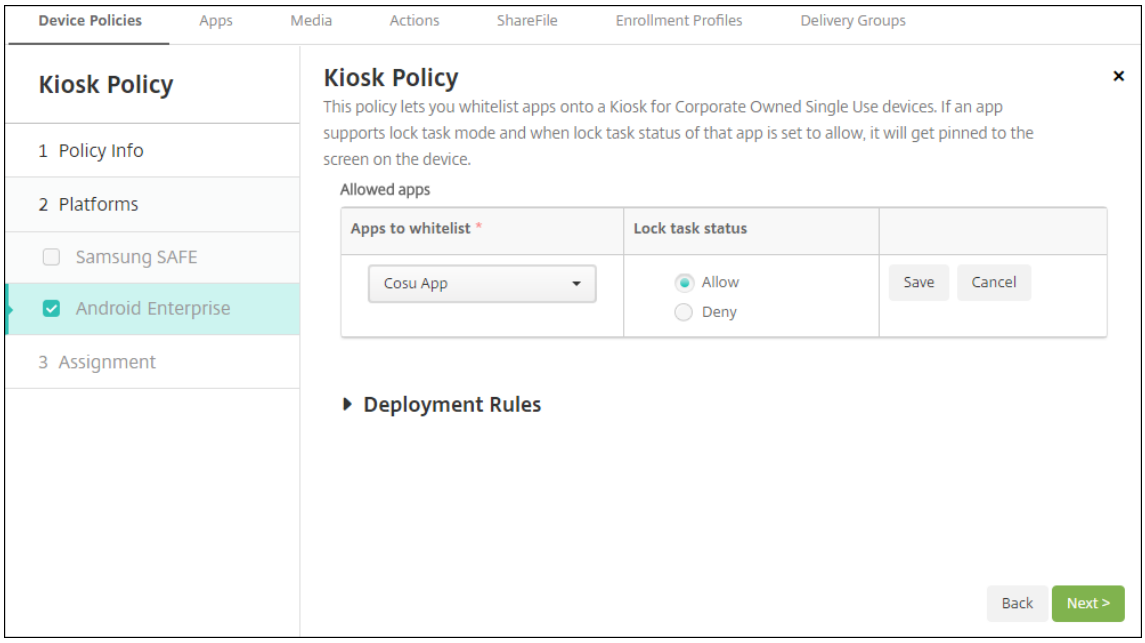
キオスクポリシーを追加するには:

1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］の順にクリックします。［デバイスポリシー］ページが開きます。
2. ［追加］をクリックします。［新しいポリシーの追加］ダイアログボックスが開きます。
3. ［詳細］を展開した後、［セキュリティ］の下の ［キオスク］をクリックします。［キオスクポリシー］ページが開きます。
4. ［プラットフォーム］で ［**Android Enterprise**］を選択します。他のプラットフォームをクリアします。
5. ［ポリシー情報］ペインで、［ポリシー名］および任意で ［説明］を入力します。

6. ［次へ］をクリックし、［追加］をクリックします。
7. アプリを許可し、そのタスクのロックタスクモードを許可または拒否するには：

   一覧から許可するアプリを選択します。

   ユーザーがアプリを起動したときにアプリをデバイス画面に固定するには、［許可］を選択します。アプリをデバイス画面に固定しない場合は、［拒否］を選択します。デフォルトは ［許可］です。



8. ［保存］をクリックします。
9. 別のアプリを許可し、そのタスクのロックタスクモードを許可または拒否する場合は、［追加］をクリックします。
10. 展開規則を構成し、デリバリーグループを選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise での仕事用プロファイルデバイスまたは会社所有のデバイスの仕事用プロファイルのプロビジョニング

Android 9.0～10.x を実行しているデバイスは、「仕事用プロファイルで完全に管理されている」として登録されます。Android 11 以降、デバイスは「会社所有のデバイスの仕事用プロファイル」として登録されます。これらのデバイスはすべて、仕事用と個人用の両方を目的とした会社所有のデバイスです。組織はデバイス全体を管理します。あるポリシーのセットをデバイスに適用し、別のポリシーのセットを仕事用プロファイルに適用できます。

Citrix Endpoint Management コンソールでは、仕事用プロファイルで完全に管理されたデバイスは次の用語で表示されます：

- デバイス所有権は「Corporate」です。
- デバイスの Android Enterprise インストールの種類は「Corporate Owner Personally Enabled」です。

システム要件

- 仕事用プロファイルで完全に管理されたデバイスの登録は、Android 9.0 以降でサポートされます。

デバイスを登録するには

新しいデバイスおよび工場出荷時リセットデバイスは、仕事用プロファイルで完全に管理されたデバイスとして登録します。これらのデバイスは、「Android Enterprise の完全に管理されたデバイスのプロビジョニング」の説明のとおり、他の完全に管理されたデバイスで使用されている登録方法のいずれかを使用します。Android 11 を実行しているデバイスは、そのセクションで説明されている QR コードまたはゼロタッチ登録方法を使用して、会社所有のデバイスの仕事用プロファイルモードで登録できます。

> 重要:
>
> QR コード方式を使用して会社所有のデバイスの仕事用プロファイルモードでデバイスを登録する場合は、JSON 出力の`serverURL`フィールドの上に次を追加します:
> `"desiredProvisioningMode": "managedProfile",`
>
> JSON output
>
> ```
> {
>     "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
> "com.zenprise/com.zenprise.configuration.AdminFunction",
>     "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
> "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
>     "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
> "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
>     "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
>     "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
>     "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
>     "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
>         "desiredProvisioningMode": "managedProfile",
>         "serverURL": "https://testServer.xmqa.cloud.com",
>         "username": "username",
>         "password": "password"
>     }
> ```

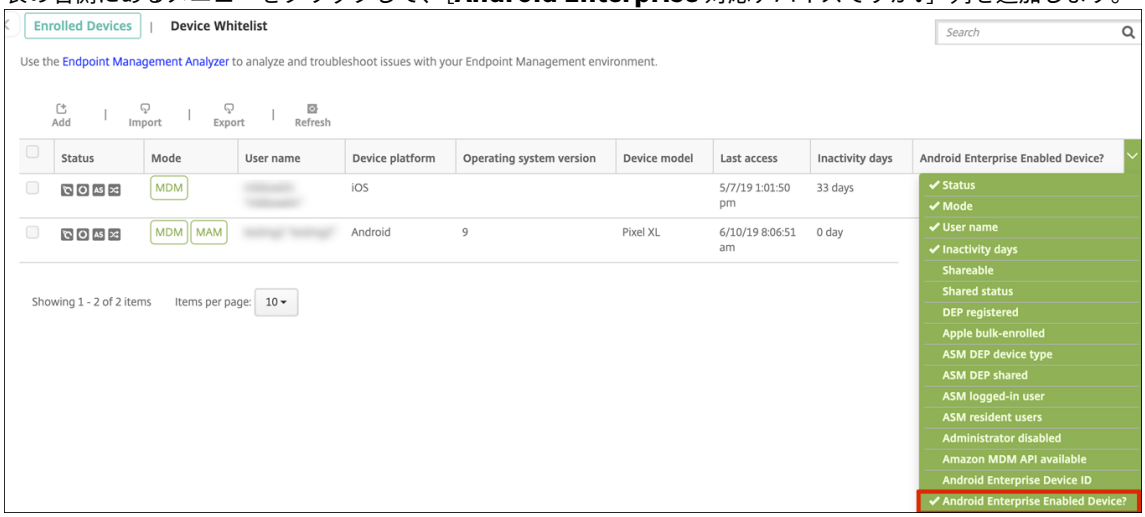
新しいデバイスまたは工場出荷時の状態にリセットされたデバイスではない場合、「Android Enterprise の仕事用プロファイルデバイスのプロビジョニング」の説明に従って仕事用プロファイルデバイスとして登録されます。

Citrix Endpoint Management コンソールでの **Android Enterprise** デバイスの表示

Android Enterprise の完全に管理されたデバイス、専用デバイス、および仕事用プロファイルで完全に管理されたデバイスを表示するには:

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］の順に移動します。

2. 表の右側にあるメニューをクリックして、[**Android Enterprise** 対応デバイスですか**?**] 列を追加します。



3. 利用可能なセキュリティアクションを表示するには、完全に管理されたデバイスを選択して ［セキュリティ］をクリックします。デバイスが完全に管理されている場合、完全なワイプ操作は使用できますが、選択的なワイプ操作は使用できません。これは、デバイスが管理対象 Google Play ストアのアプリのみを許可するためです。ユーザーがパブリックストアからアプリケーションをインストールするオプションはありません。組織はデバイス上のすべてのコンテンツを管理しています。

Android Enterprise デバイスポリシーとアプリポリシーの構成

デバイスレベルとアプリレベルの両方で制御されるポリシーの概要については、「Android Enterprise でサポートされているデバイスポリシーと MDX ポリシー」を参照してください。

ポリシーについて以下のことを把握してください:

- デバイスの制限：数十のデバイス制限により、次のような機能を制御できます：
  - デバイスカメラの使用
  - 仕事用プロファイルと個人用プロファイル間のコピーおよび貼り付けの使用
- **Per-App VPN**：管理対象構成デバイスポリシーを使用して、Android Enterprise の VPN プロファイルを構成します。
- メールポリシー：管理対象構成デバイスポリシーを使用してアプリを構成することをお勧めします。

デバイスポリシー

次の表は、Android Enterprise デバイスで使用可能なデバイスポリシーの一覧です。

> 重要：
>
> Android Enterprise に登録して MDX アプリを使用するデバイスの場合：MDX および Android Enterprise を介して一部の設定を制御できます。MDX に対して最も制限の少ないポリシー設定を使用し、Android Enterprise を介してポリシーを制御します。

アプリの権限	アプリインベントリ	アプリのアンインストール
管理対象アプリの自動更新	接続スケジュール	資格情報
カスタム XML	Citrix Endpoint Management オプション	ファイル
Keyguard 管理	キオスク	Launcher 構成
位置情報	管理対象の構成	ネットワーク
OS 更新	パスコード	制限

仕事用プロファイルで完全に管理されたデバイス（**COPE** デバイス）のデバイスポリシー

仕事用プロファイルで完全に管理されたデバイスの場合、デバイスポリシーによっては、デバイス全体と仕事用プロファイルに個別の設定を適用できます。他のデバイスポリシーを使用して、デバイス全体にのみ設定を適用することも、仕事用プロファイルで完全に管理されたデバイスの仕事用プロファイルにのみ設定を適用することもできます。会社所有のデバイスの仕事用プロファイルモードに登録されているデバイスの場合、ポリシーは仕事用プロファイルにのみ適用され、デバイス全体には適用されません。

ポリシー	適用製品
アプリの権限	仕事用プロファイル
アプリインベントリ	仕事用プロファイル
アプリのアンインストール	仕事用プロファイル
管理対象アプリの自動更新	仕事用プロファイル
接続スケジュール	仕事用プロファイル
資格情報	仕事用プロファイル
カスタム XML	-
Citrix Endpoint Management オプション	仕事用プロファイル
ファイル	仕事用プロファイル
Keyguard 管理	デバイスと仕事用プロファイル
キオスク	-
Launcher 構成	デバイスと仕事用プロファイル
位置情報	デバイス（位置情報モードのみ）
管理対象の構成	仕事用プロファイル
ネットワーク	Device
OS 更新	-
パスコード	デバイスと仕事用プロファイル
制限	デバイスと仕事用プロファイル（デバイス向けと仕事用プロファイル向けに個別のポリシーを作成する）
VPN	-

「Android Enterprise でサポートされているデバイスポリシーと MDX ポリシー」および「MAM SDK の概要」も参照してください。

セキュリティ操作

Android Enterprise は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

セキュリティ操作	仕事用プロファイル	完全管理対象
証明書の書き換え	はい	はい
完全なワイプ	はい（選択的なワイプ後）	はい
検索	はい	はい
ロック	はい	はい
パスワードのロックとリセット	番号	はい
通知（通知音）	はい	はい
取り消し	はい	はい
選択的なワイプ	はい	はい

セキュリティ操作の注意事項

- 位置情報デバイスポリシーでデバイスの位置情報モードが ［高精度］モードまたは ［バッテリー節約］モードに設定されていない限り、検索セキュリティ操作は失敗します。「位置情報デバイスポリシー」を参照してください。
- Android 9.0 より前のバージョンの Android を実行する仕事用プロファイルデバイスの場合：
  - ロックおよびパスワードのリセット操作はサポートされていません。
- Android 9.0 以降の仕事用プロファイルデバイスの場合：
  - 送信されたパスコードによって仕事用プロファイルはロックされます。デバイス自体はロックされません。
  - 仕事用プロファイルにパスコードが設定されていない場合：
    - パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていない場合：デバイスはロックされません。
  - 仕事用プロファイルにパスコードが設定されている場合：
    - パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていない場合：仕事用プロファイルはロックされますが、デバイス自体はロックされません。

Android Enterprise エンタープライズの登録を解除する

Android Enterprise エンタープライズを使用しない場合は、エンタープライズの登録を解除できます。

> 警告:
>
> エンタープライズの登録を解除すると、エンタープライズ経由で登録されていたデバイスの Android Enterprise アプリはデフォルトの状態にリセットされます。これらのデバイスは Google の管理対象外になります。新しい Android Enterprise エンタープライズに登録する場合は、管理対象 Google Play から新しい組織のアプリを承認する必要があります。その後、Citrix Endpoint Management コンソールでアプリを更新できます。

Android Enterprise エンタープライズの登録を解除した後:

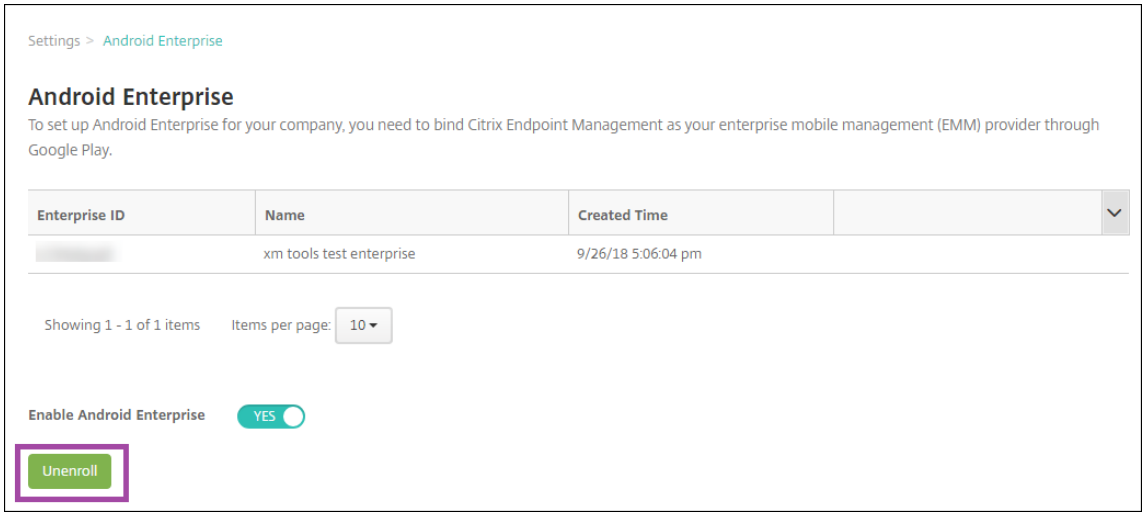
- エンタープライズ経由で登録されていたデバイスとユーザーの Android Enterprise アプリは、デフォルト状態にリセットされます。以前に適用されていた［管理対象の構成］ポリシーは無効になります。
- Citrix Endpoint Management は、エンタープライズ経由で登録されたデバイスを管理します。Google からは、これらのデバイスは管理されてないと見なされるため、新しい Android Enterprise アプリを追加することはできません。［管理対象の構成］ポリシーは適用できません。［スケジュール設定］、［パスワード］、［制限］などのその他のポリシーは、これらのデバイスに適用できます。
- Android Enterprise にデバイスを登録しようとすると、Android Enterprise デバイスではなく Android デバイスとして登録されます。

Citrix Endpoint Management サーバーコンソールと Citrix Endpoint Management ツールを使用して、Android Enterprise エンタープライズの登録を解除できます。

このタスクを実行すると、Citrix Endpoint Management の［ツール］ポップアップウィンドウが表示されます。始める前に、Web ブラウザーに、ポップアップウィンドウを開く権限があることを確認してください。Google Chrome などの一部の Web ブラウザーでは、ポップアップブロックを無効にし、Citrix Endpoint Management サイトのアドレスをポップアップの許可リストに追加する必要があります。

Android Enterprise エンタープライズの登録を解除するには:

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで、［**Android Enterprise**］をクリックします。
3. ［登録解除］をクリックします。



Android Enterprise アプリの配布

March 15, 2024

Citrix Endpoint Management はデバイスに展開されたアプリを管理します。次の種類の Android Enterprise アプリを編成して展開できます。

- 管理対象アプリストアのアプリ：これらのアプリには、管理対象 Google Play ストアで入手できる無料のアプリが含まれます。たとえば、GoToMeeting です。
- **MDX**： MAM SDK で準備された、または MDX Toolkit でラップされたアプリ。これらのアプリには MDX ポリシーが含まれます。MDX アプリは内部ソースおよび公開ストアから取得します。Citrix 業務用モバイルアプリを MDX アプリとして展開します。
- エンタープライズ：別のソースから開発または入手したプライベートアプリ。これらのアプリは、管理対象 Google Play ストアを通じてユーザーに提供します。管理対象 Google Play ストアは、Google エンタープライズのアプリストアです。
- **MDX** 対応のプライベートアプリ： MAM SDK で準備された、または MDX Toolkit でラップされたエンタープライズアプリ。

エンタープライズアプリと MDX 対応のプライベートアプリは、2 つの異なる方法で追加できます。

- この記事の「エンタープライズアプリ」と「MDX 対応のプライベートアプリ」で説明したように、エンタープライズアプリとして Citrix Endpoint Management コンソールにアプリを追加します。
- Google デベロッパーアカウントを使用して、管理対象 Google Play ストアにアプリを直接公開します。次に、管理対象アプリストアのアプリとしてアプリを Citrix Endpoint Management コンソールに追加します。「管理対象アプリストアのアプリ」を参照してください。

Google デベロッパーアカウントを使用してアプリを公開してから、Citrix Endpoint Management コンソールの

使用に切り替えた場合は、アプリの所有権が異なります。この場合、両方の場所でアプリを管理する必要があります。どちらか一方の方法を使用してアプリを追加することをお勧めします。

管理対象の Google Play ストアから自己管理アプリを削除する必要がある場合は、Google でチケットを開きます。開発者は、管理対象の Google Play ストアからアプリを無効にすることはできますが、削除することはできません。

次のセクションでは、Android Enterprise アプリの構成に関する詳細を説明します。アプリの配布については、「アプリの追加」を参照してください。この記事の内容は次のとおりです。

- Web アプリおよび SaaS アプリ、または Web リンクを追加するための一般的なワークフロー
- 必須アプリのワークフロー（エンタープライズアプリおよびパブリックストアアプリの場合）
- エンタープライズアプリ用の Citrix コンテンツ配信ネットワーク（CDN）でエンタープライズアプリを配信する方法

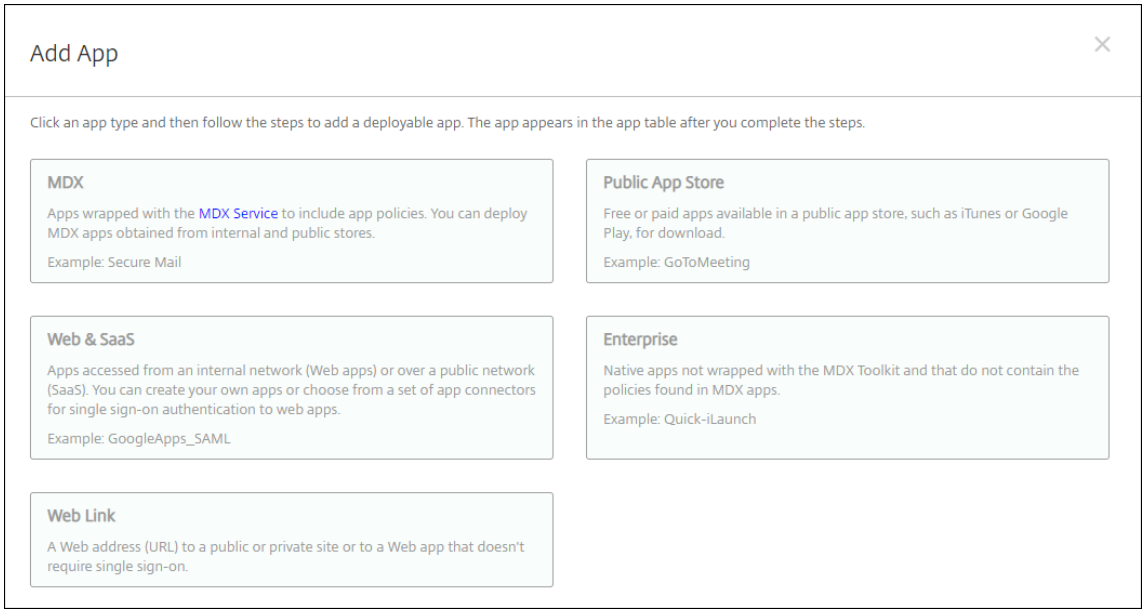
管理対象アプリストアのアプリ

管理対象 Google Play ストアから入手できる無料アプリを Citrix Endpoint Management に追加できます。

> 注:
>
> Google Play ストアのすべてのアプリに管理対象 Google Play からアクセスできるようにするには、サーバープロパティ **Access all apps in the managed Google Play store** を使用します「サーバープロパティ」を参照してください。このプロパティを **true** に設定すると、すべての Android Enterprise ユーザーがパブリック Google Play ストアアプリにアクセスできます。次に、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

手順 **1**：アプリの追加および構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。［追加］をクリックします。
2. ［パブリックアプリストア］をクリックします。



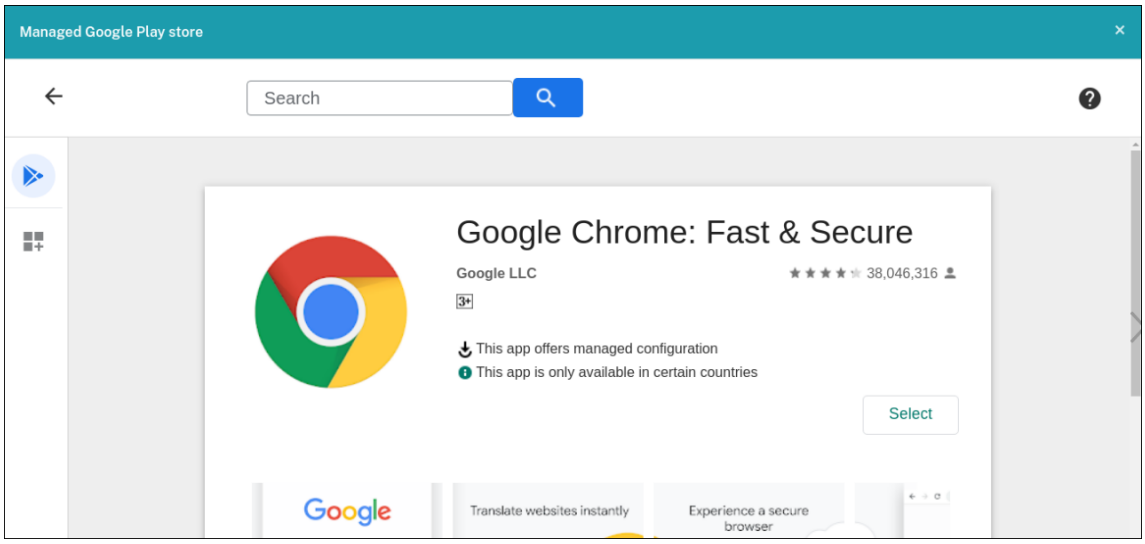
3. ［アプリ情報］ペインで、以下の情報を入力します:

   - 名前: アプリを説明する名前を入力します。この名前は、［アプリ］テーブルの ［アプリ名］の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。

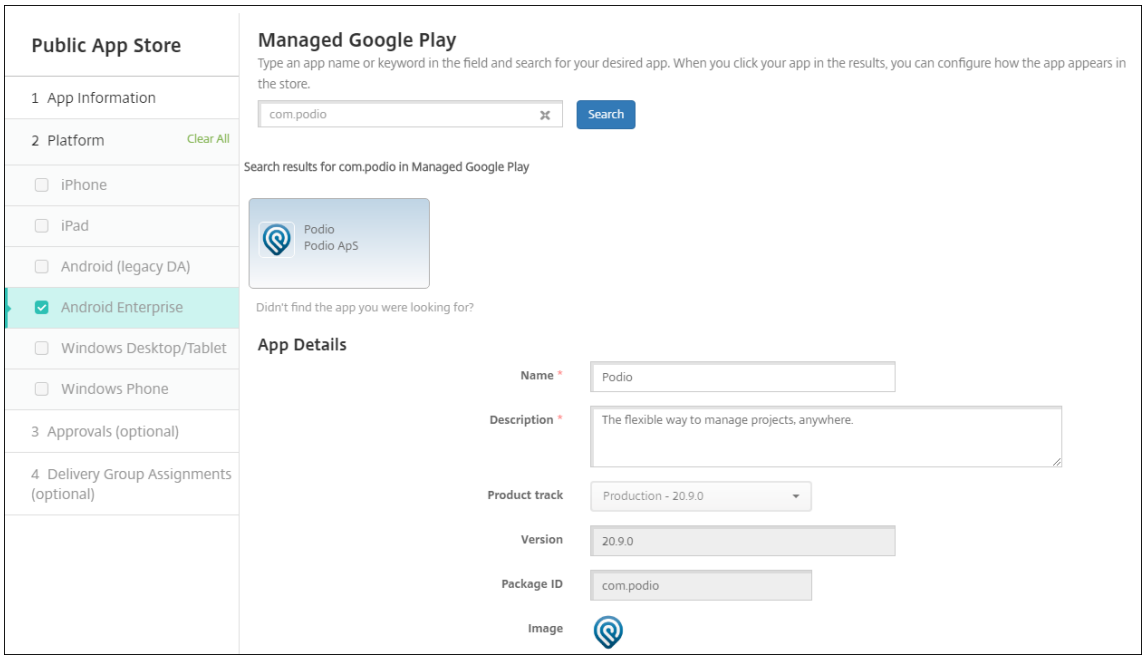
4. プラットフォームとして ［**Android Enterprise**］を選択します。

5. 検索ボックスにアプリ名またはパッケージ ID を入力して、［検索］をクリックします。パッケージ ID は、Google Play ストアで把握することができます。この ID はアプリの URL に含まれています。たとえば、`com.Slack`は`https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`のパッケージ ID です。

6. 検索条件に一致するアプリが表示されます。目的のアプリをクリックしてから、［選択］をクリックします。



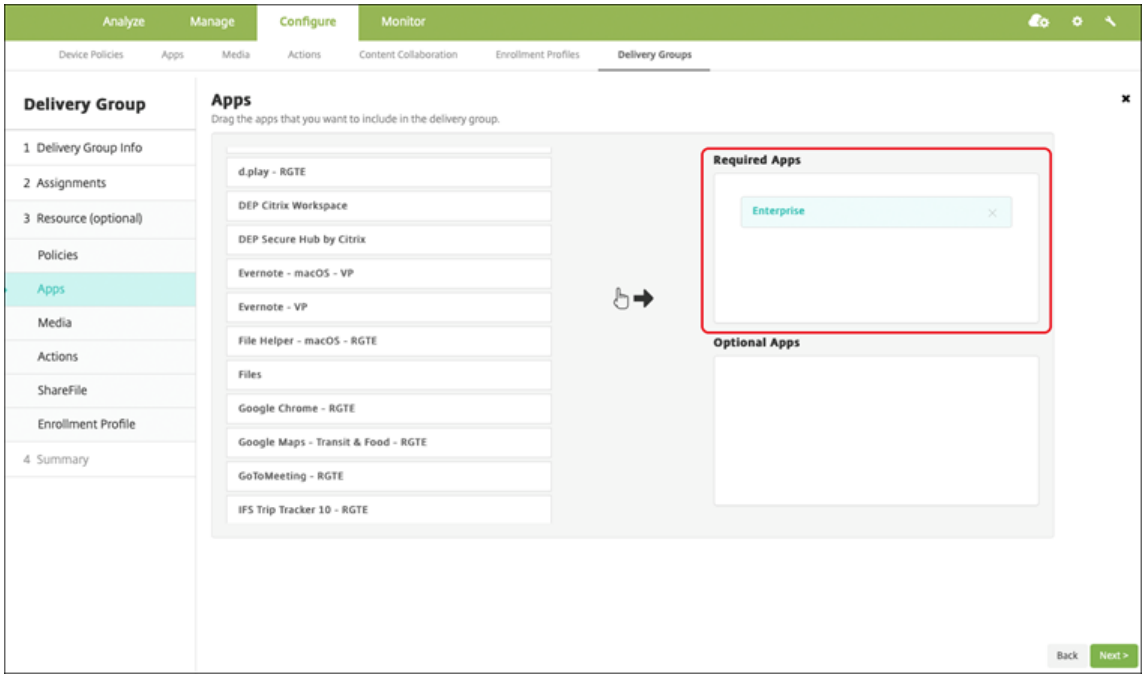
7. もう一度 ［選択］をクリックします。
8. アプリのアイコンをクリックして、アプリの ［名前］と ［説明］を構成します。



9. デリバリーグループをアプリに割り当て、［保存］をクリックします。詳しくは、「リソースの展開」を参照してください。

手順 **2**: アプリの展開を構成

1. ［構成］ **>** ［デリバリーグループ］の順に移動して、構成したデリバリーグループを選択します。［編集］をクリックします。
2. ［アプリ］セクションで、目的のアプリを ［必須アプリ］ボックスにドラッグします。



3. ［概要］ページで ［保存］をクリックします。
4. ［デリバリーグループ］ページで、デリバリーグループを選択して ［展開］をクリックします。

MDX アプリ

MDX ファイルを Citrix Endpoint Management に追加し、アプリの詳細とポリシー設定を構成します。Android Enterprise 用に Citrix 業務用モバイルアプリを構成するには、それらを MDX アプリとして追加します。各デバイスプラットフォームの種類で使用できるアプリポリシーについて詳しくは、以下を参照してください:

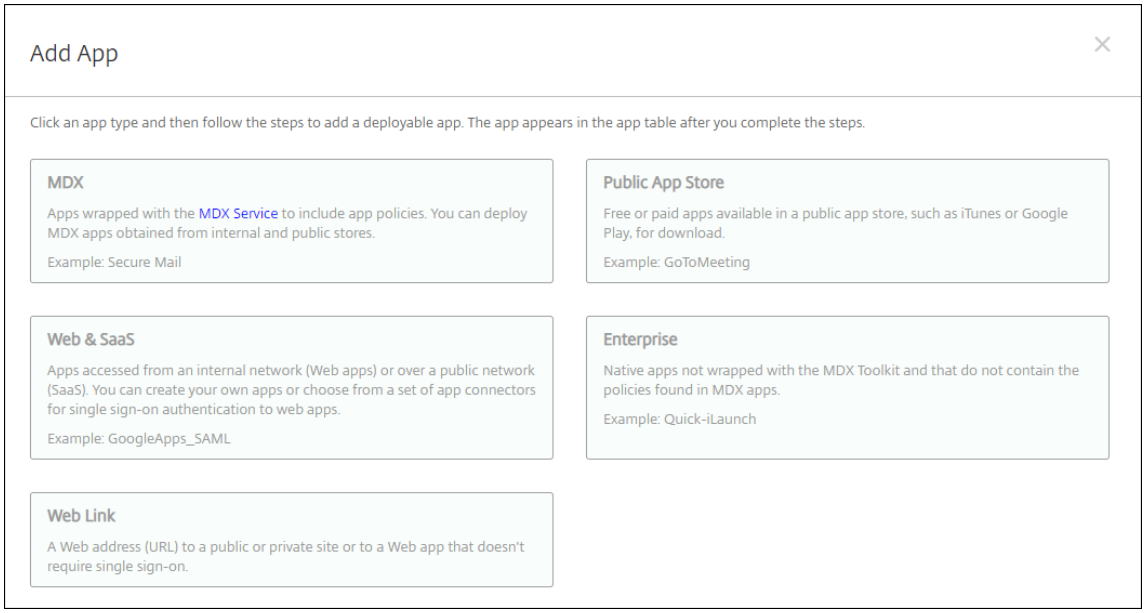
- MAM SDK の概要
- MDX ポリシーの概要

手順 **1**: アプリの追加および構成

1. Citrix 業務用モバイルアプリの場合は、パブリックストア MDX ファイルをダウンロードします。https://www.citrix.com/downloadsに移動します。**Citrix Endpoint Management**（**XenMobile**）、**Citrix Endpoint Management Productivity Apps** の順に移動します。

   他の種類の MDX アプリについては、MDX ファイルを入手します。

2. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］の順にクリックします。［追加］をクリックします。［アプリの追加］ダイアログボックスが開きます。



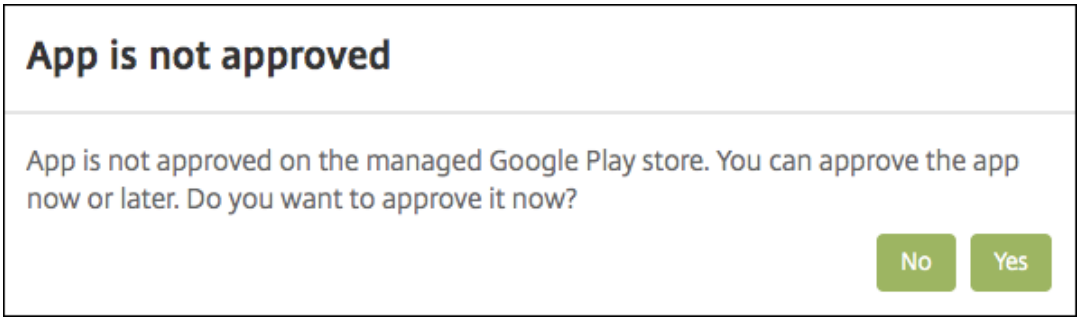
3. [**MDX**] をクリックします。[**MDX** アプリ情報] ページが開きます。[アプリ情報] ペインで、以下の情報を入力します:

   - 名前: アプリを説明する名前を入力します。この名前は、[アプリ] テーブルの [アプリ名] の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。

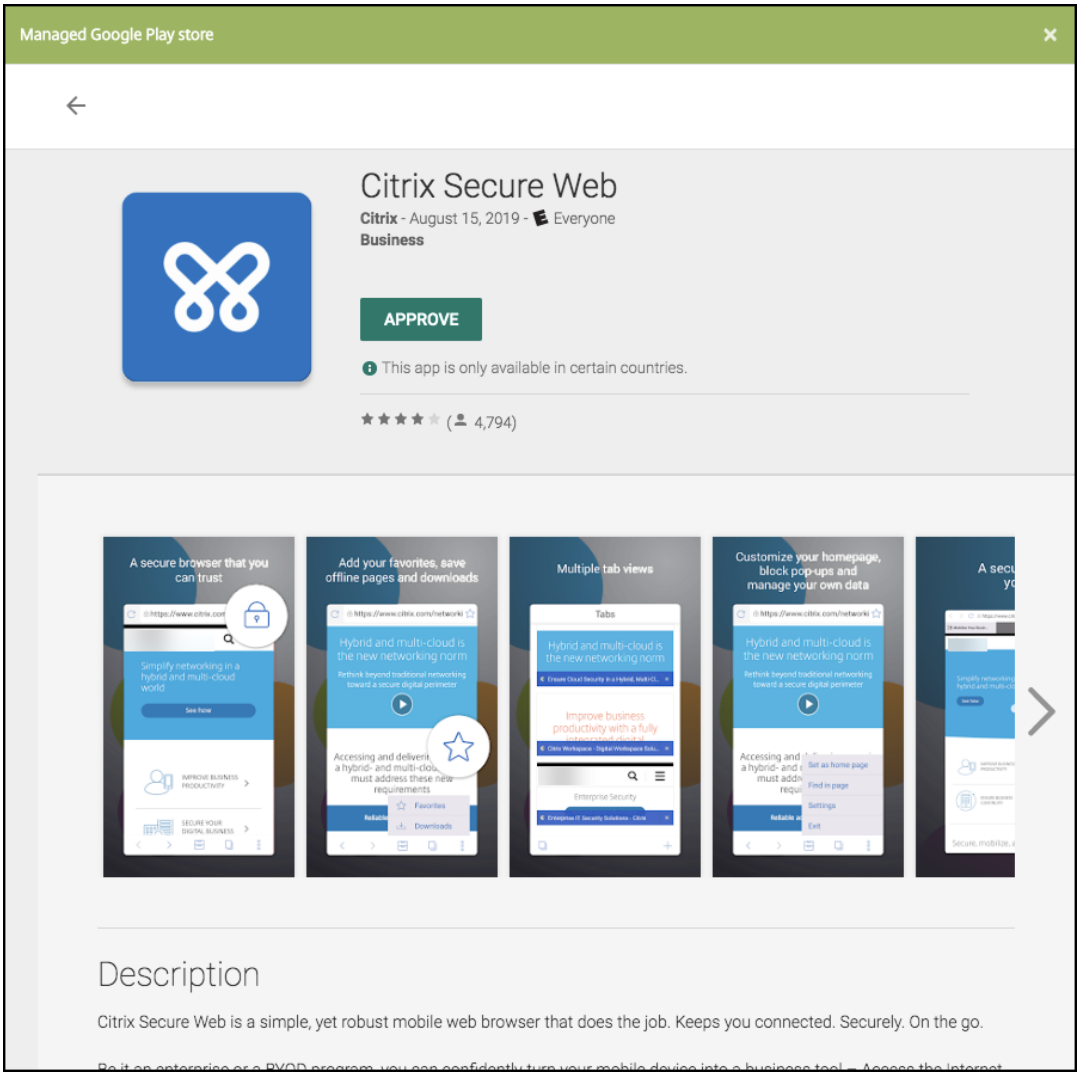
4. プラットフォームとして [**Android Enterprise**] を選択します。

5. [アップロード] をクリックして、MDX ファイルに移動します。Android Enterprise は、MAM SDK または MDX Toolkit で準備されたアプリのみをサポートします。

   - 追加されたアプリケーションが、管理対象 Google Play ストアからの承認を必要としているかどうかが UI によって通知されます。Citrix Endpoint Management コンソールを終了せずにアプリケーションを承認するには、[はい] をクリックします。

     管理対象 Google Play ストアが開いたら、画面の指示に従ってアプリを承認して保存します。



アプリが正常に追加されると、［アプリケーション詳細］ページが表示されます。

6. 次の設定を構成します：

   - ファイル名：アプリに関連付けられているファイル名を入力します。
   - アプリの説明：アプリの説明を入力します。
   - アプリのバージョン：任意で、アプリのバージョン番号を入力します。
   - パッケージ **ID**：管理対象 Google Play ストアから取得したアプリのパッケージ ID を入力します。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。

7. **MDX** ポリシーを構成します。MDX ポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域で適用するオプションが含まれます。コンソールでは、ポリシーごとに、

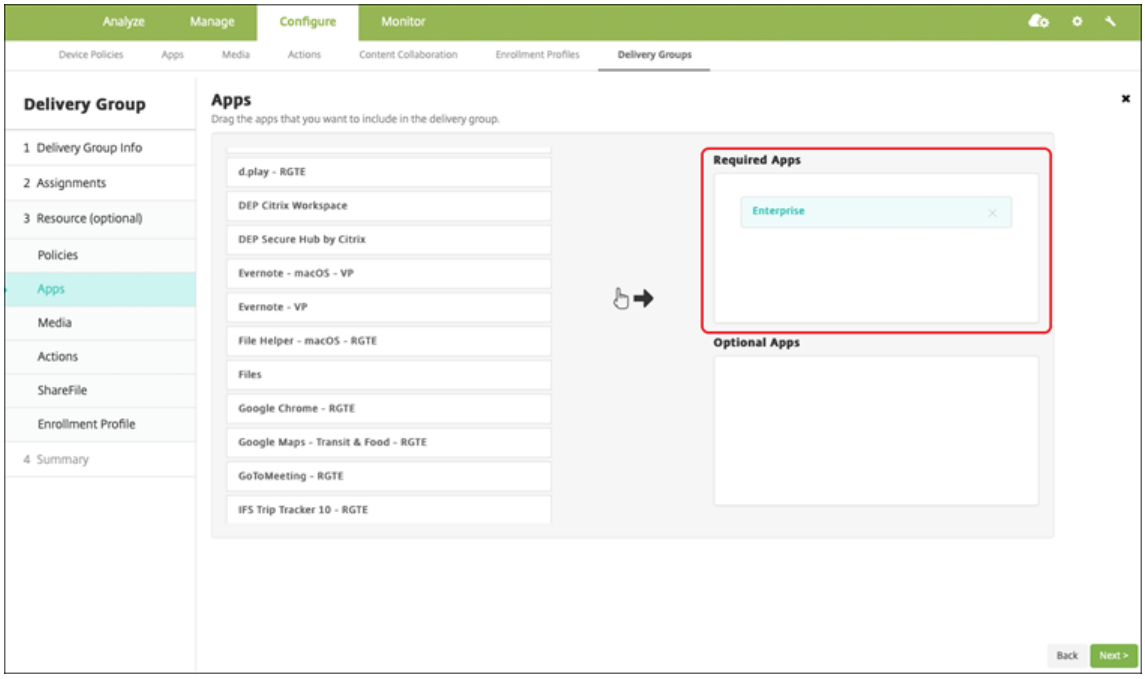
ポリシーを説明するヒントが提供されます。各デバイスプラットフォームの種類で使用できるアプリポリシーについて詳しくは、以下を参照してください:

- MAM SDK の概要
- MDX ポリシーの概要

8. 展開規則とストア構成を構成します。
9. デリバリーグループをアプリに割り当て、[保存] をクリックします。詳しくは、「リソースの展開」を参照してください。

手順 **2**: アプリの展開を構成

1. [構成] **>** [デリバリーグループ] の順に移動して、構成したデリバリーグループを選択します。[編集] をクリックします。
2. [アプリ] セクションで、目的のアプリを [必須アプリ] ボックスにドラッグします。



3. [概要] ページで [保存] をクリックします。
4. [デリバリーグループ] ページで、デリバリーグループを選択して [展開] をクリックします。

エンタープライズアプリ

エンタープライズアプリは、MAM SDK または MDX Toolkit で準備されていないプライベートアプリです。これらのアプリは自分で開発するか、他のソースから直接入手します。エンタープライズアプリを追加するには、アプリに

関連付けられた APK ファイルが必要です。Google のプライベートアプリのベストプラクティスに従っていることを確認してください。

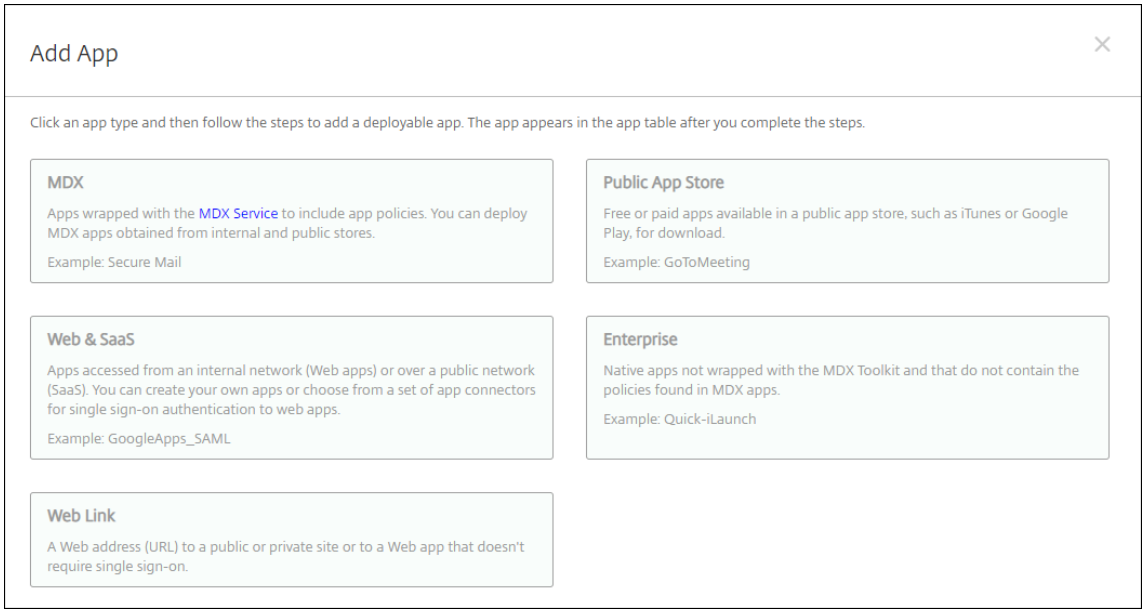
詳しくは、このビデオをご覧ください:

手順 **1**: アプリの追加および構成

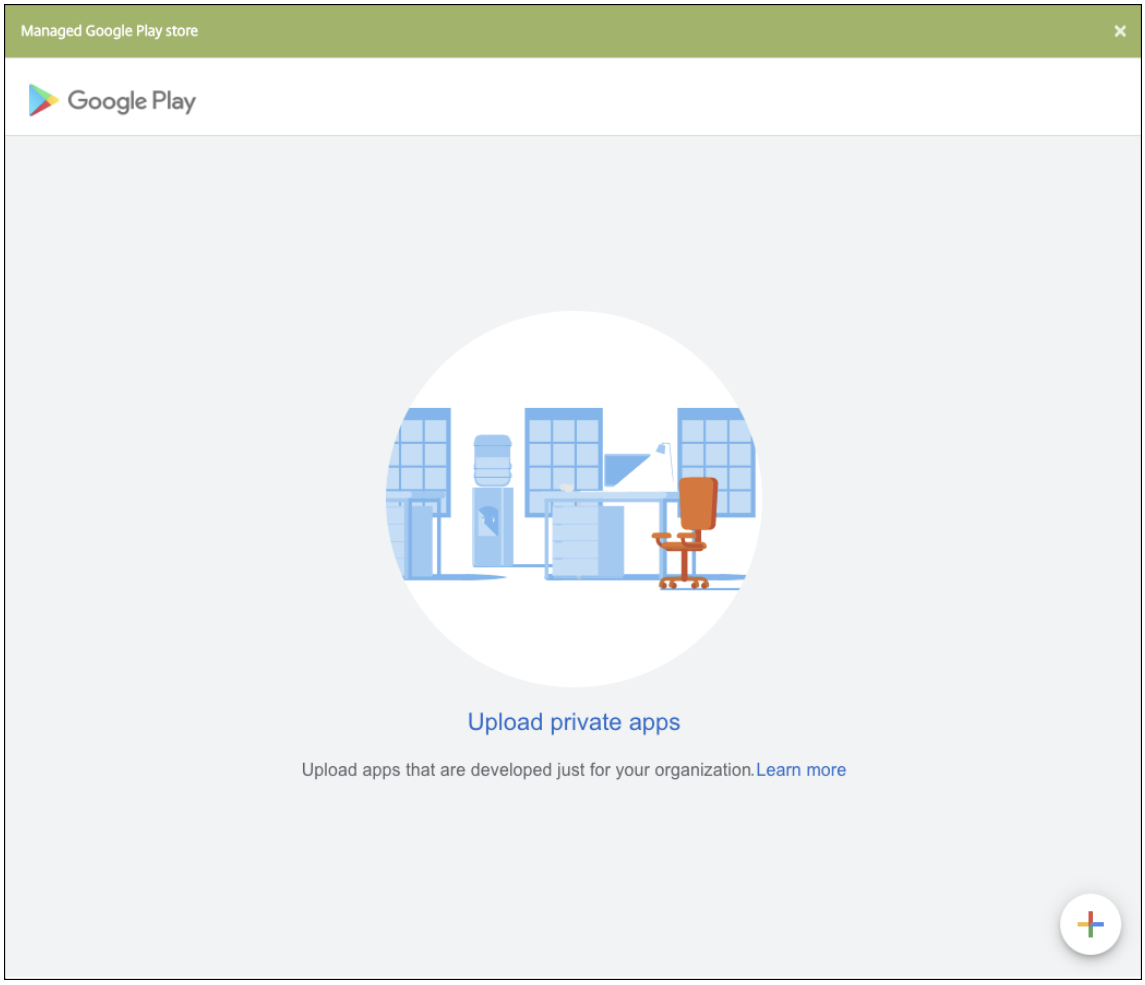
2 つのうちどちらかの方法でアプリを追加します:

- アプリを管理対象 Google Play ストアに直接公開し、管理対象 Play ストアアプリとして Citrix Endpoint Management コンソールに追加します。限定公開アプリを公開する方法は Google のドキュメントに従い、その後「管理対象アプリストアのアプリ」セクションの手順に従います。
- アプリをエンタープライズアプリとして Citrix Endpoint Management コンソールに追加します。次の手順を実行します:

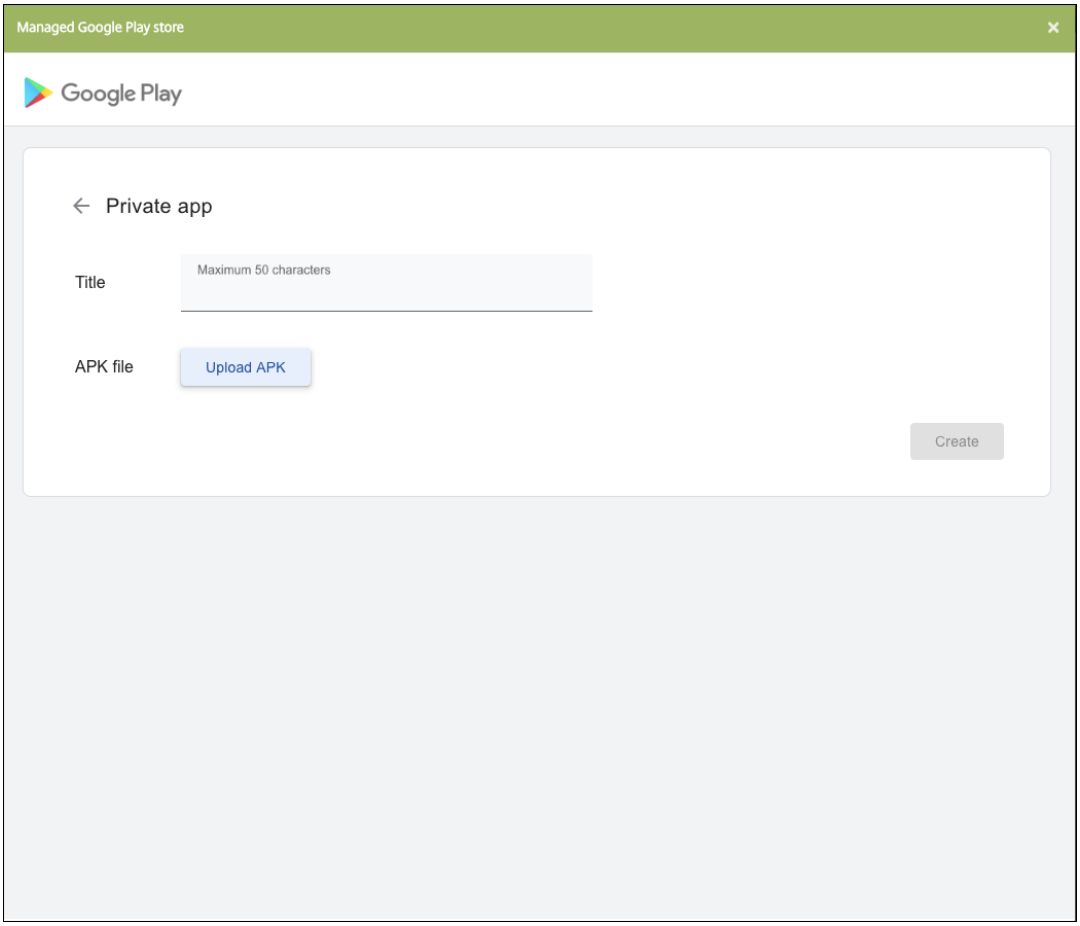
1. Citrix Endpoint Management コンソールで、[構成] **>** [アプリ] の順にクリックします。[追加] をクリックします。[アプリの追加] ダイアログボックスが開きます。



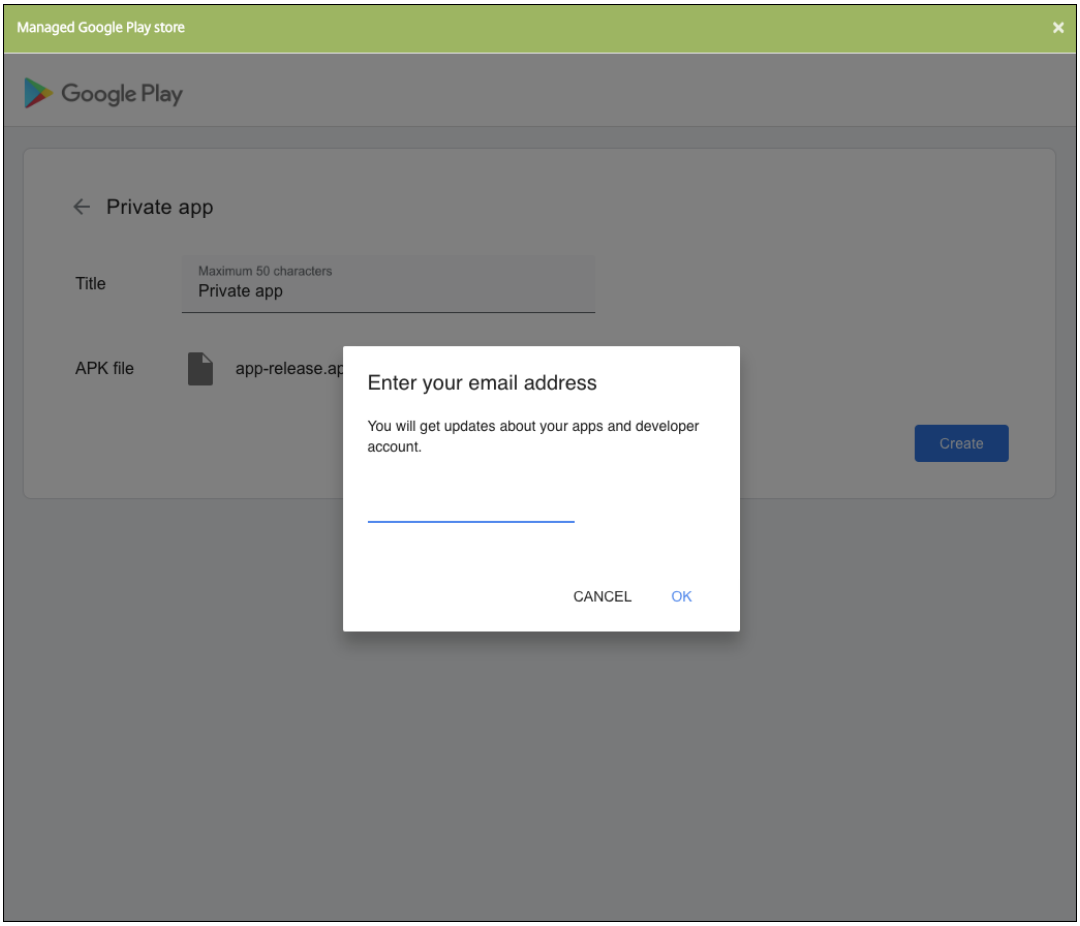
2. ［エンタープライズ］をクリックします。［アプリ情報］ペインで、以下の情報を入力します：
   - 名前：アプリの説明的な名前を入力します。この名前は、［アプリ］の表の［アプリ名］の下に表示されます。
   - 説明：任意で、アプリの説明を入力します。
3. プラットフォームとして ［**Android Enterprise**］を選択します。
4. ［アップロード］ボタンをクリックすると、管理対象 Google Play ストアが開きます。プライベートアプリを公開するために開発者アカウントを登録する必要はありません。右下隅にある ［＋］アイコンをクリックして続行します。



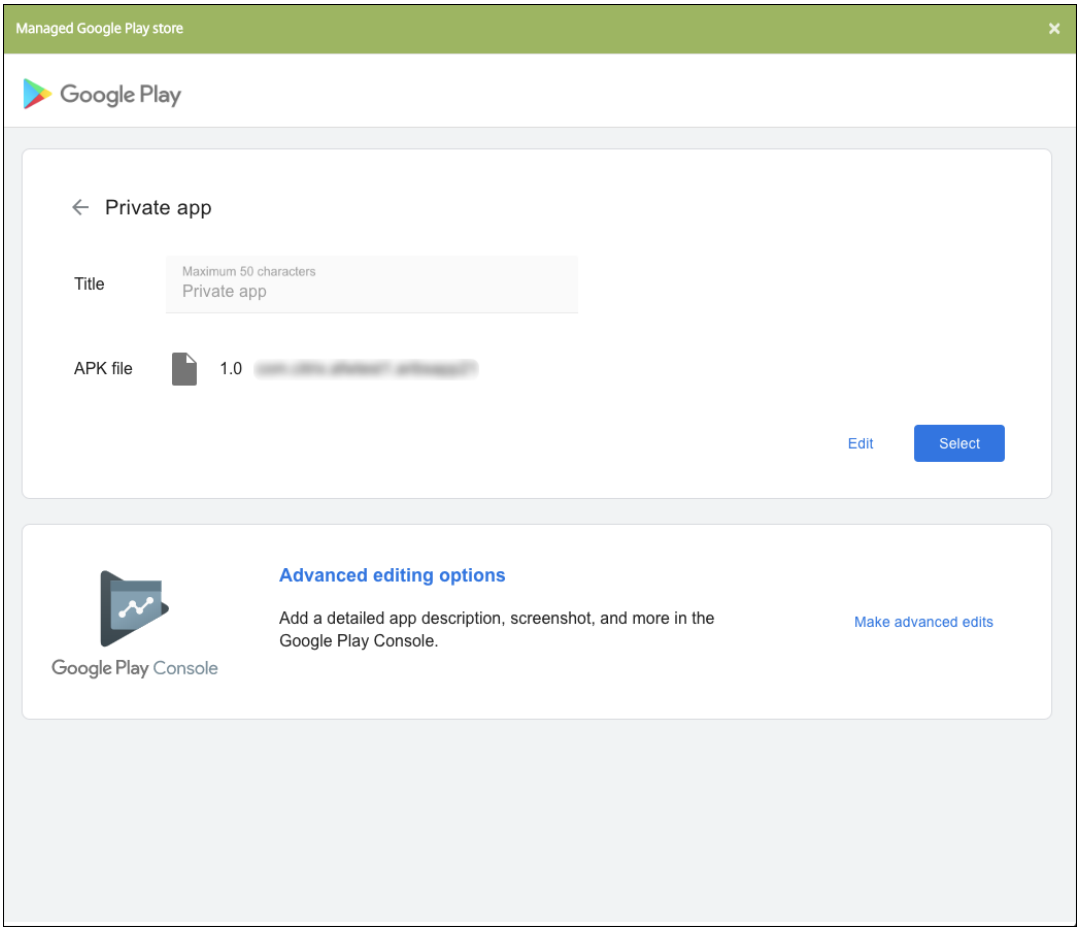
a) アプリの名前を入力し、.apk ファイルをアップロードします。入力が終わったら、［作成］をクリックします。プライベートアプリが公開されるまでに最大 10 分かかる場合があります。



b) メールアドレスを入力すると、アプリに関する最新情報が得られます。



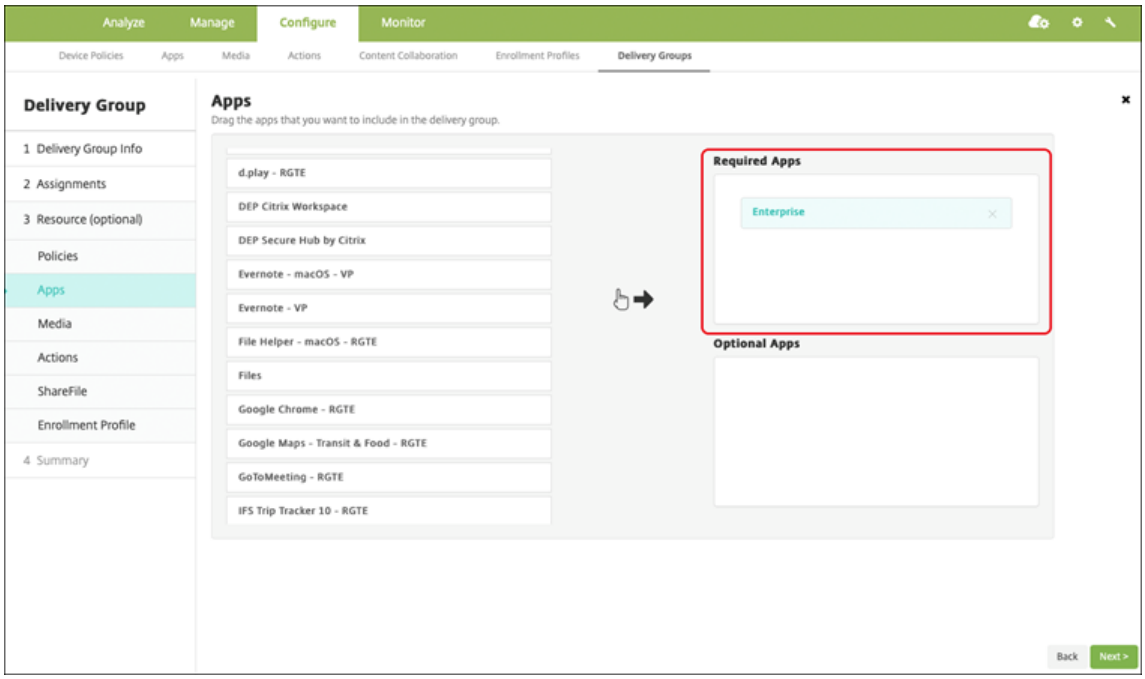
c) アプリケーションが公開されたら、プライベートアプリのアイコンをクリックします。アプリの説明を追加したり、アプリのアイコンを変更したりする場合は、［高度な編集を行う］をクリックします。それ以外の場合は、［選択］をクリックしてアプリ情報のページを開きます。



5. ［次へ］をクリックします。プラットフォームのアプリ情報ページが開きます。
6. プラットフォームの種類について、以下の設定を構成します：
   - ファイル名：任意で、アプリの名前を新たに入力します。
   - アプリの説明：任意で、アプリの説明を新たに入力します。
   - アプリのバージョン：このフィールドは変更できません。
   - パッケージ **ID**：アプリの一意の識別子。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
7. 展開規則とストア構成を構成します。
8. デリバリーグループをアプリに割り当て、［保存］をクリックします。詳しくは、「リソースの展開」を参照してください。

手順 **2**：アプリの展開を構成

1. ［構成］**>**［デリバリーグループ］の順に移動して、構成したデリバリーグループを選択します。［編集］をクリックします。
2. ［アプリ］セクションで、目的のアプリを ［必須アプリ］ボックスにドラッグします。



3. ［概要］ページで ［保存］をクリックします。
4. ［デリバリーグループ］ページで、デリバリーグループを選択して ［展開］をクリックします。

MDX 対応のプライベートアプリ

Android Enterprise アプリを MDX 対応エンタープライズアプリとして追加するには、以下を実行します：

1. プライベート Android Enterprise アプリを作成し、アプリを MDX 対応にします。
2. Citrix Endpoint Management コンソールにアプリを追加します。
   - 管理対象 Google Play ストアでアプリをホストして公開します。
   - アプリを Enterprise アプリとして Citrix Endpoint Management コンソールに追加します。
3. MDX ファイルを Citrix Endpoint Management に追加します。

Google Play ストアにアプリをホストして公開する場合、Google 証明書の署名をオプトインしないでください。アプリの MDX 対応に使用したのと同じ証明書でアプリに署名します。アプリの公開について詳しくは、アプリを公開するとアプリへの署名に関する Google ドキュメントを参照してください。MAM SDK はアプリをラップしないため、アプリの開発で使用した証明書以外の証明書は必要ありません。

Google Play コンソールを使用したプライベートアプリの公開について詳しくは、Play Console から限定公開アプリを公開する方法についての Google ドキュメントを参照してください。

Citrix Endpoint Management からアプリを公開するには、以下のセクションを参照してください。

Android Enterprise アプリの準備

Android Enterprise アプリを作成するには、必ず Google の限定公開アプリに関するお勧めの方法に従います。

Android Enterprise アプリの作成後、MAM SDK をアプリと統合するか、MDX Toolkit を使用してアプリをラップします。次に、作成されたファイルを XenMobile に追加します。

更新された.apk ファイルをアップロードすることで、アプリを更新できます。次の手順で、MDX Toolkit を使用したアプリのラッピングについて説明します。

1. Android Enterprise アプリを作成し、署名付きの.apk ファイルを生成します。
2. 次のサンプルファイルには、すべての既知のポリシーが含まれていますが、一部はご使用の環境に該当しない場合があります。使用できない設定は無視されます。次のパラメーターを使用して XML ファイルを作成します:

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
        <ActivePollPeriod>60</ActivePollPeriod>
        <PublicFileAccessLimitsList/>
        <CutAndCopy>Unrestricted</CutAndCopy>
        <Paste>Unrestricted</Paste>
        <DocumentExchange>Unrestricted</DocumentExchange>
        <OpenInExclusionList/>
        <InboundDocumentExchange>Unrestricted</
            InboundDocumentExchange>
```



```
        <InboundDocumentExchangeWhitelist/>
        <connectionSecurityLevel>TLS</connectionSecurityLevel>
        <DisableCamera>false</DisableCamera>
        <DisableGallery>false</DisableGallery>
        <DisableMicrophone>false</DisableMicrophone>
        <DisableLocation>false</DisableLocation>
        <DisableSms>false</DisableSms>
        <DisableScreenCapture>false</DisableScreenCapture>
        <DisableSensor>false</DisableSensor>
        <DisableNFC>false</DisableNFC>
        <BlockLogs>false</BlockLogs>
        <DisablePrinting>false</DisablePrinting>
        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
           MvpnNetworkAccess>
        <MvpnSessionRequired>False</MvpnSessionRequired>
        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
        <DisableLocalhostConnections>false</
           DisableLocalhostConnections>
        <CertificateLabel/>
        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
        <DefaultLoggerLevel>15</DefaultLoggerLevel>
        <MaxLogFiles>2</MaxLogFiles>
        <MaxLogFileSize>2</MaxLogFileSize>
        <RedirectSystemLogs>false</RedirectSystemLogs>
        <EncryptLogs>false</EncryptLogs>
        <GeofenceLongitude>0</GeofenceLongitude>
        <GeofenceLatitude>0</GeofenceLatitude>
        <GeofenceRadius>0</GeofenceRadius>
        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
        <Authentication>OfflineAccessOnly</Authentication>
        <ReauthenticationPeriod>480</ReauthenticationPeriod>
        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
    </Policies>
</MobileAppPolicies>
<!--NeedCopy-->
```

3. MDX Toolkit を使用してアプリをラップします。MDX Toolkit の使用について詳しくは、「Android モバイルアプリのラッピング」を参照してください。

   apptype パラメーターを **Premium** に設定します。次に説明するコマンドで、前の手順の XML ファイルを使用します。

   アプリのストア URL がわかっている場合は、**storeURL** パラメーターをストア URL に設定します。アプリを公開した後、ストア URL からアプリをダウンロードします。

   以下に、SampleAEapp というアプリをラップするために使用する MDX Toolkit コマンドの例を示します:

```
```
 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
    Duser.variant
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
```

 
```

```
  -MinPlatform 5.0
  -keystore /MyKeystore
  -storepass mystorepwd123
  -keyalias key0
  -keypass mykeypwd123
  -storeURL "https://play.google.com/store/apps/details?id=
     SampleAEappPackage"
  -appType Premium
  -premiumMdxPolicies <Path to Premium policy XML>
<!--NeedCopy--> ```
```

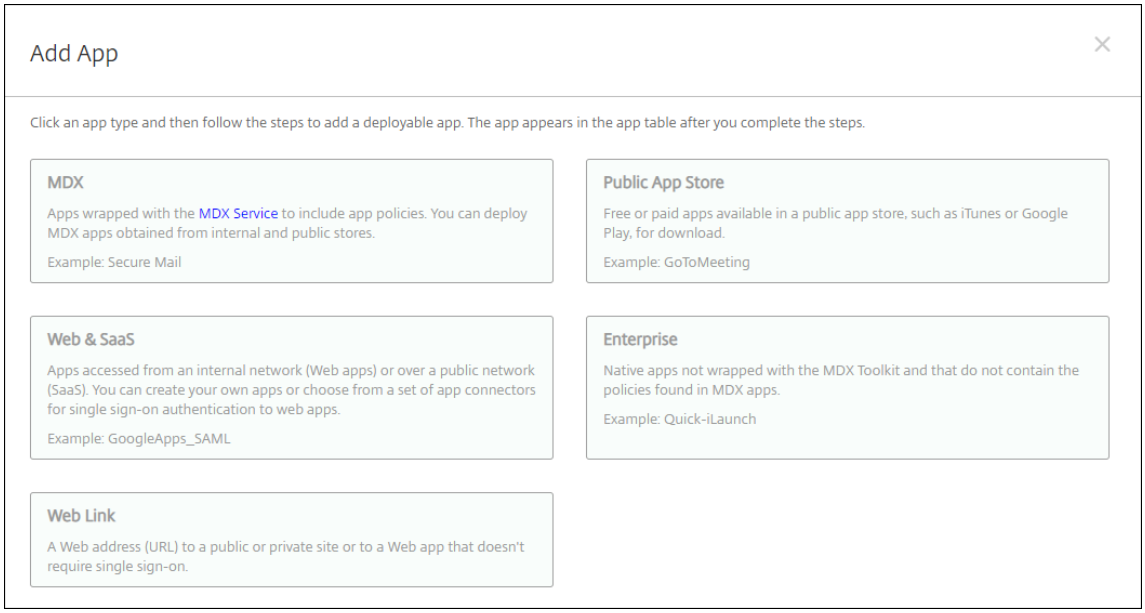
アプリをラップすると、ラップされた.apk ファイルと.mdx ファイルが生成されます。

ラップされた**.apk** ファイルを追加する

2 つのうちどちらかの方法でアプリを追加します:

- アプリを管理対象 Google Play ストアに直接公開し、管理対象 Play ストアアプリとして Citrix Endpoint Management コンソールに追加します。限定公開アプリを公開する方法は Google のドキュメントに従い、その後「管理対象アプリストアのアプリ」セクションの手順に従います。
- アプリをエンタープライズアプリとして Citrix Endpoint Management コンソールに追加します。次の手順を実行します:

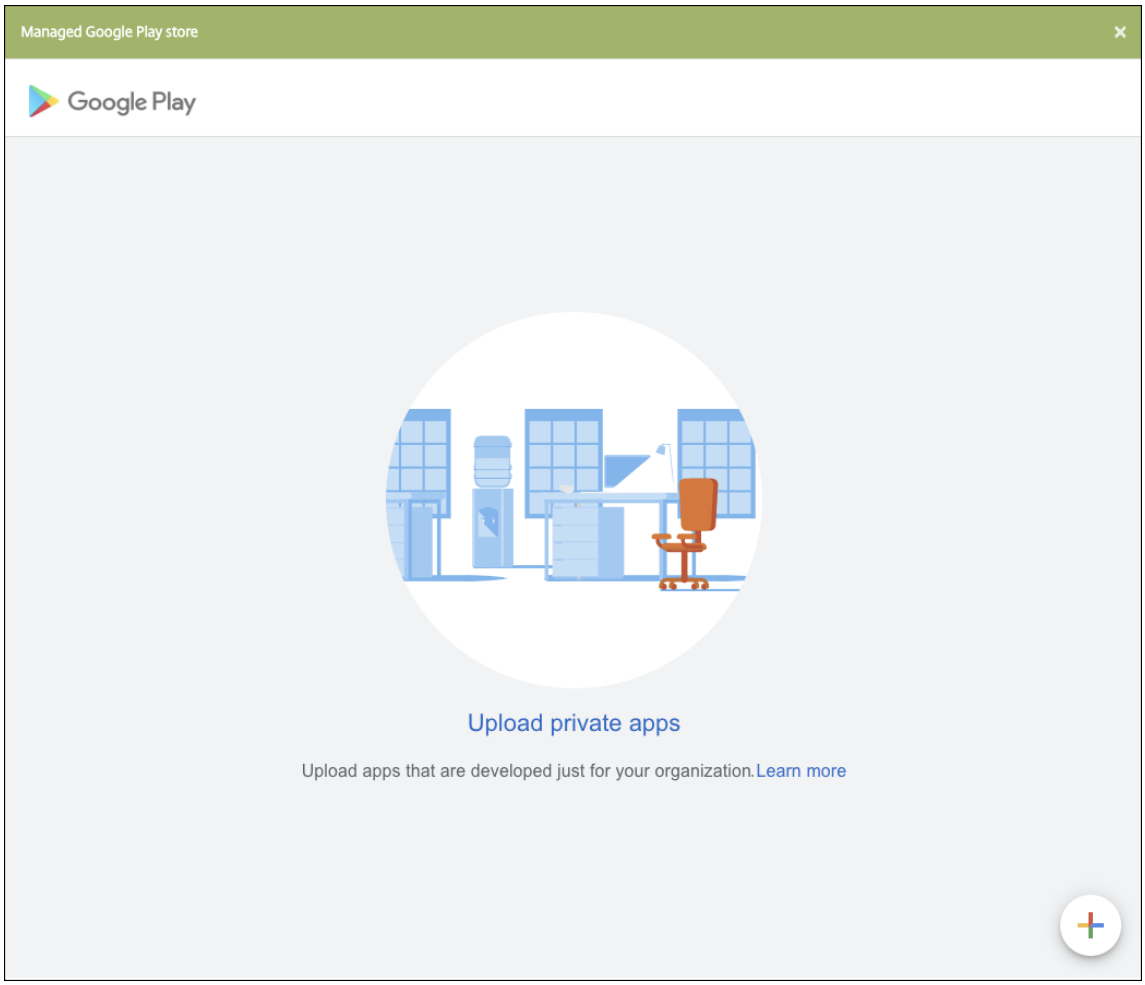
1. Citrix Endpoint Management コンソールで、[構成] > [アプリ] の順にクリックします。[アプリ] ページが開きます。
2. [追加] をクリックします。[アプリの追加] ダイアログボックスが開きます。



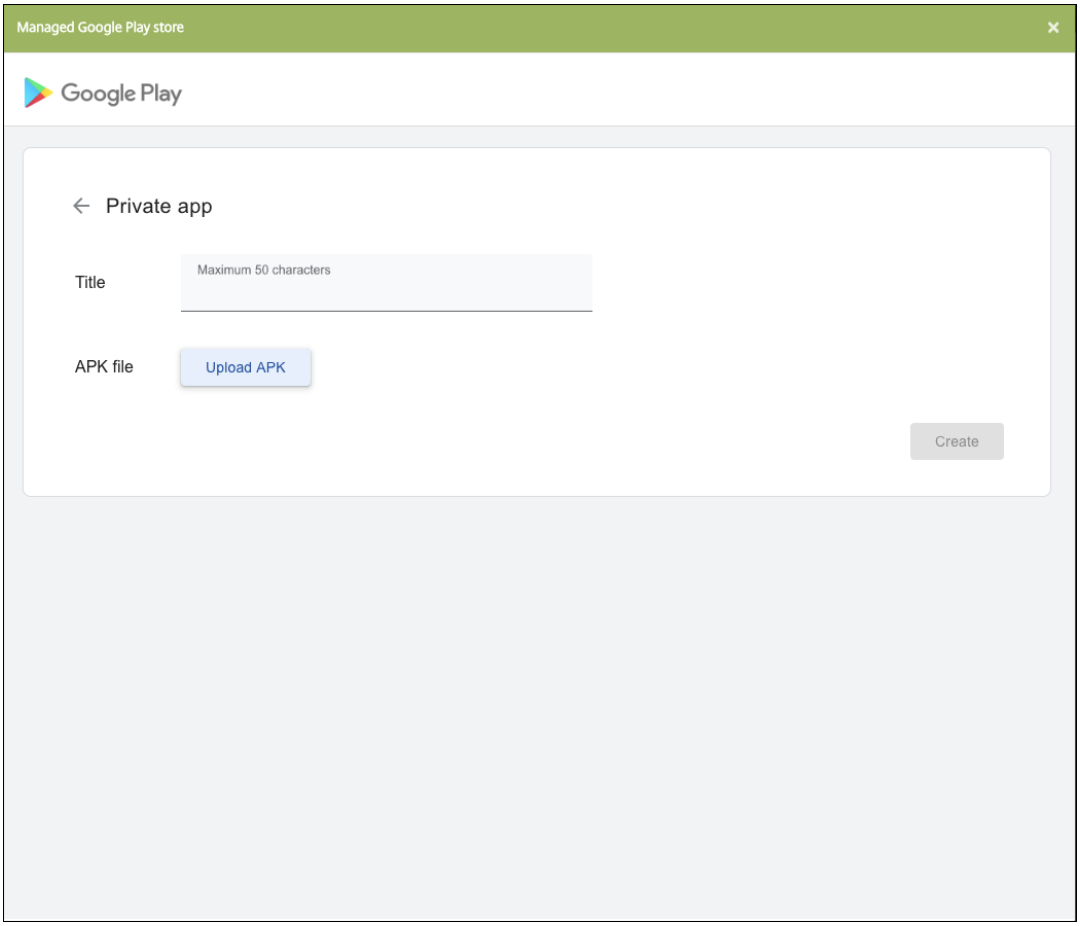
3. [エンタープライズ] をクリックします。[アプリ情報] ペインで、以下の情報を入力します:

- 名前：アプリの説明的な名前を入力します。この名前は、［アプリ］の表の［アプリ名］の下に表示されます。
- 説明：任意で、アプリの説明を入力します。

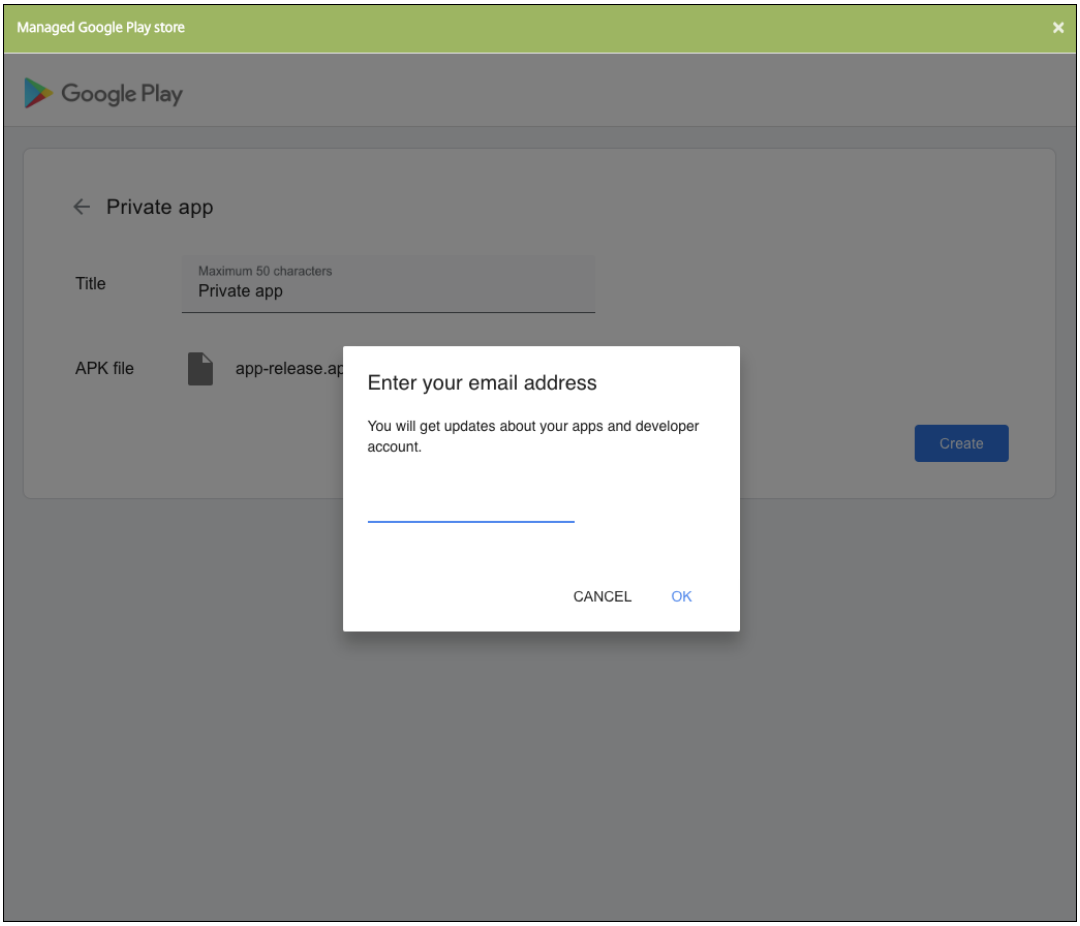
4. プラットフォームとして ［**Android Enterprise**］を選択します。
5. ［アップロード］ボタンをクリックすると、管理対象 Google Play ストアが開きます。プライベートアプリを公開するために開発者アカウントを登録する必要はありません。右下隅にある ［+］アイコンをクリックして続行します。



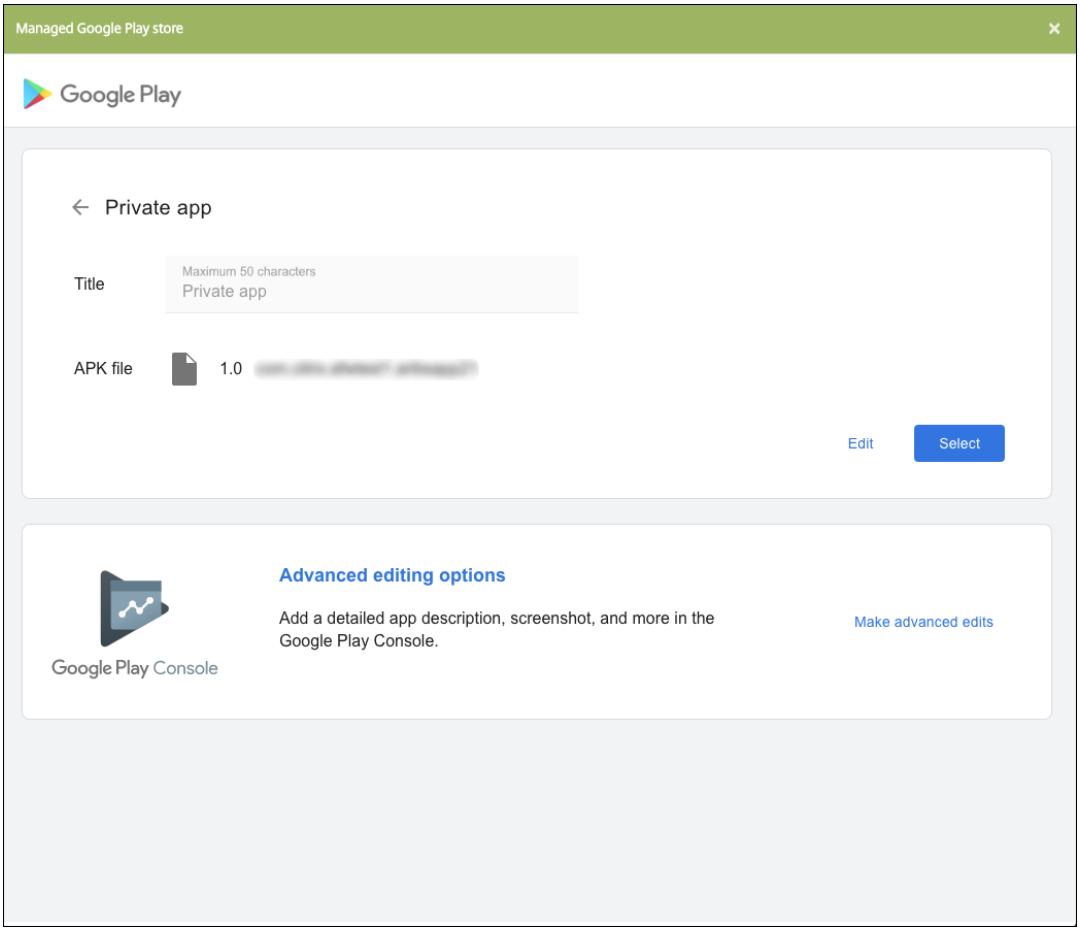
   a) アプリの名前を入力し、.apk ファイルをアップロードします。入力が終わったら、［作成］をクリックします。プライベートアプリが公開されるまでに最大 10 分かかる場合があります。



b) メールアドレスを入力すると、アプリに関する最新情報が得られます。



c) アプリケーションが公開されたら、プライベートアプリのアイコンをクリックし、［選択］をクリックしてアプリの情報ページを開きます。



6. ［次へ］をクリックします。プラットフォームのアプリ情報ページが開きます。
7. プラットフォームの種類について、以下の設定を構成します：
   - ファイル名：任意で、アプリの名前を新たに入力します。
   - アプリの説明：任意で、アプリの説明を新たに入力します。
   - アプリのバージョン：このフィールドは変更できません。
   - パッケージ **ID**：アプリの一意の識別子。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
8. 展開規則とストア構成を構成します。
9. ［エンタープライズ アプリ］ページで、［次へ］をクリックします。［承認］ページが開きます。

   ワークフローを使用して、ユーザーにアプリへのアクセス許可を出す前に承認を必要とする設定にする方法については、「ワークフローの適用」を参照してください。承認ワークフローを設定する必要がない場合は、手順 13 に進みます。

10. ［次へ］をクリックします。
11. ［デリバリーグループ割り当て］ページが開きます。このページではアクションは不要です。.mdx ファイルを追加するときに、このアプリのデリバリーグループと展開スケジュールを構成します。［保存］をクリックします。

オプション：ストア **URL** を追加または変更する

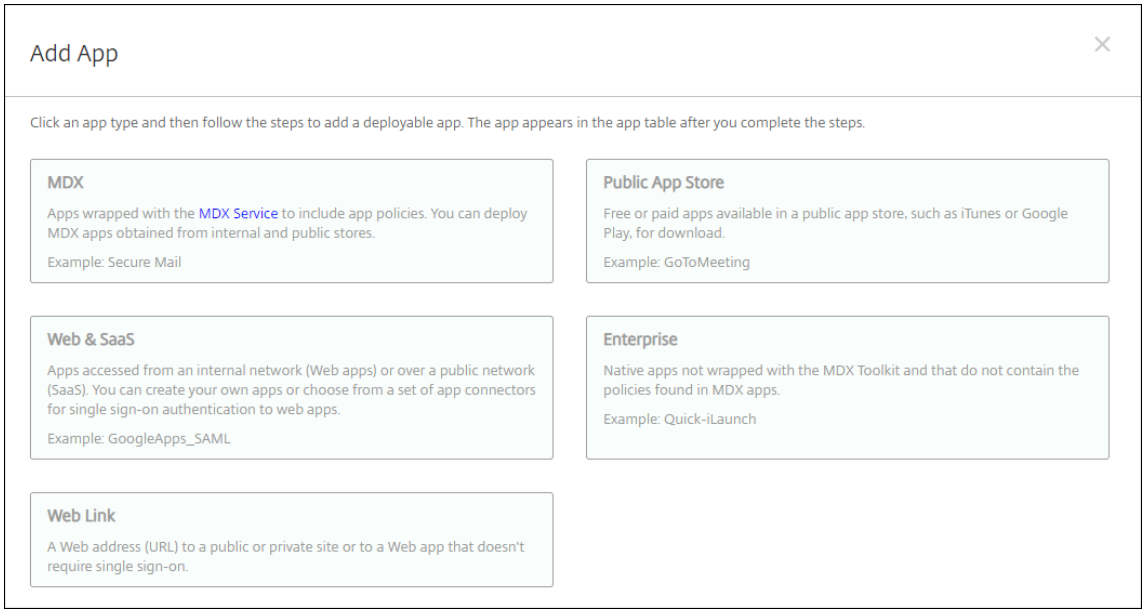
アプリのラップ時にストア URL がわからなかった場合は、ここでストア URL を追加します。

1. 管理対象 Google Play ストアでアプリを表示します。アプリを選択すると、Web ブラウザーのアドレスバーにストア URL が表示されます。アプリのパッケージ名を URL フォームからコピーします。例：`https://play.google.com/store/apps/details?id=SampleAEappPackage`。コピーする URL は`https://play.google.com/work/`で始まる場合があります。`work`を`store`に変更してください。
2. MDX Toolkit を使用して、次のように.mdx ファイルにストア URL を追加します：

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

.mdx ファイルを追加します

1. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］の順にクリックします。［追加］をクリックします。［アプリの追加］ダイアログボックスが開きます。



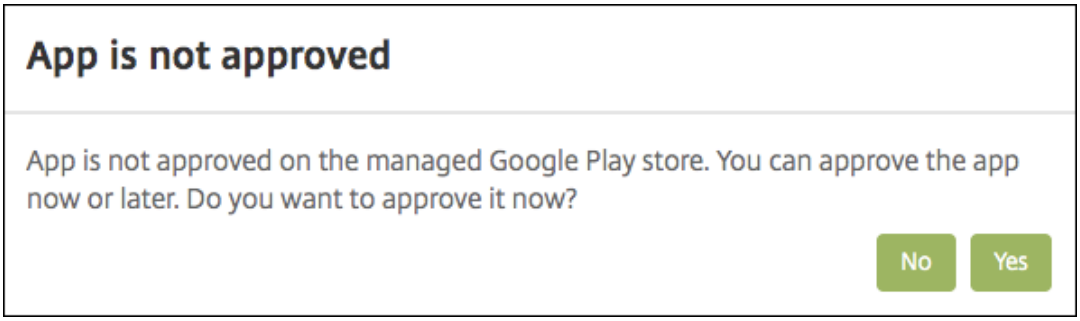
2. [**MDX**] をクリックします。[**MDX** アプリ情報] ページが開きます。[アプリ情報] ペインで、以下の情報を入力します:

   - 名前: アプリを説明する名前を入力します。この名前は、[アプリ] テーブルの [アプリ名] の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。

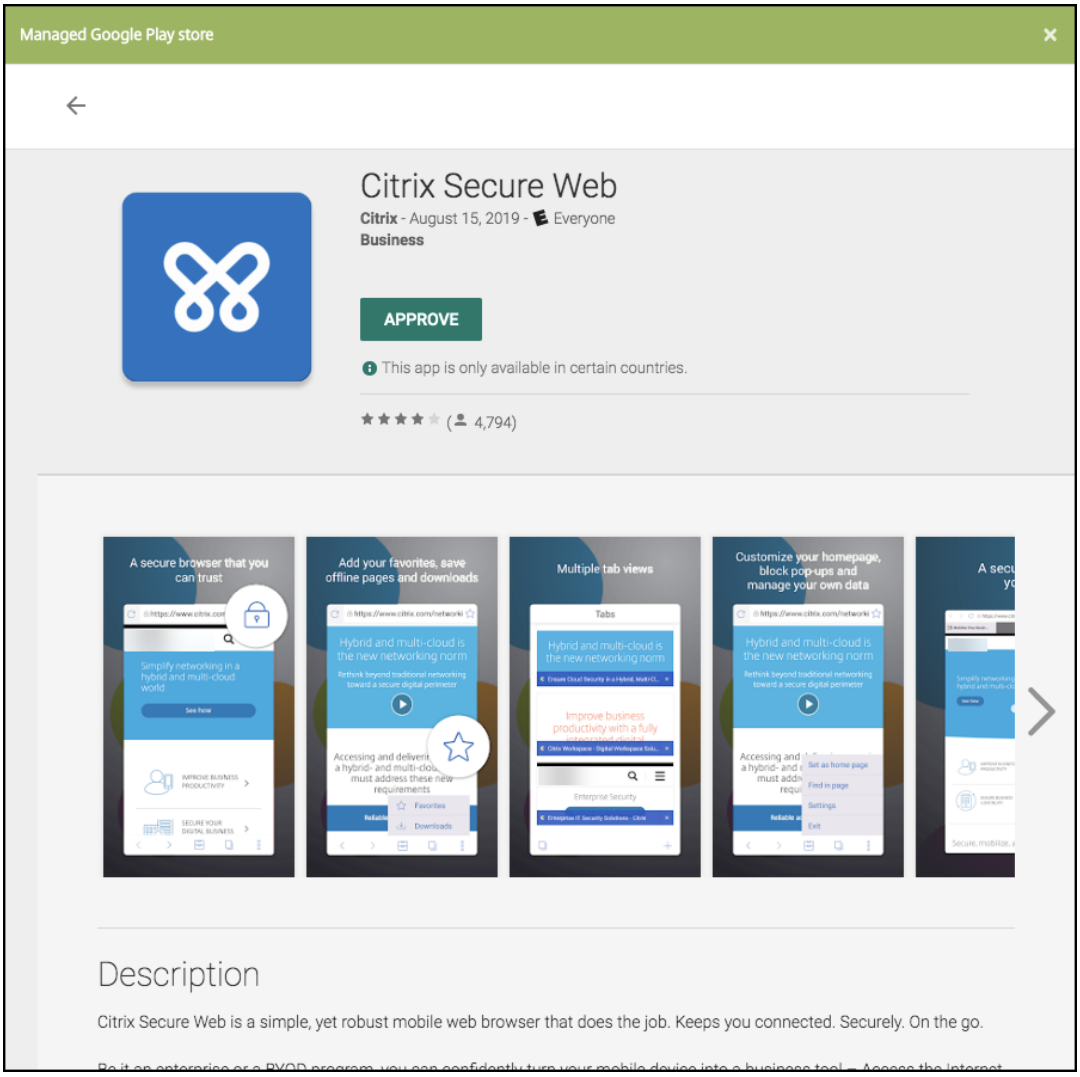
3. プラットフォームとして [**Android Enterprise**] を選択します。

4. [アップロード] をクリックして、MDX ファイルに移動します。Android Enterprise は、MDX Toolkit でラップされたアプリのみをサポートします。

   - 追加されたアプリケーションが、管理対象 Google Play ストアからの承認を必要としているかどうかが UI によって通知されます。Citrix Endpoint Management コンソールを終了せずにアプリケーションを承認するには、[はい] をクリックします。

     管理対象 Google Play ストアが開いたら、画面の指示に従ってアプリを承認して保存します。



アプリが正常に追加されると、［アプリケーション詳細］ページが表示されます。

5. 次の設定を構成します：

   - ファイル名：アプリに関連付けられているファイル名を入力します。
   - アプリの説明：アプリの説明を入力します。
   - アプリのバージョン：任意で、アプリのバージョン番号を入力します。
   - パッケージ **ID**：管理対象 Google Play ストアから取得したアプリのパッケージ ID を入力します。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。

6. **MDX** ポリシーを構成します。MDX ポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域で適用するオプションが含まれます。コンソールでは、ポリシーごとに、

ポリシーを説明するヒントが提供されます。各デバイスプラットフォームの種類で使用できるアプリポリシーについて詳しくは、以下を参照してください:

- MAM SDK の概要
- サードパーティアプリの MDX ポリシーの概要

7. 展開規則とストア構成を構成します。

   [常時接続に対する展開]は、[設定] > [サーバープロパティ]において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

   常時接続オプション:

   - iOS デバイスでは使用できません。
   - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
   - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

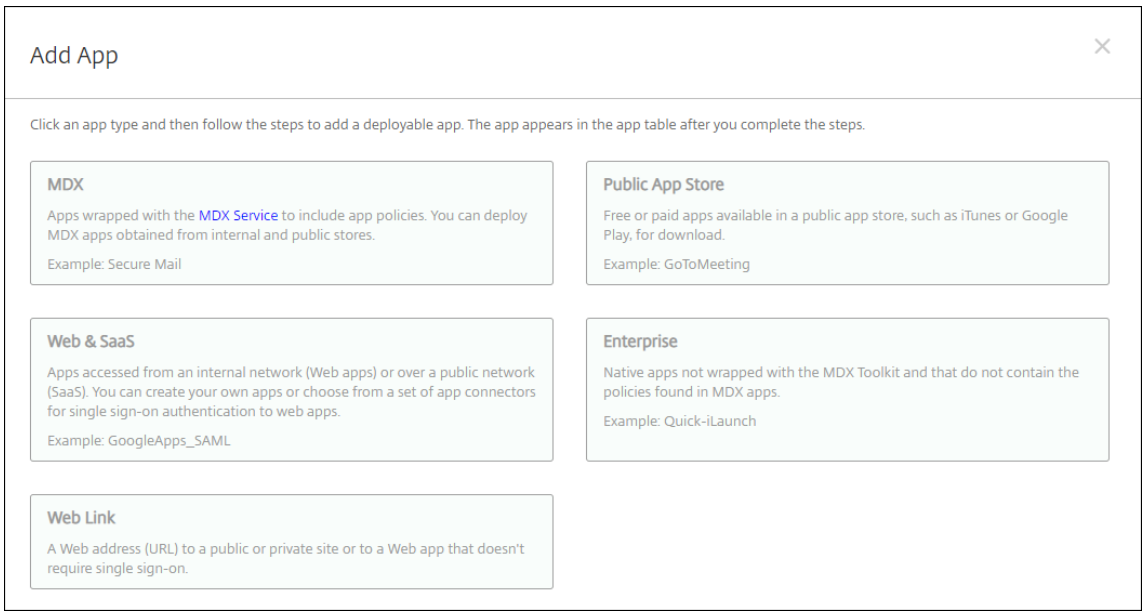
   構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、[常時接続に対する展開]は適用されません。

8. デリバリーグループをアプリに割り当て、[保存]をクリックします。詳しくは、「リソースの展開」を参照してください。

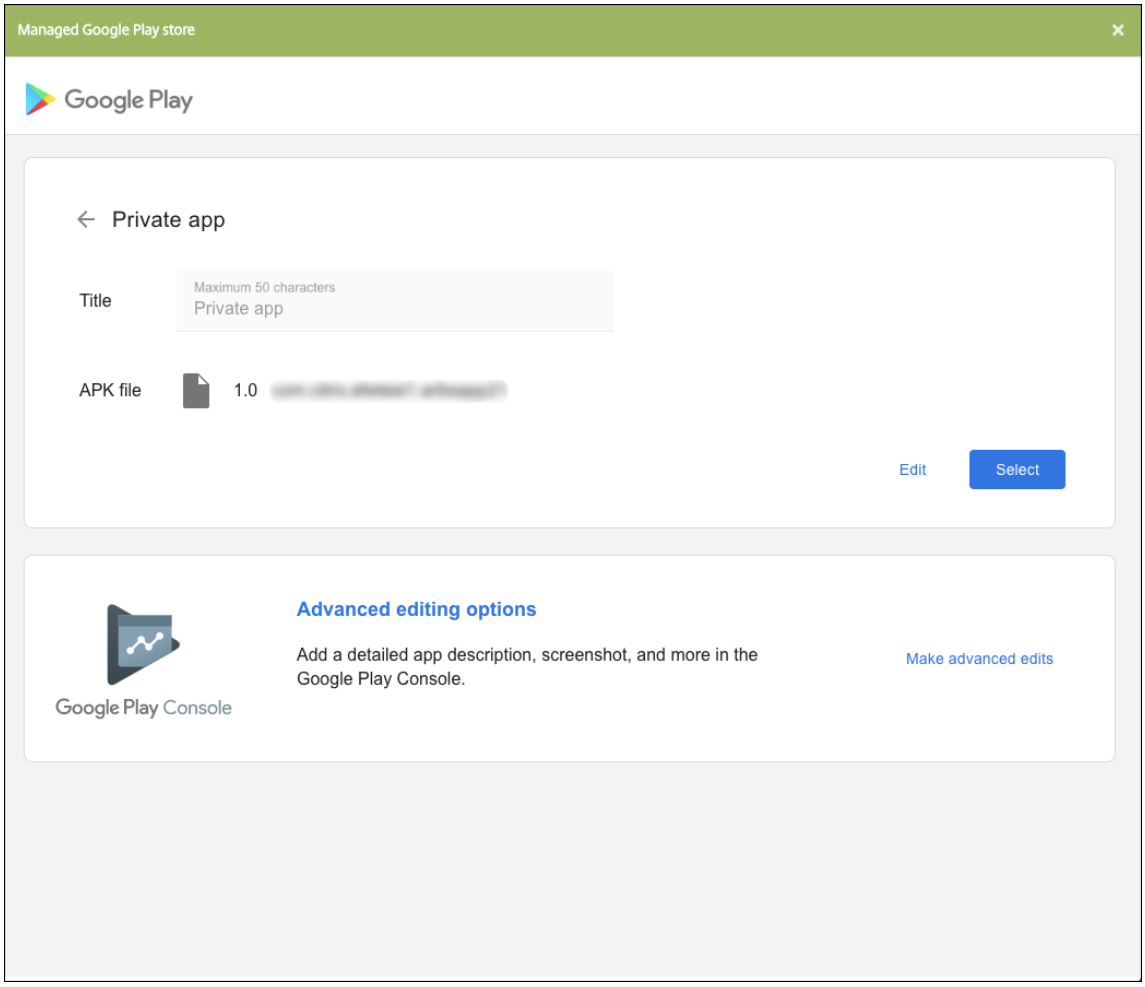
アプリを更新する

Android Enterprise アプリを更新するには、更新された.apk ファイルをラップしてアップロードします:

1. MAM SDK または MDX Toolkit を使用して、更新されたアプリの.apk ファイルをラップします。
2. Citrix Endpoint Management コンソールで、[構成] > [アプリ]の順にクリックします。[アプリ]ページが開きます。



3. ［追加］をクリックします。［アプリの追加］ダイアログボックスが開きます。
4. ［エンタープライズ］をクリックします。［アプリ情報］ペインで、以下の情報を入力します:
   - 名前：アプリの説明的な名前を入力します。この名前は、［アプリ］の表の［アプリ名］の下に表示されます。
   - 説明：任意で、アプリの説明を入力します。
5. プラットフォームとして ［**Android Enterprise**］を選択します。
6. ［次へ］をクリックします。［エンタープライズ アプリ］ページが表示されます。
7. ［アップロード］をクリックします。
8. 管理対象 Google Play ストアのページで、更新するアプリを選択します。
9. ［アプリ情報］ページで、.apk ファイル名の横にある ［編集］をクリックします。



10. 新しい.apk ファイルに移動してアップロードします。
11. 管理対象 Google Play ストアページで、［保存］をクリックします。

Google Workspace（旧称：G Suite）ユーザー向けの従来の Android Enterprise

November 29, 2023

Google Workspace ユーザーが従来の Android Enterprise を構成するには、従来の Android Enterprise の設定を使用する必要があります。Google は最近、G Suite の名称を Google Workspace に変更しました。

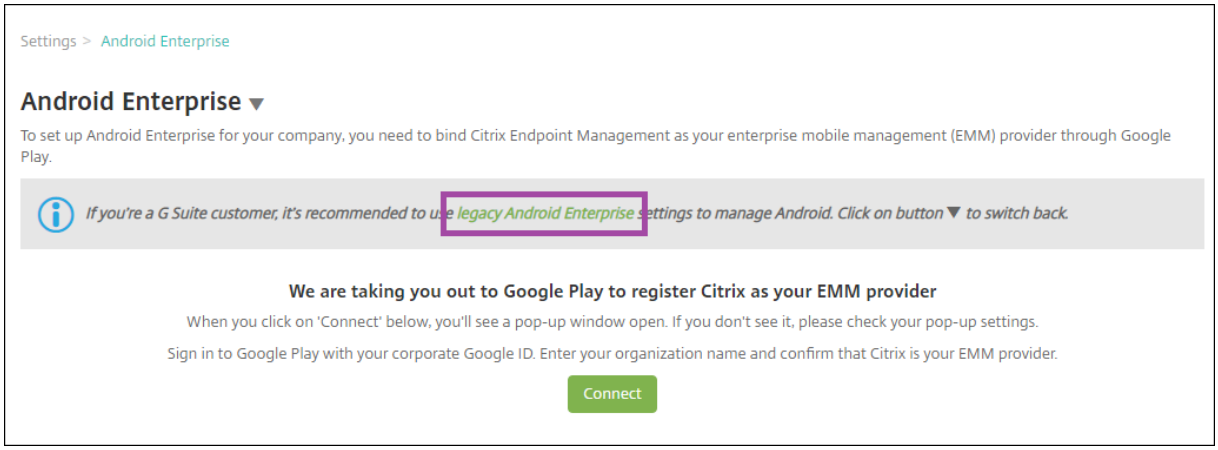
組織が既に Google Workspace を使用してユーザーに Google アプリのアクセスを提供している場合、Google Workspace を使用して Citrix を EMM として使用できます。組織が Google Workspace を使用している場合、既存のエンタープライズ ID および既存のユーザー用 Google アカウントが存在します。Citrix Endpoint Management で Google Workspace を使用するには、使用している LDAP ディレクトリと同期し、Google Directory API を使用して Google アカウント情報を Google から取得します。この種類のエンタープライズは既存のドメインに関連付

けられているため、各ドメインは 1 つのエンタープライズのみを作成できます。Citrix Endpoint Management にデバイスを登録するには、各ユーザーが既存の Google アカウントで手動でサインインする必要があります。このアカウントでは、Google Workspace プランで提供される他の Google サービスに加えて、ビジネス向け Google Play にアクセスできるようになります。

従来の Android Enterprise の要件:

- パブリックにアクセスできるドメイン
- Google 管理者アカウント
- プロファイルのサポートを管理している Android デバイス
- Google Play がインストールされている Google アカウント
- デバイスで設定されたワークプロファイル

従来の Android Enterprise の構成を始めるには、Citrix Endpoint Management 設定の［**Android Enterprise**］ページで ［従来の **Android Enterprise**］をクリックします。



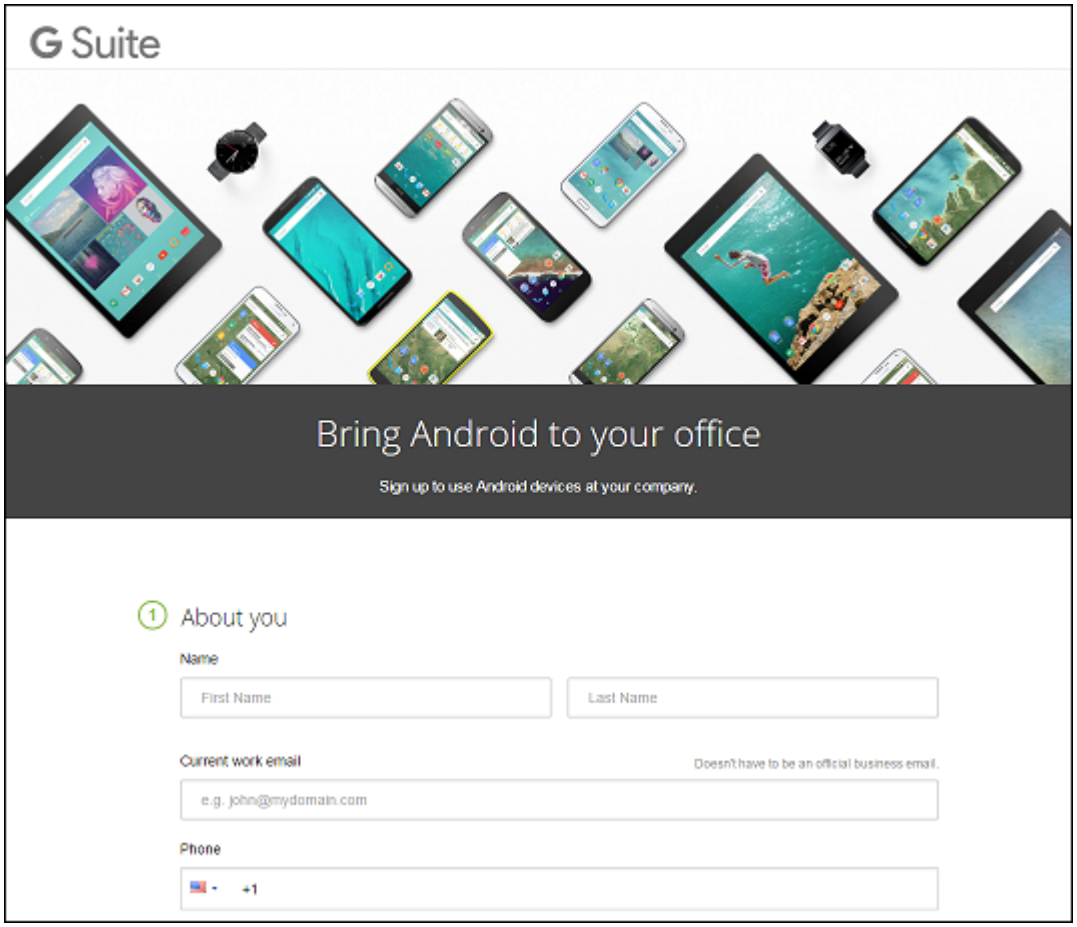
Android Enterprise アカウントの作成

Android Enterprise アカウントをセットアップするには、Google でドメイン名を検証する必要があります。

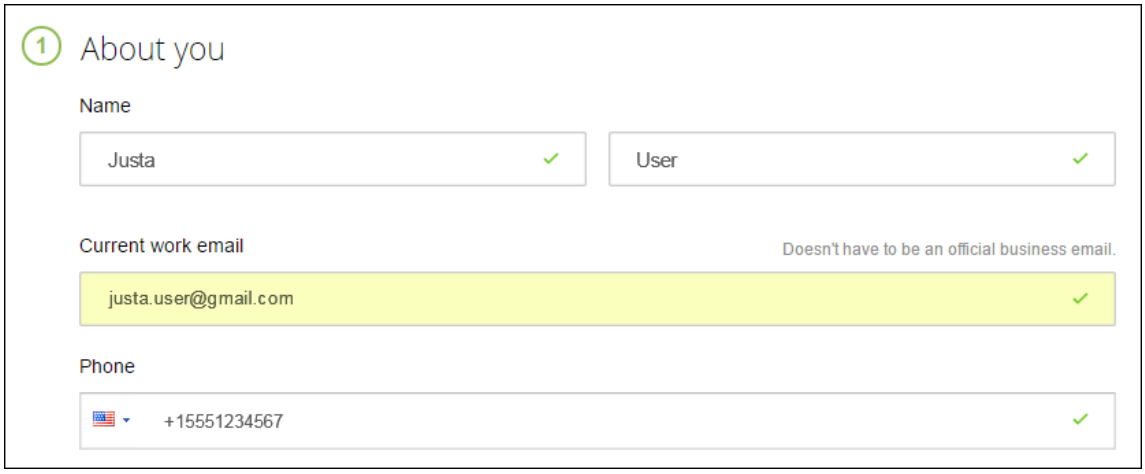
ドメイン名が既に Google で検証済みの場合は、以下の手順を省略し、「Android Enterprise サービスアカウントの設定と Android Enterprise 証明書のダウンロード」に進んでください。

1. https://gsuite.google.com/signup/basic/welcomeにアクセスします。

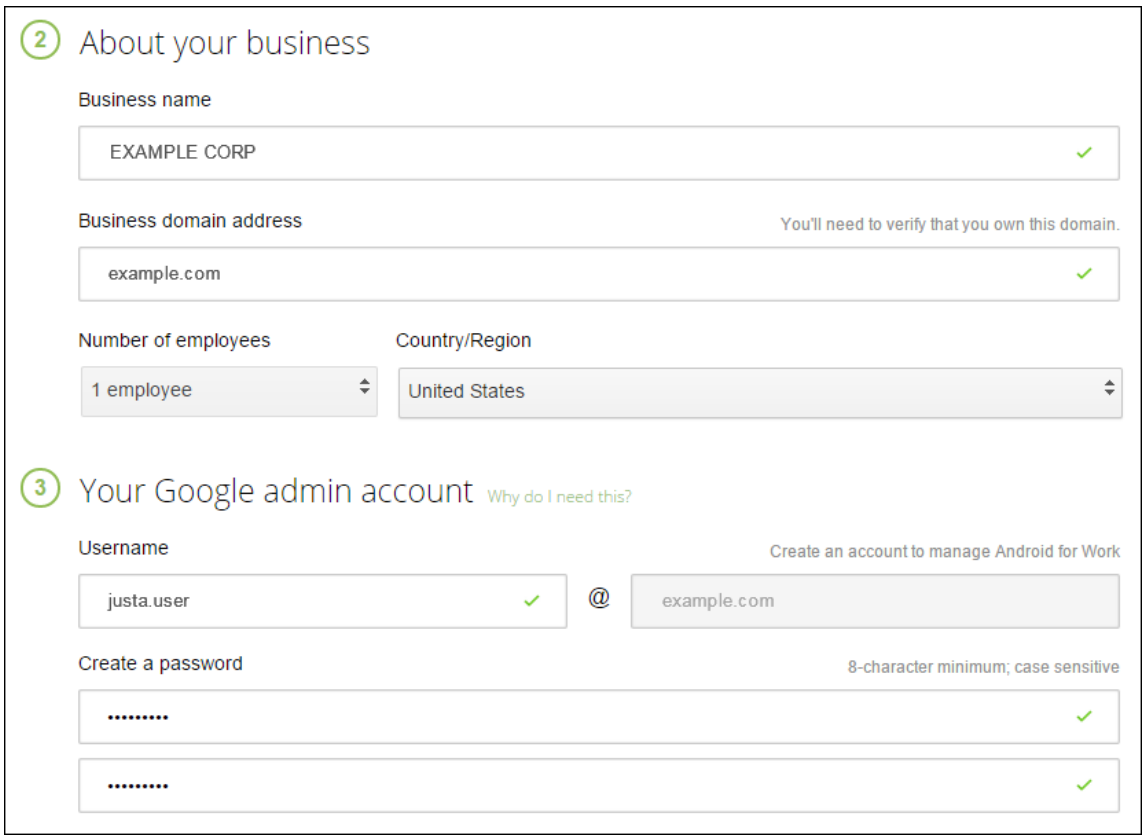
   管理者情報と会社情報を入力する次のページが開きます。



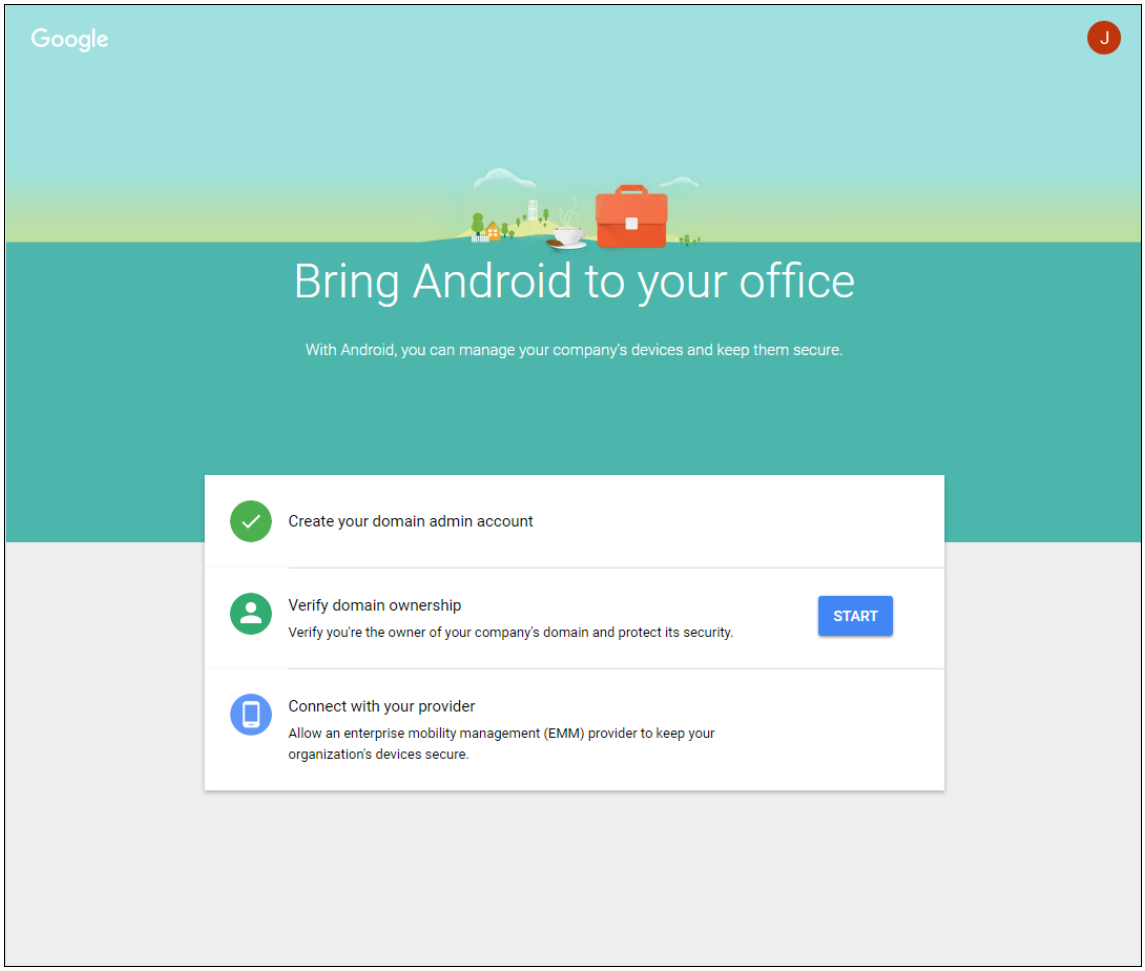
2. 管理者のユーザー情報を入力します。



3. 管理者のアカウント情報だけでなく、会社情報も入力してください。



プロセスの最初の手順が完了します。以下のページが開きます。



ドメイン所有権の検証

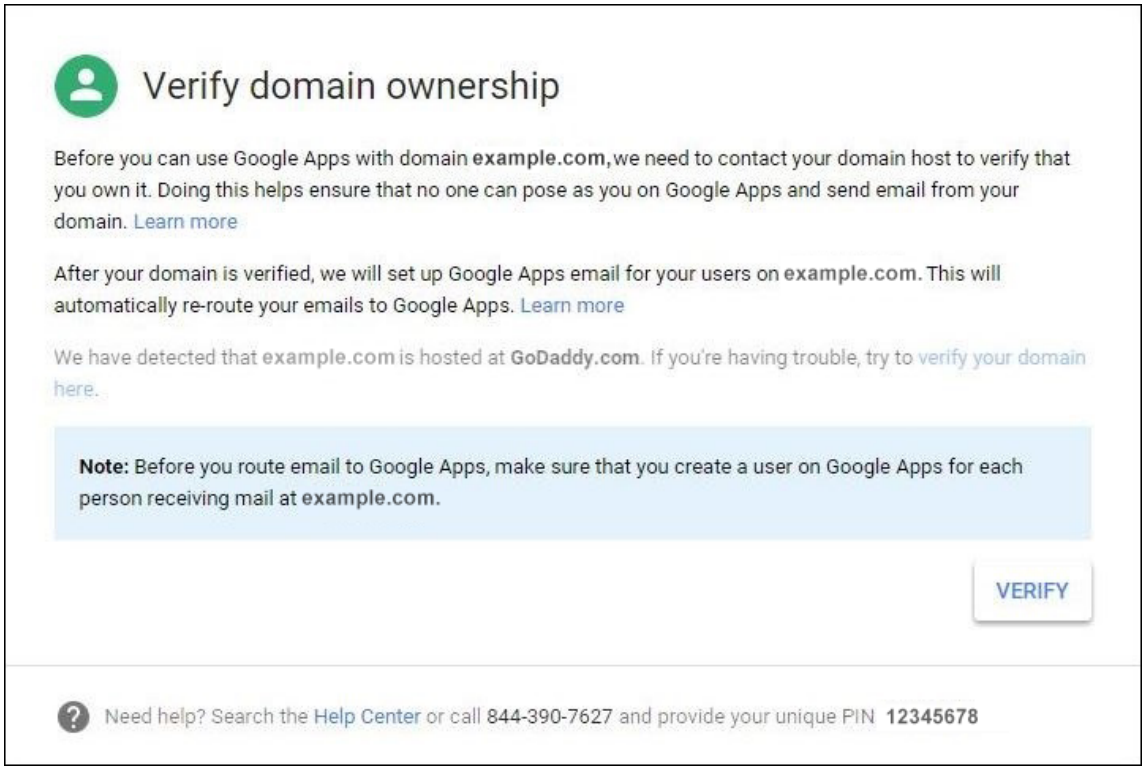
以下のいずれかの方法で、Google がドメインを検証できるようにします。

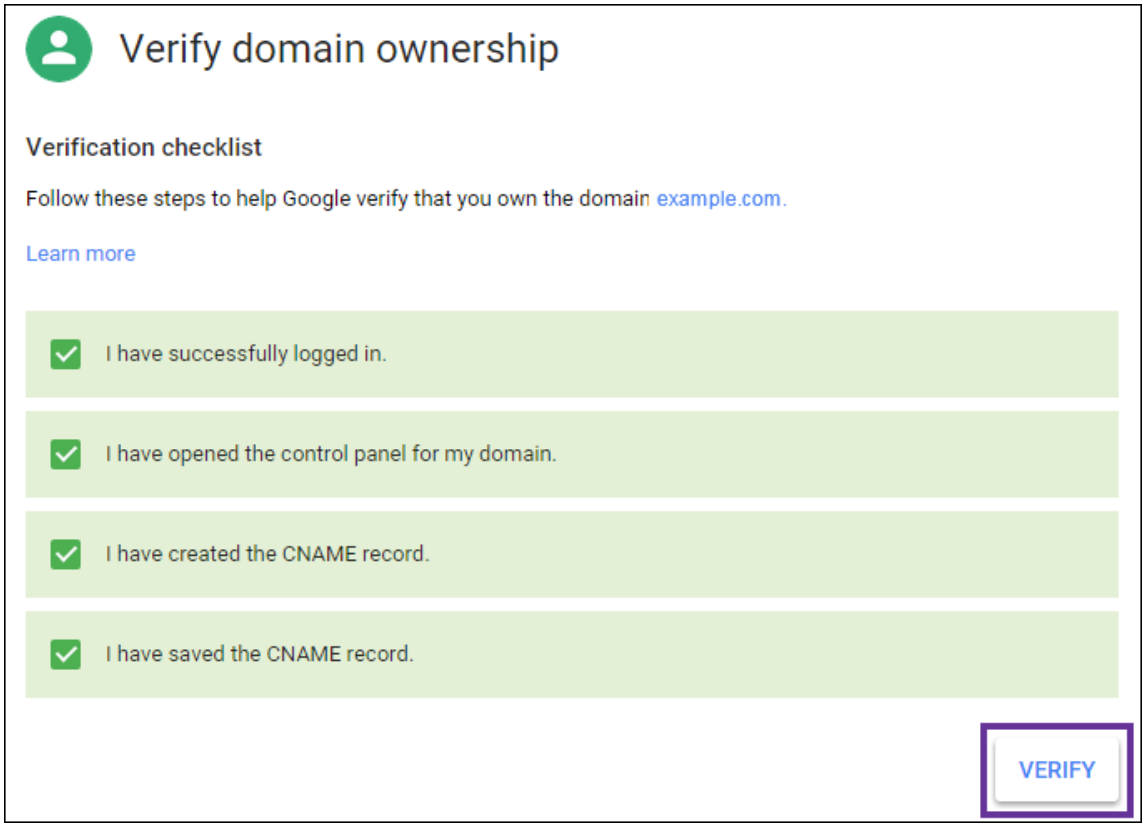
- ドメインホストの Web サイトに TXT または CNAME レコードを追加します。
- HTML ファイルをドメインの Web サーバーにアップロードします。
- ホームページに<meta>タグを追加します。Google では最初の方法を推奨しています。ドメインの所有権を検証する手順についてはこの記事では扱いませんが、必要な情報はhttps://support.google.com/a/answer/6248925/に記載されています。

1. [**Start**] をクリックして、ドメインの検証を開始します。

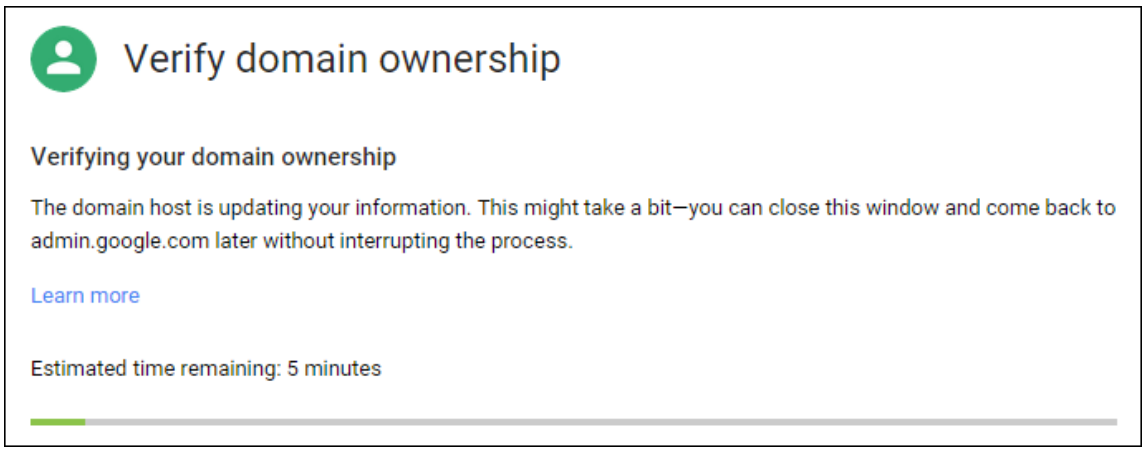
   [**Verify domain ownership**] ページが開きます。画面の指示に従ってドメインを検証します。

2. [**Verify**] をクリック します。

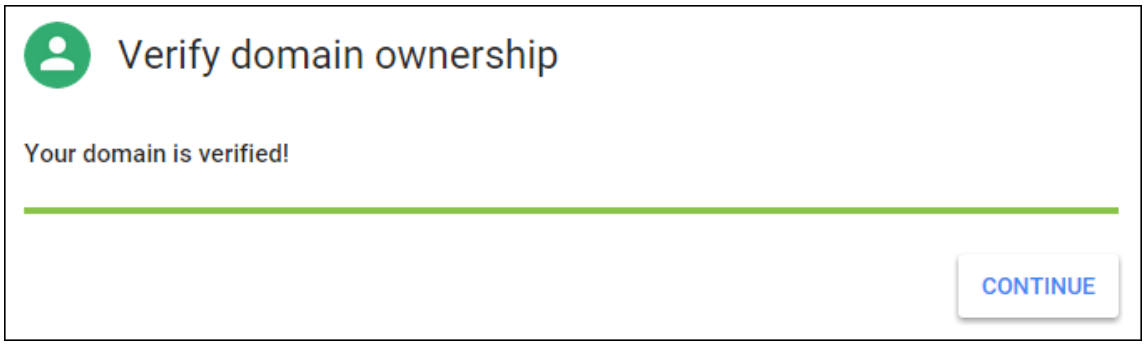




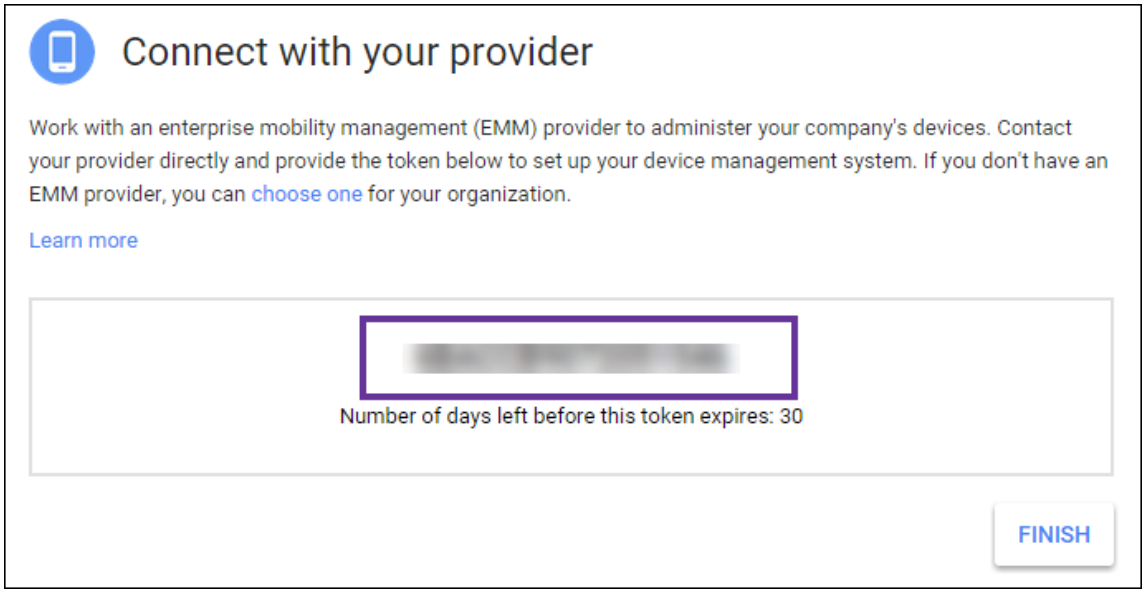
3. Google によってドメイン所有権が検証されます。



4. 検証が成功すると、次のページが開きます。［続行］をクリックします。



5. Citrix に提供し Android Enterprise 設定を構成するときに使用する EMM バインドトークンが、Google によって作成されます。トークンをコピーして保存します。後でセットアップ中に必要になります。



6. ［**Finish**］をクリックして Android Enterprise の設定を完了します。ドメインの検証に成功したことを示すページが表示されます。

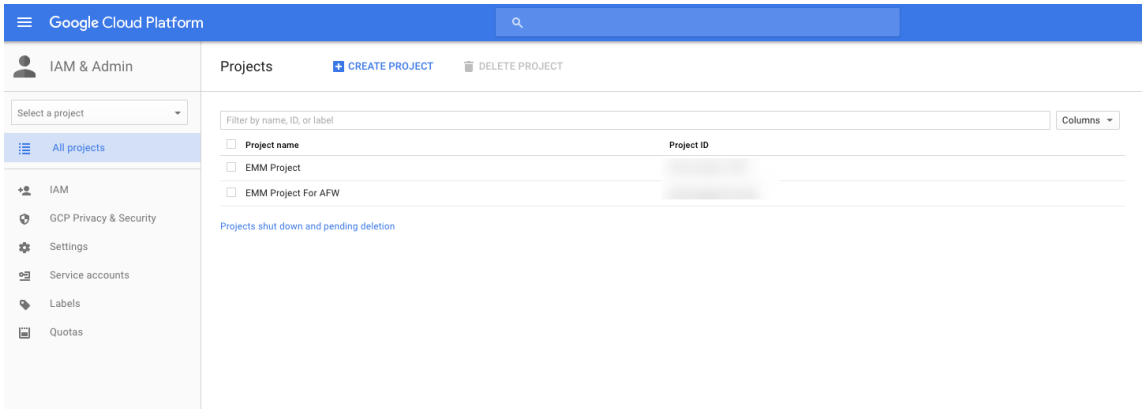
Android Enterprise サービスアカウントを作成したら、Google Admin コンソールにサインインしてモビリティ

管理設定を管理できます。

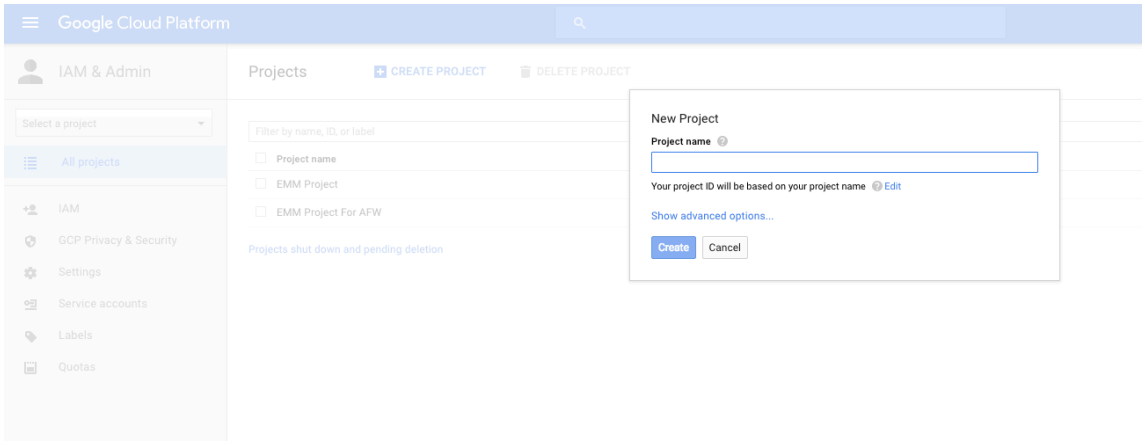
Android Enterprise サービスアカウントの設定と **Android Enterprise** 証明書のダウンロード

Citrix Endpoint Management から Google Play サービスおよび Directory サービスにアクセスできるようにするには、Google のデベロッパー用プロジェクトポータルを使用してサービスアカウントを作成する必要があります。このサービスアカウントは、Citrix Endpoint Management と Google の Android 用各種サービスのサーバー間通信で使用します。使用されている認証プロトコルについて詳しくは、「https://developers.google.com/identity/protocols/OAuth2ServiceAccount」にアクセスしてください。

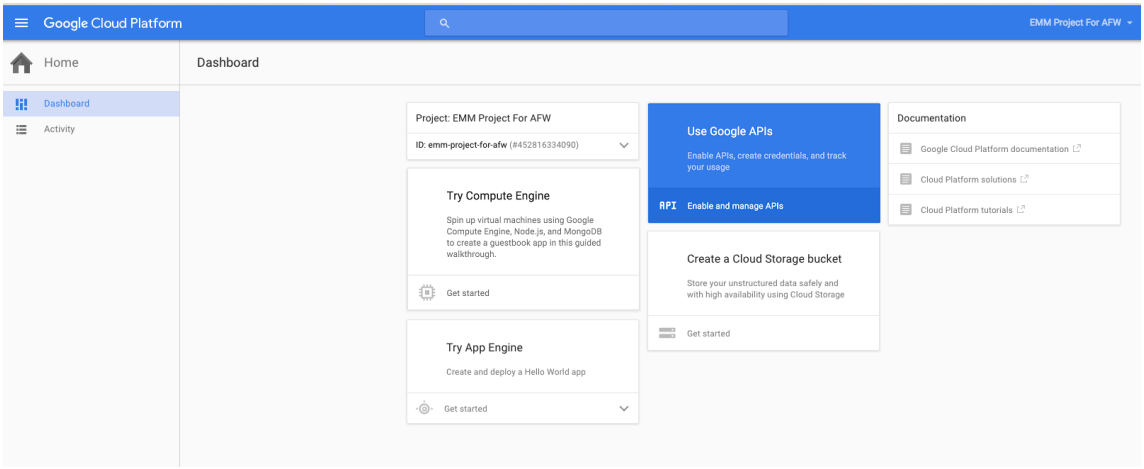
1. Web ブラウザーでhttps://console.cloud.google.com/projectを開いて、Google 管理者の資格情報でサインインします。
2. [**Projects**] の一覧で、[**Create Project**] をクリックします。



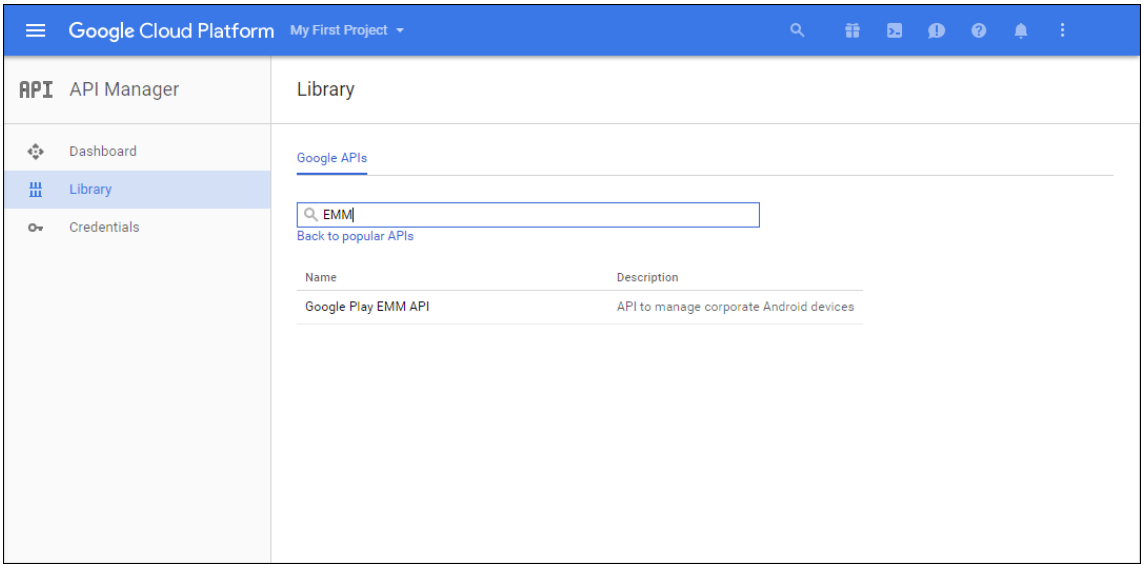
3. [**Project name**] ボックスに、プロジェクトの名前を入力します。



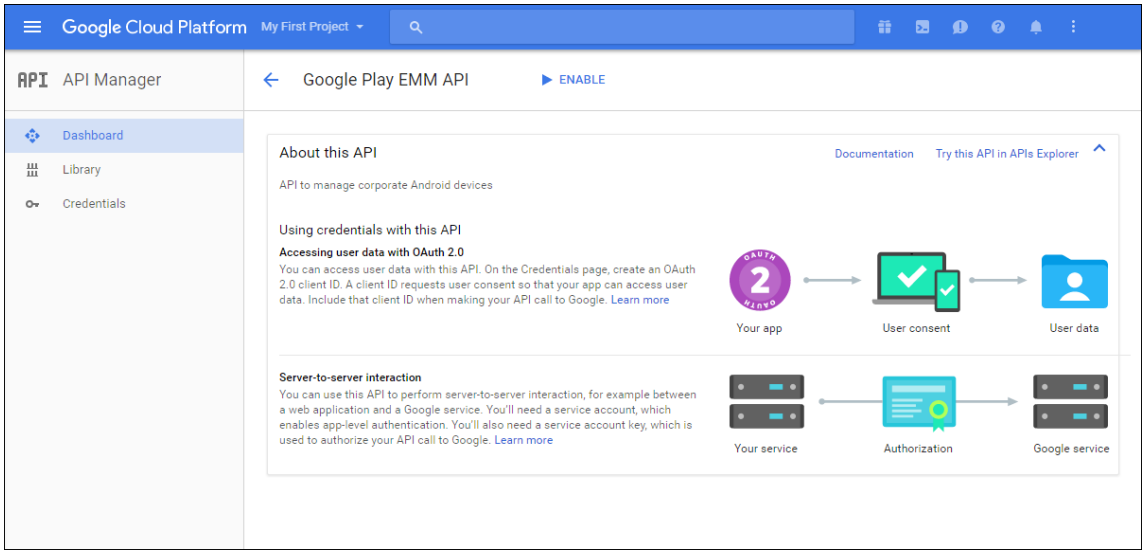
4. [Dashboard] ページで、[**Use Google APIs**] をクリックします。



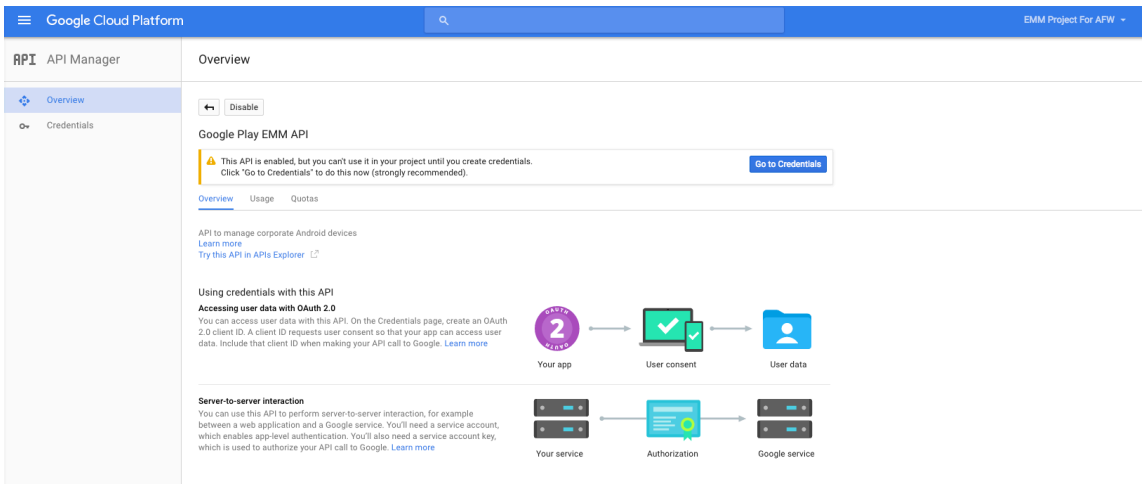
5. [**Library**] をクリックして、[**Search**] に **EMM** と入力して、検索結果をクリックします。



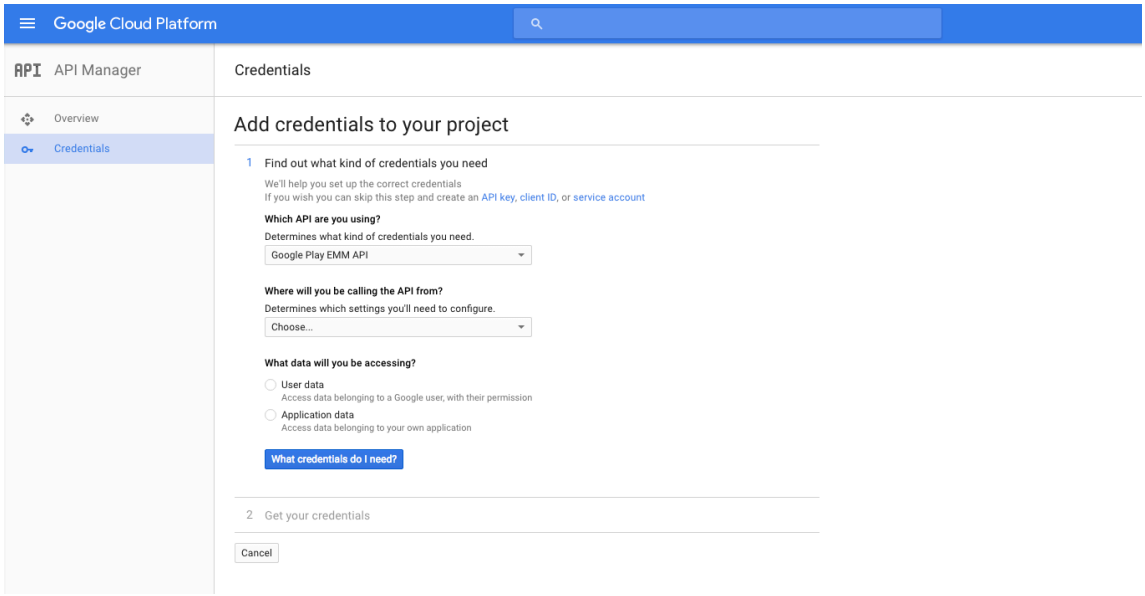
6. [**Overview**] ページで、[**Enable**] をクリックします。



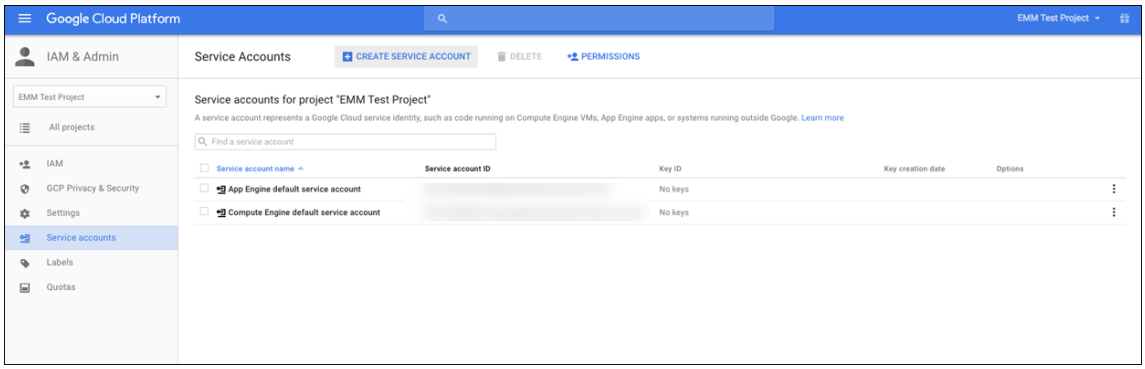
7. [**Google Play EMM API**] の横にある [**Go to Credentials**] をクリックします。



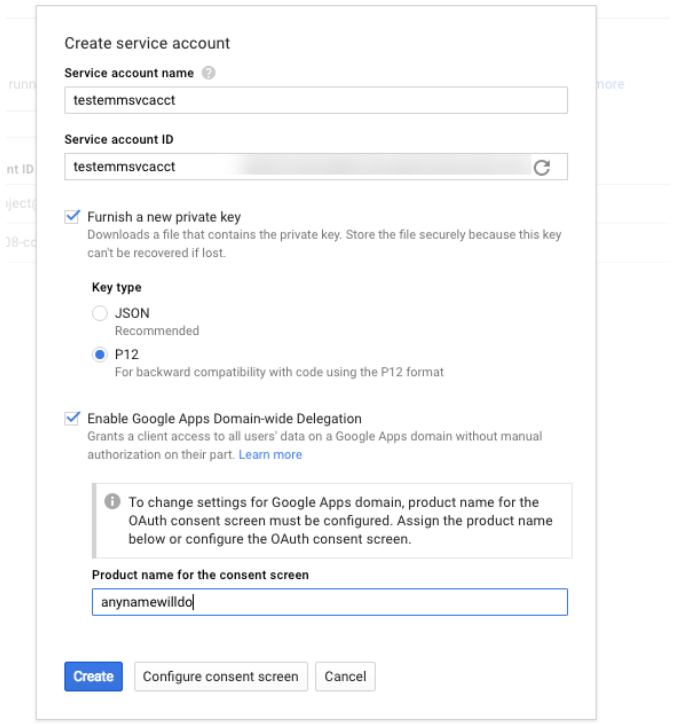
8. [**Add credentials to our project**] の一覧の手順 1 で、[**service account**] をクリックします。



9. [**Service Accounts**] ページで、[**Create Service Account**] をクリックします。

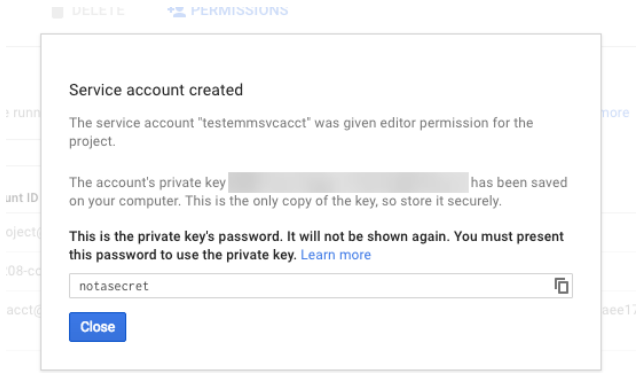


10. [**Create service account**] で、アカウントに名前を付けて、[**Furnish a new private key**] をオンにします。[**P12**] を選択して、[**Enable Google Apps Domain-wide Delegation**] をオンにし、[**Create**] をクリックします。

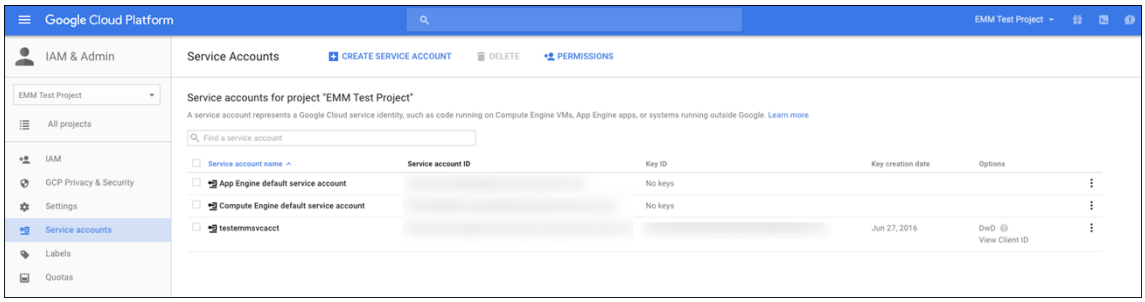


証明書（P12 ファイル）がコンピューターにダウンロードされます。証明書を安全な場所に保存してください。

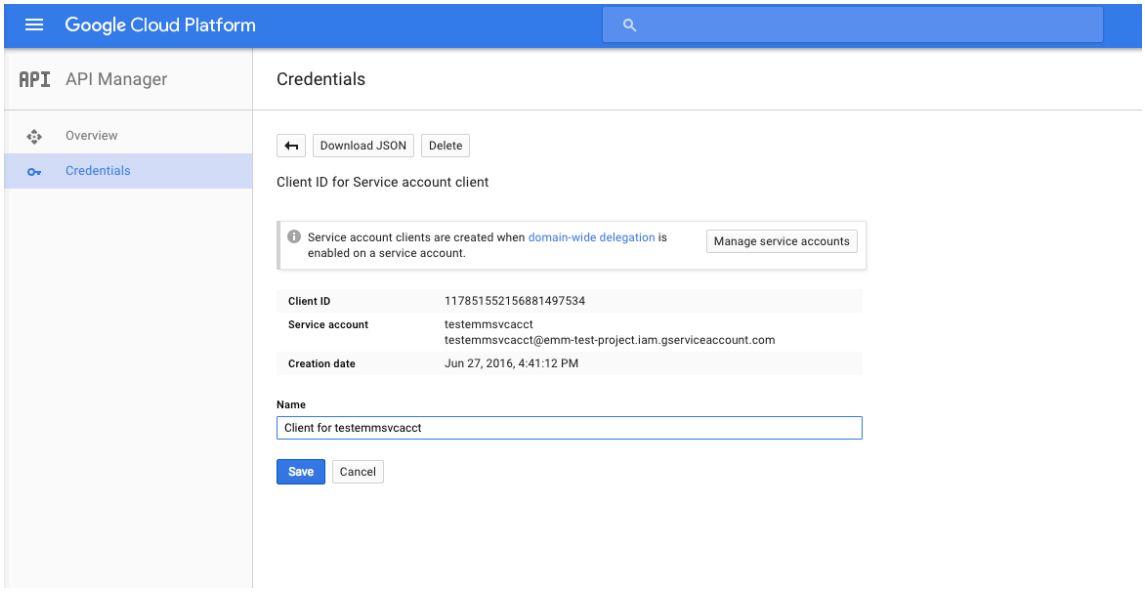
11. [**Service account created**] 確認画面で、[**Close**] をクリックします。



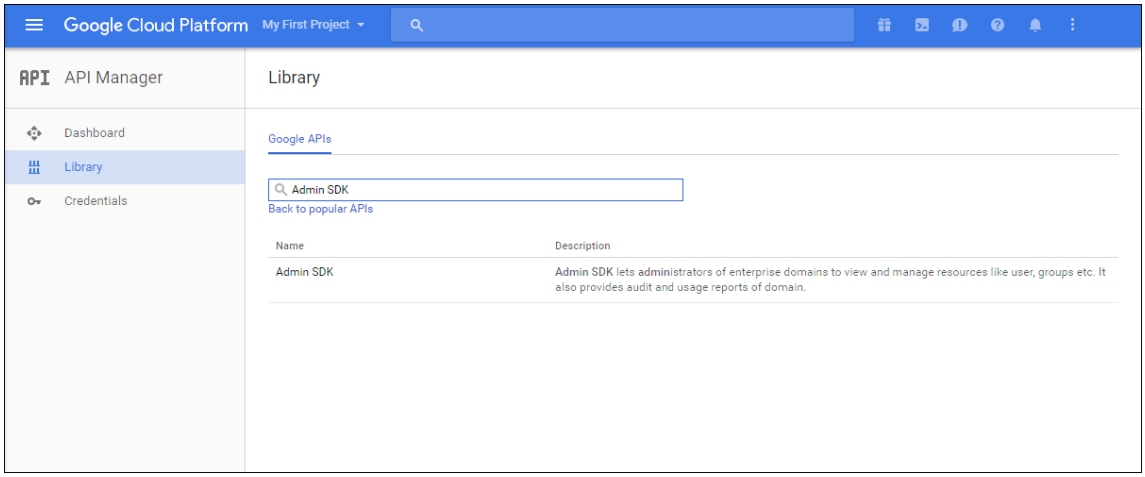
12. [**Permissions**] ページで [**Service accounts**] をクリックし、サービスアカウントの [**Options**] の下で、[**View Client ID**] をクリックします。



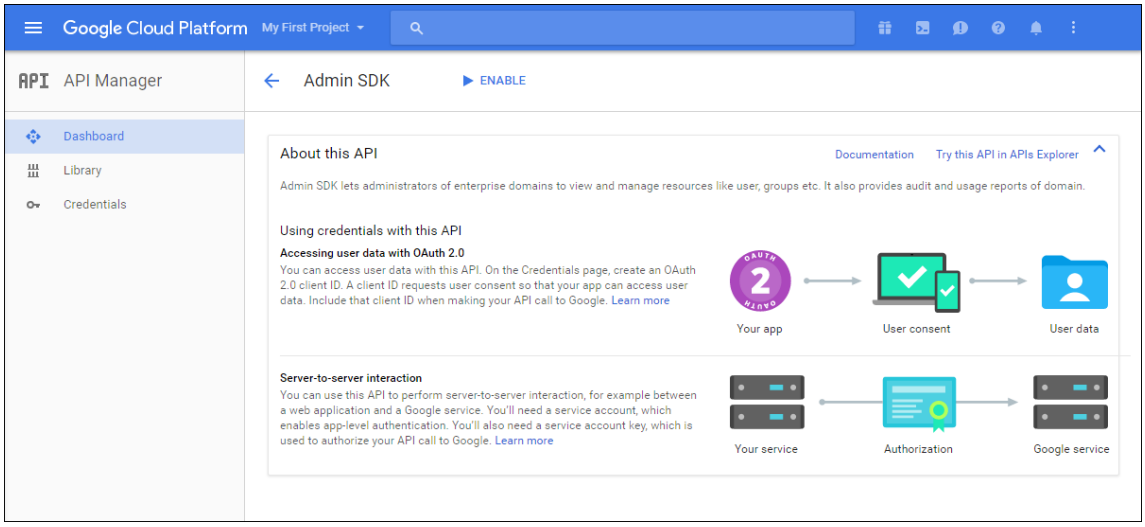
13. Google 管理コンソールでアカウントの承認に必要になる詳細情報が表示されます。[**Client ID**] と [**Service account ID**] を、後でこの情報を引き出せる場所にコピーします。この情報は、ドメイン名と共に、許可リストへの追加の目的で Citrix サポートに送信するときに必要になります。



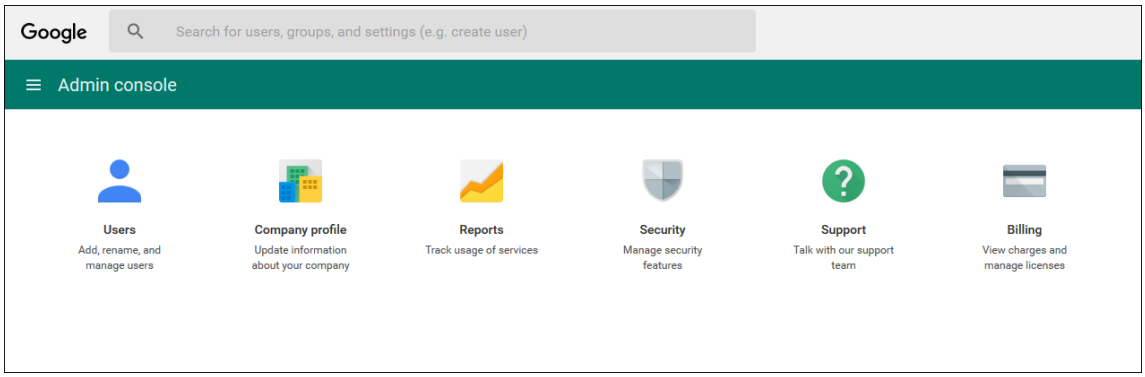
14. [**Library**] ページで **Admin SDK** を検索して、検索結果をクリックします。



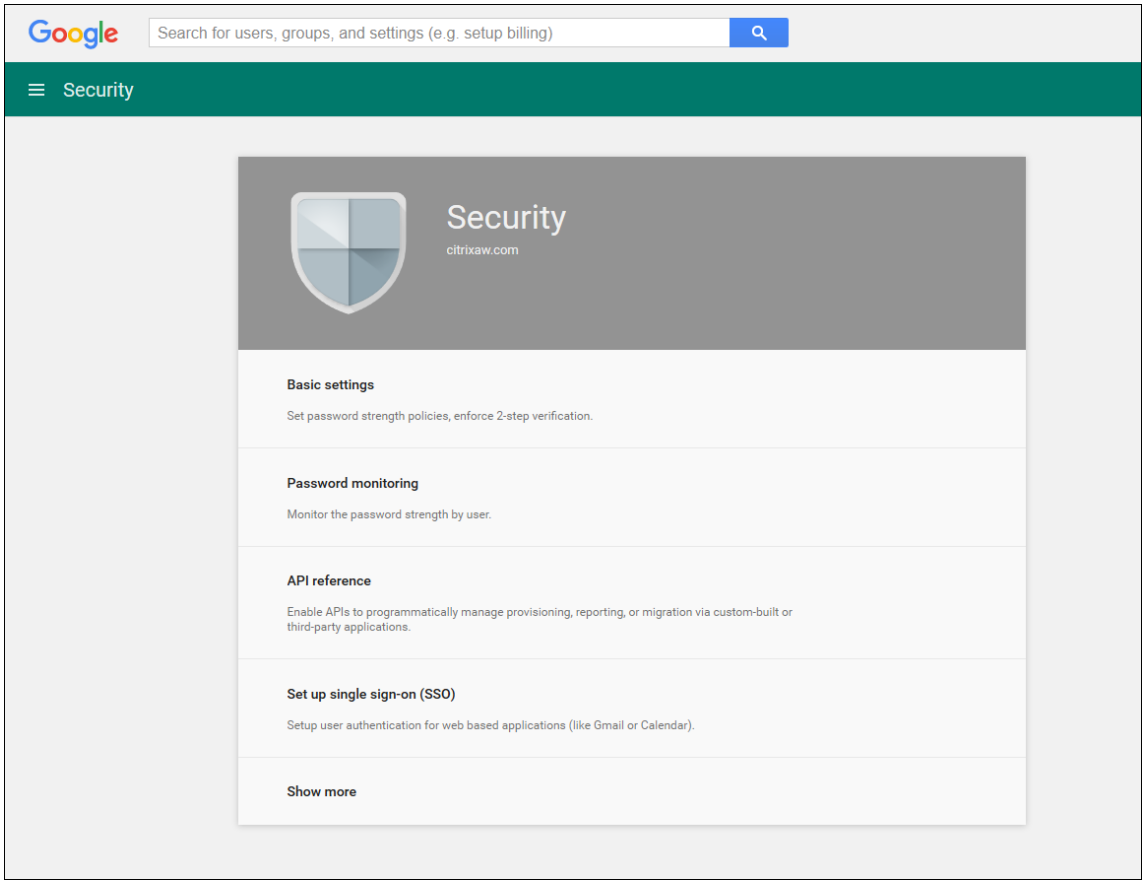
15. [**Overview**] ページで、[**Enable**] をクリックします。

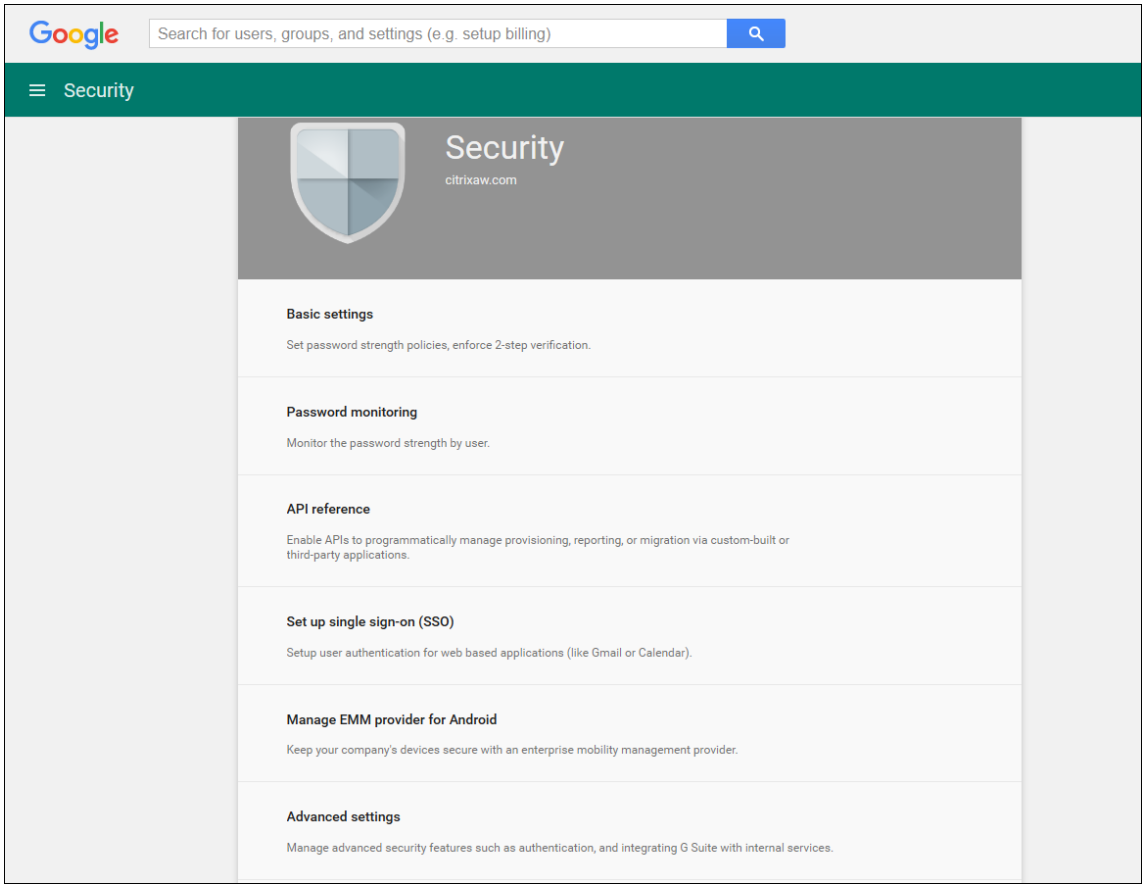


16. ユーザーのドメインの Google 管理コンソールを開き、[**Security**] をクリックします。

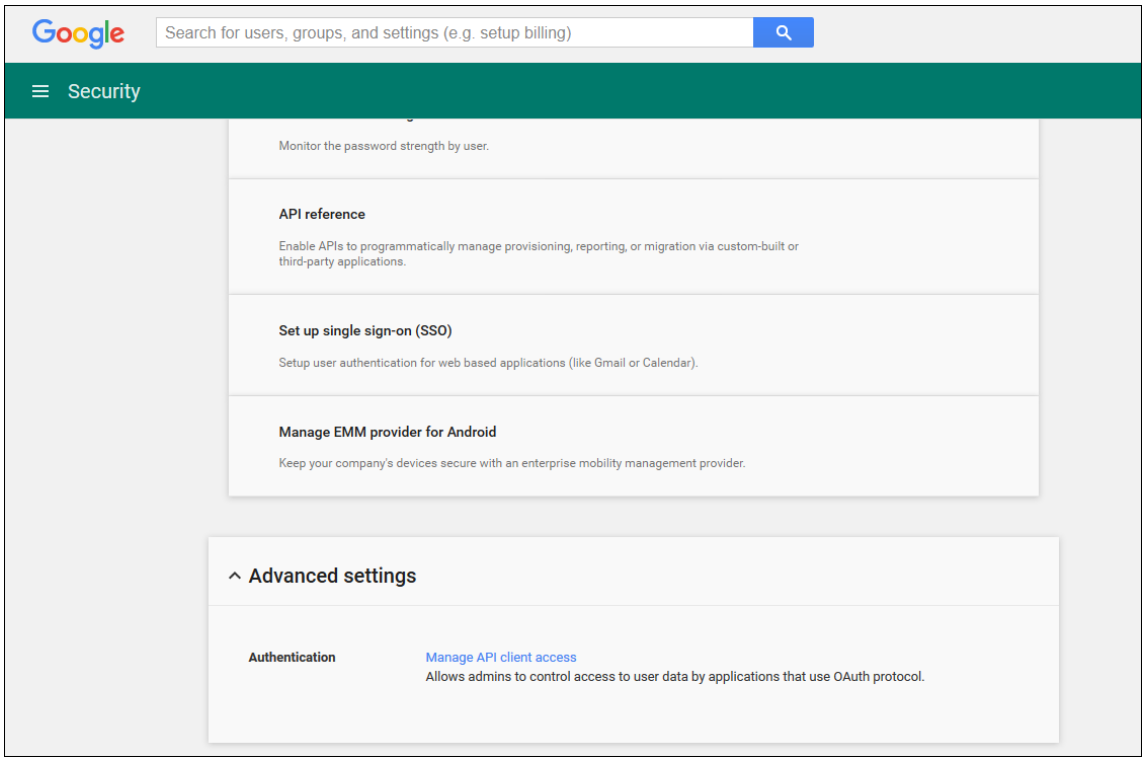


17. [**Settings**] ページで [**Show more**] をクリックして、[**Advanced settings**] を選択します。

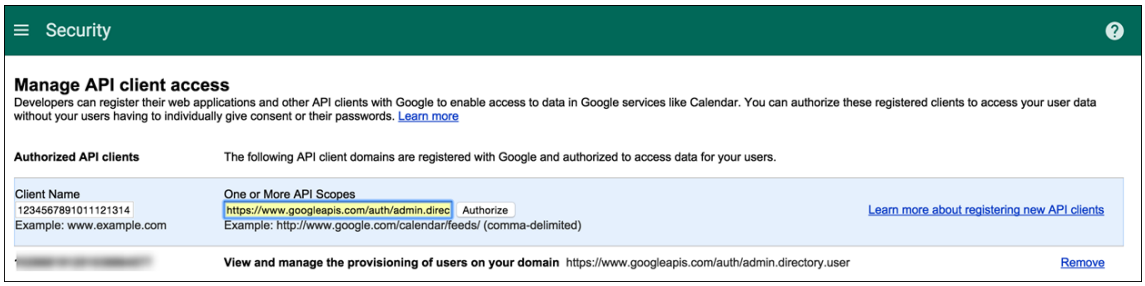




18. [**Manage API client access**] をクリックします。



19. [**Client Name**] ボックスに前の手順で保存したクライアント ID を入力し、[**One or More API Scopes**] ボックスに「`https://www.googleapis.com/auth/admin.directory.user`」と入力して、[**Authorize**] をクリックします。



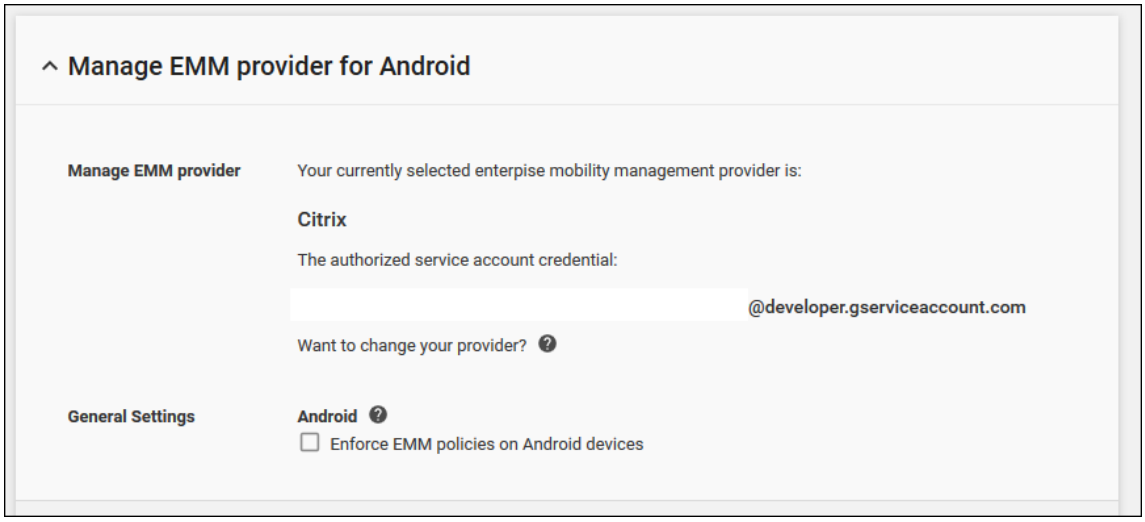
EMM へのバインド

Citrix Endpoint Management を使用して Android デバイスを管理するには、Citrix テクニカルサポートにドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。Citrix では、いただいたトークンを EMM（Enterprise Mobility Management：エンタープライズモビリティ管理）プロバイダーとして Citrix Endpoint Management にバインドします。Citrix テクニカルサポートへのお問い合わせは、Citrix テクニカルサポートを参照してください。

1. バインドを確認するには、Google Admin ポータルにサインインして [**Security**] をクリックします。
2. [**Manage EMM provider for Android**] をクリックします。

   Google Android Enterprise アカウントが EMM プロバイダーである Citrix にバインドされていることが表示されます。

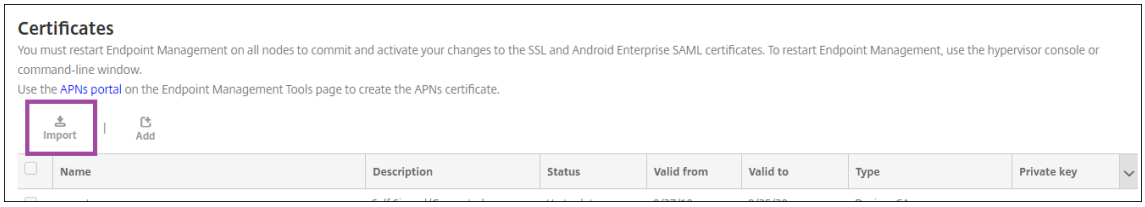
   トークンのバインドを確認した後で、Citrix Endpoint Management コンソールを使用して Android デバイスの管理を開始できます。手順 14 で生成した P12 証明書をインポートします。Android Enterprise サーバー設定をセットアップし、SAML ベースのシングルサインオン（Single Sign-On：SSO）を有効化し、少なくとも Android Enterprise デバイスポリシーを 1 つ定義する必要があります。



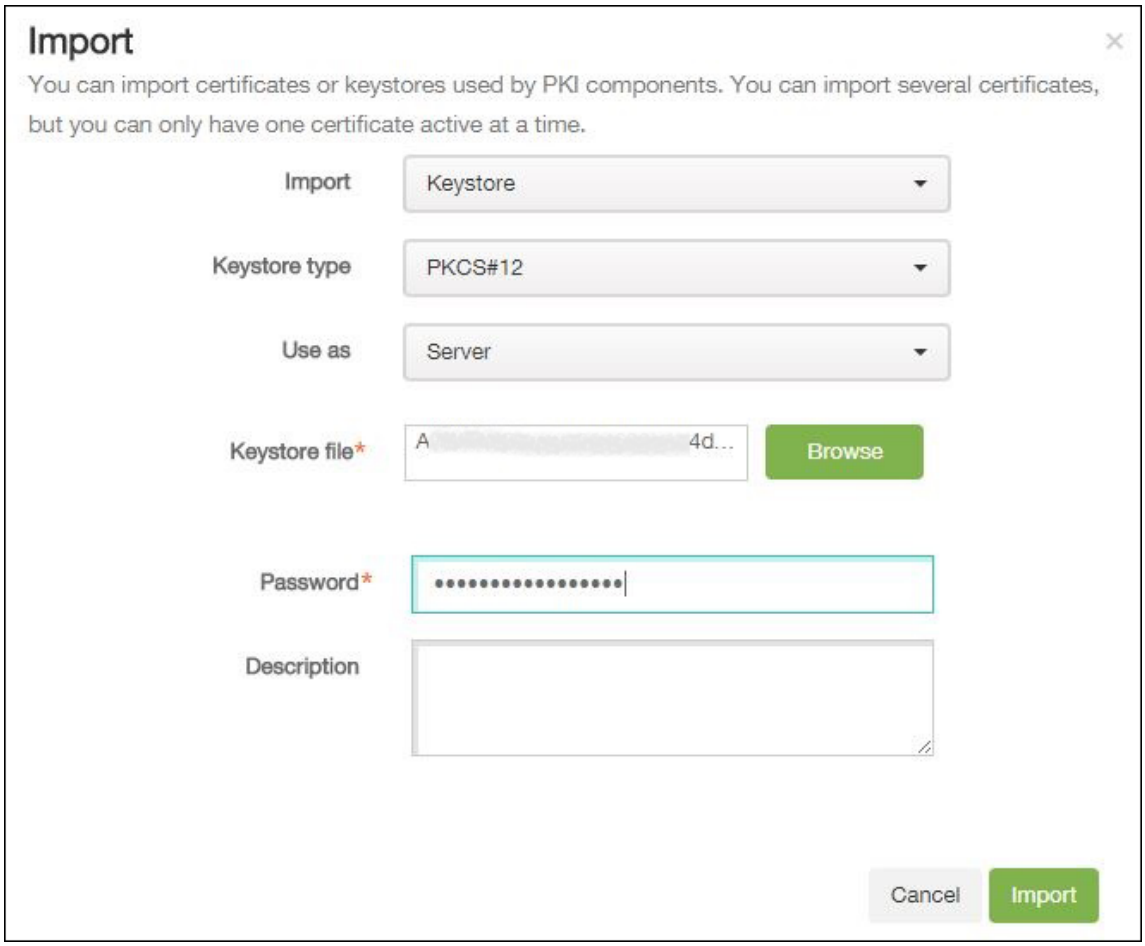
P12 証明書のインポート

以下の手順に従って Android Enterprise の P12 証明書をインポートします:

1. Citrix Endpoint Management コンソールで、コンソールの右上にある歯車アイコンをクリックして ［設定］ページを開き、［証明書］をクリックします。［証明書］ページが開きます。



2. ［インポート］をクリックします。［インポート］ダイアログボックスが開きます。



次の設定を構成します:

- インポート: ボックスの一覧から、［キーストア］を選択します。
- キーストアの種類: ボックスの一覧から、［**PKCS#12**］を選択します。
- 使用目的: ボックスの一覧から、［サーバー］を選択します。
- キーストアファイル: ［ブラウザー］をクリックして、P12 証明書を選択します。

- パスワード：証明書のパスワードを入力します。これは、Android Enterprise アカウントをセットアップするときに作成した秘密キーのパスワードです。
- 説明：任意で、証明書の説明を入力します。

3. ［インポート］をクリックします。

Android Enterprise サーバー設定のセットアップ

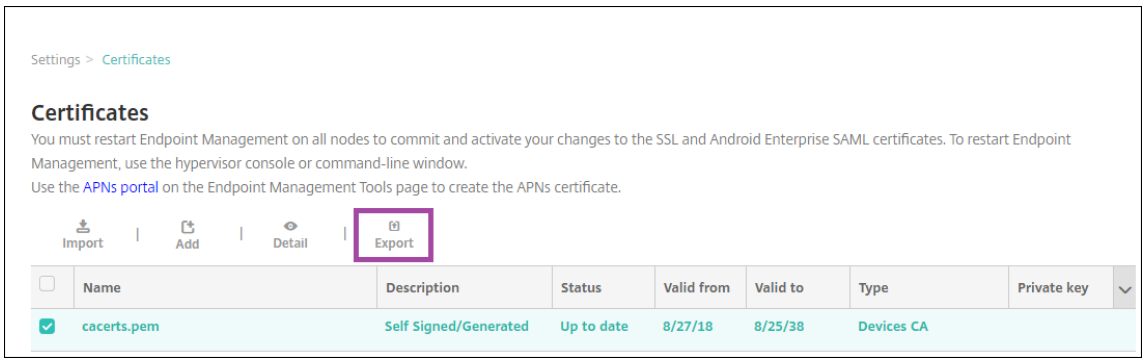
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［プラットフォーム］で［**Android Enterprise**］を選択します。［**Android Enterprise**］ページが開きます。

次の設定を構成し、［保存］をクリックします。

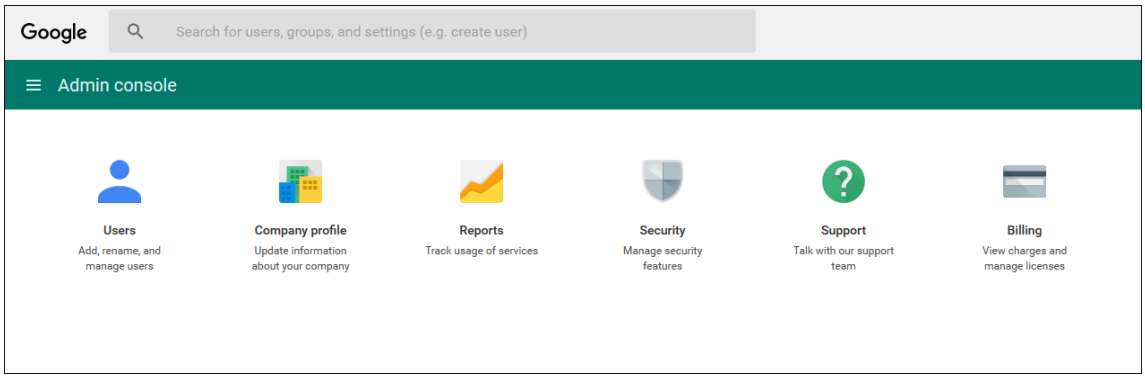
- ドメイン名： Android Enterprise のドメイン名を入力します（例：domain.com）。
- ドメイン管理アカウント：ドメイン管理者のユーザー名を入力します（例：Google Developer Portal で使用しているメールアカウント）。
- サービスアカウント **ID**：サービスアカウント ID を入力します（例：Google Service Account（serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com）に関連付けられたメールアドレス）。
- クライアント **ID**： Google サービスアカウントの数値形式のクライアント ID を入力します。
- **Android Enterprise** の有効化： Android Enterprise を有効にするのか、無効にするのかを選択します。

SAML ベースのシングルサインオンの有効化

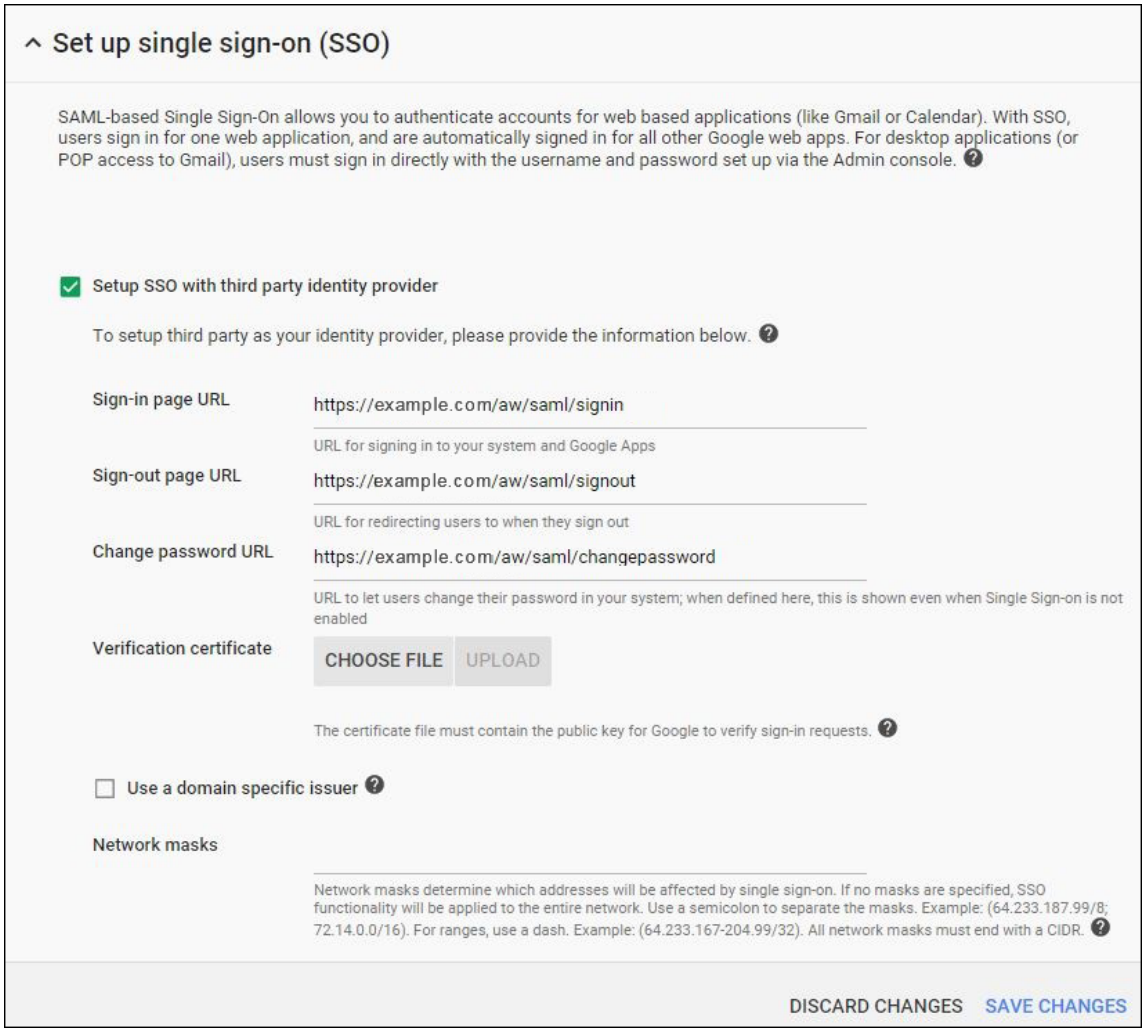
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［証明書］をクリックします。［証明書］ページが開きます。



3. 証明書の一覧から、SAML 証明書を選択します。
4. [エクスポート] をクリックして証明書をコンピューターに保存します。
5. Android Enterprise の管理者資格情報で Google Admin ポータルにサインインします。ポータルへのアクセスについて詳しくは、Google Admin portalを参照してください。
6. [**Security**] をクリックします。



7. [**Security**] の下の [**Set up single sign-on**（**SSO**）] をクリックして以下の設定を構成します。

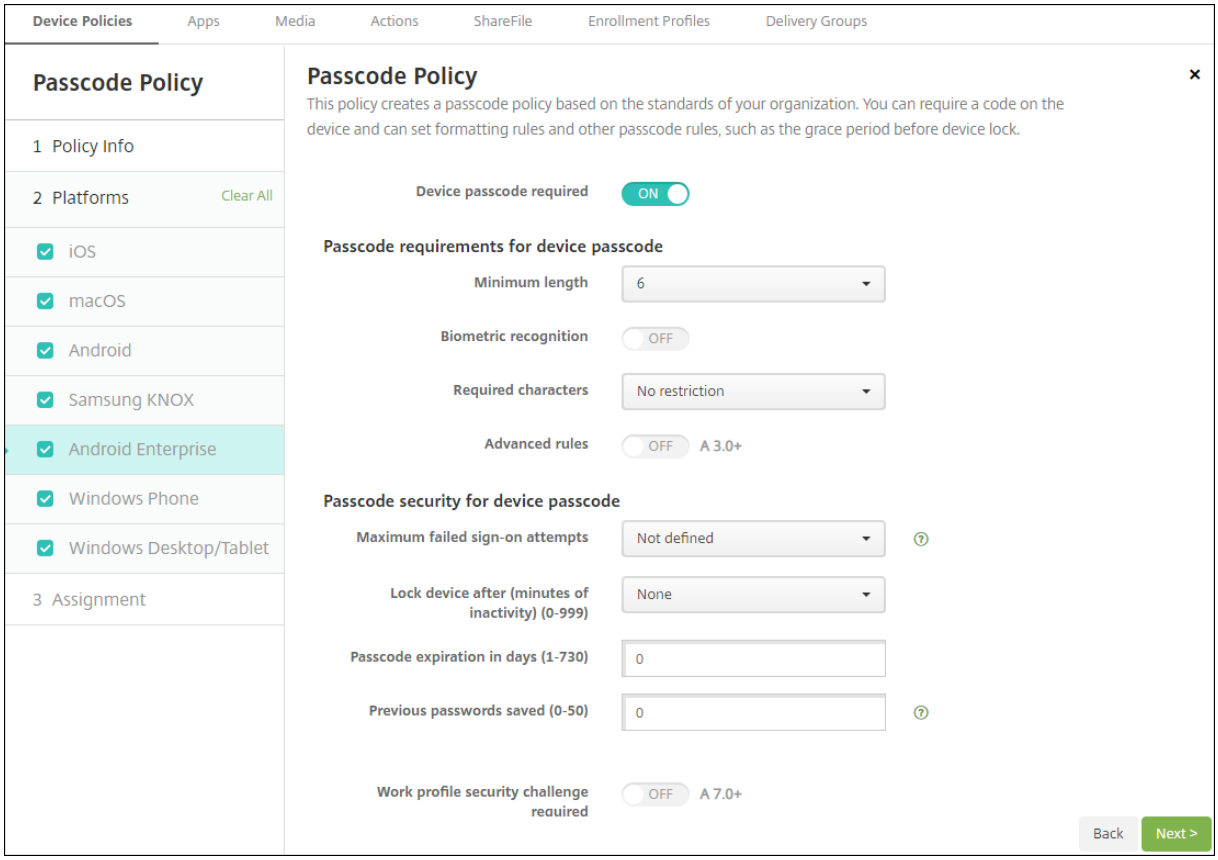


- **Sign-in page URL**：お使いのシステムおよび Google Apps にサインインするページの URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/signin`。
- **Sign-out page URL**：ユーザーがサインアウト時にリダイレクトされる URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/signout`。
- **Change password URL**：ユーザーがシステム内でパスワードを変更するときにアクセスする URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/changepassword`。このフィールドが定義されると、SSO が使用できない場合でもこのメッセージが表示されます。
- **Verification certificate**：[**CHOOSE FILE**] をクリックして、Citrix Endpoint Management からエクスポートした SAML 証明書を選択します。

8. [**SAVE CHANGES**] をクリックします。

Android Enterprise デバイスポリシーのセットアップ

パスコードポリシーをセットアップして、ユーザーが初めて登録するときにデバイスでのパスコード設定を必須にします。



デバイスポリシーの基本的なセットアップ手順は以下のとおりです。

1. Citrix Endpoint Management コンソールで、[構成]、[デバイスポリシー] の順にクリックします。
2. [追加] をクリックして、[新しいポリシーの追加] ダイアログボックスから追加するポリシーを選択します。この例では [パスコード] をクリックします。
3. [ポリシー情報] ページに入力します。
4. [**Android Enterprise**] をクリックしてポリシーの設定を構成します。
5. ポリシーをデリバリーグループに割り当てます。

Android Enterprise アカウント設定の構成

デバイスの Android アプリとポリシーを管理するには、Citrix Endpoint Management で Android Enterprise のドメインおよびアカウント情報を設定する必要があります。まず、Google で Android Enterprise の設定タスクを完了してドメイン管理者を設定し、サービスアカウント ID とバインドトークンを取得する必要があります。

1. Citrix Endpoint Management Web コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [プラットフォーム] で [**Android Enterprise**] を選択します。[**Android Enterprise**] 構成ページが開きます。

1. [**Android Enterprise**] ページで以下の設定を構成します:
   - ドメイン名: ドメイン名を入力します。
   - ドメイン管理アカウント: ドメイン管理者のユーザー名を入力します。
   - サービスアカウント **ID**: Google のサービスアカウント ID を入力します。
   - クライアント **ID**: Google サービスアカウントのクライアント ID を入力します。
   - **Android Enterprise** の有効化: Android Enterprise を有効にするかどうかを選択します。
2. [保存] をクリックします。

Citrix Endpoint Management の **Google Workspace** パートナーアクセスのセットアップ

Chrome の一部の Citrix Endpoint Management 機能では、Citrix Endpoint Management と Google Workspace ドメイン間の通信に Google パートナー API を使用します。たとえば、Citrix Endpoint Management では、シークレットモードやゲストモードなどの Chrome 機能を管理するデバイスポリシーにこうした API が必要です。

パートナー API を有効にするには、Citrix Endpoint Management コンソールで Google Workspace ドメインをセットアップしてから、Google Workspace アカウントを構成します。

Citrix Endpoint Management で **Google Workspace** ドメインをセットアップする

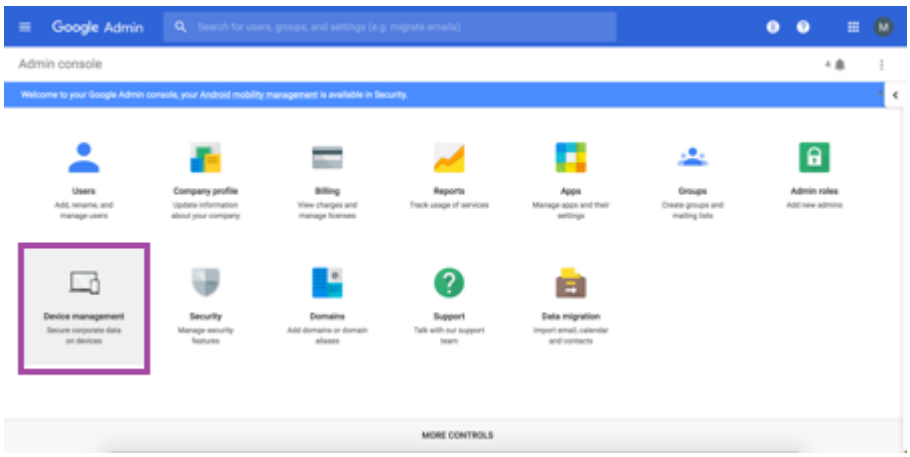
Citrix Endpoint Management と Google Workspace ドメインの API を通信できるようにするには、[設定] > [**Google Chrome** の構成] で設定を構成します。

- **Google Workspace** ドメイン: Citrix Endpoint Management に必要な API をホストする Google Workspace ドメイン。
- **Google Workspace** 管理者アカウント: Google Workspace ドメインの管理者アカウント。
- **Google Workspace** クライアント **ID**: シトリックスのクライアント ID。Google Workspace ドメインのパートナーアクセスを構成する場合は、この値を使用します。

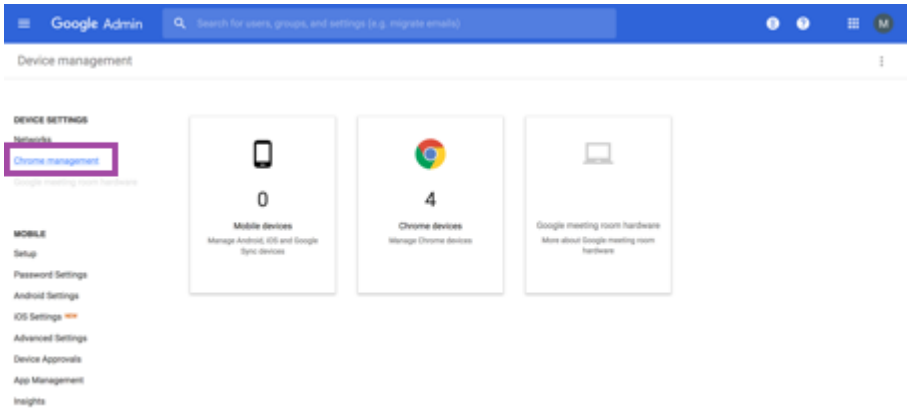
- **Google Workspace** エンタープライズ **ID**：アカウントのエンタープライズ ID。お客様の Google エンタープライズアカウントから入力されます。

Google Workspace ドメイン内のデバイスとユーザーのパートナーアクセスを有効にする

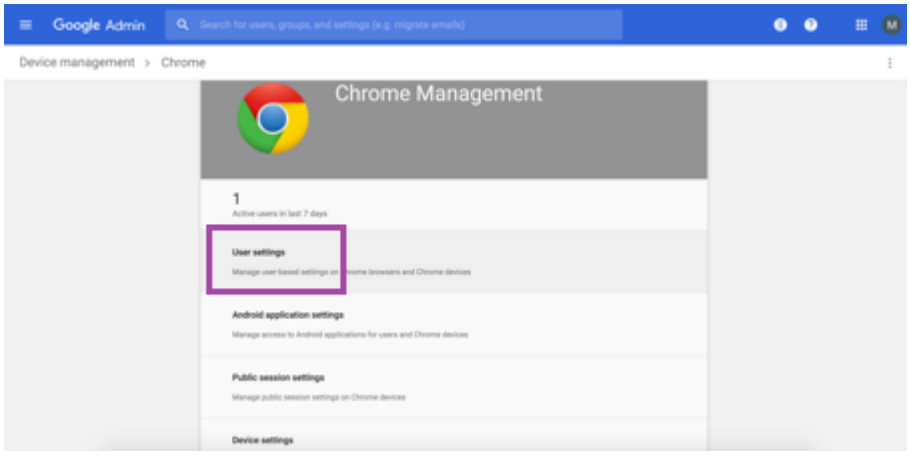
1. Google 管理コンソールにログインします：https://admin.google.com
2. [端末管理] をクリックします。



3. [**Chrome** 管理] をクリックします。

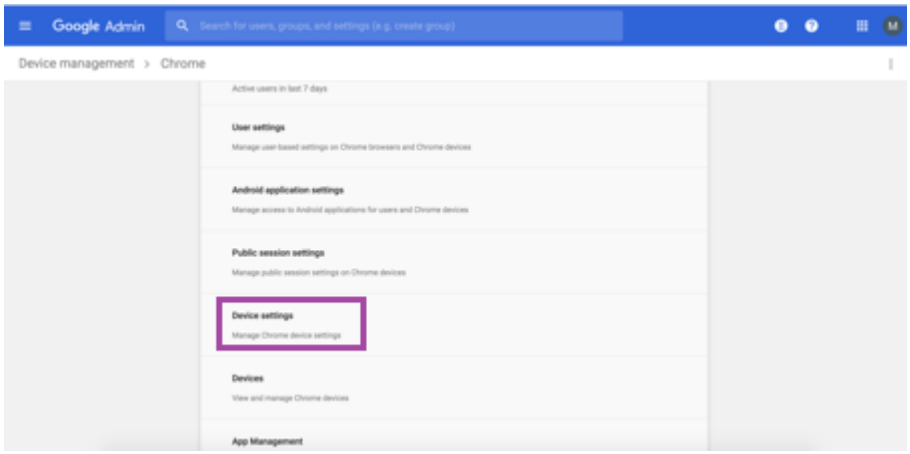


4. [ユーザー設定] をクリックします。



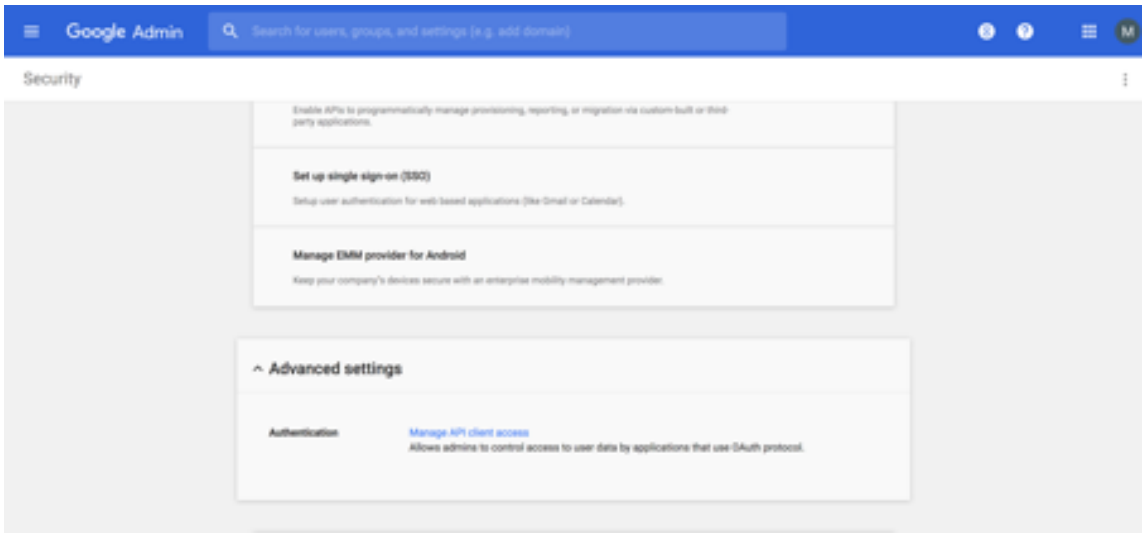
5. [**Chrome** 管理**-**パートナーアクセス］を見つけます。

6. [**Chrome** 管理**-**パートナーアクセスを有効にします］チェックボックスをオンにします。
7. パートナーアクセスについて了承し、有効にする必要があることに同意します。[保存］をクリックします。
8. [Chrome 管理］ページで ［端末設定］をクリックします。

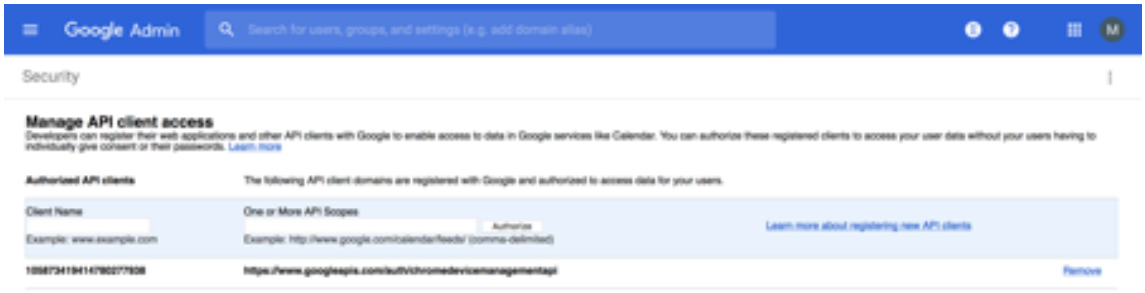


9. ［**Chrome** 管理**-**パートナーアクセス］を見つけます。

10. ［**Chrome** 管理**-**パートナーアクセスを有効にします］チェックボックスをオンにします。
11. パートナーアクセスについて了承し、有効にする必要があることに同意します。［保存］をクリックします。
12. ［セキュリティ］ページに移動し、［詳細設定］をクリックします。



13. ［**API** クライアントアクセスを管理する］をクリックします。
14. Citrix Endpoint Management コンソールで、［設定］**>**［**Google Chrome** の構成］に移動し、［G Suite クライアント ID］の値をコピーします。次に、［**API** クライアントアクセスを管理する］ページに戻り、コピーした値を ［クライアント名］フィールドに貼り付けます。
15. ［**1** つ以上の **API** の範囲］に次の URL を追加します: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. ［承認］をクリックします。

    「設定が保存されました」というメッセージが表示されます。

Android Enterprise デバイスの登録

デバイス登録処理でユーザーがユーザー名またはユーザー ID を入力する必要がある場合、使用可能な形式は、Citrix Endpoint Management がユーザープリンシパル名（UPN）または SAM アカウント名でユーザーを検索するように構成されているかどうかによって異なります。

Citrix Endpoint Management サーバーが UPN でユーザーを検索するように構成されている場合、ユーザーは以下の形式で UPN を入力する必要があります：

- ユーザー名 @ ドメイン

Citrix Endpoint Management サーバーが SAM でユーザーを検索するように構成されている場合、ユーザーは以下のどちらかの形式で SAM を入力する必要があります：

- ユーザー名 @ ドメイン
- ドメイン\ユーザー名

Citrix Endpoint Management サーバーがどちらのユーザー名の種類を使用するように構成されているか確認するには：

1. Citrix Endpoint Management サーバーコンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［**LDAP**］をクリックして、LDAP 接続の設定を表示します。
3. ページの下部にある ［ユーザー検索基準］フィールドを表示します。
    - ［**userPrincipalName**］に設定すると、Citrix Endpoint Management サーバーは UPN で検索するように設定されます。
    - ［**sAMAccountName**］に設定すると、Citrix Endpoint Management サーバーは SAM で検索するように設定されます。

Android Enterprise エンタープライズの登録解除

Citrix Endpoint Management サーバーコンソールと Citrix Endpoint Management ツールを使用して、Android Enterprise エンタープライズの登録を解除できます。

このタスクを実行すると、Citrix Endpoint Management サーバーに Citrix Endpoint Management ツールのポップアップウィンドウが表示されます。始める前に、Citrix Endpoint Management サーバーに、使用する Web ブラウザーでポップアップウィンドウを開く権限があることを確認してください。Google Chrome などの一部の Web ブラウザーでは、ポップアップブロックを無効にし、Citrix Endpoint Management サイトのアドレスをポップアップの許可リストに追加する必要があります。

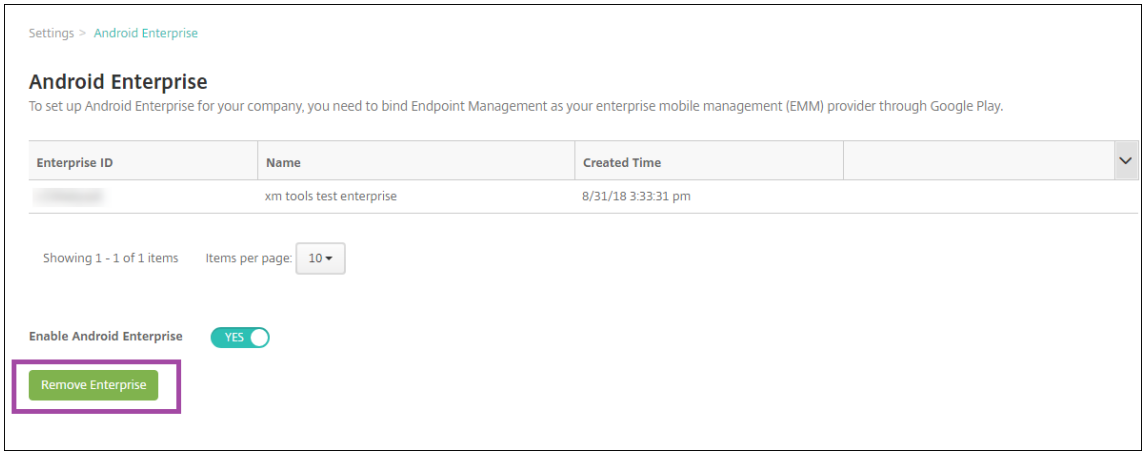
> 警告:
>
> エンタープライズの登録を解除すると、エンタープライズ経由で登録されていたデバイスの Android Enterprise アプリはデフォルトの状態にリセットされます。デバイスは Google によって管理されなくなります。それらのデバイスを Android Enterprise エンタープライズで再登録しても、以前の機能を復元することはできません。追加で構成を行う必要があります。

Android Enterprise エンタープライズの登録を解除した後:

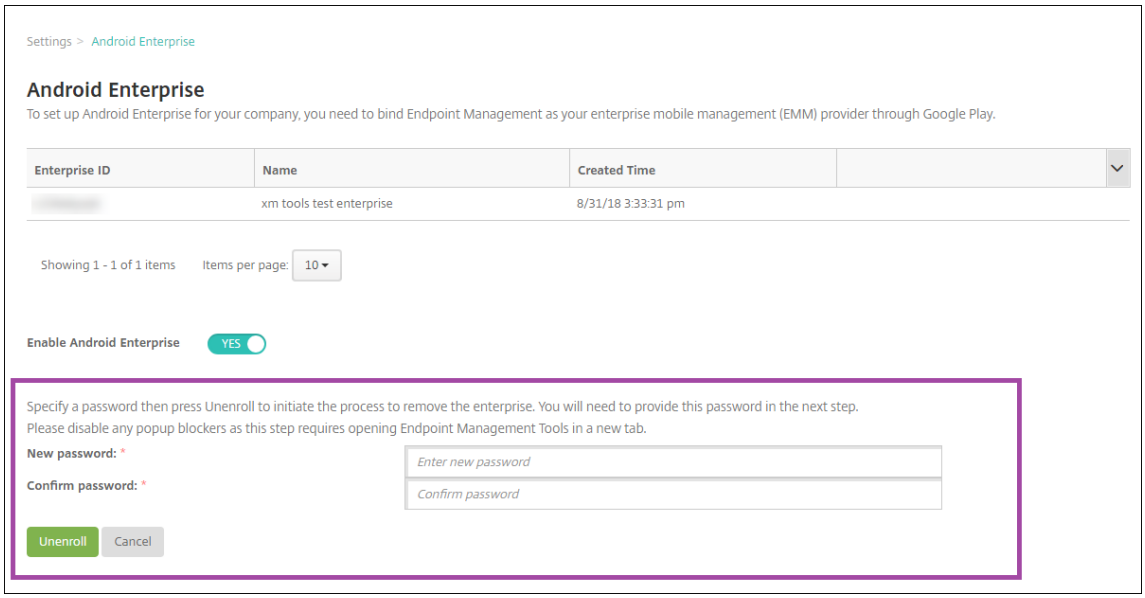
- エンタープライズ経由で登録されていたデバイスとユーザーの Android Enterprise アプリは、デフォルト状態にリセットされます。以前に適用されていた［アプリの権限］ポリシーと［管理対象の構成］ポリシーは無効になります。
- エンタープライズ経由で登録されていたデバイスは Citrix Endpoint Management によって管理されますが、Google の観点からは管理されません。新しい Android Enterprise アプリを追加することはできません。［アプリの権限］ポリシーと［管理対象の構成］ポリシーは適用できません。ただし、これらのデバイスには引き続き、スケジュール設定、パスワード、制限などのポリシーは適用できます。
- Android Enterprise にデバイスを登録しようとすると、Android Enterprise デバイスではなく Android デバイスとして登録されます。

Android Enterprise エンタープライズの登録を解除するには:

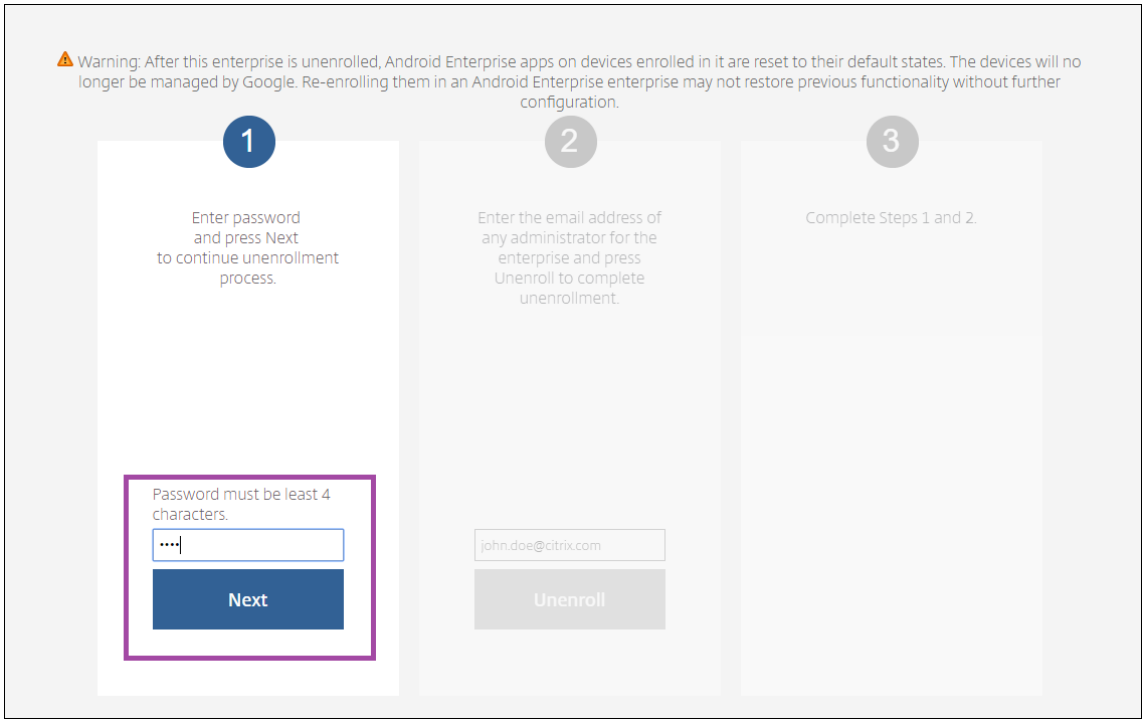
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで、［**Android Enterprise**］をクリックします。
3. ［エンタープライズの削除］をクリックします。



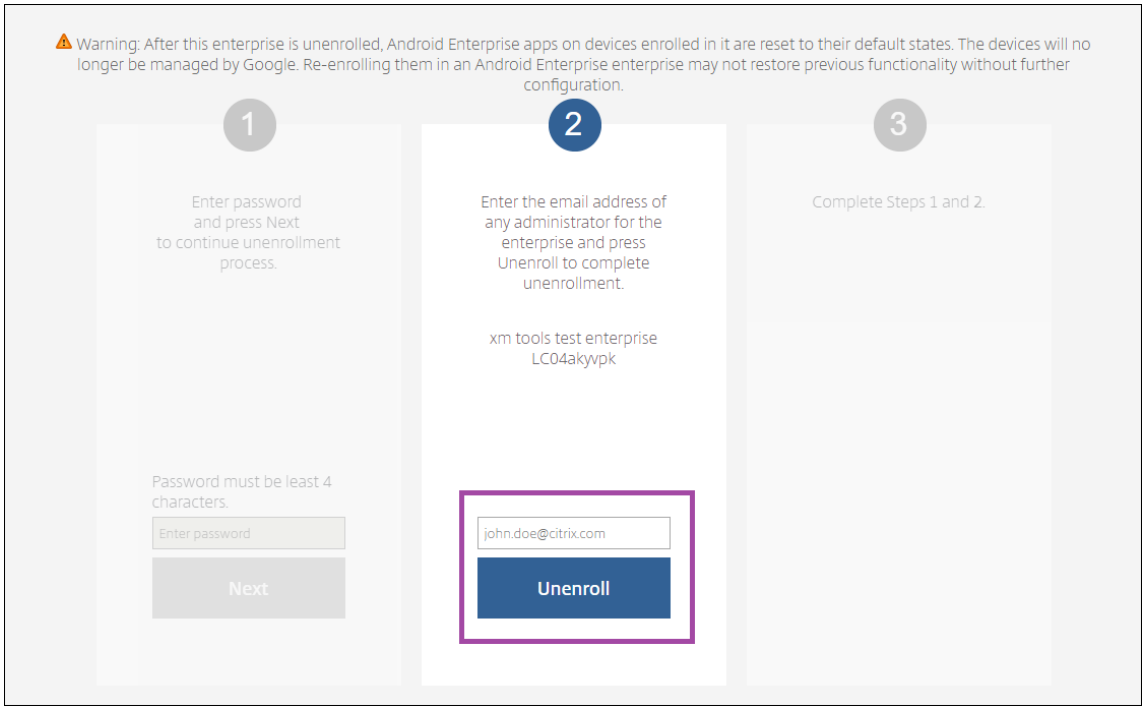
4. パスワードを指定します。登録解除を完了するには、次のステップでこのパスワードが必要になります。[登録解除] をクリックします。



5. [Citrix Endpoint Management Tools] ページが開いたら、前の手順で作成したパスワードを入力します。



6. [登録解除] をクリックします。



Android Enterprise での完全に管理されたデバイスのプロビジョニング

Android Enterprise で完全に管理されたデバイスとして使用できるのは、会社所有のデバイスのみです。完全に管理されたデバイスでは、仕事用プロファイルだけでなく、デバイス全体が会社または組織によって管理されます。完

全に管理されたデバイスは、仕事用管理対象デバイスとも呼ばれます。

Citrix Endpoint Management は、完全に管理されたデバイスで以下の登録方法をサポートしています:

- **afw#xenmobile**: この登録方法では、ユーザーがデバイスの設定時に「afw#xenmobile」という文字を入力します。このトークンにより、デバイスが Citrix Endpoint Management の管理対象であると識別され、Citrix Secure Hub がダウンロードされます。
- **QR** コード: QR コードプロビジョニングは、NFC をサポートしていない、タブレットなどの分散型端末を簡単にプロビジョニングする方法です。QR コード登録方法は、出荷時の設定にリセットされたフリートデバイスで使用できます。QR コードによる登録方法では、セットアップウィザードから QR コードをスキャンすることによって、完全に管理されたデバイスを設定および構成します。
- **NFC**（近距離無線通信）バンプ: NFC バンプ登録方法は、出荷時の設定にリセットされたフリートデバイスで使用できます。NFC バンプは、近距離無線通信を使用して 2 つのデバイス間でデータを転送します。工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびそのほかの通信モードは無効になっています。この状態のデバイスが使用する通信プロトコルは NFC のみです。

afw#xenmobile

この登録方法は、新規デバイスまたは工場出荷時設定にリセットされたデバイスの電源を入れ、初期セットアップを行った後に使用します。ユーザーは、Google アカウントの入力を求められたら「afw#xenmobile」と入力します。この操作により、Citrix Secure Hub がダウンロードされインストールされます。インストール後、Citrix Secure Hub の設定プロンプトに従って登録を完了します。

この登録方法では Citrix Secure Hub の最新バージョンが Google Play ストアからダウンロードされるため、ほとんどのお客様に推奨されます。他の登録方法とは異なり、Citrix Endpoint Management サーバーでダウンロード用に Citrix Secure Hub を提供することはありません。

前提条件:

- Android OS を実行するすべての Android デバイスでサポートされます。

QR コード

QR コードを使用してデバイスモードでデバイスを登録するには、JSON を作成してから QR コードに変換して、QR コードを生成します。この QR コードをデバイスカメラでスキャンし、デバイスを登録します。

前提条件:

- Android 7.0 以降を実行するすべての Android デバイスでサポートされます。

JSON から **QR** コードを作成する　次のフィールドがある JSON を作成します。

これらのフィールドは必須です。

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

値：com.zenprise / com.zenprise.configuration.AdminFunction

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

値：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

値：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

これらのフィールドはオプションです。

- **android.app.extra.PROVISIONING_LOCALE**：言語コードおよび国コードを入力します。

  言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。

- **android.app.extra.PROVISIONING_TIME_ZONE**：これはデバイスが実行されているタイムゾーンです。

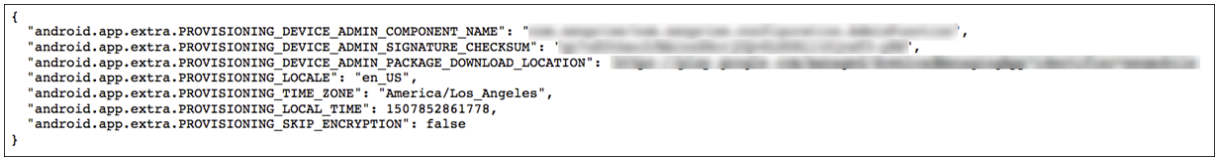
  エリア/場所のデータベース名を入力します。たとえば、米国太平洋標準時の場合は「アメリカ/ロサンジェルス」と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。

- **android.app.extra.PROVISIONING_LOCAL_TIME:** エポックからのミリ秒単位の時間。

  Unix エポック（または Unix 時間または POSIX 時間または Unix タイムスタンプ）は、1970 年 1 月 1 日（UTC/GMT 午前 0 時）から経過した秒数で、うるう秒数は含まれません（ISO 8601: 1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**：プロファイル作成時に暗号化をスキップするには、**true** に設定します。プロファイルの作成時に暗号化を強制するには、**false** に設定します。

以下の図に、典型的な JSON の例を示します。



https://jsonlint.comなどの JSON 検証ツールを使用して作成された JSON を検証します。オンライン QR コードジェネレーターを使用して、JSON 文字列を QR コードに変換します。

この QR コードは工場出荷時の設定にリセットされたデバイスによってスキャンされ、これによってデバイスを完全に管理されたデバイスとして登録できます。

デバイスを登録するには

完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットする必要があります。

1. ようこそ画面で画面を 6 回タップすると、QR コードの登録フローが開始されます。
2. プロンプトが表示されたら、Wi-Fi に接続します。（JSON でエンコードされた）QR コードにある Citrix Secure Hub のダウンロード場所には、この Wi-Fi ネットワーク経由でアクセスできます。

   端末が Wi-Fi に接続されると、Google から QR コードリーダーをダウンロードしてカメラを起動します。
3. カメラを QR コードに合わせて、コードをスキャンします。

   Android は、QR コードのダウンロード場所から Citrix Secure Hub をダウンロードし、署名証明書の署名を検証し、Citrix Secure Hub をインストールし、デバイス所有者として設定します。

QR コード方式を使用したデバイスのプロビジョニングについて詳しくは、Android EMM 開発者のための Google API ドキュメントを参照してください。

NFC バンプ

NFC バンプを使用して完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットされたデバイスと、Citrix Endpoint Management プロビジョニングツールを実行するデバイスの 2 台のデバイスが必要です。

前提条件：

- サポートされる Android デバイス
- Android Enterprise を有効にした Citrix Endpoint Management
- 完全に管理されたデバイスとして Android Enterprise 向けにプロビジョニングされた、新規または工場出荷時設定にリセットされたデバイス。この前提条件を完了する手順については、後述します。
- 構成済みのプロビジョニングツールを実行している、NFC 機能が備わった別のデバイス。Provisioning Tool は、Citrix Secure Hub またはCitrix ダウンロードページから入手できます。

各デバイスには、エンタープライズモビリティ管理（EMM）アプリで管理された Android Enterprise プロファイルを 1 つのみ設定できます。Citrix Endpoint Management では、Citrix Secure Hub が EMM アプリとなります。各デバイスには、1 つのプロファイルしか許可されません。2 つ目の EMM アプリを追加すると、1 つ目の EMM アプリが削除されます。

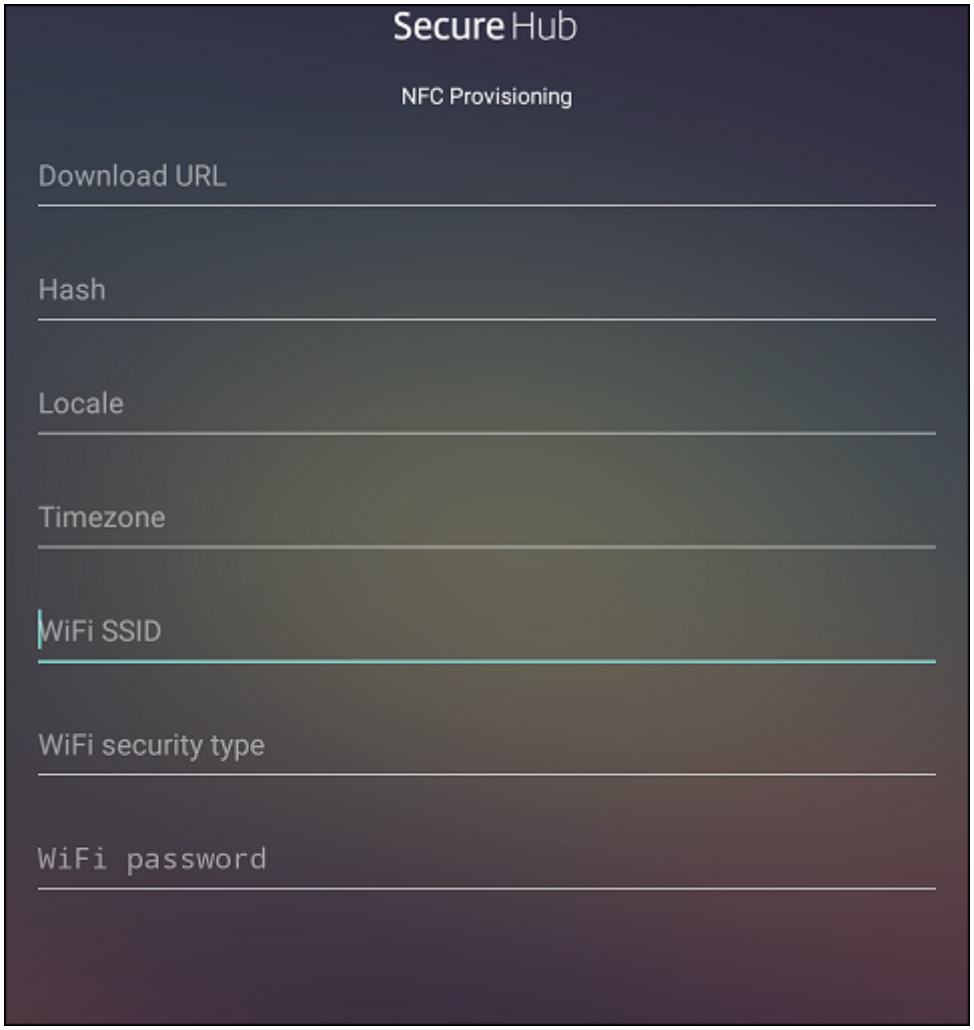
NFC バンプを介して転送されるデータ　工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータを NFC バンプ経由で送信して Android Enterprise を初期化する必要があります：

- デバイス所有者として機能する EMM プロバイダーアプリ（この場合は、Citrix Secure Hub）のパッケージ名。
- デバイスが EMM プロバイダーアプリをダウンロードできるイントラネット/インターネット上の場所。
- ダウンロードが正常に完了したかどうかを確認する EMM プロバイダーアプリの SHA-256 ハッシュ。
- 工場出荷時の設定にリセットされたデバイスが EMM プロバイダーアプリに接続してダウンロードできるようにする Wi-Fi 接続の詳細。注：現時点では、Android はこの手順での 802.1x Wi-Fi をサポートしていません。

- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、プロビジョニングツールのデータが工場出荷時の設定にリセットされたデバイスに送信されます。このデータはその後、管理者設定での Citrix Secure Hub のダウンロードに使用されます。タイムゾーンと場所の値を入力しない場合、新しいデバイスでは Android によって自動的にこれらの値が構成されます。

Citrix Endpoint Management プロビジョニングツールの構成　NFC バンプを行う前に、プロビジョニングツールを構成する必要があります。この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFC バンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルから入力することもできます。次の手順では、テキストファイルを構成する方法と各フィールドに説明を含める方法について説明します。入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

テキストファイルを使用してプロビジョニングツールを構成するには　ファイルの名前を nfcprovisioning.txt にして、デバイスの SD カードの**/sdcard/**フォルダーに格納します。アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには、次のデータを含める必要があります。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

この行は、EMM プロバイダーアプリのイントラネット/インターネットの場所です。工場出荷時設定のデバイスが NFC バンプの後に Wi-Fi に接続した場合、デバイスはダウンロードのためにこの場所にアクセスする必要があります。URL は通常の URL で、特別な形式にする必要はありません。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

この行は、EMM プロバイダーアプリのチェックサムです。このチェックサムはダウンロードが成功したかを検証するために使用されます。チェックサムを取得する手順については、後述します。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

この行は、プロビジョニングツールを実行しているデバイスが接続されている Wi-Fi の SSID です。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

サポートされる値は WEP および WPA2 です。Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

`android.app.extra.PROVISIONING_LOCALE=<locale>`

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

デバイスが実行されるタイムゾーンです。エリア/場所のデータベース名を入力します。たとえば、米国太平洋標準時の場合は「アメリカ/ロサンジェルス」と入力します。名前を入力しない場合、タイムゾーンは自動的に入力されます。

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

このデータは Citrix Secure Hub としてアプリにハードコードされるため、必須ではありません。ここでは、情報の完全性を守るためだけに記載しています。

WPA2 を使用して保護された Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

保護されていない Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGR
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Citrix Secure Hub のチェックサムを取得するには　Citrix Secure Hub のチェックサムは次の定数値です: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。Citrix Secure Hub の APK ファイルをダウンロードするには、次の Google Play ストアのリンクを使用します: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

アプリのチェックサムを取得するには　前提条件:

- Android SDK ビルドツールの **apksigner** ツール
- OpenSSL コマンドライン

アプリのチェックサムを取得するには、次の手順に従います:

1. Google Play ストアからアプリの APK ファイルをダウンロードします。
2. OpenSSL コマンドラインで、**apksigner** ツール`android-sdk/build-tools/<version>/apksigner`に移動して、以下を入力します:


```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```

コマンドから有効なチェックサムが返されます。

3. QR コードを生成するには、PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUMフィールドにチェックサムを入力します。例:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

使用するライブラリ　プロビジョニングツールでは、以下のライブラリがソースコードに使用されています。

- v7 appcompat library、Design support library、および v7 Palette support library

  詳しくは、Android の開発者向けドキュメントの「サポートライブラリの機能ガイド」を参照してください。

- Butter Knife by Jake Wharton（Apache license 2.0）

Android Enterprise での仕事用プロファイルデバイスのプロビジョニング

Android Enterprise の仕事用プロファイルデバイスでは、デバイス上の会社領域と個人領域を安全に分離できます。たとえば、BYOD デバイスを仕事用プロファイルデバイスにすることができます。仕事用プロファイルデバイスの登録手順は、Citrix Endpoint Management で Android を登録する場合と同様です。ユーザーは Google Play から Citrix Secure Hub をダウンロードし、デバイスを登録します。

デバイスが Android Enterprise の仕事用プロファイルデバイスとして登録されている場合、デフォルトでは USB デバッグおよび不明なソース設定は無効になっています。

> ヒント:
>
> Android Enterprise のデバイスを仕事用プロファイルデバイスとして登録する場合は、必ず Google Play にアクセスしてください。そこから、ユーザーの個人プロファイルでの Citrix Secure Hub の表示を有効にします。

Android OS

November 29, 2023

> 注:
>
> このページの内容は、Android Enterprise で管理されているデバイスには適用されません。これらのデバイスについて詳しくは、このセクションの他のページを参照してください。

Citrix Endpoint Management は、Android または Samsung エンタープライズプログラム経由で管理されていない Android OS デバイスもサポートします。Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御するには、Firebase Cloud Messaging (FCM) を使用します。詳しくは、「Firebase Cloud Messaging」を参照してください。

登録プロファイルで、Android デバイスを MAM、MDM、または MDM+MAM のいずれで登録するか、およびユーザーが MDM をオプトアウトするオプションを決定します。Citrix Endpoint Management は、MDM+MAM の Android デバイスに対して、次の種類の認証をサポートします。詳しくは、次の記事を参照してください:

- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- ID プロバイダー:
  - Citrix Cloud を介した Azure Active Directory での認証
  - Citrix Cloud を介した Okta での認証

使用頻度が少ない別の認証方法には、クライアント証明書とセキュリティトークンの組み合わせがあります。詳しくは、「https://support.citrix.com/article/CTX215200」を参照してください。

Android デバイスの管理を開始するための一般的なワークフローは次のとおりです:

1. オンボーディングプロセスの完了。「オンボードとリソースのセットアップ」と「デバイス登録およびリソース配信の準備」を参照してください。
2. 登録方法の選択と構成。「サポートされている登録方法」を参照してください。
3. Android デバイスポリシーを構成します。
4. Android デバイスを登録します。

5. デバイスとアプリのセキュリティ操作の設定。「セキュリティ操作」を参照してください。

サポートされているオペレーティングシステムについては、「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。

サポートされている登録方法

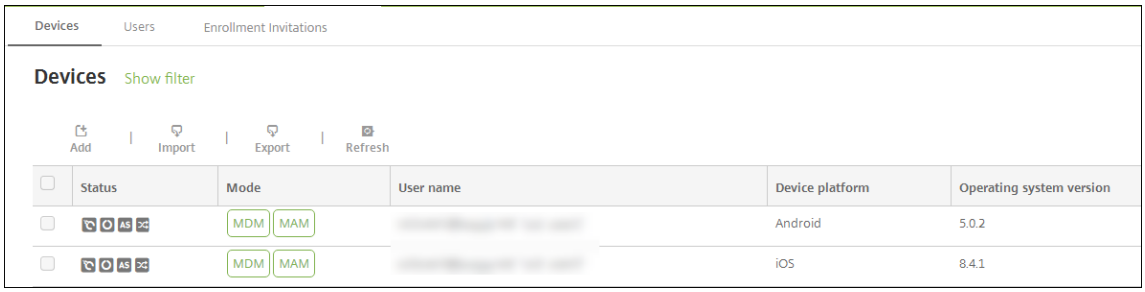
次の表は、Android デバイスでサポートされている Citrix Endpoint Management での登録方法を示しています:

方法	サポート対象
一括登録	番号
手動登録	はい
登録招待	はい

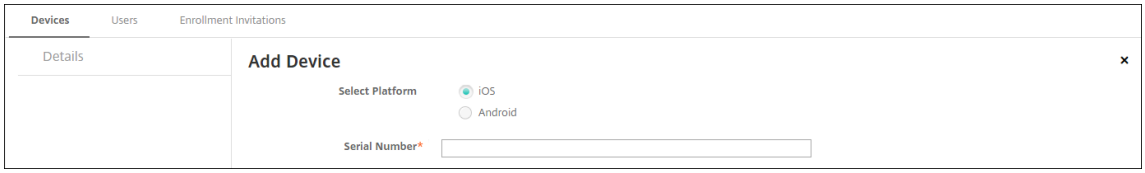
手動による **Android** デバイスの追加

テスト目的など、Android デバイスまたは iOS デバイスを手動で追加する場合は、次の手順に従います。

1. Citrix Endpoint Management コンソールで、[管理] **>** [デバイス] の順にクリックします。[デバイス] ページが開きます。



2. [追加] をクリックします。[デバイスの追加] ページが開きます。



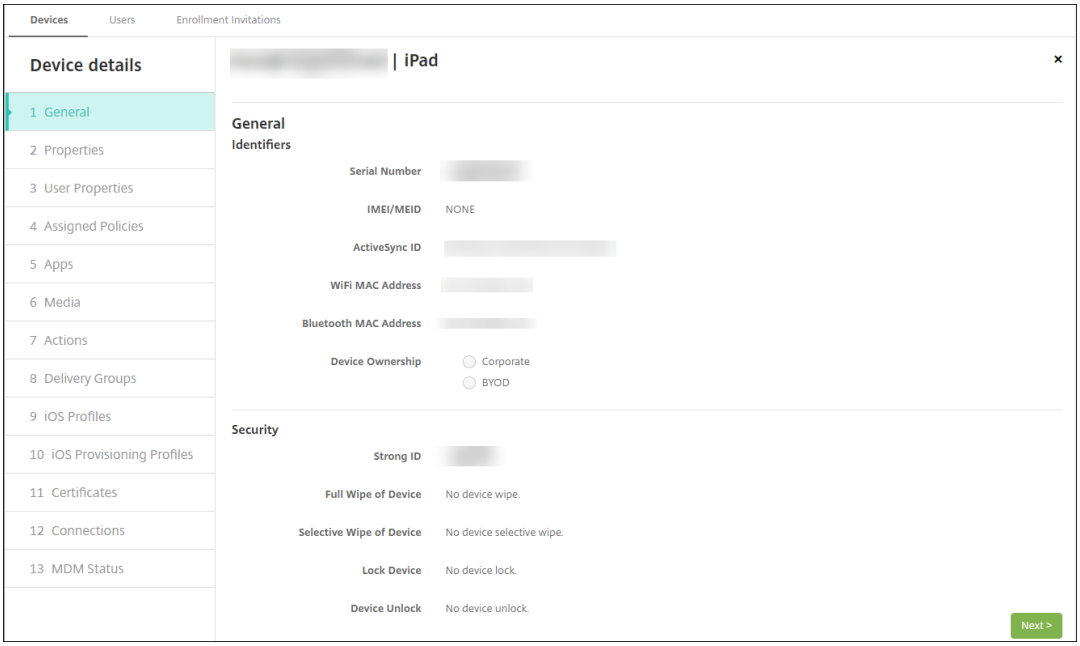
3. 次の設定を構成します:

   - プラットフォーム選択: [**Android**] を選択します。
   - シリアル番号: デバイスのシリアル番号を入力します。
   - **IMEI/MEID**: 任意で、デバイスの IMEI/MEID 情報を入力します。

4. ［追加］をクリックします。［デバイス］の表に示される一覧の一番下に、追加したデバイスが表示されます。デバイスの詳細を表示して確認するには：追加したデバイスを選択して表示されるメニューで ［編集］をクリックします。

   > 注：
   >
   > デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

   - 構成された LDAP
   - ローカルグループおよびローカルユーザーを使用する場合：
     - 1 つまたは複数のローカルグループ。
     - ローカルグループに割り当てられたローカルユーザー。
     - デリバリーグループはローカルグループと関連付けられます。
   - Active Directory を使用する場合：
     - デリバリーグループは Active Directory グループと関連付けられます。



5. ［一般］ページには、シリアル番号やプラットフォームの種類に関するその他の情報など、デバイスの識別子が表示されます。［デバイス所有権］で、［コーポレート］または ［**BYOD**］を選択します。

   ［一般］ページには、デバイスの ［セキュリティ］プロパティ（[Strong ID]、［デバイスのロック］、［アクティベーションロックバイパス］、プラットフォームの種類に関するその他の情報など）も表示されます。［デバイスの完全なワイプ］フィールドには、ユーザーの PIN コードが含まれます。デバイスがワイプされた後、ユーザーはこのコードを入力する必要があります。ユーザーがコードを忘れた場合は、こちらで確認できます。

6. ［プロパティ］ページには、Citrix Endpoint Management がプロビジョニングするデバイスのプロパティが表示されます。この一覧は、デバイスの追加に使用されるプロビジョニングファイルに含まれるデバイスのプロパティを表示します。プロパティを追加するには、［追加］をクリックして一覧からプロパティを選択します。各プロパティの有効な値に関しては、デバイスのプロパティ名と値に関する PDF を参照してください。

   プロパティを追加すると、最初に追加したカテゴリに表示されます。［次へ］をクリックして ［プロパティ］ページに戻ると、プロパティは適切な一覧に表示されます。

   プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の ［**X**］をクリックします。Citrix Endpoint Management デバイスによりその項目が削除されます。

7. 残りの ［デバイス詳細］セクションには、デバイスの概要が表示されます。

   - ユーザープロパティ：ユーザーの RBAC の役割、グループメンバーシップ、管理対象の Google Play アカウント、およびプロパティを表示します。このページでインベントリから管理対象の Google Play アカウントを削除できます。
   - 割り当て済みポリシー：展開済みのポリシー、保留中のポリシー、失敗したポリシーの数が表示されます。各ポリシーの名前、種類、最新展開の情報が表示されます。展開ステータスをリセットして保留にしたり、ユーザーが削除したポリシーを再展開したりできます。
   - アプリ：インストール済み、保留中、失敗のアプリ展開数を含む、最新のインベントリ時点のアプリ数が表示されます。アプリ名、ID、種類、その他の情報が表示されます。**HasUpdateAvailable** などの iOS および macOS のインベントリキーの説明については、「モバイルデバイス管理（MDM）プロトコル」を参照してください。
   - メディア：展開済み、保留中、失敗のメディア展開数を含む、最新のインベントリ時点のメディア数が表示されます。
   - 操作：展開済み、保留中、失敗のアクション数を含む、アクション数が表示されます。最新展開のアクション名と時間が表示されます。
   - デリバリーグループ：成功、保留中、失敗したデリバリーグループの数が表示されます。各展開のデリバリーグループ名と展開時間が表示されます。デリバリーグループを選択すると、状態、アクション、チャネル、またはユーザーなどの詳細な情報を表示できます。
   - **iOS** プロファイル：名前、種類、組織、説明など、最新の iOS プロファイルインベントリが表示されます。
   - **iOS** プロビジョニングプロファイル： UUID、有効期限、管理対象かどうかなど、エンタープライズ配布プロビジョニングプロファイルの情報を表示します。
   - 証明書：有効な証明書と期限切れまたは失効した証明書が表示され、種類、プロバイダー、発行者、シリアル番号、期限切れまでの残日数などの情報も表示されます。
   - 接続：最初の接続状態と最後の接続状態が表示されます。各接続のユーザー名、最後から 2 番目の認証時間、最後の認証時間が表示されます。
   - **MDM** ステータス： MDM ステータス、最後のプッシュ時間、最後のデバイス応答時間などの情報が表示されます。

Android デバイスポリシーの構成

デバイスポリシーを使用して、Citrix Endpoint Management と Android を実行するデバイスとの通信に関する構成を行います。次の表は、Android デバイスで使用可能なデバイスポリシーの一覧です。

–	–	–
[アクセスポイント名](/ja-jp/citrix-endpoint-management/policies/apn-policy.html#android-settings)	[アプリアクセス](/ja-jp/citrix-endpoint-management/policies/app-access-policy.html)	[アプリインベントリ](/ja-jp/citrix-endpoint-management/policies/app-inventory-policy.html)
[アプリのロック](/ja-jp/citrix-endpoint-management/policies/app-lock-policy.html#android-legacy-da-settings)	[アプリのアンインストール](/ja-jp/citrix-endpoint-management/policies/app-uninstall-policy.html)	[資格情報](/ja-jp/citrix-endpoint-management/policies/credentials-policy.html#android-settings)
[Citrix Endpoint Management オプション](/ja-jp/citrix-endpoint-management/policies/options-policy.html)	[Citrix Endpoint Management のアンインストール](/ja-jp/citrix-endpoint-management/policies/uninsta policy.html)	[ファイル](/ja-jp/citrix-endpoint-management/policies/files-policy.html)
[Launcher 構成](/ja-jp/citrix-endpoint-management/policies/launcher-configuration-policy.html)	[位置情報](/ja-jp/citrix-endpoint-management/policies/location-policy.html#android-legacy-da-settings)	[ネットワーク](/ja-jp/citrix-endpoint-management/policies/network-policy.html#android-legacy-da-settings)
[パスコード](/ja-jp/citrix-endpoint-management/policies/passcode-policy.html#android-legacy-da-settings)	[制限](/ja-jp/citrix-endpoint-management/policies/restrictions-policy.html#android-settings)	[スケジューリング](/ja-jp/citrix-endpoint-management/policies/connection-scheduling-policy.html)
[ストア](/ja-jp/citrix-endpoint-management/policies/store-policy.html)	[使用条件](/ja-jp/citrix-endpoint-management/policies/terms-and-conditions-policy.html)	[トンネル](/ja-jp/citrix-endpoint-management/policies/tunnel-policy.html)
VPN	Web クリップ

Android デバイスの登録

1. Android デバイスで Google Play ストアにアクセスして、Citrix Secure Hub アプリをダウンロードしてタップします。
2. インストールを求めるメッセージが表示されたら、［次へ］をクリックし、［インストール］をクリックします。
3. Citrix Secure Hub のインストールが完了したら、［開く］をタップします。
4. Android 6.0 以降を実行しているデバイスの場合、必要な権限を承諾します:
    - Citrix Secure Hub による通話の発信と管理を許可するか?（必須）
    - Citrix Secure Hub によるデバイス上の写真、メディア、ファイルへのアクセスを許可するか?（必須）

- Citrix Secure Hub によるこのデバイスの場所へのアクセスを許可するか?（オプション）

5. 会社の資格情報として、Citrix Endpoint Management サーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなどを入力します。入力後、［次へ］をクリックします。
6. デバイスの登録方法を選択します：
   - MDM+MAM で登録するには、［はい、登録します］をタップします。
   - MAM で登録するには、［いいえ］をタップします。
7. ［デバイス管理者を有効にしますか］画面で、［有効にする］をタップします。
8. 会社のパスワードを入力し、［サインオン］をタップします。
9. Citrix Endpoint Management の構成方法によっては、Citrix PIN を作成するよう求められます。この PIN を使用すると、Citrix Secure Hub やその他の Citrix Endpoint Management 対応アプリ（Citrix Secure Mail および Citrix Files など）にサインオンできます。Citrix PIN は 2 回入力します。［**Citrix PIN** の作成］画面で、PIN を入力します。
10. PIN を再入力します。Citrix Secure Hub が開きます。その後、アプリストアにアクセスすると、Android デバイスにインストール可能なアプリを確認できます。
11. 登録後にアプリをデバイスに自動的にプッシュするように Citrix Endpoint Management を構成している場合は、アプリのインストールを求めるプロンプトがユーザーに表示されます。また、Citrix Endpoint Management で構成済みのポリシーがデバイスに展開されます。［インストール］をタップしてアプリをインストールします。

Android デバイスを登録解除および再登録するには

ユーザーは Citrix Secure Hub 内から登録解除できます。次の方法で登録解除する場合、デバイスは Citrix Endpoint Management コンソールのデバイスインベントリに表示され続けます。ただし、そのデバイスで操作を実行することはできません。たとえば、該当デバイスを追跡したり、デバイスのコンプライアンスを監視したりすることはできません。

1. Citrix Secure Hub アプリをタップして開きます。
2. スマートフォンかタブレットかに応じて、次の操作を行います。

   スマートフォンの場合：

   - 画面左側からスワイプして設定ペインを開きます。
   - ［設定］、［アカウント］、［アカウントの削除］の順にタップします。

   タブレットの場合：

   - 右上のメールアドレスの横の矢印をタップします。

- ［設定］、［アカウント］、［アカウントの削除］の順にタップします。

3. ［アカウントの削除］ウィンドウで、［はい、削除します］をタップします。
   Citrix Secure Hub はデバイスの登録を解除します。画面の指示に従って、デバイスを再登録します。

セキュリティ操作

Android は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

アプリのロック	アプリのワイプ	証明書の書き換え
完全なワイプ	検索	ロック
パスワードのロックとリセット	Notify	取り消し
選択的なワイプ		

> 注:
>
> Android 6.0 以降を実行するデバイスの場合、検索セキュリティ操作には、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しない選択をできます。登録時にユーザーによって権限が付与されないと、Citrix Endpoint Management は Locate コマンドの送信時に検索の権限を再度要求します。

Firebase Cloud Messaging

November 29, 2023

> 注:
>
> Firebase Cloud Messaging（FCM）は以前は Google Cloud Messaging（GCM）と呼ばれていました。Citrix Endpoint Management コンソールのラベルとメッセージの一部には、GCM 用語が使用されています。

Firebase Cloud Messaging（FCM）を使用して Android デバイスが Citrix Endpoint Management に接続するタイミングと方法を制御することを Citrix ではお勧めします。Citrix Endpoint Management で FCM が構成されている場合、FCM を有効にした Android デバイスへの接続通知を送信します。セキュリティ操作や展開コマンドによって、ユーザーに Citrix Endpoint Management サーバーへの再接続を求めるプッシュ通知が送信されます。

この記事の構成手順を完了し、デバイスがチェックインすると、デバイスは Citrix Endpoint Management で FCM サービスに登録します。これにより、FCM を使用して Citrix Endpoint Management サービスからデバイスにほぼリアルタイムで通信することができます。FCM の登録は、新しく登録するデバイスおよび以前に登録されたデバイスで機能します。

Citrix Endpoint Management がデバイスへの接続を開始するとき、Citrix Endpoint Management は FCM サービスに接続し、FCM サービスは接続するようにデバイスに通知します。この種類の接続は、Apple プッシュ通知サービスでの接続と似ています。

前提条件

- 最新の Citrix Secure Hub クライアント
- Google デベロッパーアカウントの資格情報
- FCM 対応 Android デバイスにインストールされた Google Play サービス

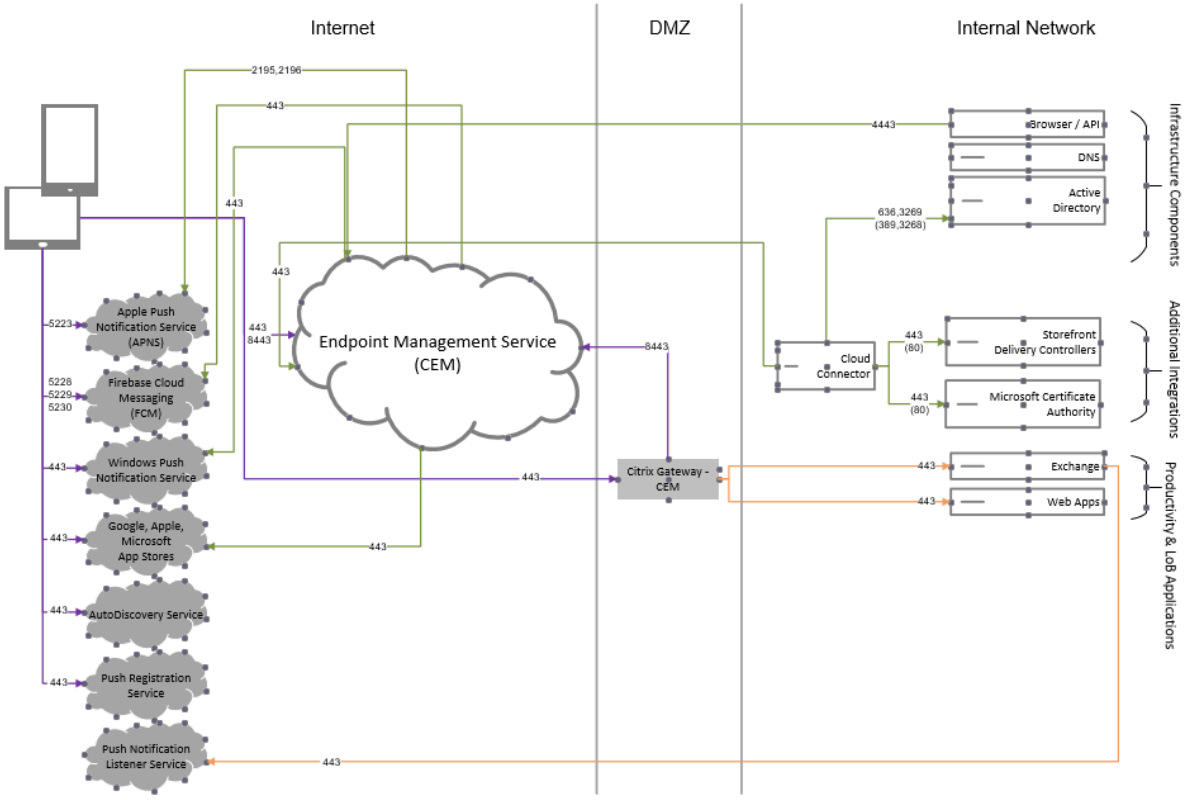
ファイアウォールポート

- Citrix Endpoint Management のポート 443 を`fcm.googleapis.com`および`Google.com`に開きます。
- デバイスの Wi-Fi によるインターネット送信接続用にポート 5228、5229、5230 を開きます。
- 送信接続を許可するには、IP 制限なしでポート 5228～5230 を許可リストに追加することをお勧めします。ただし、IP 制限が必要な場合は、IPv4 および IPv6 ブロック内のすべての IP アドレスを許可リストに追加することをお勧めします。ブロックは、Google のASN 15169に記載されています。このリストは、毎月更新してください。

詳しくは、「ポート要件」を参照してください。

アーキテクチャ

次の図は、外部および内部ネットワークにおける FCM の通信フローを示しています。

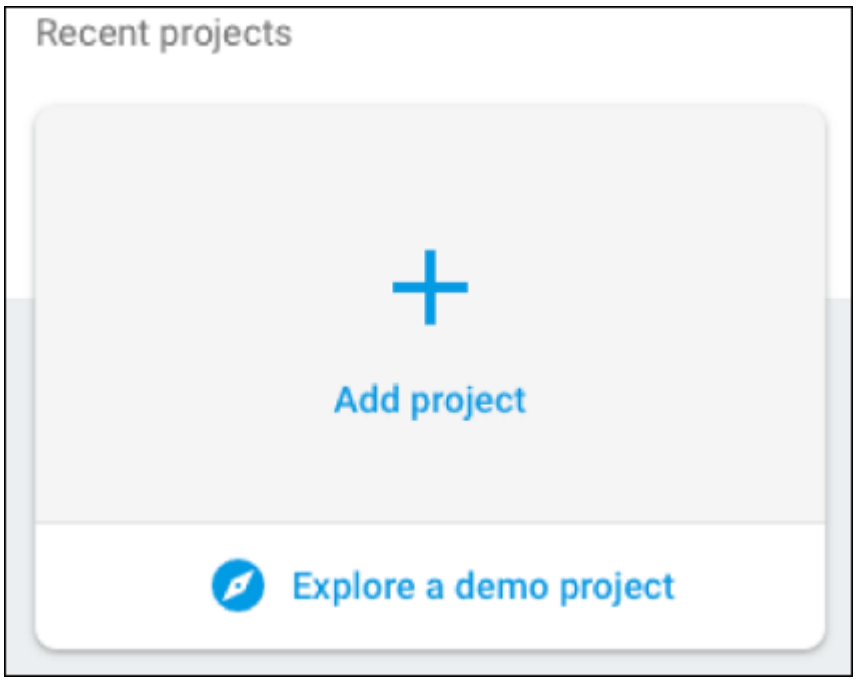


Google アカウントを **FCM** 向けに構成するには

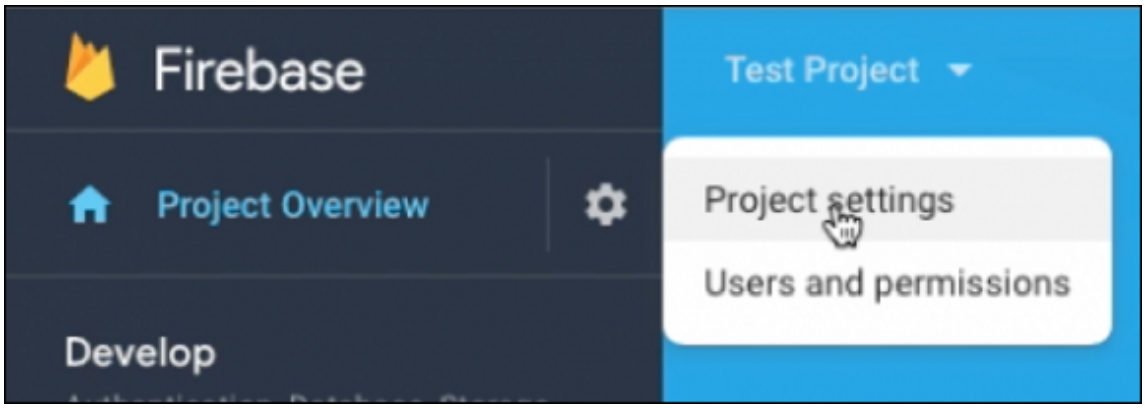
1. Google デベロッパーアカウントの資格情報を使用して次の URL にサインインします:

   https://console.firebase.google.com/

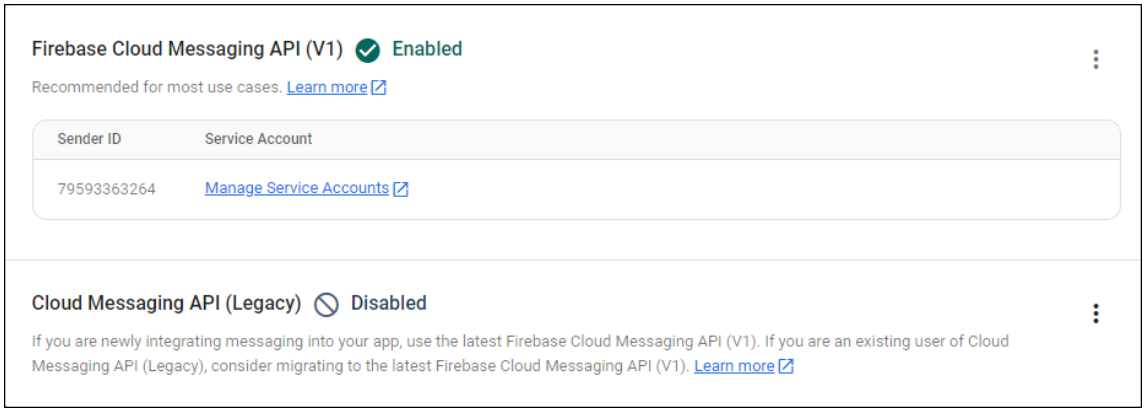
2. [**Add project**] をクリックします。



3. プロジェクトを作成したら、[**Project settings**]をクリックします。



4. [**Cloud Messaging**]タブを選択します。Firebase Cloud Messaging API が有効になっていることを確認し、[**Manage Service Accounts**]をクリックします。



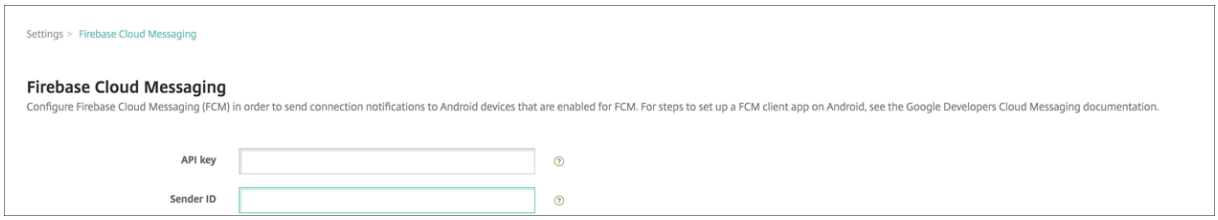
5. [**Key**] フィールドと [**OAuth 2 Client ID**] フィールドの値をコピーします。キーが一覧にない場合は、[**Actions**] の下の省略記号（…）をクリックして、新しいキーを追加します。

Android 上で FCM のクライアントアプリをセットアップする手順については、この Google Developers の Cloud Messaging の記事を参照してください：https://firebase.google.com/docs/cloud-messaging/android/client。

Citrix Endpoint Management を **FCM** 用に構成するには

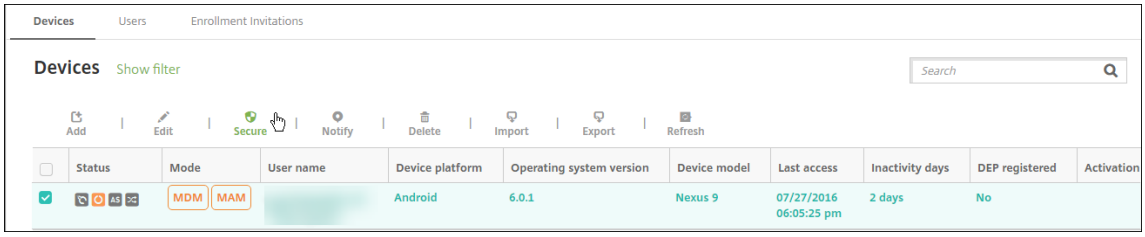
Citrix Endpoint Management コンソールで、[設定] > [**Firebase Cloud Messaging**] の順に選択します。

- [**API** キー] を編集して、Firebase Cloud Messaging 構成の最後の手順でコピーした Firebase Cloud Messaging の **Key** 値を入力します。
- [送信者 **ID**] を編集して、前の手続きでコピーした **OAuth 2 Client ID** 値を入力します。

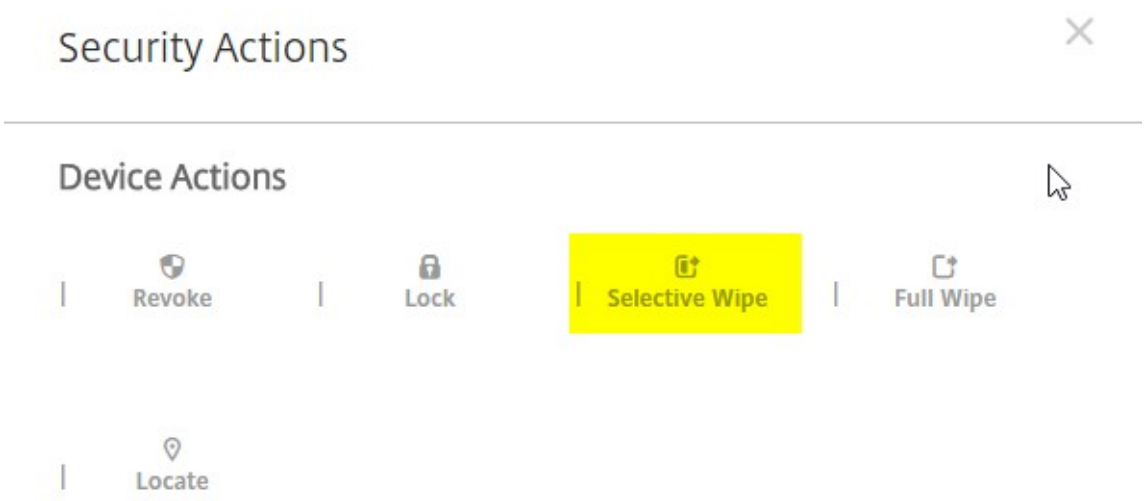


構成をテストするには

1. Android デバイスを登録します。
2. このデバイスを Citrix Endpoint Management から切断するため、少しの時間アイドル状態にします。
3. Citrix Endpoint Management コンソールで [管理] をクリックし、Android デバイスを選択して [保護] をクリックします。



4. [デバイス操作] で、[選択的なワイプ] をクリックします。



正常に構成されている場合、Endpoint Management に再接続せずにデバイスで選択的なワイプが行われます。

Android SafetyNet

November 29, 2023

Android SafetyNet 機能を使用して、Citrix 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設定できます。Android SafetyNet は、MAM 展開では使用できません。

この機能を有効にすると、SafetyNet Attestation API はデバイスのソフトウェアとハードウェアの情報を調査し、そのデバイスのプロファイルを作成します。次に、Android 互換性テストをパスしたデバイスモデル一覧で、同じプロファイルがあるかを確認します。この情報は、Citrix Secure Hub が不明なソースによって変更されているかどうかを判断するためにも使用できます。

Android SafetyNet 機能が有効な場合、Citrix Secure Hub は SafetyNet Attestation API 要求を Google Play サービスに送信し、結果は Citrix Endpoint Management に報告されます。Citrix Endpoint Management は、この構成証明の結果でデバイス情報を更新します。この結果をデバイス上での操作をトリガーするために使用して、自動化された操作を設定できます。

SafetyNet Attestation API の機能について詳しくは、Android の開発者向けドキュメントを参照してください。

必要な **SafetyNet Attestation API** 要求の数を見積もる

以下の場合に、SafetyNet Attestation API 要求が送信されます:

- デバイスが Citrix Endpoint Management に登録済みである。

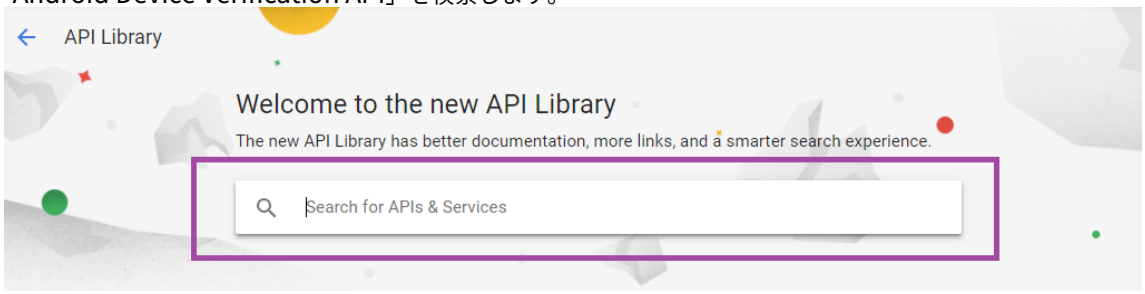
- Citrix Secure Hub のオンライン認証が発生した。サーバーセッションの有効期限が切れると、またはユーザーがサーバーからサインオフして再度サインオンすると、オンライン認証が発生します。Citrix Secure Hub は、ユーザーがサーバーで認証するために資格情報を提供するように求めます。
- デバイスが再起動された。
- 24 時間～1,000 時間の値で構成した定期的な時間間隔。

Citrix Endpoint Management 展開が 1 日あたり 10,000 を超える要求を送信する場合、この割り当てリクエストフォームに入力します。

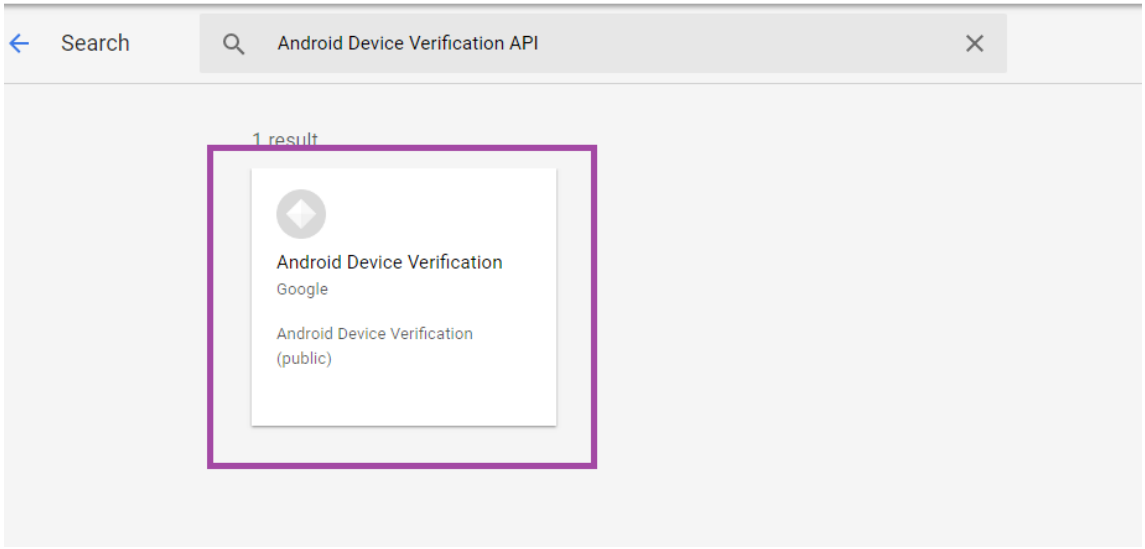
SafetyNet API キーを取得する

Citrix Endpoint Management で Android SafetyNet を有効にするには、SafetyNet API キーが必要です。

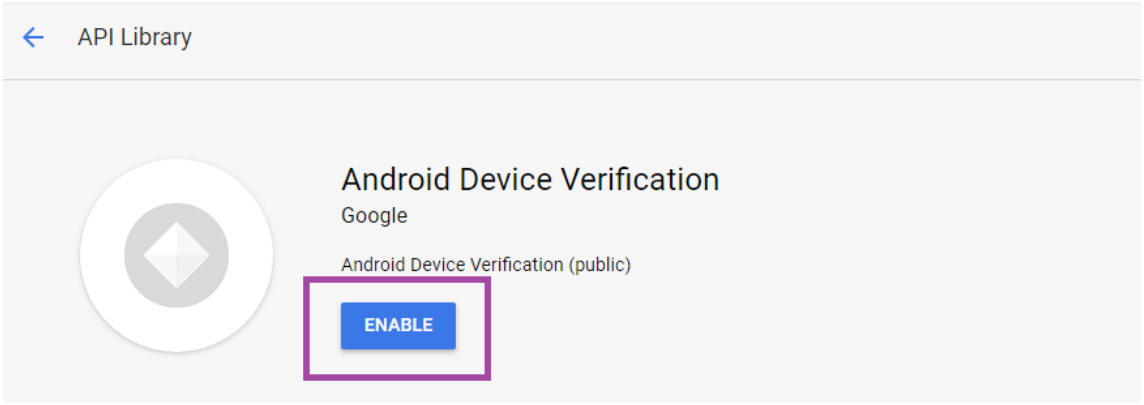
1. Google 管理者アカウントの資格情報を使用して Google API コンソールにログインします。
2. ライブラリページに移動します。
3. 「Android Device Verification API」を検索します。



4. **Android Device Verification API** をクリックします。

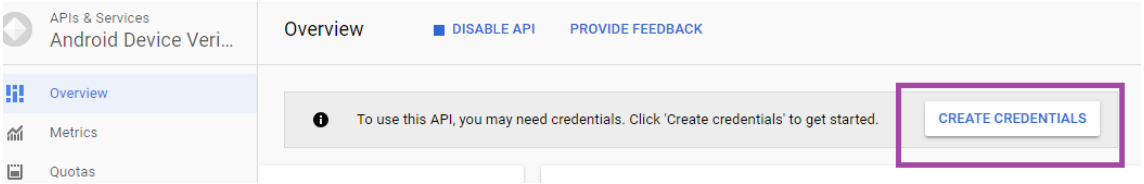


5. API がまだ有効になっていない場合は、［有効にする］をクリックします。

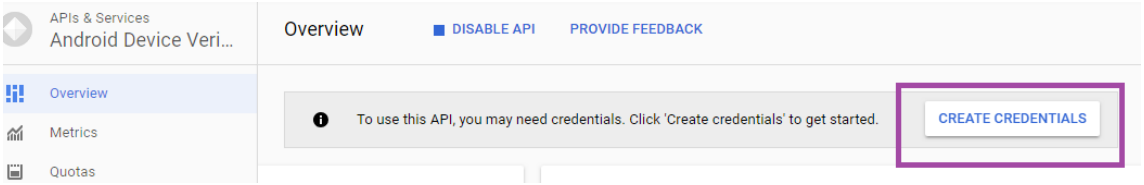


6. ［管理］をクリックします。

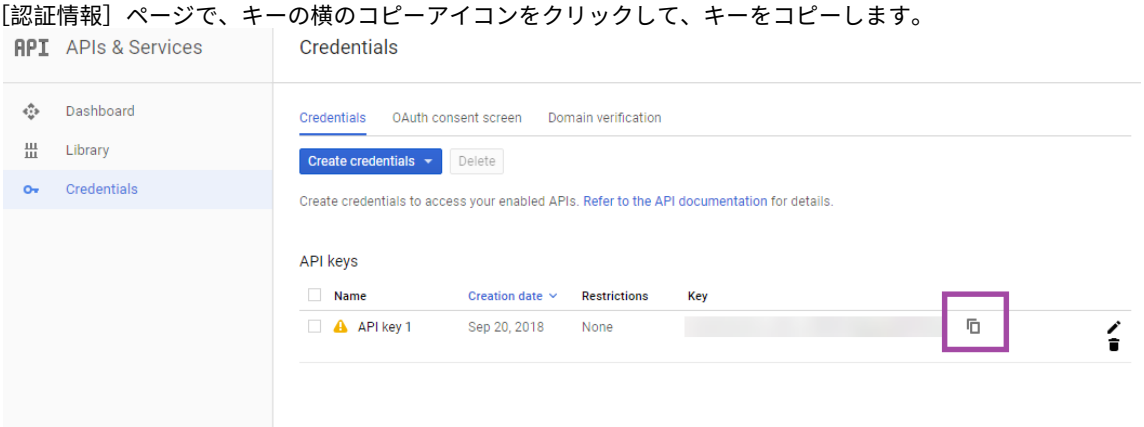
7. ［認証情報を作成］をクリックして API キーを生成します。



8. **Android Device Verification** を選択して **What credentials do I need** をクリックします。完了したら ［**Done**］をクリックします。



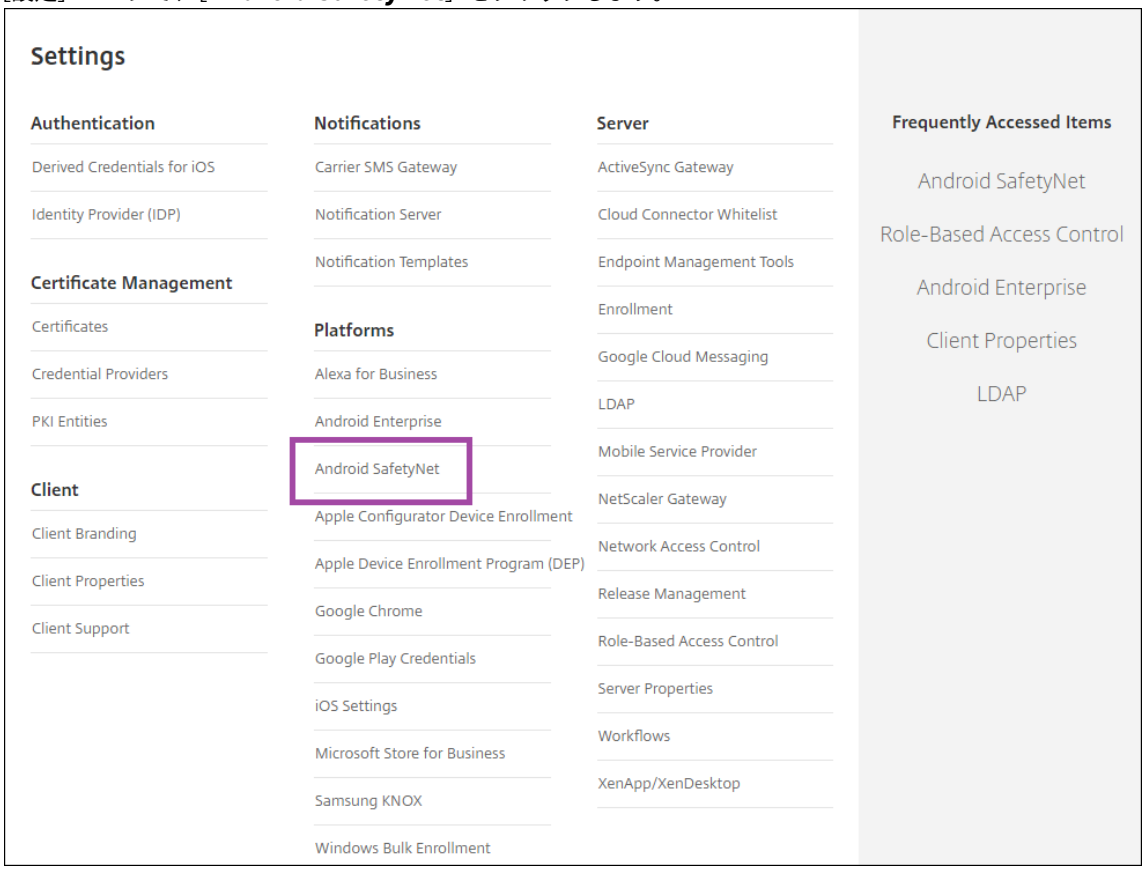
9. ［認証情報］ページで、キーの横のコピーアイコンをクリックして、キーをコピーします。



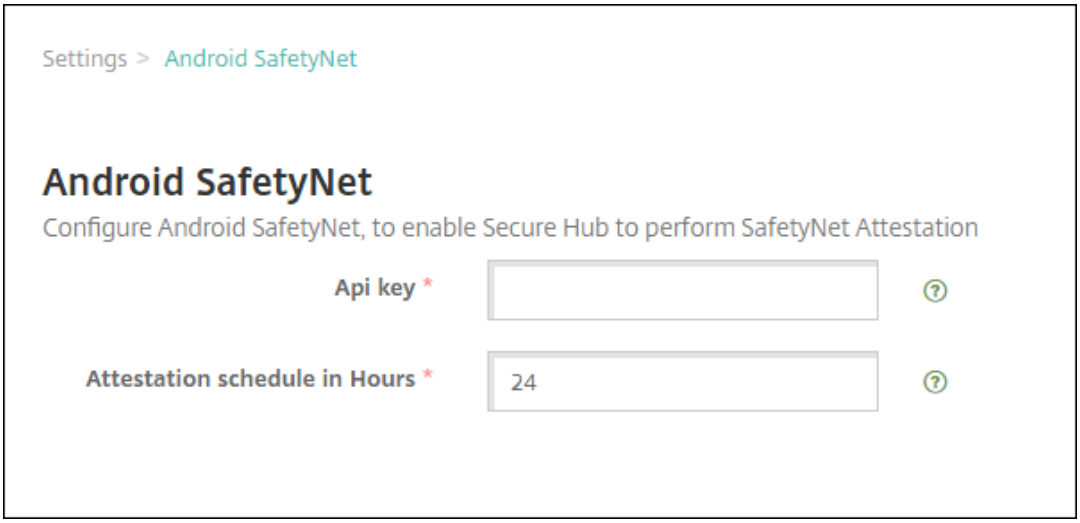
10. Android SafetyNet を有効にすると、キーを保存して Citrix Endpoint Management コンソールに貼り付けることができます。

Android SafetyNet を有効にする

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで、［**Android SafetyNet**］をクリックします。



3. 次の設定を構成します:
   - **API** キー。Google API コンソールから取得した SafetyNet API キーを貼り付けます。
   - 構成証明スケジュール（時間）。SafetyNet Attestation API が Android デバイスを評価する間隔を時間単位で指定します。最小値は 24 時間です。最大値は 1000 時間です。デフォルト値は 24 時間です。



4. ［保存］をクリックします。

Android SafetyNet の結果を表示する

デバイスの SafetyNet Attestation API 評価の結果を表示するには:

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］の順にクリックします。
2. Android デバイスを選択して SafetyNet Attestation API の結果を表示します。［詳細表示］をクリックします。
3. ［デバイスの詳細］ページで ［プロパティ］を選択します。
4. 結果は、［セキュリティ］セクションに表示されます。

SafetyNet Attestation API は、各デバイスの次の状態を返します。

- **SafetyNet CTS profile match**: この値が **True** の場合、デバイスには Android Compatibility Test Suite（CTS）をパスしたプロファイルのいずれかに一致するプロファイルがあります。この値が **False** の場合、デバイスには Android CTS をパスしたプロファイルと一致するプロファイルはありません。

- **SafetyNet basic integrity**: この値が **True** の場合、SafetyNet Attestation API は、デバイス上の Citrix Secure Hub が不明なソースによって変更されたという証拠を見つけることができませんでした。この値が **False** の場合、デバイス上の Citrix Secure Hub が不明なソースによって変更されています。
- **SafetyNet last known status**: デバイスで最後に認識されている SafetyNet の状態を以下のように表示します:
  - **Success**: SafetyNet Attestation API は、デバイス上の Citrix Secure Hub が不明なソースによって変更されたという証拠を見つけることができませんでした。
  - **LOCK_BOOTLOADER**: ユーザーはデバイスのブートローダーをロックする必要があります。デバイス上の Citrix Secure Hub が不明なソースによって変更されています。
  - **RESTORE_TO_FACTORY_ROM**: ユーザーはデバイスをクリーンな工場出荷時 ROM に復元する必要があります。デバイス上の Citrix Secure Hub が不明なソースによって変更されています。

Play Integrity API

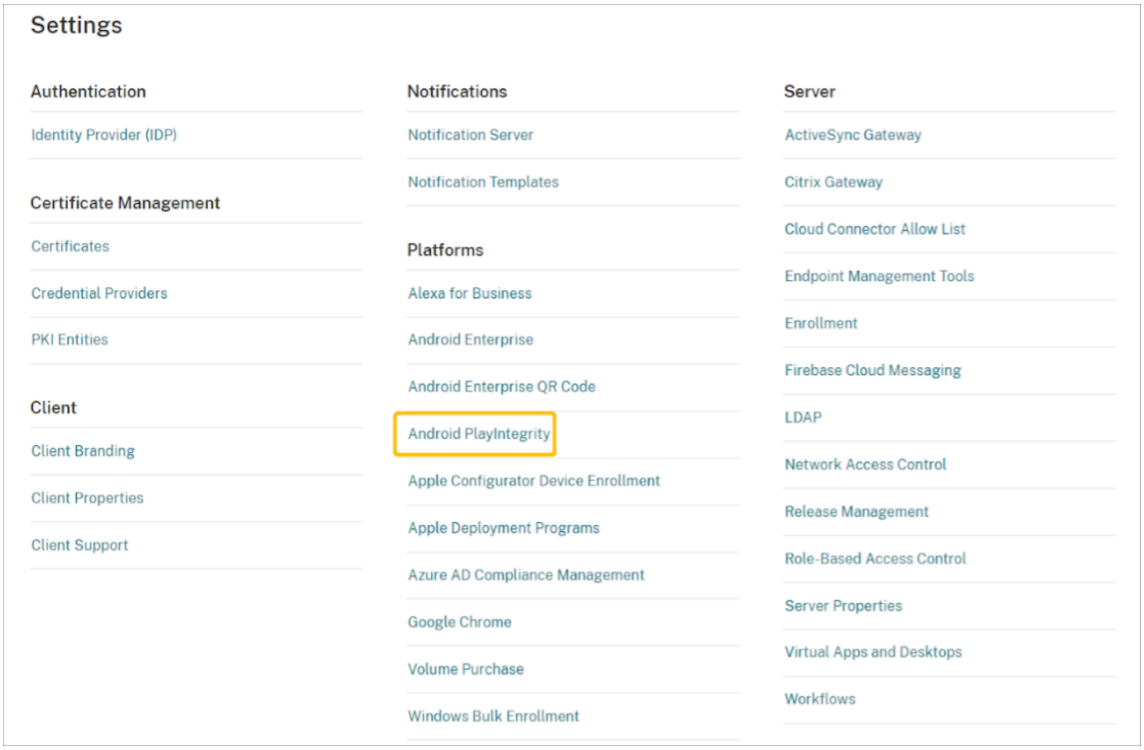
November 29, 2023

Play Integrity API は、不正行為や不正アクセスなど、潜在的にリスクの高い不正なやりとりからアプリやゲームを保護するのに役立ち、攻撃を防いだり不正使用を減らしたりするための適切な対応を取ることができます。詳しくは、「Play Integrity API」を参照してください。

Play Integrity API の有効化

Play Integrity API に切り替えるには、次の手順を実行します。

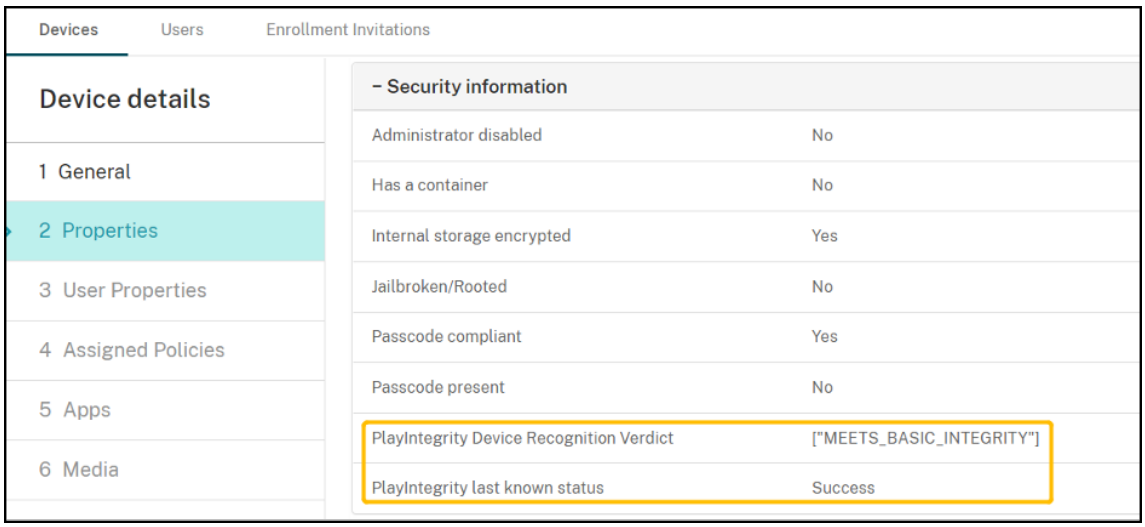
1. *afw.safetynet.attestation.api.* 廃止フィーチャーフラグを、指定した Citrix Endpoint Management サーバーに対して、オンにします。
2. Citrix Endpoint Management コンソールで、[**Android** の **Play Integrity**] を [設定] ページから選択します。



3. ［構成証明スケジュール（時間）］フィールドに値を入力します。これは、PlayIntegrity Attestation API がデバイスを評価する間隔の時間です。最小値は 24 時間で、最大値は 1000 時間です。デフォルト値は 24 時間です。［保存］をクリックします。
4. Citrix Secure Hub Android バージョン 23.7.0 へのアップグレードデバイスからサインオフし、Citrix Secure Hub にサインインして、Play Integrity API 経由で Attest をトリガーします。

Play Integrity API の構成証明による結果の表示と分析

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］に移動します。
2. Play Integrity API の構成証明の結果を表示するデバイスを選択します。［詳細を表示］をクリックします。
3. ［デバイス］タブで、［プロパティ］を選択します。結果が ［セキュリティ情報］セクションに表示されます。



4. Play Integrity API の構成証明は次のステータスを返します。

   - ［**Play Integrity** デバイスの認識判定］フィールドに「**MEETS_BASIC_INTEGRITY**」が含まれている場合、そのデバイス上で実行されている Citrix Secure Hub が少なくとも基本的なシステム整合性を満たしていることを意味します。
   - ［**Play Integrity** デバイスの認識判定］フィールドに「**MEETS_BASIC_INTEGRITY**」が含まれていない場合、そのデバイス上の Citrix Secure Hub は、認識できないバージョンの Android で実行されているか、ロック解除されているブートローダーがあるか、製造元によって認定されていない可能性があることを意味します。
   - ［**Play Integrity** の直前の既知の状態］が ［成功］の場合、PlayIntegrity API の構成証明が正常に実行されたことを意味します。
   - ［**Play Integrity** の直前の既知の状態］が ［失敗］の場合、PlayIntegrity API の構成証明の実行が失敗したことを意味します。

> 注:
>
> 管理者は、2023 年 11 月末の SafetyNet Attestation の最終ターンダウンの前に、SafetyNet の使用を許可するフィーチャーフラグをクリアできます。

制限事項

1. 新規登録された COSU デバイスと DO デバイスについては、適合しているデバイスであっても不適合と表示されます。

   Play Integrity API は、DO の登録中の最初の構成証明について空の値を返します。これにより、デバイスが不適合のように見えます。これは Google での既知の問題であり、この問題を修正するために DPC Support Lib 20230418 が公開されています。

   この修正は、23.9.0 リリースから利用可能です。それまでは以下の手順を回避策として使用できます。

- フィーチャーフラグをクリアし、引き続き SafetyNet API を使用して SafetyNet Attestation API の使用を継続します。
- サインオフして再びサインインし、登録後に構成証明をトリガーします。また、次回の定期的な構成証明を待つこともできます（デフォルトでは 24 時間ごとに行われます）。

この問題は登録中にのみ発生します。登録後、Play Integrity API は正常に機能します。

2. 新規登録された WPCOD デバイスは、適合している場合でも、不適合と表示されます。この問題は、Google によって確認中です。

Samsung

November 29, 2023

Samsung は、Citrix Endpoint Management と互換性のあるいくつかのソリューションを提供しています。

Android デバイスが Citrix Endpoint Management サービスに接続する方法とタイミングを制御するには、Firebase Cloud Messaging（FCM）を使用します。詳しくは、「Firebase Cloud Messaging」を参照してください。

登録プロファイルで、Android デバイスを MAM、MDM、または MDM+MAM のいずれで登録するか、およびユーザーが MDM をオプトアウトするオプションを決定します。Citrix Endpoint Management は、MDM+MAM で登録した Android デバイスに対して、次の種類の認証をサポートします。詳しくは、次の記事を参照してください：

- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- ID プロバイダー：
  - Citrix Cloud を介した Azure Active Directory での認証
  - Citrix Cloud を介した Okta での認証

使用頻度が少ない別の認証方法には、クライアント証明書とセキュリティトークンの組み合わせがあります。詳しくは、「https://support.citrix.com/article/CTX215200」を参照してください。

Android デバイスの管理を開始するための一般的なワークフローは次のとおりです：

1. オンボーディングプロセスの完了。「オンボードとリソースのセットアップ」と「デバイス登録およびリソース配信の準備」を参照してください。
2. 登録方法の選択と構成。「サポートされている登録方法」を参照してください。
3. Samsung ライセンスキーを展開します。
4. Samsung デバイスポリシーを構成します。
5. デバイスとアプリのセキュリティ操作の設定。「セキュリティ操作」を参照してください。

サポートされているオペレーティングシステムについては、「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。

サポートされている登録方法

次の表は、Android デバイスでサポートされている Citrix Endpoint Management での登録方法を示しています:

方法	サポート対象
手動登録	はい
登録招待	はい

デバイスの登録について詳しくは、「Android デバイスの登録」を参照してください。

Samsung ライセンスキーの展開

Samsung には Enterprise License Management（ELM）キーがあります。Samsung ライセンスは、Samsung から購入します。

Samsung デバイスポリシーの構成

デバイスポリシー:

[アプリ制限](/en-us/citrix-endpoint-management/policies/app-restrictions-policy.html)	[アプリのアンインストール](/ja-jp/citrix-endpoint-management/policies/app-uninstall-policy.html)	[ブラウザー](/ja-jp/citrix-endpoint-management/policies/browser-policy.html)
[Samsung コンテナへのアプリのコピー](/ja-jp/citrix-endpoint-management/policies/copy-apps-to-samsung-container-policy.html)	[Exchange](/ja-jp/citrix-endpoint-management/policies/exchange-policy.html)	[パスコード](/ja-jp/citrix-endpoint-management/policies/passcode-policy.html)
制限	VPN

セキュリティ操作

Android は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

アプリのロック	アプリのワイプ	証明書の書き換え
完全なワイプ	検索	ロック
パスワードのロックとリセット	Notify	取り消し
選択的なワイプ		

> 注:
>
> Android 6.0 以降を実行するデバイスの場合、検索セキュリティ操作には、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しないことを選択できます。登録時にユーザーによって権限が付与されないと、Citrix Endpoint Management は検索コマンドの送信時に再度検索の権限を要求します。

ネットワークアクセス制御

March 15, 2024

ネットワークアクセス制御（NAC）ソリューションを使用して、Android デバイスおよび Apple デバイスの Citrix Endpoint Management デバイスのセキュリティ評価を拡張できます。NAC ソリューションは Citrix Endpoint Management のセキュリティ評価を使用して、認証の決定を効率的に処理します。Citrix Endpoint Management で構成するデバイスポリシーと NAC フィルターは、NAC アプライアンスを構成した後に適用されます。

Citrix Endpoint Management を NAC ソリューションと組み合わせると、ネットワーク内部のデバイスに対する QoS を向上させ、よりきめ細かい制御を行うことができます。NAC と Citrix Endpoint Management を統合する利点の概要については、「アクセス制御」を参照してください。

Citrix では Citrix Endpoint Management と統合するための以下のソリューションをサポートしています:

- Citrix Gateway
- ForeScout

他の NAC ソリューションとの統合は保証されていません。

ネットワーク内の NAC アプライアンスを使用する場合:

- Citrix Endpoint Management では、iOS、Android Enterprise、および Android デバイスのエンドポイントセキュリティ機能として NAC がサポートされています。
- Citrix Endpoint Management でフィルターを有効にして、規則またはプロパティに基づいてデバイスを NAC の準拠または非準拠として設定できます。例:

- Citrix Endpoint Management の管理対象デバイスが指定された条件を満たしていない場合、デバイスは［非準拠］としてマークされます。NAC アプライアンスは、ネットワーク上で非準拠デバイスをブロックします。
- Citrix Endpoint Management 管理対象デバイスに非準拠のアプリがインストールされている場合、NAC フィルターで VPN 接続をブロックできます。その結果、準拠していないユーザーデバイスは、VPN 経由でアプリや Web サイトにアクセスできなくなります。
- NAC 用の Citrix Gateway を使用する場合は、分割トンネリングを有効にして、Citrix Gateway プラグインが Citrix Gateway に不要なネットワークトラフィックを送信しないようにすることができます。分割トンネリングについて詳しくは、「分割トンネリングの構成」を参照してください。

サポートされる **NAC** 準拠フィルター

Citrix Endpoint Management では、次の NAC 準拠フィルターがサポートされます：

匿名デバイス：デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときに Citrix Endpoint Management がユーザーを再認証できない場合に使用できます。

禁止アプリ：デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。このポリシーについて詳しくは、「アプリアクセスデバイスポリシー」を参照してください。

非アクティブデバイス：［サーバープロパティ］で デバイスの［非アクティブな日数のしきい値］で定義された期間、非アクティブであったかを確認します。詳しくは、「サーバープロパティ」を参照してください。

不足必須アプリ：デバイスにアプリアクセスポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ：デバイスにアプリアクセスポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード：ユーザーパスワードが正しいかを確認します。iOS デバイスおよび Android デバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかを Citrix Endpoint Management が確認できます。たとえば、iOS では、Citrix Endpoint Management がデバイスにパスコードポリシーを送信する場合、ユーザーは 60 分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス違反かどうかを確認します。通常、このプロパティは自動化された操作により変更されるか、Citrix Endpoint Management API を利用するサードパーティにより変更されます。

失効状態：デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

ルート化された **Android** およびジェイルブレイクした **iOS** デバイス： Android または iOS デバイスがジェイルブレイクされていないかを確認します。

非管理デバイス： Citrix Endpoint Management がデバイスを管理しているかどうかを確認します。たとえば、MAM で登録されているデバイスや未登録のデバイスは管理されていません。

> 注:
>
> ［暗黙的な準拠/非準拠］または［非準拠］フィルターは、Citrix Endpoint Management が管理しているデバイスでのみデフォルト値を設定します。たとえば、禁止されたアプリがインストールされている、または登録されていないデバイスは、非準拠としてマークされます。NAC アプライアンスは、これらのデバイスをネットワークからブロックします。

構成の概要

NAC コンポーネントは、リストされた順序で構成することを推奨します。

1. NAC をサポートするデバイスポリシーを構成します:

   iOS デバイスの場合:「NAC をサポートするように VPN デバイスポリシーを構成する」を参照してください。

   Android Enterprise デバイスの場合:「Citrix SSO に対する Android Enterprise 管理対象の構成の作成」を参照してください。

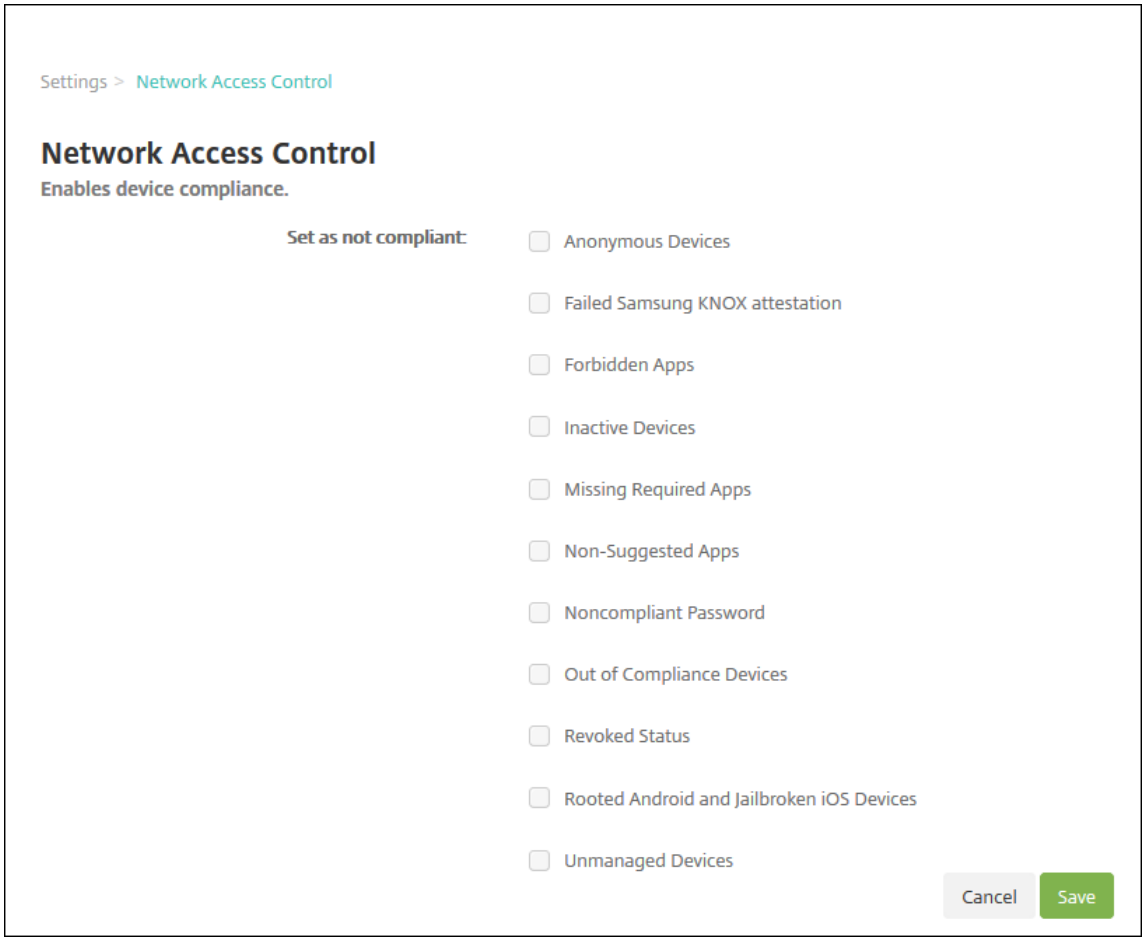
   Android デバイスの場合:「Android 向け Citrix SSO プロトコルを構成する」を参照してください。
2. Citrix Endpoint Management で NAC フィルターを有効にします。
3. NAC ソリューションを構成します:

   - Citrix Gateway。詳細は「NAC をサポートするように Citrix Gateway ポリシーを更新する」を参照してください。

     デバイスに Citrix SSO をインストールする必要があります。「Citrix Gateway クライアント」を参照してください。
   - ForeScout: ForeScout のドキュメントを参照してください。

Citrix Endpoint Management で **NAC** フィルターを有効にする

1. Citrix Endpoint Management コンソールで、［設定］**>**［ネットワークアクセス制御］に移動します。



2. 有効にする ［非準拠として設定］フィルターのチェックボックスをオンにします。
3. ［保存］をクリックします。

NAC をサポートするように Citrix Gateway ポリシーを更新する

VPN 仮想サーバーでは、（クラシックではない）高度な認証ポリシーと VPN セッションポリシーを構成する必要があります。

これらの手順では、次のいずれかの特性を利用して Citrix Gateway を更新します:

- Citrix Endpoint Management と統合されている。
- Citrix Endpoint Management 環境の一部ではなく VPN に設定されており、Citrix Endpoint Management に到達できる。

仮想 VPN サーバー上のコンソールウィンドウで、次の操作を行います。コマンドと例で使用されている FQDN と IP アドレスは架空のものです。

1. VPN 仮想サーバーでクラシックポリシーを使用している場合は、すべてのクラシックポリシーを削除してバインド解除します。クラシックポリシーを確認するには、以下のように入力します:


```
show vpn vserver <VPN_VServer>
```

Classic という単語が含まれている結果をすべて削除します。たとえば、次のようになります: VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0

ポリシーを削除するには、以下のように入力します。

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 以下のように入力して、対応する詳細セッションポリシーを作成します。

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

たとえば、次のようになります: add vpn sessionPolicy vpn_nac **true** AC_OS_10.10.1.1_A_

3. 以下のように入力して、ポリシーを VPN 仮想サーバーにバインドします。

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority
 100
```

4. 以下のように入力して、認証仮想サーバーを作成します。

```
add authentication vserver <authentication vserver name> <service
 type> <ip address>
```

例: add authentication vserver authvs SSL 0.0.0.0
この例では、0.0.0.0は認証仮想サーバーが公開されていないことを示します。

5. 以下のように入力して、SSL 証明書を仮想サーバーにバインドします。

```
bind ssl vserver <authentication vserver name> -certkeyName <
Webserver certificate>
```

たとえば、次のようになります: bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY

6. VPN 仮想サーバーの認証プロファイルを認証仮想サーバーに関連付けます。最初に、以下のように入力して認証プロファイルを作成します。

```
add authentication authnProfile <profile name> -authnVsName <
authentication vserver name>
```

例:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 以下のように入力して、認証プロファイルを VPN 仮想サーバーに関連付けます。

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile
name>
```

例:


```
set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
```

8. 以下のように入力して、Citrix Gateway からデバイスへの接続を確認します。

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/
   Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<
   device_id>"
   ```

   たとえば、このクエリは、環境に登録されている最初のデバイス（deviceid_1）の準拠ステータスを取得して接続を検証します：

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header
    "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   成功した結果は、次の例のようになります。

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. 前の手順が成功したら、Citrix Endpoint Management への Web 認証アクションを作成します。まず、iOS VPN プラグインからデバイス ID を抽出するポリシー式を作成します。次のように入力します。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY
   (10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 以下のように入力して、Citrix Endpoint Management に要求を送信します。この例では、Citrix Endpoint Management の IP アドレスは10.207.87.82、FQDN はexample.em.cloud.com:4443です。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -
    serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP
    /1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-
    Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https
     -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-
    Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    Citrix Endpoint Management NAC の正常な応答は、HTTP status 200 OKです。X-Citrix-Device-Stateヘッダーには、Compliantの値が必要です。

11. 以下のように入力して、アクションを関連付ける認証ポリシーを作成します。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
     authentication action>
    ```

    たとえば、次のようになります：add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac

12. 以下のように入力して、既存の LDAP ポリシーを拡張ポリシーに変換します。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <
    LDAP action name>
    ```

    たとえば、次のようになります: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 以下のように入力して、LDAP ポリシーを関連付けるポリシーラベルを追加します。

    ```
    add authentication policylabel <policy_label_name>
    ```

    たとえば、次のようになります: `add authentication policylabel ldap_pol_label`

14. 以下のように入力して、LDAP ポリシーをポリシーラベルに関連付けます。

    ```
    bind authentication policylabel ldap_pol_label -policyName
    ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. 準拠デバイスを接続して NAC テストを実行し、LDAP 認証が正常に行われたことを確認します。次のように入力します。

    ```
    bind authentication vserver <authentication vserver> -policy <web
     authentication policy> -priority 100 -nextFactor <ldap policy
    label> -gotoPriorityExpression END
    ```

16. 認証仮想サーバーに関連付ける UI を追加します。次のコマンドを入力してデバイス ID を取得します。

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule>
    -action lschema_single_factor_deviceid
    ```

17. 以下のように入力して、認証仮想サーバーをバインドします。

    ```
    bind authentication vserver authvs -policy lschema_xm_nac_pol -
    priority 100 -gotoPriorityExpression END
    ```

18. Citrix Secure Hub 接続を有効にする LDAP 拡張認証ポリシーを作成します。次のように入力します。

    ```
    add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
    (\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
    ```

    ```
    bind authentication vserver authvs -policy ldap_xm_test_pol -
    priority 110 -gotoPriorityExpression NEXT
    ```

iOS

November 29, 2023

Citrix Endpoint Management で iOS デバイスを管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書を設定します。詳しくは、「APN 証明書」を参照してください。

登録プロファイルで、iOS デバイスを MDM+MAM で登録するかどうか、およびユーザーがモバイルデバイス管理（MDM：Mobile Device Management）をオプトアウトするオプションを決定します。Citrix Endpoint Management は、MDM+MAM の iOS デバイスに対して、次の種類の認証をサポートします。詳しくは、次の記事を参照してください：

- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- ID プロバイダー：
  - Citrix Cloud を介した Azure Active Directory での認証
  - Citrix Cloud を介した Okta での認証

> **iOS 13** での信頼された証明書の要件：
>
> Apple では、TLS サーバー証明書の新しい要件を設定しています。すべての証明書が新しい Apple の要件に準拠していることを確認します。アップルの出版物である「https://support.apple.com/en-us/HT210176」を参照してください。証明書の管理については、「証明書のアップロード」を参照してください。

iOS デバイスの管理を開始するための一般的なワークフローは次のとおりです：

1. オンボーディングプロセスの完了。「オンボードとリソースのセットアップ」と「デバイス登録およびリソース配信の準備」を参照してください。
2. 登録方法の選択と構成。「サポートされている登録方法」を参照してください。
3. iOS デバイスポリシーの構成。
4. iOS デバイスの登録。
5. デバイスとアプリのセキュリティ操作の設定。「セキュリティ操作」を参照してください。

サポートされているオペレーティングシステムについては、「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。

iOS 14 との互換性

Citrix Endpoint Management と Citrix モバイルアプリは iOS 14 と互換性がありますが、現在 iOS 14 の新機能をサポートしていません。

監視対象の iOS デバイスの場合、ソフトウェアのアップグレードを最大 90 日間延期できます。iOS の制限デバイスポリシーで、次の設定を使用します：

- ソフトウェア更新の強制延期
- ソフトウェア更新の強制延期

「iOS の設定」を参照してください。これらの設定は、ユーザー登録モードまたは監視対象外（完全 MDM）モードのデバイスでは使用できません。

開いたままにする必要がある **Apple** のホスト名

iOS、macOS、Apple App Store を正しく動作させるには、一部の Apple ホスト名を開いたままにしておく必要があります。これらのホスト名をブロックすると、インストール、更新、および以下の適切な操作に影響が出る可能性があります：iOS、iOS アプリ、MDM の操作およびデバイスとアプリの登録詳しくは、https://support.apple.com/en-us/HT201999を参照してください。

サポートされている登録方法

登録プロファイルで iOS デバイスの管理方法を指定します。次の登録設定から選択できます：

- **Apple** ユーザー登録： BYOD（Bring Your Own Device）デバイスの場合、個人データのプライバシーと企業データのセキュリティのバランスをとることができます。この登録モードは、公開プレビューとして使用できます。この機能を有効にするには、サポートチームにお問い合わせください。
- **Apple** デバイスの登録：監視対象の iOS デバイスの場合、デバイスに個人プロファイルと企業プロファイルがあります。
- デバイスを管理しない：アプリのみを管理する場合は、これらのデバイスを MDM から除外します。

登録プロファイルの作成について詳しくは、「登録プロファイル」を参照してください。

Citrix Endpoint Management は、iOS デバイスについて次の登録方法をサポートしています：

方法	サポート対象
Apple Business Manager	はい
Apple School Manager	はい
Apple Configurator	はい
手動登録	はい
登録招待	はい

Apple Deployment Programs には、企業組織向けの Apple Business Manager（ABM）と、教育機関向けの Apple School Manager（ASM）が含まれます。詳しくは、「Apple Deployment Programs でのデバイスの展開」を参照してください。

Apple School Manager は、教育向け Apple Deployment Program の一種です。「Apple Education 機能との統合」を参照してください。

Apple Deployment Programs を使用して、iOS、iPadOS、macOS デバイスを一括登録することができます。これらのデバイスは、Apple から直接購入するか、Apple 正規販売代理店、または通信事業者から購入することができます。Apple から直接購入したかどうかにかかわらず Apple Configurator を使用して iOS デバイスを登録できます。「Apple デバイスの一括登録」を参照してください。

管理対象 **Apple ID**

ユーザー登録は、管理対象 Apple ID と緊密に統合されています。ABM/ASM を使用して手作業で、または Azure Active Directory（AAD）で動的に、管理対象 Apple ID を作成できます。

非フェデレーション認証の場合、ABM/ASM を使用して管理対象 Apple ID を作成し、アカウントを追加します。ABM/ASM でのアカウントの追加については、`https://support.apple.com/guide/apple-business-manager/welcome/web`にある Apple のドキュメント、および`https://support.apple.com/guide/apple-school-manager/welcome/web`にある ASM を参照してください。ユーザー登録の際、余分な手順を回避するために、次のことをお勧めします:

- 管理対象 Apple ID を作成するときは、会社のメールアドレスと一致するメールを使用してください。
- ユーザー役割を ［**Staff**］に設定します。
- 登録する前に、ユーザーに手作業でパスワードを変更してもらいます。企業アカウントと同じパスワードを使用することが推奨されることをユーザーに知らせます。

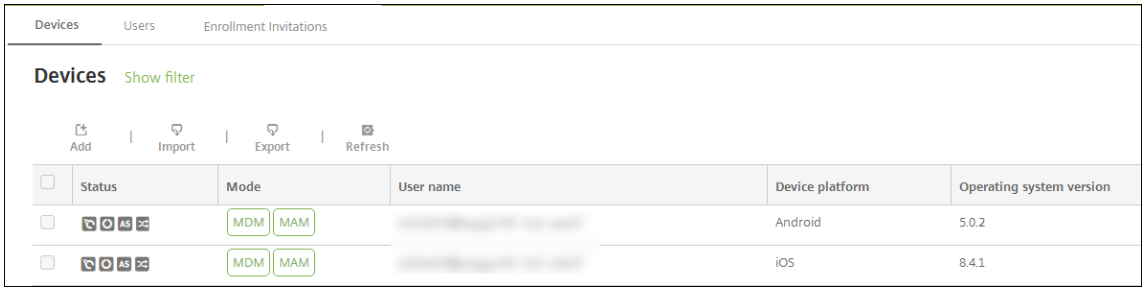
管理対象 Apple ID を動的に作成するには、ID プロバイダーとして AAD を使用するように Citrix Cloud を構成します。AAD を使用するように Citrix Cloud を構成する方法について詳しくは、「Citrix Cloud を介した Azure Active Directory での認証」を参照してください。また、ABM/ASM でフェデレーション認証を構成してください。ABM または ASM でフェデレーション認証を構成する方法について詳しくは、「Apple Business Manager ユーザーガイド」または「Apple School Manager ユーザーガイド」を参照してください。

管理対象 Apple ID を手作業で作成する場合、デフォルトのドメインの代わりに使用するカスタムドメインを構成できます。構成するカスタムドメインは、既存のドメインに置き換わります。たとえば、企業のメールアドレスは`first.last@company.com`という形式だが、代わりに管理対象 Apple ID のドメインとして`mycompany.website.com`という形式を使用したい場合です。ABM/ASM で管理対象 Apple ID を作成する場合、メールアドレスの形式は`first.last@mycompany.website.com`になります。

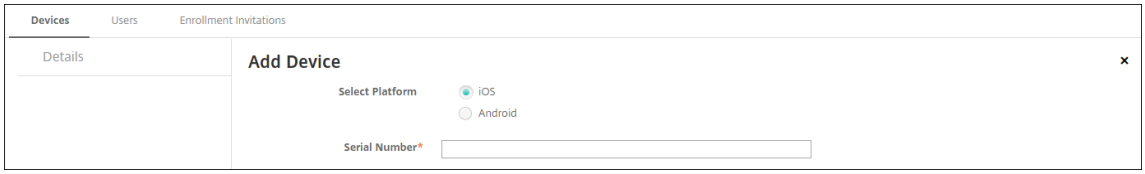
手動による **iOS** デバイスの追加

テスト目的など、iOS デバイスを手動で追加する場合は、次の手順に従います。

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］の順にクリックします。［デバイス］ページが開きます。



2. [追加] をクリックします。[デバイスの追加] ページが開きます。



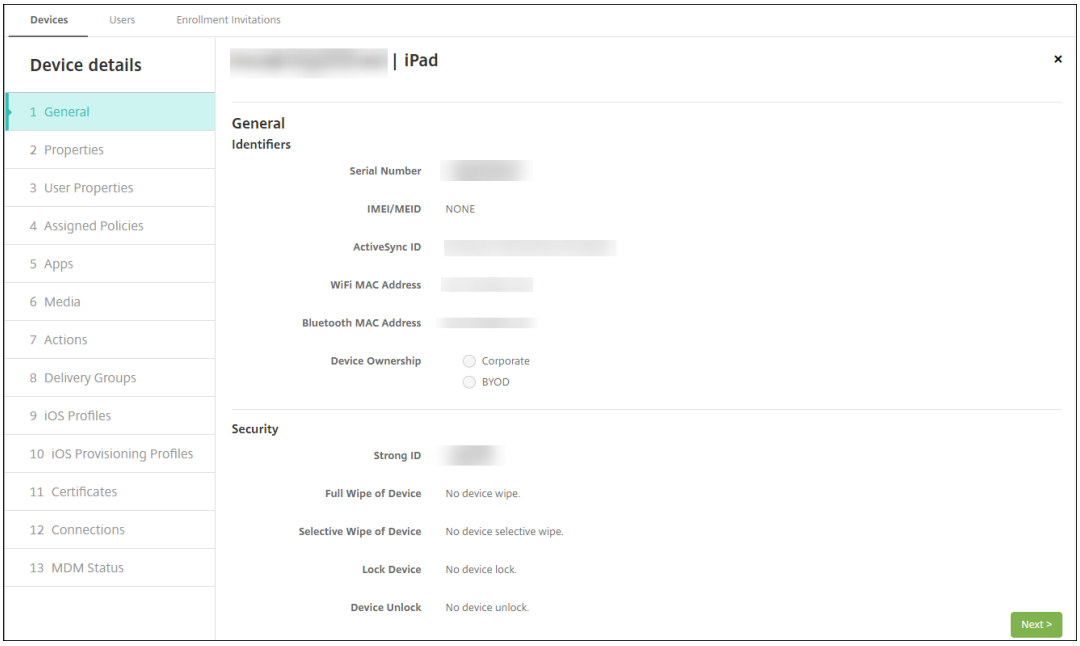
3. 次の設定を構成します:

   - プラットフォーム選択: [**iOS**] を選択します。
   - シリアル番号: デバイスのシリアル番号を入力します。

4. [追加] をクリックします。[デバイス] の表に示される一覧の一番下に、追加したデバイスが表示されます。デバイスの詳細を表示して確認するには: 追加したデバイスを選択して表示されるメニューで [編集] をクリックします。

   > 注:
   >
   > デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧の項目をクリックすると、その項目の右側にオプションメニューが表示されます。

   - 構成された LDAP
   - ローカルグループおよびローカルユーザーを使用する場合:
     - 1 つまたは複数のローカルグループ。
     - ローカルグループに割り当てられたローカルユーザー。
     - デリバリーグループはローカルグループと関連付けられます。
   - Active Directory を使用する場合:
     - デリバリーグループは Active Directory グループと関連付けられます。



5. ［一般］ページには、シリアル番号やプラットフォームの種類に関するその他の情報など、デバイスの識別子が表示されます。［デバイス所有権］で、［コーポレート］または ［**BYOD**］を選択します。

   ［一般］ページには、デバイスの ［セキュリティ］プロパティ（[Strong ID]、［デバイスのロック］、［アクティベーションロックバイパス］、プラットフォームの種類に関するその他の情報など）も表示されます。［デバイスの完全なワイプ］フィールドには、ユーザーの PIN コードが含まれます。デバイスがワイプされた後、ユーザーはこのコードを入力する必要があります。ユーザーがコードを忘れた場合は、こちらで確認できます。

6. ［プロパティ］ページには、Citrix Endpoint Management がプロビジョニングするデバイスのプロパティが表示されます。この一覧は、デバイスの追加に使用されるプロビジョニングファイルに含まれるデバイスのプロパティを表示します。プロパティを追加するには、［追加］をクリックして一覧からプロパティを選択します。各プロパティの有効な値に関しては、デバイスのプロパティ名と値に関する PDF を参照してください。

   プロパティを追加すると、最初に追加したカテゴリに表示されます。［次へ］をクリックして ［プロパティ］ページに戻ると、プロパティは適切な一覧に表示されます。

   プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の ［**X**］をクリックします。Citrix Endpoint Management デバイスによりその項目が削除されます。

7. 残りの ［デバイス詳細］セクションには、デバイスの概要が表示されます。

   - ユーザープロパティ：ユーザーの RBAC の役割、グループメンバーシップ、一括購入アカウント、およびプロパティを表示します。このページでインベントリから一括購入アカウントを削除できます。
   - 割り当て済みポリシー：展開済みのポリシー、保留中のポリシー、失敗したポリシーの数が表示されます。各ポリシーの名前、種類、最新展開の情報が表示されます。展開ステータスをリセットして保留にしたり、ユーザーが削除したポリシーを再展開したりできます。
   - アプリ：インストール済み、保留中、失敗のアプリ展開数を含む、最新のインベントリ時点のアプリ数が表示されます。アプリ名、ID、種類、その他の情報が表示されます。**HasUpdateAvailable** などの

iOS および macOS のインベントリキーの説明については、「モバイルデバイス管理（MDM）プロトコル」を参照してください。

- メディア：展開済み、保留中、失敗のメディア展開数を含む、最新のインベントリ時点のメディア数が表示されます。
- 操作：展開済み、保留中、失敗のアクション数を含む、アクション数が表示されます。最新展開のアクション名と時間が表示されます。
- デリバリーグループ：成功、保留中、失敗したデリバリーグループの数が表示されます。各展開のデリバリーグループ名と展開時間が表示されます。デリバリーグループを選択すると、状態、アクション、チャネル、またはユーザーなどの詳細な情報を表示できます。
- **iOS** プロファイル：名前、種類、組織、説明など、最新の iOS プロファイルインベントリが表示されます。
- **iOS** プロビジョニングプロファイル： UUID、有効期限、管理対象かどうかなど、エンタープライズ配布プロビジョニングプロファイルの情報を表示します。
- 証明書：有効な証明書と期限切れまたは失効した証明書が表示され、種類、プロバイダー、発行者、シリアル番号、期限切れまでの残日数などの情報も表示されます。
- 接続：最初の接続状態と最後の接続状態が表示されます。各接続のユーザー名、最後から 2 番目の認証時間、最後の認証時間が表示されます。
- **MDM** ステータス： MDM ステータス、最後のプッシュ時間、最後のデバイス応答時間などの情報が表示されます。

iOS デバイスポリシーの構成

デバイスポリシーを使用して、Citrix Endpoint Management と iOS または iPadOS を実行するデバイスとの通信に関する構成を行います。次の表は、iOS および iPadOS デバイスで使用可能なデバイスポリシーの一覧です：

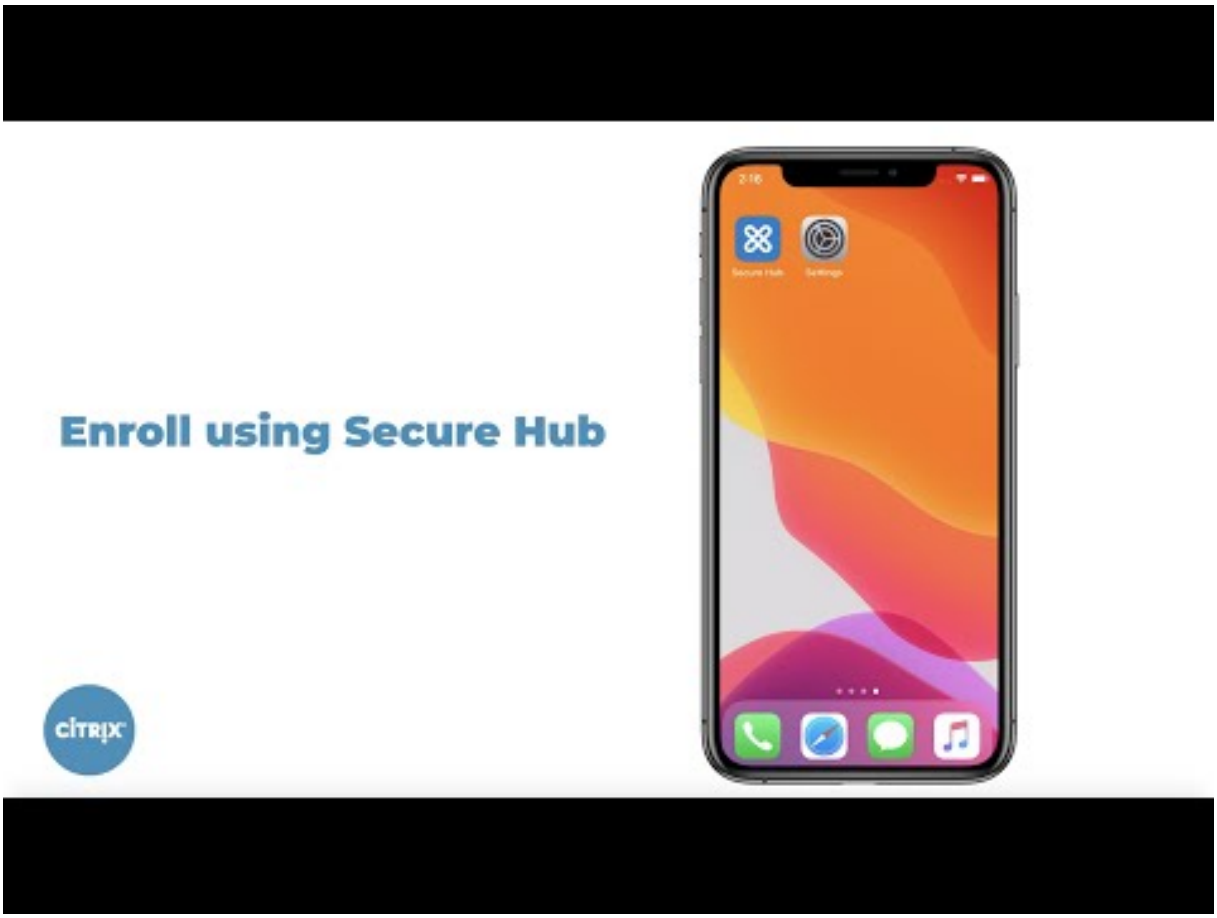
–	–	–
[AirPlay ミラーリング](/ja-jp/citrix-endpoint-management/policies/airplay-mirroring-ios-policy.html)	[AirPrint](/ja-jp/citrix-endpoint-management/policies/airprint-ios-policy.html)	[アクセスポイント名](/ja-jp/citrix-endpoint-management/policies/apn-policy.html#ios-settings)
[アプリアクセス](/ja-jp/citrix-endpoint-management/policies/app-access-policy.html)	[アプリ属性](/ja-jp/citrix-endpoint-management/policies/app-attributes-policy.html)	[アプリ構成](/ja-jp/citrix-endpoint-management/policies/app-configuration-policy.html#ios-settings)
[アプリインベントリ](/ja-jp/citrix-endpoint-management/policies/app-inventory-policy.html)	[アプリのロック](/ja-jp/citrix-endpoint-management/policies/app-lock-policy.html#ios-settings)	[アプリのアンインストール](/ja-jp/citrix-endpoint-management/policies/app-uninstall-policy.html#ios-and-macos-settings)
[アプリ通知](/ja-jp/citrix-endpoint-management/policies/apps-notifications-policy.html)	[Bluetooth](/ja-jp/citrix-endpoint-management/policies/bluetooth-policy.html)	[カレンダー（CalDAV）](/ja-jp/citrix-endpoint-management/policies/calendar-caldav-ios-policy.html)

|[携帯ネットワーク](/ja-jp/citrix-endpoint-management/policies/cellular-policy.html) |[連絡先（CardDAV）](/ja-jp/citrix-endpoint-management/policies/contacts-carddav-ios-policy.html) |[資格情報](/ja-jp/citrix-endpoint-management/policies/credentials-policy.html#ios-settings)
|[デバイス名](/ja-jp/citrix-endpoint-management/policies/device-name-policy.html) |[Education の構成](/ja-jp/citrix-endpoint-management/policies/education-configuration-policy.html) |[Exchange](/ja-jp/citrix-endpoint-management/policies/exchange-policy.html#ios-settings)
|[フォント](/ja-jp/citrix-endpoint-management/policies/font-policy.html) |[ホーム画面のレイアウト](/ja-jp/citrix-endpoint-management/policies/home-screen-layout-policy.html) |[iOS および macOS プロファイルのインポート](/ja-jp/citrix-endpoint-management/policies/import-ios-mac-os-x-profile-policy.html)
|[LDAP](/ja-jp/citrix-endpoint-management/policies/ldap-policy.html) |[位置情報](/ja-jp/citrix-endpoint-management/policies/location-policy.html) |[ロック画面のメッセージ](/ja-jp/citrix-endpoint-management/policies/lock-screen-message-policy.html)
|[メール](/ja-jp/citrix-endpoint-management/policies/mail-policy.html) |[管理対象ドメイン](/ja-jp/citrix-endpoint-management/policies/managed-domains-policy.html) |[最大常駐ユーザー数](/ja-jp/citrix-endpoint-management/policies/maximum-resident-users-policy.html)
|[MDM オプション](/ja-jp/citrix-endpoint-management/policies/mdm-options-policy.html) |[ネットワーク](/ja-jp/citrix-endpoint-management/policies/network-policy.html#ios-settings)|[ネットワーク使用状況](/ja-jp/citrix-endpoint-management/policies/network-usage-policy.html)
|[組織情報](/ja-jp/citrix-endpoint-management/policies/organization-info-policy.html) |[OS 更新](/ja-jp/citrix-endpoint-management/policies/control-os-updates.html#ios-settings) |[パスコード](/ja-jp/citrix-endpoint-management/policies/passcode-policy.html#ios-settings)
|[パスコードロックの猶予期間](/ja-jp/citrix-endpoint-management/policies/passcode-lock-grace-period.html) |[パーソナルホットスポット](/ja-jp/citrix-endpoint-management/policies/personal-hotspot-policy.html) |[プロファイルの削除](/ja-jp/citrix-endpoint-management/policies/profile-removal-policy.html)
|[プロビジョニングプロファイル](/ja-jp/citrix-endpoint-management/policies/provisioning-profile-policy.html) |[プロビジョニングプロファイルの削除](/ja-jp/citrix-endpoint-management/policies/provisioning-profile-removal-policy.html) |[プロキシ](/ja-jp/citrix-endpoint-management/policies/proxy-policy.html)
|[制限](/ja-jp/citrix-endpoint-management/policies/restrictions-policy.html#ios-settings) |[ローミング](/ja-jp/citrix-endpoint-management/policies/roaming-policy.html) |[SCEP](/ja-jp/citrix-endpoint-management/policies/scep-policy.html)
|[SSO アカウント](/ja-jp/citrix-endpoint-management/policies/sso-account-policy.html) |[ストア](/ja-jp/citrix-endpoint-management/policies/store-policy.html) |[サブスクライブされたカレンダー](/ja-jp/citrix-endpoint-management/policies/subscribed-calendars-policy.html)
|[使用条件](/ja-jp/citrix-endpoint-management/policies/terms-and-conditions-policy.html) |[VPN](/ja-jp/citrix-endpoint-management/policies/vpn-policy.html#ios-settings) |[壁紙](/ja-jp/citrix-endpoint-management/policies/wallpaper-policy.html)

|Web コンテンツフィルター |Web クリップ | | |

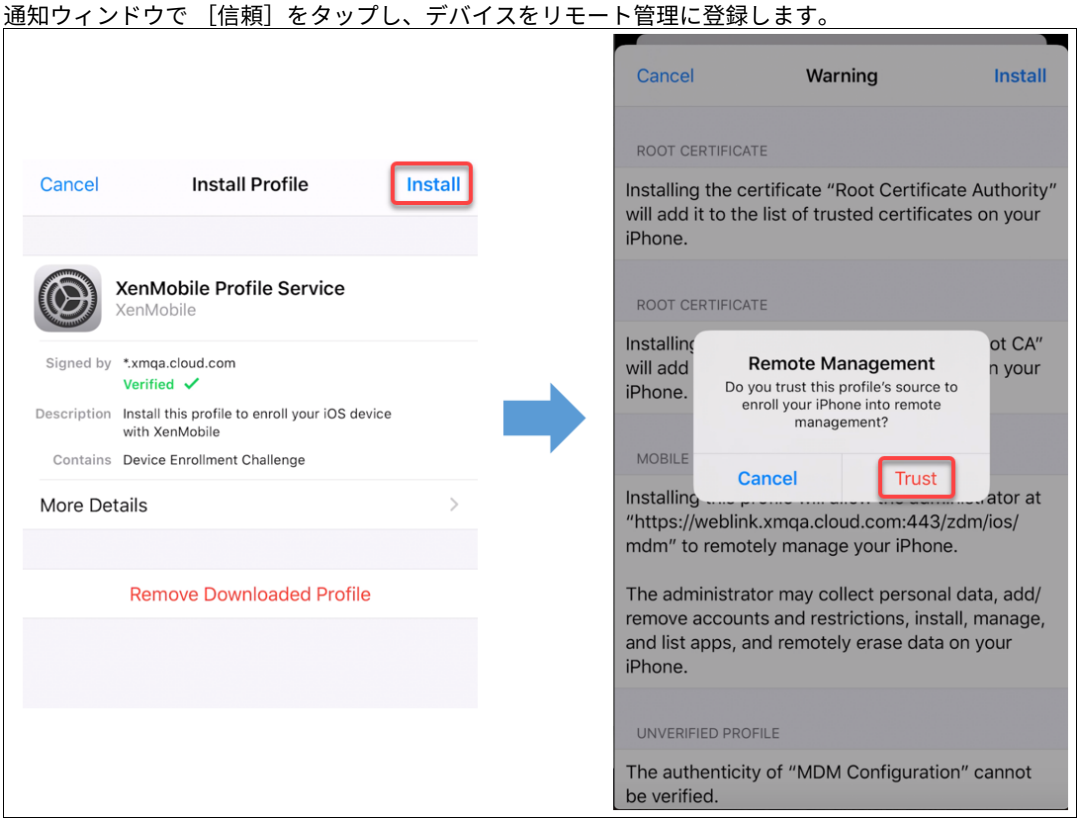
iOS デバイスの登録

このセクションでは、ユーザーが iOS デバイス（12.2 以降）を Citrix Endpoint Management に登録する方法について説明します。iOS の登録について詳しくは、次のビデオを確認してください:



1. iOS デバイスで Apple ストアにアクセスし、Citrix Secure Hub アプリをダウンロードしてタップします。
2. アプリをインストールするよう求められたら、［次へ］をタップし、［インストール］をタップします。
3. Citrix Secure Hub のインストールが完了したら、［開く］をタップします。
4. 会社の資格情報として、Citrix Endpoint Management サーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなどを入力します。入力後、［次へ］をクリックします。
5. ［はい、登録します］をタップし、iOS デバイスを登録します。
6. Citrix Endpoint Management が収集したデータの一覧が表示されます。　［次へ］をクリックします。組織でそのデータがどのように使用されるかについての説明が表示されます。［次へ］をクリックします。
7. 資格情報を入力し、プロンプトが表示されたら ［許可］をタップし、構成プロファイルをダウンロードします。構成プロファイルをダウンロードしたら、［閉じる］をタップします。
8. デバイス設定で、XenMobile プロファイルをインストールします。

- ［設定］**>**［全般］**>**［プロファイル］**>**［**XenMobile Profile Service**］に移動し、［インストール］をタップしてプロファイルを追加します。
- 通知ウィンドウで ［信頼］をタップし、デバイスをリモート管理に登録します。



9. 登録に成功すると、Citrix Secure Hub が開きます。MDM+MAM に登録する場合：認証情報を検証した後、プロンプトが表示されたら Citrix PIN を作成および確認します。
10. ワークフローの完了後、デバイスが登録されます。その後、アプリストアにアクセスし、iOS デバイスにインストールできるアプリを確認することができます。

セキュリティ操作

iOS のデバイス登録は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

- アクティベーションロックのバイパス
- アプリのロック
- アプリのワイプ
- ASM アクティベーションロック
- 証明書の書き換え
- 制限の削除
- 紛失モードを有効化/無効化
- 追跡を有効/無効にする

- 完全なワイプ
- 検索
- ロック
- 警報
- AirPlay ミラーリングの要求/停止
- 再起動/シャットダウン
- 取り消し/承認
- 選択的なワイプ
- ロック解除

iOS のユーザー登録は、次のセキュリティ操作をサポートしています:

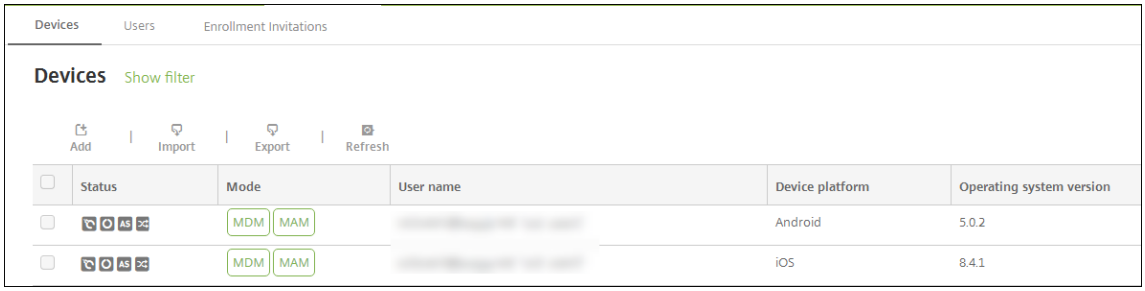
- 取り消し
- ロック
- 選択的なワイプ
- 証明書の書き換え

iOS デバイスのロック

iOS デバイスをロックし、デバイスのロック画面にメッセージと電話番号を表示することができます。

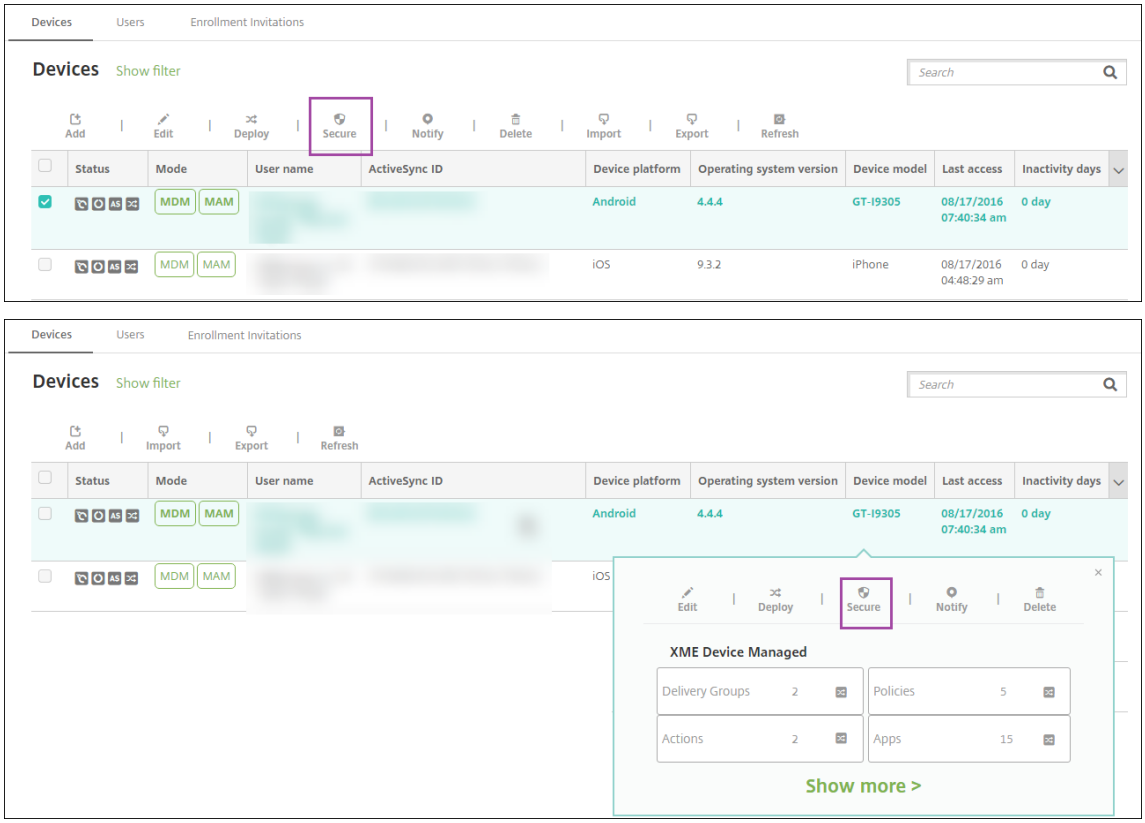
ロックされたデバイスでメッセージと電話番号を表示するには、Citrix Endpoint Management コンソールで［パスコード］ポリシーが **true** に設定されている必要があります。代わりに、ユーザーはデバイス上でパスコードを手動で有効化できます。

1. ［管理］**>**［デバイス］の順にクリックします。［デバイス］ページが開きます。

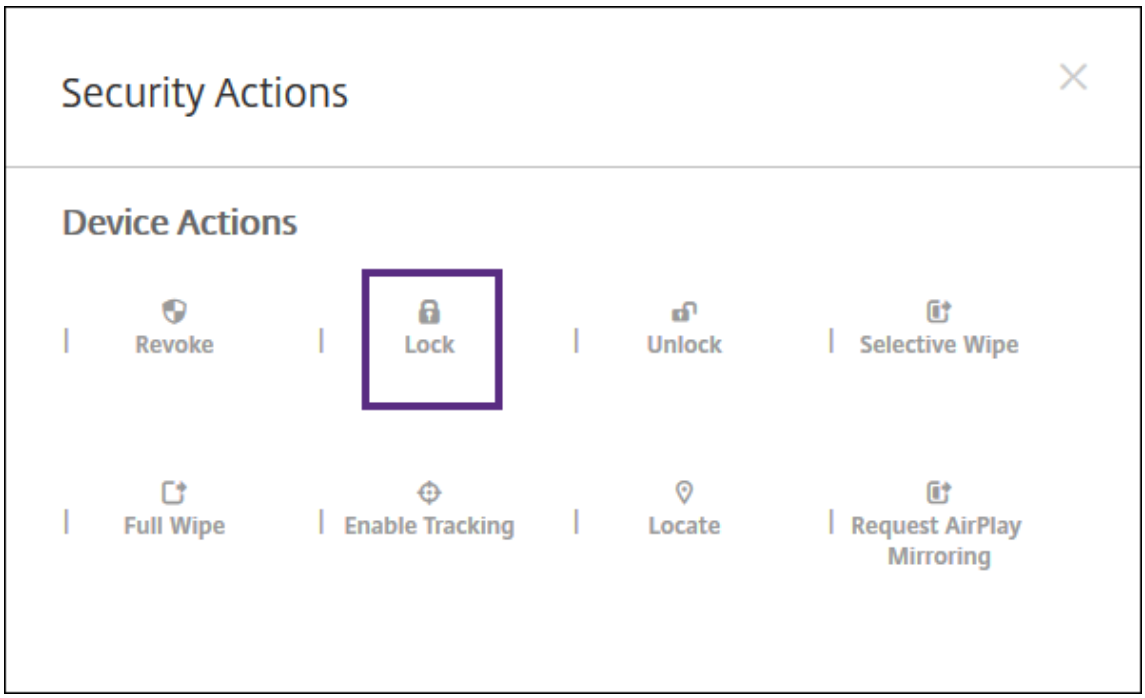


2. ロックする iOS デバイスを選択します。

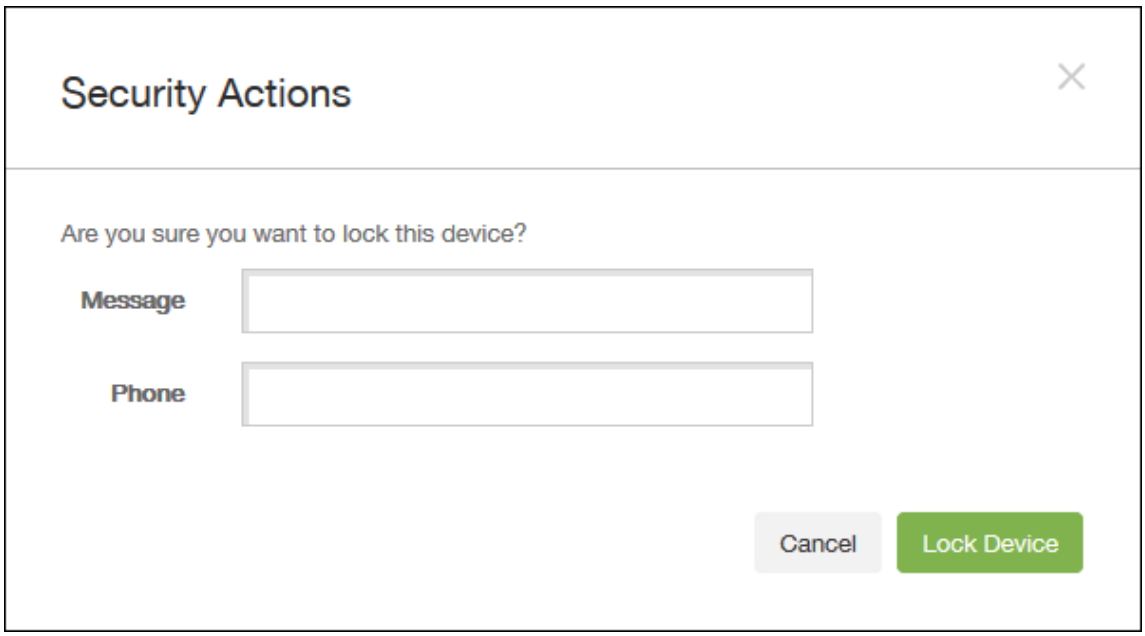
   デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。



3. オプションメニューの ［保護］を選択します。［セキュリティ操作］ダイアログボックスが開きます。



4. ［ロック］をクリックします。［セキュリティ操作］確認ダイアログボックスが開きます。



5. 必要に応じて、デバイスのロック画面に表示するメッセージと電話番号を入力します。

   iOS は「Lost iPad」という文字列をユーザーが ［メッセージ］フィールドに入力した内容に追加します。

   ［メッセージ］フィールドを空白にして電話番号を指定すると、Apple はメッセージ「Call owner」をデバイスのロック画面に表示します。

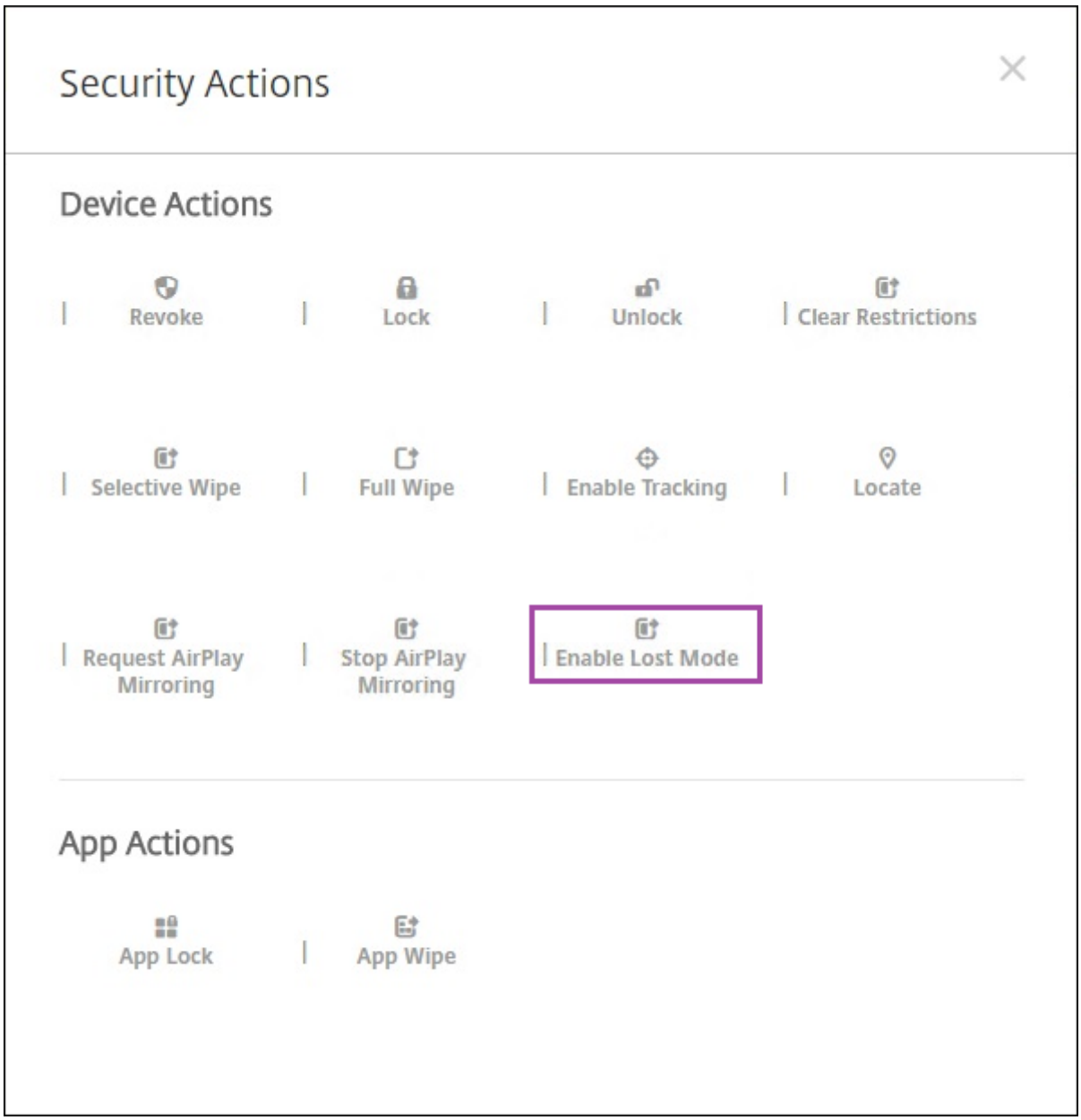
6. ［デバイスのロック］をクリックします。

iOS デバイスを紛失モードにする

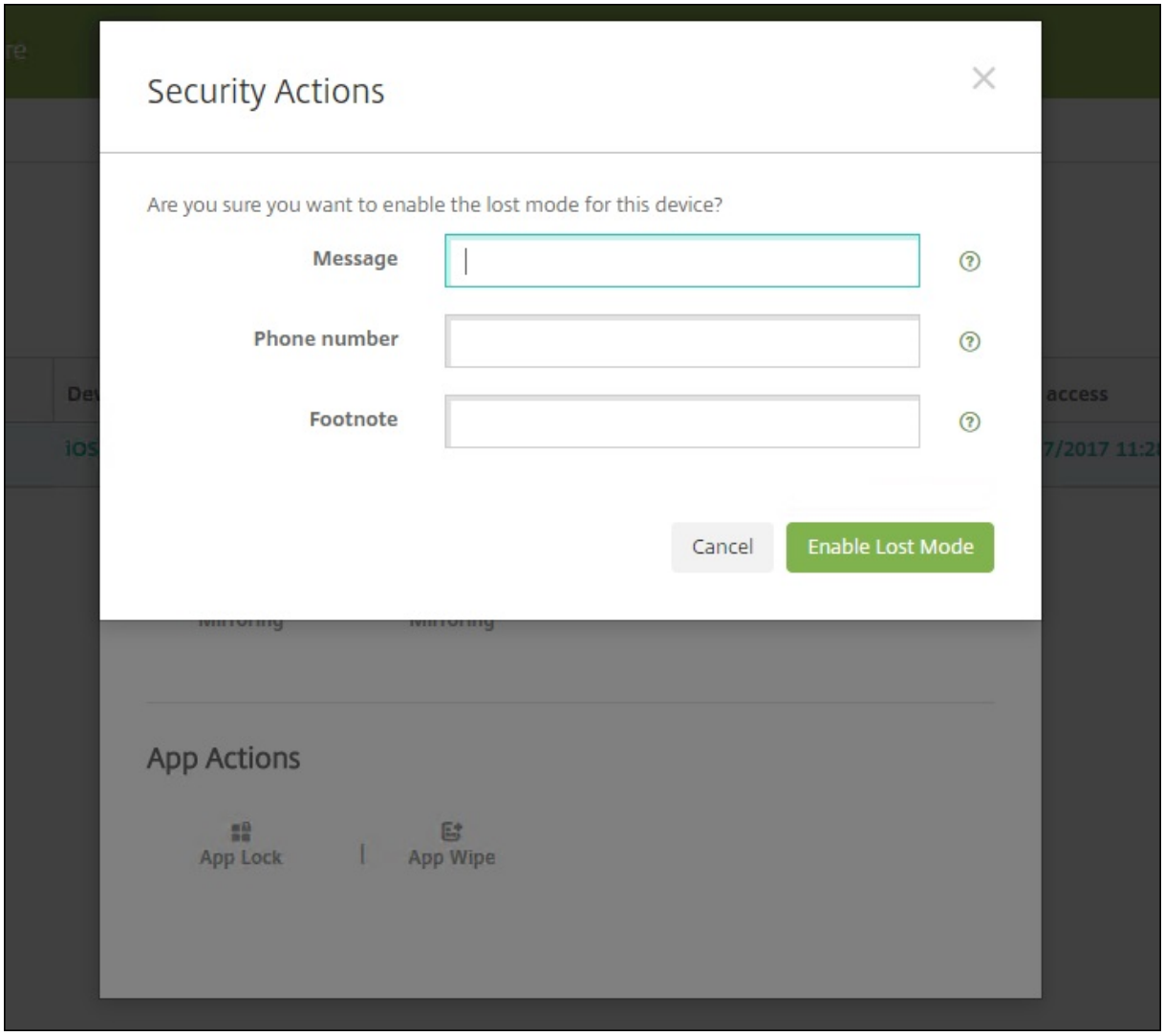
Citrix Endpoint Management の紛失モードデバイスプロパティで、iOS デバイスを紛失モードにします。Apple のマネージド紛失モードと異なり、Citrix Endpoint Management の紛失モードでは、ユーザーは自分のデバイスを探せるようにするために、次のどちらの操作も実行する必要がありません：［**iPhone/iPad** を探す］設定を構成するか、または Citrix Secure Hub の位置情報サービスを有効化する。

ただし、Citrix Endpoint Management の紛失モードでは、デバイスのロックを解除できるのは Citrix Endpoint Management だけです。一方、Citrix Endpoint Management のデバイスロック機能を使用すると、ユーザーは管理者から提供された PIN コードを使用して、直接デバイスをロック解除できます。

紛失モードを有効または無効にするには：［管理］**>** ［デバイス］に移動し、監視対象デバイスを選択して ［保護］をクリックします。次に、［紛失モードを有効化］または ［紛失モードを無効化］をクリックします。

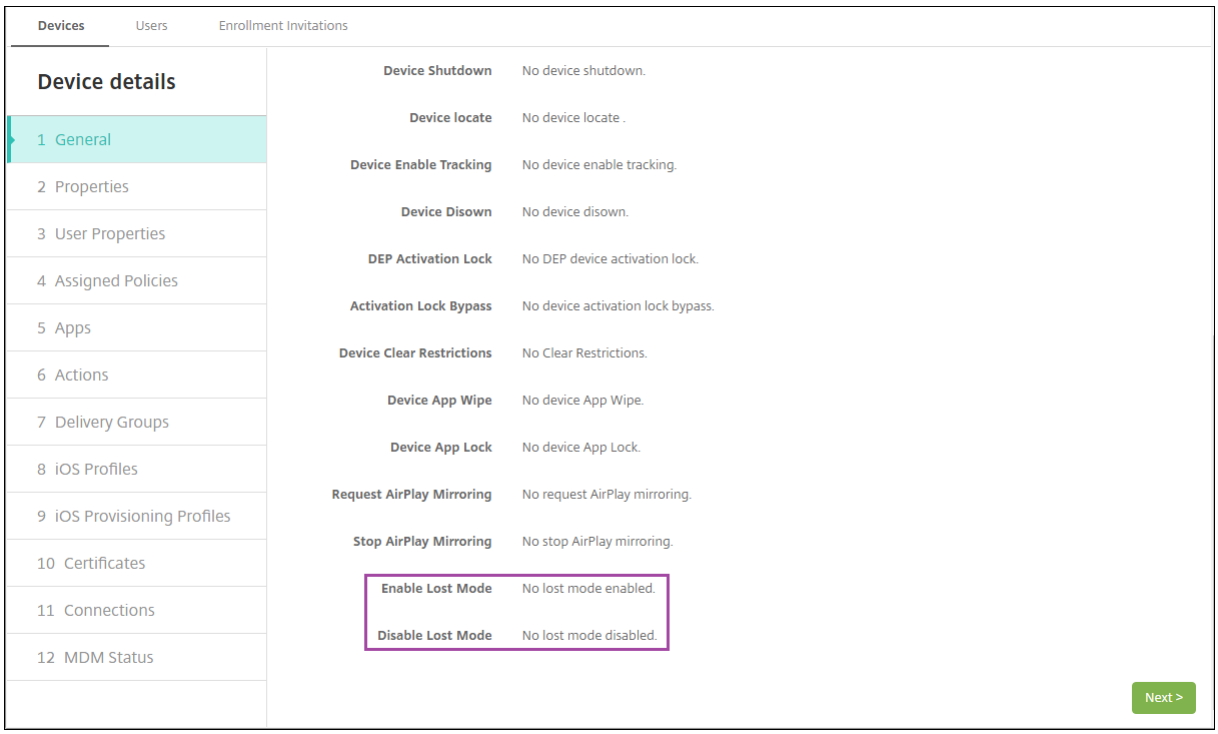


［紛失モードを有効化］をクリックした場合は、デバイスが紛失モードになったときにデバイスに表示される情報を入力します。

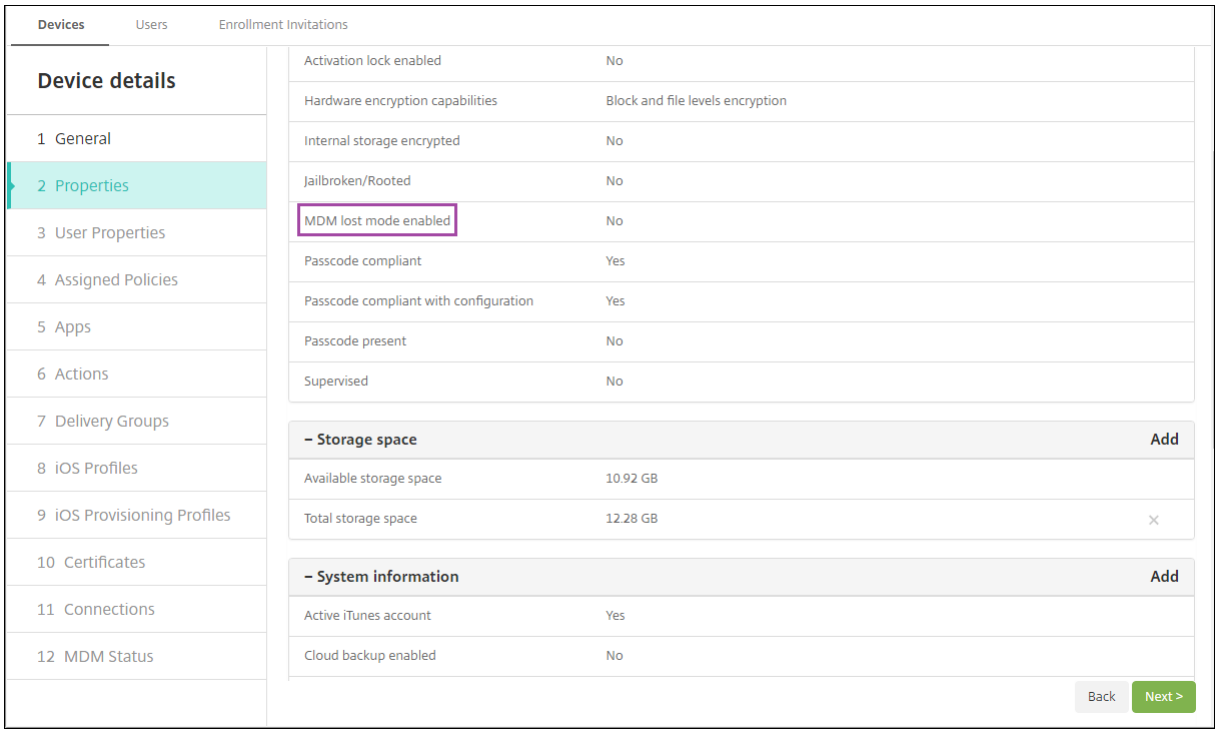


次のいずれかの方法を使って紛失モードの状態を確認する：

- ［セキュリティ操作］ウィンドウで、ボタンが ［紛失モードを無効化］であることを確認します。
- ［管理］**>**［デバイス］から、［セキュリティ］の ［一般］タブで、［紛失モードを有効化］または［紛失モードを無効化］の最後の操作を確認します。



- [管理] > [デバイス] から [プロパティ] タブで、[**MDM** の紛失モードの有効化] の設定値が正しいことを確認します。



iOS デバイスで Citrix Endpoint Management の紛失モードを有効化すると、Citrix Endpoint Management コンソールも以下のように変更されます:

- ［構成］**>**［操作］の ［操作］一覧には、自動化された操作 ［デバイスを失効］、［デバイスの選択的なワイプ］、［デバイスを完全にワイプ］は含まれません。
- ［管理］**>**［デバイス］の ［セキュリティ操作］一覧に、［失効］および ［選択的なワイプ］デバイス操作が含まれなくなりました。必要に応じて、セキュリティ操作を使ってフルワイプを実行することは引き続き可能です。

iOS は「Lost iPad」という文字列をユーザーが ［セキュリティ操作］画面の ［メッセージ］に入力した内容に追加します。

［メッセージ］を空白にして電話番号を指定すると、Apple はメッセージ「Call owner」をデバイスのロック画面に表示します。

iOS アクティベーションロックのバイパス

アクティベーションロックは、紛失したり盗まれたりした管理対象デバイスが再アクティブ化されないようにすることを目的とした［iPhone/iPad を探す］の機能です。アクティベーションロックでは、ユーザーの Apple ID とパスワードを入力してからでないと、以下の操作を実行することはできません：［iPhone/iPad を探す］をオフにする、デバイスを消去する、またはデバイスを再アクティブ化する。組織所有のデバイスの場合は、デバイスのリセットや再割り当てなどを行う際にアクティベーションロックをバイパスする必要があります。

アクティベーションロックを有効にするには、Citrix Endpoint Management の MDM オプションデバイスポリシーを構成し、展開します。これにより、ユーザーの Apple 資格情報なしで、Citrix Endpoint Management コンソールからデバイスを管理できるようになります。アクティベーションロックで必要な Apple 資格情報の入力を省略するには、Citrix Endpoint Management コンソールで［アクティベーションロックバイパス］セキュリティ操作を発行します。

たとえば、紛失した iPhone がユーザーによって返却された場合や、フルワイプの前後にデバイスを設定する場合、iPhone で Apple App Store アカウントの資格情報を求められた際に、［アクティベーションロックバイパス］セキュリティ操作を発行することでこの手順を省略します。

アクティベーションロックバイパスのデバイス要件

- Apple Configurator または Apple Deployment Program による監視対象である
- iCloud アカウントで構成済みである
- ［iPhone/iPad を探す］が有効になっている
- Citrix Endpoint Management に登録済みである
- MDM オプションデバイスポリシー（アクティベーションロックが有効になっている）がデバイスに展開されている

デバイスのフルワイプを発行する前にアクティベーションロックをバイパスするには、次の手順を実行します：

1. ［管理］**>**［デバイス］の順に選択し、デバイスを選択して ［保護］、［アクティベーションロックバイパス］の順にクリックします。
2. デバイスをワイプします。デバイスの設定時に、アクティベーションロック画面は表示されません。

デバイスのフルワイプを発行した後にアクティベーションロックをバイパスするには、次の手順を実行します:

1. デバイスをリセットまたはワイプします。デバイスの設定時に、アクティベーションロック画面が表示されます。
2. ［管理］**>**［デバイス］の順に選択し、デバイスを選択して ［保護］、［アクティベーションロックバイパス］の順にクリックします。
3. デバイスの［戻る］ボタンをタップします。ホーム画面が開きます。

次のことに注意してください:

- ユーザーが「iPhone/iPad を探す」をオフにしないようアドバイスしてください。デバイスからフルワイプを実行しないでください。いずれの場合も、ユーザーは iCloud アカウントのパスワードを入力するよう求められます。アカウントの検証後にすべてのコンテンツと設定が消去されると、iPhone/iPad のアクティブ化画面がユーザーに表示されなくなります。
- アクティベーションロックバイパスコードを作成済みのデバイス、およびアクティベーションロックが有効になっているデバイスの場合は、フルワイプ後に［iPhone/iPad のアクティブ化］ページを省略できなくても、Citrix Endpoint Management からデバイスを削除する必要はありません。管理者またはユーザーが Apple サポートに連絡することで、デバイスのブロックを直接解除することができます。
- ハードウェアインベントリの際に、Citrix Endpoint Management はデバイスのアクティベーションロックバイパスコードの照会を行います。バイパスコードが使用可能な場合は、デバイスから Citrix Endpoint Management にバイパスコードが送信されます。その後、バイパスコードをデバイスから削除するには、Citrix Endpoint Management コンソールから［アクティベーションロックバイパス］セキュリティ操作を送信します。この時点で、Citrix Endpoint Management と Apple に、デバイスのブロック解除に必要なバイパスコードが存在します。
- ［アクティベーションロックバイパス］のセキュリティ操作は、Apple のサービスの可用性に依存しています。操作がうまくいかない場合は、以下の方法のいずれかで、デバイスのブロックを解除できます:
  - デバイスで、iCloud アカウントの資格情報を手動で入力します。
  - ［ユーザー名］フィールドは空のままにして、［パスワード］フィールドにバイパスコードを入力します。バイパスコードを見つけるには、［管理］**>**［デバイス］に移動し、デバイスを選択して ［編集］、［プロパティ］の順にクリックします。［セキュリティ情報］の下に ［アクティベーションロックバイパスコード］があります。

macOS

November 29, 2023

Citrix Endpoint Management で macOS デバイスを管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書を設定します。詳しくは、「APN 証明書」を参照してください。

Citrix Endpoint Management は、macOS デバイスを MDM に登録します。Citrix Endpoint Management は、MDM の macOS デバイスに対して、次の種類の登録認証をサポートします。

- ドメイン
- ドメインおよびワンタイムパスワード
- 招待 URL およびワンタイムパスワード

> **macOS 15** での信頼された証明書の要件:
>
> Apple では、TLS サーバー証明書の新しい要件を設定しています。すべての証明書が新しい Apple の要件に準拠していることを確認します。アップルの出版物である「https://support.apple.com/en-us/HT210176」を参照してください。証明書の管理については、「証明書のアップロード」を参照してください。

macOS デバイスの管理を開始するための一般的なワークフローは次のとおりです:

1. オンボーディングプロセスの完了。「オンボードとリソースのセットアップ」と「デバイス登録およびリソース配信の準備」を参照してください。
2. 登録方法の選択と構成。「サポートされている登録方法」を参照してください。
3. macOS デバイスポリシーを構成します。
4. macOS デバイスを登録します。
5. デバイスとアプリのセキュリティ操作の設定。「セキュリティ操作」を参照してください。

サポートされているオペレーティングシステムについては、「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。

開いたままにする必要がある **Apple** のホスト名

iOS、macOS、Apple App Store を正しく動作させるには、一部の Apple ホスト名を開いたままにしておく必要があります。これらのホスト名をブロックすると、インストール、更新、および以下の適切な操作に影響が出る可能性があります: iOS、iOS アプリ、MDM の操作およびデバイスとアプリの登録詳しくは、https://support.apple.com/en-us/HT201999を参照してください。

サポートされている登録方法

次の表は、macOS デバイスでサポートされている Citrix Endpoint Management での登録方法を示しています:

方法	サポート対象
Apple Deployment Programs	はい

方法	サポート対象
Apple School Manager	はい
Apple Configurator	番号
手動登録	はい
登録招待	はい

Apple では、ビジネスおよび教育機関アカウント向けのデバイス登録プログラムが提供されています。ビジネス用アカウントの場合、デバイスを Citrix Endpoint Management で登録して管理するには、Apple Deployment Program に登録して、Apple Deployment Program を利用する必要があります。これは、iOS、macOS、Apple TV デバイス向けのプログラムです。「Apple Deployment Program でのデバイスの展開」を参照してください。

教育機関アカウントの場合は、Apple School Manager アカウントを作成します。Apple School Manager では、Deployment Program と一括購入が統合されています。Apple School Manager は、教育向け Apple Deployment Program の一種です。「Apple Education 機能との統合」を参照してください。

Apple Deployment Program を使用して、iOS、macOS、および Apple TV デバイスを一括登録することができます。これらのデバイスは、Apple から直接購入するか、Apple 正規販売代理店、または通信事業者から購入することができます。

macOS デバイスポリシーの構成

デバイスポリシーを使用して、Citrix Endpoint Management と macOS を実行するデバイスとの通信に関する構成を行います。次の表は、macOS デバイスで使用可能なデバイスポリシーの一覧です:

AirPlay ミラーリング	アプリインベントリ	アプリのアンインストール
カレンダー（CalDAV）	連絡先（CardDAV）	資格情報
デバイス名	Exchange	FileVault
ファイアウォール	フォント	iOS および macOS プロファイルのインポート
LDAP	メール	ネットワーク
OS 更新	パスコード	プロファイルの削除
制限	SCEP	VPN
Web クリップ		

macOS デバイスの登録

Citrix Endpoint Management には、macOS を実行するデバイスの登録方法は 2 種類あります。いずれの方法でも、macOS ユーザーは各自のデバイスから無線経由で直接登録できます。

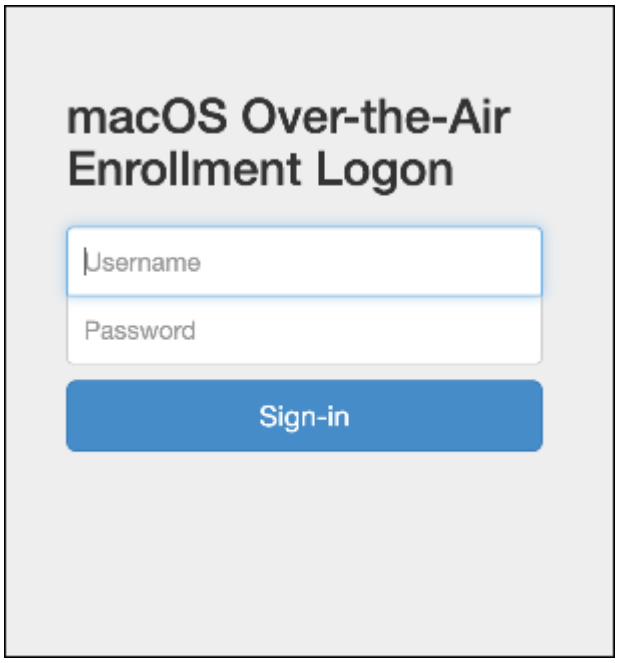
- ユーザーに登録招待を送信します。この登録方法を使用すると、以下の macOS デバイスの登録セキュリティモードをいずれも設定できます:
  - ユーザー名およびパスワード
  - ユーザー名および PIN
  - 2 要素認証

  ユーザーが登録招待の指示に従うと、ユーザー名が入力されたサインオン画面が表示されます。
- ユーザーに登録リンクを送信します。この macOS デバイスの登録方法ではユーザーに登録リンクを送信し、ユーザーは Safari ブラウザーまたは Chrome ブラウザーでこのリンクを開くことができます。ユーザーはユーザー名とパスワードを入力して登録を行います。

  macOS デバイスでの登録リンクの使用を防ぐには、サーバープロパティ ［**Enable macOS OTAE**］を **false** に設定します。これにより、macOS ユーザーは登録招待を使用してのみ登録できるようになります。

macOS ユーザーへの登録招待の送信

1. macOS ユーザーを登録するための招待を追加します。「登録招待の送信」を参照してください。
2. ユーザーが招待を受信してリンクをクリックすると、Safari ブラウザーに次の画面が表示されます。ユーザー名は Citrix Endpoint Management によって入力されます。登録セキュリティモードに ［**2** 要素］を選択すると、別のフィールドが表示されます。



3. 必要に応じて、ユーザーが証明書をインストールします。ユーザーに証明書のインストールを求めるメッセージが表示されるかは、管理者が macOS 用の公式に信頼される SSL 証明書および公式に信頼されるデジタル署名証明書を構成したかどうかによります。証明書について詳しくは、「証明書と認証」を参照してください。
4. 要求された資格情報をユーザーが入力します。

   Mac のデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、Citrix Endpoint Management で macOS デバイスを管理できるようになります。

macOS ユーザーへのインストールリンクの送信

1. 登録リンク（`https://serverFQDN:8443/instanceName/macos/otae`）を送信します。ユーザーはこのリンクを Safari ブラウザーまたは Chrome ブラウザーで開くことができます。

   - **serverFQDN** には、Citrix Endpoint Management を実行しているサーバーの完全修飾ドメイン名（FQDN）を入力します。
   - ポート **8443** は、デフォルトのセキュアポートです。別のポートを構成している場合は、8443 ではなく、構成済みのポートを使用します。
   - 通常`zdm`と表示される **instanceName** は、サーバーのインストール時に指定された名前です。

   インストールリンクの送信について詳しくは、「インストールリンクを送信するには」を参照してください。
2. 必要に応じて、ユーザーが証明書をインストールします。管理者が iOS および macOS 用の公式に信頼される SSL 証明書およびデジタル署名証明書を構成すると、ユーザーに証明書のインストールを求めるメッセージが表示されます。証明書について詳しくは、「証明書と認証」を参照してください。
3. ユーザーが Mac にサインオンします。

   Mac のデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、Citrix Endpoint Management で macOS デバイスを管理できるようになります。

セキュリティ操作

macOS は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

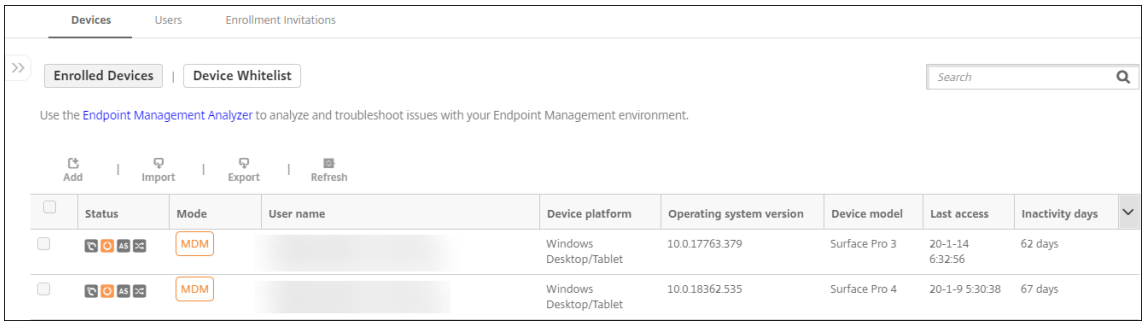
取り消し	ロック	選択的なワイプ
完全なワイプ	証明書の書き換え	個人用回復キーの交換

macOS デバイスのロック

紛失した macOS デバイスをリモートでロックできます。Citrix Endpoint Management は、デバイスをロックします。その後 PIN コードが生成されてデバイスに設定されます。デバイスにアクセスするには、PIN コードを入力します。Citrix Endpoint Management コンソールからロックを解除するには ［ロックのキャンセル］ を使用します。

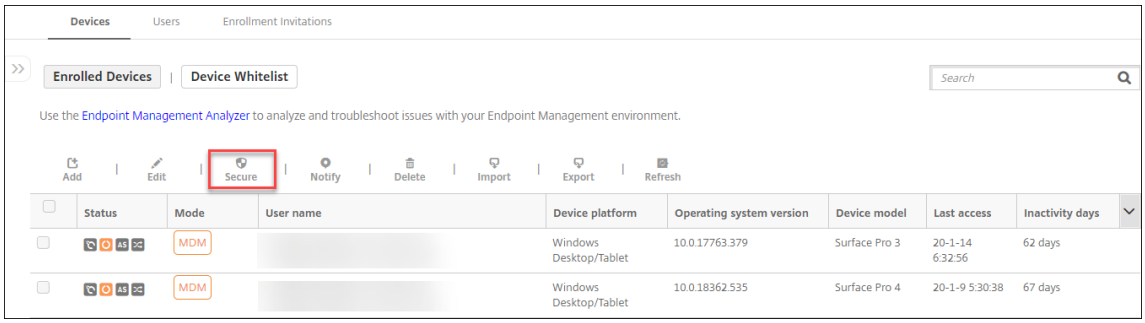
パスコードデバイスポリシーを使用して、PIN コードに関連した設定をさらに構成できます。詳しくは、「macOS 設定」を参照してください。

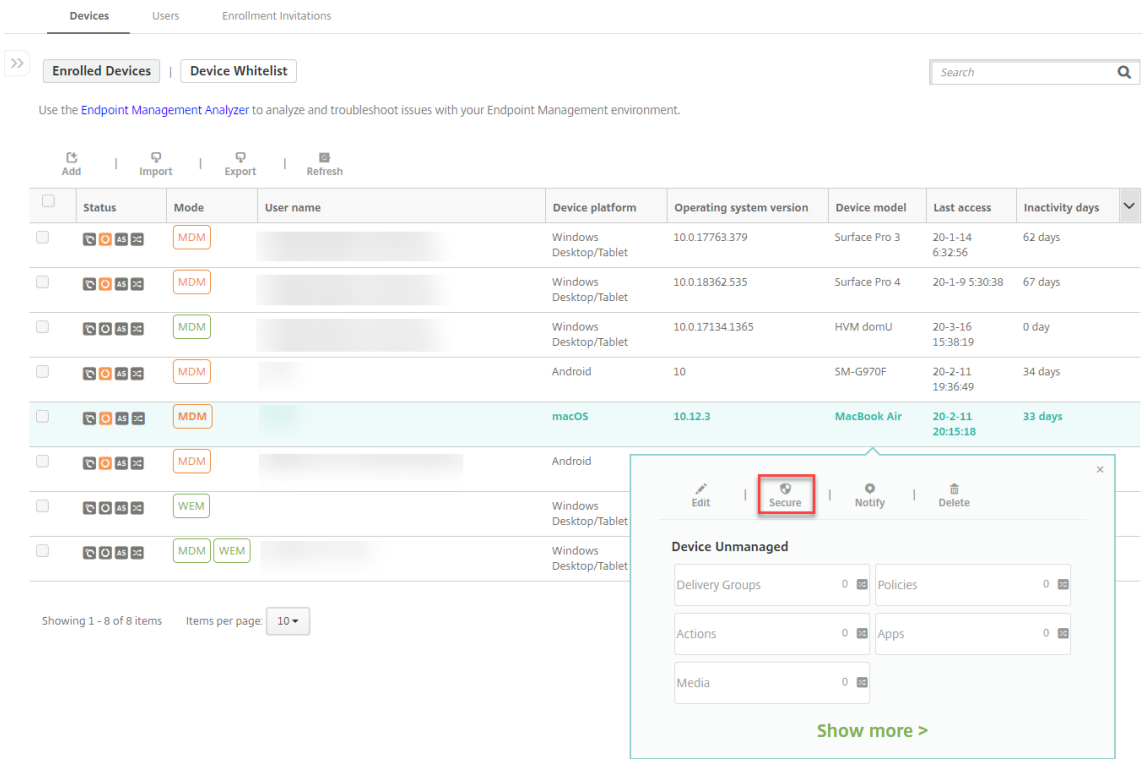
1. ［管理］ **>** ［デバイス］ の順にクリックします。［デバイス］ ページが開きます。



2. ロックする macOS デバイスを選択します。

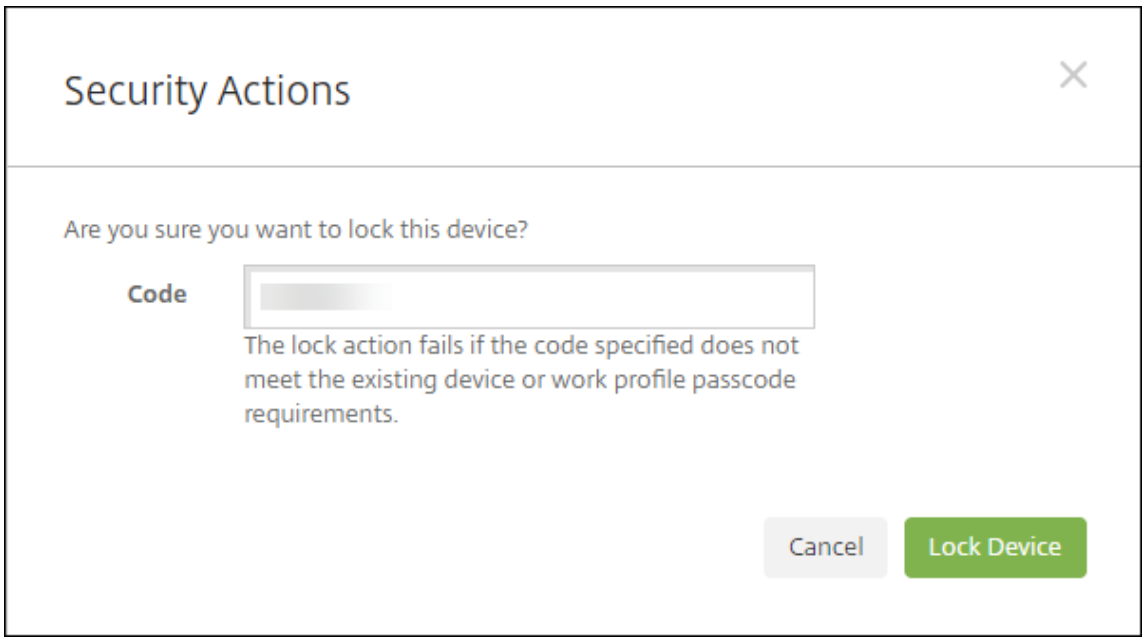
   デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。





3. オプションメニューの ［保護］を選択します。［セキュリティ操作］ダイアログボックスが開きます。

4. ［ロック］をクリックします。［セキュリティ操作］確認ダイアログボックスが開きます。



5. ［デバイスのロック］をクリックします。

> 重要:
>
> Citrix Endpoint Management が生成するコードを使用する代わりに、パスコードを指定することもできます。指定されたコードが既存のデバイスや既存の仕事用プロファイルのコード要件に一致しない場合、ロック操作が失敗します。

Bootstrap Token

Bootstrap Token は、macOS デバイスにサインオンするときにアカウントに SecureToken macOS 属性を付与するのに役立ちます。SecureToken は、信頼できるアカウントから別のアカウントに受け継がれます。SecureToken 対応のアカウントは、デバイスで暗号化操作を実行できます。Bootstrap Token がない場合、個々のユーザーアカウントを追加する前に、複雑なワークフローに従ってそのデバイスでアカウントを作成する必要があります。

Citrix Endpoint Management は、Apple Deployment Program 経由で登録された macOS デバイスの Bootstrap Token のエスクローをサポートします。Apple Deployment Program を使用して、Apple から直接、または Apple 正規販売代理店や通信事業者から購入した macOS デバイスを登録します。Apple Deployment Program での登録について詳しくは、「Apple Deployment Program でのデバイスの展開」を参照してください。

Bootstrap Token は、セットアップアシスタントのワークフロー中に生成されます。具体的には、ローカルユーザーアカウントの作成中に生成されます。セットアップアシスタントは、ユーザーがデバイスを初めて起動したときに実行されます。このトークンは Citrix Endpoint Management データベースに保存され、管理者やエンドユーザーには表示されません。Citrix Endpoint Management サイトからデバイスを削除すると、トークンが削除されます。工場出荷時の状態にリセットしても、削除されません。

前提条件:

- macOS 11.0 以降
- Apple T2 セキュリティチップを搭載した macOS デバイス
- Apple Deployment Program 経由で登録された macOS デバイス

Citrix Endpoint Management を使用して Bootstrap Token をエスクローする利点の 1 つは、リモートアカウントで FileVault を有効にし、FileVault ボリュームのロックを解除できることです。FileVault について詳しくは、「FileVault デバイスポリシー」を参照してください。

Apple Deployment Program でのデバイスの展開

March 15, 2024

Apple Deployment Program（ADP）を使用すると、ユーザーがデバイスを手にする前に、デバイスに触れたり準備したりしなくても、Apple デバイスを Citrix Endpoint Management に自動的に登録できます。ユーザーがデバイスを箱から取り出してアクティブ化すると、デバイスは自動的に Citrix Endpoint Management に登録され、すべての管理設定、アプリ、ブックがユーザーに提供されます。

ADP には、企業組織向けの Apple Business Manager（ABM）と、教育機関向けの Apple School Manager（ASM）が含まれます。ABM と ASM は、iOS、iPadOS、および macOS デバイスで使用できます。デバイスの適格性について詳しくは、「Apple Business Manager ユーザガイド」および「Apple School Manager ユーザガイド」を参照してください。

> 注:
>
> ABM と ASM は、以前の Apple の Device Enroll Program と Volume Purchase Program を組み合わせたものです。

この記事では、ABM または ASM を使用した一般的な展開ワークフローについて説明します:

1. ABM または ASM への登録
2. ABM または ASM アカウントの Citrix Endpoint Management への接続
3. デバイスの注文
4. デバイスの Citrix Endpoint Management への割り当て
5. コンテンツの一括購入と Citrix Endpoint Management への同期
6. デバイスポリシーの展開規則およびアプリの構成
7. 割り当てられたユーザーとリソースを含むデリバリーグループの追加

この展開プロセスを完了すると、デバイスを箱から取り出し、アクティブ化して、自動デバイス登録を行う準備が整います。

前提条件

Citrix Endpoint Management と Apple を接続するには、必要なポートを開きます。詳しくは、「ポート要件」を参照してください。

ABM または ASM への登録

Apple でデバイスの展開を開始するには、ABM または ASM に登録します。

ABM と ASM は、個人ではなく組織で利用できます。アカウントを作成するには、多くの組織の詳細と情報を提供する必要があります。アカウントの要求と承認の取得には時間がかかる場合があります。

ABM への登録

ABM に登録するには、business.apple.comにアクセスします。[今すぐ登録する] をクリックして、新しいアカウントを申請します。

`deployment@company.com`などの組織のメールアドレスを使用することをお勧めします。登録処理には数日かかる場合があります。ログオン資格情報を受け取ったら、ABM に示される手順に従ってアカウントを作成します。

ASM への登録

ASM アカウントを作成するには、Apple School Managerにアクセスし、指示に従って登録します。ASM への初回ログオン時に、セットアップアシスタントが開きます。

- ASM の前提条件、セットアップアシスタント、管理タスクについて詳しくは、「Apple School Manager ユーザガイド」を参照してください。
- ASM ユーザーアカウントのセットアップには、Active Directory のドメイン名とは異なるドメイン名を使用します。たとえば、ASM のドメイン名には「`appleid`」のようなプレフィックスを付けます。
- ASM を名簿データに接続すると、ASM によって講師と生徒の管理対象 Apple ID が作成されます。名簿データには講師、生徒、およびクラスを含めるようにします。ASM への名簿データの追加については、このリストの前半にリンクされている「Apple School Manager ユーザガイド」を参照してください。
- このリストの前半にリンクされている前述の「Apple School Manager ユーザガイド」で説明されているように、管理対象 Apple ID の形式を所属機関に合わせてカスタマイズできます。

  > 重要:
  >
  > ASM 情報を Citrix Endpoint Management にインポートした後に、管理対象 Apple ID を変更しないでください。

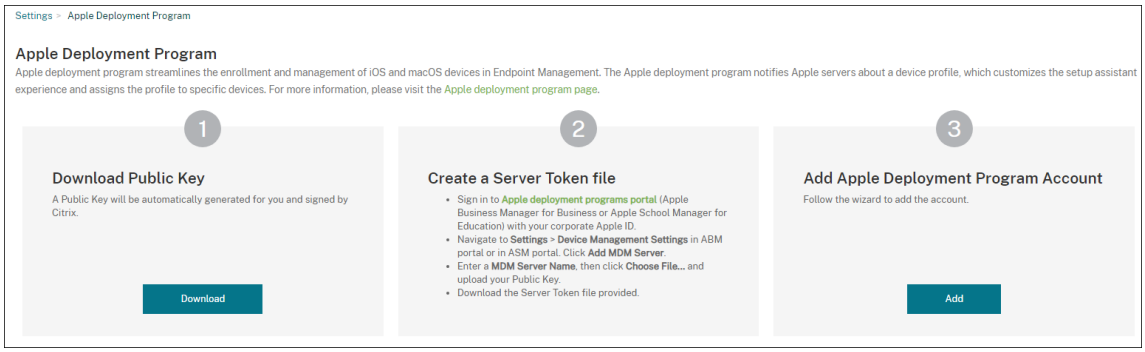
- 正規販売店や通信事業者を通じてデバイスを購入した場合は、ASM にデバイスをリンクします。詳しくは、このリストの前半にリンクされている「Apple School Manager ユーザガイド」を参照してください。

ABM または ASM アカウントの Citrix Endpoint Management への接続

ABM または ASM アカウントを作成したら、それを Citrix Endpoint Management サーバー環境に接続します。

手順 1: Citrix Endpoint Management サーバーから公開キーをダウンロードします

1. Citrix Endpoint Management コンソールで、［設定］> ［**Apple Deployment Programs**］の順に移動します。



2. ［公開キーのダウンロード］の下にある ［ダウンロード］をクリックします。

手順 2: Apple アカウントからサーバートークンファイルを作成してダウンロードします

1. 管理者またはデバイス登録マネージャーのアカウントを使用して、Apple Business ManagerまたはApple School Managerにサインインします。
2. サイドバーの下部にある ［**Settings**］をクリックし、［**Device Management Settings**］> ［**Add MDM Server**］をクリックします。
3. ［**MDM Server Name**］設定で、Citrix Endpoint Management サーバーの名前を入力します。入力するサーバー名は参照用です。サーバーの URL や名前ではありません。
4. ［**Upload Public Key**］にある ［**Choose File**］をクリックします。Citrix Endpoint Management からダウンロードした公開キーをアップロードして、変更を保存します。
5. ［**Download Token**］をクリックして、サーバートークンファイルをコンピューターにダウンロードします。

   Citrix Endpoint Management に ABM または ASM アカウントを追加するときに、このサーバートークンファイルをアップロードします。トークンファイルをインポートすると、トークン情報が Citrix Endpoint Management コンソールに表示されます。

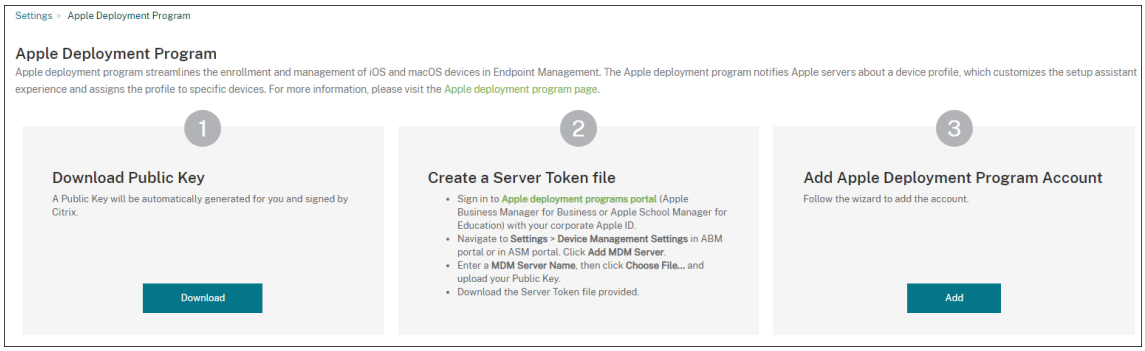
6. [**Default Device Assignment**] で [**Change**] をクリックします。どのようにデバイスを割り当てるかを選択して求められる情報を入力します。詳しくは、「Apple Business Manager ユーザガイド」または「Apple School Manager ユーザガイド」を参照してください。

手順 **3**: アカウントを **Citrix Endpoint Management** に追加する

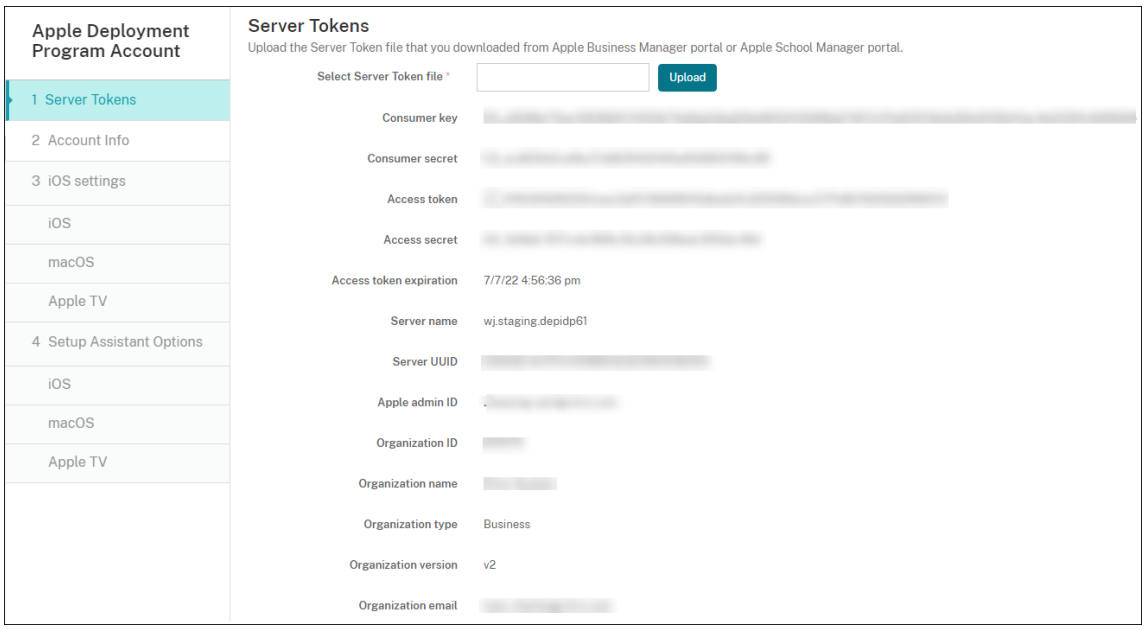
Citrix Endpoint Management には、複数の ABM または ASM アカウントを追加できます。この機能によって、国や部門などによって異なる登録設定や設定補助オプションを利用できるようになります。追加後、ABM または ASM アカウントをさまざまなデバイスポリシーに関連付けます。

たとえば、異なる国々からの ABM または ASM アカウントすべてを同一の Citrix Endpoint Management サーバーに集中させて、すべての ABM または ASM デバイスのインポートおよび監視を行うことができます。最初に、登録設定をカスタマイズし、部門、組織階層、またはその他の構造ごとに、アシスタントオプションを設定します。次に、組織全体に適切な機能を提供し、ユーザーが適切な支援を受けられるようにポリシーを構成します。

1. Citrix Endpoint Management コンソールで、[設定]**>**[**Apple Deployment Program**]に移動し、[**Apple Deployment Programs** アカウントの追加] の [追加] をクリックします。

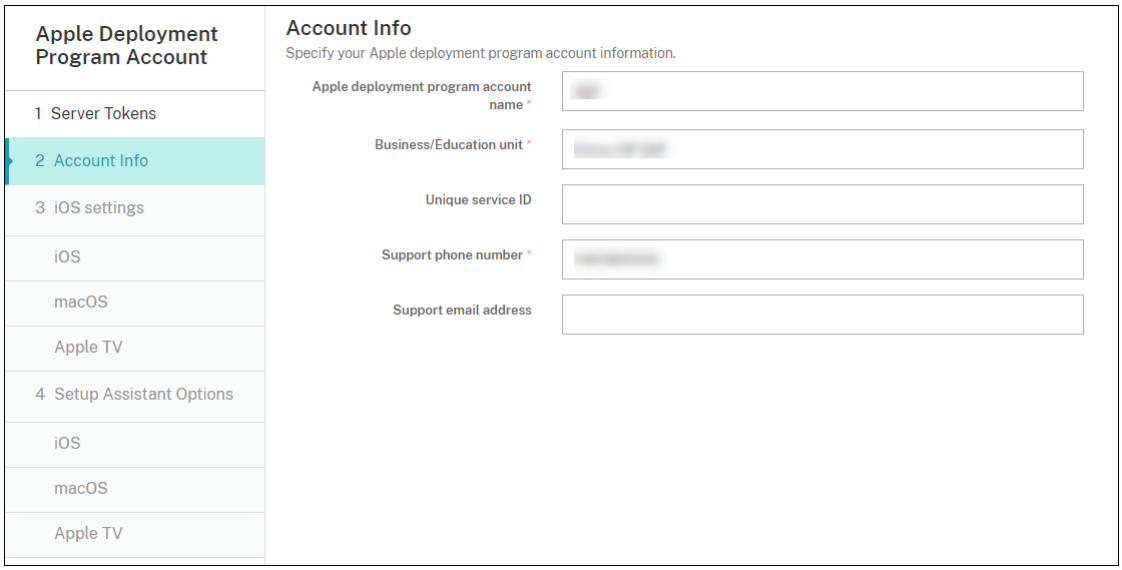


2. [サーバートークン] ページでサーバートークンファイルを指定し、[アップロード] をクリックします。



サーバートークンの情報が表示されます。

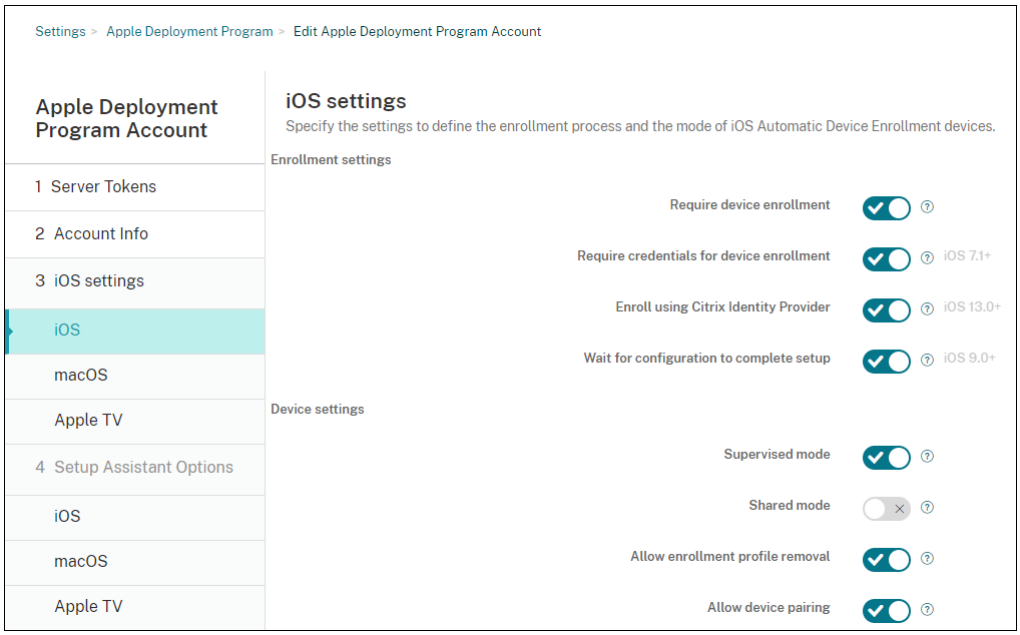
3. ［アカウント情報］ページで次の設定を入力します。



- **Apple Deployment Program** アカウント名：この ADP アカウントの一意の説明的な名前により、国ごとに、または組織階層ごとになど、ADP アカウントがどのように編成されているかを識別します。
- 事業/教育単位：デバイスを割り当てる事業単位または部門。このフィールドは必須です。
- 一意のサービス **ID**：アカウントの識別に役立つオプションの一意の ID です。
- サポート用電話番号：ユーザーがセットアップ時にサポートが必要となった場合に連絡するサポートの電話番号。このフィールドは必須です。
- サポート用メールアドレス：エンドユーザーが使用できるサポート用のメールアドレス（オプション）。
- 教育機関のサフィックス： ASM アカウントの場合。このアカウントを通じて登録されたデバイスに割

り当てられたサフィックスを入力します。

4. ［**iOS** 設定］で次の設定を入力します。



登録設定：

- デバイス登録を必須にする：ユーザーにデバイス登録を要求するかどうか。デフォルトは ［オン］です。
- デバイス登録のための資格情報を求める： ABM および ASM のセットアップ時にユーザーに資格情報の入力を要求するかどうか。デバイス登録の際、すべてのユーザーに資格情報の入力を要求し、認証済みのユーザーだけがデバイスを登録できるようにすることをお勧めします。デフォルトは ［オン］です。

  初回セットアップ前に ABM または ASM を有効にし、このオプションを選択しない場合、Citrix Endpoint Management によって ABM または ASM コンポーネントが作成されます。作成されるコンポーネントには、ユーザー、Citrix Secure Hub、ソフトウェアインベントリ、展開グループなどが含まれます。このオプションを選択すると、Citrix Endpoint Management によってコンポーネントは作成されません。そのため、後でこのオプションをオフにしても、これらのコンポーネントが存在しないため、資格情報を入力していないユーザーは ABM または ASM で登録できません。その場合、ABM または ASM コンポーネントを追加するには、ABM または ASM アカウントを無効化してからもう一度有効化します。
- **Enroll using Citrix Identity Provider**： Citrix ID プロバイダーを使用して登録するかどうか。この設定は、ABM アカウントでのみ使用できます。［オン］の場合、ADP 対応の iOS デバイスは Citrix ID プロバイダーを使用してのみ登録します。デフォルトは ［オフ］です。

  この設定を有効にするには、最初に Citrix ID プロバイダーを ID プロバイダーとして構成する必要があります。［設定］**>** ［**ID** プロバイダー（**IDP**）］に移動し、［追加］をクリックして ［**Citrix ID** プロバイダー］を選択します。

  この設定が ［オン］の場合、次の考慮事項に注意してください：

  - ［設定］**>** ［**ID** プロバイダー（**IDP**）］ページで対応する Citrix ID プロバイダーの構成を削除することはできません。
  - 対応する Citrix ID プロバイダー構成を編集する場合、別の ID プロバイダーに切り替えることはできません。

- セットアップを完了するため構成を待機する：すべての MDM リソースがユーザーのデバイスに展開されるまで、デバイスをセットアップアシスタントモードのままにしておく必要があるかどうか。この設定は監視モードのデバイスでのみ使用できます。デフォルトは ［オフ］です。
- Apple のドキュメントによると、デバイスがセットアップアシスタントモードの間は以下のコマンドが機能しない場合があります。
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

デバイス設定：

- 監視モード：登録したデバイスを Apple Configurator で管理する場合、または ［セットアップを完了するため構成を待機する］が有効な場合は、［オン］に設定します。デフォルトは ［オン］です。iOS デバイスを監視モードにすることについて詳しくは、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。
- 登録プロファイルの削除を許可：リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。デフォルトは ［オフ］です。
- デバイスのペアリングを許可：登録したデバイスを Apple Music および Apple Configurator で管理できるかどうか。デフォルトは ［オフ］です。

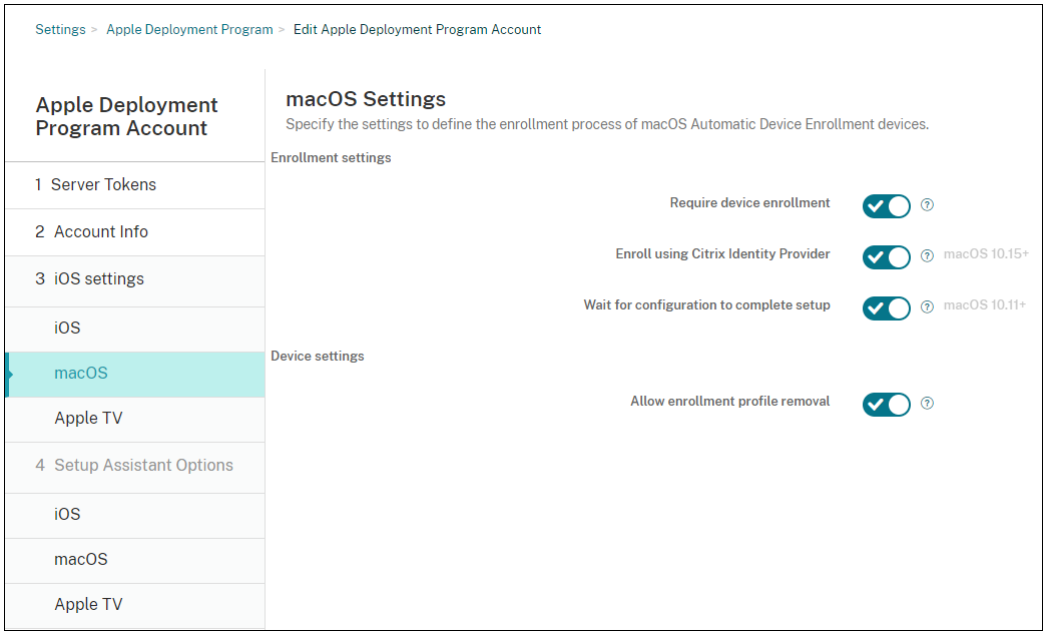
監視 ID

GroundControl ツールを使用する場合は、証明書を追加すると次のことができます：

- 「Trust this host」プロンプトが表示されないように、ペアリングの制限を無効にします。
- 管理対象デバイスの操作を USB 経由でエスカレートし、ユーザー操作なくプロファイルのインストールなどの作業を実行します。これにより、GroundControl はチェックアウトのためにシングルアプリモードとデバイスロックを有効にすることができます。
- ABM または ASM デバイスにバックアップを復元します。

GroundControl について詳しくは、GroundControl の Web サイトを参照してください。

5. ［**macOS** 設定］で設定を入力します。



登録設定:

- デバイス登録を必須にする: ユーザーにデバイス登録を要求するかどうか。デフォルトは ［オン］です。
- **Enroll using Citrix Identity Provider**: Citrix ID プロバイダーを使用して登録するかどうか。この設定は、ABM アカウントでのみ使用できます。［オン］の場合、ADP 対応の macOS デバイスは Citrix ID プロバイダーのみを使用して登録します。デフォルトは ［オフ］です。

  この設定を有効にするには、最初に Citrix ID プロバイダーを ID プロバイダーとして構成する必要があります。［設定］**>** ［**ID** プロバイダー（**IDP**）］に移動し、［追加］をクリックして ［**Citrix ID** プロバイダー］を選択します。

  この設定が ［オン］の場合、次の考慮事項に注意してください:

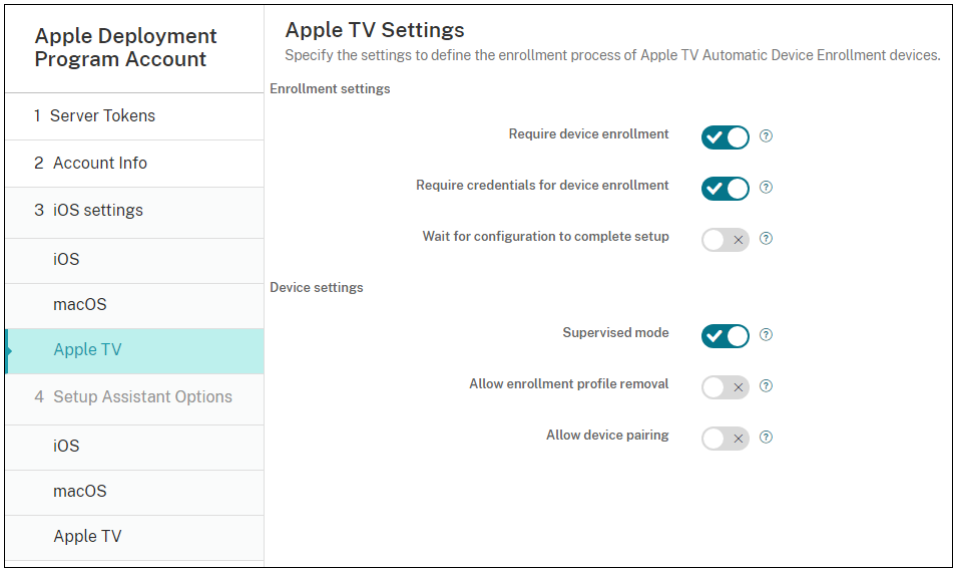
  - ［設定］**>** ［**ID** プロバイダー（**IDP**）］ページで対応する Citrix ID プロバイダーの構成を削除することはできません。
  - 対応する Citrix ID プロバイダー構成を編集する場合、別の ID プロバイダーに切り替えることはできません。
- セットアップを完了するため構成を待機する: ［オン］の場合、MDM リソースパスコードがデバイスに展開されるまで、macOS デバイスはセットアップアシスタントを続行しません。その展開が行われるのは、ローカルアカウントの作成前になります。この設定は macOS 10.11 以降のデバイスで使用できます。デフォルトは ［オフ］です。

デバイス設定:

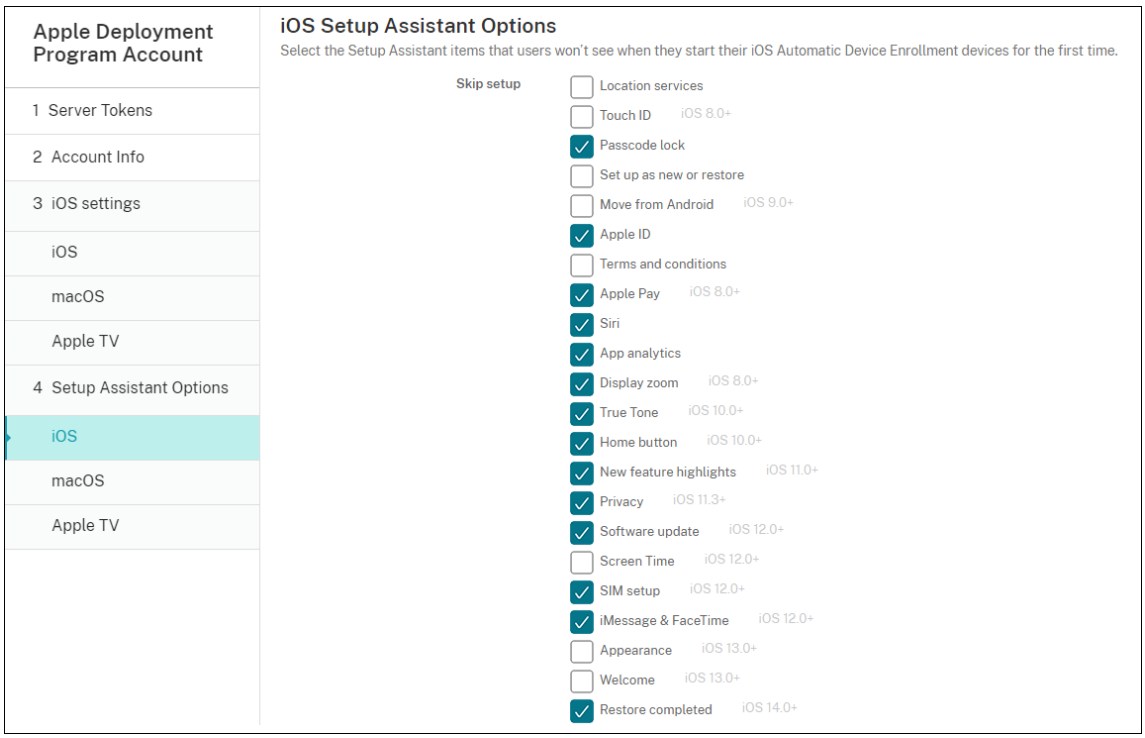
- 登録プロファイルの削除を許可: リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。デフォルトは ［オフ］です。

6. ［**Apple TV** 設定］で、次の設定を指定します。

- デバイス登録を必須にする：ユーザーがデバイス登録をスキップできないようにします。
- デバイス登録のための資格情報を求める：登録時に資格情報を確認します。この設定が無効の場合、Apple TV はデフォルトの「デバイス登録プログラムユーザー」として登録されます。
- セットアップを完了するため構成を待機する：デバイスは、すべてのリソースが展開されるまで ［セットアップアシスタント］画面のまま待機します。
- 監視モード：管理者は制限を構成するとともに、さらに多くの機能を使用できるようになります。
- 登録プロファイルの削除を許可：ユーザーが登録プロファイルを削除できるようにします。
- デバイスのペアリングを許可：デバイス登録プログラムを介して登録されたデバイスを、Apple App Store や Apple Configurator などの Apple ツールで管理できるようにします。



7. ［**iOS** 設定アシスタントのオプション］で、ユーザーが初めてデバイスを起動するときにスキップする iOS 設定アシスタントの手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。これらの機能へのアクセスを完全に制限しない限り、ユーザーはセットアップの完了後にスキップされた機能を構成できます。機能へのアクセスの制限について詳しくは、「制限デバイスポリシー」を参照してください。すべての項目は、デフォルトで選択が解除されています。以下の説明では、設定が選択されたときに何が起こるかについて解説しています。

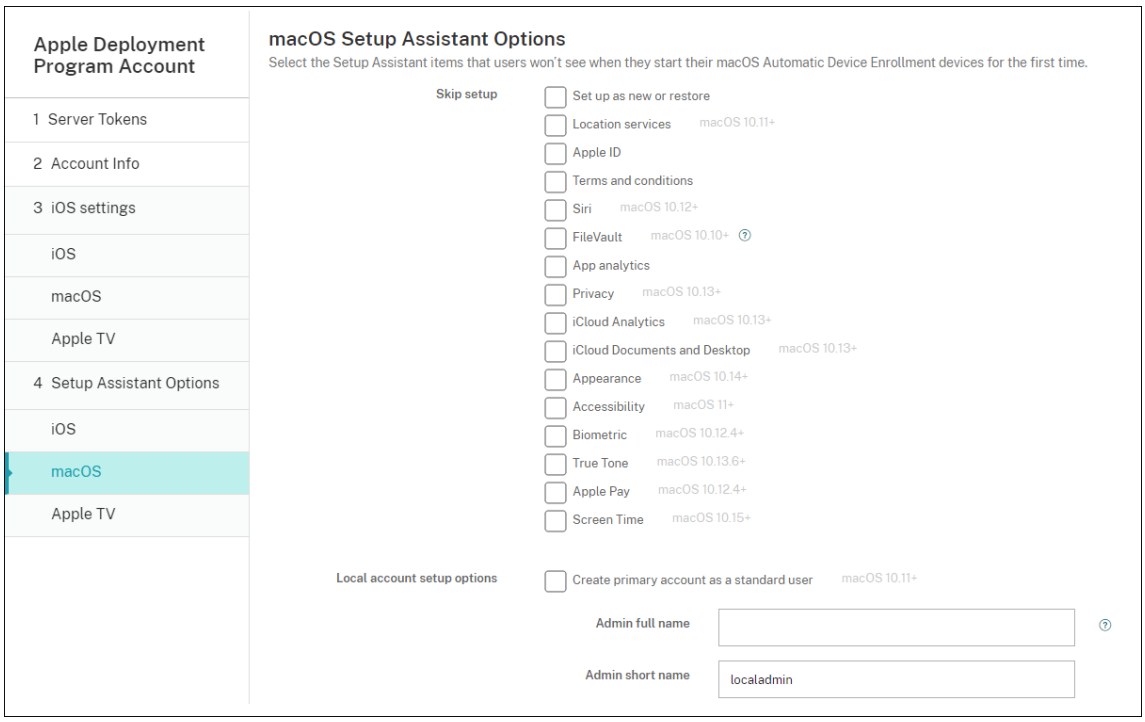


- 位置情報サービス：ユーザーがデバイスで位置情報サービスを設定できないようにします。
- **Touch ID**：ユーザーが iOS デバイスで Touch ID または Face ID を設定できないようにします。
- パスコードロック：ユーザーがデバイスのパスコードを設定できないようにします。パスコードが存在しない場合、ユーザーは Touch ID または Apple Pay を利用できません。
- 新規としてセットアップまたは復元：ユーザーが新規として、または iCloud または Apple App Store のバックアップから、デバイスを設定できないようにします。
- **Android** から移動：ユーザーが Android デバイスから iOS デバイスにデータを転送できないようにします。このオプションは、［新規としてセットアップまたは復元］がオンの場合（すなわち、手順をスキップする場合）にのみ使用できます。
- **Apple ID**：ユーザーがデバイスの管理対象 Apple ID アカウントを設定できないようにします。
- 使用条件：ユーザーがデバイスの使用契約条件を読んで承諾できないようにします。
- **Apple Pay**：ユーザーが Apple Pay を設定できないようにします。この設定がオフになっている場合、ユーザーは Touch ID と Apple ID を設定する必要があります。これらの設定がオフになっていることを確認してください。
- **Siri**：ユーザーが Siri を構成できないようにします。
- **App Analytics**：ユーザーがクラッシュデータおよび使用状況の統計情報を Apple と共有するかどうかを設定できないようにします。
- ディスプレイズーム： iOS デバイスにディスプレイ解像度（標準またはズーム）を設定できないようにします。
- **True Tone**：ユーザーが 4 チャネルセンサーを設定して、ディスプレイのホワイトバランスを動的に調整できないようにします。
- ホームボタン：ユーザーがフィードバックのホームボタンのスタイルを設定できないようにします。

- 新機能のハイライト：ユーザーに Apple ソフトウェアの新機能に関する情報画面が表示されないようにします。
- プライバシー：ユーザーが［データおよびプライバシー］ペインを確認できないようにします。iOS 11.3 以降の場合。
- ソフトウェアの更新：ユーザーが iOS を最新バージョンに更新できないようにします。iOS 12.0 以降の場合。
- スクリーンタイム：ユーザーがスクリーンタイムを有効にできないようにします。iOS 12.0 以降の場合。
- **SIM** のセットアップ：ユーザーが通信プランを設定できないようにします。iOS 12.0 以降の場合。
- **iMessage & FaceTime**：ユーザーが iMessage と FaceTime を有効にできないようにします。iOS 12.0 以降の場合。
- 外観：ユーザーが外観モードを選択できないようにします。iOS 13.0 以降の場合。
- ようこそ：ユーザーに ［開始］画面が表示されないようにします。iOS 13.0 以降の場合。
- 復元が完了しました：セットアップ中に復元が完了したかどうかをユーザーが確認できないようにします。iOS 14.0 以降の場合。
- 更新が完了しました：セットアップ中にソフトウェアの更新が完了したかどうかをユーザーが確認できないようにします。iOS 14.0 以降の場合。
- **App Store**：ユーザーが App Store を設定できないようにします。iOS 11.1 以降の場合。

アカウントを表示するには、［設定］**>** ［**Apple Deployment Program**］に移動します。

8. ［**macOS** 設定アシスタントのオプション］で、ユーザーが初めてデバイスを起動するときにスキップする macOS セットアップアシスタントの手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。これらの機能へのアクセスを完全に制限しない限り、ユーザーはセットアップの完了後にスキップされた機能を構成できます。機能へのアクセスの制限について詳しくは、「制限デバイスポリシー」を参照してください。すべての項目は、デフォルトで選択が解除されています。以下の説明では、設定が選択されたときに何が起こるかについて解説しています。



- 新規としてセットアップまたは復元：ユーザーがデバイスを新規または Time Machine バックアップから設定したり、システム移行を実行したりできないようにします。
- 位置情報サービス：ユーザーがデバイスで位置情報サービスを設定できないようにします。macOS 10.11 以降の場合。
- **Apple ID**：ユーザーがデバイスの管理対象 Apple ID アカウントを設定できないようにします。
- 使用条件：ユーザーがデバイスの使用契約条件を読んで承諾できないようにします。
- **Siri**：ユーザーが Siri を構成できないようにします。macOS 10.12 以降の場合。
- **FileVault**： FileVault を使用して起動ディスクを暗号化します。Citrix Endpoint Management が FileVault の設定を適用するのは、ローカルユーザーアカウントがシステムに 1 つで、そのアカウントが iCloud にサインインしている場合のみです。

  macOS の FileVault ディスク暗号化機能を使ってコンテンツを暗号化し、システムボリュームを保護します（https://support.apple.com/en-us/HT204837）。FileVault がオンになっていない旧モデルのポータブル Mac でセットアップアシスタントを実行すると、この機能を有効にするように求められることがあります。このプロンプトは、新しいシステムと OS X 10.10 または 10.11 にアップグレードされたシステムの両方に表示されますが、システムのローカル管理者アカウントが 1 つで、そのアカウントが iCloud にサインインしている場合にのみ表示されます。
- **App Analytics**：ユーザーがクラッシュデータおよび使用状況の統計情報を Apple と共有するかどうかを設定できないようにします。
- プライバシー：ユーザーが［データおよびプライバシー］ペインを確認できないようにします。macOS 10.13 以降の場合。

- **iCloud Analytics**：ユーザーが iCloud 診断データを Apple に送信するかどうかを選択できないようにします。macOS 10.13 以降の場合。
- **iCloud** の“書類”と”デスクトップ”：ユーザーが iCloud の書類とデスクトップを設定できないようにします。macOS 10.13 以降の場合。
- 外観：ユーザーが外観モードを選択できないようにします。macOS 10.14 以降の場合。
- アクセシビリティ：ユーザーがボイスオーバーを自動的に聞くことができないようにします。デバイスがイーサネットに接続されている場合にのみ使用できます。macOS 11 以降の場合。
- 生体認証：ユーザーが Touch ID と Face ID を設定できないようにします。macOS 10.12.4 以降の場合。
- **True Tone**：ユーザーが 4 チャネルセンサーを設定して、ディスプレイのホワイトバランスを動的に調整できないようにします。macOS 10.13.6 以降の場合。
- **Apple Pay**：ユーザーが Apple Pay を設定できないようにします。この設定がオフになっている場合、ユーザーは Touch ID と Apple ID を設定する必要があります。**Apple ID** および生体認証の設定がオフになっていることを確認してください。
- スクリーンタイム：ユーザーがスクリーンタイムを有効にできないようにします。macOS 10.15 以降の場合。
- **App Store**：ユーザーが App Store をセットアップできないようにします。macOS 11.1 以降の場合。
- **Apple Watch** によるロック解除：ユーザーが Apple Watch で Mac のロックを解除できないようにします。macOS 12 以降の場合。
- ローカルアカウントのセットアップオプション：デバイスでアカウントを作成する設定を指定します。Citrix Endpoint Management は、ここで指定された情報を使用して最初にローカル管理者アカウントを作成します。ユーザーがデバイスをアクティブ化すると、ユーザーアカウントがプライマリアカウントとして作成されます。［標準ユーザーとしてプライマリアカウントを作成します］オプションで、プライマリアカウントに管理者権限を付与するかどうかを決定します。

> 重要：
>
> ［**macOS** 設定］ページで、［セットアップを完了するため構成を待機する］を ［オン］に設定した後でのみ、［標準ユーザーとしてプライマリアカウントを作成する］を選択できます。

- 標準ユーザーとしてプライマリアカウントを作成します：これを選択すると、Citrix Endpoint Management によってデバイスのユーザー管理者権限ではなく標準権限を持つユーザーが作成されます。デバイスのユーザー管理者権限を付与する場合は、このオプションをスキップしてください。デフォルトではこのオプションは選択されていません。
- 管理者のフルネーム：管理者アカウントに対してシステムに表示される名前を入力します。
- 管理者の短い名前：デバイスやシェルに表示されるホームフォルダーの名前を入力します。
- 管理者パスワード：管理者アカウント用の安全なパスワードを入力します。

- ユーザーおよびグループで管理者アカウントを表示する：これがオフになっている場合、管理者アカウントは macOS 設定の ［ユーザーとグループ］に表示されません。プライマリアカウントを標準ユーザーとして作成する場合は、この設定を有効にして、Citrix Endpoint Management が最初に作成する管理者アカウントを非表示にします。

セキュリティを強化するために、Citrix Endpoint Management は、管理者アカウントのパスワードをローテーションするかどうかを毎日チェックします。デフォルトでは、Citrix Endpoint Management は 7 日ごとにパスワードをローテーションします。デフォルトを変更するには、`mac.dep.admin.passwd.rotate`サーバーのプロパティを更新します。詳しくは、「サーバープロパティ」を参照してください。

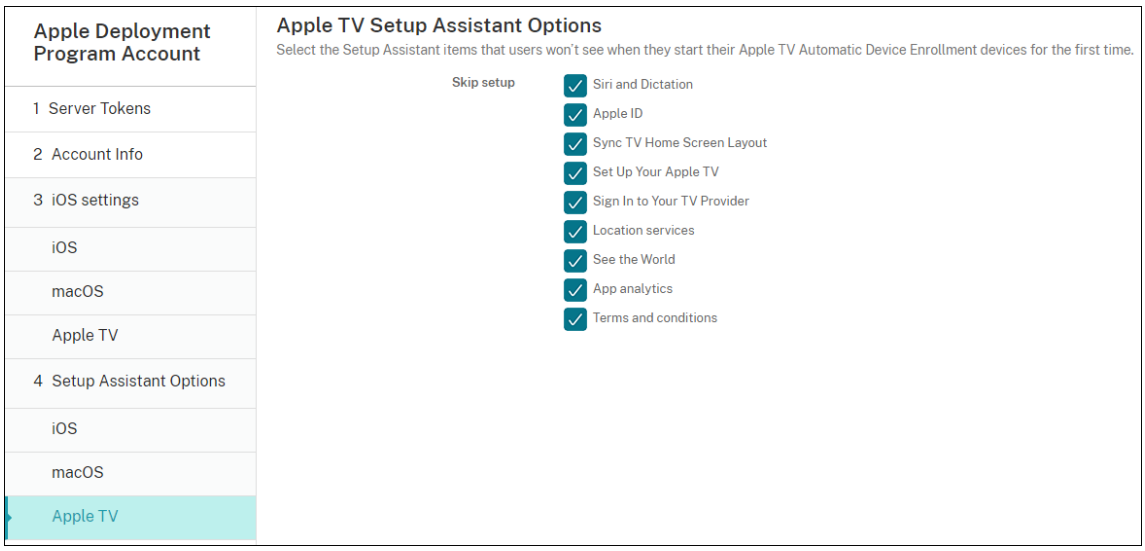
パスワードの安全性とセキュリティを強化するために、Citrix Endpoint Management は次のようにパスワードを生成します：

- 長さ 12 文字
- 大文字 3 文字
- 小文字 3 文字
- 3 つの数字
- 3 つの特殊文字：`! \@ \\# \$ % \\^ \* ? + = -`

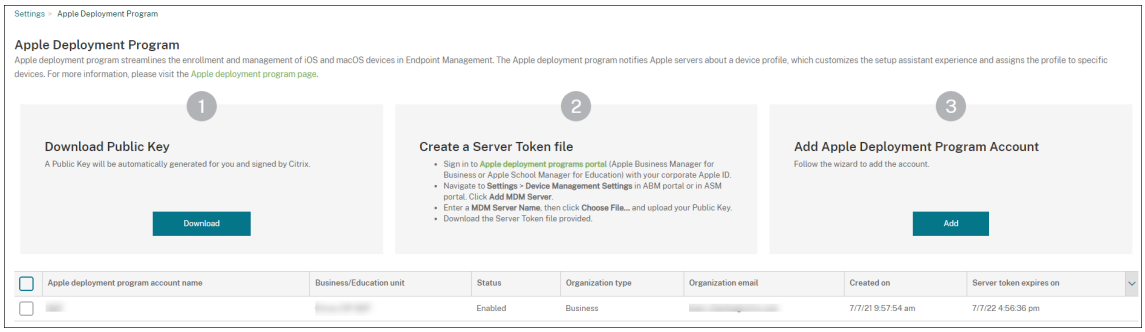
デバイスの以前のパスワード、現在のパスワード、パスワード変更ステータスを表示するには、［管理］**>**［デバイス］の順に移動します。そのデバイスをクリックし、［詳細表示］をクリックしてから、［デバイス詳細］**>**［全般］ページを表示します。［セキュリティ］セクションには、以下が表示されます：

- 以前の管理者パスワード：以前のパスワードを表示できます。Citrix Endpoint Management は、最新のパスワードのみを表示します。［パスワードの表示］をクリックして、パスワードを表示します。
- 現在の管理者パスワード：現在のパスワードを表示できます。
- 管理者パスワードの変更：パスワードの変更ステータスを表示できます。実際のステータスによっては、次の情報が表示される場合があります：
  - < 特定の時間（値）> にパスワードの変更が要求されました。
  - < 特定の時間（値）> にパスワードが変更されました。
  - < 特定の時間（値）> にパスワードの変更に失敗しました。
  - パスワードはまだ変更されていません。

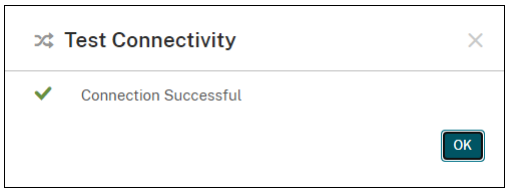
9. ［**Apple TV** 設定アシスタントのオプション］で、ユーザーが初めてデバイスを起動して使用するときにスキップできる Apple TV 設定アシスタントの手順を選択します。すべての項目は、デフォルトで選択が解除されています。変更を保存します。



10. アカウントを表示するには、［設定］**>** ［**Apple Deployment Program**］に移動します。Citrix Endpoint Management と Apple 間の接続をテストするには、アカウントを選択して ［接続性をテスト］をクリックします。



状態を示すメッセージが表示されます。



デバイスの注文

以下のチャネルからデバイスを直接注文できます:

- Apple。Apple の顧客番号を販売者に提供します。
- Apple 正規販売代理店または通信事業者。販売者に組織 ID を提供し、その販売店 ID を取得します。

デバイスサプライヤーの管理について詳しくは、「Apple Business Manager ユーザガイド」または「Apple School Manager ユーザガイド」を参照してください。

注文の発送後、購入した Apple デバイスが ABM または ASM アカウントに追加されます。

デバイスの **Citrix Endpoint Management** への割り当て

ABM または ASM ポータルで、注文番号を検索し、注文番号を使用して、この注文のデバイスを Citrix Endpoint Management に割り当てます。デバイスの購入場所に関係なく、Apple Configurator 2 を使用して、iPhone、iPad、iPod touch、および Apple TV デバイスを ABM または ASM に追加することもできます。

詳しくは、「Apple Business Manager ユーザガイド」または「Apple School Manager ユーザガイド」を参照してください。

コンテンツの一括購入と **Citrix Endpoint Management** への同期

ABM と ASM を使用すると、単一の組織アカウントで、アプリやブックのライセンスを一括購入、配信、および管理できます。Citrix Endpoint Management が ABM または ASM と通信して配信用のライセンス情報を取得できるようにするには、次の手順を実行します:

1. ABM または ASM ポータル内の、［アプリとブック］で公開アプリやブックを購入し、［カスタムアプリ］で Citrix Endpoint Management 用に開発されたカスタムアプリを購入します。
2. ABM または ASM ポータルで、Citrix Endpoint Management に割り当てられたコンテンツトークンをダウンロードします。

   手順 1 と 2 について詳しくは、「Apple Business Manager ユーザガイド」または「Apple School Manager ユーザガイド」を参照してください。
3. Citrix Endpoint Management コンソールで、ダウンロードしたコンテンツトークンに基づいて一括購入アカウントを作成します。

   詳しくは、「Apple の一括購入を使用したアプリの追加」を参照してください。

   一括購入アカウントが作成されると、購入したアプリとブックが［管理］>［アプリ］に表示され、Citrix Endpoint Management サーバーに割り当てられたデバイスが ［管理］**>**［デバイス］に表示されます。

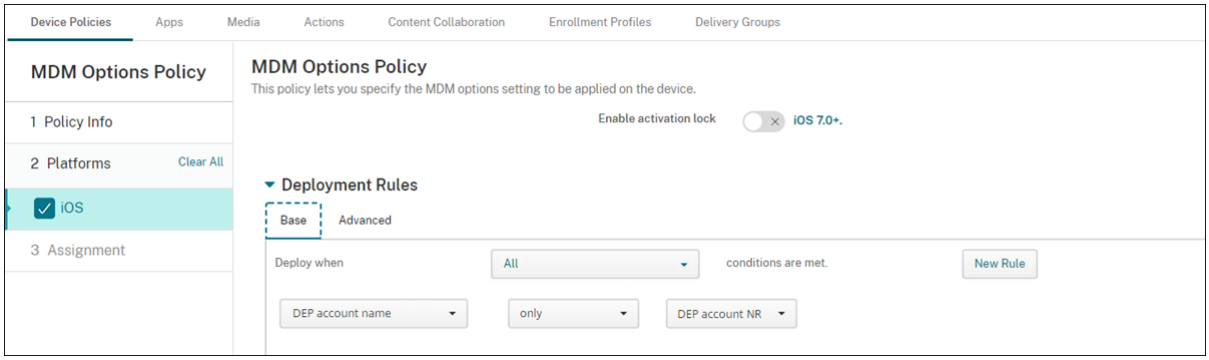
デバイスポリシーの展開規則およびアプリの構成

デバイスポリシーとアプリを構成するとき、ABM または ASM アカウントをさまざまなデバイスポリシーとアプリに関連付けることができます。

1. ［構成］**>**［デバイスポリシー］ページと ［構成］**>**［アプリ］ページで、［展開規則］を開きます。
2. 特定の ABM アカウント、または選択したアカウントを除くすべての ABM アカウントに、ポリシーまたはアプリが展開されるように指定します。

ABM アカウントの一覧には、ステータスが有効または無効のアカウントのみが含まれます。ABM アカウントが無効の場合、ABM デバイスはこのアカウントに属しません。このため、Citrix Endpoint Management ではこれらのデバイスにアプリまたはポリシーが展開されません。

以下の例では、デバイスポリシーを、ABM アカウント名が「ABM Account NR」に設定されているデバイスのみに展開するように構成しています。



Apple デバイスの一括登録

March 15, 2024

次の 2 つの方法で多数の iOS デバイス、iPadOS デバイス、macOS デバイスを Citrix Endpoint Management に登録できます。

- Apple Deployment Programs（ADP）を使用して、Apple、Apple 正規販売代理店、または通信事業者から直接購入した Apple デバイスを登録する。

  ADP 対応デバイスの展開について詳しくは、「Apple Deployment Programs でのデバイスの展開」を参照してください。この記事では、ユーザーが ADP 対応デバイスを登録する方法と、デバイスを再登録する方法について説明します。

- Apple から直接購入したかどうかに関係なく、Apple Configurator 2 を使用して iOS デバイスを登録する。

この記事では、Apple Configurator 2 を使用してデバイスを一括展開する方法について説明します。

一括登録について

ADP には、企業向けの Apple Business Manager（ABM）と、教育機関向けの Apple School Manager（ASM）が含まれます。ADP を使用した一括登録には、以下の特徴があります：

- 実物のデバイスを直に設定つまり準備する必要はありません。
- Citrix Endpoint Management の展開設定が完了すると、ユーザーは、登録されたデバイスをすぐに使い始めることができます。

- セットアップアシスタントの手順の一部を省くことで、ユーザーのセットアッププロセスを簡素化できます。
- ABM および ASM のセットアップについて詳しくは、Apple Business ManagerおよびApple School Managerで入手可能なドキュメントを参照してください。

Apple Configurator 2 を使用した一括登録には、以下の特徴があります:

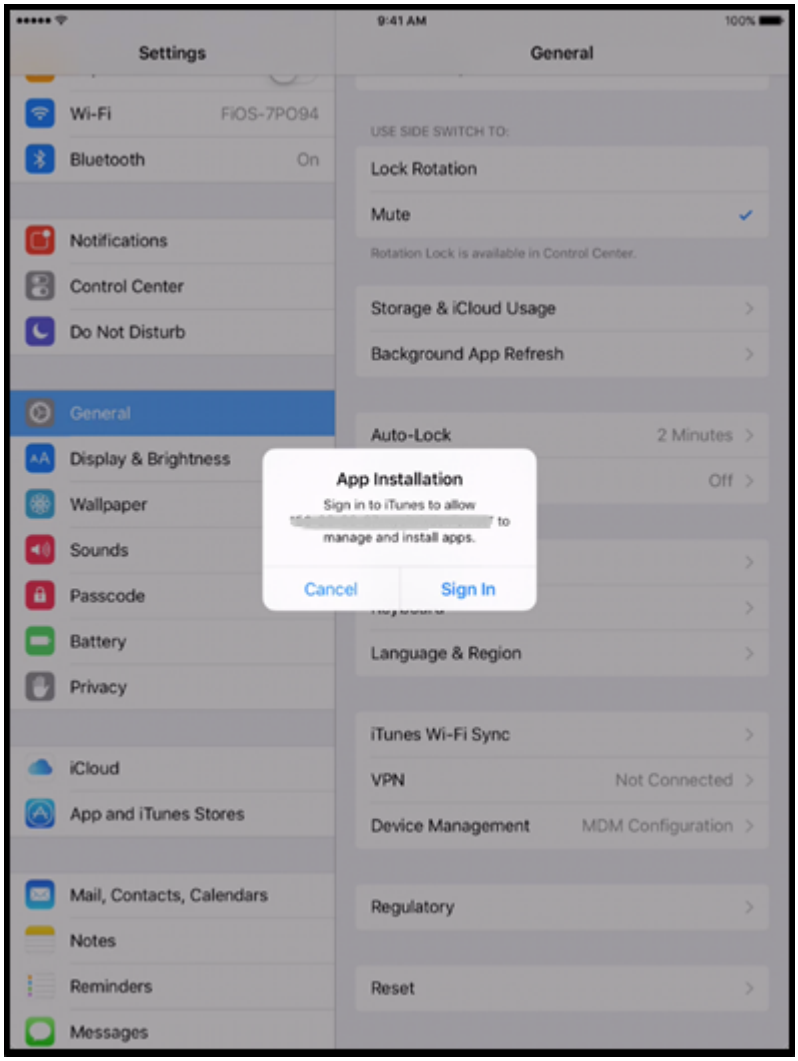
- macOS 10.7.2 以降および Apple Configurator 2 アプリが動作する Mac に iOS デバイスを接続します。Apple Configurator 2 を介して iOS デバイスを準備しポリシーを構成します。
- デバイスは、セットアッププロセス中に Citrix Endpoint Management に自動的に登録されます。セットアップが完了すると、Citrix Endpoint Management はポリシー、アプリ、その他のリソースをデバイスにプッシュします。その後、デバイスの管理を開始できます。
- Apple Configurator 2 の使用について詳しくは、「Apple Configurator ヘルプ」を参照してください。

ユーザーが **ADP** 対応デバイスを登録する方法

ユーザーは、次のようにデバイスを Citrix Endpoint Management に登録します:

1. ユーザーがデバイスを起動します。
2. Citrix Endpoint Management は、[設定] **>** [**Apple Deployment Programs**] ページで構成した ADP 設定をデバイスに配信します。
3. ユーザーのデバイスで初期設定を構成します。
4. デバイスが自動的に Citrix Endpoint Management デバイス登録処理を開始します。
5. ユーザーのデバイスでその他の初期設定を続行します。
6. ホーム画面では、ユーザーが Citrix Secure Hub をダウンロードできるように、Apple App Store へのサインインを求められることがあります。

   > 注:
   >
   > Citrix Endpoint Management が、デバイスベースの一括購入アプリの割り当てを使用して Citrix Secure Hub アプリを展開するように設定されている場合、この手順は省略可能です。この場合、Apple App Store アカウントを作成、または既存のアカウントを使用する必要はありません。



7. Citrix Secure Hub を開いて資格情報を入力します。ポリシーにより求められる場合、Citrix PIN を作成して検証するよう求めるメッセージが表示されることがあります。

   Citrix Endpoint Management が残りの必要なアプリをデバイスにすべて展開します。

ADP 対応デバイスの再登録

ADP 対応デバイスは、工場出荷時のリセット状態で登録します。ADP 対応デバイスを再登録するには、最初にフルワイプを完了してデバイスの登録を解除する必要があります。詳細な手順は次のとおりです:

1. [管理] **>** [デバイス] ページで、デバイスを選択します。
2. [**Security**] をクリックします。
3. [完全なワイプ] をクリックして、デバイスの登録を解除して工場出荷時のリセット状態にします
4. デバイスを起動します。

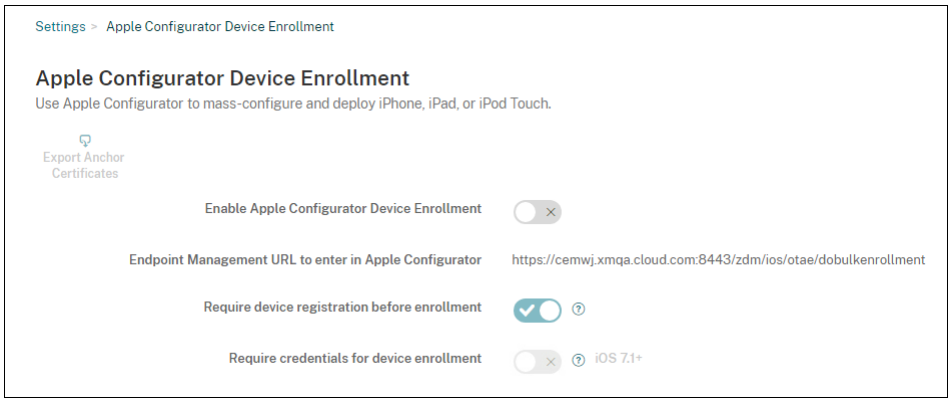
> 重要:
>
> ADP を登録するためにはデバイスが工場出荷時のリセット状態である必要があるため、ADP 対応デバイスの登録を解除するのに ［選択的なワイプ］を使用しないでください。

Apple Configurator 2 を使用したデバイスの展開

Apple Configurator 2 を使用して、設定、アプリ、およびデータを含む多数のデバイスを展開し、これらのデバイスを Citrix Endpoint Management に登録できます。

手順 **1**: **Citrix Endpoint Management** で設定を構成する

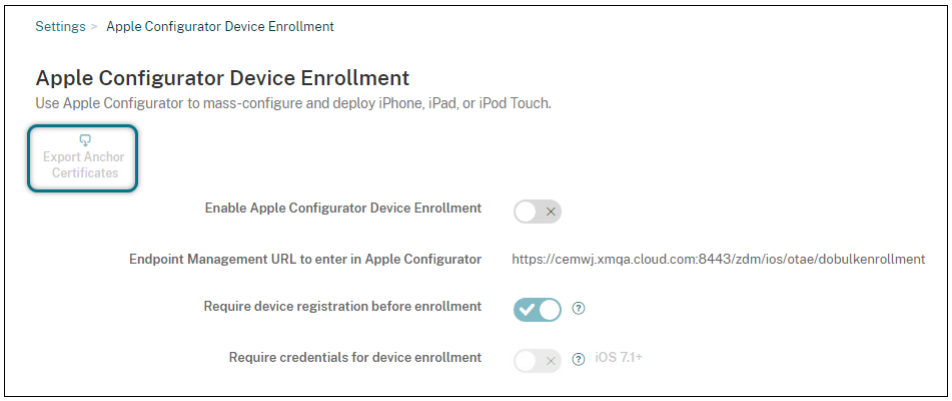
1. Citrix Endpoint Management コンソールで、［設定］**>** ［**Apple Configurator** デバイス登録］の順に選択します。



2. ［**Apple Configurator** デバイス登録を有効にする］を ［はい］に設定します。
3. Apple Configurator 2 で設定を構成するときに、［**Apple Configurator** で入力する登録 **URL**］設定の値をコピーして、この URL を貼り付けます。この設定によって、Apple と通信する Citrix Endpoint Management サーバーの URL が提供されます。登録用 URL は、Citrix Endpoint Management サーバーの完全修飾ドメイン名（FQDN。`mdm.server.url.com`など）または IP アドレスです。
4. 認識のないデバイスが登録されないようにするには、［登録前にデバイスの登録が必要です］を ［はい］に設定します。注: この設定が ［はい］の場合、登録前に Citrix Endpoint Management の ［管理］**>** ［デバイス］から手動で行うか、CSV ファイルを使用して、設定済みのデバイスを追加する必要があります。
5. iOS デバイスのユーザーに対して、登録時に資格情報の入力を要求するには、［デバイス登録のための資格情報を求める］を ［はい］に設定します。デフォルトは ［いいえ］です。

> 注:
>
> Citrix Endpoint Management サーバーで信頼済みの SSL 証明書を使用する場合は、この手順はスキ

> ップしてください。［アンカー証明書のエクスポート］をクリックして、certchain.pem ファイルを macOS キーチェーン（ログインまたはシステム）に保存します。



手順 **2**：**Apple Configurator 2** で設定を構成する

1. macOS 10.7.2 以降を実行し、Apple Configurator 2 がインストールされている Mac を準備します。
2. Dock コネクタ USB ケーブルを使用して、Apple デバイスを Mac に接続します。最大 30 台の接続デバイスを同時に構成できます。Dock コネクタがない場合は、1 台または複数の Powered USB 2.0 高速ハブを使用してデバイスを接続します。
3. Apple Configurator 2 を起動します。監視の準備が整っているデバイスが Configurator に表示されます。
4. デバイスの監視の準備を行うには：
   - 構成を定期的に再適用することによってデバイスを管理する場合は、［**Supervise devices**］を選択します。［次へ］をクリックします。

     > 重要：
     >
     > デバイスを Supervised モードにすると、特定のバージョンの iOS がデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリがデバイスから完全に消去されます。

   - 最新バージョンの iOS をインストールする場合、［iOS］ボックスの一覧で ［**Latest**］を選択します。
5. ［**Enroll in MDM Server**］で MDM サーバーを選択します。サーバーを追加するには、［**Next**］をクリックします。
6. ［**Define an MDM server**］にサーバーの名前を指定し、Citrix Endpoint Management コンソールから MDM サーバーの URL を貼り付けます。
7. ［**Assign to organization**］で、デバイスを監視する組織を選択します。

   Apple Configurator 2 を使用したデバイスの準備について詳しくは、Apple Configurator のヘルプページ「デバイスを準備する」を参照してください。

8. 準備ができたデバイスから電源を入れて iOS 設定アシスタントを開始し、初回使用のためにデバイスを準備します。

Apple Configurator 2 を使用した **ABM** または **ASM** へのデバイスの追加

デバイスの購入場所に関係なく、Apple Configurator 2 を使用して、iPhone、iPad、および Apple TV デバイスを ABM または ASM アカウントに追加することができます。
デバイスを追加すると、[**Devices**] セクションに表示されます。これらのデバイスには、Apple Configurator 2 を通じて割り当てられた登録設定が含まれなくなりました。詳しくは、「Apple Business Manager ユーザガイド」または「Apple School Manager ユーザガイド」を参照してください。

ADP トークンの更新

ADP トークンの有効期限が切れると、Citrix Endpoint Management はライセンスの有効期限の警告を表示します。ASM または ABM でトークンを置き換えます。

手順 **1**: **Citrix Endpoint Management** サーバーから公開キーをダウンロードします

1. Citrix Endpoint Management コンソールで、[設定] **>** [**Apple Deployment Program**] に移動して新しい公開キーをダウンロードします。

手順 **2**: **Apple** アカウントからサーバートークンファイルを作成してダウンロードします

1. ABM にサインインしてトークンをダウンロードします。
2. [設定] を開いてトークンが必要なサーバーを選択します。[編集] をクリックします。
3. [**MDM Server Settings**] で、Citrix Endpoint Management からダウンロードした新しい公開キーをアップロードして、変更を保存します。
4. [トークンのダウンロード] をクリックして新しいトークンをダウンロードします。

手順 **3**: **Citrix Endpoint Management** にサーバートークンファイルをアップロードします

1. Citrix Endpoint Management で、[設定] **>** [**Apple Deployment Program**] の順に移動します。
2. Deployment Program アカウントを選択して、[編集] をクリックし、サーバートークンファイルをアップロードします。
3. [次へ] をクリックして変更を保存します。

Apple Education 機能との統合

November 29, 2023

Apple Education を使用する環境で、Citrix Endpoint Management をモバイルデバイス管理（MDM）ソリューションとして使用できます。Citrix Endpoint Management のサポートには、Apple School Manager（ASM）や iPad 用のクラスルームアプリが含まれています。Citrix Endpoint Management の教育の構成デバイスポリシーでは、Apple Education を使用する講師および生徒のデバイスを構成します。

講師と生徒には事前に構成された監視対象 iPad が提供されます。この構成には、Citrix Endpoint Management での ASM の登録、新しいパスワードで構成された管理対象 Apple ID アカウント、および必須の一括購入アプリと iBooks が含まれます。

Apple の教育向け機能について詳しくは、Apple の「教育」サイトおよび同サイトの「教育用導入ガイド」を参照してください。

Apple School Manager

Citrix Endpoint Management を ASM と統合するには、次の一般的な手順に従います。

1. ASM で所属機関のアカウントを作成して、所属機関を ASM に登録します。
2. Apple School Manager の教育用一括購入アカウントを構成します。
3. Apple School Manager ユーザーのパスワードを追加します。
4. リソースとデリバリーグループを計画して Citrix Endpoint Management に追加します。
5. 講師および生徒のデバイス登録をテストします。
6. 事前に構成されたデバイスを講師と生徒に提供します。
7. 講師、生徒、およびクラスのデータの管理
8. デバイスの紛失または盗難が発生した場合は、デバイスをロックしたり検索したりすることができます。

ASM への登録、およびアカウントと Citrix Endpoint Management の接続については、「Apple Deployment Program でのデバイスの展開」を参照してください。

前提条件

- Citrix Gateway
- MDM+MAM 用に構成された登録プロファイル。
- Apple iPad 第 3 世代（最小バージョン）、または iOS 9.3（最小バージョン）を実行する iPad Mini

> 注:
>
> Citrix Endpoint Management は、LDAP または Active Directory に対する ASM ユーザーアカウントの検証を行いません。ただし、Citrix Endpoint Management を LDAP または Active Directory に接続して、ASM の講師や生徒と関連付けられていないユーザーとデバイスを管理できます。たとえば、Active Directory を使用して、そのほかの ASM メンバー（IT 管理者やマネージャーなど）に Citrix Secure Mail と Citrix Secure Web を提供できます。
>
> ASM の講師と生徒はローカルユーザーであるため、彼らのデバイスに Citrix Secure Hub を展開する必要はありません。
>
> Citrix Gateway の認証を含む MAM 登録では、ローカルユーザーはサポートされません（Active Directory ユーザーのみ）。このため、Citrix Endpoint Management は講師と生徒のデバイスに必須の一括購入アプリと iBooks のみを展開します。

iPad 用クラスルームアプリ

iPad 用クラスルームアプリを使用すると、講師は生徒のデバイスに接続してデバイスを管理できます。デバイス画面を表示したり、iPad でアプリを開いたり、Web リンクを共有して開いたり、生徒の画面を Apple TV に表示したりすることができます。

クラスルームアプリは、App Store で無料で入手できます。Citrix Endpoint Management コンソールにアプリをアップロードします。次に教育の構成デバイスポリシーを使用して、講師のデバイスに展開するクラスルームアプリを構成します。

クラスルームアプリを展開する方法について詳しくは、「Apple アプリの配布」を参照してください。

クラスルームアプリの要件、セットアップ、機能について詳しくは、Apple サポートサイトのクラスルームユーザーガイドを参照してください。

Apple School Manager ユーザーのパスワードの追加

ASM アカウントが追加されると、Citrix Endpoint Management が ASM からクラスとユーザーをインポートします。Citrix Endpoint Management はクラスをローカルグループとして扱い、コンソール内で「グループ」の用語が使用されます。ASM でグループ名があるクラスには、Citrix Endpoint Management によってグループ名が割り当てられます。それ以外の場合、Citrix Endpoint Management ではグループ名にソースシステム ID を使用します。ASM のコース名は一意でないため、Citrix Endpoint Management ではクラス名にコース名を使用しません。

Citrix Endpoint Management は管理対象 Apple ID を使用して、ユーザーの種類が **ASM** のローカルユーザーを作成します。ASM では、すべての外部データソースとは別に資格情報が作成されるため、ユーザーはローカルです。そのため、Citrix Endpoint Management ではこれらの新しいユーザーの認証にディレクトリサーバーを使用しません。

ASM は、一時的なユーザーパスワードを Citrix Endpoint Management に送信しません。CSV ファイルからインポートするか、手動で追加します。一時的なユーザーパスワードをインポートするには、次の手順を実行します:

1. 管理対象 Apple ID の一時的なパスワードを作成するときに ASM によって生成された CSV ファイルを取得します。
2. CSV ファイルを編集し、一時的なパスワードを、Citrix Endpoint Management への登録でユーザーが入力した新しいパスワードに置き換えます。この目的では、パスワードの種類に対する制約はありません。

   以下の形式で CSV ファイルに入力します: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   場所:

   ユーザー: `user@appleid.citrix.com`

   名: `Firstname`

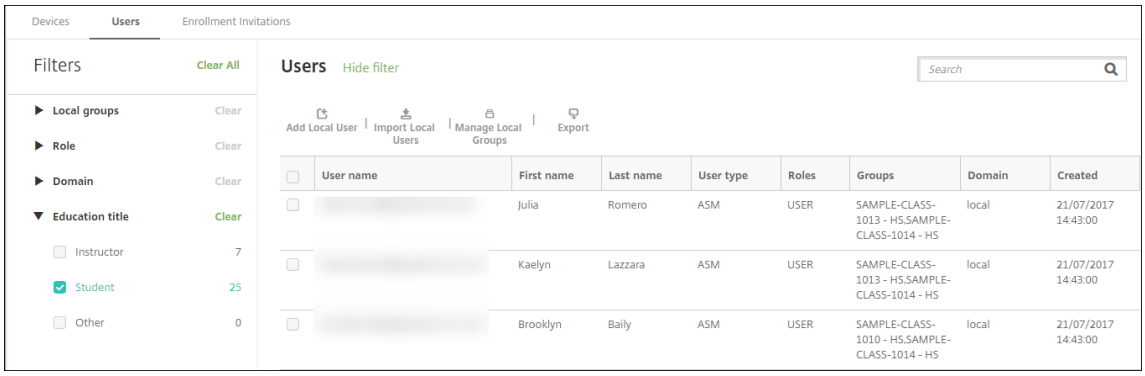
   ミドルネーム: `Middle`

   姓: `Lastname`

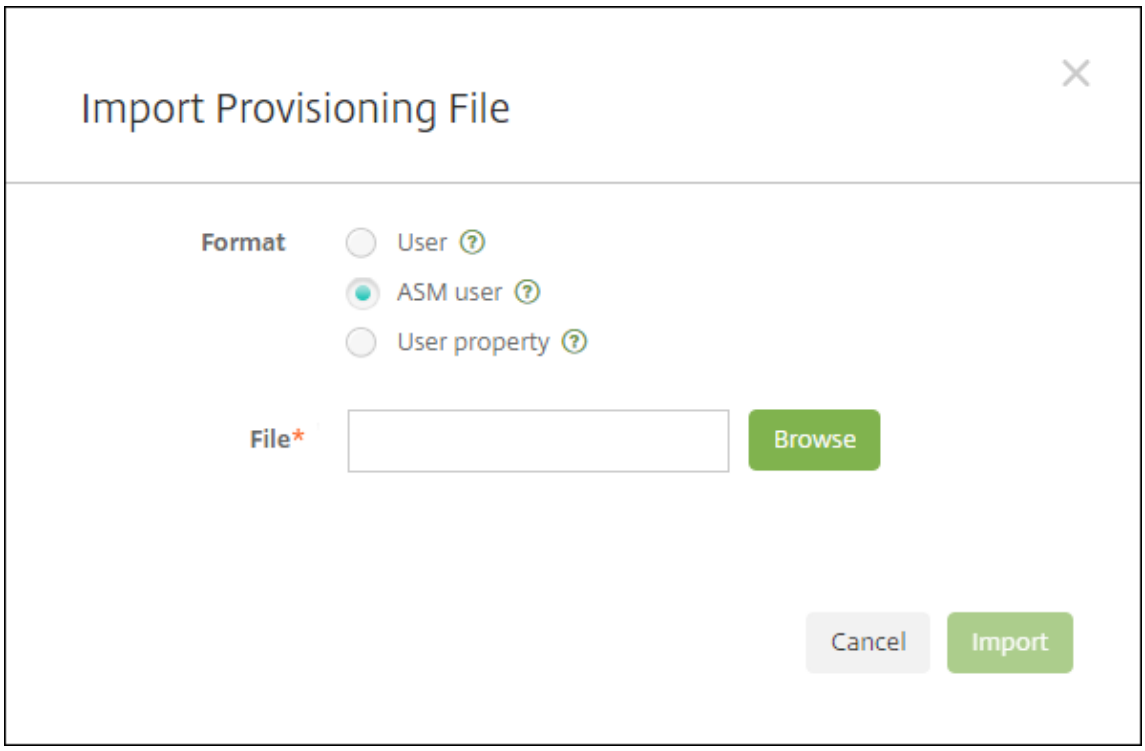
   パスワード: `Password123!`
3. Citrix Endpoint Management コンソールで、[管理] **>** [ユーザー] の順にクリックします。[ユーザー] ページが開きます。

   次の [管理] **>** [ユーザー] 画面の例では、ASM からインポートされたユーザー一覧が表示されています。[ユーザー] 一覧には以下のように表示されます。

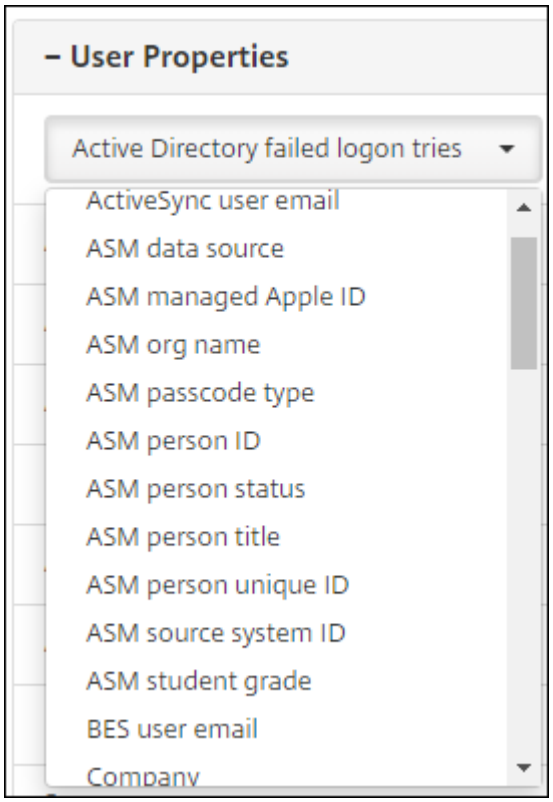
   - [ユーザー名] には管理対象 Apple ID が表示されます。
   - [ユーザーの種類] の **ASM** は、ASM 由来のアカウントであることを示しています。
   - [グループ] にはクラスが表示されます。



4. [ローカルユーザーのインポート] をクリックします。[プロビジョニングファイルのインポート] ダイアログボックスが開きます。
5. [形式] では [**ASM** ユーザー] を選択し、手順 2 で準備した CSV ファイルに移動して、[インポート] をクリックします。



6. ローカルユーザーのプロパティを表示するには、該当するユーザーを選択して ［編集］をクリックします。



name プロパティに加えて、次の ASM プロパティを使用できます:

- **ASM** のデータソース：クラスのデータソース（**CSV** または **SFTP** など）です。
- **ASM** の管理対象 **Apple ID**：管理対象 Apple ID には、所属機関名と`appleid`を含めることができます。たとえば、ID は johnappleseed@appleid.myschool.edu のようになります。Citrix Endpoint Management では、管理対象 Apple ID の認証が要求されます。
- **ASM** 組織名： Citrix Endpoint Management でアカウントに付けた名前です。
- **ASM** のパスコードの種類：複合（8 つ以上の英数字で構成された生徒以外のパスワード）、**4**（桁）、または **6**（桁）の、個人のパスワードポリシーです。
- **ASM** の一意の個人 **ID**：ユーザーの識別子です。
- **ASM** の個人の状態：管理対象 Apple ID がアクティブか非アクティブかを指定します。管理対象 Apple ID アカウントにユーザーが新しいパスワードを入力すると、この状態がアクティブになります。
- **ASM** の個人の役職：講師、生徒、そのほかのいずれかです。
- **ASM** の一意の個人 **ID**：ユーザーの識別子です。
- **ASM** ソースシステム **ID**：システムソースの識別子です。
- **ASM** の生徒の学年：生徒の学年情報です（講師は使用しません）。

リソースとデリバリーグループの計画と **Citrix Endpoint Management** への追加

デリバリーグループで、ユーザーのカテゴリに展開するリソースを指定できます。たとえば、講師と生徒のデリバリーグループを 1 つ作成できます。または、複数のデリバリーグループを作成して、さまざまな講師や生徒に送信するアプリ、メディア、ポリシーをカスタマイズできます。クラスごとに 1 つまたは複数のデリバリーグループを作成できます。また、マネージャー（教育機関のそのほかの職員）のデリバリーグループを 1 つまたは複数作成することもできます。

ユーザーデバイスに展開するリソースには、デバイスポリシー、一括購入アプリ、および iBooks が含まれます。

- デバイスポリシー：

  講師がクラスルームアプリを使用する場合は、教育の構成デバイスポリシーが必要です。そのほかのデバイスポリシーを確認して、講師と生徒の iPad をどのように構成および制限するかを決定します。

- 一括購入アプリ：

  Citrix Endpoint Management では、一括購入アプリを必須アプリとして教育ユーザーに展開する必要があります。Citrix Endpoint Management では、このような一括購入アプリをオプションとして展開することはサポートされません。

  Apple のクラスルームアプリを使用する場合は、講師のデバイスにのみ展開します。

  講師や生徒に提供するそのほかのアプリを展開します。このソリューションでは Citrix Secure Hub アプリを使用しないため、講師や生徒に展開する必要はありません。

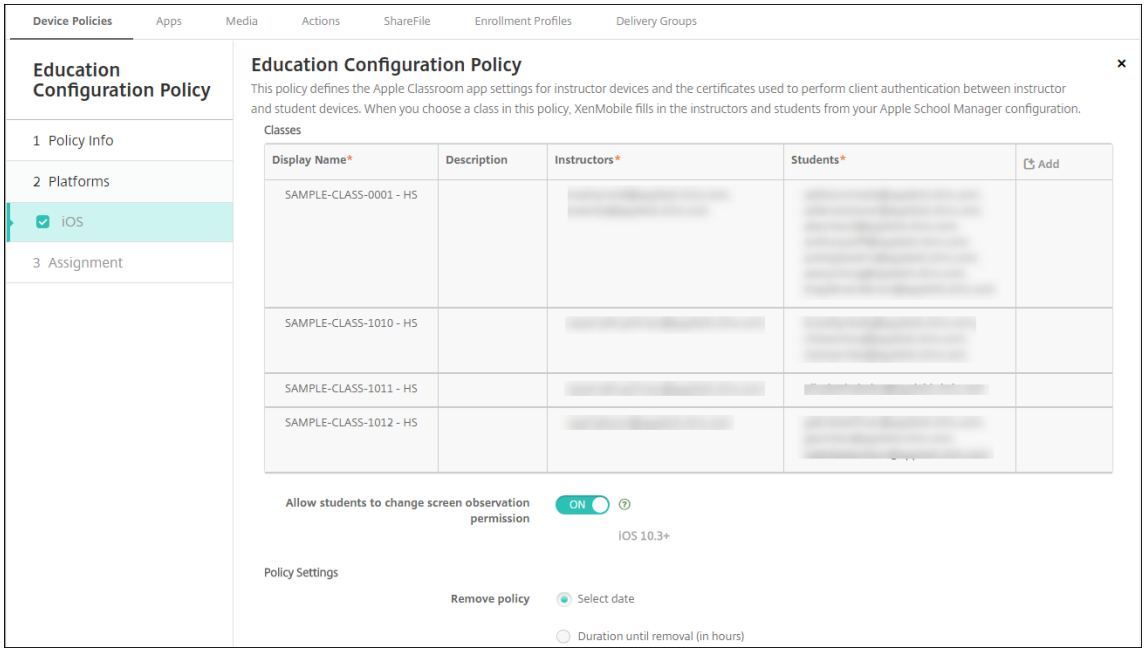
- 一括購入 iBooks：

  Citrix Endpoint Management Server を ASM アカウントに接続すると、Citrix Endpoint Management コンソールの ［構成］**>**［メディア］に、購入した iBooks が表示されます。このページに一覧表示された

iBooks を、デリバリーグループに追加できます。Citrix Endpoint Management では、iBooks を必須メディアとしてのみ追加できます。

講師および生徒のリソースとデリバリーグループを計画したら、Citrix Endpoint Management コンソールでこれらのアイテムを作成できます。

1. 講師または生徒のデバイスに展開するデバイスポリシーを作成します。教育の構成デバイスポリシーについて詳しくは、「教育の構成デバイスポリシー」を参照してください。

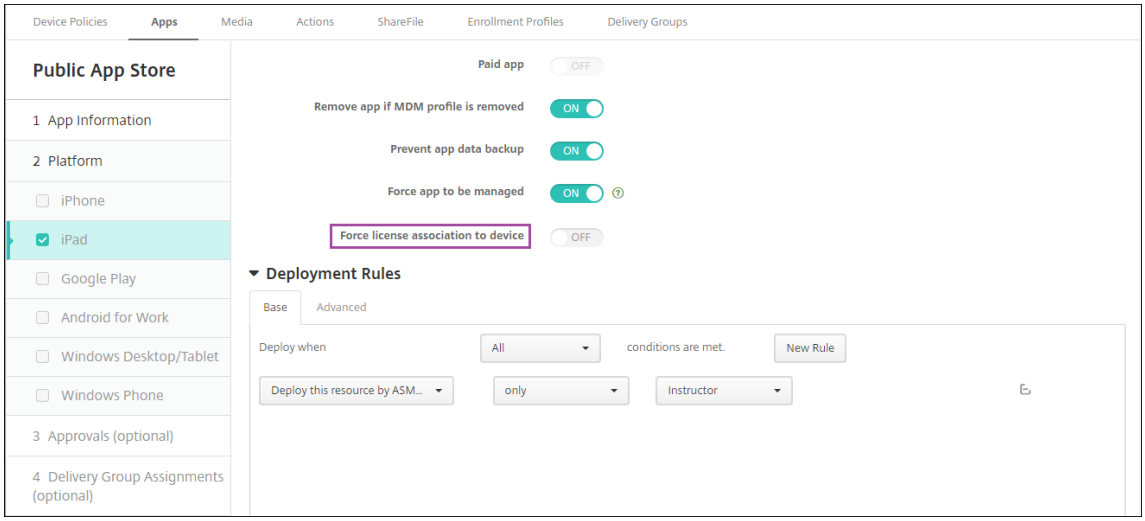


デバイスポリシーについて詳しくは、「デバイスポリシー」および個々のポリシーに関する記事を参照してください。

2. アプリ（[構成] > [アプリ]）と iBooks（[構成] > [メディア]）を構成します。

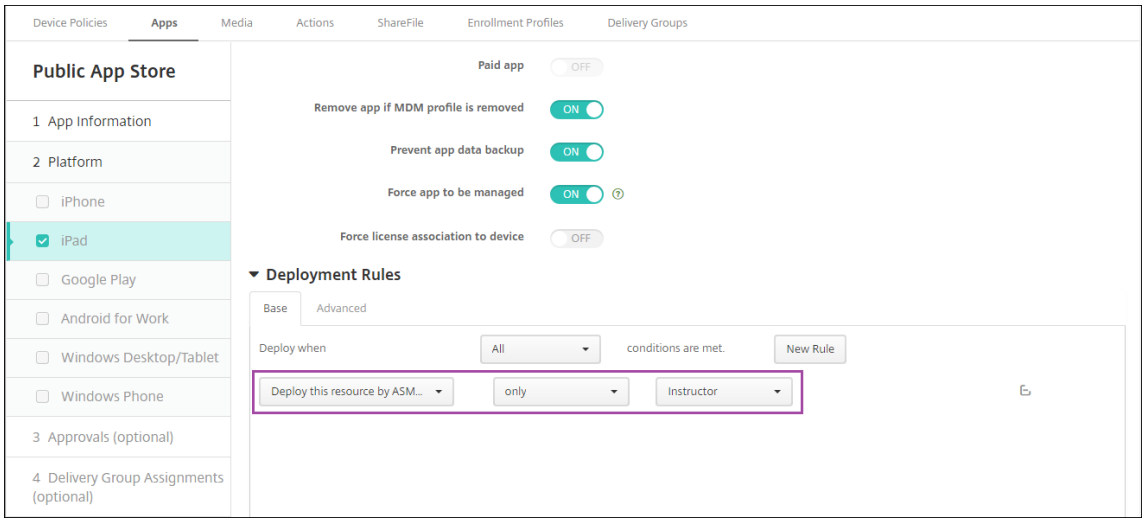
   - デフォルトで、Citrix Endpoint Management はアプリと iBooks をユーザーレベルで展開します。初回展開時に、ASM への登録を求めるメッセージが講師と生徒に送信されます。招待状を受け入れると、ユーザーは次回展開時（6 時間以内）に ASM アプリと iBooks を受信します。新規 ASM ユーザーに、アプリと iBooks の強制展開を適用することを Citrix ではお勧めします。これを実行するには、デリバリーグループを選択して ［展開］をクリックします。

     デバイスレベルで、アプリ（iBooks は除く）の割り当てを選択できます。これを実行するには、［デバイスへの強制ライセンス割り当て］の設定を ［オン］に変更します。デバイスレベルでアプリを割り当てる場合、一括購入プログラム参加の招待状はユーザーに送信されません。



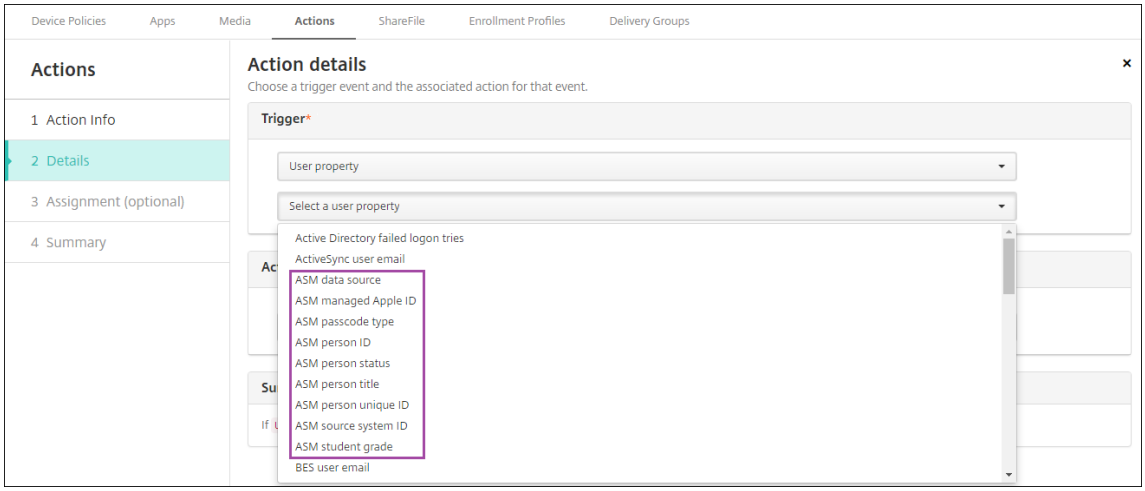
- 講師にのみアプリを展開するには、講師のみを含むデリバリーグループを選択するか、次の展開規則を使用します。

```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```



- 一括購入アプリの追加方法について詳しくは、「パブリックアプリストアのアプリの追加」を参照してください。

3. オプションです。ASM のユーザープロパティに基づいてアクションを作成します。たとえば、新しいアプリのインストール時に生徒のデバイスに通知を送信するアクションを作成できます。または、次の例に示すように、ユーザープロパティによってトリガーされるアクションを作成できます。

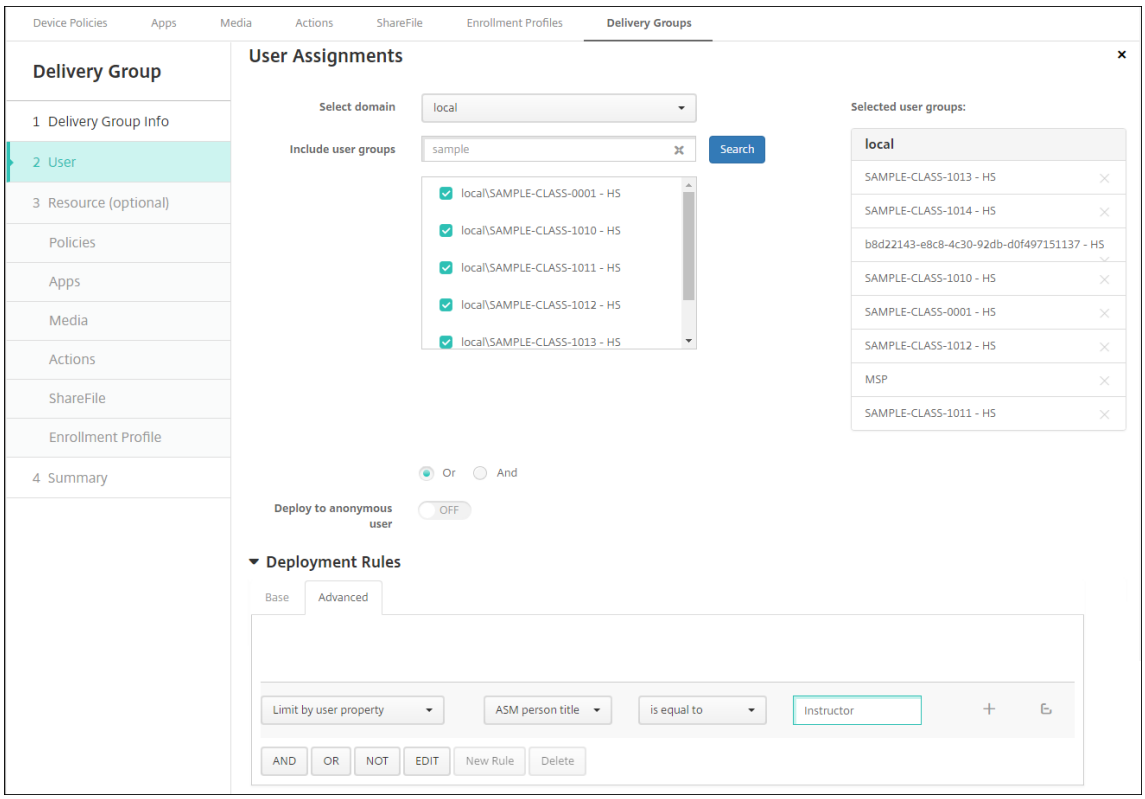


アクションを作成するには、［構成］**>**［アクション］の順に選択します。アクションの構成について詳しくは、「自動化されたアクション」を参照してください。

4. ［構成］**>**［デリバリーグループ］の順に選択し、講師と生徒のデリバリーグループを作成します。ASM からインポートしたクラスを選択します。また、講師と生徒の展開規則も作成します。

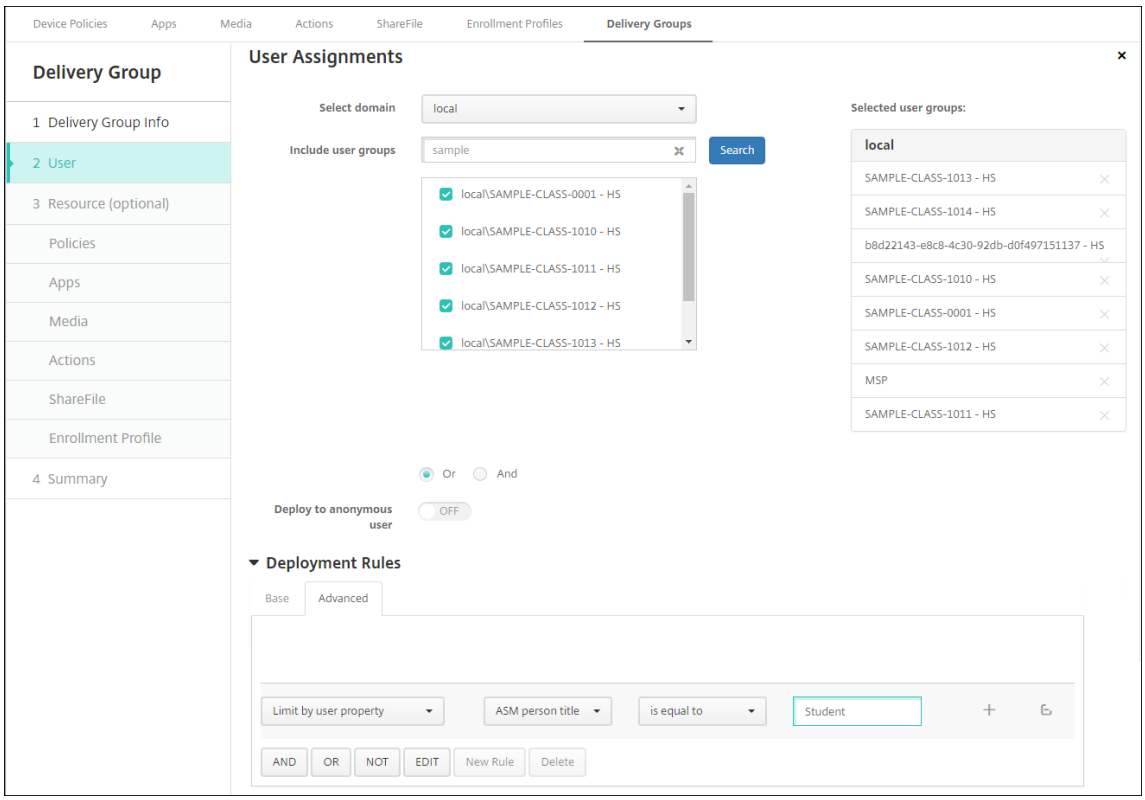
   たとえば、講師のユーザー割り当てを次に示します。展開規則は次のとおりです。

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

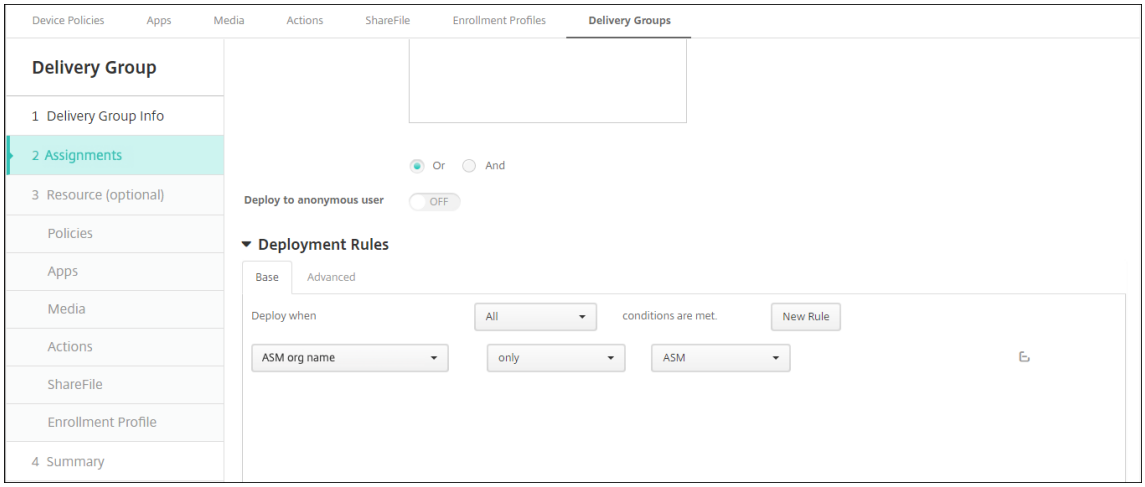



生徒のユーザー割り当てを次に示します。展開規則は次のとおりです。

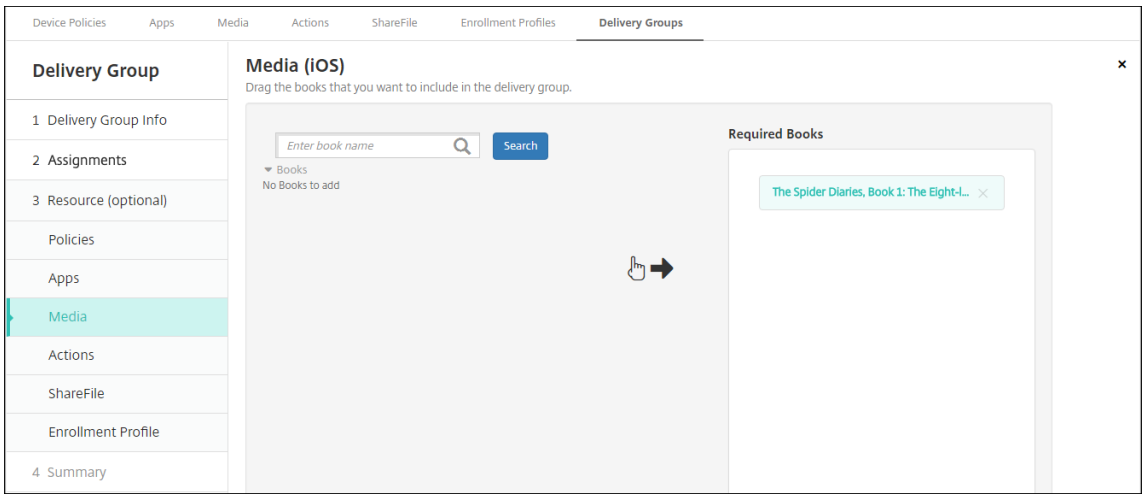
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

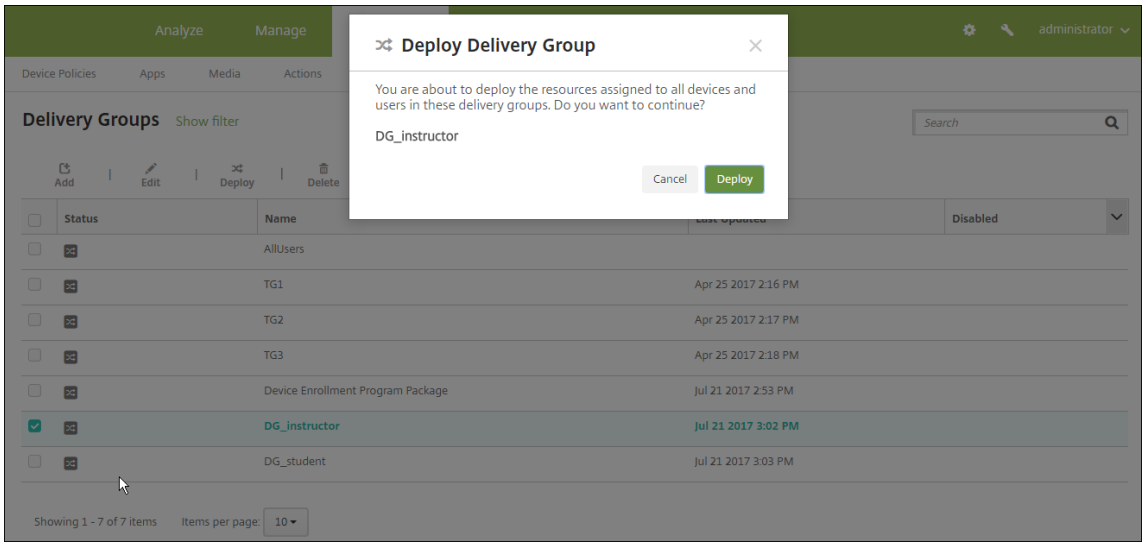
ASM 組織名に基づく展開規則を使用して、デリバリーグループをフィルター処理することもできます。



5. リソースをデリバリーグループに割り当てます。次の例は、デリバリーグループに含まれる iBook を示しています。



次の例は、デリバリーグループを選択して ［展開］をクリックすると開く確認ダイアログボックスを示しています。



詳しくは、「リソースの展開」の「デリバリーグループを編集するには」と「デリバリーグループを展開するには」を参照してください。

講師および生徒のデバイス登録のテスト

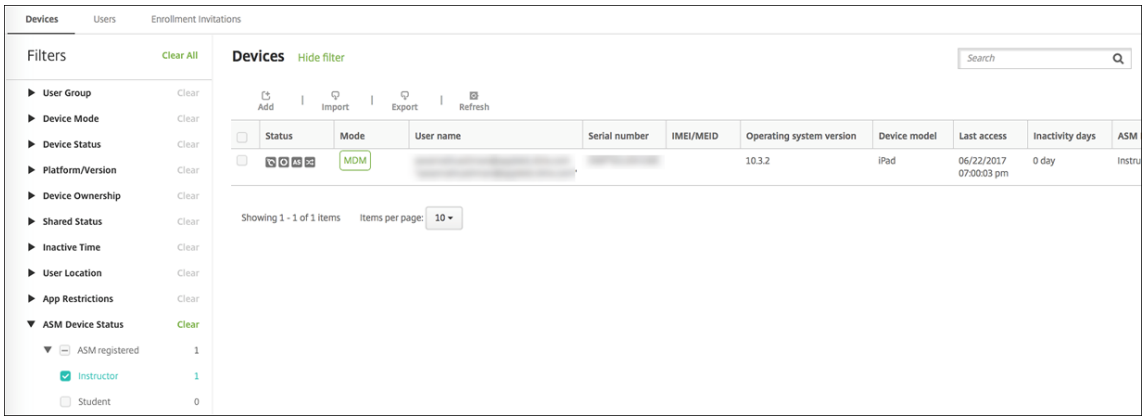
次の方法のいずれかを使用してデバイスを登録できます。

- 学校管理者は、Citrix Endpoint Management コンソールで設定したユーザーパスワードを使用して、講師と生徒のデバイスを登録できます。これにより、アプリとメディアが既にセットアップされたデバイスをユーザーに提供できます。
- デバイスを受け取ったユーザーは、管理者によって提供されたユーザーパスワードを使用して登録します。登録が完了すると、Citrix Endpoint Management によってデバイスポリシー、アプリ、およびメディアがデバイスに送信されます。

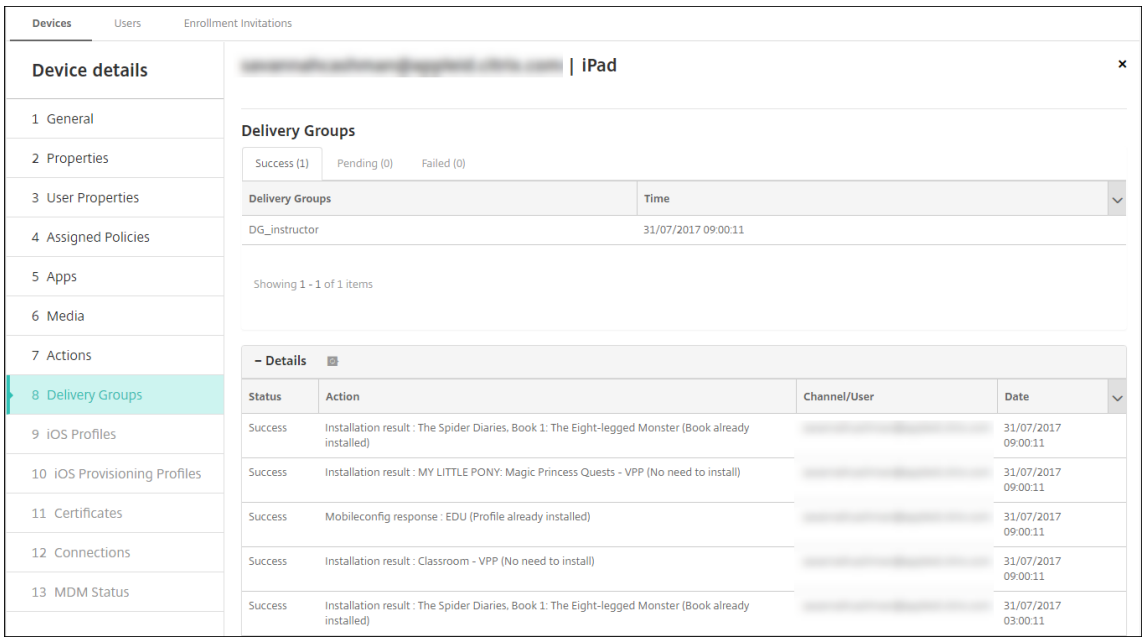
登録をテストするには、ASM にリンクした Apple Deployment Program デバイスを使用します。

1. デバイスが ASM にリンクしていない場合は、ハードリセットを実行してデバイスのコンテンツと設定を消去します。
2. 講師の ASM デバイスを登録します。次に、生徒の ASM デバイスを登録します。
3. [管理] > [デバイス] ページで、両方の ASM デバイスが MDM のみに登録されていることを確認します。

   [デバイス] ページを、ASM デバイスの状態（[**ASM** 登録済み]、[**ASM** 共有]、[講師]、[生徒]）ごとにフィルター処理できます。



4. MDM リソースが各デバイスに適切に展開されたことを確認するには、デバイスを選択し、[編集] をクリックして、各種ページを確認します。



デバイスの配布

Apple では、講師と生徒にデバイスを配布できるように、イベントをホストすることを推奨しています。

事前登録済みのデバイスを配布しない場合も、これらのユーザーに以下を提供します:

- 登録用の Citrix Endpoint Management パスワード
- 管理対象 Apple ID 用の、ASM の一時的なパスワード。

初回時のユーザーエクスペリエンスは次のとおりです。

1. ハードリセット後にユーザーが初めてデバイスを起動すると、Citrix Endpoint Management により登録画面でデバイスを登録するように求められます。
2. ユーザーは管理対象 Apple ID と、Citrix Endpoint Management への認証に使用する Citrix Endpoint Management パスワードを入力します。
3. Apple ID のセットアップ手順で、管理対象 Apple ID と ASM の一時的なパスワードの入力を求めるメッセージがデバイスに表示されます。これらの項目によって、Apple サービスへのユーザー認証が行われます。
4. iCloud でのデータの保護に使用される、管理対象 Apple ID のパスワード作成を求めるメッセージがデバイスに表示されます。
5. セットアップアシスタントの終了時に、Citrix Endpoint Management によりデバイスへのポリシー、アプリ、メディアのインストールが開始されます。ユーザーレベルで割り当てられるアプリと iBooks については、講師と生徒に一括購入への登録を促すメッセージがセットアップアシスタントにより表示されます。招待状を受け入れると、ユーザーは次回展開時（6 時間以内）に一括購入アプリと iBooks を受信します。

講師、生徒、およびクラスのデータの管理

講師、生徒、およびクラスのデータを管理する場合は、次のことに注意してください。

- ASM 情報を Citrix Endpoint Management にインポートした後に、管理対象 Apple ID を変更しないでください。Citrix Endpoint Management は、ユーザーの特定に ASM のユーザー識別子も使用します。
- 1 つまたは複数の教育の構成デバイスポリシーを作成した後に、ASM にクラスデータの追加や変更を行った場合は、ポリシーを編集してから再展開します。
- 教育の構成デバイスポリシーを展開した後にクラスの講師を変更する場合は、ポリシーを確認して Citrix Endpoint Management コンソールで確実に更新してから、ポリシーを再展開します。
- ASM ポータルでユーザープロパティを更新すると、Citrix Endpoint Management でもコンソールでプロパティが更新されます。ただし、Citrix Endpoint Management では、そのほかのプロパティと同じ方法で［ASM の個人の役職］プロパティ（講師、生徒、またはそのほか）が受信されません。このため、ASM で ASM の個人の役職を変更する場合は、次の手順を完了して Citrix Endpoint Management に変更が反映されるようにします。

データを管理するには:

1. ASM ポータルで、生徒の学年を更新し、講師の学年を削除します。

2. 生徒のアカウントを講師のアカウントに変更した場合は、クラスの生徒一覧からそのユーザーを削除します。次に、同じまたは別のクラスの講師一覧に、そのユーザーを追加します。

   講師のアカウントを生徒のアカウントに変更した場合は、クラスからそのユーザーを削除します。次に、同じまたは別のクラスの生徒一覧に、そのユーザーを追加します。更新内容は、次回の同期時（デフォルトで 5 分ごと）またはフェッチ時（デフォルトで 24 時間ごと）に、Citrix Endpoint Management コンソールに表示されます。

3. 教育の構成デバイスポリシーを編集し、変更を適用して再展開します。

   - ASM ポータルからユーザーを削除すると、Citrix Endpoint Management でもフェッチ後に Citrix Endpoint Management コンソールからそのユーザーが削除されます。

     サーバープロパティ値 **bulk.enrollment.fetchRosterInfoDelay** を変更することで、2 つのベースライン間の間隔を短縮できます（デフォルトは **1440** 分）。

   - リソース展開後に、生徒をクラスに参加させる場合は、その生徒だけで構成されたデリバリーグループを作成してリソースを展開します。

   - 生徒や講師が一時的なパスワードを紛失した場合は、ASM 管理者に問い合わせるようにします。管理者によって一時的なパスワードが提供されるか、または新しいパスワードが生成されます。

紛失したか盗難に遭ったデバイスの管理

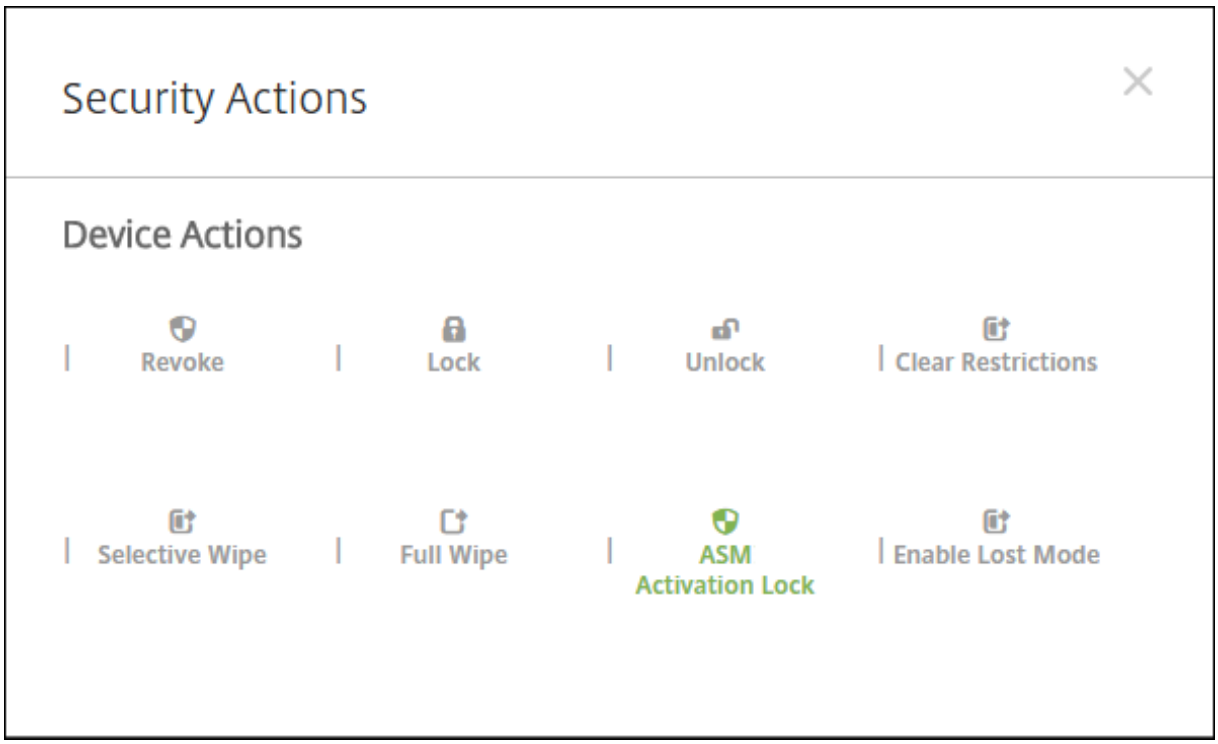
Apple の［iPhone/iPad を探す］サービスには、アクティベーションロック機能が含まれています。アクティベーションロックは、Apple Deployment Program に登録済みのデバイスが紛失または盗難に遭った場合に、不正ユーザーがそのデバイスを使用したり転売したりすることを防止します。

Citrix Endpoint Management には、ASM Apple Deployment Program に登録済みのデバイスにロックコードを送信できる、［**ASM** アクティベーションロック］のセキュリティ操作が含まれています。

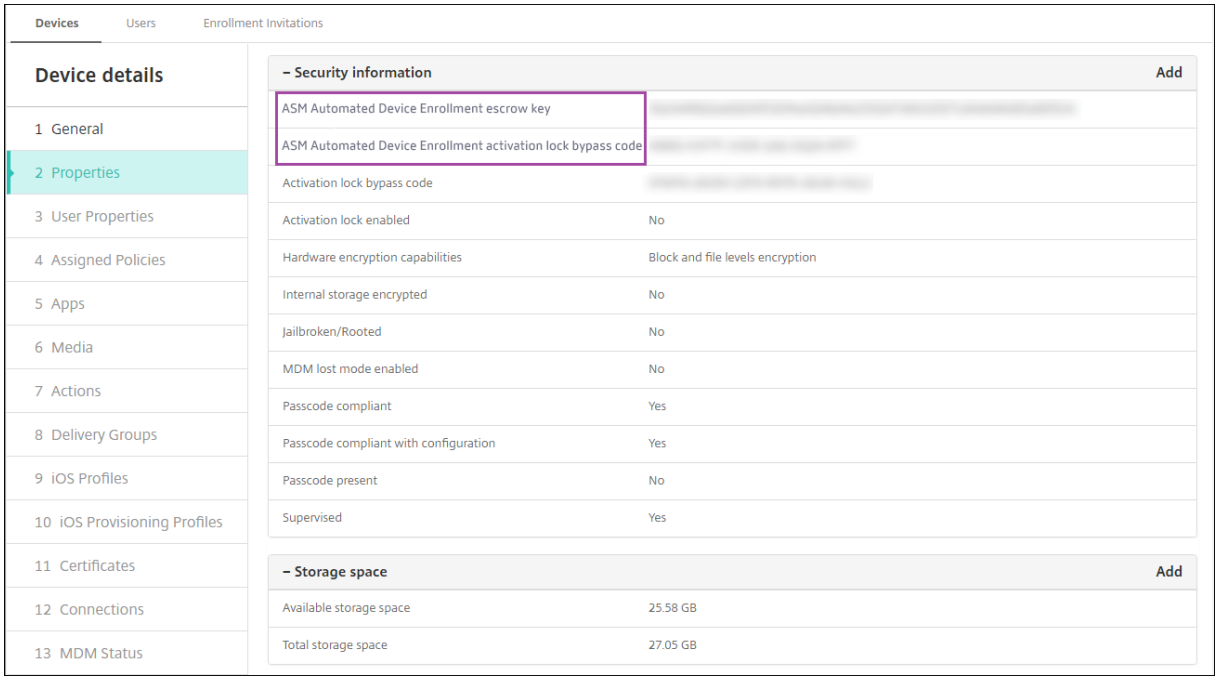
［**ASM** アクティベーションロック］のセキュリティ操作を使用すると、ユーザーに［iPhone/iPad を探す］サービスの有効化を要求せずに、Citrix Endpoint Management でデバイスを検索できます。ASM デバイスが強制リセットまたは完全にワイプされた場合、ユーザーは管理対象 Apple ID とパスワードを入力してデバイスのロックを解除します。

コンソールからロックを解除するには、セキュリティ操作 ［アクティベーションロックバイパス］をクリックします。アクティベーションロックをバイパスする方法については、「iOS アクティベーションロックのバイパス」を参照してください。ログインパネルを空白のままにして、パスワードとして ［**ASM** アクティベーションロックバイパスコード］を入力することもできます。この情報は、［プロパティ］タブの ［デバイス詳細］で入手できます。

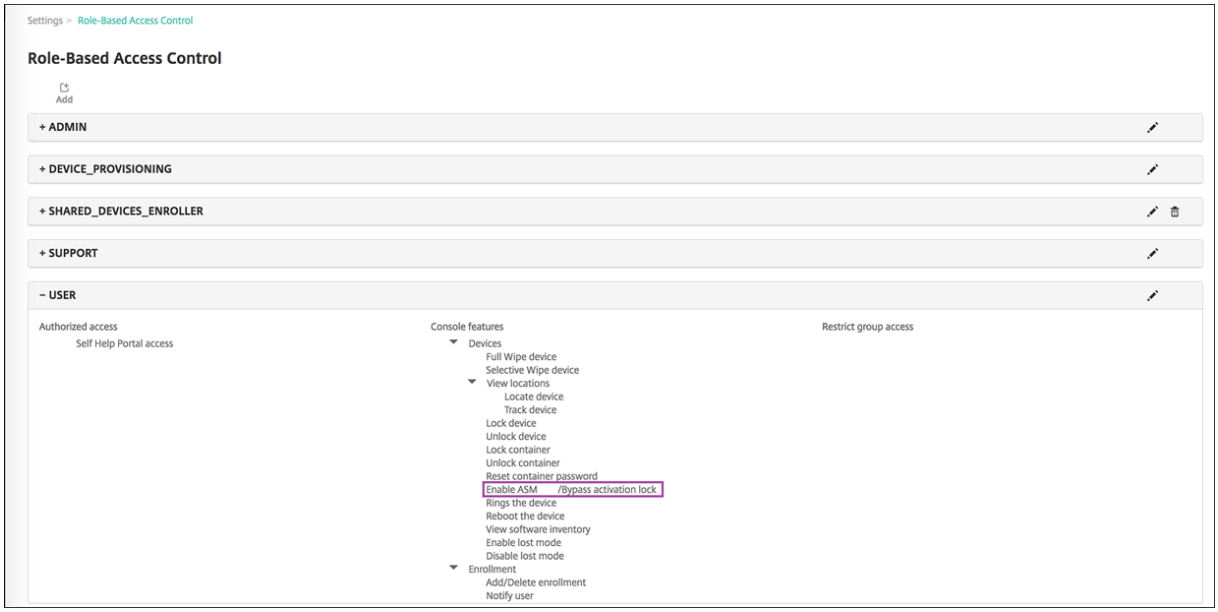
アクティベーションロックを設定するには、［管理］**>**［デバイス］の順に選択し、該当するデバイスを選択して、［セキュリティ］、［**ASM** アクティベーションロック］の順にクリックします。



[**ASM** エスクローキー］と ［**ASM** アクティベーションロックバイパスコード］のプロパティが、［デバイス詳細］に表示されます。



ASM アクティベーションロックに対する RBAC の権限は、［デバイス］ **>** ［**ASM/**バイパスアクティベーションロックを有効化］です。



共有 **iPad**

November 29, 2023

共有 iPad 機能により、複数のユーザーが iPad を使用できます。デバイスが共有されている場合でも、ユーザーエクスペリエンスをパーソナライズできます。共有 iPad は教育やビジネスに使用できます。Apple School Manager（ASM）は、Apple Business Manager（ABM）がサポートする役割に加えて、講師と生徒の役割をサポートします。

共有 **iPad** の前提条件

- Apple Business Manager または Apple School Manager
- Citrix Endpoint Management
- iPad Pro、iPad 第 5 世代、iPad Air 2 以降、iPad mini 4 以降
- 32GB 以上のストレージ容量
- 監視対象デバイス

共有 **iPad** の構成

複数の生徒または従業員がさまざまな目的で iPad を共有できます。

管理者かデバイス所有者が共有 iPad を登録し、デバイスポリシー、アプリ、メディアをデバイスに展開します。その後、ユーザーが管理対象 Apple ID の資格情報を入力して共有 iPad にサインインします。以前生徒に［教育の構成］

ポリシーを展開したことがある場合、生徒はデバイスを共有するために「その他のユーザー」としてサインインする必要はありません。

Citrix Endpoint Management は、共有 iPad で次の 2 つの通信チャネルを使用します：デバイス所有者（講師または管理者）用のシステムチャネルおよび現在の常駐ユーザー（生徒または従業員）用のユーザーチャネル。Citrix Endpoint Management は、これらのチャネルから Apple がサポートするリソースに対応した適切な MDM コマンドを送信します。

システムチャネル上に展開されるリソースは次のとおりです。

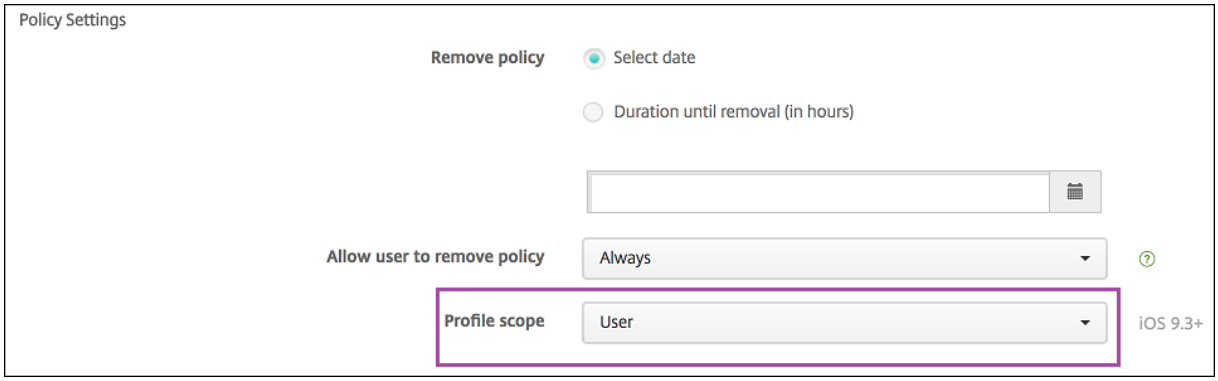
- 教育の構成、ロック画面のメッセージ、最大常駐ユーザー数、パスコードロックの猶予期間などのデバイスポリシー
- デバイスベースの一括購入アプリ
  Apple は、共有 iPad でエンタープライズアプリやユーザーベースの一括購入アプリをサポートしていません。共有 iPad では、アプリはユーザーごとではなく、デバイス全体にインストールされます。
- ユーザーベースの一括購入 iBoos
  Apple は、共有 iPad でのユーザーベースの一括購入 iBooks の割り当てをサポートしています。

ユーザーチャネル上に展開されるリソースは次のとおりです。

- デバイスポリシー：アプリ通知、ホーム画面レイアウト、制限、Web クリップ。

  Citrix Endpoint Management は、ユーザーチャネル上のデバイスポリシーのみをサポートしています。

デバイスポリシーを構成する場合、ポリシー設定の ［プロファイルの対象］で展開するチャネルを指定します。



ユーザーチャネルで展開したデバイスポリシーを削除する場合、［プロファイルの削除］ポリシーの ［展開範囲］で［ユーザー］を選択するようにしてください。

一般的なワークフロー

通常、デバイス所有者には事前に構成された監視対象共有 iPad が提供されます。次に、それらの個人はデバイスを生徒または従業員に配布します。事前登録済みの共有 iPad を配布しない場合は、デバイス所有者に Citrix Endpoint Management サーバーのパスワードを提供して、デバイスを登録できるようにしてください。

共有 iPad の構成と登録の一般的なワークフローは次のとおりです。

1. Citrix Endpoint Management サーバーコンソールで共有モードを有効にして、ASM または ABM アカウントを追加します（[設定] **>** [**Apple Deployment Program**]）。詳しくは、「共有 iPad のアカウントを管理する」を参照してください。
2. このセクションで説明するように、必要なデバイスポリシー、アプリ、メディアを Citrix Endpoint Management に追加して、これらのリソースをデリバリーグループに割り当てます。
3. デバイス所有者に共有 iPad のハードリセットを実行するよう指示します。登録の［Remote Management］画面が開きます。
4. デバイス所有者が共有 iPad を登録します。
   Citrix Endpoint Management は、登録済みの各共有 iPad に構成済みのリソースを展開します。自動再起動後、デバイス所有者はユーザーとデバイスを共有できるようになります。サインインページが iPad に表示されます。
5. デバイスユーザーは、管理対象 Apple ID と一時的な ASM パスワードを入力します。
   共有 iPad が ASM を認証すると、ユーザーは ASM パスワードを作成するよう促されます。次回の共有 iPad へのサインインでは、デバイスユーザーは新しい ASM パスワードを使用します。
6. iPad を共有している別のデバイスユーザーは、ここまでの手順を繰り返してサインインすることができます。

共有 **iPad** のアカウントを管理する

既に Apple Education または Apple Business で Citrix Endpoint Management を使用している場合：デバイス所有者が使用するデバイスなど、共有されていないデバイスに対しては、Citrix Endpoint Management に既存の ASM/ABM アカウントが設定されています。同一の ASM/ABM アカウントと Citrix Endpoint Management サーバーを、共有デバイスと非共有デバイスの両方に使用できます。

共有 **iPad** をデバイスグループにまとめる

ASM/ABM によって、複数の MDM サーバーを作成して、デバイスをグループに編成できます。共有 iPad を MDM サーバーに割り当てる時は、共有 iPad のグループごとにデバイスグループを作成します。

- グループ 1 の共有 iPad> デバイスグループ 1 MDM サーバー
- 共有 iPad のグループ 2> デバイスグループ 2 MDM サーバー
- 共有 iPad のグループ N> デバイスグループ N MDM サーバー

各デバイスグループに **ASM** アカウントを追加する

Citrix Endpoint Management サーバーコンソールで複数の ASM/ABM アカウントを作成すると、共有 iPad のグループが自動的にインポートされます：

- デバイスグループ 1 MDM サーバー > デバイスグループ 1 アカウント
- デバイスグループ 2 MDM サーバー > デバイスグループ 2 アカウント
- デバイスグループ N MDM サーバー > デバイスグループ N アカウント

共有 iPad に固有の要件は以下のとおりです。

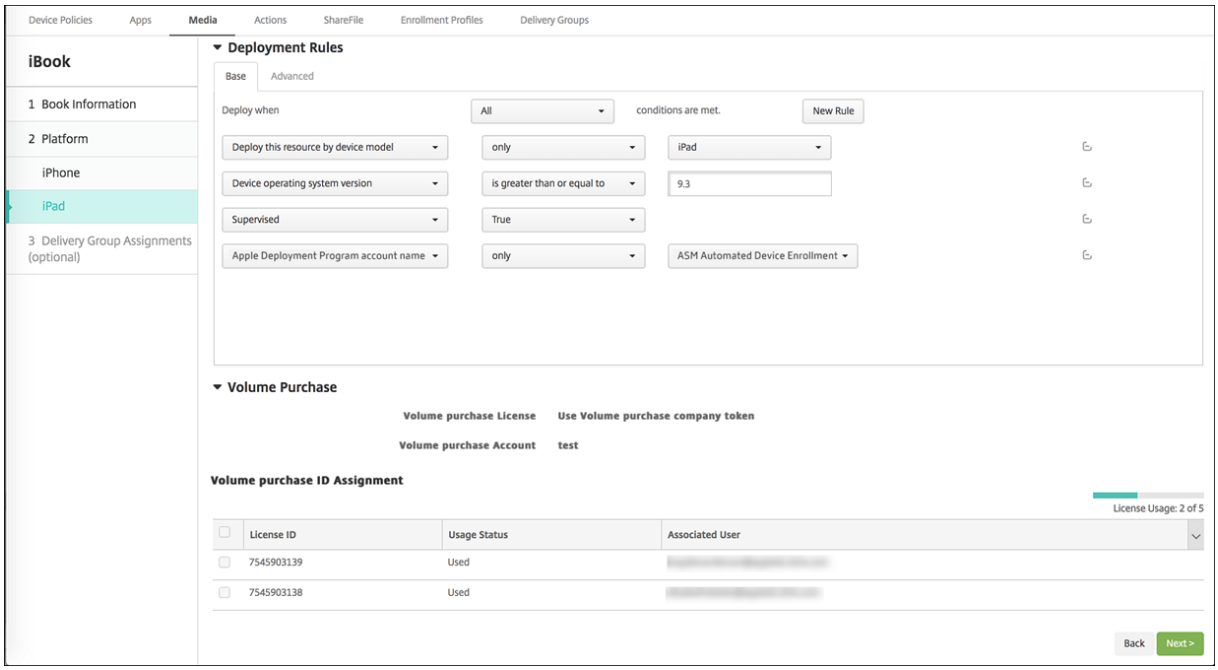
- デバイスグループごとに 1 つの ASM/ABM アカウントを用意し、以下の設定を有効にします。
  - デバイス登録を必須にする
  - 監視モード
  - 共有モード
- 同じ教育機関では、すべての ASM アカウントに同じ教育機関のサフィックスを使用してください。

共有 **iPad** のアプリ

共有 iPad は、デバイスベースの一括購入アプリの割り当てをサポートしています。Citrix Endpoint Management サーバーは共有 iPad にアプリを展開する前に、デバイスに一括購入ライセンスを割り当てるよう Apple 一括購入サーバーに要求を送信します。一括購入の割り当てを確認するには、[構成] > [アプリ] > [**iPad**] に進み、[一括購入] を展開します。

共有 **iPad** 用のメディア

共有 iPad はユーザーベースの一括購入 iBooks の割り当てをサポートしています。Citrix Endpoint Management サーバーは共有 iPad に iBooks を展開する前に、ユーザーに一括購入ライセンスを割り当てるよう Apple 一括購入サーバーに要求を送信します。一括購入の割り当てを確認するには、[構成] > [メディア] > [**iPad**] に進み、[一括購入] を展開します。



共有 **iPad** の展開規則

デリバリーグループレベルの規則はユーザープロパティに関するものであるため、共有 iPad を展開する場合これらの規則は適用されません。デバイスのグループごとにポリシー、アプリ、メディアを絞り込むには、アカウント名に基づいて、リソースの展開規則を追加します。例:

- デバイスグループ 1 のアカウントでは、次の展開規則を設定します:

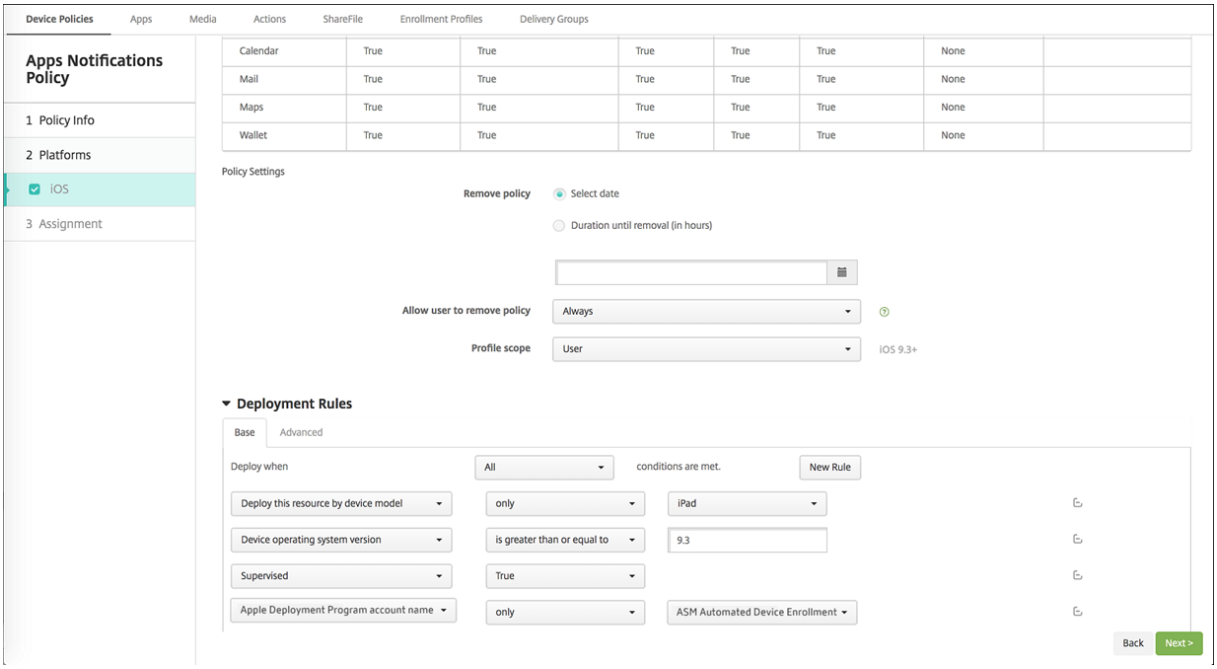
```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```

- デバイスグループ 2 のアカウントでは、次の展開規則を設定します:

```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- デバイスグループ N のアカウントでは、次の展開規則を設定します:

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```

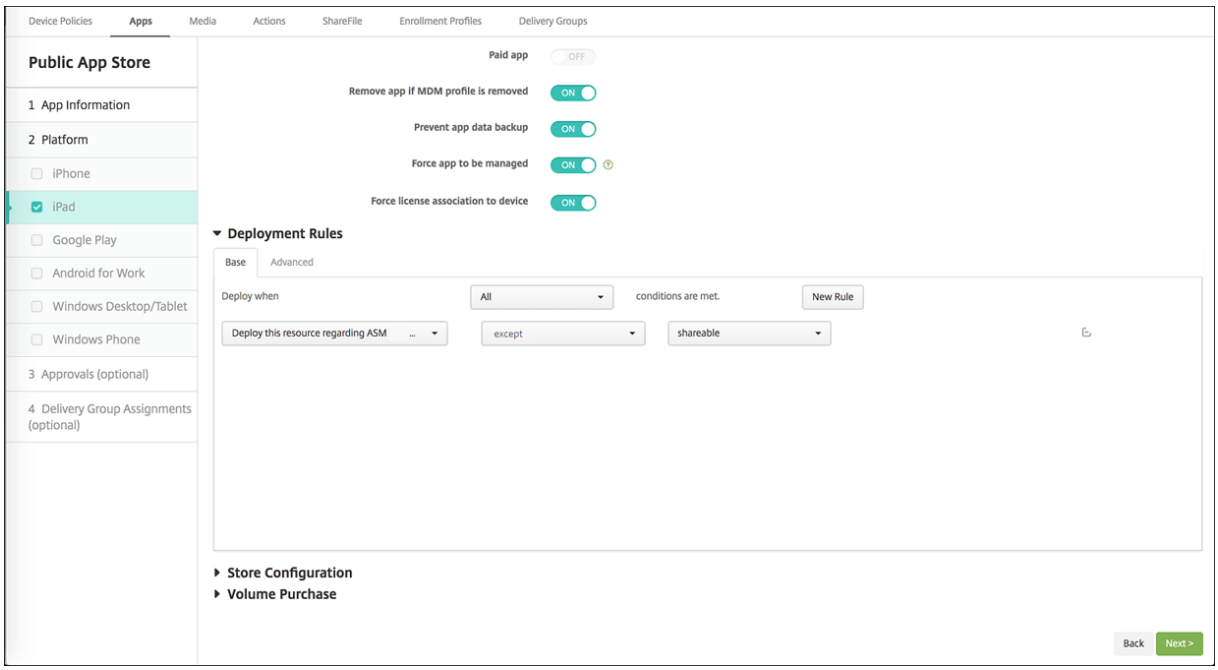


非共有の iPad を使用してデバイス所有者にのみ Apple クラスルームアプリを展開する場合、ASM の共有状態を次の展開規則で絞り込みます:

```
Deploy this resource regarding ASM/ABM shared mode
only
unshared

<!--NeedCopy-->
```

または:

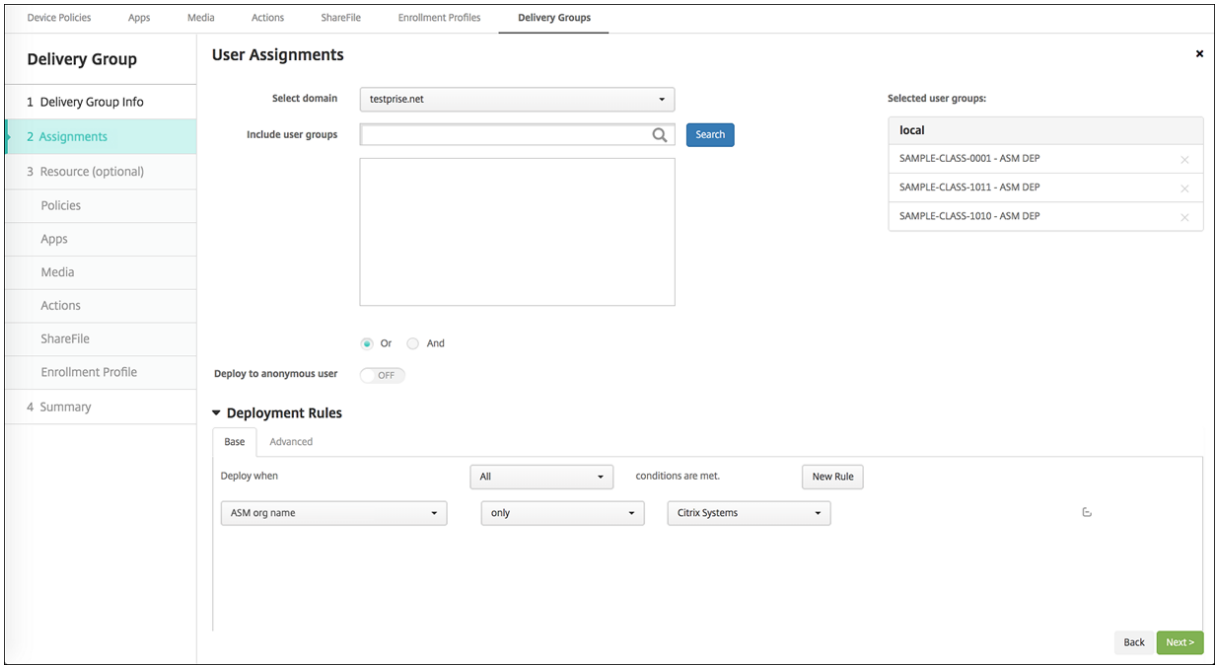
```
Deploy this resource regarding ASM/ABM shared mode
except
shareable

<!--NeedCopy-->
```



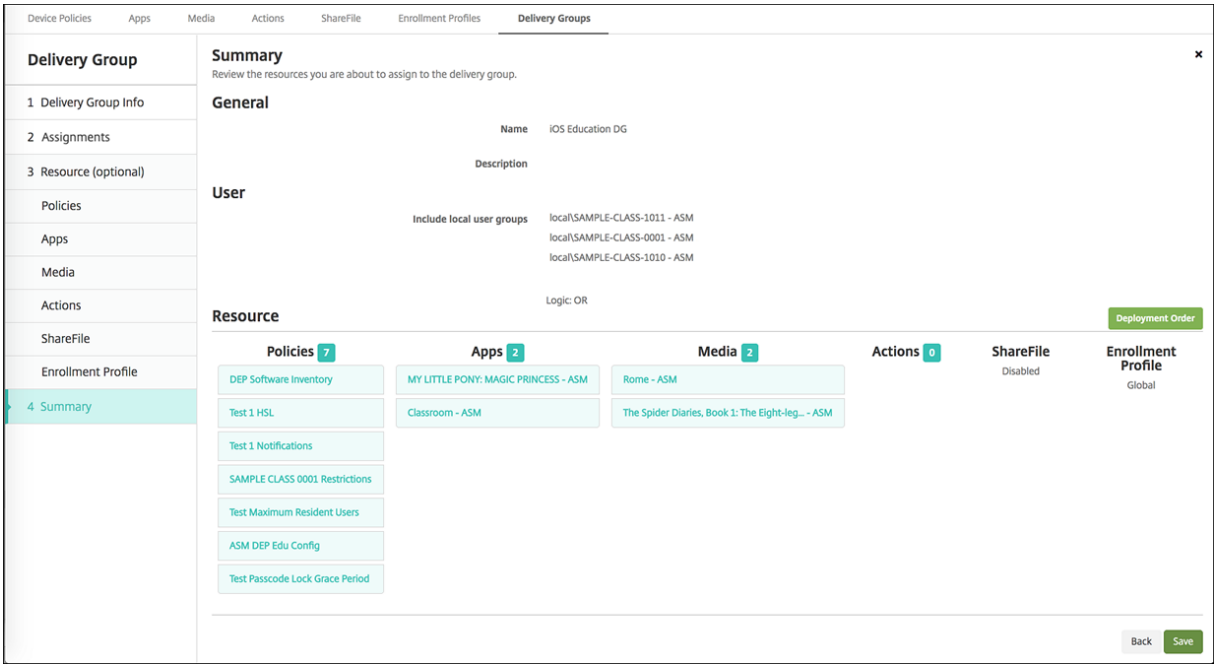
共有 **iPad** のデリバリーグループ

デバイスグループの場合:

- 1 つのデリバリーグループを構成する。講師には、［教育の構成］ポリシーで定義されているすべてのクラスを割り当てます。



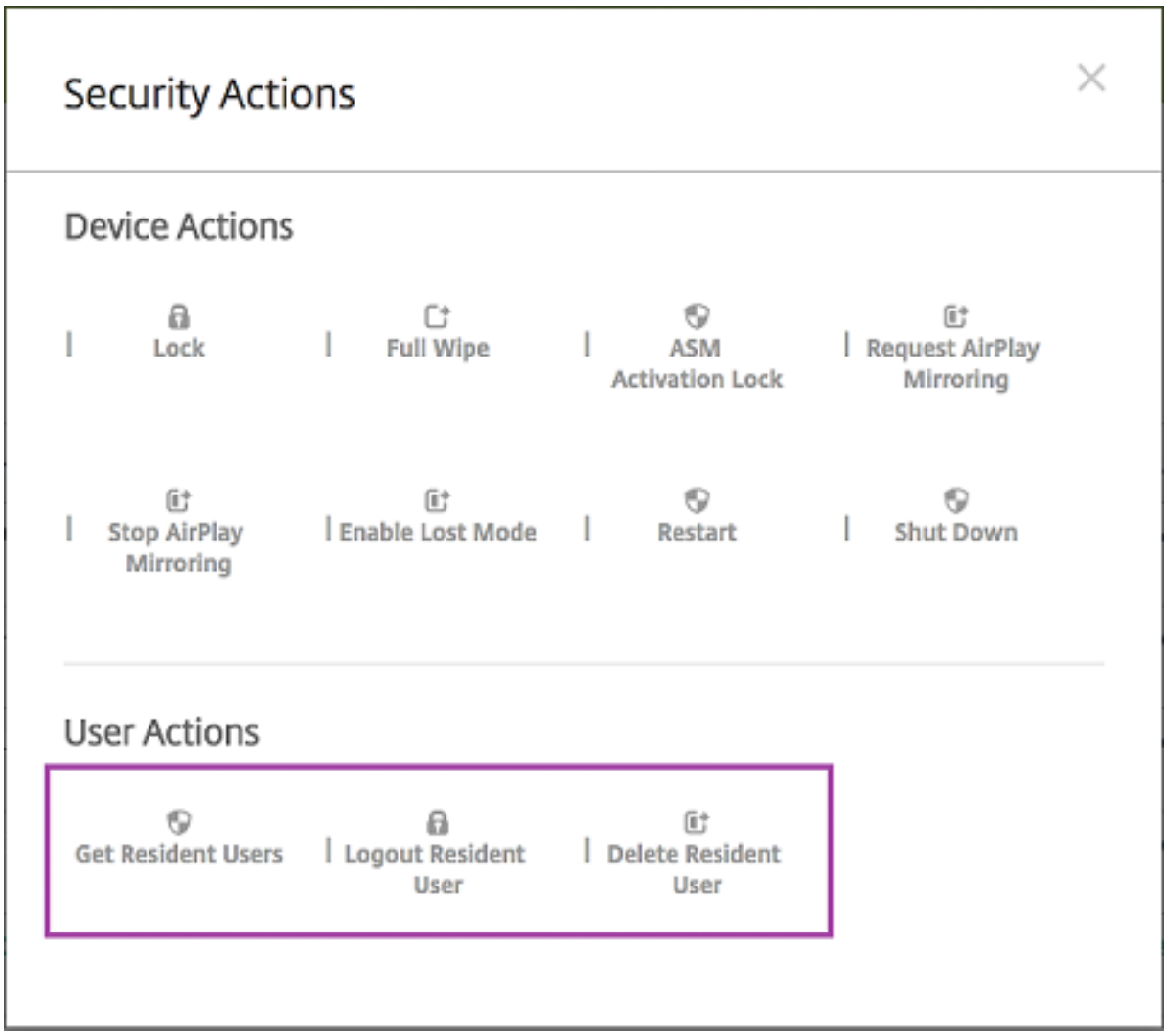
- このデリバリーグループには、次の MDM リソースを含める必要があります。
  - デバイスポリシー：
    - 教育の構成（ASM 用）
    - ロック画面のメッセージ
    - アプリ通知
    - ホーム画面のレイアウト
    - 制限
    - 最大常駐ユーザー数
    - パスコードロックの猶予期間
  - 必要な一括購入アプリ
  - 必要な一括購入 iBooks



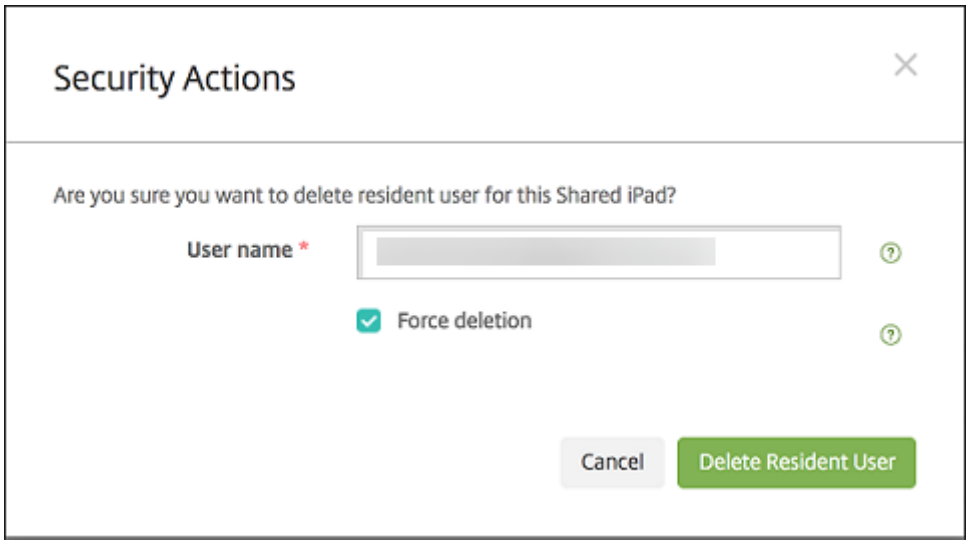
共有 **iPad** のセキュリティ操作

既存のセキュリティ操作に加えて、共有 iPad では次のセキュリティ操作を使用できます:

- 常駐ユーザーの取得：現在のデバイスで有効なアカウントを持つユーザーの一覧を表示します。この操作により、デバイスと Citrix Endpoint Management コンソール間で強制的に同期が行われます。
- 常駐ユーザーのログアウト：現在のユーザーを強制的にログアウトさせます。
- 常駐ユーザーの削除：指定したユーザーの現在のセッションを削除します。ユーザーは再びサインインできます。
- **Delete All Users**：デバイス上のすべてのユーザーを削除します。



［常駐ユーザーの削除］のクリック後、ユーザー名を指定できます。

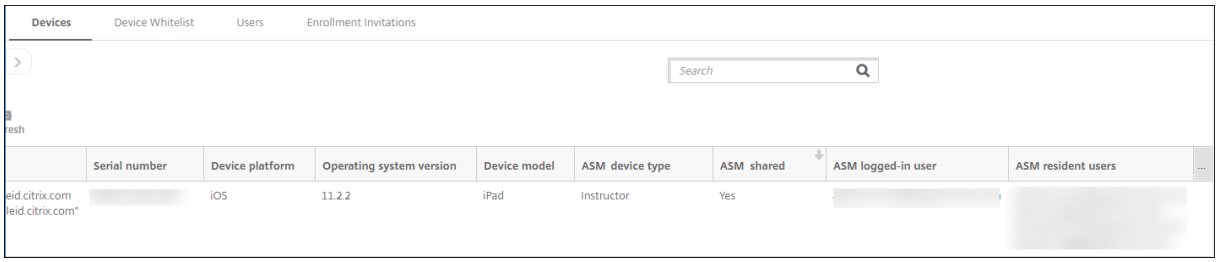


セキュリティ操作の結果は、[管理] > [デバイス] > [一般] ページおよび [管理] > [デバイス] > [デリバリーグループ] ページに表示されます。

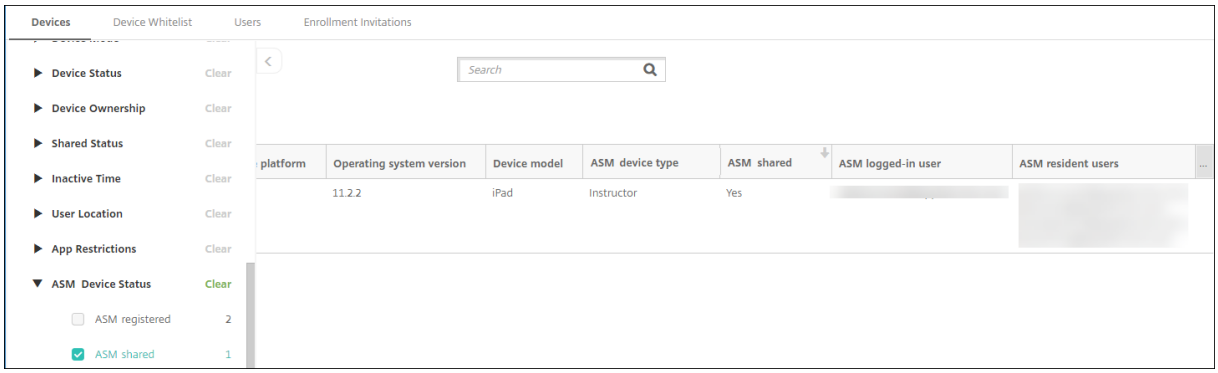
共有 iPad の情報を取得する

共有 iPad に関する情報は、[管理] > [デバイス] ページで確認できます。

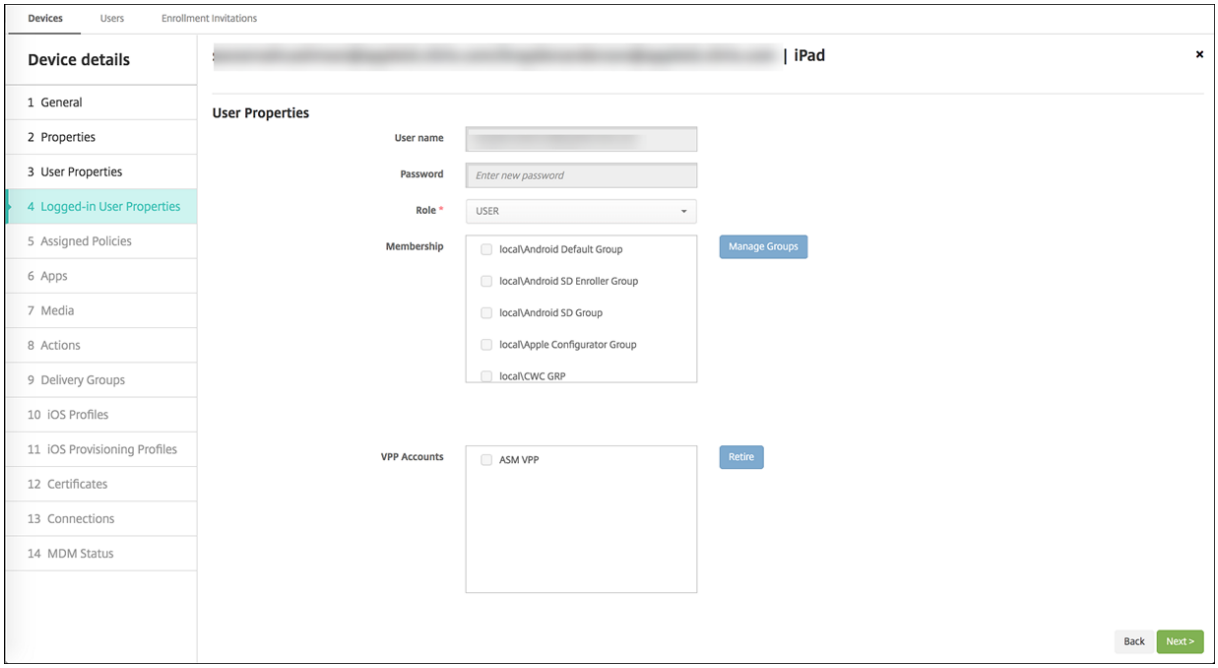
- 次を検索できます。
  - デバイスが共有されているか（[**ASM/ABM** 共有]）
  - 共有デバイスにログインしているユーザー（[**ASM/ABM** ログイン済みユーザー]）
  - 共有デバイスに割り当てられているすべてのユーザー（[**ASM/ABM** 常駐ユーザー]）

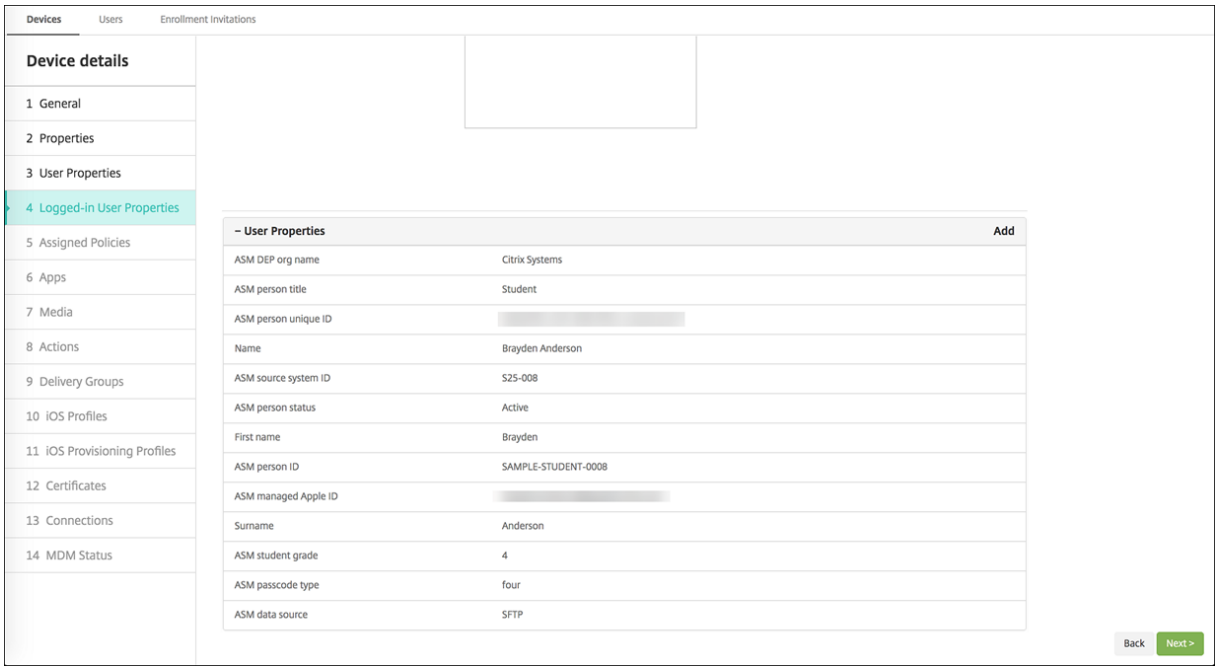


- [**ASM/ABM** デバイスの状態] でデバイス一覧を絞り込むことができます:

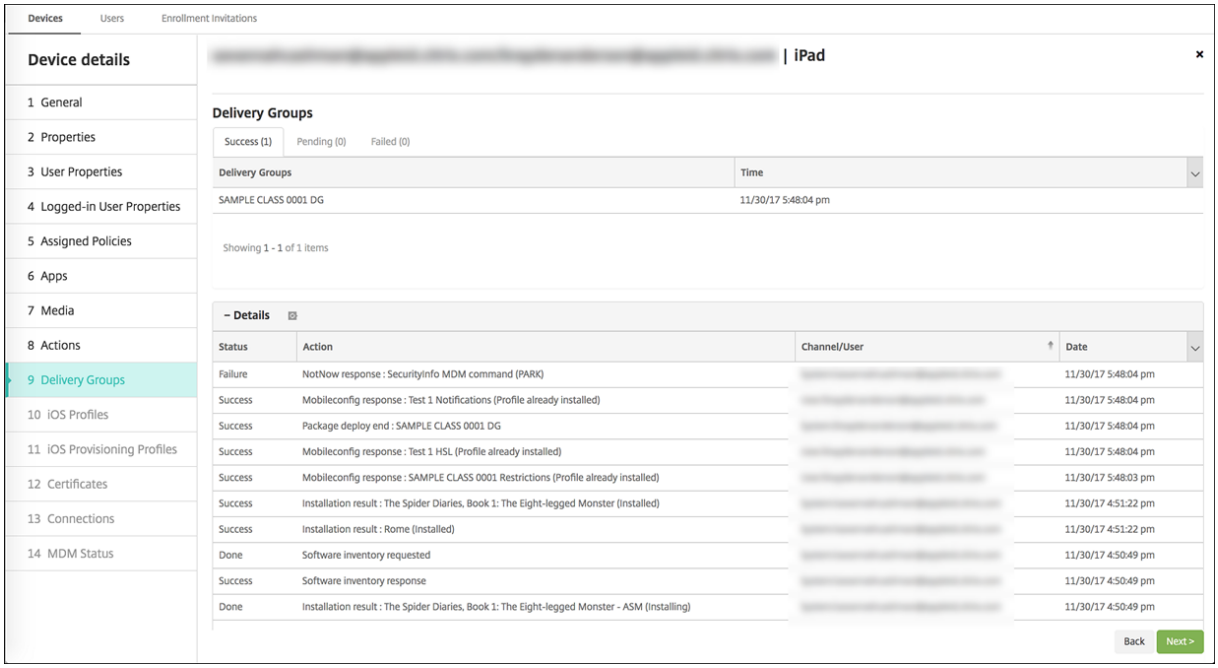


- [管理] > [デバイス] > [ログイン済みユーザーのプロパティ] ページで、共有 iPad にログインしているユーザーの詳細を確認できます。

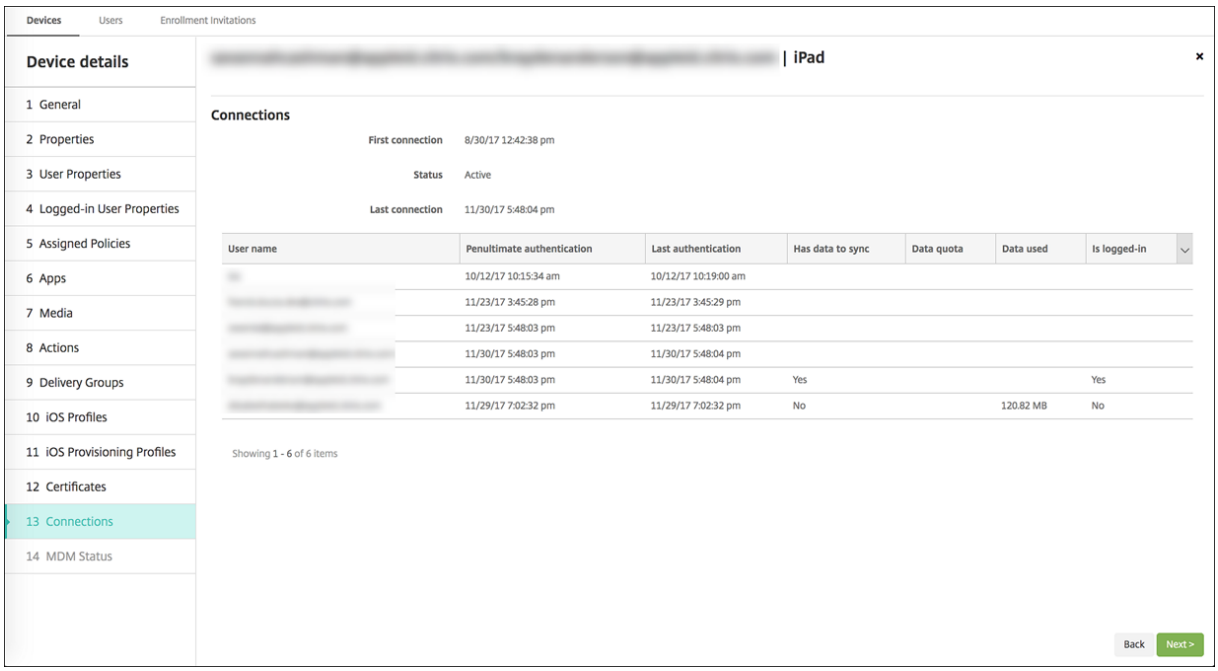




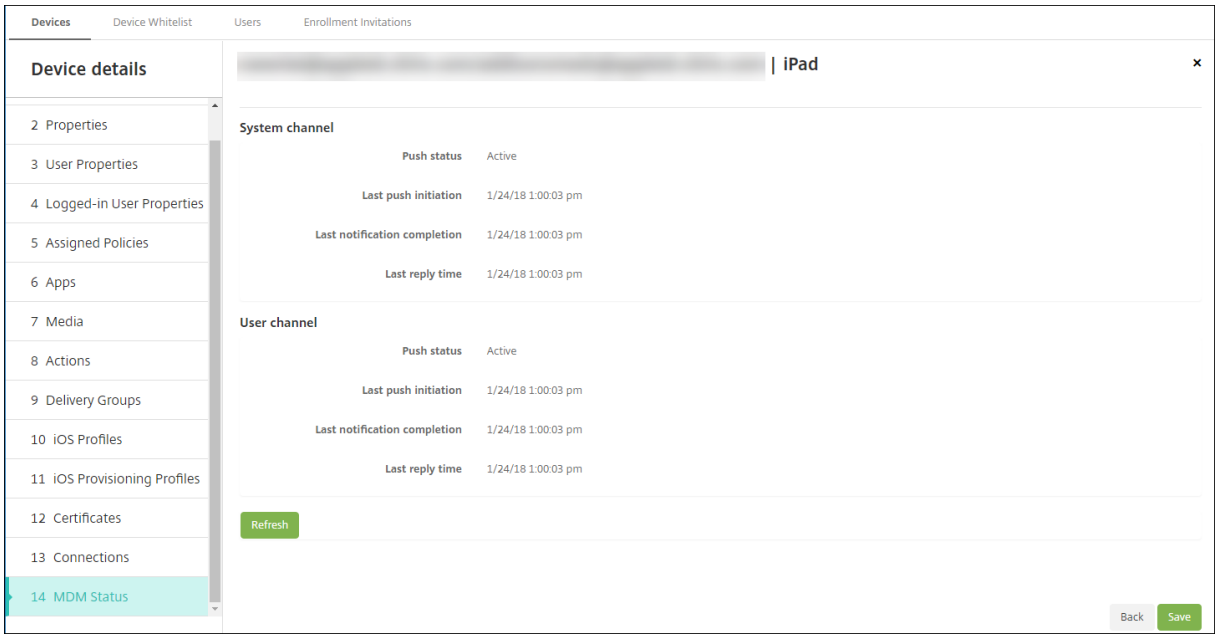
- [管理] > [デバイス] > [デリバリーグループ] ページでは、デリバリーグループのデバイス所有者およびユーザーへのリソース展開に使用されているチャネルを確認できます。[チャネル/ユーザー] 列には、チャネルの種類（[システム] または [ユーザー]）と受信者が表示されます。



- 常駐ユーザーの情報を取得できます。
  - 同期するデータがある：クラウドに同期させるデータをユーザーが持っているかどうか。
  - データクォータ：ユーザーに設定されているデータクォータ（バイト単位）。ユーザークォータが一時的にオフになっているか、ユーザーに割り当てられていない場合は、クォータが表示されないことがあります。
  - 使用済みデータ：ユーザーが使用したデータ量（バイト単位）。システムの情報収集時にエラーが発生した場合、値が表示されないことがあります。
  - ログイン中：ユーザーがデバイスにログオンしているかどうか。



- 両方のチャネルのプッシュステータスを確認できます。



Apple アプリの配布

November 29, 2023

Citrix Endpoint Management はデバイスに展開されたアプリを管理します。次の種類の iOS、iPadOS、macOS

アプリを編成して展開できます。

- パブリックアプリストア（**iOS/iPadOS** のみ）：これらのアプリには、Apple App Store や Google Play などのパブリックアプリストアで無料または有料で提供されているアプリが含まれます。たとえば、GoToMeeting です。
- エンタープライズ（**iOS/iPadOS/macOS**）： MDX アプリに関連付けられたポリシーを含んでいない、MDX 対応のネイティブアプリです。
- **MDX**（**iOS/iPadOS** のみ）： MAM SDK で準備されたアプリまたは MDX Toolkit でラップされたアプリ。これらのアプリには MDX ポリシーが含まれます。MDX アプリは内部ソースおよび公開ストアから取得します。
- 一括購入（**iOS/iPadOS/macOS**）：ライセンスが Apple の一括購入プログラムで管理されるアプリです。
- **iOS** カスタムアプリ（**iOS/iPadOS** のみ）：社内またはサードパーティ開発による独自の B2B（business-to-business）アプリです。

さまざまな種類のアプリについて詳しくは、「アプリの追加」を参照してください。

展開によっては、Apple Business Manager（ABM）または Apple School Manager（ASM）アカウントが必要です。詳しくは、後のセクションを参照してください。

アプリの種類と配布方法ごとに、対応した組み合わせの構成を使用することを Citrix ではお勧めします。その他のプラットフォームでのアプリの配布方法については、「アプリの追加」を参照してください。次のセクションでは、iOS アプリの構成に関する詳細を提供します。

アプリの配布に関する一般的な手順

シナリオ	手順 1：アカウントのリンク	手順 2：アプリの追加および構成	手順 3：デリバリーグループの構成およびアプリの展開
パブリックアプリストアのアプリ。Citrix モバイルアプリを含む	該当なし	**Citrix Endpoint Management** で ［構成］ **>** ［アプリ］ から iPhone または iPad の ［パブリックアプリストア］ アプリを追加します。アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。

シナリオ	手順 1：アカウントのリンク	手順 2：アプリの追加および構成	手順 3：デリバリーグループの構成およびアプリの展開
Apple の一括購入で配布されたパブリックアプリストアのアプリ。Citrix モバイルアプリを含む	Apple Deployment Program に登録します。**Citrix Endpoint Management** で ［設定］**>**［一括購入］に移動して利用中の一括購入アカウントを追加します。	**ABM** または **ASM** で［App とブック］からアプリを購入して追加します。**Citrix Endpoint Management** で ［構成］**>**［アプリ］に移動してアプリを構成し、デリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。
エンタープライズアプリ	該当なし	**Citrix Endpoint Management** で ［構成］**>**［アプリ］に移動します。［追加］、［エンタープライズ］をクリックします。IPA ファイルをアップロードします。アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。
MDX アプリ	該当なし	**Citrix Endpoint Management** で ［構成］**>**［アプリ］に移動します。［追加］、［**MDX**］をクリックします。プラットフォームで **iPad**/**iPhone** を選択してください。MDX ファイルをアップロードします。アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。

シナリオ	手順 1：アカウントのリンク	手順 2：アプリの追加および構成	手順 3：デリバリーグループの構成およびアプリの展開
Apple の一括購入を使用して配布された MDX アプリ	Apple Deployment Program に登録します。**Citrix Endpoint Management** で ［設定］ **>**［一括購入］に移動して利用中の一括購入アカウントを追加します。	**ABM** で［App とブック］から MDX アプリを購入して追加します。利用中の ABM アカウントにアプリをリンクします。**Citrix Endpoint Management** で ［構成］ **>**［アプリ］に移動してアプリを構成し、デリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。
カスタムアプリ	Apple Deployment Program に登録します。**Citrix Endpoint Management** で ［設定］ **>**［一括購入］に移動して利用中の一括購入アカウントを追加します。	**ABM** で App Store にアプリをプライベートアプリとして追加します。このアプリを ABM アカウントにリンクします。**Citrix Endpoint Management** で ［構成］ **>**［アプリ］に移動してアプリを構成し、デリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。
MDX 対応カスタムアプリ	Apple Deployment Program に登録します。**Citrix Endpoint Management** で ［設定］ **>**［一括購入］に移動して利用中の一括購入アカウントを追加します。	**ABM** で App Store にアプリをプライベートアプリとして追加します。このアプリを ABM アカウントにリンクします。**Citrix Endpoint Management** で ［構成］ **>**［アプリ］に移動して MDX ファイルをアップロードします。アプリを構成してデリバリーグループに割り当てます。	**Citrix Endpoint Management** でデリバリーグループを使用してアプリを構成し、展開します。

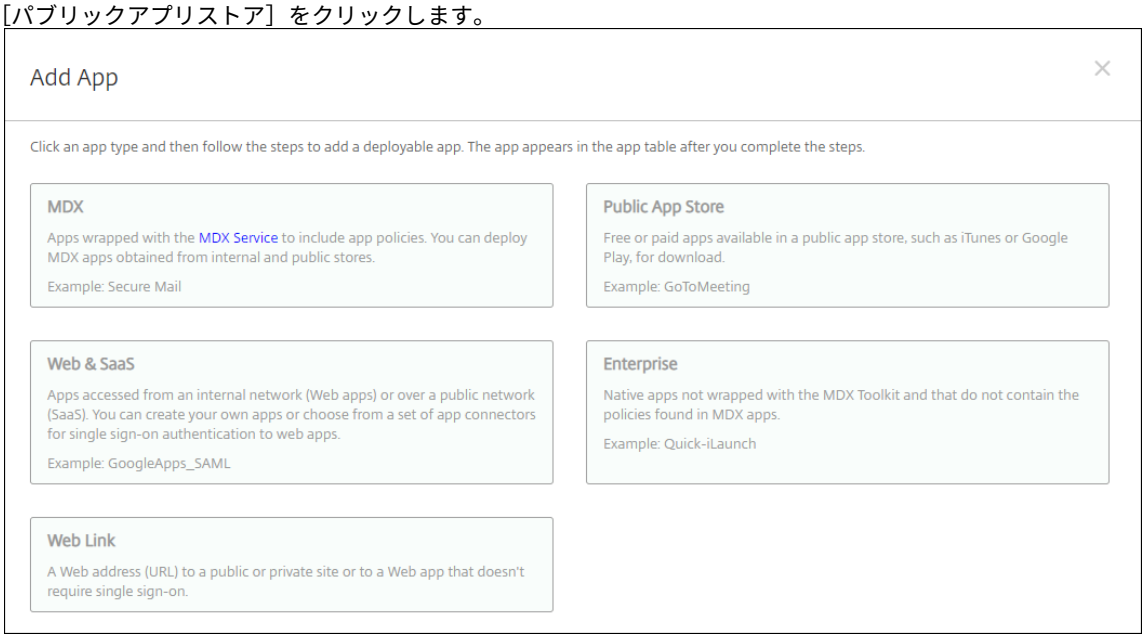
パブリックアプリストアのアプリ

App Store から利用できる無料アプリおよび有料アプリを Citrix Endpoint Management に追加できます。

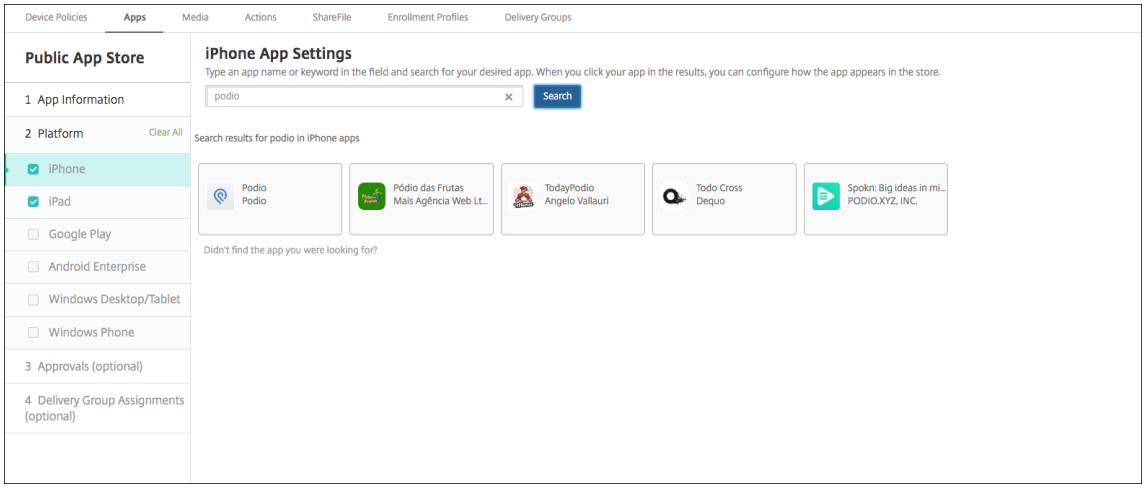
利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	番号
利用可能	iOS/iPadOS

手順 **1**：アプリの追加および構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。［追加］をクリックします。
2. ［パブリックアプリストア］をクリックします。



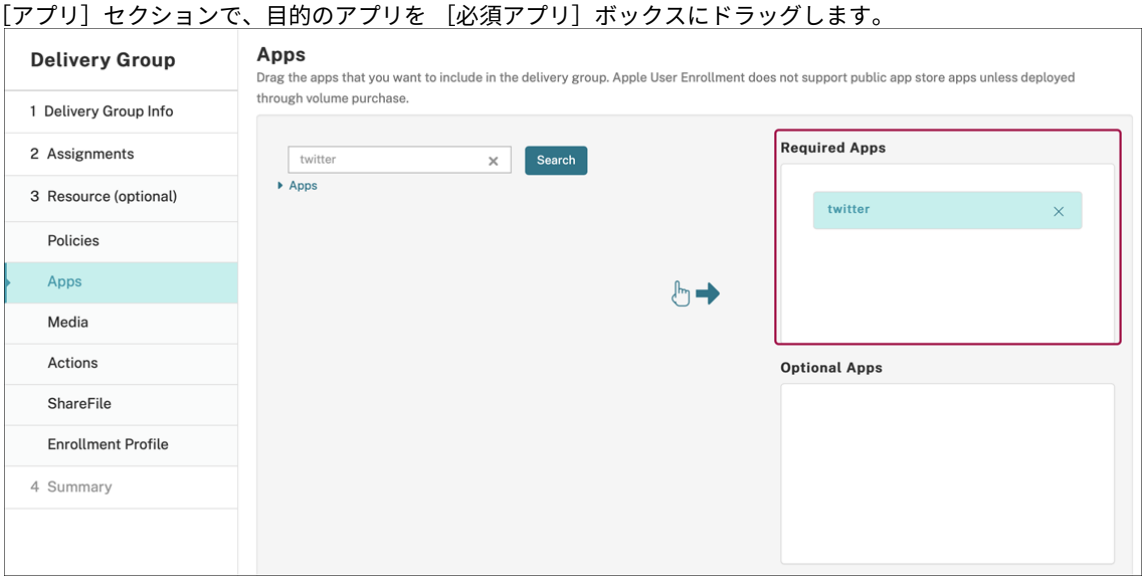
3. プラットフォームで **iPhone** か **iPad** かを選択します。
4. 検索ボックスにアプリ名を入力し、［検索］をクリックします。



5. 検索条件に一致するアプリが表示されます。必要なアプリをクリックします。
6. デリバリーグループをアプリに割り当て、［保存］をクリックします。

手順 **2**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。
2. 構成するアプリを選択して ［編集］をクリックします。
3. ［管理されるアプリ］機能を有効にすることをお勧めします。
4. 任意のデリバリーグループを割り当て、［保存］をクリックします。
5. ［構成］**>**［デリバリーグループ］に移動してから ［追加］をクリックします。
6. ［アプリ］セクションで、目的のアプリを ［必須アプリ］ボックスにドラッグします。



7. ［構成］**>**［デリバリーグループ］に戻ります。
8. デリバリーグループを選択して ［展開］をクリックします。
9. ユーザーがアプリをインストールする要求を受信し、ユーザーの承認後にアプリがバックグラウンドでインストールされます。

Apple の一括購入で配布されたパブリックアプリストアのアプリ

iOS/iPadOS アプリのライセンスは Apple の一括購入プログラムで管理できます。以下の手順で Citrix Endpoint Management に一括購入アプリを追加します。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS/macOS

手順 **1**：アカウントのリンク

1. Apple Business Manager（ABM）または Apple School Manager（ASM）でセットアップして登録します。これらのプログラムについて詳しくは、Apple のドキュメントを参照してください。
2. 利用中の ABM/ASM アカウントを Citrix Endpoint Management にリンクします。一括購入アカウントのリンクについて詳しくは、「Apple Volume Purchase」を参照してください。

3. 一括購入アカウントを追加する場合、[アプリの自動更新] を有効にします。この設定は、Apple Store に更新がアップされるとユーザーデバイス上のアプリが自動的に更新されるようにします。[管理されるアプリ] 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。

   [管理されるアプリ] および [アプリの自動更新] 設定を使用するには、`apple.app.force.managed` サーバープロパティを有効にします。「サーバープロパティ」を参照してください。

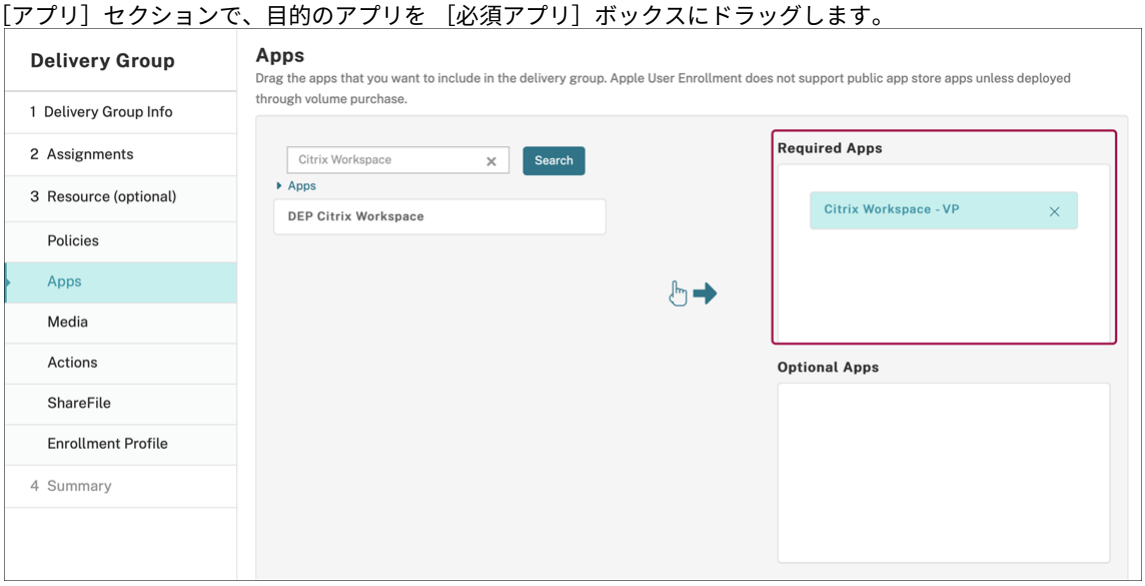
手順 **2**: **Apple** からアプリおよびライセンスを入手

ABM/ASM アカウントでアプリを購入します。Apple Books（iOS または iPadOS 用のみ）と Apple App Store で購入できます。無料の場合であっても「購入」する必要があることに注意してください。ABM/ASM でライセンスを購入したら、Citrix Endpoint Management はアプリを自動的に表示します。

アプリを業務で使用できるようにする方法については、Apple のドキュメントを参照してください。

手順 **3**: アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］ **>** ［アプリ］ の順に移動します。
2. 構成する一括購入アプリを選択して ［編集］ をクリックします。
3. プラットフォームで **iPhone**、**iPad**、または **macOS** を選択します。
4. ［管理されるアプリ］ 機能を有効にすることを Citrix ではお勧めします（iOS/iPadOS のみ）。
5. 任意のデリバリーグループを割り当て、［保存］ をクリックします。
6. ［構成］ **>** ［デリバリーグループ］ に移動してから ［追加］ をクリックします。
7. ［アプリ］ セクションで、目的のアプリを ［必須アプリ］ ボックスにドラッグします。



8. ［構成］ **>** ［デリバリーグループ］ に戻ります。
9. デリバリーグループを選択して ［展開］ をクリックします。

10. ユーザーがアプリをインストールする要求を受信し、ユーザーの承認後にアプリがバックグラウンドでインストールされます。

エンタープライズアプリ

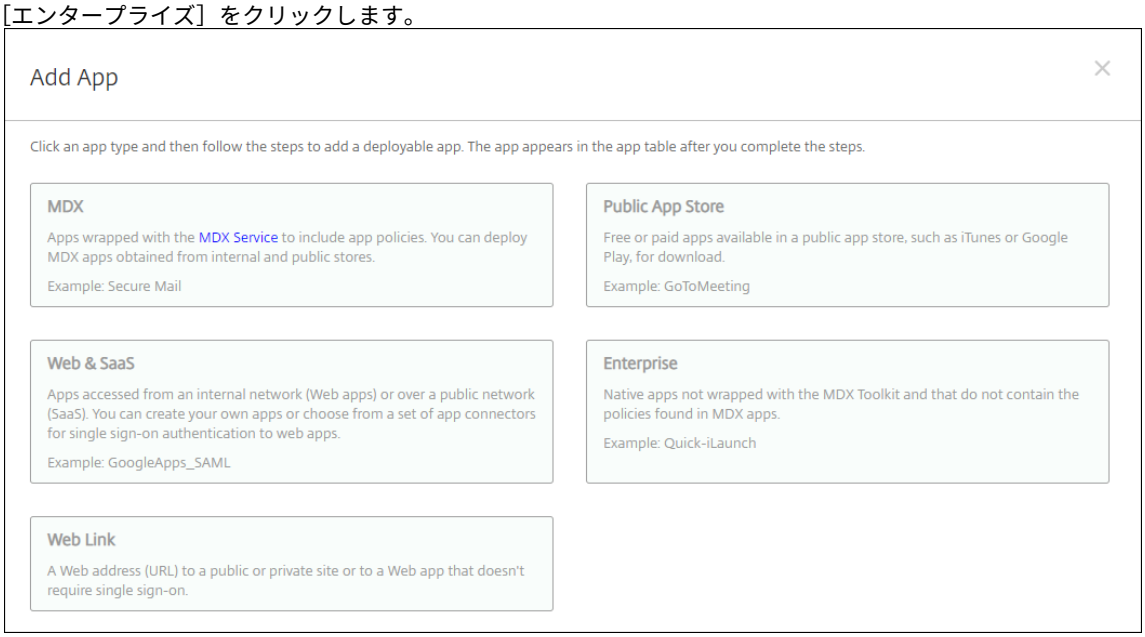
MDX ポリシーが関連付けられていないネイティブアプリを追加することもできます。以下の手順で App Store にはないアプリを追加します。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
OS	iOS/iPadOS/macOS

手順 **1**: アプリの追加および構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。［追加］をクリックします。

2. ［エンタープライズ］をクリックします。



3. ［アプリ情報］ページで以下を構成します：

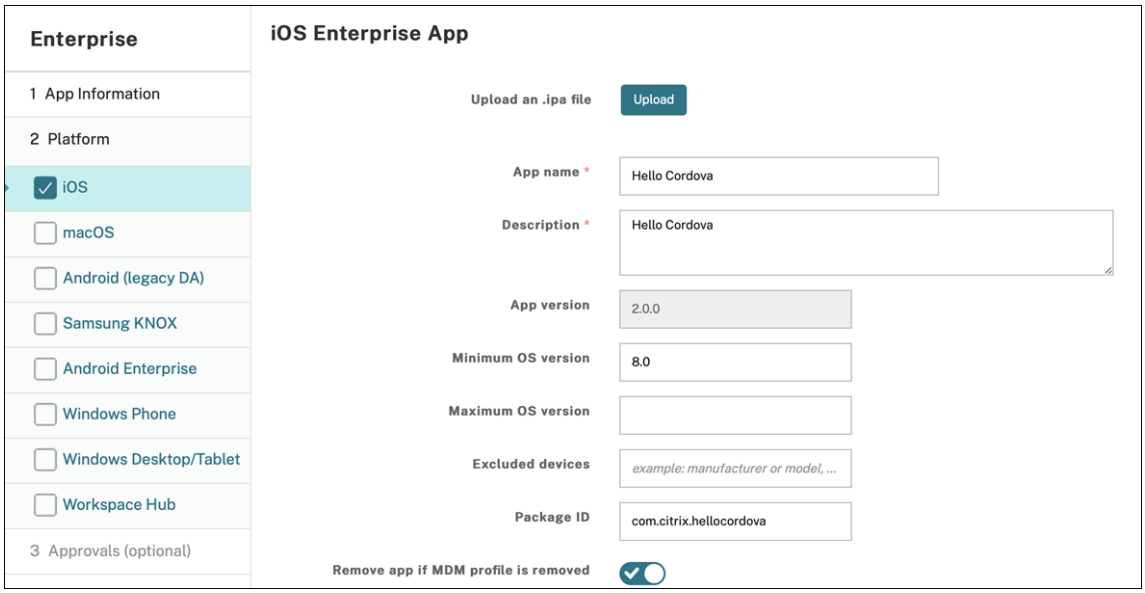
   - 名前：アプリを説明する名前を入力します。この名前は、［アプリ］テーブルの［アプリ名］の下に表示されます。
   - 説明：任意で、アプリの説明を入力します。
   - アプリカテゴリ：任意で、一覧からアプリを追加するカテゴリを選択します。

4. ［次へ］をクリックします。アプリのプラットフォームページが開きます。
5. プラットフォームで **iPhone**、**iPad**、または **macOS** を選択します。
6. IPA ファイル（iOS/iPadOS）か、PKG ファイル（macOS）をアップロードします。
7. ［次へ］をクリックします。［アプリケーション詳細］ページが開きます。
8. 次の設定を構成します：

   - ファイル名：任意で、アプリの名前を新たに入力します。
   - アプリの説明：任意で、アプリの説明を新たに入力します。
   - アプリのバージョン：このフィールドは変更できません。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
   - **MDM** プロファイルが削除されたらアプリを削除します： MDM プロファイルが削除された場合にデバイスからアプリを削除するかどうかを選択します。デフォルトは［オン］です。（iOS/iPadOS のみ）
   - アプリデータのバックアップを阻止します：アプリのデータをバックアップできないようにするかどうかを選択します。デフォルトは［オン］です。（iOS/iPadOS のみ）

- 管理されるアプリケーション：非管理対象のアプリをインストールするとき、監視対象ではないデバイスのユーザーにアプリの管理を許可するよう求める場合は、［オン］を選択します。ユーザーがこの要求を受け入れた場合、アプリは管理対象になります。［管理されるアプリ］設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。（iOS/iPadOS のみ）

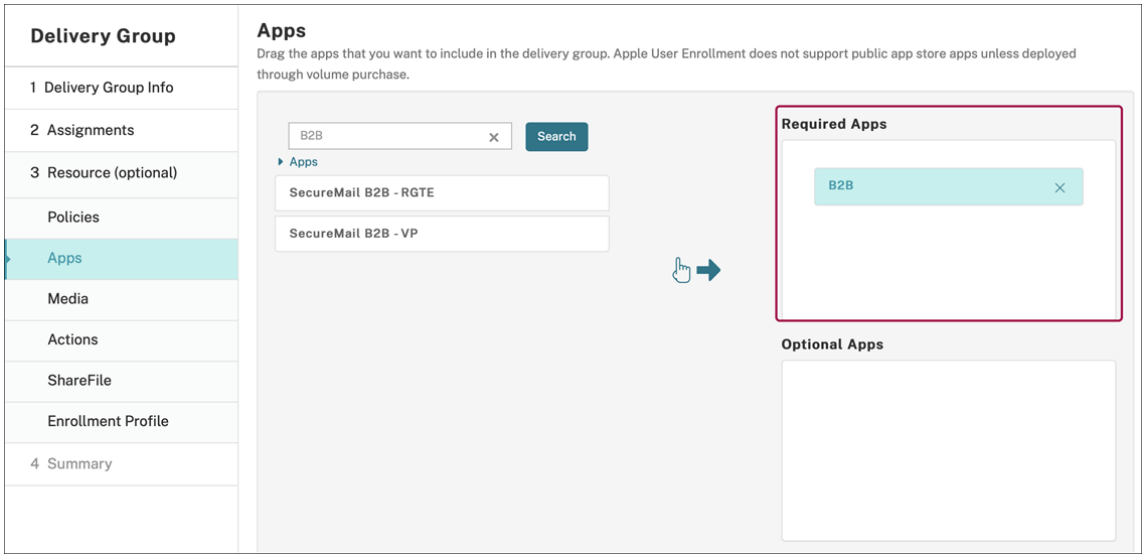
［管理されるアプリ］および［アプリの自動更新］設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。「サーバープロパティ」を参照してください。



9. デリバリーグループをアプリに割り当て、［保存］をクリックします。

手順 **2**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［デリバリグループ］の順に移動します。デリバリーグループを選択して構成し、［アプリ］ページをクリックします。
2. 目的のアプリを ［必須アプリ］ボックスにドラッグします。



3. [構成] > [デリバリーグループ] に移動します。
4. デリバリーグループを選択して [展開] をクリックします。
5. ユーザーがアプリをインストールする要求を受信し、ユーザーの承認後にアプリがバックグラウンドでインストールされます。

MDX アプリ

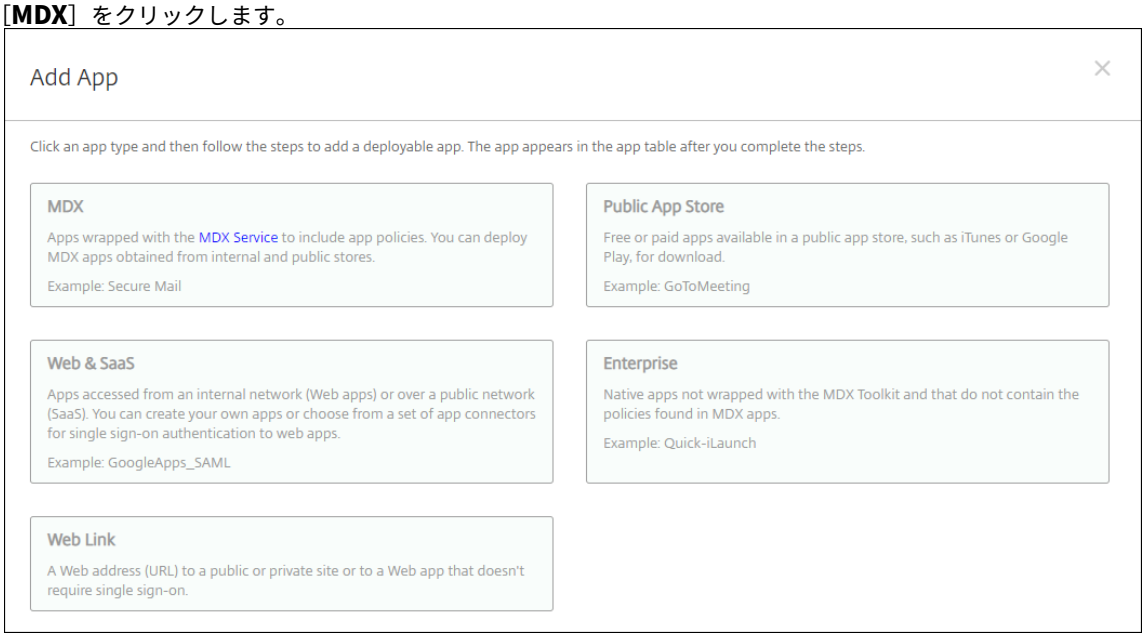
MDX ポリシーとセキュリティ機能を使用するには、MAM SDK 対応アプリまたは MDX でラップされたアプリを追加します。一括購入を使用しなくても、MDX アプリを展開できます。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

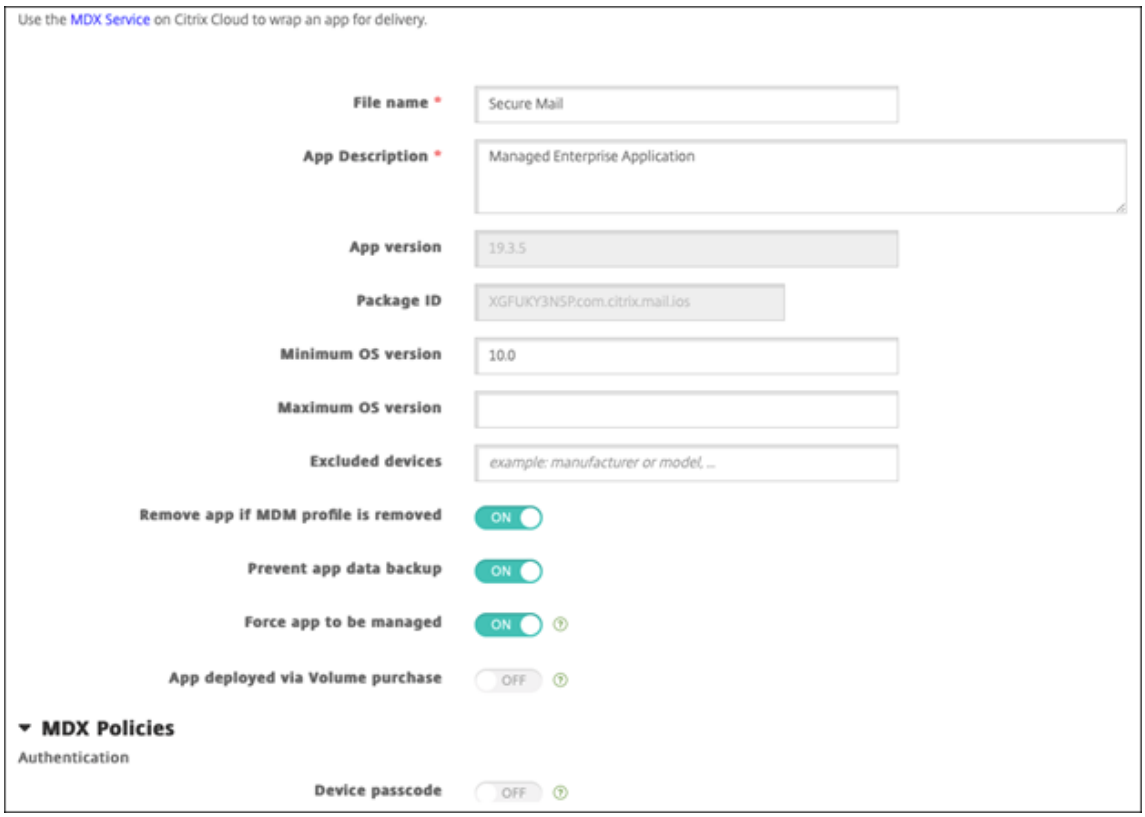
パブリックアプリストアの MDX バージョンのアプリを追加するには、「パブリックアプリストアのアプリ」の手順を実行してから、このセクションの手順を実行します。

手順 **1**：アプリの追加および構成

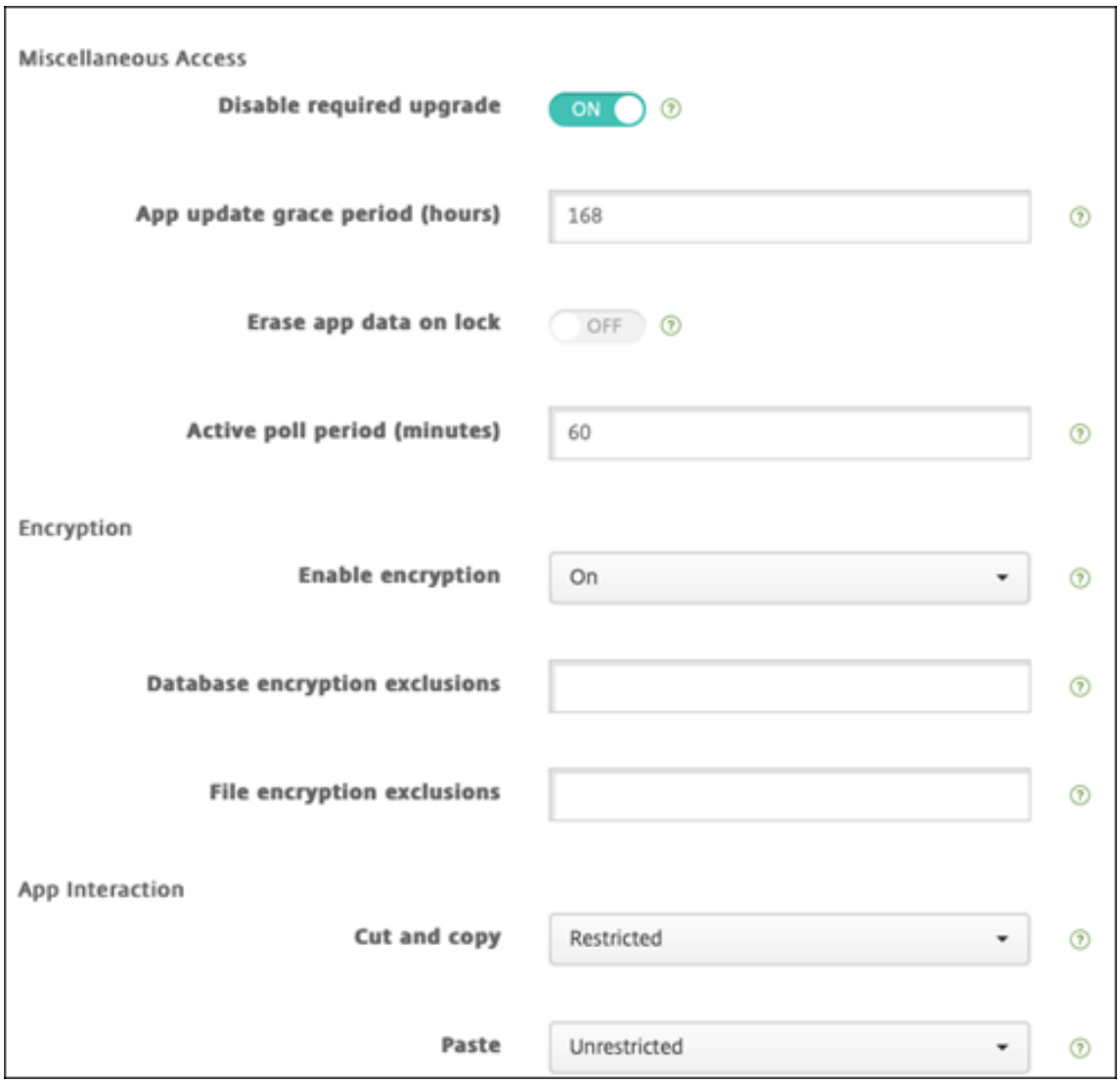
1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。［追加］をクリックします。
2. ［**MDX**］をクリックします。



3. プラットフォームで **iPhone** か **iPad** かを選択します。
4. MDX ファイルをアップロードします。
5. アプリの詳細を構成します。［一括購入経由で展開されたアプリ］を ［オフ］に設定します。また、［管理されるアプリ］機能を有効にすることをお勧めします。



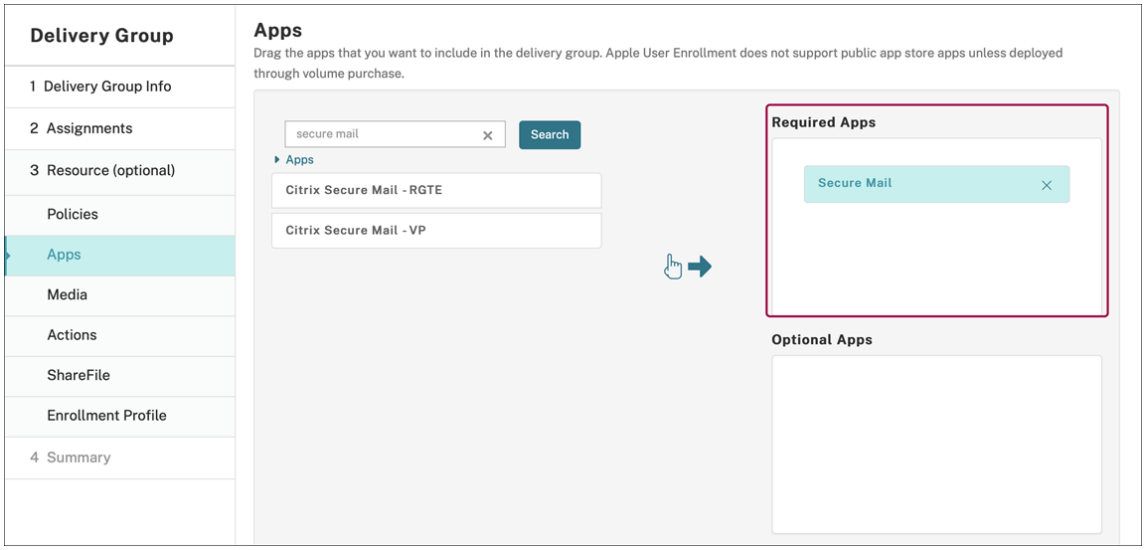
6. MDX ポリシーを構成します。［必要なアップグレードを無効化］を ［オン］に設定します。



7. デリバリーグループをアプリに割り当て、［保存］をクリックします。

手順 **2**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［デリバリグループ］の順に移動して、［追加］をクリックします。
2. ［アプリ］セクションで、目的のアプリを ［必須アプリ］ボックスにドラッグします。



3. [構成] > [デリバリーグループ] に移動します。
4. デリバリーグループを選択して [展開] をクリックします。
5. ユーザーがアプリをインストールする要求を受信し、ユーザーの承認後にアプリがバックグラウンドでインストールされます。

Apple の一括購入を使用して配布された **MDX** アプリ

MDX ポリシーとセキュリティ機能を使用するには、MAM SDK 対応アプリまたは MDX でラップされたアプリを追加します。一括購入を使用してアプリを展開するには、アプリがアプリストアに存在する必要があります。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

手順 **1**: アカウントのリンク

1. Apple Business Manager（ABM）または Apple School Manager（ASM）でセットアップして登録します。これらのプログラムについて詳しくは、Apple のドキュメントを参照してください。
2. 利用中の ABM/ASM アカウントを Citrix Endpoint Management にリンクします。一括購入アカウントのリンクについて詳しくは、「Apple Volume Purchase」を参照してください。
3. 一括購入アカウントを追加する場合、[アプリの自動更新] を有効にします。この設定は、Apple Store に更新がアップされるとユーザーデバイス上のアプリが自動的に更新されるようにします。[管理されるアプリ] 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。

   [管理されるアプリ] および [アプリの自動更新] 設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。「サーバープロパティ」を参照してください。

手順 **2**: **Apple** からアプリおよびライセンスを入手

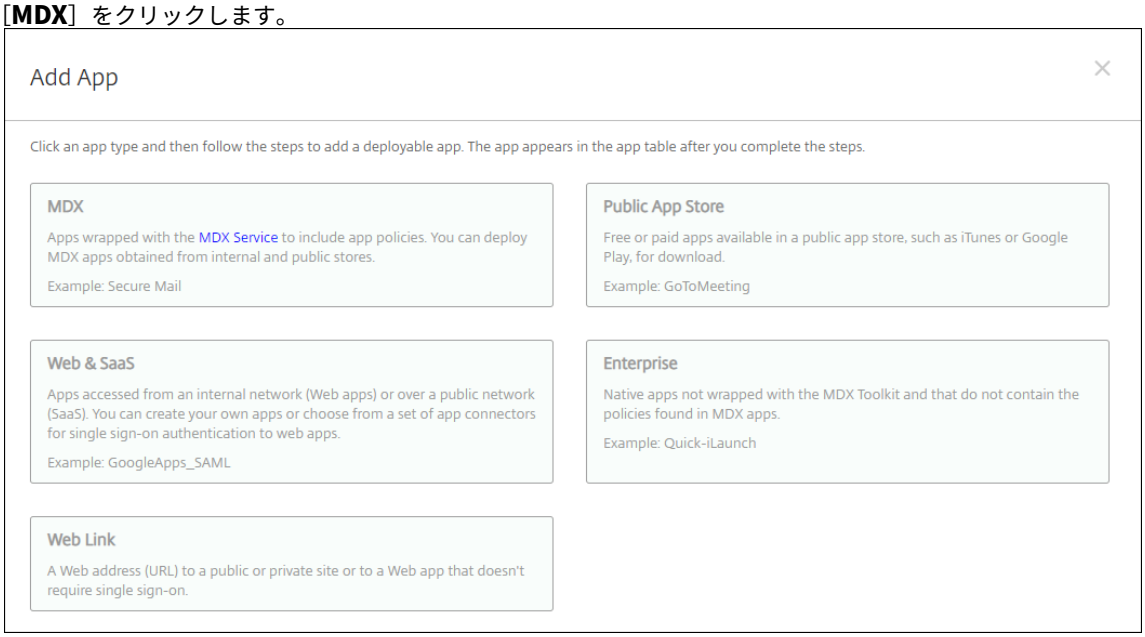
ABM/ASM アカウントでアプリを購入します。Apple Books（iOS または iPadOS 用のみ）と Apple App Store で購入できます。無料の場合であっても「購入」する必要があることに注意してください。ABM/ASM でライセンスを購入したら、Citrix Endpoint Management はアプリを自動的に表示します。

アプリを業務で使用できるようにする方法については、Apple のドキュメントを参照してください。

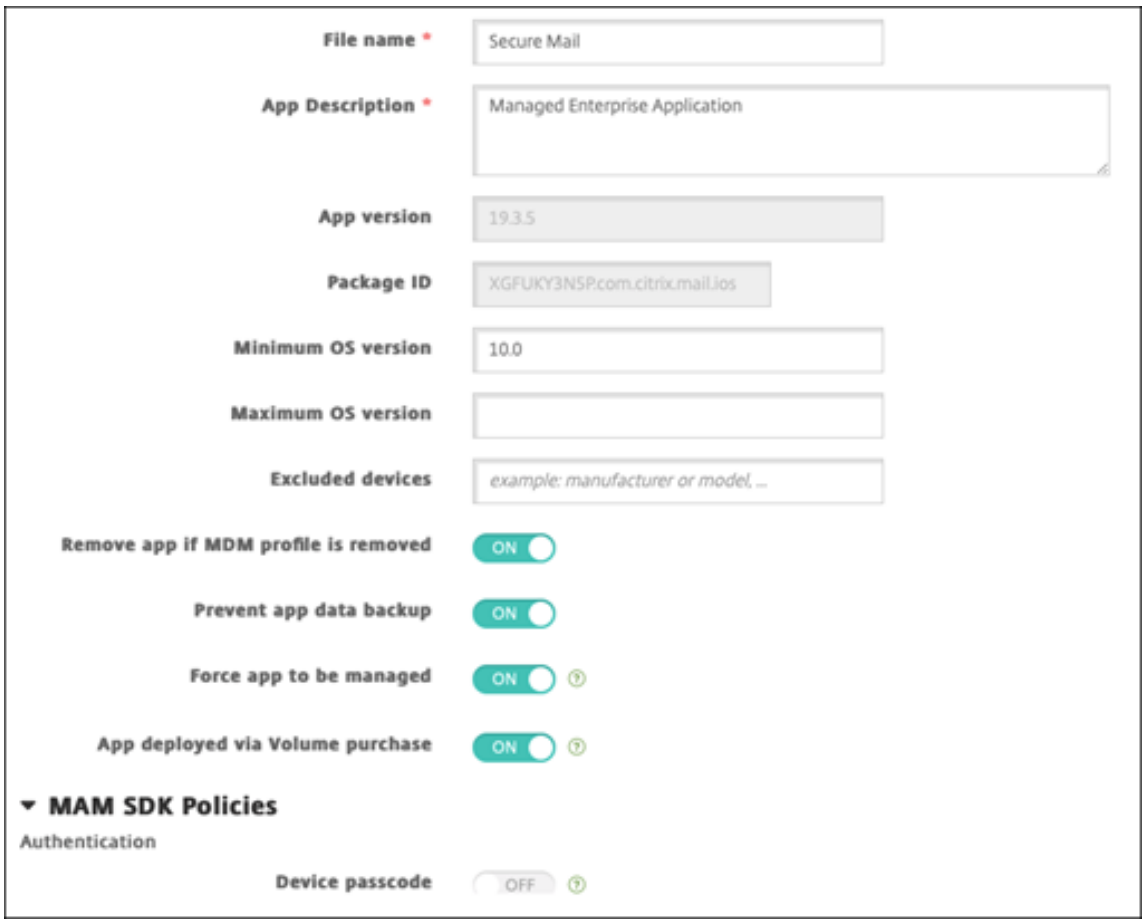
手順 **3**: アプリの追加および構成

1. Citrix Endpoint Management コンソールで ［構成］ **>** ［アプリ］ の順に移動します。[追加] をクリックします。

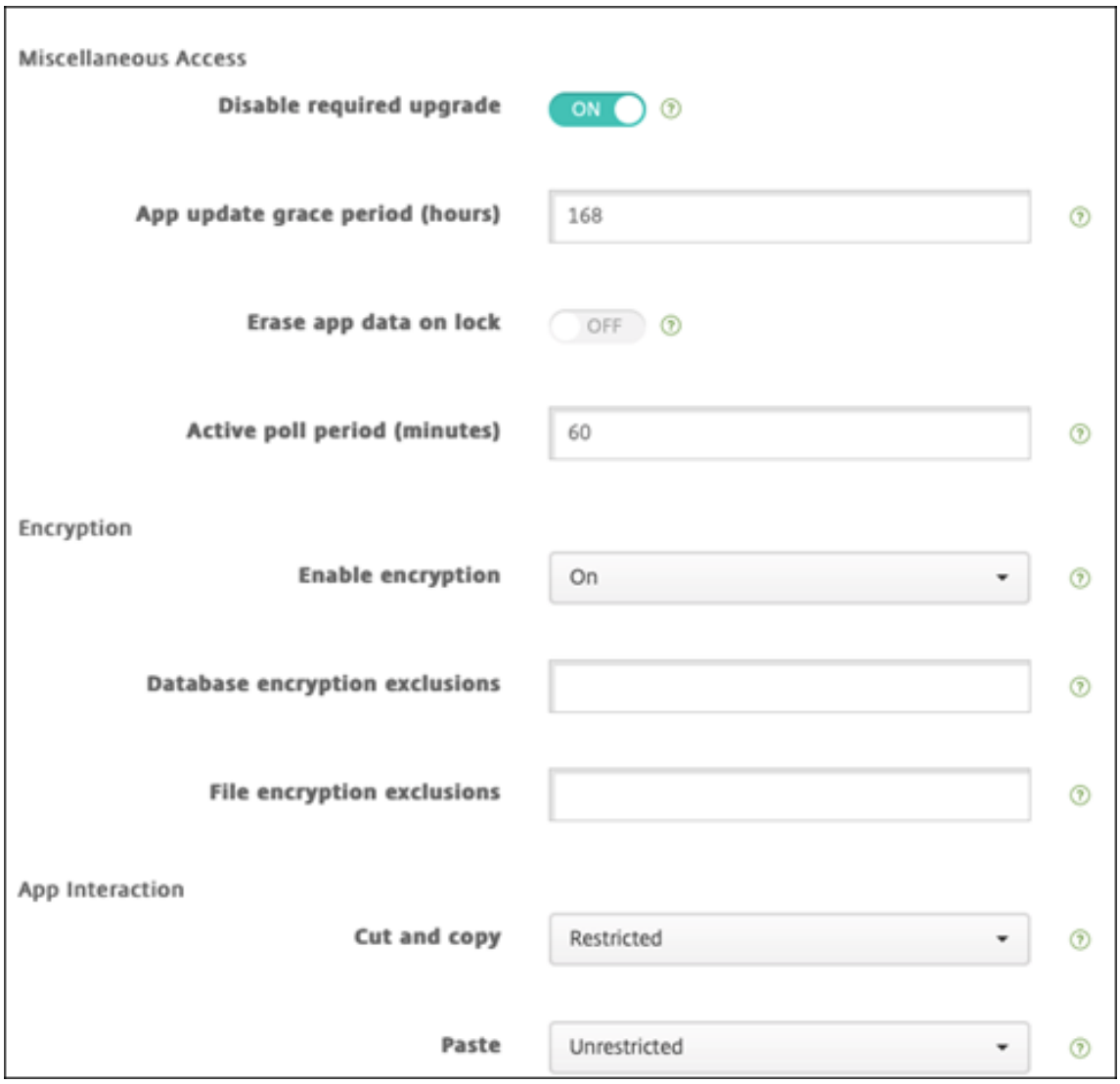
2. [**MDX**] をクリックします。



3. プラットフォームで **iPhone** か **iPad** かを選択します。
4. MDX ファイルをアップロードします。
5. アプリの詳細を構成します。[一括購入経由で展開されたアプリ] を [オン] に設定します。また、[管理されるアプリ] 機能を有効にすることをお勧めします。



6. MDX ポリシーを構成します。[必要なアップグレードを無効化] を [オン] に設定します。

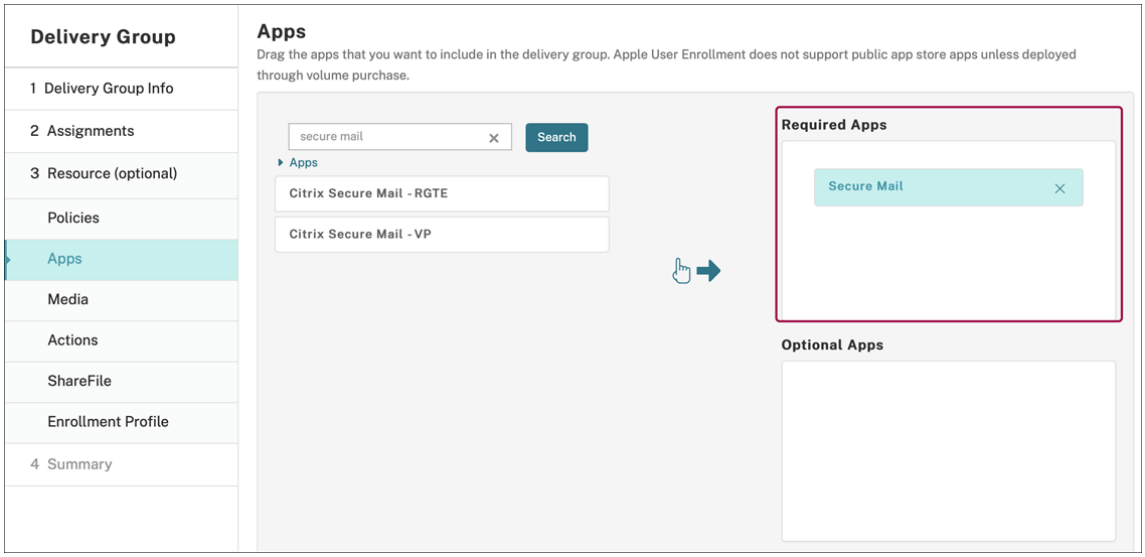


7. デリバリーグループをプラットフォームごとにアプリに割り当て、［保存］をクリックします。

この構成によって、アプリ一覧のこのアプリに 2 つのエントリが表示されます。構成するアプリを選択する場合、種類が **MDX** のアプリを選択します。

手順 **4**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［デリバリグループ］の順に移動して、［追加］をクリックします。
2. ［アプリ］セクションで、目的の MDX アプリを ［必須アプリ］ボックスにドラッグします。



3. [構成] > [デリバリーグループ] に移動します。
4. デリバリーグループを選択して [展開] をクリックします。
5. ユーザーがアプリをインストールする要求を受信し、ユーザーの承認後にアプリがバックグラウンドでインストールされます。

カスタムアプリ

カスタムアプリは独自の B2B（business-to-business）アプリです。Citrix Endpoint Management および Apple 一括購入を使用して、独自のアプリを非公開かつ安全な方法で配布できます。特定のパートナー、クライアント、フランチャイズ加盟店、社内の従業員にアプリを配布できます。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

カスタムアプリの要件

- Apple Business Manager または Apple School Manager アカウント
- Apple の一括購入アカウント（iOS 7 以降を実行しているデバイスが必要です）
- 以下のいずれかの Apple 登録モードを使用して、Citrix Endpoint Management にデバイスを登録します:
  - 自動デバイス登録
  - デバイス登録
  - ユーザー登録

手順 **1**: アカウントのリンク

一括購入を使用してカスタムアプリを展開するには、ご利用中の一括購入アカウントを Citrix Endpoint Management にリンクします。

1. Apple Business Manager（ABM）でセットアップして登録します。これらのプログラムについて詳しくは、Apple のドキュメントを参照してください。
2. 利用中の ABM アカウントを Citrix Endpoint Management にリンクします。一括購入アカウントのリンクについて詳しくは、「Apple Volume Purchase」を参照してください。
3. 一括購入アカウントを追加する場合、[アプリの自動更新] を有効にします。この設定は、Apple Store に更新がアップされるとユーザーデバイス上のアプリが自動的に更新されるようにします。[管理されるアプリ] 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。

   [管理されるアプリ] および [アプリの自動更新] 設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。「サーバープロパティ」を参照してください。

手順 **2**：**ABM** でアプリを構成

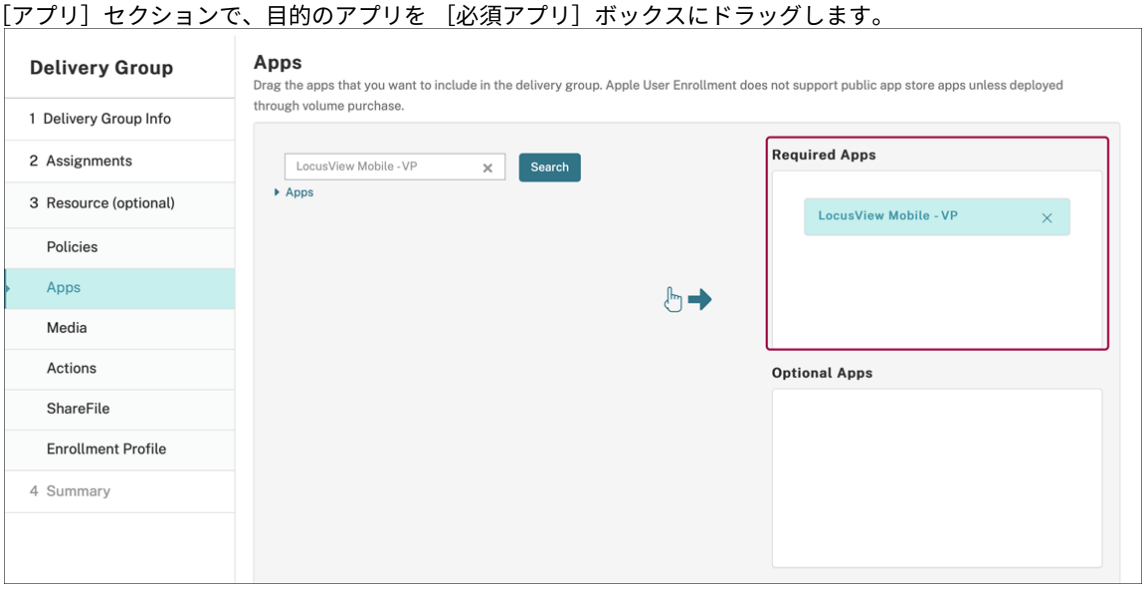
利用中の ABM アカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布するか、他の組織からカスタムアプリのライセンスを購入できます。ABM でカスタムアプリを追加して有効にする方法については、Apple のドキュメントを参照してください。

手順 **3**：**Citrix Endpoint Management** でアプリを追加および構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。一括購入アプリがアプリの一覧に表示されます。
2. 構成するアプリを選択します。［編集］をクリックします。
3. プラットフォームで **iPhone**、**iPad**、または **macOS** を選択します。
4. アプリの配布先のデリバリーグループを選択します。［保存］をクリックします。

手順 **4**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［デリバリグループ］の順に移動して、［追加］をクリックします。
2. ［アプリ］セクションで、目的のアプリを ［必須アプリ］ボックスにドラッグします。



3. ［構成］**>**［デリバリーグループ］に戻ります。
4. 展開されるデリバリーグループを選択して ［展開］をクリックします。
5. ユーザーがアプリ展開要求を受け取ります。アプリは、ユーザーが承認後にバックグラウンドでインストールされます。

MDX 対応カスタムアプリ

MDX ポリシーとセキュリティ機能を使用するには、MAM SDK 対応アプリまたは MDX でラップされたアプリを追加します。

利用できる機能	
デバイスの監視が必要	番号
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

手順 **1**: アカウントのリンク

一括購入を使用してカスタムアプリを展開するには、ご利用中の一括購入アカウントを Citrix Endpoint Management にリンクします。

1. Apple Business Manager（ABM）でセットアップして登録します。これらのプログラムについて詳しくは、Apple のドキュメントを参照してください。

2. 利用中の ABM アカウントを Citrix Endpoint Management にリンクします。一括購入アカウントのリンクについて詳しくは、「Apple Volume Purchase」を参照してください。
3. 一括購入アカウントを追加する場合、[アプリの自動更新] を有効にします。この設定は、Apple Store に更新がアップされるとユーザーデバイス上のアプリが自動的に更新されるようにします。[管理されるアプリ] 設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。

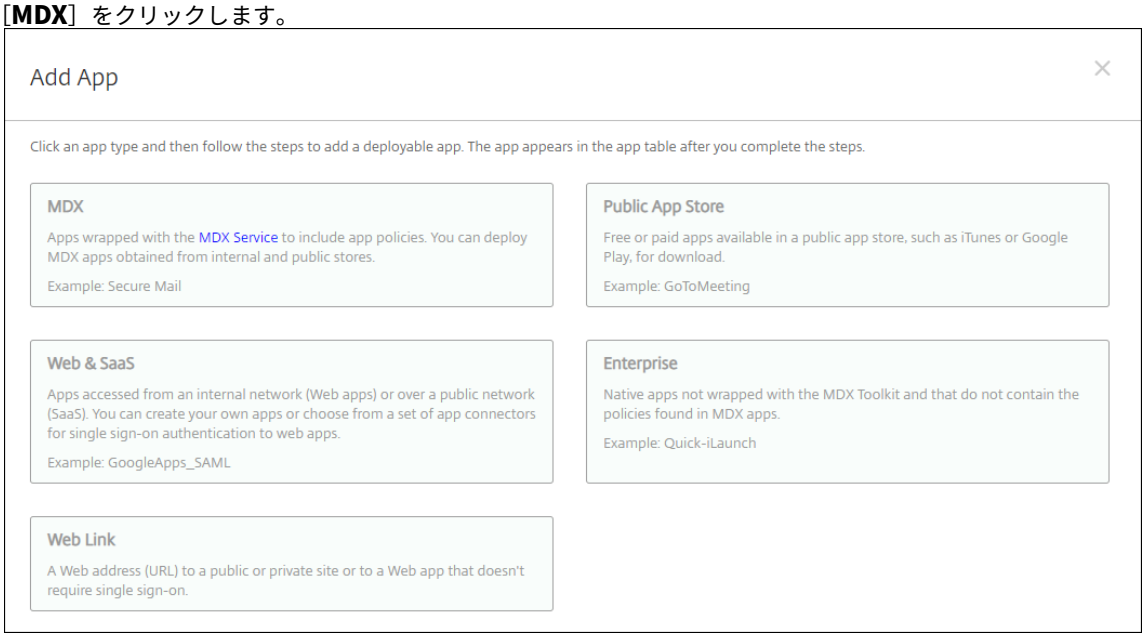
   [管理されるアプリ] および [アプリの自動更新] 設定を使用するには、`apple.app.force.managed`サーバープロパティを有効にします。「サーバープロパティ」を参照してください。

手順 **2**: **ABM** でアプリを構成

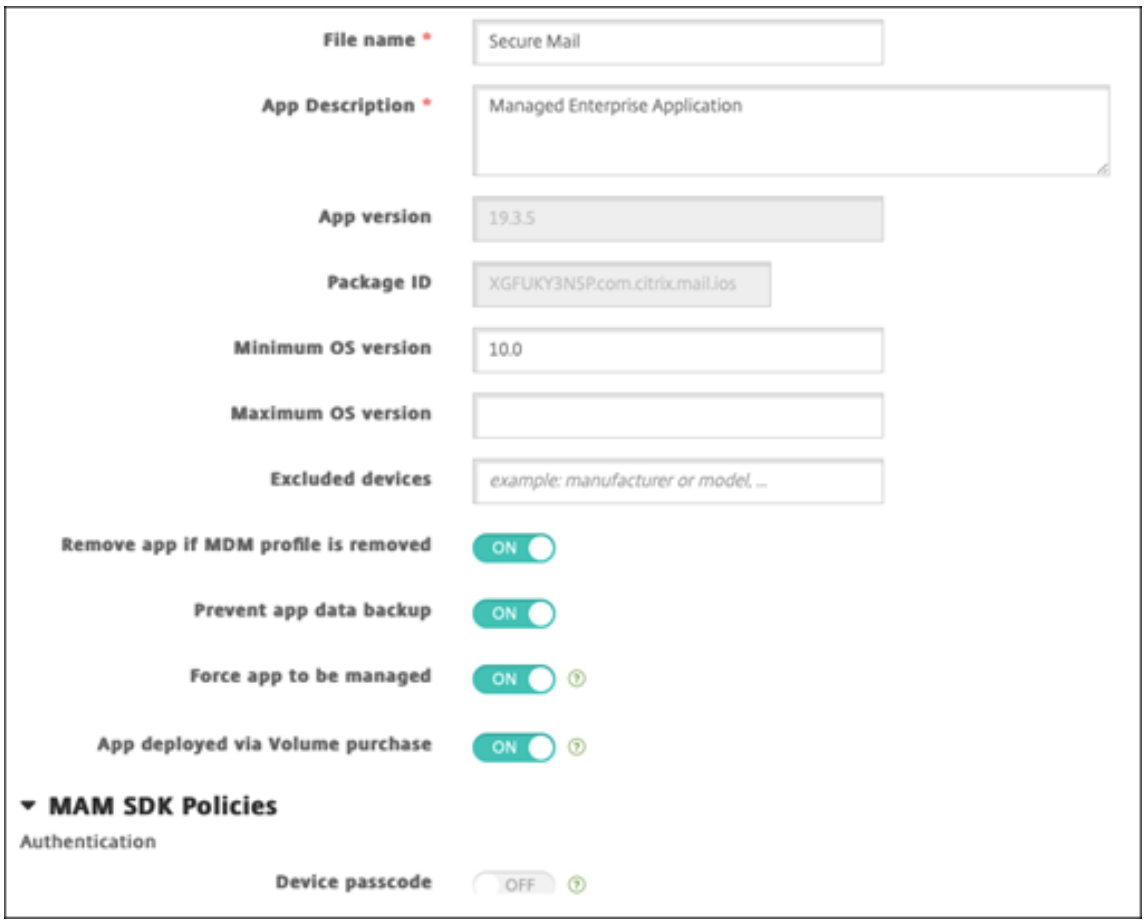
利用中の ABM アカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布するか、他の組織からカスタムアプリのライセンスを購入できます。ABM でカスタムアプリを追加して有効にする方法については、Apple のドキュメントを参照してください。

手順 **3**: **Citrix Endpoint Management** でアプリを追加および構成

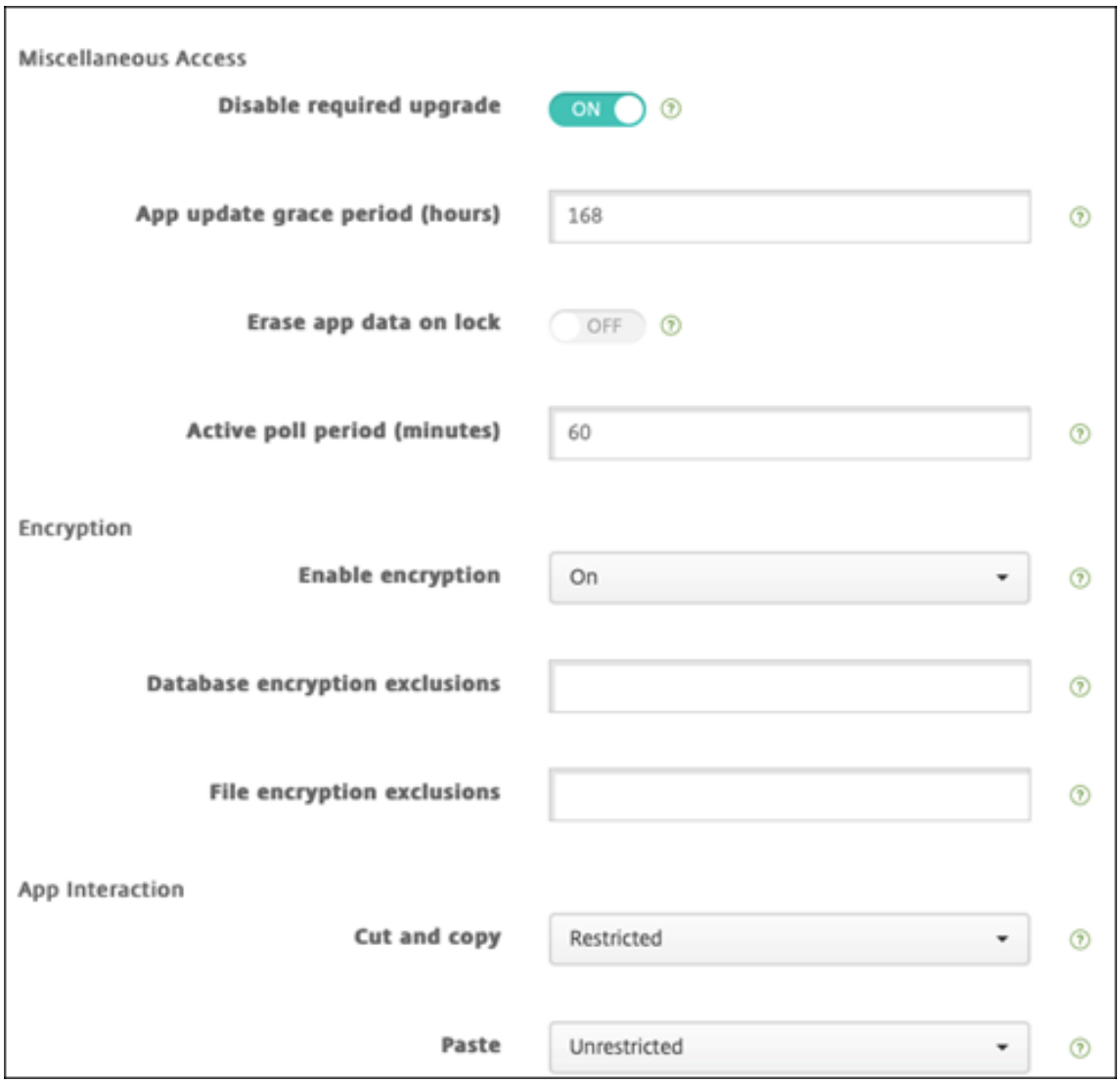
1. Citrix Endpoint Management コンソールで [構成] **>** [アプリ] の順に移動します。[追加] をクリックします。
2. [**MDX**] をクリックします。



3. プラットフォームで **iPhone** か **iPad** かを選択します。
4. 追加するアプリの MDX ファイルをアップロードします。
5. アプリの詳細を構成します。[一括購入経由で展開されたアプリ] を [オン] に設定します。また、[管理されるアプリ] 機能を有効にすることをお勧めします。



6. MDX ポリシーを構成します。[必要なアップグレードを無効化] を [オン] に設定します。

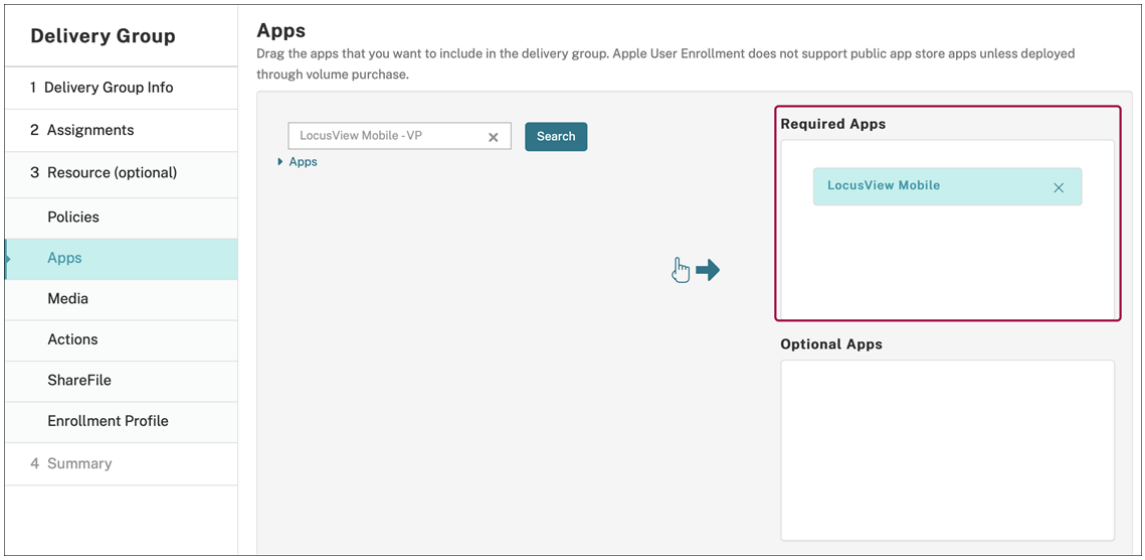


7. デリバリーグループをアプリに割り当て、［保存］をクリックします。

この構成によって、アプリ一覧のこのアプリに 2 つのエントリが表示されます。構成するアプリを選択する場合、種類が **MDX** のアプリを選択します。

手順 **4**：アプリの展開を構成

1. Citrix Endpoint Management コンソールで ［構成］**>**［アプリ］の順に移動します。一括購入アプリがアプリの一覧に表示されます。
2. 構成するアプリを選択します。［編集］をクリックします。
3. プラットフォームごとにアプリの配布先のデリバリーグループを選択します。［保存］をクリックします。
4. ［構成］**>**［デリバリーグループ］に移動してから ［追加］をクリックします。
5. ［アプリ］セクションで、目的の MDX アプリを ［必須アプリ］ボックスにドラッグします。



6. [構成] > [デリバリーグループ] に戻ります。
7. 展開されるデリバリーグループを選択して [展開] をクリックします。
8. ユーザーがアプリ展開要求を受け取ります。アプリは、ユーザーが承認後にバックグラウンドでインストールされます。

任意アプリ（**iOS/iPadOS** のみ）

アプリを必須として展開することをお勧めします。必須アプリはユーザーのデバイスにサイレントモードでインストールされるため、操作を最小限に抑えることができます。この機能を有効にすると、アプリの自動更新も有効になります。

任意アプリでは、ユーザーがインストールするアプリを選択できますが、Citrix Secure Hub で手動でインストールを初期化する必要があります。

任意アプリをインストールするには、ユーザーは Citrix Secure Hub を起動し、［ストア］に移動し、［詳細］を選択して ［追加］をクリックする必要があります。

ネットワークアクセス制御

March 15, 2024

ネットワークアクセス制御（NAC）ソリューションを使用して、Android デバイスおよび Apple デバイスの Citrix Endpoint Management デバイスのセキュリティ評価を拡張できます。NAC ソリューションは Citrix Endpoint Management のセキュリティ評価を使用して、認証の決定を効率的に処理します。Citrix Endpoint Management で構成するデバイスポリシーと NAC フィルターは、NAC アプライアンスを構成した後に適用されます。

Citrix Endpoint Management を NAC ソリューションと組み合わせると、ネットワーク内部のデバイスに対する QoS を向上させ、よりきめ細かい制御を行うことができます。NAC と Citrix Endpoint Management を統合する利点の概要については、「アクセス制御」を参照してください。

Citrix では Citrix Endpoint Management と統合するための以下のソリューションをサポートしています：

- Citrix Gateway

- ForeScout

他の NAC ソリューションとの統合は保証されていません。

ネットワーク内の NAC アプライアンスを使用する場合:

- Citrix Endpoint Management では、iOS、Android Enterprise、および Android デバイスのエンドポイントセキュリティ機能として NAC がサポートされています。
- Citrix Endpoint Management でフィルターを有効にして、規則またはプロパティに基づいてデバイスを NAC の準拠または非準拠として設定できます。例:
  - Citrix Endpoint Management の管理対象デバイスが指定された条件を満たしていない場合、デバイスは［非準拠］としてマークされます。NAC アプライアンスは、ネットワーク上で非準拠デバイスをブロックします。
  - Citrix Endpoint Management 管理対象デバイスに非準拠のアプリがインストールされている場合、NAC フィルターで VPN 接続をブロックできます。その結果、準拠していないユーザーデバイスは、VPN 経由でアプリや Web サイトにアクセスできなくなります。
  - NAC 用の Citrix Gateway を使用する場合は、分割トンネリングを有効にして、Citrix Gateway プラグインが Citrix Gateway に不要なネットワークトラフィックを送信しないようにすることができます。分割トンネリングについて詳しくは、「分割トンネリングの構成」を参照してください。

サポートされる **NAC** 準拠フィルター

Citrix Endpoint Management では、次の NAC 準拠フィルターがサポートされます:

匿名デバイス: デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときに Citrix Endpoint Management がユーザーを再認証できない場合に使用できます。

禁止アプリ: デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。このポリシーについて詳しくは、「アプリアクセスデバイスポリシー」を参照してください。

非アクティブデバイス: ［サーバープロパティ］で デバイスの［非アクティブな日数のしきい値］で定義された期間、非アクティブであったかを確認します。詳しくは、「サーバープロパティ」を参照してください。

不足必須アプリ: デバイスにアプリアクセスポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ: デバイスにアプリアクセスポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード: ユーザーパスワードが正しいかを確認します。iOS デバイスおよび Android デバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかを Citrix Endpoint Management が確認できます。たとえば、iOS では、Citrix Endpoint Management がデバイスにパスコードポリシーを送信する場合、ユーザーは 60 分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス違反かどうかを確認します。通常、このプロパティは自動化された操作により変更されるか、Citrix Endpoint Management API を利用するサードパーティにより変更されます。

失効状態：デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

ルート化された **Android** およびジェイルブレイクした **iOS** デバイス： Android または iOS デバイスがジェイルブレイクされていないかを確認します。

非管理デバイス： Citrix Endpoint Management がデバイスを管理しているかどうかを確認します。たとえば、MAM で登録されているデバイスや未登録のデバイスは管理されていません。

> 注：
>
> ［暗黙的な準拠/非準拠］または［非準拠］フィルターは、Citrix Endpoint Management が管理しているデバイスでのみデフォルト値を設定します。たとえば、禁止されたアプリがインストールされている、または登録されていないデバイスは、非準拠としてマークされます。NAC アプライアンスは、これらのデバイスをネットワークからブロックします。

構成の概要

NAC コンポーネントは、リストされた順序で構成することを推奨します。

1. NAC をサポートするデバイスポリシーを構成します：

   iOS デバイスの場合：「NAC をサポートするように VPN デバイスポリシーを構成する」を参照してください。

   Android Enterprise デバイスの場合：「Citrix SSO に対する Android Enterprise 管理対象の構成の作成」を参照してください。

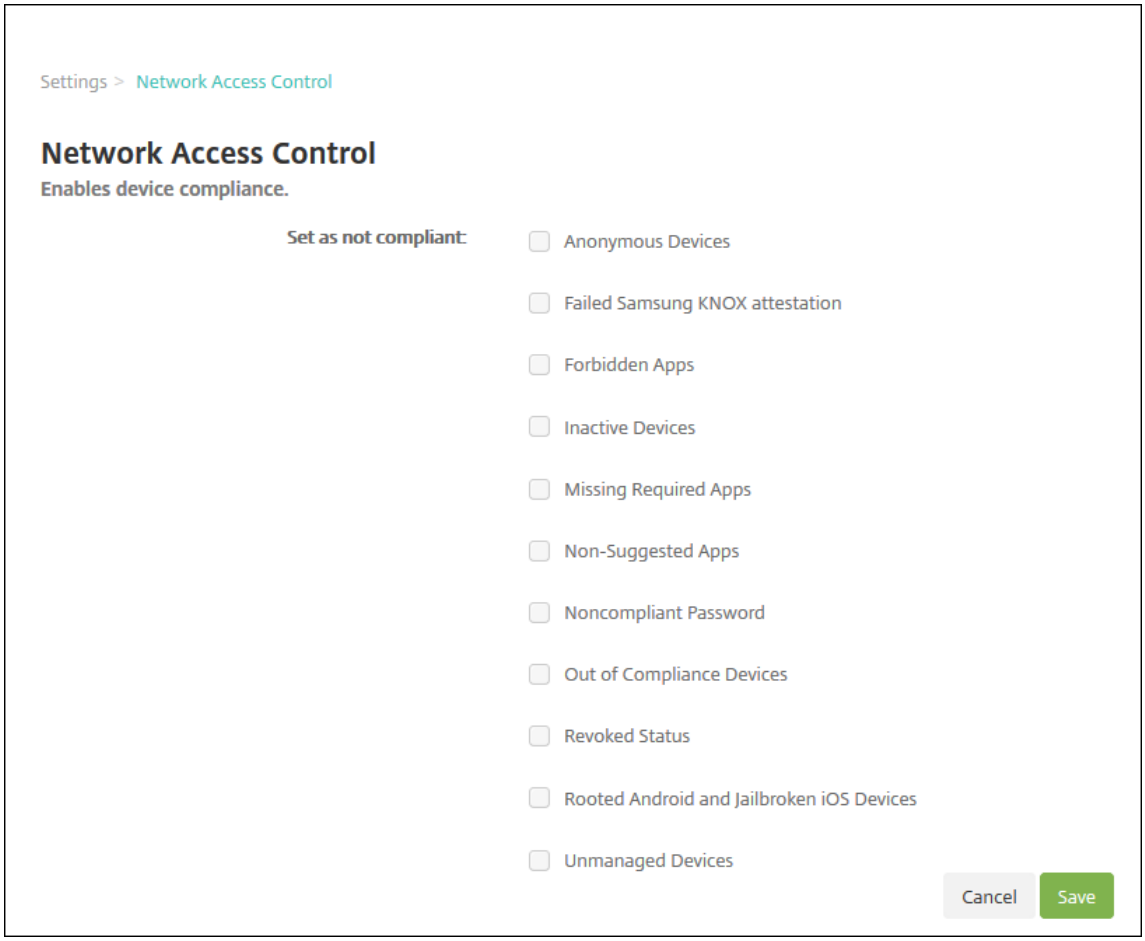
   Android デバイスの場合：「Android 向け Citrix SSO プロトコルを構成する」を参照してください。
2. Citrix Endpoint Management で NAC フィルターを有効にします。
3. NAC ソリューションを構成します：

   - Citrix Gateway。詳細は「NAC をサポートするように Citrix Gateway ポリシーを更新する」を参照してください。

     デバイスに Citrix SSO をインストールする必要があります。「Citrix Gateway クライアント」を参照してください。
   - ForeScout：ForeScout のドキュメントを参照してください。

Citrix Endpoint Management で **NAC** フィルターを有効にする

1. Citrix Endpoint Management コンソールで、［設定］**>**［ネットワークアクセス制御］に移動します。



2. 有効にする ［非準拠として設定］フィルターのチェックボックスをオンにします。
3. ［保存］をクリックします。

NAC をサポートするように Citrix Gateway ポリシーを更新する

VPN 仮想サーバーでは、（クラシックではない）高度な認証ポリシーと VPN セッションポリシーを構成する必要があります。

これらの手順では、次のいずれかの特性を利用して Citrix Gateway を更新します:

- Citrix Endpoint Management と統合されている。
- Citrix Endpoint Management 環境の一部ではなく VPN に設定されており、Citrix Endpoint Management に到達できる。

仮想 VPN サーバー上のコンソールウィンドウで、次の操作を行います。コマンドと例で使用されている FQDN と IP アドレスは架空のものです。

1. VPN 仮想サーバーでクラシックポリシーを使用している場合は、すべてのクラシックポリシーを削除してバインド解除します。クラシックポリシーを確認するには、以下のように入力します:


```
show vpn vserver <VPN_VServer>
```

Classic という単語が含まれている結果をすべて削除します。たとえば、次のようになります: VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0

ポリシーを削除するには、以下のように入力します。

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. 以下のように入力して、対応する詳細セッションポリシーを作成します。

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

たとえば、次のようになります: add vpn sessionPolicy vpn_nac **true** AC_OS_10.10.1.1_A_

3. 以下のように入力して、ポリシーを VPN 仮想サーバーにバインドします。

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority
 100
```

4. 以下のように入力して、認証仮想サーバーを作成します。

```
add authentication vserver <authentication vserver name> <service
 type> <ip address>
```

例: add authentication vserver authvs SSL 0.0.0.0
この例では、0.0.0.0は認証仮想サーバーが公開されていないことを示します。

5. 以下のように入力して、SSL 証明書を仮想サーバーにバインドします。

```
bind ssl vserver <authentication vserver name> -certkeyName <
Webserver certificate>
```

たとえば、次のようになります: bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY

6. VPN 仮想サーバーの認証プロファイルを認証仮想サーバーに関連付けます。最初に、以下のように入力して認証プロファイルを作成します。

```
add authentication authnProfile <profile name> -authnVsName <
authentication vserver name>
```

例:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. 以下のように入力して、認証プロファイルを VPN 仮想サーバーに関連付けます。

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile
name>
```

例:


```
set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
```

8. 以下のように入力して、Citrix Gateway からデバイスへの接続を確認します。

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   たとえば、このクエリは、環境に登録されている最初のデバイス（deviceid_1）の準拠ステータスを取得して接続を検証します：

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   成功した結果は、次の例のようになります。

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. 前の手順が成功したら、Citrix Endpoint Management への Web 認証アクションを作成します。まず、iOS VPN プラグインからデバイス ID を抽出するポリシー式を作成します。次のように入力します。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. 以下のように入力して、Citrix Endpoint Management に要求を送信します。この例では、Citrix Endpoint Management の IP アドレスは10.207.87.82、FQDN はexample.em.cloud.com:4443です。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "Host: example.em.cloud.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+ xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

    Citrix Endpoint Management NAC の正常な応答は、HTTP status 200 OKです。X-Citrix-Device-Stateヘッダーには、Compliantの値が必要です。

11. 以下のように入力して、アクションを関連付ける認証ポリシーを作成します。

    ```
    add authentication Policy <policy name> -rule <rule> -action <web authentication action>
    ```

    たとえば、次のようになります：add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac

12. 以下のように入力して、既存の LDAP ポリシーを拡張ポリシーに変換します。

    ```
    add authentication Policy <policy_name> -rule <rule> -action <
    LDAP action name>
    ```

    たとえば、次のようになります: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 以下のように入力して、LDAP ポリシーを関連付けるポリシーラベルを追加します。

    ```
    add authentication policylabel <policy_label_name>
    ```

    たとえば、次のようになります: `add authentication policylabel ldap_pol_label`

14. 以下のように入力して、LDAP ポリシーをポリシーラベルに関連付けます。

    ```
    bind authentication policylabel ldap_pol_label -policyName
    ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
    ```

15. 準拠デバイスを接続して NAC テストを実行し、LDAP 認証が正常に行われたことを確認します。次のように入力します。

    ```
    bind authentication vserver <authentication vserver> -policy <web
     authentication policy> -priority 100 -nextFactor <ldap policy
    label> -gotoPriorityExpression END
    ```

16. 認証仮想サーバーに関連付ける UI を追加します。次のコマンドを入力してデバイス ID を取得します。

    ```
    add authentication loginSchemaPolicy <schema policy>-rule <rule>
    -action lschema_single_factor_deviceid
    ```

17. 以下のように入力して、認証仮想サーバーをバインドします。

    ```
    bind authentication vserver authvs -policy lschema_xm_nac_pol -
    priority 100 -gotoPriorityExpression END
    ```

18. Citrix Secure Hub 接続を有効にする LDAP 拡張認証ポリシーを作成します。次のように入力します。

    ```
    add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER
    (\"User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
    ```

    ```
    bind authentication vserver authvs -policy ldap_xm_test_pol -
    priority 110 -gotoPriorityExpression NEXT
    ```

Windows デスクトップとタブレット

December 8, 2023

Citrix Endpoint Management は、Windows 10 および Windows 11 デバイスをモバイルデバイス管理（MDM: Mobile Device Management）に登録します。Citrix Endpoint Management では、MDM で登録した Windows 10 および Windows 11 デバイスに対して、次の種類の認証をサポートしています:

- ドメインベース認証
  - Active Directory
  - Azure Active Directory
- ID プロバイダー:
  - Azure Active Directory
  - Citrix ID プロバイダー

サポートされている認証方法について詳しくは、「証明書と認証」を参照してください。

Windows 10 または Windows 11 デバイスの管理を開始するための一般的なワークフローは次のとおりです:

1. オンボーディングプロセスの完了。「オンボードとリソースのセットアップ」と「デバイス登録およびリソース配信の準備」を参照してください。

   AutoDiscovery サービスを使用して Windows デバイスを登録する場合は、Citrix AutoDiscovery サービスを構成する必要があります。Citrix テクニカルサポートにサポートを要請してください。詳しくは、「Windows デバイスの AutoDiscovery の要請」を参照してください。
2. 登録方法の選択と構成。「サポートされている登録方法」を参照してください。
3. Windows デスクトップデバイスおよびタブレットデバイスポリシーを構成します。
4. ユーザーは Windows 10 および Windows 11 デバイスを登録します。
5. デバイスとアプリのセキュリティ操作の設定。「セキュリティ操作」を参照してください。

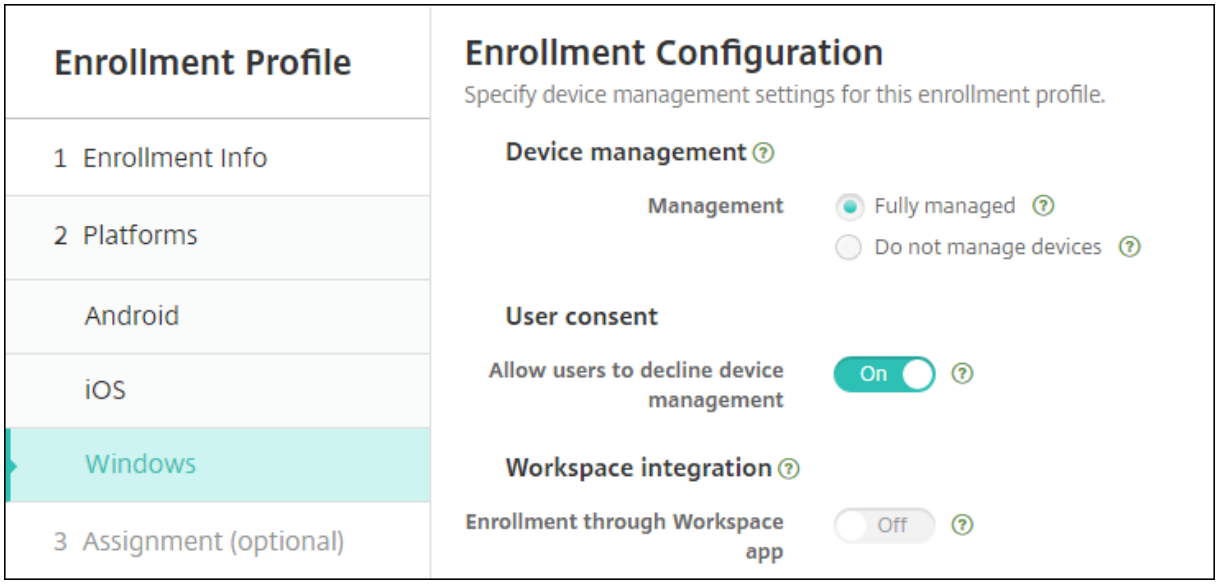
サポートされているオペレーティングシステムについては、「サポートされるデバイスオペレーティングシステム」を参照してください。

サポートされている登録方法

登録プロファイルで Windows 10 および Windows 11 デバイスの管理方法を指定します。次の 2 つのオプションを使用できます:

- 完全管理対象（MDM 登録）
- デバイスを管理しない（MDM 登録なし）

Windows 10 および Windows 11 デバイスの登録設定を構成するには、[構成] **>** [登録プロファイル] **>** [**Windows**] の順に移動します。登録プロファイルについて詳しくは、「登録プロファイル」を参照してください。



次の表は、Windows 10 および Windows 11 デバイスでサポートされている Citrix Endpoint Management での登録方法を示しています:

方法	サポート対象
Azure Active Directory の登録	はい
AutoDiscovery サービスの登録	はい
Windows 一括登録	はい
手動登録	はい
登録招待	番号

> 注:
>
> - 手動登録では、ユーザーは Citrix Endpoint Management サーバーの完全修飾ドメイン名（FQDN）を入力する必要があります。手動登録はお勧めしません。代わりに、他の方法で、ユーザーの登録プロセスを簡略化します。
> - Windows デバイスに登録招待を送信することはできません。Windows ユーザーはデバイスから直接登録します。

Windows デスクトップデバイスおよびタブレットデバイスポリシーの構成

デバイスポリシーを使用して、Citrix Endpoint Management と、Windows 10 または Windows 11 を実行しているデスクトップデバイスおよびタブレットデバイスを実行するデバイスとの通信に関する構成を行います。次の表は、Windows デスクトップデバイスおよびタブレットデバイスで使用可能なデバイスポリシーの一覧です。

–	–	–
[アプリ構成](/ja-jp/citrix-endpoint-management/policies/app-configuration-policy.html#windows-desktoptablet-settings)	[アプリインベントリ](/ja-jp/citrix-endpoint-management/policies/app-inventory-policy.html)	[アプリのロック](/ja-jp/citrix-endpoint-management/policies/app-lock-policy.html#windows-desktop-and-tablet-settings)
[アプリのアンインストール](/ja-jp/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Application Guard](/ja-jp/citrix-endpoint-management/policies/application-guard-policy.html)	[BitLocker](/ja-jp/citrix-endpoint-management/policies/bitlocker-policy.html#windows-desktop-and-tablet-settings)
[資格情報](/ja-jp/citrix-endpoint-management/policies/credentials-policy.html#windows-desktoptablet-settings)	[カスタム XML](/ja-jp/citrix-endpoint-management/policies/custom-xml-policy.html)	[Defender](/ja-jp/citrix-endpoint-management/policies/defender-policy.html)
[Device Guard](/ja-jp/citrix-endpoint-management/policies/device-guard-policy.html)	[デバイス正常性構成証明](/ja-jp/citrix-endpoint-management/policies/device-health-attestation-policy.html)	[Exchange](/ja-jp/citrix-endpoint-management/policies/exchange-policy.html#windows-desktoptablet-settings)
[ファイアウォール](/ja-jp/citrix-endpoint-management/policies/firewall-device-policy.html#windows-desktop-and-tablet-settings)	[キオスク](/ja-jp/citrix-endpoint-management/policies/kiosk-policy.html#windows-desktop-and-tablet-settings)	[ネットワーク](/ja-jp/citrix-endpoint-management/policies/ne
policy.html#windows-desktoptablet-settings)
[Office](/ja-jp/citrix-endpoint-management/policies/office-policy.html)	[OS 更新](/ja-jp/citrix-endpoint-management/policies/control-os-updates.html#windows-desktop-and-tablet-settings)	[パスコード](/ja-jp/citrix-endpoint-management/policies/passcode-policy.html#windows-desktoptablet-settings)
[制限](/ja-jp/citrix-endpoint-management/policies/restrictions-policy.html#windows-desktoptablet-settings)	[ストア](/ja-jp/citrix-endpoint-management/policies/store-policy.html)	[使用条件](/ja-jp/citrix-endpoint-management/policies/terms-and-conditions-policy.html#windows-tablet-settings)
[VPN](/ja-jp/citrix-endpoint-management/policies/vpn-policy.html#windows-desktoptablet-settings)	[Web クリップ](/ja-jp/citrix-endpoint-management/policies/webclip-policy.html#windows-desktoptablet-settings)	[Windows エージェント](/ja-jp/citrix-endpoint-management/policies/windows-agent-policy.html)
Windows GPO の構成	Windows Hello for Business

Azure Active Directory を使用した **Windows 10** および **Windows 11** デバイスの登録

> 重要:

> ユーザーが登録する前に、Azure で Azure Active Directory（AD）設定を構成してから Citrix Endpoint Management を構成する必要があります。詳しくは、「Citrix Endpoint Management の Azure AD への接続」を参照してください。

Windows 10 および Windows 11 デバイスは、AD 認証の統合手段として Azure に登録できます。この登録には Azure AD のプレミアムサブスクリプションが必要です。

管理者は、以下のいずれかの方法を用いて、Windows 10 および Windows 11 デバイスを Microsoft Azure AD に統合できます:

- 会社所有のデバイスの場合:
  - 初めてデバイスに電源を入れて Azure AD に参加させるときに MDM を登録する。このシナリオでは、ユーザーは次の記事で説明されているとおりに登録を完了します:「https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx」。

    この方法で登録する Windows デバイスの場合は、Windows AutoPilot を使用してデバイスのセットアップと事前構成を行うことができます。詳しくは、「Windows AutoPilot を使用してデバイスをセットアップおよび構成する」を参照してください。
  - デバイスを構成したあと Windows の ［設定］ページからデバイスを Azure AD に参加させるときに MDM に登録する。このシナリオでは、ユーザーは「デバイスを構成したあと Azure AD に参加するときに MDM に登録する」で説明されているとおりに登録を完了します。
- 個人用デバイス（BYOD またはモバイルデバイス）の場合:
  - Microsoft の仕事用アカウントを Windows に追加して Azure AD に登録するときに MDM に登録する。このシナリオでは、ユーザーは「Azure AD に登録するときに MDM に登録する」で説明されているとおりに登録を完了します。

デバイスを構成したあと **Azure AD** に参加するときに **MDM** に登録する

1. デバイスで、［スタート］メニューから ［設定］**>** ［アカウント］**>** ［職場または学校へのアクセス］に移動して［接続］をクリックします。
2. ［職場または学校アカウントのセットアップ］ダイアログボックスの ［別の操作］で、［このデバイスを **Azure Active Directory** に参加させる］をクリックします。
3. Azure AD の資格情報を入力し、［サインイン］をクリックします。
4. 組織が要求している契約条件に同意します。
   - ユーザーが［拒否］をクリックすると、デバイスは Azure AD に参加せず、Citrix Endpoint Management にも登録されません。
5. 登録処理を続行するには、［参加］をクリックします。
6. ［完了］をクリックして、登録処理を完了します。

Azure AD に登録するときに **MDM** に登録する

1. デバイスで、［スタート］メニューから ［設定］**>**［アカウント］**>**［職場または学校へのアクセス］に移動して［接続］をクリックします。
2. ［職場または学校アカウントのセットアップ］ダイアログボックスで、Azure AD 資格情報を入力して ［サインイン］をクリックします。
3. 組織が要求している契約条件に同意します。デバイスが Azure AD に登録され、Citrix Endpoint Management に登録されます。
    - ユーザーが ［拒否］をクリックすると、デバイスは Azure AD に登録されますが、Citrix Endpoint Management には登録されません。そのアカウントには ［情報］ボタンがありません。
4. 登録処理を続行するには、［参加］をクリックします。
5. ［完了］をクリックして、登録処理を完了します。

AutoDiscovery サービスを使用した **Windows** デバイスの登録

Windows デバイスの AutoDiscovery サービスを構成するには、Citrix テクニカルサポートにサポートを要請してください。詳しくは、「Windows デバイスの AutoDiscovery の要請」を参照してください。

> 注:
>
> Windows デバイスの登録では、SSL リスナー証明書が公開証明書である必要があります。自己署名 SSL 証明書の登録は失敗します。

ユーザーは次の手順を実行して登録を完了します:

1. デバイスで、［スタート］メニューから ［設定］**>**［アカウント］**>**［職場または学校へのアクセス］に移動して［デバイス管理でのみ登録］をクリックします。
2. ［職場または学校アカウントのセットアップ］ダイアログボックスで会社のメールアドレスを入力し、［次へ］をクリックします。

    ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します (例: `foo\@mydomain.com`)。存在しないメールアドレスを使用すると、ユーザーは Windows の組み込みのデバイス管理によって登録が実行される、既知の Microsoft の制限を回避できます。［サービスに接続しています］ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。デバイスが Citrix Endpoint Management サーバーを検出し、登録処理が開始されます。
3. 認証情報を入力し、［続行］をクリックします。
4. ［使用条件］ダイアログボックスで、デバイスの管理に同意して、［同意する］をクリックします。

ドメインポリシーが MDM 登録を無効にしている場合、AutoDiscovery サービスを介してドメイン参加済み Windows デバイスを登録しようとすると失敗します。ユーザーは代わりに次のいずれかの方法を使用できます:

- デバイスをドメインから削除し、登録してから再度参加させます。
- Citrix Endpoint Management サーバーの FQDN を入力して続行します。

Windows 一括登録

Windows 一括登録では、デバイスを再イメージ化することなく、MDM サーバーで管理する多数のデバイスをセットアップできます。プロビジョニングパッケージを使用して、Windows 10 および Windows 11 デスクトップデバイスおよびノートブックデバイスを一括登録します。詳しくは、「Windows デバイスの一括登録」を参照してください。

セキュリティ操作

Windows 10 および Windows 11 デバイスでは、次のセキュリティ操作がサポートされています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

検索	ロック	Reboot
取り消し	選択的なワイプ	ワイプ

Citrix Endpoint Management の Azure AD への接続

Windows 10 および Windows 11 デバイスは Azure に登録できます。Azure AD で作成されたユーザーは、デバイスにアクセスできます。Citrix Endpoint Management は、MDM サービスとして Microsoft Azure に展開されます。Citrix Endpoint Management を Azure AD に接続すると、ユーザーはデバイスを Azure AD に登録するときに、デバイスを Citrix Endpoint Management に自動的に登録できます。

Citrix Endpoint Management を Azure AD に接続するには、次の手順を実行します:

1. Azure ポータルで［**Azure Active Directory**］**>**［モビリティ（**MDM** および **MAM**）］**>**［アプリケーションの追加］に移動して、［オンプレミス **MDM** アプリケーション］をクリックします。
2. アプリケーションの名前を入力し、［追加］をクリックします。
3. （オプション）Azure では、cloud.com などの検証されていないドメインの IDP 構成への使用は許可されていません。Citrix Endpoint Management の登録 FQDN に cloud.com が含まれている場合は、Citrix サポートに連絡して、Azure の TXT レコードを提供してください。Citrix サポートがサブドメインを検証し、構成の続行を許可します。FQDN が独自のドメインにある場合、通常は Azure 内で検証できます。
4. 作成したアプリケーションを選択し、以下を構成して、［保存］をクリックします。
    - **MDM** ユーザースコープ。［すべて］を選択します。

- **MDM** 利用規約 **URL**。「`https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`」の形式で入力します。
- **MDM** 検出 **URL**。「`https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`」の形式で入力します。

5. ［オンプレミス **MDM** アプリケーションの設定］をクリックします。
   - ［プロパティ］ペインで、「`https://< Citrix Endpoint Management Enrollment FQDN>:8443`」の形式で ［アプリ **ID URI**］を設定します。このアプリ ID URI は、他のアプリで再び使用できない一意の ID です。
   - ［必要なアクセス許可］ペインで、［**Microsoft Graph**］および［**Windows Azure Active Directory**］を選択します。
   - ［キー］ペインで、認証キーを作成します。［保存］をクリックして、キー値を表示します。キー値は 1 回だけ表示されます。後で使用するためにキーを保存します。手順 7 でキーが必要になります。
6. Citrix Endpoint Management コンソールで ［設定］**>**［**ID** プロバイダー（**IDP**）］に移動し、［追加］をクリックします。
7. ［検出 **URL**］ページで、以下を構成して ［次へ］をクリックします。
   - **IDP** 名。作成する ID プロバイダー接続を識別できる一意の名前を入力します。
   - **IDP** の種類。［**Azure Active Directory**］を選択します。
   - テナント **ID**。Azure のディレクトリ **ID**。Azure で ［**Azure Active Directory**］**>**［プロパティ］に移動すると確認できます。
8. ［**Windows MDM** 情報］ページで、以下を構成して ［次へ］をクリックします。
   - アプリ **ID URI**。Azure に入力した APP ID URI 値。
   - クライアント **ID**。Azure の ［プロパティ］ペインに表示されるアプリケーション ID。
   - キー。上記の手順 4 で作成して保存したキー値。
9. ［**IDP** クレームの使用状況］ページで、以下を構成して［次へ］をクリックします。
   - ユーザー識別子の種類。［**userPrincipalName**］を選択します。
   - ユーザー識別子の文字列。「`${ id_token } .upn`」を入力します。
10. ［保存］をクリックします。
11. Azure AD ユーザーをローカルユーザーとして追加し、ローカルユーザーグループに割り当てます。
12. 契約条件デバイスポリシーと、そのローカルユーザーグループを含むデリバリーグループを作成します。

Workspace Environment Management と統合した場合のデバイス管理

Workspace Environment Management（WEM）だけでは、MDM は展開できません。Citrix Endpoint Management だけでは、Windows 10 および Windows 11 デバイスしか管理できません。この 2 つを統合することで、

WEM は MDM 機能にアクセスでき、Citrix Endpoint Management を通じて幅広い Windows オペレーティングシステムを管理できます。管理は、Windows GPO の構成という形で行われます。現在、管理者は ADMX ファイルを Citrix Endpoint Management にインポートし、Windows 10 および Windows 11 のデスクトップおよびタブレットにプッシュして特定のアプリケーションを構成しています。Windows GPO の構成デバイスポリシーを使用して、GPO を構成し、変更を WEM サービスにプッシュできます。次に WEM エージェントを使用して GPO をデバイスとそのアプリに適用します。

MDM 管理は、WEM 統合の要件ではありません。Citrix Endpoint Management がネイティブでサポートしていないデバイスであっても、WEM がサポートするすべてのデバイスに GPO 構成をプッシュできます。

サポートされているデバイスの一覧については、「オペレーティングシステムの要件」を参照してください。

Windows GPO の構成デバイスポリシーを受信するデバイスは、WEM という新しい Citrix Endpoint Management モードで実行されます。登録済みデバイスの ［管理］**>**［デバイス］一覧で WEM 管理対象デバイスの ［モード］列に **WEM** が表示されます。

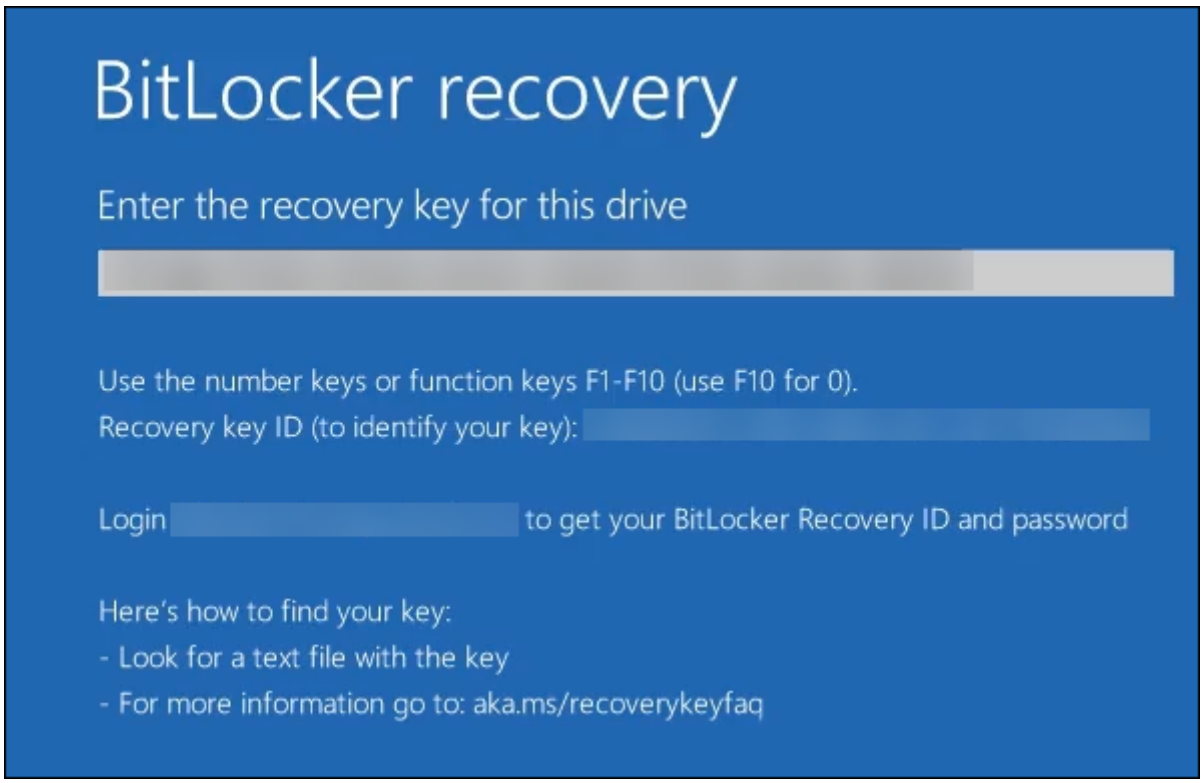
詳しくは、「Windows GPO の構成デバイスポリシー」を参照してください。

BitLocker 回復キー

BitLocker を使用したディスクの暗号化は、有用なセキュリティ機能です。ただし、ユーザーが BitLocker 回復キーを紛失した場合、デバイスのロック解除が困難な場合があります。Citrix Endpoint Management では、ユーザーの BitLocker 回復キーを自動で安全に保存できるようになりました。BitLocker 回復キーは、Self-Help Portal で確認できます。BitLocker 回復キーを有効にして検索するには、次の手順を実行します:

1. Citrix Endpoint Management コンソールで、［設定］**>**［サーバープロパティ］の順に移動します。
2. `shp`を検索して`shp.console.enable`機能を有効にします。`enable.new.shp`が無効のままであることを確認します。Self Help Portal の有効化について詳しくは、「登録セキュリティモードを構成する」を参照してください。
3. ［構成］**>**［デバイスポリシー］に移動します。BitLocker ポリシーを見つけるかポリシーを作成して、［**Citrix Endpoint Management** への **BitLocker** 回復バックアップ］の設定を有効にします。

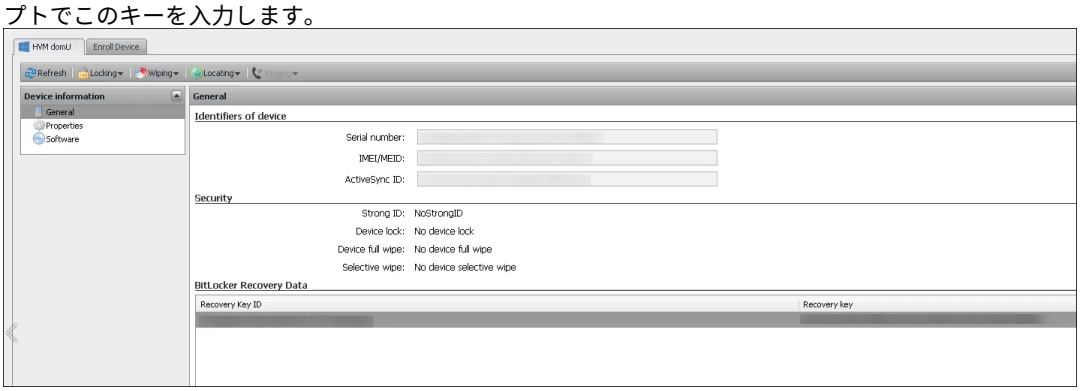
デバイスのロックを解除すると、エンドユーザーにキーの入力を求めるメッセージが表示されます。メッセージには、回復キー ID も表示されます。



BitLocker 回復キーを見つけるには、Self-Help Portal に移動します。

1. ［全般］の ［**BitLocker** 回復データ］を参照します。

    - 回復キー **ID**：ディスクの暗号化に使用される BitLocker 回復キーの識別子。この ID は、前のメッセージで指定されたキー ID と一致する必要があります。
    - 回復キー：ユーザーがディスクのロックを解除するために入力する必要があるキー。ロック解除プロンプトでこのキーを入力します。



BitLocker デバイスポリシーについて詳しくは、「BitLocker デバイスポリシー」を参照してください。

Windows デバイスの一括登録

November 29, 2023

Citrix Endpoint Management は、Windows 10 および Windows 11 デスクトップおよびタブレットデバイスの一括登録をサポートしています。一括登録では、デバイスの再イメージ化を行うことなく Citrix Endpoint Management で管理する多くのデバイスを設定できます。一括登録には、プロビジョニングパッケージを使用します。

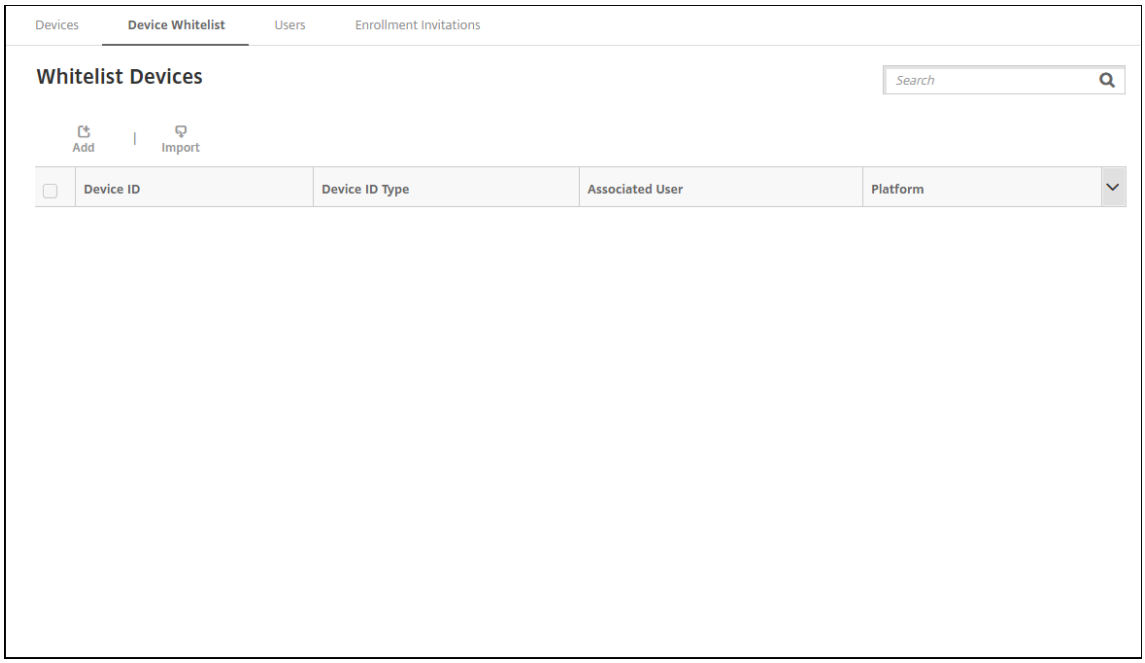
Windows 10 および Windows 11 デバイスを一括登録する一般的なワークフローは次のとおりです:

1. デバイスを割り当てます。デバイスは、デバイス単位または一括で割り当てることができます。
2. 一括登録を設定します。
3. プロビジョニングパッケージを作成し、デバイスごとにそのパッケージを適用します。

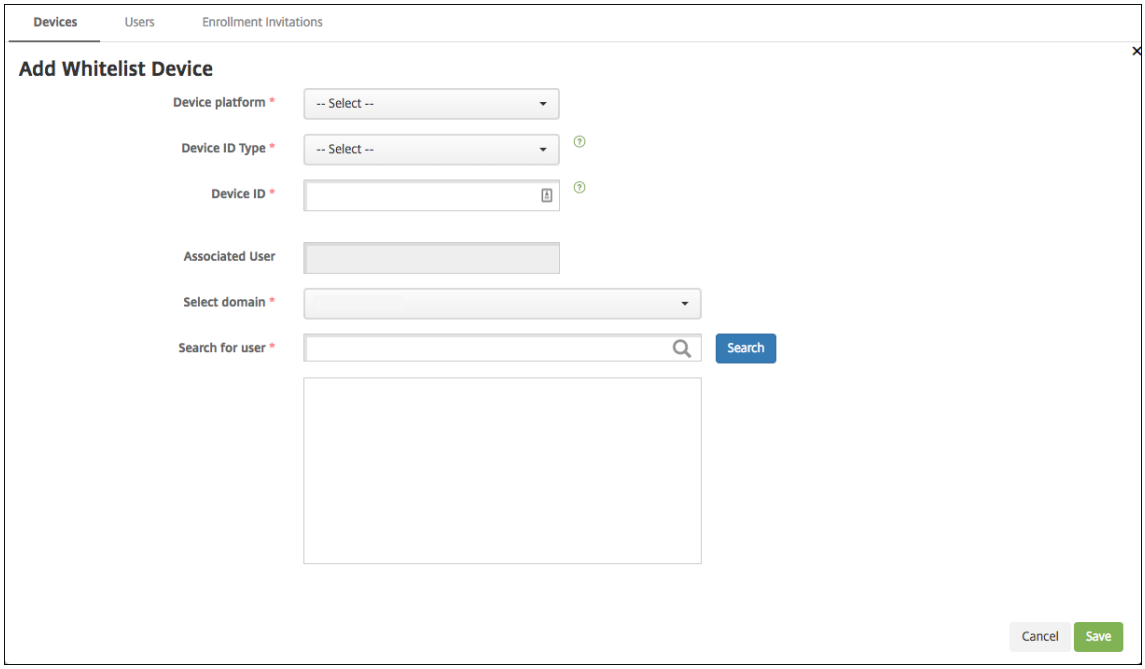
一括登録を実行する前に、すべてのデバイスが正しいユーザーに割り当てられていることを確認してください。デバイスをデバイス単位または一括で追加して、この割り当てを実行します。

デバイス単位でのデバイスの割り当て

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］**>**［デバイス許可リスト］の順に移動します。



2. 各デバイスを追加するには、［追加］をクリックします。



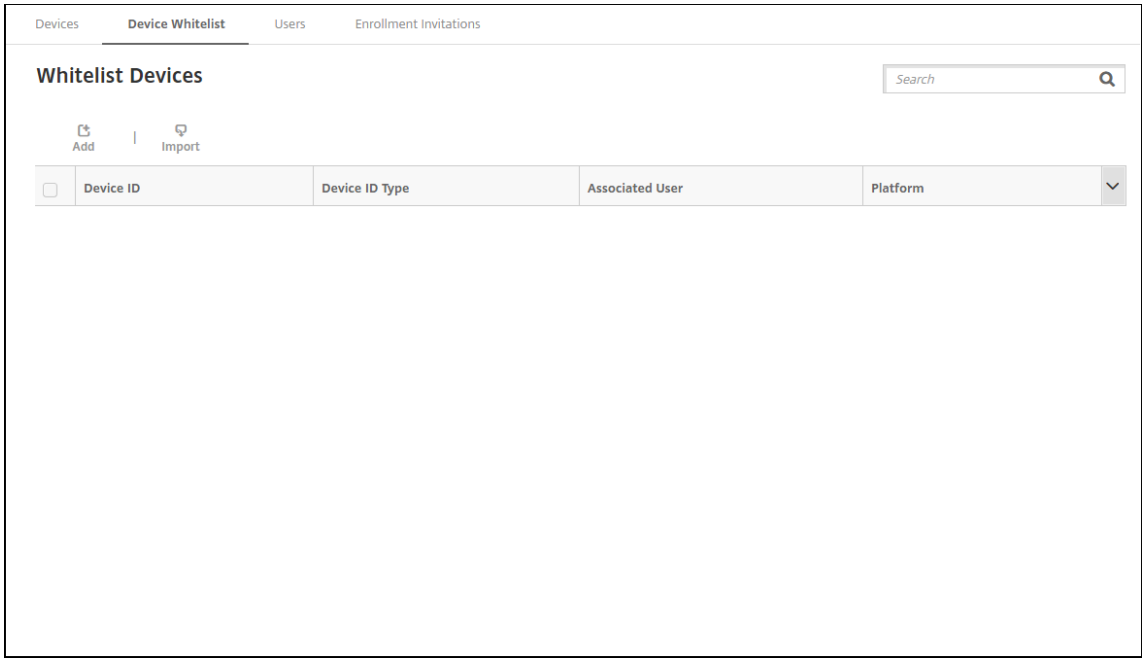
3. 次の情報を入力します:

   - デバイスプラットフォーム:［**Windows**］を選択します。
   - デバイス **ID** の種類:デバイスを識別する ID を選択します。Windows デバイスについては、Citrix Endpoint Management では ［ハードウェア **ID**］と ［デバイス名］のみをサポートします。
   - デバイス **ID**:デバイスに対して以前に選択した種類に対応する ID を入力します。
   - 関連ユーザー:このデバイスに関連付けられたユーザーを表示します。このフィールドには、選択したユーザーが自動的に入力されます。
   - ドメインを選択:関連ユーザーを検索するドメインを選択します。
   - ユーザーの検索:ユーザー名の一部または全部を入力して ［検索］をクリックし、このデバイスに関連付けるユーザーを検索します。

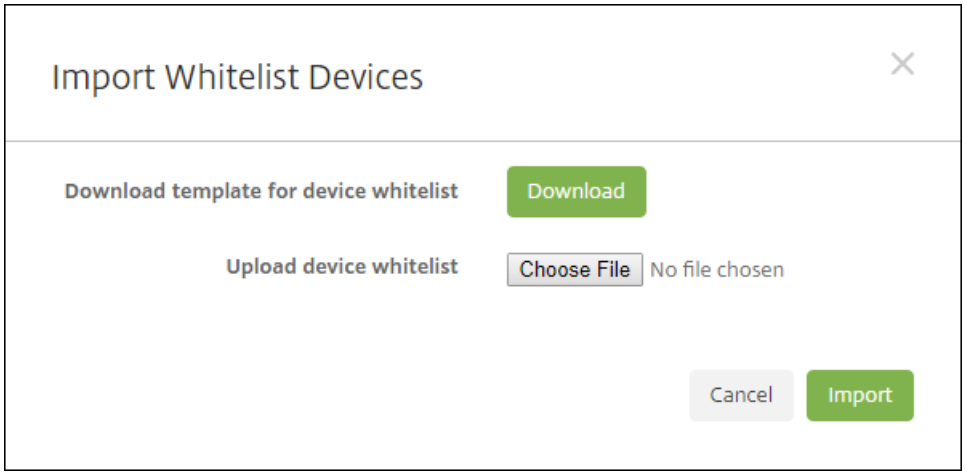
4. ［保存］をクリックします。

デバイスの一括追加

1. Citrix Endpoint Management コンソールで、［管理］**>**［デバイス］**>**［デバイス許可リスト］の順に移動します。



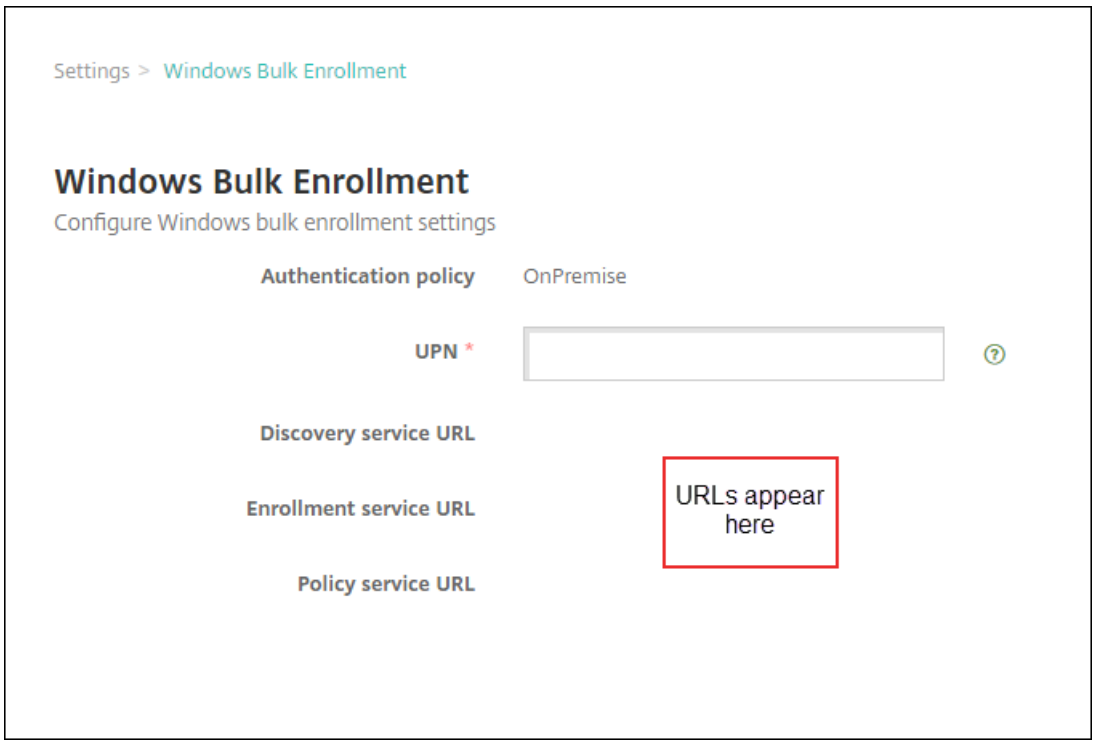
2. ［インポート］をクリックします。



3. ［ダウンロード］をクリックして、デバイスの許可リストのテンプレート（スプレッドシート）をダウンロードします。そのスプレッドシートに入力したら、［ファイルの選択］と ［インポート］を使用してスプレッドシートをアップロードします。

一括登録の設定

1. Citrix Endpoint Management コンソールで、［設定］**>** ［**Windows** 一括登録］の順に移動します。
2. ［**UPN**］フィールドに、すべてのデバイスの展開に使用するユーザー名を入力します。UPN は、登録権限を持つ Citrix Endpoint Management の有効なユーザーである必要があります。以前に選択した関連ユーザーとは異なる UPN を入力できます。



Windows Configuration Designer でプロビジョニングパッケージを作成するには URL が必要です。

3. ［保存］をクリックします。

プロビジョニングパッケージの作成と適用

デバイスを一括プロビジョニングするには、Microsoft ストアから Windows 構成デザイナーをダウンロードします。Windows 構成デザイナーは、デバイスのイメージ作成で使用するプロビジョニングパッケージを作成します。パッケージの一部として Citrix Endpoint Management の一括登録設定を含めて、プロビジョニングされたデバイスが Citrix Endpoint Management に自動的に登録されるようにすることができます。

プロビジョニングパッケージの使用について詳しくは、https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-toolを参照してください。このドキュメントの 「オンプレミスの認証用にプロビジョニング パッケージを作成して適用する」セクションで説明されている手順に従います。手順に従って、以下の Citrix Endpoint Management の一括登録構成設定を含めて、各デバイスにパッケージを適用します。

- 検出サービス **URL**
- 登録サービス **URL**
- ポリシーサービス **URL**
- シークレット UPN のパスワード。以前に［UPN］フィールドに入力したユーザー名です。

デバイスを追加設定なしで一括登録

Citrix Endpoint Management は、追加設定のない Windows デバイスの一括登録をサポートしています。以下の手順で、一括登録をセットアップして実行します：

1. Citrix Endpoint Management コンソールを使用してデバイスを追加し（デバイス単位または一括）、一括登録を設定します。詳しくは、「デバイスの一括追加」と「一括登録の設定」を参照してください。
2. 「プロビジョニングパッケージの作成と適用」の説明に従って、プロビジョニングパッケージを作成します。

   > 注：
   >
   > プロビジョニングパッケージを作成するときは、各デバイスのデバイス名を設定する必要があります。これを行うには、Windows Configuration Designer で、［ランタイムの設定］**>**［アカウント］**>**［**ComputerAccount**］**>**［**ComputerName**］に移動し、デバイスの名前を指定します。各デバイスに指定するデバイス名は、許可リストデバイスをインポートするときに使用した名前と一致している必要があります。

3. プロビジョニングパッケージを USB スティックに入れます。
4. デバイスの電源を初めてオンにした時に、USB スティックをターゲットデバイスに挿入します。

   Windows デバイスが、USB スティック上のプロビジョニングパッケージ（.ppkg）を自動的に検出します。詳しい手順については、初期セットアップ中のプロビジョニングパッケージの適用方法に関する Microsoft 社のドキュメントを参照してください。

デバイスは自動的に Citrix Endpoint Management に登録されます。

Windows 10（バージョン 2004 以降）または Windows 11 がインストールされているデバイスの場合、プロビジョニングパッケージを 1 つ作成するだけで、登録プロセスを簡素化できます。作成後、プロビジョニングパッケージはすべてのデバイスに適用できます。その結果、デバイス単位でプロビジョニングパッケージを作成する必要がなくなります。

登録プロセスを簡素化するには、プロビジョニングパッケージの作成時に次の手順を実行します：

1. Windows Configuration Designer で、［ランタイムの設定］**>**［アカウント］**>**［**ComputerAccount**］**>**［**ComputerName**］に移動します。
2. ［**ComputerName**］フィールドに、デバイス名の一部として次の文字列を含めます：`%SERIAL%`。例：`Surface-%SERIAL%`。この文字列は、各デバイスの BIOS シリアル番号に展開されます。

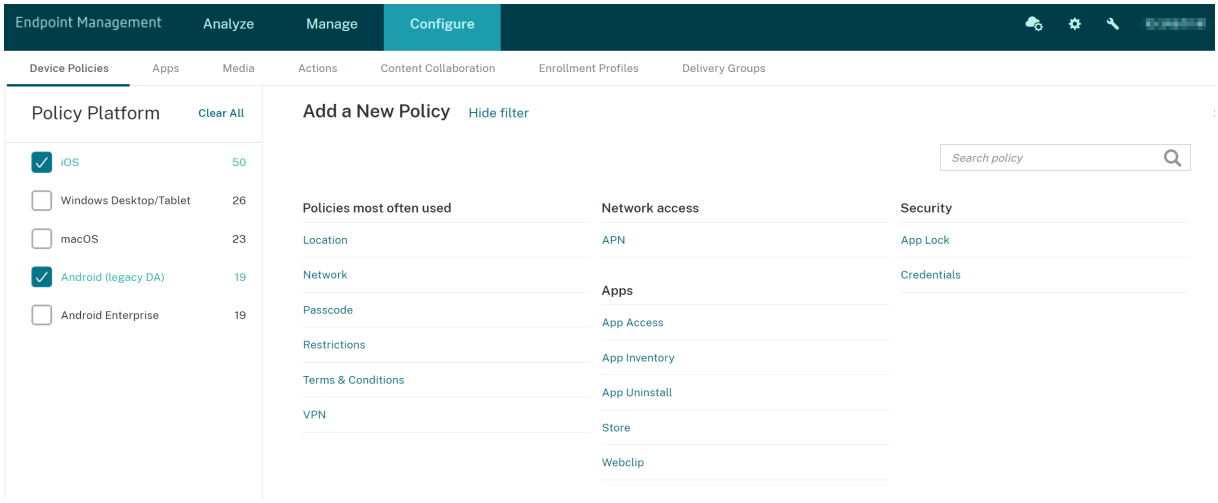
デバイスポリシー

March 15, 2024

ポリシーを作成して、Citrix Endpoint Management とデバイスの連携方法を構成できます。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、プラットフォーム間で異なる場合や、Android デバイスの製造元によっても違いがある場合があります。

プラットフォーム別ポリシーを参照するには、次の手順を実行します:

1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］に移動します。
2. ［追加］をクリックします。
3. デバイスプラットフォームが、［ポリシープラットフォーム］ペインに一覧表示されます。このペインが開いていない場合は、［フィルターを表示］をクリックします。
4. 1 つのプラットフォームで使用可能なすべてのポリシーの一覧を表示するには、このプラットフォームを選択します。複数のプラットフォームで使用可能なポリシーの一覧を表示するには、各プラットフォームを選択します。ポリシーは、選択した各プラットフォームに適用される場合にのみ一覧に表示されます。



各デバイスポリシーの概要説明については、この記事の「デバイスポリシーの概要」を参照してください。

> 注:
>
> 環境がグループポリシーオブジェクト（GPO）で構成されている場合:
>
> Windows 10 および Windows 11 で Citrix Endpoint Management デバイスポリシーを構成するときは、次のルールに留意してください。登録済みのデバイス間でポリシーの競合が発生した場合、GPO に合っているポリシーが優先されます。

Android Enterprise コンテナがサポートするポリシーを確認するには、「Android Enterprise」を参照してください。

前提条件

- 使用する予定のデリバリーグループを作成します。
- 必要な CA 証明書をインストールします。

デバイスポリシーの追加

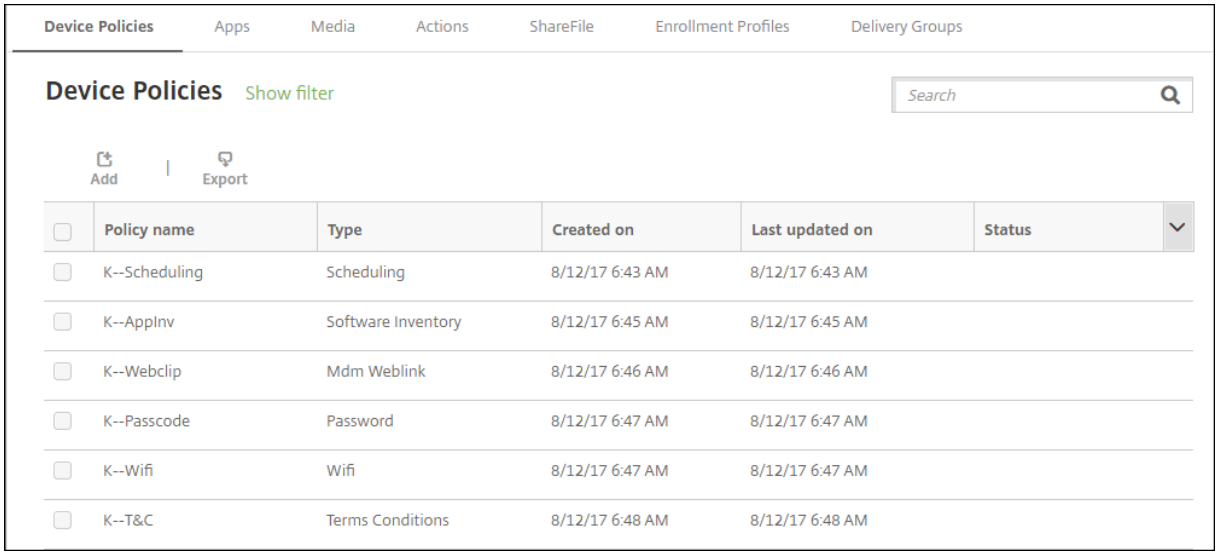
デバイスポリシーの基本的な作成手順は次のとおりです:

1. ポリシーの名前と説明を指定します。

   > 重要:
   >
   > ポリシー名にはスラッシュ（/）を使用しないでください。使用すると、後でポリシーを編集するときにエラーが発生することがあります。

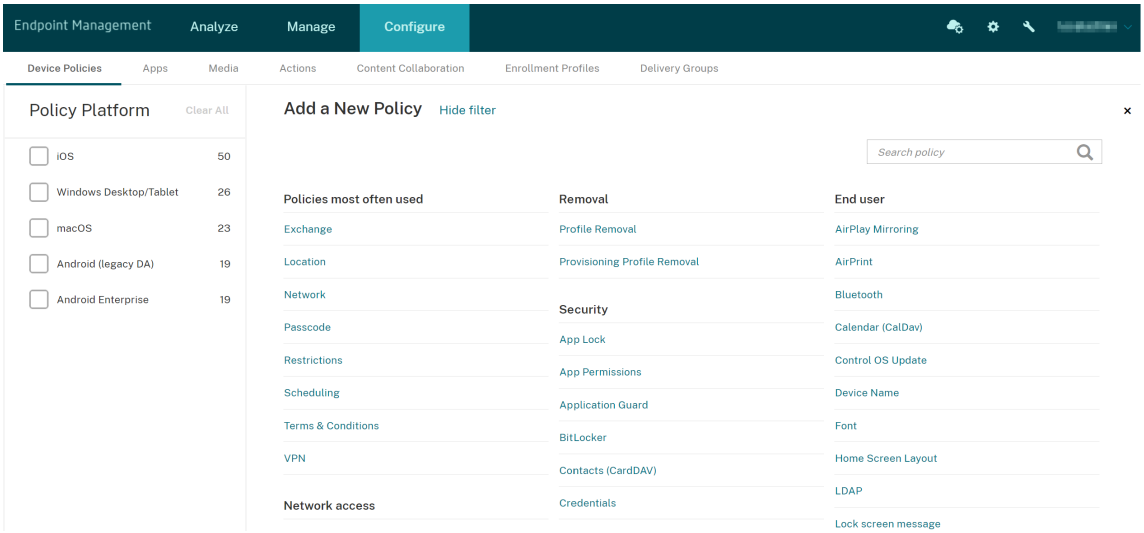
2. 1 つまたは複数のプラットフォームのポリシーを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

デバイスポリシーを作成し、管理するには、［構成］**>**［デバイスポリシー］の順に選択します。

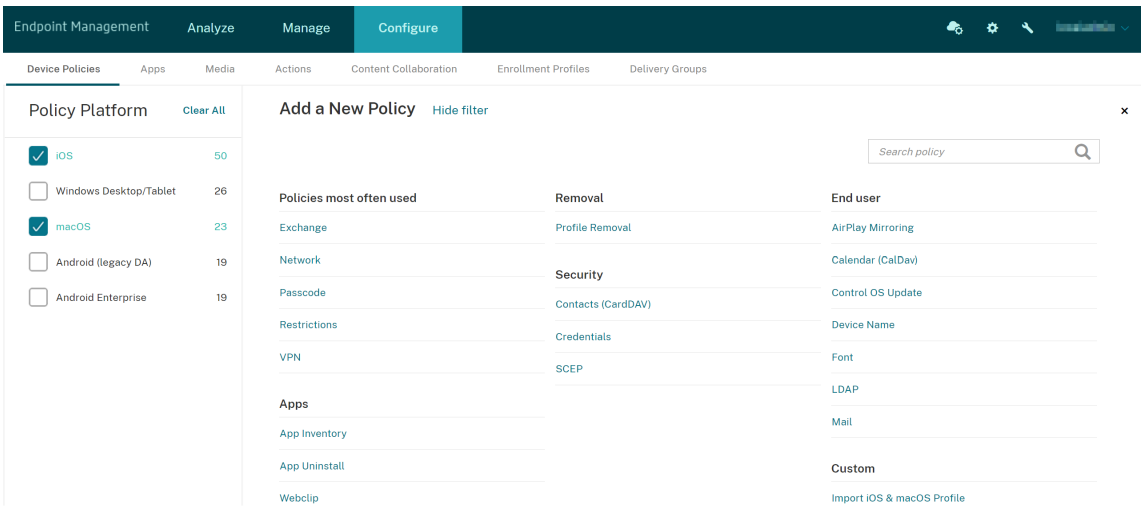


ポリシーを追加するには、次の手順に従います:

1. ［デバイスポリシー］ページで、［追加］をクリックします。［新しいポリシーの追加］ページが開きます。



2. 1 つまたは複数のプラットフォームをクリックし、選択したプラットフォームのデバイスポリシー一覧を表示します。ポリシーの追加を続けるにはポリシー名をクリックします。



検索ボックスにポリシーの名前を入力することもできます。入力すると一致候補が表示されます。一覧の中に目的のポリシーがあれば、それをクリックします。その結果、選択したポリシーのみが残ります。それをクリックして、そのポリシーの ［ポリシー情報］ページを開きます。

3. ポリシーに含めるプラットフォームを選択します。選択したプラットフォームの構成ページが手順 5. で表示されます。

4. ［ポリシー情報］ページで必要な情報を入力して、［次へ］をクリックします。［ポリシー情報］ページにはポリシー名などの情報が集約されているため、ポリシーの識別や追跡に役立ちます。このページはすべてのポリシーで類似しています。

5. プラットフォームページの入力を完了します。手順 3 で選択した各プラットフォームのページが開きます。これらのページはポリシーごとに異なります。ポリシーはプラットフォームによって異なる可能性があります。すべてのポリシーがすべてのプラットフォームに適用される訳ではありません。

一部のページにはアイテムの表が含まれています。既存の項目を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログで、[削除] をクリックします。

既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。

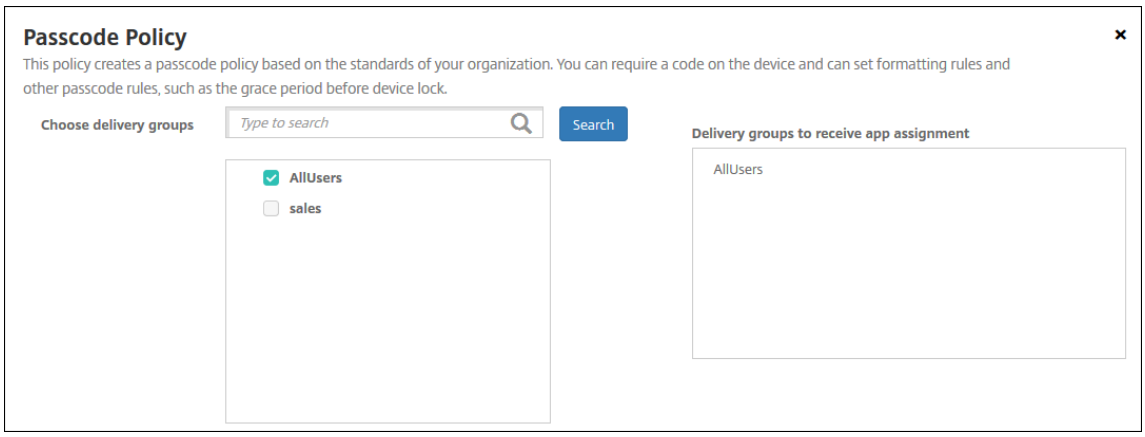
展開ルール、割り当て、およびスケジュールを構成するには

展開規則の構成について詳しくは、「リソースの展開」を参照してください。

1. プラットフォームのページで、[展開規則] を展開して以下の設定を構成します。デフォルトでは [基本] タブが表示されます。
   - 一覧から、展開条件を指定するオプションをクリックします。すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトオプションは **All** に設定されています。
   - [新しい規則] をクリックして条件を定義します。
   - 一覧から [デバイス所有権] や [**BYOD**] などの条件を選択します。
   - 条件をさらに追加する場合は、[新しい規則] をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. [詳細] タブをクリックし、ブール値オプションを使用して規則を組み合わせます。[基本] タブで選択した条件が表示されます。
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   - [**AND**]、[**OR**]、または [**NOT**] をクリックします。
   - 一覧から、規則に追加する条件を選択します。次に右側のプラス記号（**+**）をクリックし、規則に条件を追加します。

     いつでも、条件をクリックして選択し、[編集] または [削除] をクリックできます。
   - [新しい規則] をクリックして別の条件を追加します。
4. [次へ] をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、[割り当て] ページに移動します。
5. [割り当て] ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、[アプリ割り当てを受信するためのデリバリーグループ] ボックスにそのグループが表示されます。

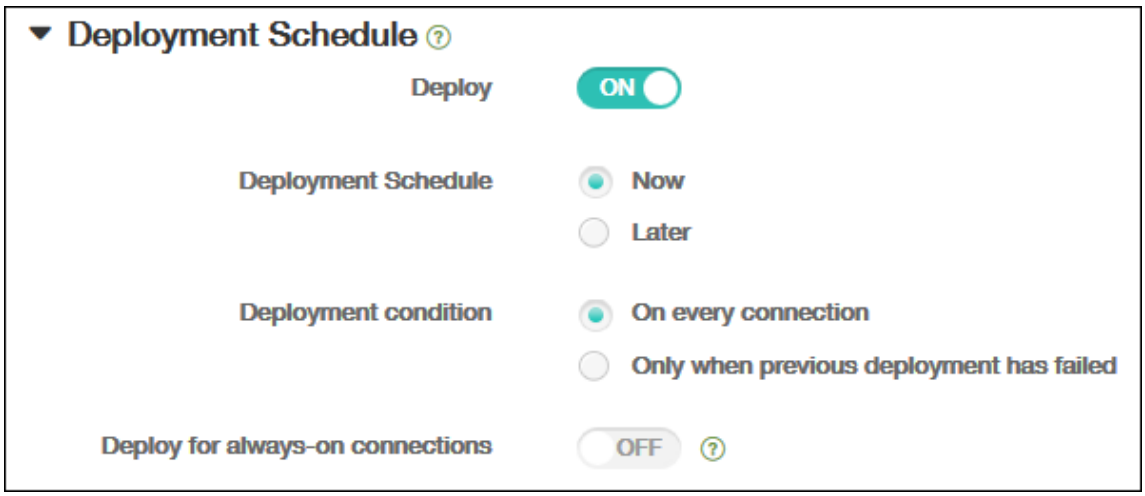
   [アプリ割り当てを受信するためのデリバリーグループ] ボックスは、デリバリーグループを選択するまで表示されません。



6. ［割り当て］ページで ［展開スケジュール］を展開して以下の設定を構成します：

   - ［展開］の横の ［オン］をクリックすると展開がスケジュールされ、［オフ］をクリックすると展開が行われません。デフォルトのオプションは、［オン］です。
   - ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。デフォルトのオプションは、［**Now**］に設定されています。
   - ［あとで］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
   - ［展開状態］の横の ［接続するたび］をクリックするか、［以前の展開が失敗した場合のみ］をクリックします。デフォルトのオプションは、［**On every connection**］です。
   - ［常時接続に対する展開］の横の ［オン］または ［オフ］をクリックします。デフォルトのオプションは、［オフ］です。

     > 注：
     >
     > このオプションは、［設定］**>**［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。
     >
     > 常時接続オプション：
     >
     > - iOS デバイスでは使用できません。
     > - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
     > - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません。
     >
     > 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。



7. ［保存］をクリックします。

   ポリシーが ［デバイスポリシー］の表に表示されます。

デバイスからのデバイスポリシーの削除

デバイスからデバイスポリシーを削除する手順は、プラットフォームによって異なります。

- Android

  Android デバイスからデバイスポリシーを削除するには、Citrix Endpoint Management アンインストールデバイスポリシーを使用します。詳しくは、「Citrix Endpoint Management アンインストールデバイスポリシー」を参照してください。

- iOS と macOS

  iOS または macOS デバイスからデバイスポリシーを削除するには、プロファイル削除デバイスポリシーを使用します。iOS および macOS デバイスでは、すべてのポリシーが MDM プロファイルの一部です。したがって、削除するポリシーに限定したプロファイル削除デバイスポリシーを作成できます。その他のポリシーとプロファイルはデバイスに残ります。詳しくは、「プロファイル削除デバイスポリシー」を参照してください。

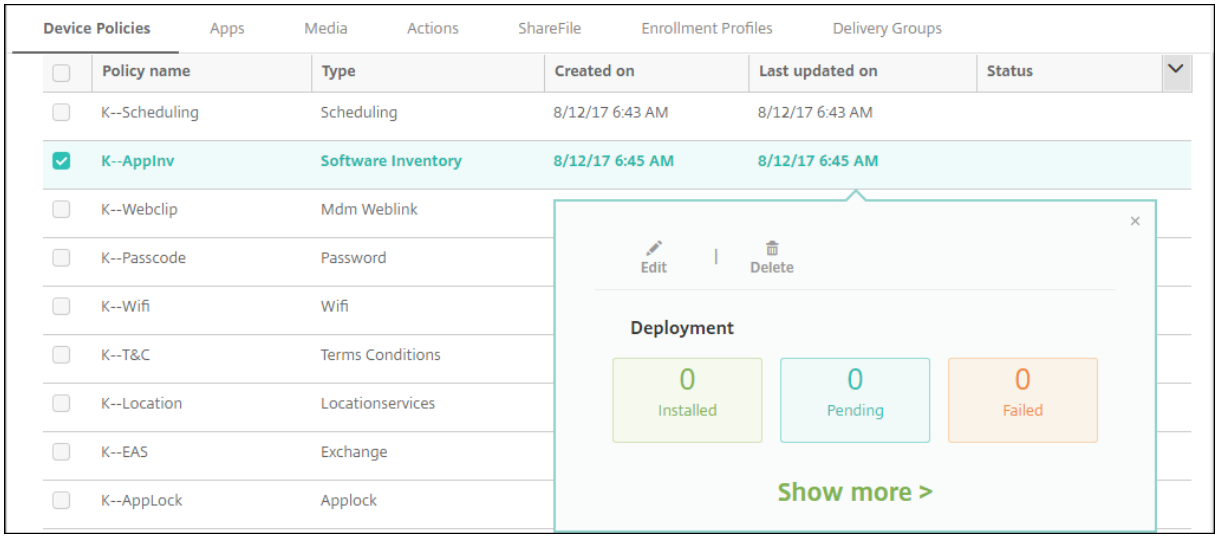
- Windows 10 および Windows 11

  Windows デスクトップまたはタブレットデバイスから直接デバイスポリシーを削除することはできません。ただし、次のいずれかの方法を使用できます:

  - デバイスの登録を解除し、新しいポリシーセットをデバイスにプッシュします。その後、ユーザーが再登録します。
  - 特定のデバイスを選択的にワイプするには、セキュリティ操作をプッシュします。この操作は、企業のすべてのアプリとデータをデバイスから削除します。次に、そのデバイスだけを含むデリバリーグループからデバイスポリシーを削除し、デリバリーグループをデバイスにプッシュします。その後、ユーザーが再登録します。

デバイスポリシーの編集

ポリシーを編集するには、ポリシーの横にあるチェックボックスをオンにします。ポリシーリストの上にオプションメニューが表示されます。または、リスト内のポリシーをクリックして、より多くのコントロールを表示します。



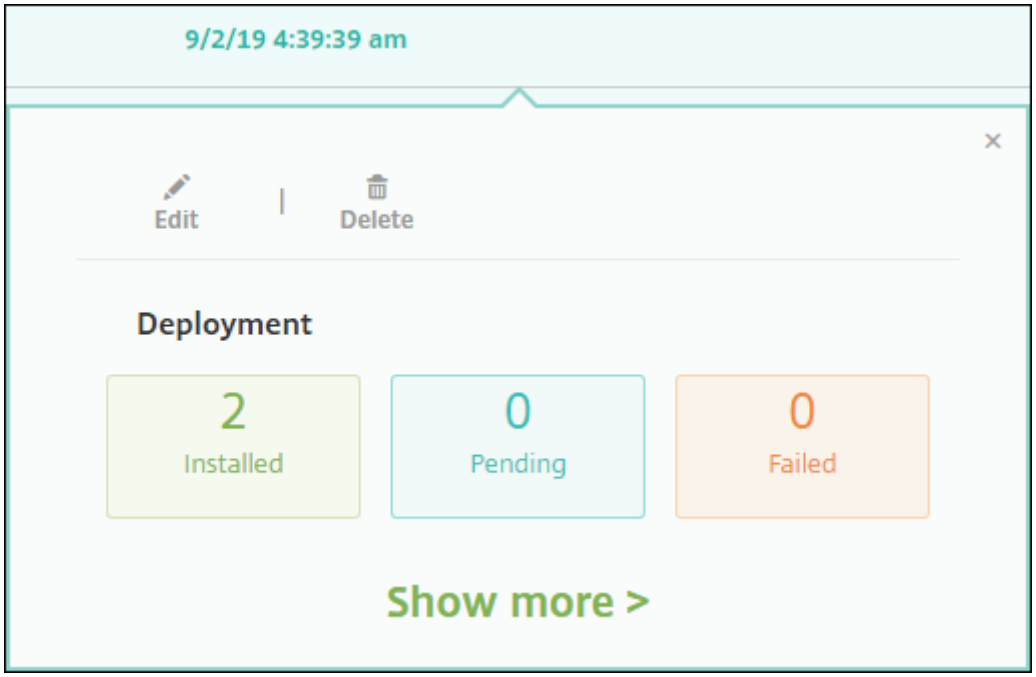
ポリシーの詳細を表示するには、［詳細表示］をクリックします。

デバイスポリシーのすべての設定を編集するには、［編集］をクリックします。

［削除］をクリックすると、確認ダイアログボックスが開きます。ポリシーを削除するには、もう一度 ［削除］をクリックします。

ポリシー展開ステータスの確認

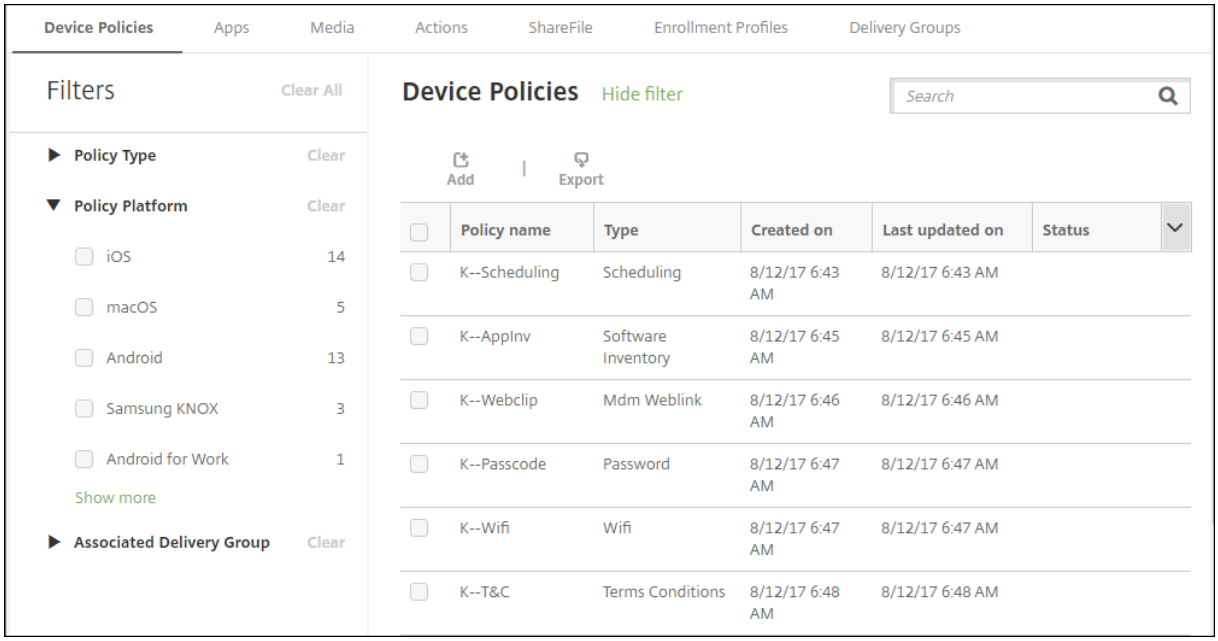
［構成］**>**［デバイスポリシー］ページでポリシー行をクリックし、展開ステータスを確認します。



ポリシーの展開が保留中の場合、ユーザーは ［環境設定］ > ［デバイス情報］ > ［ポリシーの更新］ の順にタップし、Citrix Secure Hub からポリシーを更新できます。

追加されたデバイスポリシーの一覧のフィルター

ポリシーの種類、プラットフォーム、および関連するデリバリーグループで追加されたポリシー一覧にフィルターすることができます。［構成］ > ［デバイスポリシー］ ページで、［フィルターを表示］ をクリックします。一覧で、表示する項目のチェックボックスをオンにします。



［このビューを保存］をクリックしてフィルターを保存します。フィルターの名前が、［このビューを保存］ボタンの下のボタンに表示されます。

デバイスポリシーの概要

デバイスポリシー名	デバイスポリシーの説明
AirPlay ミラーリング	特定の AirPlay デバイス（Apple TV やほかの Mac コンピューターなど）を iOS デバイスに追加します。監視対象デバイスの許可リストにデバイスを追加することもできます。このオプションは、許可リストの AirPlay デバイスのみにユーザーを制限します。
AirPrint	AirPrint プリンターを iOS デバイスの AirPrint プリンター一覧に追加します。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。
アクセスポイント名	特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。ほとんどの新しい電話機において、この設定はすでに定義されています。このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマー APN を使用しない組織で使用します。
アプリアクセス	デバイス上で必須、オプション、または禁止されるアプリの一覧を定義します。次に、そのアプリ一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。
アプリ属性	iOS デバイスのための属性（管理対象アプリのバンドル ID やアプリごとの VPN 識別子など）を指定します。
アプリ構成	管理対象の構成をサポートするアプリのさまざまな設定や動作をリモートで構成します。そのために、XML 構成ファイル（プロパティリスト、または`plist`と呼ばれる）を iOS デバイスに展開します。または、キー/値ペアを Windows 10 のデスクトップまたはタブレットデバイスに展開します。

デバイスポリシー名	デバイスポリシーの説明
アプリインベントリ	管理対象デバイス上のアプリのインベントリを収集します。これにより、Citrix Endpoint Management はインベントリを、そのデバイスに展開済みのアプリアクセスポリシーと比較します。この方法で、アプリアクセスの許可リストまたは禁止リストにあるアプリを検出し、それに応じて対応できます。
アプリのロック	ユーザーが iOS または特定の Android デバイスで実行できるアプリと実行できないアプリの一覧を定義します。iPad をキオスクにすることができます。
アプリの権限	仕事用プロファイル内で、Android Enterprise アプリへの要求で、Google で「危険」とされる権限をどう処理するかを構成します。
アプリのアンインストール	ユーザーのデバイスからアプリを削除します。
アプリのアンインストール制限	ユーザーがアンインストールできる、またはアンインストールできないアプリを指定します。
Application Guard	Microsoft Edge ブラウザーの場合のみ、このポリシーは Windows Defender Application Guard の設定を指定します。この設定には、エンタープライズサイトで外部コンテンツをブロックするかどうかが含まれます。
アプリ通知	iOS ユーザーが指定したアプリから通知を受け取る方法を制御します。
管理対象アプリの自動更新	インストールされている管理対象アプリを Android Enterprise デバイスで更新する方法を制御します。
BitLocker	Windows 10 および Windows 11 デバイスの BitLocker インターフェイスで使用できる設定を構成します。
Bluetooth	iOS デバイスで Bluetooth を有効または無効にします。
ブラウザー	ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、デバイスで使用できるブラウザー機能を定義したりします。
カレンダー（CalDAV）	カレンダー（CalDAV）アカウントを iOS または macOS デバイスに追加します。CalDAV アカウントによって、ユーザーはスケジュールデータを CalDAV をサポートするサーバーと同期させることができます。
モバイル	携帯ネットワーク設定を構成します。

デバイスポリシー名	デバイスポリシーの説明
接続スケジュール	Android デバイスで MDM 管理、アプリのプッシュ、ポリシーの展開を行う上で Citrix Endpoint Management に接続するために必要です。このポリシーをデバイスに送信せず、Google FCM を有効にしない場合、デバイスはサーバーに接続することができません。
連絡先（CardDAV）	iOS 連絡先（CardDAV）アカウントを iOS または macOS デバイスに追加します。CardDAV アカウントによって、ユーザーは連絡先データを CardDAV をサポートするサーバーと同期させることができます。
資格情報	Citrix Endpoint Management PKI 構成で統合認証を有効にします。たとえば、PKI エンティティ、キーストア、資格情報プロバイダー、サーバー証明書などを使用します。
カスタム XML	デバイスのプロビジョニング、デバイス機能の有効化、デバイスの構成、障害の管理などの機能をカスタマイズします。
Defender	デスクトップおよびタブレットの Windows 10 および Windows 11 で Windows Defender 設定を構成します。
Device Guard	セキュアブート、UEFI ロック、仮想化などのセキュリティ機能を有効にします。
デバイス正常性構成証明	Windows 10 および Windows 11 デバイスにデバイスの正常性状態を報告させます。そのため、分析目的で特定のデータおよびランタイム情報を Health Attestation Service （HAS）に送信させます。HAS は、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスから Citrix Endpoint Management に送信されます。Citrix Endpoint Management は正常性構成証明書を受信すると、その内容に基づいて、管理者が構成した自動アクションを展開します。
デバイス名	デバイスを特定できるように、iOS デバイスおよび macOS デバイスに名前を設定します。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。

デバイスポリシー名	デバイスポリシーの説明
教育の構成	Apple の教育向け機能を使用するように講師および生徒のデバイスを構成します。講師がクラスルームアプリを使用する場合は、教育の構成デバイスポリシーが必要です。iOS（iPadOS）デバイスでサポートされています。
Citrix Endpoint Management オプション	Android デバイスから Citrix Endpoint Management に接続するときの Citrix Secure Hub の動作を構成します。
Citrix Endpoint Management のアンインストール	Citrix Endpoint Management を Android デバイスからアンインストールします。このポリシーを展開すると、展開グループ内のすべてのデバイスから Citrix Endpoint Management が削除されます。
Exchange	デバイス上のネイティブの電子メールクライアントで ActiveSync メールを有効にします。
ファイル	ユーザーに対して特定の機能を実行するスクリプトファイルを Citrix Endpoint Management に追加します。または、Android デバイスユーザーがデバイスでアクセスできるドキュメントファイルを追加することができます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。
FileVault	このポリシーによって、macOS デバイスで登録された FileVault デバイスの暗号化を有効にできます。ログイン中にユーザーが FileVault のセットアップをスキップできる回数を制御することもできます。macOS 10.7 以降で使用できます。
ファイアウォール	ファイアウォールの設定を構成します。デバイスで許可または禁止する IP アドレス、ポート、ホスト名を入力します。プロキシおよびプロキシ再ルーティングの設定を構成することもできます。
フォント	iOS デバイスおよび macOS デバイスにフォントを追加します。フォントは TrueType（.TTF）または OpenType（.OFT）である必要があります。Citrix Endpoint Management はフォントコレクション（.TTC、.OTC）をサポートしていません。
ホーム画面のレイアウト	監視対象の iOS デバイスのホーム画面について、アプリとフォルダーのレイアウトを指定します。

デバイスポリシー名	デバイスポリシーの説明
iOS および macOS プロファイルのインポート	iOS および macOS デバイス用のデバイス構成 XML ファイルを Citrix Endpoint Management にインポートします。XML ファイルには、Apple Configurator を使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。
Keyguard 管理	デバイス Keyguard と仕事用チャレンジ Keyguard をロック解除する前に、ユーザーが利用できる機能を制御します。また、完全に管理されたデバイスと専用デバイスのデバイス Keyguard 機能を制御することもできます。たとえば、指紋によるロック解除、信頼できるエージェント、通知などのロック画面機能を無効にできます。
Launcher 構成	許可されたアプリや Launcher アイコン用のカスタムロゴイメージなど、Android デバイス上の Citrix Launcher の設定を指定します。
LDAP	LDAP サーバーホスト名などの必要なアカウント情報など、iOS デバイスに使用する LDAP サーバーに関する情報を指定します。また、LDAP サーバーの照会に使用する LDAP 検索ポリシーのセットが提供されます。
位置情報	そのデバイスの GPS が Citrix Secure Hub に対応している場合に、地図上で位置を検出できるデバイスを許可します。このポリシーをデバイスに展開した後、位置を確認するコマンドを Citrix Endpoint Management から送信できます。デバイスはその後位置情報を返信します。Citrix Endpoint Management は、ジオフェンシングおよび追跡ポリシーもサポートします。
ロック画面のメッセージ	共有 iPad と監視対象の iOS デバイスを紛失したときに、ログインウィンドウ（iPad の場合）とロック画面（iOS デバイスの場合）に表示するメッセージを表示します。
メール	iOS デバイスまたは macOS デバイスのメールアカウントを構成します。
管理対象の構成	Android Enterprise デバイスのさまざまなアプリ設定オプションとアプリの制限を管理します。

デバイスポリシー名	デバイスポリシーの説明
管理対象ドメイン	メールおよび Safari ブラウザーに適用する管理対象ドメインを定義します。管理対象ドメインを使用すると、Safari を使用してドメインからダウンロードしたドキュメントを開くことができるアプリを制御して、会社のデータを保護することができます。iOS の監視対象デバイスでは、URL またはサブドメインを指定して、ユーザーがドキュメント、添付ファイル、および Web ブラウザーからのダウンロードファイルを開く方法を制御できます。
最大常駐ユーザー数	共有 iPad の最大ユーザー数を指定します。iOS デバイスおよび iPadOS デバイスでサポートされています。
MDM オプション	監視対象の iOS デバイスで［iPhone と iPad を探す］の［アクティベーションロック］を管理します。
ネットワーク	管理者が Wi-Fi ルーターの詳細を管理対象デバイスに展開することを許可します。ルーターの詳細には、SSID、認証データ、構成データなどがあります。
ネットワーク使用状況	ネットワーク使用状況規則を設定して、iOS デバイスで管理対象のアプリが携帯データネットワークなどのネットワークをどのように使用するのかを指定します。規則は管理対象のアプリにのみ適用されます。管理対象のアプリとは、Citrix Endpoint Management を使用してユーザーのデバイスに展開されるアプリです。
Office	Microsoft Office アプリを、Windows 10（バージョン 1709 以降）または Windows 11 を実行しているすべてのデバイスに展開します。
組織情報	Citrix Endpoint Management が iOS デバイスに展開するアラートメッセージの組織情報を指定します。
OS 更新	サポートされている監視対象デバイスに最新の OS 更新を展開します。
パスコード	管理対象デバイスに PIN コードまたはパスワードを適用します。デバイス上でパスコードの複雑さやタイムアウトを設定できます。
パスコードロックの猶予期間	共有 iPad の画面がロックされてから、画面のロック解除のためにパスコードの入力が必要になるまでの時間（分）を指定します。iOS デバイスおよび iPadOS デバイスでサポートされています。

デバイスポリシー名	デバイスポリシーの説明
パーソナルホットスポット	ユーザーが Wi-Fi ネットワーク圏外にいてもインターネットに接続できるようにします。ユーザーは、個人用ホットスポット機能を介して iOS デバイスの携帯データネットワーク接続で接続します。
プロファイルの削除	macOS デバイスからアプリプロファイルが削除されます。
プロビジョニング プロファイル	エンタープライズ配信のプロビジョニングプロファイルを指定してデバイスに送信します。iOS エンタープライズアプリを開発し、コード署名をするときは、通常は、プロビジョニングプロファイルを含めます。Apple は、iOS デバイスで実行するアプリについてはプロファイルを要求します。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。
プロビジョニングプロファイルの削除	iOS プロビジョニングプロファイルを削除します。
プロキシ	iOS を実行しているデバイスのグローバル HTTP プロキシ設定を指定します。グローバル HTTP プロキシポリシーはデバイスごとに 1 つのみ展開できます。
制限	管理対象デバイスをロックダウンしたり、機能を制御する数百のオプションが提供されています。制限オプションの例：カメラやマイクの無効化、ローミング規則の適用、アプリストアのようなサードパーティサービスへのアクセスの適用。
ローミング	iOS デバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成します。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。
Samsung MDM ライセンスキー	デバイスに展開する必要がある組み込みの Samsung Enterprise License Management（ELM）キーを指定します。Citrix Endpoint Management は、Samsung Enterprise Firmware-Over-The-Air（E-FOTA）サービスもサポートしています。

デバイスポリシー名	デバイスポリシーの説明
SCEP	iOS デバイスおよび macOS デバイスを構成し、外部 SCEP サーバーから証明書を取得します。Citrix Endpoint Management に接続されている PKI から SCEP を使用してデバイスに証明書を配布することもできます。そのためには、PKI エンティティと PKI プロバイダーを分散モードで作成します。
シングルサインオン（SSO）アカウント	ユーザーが 1 回サインオンするだけで、Citrix Endpoint Management および社内リソースにアクセスすることができるように、SSO アカウントを作成します。デバイスに資格情報を保存する必要はありません。Citrix Endpoint Management では、SSO アカウントのエンタープライズユーザーの資格情報は、App Store からのアプリを含む複数のアプリで使用されます。このポリシーは、Kerberos 認証と互換性があります。iOS で使用できます。
ストレージ暗号化	内部ストレージおよび外部ストレージを暗号化します。一部のデバイスについては、このポリシーによって、ユーザーがデバイスでメモリーカードを使用できなくなります。
ストア	アプリストアの Web クリップが、ユーザーデバイスのホーム画面に表示されるかどうかを指定します。
サブスクライブされたカレンダー	サブスクライブされたカレンダーを iOS デバイスのカレンダー一覧に追加します。ユーザーのデバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みであることを確認します。
使用条件	ユーザーが社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに要求します。ユーザーが Citrix Endpoint Management にデバイスを登録するときに、ユーザーは自分のデバイスを登録するために契約条件に同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。
トンネル	モバイルデバイスアプリのクライアントコンポーネントとアプリサーバーコンポーネント間のプロキシパラメーターを定義します。

デバイスポリシー名	デバイスポリシーの説明
VPN	従来の VPN Gateway テクノロジを使用するバックエンドシステムへのアクセスを提供します。このポリシーでは、デバイスに展開できる VPN ゲートウェイ接続の詳細を提供します。Citrix Endpoint Management は、Cisco AnyConnect、Juniper、および Citrix VPN などの、いくつかの VPN プロバイダーをサポートしています。VPN ゲートウェイがこのオプションをサポートしている場合、このポリシーを CA にリンクして、VPN オンデマンドを有効にできます。
壁紙	.png ファイルまたは.jpg ファイルを追加して、iOS デバイスのロック画面かホーム画面、または両方の画面の壁紙に設定します。iPad および iPhone で異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開します。
Web クリップ	ショートカットや Web クリップを Web サイトに配置してユーザーデバイスのアプリと一緒に表示します。iOS、macOS、Android デバイスの Web クリップを表す独自のアイコンを指定できます。Windows タブレットのみ、ラベルおよび URL が必要になります。
Web コンテンツフィルター	iOS デバイスの Web コンテンツをフィルターします。Citrix Endpoint Management は、Apple のオートフィルター機能および許可リストと禁止リストに追加したサイトを使用します。iOS の監視対象デバイスでのみ利用できます。
Windows エージェント	このポリシーを有効にして、Windows デスクトップおよびタブレットでアップロードされた PowerShell スクリプトを実行できるようにします。
Windows GPO の構成	Citrix Workspace Environment Management でサポートされているすべての Windows デバイスでグループポリシーオブジェクト（GPO）を構成します。
Windows Hello for Business	Windows 機能を有効にして、ユーザーがデバイスへ Windows Hello for Business をプロビジョニングできるようにします。このポリシーでは、パスコードの制限などのセキュリティ機能を構成することもできます。

プラットフォームごとのデバイスポリシー

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
AirPlay ミラーリングデバイスポリシー	X	X				
AirPrint デバイスポリシー	X					
APN デバイスポリシー	X			X		
アプリアクセスデバイスポリシー	X			X		
アプリ属性デバイスポリシー	X					
アプリ構成デバイスポリシー	X				X	
アプリインベントリデバイスポリシー	X	X	X	X	X	
アプリのロックデバイスポリシー	X			X	X	
アプリの権限デバイスポリシー			X			
アプリのアンインストールデバイスポリシー	X	X	X	X		
アプリのアンインストール制限デバイスポリシー						X
Application Guard デバイスポリシー					X	

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
アプリ通知デバイスポリシー	X					
管理対象アプリの自動更新			X			
BitLocker デバイスポリシー					X	
Bluetooth デバイスポリシー	X					
ブラウザーデバイスポリシー						X
カレンダー (CalDav) デバイスポリシー	X	X				
モバイルデバイスポリシー	X					
接続のスケジューリングデバイスポリシー			X	X		
連絡先 (CardDAV) デバイスポリシー	X	X				
Samsung コンテナへのアプリのコピーデバイスポリシー						X
資格情報デバイスポリシー	X	X	X	X	X	

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
カスタム XML デバイスポリシー			X		X	
Defender デバイスポリシー					X	
Device Guard デバイスポリシー					X	
デバイス正常性構成証明デバイスポリシー					X	
デバイス名デバイスポリシー	X	X				
Education の構成デバイスポリシー	X					
Citrix Endpoint Manage-ment オプションデバイスポリシー			X	X		
Citrix Endpoint Manage-ment アンインストールデバイスポリシー				X		
Exchange デバイスポリシー	X	X	X	X	X	

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
ファイルデバイスポリシー			X	X		
FileVault デバイスポリシー		X				
ファイアウォールデバイスポリシー		X			X	
フォントデバイスポリシー	X	X				
ホーム画面のレイアウトに関するデバイスポリシー	X					
デバイス構成のインポートのデバイスポリシー						X
iOS および macOS プロファイルのインポートデバイスポリシー	X	X				
Keyguard 管理デバイスポリシー			X			
キオスクデバイスポリシー			X		X	
Launcher 構成デバイスポリシー			X	X		
LDAP デバイスポリシー	X	X				
位置情報デバイスポリシー	X		X	X		

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
ロック画面のメッセージデバイスポリシー	X					
メールデバイスポリシー	X	X				
管理対象の構成デバイスポリシー			X			
管理対象ドメインデバイスポリシー	X					
最大常駐ユーザー数デバイスポリシー	X					
MDM オプションデバイスポリシー	X					
ネットワークデバイスポリシー	X		X	X		
ネットワーク使用状況デバイスポリシー	X					
Office デバイスポリシー					X	
組織情報デバイスポリシー	X					
OS の更新デバイスポリシー	X	X	X		X	
パスコードデバイスポリシー	X	X	X	X	X	

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
パスコードロックの猶予期間デバイスポリシー	X					
個人用ホットスポットデバイスポリシー	X					
プロファイル削除デバイスポリシー	X	X				
Provisioning プロファイルデバイスポリシー	X					
Provisioning プロファイル削除デバイスポリシー	X					
プロキシデバイスポリシー	X					
制限デバイスポリシー	X	X		X	X	
ローミングデバイスポリシー	X					
Samsung MDM ライセンスキーデバイスポリシー			X			
SCEP デバイスポリシー	X	X				
Siri とディクテーションのポリシー	X					

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
SSO アカウントデバイスポリシー	X					
ストレージ暗号化デバイスポリシー						
ストアデバイスポリシー	X			X	X	
サブスクライブされたカレンダーデバイスポリシー	X					
契約条件デバイスポリシー	X			X	X	
トンネルデバイスポリシー				X		
VPN デバイスポリシー	X	X		X	X	
壁紙デバイスポリシー	X					
Web クリップデバイスポリシー	X	X		X	X	
Web コンテンツフィルターデバイスポリシー	X					
Windows エージェントのデバイスポリシー					X	
Windows GPO の構成デバイスポリシー					X	

ポリシー	iOS	macOS	Android Enterprise	Android（レガシデバイス管理者）	Windows デスクトップ/タブレット	その他
Windows Hello for Business デバイスポリシー					X	

AirPlay ミラーリングデバイスポリシー

November 29, 2023

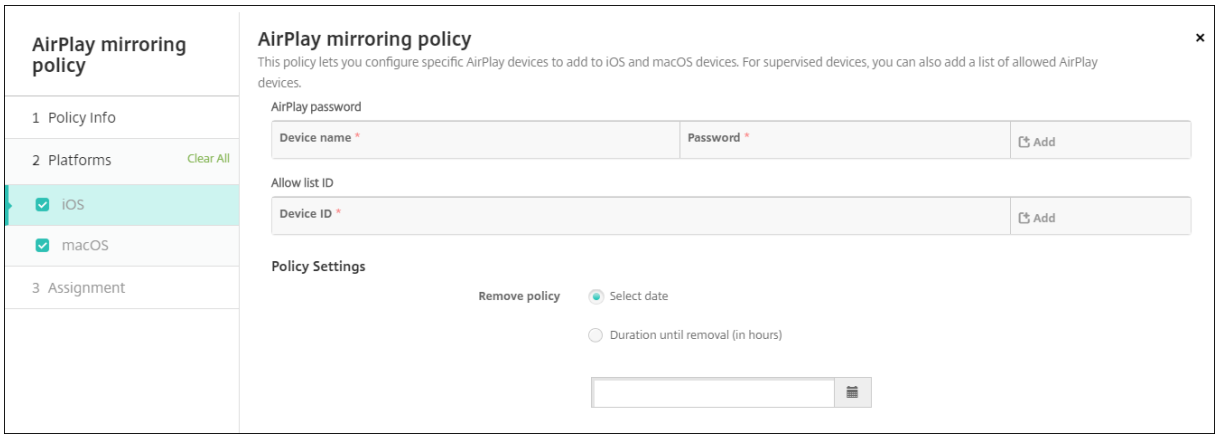
Apple AirPlay 機能を使用すると、Apple TV を介して iOS デバイスから TV 画面にコンテンツをワイヤレスでストリーム配信したり、デバイス上の表示を TV 画面またはほかの Mac コンピューターに正確にミラーリングしたりすることができます。

Citrix Endpoint Management でデバイスポリシーを追加して、特定の AirPlay デバイス（Apple TV やほかの Mac コンピューターなど）を iOS デバイスに追加することができます。また、デバイスを監視対象デバイスの許可リストに追加して、ユーザーを該当する AirPlay デバイスのみに限定するオプションもあります。デバイスを監視モードにすることについては、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

> 注:
>
> 続行する前に、追加するすべてのデバイスのデバイス ID とパスワードがあることを確認してください。

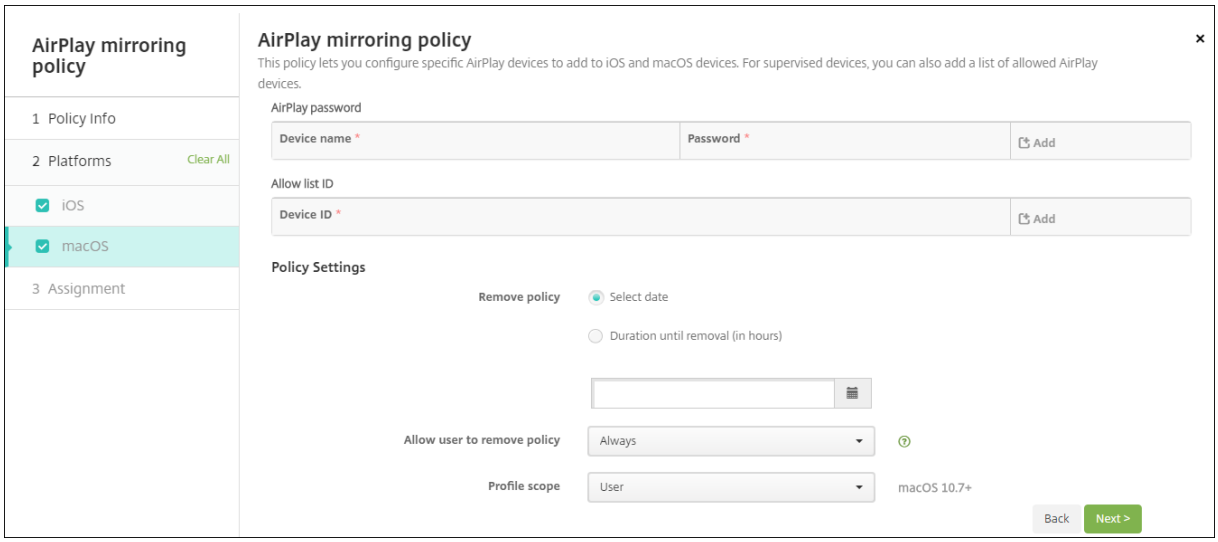
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **AirPlay** パスワード：追加するデバイスごとに、［追加］をクリックして以下の操作を行います。
  - デバイス名：ハードウェアのアドレス（MAC アドレス）を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - パスワード：任意で、デバイスのパスワードを入力します。
  - ［追加］をクリックしてデバイスを追加するか、［キャンセル］をクリックしてデバイスの追加を取り消します。
- 禁止リスト **ID**：この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーデバイスで使用できる AirPlay デバイスのデバイス ID のみを追加できます。一覧に追加する AirPlay デバイスごとに、［追加］をクリックして以下の操作を行います。
  - デバイス **ID**：デバイス ID を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - ［追加］をクリックしてデバイスを追加するか、［キャンセル］をクリックしてデバイスの追加を取り消します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

macOS 設定



- **AirPlay** パスワード：追加するデバイスごとに、［追加］をクリックして以下の操作を行います。
  - デバイス名：ハードウェアのアドレス（MAC アドレス）を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - パスワード：任意で、デバイスのパスワードを入力します。
  - ［追加］をクリックしてデバイスを追加するか、［キャンセル］をクリックしてデバイスの追加を取り消します。
- 禁止リスト **ID**：この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーデバイスで使用できる AirPlay デバイスのデバイス ID のみを追加できます。一覧に追加する AirPlay デバイスごとに、［追加］をクリックして以下の操作を行います。
  - デバイス **ID**：デバイス ID を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - ［追加］をクリックしてデバイスを追加するか、［キャンセル］をクリックしてデバイスの追加を取り消します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

AirPrint デバイスポリシー

February 16, 2022

AirPrint デバイスポリシーで、AirPrint プリンターを iOS デバイスの AirPrint プリンター一覧に追加します。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。

> 注:
>
> AirPrint デバイスポリシーを構成するには、各プリンターの IP アドレスとリソースパスが必要です。

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- **AirPrint** 出力先: 追加する AirPrint の出力先ごとに、[追加] をクリックして以下の操作を行います。
  - **IP** アドレス: AirPrint プリンターの IP アドレスを入力します。
  - リソースパス: プリンターに関連付けられているリソースパスを入力します。この値は、`_ipps.tcp` Bonjour レコードのパラメーターに対応します。たとえば、`printers/Canon_MG5300_series`または`printers/Xerox_Phaser_7600`などです。
- ポリシー設定
  - ポリシーの削除: ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、[日付を選択] と [削除までの期間（時間）を指定] です。
    - 日付を選択: カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定: ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

アプリの権限デバイスポリシー

March 15, 2024

仕事用プロファイル内の Android Enterprise アプリの場合: これらのアプリへの要求で、Google が「危険な」権限と呼ぶ権限をどう処理するかを構成できます。アプリからの権限要求を許可または拒否するためのプロンプトをユーザーに表示するかどうかを制御します。この機能は、Android 7.0 以降を実行するデバイス向けです。

Google では、危険な権限は、以下の権限として定義されています:

- ユーザーの個人情報を含むデータまたはリソースにアプリがアクセスできる権限。

- または、ユーザーの保存データや他のアプリの操作に影響を与える可能性がある権限。たとえば、ユーザーの連絡先を読み取れるというのは、危険な権限です。

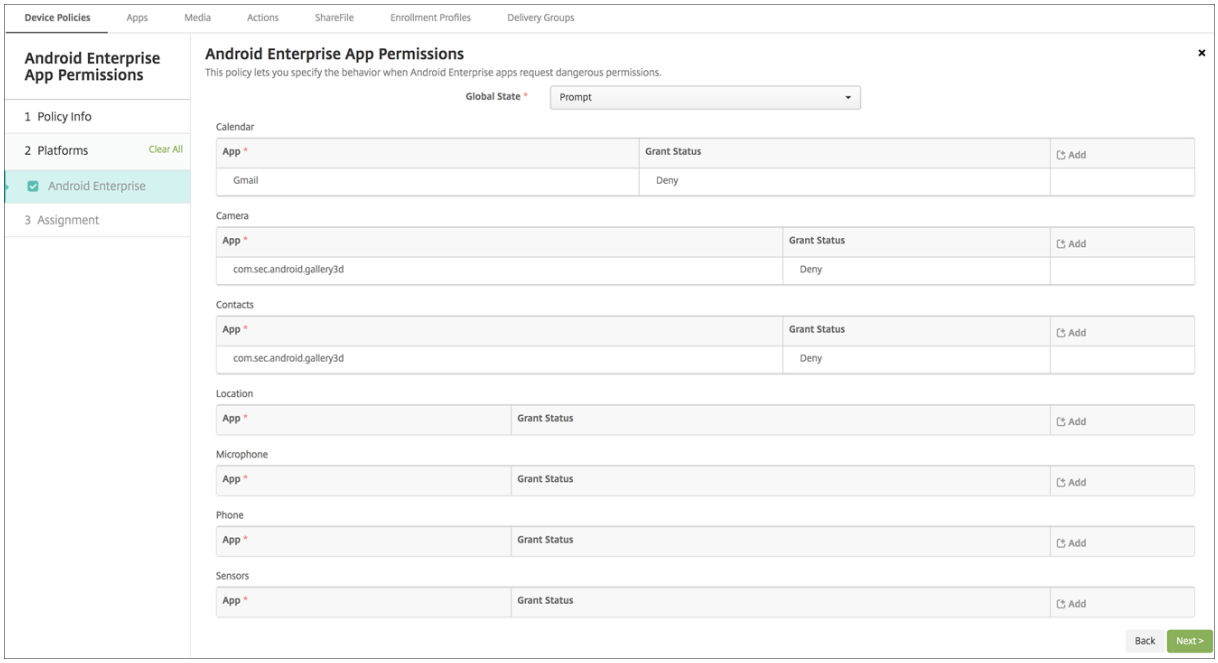
グローバルな状態を構成して、すべての危険な権限要求の動作を制御することができます。この構成の範囲は、仕事用プロファイル内にある Android Enterprise アプリです。Google で定義されているように、アプリごとに、個々の権限グループに対して危険な権限の要求の動作を制御することもできます。これらの個々の設定は、グローバルな状態を上書きします。

Google が権限グループをどのように定義しているかについては、『Android 開発者ガイド』を参照してください。

デフォルトでは、危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise の設定



- グローバルの状態：すべての危険な権限要求の動作を制御します。一覧で［プロンプト］、［許可］、または ［拒否］をクリックします。

  - プロンプト：危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。
  - 許可：すべての危険な権限要求は許可されます。ユーザーにはプロンプトは表示されません。
  - 拒否：すべての危険な権限要求は拒否されます。ユーザーにはプロンプトは表示されません。

  デフォルトは ［プロンプト］です。

- 各アプリについて各権限グループの個別の動作を設定します。権限グループの動作を構成するには、［追加］をクリックし、［アプリ］の下の一覧からアプリを選択します。Android Enterprise システムアプリを構成す

る場合、［新規追加］をクリックして、制限デバイスポリシーで有効にしたアプリケーションパッケージ名を入力します。［状態を許可］で ［プロンプト］、［許可］、または ［拒否］を選択します。この状態の許可は、グローバルの状態を上書きします。

- プロンプト：このアプリのこの権限グループからの危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。
- 許可：このアプリのこの権限グループからの危険な権限要求が許可されます。ユーザーにはプロンプトは表示されません。

  > 注：
  >
  > プロファイル所有者モードで登録されているデバイスの場合、デバイスが Android 12 以降で実行されていると、カメラ、位置情報、マイク、およびセンサーに対する権限の付与は適用されません。

- 拒否：このアプリのこの権限グループからの危険な権限要求が拒否されます。ユーザーにはプロンプトは表示されません。

デフォルトは ［プロンプト］です。

- アプリと［状態を許可］の横にある ［保存］をクリックします。
- 権限グループにアプリを追加するには、もう一度 ［追加］をクリックして、これらの手順を繰り返します。
- 権限グループの ［状態を許可］の設定が完了したら、［次へ］をクリックします。

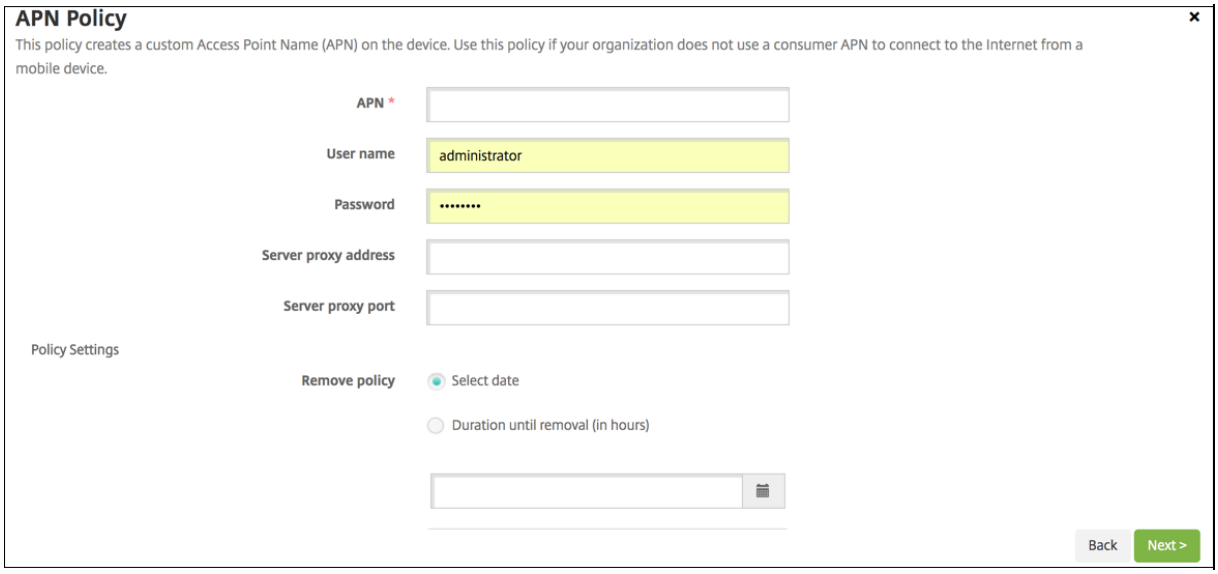
APN デバイスポリシー

February 16, 2022

iOS および Android デバイスに、カスタムアクセスポイント名（APN）デバイスポリシーを追加できます。このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマー APN を使用しない組織で使用します。APN ポリシーによって、特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。ほとんどの新しい電話機において、この設定は既に定義されています。

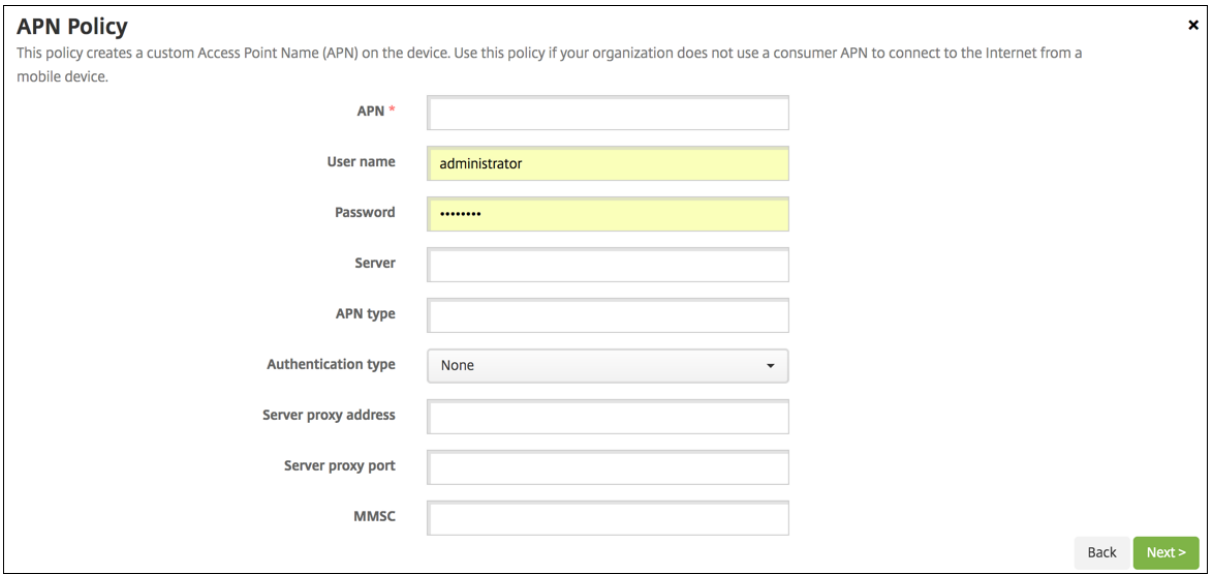
このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **APN**: アクセスポイントの名前を入力します。この名前は承認されている iOS の APN と一致する必要があります。一致しない場合、ポリシーは機能しません。
- ユーザー名: この APN のユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- パスワード: この APN のユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- サーバープロキシアドレス: APN プロキシの IP アドレスまたは URL です。
- サーバープロキシポート: APN プロキシのポート番号です。サーバーのプロキシアドレスを入力した場合、ポート番号は必須です。
- [ポリシー設定] の下の [ポリシーの削除] の横にある、[日付を選択] または [削除までの期間（日）を指定] をクリックします。
  - [日付を選択] オプションの場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [パスワードが必要] オプションの場合、パスワードを入力します。
- ポリシー設定
  - ポリシーの削除: ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、[日付を選択] と [削除までの期間（時間）を指定] です。
    * 日付を選択: カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定: ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

Android の設定



- **APN**：アクセスポイントの名前を入力します。この名前は承認されている Android の APN と一致する必要があります。一致しない場合、ポリシーは機能しません。
- ユーザー名：この APN のユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- パスワード：この APN のユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- サーバー：この設定はスマートフォンに先行するもので、通常は空白です。標準の Web サイトにアクセスできない、または標準の Web サイトを表示できない電話機用のワイヤレスアプリケーションプロトコル（WAP）ゲートウェイサーバーを参照します。
- **APN** の種類：この設定は、電話会社が想定しているアクセスポイントの使用方法に一致している必要があります。内容は APN サービス指定子のコンマ区切り文字列であり、携帯電話会社が公開している定義と一致している必要があります。以下に例を示します：
  - `\*`：すべてのトラフィックがこのアクセスポイントを経由します。
  - `mms`：マルチメディアトラフィックがこのアクセスポイントを経由します。
  - **`default`**：マルチメディアトラフィックを含め、すべてのトラフィックがこのアクセスポイントを経由します。
  - `supl`：SUPL（Secure User Plane Location）は補助 GPS に関連付けられています。
  - `dun`：ダイヤルアップネットワークは古いため、ほとんど使用されません。
  - `hipri.`：高優先度ネットワークです。
  - `fota`：FOTA（Firmware over the air）は、ファームウェア更新の受信に使用されます。
- 認証の種類：一覧から、使用する認証の種類を選択します。デフォルトは［なし］です。
- サーバープロキシアドレス：電話会社の APN HTTP プロキシの IP アドレスまたは URL です。

- サーバープロキシポート： APN プロキシのポート番号です。サーバーのプロキシアドレスを入力した場合、ポート番号は必須です。
- **MMSC**：電話会社が提供する MMS ゲートウェイサーバーのアドレスです。
- マルチメディアメッセージングサーバー（**MMS**）プロキシアドレス： MMS トラフィック用のマルチメディアメッセージングサービスサーバーのアドレスです。MMS は SMS の後継で、画像やビデオなどのマルチメディアコンテンツを含む大きいサイズのメッセージを送信できます。これらのサーバーは特定のプロトコルを必要とします（MM1、…MM11）。
- **MMS** ポート： MMS プロキシに使用されるポートです。

アプリアクセスデバイスポリシー

November 29, 2023

アプリアクセスデバイスポリシーを使用すると、インストールする必要がある、インストールできる、またはインストールしてはならないアプリの一覧を定義できます。デバイス上のアプリがこのポリシーと矛盾する場合、Citrix Endpoint Management はデバイスをコンプライアンス違反としてマークします。次に、そのデバイスのコンプライアンスに対して行う自動化された操作を作成できます。

> 重要：
>
> アプリアクセスデバイスポリシーは、ユーザーが禁止アプリをインストールしたり、必須アプリをアンインストールしたりすることを妨げるものではありません。

アクセスポリシーは一度に 1 種類のみ構成できます。各ポリシーは必須アプリ、推奨アプリ、禁止アプリのいずれかの一覧を含みますが、同じアプリアクセスポリシー内に混在させることはできません。一覧の種類ごとにポリシーを作成する場合、どのポリシーがどのアプリケーション一覧に適用されるかがわかるようにするため、各ポリシーの名前付けに注意してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **Android**（従来のデバイス管理者）の設定

- アクセスポリシー：このポリシー用に構成する一覧の種類を選択します。
  - 必須：アプリはデバイスに存在する必要があります。アプリが存在しない場合、デバイスはコンプライアンス違反としてマークされます。必須はデフォルトのオプションです。
  - 禁止：アプリはデバイス上に存在してはなりません。アプリが存在する場合、デバイスはコンプライアンス違反としてマークされます。
- 一覧に 1 つまたは複数のアプリを追加するには、次を実行します：

1. ［追加］をクリックして、以下を構成します：
   - アプリ名：アプリ名を入力します。
   - アプリ識別子：任意で、アプリ識別子を入力します。
2. ［保存］をクリックします。
3. 追加するアプリごとに上記の手順を繰り返します。

アプリアクセスのコンプライアンスに基づいて自動化された操作を構成する

1. アプリを必須または禁止にするアプリアクセスポリシーを追加します。
2. 対象のアプリが必須か禁止かに基づいて、2 つの自動化された操作を構成します。
   - 必須
     - 必須アプリがデバイスに存在しない場合は、デバイスをコンプライアンス違反としてマークします。
     - 必須アプリがインストールされたら、デバイスを準拠としてマークします。
   - 使用不可
     - 禁止アプリがデバイスに存在する場合は、デバイスをコンプライアンス違反としてマークします。
     - 禁止アプリが削除された後、デバイスを準拠としてマークします。

     自動化された操作の設定について詳しくは、「自動化された操作」を参照してください。
3. コンプライアンス違反のデバイスに実装する設定を使用して制限ポリシーを作成します。
   a) 制限ポリシーの一部として、［ブールデバイスプロパティで制限する］、［コンプライアンス違反］、［真］オプションを使用して高度な展開規則を追加します。「制限デバイスポリシー」を参照してください。

4. プロファイル削除ポリシーを作成して、デバイスがコンプライアンス状態に戻ったら制限ポリシーを削除します。
5. ［ブールデバイスプロパティで制限する］、［コンプライアンス違反］、［偽］オプションを使用して高度な展開規則を追加します。「プロファイル削除デバイスポリシー」を参照してください。

アプリ属性デバイスポリシー

November 18, 2021

アプリ属性デバイスポリシーを使用すると、iOS デバイス上のアプリの属性を指定できます。この種類のポリシーを構成することにより、次のことを実現できます:

- Per-App VPN をアプリに割り当てます。
- ユーザーがミッションクリティカルなアプリをアンインストールできないようにします。iOS 14 以降に適用されます。
- 関連付けられた機能が有効になっている場合は、アプリに追加する関連ドメインを指定します。iOS 13 以降に適用されます。

  詳しくは、「関連付けられたドメインについて」を参照してください。

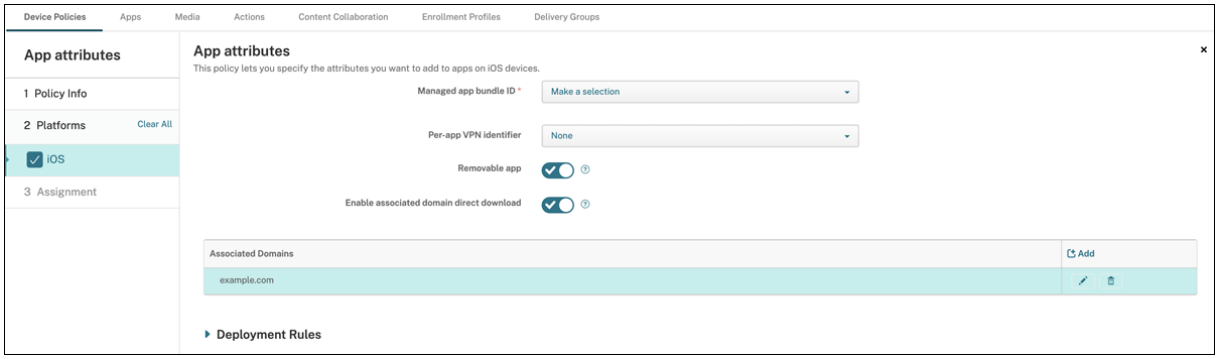
このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

関連付けられたドメインについて

関連付けられたドメインを使用すると、ドメインとアプリの間にセキュアな関連付けを確立できるため、Web サイトからアプリで資格情報を共有したり、機能を提供したりできます。たとえば、この機能を有効にすると、組織内のアプリと Web サイト間でデータとサインイン資格情報を共有できます。

この機能を有効にする方法について詳しくは、Apple Web サイトのSupporting Associated Domainsを参照してください。

iOS の設定



- 管理対象アプリのバンドル **ID**: 次の方法でアプリを指定します:

  - アプリバンドル ID を選択します。オプションは、管理対象デバイス上のアプリのインベントリを収集するアプリインベントリデバイスポリシーを有効にした後でのみ使用できます。
  - ［新規追加］を選択し、アプリバンドル ID を入力します。
    アプリバンドル ID を見つけるには、「App Store でアプリのバンドル ID を見つける」を参照してください。

- **Per-app VPN** 識別子：（オプション）このアプリの Per-app VPN を選択します。オプションには ［デバイスポリシー］ **>** ［**VPN** ポリシー］ページで構成した Per-app VPN 接続も含まれます。
  詳しくは、「Per-App VPN の構成」を参照してください。
- **Removable app**：（オプション）このアプリが管理対象アプリの場合、ユーザーによって削除できるかを指定します。ユーザーがこのアプリをアンインストールできないようにするには、このオプションを ［オフ］に設定します。デフォルトは ［オン］です。
- **Enable associated domain direct download**：（オプション）デフォルトは ［オン］です。このアプリが要求されたサイトの関連付けの検証を、Apple のサーバーではなくドメインで直接実行することを示します。インターネットにアクセスできないドメインの場合のみ、このオプションを ［オン］に設定します。
- **Associated Domains**：（オプション）このアプリの関連付けられたドメインを追加するには、［**Add**］をクリックし、完全修飾ドメイン名（FQDN）を入力します。

App Store でアプリのバンドル **ID** を見つける

1. App Store でアプリを見つけ、URL の末尾にある番号をコピーします。たとえば、363501921 は Citrix Workspace アプリのアプリ ID です。
2. `https://itunes.apple.com/lookup?id=`に移動し、その URL の後にこの番号を貼り付けます。TXT ファイルがコンピューターに自動的にダウンロードされます。
3. TXT ファイルで`bundleId`を検索し、アプリのバンドル ID を取得します。例：Citrix Workspace アプリのバンドル ID は`com.citrix.ReceiveriPad`です。

アプリ構成デバイスポリシー

March 15, 2024

以下を展開することによって、管理対象の構成をサポートするアプリをリモートで構成できます。

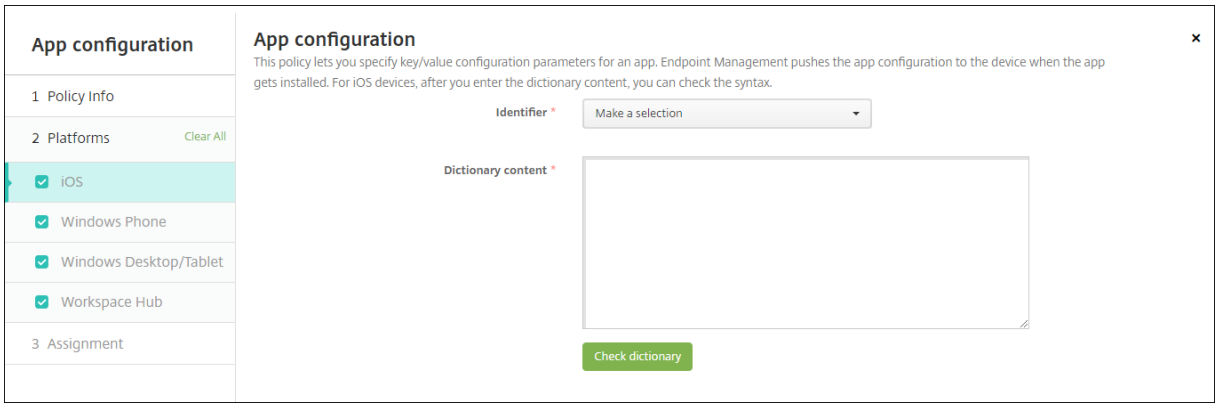
- XML 構成ファイル（`.plist`、またはプロパティ一覧と呼ばれる）を iOS デバイスに展開します。
- キー/値ペアを Windows 10 または Windows 11 を実行しているデスクトップまたはタブレットデバイスに展開します。

この構成では、アプリ内のさまざまな設定や動作を指定します。ユーザーがアプリをインストールすると、Citrix Endpoint Management はこの構成をデバイスにプッシュします。設定できる実際の設定と動作はアプリによって異なり、この記事では扱いません。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

> 注:
>
> アプリ構成の変数は、それぞれのアプリケーション所有者によって定義されます。
> たとえば、Chrome のアプリ構成の変数は、Chrome によって管理、維持されます。詳しくは、Chrome アプリの構成変数を参照してください。

iOS の設定



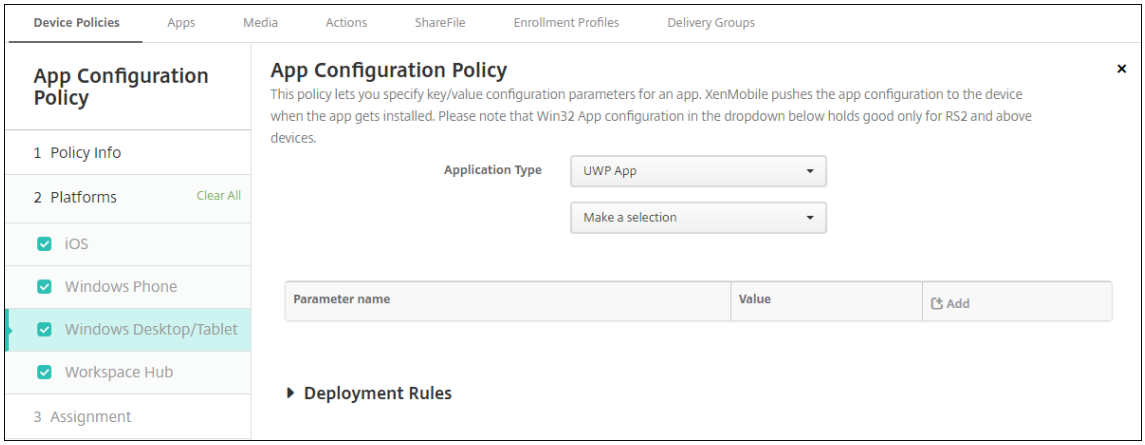
- 識別子：一覧から構成するアプリを選択するか、［新規追加］をクリックしてアプリを一覧に追加します。
  - ［新規追加］をクリックした場合は、表示されるフィールドにアプリ識別子を入力します。
- ディクショナリの内容： XML プロパティ一覧（`.plist`）の構成情報を入力するか、コピーして貼り付けます。
- ［ディクショナリをチェック］をクリックします。Citrix Endpoint Management が XML を検証します。エラーがなければ、コンテンツボックスの下に「有効な **XML**」と表示されます。コンテンツボックスの下に何らかの構文エラーが表示された場合は、続行する前にエラーを修正する必要があります。

Windows デスクトップ/タブレットの設定

ユニバーサル Windows プラットフォーム（UWP）アプリか Win 32 アプリのいずれかを構成できます。Microsoft 管理用テンプレート（ADMX）ポリシー設定をインポートするには、Win 32 アプリを構成します。

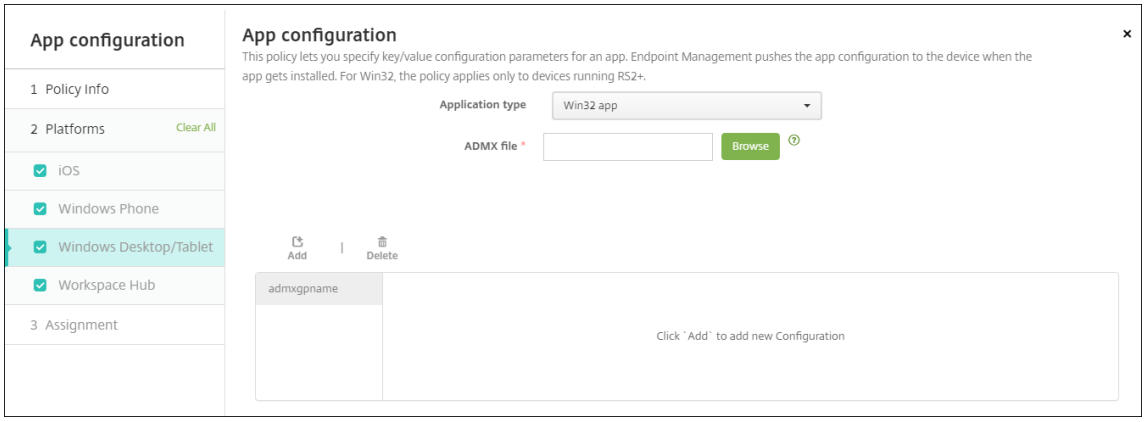
> 注:
>
> アプリ構成デバイスポリシーでは、Office などのサードパーティアプリケーション向けに、サードパーティの ADMX ファイルをサポートしています。`%SystemRoot%\PolicyDefinitions<!--NeedCopy-->`にオペレーティングシステムグループポリシーとして用意されている Windows 用の Microsoft 製 ADMX テンプレートはサポートされません。

- [**UWP** アプリ] を選択した場合：[選択] 一覧から構成するアプリをクリックするか、[新規追加] をクリックしてアプリを一覧に追加します。

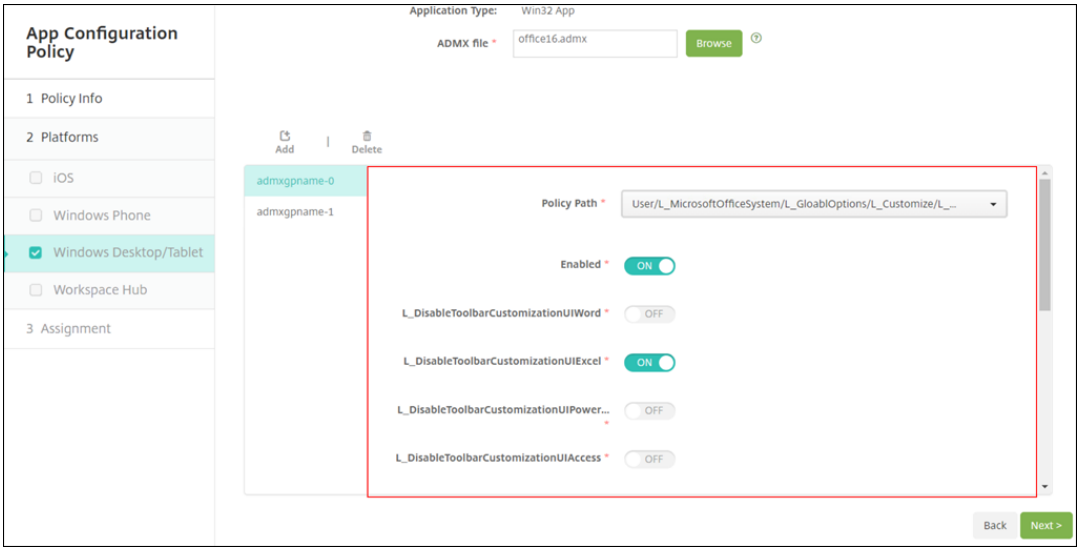


  - [新規追加] をクリックした場合は、表示されるフィールドにパッケージファミリ名を入力します。
  - 構成パラメーターごとに、[追加] をクリックして以下の操作を行います：
    - パラメーター名： Windows デバイスのアプリケーション設定のキー名を入力します。Windows アプリの設定については、Microsoft 社のドキュメントを参照してください。
    - 値：指定されたパラメーターの値を入力します。
    - [追加] をクリックしてパラメーターを追加するか、[キャンセル] をクリックしてパラメーターの追加を取り消します。

- [**Win32** アプリ] を選択した場合：[参照] をクリックし、ポリシーを構成するために使用する ADMX ファイルに移動します。



  - [追加] をクリックします。ADMX ファイルの設定オプションがページの右側に表示されます。



- ポリシーパスを選択します。同じパスを複数回選択した場合、直近のバージョンに関連付けられた構成が適用されます。
- ［有効化］を ［オン］に設定します。
- 必要な一覧の要素の値を、キーと値のペアとして入力します。各キーと値のペアおよびそのペア内の値とキーは、テキスト文字列「**&#xF000**」を使用して区切ります。
- 小数点を含む要素の値には、特定の範囲内の値が必要な場合があります。

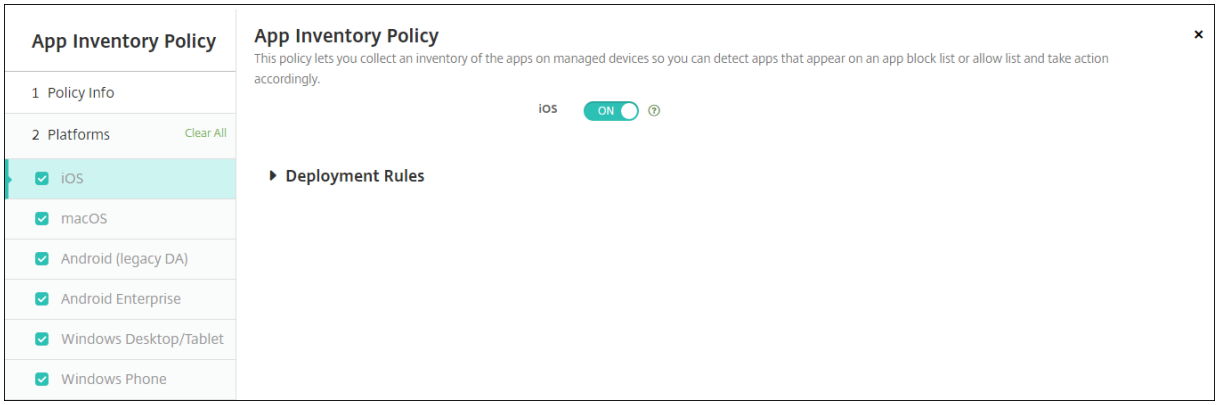
アプリインベントリデバイスポリシー

November 29, 2023

アプリインベントリポリシーでは、管理対象デバイス上のアプリのインベントリを収集できます。これにより、Citrix Endpoint Management はインベントリを、そのデバイスに展開済みのアプリアクセスポリシーと比較できます。この方法で、アプリの許可リストまたは禁止リストにあるアプリを検出し、それに応じて対応できます。アプリのアクセスポリシーを使用して、許可リストまたは禁止リストを定義します。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS、**macOS**、**Android**（従来のデバイス管理者）、**Android Enterprise**、**Windows** デスクトップ/タブレット



- 選択したプラットフォームごとに、デフォルト設定のままにしておくか、設定を ［オフ］に変更します。デフォルトは ［オン］です。

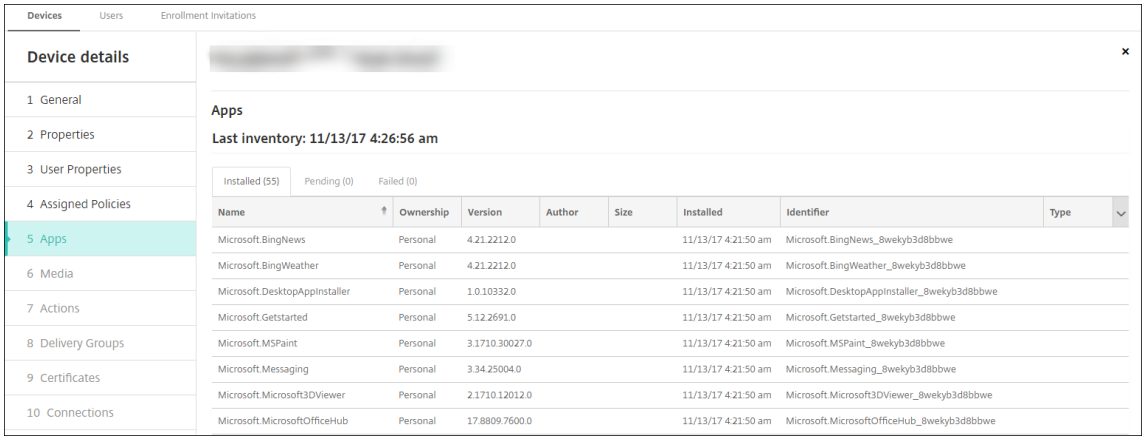
Win32 アプリのインベントリと削除

ユーザーデバイス上の Win32 アプリがアプリアクセスデバイスポリシーに準拠しているかどうかを判別できます。管理対象の Windows 10 および Windows 11 デスクトップデバイスおよびタブレットデバイスの Win32 アプリのインベントリを表示するには:

1. ［構成］**>** ［デバイスポリシー］に移動し、**Windows** デスクトップ/タブレットプラットフォームの［アプリインベントリ］ポリシーを追加します。ポリシーを展開します。
2. ［管理］**>** ［デバイス］に移動して、表示する Windows 10 および Windows 11 デバイスを選択し、［編集］をクリックして ［アプリ］タブをクリックします。

   インベントリの結果が表示されます。

   > 注:
   >
   > Windows 11 デバイスを構成している場合、Microsoft の設計どおりに正確なインベントリ結果を得るには最大 24 時間待つ必要があります。



3. 実際のアプリのインベントリを［アプリインベトリ］デバイスポリシーと比較します。デバイスに禁止リスト登録済みのアプリがインストールされている場合、デバイスから削除できます。

誤った製品コードに起因するアプリのインストールとアンインストールの問題

Win32 アプリが誤った製品コードで構成されている場合、アプリは初めはインストールされますが、Microsoft から Citrix Endpoint Management にこのアプリの状態が返されません。次のような結果になります:

- ［アプリのアンインストール］デバイスポリシーでアプリがアンインストールされません。
- Citrix Endpoint Management はアプリのインストールを確認していないため、引き続きアプリを展開します。アプリは既にインストールされているため、展開のたびにデバイスはエラーコードを生成します。［管理］**>**［デバイス］**>**［デリバリーグループ詳細］に表示されるエラーは次のとおりです: `Msi Application received: Reporting:AppPush id:7z1701-x64.msi : Command execution failed -2147023293`

製品コードを修正するには、以下の操作を行います:

1. アプリを手動でデバイスから削除します。
2. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］に移動して、Win32 アプリの製品コードを修正します。
3. Win32 アプリを展開します。

Application Guard デバイスポリシー

February 16, 2022

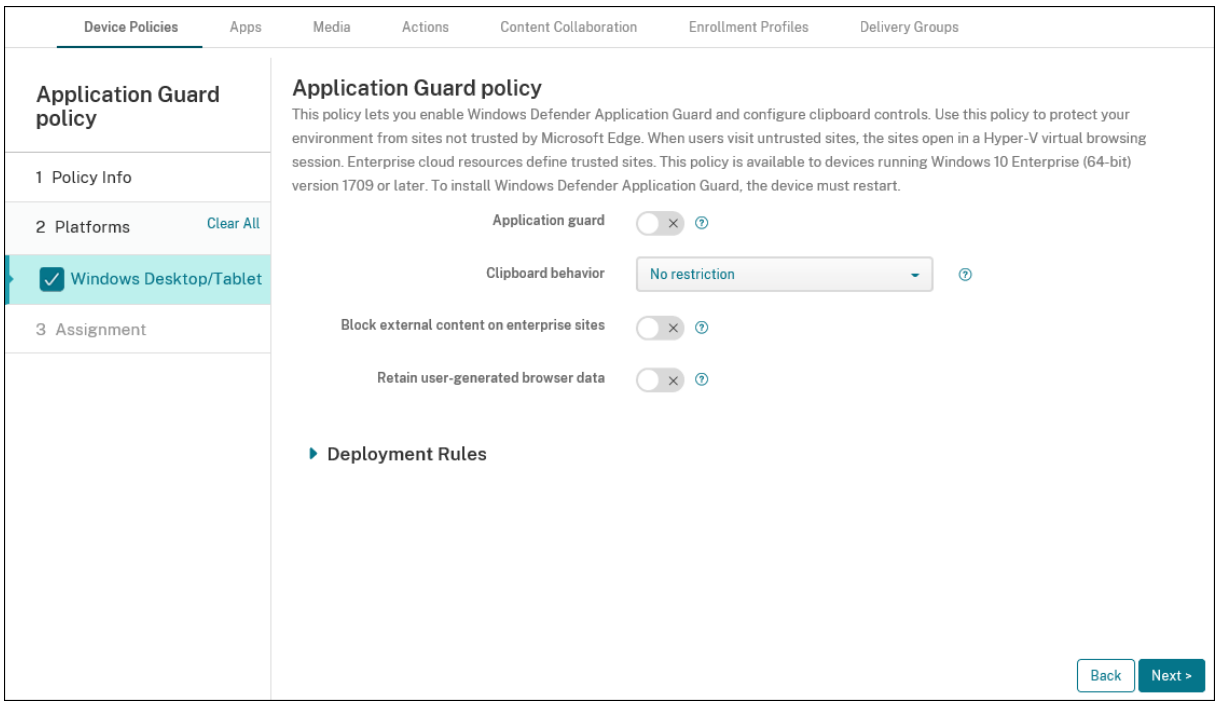
Application Guard ポリシーは、Windows Defender Application Guard の設定を指定します。この設定には、Application Guard を有効にするかどうかや、クリップボード動作の制御が含まれます。

Windows Defender Application Guard は、組織が信頼するサイトとして定義していないサイトから環境を保護します。ユーザーが分離ネットワーク境界に表示されていないサイトにアクセスすると、サイトは Hyper-V の仮想閲覧セッションで開きます。エンタープライズクラウドリソースは信頼済みサイトを定義します。

要件

- Windows 10 Enterprise（64 ビット）または Windows 11 Enterprise（64 ビット）を実行しているデバイス。Windows Defender Application Guard をインストールするには、デバイスを再起動する必要があります。
- Microsoft Edge ブラウザー

Windows デスクトップとタブレットの設定



- **Application Guard**: Application Guard を有効にするかどうかを指定します。デフォルトは ［オフ］です。
  - エンタープライズクラウドリソース：エンタープライズクラウドドメインをコンマで区切って列挙します。
- クリップボードの動作：コンテンツをコピーして貼り付けることができる方向を制御します。使用できるオプションは、次のとおりです。
  - 未構成

  - ブラウザーから **PC** へのコピーと貼り付けのみを許可： Web ブラウザーから PC にのみコンテンツをコピーして貼り付けることができます。
  - **PC** からブラウザーへのコピーと貼り付けのみを許可： PC から Web ブラウザーにのみコンテンツをコピーして貼り付けることができます。
  - **PC** と **Web** ブラウザー間でコピーと貼り付けを許可： PC と Web ブラウザー間で自由にコンテンツをコピーして貼り付けられます。
  - **PC** と **Web** ブラウザー間のコピーと貼り付けを禁止： PC とブラウザー間でのコンテンツのコピーおよび貼り付けを禁止します。

- クリップボードのコンテンツ：ユーザーがコピーおよび貼り付けできるコンテンツを制御します。使用できるオプションは、次のとおりです。

  - 制限なし
  - テキストのコピーを許可する：テキストのみコピーできるようにします。
  - 画像のコピーを許可する：画像のみをコピーできるようにします。
  - テキストと画像両方のコピーを許可する：テキストと画像の両方をコピーできるようにします。

- エンタープライズサイトで外部コンテンツをブロックする：[オン]の場合、Windows Defender Application Guard により、エンタープライズサイトでの未承認サイトのコンテンツの読み込みが禁止されます。デフォルトは ［オフ］です。
- ユーザー生成 **Web** ブラウザーデータを保持する：［オン］の場合、Application Guard の仮想閲覧セッション中に作成されたユーザーデータを保存できます。このデータには、パスワード、お気に入り、Cookie などが含まれます。デフォルトは ［オフ］です。

アプリのロックデバイスポリシー

November 29, 2023

アプリのロックデバイスポリシーは、次のいずれかのアプリの一覧を定義します：

- デバイス上で実行できる。
- デバイス上で実行できない。

ポリシーの厳密な機能は、サポートされるプラットフォームごとに異なります。たとえば、iOS デバイスで複数のアプリを禁止することはできません。

また、iOS デバイスで選択できる iOS アプリは、ポリシーあたり 1 つのみです。デバイスで実行できるのは 1 つのアプリのみになります。アプリのロックデバイスポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。

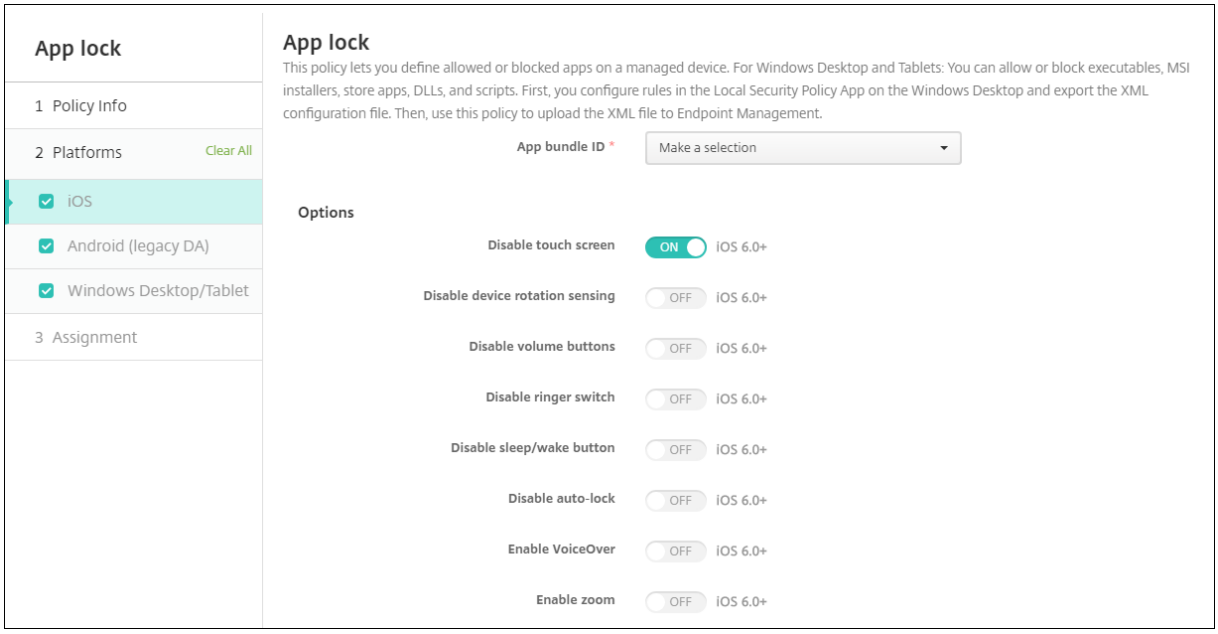
また、iOS デバイスは、アプリのロックポリシーをプッシュするように監視される必要があります。

デバイスポリシーは大部分の Android L および M デバイスで機能しますが、アプリのロックは Android N 以降のデバイスでは機能しません。これは、Google が必要な API を廃止したためです。

管理対象の Windows デスクトップとタブレットでは、許可リストおよび禁止リストに登録されたアプリの一覧を定義するアプリのロックデバイスポリシーを作成できます。実行可能ファイル、MSI インストーラー、ストアアプリ、DLL、スクリプトを許可またはブロックできます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- アプリバンドル **ID**: このポリシーを適用するアプリを一覧から選択するか、［新規追加］をクリックして、アプリを一覧に追加します。［新規追加］をクリックした場合は、表示されるフィールドにアプリ名を入力します。
- オプション: ［タッチスクリーンを無効化］を除き、各オプションのデフォルトは ［オフ］です（［タッチスクリーンを無効化］はデフォルトで ［オン］に設定されています）。
  - タッチスクリーンを無効化
  - デバイスの回転検出を無効化
  - 音量ボタンを無効化
  - 着信/サイレントスイッチを無効化

    ［着信/サイレントスイッチを無効化］が ［オン］の場合、着信動作は、スイッチが最初に無効化されたときの場所に依存します。
  - スリープ/スリープ解除ボタンを無効化
  - 自動ロックを無効化

  - VoiceOver を無効化
  - ズームを有効化
  - 色の反転を有効化
  - AssistiveTouch を有効化
  - 選択項目の読み上げを有効化
  - モノラルオーディオを有効化
  - 音声制御を有効にする

- ユーザーが有効化するオプション：各オプションのデフォルトは ［オフ］です。
  - VoiceOver の調整を許可
  - ズームの調整を許可
  - 色の反転の調整を許可
  - AssitiveTouch の調整を許可
  - 音声制御の調整を許可

- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

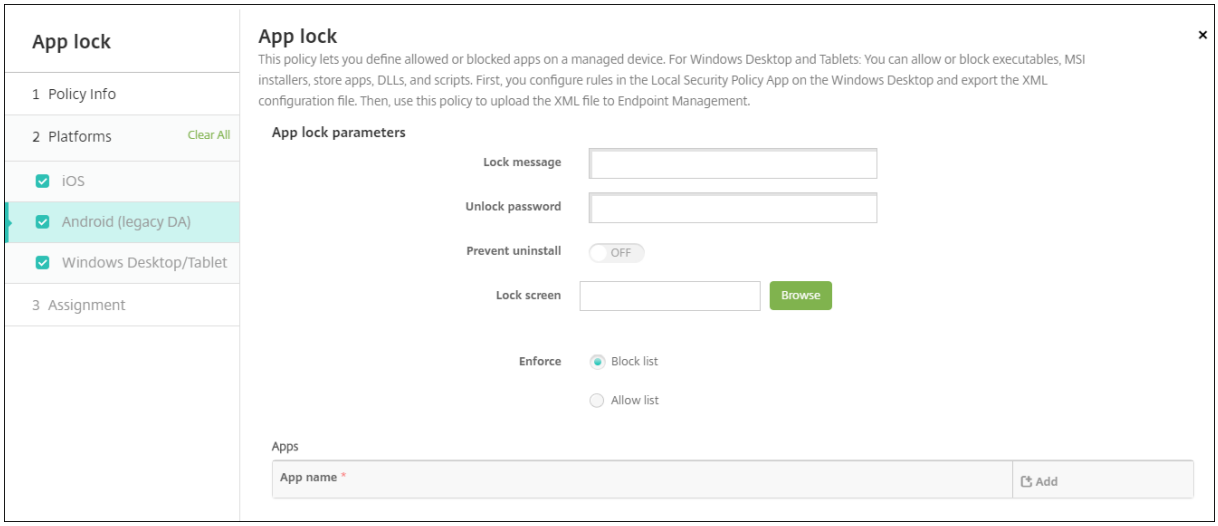
iPad をキオスクとして構成する

アプリのロックデバイスポリシーを使用して、監視対象の iPad をキオスクとして実行できます。Apple ではこの機能を「シングル App モード」と呼びます。これらの機能について詳しくは、Apple 社のドキュメントを参照してください。このポリシーを展開する前に、実行するアプリを展開してください。

1. ［構成］**>**［デバイスポリシー］に移動して、［追加］をクリックします。
2. ［アプリのロック］ポリシーを選択します。
3. ［ポリシー名］、およびオプションの ［説明］に入力します。
4. ［**iOS**］プラットフォームのみを選択します。
5. ［アプリバンドル **ID**］で、iPad で実行するアプリを選択します。
6. 前述のとおり、必要なオプションを構成し、ポリシーを保存します。
7. iPad と同じデリバリーグループにポリシーを追加して、そのポリシーを展開します。

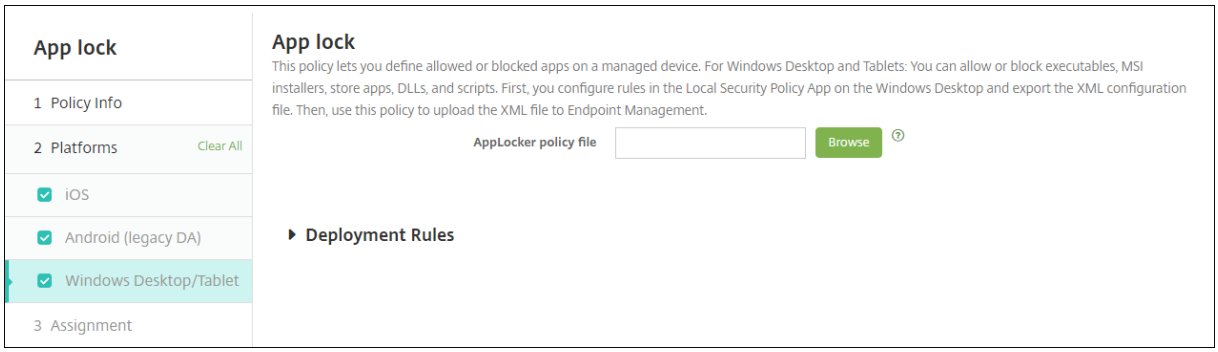
Android（レガシデバイス管理者）の設定

> 注:
>
> Android の設定アプリは、アプリのロックデバイスポリシーを使用してブロックできません。



- アプリロックのパラメーター
  - ロックメッセージ：ユーザーがロックされているアプリを開こうとしたときに表示されるメッセージを入力します。
  - ロック解除のパスワード：アプリのロックを解除するパスワードを入力します。
  - アンインストールを禁止：ユーザーにアプリのアンインストールを許可するかどうかを選択します。デフォルトは ［オフ］です。
  - ロック画面：［参照］をクリックして、デバイスのロック画面に表示する画像ファイルの場所に移動し、そのファイルを選択します。
  - 適用：デバイスでの実行が許可されないアプリの一覧を作成するには、［禁止リスト］をクリックします。デバイスでの実行が許可されるアプリの一覧を作成するには、［許可リスト］をクリックします。
- アプリ：［追加］をクリックして、以下の操作を行います：
  - アプリ名：一覧から許可リストまたは禁止リストに追加するアプリの名前をクリックします。または、［新規追加］をクリックして、使用可能なアプリの一覧にアプリを追加します。
  - ［新規追加］をクリックした場合は、表示されるフィールドにアプリ名を入力します。
  - ［保存］または ［キャンセル］をクリックします。
  - 許可リストまたは禁止リストに追加するアプリごとに、上記の手順を繰り返します。

Windows デスクトップとタブレットの設定



アプリのロックの前提条件

- Windows では、Windows 10 または Windows 11 のデスクトップ上のローカルセキュリティポリシーエディターで規則を構成します。
- ポリシー XML ファイルをエクスポートします。Windows でデフォルトの規則を作成して、デフォルトの構成がロックされたり、デバイスに問題が発生したりすることを回避してください。
- 次に、アプリのロックデバイスポリシーを使用して XML ファイルを Citrix Endpoint Management にアップロードします。詳しくは、Microsoft 社のこの記事を参照してください: https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview

Windows からポリシー XML ファイルを構成およびエクスポートするには

> 重要:
>
> ポリシー XML ファイルを Windows ポリシーエディターで構成する場合、監査専用モードを使用してください。

1. Windows コンピューターで、ローカルセキュリティポリシーエディターを起動します。[スタート] をクリックし、「ローカルセキュリティポリシー」と入力して、[ローカルセキュリティポリシー] をクリックします。
2. コンソールツリーで、[アプリケーション制御ポリシー] を展開します。
3. [**AppLocker**] をクリックし、中央のウィンドウで [規則の実施の構成] をクリックします。
4. [構成済み] を選択し、[規則の実施] を選択します。規則を有効にすると、[規則の実施] がデフォルトになります。
5. [**AppLocker**] を右クリックし、[ポリシーのエクスポート] をクリックして、XML ファイルを保存します。

> 注:
>
> 実行可能ファイルの規則、**Windows** インストーラーの規則、スクリプトの規則、パッケージアプリの規則を作成できます。このためには、フォルダーを右クリックし、[新しい規則の作成] をクリックします。

Citrix Endpoint Management にポリシー **XML** ファイルをインポートするには

アプリのロックポリシーを作成します。［アプリのロックポリシーファイル］設定の横の ［参照］をクリックし、XML ファイルに移動します。

アプリのロックポリシーの適用を停止するには

Citrix Endpoint Management でアプリのロックポリシーを展開後、アプリのロックポリシーの適用を停止するには、空の XML ファイルを作成します。次に、別のアプリのロックポリシーを作成し、ファイルをアップロードし、ポリシーを展開します。アプリのロックを有効にしたデバイスは影響を受けません。初めてポリシーを受信するデバイスには、アプリのロックポリシーは設定されません。

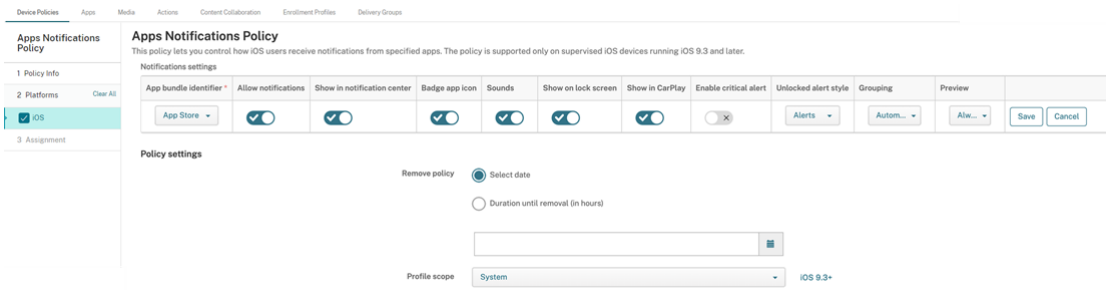
アプリ通知デバイスポリシー

February 16, 2022

アプリ通知ポリシーでは、iOS ユーザーが指定したアプリから通知を受け取る方法を制御できます。このポリシーは、iOS 9.3 以降を実行している監視対象の iOS デバイスでのみサポートされます。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- アプリバンドル **ID**：通知設定を管理するアプリを指定します。
  - アプリバンドル ID を選択します。オプションは、管理対象デバイス上のアプリのインベントリを収集するアプリインベントリデバイスポリシーを有効にした後でのみ使用できます。
  - ［新規追加］を選択し、アプリバンドル ID を入力します。
    アプリバンドル ID を見つけるには、「App Store でアプリのバンドル ID を見つける」を参照してください。

- 通知を許可：［オン］を選択すると、通知が許可されます。
- 通知センターに表示：［オン］を選択すると、ユーザーデバイスの通知センターに通知が表示されます。
- アプリアイコンをバッジ表示：［オン］を選択すると、通知がある場合、アプリアイコンにバッジ表示されます。
- サウンド：オン を選択すると通知にサウンドが含まれます。
- ロック画面に表示：［オン］を選択すると、ユーザーデバイスのロック画面に通知が表示されます。
- **CarPlay** で表示：［オン］を選択すると、Apple CarPlay に通知が表示されます。iOS 12 以降に適用されます。デフォルトは ［オン］です。
- 重大アラートを有効にする：［オン］を選択すると、アプリが通知を重大な通知としてマークできます。この設定の場合、［応答不可］および警告設定は無視されます。iOS 12 以降に適用されます。デフォルトは ［オフ］です。
- ロック解除されたアラートスタイル：［なし］、［バナー］、または ［アラート］を選択して、ロック解除されたアラートの外観を構成します。
- **Preview**：デバイスがアプリの通知プレビューを表示する方法を選択します。iOS 14 以降に適用されます。
  - **Always**：デバイスがロックまたはロック解除されたときに通知プレビューを表示します。
  - **When Unlocked**：デバイスのロックが解除されている場合にのみ通知プレビューを表示します。
  - **Never**：デバイスの通知プレビューをオフにします。
- **Grouping**：デバイスがアプリからの通知をグループ化する方法を選択します。iOS 12 以降のデバイスに適用されます。
  - **Automatic**：通知をアプリで指定されたグループにグループ化します。
  - **By app**：通知をアプリごとに 1 つにグループ化します。
  - **Off**：アプリの通知のグループ化をオフにします。デバイスはすべての通知を順番に表示します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。オプションは次のとおりです：
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降に適用されます。
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。iOS 9.3 以降に適用されます。

アプリのアンインストールデバイスポリシー

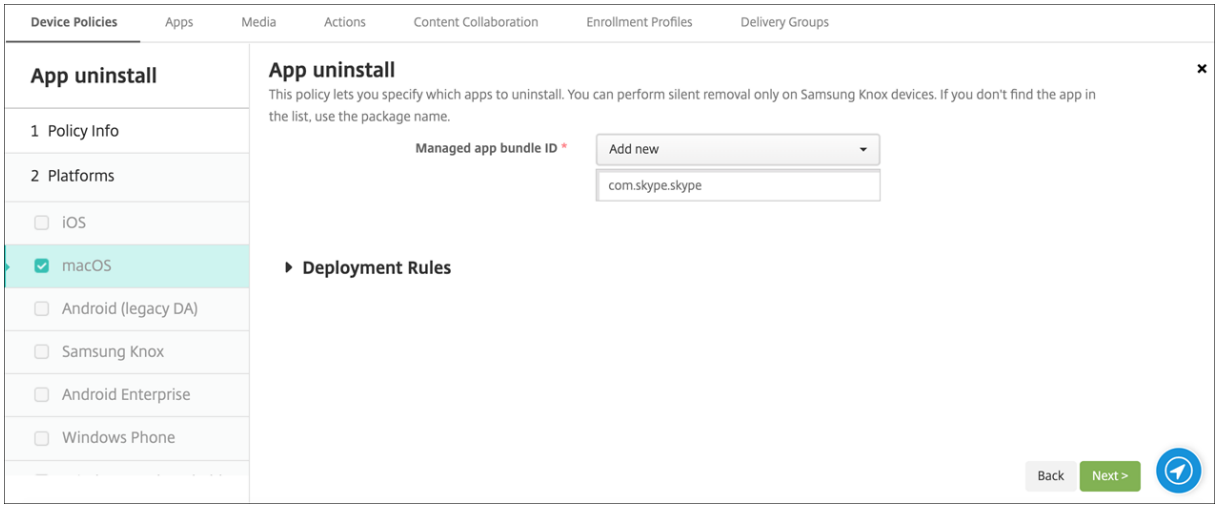
November 29, 2023

［アプリのアンインストール］ポリシーを使用すると、ユーザーデバイスからアプリを削除できます。アプリをサポートする必要がなくなった場合、または別のベンダーの同様のアプリに置き換えたい場合は、アプリを削除できます。

このポリシーがユーザーデバイスに展開されると、ユーザーにアプリのアンインストールメッセージが表示され、その後にアプリが削除されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **macOS** の設定



- 管理対象アプリバンドル **ID**：一覧で、既存の管理対象アプリを選択するか、［新規追加］を選択します。このプラットフォーム用に構成されたアプリがない場合、一覧は空であるため、新しい管理対象アプリを追加する必要があります。［新規追加］を選択すると、管理対象アプリ名を入力できるフィールドが表示されます。iOS 5.0 以降および macOS 11.0 以降で利用できます。

Android（レガシデバイス管理者）、**Android Enterprise**、**Windows** デスクトップ**/**タブレットの設定

- アンインストールするアプリ：構成パラメーターごとに、［追加］をクリックして以下の操作を行います：
  - アプリ名：一覧で既存のアプリを選択するか、［新規追加］をクリックして新しいアプリ名を入力します。このプラットフォームでアプリが構成されていない場合は一覧が空になるため、新しいアプリを追加する必要があります。
  - ［保存］をクリックしてアプリを追加するか、［キャンセル］をクリックしてアプリの追加を取り消します。

Android Enterprise アプリの場合、アプリインベントリデバイスポリシーも有効にします。「アプリインベントリデバイスポリシー」を参照してください。

対応するパブリックアプリストアのアプリをインストールした後、エンタープライズアプリを自動的にアンインストールします

Citrix Endpoint Management を構成して、Citrix アプリのパブリックアプリストアバージョンをインストールするときに、エンタープライズバージョンを削除することができます。この機能によって、パブリックアプリストアバージョンのインストール後に、ユーザーのデバイスが 2 つの同じアプリアイコンを持つことを防ぎます。

アプリのアンインストールデバイスポリシーの展開条件によって、新バージョンのインストール時に、Citrix Endpoint Management はユーザーのデバイスから旧バージョンを削除します。この機能は、Enterprise モード（XME）の Citrix Endpoint Management サーバーに接続した管理対象 iOS デバイスでのみ使用できます。

インストールしたアプリ名の条件で展開規則を構成するには：

- エンタープライズアプリの ［管理対象アプリのバンドル **ID**］を指定します。
- 規則を追加します。［新しい規則］をクリックし、サンプルに示すように、［インストール済みのアプリ名］と［は、次のものと等しい］を選択します。パブリックアプリストアのアプリのアプリバンドル ID を入力します。

この例では、指定したデリバリーグループのデバイスにパブリックアプリストアのアプリ（com.citrix.mail.ios）がインストールされると、Citrix Endpoint Management によってエンタープライズバージョン（com.citrix.mail）が削除されます。

アプリのアンインストール制限デバイスポリシー

July 7, 2022

ユーザーに Amazon デバイスでのアンインストールを許可する、または許可しないアプリを指定することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Amazon の設定

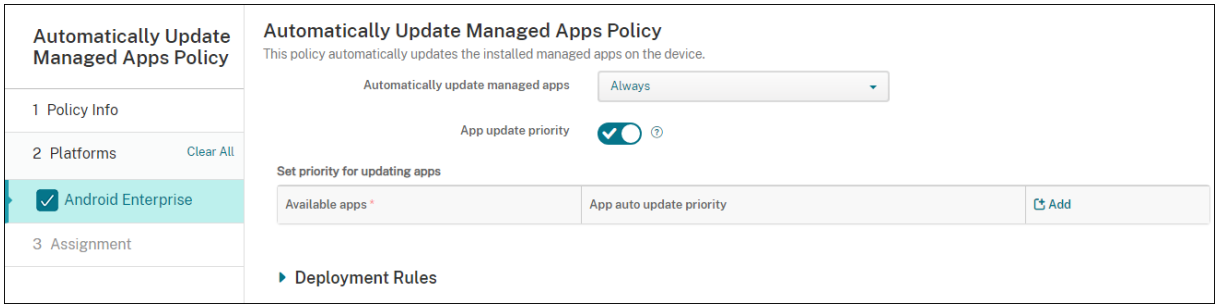
- アプリのアンインストール制限設定：追加するアプリ規則ごとに、［追加］をクリックして以下の操作を行います：
  - アプリ名：一覧でアプリをクリックするか、または ［新規追加］をクリックして新しいアプリを追加します。
  - 規則：ユーザーがアプリをアンインストールできるかどうかを選択します。デフォルトの設定ではアンインストールが許可されています。
  - ［保存］または ［キャンセル］をクリックします。

管理対象アプリの自動更新デバイスポリシー

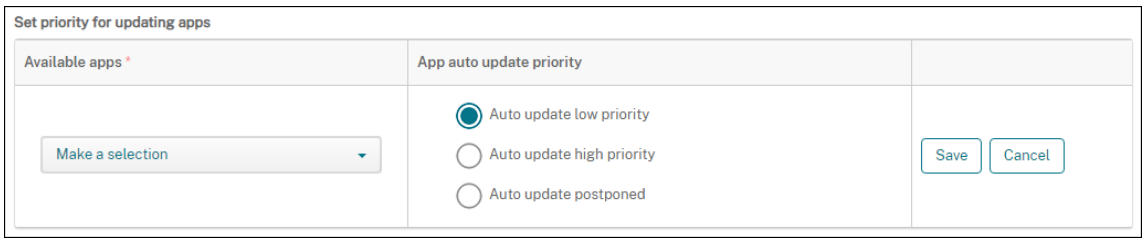
May 10, 2022

このポリシーは、インストールされている管理対象アプリが Android Enterprise デバイスでどのように更新されるかを制御します。デバイス上のアプリの自動更新を使用できるユーザー機能を制限することができます。ユーザーがデバイス上のアプリの自動更新を制御できるようにすると、管理対象の Google Play ストアでアプリの自動更新ポリシーが設定されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。



- 管理対象アプリの自動更新
  - 常に実行：アプリの自動更新を有効にします。［常に実行］がデフォルトです。
  - ユーザーによるポリシーの構成を許可：ユーザーが管理対象の Google Play ストアでデバイス上のアプリの自動更新ポリシーを構成できるようにします。
  - 実行しない：アプリの自動更新を無効にします。
  - **Only when device is connected to Wi-Fi:**：デバイスが Wi-Fi に接続されている場合にのみアプリの自動更新を許可します。
- **App update priority**：［オン］の場合、管理対象アプリごとに更新の優先度レベルを構成できます。
- **Set priority for updating apps**：［**Add**］をクリックしてアプリの構成の優先度を構成します。



  - **Available apps**：メニューからアプリを選択して、更新の優先度を設定します。
  - **App auto-update priority**：以下から更新の優先度を選択します：
    - **Auto update low priority**：デバイスが充電中でアクティブに使用されておらず、接続されているのが従量制のネットワークではない場合、アプリは更新されます。

    - **Auto update high priority**：アプリは制約なしにできるだけ早いタイミングで更新されます。
    - **Auto update postponed**：新しいバージョンが利用可能になってから最大 90 日間、アプリは自動的に更新されません。90 日後、アプリは低い優先度で自動的に更新されます。アプリの更新後、アプリはさらに 90 日間自動的に更新されません。ユーザーはいつでも手動でアプリを更新できます。
  - 変更が完了したら［**Save**］をクリックします。鉛筆アイコンをクリックすると、構成を編集できます。構成を削除するには、ごみ箱をクリックします。

BitLocker デバイスポリシー

November 29, 2023

Windows 10 および Windows 11 にはディスク暗号化機能 BitLocker が搭載されており、紛失または盗難に遭った Windows デバイスへの不正アクセスに対して、ファイルとシステムの保護が強化されています。さらに保護を強化するために、BitLocker とトラステッドプラットフォームモジュール（TPM）チップ（バージョン 1.2 以降）を組み合わせて使用できます。TPM チップは暗号化操作を処理し、暗号化キーの生成、保存、および使用の制限を行います。

Windows 10 のビルド 1703 以降では、MDM ポリシーで BitLocker を制御できるようになりました。Citrix Endpoint Management の BitLocker デバイスポリシーを使用して、Windows 10 および Windows 11 デバイスの BitLocker ウィザードで使用可能な設定を構成します。たとえば、BitLocker が有効になっているデバイスでは、BitLocker はユーザーにいくつかのオプションを提示します:

- 起動時にドライブをロック解除する方法
- 回復キーをバックアップする方法
- 固定ドライブをロック解除する方法。

BitLocker デバイスポリシーの設定では、以下についても構成します。

- TPM チップの内蔵されていないデバイスで BitLocker を有効にするかどうか。
- BitLocker インターフェイスに回復オプションを表示するかどうか。
- BitLocker が有効でない場合に、固定ドライブやリムーバブルドライブへの書き込みを拒否するかどうか。
- 暗号化された BitLocker 回復キーを安全に保存し、ユーザーがキーを忘れたり紛失したりした場合に備えてアクセスできるようにします。このキーは、Self-Help Portal にあります。

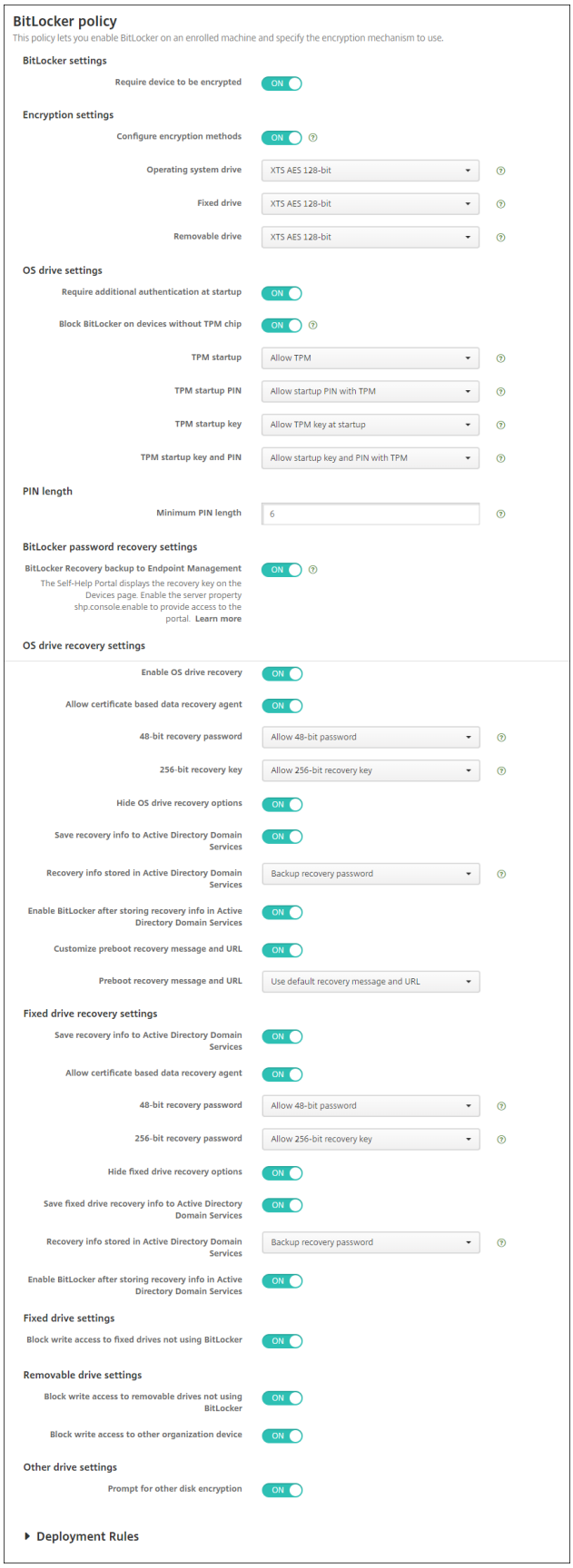
> 注
>
> BitLocker 暗号化がデバイスで開始されると、更新された BitLocker デバイスポリシーをデバイスに展開して BitLocker の設定を変更できなくなります。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

要件

- BitLocker デバイスポリシーには、Windows 10 Enterprise Edition または Windows 11 Enterprise Edition が必要です。
- BitLocker デバイスポリシーを展開する前に、BitLocker の使用に向けて環境を準備します。BitLocker のシステム要件とセットアップなどの Microsoft 社が提供する情報について詳しくは、「BitLocker」を参照してください。

Windows デスクトップとタブレットの設定



- **Bitlocker** 設定
  - デバイスの暗号化が必須： Windows デスクトップまたはタブレットで BitLocker の暗号化を有効にするよう求めるメッセージをユーザーに表示するかどうかを決定します。［オン］にすると、登録完了後に、組織によってデバイスの暗号化が求められていることを示すメッセージがデバイスに表示されます。［オフ］の場合、ユーザーにメッセージは表示されず、BitLocker はポリシー設定を使用します。デフォルトは、［オフ］です。
- 暗号化設定
  - 暗号化方式を構成する：特定の種類のドライブに使用する暗号化方式を決定します。［オフ］の場合、BitLocker ウィザードによって、ドライブの種類に使用する暗号化方式を尋ねるメッセージがデバイスユーザーに表示されます。デフォルトでは、すべてのドライブの暗号化方式は XTS-AES 128 ビットです。デフォルトでは、リムーバブルドライブの暗号化方式は AES-CBC 128 ビットです。［オン］にすると、BitLocker はポリシーで指定された暗号化方式を使用します。［オン］の場合は、オペレーティングシステムドライブ、固定ドライブ、リムーバブルドライブの追加の設定が表示されます。ドライブの種類ごとに、デフォルトの暗号化方式を選択します。デフォルトは、［オフ］です。
- **OS** ドライブ設定
  - スタートアップ時に追加の認証を要求する：デバイスの起動時に必要な、追加の認証を指定します。また、TPM チップの内蔵されていないデバイスで、BitLocker を許可するかどうかも指定します。［オフ］の場合、TPM の内蔵されていないデバイスでは、BitLocker の暗号化を使用できません。TPM について詳しくは、Microsoft の「トラステッドプラットフォームモジュール技術概要」を参照してください。［オン］の場合は、次の追加の設定が表示されます。デフォルトは、［オフ］です。
  - **TPM** チップの内蔵されていないデバイスで **BitLocker** をブロックする： TPM チップの内蔵されていないデバイスで、BitLocker はユーザーにロック解除のパスワードまたはスタートアップキーを作成するように要求します。スタートアップキーは USB ドライブに保存し、ユーザーは起動前にこれをデバイスに接続する必要があります。ロック解除のパスワードは、8 文字以上含める必要があります。デフォルトは、［オフ］です。
  - **TPM** スタートアップ： TPM の内蔵されたデバイスには、TPM-only、TPM と PIN、TPM とキー、TPM と PIN とキーの、4 つのロック解除モードがあります。［TPM スタートアップ］は、暗号キーが TPM チップに保存されている、TPM-only のモードです。このモードで、ユーザーに追加のロック解除データを入力するよう要求することはありません。起動時には TPM チップから暗号キーが使用されて、ユーザーデバイスは自動的にロック解除されます。デフォルトは ［**TPM** を許可する］です。
  - **TPM** スタートアップ **PIN**： この設定は、TPM と PIN の組み合わせのロック解除モードです。PIN には、最大 20 文字の数字を含めることができます。［**PIN** の最小文字数］の設定を使用して、PIN の最小文字数を指定します。ユーザーは、BitLocker のセットアップ時に PIN を構成し、デバイスの起動時に PIN を入力します。
  - **TPM** スタートアップキー： この設定は、TPM とキーの組み合わせのロック解除モードです。スタートアップキーは USB ドライブまたは他のリムーバブルドライブに保存し、ユーザーは起動前にこれをデ

バイスに接続する必要があります。

- **TPM** スタートアップキーと **PIN**：この設定は、TPM と PIN とキーを組み合わせたロック解除モードです。

  ロック解除に成功すると、オペレーティングシステムがロードを開始します。失敗した場合、デバイスはリカバリモードになります。

- **PIN** 長
  - **PIN** の最小文字数： TPM スタートアップ PIN の最小文字数です。デフォルトは **6** です。
- **BitLocker** パスワード回復設定
  - **Citrix Endpoint Management** への **BitLocker** 回復バックアップ：このオプションを有効にすると、デバイスのロックを解除する必要があるユーザーは、Self-Help Portal で BitLocker 回復キーを入手できます。Citrix Endpoint Management の管理者は、ユーザーの BitLocker 回復キーを表示することはできません。BitLocker 回復キーの表示について詳しくは、「BitLocker 回復キー」を参照してください。
- **OS** ドライブの回復設定： BitLocker で暗号化された OS ドライブに対する、ユーザーの回復オプションを構成します。
  - **OS** ドライブの回復の有効化：ロック解除のステップに失敗すると、BitLocker は、構成された回復キーの入力を求めるメッセージをユーザーに表示します。この設定では、ユーザーがロック解除パスワードや USB のスタートアップキーを持っていない場合に使用できる、オペレーティングシステムドライブの回復オプションを構成します。デフォルトは ［オフ］です。
  - 証明書に基づくデータ回復エージェントを許可する：証明書ベースのデータ回復エージェントを許可するかどうかを指定します。グループポリシー管理コンソール（GPMC）またはローカルグループポリシーエディターで公開キーポリシーを見つけて、データ回復エージェントを追加します。データ回復エージェントについて詳しくは、BitLocker の基本的な展開に関する Microsoft の記事を参照してください。デフォルトは ［オフ］です。
  - **48** ビットの回復パスワード：回復パスワードの使用をユーザーに許可または要求するかどうかを指定します。BitLocker はパスワードを生成し、ファイルまたは Microsoft Cloud アカウントに保存します。デフォルトは ［**48** ビットパスワードを許可］です。
  - **256** 桁の回復キー：回復キーの使用をユーザーに許可または要求するかどうかを指定します。回復キーは BEK ファイルであり、USB ドライブに保存されます。デフォルトは ［**256** ビットの回復キーを許可する］です。
  - **OS** ドライブの回復オプションを非表示にする： BitLocker インターフェイスに回復オプションを表示または非表示にするかどうかを指定します。［オン］にすると、BitLocker インターフェイスに回復オプションは表示されません。この場合はデバイスを Active Directory に登録し、回復オプションを Active Directory に保存して、［回復情報を **AD DS** に保存］を ［オン］に設定します。デフォルトは［オフ］です。

  - 回復情報を **Active Directory Domain Services** に保存：回復オプションを Active Directory Domain Services に保存するかどうかを指定します。デフォルトは ［オフ］です。
  - **Active Directory Domain Services** に保存された回復情報を構成する： BitLocker の回復パスワード、または回復パスワードとキーパッケージを、Active Directory Domain Services に保存するかどうかを指定します。キーパッケージを保存すると、物理的に破損したドライブからのデータの回復がサポートされます。デフォルトは、［回復パスワードをバックアップする］です。
  - 回復情報を **Active Directory Domain Services** に保存した後に **BitLocker** を有効にする：デバイスがドメインに接続され、BitLocker 回復情報の Active Directory へのバックアップが正常に完了するまでは、ユーザーが BitLocker を有効にすることを禁止するかどうかを指定します。［オン］にすると、BitLocker を起動する前にデバイスをドメインに参加させる必要があります。デフォルトは ［オフ］です。
  - プリブート回復メッセージおよび **URL**： BitLocker が、回復の画面でカスタマイズされたメッセージと URL を表示するかどうかを指定します。［オン］にすると次の追加設定が表示されます：［既定の回復メッセージと **URL** を表示する］、［空の回復メッセージと **URL** を使用する］、［カスタム回復メッセージを使用する］、［カスタム回復 **URL** を使用する］、［**Citrix Endpoint Management** 回復メッセージおよび **URL** を使用する］。［オフ］の場合は、デフォルトの回復メッセージと URL が表示されます。デフォルトは ［オフ］です。

- 固定ドライブの回復設定： BitLocker で暗号化された固定ドライブに対する、ユーザーの回復オプションを構成します。BitLocker は、固定ドライブの暗号化に関するメッセージをユーザーに表示しません。起動時にドライブのロックを解除するには、パスワードまたはスマートカードを使用します。ユーザーが固定ドライブでの BitLocker 暗号化を有効にすると、このポリシーにはない起動時のロック解除の設定が BitLocker インターフェイスに表示されます。関連設定について詳しくは、この一覧で前述した「**OS** ドライブの回復の構成」を参照してください。デフォルトは ［オフ］です。
- 固定ドライブ設定
  - **BitLocker** を使用しない固定ドライブへの書き込みアクセスをブロックする：［オン］にすると、固定ドライブが BitLocker で暗号化されている場合にのみ、ユーザーはこれらのドライブに書き込むことができます。デフォルトは ［オフ］です。
- リムーバブルドライブ設定
- **BitLocker** を使用しないリムーバブルドライブへの書き込みアクセスをブロックする：［オン］にすると、リムーバブルドライブが BitLocker で暗号化されている場合にのみ、ユーザーはこれらのドライブに書き込むことができます。他の組織のリムーバブルドライブへの書き込みが、組織によって許可されているかどうかに従って、この設定を構成します。デフォルトは ［オフ］です。
- 組織の他のデバイスへの書き込みアクセスをブロック：［オン］の場合、ユーザーは組織内の他のデバイス（ネットワークドライブなど）に書き込むことができません。
- 他のドライブ設定

- 他のディスク暗号化のプロンプトを表示：デバイス上の他のディスク暗号化に対する警告プロンプトを無効にすることができます。デフォルトは、［オフ］です。

Bluetooth デバイスポリシー

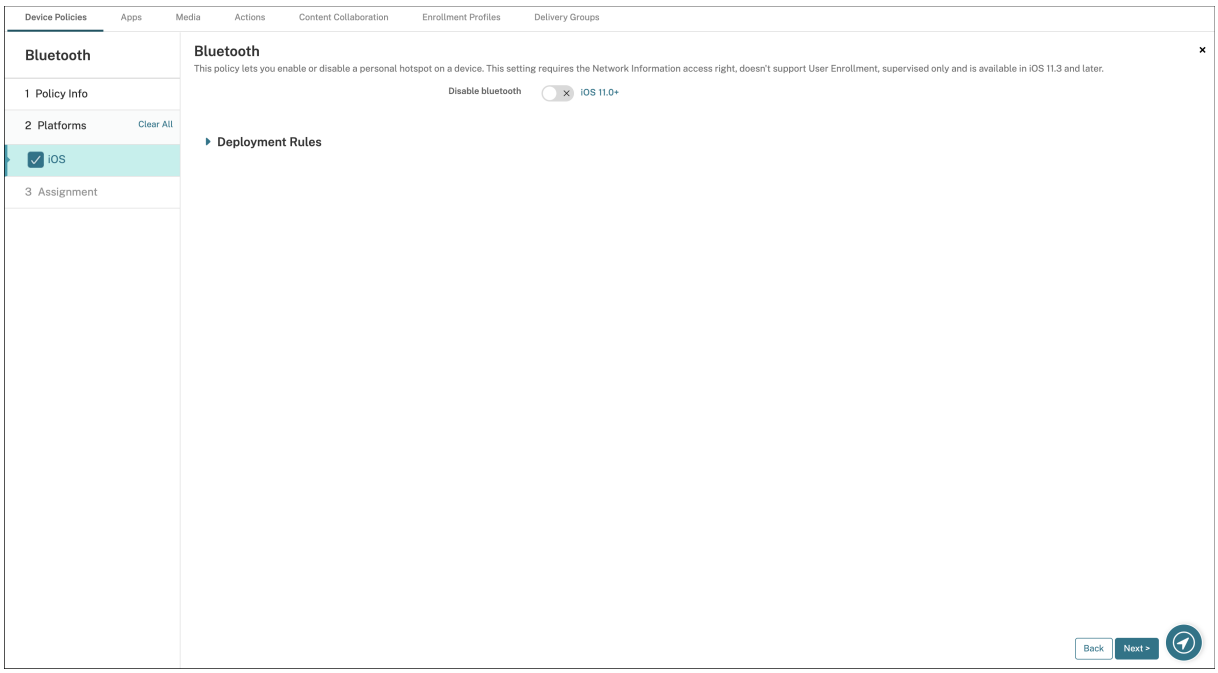
February 16, 2022

監視対象の iOS デバイスで Bluetooth ポリシーを構成して、Bluetooth を有効または無効にすることができます。

この設定にはネットワーク情報アクセス権が必要であり、ユーザー登録をサポートしておらず、iOS 11.3 以降で使用できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **Bluetooth** を無効にする：監視対象デバイスで Bluetooth を無効または有効にできます。

カレンダー（**CalDav**）デバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、カレンダー（CalDAV）アカウントをユーザーの iOS デバイスまたは macOS デバイスに追加し、CalDAV をサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明：アカウントの説明を入力します。このフィールドは必須です。
- ホスト名： CalDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート： CalDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**：ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名：ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード：任意で、ユーザーのパスワードを入力します。
- **SSL** を使用： CalDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

macOS 設定

- アカウントの説明：アカウントの説明を入力します。このフィールドは必須です。
- ホスト名： CalDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート： CalDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。

- プリンシパル **URL**：ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名：ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード：任意で、ユーザーのパスワードを入力します。
- **SSL** を使用： CalDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

モバイルデバイスポリシー

November 29, 2023

このポリシーを使用すると、iOS デバイスのモバイルネットワーク設定を構成できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

プロキシサーバーポートなど、文字列以外のフィールドにマクロを使用できます。

たとえば、`${ device.xyz }`や`${ setting.xyz }`などのマクロを使用して整数に展開できます。また、マクロは、［iOS および macOS プロファイルのインポート］デバイスポリシーで Citrix Endpoint Management にインポートしたデバイス構成 XML ファイルでも使用できます。

- **APN** をアタッチ
  - 名前：この構成の名前です。

  - 認証の種類：一覧から、[**CHAP**]（Challenge-Handshake Authentication Protocol：チャレンジハンドシェイク認証プロトコル）または [**PAP**]（Password Authentication Protocol：パスワード認証プロトコル）のいずれかを選択します。デフォルトは [**PAP**] です。
  - [ユーザー名] と [パスワード]：認証に使用するユーザー名とパスワードです。

- アクセスポイント名
  - 名前： APN（Access Point Name：アクセスポイント名）構成の名前です。
  - 認証の種類：一覧から、[**CHAP**] または [**PAP**] を選択します。デフォルトは [**PAP**] です。
  - [ユーザー名] と [パスワード]：認証に使用するユーザー名とパスワードです。
  - プロキシサーバー：プロキシサーバーのネットワークアドレスです。
  - プロキシサーバーポート：プロキシサーバーのポート番号です。

- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、[日付を選択] と [削除までの期間（時間）を指定] です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

接続のスケジューリングデバイスポリシー

November 29, 2023

> 重要：
>
> Firebase Cloud Messaging（FCM）を使用して Android および Android Enterprise デバイスから Citrix Endpoint Management への接続を制御することをお勧めします。FCM の使用について詳しくは、「Firebase Cloud Messaging」を参照してください。

FCM を使用しない場合は、接続スケジュールポリシーを作成して、ユーザーデバイスを Citrix Endpoint Management に接続する方法と時間を管理します。FCM を使用する場合は、接続スケジュールポリシーも作成する必要があります。

ユーザーが手動でデバイスを接続するか、定義した期間内にデバイスが接続されるようにするかを指定できます。

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android および **Android Enterprise** の設定

- デバイスに接続を要求：このスケジュールに対して設定するオプションをクリックします。

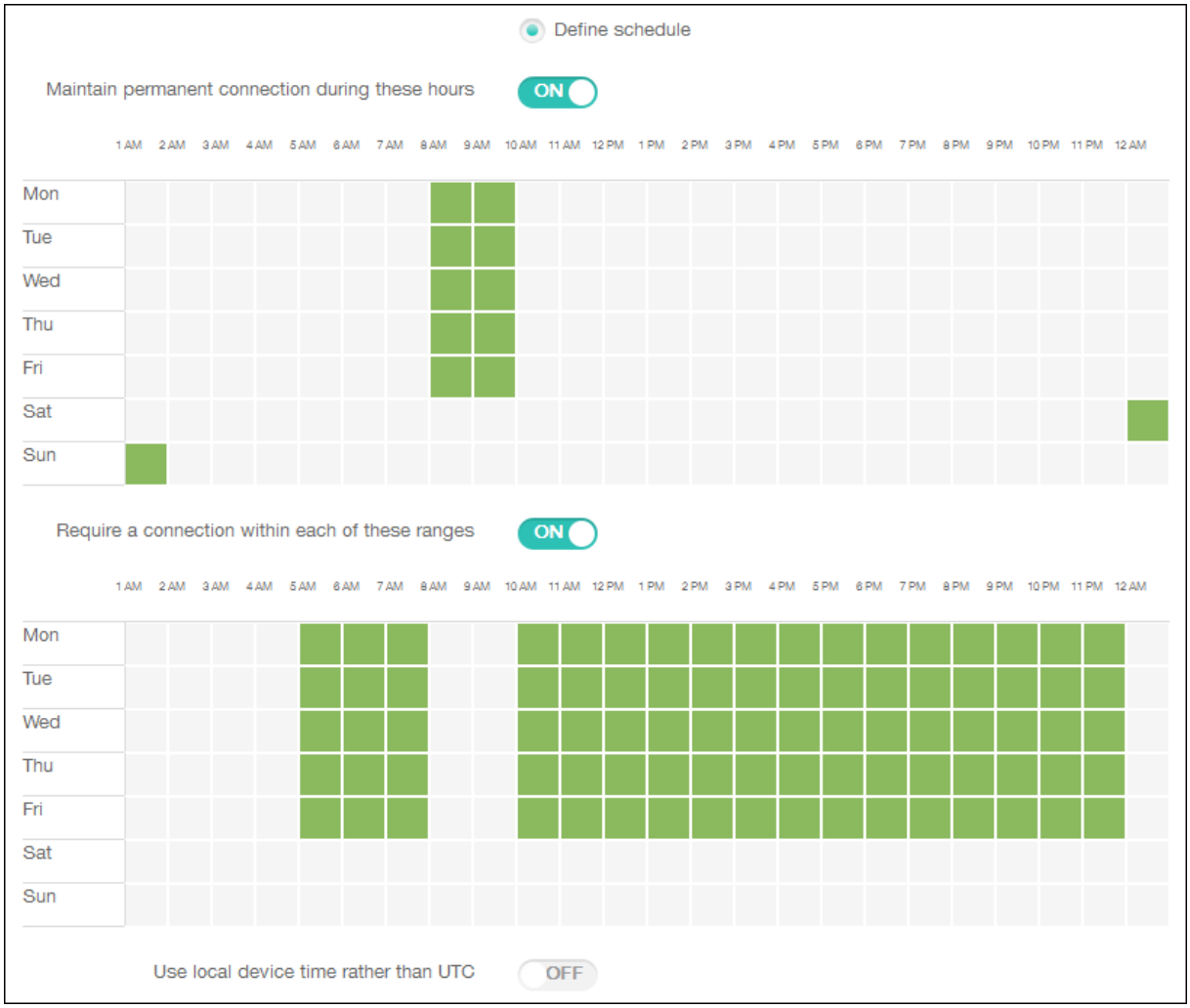
- しない：手動で接続します。ユーザーがデバイス上の Citrix Endpoint Management から接続を開始する必要があります。デバイスにセキュリティポリシーを展開できず、ユーザーは新しいアプリやポリシーを受信しないため、実稼働環境ではこのオプションはお勧めしません。デフォルトでは、［しない］オプションは有効になっています。
- 毎：指定された間隔で接続します。このオプションが有効な状態でロックやワイプなどのセキュリティポリシーを送信すると、この操作は次回デバイスが接続されたときに処理されます。このオプションを選択すると、［**N** 分ごとに接続］フィールドが表示されます。このフィールドに、デバイスが再接続されるまでの分数を入力する必要があります。デフォルトは最小値の **120** です。
- スケジュールを定義：ユーザーデバイス上の Citrix Endpoint Management は、ネットワーク接続が失われると Citrix Endpoint Management サーバーへの再接続を試行します。また、指定した期間にわたり、一定の間隔でコントロールパケットを送信することで接続を監視します。接続期間の定義方法については、「接続期間の定義」を参照してください。
  - これらの各範囲内で接続を要求：定義した期間内に 1 回以上、ユーザーのデバイスが接続される必要があります。
  - **UTC** ではなくローカルデバイスの時間を使用：定義した期間を、UTC（Coordinated Universal Time：協定世界時）ではなくローカルデバイスの時間に同期させます。

接続期間の定義

以下のオプションを有効にすると時間軸が表示されます。これを使用して必要な期間を定義できます。特定の時間内に永続的な接続を必要とするオプション、または特定の期間内に 1 回の接続を必要とするオプションのいずれか、またはその両方を有効にできます。時間軸の 1 つの四角が 1 時間に相当します。平日の午前 8:00～午前 9:00 に接続を指定する場合は、時間軸で平日の［午前 8 時］と［午前 9 時］の間にある四角をクリックします。

たとえば、以下の接続が必要な場合は、次の図のように 2 種類の時間軸を指定します：

- 平日午前 8 時から午前 10 時までの永続的な接続
- 土曜日の午前 1 時から日曜日の午前 2 時までの永続的な接続
- 平日の午前 5 時から午前 8 時までまたは午前 10 時から午前 0 時までの少なくとも 1 回の接続



連絡先（**CardDAV**）デバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、iOS 連絡先（CardDAV）アカウントをユーザーの iOS デバイスまたは macOS デバイスに追加し、CardDAV をサポートするサーバーとそのデバイスの連絡先データを同期することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明：アカウントの説明を入力します。このフィールドは必須です。

- ホスト名： CardDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート： CardDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**：ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名：ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード：任意で、ユーザーのパスワードを入力します。
- **SSL** を使用： CardDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

macOS 設定

- アカウントの説明：アカウントの説明を入力します。このフィールドは必須です。
- ホスト名： CardDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート： CardDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**：ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名：ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード：任意で、ユーザーのパスワードを入力します。
- **SSL** を使用： CardDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します

- プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

カスタム **XML** デバイスポリシー

November 29, 2023

Citrix Endpoint Management でカスタム XML ポリシーを作成して、サポートされる Windows デバイスの次の機能をカスタマイズできます：

- プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。
- デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。
- ソフトウェアのアップグレード。アプリやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。
- 障害管理。デバイスからのエラーおよび状態レポートの受信などです。

> 注：
>
> XML コンテンツを作成するときは、% 文字の使用に注意してください。% 文字は XML の予約文字であり、XML 特殊文字をエスケープするためにのみ使用されます名前で% を使用するには、「%25」としてエンコードします。

Windows デバイスの場合、Windows で Open Mobile Alliance Device Management（OMA DM）API を使用して、カスタム XML 構成を作成します。OMA DM API を使用したカスタム XML の作成については、このトピックでは扱いません。OMA DM API の使用について詳しくは、Microsoft Developer Network サイトの「OMA DM プロトコルのサポート」を参照してください。

Android Enterprise デバイスの場合、MX Management System（MXMS）を使用してカスタム XML 構成を作成します。MXMS API を使用したカスタム XML の作成については、この記事では扱いません。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップ/タブレットの設定

XML コンテンツ：ポリシーに追加するカスタム XML コードを入力するか、コピーして貼り付けます。

［次へ］をクリックすると、Citrix Endpoint Management で XML コンテンツの構文がチェックされます。構文エラーがある場合、コンテンツボックスの下に表示されます。続行するにはエラーを修正してください。

構文エラーがない場合は、［**Custom XML Policy**］割り当てページが開きます。

Windows AutoPilot を使用してデバイスをセットアップおよび構成する

Windows AutoPilot は、新しいデバイスのセットアップと事前設定に使用されるテクノロジの集まりで、生産性の高い使用を可能にします。Windows AutoPilot では、デバイスのリセット、用途変更、および復元を行うことができます。AutoPilot では、最新のオペレーティングシステムの展開作業を簡単に行えるようになります。AutoPilot を使用すると、こうした作業を単純な設定と操作にまとめ、デバイスの使用準備を素早く効率的に行うことができます。

Citrix Endpoint Management での Windows AutoPilot の使用の概要については、このビデオをご覧ください。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

前提条件

- Azure Active Directory ポータルで会社のブランド設定を構成している。
- 会社が Azure Active Directory の Premium P1 または P2 サブスクリプションを所有している。
- Azure Active Directory を Citrix Endpoint Management の ID プロバイダータイプとして構成している。Citrix Endpoint Management コンソールで、[設定] **>** [**ID** プロバイダー（**IDP**）] に移動して構成します。
- Windows AutoPilot で使用するクラウドサービスにネットワークで接続できる。
- デバイスに Windows 10 Professional、Enterprise、または Education（バージョン 1703 以降）、または Windows 11 Professional、Enterprise、または Education がプリインストールされている。
- デバイスがインターネットにアクセスできる。

前提条件の構成について詳しくは、AutoPilot の Microsoft Windows ドキュメントを参照してください: https://docs.microsoft.com

AutoPilot デバイス用に **Citrix Endpoint Management** で **Windows** の自動再展開を構成するには

1. カスタム XML デバイスポリシーで、手順に従ってカスタム XML ポリシーを追加します。[**XML** コンテンツ] に以下を追加します。

```
<Add>
<CmdID>\_cmdid\_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
<Data>0</Data>
</Item>
</Add>
```



```
13
14  <!--NeedCopy-->
```

2. Windows のロック画面で、**CTRL+Windows** キー **+R** を押します。
3. Azure Active Directory アカウントでログインします。
4. デバイスにより、ユーザーにデバイスの再展開を行う権限があるか確認されます。その後、デバイスの再展開が行われます。
5. AutoPilot の構成でデバイスが更新されると、ユーザーは新しく構成されたデバイスにログインできるようになります。

Windows 11 デバイスに単一アプリのキオスクを展開する

> 注:
>
> Windows 11 デバイスは、単一アプリのキオスクモードのみをサポートします。

[**XML** コンテンツ] テキストボックスで、次の XML スクリプトをコピーして貼り付けてから、設定で次の文字列に置き換えます。

- `your_username_here`（2 つのインスタンス）: デバイスで作成するユーザー名。両方のインスタンスで同じ設定を維持します。
- `your password_here`: ユーザーのパスワード。
- `your_UWP_app_id_here`: デバイスに展開する UMP アプリの AUMID。

XML スクリプト:

```
1  <Add>
2      <CmdID>\_cmdid\_</CmdID>
3      <Item>
4          <Target>
5              <LocURI>./Device/Vendor/MSFT/Accounts/Users/
                   your_username_here/Password</LocURI>
6          </Target>
7          <Meta>
8              <Format xmlns="syncml:metinf">chr</Format>
9          </Meta>
10         <Data>your_password_here</Data>
11     </Item>
12 </Add>
13 <Replace>
14     <CmdID>\_cmdid\_</CmdID>
15     <Item>
16         <Target>
17             <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
                   LocURI>
18         </Target>
19         <Meta>
```



```
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
            config">
            <Profiles>
                <Profile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"
                        />
                </Profile>
            </Profiles>
            <Configs>
                <Config>
                    <Account>your_username_here</Account>
                    <DefaultProfile Id="{
AFF9DA33-AE89-4039-B646-3A5706E92957 }
"/>
                </Config>
            </Configs>
        </AssignedAccessConfiguration>]]></Data>
    </Item>
</Replace>
<!--NeedCopy-->
```

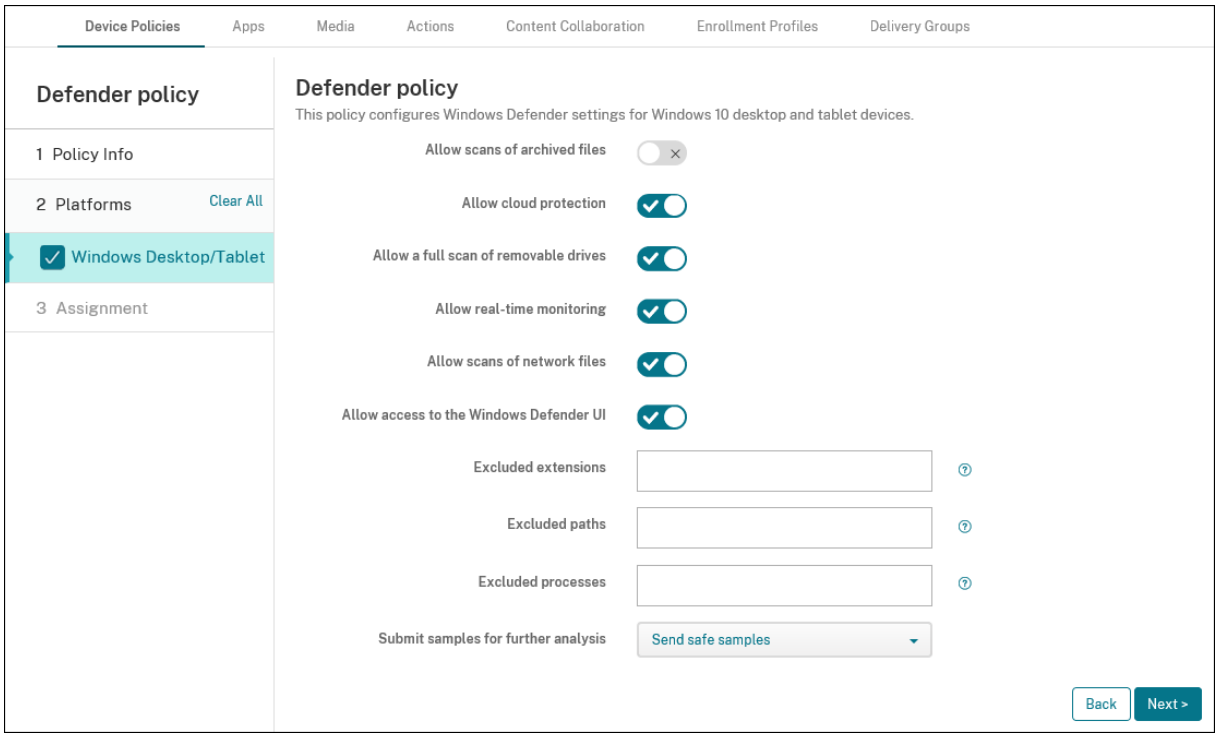
Defender デバイスポリシー

November 29, 2023

Windows Defender は、Windows 10 および Windows 11 に搭載されたマルウェア対策ソフトです。Citrix Endpoint Management デバイスポリシー［Defender］を使用して、Windows 10 および Windows 11 のデスクトップおよびタブレットデバイスの Microsoft Defender ポリシーを構成できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップとタブレットの設定



- アーカイブ済みファイルのスキャンを許可する： Defender がアーカイブファイルをスキャンすることを許可または禁止します。デフォルトは、［オフ］です。
- クラウド保護を許可する： Defender がマルウェアの活動について Microsoft に情報を送信することを許可または禁止します。デフォルトは、［オン］です。
- リムーバブルドライブのスキャンを許可する： Defender が USB スティックなどのリムーバブルドライブをスキャンすることを許可または禁止します。デフォルトは、［オン］です。
- リアルタイム監視を許可する：デフォルトは ［オン］です。
- ネットワークファイルのスキャンを許可する： Defender がネットワークファイルをスキャンすることを許可または禁止します。デフォルトは、［オン］です。
- **Windows Defender** の **UI** へのアクセスを許可する：ユーザーが Windows Defender ユーザーインターフェイスにアクセスできるかどうかを指定します。この設定は、次にユーザーデバイスが起動するときに有効になります。この設定が ［オフ］の場合、ユーザーは Windows Defender の通知を受け取りません。デフォルトは、［オン］です。
- 除外された拡張子：リアルタイムまたは定時スキャンから除外する拡張子。拡張子を区切るには、|文字を使用します。例：`lib\|obj`。
- 除外されたパス：リアルタイムまたは定時スキャンから除外するパス。パスを区切るには、|文字を使用します。例：`C:\Example|C:\Example1`。
- 除外された処理：リアルタイムまたは定時スキャンから除外する処理。処理を区切るには、|文字を使用します。例：`C:\Example.exe|C:\Example1.exe`。
- 詳細な分析のためにサンプルを提出する：悪意があるかどうかを判断するために、さらに分析が必要なファイ

ルを Microsoft に送信するかどうかを制御します。オプション：［常に確認する］、［安全なサンプルを送信する］、［送信しない］、［すべてのサンプルを送信する］。デフォルトは、［安全なサンプルを送信する］です。

Device Guard デバイスポリシー

November 29, 2023

Device Guard は、Windows 10 および Windows 11 で使用できるセキュリティ機能です。この機能は、Windows Hypervisor を使用してデバイス上のセキュリティサービスをサポートすることにより、仮想化ベースのセキュリティを実現します。Device Guard ポリシーは、セキュアブート、UEFI ロック、仮想化などのセキュリティ機能を有効にします。

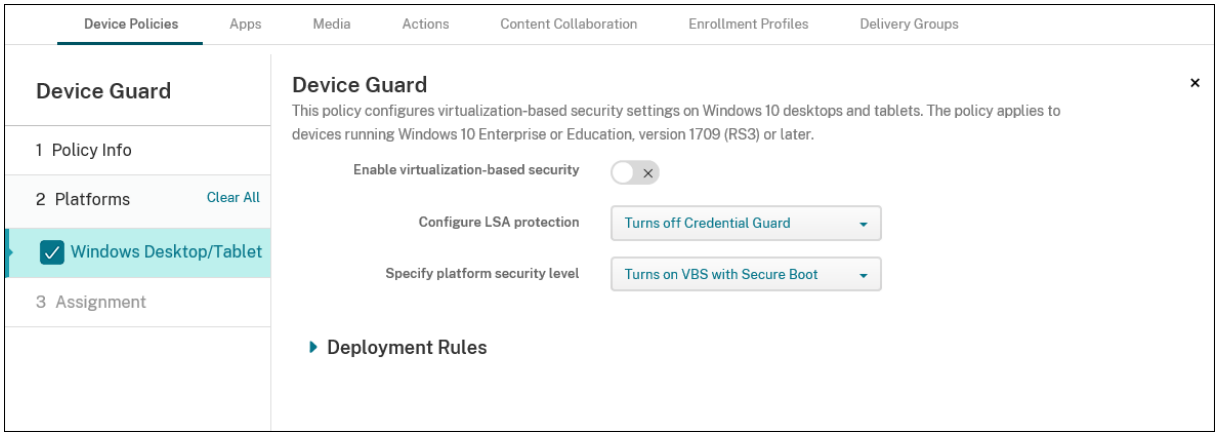
前提条件

- Enterprise ライセンスまたは Education ライセンスが設定された Windows 10 および Windows 11 デスクトップおよびタブレット
- Windows で Device Guard が有効になっている

  Device Guard について詳しくは、「https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップとタブレットの設定



- 仮想化ベースのセキュリティを有効にする：仮想化ベースのセキュリティ機能を無効または有効にします。仮想化ベースのセキュリティは、Windows Hypervisor を使用してセキュリティサービスをサポートします。

- **LSA** 保護を構成する： Credential Guard を構成できます。この設定により、ユーザーは仮想化ベースのセキュリティ機能を備えた Credential Guard を有効にして、次回再起動時に資格情報を保護することができます。オプションは、［**Credential Guard** を無効にする］、［**UEFI** ロックありで **Credential Guard** を有効にする］、［**UEFI** ロックなしで **Credential Guard** を有効にする］です。デフォルトは ［**Credential Guard** を無効にする］です。
- プラットフォームのセキュリティレベルを指定する：次回の再起動時のプラットフォームのセキュリティレベルを指定できます。オプションは ［セキュアブートで **VBS** を有効にする］、［セキュアブートと直接メモリアクセスで **VBS** を有効にする］です。デフォルトは ［セキュアブートで **VBS** を有効にする］です。

Citrix Endpoint Management はデバイスにクエリを行い、仮想化ベースのセキュリティ設定がサーバーの設定と一致するかどうかを判定します。セキュリティ設定が一致する場合、Citrix Endpoint Management はこのポリシーをデバイスに展開しません。セキュリティ設定が一致しない場合、Citrix Endpoint Management はポリシーを展開します。

デバイス正常性構成証明デバイスポリシー

November 29, 2023

Citrix Endpoint Management では、Windows 10 および Windows 11 デバイスに正常性状態の報告を義務付けることができます。この報告では、デバイスは分析目的で特定のデータおよびランタイム情報を Health Attestation Service（HAS）に送信します。HAS は、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスから Citrix Endpoint Management に送信されます。Citrix Endpoint Management は正常性構成証明書の内容に基づいて、設定済みの自動アクションを展開します。

HAS によって検証されるデータは以下のとおりです。

- AIK の有無
- BitLocker の状態
- ブートデバッグが有効化されているかどうか
- ブートマネージャー Rev リストバージョン
- コードの整合性チェックが有効化されているかどうか
- コードの整合性 Rev リストバージョン
- Apple Deployment Program ポリシー
- ELAM ドライバーが起動されているかどうか
- 発行時刻
- カーネルのデバッグが有効化されているかどうか
- PCR
- リセット回数
- 再起動回数
- セーフモードが有効化されているかどうか

- SBCP ハッシュ
- セキュアブートが有効化されているかどうか
- テスト署名が有効化されているかどうか
- VSM が有効であること。
- WinPE が有効であること。

詳しくは、Microsoft 社の「Device HealthAttestation CSP」ページを参照してください。

DHA は、次のように Microsoft Cloud またはオンプレミスの Windows DHA サーバーを使用して構成できます:

- Microsoft Cloud を使用して DHA を構成する: デバイス正常性構成証明ポリシーを追加し、この記事の説明に従って構成します。
- オンプレミスの Windows DHA サーバーを使用して DHA を構成する: DHA サーバーを構成します。その後、デバイス正常性構成証明ポリシーを追加し、この記事の説明に従って構成します。

  DHA サーバーを構成するには、Windows Server 2016 Technical Preview 5 以降を実行するマシンで DHA サーバーの役割をインストールします。手順については、「オンプレミスのデバイス正常性構成証明サービス (DHA) の構成」を参照してください。

このポリシーを追加または構成するには、[構成] **>** [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップ/タブレットの設定

Microsoft Cloud を使用して **DHA** を構成する場合

- デバイス正常性構成証明を有効にする: デバイス正常性構成証明を必須とするかどうかを選択します。デフォルトは [オフ] です。

オンプレミスの **Windows DHA** サーバーを使用して **DHA** を構成する場合

- デバイス正常性構成証明を有効にする: [オン] にします。
- 社内のデバイス正常性構成証明サービス (**DHA**) の構成: [オン] にします。
- 社内の **DHA** サービスの **FQDN**: セットアップした DHA サーバーの完全修飾ドメイン名を入力します。
- 社内の **DHA** の **API** バージョン: DHA サーバーにインストールする DHA サービスのバージョンを選択します。

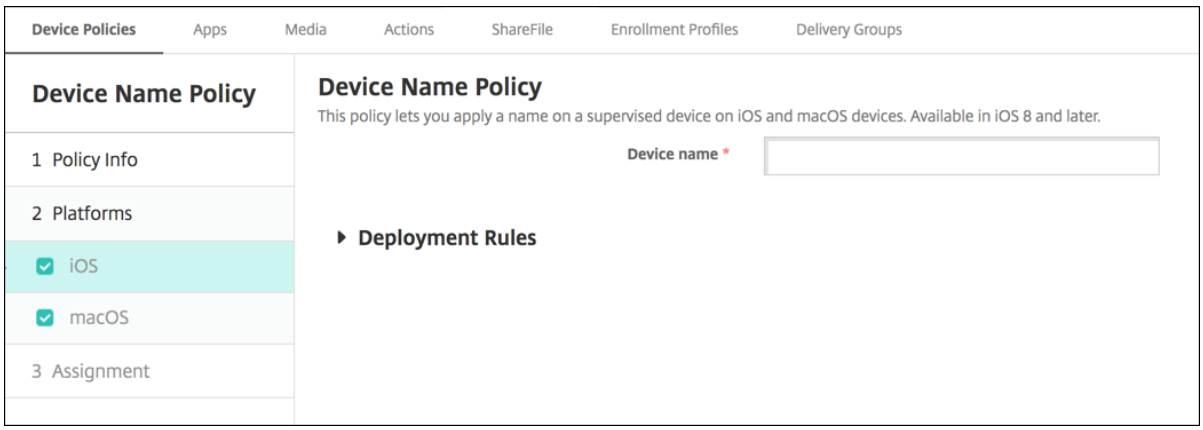
デバイス名デバイスポリシー

November 29, 2023

デバイスを特定しやすくするために、監視対象 iOS デバイスおよび macOS デバイスに名前を設定できます。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。たとえば、デバイス名をデバイスのシリアル番号として設定するには、${device.serialnumber} を使用します。デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.com を使用します。マクロについて詳しくは、「Citrix Endpoint Management のマクロ」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **macOS** の設定



- デバイス名：マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。たとえば、デバイス名を各デバイスのシリアル番号に設定するには、${device.serialnumber} を使用します。デバイス名にユーザーの Apple ID を含めるには、${device.serialnumber} ${ user.username} を使用します。

Education の構成デバイスポリシー

November 29, 2023

Education の構成デバイスポリシーでは、以下について定義します：

- 講師用デバイスの Apple クラスルームアプリの設定。
- 講師用デバイスと生徒用デバイス間でクライアント認証を実行するために使用する証明書。

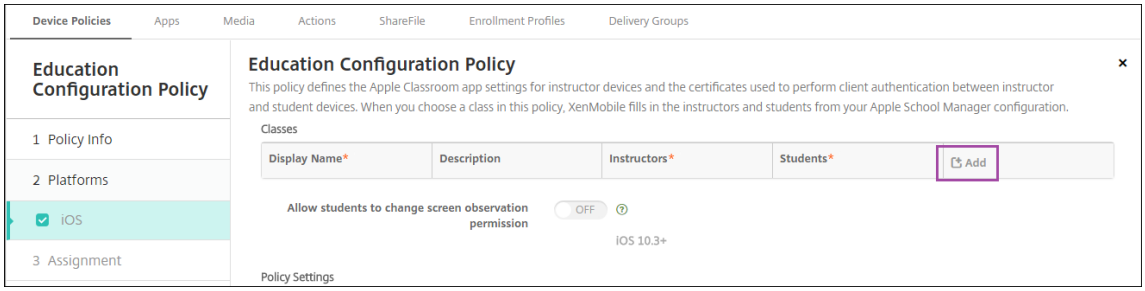
［教育の構成］デバイスポリシーは iOS（iPadOS）デバイスでサポートされています。

このポリシーでクラスを選択すると、Citrix Endpoint Management コンソールで Apple School Manager の構成から講師と生徒が記入されます。このポリシーの Apple クラスルームアプリの設定がすべてのクラスで同じ場合は、ポリシーを 1 つ作成します。

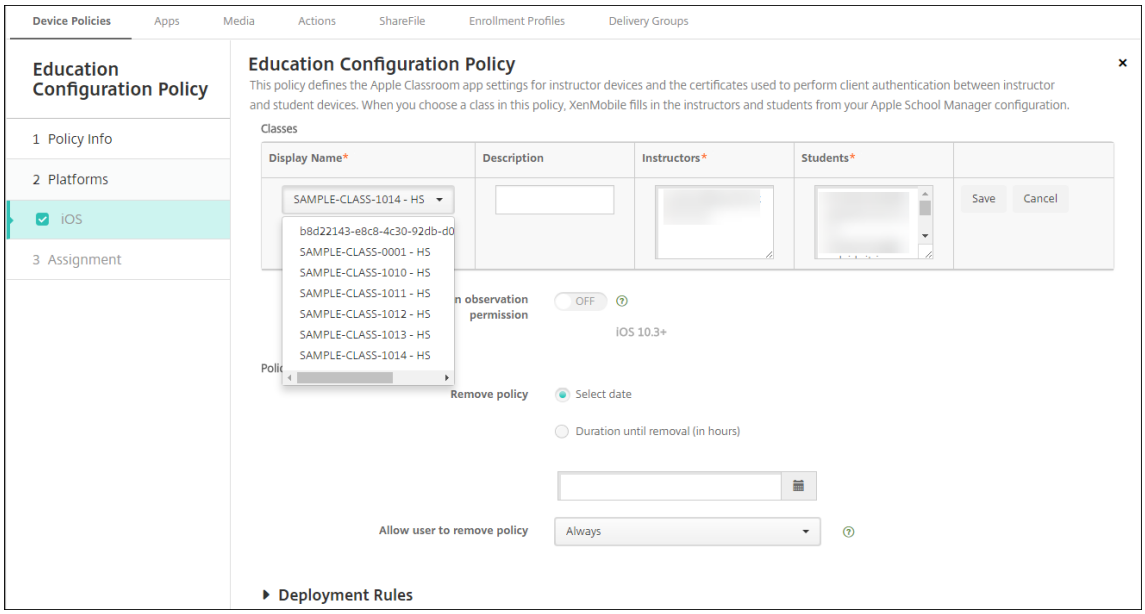
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

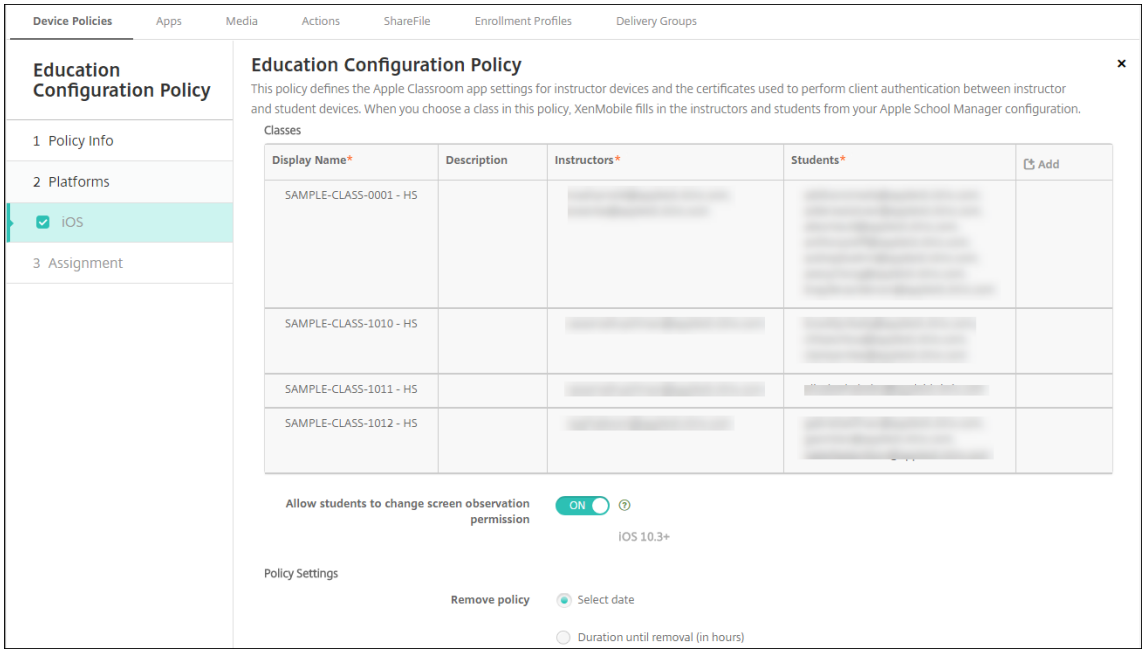
- クラス：クラスを追加するには、［追加］をクリックします。



次に、［表示名］一覧をクリックします。接続した Apple School Manager アカウントから取得したクラスの一覧が表示されます。



［表示名］からクラスを選択すると、Citrix Endpoint Management によって講師と生徒が入力されます。引き続きクラスを追加します。

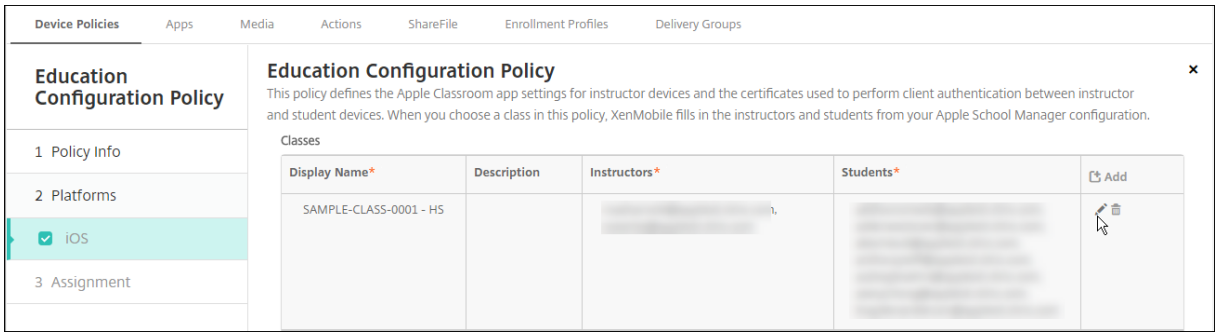


- 生徒に画面監視の権限の変更を許可：［オン］の場合、管理対象クラスに登録された生徒は、使用デバイスの画面の監視を講師に許可するかどうかを選択できます。デフォルトは ［オフ］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

ポリシーのクラス情報を編集するには

クラスに説明を加えることができます（クラスルームアプリの「表示名」）。また、講師や生徒を追加したり削除したりすることもできます。Citrix Endpoint Management では、このような変更は Apple School Manager アカウントに保存されません。詳しくは、「Apple の教育向け機能との統合」の「講師、生徒、クラスのデータ管理」を参照してください。

編集するクラスの ［追加］列の上にマウスポインターを置き、鉛筆アイコンをクリックします。



ポリシーからクラスを削除するには、削除するクラスの ［追加］列の上にマウスポインタを置き、ごみ箱アイコンをクリックします。

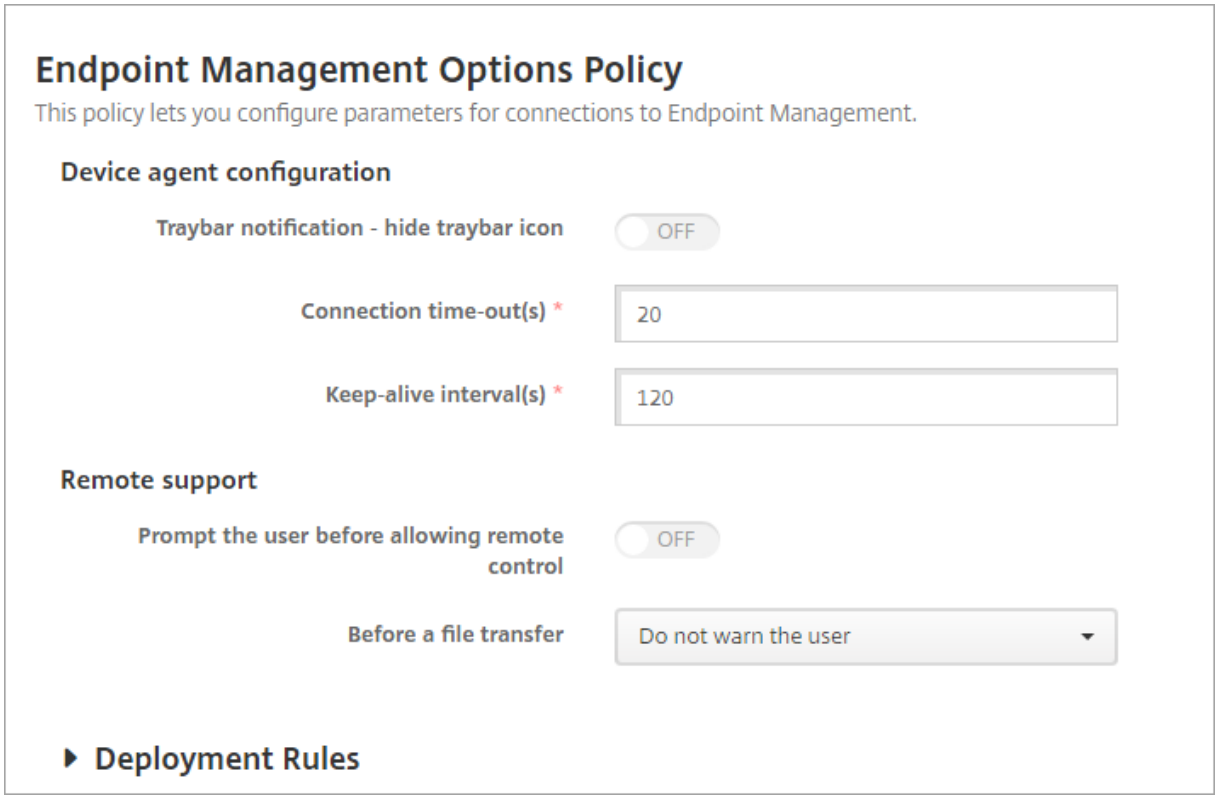
Endpoint Management オプションデバイスポリシー

March 15, 2024

Citrix Endpoint Management オプションポリシーを追加すると、Android デバイスから Citrix Endpoint Management に接続するときの Citrix Secure Hub の動作を構成できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

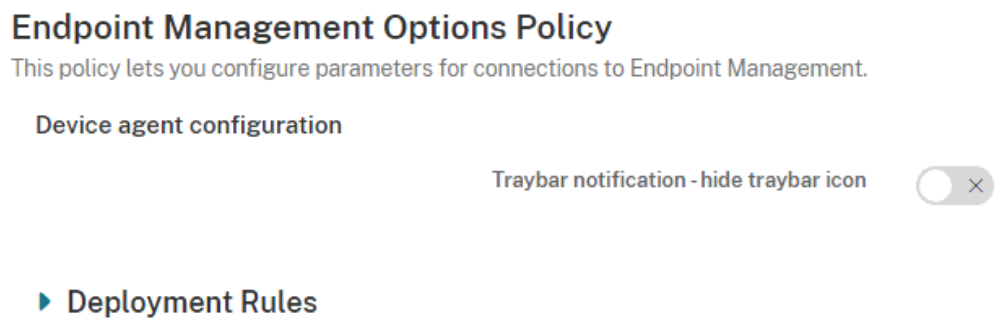
Android の設定



- トレイバー通知-トレイバーアイコンを隠す：トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは ［オフ］です。
- 接続タイムアウト：接続のアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、接続はタイムアウトになります。デフォルトは 20 秒です。
- **Keep-alive** 間隔：接続を開いたままにする時間（秒）を入力します。デフォルトは 120 秒です。

- リモート制御を許可する前にユーザーに確認メッセージを表示：リモートサポートの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは ［オフ］です。
- ファイル転送の前：一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。使用可能な値は、［ユーザーに警告しない］、［ユーザーに警告］、および ［ユーザーの許可を求める］です。デフォルトは ［ユーザーに警告しない］です。

Android Enterprise の設定



Android バージョン 7 以降でサポートされています。

トレイバー通知-トレイバーアイコンを隠す：トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは ［オフ］です。

> 注：
>
> Android Enterprise 上で動作するデバイスの VPN サービスを有効にする場合は、**VPN** デバイスポリシーの ［［常時 **VPN** に接続］を有効にする］オプションを有効にできます。以前のリリースの **Endpoint Management** オプションデバイスポリシーで ［[常時 **VPN** に接続］を有効にする］オプションを既に有効にしている場合は、**VPN** デバイスポリシーでも同じオプションを再度有効にしてください。

Citrix Endpoint Management アンインストールデバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、Citrix Endpoint Management を Android デバイスからアンインストールすることができます。このポリシーを展開すると、展開グループ内のすべてのデバイスから Citrix Endpoint Management が削除されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android の設定

- **Citrix Endpoint Management** をデバイスからアンインストール：このポリシーを展開するすべてのデバイスから Citrix Endpoint Management をアンインストールするかどうかを選択します。デフォルトは［オフ］です。

Exchange デバイスポリシー

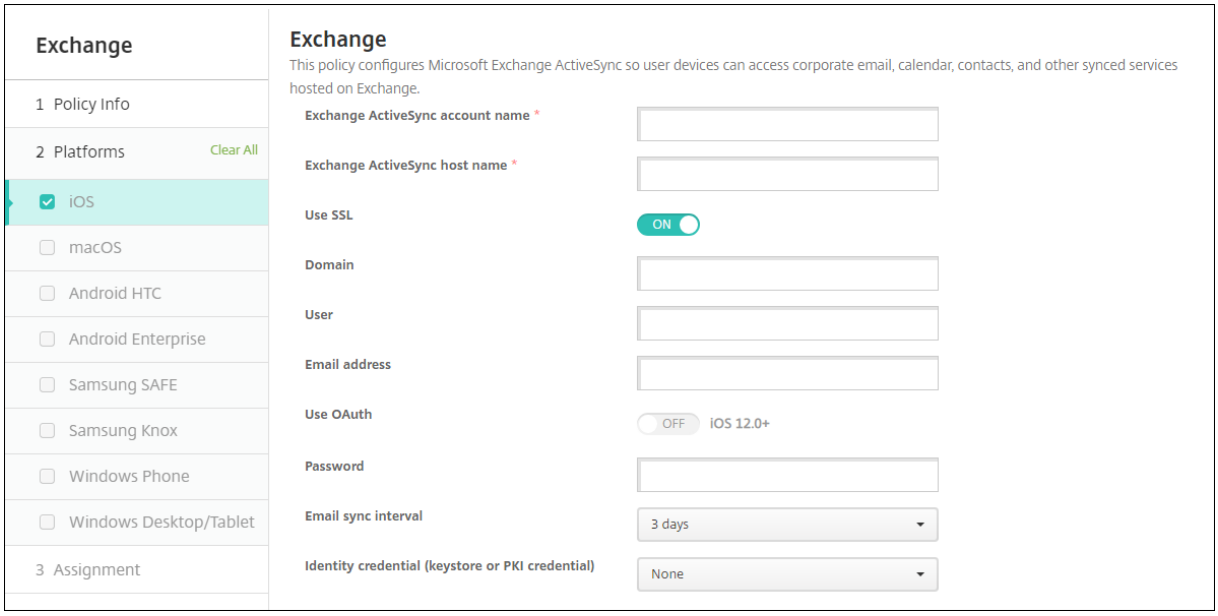
March 15, 2024

Exchange ActiveSync デバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchange でホストされている会社のメールにアクセスできるようにすることができます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、以下のセクションで説明しています。

このポリシーを作成するには、Exchange Server のホスト名または IP アドレスが必要です。ActiveSync の設定について詳しくは、Microsoft 社の記事「ActiveSync CSP」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **Exchange ActiveSync** のアカウント名：ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **Exchange ActiveSync** のホスト名：メールサーバーのアドレスを入力します。
- **SSL** を使用：ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］です。
- ドメイン： Exchange Server があるドメインを入力します。このフィールドでシステムマクロ`$user.domainname`を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ`$user.username`を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス：完全なメールアドレスを指定します。このフィールドでシステムマクロ`$user.mail`を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **OAuth** を使用：［オン］に設定すると、接続の認証で OAuth が使用されます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
- パスワード：任意で、Exchange ユーザーアカウントのパスワードを入力します。この設定は、[**OAuth** を使用］が ［オン］の場合には表示されません。
- メールの同期間隔：一覧から、メールを Exchange Server と同期する頻度を選択します。デフォルトは ［**3** 日］です。
- **ID** 資格情報（キーストアまたは **PKI**）： Citrix Endpoint Management の ID プロバイダーを構成している場合、オプションとして、ボックスの一覧で ID 資格情報を選択します。このフィールドは、Exchange でクライアント証明書認証が必要な場合にのみ必要です。デフォルトは ［なし］です。
- アカウント間でのメールの移動を承認：ユーザーに以下の実行を許可するかを指定します：
  - このアカウントから別のアカウントにメールを移動する
  - 別のアカウントからメールを転送する
  - 別のアカウントから返信する

  デフォルトは ［オフ］です。
- メールアプリからのみメールを送信：ユーザーのメール送信を iOS メールアプリからのみに制限するかどうかを選択します。デフォルトは ［オフ］です。
- ユーザーが最近使用したアドレスを同期できないようにする：ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは ［オフ］です。
- メールドロップを許可：アカウントにメールドロップの使用を許可するかどうかを選択します。デフォルトは［オフ］です。
- **S/MIME** 署名の有効化：アカウントで S/MIME 署名をサポートするかどうかを指定します。デフォルトは［オン］です。［オン］に設定した場合、以下の 2 つのフィールドが表示されます：

  - 署名 **ID** 資格情報：使用する署名資格情報を選択します。
  - **S/MIME** 署名のユーザー上書き可能：［オン］に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
  - **S/MIME** 署名証明書 **UUID** のユーザー上書き可能：［オン］に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。

- **S/MIME** 暗号化の有効化：このアカウントで S/MIME 暗号化をサポートするかどうかを選択します。デフォルトは ［オフ］です。［オン］に設定した場合、以下の 2 つのフィールドが表示されます：

  - 暗号化 **ID** 資格情報：使用する暗号化資格情報を選択します。
  - メッセージごとの **S/MIME** 切り替えの有効化：［オン］に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］です。
  - **S/MIME** 暗号化のユーザー上書き可能：［オン］に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
  - **S/MIME** 暗号化証明書 **UUID** のユーザー上書き可能：［オン］に設定した場合、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。

- ポリシー設定

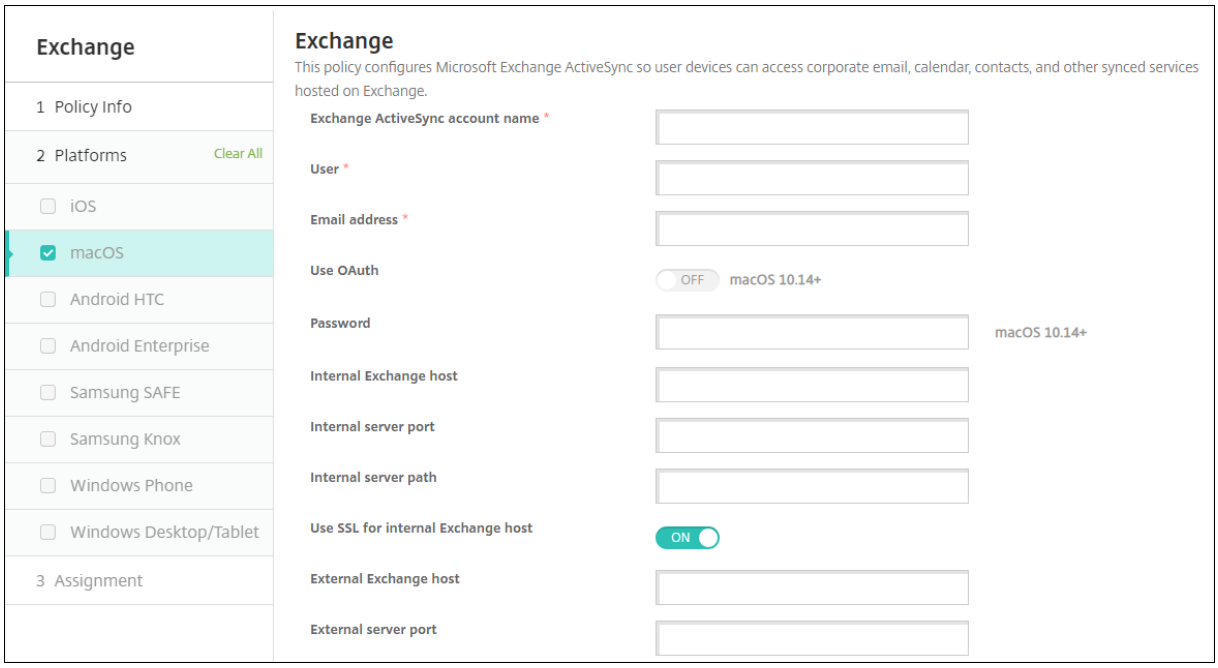
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

同期済み **Exchange** サービス

同期済み Exchange サービスの設定では、次の機能を同期するかを指定できます：

- カレンダー
- 連絡先
- メール
- メモ
- 通知

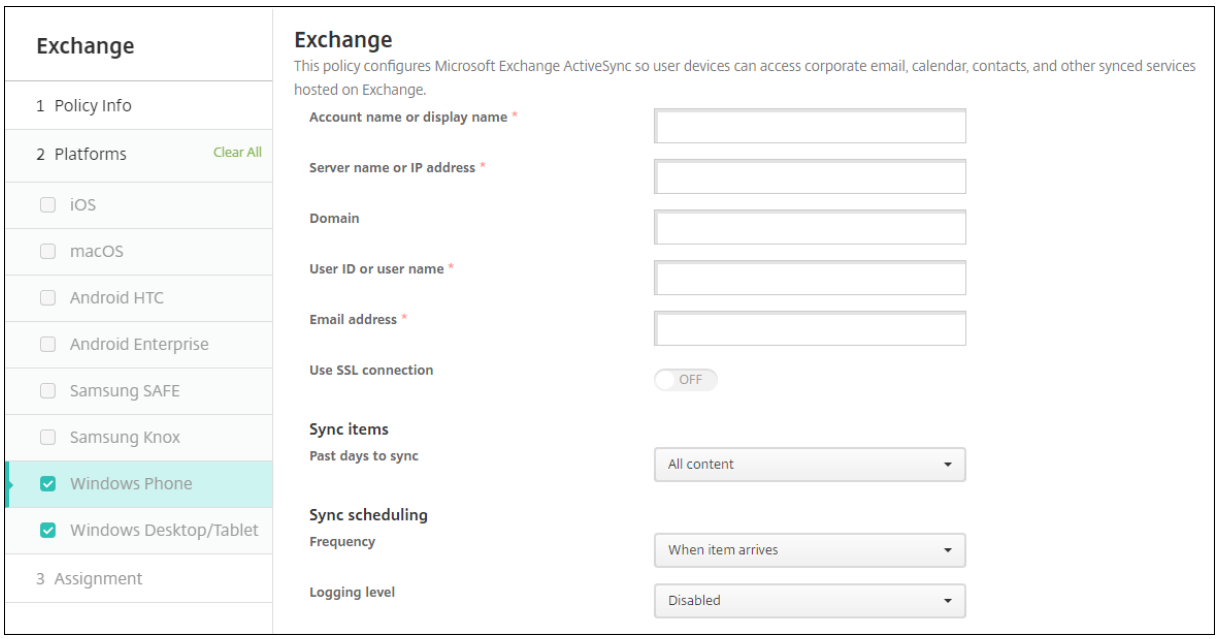
macOS 設定



- **Exchange ActiveSync** のアカウント名：ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- ユーザー： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ`$user.username`を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス：完全なメールアドレスを指定します。このフィールドでシステムマクロ`$user.mail`を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **OAuth** を使用：［オン］に設定すると、接続の認証で OAuth が使用されます。デフォルトは ［オフ］です。このオプションは macOS 10.14 以降に適用されます。
- **OAuth** サインイン **URL**： AutoDiscovery サービスを使用しない場合に、OAuth 認証用に Web ビューで読み込むサインイン URL を指定します。このフィールドは、［**OAuth** を使用］を ［オン］に設定すると表示されます。
- パスワード：任意で、Exchange ユーザーアカウントのパスワードを入力します。この設定は、［**OAuth** を使用］が ［オン］の場合には表示されません。
- 内部 **Exchange** ホスト： Exchange のホスト名を内部と外部で別のものにする場合、任意で内部の Exchange ホスト名を入力します。
- 内部サーバーポート： Exchange のサーバーポートを内部と外部で別のものにする場合、任意で内部の Exchange サーバーのポート番号を入力します。
- 内部サーバーパス：Exchange のサーバーパスを内部と外部で別のものにする場合、任意で内部の Exchange サーバーパスを入力します。

- 内部 **Exchange** ホストに **SSL** を使用：ユーザーのデバイスと内部の Exchange ホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］です。
- 外部 **Exchange** ホスト： Exchange のホスト名を内部と外部で別のものにする場合、任意で外部の Exchange ホスト名を入力します。
- 外部サーバーポート： Exchange のサーバーポートを内部と外部で別のものにする場合、任意で外部の Exchange サーバーのポート番号を入力します。
- 外部サーバーパス：Exchange のサーバーパスを内部と外部で別のものにする場合、任意で外部の Exchange サーバーパスを入力します。
- 外部 **Exchange** ホストに **SSL** を使用：ユーザーのデバイスと外部の Exchange ホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］です。
- メールドロップを許可：ユーザーが 2 台の Mac 間で、既存のネットワークに接続することなくワイヤレスでファイルを共有できるようにするかどうかを選択します。デフォルトは ［オフ］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

Windows デスクトップ/タブレットの設定



> 注:
>
> このポリシーを使ってユーザーパスワードを設定することはできません。ユーザーはポリシーがプッシュされた後に、デバイスでパラメーターを設定する必要があります。

- アカウント名または表示名: Exchange ActiveSync アカウント名を入力します。
- サーバー名または **IP** アドレス: Exchange Server のホスト名または IP アドレスを入力します。
- ドメイン: Exchange Server があるドメインを入力します。このフィールドでシステムマクロ`$user.domainname`を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー **ID** またはユーザー名: Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ`$user.username`を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス: 完全なメールアドレスを指定します。このフィールドでシステムマクロ`$user.mail`を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **SSL** 接続を使用: ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは [オフ] です。
- 同期する期間: ボックスの一覧で、デバイス上のすべての内容を Exchange Server と過去にさかのぼって同期する日数を選択します。デフォルトは [すべての内容] です。
- 頻度: ボックスの一覧で、Exchange Server からデバイスへ送信されるデータの同期に使用するスケジュールを選択します。デフォルトは [アイテムを受信したとき] です。
- ログレベル: ボックスの一覧で、[無効]、[基本]、または [詳細] を選択して、Exchange のアクティビティをログ記録する詳細レベルを指定します。デフォルトは [無効] です。

ファイルデバイスポリシー

November 7, 2022

ユーザーが Android および Android Enterprise デバイスでアクセスできるように、ファイルを追加および展開できます。デバイス上でファイルを保存するディレクトリを指定します。たとえば、ユーザーが会社のドキュメントまたは.pdf ファイルを受け取るようにします。ファイルをデバイスに展開し、ファイルの場所をユーザーに知らせます。

Android デバイスは、スクリプトのネイティブ実行をサポートしていません。ユーザーがスクリプトを実行するには、サードパーティのソフトウェアが必要です。

このポリシーで追加できるファイルの種類は次のとおりです:

- テキストベースのファイル（.xml、.html、.py など）
- ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise の設定

- インポートするファイル: インポートするファイルを選択するには、[参照] をクリックしてインポートするファイルの場所へ移動します。
- ターゲットフォルダー: アップロードしたファイルを格納する場所を一覧から選択するか、[新規追加] を選択してファイルの場所を指定します。%Flash Storage%\または%XenMobile Storage%\マクロを選択して、アップロードしたファイルを格納する場所を指定します。マクロは、各デバイスの該当する場所に展開されます。
  - %XenMobile Storage%\は、内部ストレージディレクトリのAndroid/data/com.zenprise/に展開されます。
  - Android 9.0 以前の場合、%Flash Storage%\はファイルを外部ストレージディレクトリに保存します。
  - Android 10.0 以降の場合、%Flash Storage%\はファイルを内部ストレージディレクトリの **Downloads** フォルダーに保存します。
  - Android 11.0 以降の場合、Google がターゲットの場所へのアクセスに制限を課したため、%XenMobile Storage%\は適用されません。
- 保存先ファイル名: 任意です。デバイスに展開する前にファイル名を変更する必要がある場合は、ファイル名を入力します。
- ファイルが存在する場合: 一覧で、既存のファイルをコピーするかどうかを選択します。デフォルトは、[異なる場合にのみファイルをコピーする] です。

> 重要:
>
> ファイルデバイスポリシーは、Android Enterprise でのスクリプトの追加をサポートしなくなりました。既存のポリシーにスクリプトが含まれている場合、ポリシーを選択するとエラーメッセージが表示されます。ポリシーを再度追加することで問題を解決できます。

Android の設定

- インポートするファイル: インポートするファイルを選択するには、[参照] をクリックしてインポートするファイルの場所へ移動します。
- ファイルタイプ: [ファイル] または [スクリプト] を選択します。
- 今すぐに実行: [スクリプト] を選択すると、[今すぐに実行] オプションが表示されます。この設定を有効にしても何も起こりません。ユーザーはスクリプトを手動で実行する必要があります。
- マクロ表現を置換: スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。マクロ構文については、「マクロ」を参照してください。デフォルトは [オフ] です。
- ターゲットフォルダー: アップロードしたファイルを格納する場所を一覧から選択するか、[新規追加] を選択してファイルの場所を指定します。%Flash Storage%\または%XenMobile Storage%\マクロを選択して、アップロードしたファイルを格納する場所を指定します。マクロは、各デバイスの該当する場所に展開されます。
  - %XenMobile Storage%\は、内部ストレージディレクトリのAndroid/data/com.zenprise/に展開されます。
  - Android 9.0 以前の場合、%Flash Storage%\はファイルを外部ストレージディレクトリに保存します。
  - Android 10.0 以降の場合、%Flash Storage%\はファイルを内部ストレージディレクトリの **Downloads** フォルダーに保存します。
  - Android 11.0 以降の場合、Google がターゲットの場所へのアクセスに制限を課したため、%XenMobile Storage%\は適用されません。
- 保存先ファイル名: 任意です。デバイスに展開する前にファイル名を変更する必要がある場合は、ファイル名を入力します。
- ファイルが存在する場合: 一覧で、既存のファイルをコピーするかどうかを選択します。デフォルトは、[異なる場合にのみファイルをコピーする] です。

FileVault デバイスポリシー

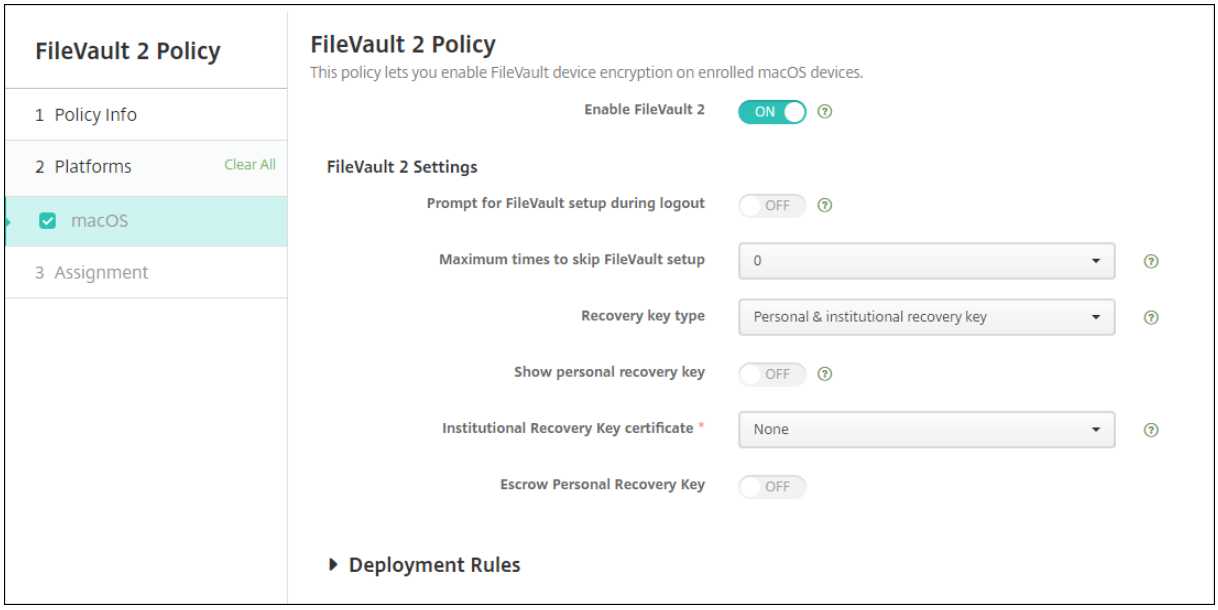
November 29, 2023

macOS の FileVault フルディスク暗号化（FileVault 2）機能を使用すると、コンテンツを暗号化することでシステムボリュームを保護できます。FileVault が有効になっている macOS デバイスでは、デバイスが起動するたびに、ユーザーはアカウントパスワードでログインします。ユーザーがパスワードをなくした場合は、復元キーを使用すると、ディスクのロックを解除してパスワードをリセットできます。

このデバイスポリシーで、FileVault のユーザー設定画面を有効にし、回復キーなどの設定を構成します。FileVault について詳しくは、Apple のサポートサイトを参照してください。

FileVault ポリシーを追加するには、［構成］**>**［デバイスポリシー］の順に選択します。

macOS 設定



- **FileVault** を有効にする：［オン］の場合、［**FileVault** のセットアップをスキップする最大回数］で指定されている次の N 回目のログアウト時に、FileVault を有効にするようユーザーに要求するメッセージが表示されます。［オフ］の場合、ユーザーに FileVault を有効にするメッセージは表示されませんが、FileVault を自身で有効にすることはできます。
- ログオン時に **FileVault** のセットアップを要求：［オン］の場合、ログアウト時に、FileVault を有効にするようユーザーに要求するメッセージが表示されます。
- **FileVault** のセットアップをスキップする最大回数：ユーザーが FileVault のセットアップをスキップできる最大回数。最大回数に達すると、ユーザーはログインするために FileVault を設定する必要があります。**0** の場合、ユーザーは最初のログイン試行時に FileVault を有効にする必要があります。デフォルト値は **0** です。
- 復元キーの種類：ユーザーがパスワードを忘れた場合、復元キーを入力することでディスクのロックを解除し、パスワードをリセットできます。復元キーのオプションは次の通りです。
  - 個人用復元キー：個人用復元キーは、ユーザーに固有のものです。FileVault のセットアップ中に、ユーザーは、復元キーを作成するか iCloud アカウントでディスクのロックを解除するかを選択します。

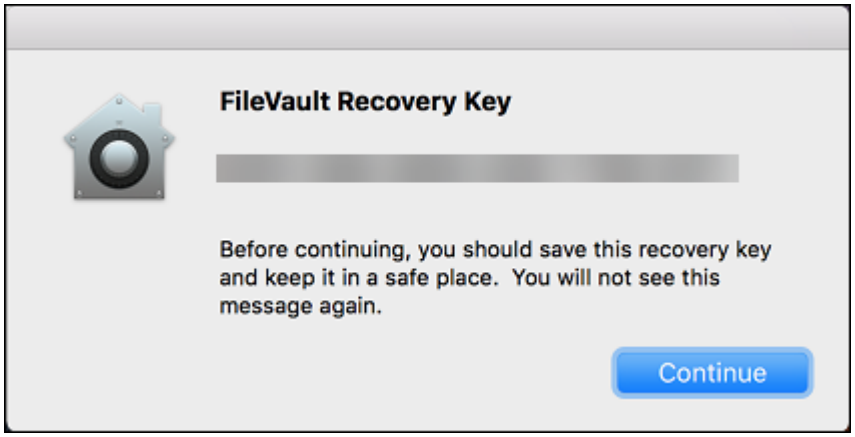
FileVault 設定の完了後にユーザーに復元キーを表示するには、［個人用復元キーの表示］を有効にします。キーを表示することで、ユーザーが今後の使用に備えてキーを記録できます。ユーザーがキーを紛失した場合に検索できるようにするには、［個人用回復キーのエスクロー］を有効にします。

セキュリティ操作により、個人用回復キーを交換することもできます。個人用回復キーの交換について詳しくは、「セキュリティ操作」を参照してください。

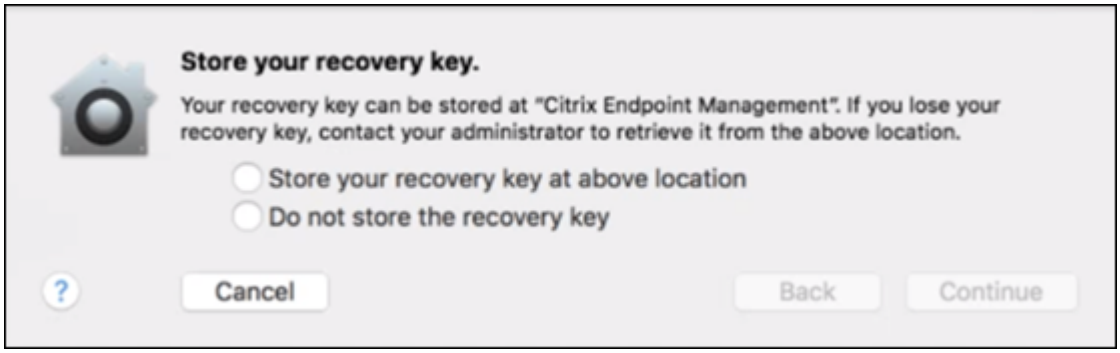
復元キーの管理について詳しくは、Apple のサポートサイトを参照してください。

- 組織用回復キー：組織用（メイン）回復キーと FileVault 証明書を作成できます。これらはユーザーデバイスのロック解除に使用します。詳しくは、Apple のサポートサイトを参照してください。Citrix Endpoint Management を使用して、FileVault 証明書をデバイスに展開します。詳しくは、「証明書および認証」を参照してください。
- 個人用復元キーと組織用復元キー：両方の種類の復元キーを有効にすることで、ユーザーデバイスのロック解除が必要になるのは、ユーザーが個人用復元キーを紛失した場合だけになります。

- 組織用回復キー証明書：回復キーの種類として ［組織用回復キー］または ［個人用回復キーと組織用回復キー］を選択している場合は、そのキーの回復キー証明書を選択します。
- 個人用回復キーの表示：［オン］の場合は、FileVault を設定すると、ユーザーデバイスに個人用回復キーが表示されます。デフォルトは、［オフ］です。

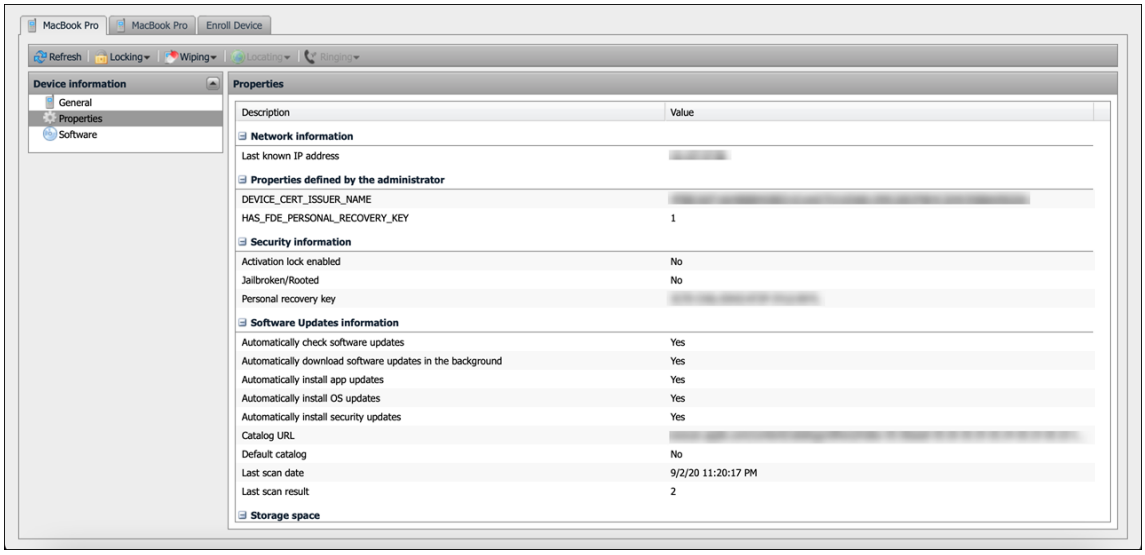


- 個人用回復キーのエスクロー：有効にすると、ユーザーは Citrix Endpoint Management を使用して各デバイスの個人用回復キーのコピーを保存できます。



Citrix Endpoint Management からキーにアクセスするには、[管理] > [デバイス] に移動し、macOS デバイスを選択して [編集] をクリックします。次に、[デバイスの詳細] > [一般] に移動し、[個人用回復キー] を見つけます。

ユーザーが Self Help Portal から回復キーを表示できるようにするには、個人用回復キーのエスクローを有効にし、個人回復キーをユーザーに表示します。キーは、Self Help Portal の [プロパティ] ページにある [セキュリティ情報] の下に表示されます。Self Help Portal について詳しくは、「Self-Help Portal」を参照してください。



[**FileVault** を有効にする] をオンにしていない場合でも、[個人用回復キーのエスクロー] の設定を有効にすることができます。[**FileVault** を有効にする] 設定をオフにしても、ユーザーは自身で FileVault を有効にすることができます。この状況で [個人用回復キーのエスクロー] を有効にすると、ユーザーは Citrix Endpoint Management でキーのコピーを保存できます。

ユーザーがデバイスを Citrix Endpoint Management に登録する前に FileVault を有効にした場合、Citrix Endpoint Management は回復キーを保存しません。デバイスは、コンソールで FileVault が有効になると表示されます。

ファイアウォールデバイスポリシー

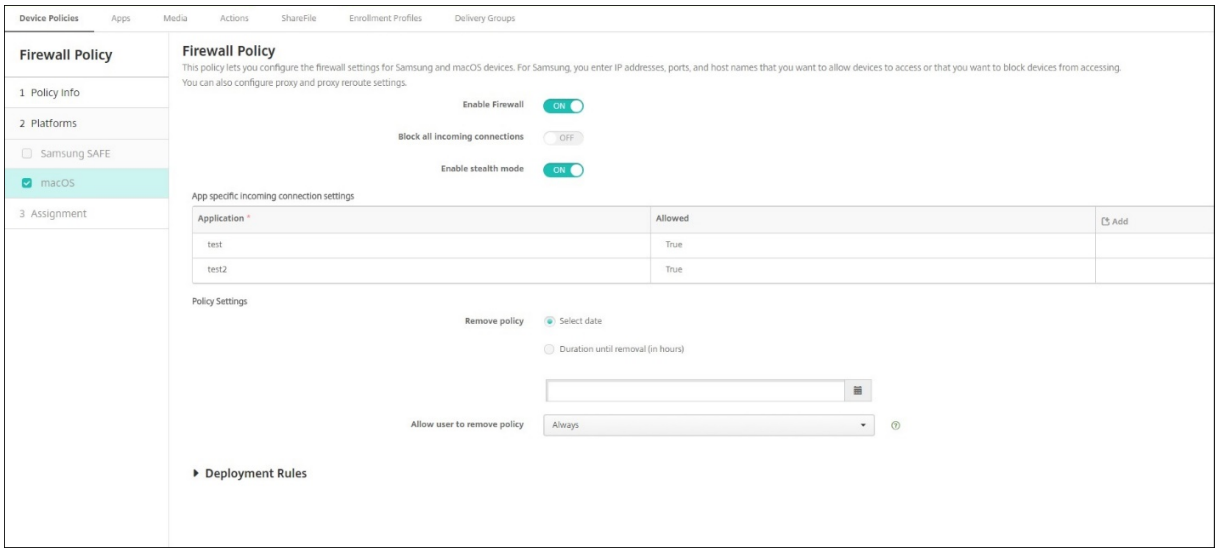
July 7, 2022

このポリシーにより、Samsung、macOS、および Windows デバイスのファイアウォール設定を構成できます。

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

macOS 設定

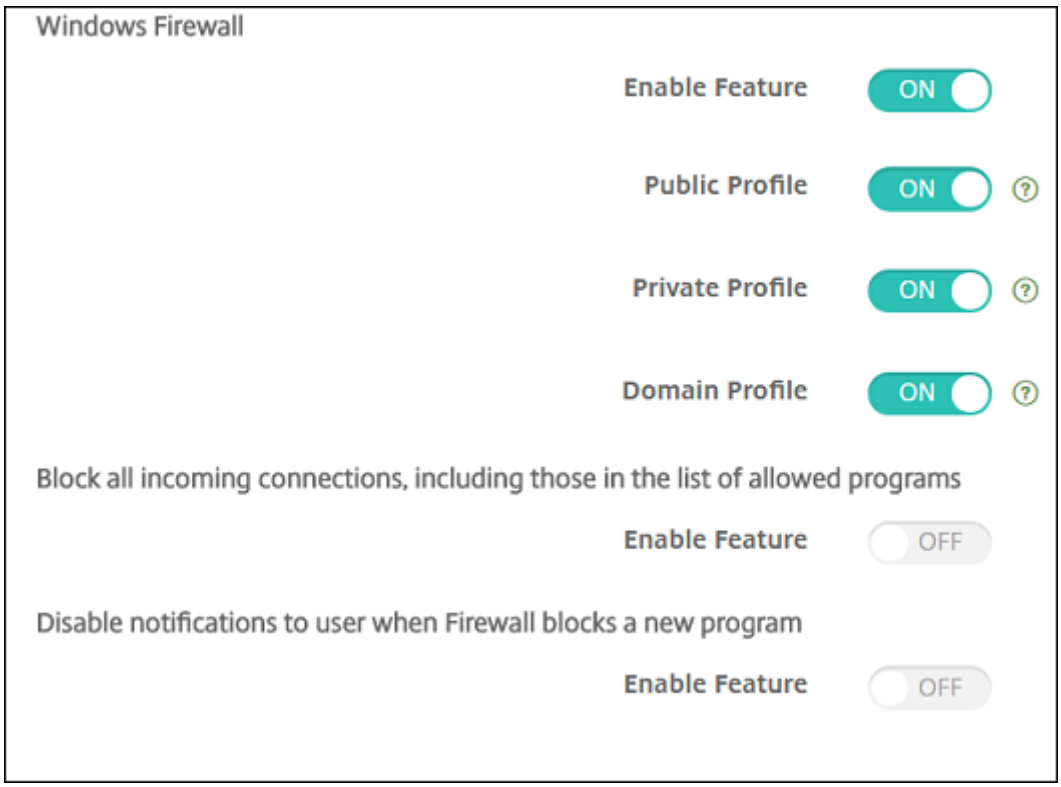
macOS 10.12 以降が必要です。



- ファイアウォールを有効にする。ファイアウォールを有効にするには、このオプションを ［オン］に設定します。
- すべての受信接続をブロックする。このオプションを ［オン］に設定すると、基本サービスに必要な接続以外のすべての受信接続がブロックされます。
- ステルスモードを有効にする。ステルスモードでは、Ping などの ICMP を使用したテストアプリケーションによるネットワークからのアクセスの試みに対して、応答または承認しません。ステルスモードを有効にするには、このオプションを ［オン］に設定します。
- アプリ固有の受信接続設定。特定のアプリで接続を受信できるようにするには、アプリを追加し、［許可］を［はい］に設定します。

Windows デスクトップとタブレットの設定

Windows 10（バージョン 1709 以降）または Windows 11 を実行している Windows デスクトップおよびタブレットデバイスが必要です。



- 機能を有効にする：このポリシーを展開したコンピューターで送受信トラフィックを制御するかどうかを指定します。デフォルトは ［オン］です。
- パブリックプロファイル：コンピューターが公共の場所（空港や喫茶店など）で信頼できないネットワークに接続するときに、Windows ファイアウォールを制御するかどうかを指定します。デフォルトは ［オン］です。
- プライベートプロファイル：コンピューターが信頼できるネットワーク（ホームネットワークなど）に接続するときに、Windows ファイアウォールを制御するかどうかを指定します。デフォルトは ［オン］です。
- ドメインプロファイル：コンピューターがオフィスなどでドメインネットワークに接続するときに、Windows ファイアウォールを制御するかどうかを指定します。デフォルトは ［オン］です。
- 許可されたプログラム一覧にあるものを含むすべての受信接続をブロックする：デフォルトは ［オフ］です。
- ファイアウォールが新しいプログラムをブロックしたときの通知を無効にする：デフォルトは ［オフ］です。

フォントデバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、さらにフォントを iOS デバイスおよび macOS デバイスに追加することができます。フォントは TrueType（`.ttf`）または OpenType（`.oft`）である必要があります。フォントコレクション（`.ttc`または`.otc`）はサポートされません。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポ

リシー」を参照してください。

iOS の設定

- ユーザーに表示される名前：ユーザーのフォント一覧に表示される名前を入力します。
- フォントファイル：フォントファイルを選択してユーザーデバイスに追加するには、［参照］をクリックしてファイルの場所に移動します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

macOS 設定

- ユーザーに表示される名前：ユーザーのフォント一覧に表示される名前を入力します。
- フォントファイル：フォントファイルを選択してユーザーデバイスに追加するには、［参照］をクリックしてファイルの場所に移動します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

ホーム画面のレイアウトに関するデバイスポリシー

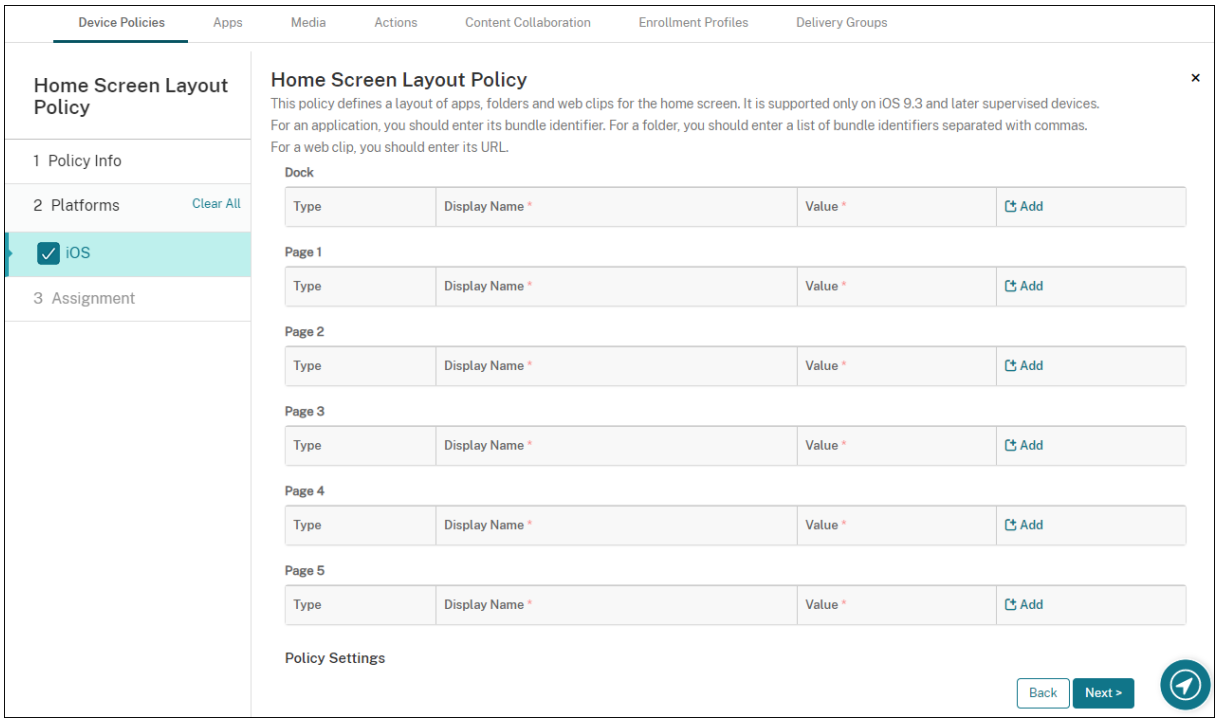
November 29, 2023

ホーム画面のレイアウトに関するデバイスポリシーにより、監視対象の iOS デバイスのホーム画面でのアプリとフォルダーのレイアウトを指定します。

> 重要:
>
> 複数のホーム画面のレイアウトに関するポリシーを 1 台のデバイスに展開すると、デバイスで iOS エラーが発生します。この制限は、この Citrix Endpoint Management ポリシーまたは Apple Configurator を使用してホーム画面を定義するかどうかに関係なく適用されます。

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

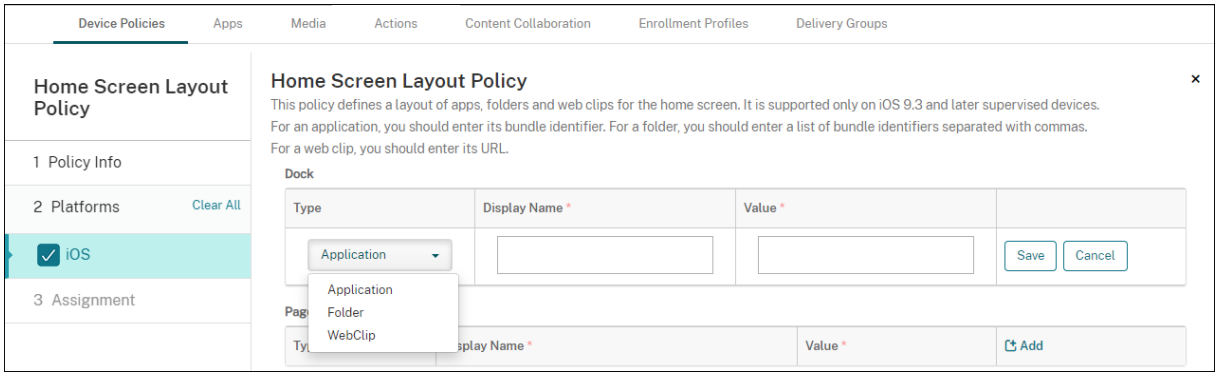
iOS の設定



- 構成する各画面の領域（ドックやページ **1** など）で、[追加] をクリックします。
- 種類：[アプリケーション]、[フォルダー]、[**Web** クリップ] のいずれかを選択します。

  制限デバイスポリシーの [アプリ使用の制限] > [指定したアプリのみ許可する] 設定によって、ホーム画面で Web クリップが正しく表示されない場合があります。Web クリップを正しく表示するには、次のいずれかを実行します：

  - [アプリ使用の制限] を [すべてのアプリを許可] または [アプリによっては許可しない] に設定します。
  - [アプリ使用の制限] を [指定したアプリのみ許可する] に設定し、バンドル ID `com.apple.webapp`のアプリを追加して Web クリップを許可します。



- 表示名：アプリまたはフォルダーのホーム画面に表示される名前。
- 値：アプリの場合は、バンドル識別子を入力します。フォルダーの場合は、コンマで区切られたバンドル識別子のリストを入力します。Web クリップの場合、バンドル ID `com.apple.webClip.managed`を入力し、Web クリップポリシーで Web クリップの URL を構成します。同じ URL に複数の Web クリップ値が存在する場合、動作は iOS 11.3 以降のデバイスでは未定義です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは iOS 9.3 以降でのみ使用できます。

iOS および macOS プロファイルのインポートデバイスポリシー

November 29, 2023

iOS および macOS デバイス用のデバイス構成 XML ファイルを Citrix Endpoint Management にインポートできます。XML ファイルには、Apple Configurator 2 または Profile Creator を使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。構成 XML ファイルには、マクロを含めることができます。詳しくは、「Macros（マクロ）」を参照してください。

使用例

Profile Creator を使用して、macOS デバイス用の Citrix Endpoint Management の外部で作成された次の構成をインポートします：

- システムポリシーコントロール：このポリシーは、認定された Apple デベロッパーによって署名されたアプリケーションを識別し、ユーザーが Mac App Store から検証済みのアプリケーションをダウンロードできるようにします。

  ポリシーを構成する場合：

  - ［**Enable Gatekeeper**］を選択して、検証済みで信頼できるソフトウェアだけをユーザーが実行するようにします。
  - ［**Allow Identified Developers**］を選択して、認定された Apple デベロッパーによって署名されたアプリのみをユーザーがインストールするようにします。

- プライバシー設定ポリシーコントロール：このポリシーを使用すると、位置情報サービス、カメラ、スクリーンショットなどの特定のファイルや機能へのアプリケーション間のアクセスを許可または制限できます。

  展開予定の設定を構成します。詳しくは、「プライバシー設定ポリシーコントロールのペイロード設定」を参照してください。

- カーネル拡張ポリシー：このポリシーを使用すると、ユーザーがオペレーティングシステムのネイティブ機能を拡張するアプリ拡張をインストールできるようになります。カーネル拡張はカーネルレベルで実行されます。

  展開予定の設定を構成します。詳しくは、「カーネル拡張ポリシーのペイロード設定」を参照してください。

- イーサネット設定ポリシー：このポリシーを使用すると、イーサネットネットワーク接続を管理できます。

  展開予定の設定を構成します。詳しくは、「イーサネット設定」を参照してください。

Apple Configurator 2 または Profile Creator を使用して、macOS および iOS デバイスの次のポリシーを構成します：

- **Wi-Fi** ポリシー：このポリシーを使用すると、ユーザーがデバイスを Wi-Fi ネットワークに接続する方法を管理できます。

  ポリシーを構成する場合：

  - ターゲット SSID を優先度リストの先頭に追加します。
  - ユーザーがネットワークに参加するときに使用する接続モードを選択します。［システム］を選択すると、デバイスはシステムの資格情報を使用してユーザーを認証します。［ログインウィンドウ］を選択すると、デバイスはログインウィンドウで入力されたものと同じ資格情報を使用してユーザーを認証します。

  詳しくは、「Wi-Fi 設定」を参照してください。

- 制限ポリシー：このポリシーで、ユーザーデバイス上の特定の機能の使用を許可または制限します。

  展開予定の設定を構成します。詳しくは、「制限の概要」を参照してください。

- **VPN** ポリシー：このポリシーは、プライベートネットワークへのデバイスレベルの暗号化接続を提供します。

  展開予定の設定を構成します。詳しくは、「VPN の概要」を参照してください。

Apple Configurator 2 を使用する構成プロファイルの作成

1. Apple App Store から Apple Configurator 2 をインストールします。
2. Apple Configurator 2 を起動し、[**File**] > [**New Profile**] の順に選択します。新しい構成ウィンドウが開きます。
3. [**General**] 設定ペインで、プロファイルの名前と識別子を入力し、追加のペイロードオプションを追加します。
4. 左側のペインで、ペイロードを選択し、[**Configure**] をクリックして設定を入力します。署名入りプロファイルはサポートされていないため、プロファイルに署名しないでください。

   1 つのプロファイル内に複数のペイロードを追加するには、ペイロードを選択し、右上隅にある [**Add Payload**] をクリックします。
5. [**File**] > [**Save**] の順に選択し、XML ファイルの名前と保存する場所を選択し、[**Save**] をクリックします。

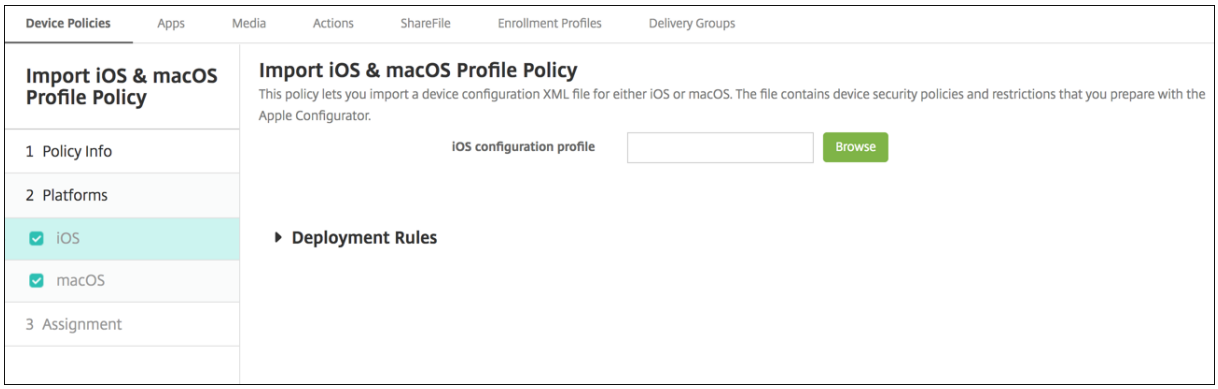
Profile Creator を使用する構成プロファイルの作成

1. GitHubから Profile Creator をインストールします。
2. Profile Creator を起動し、[**File**] > [**New**] の順に選択します。新しい構成ウィンドウが開きます。
3. [**General**] 設定ペインで、プロファイルの名前と説明を入力し、追加のペイロードオプションを追加します。
   - 推奨事項: [**Prevent users from removing this profile**] を選択してください。
   - [**Payload Scope**] を [**System**] または [**User**] に設定します。
4. 左側のペインでポリシーを選択し、設定を構成し、右上隅の [**Add**] をクリックします。

   1 つのプロファイル内に複数のポリシーを設定するには、ポリシーを選択して、[**Add**] をクリックします。
5. [**File**] > [**Export**] の順に選択し、XML ファイルの名前と保存する場所を選択し、[**Save**] をクリックします。

Citrix Endpoint Management コンソールで iOS および macOS のプロファイルデバイスポリシーの構成ファイルをインポートするには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および macOS の設定



- **iOS** 構成プロファイルまたは **macOS** 構成プロファイル：［参照］をクリックしてインポートする構成ファイルの場所へ移動し、対象ファイルを選択します。

Keyguard 管理デバイスポリシー

April 12, 2023

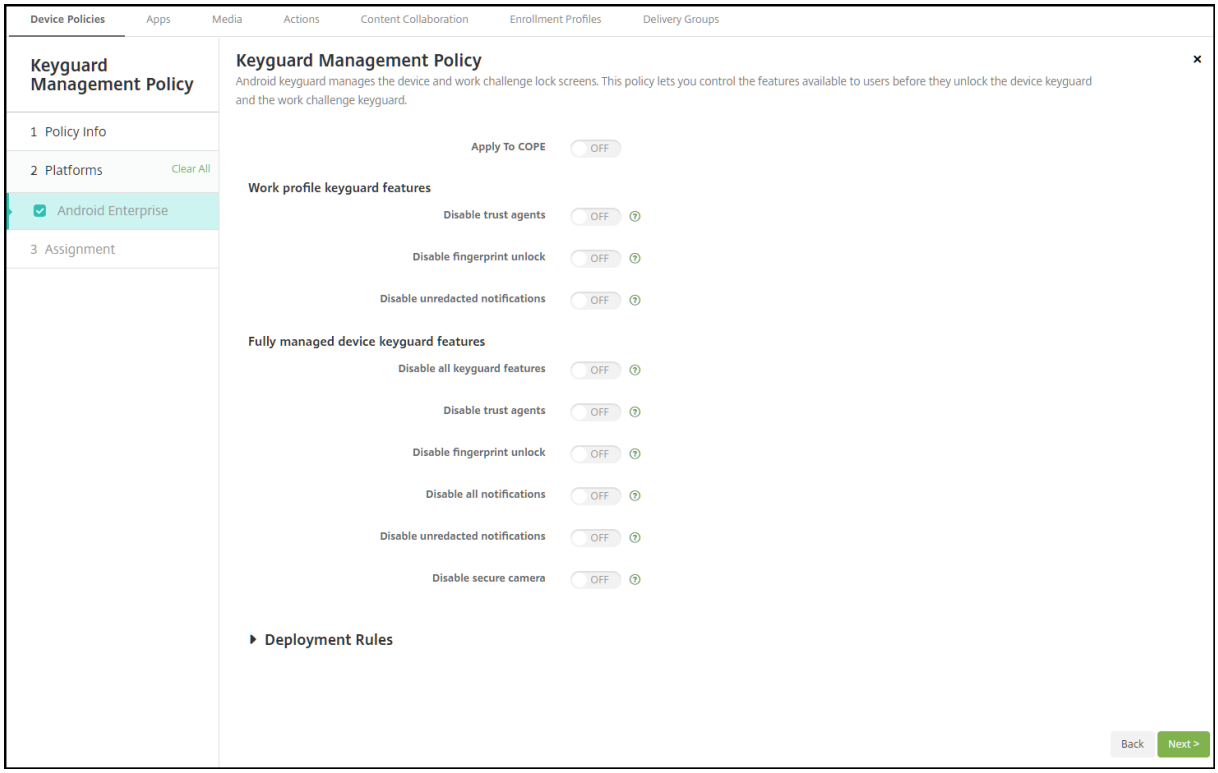
Android の Keyguard は、デバイスのロック画面および仕事用チャレンジのロック画面を管理します。このポリシーでは、ユーザーが Android Enterprise のデバイスの仕事用プロファイル Keyguard と詳細デバイス Keyguard の機能を管理できます。以下を制御できます：

- 仕事用プロファイルデバイスの Keyguard 管理。デバイス Keyguard と仕事用チャレンジ Keyguard をロック解除する前に、ユーザーが利用できる機能を指定できます。たとえば、デフォルトでは、ユーザーは指紋によるロック解除を使用でき、ロック画面でマスキングされていない通知を表示できます。
- 完全に管理された専用デバイスでの Keyguard 管理。Keyguard 画面のロックを解除する前に、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。
- 仕事用プロファイルで完全に管理されたデバイスの Keyguard 管理。これらのデバイスは、以前は COPE（個人使用可能なコーポレート所有）デバイスと呼ばれていました。1 つの Keyguard 管理ポリシーを使用して、デバイスと仕事用プロファイルに個別の設定を適用できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

詳しくは、このビデオをご覧ください：

Android Enterprise の設定



- **COPE** に適用：仕事用プロファイルで完全に管理されたデバイスの Keyguard 管理デバイスポリシー設定を

構成できます。

この設定が ［オン］の場合、個別の設定をデバイスおよび仕事用プロファイルで完全に管理されたデバイスの仕事用プロファイルに適用できます。

この設定を ［オフ］すると、仕事用プロファイルデバイスまたは完全に管理されたデバイスに設定を適用できます。仕事用プロファイルを構成した設定は、仕事用プロファイルデバイスにのみ適用されます。完全に管理されたデバイス用に構成する設定は、完全に管理されたデバイスにのみ適用されます。

デフォルトは ［オフ］です。

- 仕事用プロファイル **Keyguard** 機能：ユーザーが仕事用プロファイル Keyguard（ロック画面）のロックを解除する前に、次の機能を使用できるかどうかを制御します。
  - 信頼できるエージェントを無効にする：［オフ］に設定すると、仕事用プロファイルにチャレンジが設定されている場合に、信頼できるエージェントがセキュアな Keyguard 画面で作業できます。仕事用プロファイルで信頼できるエージェントをすべて無効にするには、［オン］に設定します。デフォルトは ［オフ］です。
  - 生体認証を無効にする：［オフ］に設定すると、仕事用プロファイルにチャレンジが設定されている場合に、セキュアな Keyguard 画面で生体認証を利用できます。仕事用プロファイルで生体認証を無効にするには、［オン］に設定します。この設定により、指紋によるロック解除、顔認証、虹彩認証が無効になります。デフォルトは ［オフ］です。Android 9.0 以降。
  - 指紋によるロック解除を無効にする：［オフ］に設定すると、仕事用プロファイルにチャレンジが設定されている場合に、セキュアな Keyguard 画面で指紋によるロック解除を利用できます。仕事用プロファイルの指紋によるロック解除を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。
  - 顔認証を無効にする：［オフ］に設定すると、仕事用プロファイルにチャレンジが設定されている場合に、セキュアな Keyguard 画面で顔認証を利用できます。仕事用プロファイルで顔認証を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。Android 9.0 以降。
  - 虹彩認証を無効にする：［オフ］に設定すると、仕事用プロファイルにチャレンジが設定されている場合に、セキュアな Keyguard 画面で虹彩認証を利用できます。仕事用プロファイルで虹彩認証を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。Android 9.0 以降。
  - マスキングされていない通知を無効にする：［オフ］に設定すると、セキュアな Keyguard 画面にマスキングされている通知と、されていない通知の両方が表示されます。マスキングされていない通知を無効にし、マスキングされた通知のみを表示するには、［オン］に設定します。デフォルトは ［オフ］です。
- 完全に管理されているデバイスの **Keyguard** 機能：ユーザーがデバイス Keyguard（ロック画面）のロックを解除する前に、次の機能を使用できるかどうかを制御します。これらの機能は、完全に管理されたデバイスまたは専用デバイスに適用されます。
  - すべての **Keyguard** 機能を無効にする：［オフ］に設定すると、現在および将来の Keyguard のカスタマイズを、セキュアな Keyguard 画面ですべて利用できます。Keyguard のカスタマイズをすべて無効にするには、［オン］に設定します。デフォルトは ［オフ］です。
  - 信頼できるエージェントを無効にする：［オフ］に設定すると、信頼できるエージェントがセキュアな Keyguard 画面で作業できます。信頼できるエージェントを無効にするには、［オン］に設定します。デ

フォルトは ［オフ］です。

- 生体認証を無効にする：［オフ］に設定すると、デバイスにチャレンジが設定されている場合に、セキュアな Keyguard 画面で生体認証を利用できます。デバイスで生体認証を無効にするには、［オン］に設定します。これにより、指紋によるロック解除、顔認証、虹彩認証が無効になります。デフォルトは［オフ］です。Android 9.0 以降。
- 指紋によるロック解除を無効にする：［オフ］に設定すると、デバイスにチャレンジが設定されている場合に、セキュアな Keyguard 画面で指紋によるロック解除を利用できます。デバイスで指紋によるロック解除を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。
- 顔認証を無効にする：［オフ］に設定すると、デバイスにチャレンジが設定されている場合に、セキュアな Keyguard 画面で顔認証を利用できます。デバイスで顔認証を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。Android 9.0 以降。
- 虹彩認証を無効にする：［オフ］に設定すると、デバイスにチャレンジが設定されている場合に、セキュアな Keyguard 画面で虹彩認証を利用できます。デバイスで虹彩認証を無効にするには、［オン］に設定します。デフォルトは ［オフ］です。Android 9.0 以降。
- すべての通知を無効にする：［オフ］に設定すると、セキュアな Keyguard 画面にすべての通知が表示されます。すべての通知を表示するには、［オン］に設定します。デフォルトは ［オフ］です。
- マスキングされていない通知を無効にする：［オフ］に設定すると、セキュアな Keyguard 画面にマスキングされている通知と、されていない通知の両方が表示されます。マスキングされていない通知を無効にし、マスキングされた通知のみを表示するには、［オン］に設定します。デフォルトは ［オフ］です。
- セキュアカメラを無効にする：［オフ］に設定すると、セキュアな Keyguard 画面でセキュアカメラを利用できます。セキュアカメラを無効にするには、［オン］に設定します。デフォルトは ［オフ］です。

キオスクデバイスポリシー

November 29, 2023

キオスクポリシーでは、実行可能なアプリを制限することで、デバイスをキオスクモードに制限できます。Citrix Endpoint Management が、キオスクモードでデバイスのどの部分がロックされるかを制御することはありません。ポリシーの展開後、デバイスがキオスクモード設定を管理します。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

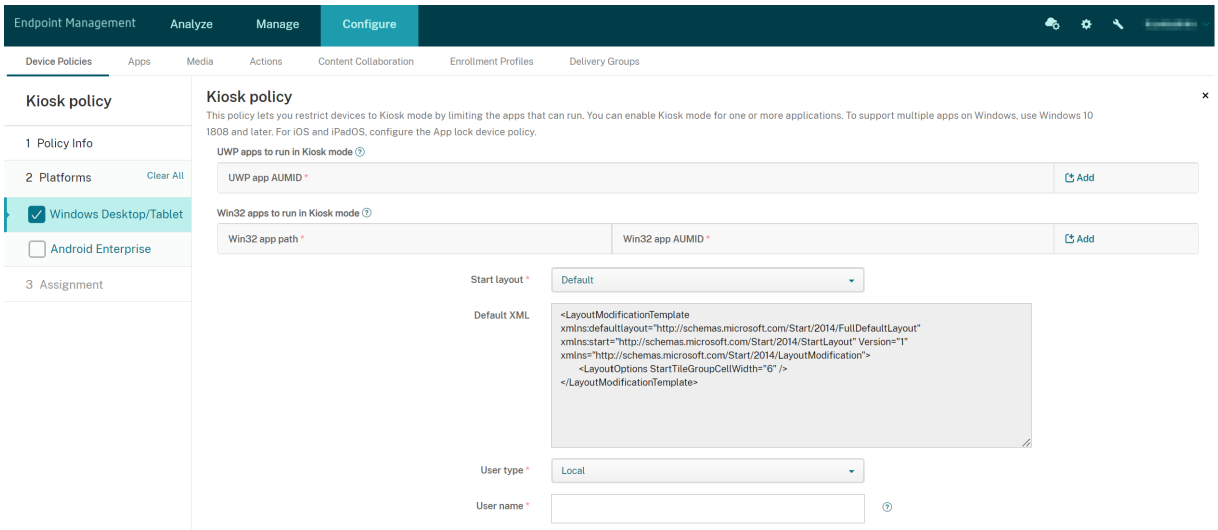
iPad をキオスクモードで実行するように設定するには、アプリのロックデバイスポリシーを使用します。iPad をキオスクとして設定する方法について詳しくは、「iPad をキオスクとして構成する」を参照してください。単一の Web サイトのみを開くように iPad を構成することもできます。詳しくは、「Web クリップポリシー」を参照してください。

Windows デスクトップとタブレットの設定

Windows デスクトップおよびタブレットデバイスの場合、キオスクポリシーはローカルユーザーと Azure Active Directory に登録されているユーザーにのみ適用されます。

1 つのアプリまたは複数のアプリを Windows デスクトップおよびタブレットデバイス上で、キオスクモードで実行できます。

> 注:
>
> キオスクデバイスポリシーは、Windows 10 デバイスにのみ適用されます。
> Windows 11 デバイスに単一アプリのキオスクを展開するには、カスタム XML デバイスポリシーを使用して、デバイスに提供する XML スクリプトを展開できます。詳しくは、「Windows 11 デバイスに単一アプリのキオスクを展開する」を参照してください。



- **UWP** アプリ **AUMID**: [追加] をクリックしてユニバーサル Windows プラットフォーム (UWP) アプリを選択し、各 UWP アプリのアプリケーションユーザーモデル (AUMID) を入力します。たとえば、次の AUMID を入力します:
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Win32** アプリパスおよび **Win32** アプリ **AUMID**: [追加] をクリックして Windows デスクトップ (Win32) アプリを選択し、各 Win32 アプリのパスと AUMID を入力します。たとえば、次のパスと AUMID を入力します:
  - `%windir%\system32\mspaint.exe` または `C:\Windows\System32\mspaint.exe`
  - `{ 1AC14E77-02E7-4E5D-B744-2EB1AE5198B7 } \mspaint.exe`
- レイアウトの開始: アプリのデフォルトのスタート画面のみ利用可能です。
- デフォルト **XML**: デフォルトの XML スクリプトのみ利用可能です。

- ユーザーの種類の選択：キオスクポリシーを受け取るユーザーの種類を指定します。選択できるオプションは以下のとおりです：
  - ローカル： Citrix Endpoint Management はターゲットデバイス用にユーザーを作成するか、既存のユーザーを追加します。
  - **Azure AD**： Citrix Endpoint Management は Azure AD に登録されているユーザーを追加します。
- ユーザー名：キオスクポリシーを受け取るユーザー名を入力します。
  - ターゲットデバイス上にローカルユーザー名を作成するには、名前を入力します。ローカルユーザー名にドメインが含まれていないことを確認してください。既存のユーザー名を入力した場合、Citrix Endpoint Management によってユーザーが作成されたり、現在のパスワードが変更されたりすることはありません。
  - Azure AD ユーザーを追加するには、`azuread\user`の形式でユーザー名を入力します。`user`の部分は Azure AD でユーザーを作成するときに入力した ［名前］、または Azure AD でユーザーを作成するときに入力した ［ユーザー名］ になります。割り当てられたユーザーは Azure AD 管理者になることはできません。
- パスワード： Azure AD ユーザーの場合はパスワードの設定はありません。パスワードはローカルユーザー名の場合のみ入力します。
- タスクバーの表示：タスクバーを有効にすると、ユーザーはアプリケーションを簡単に表示および管理できます。デフォルトは ［オフ］ です。
- ［次へ］ をクリックして変更を保存します。

キオスクモードで許可する UWP アプリの場合は、AUMID を提供する必要があります。現在のデバイスユーザー用にインストールされているすべての Microsoft Store アプリの AUMID の一覧を取得するには、次の PowerShell コマンドを実行します：

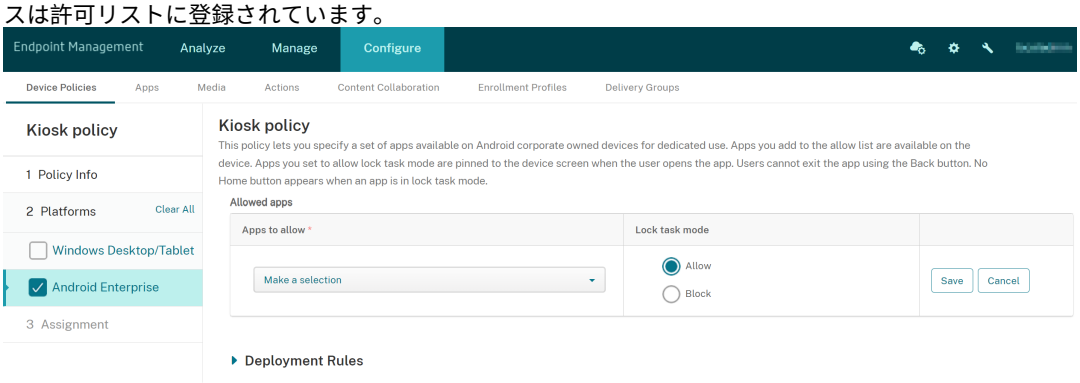
```
$installedapps = get-AppxPackage

$aumidList = @()
foreach ($app in $installedapps)
{

    foreach ($id in (Get-AppxPackageManifest $app).package.applications
        .application.id)
    {

        $aumidList += $app.packagefamilyname + "!"+ $id
     }

 }


$aumidList
<!--NeedCopy-->
```


Android Enterprise の設定

Android Enterprise 専用デバイス（特定業務専用コーポレート所有（COSU）デバイスとも呼ばれる）の場合は、アプリを許可し、ロックタスクモードを設定できます。

アプリを許可するには、[追加] をクリックします。複数のアプリを許可リストに追加できます。詳しくは、「Android Enterprise」を参照してください。

- 許可するアプリ：許可するアプリのパッケージ名を入力するか、リストからアプリを選択します。
  - [新規追加] をクリックして、リストで許可するアプリのパッケージ名を入力します。
  - リストから既存のアプリを選択します。このリストには、Citrix Endpoint Management にアップロードされているアプリが表示されます。デフォルトでは、Citrix Secure Hub と Google Play サービスは許可リストに登録されています。



- ロックタスクモード：ユーザーがアプリを起動した時にアプリをデバイス画面に固定するには、[許可] を選択します。アプリをデバイス画面に固定しない場合は、[禁止] を選択します。デフォルトは [許可] です。

アプリがロックタスクモードになると、ユーザーがアプリを開いたときにデバイス画面にアプリが固定されます。ホームボタンは表示されず、[戻る] ボタンは無効になります。ユーザーは、サインアウトなど、アプリでプログラムされた操作を使用してアプリを終了します。

Launcher 構成デバイスポリシー

November 29, 2023

Citrix Launcher を使用すると、Citrix Endpoint Management によって展開された Android Enterprise デバイスおよび従来の Android デバイスのユーザーエクスペリエンスをカスタマイズできます。

Launcher 構成ポリシーを使用すると、次の Citrix Launcher 機能を制御できます：

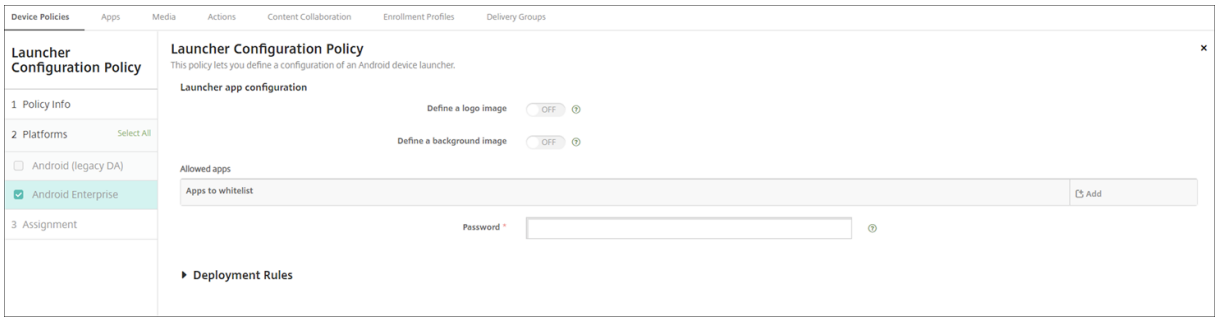
- ユーザーが指定したアプリにのみアクセスできるように、Android Enterprise デバイスと従来の Android デバイスを管理する。

- Citrix Launcher アイコンのカスタムロゴ画像と、Citrix Launcher のカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

Citrix Launcher は、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android および **Android Enterprise** の設定



- ロゴ画像を定義： Citrix Launcher アイコンにカスタムロゴ画像を使用するかどうかを選択します。デフォルトは ［オフ］です。
- ロゴ画像：［ロゴ画像を定義］を有効にした場合、［参照］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、および GIF です。
- 背景画像を定義： Citrix Launcher の背景にカスタム画像を使用するかどうかを選択します。デフォルトは［オフ］です。
- 背景画像：［背景画像を定義］を有効にした場合、［参照］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、および GIF です。
- 許可するアプリ： Citrix Launcher で許可するアプリごとに、［追加］をクリックして以下の操作を行います：
  - 追加する新規アプリ：追加するアプリの完全な名前を入力します。たとえば、Android のカレンダーアプリの場合は「com.android.calendar」です。
  - ［保存］をクリックしてアプリを追加するか、［キャンセル］をクリックしてアプリの追加を取り消します。
- パスワード： Citrix Launcher を終了するために入力する必要があるパスワード。

LDAP デバイスポリシー

November 29, 2023

Citrix Endpoint Management で iOS デバイスの LDAP ポリシーを作成して、必要なアカウント情報など、使用する LDAP サーバーに関する情報を指定できます。また、LDAP サーバーの照会に使用する LDAP 検索ポリシーのセットが提供されます。

このポリシーを構成するには、LDAP ホスト名が必要です。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明：オプションで、アカウントの説明を入力します。
- アカウントユーザー名：オプションで、ユーザー名を入力します。
- アカウントパスワード：オプションで、パスワードを入力します。このフィールドは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP** ホスト名： LDAP サーバーのホスト名を入力します。このフィールドは必須です。
- **SSL** を使用： LDAP サーバーに対して SSL（Secure Socket Layer）接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- 検索設定： LDAP サーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも 1 つ入力してください。［追加］をクリックして、以下の操作を行います。
  - 説明：検索設定の説明を入力します。このフィールドは必須です。
  - スコープ：［ベース］、［**1** レベル］、［サブツリー］のいずれかを選択して、LDAP ツリーをどの深さまで検索するかを定義します。デフォルトは ［ベース］です。
    - ［ベース］を選択すると、［検索ベース］で参照されているノードを検索します。
    - ［**1** レベル］を選択すると、［ベース］を選択した場合の検索対象ノードとその 1 つ下のレベルを検索します。
    - ［サブツリー］を選択すると、［ベース］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - 検索ベース：検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」です。このフィールドは必須です。
  - ［保存］をクリックして検索設定を追加するか、［キャンセル］をクリックして検索設定の追加を取り消します。
  - 追加する検索設定ごとに上記の手順を繰り返します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

macOS 設定

- アカウントの説明：オプションで、アカウントの説明を入力します。
- アカウントユーザー名：オプションで、ユーザー名を入力します。
- アカウントパスワード：オプションで、パスワードを入力します。このフィールドは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP** ホスト名： LDAP サーバーのホスト名を入力します。このフィールドは必須です。
- **SSL** を使用：LDAP サーバーに対して SSL（Secure Socket Layer）接続を使用するかどうかを選択します。デフォルトは ［オン］です。
- 検索設定： LDAP サーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも 1 つ入力してください。［追加］をクリックして、以下の操作を行います。
  - 説明：検索設定の説明を入力します。このフィールドは必須です。
  - スコープ：［ベース］、［**1** レベル］、［サブツリー］のいずれかを選択して、LDAP ツリーをどの深さまで検索するかを定義します。デフォルトは ［ベース］です。
    - ［ベース］を選択すると、［検索ベース］で参照されているノードを検索します。
    - ［**1** レベル］を選択すると、［ベース］を選択した場合の検索対象ノードとその 1 つ下のレベルを検索します。
    - ［サブツリー］を選択すると、［ベース］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - 検索ベース：検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」です。このフィールドは必須です。
  - ［保存］をクリックして検索設定を追加するか、［キャンセル］をクリックして検索設定の追加を取り消します。
  - 追加する検索設定ごとに上記の手順を繰り返します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

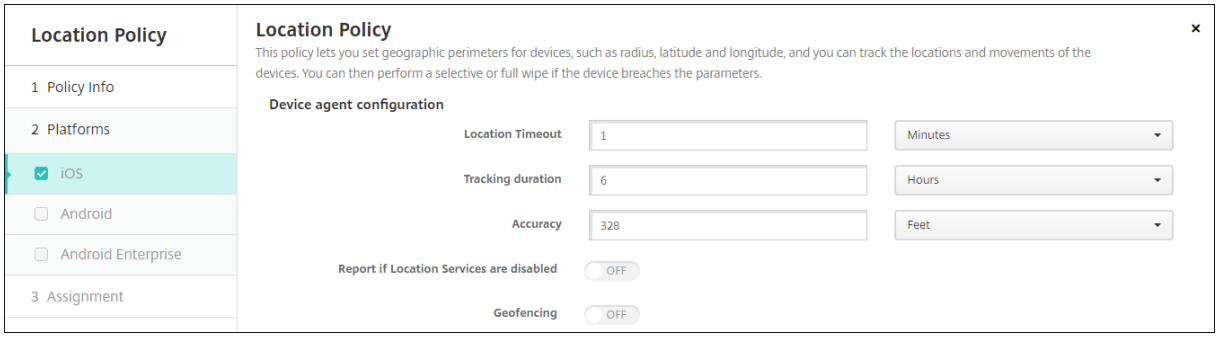
位置情報デバイスポリシー

November 29, 2023

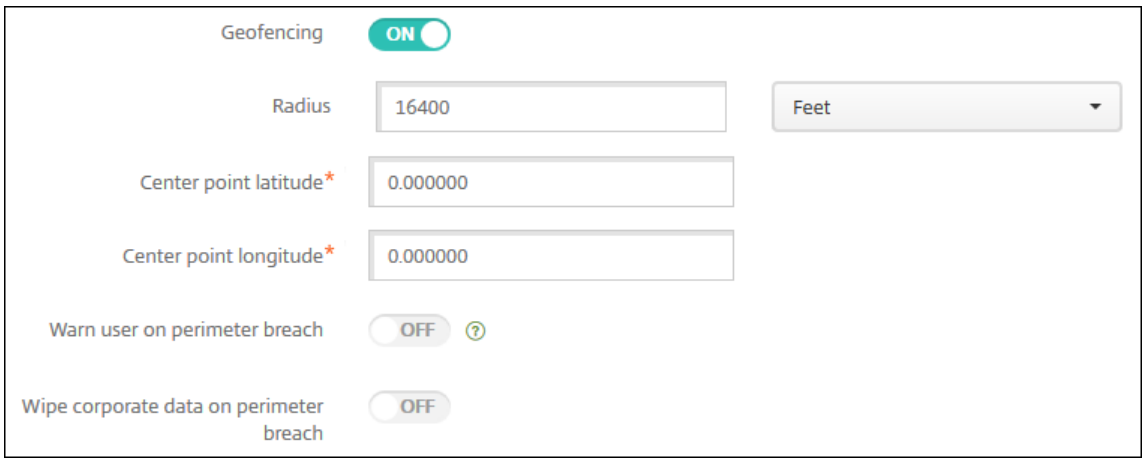
Citrix Endpoint Management で位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。定義された境界（ジオフェンスとも呼ばれます）の外にユーザーが出た場合、Citrix Endpoint Management では特定のアクションを実行できます。たとえば、定義された境界の外にユーザーが出た場合に、警告メッセージを表示するようにポリシーを構成できます。また、境界違反時にユーザーの企業データを即時または一定の時間が経過してからワイプするように構成することもできます。デバイスの追跡と検索の有効化などのセキュリティ操作については、「セキュリティ操作」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- 位置タイムアウト：数値を入力して、［秒］または ［分］を選択し、Citrix Endpoint Management がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、60～900 秒または 1～15 分です。デフォルトは **1** 分です。
- 追跡期間：数値を入力して、［時間］または ［分］を選択し、Citrix Endpoint Management がデバイスを追跡する時間を設定します。有効な値は、1～10 時間または 10～600 分です。デフォルトは **6** 時間です。
- 精度：数値を入力して、ボックスの一覧で ［メートル］、［フィート］、［ヤード］のいずれかを選択し、Citrix Endpoint Management がデバイスを追跡する精度を設定します。有効な値は、10～5000m、10～5000 ヤード、または 30～15000 フィートです。デフォルトは **328** フィート（**100m**）です。
- 位置情報サービスが無効の場合は報告： GPS を無効にした場合に、デバイスから Citrix Endpoint Management にレポートを送信するかどうかを選択します。デフォルトは ［オフ］です。
- ジオフェンシング

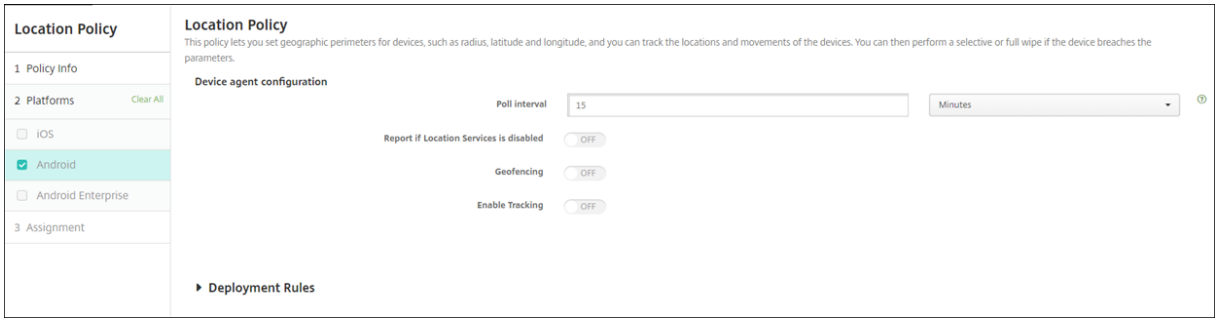


［ジオフェンシング］を選択した場合は、次の設定を構成します：

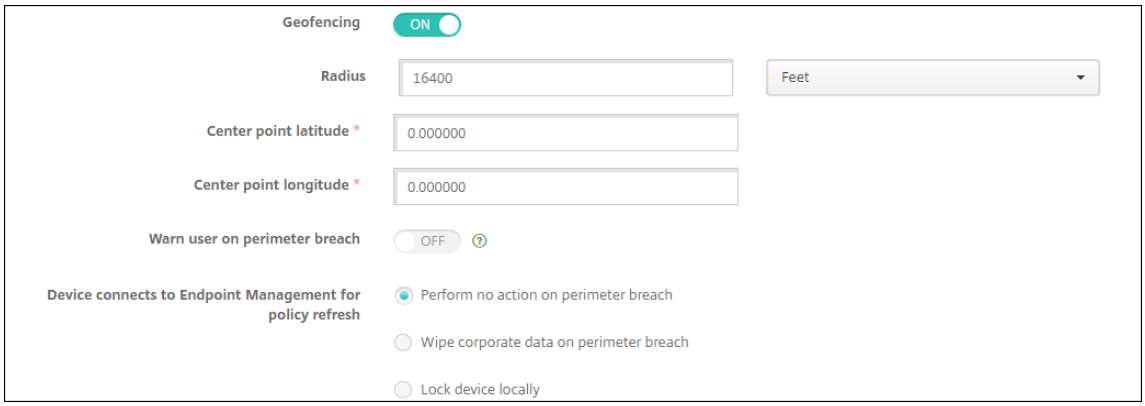
- 半径：数値を入力して、半径の測定に使用する単位を選択します。デフォルトは **16400** フィート（**5000m**）です。有効な半径の値は次のとおりです。
  - 164～16400 フィート
  - 50～50000m
  - 54～54680 ヤード
  - 1～31 マイル
- 中心点の緯度：緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。
- 中心点の経度：経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［オフ］です。警告メッセージの表示に Citrix Endpoint Management への接続は必要ありません。
- 境界違反時に企業データをワイプ：ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。デフォルトは［オフ］です。このオプションを有効にすると、［ローカルワイプを延期］フィールドが表示されます。
  - 数値を入力し、［秒］または［分］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが Citrix Endpoint Management によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。

Android（レガシデバイス管理者）の設定

Android の位置情報の追跡には、Android 9 以降が必要です。



- ポーリング間隔：数値を入力して、[分]、[時間]、[日] のいずれかを選択し、Citrix Endpoint Management がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、15～1440 分、1～24 時間、または任意の日数です。デフォルトは **15** 分です。
- 位置情報サービスが無効の場合は報告： GPS を無効にした場合に、デバイスから Citrix Endpoint Management にレポートを送信するかどうかを選択します。デフォルトは ［オフ］ です。
- ジオフェンシング



［ジオフェンシング］ を選択した場合は、次の設定を構成します：

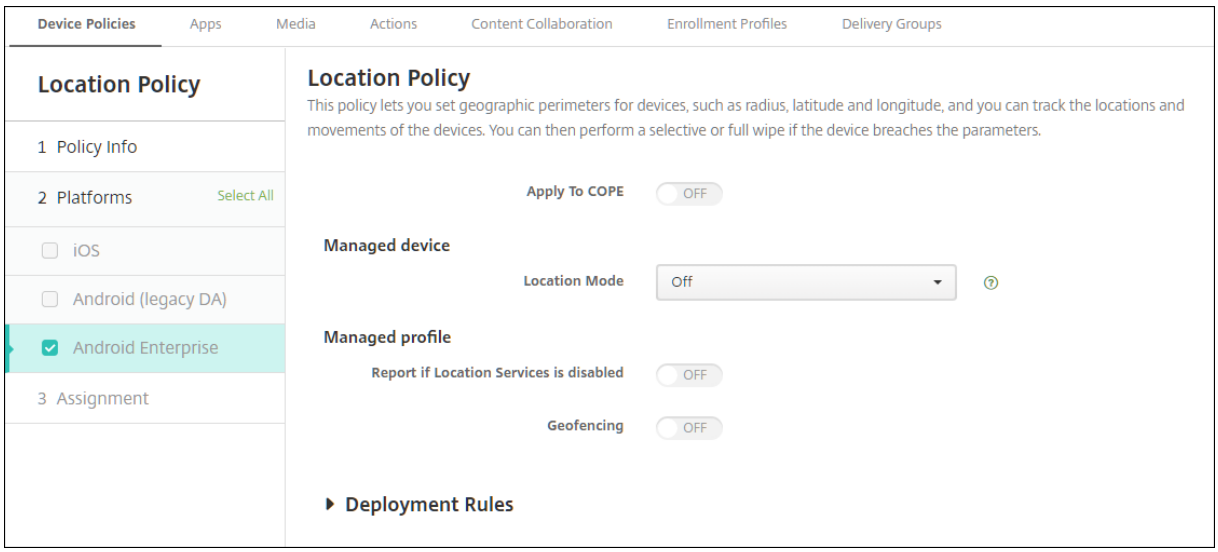
- 半径：数値を入力して、半径の測定に使用する単位を選択します。デフォルトは **16400** フィート（**5000m**）です。有効な半径の値は次のとおりです。
  - 164～164000 フィート
  - 1～50km
  - 50～50000m
  - 54～54680 ヤード
  - 1～31 マイル
- 中心点の緯度：緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。
- 中心点の経度：経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［オフ］です。警告メッセージの表示に Citrix Endpoint Management への接続は必要ありません。

- ポリシー更新のためデバイスを **Citrix Endpoint Management** に接続：ユーザーが境界の外に出た場合のオプションを以下から選択します：
  - 境界違反時に何も実行しない：何もしません。これがデフォルトの設定です。
  - 境界違反時に企業データをワイプ：指定時間後に企業データをワイプします。このオプションを有効にすると、［ローカルワイプを延期］フィールドが表示されます。
    * 数値を入力し、［秒］または ［分］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが Citrix Endpoint Management によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。
  - デバイスをローカルにロック：指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、［ロックを延期］フィールドが表示されます。
    * 数値を入力し、［秒］または ［分］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスが Citrix Endpoint Management によってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。
- 追跡を有効にする：デバイスがユーザーの場所を追跡するかを選択します。デフォルトは ［オフ］です。

Android Enterprise の設定

Android デバイスの位置の追跡を機能させるには、次の要件が満たされている必要があります：

- Android 9 以降
- Android Enterprise のデバイス制限ポリシーで、現在地の共有を許可する設定が有効になっていること
- 接続のスケジュール設定（Firebase Cloud Messaging を推奨）



仕事用プロファイルで完全に管理されているデバイスに適用

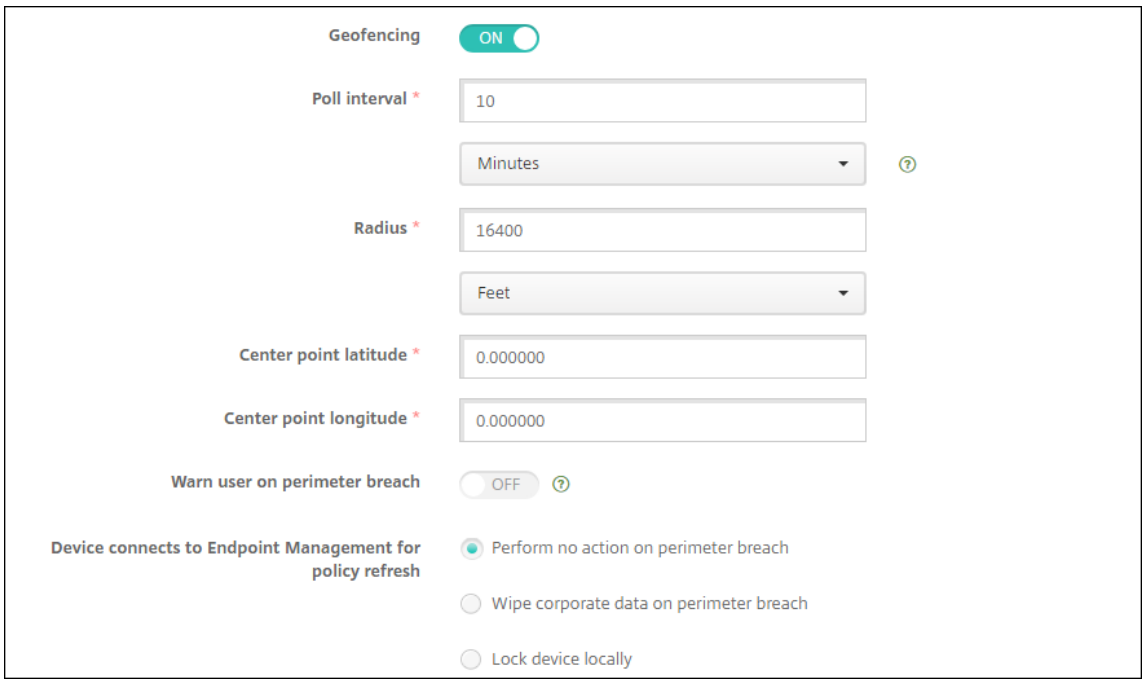
仕事用プロファイルで完全に管理されたデバイス（以前の COPE デバイス）では、位置情報モード設定のみを使用できます。

- 仕事用プロファイルで完全に管理されているデバイスに適用 **/**会社所有のデバイスの仕事用プロファイルに適用：仕事用プロファイルで完全に管理されたデバイスの位置情報モードを構成できます。この設定がオンの場合、仕事用プロファイルの設定を構成します。
  - 位置情報サービスが無効の場合は報告： GPS を無効にした場合に、デバイスから Citrix Endpoint Management にレポートを送信するかどうかを選択します。デフォルトは ［オフ］です。
  - ジオフェンシング：前述の「管理対象デバイス」の設定を参照してください。

［仕事用プロファイルで完全に管理されているデバイスに適用 **/**会社所有のデバイスの仕事用プロファイルに適用］がオフの場合、次のセクションに示すように、設定は管理対象デバイスおよび仕事用プロファイルに適用されます。デフォルトは ［オフ］です。

管理対象デバイス

- 位置情報モード：有効にする位置情報検出のレベルを指定します。位置情報モードが ［高精度］または ［バッテリー節約］に設定されている場合のみ、検索セキュリティアクションを使用できます。デフォルトは ［高精度］です。
  - 高精度： GPS、ネットワーク、その他のセンサーなど、すべての位置検出方法を有効にします。
  - センサーのみ： GPS およびその他のセンサーのみを有効にします。
  - バッテリー節約：ネットワーク位置情報プロバイダーのみを有効にします。
  - オフ：位置の検出を無効にします。
- ジオフェンシング：



［ジオフェンシング］を選択した場合は、次の設定を構成します：

- ポーリング間隔：数値を入力して、［分］、［時間］、［日］のいずれかを選択し、Citrix Endpoint Management がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1～1440 分、1～24 時間、または任意の日数です。デフォルトは **10** 分です。この値を 10 分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- 半径：数値を入力して、半径の測定に使用する単位を選択します。デフォルトは **16400** フィート（**5000m**）です。有効な半径の値は次のとおりです。
  - 164～164000 フィート
  - 1～50km
  - 50～50000m
  - 54～54680 ヤード
  - 1～31 マイル
- 中心点の緯度：緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。値を検索するには、［管理］**>**［デバイス］の順に移動し、デバイスを選択して ［セキュリティ］、［検索］の順にクリックします。デバイスの検出後、Citrix Endpoint Management は ［セキュリティ］の ［デバイス詳細］**>**［一般］ページでデバイスの位置情報を報告します。
- 中心点の経度：経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［オフ］です。警告メッセージの表示に Citrix Endpoint Management への接続は必要ありません。

- ポリシー更新のためデバイスを **Citrix Endpoint Management** に接続：ユーザーが境界の外に出た場合のオプションを以下から選択します：
  - 境界違反時に何も実行しない：何もしません。この設定がデフォルトです。
  - 境界違反時に企業データをワイプ：指定時間後に企業データをワイプします。このオプションを有効にすると、［ローカルワイプを延期］フィールドが表示されます。
    - 数値を入力し、［秒］または ［分］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが Citrix Endpoint Management によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。
  - デバイスをローカルにロック：指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、［ロックを延期］フィールドが表示されます。
    - 数値を入力し、［秒］または ［分］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスが Citrix Endpoint Management によってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。

仕事用プロファイル

- 位置情報サービスが無効の場合は報告： GPS を無効にした場合に、デバイスから Citrix Endpoint Management にレポートを送信するかどうかを選択します。デフォルトは ［オフ］です。
- ジオフェンシング：前述の「管理対象デバイス」の設定を参照してください。

ロック画面のメッセージデバイスポリシー

February 16, 2022

ロック画面のメッセージポリシーを使用すると、次の iOS デバイスの紛失時に表示するメッセージを設定できます。

- 共有 iPad のログインウィンドウ
- 監視対象の iOS デバイスのロック画面

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- デバイスの資産タグ情報：デバイスの資産タグ。Apple デバイスは長い文字列を省略するため、ポリシーを実稼働環境に展開する前に文字列をテストするようにしてください。文字列の長さは、Apple デバイスのモデルと Apple 設定によって変わります。

- ログインウィンドウとロック画面の脚注：住所やその他の連絡先情報など、デバイスの返却に役立つ情報。たとえば、メッセージを「紛失時の返却先」という形式にすることができます。Apple デバイスは長い文字列を省略するため、ポリシーを実稼働環境に展開する前に文字列をテストするようにしてください。文字列の長さは、Apple デバイスのモデルと Apple 設定によって変わります。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

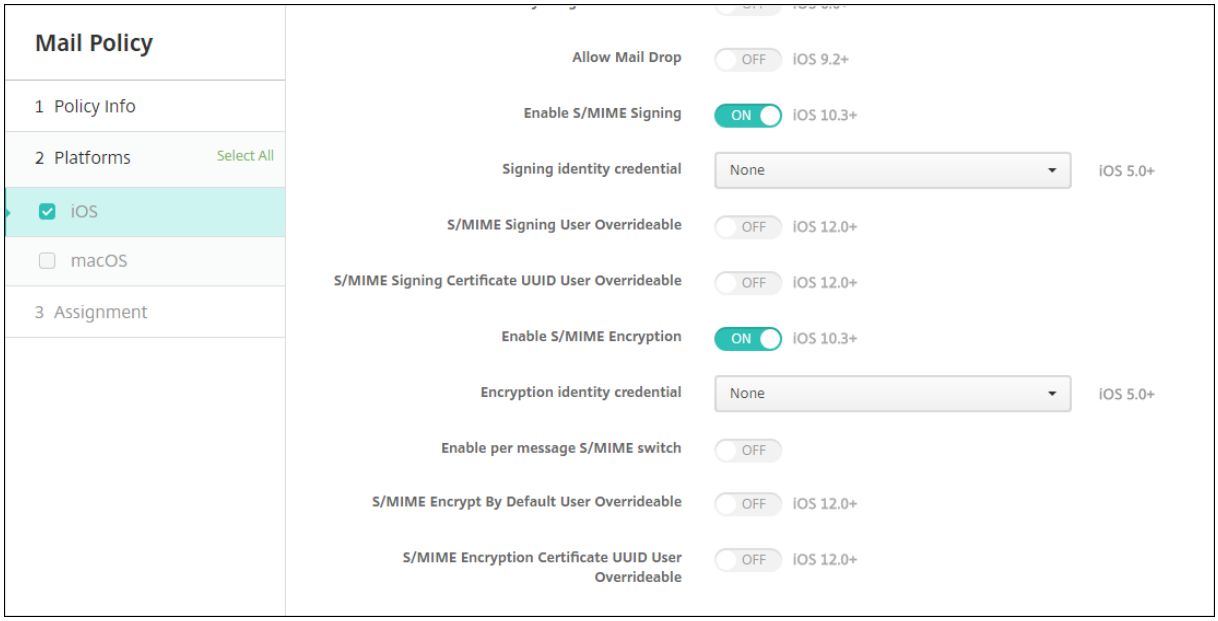
メールデバイスポリシー

November 29, 2023

Citrix Endpoint Management でメールデバイスポリシーを追加して、iOS または macOS デバイスのメールアカウントを構成することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **macOS** の設定



- アカウントの説明：メールおよび設定アプリに表示される、アカウントの説明を入力します。このフィールドは必須です。
- アカウントの種類：［**IMAP**］または ［**POP**］を選択し、ユーザーアカウントで使用するプロトコルを選択します。デフォルトは［**IMAP**］です。［**POP**］を選択した場合、以下の ［パスのプレフィックス］オプションは表示されなくなります。
- パスのプレフィックス：「**INBOX**」と入力するか、IMAP メールアカウントのパスのプレフィックスを入力します。このフィールドは必須です。
- ユーザー表示名：メッセージやその他の目的で使用する完全なユーザー名を入力します。このフィールドは必須です。
- メールアドレス：アカウントの完全なメールアドレスを入力します。このフィールドは必須です。
- 受信メール設定
  - メールサーバーのホスト名：受信メールサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
  - メールサーバーのポート：受信メールサーバーのポート番号を入力します。デフォルトは **143** です。このフィールドは必須です。
  - ユーザー名：メールアカウントのユーザー名を入力します。この名前は一般的に、メールアドレスの @ 記号より前の部分と同じです。このフィールドは必須です。
  - 認証の種類：使用する認証の種類を選択します。デフォルトは ［パスワード］です。［なし］を選択した場合、以下の ［パスワード］フィールドは表示されなくなります。
  - パスワード：任意で、受信メールサーバーのパスワードを入力します。
  - **SSL** を使用：受信メールサーバーで SSL（Secure Socket Layer）認証を使用するかどうかを選択します。デフォルトは ［オフ］です。
- 送信メール設定
  - メールサーバーのホスト名：送信メールサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
  - メールサーバーのポート：送信メールサーバーのポート番号を入力します。ポート番号を入力しなかった場合、指定されたプロトコルのデフォルトポートが使用されます。
  - ユーザー名：メールアカウントのユーザー名を入力します。この名前は一般的に、メールアドレスの @ 記号より前の部分と同じです。このフィールドは必須です。
  - 認証の種類：使用する認証の種類を選択します。デフォルトは ［パスワード］です。
  - パスワード：任意で、送信メールサーバーのパスワードを入力します。
  - 送信と受信に同じパスワードを使用：受信パスワードと送信パスワードが同じであるかどうかを選択します。デフォルトは ［オフ］で、パスワードが異なることを意味します。
  - **SSL** を使用：送信メールサーバーで SSL（Secure Socket Layer）認証を使用するかどうかを選択します。デフォルトは ［オフ］です。
- ポリシー
  - アカウント間でのメールの移動を承認：ユーザーに以下の実行を許可するかを指定します：

    * このアカウントから別のアカウントにメールを移動する
    * 別のアカウントからメールを転送する
    * 別のアカウントから返信する

  デフォルトは ［オフ］です。

- メールアプリからのみメールを送信：ユーザーの電子メールの送信を iOS メールアプリからのみに制限するかどうかを選択します。
- メールの最近の同期を無効化：ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは ［オフ］です。このオプションは iOS 6.0 以降にのみ適用されます。
- メールドロップを許可： iOS 9.2 以降を実行するデバイスに対して Apple Mail Drop の使用を許可するかどうかを選択します。デフォルトは ［オフ］です。
- **S/MIME** 署名の有効化：アカウントで S/MIME 署名をサポートするかどうかを指定します。デフォルトは ［オン］です。［オン］に設定した場合、以下の 2 つのフィールドが表示されます：
    * 署名 **ID** 資格情報：使用する署名資格情報を選択します。
    * **S/MIME** 署名（ユーザー上書き可能）：［オン］に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
    * **S/MIME** 署名証明書 **UUID**（ユーザー上書き可能）：［オン］に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
- **S/MIME** 暗号化の有効化：このアカウントで S/MIME 暗号化をサポートするかどうかを選択します。デフォルトは ［オフ］です。［オン］に設定した場合、以下の 2 つのフィールドが表示されます：
    * 暗号化 **ID** 資格情報：使用する暗号化資格情報を選択します。
    * メッセージごとの **S/MIME** 切り替えの有効化：［オン］に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］です。
    * デフォルトの **S/MIME** 暗号化（ユーザー上書き可能）：［オン］に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。
    * **S/MIME** 暗号化証明書 **UUID**（ユーザー上書き可能）：［オン］に設定した場合、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］です。このオプションは iOS 12.0 以降に適用されます。

- ポリシー設定
    - ポリシーの削除：後でポリシーを削除するには、［日付を選択］または ［削除までの期間（時間）を指定］でポリシーを削除するようこの設定を構成します。
    - ユーザーにポリシーの削除を許可：ユーザーが常にメールポリシーを削除できるか、削除するためにパスコードが必要か、ユーザーによるポリシーの削除を許可しないのかを選択できます。macOS でのみ利用可能です。

- プロファイルの対象： macOS のみ。ポリシーをユーザーレベルで適用するか、システム全体で適用するかを選択します。

管理対象の構成ポリシー

March 15, 2024

管理対象構成デバイスポリシーは、さまざまなアプリ構成オプションとアプリの制限を管理します。このポリシーは、制御する Android Enterprise アプリごとに作成します。

アプリで使用できるオプションとツールチップは、アプリ開発者によって定義されます。ツールチップに「テンプレートの値」を使用すると記述されている場合は、代わりに対応する Citrix Endpoint Management マクロを使用します。詳しくは、「Remote configuration overview」（Android Developer サイト）と「マクロ」を参照してください。

アプリ構成の設定には、次のような項目が含まれます：

- メールアプリの設定
- Web ブラウザーの URL の許可または禁止
- 携帯ネットワーク接続経由または Wi-Fi 接続のみでアプリコンテンツの同期を制御するオプション

アプリに表示される設定について詳しくは、アプリ開発者に問い合わせてください。

前提条件

- Google で Android Enterprise セットアップタスクを完了し、Android Enterprise を managed Google Play に接続します。詳しくは、「Android Enterprise」を参照してください。
- Android Enterprise アプリを Citrix Endpoint Management に追加します。詳しくは、「Citrix Endpoint Management へのアプリの追加」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Per-App VPN の要件

Android Enterprise 用の Per-App VPN を作成するには、管理対象の構成デバイスポリシーの設定に加えて、追加の手順を実行する必要があります。また、次の前提条件が満たされていることを確認する必要があります：

- オンプレミスの Citrix Gateway
- 次のアプリケーションがデバイスにインストールされています：

  - Citrix SSO
  - Citrix Secure Hub

AE デバイスの Per-App VPN を構成するための一般的なワークフローは次のとおりです:

1. この記事の説明に従って VPN プロファイルを構成します。
2. Per-App VPN からのトラフィックを受け入れるように Citrix ADC を構成します。詳しくは、「Citrix Gateway での完全 VPN のセットアップ」を参照してください。

制限事項

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

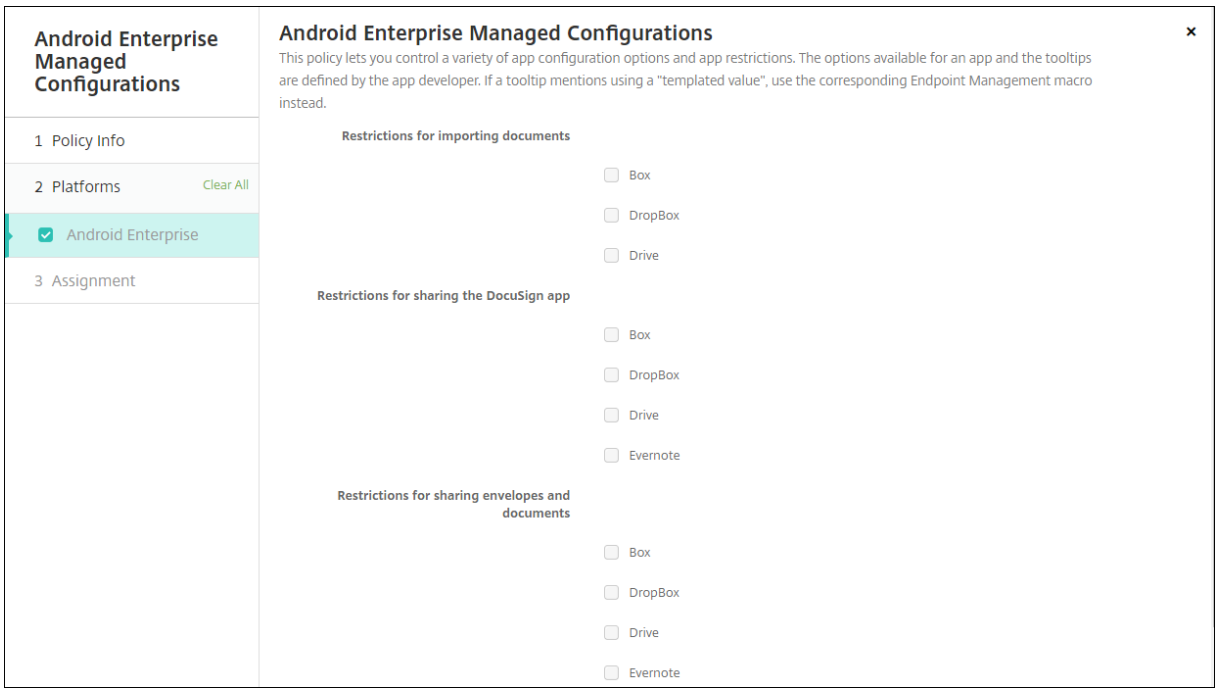
- 許可/拒否リストに含まれるアプリが、VPN セッションの開始後にデバイスに展開された場合、アプリが VPN セッションでトラフィックをルーティングできるようにするには、エンドユーザーが VPN セッションを再起動する必要があります。
- エンドユーザーは、Per-App VPN が Always On VPN セッションで使用している場合に、アプリのトラフィックが VPN セッションでルーティングされるようにするには、デバイスに新しいアプリをインストールした後、仕事用プロファイルを再起動するか、デバイスを再起動する必要があります。

> 注:
>
> これらの制限は、Android 向け Citrix SSO 23.8.1 以降のバージョンを使用している場合には適用されません。詳しくは、「Automatic restart of Always On VPN」を参照してください。

Android Enterprise の設定

管理対象の構成デバイスポリシーを追加することを選択すると、アプリを選択するように促すメッセージが表示されます。Android Enterprise アプリが Citrix Endpoint Management に追加されていない場合は、続行できません。

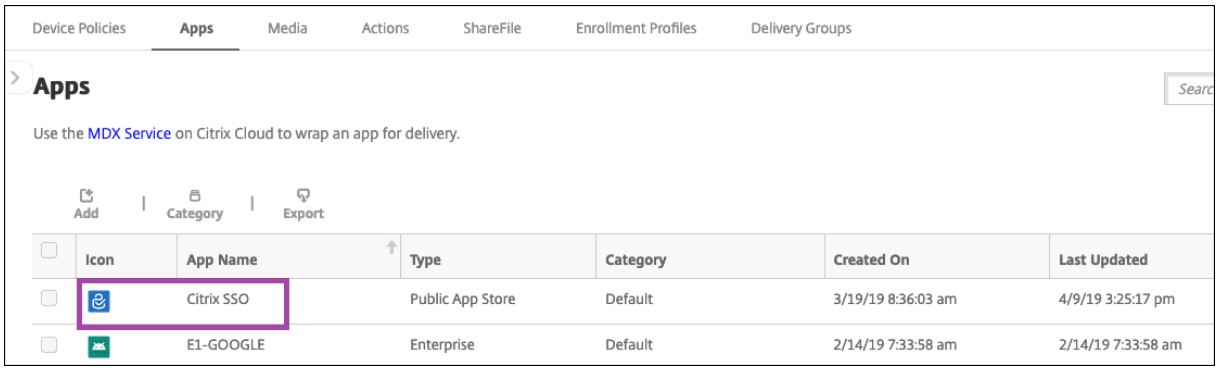
アプリを選択した後、ポリシー設定を構成します。設定は各アプリに固有です。



Android Enterprise に対する **VPN** プロファイルの構成

管理された構成のデバイスポリシーに基づき、Citrix SSO アプリを使用して VPN プロファイルを Android Enterprise デバイスで使用できるようにします。

最初に、Google Play ストアアプリとして Citrix SSO を Citrix Endpoint Management コンソールに追加します。「パブリックアプリストアのアプリの追加」を参照してください。



詳しくは、このビデオをご覧ください:

Citrix SSO に対する **Android Enterprise** 管理対象の構成の作成

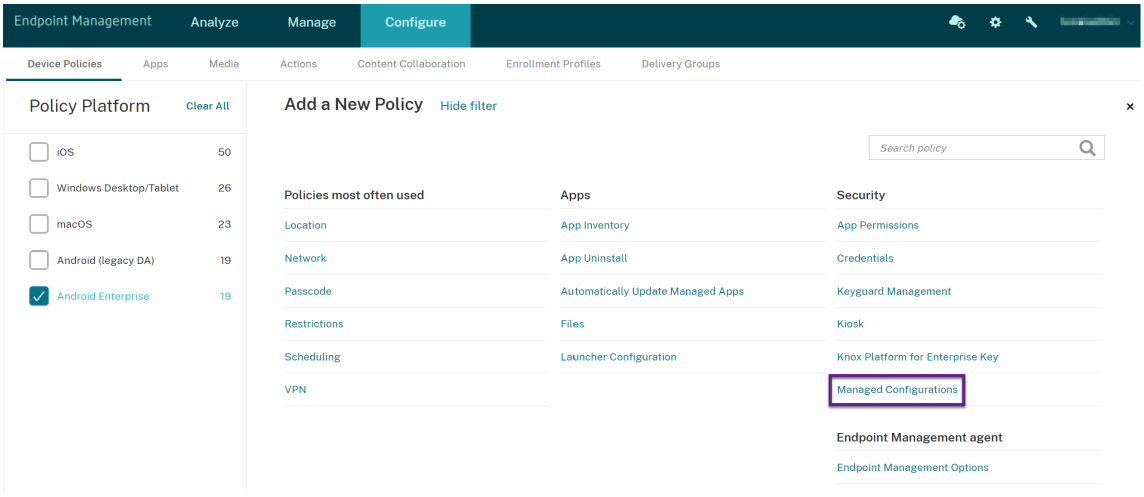
VPN プロファイルを作成するため、Citrix SSO に対する管理対象の構成デバイスポリシーを構成します。Citrix SSO アプリがインストールされており、ポリシーが展開されているデバイスは、作成した VPN プロファイルにアクセスできます。

Citrix Endpoint Management は、次の場合にデバイスキーストアのユーザー証明書を使用します:

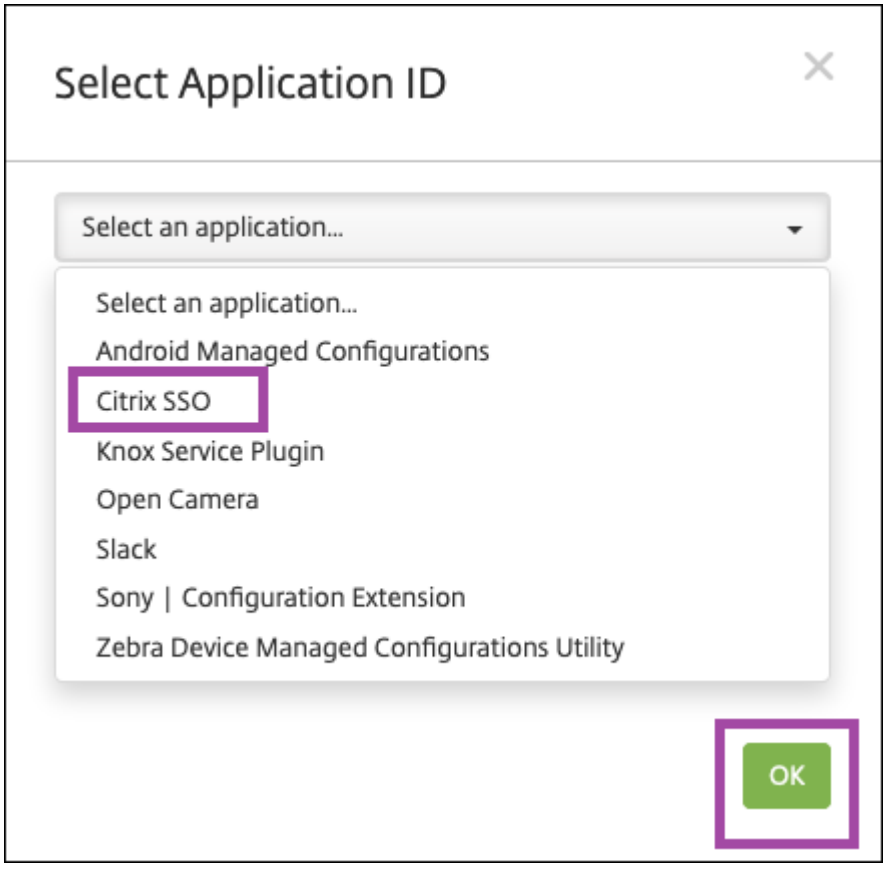
- 証明書ベースの認証用に Citrix Gateway が構成されている。
- Citrix Endpoint Management ページの ［設定］**>** ［**Citrix Gateway**］で、［認証用のユーザー証明書を配信］が有効になっている。

Citrix Gateway の完全修飾ドメイン名とポートが必要です。

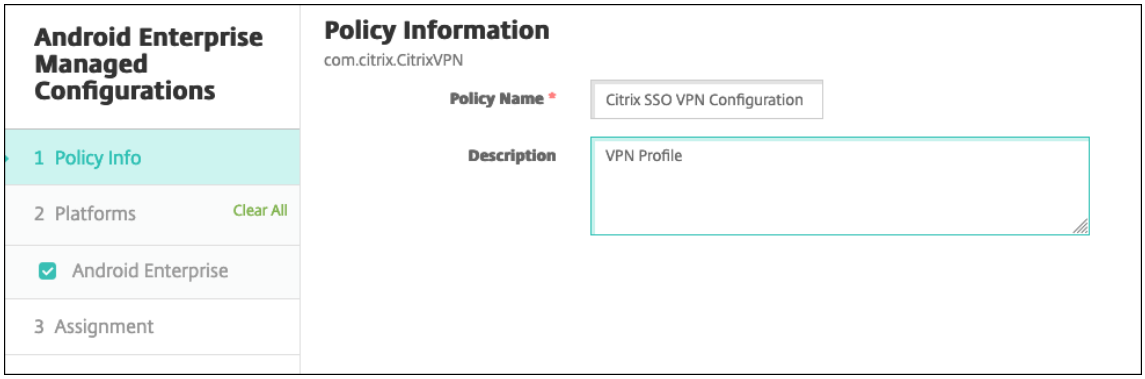
1. Citrix Endpoint Management コンソールで、［構成］**>** ［デバイスポリシー］の順にクリックします。［追加］をクリックします。
2. ［**Android Enterprise**］を選択します。［管理対象の構成］をクリックします。



3. ［アプリケーション **ID** の選択］ウィンドウが表示されたら、リストから ［**Citrix SSO**］をクリックし、［**OK**］をクリックします。



4. Citrix SSO VPN 構成の名前と説明を入力します。［次へ］をクリックします。



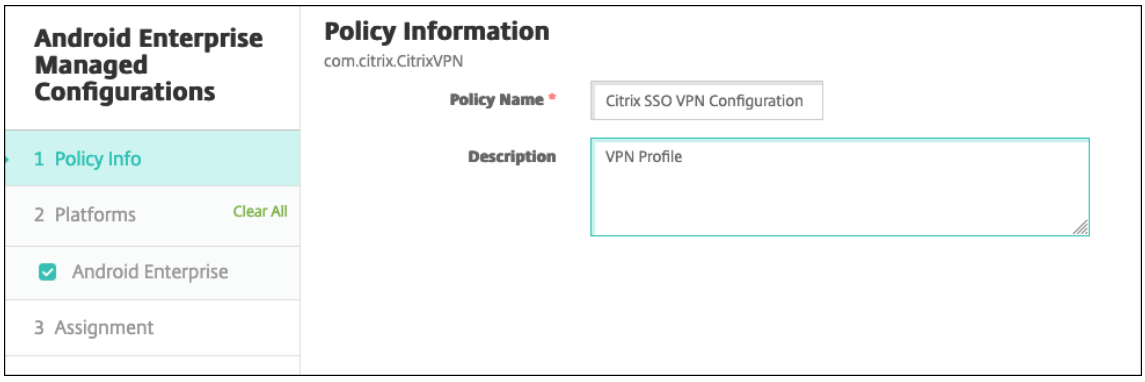
5. VPN プロファイルパラメーターを構成します。

   - **VPN** プロファイル名： VPN プロファイルの名前を入力します。複数の VPN プロファイルを作成している場合は、それぞれに一意の名前を使用します。名前を入力しないと、［サーバーアドレス］フィールドに入力したアドレスが VPN プロファイル名として使用されます。
   - サーバーアドレス（*）： Citrix Gateway の完全修飾ドメイン名を入力します。Citrix Gateway のポートが 443 ではない場合は、ポートも入力します。URL 形式を使用します。たとえば、`https://gateway.mycompany.com:8443`のようにします。
   - ユーザー名（オプション）：エンドユーザーが Citrix Gateway の認証に使用するユーザー名を入力します。このフィールドには、Citrix Endpoint Management マクロ {user.username} を使用できます。（「マクロ」を参照）。ユーザー名を入力しないと、Citrix Gateway への接続時にユーザー名の入力を求められます。
   - パスワード（オプション）：エンドユーザーが Citrix Gateway の認証に使用するパスワードを入力します。パスワードを入力しないと、Citrix Gateway への接続時にユーザーがパスワードの入力を求められます。
   - 証明書のエイリアス（オプション）：証明書のエイリアスを入力します。証明書のエイリアスを使用すると、アプリが証明書にアクセスしやすくなります。資格情報デバイスポリシーで同じ証明書エイリアスを使用すると、ユーザーが操作しなくても、アプリが証明書を取得して VPN を認証します。
   - ゲートウェイ証明書 **PIN**（オプション）：NetScaler Gateway に使用される証明書 PIN を記述する JSON オブジェクトです。値の例：`{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`。詳しくは、「NetScaler Gateway certificate pinning with Android Citrix SSO」を参照してください。
   - **Per-App VPN** の種類（オプション）： Per-App VPN を使用してこの VPN を使用するようにアプリを制限している場合、この設定を構成できます。［許可］を選択した場合、［**Per-App VPN** アプリ一覧］に含まれるアプリパッケージ名のネットワークトラフィックが VPN を介してルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN 外でルーティングされます。［許可しない］を選択した場合、［**Per-App VPN** アプリ一覧］に含まれるアプリパッケージ名のネットワークトラフィ

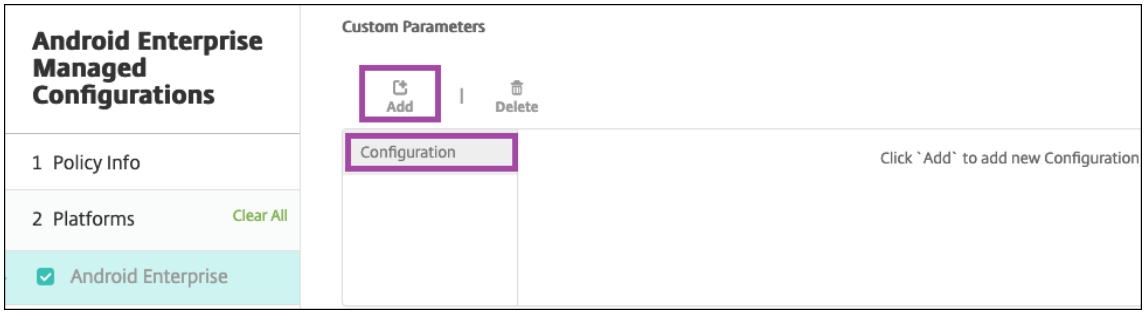
ックが VPN 外でルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN を介してルーティングされます。デフォルトは ［許可］です。

- **PerAppVPN** アプリ一覧：［**Per-App VPN** の種類］の値に応じ、トラフィックが VPN で許可されるか禁止されるアプリの一覧。アプリパッケージ名がカンマまたはセミコロンで区切って一覧にされます。アプリパッケージ名は大文字と小文字が区別され、この一覧でも Google Play ストアに表示されているのと同じように表示される必要があります。この一覧はオプションです。デバイス全体の VPN をプロビジョニングする場合は、この一覧を空のままにします。
- デフォルトの **VPN** プロファイル：ユーザーが特定のプロファイルではなく、Citrix SSO アプリで接続スイッチをタップした場合に使用する VPN プロファイルの名前を入力します。このフィールドを空白のままにすると、メインプロファイルが接続に使用されます。構成されているプロファイルが 1 つだけの場合は、それがデフォルトプロファイルに設定されます。常時 VPN の場合、このフィールドは常時 VPN を確立するために使用する VPN プロファイル名に設定する必要があります。
- ユーザープロファイルの無効化：この設定が［オン］の場合、ユーザーは自分のデバイスで独自の VPN を作成できません。この設定が［オフ］の場合、ユーザーは自分のデバイスで独自の VPN を作成できます。デフォルトは［オフ］です。
- 信頼されていないサーバーをブロックする：次のシナリオのいずれかでこの設定が［オフ］になります：
  - Citrix Gateway で自己署名証明書を使用している場合
  - Cittrix Gateway の証明書を発行する証明機関のルート証明書がシステムの証明機関リストに含まれていない場合

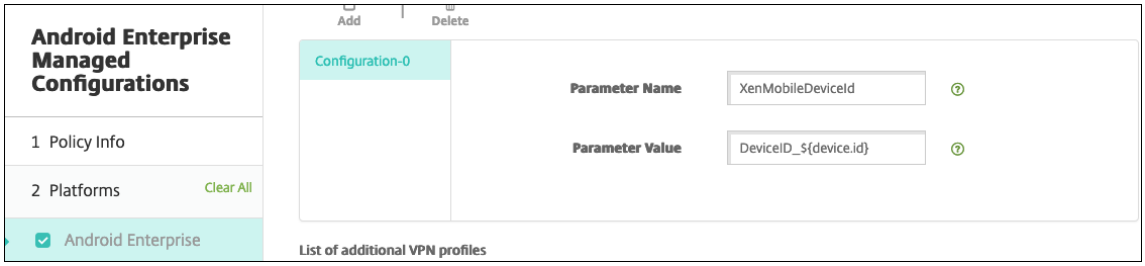
  この設定が［オン］の場合、Citrix Gateway の証明書は Android オペレーティングシステムによって検証されます。検証に失敗した場合、接続は許可されません。デフォルトの値は［オン］です。



6. オプションで、カスタムパラメーターを作成します。カスタムパラメーター **XenMobileDeviceId** および **UserAgent** がサポートされています。現在の VPN 設定を選択し、［追加］をクリックします。

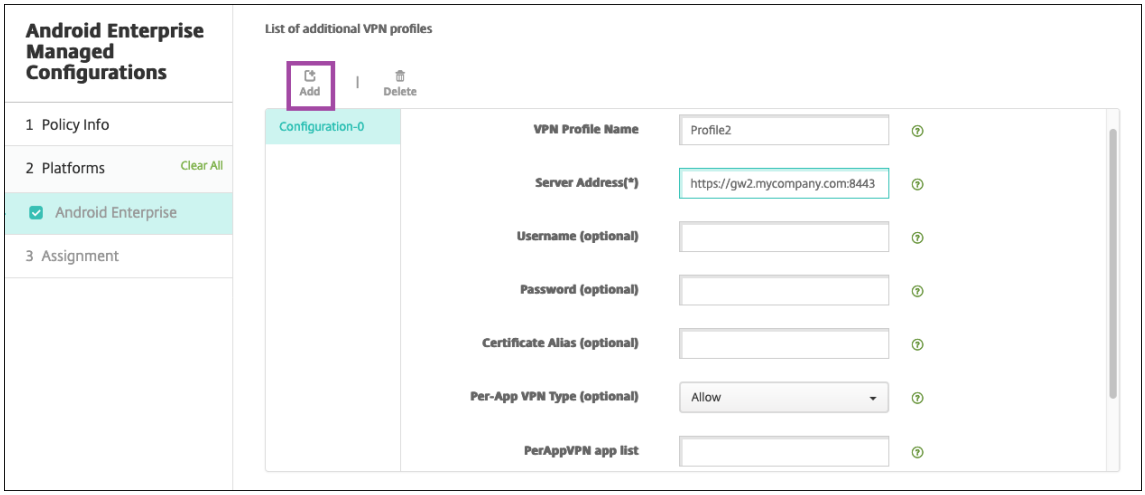


パラメーター名	説明	Value
XenMobileDeviceId	このフィールドは、Citrix Endpoint Management でのデバイス登録に基づくネットワークアクセスチェックに使用するデバイス ID です。デバイスが Citrix Endpoint Management で登録および管理されている場合、VPN 接続は許可されます。登録および管理されていない場合、認証は VPN の確立時に拒否されます。	Citrix Endpoint Management でデバイスの登録および管理状態を特定できるよう、XenMobileDeviceID の値が`DeviceID_${ device.id }`に設定されます。
UserAgent	このテキストは、Citrix Gateway への追加チェックを実行するため、User-Agent HTTP ヘッダーに追加されます。このテキストの値は、Citrix Gateway との通信時に Citrix SSO アプリによって User-Agent HTTP ヘッダーに追加されます。	User-Agent HTTP ヘッダーに追加する任意のテキストを入力します。このテキストは、User-Agent HTTP の指定に準拠している必要があります。
EnableDebugLogging	Citrix SSO アプリでデバッグのログを有効にすると、Always On VPN の場合に VPN 接続の問題が発生したときのトラブルシューティングに役立ちます。このオプションは、管理対象の VPN 構成のいずれかで有効にすることができます。デバッグのログは、管理対象の構成を処理するときに有効になります。	**True**：デバッグのログを有効にします。デフォルト値：**False**



別のカスタムパラメーターを作成するには、再び ［追加］をクリックします。

7. オプションで、追加の VPN プロファイル構成を作成します。構成リストで ［追加］をクリックします。新しい構成がリストに表示されます。新しい構成を選択し、手順 5 と、オプションで手順 6 を繰り返します。



8. 必要な VPN プロファイルをすべて作成したら、**[次へ]** をクリックします。
9. Citrix SSO に対するこの管理対象構成の展開規則を構成します。
10. ［保存］をクリックします。

Citrix SSO に対するこの管理対象構成が、構成済みデバイスポリシーのリストに表示されます。

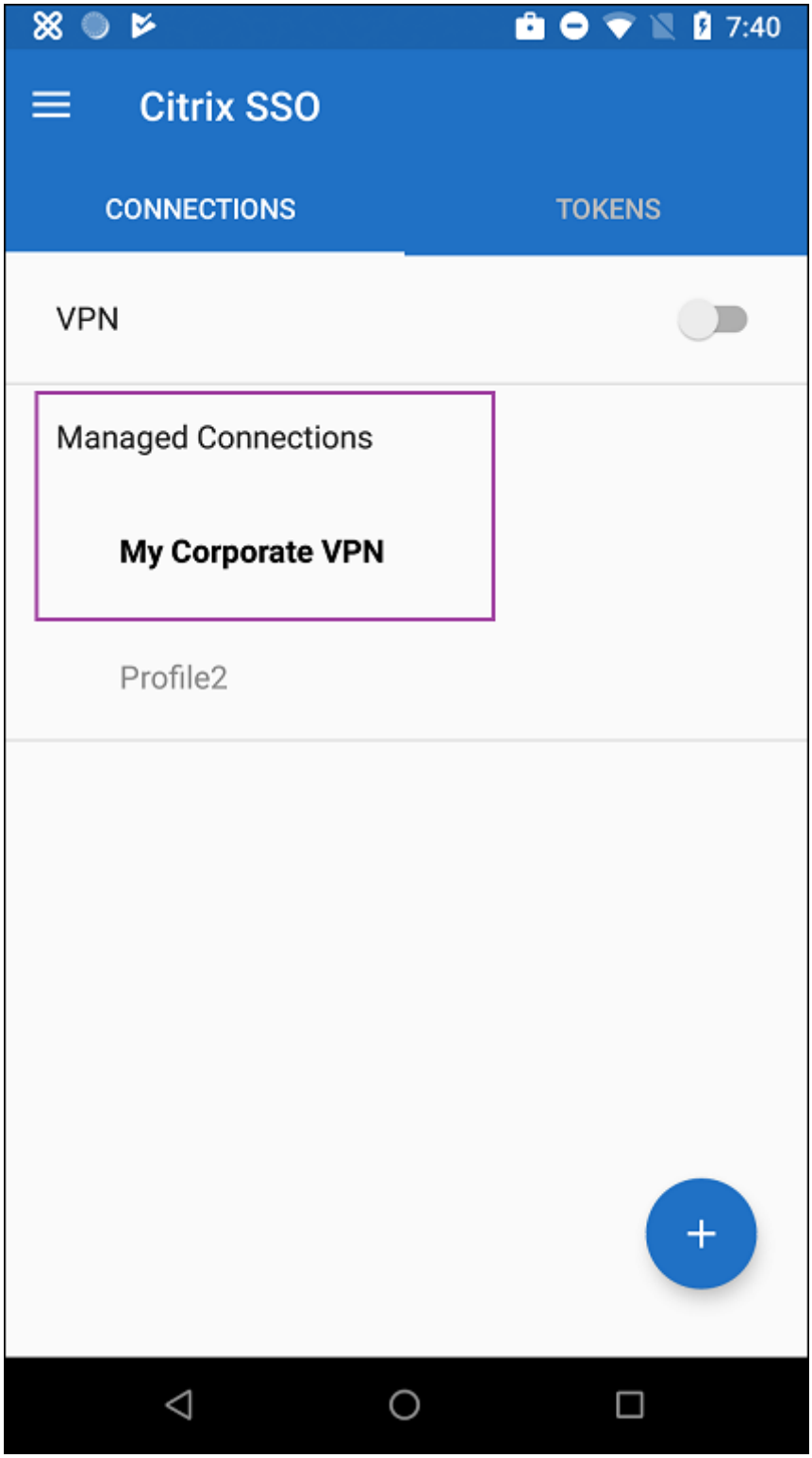
構成した VPN プロファイルの常時接続を有効にするには、「Citrix Endpoint Management オプションデバイスポリシー」を設定します。

> 注:
>
> Android Enterprise で VPN 常時接続にするには、Citrix Secure Hub 19.5.5 以降が必要です。

デバイスから **VPN** プロファイルへのアクセス

作成した VPN プロファイルにアクセスするには、Android Enterprise ユーザーが管理対象 Google Play ストアから Citrix SSO をインストールします。

構成した 1 つまたは複数の VPN プロファイルが、アプリの ［管理接続］領域に表示されます。ユーザーは VPN プロファイルをタップし、その VPN プロファイルを使用して接続します。



ユーザーが認証され、接続されると、VPN プロファイルの横にチェックマークが表示されます。鍵のアイコンは、VPN に接続されていることを示します。

Zebra OEMConfig を使用した **Zebra Android** デバイスの管理

Zebra Technologies の OEMConfig 管理ツールを使用して Zebra Android デバイスを管理します。Zebra OEMConfig アプリについて詳しくは、Zebra Technologies の Web サイトを参照してください。

Citrix Endpoint Management は、Zebra OEMConfig バージョン 9.2 以降をサポートしています。Zebra OEMConfig をデバイスにインストールするためのシステム要件については、Zebra Technologies の Web サイトでOEMConfig Setup を参照してください。

現在、次の Zebra デバイスがサポートされています:

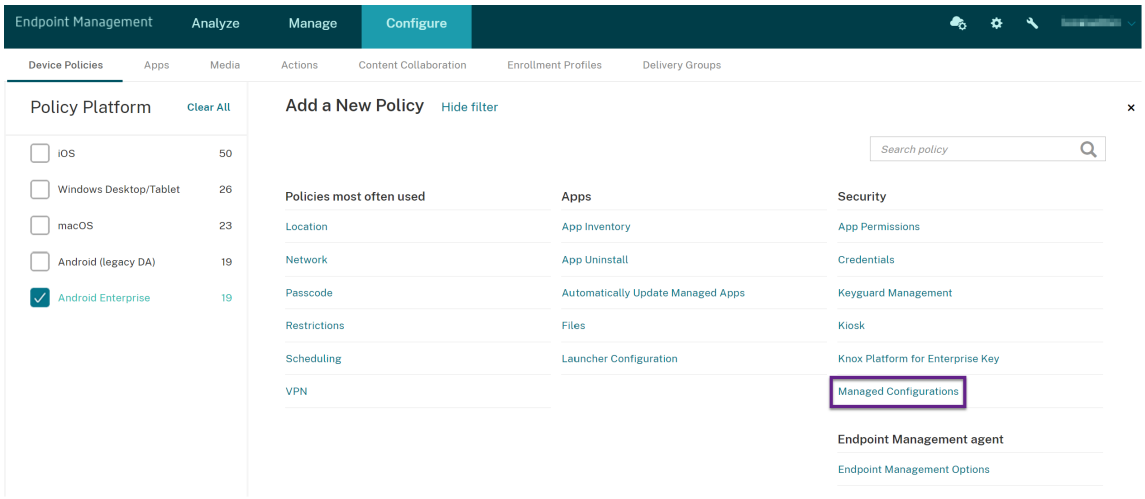
- EC50、EC55、ET56
- TC52x、TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

最初に、Google Play ストアアプリとして Zebra OEMConfig アプリを Citrix Endpoint Management コンソールに追加します。「パブリックアプリストアのアプリの追加」を参照してください。

Zebra OEMConfig アプリに対する **Android Enterprise** 管理対象の構成の作成

Zebra OEMConfig アプリの管理対象の構成デバイスポリシーを設定します。このポリシーは、Zebra OEMConfig アプリがインストールされ、ポリシーが展開されている Zebra デバイスに適用されます。

1. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］の順にクリックします。［追加］をクリックします。
2. ［**Android Enterprise**］を選択します。［管理対象の構成］をクリックします。



3. ［アプリケーション **ID** の選択］ウィンドウが表示されたら、一覧から ［**ZebraOEMConfig powered by MX**］を選択し、［**OK**］をクリックします。

4. Zebra OEMConfig 構成の名前と説明を入力します。［次へ］をクリックします。
5. Zebra OEMConfig 構成の名前を入力します。
6. 使用可能なパラメーターを構成します。例:
    - デバイスの前面にあるカメラを無効にするには、［**Camera Configuration**］を選択し ［**Use of Front Camera**］を ［**Off**］に設定します。
    - デバイスの時刻形式を変更するには、［**Clock Configuration**］を選択し ［**Time Format**］を **12**（12 時間）または **24**（24 時間）に設定します。

使用可能なすべての構成の一覧と説明については、Zebra Technologies の Web サイトでZebra Managed Configurationsを参照してください。

1. オプションで、追加の Zebra OEMConfig 構成を作成します。構成リストで ［追加］をクリックします。新しい構成がリストに表示されます。新しい構成を選択し、パラメーターを設定します。
2. 必要な Zebra OEMConfig 構成をすべて作成し、［**Next**］をクリックします。
3. Zebra OEMConfig に対するこの管理対象構成の展開規則を構成します。
4. ［保存］をクリックします。

管理対象ドメインデバイスポリシー

September 17, 2021

メールおよび Safari ブラウザーに適用する管理対象ドメインを定義できます。管理対象ドメインを使用すると、Safari を使用してドメインからダウンロードしたドキュメントを開くことができるアプリを制御して、会社のデータを保護することができます。

iOS 監視対象デバイスの場合は、以下を指定します:

- ユーザーがドキュメント、添付ファイル、および Web ブラウザーからのダウンロードファイルを開く方法を制御する URL またはサブドメイン。
- ユーザーが Safari でパスワードを保存できる URL。

iOS デバイスを監視モードに設定する方法について詳しくは、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。

ドキュメント、添付ファイル、ダウンロードファイルなどのアイテムの場合: ユーザーが Safari を使用して、管理対象 Web ドメイン一覧に含まれている Web ドメインから取得したアイテムを開くと、適切な社内アプリによってア

イテムが開かれます。アイテムが管理対象 Web ドメイン一覧にある Web ドメインから取得されたものでない場合、ユーザーは社内アプリでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリを使用する必要があります。

管理対象デバイスの場合（Safari パスワード自動入力ドメインを指定しない場合でも）：デバイスがエフェメラルマルチユーザーとして構成されている場合、ユーザーはパスワードを保存できません。ただし、デバイスがエフェメラルマルチユーザーとして構成されていない場合、ユーザーはすべてのパスワードを保存できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

ドメインの指定方法

形式	説明
example.com	example.comのすべてのパスを管理対象として扱いますが、site.example.com/は
foo.example.com	foo.example.comのすべてのパスを管理対象として扱いますが、example.com/とb
*.example.com	foo.example.comまたはbar.example.comのすべてのパスを管理対象として扱いま
example.com/sub	example.com/subとそのすべてのパスを管理対象として扱いますが、example.com/
foo.example.com/sub	foo.example.com/subのすべてのパスを管理対象として扱いますが、example.com
*.example.com/sub	foo.example.com/subまたはbar.example.com/subのすべてのパスを管理対象

規則

- ドメインの比較時に URL の前半部の「www.」および末尾のスラッシュは無視されます。
- エントリにポート番号が含まれる場合は、そのポート番号を指定しているアドレスのみが管理対象と見なされます。ポート番号が含まれない場合は、標準のポートが管理対象と見なされます（http の場合はポート 80、https の場合はポート 443）。たとえば、*.example.com:8080というパターンはhttps://site.example.com:8080/page.htmlと一致しますが、https://site.example.com/page.htmlとは一致しません。これに対して、*.example.comというパターンは、https://site.example.com/page.htmlとhttps://site.example.com/page.htmlとは一致しますが、https://site.example.com:8080/page.htmlとは一致しません。
- 管理対象の Safari Web ドメインの定義は蓄積されます。URL リクエストとの照合には、すべての管理対象 Safari Web ドメインのペイロードで定義されたパターンが使用されます。

設定：

- 管理対象ドメイン

  - マークされていないメールドメイン：一覧に含めるメールドメインごとに、［追加］をクリックして以下の操作を行います。
    * 管理対象のメールドメイン：メールドメインを入力します。
    *［保存］をクリックしてメールドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
  - 管理対象の **Safari Web** ドメイン：一覧に含める Web ドメインごとに、［追加］をクリックして以下の操作を行います。
    * 管理対象の **Web** ドメイン： Web ドメインを入力します。
    *［保存］をクリックして Web ドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
  - **Safari** のパスワードオートフィルドメイン：一覧に含める自動入力ドメインごとに、［追加］をクリックして以下の操作を行います。
    * **Safari** のパスワードオートフィルドメイン：自動入力ドメインを入力します。
    *［保存］をクリックして自動入力ドメインを保存するか、［キャンセル］をクリックして自動入力ドメインを取り消します。

- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

最大常駐ユーザー数デバイスポリシー

November 29, 2023

最大常駐ユーザー数デバイスポリシーは、iOS（iPadOS）を実行している共有デバイス用の機能です。共有 iPad について詳しくは、「Apple の教育向け機能との統合」を参照してください。

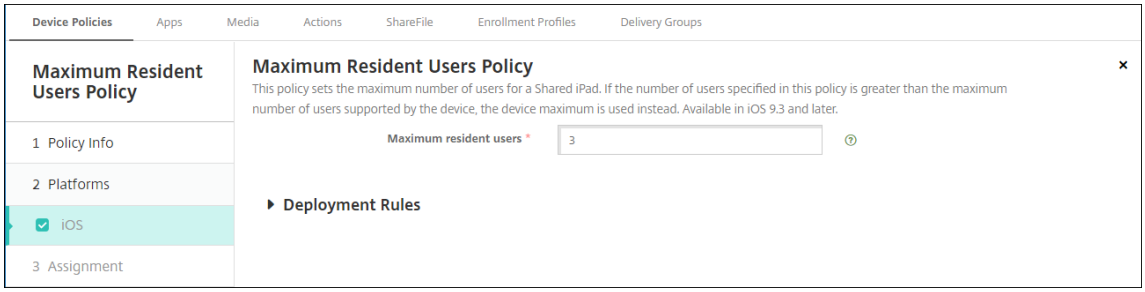
このポリシーは、設定アシスタントの実行中に iPad が「設定待ち」の段階にあるときに展開する必要があります。Apple により、このポリシーを共有 iPad の登録後に展開することは禁止されています。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 最大常駐ユーザー数：共有 iPad の最大ユーザー数。このポリシーで指定したユーザー数がデバイスでサポートされる最大ユーザー数を超えている場合、Citrix Endpoint Management ではデバイスの最大ユーザー数を使用します。デフォルトは **5** ユーザーです。

  Apple により、［最大常駐ユーザー数］の値はできるだけ小さくすることが推奨されています。値を小さくすると、各ユーザーの iPad ストレージ容量が最大になります。また、値を小さくすることで iCloud との通信回数が最小限に抑えられるため、サインインにかかる時間が短縮されます。iPad 上での Apple による共有ストレージの取り扱いについては、「https://developer.apple.com/education/shared-ipad/」を参照してください。



MDM オプションデバイスポリシー

November 29, 2023

MDM オプションデバイスポリシーでは、監視対象の iOS デバイスで［iPhone/iPad を探す］の［アクティベーションロック］を管理することができます。iOS デバイスを監視モードに設定する方法について詳しくは、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

アクティベーションロックは、紛失したり盗まれたりした管理対象デバイスが再アクティブ化されないようにすることを目的とした［iPhone/iPad を探す］の機能です。アクティベーションロックでは、ユーザーの Apple ID とパスワードを入力してからでないと、［iPhone/iPad を探す］をオフにしたり、デバイスを消去したり、デバイスを再アクティブ化したりすることはできません。組織所有のデバイスの場合は、デバイスのリセットや再割り当てなどを行う際にアクティベーションロックをバイパスする必要があります。

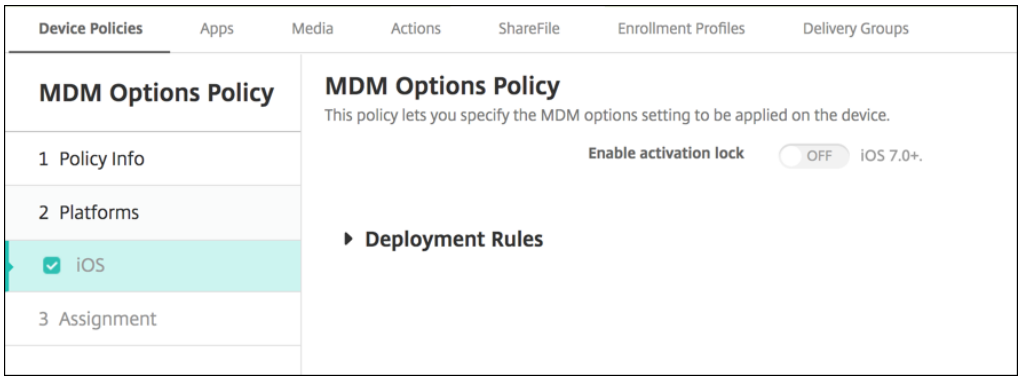
アクティベーションロックを有効にするには、Citrix Endpoint Management の MDM オプションデバイスポリシーを構成し、展開します。これにより、ユーザーの Apple 資格情報なしで、Citrix Endpoint Management コンソールからデバイスを管理できるようになります。アクティベーションロックで必要な Apple 資格情報の入力を省略するには、Citrix Endpoint Management コンソールで［アクティベーションロックバイパス］セキュリティ操作を発行します。

たとえば、紛失した iPhone がユーザーによって返却された場合や、フルワイプの前後にデバイスを設定する場合、iPhone で Apple App Store アカウントの資格情報を求められた際に、Citrix Endpoint Management コンソー

ルで［アクティベーションロックバイパス］セキュリティ操作を発行することでこの手順を省略することができます。

このポリシーを追加または構成するには、［構成］>［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- アクティベーションロックを有効化：このポリシーを展開するデバイスでアクティベーションロックを有効にするかどうかを選択します。デフォルトは ［オフ］です。

MDM オプションデバイスポリシーを展開してアクティベーションロックを有効にした後：［管理］>［デバイス］ページで該当するデバイスを選択し、［セキュリティ］をクリックすると、セキュリティ操作の ［アクティベーションロックバイパス］が表示されます。アクティベーションロックバイパスを使用すると、デバイスユーザーの Apple ID とパスワードがわからなくても、デバイスをアクティブ化する前に管理対象デバイスからアクティベーションロックを削除することができます。フルワイプの前または後に、デバイスにアクティベーションロックバイパスを送信できます。詳細については、「iOS アクティベーションロックのバイパス」を参照してください。

ネットワークデバイスポリシー

March 15, 2024

ネットワークデバイスポリシーを使用すると、次の項目を定義して、ユーザーがデバイスを Wi-Fi ネットワークに接続する方法を管理できます：

- ネットワーク名と種類
- 認証およびセキュリティポリシー
- プロキシサーバーの使用
- その他の Wi-Fi 関連の詳細

このポリシーを追加または構成するには、［構成］>［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

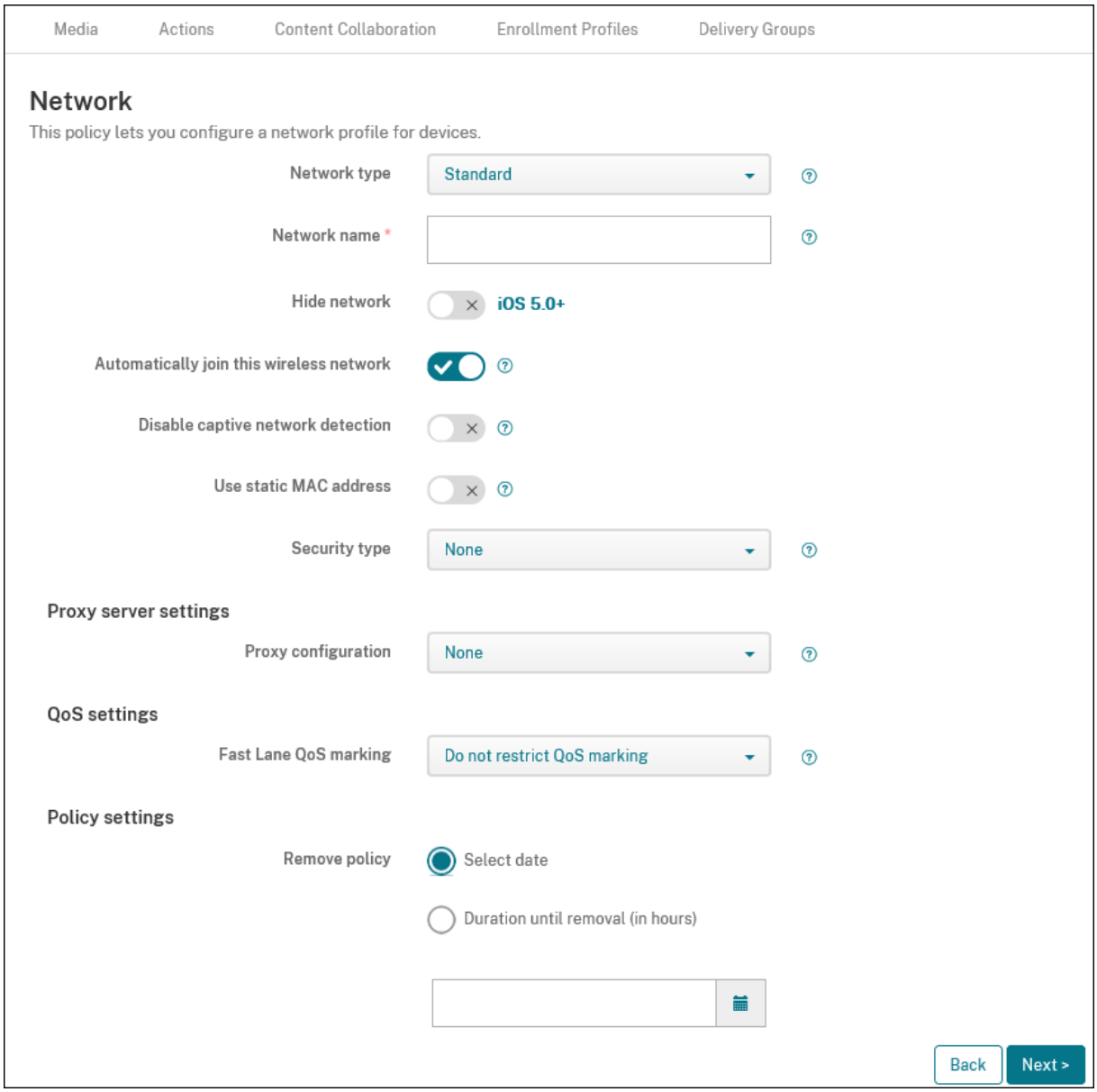
前提条件

ポリシーを作成する前に、以下を完了してください:

- 使用する予定のデリバリーグループを作成します。
- ネットワークの名前と種類を確認します。
- 使用する予定の認証またはセキュリティの種類を確認します。
- 必要な場合、プロキシサーバーの情報を確認します。
- 必要な CA 証明書をインストールします。
- 必要な共有キーを取得します。
- 証明書に基づいた認証のために PKI エンティティを作成します。
- 資格情報プロバイダーを構成します。

詳しくは、「認証」とそのサブ記事を参照してください。

iOS の設定



- ネットワークの種類：一覧で、[標準]、[従来のホットスポット]、または ［**Hotspot 2.0**］を選択して、使用するネットワークの種類を設定する必要があります。
- ネットワーク名：デバイスで使用可能なネットワークの一覧に表示される SSID を入力します。**Hotspot 2.0** には適用されません。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。
- このワイヤレスネットワークに自動的に参加：デバイスが自動でネットワークに参加するかどうかを選択します。デバイスが別のネットワークに接続されている場合は、このネットワークには参加しません。ユーザーは、デバイスが自動的に接続する前に、以前のネットワークから切断する必要があります。デフォルトは ［オン］

です。

- キャプティブネットワークの検出を無効にする：キャプティブネットワークアシスタントは、ユーザーがサブスクリプションネットワークまたは Wi-Fi ホットスポットネットワークにアクセスできるようにします。通常、これらのネットワークは、コーヒーショップ、ホテル、その他の公共の場所にあります。［オン］の場合、デバイスはキャプティブネットワークに接続できますが、ユーザーは Web ブラウザーを開いて手動でログインする必要があります。デフォルトは ［オフ］です。
- 静的 **MAC** アドレスを使用する： MAC アドレスは、デバイスがネットワーク内で送信する一意の識別子です。プライバシーを強化するために、iOS デバイスと iPadOS デバイスは、ネットワークに接続するたびに異なる MAC アドレスを使用できます。［オン］の場合、デバイスはこのネットワークに接続するときに常に同じ MAC アドレスを使用します。［オフ］の場合、デバイスはこのネットワークに接続するたびに異なる MAC アドレスを使用します。デフォルトは ［オフ］です。
- セキュリティの種類：一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0** には適用されません。
  - なし - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2/WPA3 パーソナル
  - 任意（パーソナル）
  - WEP エンタープライズ
  - WPA/WPA2/WPA3 エンタープライズ：Windows 10 の最新リリースでは、WPA-2 エンタープライズを使用するために Simple Certificate Enrollment Protocol（SCEP）を構成します。SCEP を構成すると、Citrix Endpoint Management から証明書をデバイスに送信して Wi-Fi サーバーを認証することができます。SCEP を構成するには、［設定］**>**［資格情報プロバイダー］の［ディストリビューション］ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。
  - 任意（エンタープライズ）

以下では、上記の接続の種類ごとに、構成するオプションを示します。

- プロキシサーバーの設定
  - プロキシの構成：一覧から、［なし］、［手動］、または ［自動］を選択して VPN 接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルトは ［なし］で、そのほかの構成は不要です。
  - ［手動］を選択した場合は、次の設定を構成します：
    - ホスト名または **IP** アドレス：プロキシサーバーのホスト名または IP アドレスを入力します。
    - ポート：プロキシサーバーのポート番号を入力します。
    - ユーザー名：任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - パスワード：任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［自動］を選択した場合は、次の設定を構成します：
    - サーバー **URL**：プロキシ構成を定義する PAC ファイルの URL を入力します。

    - **PAC** に到達不能である場合は直接接続を許可： PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは ［オン］ です。

- 高速レーン **QoS** マーキング： Cisco の高速レーン QoS をサポートする Wi-Fi ネットワークの QoS マーキングを制限しない場合、すべてのアプリが許可され、L2 および L3 マーキングを使用できます。QoS マーキングを制限する場合は、L2 および L3 マーキングを使用できるアプリを指定します。

  - **QoS** マーキングを有効にする： QoS マーキングを制限する場合、この設定を使用して完全に無効にするか、特定のアプリのみをマークします。［オフ］ の場合、QoS マーキングは完全に無効になります。［オン］ の場合、QoS マーキングを使用できるアプリの一覧を構成します。デフォルトは ［オン］ です。
  - **Apple** オーディオ**/**ビデオ通話を許可：オーディオ/ビデオ通話アプリが QoS マーキングを使用できるかどうかを選択します。［オフ］ の場合、オーディオ/ビデオ通話の品質が悪くなることがあります。
  - 指定したアプリを許可：アプリパッケージ ID をこのリストに追加して、アプリが QoS マーキングを使用できるようにします。

- **Hotspot 2.0** の設定

  - 表示される通信事業者名：ホットスポットデバイスによってブロードキャストされるフレンドリ名。この名前は、使用できる Wi-Fi ネットワークの一覧に表示されます。
  - ドメイン名： Hotspot 2.0 のネゴシエーションに使用するドメイン名。
  - ローミングパートナーのネットワークへの接続を許可：［オン］ の場合、デバイスはホームネットワーク外からのデバイスローミングでパートナーネットワークに接続できます。
  - ローミングコンソーシアムの組織識別子（**OI**）： デバイスがアクセスできる組織識別子の一覧を追加します。ローミングコンソーシアム OI は、共有認証方法を持つ組織に属します。構成しているホットスポットを使用できない場合、デバイスはここに表示されるローミングコンソーシアム OI に接続します。
  - ネットワークアクセス識別子（**NAI**）の領域名：ローミングネットワークのユーザーを識別するのに使用される領域名の一覧を構成します。NAI は`user@realm`の形式で送信します。
  - **Mobile Country Code**（**MCC**）およびモバイルネットワークの構成（**MNC**）： Mobile Country Code は、ネットワークの国を識別する 3 桁の文字で構成されます。Mobile Network Code は、2 桁または 3 桁の一意の文字で構成されます。共に使用すると、MCC/MNC で通信事業者やキャリアが一意に識別されます。

- ポリシー設定

  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］ と ［削除までの期間（時間）を指定］ です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］ または ［許可しない］ を選択します。［パスコードが必要です］ を選択する場合、［削除のパスコード］ フィールドに入力します iOS では使用できません。

iOS の **WPA**、**WPA** パーソナル、任意（パーソナル）の設定

パスワード：任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。

iOS の **WEP** エンタープライズ、**WPA** エンタープライズ、**WPA2** エンタープライズ、**WPA3** エンタープライズ、任意（エンタープライズ）の設定

これらのセキュリティタイプのいずれかを選択すると、**QoS**（サービス品質）設定後に EAP 設定が表示されます。

> 重要：
>
> セキュリティタイプとして **WPA2 Enterprise** を選択する場合は、少なくとも 1 つの EAP プロトコルを許可する必要があります。

- 許容される **EAP** プロトコル：サポートする EAP の種類を有効にして、関連する設定を構成します。使用できる各 EAP の種類のデフォルトは ［オフ］です。
- 内部認証 **(TTLS)**： *TTLS* を有効にする場合にのみ必要です。一覧から、使用する内部認証方法を選択します。オプションは、［**PAP**］、［**CHAP**］、［**MSCHAP**］、または ［**MSCHAPv2**］です。デフォルトは ［**MSCHAPv2**］です。
- **PAC** を使用した **EAP-FAST**：保護されたアクセス資格情報（PAC）を使用するかどうかを選択します。
  - ［**PAC** を使用］を選択した場合は、プロビジョニング PAC を使用するかどうかを選択します。
    - ［**PAC** をプロビジョニング］を選択した場合は、エンドユーザーのクライアントと Citrix Endpoint Management の間で匿名 TLS ハンドシェイクを許可するかどうかを選択します。
      - 匿名で **PAC** をプロビジョニング
- 認証：
  - ユーザー名：ユーザー名を入力します。
  - 接続ごとのパスワード：ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
  - パスワード：任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。
  - **ID** 資格情報（キーストアまたは **PKI** 資格情報）：一覧から、ID 資格情報の種類を選択します。デフォルトは ［なし］です。
  - 外部 **ID**：［**PEAP**］、［**TTLS**］、または ［**EAP-FAST**］を有効にした場合にのみ必要です。画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」などの汎用的な用語を入力して、セキュリティを高めることができます。
  - **TLS** 証明書を要求： TLS 証明書を必須とするかどうかを選択します。
- 信頼
  - 信頼された証明書：信頼された機関からの証明書を追加するには、［追加］をクリックして、追加する証明書ごとに以下の操作を行います。

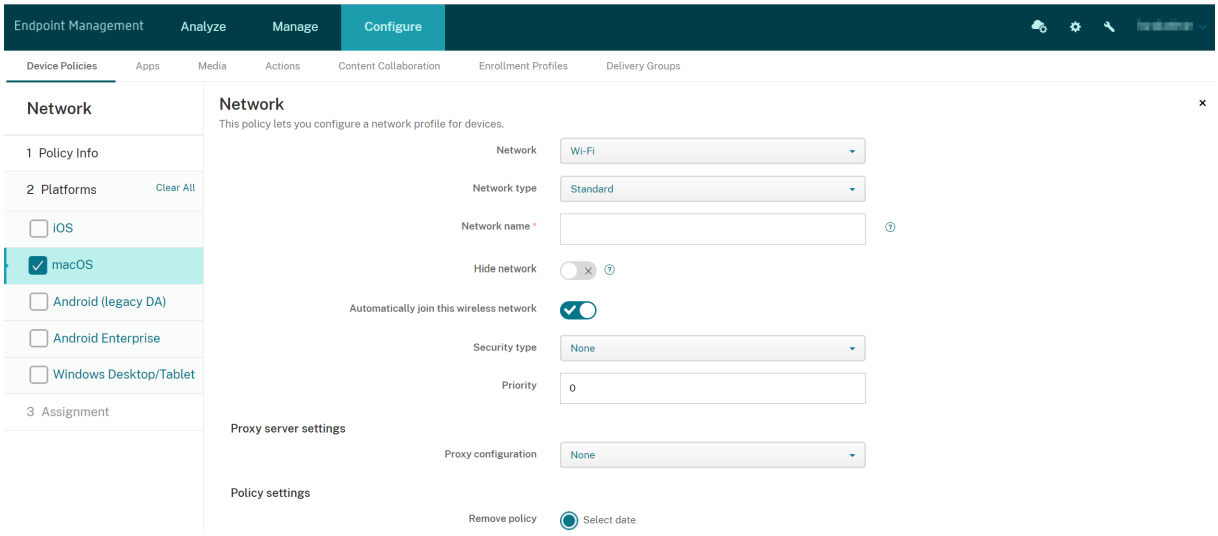
* アプリケーション：一覧から、追加するアプリケーションを選択します。
* ［保存］をクリックして証明書を保存するか、［キャンセル］をクリックします。

– 信頼されたサーバー証明書の名前：信頼されたサーバー証明書の一般名を追加するには、［追加］をクリックして、追加する名前ごとに以下の操作を行います。

* 証明書：サーバー証明書の名前を入力します。ワイルドカード文字を使用して、名前を「wpa.*.example.com」のように指定することができます。
* ［保存］をクリックして証明書名を保存するか、［キャンセル］をクリックします。

- 信頼の例外を許可：証明書が信頼できないときに、デバイスに証明書信頼ダイアログを表示するかどうかを選択します。デフォルトは ［オン］です。

macOS 設定



- ネットワーク：一覧で、使用する予定のネットワークオプションを選択します。デフォルトは **Wi-Fi** です。
  - Wi-Fi
  - グローバルイーサネット
  - 1 番目のアクティブなイーサネット
  - 2 番目のアクティブなイーサネット
  - 3 番目のアクティブなイーサネット
  - 1 番目のイーサネット
  - 2 番目のイーサネット
  - 3 番目のイーサネット
- ネットワークの種類：一覧で、［標準］、［従来のホットスポット］、または ［**Hotspot 2.0**］を選択して、使用するネットワークの種類を設定する必要があります。
- ネットワーク名：デバイスで使用可能なネットワークの一覧に表示される SSID を入力します。**Hotspot 2.0** には適用されません。

- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。
- このワイヤレスネットワークに自動的に参加：ネットワークに自動的に参加するかどうかを選択します。デバイスが既に別のネットワークに接続されている場合は、このネットワークには参加しません。ユーザーは、デバイスが自動的に接続する前に、以前のネットワークから切断する必要があります。デフォルトは ［オン］です。
- セキュリティの種類：一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0** には適用されません。
  - なし - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2 パーソナル
  - 任意（パーソナル）
  - WEP エンタープライズ
  - WPA/WPA2 エンタープライズ
  - 任意（エンタープライズ）

  以下では、上記の接続の種類ごとに、構成するオプションを示します。
- 優先度：複数ネットワークの場合、ネットワーク接続の優先度を定義する数値を入力します。デバイスは、プライオリティ番号が最も低いネットワークに最初に接続します。負の数を入力できます。デフォルトは ［**0**］です。
- プロキシサーバーの設定
  - プロキシの構成：一覧から、［なし］、［手動］、または ［自動］を選択して VPN 接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルトは ［なし］で、そのほかの構成は不要です。
  - ［手動］を選択した場合は、次の設定を構成します：
    - ホスト名または **IP** アドレス：プロキシサーバーのホスト名または IP アドレスを入力します。
    - ポート：プロキシサーバーのポート番号を入力します。
    - ユーザー名：任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - パスワード：任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［自動］を選択した場合は、次の設定を構成します：
    - サーバー **URL**：プロキシ構成を定義する PAC ファイルの URL を入力します。
    - **PAC** に到達不能である場合は直接接続を許可： PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは ［オン］です。
- **Hotspot 2.0** の設定
  - 表示される通信事業者名：ホットスポットデバイスによってブロードキャストされるフレンドリ名。この名前は、使用できる Wi-Fi ネットワークの一覧に表示されます。
  - ドメイン名： Hotspot 2.0 のネゴシエーションに使用するドメイン名。

  - ローミングパートナーのネットワークへの接続を許可：［オン］の場合、デバイスはホームネットワーク外からのデバイスローミングでパートナーネットワークに接続できます。
  - ローミングコンソーシアムの組織識別子（**OI**）：デバイスがアクセスできる組織識別子の一覧を追加します。ローミングコンソーシアム OI は、共有認証方法を持つ組織に属します。構成しているホットスポットを使用できない場合、デバイスはここに表示されるローミングコンソーシアム OI に接続します。
  - ネットワークアクセス識別子（**NAI**）の領域名：ローミングネットワークのユーザーを識別するのに使用される領域名の一覧を構成します。NAI は`user@realm`の形式で送信します。
  - **Mobile Country Code**（**MCC**）およびモバイルネットワークの構成（**MNC**）： Mobile Country Code は、ネットワークの国を識別する 3 桁の文字で構成されます。Mobile Network Code は、2 桁または 3 桁の一意の文字で構成されます。共に使用すると、MCC/MNC で通信事業者やキャリアが一意に識別されます。

- ポリシー設定

  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

macOS の **WPA**、**WPA** パーソナル、**WPA 2** パーソナル、任意（パーソナル）の設定

- パスワード：任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。

macOS の **WEP** エンタープライズ、**WPA** エンタープライズ、**WPA2** エンタープライズ、任意（エンタープライズ）の設定

- 接続モード：［オン］の場合、ユーザーがネットワークに参加するときに使用する接続モードを選択します。デフォルトは ［オフ］です。

  - システム：オンにすると、デバイスはシステムの資格情報を使用してユーザーを認証します。デフォルトはオフにされています。
  - ログインウィンドウ：オンにすると、デバイスはログインウィンドウで入力されたものと同じ資格情報を使用してユーザーを認証します。デフォルトはオフにされています。

これらのセキュリティタイプのいずれかを選択すると、**QoS**（サービス品質）設定後に EAP 設定が表示されます。

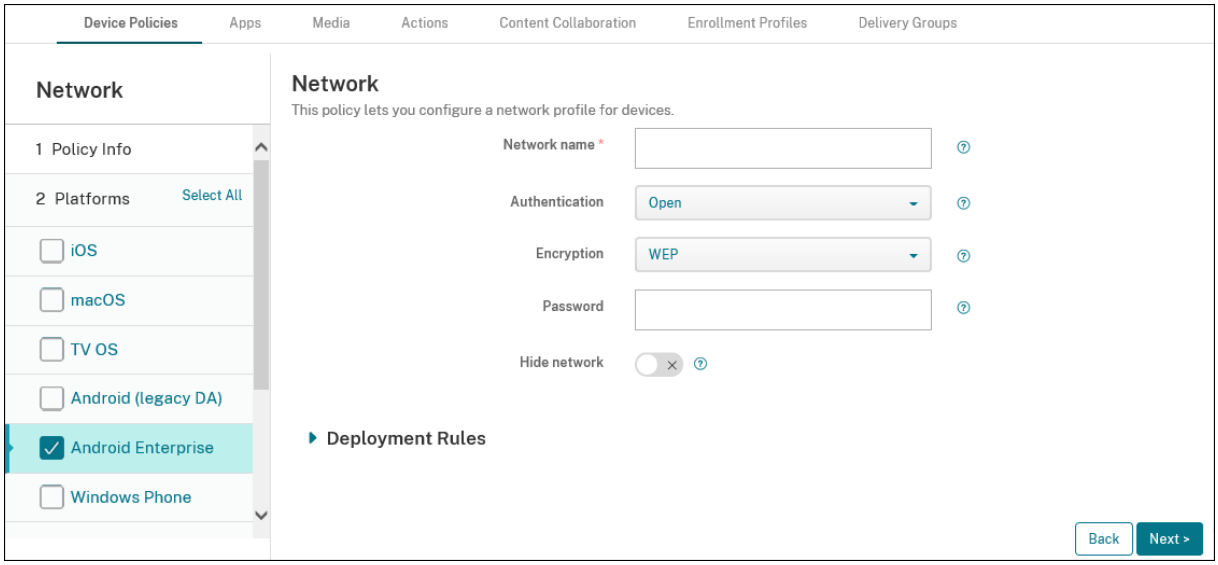
> 重要:
>
> セキュリティタイプとして **WPA2 Enterprise** を選択する場合は、少なくとも 1 つの EAP プロトコルを許可する必要があります。

- 許容される **EAP** プロトコル: サポートする EAP の種類を有効にして、関連する設定を構成します。使用できる各 EAP の種類のデフォルトは ［オフ］です。
- 内部認証 **(TTLS)**: *TTLS* を有効にする場合にのみ必要です。一覧から、使用する内部認証方法を選択します。オプションは、[**PAP**]、[**CHAP**]、[**MSCHAP**]、または ［**MSCHAPv2**］です。デフォルトは ［**MSCHAPv2**］です。
- **PAC** を使用した **EAP-FAST**: 保護されたアクセス資格情報（PAC）を使用するかどうかを選択します。
  - ［**PAC** を使用］を選択した場合は、プロビジョニング PAC を使用するかどうかを選択します。
    - ［**PAC** をプロビジョニング］を選択した場合は、エンドユーザーのクライアントと Citrix Endpoint Management の間で匿名 TLS ハンドシェイクを許可するかどうかを選択します。
      - 匿名で **PAC** をプロビジョニング
- 認証:
  - **Active Directory** 認証を使用する: Active Directory 認証を有効にするかどうかを選択します。macOS 10.7 以降で使用できます。このオプションを使用できるようにするには、次の手順を実行します:
    - ［**PEAP**］を EAP プロトコルとして設定します。
    - プロファイルの対象を［システム］に設定します。この設定オプションは、システム全体にポリシーを適用する場合にのみ使用できます。
  - ユーザー名: ユーザー名を入力します。
  - 接続ごとのパスワード: ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
  - パスワード: 任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。
  - **ID** 資格情報（キーストアまたは **PKI** 資格情報）: 一覧から、ID 資格情報の種類を選択します。デフォルトは ［なし］です。
  - 外部 **ID**: ［**PEAP**］、［**TTLS**］、または ［**EAP-FAST**］を有効にした場合にのみ必要です。画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
  - **TLS** 証明書を要求: TLS 証明書を必須とするかどうかを選択します。
- 信頼
  - 信頼された証明書: 信頼された機関からの証明書を追加するには、［追加］をクリックして、追加する証明書ごとに以下の操作を行います。
    - アプリケーション: 一覧から、追加するアプリケーションを選択します。
    - ［保存］をクリックして証明書を保存するか、［キャンセル］をクリックします。

- 信頼されたサーバー証明書の名前：信頼されたサーバー証明書の一般名を追加するには、［追加］をクリックして、追加する名前ごとに以下の操作を行います。
  * 証明書：追加するサーバー証明書の名前を入力します。ワイルドカード文字を使用して、名前を「wpa.*.example.com」のように指定することができます。
  * ［保存］をクリックして証明書名を保存するか、［キャンセル］をクリックします。

- 信頼の例外を許可：証明書が信頼できないときに、ユーザーデバイスに証明書信頼ダイアログを表示するかどうかを選択します。デフォルトは ［オン］です。

Android Enterprise の設定



- ネットワーク名：ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- 認証：一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - 開く
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下では、上記の接続の種類ごとに、構成するオプションを示します。デフォルトは ［オープン］です。

Android Enterprise のオープン、共有設定

- 暗号化：一覧から、［無効］または ［**WEP**］を選択します。デフォルトは ［**WEP**］です。

- パスワード：任意で、パスワードを入力します。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

Android Enterprise の **WPA**、**WPA-PSK**、**WPA2**、**WPA2-PSK** 設定

- 暗号化：一覧から、［**TKIP**］または［**AES**］を選択します。デフォルトは［**TKIP**］です。
- パスワード：任意で、パスワードを入力します。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

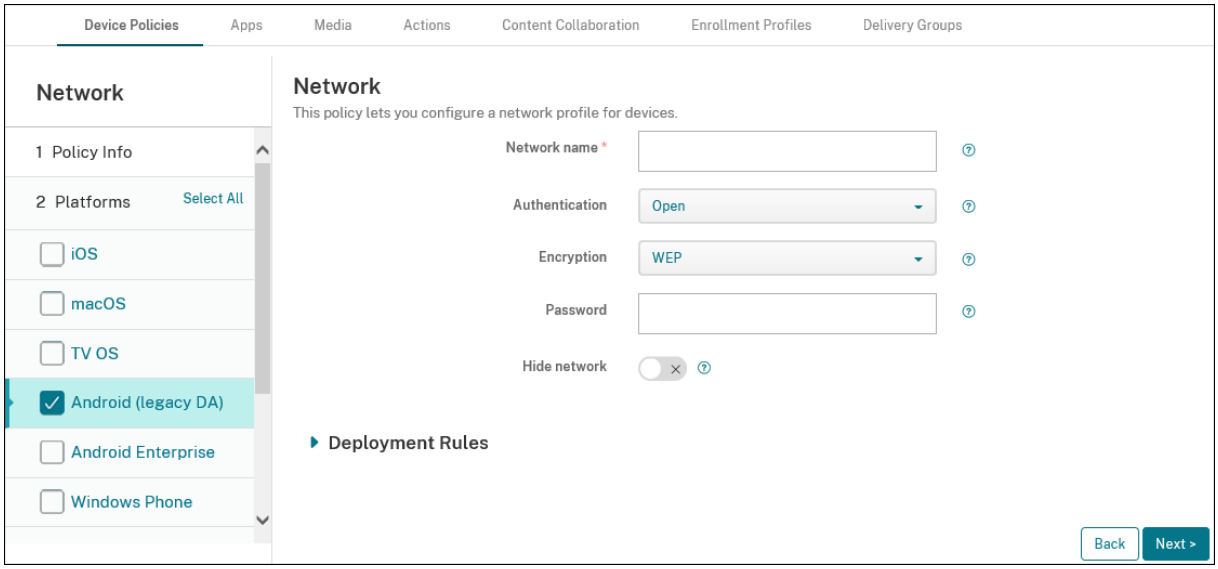
Android Enterprise の **802.1x** 設定

- **EAP** タイプ：一覧から、［**PEAP**］、［**TLS**］、または ［**TTLS**］を選択します。デフォルトは ［**PEAP**］です。
- パスワード：任意で、パスワードを入力します。
- 認証フェーズ **2**：一覧から、［なし］、［**PAP**］、［**MSCHAP**］、［**MSCHAPPv2**］、または ［**GTC**］を選択します。デフォルトは ［**PAP**］です。
- **ID**：オプションのユーザー名およびドメインを入力します。
- 匿名：任意で、画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
- **CA** 証明書：一覧から、使用する証明書を選択します。
- ドメイン：ドメイン名を入力します。詳しくは、「ドメイン」を参照してください。

  > 注：
  >
  > Android 13 以降が実行されているデバイスの Wi-Fi ポリシーを構成する場合、［**CA** 証明書］と ［ドメイン］フィールドは強制的に更新する必要があります。更新しない場合、構成が失敗します。

- **ID** 資格情報：一覧から、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

Android（レガシデバイス管理者）の設定



- ネットワーク名：ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- 認証：一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - 開く
  - 共有（Android Enterprise のみ）
  - WPA（Android Enterprise のみ）
  - WPA-PSK（Android Enterprise のみ）
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Android のオープン、共有設定

- 暗号化：一覧から、［無効］または ［**WEP**］を選択します。デフォルトは ［**WEP**］です。
- パスワード：任意で、パスワードを入力します。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

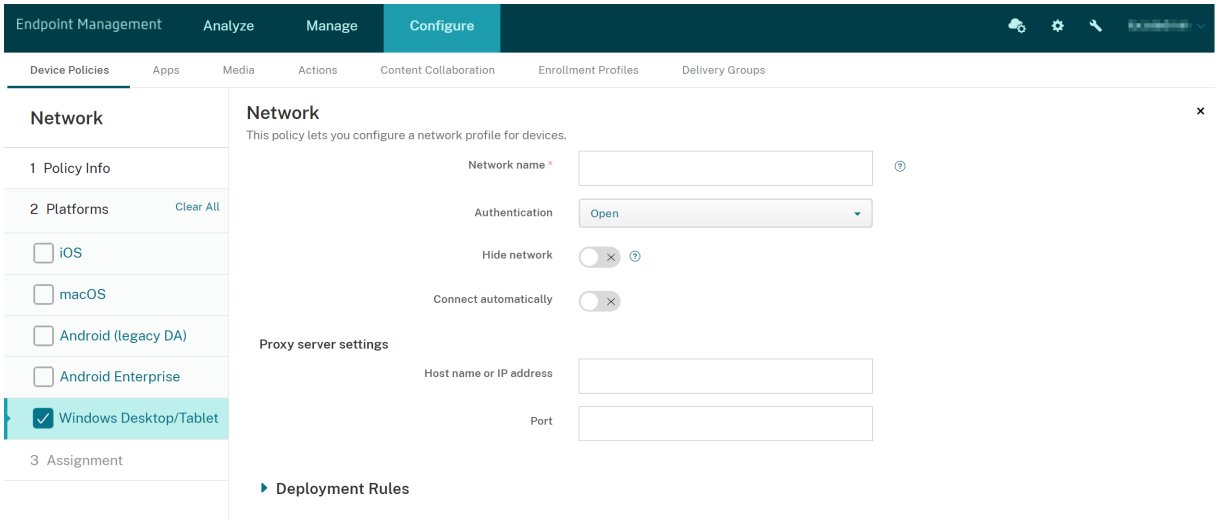
Android の WPA、WPA-PSK、WPA2、WPA2-PSK 設定

- 暗号化：一覧から、［**TKIP**］または［**AES**］を選択します。デフォルトは［**TKIP**］です。
- パスワード：任意で、パスワードを入力します。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

Android の 802.1x 設定

- **EAP** タイプ：一覧から、［**PEAP**］、［**TLS**］、または ［**TTLS**］を選択します。デフォルトは ［**PEAP**］です。
- パスワード：任意で、パスワードを入力します。
- 認証フェーズ **2**：一覧から、［なし］、［**PAP**］、［**MSCHAP**］、［**MSCHAPPv2**］、または ［**GTC**］を選択します。デフォルトは ［**PAP**］です。
- **ID**：オプションのユーザー名およびドメインを入力します。
- 匿名：任意で、画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
- **CA** 証明書：一覧から、使用する証明書を選択します。
- **ID** 資格情報：一覧から、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。

Windows デスクトップ/タブレットの設定



- ネットワーク名：使用可能なネットワークの一覧に表示される SSID。
- 認証：一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - 開く
  - WPA パーソナル
  - WPA-2 パーソナル
  - WPA エンタープライズ
  - WPA-2 エンタープライズ：Windows 10 の最新リリースでは、WPA-2 エンタープライズを使用するために SCEP を構成します。SCEP を構成すると、Citrix Endpoint Management から証明書をデバイスに送信して Wi-Fi サーバーを認証することができます。SCEP を構成するには、［設定］**>**［資格情報プロバイダー］の ［ディストリビューション］ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Windows 10 および **Windows 11** の設定を開く

- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続：ネットワークに自動的に接続するかどうかを選択します。

Windows 10 および **Windows 11** の **WPA** パーソナル、**WPA-2** パーソナル設定

- 暗号化：一覧から、[**AES**] または [**TKIP**] を選択して、暗号化の種類を設定します。デフォルトは [**AES**] です。
- 共有キー：選択した方法の暗号化キーを指定します。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続：ネットワークに自動的に接続するかどうかを選択します。

Windows 10 および **Windows 11** の **WPA-2** エンタープライズ設定

- 暗号化：一覧から、[**AES**] または [**TKIP**] を選択して、暗号化の種類を設定します。デフォルトは [**AES**] です。
- **EAP** タイプ：一覧から、[**PEAP-MSCHAPv2**] または [**TLS**] を選択して、EAP の種類を設定します。デフォルトは [**PEAP-MSCHAPv2**] です。
- ネットワークを非表示にする：ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続：ネットワークに自動的に接続するかどうかを選択します。
- **SCEP** の有効化?: SCEP を使用して証明書をユーザーデバイスにプッシュするかどうかを選択します。
- **SCEP** の資格情報プロバイダー：ボックスの一覧で、SCEP 資格情報プロバイダーを選択します。デフォルトは [なし] です。

ネットワーク使用状況デバイスポリシー

November 29, 2023

ネットワーク使用状況の規則を設定することで、iOS デバイスが携帯データネットワークなどのネットワークをどのように使用するのかを指定できます。規則は管理対象アプリと指定の SIM に適用されます。管理対象のアプリとは、Citrix Endpoint Management を使用してユーザーのデバイスに展開されるアプリです。これには、ユーザーが Citrix Endpoint Management を使用して展開することなく直接デバイスにダウンロードしたアプリは含まれません。また、デバイスを Citrix Endpoint Management に登録したときに既にデバイスにインストールされていたアプリも含まれません。このポリシーは、iOS 13 デバイスの SIM に適用されます。アプリ規則か SIM 規則、またはその両方を構成できます。SIM 規則は、そのデバイス上のすべての管理対象アプリに適用されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アプリケーション規則
  - 携帯データのローミングを許可：指定したアプリに、ローミング中に携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは ［オフ］です。
  - 携帯データを許可：指定したアプリに、携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは ［オフ］です。
  - アプリ **ID** 照合：一覧に追加するアプリごとに、［追加］をクリックして以下を構成します：
    - アプリ **ID**：アプリ識別子を入力します。
  - ［保存］をクリックしてアプリを一覧に追加するか、［キャンセル］をクリックして操作を取り消します。
- **SIM** 規則
  - **SIM Wi-Fi** アシストポリシー：［接続不良時に **Wi-Fi** から切り替える］を有効にすると、Wi-Fi アシストポリシーが接続状態の悪い Wi-Fi から携帯ネットワーク接続に切り替わりやすくなります。この設定により、携帯データネットワークの使用が増加し、バッテリー寿命に影響を与える可能性があります。
  - **SIM ICCID**：一覧に追加する SIM ごとに、［追加］をクリックしてから以下を構成します：
    - **ICCID**：追加する SIM カードの 19 桁または 20 桁の番号を入力します。

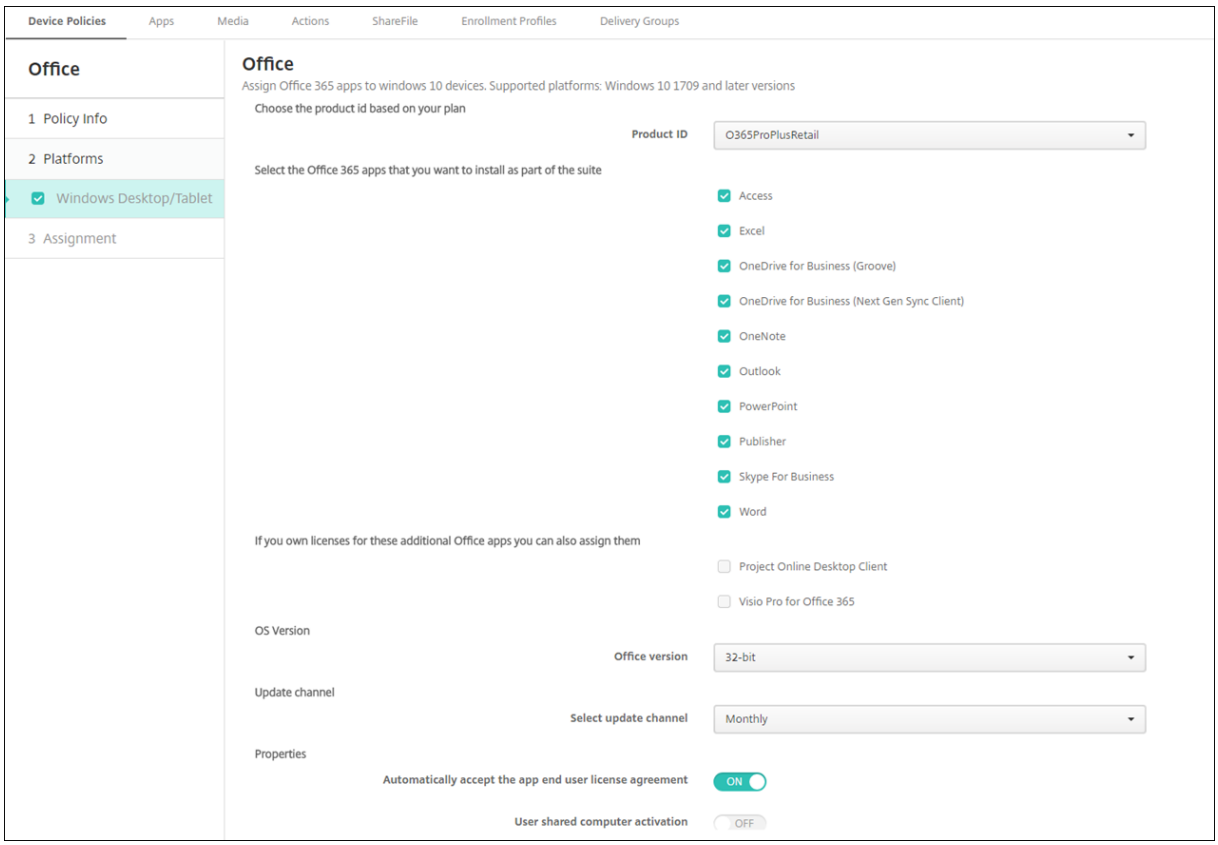
Office デバイスポリシー

November 29, 2023

Citrix Endpoint Management では、Office 構成サービスプロバイダー（CSP）を使用して Microsoft Office 365 製品を展開することができます。Office デバイスポリシーを構成することにより、Microsoft Office アプリを、Windows 10（バージョン 1709 以降）または Windows 11 を実行しているすべてのデバイスに展開できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップ/タブレットの設定



- 製品 **ID**: Office 365 プランに基づいて製品 ID を選択します。オプションは[**O365ProPlusRetail**]、[**O365BusinessRetail**]です。
- **Office 365** アプリ：展開する Office 365 アプリを選択します。デフォルトではすべてのアプリが選択されています。
- その他の **Office** アプリ：**Project Online** のデスクトップクライアントまたは **Visio Pro for Office 365** のライセンスを所有している場合は、これらのアプリをインストール対象に選択できます。
- **Office** バージョン：インストールする Office のバージョンを［**32** ビット］と［**64** ビット］から選択します。
- 更新チャネル：更新頻度を選択します。オプションは［毎月］、［毎月（対象限定）］、［半年ごと］、［半年ごと（対象限定）］です。
- プロパティ：
  - アプリのエンドユーザーライセンス契約の自動承諾：［オン］または ［オフ］を選択します。デフォルトは、［オン］です。
  - ユーザー共有コンピューターのライセンス認証：コンピューターを共有するかどうかを選択します。オプションは ［オン］または ［オフ］です。デフォルトは、［オフ］です。
- **Office** の言語：Office は、Windows にインストール済みのすべての言語版で自動的にインストールされます。追加でインストールする言語を選択できます。

組織情報デバイスポリシー

November 29, 2023

組織情報デバイスポリシーでは、Citrix Endpoint Management から iOS デバイスにプッシュされるアラートメッセージの組織情報を指定できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 名前： Citrix Endpoint Management を実行している組織の名前を入力します。
- 住所：組織の住所を入力します。
- 電話：組織のサポート電話番号を入力します。
- メール：サポートメールアドレスを入力します。
- マジック：組織が管理しているサービスについて説明する語句を入力します。

OS の更新デバイスポリシー

March 15, 2024

OS の更新デバイスポリシーを使用すると、次の更新プログラムを展開できます：

- 監視対象の iOS デバイスへの最新の OS 更新プログラムの展開。

  OS の更新デバイスポリシーは、Apple Deployment Program で登録されている監視対象デバイスのみで機能します。

- macOS 10.11.5 以降を実行している Apple Deployment Program 登録済み macOS デバイスへの、最新の OS とアプリの更新プログラムの展開。

> 注：
>
> 現在 Apple は、OS の更新をメジャーバージョンのみに制限しています。管理者はマイナーバージョンの更新を許可されていません。詳しくは、Apple 社のドキュメントのこの記事を参照してください。

- Windows 10 または Windows 11 を実行している監視対象のデスクトップおよびタブレットデバイスに対する最新の OS アップデート。

  Windows 10（バージョン 1607 以降）または Windows 11 を実行しているデスクトップとタブレットでは、OS の更新ポリシーを使用して配信の最適化設定を管理することもできます。配信の最適化は、Microsoft 社

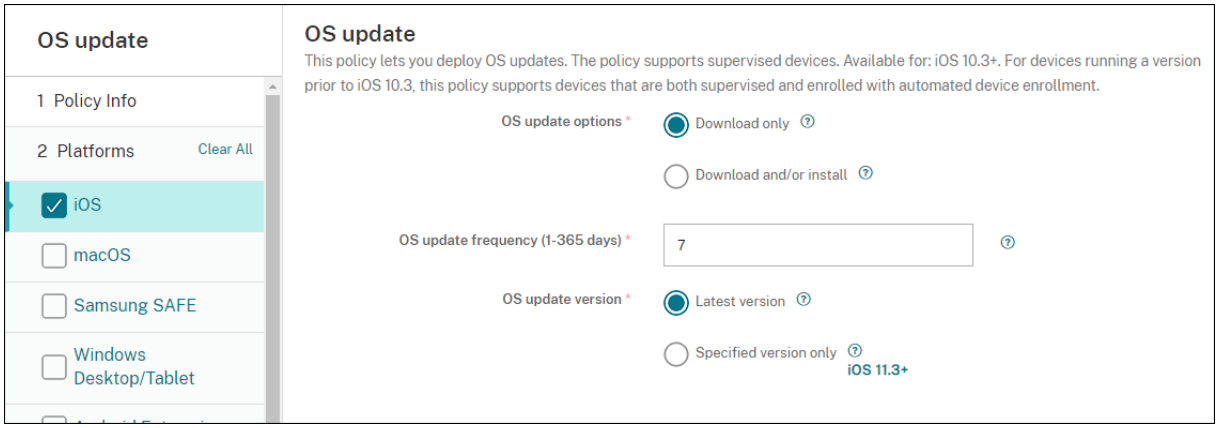
が Windows 10 および Windows 11 の更新で提供するピアツーピアクライアント更新サービスです。これは、更新処理中の帯域幅の問題を軽減するために導入されました。帯域幅の削減は、複数のデバイス間でダウンロードタスクを共有することによって実現できます。詳しくは、Microsoft の記事「Windows 10 更新プログラムの配信の最適化の構成」を参照してください。

- 管理対象の Android Enterprise デバイス（Android 7.0 以降）への最新の OS 更新プログラムの展開。

> 重要:
>
> OS の更新ポリシーでは、更新を完全に無効にすることはできません。更新を最大 90 日間延期するには、制限ポリシーを作成します。「制限デバイスポリシー」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

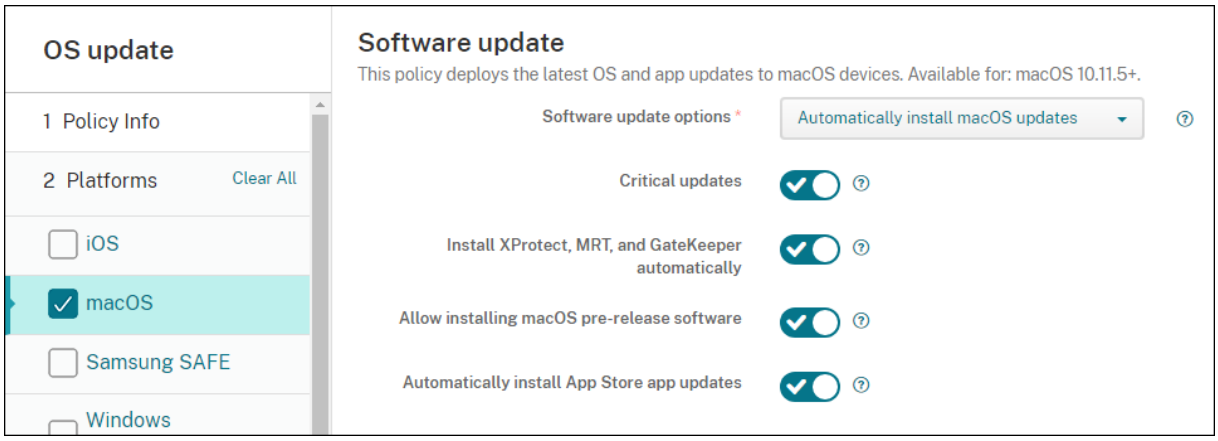
iOS の設定



監視対象 iOS デバイス向けの設定を以下に示します。

- **OS** の更新オプション：いずれのオプションでも［**OS** の更新頻度］に従って、最新の OS 更新プログラムが監視対象デバイスにダウンロードされます。デバイスにより、更新プログラムのインストールが促されます。ユーザーがデバイスのロックを解除すると、プロンプトが表示されます。
- **OS** の更新頻度：Citrix Endpoint Management がデバイスの OS をチェックして更新する頻度を決定します。デフォルトは **7** 日です。
- **OS** の更新バージョン：監視対象の iOS デバイスの更新に使用するバージョンを指定します。デフォルトは［最新バージョン］です。
  - 最新バージョン：最新バージョンの OS に更新する場合に選択します。
  - 指定バージョンのみ：特定の OS バージョンに更新する場合は、このオプションを選択してバージョン番号を入力します。

macOS 設定



- ソフトウェアの更新オプション： macOS デバイスが更新をチェックしてインストールする方法を制御します。次のオプションを選択します：
  - **macOS** の更新を自動インストール：更新を自動的にダウンロードしてインストールします。
  - 利用可能な場合は新しい更新プログラムをダウンロード：更新をダウンロードしますが、手動インストールが必要です。
  - 更新プログラムをチェック：更新が存在するかチェックしますが、更新のダウンロードやインストールは自動で行いません。
  - 更新プログラムをチェックしない：新しい更新のチェック、更新のダウンロードやインストールを自動で行いません。ユーザーは引き続き手動で更新をインストールできます。
- 重要な更新：重要な macOS 更新の自動インストールを許可します。
- **Xproject**、**MRT**、および **GateKeeper** の更新を自動インストール： macOS デバイスが、セキュリティソフトウェアの更新を自動的にインストールできるようにします。
- **macOS** プレリリース版ソフトウェアのインストールを許可する： macOS プレリリース版ソフトウェアのインストールを許可します。
- **App Store** アプリの更新を自動インストール： App Store アプリの自動更新を許可します。

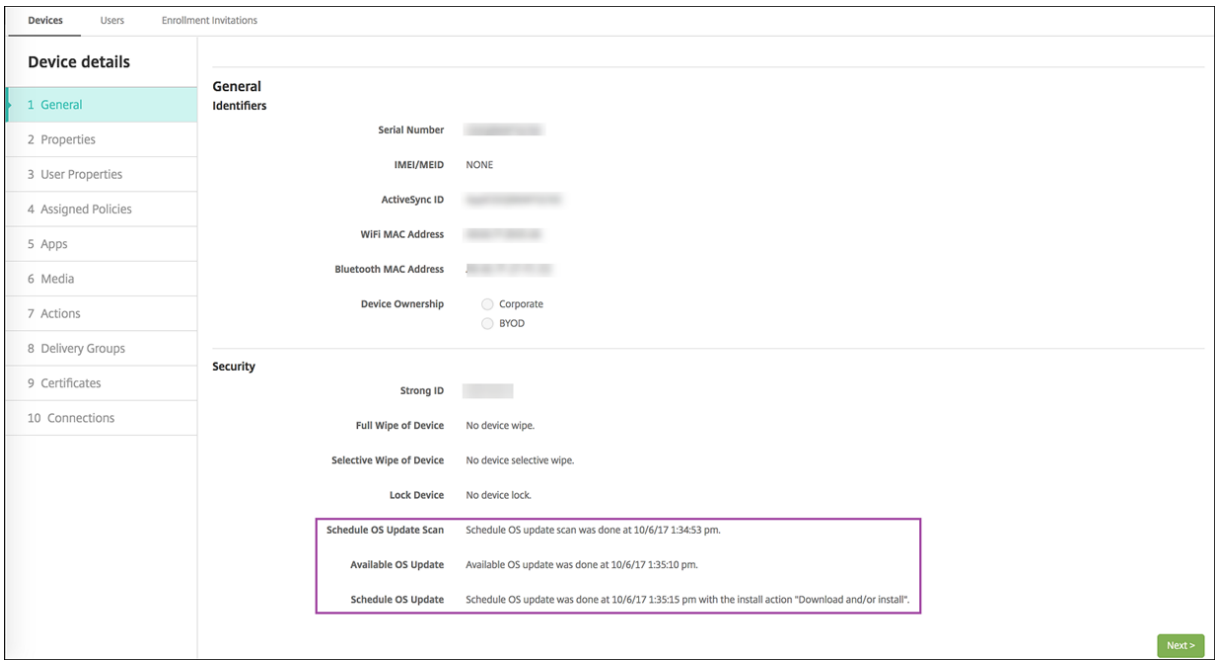
iOS と macOS の更新操作のステータス取得

iOS と macOS の場合、Citrix Endpoint Management は OS 更新の制御ポリシーをデバイスに展開しません。代わりに、Citrix Endpoint Management はこのポリシーを使用して、次の MDM コマンドをデバイスに送信します：

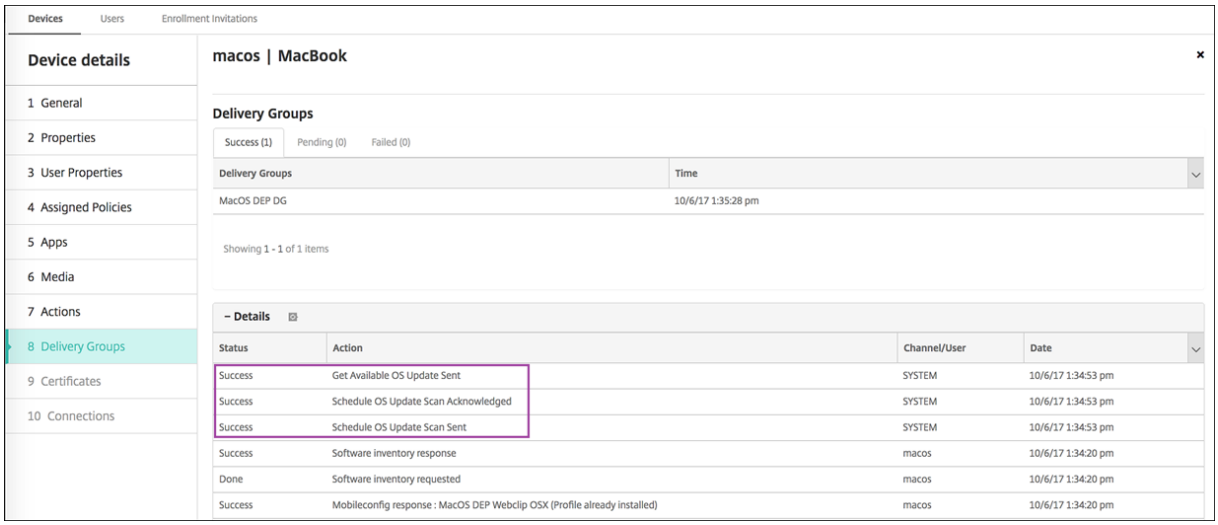
- OS 更新プログラムのスキャンスケジュール：デバイスが OS 更新プログラムのバックグラウンドスキャンを実行するように要求します。（iOS ではオプション）
- 利用可能な OS 更新プログラム：利用可能な OS 更新プログラムの一覧をデバイスに問い合わせます。

- OS 更新プログラムのスケジュール：デバイスが macOS の更新プログラム、アプリの更新プログラム、またはその両方を実行するように要求します。したがって、デバイス OS は、OS およびアプリの更新プログラムをダウンロードまたはインストールするタイミングを決定します。

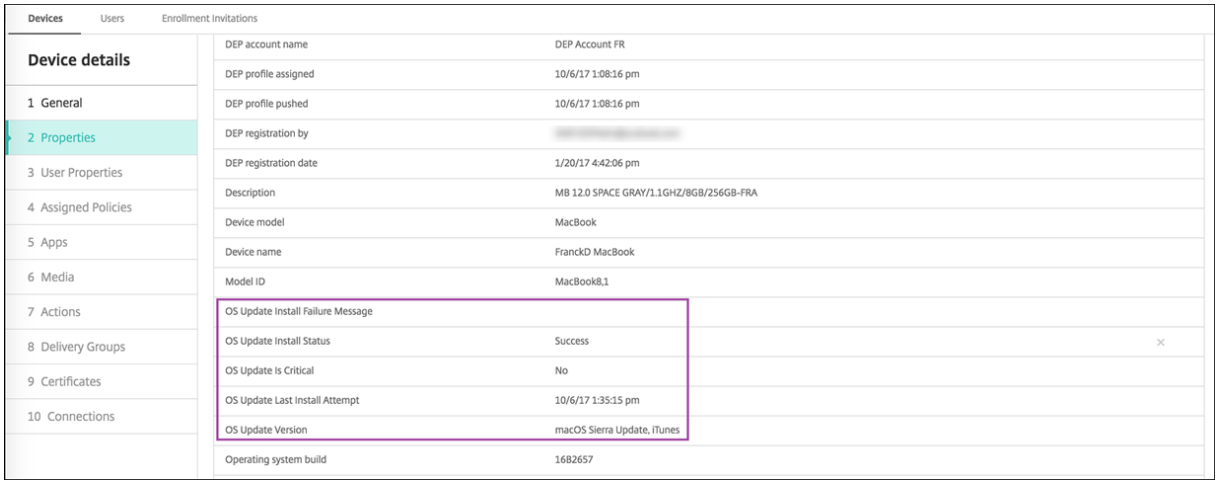
［管理］**>**［デバイス］**>**［デバイス詳細（全般）］ページには、スケジュールされた使用可能な OS 更新プログラムスキャンのステータスと、スケジュールされた macOS とアプリの更新プログラムが表示されます。

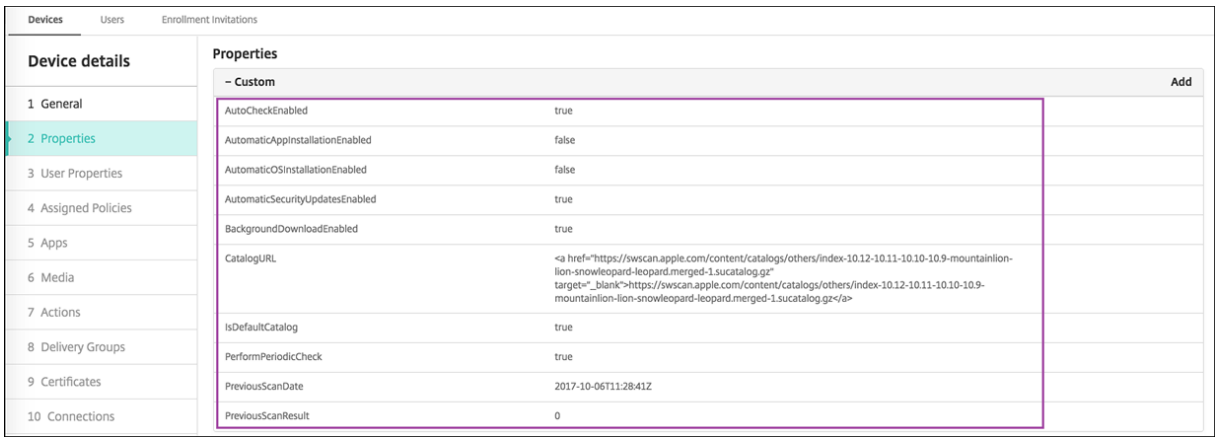


更新操作のステータスについて詳しくは、［管理］**>**［デバイス］**>**［デバイス詳細（デリバリーグループ）］ページを参照してください。

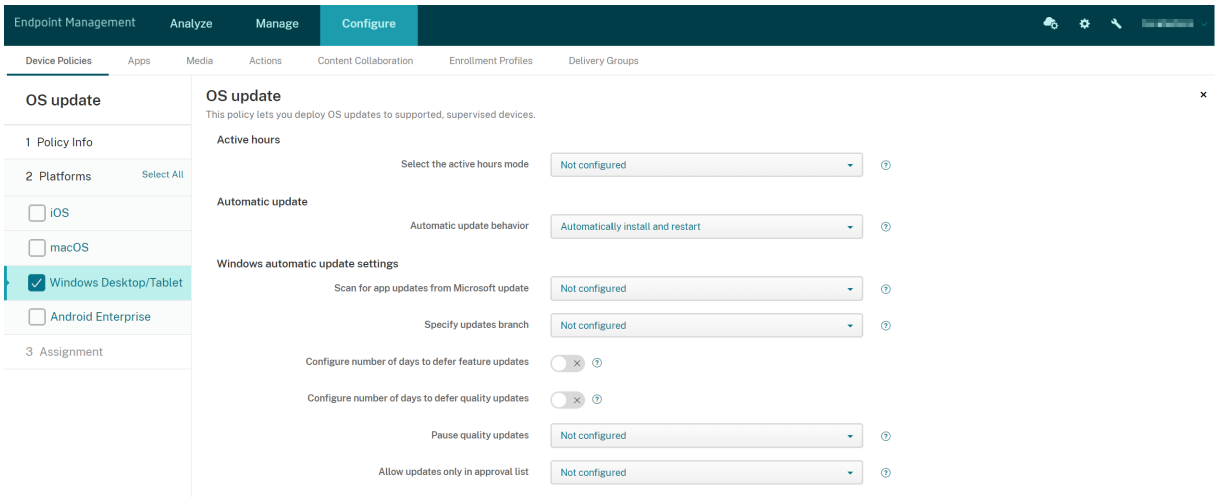


利用可能な OS 更新プログラムや最後のインストールの試行などについて詳しくは、［管理］**>**［デバイス］**>**［デバイス詳細（プロパティ）］ページを参照してください。





Windows デスクトップとタブレットの設定



- アクティブ時間モードを選択： OS の更新を実行するアクティブ時間の構成モードを選択します。時間の範囲を指定するか、開始時刻と終了時刻を指定します。モードを選択すると、［アクティブ時間の最大範囲を指定］

設定または ［アクティブ時間の開始］と ［アクティブ時間の終了］の各設定が追加表示されます。［未構成］を指定した場合、Windows でいつでも OS の更新を実行できます。デフォルトは ［未構成］です。

- 自動更新の動作：ユーザーデバイス上の Windows Update サービスのダウンロード、インストール、再起動の動作を構成します。デフォルトは ［自動でインストールして再起動］です。
  - 更新をダウンロードする前にユーザーに通知する：更新プログラムが利用可能な場合、Windows からユーザーに通知されます。Windows が自動で更新プログラムをダウンロードしてインストールすることはありません。ユーザーがダウンロードおよびインストール操作を開始する必要があります。
  - 自動でインストールしてデバイスの再起動スケジュールを通知：Windows は定額制課金接続で更新プログラムを自動的にダウンロードします。Windows は、デバイスが使用されておらず、バッテリー電源で動作していない時の自動メンテナンス中に更新をインストールします。自動メンテナンスで 2 日間更新プログラムをインストールできない場合、Windows Update は更新プログラムを直ちにインストールします。インストールで再起動が必要な場合、Windows は再起動時間をスケジュールするようユーザーに求めます。ユーザーは再起動を 7 日までの範囲でスケジュールする必要があります。7 日が経過すると、Windows はデバイスを強制的に再起動します。ユーザーが開始時刻を制御できるようにすることで、アプリが再起動時に正常にシャットダウンされないことで生じる不慮のデータ損失のリスクを抑えられます。
  - 自動でインストールして再起動：デフォルト設定。Windows は定額制課金接続で更新プログラムを自動的にダウンロードします。Windows は、デバイスが使用されておらず、バッテリー電源で動作していない時の自動メンテナンス中に更新をインストールします。自動メンテナンスで 2 日間更新プログラムをインストールできない場合、Windows Update は更新プログラムを直ちにインストールします。インストールに再起動が必要な場合、Windows はデバイスが非アクティブの時にデバイスを自動的に再起動します。
  - 指定した時間に自動でインストールして再起動：このオプションを選択すると、日付と時刻を指定するための詳細設定が表示されます。デフォルトは毎日午前 3 時です。指定された時刻に自動インストールが行われ、15 分のカウントダウン後にデバイスが再起動します。Windows を再起動する準備ができている場合、ログインしているユーザーは 15 分のカウントダウンを中断して再起動を遅らせることができます。
  - エンドユーザーの制御なしで自動でインストールして再起動： Windows は定額制課金接続で更新プログラムを自動的にダウンロードします。Windows は、デバイスが使用されておらず、バッテリー電源で動作していない時の自動メンテナンス中に更新をインストールします。自動メンテナンスで 2 日間更新プログラムをインストールできない場合、Windows Update は更新プログラムを直ちにインストールします。インストールに再起動が必要な場合、Windows はデバイスが非アクティブの時にデバイスを自動的に再起動します。また、このオプションでは、ユーザーコントロールパネルが読み取り専用になります。
  - 自動更新を無効にする：デバイスの Windows 自動更新を無効にします。
- **Microsoft Update** からアプリの更新をスキャンする： Windows が Microsoft Update サービスの他の Microsoft アプリの更新を受け入れるかどうかを指定します。デフォルトは ［未構成］です。
  - 未構成：動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイス上の関連 UI

を変更しません。ユーザーは他の Microsoft アプリの更新を承認または拒否できます。
  - はい： Windows で、Windows Update サービスからアプリの更新プログラムをインストールできます。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。
  - いいえ： Windows で、Windows Update サービスからアプリの更新プログラムをインストールすることはできません。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。

- 更新分岐の指定：更新に使用する Windows Update サービスのブランチを指定します。デフォルトは ［未構成］です。

  - 未構成：動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイス上の関連 UI を変更しません。ユーザーは Windows Update サービスのブランチを選択できます。
  - 現在のブランチ： Windows は現在のブランチから更新プログラムを受け取ります。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。
  - 会社の現在のブランチ： Windows は会社の現在のブランチから更新プログラムを受け取ります。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。

- 機能の更新を保留する日数を構成する：［オン］の場合、Windows は機能の更新を指定された日数だけ延期し、ユーザーは設定を変更できません。［オフ］の場合、ユーザーは機能の更新を延期する日数を変更できます。デフォルトは、［オフ］です。
- 機能の更新を保留する日数を構成する：［オン］の場合、Windows は品質の更新を指定された日数だけ延期し、ユーザーは設定を変更できません。［オフ］の場合、ユーザーは品質の更新を延期する日数を変更できます。デフォルトは、［オフ］です。
- 品質更新の一時停止：品質の更新を 35 日間一時停止するかどうかを指定します。デフォルトは ［未構成］です。

  - 未構成：動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイス上の関連 UI を変更しません。ユーザーは 35 日間、品質の更新を一時停止することができます。
  - はい： Windows は 35 日間、Windows Update サービスからの品質の更新プログラムのインストールを一時停止します。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。
  - いいえ： Windows は、Windows Update サービスからの品質の更新プログラムをインストールを一時停止することはできません。ユーザーデバイス上の関連設定は非アクティブであるため、ユーザーは設定を変更できません。

- 承認一覧の更新のみを許可： MDM サーバーが承認する更新のみをインストールするかどうかを指定します。Citrix Endpoint Management では、更新の承認一覧の構成はサポートしていません。デフォルトは ［未構成］です。

  - 未構成：動作を構成しない場合は、この設定を使用します。Windows はユーザーデバイス上の関連 UI を変更しません。ユーザーは、許可する更新プログラムを選択できます。
  - はい。承認された更新のみをインストールします：承認された更新のみをインストールできます。
  - いいえ。すべての更新をインストールします：該当する更新をデバイスにインストールできます。

- 内部更新サーバーを使用する： Windows Update サービスまたは内部更新サーバーから Windows Server Update Services（WSUS）を使用して更新を取得するかどうかを指定します。［オフ］の場合、デバイスは Windows Update サービスを使用します。［オン］の場合、デバイスは指定された WSUS サーバーに接続して更新を行います。デフォルトは、［オフ］です。
  - **Microsoft** 以外のエンティティが署名した更新を承認する： Microsoft 以外のサードパーティエンティティによって署名された更新を受け入れるかどうかを指定します。この機能を使用するには、デバイスがサードパーティのベンダー証明書を信頼する必要があります。デフォルトは、［オフ］です。
  - **Microsoft Update** サービスへの接続を許可する：デバイスが WSUS サーバーから更新プログラムを取得するように構成されている場合でも、デバイス上の Windows 更新プログラムを Microsoft Update サービスに定期的に接続できるようにします。デフォルトは、［オン］です。
  - **WSUS** サーバー： WSUS サーバーのサーバー URL を指定します。
  - 更新をホストする代替イントラネットサーバー：更新をホストし、レポート情報を受け取る代替のイントラネットサーバー URL を指定します。
- 配信の最適化を構成する： Windows 10 および Windows 11 更新プログラムの配信の最適化を使用するかを指定します。デフォルトは ［オフ］です。
- キャッシュサイズ：配信の最適化キャッシュの最大サイズ。**0** に設定すると、キャッシュサイズは無制限になります。デフォルトは **10**GB です。
- **VPN** ピアキャッシュを許可： VPN 経由でドメインネットワークに接続する場合、デバイスをピアキャッシュに追加するかを指定します。［オン］にすると、デバイスは VPN 上または企業ドメインネットワーク上のどちらでも、他のドメインネットワークデバイスとの間でダウンロードまたはアップロードを実行することができます。デフォルトは ［オフ］です。
- ダウンロード方法：配信の最適化で Windows Update、アプリ、アプリの更新プログラムのダウンロードに配信の最適化で使用できるダウンロード方法。デフォルトは ［**HTTP** と同じ **NAT** でのピアリングの組み合わせ］です。次のオプションがあります：
  - **HTTP** のみ、ピアリングなし：ピアツーピアキャッシュを無効にしますが、配信の最適化で、Windows Update サーバーまたは Windows Server Update Services（WSUS）サーバーからコンテンツをダウンロードできるようにします。
  - **HTTP** と同じ **NAT** でのピアリングの組み合わせ：同じネットワーク上でのピア共有を可能にします。配信の最適化クラウドサービスは、ターゲットクライアントと同じパブリック IP アドレスを使用してインターネットに接続する他のクライアントを検出します。次に、これらのクライアントが、プライベートサブネット IP を使用して同じネットワーク上の他のピアに接続しようとします。
  - **HTTP** とプライベートグループでのピアリングの組み合わせ：デバイスの Active Directory ドメインサービス（AD DS）サイトまたはデバイスの認証先のドメインに基づいて、グループを自動的に選択します。ピアリングは、同じグループに属しているデバイス間（リモートオフィス内のデバイスを含む）の内部サブネット間で発生します。
  - **HTTP** とインターネットピアリングの組み合わせ：配信の最適化でインターネットピアソースを使用可能にします。
  - ピアリングなしの簡易ダウンロードモード：配信の最適化クラウドサービスの使用を無効にします。配

信の最適化クラウドサービスが利用できない場合、サービスに接続できない場合、またはコンテンツファイルのサイズが 10MB 未満の場合、配信の最適化はこのモードに自動的に切り替わります。このモードでは、配信の最適化により、ピアツーピアキャッシュなしでも信頼性の高いダウンロードエクスペリエンスが提供されます。

  - 配信の最適化の代わりに **BITS** を使用する：クライアントで BranchCache を使用できるようにします。詳しくは、Microsoft の記事「BranchCache」を参照してください。

- 最大ダウンロード帯域幅：最大ダウンロード帯域幅 (KB /秒)。デフォルトは **0** で、帯域幅を動的に調整します。
- 最大ダウンロード帯域幅の割合：同時ダウンロード操作のうち配信の最適化で使用可能な最大ダウンロード帯域幅。値は利用可能なダウンロード帯域幅の割合です。デフォルトは **0** で、動的な調整を行います。
- 最大アップロード帯域幅：最大アップロード帯域幅（KB /秒）。デフォルト値は **0** です。値が **0** の場合、帯域幅は無限になります。
- 月単位のデータアップロード上限：暦月ごとに配信の最適化でインターネットピアにアップロードできる最大サイズ（GB）す。デフォルトは 20GB です。値を **0** にすると、月ごとのアップロードサイズは無制限になります。

Citrix Endpoint Management が **Windows** デスクトップおよびタブレットデバイスの承認された更新プログラムを処理する方法

承認された更新プログラムのみをインストールするかどうかを指定できます。Citrix Endpoint Management は、次のように更新プログラムを処理します：

- セキュリティ更新プログラム(Windows Defender の定義など)については、Citrix Endpoint Management は更新プログラムを自動的に承認し、次回の同期中にデバイスにインストールコマンドを送信します。
- 他のすべての更新プログラムについては、Citrix Endpoint Management は管理者の承認を待ってから、インストールコマンドをデバイスに送信します。

前提条件

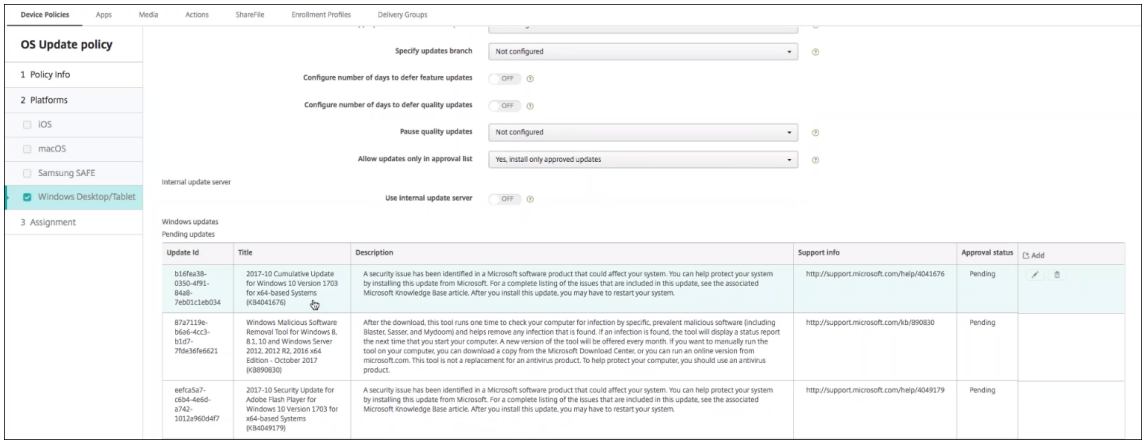
- Microsoft ルート証明書をサーバー証明書として Citrix Endpoint Management サーバーにアップロードする必要があります。
- サーバー証明書のインポート方法については、「証明書および認証」の「証明書をインポートするには」を参照してください。

承認された更新のみをインストールには

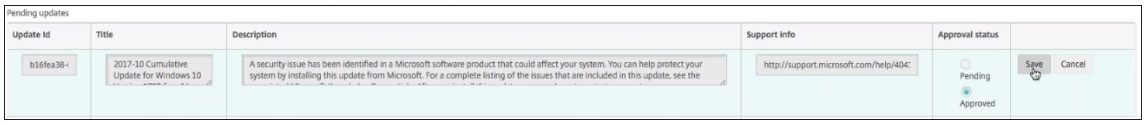
1. ［構成］ **>** ［デバイスポリシー］に移動して、OS の更新デバイスポリシーを開きます。
2. ［承認一覧の更新のみを許可］の設定を ［はい。承認された更新のみをインストールします］に変更します。

更新プログラムを承認するには

1. OS の更新デバイスポリシーで、［保留中の更新］テーブルに移動します。Citrix Endpoint Management により、デバイスのテーブルにある更新が取得されます。
2. ［承認ステータス］が ［保留中］の更新プログラムを見つけます。
3. 承認する更新プログラムの行をクリックし、その行の ［追加］列にある編集アイコンをクリックします。

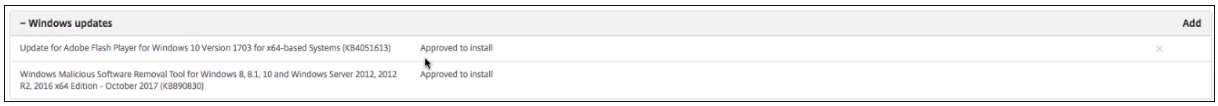


4. 更新を承認する場合は ［承認済み］をクリックし、［保存］をクリックします。



> 注:
>
> ［保留中の更新］テーブルには追加コマンドおよび削除コマンドが表示されますが、これらのコマンドを実行しても Citrix Endpoint Management データベースは変更されません。保留中の更新に対して実行できる操作は、承認ステータスの編集のみです。

デバイスの Windows Update の状態を確認するには、［管理］**>**［デバイス］**>**［プロパティ］に移動します。



更新プログラムが公開されると、更新 **ID** がステータス（[成功］または［失敗]）とともに最初の列に表示されます。更新が失敗したデバイスについて、レポートまたは自動アクションを作成できます。公開日時も表示されます。

初回以降の展開での更新の仕組み　初回展開とデバイス更新後の展開では、デバイスに対する OS の更新デバイスポリシーの影響が異なります。

- Citrix Endpoint Management がデバイスに更新の有無を照会できるようにするには、少なくとも 1 つの OS の更新デバイスポリシーを構成し、デリバリーグループに割り当てる必要があります。

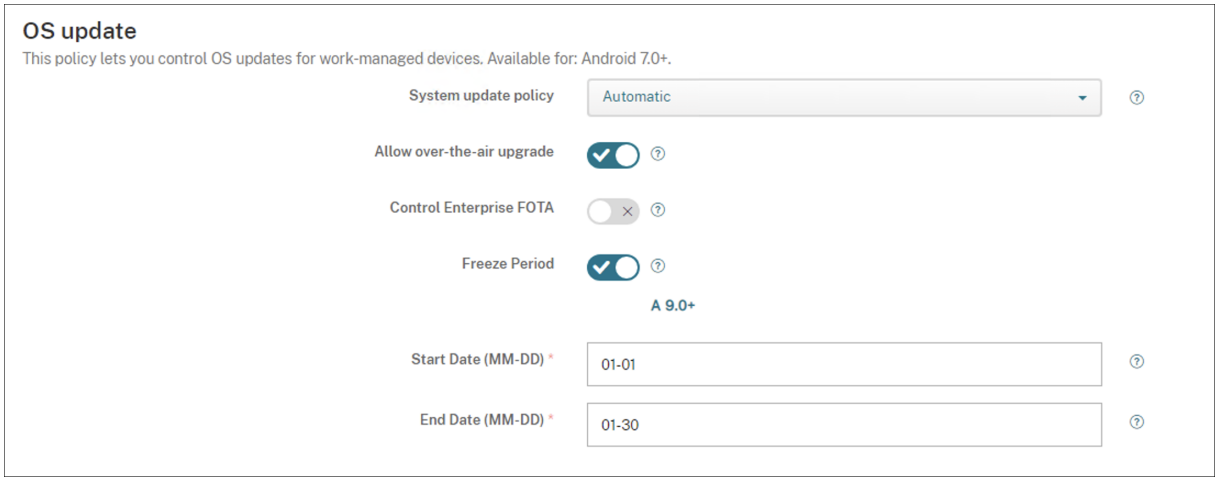
  Citrix Endpoint Management は、デバイスの MDM 同期中に、インストール可能な更新プログラムがあるかどうかデバイスに照会します。

- OS の更新デバイスポリシーを初めて展開した後は、デバイスからの報告が行われていないため、Windows 更新プログラムの一覧は空になります。
- 割り当て済みのデリバリーグループ内のデバイスが更新プログラムを報告すると、Citrix Endpoint Management はそれらの更新プログラムをデータベースに保存します。報告された更新プログラムを承認するには、ポリシーを再度編集します。

  更新プログラムの承認は、編集中のポリシーにのみ適用されます。あるポリシーで承認された更新が、別のポリシーで承認済みとして表示されることはありません。次回のデバイスの同期時に、Citrix Endpoint Management は更新プログラムが承認されたことを示すコマンドをデバイスに送信します。
- 2 番目の OS の更新デバイスポリシーの更新プログラムの一覧には、Citrix Endpoint Management データベースに保存されている更新プログラムが含まれます。各ポリシーの更新を承認します。

  更新プログラムがインストールされたとデバイスから報告されるまで、Citrix Endpoint Management は各デバイスの同期中にデバイスに承認済み更新プログラムの状態を照会します。インストール後に再起動が必要な更新プログラムについては、Citrix Endpoint Management はデバイスからインストール完了と報告されるまで更新プログラムの状態を照会します。
- Citrix Endpoint Management のポリシー構成ページに表示される更新プログラムは、デリバリーグループやデバイスで限定されることはありません。一覧には、デバイスから報告された更新プログラムがすべて表示されます。

Android Enterprise の設定



- システム更新ポリシー：システムの更新を行うタイミングを指定します。［**Enterprise FOTA** の制御］設定を有効にすると、この設定の構成に関係なく更新が自動的に行われます。
  - 自動：更新プログラムが利用可能になるとインストールされます。
  - ウィンドウ：［開始時間］と ［終了時間］で指定した毎日のメンテナンスウィンドウ内に更新プログラムが自動でインストールされます。

    - 開始時間：メンテナンスウィンドウの開始時間（分単位。**0**～**1440**）。デバイスのローカル時間の午前 0 時を基準とします。デフォルト値は **0** です。
    - 終了時間：メンテナンスウィンドウの終了時間（分単位。**0**～**1440**）。デバイスのローカル時間の午前 0 時を基準とします。デフォルトは **120** です。
  - 延期：ユーザーは最大 30 日間更新を延期できます。
  - デフォルト：更新ポリシーをシステムのデフォルトに設定します。

- 無線アップグレードを許可：無効にすると、ユーザーデバイスはソフトウェアの更新プログラムをワイヤレスで受信できません。デフォルトは ［オン］ です。
- 凍結期間：［オン］の場合、［自動］、［延期］、［ウィンドウ］更新ポリシーについて、下記で指定する日付範囲の期間、OS 更新プログラムがデバイスにインストールされません。デバイスに一度に設定できる凍結期間は 1 つだけです。凍結期間の長さは、90 日以内にする必要があります。

  - 開始日/終了日：［凍結期間］がオンになっている場合に、OS 更新プログラムがインストールされない日付範囲。

- 凍結期間：［オン］の場合、［自動］、［延期］、［ウィンドウ］更新ポリシーについて、下記で指定する日付範囲の期間、OS 更新プログラムがデバイスにインストールされません。デバイスに一度に設定できる凍結期間は 1 つだけです。凍結期間の長さは、90 日以内にする必要があります。

  - 開始日/終了日：［凍結期間］がオンになっている場合に、OS 更新プログラムがインストールされない日付範囲。

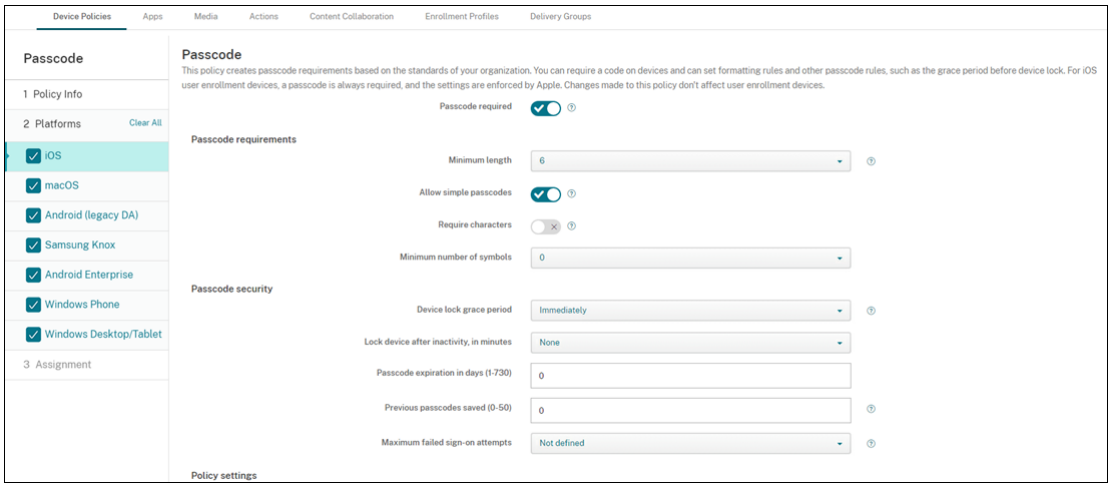
パスコードデバイスポリシー

November 29, 2023

組織の基準に基づいて、Citrix Endpoint Management でパスコードポリシーを作成します。ユーザーのデバイスでパスコードを要求し、さまざまな形式およびパスコード規則を設定することができます。iOS、macOS、Android、Android Enterprise、および Windows デスクトップ/タブレットに対してポリシーを作成します。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



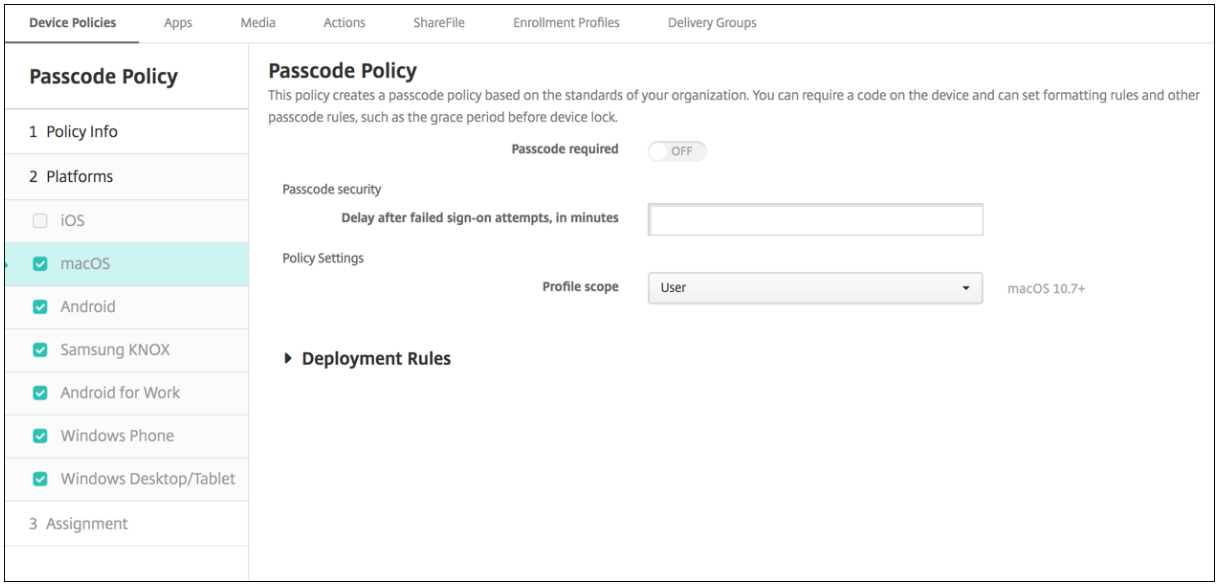
- パスコードを要求：このオプションをオンにするとパスコードが必須になり、iOS のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、ポリシー設定を構成できます。
- パスコード要件
  - 最小の長さ：一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。
  - 単純なパスコードを許可：簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。デフォルトは ［オン］ です。
  - 必須文字：パスコードに文字を 1 つ以上含める必要があるかどうかを選択します。デフォルトは ［オフ］ です。
  - 記号の最小数：一覧から、パスコードに含める必要がある記号の数を選択します。デフォルトは ［**0**］ です。
- パスコードセキュリティ
  - デバイスロックの猶予期間：一覧から、ユーザーがパスコードを入力してデバイスのロックを解除することが必要になるまでの時間を選択します。デフォルトは ［即時］ です。
  - 非アクティブ状態の後にデバイスをロックする：このボックスに、デバイスを非アクティブにしておくことができる時間を入力します。この時間が過ぎると、デバイスはロックされます。値には 1～15 分を指定できます。このポリシーを無効にするには、値を ［なし］ に設定します。デフォルトは ［なし］ です。
  - パスコードの有効期限（**1-730** 日）：パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）：保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0～50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - サインオン失敗回数の上限：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。

* この数値を 6 より大きく設定すると、6 回目の試行の後、次の試行までに間隔を空ける必要があります。この間隔は、試行が失敗するたびに増加します。最後の試行の後、すべてのデータと設定が安全に消去されます。
* 数値を 6 以下に設定すると、この間隔を空けずにデバイスが消去されます。
* ［未定義］を選択した場合、6 回の試行後、デバイスは試行間の間隔を増やしますが、ワイプは実行されません。

デフォルトは ［未定義］です。

- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

macOS 設定



- パスコードを要求：このオプションをオンにするとパスコードが必須になり、iOS のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、ポリシー設定を構成できます。
- ［パスコードを要求］を無効にする場合は、［サインオン試行失敗後の待機時間（分）］の横で、ユーザーがパスコードを再入力できるようになるまでの待機時間を分単位で入力します。
- ［パスコードを要求］を有効にした場合は、次の設定を構成します：
- パスコード要件
  - 最小の長さ：一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。

- 単純なパスコードを許可：簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。デフォルトは ［オン］ です。
- 必須文字：パスコードに文字を 1 つ以上含める必要があるかどうかを選択します。デフォルトは ［オフ］ です。
- 記号の最小数：一覧から、パスコードに含める必要がある記号の数を選択します。デフォルトは ［**0**］ です。

- パスコードセキュリティ

  - デバイスロックの猶予期間：一覧から、ユーザーがパスコードを入力してデバイスのロックを解除することが必要になるまでの時間を選択します。デフォルトは ［なし］ です。
  - 非アクティブ状態の後にデバイスをロックする：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。値は 1～5 分にすることができます。このポリシーを無効にするには、値を ［なし］ に設定します。デフォルトは ［なし］ です。
  - パスコードの有効期限（**1-730** 日）：パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）：保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0～50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - サインオン失敗回数の上限：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。

    * この数値を 6 より大きく設定すると、6 回目の試行の後、次の試行までに間隔を空ける必要があります。この間隔は、試行が失敗するたびに増加します。最後の試行の後、デバイスはロックされます。
    * 数値を 6 以下に設定すると、この間隔を空けずにデバイスがロックされます。
    * ［未定義］ を選択した場合、6 回の試行後、デバイスは試行間の間隔を増やしますが、ロックは実行されません。

    デフォルトは ［未定義］ です。
  - サインオン試行失敗後の待機時間（分）：ユーザーが失敗した試行の上限に達した後、ログインウィンドウが表示されるまでの分数を入力します。
  - パスコードの強制リセット：［オフ］ の場合、デバイスがこのポリシーを受信した後の次回認証時にパスコードをリセットする必要はありません。デフォルトは ［オン］ です。

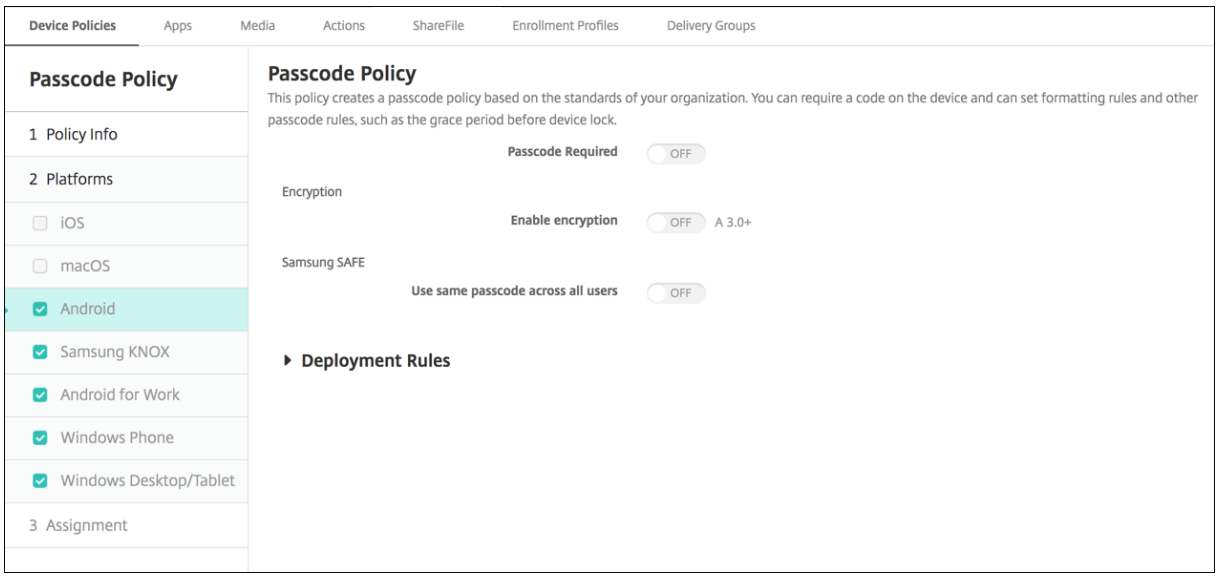
- ポリシー設定

  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］ と ［削除までの期間（時間）を指定］ です。

    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。

- ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
- プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

Android（レガシデバイス管理者）の設定



> 注：
>
> Android のデフォルト設定は ［オフ］です。

- パスコードを要求：このオプションをオンにするとパスコードが必須になり、Android のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、および暗号化の設定を構成できます。
- パスコード要件
  - 最小の長さ：一覧から、パスコードの最小文字数を選択します。デフォルトは 6 です。
  - バイオメトリック認識：生体認証を有効にするかどうかを選択します。このオプションを有効にした場合、［必須文字］フィールドは非表示になります。デフォルトは ［オフ］です。
  - 必須文字：一覧から ［制限なし］、［数字と文字の両方］、［数字のみ］、［文字のみ］のいずれかをクリックして、パスコードの作成方法を構成します。デフォルトは ［制限なし］です。
  - 詳細な規則：詳細なパスコード規則を適用するかどうかを選択します。デフォルトは ［オフ］です。
  - ［詳細な規則］を有効にした場合、以下のボックスの一覧のそれぞれで、パスコードに含める必要がある文字、記号、または数字の数を、種類ごとに選択します。
    - 記号：記号の最小使用数
    - 文字：文字の最小使用数
    - 小文字：小文字の最小使用数

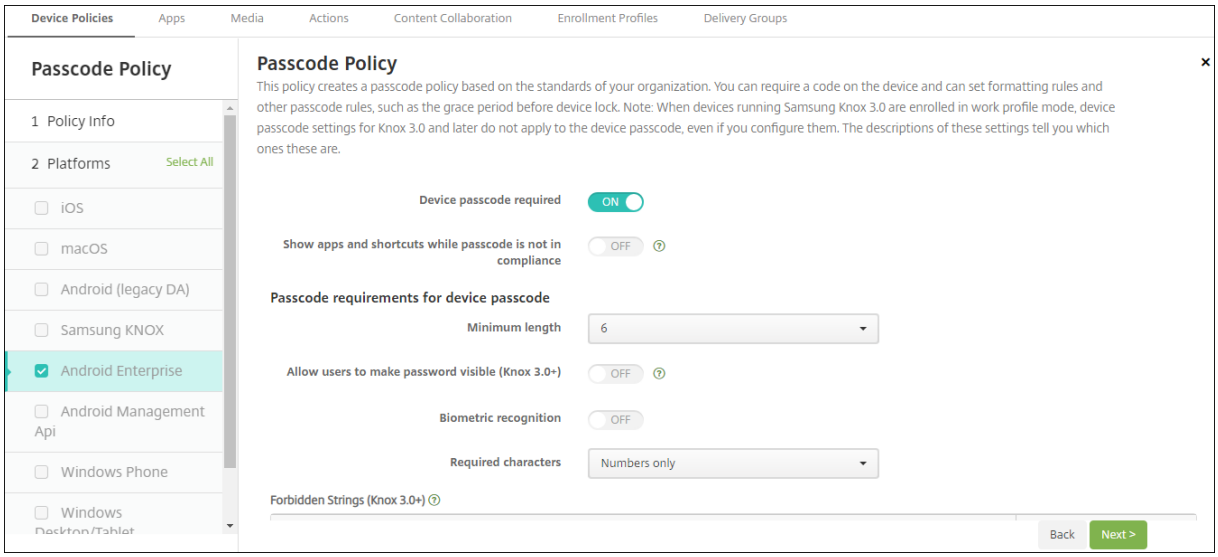
    - 大文字：大文字の最小使用数
    - 数字または記号：数字または記号の最小使用数
    - 数字：数字の最小使用数

- パスコードセキュリティ
  - 非アクティブ状態の後にデバイスをロックする：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは［なし］です。
  - パスコードの有効期限（**1-730** 日）：パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）：保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0～50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - サインオン失敗回数の上限：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。デフォルトは ［未定義］です。

- 暗号化
  - 暗号化を有効化：暗号化を有効にするかどうかを選択します。このオプションは、［パスコードを要求］設定にかかわらず使用できます。

    デバイスを暗号化するには、ユーザーはまず充電済みのバッテリーを用意し、暗号化が完了するまでデバイスをコンセントに接続したままにする必要があります。このプロセスには 1 時間以上かかる場合があります。暗号化処理を中断すると、デバイス上のデータの一部またはすべてが失われる可能性があります。デバイスを暗号化した後は、出荷時の設定へのリセットを実行してデバイス上のすべてのデータを消去しない限り、元に戻すことはできません。

Android Enterprise の設定



Android Enterprise デバイスの場合は、デバイスのパスコードか Android Enterprise の仕事用プロファイルのセキュリティ確認、またはその両方を必須条件にできます。

- デバイスのパスコードを要求：デバイスにパスコードが必要です。この設定が ［オン］の場合は、［デバイスのパスコードのパスコード要件］と ［デバイスのパスコードのパスコードセキュリティ］を設定します。デフォルトは ［オフ］です。
- パスコードの要件に準拠していないときにアプリとショートカットを表示する：この設定を ［オン］にすると、パスコードが要件に準拠していない場合でも、デバイス上のアプリとショートカットが非表示になりません。この設定を ［オフ］にすると、パスコードが要件に準拠していない場合、アプリとショートカットが非表示になります。Citrix では、この設定を有効にする場合、パスコードが要件に準拠していないときにデバイスを非準拠としてマークする自動化された操作を作成することをお勧めします。デフォルトは ［オフ］です。
- デバイスのパスコードのパスコード要件：
  - 最小の長さ：パスコードの最小文字数を選択します。デフォルトは 6 です。
  - バイオメトリック認識：生体認証を有効にします。この設定が ［オン］の場合、［必須文字］フィールドは非表示になります。デフォルトは ［オフ］です。
  - 必須文字：パスコードに必要な文字の種類を指定します。一覧から、［制限なし］、［数字と文字の両方］、［数字のみ］、または ［文字のみ］を選択します。［制限なし］は、Android 7.0 を実行しているデバイスにのみ使用します。Android 7.1 以降では、［制限なし］設定は適用されません。デフォルトは［数字と文字の両方］です。
  - 詳細な規則：パスコードに使用できる文字の種類を、規則で詳しく設定します。この設定が ［オン］の場合は、［最小数］および ［最大数］を設定します。この設定は、Android 5.0 より前の Android デバイスでは使用できません。デフォルトは ［オフ］です。
  - 最小数：
    - 記号：記号の最小使用数を指定します。デフォルト値は **0** です。
    - 文字：文字の最小使用数を指定します。デフォルト値は **0** です。
    - 小文字：小文字の最小使用数を指定します。デフォルト値は **0** です。
    - 大文字：大文字の最小使用数を指定します。デフォルト値は **0** です。
    - 数字または記号：数字または記号の最小使用数を指定します。デフォルト値は **0** です。
    - 数字：数字の最小使用数を指定します。デフォルト値は **0** です。
    - 変更する文字数：有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス用のみの設定です。仕事用プロファイルデバイスとして登録されているデバイスには適用されません。ユーザーが前のパスコードから変更する必要がある文字数を指定します。デフォルトは ［**0**］です。
  - 最大数：有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス用のみの設定です。仕事用プロファイルデバイスとして登録されているデバイスには適用されません。
    - 同一文字の最大使用回数：パスコード内に 1 つの文字を繰り返し使用できる最大回数を指定します。デフォルトは **0** で、制限がないことを意味します。
    - アルファベットの最大連続数：パスコードに含まれる、連続するアルファベットの最大文字数を指

定します。デフォルトは **0** で、制限がないことを意味します。

* 数字の最大連続数：パスコードに含まれる、連続する数字の最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。

- デバイスのパスコードのパスコードの複雑さ（**Android 12** 以降）：
  - 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 Citrix 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
      - 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

        > 注：
        > 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。

- デバイスのパスコードのパスコードセキュリティ：
  - デバイスをワイプ（サインオンの失敗回数が次を超えた場合）：ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、デバイスは完全にワイプされます。デフォルトは ［未定義］です。
  - 非アクティブ状態の後にデバイスをロックする：デバイスを非アクティブにしておくことができる分数を指定します。この時間が過ぎると、デバイスはロックされます。このポリシーを無効にするには、値を 0 に設定します。
  - パスコードの有効期限（**1-730** 日）：パスコードを有効期限切れにするまでの日数を指定します。有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）：保存する使用済みパスワードの数を指定します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0～50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。

- 仕事用プロファイルのセキュリティ確認： Android Enterprise の仕事用プロファイル内で実行されるアプリへのアクセスに対して、ユーザーにセキュリティの確認を求めます。Android 7.0 以降を実行するデバイス

向けです。この設定が ［オン］の場合は、［仕事用プロファイルのセキュリティ確認用のパスコード要件］と［仕事用プロファイルのセキュリティ確認用のパスコードセキュリティ］を設定します。デフォルトは ［オフ］です。

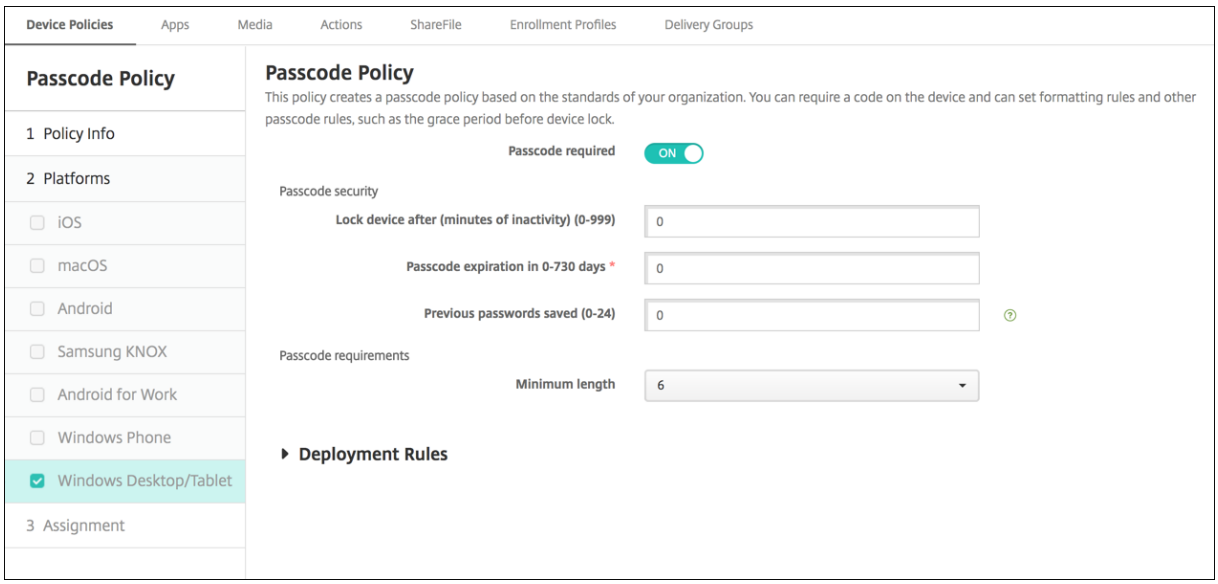
- 仕事用プロファイルのセキュリティ確認用のパスコード要件:
  - 最小の長さ：パスコードの最小文字数を選択します。デフォルトは 6 です。
  - バイオメトリック認識：生体認証を有効にします。この設定が ［オン］の場合、［必須文字］フィールドは非表示になります。デフォルトは ［オフ］です。
  - 必須文字：パスコードに必要な文字の種類を指定します。一覧から、［制限なし］、［数字と文字の両方］、［数字のみ］、または ［文字のみ］を選択します。［制限なし］は、Android 7.0 を実行しているデバイスにのみ使用します。Android 7.1 以降では、［制限なし］設定は適用されません。デフォルトは［数字と文字の両方］です。
  - 詳細な規則：パスコードに使用できる文字の種類を、規則で詳しく設定します。この設定が ［オン］の場合は、［最小数］および ［最大数］を設定します。この設定は、Android 5.0 より前の Android デバイスでは使用できません。デフォルトは ［オフ］です。
  - 最小数:
    - 記号：記号の最小使用数を指定します。デフォルト値は **0** です。
    - 文字：文字の最小使用数を指定します。デフォルト値は **0** です。
    - 小文字：小文字の最小使用数を指定します。デフォルト値は **0** です。
    - 大文字：大文字の最小使用数を指定します。デフォルト値は **0** です。
    - 数字または記号：数字または記号の最小使用数を指定します。デフォルト値は **0** です。
    - 数字：数字の最小使用数を指定します。デフォルト値は **0** です。
    - 変更する文字数：有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。ユーザーが前のパスコードから変更する必要がある文字数を指定します。デフォルトは ［**0**］です。
  - 最大数：有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。
    - 同一文字の最大使用回数：パスコード内に 1 つの文字を繰り返し使用できる最大回数を指定します。デフォルトは **0** で、制限がないことを意味します。
    - アルファベットの最大連続数：パスコードに含まれる、連続するアルファベットの最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。
    - 数字の最大連続数：パスコードに含まれる、連続する数字の最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。
- 仕事用プロファイルのセキュリティ確認用のパスコードの複雑さ（**Android 12** 以降）:
  - 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 Citrix 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
        - 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

        > 注：
        > 仕事用プロファイルのパスコードの複雑さを有効にする場合は、デバイスに対してもパスコードを有効にする必要があります。

- 仕事用プロファイルのセキュリティ確認用のパスコード セキュリティ
    - コンテナをワイプ（サインオンの失敗回数が次を超えた場合）：ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、仕事用プロファイルとそのデータがデバイスからワイプされます。ユーザーは、ワイプが発生した後、仕事用プロファイルを再度初期化する必要があります。デフォルトは ［未定義］です。
    - 非アクティブ状態の後にコンテナをロックする：デバイスを非アクティブにしておくことができる分数を指定します。この時間が過ぎると、仕事用プロファイルはロックされます。値は 0～999 分にすることができます。このポリシーを無効にするには、値を 0 に設定します。
    - パスコードの有効期限（**1-730** 日）：パスコードを有効期限切れにするまでの日数を指定します。有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
    - 使用済みパスワードの保存数（**0 - 50**）：保存する使用済みパスワードの数を指定します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0～50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。

Windows デスクトップ/タブレットの設定



- パスコードを要求： Windows デスクトップ/タブレットデバイスでパスコードを要求しない場合、このオプションを選択します。デフォルト設定は ［オン］で、パスコードを要求します。この設定を無効にすると、ページが折りたたまれ、以下のオプションは表示されなくなります。
- パスコードセキュリティ
  - 非アクティブ状態の後にデバイスをロックする：デバイスを非アクティブにしておくことができる分数を入力します。この時間が過ぎると、デバイスはロックされます。デフォルトは ［**0**］です。
  - パスコードの有効期限（**0**～**730** 日）：パスコードを有効期限切れにするまでの日数を入力します有効な値は 1～730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0-24**）：保存する使用済みパスコードの数を入力します。ユーザーはこの一覧にあるパスコードを使用できません。有効な値は 1～24 です。このフィールドには 1～24 の数値を入力します。デフォルトは ［**0**］です。
- パスコード要件
  - 最小の長さ：一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。

パスコードロックの猶予期間デバイスポリシー

February 16, 2022

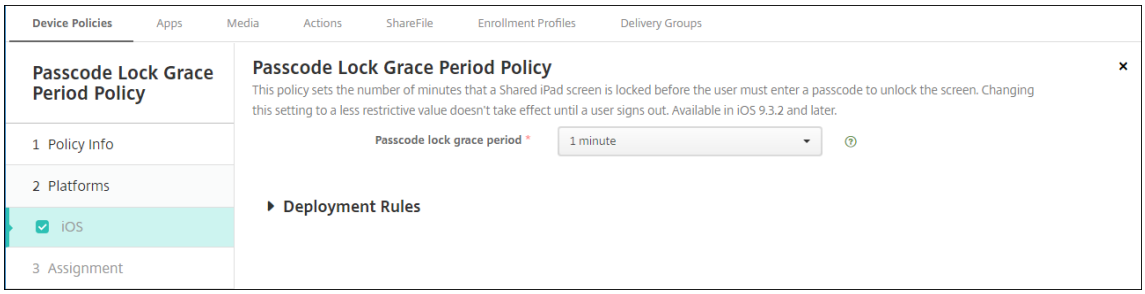
パスコードロックの猶予期間デバイスポリシーは、iOS（iPadOS）を実行している共有デバイス用の機能です。共有 iPad について詳しくは、「Apple の教育向け機能との統合」を参照してください。

このポリシーを追加または構成するには、［構成］>［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- パスコードロックの猶予期間：共有 iPad の画面がロックされてから、画面のロック解除のためにパスコードの入力が必要になるまでの時間（分）。この設定をゆるい値にした場合、ユーザーがサインアウトするまで反映されません。デフォルトは ［即時］です。

  デフォルトでは、共有 iPad は 2 分間使用しないと自動的にロックされます。



個人用ホットスポットデバイスポリシー

May 25, 2021

iOS デバイスの個人用ホットスポット機能を介して携帯データネットワーク接続を使用することにより、ユーザーが Wi-Fi ネットワーク圏外にいてもインターネットに接続できるようにすることができます。

このポリシーを追加または構成するには、［構成］>［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- パーソナルホットスポットを無効化：ユーザーのデバイスで個人用ホットスポット機能を無効にするかどうかを選択します。デフォルトは ［オフ］で、ユーザーのデバイスで個人用ホットスポットは無効になっています。このポリシーでは機能は無効になりません。ユーザーは、引き続きデバイスで個人用ホットスポットを使用できますが、ポリシーが展開されると、デフォルトでオンのままにならないように、個人用ホットスポットがオフになります。

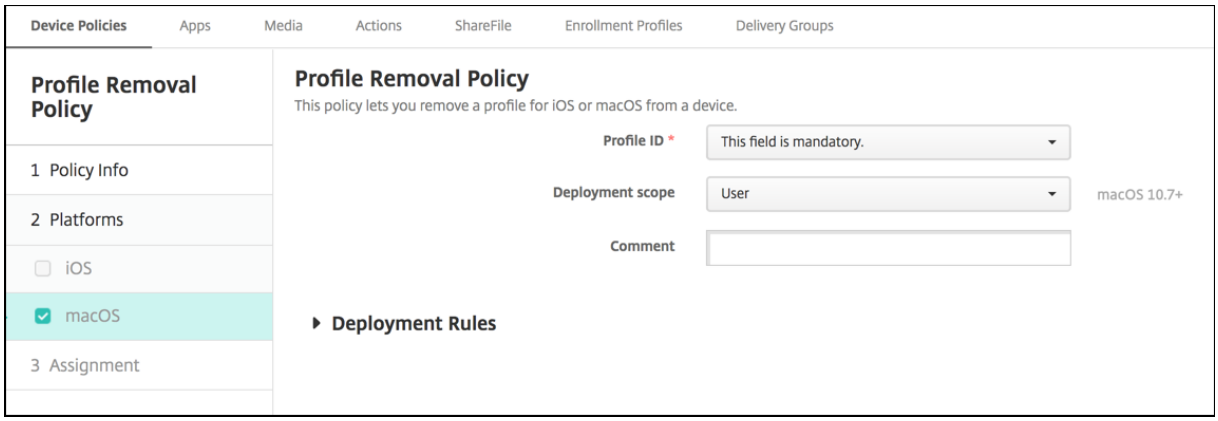
プロファイル削除デバイスポリシー

November 29, 2023

Citrix Endpoint Management で、アプリプロファイル削除デバイスポリシーを作成することができます。ポリシーを展開すると、ユーザーの iOS デバイスまたは macOS デバイスからアプリプロファイルが削除されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

macOS 設定



- プロファイル **ID**：一覧から、アプリプロファイル ID を選択します。このフィールドは必須です。
- 展開範囲：一覧から、［ユーザー］または ［システム］を選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。
- コメント：任意でコメントを入力します。

Provisioning プロファイルデバイスポリシー

November 29, 2023

iOS エンタープライズアプリを開発しコード署名するときは、通常は、iOS デバイスで実行するアプリに Apple が求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。

プロビジョニングプロファイルの主な問題は、Apple Developer Portal で生成されてから 1 年で期限が切れるので、ユーザーによって登録されたすべての iOS デバイス上のすべてのプロビジョニングファイルの期限を追跡する必要があることです。期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信す

る、プロビジョニングプロファイルを Web ポータルに置いてダウンロードとインストールを可能にする、という 2 つの方法があります。これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Web ポータルにアクセスして適切なプロファイルをダウンロードしインストールすることを求めたりするので、エラーが発生する傾向があります。

このプロセスをユーザーが意識しないで済むように、Citrix Endpoint Management ではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。

プロビジョニングプロファイルポリシーを作成するには、プロビジョニングプロファイルのファイルを作成する必要があります。詳しくは、Apple Developer サイトで開発用プロビジョニングプロファイルの作成方法に関する Apple の記事を参照してください。

iOS の設定

- **iOS** プロビジョニングプロファイル：［参照］をクリックしてインポートするプロビジョニングプロファイルファイルの場所へ移動し、そのファイルを選択します。

プロビジョニングプロファイル削除デバイスポリシー

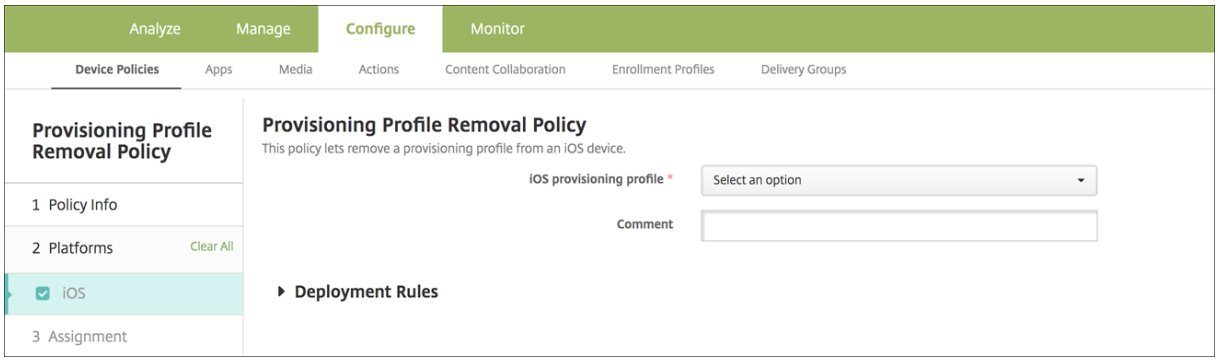
February 16, 2022

プロビジョニングプロファイルを使用すると、iOS アプリをユーザーデバイスに配布できます。iOS デバイス上でのアプリの実行を許可するには、プロビジョニングプロファイルを使用してアプリに署名することが必要とされます。詳しくは、「プロビショニングプロファイルデバイスポリシー」を参照してください。

古いプロビジョニングプロファイルを削除または置き換えるには、プロビジョニングプロファイルの削除デバイスポリシーを使用します。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **iOS** プロビジョニングプロファイル：一覧から削除するプロビジョニングプロファイルを選択します。
- コメント：必要に応じてコメントを追加します。

プロキシデバイスポリシー

September 17, 2021

プロキシデバイスポリシーでは、サポート対象の iOS デバイスのグローバル HTTP プロキシ設定を指定できます。グローバル HTTP プロキシポリシーはデバイスごとに 1 つのみ展開できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提条件

このポリシーを展開する前に、グローバル HTTP プロキシを設定するすべての iOS デバイスを必ず監視モードに設定してください。詳しくは、「Apple Configurator 2 を使用したデバイスの展開」または「Apple Deployment Program でのデバイスの展開」を参照してください。

展開規則を設定して、プロキシポリシーをデバイスに送信する前にデバイスを登録します。

iOS の設定

- プロキシ構成：ユーザーのデバイスでのプロキシの構成方法に関して、一覧から ［手動］または ［自動］を選択します。
  - ［手動］を選択した場合は、次の設定を構成します。
    - プロキシサーバーのホスト名または **IP** アドレス：プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。

    * プロキシサーバーのポート：プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    * ユーザー名：任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    * パスワード：任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［自動］を選択した場合は、次の設定を構成します。
    * プロキシ **PAC URL**：プロキシ構成を定義する PAC ファイルの URL を入力します。
    * **PAC** に到達不能である場合は直接接続を許可： PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは ［オン］です。

- キャプティブ ネットワークへのアクセスのためにプロキシのバイパスを許可：プロキシを使用せずにキャプティブネットワークにアクセスできるようにするかどうかを選択します。デフォルトは ［オフ］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

制限デバイスポリシー

March 15, 2024

> 注:
>
> アップグレードに新しい制限デバイスポリシーの設定を含める場合は、このポリシーを編集して保存する必要があります。アップグレード後の制限デバイスポリシーは、保存するまで Citrix Endpoint Management で展開されません。

制限デバイスポリシーでは、ユーザーデバイスの特定の機能（カメラなど）を許可または制限します。セキュリティ制限とメディアコンテンツ制限を設定できます。ユーザーがインストールできるアプリとインストールできないアプリの種類を制限することもできます。ほとんどの制限設定は、デフォルトでは ［オン］（許可）に設定されています。例外は、iOS セキュリティの強制機能とすべての Windows タブレット機能です。デフォルトで ［オフ］（制限）に設定されています。

オプションで ［オン］を選択した場合、ユーザーが該当する操作を実行、または該当する機能を使用できるようになります。例:

- カメラ:［オン］の場合、ユーザーはデバイスでカメラを使用できます。［オフ］の場合、ユーザーはデバイスでカメラを使用できません。

- スクリーンショット：［オン］の場合、ユーザーデバイスでスクリーンショットを撮ることができます。［オフ］の場合、ユーザーデバイスでスクリーンショットを撮ることができません。

制限デバイスポリシーとキオスクデバイスポリシーの両方が構成されている場合は、制限デバイスポリシーが優先されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

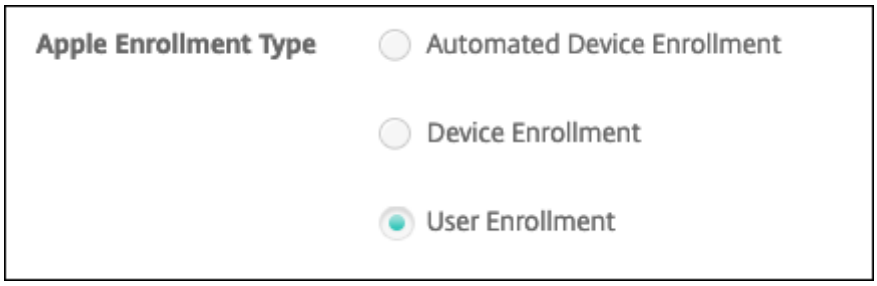
iOS の設定

一部の iOS 制限ポリシー設定は、こちらおよび Citrix Endpoint Management コンソールの［制限ポリシー］ページで説明されているように、特定の iOS バージョンにのみ適用されます。

これらの設定は、デバイスがユーザー登録モード、監視対象外（完全 MDM）モード、または監視モードで登録されている場合に適用されます。次の表に、iOS 13 以降の各設定で使用できる登録モードを示します。

- 自動デバイス登録：監視対象デバイス。これらは、一括登録で登録されたデバイスです。
- デバイス登録：監視対象ではないデバイス。これらのデバイスは個別に登録され、デバイス全体が完全 MDM です。
- ユーザー登録：特定のユーザーのみが管理されるデバイス。ユーザー登録について詳しくは、Apple 社のドキュメントを参照してください。

iOS 制限ポリシー設定は、デバイスがユーザー登録モード、監視対象外（完全 MDM）モード、または監視モードで登録されている場合に適用される可能性があります。次の表に、iOS 13 以降の各制限ポリシー設定で使用できる登録モードを示します。



表で述べたように、以前は監視対象外モードと監視モードで使用できた設定の一部は、iOS 13 以降では監視モードでのみ使用できます。次のルールが適用されます：

- iOS 13 以上の監視対象デバイスが Citrix Endpoint Management に登録される場合、設定はデバイスに適用されます。
- iOS 13 以上の監視対象外デバイスが Citrix Endpoint Management に登録される場合、設定はデバイスに適用されません。
- 既に Citrix Endpoint Management に登録されている iOS 12 以下のデバイスが iOS 13 にアップグレードされる場合、変更はありません。設定は、アップグレード前と同じようにデバイスに適用されます。

iOS デバイスを監視モードに設定する方法については、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

設定	ユーザー登録	監視対象外	監視対象
ハードウェアの制御を許可			
カメラ	いいえ	はい	はい
FaceTime	いいえ	いいえ	はい
画面の取り込み	はい	いいえ	はい
クラスルームアプリが生徒の画面をリモートで監視することを許可する	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリが AirPlay と画面表示を実行できるようにする	いいえ	いいえ	はい
フォトストリーム	いいえ	はい	はい
フォトストリームを共有	いいえ	はい	はい

設定	ユーザー登録	監視対象外	監視対象
共有 iPad の一時セッションを許可	いいえ	いいえ	はい
音声ダイヤル	いいえ	はい	はい
Siri	はい	はい	はい
デバイスのロック中に許可	はい	はい	はい
Siri の不適切な単語フィルター	いいえ	いいえ	はい
アプリのインストール	いいえ	いいえ	はい
ローミング中にグローバルバックグラウンドフェッチを許可する	いいえ	はい	はい
アプリを許可			
Apple App Store	いいえ	いいえ	はい
アプリ内課金	いいえ	はい	はい
購入時に Apple App Store パスワードを要求	いいえ	はい	はい
Safari	いいえ	いいえ	はい
オートフィル	いいえ	いいえ	はい
不正な Web サイトに対する警告を表示	はい	はい	はい
JavaScript を有効化	いいえ	はい	はい
ポップアップをブロック	いいえ	はい	はい
Cookie を受け入れる	いいえ	はい	はい
ネットワーク **- iCloud** の操作を許可			
iCloud ドキュメントおよびデータ	いいえ	いいえ	はい
iCloud バックアップ	いいえ	はい	はい
iCloud フォトキーチェーン	いいえ	はい	はい
iCloud のフォトライブラリ	いいえ	はい	はい
セキュリティ **-** 強制			

設定	ユーザー登録	監視対象外	監視対象
バックアップを暗号化	はい	はい	はい
追跡型広告を制限	いいえ	はい	はい
最初の AirPlay ペアリングでパスコードを要求	はい	はい	はい
手首検出を使用するためのペアリングされた Apple Watch	はい	はい	はい
AirDrop を使用して管理対象のドキュメントを共有します	はい	はい	はい
セキュリティ - 許可			
信頼されていない SSL 証明書の受け入れ	いいえ	はい	はい
証明書信頼設定の自動更新	いいえ	はい	はい
管理されたペーストボードが必要	はい	はい	はい
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	はい	はい	はい
非管理対象アプリによる管理対象アカウント連絡先の読み取り	いいえ	いいえ	はい
管理対象アプリによる非管理対象アカウント連絡先への書き込み	いいえ	いいえ	はい
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	はい	はい	はい
診断データを Apple に送信	はい	はい	はい
Touch ID によるデバイスのロック解除	いいえ	はい	はい
自動ロック解除	いいえ	はい	はい
ロック時の Wallet 通知を表示	いいえ	はい	はい
Handoff	いいえ	はい	はい

設定	ユーザー登録	監視対象外	監視対象
管理対象アプリの iCloud 同期	はい	はい	はい
エンタープライズブックのバックアップ	はい	はい	はい
エンタープライズブックのメモとハイライトの同期	はい	はい	はい
Spotlight でインターネット検索結果を表示	いいえ	はい	はい
エンタープライズアプリケーションを信頼する	いいえ	はい	はい
Apple のパーソナライズされた広告を許可する 監視対象のみの設定 **-** 許可	いいえ	はい	はい
eSIM の変更を許可	いいえ	いいえ	はい
すべてのコンテンツと設定を消去	いいえ	いいえ	はい
スクリーンタイム	いいえ	いいえ	はい
ポッドキャスト	いいえ	いいえ	はい
構成プロファイルのインストール	いいえ	いいえ	はい
Touch ID と Face ID の変更	いいえ	いいえ	はい
デバイスからアプリをインストールします	いいえ	いいえ	はい
キーボードショートカット	いいえ	いいえ	はい
ペアリングされた Apple Watch	いいえ	いいえ	はい
パスコードの変更	いいえ	いいえ	はい
デバイス名の変更	いいえ	いいえ	はい
壁紙の変更	いいえ	いいえ	はい
自動的にアプリをダウンロードします	いいえ	いいえ	はい
AirDrop	いいえ	いいえ	はい
iMessage	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視対象
Siri にユーザー生成コンテンツを表示	いいえ	いいえ	はい
iBooks	いいえ	いいえ	はい
アプリの削除	いいえ	はい	はい
ゲームセンター	いいえ	いいえ	はい
友達を追加	いいえ	いいえ	はい
マルチプレーヤーゲーム	いいえ	いいえ	はい
アカウント設定の変更	いいえ	いいえ	はい
アプリの携帯ネットワークデータ設定の変更	いいえ	いいえ	はい
アプリの携帯ネットワークデータ設定の変更	いいえ	いいえ	はい
ネットワークドライブ接続を許可	いいえ	いいえ	はい
USB デバイス接続を許可	いいえ	いいえ	はい
[[デバイス］を探す］を許可	いいえ	いいえ	はい
[友達を探す］設定を許可	いいえ	いいえ	はい
[友達を探す］設定の変更	いいえ	いいえ	はい
Configurator 以外のホストとのペアリング	いいえ	いいえ	はい
予測キーボード	いいえ	いいえ	はい
キーボード自動修正	いいえ	いいえ	はい
キーボードスペルチェック	いいえ	いいえ	はい
QuickPath キーボードを許可	いいえ	いいえ	はい
定義参照	いいえ	いいえ	はい
単一のアプリバンドル **ID**			
ニュース	いいえ	いいえ	はい
Apple Music サービス	いいえ	いいえ	はい
Apple Music	いいえ	いいえ	はい
通知の変更	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視対象
アプリ使用の制限	いいえ	いいえ	はい
診断データの送信の変更	いいえ	いいえ	はい
Bluetooth の変更	いいえ	いいえ	はい
ディクテーションを許可	いいえ	いいえ	はい
Wi-Fi のオンとオフを変更	いいえ	いいえ	はい
ネットワークポリシーでインストールされた Wi-Fi ネットワークのみに参加する	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリが AirPlay と画面表示を実行できるようにする	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリがアプリとデバイスをロックできるようにする	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリのクラスに自動的に参加する	いいえ	いいえ	はい
AirPrint を許可	いいえ	いいえ	はい
AirPrint 資格情報のキーチェーンへの保存を許可する	いいえ	いいえ	はい
iBeacon を使用した AirPrint プリンターの検出を許可する	いいえ	いいえ	はい
信頼された証明書がある出力先に対してのみ AirPrint を許可する	いいえ	いいえ	はい
VPN 構成の追加	いいえ	いいえ	はい
携帯の通信プラン設定の変更	いいえ	いいえ	はい
システムアプリの削除	いいえ	いいえ	はい
近くの新しいデバイスをセットアップ	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視対象
USB 制限モードを許可	いいえ	いいえ	はい
ソフトウェア更新の強制延期	いいえ	いいえ	はい
ソフトウェア更新の強制延期	いいえ	いいえ	はい
クラスを離れるときの許可の要求を強制する	いいえ	いいえ	はい
自動入力の前に認証を強制	いいえ	いいえ	はい
自動的な日付と時刻を強制	いいえ	いいえ	はい
パスワードの自動入力	いいえ	いいえ	はい
パスワード近接要求	いいえ	いいえ	はい
パスワード共有	いいえ	いいえ	はい
パーソナルホットスポットの変更を許可	いいえ	いいえ	はい
ペアリングされていないデバイスからのブートによる復元を許可する	いいえ	いいえ	はい
緊急セキュリティ対応をインストールする	いいえ	いいえ	はい
緊急セキュリティ対応を削除する	いいえ	いいえ	はい
メールのプライバシー保護を許可する	いいえ	いいえ	はい
NFC	いいえ	いいえ	はい
App Clip を許可する	いいえ	いいえ	はい
セキュリティ - ロック画面に表示			
コントロール センター	はい	はい	はい
通知	はい	はい	はい
今日ビュー	はい	はい	はい
メディアコンテンツ - 許可			
不適切な音楽、Podcast、iTunes U コンテンツ	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視対象
iBooks の不適切な性的コンテンツ	いいえ	はい	はい
レーティング地域	いいえ	はい	はい
ムービー	いいえ	はい	はい
テレビ番組	いいえ	はい	はい
アプリ	いいえ	はい	はい

- ハードウェアの制御を許可
  - カメラ：ユーザーがデバイスでカメラを使用できるようにします。
    - **FaceTime**：ユーザーがデバイスで FaceTime を使用できるようにします。監視対象の iOS デバイス向けです。
  - スクリーンショット：ユーザーがデバイスでスクリーンショットを撮れるようにします。
    - クラスルームアプリが生徒の画面をリモートで監視することを許可する：この制限が選択されていない場合、講師はクラスルームアプリを使用してリモートで生徒の画面を監視することはできません。デフォルト設定が選択されている場合、講師はクラスルームアプリを使用して生徒の画面を監視できます。［プロンプトを表示せずにクラスルーム アプリが **AirPlay** と画面表示を実行できるようにする］の設定では、講師に権限を与えるためのプロンプトを生徒に表示するかどうかを決めます。監視対象の iOS デバイス向けです。
    - プロンプトを表示せずにクラスルームアプリが **AirPlay** と画面表示を実行できるようにする：この制限が選択されている場合、講師は生徒のデバイスで AirPlay と画面表示を実行でき、権限を求めるプロンプトは表示されません。デフォルト設定では、選択解除されています。監視対象の iOS デバイス向けです。
  - フォトストリーム： MyPhotoStream を使い、iCloud を介してすべての iOS デバイスでユーザーが写真を共有できるようにします。
  - フォトストリームを共有： iCloud Photo Sharing を使い、仕事仲間、友人、および家族とユーザーが写真を共有できるようにします。
  - 共有 **iPad** の一時セッションを許可：共有 iPad の一時セッションにアクセスできないようにします。
  - 音声ダイヤル：ユーザーデバイスで音声ダイヤルを可能にします。
  - **Siri**：ユーザーが Siri を使用できるようにします。
    - デバイスのロック中に許可：デバイスがロックされている間にユーザーが Siri を使用できるようにします。
    - **Siri** の不適切な単語フィルター： Siri の不適切な単語フィルターを有効にします。デフォルトではこの機能は制限されており、不適切な言葉はフィルタリングされません。
      Siri とセキュリティについて詳しくは、「Siri とディクテーションのポリシー」を参照してください。

  - アプリのインストール：ユーザーがアプリをインストールできるようにします。監視対象の iOS デバイス向けです。
  - ローミング中にグローバルバックグラウンドフェッチを許可する：デバイスのローミング中に iCloud とのメールアカウントの自動同期を許可するかを設定します。［オフ］の場合、iOS スマートフォンのローミング中はグローバルバックグラウンドフェッチが無効になります。デフォルトは、［オン］です。

- アプリを許可

  - **Apple App Store**：ユーザーが Apple App Store にアクセスできるようにします。監視対象の iOS デバイス向けです。
  - アプリ内課金：ユーザーがアプリ内課金で購入できるようにします。
    * 購入時に **Apple App Store** のパスワードを要求：アプリ内購入時にパスワードを求めます。デフォルトではこの機能は制限されており、アプリ内での購入ではパスワードは必要ありません。
  - **Safari**：ユーザーが Safari にアクセスできるようにします。監視対象の iOS デバイス向けです。
    * オートフィル：ユーザーが Safari でユーザー名とパスワードの自動入力をセットアップできるようにします。
    * 不正な **Web** サイトに対する警告を表示：この設定が有効で、ユーザーがフィッシング詐欺の疑いのある Web サイトにアクセスした場合、Safari はユーザーに警告します。デフォルトではこの機能は制限されており、警告が発せられません。
    * **JavaScript** を有効化： JavaScript を Safari で実行できます。
    * ポップアップをブロック： Web サイトの閲覧中にポップアップをブロックします。デフォルトではこの機能は制限されており、ポップアップはブロックされません。
  - **Cookie** を受け入れる：許可する cookie を設定します。一覧で、cookie を許可または制限するオプションを選択します。デフォルトのオプションは ［常時］で、Safari ですべての Web サイトの cookie の保存を許可します。ほかには、[現在の **Web** サイトのみ]、[許可しない]、および ［訪問したサイトからのみ］というオプションがあります。

- ネットワーク **- iCloud** の操作を許可

  - **iCloud** ドキュメントおよびデータ：ユーザーがドキュメントとデータを iCloud へ同期できるようにします。監視対象の iOS デバイス向けです。
  - **iCloud** バックアップ：ユーザーが iCloud へデバイスをバックアップできるようにします。
  - **iCloud** キーチェーン：ユーザーが、iCloud キーチェーンにパスワード、Wi-Fi ネットワーク、クレジットカードなどの情報を保存できるようにします。
  - **iCloud** のフォトライブラリ：ユーザーが iCloud の写真ライブラリにアクセスできるようにします。

- セキュリティ **-** 強制

  デフォルトでは次の機能が制限され、有効になっているセキュリティ機能はありません。

  - バックアップを暗号化：暗号化のため iCloud に強制的にバックアップします。
  - 追跡型広告を制限：ターゲティング広告の追跡をブロックします。

- 最初の **AirPlay** ペアリングでパスコードを要求： AirPlay 対応デバイスで AirPlay を使用する前に、ワンタイムオンスクリーンコードで検証するように求めます。
- 手首検出を使用するためのペアリングされた **Apple Watch**: 手首検出を使用するために Apple Watch のペアリングを求めます。
- **AirDrop** を使用して管理対象のドキュメントを共有します：このオプションを ［オン］に設定すると、AirDrop は管理対象外のドロップ先として表示されます。

• セキュリティ **-** 許可

- 信頼されていない **SSL** 証明書の受け入れ： Web サイトの信頼されていない SSL 証明書をユーザーが承認できるようにします。
- 証明書信頼設定の自動更新：信頼された機関からの証明書を自動的に更新できます。
- 管理されたペーストボードが必要：［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］および ［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］に適用する場合と同じ制限をコピーと貼り付け機能に許可します。
  たとえば、次のように構成します。
  * 管理されたペーストボードが必要：オン
  * 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：オフ
  * 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：オン
    ポリシーを iOS デバイスに展開した後、ユーザーは管理対象アプリから非管理対象アプリにデータをコピーして貼り付けることはできませんが、非管理対象アプリから管理対象アプリにデータをコピーして貼り付けることはできます。
- 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：ユーザーが、管理されている（企業）アプリから管理されていない（個人）アプリへのデータを移動できるようにします。
- 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：ユーザーが管理されていない（個人）アプリから管理されている（企業）アプリへデータを移動できるようにします。
- 診断データを **Apple** に送信：ユーザーのデバイスに関する匿名診断データの Apple への送信を許可します。
- **Touch ID** または **Face ID** によるデバイスのロック解除：ユーザーが Touch ID または Face ID を使ってデバイスのロックを解除できるようにします。
- 自動ロック解除：［オフ］の場合、ユーザーは Apple Watch を使用してペアリングされた iPhone のロックを解除することはできません。デフォルトは ［オン］です。iOS 14.5 以降で利用可能です。
- ロック時に **Wallet** 通知を表示：ロック画面での Wallet 通知の表示を許可します。
- **Handoff**：ユーザーが、ある iOS デバイスから近くにある別の iOS デバイスへアクティビティを転送できるようにします。
- 管理対象アプリの **iCloud** 同期：ユーザーが、管理されているアプリを iCloud と同期できるようにします。
- エンタープライズブックのバックアップ：エンタープライズブックの iCloud へのバックアップを許可します。
- エンタープライズブックのメモとハイライトの同期：ユーザーがエンタープライズブックに追加したメ

モやハイライトを iCloud と同期できるようにします。

- エンタープライズアプリを信頼する：エンタープライズアプリケーションを信頼できるようにします。エンタープライズアプリは、組織向けのカスタムメイドアプリです。これらは社内で作成することも、開発した外部ベンダーから購入することもできます。詳しくは、iOS でカスタムのエンタープライズ App をインストールするを参照してください。
- **Spotlight** でインターネット検索結果を表示： Spotlight で、デバイスのほかにインターネットから検索結果を表示できるようにします。
- 非管理対象アプリによる管理対象アカウント連絡先の読み取り：オプション。［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］が無効になっている場合にのみ利用できます。このポリシーを有効にすると、非管理対象アプリが管理対象アカウントの連絡先からデータを読み取ることができるようになります。デフォルトは ［オフ］です。iOS 12 以降で利用できます。
- 管理対象アプリによる非管理対象アカウント連絡先への書き込み：オプション。有効にすると、管理対象アプリによる非管理対象アカウントの連絡先への書き込みを許可します。［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］を有効にすると、この制限は有効になりません。デフォルトは［オフ］です。iOS 12 以降で利用できます。
- **Apple** のパーソナライズされた広告を許可する：［オフ］の場合、Apple 広告プラットフォームはパーソナライズされた広告を配信するためにユーザーのデータを使用しません。デフォルトは ［オン］です。iOS 14.0 以降で利用可能です。

- 監視対象のみの設定 - 許可

  これらの設定は、監視対象のデバイスにのみ適用されます。iOS デバイスを監視モードに設定する方法について詳しくは、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

  - **eSIM** の変更を許可：ユーザーがデバイスで eSIM 設定を変更できるようにします。
  - すべてのコンテンツと設定を消去：ユーザーがデバイスからすべてのコンテンツと設定を消去できるようにします。
  - スクリーンタイム：ユーザーがスクリーンタイムを有効にできるようにします。
  - ポッドキャスト：ユーザーがポッドキャストをダウンロードおよび同期できるようにします。
  - 構成プロファイルのインストール：管理者が展開した構成プロファイル以外の構成プロファイルを、ユーザーがインストールできるようにします。
  - **Touch ID** と **Face ID** の変更：ユーザーが Touch ID または Face ID を変更または削除できるようにします。
  - デバイスからアプリをインストールします：ユーザーがアプリをインストールできるようにします。この設定を無効にすると、エンドユーザーは新しいアプリをインストールできなくなります。App Store が無効になり、アイコンがホーム画面から削除されます。
  - キーボードショートカット：ユーザーが使用頻度の高い単語やフレーズのカスタムキーボードショートカットを作成できるようにします。

- ペアリングされた **Apple Watch**：ユーザーが Apple Watch と監視対象デバイスをペアリングできるようにします。
- パスコードの変更：ユーザーが監視対象デバイスでパスコードを変更できるようにします。
- デバイス名の変更：ユーザーがデバイスの名前を変更できるようにします。
- 壁紙の変更：ユーザーがデバイスの壁紙を変更できるようにします。
- 自動的にアプリをダウンロードします：アプリのダウンロードを許可します。
- **AirDrop**：ユーザーが写真、ビデオ、Web サイト、場所、およびそれ以外のものを近くの iOS デバイスで共有できるようにします。
- **iMessage**：ユーザーが Wi-Fi を使って iMessage を送信できるようにします。
- **Siri** にユーザー生成コンテンツを表示： Web のユーザー生成コンテンツを Siri でクエリできるようにします。ユーザー生成コンテンツは、従来のジャーナリストではなく、一般のユーザーが作成したものです。たとえば、Twitter や Facebook に見られるコンテンツは、ユーザー生成コンテンツです。
- **iBooks**：ユーザーが iBooks アプリを使用できるようにします。
- アプリの削除：ユーザーがデバイスからアプリを削除できるようにします。
- **Game Center**：ユーザーがデバイスの Game Center を介してオンラインゲームをプレイできるようにします。
  * 友達を追加：ユーザーが友人に通知を送信してゲームをプレイできるようにします。
  * マルチプレーヤーゲーム：ユーザーがデバイス上でマルチプレーヤーゲームを起動できるようにします。
- アカウント設定の変更：ユーザーがデバイスのアカウント設定を変更できるようにします。
- アプリの携帯データネットワーク設定の変更：携帯データネットワークをアプリがどのように使用するのか、ユーザーが変更できるようにします。
- ネットワークドライブ接続を許可： Files アプリで、ネットワークドライブに接続できないようにします。
- **USB** デバイス接続を許可： Files アプリで、接続されている USB デバイスに接続できないようにします。
- ［[デバイス］を探す］を許可：［アプリを探す］にある ［デバイスを探す］オプションを無効にします。
- ［友達を探す］設定を許可：［アプリを探す］にある ［友達を探す］オプションを無効にします。
- ［友達を探す］設定の変更：友達を探す設定をユーザーが変更できるようにします。
- **Configurator** 以外のホストとのペアリング：ユーザーデバイスがペアリングできるデバイスを管理者が制御できるようにします。この設定を無効にすると、Apple Configurator を実行している監視中のホスト以外とは、ペアリングできなくなります。監視中のホストの証明書が構成されていない場合は、すべてのペアリングが無効です。

- 予測キーボード：ユーザーデバイスで、キーボードからの入力時に候補となる単語を予測変換できるようにします。ユーザーに候補の単語を表示しない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- キーボード自動修正：ユーザーデバイスでキーボードの自動修正を使用できるようにします。ユーザーに自動修正を適用しない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- キーボードスペルチェック：ユーザーデバイスで入力中にスペルチェックを使用できるようにします。ユーザーにスペルチェッカーへアクセスさせない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- 定義参照：ユーザーデバイスで入力中に定義の検索を使用できるようにします。ユーザーに入力時での定義の検索をできるようにしない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- 単一のアプリバンドル **ID**：デバイス上のコントロールを維持し、ほかのアプリや機能との相互作用を防ぐことができるアプリの一覧を作成します。
  アプリを追加するには、［追加］をクリックし、アプリ名を入力して ［保存］をクリックします。追加するアプリごとにこの手順を繰り返します。
- **News**：ユーザーが News アプリを使用できるようにします。
- **Apple Music** サービス：ユーザーが Apple Music サービスを使用できるようにします。Apple Music サービスを許可しない場合、Music アプリはクラシックモードで動作します。
- **Apple Music**：ユーザーが Apple Music を使用できるようにします。
- 通知の変更：ユーザーが通知設定を変更できるようにします。
- アプリ使用の制限：指定したバンドル ID に基づいて、ユーザーにすべてのアプリの使用を許可するか、またはアプリの使用を個別に許可または禁止できます。監視対象のデバイスにのみ適用されます。［一部のアプリのみ許可］を選択する場合、バンドル ID `com.apple.webapp`と共にアプリを追加して Web クリップを許可します。

  > 注：
  >
  > iOS 11 以降、アプリの制限で利用できるポリシーが変更されました。適切な iOS アプリケーションバンドルを制限することで、設定アプリと電話アプリへのアクセスを削除することができなくなりました。

  いくつかのアプリをブロックするように制限デバイスポリシーを構成して展開した後で、これらのアプリの一部またはすべてを許可する必要が生じた場合、制限デバイスポリシーを変更して展開しても制限は変更されません。これは、iOS では変更内容が iOS プロファイルに適用されないためです。変更内容を適用するには、プロファイルの削除ポリシーを使用して該当する iOS プロファイルを削除してから、更新した制限デバイスポリシーを展開します。

この設定を ［一部のアプリのみ許可］に変更する場合：このポリシーを展開する前に、Apple Deployment Program を使用して登録したデバイスのユーザーに、セットアップアシスタントから Apple アカウントにサインインするよう指示してください。それ以外の場合、ユーザーが Apple アカウントにサインインして許可されたアプリにアクセスするには、各自のデバイスで 2 要素認証を無効にする必要があります。

- 診断データの送信の変更：ユーザーが ［設定］**>**［診断と使用状況］ペインで診断データの送信とアプリ分析に関する設定を変更できるようにします。
- **Bluetooth** の変更：ユーザーが Bluetooth の設定を変更できるようにします。
- ディクテーションを許可：監視のみ。この制限が ［オフ］に設定されている場合、ディクテーションを使用した入力（音声テキスト変換を含む）は許可されません。デフォルトでは、［オン］になっています。
- **Wi-Fi** のオンとオフを変更：設定またはコントロールセンターで Wi-Fi がオンまたはオフにならないようにします。また、機内モードに入っても影響はありません。この制限によって、使用する Wi-Fi ネットワークの選択が妨げられることはありません。
- ネットワークポリシーでインストールされた **Wi-Fi** ネットワークのみに参加する：オプション。監視のみ。この制限が ［オン］に設定されている場合、構成プロファイルを使用して設定されたデバイスのみが Wi-Fi ネットワークに接続できます。デフォルトでは ［オフ］になっています。
- プロンプトを表示せずにクラスルームアプリが **AirPlay** と画面表示を実行できるようにする：この制限が選択されている場合、講師は生徒のデバイスで AirPlay と画面表示を実行でき、権限を求めるプロンプトは表示されません。デフォルト設定では、選択解除されています。監視対象の iOS デバイス向けです。
- プロンプトを表示せずにクラスルームアプリがアプリとデバイスをロックできるようにする：この制限が ［オン］に設定されている場合、クラスルームアプリはユーザープロンプトを表示せず自動的に、アプリに対してユーザーデバイスをロックし、ユーザーデバイスをロックします。デフォルトでは ［オフ］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- プロンプトを表示せずにクラスルームアプリのクラスに自動的に参加する：この制限が ［オン］に設定されている場合、クラスルームアプリはユーザーにプロンプトを表示せずに自動的にクラスに参加します。デフォルトでは ［オフ］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- **AirPrint** を許可：この制限が ［オフ］に設定されている場合、ユーザーは AirPrint で印刷できません。デフォルトでは、［オン］になっています。この制限が ［オン］の場合、さらに次の制限が表示されます。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
  * **AirPrint** 資格情報のキーチェーンへの保存を許可する：この制限が選択されていない場合、AirPrint のユーザー名とパスワードはキーチェーンに保存されません。デフォルト設定では選択されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
  * **iBeacons** を使用した **AirPrint** プリンターの検出を許可する：この制限が選択されていない場合、AirPrint プリンターの iBeacon 検出は無効になります。この設定により、偽の AirPrint

Bluetooth ビーコンのネットワークトラフィックがフィッシングされるのを防止します。デフォルト設定では選択されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。

* 信頼された証明書がある出力先に対してのみ **AirPrint** を許可する：この制限が選択されている場合、ユーザーは、信頼された機関からの証明書がある出力先にのみ AirPrint を使用して印刷できます。デフォルト設定では、選択解除されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。

- **VPN** 構成の追加：この制限が ［オフ］に設定されている場合、ユーザーは VPN 構成を作成できません。デフォルトでは、［オン］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- 携帯の通信プラン設定の変更：この制限が ［オフ］に設定されている場合、ユーザーは携帯の通信プラン設定を変更できません。デフォルトでは、［オン］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- システムアプリの削除：この制限が ［オフ］に設定されている場合、ユーザーはデバイスからシステムアプリを削除できません。デフォルトでは、［オン］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- 近くの新しいデバイスをセットアップ：この制限が［オフ］に設定されている場合、ユーザーは近くの新しいデバイスを設定できません。デフォルトでは、［オン］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- **USB** 制限モードを許可：［オフ］の場合、デバイスはロックされた状態でも常に USB アクセサリーに接続できます。デフォルトは ［オン］です。iOS 11.3 以降の監視対象デバイスでのみ利用できます。
- ソフトウェア更新の延期を強制する：［オン］の場合、ソフトウェアの更新がユーザーに表示される時期が延期されます。この制限が設定されている場合、ソフトウェアの更新がリリースされてから指定された日数が経過するまで、ソフトウェアの更新は表示されません。デフォルトは ［オフ］です。iOS 11.3 以降の監視対象デバイスでのみ利用できます。OS の更新ポリシーには、デバイスが更新を受信する頻度を制御するためのさらに多くの設定が含まれています。詳しくは、「OS の更新デバイスポリシー」を参照してください。
- ソフトウェア更新の強制延期期間（日）：デバイス上でソフトウェアの更新を遅らせる日数を指定できます。最大延期日数は **90** 日です。デフォルトは **30** 日です。iOS 11.3 以降の監視対象デバイスでのみ利用できます。
- クラスルームを離れるときの許可の要求を強制する：［オン］の場合、クラスルームの管理対象外コースに登録した学生は、コースを離れるときに教師の許可を求める必要があります。デフォルトは ［オフ］です。iOS 11.3 以降の監視対象デバイスでのみ利用できます。
- 自動入力の前に認証を強制：ユーザーが自動入力機能を使用する前に、ユーザーに認証を強制します。
- 日時の自動設定を強制する：監視対象デバイスの日時を自動で設定できます。［オン］の場合、デバイスユーザーは ［一般］**>**［日付と時刻］で ［自動設定］をオフにできません。デバイスのタイムゾーン

は、デバイスが現在位置を特定できる場合にのみ更新されます。つまり、デバイスが移動体通信ネットワークまたは Wi-Fi に接続しており、位置情報サービスが有効になっている場合のみです。デフォルトは ［オフ］です。iOS 12 以降の監視対象デバイスでのみ利用できます。

- パスワードの自動入力：オプション。無効にすると、ユーザーはパスワードの自動入力または自動強力パスワード機能を使用できません。デフォルトは ［オン］です。iOS 12 以降で利用できます。
- パスワード近接要求：オプション。無効にすると、ユーザーのデバイスは近くのデバイスにパスワードを要求しません。デフォルトは ［オン］です。iOS 12 以降で利用できます。
- パスワード共有：オプション。無効にすると、ユーザーは AirDrop パスワード機能を使用してパスワードを共有できません。デフォルトは ［オン］です。iOS 12 以降で利用できます。
- パーソナルホットスポットの変更を許可：ユーザーがパーソナルホットスポットの設定を変更できないようにします。
- ペアリングされていないデバイスからのブートによる復元を許可する：［オン］の場合、デバイスはペアリングされていないデバイスからのブートによって復元できます。デフォルトは ［オフ］です。iOS 14.5 以降で利用可能です。
- 緊急セキュリティ対応をインストールする：［オフ］の場合、緊急セキュリティ対応のインストールが禁止されます。デフォルトは ［オン］です。
- 緊急セキュリティ対応を削除する：［オフ］の場合、緊急セキュリティ対応の削除が禁止されます。デフォルトは ［オン］です。
- メールのプライバシー保護を許可する：［オフ］の場合、デバイスでのメールのプライバシー保護が無効になります。デフォルトは ［オン］です。iOS 15.2 以降で利用可能です。
- **NFC**：［オフ］の場合、NFC が無効になります。デフォルトは ［オン］です。iOS 14.2 以降で利用可能です。
- **App Clip** を許可する：［オフ］の場合、ユーザーは App Clip を追加できなくなり、デバイス上の既存の App Clip が削除されます。デフォルトは ［オン］です。iOS 14.0 以降で利用可能です。

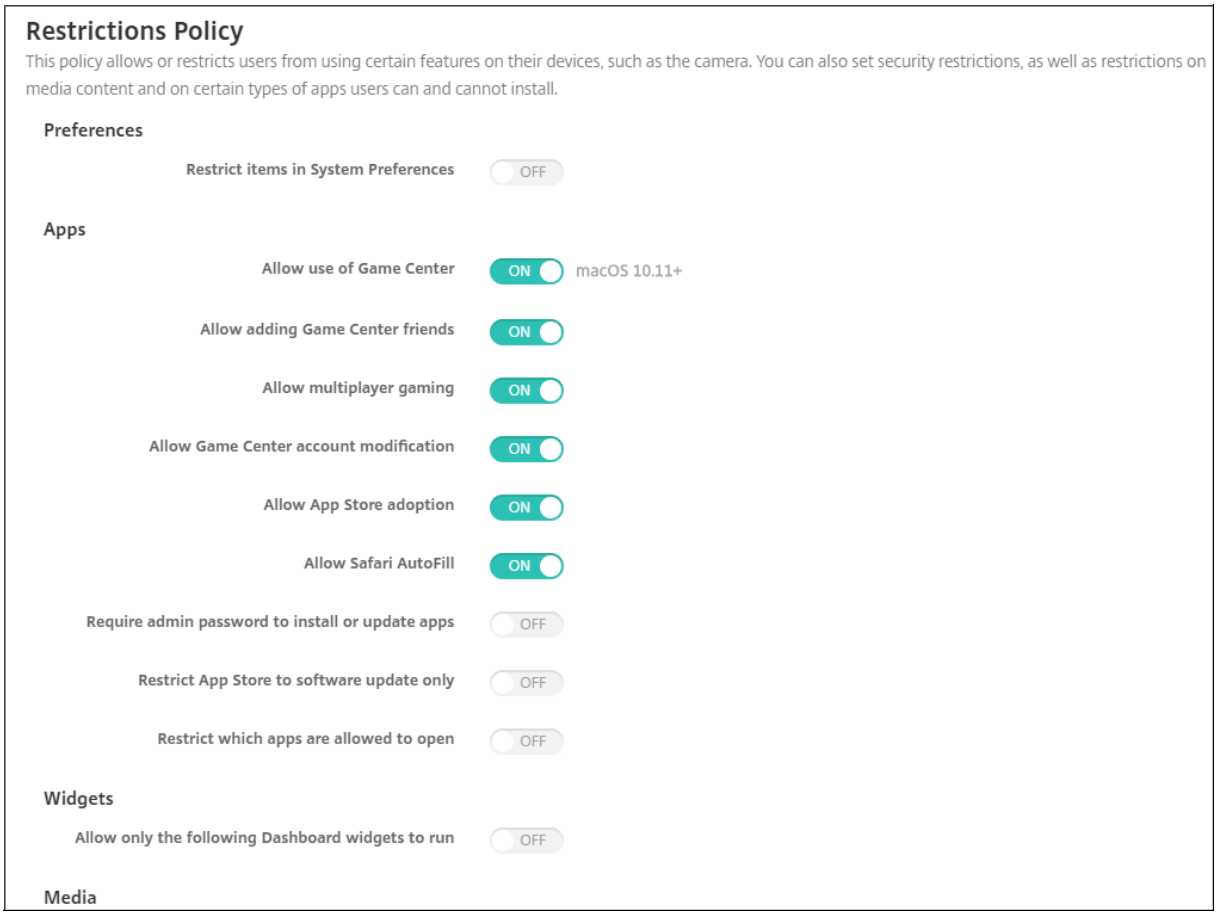
- セキュリティ **-** ロック画面に表示
  - コントロールセンター：ロック画面のコントロールセンターへアクセスできるようにします。コントロールセンターでは、機内モード、Wi-Fi、Bluetooth、おやすみモード、画面の向きをロックといった設定をユーザーが簡単に変更できます。
  - 通知：ロック画面上へ通知できるようにします。
  - 今日ビュー：天気や当日の予定といった情報を表示する今日の表示をロック画面上で有効にします。
- メディアコンテンツ **-** 許可
  - 不適切な音楽、**Podcast**、**iTunes U** コンテンツ：ユーザーのデバイスで成人向けのコンテンツを許可します。

- **iBooks** の不適切な性的コンテンツ： iBooks から成人向けのコンテンツをダウンロードできるようにします。
- レーティング地域：ペアレンタルコントロールのレートを取得する地域を設定します。一覧では、国をクリックするとレート地域が設定されます。デフォルトは ［米国］です。
- ムービー：ユーザーのデバイスでムービーを操作できるかどうかを設定します。ムービーの操作が許可される場合は、オプションでムービーのレートレベルを設定します。一覧で、デバイスでムービーを許可または制限するオプションをクリックします。デフォルトは［すべてのムービーを許可］です。
- テレビ番組：ユーザーのデバイスでテレビ番組を操作できるかどうかを設定します。テレビ番組の操作が許可される場合は、オプションでテレビ番組のレートレベルを設定します。一覧で、デバイスでテレビ番組を許可または制限するオプションをクリックします。デフォルトは［すべてのテレビ番組を許可］です。
- アプリ：ユーザーのデバイスでアプリを操作できるかどうかを設定します。アプリの操作が許可される場合は、オプションでムービーのレートレベルを設定します。一覧で、デバイスでアプリを許可または制限するオプションをクリックします。デフォルトは［すべてのアプリを許可］です。

- ポリシー設定

  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは iOS 9.3 以降でのみ使用できます。

macOS 設定



設定	監視対象外	監視対象
アプリ		
Game Center の使用を許可	いいえ	はい
Game Center の友達の追加を許可	いいえ	はい
マルチプレーヤーゲームを許可	いいえ	はい
Game Center のアカウント変更を許可	はい	はい
App Store の採用を許可	はい	はい
Safari の自動入力を許可	いいえ	はい
アプリのインストールまたはアップデートで管理者パスワードを必須にする	はい	はい
App Store をソフトウェアの更新のみに制限	はい	はい

設定	監視対象外	監視対象
開くのを許可するアプリの制限	はい	はい
メディア		
AirDrop を許可	いいえ	はい
機能		
デスクトップ画像をロック	いいえ	はい
カメラの使用を許可	いいえ	はい
Apple Music を許可する	いいえ	はい
Spotlight の検索候補を許可	はい	はい
検索を許可	はい	はい
ローカルアカウントでの iCloud パスワードの使用を許可	はい	はい
iCloud ドキュメントおよびデータを許可	はい	はい
iCloud で”デスクトップ”と”書類”を許可する	いいえ	はい
iCloud キーチェーンの同期を許可する	いいえ	はい
iCloud で“メール”を許可する	はい	はい
iCloud で“連絡先”を許可する	はい	はい
iCloud で“カレンダー”を許可する	はい	はい
iCloud で“リマインダー”を許可する	はい	はい
iCloud ブックマークを許可する	はい	はい
iCloud で“メモ”を許可する	はい	はい
iCloud で”写真”を許可する	はい	はい
自動ロックの解除を許可する	はい	はい
Mac のロック解除に Touch ID を許可する	はい	はい
ソフトウェア更新の強制延期	いいえ	はい
パスワードの自動入力	いいえ	はい
パスワード近接要求	いいえ	はい

パスワード共有	はい	はい

- 環境設定
  - システム環境設定のアイテムの制限：システム環境設定へのユーザーのアクセスを許可または制限します。デフォルトは ［オフ］で、ユーザーにはシステム環境設定へのフルアクセス権が付与されます。有効にした場合は、次の設定を構成します。
    - システム環境設定ペイン：選択した設定を有効にするのか、無効にするのかを選択します。デフォルトではすべての設定が有効になるように、すなわち ［オン］に設定されています。
      - ユーザーおよびグループ
      - 一般
      - アクセシビリティ
      - App Store
      - ソフトウェアの更新
      - Bluetooth
      - CD と DVD
      - 日時
      - デスクトップとスクリーンセーバー
      - ディスプレイ
      - ドック
      - エネルギーセーバー
      - 拡張機能
      - ファイバーチャネル
      - iCloud
      - インク
      - インター ネットアカウント
      - キーボード
      - 言語とテキスト
      - Mission Control
      - マウス
      - ネットワーク
      - 通知
      - ペアレンタルコントロール
      - プリンターとスキャナー
      - プロファイル
      - セキュリティとプライバシー
      - 共有
      - サウンド
      - ディクテーションと音声入力
      - Spotlight

・起動ディスク
・Time Machine
・トラックパッド
・Xsan

- アプリ
  - **Game Center** の使用を許可：ユーザーが Game Center を介してオンラインゲームをプレイできるようにします。デフォルトは ［オン］です。
  - **Game Center** の友達の追加を許可：ユーザーが友人に通知を送信してゲームをプレイできるようにします。デフォルトは ［オン］です。
  - マルチプレーヤーゲームを許可：ユーザーがマルチプレーヤーゲームを開始できるようにします。デフォルトは ［オン］です。
  - **Game Center** のアカウント変更を許可：ユーザーが各自の Game Center アカウント設定を変更できるようにします。デフォルトは ［オン］です。
  - **App Store** の採用を許可： OS X に既に存在するアプリの App Store への登録を許可または制限します。デフォルトは ［オン］です。
  - **Safari** の自動入力を許可： Safari に保存されているパスワード、アドレス、およびその他の基本情報が自動的に Web サイトのフィールドに入力されるようにします。デフォルトは ［オン］です。
  - アプリのインストールまたはアップデートで管理者パスワードを必須にする：アプリをインストールまたは更新するときに管理者のパスワードを必須にします。デフォルトは ［オフ］で、管理者のパスワードが不要であることを意味します。
  - **App Store** をソフトウェアの更新のみに制限： App Store を更新のみに制限します。つまり、［アップデート］以外の App Store のタブはすべて無効になります。デフォルトは ［オフ］で、App Store へのフルアクセスが許可されます。
  - 開くのを許可するアプリ制限ポリシー：ユーザーが使用できるアプリを制限または許可します。デフォルトは［オフ］で、すべてのアプリの使用が許可されます。有効にした場合は、次の設定を構成します：
    * 許可するアプリ：［追加］をクリックして、起動を許可するアプリの名前およびバンドル ID を入力し、［保存］をクリックします。Citrix 業務用モバイルアプリの場合は、アプリを追加するときに［パッケージ **ID**］フィールドの ID を使用します。各アプリで起動を許可するたびに、この手順を繰り返します。
    * 許可しないフォルダー：［追加］をクリックして、ユーザーアクセスを制限するフォルダーまでのファイルパス（例：/Applications/Utilities）を入力し、［保存］をクリックします。ユーザーにアクセスできないようにするすべてのフォルダーについて、この手順を繰り返します。
    * 許可するフォルダー：［追加］をクリックして、ユーザーアクセスを許可するフォルダーまでのファイルパスを入力し、［保存］をクリックします。ユーザーにアクセスできるようにするすべてのフォルダーについて、この手順を繰り返します。
- ウィジェット
  - 以下のダッシュボードウィジェットのみ実行を許可：［オン］の場合、ユーザーはこの設定で構成されたダッシュボードウィジェットのみを実行できます。デフォルトは ［オフ］で、ユーザーはすべてのウィ

ジェットを実行できます。有効にした場合は、次の設定を構成します：

* 許可するウィジェット：［追加］をクリックして、実行を許可するウィジェットの名前および ID を入力し、［保存］をクリックします。ダッシュボードでの実行を許可するウィジェットごとに、この手順を繰り返します。

- メディア
  - **AirDrop** を許可：ユーザーが写真、ビデオ、Web サイト、場所、およびそれ以外のものを近くの iOS デバイスで共有できるようにします。
- 共有
  - 新しい共有サービスを自動で有効にする：共有サービスを自動的に有効にするかどうかを選択します。
  - メール：共有メールボックスを許可するかどうかを選択します。
  - **Facebook**：共有 Facebook アカウントを許可するかどうかを選択します。
  - ビデオサービス **- Flickr**、**Vimeo**、**Tudou**、**Youku**：共有ビデオサービスを許可するかどうかを選択します。
  - **Aperture** に追加： Aperture への追加を行う共有機能を許可するかどうかを選択します。
  - **Sina Weibo**：共有 Sina Weibo アカウントを許可するかどうかを選択します。
  - **Twitter**：共有 Twitter アカウントを許可するかどうかを選択します。
  - メッセージ：メッセージへの共有アクセスを許可するかどうかを選択します。
  - **iPhoto** に追加： iPhoto への追加を行う共有機能を許可するかどうかを選択します。
  - リーディングリストに追加：リーディングリストへの追加を行う共有機能を許可するかどうかを選択します。
  - **AirDrop**：共有 AirDrop アカウントを許可するかどうかを選択します。
- 機能
  - デスクトップ画像をロック：ユーザーがデスクトップの画像を変更できるかどうかを選択します。デフォルトは ［オフ］で、ユーザーがデスクトップの画像を変更できることを意味します。
  - カメラの使用を許可：ユーザーが Mac でカメラを使用できるかどうかを選択します。デフォルトは［オフ］で、ユーザーがカメラを使用できないことを意味します。
  - **Apple Music** を許可する：ユーザーが Apple Music サービスを使用できるようにします（macOS 10.12 以降）。Apple Music サービスを許可しない場合、Music アプリはクラシックモードで動作します。監視対象のデバイスにのみ適用されます。デフォルトは、［オン］です。
  - **Spotlight** の検索候補を許可：ユーザーが［Spotlight の検索候補］を使用して Mac を検索したり、［Spotlight の検索候補］にインターネットや App Store の項目を表示したりできるかどうかを選択します。デフォルトは ［オフ］で、ユーザーは［Spotlight の検索候補］を使用できません。
  - 検索を許可：ユーザーがコンテキストメニューまたは Spotlight 検索メニューで単語の定義を検索できるかどうかを選択します。デフォルトは［オフ］で、この場合、ユーザーは Mac で検索機能を使用できません。
  - ローカルアカウントでの **iCloud** パスワードの使用を許可：ユーザーが各自の Apple ID および iCloud パスワードを使用して Mac にサインオンできるかどうかを選択します。これを有効にすることは、ユー

ザーが Mac のすべてのログイン画面で同じ ID およびパスワードを使用することを意味します。デフォルトは ［オン］で、ユーザーは各自の Apple ID および iCloud パスワードを使用して Mac にアクセスすることができます。

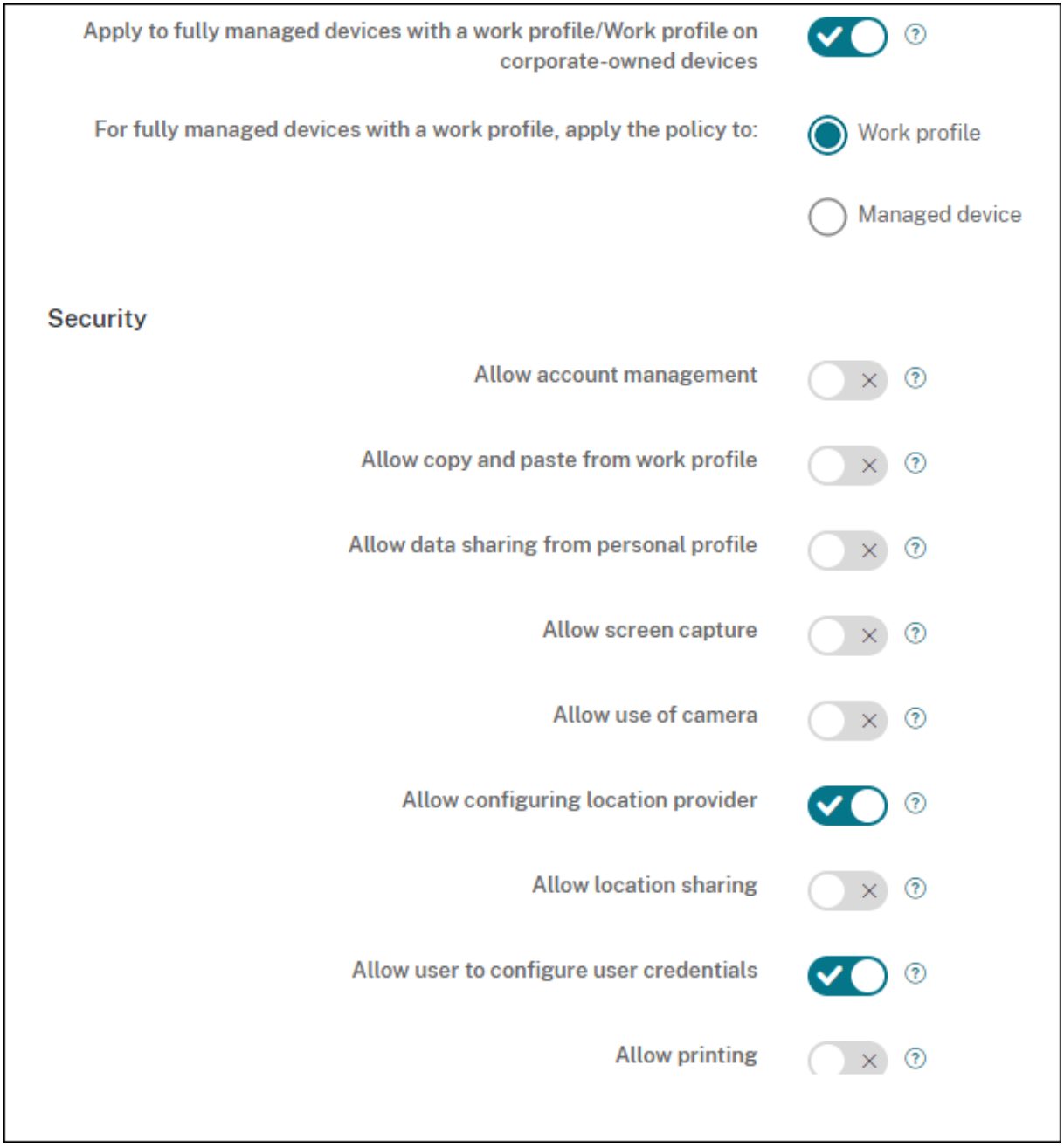
- **iCloud** ドキュメントおよびデータを許可：ユーザーが Mac から iCloud に保存されているドキュメントおよびデータにアクセスするのを許可するかどうかを選択します。デフォルトは［オン］で、ユーザーは Mac から iCloud に保存されているドキュメントおよびデータを使用できないようになっています。
  - **iCloud** で”デスクトップ”と”書類”を許可する：（macOS 10.12.4 以降）デフォルトは［オン］です。
- **iCloud** キーチェーンの同期を許可する： iCloud キーチェーンの同期を許可します（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”メール”を許可する：ユーザーが iCloud メールを使用できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”連絡先”を許可する：ユーザーが iCloud の連絡先を使用できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”カレンダー”を許可する：ユーザーが iCloud のカレンダーを使用できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”リマインダー”を許可する：ユーザーが iCloud のリマインダーを使用できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** ブックマークを許可する：ユーザーが iCloud のブックマークと同期できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”メモ”を許可する：ユーザーが iCloud のメモを使用できるようにします（macOS 10.12 以降）。デフォルトは ［オン］です。
- **iCloud** で”写真”を許可する：この設定を［オフ］に変更すると、iCloud のフォトライブラリから完全にダウンロードされていない写真はすべてデバイスのローカルストレージから削除されます（macOS 10.12 以降）。デフォルトは ［オン］です。
- 自動ロックの解除を許可する：このオプションと Apple Watch については、https://www.imore.com/auto-unlockを参照してください（macOS 10.12 以降）。デフォルトは ［オン］です。
- **Mac** のロック解除に **Touch ID** を許可する：（macOS 10.12.4 以降）デフォルトは ［オン］です。
- ソフトウェア更新の延期を強制する：［オン］の場合、ソフトウェアの更新がユーザーに表示されるまでの時間が延期されます。ソフトウェアの更新がリリースされてから指定の日数が経過するまで、ユーザーにソフトウェアの更新は表示されません。デフォルトは ［オフ］です。macOS 10.13.4 以降を実行する監視対象デバイスでのみ利用できます。OS の更新ポリシーには、デバイスが更新を受信する頻度を制御するためのさらに多くの設定が含まれています。詳しくは、「OS の更新デバイスポリシー」を参照してください。
- ソフトウェア更新の強制延期期間（日）：デバイス上でソフトウェアの更新を延期する日数を指定します。日数の上限は 90 日です。デフォルトは **30** です。macOS 10.13.4 以降を実行する監視対象デバイスでのみ利用できます。
- パスワードの自動入力：オプション。無効にすると、ユーザーはパスワードの自動入力または自動強力パスワード機能を使用できません。デフォルトは ［オン］です（macOS 10.14 以降）。

- パスワード近接要求：オプション。無効にすると、ユーザーのデバイスは近くのデバイスにパスワードを要求しません。デフォルトは ［オン］ です（macOS 10.14 以降）。
- パスワード共有：オプション。無効にすると、ユーザーは AirDrop パスワード機能を使用してパスワードを共有できません。デフォルトは ［オン］ です（macOS 10.14 以降）。

Android の設定

- カメラ：ユーザーがデバイスでカメラを使用できるようにします。［オフ］ の場合、カメラは無効になります。デフォルトは、［オン］ です。

Android Enterprise の設定



新規のまたは工場出荷時の設定にリセットされた Android デバイスが仕事用プロファイルモードで登録されると、Android 9.0～10.x を実行しているデバイスは、仕事用プロファイルを持つ管理対象デバイスとして登録されます。Android 11 以降、デバイスは会社所有のデバイスの仕事用プロファイルとして登録されます。制限ポリシーは、デバイスの仕事用プロファイルまたは管理対象デバイスのいずれかに適用できます。

会社所有のデバイスの仕事用プロファイルモードに登録されているデバイスでは、次の制限は機能しません:

- バックアップ サービスを許可

- システムアプリを有効にする
- Keyguard がデバイスをロックしないようにする
- ステータスバーの使用を許可
- デバイス画面を有効なまま維持する
- ユーザーにアプリケーション設定の制御を許可
- ユーザーにユーザー資格情報の構成を許可
- VPN 構成を許可
- USB 大容量ストレージを許可
- 工場出荷時リセットを許可
- アプリのアンインストールを許可
- Google Play 非対応アプリを許可
- プロファイル間でコピーと貼り付けを許可
- アプリの検証を有効化
- アカウント管理を許可
- 印刷を許可
- NFC を許可
- ユーザーの追加を許可

デバイスが Android Enterprise の仕事用プロファイルモードで登録されている場合、デフォルトでは **USB** デバッグおよび不明なソース設定は無効になっています。

詳しくは、このビデオをご覧ください:

- 仕事用プロファイルで完全に管理されているデバイスに適用 **/**会社所有のデバイスの仕事用プロファイルに適用：仕事用プロファイルで完全に管理されたデバイスの制限ポリシー設定を構成できます。これらのデバイス

は、COPE（個人使用可能なコーポレート所有）デバイスとも呼ばれます。この設定が ［オン］の場合、次のいずれかの設定を選択します：

- 仕事用プロファイル：構成した制限設定は、デバイスの仕事用プロファイルにのみ適用されます。
- 管理対象デバイス：構成した制限設定は、デバイスにのみ適用されます。

この設定が ［オフ］の場合、構成する資格情報設定はデバイスに適用されます（明示的に仕事用プロファイルに適用される設定を除く）。デフォルトは ［オフ］です。

［仕事用プロファイルで完全に管理されているデバイスに適用 **/**会社所有のデバイスの仕事用プロファイルに適用］がオフの場合、次の設定を構成します：

- セキュリティ
  - アカウント管理を許可：仕事用プロファイルおよび管理対象デバイスでアカウントを追加できるようにします。デフォルトは ［オフ］です。
  - 仕事用プロファイルからのコピーと貼り付けを許可：［オン］の場合、ユーザーは仕事用プロファイルのアプリから個人用プロファイルのアプリにデータをコピーして貼り付けることができます。デフォルトは ［オフ］です。
  - 個人用プロファイルからのデータ共有を許可：［オン］の場合、ユーザーは個人用プロファイルの アプリから仕事用プロファイルのアプリに共有データをコピーして貼り付けることができます。デフォルトは［オフ］です。
  - スクリーンショットを許可：ユーザーがデバイス画面のスクリーンショットを取得できるかどうかを指定します。デフォルトは ［オフ］です。
  - カメラの使用を許可：ユーザーがデバイスのカメラで写真やビデオを撮ることができます。デフォルトは ［オフ］です。
  - **VPN** 構成を許可：ユーザーが VPN 構成を作成できるようにします。Android 6 以降を実行する仕事用プロファイルデバイスおよび完全に管理されているデバイス向けです。デフォルトは ［オン］です。
  - バックアップサービスを許可：ユーザーがデバイス上にアプリケーションやシステムデータをバックアップできるようにします。デフォルトは ［オン］です。
  - **NFC** を許可：近距離無線通信（NFC：Near Field Communication）を使用して、ユーザーが手元のデバイスから他のデバイスに Web ページ、写真、ビデオなどのコンテンツを送信できるようにします。MDM 4.0 以降。デフォルトは ［オン］です。
  - 位置情報プロバイダーの構成を許可：ユーザーがデバイスで GPS をオンにできるようにします。Android API 28 以降で使用します。デフォルトは ［オン］です。
  - 位置情報の共有を許可：管理対象プロファイルの場合、デバイス所有者は設定を上書きできます。デフォルトは ［オフ］です。

> ヒント：
>
> Citrix Endpoint Management で位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。「位置情報デバイスポリシー」を参照してください。

  - ユーザーにユーザー資格情報の構成を許可：ユーザーが管理対象のキーストアで認証情報を設定できるかどうかを指定します。デフォルトは ［オン］です。
  - 印刷を許可：［オン］にすると、ユーザーデバイスからアクセス可能なプリンターへの印刷が許可されます。デフォルトは ［オフ］です。利用可能：Android 9 以降。
  - **USB** デバッグを許可：デフォルトは ［オフ］です。

- アプリ
  - システムアプリを有効化：ユーザーが事前インストールされたデバイスアプリを実行できるようにします。デフォルトは［オフ］です。特定のアプリを有効にするには、［システムアプリ一覧］の表で ［追加］をクリックします。
    * システムアプリ一覧：デバイスで有効にするシステムアプリの一覧。［システムアプリを有効化］を ［オン］に設定して、アプリのパッケージ名を追加します。システムアプリのパッケージ名を検索するには、Android Debug Bridge（adb）を使用して Android パッケージマネージャー（pm）コマンドを呼び出します。たとえば `adb shell "pm list packages -f name"`で、ここで「名前」はパッケージ名の一部です。詳しくは、https://developer.android.com/studio/command-line/adbを参照してください。Android Enterprise デバイスでは、Android Enterprise アプリの権限ポリシーを使用してアプリの権限を制限できます。
  - アプリケーションを無効化：指定したアプリの一覧がデバイス上で実行されるのを禁止します。デフォルトは ［オフ］です。インストールされているアプリを無効にするには、設定を ［オン］に変更し、［アプリケーション一覧］表で ［追加］をクリックします。
    * アプリ一覧：禁止するアプリの一覧。［アプリケーションを無効にする］を ［オン］に設定してアプリを追加し、アプリのパッケージ名を入力します。アプリ一覧を変更して展開すると、以前のアプリ一覧が上書きされます。例：com.example1 と com.example2 を無効にしてから、アプリ一覧の内容を com.example1 と com.example3 に変更すると、com.example.2 が有効になります。
  - アプリの検証を有効化： OS がアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは ［オン］です。
  - **Google Apps** を有効化：ユーザーが Google Mobile Services からデバイスにアプリをダウンロードできるようにします。デフォルトは ［オン］です。
  - **Google Play** 非対応アプリを許可： Google Play 以外のストアからアプリをインストールできるようにします。デフォルトは ［オフ］です。
  - すべてのプロファイルで **Google Play** 以外のアプリを許可：［オン］の場合、ユーザーは Google Play 以外のストアのアプリをデバイスのすべてのプロファイルにインストールできます。デフォルトは ［オフ］です。

  - ユーザーにアプリケーション設定の制御を許可：ユーザーがアプリのアンインストール、アプリの無効化、キャッシュやデータの消去、アプリの強制停止、デフォルト値のクリアをできるようにします。ユーザーは、設定アプリからこれらのアクションを実行します。デフォルトは ［オフ］です。
  - アプリのアンインストールを許可：ユーザーが管理対象の Google Play ストア内からアプリをアンインストールできるようにします。デフォルトは ［オフ］です。

- **BYOD/**仕事用プロファイル

  - 接続されたアプリを有効にする：有効にすると、ユーザーは仕事と個人の両方のデータを利用して、仕事と個人のプロファイル間で通信できるアプリを選択できます。有効にした後、［追加］をクリックし、目的のアプリを選択して、［保存］をクリックします。この機能を有効にするには、作業プロファイルが必要です。デフォルトは ［オフ］です。
  - ホーム画面で仕事用プロファイルアプリウィジェットを許可する：この設定が ［オン］の場合、ユーザーが仕事用プロファイルアプリウィジェットをデバイスのホーム画面に配置できます。この設定が ［オフ］の場合、ユーザーは仕事用プロフィールアプリウィジェットを端末のホーム画面に配置できません。デフォルトは ［オフ］です。
    * ウィジェットが許可されたアプリ：ホーム画面で許可するアプリの一覧。［ホーム画面で仕事用プロファイルアプリのウィジェットを許可］を ［オン］に設定して対象のアプリを追加します。［追加］をクリックし、一覧からホーム画面で許可するアプリを選択します。［保存］をクリックします。この手順を繰り返して、ほかのアプリウィジェットも許可します。
  - デバイスの連絡先で仕事用プロファイルの連絡先を許可：着信時に、管理対象の Android Enterprise プロファイルの連絡先を親プロファイルに表示します（Android 7.0 以降）。デフォルトは［オフ］です。

- 完全管理対象デバイスのみ

  - ユーザーの追加を許可：ユーザーがデバイスに新しいユーザーを追加できるようにします。デフォルトは ［オン］です。
  - データローミングを許可：ユーザーがローミング中に携帯データネットワークを使用できるようにします。デフォルトは［オフ］で、ユーザーのデバイスでローミングが無効になっています。デフォルトは［オフ］です。
  - **SMS** を許可：ユーザーが SMS メッセージを送受信できるようにします。デフォルトは ［オフ］です。
  - ステータスバーの使用を許可：［オン］に設定すると、管理対象デバイスおよび専用デバイス（COSU デバイス）上でステータスバーが有効になります。この設定により、通知、クイック設定、その他の画面オーバーレイで全画面モードから移動することができなくなります。ユーザーはシステム設定に移動して通知を表示できます。Android 6.0 以降の場合、デフォルトは ［オフ］です。
  - **Bluetooth** を許可：ユーザーが Bluetooth を使用できるようにします。デフォルトは ［オン］です。
    * **Bluetooth** 共有を許可：オフになっている場合、ユーザーはデバイスで送信による Bluetooth 共有を確立できません。デフォルトではオンになっています。
  - 日付と時刻の構成を許可：ユーザーがデバイスの日付と時刻を変更できるようにします。デフォルトは［オン］です。

- 工場出荷時リセットを許可：ユーザーがデバイスを出荷時の設定に戻すことができるようにします。デフォルトは ［オン］です。
- デバイス画面を有効なまま維持する：この設定を ［オン］に設定すると、デバイスを接続してもデバイス画面はオンのままです。デフォルトは ［オフ］です。
- **USB** 大容量ストレージを許可： USB 接続上で、ユーザーのデバイスとコンピューター間で大容量のデータファイルを転送できるようにします。デフォルトは ［オン］です。
- マイクを許可：ユーザーがデバイスでマイクを使用できるようにします。デフォルトは ［オン］です。
- テザリングを許可：ユーザーがポータブルホットスポットとテザリングデータを構成できるようにします。デフォルトは ［オフ］です。
- **Keyguard** がデバイスをロックしないようにする：［オン］の場合、この設定により管理対象デバイスおよび専用デバイス（COSU デバイス）のロック画面で Keyguard が無効になります。デフォルトは ［オフ］です。
- **Wi-Fi** の変更を許可：［オン］場合、ユーザーは Wi-Fi をオンまたはオフにして、Wi-Fi ネットワークに接続できます。デフォルトは ［オン］です。
- ファイル転送を許可： USB 上でファイル転送できるようにします。デフォルトは ［オフ］です。

- **Samsung**

  - **TIMA** キーストアを有効化： TIMA KeyStore は、対称キーの TrustZone ベースのセキュアなキーストレージを提供します。RSA キーペアと証明書は、ストレージのデフォルトのキーストアプロバイダーを経由します。デフォルトは ［オフ］です。
  - 共有一覧を許可：ユーザーが Share Via の一覧にあるアプリ間でコンテンツを共有できるようにします。デフォルトは ［オン］です。
  - 監査ログを有効化：デバイスのフォレンジック解析用イベント監査ログの作成を有効にします。デフォルトは ［オフ］です。

- **Samsung**：完全管理対象デバイスのみ

  - **ODE** 信頼済み起動検証を有効化： ODE 信頼済みブート検証を使って、ブートローダーからシステムイメージへの信頼のチェーンを確立します。デフォルトは ［オン］です。
  - 緊急電話のみを許可：ユーザーがデバイスで緊急電話のみモードを有効にできるようにします。デフォルトは ［オフ］です。
  - ファームウェアリカバリを許可：ユーザーがデバイスでファームウェアを復元できるようにします。デフォルトは ［オン］です。
  - 高速暗号化を許可：使用済みのメモリ領域のみ暗号化を許可します。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは対照的な方法です。このデータには設定、アプリケーションデータ、ダウンロードしたファイルおよびアプリケーション、メディア、およびその他のファイルが含まれます。デフォルトは ［オン］です。
  - 情報セキュリティ国際評価基準（**Common Criteria**）モードを有効化：デバイスを情報セキュリティ国際評価基準モードにします。Common Criteria 構成は、厳重なセキュリティプロセスを遂行します。デフォルトは ［オン］です。

- 再起動バナーを有効化：ユーザーのデバイスが再起動されたときに、DoD 承認システム使用通知メッセージまたはバナーを表示します。デフォルトは ［オフ］です。
- 設定の変更を許可：ユーザーが完全管理対象デバイスの設定を変更できるようにします。デフォルトは ［オン］です。
- バックグラウンドデータの使用を有効化：アプリがバックグラウンドでデータを同期できるようにします。完全管理対象デバイス向けの設定です。デフォルトは ［オン］です。
- クリップボードを許可：ユーザーがデバイスでデータをクリップボードにコピーできるようにします。
  * クリップボード共有を許可：ユーザーが自分のデバイスとコンピューター間でクリップボードのコンテンツを共有できるようにします（MDM 4.0 以降）。
- ホームキーを許可：ユーザーが完全管理対象デバイスで **Home** キーを使用できるようにします。デフォルトは ［オン］です。
- 疑似ロケーションを許可：ユーザーが GPS の場所を偽装できるようにします。完全に管理されているデバイス用の設定です。デフォルトは ［オフ］です。
- **NFC**：ユーザーが完全に管理されたデバイスで NFC を使用できるようにします（MDM 3.0 以降）。デフォルトは ［オン］です。
- 電源オフを許可：ユーザーが完全管理対象デバイスの電源を切れるようにします（MDM 3.0 以降）。デフォルトは ［オン］です。
- **Wi-Fi** ダイレクトを許可：ユーザーが Wi-Fi 接続を介して、ほかのデバイスに直接接続できるようにします。デフォルトは ［オン］です。［オン］の場合、[**Wi-Fi** の変更を許可］設定を有効にする必要があります。
- **SD** カードを許可：ユーザーが、可能な場合にはデバイスで SD カードを使用できるようにします。デフォルトは ［オン］です。
- **USB** ホストストレージを許可： USB デバイスがユーザーのデバイスに接続されたとき、ユーザーのデバイスが USB ホストとして機能するようにできます。これにより、ユーザーのデバイスが USB デバイスに電源を供給します。デフォルトは ［オン］です。
- 音声ダイヤラーを許可：ユーザーがデバイスで音声ダイヤラーを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **S Beam** を許可：ユーザーが NFC や Wi-Fi Direct を使ってほかのユーザーとコンテンツを共有できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **S Voice** を許可：ユーザーがデバイスでインテリジェントパーソナルアシスタントおよびナレッジナビゲーターを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **USB** テザリングを許可：ユーザーが、USB 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
- **Bluetooth** テザリングを許可：ユーザーが、Bluetooth 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
  * **Bluetooth** 共有を許可：オフになっている場合、ユーザーはデバイスで送信による Bluetooth 共有を確立できません。デフォルトではオンになっています。

- **Wi-Fi** テザリングを許可：ユーザーが、Wi-Fi 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
- 受信 **MMS** を許可：ユーザーが MMS（Microsoft メディアストリーミング）メッセージを受信できるようにします。デフォルトは ［オフ］です。［オン］の場合、［**SMS** を許可］設定をオンにする必要があります。
- 送信 **MMS** を許可：ユーザーが MMS（Microsoft メディアストリーミング）メッセージを送信できるようにします。デフォルトは ［オフ］です。［オン］の場合、［**SMS** を許可］設定をオンにする必要があります。
- 受信 **SMS** を許可：ユーザーが SMS メッセージを受信できるようにします。デフォルトは ［オフ］です。［オン］の場合、［**SMS** を許可］設定をオンにする必要があります。
- 送信 **SMS** を許可：ユーザーが SMS メッセージを送信できるようにします。デフォルトは ［オフ］です。［オン］の場合、［**SMS** を許可］設定をオンにする必要があります。
- モバイルネットワークを構成：ユーザーが携帯データネットワーク接続を使用できるようにします。デフォルトは ［オフ］です。
- 日単位で制限（**MB**）：ユーザーが一日に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 週単位で制限（**MB**）：ユーザーが一週間に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 月単位で制限（**MB**）：ユーザーが 1 か月に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- セキュリティで保護された **VPN** 接続のみを許可：ユーザーがセキュリティで保護された接続のみを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- オーディオ録音を許可：ユーザーがデバイスでオーディオを録音できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。［オン］の場合、［マイクを許可］設定をオンにする必要があります。
- ビデオ録画を許可：ユーザーがデバイスでビデオを録画できるようにします（MDM 4.0 以降）。デフォルトは ［オフ］です。［オン］の場合、［カメラの使用を許可］設定をオンにする必要があります。
- ローミング時のプッシュメッセージを許可：ユーザーが携帯データネットワークを使用してプッシュできるようにします。デフォルトは ［オフ］です。［オン］の場合、［データローミングを許可］設定を有効にする必要があります。
- ローミング時に自動同期を許可：ユーザーが携帯データネットワークを使用して同期できるようにします。デフォルトは ［オフ］です。［オン］の場合、［データローミングを許可］設定を有効にする必要があります。
- ローミング時に音声通話を許可：ユーザーが音声通話に携帯データネットワークを使用できるようにします。デフォルトは ［オフ］です。［オン］の場合、［データローミングを許可］設定を有効にする必要があります。

- **Samsung**：完全管理対象デバイス

  - 失効チェックを有効化：失効した証明書のチェックを有効にします。デフォルトは ［オフ］です。

［仕事用プロファイルで完全に管理されているデバイスに適用 /会社所有のデバイスの仕事用プロファイルに適用］がオンになっていて、［完全に管理されているデバイスが仕事用プロファイルを持つ場合、ポリシーを次のプロファイルに適用］が ［仕事用プロファイル］に設定されている場合、次の設定を構成します：

- セキュリティ
  - アカウント管理を許可：仕事用プロファイルおよび管理対象デバイスでアカウントを追加できるようにします。デフォルトは ［オフ］です。
  - プロファイル間でコピーと貼り付けを許可：［オン］の場合、ユーザーは Android Enterprise プロファイルのアプリと個人的領域のアプリの間でコピーして貼り付けることができます。デフォルトは ［オフ］です。
  - スクリーンショットを許可：ユーザーがデバイス画面のスクリーンショットを取得できるかどうかを指定します。デフォルトは ［オフ］です。
  - カメラの使用を許可：ユーザーがデバイスのカメラで写真やビデオを撮ることができます。デフォルトは ［オフ］です。
  - 位置情報プロバイダーの構成を許可：ユーザーがデバイスで GPS をオンにできるようにします。Android API 28 以降で使用します。デフォルトは ［オン］です。
  - 位置情報の共有を許可：管理対象プロファイルの場合、デバイス所有者は設定を上書きできます。デフォルトは ［オフ］です。

    > ヒント：
    >
    > Citrix Endpoint Management で位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。「位置情報デバイスポリシー」を参照してください。

  - ユーザーにユーザー資格情報の構成を許可：ユーザーが管理対象のキーストアで認証情報を設定できるかどうかを指定します。デフォルトは ［オン］です。
  - 印刷を許可：［オン］にすると、ユーザーデバイスからアクセス可能なプリンターへの印刷が許可されます。デフォルトは ［オフ］です。利用可能：Android 9 以降。
- アプリ
  - システムアプリを有効化：ユーザーが事前インストールされたデバイスアプリを実行できるようにします。デフォルトは［オフ］です。特定のアプリを有効にするには、［システムアプリ一覧］の表で ［追加］をクリックします。
    - システムアプリ一覧：デバイスで有効にするシステムアプリの一覧。［システムアプリを有効化］を ［オン］に設定して、アプリのパッケージ名を追加します。システムアプリのパッケージ名を検索するには、Android Debug Bridge（adb）を使用して Android パッケージマネージャー（pm）コマンドを呼び出します。たとえば `adb shell "pm list packages -f name"`で、ここで「名前」はパッケージ名の一部です。詳しくは、https://developer.android.com/studio/command-line/adbを参照してください。

Android Enterprise デバイスでは、Android Enterprise アプリの権限ポリシーを使用してアプリの権限を制限できます。

- アプリケーションを無効化：指定したアプリの一覧がデバイス上で実行されるのを禁止します。デフォルトは ［オフ］です。インストールされているアプリを無効にするには、設定を ［オン］に変更し、［アプリケーション一覧］表で ［追加］をクリックします。
  - アプリ一覧：禁止するアプリの一覧。［アプリケーションを無効にする］を ［オン］に設定してアプリを追加し、アプリのパッケージ名を入力します。アプリ一覧を変更して展開すると、以前のアプリ一覧が上書きされます。例：com.example1 と com.example2 を無効にしてから、アプリ一覧の内容を com.example1 と com.example3 に変更すると、com.example.2 が有効になります。
- アプリの検証を有効化： OS がアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは ［オン］です。
- **Google Apps** を有効化：ユーザーが Google Mobile Services からデバイスにアプリをダウンロードできるようにします。デフォルトは ［オン］です。
- **Google Play** 非対応アプリを許可： Google Play 以外のストアからアプリをインストールできるようにします。デフォルトは ［オフ］です。
- ユーザーにアプリケーション設定の制御を許可：ユーザーがアプリのアンインストール、アプリの無効化、キャッシュやデータの消去、アプリの強制停止、デフォルト値のクリアをできるようにします。ユーザーは、設定アプリからこれらのアクションを実行します。デフォルトは ［オフ］です。
- アプリのアンインストールを許可：ユーザーが管理対象の Google Play ストア内からアプリをアンインストールできるようにします。デフォルトは ［オフ］です。

- **BYOD**/仕事用プロファイル
  - ホーム画面で仕事用プロファイルアプリウィジェットを許可する：この設定が ［オン］の場合、ユーザーが仕事用プロファイルアプリウィジェットをデバイスのホーム画面に配置できます。この設定が ［オフ］の場合、ユーザーは仕事用プロフィールアプリウィジェットを端末のホーム画面に配置できません。デフォルトは ［オフ］です。
    - ウィジェットが許可されたアプリ：ホーム画面で許可するアプリの一覧。［ホーム画面で仕事用プロファイルアプリのウィジェットを許可］を ［オン］に設定して対象のアプリを追加します。［追加］をクリックし、一覧からホーム画面で許可するアプリを選択します。［保存］をクリックします。この手順を繰り返して、ほかのアプリウィジェットも許可します。
  - デバイスの連絡先で仕事用プロファイルの連絡先を許可：着信時に、管理対象の Android Enterprise プロファイルの連絡先を親プロファイルに表示します（Android 7.0 以降）。デフォルトは［オフ］です。

- **Samsung**
  - **TIMA** キーストアを有効化： TIMA KeyStore は、対称キーの TrustZone ベースのセキュアなキーストレージを提供します。RSA キーペアと証明書は、ストレージのデフォルトのキーストアプロバイダーを経由します。デフォルトは ［オフ］です。

  - 共有一覧を許可：ユーザーが Share Via の一覧にあるアプリ間でコンテンツを共有できるようにします。デフォルトは ［オン］です。
  - 監査ログを有効化：デバイスのフォレンジック解析用イベント監査ログの作成を有効にします。デフォルトは ［オフ］です。

- **Samsung**：完全管理対象デバイス

  - 失効チェックを有効化：失効した証明書のチェックを有効にします。デフォルトは ［オフ］です。

［仕事用プロファイルで完全に管理されているデバイスに適用/会社所有のデバイスの仕事用プロファイルに適用］がオンになっていて、［完全に管理されているデバイスが仕事用プロファイルを持つ場合、ポリシーを次のプロファイルに適用］が ［管理対象デバイス］に設定されている場合、次の設定を構成します：

- セキュリティ

  - アカウント管理を許可：仕事用プロファイルおよび管理対象デバイスでアカウントを追加できるようにします。デフォルトは ［オフ］です。
  - プロファイル間でコピーと貼り付けを許可：［オン］の場合、ユーザーは Android Enterprise プロファイルのアプリと個人的領域のアプリの間でコピーして貼り付けることができます。デフォルトは ［オフ］です。
  - スクリーンショットを許可：ユーザーがデバイス画面のスクリーンショットを取得できるかどうかを指定します。デフォルトは ［オフ］です。
  - カメラの使用を許可：ユーザーがデバイスのカメラで写真やビデオを撮ることができます。デフォルトは ［オフ］です。
  - **VPN** 構成を許可：ユーザーが VPN 構成を作成できるようにします。Android 6 以降を実行する仕事用プロファイルデバイスおよび完全に管理されているデバイス向けです。デフォルトは ［オン］です。
  - バックアップサービスを許可：ユーザーがデバイス上にアプリケーションやシステムデータをバックアップできるようにします。デフォルトは ［オン］です。
  - **NFC** を許可：近距離無線通信（NFC：Near Field Communication）を使用して、ユーザーが手元のデバイスから他のデバイスに Web ページ、写真、ビデオなどのコンテンツを送信できるようにします。MDM 4.0 以降。デフォルトは ［オン］です。
  - 位置情報プロバイダーの構成を許可：ユーザーがデバイスで GPS をオンにできるようにします。Android API 28 以降で使用します。デフォルトは ［オン］です。
  - 位置情報の共有を許可：管理対象プロファイルの場合、デバイス所有者は設定を上書きできます。デフォルトは ［オフ］です。

    > ヒント：
    >
    > Citrix Endpoint Management で位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。「位置情報デバイスポリシー」を参照してください。

- ユーザーにユーザー資格情報の構成を許可：ユーザーが管理対象のキーストアで認証情報を設定できるかどうかを指定します。デフォルトは ［オン］です。
- 印刷を許可：［オン］にすると、ユーザーデバイスからアクセス可能なプリンターへの印刷が許可されます。デフォルトは ［オフ］です。利用可能：Android 9 以降。
- **USB** デバッグを許可：デフォルトは ［オフ］です。

- アプリ
  - システムアプリを有効化：ユーザーが事前インストールされたデバイスアプリを実行できるようにします。デフォルトは［オフ］です。特定のアプリを有効にするには、［システムアプリ一覧］の表で ［追加］をクリックします。
    * システムアプリ一覧：デバイスで有効にするシステムアプリの一覧。［システムアプリを有効化］を ［オン］に設定して、アプリのパッケージ名を追加します。システムアプリのパッケージ名を検索するには、Android Debug Bridge（adb）を使用して Android パッケージマネージャー（pm）コマンドを呼び出します。たとえば `adb shell "pm list packages -f name"`で、ここで「名前」はパッケージ名の一部です。詳しくは、https://developer.android.com/studio/command-line/adbを参照してください。Android Enterprise デバイスでは、Android Enterprise アプリの権限ポリシーを使用してアプリの権限を制限できます。
  - アプリケーションを無効化：指定したアプリの一覧がデバイス上で実行されるのを禁止します。デフォルトは ［オフ］です。インストールされているアプリを無効にするには、設定を ［オン］に変更し、［アプリケーション一覧］表で ［追加］をクリックします。
    * アプリ一覧：禁止するアプリの一覧。［アプリケーションを無効にする］を ［オン］に設定してアプリを追加し、アプリのパッケージ名を入力します。アプリ一覧を変更して展開すると、以前のアプリ一覧が上書きされます。例：com.example1 と com.example2 を無効にしてから、アプリ一覧の内容を com.example1 と com.example3 に変更すると、com.example.2 が有効になります。
  - アプリの検証を有効化： OS がアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは ［オン］です。
  - **Google Apps** を有効化：ユーザーが Google Mobile Services からデバイスにアプリをダウンロードできるようにします。デフォルトは ［オン］です。
  - **Google Play** 非対応アプリを許可： Google Play 以外のストアからアプリをインストールできるようにします。デフォルトは ［オフ］です。
  - ユーザーにアプリケーション設定の制御を許可：ユーザーがアプリのアンインストール、アプリの無効化、キャッシュやデータの消去、アプリの強制停止、デフォルト値のクリアをできるようにします。ユーザーは、設定アプリからこれらのアクションを実行します。デフォルトは ［オフ］です。
  - アプリのアンインストールを許可：ユーザーが管理対象の Google Play ストア内からアプリをアンインストールできるようにします。デフォルトは ［オフ］です。

- 完全管理対象デバイスのみ

- ユーザーの追加を許可：ユーザーがデバイスに新しいユーザーを追加できるようにします。デフォルトは ［オン］です。
- データローミングを許可：ユーザーがローミング中に携帯データネットワークを使用できるようにします。デフォルトは［オフ］で、ユーザーのデバイスでローミングが無効になっています。デフォルトは［オフ］です。
- **SMS** を許可：ユーザーが SMS メッセージを送受信できるようにします。デフォルトは ［オフ］です。
- ステータスバーの使用を許可：［オン］に設定すると、管理対象デバイスおよび専用デバイス（COSU デバイス）上でステータスバーが有効になります。この設定により、通知、クイック設定、その他の画面オーバーレイで全画面モードから移動することができなくなります。ユーザーはシステム設定に移動して通知を表示できます。Android 6.0 以降の場合、デフォルトは ［オフ］です。
- **Bluetooth** を許可：ユーザーが Bluetooth を使用できるようにします。デフォルトは ［オン］です。
  - **Bluetooth** 共有を許可：オフになっている場合、ユーザーはデバイスで送信による Bluetooth 共有を確立できません。デフォルトではオンになっています。
- 日付と時刻の構成を許可：ユーザーがデバイスの日付と時刻を変更できるようにします。デフォルトは［オン］です。
- 工場出荷時リセットを許可：ユーザーがデバイスを出荷時の設定に戻すことができるようにします。デフォルトは ［オン］です。
- 工場出荷時のリセット保護を許可：［オン］に設定されている場合、デバイスがリカバリモードでリセットされると、ユーザーはリセット前のデバイスのアカウント資格情報を入力する必要があります。リセット前にデバイスロックを設定した場合は、デバイスロックを設定することもできます。［オフ］に設定されている場合、リセット後に認証は必要ありません。デフォルトは ［オン］です。
- デバイス画面を有効なまま維持する：この設定を ［オン］に設定すると、デバイスを接続してもデバイス画面はオンのままです。デフォルトは ［オフ］です。
- **USB** 大容量ストレージを許可： USB 接続上で、ユーザーのデバイスとコンピューター間で大容量のデータファイルを転送できるようにします。デフォルトは ［オン］です。
- マイクを許可：ユーザーがデバイスでマイクを使用できるようにします。デフォルトは ［オン］です。
- テザリングを許可：ユーザーがポータブルホットスポットとテザリングデータを構成できるようにします。デフォルトは ［オフ］です。この設定をオンにすると、Samsung デバイスで以下の設定を使用できます：
- **Keyguard** がデバイスをロックしないようにする：［オン］の場合、この設定により管理対象デバイスおよび専用デバイス（COSU デバイス）のロック画面で Keyguard が無効になります。デフォルトは［オフ］です。
- **Wi-Fi** の変更を許可：［オン］場合、ユーザーは Wi-Fi をオンまたはオフにして、Wi-Fi ネットワークに接続できます。デフォルトは ［オン］です。
- ファイル転送を許可： USB 上でファイル転送できるようにします。デフォルトは ［オフ］です。

- **Samsung**

  - **TIMA** キーストアを有効化： TIMA KeyStore は、対称キーの TrustZone ベースのセキュアなキーストレージを提供します。RSA キーペアと証明書は、ストレージのデフォルトのキーストアプロバイダー

を経由します。デフォルトは ［オフ］です。
- 共有一覧を許可：ユーザーが Share Via の一覧にあるアプリ間でコンテンツを共有できるようにします。デフォルトは ［オン］です。
- 監査ログを有効化：デバイスのフォレンジック解析用イベント監査ログの作成を有効にします。デフォルトは ［オフ］です。

- **Samsung**：完全管理対象デバイスのみ
  - **ODE** 信頼済み起動検証を有効化： ODE 信頼済みブート検証を使って、ブートローダーからシステムイメージへの信頼のチェーンを確立します。デフォルトは ［オン］です。
  - 緊急電話のみを許可：ユーザーがデバイスで緊急電話のみモードを有効にできるようにします。デフォルトは ［オフ］です。
  - ファームウェアリカバリを許可：ユーザーがデバイスでファームウェアを復元できるようにします。デフォルトは ［オン］です。
  - 高速暗号化を許可：使用済みのメモリ領域のみ暗号化を許可します。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは対照的な方法です。このデータには設定、アプリケーションデータ、ダウンロードしたファイルおよびアプリケーション、メディア、およびその他のファイルが含まれます。デフォルトは ［オン］です。
  - 情報セキュリティ国際評価基準（**Common Criteria**）モードを有効化：デバイスを情報セキュリティ国際評価基準モードにします。Common Criteria 構成は、厳重なセキュリティプロセスを遂行します。デフォルトは ［オン］です。
  - 再起動バナーを有効化：ユーザーのデバイスが再起動されたときに、DoD 承認システム使用通知メッセージまたはバナーを表示します。デフォルトは ［オフ］です。
  - 設定の変更を許可：ユーザーが完全管理対象デバイスの設定を変更できるようにします。デフォルトは ［オン］です。
  - バックグラウンドデータの使用を有効化：アプリがバックグラウンドでデータを同期できるようにします。完全管理対象デバイス向けの設定です。デフォルトは ［オン］です。
  - クリップボードを許可：ユーザーがデバイスでデータをクリップボードにコピーできるようにします。デフォルトは ［オン］です。
    * クリップボード共有を許可：ユーザーが自分のデバイスとコンピューター間でクリップボードのコンテンツを共有できるようにします（MDM 4.0 以降）。
  - ホームキーを許可：ユーザーが完全管理対象デバイスで **Home** キーを使用できるようにします。デフォルトは ［オン］です。
  - 疑似ロケーションを許可：ユーザーが GPS の場所を偽装できるようにします。完全に管理されているデバイス用の設定です。デフォルトは ［オフ］です。
  - **NFC**：ユーザーが完全に管理されたデバイスで NFC を使用できるようにします（MDM 3.0 以降）。デフォルトは ［オン］です。
  - 電源オフを許可：ユーザーが完全管理対象デバイスの電源を切れるようにします（MDM 3.0 以降）。デフォルトは ［オン］です。
  - **Wi-Fi** ダイレクトを許可：ユーザーが Wi-Fi 接続を介して、ほかのデバイスに直接接続できるようにし

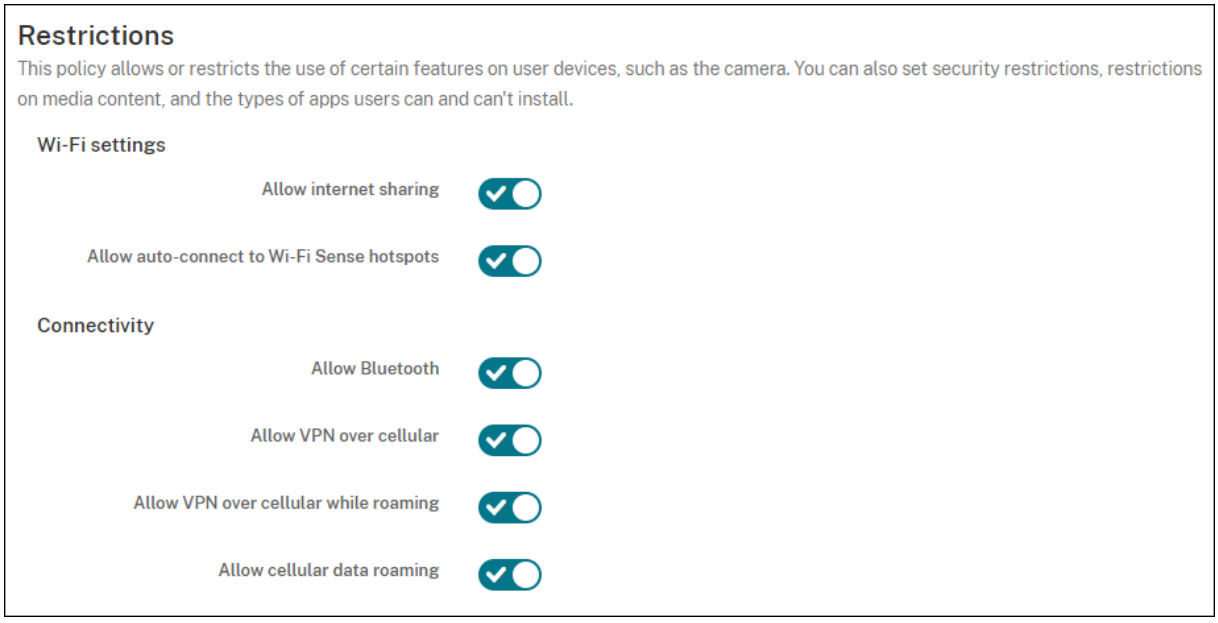
ます。デフォルトは ［オン］です。［オン］の場合、[**Wi-Fi** の変更を許可］設定を有効にする必要があります。

- **SD** カードを許可：ユーザーが、可能な場合にはデバイスで SD カードを使用できるようにします。デフォルトは ［オン］です。
- **USB** ホストストレージを許可： USB デバイスがユーザーのデバイスに接続されたとき、ユーザーのデバイスが USB ホストとして機能するようにできます。これにより、ユーザーのデバイスが USB デバイスに電源を供給します。デフォルトは ［オン］です。
- 音声ダイヤラーを許可：ユーザーがデバイスで音声ダイヤラーを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **S Beam** を許可：ユーザーが NFC や Wi-Fi Direct を使ってほかのユーザーとコンテンツを共有できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **S Voice** を許可：ユーザーがデバイスでインテリジェントパーソナルアシスタントおよびナレッジナビゲーターを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］です。
- **USB** テザリングを許可：ユーザーが、USB 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
- **Bluetooth** テザリングを許可：ユーザーが、Bluetooth 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
- **Wi-Fi** テザリングを許可：ユーザーが、Wi-Fi 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。デフォルトは ［オフ］です。［オン］の場合、［テザリングを許可］設定も ［オン］にする必要があります。
- 受信 **MMS** を許可：ユーザーが MMS（Microsoft メディアストリーミング）メッセージを受信できるようにします。デフォルトは ［オフ］です。［オン］の場合、[**SMS** を許可］設定をオンにする必要があります。
- 送信 **MMS** を許可：ユーザーが MMS（Microsoft メディアストリーミング）メッセージを送信できるようにします。デフォルトは ［オフ］です。［オン］の場合、[**SMS** を許可］設定をオンにする必要があります。
- 受信 **SMS** を許可：ユーザーが SMS メッセージを受信できるようにします。デフォルトは ［オフ］です。［オン］の場合、[**SMS** を許可］設定をオンにする必要があります。
- 送信 **SMS** を許可：ユーザーが SMS メッセージを送信できるようにします。デフォルトは ［オフ］です。［オン］の場合、[**SMS** を許可］設定をオンにする必要があります。
- モバイルネットワークを構成：ユーザーが携帯データネットワーク接続を使用できるようにします。デフォルトは ［オフ］です。
- 日単位で制限（**MB**）：ユーザーが一日に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 週単位で制限（**MB**）：ユーザーが一週間に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 月単位で制限（**MB**）：ユーザーが 1 か月に使用できるモバイルデータの MB 数を入力します。デフォル

トは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- セキュリティで保護された **VPN** 接続のみを許可：ユーザーがセキュリティで保護された接続のみを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
- オーディオ録音を許可：ユーザーがデバイスでオーディオを録音できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。［オン］ の場合、［マイクを許可］ 設定をオンにする必要があります。
- ビデオ録画を許可：ユーザーがデバイスでビデオを録画できるようにします（MDM 4.0 以降）。デフォルトは ［オフ］ です。［オン］ の場合、［カメラの使用を許可］ 設定をオンにする必要があります。
- ローミング時のプッシュメッセージを許可：ユーザーが携帯データネットワークを使用してプッシュできるようにします。デフォルトは ［オフ］ です。［オン］ の場合、［データローミングを許可］ 設定を有効にする必要があります。
- ローミング時に自動同期を許可：ユーザーが携帯データネットワークを使用して同期できるようにします。デフォルトは ［オフ］ です。［オン］ の場合、［データローミングを許可］ 設定を有効にする必要があります。
- ローミング時に音声通話を許可：ユーザーが音声通話に携帯データネットワークを使用できるようにします。デフォルトは ［オフ］ です。［オン］ の場合、［データローミングを許可］ 設定を有効にする必要があります。

- **Samsung**：完全管理対象デバイス
  - 失効チェックを有効化：失効した証明書のチェックを有効にします。デフォルトは ［オフ］ です。

Windows デスクトップ/タブレットの設定



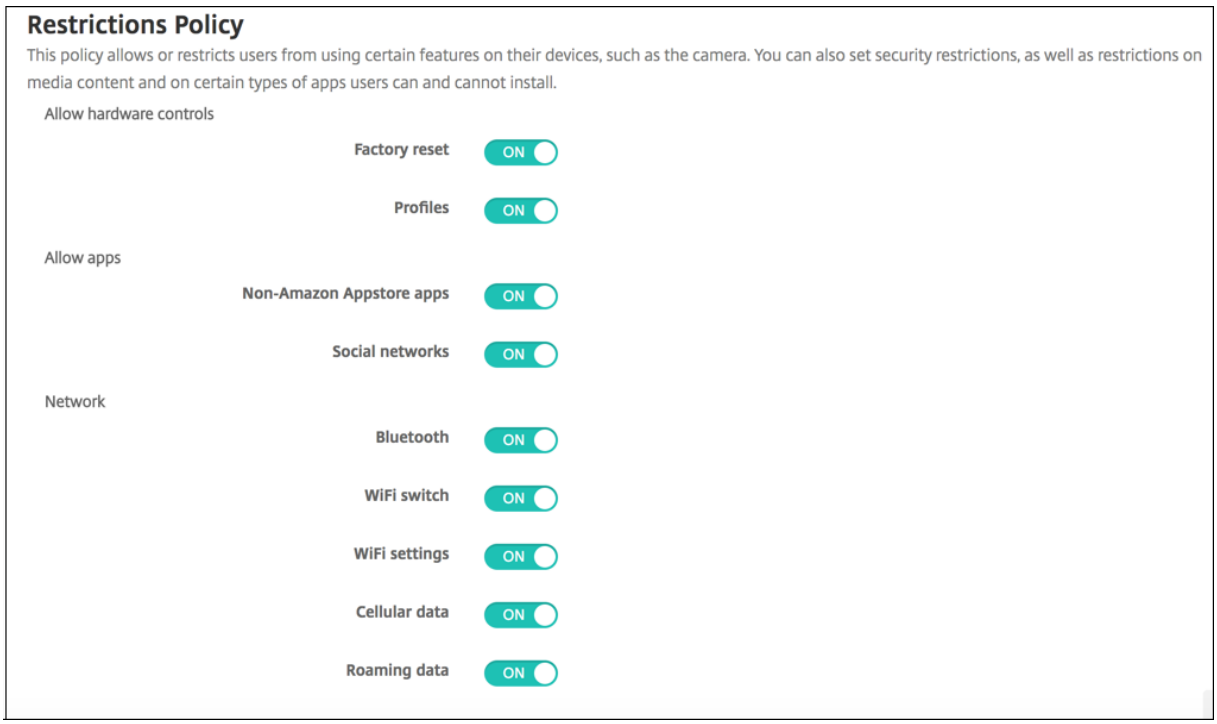
- **Wi-Fi** 設定

  - インターネット共有を許可： Wi-Fi ホットスポットに切り替えてデバイスがインターネット接続をほかのデバイスと共有できるようにします。

- 接続
  - **Bluetooth** を許可：デバイスが Bluetooth を介して接続できるようにします。
  - 携帯ネットワーク経由の **VPN** を許可：デバイスが VPN 上で携帯ネットワークと接続できるようにします。
  - ローミング時の携帯ネットワーク経由の **VPN** を許可：デバイスが携帯ネットワーク上をローミングしたら、デバイスが VPN 上で接続できるようにします。
  - 携帯ネットワークデータのローミングを許可：ローミングの間にユーザーが携帯データネットワークを使えるようにします。
- アカウント
  - **Microsoft** アカウントの接続を許可：デバイスが、非メール関連の接続認証とサービスに Microsoft アカウントを使用できるようにします。
  - **Microsoft** 以外のメールを許可：ユーザーが Microsoft 以外のメールアカウントを追加できるようにします。
- システム
  - ストレージカードを許可：デバイスでストレージカードの使用を許可します。
  - テレメトリ：一覧で、デバイスによる利用統計情報の送信を許可または制限するオプションをクリックします。デフォルトは ［許可］です。そのほかのオプションには、［許可しない］および ［許可（セカンダリデータ要求を除く）］があります。
  - 位置情報サービスへのアプリアクセスを許可する：位置情報サービスへのアプリアクセスを許可します。
  - 内部ビルドのプレビューを許可：ユーザーが Microsoft 内部ビルドをプレビューできるようにします。
- カメラ： Windows デスクトップ/タブレットのみ
  - カメラの使用を許可：ユーザーがデバイスのカメラを使用できるようにします。
- **Bluetooth**： Windows デスクトップ/タブレットのみ
  - 検出可能モードを許可： Bluetooth デバイスがローカルデバイスを検出できるようにします。
  - ローカルデバイス名：ローカルデバイスの名前。
- 操作性： Windows デスクトップ/タブレットのみ
  - **Cortana** を許可：ユーザーが Cortana のインテリジェントパーソナルアシスタントおよびナレッジナビゲーターにアクセスできるようにします。
  - デバイスの検出を許可：デバイスのネットワーク検出を有効にします。
  - 手動の **MDM** 登録解除を許可：ユーザーが Citrix Endpoint Management MDM から手動でデバイスの登録を解除できるようにします。
  - デバイス設定の同期を許可：ユーザーがローミング時に Windows 10 および Windows 11 デバイス間で設定を同期できるようにします。

- ロック例外： Windows デスクトップ/タブレットのみ
  - ロック画面でトースト通知を許可：ロック画面でトースト通知を許可します。Windows デスクトップ/タブレットのみ
- アプリ
  - **Appstore** の自動更新を許可：アプリストアによるアプリの自動更新を許可します。Windows デスクトップ/タブレットのみ。
- プライバシー： Windows デスクトップ/タブレットのみ
  - 入力の個人設定を許可：入力の個人設定サービスの実行を許可します。ペンやタッチキーボードなどでユーザーが入力した内容をベースに、予測変換の精度を向上します。
- 設定： Windows デスクトップ/タブレットのみ。
  - 自動再生を許可：ユーザーが自動再生設定を変更できるようにします。
  - データセンターを許可：ユーザーがデータセンサー設定を変更できるようにします。
  - 日付**/**時刻を許可：ユーザーが日付/時刻設定を変更できるようにします。
  - 言語を許可：ユーザーが言語設定を変更できるようにします。
  - 電源スリープを許可：ユーザーが電源設定およびスリープ設定を変更できるようにします。
  - リージョンを許可：ユーザーがリージョン設定を変更できるようにします。
  - サインインオプションを許可：ユーザーがサインイン設定を変更できるようにします。
  - ワークプレースを許可：ユーザーがワークプレース設定を変更できるようにします。
  - アカウントを許可：ユーザーがアカウント設定を変更できるようにします。

Amazon の設定



- ハードウェアの制御を許可
  - 工場出荷時リセット：ユーザーがデバイスを出荷時の設定に戻すことができるようにします。
  - プロファイル：ユーザーがデバイスでハードウェアプロファイルを変更できるようにします。
- アプリを許可
  - **Amazon** アプリストア非対応アプリを許可：ユーザーが Amazon アプリストアに対応していないアプリをデバイスにインストールできるようにします。
  - ソーシャルネットワーク：ユーザーがデバイスからソーシャルネットワークにアクセスできるようにします。
- ネットワーク
  - **Bluetooth**：ユーザーが Bluetooth を使用できるようにします。
  - **Wi-Fi** スイッチ：アプリで Wi-Fi 接続の状態を変更できるようにします。
  - **Wi-Fi** 設定：ユーザーが Wi-Fi 設定を変更できるようにします。
  - モバイルネットワークを構成：ユーザーが携帯データネットワーク接続を使用できるようにします。
  - ローミングデータ：ローミングの間にユーザーが携帯データネットワークを使えるようにします。
  - 位置情報サービス：ユーザーが GPS を使用できるようにします。
- **USB** 操作：
  - デバッグ：デバッグのためユーザーのデバイスが USB を介してコンピューターに接続できるようにします。

ローミングデバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、サポート対象の iOS デバイスで音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 音声ローミングを無効化：音声通話ローミングを無効にするかどうかを選択します。このオプションを有効にした場合、データローミングは自動的に無効になります。デフォルトは ［オフ］で、音声通話ローミングを許可します。
- データローミングを無効化：データローミングを無効にするかどうかを選択します。このオプションは、音声通話ローミングが有効になっている場合にのみ使用できます。デフォルトは ［オフ］で、データローミングを許可します。

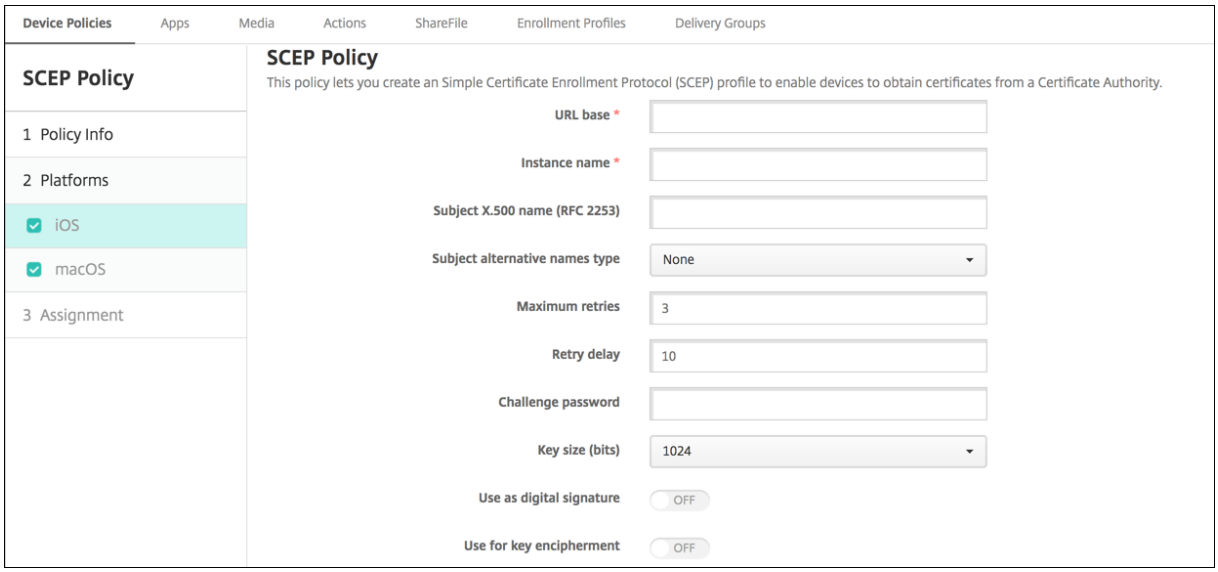
SCEP デバイスポリシー

November 29, 2023

このポリシーで iOS デバイスと macOS デバイスを構成し、SCEP（Simple Certificate Enrollment Protocol）を使用して外部 SCEP サーバーから証明書を取得することができます。Citrix Endpoint Management に接続されている PKI から SCEP を使用してデバイスに証明書を配布する場合は、PKI エンティティと PKI プロバイダーを分散モードで作成します。詳しくは、「PKI エンティティ」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

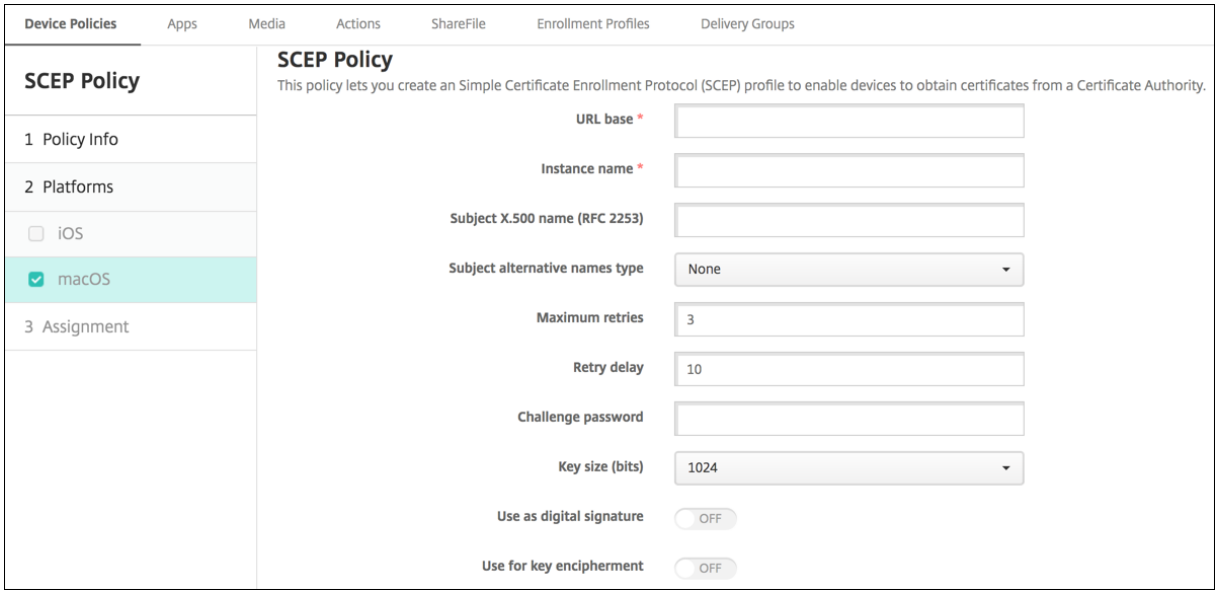


- **URL** ベース： HTTP または HTTPS を介した SCEP 要求の送信先を定義する SCEP サーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ワンタイムパスワードが再利用されるように構成している場合は、HTTPS を使用してパスワードを保護します。これは必須の手順です。
- インスタンス名： SCEP サーバーで認識される文字列を入力します。たとえば、example.org のようなドメイン名です。CA に複数の CA 証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **X.500** サブジェクト名（**RFC 2253**）：オブジェクト識別子（OID）と値の配列として X.500 の名前の表現を入力します。たとえば「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」と入力します。これは、「[[[“C” , “US”]], [[“O” , “Apple Inc.”]], …, [[“1.2.5.3” , “bar”]]]」に変換されます。OID はドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
- サブジェクトの別名の種類：代替名の種類を選択します。オプションの代替名の種類で、CA が証明書を発行するために必要な値を指定できます。［なし］、［**RFC 822** 名］、［**DNS** 名］、［**URI**］のいずれかを指定できます。
- 最大再試行回数： SCEP サーバーが PENDING 応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは **3** です。
- 再試行の延期：次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは **10** です。
- チャレンジパスワード：事前共有シークレットを入力します。
- キーサイズ（ビット）： **2048** 以上のキーサイズ（ビット）を選択します。
- デジタル署名として使用：デジタル署名として証明書を使用するかどうかを指定します。SCEP サーバーは、

公開キーを使用してハッシュを暗号化解除する前に、証明書がデジタル署名として使用されていることを確認します。

- キーの暗号化に使用：キーの暗号化に証明書を使用するかどうかを選択します。サーバーはまず、クライアントから提供された証明書がキーの暗号化で許可されているかどうかをチェックします。次に、サーバーは証明書内の公開キーを使用して、データが秘密キーを使用して暗号化されていることを確認します。できない場合は、操作に失敗します。
- **SHA-256** フィンガープリント（**16** 進数の文字列）： CA で HTTP が使われている場合、このフィールドを使って、CA 証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CA の応答の信頼性を確認するためにデバイスで使われます。SHA-256 フィンガープリントを提供することも、署名をインポートする証明書を選択することもできます。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

macOS 設定



- **URL** ベース： HTTP または HTTPS を介した SCEP 要求の送信先を定義する SCEP サーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ワンタイムパスワードが再利用されるように構成している場合は、HTTPS を使用してパスワードを保護します。これは必須の手順です。

- インスタンス名： SCEP サーバーで認識される文字列を入力します。たとえば、example.org のようなドメイン名です。CA に複数の CA 証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **X.500** サブジェクト名（**RFC 2253**）：オブジェクト識別子（OID）と値の配列として X.500 の名前の表現を入力します。たとえば「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」と入力します。これは、「[[[“C” , “US”]], [[“O” , “Apple Inc.”]], …, [[“1.2.5.3” , “bar”]]]」に変換されます。OID はドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
- サブジェクトの別名の種類：代替名の種類を選択します。オプションの代替名の種類で、CA が証明書を発行するために必要な値を指定できます。［なし］、［**RFC 822** 名］、［**DNS** 名］、［**URI**］のいずれかを指定できます。
- 最大再試行回数： SCEP サーバーが PENDING 応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは **3** です。
- 再試行の延期：次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは **10** です。
- チャレンジパスワード：事前共有シークレットを入力します。
- キーサイズ（ビット）： **2048** 以上のキーサイズ（ビット）を選択します。
- デジタル署名として使用：デジタル署名として証明書を使用するかどうかを指定します。SCEP サーバーは、公開キーを使用してハッシュを暗号化解除する前に、証明書がデジタル署名として使用されていることを確認します。
- キーの暗号化に使用：キーの暗号化に証明書を使用するかどうかを選択します。サーバーはまず、クライアントから提供された証明書がキーの暗号化で許可されているかどうかをチェックします。次に、サーバーは証明書内の公開キーを使用して、データが秘密キーを使用して暗号化されていることを確認します。できない場合は、操作に失敗します。
- **SHA-256** フィンガープリント（**16** 進数の文字列）： CA で HTTP が使われている場合、このフィールドを使って、CA 証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CA の応答の信頼性を確認するためにデバイスで使われます。SHA-256 フィンガープリントを提供することも、署名をインポートする証明書を選択することもできます。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します

- プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

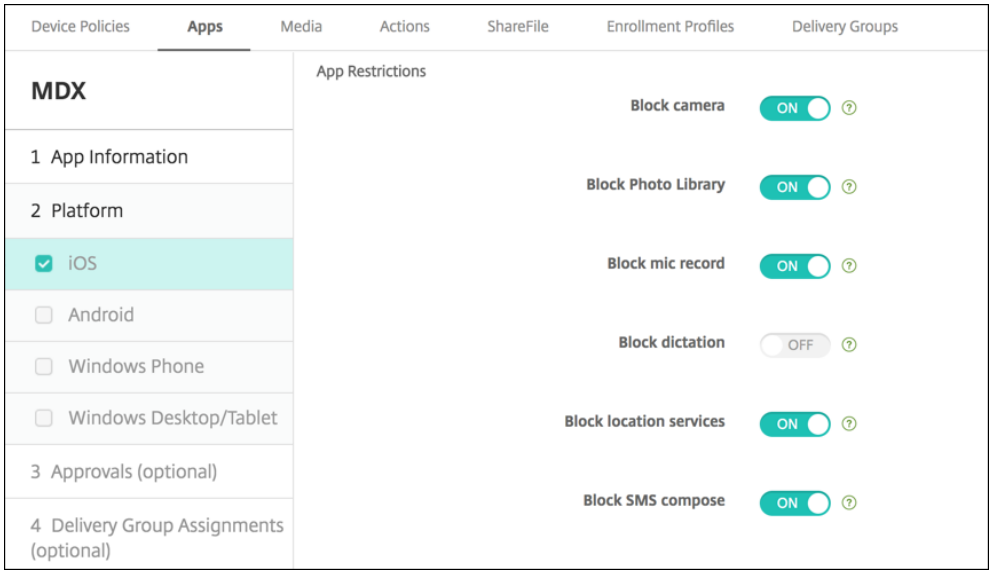
Siri とディクテーションのポリシー

November 29, 2023

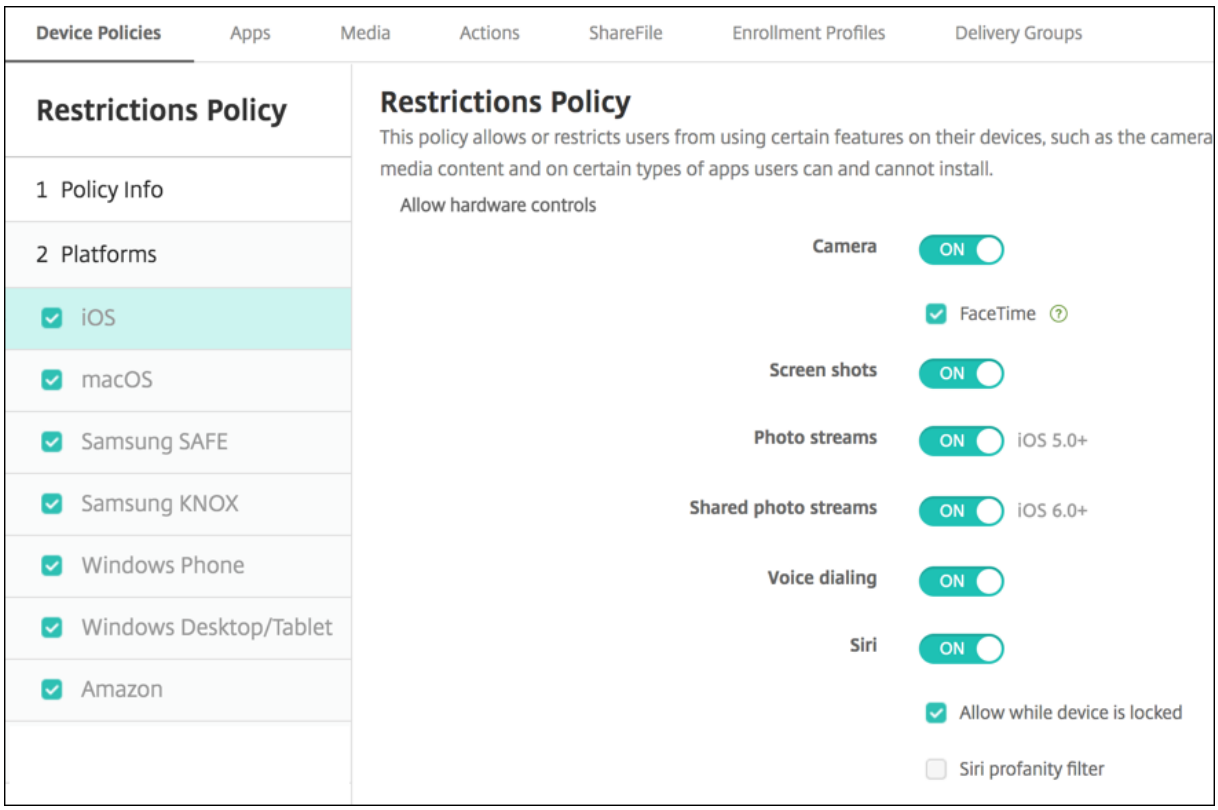
管理された iOS デバイス上でユーザーが Siri に何かを求めるか、テキストを口述する場合、Apple は Siri の改善のために音声データを収集します。音声データは Apple のクラウドベースのサービスを通過し、したがって、セキュアな Citrix Endpoint Management コンテナの外側に存在します。ただし、ディクテーションの結果として生じたテキストは、コンテナ内に残ります。

Citrix Endpoint Management では、セキュリティのニーズの要件に応じて、Siri およびディクテーションサービスをブロックできます。

MAM 展開では、各アプリのディクテーションを禁止ポリシーはデフォルトで ［オン］であり、デバイスのマイクは無効になります。ディクテーションを許可する場合、［オフ］に設定します。Citrix Endpoint Management コンソールの ［構成］**>**［アプリ］で、ポリシーを検出できます。アプリを選択し、［編集］をクリックしてから ［**iOS**］をクリックします。



MDM 展開では、［構成］**>**［デバイスポリシー］で、Siri ポリシーとともに Siri を無効にすることもできます。Siri の使用は、デフォルトで許可されています。



Siri およびディクテーションを許可するかどうか決定するときの留意事項:

- Apple が公開した情報によると、Apple は Siri およびディクテーション音声クリップデータを最大で 2 年間保持します。データにはユーザーを表す乱数が割り当てられ、音声ファイルはこの乱数に関連付けられます。
- iOS デバイスで ［設定］ > ［一般］ > ［キーボード］ と移動して、［音声入力］ の下のリンクをタップすると、Apple のプライバシーポリシーを確認できます。

SSO アカウントデバイスポリシー

November 29, 2023

SSO アカウントデバイスポリシーでは、Citrix Endpoint Management でのシングルサインオン（SSO）アカウントを作成できます。これらのアカウントを作成することにより、ユーザーが 1 回サインオンするだけで、さまざまなアプリから Citrix Endpoint Management および社内リソースにアクセスできるようになります。デバイスに資格情報を保存する必要はありません。SSO アカウントエンタープライズユーザーの資格情報は、App Store からのアプリを含む複数のアプリで使用されます。このポリシーは、Kerberos 認証バックエンドで動作するように設計されています。

このポリシーを追加または構成するには、［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウント名：ユーザーのデバイスで表示される Kerberos SSO アカウント名を入力します。このフィールドは必須です。
- **Kerberos** プリンシパル名： Kerberos プリンシパル名を入力します。このフィールドは必須です。
- **ID** 資格情報（キーストアまたは **PKI** 資格情報）：一覧から、オプションとして、ID 資格情報を選択します。これを使用して、Kerberos 資格情報をユーザー操作なしで更新できます。
- **Kerberos** 領域：このポリシーの Kerberos レルムを入力します。これは通常、ドメイン名をすべて大文字にしたものです（例：EXAMPLE.COM）。このフィールドは必須です。
- 許可されている **URL**：シングルサインオンを要求する URL ごとに、［追加］をクリックして以下の操作を行います。
  - 許可されている **URL**：ユーザーが iOS デバイスからアクセスしたときに SSO を要求する URL を入力します。

    たとえば、ユーザーがサイトを参照しようとし、Web サイトが Kerberos チャレンジを開始した場合、そのサイトが URL 一覧にないと、iOS デバイスでは、前の Kerberos ログオンでデバイスにキャッシュされた可能性がある Kerberos トークンを提供した SSO は試行されません。URL は、ホスト部分が正確に一致する必要があります。たとえば、`https://shopping.apple.com`は有効ですが、`https://*.apple.com`は有効ではありません。

    また、Kerberos がホストの一致に基づいてアクティブ化されない場合でも、URL は標準の HTTP 呼び出しにフォールバックします。これは、URL に Kerberos を使用する SSO だけが構成されている場合であっても、標準パスワードチャレンジや HTTP エラーなどを含むほとんどすべてのことを意味する可能性があります。
  - ［追加］をクリックして URL を追加するか、［キャンセル］をクリックして URL の追加を取り消します。
- アプリ識別子：このログインを許可するアプリごとに、［追加］をクリックして以下の操作を行います。
  - アプリ識別子：このログインを使用できるアプリのアプリ ID を入力します。アプリ ID を追加しなかった場合、このログインはすべてのアプリ ID に一致します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

ストアデバイスポリシー

November 29, 2023

Citrix Endpoint Management でポリシーを作成して、デバイスのホーム画面でアプリストアの Web クリップを表示するかどうかを指定できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS、**Android**、**Windows** デスクトップ/タブレットの設定

構成するプラットフォームごとに、ユーザーデバイスにアプリストア Web クリップを表示するかどうかを選択します。デフォルトは ［オン］です。

サブスクライブされたカレンダーデバイスポリシー

November 29, 2023

Citrix Endpoint Management でデバイスポリシーを追加して、サブスクライブされたカレンダーを iOS デバイスのカレンダー一覧に追加することができます。サブスクライブできる公開カレンダーの一覧は、Apple サポートサイトのダウンロードにあります。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提条件

デバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みである必要があります。

iOS の設定

- 説明：カレンダーの説明を入力します。このフィールドは必須です。
- **URL**：カレンダーの URL を入力します。iCalendar ファイル（.ics）への`webcal://`URL または`https://`リンクを入力できます。このフィールドは必須です。
- ユーザー名：ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード：任意で、ユーザーのパスワードを入力します。
- **SSL** を使用：カレンダーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オフ］です。
- ポリシー設定

- ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
  - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
  - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

契約条件デバイスポリシー

November 29, 2023

社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、Citrix Endpoint Management で契約条件デバイスポリシーを作成します。ユーザーが Citrix Endpoint Management にデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。

社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。Android デバイスおよび iOS デバイスの場合は、PDF ファイルを提供する必要があります。Windows デバイスの場合は、テキスト（TXT）ファイルと付属のイメージファイルを提供する必要があります。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **Android** の設定

- インポートするファイル：［参照］をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。
- デフォルトの契約条件：このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは ［オフ］です。

> 注：
>
> iOS デバイスがデバイス登録プログラム（DEP）を通じて登録されている場合、使用条件は表示されません。

Windows タブレットの設定

- インポートするファイル：［参照］をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。

- イメージ:［参照］をクリックしてインポートするイメージファイルの場所へ移動し、そのファイルを選択します。
- デフォルトの契約条件:このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは ［オフ］です。

トンネルデバイスポリシー

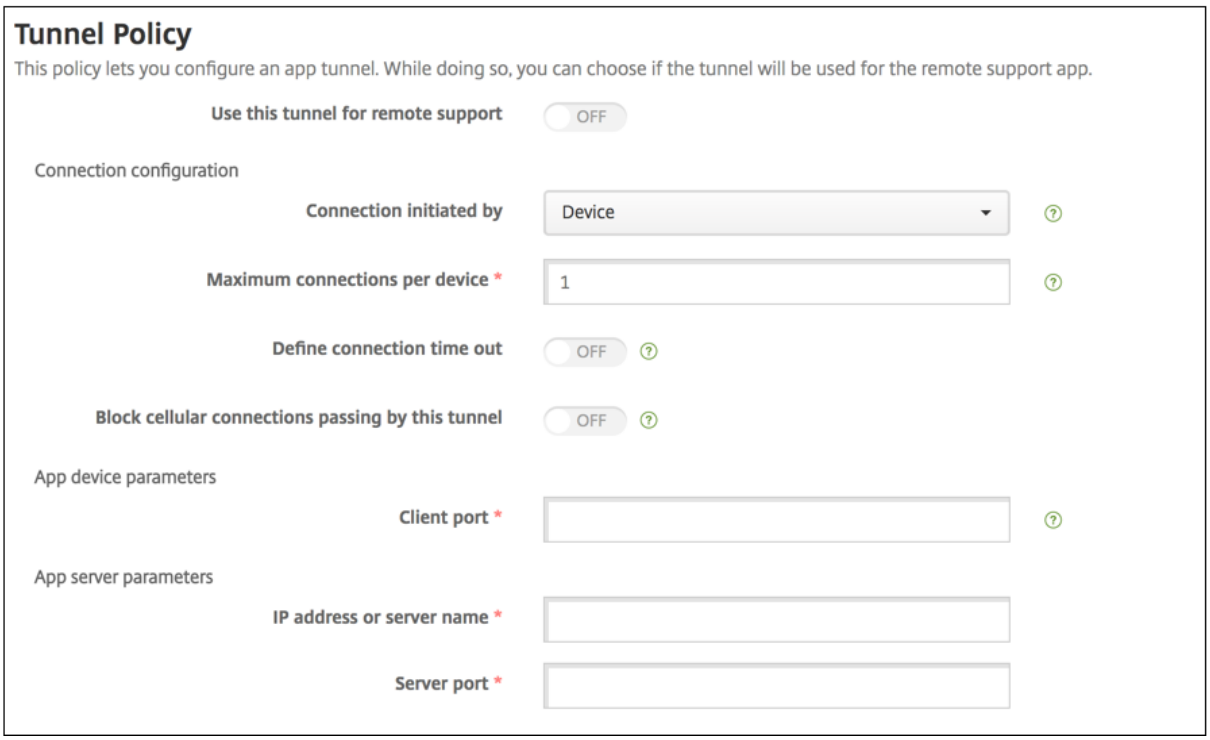
November 29, 2023

アプリトンネルは、モバイルアプリのサービスの継続性およびデータ転送の信頼性を向上させるように設計されています。アプリトンネルは、モバイルデバイスアプリのクライアントコンポーネントとアプリサーバーコンポーネント間のプロキシパラメーターを定義します。トンネルポリシーは、Android デバイスに対して構成できます。

このポリシーで定義したトンネルを使用して送信されるアプリトラフィックは、Citrix Endpoint Management を経由してから、アプリを実行するサーバーにリダイレクトされます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android の設定



- 接続を開始する側:［デバイス］または ［サーバー］を選択して、接続の開始元を指定します。

- デバイスごとの最大接続数：数値を入力して、アプリケーションが確立できる同時 TCP 接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
- 接続のタイムアウトを定義：アプリのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
  - 接続タイムアウト：［接続のタイムアウトを定義］を ［オン］に設定した場合に、アプリのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
- このトンネルを通過する携帯ネットワーク接続をブロック：ローミング中にこのトンネルをブロックするかどうか選択します。WiFi と USB 接続はブロックされません。
- クライアントポート：クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
- **IP** アドレスまたはサーバー名：アプリサーバーの IP アドレスまたは名前を入力します。このフィールドはデバイスで開始する接続にのみ適用されます。
- サーバーポート：サーバーのポート番号を入力します。

VPN デバイスポリシー

March 15, 2024

VPN デバイスポリシーでは、VPN（Virtual Private Network：仮想プライベートネットワーク）の設定を構成し、ユーザーデバイスが社内リソースに安全に接続できるようにすることができます。次のプラットフォームで VPN デバイスポリシーを構成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、この記事で説明しています。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Per-App VPN の要件

VPN ポリシーを使用して、次のプラットフォームの Per-App VPN 機能を構成します。

- iOS
- macOS
- Android（レガシデバイス管理者）

Android Enterprise の場合、管理対象構成デバイスポリシーを使用して、VPN プロファイルを構成します。

Per-App VPN オプションは、特定の接続の種類で使用できます。次の表は、Per-App VPN オプションが利用できる条件を示しています。

プラットフォーム	接続の種類	注釈
iOS	Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO、またはカスタム SSL。	
macOS	Cisco AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、またはカスタム SSL。	
Android（レガシデバイス管理者）	Citrix SSO	

Citrix SSO アプリを使用して iOS および Android（レガシデバイス管理者）デバイス用の Per-App VPN を作成するには、VPN ポリシーの構成に加えて、追加の手順を実行する必要があります。また、次の前提条件が満たされていることを確認する必要があります：

- オンプレミスの Citrix Gateway
- 次のアプリケーションがデバイスにインストールされています：
  - Citrix SSO
  - Citrix Secure Hub

Citrix SSO アプリを使用して、iOS および Android デバイスの Per-App VPN を構成するための一般的なワークフローは次のとおりです：

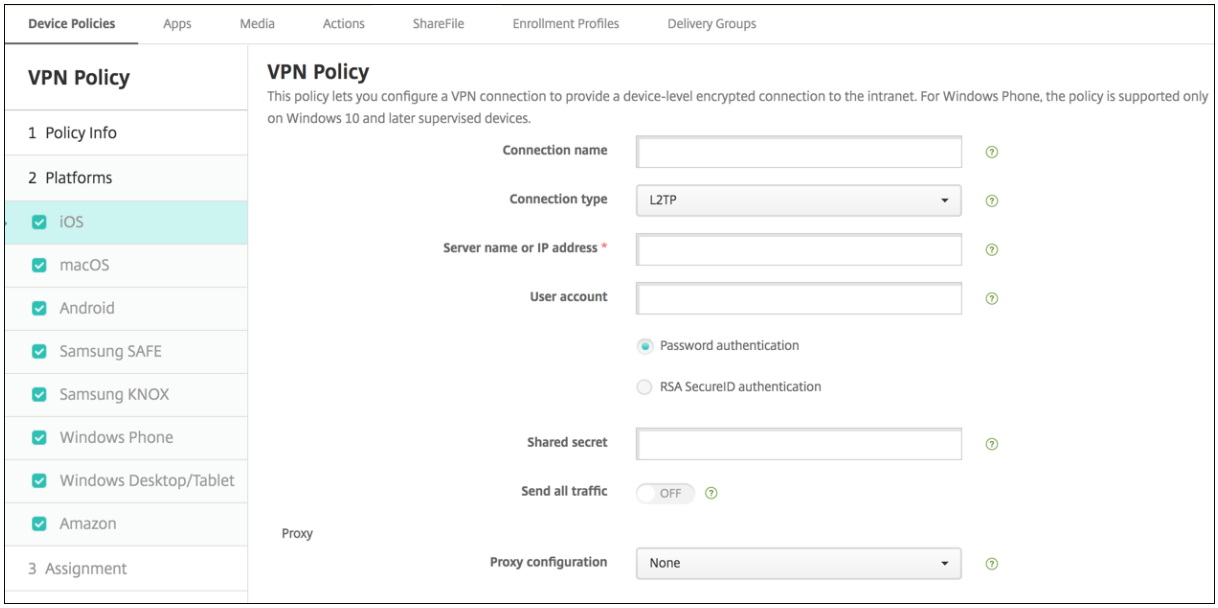
1. この記事の説明に従って、VPN デバイスポリシーを構成します。
   - iOS の場合、「iOS 向け Citrix SSO プロトコルの構成」を参照してください。VPN デバイスポリシーによって iOS の Citrix SSO プロトコルを構成した後、アプリを Per-App VPN ポリシーに関連付けるためのアプリ属性ポリシーも作成する必要があります。詳しくは、「Per-App VPN の構成」を参照してください。
     - ［接続の認証の種類］フィールドで、［証明書］を選択する場合、最初に Citrix Endpoint Management の証明書ベースの認証を構成する必要があります。「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。
   - Android（レガシデバイス管理者）の場合は、「Android 向け Citrix SSO プロトコルを構成する」を参照してください。
     - ［接続の認証の種類］フィールドで、［証明書］または ［パスワードおよび証明書］を選択する場合、最初に Citrix Endpoint Management の証明書ベースの認証を構成する必要があります。「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照してください。

2. Per-App VPN からのトラフィックを受け入れるように Citrix ADC を構成します。詳しくは、「Citrix Gateway での完全 VPN のセットアップ」を参照してください。

iOS の設定

iOS 用の VPN デバイスポリシーの Citrix VPN 接続タイプは、iOS 12 をサポートしていません。VPN デバイスポリシーを削除し、Citrix SSO 接続の種類で VPN デバイスポリシーを作成するには、以下の手順に従います:

1. iOS の VPN デバイスポリシーを削除します。
2. 次の設定で、iOS の VPN デバイスポリシーを追加します:
    - 接続の種類: **Citrix SSO**
    - **Per-App VPN** を有効にする: オン
    - プロバイダーの種類: パケットトンネル
3. iOS のアプリ属性デバイスポリシーを追加します。[**Per-App VPN** 識別子] で **iOS_VPN** を選択します。



- 接続名: 接続名を入力します。
- 接続の種類: 一覧から、この接続において使用するプロトコルを選択します。デフォルトは [**L2TP**] です。
    - **L2TP**: レイヤー 2 トンネリングプロトコルと事前共有キー認証。
    - **PPTP**: Point-to-Point トンネリング。
    - **IPSec**: 社内 VPN 接続
    - **Cisco Legacy AnyConnect**: この接続の種類では、従来の Cisco AnyConnect VPN クライアントがユーザーデバイスにインストールされている必要があります。Cisco は、廃止された VPN フレームワークに基づいていた従来の Cisco AnyConnect クライアントを段階的に廃止しています。

現在の Cisco AnyConnect クライアントを使用するには、接続の種類はカスタム **SSL** を使用します。必要な設定については、このセクションの「カスタム SSL プロトコルの構成」を参照してください。

- **Juniper SSL**: Juniper Networks SSL VPN クライアント
- **F5 SSL**: F5 Networks SSL VPN クライアント
- **SonicWALL Mobile Connect**: iOS 用 Dell 統合 VPN クライアント
- **Ariba VIA**: Aruba Networks 仮想インターネットアクセスクライアント
- **IKEv2**（**iOS only**）: iOS 専用インターネットキー交換バージョン 2
- **AlwaysOn IKEv2**: IKEv2 を使用した常時アクセス。
- **AlwaysOn IKEv2** デュアル構成: IKEv2 デュアル構成を使用した常時アクセス。
- **Citrix SSO**: iOS 12 以降の Citrix SSO クライアント。
- カスタム **SSL**: カスタム SSL（Secure Socket Layer）この接続の種類は、バンドル ID が **com.cisco.anyconnect** の Cisco AnyConnect クライアントに必要です。**Cisco AnyConnect** の接続名を指定します。また、VPN ポリシーを展開して、iOS デバイス用のネットワークアクセス制御（NAC）フィルターを有効にすることもできます。このフィルターで、非準拠のアプリがインストールされているデバイスの VPN 接続をブロックできます。この構成では、iOS VPN ポリシーの特定の設定が必要です（下記の iOS セクションを参照）。NAC フィルターを有効にするために必要なその他の設定の詳細については、「ネットワークアクセス制御」を参照してください。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

iOS 向け **L2TP** プロトコルの設定

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- ［パスワード認証］または ［**RSA SecurID** 認証］をクリックします。
- 共有シークレット: IPsec 共有シークレットキーを入力します。
- すべてのトラフィックを送信: VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］です。

iOS 向け **PPTP** プロトコルの設定

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- ［パスワード認証］または ［**RSA SecurID** 認証］をクリックします。
- 暗号化レベル: 一覧から、暗号化レベルを選択します。デフォルトは ［なし］です。
  - なし: 暗号化を使用しません。
  - 自動: サーバーでサポートされている最も強力な暗号化レベルを使用します。

  - 最大（**128** ビット）：常に 128 ビットの暗号化を使用します。

- すべてのトラフィックを送信： VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］です。

iOS 向け **IPsec** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧から、この接続の認証の種類として、［共有シークレット］または ［証明書］を選択します。デフォルトは ［共有シークレット］です。
- ［共有シークレット］を有効にした場合は、次の設定を構成します：
  - グループ名：任意で、グループ名を入力します。
  - 共有シークレット：任意で、共有シークレットキーを入力します。
  - ハイブリッド認証を使用：ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対する認証を行い、次にクライアントがサーバーに対する認証を行います。デフォルトは ［オフ］です。
  - パスワードの入力を要求：ネットワークへの接続時にユーザーにパスワードの入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
- ［証明書］を有効にした場合は、次の設定を構成します：
  - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
  - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーによる PIN の入力を必須とするかどうかを選択します。デフォルトは ［オフ］です。
  - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。
- オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］です。
- **Safari** ドメイン：［追加］をクリックして、Safari ドメイン名を追加します。

従来の **iOS** 向け **Cisco AnyConnect** プロトコルの構成

従来の Cisco AnyConnect クライアントから新しい Cisco AnyConnect クライアントに移行するには、カスタム SSL プロトコルを使用します。

- プロバイダーのバンドル識別子: 従来の AnyConnect クライアントの場合、バンドル ID は com.cisco.anyconnect.gui です。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- グループ: 任意で、グループ名を入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します:
    - **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- すべてのネットワークを含める: すべてのネットワークにこの接続の使用を許可するかを選択します。デフォルトは ［オフ］です。
- ローカルネットワークを除外する: ローカルネットワークを接続での使用から除外するか、ネットワークを許可するかを選択できます。デフォルトは ［オフ］です。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します:
  - オンデマンドマッチアプリが有効: Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］です。
  - プロバイダーの種類: Per-App VPN が ［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは ［アプリプロキシ］です。
  - **Safari** ドメイン: Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います:
    - ドメイン: 追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **Juniper SSL** プロトコルの構成

- プロバイダーのバンドル識別子: Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。

- 領域：オプションの領域名を入力します。
- 役割：オプションの役割名を入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］です。
  - プロバイダーの種類： Per-App VPN が ［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは ［アプリプロキシ］です。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    - ドメイン：追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **F5 SSL** プロトコルの構成

- プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。

        * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
    - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
    - プロバイダーの種類： Per-App VPN が ［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは ［アプリプロキシ］です。
    - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
        * ドメイン：追加するドメインを入力します。
        *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **SonicWALL** プロトコルの構成

- プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- ログオングループまたはドメイン：任意で、ログオングループまたはドメインを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
    -［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
    -［証明書］を有効にした場合は、次の設定を構成します：
        * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
        * 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
        * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを［オン］に設定した場合は、次の設定を構成します：

- オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
- プロバイダーの種類： Per-App VPN が ［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは ［アプリプロキシ］です。
- **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
  * ドメイン：追加するドメインを入力します。
  *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **Ariba VIA** プロトコルの構成

- プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  -［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  -［証明書］を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    * 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    * ドメイン：追加するドメインを入力します。
    *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **IKEv2** プロトコルの構成

このセクションには、IKEv2、Always On IKEv2、Always On IKEv2 のデュアル構成プロトコルで使用する設定が含まれます。Always On IKEv2 デュアル構成プロトコルの場合は、携帯電話ネットワークと Wi-Fi ネットワークの両方でこれらの設定をすべて構成します。

- 自動接続の無効化をユーザーに許可： Always On プロトコルが対象です。デバイスでネットワークへの自動接続を無効にすることをユーザーに許可するかどうかを選択します。デフォルトは ［オフ］です。
- サーバーのホスト名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ローカル識別子： IKEv2 クライアントの FQDN または IP アドレスを入力します。このフィールドは必須です。
- リモート識別子： VPN サーバーの FQDN または IP アドレスを入力します。このフィールドは必須です。
- デバイス認証：この接続の認証の種類として、［共有シークレット］、［証明書］または ［デバイス識別子ベースのデバイス証明書］を選択します。デフォルトは ［共有シークレット］です。
  - 共有シークレット：任意で、共有シークレットキーを入力します。
  - ［証明書］を選択した場合は、［**ID** 資格情報］の使用を選択します。デフォルトは ［なし］です。
  - ［デバイス識別子ベースのデバイス証明書］を選択した場合は、［デバイス **ID** の種類］を選択します。デフォルトは ［**IMEI**］です。このオプションを使用するには、REST API を使用して証明書を一括インポートします。「REST API を使用した証明書の一括アップロード」を参照してください。［**Always On IKEv2**］を選択した場合にのみ使用できます。
- 拡張認証が有効：拡張認証プロトコル（EAP）を有効にするかどうかを選択します。［オン］にした場合は、ユーザーアカウントと認証パスワードを入力します。
- 停止ピア検出間隔：ピアデバイスが到達可能であるかを確認するための問い合わせ頻度を選択します。デフォルトは ［なし］です。次のオプションがあります：
  - なし：使用不能なピアの検出を無効にします。
  - 低： 30 分ごとにピアに問い合わせます。
  - 中： 10 分ごとにピアに問い合わせます。
  - 高： 1 分ごとにピアに問い合わせます。
- モビリティおよびマルチホーミングを無効化：この機能を無効にするかどうかを選択します。
- **IPv4/IPv6** 内部サブネット属性の使用：この機能を有効にするかどうかを選択します。
- リダイレクトを無効化：リダイレクトを無効にするかどうかを選択します。
- フォールバックを有効にする：この設定を有効にすると、Wi-Fi アシストの対象で VPN が必要なトラフィックを携帯データネットワーク経由のトンネルで伝送できます。デフォルトは ［オフ］です。

- デバイスのスリープ中 **NAT** キープアライブを有効化： Always On プロトコルが対象です。キープアライブパケットは IKEv2 接続の NAT マッピングを維持するために使用されます。このパケットは、デバイスがオンになっているとチップによって定期的な間隔で送信されます。設定を［オン］にすると、デバイスがスリープ中でもキープアライブパケットはチップで送信されます。デフォルト間隔は、Wi-Fi 経由で 20 秒、携帯経由で 110 秒です。この間隔は、NAT キープアライブ間隔のパラメーターを使用して変更できます。
- **NAT** キープアライブ間隔（秒）：デフォルトでは 20 秒です。
- **Perfect Forward Secrecy** を有効化：この機能を有効にするかどうかを選択します。
- **DNS** サーバーの **IP** アドレス：オプション。DNS サーバーの IP アドレス文字列の一覧です。これらの IP アドレスには、IPv4 アドレスと IPv6 アドレスを混在させることができます。［追加］をクリックしてアドレスを入力します。
- ドメイン名：オプション。トンネルのプライマリドメインです。
- 検索ドメイン：オプション。単一ラベルホスト名の完全修飾に使用されるドメインの一覧です。
- 補足マッチドメインをリゾルバー一覧に追加する：オプション。補足マッチドメイン一覧を、リゾルバーの検索ドメイン一覧に追加するかどうかを決定します。デフォルトは ［オン］です。
- 補足マッチドメイン：オプション。どの DNS クエリが DNS サーバーアドレスに含まれる DNS リゾルバー設定を使用するかを判別するドメイン文字列の一覧です。このキーは、特定のドメインのホストのみがトンネルの DNS リゾルバーを使用して解決される、分割 DNS 設定を作成するために使用されます。この一覧のドメインにないホストは、システムのデフォルトのリゾルバーを使用して解決されます。

このパラメーターに空の文字列が含まれる場合は、この文字列がデフォルトのドメインです。これにより、分割トンネルの設定によって、すべての DNS クエリをプライマリ DNS サーバーの前にまず VPN DNS サーバーに振り分けることができます。VPN トンネルがネットワークのデフォルトルートである場合、一覧に追加された DNS サーバーはデフォルトのリゾルバーになります。この場合、補足マッチドメインの一覧は無視されます。

- **IKE SA** パラメーターおよび 子 **SA** パラメーター： Security Association（SA）パラメーターオプションごとに、次の設定を構成します：
  - 暗号化アルゴリズム：一覧から、使用する IKE 暗号化アルゴリズムを選択します。デフォルトは **3DES** です。
  - 整合性アルゴリズム：一覧から、使用する整合性アルゴリズムを選択します。デフォルトは **SHA-256** です。
  - **Diffie Hellman** グループ：一覧から、Diffie Hellman グループ番号を選択します。デフォルトは **2** です。
  - **ike** 有効期間（分）： SA の有効期間（キー更新間隔）を表す 10～1440 の整数を入力します。デフォルトは **1440** 分です。
- サービスの例外： Always On プロトコルが対象です。サービスの例外とは、Always On VPN から除外されたシステムサービスです。次のサービス例外設定を構成します

  - ボイスメール：一覧から、ボイスメールの例外を処理する方法を選択します。デフォルトは ［トンネル経由のトラフィックを許可］です。
  - **AirPrint**：一覧から、AirPrint の例外を処理する方法を選択します。デフォルトは ［トンネル経由のトラフィックを許可］です。
  - **VPN** トンネル外のキャプティブ **Web** シートからのトラフィックを許可：ユーザーが VPN トンネルの外側にある公衆ホットスポットに接続するのを許可するかどうかを選択します。デフォルトは ［オフ］です。
  - **VPN** トンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可： VPN トンネルの外側にあるすべてのホットスポットネットワーキングアプリを許可するかどうかを選択します。デフォルトは ［オフ］です。
  - キャプティブネットワークアプリのバンドル **ID**：ユーザーによるアクセスが許可されているホットスポットネットワーキングのアプリバンドル ID ごとに、［追加］をクリックしてホットスポットネットワーキングのアプリバンドル **ID** を入力します。［保存］をクリックしてアプリバンドル ID を保存します。

- **Per-app VPN**：次の設定を IKEv2 の接続の種類用に構成します。
  - **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。
  - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］です。
  - **Safari** ドメイン：［追加］をクリックして、Safari ドメイン名を追加します。
- プロキシ構成：プロキシサーバー経由での VPN 接続のルーティング方法を選択します。デフォルトは ［なし］です。

iOS 向け **Citrix SSO** プロトコルの構成

Citrix SSO クライアントは、Apple Store で入手することができます。

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。

    * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを［オン］に設定した場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  - プロバイダーの種類： Per-App VPN が ［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは ［アプリプロキシ］です。
  - プロバイダーの種類：［パケットトンネル］に設定します。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    * ドメイン：追加するドメインを入力します。
    *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- カスタム **XML**：追加するカスタム XML パラメーターごとに、［追加］をクリックしてキーと値のペアを指定します。使用できるパラメーターは次のとおりです：
  - **disableL3**：システムレベルの VPN を無効化します。アプリごとの VPN のみ許容します。値は不要です。
  - **user agent**：このデバイスポリシーに、VPN プラグインクライアントを対象とする任意の Citrix Gateway ポリシーを関連付けます。このキーの値は、プラグインによって開始される要求に対応して、VPN プラグインに自動的に追加されます。

iOS 向けカスタム **SSL** プロトコルの構成

従来の Cisco AnyConnect クライアントから Cisco AnyConnect クライアントに移行するには：

1. カスタム SSL プロトコルを使用して VPN デバイスポリシーを構成します。iOS デバイスにポリシーを展開します。
2. Cisco AnyConnect クライアントをhttps://apps.apple.com/us/app/cisco-secure-client/id1135064690からアップロードし、このアプリを Citrix Endpoint Management に追加してから iOS デバイスに展開します。
3. iOS デバイスから古い VPN デバイスポリシーを削除します。

設定：

- カスタム **SSL** 識別子（リバース **DNS** 形式）：バンドル ID に設定します。Cisco AnyConnect クライアントの場合は、**com.cisco.anyconnect** を使用します。

- プロバイダーのバンドル識別子：［カスタム **SSL** 識別子］で指定したアプリに同じ種類（アプリプロキシまたはパケットトンネル）の VPN プロバイダーが複数設定されている場合、このバンドル ID を指定します。Cisco AnyConnect クライアントの場合は、**com.cisco.anyconnect** を使用します。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- すべてのネットワークを含める：すべてのネットワークにこの接続の使用を許可するかを選択します。デフォルトは ［オフ］です。
- ローカルネットワークを除外する：ローカルネットワークを接続での使用から除外するか、ネットワークを許可するかを選択できます。デフォルトは ［オフ］です。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを［オン］に設定した場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  - プロバイダーの種類：プロバイダーの種類では、プロバイダーが VPN サービスとプロキシサービスのどちらであるかを指定します。VPN サービスの場合は ［パケットトンネル］を選択します。プロキシサービスの場合は ［アプリプロキシ］を選択します。Cisco AnyConnect クライアントの場合は、［パケットトンネル］を選択します。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    - ドメイン：追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- カスタム **XML**：追加するカスタム XML パラメーターごとに、［追加］をクリックして以下の操作を行います。
  - パラメーター名：追加するパラメーターの名前を入力します。
  - 値：［パラメーター名］に関連付ける値を入力します。
  - ［保存］をクリックしてパラメーターを保存するか、［キャンセル］をクリックして操作を取り消します。

NAC をサポートするように **VPN** デバイスポリシーを構成する

1. NAC フィルターを設定するには、カスタム **SSL** の接続の種類が必要です。
2. **VPN** の ［接続名］を指定します。
3. ［カスタム **SSL** 識別子］に、「**com.citrix.NetScalerGateway.ios.app**」と入力します。
4. ［プロバイダーのバンドル識別子］に、「**com.citrix.NetScalerGateway.ios.app.vpnplugin**」と入力します。

手順 3 と手順 4 の値は、NAC のフィルタリングに必要な Citrix SSO インストールの値です。認証パスワードは設定しないでください。NAC 機能の使用の詳細については、「ネットワークアクセス制御」を参照してください。

iOS 向け［オンデマンドに **VPN** を有効化］オプションの構成

- オンデマンドドメイン：ドメインごと、およびユーザーがドメインに接続したときに実行される関連アクションごとに、［追加］をクリックして以下の操作を行います：
- ドメイン：追加するドメインを入力します。
- アクション：一覧から、提供されているアクションのいずれかを選択します：
  - 常に確立：ドメインは常に VPN 接続をトリガーします。
  - 確立しない：ドメインは VPN 接続をトリガーしません。
  - 必要な場合確立：ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
  - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- オンデマンドルール
  - アクション：一覧から、実行するアクションを選択します。デフォルトは ［**EvaluateConnection**］です。選択できるアクションは以下のとおりです：
    - 許可：トリガーされたときに VPN オンデマンドで接続できるようにします。
    - 接続：無条件で VPN 接続を開始します。
    - 切断： VPN 接続を解除し、規則と一致しない限りオンデマンドの再接続を行いません。
    - **EvaluateConnection**：接続ごとに、ActionParameters 配列を評価します。
    - 無視：既存の VPN 接続を動作中のままにします。ただし、規則と一致しない限りオンデマンドの再接続を行いません。
  - **DNSDomainMatch**：デバイスの検索ドメイン一覧と一致する可能性のある、追加するドメインごとに、［追加］をクリックして以下の操作を行います：
    - **DNS** ドメイン：ドメイン名を入力します。ワイルドカード文字「*」をプレフィックスに使用すると、複数のドメインと一致させることができます。たとえば、*.example.com は、mydomain.example.com、yourdomain.example.com、herdomain.example.com と一致します。

    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- **DNSServerAddressMatch**：ネットワークの指定された DNS サーバーと一致する可能性のある、追加する IP アドレスごとに、［追加］をクリックして以下の操作を行います。
    - **DNS** サーバーアドレス：追加する DNS サーバーアドレスを入力します。ワイルドカード文字「*」をサフィックスに使用すると、複数の DNS サーバーと一致させることができます。たとえば、17.* はクラス A サブネットのすべての DNS サーバーと一致します。
    - ［保存］をクリックして DNS サーバーアドレスを保存するか、［キャンセル］をクリックして操作を取り消します。
- **InterfaceTypeMatch**：一覧から、使用中のプライマリネットワークインターフェイスハードウェアの種類を選択します。デフォルトは ［未指定］です。使用できる値は以下のとおりです：
    - 未指定：あらゆるネットワークインターフェイスハードウェアと一致します。このオプションがデフォルトです。
    - イーサネット：イーサネットネットワークインターフェイスハードウェアのみと一致します。
    - **Wi-Fi**： Wi-Fi ネットワークインターフェイスハードウェアのみと一致します。
    - 携帯ネットワーク：携帯ネットワークインターフェイスハードウェアのみと一致します。
- **SSIDMatch**：現在のネットワークと照合する、追加する SSID ごとに、［追加］をクリックして以下の操作を行います。
    - **SSID**：追加する SSID を入力します。ネットワークが Wi-Fi ネットワークでない場合、または SSID が表示されない場合は照合できません。すべての SSID と一致させるには、この一覧を空白のままにします。
    - ［保存］をクリックして SSID を保存するか、［キャンセル］をクリックして操作を取り消します。
- **URLStringProbe**：フェッチする URL を入力します。この URL がリダイレクトされず正常にフェッチされた場合は、この規則に一致しています。
- **ActionParameters**：**Domains**： EvaluateConnection のチェック対象となる、追加するドメインごとに、［追加］をクリックして以下の操作を実行します：
    - ドメイン：追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- **ActionParameters : DomainAction**：一覧から、**ActionParameters : Domains** で指定したドメインに対する **VPN** の動作を選択します。デフォルトは ［**ConnectIfNeeded**］です。選択できるアクションは以下のとおりです：
    - **ConnectIfNeeded**：ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
    - **NeverConnect**：ドメインは VPN 接続をトリガーしません。
- **Action Parameters**：**RequiredDNSServers**：指定したドメインの解決に使用する DNS サーバーごとに、［追加］をクリックして以下の操作を行います：
    - **DNS** サーバー： **ActionParameters** :**DomainAction** が **ConnectIfNeeded** の場合にのみ有効です。DNS サーバーの IP アドレスを入力します。このサーバーは、デバイスの現在のネット

ワーク構成外に配置できます。この DNS サーバーに到達できない場合、対応として VPN 接続が確立されます。この DNS サーバーが、内部 DNS サーバーまたは信頼できる外部 DNS サーバーであることを確認します。

  * ［保存］をクリックして DNS サーバーを保存するか、［キャンセル］をクリックして操作を取り消します。

- **ActionParameters : RequiredURLStringProbe**：任意で、プローブする HTTP または HTTPS（推奨）の URL を、GET リクエストを使用して入力します。URL のホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、対応として VPN 接続が確立されます。**ActionParameters** : **DomainAction** が **ConnectIfNeeded** の場合にのみ有効です。
- **OnDemandRules : XML content**：XML 構成オンデマンド規則を入力するか、コピーして貼り付けます。

  * ［ディクショナリをチェック］をクリックし、XML コードを検証します。XML が有効な場合は、［**XML** コンテンツ］テキストボックスの下に「有効な **XML**」と表示されます。有効でない場合は、エラーを説明するエラーメッセージが表示されます。

- プロキシ

  - プロキシ構成：一覧から、VPN 接続のプロキシサーバーのルーティング方法を選択します。デフォルトは ［なし］です。

    * ［手動］を有効にした場合は、次の設定を構成します：
      - プロキシサーバーのホスト名または **IP** アドレス：プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
      - プロキシサーバーのポート：プロキシサーバーのポート番号を入力します。このフィールドは必須です。
      - ユーザー名：任意で、プロキシサーバーのユーザー名を入力します。
      - パスワード：任意で、プロキシサーバーのパスワードを入力します。
    * ［自動］を選択した場合は、次の設定を構成します：
      - プロキシサーバー **URL**：プロキシサーバーの URL を入力します。このフィールドは必須です。

- ポリシー設定

  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。

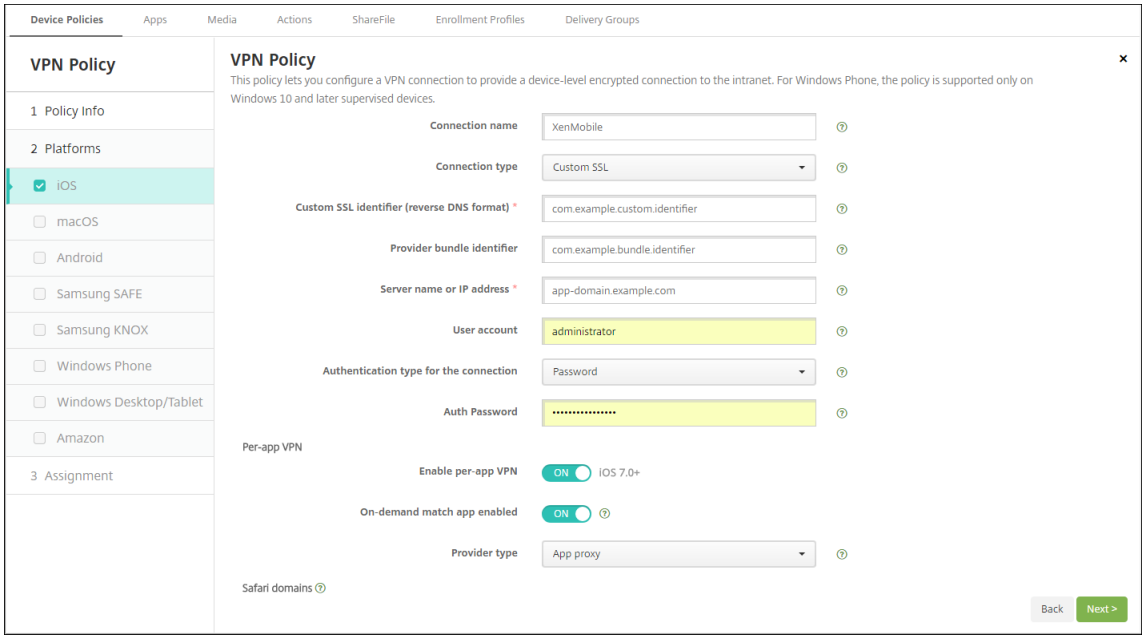
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

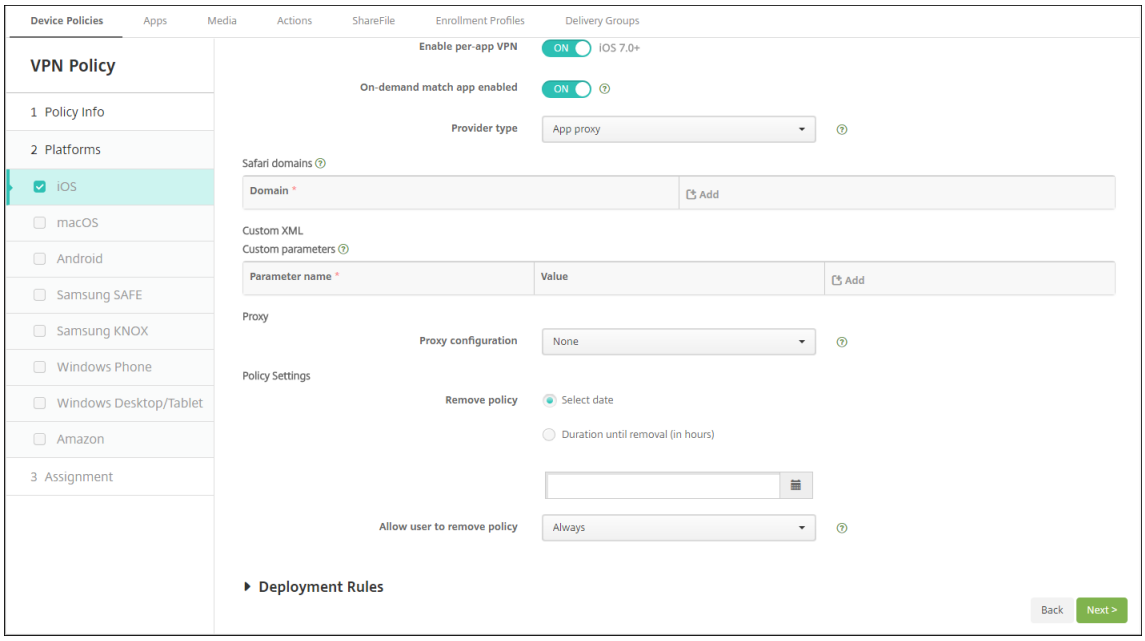
Per-App VPN の構成

iOS 向けの Per-App VPN オプションは、Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO、およびカスタム SSL の接続の種類で使用できます。

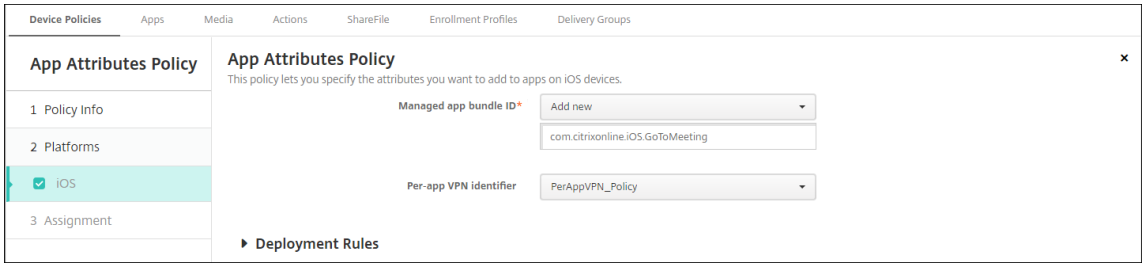
Per-App VPN を構成するには次の手順に従います。

1. ［構成］**>**［デバイスポリシー］で、VPN ポリシーを作成します。例:

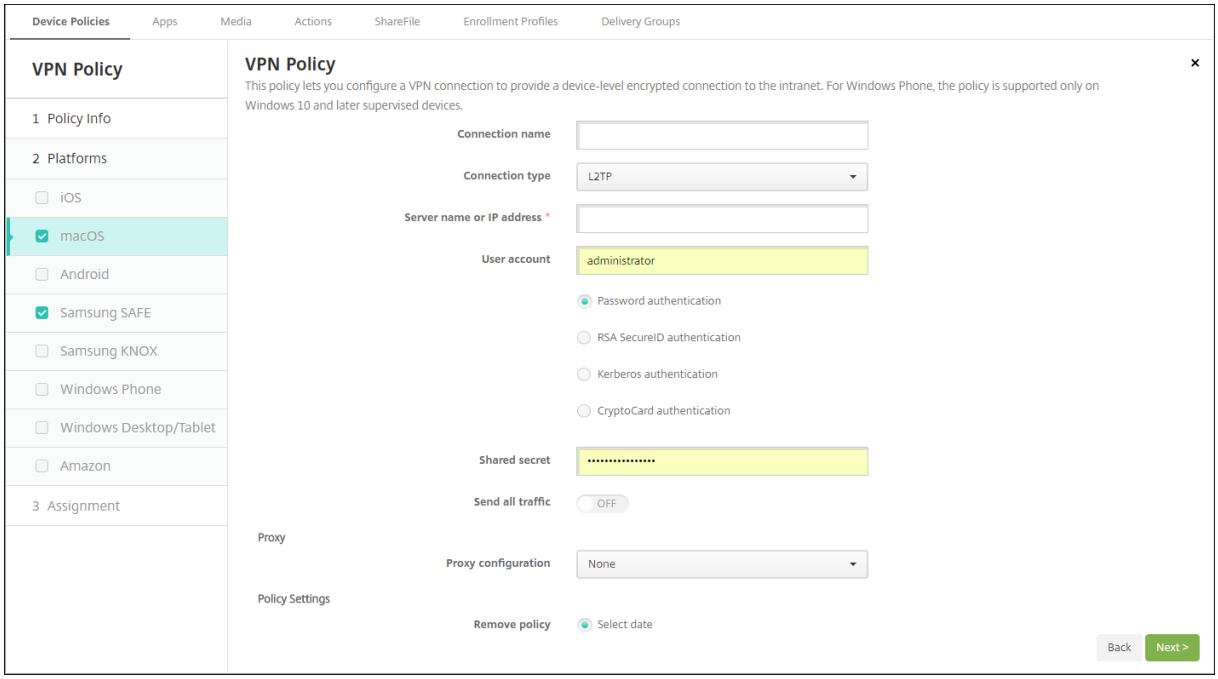




2. ［構成］**>**［デバイスポリシー］でアプリ属性ポリシーを作成し、アプリをこの Per-App VPN ポリシーに関連付けます。［**Per-app VPN** 識別子］では、手順 1 で作成した VPN ポリシーの名前を選択します。［管理対象アプリのバンドル **ID**］は、アプリ一覧から選択するか、アプリバンドル ID を入力します（iOS アプリインベントリポリシーを展開している場合は、アプリ一覧にアプリが含まれます）。



macOS 設定



- 接続名：接続名を入力します。
- 接続の種類：一覧から、この接続において使用するプロトコルを選択します。デフォルトは［L2TP］です。
  - **L2TP**：レイヤー 2 トンネリングプロトコルと事前共有キー認証。
  - **PPTP**： Point-to-Point トンネリング。
  - **IPSec**：社内 VPN 接続
  - **Cisco AnyConnect**： Cisco AnyConnect VPN クライアント
  - **Juniper SSL**： Juniper Networks SSL VPN クライアント
  - **F5 SSL**： F5 Networks SSL VPN クライアント
  - **SonicWALL Mobile Connect**： iOS 用 Dell 統合 VPN クライアント
  - **Ariba VIA**： Aruba Networks 仮想インターネットアクセスクライアント
  - **Citrix VPN**： Citrix VPN クライアント
  - カスタム **SSL**：カスタム SSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

macOS 向け **L2TP** プロトコルの設定

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- ［パスワード認証］、［**RSA SecurID** 認証］、［**Kerberos** 認証］、［**CryptoCard** 認証］のいずれかを選択します。デフォルトは ［パスワード認証］です。
- 共有シークレット： IPsec 共有シークレットキーを入力します。
- すべてのトラフィックを送信： VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］です。

macOS 向け **PPTP** プロトコルの設定

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- ［パスワード認証］、［**RSA SecurID** 認証］、［**Kerberos** 認証］、［**CryptoCard** 認証］のいずれかを選択します。デフォルトは ［パスワード認証］です。
- 暗号化レベル：必要な暗号化レベルを選択します。デフォルトは ［なし］です。
  - なし：暗号化を使用しません。
  - 自動：サーバーでサポートされている最も強力な暗号化レベルを使用します。
  - 最大（128 ビット）：常に 128 ビットの暗号化を使用します。
- すべてのトラフィックを送信： VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］です。

macOS 向け **IPsec** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧から、この接続の認証の種類として、［共有シークレット］または ［証明書］を選択します。デフォルトは ［共有シークレット］です。
  - ［共有シークレット］認証を有効にした場合は、次の設定を構成します。
    - グループ名：任意で、グループ名を入力します。
    - 共有シークレット：任意で、共有シークレットキーを入力します。
    - ハイブリッド認証を使用：ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対する認証を行い、次にクライアントがサーバーに対する認証を行います。デフォルトは ［オフ］です。
    - パスワードの入力を要求：ネットワークへの接続時にユーザーにパスワードの入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
  - ［証明書］認証を有効にした場合は、次の設定を構成します。

    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求：ネットワークへの接続時にユーザーによる PIN の入力を必須とするかどうかを選択します。デフォルトは ［オフ］です。
    * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］オプションの構成」を参照してください。

macOS 向け **Cisco AnyConnect** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- グループ：任意で、グループ名を入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    * 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
  - **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
    * プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。デフォルトは ［オフ］です。
    * **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
      - ドメイン：追加するドメインを入力します。
      - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

macOS 向け **Juniper SSL** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。

- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 領域：オプションの領域名を入力します。
- 役割：オプションの役割名を入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します。
  - プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。デフォルトは ［オフ］です。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    - ドメイン：追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

macOS 向け **F5 SSL** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］

であるときの設定の構成について詳しくは、「[オンデマンドに VPN を有効化］オプションの構成」を参照してください。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
  - プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。デフォルトは ［オフ］です。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    * ドメイン：追加するドメインを入力します。
    * ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

macOS 向け **SonicWALL Mobile Connect** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- ログオングループまたはドメイン：任意で、ログオングループまたはドメインを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    * 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    * オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「[オンデマンドに VPN を有効化］オプションの構成」を参照してください。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
  - プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。デフォルトは ［オフ］です。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    * ドメイン：追加するドメインを入力します。
    * ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

macOS 向け **Ariba VIA** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
- 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。
    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
  - プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。デフォルトは ［オフ］です。
  - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
    - ドメイン：追加するドメインを入力します。
    - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

macOS 向けカスタム **SSL** プロトコルの構成

- カスタム **SSL** 識別子（リバース **DNS** 形式）： SSL 識別子を逆引き DNS 形式で入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。このフィールドは必須です。
- ユーザーアカウント：任意で、ユーザーアカウントを入力します。
  - 接続の認証の種類：一覧で、この接続の認証の種類に ［パスワード］か ［証明書］のどちらを使用するかを選択します。デフォルトは ［パスワード］です。
  - ［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  - ［証明書］を有効にした場合は、次の設定を構成します：
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］です。

    - 接続時に **PIN** を要求：ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］です。
    - オンデマンドに **VPN** を有効化：ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］です。［オンデマンドに **VPN** を有効化］が ［オン］であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］オプションの構成」を参照してください。
  - **Per-app VPN**：アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］です。このオプションを有効にした場合は、次の設定を構成します：
    - オンデマンドマッチアプリが有効： Per-App VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、Per-App VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
    - **Safari** ドメイン： Per-App VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います：
      - ドメイン：追加するドメインを入力します。
      - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

- カスタム **XML**：追加するカスタム XML パラメーターごとに、［追加］をクリックして以下の操作を行います。
  - パラメーター名：追加するパラメーターの名前を入力します。
  - 値：［パラメーター名］に関連付ける値を入力します。
  - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

［オンデマンドに **VPN** を有効化］オプションの構成

- オンデマンドドメイン：追加するドメインおよびユーザーがドメインに接続したときに実行される関連アクションごとに、［追加］をクリックして以下の操作を行います：
  - ドメイン：追加するドメインを入力します。
  - アクション：一覧から、提供されているアクションのいずれかを選択します：
    - 常に確立：ドメインは常に VPN 接続をトリガーします。
    - 確立しない：ドメインは VPN 接続をトリガーしません。
    - 必要な場合確立：ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
  - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- オンデマンドルール
  - アクション：一覧から、実行するアクションを選択します。デフォルトは ［**EvaluateConnection**］です。選択できるアクションは以下のとおりです：

    * 許可：トリガーされたときに VPN オンデマンドで接続できるようにします。
    * 接続：無条件で VPN 接続を開始します。
    * 切断： VPN 接続を解除し、規則と一致しない限りオンデマンドの再接続を行いません。
    * **EvaluateConnection**：接続ごとに、**ActionParameters** 配列を評価します。
    * 無視：既存の VPN 接続を動作中のままにします。ただし、規則と一致しない限りオンデマンドの再接続を行いません。

- **DNSDomainMatch**：デバイスの検索ドメイン一覧と一致する可能性のあるドメインの ［追加］をクリックして以下の操作を行います：
    * **DNS** ドメイン：ドメイン名を入力します。ワイルドカード文字「*」をプレフィックスに使用すると、複数のドメインと一致させることができます。たとえば、*.example.com は、mydomain.example.com、yourdomain.example.com、herdomain.example.com と一致します。
    *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- **DNSServerAddressMatch**：ネットワークの指定された DNS サーバーと一致する可能性のある、追加する IP アドレスごとに、［追加］をクリックして以下の操作を行います。
    * **DNS** サーバーアドレス：追加する DNS サーバーアドレスを入力します。ワイルドカード文字「*」をサフィックスに使用すると、複数の DNS サーバーと一致させることができます。たとえば、17.* はクラス A サブネットのすべての DNS サーバーと一致します。
    *［保存］をクリックして DNS サーバーアドレスを保存するか、［キャンセル］をクリックして操作を取り消します。
- **InterfaceTypeMatch**：一覧から、使用中のプライマリネットワークインターフェイスハードウェアの種類を選択します。デフォルトは ［未指定］です。使用できる値は以下のとおりです：
    * 未指定：あらゆるネットワークインターフェイスハードウェアと一致します。このオプションがデフォルトです。
    * イーサネット：イーサネットネットワークインターフェイスハードウェアのみと一致します。
    * **Wi-Fi**： Wi-Fi ネットワークインターフェイスハードウェアのみと一致します。
    * 携帯ネットワーク：携帯ネットワークインターフェイスハードウェアのみと一致します。
- **SSIDMatch**：現在のネットワークと照合する、追加する SSID ごとに、［追加］をクリックして以下の操作を行います。
    * **SSID**：追加する SSID を入力します。ネットワークが Wi-Fi ネットワークでない場合、または SSID が表示されない場合は照合できません。すべての SSID と一致させるには、この一覧を空白のままにします。
    *［保存］をクリックして SSID を保存するか、［キャンセル］をクリックして操作を取り消します。
- **URLStringProbe**：フェッチする URL を入力します。この URL がリダイレクトされず正常にフェッチされた場合は、この規則に一致しています。
- **ActionParameters**：**Domains**： EvaluateConnection のチェック対象となる、追加するドメインごとに、［追加］をクリックして以下の操作を実行します：
    * ドメイン：追加するドメインを入力します。

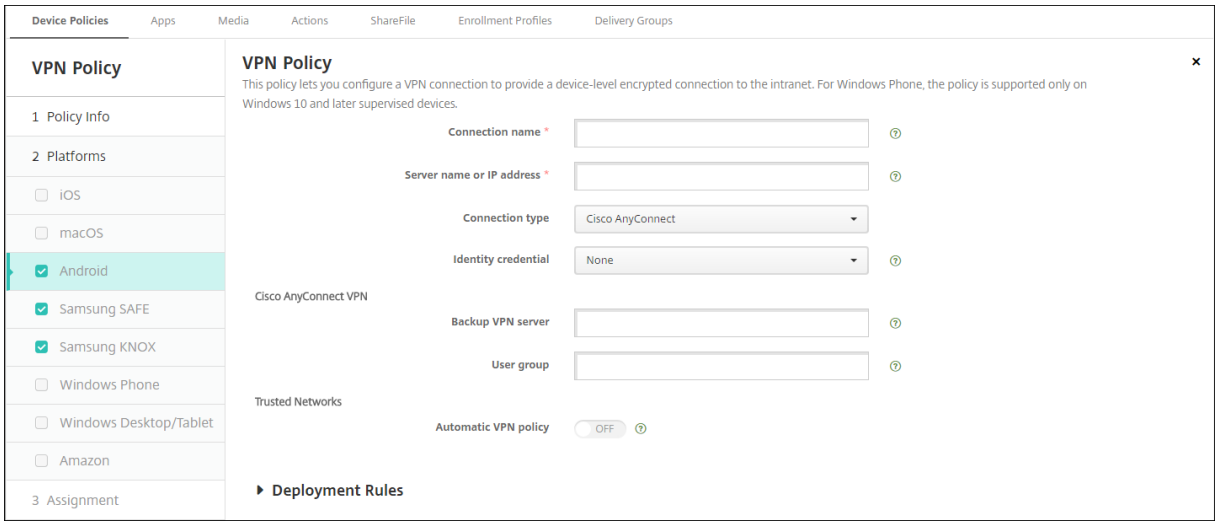
    * ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
  - **ActionParameters : DomainAction**：一覧から、**ActionParameters : Domains** で指定したドメインに対する **VPN** の動作を選択します。デフォルトは ［**ConnectIfNeeded**］です。選択できるアクションは以下のとおりです：
    * **ConnectIfNeeded**：ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
    * **NeverConnect**：ドメインは VPN 接続をトリガーしません。
  - **Action Parameters**：**RequiredDNSServers**：指定したドメインの解決に使用する DNS サーバーごとに、［追加］をクリックして以下の操作を行います：
    * **DNS** サーバー： **ActionParameters** :**DomainAction** が **ConnectIfNeeded** の場合にのみ有効です。追加する DNS サーバーの IP アドレスを入力します。このサーバーは、デバイスの現在のネットワーク構成外に配置できます。この DNS サーバーに到達できない場合、対応として VPN 接続が確立されます。この DNS サーバーは、内部 DNS サーバーまたは信頼できる外部 DNS サーバーである必要があります。
    * ［保存］をクリックして DNS サーバーを保存するか、［キャンセル］をクリックして操作を取り消します。
  - **ActionParameters : RequiredURLStringProbe**：任意で、プローブする HTTP または HTTPS（推奨）の URL を、GET リクエストを使用して入力します。URL のホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、対応として VPN 接続が確立されます。**ActionParameters** : **DomainAction** が **ConnectIfNeeded** の場合にのみ有効です。
  - **OnDemandRules : XML content**：XML 構成オンデマンド規則を入力するか、コピーして貼り付けます。
    * ［ディクショナリをチェック］をクリックし、XML コードを検証します。XML が有効な場合は、［**XML** コンテンツ］テキストボックスの下に「有効な **XML**」と表示されます。有効でない場合は、エラーを説明するエラーメッセージが表示されます。

- プロキシ
  - プロキシ構成：一覧から、VPN 接続のプロキシサーバーのルーティング方法を選択します。デフォルトは ［なし］です。
    * ［手動］を有効にした場合は、次の設定を構成します：
      - プロキシサーバーのホスト名または **IP** アドレス：プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
      - プロキシサーバーのポート：プロキシサーバーのポート番号を入力します。このフィールドは必須です。
      - ユーザー名：任意で、プロキシサーバーのユーザー名を入力します。
      - パスワード：任意で、プロキシサーバーのパスワードを入力します。
    * ［自動］を選択した場合は、次の設定を構成します：

・ プロキシサーバー **URL**：プロキシサーバーの URL を入力します。このフィールドは必須です。

- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します
  - プロファイル対策：このポリシーを ［ユーザー］または ［システム］全体に適用するかを選択します。デフォルトは ［ユーザー］です。このオプションは macOS 10.7 以降でのみ使用できます。

Android（レガシデバイス管理者）の設定



Android 向け **Cisco AnyConnect VPN** プロトコルの構成

- 接続名： Cisco AnyConnect VPN 接続の名前を入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス： VPN サーバーの名前または IP アドレスを入力します。このフィールドは必須です。
- **ID** 資格情報：一覧から、ID 資格情報を選択します。
- バックアップ **VPN** サーバー：バックアップ VPN サーバー情報を入力します。
- ユーザーグループ：ユーザーグループ情報を入力します。
- 信頼されたネットワーク

- 自動 **VPN** ポリシー：このオプションをオンまたはオフにして、信頼できるネットワークおよび信頼できないネットワークに対する VPN の動作方法を設定します。有効にした場合は、次の設定を構成します：
  - 信頼されたネットワークポリシー：一覧から、目的のポリシーを選択します。デフォルトは ［切断］です。選択できるオプションは以下のとおりです：
    - 切断：クライアントにより、信頼できるネットワーク圏内の VPN 接続が終了されます。この設定がデフォルトです。
    - 接続：クライアントにより、信頼できるネットワーク圏内の VPN 接続が開始されます。
    - 何もしない：クライアントによるアクションはありません。
    - 一時停止：信頼できるネットワーク圏外で VPN セッションが確立された後、信頼済みとして構成されたネットワークにユーザーがアクセスすると、VPN セッションが一時停止されます。ユーザーが信頼できるネットワークから離れると、セッションが再開されます。この設定により、信頼できるネットワークを離れた後に新しい VPN セッションを確立する手間が省かれます。
  - 信頼されていないネットワークポリシー：一覧から、目的のポリシーを選択します。デフォルトは［接続］です。選択できるオプションは以下のとおりです：
    - 接続：クライアントにより、信頼できないネットワーク圏内で VPN 接続が開始されます。
    - 何もしない：クライアントにより、信頼できないネットワーク圏内で VPN 接続が開始されます。このオプションにより、［常時 VPN に接続］が無効化されます。
- 信頼されたドメイン：クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるドメインサフィックスごとに、［追加］をクリックして以下の操作を行います：
  - ドメイン：追加するドメインを入力します。
  - ［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。
- 信頼されたサーバー：クライアントが信頼できるネットワーク圏内にある場合、ネットワークインターフェイスに設定することができるサーバーアドレスごとに、［追加］をクリックして以下の操作を行います。
  - サーバー：追加するサーバーを入力します。
  - ［保存］をクリックしてサーバーを保存するか、［キャンセル］をクリックして操作を取り消します。

Android 向け **Citrix SSO** プロトコルを構成する

- 接続名： VPN 接続名を入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス： Citrix Gateway の FQDN または IP アドレスを入力します。
- 接続の認証の種類：認証の種類を選択し、選択した種類に応じて表示される次のフィールドに入力します。
  - ［ユーザー名］と ［パスワード］：認証の種類 で ［パスワード］または ［パスワードおよび証明書］を選択した場合に、VPN 資格情報を入力します。オプションです。VPN 資格情報を入力しない場合は、Citrix VPN アプリによってユーザー名とパスワードの入力が求められます。

  - **ID** 資格情報：認証の種類 が ［証明書］または ［パスワードおよび証明書］の場合に表示されます。一覧で、ID 資格情報を選択します。

- **Per-App VPN** の有効化：アプリごとの VPN を有効にするかどうかを選択します。Per-App VPN を有効にしない場合は、すべてのトラフィックが Citrix VPN トンネルを経由します。Per-App VPN を有効にした場合は、次の設定を指定します。デフォルトは ［オフ］です。

  - 許可リストまたは禁止リスト：［許可リスト］の場合は、許可リストに登録されたすべてのアプリがこの VPN を経由します。［禁止リスト］の場合は、禁止リストに登録されたアプリ以外のすべてのアプリがこの VPN を経由します。
  - アプリケーションリスト：許可リストまたは禁止リストに登録されているアプリ。［追加］をクリックし、アプリのパッケージ名のコンマ区切りの一覧を入力します。

- カスタム **XML**：［追加］をクリックし、カスタムパラメーターを入力します。Citrix Endpoint Management では、Citrix VPN について次のパラメーターがサポートされます。

  - **DisableUserProfiles**：オプションです。このパラメーターを有効にするには、［値］に「**Yes**」と入力します。有効にした場合、ユーザーが追加した VPN 接続が Citrix Endpoint Management に表示されなくなり、ユーザーは接続を追加できなくなります。この設定はグローバルな制限で、すべての VPN プロファイルに適用されます。
  - **userAgent**：文字列値です。各 HTTP 要求で送信する任意のユーザーエージェント文字列を指定できます。指定したユーザーエージェント文字列は、Citrix VPN の既存のユーザーエージェントの末尾に追加されます。

NAC をサポートするように **VPN** を構成する

1. NAC フィルターを構成するには、カスタム **SSL** の接続の種類を使用します。
2. **VPN** の ［接続名］を指定します。
3. ［カスタム **XML**］で、［追加］をクリックし、次の操作を行います：

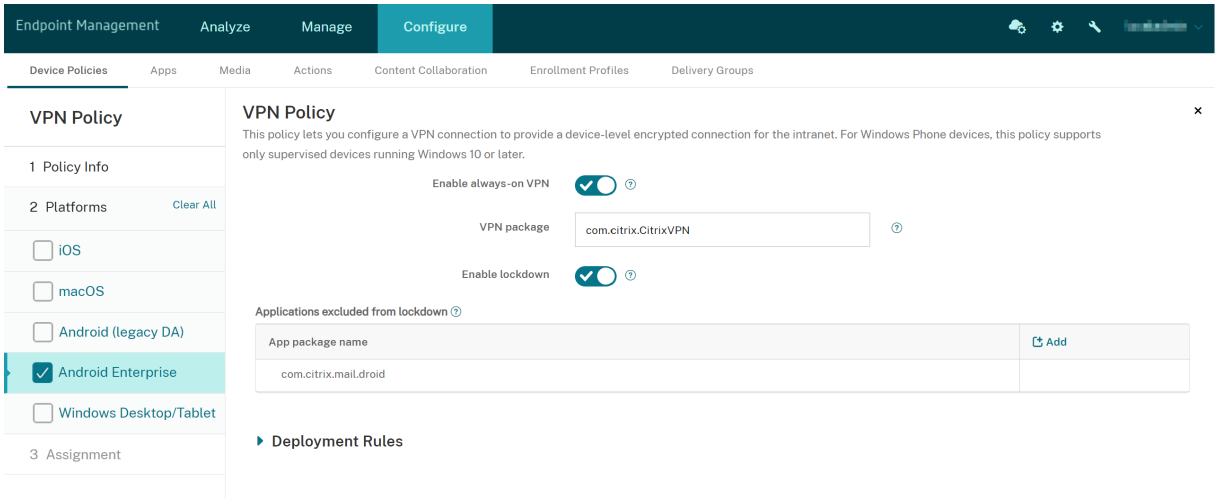
   - パラメーター名： **XenMobileDeviceId** を入力します。このフィールドは、Citrix Endpoint Management でのデバイス登録に基づく NAC チェックに使用するデバイス ID です。デバイスが Citrix Endpoint Management で登録および管理されている場合、VPN 接続は許可されます。登録および管理されていない場合、認証は VPN の確立時に拒否されます。
   - 値：「**DeviceID_$ {device.id}**」と入力します。これは、パラメーター **XenMobileDeviceId** の値です。
   - ［保存］をクリックしてパラメーターを保存します。

Android Enterprise に対する **VPN** の構成

Android Enterprise デバイスに対して VPN を構成するには、Citrix SSO アプリに対する Android Enterprise 管理対象の構成デバイスポリシーを作成します。「Android Enterprise に対する VPN プロファイルの構成」を参照し

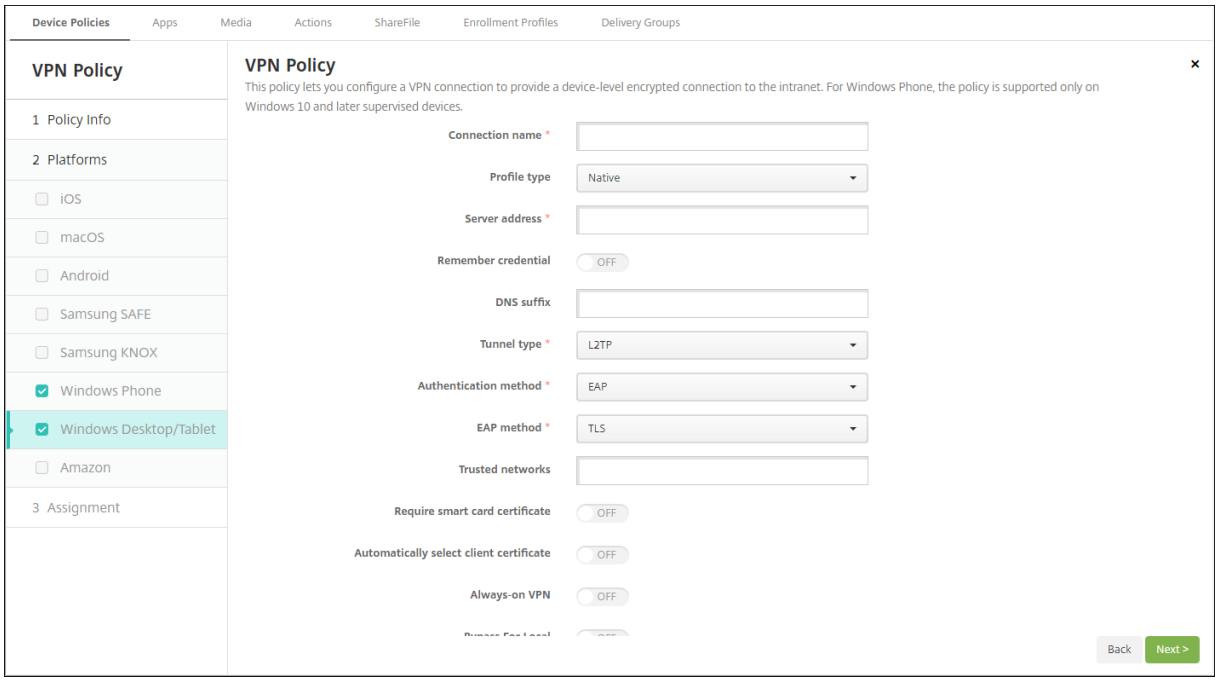
てください。

Android Enterprise の設定



- **VPN** 常時接続を有効にする： VPN を常にオンにするかどうかを選択します。デフォルトは ［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
- **VPN** パッケージ：デバイスが使用する VPN アプリのパッケージ名を入力します。
- ロックダウンを有効にする：無効にすると、VPN 接続が存在しない場合、アプリはネットワークにアクセスできません。有効にすると、VPN 接続が存在しない場合でも、次の設定で構成したアプリがネットワークにアクセスできます。Android 10 以降のデバイスで使用できます。
- ロックダウンから除外されたアプリケーション：［追加］をクリックして、ロックダウン設定をバイパスするアプリのパッケージ名を入力します。

Windows デスクトップ/タブレットの設定



- 接続名：接続名を入力します。このフィールドは必須です。
- プロファイルの種類：一覧から、［ネイティブ］または ［プラグイン］を選択します。デフォルトは ［ネイティブ］です。
- ネイティブプロファイルタイプの構成：以下の設定は、ユーザーの Windows デバイスに組み込まれている VPN に適用されます。
  - サーバーアドレス： VPN サーバーの IP アドレスを入力します。このフィールドは必須です。
  - 資格情報を保存：資格情報をキャッシュするかどうかを選択します。デフォルトは ［オフ］です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **DNS** サフィックス： DNS サフィックスを入力します。
  - トンネルタイプ：一覧から、使用する VPN トンネルの種類を選択します。デフォルトは ［**L2TP**］です。選択できるオプションは以下のとおりです：
    - **L2TP**：レイヤー 2 トンネリングプロトコルと事前共有キー認証。
    - **PPTP**： Point-to-Point トンネリング。
    - **IKEv2**：インターネットキー交換バージョン 2
  - 認証方法：一覧から、使用する認証方法を選択します。デフォルトは ［**EAP**］です。選択できるオプションは以下のとおりです：
    - **EAP**：拡張認証プロトコル。
    - **MSChapV2**：相互認証に Microsoft のチャレンジハンドシェイク認証プロトコルを使用します。トンネルタイプで ［**IKEv2**］を選択すると、このオプションは使用できません。
  - **EAP** メソッド：一覧から、使用する EAP 方法を選択します。デフォルトは［**TLS**］です。[MSChapV2] 認証が有効になっている場合、このフィールドは使用できません。選択できるオプションは以下のとお

りです:

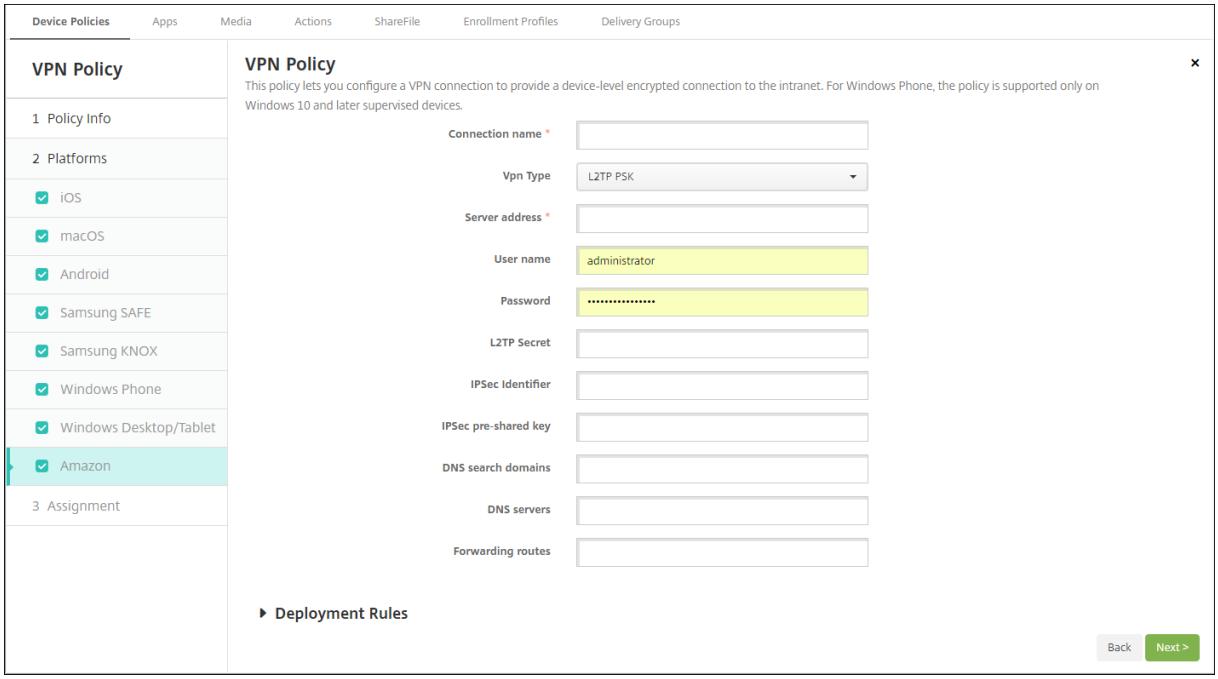
* **TLS**: Transport Layer Security
* **PEAP**: 保護された拡張認証プロトコル

- 信頼されたネットワーク: アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- スマートカード証明書を要求: スマートカード証明書を必須とするかどうかを選択します。デフォルトは ［オフ］です。
- クライアント証明書を自動的に選択: 認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。デフォルトは ［オフ］です。［スマートカード証明書を要求］が有効な場合、このオプションは使用できません。
- 常時 **VPN** に接続: VPN を常にオンにするかどうかを選択します。デフォルトは ［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
- ローカル用バイパス: ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

- プラグインプロファイルタイプの構成: 以下の設定は、Windows Store から取得し、ユーザーのデバイスにインストールした VPN プラグインに適用されます。

  - サーバーアドレス: VPN サーバーの IP アドレスを入力します。このフィールドは必須です。
  - 資格情報を保存: 資格情報をキャッシュするかどうかを選択します。デフォルトは ［オフ］です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **DNS** サフィックス: DNS サフィックスを入力します。
  - クライアントアプリ **ID**: VPN プラグインのパッケージファミリ名を入力します。
  - プラグインプロファイル **XML**: 使用するカスタム VPN プラグインプロファイルの場所に ［参照］をクリックして移動し、ファイルを選択します。形式などについて詳しくは、プラグインプロバイダーにお問い合わせください。
  - 信頼されたネットワーク: アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - 常時 **VPN** に接続: VPN を常にオンにするかどうかを選択します。デフォルトは ［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
  - ローカル用バイパス: ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

Amazon の設定



- 接続名：接続名を入力します。
- **VPN** の種類：一覧から、接続の種類を選択します。選択できるオプションは以下のとおりです：
  - **L2TP PSK**：レイヤー 2 トンネリングプロトコルと事前共有キー認証。この設定がデフォルトです。
  - **L2TP RSA**：レイヤー 2 トンネリングプロトコルと RSA 認証。
  - **IPSEC** 拡張認証 **PSK**：インターネットプロトコルセキュリティと事前共有キーおよび拡張認証。
  - **IPSEC** ハイブリッド **RSA**：インターネットプロトコルセキュリティとハイブリッド RSA 認証。
  - **PPTP**： Point-to-Point トンネリング。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

Amazon 向け L2TP PSK の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。
- **L2TP** シークレット：共有シークレットキーを入力します。
- **IPSec** 識別子：接続時にユーザーのデバイスに表示される VPN 接続の名前を入力します。
- **IPSec** 事前共有キー：秘密キーを入力します。
- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、[追加] をクリックして以下の操作を行います。

  - 転送ルート：転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

Amazon 向け **L2TP RSA** の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。
- **L2TP** シークレット：共有シークレットキーを入力します。
- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書：一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書：一覧から、使用する CA 証明書を選択します。
- **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート：転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

Amazon 向け **IPSEC XAUTH PSK** の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。
- **IPSec** 識別子：接続時にユーザーのデバイスに表示される VPN 接続の名前を入力します。
- **IPSec** 事前共有キー：共有シークレットキーを入力します。
- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート：転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

Amazon 向け **IPSEC AUTH RSA** の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。

- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書：一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書：一覧から、使用する CA 証明書を選択します。
- **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、[追加] をクリックして以下の操作を行います。
  - 転送ルート：転送ルートの IP アドレスを入力します。
  - [保存] をクリックしてルートを保存するか、[キャンセル] をクリックして操作を取り消します。

Amazon 向け **IPSEC HYBRID RSA** の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。
- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書：一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書：一覧から、使用する CA 証明書を選択します。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、[追加] をクリックして以下の操作を行います。
  - 転送ルート：転送ルートの IP アドレスを入力します。
  - [保存] をクリックしてルートを保存するか、[キャンセル] をクリックして操作を取り消します。

Amazon 向け **LPPTP** の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名：任意で、ユーザー名を入力します。
- パスワード：任意で、パスワードを入力します。
- **DNS** 検索ドメイン：ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー：指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- **PPP** 暗号化（**MPPE**）： Microsoft Point-to-Point 暗号化（MPPE）によるデータの暗号化を有効にするかどうかを選択します。デフォルトは [オフ] です。
- 転送ルート：社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、[追加] をクリックして以下の操作を行います。
  - 転送ルート：転送ルートの IP アドレスを入力します。
  - [保存] をクリックしてルートを保存するか、[キャンセル] をクリックして操作を取り消します。

壁紙デバイスポリシー

February 16, 2022

壁紙デバイスポリシーでは、.png ファイルまたは.jpg ファイルを追加して、iOS デバイスのロック画面かホーム画面、または両方の画面の壁紙に設定できます。このポリシーは、監視対象デバイスでのみ使用できます。iPad および iPhone で異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。

次の表に、Apple 社が iOS デバイス用に推奨しているイメージサイズを示します。

iPhone

デバイス	イメージサイズ（ピクセル）
iPhone 12 Pro Max	2778 x 1284
iPhone 12 & iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X、XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE（第 2 世代）	1334 x 750
iPhone 7 PLus、8 PLus	2208 x 1242
iPhone 7、8	1334 x 750
iPhone 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

デバイス	イメージサイズ（ピクセル）
iPad Pro 12.9 インチ（第 1、第 2、第 3 世代）	2732 x 2048
iPad Pro 10.5 インチ	2224 x 1668
iPad Pro（9.7 インチ）	1536 x 2048
iPad Air 2	2048 x 1536

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 適用先：一覧から、［画面をロック］、［ホーム（アイコン一覧）画面］、［ロック画面およびホーム画面］のいずれかを選択して、壁紙を表示する場所を設定します。
- 壁紙ファイル：壁紙ファイルを選択するには、［参照］をクリックしてファイルの場所に移動します。

Web コンテンツフィルターデバイスポリシー

November 29, 2023

Apple のオートフィルター機能と特定のサイトの許可リストおよび禁止リストへの追加を組み合わせて、iOS デバイスで Web コンテンツをフィルタリングできます。Web コンテンツフィルターデバイスポリシーは、監視モードの iOS デバイスでのみ使用できます。iOS デバイスを監視モードにすることについては、「Apple Configurator 2 を使用したデバイスの展開」を参照してください。

> 注：
>
> Android デバイスでは Web コンテンツフィルタリングがサポートされていません。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- フィルターの種類：一覧から ［組み込み］または ［プラグイン］を選択し、選択したオプションに応じた手順を実行します。デフォルトは ［組み込み］です。

組み込みフィルターの種類

- **Web** コンテンツフィルター
  - 自動フィルターが有効: Apple のオートフィルター機能を使用して、Web サイトに不適切なコンテンツがないかを分析するか否か。デフォルトは ［オフ］です。
  - 許可されている **URL**: この一覧は、［自動フィルターが有効］が ［オフ］に設定されている場合は無視されます。［自動フィルターが有効］が ［オン］に設定されている場合、この一覧に含まれる項目は、オートフィルターがアクセスを許可しているかどうかにかかわらず常にアクセスできます。許可リストに追加する URL ごとに、［追加］をクリックして以下の操作を行います:
    * 許可する Web サイトの URL を入力します。Web アドレスの前には、`https://`または`https://`を付ける必要があります。
    * Web サイトを許可リストに保存する場合は ［保存］をクリックし、保存しない場合は ［キャンセル］をクリックします。
  - 禁止する **URL**: このリストに含まれる項目は常にブロックされます。禁止リストに追加する URL ごとに、［追加］をクリックして以下の操作を行います:
    * ブロックする Web サイトの URL を入力します。Web アドレスの前には、`https://`または`https://`を付ける必要があります。
    * Web サイトを禁止リストに保存する場合は ［保存］をクリックし、保存しない場合は ［キャンセル］をクリックします。
- 許可リストをブックマーク
  - 許可リストをブックマーク: ユーザーがアクセスできるサイトを指定します。Web サイトへのアクセスを有効にするには、Web サイトの URL を追加します。
    * **URL**: ユーザーがアクセスできる各 Web サイトの URL。たとえば、Citrix Secure Hub ストアにアクセスできるようにするには、［**URL**］リストに Citrix Endpoint Management サーバーの URL を追加します。Web アドレスの前には、`https://`または`https://`を付ける必要があります。このフィールドは必須です。
    * フォルダーのブックマーク: 任意で、ブックマークフォルダー名を入力します。このフィールドを空白のままにすると、ブックマークはデフォルトのブックマークディレクトリに追加されます。
    * タイトル: Web サイトの説明的なタイトルを入力します。たとえば、`https://google.com`という URL に対して「Google」と入力します。
    * Web サイトを許可リストに保存する場合は ［保存］をクリックし、保存しない場合は ［キャンセル］をクリックします。

プラグインフィルターの種類

- フィルター名: フィルターの固有の名前を入力します。
- 識別子: フィルタリングサービスを提供するプラグインのバンドル ID を入力します。

- サービスアドレス：任意で、サーバーアドレスを入力します。有効な形式は、IP アドレス、ホスト名、または URL です。
- ユーザー名：任意で、サービスのユーザー名を入力します。
- パスワード：任意で、デバイスのパスワードを入力します。
- 証明書：一覧から、任意で、サービスでユーザーを認証するために使用する ID 証明書を選択します。デフォルトは ［なし］です。
- **WebKit** のトラフィックをフィルター： WebKit トラフィックをフィルタリングするかどうかを選択します。
- ソケットトラフィックをフィルター：ソケットトラフィックをフィルタリングするかどうかを選択します。
- カスタムデータ： Web フィルターに追加するカスタムキーごとに、［追加］をクリックして以下の操作を行います。
  - キー：カスタムキーを入力します。
  - 値：カスタムキーの値を入力します。
  - カスタムキーを保存する場合は ［保存］をクリックし、保存しない場合は ［キャンセル］をクリックします。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    - 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    - 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。

Web クリップデバイスポリシー

March 15, 2024

ショートカットや Web クリップを Web サイトに配置してユーザーデバイスのアプリと一緒に表示できます。iOS、iPadOS、macOS、Android デバイスの Web クリップを表す独自のアイコンを指定できます。Windows タブレットは、ラベルおよび URL のみが必要になります。iOS および iPadOS デバイスの場合、ホーム画面レイアウトのデバイスポリシーを構成して、作成した Web クリップを整理します。iOS 上のアプリへのアクセスを制限する場合は、制限デバイスポリシーを構成して Web クリップを許可するようにしてください。これらのポリシーの構成について詳しくは、「ホーム画面のレイアウトに関するデバイスポリシー」および「制限デバイスポリシー」を参照してください。

このポリシーを追加または構成するには、［構成］**>** ［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- ラベル： Web クリップとともに表示するラベルを入力します。
- **URL**： Web クリップに関連付ける URL を入力します。URL はプロトコル（例：`https://server`）で始まる必要があります。
- 削除可能：ユーザーが Web クリップを削除できるかどうかを選択します。デフォルトは ［オフ］です。このオプションは共有 iPad ではサポートされていません。
- 更新するアイコン：［参照］をクリックしてファイルの場所に移動し、Web クリップに使用するアイコンを選択します。
- 画像処理済みアイコン：アイコンにエフェクト（角丸、影付き、反射光）を適用するかどうかを選択します。デフォルトは ［オフ］で、エフェクトが追加されます。
- 全画面：リンクされている Web ページを全画面モードで開くかどうかを選択します。この設定により、iPad が単一の Web サイトのみ開くようにすることもできます。または、アプリのロックデバイスポリシーを使用して、iPad をキオスクモードで実行するように設定することもできます。詳しくは、「iPad をキオスクとして構成する」を参照してください。デフォルトは ［オフ］です。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。
    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。iOS 6.0 以降でのみ使用できます。
  - プロファイル対策：このポリシーを［ユーザー］または［システム］全体に適用するかを選択します。デフォルト値は ［システム］です。iOS 9.3 以降のみで利用できます。

macOS 設定

- ラベル： Web クリップとともに表示するラベルを入力します。
- **URL**： Web クリップに関連付ける URL を入力します。URL はプロトコル（例：`https://server`）で始まる必要があります。
- 更新するアイコン：［参照］をクリックしてファイルの場所に移動し、Web クリップに使用するアイコンを選択します。
- ポリシー設定
  - ポリシーの削除：ポリシーの削除をスケジュール設定する方法を選択します。利用可能なオプションは、［日付を選択］と ［削除までの期間（時間）を指定］です。
    * 日付を選択：カレンダーをクリックして削除を実行する特定の日付を選択します。

    * 削除までの期間（時間）を指定：ポリシーが削除されるまでの時間単位の数値を入力します。
  - ユーザーにポリシーの削除を許可：ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューで ［常に］、［パスコードが必要です］または ［許可しない］を選択します。［パスコードが必要です］を選択する場合、［削除のパスコード］フィールドに入力します

Android の設定

- 規則：このポリシーで Web クリップを追加または削除するかどうかを選択します。デフォルトは［**Add**］です。
- ラベル： Web クリップとともに表示するラベルを入力します。
- **URL**： Web クリップに関連付ける URL を入力します。
- アイコンを定義：アイコンファイルを使用するかどうかを選択します。デフォルトは ［オフ］です。
- アイコンファイル：［アイコンを定義］が ［オン］の場合は、［参照］をクリックしてアイコンファイルの場所に移動し、ファイルを選択します。

Windows デスクトップ**/**タブレットの設定

- 名前： Web クリップとともに表示するラベルを入力します。
- **URL**： Web クリップに関連付ける URL を入力します。

Windows エージェントのデバイスポリシー

November 29, 2023

Windows エージェントのデバイスポリシーを使用して、管理された Windows デスクトップおよびタブレットで PowerShell スクリプトを実行します。Citrix Endpoint Management にエンタープライズアプリケーションとしてアップロードされたスクリプトファイル、およびスクリプトをホストする他のサーバーを指定することができます。エンタープライズアプリケーションの追加については、「アプリケーションの追加」を参照してください。

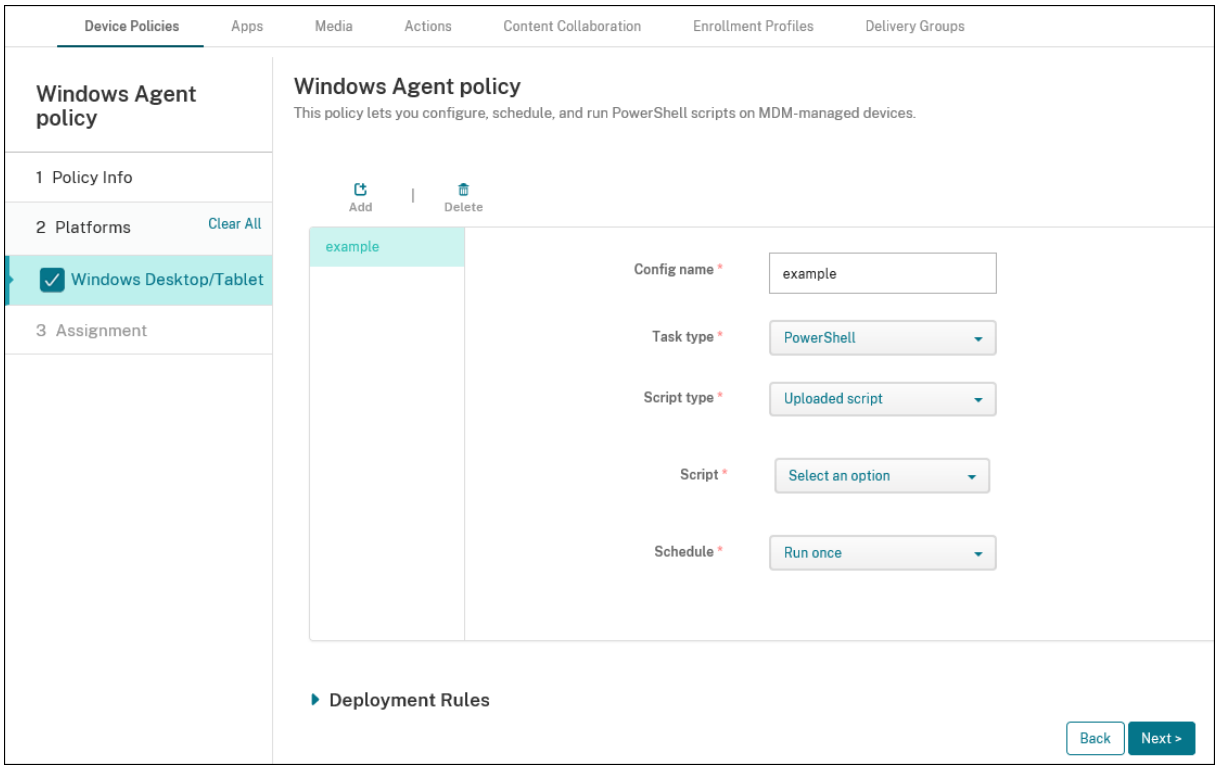
すべてのスクリプトは特権ステータスで実行されるので、スクリプトを管理者として実行する必要はありません。

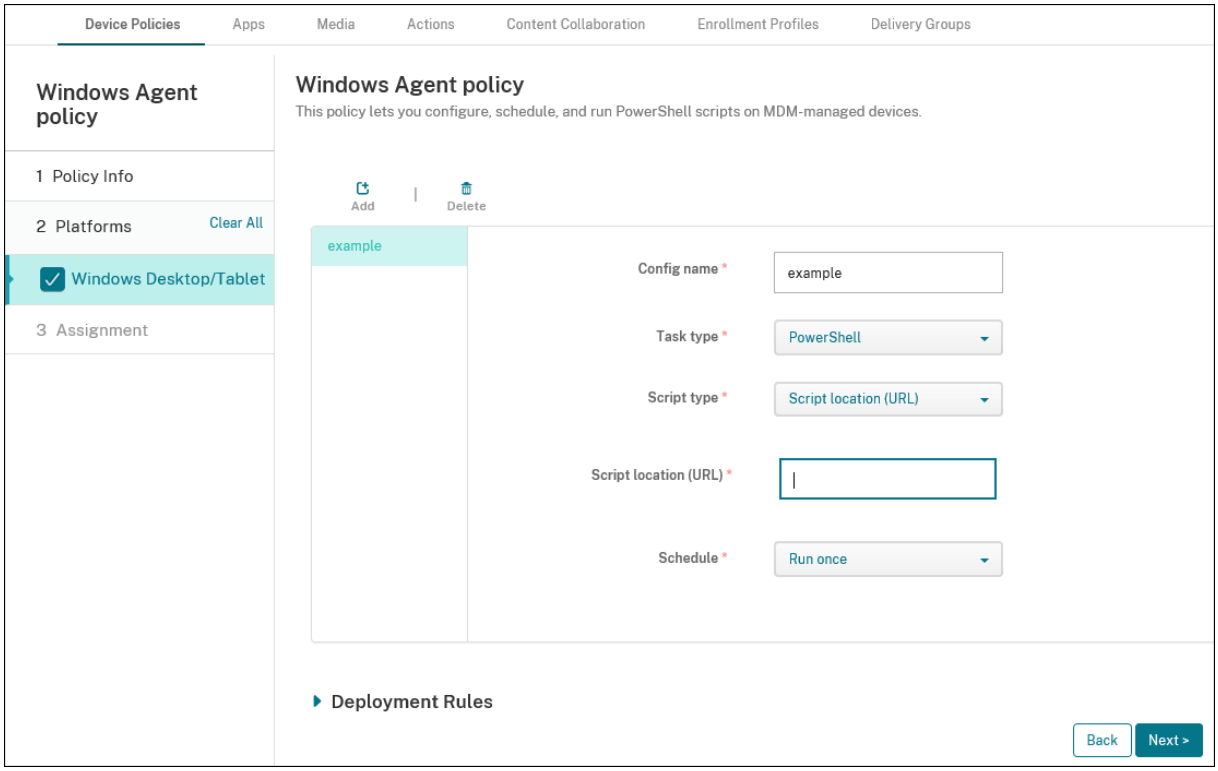
スクリプトを展開して実行した後、スクリプトの結果に基づいて自動化された操作を構成できます。たとえば、レジストリキーを監視するスクリプトを実行すると、結果が返されます。返された結果に基づいて、自動化された操作が実行されます。この操作はアプリへのアクセスを許可または拒否する、デバイスをコンプライアンス違反としてマークする、またはその他の操作を実行します。

msi ファイルと.mst ファイルを指定する PowerShell スクリプトを構成することで、このポリシーを使用してカスタマイズされた MSI インストーラーを展開できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップとタブレットの設定





- 構成名：構成のわかりやすい名前を入力します。

- タスクの種類：［**PowerShell**］を選択します。
- スクリプトの種類： Citrix Endpoint Management サーバーにアップロード済みのスクリプトを指定する場合は ［アップロードされたスクリプト］、外部でホストしているスクリプトを指定する場合は ［スクリプトの場所（**URL**）］を選択します。Citrix Endpoint Management にスクリプトをアップロードする方法について詳しくは、「Win32 アプリをエンタープライズアプリとして追加」を参照してください。
  - スクリプトの選択：［アップロード済みのスクリプト］を選択した場合は、実行するスクリプトを選択します。
  - スクリプトの場所（**URL**）：［スクリプトの場所（**URL**）］を選択した場合は、実行するスクリプトがある場所を入力します。この URL では、スクリプトがペイロードとして配信される必要があります。Citrix Endpoint Management では、スクリプトを JavaScript ダウンロードとして配信する URL はサポートされません。また、スクリプトは公開されたものでなければなりません。
- スケジュール：［**1** 回実行する］を選択して選択されたスクリプトを 1 回のみ実行するか、または ［定期的に実行する］を選択してスクリプトを定期的に実行します。
  - 実行間隔（時間）：スクリプトの実行間隔を時間数で入力します。

スクリプトの状態を確認するには、コンソールで ［管理］**>**［デバイス］に移動します。スクリプトの状態を確認するデバイスを選択し、［編集］をクリックします。［プロパティ］で、［**Windows** エージェント］の下にある ［ダウンロード］をクリックすると、スクリプトの状態を確認できます。

自動化された操作をトリガーする **PowerShell** スクリプトの展開

1. PowerShell スクリプトを作成して、レジストリキーを監視します。以下の PowerShell スクリプトは、ファイアウォールが有効になっているかを確認します。

```
$body = @{
  }

$firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
   CurrentControlSet\Services\SharedAccess\Parameters\
   FirewallPolicy\StandardProfile -Name EnableFirewall
if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"
 }
  else {

$body["firewallEnabled"]="false"
 }

$body | ConvertTo-Json -Depth 10
<!--NeedCopy-->
```

   このスクリプトは、次のいずれかの値を返します。


```
{

    "firewallEnabled":  "true"
 }

<!--NeedCopy-->
```

または

```
{

    "firewallEnabled":  "false"
 }

<!--NeedCopy-->
```

2. スクリプトをエンタープライズアプリとして Citrix Endpoint Management コンソールにアップロードする、またはアクセス可能な URL でスクリプトをホストします。
3. ここでの説明に従って、Windows エージェントのデバイスポリシーを構成します。スクリプトがすぐに実行されるようにスケジュールされていることを確認します。
4. スクリプトの実行後、スクリプトの状態を確認します。

   a) コンソールで、［監理］**>**［デバイス］に移動します。
   b) スクリプトの状態を確認するデバイスを選択し、［編集］をクリックします。
   c) ［**Windows** エージェント］の項目の下にある ［ダウンロード］をクリックします。

5. 受信した状態に基づいて自動化された操作を構成します。自動化された操作の構成について詳しくは、「Windows エージェントのデバイスポリシーの結果を使用した自動化された操作の作成」を参照してください。このセクションには、スクリプト例で作成された特定の自動化された操作と Windows エージェントのデバイスポリシーが記載されています。

Windows GPO の構成デバイスポリシー

November 29, 2023

Windows GPO の構成デバイスポリシーでは次のことが可能です:

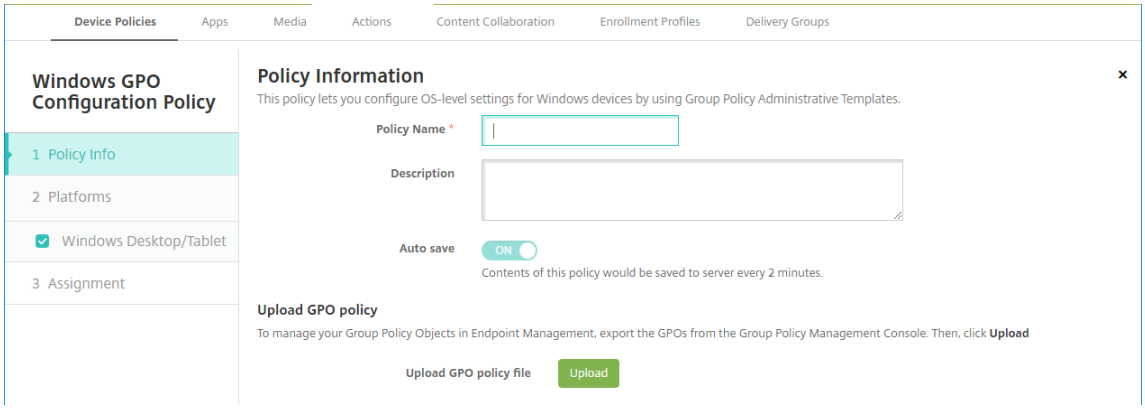
- Citrix Endpoint Management コンソールを使用してグループポリシーオブジェクト（GPO）をインポートし、それを Windows 10 および Windows 11 デバイスに展開する。
- Citrix Workspace Environment Management でサポートされているすべての Windows デバイスで GPO を構成する。
- デバイスおよびユーザーレベルで GPO を構成する。

Windows 10 および **Windows 11** デバイスに展開する **GPO** のインポート

グループポリシー管理コンソールを使用して GPO を管理する際、AD 管理者に頼ることなく、Citrix Endpoint Management コンソールから GPO をインポートして展開できます。

Citrix Endpoint Management で GPO のバックアップを作成するには:

1. AD 管理者にグループポリシー管理コンソールから GPO をエクスポートし、ファイルを提供するよう依頼してください。
2. Citrix Endpoint Management コンソールで、［構成］**>**［デバイスポリシー］に移動し、**Windows GPO** の構成 ポリシーを作成します。
3. ［アップロード］をクリックしてファイルを見つけ、［開く］をクリックしてファイルをインポートします。



GPO の設定については、「Windows デスクトップとタブレットの設定」を参照してください。

Citrix Workspace Environment Management に展開する **GPO** の構成

Windows GPO の構成デバイスポリシーを使用すると、Citrix Workspace Environment Management（WEM）でサポートされているすべての Windows デバイスで GPO を構成できます。Citrix Endpoint Management はポリシーを Citrix WEM サービスにプッシュします。次に WEM サービスは、デバイスにインストールされている WEM エージェントを使用して GPO をデバイスとそのアプリに適用します。

Workspace Environment Management エージェントのインストールについて詳しくは、「インストールと構成」を参照してください。

このポリシーでは、すべての Windows OS ADMX ファイルが使用されます。サードパーティ ADMX ファイルをアップロードする場合は、アプリ構成デバイスポリシーを使用します。サードパーティ ADMX ファイルのアップロードについて詳しくは、「アプリケーション構成デバイスポリシー」を参照してください。

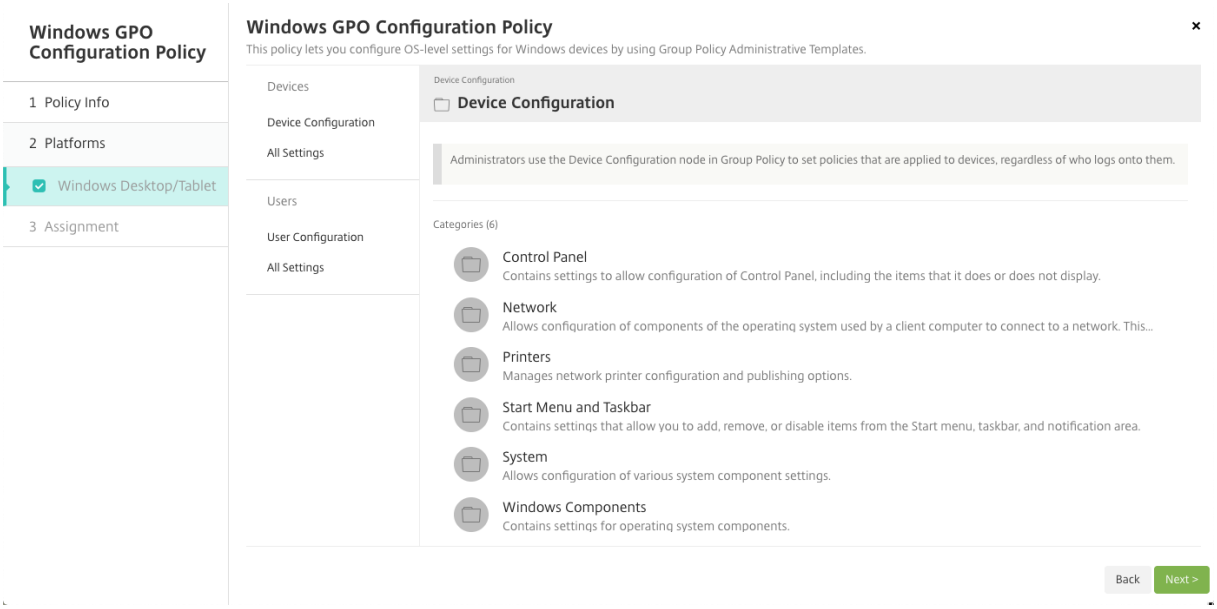
- Citrix Endpoint Management がネイティブでサポートしていないデバイスであっても、WEM がサポートするすべてのデバイスに GPO の構成をプッシュできます。サポートされているデバイスの一覧については、「オペレーティングシステムの要件」を参照してください。

- このポリシーでは、デバイスに WEM エージェントがインストールされ構成されている必要があります。デバイスを MDM または MAM に登録する必要はありません。
- Citrix Endpoint Management は WEM チャネル経由で GPO 設定をプッシュします。（Microsoft は、MDM チャネル経由でのデバイスレベル設定のプッシュをサポートしません）。Windows GPO の構成デバイスポリシーを受信するデバイスは、Citrix Endpoint Management の WEM と呼ばれるモードで動作します。登録済みデバイスの ［管理］**>**［デバイス］一覧で WEM 管理対象デバイスの ［モード］列に **WEM** が表示されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップとタブレットの設定

このポリシーでは、デバイスおよびユーザーレベルで GPO を構成できます。



Windows デバイスに展開する Windows GPO を選択して構成します。［デバイス構成］および ［ユーザー構成］は変更できます。ポリシーはツリー構造で表示されます。すべての設定を表示するには、［すべての設定］を選択します。設定について詳しくは、Microsoft 社サイトから GPO リファレンスシートをダウンロードしてください。

設定を構成するには、最初に設定を有効にします。構成中、Citrix Endpoint Management は変更を自動的に保存して、これらの設定を保持します。設定を保存する前にページを終了しようとすると、未保存の変更があることを示すポップアップメッセージが開きます。

設定に 2 つのオプションがある場合は、選択用のラジオボタンが表示されます。3 つ以上のオプションがあると、メニューが表示されます。

> 注:
>
> 構成した設定を確認する必要がある場合は、次の操作を実行できます。
>
> 1. Citrix Endpoint Management コンソールで、編集する **Windows GPO** の構成 ポリシーを開きます。
> 2. ［デバイス］または ［ユーザー］で ［すべての設定］を選択します。
> 3. 表を ［状態］で昇順に並べ替えます。未構成のすべてのポリシーの状態は、［未構成］と表示されます。構成したポリシーは上部に表示されます。

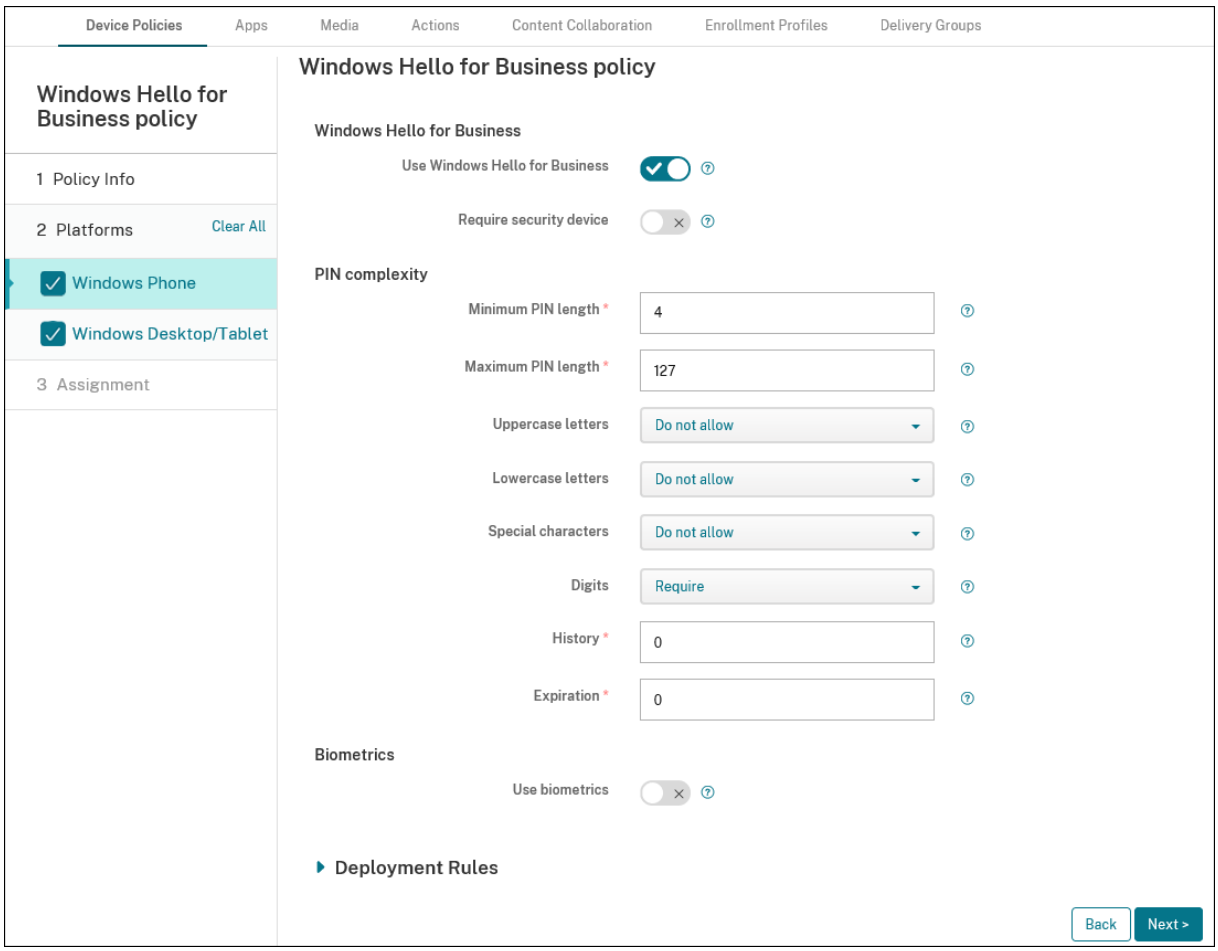
Windows Hello for Business デバイスポリシー

February 16, 2022

Windows Hello for Business では、ユーザーは Active Directory または Azure Active Directory のアカウントを使用して Windows デバイスにサインオンできます。この機能を有効にしてユーザーがデバイスへ Windows Hello for Business のプロビジョニングできるようにするには、Windows Hello for Business デバイスポリシーを使用します。このポリシーでは、パスコードの制限などのセキュリティ機能を構成することもできます。

Windows Hello for Business ポリシーを追加するには、［構成］**>** ［デバイスポリシー］の順に選択します。次の設定を構成します:

Windows デスクトップ/タブレットの設定



- **Windows Hello for Business** の使用：この機能を有効にしてユーザーがデバイスに Windows Hello for Business をプロビジョニングできるようにするかどうかを指定します。
- セキュリティデバイスが必要です：サインオンにトラステッドプラットフォームモジュール（Trusted Platform Module：TPM）を必須にするかどうかを指定します。
- ［最小 **PIN** 長］/［最大 **PIN** 長］：ユーザー PIN の最小長および最大長。［最小 **PIN** 長］のデフォルト値は **4** です。［最大 **PIN** 長］のデフォルト値は **127** です。
- ［大文字］、［小文字］、［特殊文字］：各種類の文字について、［許可］、［必須］、または ［許可しない］のいずれかを選択します。デフォルトは ［許可しない］です。
- 数字：数字について［許可］、［必須］、［許可しない］のいずれかを選択します。デフォルトは ［必須］です。
- 履歴：ユーザーに再利用を禁止する過去の PIN の数。デフォルト値は **0** であり、ユーザーはすべての PIN を再利用できます。
- 有効期限： PIN の変更が必要になるまでの日数。デフォルト値は **0** であり、PIN に有効期限はありません。
- 生体認証を使用する：ユーザーのサインインで PIN の代わりに生体認証の使用を許可するかどうかを指定します。

アプリの追加

March 15, 2024

Citrix Endpoint Management にアプリを追加すると、モバイルアプリケーション管理（MAM：Mobile Application Management）機能が提供されます。Citrix Endpoint Management はアプリケーション配信、ソフトウェアライセンス、構成、アプリケーションライフサイクル管理を支援します。

MDX 対応アプリは、一部の種類のアプリをユーザーデバイスに配布する準備をする上で重要な部分です。MDX の概要については、「Citrix Endpoint Management コンポーネント」と「MAM SDK の概要」を参照してください。

- MDX 対応アプリには MAM SDK を使用することをお勧めします。または、MDX Toolkit が廃止されるまで、アプリを MDX ラップし続けることができます。「廃止」を参照してください。
- MDX Toolkit を使用して Citrix 業務用モバイルアプリをラップすることはできません。業務用モバイルアプリの MDX ファイルは、Citrix のダウンロードから入手します。

Citrix Endpoint Management コンソールにアプリを追加すると、次のことが可能になります：

- アプリ設定を構成する
- Citrix Secure Hub でアプリをカテゴリに分類して編成する（オプション）
- ユーザーにアプリへのアクセスを許可する前に承認を必要とするワークフローを定義する（オプション）
- アプリをユーザーに展開する

この記事では、アプリを追加するための一般的なワークフローについて説明します。各プラットフォームについて詳しくは、次の記事を参照してください：

- Android Enterprise アプリの配布
- Apple アプリの配布

> 重要：
>
> Citrix Endpoint Management は、最大 300 個のアプリの追加と維持に対応しています。この制限を超えると、システムが不安定になります。

アプリの種類と機能

次の表は、Citrix Endpoint Management で展開できるアプリの種類をまとめたものです。

アプリの種類	ソース	メモ	参照
MDX	ユーザー向けに開発した iOS および Android アプリ。Citrix 業務用モバイルアプリ。	iOS または Android アプリは、MAM SDK を使用して開発するか、MDX Toolkit でラップします。業務用モバイルアプリの場合は、Citrix ダウンロードページからパブリックストア MDX ファイルをダウンロードします。その後で、アプリを Citrix Endpoint Management に追加します。	MDX アプリケーションの追加
パブリックアプリストア	Google Play や Apple App Store などの公開アプリストアからの無料または有料のアプリ。	アプリをアップロードし、アプリを MDX 対応にしてから、Citrix Endpoint Management に追加します。	パブリックアプリストアのアプリの追加
Web および SaaS	内部ネットワーク（Web アプリ）またはパブリックネットワーク（SaaS）。	Citrix Endpoint Management は、MDM に登録されている iOS および Android デバイスからネイティブ SaaS アプリへのモバイルシングルサインオンを提供します。または、セキュリティアサーションマークアップランゲージ（SAML）アプリケーションコネクタを使用します	Web または SaaS アプリの追加
Enterprise	Win32 アプリなどの MDX に対応していないプライベートアプリ。MDX 対応のプライベート Android Enterprise アプリ。Enterprise アプリは、CDN 内または Citrix Endpoint Management サーバー内にあります。	アプリを Citrix Endpoint Management に追加します。	エンタープライズアプリの追加

アプリの種類	ソース	メモ	参照
Web リンク	シングルサインオンを必要としないインターネット Web アドレス、イントラネット Web アドレス、または Web アプリ。	Web リンクは Citrix Endpoint Management で構成します。	Web リンクの追加

アプリの配布を計画するときは、次の機能を考慮してください:

- サイレントインストールについて
- 必須アプリと任意アプリについて
- アプリのカテゴリについて
- Citrix CDN によるエンタープライズアプリの配信
- Microsoft 365 アプリの有効化
- ワークフローの適用
- アプリストアおよび Citrix Secure Hub のブランド設定
- アプリストア経由の Citrix Virtual Apps and Desktops

サイレントインストールについて

Citrix では、iOS、Android Enterprise、Samsung のアプリのサイレントインストールおよびアップグレードをサポートします。サイレントインストールとは、ユーザーはデバイスに展開するアプリのインストールを求められないことを意味します。アプリはバックグラウンドで自動的にインストールされます。

サイレントインストールを実装する前提条件

- iOS の場合、管理されている iOS デバイスを監視モードにします。詳しくは、「iOS および macOS プロファイルのインポートデバイスポリシー」を参照してください。
- Android Enterprise の場合、アプリはデバイスに仕事用プロファイルでインストールされます。詳しくは、「Android Enterprise」を参照してください。
- Samsung デバイスの場合、デバイスで Samsung Knox を有効にします。

  このためには、Samsung MDM ライセンスキーデバイスポリシーを設定して、Samsung ELM および Knox ライセンスアクセスコードを生成します。詳しくは、「Samsung MDM ライセンスキーデバイスポリシー」を参照してください。

必須アプリと任意アプリについて

デリバリーグループにアプリを追加するときに、アプリが任意か必須かを選択します。アプリを必須として展開することをお勧めします。

- 必須アプリはユーザーのデバイスにサイレントモードでインストールされるため、操作を最小限に抑えることができます。この機能を有効にすると、アプリの自動更新も有効になります。
- 任意アプリでは、ユーザーがインストールするアプリを選択できますが、Citrix Secure Hub で手動でインストールを開始する必要があります。

必須とマーク付けされたアプリについては、次のような場合に、ユーザーはすみやかに更新プログラムを受信できます:

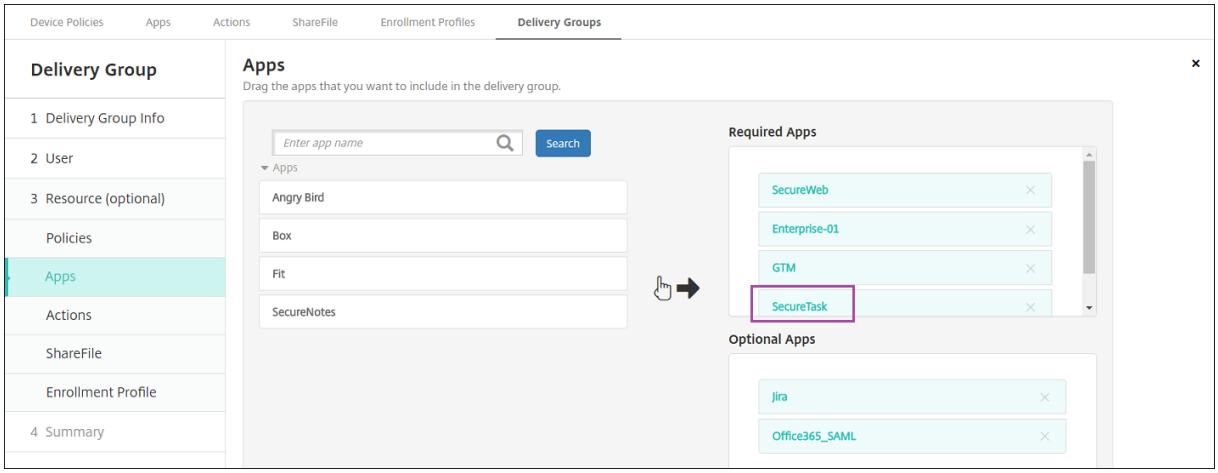
- アップロードした新しいアプリを必須アプリとしてマーク付けした場合。
- 既存のアプリを必須アプリとしてマーク付けした場合。
- 必須アプリをユーザーが削除した場合。
- Citrix Secure Hub の更新が利用可能な場合。

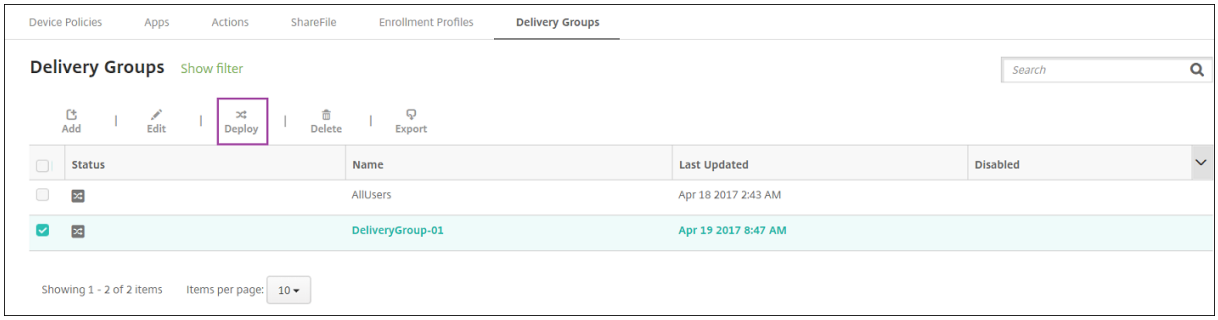
必須アプリを強制展開するための要件

- Citrix Secure Hub: iOS で 10.5.15、Android で 10.5.20（最小バージョン）
- MAM SDK または MDX Toolkit 10.6（最小バージョン）
- Citrix Endpoint Management と Citrix Secure Hub のアップグレード後: 登録済みデバイスを使用するユーザーは、Citrix Secure Hub からサインオフして再びサインオンし、必須アプリの展開の更新プログラムを取得する必要があります。

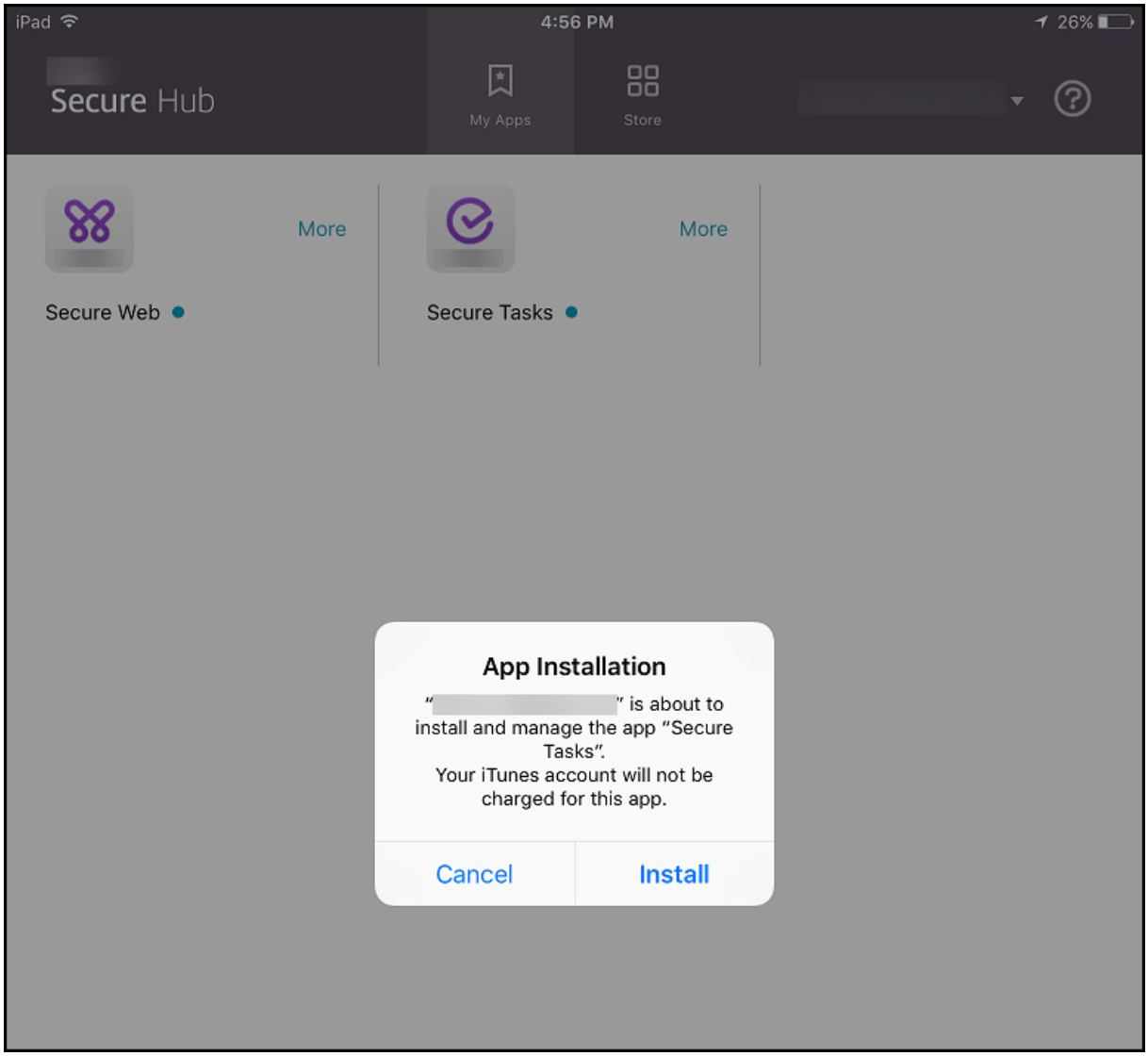
例

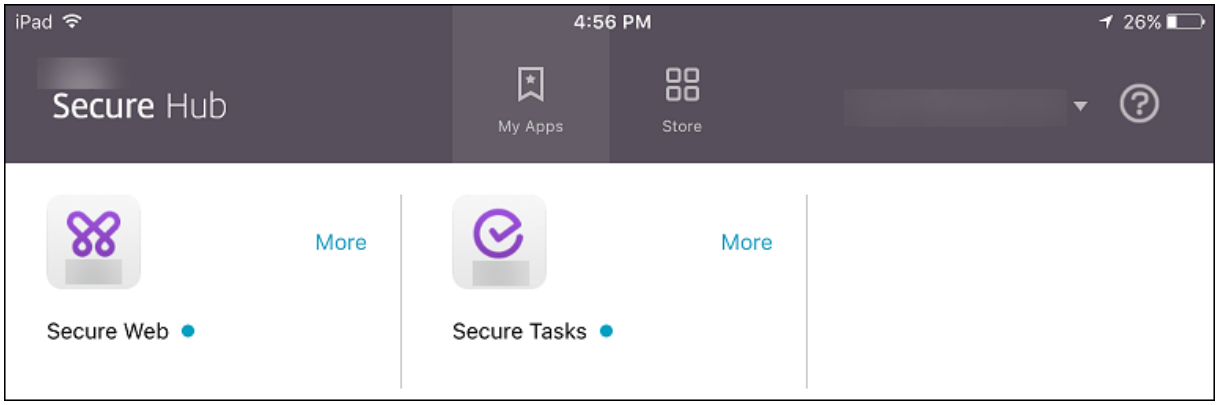
次の例で、アプリケーション名の Secure Tasks をデリバリーグループに追加し、そのデリバリーグループを展開する流れを示します。





サンプルアプリである Citrix Secure Tasks をユーザーデバイスに展開すると、Citrix Secure Hub によってアプリのインストールを求めるプロンプトがユーザーに表示されます。





> 重要:
>
> エンタープライズアプリやパブリックアプリストアのアプリなどの MDX 対応の必須アプリは、即時アップグレードされます。アップグレードは、アプリの更新猶予期間の MDX ポリシーを構成し、ユーザーが後でアプリをアップグレードすることを選択した場合でも発生します。

iOS 必須アプリのワークフロー（エンタープライズアプリおよびパブリックストアアプリの場合）

1. 初回登録時に Citrix 業務用モバイルアプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Management コンソールでアプリを更新します。
3. Citrix Endpoint Management コンソールを使用して、必須アプリを展開します。
4. ホーム画面のアプリが更新されます。また、パブリックストアアプリの場合は、アップグレードが自動的に開始されます。ユーザーに更新のメッセージは表示されません。
5. ユーザーはホーム画面からアプリを開きます。アプリ更新の猶予期間が設定済みで、後でアプリをアップグレードするようにユーザーが選択した場合でも、アプリは直ちにアップグレードされます。

Android 必須アプリのワークフロー（エンタープライズアプリの場合）

1. 初回登録時に Citrix 業務用モバイルアプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Management コンソールを使用して、必須アプリを展開します。
3. アプリがアップグレードします。（Nexus デバイスでは更新プログラムのインストールを求めるメッセージが表示されますが、Samsung デバイスではサイレントインストールが行われます。）
4. ユーザーはホーム画面からアプリを開きます。アプリ更新の猶予期間が設定済みで、後でアプリをアップグレードするようにユーザーが選択した場合でも、アプリは直ちにアップグレードされます。（Samsung デバイスではサイレントインストールが行われます。）

Android 必須アプリのワークフロー（パブリックストアアプリの場合）

1. 初回登録時に Citrix 業務用モバイルアプリを展開します。必須アプリがデバイスにインストールされます。
2. Citrix Endpoint Management コンソールでアプリを更新します。

3. Citrix Endpoint Management コンソールを使用して、必須アプリを展開します。または、デバイス上で Citrix Secure Hub ストアを開きます。アップデートアイコンがストアに表示されます。
4. 自動的にアプリのアップグレードが始まります。(Nexus デバイスにより、更新プログラムのインストールがユーザーに促されます。)
5. ホーム画面でアプリを開きます。アプリがアップグレードします。猶予期間に関するメッセージはユーザーに表示されません。(Samsung デバイスではサイレントインストールが行われます。)

必須アプリとして構成されているアプリのアンインストール

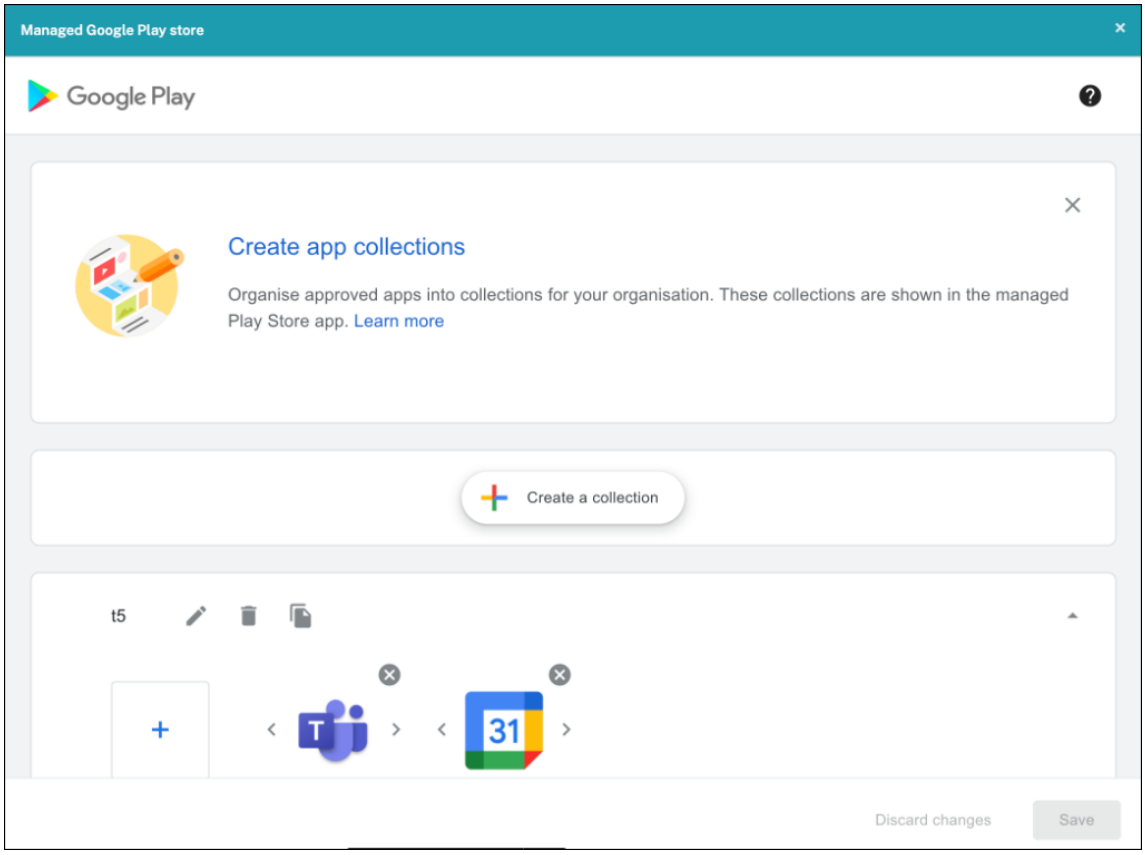
ユーザーに、必須アプリとして構成されているアプリのアンインストールを許可できます。[構成] **>** [デリバリーグループ] で対象アプリを [必須アプリ] から [任意アプリ] に移動します。

推奨: この目的のためのデリバリーグループでアプリを一時的に任意に変更して、特定のユーザーがアプリをアンインストールできるようにします。既存の必須アプリを任意に変更し、このアプリをこのデリバリーグループに展開し、これらのデバイスからアプリをアンインストールできます。今後、このデリバリーグループで必須アプリを登録する場合は、アプリの設定を必須に戻すことができます。

アプリの整理 (**Android Enterprise**)

ユーザーが Citrix Secure Hub にログオンすると、Citrix Endpoint Management で設定済みのアプリ、Web リンク、ストアの一覧が表示されます。Android Enterprise では、これらのアプリをコレクションに整理して、ユーザーが特定のアプリ、ストア、または Web リンクにのみアクセスできるようにすることができます。たとえば、「Finance」コレクションを作成して財務関連にのみ関係するアプリを追加したり、「Sales」コレクションを構成して営業関連のアプリを追加したりすることができます。

1. Citrix Endpoint Management コンソールで、[構成] **>** [アプリ] **>** [アプリの整理] の順にクリックします。[管理対象 **Google Play** ストア] ウィンドウが表示されます。



2. ［コレクションの作成］をクリックして、そのコレクションに追加するアプリを選択します。
3. コレクションの追加が完了したら、［保存］をクリックします。

> 注:
>
> IT 管理者は、アプリを［管理対象 Google Play］ウィンドウのコレクションに追加する前に承認する必要があります。IT 管理者は、https://play.google.com/workに移動してアプリを承認できます。将来のリリースでは、コレクションに追加する前にアプリを承認する必要はなくなります。

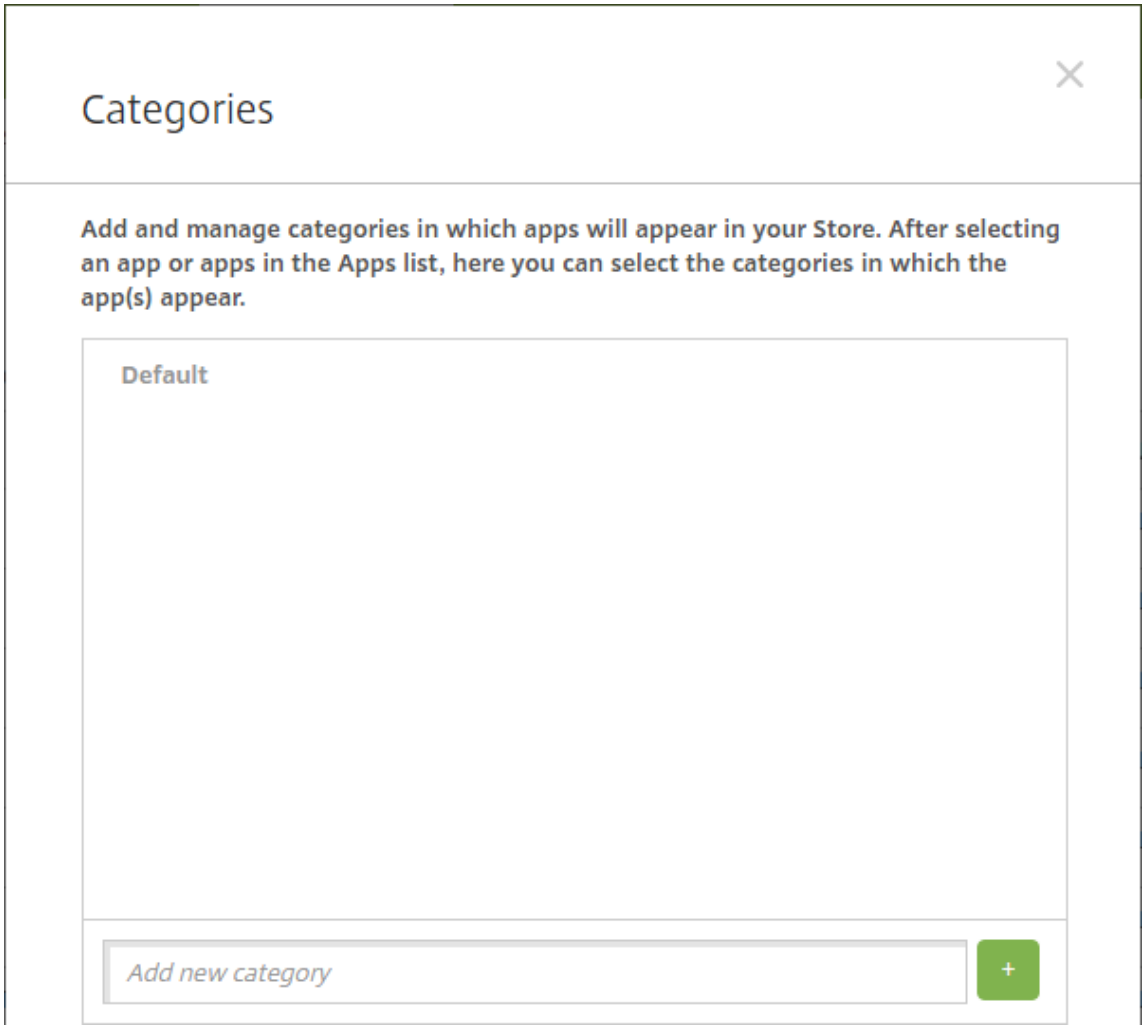
アプリのカテゴリについて（**iOS** および **MDX**）

ユーザーが Citrix Secure Hub にログオンすると、Citrix Endpoint Management で設定済みのアプリ、Web リンク、ストアの一覧が表示されます。iOS や MDX では、管理者がアプリカテゴリを使用することにより、ユーザーは指定されたアプリ、ストア、または Web リンクだけにアクセスできます。たとえば、「Finance」カテゴリを作成して財務関連のアプリを追加したり、「Sales」カテゴリを構成して営業関連のアプリを追加したりすることができます。

アプリ、Web リンク、ストアを追加または編集するとき、構成した 1 つまたは複数のカテゴリにアプリを追加できます。

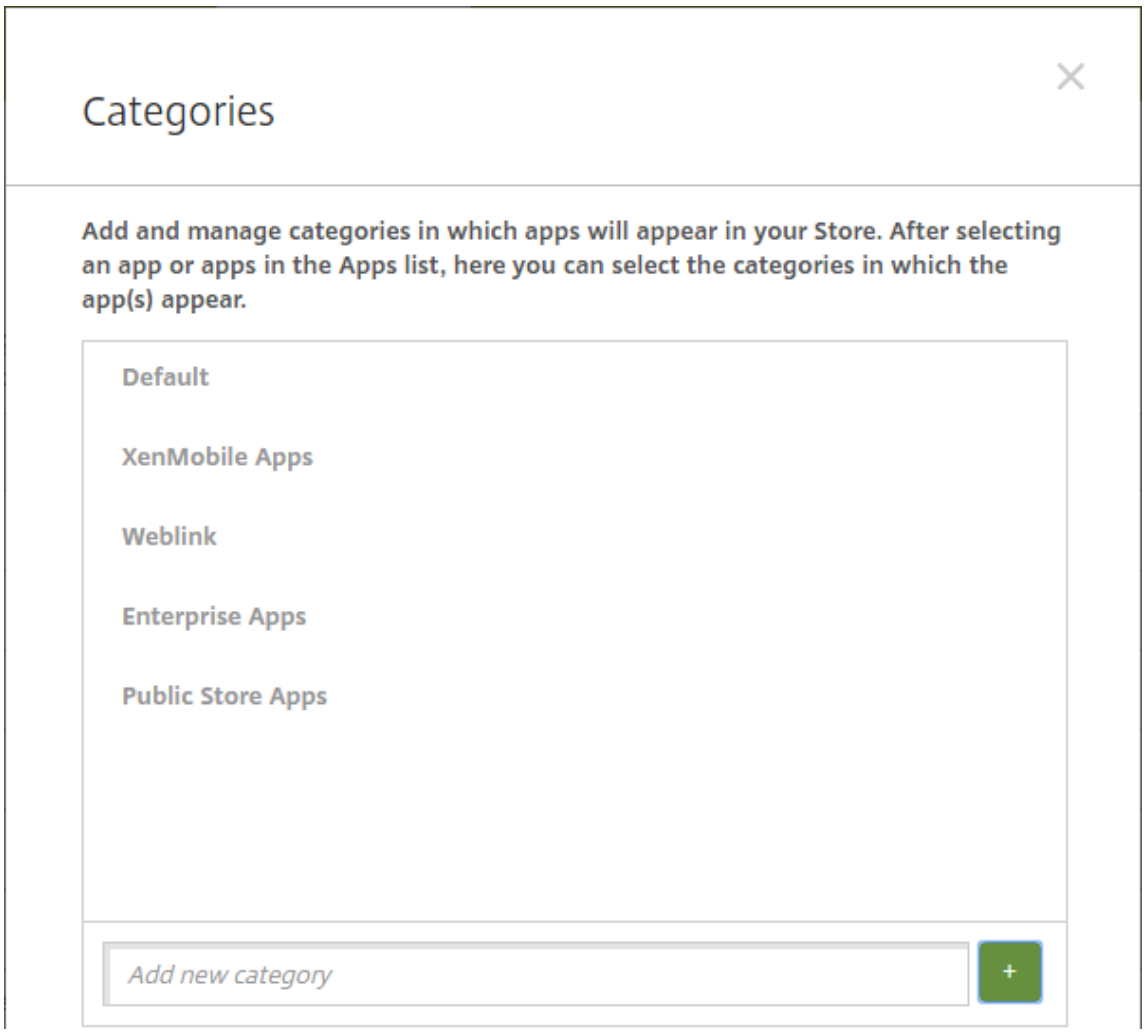
1. Citrix Endpoint Management コンソールで、［構成］**>** ［アプリ］**>** ［カテゴリ］の順にクリックします。［カ

テゴリ］ダイアログボックスが開きます。



2. 追加するカテゴリごとに、以下の操作を行います：

   - ダイアログボックス下部にある ［新しいカテゴリの追加］フィールドに、追加するカテゴリの名前を入力します。たとえば、「Enterprise Apps」と入力して、エンタープライズアプリのカテゴリを作成することができます。
   - プラス記号（+）をクリックしてカテゴリを追加します。新しく作成したカテゴリが追加され、［カテゴリ］ダイアログボックスに表示されます。



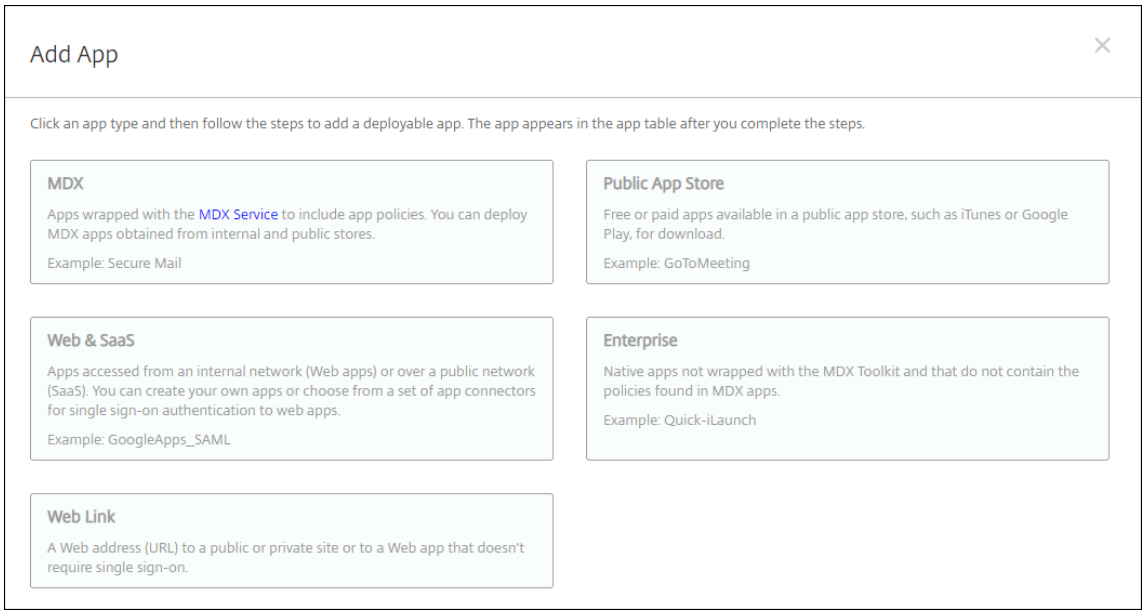
3. カテゴリの追加が終了したら、［カテゴリ］ダイアログボックスを閉じます。
4. ［アプリ］ページで、既存のアプリを新しいカテゴリに分類できます。
   - 分類するアプリを選択します。
   - ［編集］をクリックします。［アプリ情報］ページが開きます。
   - ［アプリカテゴリ］の一覧で、新しいカテゴリのチェックボックスをオンにしてカテゴリを適用します。既存のカテゴリでアプリに適用しないものについては、チェックボックスをオフにします。
   - ［デリバリーグループ割り当て］タブをクリックするか、後続の各ページで ［次へ］をクリックして、残りのアプリセットアップページに示される手順に従います。
   - ［デリバリーグループ割り当て］のページの ［保存］をクリックして新しいカテゴリを適用します。新しいカテゴリがアプリに適用され、［アプリ］の表に表示されます。

MDX アプリケーションの追加

iOS アプリまたは Android アプリ用の MDX ファイルを受け取ったら、そのアプリを Citrix Endpoint Management にアップロードできます。アプリをアップロードした後、アプリの詳細とポリシー設定を構成できます。各デバイスプラットフォームの種類で使用できるアプリポリシーについて詳しくは、以下を参照してください:

- MAM SDK の概要
- MDX ポリシーの概要

1. Citrix 業務用モバイルアプリの場合は、パブリックストア MDX ファイルをダウンロードします。https://www.citrix.com/downloadsに移動します。**Citrix Endpoint Management**（**XenMobile**）、**Citrix Endpoint Management Productivity Apps** の順に移動します。
2. 他の種類の MDX アプリについては、MDX ファイルを入手します。
3. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］**>**［追加］の順にクリックします。［アプリの追加］ダイアログボックスが開きます。

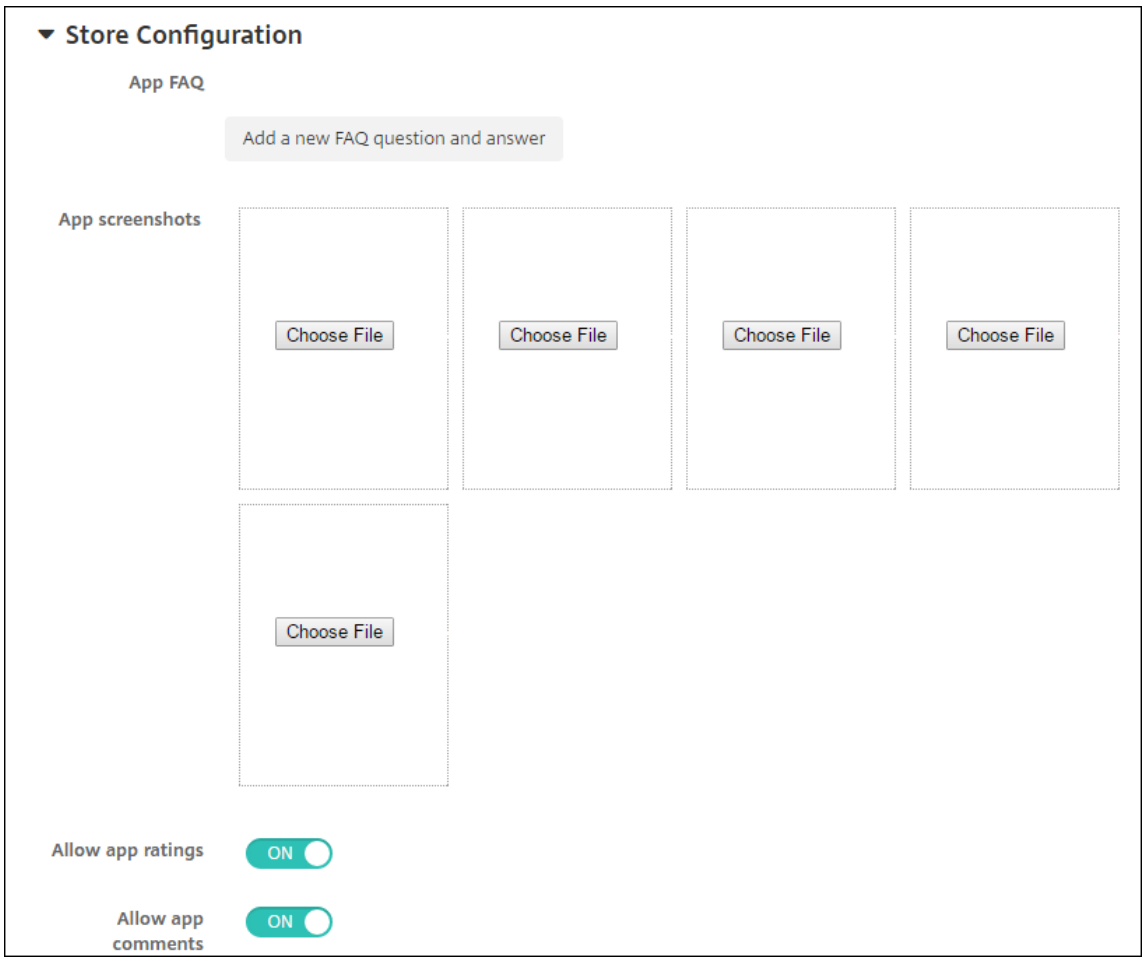


4. ［**MDX**］をクリックします。［**MDX** アプリ情報］ページが開きます。
5. ［アプリ情報］ペインで、以下の情報を入力します:
   - 名前: アプリを説明する名前を入力します。この名前は、［アプリ］テーブルの ［アプリ名］の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。
   - アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリのカテゴリについて」を参照してください。
6. ［次へ］をクリックします。アプリのプラットフォームページが開きます。

7. ［プラットフォーム］で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。
8. ［アップロード］をクリックしてアップロードする MDX ファイルの場所へ移動し、そのファイルを選択します。
9. ［アプリの詳細］ページで、次の設定を構成します：

    - ファイル名：アプリに関連付けられているファイル名を入力します。
    - アプリの説明：アプリの説明を入力します。
    - アプリのバージョン：任意で、アプリのバージョン番号を入力します。
    - パッケージ **ID**：管理対象 Google Play ストアから取得したアプリのパッケージ ID を入力します。
    - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
    - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
    - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
    - **MDM** プロファイルが削除されたらアプリを削除します： MDM プロファイルが削除された場合に iOS デバイスからアプリを削除するかどうかを選択します。デフォルトは ［オン］です。
    - アプリデータのバックアップを阻止します：ユーザーが iOS デバイスのアプリデータをバックアップできないようにするかどうかを選択します。デフォルトは ［オン］です。
    - 製品トラック： iOS デバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、そのトラックを選択してユーザーに割り当てることができます。デフォルトは［実稼働］です。
    - 管理されるアプリ：アプリが非管理対象としてインストールされたときに、ユーザーに監視対象ではない iOS デバイスでのアプリの管理を許可するように求めるかどうかを選択します。デフォルトは ［オン］です。
    - 一括購入経由で展開されたアプリ： Apple の一括購入を使用してアプリを展開するかどうかを選択します。これが ［オン］で、MDX バージョンのアプリを展開し、アプリの展開に一括購入を使用する場合、Citrix Secure Hub では一括購入インスタンスのみが表示されます。デフォルトは ［オフ］です。

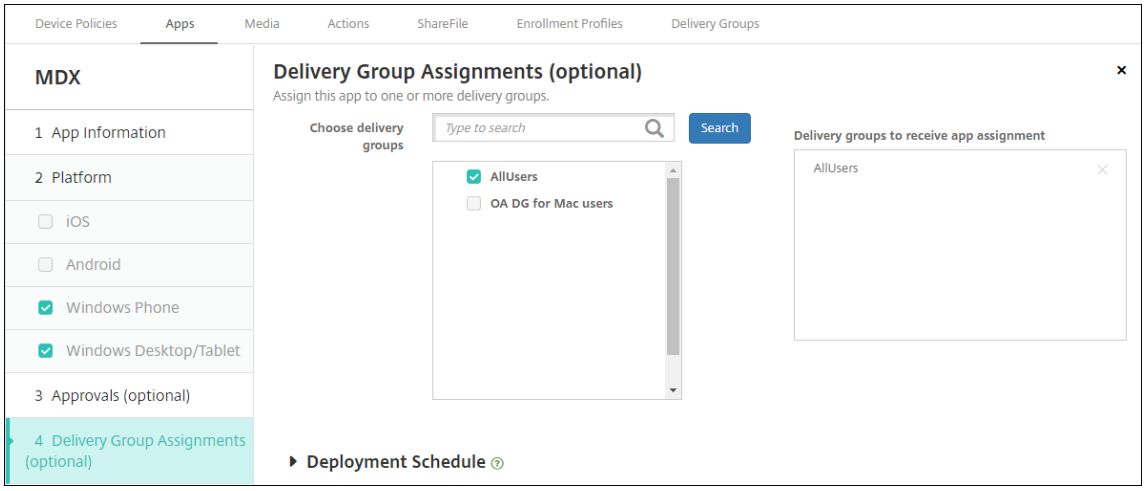
10. **MDX** ポリシーを構成します。MDX ポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域で適用するオプションが含まれます。コンソールでは、ポリシーごとに、ポリシーを説明するヒントが提供されます。
11. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。
12. ［ストア構成］を展開します。



オプションで、以下を構成できます:

- アプリの **FAQ**:［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加:アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可:ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可:ユーザーがアプリストアのアプリにコメントを残すことを許可します。

13.［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。



14. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

15. ［展開スケジュール］を展開して以下の設定を構成します：

    - 展開：アプリをデバイスに展開するかどうかを選択します。デフォルトは ［オン］です。
    - 展開スケジュール：アプリを ［すぐに］展開するか、［後で］展開するかを選択します。［後で］を選択した場合は、アプリを展開する日時を設定します。デフォルトは ［すぐに］です。
    - 展開条件：［すべての接続で］を選択すると、デバイスが接続するたびにアプリを展開します。［以前の展開が失敗した場合のみ］を選択すると、以前にデバイスがアプリを受信できなかった場合にアプリを展開します。デフォルトは ［すべての接続で］です。

    ［常時接続に対する展開］オプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

    常時接続オプション：

    - iOS デバイスでは使用できません。
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

    構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

16. ［保存］をクリックします。

パブリックアプリストアのアプリの追加

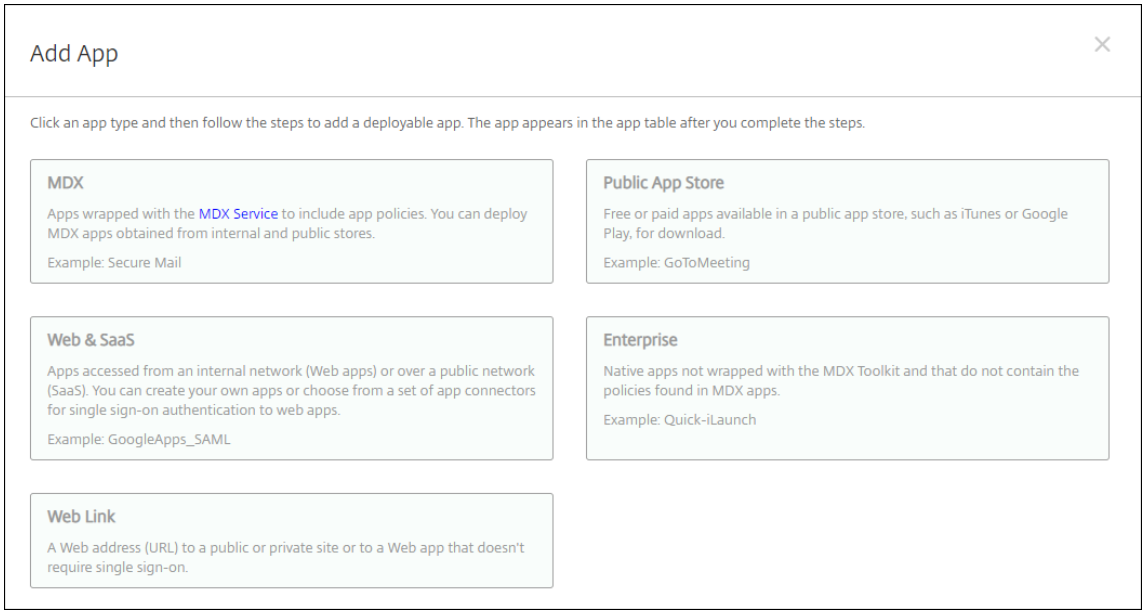
Apple App Store や Google Play などのパブリックアプリストアで配布されている無料アプリや有料アプリを、Citrix Endpoint Management に追加できます。

Apple App Store からアプリの名前と説明を取得するための設定を構成できます。ストアからアプリ情報を取得すると、Citrix Endpoint Management により既存の名前と説明が上書きされます。Google Play ストアのアプリ情報は手動で構成する必要があります。

Android Enterprise 用のパブリックアプリストアの有料アプリを追加する場合、一括購入ライセンスの状態を確認できます。状態に含まれる情報は、使用できる合計ライセンス数、使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレスです。Android Enterprise の一括購入プランを利用すると、組織のアプリやその他のデータの検索、購入、配布の処理が簡単になります。

アプリ情報を構成し、アプリを配信するプラットフォームを選択します:

1. Citrix Endpoint Management コンソールで、[構成] > [アプリ] > [追加] の順にクリックします。[アプリの追加] ダイアログボックスが開きます。



2. [パブリックアプリストア] をクリックします。[アプリ情報] ページが開きます。
3. [アプリ情報] ペインで、以下の情報を入力します:
   - 名前: アプリの説明的な名前を入力します。この名前は、[アプリ] の表の [アプリ名] の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。
   - アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリのカテゴリについて」を参照してください。
4. [次へ] をクリックします。アプリのプラットフォームページが開きます。

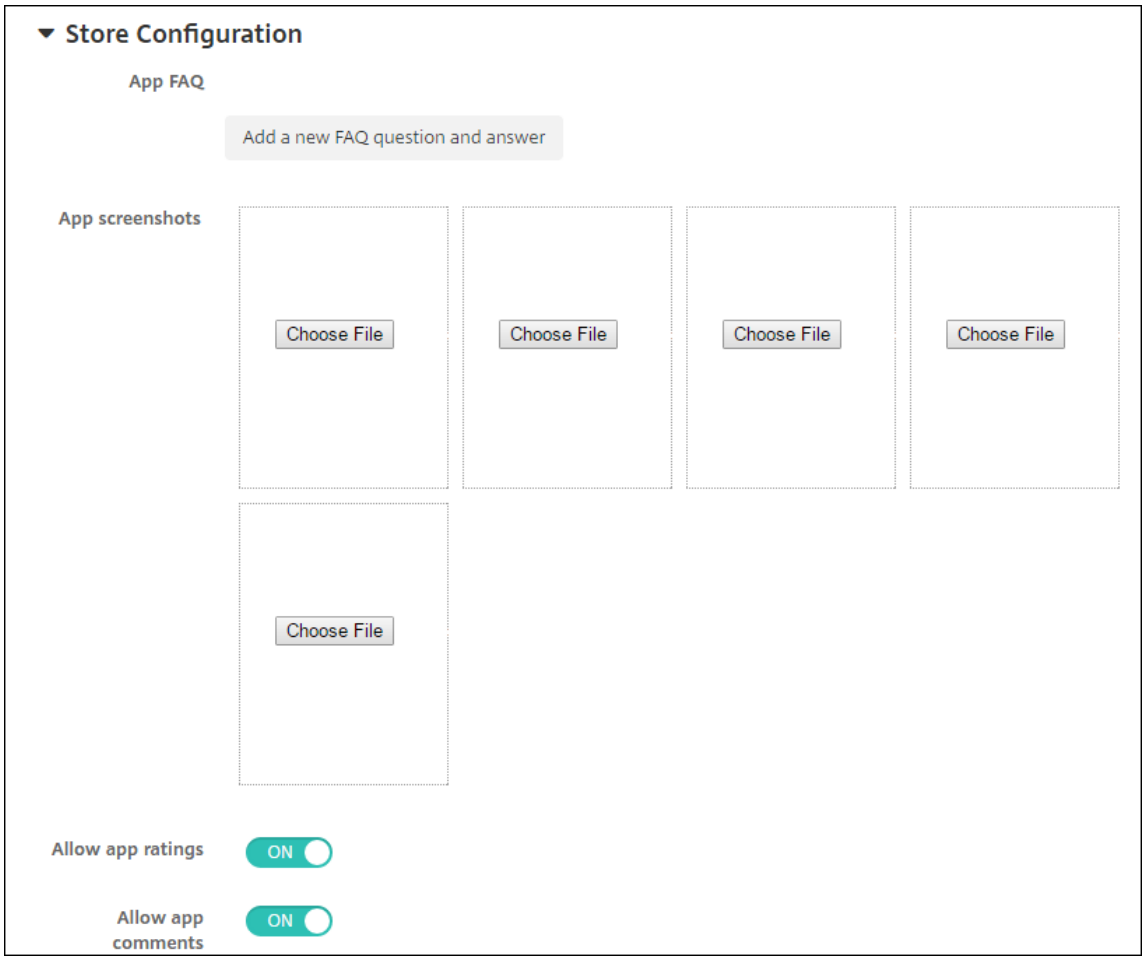
5. ［プラットフォーム］で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

次に、各プラットフォームのアプリ設定を構成します。次を参照してください:

- Google Play アプリのアプリ設定を構成する
- 管理対象アプリストアのアプリ
- iOS アプリ用のアプリ設定の構成

1 つのプラットフォームの設定の構成が完了したら、プラットフォームの展開規則とアプリストア構成を設定します。

1. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。
2. ［ストア構成］を展開します。



オプションで、以下を構成できます:

- アプリの **FAQ**:［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。

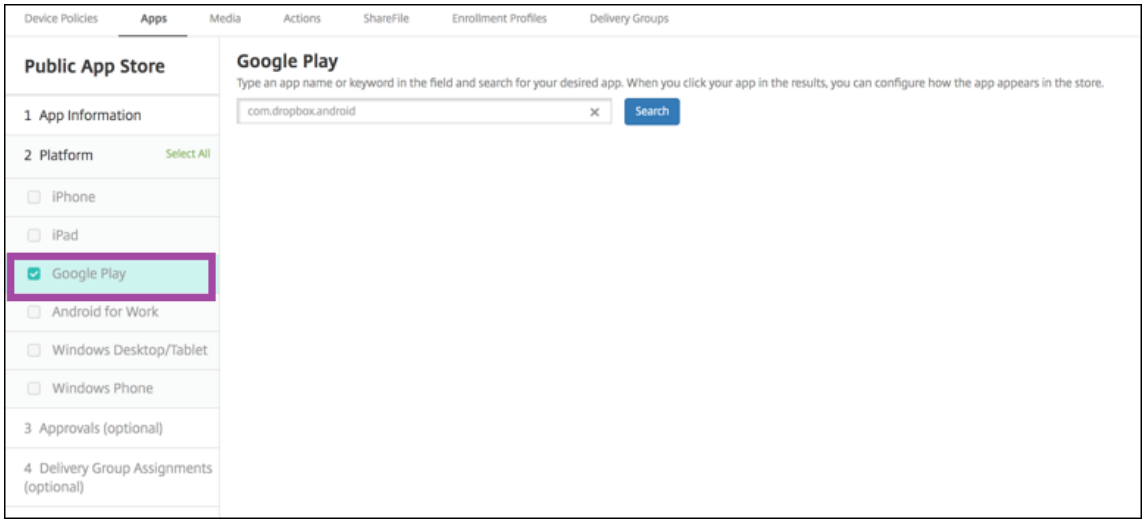
- スマホ/タブレット用のスクリーンショットを追加：アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可：ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可：ユーザーがアプリストアのアプリにコメントを残すことを許可します。

Google Play アプリのアプリ設定を構成する

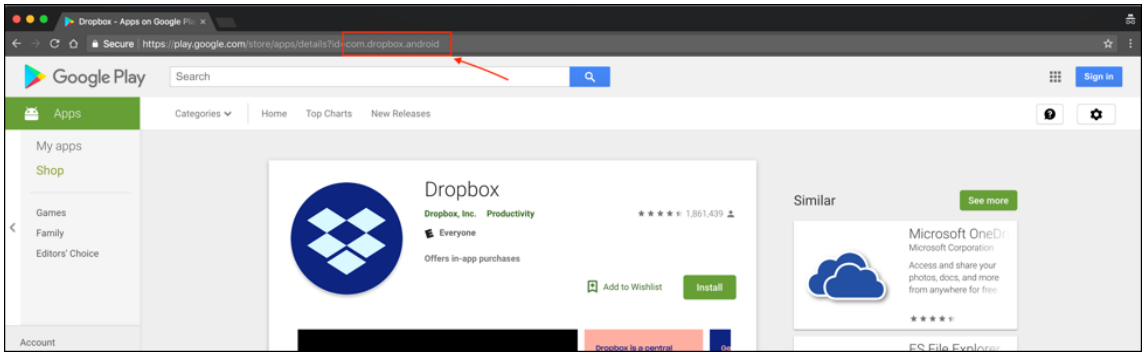
> 注：
>
> Google Play ストアのすべてのアプリに管理対象 Google Play からアクセスできるようにするには、サーバープロパティ **Access all apps in the managed Google Play store** を使用します（「サーバープロパティ」を参照してください）。このプロパティを **true** に設定すると、すべての Android Enterprise のユーザーがパブリック Google Play ストアアプリにアクセスできます。次に、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

Google Play ストアのアプリ設定を構成するには、他のプラットフォームのアプリとは異なる手順が必要です。Google Play ストアのアプリ情報は手動で構成する必要があります。

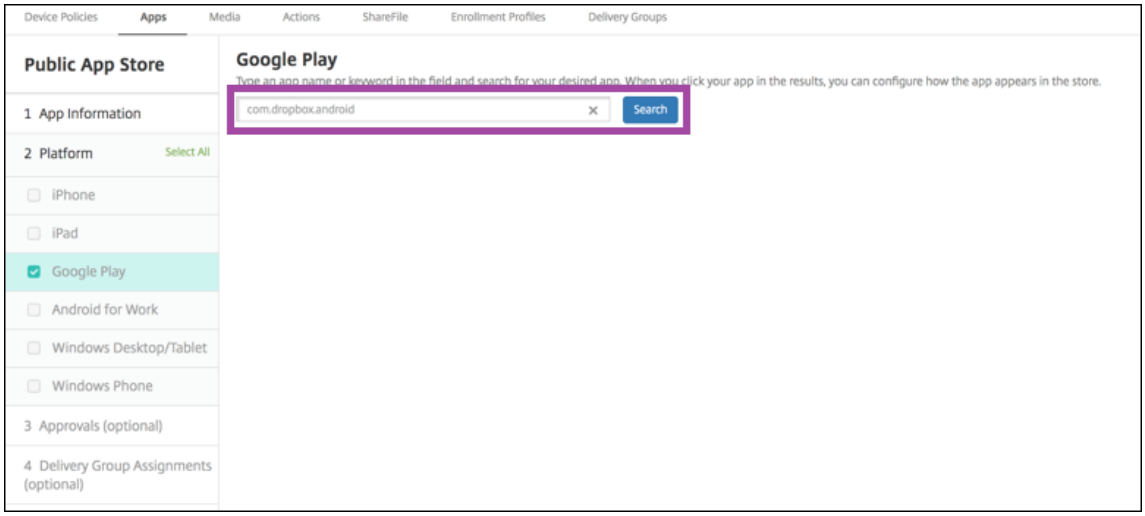
1. ［プラットフォーム］で ［**Google Play**］が選択されていることを確認します。



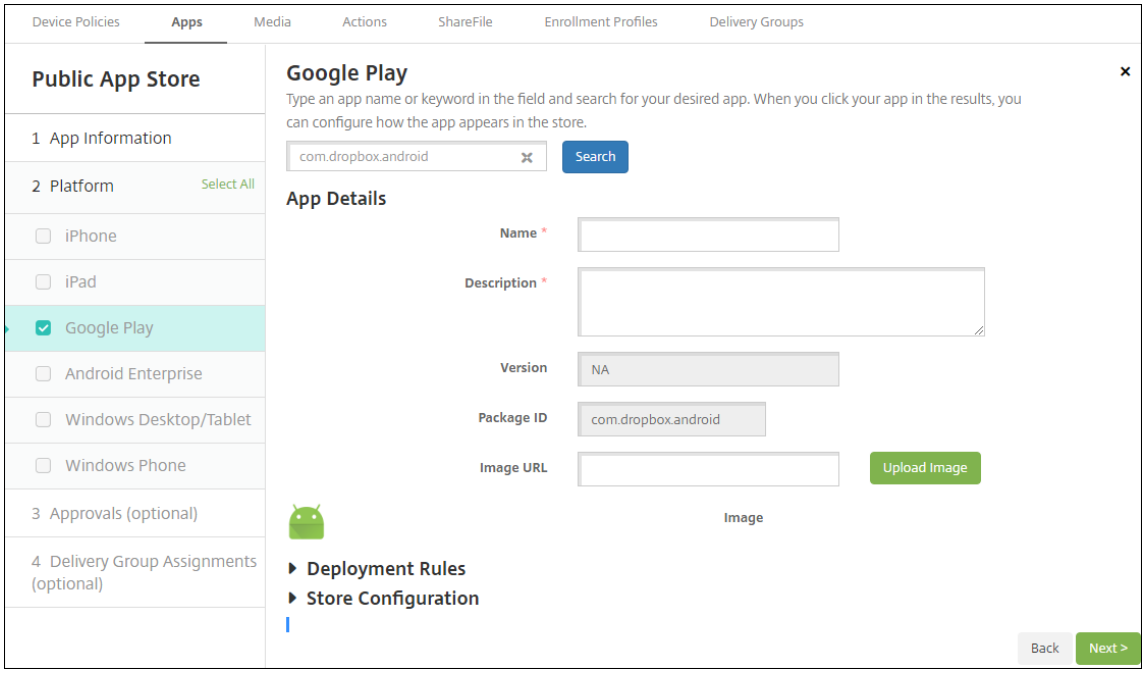
2. Google Play ストアに移動します。Google Play ストアからパッケージ ID をコピーします。この ID はアプリの URL に含まれています。



3. パブリックストアのアプリを Citrix Endpoint Management コンソールに追加する際に、検索バーに含まれるパッケージ ID を貼り付けます。［検索］をクリックします。



4. パッケージ ID が有効な場合は、アプリの詳細を入力できる UI が表示されます。



5. ストアのアプリと共に表示する画像の URL を構成できます。Google Play ストアの画像を使用するには:

   a) Google Play ストアに移動します。アプリの画像を右クリックし、画像のアドレスをコピーします。

   b) アドレスを ［画像 **URL**］フィールドに貼り付けます。

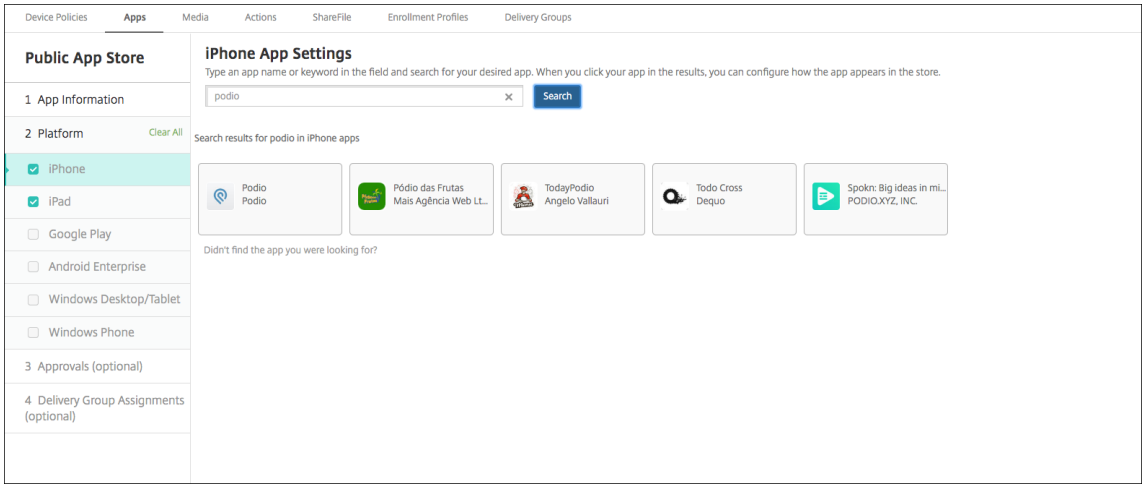
   c)［画像のアップロード］をクリックします。画像が ［イメージ］の横に表示されます。

画像を構成しない場合は、Android の一般的な画像がアプリに表示されます。

iOS アプリ用のアプリ設定の構成

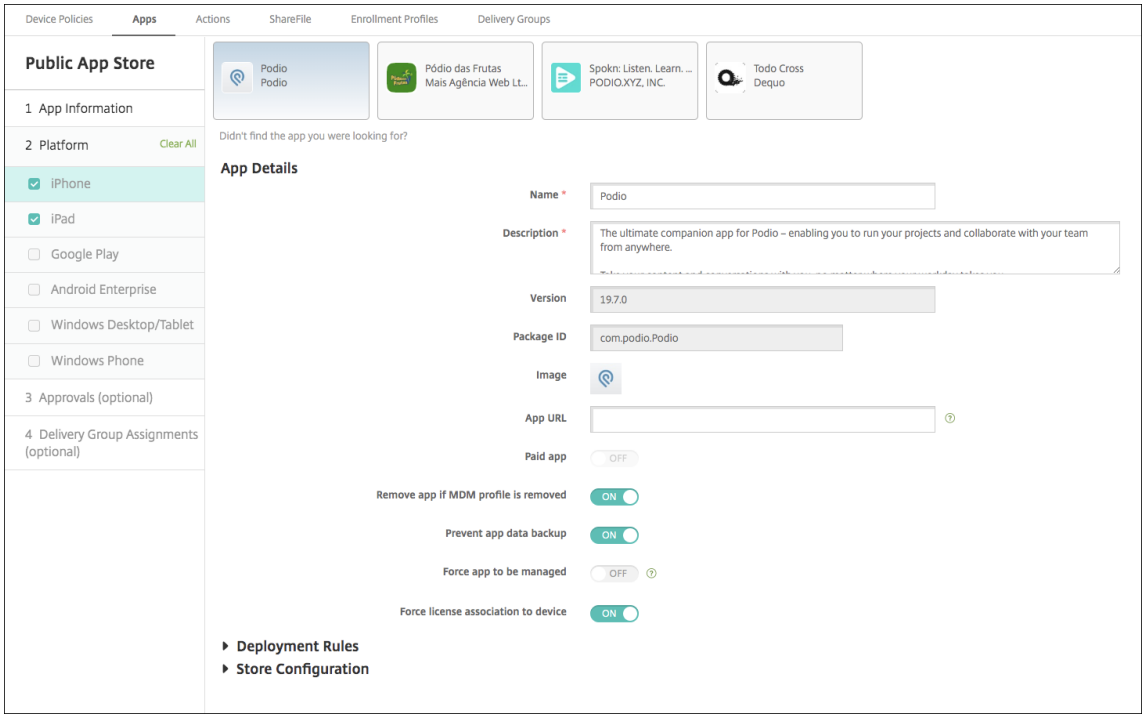
1. 検索ボックスにアプリ名を入力し、［検索］をクリックします。検索条件に一致するアプリが表示されます。検索条件に一致するアプリが表示されます。

   次の図は、iPhone アプリでの「**podio**」の検索結果を示しています。



2. 追加するアプリをクリックします。

3.［アプリの詳細］フィールドには、選択したアプリに関連する情報（名前、説明、バージョン番号、関連付けられた画像など）が事前に設定されています。

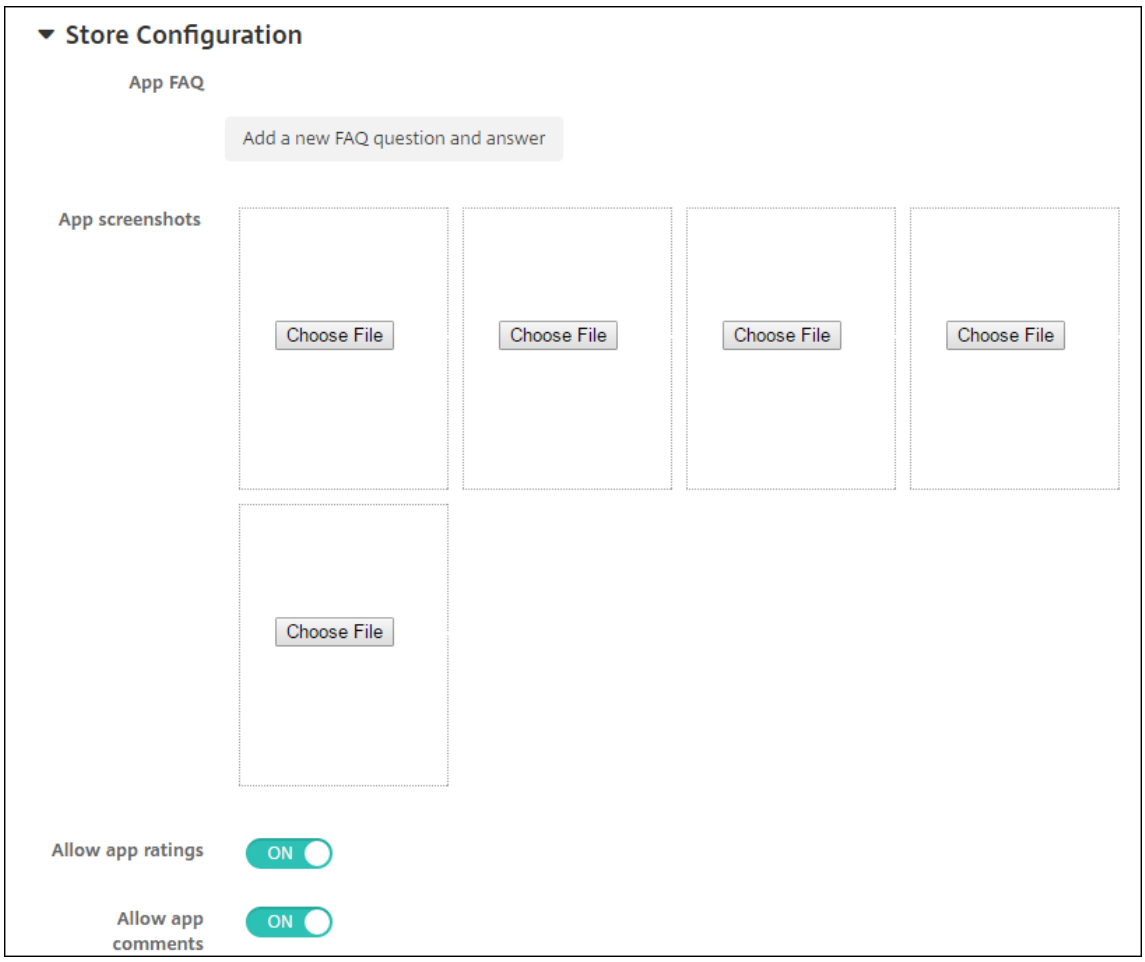


4. 次の設定を構成します。

   - 必要に応じて、アプリの名前と説明を変更します。
   - アプリの **URL**： Citrix Workspace アプリからアプリを起動するために使用する URL をコンマ区切りで入力します。このフィールドは、iPhone および iPad デバイスでのみ使用できます。
   - 有料アプリ：このフィールドは事前に構成されており、変更できません。
   - **MDM** プロファイルが削除されたらアプリを削除します： MDM プロファイルが削除された場合にアプリを削除するかどうかを選択します。デフォルトは ［オン］です。
   - アプリデータのバックアップを阻止します：アプリのデータをバックアップできないようにするかどうかを選択します。デフォルトは ［オン］です。
   - 製品トラック：ユーザーデバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、そのトラックを選択してユーザーに割り当てることができます。デフォルトは［実稼働］です。
   - 管理されるアプリ：アプリが非管理対象としてインストールされたときに、ユーザーに監視対象ではない iOS デバイスでのアプリの管理を許可するように求めるかどうかを選択します。デフォルトは ［オフ］です。ユーザー登録を通じて登録された iOS デバイスの場合、Citrix Endpoint Management はこの設定を強制せず、アプリ管理の許可をユーザーに求めません。
   - デバイスへの強制ライセンス割り当て：（デバイスの関連付けを有効にして開発された）アプリをユーザーではなくデバイスに関連付けるかどうかを選択します。選択したアプリがデバイスへの割り当てをサポートしていない場合、この設定は変更できません。

5. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。

6. ［ストア構成］を展開します。



オプションで、以下を構成できます:

- アプリの **FAQ**:［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加:アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可:ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可:ユーザーがアプリストアのアプリにコメントを残すことを許可します。

7. iPhone または iPad の場合、［一括購入］を展開します。

   a) Citrix Endpoint Management でアプリケーションの一括購入ライセンスを適用できるようにする場合は、［一括購入ライセンス］の一覧から、［一括購入ライセンスをアップロードする］を選択します。

   b) ダイアログボックスが開いたら、ライセンスをインポートします。

      ライセンス割り当て表によって、そのアプリの利用可能な全ライセンスの中で使用中のライセンスの数が分かります。

      個人ユーザーの一括購入ライセンスを解除することができます。それによってライセンスの割り当てが終了し、ライセンスを空けることができます。

c) 一括購入アカウントを追加する場合、［アプリの自動更新］を有効にします。この設定は、Apple Store に更新がアップされるとユーザーデバイス上のアプリが自動的に更新されるようにします。［管理されるアプリ］設定が有効になっている場合、ユーザーにプロンプトを表示せずに更新されます。更新は、アプリが必須かオプションかに関係なく行われます。

8. ［一括購入］（Volume Purchase）設定が完了したら、［次へ］をクリックします。［承認］ページが開きます。

   ワークフローを使用して、ユーザーにアプリへのアクセス許可を出す前に承認を必要とする設定にする方法については、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順を続行します。

9. ［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。

10. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

11. ［展開スケジュール］を展開して以下の設定を構成します：

    - 展開：アプリをデバイスに展開するかどうかを選択します。デフォルトは ［オン］です。
    - 展開スケジュール：アプリを ［すぐに］展開するか、［後で］展開するかを選択します。［後で］を選択した場合は、アプリを展開する日時を設定します。デフォルトは ［すぐに］です。
    - 展開条件：［すべての接続で］を選択すると、デバイスが接続するたびにアプリを展開します。［以前の展開が失敗した場合のみ］を選択すると、以前にデバイスがアプリを受信できなかった場合にアプリを展開します。デフォルトは ［すべての接続で］です。

    ［常時接続に対する展開］オプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

    常時接続オプション：

    - iOS デバイスでは使用できません。
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

    構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

12. ［保存］をクリックします。

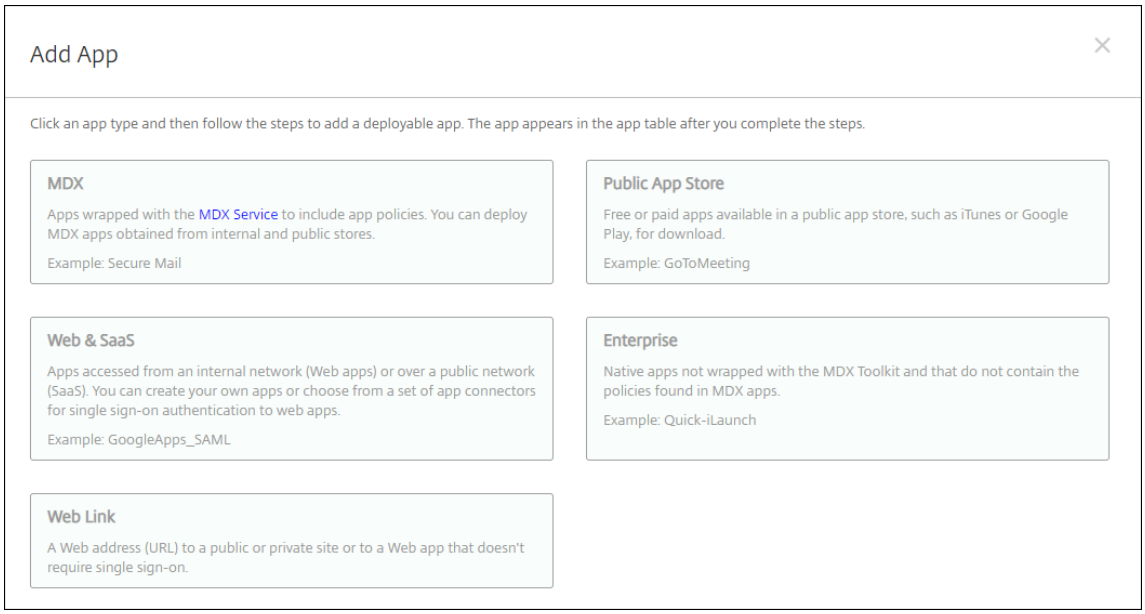
Web または **SaaS** アプリの追加

Citrix Endpoint Management コンソールを使用して、エンタープライズ、Web、SaaS アプリへの SSO（Single Sign-On：シングルサインオン）認証をユーザーに提供できます。

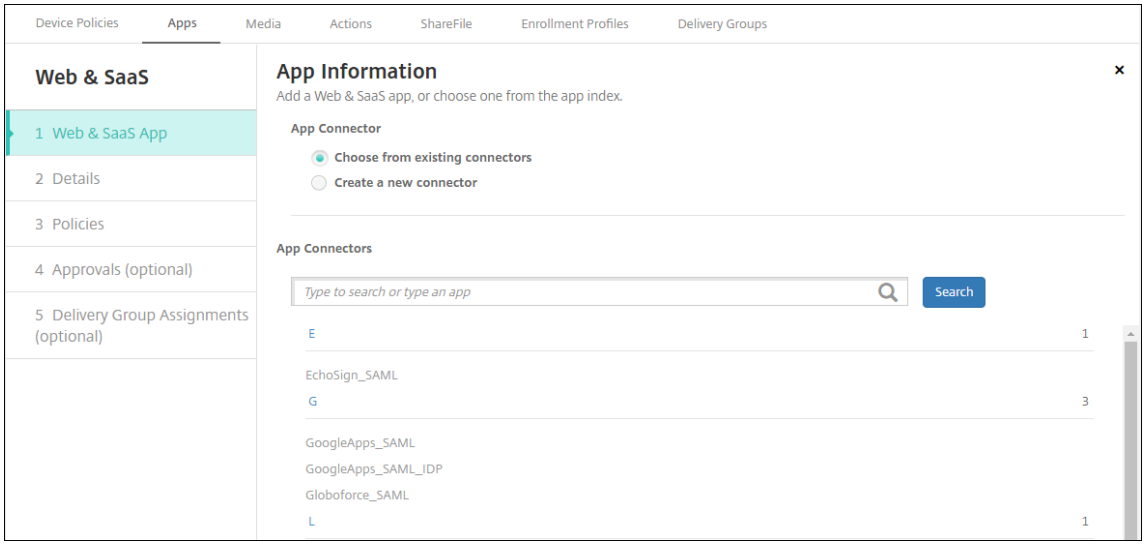
Web アプリまたは SaaS アプリを追加するとき、Citrix Endpoint Management で独自のコネクタを構築できます。Citrix Endpoint Management で使用できるコネクタの種類の一覧については、「アプリケーションコネクタの種類」を参照してください。

アプリが SSO のみに対応している場合：設定を保存すると、アプリは Citrix Endpoint Management コンソールの ［アプリ］タブに表示されます。

1. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］**>**［追加］の順にクリックします。［アプリの追加］ダイアログボックスが開きます。



2. ［**Web** および **SaaS**］を選択します。［アプリ情報］ページが開きます。



3. 既存のまたは新しいアプリコネクタは、以下のように構成します。

既存のアプリコネクタを構成するには

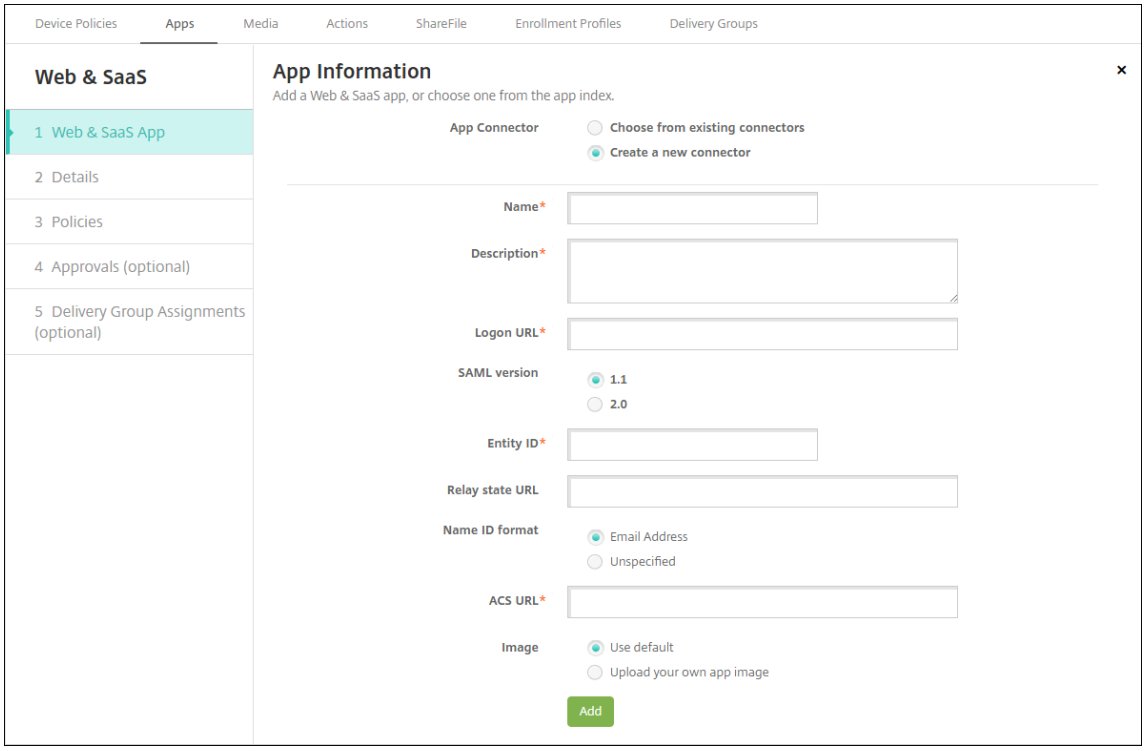
1. ［アプリ情報］のページで、上で示したように［既存のコネクタから選択します］が既に選択されています。［アプリコネクタ］一覧で、使用するコネクタを選択します。アプリコネクタの情報が表示されます。
2. 次の設定を構成します：

   - アプリ名：事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
   - アプリの説明：事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
   - **URL**：事前に入力されている URL をそのまま使用するか、アプリの Web アドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
   - ドメイン名：該当する場合、アプリのドメイン名を入力します。
   - アプリは内部ネットワークでホストされます：内部ネットワークのサーバーでアプリを実行するかどうかを選択します。ユーザーがリモートから内部アプリに接続する場合は、NetScaler Gateway Gateway を介して接続する必要があります。このオプションを［オン］に設定すると、VPN キーワードがアプリに追加され、NetScaler Gateway Gateway を介して接続できるようになります。デフォルトは ［オフ］です。
   - アプリカテゴリ：ドロップダウンリストから、アプリに適用する任意のカテゴリを選択します。
   - ユーザーアカウントプロビジョニング：アプリケーションのユーザーアカウントを作成するかどうかを選択します。Globalforce_SAML コネクタを使用している場合は、このオプションを有効にして、シームレスな SSO 統合が行われるようにする必要があります。
   - ［ユーザーアカウントのプロビジョニング］を有効にした場合は、次の設定を構成します：
     - サービス アカウント
       * ユーザー名：アプリ管理者の名前を入力します。このフィールドは必須です。
       * パスワード：アプリ管理者のパスワードを入力します。このフィールドは必須です。
     - ユーザーアカウント
       * ユーザー権利の終了時：ドロップダウンリストから、ユーザーがアプリへのアクセスを許可されなくなった場合に実行するアクションを選択します。デフォルトは ［アカウントの無効化］です。
     - ユーザー名規則
       * 追加するユーザー名の規則ごとに、以下の操作を行います：
         - ユーザー属性：ドロップダウンリストから、規則に追加するユーザー属性を選択します。
         - 長さ（文字）：ドロップダウンリストから、ユーザー名の規則で使用するユーザー属性の文字数を選択します。デフォルトは ［すべて］です。
         - 規則：追加した各ユーザー属性が、ユーザー名の規則に自動的に追加されます。
   - パスワード要件
     - 長さ：ユーザーパスワードの最小文字数を入力します。デフォルトは **8** です。
   - パスワードの有効期限

- 有効期間（日）：パスワードの有効期間（日数）を入力します。有効な値は **0**～**90** です。デフォルトは 90 です。
- 有効期限が切れた後にパスワードを自動的にリセット：有効期限が切れたときにパスワードを自動的にリセットするかどうかを選択します。デフォルトは ［オフ］です。このフィールドを有効にしないと、ユーザーパスワードの有効期限が切れたときにアプリを開くことができなくなります。

新しいアプリコネクタを構成するには

1. ［アプリ情報］のページで、［新しいコネクタの作成］を選択します。アプリコネクタのフィールドが表示されます。

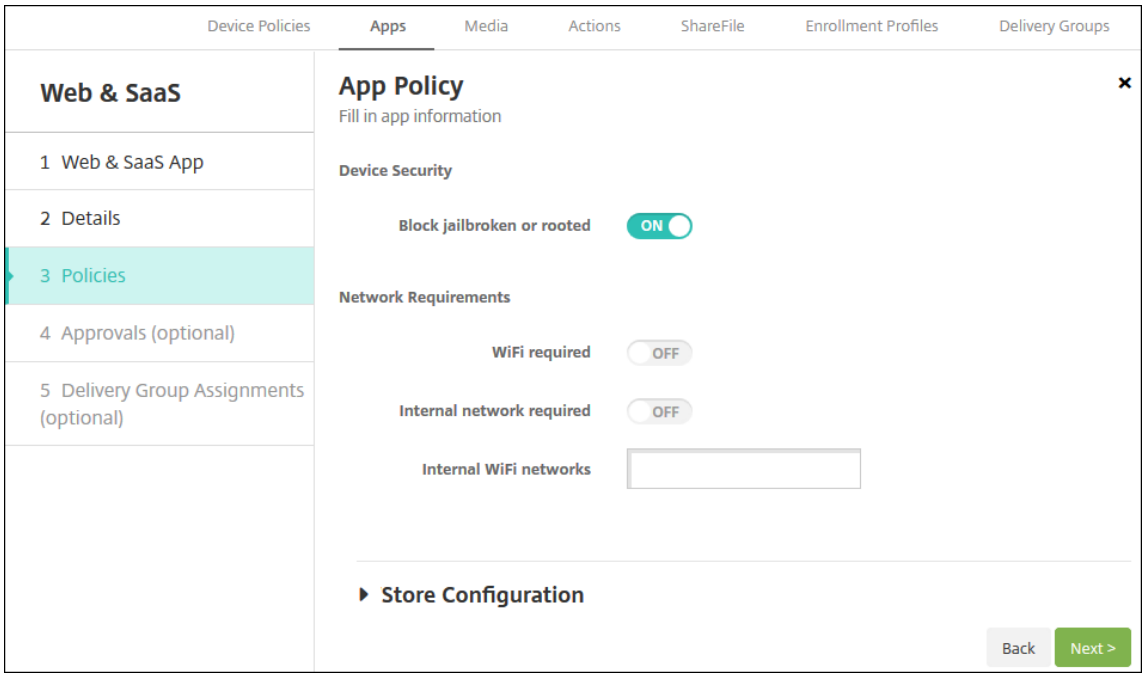


2. 次の設定を構成します：

- 名前：コネクタの名前を入力します。このフィールドは必須です。
- 説明：コネクタの説明を入力します。このフィールドは必須です。
- ログオン **URL**：ユーザーがサイトにログオンするときに使用する URL を入力するか、コピーして貼り付けます。たとえば、追加するアプリにログオンページがある場合、Web ブラウザーを開いてアプリのログオンページに移動します。「`https://www.example.com/logon`」などです。このフィールドは必須です。
- **SAML** のバージョン：［**1.1**］または ［**2.0**］を選択します。デフォルトは ［**1.1**］です。
- エンティティ **ID**： SAML アプリの ID を入力します。
- リレー状態 **URL**： SAML アプリの Web アドレスを入力します。リレーステート URL はアプリからの応答 URL です。

- 名前 **ID** 形式：［メールアドレス］または［未指定］を選択します。デフォルトは［メールアドレス］です。
- **ACS URL**：ID プロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービス URL（ACS URL）を入力します。ACS URL では、ユーザーがシングルサインオン機能を使用できます。
- イメージ：デフォルトの Citrix イメージを使用するのか、独自のアプリイメージをアップロードするのかを選択します。デフォルトは［デフォルトを使用］です。
  - 独自のイメージをアップロードする場合は、［参照］をクリックしてアップロードするファイルの場所に移動します。そのファイルは、.PNG ファイルである必要があります。JPEG ファイルや GIF ファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。

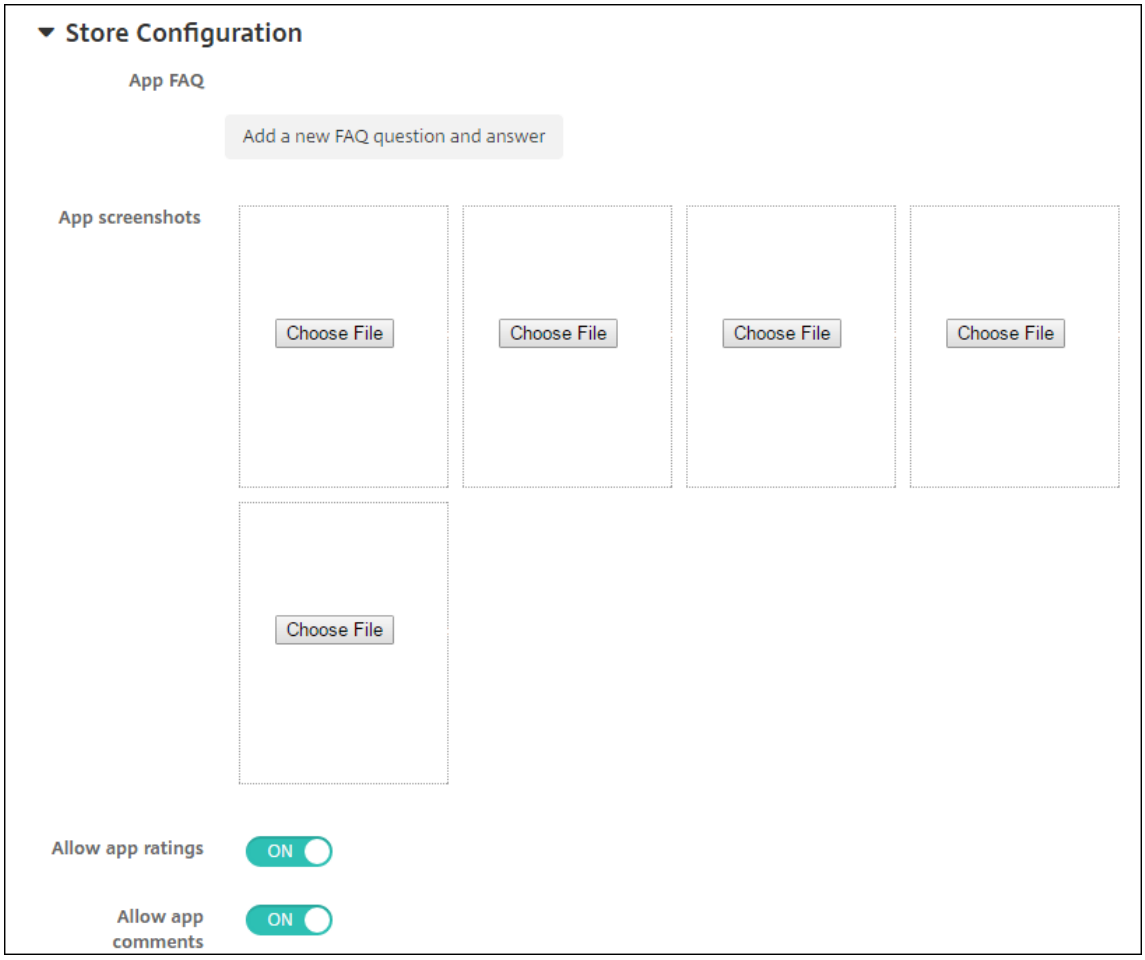
3. 完了したら、［追加］をクリックします。［詳細］のページが開きます。
4. ［次へ］をクリックします。［アプリのポリシー］ページが開きます。



5. 次の設定を構成します：

- デバイスのセキュリティ
- ジェイルブレイクまたは **Root** 化をブロックします：ジェイルブレイク済みまたはルート化済みのデバイスによるアプリへのアクセスをブロックするかどうかを選択します。デフォルトは ［オン］です。
- ネットワークの要件
- **Wi-Fi** が必要です：アプリの実行に Wi-Fi 接続が必要であるかどうかを選択します。デフォルトは ［オフ］です。
- 内部ネットワークが必要です：アプリの実行に内部ネットワークが必要であるかどうかを選択します。デフォルトは ［オフ］です。
- 内部 **Wi-Fi** ネットワーク：［**Wi-Fi** が必要です］を有効にした場合は、使用する内部 Wi-Fi ネットワークを入力します。

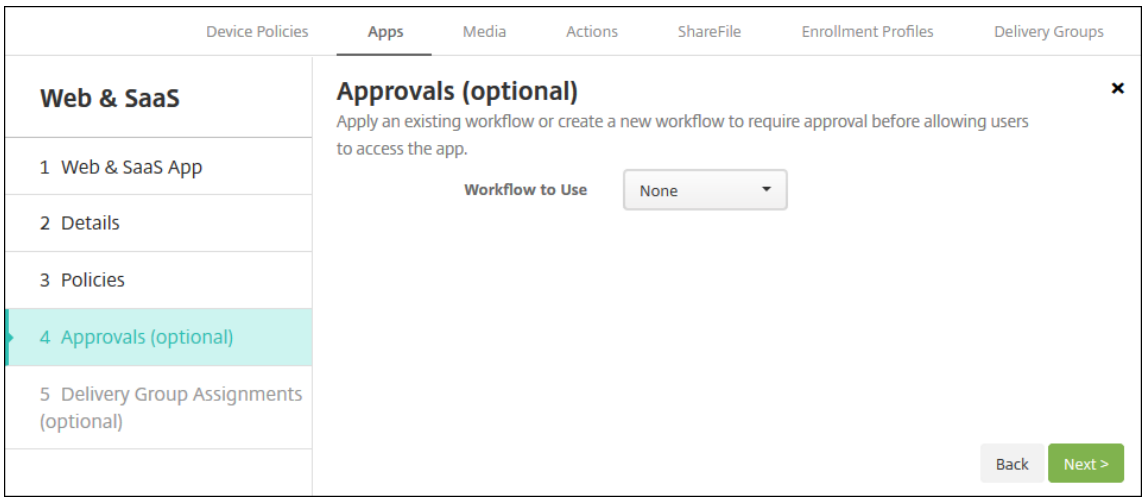
6. ［ストア構成］を展開します。



オプションで、以下を構成できます：

- アプリの **FAQ**：［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加：アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可：ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可：ユーザーがアプリストアのアプリにコメントを残すことを許可します。

7. ［次へ］をクリックします。［承認］ページが開きます。



ワークフローを使用して、ユーザーにアプリへのアクセス許可を出す前に承認を必要とする設定にする方法については、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順を続行します。

8. ［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。
9. ［デリバリーグループを選択］の横に、デリバリーグループを入力して検索するか、1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。
10. ［展開スケジュール］を展開して以下の設定を構成します：

    - 展開：アプリをデバイスに展開するかどうかを選択します。デフォルトは ［オン］です。
    - 展開スケジュール：アプリを ［すぐに］展開するか、［後で］展開するかを選択します。［後で］を選択した場合は、アプリを展開する日時を設定します。デフォルトは ［すぐに］です。
    - 展開条件：［すべての接続で］を選択すると、デバイスが接続するたびにアプリを展開します。［以前の展開が失敗した場合のみ］を選択すると、以前にデバイスがアプリを受信できなかった場合にアプリを展開します。デフォルトは ［すべての接続で］です。

    ［常時接続に対する展開］オプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

    常時接続オプション：

    - iOS デバイスでは使用できません。
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

    構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

11. ［保存］をクリックします。

エンタープライズアプリの追加

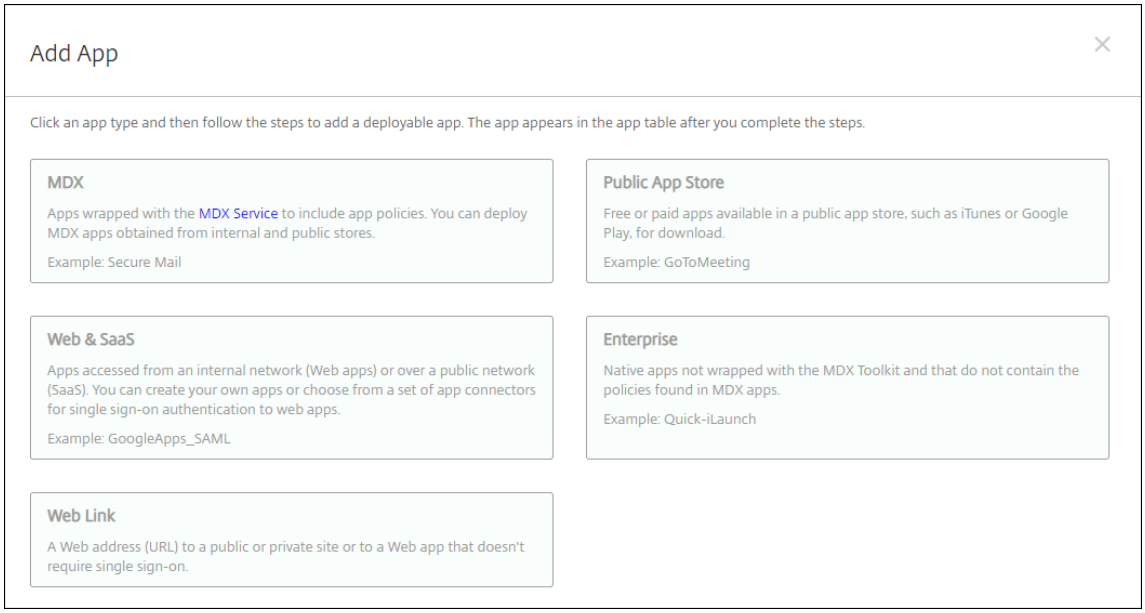
Citrix Endpoint Management のエンタープライズアプリは、別のソースから開発または取得するプライベートアプリです。MDX 対応アプリとして提供されるプライベート Android Enterprise アプリを除いて、エンタープライズアプリは MAM SDK または MDX Toolkit で準備されていません。エンタープライズアプリのアップロードは、Citrix Endpoint Management コンソールの ［アプリ］タブで行うことができます。エンタープライズアプリは、以下のプラットフォーム（および対応するファイルの種類）をサポートします：

- iOS（.ipa ファイル）
- macOS（.pkg ファイル）

  Citrix Endpoint Management は、アップロードする PKG ファイルのサイズを制限しませんが、ファイルのアップロード時間を制限します。デフォルトでは、100 秒以内にアップロードを完了する必要があります。詳しくは、「サーバープロパティ」を参照してください。
- Android（.apk ファイル）
- Android Enterprise（.apk ファイル）
- 参照：Win32 アプリをエンタープライズアプリとして追加
- 参照：MDX 対応のプライベートアプリ

Google Play ストアからダウンロードしたアプリをエンタープライズアプリとして追加することはサポートされていません。代わりに、パブリックアプリストアのアプリとして Google Play ストアから入手したアプリを追加します。「パブリックアプリストアのアプリの追加」を参照してください。

1. Citrix Endpoint Management コンソールで、［構成］**>** ［アプリ］**>** ［追加］の順にクリックします。［アプリの追加］ダイアログボックスが開きます。



2. ［エンタープライズ］をクリックします。［アプリ情報］ページが開きます。
3. ［アプリ情報］ペインで、以下の情報を入力します：

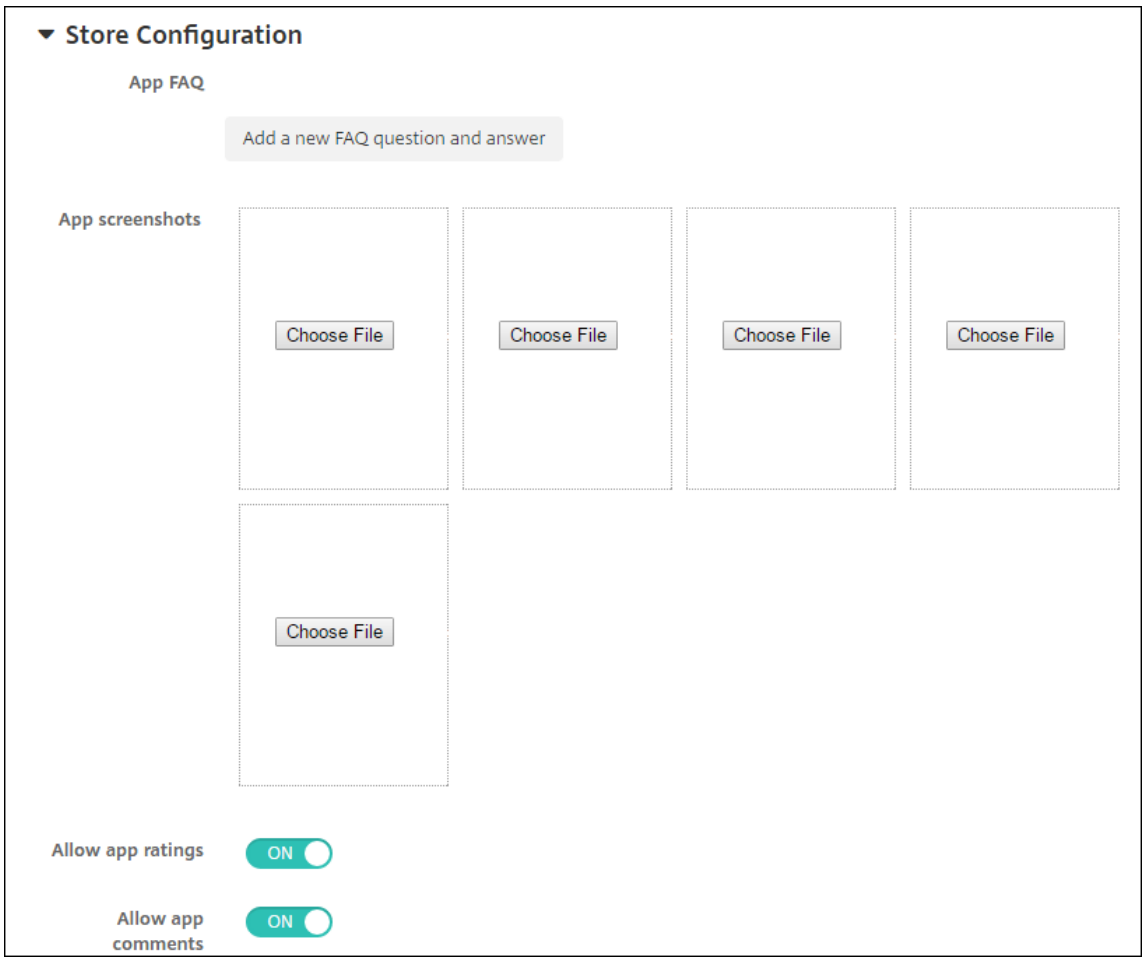
   - 名前：アプリの説明的な名前を入力します。この名前は、［アプリ］の表の［アプリ名］の下に表示されます。
   - 説明：任意で、アプリの説明を入力します。
   - アプリカテゴリ：任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリのカテゴリについて」を参照してください。

4. ［次へ］をクリックします。アプリのプラットフォームページが開きます。
5. ［プラットフォーム］で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。
6. 選択したプラットフォームごとに、［アップロード］をクリックしてアップロードするファイルの場所に移動し、そのファイルを選択します。
7. ［次へ］をクリックします。プラットフォームのアプリ情報ページが開きます。
8. プラットフォームの種類について、以下の設定を構成します：

   - ファイル名：任意で、アプリの名前を新たに入力します。
   - アプリの説明：任意で、アプリの説明を新たに入力します。
   - アプリのバージョン：このフィールドは変更できません。
   - 最小 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン：任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス：任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。

- パッケージ **ID**：アプリの一意の識別子。
- **MDM** プロファイルが削除されたらアプリを削除します： MDM プロファイルが削除された場合にデバイスからアプリを削除するかどうかを選択します。デフォルトは ［オン］ です。この設定は、macOS には適用されません。
- アプリデータのバックアップを阻止します：アプリのデータをバックアップできないようにするかどうかを選択します。デフォルトは ［オン］ です。この設定は、macOS には適用されません。
- 管理されるアプリ：監視対象ではないデバイスで管理対象アプリとしてアプリをインストールするかどうかを選択します。有効になっている場合、Citrix Endpoint Management がこの設定を処理する方法がデバイスの種類によって決まります。この設定を有効にすると、ユーザーにプロンプトを表示せずにアプリが更新されます。更新は、アプリが必須かオプションかに関係なく行われます。デフォルトは ［オフ］ です。
  - iOS デバイスの場合、アプリが既にインストールされていると、アプリの管理を許可するよう求めるプロンプトがユーザーの画面に表示されます。アプリが存在しないデバイスにアプリを展開すると、この設定の状態に関係なく、アプリは管理対象アプリとしてインストールされます。iOS 9.0 以降で利用できます。ユーザー登録を通じて登録された iOS デバイスの場合、Citrix Endpoint Management はこの設定を強制せず、アプリ管理の許可をユーザーに求めません。
  - macOS デバイスの場合、設定を有効にしてから、アプリをデバイスに展開します。アプリは管理対象アプリとして自動的にインストールされます。ユーザーの画面にプロンプトは表示されません。アプリが存在しないデバイスにアプリを展開すると、この設定の状態に関係なく、アプリは管理対象アプリとしてインストールされます。macOS 11.0 以降で利用できます。

9. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。
10. ［ストア構成］ を展開します。



オプションで、以下を構成できます:

- アプリの **FAQ**:［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加:アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可:ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可:ユーザーがアプリストアのアプリにコメントを残すことを許可します。

11. ［次へ］をクリックします。［承認］ページが開きます。

    ワークフローを使用して、ユーザーにアプリへのアクセス許可を出す前に承認を必要とする設定にする方法については、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順を続行します。

12. ［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。

13. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

14. ［展開スケジュール］を展開して以下の設定を構成します：

    - 展開：アプリをデバイスに展開するかどうかを選択します。デフォルトは ［オン］です。
    - 展開スケジュール：アプリを ［すぐに］展開するか、［後で］展開するかを選択します。［後で］を選択した場合は、アプリを展開する日時を設定します。デフォルトは ［すぐに］です。
    - 展開条件：［すべての接続で］を選択すると、デバイスが接続するたびにアプリを展開します。［以前の展開が失敗した場合のみ］を選択すると、以前にデバイスがアプリを受信できなかった場合にアプリを展開します。デフォルトは ［すべての接続で］です。

    ［常時接続に対する展開］オプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

    常時接続オプション：

    - iOS デバイスでは使用できません。
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

    構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

15. ［保存］をクリックします。

Win32 アプリをエンタープライズアプリとして追加

Win32 アプリ用の MSI、APPX、AppxBundle、PS1、または EXE ファイルを Citrix Endpoint Management にアップロードして、管理対象の Windows 10 および Windows 11 デスクトップデバイスおよびタブレットデバイスに展開できます。Citrix Endpoint Management を使用してこのファイルを展開すると、次のように Windows デバイスにアプリがインストールされます：

- インストール中にアップグレード後のアプリにより旧バージョンが削除される場合、デバイスにはアップグレード後のアプリのみが含まれます。
- アップグレード後のアプリで旧バージョンを削除できないものの、新バージョンはインストール可能な場合、デバイスには両方のバージョンのアプリが含まれます。Citrix Endpoint Management では、旧バージョンの情報は保存されなくなります。
- 旧バージョンが存在するとアップグレード後のアプリをインストールできない場合、新しいアプリはインストールされません。この場合には、まず ［アプリのアンインストール］デバイスポリシーを展開して旧バージョンのアプリを削除します。次に、新しいバージョンのアプリを展開します。

要件

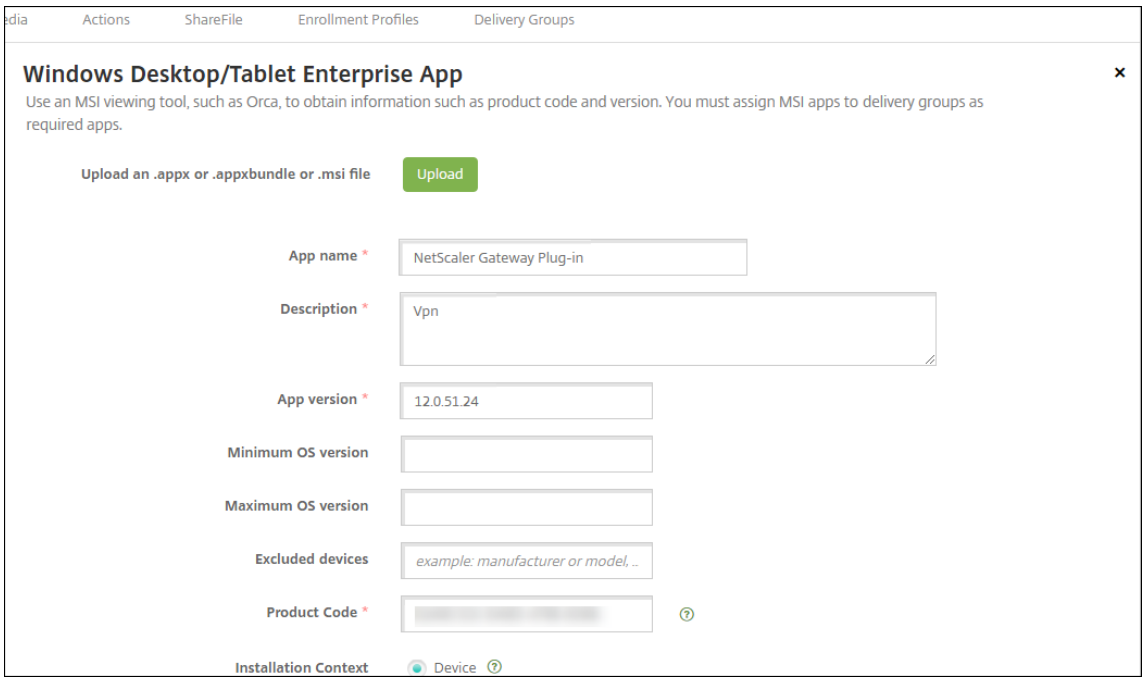
- Windows 10（バージョン 1607 以降）または Windows 11
- Windows 10 Professional または Windows 11 Professional
- Windows 10 Enterprise または Windows 11 Enterprise
- /quiet オプションを指定してインストールされたスタンドアロンの Win 32 MSI アプリ。この展開のユースケースでは、Microsoft は複数のアプリを使用する MSI、ネストされた MSI、インタラクティブインストールをサポートしていません。

メタデータを調べる　Citrix Endpoint Management に Win32 アプリを追加する場合、そのアプリのメタデータを指定します。メタデータを調べるには、Windows コンピューターで Orca アプリケーションを使用し、次の情報を記録します：

- 製品コード
- 製品名
- 製品バージョン
- パッケージのインストールタイプ（ユーザーごとまたはマシンごと）

Citrix Endpoint Management に **Win32** アプリを追加する

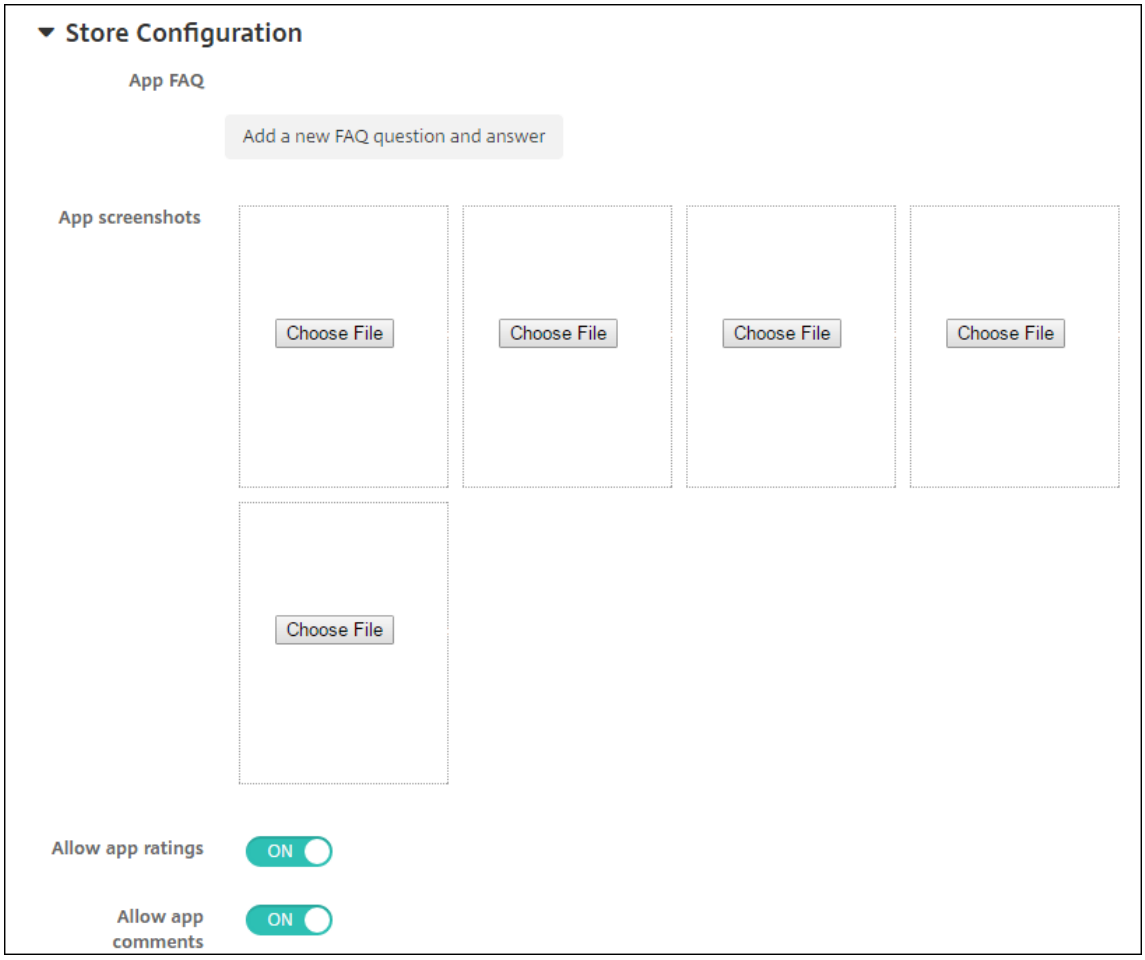
1. ［構成］**>**［アプリ］に移動して ［エンタープライズ］をクリックし、［アプリケーション情報］ページにアプリの名前を入力します。
2. ［**Windows** デスクトップ**/**タブレット］を除くすべてのプラットフォームのチェックボックスをオフにします。
3. ［**Windows** デスクトップ**/**タブレットのエンタープライズアプリ］ページで、［アップロード］をクリックして目的のファイルを選択します。
4. 次の設定を構成します：



- アプリ名：アプリのメタデータに記載されているアプリの名前。
- 説明：アプリの説明。
- アプリバージョン：アプリのメタデータに記載されているアプリのバージョン番号。
- 最小 **OS** バージョン：オプション。アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョン。
- 最大 **O** バージョン：オプション。アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョン。
- 除外するデバイス：オプション。アプリの実行を禁止するデバイスの製造元またはモデル。
- 製品コード：アプリのメタデータに記載されている、UUID 形式の MSI アプリの製品コード。
- インストールコンテキスト：アプリのメタデータに基づいて、アプリをデバイスとユーザーのどちらにインストールするかを選択します。この設定は、EXE ファイルでは使用できません。
- コマンドライン： MSIEXEC.exe の呼び出しで使用するコマンドラインオプション。
- コマンドラインのインストール： EXE ファイルをサイレントインストールするためのコマンドライン引数を追加します。
- コマンドラインのアンインストール： EXE ファイルをサイレントアンインストールするためのコマンドライン引数を追加します。
- 再試行回数：インストールを失敗としてマークするまでにダウンロードおよびインストール操作を試行できる回数。
- タイムアウト：インストーラーがインストールを失敗して監視を中止するまでインストール処理を実行できる時間（分）。
- 再試行の間隔：再試行できるようになるまでの時間（分）。

5. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。

6. ［ストア構成］を展開します。



オプションで、以下を構成できます：

- アプリの **FAQ**：［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加：アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可：ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可：ユーザーがアプリストアのアプリにコメントを残すことを許可します。

7. ［概要］ページが表示されるまで ［次へ］をクリックし、［保存］をクリックします。
8. ［構成］ **>** ［デリバリーグループ］に移動して、構成した Win32 アプリを必須アプリとして追加します。
9. 追加したアプリを展開してから、ユーザーにアプリが利用可能になったことを知らせます。

Win32 アプリのアップグレード

1. 前述の「メタデータを調べる」の説明に従い、アプリのメタデータを調べます。

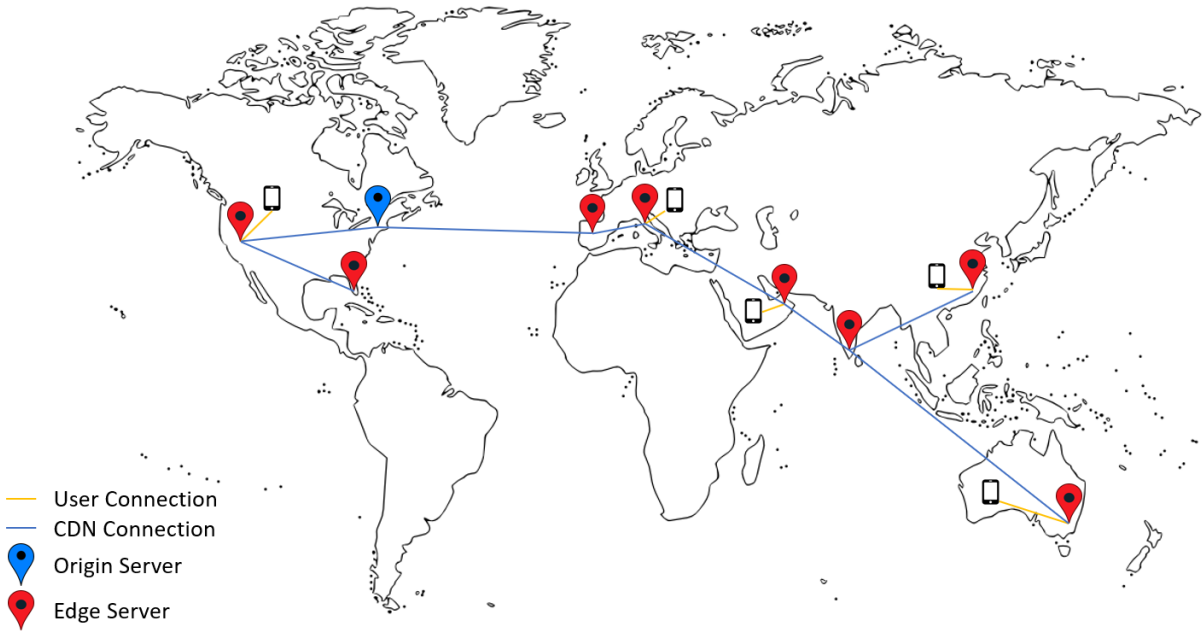
2. ［構成］**>**［アプリ］に移動して新バージョンのアプリをアップロードし、［アプリのバージョン］を更新します。アプリの製品コードが新バージョンで変更されている場合は、この設定も更新します。
3. 変更を送信し、アプリを展開します。

Citrix CDN によるエンタープライズアプリおよび **MDX** アプリの配信

Citrix コンテンツ配信ネットワーク（CDN）でエンタープライズアプリと MDX アプリを配信できます。CDN では、地理的に分散されたサーバーのグループが連携して機能し、アプリケーションコンテンツをすばやく安全に配信します。ローカルサーバーは、アプリをモバイルデバイスに配信します。

CDN は、近くの CDN 配信ポイントを使用して地理的に近いモバイルデバイスにコンテンツを配信し、アプリのダウンロード時間を短縮します。CDN は、ユーザーに最も近いポイントオブプレゼンス（POP）の場所からアプリを配信します。

次の図は、CDN がモバイルデバイスユーザーに最も近いエッジサーバーにアプリを配信する例です。モバイルデバイスがアプリを要求すると、エッジサーバーは配信元サーバーのコンテンツをキャッシュします。



ユーザーは Citrix Secure Hub を使ってアプリに接続できます。アプリを追加すると、Citrix Endpoint Management によりそのアプリコネクタが作成されます。

エンタープライズアプリの Citrix CDN サポートは、次のプラットフォームで利用できます：

- iOS（MDM または MAM 登録）
- Android（MDM または MAM 登録）
- Windows デスクトップまたはタブレット（MDM 登録）
- macOS（MDM 登録）

MDX アプリの Citrix CDN サポートは、次のプラットフォームで利用できます:

- iOS（MDM または MAM 登録）
- Android（MDM または MAM 登録）

CDN のしくみ

CDN サービスの中核となるのは、アプリをより短時間で配信することを目的としてリンクされた複数のサーバーです。この目的は、世界中のさまざまな配信ポイントにアプリを安全に配置することで達成されます。Citrix Endpoint Management サーバーへの最初の接続で使用されるモバイルデバイスの DNS サーバーが、配信ポイントを決定します。

たとえば、モバイルデバイスの DNS サーバー IP がフロリダ州フォートローダーデールのものであるとします。CDN は、この場所に最も近いローカルの配信ポイントを使用して、アプリをモバイルデバイスに配信します。このように CDN を使用することで、アプリのダウンロード時間が短縮されます。

モバイルデバイスが最初にエンタープライズアプリを要求またはプッシュすると、Citrix Endpoint Management はアプリをローカルの配信ポイントにコピーし、他のローカルデバイスのダウンロードのためにそこで 24 時間保持します。

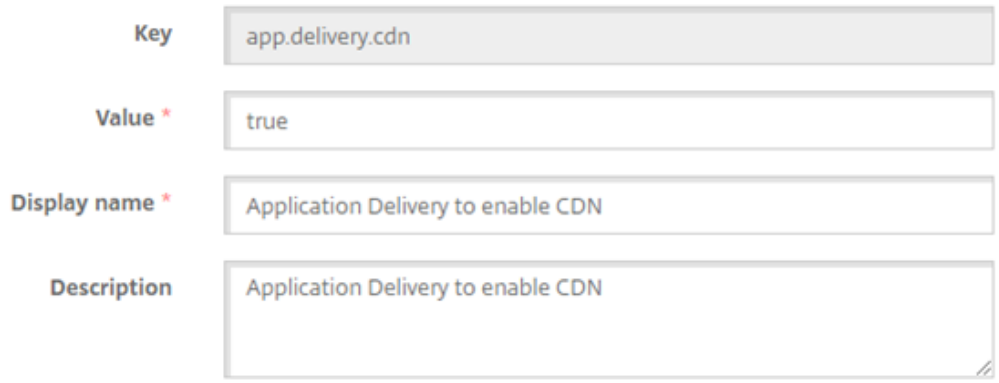
Citrix CDN によるエンタープライズアプリの配信

Citrix Endpoint Management リリース 19.4.1 では、エンタープライズアプリの配信はデフォルトですべての新しいマルチテナントの顧客向けにコンテンツ配信ネットワークで配信します。これより前のリリースを使用しているお客様の場合、次のセクションの手順を実行してください。

Citrix Endpoint Management サーバーに既に存在するエンタープライズアプリの場合、Citrix Endpoint Management は、以下の手順の完了後、アプリが再度アップロードされるまで、引き続きサーバーからアプリを配信します。

> 重要:
>
> アカウントの CDN を有効にできるのは Citrix Cloud 管理者のみです。サーバープロパティ `app.delivery.cdn` は、Citrix Cloud 管理者としてログオンした場合にのみ、Citrix Endpoint Management に表示されます。Citrix Cloud 管理者について詳しくは、「Citrix Cloud 管理者を管理する」を参照してください。

1. アカウントで CDN を有効にする：Citrix Endpoint Management コンソールで、［設定］**>**［サーバープロパティ］に移動します。
2. `app.delivery.cdn` を検索して、［編集］をクリックします。
3. 値を **true** に変更します。



4. Citrix Endpoint Management コンソールで、再度エンタープライズアプリをアップロードします:

   a) ［構成］**>** ［アプリ］に移動し、種類（エンタープライズ）およびプラットフォームでアプリ一覧を絞り込みます。
   b) アプリを選択して、［編集］、［次へ］、［アップロード］の順にクリックします。
   c) エンタープライズアプリごとにこの手順を繰り返します。

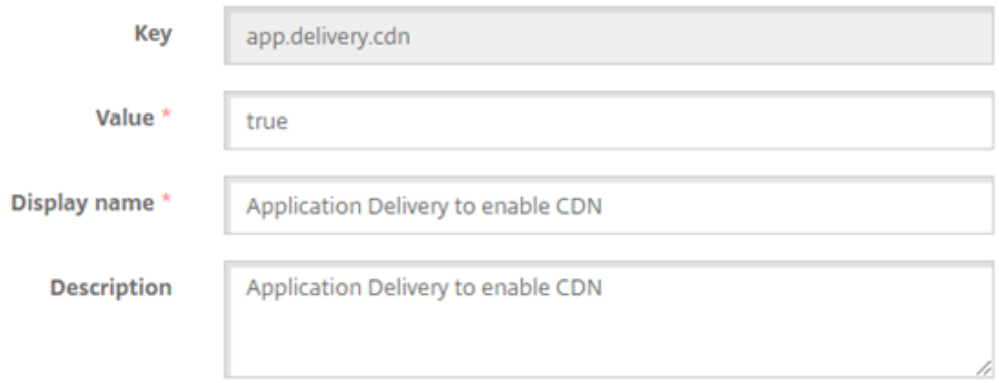
Citrix CDN から **MDX** アプリを配信する

Citrix Endpoint Management リリース 20.12.0 では、MDX アプリの配信は、すべての新しいマルチテナントの顧客に対し、デフォルトで CDN 配信に設定されています。これより前のリリースを使用しているお客様の場合、次のセクションの手順を実行してください。

Citrix Endpoint Management サーバーに既に存在する MDX アプリの場合、Citrix Endpoint Management は、以下の手順の完了後、アプリが再度アップロードされるまで、引き続きサーバーからアプリを配信します。

> 重要:
>
> アカウントの CDN を有効にできるのは Citrix Cloud 管理者のみです。サーバープロパティ`app.delivery.cdn`は、Citrix Cloud 管理者としてログオンした場合にのみ、Citrix Endpoint Management に表示されます。Citrix Cloud 管理者について詳しくは、「Citrix Cloud 管理者を管理する」を参照してください。

1. アカウントで CDN を有効にする: Citrix Endpoint Management コンソールで、［設定］**>** ［サーバープロパティ］に移動します。
2. `app.delivery.cdn`を検索して、［編集］をクリックします。
3. 値を **true** に変更します。



4. Citrix Endpoint Management コンソールで、再度 MDX アプリをアップロードします:

   a) ［構成］**>** ［アプリ］に移動し、種類（**MDX**）およびプラットフォームでアプリ一覧を絞り込みます。
   b) アプリを選択して、［編集］、［次へ］、［アップロード］の順にクリックします。
   c) MDX アプリごとに、この手順を繰り返します。

Web リンクの追加

Web リンクはインターネットサイトまたはイントラネットサイトの Web アドレスです。Web リンクは、SSO を必要としない Web アプリも参照できます。Web リンクの構成が完了すると、このリンクがアプリストアにアイコンとして表示されます。ユーザーが Citrix Secure Hub を使ってログオンすると、リンクは使用可能なアプリおよびデスクトップの一覧と共に表示されます。

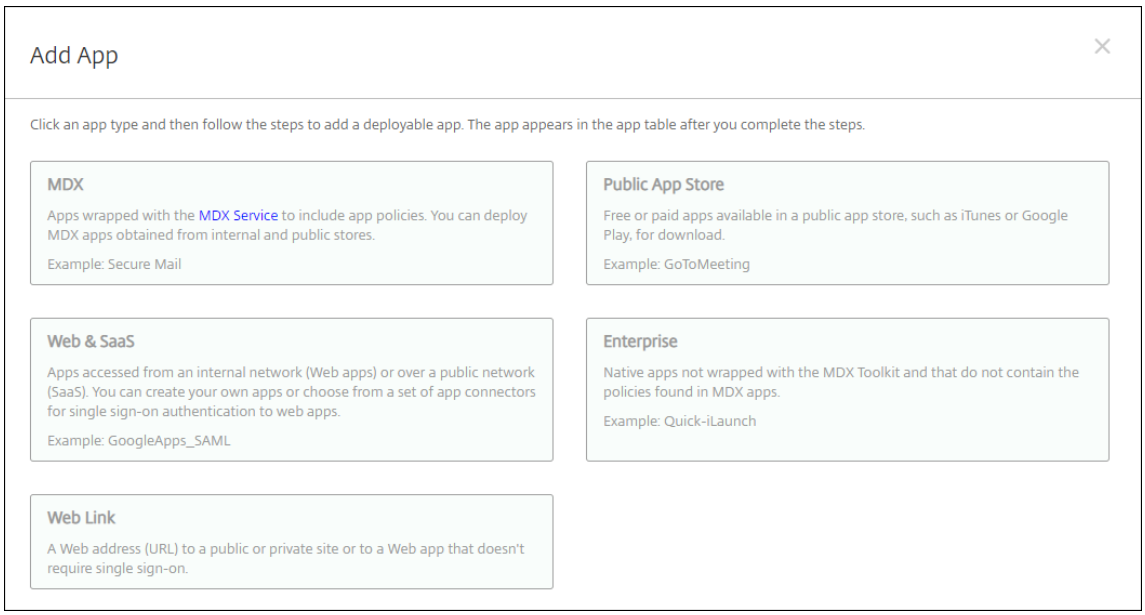
Web リンクの構成は、Citrix Endpoint Management コンソールの ［アプリ］タブで行うことができます。Web リンクの構成が完了すると、リンクは ［アプリ］の表にある一覧にリンクアイコンとして表示されます。ユーザーが Citrix Secure Hub を使ってログオンすると、リンクは使用可能なアプリおよびデスクトップの一覧と共に表示されます。

詳しくは、このビデオをご覧ください:

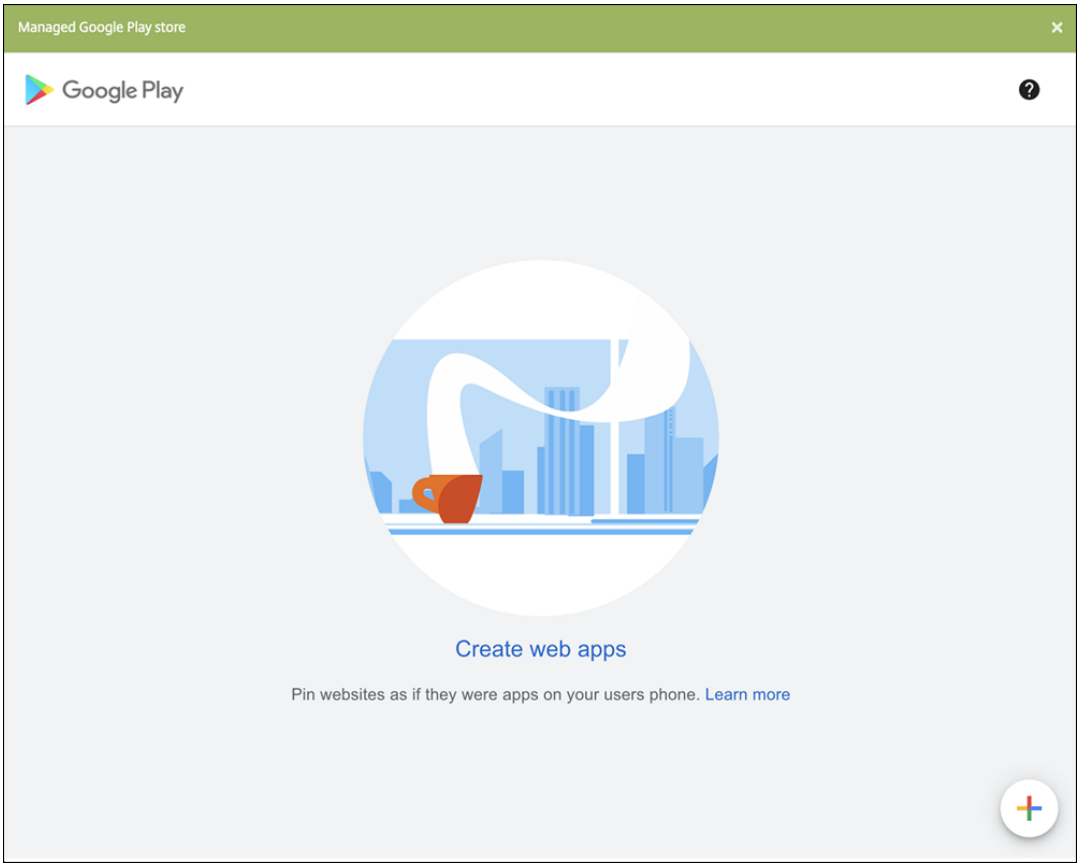
リンクを追加するには、次の情報を指定します:

- リンクの名前
- リンクの説明
- Web アドレス（URL）
- カテゴリ
- 役割
- .png 形式の画像（オプション）

1. Citrix Endpoint Management コンソールで、［構成］**>**［アプリ］**>**［追加］の順にクリックします。［アプリの追加］ダイアログボックスが開きます。

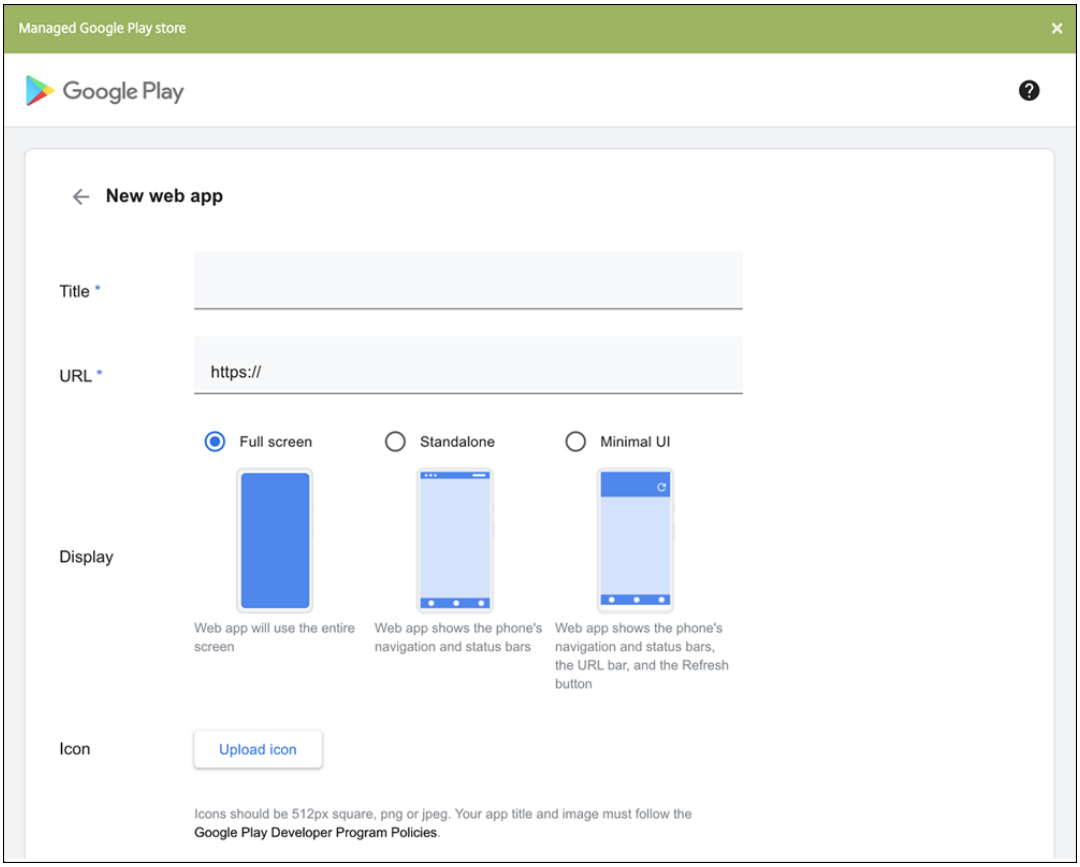


2. [**Web** リンク] をクリックします。[アプリ情報] ページが開きます。
3. [アプリ情報] ペインで、以下の情報を入力します:
   - 名前: アプリの説明的な名前を入力します。この名前は、[アプリ] の表の [アプリ名] の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。
   - アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリのカテゴリについて」を参照してください。
4. [次へ] をクリックします。アプリのプラットフォームページが開きます。
5. [プラットフォーム] で、[他のプラットフォーム] を選択して iOS、Android (従来のデバイス管理者)、Windows 8 用の Web アプリを追加するか、[**Android Enterprise**] を選択します。含めないプラットフォームのチェックボックスをオフにします。
   - [他のプラットフォーム] を選択した場合は、次の手順を続行して設定を構成します。
   - [**Android Enterprise**] を選択した場合、[アップロード] をクリックすると、管理対象 Google Play ストアが開きます。Web アプリを公開するために開発者アカウントを登録する必要はありません。右下隅にある [+] アイコンをクリックして続行します。



次の設定を構成します:

- タイトル: Web アプリの名前を入力します。
- **URL**: アプリの Web アドレスを入力します。
- 表示: ユーザーデバイスでの Web アプリの表示方法を選択します。使用可能なオプションは、[全画面]、[スタンドアロン]、および [最小 **UI**] です。
- アイコン: Web アプリ用の独自の画像をアップロードします。



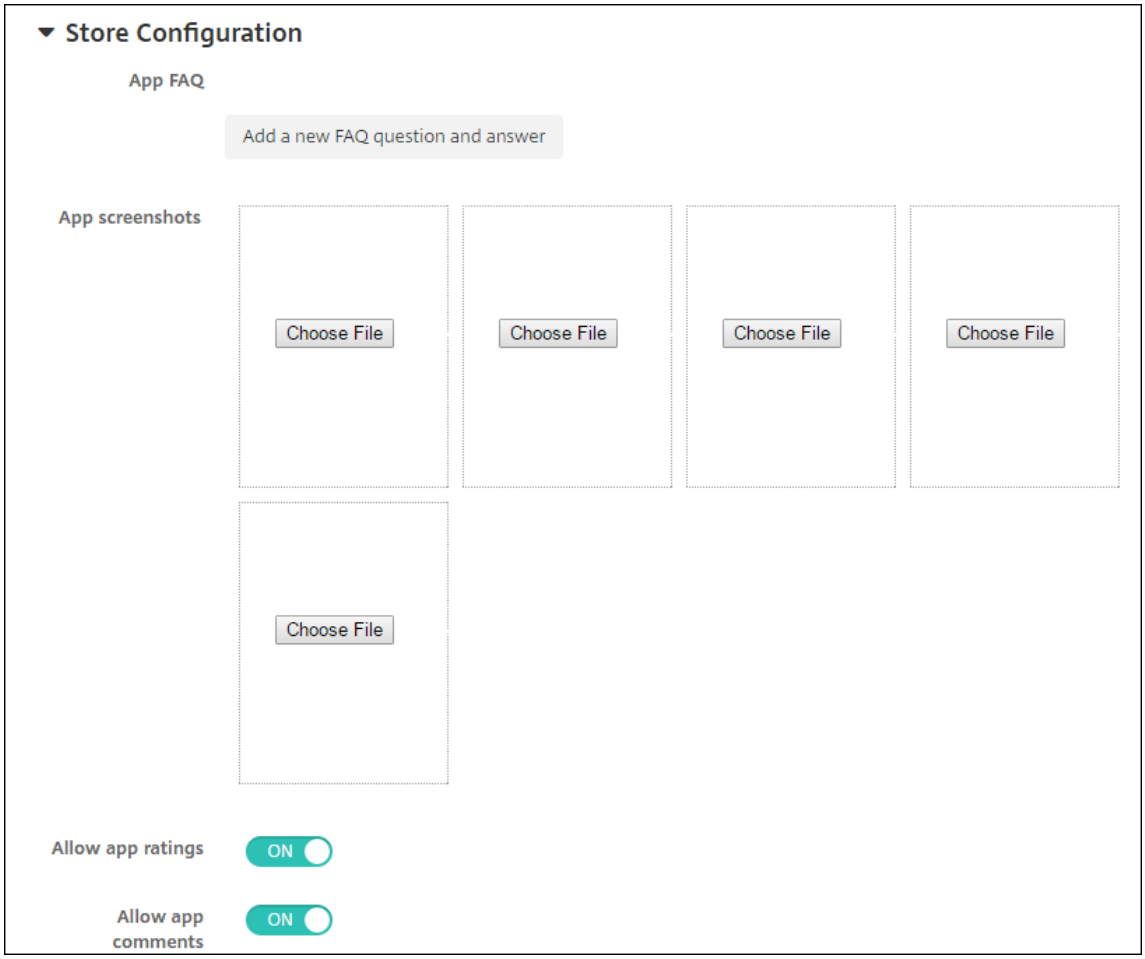
入力が終わったら、[作成]をクリックします。Web アプリが公開されるまでに最大 10 分かかる場合があります。

6. Android Enterprise 以外のプラットフォームでは、次の設定を構成します:

- アプリ名: 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- アプリの説明: 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL**: 事前に入力されている URL をそのまま使用するか、アプリの Web アドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
- アプリは内部ネットワークでホストされます: 内部ネットワークのサーバーでアプリを実行するかどうかを選択します。ユーザーがリモートから内部アプリに接続する場合は、NetScaler Gateway Gateway を介して接続する必要があります。このオプションを［オン］に設定すると、VPN キーワードがアプリに追加され、NetScaler Gateway Gateway を介して接続できるようになります。デフォルトは ［オフ］です。
- アプリカテゴリ: ドロップダウンリストから、アプリに適用する任意のカテゴリを選択します。
- イメージ: デフォルトの Citrix イメージを使用するのか、独自のアプリイメージをアップロードするのかを選択します。デフォルトは［デフォルトを使用］です。
  - 独自のイメージをアップロードする場合は、［参照］をクリックしてアップロードするファイルの場所に移動します。そのファイルは、.PNG ファイルである必要があります。JPEG ファイルや

GIF ファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。

7. 展開規則を構成します。詳しくは「展開規則の構成」を参照してください。
8. ［ストア構成］を展開します。



オプションで、以下を構成できます:

- アプリの **FAQ**:［新しい **FAQ** の質問と回答を追加］をクリックして、アプリに関する FAQ を作成します。
- スマホ/タブレット用のスクリーンショットを追加:アプリストアに表示される画面キャプチャを追加します。
- アプリ評価を許可:ユーザーがアプリストアでアプリを評価できるようにします。
- アプリコメントを許可:ユーザーがアプリストアのアプリにコメントを残すことを許可します。

9. ［次へ］をクリックします。［デリバリーグループ割り当て］ページが開きます。
10. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

11. ［展開スケジュール］を展開して以下の設定を構成します：

    - 展開：アプリをデバイスに展開するかどうかを選択します。デフォルトは ［オン］です。
    - 展開スケジュール：アプリを ［すぐに］展開するか、［後で］展開するかを選択します。［後で］を選択した場合は、アプリを展開する日時を設定します。デフォルトは ［すぐに］です。
    - 展開条件：［すべての接続で］を選択すると、デバイスが接続するたびにアプリを展開します。［以前の展開が失敗した場合のみ］を選択すると、以前にデバイスがアプリを受信できなかった場合にアプリを展開します。デフォルトは ［すべての接続で］です。

    ［常時接続に対する展開］オプションは、［設定］**>** ［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

    常時接続オプション：

    - iOS デバイスでは使用できません。
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
    - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません

    構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

12. ［保存］をクリックします。

Microsoft 365 アプリの有効化

MDX コンテナを開いて、Citrix Secure Mail、Citrix Secure Web、および Citrix Files が Microsoft Office 365 アプリにドキュメントやデータを転送するようにできます。詳しくは、「Office 365 アプリとのセキュアな対話式操作の許可」を参照してください。

ワークフローの適用

ワークフローを割り当てるか作成するには、次の設定を構成します：

- 使用するワークフロー：ドロップダウンリストから既存のワークフローを選択するか、［新しいワークフローの作成］をクリックします。デフォルトは ［なし］です。

  ［新しいワークフローの作成］を選択した場合は、次の設定を構成します。

  - 名前：ワークフローの固有の名前を入力します。
  - 説明：任意で、ワークフローの説明を入力します。

- メール承認テンプレート：一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
- マネージャー承認のレベル：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［1 つのレベル］です。選択できるオプションは以下のとおりです：
  * 不必要
  * 1 つのレベル
  * 2 つのレベル
  * 3 つのレベル
- **Active Directory** ドメインの選択：一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
- 追加の必須承認者を検索：検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］の一覧に表示されます。

  ［選択した追加の必須承認者］の一覧からユーザーを削除するには、次のいずれかを行います：
  * ［検索］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
  * 名前の全体または一部を検索ボックスに入力して ［検索］をクリックし、検索結果を絞り込みます。
  * ［選択した追加の必須承認者］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

アプリストアおよび **Citrix Secure Hub** のブランド設定

ストアでのアプリの表示方法を設定したり、Citrix Secure Hub およびアプリストアにロゴを追加したりすることができます。このブランド設定機能は、iOS および Android デバイスでのみ利用できます。

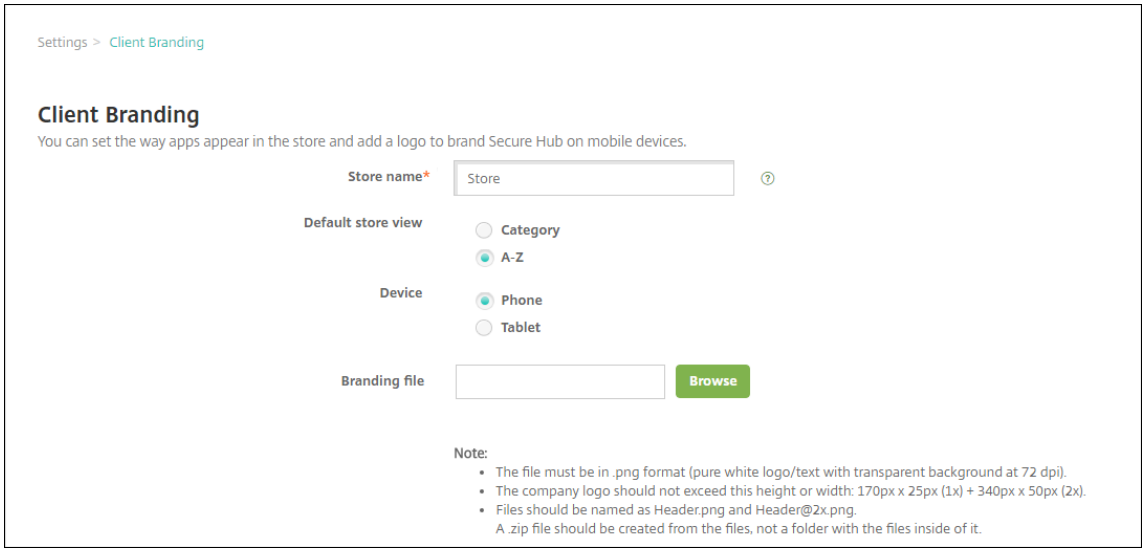
始める前に、カスタム画像を準備してアクセスできるようにしてください。

カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png 形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社のロゴは次の高さと幅以内である必要があります：170px x 25px（1x）および 340px x 50px（2x）。
- ファイルに`Header.png`および`Header@2x.png`という名前を付けます。
- ファイルを含むフォルダーではなく、ファイルから.zip ファイルを作成します。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。

2. ［クライアント］で ［クライアントブランド化］をクリックします。［クライアントブランド化］ページが開きます。



次の設定を構成します:

- ストア名: ユーザーのアカウント情報にストア名が表示されます。この名前を変更すると、ストアサービスへのアクセスに使用される URL も変更されます。通常、デフォルトの名前をそのまま使用します。

  > 重要:
  >
  > ストア名に使用できるのは英数字のみです。

- デフォルトストアビュー: ［カテゴリ］または ［**A**～**Z**］を選択します。デフォルトは ［**A**～**Z**］です。
- デバイスのオプション: ［電話］または ［タブレット］を選択します。デフォルトは ［電話］です。
- **Branding file**: ［**Browse**］をクリックしてブランド設定に使用するイメージまたはイメージの.zip ファイルの場所に移動し、ファイルを選択します。

3. ［保存］をクリックします。

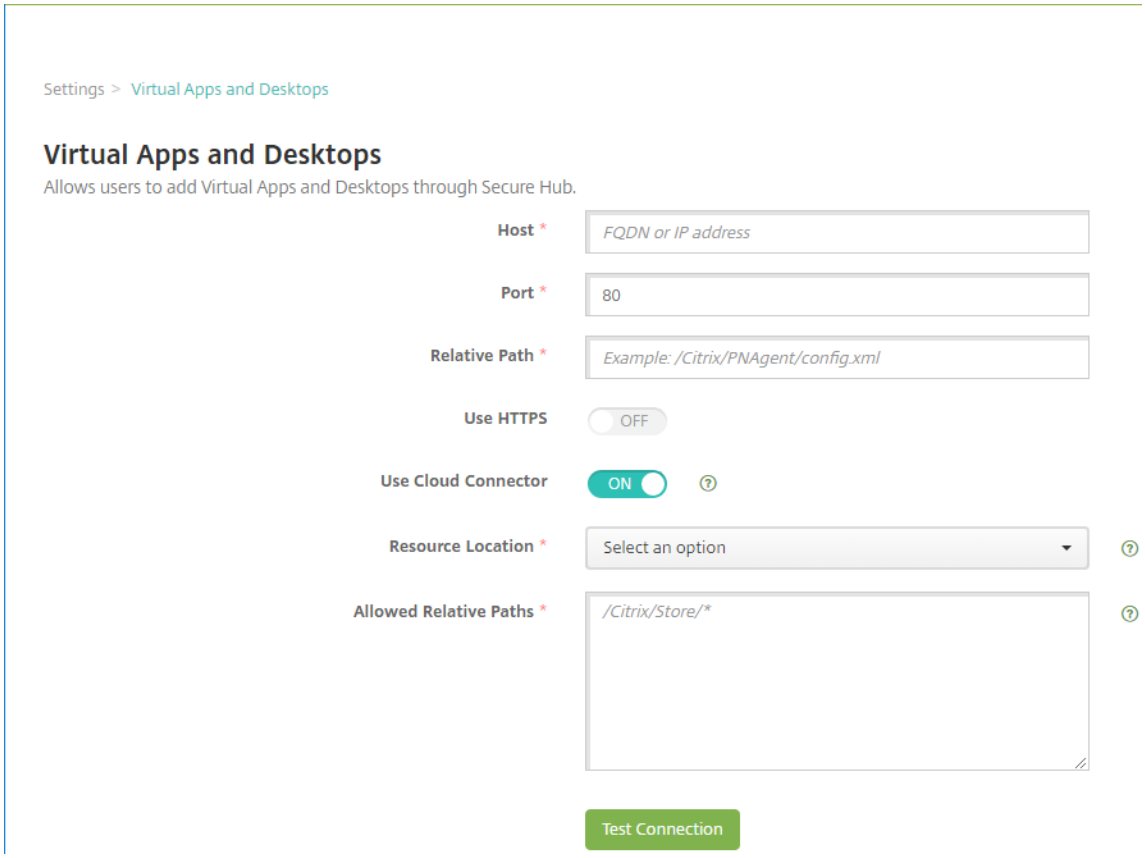
このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、展開します。

アプリストア経由の **Citrix Virtual Apps and Desktops**

Citrix Endpoint Management では、Citrix Virtual Apps and Desktops からアプリを収集して、アプリストアでモバイルデバイスユーザーにそのアプリを配布できます。ユーザーは、アプリストア内から直接アプリをサブスクライブして、Citrix Workspace から起動します。アプリを起動するには、ユーザーデバイスに Citrix Workspace アプリをインストールする必要があります。

この設定を構成するには、オンプレミス StoreFront の完全修飾ドメイン名（Fully Qualified Domain Name: FQDN）または IP アドレスと、ポート番号が必要です。

1. Citrix Endpoint Management Web コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [**Virtual Apps and Desktops**] をクリックします。[**Virtual Apps and Desktops**] ページが開きます。



3. 次の設定を構成します:

   - ホスト: StoreFront の完全修飾ドメイン名（FQDN）または IP アドレスを入力します。
   - ポート: StoreFront のポート番号を入力します。デフォルトは 80 です。
   - 相対パス: パスを入力します。たとえば、「/Citrix/PNAgent/config.xml」と入力します。
   - **HTTPS** の使用: StoreFront とクライアントデバイスの間で安全な認証を有効にするかどうかを選択します。デフォルトは [オフ] です。
   - **Cloud Connector** を使用します: [オン] を選択して Cloud Connector を使用し、StoreFront サーバーに接続します。次に、[リソースの場所] と接続を [許可する相対パス] を指定します。
     - リソースの場所: Citrix Cloud Connectorで定義されているリソースの場所から選択します。
     - 許可する相対パス: 指定したリソースの場所に対して許可する相対パス。1 行に 1 つのパスを指定します。ワイルドカード文字としてアスタリスク（*）を使用できます。

     リソースの場所が`https://StoreFront.company.com`で、次の URL へのアクセスを提供する場合。

- https://StoreFront.company.com/Citrix/PNAgent/Config.xml
- https://StoreFront.company.com/Citrix/PNAgent/enum.aspx
- https://StoreFront.company.com/Citrix/PNAgent/launch.aspx

URL https://StoreFront.company.com/Citrix/PNAgent/*ですべてのリクエストを許可するには、次のパスを入力します。/Citrix/PNAgent/*

Citrix Endpoint Management は他のすべてのパスをブロックします。

4. ［接続のテスト］をクリックして、Citrix Endpoint Management が特定の StoreFront サーバーに接続可能なことを検証します。
5. ［保存］をクリックします。

アプリコネクタの種類

March 15, 2024

次の表に、Web アプリまたは SaaS アプリを追加する場合に Citrix Endpoint Management 内で使用できるコネクタとコネクタの種類を示します。Web または SaaS アプリを追加すると、新しいコネクタを追加することもできます。

この表は、各コネクタがユーザーアカウント管理をサポートするかどうかについて示します。ユーザーアカウント管理がサポートされる場合、管理者は新しいアカウントを自動的に作成したり、ワークフローを使って作成したりできます。

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
EchoSign_SAML	Y	Y
Globoforce_SAML		注：このコネクタを使用する場合は、プロビジョニングのユーザー管理を有効にして、シームレスな SSO 統合が行われるようにする必要があります。
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
Salesforce_SAML_SP	Y	Y
SandBox_SAML	Y	
SuccessFactors_SAML	Y	
ShareFile_SAML	Y	
ShareFile_SAML_SP	Y	
WebEx_SAML_SP	Y	Y

Citrix Launcher

March 15, 2024

Citrix Launcher を使用すると、Citrix Endpoint Management によって展開された Android Enterprise デバイスおよび従来の Android デバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix Launcher を使用すると、ユーザーが特定のデバイス設定にアクセスできないようにし、1 つのアプリまたは少数のアプリセットにデバイスを制限できます。

Citrix Launcher の Citrix Secure Hub 管理でサポートされる Android の最小バージョンは、Android 6.0 です。

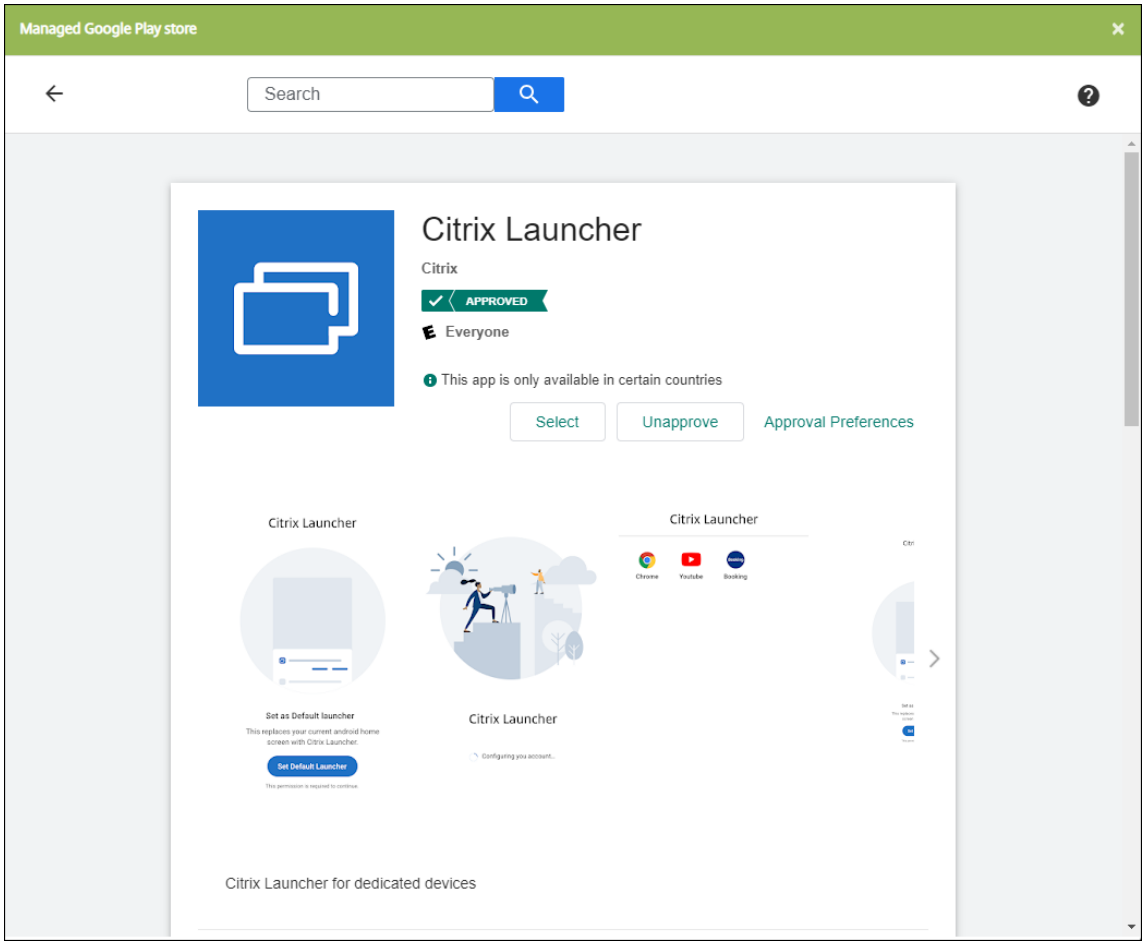
Launcher 構成ポリシーを使用すると、次の Citrix Launcher 機能を制御できます:

- ユーザーが指定したアプリにのみアクセスできるように、Android Enterprise デバイスと従来の Android デバイスを管理する。
- Citrix Launcher アイコンのカスタムロゴ画像と、Citrix Launcher のカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

Citrix Launcher は、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Android Enterprise デバイス用の **Citrix Launcher** のセットアップ

1. Citrix Launcher アプリ（com.citrix.launcher.droid）をパブリックストアアプリとして Citrix Endpoint Management に追加します。［構成］**>** ［アプリ］で、［追加］ > ［パブリックアプリストア］の順にクリックします。詳しくは、「パブリックアプリケーションストアのアプリケーションの追加」を参照してください。



2. キオスクデバイスポリシーで、専用の会社所有デバイス（Android 特定業務専用コーポレート所有端末（COSU）とも呼ばれる）で使用可能にする必要があるアプリを指定します。[構成] > [デバイスポリシー] に移動して [追加] をクリックし、[キオスク] を選択します。次に、Citrix Launcher アプリおよび許可リストにある追加のアプリを選択します。以前、アプリをリストに追加している場合は、アプリを再度アップロードする必要はありません。詳しくは、「Android Enterprise の設定」を参照してください。

3. Launcher 構成デバイスポリシーを追加します。[構成] > [デバイスポリシー] に移動して [追加] をクリックし、[**Launcher** 構成] を選択します。Launcher 構成ポリシーで、キオスクポリシーで指定したアプリを追加します。キオスクポリシーで指定したすべてのアプリを追加する必要はありません。Citrix Launcher アプリは、キオスクポリシーにのみ追加する必要があります。詳しくは、「Launcher 構成ポリシー」を参照してください。

4. デリバリーグループを作成し、リソースを展開します。詳しくは、以下の「デリバリーグループの追加とリソースの展開」セクションを参照してください。

Citrix Launcher を会社所有の専用の Android Enterprise デバイスに展開した後、Citrix Endpoint Management はアプリをインストールし、デフォルトの Citrix Secure Hub ランチャーを置き換えます。Citrix Launcher アプリを終了すると、Citrix Secure Hub が再びデフォルトのランチャーになります。

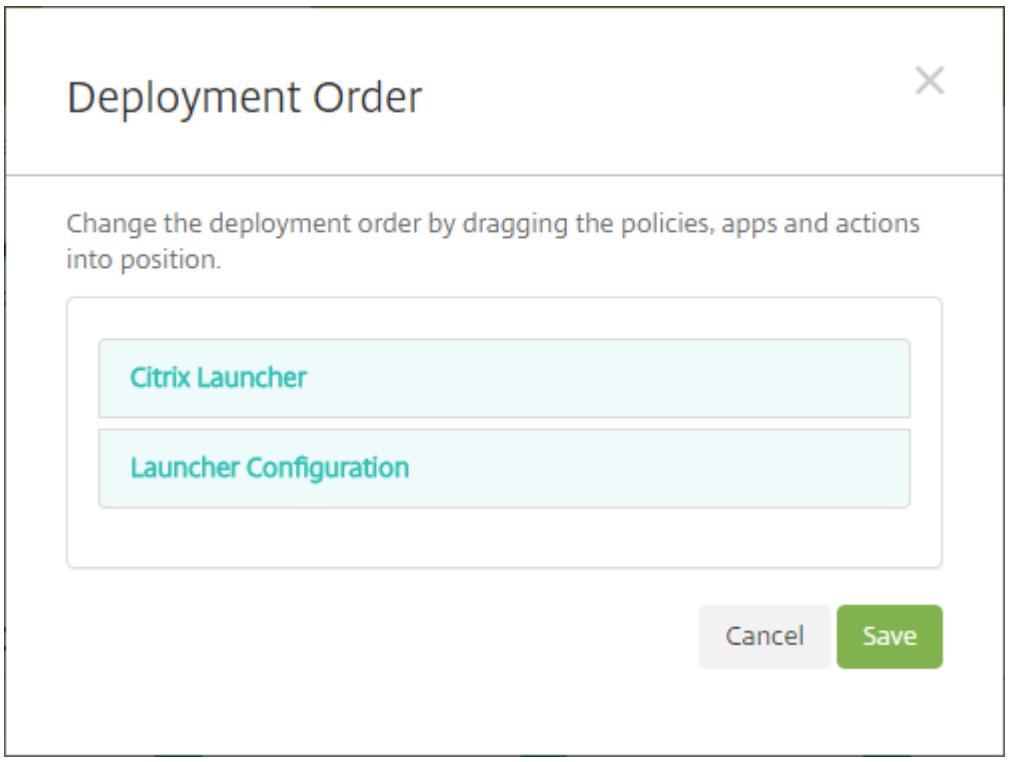
従来の **Android** デバイス用の **Citrix Launcher** のセットアップ

> 注:
>
> 2020 年 8 月、Citrix は従来の Android デバイス用の CitrixLauncher.apk のサポートを廃止しました。新機能のアップデートを受け取らなくても、Android デバイス用の従来の Citrix Launcher アプリ（com.citrix.launcher）は引き続き使用できます。

1. Citrix Launcher アプリを見つけるには、Citrix Endpoint Management のダウンロードページに移動して **Citrix Launcher** を検索します。最新のファイルをダウンロードします。ファイルは Citrix Endpoint Management にアップロードできる状態で、ラッピングを必要としません。
2. Launcher 構成デバイスポリシーを追加します。［構成］**>** ［デバイスポリシー］に移動して ［追加］をクリックし、［**Launcher** 構成］を選択します。詳しくは、「Launcher 構成ポリシー」を参照してください。
3. Citrix Launcher アプリをエンタープライズアプリとして Citrix Endpoint Management に追加します。［構成］**>** ［アプリ］で、［追加］、［エンタープライズ］の順にクリックします。詳しくは、「エンタープライズアプリの追加」を参照してください。
4. デリバリーグループを作成し、リソースを展開します。詳しくは、以下の「デリバリーグループの追加とリソースの展開」セクションを参照してください。

デリバリーグループの追加とリソースの展開

1. ［構成］**>** ［デリバリーグループ］で次のように構成して、Citrix Launcher のデリバリーグループを作成します。
   - ［ポリシー］ページで、［**Launcher** 構成ポリシー］を追加します。
   - ［アプリ］ページで、**Citrix Launcher** を ［必須アプリ］にドラッグします。
   - ［**Summary**］ページで ［**Deployment Order**］をクリックして、**Citrix Launcher** アプリが **Launcher Configuration** ポリシーよりも先であることを確認します。



2. デリバリーグループのすべてのユーザーにプッシュ通知を送信して、デリバリーグループにリソースを展開します。デリバリーグループへのリソースの追加について詳しくは、「リソースの展開」を参照してください。

Citrix Launcher を使用しないデバイスの管理

Citrix Launcher を使用する代わりに、既に利用可能な機能を使用できます。

専用デバイスをプロビジョニングするには:

1. デバイス所有者モードを専用デバイスに設定して、登録プロファイルを作成します。「Android Enterprise 専用デバイスのプロビジョニング」および「登録プロファイル」を参照してください。
2. キオスクデバイスポリシーを作成して、アプリを許可リストに追加し、ロックタスクモードを設定します。以前、アプリをリストに追加している場合は、アプリを再度アップロードする必要はありません。詳しくは、「Android Enterprise の設定」を参照してください。
3. 作成した登録プロファイルに各デバイスを登録します。

Apple の一括購入を使用したアプリの追加

November 29, 2023

Apple Business Manager（ABM）と Apple School Manager（ASM）を使用すると、アプリやブックのライセンスを一括で購入し、一括購入情報を Citrix Endpoint Management と同期することができます。その後、Citrix Endpoint Management を使用して、これらのアプリとブックを iOS および macOS デバイスに展開できます。コンテンツの一括購入は、1 つの組織のアプリやブックを検索、購入、配信するプロセスを簡素化します。

ABM または ASM を使用してコンテンツを購入することについて詳しくは、「Apple Business Manager ユーザーガイド」または「Apple School Manager ユーザーガイド」を参照してください。この記事では、ABM および ASM で一括購入したライセンスを Citrix Endpoint Management に同期する方法と、ライセンスを管理する方法について説明します。

> 注:
>
> Apple Volume Purchase Program（VPP）は、2021 年 1 月 14 日をもって利用できなくなりました。一括購入機能は ABM と ASM に統合されました。現在、デバイス登録プログラム（DEP：Device Enrollment Program）、または VPP を使用している場合は、ABM または ASM にアップグレードできます。詳しくは、Apple ドキュメントの「Apple Deployment Program からアップグレードする」を参照してください。

Apple の一括購入について

ABM または ASM を使用してコンテンツを一括購入する場合は、以下の点に注意してください：

- 次のコンテンツのライセンスを購入できます：
  - 公開アプリおよびブック
  - 組織向けに特別に開発されたカスタムアプリ
- 一括購入したアプリやブックを、組織が所有するデバイスや BYO デバイスに展開できます。ABM または ASM で登録した組織所有のデバイスでは、MDM（モバイルデバイス管理）登録または MDM+MAM 登録がサポートされており、MAM（モバイルアプリケーション管理）登録はサポートされていません。
- アプリの配布については、「Apple アプリの配布」を参照してください。
- 既知の問題の一覧については、Knowledge Center 記事のCTX222633を参照してください。

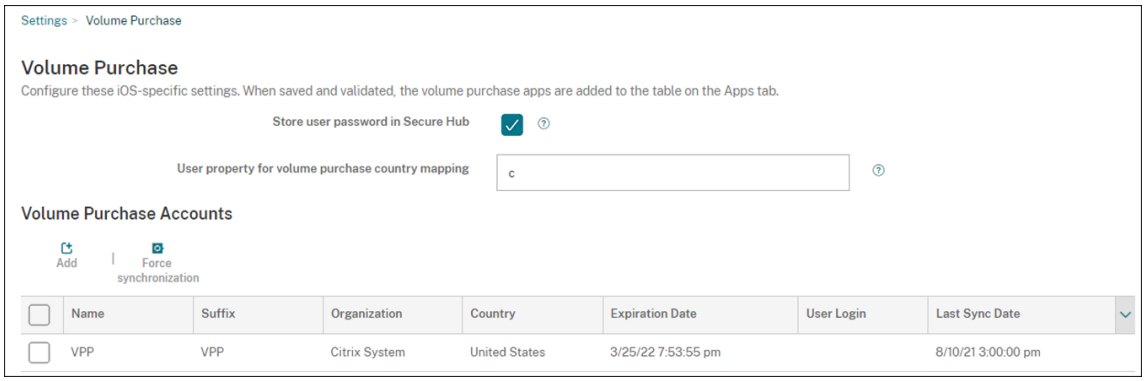
一括購入アカウントの追加

ABM または ASM ポータルでコンテンツを購入した後、Citrix Endpoint Management に関連付けられたコンテンツトークンをポータルからダウンロードします。次に、Citrix Endpoint Management で、このコンテンツコードに基づいて一括購入アカウントを作成します。このコードにより、Citrix Endpoint Management は ABM または ASM からのコンテンツライセンスを同期できます。

一括購入では、管理対象のライセンスを使用してコンテンツを購入し、デバイスに展開できます。現在引き換えコードを使用中で、管理対象のライセンスに変更する場合は、Apple 社のサポートドキュメントを参照してください。

Citrix Endpoint Management に一括購入アカウントを追加するには

1. ABM または ASM ポータルで、必要に応じてコンテンツを購入し、コンテンツコードファイルを安全な場所にダウンロードします。
2. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
3. ［一括購入］をクリックします。［一括購入］構成ページが開きます。

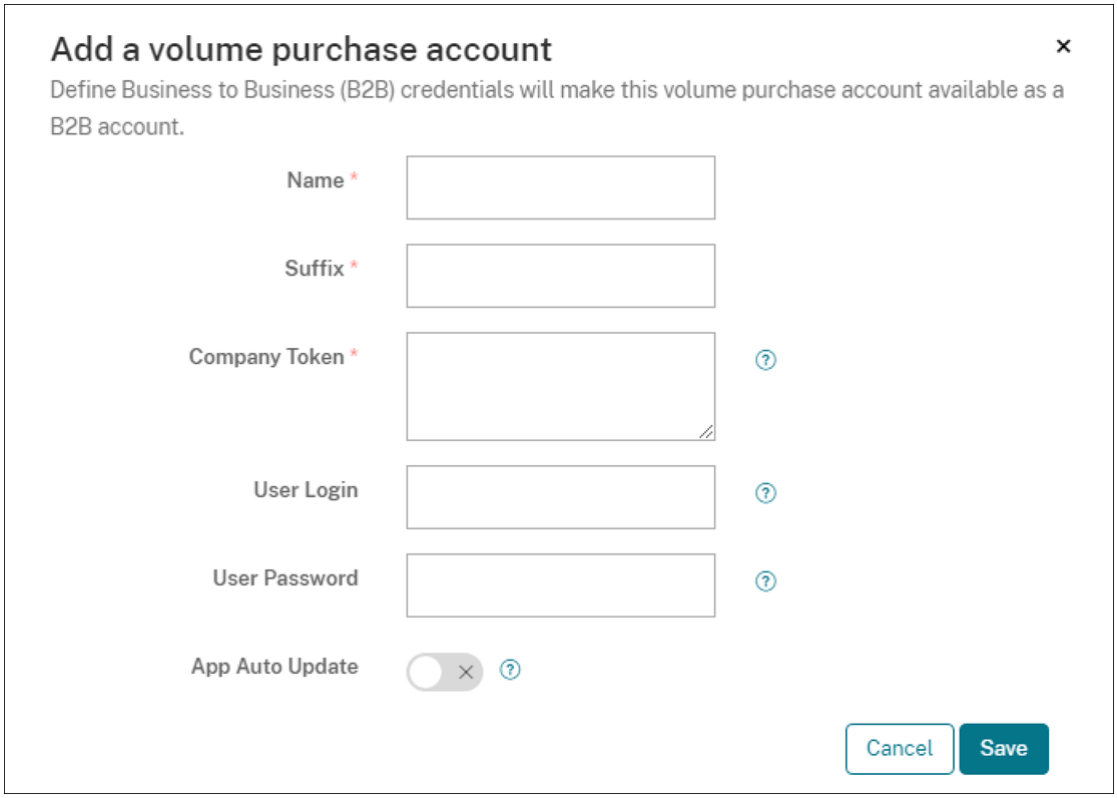


4. 次の設定を構成します：

   - **Citrix Secure Hub** のユーザーパスワードを保存する： Citrix Endpoint Management 認証用のユーザー名とパスワードを Citrix Secure Hub に保存するかどうかを選択します。デフォルトは ［オン］です。
   - 一括購入国ユーザープロパティマッピング：ユーザーが国固有のアプリストアからアプリをダウンロードできるようにする国マッピングコードを入力します。このコードについては、コンテンツマネージャーにお問い合わせください。

     Citrix Endpoint Management は、この国マッピングコードを使用して、一括購入のプロパティプールを選択します。たとえば、ユーザープロパティが米国で、マッピングコードが日本の場合、そのユーザーはアプリをダウンロードできません。

5. ［追加］をクリックします。［一括購入アカウントの追加］ダイアログボックスが開きます。



6. 次のアカウント設定を構成します：

> 注：
>
> Apple Configurator 1 を使用している場合、次の手順でライセンスファイルをアップロードします：［構成］>［アプリ］をクリックし、アプリのプラットフォームページに移動してから、［一括購入］を開きます。

- 名前：アカウントを識別するためのわかりやすい名前を入力します。
- サフィックス： Apple ストアから継承したアプリ名とともに表示されるサフィックスを入力します。たとえば、「**VP**」と入力すると、**Citrix Secure Mail** アプリはアプリ一覧で「**Citrix Secure Mail - VP**」と表示されます。
- 会社トークン：手順 1 でダウンロードしたコンテンツトークンをコピーして貼り付けます。
- ユーザーログイン：（オプション）この一括購入アカウントの管理者のユーザー名を入力します。構成されている場合、一括購入したカスタムアプリを Citrix Endpoint Management に同期するには、ユーザー名とパスワードが必要です。
- ユーザーパスワード：（オプション）入力したユーザー名のパスワードを入力します。
- アプリの自動更新：この設定がオンの場合、新しいバージョンが使用可能になったときに、Citrix Endpoint Management コンソールで一括購入アプリと任意アプリが自動的に更新されます。ただし、エンタープライズアプリとパブリックアプリストアのアプリは、Citrix Endpoint Management コンソールで手動で更新する必要があります。この設定がオフの場合でも、一括購入アプリは Citrix Endpoint Management コンソールで手動で更新できます。コンソールでアプリが更新されると、アプリがインストールされているデバイスもその更新を受け取ります。デフォルトは ［オフ］です。

一括アカウントが正常に追加されると、次のことを通知するメッセージが表示されます:

- ［構成］**>**［アプリ］ページでは、一括購入したアプリがアプリ一覧に表示されます。アプリ名は、構成したサフィックスとともに表示されます。
- ［構成］**>**［メディア］ページでは、一括購入したブックがメディア一覧に表示されます。ブック名は、構成したサフィックスとともに表示されます。

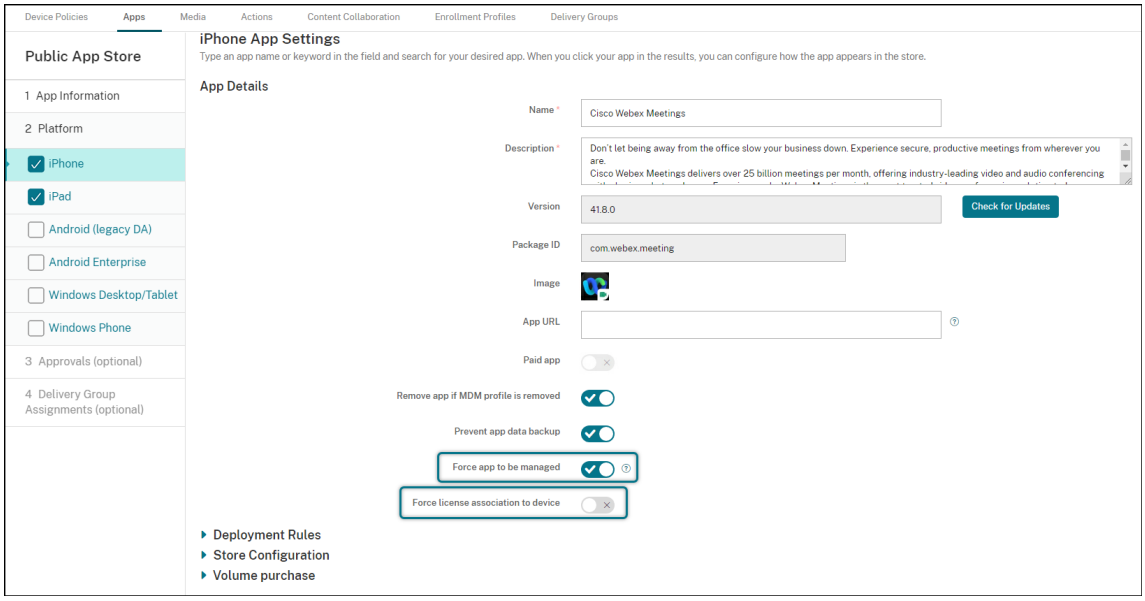
一括購入アプリの構成

一括購入アカウントを追加すると、アプリ情報は Citrix Endpoint Management に同期され、［構成］**>**［アプリ］ページに表示されます。これらのアプリを構成し、iOS および macOS デバイスのデリバリーグループおよびデリバリーポリシー設定を調整できるようになりました。この構成を完了すると、ユーザーはデバイスを登録できるようになります。

一括購入アプリを構成するときは、次の設定に注意してください:

- ［構成］**>**［アプリ］ページで:
  - Citrix Endpoint Management がアプリをユーザーではなくデバイスに展開できるようにするには、［デバイスへの強制ライセンス割り当て］をオンにします。この設定がオンのとき、ユーザーは Apple ID を使用する必要がなく、App Store アカウントにサインインしなくてもアプリをダウンロードできます。
  - アプリの ［管理されるアプリ］をオンにして、管理対象アプリとして自動的にインストールされるようにすることをお勧めします。

> 注:
>
> ［管理されるアプリ］設定を有効にするには、［設定］**>**［サーバープロパティ］ページのサーバープロパティ`apple.app.force.managed`を ［**True**］に構成する必要があります。詳しくは、「サーバープロパティ」を参照してください。



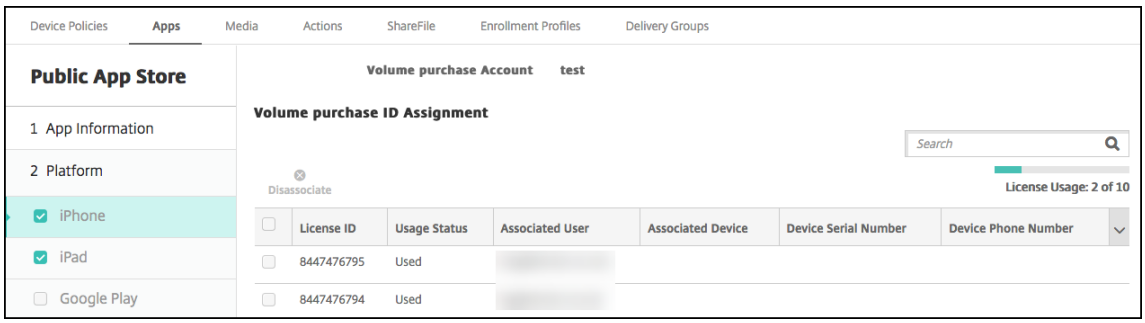
- ［構成］**>**［デリバリーグループ］ページで:

  ユーザーとのやりとりを最小限にしてアプリをユーザーデバイスにサイレントインストールするには、［アプリ］ページに移動し、［必須アプリ］一覧にアプリをドラッグします。デフォルトでは、Citrix Secure Hub 以外のアプリは ［任意アプリ］になります。つまり、ユーザーは Citrix Secure Hub を介してアプリのインストールを手動で開始する必要があります。

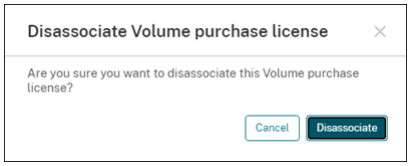
アプリライセンス使用の追跡および管理

アプリのライセンス使用状況を追跡できます。必要に応じて、使用されているライセンスを取り消し、そのライセンスを別のユーザーまたはデバイスで使用できるようにすることができます。

1. ［構成］**>**［アプリ］をクリックします。
2. アプリを選択し、［編集］をクリックします。
3. ［プラットフォーム］ページに移動し、［一括購入］を開きます。
   ［一括購入 **ID** 割り当て］の表では、使用されているライセンスの数と、使用しているのがユーザーかデバイスかという情報を追跡できます。



4. ライセンスを取り消すには、ライセンスを選択し、［割り当て解除］をクリックします。

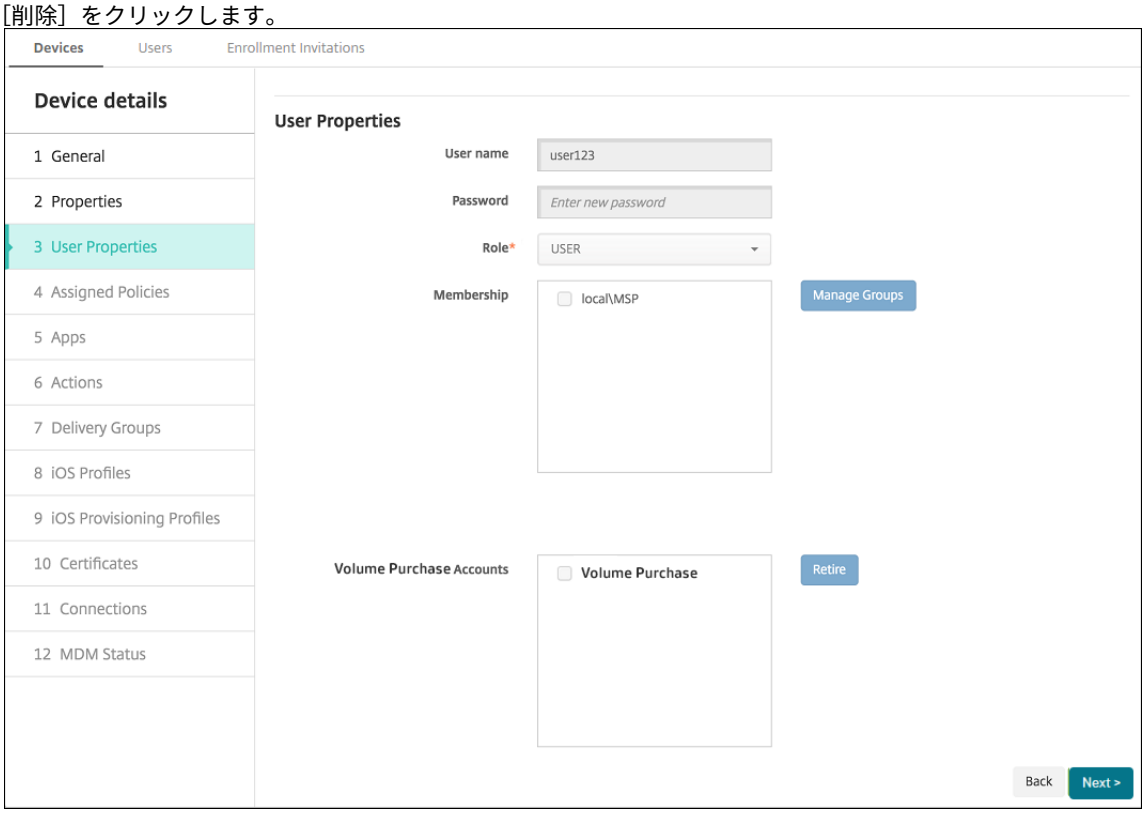


5. ［割り当て解除］をクリックして、その操作を確認します。

一括購入アカウントからのユーザーの削除

アプリライセンスをユーザーに関連付けると、一括購入アカウントからユーザーを削除して、それらのユーザーに割り当てられているすべてのライセンスを取り消すことができます。ユースケースには、ユーザーが組織から離れる場合などがあります。

1. ［管理］**>**［デバイス］の順にクリックします。
2. ターゲットユーザーに属するデバイスを選択し、［編集］をクリックします。
3. ［ユーザープロパティ］ページに移動し、必要に応じて一括購入アカウントを選択します。
4. ［削除］をクリックします。



Citrix Endpoint Management は、選択した一括購入アカウントのユーザーのアプリライセンスを取り消します。

アプリ情報の同期

Citrix Endpoint Management は、ABM または ASM でアプリ情報を定期的に同期します。必要に応じて、アプリ情報を手動で同期できます。同期により、アプリのライセンスとその他のアプリ情報にすべての変更が反映されます。このような変更には、一括購入アカウントからアプリを手動で削除する場合も含まれます。

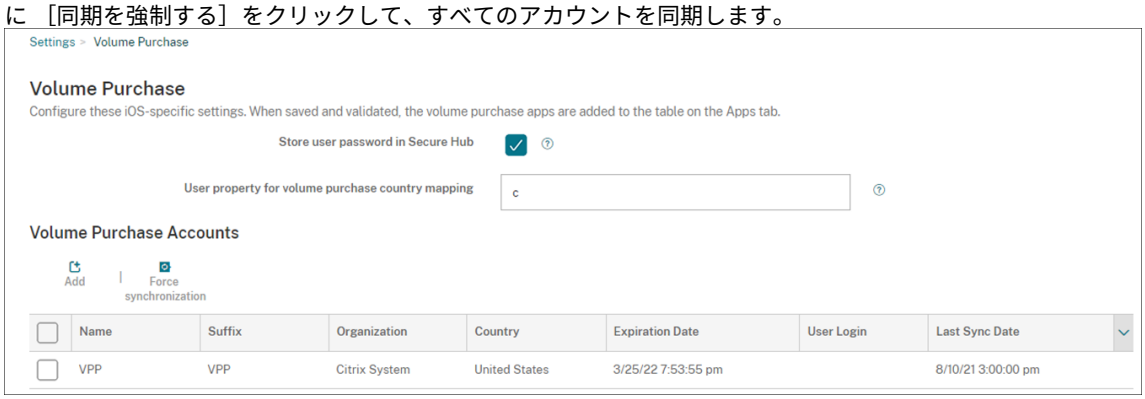
デフォルトの同期間隔の変更

デフォルトで、Citrix Endpoint Management は一括購入ライセンスの基準を最低 1440 分（24 時間）ごとに更新します。Citrix Cloud 管理者は、サーバープロパティ`vpp.baseline`を使用してデフォルトの同期間隔を変更できます。詳しくは、「サーバープロパティ」を参照してください。

アプリ情報の手動による同期

ABM または ASM で同期を強制し、最新のアプリ情報をすぐに取得できます。

1. ［設定］**>**［一括購入］をクリックします。
2. 一括購入アカウントを選択し、［同期を強制する］をクリックします。または、一括購入アカウントを選択せずに ［同期を強制する］をクリックして、すべてのアカウントを同期します。



3. 同期操作を確認します。同期が開始されます。

   一括購入ライセンスの数によっては、同期に数分かかることがあります。同期が完了すると、Citrix Endpoint Management は ［一括購入］ページを更新し、新規追加された ［最後の同期日付］列の同期日時を更新します。

アプリの更新のチェック

一括購入アカウントを追加するときに ［アプリの自動更新］設定をオンにすると、Citrix Endpoint Management は一括購入アプリと任意アプリの新しいバージョンを定期的にチェックし、更新を行います。必要に応じて、アプリの新しいバージョンを手動で確認し、そのアプリの更新を Citrix Endpoint Management に適用できます。

Citrix Endpoint Management は、必要なアプリの新しいバージョンを受信すると、ユーザーにプロンプトを表示せずに、新しいバージョンをデバイスにプッシュしてサイレントインストールします。

アプリの新しいバージョンを確認して適用するには

1. ［構成］**>**［アプリ］をクリックします。［アプリ］ページが開きます。
2. アプリを選択し、［編集］をクリックします。
3. ［プラットフォーム］ページに移動し、［バージョン］の横にある ［更新の確認］をクリックします。
4. ［プラットフォーム］ページに移動し、［バージョン］の横にある ［更新の確認］をクリックします。
5. 表示される ［更新］ダイアログボックスで、新しいバージョンを入手できる場合は更新を適用します。

一括購入アカウントのコンテンツトークンの更新

コンテンツトークンの有効期限は 1 年です。トークンの有効期限が近づくと、Citrix Endpoint Management はライセンスの有効期限の警告を表示します。ユーザーの妨げにならないように、コンテンツトークンを期限内に更新してください。

1. ABM ポータルまたは ASM ポータルから、更新されたトークンをダウンロードします。
2. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
3. ［一括購入］をクリックします。［一括購入］構成ページが開きます。
4. 更新されたトークン情報を使用して、一括購入アカウントを編集します。

ShareFile を **Citrix Endpoint Management** で使用する

March 15, 2024

Citrix Endpoint Management と ShareFile の統合には、2 つのオプションがあります。Citrix Files と StorageZone コネクタです。

Citrix Files

ShareFile アカウントへのアクセスを提供するように Citrix Endpoint Management を構成できます。この構成により以下の機能が実現します:

- モバイルユーザーに、ファイル共有、ファイル同期、ストレージゾーンコネクタなどの ShareFile の完全な機能セットへのアクセス権を与えることができます。

- 業務用モバイル アプリユーザーのシングルサインオン認証および包括的なアクセス制御ポリシーを Citrix Files で使用できます。
- Citrix Endpoint Management コンソールから ShareFile の構成、サービスレベルの監視、およびライセンスの使用状況の監視を行うことができます。

Enterprise アカウント用の Citrix Endpoint Management の構成について詳しくは、「Citrix Files での SAML によるシングルサインオン」を参照してください。

ストレージゾーンコネクタ

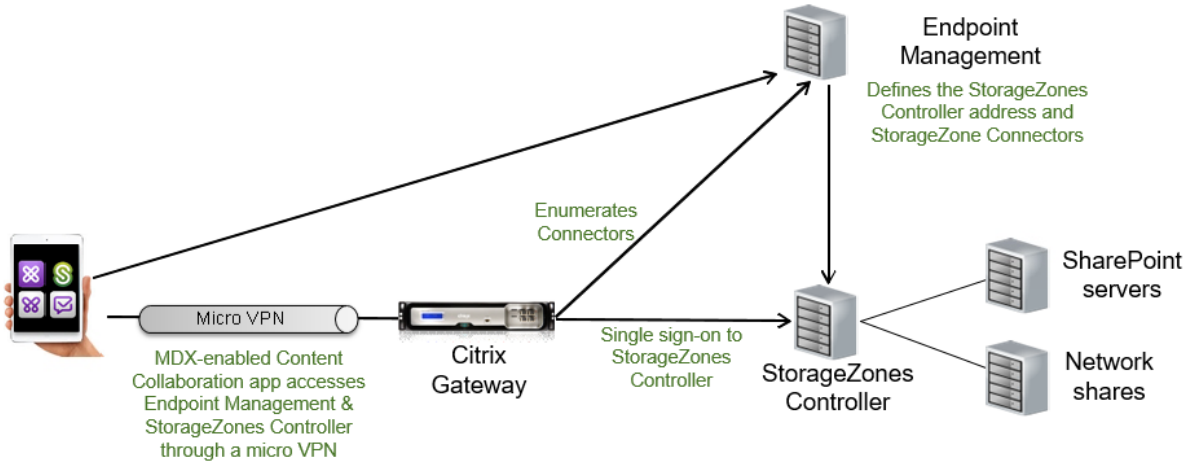
Citrix Endpoint Management コンソールで作成したストレージゾーンコネクタだけにアクセスできるように Citrix Endpoint Management を構成することも可能です。この構成により以下の機能が実現します:

- SharePoint サイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。
- ShareFile サブドメインの設定や Citrix Files データのホストが不要になります。
- iOS および Android 用の Citrix Files 向け Citrix 業務用モバイルアプリでデータにモバイルアクセスできます。Microsoft Office ドキュメントを編集できます。モバイル デバイスから Adobe PDF ファイルのプレビューおよび注釈もできます
- 社内ネットワーク外へのユーザー情報漏洩に対するセキュリティ規制に準拠します。
- Citrix Endpoint Management コンソールからストレージゾーンコネクタを簡単にセットアップできます。後で Citrix Endpoint Management で完全な Citrix Files 機能を使用することにした場合は、Citrix Endpoint Management コンソールで構成を変更できます。

Citrix Endpoint Management をストレージゾーンコネクタのみと統合する場合:

- ShareFile は、NetScaler Gateway Gateway へのシングルサインオン構成を使用して StorageZone Controller に対する認証を行います。
- Citrix Files コントロールプレーンが使用されないため、Citrix Endpoint Management での SAML 経由での認証は行われません。

次の図に、Citrix Endpoint Management とストレージゾーンコネクタを組み合わせて使う高度なアーキテクチャを示します。



要件

- 各コンポーネントの最小バージョンは次のとおりです。
  - ShareFile for iOS（MDX）5.3
  - ShareFile for Android（MDX）5.3
  - StorageZone Controller 5.11.20

    この記事では、StorageZone Controller 5.0 の構成方法を説明します
- Storage Zone Controller を実行するサーバーがシステム要件を満たしていることを確認してください。要件について詳しくは「System requirements（システム要件）」を参照してください。

Storage Zone for Citrix Files Data および制限付きストレージゾーンに関する要件は、Citrix Endpoint Management とストレージゾーンコネクタのみとの統合には適用されません。

Citrix Endpoint Management では、Documentum コネクタはサポートされません。

- PowerShell スクリプトを実行するには
  - スクリプトは、32 ビット（x86）バージョンの PowerShell で実行します。

インストール作業

Storage Zone Controller のインストールと設定を行うには、次の作業を記載順に実行します。これらの手順は、Citrix Endpoint Management とストレージゾーンコネクタのみとの統合に固有のものです。以下の記事の一部は、Storage Zone Controller のドキュメントのものです。

1. Storage Zone Controller 用の NetScaler の構成

   NetScaler Gateway を StorageZone Controller の DMZ プロキシとして使用できます。

2. SSL 証明書のインストール

   Storage Zone Controller で標準ゾーンをホストする場合、SSL 証明書が必要になります。Storage Zone Controller で制限付きゾーンをホストし、内部アドレスを使用する場合は、SSL 証明書は必要ありません。

3. サーバーの準備

   ストレージゾーンコネクタに対して IIS と ASP.NET を設定する必要があります。

4. Storage Zone Controller をインストールする

5. Storage Zone Controller をストレージゾーンコネクタのみで使用するように準備する

6. ストレージゾーンのプロキシサーバーを指定する

   Storage Zone Controller コンソールでは、Storage Zone Controller のプロキシサーバーを指定できます。プロキシサーバーは他の方法で指定することもできます。

7. 委任のために Storage Zone Controller を信頼するようにドメインコントローラーを構成する

   ネットワーク共有上または SharePoint サイト上の NTLM か Kerberos 認証をサポートするようにドメインコントローラーを構成します。

8. ストレージゾーンにセカンダリ Storage Zone Controller を統合する

   ストレージゾーンを高可用性に構成するには、2 つ以上の Storage Zone Controller を接続します。

Storage Zone Controller をインストールする

1. Storage Zone Controller ソフトウェアをダウンロードしてインストールします:

   a) Citrix Files のダウンロードページ（https://www.citrix.com/downloads/sharefile.html）でログオンして、最新の Storage Zone Controller インストーラーをダウンロードします。

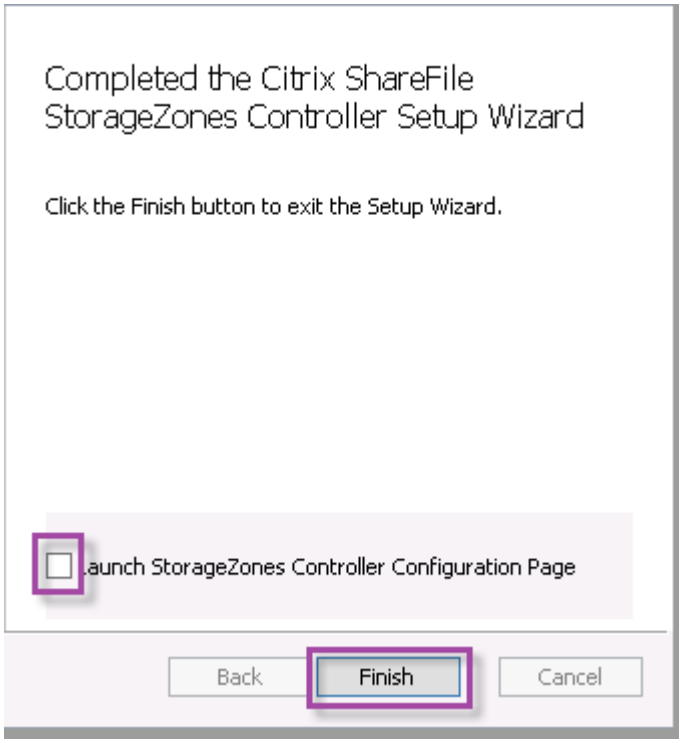
   b) Storage Zone Controller をインストールすると、サーバーのデフォルトの Web サイトが Storage Zone Controller のインストールパスに変更されます。デフォルトの Web サイトで匿名認証を有効にします。

2. Storage Zone Controller をインストールするサーバー上で StorageCenter.msi を実行します。

   Storage Zone Controller セットアップウィザードが起動します。

3. プロンプトに従ってインストールを進めます。

   - インターネットインフォメーションサービス（IIS：Internet Information Services）がデフォルトの場所にインストールされている場合、［ターゲットフォルダー］ページの設定はデフォルトのままにします。IIS がデフォルトの場所以外にインストールされている場合は、IIS のインストール先を指定します。
   - インストールが完了したら、［**Storage Zone Controller** の構成ページを起動］チェックボックスをオフにして ［完了］をクリックします。



4. メッセージが表示されたら、Storage Zone Controller を再起動します。
5. インストールが成功したかテストするために、`https://localhost/`にアクセスします。証明書エラーが発生した場合は、HTTP に変更して接続してください。インストールが成功すると、Citrix Files のロゴが表示されます。

   Citrix Files のロゴが表示されない場合は、ブラウザーのキャッシュを削除してもう一度アクセスしてください。

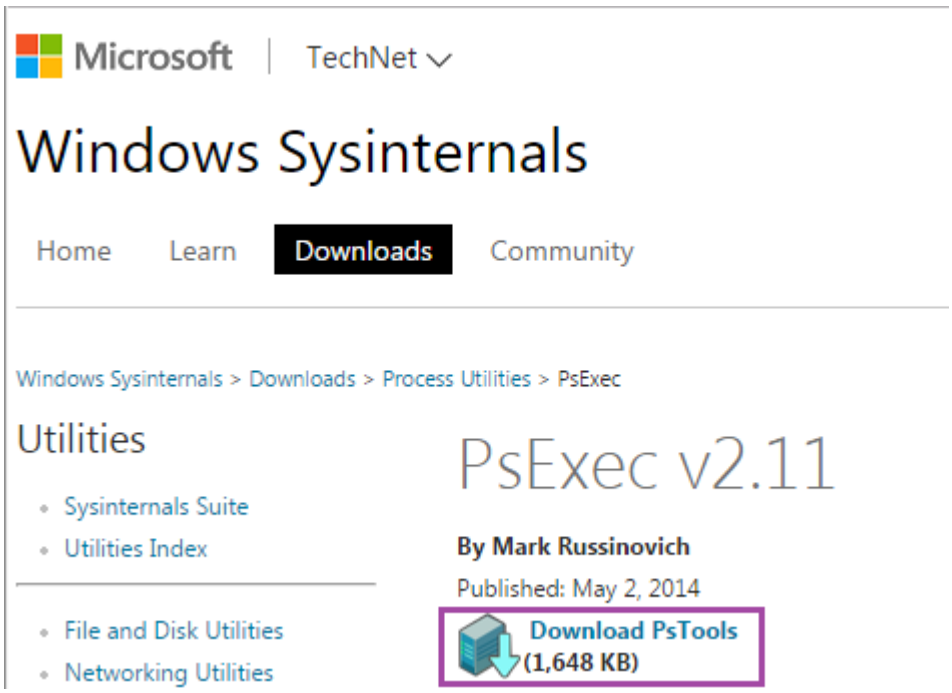
   > 重要:
   >
   > Storage Zone Controller を複製する予定がある場合は、Storage Zone Controller の構成を続ける前にディスクイメージをキャプチャします。

Storage Zone Controller をストレージゾーンコネクタのみで使用するように準備する

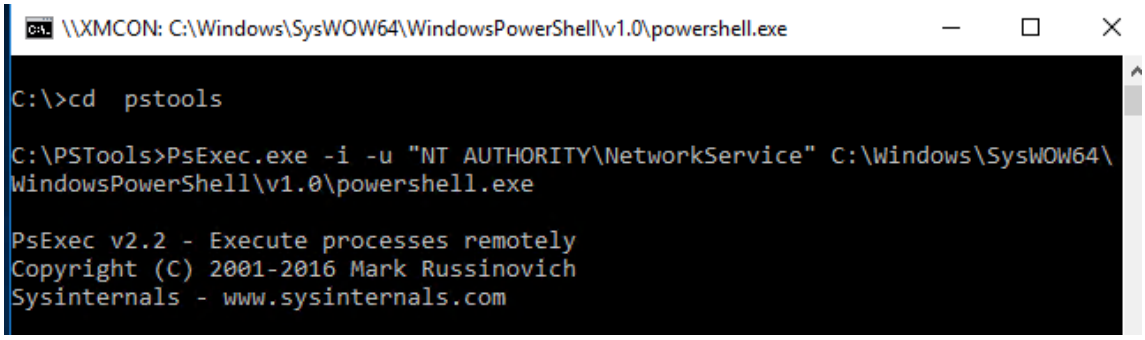
ストレージゾーンコネクタのみと統合する場合、Storage Zone Controller の管理コンソールは使用しません。これは、管理コンソールではこのソリューションに必要ない Citrix Files の管理者アカウントが求められるためです。このため、PowerShell スクリプトを実行して、Storage Zone Controller を Citrix Files コントロールプレーンなしで使用するように準備します。このスクリプトでは次の操作が行われます。

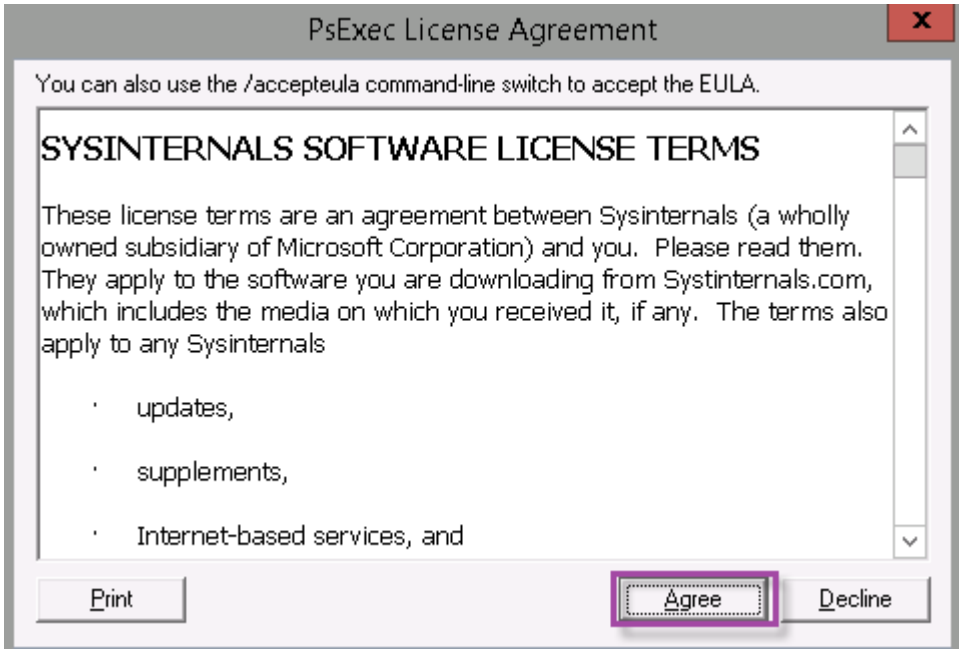
- 現在の Storage Zone Controller をプライマリ Storage Zone Controller として登録します。後で、このプライマリ Storage Zone Controller にセカンダリ Storage Zone Controller を追加できます。
- ゾーンの作成およびゾーンのパスフレーズの設定

1. StorageZone Controller サーバーでの PsExec ツールのダウンロード：Microsoft Windows Sysinternalsにアクセスし、［**PsTools** のダウンロード］をクリックします。ダウンロードしたツールを C ドライブのルートに展開します。



2. PsExec ツールの実行：管理者ユーザーとしてコマンドプロンプトを開き、次のように入力します。

```
```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy--> ```
```




3. メッセージが表示されたら、［同意］をクリックして Sysinternals ツールを実行します。

 
```



PowerShell ウィンドウが開きます。

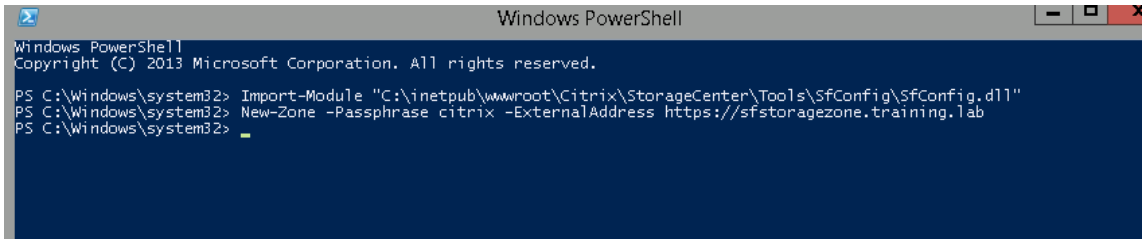
4. PowerShell ウィンドウで次のよう入力します。

```
1 ```
2 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
    SfConfig\SfConfig.dll"
3 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
    com
4 <!--NeedCopy--> ```
```

各項目の意味は次のとおりです:

Passphrase: サイトに割り当てるパスフレーズを指定します。このパスフレーズはメモしておいてください。Storagezone Controller でパスフレーズを回復することはできません。パスフレーズを紛失すると、ストレージゾーンの再インストール、ストレージゾーンへの Storage Zone Controller の追加、およびサーバーに障害が発生した場合のストレージゾーンの回復ができなくなります。

ExternalAddress: Storage Zone Controller サーバーの外部完全修飾ドメイン名を指定します。



これで、プライマリ Storage Zone Controller の準備ができました。

該当する場合は、Citrix Endpoint Management にログインしてストレージゾーンコネクタを作成する前に、以下の構成を行います:

ストレージゾーンのプロキシサーバーを指定する

委任のために Storage Zone Controller を信頼するようにドメインコントローラーを構成する

ストレージゾーンにセカンダリ Storage Zone Controller を統合する

ストレージゾーンコネクタを作成する方法については、「Citrix Endpoint Management で StorageZone Controller の接続を定義する」を参照してください。

ストレージゾーンにセカンダリ **Storage Zone Controller** を統合する

ストレージゾーンを高可用性に構成するには、2 つ以上の Storage Zone Controller を接続します。ゾーンにセカンダリ Storage Zone Controller を追加するには、2 台目のサーバーに Storage Zone Controller をインストールします。その後、インストールした StorageZone Controller を、プライマリ StorageZone Controller のゾーンに追加します。

1. プライマリサーバーに追加する Storage Zone Controller サーバーで、PowerShell ウィンドウを開きます。
2. PowerShell ウィンドウで次のよう入力します。

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP
   >
   ```

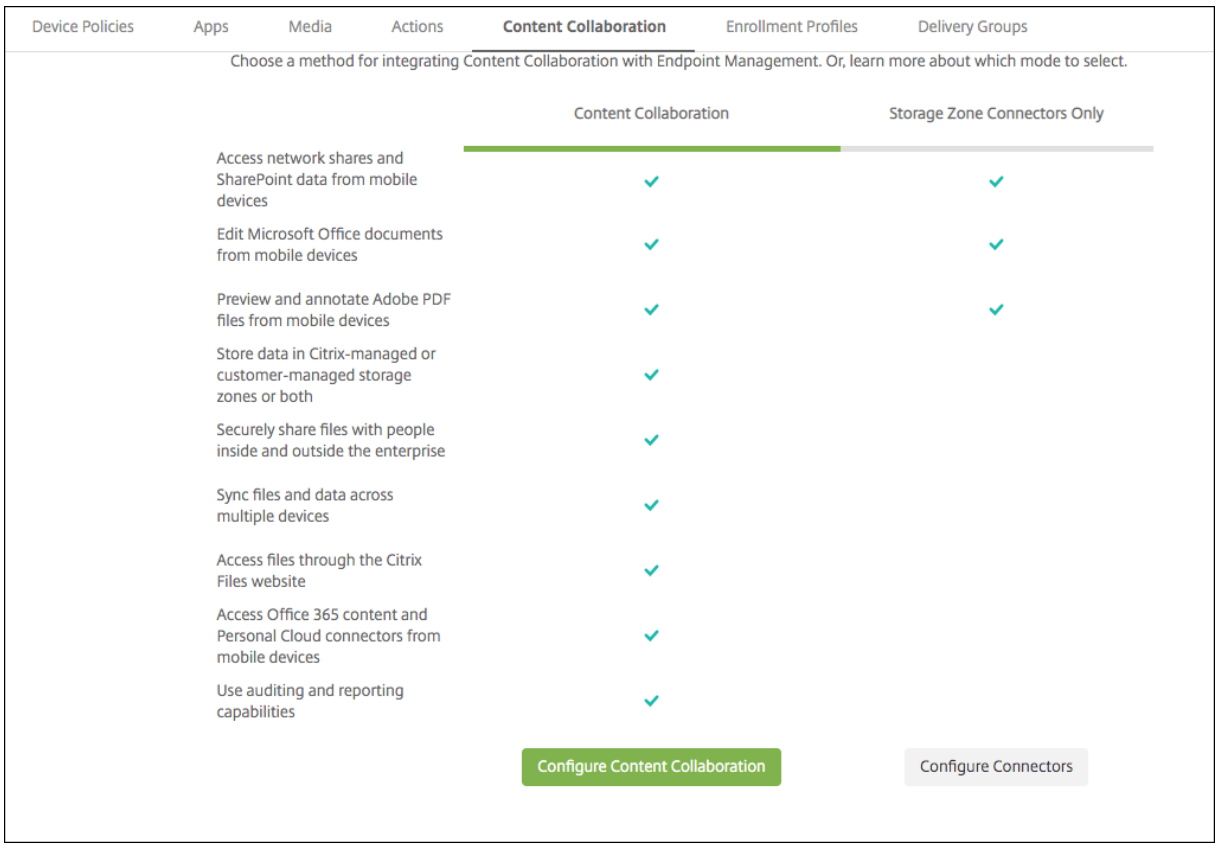
   例:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

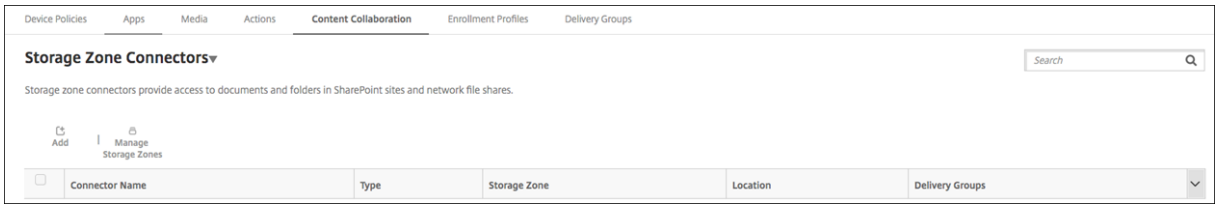
Citrix Endpoint Management で **Storage Zone Controller** の接続を定義する

ストレージゾーンコネクタを追加する前に、ストレージゾーンコネクタが有効な Storage Zone Controller の接続情報を構成します。このセクションの説明通りに Storage Zone Controller を定義してください。つまり、コネクタを追加する場合の手順は以下の通りです。

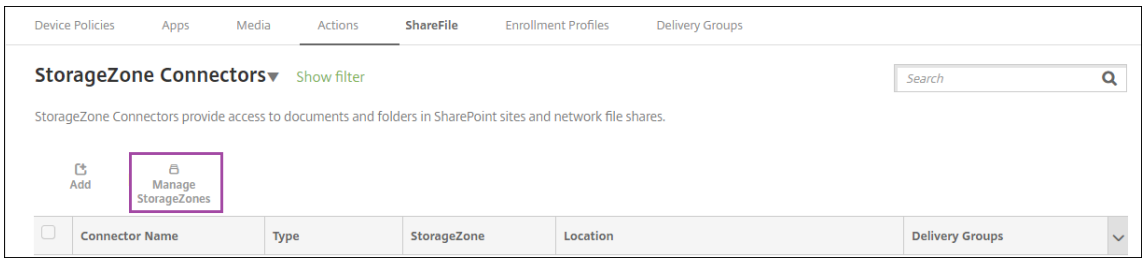
初めて ［構成］**>** ［**ShareFile**］ページにアクセスすると、Citrix Endpoint Management を Enterprise アカウントと組み合わせた場合とストレージゾーンコネクタと組み合わせた場合との差異の要約が表示されます。



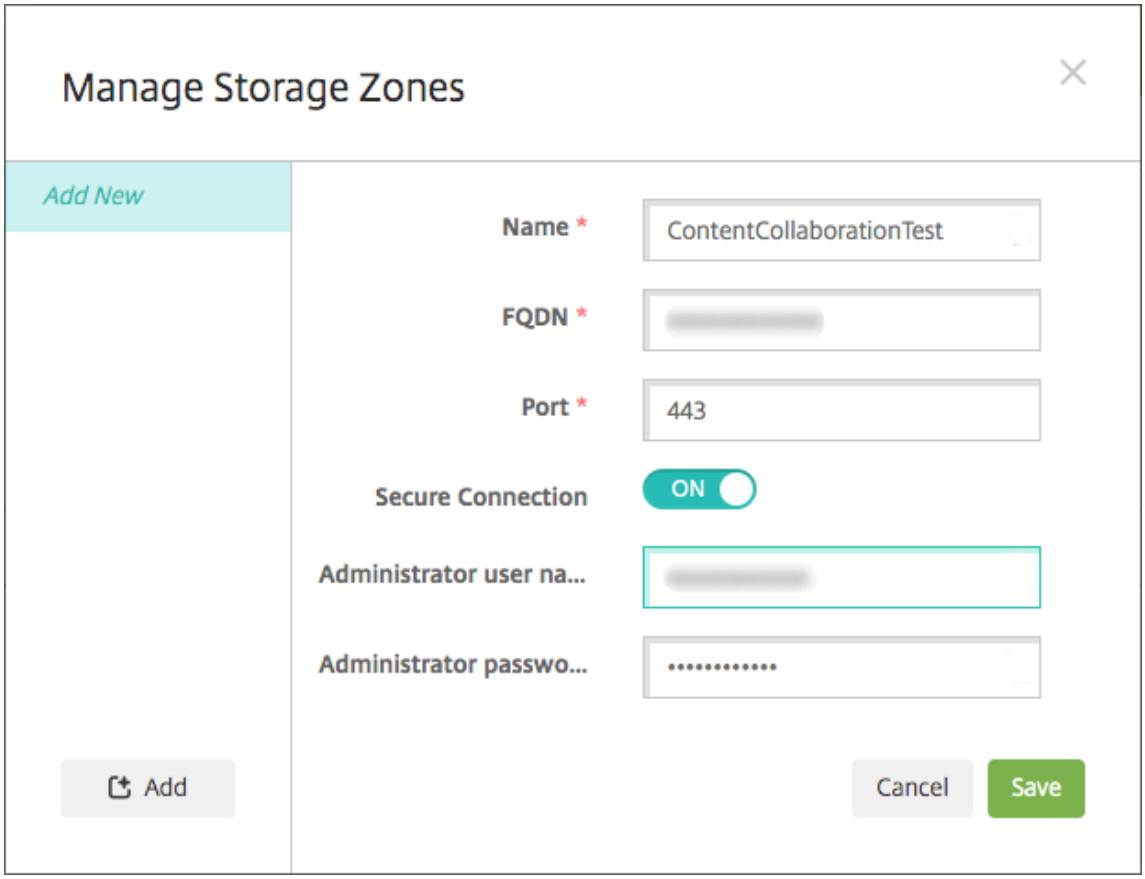
［コネクタの構成］をクリックしてこの記事の構成手順を進めます。



1. ［構成］**>** ［**ShareFile**］で、［ストレージゾーンの管理］をクリックします。



2. ［ストレージゾーンの管理］で、接続情報を追加します。



- 名前：ストレージゾーンの説明的な名前で、Citrix Endpoint Management でストレージゾーンを識別するのに使用されます。名前に空白や特殊文字は含めないでください。
- **FQDN** およびポート： Citrix Endpoint Management サーバーからアクセス可能な StorageZone Controller の完全修飾ドメイン名（FQDN）とポート番号。
- セキュリティで保護された接続： StorageZone Controller との接続に SSL を使用する場合は、デフォルト設定の［オン］を使用します。接続に SSL を使用しないのであれば、この設定を［オフ］に変更します。
- ［管理者ユーザー名］と［管理者パスワード］: 管理者サービスアカウントのユーザー名（domain\admin 形式）とパスワード。または、Storage Zone Controller の読み取り権限と書き込み権限を持つユーザーアカウントを指定します。

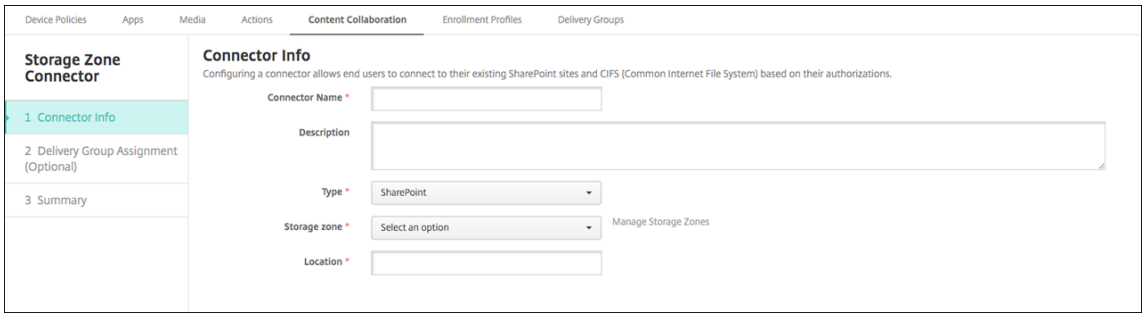
3. ［保存］をクリックします。
4. 接続をテストするために、Citrix Endpoint Management サーバーがポート 443 で Storage Zone Controller の完全修飾ドメイン名に接続できることを確認します。
5. 別の Storage Zone Controller 接続を設定するには、［ストレージゾーンの管理］の ［追加］ボタンをクリックします。

   Storage Zone Controller の接続情報を編集したり、削除するには、［ストレージゾーンの管理］で接続名を選択します。続いて、［編集］または ［削除］をクリックします。

Citrix Endpoint Management にストレージゾーンコネクタを追加する

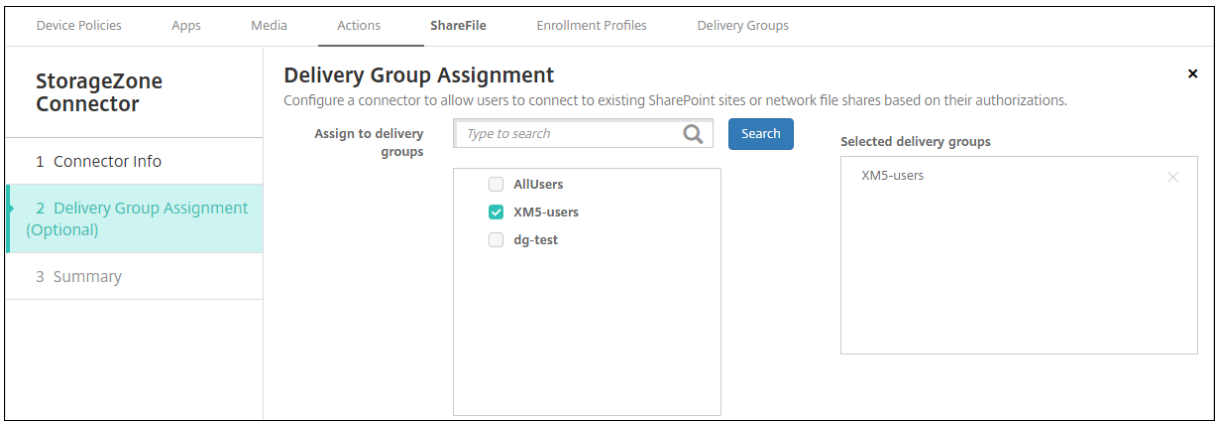
1. ［構成］**>**［**ShareFile**］に移動し、［追加］をクリックします。

2. ［コネクタ情報］ページで、次の設定を行います。



- コネクタ名： Citrix Endpoint Management で StorageZone コネクタを識別する名前。
- 説明：このコネクタに関するオプションのメモ。
- 種類：［**SharePoint**］または ［ネットワーク］のいずれかを選択します。
- **StorageZone**：コネクタに関連付けられたストレージゾーンを選択します。ストレージゾーンが表示されない場合は、［ストレージゾーンの管理］をクリックして、Storage Zone Controller を定義します。
- 場所： SharePoint の場合は、SharePoint ルートレベルのサイト、サイトコレクション、またはドキュメントライブラリの URL を`https://sharepoint.company.com`の形式で指定します。ネットワーク共有の場合は、UNC（Uniform Naming Convention）パスの完全修飾ドメイン名を\\server\share の形式で指定します。

3. ［デリバリーグループ割り当て］ページで、オプションでコネクタをデリバリーグループに割り当てます。コネクタのデリバリーグループへの関連付けには、［構成］**>**［デリバリーグループ］を使うこともできます。



1. ［概要］ページで、構成したオプションを確認できます。構成を調整するには、［戻る］をクリックします。
2. ［保存］をクリックしてコネクタを保存します。
3. コネクタをテストします：

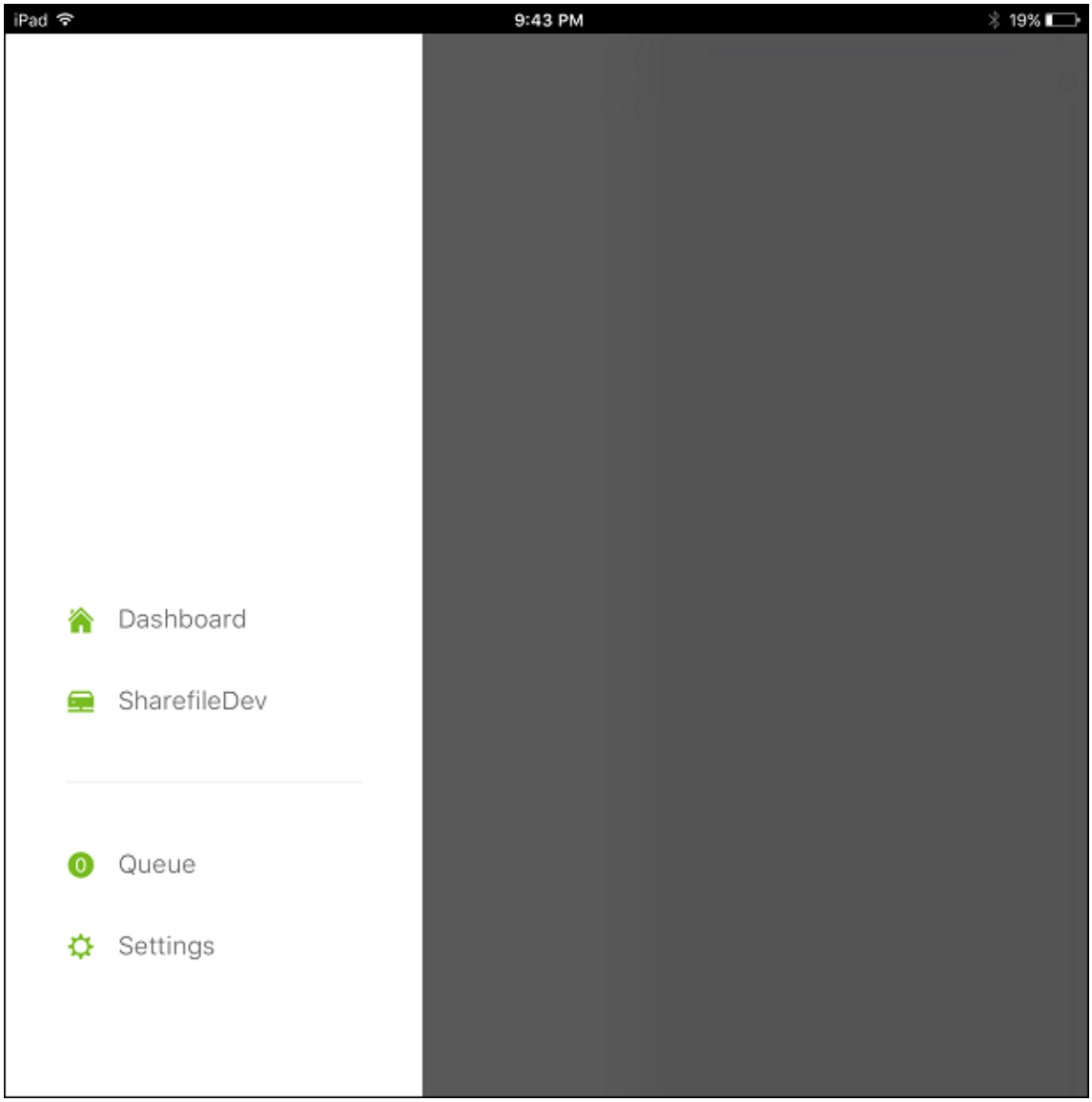
   a) Citrix Files クライアントをラップする場合は、ネットワークアクセスポリシーを ［トンネル **- Web SSO**］に設定します。

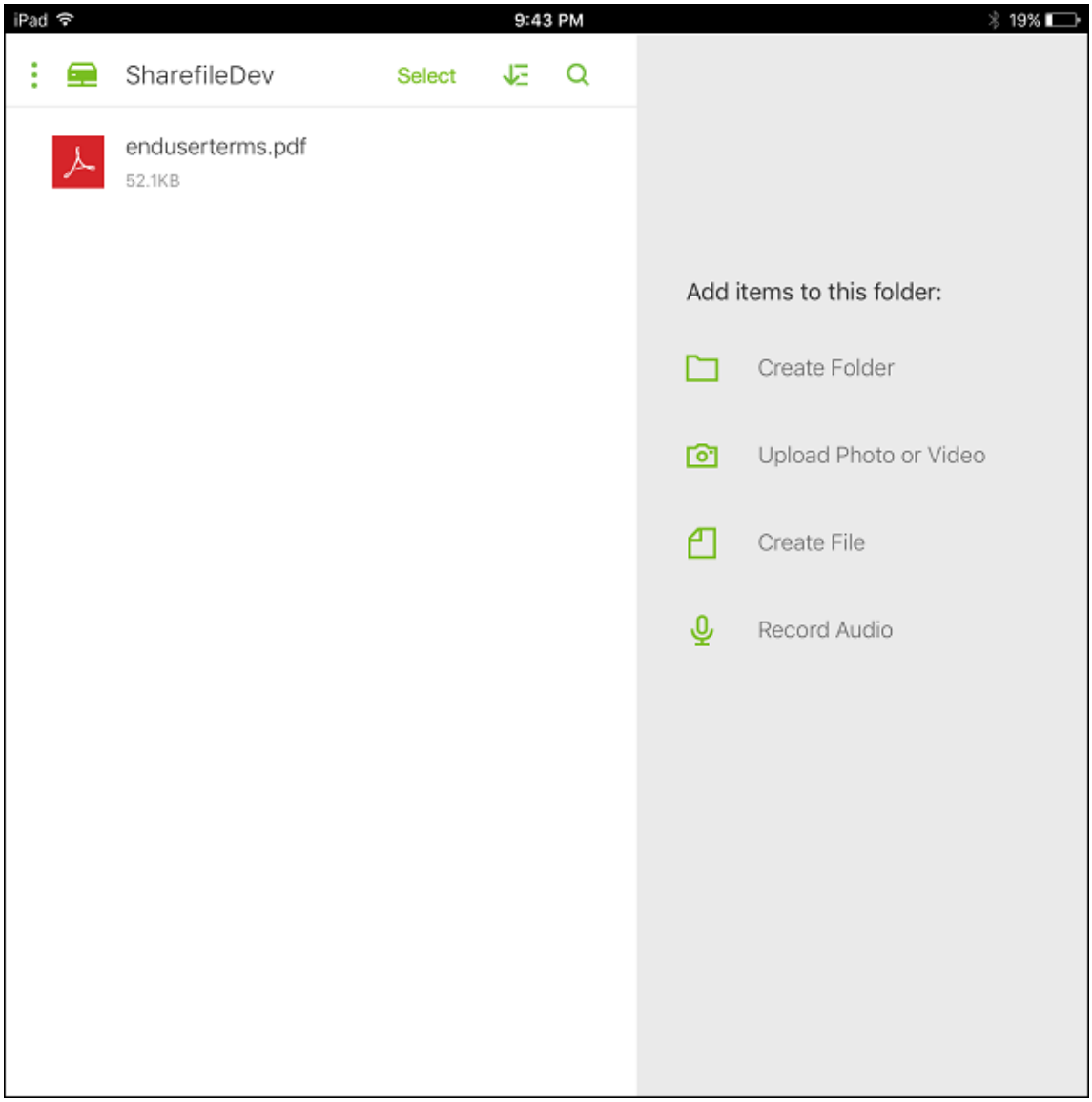
   このトンネルモードでは、MDX アプリからの SSL/HTTP トラフィックが MDX フレームワークによって終了されます。その後、ユーザーに代わって MDX により内部接続に対する新しい接続が開始されます。このポリシー設定では、MDX フレームワークが、Web サーバーから発行された認証チャレンジを検出してそれに応答できます。

   b) Citrix Files クライアントを Citrix Endpoint Management に追加します。詳しくは、「Citrix Files クライアントを Citrix Endpoint Management に追加するには」を参照してください。

   c) サポート対象のデバイスで、Citrix Files およびコネクタへのシングルサインオンを確認します。

次の例の SharefileDev はコネクタの名前です。

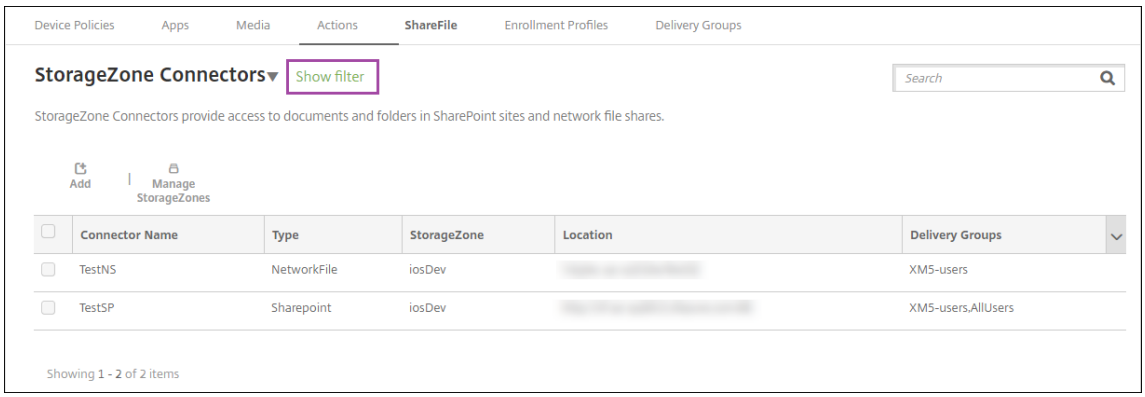




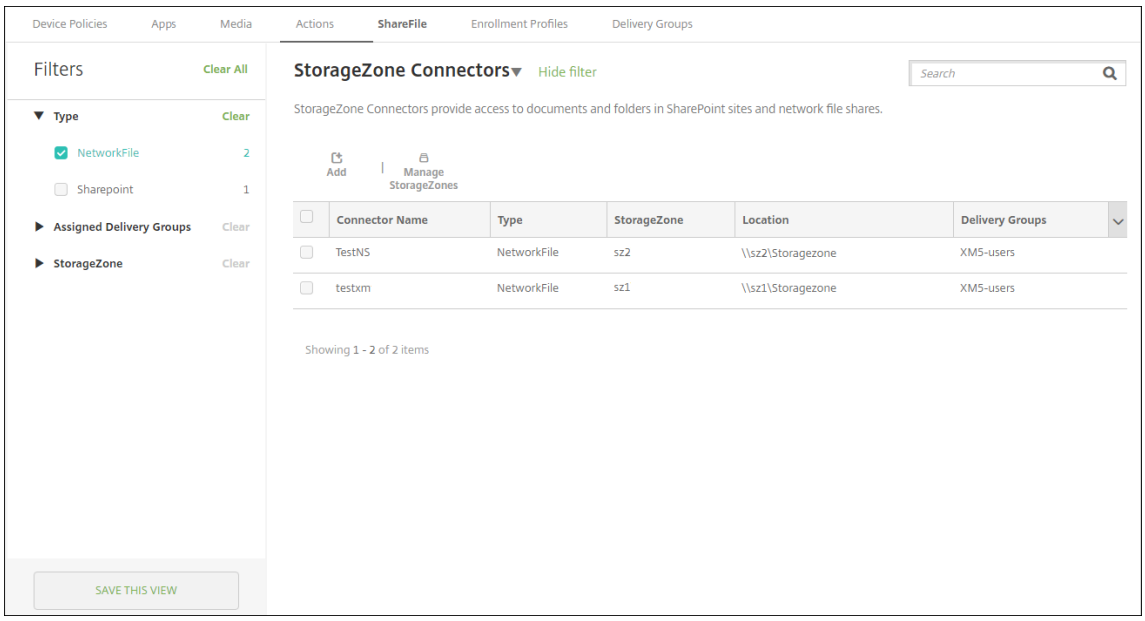
ストレージゾーンコネクター一覧をフィルターする

ストレージゾーンコネクタの一覧は、コネクタタイプ、割り当てられているデリバリーグループ、およびストレージゾーンでフィルタリングできます。

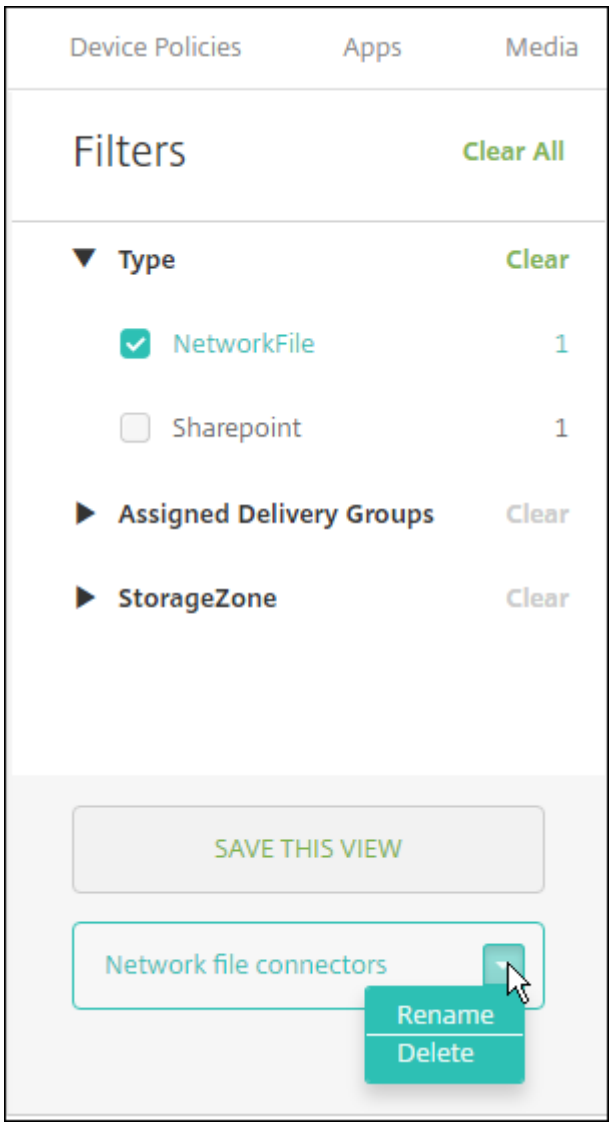
1. ［構成］**>** ［**ShareFile**］に移動し、［フィルターを表示］をクリックします。



2. フィルターの見出しを展開して選択します。フィルターを保存するには、［このビューを保存］をクリックし、フィルター名を入力して ［保存］をクリックします。



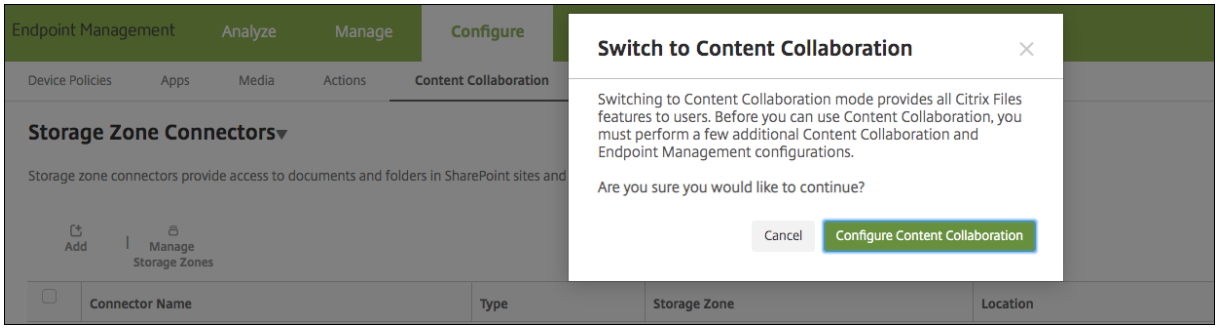
3. フィルターの名前を変更または削除するには、フィルター名の横にある矢印アイコンをクリックします。



Enterprise アカウントに切り替える

ストレージゾーンコネクタを Citrix Endpoint Management と統合した後にも、Enterprise の全機能セットに切り替えることができます。Citrix Endpoint Management では、既存のストレージゾーンコネクタの統合設定が保持されます。

［構成］**>**［**ShareFile**］に移動し、［ストレージゾーンコネクタ］ボックスの一覧をクリックし、［**ShareFile** の構成］をクリックします。



Enterprise アカウントの構成については、「Citrix Files での SAML によるシングルサインオン」を参照してください。

HDX アプリ向け SmartAccess

March 15, 2024

この機能により、デバイスプロパティ、デバイスのユーザープロパティ、デバイスにインストールされたアプリケーションに基づいて HDX アプリへのアクセスを制御できます。この機能を使用するには、デバイスをコンプライアンス違反に指定してアクセスを拒否する、自動化された操作を設定します。この機能を使用する HDX アプリを Citrix Virtual Apps and Desktops で構成するには、コンプライアンス違反のデバイスへのアクセスを拒否する SmartAccess ポリシーを使用します。Citrix Endpoint Management は、署名された暗号化タグを使って、StoreFront にデバイスの状態を伝えます。すると StoreFront は、アプリのアクセス制御ポリシーに基づいてアクセスを許可または拒否します。

この機能を使用するには、次の環境が必要です。

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- タグの署名と暗号化に使用する SAML 証明書が構成された Citrix Endpoint Management。秘密キーのない同じ証明書が StoreFront サーバーにアップロードされます。

この機能を使い始めるには:

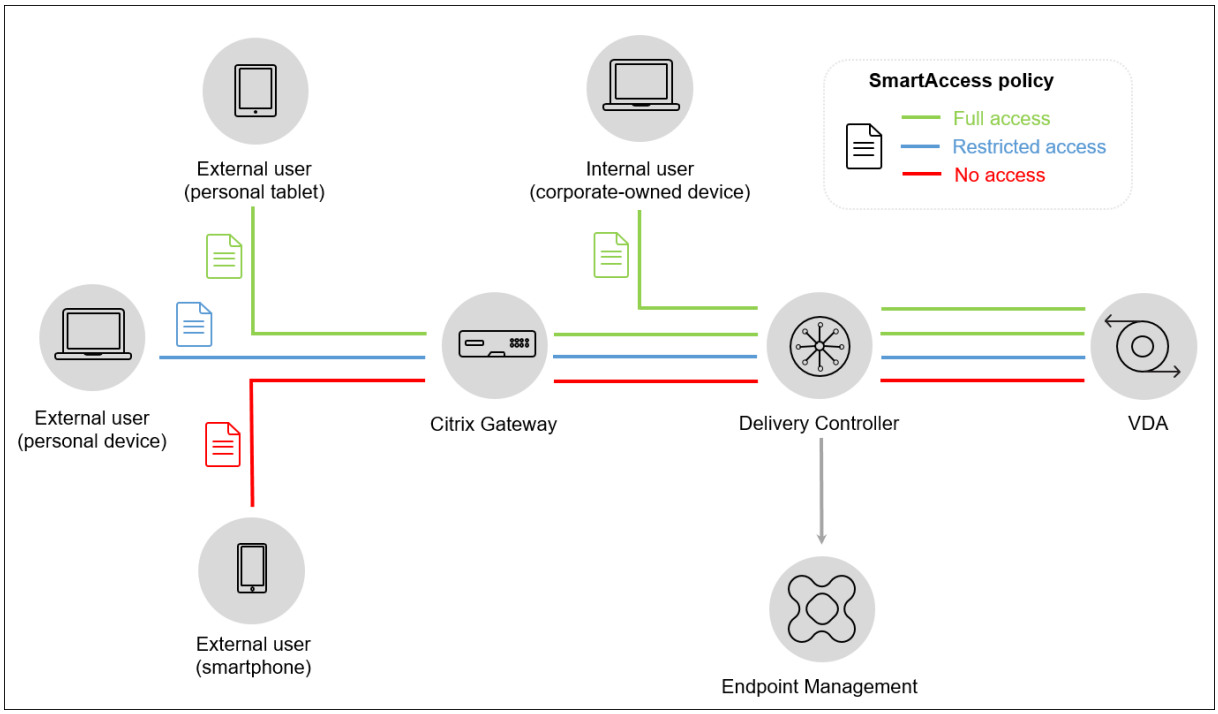
- Citrix Endpoint Management サーバー証明書を StoreFront ストアに構成します。
- 必要な SmartAccess ポリシーを使用して、少なくとも 1 つの Citrix Virtual Apps and Desktops デリバリーグループを構成します。
- Citrix Endpoint Management で自動化された操作を設定します。

エンドポイントの HDX アプリ向け SmartAccess

この機能により、ポリシーベースのアクセス制御を適用して HDX アプリへのデバイスのアクセスを制限できます。HDX アプリに次のアクセスレベルを適用できます:

- フルアクセス。デバイスは、Citrix Secure Hub ストアが提供するすべての HDX アプリにアクセスできます。
- 制限付きアクセス。デバイスは、1 つまたは複数の HDX アプリにアクセスできますが、すべての HDX アプリにアクセスすることはできません。
- アクセスなし。デバイスは、どの HDX アプリにもアクセスできません。

次の図は、アクセス制御のしくみを示しています。Citrix Secure Hub で HDX アプリを起動しようとすると、Delivery Controller に要求がトリガーされます。Delivery Controller が Citrix Endpoint Management サーバーに要求を転送すると、検証が行われます。検証結果によって、デバイスのアクセスレベルが決まります。たとえば、ジェイルブレイクされたデバイスの場合、HDX アプリへのアクセスは拒否されます。



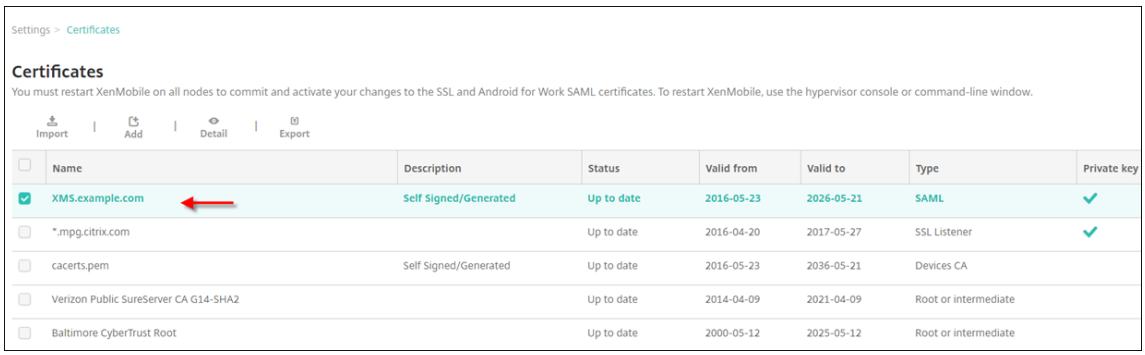
Citrix Endpoint Management サーバー証明書のエクスポートと構成、および **StoreFront** ストアへのアップロード

SmartAccess は、署名された暗号化タグを使用して、Citrix Endpoint Management サーバーと StoreFront サーバー間で通信します。この通信を有効にするには、Citrix Endpoint Management サーバー証明書を StoreFront ストアに追加します。

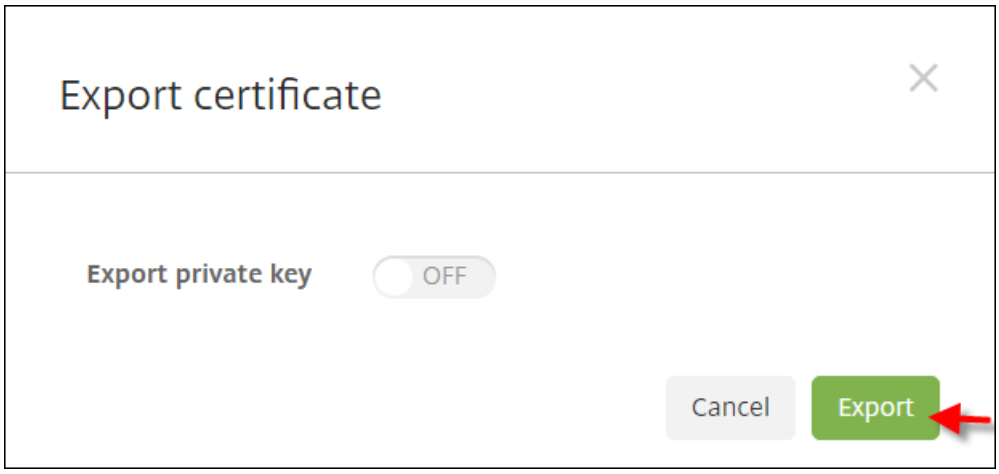
Citrix Endpoint Management がドメインおよび証明書ベースの認証で有効な場合に StoreFront と Citrix Endpoint Management を統合する方法について詳しくは、Support Knowledge Centerを参照してください。

SAML 証明書を **Citrix Endpoint Management** からエクスポートする

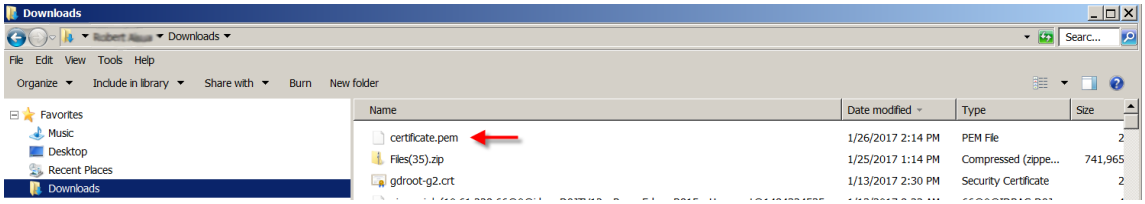
1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。［証明書］をクリックします。
2. Citrix Endpoint Management サーバーの SAML 証明書を見つけます。



3. ［機密キーをエクスポート］が ［オフ］に設定されていることを確認します。［エクスポート］をクリックして、証明書をダウンロードディレクトリにエクスポートします。

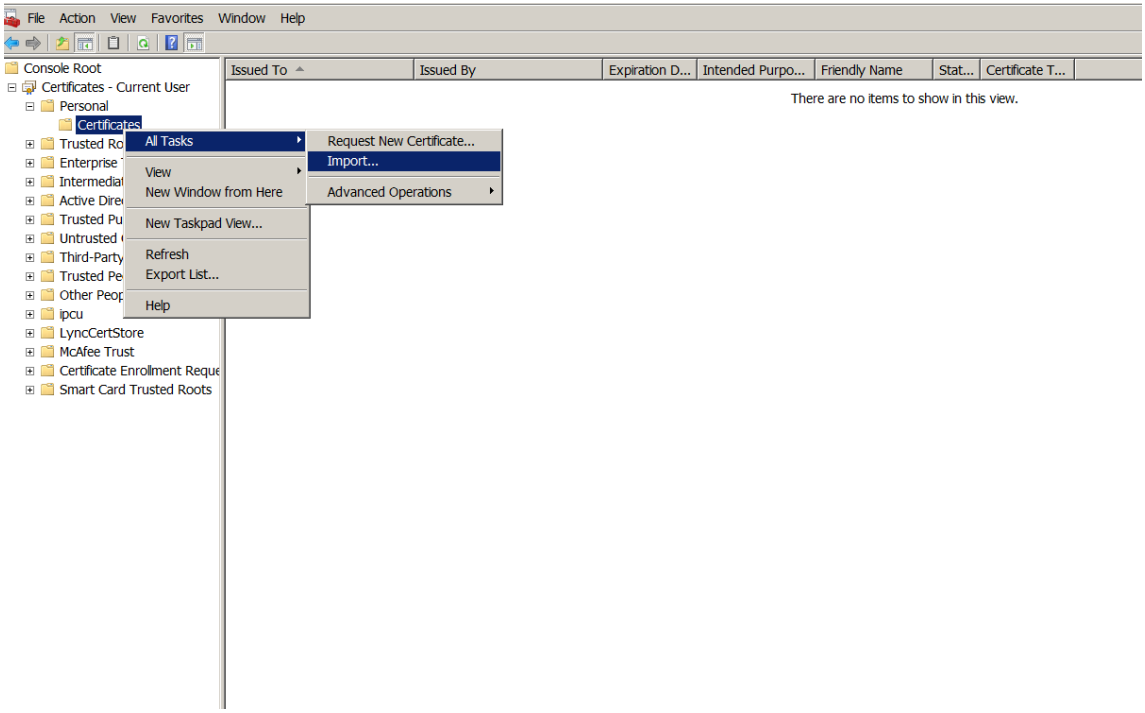


4. ダウンロードディレクトリで証明書を検索します。証明書は PEM 形式です。

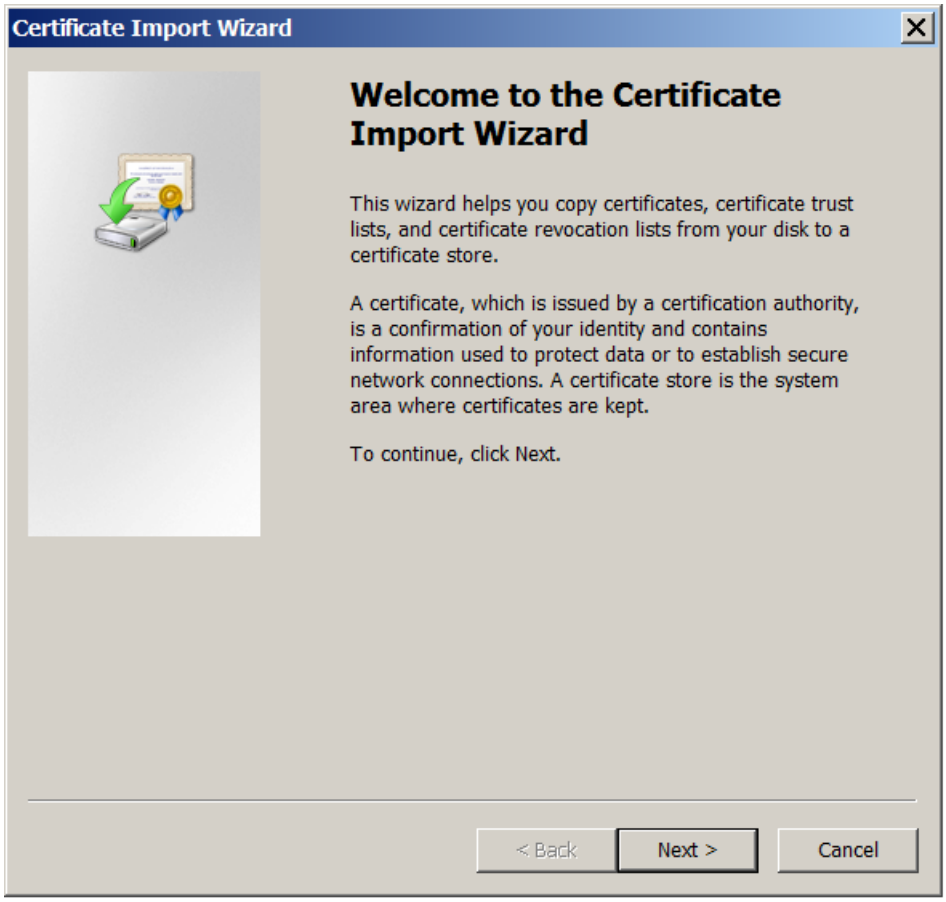


証明書を **PEM** から **CER** に変換する

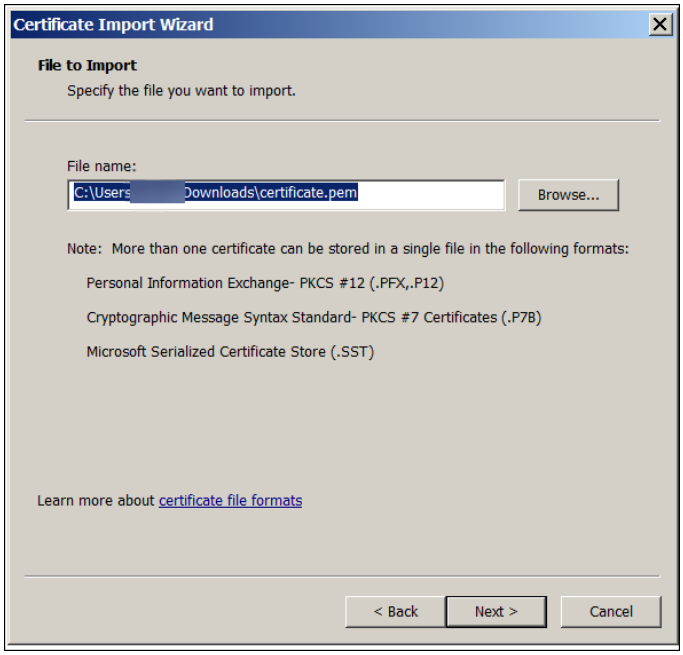
1. Microsoft 管理コンソール（MMC）を開き、［証明書］**>**［すべてのタスク］**>**［インポート］を右クリックします。



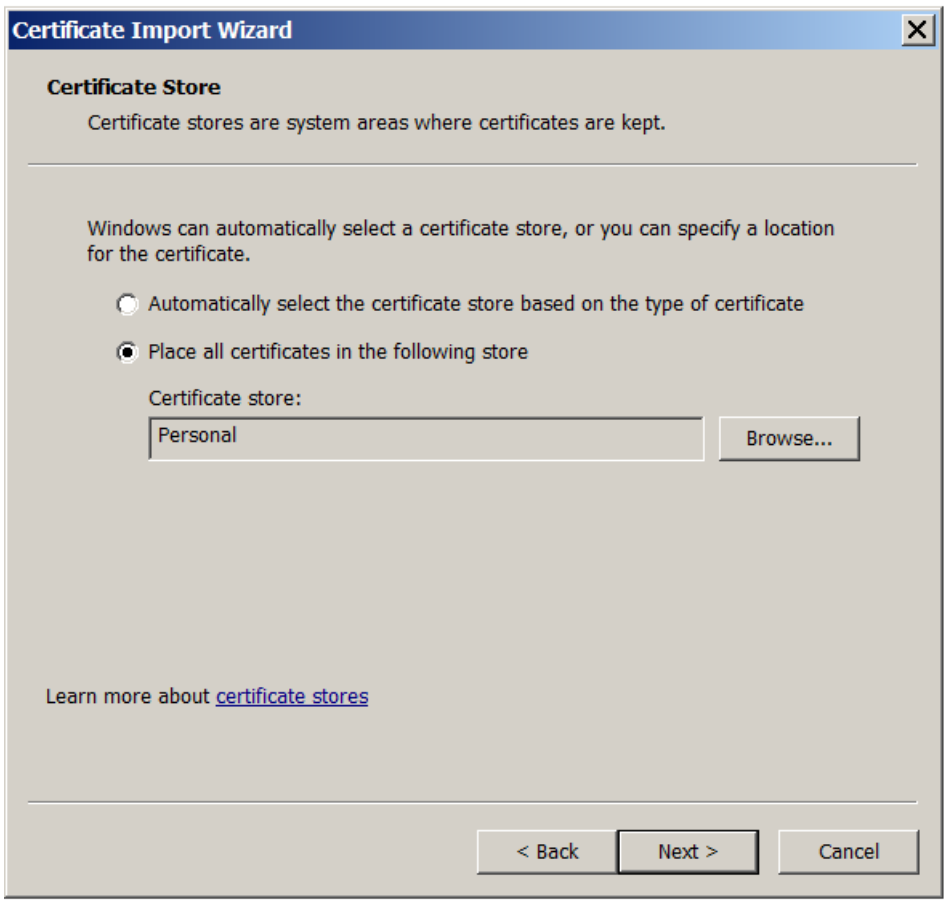
2. 証明書のインポートウィザードが表示されたら、［次へ］をクリックします。



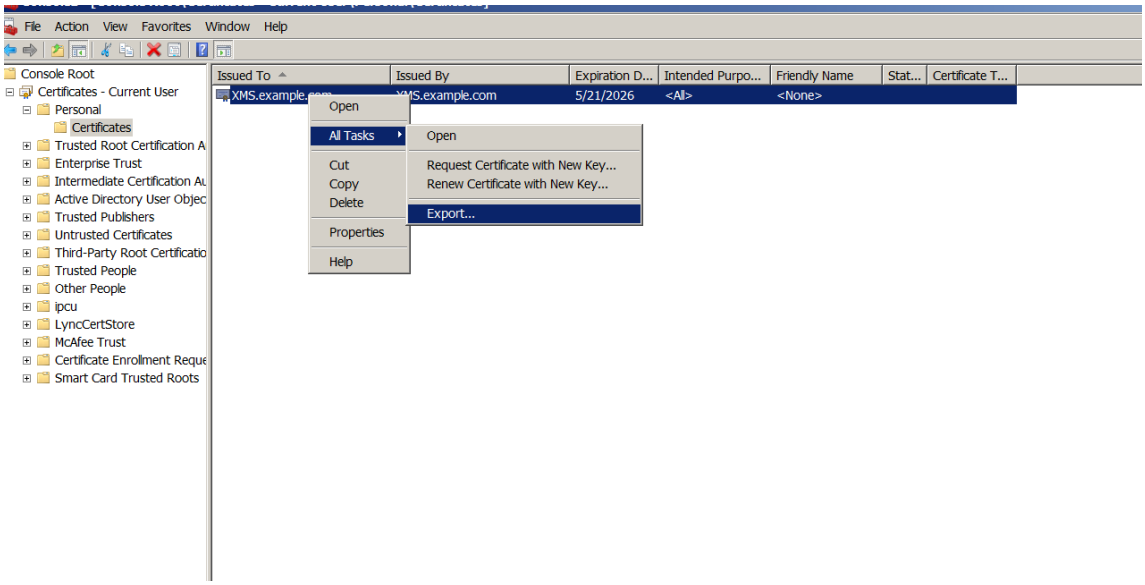
3. ダウンロードディレクトリで証明書を参照します。



4. ［証明書をすべて次のストアに配置する］をクリックし、証明書ストアとして ［個人］を選択します。［次へ］をクリックします。

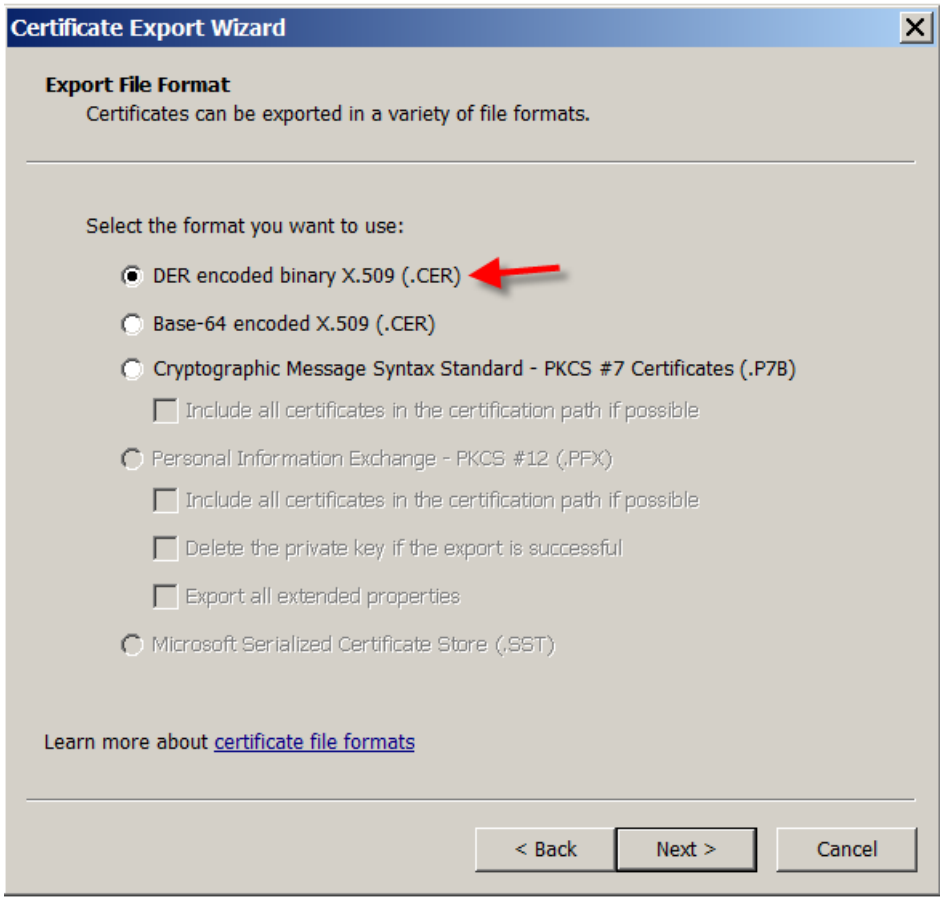


5. 選択した内容を確認し、［完了］をクリックします。［**OK**］をクリックして確認ウィンドウを閉じます。
6. MMC で証明書を右クリックし、［すべてのタスク］、［エクスポート］の順に選択します。

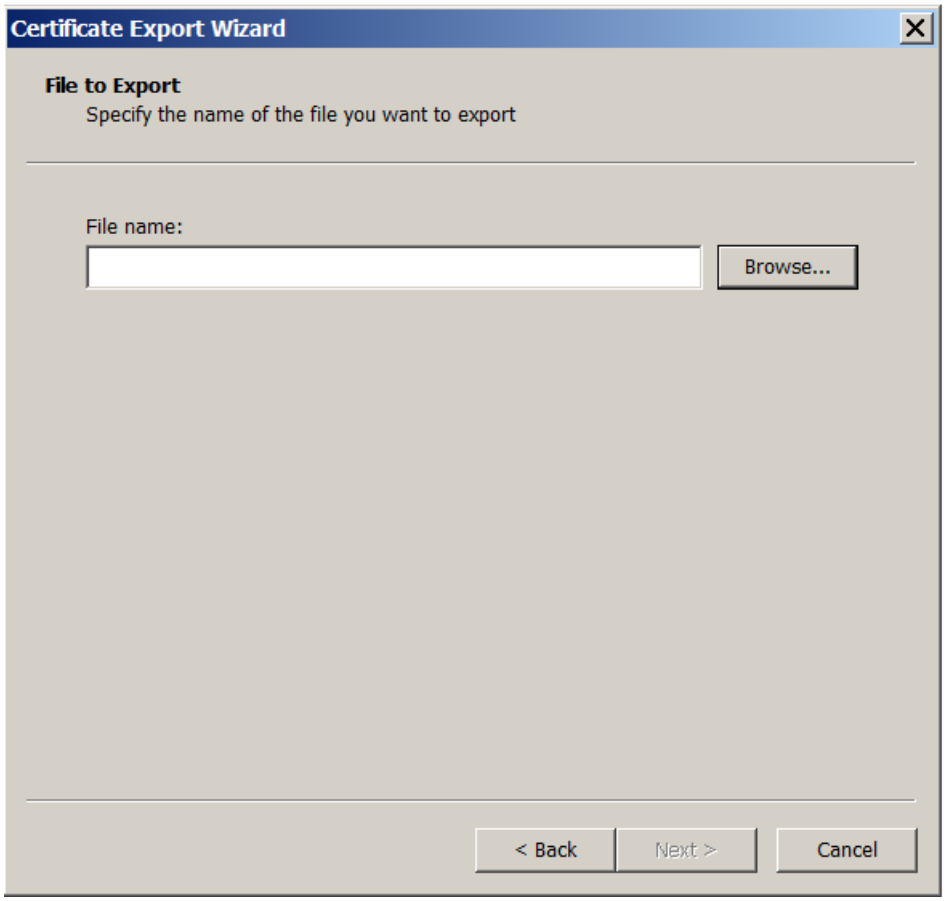


7. 証明書のエクスポートウィザードが表示されたら、［次へ］をクリックします。

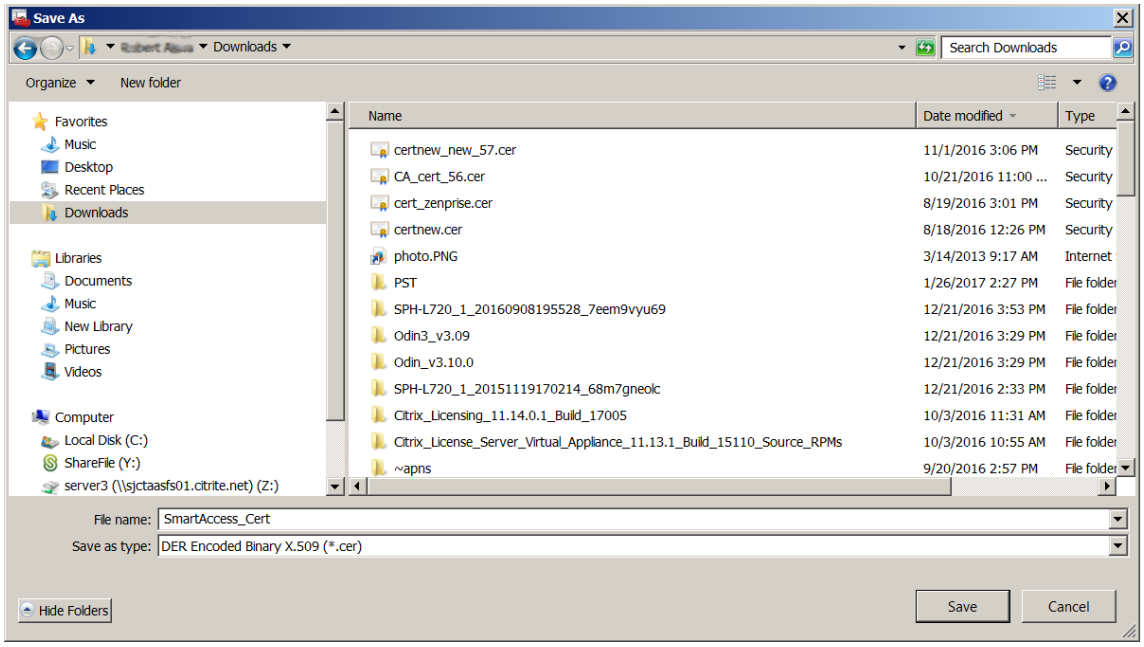
8. ［**DER encoded binary X.509 (.CER)**］の形式を選択します。［次へ］をクリックします。



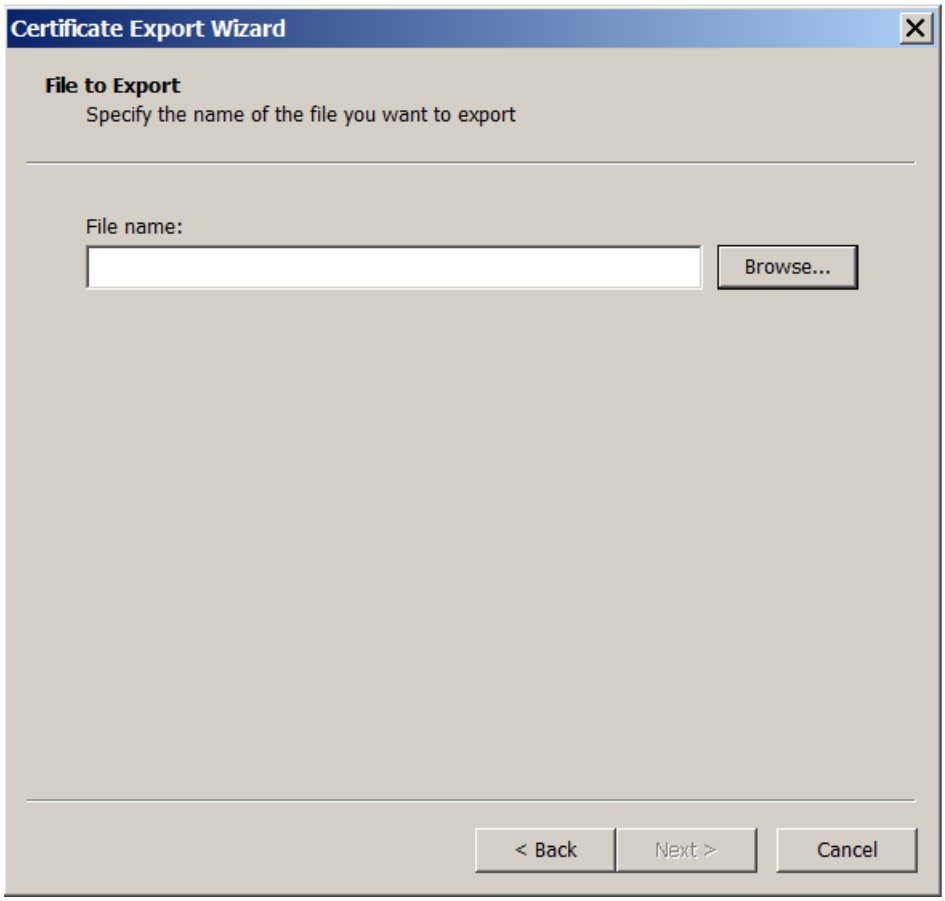
9. 証明書を参照します。証明書の名前を入力し、［次へ］をクリックします。



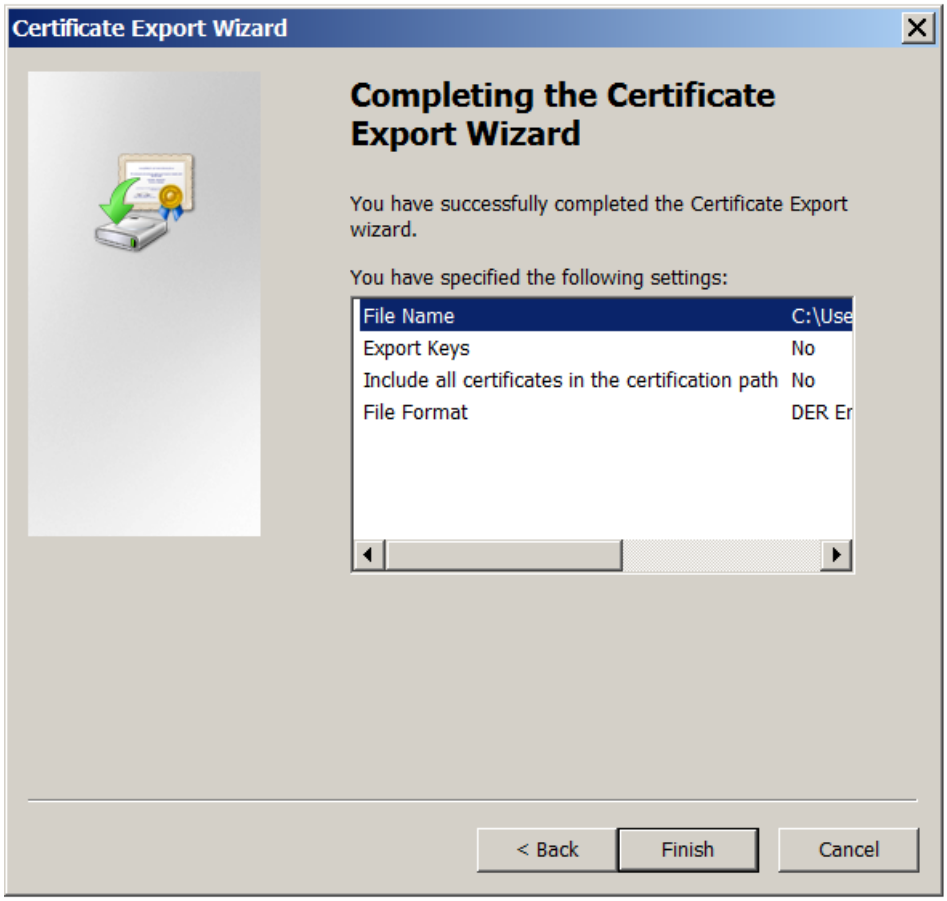
10. 証明書を保存します。



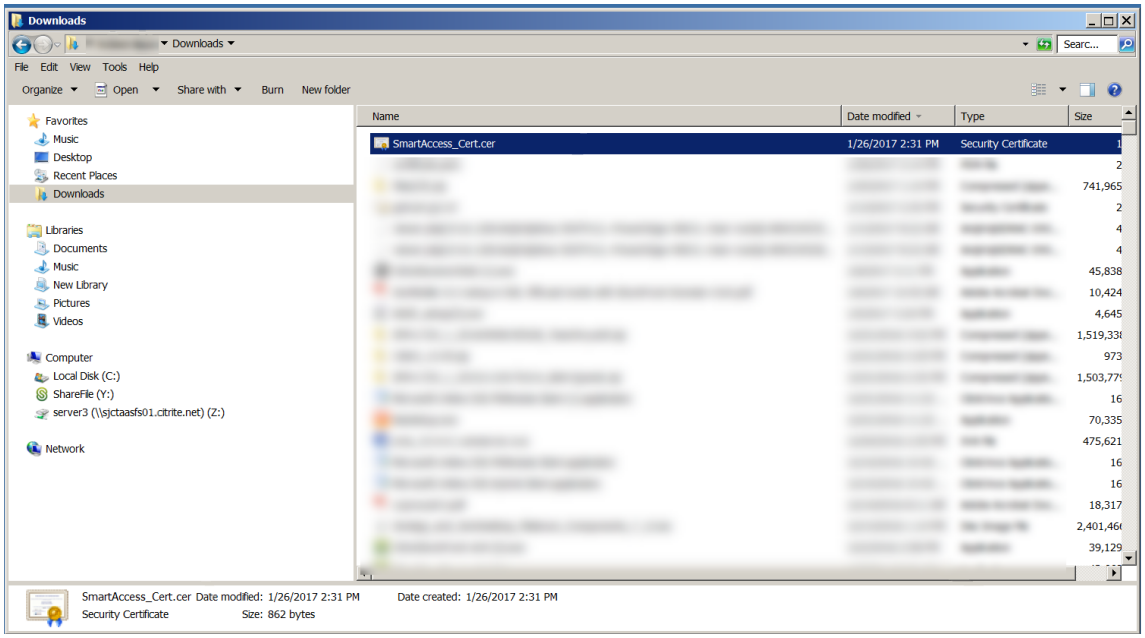
11. 証明書を参照し、［次へ］をクリックします。



12. 選択した内容を確認し、［完了］をクリックします。［**OK**］をクリックして確認ウィンドウを閉じます。

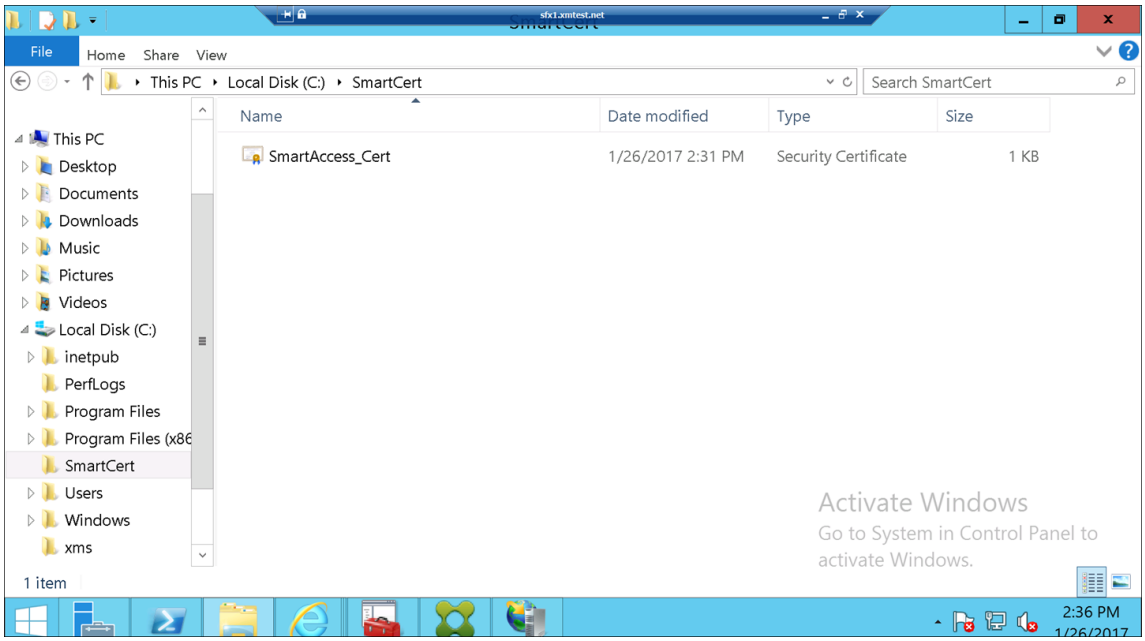


13. ダウンロードディレクトリで証明書を検索します。証明書は CER 形式です。



証明書を **StoreFront** サーバーにコピーする

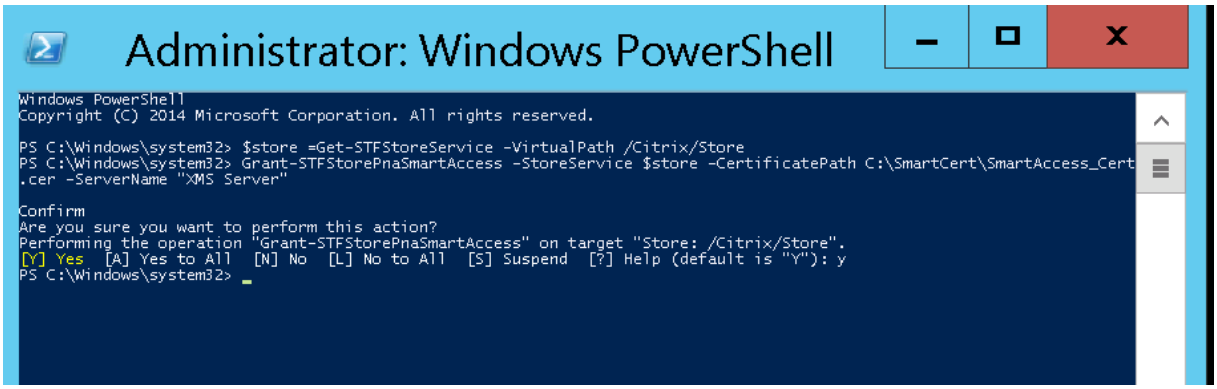
1. StoreFront サーバーで、**SmartCert** という名前のフォルダーを作成します。
2. 証明書を **SmartCert** フォルダーにコピーします。



StoreFront ストアで証明書を構成する

StoreFront サーバーで、次の PowerShell コマンドを実行して、変換した Citrix Endpoint Management サーバー証明書をストアに構成します:

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2  <!--NeedCopy-->
```



StoreFront ストアに既存の証明書が存在する場合は、次の PowerShell コマンドを実行して証明書を無効にします。


```
    Revoke-STFStorePnaSmartAccess  -StoreService $store  -All
<!--NeedCopy-->
```

あるいは、StoreFront サーバー上で次の PowerShell コマンドのいずれかを実行して、StoreFront ストア上の既存の証明書を取り消すこともできます:

- 名前で取り消す:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -ServerName  "
       My XM Server"
<!--NeedCopy-->
```

- 拇印で取り消す:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -
       CertificateThumbprint "[Thumbprint]
<!--NeedCopy-->
```

- サーバーオブジェクトで取り消す:

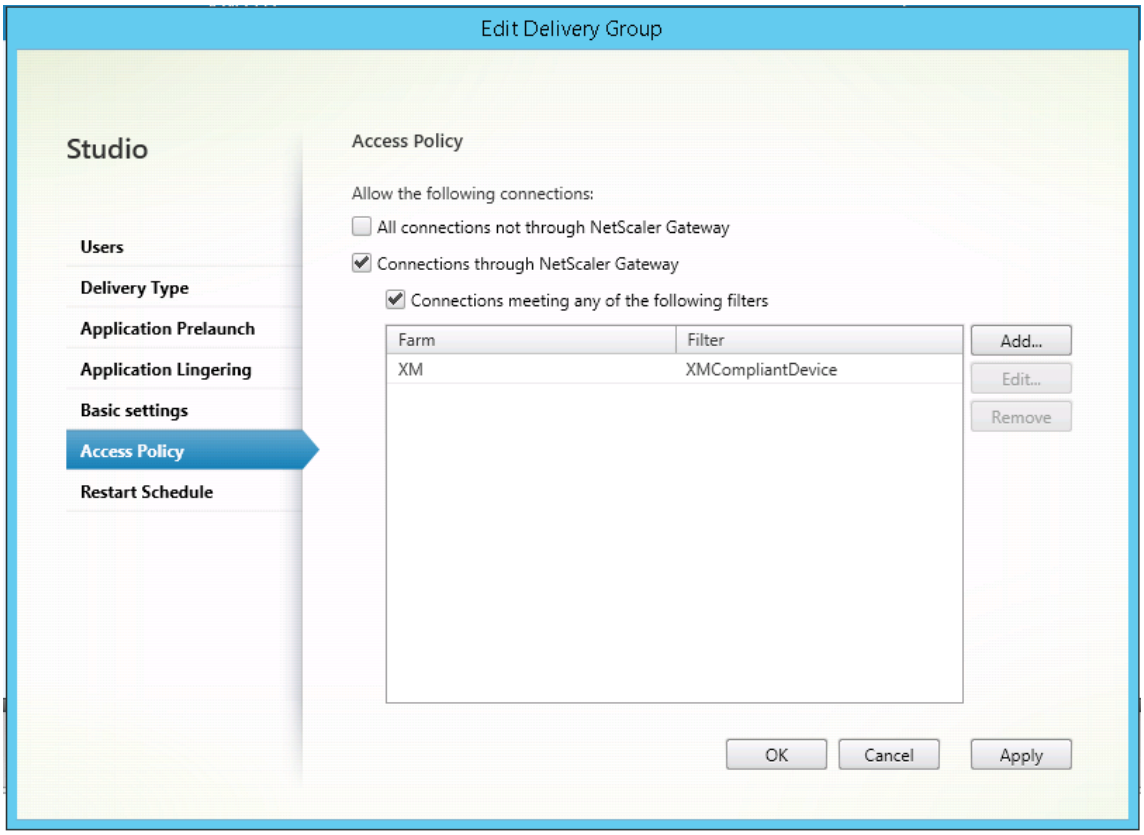
```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  -StoreService $store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Citrix Virtual Apps and Desktops での SmartAccess ポリシーの構成

HDX アプリを配信するデリバリーグループに必要な SmartAccess ポリシーを追加するには、次の手順を行います。

1. Citrix Cloud コンソールで Citrix Studio を開きます。
2. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
3. アプリを配信するグループまたはアクセスを制御するアプリを選択します。［操作］ペインの ［デリバリーグループの編集］を選択します。

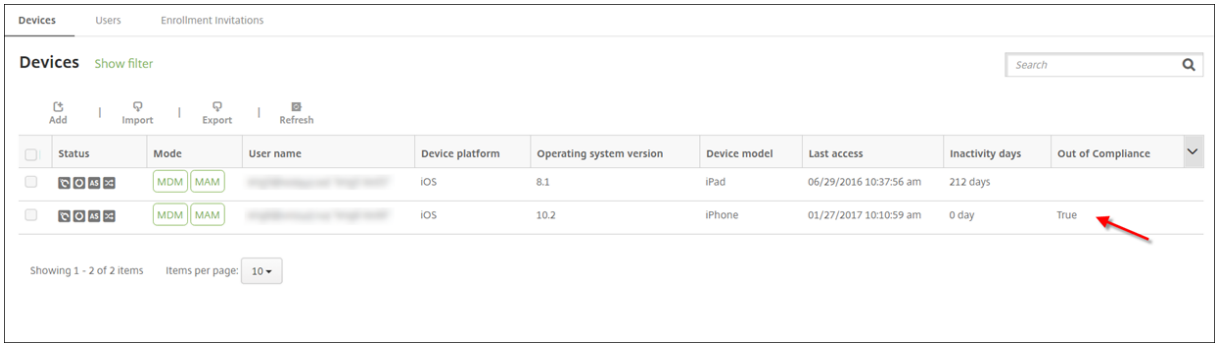
4. ［アクセスポリシー］ページで、［**NetScaler Gateway** を経由する接続］と ［次のいずれかに一致する接続］を選択します。
5. ［追加］をクリックします。
6. ［ファーム］が「**XM**」で、［フィルター］が「**XMCompliantDevice**」のアクセスポリシーを追加します。



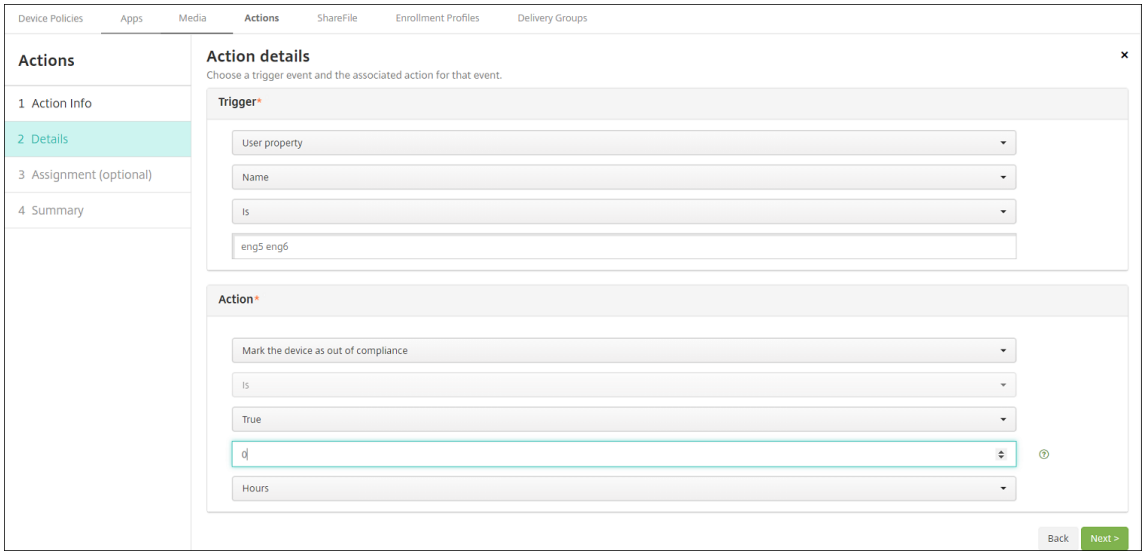
7. ［適用］をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

Citrix Endpoint Management で自動化された操作を設定する

HDX アプリのデリバリーグループに設定した SmartAccess ポリシーは、デバイスがコンプライアンス違反である場合にそのデバイスへのアクセスを拒否します。自動化された操作を使用して、そのデバイスをコンプライアンス違反としてマークします。



1. Citrix Endpoint Management コンソールで、[構成] **>** [アクション] の順にクリックします。[操作] ページが開きます。
2. [追加] をクリックして操作を追加します。[アクション情報] ページが開きます。
3. [アクション情報] ページで、操作の名前と説明を入力します。
4. [次へ] をクリックします。[アクションの詳細] ページが開きます。次の例では、ユーザープロパティ名が **eng5** または **eng6** の場合に、デバイスを直ちにコンプライアンス違反と指定するトリガーを作成します。



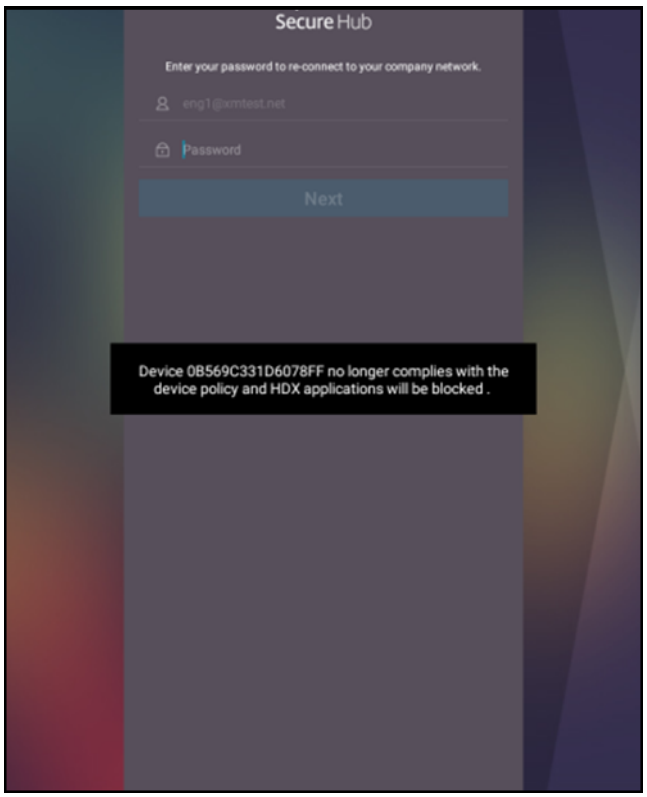
5. [トリガー] 一覧で、[デバイスプロパティ]、[ユーザープロパティ]、または [インストール済みアプリ名] を選択します。SmartAccess はイベントトリガーをサポートしていません。
6. [アクション] 一覧で、以下を実行します。
   - [コンプライアンス違反としてデバイスをマーク] を選択します。
   - [=] を選択します。
   - [真] を選択します。
   - トリガー条件が満たされたときに、直ちにデバイスをコンプライアンス違反としてマークされるように操作を設定するには、時間枠を **0** に設定します。
7. Citrix Endpoint Management デリバリーグループまたはこの操作を適用するグループを選択します。

8. 操作の概要を確認します。
9. ［次へ］をクリックし、［保存］をクリックします。

デバイスがコンプライアンス違反としてマークされると、HDX アプリは Citrix Secure Hub ストアに表示されなくなります。ユーザーはアプリにサブスクライブされなくなります。デバイスに通知は送信されず、Citrix Secure Hub ストアでは HDX アプリが以前は利用可能であったことは示されません。

デバイスがコンプライアンス違反としてマークされたときにユーザーに通知する場合は、通知を作成し、その通知を送信する自動化された操作を作成します。

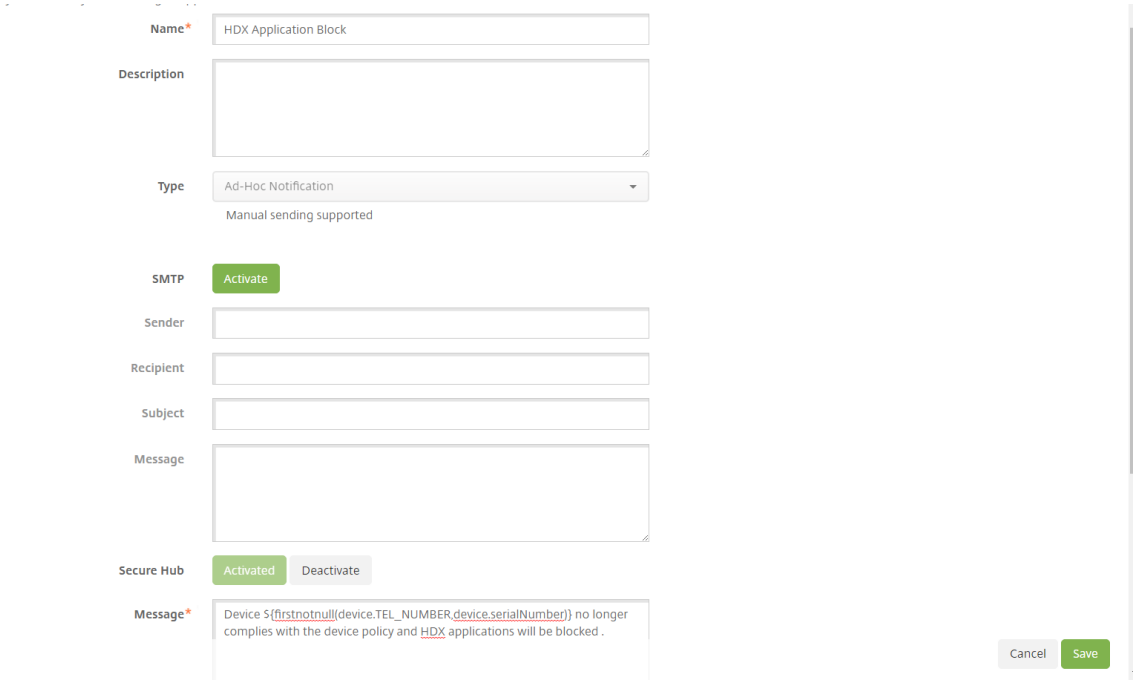
この例では、デバイスがコンプライアンス違反としてマークされたときに「Device serial number or telephone number no longer complies with the device policy and HDX applications will be blocked.」という通知を作成して送信します。



デバイスがコンプライアンス違反としてマークされたときにユーザーに表示される通知を作成する

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［通知テンプレート］をクリックします。［通知テンプレート］ページが開きます。
3. ［通知テンプレート］ページで ［追加］をクリックして追加します。
4. 次の設定を構成します：

- 名前： HDX アプリケーションブロック
- 説明：デバイスがコンプライアンス違反である場合のエージェント通知
- タイプ：アドホック通知
- **Citrix Secure Hub**：アクティブ
- メッセージ： デバイス${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}がデバイスポリシーに準拠しなくなりましたので、HDX アプリケーションがブロックされます。



5. ［保存］をクリックします。

デバイスがコンプライアンス違反としてマークされたときに通知を送信する操作を作成する

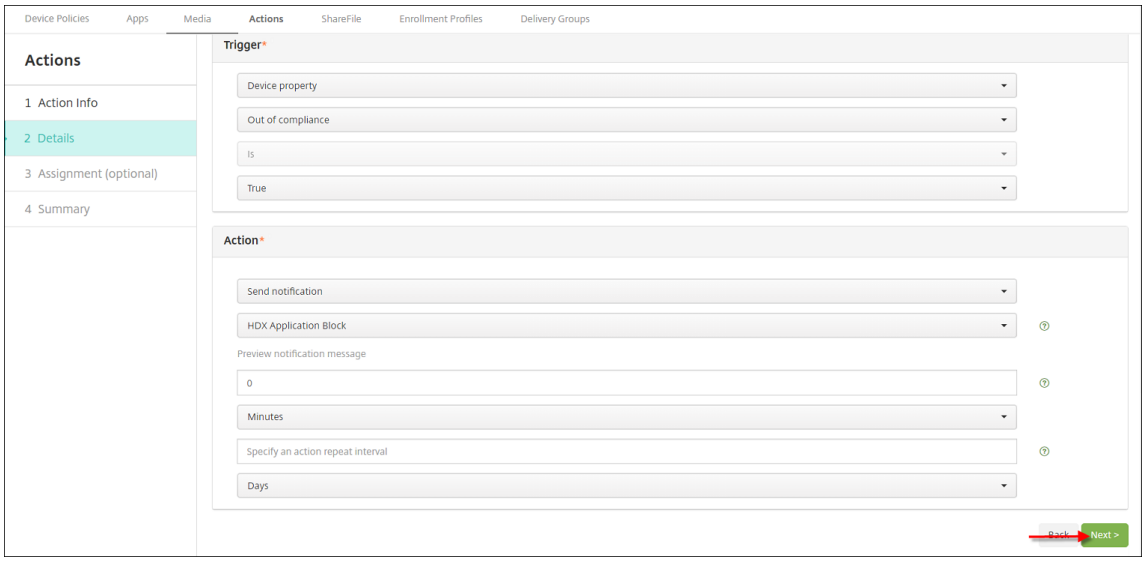
1. Citrix Endpoint Management コンソールで、［構成］**>**［アクション］の順にクリックします。［操作］ページが開きます。
2. ［追加］をクリックして操作を追加します。［アクション情報］ページが開きます。
3. ［アクション情報］ページで、操作の名前と説明を入力します。

   - 名前：HDX ブロック通知
   - 説明：デバイスがコンプライアンス違反である場合の HDX ブロック通知

4. ［次へ］をクリックします。［アクションの詳細］ページが開きます。
5. ［トリガー］一覧で、以下を実行します。

   - ［デバイスプロパティ］を選択します。

- ［コンプライアンス違反］を選択します。
- ［=］を選択します。
- ［真］を選択します。



6. ［操作］一覧で、トリガーが満たされたときに実行される操作を指定します。

   - ［通知を送信］を選択します。
   - 作成した通知である［**HDX Application Block**］を選択します。
   - **0** を選択します。この値を 0 に設定すると、トリガー条件が満たされるとすぐに通知が送信されます。

7. Citrix Endpoint Management デリバリーグループまたはこの操作を適用するグループを選択します。この例では、［**AllUsers**］を選択します。
8. 操作の概要を確認します。
9. ［次へ］をクリックし、［保存］をクリックします。

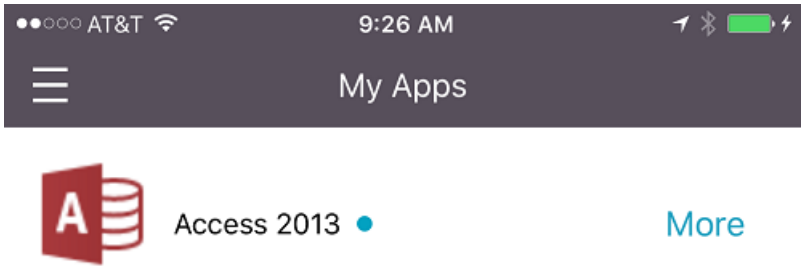
自動化された操作の設定について詳しくは、「自動化された操作」を参照してください。

ユーザーが **HDX** アプリに再度アクセスする方法

デバイスがコンプライアンスを再び満たすようになると、ユーザーは HDX アプリに再びアクセスできます。

1. デバイスで、Citrix Secure Hub ストアにアクセスして、ストア内のアプリを更新します。
2. 対象のアプリに移動して ［追加］をタップします。

アプリが追加されると、［マイアプリ］の横に青い点を付けて表示され、新しくインストールされたアプリであることを示します。

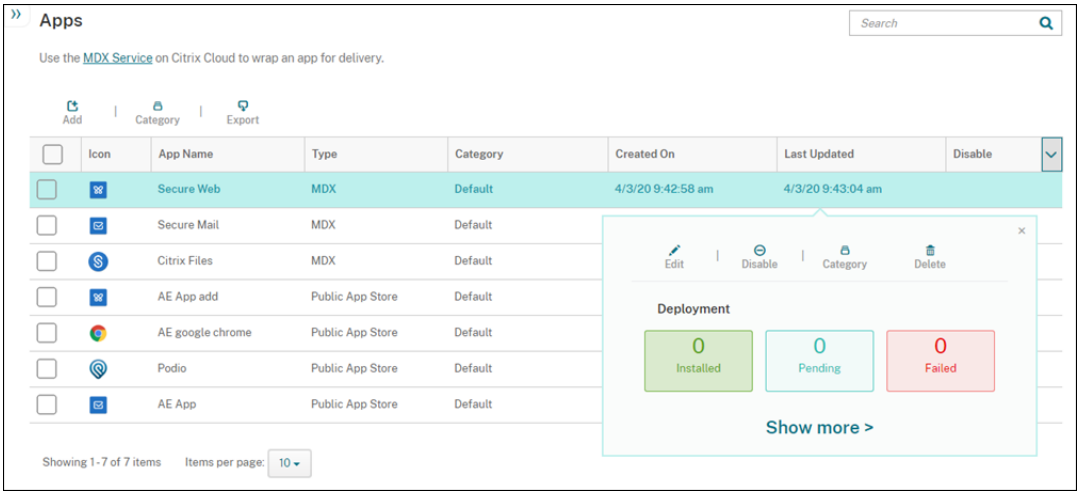


MDX またはエンタープライズアプリのアップグレード

March 15, 2024

Citrix Endpoint Management で MDX またはエンタープライズアプリをアップグレードするには、Citrix Endpoint Management コンソールでアプリを無効にしてから、アプリの新しいバージョンをアップロードします。

1. Citrix Endpoint Management コンソールで、[構成] > [アプリ] の順にクリックします。[アプリ] ページが開きます。
2. 管理対象デバイス（モバイルデバイス管理で Citrix Endpoint Management に登録されたデバイス）の場合は、スキップして手順 3 に進みます。非管理対象デバイス（エンタープライズアプリ管理の目的のみで Citrix Endpoint Management に登録されたデバイス）の場合は、次の手順に従います:
   a) [アプリ] の表で、アプリの横のチェックボックスをオンにするか、更新するアプリを含む行をクリックします。
   b) 表示されるメニューで、[無効にする] をクリックします。



c) 確認のダイアログボックスで ［無効］をクリックします。アプリの ［無効にする］列に「無効」と表示されます。

> 注:
>
> アプリが無効になっている場合、ユーザーはログオフ後にそのアプリに再接続することはできません。アプリの無効化は任意の設定ですが、アプリの機能の問題を避けるために、アプリを無効にすることをお勧めします。たとえば、管理者が新しいバージョンをアップロードしているときにユーザーがアプリのダウンロードを要求する場合、問題が発生する可能性があります。

3. ［アプリ］の表で、アプリの横のチェックボックスをオンにするか、更新するアプリを含む行をクリックします。
4. 表示されるメニューで、［編集］をクリックします。アプリに対して最初に選択したプラットフォームが選択された状態で、［アプリ情報］ページが開きます。
5. 次の設定を構成します:

   - 名前: 任意で、アプリ名を変更します。
   - 説明: 任意で、アプリの説明を変更します。
   - アプリカテゴリ: 任意で、アプリのカテゴリを変更します。

6. ［次へ］をクリックします。最初に選択したプラットフォームのページが開きます。選択したプラットフォームごとに、以下の操作を行います。

   a) ［アップロード］をクリックしてアップロードするファイルの場所に移動し、置き換えるファイルを選択します。アプリが Citrix Endpoint Management にアップロードされます。

   Android Enterprise 用のアプリをアップロードする場合は、管理対象 Google Play ウィンドウが開きます。ここにアプリの新しいバージョンをアップロードします。詳しくは、「Android Enterprise アプリの配布」を参照してください。

b) 任意で、プラットフォームのアプリの詳細とポリシー設定を変更します。

c) 任意で、展開規則の構成およびアプリストアの構成を行います。詳しくは、「MDX アプリの追加」を参照してください。

7. ［保存］をクリックします。［アプリ］ページが開きます。

8. 手順 2 でアプリを無効にした場合は、次の手順に従います。

a) ［アプリ］の表で更新したアプリをクリックして選択し、表示されるメニューで ［有効にする］をクリックします。

b) 確認ダイアログボックスが表示されたら、［有効にする］をクリックします。これで、ユーザーがアプリにアクセスでき、アプリのアップグレードを求める通知を受信できるようになりました。

メディアの追加

March 15, 2024

Citrix Endpoint Management にメディアを追加して、ユーザーデバイスにそのメディアを展開できます。Citrix Endpoint Management を使用して、Apple の一括購入を介して取得した Apple Books を展開することができます。

Citrix Endpoint Management で一括購入アカウントを構成すると、購入済みブックや無料ブックが ［構成］> ［メディア］に表示されます。［メディア］ページでデリバリーグループを選択し、展開規則を指定して、iOS デバイスに展開するブックを構成します。

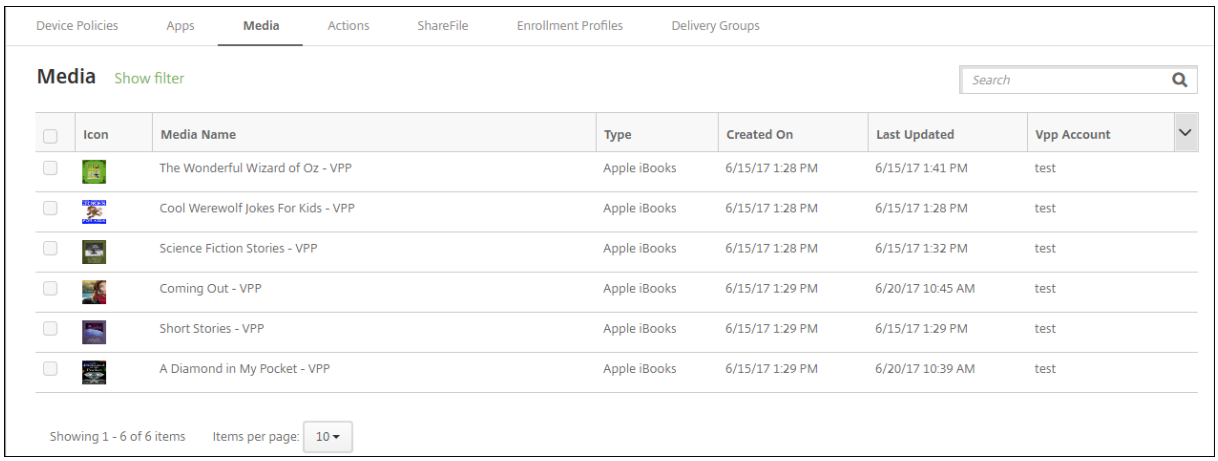
ユーザーが初めてブックを受信し、一括購入ライセンス契約に同意したときに、展開されたブックがデバイスにインストールされます。ブックは Apple Book アプリに表示されます。ユーザーからブックライセンスの割り当てを解除したり、デバイスからブックを削除することはできません。Citrix Endpoint Management では、ブックは必須メディアとしてインストールされます。インストールされたブックがユーザーによってデバイスから削除されても、そのブックは Apple Book アプリ内に保持されて、いつでもダウンロードできます。

前提条件

- iOS デバイス
- 「Apple の一括購入」の説明に従って、Citrix Endpoint Management で Apple の一括購入を構成します。

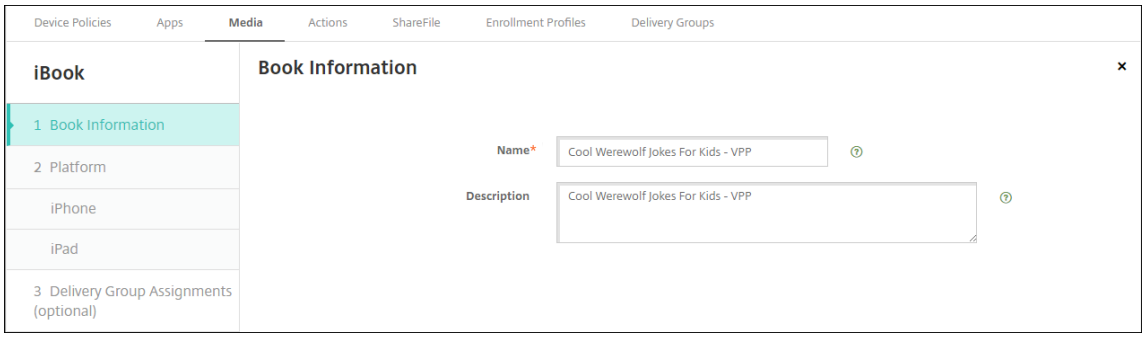
ブックの構成

一括購入を介して取得した Apple Books は、［構成］> ［メディア］ページに表示されます。



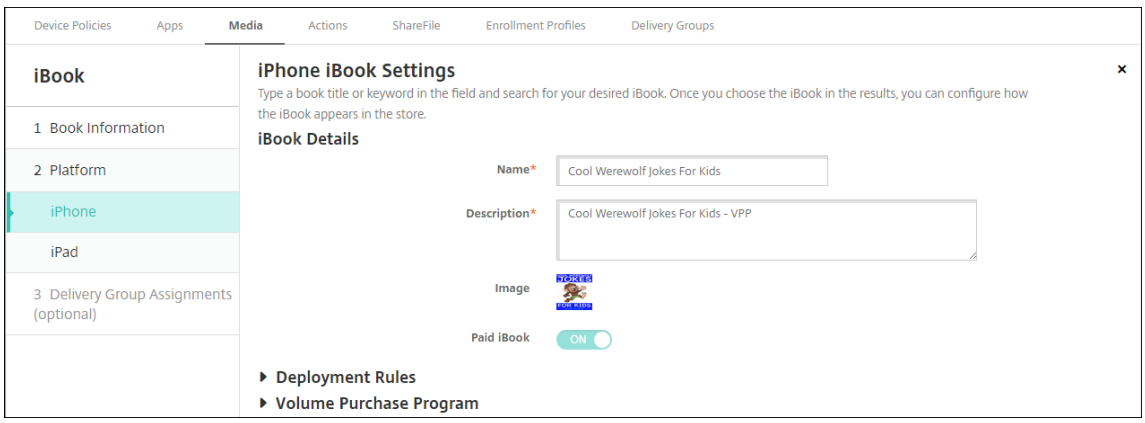
展開の **Apple Book** を構成するには

1. ［構成］**>**［メディア］の順に選択し、ブックを選択して ［編集］をクリックします。［ブック情報］ページが開きます。

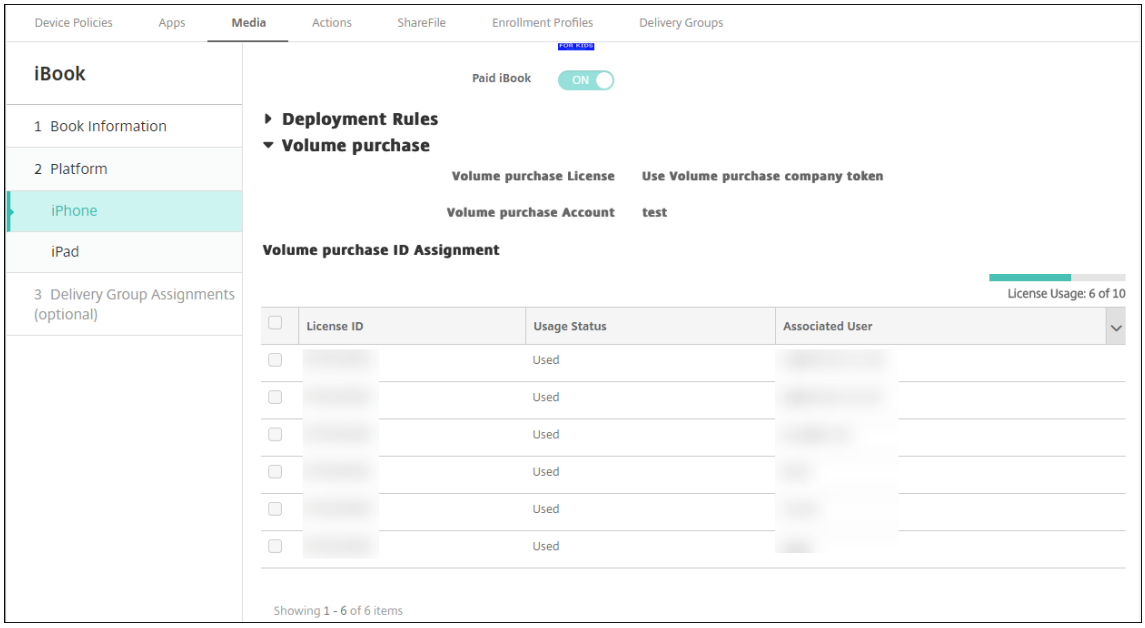


名前と説明は、Citrix Endpoint Management コンソールとログにのみ表示されます。

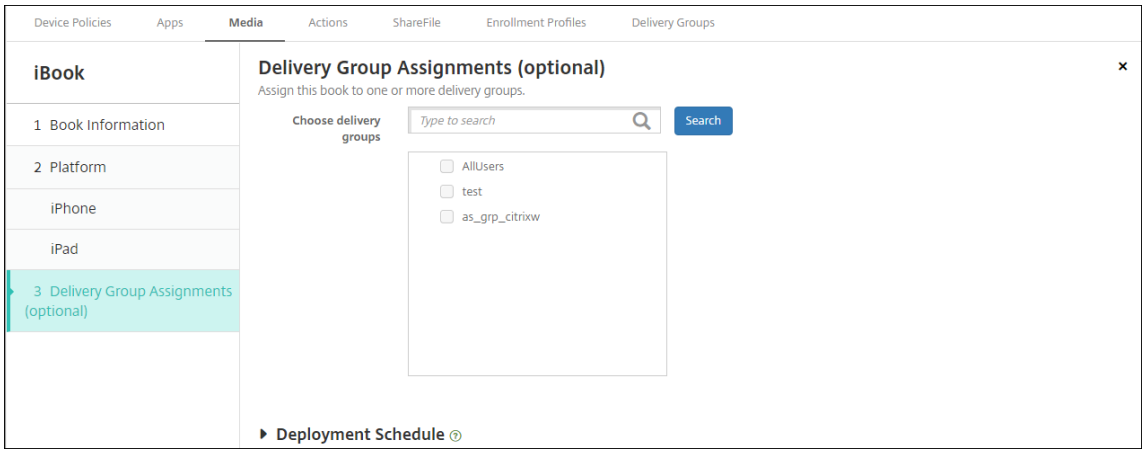
2. ［**iPhone iBook** の設定］ページと ［**iPad iBook** の設定］ページで、ブックの名前と説明は任意で変更できますが、これらの設定は変更しないことをお勧めします。画像は参考用であり、編集することはできません。［購入済み **iBook**］には、Apple の一括購入を介して購入したブックであることが表示されます。



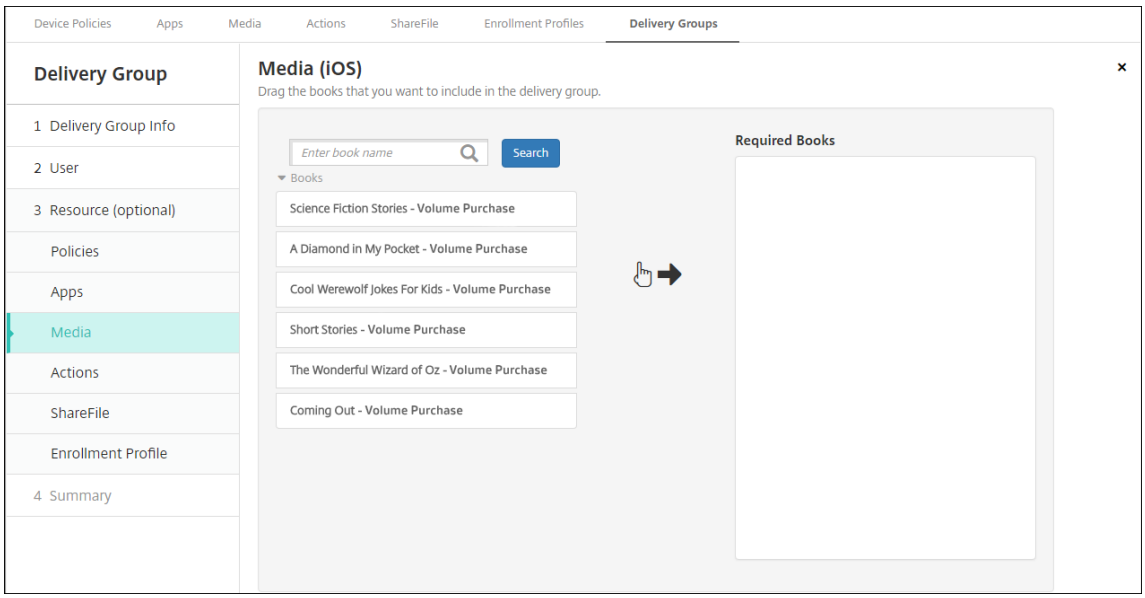
展開規則を指定したり、一括購入情報を表示したりすることもできます。



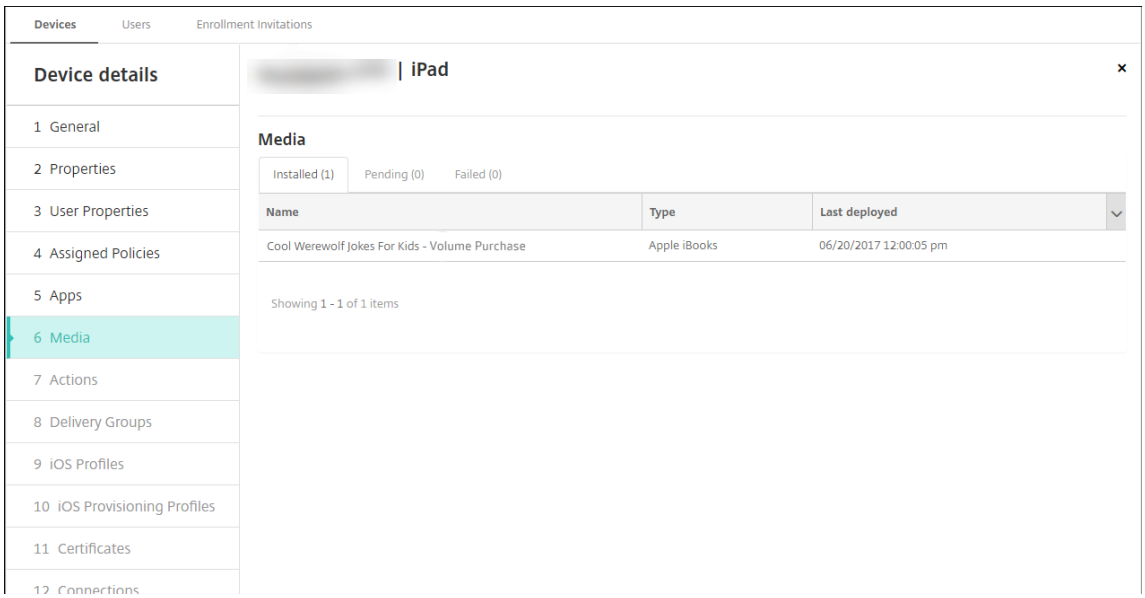
3. オプションで、ブックをデリバリーグループに割り当てて、展開スケジュールを設定することもできます。



また、[構成] > [デリバリー グループ] の順に選択し、[メディア] タブでデリバリーグループにブックを割り当てることもできます。Citrix Endpoint Management では必須ブックの展開のみがサポートされます。

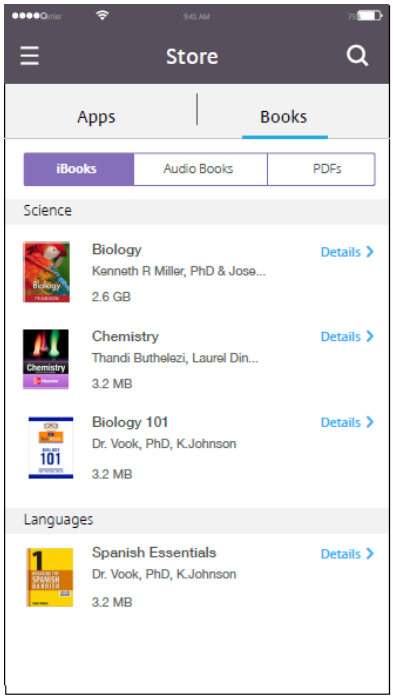


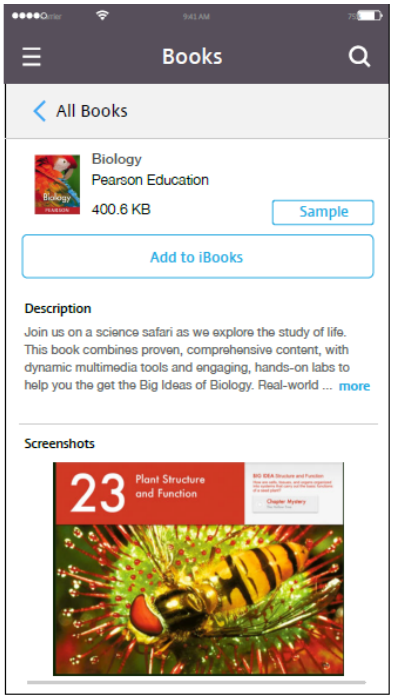
4. ［管理］> ［デバイス］の順に選択し、［メディア］タブを使用して展開状況を表示します。

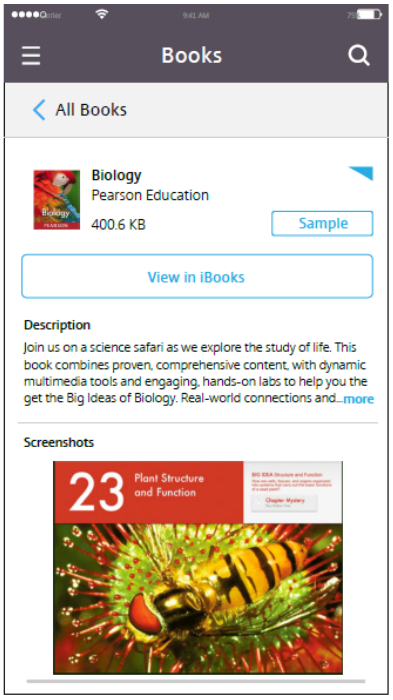


> 注:
>
> ［構成］> ［メディア］ページで、ブックを選択して ［削除］をクリックすると、Citrix Endpoint Management ではそのブックが一覧から削除されます。ただし、Apple の一括購入から削除されない限り、Citrix Endpoint Management が次に Apple の一括購入と同期するときに、そのブックは再び一覧に表示されます。ブックを一覧から削除しても、デバイスからは削除されません。

ブックは、次の例のようにユーザーデバイスに表示されます。







リソースの展開

March 15, 2024

デバイスの構成および管理は、通常 Citrix Endpoint Management コンソールでリソース（ポリシー、アプリ、メディア）および操作（アクション）を作成し、デリバリーグループを使用してそれらをパッケージ化します。デリバリーグループがユーザーのカテゴリを定義することによって、特定のポリシー、アプリ、メディア、アクションをデバイスに展開できます。Citrix Endpoint Management コンソールを使用して、以下のことを実行できます:

- デリバリーグループを追加、管理、および展開する。
- Citrix Endpoint Management がリソースおよび操作をデリバリーグループでデバイスにプッシュする順番を変更する。この順序は、_ 展開順 _ と呼ばれます。

  展開順は、Citrix Endpoint Management コンソールで指定できます。ただし、ユーザーが複数のデリバリーグループに属していて、そのデリバリーグループにポリシーの重複または矛盾があるときには、Citrix Endpoint Management が展開順を決定します。「計算の手順」を参照してください。

デリバリーグループについて

通常、デリバリーグループへの追加は、ユーザーの会社、国、部門、オフィスの住所、役職などの特性に基づいて行われます。デリバリーグループを使用することにより、どのユーザーがどのリソースをいつ取得するかを詳細に管理できます。デリバリーグループは、全員に展開することや、定義したユーザーグループに展開することができます

Citrix Endpoint Management をインストールして構成すると、デフォルトの AllUsers デリバリーグループが作成されます。このグループには、すべてのローカルユーザーと Active Directory ユーザーが含まれます。AllUsers グループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。「AllUsers デリバリーグループの有効化および無効化」を参照してください。

デリバリーグループにリソースを展開する場合は、デリバリーグループのすべてのユーザーにプッシュ通知を送信します。Apple デバイスの場合は、Apple プッシュ通知サービスを使用して通知を送信します。詳しくは、「APN 証明書」を参照してください。Android デバイスの場合は、Firebase Cloud Messaging（FCM）を使用します。詳しくは、「Firebase Cloud Messaging」を参照してください。Windows デバイスの場合は、Windows プッシュ通知サービス（WNS）を使用します。

リソースの展開について

リソースをデバイスにプッシュする場合は、次の点を考慮してください：

- 展開順： Citrix Endpoint Management がリソース（ポリシー、アプリ、メディア）および操作をデバイスにプッシュする順序です。展開順は、デバイス管理（MDM）用に、またはアプリケーション管理（MAM）と MDM の組み合わせ用に構成された登録プロファイルを持つデリバリーグループ内のデバイスに適用されます。
- 展開規則： Citrix Endpoint Management は、展開規則によってユーザープロパティとデバイスプロパティを指定して、ポリシー、アプリ、メディア、操作、デリバリーグループをフィルター処理できます。たとえば、ドメイン名が特定の値に一致した場合、展開規則が展開パッケージをプッシュするよう指定できます。

  デリバリーグループ内で、ユーザーとデバイスのプロパティに基づいて、リソースを受け取るユーザーとデバイスのサブセットを指定できます。デリバリーグループ内のユーザーとデバイスのプロパティによるフィルタリングは、リソースに設定されている展開規則よりも優先されます。
- 展開スケジュール： Citrix Endpoint Management では、ポリシー、アプリ、メディア、操作に対して指定する展開スケジュールを使用して、これらのアイテムの展開を制御できます。展開が即座に実行されるか、特定の日時に実行されるか、展開条件が満たされたときに実行されるかを指定できます。規則を作成するときにスケジュールを指定します。「展開規則を構成する」を参照してください。

デリバリーグループを追加する前に、展開の順序、規則、スケジュールを展開の目標に対応させる方法を検討します。

展開順

展開順は Citrix Endpoint Management がリソースをデバイスにプッシュする順番です。リソースの前提条件とリソース間の依存関係がある場合、展開の順序は重要です。リソースには、ポリシー、アプリ、アクション、デリバリーグループが含まれます。

たとえば、証明書ベースの認証がある Wi-Fi ポリシーをプッシュする場合は、Wi-Fi ポリシーの前に証明書ポリシーをプッシュする必要があります。これを実行しないと、エラーが発生します。逆に、一部のポリシー（利用規約、ソフトウェアインベントリ、アクションなど）では、展開の順序は重要ではありません。

デリバリーグループを追加するときに、リソースがデバイスに展開される順序を指定できます。ただし、ユーザーが複数のデリバリーグループに属していて、そのデリバリーグループにポリシーの重複または矛盾があるときには、Citrix Endpoint Management が常にそれぞれの状況を特定します。このような場合、Citrix Endpoint Management は、デバイスに配信するオブジェクトと実行するアクションの両方の展開順を計算します。

展開順を判断する際、Citrix Endpoint Management はリソースにフィルターを適用して条件（展開規則、展開スケジュール）を制御します。次の表は、これらの基準のどれを各リソースの種類に適用できるかを示しています。

リソース	デバイスプラットフォーム	展開規則	展開スケジュール	ユーザー/グループ
デバイスポリシー	Y	Y	Y	-
アプリ	Y	Y	Y	-
メディア	Y	Y	Y	-
操作	-	Y	Y	-
デリバリー グループ	-	Y	-	Y

計算の手順

Citrix Endpoint Management が展開順を計算する必要がある場合、これらの手順を実行します。

> 注:
>
> デバイスのプラットフォームは計算の手順に影響しません。

1. ユーザーやグループのフィルターおよび展開規則に基づいて、特定のユーザーが存在するすべてのデリバリーグループを判断します。
2. 選択したデリバリーグループ内のすべてのリソース（ポリシー、アプリ、メディア、操作）の順序付き一覧を作成します。その一覧は、デバイスプラットフォーム、展開規則、および展開スケジュールのフィルターに基づいています。順序のアルゴリズムは、次のとおりです:
    a) ユーザー定義の展開順があるデリバリーグループのリソースを、展開順がないデリバリーグループのリソースの前に配置します。「ユーザー定義の順序での計算例」を参照してください。
    b) 同じ条件のデリバリーグループの中から、デリバリーグループ名のアルファベットの降順にリソースを順序付けします。たとえば、Citrix Endpoint Management はデリバリーグループ B のリソースをデリバリーグループ A のリソースの前に配置します。
    c) 並べ替え中、デリバリーグループのリソースに管理者定義の展開順が指定されている場合、その順序を保持します。そうでない場合は、デリバリーグループ内でリソースをリソース名で並べ替えることができます。

d) 同じリソースが複数回表示される場合、重複するリソースを削除します。これらのリソースのうち最初の 1 つだけを提供します。

管理者定義の順序を持つリソースを、管理者定義の順序のないリソースの前に展開します。

管理者定義の順序での計算例　2 つのデリバリーグループがあるとします:

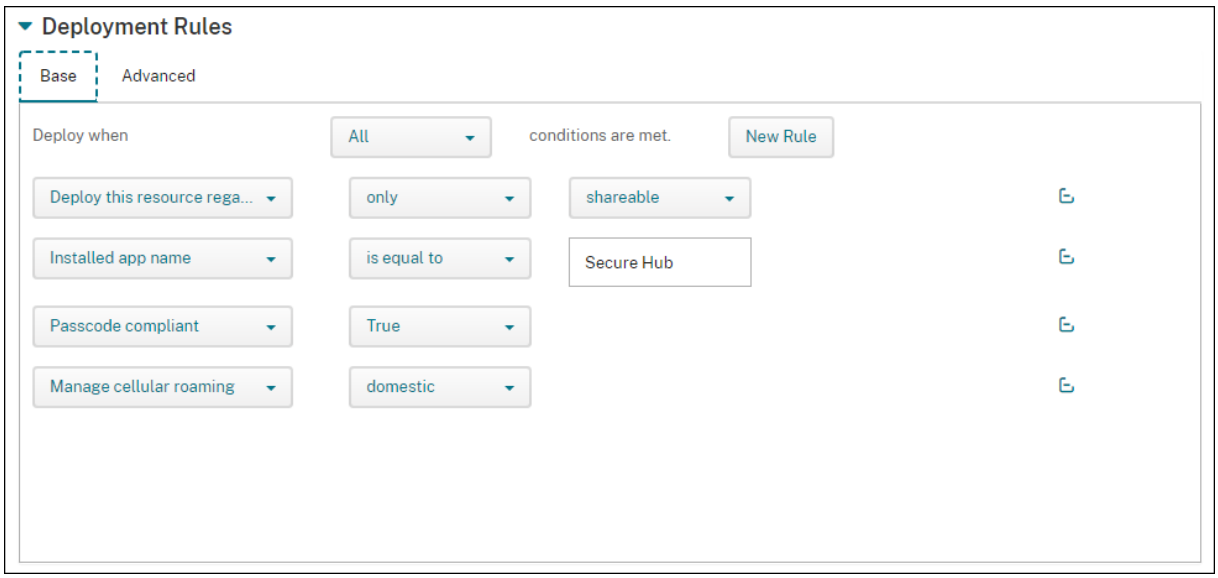
- デリバリーグループ、Account Manager 1: リソースの順序が _ 未指定 _ です。ネットワークポリシーおよびパスコードポリシーを含みます。
- デリバリーグループ、Account Manager 2: リソースの順序が _ 指定 _ です。接続のスケジューリングポリシー、制限ポリシー、パスコードポリシー、およびネットワークポリシーが順番に含まれます。

計算アルゴリズムが名前のみを基準に展開グループを順序づけた場合、Citrix Endpoint Management はデリバリーグループ Account Manager 1 から開始して、次の順序で展開します: ネットワーク、パスコード、接続のスケジューリングおよび制限。Citrix Endpoint Management は、Account Manager 2 デリバリーグループの重複するパスコードおよびネットワークを無視します。

ただし、Account Managers 2 グループには、管理者指定の展開順序があります。したがって、計算アルゴリズムによって、Account Managers 2 デリバリーグループのリソースが、Account Managers 1 デリバリーグループのリソースより、一覧の上位に配置されます。その結果、Citrix Endpoint Management はこの順序でポリシーを展開します: 接続のスケジューリング、制限、パスコード、およびネットワーク。Citrix Endpoint Management は、Account Manager 1 デリバリーグループからのネットワークポリシーおよびパスコードポリシーを無視します。重複しているためです。このアルゴリズムは、Citrix Endpoint Management 管理者によって指定された順序を優先します。

展開規則を構成する

特定の条件が満たされた場合にリソースを配信するように展開規則を構成します。基本または高度な展開規則を構成できます。



基本エディターを使用して展開規則を追加する場合は、最初にリソースを展開するタイミングを選択します。

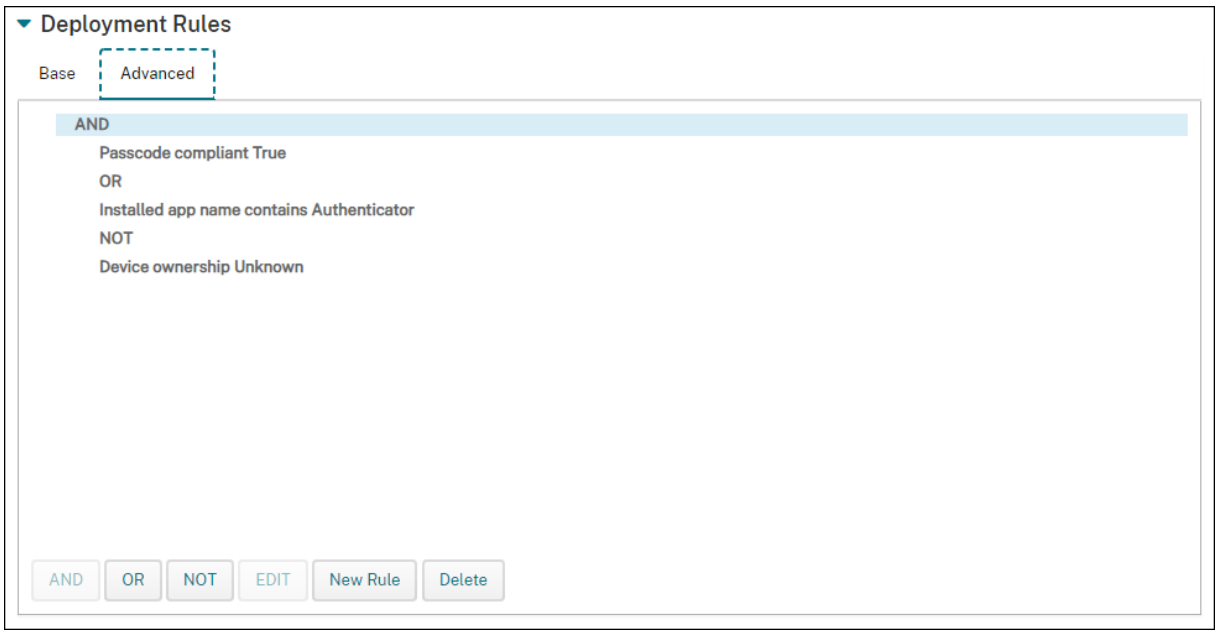
- すべて：ユーザーまたはデバイスが構成したすべての条件を満たしたときに、リソースを配信します。
- いずれか：ユーザーまたはデバイスが構成した条件の少なくとも 1 つを満たしたときに、リソースを配信します。

追加する利用可能な規則の一覧から規則を選択するには、[新しい規則] をクリックします。利用可能な規則は、展開されているリソースと、リソースを構成するプラットフォームによって異なります。各規則には条件があります。

リソースの展開を指定できます：

- 選択したプロパティが存在する場合のみ、または選択したプロパティが存在する場合以外。
- 入力したテキストとプロパティが完全に一致する場合、入力したテキストがプロパティに含まれている場合、または入力したテキストとプロパティが一致しない場合。
- デバイスまたはユーザーが、選択したプロパティに準拠している場合、または選択したプロパティに準拠していない場合。
- デバイスまたはユーザーのプロパティが、事前定義された一覧から選択した条件に一致する場合。

高度なエディターを使用して、より複雑な展開規則を作成します。選択する規則は他にもあり、高度な規則を作成する場合にさまざまなブール論理演算子を組み合わせることができます。



デリバリーグループと連携する

次の方法でデリバリーグループと連携できます:

- デリバリーグループの追加
- デリバリーグループへの展開
- デリバリー グループの削除
- デリバリーグループの編集
- AllUsers デリバリーグループの有効化および無効化。

デリバリーグループの追加

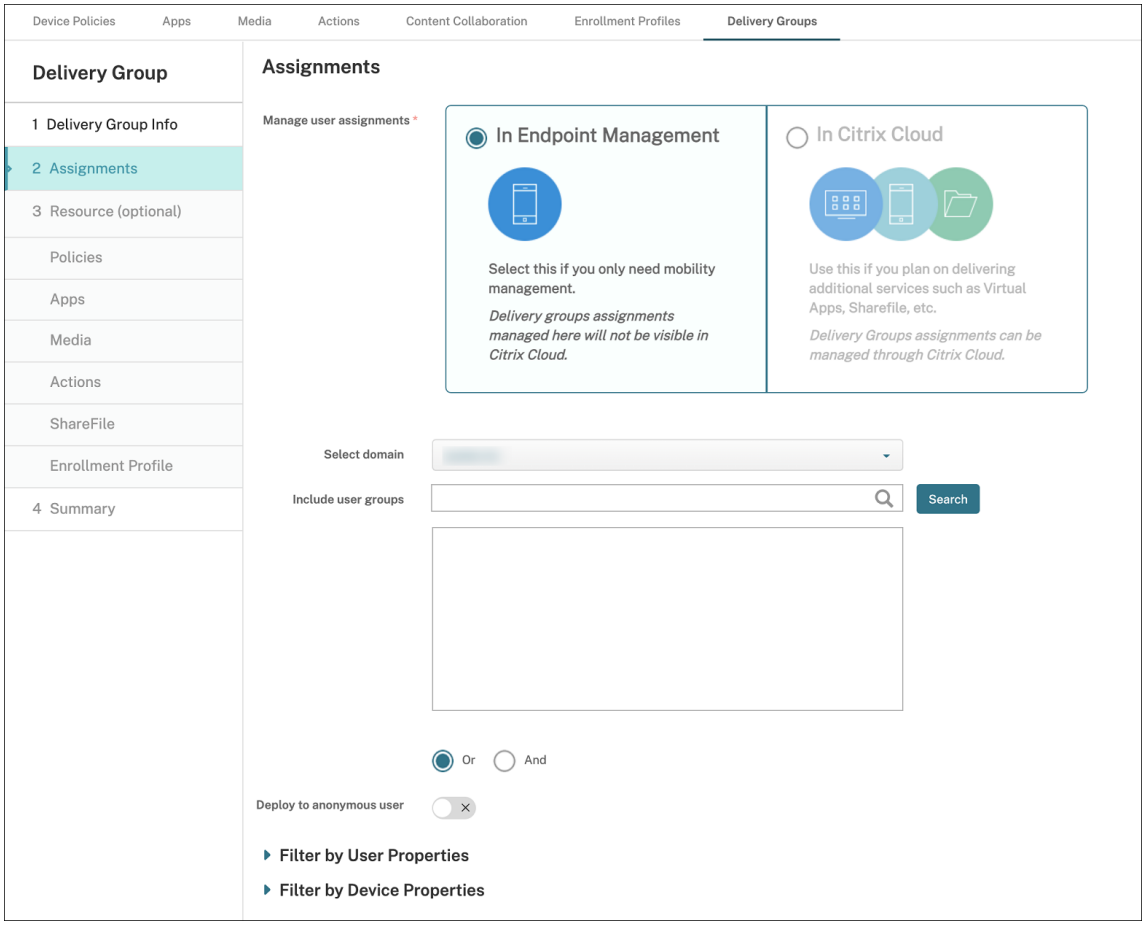
デリバリーグループを作成するときは、Citrix Endpoint Management または Citrix Cloud でユーザー割り当てを管理するかどうかを指定します。この仕様は、デリバリーグループを作成した後は変更できません。

デリバリーグループを使用して他の Citrix Cloud サービスを提供する予定である場合は、ユーザー割り当てが Citrix Cloud で管理されるように指定します。その他の Citrix Cloud サービスには、Citrix Virtual Apps and Desktops、ShareFile、または Secure Browser サービスが含まれます。Active Directory ユーザーは、Citrix Cloud で管理されているデリバリーグループにのみ追加できます。

ユーザーやアプリのデリバリーグループのモビリティ管理のみが必要な場合、[ユーザー割り当ての管理] を [**Citrix Endpoint Management** 使用] に設定します。Citrix Cloud の Citrix Endpoint Management で管理されているユーザーを含むデリバリーグループは表示できません。したがって、Citrix Endpoint Management で管理されるデリバリーグループを使用して他のサービスを配信することはできません。

> 注:
>
> デバイスポリシーと登録プロファイルを作成する前に、デリバリーグループを作成することをお勧めします。これらの作成については、「デバイスポリシー」と「登録プロファイル」を参照してください。

1. Citrix Endpoint Management コンソールで、[構成] > [デリバリーグループ] の順にクリックします。
2. [デリバリーグループ] ページで、[追加] をクリックします。
3. [デリバリーグループ情報] ページでデリバリーグループの名前と説明を入力して、[次へ] をクリックします。
4. [割り当て] ページで、デリバリーグループの割り当てを管理する方法を指定します。



- ユーザー割り当ての管理:
  - **Citrix Endpoint Management** の場合:モビリティ管理だけが必要なユーザーとアプリのデリバリーグループを作成する場合は、このオプションを選択します。ユーザー割り当てが Citrix Cloud の Citrix Endpoint Management で管理されているデリバリーグループは、表示されず、他のサービスの配信には使用できません。
  - **Citrix Cloud** の場合:デリバリーグループを使用して他のサービスを配信する場合は、このオプションを選択します。これらのサービスには、Citrix Virtual Apps and Desktops や ShareFile などが含まれます。

5. デリバリーグループにユーザーを追加します。

> 重要:
>
> デリバリーグループの作成後に ［ユーザー割り当ての管理］設定を変更することはできません。

- ドメインを選択：一覧から、ユーザーを選択するドメインを選択します。
- ユーザーグループを含める：次のいずれかを行います：
  - ユーザーグループの一覧で、追加するグループを選択します。選択したグループが ［選択したユーザーグループ］一覧に表示されます。
  - ［検索］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。検索ボックスにグループ名の全部または一部を入力してから ［検索］をクリックして、検索を絞り込むこともできます。

  ［選択したユーザーグループ］の一覧からユーザーグループを削除するには、次のいずれかを行います：

  - ［選択したユーザーグループ］の一覧で、削除する各グループの横にある ［**X**］をクリックします。
  - ［検索］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。または、グループ名の全部または一部を入力してから ［検索］をクリックして、検索を絞り込むことができます。削除する各グループのチェックボックスをオフにします。
- **Or/And**：リソースが展開されるユーザーがいずれかのグループに属していればよいか（[Or]）、すべてのグループに属している必要があるか（[And]）を選択します。
- 匿名ユーザーに展開：デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスを Citrix Endpoint Management に接続することを許可したユーザーを指します。

6. ［フィルター基準：ユーザープロパティ］または ［フィルター基準：デバイスプロパティ］を開いて、デリバリーグループのリソース管理方法を指定します。

- ［フィルター基準：デバイスプロパティ］を選択した場合は、デバイスプラットフォームを展開して、展開規則を構成します：
  - デバイスプロパティ **- Android**（「Android デバイスにリソースを展開するための規則を作成する」を参照）
  - デバイスプロパティ **- iOS**
  - デバイスプロパティ **- Windows** デスクトップ/タブレットのみ
- デフォルトでは ［基本］タブが表示されます。［基本］タブで、ポリシーをいつ展開するかを指定します。すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトオプションは **All** に設定されています。
  - ［新しい規則］をクリックして条件を定義します。
  - 一覧から条件を選択します。たとえば、［デバイス所有権］と［BYOD］を選択します。
  - 追加する条件ごとに ［新しい規則］をクリックします。

- ［詳細］タブをクリックし、ブール値オプションを使用して規則を組み合わせます。［基本］タブで選択した条件が表示されます。
  - ［**AND**］、［**OR**］、または ［**NOT**］を選択して、［新しい規則］をクリックします。
  - 一覧で、規則に追加する条件を選択し、右側のプラス記号（＋）をクリックします。
    いつでも、条件をクリックして選択し、［編集］をクリックして条件を変更したり、［削除］をクリックして条件を削除したりすることができます。

7. ［次へ］をクリックして、［ポリシー］ページに移動します。オプションとして、このページでデリバリーグループのポリシー、アプリ、メディア、アクションを追加します。詳しくは、次のページを参照してください：

   - デリバリーグループへのポリシーの追加
   - デリバリーグループへのアプリの追加
   - デリバリーグループへのメディアの追加
   - デリバリーグループへのアクションの追加

8. デリバリーグループに問題がなければ、［概要］をクリックして構成の概要を表示します。
9. ［保存］をクリックします。新しいデリバリーグループが ［デリバリーグループ］ページに表示されます。

デリバリーグループへのポリシーの追加

1. ［**Resources**（**optional**）］一覧から ［**Policies**］をクリックします。
2. 追加するポリシーごとに、以下の操作を行います：

   - 使用可能なポリシーの一覧をスクロールして、追加するポリシーを見つけます。または、検索ボックスにポリシー名の全体または一部を入力して ［検索］をクリックします。
   - 追加するポリシーを右側のボックス内へドラッグします。

   ボックスからポリシーを削除するには、ポリシー名の横にある ［**X**］をクリックします。

3. ［次へ］をクリックして、［アプリ］リソースページに移動します。

デリバリーグループへのアプリの追加

1. 追加するアプリごとに、以下の操作を行います：

   - 使用可能なアプリの一覧をスクロールして、追加するアプリを見つけます。または、検索ボックスにアプリ名の全体または一部を入力して ［検索］をクリックします。
   - アプリを ［必須アプリ］ボックス内または ［任意アプリ］ボックス内へドラッグします。

   必須とマーク付けされたアプリについては、次のような場合に、ユーザーはすみやかに更新プログラムを受信できます：

   - アップロードした新しいアプリを必須アプリとしてマーク付けした場合。

- 既存のアプリを必須アプリとしてマーク付けした場合。
- 必須アプリをユーザーが削除した場合。
- Citrix Secure Hub の更新が利用可能な場合。

この機能を有効にする方法を含む、必須アプリの強制展開については、「必須のアプリとオプションのアプリについて」を参照してください。

ボックスからアプリを削除するには、アプリケーション名の横にある ［**X**］をクリックします。

2. ［次へ］をクリックして、［メディア］ページに移動します。

デリバリーグループへのメディアの追加

1. 追加する各ブックで、次の手順を実行します。

   - 使用可能なブックの一覧をスクロールして、追加するブックを見つけます。または、検索ボックスにブック名の全体または一部を入力して ［検索］をクリックします。
   - 追加するブックを ［必須ブック］ボックス内へドラッグします。

   必須とマーク付けされたブックについては、次のような場合に、ユーザーはすみやかに更新プログラムを受信します。

   - アップロードした新しいブックを必須ブックとしてマーク付けした場合。
   - 既存のブックを必須ブックとしてマーク付けした場合。
   - 必須ブックをユーザーが削除した場合。
   - Citrix Secure Hub の更新が利用可能な場合。

   ボックスからブックを削除するには、ブック名の横にある ［**X**］をクリックします。

2. ［次へ］をクリックして、［アクション］ページに移動します。

デリバリーグループへのアクションの追加

1. 追加するアクションごとに、以下の操作を行います:

   - 使用可能なポリシーの一覧をスクロールして、追加するアクションを見つけます。または、検索ボックスにアクション名の全体または一部を入力して ［検索］をクリックします。
   - 追加するアクションを右側のボックス内へドラッグします。

   ボックスからアクションを削除するには、アクション名の横にある ［**X**］をクリックします。

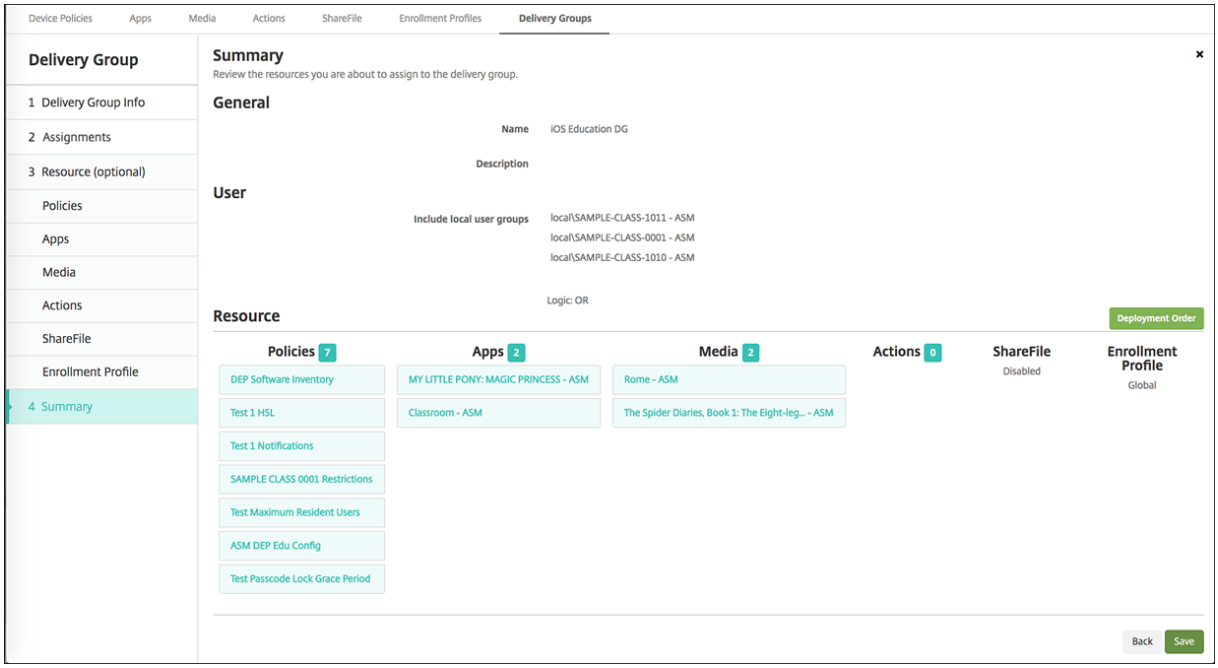
2. ［次へ］をクリックして ［**ShareFile**］ページに移動します。

ShareFile 構成を適用する　Citrix ShareFile ページの表示は、Citrix Endpoint Management（［構成］**>** [**ShareFile**]）を Enterprise アカウント用に構成したか、ストレージゾーンコネクタ用に構成したかによって異なります。

- Citrix Endpoint Management で使用するために Enterprise アカウントを構成した場合、［**ShareFile** を有効化］を ［オン］に設定します。この設定により、デリバリーグループは ShareFile のコンテンツとデータにシングルサインオンでアクセスできます。
- ストレージゾーンコネクタを Citrix Endpoint Management と組み合わせて使用するように構成した場合、ストレージゾーンコネクタを右側のボックスにドラッグしてデリバリーグループに含めます。

構成したオプションの確認および展開順序の変更　［概要］ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。［概要］ページには、リソースがカテゴリ別に表示されます。［概要］ページは、展開順序を表示しません。

> 注:
>
> ［戻る］をクリックして前のページに戻り、構成を変更します。

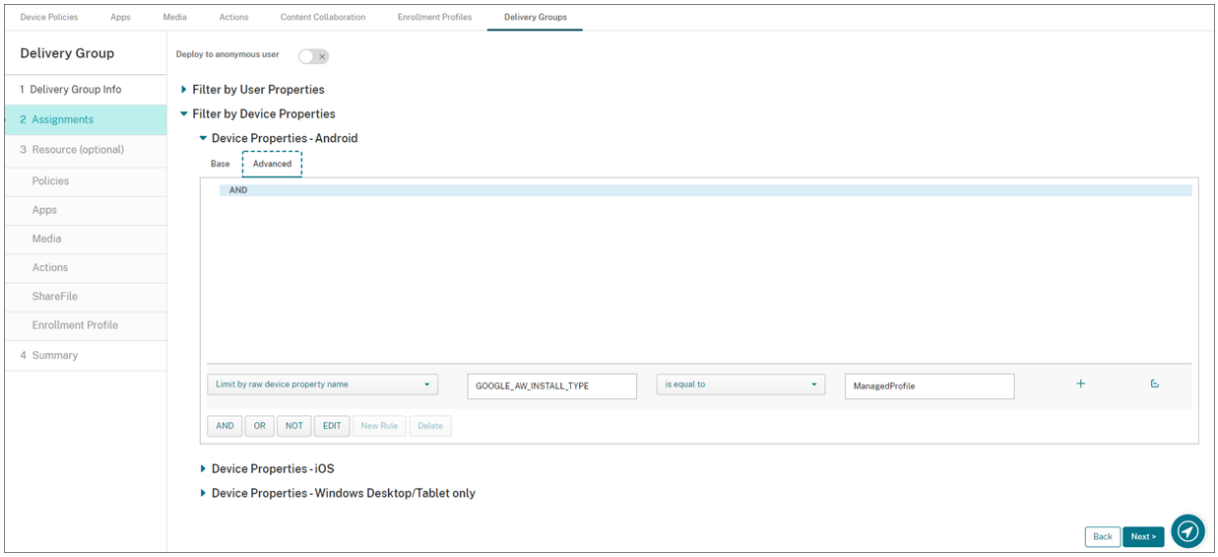


展開順を表示または変更するには:

1. ［展開順］をクリックします。
2. ［展開順］ダイアログボックスで、リソースを展開する順序の場所にドラッグします。リソースは上位から下位の順序で展開されます。
3. ［保存］をクリックして、展開順序を保存します。

デリバリーグループの構成が完了したら、［概要］ページで ［保存］をクリックします。

Android Enterprise にリソースを展開するためのルールを作成する　Android デバイスのプロパティ規則を使用して、Android Enterprise デバイスへのデリバリーグループの展開を管理できます。同じユーザーに複数のデバイスを登録する場合は、デバイス登録モードまたはデバイスアプリケーションパッケージ ID に基づいて、Android Enterprise の高度なフィルターを作成できます。



デバイス登録モードを使用して、デリバリーグループを Android Enterprise デバイスに展開するには:

1. デリバリーグループを作成します。
2. ［割り当て］ページで、［フィルター基準：デバイスプロパティ］を展開します。
3. ［デバイスプロパティ **- Android**］で、［詳細設定］タブを開き、［新しい規則］をクリックします。
4. 一覧から、規則に追加する条件を選択します:
    - 新しい Android Enterprise デバイスの場合は、［未処理のデバイスプロパティ名で制限する］を選択し、最初の値フィールドに「**GOOGLE_AW_INSTALL_TYPE**」を入力します。次に、条件をいずれかの登録モードと同じ設定にする必要があります。
    - 既存の Android Enterprise デバイスの場合は、［未処理のデバイスプロパティ名で制限する］を選択し、最初の値フィールドで ［**Android Enterprise** インストールの種類］を選択します。次に、条件をいずれかの登録モードと同じ設定にする必要があります。
5. 2 番目のフィールドに、Android Enterprise デバイスの登録モードを入力します:
    - **DeviceAdministrator**：仕事での使用のみを目的とした会社所有のデバイスを指定します（デバイス所有者モードとも呼ばれます）
    - **ManagedProfile**：仕事用プロファイル管理に登録されている BYOD 個人用デバイスを指定します（プロファイル所有者モードとも呼ばれます）
    - **CorporateOwnedSingleUse**：専用デバイスを指定します（以前は特定業務専用コーポレート所有端末と呼ばれていました）

- **CorporateOwnedPersonallyEnabled**：仕事用プロファイルを持つ完全管理対象デバイスを指定します（以前は個人対応コーポレート所有端末と呼ばれていました）

6.「デリバリーグループの追加」で説明したように、デリバリーグループの構成を完了します。

詳しくは、「デバイス展開シナリオとプロファイル」を参照してください。

デバイスアプリケーションパッケージ ID を使用して、Android Enterprise デバイスにデリバリーグループを展開するには：

1.［デバイスプロパティ **- Android**］で、［詳細設定］タブを開き、［新しい規則］をクリックします。
2. 一覧で、［インストール済みアプリ名］を選択し、アプリケーションパッケージ ID を入力します。

デリバリーグループの編集

既存のデリバリーグループの名前は変更できません。他の設定を更新するには、［構成］**>**［デリバリーグループ］の順に選択し、編集するグループを選択して、［編集］をクリックします。

AllUsers デリバリーグループの有効化および無効化

AllUsers は、有効化または無効化することができる唯一のデリバリーグループです。他のデリバリーグループとは異なり、AllUsers を削除することはできません。

［デリバリーグループ］ページで、［**AllUsers**］の横にあるチェックボックスをオンにするか、［**AllUsers**］を含む行をクリックして、AllUsers デリバリーグループを選択します。次に、以下のいずれかを行います。

- AllUsers デリバリーグループを無効化するには、［無効］をクリックします。このコマンドは、AllUsers グループが有効（デフォルト）になっている場合にのみ使用できます。デリバリーグループの表の ［無効］の見出しの下に、［無効］が表示されます。
- AllUsers デリバリーグループを有効化するには、［有効］をクリックします。このコマンドは、AllUsers グループが無効になっている場合にのみ使用できます。デリバリーグループの表の ［無効］の見出しの下に、［無効］が表示されなくなりました。

デリバリーグループへの展開

デリバリーグループへの展開とは、Apple、Android、Windows タブレットデバイスを持つすべてのユーザーにプッシュ通知を送信することを意味します。

その他のプラットフォームのデバイスを持つユーザーは、デバイスが既に Citrix Endpoint Management に接続済みであれば、すぐにそのリソースを受信します。接続していない場合は、スケジューリングポリシーに基づいて、次に接続するときにリソースを受信します。

Android デバイスで、アプリストアの［更新可能］の一覧に更新されたアプリが表示されるようにするには、最初にアプリインベントリポリシーをユーザーのデバイスに展開します。

1. ［デリバリーグループ］ページで、次のいずれかを行います：

   - 複数のデリバリーグループに同時に展開するには、展開するグループの横にあるチェックボックスをオンにします。
   - 1 つのデリバリーグループに展開するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

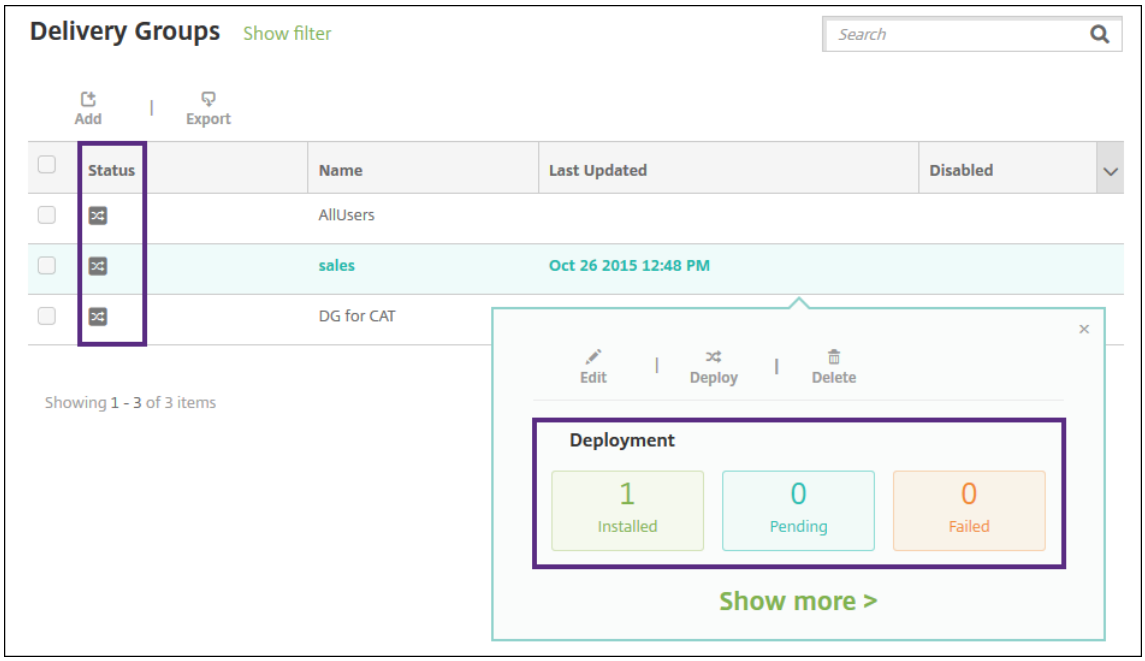
2. ［展開］をクリックします。

   1 つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に ［展開］コマンドが表示されます。

   アプリ、ポリシー、アクションを展開するグループが一覧にあることを確認しします。次に、［展開］をクリックします。デバイスプラットフォームとスケジュール設定ポリシーに基づいて、選択したグループにアプリ、ポリシー、アクションが展開されます。

   ［デリバリーグループ］ページで、次のいずれかの方法により展開ステータスを確認できます。

   - デリバリーグループの ［状態］の見出しの下で、展開エラーを示す展開アイコンを確認します。
   - デリバリーグループを含む行をクリックし、［インストール済み］、［保留中］、［失敗］の展開を示すオーバーレイを表示します。



デリバリーグループの複製

既存のデリバリーグループに類似したデリバリーグループを作成する場合は、デリバリーグループの複製を作成します。新しいデリバリーグループ作成の開始点として複製を使用します。次に、登録プロファイルや AD ユーザーの新しいセットを追加するなど、複製に変更を加えます。

1. Citrix Endpoint Management コンソールで、［構成］>［デリバリーグループ］タブの順に選択します。
2. デリバリーグループの一覧から、新しいグループのベースとして使用するものを選択します。
3. ［複製］を選択します。
4. デリバリーグループを複製するダイアログボックスで、新しいグループの名前と、オプションで説明を入力します。
5. ［複製］を選択します。

デリバリーグループの削除

AllUsers デリバリーグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。「AllUsers デリバリーグループの有効化および無効化」を参照してください。

> 重要:
>
> 削除を取り消すことはできません。

1. ［デリバリーグループ］ページで、次のいずれかを行います:
   - 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。
   - 1 つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。
2. ［削除］をクリックします。

   1 つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に ［削除］コマンドが表示されます。
3. ［削除］ダイアログボックスで ［削除］をクリックします。

［デリバリーグループ］表のエクスポート

1. ［デリバリーグループ］の表の上にある ［エクスポート］をクリックします。Citrix Endpoint Management によって ［デリバリーグループ］表の情報が抽出され、.csv ファイルに変換されます。
2. ブラウザーの通常の手順に従って、.csv ファイルをオープンまたは保存します。

マクロ

March 15, 2024

Citrix Endpoint Management では、次の項目のテキストフィールド内にユーザーまたはデバイスのプロパティデータを設定する方法としてマクロを利用できます:

- ポリシー
- 通知
- 登録テンプレート
- デバイス構成 XML ファイル
- 自動化された操作
- 資格情報プロバイダー証明書署名要求

マクロは、Citrix Endpoint Management により対応するユーザーまたはシステムの値に置換されます。たとえば、何千人ものユーザーがいる 1 つの Exchange プロファイルに、ユーザーのメールボックスの値を事前に設定できます。

マクロの構文

マクロの形式は次のとおりです。

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

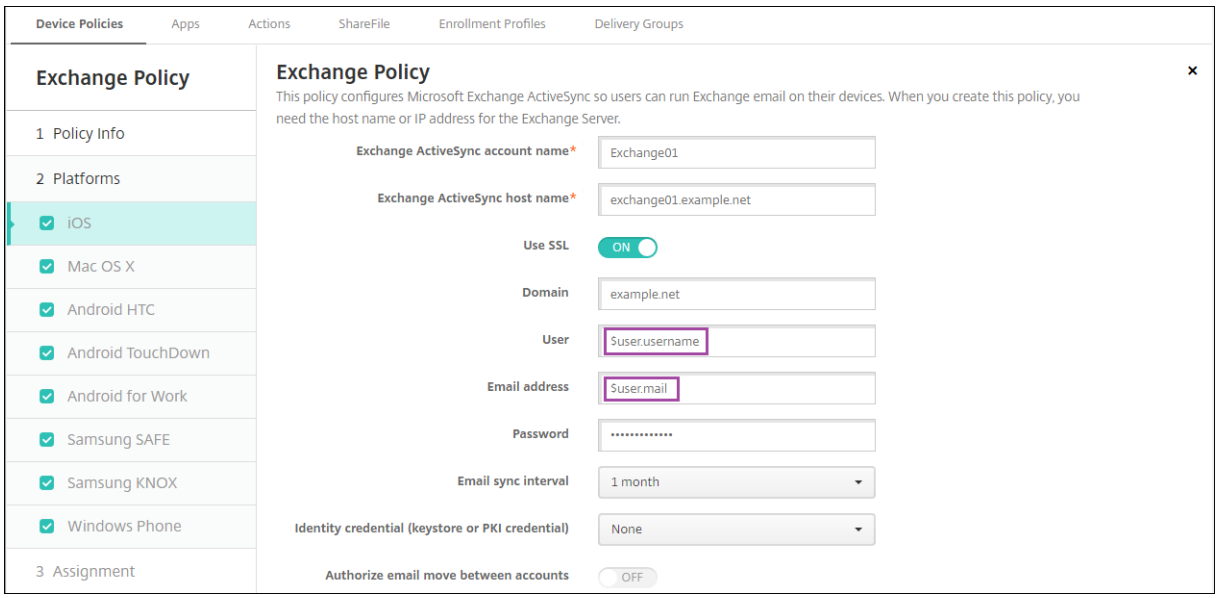
ドル記号（$）に続くすべての構文は中かっこ（{ }）で囲みます。

- 修飾されたプロパティ名は、ユーザープロパティ、デバイスプロパティ、またはカスタムプロパティを示します。
- 修飾されたプロパティ名は、プレフィックスと実際のプロパティ名で構成されます。
- ユーザープロパティの形式は次のとおりです。`${ user.[PROPERTYNAME] (prefix="user.")}`
- デバイスプロパティの形式は次のとおりです。`${ device.[PROPERTYNAME] (prefix="device.")}`
- プロパティ名の大文字と小文字は区別されます。
- 関数を定義するサードパーティの参照に対して、関数の一覧またはリンクを制限できます。通知メッセージのこのマクロには、関数`firstnotnull`が含まれます:

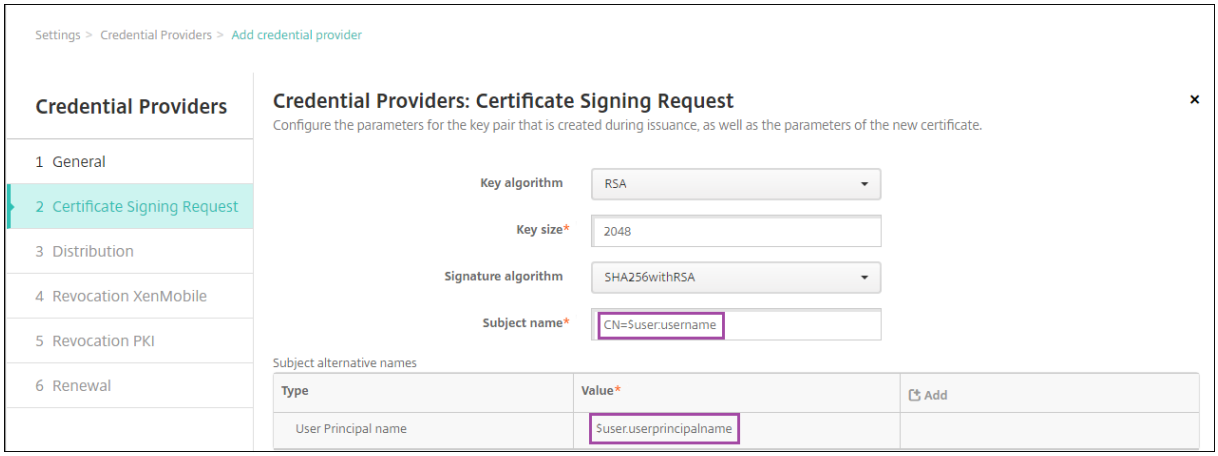
デバイス`${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`がブロックされました…

- カスタムマクロ（ユーザーが定義するプロパティ）の場合、プレフィックスは`${ custom }`です。プレフィックスは省略できます。

以下は、ポリシーのテキストフィールドにユーザー名の値を設定する、一般的なマクロ`${ user.username }`の例です。このマクロは、複数のユーザーが使用する Exchange ActiveSync プロファイルおよびそのほかのプロファイルを構成するのに便利です。次の例は、Exchange ポリシーでのマクロの使用方法を示しています。ユーザーのマクロは`${ user.username }`です。電子メールアドレス のマクロは`${ user.mail }`です。

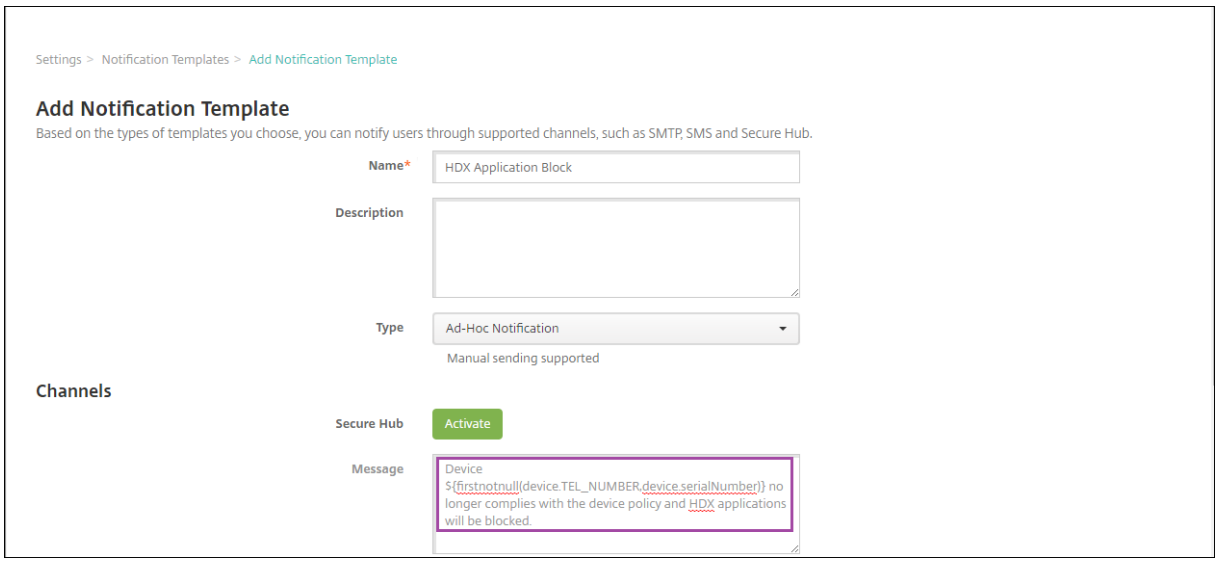


次の例は、証明書署名要求でのマクロの使用方法を示しています。サブジェクト名のマクロは **CN=$user.username** です。サブジェクトの別名の値のマクロは **$user.userprincipalname** です。



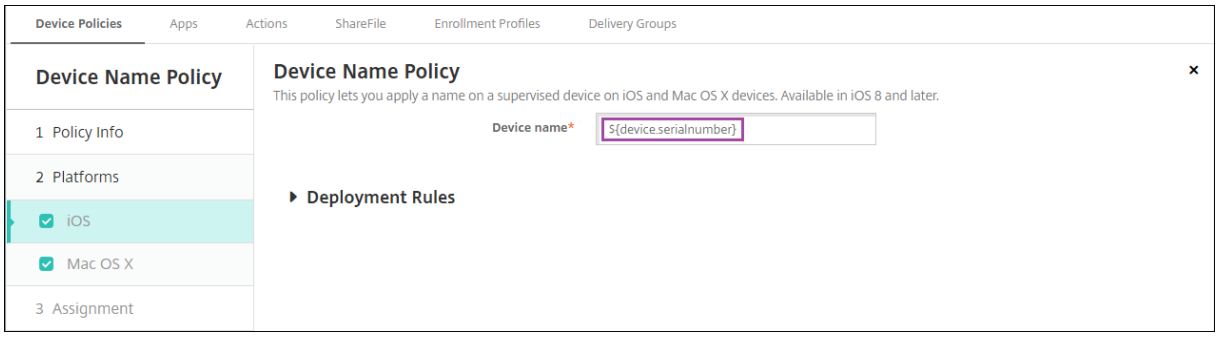
次の例は、通知テンプレートでのマクロの使用方法を示しています。このテンプレート例では、デバイスが非準拠のため HDX アプリケーションがブロックされた場合にユーザーに送信されるメッセージを定義します。[メッセージ] のマクロは次のとおりです。

デバイス`${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`がデバイスポリシーに準拠しなくなりましたので、HDX アプリケーションがブロックされます。



通知で使用されるマクロの例については、［設定］**>**［通知テンプレート］の順に移動し、事前定義されたテンプレートを選択して、［編集］をクリックします。

次の例は、デバイス名デバイスポリシーのマクロを示しています。マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。たとえば、デバイス名を各デバイスのシリアル番号に設定するには、`${ device.serialnumber }`を使用します。デバイス名にユーザー名を含めるには、`${ device.serialnumber } ${ user.username }`を使用します。デバイス名デバイスポリシーは、監視対象の iOS デバイスおよび macOS デバイスで機能します。



デフォルトの通知テンプレートのマクロ

デフォルトの通知テンプレートで次のマクロを使用できます。

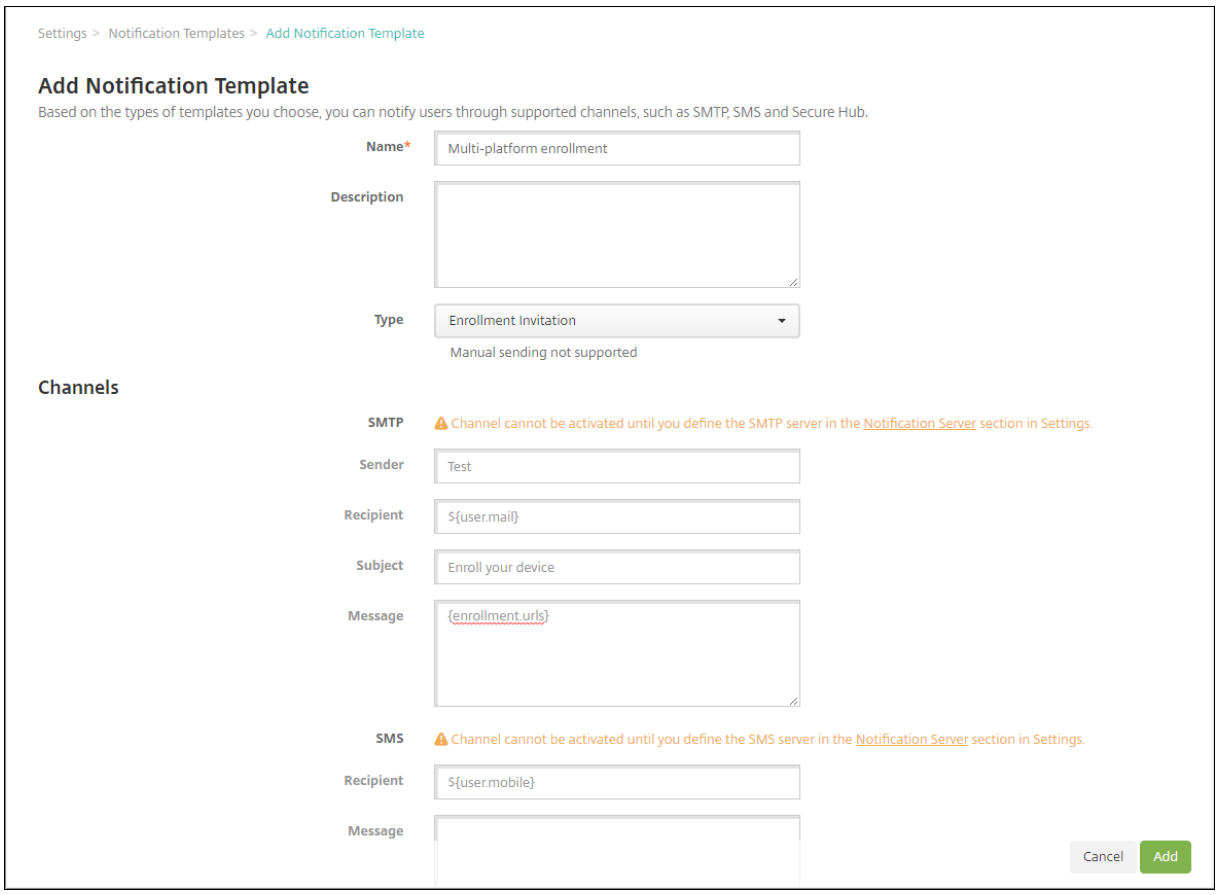
- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`

- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

> 注:
>
> Citrix Endpoint Management コンソールには、「ブラックリスト」、「ホワイトリスト」という用語が含まれています。これらの用語は、今後のリリースで「禁止リスト」、「許可リスト」に変更されます。

次の例は、複数のデバイスプラットフォームの登録用 URL を含む通知を作成する方法を示しています。[メッセージ] のマクロは次のとおりです。

${enrollment.urls}



次の例は、ユーザーに各自のデバイスプラットフォームに当てはまる登録用 URL をクリックすることを促す、通知メッセージを作成する方法を示しています。

例 1:

```
To enroll, click the link below that applies to your device platform:

${
 enrollment.ios.platform }
  - ${
 enrollment.ios.url }


${
 enrollment.macos.platform }
  - ${
 enrollment.macos.url }


${
 enrollment.android.platform }
  - ${
 enrollment.android.url }

```



```
<!--NeedCopy-->
```

例 2:

```
To enroll an iOS device, click the link ${
 enrollment.ios.url }
 .

To enroll a macOS device, click the link ${
 enrollment.macos.url }
 .

To enroll an Android device, click the link ${
 enrollment.android.url }
 .

<!--NeedCopy-->
```

特定のポリシーのマクロ

デバイス名デバイスポリシー（iOS と macOS 用）では、デバイス名に次のマクロを使用できます。デバイス名:

- ${ device.serialnumber }
- ${ user.username } @example.com
- ${ device.serialnumber }
- ${ device.serialnumber }
- ${ user.username }
- ${ enrollment.pin }
- ${ user.dnsroot }

モバイルデバイスポリシー（iOS の場合）では、非文字列フィールド（[プロキシサーバーポート] など）の値にマクロを使用できます。たとえば、${ device.xyz }や${ setting.xyz }などのマクロを使用して整数に展開できます。

[**iOS** および **macOS** プロファイルのインポート] デバイスポリシーで Citrix Endpoint Management にインポートするデバイス構成 XML ファイルでは、非文字列フィールドの値にマクロを使用できます。

Samsung MDM ライセンスキーのデバイスポリシーでは、**ELM** ライセンスキーに次のマクロを使用できます:

- ${ elm.license.key }

Web クリップデバイスポリシーの場合は、**URL** で次のマクロを使用できます:

- ${ webeas-url }

組み込みのデバイスプロパティを取得するためのマクロ

表示名	マクロ
デバイス ID	`$device.id`
デバイスの GUID	`$device.uniqueid`
デバイスの IMEI	`$device.imei`
OS ファミリ	`$device.OSFamily`
シリアル番号	`$device.serialNumber`

すべてのデバイスプロパティ向けのマクロ

表示名：アカウントを一時停止しますか?

- **Web** 要素：`GOOGLE_AW_DIRECTORY_SUSPENDED`
- マクロ：`${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

表示名：アクティベーションロックバイパスコード

- **Web** 要素：`ACTIVATION_LOCK_BYPASS_CODE`
- マクロ：`${ device.ACTIVATION_LOCK_BYPASS_CODE }`

表示名：アクティベーションロックが有効になっています

- **Web** 要素：`ACTIVATION_LOCK_ENABLED`
- マクロ：`${ device.ACTIVATION_LOCK_ENABLED }`

表示名：アクティブな Apple App Store アカウント

- **Web** 要素：`ACTIVE_ITUNES`
- マクロ：`${ device.ACTIVE_ITUNES }`

表示名：管理者が無効になっています

- **Web** 要素：`ADMIN_DISABLED`
- マクロ：`${ device.ADMIN_DISABLED }`

表示名： AIK は存在しますか?

- **Web** 要素：`WINDOWS_HAS_AIK_PRESENT`
- マクロ：`${ device.WINDOWS_HAS_AIK_PRESENT }`

表示名： Amazon MDM API 実行可能

- **Web** 要素: `AMAZON_MDM`
- マクロ: `${ device.AMAZON_MDM }`

表示名: Android Enterprise デバイス ID

- **Web** 要素: `GOOGLE_AW_DEVICE_ID`
- マクロ: `${ device.GOOGLE_AW_DEVICE_ID }`

表示名: Android Enterprise 対応デバイスですか?

- **Web** 要素: `GOOGLE_AW_ENABLED_DEVICE`
- マクロ: `${ device.GOOGLE_AW_ENABLED_DEVICE }`

表示名: Android Enterprise インストールの種類

- **Web** 要素: `GOOGLE_AW_INSTALL_TYPE`
- マクロ: `${ device.GOOGLE_AW_INSTALL_TYPE }`

表示名: スパイウェア対策の署名の状態

- **Web** 要素: `ANTI_SPYWARE_SIGNATURE_STATUS`
- マクロ: `${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

表示名: スパイウェア対策の状態

- **Web** 要素: `ANTI_SPYWARE_STATUS`
- マクロ: `${ device.ANTI_SPYWARE_STATUS }`

表示名: ウイルス対策の署名の状態

- **Web** 要素: `ANTI_VIRUS_SIGNATURE_STATUS`
- マクロ: `${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

表示名: ウイルス対策の状態

- **Web** 要素: `ANTI_VIRUS_STATUS`
- マクロ: `${ device.ANTI_VIRUS_STATUS }`

表示名: ASM Deployment Program アクティベーションロックバイパスコード

- **Web** 要素: `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- マクロ: `${ device.DEP_ACTIVATION_LOCK_BYPASS_CODE }`

表示名: ASM Deployment Program エスクローキー

- **Web** 要素: `DEP_ESCROW_KEY`
- マクロ: `${ device.DEP_ESCROW_KEY }`

表示名: アセットタグ

- **Web** 要素: `ASSET_TAG`
- マクロ: `${ device.ASSET_TAG }`

表示名: ソフトウェアの更新を自動確認

- **Web** 要素: `AutoCheckEnabled`
- マクロ: `${ device.AutoCheckEnabled }`

表示名: ソフトウェアの更新をバックグラウンドで自動ダウンロード

- **Web** 要素: `BackgroundDownloadEnabled`
- マクロ: `${ device.BackgroundDownloadEnabled }`

表示名: アプリの更新プログラムを自動的にインストールする

- **Web** 要素: `AutomaticAppInstallationEnabled`
- マクロ: `${ device.AutomaticAppInstallationEnabled }`

表示名: OS アップデートを自動的にインストールする

- **Web** 要素: `AutomaticOSInstallationEnabled`
- マクロ: `${ device.AutomaticOSInstallationEnabled }`

表示名: セキュリティの更新を自動インストール

- **Web** 要素: `AutomaticSecurityUpdatesEnabled`
- マクロ: `${ device.AutomaticSecurityUpdatesEnabled }`

表示名: 自動更新ステータス

- **Web** 要素: `AUTOUPDATE_STATUS`
- マクロ: `${ device.AUTOUPDATE_STATUS }`

表示名: 使用できる RAM

- **Web** 要素: `MEMORY_AVAILABLE`
- マクロ: `${ device.MEMORY_AVAILABLE }`

表示名: 使用可能なソフトウェアの更新

- **Web** 要素: AVAILABLE_OS_UPDATE_HUMAN_READABLE
- マクロ: ${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }

表示名: 使用できるストレージ領域

- **Web** 要素: FREEDISK
- マクロ: ${ device.FREEDISK }

表示名: バックアップバッテリー

- **Web** 要素: BACKUP_BATTERY_PERCENT
- マクロ: ${ device.BACKUP_BATTERY_PERCENT }

表示名: ベースバンドファームウェアのバージョン

- **Web** 要素: MODEM_FIRMWARE_VERSION
- マクロ: '${device.MODEM_FIRMWARE_VERSION}

表示名: バッテリー充電

- **Web** 要素: BATTERY_CHARGING_STATUS
- マクロ: ${ device.BATTERY_CHARGING_STATUS }

表示名: バッテリー充電

- **Web** 要素: BATTERY_CHARGING
- マクロ: ${ device.BATTERY_CHARGING }

表示名: バッテリー残量

- **Web** 要素: BATTERY_ESTIMATED_CHARGE_REMAINING
- マクロ: ${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }

表示名: バッテリー駆動中

- **Web** 要素: BATTERY_RUNTIME
- マクロ: ${ device.BATTERY_RUNTIME }

表示名: バッテリー状態

- **Web** 要素: BATTERY_STATUS
- マクロ: ${ device.BATTERY_STATUS }

表示名: BES PIN

- **Web** 要素: `BES_PIN`
- マクロ: `${ device.BES_PIN }`

表示名: BES サーバーエージェント ID

- **Web** 要素: `AGENT_ID`
- マクロ: `${ device.AGENT_ID }`

表示名: BES サーバー名

- **Web** 要素: `BES_SERVER`
- マクロ: `${ device.BES_SERVER }`

表示名: BES サーバーのバージョン

- **Web** 要素: `BES_VERSION`
- マクロ: `${ device.BES_VERSION }`

表示名: BIOS 情報

- **Web** 要素: `BIOS_INFO`
- マクロ: `${ device.BIOS_INFO }`

表示名: BitLocker の状態

- **Web** 要素: `WINDOWS_HAS_BIT_LOCKER_STATUS`
- マクロ: `${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

表示名: Bluetooth MAC アドレス

- **Web** 要素: `BLUETOOTH_MAC`
- マクロ: `${ device.BLUETOOTH_MAC }`

表示名: ブートデバッグは有効ですか?

- **Web** 要素: `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

表示名: ブートマネージャーのバージョン

- **Web** 要素: `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- マクロ: `${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

表示名: キャリアコード

- **Web** 要素: `CARRIER_CODE`
- マクロ: `${ device.CARRIER_CODE }`

表示名: キャリア設定バージョン

- **Web** 要素: `CARRIER_SETTINGS_VERSION`
- マクロ: `${ device.CARRIER_SETTINGS_VERSION }`

表示名: カタログの URL

- **Web** 要素: `CatalogURL`
- マクロ: `${ device.CatalogURL }`

表示名: 携帯ネットワークの高度

- **Web** 要素: `GPS_ALTITUDE_FROM_CELLULAR`
- マクロ: `${ device.GPS_ALTITUDE_FROM_CELLULAR }`

表示名: 携帯ネットワークのコース

- **Web** 要素: `GPS_COURSE_FROM_CELLULAR`
- マクロ: `${ device.GPS_COURSE_FROM_CELLULAR }`

表示名: 携帯ネットワークの水平精度

- **Web** 要素: `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- マクロ: `${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }`

表示名: 携帯ネットワーク緯度

- **Web** 要素: `GPS_LATITUDE_FROM_CELLULAR`
- マクロ: `${ device.GPS_LATITUDE_FROM_CELLULAR }`

表示名: 携帯ネットワーク経度

- **Web** 要素: `GPS_LONGITUDE_FROM_CELLULAR`
- マクロ: `${ device.GPS_LONGITUDE_FROM_CELLULAR }`

表示名: 携帯ネットワークの速度

- **Web** 要素: `GPS_SPEED_FROM_CELLULAR`
- マクロ: `${ device.GPS_SPEED_FROM_CELLULAR }`

表示名: 携帯ネットワークテクノロジ

- **Web** 要素: `CELLULAR_TECHNOLOGY`
- マクロ: `${ device.CELLULAR_TECHNOLOGY }`

表示名: 携帯ネットワークタイムスタンプ

- **Web** 要素: `GPS_TIMESTAMP_FROM_CELLULAR`
- マクロ: `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

表示名: 携帯ネットワークの垂直精度

- **Web** 要素: `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- マクロ: `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

表示名: 次回のログイン時にパスワードを変更しますか?

- **Web** 要素: `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- マクロ: ‘${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

表示名: クライアントデバイス ID

- **Web** 要素: `CLIENT_DEVICE_ID`
- マクロ: `${ device.CLIENT_DEVICE_ID }`

表示名: クラウドバックアップが有効になりました

- **Web** 要素: `CLOUD_BACKUP_ENABLED`
- マクロ: `${ device.CLOUD_BACKUP_ENABLED }`

表示名: コードの整合性は有効ですか?

- **Web** 要素: `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

表示名: コード整合性のバージョン

- **Web** 要素: `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- マクロ: `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

表示名: 色

- **Web** 要素: `COLOR`
- マクロ: `${ device.COLOR }`

表示名: CPU クロック速度

- **Web** 要素: `CPU_CLOCK_SPEED`
- マクロ: `${ device.CPU_CLOCK_SPEED }`

表示名: CPU の種類

- **Web** 要素: `CPU_TYPE`
- マクロ: `${ device.CPU_TYPE }`

表示名: 作成時刻

- **Web** 要素: `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }`

表示名: 重要なソフトウェアの更新

- **Web** 要素: `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- マクロ: `${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }`

表示名: 現在の通信事業者ネットワーク

- **Web** 要素: `CARRIER`
- マクロ: `${ device.CARRIER }`

表示名: 現在のモバイル国コード

- **Web** 要素: `CURRENT_MCC`
- マクロ: `${ device.CURRENT_MCC }`

表示名: 現在のモバイルネットワークコード

- **Web** 要素: `CURRENT_MNC`
- マクロ: `${ device.CURRENT_MNC }`

表示名: データローミングが許可されました

- **Web** 要素: `DATA_ROAMING_ENABLED`
- マクロ: `${ device.DATA_ROAMING_ENABLED }`

表示名: 最新の iCloud バックアップ日

- **Web** 要素: `LAST_CLOUD_BACKUP_DATE`
- マクロ: `${ device.LAST_CLOUD_BACKUP_DATE }`

表示名: デフォルトカタログ

- **Web** 要素: `IsDefaultCatalog`
- マクロ: `${ device.IsDefaultCatalog }`

表示名: Apple Deployment Program アカウント名

- **Web** 要素: `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- マクロ: `${ device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME }`

表示名: Apple Deployment Program ポリシー

- **Web** 要素: `WINDOWS_HAS_DEP_POLICY`
- マクロ: `${ device.WINDOWS_HAS_DEP_POLICY }`

表示名: 割り当てられた Apple Deployment Program プロファイル

- **Web** 要素: `PROFILE_ASSIGN_TIME`
- マクロ: `${ device.PROFILE_ASSIGN_TIME }`

表示名: プッシュされた Apple Deployment Program プロファイル

- **Web** 要素: `PROFILE_PUSH_TIME`
- マクロ: `${ device.PROFILE_PUSH_TIME }`

表示名: 削除された Apple Deployment Program プロファイル

- **Web** 要素: `PROFILE_REMOVE_TIME`
- マクロ: `${ device.PROFILE_REMOVE_TIME }`

表示名: Apple Deployment Program 登録者

- **Web** 要素: `DEVICE_ASSIGNED_BY`
- マクロ: `${ device.DEVICE_ASSIGNED_BY }`

表示名: Apple Deployment Program 登録日

- **Web** 要素: `DEVICE_ASSIGNED_DATE`
- マクロ: `${ device.DEVICE_ASSIGNED_DATE }`

表示名: 説明

- **Web** 要素: `DESCRIPTION`
- マクロ: `${ device.DESCRIPTION }`

表示名: デバイスのモデル

- **Web** 要素: `SYSTEM_OEM`
- マクロ: `${ device.SYSTEM_OEM }`

表示名: デバイス名

- **Web** 要素: `DEVICE_NAME`
- マクロ: `${ device.DEVICE_NAME }`

表示名: デバイスの種類

- **Web** 要素: `DEVICE_TYPE`
- マクロ: `${ device.DEVICE_TYPE }`

表示名: ボイスメールへ自動転送がアクティブになりました

- **Web** 要素: `DO_NOT_DISTURB`
- マクロ: `${ device.DO_NOT_DISTURB }`

表示名: ELAM ドライバーは読み込まれていますか?

- **Web** 要素: `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- マクロ: `${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }`

表示名: 暗号化のコンプライアンス

- **Web** 要素: `ENCRYPTION_COMPLIANCE`
- マクロ: `${ device.ENCRYPTION_COMPLIANCE }`

表示名: ENROLLMENT_KEY_GENERATION_DATE

- **Web** 要素: `ENROLLMENT_KEY_GENERATION_DATE`
- マクロ: `${ device.ENROLLMENT_KEY_GENERATION_DATE }`

表示名: エンタープライズ ID

- **Web** 要素: `ENTERPRISEID`
- マクロ: `${ device.ENTERPRISEID }`

表示名: 外部ストレージ 1: 使用可能領域

- **Web** 要素: `EXTERNAL_STORAGE1_FREE_SPACE`
- マクロ: `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

表示名: 外部ストレージ 1: 使用可能領域

- **Web** 要素: `EXTERNAL_STORAGE1_FREE_SPACE`
- マクロ: `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

表示名: 外部ストレージ 1: 名前

- **Web** 要素: `EXTERNAL_STORAGE1_NAME`
- マクロ: `${ device.EXTERNAL_STORAGE1_NAME }`

表示名: 外部ストレージ 1: 総領域

- **Web** 要素: `EXTERNAL_STORAGE1_TOTAL_SPACE`
- マクロ: `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

表示名: 外部ストレージ 2: 使用可能領域

- **Web** 要素: `EXTERNAL_STORAGE2_FREE_SPACE`
- マクロ: `${ device.EXTERNAL_STORAGE2_FREE_SPACE }`

表示名: 外部ストレージ 2: 名前

- **Web** 要素: `EXTERNAL_STORAGE2_NAME`
- マクロ: `${ device.EXTERNAL_STORAGE2_NAME }`

表示名: 外部ストレージ 2: 総領域

- **Web** 要素: `EXTERNAL_STORAGE2_TOTAL_SPACE`
- マクロ: `${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }`

表示名: 外部ストレージが暗号化されました

- **Web** 要素: `EXTERNAL_ENCRYPTION`
- マクロ: `${ device.EXTERNAL_ENCRYPTION }`

表示名: FileVault が有効です

- **Web** 要素: `IS_FILEVAULT_ENABLED`
- マクロ: `${ device.IS_FILEVAULT_ENABLED }`

表示名: ファイアウォールの状態

- **Web** 要素: `DEVICE_FIREWALL_STATUS`
- マクロ: `${ device.DEVICE_FIREWALL_STATUS }`

表示名: ファイアウォールの状態

- **Web** 要素: `DEVICE_FIREWALL_STATUS`
- マクロ: `${ device.DEVICE_FIREWALL_STATUS }`

表示名: ファイアウォールの状態

- **Web** 要素: `FIREWALL_STATUS`
- マクロ: `${ device.FIREWALL_STATUS }`

表示名: ファームウェアのバージョン

- **Web** 要素: `FIRMWARE_VERSION`
- マクロ: `${ device.FIRMWARE_VERSION }`

表示名: 最初の同期

- **Web** 要素: `ZMSP_FIRST_SYNC`
- マクロ: `${ device.ZMSP_FIRST_SYNC }`

表示名: Google ディレクトリのエイリアス

- **Web** 要素: `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

表示名: Google ディレクトリのファミリ名

- **Web** 要素: `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

表示名: Google ディレクトリ名

- **Web** 要素: `GOOGLE_AW_DIRECTORY_NAME`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_NAME }`

表示名: Google ディレクトリのプライマリメール

- **Web** 要素: `GOOGLE_AW_DIRECTORY_PRIMARY`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

表示名: Google ディレクトリユーザー ID

- **Web** 要素: `GOOGLE_AW_DIRECTORY_USER_ID`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

表示名: GPS 高度

- **Web** 要素: `GPS_ALTITUDE_FROM_GPS`
- マクロ: `${ device.GPS_ALTITUDE_FROM_GPS }`

表示名: GPS のコース

- **Web** 要素: `GPS_COURSE_FROM_GPS`
- マクロ: `${ device.GPS_COURSE_FROM_GPS }`

表示名: GPS の水平精度

- **Web** 要素: `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- マクロ: `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

表示名: GPS 緯度

- **Web** 要素: `GPS_LATITUDE_FROM_GPS`
- マクロ: `${ device.GPS_LATITUDE_FROM_GPS }`

表示名**:** GPS 経度

- **Web** 要素: `GPS_LONGITUDE_FROM_GPS`
- マクロ: `${ device.GPS_LONGITUDE_FROM_GPS }`

表示名: GPS の速度

- **Web** 要素: `GPS_SPEED_FROM_GPS`
- マクロ: `${ device.GPS_SPEED_FROM_GPS }`

表示名: GPS タイムスタンプ

- **Web** 要素: `GPS_TIMESTAMP_FROM_GPS`
- マクロ: `${ device.GPS_TIMESTAMP_FROM_GPS }`

表示名: GPS の垂直精度

- **Web** 要素: `GPS_VERTICAL_ACCURACY_FROM_GPS`
- マクロ: `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

表示名: ハードウェアデバイス ID

- **Web** 要素: `HW_DEVICE_ID`
- マクロ: `${ device.HW_DEVICE_ID }`

表示名: ハードウェア暗号化機能

- **Web** 要素: `HARDWARE_ENCRYPTION_CAPS`
- マクロ: `${ device.HARDWARE_ENCRYPTION_CAPS }`

表示名: HAS_CONTAINER

- **Web** 要素: `HAS_CONTAINER`
- マクロ: `${ device.HAS_CONTAINER }`

表示名: 現在ログオンしている Apple App Store アカウントのハッシュ

- **Web** 要素: `ITUNES_STORE_ACCOUNT_HASH`
- マクロ: `${ device.ITUNES_STORE_ACCOUNT_HASH }`

表示名: ホームキャリアネットワーク

- **Web** 要素: `SIM_CARRIER_NETWORK`
- マクロ: `${ device.SIM_CARRIER_NETWORK }`

表示名: ホームモバイル国コード

- **Web** 要素: `SIM_MCC`
- マクロ: `${ device.SIM_MCC }`

表示名: ホームモバイルネットワークコード

- **Web** 要素: `SIM_MNC`
- マクロ: `${ device.SIM_MNC }`

表示名: ICCID

- **Web** 要素: `ICCID`
- マクロ: `${ device.ICCID }`

表示名: ID

- **Web** 要素: `AS_DEVICE_IDENTITY`
- マクロ: `${ device.AS_DEVICE_IDENTITY }`

表示名: IMEI/MEID 番号

- **Web** 要素: `IMEI`
- マクロ: `${ device.IMEI }`

表示名: IMSI

- **Web** 要素: `SIM_ID`
- マクロ: `${ device.SIM_ID }`

表示名: 内部ストレージが暗号化されました

- **Web** 要素: `LOCAL_ENCRYPTION`
- マクロ: `${ device.LOCAL_ENCRYPTION }`

表示名: IP の場所

- **Web** 要素: `IP_LOCATION`
- マクロ: `${ device.IP_LOCATION }`

表示名: IPv4 アドレス

- **Web** 要素: `IP_ADDRESSV4`
- マクロ: `${ device.IP_ADDRESSV4 }`

表示名: IPv6 アドレス

- **Web** 要素: `IP_ADDRESSV6`
- マクロ: `${ device.IP_ADDRESSV6 }`

表示名: 発行時刻

- **Web** 要素: `WINDOWS_HAS_ISSUED_AT`
- マクロ: `${ device.WINDOWS_HAS_ISSUED_AT }`

表示名: ジェイルブレイク済み/Root 化済み

- **Web** 要素: `ROOT_ACCESS`
- マクロ: `${ device.ROOT_ACCESS }`

表示名: カーネルデバッグは有効ですか?

- **Web** 要素: `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

表示名: キオスクモード

- **Web** 要素: `IS_KIOSK`
- マクロ: `${ device.IS_KIOSK }`

表示名: 前回認知した IP アドレス

- **Web** 要素: `LAST_IP_ADDR`
- マクロ: `${ device.LAST_IP_ADDR }`

表示名: 前回のポリシー更新時間

- **Web** 要素: `LAST_POLICY_UPDATE_TIME`
- マクロ: `${ device.LAST_POLICY_UPDATE_TIME }`

表示名: 前回のスキャン日

- **Web** 要素: `PreviousScanDate`
- マクロ: `${ device.PreviousScanDate }`

表示名: 前回のスキャン結果

- **Web** 要素: `PreviousScanResult`
- マクロ: `${ device.PreviousScanResult }`

表示名: 前回スケジュールされたソフトウェアの更新

- **Web** 要素: `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- マクロ: `${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }`

表示名: 前回スケジュールされたソフトウェアの更新の失敗メッセージ

- **Web** 要素: `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- マクロ: `${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }`

表示名: 前回スケジュールされたソフトウェアの更新の状態

- **Web** 要素: `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- マクロ: `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

表示名: 前回の同期

- **Web** 要素: `ZMSP_LAST_SYNC`
- マクロ: `${ device.ZMSP_LAST_SYNC }`

表示名: ロケーターサービスが有効になっています

- **Web** 要素: `DEVICE_LOCATOR`
- マクロ: `${ device.DEVICE_LOCATOR }`

表示名: MAC アドレス

- **Web** 要素: `MAC_ADDRESS`
- マクロ: `${ device.MAC_ADDRESS }`

表示名: MAC アドレスネットワーク接続

- **Web** 要素: `MAC_NETWORK_CONNECTION`
- マクロ: `${ device.MAC_NETWORK_CONNECTION }`

表示名: MAC アドレスの種類

- **Web** 要素: `MAC_ADDRESS_TYPE`
- マクロ: `${ device.MAC_ADDRESS_TYPE }`

表示名: メールボックスセットアップ

- **Web** 要素: `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

表示名: メインバッテリー

- **Web** 要素: `MAIN_BATTERY_PERCENT`
- マクロ: `${ device.MAIN_BATTERY_PERCENT }`

表示名: MDM の紛失モードが有効になっています

- **Web** 要素: `IS_MDM_LOST_MODE_ENABLED`
- マクロ: `${ device.IS_MDM_LOST_MODE_ENABLED }`

表示名: MDX_SHARED_ENCRYPTION_KEY

- **Web** 要素: `MDX_SHARED_ENCRYPTION_KEY`
- マクロ: `${ device.MDX_SHARED_ENCRYPTION_KEY }`

表示名: MEID

- **Web** 要素: `MEID`
- マクロ: `${ device.MEID }`

表示名: 携帯電話番号

- **Web** 要素: `TEL_NUMBER`
- マクロ: `${ device.TEL_NUMBER }`

表示名: モデル ID

- **Web** 要素: `MODEL_ID`
- マクロ: `${ device.MODEL_ID }`

表示名: モデル番号

- **Web** 要素: `MODEL_NUMBER`
- マクロ: `${ device.MODEL_NUMBER }`

表示名: ネットワークアダプターの種類

- **Web** 要素: `NETWORK_ADAPTER_TYPE`
- マクロ: `${ device.NETWORK_ADAPTER_TYPE }`

表示名: オペレーティングシステムビルド

- **Web** 要素: `SYSTEM_OS_BUILD`
- マクロ: `${ device.SYSTEM_OS_BUILD }`

表示名: オペレーティングシステムのエディション

- **Web** 要素: `OS_EDITION`
- マクロ: `${ device.OS_EDITION }`

表示名: オペレーティングシステム言語（ロケール）

- **Web** 要素: `SYSTEM_LANGUAGE`
- マクロ: `${ device.SYSTEM_LANGUAGE }`

表示名: オペレーティングシステムバージョン

- **Web** 要素: `SYSTEM_OS_VERSION`
- マクロ: `${ device.SYSTEM_OS_VERSION }`

表示名: 組織の住所

- **Web** 要素: `ORGANIZATION_ADDRESS`
- マクロ: `${ device.ORGANIZATION_ADDRESS }`

表示名: 組織のメール

- **Web** 要素: `ORGANIZATION_EMAIL`
- マクロ: `${ device.ORGANIZATION_EMAIL }`

表示名: 組織のマジック

- **Web** 要素: `ORGANIZATION_MAGIC`
- マクロ: `${ device.ORGANIZATION_MAGIC }`

表示名: 組織名

- **Web** 要素: `ORGANIZATION_NAME`
- マクロ: `${ device.ORGANIZATION_NAME }`

表示名: 組織の電話番号

- **Web** 要素: `ORGANIZATION_PHONE`
- マクロ: `${ device.ORGANIZATION_PHONE }`

表示名: コンプライアンス違反

- **Web** 要素: `OUT_OF_COMPLIANCE`
- マクロ: `${ device.OUT_OF_COMPLIANCE }`

表示名: 所有者

- **Web** 要素: `CORPORATE_OWNED`
- マクロ: `${ device.CORPORATE_OWNED }`

表示名: パスコード準拠

- **Web** 要素: `PASSCODE_IS_COMPLIANT`
- マクロ: `${ device.PASSCODE_IS_COMPLIANT }`

表示名: 構成に準拠したパスコード

- **Web** 要素: `PASSCODE_IS_COMPLIANT_WITH_CFG`
- マクロ: `${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }`

表示名: 現在のパスコード

- **Web** 要素: `PASSCODE_PRESENT`
- マクロ: `${ device.PASSCODE_PRESENT }`

表示名: PCR0

- **Web** 要素: `WINDOWS_HAS_PCR0`
- マクロ: `${ device.WINDOWS_HAS_PCR0 }`

表示名: 境界違反

- **Web** 要素: `GPS_PERIMETER_BREACH`
- マクロ: `${ device.GPS_PERIMETER_BREACH }`

表示名: 定期的な確認

- **Web** 要素: `PerformPeriodicCheck`
- マクロ: `${ device.PerformPeriodicCheck }`

表示名: パーソナルホットスポットがアクティブになりました

- **Web** 要素: `PERSONAL_HOTSPOT_ENABLED`
- マクロ: `${ device.PERSONAL_HOTSPOT_ENABLED }`

表示名: ジオフェンスの PIN コード

- **Web** 要素: `PIN_CODE_FOR_GEO_FENCE`
- マクロ: `${ device.PIN_CODE_FOR_GEO_FENCE }`

表示名: プラットフォーム

- **Web** 要素: `SYSTEM_PLATFORM`
- マクロ: `${ device.SYSTEM_PLATFORM }`

表示名: プラットフォーム API レベル

- **Web** 要素: `API_LEVEL`
- マクロ: `${ device.API_LEVEL }`

表示名: ポリシー名

- **Web** 要素: `POLICY_NAME`
- マクロ: `${ device.POLICY_NAME }`

表示名: プライマリ電話番号

- **Web** 要素: `IDENTITY1_PHONENUMBER`
- マクロ: `${ device.IDENTITY1_PHONENUMBER }`

表示名: プライマリ SIM の通信事業者

- **Web** 要素: `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- マクロ: `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

表示名: プライマリ SIM ICCID

- **Web** 要素: `IDENTITY1_ICCID`
- マクロ: `${ device.IDENTITY1_ICCID }`

表示名: プライマリ SIM IMEI

- **Web** 要素: `IDENTITY1_IMEI`
- マクロ: `${ device.IDENTITY1_IMEI }`

表示名: プライマリ SIM IMSI

- **Web** 要素: `IDENTITY1_IMSI`
- マクロ: `${ device.IDENTITY1_IMSI }`

表示名: プライマリ SIM ローミング

- **Web** 要素: `IDENTITY1_ROAMING`
- マクロ: `${ device.IDENTITY1_ROAMING }`

表示名: プライマリ SIM ローミング

- **Web** 要素: `IDENTITY1_ROAMING_COMPLIANCE`
- マクロ: `${ device.IDENTITY1_ROAMING_COMPLIANCE }`

表示名: 製品名

- **Web** 要素: `PRODUCT_NAME`
- マクロ: `${ device.PRODUCT_NAME }`

表示名: 発行元デバイス ID

- **Web** 要素: `PUBLISHER_DEVICE_ID`
- マクロ: `${ device.PUBLISHER_DEVICE_ID }`

表示名: リセット回数

- **Web** 要素: `WINDOWS_HAS_RESET_COUNT`
- マクロ: `${ device.WINDOWS_HAS_RESET_COUNT }`

表示名: 再起動の回数

- **Web** 要素: `WINDOWS_HAS_RESTART_COUNT`
- マクロ: `${ device.WINDOWS_HAS_RESTART_COUNT }`

表示名: セーフモードは有効になっていますか?

- **Web** 要素: `WINDOWS_HAS_SAFE_MODE`
- マクロ: `${ device.WINDOWS_HAS_SAFE_MODE }`

表示名: SBCP ハッシュ

- **Web** 要素: `WINDOWS_HAS_SBCP_HASH`
- マクロ: `${ device.WINDOWS_HAS_SBCP_HASH }`

表示名: 画面: 高さ

- **Web** 要素: `SCREEN_HEIGHT`
- マクロ: `${ device.SCREEN_HEIGHT }`

表示名: 画面: 色数

- **Web** 要素: `SCREEN_NB_COLORS`
- マクロ: `${ device.SCREEN_NB_COLORS }`

表示名: 画面: サイズ

- **Web** 要素: `SCREEN_SIZE`
- マクロ: `${ device.SCREEN_SIZE }`

表示名: 画面: 幅

- **Web** 要素: `SCREEN_WIDTH`
- マクロ: `${ device.SCREEN_WIDTH }`

表示名: 画面: X 軸解像度

- **Web** 要素: `SCREEN_XDPI`
- マクロ: `${ device.SCREEN_XDPI }`

表示名: 画面: Y 軸解像度

- **Web** 要素: `SCREEN_YDPI`
- マクロ: `${ device.SCREEN_YDPI }`

表示名: セカンダリ電話番号

- **Web** 要素: `IDENTITY2_PHONENUMBER`
- マクロ: `${ device.IDENTITY2_PHONENUMBER }`

表示名: セカンダリ SIM の通信事業者

- **Web** 要素: `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- マクロ: `${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }`

表示名: セカンダリ SIM ICCID

- **Web** 要素: `IDENTITY2_ICCID`
- マクロ: `${ device.IDENTITY2_ICCID }`

表示名: セカンダリ SIM IMEI

- **Web** 要素: `IDENTITY2_IMEI`
- マクロ: `${ device.IDENTITY2_IMEI }`

表示名: セカンダリ SIM IMSI

- **Web** 要素: `IDENTITY2_IMSI`
- マクロ: `${ device.IDENTITY2_IMSI }`

表示名: セカンダリ SIM ローミング

- **Web** 要素: `IDENTITY2_ROAMING`
- マクロ: `${ device.IDENTITY2_ROAMING }`

表示名: セカンダリ SIM ローミングのコンプライアンス

- **Web** 要素: `IDENTITY2_ROAMING_COMPLIANCE`
- マクロ: `${ device.IDENTITY2_ROAMING_COMPLIANCE }`

表示名: セキュアブートは有効ですか?

- **Web** 要素: `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

表示名: セキュアブートの状態

- **Web** 要素: `SECURE_BOOT_STATE`
- マクロ: `${ device.SECURE_BOOT_STATE }`

表示名: SecureContainer 有効

- **Web** 要素: `DLP_ACTIVE`
- マクロ: `${ device.DLP_ACTIVE }`

表示名: セキュリティパッチレベル

- **Web** 要素: `SYSTEM_SECURITY_PATCH_LEVEL`
- マクロ: `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

表示名: シリアル番号

- **Web** 要素: `SERIAL_NUMBER`
- マクロ: `${ device.SERIAL_NUMBER }`

表示名: SMS 可

- **Web** 要素: `IS_SMS_CAPABLE`
- マクロ: `${ device.IS_SMS_CAPABLE }`

表示名: 監視

- **Web** 要素: `SUPERVISED`
- マクロ: `${ device.SUPERVISED }`

表示名: 一時停止理由

- **Web** 要素: `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

表示名: 改ざん状態

- **Web** 要素: `TAMPERED_STATUS`
- マクロ: `${ device.TAMPERED_STATUS }`

表示名: 使用条件

- **Web** 要素: `TERMS_AND_CONDITIONS`
- マクロ: `${ device.TERMS_AND_CONDITIONS }`

表示名: 条件および契約を承認しますか?

- **Web** 要素: `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- マクロ: `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

表示名: テスト署名は有効になっていますか?

- **Web** 要素: `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

表示名: RAM 合計

- **Web** 要素: `MEMORY`
- マクロ: `${ device.MEMORY }`

表示名: 総ストレージ領域

- **Web** 要素: `TOTAL_DISK_SPACE`
- マクロ: `${ device.TOTAL_DISK_SPACE }`

表示名: TPM バージョン

- **Web** 要素: `TPM_VERSION`
- マクロ: `${ device.TPM_VERSION }`

表示名: UDID

- **Web** 要素: `UDID`
- マクロ: `${ device.UDID }`

表示名: ユーザーアカウント制御の状態

- **Web** 要素: `UAC_STATUS`
- マクロ: `${ device.UAC_STATUS }`

表示名: ユーザーエージェント

- **Web** 要素: `USER_AGENT`
- マクロ: `${ device.USER_AGENT }`

表示名: ユーザー定義 #1

- **Web** 要素: `USER_DEFINED_1`
- マクロ: `${ device.USER_DEFINED_1 }`

表示名: ユーザー定義 #2

- **Web** 要素: `USER_DEFINED_2`
- マクロ: `${ device.USER_DEFINED_2 }`

表示名: ユーザー定義 #3

- **Web** 要素: `USER_DEFINED_3`
- マクロ: `${ device.USER_DEFINED_3 }`

表示名: ユーザー言語（ロケール）

- **Web** 要素: `USER_LANGUAGE`
- マクロ: `${ device.USER_LANGUAGE }`

表示名: ベンダー

- **Web** 要素: `VENDOR`
- マクロ: `${ device.VENDOR }`

表示名: 音声可

- **Web** 要素: `IS_VOICE_CAPABLE`
- マクロ: `${ device.IS_VOICE_CAPABLE }`

表示名: 音声ローミングが許可されました

- **Web** 要素: `VOICE_ROAMING_ENABLED`
- マクロ: `${ device.VOICE_ROAMING_ENABLED }`

表示名: VSM は有効になっていますか?

- **Web** 要素: `WINDOWS_HAS_VSM_ENABLED`
- マクロ: `${ device.WINDOWS_HAS_VSM_ENABLED }`

表示名: Wi-Fi MAC アドレス

- **Web** 要素: `WIFI_MAC`
- マクロ: `${ device.WIFI_MAC }`

表示名: WINDOWS_ENROLLMENT_KEY

- **Web** 要素: `WINDOWS_ENROLLMENT_KEY`
- マクロ: `${ device.WINDOWS_ENROLLMENT_KEY }`

表示名: WinPE は有効になっていますか?

- **Web** 要素: `WINDOWS_HAS_WINPE`
- マクロ: `${ device.WINDOWS_HAS_WINPE }`

表示名: WNS 通知の状態

- **Web** 要素: `PROPERTY_WNS_PUSH_STATUS`
- マクロ: `${ device.PROPERTY_WNS_PUSH_STATUS }`

表示名: WNS 通知 URL

- **Web** 要素: `PROPERTY_WNS_PUSH_URL`
- マクロ: `${ device.PROPERTY_WNS_PUSH_URL }`

表示名: WNS 通知 URL 有効期限

- **Web** 要素: `PROPERTY_WNS_PUSH_URL_EXPIRY`
- マクロ: `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

表示名: Citrix Endpoint Management エージェント ID

- **Web** 要素: `ENROLLMENT_AGENT_ID`
- マクロ: {device.ENROLLMENT_AGENT_ID}‘

表示名: Citrix Endpoint Management エージェントリビジョン

- **Web** 要素: `EW_REVISION`
- マクロ: `${ device.EW_REVISION }`

表示名: Citrix Endpoint Management エージェントバージョン

- **Web** 要素: `EW_VERSION`
- マクロ: `${ device.EW_VERSION }`

表示名: Zebra API 実行可能

- **Web** 要素: `ZEBRA_MDM`
- マクロ: `${ device.ZEBRA_MDM }`

表示名: Zebra MXMF バージョン

- **Web** 要素: `ZEBRA_MDM_VERSION`
- マクロ: `${ device.ZEBRA_MDM_VERSION }`

表示名: Zebra Patch バージョン

- **Web** 要素: `ZEBRA_PATCH_VERSION`
- マクロ: `${ device.ZEBRA_PATCH_VERSION }`

組み込みのデバイスプロパティを取得するためのマクロ

表示名	マクロ
domainname（ドメイン名、デフォルトドメイン）	${ user.domainname }
loginname（ユーザー名とドメイン名）	${ user.loginname }
username（ログイン名からドメイン名を除去したもの（ある場合））	${ user.username }

すべてのデバイスプロパティ向けのマクロ

表示名	**Web** 要素	マクロ
Active Directory へのサインインに失敗しました	badpwdcount	${ user.badpwdcount }
ActiveSync ユーザーメール	asuseremail	${ user.asuseremail }
ASM のデータソース	asmpersonsource	${ user.asmpersonsource }
ASM Deployment Program のアカウント名	asmdepaccount	${ user.asmdepaccount }
ASM の管理対象 Apple ID	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
ASM のパスコードの種類	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM の個人 ID	asmpersonid	${ user.asmpersonid }
ASM の個人の状態	asmpersonstatus	${ user.asmpersonstatus }
ASM の個人の役職	asmpersontitle	${ user.asmpersontitle }
ASM の一意の個人 ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM のソースシステム ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }

表示名	**Web** 要素	マクロ
ASM の生徒の学年	asmpersongrade	${ user.asmpersongrade }
BES ユーザーメール	besuseremail	${ user.besuseremail }
会社	company	${ user.company }
会社名	companyname	${ user.companyname }
国	c	${ user.c }
部署	department	${ user.department }
説明	description	${ user.description }
無効なユーザー	disableduser	${ user.disableduser }
表示名	displayname	${ user.displayname }
識別名	distinguishedname	${ user.distinguishedname }
ドメイン名	domainname	${ user.domainname }
メール	mail	${ user.mail }
名	givenname	${ user.givenname }
自宅の住所	homestreetaddress	${ user.homestreetaddress }
自宅の市区町村	homecity	${ user.homecity }
自宅の国	homecountry	${ user.homecountry }
自宅のファックス	homefax	${ user.homefax }
自宅の電話	homephone	${ user.homephone }
自宅の都道府県	homestate	${ user.homestate }
自宅の郵便番号	homezip	${ user.homezip }
IP 電話	ipphone	${ user.ipphone }
ミドルネーム、イニシャル	middleinitial	${ user.middleinitial }
ミドルネーム	middlename	${ user.middlename }
モバイル	mobile	${ user.mobile }

表示名	**Web** 要素	マクロ
名前	cn	${ user.cn }
会社の住所	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
会社の市区町村	l	${ user.l }
会社のファックス番号	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
会社の都道府県	st	${ user.st }
会社の番地	officestreetaddress	${ user.officestreetaddress }
会社の電話番号	telephonenumber	${ user.telephonenumber }
会社の郵便番号	postalcode	${ user.postalcode }
私書箱	postofficebox	${ user.postofficebox }
ポケベル	pager	${ user.pager }
プライマリグループ ID	primarygroupid	${ user.primarygroupid }
SAM アカウント	samaccountname	${ user.samaccountname }
番地	streetaddress	${ user.streetaddress }
姓	sn	${ user.sn }
タイトル	title	${ user.title }
ユーザーログオン名	userprincipalname	${ user.userprincipalname }

自動化された操作

March 15, 2024

Citrix Endpoint Management で自動化された操作を作成し、次に対する反応をプログラムします:

- イベント
- ユーザーまたはデバイスのプロパティ
- ユーザーデバイス上のアプリの存在

自動化された操作を作成する場合は、操作に対して定義したトリガーによって、ユーザーのデバイスが Citrix Endpoint Management に接続したときにそのデバイス上で何が起きるかが決まります。イベントがトリガーされたときに、より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信できます。

自動的に発生する効果は、次の範囲から設定します:

- デバイスに選択的ワイプまたは完全なワイプを実行する。
- デバイスをコンプライアンス違反に設定する。
- デバイスを取り消す。
- より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信する。

MAM のみモードでのアプリロックとアプリワイプ操作を構成できます。

自動化された操作により、Azure Active Directory（AD）に参加している Windows 10 および Windows 11 デバイスを、Azure AD でコンプライアンス違反としてマークできます。

> 注:
>
> ユーザーに通知するには、Citrix Endpoint Management がメッセージを送信できるように、Citrix Endpoint Management の設定で通知サーバー（SMTP）を構成している必要があります。詳しくは、「通知」を参照してください。また、続行する前に使用予定の通知テンプレートを設定します。詳しくは、「通知」を参照してください。「通知テンプレートの作成および更新」を参照してください。

操作の例

自動化された操作の使用例を次に示します:

例 1

- 以前に禁止したアプリ（例:「Words with Friends」）を検出するとします。「Words with Friends」アプリが検出された場合に、ユーザーデバイスをコンプライアンス違反に設定するトリガーを指定できます。この操作では次に、そのアプリを削除して、デバイスが再度コンプライアンス遵守状態に戻す必要があることがユーザーに通知されます。ユーザーが遵守するのを待つ時間を設定することもできます。その期限が過ぎると、デバイスの選択的なワイプなどの定義された操作が実行されます。

例 2

- 顧客が最新のファームウェアを使用しているかどうかを確認し、ユーザーがデバイスを更新する必要がある場合はリソースへのアクセスを禁止するとします。ユーザーのデバイスに最新バージョンがない場合に、ユーザーデバイスをコンプライアンス違反に設定するトリガーを指定できます。自動化された操作を使用して、リソースを禁止して、顧客に通知します。

例 3

- ユーザーデバイスがコンプライアンス違反状態になり、ユーザーがそのデバイスを修正します。ポリシーを構成して、デバイスをコンプライアンス準拠状態へとリセットするパッケージを展開できます。

例 4

- 一定期間非アクティブであったユーザーデバイスをコンプライアンス違反としてマークするとします。次のように、非アクティブなデバイスの自動化された操作を作成できます:

  1. Citrix Endpoint Management コンソールで、［設定］**>**［ネットワークアクセス制御］をクリックし、［非アクティブデバイス］を選択します。［非アクティブデバイス］設定について詳しくは、「ネットワークアクセス制御」を参照してください。
  2. 「操作の追加と管理」で概説されている手順に従って、操作を追加します。唯一の違いは、［操作の詳細］ページで次のように設定を構成することです:
     - トリガー。［デバイスプロパティ］、［コンプライアンス違反］、［真］を選択します。
     - 操作。［通知を送信］を選択し、［設定］の ［通知テンプレート］を使用して、作成したテンプレートを選択します。次に、操作を実行するまでの遅延を日、時間、または分単位で設定します。ユーザーがトリガーの問題に対処するまで、操作が繰り返される間隔を設定します。

  > ヒント:
  >
  > 非アクティブデバイスを一括で削除するには、Citrix Endpoint Management Public REST APIを使用します。まず、削除する非アクティブなデバイスのデバイス ID を手動で取得してから、この削除 API を実行してそれらを一括で削除します。

操作の追加と管理

自動化された操作を追加、編集、フィルタリングするには:

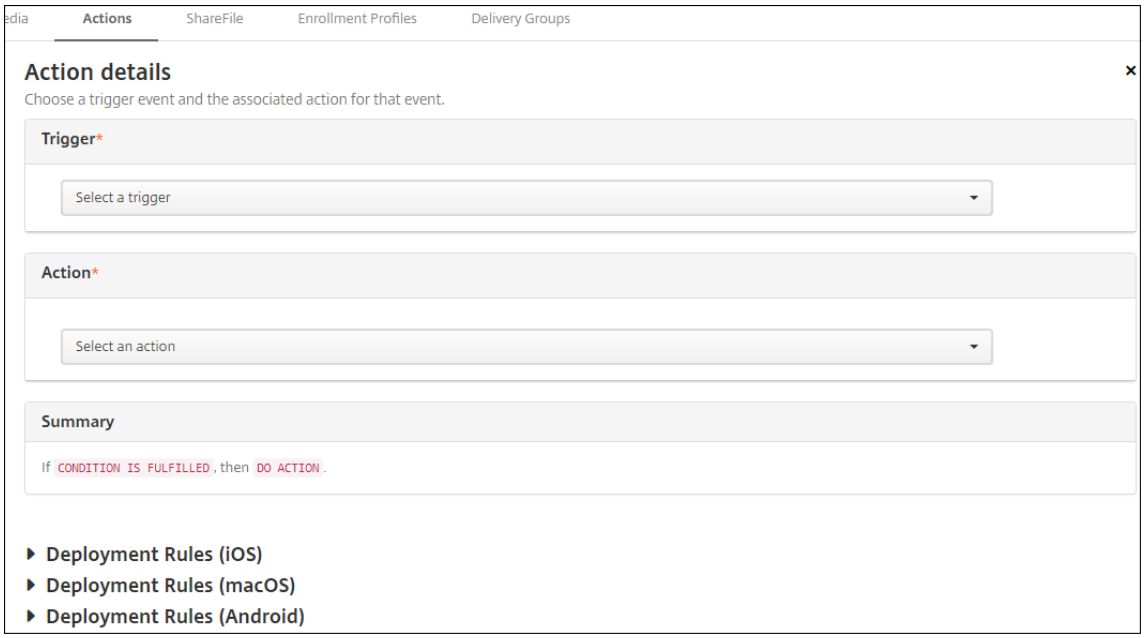
1. Citrix Endpoint Management コンソールで、［構成］**>**［アクション］の順にクリックします。［操作］ページが開きます。
2. ［アクション］ページで、次のいずれかを行います:
   - ［追加］をクリックして操作を追加します。
   - 編集または削除する既存の操作を選択します。使用するオプションをクリックします。

3. ［アクション情報］ページが開きます。
4. ［アクション情報］ページで、次の情報を入力または変更します：

   - 名前：操作を識別する名前を入力します。このフィールドは必須です。
   - 説明：操作の意図する内容を説明します。

5. ［次へ］をクリックします。［アクションの詳細］ページが開きます。

   次の例はイベントトリガーの設定方法を示しています。別のトリガーを選択した場合、この図で示されているものとは異なるオプションになります。



6. ［アクションの詳細］ページで、次の情報を入力または変更します：

   ［トリガー］一覧で、この操作に対するイベントトリガーの種類をクリックします。次のいずれかのトリガーを選択します：

   - イベント：デバイスのステータスが選択した非準拠イベントと一致するかどうかを確認して、それに対応します。
   - デバイスプロパティ： MDM 管理のデバイスのデバイス属性が特定の値か確認して、それに対応します。詳しくは、「デバイスのプロパティ名と値」（PDF）を参照してください。
   - ユーザープロパティ：ユーザー属性（通常、Active Directory からの属性）の特定の値に対応します。
   - インストールされているアプリ名：インストール中のアプリに対応します。MAM のみモードには適用されません。デバイスでアプリインベントリポリシーを有効にする必要があります。デフォルトでは、アプリインベントリポリシーはすべてのプラットフォームで有効です。詳しくは、「アプリインベントリデバイスポリシー」を参照してください。
   - ポリシーの戻り値： PowerShell スクリプトからの戻り値が特定の論理条件を満たしているかを確認します。Windows エージェントポリシーを有効にして、構成済みにする必要があります。Windows エ

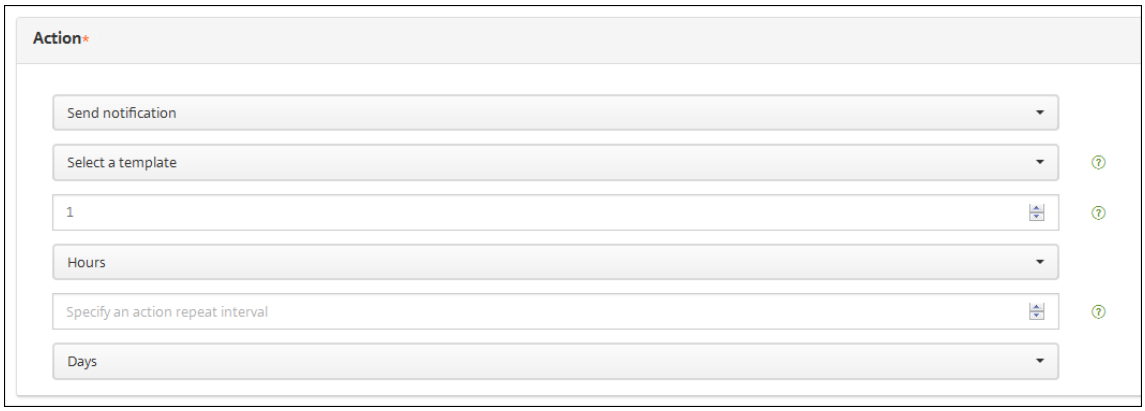
ージェントポリシーについて詳しくは、「Windows エージェントのデバイスポリシー」を参照してください。

7. 次の一覧で、トリガーに対する応答をクリックします。
8. ［アクション］の一覧で、トリガーの条件が満たされたときに実行される操作をクリックします。［通知を送信］アクション以外では、トリガーの原因となった問題をユーザーが解決できる期間を選択します。その期間内に問題が解決されない場合は、選択した操作が実行されます。操作の定義については、「セキュリティ操作」を参照してください。

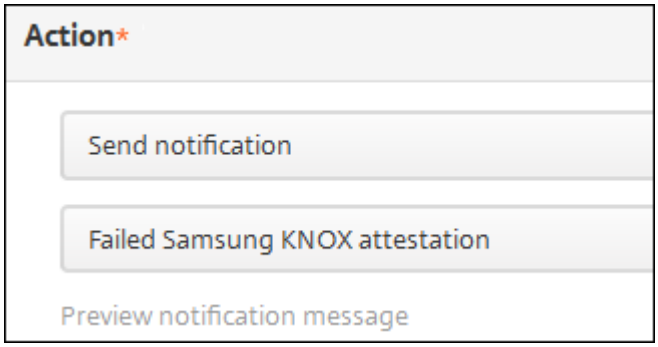
   ［通知を送信］を選択した場合は、次の手順を実行して通知を送信します。

9. 次の一覧で、通知に使用するテンプレートを選択します。選択したイベントに関連する通知テンプレートが表示されます。通知の種類のテンプレートがない場合、テンプレートの構成を促す次のメッセージが表示されます：このイベントの種類用のテンプレートはありません。［設定］の通知テンプレートを使用してテンプレートを作成します。

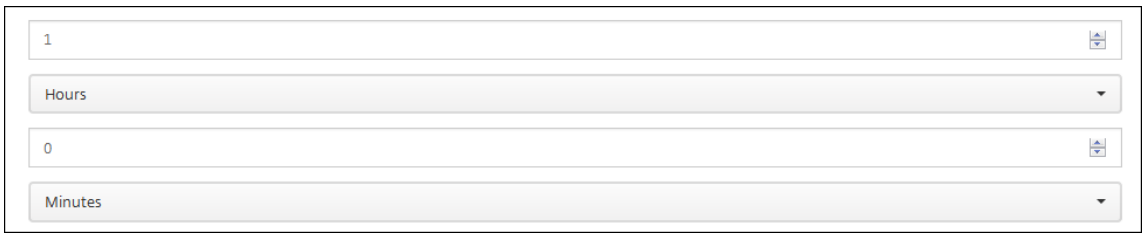
   ユーザーに通知するには、［設定］**>**［通知サーバー］を使用して SMTP の設定を構成し、Citrix Endpoint Management がメッセージを送信できるようにします。「通知」を参照してください。また、続行する前に、［設定］**>**［通知テンプレート］を使用して、使用予定の通知テンプレートを設定します。「通知テンプレートの作成および更新」を参照してください。



   テンプレートを選択した後、［通知メッセージのプレビュー］をクリックします。



10. 次のフィールドでは、操作を実行するまでの遅延を日、時間、または分単位で設定します。ユーザーがトリガーの問題に対処するまで、操作が繰り返される間隔を設定します。



11. ［概要］で、意図したとおりに、自動化された操作を作成したことを確認します。

12. 操作の詳細を構成したら、プラットフォームごとに個別に展開規則を構成できます。これを行うには、選択した各プラットフォームに対して、手順 13 を実行します。
13. 展開規則を構成します展開規則の構成に関する一般情報については、「リソースの展開」を参照してください。

    この例の場合：

    - デバイスの所有権は **BYOD** でなければなりません。
    - デバイスはパスコードに準拠している必要があります。
    - デバイスのモバイル国コードを Andorra のみにすることはできません。

14. 操作のプラットフォームの展開規則の構成が完了したら、［次へ］をクリックします。アクション割り当てのページが開きます。ここで操作をデリバリーグループに割り当てます。この手順はオプションです。
15. ［デリバリーグループを選択］の横にデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。
16. ［展開スケジュール］を展開して以下の設定を構成します：

    - ［展開］の横の ［オン］をクリックすると展開がスケジュールされ、［オフ］をクリックすると展開が行われません。デフォルトのオプションは、［オン］です。［オフ］を選択した場合、そのほかのオプションは必要はありません。
    - ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。デフォルトのオプションは、［**Now**］に設定されています。
    - ［あとで］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    - ［展開状態］の横の ［接続するたび］をクリックするか、［以前の展開が失敗した場合のみ］をクリックします。デフォルトのオプションは、［**On every connection**］です。
    - ［常時接続に対する展開］の横の ［オン］または ［オフ］をクリックします。デフォルトのオプションは、［オフ］です。

このオプションは、［設定］**>**［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

> 注:
>
> このオプションは、［設定］**>**［サーバープロパティ］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。
>
> 常時接続オプション:
>
> - iOS デバイスでは使用できません。
> - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 以降のバージョンで始めた顧客は、使用できません
> - Android および Android Enterprise 上で Citrix Endpoint Management の使用をバージョン 10.18.19 より前のバージョンで始めた顧客には、お勧めしません。
>
> 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし、［常時接続に対する展開］は適用されません。

17. ［次へ］をクリックします。［概要］ページが開きます。ここで操作の構成を確認できます。
18. ［保存］をクリックして変更を保存します。

MAM のみモードでのアプリロックとアプリワイプ操作

Citrix Endpoint Management コンソールに一覧表示されたトリガーの 4 種類のカテゴリすべてについて、デバイスでアプリをワイプまたはロックできます: トリガーの種類は、「イベント」、「デバイスプロパティ」、「ユーザープロパティ」、「インストール済みアプリ名」です。

自動でアプリのワイプまたはロックを構成するには

1. Citrix Endpoint Management コンソールで、［構成］**>**［アクション］の順にクリックします。
2. ［アクション］ページで、［追加］をクリックします。
3. ［アクション情報］ページで、アクションの名前および任意で説明を入力します。
4. ［アクションの詳細］ページで、目的のトリガーを選択します。
5. ［アクション］でアクションを選択します。

   この段階で、以下の条件に注意してください:

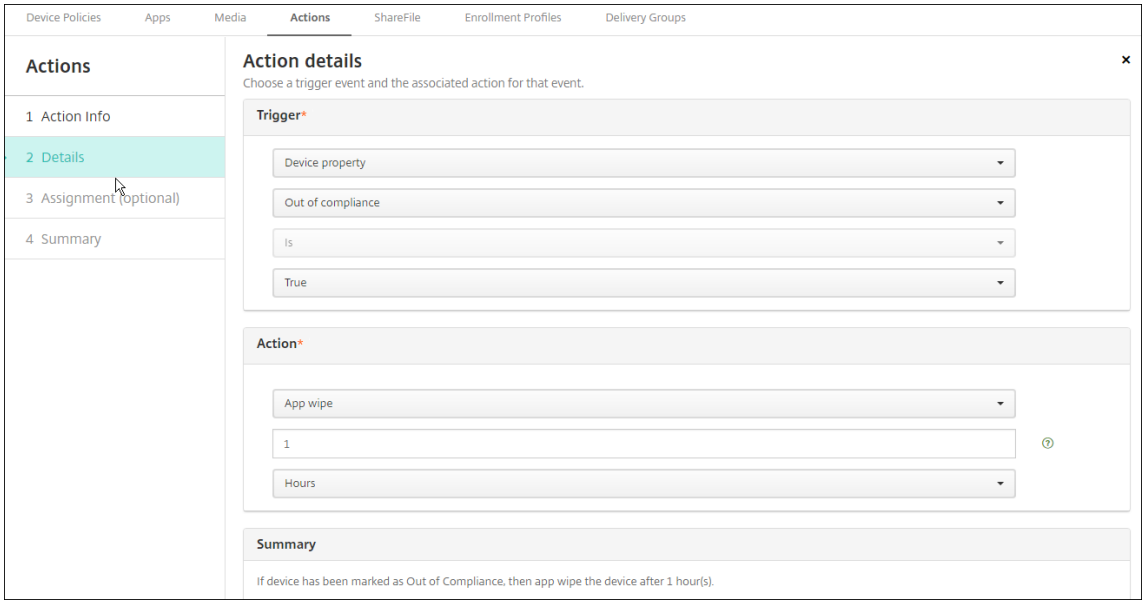
   トリガーの種類が ［イベント］で値が ［**Active Directory** 無効ユーザー］ではない場合、［アプリのワイプ］および ［アプリのロック］アクションは表示されません。

   トリガーの種類が ［デバイスプロパティ］で値が ［**MDM** の紛失モードが有効になっています］である場合、次のアクションは表示されません:

- デバイスを選択的にワイプ
- デバイスを完全にワイプ
- デバイスを取り消す

各オプションでは、自動で 1 時間の遅延が設定されていますが、遅延の期間は分単位、時間単位、日数単位を選択できます。遅延の目的は、アクションが発生する前に問題を修正する時間をユーザーに与えることです。［アプリのワイプ］および［アプリのロック］アクションの詳細については、「セキュリティ操作」を参照してください。

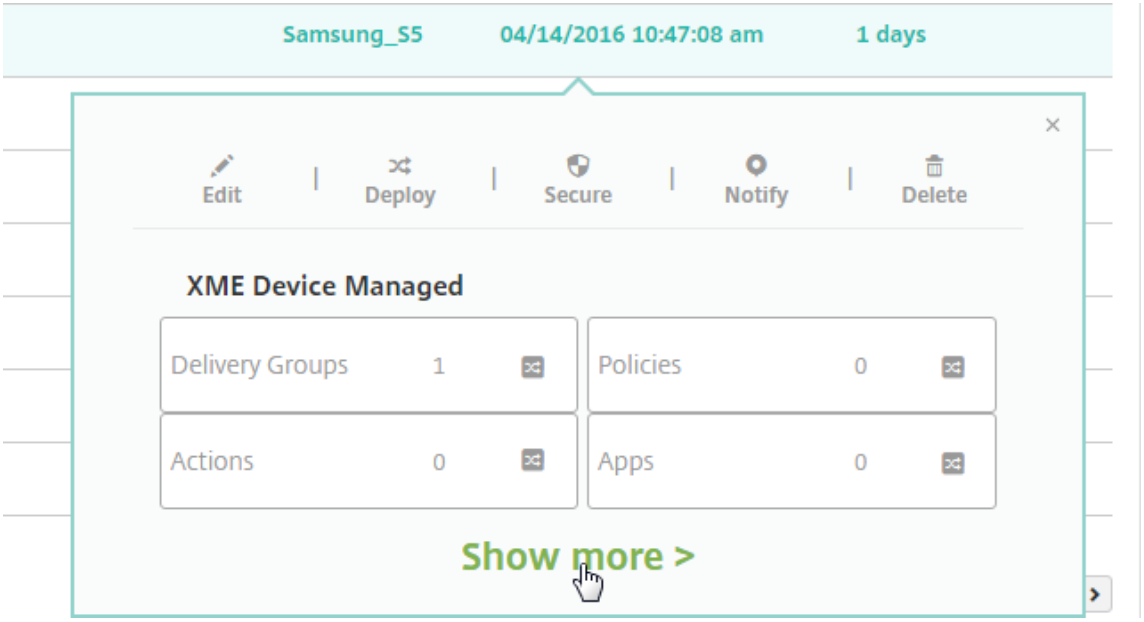
> 注:
>
> トリガーを ［イベント］に設定すると、繰り返し間隔は自動的に最小 1 時間となります。通知を生成するには、デバイスはポリシーの更新を実行して、サーバーと同期する必要があります。通常、ユーザーのサインオン時、または Citrix Secure Hub でポリシーを手動で更新すると、デバイスはサーバーと同期します。
>
> Active Directory データベースと Citrix Endpoint Management との同期を許可するアクションが実行される前に、さらに約 1 時間、遅延を追加できます。



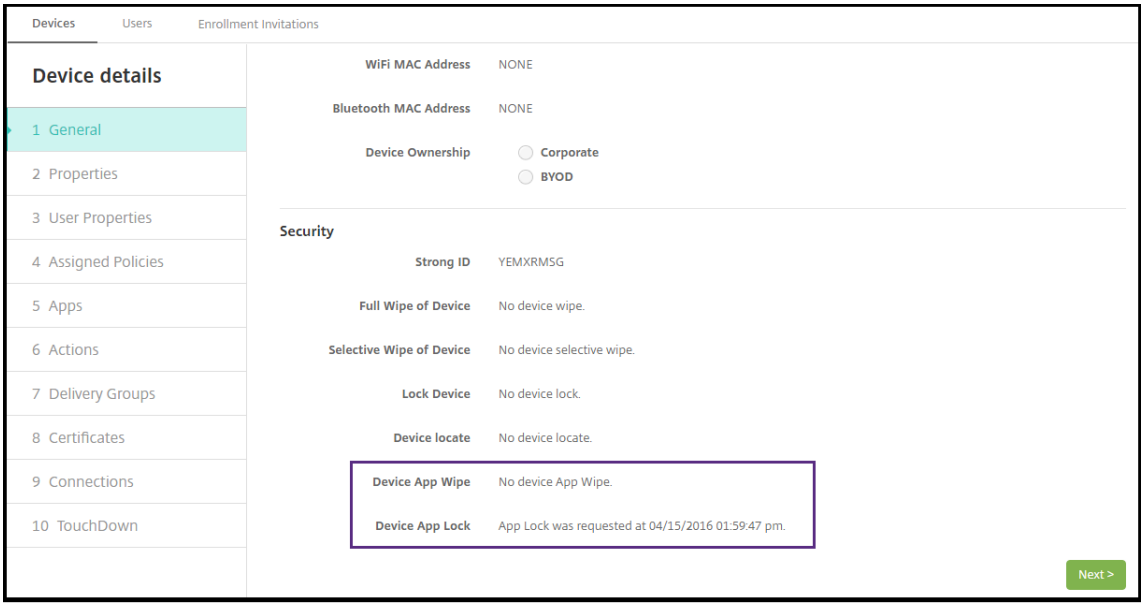
6. 展開規則を構成して、［次へ］をクリックします。
7. デリバリーグループの割り当てと展開スケジュールを構成して、［次へ］をクリックします。
8. ［保存］をクリックします。

アプリロックとアプリワイプの状態を確認するには

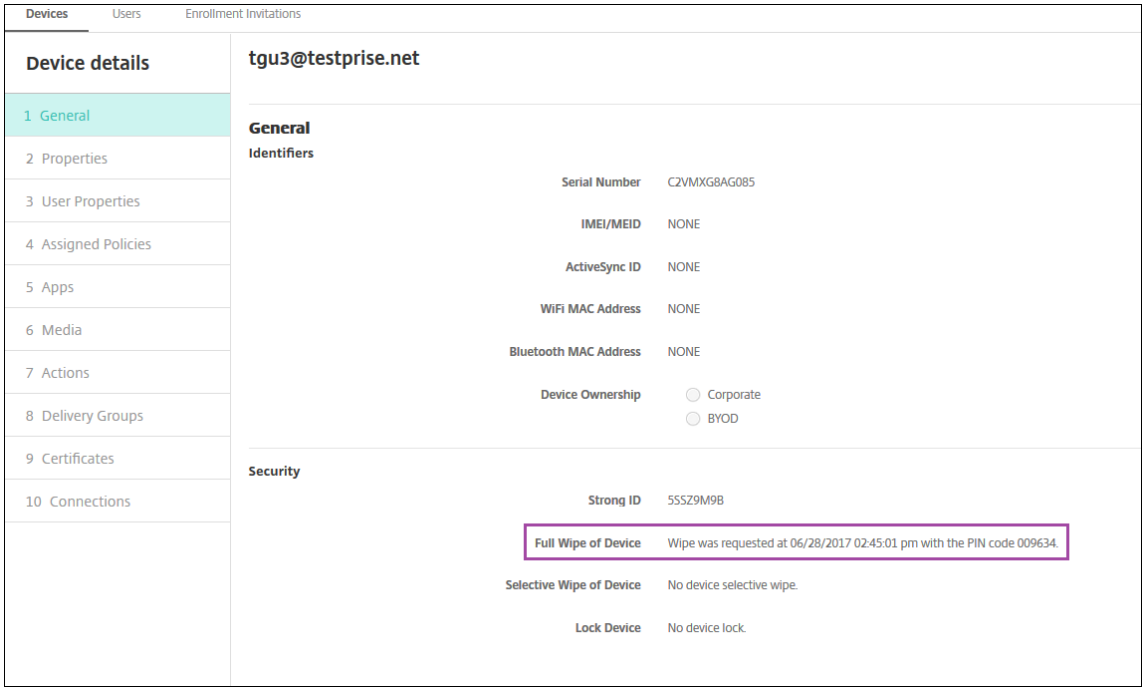
1. ［管理］**>** ［デバイス］に移動し、デバイスをクリックしてから ［詳細表示］をクリックします。



2. ［デバイスのアプリのワイプ］および ［デバイスのアプリのロック］までスクロールします。



デバイスがワイプされると、PIN コードの入力を要求するメッセージがユーザーに表示されます。ユーザーがコードを忘れた場合は、［デバイス詳細］で確認できます。



Azure AD で **Windows 10** および **Windows 11** デバイスをコンプライアンス違反としてマーキング

Azure AD に参加している Windows 10 および Windows 11 デバイスが、Citrix Endpoint Management によってコンプライアンス違反としてマークされている場合は、Azure AD でコンプライアンス違反のマークを付けることもできます。この機能を有効にするには、Azure AD ポータルの Microsoft Graph API にアクセスする権限をオンプレミス MDM アプリケーションに追加します。

1. Azure AD 管理者の資格情報で Azure AD ポータルにログインします。
2. Azure AD ポータルで［**Azure Active Directory**］**>** ［**Mobility**（**MDM and MAM**）］に移動します。［**On-premises MDM application**］を選択します。
3. ［**On-premises Application Settings**］**>** ［**Required Permissions**］**>** ［**Add**］**>** ［**Select an API**］**>** ［**Microsoft Graph**］をクリックします。［**Select**］をクリックして保存します。
4. ［**Required permissions**］で ［**Microsoft Graph**］を選択します。［**Enable Access**］で ［**Read and write directory data**］を選択します。
5. ［**Required permissions**］で ［**Microsoft Graph**］を選択します。次に ［**Grant permissions**］をクリックします。
6. ［**Yes**］をクリックして権限を付与します。

Windows 10 および Windows 11 を起動している Azure AD 登録済みデバイスがコンプライアンス違反としてマークされると、Citrix Endpoint Management はそのデバイスを Azure AD でもコンプライアンス違反としてマークします。

Windows エージェントのデバイスポリシーを使用した自動化された操作の作成

Windows エージェントのデバイスポリシーを使用して、管理された Windows デスクトップおよびタブレットでレジストリ値を監視するスクリプトを展開します。スクリプトの戻り値を基にして、自動化された操作を構成して実行できます。

1. Windows エージェントのデバイスポリシーを構成し、スクリプトの戻り値を確認します。Windows エージェントのデバイスポリシーについて詳しくは、「Windows エージェントのデバイスポリシー」を参照してください。

   上記の記事とこのセクションには`EntApp_2019_checkFirewall`というスクリプトのサンプルが含まれています。関連する Windows エージェントのデバイスポリシーで`cName_checkFirewall`という名前の構成を定義します。この構成は、サンプルスクリプトを実行します。

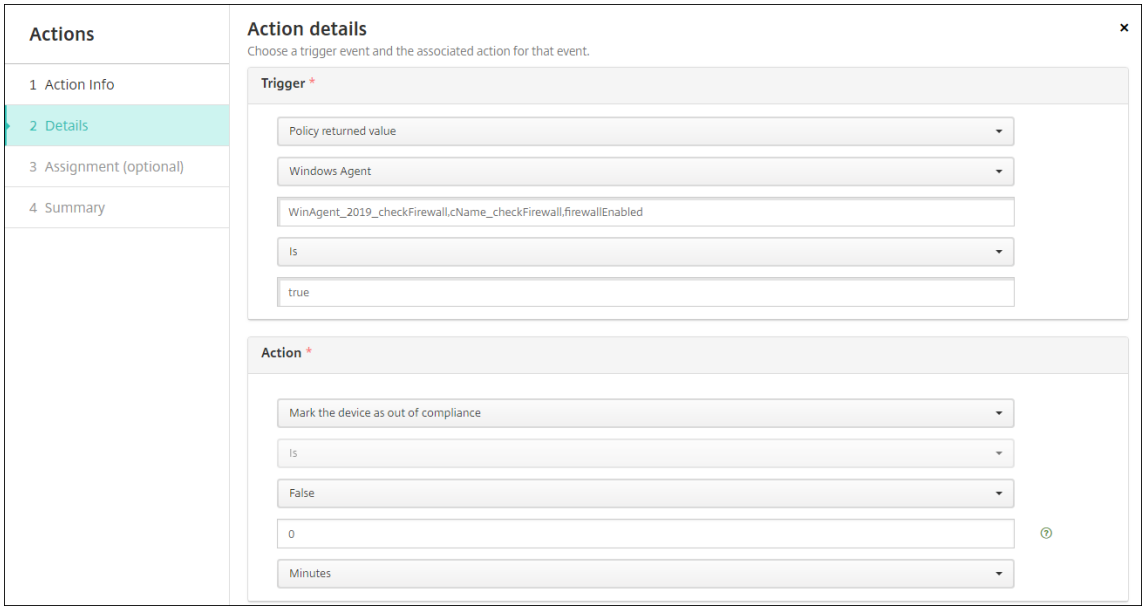
   「Windows エージェントのデバイスポリシー」で説明されているとおり、デバイス上でスクリプトが実行された後、ユーザーは操作の作成に必要な情報を取得します。

2. Citrix Endpoint Management コンソールで、［構成］**>**［アクション］の順にクリックします。
3. ［アクション］ページで、［追加］をクリックします。
4. ［アクション情報］ページで、アクションの名前および任意で説明を入力します。
5. ［アクションの詳細］ページで、［ポリシーの戻り値］トリガーを選択します。

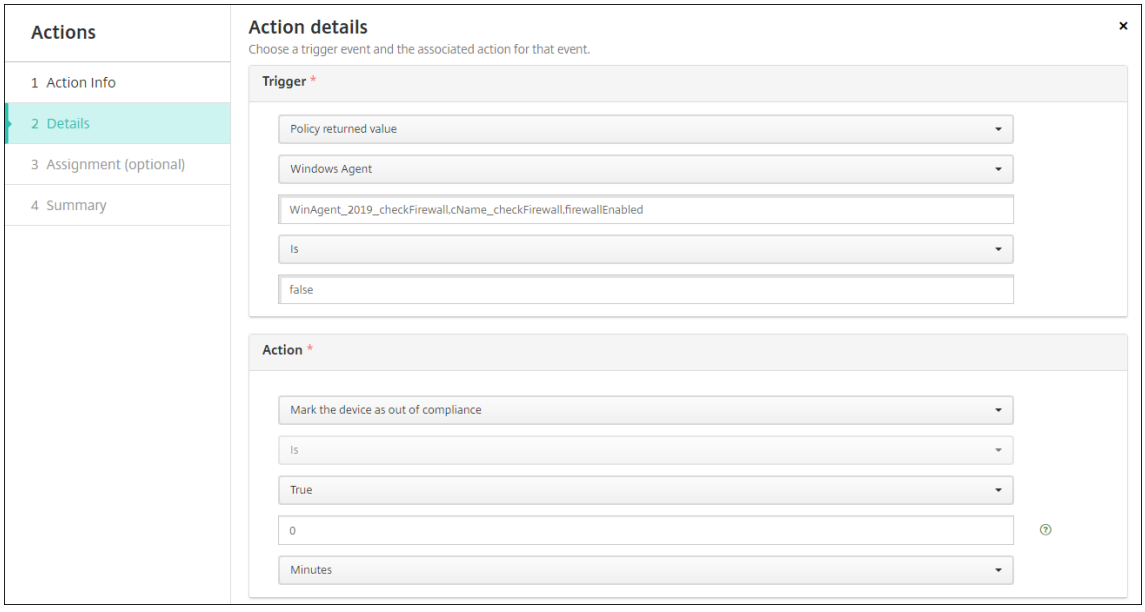
6. 表示されたフィールドで、トリガーとアクションを定義します:

   - **Windows** エージェント設定: 作成した Windows エージェントポリシーのポリシー名、構成名、キー名を入力します。
   - ドロップダウンメニュー: ［=］、［≠］、［含む］、または ［含まない］を選択します。この論理は次のフィールドに適用され、論理が適用されるとアクションがトリガーされます。
   - 文字列を入力: ポリシーでアップロードされた PowerShell スクリプトを実行した結果の文字列を入力します。この文字列について詳しくは、「Windows エージェントのデバイスポリシー」を参照してください。
   - アクション: アクション、アクションの値を選択して、アクションの解決に必要な時間を選択します。

この例では、キー名`firewallEnabled`が値**`true`**を返す場合、次のアクションによって、デバイスがコンプライアンス内としてマークされます。



この例では、キー名`firewallEnabled`が値**`false`**を返す場合、次のアクションによって、デバイスがコンプライアンス違反としてマークされます。



7. 必要に応じて展開スケジュールを設定し、デリバリーグループを選択します。

モニターとサポート

March 15, 2024

Citrix Endpoint Management ダッシュボードと Citrix Endpoint Management サポートページを使用して、Citrix Endpoint Management サーバーの監視およびトラブルシューティングを行えます。Citrix Endpoint Management サポートページを使用すると、サポートに関連する情報とツールにアクセスできます。

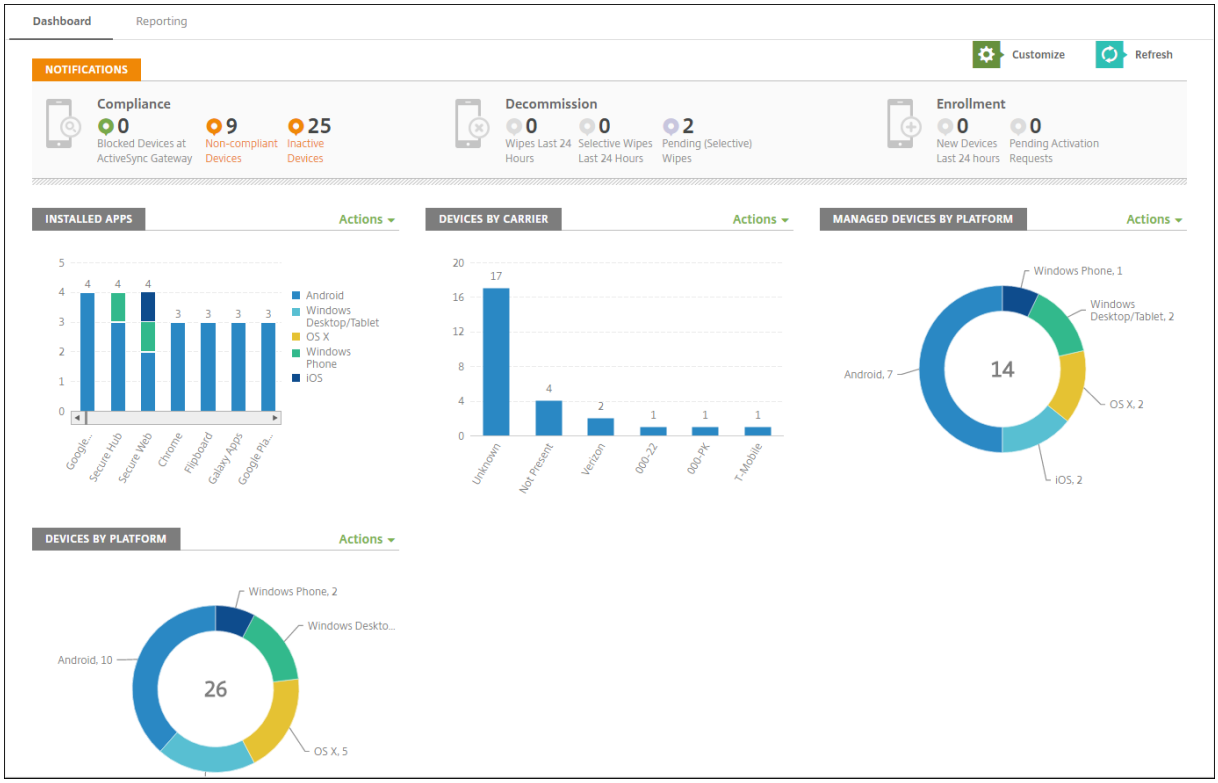
Citrix Endpoint Management コンソールで、右上のレンチアイコンをクリックします。

［トラブルシューティングとサポート］ページが開きます。

Citrix Endpoint Management の ［トラブルシューティングとサポート］ページでは、以下を行うことができます:

- 診断へのアクセス
- Citrix 製品ドキュメントおよび Knowledge Center へのリンクへのアクセス
- ログ操作へのアクセス
- 高度な構成オプションの使用
- 一連のツールおよびユーティリティへのアクセス

Citrix Endpoint Management コンソールのダッシュボードにアクセスして、情報を一目で確認することもできます。この情報を使用して、ウィジェットで問題や成功を速やかに確認できます。

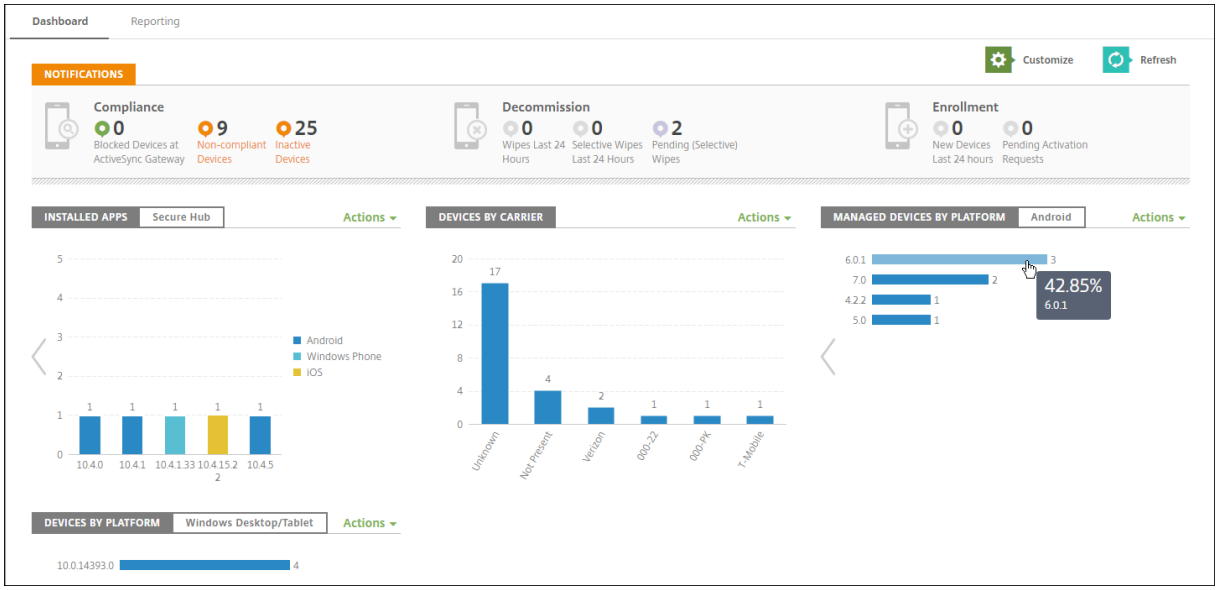


ダッシュボードは、Citrix Endpoint Management コンソールにサインオンすると通常最初に表示されるページです。コンソールの別の場所からダッシュボードにアクセスするには、［分析］をクリックします。ページのレイアウトを編集したり表示されるウィジェットを編集するには、ダッシュボードの ［カスタマイズ］をクリックします。

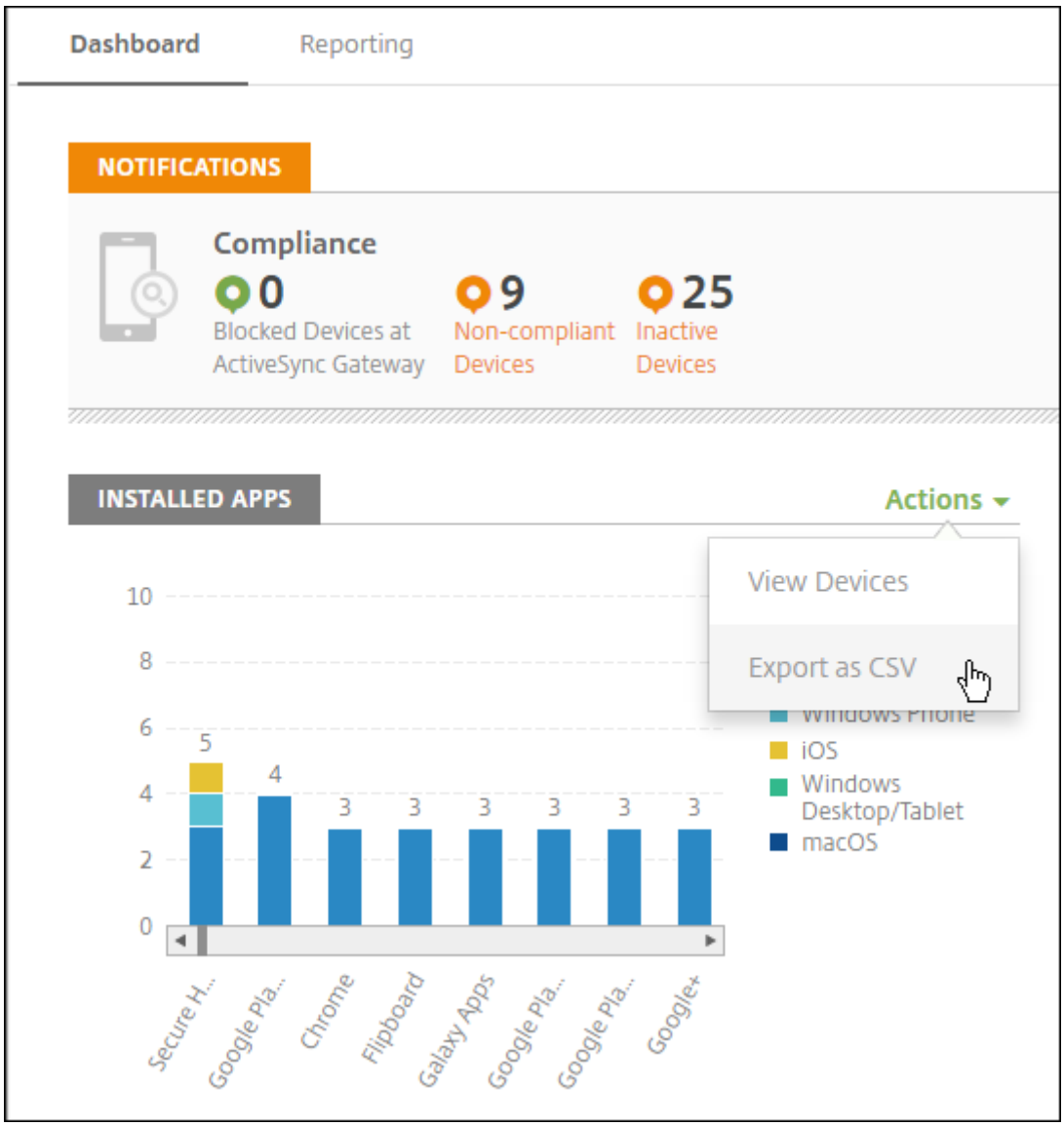
- マイダッシュボード：最大 4 つのダッシュボードを保存できます。ダッシュボードを個別に編集し、保存したダッシュボードを選択してそれぞれを表示することができます。
- レイアウトスタイル：この行では、ダッシュボードに表示するウィジェットの数とレイアウトを選択することができます。
- ウィジェット選択：ダッシュボードに表示する情報を選択することができます。
  - 通知：左側の数字の上のチェックボックスをオンにして、ウィジェットの上に通知バーを追加します。このバーには、準拠デバイス数、非アクティブデバイス数、24 時間以内にワイプまたは登録されたデバイス数が表示されます。
  - プラットフォームごとのデバイス：プラットフォームごとの管理対象デバイス数と管理対象外デバイス数が表示されます。
  - キャリアごとのデバイス：キャリアごとの管理対象デバイス数と管理対象外デバイス数が表示されます。各バーをクリックすると、プラットフォームごとの内訳が表示されます。
  - プラットフォームにより管理されているデバイス：プラットフォームごとの管理対象デバイス数が表示されます。
  - プラットフォームにより管理されていないデバイス：プラットフォームごとの管理対象外デバイス数が表示されます。このグラフに表示されるデバイスにはエージェントがインストールされている場合がありますが、特権が失効またはワイプされています。

- **ActiveSync** ゲートウェイ状態ごとのデバイス： ActiveSync ゲートウェイの状態ごとにグループ化されたデバイス数が表示されます。この情報では拒否、許可、または不明の状態が表示されます。各バーをクリックするとプラットフォームごとの内訳が表示されます。
- 所有権ごとのデバイス：所有権の状態ごとにグループ化されたデバイス数が表示されます。この情報ではコーポレート所有、従業員所有、または不明の所有権状態が表示されます。
- 失敗したデリバリーグループ展開：失敗した展開の合計数がパッケージごとに表示されます。展開に失敗したパッケージのみが表示されます。
- ブロックされた理由ごとのデバイス： ActiveSync でブロックされたデバイス数が表示されます。
- インストール済みアプリ：アプリ名を入力すると、アプリ情報のグラフが表示されます。
- 一括購入アプリライセンス使用状況： Apple の一括購入アプリのライセンス使用状況に関する統計データが表示されます。

各ウィジェットでは個々の部分をクリックして、さらに情報をドリルダウンできます。



［操作］メニューをクリックして、情報を.csv ファイルとしてエクスポートすることもできます。



ヘルプデスク管理者のためのモニターページ

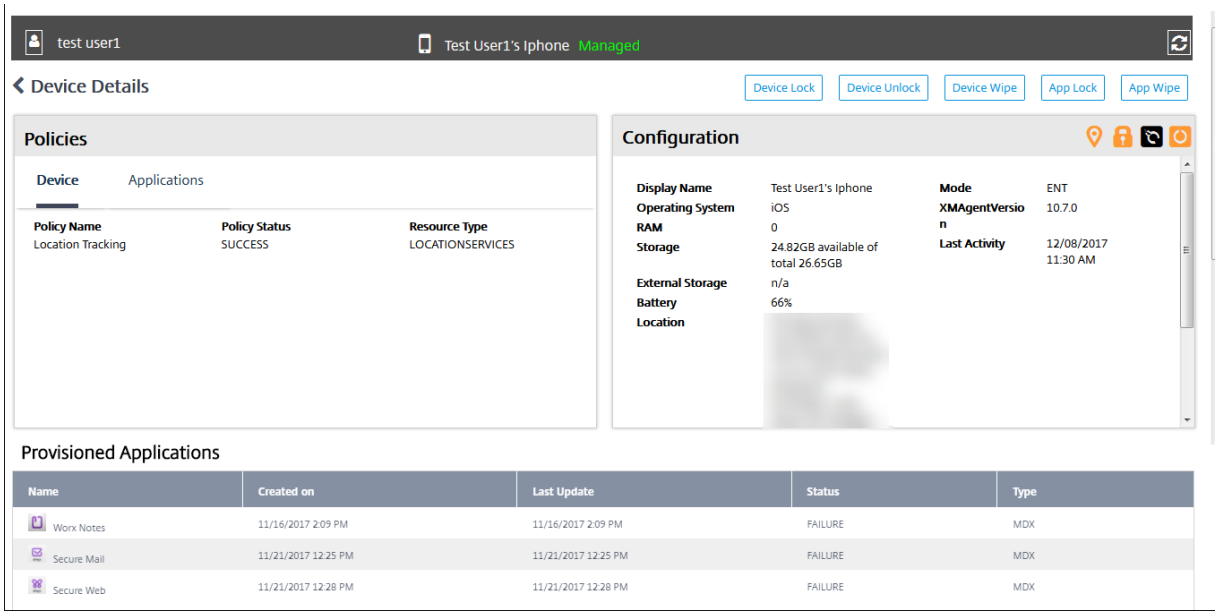
［モニター］ページでは、Citrix Endpoint Management Service の監視およびトラブルシューティングを実行できます。このインターフェイスは、ヘルプデスク管理者がユーザーごとのトラブルシューティングを効率的に実行できるようにカスタマイズされています。

ヘルプデスク管理者が ［モニター］タブとすべての利用可能なワークフローにアクセスするには、次の権限が必要です。

- 承認済みアクセス
  - 管理コンソールへのアクセス
  - パブリック API へのアクセス

- コンソール機能
  - 監視
  - デバイス
  - デバイスの完全なワイプ
  - 場所の表示
    - デバイスの場所の確認
    - デバイスの追跡
  - デバイスのロック
  - デバイスのロック解除
  - アプリのロック
  - アプリのワイプ
  - アプリ

［モニター］ページには、デバイスポリシーと構成をまとめたビューが表示されます。このビューでは、アプリのロック/ロック解除、アプリのワイプ、デバイスのロック/ロック解除、デバイスのワイプなどのトラブルシューティング操作を行うことができます。



［モニター］ページでは以下の操作が可能です：

- トラブルシューティングを行う Active Directory（AD）のユーザーおよびデバイスを検索する。
- 以下の項目がある ［デバイス詳細］ページで分析する：
  - ポリシー：選択したデバイスとアプリのデバイスポリシーとアプリポリシーが表示されます。ポリシーの変更方法については、「デバイスポリシー」と「アプリの追加」を参照してください。
  - 構成：デバイスの構成が表示されます。このパネルには、デバイスの位置情報サービスの状態とジェイルブレイクの有無、およびデバイスが MAM または MDM の管理対象かどうかを示す各種アイコンが表示されます。また、ストレージの暗号化状態も表示されます。

  - ［実行中のアプリ］テーブル：デバイスで現在実行されているアプリケーションの詳細が表示されます。

- デバイスのトラブルシューティング。このページで実行できるセキュリティ操作は、デバイスの登録状態およびログイン済みの管理者が持つ権限によって決まります。

  - デバイスのロック/ロック解除
  - デバイスのワイプ
  - アプリのロック/ロック解除（デバイスが MAM に登録済みの場合に利用可能）
  - アプリのワイプ（デバイスが MAM に登録済みの場合に利用可能）

実行できる操作について詳しくは、「セキュリティ操作」を参照してください。

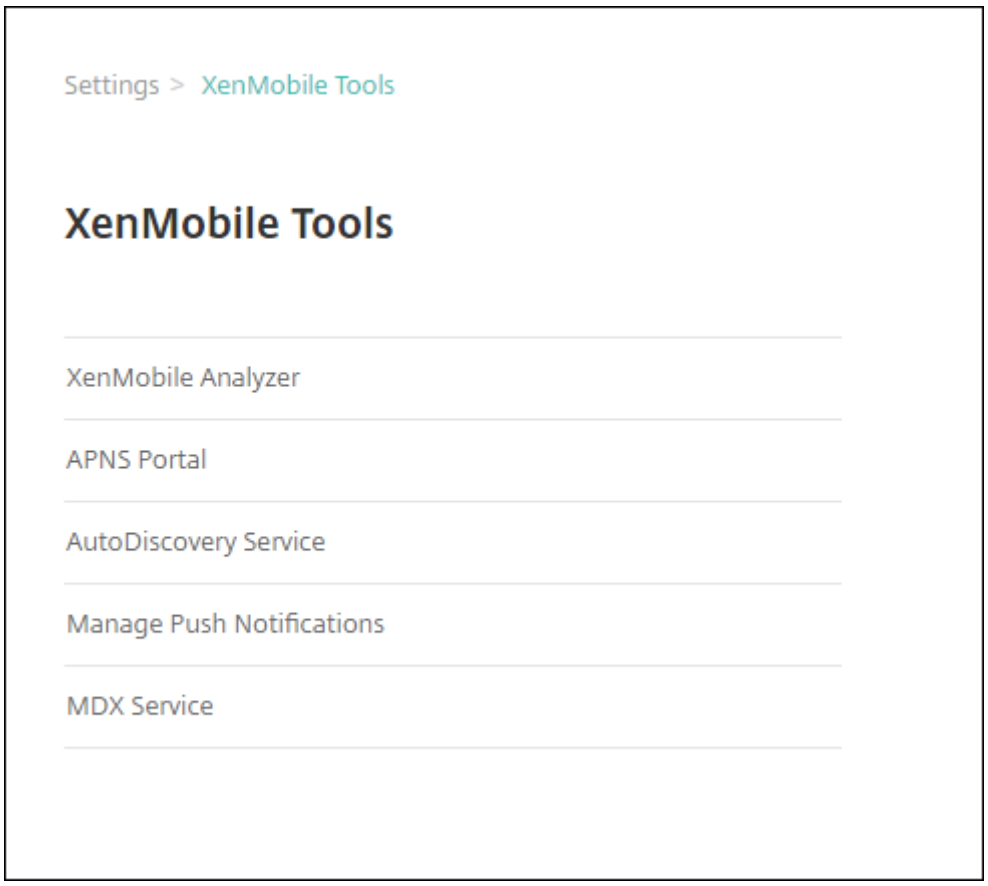
［モニター］ページではログイントークンの更新が行われないため、最後の読み込みから 60 分が経過すると正常に動作しなくなる場合があります。この問題を回避するには、サービスコンソールで［**Citrix Cloud**］リンクをクリックして［**Citrix Endpoint Management**］**>**［管理］**>**［モニター］の順にクリックし、ページを再読み込みしてトークンを更新します。

コンソールから **Citrix Endpoint Management** ツールへのアクセス

Citrix Endpoint Management コンソールでは、以下の Citrix Endpoint Management ツールにアクセスできます:

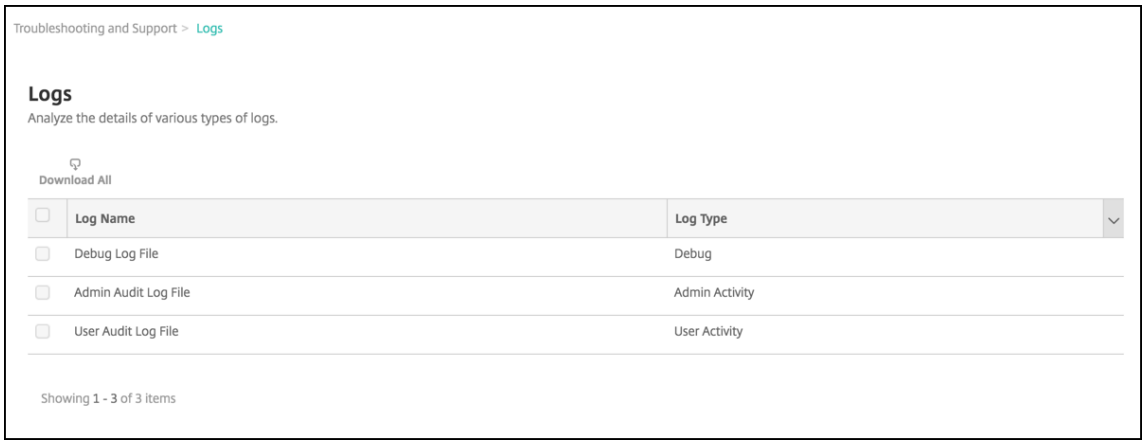
- **APNs** ポータル–Citrix に APNs 証明書への署名を求める要求を送信します。署名された証明書は、Apple に提出します。
- 自動検出サービス–ドメインの Citrix Endpoint Management の AutoDiscovery を要求および構成します。
- プッシュ通知の管理–iOS および Windows のモバイルアプリのプッシュ通知を管理します。

これらのツールにアクセスするには、［設定］**>**［**Citrix Endpoint Management** ツール］に移動します。このページは、Cloud Admin または Customer Admin の役割を持つユーザーが使用できます。



Citrix Endpoint Management でのログファイルの表示および分析

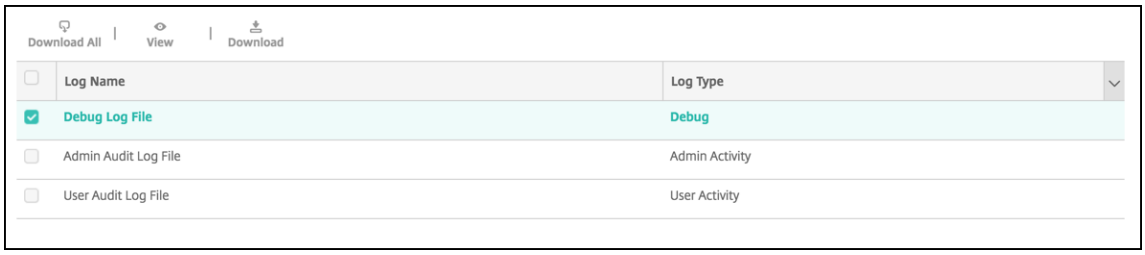
1. Citrix Endpoint Management コンソールで、右上のレンチアイコンをクリックします。［トラブルシューティングとサポート］ページが開きます。
2. ［ログの操作］の ［ログ］をクリックします。［ログ］ページが開きます。表に個別のログが表示されます。



3. 表示するログをオンにします。

- デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrix のサポート担当者向けの有用な情報が含まれています。
- 管理監査ログファイルには、Citrix Endpoint Management コンソール上のアクティビティについての監査情報が含まれています。
- ユーザー監査ログファイルには構成済みユーザーに関連する情報が含まれています。

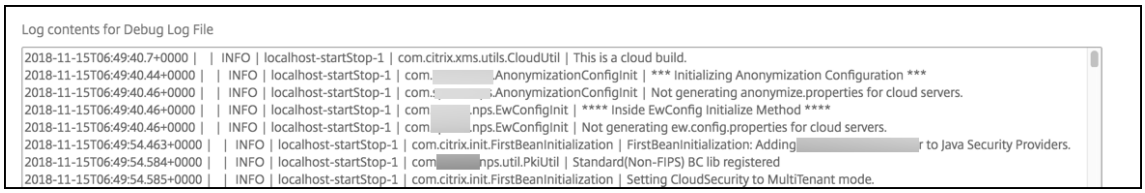
4. 表の上にあるアクションを使用して、すべてダウンロード、表示、または単一ログのダウンロードを行います。



> 注:
>
> 複数のログファイルを選択した場合は、［すべてダウンロード］のみを使用できます。

5. 次のいずれかを行います:

- すべてをダウンロード: システム上に存在するすべてのログ（デバッグ、管理監査、ユーザー監査、サーバーのログなど）をダウンロードします。
- 表示: 表の下に選択したログの内容を表示します。
- ダウンロード: コンソールは、選択した単一のログファイルタイプのみをダウンロードします。コンソールは同じタイプのアーカイブされたログもダウンロードします。



Citrix Endpoint Management は、log4j syslog アペンダーを使用して、RFC5424 形式の syslog メッセージを送信します。syslog メッセージのデータは、特定の形式のないプレーンテキストです。

接続確認

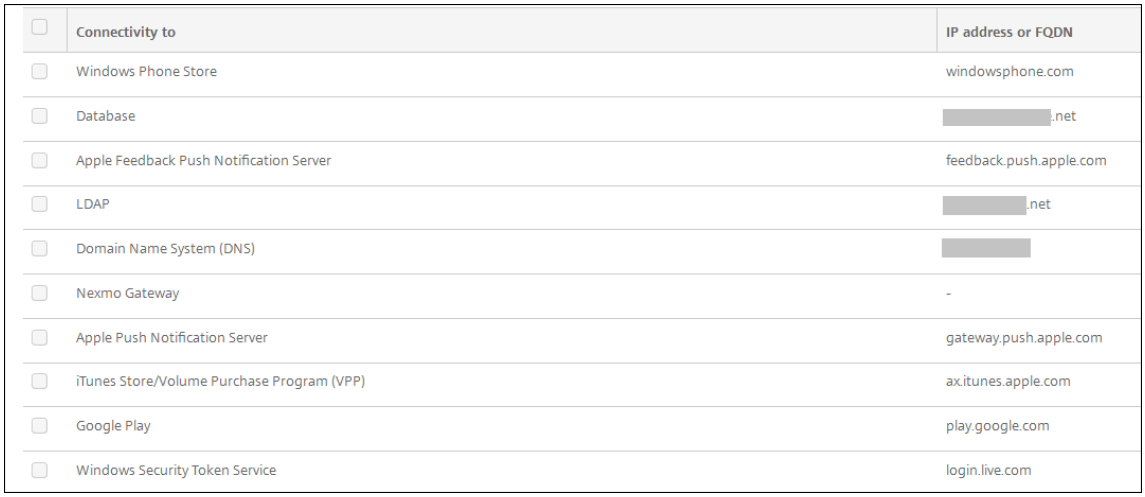
November 29, 2023

Citrix Endpoint Management の［トラブルシューティングとサポート］ページで、Citrix Gateway およびそのほかのサーバーや場所への Citrix Endpoint Management の接続を確認できます。Citrix Endpoint Management 接続性チェックを実行するには、Support または Admin の役割が必要です。役割ベースのアクセス制御（RBAC）

を使用してこの役割を設定します。役割の割り当てについて詳しくは、「RBAC を使用した役割の構成」を参照してください。

Citrix Endpoint Management 接続性チェックを実行する

1. Citrix Endpoint Management コンソールで、右上のレンチアイコンをクリックします。［トラブルシューティングとサポート］ページが開きます。
2. ［診断］の下の ［**Citrix Endpoint Management** 接続性チェック］をクリックします。［**Citrix Endpoint Management** 接続性チェック］ページが開きます。Citrix Endpoint Management 環境内にクラスターノードがある場合は、すべてのノードが表示されます。

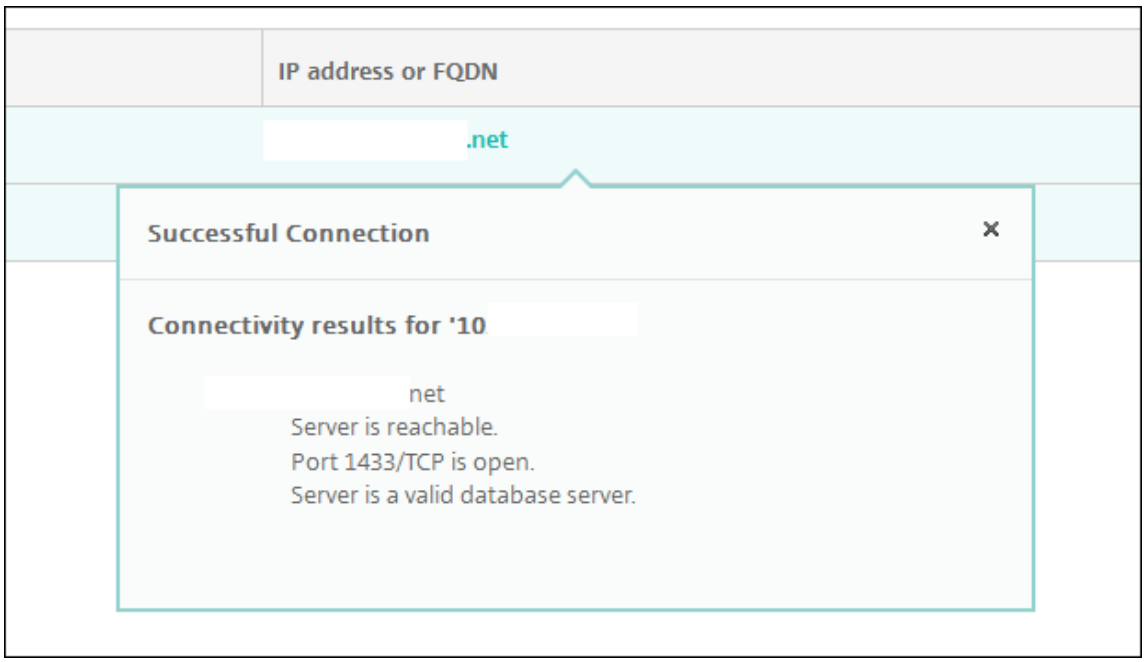


Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. 接続テストに含めるサーバーをオンにして、［接続性をテスト］をクリックします。［テスト結果］ページが開きます。

Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

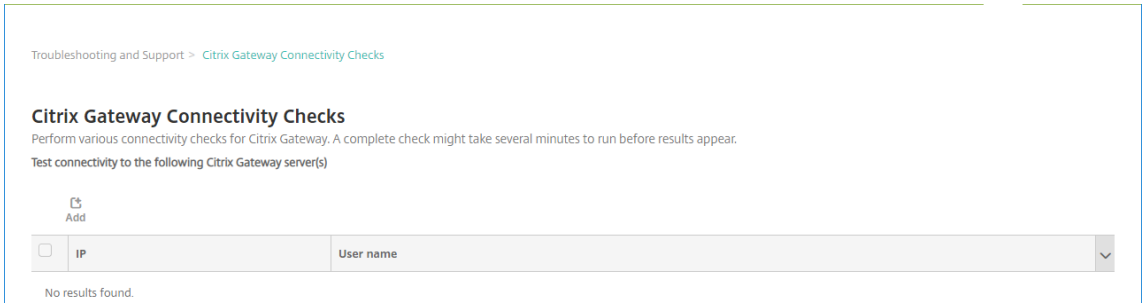
4. ［テスト結果］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。



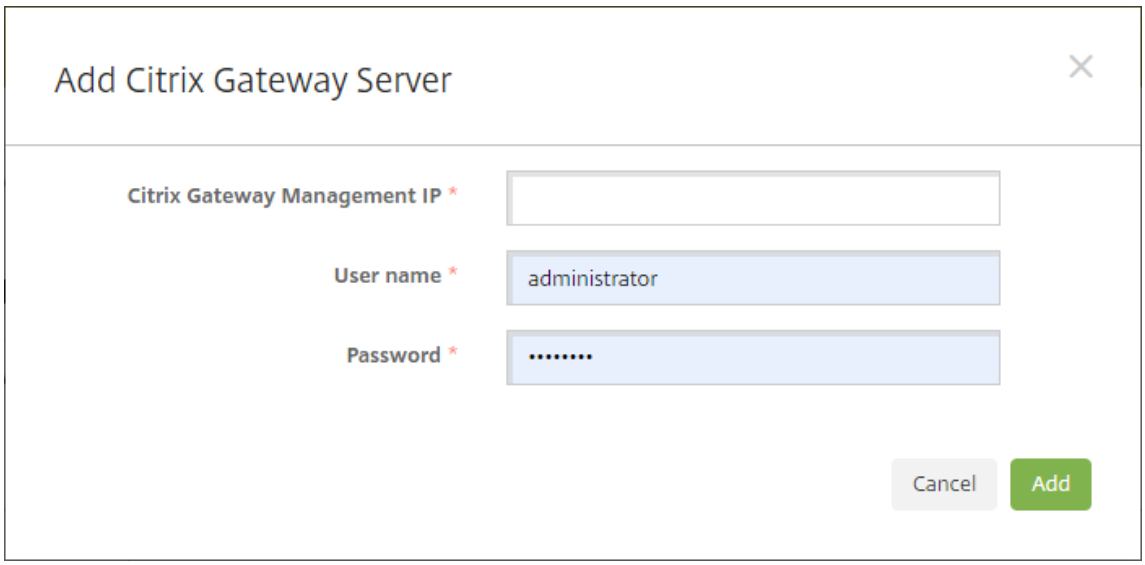
Citrix Endpoint Management で実行できる接続チェックとその詳細については、「接続チェックの詳細」を参照してください。

Citrix Gateway の接続チェックの実行

1. ［トラブルシューティングとサポート］ページで、［診断］の下の ［**Citrix Gateway** 接続性チェック］をクリックします。［**Citrix Gateway** 接続性チェック］ページが開きます。Citrix Endpoint Management と Citrix Gateway 間に接続がない場合、表は空です。



2. ［追加］をクリックします。［**Citrix Gateway** サーバーの追加］ダイアログボックスが開きます。



3. ［**Citrix Gateway** 管理 **IP**］ボックスに、テストする Citrix Gateway を実行しているサーバーの管理 IP アドレスを入力します。

   既に追加されている Citrix Gateway サーバーの接続確認を実行する場合、IP アドレスは入力されています。

4. この Citrix Gateway の管理者資格情報を入力します。

   既に追加されている Citrix Gateway サーバーの接続確認を実行する場合、ユーザー名は入力されています。

5. ［追加］をクリックします。Citrix Gateway が、［**Citrix Gateway** 接続性チェック］ページの表に追加されます。

6. Citrix Gateway サーバーを選択して、［接続性をテスト］をクリックします。［テスト結果］の表に結果が表示されます。

7. ［テスト結果］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

接続チェックの詳細

次の表は、Citrix Endpoint Management で実行できるさまざまな接続チェックと各チェックの詳細の一覧です。

接続先	**IP** アドレスまたは **FQDN**	詳細
Apple プッシュ通知サーバー	api.push.apple.com	Apple プッシュ通知サーバーと Citrix Endpoint Management ノード間の接続を確認します。iOS および macOS デバイスにメッセージを送信するには、Apple プッシュ通知サーバーが必要です。

接続先	**IP** アドレスまたは **FQDN**	詳細
Apple フィードバックプッシュ通知サーバー	feedback.push.apple.com	Apple フィードバックサーバーと Citrix Endpoint Management ノード間の接続を確認します。Apple フィードバックプッシュ通知サーバーは、iOS デバイスおよび macOS デバイスに送信された、失敗したリモート通知に関する情報を提供します。
Citrix ライセンスサーバー	ライセンスサーバーの IP アドレス	Citrix ライセンスサーバーと Citrix Endpoint Management ノード間の接続を確認します。Citrix 製品が動作するサーバーが Citrix ライセンスサーバーと通信し、必要なライセンスを取得します。
Citrix Gateway	Citrix Endpoint Management で構成された Citrix Gateway の完全修飾ドメイン名	Citrix Gateway と Citrix Endpoint Management ノード間の接続を確認します。Citrix Gateway は、VPN サーバーを介して接続して内部ネットワークにアクセスするために、Citrix Endpoint Management クライアントアプリ（Citrix Secure Mail、Citrix Secure Web など）によって使用されます。
データベース	データベースサーバーの IP アドレスまたは FQDN	Citrix Endpoint Management データベースと Citrix Endpoint Management ノード間の接続を確認します。
ドメインネームシステム（DNS）	Citrix Endpoint Management で構成された IP アドレス	DNS サーバーと Citrix Endpoint Management ノード間の接続を確認します。
Secure Ticket Authority サービス	localhost	認証サービス、STA（Secure Ticket Authority）サービス、およびクラスターサービスへの Citrix Endpoint Management ノードの接続を確認します。

接続先	**IP** アドレスまたは **FQDN**	詳細
Firebase Cloud Messaging（FCM）サーバー		FCM サーバーと Citrix Endpoint Management ノード間の接続を確認します。FCM を使用すると、新しいメールやその他のデータを同期できることをクライアントアプリに通知できます。通知メッセージを送信して、ユーザーのエンゲージメントと維持を促進できます。FCM は、Google Cloud Messaging（GCM）の代わりになります。
Google Play	play.google.com	Google ストアサーバーと Citrix Endpoint Management ノード間の接続を確認します。Google Play を使用すると、管理対象のプライベートエンタープライズアプリ配信ストアを含むサービスが提供されます。
iTunes Store/一括購入	vpp.itunes.apple.com	Apple Store サーバーと Citrix Endpoint Management ノード間の接続を確認します。Apple Store を使用すると、管理対象のプライベートエンタープライズアプリ配信ストアを含むサービスが提供されます。
LDAP	Citrix Endpoint Management で構成された LDAP の IP アドレスまたは完全修飾ドメイン名	LDAP サーバーと Citrix Endpoint Management ノード間の接続を確認します。
Microsoft プッシュ通知サーバー	sin.notifiy.windows.com	Windows 通知サーバーと Citrix Endpoint Management ノード間の接続を確認します。Windows 通知サーバーは、Windows デバイスにメッセージを送信するために使用します。
ShareFile サービス	Citrix Endpoint Management で構成された ShareFile サービスの IP アドレスまたは完全修飾ドメイン名	ShareFile サービスと Citrix Endpoint Management の間の接続を確認します。ShareFile サービスは、企業が大きなファイルを保存および共有するための安全なクラウドベースのプラットフォームです。

接続先	**IP** アドレスまたは **FQDN**	詳細
Windows デスクトップ/タブレットストア	windows.microsoft.com	Windows デスクトップストア、Windows タブレットストアと Citrix Endpoint Management ノード間の接続を確認します。Windows デスクトップストア、Windows タブレットストアを使用すると、管理対象のプライベートエンタープライズアプリ配信ストアを含むサービスが提供されます。
Windows セキュリティトークンサービス	login.live.com	Windows セキュリティトークンサーバーと Citrix Endpoint Management ノード間の接続を確認します。Windows セキュリティトークンサービスは、Windows デバイスの 2 要素認証（ドメインとセキュリティトークン）をサポートします。

モバイルサービスプロバイダー

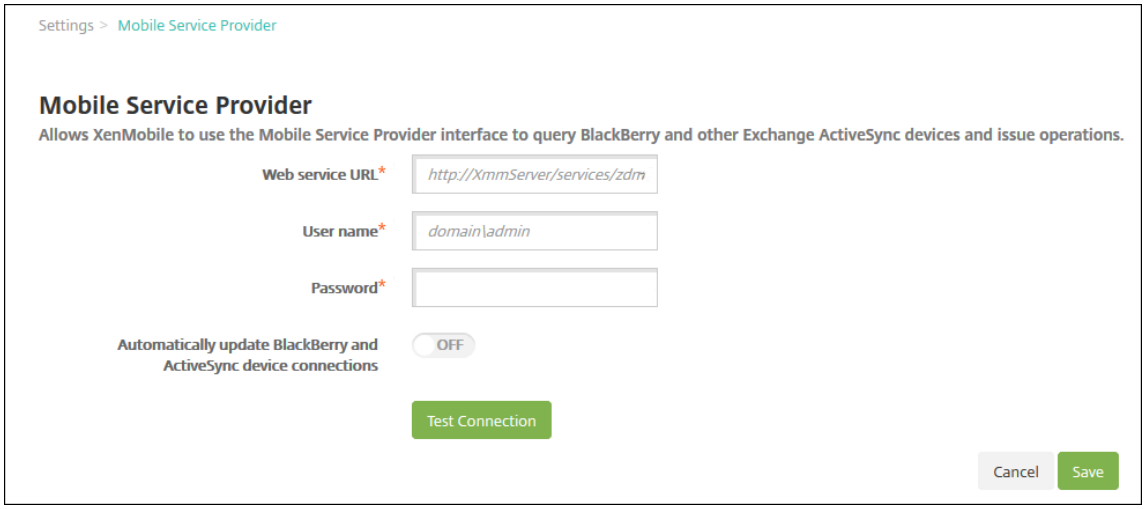
November 29, 2023

Citrix Endpoint Management でモバイルサービスプロバイダーインターフェイスの使用を有効にして、BlackBerry や Exchange ActiveSync デバイスに対してクエリを実行したり、操作を発行したりできます。

たとえば、組織に 1,000 ユーザーが存在し、各ユーザーが 1 つまたは複数のデバイスを使用するとします。すべてのユーザーに対して、デバイスを Citrix Endpoint Management に登録するように通知した後、Citrix Endpoint Management コンソールはユーザーが登録したデバイスの数を表示します。この設定を構成することで、Exchange Server に接続しているデバイスの数を判断できます。これによって、次の操作を実行できます。

- ほかにデバイスを登録する必要のあるユーザーがいるかどうかを確認する。
- Exchange Server に接続するユーザーデバイスにコマンド（データワイプなど）を発行する。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［サーバー］の下の ［モバイルサービスプロバイダー］をクリックします。［モバイルサービスプロバイダー］ページが開きます。



3. 次の設定を構成します:

   - **Web サービス URL**: Web サービスの URL（`https://XmmServer/services/xdmservice`など）を入力します。
   - ユーザー名: `domain\\admin`の形式でユーザー名を入力します。
   - パスワード: パスワードを入力します。
   - **BlackBerry** および **ActiveSync** デバイス接続を自動的に更新: デバイス接続を自動的に更新するかどうかを選択します。デフォルトは ［オフ］ です。
   - ［接続のテスト］をクリックして、接続を検証します。

4. ［保存］をクリックします。

レポート

March 15, 2024

Citrix Endpoint Management には、以下の事前定義されたレポートが用意されており、アプリおよびデバイスの展開を分析できます。各レポートは表とグラフで表示されます。表は、列を基準にして並び替えとフィルターを行うことができます。グラフ内の要素を選択すると詳細を確認できます。

- アプリ展開の合計試行回数: ユーザーがデバイスへのインストールを試みた展開済みのアプリを一覧表示します。
- プラットフォームを基準とするアプリ: アプリとアプリバージョンを、デバイスプラットフォーム別およびバージョン別に一覧表示します。
- 種類別アプリ: アプリをバージョン別、種類別、およびカテゴリ別に一覧表示します。
- デバイス登録: すべての登録済みデバイスを一覧表示します。
- デバイスおよびアプリ: 管理対象アプリを実行しているデバイスを一覧表示します。

- 非アクティブデバイス：Citrix Endpoint Management サーバーのプロパティ`device.inactivity.days.threshold`で指定された日数にわたりアクティビティがないデバイスを一覧表示します。
- ジェイルブレイク**/Root** 化されたデバイス：ジェイルブレイクされた iOS デバイスと Root 化された Android デバイスを一覧表示します。
- 使用条件：使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。グラフの各領域を選択すると詳細を確認できます。
- 上位 **10** 失敗した展開：展開に失敗したアプリを最大で 10 個まで一覧表示します。
- 禁止されているアプリ（デバイス**/**ユーザー別）：ユーザーのデバイスに存在し、禁止リストに登録されているアプリを一覧表示します。
- 非準拠デバイス：準拠基準を満たしていないデバイスを一覧表示します。基準には、デバイスがジェイルブレイクされているかどうか、実行中の OS バージョン、およびデバイスにパスコードがあるかどうかなどがあります。レポートには、デバイスに関連付けられているユーザー名と、デバイスが暗号化されているかどうかも表示されます。iOS デバイスの場合、暗号化列には N/A が表示されます。

各表のデータを、Microsoft Excel などのプログラムで開く.csv 形式でエクスポートできます。各レポートのグラフは、PDF 形式でエクスポートできます。

［レポート］タブには、シリアル番号、IMEI/MEID、アプリ、接続などのデバイスの詳細が含まれています。特定のデバイスに関するより包括的なレポートについては、［管理］**>**［デバイス］の順に移動してデバイスをクリックし、［詳細表示］をクリックして、［デバイス詳細］ページを表示します。［デバイス詳細］ページには、デバイスのセキュリティプロパティ、デバイスのプロパティ、割り当てられているポリシー、アプリ、アクション、証明書などが一覧表示されます。［デバイス詳細］ページについて詳しくは、「デバイス情報の取得」を参照してください。

次の設定で、Citrix Endpoint Management が管理対象デバイスに展開またはインストールされているアプリに関する情報を収集する方法を決定します：

- デバイスの種類
- 登録方法
- アプリインベントリデバイスポリシーが展開されているかどうか

Android デバイスの場合、動作はデバイスの種類と登録方法によって異なります。次の表は、アプリが **Android Enterprise** のどこに表示されるか（［デバイス詳細］ページ、レポート、または利用不可）を示しています。特に明記されていない限り、アプリ一覧にはすべてのアプリが含まれます。

	MDM+MAM （すべてのアプリ）	MDM（すべてのアプリ）
必須アプリ（アプリインベントリポリシー未展開）	［デバイス詳細］ページとレポート	パブリックアプリ：［デバイス詳細］ページとレポート
オプションアプリ（アプリインベントリポリシー未展開）	使用できません	使用できません
必須アプリ（アプリインベントリポリシー展開済み）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート

	MDM+MAM （すべてのアプリ）	MDM（すべてのアプリ）
オプションアプリ（アプリインベントリポリシー展開済み）	エンタープライズ、MDX、パブリック、および Web リンクアプリ：レポート	［デバイス詳細］ページとレポート

次の表は、アプリが **Android**（従来の **DA**）のどこに表示されるか（[デバイス詳細］ページ、レポート、または利用不可）を示しています。特に明記されていない限り、アプリ一覧にはすべてのアプリが含まれます。

	MDM+MAM （すべてのアプリ）	MDM（パブリックおよびエンタープライズアプリ）	MAM
必須アプリ（アプリインベントリポリシー未展開）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	-
オプションアプリ（アプリインベントリポリシー未展開）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	使用できません
必須アプリ（アプリインベントリポリシー展開済み）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	-
オプションアプリ（アプリインベントリポリシー展開済み）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	使用できません

iOS デバイスの場合、動作は登録方法によって異なります。次の表は、アプリがどこに一覧表示されるか（[デバイス詳細］ページまたはレポート）を示しています。特に明記されていない限り、アプリ一覧にはすべてのアプリが含まれます。

	MDM+MAM （すべてのアプリ）	MDM（パブリックおよびエンタープライズアプリ）	MAM（すべてのアプリ）
必須アプリ（アプリインベントリポリシー未展開）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート。これらのアプリは、（インストールされていない場合でも）保留状態で表示されるか、手動でインストールされた後も保留状態のままになります。

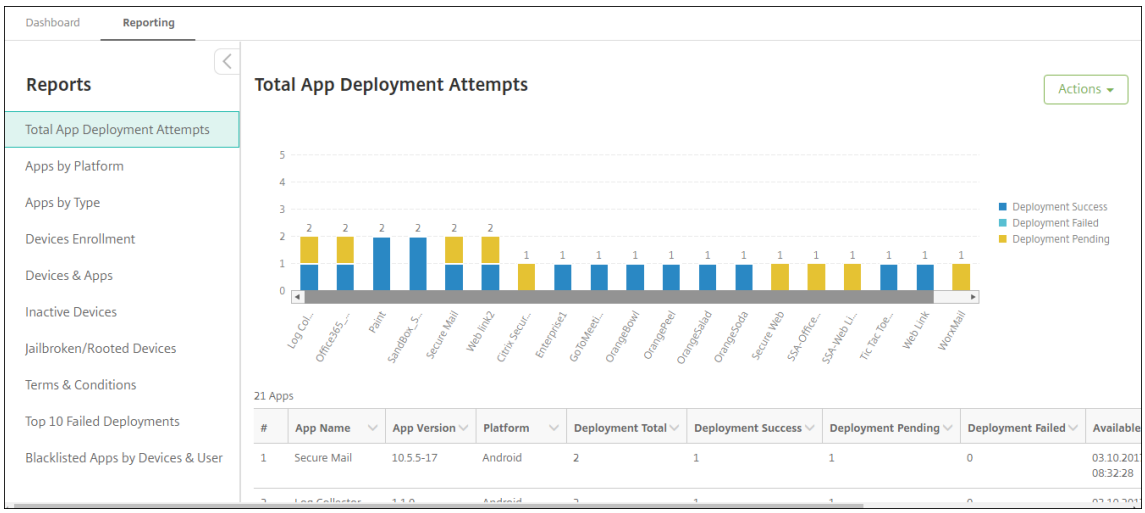
	MDM+MAM （すべてのアプリ）	MDM（パブリックおよびエンタープライズアプリ）	MAM（すべてのアプリ）
オプションアプリ（アプリインベントリポリシー未展開）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	Web、SaaS、および Web リンクアプリは、インストール済みアプリとして［デバイス詳細］ページに一覧表示されますが、レポートには一覧表示されません。エンタープライズ、MDX、およびパブリックアプリは、手動でインストールされた後、［デバイス詳細］ページに表示されません。アプリは、手動でインストールされた後、レポートに表示されません。
必須アプリ（アプリインベントリポリシー展開済み）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	アプリインベントリポリシーをデバイスに展開することはできません。アプリは、［デバイス詳細］ページとレポートに一覧表示されます。これらのアプリは、（インストールされていない場合でも）保留状態で表示されるか、手動でインストールされた後も保留状態のままになります。

	MDM+MAM （すべてのアプリ）	MDM（パブリックおよびエンタープライズアプリ）	MAM（すべてのアプリ）
オプションアプリ（アプリインベントリポリシー展開済み）	［デバイス詳細］ページとレポート	［デバイス詳細］ページとレポート	アプリインベントリポリシーをデバイスに展開することはできません。Web、SaaS、および Web リンクアプリは、インストール済みアプリとして ［デバイス詳細］ページに一覧表示されますが、レポートには一覧表示されません。エンタープライズ、MDX、およびパブリックアプリは、手動でインストールされた後、［デバイス詳細］ページに表示されません。アプリは、手動でインストールされた後、レポートに表示されません。

macOS および Windows デバイスの場合、Citrix Endpoint Management は、アプリインベントリポリシーが展開されている場合にのみアプリのインベントリを収集します。

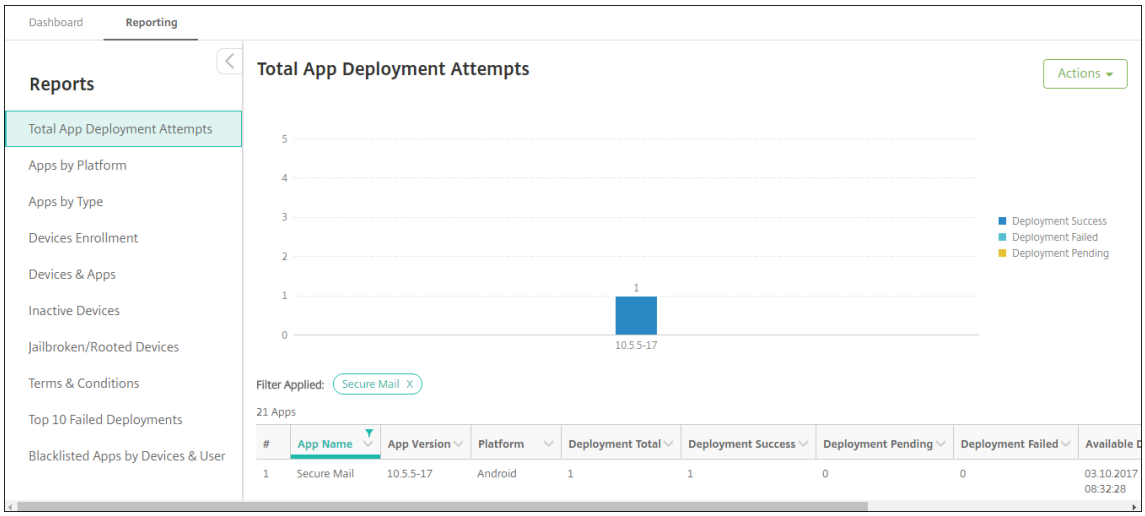
レポートを作成するには

1. Citrix Endpoint Management コンソールで ［分析］**>**［レポート］の順にクリックします。［レポート］ページが開きます。
2. 作成するレポートをクリックします。

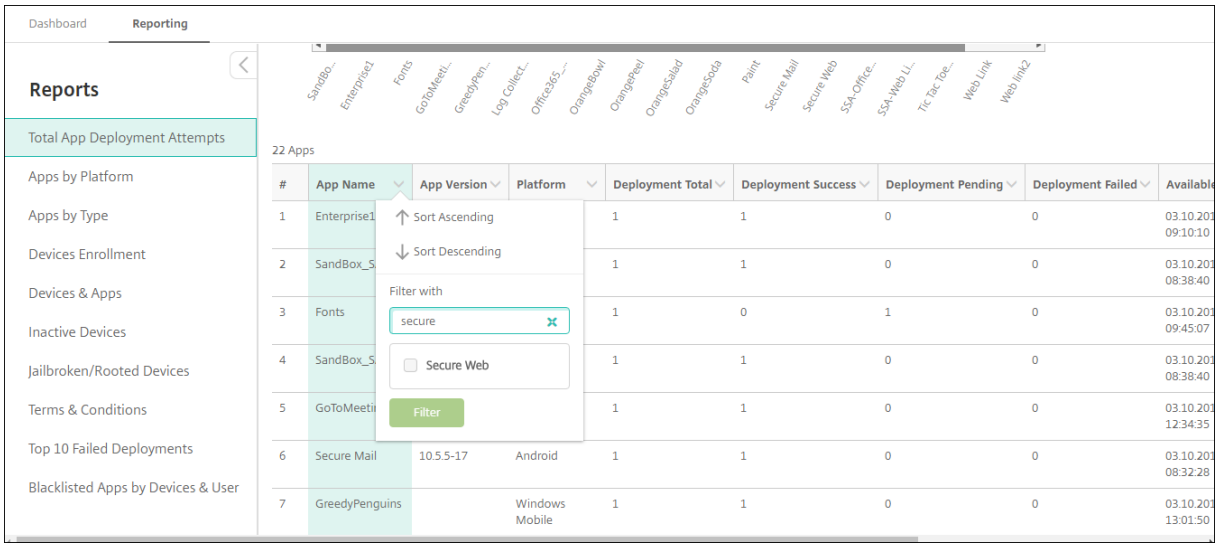


レポートの詳細を確認するには

1. グラフの各領域をクリックしてドリルダウンすると、詳細が表示されます。

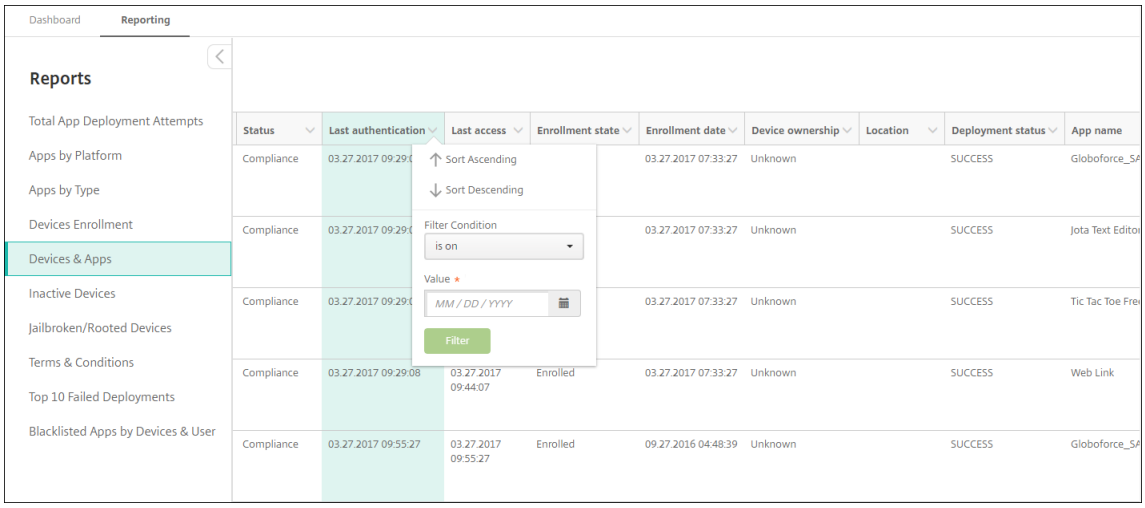


表の列を並び替え、フィルター、または検索するには、列の見出しをクリックします

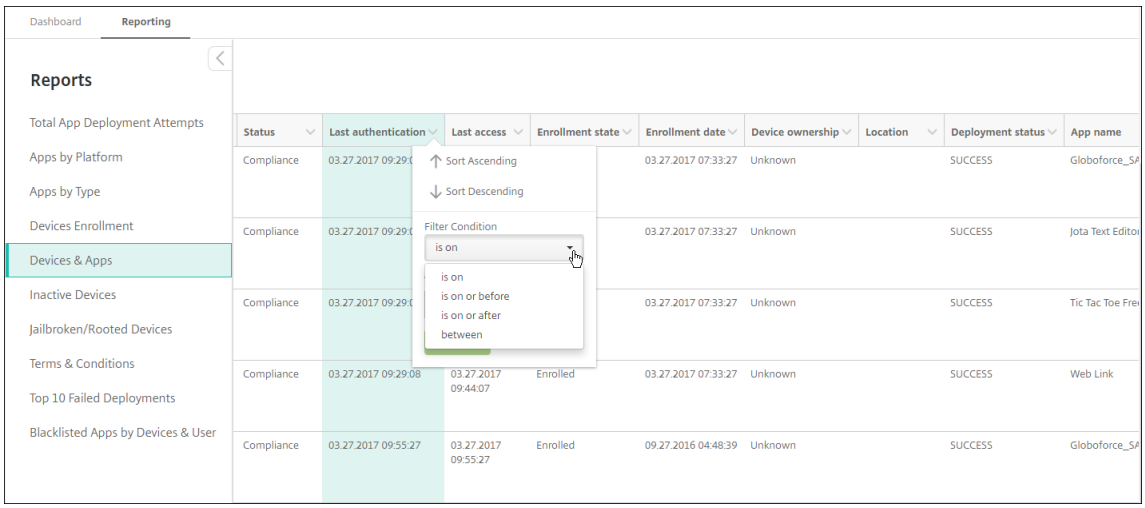


レポートを日付でフィルターするには

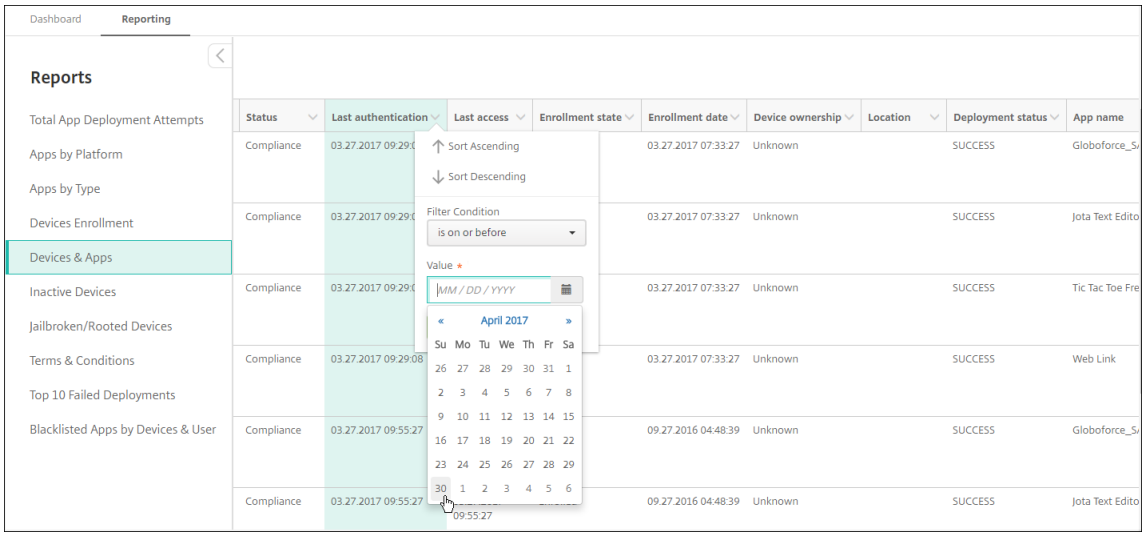
1. 列の見出しをクリックして、フィルター設定を表示します。



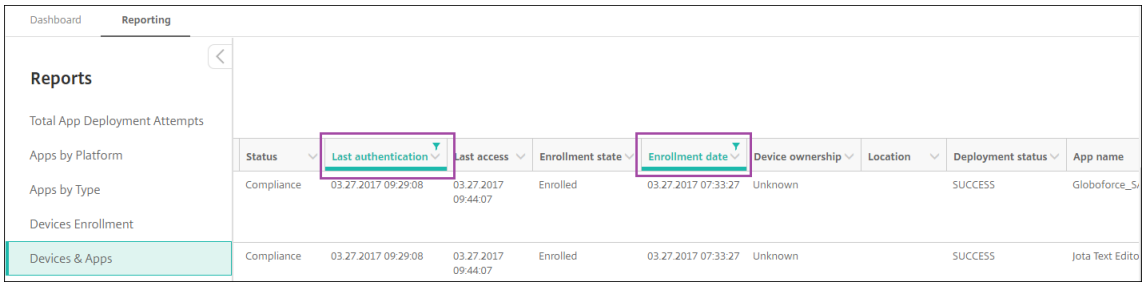
2. ［フィルター条件］で、レポート対象期間を絞り込む方法を選択します。



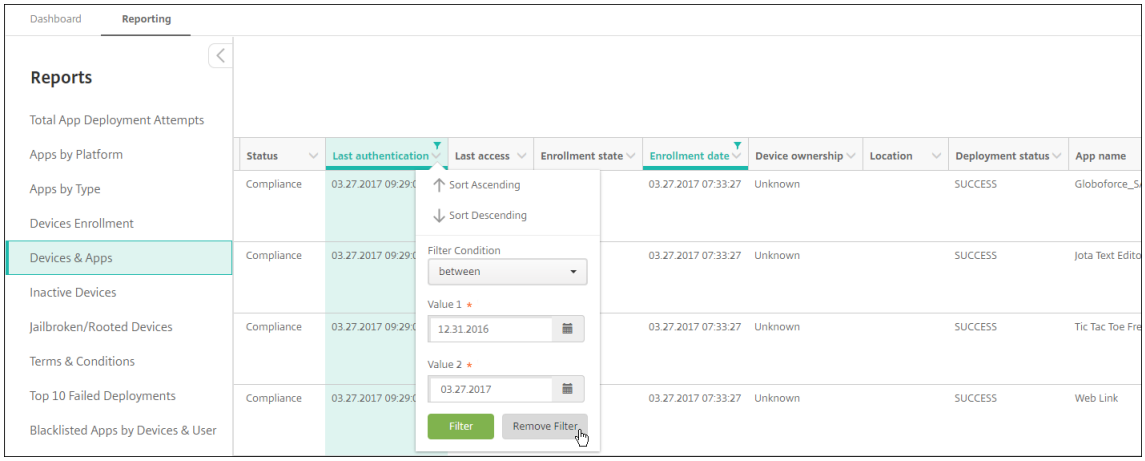
3. カレンダーを使用して日付を指定します。



4. 次の例のように、日付フィルターの付いた列が表示されます。

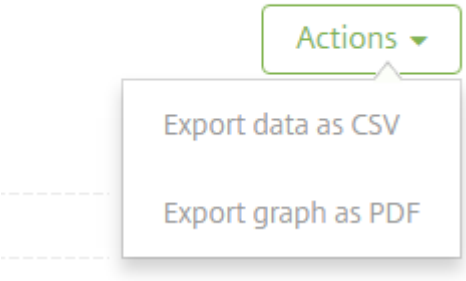


5. フィルターを削除するには、列の見出しをクリックして ［フィルターの削除］をクリックします。



グラフまたは表をエクスポートするには

- グラフを PDF 形式でエクスポートするには、［操作］>［**PDF** でグラフをエクスポート］の順にクリックします。
- 表のデータを CSV 形式でエクスポートするには、［操作］>［**CSV** でデータをエクスポート］の順にクリックします。



REST API

March 15, 2024

Citrix Endpoint Management REST API を使用すると、以下を実行できます:

- Citrix Endpoint Management コンソールに表示される呼び出しサービス
- REST クライアントを使用して、REST サービスを呼び出すことができます

API について、サービスを呼び出すために Citrix Endpoint Management コンソールにサインオンする必要はありません。

現在使用できる API の全一覧については、『Public API for REST Services』（PDF）をダウンロードしてください。

モバイルおよびデスクトップのエンドポイントデバイスを管理し、Workspace アプリの設定を構成する API を利用できます。https://developer.cloud.com/citrixworkspaceに移動し、［**Citrix Endpoint Management**］**>** ［**Mobile Application Integration**］の順に選択します。

REST API へのアクセスに必要な権限

REST API へのアクセスには、以下の権限のうち 1 つが必要です。

- Citrix Cloud 管理者
- 役割ベースのアクセス構成の一部として設定されたパブリック API アクセス権限詳しくは、「RBAC を使用した役割の構成」を参照してください。
- スーパーユーザー権限

Citrix Cloud アカウントを使用して REST API にアクセスするには、**API** キーを生成します:

1. Citrix Cloud メニューで、［**ID** およびアクセス管理］を選択します。
2. ［**API** アクセス］**>** ［セキュアクライアント］の順に選択します。
3. セキュアクライアントの名前を入力し、［クライアントの作成］をクリックします。

次に、セキュアクライアント ID とクライアントシークレットが作成されます。この情報のコピーをダウンロードし、参照用にオフラインで安全に保管してください。この情報は Citrix Cloud に保存されないため、ダイアログボックスを閉じるとアクセスできなくなります。

REST API サービスを呼び出すには

REST クライアントまたは cURL コマンドを使用して、REST API サービスを呼び出すことができます。以下の例では、Advanced REST client for Chrome を使用します。

> 注:
>
> 以下の例のホスト名とポート番号は、自分の環境に合わせて変更してください。

ログイン

ここに示す例では、Citrix Cloud API を介して取得したトークンを使用したログインについて説明します。

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

メソッドの種類: POST

コンテンツの種類: application/json

リクエストのサンプル:

```
{

 "bearerToken": "eyJ0eOiJSUzJiibGcI1AiONiJ9.
    eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"
 }

<!--NeedCopy-->
```

https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clientsCitrix Cloud API を使用してベアラートークンを取得する必要があります。詳しくは、開発者向けドキュメントを参照してください。

応答サンプル:

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
 }

<!--NeedCopy-->
```

関連情報

- Citrix Endpoint Management REST API

ActiveSync ゲートウェイ

November 29, 2023

ActiveSync は、Microsoft が開発したモバイルデータ同期プロトコルです。ActiveSync は、ハンドヘルドデバイスやデスクトップ（またはラップトップ）コンピューターとデータを同期します。

Citrix Endpoint Management で ActiveSync ゲートウェイの規則を構成できます。ActiveSync ゲートウェイは、Citrix Endpoint Management で構成されているすべてのデバイスの ActiveSync ID のリストを保持します。構成した規則に基づいて、ActiveSync ID ごとにデバイスの ActiveSync データへのアクセスを許可または拒否することができます。たとえば、［不足必須アプリ］の規則をアクティブ化した場合、Citrix Endpoint Management は必須アプリのアプリアクセスポリシーをチェックします。必須アプリが見つからない場合、ポリシーにより ActiveSync データへのアクセスが拒否されます。規則ごとに、［許可］または ［拒否］を選択できます。デフォルト設定は、［許可］です。

アプリアクセスデバイスポリシーについて詳しくは、「アプリアクセスデバイスポリシー」を参照してください。

Citrix Endpoint Management では、次の規則がサポートされます:

匿名デバイス：デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときに Citrix Endpoint Management がユーザーを再認証できない場合に使用できます。

禁止アプリ：デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。

暗示的許可および拒否：このアクションは、ActiveSync ゲートウェイのデフォルトです。その他のフィルター規則条件に合致しないすべてのデバイスの一覧が作成されます。その後、そのリストに基づいて接続が許可または拒否されます。いずれの規則にも合致しない場合、デフォルトは ［黙示的な許可］です。

非アクティブデバイス：［サーバープロパティ］で デバイスの［非アクティブな日数のしきい値］で定義された期間、非アクティブであったかを確認します。

不足必須アプリ：デバイスにアプリアクセスポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ：デバイスにアプリアクセスポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード：ユーザーパスワードが正しいかを確認します。iOS デバイスおよび Android デバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかを Citrix Endpoint Management が確認できます。たとえば、iOS では、Citrix Endpoint Management がデバイスにパスコードポリシーを送信する場合、ユーザーは 60 分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス違反かどうかを確認します。通常、このプロパティは自動化された操作により変更されるか、Citrix Endpoint Management API を利用するサードパーティにより変更されます。

失効状態：デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

ルート化された **Android** およびジェイルブレイクした **iOS** デバイス： Android または iOS デバイスがジェイルブレイクされていないかを確認します。

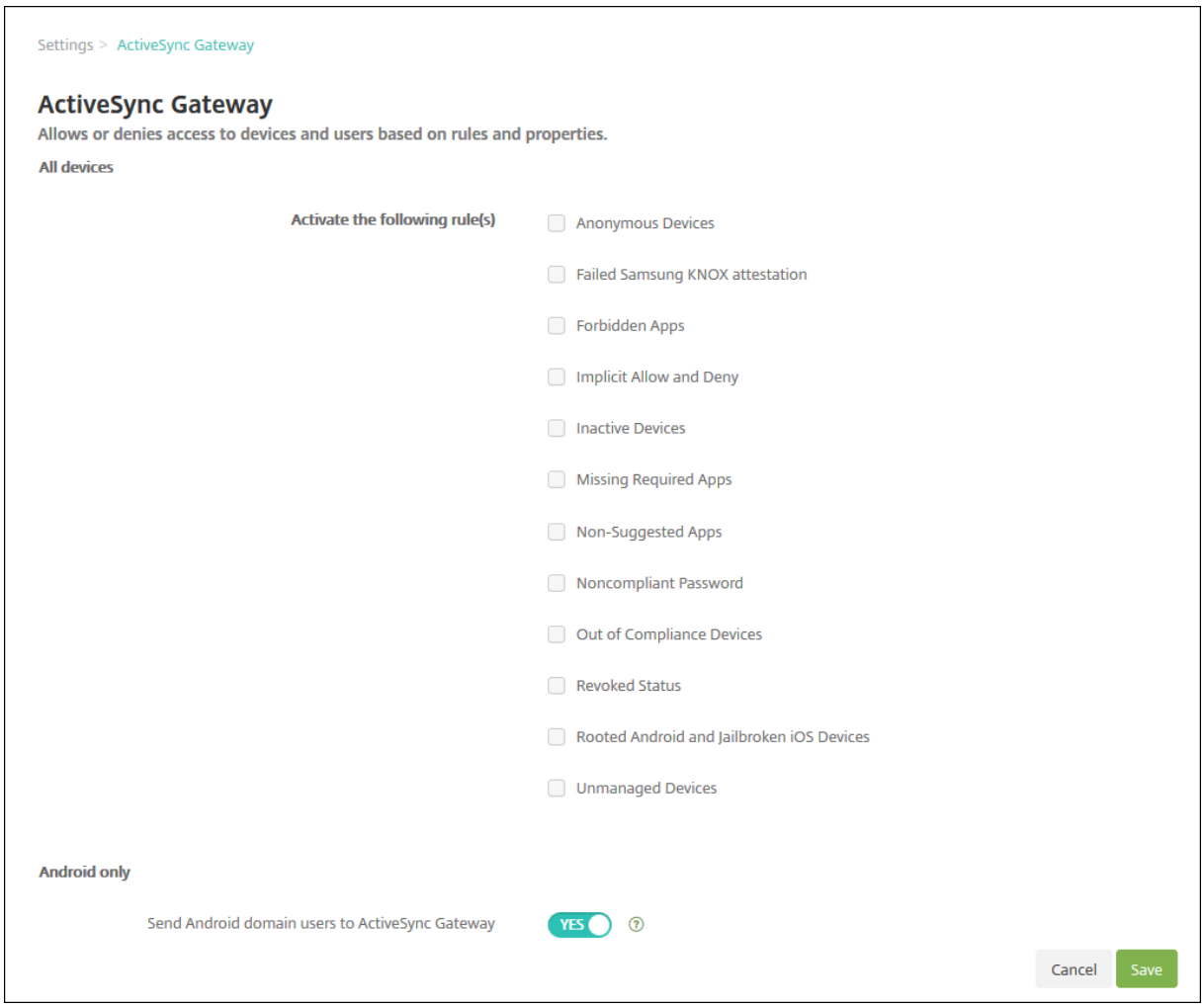
非管理デバイス：デバイスがまだ Citrix Endpoint Management の管理下にあるかを確認します。たとえば、MAM で登録されているデバイスや未登録のデバイスは管理されていません。

Android ドメインユーザーを **ActiveSync** ゲートウェイに送信： Citrix Endpoint Management によって Android デバイス所有者のユーザー名と ActiveSync ID が ActiveSync ゲートウェイに送信されるようにするには、［はい］をクリックします。レガシー構成を実行していない場合は、この機能をオフにします。最近の構成では、この機能により、デバイスに関連付けられたユーザー名がゲートウェイに存在すれば、どのデバイスでも ActiveSync データにアクセスできます。

ActiveSync ゲートウェイ設定を構成するには

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。

2. ［サーバー］の下の ［**ActiveSync** ゲートウェイ］をクリックします。［**ActiveSync** ゲートウェイ］ページが開きます。



1. ［次の規則をアクティブ化］で、有効にするルールを 1 つまたは複数オンにします。
2. ［**Android** のみ］の ［**Android** ドメインユーザーを **ActiveSync Gateway** に送信］で ［はい］をクリックし、Citrix Endpoint Management によって Android デバイスの情報が ActiveSync Gateway に送信されるようにします。
3. ［保存］をクリックします。

Citrix Endpoint Management コネクタ：**Exchange ActiveSync** 用

December 8, 2023

XenMobile Mail Manager は「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」になりました。シトリックス統合製品ラインについて詳しくは、シトリックス製品名ガイドを参照してください。

コネクタには、Citrix Endpoint Management の機能を拡張する以下の機能が備わっています：

- Exchange ActiveSync（EAS）デバイスに対するダイナミックアクセス制御。EAS デバイスの Exchange サービスに対するアクセスを自動的に許可または禁止できます。
- Exchange から提供される EAS デバイスパートナーシップ情報に Citrix Endpoint Management からアクセスできる機能。
- EAS のステータスに基づいてモバイルデバイスをワイプする Citrix Endpoint Management の機能。
- Citrix Endpoint Management から Blackberry デバイスに関する情報にアクセスできる機能、ワイプやパスワードリセットなどの制御操作を実行できる機能。

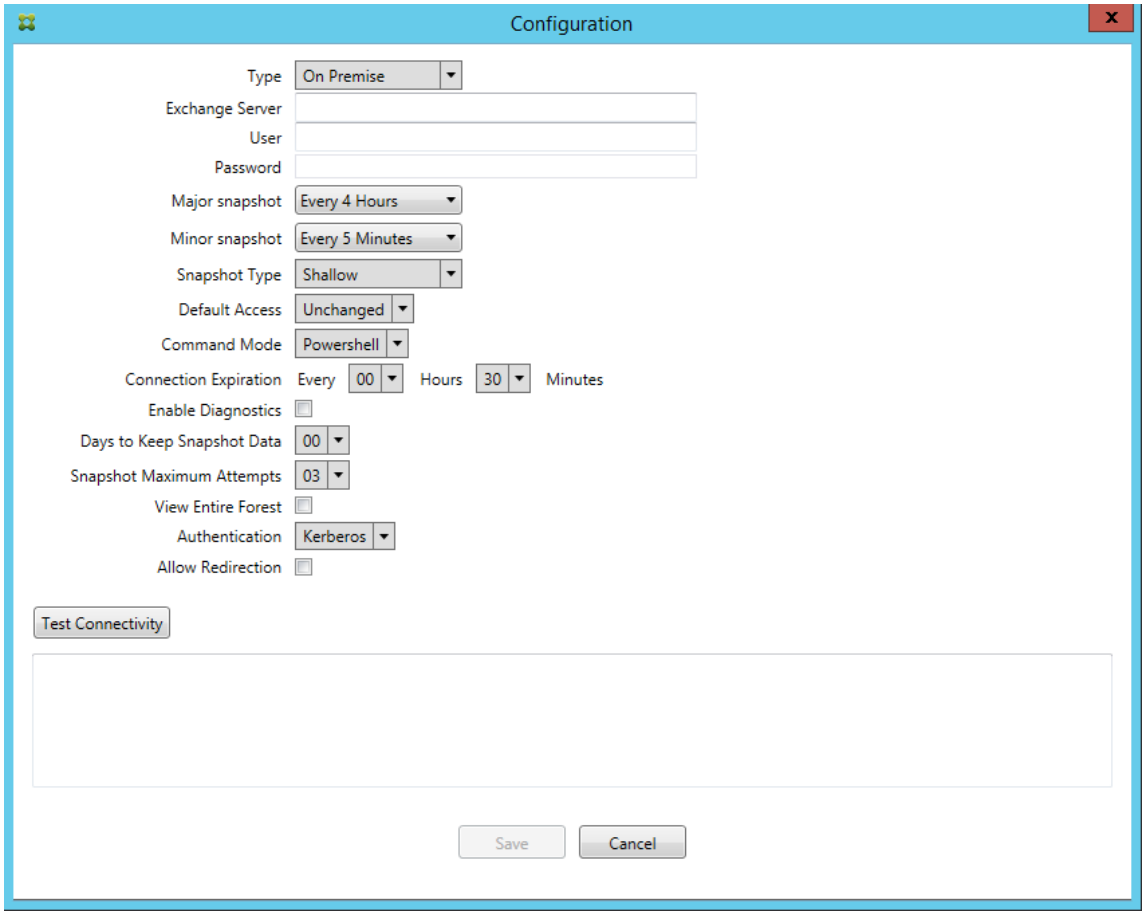
EAS のステータスに基づいてデバイスをワイプするには、ActiveSync トリガーで自動化された操作を構成します。「自動化された操作」を参照してください。

> 重要：
>
> 2022 年 10 月以降、Microsoft 社がこちらで発表した認証の変更を考慮して、Exchange ActiveSync の Citrix Endpoint Management および Citrix Gateway コネクタは、Exchange Online をサポートしなくなります。Exchange の Citrix Endpoint Management コネクタは、引き続き Microsoft Exchange Server（オンプレミス）で機能します。

バージョン **10.1.10** の新機能

バージョン 10.1.10 では、次の問題が解決されています。

- ネットワークの問題が頻繁に発生している場合、以前の 3 回の試行では、スナップショットを完了できない場合があります。このリリースでは、管理者は最大試行数（1〜10）を設定できます。この修正により、スナップショットの通信が複数回中断されても、スナップショット処理を完全に放棄する必要がなくなりました。[CXM-70837]



- 以前のバージョンでは、Exchange 構成の一覧にスナップショットの種類が表示されませんでしたが、スナップショットの種類が表示されるようになりました。[CXM-70846]
- PowerShell によって報告された PSRemotingTransport の例外は、Exchange へのセッションが実行可能ではなくなったことを示しています。この状態は、デフォルトで構成ファイルの［重大なエラー］の一覧に追加されます。これにより、PSRemotingTransportException が検出されると、この接続は後で廃棄のために［エラー］としてマークされます。次の通信で、有効な接続を使用するか、接続を作成します。[XMHELP-2184, CXM-70836]
- 構成の変更を保存すると、新しい構成を読み込む前に、以前に構成された内部コンポーネントの一部が適切に廃棄されない可能性があります。この問題により、予期しない動作が発生する可能性があります。動作は、特定の変更によって、また変更が以前の構成と競合しているかどうかによって異なります。このリリースでは、新しい構成が読み込まれる前に、すべての内部コンポーネントが破棄されます。[XMHELP-2259, CXM-71388]

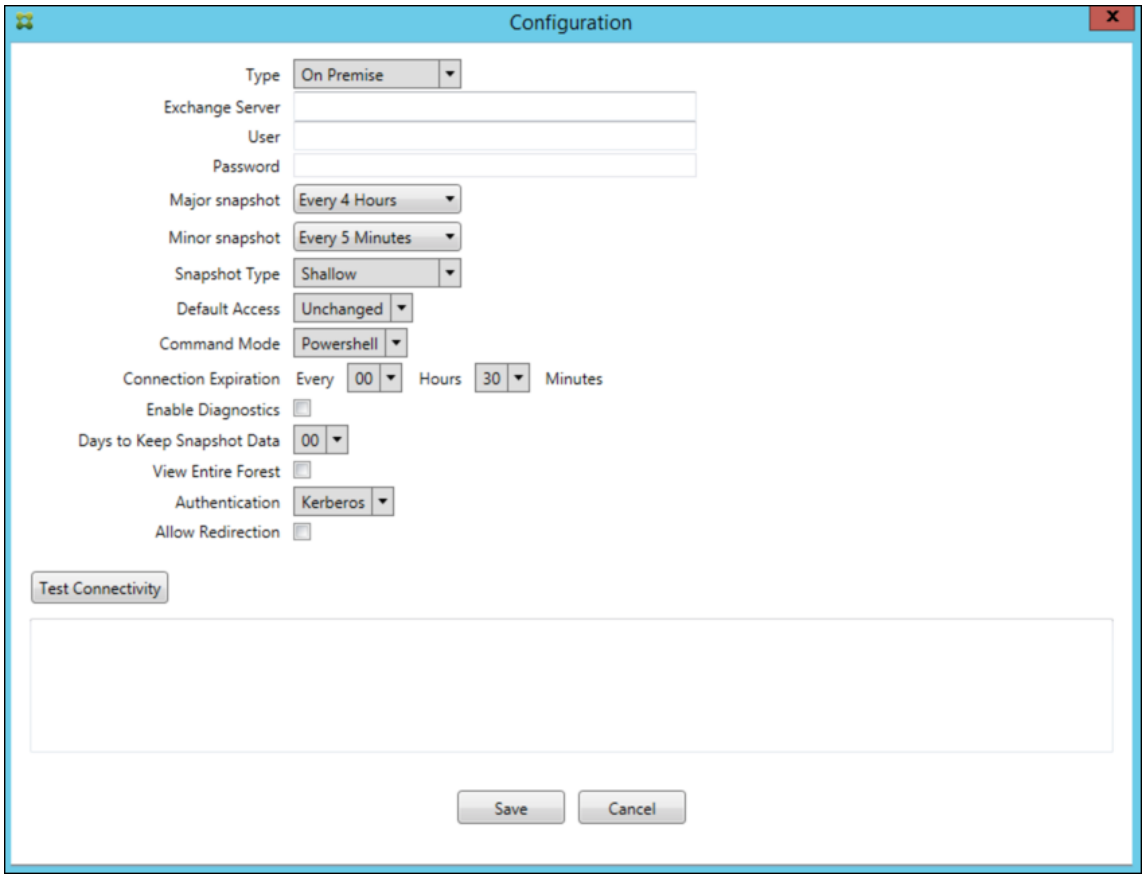
バージョン **10.1.9** の新機能

バージョン 10.1.9 では、次の問題が解決されています。

- 構成の変更は、より一貫性のある方法で処理されるようになりました。サービスが構成の変更を検出すると、各内部サブシステムが停止します。その結果、アクティブな処理またはスケジュールされた処理が中断されます。次に、新しい構成が読み込まれ、サブシステムが再起動します。つまり、すべてのスケジュールと他の内

部インフラストラクチャが新しい設定で再確立されます。これによって、バージョン 10.1.8 の既知の問題が修正されます。[CXM-47709, CXM-61330]

- アップグレード中に、既存のデータベース構成が新しい構成ファイルにマージされませんでしたが、アップグレードされた構成ファイルにデータベース構成がマージされるようになりました。[CXM-49326]
- スナップショット関連の診断ファイルで、列見出しが見つかりませんでした。この見出しは復元されます。[CXM-62680]
- 以前のバージョンからアップグレードする場合、構成ファイルのデフォルトのセクションは、使用中の構成ファイルの類似セクションによって上書きされていました。この問題により、アップグレード後にサービスによって読み込まれるデフォルトのセクションに対する追加や機能向上が無視されていました。このバージョンでは、デフォルトのセクションには常に最新の構成が反映されます。[CXM-62681]
- 管理者は、アプリケーションの実行時に Shift キーを押すことで特定のオプションにアクセスできなくなります。これらのオプションは、以前は Citrix 権限で使用できました。[Allow Redirection] などの一部のオプションは完全に使用できるようになり、[Hang Detection] や [Count Correction] などの他のオプションは廃止されました。[CXM-62767]



以前のバージョンの新機能

次のセクションでは、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用の新機能と、以前のバージョンから解決された問題の一覧を示します。

バージョン **10.1.8** の新機能

- Citrix Endpoint Management コネクタ：Exchange ActiveSync サービス用が頻繁にコマンドを発行しないように、Exchange が調整することがあります。この問題は、Office 365 への接続でよくあることです。この結果、次のコマンドの送信前にサービスが一定期間停止する必要があります。構成コンソールで、停止の残り時間が表示されるようになりました。[CXM-48044]
- 構成ファイル（config.xml）の「Watchdog」セクションや「SpecialistsDefaults」セクションが変更されても、アップグレード後の構成ファイルに変更が反映されませんでした。このリリースでは、新しい構成ファイルに変更が正しく反映されます。[CXM-52523]
- Google Analytics に送信される分析内容（特にスナップショット関連）にさらに詳細が追加されました。[CXM-56691]
- Exchange の接続性テスト機能が接続を開始しようとするのは 1 回だけです。Office 365 の接続は調整されることがあるため、調整時に接続性テストが失敗したように見えることがあります。Citrix Endpoint Management コネクタ：Exchange ActiveSync 用では、接続の開始を最大 3 回試行するようになりました。[CXM-58180]
- Exchange でポリシーを有効にするには、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用が **Set-CASMailbox** コマンドを実行して、各メールボックスですべての関連デバイスを次の 2 つの一覧に登録する必要があります：許可およびブロック。デバイスがどちらの一覧にも含まれていない場合、Exchange はデフォルトのアクセス状態にフォールバックします。このデフォルトのアクセス状態がデバイスの必要な状態とは異なる場合、デバイスはコンプライアンス違反になります。そのため、許可が必要な Exchange のデフォルトのアクセス状態がブロックである場合、ユーザーはメールにアクセスできなくなる可能性があります。または、メールへのアクセスをブロックする必要があるユーザーにアクセス権が付与される場合もあります。Citrix Endpoint Management コネクタ：Exchange ActiveSync 用によって、必要な状態を有効にしたすべてのデバイスが各 **Set-CasMailbox** コマンドに含まれるようになりました。[CXM-61251]

バージョン 10.1.8 では、次の既知の問題が確認されています。

サービスがスナップショットやポリシー評価のような長期間の操作を実行しているときに構成データを変更する構成アプリケーションで管理者が変更を加えると、サービスが不確定の状態になることがあります。その結果、ポリシーの変更が処理されない、またはスナップショットが開始されないなどの現象が発生することがあります。サービスを稼働状態に戻すには、サービスを再起動する必要があります。サービスを開始する前に、Windows サービスマネージャーでサービスプロセスの終了が必要な場合があります。[CXM-61330]

バージョン **10.1.7** の新機能

- XenMobile Mail Manager は「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」になりました。
- ［Exchange の構成］ダイアログボックスの ［パイプライン処理を無効にする］オプションは廃止されました。同じ機能を実現するには、config.xml ファイルの各コマンドに複数の手順を設定します。[CXM-54593]

バージョン 10.1.7 では、次の問題が解決されています。

- ［スナップショット履歴］ウィンドウでは、エラーメッセージにコンテキストがほとんど表示されないことがあります。エラーメッセージに、発生した場所のコンテキストが接頭辞に付くようになりました。[CXM-49157]
- XmmGoogleAnalytics .dll には、リリースに対応するファイルバージョンがありませんでした。[CXM-52518]
- 診断を改善するために、最近、メールボックスの許可/ブロック状態を設定するために使用するデバイス ID のリストの文字列形式を変更しました。ただし、デバイスが多すぎたため、仕様が最大文字列サイズを超えました。そのため内部配列データ構造を採用しました。この構造にサイズの制限はなく、データを診断の目的に適した形式にフォーマットします。[CXM-52610]
- Exchange に同期されていないデバイスポリシーが検出された場合、このデバイスポリシーのコマンドの対象には、関連するメールボックスに属していないデバイスが含まれる可能性がありました。「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」では、Exchange へのコマンドが各メールボックスに属するデバイスのみを対象とするようになりました。[CXM-54842]
- 一部の環境では、Microsoft アセンブリは使用できません。必要なアセンブリがアプリケーションとともに明示的にインストールされるようになりました。[CXM-55439]
- デバイスまたはメールボックスの識別名で、属性名と等号の間や等号の後にスペースが含まれている場合、「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」がデバイスをそのメールボックスに（またはその逆）正しく一致させないことがあります。その結果、スナップショットの調停時に一部のデバイスやメールボックスが拒否される可能性があります。[CXM-56088]

> 注：
>
> 以下の新機能セクションでは、「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」を旧称の XenMobile Mail Manager で呼びます。名前はバージョン 10.1.7 から変更されました。

バージョン **10.1.6.20** の更新点

10.1.6 に対する更新プログラムには、10.1.6.20 で追加された以下の修正が含まれています：

- Exchange に同期されていないデバイスポリシーが検出された場合、このデバイスポリシーのコマンドの対象には、関連するメールボックスに属していないデバイスが含まれる可能性がありました。XenMobile Mail Manager では、Exchange へのコマンドで各メールボックスに属するデバイスのみを対象とするようになりました。[CXM-54842]

バージョン **10.1.6** の新機能

XenMobile Mail Manager バージョン 10.1.6 では、次の問題の修正と機能の強化が行われました。

- ［スナップショット履歴］ウィンドウが時々更新されなくなることがありました。このウィンドウの更新メカニズムが改善され、更新がより確実に行われるようになりました。[CXM-47983]
- パーティション化済みのスナップショットとパーティション化されていないスナップショットに、別々のモードおよびコードパスが使用されていました。パーティション化されていないスナップショットは、単一の「*」パーティションを用いた構成でパーティション化したスナップショットと同じであったため、パーティション化なしのスナップショットモードは削除されました。デフォルトのスナップショットモードは、36 個のパーティション（0～9、A～Z）でパーティション化されたスナップショットになりました。[CXM-49093]
- ［スナップショット履歴］ウィンドウで、エラーメッセージが状態メッセージにより上書きされていました。このバージョンより、状態とエラーを同時に確認できるよう、XenMobile Mail Manager に 2 つの別々のフィールドが表示されるようになりました。[CXM-51942]
- Exchange Online（Office 365）に接続するときに、スナップショット関連のクエリによってデータセットの切り捨てが行われることがありました。この問題は、XenMobile Mail Manager で複数のコマンドをパイプラインでつないだスクリプトを実行すると発生していました。上流のコマンドから下流のコマンドへデータを渡す速度が十分ではなかったため、作業が途中で終了し、結果としてデータが不完全になっていました。このバージョンより、XenMobile Mail Manager でパイプラインそのものを再現できるようになったため、上流のコマンドが完了するまで待機してから、下流のコマンドが呼び出されるようになりました。この変更により、すべてのデータが処理され、記録されるようになります。[CXM-52280]
- Exchange に対するポリシー更新コマンドで解決不能なエラーが発生した場合、そのコマンドが長時間にわたって繰り返し作業キューへ返されていました。このため、Exchange に何度も同じコマンドが送信されていました。このバージョンの XenMobile Mail Manager では、エラーが生じたコマンドは、限られた回数だけ作業キューへ返されるようになりました。[CXM-52633]
- 特定のメールボックスのポリシー更新で全デバイスの許可またはブロックを行った場合：空のリストが **NULL** ではなく空の文字列に変換されていたため、発行した **Set-CASMailbox** コマンドが失敗していました。このバージョンより、適切なデータが送信されるようになりました。[CXM-53759]
- 新しいデバイスを処理する場合、Exchange では一定時間（通常 15 分）にわたり、「DeviceDiscovery」という状態が返されることがあります。XenMobile Mail Manager では、この状態を特に処理していませんでした。このバージョンより、XenMobile Mail Manager は、この状態を処理するようになりました。UI の［モニター］タブで、この状態にあるデバイスをフィルターできるようになりました。[CXM-53840]
- XenMobile Mail Manager では、XenMobile Mail Manager データベースへの書き込みが可能かどうかのチェックを行っていませんでした。そのため、権限に制限があると、動作を予測できない場合がありました。このバージョンより、XenMobile Mail Manager は、データベースで必要な権限を取得、検証するようになりました。XenMobile Mail Manager で、接続のテスト中（表示メッセージ）、またはメインの［構成］ウィンドウ下部のデータベースインジケーター（マウスカーソルを重ねるとメッセージを表示）に、権限が足りないことが示されるようになりました。[CXM-54219]
- 実行中のワークロードによっては、XenMobile Mail Manager サービスに命令を出してもすぐに止まらないことがありました。このため、サービスは応答なし状態のようになっていました。改善により実施中のタスク

を中断できるようになり、シャットダウンが正常に行われるようになりました。[CXM-54282]

バージョン **10.1.5** の新機能

XenMobile Mail Manager バージョン 10.1.5 では、次の問題が修正されています。

- Exchange が XenMobile Mail Manager のアクティビティを制限している場合でも、制限が行われていることがログ以外に示されていませんでした。このリリースでは、アクティブなスナップショットにマウスカーソルを重ねると、「制限中」状態が表示されるようになりました。また、XenMobile Mail Manager が制限を受けている場合、Exchange で制限が解除されるまでメジャースナップショットを開始できなくなりました。[CXM-49617]
- メジャースナップショット中に Exchange により XenMobile Mail Manager が制限されている場合：十分な時間が経過する前に、次のスナップショットが試行されることがありました。この問題により、さらに制限が行われ、スナップショットは失敗していました。このバージョンより、XenMobile Mail Manager は、各スナップショット試行の間に Exchange で指定された最小時間だけ待機するようになりました。[CXM-49618]
- 診断を有効にすると、コマンドファイルに、各プロパティ名の前にハイフンがついていない **Set-CasMailbox** コマンドが表示されていました。この問題は診断ファイルの書式内でのみ発生し、Exchange への実際のコマンドでは発生しません。ハイフンが不足しているため、コマンドを切り取って直接 PowerShell プロンプトに貼り付けて、テストや検証を行うことができませんでした。このバージョンより、ハイフンが追加されました。[CXM-52520]
- メールボックス ID の形式が「`lastname, firstname`」の場合、Exchange では、クエリのデータを返すときにコンマの前にバックスラッシュが追加されます。XenMobile Mail Manager でこの ID を使用してさらにデータのクエリを行う場合、このバックスラッシュは削除する必要があります。[CXM-52635]

既知の制限事項

> 注:
>
> バージョン 10.1.6 では次の制限が解決されています。

XenMobile Mail Manager には、Exchange に対するコマンドの失敗の原因となる可能性がある既知の問題が存在しています。ポリシーの変更を Exchange に適用する場合、XenMobile Mail Manager により **Set_CASMailbox** コマンドが発行されます。このコマンドでは、許可リストと禁止リストの 2 つのデバイスリストを取ることができます。コマンドは、メールボックスのパートナーに設定されているデバイスに適用されます。

これらの各リストの文字数は、Microsoft の API により 256 文字までに制限されています。どちらかのリストの文字数がこの制限を超えると、コマンド全体が失敗し、指定したメールボックスのデバイスにはポリシーが設定されません。エラーは次のような形で、XenMobile Mail Manager ログに表示されます。禁止リストの場合の例を次に示します。

“メッセージ：‘パラメーター ‘ActiveSyncBlockedDeviceIDs’ をターゲットにバインドできません。例外設定 “ActiveSyncBlockedDeviceIDs” :” プロパティが長すぎます。文字数の上限は 256 文字であり、指定された値の長さは…”

デバイス ID の長さはさまざまですが、通常 10 台以上のデバイスを一度に許可または禁止しようとするとこの制限を超える可能性があります。あまり行われませんが、多数のデバイスを特定のメールボックスに関連付けることは可能です。XenMobile Mail Manager が改善されこのようなシナリオに対処できるようになるまでは、ユーザーおよびメールボックスに関連付けるデバイスの数は 10 台以下に制限することをお勧めします。[CXM-52633]

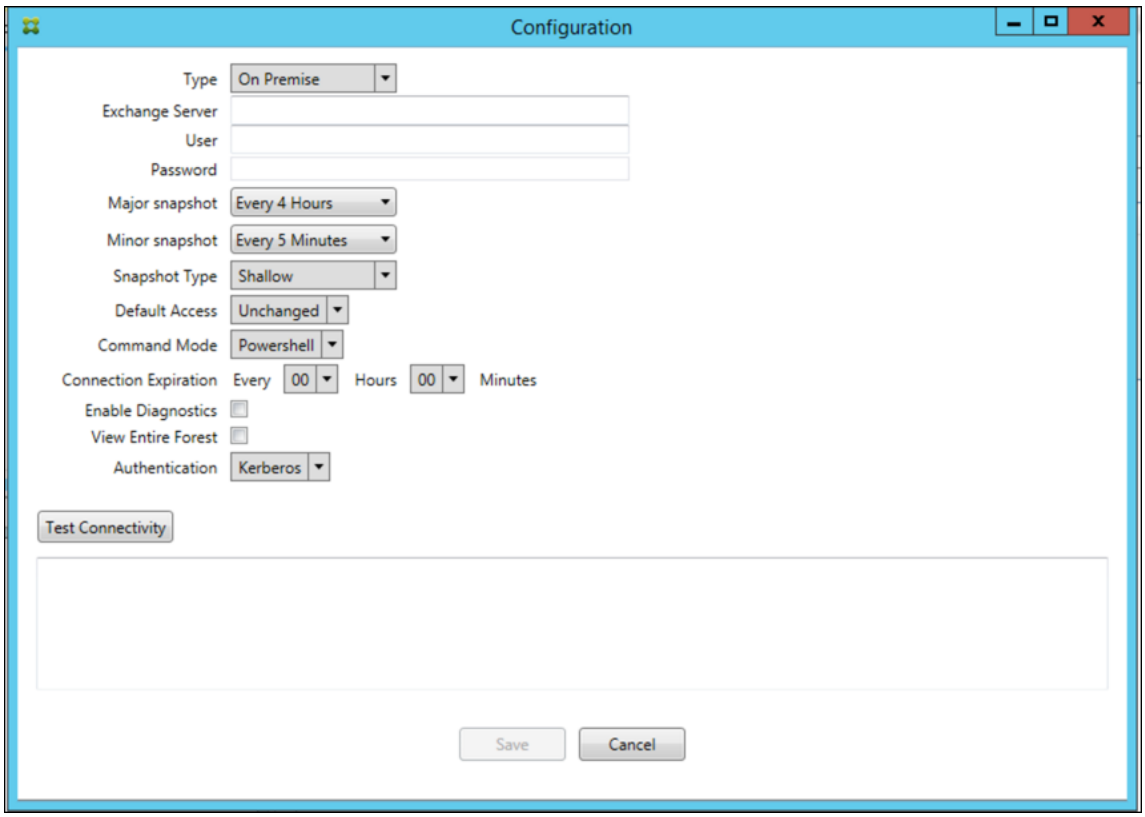
バージョン **10.1.4** の新機能

XenMobile Mail Manager バージョン 10.1.4 では、次の問題が修正されています。

- セキュリティが弱化したため、PCI 評議会は TLS 1.0 および TLS 1.1 を非推奨としました。XenMobile Mail Manager に TLS 1.2 のサポートが追加されました。[CXM-38573, CXM-32560]
- XenMobile Mail Manager に新しい診断ファイルが追加されました。Exchange の仕様で ［診断を有効にする］を選択すると、新しいスナップショット履歴ファイルが生成されます。スナップショットを試行するたびに、スナップショットの結果を含む行がファイルに追加されます。[CXM-49631]
- コマンド診断ファイルで、**Set-CASMailbox** コマンドで許可された、またはブロックされたデバイスの一覧が表示されませんでした。代わりに、関連する引数のファイルに内部クラス名が表示されていました。XenMobile Mail Manager で、deviceID の一覧がコンマ区切り一覧として表示されるようになりました。[CXM-50693]
- 不適切な仕様のために Exchange への接続の確立が失敗した場合：不適切なメッセージ「すべての接続が使用中です」でエラーメッセージが上書きされます。「すべての接続が動作不能」、「接続プールが空です」、「すべての接続が抑制されている」、「使用可能な接続がありません」などのよりわかりやすいメッセージが表示されるようになりました。[CXM-50783]
- XenMobile Mail Manager の内部キャッシュに、Allow、Block、または Wipe コマンドが複数回キューイングされることがあります。この問題により、Exchange に送信されるコマンドの遅延が発生します。XenMobile Mail Manager は、各コマンドで 1 つのインスタンスのみをキューイングするようになりました。[CXM-51524]

バージョン **10.1.3** の新機能

- **Google Analytics** のサポート：製品の改善可能な箇所に集中できるように、私たちはユーザーの皆様が XenMobile Mail Manager をどのように使用しているかについて知りたいと考えています。
- 診断を有効にするための設定：［診断を有効にする］チェックボックスが、［設定］ダイアログボックスの設定コンソールに表示されます。



Version 10.1.3 で解決された問題

- [スナップショット履歴] ウィンドウで、スナップショットの現在の状態を示すツールチップに実際の状態が反映されません。[CXM-5570]
  XenMobile Mail Manager がコマンド診断ファイルに書き込めないことがあります。これが発生すると、コマンド履歴全体が記録されません。[CXM-49217]
- 接続でエラーが発生した場合に、接続が「エラー」とマークされないことがあります。その結果、後続のコマンドが接続を使用しようとして、別のエラーを引き起こす可能性があります。[CXM-49495]
- Exchange Server からの調整が発生すると、ヘルスチェックルーチンで例外がスローされる場合があります。その結果、エラーが発生した、または期限切れになった接続が削除されないことがあります。また、XenMobile Mail Manager は調整時間の期限が切れるまで接続を作成しないことがあります。[CXM-49794].
- Exchange の最大セッション数を超えた場合に XenMobile Mail Manager から「デバイスのキャプチャに失敗した」というエラーが報告されますが、このメッセージは正確でありません。このメッセージではなく、XenMobile Mail Manager が通常 Exchange 通信に使用する 2 つのセッションが使用中であることを示すメッセージを表示する必要があります。[CXM-49994]

バージョン **10.1.2** の新機能

- **Exchange** との接続の改善: XenMobile Mail Manager は PowerShell セッションを使用して Exchange と通信します。PowerShell セッション（特に Office 365 を扱う場合）は、しばらくすると不安定になり、そ

の後のコマンドが正常に機能しなくなる可能性があります。XenMobile Mail Manager で接続の有効期限を設定できるようになりました。接続が有効期限に達すると、XenMobile Mail Manager は PowerShell セッションを即時シャットダウンしてセッションを作成します。これにより、PowerShell セッションが不安定になる可能性が低くなり、スナップショットの失敗の可能性が大幅に減少します。

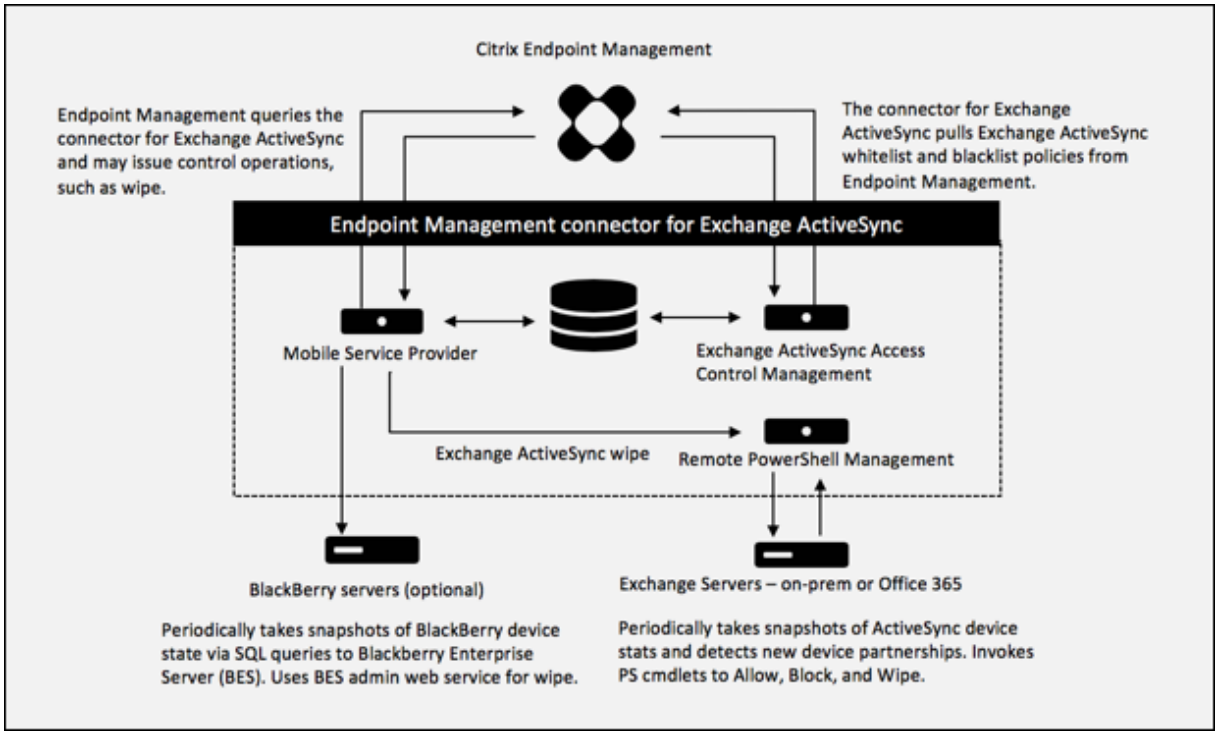
- スナップショットのワークフローの改善：大半のスナップショットは、プロセスを集中的に使用する時間のかかる操作です。スナップショット中にエラーが発生した場合に、XenMobile Mail Manager がスナップショットの完了を複数回（最大 3 回）試行するようになりました。その後の試行では最初からは開始されません。中断した場所から続行します。この機能拡張により、スナップショットの進行中に一時的なエラーが発生するのを許容することで、スナップショットの成功率が向上します。
- 診断の改善：スナップショット中に 3 つの新しい診断ファイルが生成されるようになり（オプション）、スナップショット操作のトラブルシューティングが簡単になりました。これらのファイルは、PowerShell コマンドの問題、情報が欠落しているメールボックス、およびメールボックスに関連付けできないデバイスを識別するのに役立ちます。管理者はこれらのファイルを使用して、Exchange 内の不適切なデータを識別できます。
- メモリ使用率の向上：XenMobile Mail Manager のメモリ使用効率が向上しました。管理者は、XenMobile Mail Manager を自動的に再起動し、システムにクリーンスレートが提供されるようにスケジュールできます。
- **Microsoft .NET Framework 4.6** の前提条件： Microsoft .NET Framework の前提条件バージョンがバージョン 4.6 になりました。

解決された問題

- 資格情報の要求エラー：Office 365 のセッションが不安定なために、このエラーが発生することがよくありました。Exchange への接続を改善する機能強化により、この問題に対応しています。（XMHELP-293、XMHELP-311、XMHELP-801）
- メールボックスとデバイスの数が不正確：XenMobile Mail Manager で、メールボックスとデバイスの関連付けアルゴリズムが改善されました。診断機能の改善により、XenMobile Mail Manager が責任範囲外と判断したメールボックスとデバイスを識別できるようになりました。(XMHELP-623)
- Allow、Block、Wipe コマンドが認識されない：XenMobile Mail Manager の Allow、Block、Wipe コマンドが認識されないことがあるバグが修正されました。(XMHELP-489)
- メモリ管理：メモリ管理とメモリ緩和が改善されました。(XMHELP-419)

アーキテクチャ

次の図は「Citrix Endpoint Management コネクタ：Exchange ActiveSync 用」の主要コンポーネントを示しています。詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。



次の 2 つの主要コンポーネントがあります:

- **Exchange ActiveSync** アクセス制御管理: Citrix Endpoint Management と通信して、Citrix Endpoint Management から Exchange ActiveSync ポリシーを取得します。さらに、このポリシーをローカルに定義されているポリシーと統合して、Exchange へのアクセスを許可または拒否する Exchange ActiveSync デバイスを決定します。ローカルポリシーにより、Active Directory のグループ、ユーザー、デバイスの種類、またはデバイスのユーザーエージェント（一般的にはモバイルプラットフォームのバージョン）によってアクセス制御できるように、ポリシー規則を拡張できます。
- リモート **PowerShell** 管理: リモートの PowerShell コマンドのスケジュール設定と呼び出しを処理して、Exchange ActiveSync アクセス制御管理によって作成されたポリシーを有効にします。定期的に Exchange ActiveSync データベースのスナップショットを取得し、新規の、または変更された Exchange ActiveSync デバイスを検出します。

システム要件および前提条件

Citrix Endpoint Management コネクタ: Exchange ActiveSync 用を使用するには、次の最小システム要件が必要です:

- Windows Server 2016、Windows Server 2012 R2 または Windows Server 2008 R2 Service Pack 1。英語ベースのサーバーが必要です。Windows Server 2008 R2 Service Pack 1 のサポートは 2020 年 1 月 14 日に終了し、Windows Server 2012 R2 のサポートは 2023 年 10 月 10 日に終了します。
- Microsoft SQL Server 2016 Service Pack 2、SQL Server 2014 Service Pack 3 または SQL Server 2012 Service Pack 4。

- Microsoft .NET Framework 4.6。
- Blackberry Enterprise Service バージョン 5（オプション）。

Microsoft Exchange Server のサポートされる最小バージョン：

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013（サポートは 2023 年 4 月 11 日に終了します）
- Exchange Server 2010 Service Pack 3（サポートは 2020 年 1 月 14 日に終了します）

前提条件

- Windows Management Framework がインストールされていること。
  - PowerShell V5、V4、V3
- PowerShell 実行ポリシーが Set-ExecutionPolicy RemoteSigned によって RemoteSigned に設定されていること。
- Exchange ActiveSync 用コネクタを実行しているコンピューターとリモートの Exchange Server の間で、TCP ポート 80 が開いていること。

デバイスのメールクライアント：すべてのメールクライアントが、一貫してデバイスの同じ ActiveSync ID を返すわけではありません。Exchange ActiveSync 用コネクタは、各デバイスに対して一意の ActiveSync ID を前提とするため、デバイスごとに一意の同じ ActiveSync ID を一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントは Citrix によりテスト済みで、エラーなく実行できます：

- Samsung のネイティブメールクライアント
- iOS のネイティブメールクライアント

Exchange： Exchange を実行しているオンプレミスコンピューターの要件は以下のとおりです：

Exchange の構成 UI で指定される資格情報を使用して Exchange Server に接続でき、次の Exchange 固有の PowerShell コマンドレットを実行するためのフルアクセスが付与される必要があります。

- **Exchange Server 2010 SP2** の場合：
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`

  - Get-ManagementRoleAssignment

- **Exchange Server 2013** および **Exchange Server 2016** の場合:

  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- Exchange ActiveSync 用コネクタがフォレスト全体を表示するように構成されている場合は、**Set-AdServerSettings -ViewEntireForest $true** を実行するための権限が付与されている必要があります。
- 指定された資格情報には、リモートシェルを介して、Exchange Server に接続する権限が与えられている必要があります。デフォルトでは、Exchange をインストールしたユーザーがこの権限を持ちます。
- リモート接続を確立してリモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。Set-PSSessionConfiguration を使用して管理要件を排除できますが、このコマンドの説明はこのドキュメントの範囲外です。詳しくは、Microsoft 社の記事「セッション構成について」を参照してください。
- Exchange Server は、HTTP を介してリモート PowerShell 要求をサポートするように構成されている必要があります。通常、Exchange Server で次の PowerShell コマンドを実行する管理者にとって必要なのは、WinRM QuickConfig だけです。
- Exchange には多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可される PowerShell の同時接続数が制御されます。Exchange 2010 の場合、1 人のユーザーに許可されている同時接続数のデフォルトは 18 です。接続数の上限に達すると、Exchange ActiveSync 用コネクタは Exchange Server に接続できなくなります。PowerShell の同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShell によるリモート管理に関連する、Exchange の調整ポリシーについて調べてください。

Office 365 Exchange の要件

- 権限: Exchange の構成 UI で指定される資格情報を使用して Office 365 に接続でき、次の Exchange 固有の PowerShell コマンドレットを実行するためのフルアクセスが付与される必要があります:

  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice

  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- 特権：指定された資格情報には、リモートシェルを介して、Office 365 サーバーに接続する権限が与えられている必要があります。デフォルトでは、Office 365 のオンライン管理者には、必要な権限が備えられています。
- 調整ポリシー： Exchange には多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可される PowerShell の同時接続数が制御されます。Office 365 の場合、1 人のユーザーに許可されている同時接続数のデフォルトは 3 です。接続数の上限に達すると、Exchange ActiveSync 用コネクタは Exchange Server に接続できなくなります。PowerShell の同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShell によるリモート管理に関連する、Exchange の調整ポリシーについて調べてください。

インストールと構成

1. XmmSetup.msi ファイルをクリックして、インストーラーのプロンプトに従い、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用をインストールします。
2. セットアップウィザードの最後の画面で、[**Launch the Configure utility**] をオンのままにしておきます。または、[スタート] メニューから、Exchange ActiveSync 用コネクタを開きます。
3. 次のデータベースプロパティを構成します：

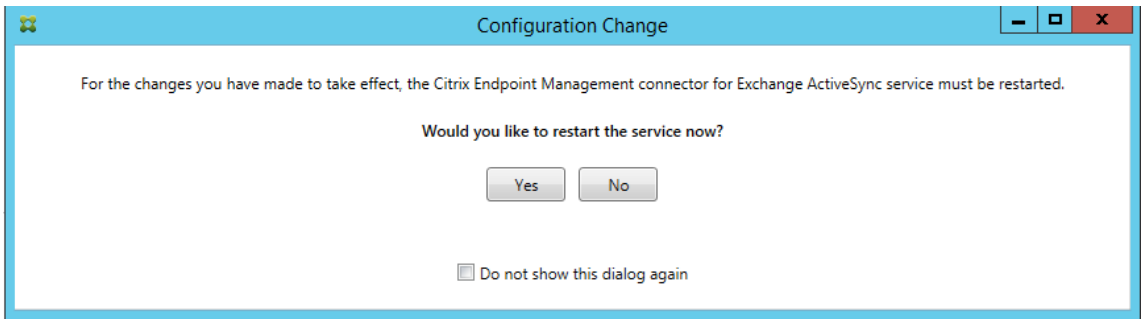
   - [**Configure**] **>** [**Database**] タブをクリックします。
   - SQL Server の名前（デフォルトは localhost）を入力します。
   - データベースはデフォルトの **CitrixXmm** のままにします。

4. SQL に使用される次のいずれかの認証モードを選択します：

   - **SQL**：有効な SQL ユーザーのユーザー名とパスワードを入力します。
   - **Windows** 統合：このオプションを選択した場合、XenMobile Mail Manager サービスのログオン資格情報を、SQL Server にアクセスするための権限を持つ Windows アカウントに変更する必要があります。これを行うには、[コントロールパネル]、[管理ツール]、[サービス] の順に選択し、XenMobile Mail Manager サービスエントリを右クリックし、[ログオン] タブをクリックします。

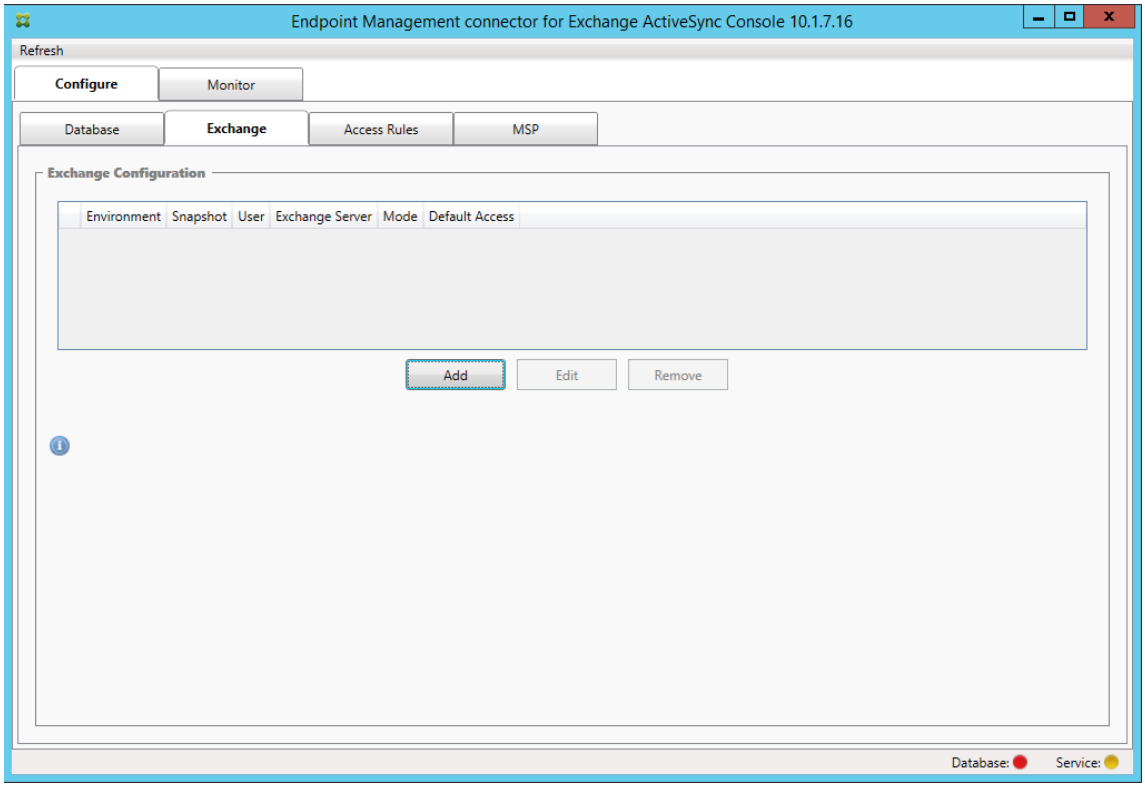
   BlackBerry データベース接続に対しても「Windows 統合」を選択している場合は、ここで指定されている Windows アカウントに BlackBerry データベースへのアクセスも付与する必要があります。

5. [**Test Connectivity**] をクリックして SQL Server に接続できることを確認し、[**Save**] をクリックします。
6. サービスの再起動を求めるメッセージが表示されます。[はい] をクリックします。



7. 1 つまたは複数の Exchange Server を構成します。

   - 単一の Exchange 環境を管理している場合は、サーバーを 1 つのみ指定します。複数の Exchange 環境を管理している場合は、Exchange 環境ごとに 1 つの Exchange Server を指定する必要があります。
   - [**Configure**] > [**Exchange**] タブをクリックし、[**Add**] をクリックします。

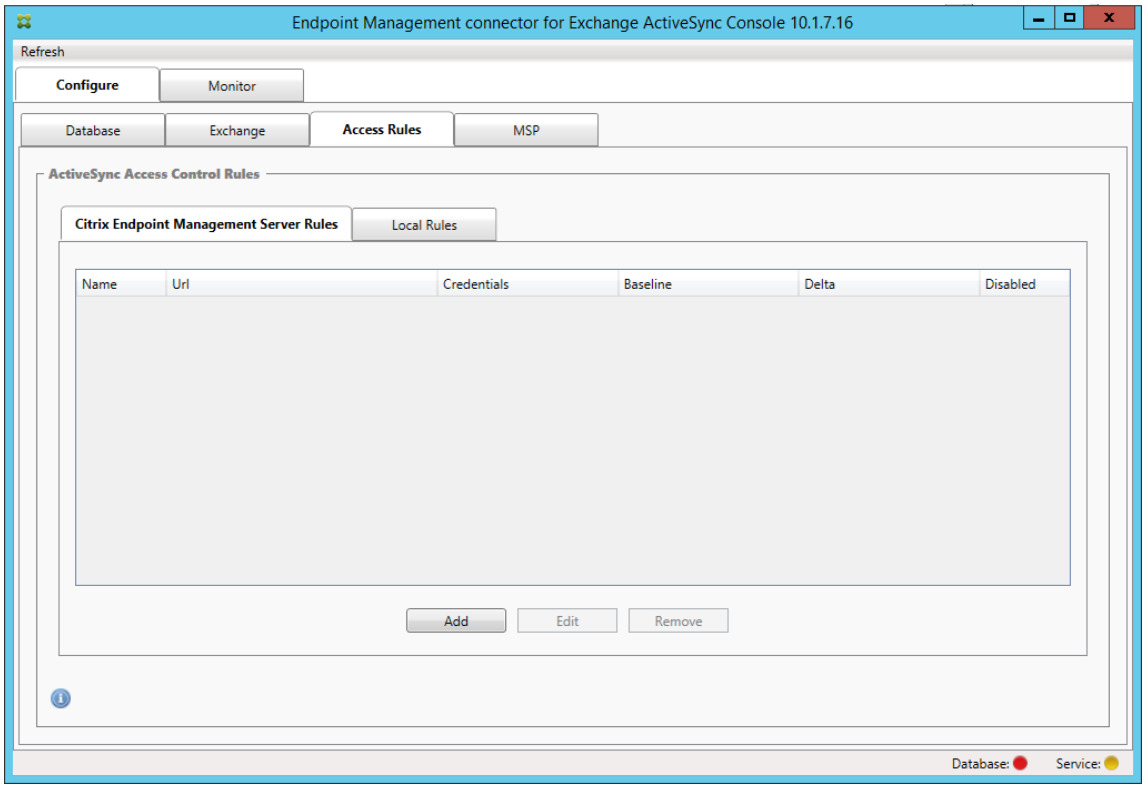


8. Exchange Server 環境の種類として [**On Premise**] または [**Office 365**] を選択します。

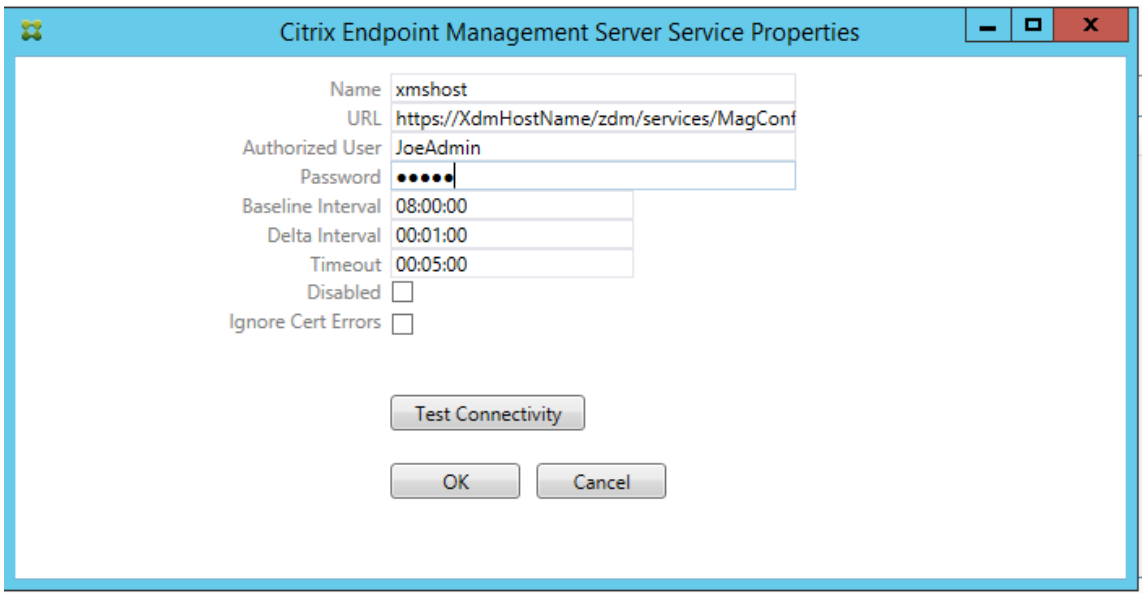
   - [**On Premise**] を選択した場合は、リモート PowerShell コマンドで使用する Exchange Server の名前を入力します。
   - 要件セクションに指定された、Exchange Server に対する適切な権限を持つ Windows ID のユーザー名を入力し、その後そのユーザーのパスワードを入力します。
   - メジャースナップショットを実行するスケジュールを選択します。メジャースナップショットにより、すべての Exchange ActiveSync パートナーシップが検出されます。

- マイナースナップショットを実行するスケジュールを選択します。マイナースナップショットにより、新しく作成された Exchange ActiveSync パートナーシップが検出されます。
- スナップショットの種類として、[**Deep**] または [**Shallow**] を選択します。通常、簡易スナップショットははるかに高速で、Exchange ActiveSync 用コネクタの Exchange ActiveSync アクセス制御機能をすべて実行するには十分です。
- [Default Access] で、[**Allow**]、[**Block**]、または [**Unchanged**] を選択します。この設定により、明示的な Citrix Endpoint Management またはローカル規則で特定されたものを除くすべてのデバイスの処理方法が制御されます。[**Allow**] を選択すると、そのようなすべてのデバイスへの ActiveSync アクセスが許可されます。[**Block**] を選択すると、アクセスは拒否されます。[**Unchanged**] を選択すると、変更は行われません。
- [ActiveSync Command Mode] で、[**PowerShell**] または [**Simulation**] を選択します。
- [**PowerShell**] モードでは、Exchange ActiveSync 用コネクタは PowerShell コマンドを発行し、必要なアクセス制御を有効にします。[Simulation] モードでは、Exchange ActiveSync 用コネクタは PowerShell コマンドを発行しませんが、想定しているコマンドと結果をデータベースに記録します。[Simulation] モードでは、PowerShell モードを有効にした場合の結果を [**Monitor**] タブを使って確認できます。
- [**Connection Expiration**] で、接続の有効期間を分単位で設定します。接続が指定された経過時間に達すると、その接続は期限切れとマークされ、接続が再度使用されることはありません。期限切れの接続が使用されなくなると、Exchange ActiveSync 用コネクタは接続を即時シャットダウンします。再接続が必要な場合は、使用可能なものがなければ、新しい接続が初期化されます。何も指定しないと、デフォルトの 30 分が使用されます。
- Exchange 環境で Active Directory フォレスト全体を表示するように Exchange ActiveSync 用コネクタを構成するには、[**View Entire Forest**] を選択します。
- 認証プロトコルとして [**Kerberos**] または [**Basic**] を選択します。Exchange ActiveSync 用コネクタは、オンプレミス展開の基本認証をサポートします。これにより、Exchange ActiveSync 用コネクタサーバーが Exchange Server が存在するドメインのメンバーでなくても、使用できるようになります。
- [**Test Connectivity**] をクリックして Exchange Server に接続できることを確認し、[**Save**] をクリックします。
- サービスの再起動を求めるメッセージが表示されます。[はい] をクリックします。

9. アクセス規則を構成します：[**Configure**] **>** [**Access Rules**] の順にタブを選択し、[**Citrix Endpoint Management Rules**] タブをクリックして、[**Add**] をクリックします。



10. [**Citrix Endpoint Management server Service Properties**] ページで、Citrix Endpoint Management サーバーを指すように URL 文字列を変更します。たとえば、インスタンス名がzdmの場合は、`https://<XdmHostName>/zdm/services/MagConfigService`と入力します。この例では、`XdmHostName`を Citrix Endpoint Management サーバーの IP アドレスまたは DNS アドレスに置き換えます。

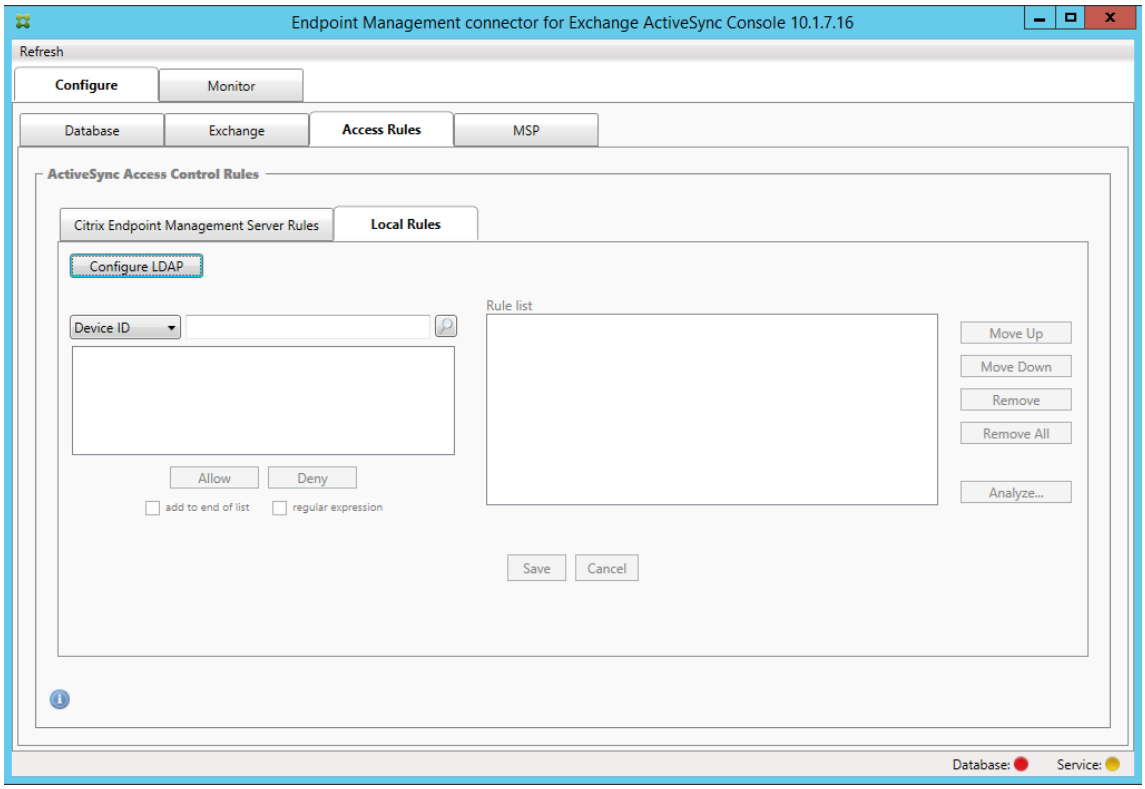


- サーバーで認証されているユーザーを入力します。

- そのユーザーのパスワードを入力します。
- [**Baseline Interval**]、[**Delta Interval**]、および [**Timeout**] の値をデフォルト値のままにします。
- [**Test Connectivity**] をクリックして、サーバーへの接続を確認し、[**OK**] をクリックします。

[**Disabled**] チェックボックスがオンの場合は、Citrix Endpoint Management Mail サービスで Citrix Endpoint Management からポリシーが収集されません。

11. [**Local Rules**] タブをクリックします。



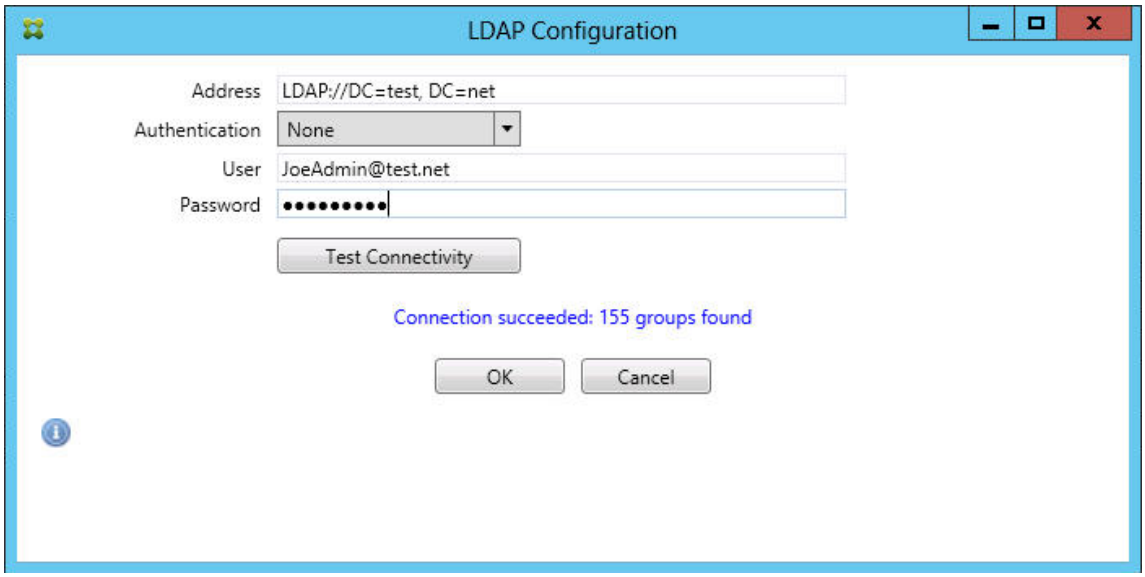
- [ActiveSync Device ID]、[Device Type]、[AD Group]、[User]、またはデバイスの [UserAgent] に基づいてローカル規則を追加できます。一覧で、適切な種類を選択します。
- テキストボックスにテキストまたはテキストフラグメントを入力します。必要に応じて、クエリボタンをクリックしてフラグメントに一致するエンティティを表示します。

[Group] 以外のすべての種類の場合、システムはスナップショットで見つかったデバイスに依存します。したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。

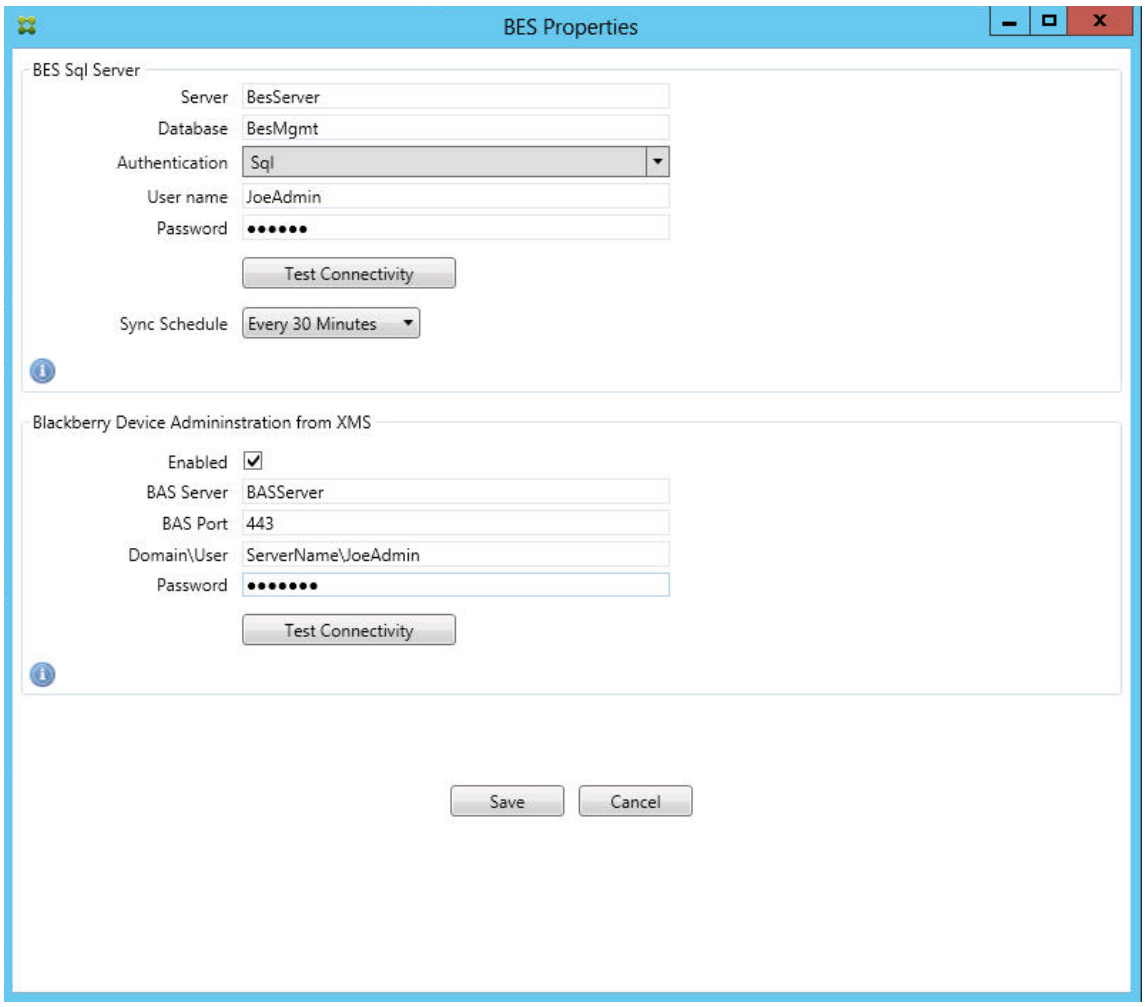
- テキスト値を選択し、[**Allow**] または [**Deny**] をクリックして右側の [**Rule List**] ペインに追加します。[**Rule List**] ペインの右側にあるボタンを使用して、規則の順序を変更したり、規則を削除したりすることができます。順序は重要です。なぜなら、指定したユーザーおよびデバイスに対して規則が表示順に評価され、上位の規則（より上部に近い規則）に一致すると以降の規則が無効になるためです。たとえば、すべての iPad デバイスを許可する規則とユーザー「Matt」をブロックする下位の規則がある場合、Matt の iPad は許可されます。この理由は、「iPad」規則の効果の優先度が「Matt」規則よりも高いからです。

- 規則一覧内の規則の分析を実行して、上書き、競合、または補足構造の可能性を検出する場合は、[**Analyze**]、[**Save**]の順にクリックします。

12. Active Directory のグループに対して使用するローカル規則を作成する場合は、[**Configure LDAP**]をクリックし、LDAP 接続プロパティを構成します。



13. 必要に応じて、BlackBerry Enterprise Server（BES）のインスタンスを 1 つ以上構成します：[**Add**]をクリックし、BES SQL Server のサーバー名を入力します



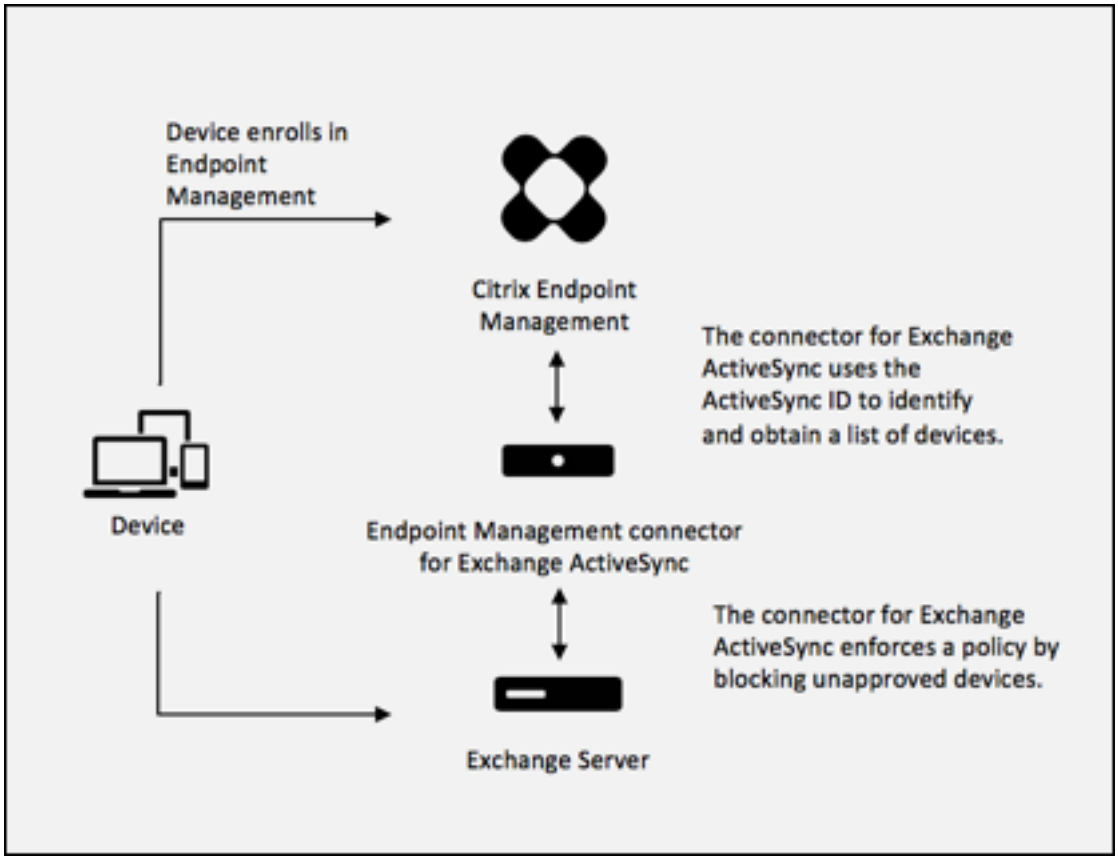
- BES 管理データベースのデータベース名を入力します。
- 認証モードを選択します。［Windows Integrated authentication］を選択する場合、Exchange ActiveSync 用コネクタサービスのユーザーアカウントが、BES SQL Server への接続に使用するアカウントになります。コネクタデータベース接続に対しても［Windows Integrated］を選択している場合は、ここで指定した Windows アカウントにコネクタデータベースへのアクセスも付与する必要があります。
- **SQL** 認証を選択する場合、ユーザー名とパスワードを入力します。
- ［**Sync Schedule**］を設定します。これは、BES SQL Server への接続とデバイス更新のチェックに使用するスケジュールです。
- ［**Test Connectivity**］をクリックして、SQL Server への接続を確認します。［Windows Integrated］を選択している場合、このテストでは、コネクタサービスのユーザーではなく、現在ログオンしているユーザーが使用されるため、SQL 認証が正確にテストされません。
- Citrix Endpoint Management からの BlackBerry デバイスのリモートワイプや ResetPassword をサポートする場合は、［**Enabled**］チェックボックスをオンにします。

- BES の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を入力します。
- 管理者 Web サービスで使用する BES ポートを入力します。
- BES サービスに必要な完全修飾ユーザー名とパスワードを入力します。
- [**Test Connectivity**] をクリックして、BES への接続をテストしてから、[**Save**] をクリックします。

ActiveSync ID によるメールポリシーの適用

企業のメールポリシーによっては、特定のデバイスで企業メールを使用することが認められない場合があります。このポリシーに従うには、そのようなデバイスから従業員が企業メールにアクセスできないようにする必要があります。このようなメールポリシーを適用させるために、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用および Citrix Endpoint Management が連携して機能します。Citrix Endpoint Management は、企業のメールアクセスポリシーを設定します。承認されていないデバイスを Citrix Endpoint Management に登録すると、Exchange ActiveSync 用コネクタがポリシーを適用します。

デバイス上のメールクライアントはデバイス ID を使用して Exchange Server（または Office 365）にクライアントの存在を通知します。この ID は ActiveSync ID としても知られており、デバイスを識別するために使用されます。Citrix Secure Hub では同様の識別子を取得し、デバイスが登録されると Citrix Endpoint Management にこの識別子を送信します。Exchange ActiveSync 用コネクタで 2 つのデバイス ID を比較することによって、特定のデバイスに企業メールへのアクセスを許可するかどうかが判定されます。次の図は、この概念を示しています：



デバイスが Exchange に公開した ID と異なる ActiveSync ID が Citrix Endpoint Management から Exchange ActiveSync 用コネクタに送信されると、コネクタから Exchange に対してそのデバイスに対する処理を指示できません。

ほとんどのプラットフォームで、ActiveSync ID は確実に一致します。ただし、一部の Android の実装で、デバイスが送信する ActiveSync ID とメールクライアントが Exchange に通知する ID が異なることが Citrix で判明しています。この問題を緩和するため、次のことを実行できます。

- すべての Android プラットフォームで、Citrix Secure Mail の使用をお勧めします。

企業のメールアクセスポリシーの適切な適用を保証するために、セキュリティについて防御的なスタンスをとることができます。静的ポリシーをデフォルトで ［拒否］に設定することで、Exchange ActiveSync 用 Citrix Endpoint Management コネクタでメールを禁止するように構成します。これは、従業員が Android デバイスで別のメールクライアントを構成し、ActiveSync ID 検出が機能しない場合、企業のメールが従業員へのアクセスを拒否することを意味します。

アクセス制御規則

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用では、Exchange ActiveSync デバイスのアクセス制御を動的に構成するための、規則に基づく手法が提供されます。コネクタのアクセス制御規則は、一致式と目的のアクセス状態（許可またはブロック）の 2 つで構成されます。特定の Exchange ActiveSync デバイスに対して規則を評価して、その規則がデバイスに適用されるかどうか、またはデバイスと一致するかどうかを判別できます。一致式にはいくつかの種類があります。たとえば、規則は、特定のデバイスの種類のすべてのデバイス、特定の Exchange ActiveSync デバイス ID、特定のユーザーのすべてのデバイスと一致するなどの条件を指定できます。

規則一覧の規則を追加、削除、および並べ替えているときに ［**Cancel**］をクリックすると、規則一覧が最初に開いたときの状態に戻ります。［**Save**］をクリックしない限り、構成ツールを閉じるとこのウィンドウに対して加えた変更が失われます。

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用には、ローカル規則、Citrix Endpoint Management サーバー規則（XDM 規則とも呼ばれます）、およびデフォルトのアクセス規則の 3 種類の規則があります。

ローカル規則：ローカル規則が最も優先されます：デバイスがローカル規則と一致すると、規則の評価は停止します。Citrix Endpoint Management サーバー規則とデフォルトのアクセス規則は参照されません。ローカル規則は、［**Configure**］**>** ［**Access Rules**］**>** ［**Local Rules**］タブから、Exchange ActiveSync 用コネクタに対してローカルに構成します。サポート一致は、特定の Active Directory グループ内のユーザーのメンバーシップに基づきます。サポート一致は、次のフィールドの正規表現に基づいています：

- Active Sync デバイス ID
- ActiveSync デバイスの種類
- ユーザー プリンシパル名 (UPN)
- ActiveSync ユーザーエージェント（通常、デバイスプラットフォームまたはメールクライアント）

メジャースナップショットが完了し、デバイスが検出されている限り、通常の規則または正規表現の規則のいずれかを追加できます。メジャースナップショットが完了していない場合、正規表現の規則のみを追加できます。

Citrix Endpoint Management サーバー規則：管理対象デバイスに関する規則を提供する外部 Citrix Endpoint Management サーバーへの参照です。Citrix Endpoint Management サーバーには、デバイスがジェイルブレイク済みかどうかや、デバイスに禁止アプリが含まれているかどうかなど、Citrix Endpoint Management が認識しているプロパティに基づいてデバイスが許可するかブロックするかを特定する独自の高レベルの規則を構成できます。Citrix Endpoint Management では、高レベルの規則が評価され、許可またはブロックする一連の ActiveSync デバイス ID が生成されて、これらが XenMobile Mail Manager に配信されます。

デフォルトのアクセス規則：デフォルトのアクセス規則は、すべてのデバイスと一致する可能性があり、常に最後に評価されるという点で独特です。この規則は、あらゆる状況に対応できる規則です。つまり、特定のデバイスがローカル規則と Citrix Endpoint Management サーバー規則のいずれにも一致しない場合は、デフォルトのアクセス規則での目的のアクセス状態によってデバイスにおける目的のアクセス状態が決まります。

- デフォルトのアクセス–許可：ローカル規則と Citrix Endpoint Management サーバー規則のいずれにも一致しないすべてのデバイスが許可されます。
- デフォルトのアクセス–ブロック：ローカル規則と Citrix Endpoint Management サーバー規則のいずれにも一致しないすべてのデバイスがブロックされます。
- デフォルトのアクセス–変更なし：ローカル規則と Citrix Endpoint Management サーバー規則のいずれにも一致しないすべてのデバイスのアクセス状態は、Exchange ActiveSync 用コネクタによって変更されません。Exchange によってデバイスが Quarantine モードになっている場合、アクションは実行されません。たとえば、Quarantine モードからデバイスを削除する方法は、ローカル規則または XDM 規則で隔離を明示的に上書きすることのみです。

規則の評価について

Exchange から Exchange ActiveSync 用コネクタに報告されるデバイスごとに、次のように優先度の高い順に規則が評価されます。

- ローカル規則
- Citrix Endpoint Management サーバー規則
- デフォルトのアクセス規則

一致が検出されると、評価は停止します。たとえば、ローカル規則が特定のデバイスと一致すると、そのデバイスは Citrix Endpoint Management サーバー規則またはデフォルトのアクセス規則に対して評価されません。このことは、特定の種類の規則内でも当てはまります。たとえば、ローカル規則一覧で、特定のデバイスに対して複数の一致がある場合、最初の一致が見つかるとすぐに評価は停止します。

デバイスプロパティが変更されたとき、デバイスが追加または削除されたとき、または規則自体が変更されたときは、現在定義されている一連の規則が Exchange ActiveSync 用コネクタによって再評価されます。メジャースナップショットにより、構成可能な間隔でデバイスのプロパティ変更または削除が確認されます。マイナースナップショットにより、構成可能な間隔で新しいデバイスが確認されます。

Exchange ActiveSync にも、アクセスを管理する規則があります。これらの規則が Exchange ActiveSync 用コネクタでどのように機能するかを理解することが重要です。Exchange は、個人の適用除外、デバイスの規則、組織の設定という 3 つのレベルの規則で構成できます。Exchange ActiveSync 用コネクタでは、リモート PowerShell 要求をプログラムで発行して個人の適用除外一覧に反映させることで、アクセス制御を自動化します。これらは、特定のメールボックスに関連する、許可またはブロックする Exchange ActiveSync デバイス ID の一覧です。展開すると、Exchange ActiveSync 用コネクタは Exchange 内の適用除外一覧の管理機能を効果的に引き継ぎます。Microsoft 社の記事「デバイスとデバイスの Exchange 管理構成マネージャー」を参照してください。

分析は、同じフィールドに対して複数の規則が定義されている場合に特に便利です。規則間の関係をトラブルシューティングできます。規則フィールドの観点から分析を実行します。たとえば、ActiveSync デバイス ID、ActiveSync デバイスの種類、ユーザー、ユーザーエージェントなどの照合されるフィールドに基づくグループで規則が分析されます。

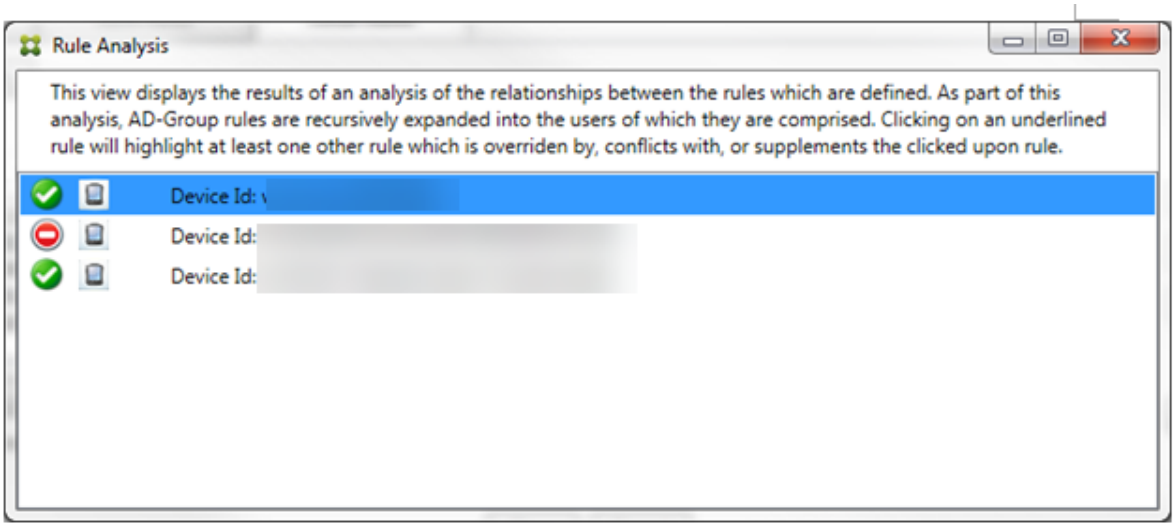
規則の用語

- 上書き規則：同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- 競合規則：同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- 補足規則：正規表現の規則が複数あるので、2 つ（またはそれ以上）の正規表現を 1 つの正規表現の規則に結合できるか、またはそれらの機能が重複していないようにする必要がある場合に補足が発生します。補足規則もアクセス（許可/ブロック）で競合する場合があります。
- プライマリ規則：プライマリ規則は、ダイアログボックス内でクリックされた規則です。この規則は、実線の罫線で囲まれて示されます。この規則には、上方向または下方向を指す 1 つまたは 2 つの緑色の矢印も示されます。矢印が上方向を指している場合は、プライマリ規則よりも優先される補助規則があることを示しています。矢印が下方向を指している場合は、プライマリ規則よりも優先度の低い補助規則があることを示しています。アクティブにできるプライマリ規則は、常に 1 つのみです。
- 補助規則：補助規則は、上書き、競合、または補足の関係のいずれかで、プライマリ規則と何らかの関係を持ちます。この規則は、破線の罫線で囲まれて示されます。各プライマリ規則に対して、1 つまたは複数の補助規則を指定できます。下線付きのエントリをクリックしたときに強調表示される補助規則は、常にプライマリ規則の観点から示されます。たとえば、補助規則がプライマリ規則によって上書きされたり、プライマリ規則とアクセスで競合したり、プライマリ規則を補足したりします。

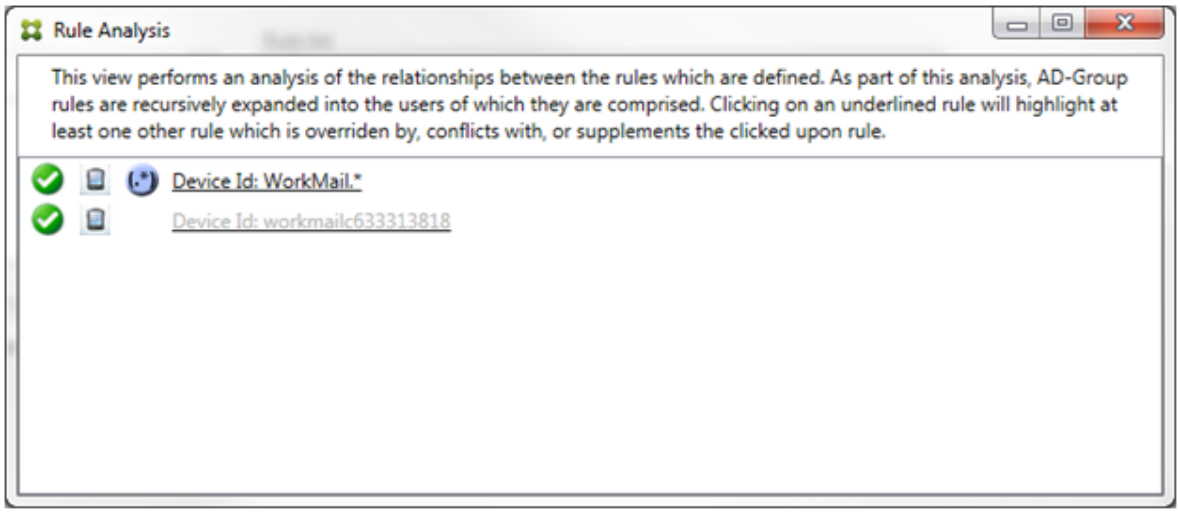
［**Rule Analysis**］ダイアログボックスに表示する規則の種類の外観

競合、上書き、または補足がない場合、［Rule Analysis］ダイアログボックスに下線付きのエントリは表示されません。どのアイテムをクリックしても影響はありません。通常の選択済みアイテムの表示になります。

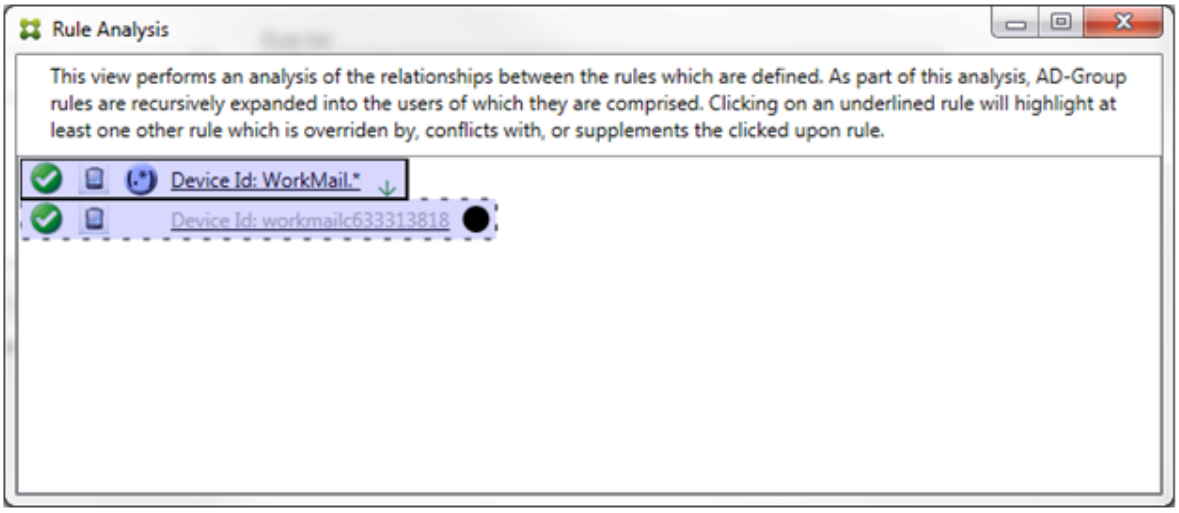
[Rule Analysis] ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。



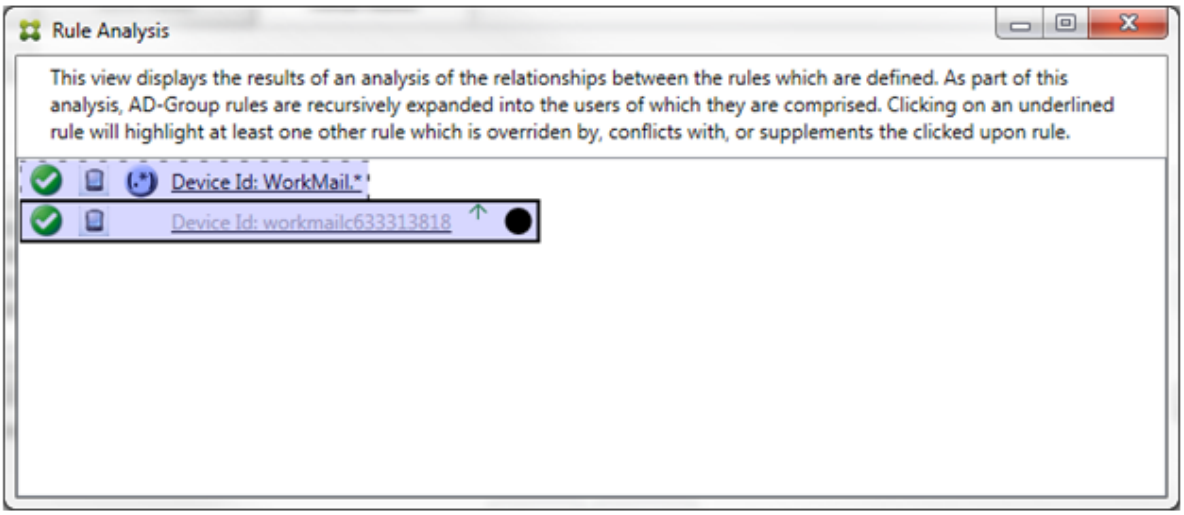
上書きが発生した場合、2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。1 つ以上の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。上書きされた規則をクリックして、その規則を上書きした規則を確認できます。規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます：



最も優先度の高い規則をクリックすると、ダイアログボックスの表示は次のようになります：

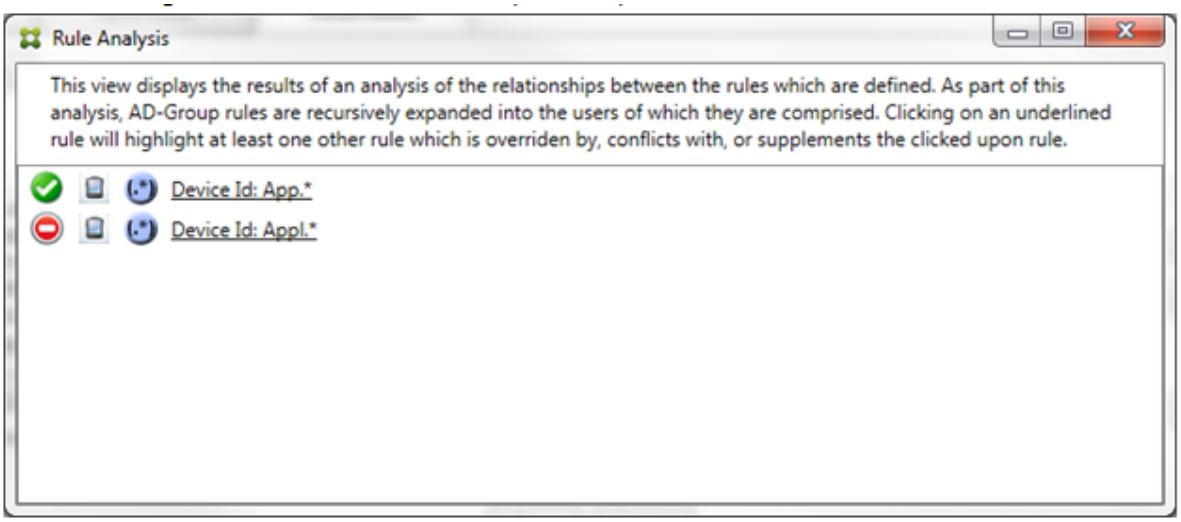


この例では、正規表現の規則`WorkMail.*`がプライマリ規則（実線の罫線で表示）で、通常の規則`workmailc633313818`が補助規則（破線の罫線で表示）です。補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります：

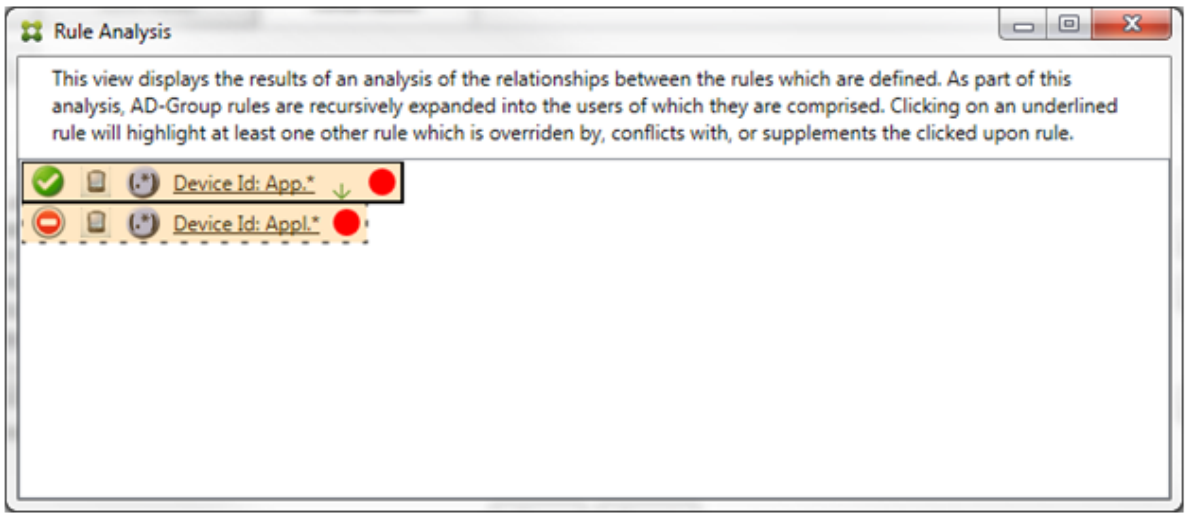


上記の例では、正規表現の規則`WorkMail.*`が補助規則（破線の罫線で表示）で、通常の規則`workmailc633313818`がプライマリ規則（実線の罫線で表示）です。このシンプルな例では、大きな違いはありません。より複雑な例については、このトピックで後述する複雑な式の例を参照してください。多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

競合が発生した場合、2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。競合している規則は赤色の点で示されます。相互に競合のみが発生している規則は、2 つ以上の正規表現の規則が定義されている場合に限り発生します。ほかのすべての競合のシナリオでは、競合のみではなく、上書きも発生します。シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます：

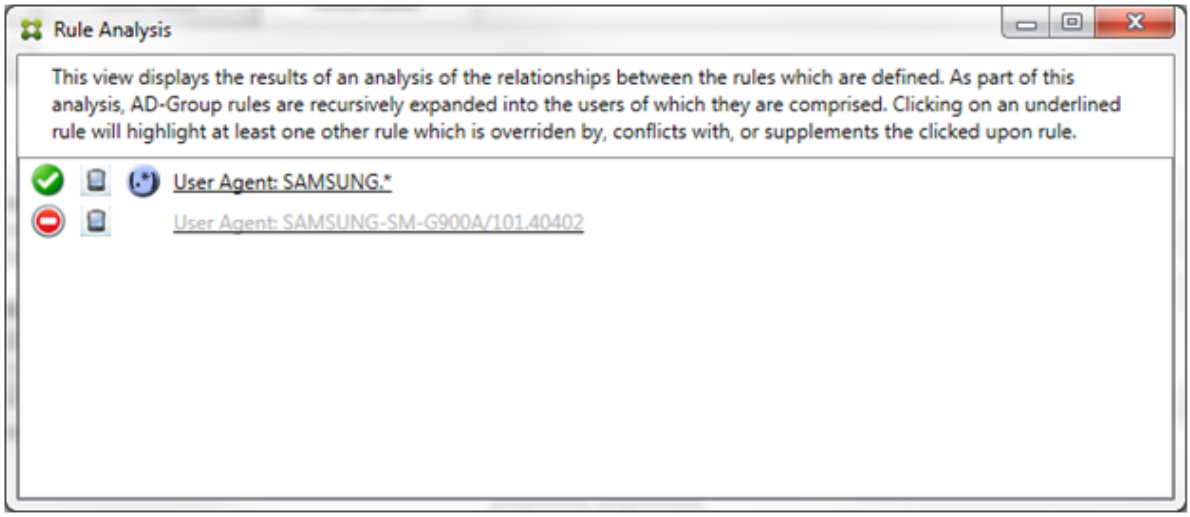


2 つの正規表現の規則を確認すると、最初の規則で「App」がデバイス ID に含まれるすべてのデバイスを許可し、2 つ目の規則で「`Appl`」がデバイス ID に含まれるすべてのデバイスを拒否することがわかります。さらに、2 つ目の規則で「`Appl`」がデバイス ID に含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは決して拒否されません。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります:



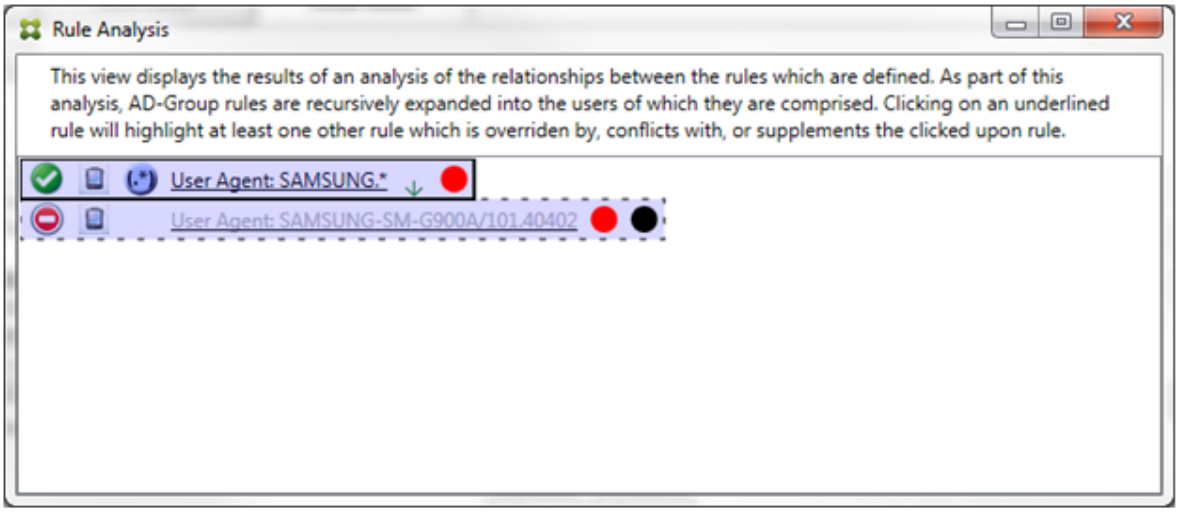
前述のシナリオでは、プライマリ規則（正規表現の規則`App.*`）と補助規則（正規表現の規則`Appl.*`）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

競合と上書きの両方を含むシナリオでは、プライマリ規則（正規表現の規則`App.*`）と補助規則（正規表現の規則`Appl.*`）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。



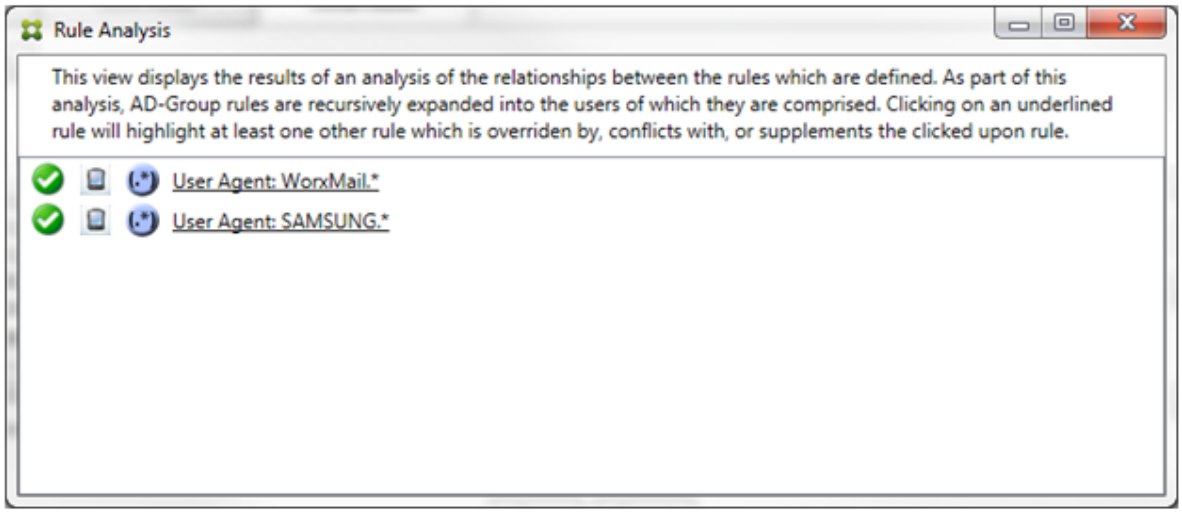
上記の例では、最初の規則（正規表現の規則SAMSUNG.*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2 つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。2 つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

正規表現の規則をクリックすると、ダイアログボックスの表示は次のようになります:

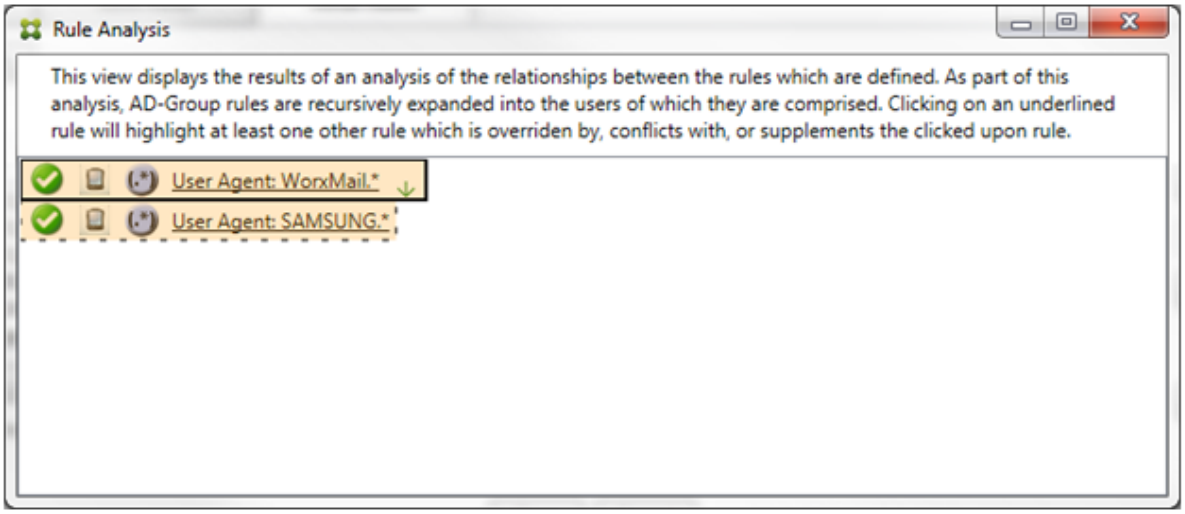


プライマリ規則（正規表現の規則SAMSUNG.*）の末尾には赤色の点が付けられて、アクセス状態が 1 つまたは複数の補助規則と競合していることが示されます。補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には赤色の点が付けられて、アクセス状態がプライマリ規則と競合していることが示されます。この規則の末尾には黒色の点が付けられて、上書きされたために非アクティブであることが示されます。

2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。相互に補足のみが発生している規則には、正規表現の規則のみが定義されています。相互に補足が発生している規則は、黄色のオーバーレイで示されます。シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます:



目視で確認すると、両方の規則が正規表現の規則で、両方とも Citrix Endpoint Management コネクタ: Exchange ActiveSync 用の［ActiveSync device ID］フィールドに適用されていることが容易にわかります。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります:

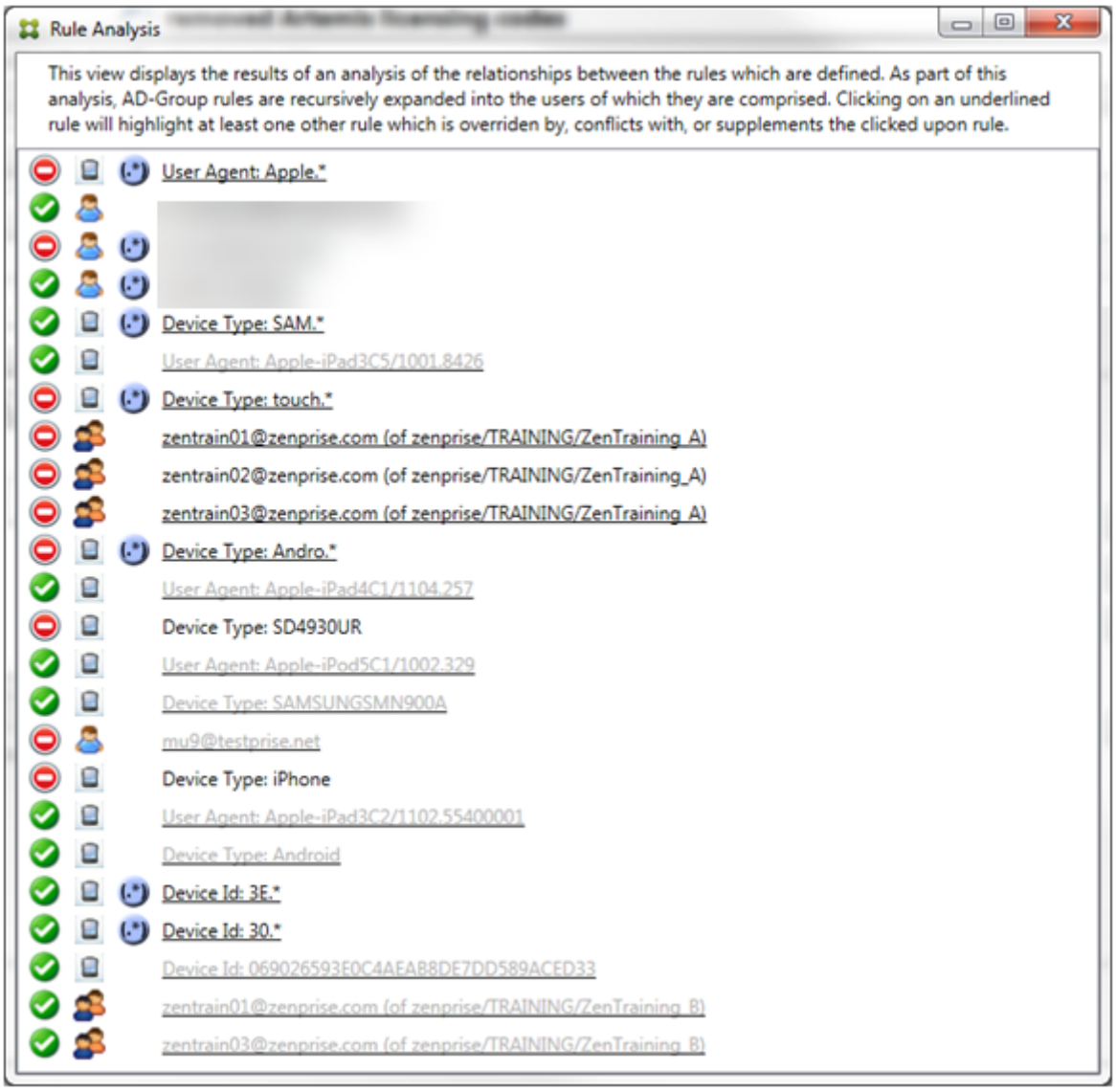


プライマリ規則（正規表現の規則`WorkMail.*`）が黄色のオーバーレイで強調表示され、正規表現の補助規則がほかに 1 つ以上存在することが示されます。補助規則（正規表現の規則`SAMSUNG.*`）が黄色のオーバーレイで強調表示され、この規則とプライマリ規則の両方が、Exchange ActiveSync 用コネクタ内の同じフィールドに適用されている正規表現の規則であることが示されます。この場合、そのフィールドは ActiveSync デバイス ID です。正規表現は重複する場合としない場合があります。正規表現が適切に作成されているかどうかの判断は、ユーザーに委ねられます。

複雑な式の例

発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。次の

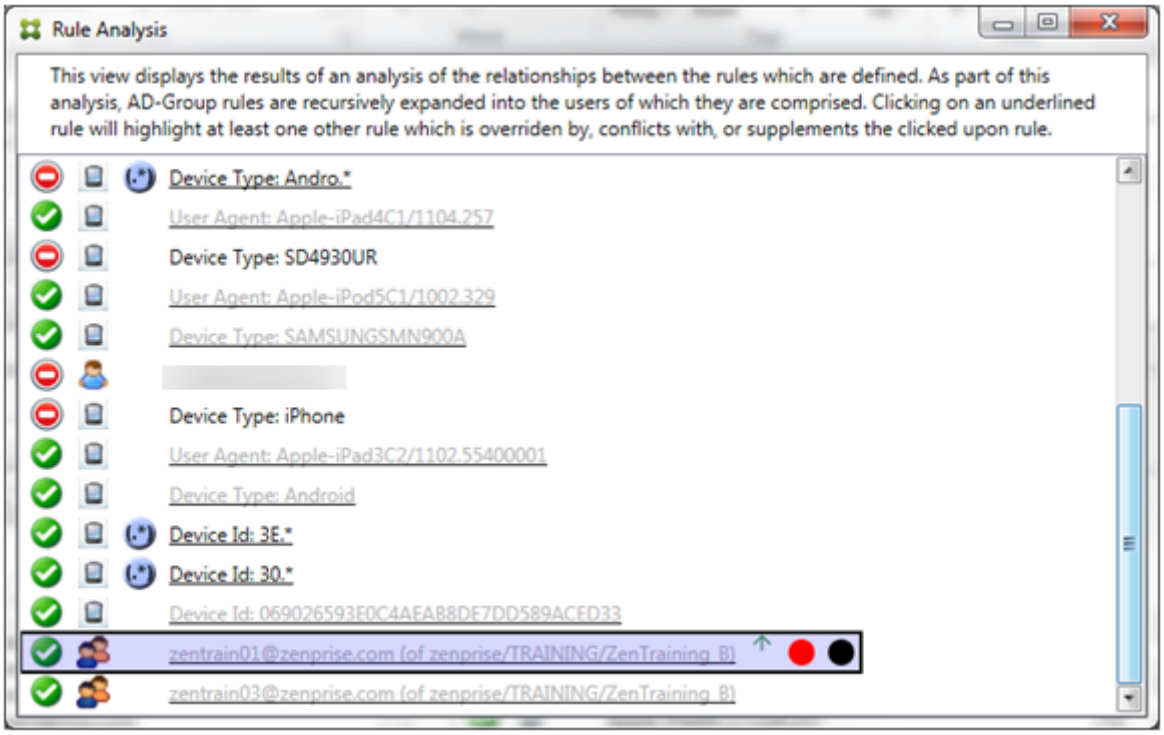
図では、ほとんどのアイテムに下線が付けられています。多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。同様に、  アイコンで示される多数の正規表現の規則も一覧に含まれています。



上書きの分析方法

特定の規則を上書きした規則を確認するには、その規則をクリックします。

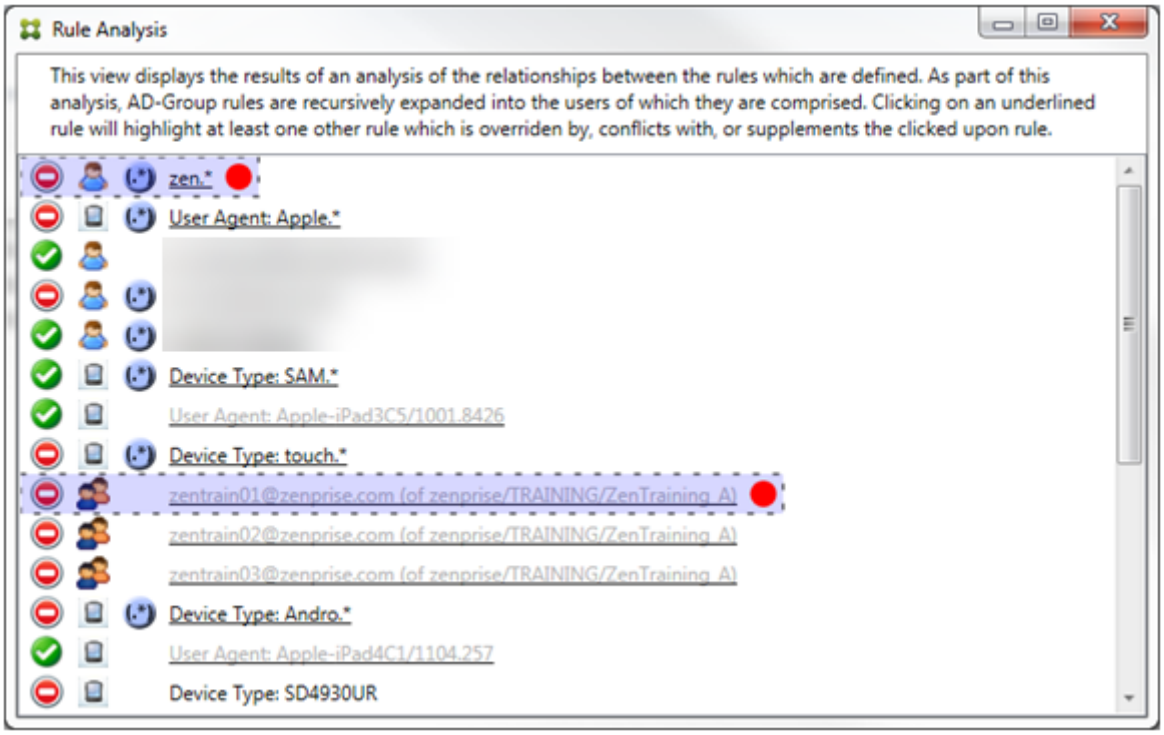
例 **1**: この例では、`zentrain01@zenprise.com`が上書きされた理由を調べます。



プライマリ規則（zentrain01@zenprise.comがメンバーとして属する AD グループ規則zenprise/TRAINING/ZenTraining B）には、次の特性があります：

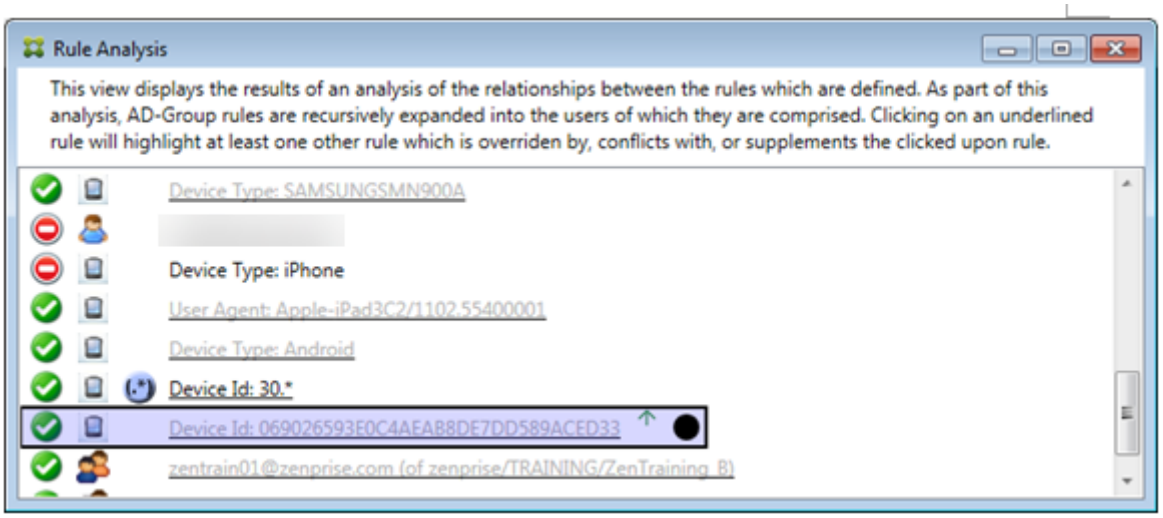
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（すべての補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、1 つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます：



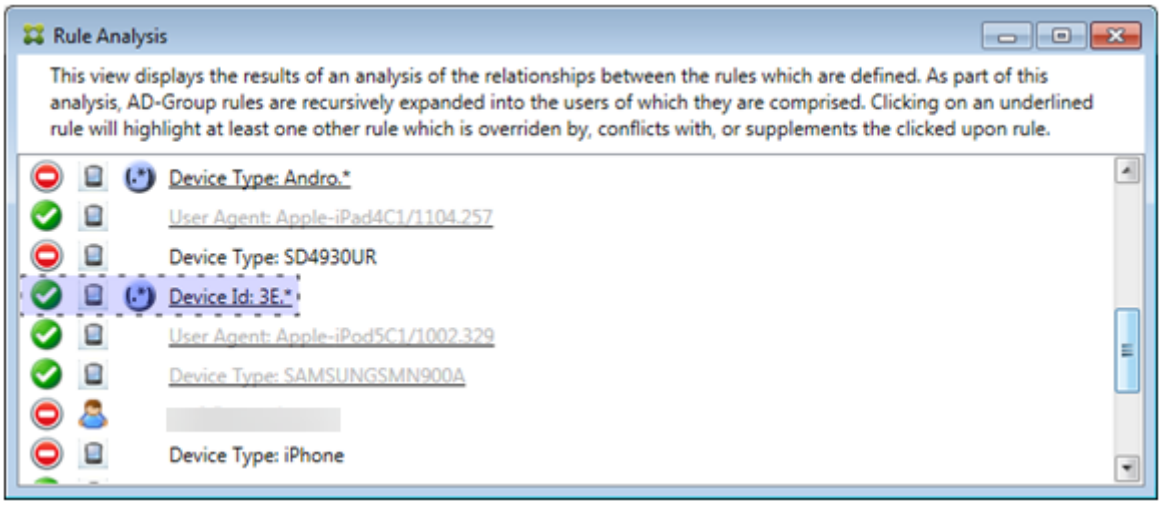
この場合、プライマリ規則を上書きする 2 つの補助規則があります: 正規表現の規則`zen.*`と通常の規則`zentrain01@zenprise.com`（`zenprise/TRAINING/ZenTraining A`の規則）です。後者の補助規則の場合、Active Directory グループ規則`ZenTraining A`にユーザー`zentrain01@zenprise.com`が含まれる一方、Active Directory グループ規則`ZenTraining B`にもユーザー`zentrain01@zenprise.com`が含まれることになります。ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、プライマリ規則は上書きされています。プライマリ規則のアクセスが許可で、両方の補助規則のアクセスがブロックであるので、これらすべての末尾に赤色の点が付けられて、アクセスが競合していることも示されています。

例 **2**: 次の例は、ActiveSync デバイス ID が`069026593E0C4AEAB8DE7DD589ACED33`であるデバイスが上書きされた理由を示しています:



このプライマリ規則（通常のデバイス ID の規則`069026593E0C4AEAB8DE7DD589ACED33`）には、次の特性があります：

- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、補助規則がそのプライマリ規則を上書きして、非アクティブであることを示す黒色の円が付けられている。

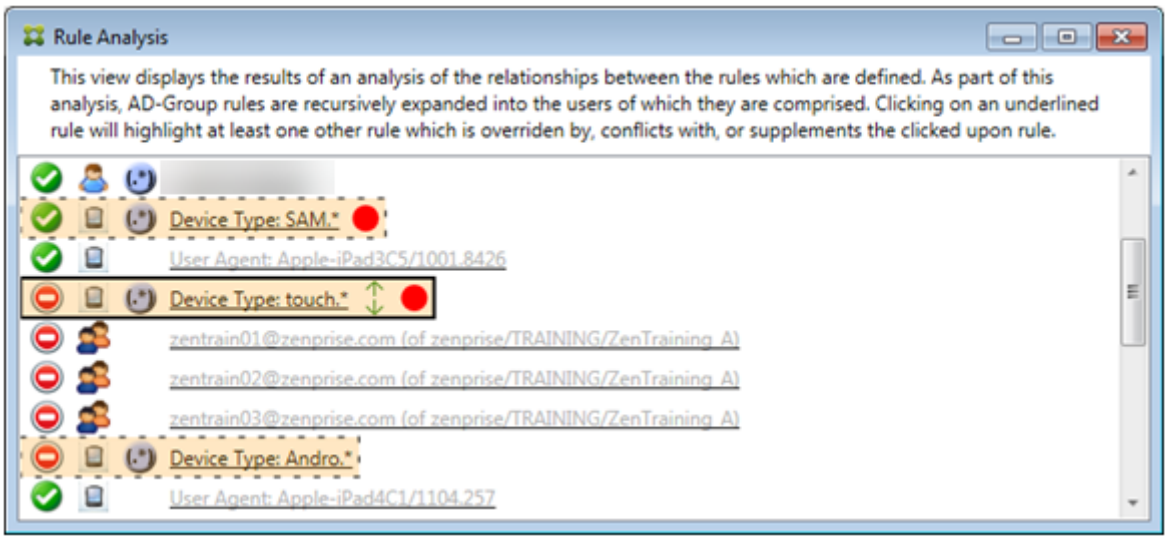


この場合、単一の補助規則（正規表現の ActiveSync デバイス ID の規則`3E.*`）がプライマリ規則を上書きします：正規表現`3E.*`が`069026593E0C4AEAB8DE7DD589ACED33`に一致するため、プライマリ規則は評価されません。

補足および競合の分析方法

この場合、プライマリ規則は正規表現の ActiveSync デバイスの種類の規則`touch.*`です。特性は次のとおりです：

- 実線の罫線で囲まれ、特定の規則フィールド（この場合は、ActiveSync デバイスの種類）に対して複数の正規表現の規則が使用されているという警告として、黄色のオーバーレイが適用されている。
- 上方向および下方向をそれぞれ指す 2 つの矢印が付けられ、より優先度の高い 1 つ以上の補助規則とより優先度の低い 1 つ以上の補助規則が存在することが示されている。
- 横に赤色の円が付けられ、1 つ以上の補助規則のアクセスが許可に設定されて、プライマリ規則のアクセス状態の禁止と競合することが示されている
- 2 つの補助規則：正規表現の ActiveSync デバイスの種類の規則`SAM.*`と正規表現の ActiveSync デバイスの種類の規則`Andro.*`が存在する。
- 両方の補助規則が破線の罫線で囲まれ、補助規則であることが示されている。
- 両方の補助規則に黄色のオーバーレイが適用され、ActiveSync デバイスの種類の規則フィールドにこれらが適用されていることが示されている。
- このようなシナリオでは、正規表現の規則が冗長でないようにする必要がある。



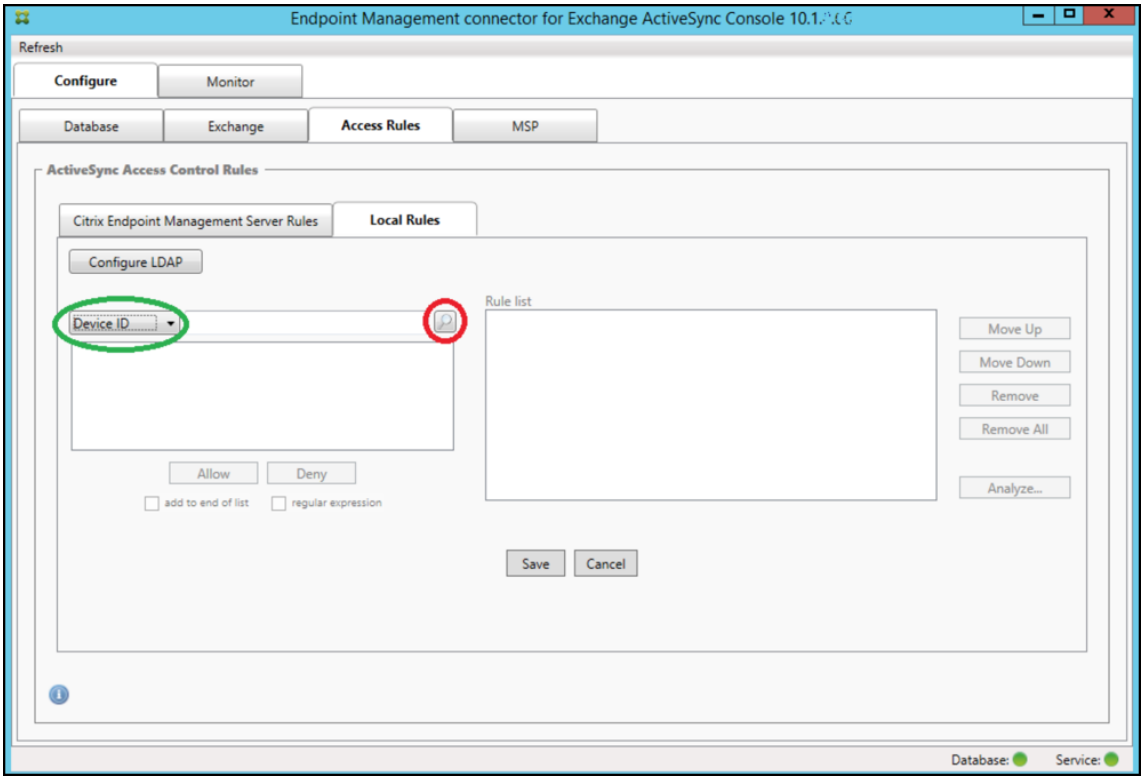
規則の高度な分析方法

次の例では、規則の関係が常にプライマリ規則の観点から示されるしくみを確認します。上記の例では、値が`touch.*`のデバイスの種類の規則フィールドに適用される正規表現規則をクリックする方法を示しました。補助規則`Andro.*`をクリックすると、さまざまな一連の補助規則が強調表示されます。

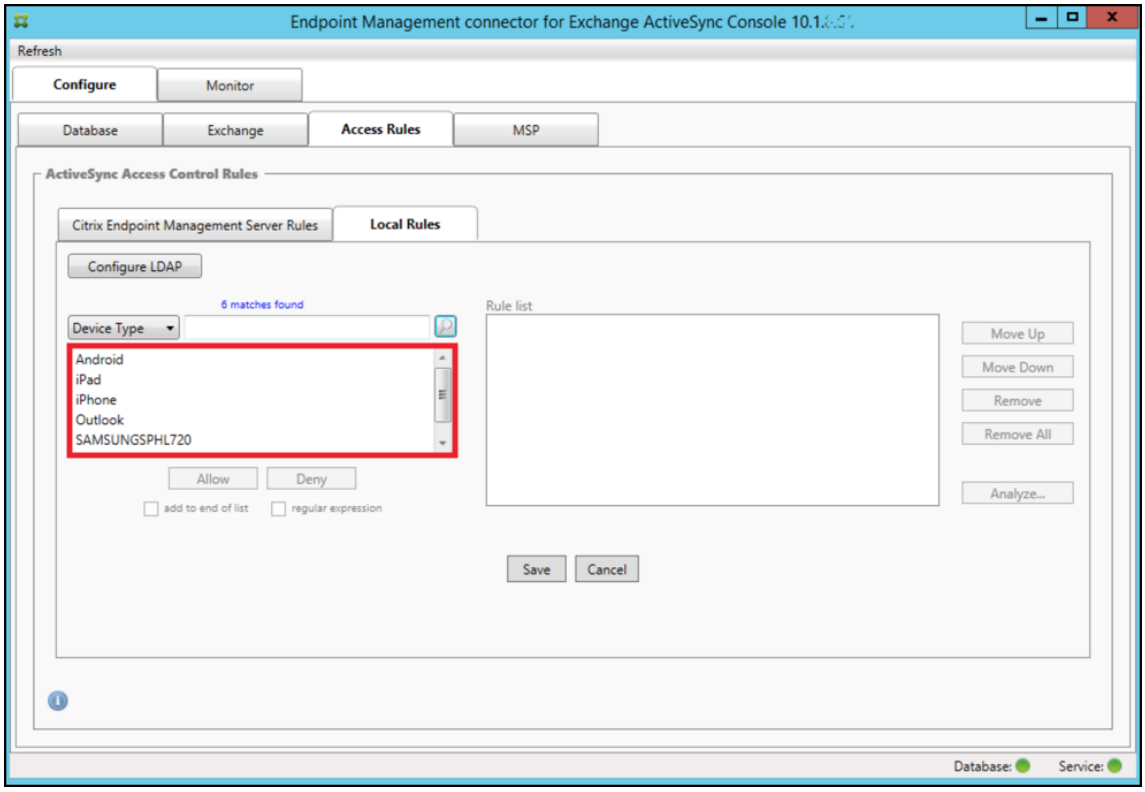
この例では、規則の関係に含まれる上書きされた規則が示されています。この規則は、通常の ActiveSync デバイスの種類の規則`Android`です。この規則は上書きされている（淡色のフォントで示され、横に黒点が付けられています）と同時に、プライマリ規則（正規表現の ActiveSync デバイスの種類の規則`Andro.*`）のアクセスと競合しています。この規則は、クリックされる前は補助規則でした。前述の例では、その時点でのプライマリ規則（正規表現の ActiveSync デバイスの種類の規則`touch.*`）の観点からは関係しなかったため、通常の ActiveSync デバイスの種類の規則`Android`は補助規則として表示されていませんでした。

通常の式のローカル規則を構成するには

1. [**Access Rules**] タブをクリックします。



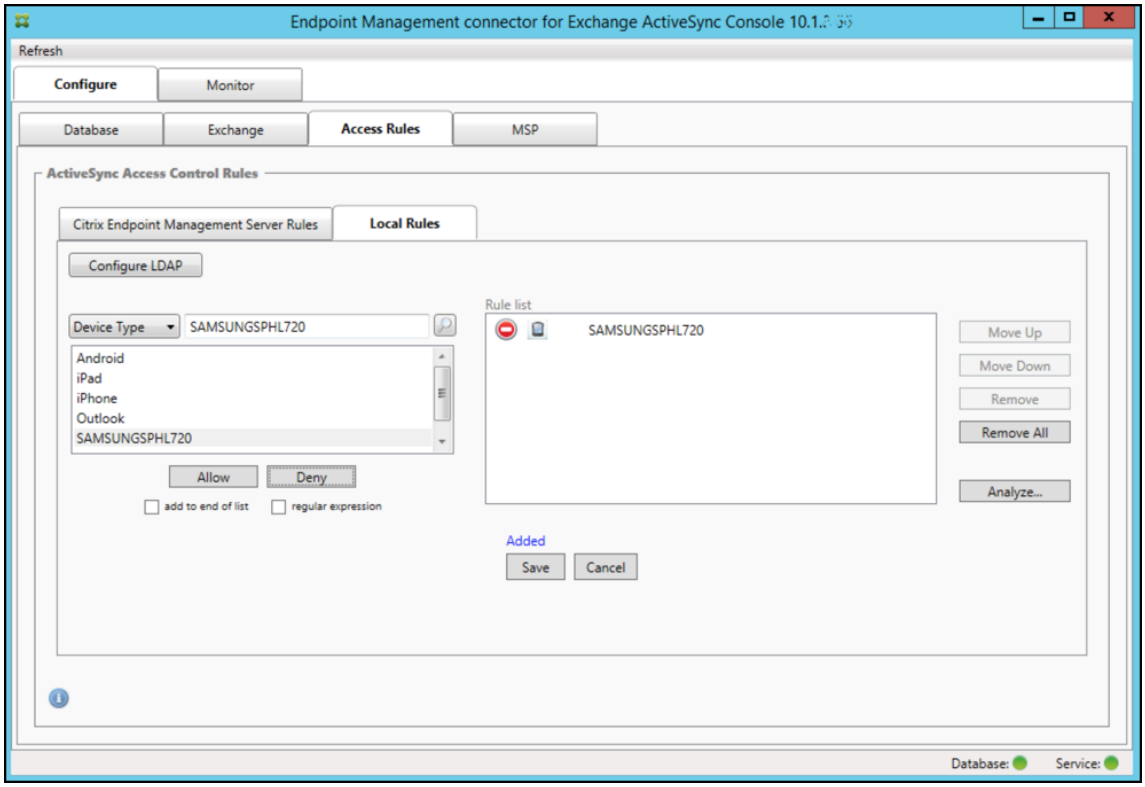
2. [**Device ID**] 一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[**Device Type**] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 表示されたリストボックスでいずれかのアイテムをクリックして、次のいずれかのオプションをクリックします:

   - **Allow**: すべての一致するデバイスに対して、ActiveSync トラフィックを許可するように Exchange が構成されます。
   - **Deny**: すべての一致するデバイスに対して、ActiveSync トラフィックを拒否するように Exchange が構成されます。

   この例では、デバイスの種類が SamsungSPhl720 であるすべてのデバイスのアクセスが拒否されます。

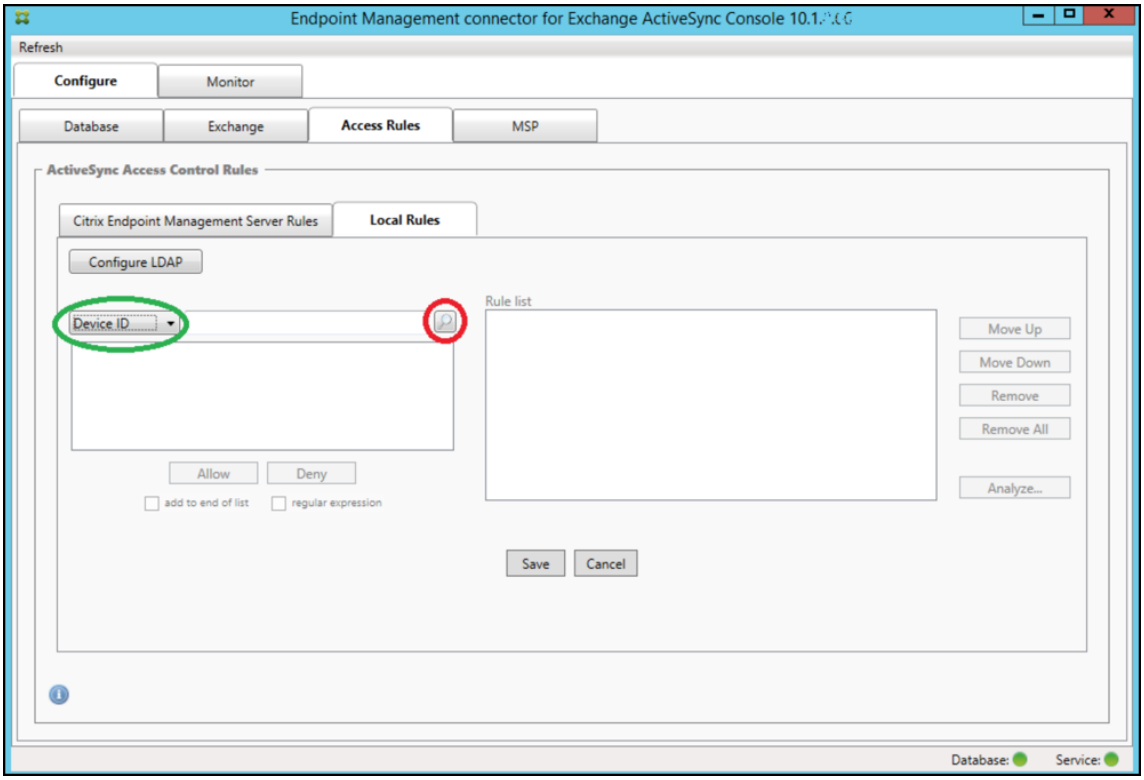


正規表現を追加するには

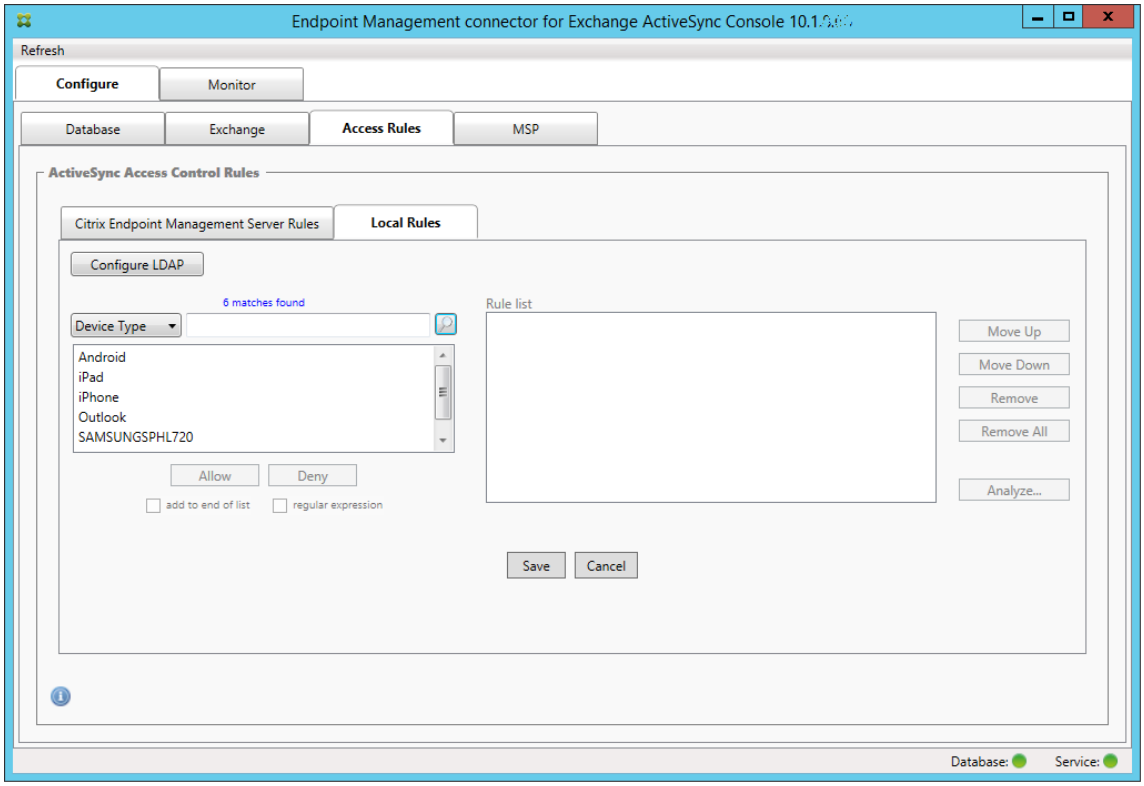
正規表現のローカル規則は、横に表示されるアイコン（  ）で識別できます。正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

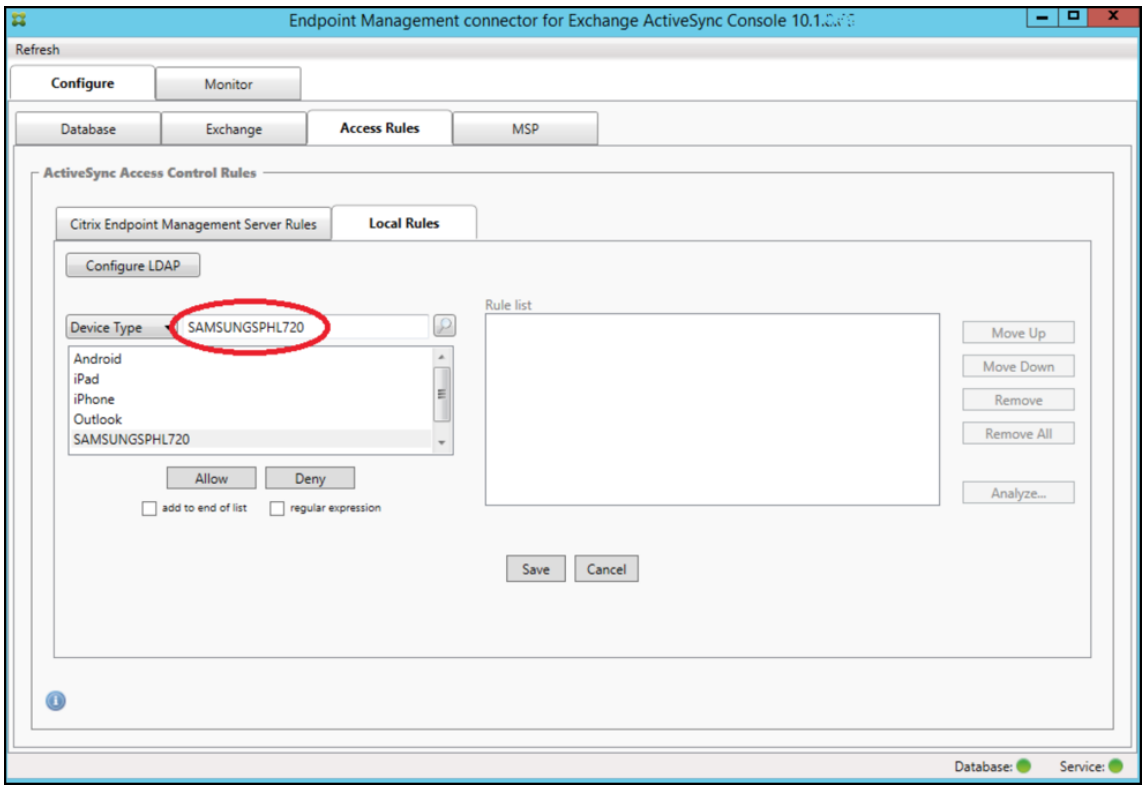
1. [**Access Rules**] タブをクリックします。



2. [**Device ID**] 一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[**Device Type**] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 結果一覧でいずれかのアイテムをクリックします。この例では、**SAMSUNGSPHL720** が選択され、それが［**Device Type**］に隣接するテキストボックスに表示されています。



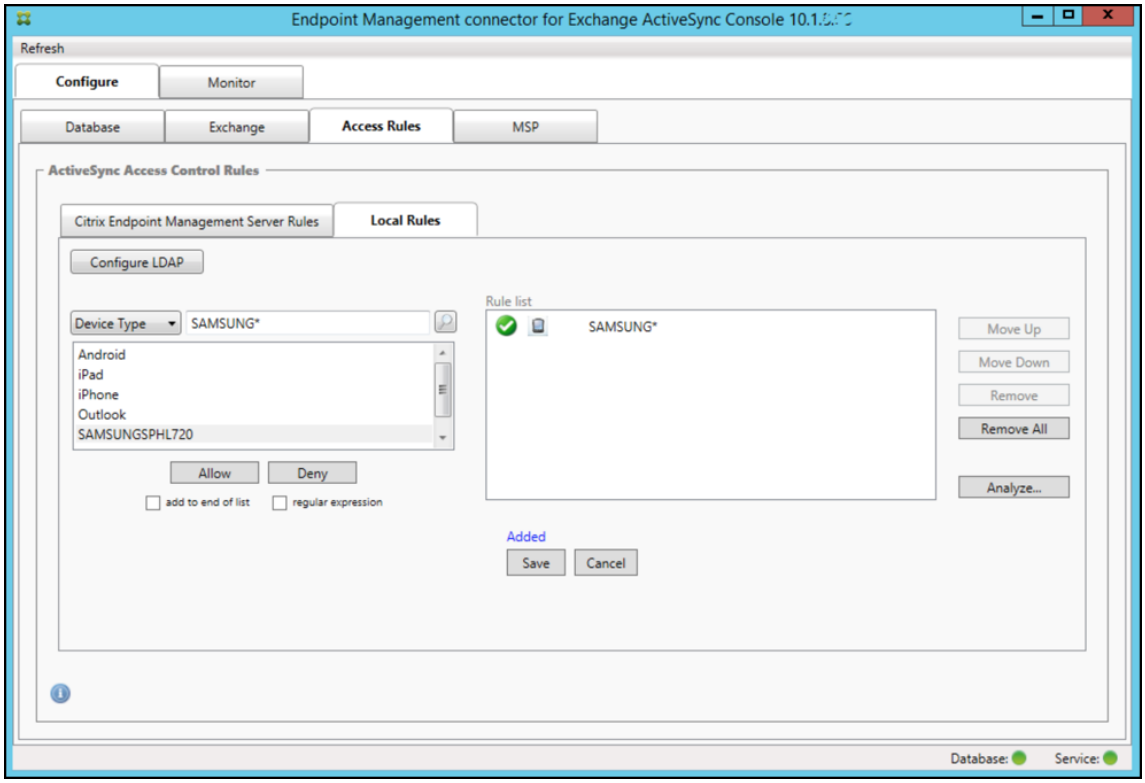
5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。

   a. 選択済みアイテムのテキストボックス内をクリックします。

   b. **SAMSUNGSPHL720** から **SAMSUNG.*** にテキストを変更します。

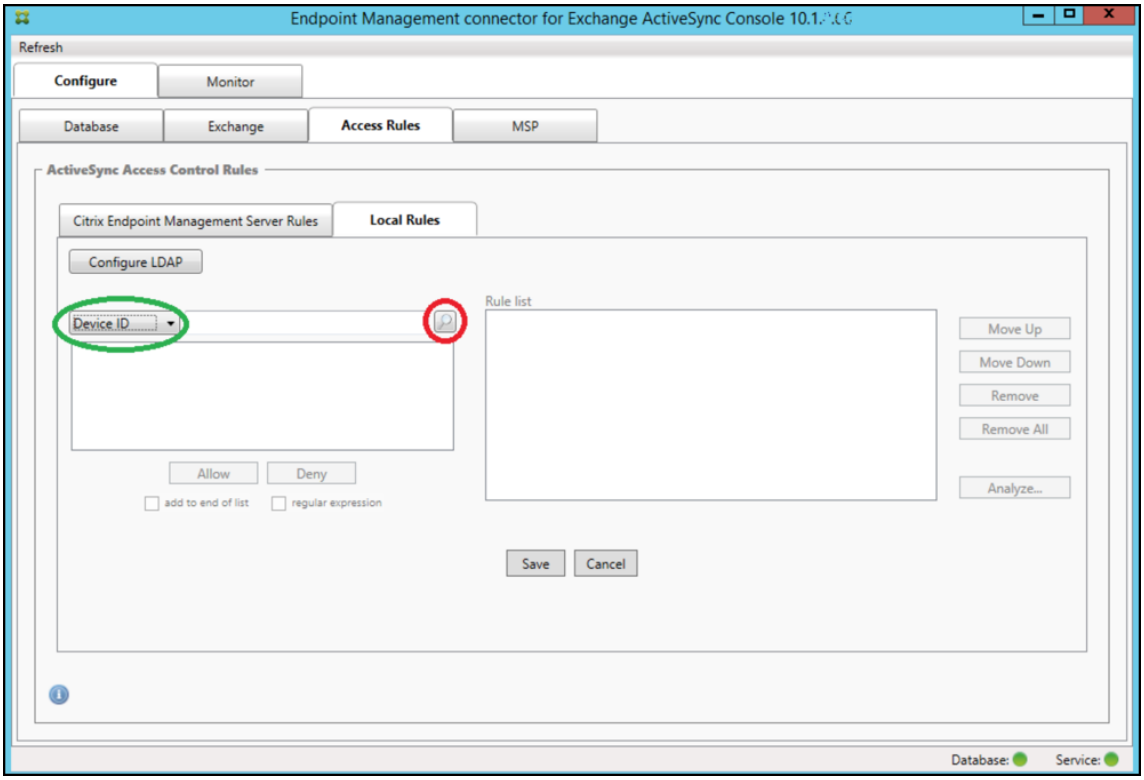
   c. ［regular expression］チェックボックスをオンにします。

   d. ［**Allow**］をクリックします。

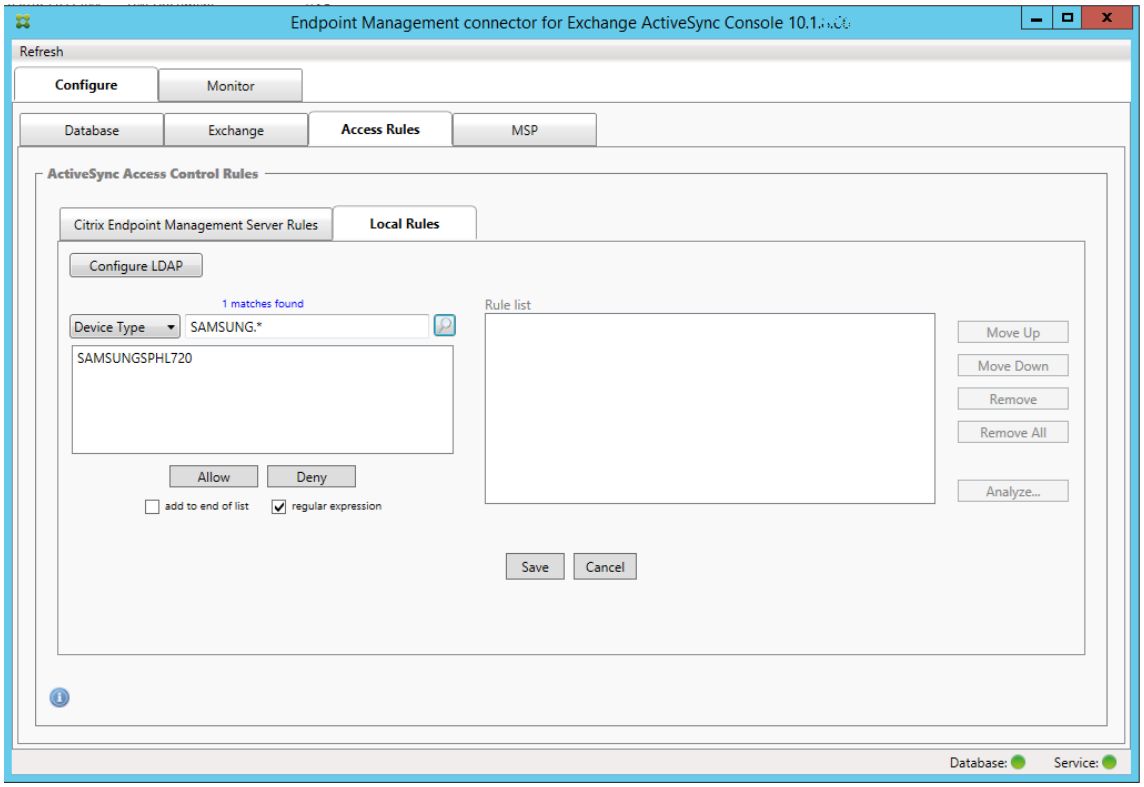


アクセス規則を作成するには

1. ［**Local Rules**］タブをクリックします。
2. 正規表現を入力するには、［Device ID］一覧と選択済みアイテムのテキストボックスの両方を使用する必要があります。



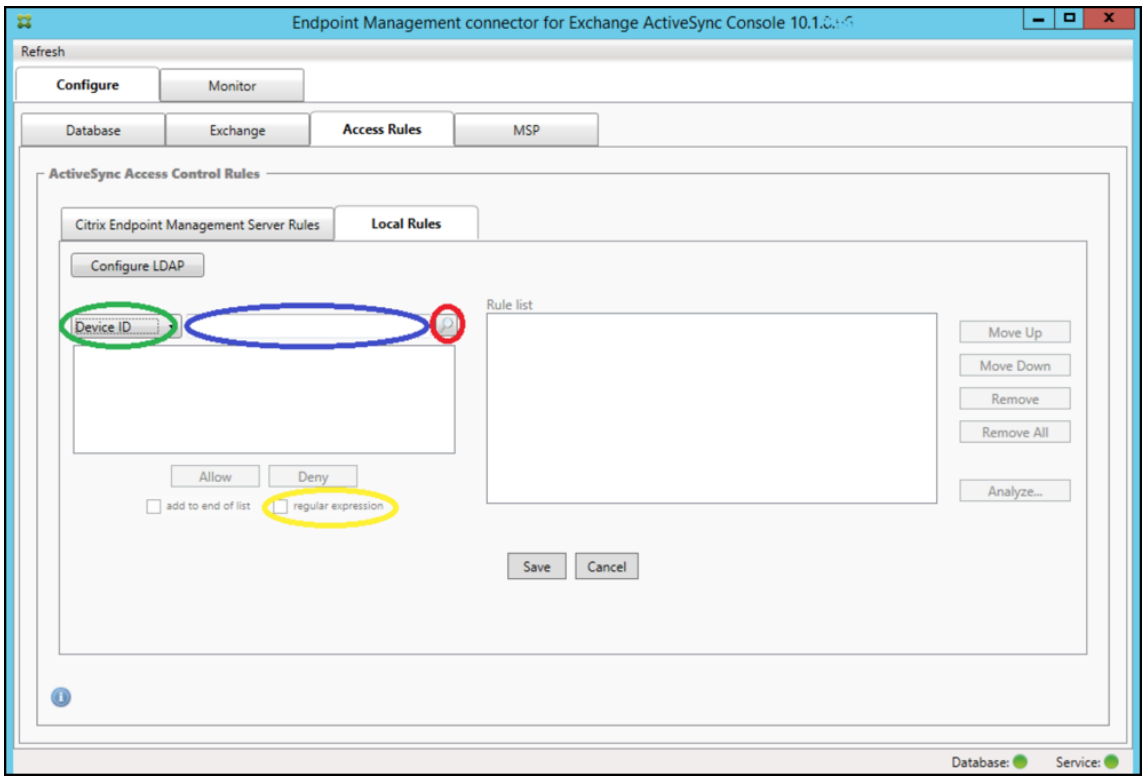
3. 照合するフィールドを選択します。この例では、[**Device Type**] を使用します。
4. 正規表現を入力します。この例では次の文字列を使用します：`samsung.*`
5. [regular expression] チェックボックスをオンにして、[**Allow**] または [**Deny**] をクリックします。この例では、[**Allow**] が選択されています。最終的な結果は次のとおりです：



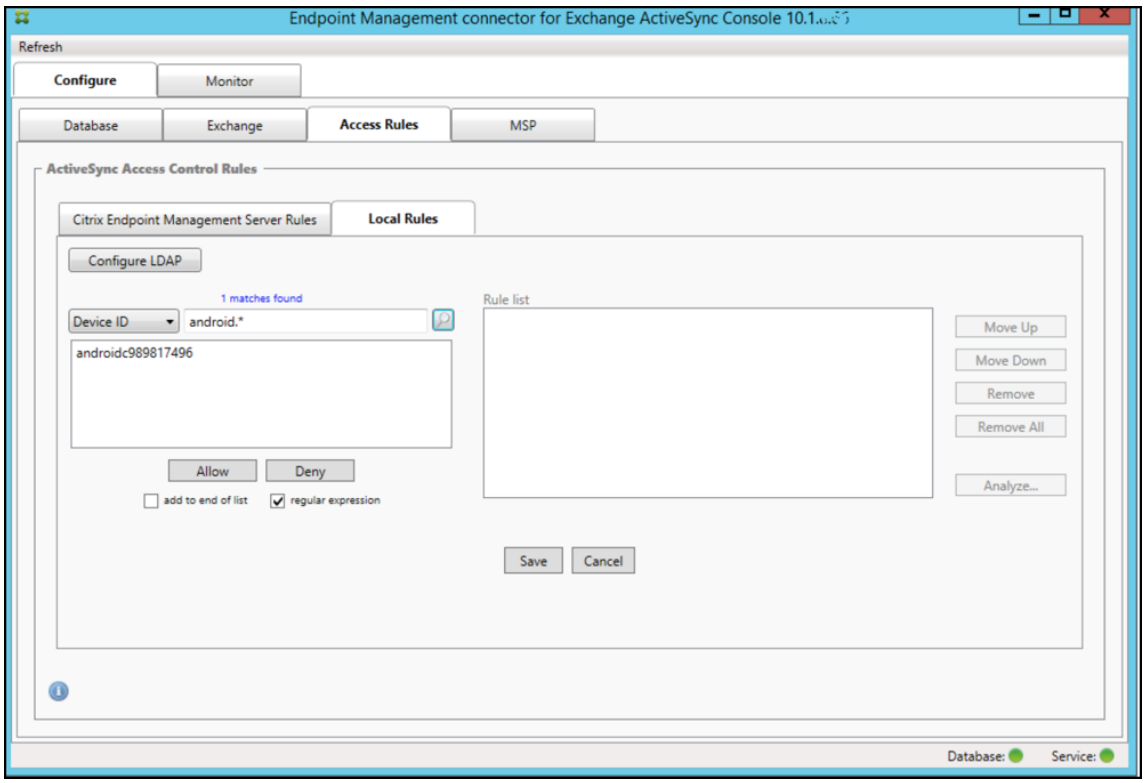
デバイスを検出するには

[regular expression] チェックボックスをオンにして、特定の式に一致する特定のデバイスの検索を実行できます。この機能は、メジャースナップショットが正常に完了している場合にのみ利用できます。正規表現の規則を使用しない場合でも、この機能を使用できます。たとえば、ActiveSync デバイス ID にテキスト「`workmail`」が含まれるすべてのデバイスを検出するとします。これを行うには、以下の手順に従います。

1. [**Access Rules**] タブをクリックします。
2. デバイスの照合フィールドセレクターが [Device ID]（デフォルト）に設定されていることを確認します。



3. 選択済みアイテムのテキストボックス内（上記の図に青色で示されています）をクリックし、「`workmail.*`」と入力します。
4. ［regular expression］チェックボックスをオンにして、虫眼鏡アイコンをクリックし、次の図に示すように一致を表示します。

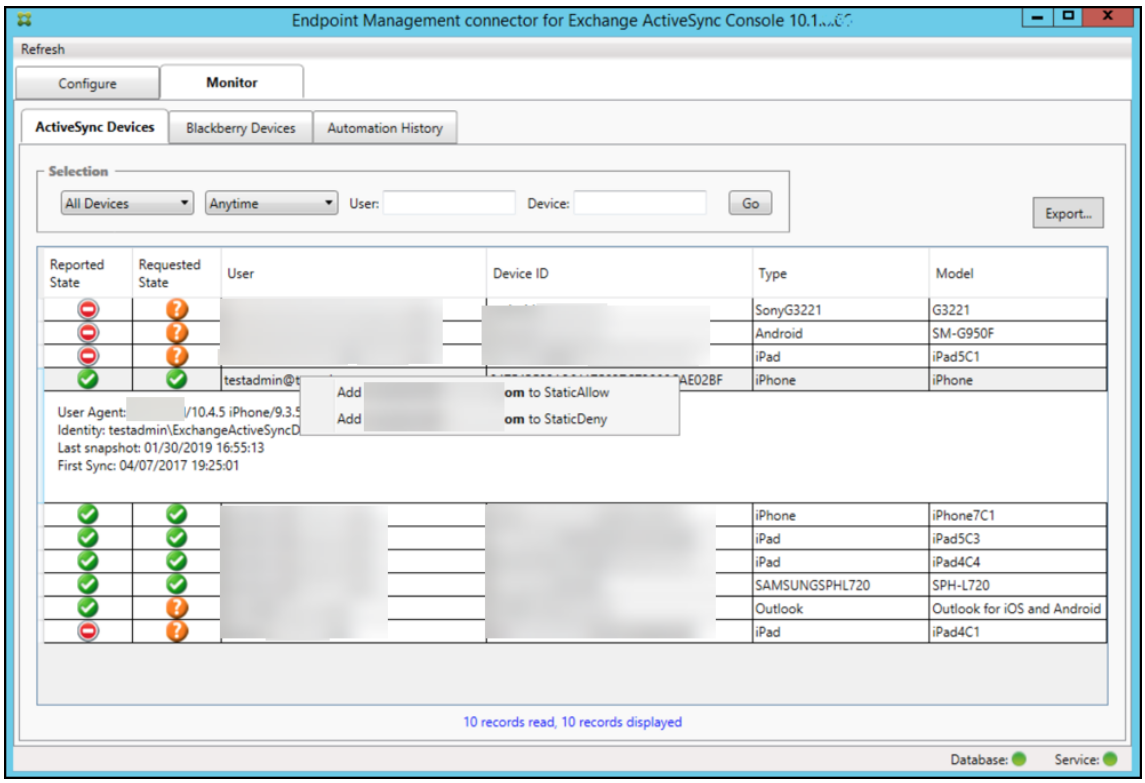


個々のユーザー、デバイス、またはデバイスの種類を静的規則に追加するには

[ActiveSync Devices] タブで、ユーザー、デバイス ID、またはデバイスの種類に基づく静的規則を追加できます。

1. [**ActiveSync Devices**] タブをクリックします。
2. 一覧で、ユーザー、デバイス、またはデバイスの種類を右クリックして、選択内容を許可するか、または拒否するかを選択します。

   次の図は、user1 を選択したときの許可/拒否オプションを示しています。



デバイス監視

Citrix Endpoint Management コネクタ: Exchange ActiveSync 用の［**Monitor**］タブでは、検出された Exchange ActiveSync デバイスおよび BlackBerry デバイスと、これまで自動で発行された PowerShell コマンドの履歴を参照できます。［**Monitor**］タブには、次の 3 つのタブがあります。

- **ActiveSync** デバイス:
  - ［**Export**］をクリックして、表示されている ActiveSync デバイスパートナーシップをエクスポートできます。
  - ［**User**］、［**Device ID**］、または［**Type**］列を右クリックし、許可またはブロックから適切な規則の種類を選択して、ローカル（静的）規則を追加できます。
  - 展開した行を折りたたむには、Ctrl キーを押しながらその行をクリックします。
- **Blackberry Devices**
- **Automation History**

［**Configure**］タブにはすべてのスナップショットの履歴が表示されます。スナップショットの履歴には、スナップショットの作成時刻、作成にかかった時間、検出されたデバイス数、発生したすべてのエラーが表示されます。

- ［**Exchange**］タブで、目的の Exchange Server の情報アイコンをクリックします。

トラブルシューティングおよび診断

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用では、エラーなどの動作情報が以下のログファイルに記録されます：*Install Folder*\log\XmmWindowsService.log Exchange ActiveSync 用コネクタは、重要なイベントを Windows イベントログにも記録します。

ログレベルを変更するには

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用には［エラー］、［情報］、［警告］、［デバッグ］、［トレース］というログレベルがあります。

> 注：
>
> 各レベルで生成される情報は、この順に詳しく（データが多く）なっていきます。たとえば、［エラー］レベルは最も情報量が少なく、［トレース］レベルは最も情報量が多くなります。

ログレベルを変更するには、次の手順を実行します：

1. C:\Program Files\Citrix\CitrixCitrix Endpoint Management connector にある nlog.config ファイルを開きます。
2. ファイル内の<rules>セクションで、*minilevel* パラメーターを任意のログレベルに変更します。例：

```
1      <rules >
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. ファイルを保存します。

   変更内容は直ちに有効になるため、Exchange ActiveSync 用コネクタを再起動する必要はありません。

一般的なエラー

一般的なエラーを以下に示します。

- Exchange ActiveSync 用コネクタサービスが開始されない

  ログファイルと Windows イベントログでエラーを確認します。一般的な原因は次のとおりです。

  - Exchange ActiveSync 用コネクタサービスが、SQL Server にアクセスできません。これは、次の問題が原因である可能性があります。
    * SQL Server サービスが実行されていない。
    * 認証エラー。

［Windows Integrated authentication］が構成されている場合、Exchange ActiveSync 用コネクタサービスのユーザーアカウントは、許可された SQL ログオンである必要があります。Exchange ActiveSync 用コネクタサービスのアカウントは、デフォルトではローカルシステムですが、ローカルの管理者権限を持つ任意のアカウントに変更できます。［SQL authentication］が構成されている場合、SQL ログオンが SQL で適切に構成されている必要があります。

トラブルシューティングツール

Support\PowerShell フォルダーに、トラブルシューティング用の PowerShell ユーティリティー式が用意されています。

トラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細 RBAC 分析を行います。すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

Citrix Gateway コネクタ：Exchange ActiveSync 用

December 8, 2023

XenMobile NetScaler Connector は Citrix Gateway コネクタ：Exchange ActiveSync 用になりました。Citrix 統合製品ラインについて詳しくは、Citrix 製品名ガイドを参照してください。

Exchange ActiveSync のコネクタでは、Exchange ActiveSync プロトコルのリバースプロキシとして動作する Citrix Gateway に、ActiveSync クライアントのデバイスレベルの認証サービスを提供します。承認は、次の組み合わせで制御します：

- Citrix Endpoint Management で定義するポリシー
- Citrix Gateway コネクタ：Exchange ActiveSync 用でローカルに定義された規則

詳細については、「ActiveSync ゲートウェイ」を参照してください。

詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。

Citrix Gateway コネクタ：Exchange ActiveSync 用の現在のリリースは、バージョン 8.5.3 です。

コネクタをダウンロードするには、以下の手順を実行します：

1. https://www.citrix.com/downloadsに移動します。
2. **Citrix Endpoint Management**（および **Citrix XenMobile Server**）**> XenMobile Server**（オンプレミス）**> Product Software > XenMobile Server 10 > Server Components** の順に移動します。
3. **Citrix Gateway** コネクタタイルで ［ファイルのダウンロード］をクリックします。

コネクタをインストールするには、「Citrix Gateway コネクタ：Exchange ActiveSync 用のインストール」を参照してください。

> 重要:
>
> 2022 年 10 月以降、Microsoft 社がこちらで発表した認証の変更を考慮して、Exchange ActiveSync の Citrix Endpoint Management および Citrix Gateway コネクタは、Exchange Online をサポートしなくなります。Exchange の Citrix Endpoint Management コネクタは、引き続き Microsoft Exchange Server（オンプレミス）で機能します。

バージョン **8.5.3** の新機能

- このリリースでは、ActiveSync プロトコル 16.0 および 16.1 のサポートが追加されています。
- Google Analytics に送信される分析内容（特にスナップショット関連）にさらに詳細が追加されました。[CXM-52261]

以前のバージョンの新機能

> 注:
>
> 以下の新機能セクションでは、「Citrix Gateway コネクタ: Exchange ActiveSync 用」を旧称の XenMobile NetScaler Connector で呼びます。名前はバージョン 8.5.2 から変更されました。

バージョン **8.5.2** の新機能

- XenMobile NetScaler Connector は Citrix Gateway コネクタ: Exchange ActiveSync 用になりました。

このリリースでは、以下の問題が解決されています。

- ポリシー規則の定義に複数の基準が使用され、1 つの基準にユーザー ID が含まれている場合、次の問題が発生する可能性があります: ユーザーに別名がある場合、ルール適用時に別名もチェックされません。[CXM-55355]

バージョン **8.5.1.11** の新機能

- システム要件の変更: 現在のバージョンの NetScaler Connector では、Microsoft .NET Framework 4.5 が必要です。
- **Google Analytics** のサポート: 製品の改善可能な箇所に集中できるように、私たちはユーザーの皆様が Connector をどのように使用しているかについて知りたいと考えています。
- **TLS 1.1** および **1.2** のサポート: セキュリティの弱化のため、PCI 評議会は TLS 1.0 および TLS 1.1 を推奨しなくなりました。XenMobile NetScaler Connector に TLS 1.2 のサポートが追加されました。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用の監視

Citrix Gateway コネクタ：Exchange ActiveSync 用の構成ユーティリティで、詳細ログが提供されます。このログを使用すると、Secure Mobile Gateway が許可または禁止する Exchange Server を通過するすべてのトラフィックを表示できます。

認証のために Citrix Gateway コネクタ：Exchange ActiveSync 用に転送される ActiveSync 要求の履歴を確認するには、［**Log**］タブを使用します。

また、Exchange ActiveSync 用コネクタ Web サービスが実行されていることを確認するには、XenMobile NetScaler Connector サーバー上のブラウザーに URL（`https://<host:port>/services/ActiveSync/Version`）をロードします。この URL をロードした結果、製品バージョンが文字列で返される場合は、Web サービスが応答しています。

Exchange ActiveSync 用コネクタで **ActiveSync** トラフィックをシミュレートするには

Citrix Gateway コネクタ：Exchange ActiveSync 用を使用して、ポリシーと ActiveSync トラフィックをシミュレートすることができます。コネクタ構成ユーティリティで、［**Simulator**］タブをクリックします。構成した規則にしたがってポリシーがどのように適用されるかが表示されます。

Exchange ActiveSync 用コネクタのフィルターの選択

Citrix Gateway コネクタ：Exchange ActiveSync 用のフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。デバイスが条件に合致すると、デバイスは［Device List］に置かれます。この［Device List］は、許可リストおよび禁止リストのどちらでもありません。これは、定義された条件に合ったデバイスの一覧です。Citrix Endpoint Management 内の Exchange ActiveSync 用コネクタでは、次のフィルターを使用できます。各フィルターの 2 つのオプションは、［**Allow**］または ［**Deny**］です。

- 匿名デバイス： Citrix Endpoint Management に登録されているが、ユーザーの ID が不明なデバイスを許可または拒否します。たとえば、登録ユーザーの Active Directory のパスワードの有効期限が切れた場合、または資格情報が不明な場合、このユーザーは未知の ID を持つとします。
- 禁止アプリ：ポリシーに含まれる禁止リストによって定義されたデバイスの一覧および禁止リスト内のアプリの存在に基づいて、デバイスが許可または拒否されます。
- 暗黙的な許可/拒否：そのほかのフィルタールール条件に合致しないすべてのデバイスの一覧が作成され、この一覧に基づいてデバイスが許可または拒否されます。［Implicit Allow/Deny］オプションを使用すると、［Devices］タブにある Exchange ActiveSync 用コネクタの状態が有効になり、デバイスのコネクタの状態が表示されます。また、［暗黙的な許可/拒否］オプションにより、選択されていないほかのすべてのコネクタのフィルターが制御されます。たとえば、コネクタは禁止リストに登録されているアプリを拒否します。ただし、［暗黙的な許可/拒否］オプションが ［許可］に設定されているため、コネクタは他のすべてのフィルターを許可します。

- 非アクティブデバイス：Citrix Endpoint Management との通信が特定の期間内に行われていないデバイスの一覧が作成されます。これらのデバイスは非アクティブと見なされます。これに従って、フィルターはデバイスを許可または拒否します。
- 不足必須アプリ：ユーザーが登録すると、インストールする必要のある必須アプリの一覧がこのユーザーに送信されます。［不足必須アプリ］のフィルターは、ユーザーが 1 つまたは複数のアプリを削除するなどして、必須アプリのうち 1 つまたは複数のアプリが不足していることを示します。
- 非推奨アプリ：ユーザーが登録すると、インストールする必要のあるアプリの一覧がこのユーザーに送信されます。［非推奨アプリ］のフィルターは、この一覧に含まれていないアプリがデバイスにインストールされていないかをチェックします。
- 非準拠パスワード：デバイスでパスコードが設定されていないすべてのデバイスの一覧が作成されます。
- コンプライアンス外デバイス：独自の内部 IT コンプライアンス条件に合致するデバイスが拒否または許可されます。コンプライアンスは、Out of Compliance という名前のデバイスプロパティによって定義される任意の設定であり、**True** または **False** のいずれかになるブール型のフラグです（このプロパティを手動で作成し、値を設定できます。または、デバイスが特定の条件を満たしているかどうかに基づいて、自動化された操作を使用して、デバイス上にこのプロパティを作成することもできます）。
  - **Out of Compliance = True**：デバイスが、IT 部門によって設定されたコンプライアンス基準およびポリシー定義に合致しない場合、デバイスはコンプライアンス違反になります。
  - **Out of Compliance = False**：デバイスが、IT 部門によって設定されたコンプライアンス基準およびポリシー定義に合致する場合、デバイスはコンプライアンスに準拠しています。
- 失効状態：取り消されたすべてのデバイスの一覧が作成され、取り消された状態に基づいてデバイスが許可または拒否されます。
- **Root** 化済み **Android** デバイス/ジェイルブレイクされた **iOS** デバイス：ルートされていることを示すフラグが付けられたすべてのデバイスの一覧が作成され、ルートされた状態に基づいてデバイスが許可または拒否されます。
- 非管理デバイス： Citrix Endpoint Management データベース内のすべてのデバイスの一覧が作成されます。Mobile Application Gateway は、ブロックモードで展開します。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用への接続を構成するには

Citrix Gateway コネクタ: Exchange ActiveSync 用では、Citrix Secure Web サービスを介して Citrix Endpoint Management およびそのほかのリモート構成プロバイダーとの通信が行われます。

1. Exchange ActiveSync 用コネクタ構成ユーティリティで、［**Config Providers**］タブをクリックし、［**Add**］をクリックします。
2. ［**Config Providers**］ダイアログボックスの ［**Name**］に、Citrix Endpoint Management サーバーでの HTTP 基本認証用の管理者権限を持つユーザー名を入力します。
3. ［**Url**］ に、Citrix Endpoint Management GCS の Web アドレス（通常は`https://<FQDN>/<instanceName>/services/<MagConfigService>`という形式）を入力します。*MagConfigService* の名前は大文字と小文字が区別されます。

4. [**Password**] に、Citrix Endpoint Management サーバーでの HTTP 基本認証に使用するパスワードを入力します。
5. [**Managing Host**] に、Exchange ActiveSync 用コネクタのサーバー名を入力します。
6. [**Baseline Interval**] で、新しく更新された動的規則のセットを Citrix Endpoint Management から取得する期間を指定します。
7. [**Delta interval**] で、動的規則の更新が取得される期間を指定します。
8. [**Request Timeout**] で、サーバー要求のタイムアウト間隔を指定します。
9. [**Config Provider**] で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
10. [**Events Enabled**] オプションについて、デバイスのブロック時に Exchange ActiveSync 用コネクタから Citrix Endpoint Management に通知する場合はこのオプションを有効にします。Citrix Endpoint Management の自動化された操作でコネクタの規則を使用する場合、このオプションが必須です。
11. [**Save**] をクリックし、[**Test Connectivity**] をクリックして、ゲートウェイから構成プロバイダーへの接続をテストします。接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い合わせてください。
12. 接続が成功した場合、[**Disabled**] チェックボックスをオフにし、[**Save**] をクリックします。

構成プロバイダーを追加すると、Exchange ActiveSync 用コネクタにより、このプロバイダーに関連付けられた 1 つまたは複数のポリシーが自動的に作成されます。`NewPolicyTemplate`セクションの`config\policyTemplates.xml`に含まれるテンプレート定義によって、ポリシーが定義されます。このセクション内で定義される各ポリシー要素に対して、新しいポリシーが作成されます。

以下が当てはまる場合は、演算子を使用して、ポリシー要素を追加、削除、または変更できます：ポリシー要素がスキーマ定義に適合しており、標準の置換文字列（中かっこで囲まれている）が変更されていない場合。次に、プロバイダーの新しいグループを追加し、ポリシーを更新してこの新しいグループを含めます。

Citrix Endpoint Management からポリシーをインポートするには

1. Exchange ActiveSync 用コネクタ構成ユーティリティで、[**Config Providers**] タブをクリックし、[**Add**] をクリックします。
2. [**Config Providers**] ダイアログボックスの [**Name**] に、Citrix Endpoint Management サーバーでの HTTP 基本認証用のユーザー名を入力します。このユーザーには管理特権が必要です。
3. [**Url**] に、Citrix Endpoint Management Gateway Configuration Service（GCS）の Web アドレス（通常は`https://<xdmHost>/xdm/services/<MagConfigService>`という形式）を入力します。MagConfigService の名前は大文字と小文字が区別されます。
4. [**Password**] に、Citrix Endpoint Management サーバーでの HTTP 基本認証に使用するパスワードを入力します。
5. [**Test Connectivity**] をクリックし、ゲートウェイから構成プロバイダーへの接続をテストします。接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い

合わせてください。

6. 接続が成功した場合、[**Disabled**] チェックボックスをオフにし、[**Save**] をクリックします。
7. [**Managing Host**] で、ローカルホストコンピューターの DNS 名をデフォルトのままにします。1 つのアレイ内で Forefront Threat Management Gateway（TMG）を複数構成済みの場合、この設定を使用して、Citrix Endpoint Management との通信を調整します。

   設定を保存してから、GCS を開きます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用ポリシーモードの構成

Citrix Gateway コネクタ：Exchange ActiveSync 用は、次の 6 つのモードで実行できます：

- **Allow All**：このポリシーモードでは、Exchange ActiveSync 用コネクタを経由するすべてのトラフィックのアクセスが許可されます。そのほかのフィルター規則は使用されません。
- **Deny All**：このポリシーモードでは、Exchange ActiveSync 用コネクタを経由するすべてのトラフィックのアクセスがブロックされます。そのほかのフィルター規則は使用されません。
- **Static Rules: Block Mode**：このポリシーモードでは、最後に暗黙的な拒否ステートメントまたはブロックステートメントを使って静的規則が実行されます。ほかのフィルター規則によって許可または許容されないデバイスは、Exchange ActiveSync 用コネクタでブロックされます。
- **Static Rules: Permit Mode**：このポリシーモードでは、最後に暗黙的な許容ステートメントまたは許可ステートメントを使って静的規則が実行されます。ほかのフィルター規則によってブロックまたは拒否されないデバイスは、Exchange ActiveSync 用コネクタで許可されます。
- **Static + ZDM Rules**： Block Mode。このポリシーモードでは、最初に静的規則が実行され、次に暗黙的な拒否ステートメントまたはブロックステートメントを使って Citrix Endpoint Management から動的規則が実行されます。デバイスは、定義済みのフィルターおよび Citrix Endpoint Management の規則に基づいて許容または拒否されます。定義済みのフィルターおよび規則に一致しないデバイスはブロックされます。
- **Static + ZDM Rules**： Permit Mode。このポリシーモードでは、最初に静的規則が実行され、次に暗黙的な許容ステートメントまたは許可ステートメントを使って Citrix Endpoint Management から動的規則が実行されます。デバイスは、定義済みのフィルターおよび Citrix Endpoint Management の規則に基づいて許容または拒否されます。定義済みのフィルターおよび規則に一致しないデバイスは許可されます。

Exchange ActiveSync 用コネクタにより、Citrix Endpoint Management から受け取った iOS モバイルデバイスおよび Windows ベースのモバイルデバイス用の一意の ActiveSync ID に応じて、動的規則に基づいて許可または禁止が処理されます。Android デバイスの場合、製造元によって動作が異なり、一部の Android デバイスでは、一意の ActiveSync ID が直ちに提供されません。代わりに、Citrix Endpoint Management により Android デバイスのユーザー ID 情報が送信され、許容するかブロックするかを決定します。その結果、ユーザーが 1 台の Android デバイスしか持っていない場合でも、許容およびブロック機能が正常に動作します。ユーザーが複数の Android デバイスを持っている場合は、Android デバイスを区別できないため、すべてのデバイスが許可されます。これらのデバイスが既知の場合は、ActiveSyncID で静的にブロックするようにゲートウェイを構成できます。また、デバイスの種類またはユーザーエージェントに基づいてブロックするようにゲートウェイを構成することもできます。

ポリシーモードを指定するには、SMG Controller Configuration ユーティリティで次の操作を実行します。

1. [**Path Filters**] タブをクリックし、[**Add**] をクリックします。
2. [**Path Properties**] ダイアログボックスの [**Policy**] リストからポリシーモードを選択し、[**Save**] をクリックします。

[**Policies**] タブで規則を確認できます。規則は、Exchange ActiveSync 用コネクタで最上位から順に処理されます。[Allow] が設定されたポリシーは緑のチェックマークで示されます。[Deny] が設定されたポリシーは中央に線が入った赤い丸で示されます。画面を更新して、最近更新された規則を表示するには、[**Refresh**] をクリックします。config.xml ファイル内の規則の順序を変更することもできます。

規則をテストするには、[**Simulator**] タブをクリックします。フィールドに値を指定します。ログから値を取得できます。[Allow] または [Block] が結果メッセージに示されます。

静的規則を構成するには

ActiveSync 接続の HTTP 要求の ISAPI フィルターによって読み取られる値を使用して静的規則を入力します。静的規則を使用すると、Exchange ActiveSync 用コネクタで次の条件に基づいてトラフィックを許可またはブロックすることができます。

- **User**: Exchange ActiveSync 用コネクタでは、承認されたユーザー値と、デバイスの登録時に取得された名前構造が使用されます。この構造は通常、LDAP 経由で Active Directory に接続された Citrix Endpoint Management を実行しているサーバーによって参照される`domain\username`形式です。コネクタ構成ユーティリティの [ログ] タブには、コネクタを経由して渡される値が表示されます。この値は、コネクタが値の構造を決定する必要がある場合、または構造が異なる場合に、渡されます。
- **DeviceID** (**ActiveSyncID**): 接続されたデバイスの ActiveSyncID とも呼ばれます。この値は、通常、Citrix Endpoint Management コンソールの特定のデバイスプロパティページ内にあります。また、Exchange ActiveSync 用コネクタ構成ユーティリティの [**Log**] タブから、この値を確認できます。
- **DeviceType**: Exchange ActiveSync 用コネクタでは、デバイスが iPhone、iPad、またはそのほかの種類のデバイスかどうかを特定し、その条件に基づいてデバイスを許可またはブロックできます。ほかの値の場合と同じように、コネクタ構成ユーティリティを使用して、ActiveSync 接続のために処理中の接続済みデバイスの種類をすべて表示できます。
- **UserAgent**: 使用する ActiveSync クライアントの情報が含まれます。通常、指定された値は、モバイルデバイスプラットフォームのオペレーティングシステムの特定のビルドおよびバージョンに対応します。

サーバーで実行中の Exchange ActiveSync 用コネクタ構成ユーティリティによって、静的規則は常に管理されます。

1. SMG Controller Configuration ユーティリティで、[**Static Rules**] タブをクリックし、[**Add**] をクリックします。
2. [**Static Rule Properties**] ダイアログボックスで、条件として使用する値を指定します。たとえば、ユーザー名（たとえば、「AllowedUser」）を入力して、アクセスを許可するユーザーを指定し、[**Disabled**] チェックボックスをオフにします。

3. ［保存］をクリックします。

   これで、静的規則が有効になりました。また、正規表現を使用して値を定義できますが、config.xml ファイルで規則処理モードを有効化する必要があります。

動的な規則を構成するには　Citrix Endpoint Management のデバイスポリシーおよびプロパティは動的な規則を定義し、Exchange ActiveSync 用コネクタの動的フィルターをトリガーできます。トリガーは、ポリシー違反またはプロパティ設定の有無に基づいています。Exchange ActiveSync 用コネクタのフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。デバイスが条件に合致すると、デバイスは［Device List］に置かれます。この［Device List］は、許可リストおよび禁止リストのどちらでもありません。これは、定義した条件に合致するデバイスの一覧です。次の構成オプションでは、Exchange ActiveSync 用コネクタを使用して［Device List］のデバイスを許可または拒否するかどうかを定義できます。

> 注:
>
> 動的規則を構成するには、Citrix Endpoint Management コンソールを使用してください。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［サーバー］の下の ［**ActiveSync** ゲートウェイ］をクリックします。［ActiveSync ゲートウェイ］ページが開きます。
3. ［次の規則をアクティブ化］で、有効にするルールを 1 つまたは複数オンにします。
4. ［Android のみ］の ［**Android** ドメインユーザーを **ActiveSync** ゲートウェイに送信］で ［はい］をクリックし、Citrix Endpoint Management から Android デバイスの情報が Secure Mobile Gateway に送信されるようにします。

   このオプションを有効にすると、デバイスユーザーの ActiveSync 識別子が Citrix Endpoint Management にない場合でも、Citrix Endpoint Management から Android デバイスの情報がコネクタに送信されます。

Exchange ActiveSync 用コネクタの **XML** ファイルを編集してカスタムポリシーを構成するには　Exchange ActiveSync 用コネクタ構成ユーティリティの ［**Policies**］タブで、デフォルトの構成の基本ポリシーを確認できます。カスタムポリシーを作成する場合、Citrix Gateway コネクタ: Exchange ActiveSync 用の XML 構成ファイル（config\config.xml）を編集できます。

1. ファイル内の **PolicyList** セクションに移動し、新しい **Policy** 要素を追加します。
2. 別の静的グループや別の GCP をサポートするグループなどの新しいグループも必要な場合は、新しい **Group** 要素を **GroupList** セクションに追加します。
3. 必要に応じて、**GroupRef** 要素を並べ替えることにより、既存のポリシー内のグループの順序を変更できます。

Exchange ActiveSync 用コネクタの **XML** ファイルの構成　Exchange ActiveSync 用コネクタは、XML 構成ファイルを使用してコネクタの動作を指示します。このファイルにより、ほかのエントリと同様に、グループファイルと、HTTP 要求を評価するときにフィルターにより実行される関連アクションが指定されます。デフォルトでは、このファイルには config.xml という名前が付けられ、次の場所に配置されます：..\Program Files\Citrix\XenMobile NetScaler Connector\config\

GroupRef ノード

GroupRef ノードにより、論理的なグループ名が定義されます。デフォルトでは、AllowGroup と DenyGroup です。

> 注：
>
> GroupRefList ノードに表示される GroupRef ノードの順序は重要です。

GroupRef ノードの ID 値により、特定のユーザーアカウントまたはデバイスを一致させるために使用するメンバーの論理的なコンテナまたはコレクションが特定されます。アクションの属性により、コレクション内の規則に一致するメンバーをフィルターで処理する方法が指定されます。たとえば、AllowGroup セット内の規則に一致するユーザーアカウントまたはデバイスは「合格」に設定されます。合格すると、Exchange CAS へのアクセスが許可されます。DenyGroup セット内の規則に一致するユーザーアカウントまたはデバイスは「拒否」されます。拒否されると、Exchange CAS へのアクセスが許可されません。

特定のユーザーアカウント/デバイスまたはその組み合わせが両方のグループの規則に一致する場合、優先する規則を使用して要求の結果が指定されます。優先順位は、config.xml ファイルの GroupRef ノードの最上位から最下位へと至る順序で表されています。GroupRef ノードは優先度によりランク付けされています。許可グループの特定条件の規則は、拒否グループの同じ条件の規則よりも常に優先されます。

グループノード

さらに、config.xml により、グループノードが定義されます。これらのノードによって、論理的なコンテナ、つまり AllowGroup および DenyGroup が外部 XML ファイルとリンクされます。外部ファイルに格納されたエントリは、フィルター規則の基礎を形成します。

> 注：
>
> このリリースでは、外部 XML ファイルのみがサポートされています。

デフォルトのインストールでは、構成に 2 つの XML ファイル（allow.xml と deny.xml）が実装されます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用の構成

[**Active Sync Service ID**]、[**Device type**]、[**User Agent**]（デバイスのオペレーティングシステム）、[**Authorized user**]、［**ActiveSync Command**］といったプロパティに基づいて、ActiveSync 要求を選択的に禁止または許可

するように Citrix Gateway コネクタ：Exchange ActiveSync 用を構成できます。

デフォルトの構成では、静的グループと動的グループの組み合わせがサポートされています。静的グループは、SMG Controller Configuration ユーティリティを使用して保守します。静的グループは、特定のユーザーエージェントを使用するすべてのデバイスなど、デバイスの既知のカテゴリで構成される場合があります。

動的グループは、ゲートウェイ構成プロバイダーと呼ばれる外部ソースによって保守されます。Exchange ActiveSync 用コネクタは、定期的にグループを接続します。Citrix Endpoint Management を使用して、許可されたデバイスとユーザーおよびブロックされたデバイスとユーザーのグループを Exchange ActiveSync 用コネクタにエクスポートできます。

動的グループは、ゲートウェイ構成プロバイダーと呼ばれる外部ソースによって保守されます。Exchange ActiveSync 用コネクタは、定期的に動的グループを収集します。Citrix Endpoint Management を使用して、許可されたデバイスとユーザーおよびブロックされたデバイスとユーザーのグループをコネクタにエクスポートできます。

ポリシーとは、アクション（許可またはブロック）が関連付けられた各グループの順序指定された一覧と、グループメンバーの一覧のことです。ポリシーには、任意の数のグループを含めることができます。ポリシー内のグループの順序は重要です。これは、1 つの一致が見つかると、グループのアクションが実行され、以降のグループは評価されないからです。

メンバーにより、要求のプロパティに一致する方法が定義されます。デバイス ID などの単一のプロパティ、またはデバイスの種類およびユーザーエージェントなどの複数のプロパティに一致することが可能です。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のセキュリティモデルの選択

あらゆる規模の組織にとって、モバイルデバイスを適切に展開するには、セキュリティモデルの確立が不可欠です。保護または隔離されたネットワーク制御を使用して、ユーザー、コンピューター、またはデバイスへのアクセスをデフォルトで許可することは一般的ですが、これは必ずしも望ましい方法ではありません。IT セキュリティを管理する各組織では、モバイルデバイスのセキュリティに対して多少異なったアプローチまたは組織に合わせたアプローチをとっている場合があります。

モバイルデバイスのセキュリティについても、同じことが言えます。多くのモバイルデバイスおよびその種類、ユーザーごとのモバイルデバイス数、利用できるオペレーティングシステムプラットフォームおよびアプリを考慮すると、許可モデルの使用はお勧めできません。多くの組織では、制限モデルの使用が最適な選択です。

Exchange ActiveSync 用コネクタと Citrix Endpoint Management の統合で利用できる構成シナリオは次のとおりです：

許可モデル（[**Permit Mode**]）

許可セキュリティモデルは、デフォルトでアクセスがすべて許可または付与されているという前提で動作します。規則およびフィルターの使用時のみ、ブロックされたり、制限が適用されたりします。許可セキュリティモデルは、モ

バイルデバイスに対するセキュリティ上の懸念が比較的少ない組織に適しています。このモデルでは、アクセスを拒否するのが適切な場合（ポリシー規則が失敗した場合）にのみ、制限コントロールが適用されます。

制限モデル（[**Block Mode**]）

制限セキュリティモデルは、デフォルトでアクセスが許可または付与されていないという前提に基づきます。セキュリティチェックポイントを通過するすべてのデータがフィルターおよび検査され、アクセスを許可する規則をパスしない限り、アクセスが拒否されます。制限セキュリティモデルは、モバイルデバイスに対するセキュリティ上の条件が比較的に厳しい組織に適しています。このモードでは、アクセスを許可するすべての規則をパスした場合にのみ、ネットワークサービスの使用と機能へのアクセスが許可されます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用の管理

Citrix Gateway コネクタ：Exchange ActiveSync 用を使用してアクセス制御規則を作成できます。この規則は、管理対象デバイスからの ActiveSync 接続要求へのアクセスを許可またはブロックします。アクセスは、デバイスのステータス、アプリの許可リストまたは禁止リスト、およびその他のコンプライアンス設定状況に基づきます。

Exchange ActiveSync 用コネクタ構成ユーティリティを使用して、社内のメールポリシーを適用する動的および静的規則を作成できます。これらの規則とポリシーで、コンプライアンス基準に違反しているユーザーをブロックすることができます。また、Exchange Server を経由して管理対象デバイスに送信されるすべての添付ファイルを暗号化するようにセットアップできます。管理対象デバイスで権限のあるユーザーのみが暗号化された添付ファイルを表示できます。

XNC をアンインストールするには

1. 管理者アカウントで XncInstaller.exe を実行します。
2. 画面の指示に従って、アンインストールを完了します。

Exchange ActiveSync 用コネクタをインストール、アップグレード、またはアンインストールするには

1. 管理者アカウントで XncInstaller.exe を実行して、Exchange ActiveSync 用コネクタをインストールするか、既存のコネクタをアップグレードまたは削除できます。
2. 画面の指示に従って、インストール、アップグレード、またはアンインストールを完了します。

Exchange ActiveSync 用コネクタをインストールした後、Citrix Endpoint Management の構成サービスおよび通知サービスを手動で再起動する必要があります。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のインストール

Exchange ActiveSync 用コネクタは、専用のサーバーまたは Citrix Endpoint Management をインストールしたサーバーにインストールできます。

次の場合は、Exchange ActiveSync 用コネクタを専用のサーバー（Citrix Endpoint Management とは別のサーバー）にインストールすることを検討してください：

- Citrix Endpoint Management サーバーがクラウドにリモートでホストされている場合（物理的な場所）
- Exchange ActiveSync 用コネクタが、Citrix Endpoint Management サーバーの再起動の影響を受けないようにする場合（可用性）
- サーバーのすべてのシステムリソースを Exchange ActiveSync 用コネクタ用に使用する場合（パフォーマンス）

Exchange ActiveSync 用コネクタがサーバーに与える CPU 負荷は、管理対象デバイスの数によって異なります。コネクタを Citrix Endpoint Management と同じサーバーに展開する場合は、CPU コアを 1 つ追加してプロビジョニングすることをお勧めします。多数のデバイス（50,000 個以上）がある場合に、クラスター環境がないときは、追加のコアが必要になることがあります。コネクタのメモリサイズは、追加メモリを保証するのに十分ではありません。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のシステム要件

Citrix Gateway コネクタ：Exchange ActiveSync 用では、Citrix Gateway アプライアンスで構成された SSL ブリッジを介して Citrix Gateway との通信が行われます。SSL ブリッジを使用すると、アプライアンスですべてのセキュアなトラフィックを Citrix Endpoint Management に直接ブリッジすることができます。Exchange ActiveSync 用コネクタには、次の最小システム構成が必要です：

コンポーネント	条件
コンピューターとプロセッサ	Pentium III 733MHz 以上のプロセッサ。Pentium III 2.0GHz 以上のプロセッサ（推奨）
Citrix Gateway	ソフトウェアバージョン 10 を備えた Citrix Gateway アプライアンス
メモリ	1GB
ハード ディスク	150MB のハードディスクスペースがある、NTFS でフォーマットしたローカルパーティション

コンポーネント	条件
オペレーティングシステム	Windows Server 2016、Windows Server 2012 R2 または Windows Server 2008 R2 Service Pack 1。英語ベースのサーバーが必要です。Windows Server 2008 R2 Service Pack 1 のサポートは 2020 年 1 月 14 日に終了し、Windows Server 2012 R2 のサポートは 2023 年 10 月 10 日に終了します。
そのほかのデバイス	ホストオペレーティングシステムと互換性があるネットワークアダプター（内部ネットワークとの通信用）
Microsoft .NET Framework。	バージョン 8.5.1.11 では、Microsoft .NET Framework 4.5 が必要です。
表示	VGA 以上の解像度のモニター

Exchange ActiveSync 用コネクタのホストコンピューターには、次の最小ハードディスクスペースが必要です：

- アプリケーション： 10～15MB（推奨値は 100MB）
- ログ： 1GB（推奨値は 20GB）

Exchange ActiveSync 用コネクタのプラットフォームのサポートについて詳しくは、「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。

デバイスのメールクライアント

すべてのメールクライアントが、デバイスに関して一貫して同じ ActiveSync ID を返すわけではありません。Exchange ActiveSync 用コネクタは、各デバイスに対して一意の ActiveSync ID を前提とするため、デバイスごとに一意の同じ ActiveSync ID を一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントはテスト済みで、エラーなく実行できます：

- Samsung のネイティブメールクライアント
- iOS のネイティブメールクライアント

Citrix Gateway コネクタ：**Exchange ActiveSync** 用の展開

Citrix Gateway コネクタ：Exchange ActiveSync 用は、Citrix Gateway を使用して、Citrix Endpoint Management サーバーによる管理対象デバイスと Citrix Endpoint Management 間の通信をプロキシ接続したり、負荷分散したりできます。Exchange ActiveSync 用コネクタと Citrix Endpoint Management 間では通信が定期的に行われ、ポリシーが同期されます。Exchange ActiveSync 用コネクタと Citrix Endpoint Management をまとめて、または別々にクラスター化できます。

Exchange ActiveSync 用コネクタのコンポーネント

- **Exchange ActiveSync** 用コネクタサービス：このサービスでは、Citrix Gateway が呼び出せる REST Web サービスのインターフェイスが提供され、デバイスからの ActiveSync 要求が承認されるかどうかが決定されます。
- **Citrix Endpoint Management** 構成サービス：このサービスでは、Citrix Endpoint Management との通信が行われ、Citrix Endpoint Management ポリシーの変更が Exchange ActiveSync 用コネクタと同期されます。
- **Citrix Endpoint Management** 通知サービス：このサービスでは、Citrix Endpoint Management への承認されていないデバイスのアクセスが通知されます。これにより Citrix Endpoint Management では、デバイスがブロックされた理由をユーザーに通知するなどの適切な処置を施すことができます。
- **Exchange ActiveSync** 用コネクタ構成ユーティリティ：このアプリケーションを使用すると、管理者は Exchange ActiveSync 用コネクタを構成して監視することができます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のリッスンアドレスをセットアップするには

Citrix Gateway コネクタ：Exchange ActiveSync 用が Citrix Gateway から要求を受信して ActiveSync トラフィックを承認できるようにするには、次の手順を実行します。Exchange ActiveSync 用コネクタが Citrix Gateway Web サービス呼び出しをリッスンするポートを指定します。

1. ［スタート］メニューから Exchange ActiveSync 用コネクタ構成ユーティリティを選択します。
2. ［**Web Service**］タブをクリックし、コネクタ Web サービスのリッスンアドレスを入力します。**HTTP** と **HTTPS** のいずれかまたは両方を選択できます。Exchange ActiveSync 用コネクタが Citrix Endpoint Management と共存している場合（同じサーバーにインストールされている場合）、Citrix Endpoint Management と競合しないポート値を選択します。
3. この値を構成した後、［**Save**］をクリックして、［**Start Service**］をクリックし、Web サービスを起動します。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用でデバイスのアクセス制御ポリシーを構成するには

管理対象デバイスに適用するアクセス制御ポリシーを構成するには、次の操作を実行します。

1. Exchange ActiveSync 用コネクタ構成ユーティリティで、［**Path Filters**］タブをクリックします。
2. 最初の行の［**Microsoft-Server-ActiveSync is for ActiveSync**］を選択し、［**Edit**］をクリックします。
3. ［**Policy**］の一覧から、目的のポリシーを選択します。Citrix Endpoint Management ポリシーが含まれるポリシーの場合、［**Static + ZDM: Permit Mode**］または［**Static + ZDM: Block Mode**］を選択します。これらのポリシーでは、ローカルの（つまり静的）規則と Citrix Endpoint Management の規則が組み合わされます。［Permit Mode］では、規則によって明示的に特定されないすべてのデバイスが ActiveSync へのアクセスを許可されます。［Block Mode］では、そのようなデバイスがブロックされます。

4. ポリシーを設定したら、[**Save**] をクリックします。

Citrix Endpoint Management との通信を構成するには

Citrix Gateway コネクタ: Exchange ActiveSync 用および Citrix Gateway で使用する Citrix Endpoint Management サーバーの名前およびプロパティを指定します。

> 注:
>
> このタスクでは、Citrix Endpoint Management がインストールされていて、構成済みであることを前提としています。Exchange ActiveSync 構成ユーティリティでは、Citrix Endpoint Management 用の構成プロバイダーという用語が使用されます。

1. Exchange ActiveSync 用コネクタ構成ユーティリティで、[**Config Providers**] タブをクリックし、[**Add**] をクリックします。
2. この展開で使用する Citrix Endpoint Management サーバーの名前および URL を入力します。マルチテナント展開で複数の Citrix Endpoint Management サーバーがある場合は、この名前は各サーバーインスタンスで固有である必要があります。
3. [**Url**] に、Citrix Endpoint Management GlobalConfig Provider (GCP) の Web アドレス (通常は`https://<FQDN>/<instanceName>/services/<MagConfigService>`という形式) を入力します。*MagConfigService* の名前は大文字と小文字が区別されます。
4. [**Password**] に、Citrix Endpoint Management Web サーバーでの HTTP 基本認証に使用するパスワードを入力します。
5. [**Managing Host**] に、Exchange ActiveSync 用コネクタをインストールしたサーバーの名前を入力します。
6. [**Baseline Interval**] で、新しく更新された動的規則のセットを Citrix Endpoint Management から取得する期間を指定します。
7. [**Request Timeout**] で、サーバー要求のタイムアウト間隔を指定します。
8. [**Config Provider**] で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
9. [**Events Enabled**] オプションについて、デバイスのブロック時に Secure Mobile Gateway から Citrix Endpoint Management に通知する場合はこのオプションを有効にします。Citrix Endpoint Management の自動化された操作で Secure Mobile Gateway の規則を使用する場合、このオプションが必要です。
10. サーバーを構成したら、[**Test Connectivity**] をクリックして、Citrix Endpoint Management への接続をチェックします。
11. 接続が確立したら、[**Save**] をクリックします。

冗長性およびスケーラビリティのための **Citrix Gateway** コネクタ：**Exchange ActiveSync** 用の展開

Citrix Gateway コネクタ：Exchange ActiveSync 用および Citrix Endpoint Management 展開のスケーラビリティを向上させるには、Exchange ActiveSync 用コネクタのインスタンスを複数の Windows サーバーにインストールします。すべてのコネクタインスタンスが同じ Citrix Endpoint Management インスタンスを指します。次に、Citrix Gateway を使用してサーバーの負荷分散を行います。

Exchange ActiveSync 用コネクタの構成には次の 2 つのモードがあります。

- 非共有モードでは、Exchange ActiveSync 用コネクタの各インスタンスが Citrix Endpoint Management サーバーと通信し、結果として生成されるポリシーの独自のプライベートコピーを保持します。たとえば、Citrix Endpoint Management サーバーのクラスターでは、各 Citrix Endpoint Management サーバーでコネクタインスタンスを実行できます。すると、コネクタは、ローカルの Citrix Endpoint Management インスタンスからポリシーを取得します。
- 共有モードでは、Exchange ActiveSync 用コネクタの 1 つのノードがプライマリノードに指定されます。コネクタは、Citrix Endpoint Management と通信します。Windows ネットワーク共有または Windows（または、サードパーティの）レプリケーションによって、結果として生成される構成がほかのノード間で共有されます。

Exchange ActiveSync 用コネクタの構成全体は、単一のフォルダー（数個の XML ファイルから構成されます）にあります。コネクタの処理によって、このフォルダー内のファイルに加えられた変更が検出され、構成が自動的に再ロードされます。共有モードのプライマリノードに対するフェイルオーバーはありません。ただし、システムは、プライマリサーバーの数分間のダウン（再起動など）を許容できます。前回正常起動時の構成は、コネクタプロセスにキャッシュされます。

高度な概念

November 1, 2023

Citrix Endpoint Management の高度な設定の記事では、Citrix Endpoint Management の製品情報をさらに詳しく紹介しています。その目的は専門家の技術を使用して開発期間の短縮を支援することです。記事では、コンテンツを作成した 1 人または複数の技術者に言及します。

Citrix Endpoint Management 環境の決定ポイント、推奨事項、よくある質問、およびユースケースについては、このセクションの「Citrix Endpoint Management の展開」を参照してください。

Citrix Endpoint Management のコミュニティサポートフォーラムについては、「Citrix Discussions」を参照してください。

Citrix Endpoint Management の展開

March 15, 2024

Citrix Endpoint Management の展開を計画する際には、考慮すべき点がたくさんあります。どんなデバイスを選ぶか。それらをどのように管理するか。良好なユーザーエクスペリエンスを実現しながらネットワークを安全に保つにはどうすればよいか。どんなハードウェアを用意し、そのトラブルシューティングをどのように行うか。本セクションの各記事は、これらの質問に答えることを目的としています。展開の問題に関連したユースケースや推奨事項を取り上げています。

ガイドラインや推奨事項は、すべての環境やユースケースに適用されるわけではないことに注意してください。Citrix Endpoint Management の展開を開始する前に、テスト環境を設定してください。

本セクションの各記事は、次の領域について説明します:

- 評価：展開を計画する際に考慮すべき共通のユースケースと質問
- 設計と構成：環境の設計と構成に関する推奨事項
- 動作と監視：実行環境の円滑な動作の確保。

評価

どの環境でも、ニーズを評価することが最優先事項です。Citrix Endpoint Management に対する一番のニーズは何ですか。管理しなければならないのは、環境内の全デバイスですか、アプリだけですか、それともその両方ですか。Citrix Endpoint Management 環境にはどの程度のレベルのセキュリティが必要ですか。展開を計画する際に考慮すべき共通のユースケースと質問を見ていきましょう。

- 管理モード
- デバイスの要件
- セキュリティとユーザーエクスペリエンス
- アプリ
- ユーザーコミュニティ
- メール戦略
- Citrix Endpoint Management の統合

設計と構成

展開ニーズの評価が完了したら、環境の設計と構成方法を決定できます。計画する項目は次のとおりです:

- サーバー用のハードウェアの選定
- アプリおよびデバイスのポリシーの設定
- ユーザーの登録

このセクションには、これらのシナリオやその他のユースケースと推奨事項が含まれています。

- NetScaler Gateway および Citrix ADC との統合
- MDX アプリの SSO とプロキシの考慮事項
- 認証
- サーバープロパティ
- デバイスポリシーとアプリポリシー
- ユーザー登録オプション

動作と監視

Citrix Endpoint Management 環境が稼働したら、スムーズに動作するように監視を行います。「監視」セクションでは、Citrix Endpoint Management とそのコンポーネントが生成するさまざまなログとメッセージの格納場所と、それらのログの見方について説明します。また、このセクションでは、カスタマーサポートのフィードバックにかかる時間を短縮できる一般的なトラブルシューティングの手順も紹介します。

- アプリのプロビジョニングとプロビジョニング解除
- ダッシュボードベースの操作
- 役割ベースのアクセス制御と Citrix Endpoint Management のサポート
- モニターとサポート
- Citrix のサポートプロセス

管理モード

March 15, 2024

管理モードには、モバイルデバイス管理（MDM）とモバイルアプリケーション管理（MAM）が含まれます。以下の項目を構成できます。

- Android デバイスと iOS デバイスを MDM、MAM、またはその両方（MDM+MAM）に登録するための登録プロファイル。MDM+MAM を選択した場合、ユーザーは MDM をオプトアウトできます。
- Windows 10 および Windows 11 デバイスを MDM に登録するための登録プロファイル。

登録プロファイルでは、デリバリーグループに添付する登録オプションを指定します。登録オプションについては、「登録プロファイル」を参照してください。次のセクションでは、デバイスとアプリの管理に関する考慮事項を中心に説明します。

モバイルデバイス管理（**MDM**）

MDM を使用すると、モバイルデバイスを設定、保護、およびサポートできます。MDM では、システムレベルでデバイス上のデバイスとデータを保護できます。ポリシー、アクション、およびセキュリティ機能を設定できます。たとえば、デバイスが紛失や盗難にあったり、コンプライアンス違反となった場合に、デバイスを選択的にワイプできます。

デバイス上のアプリの管理を選択しなくても、パブリックアプリストアやエンタープライズアプリなどのモバイルアプリを配信できます。

以下は、MDM の一般的なユースケースです：

- MDM は、デバイスレベルの管理ポリシーや一定の制約が必要な企業所有デバイスが考慮されています。このような制約には、完全なワイプ、選択的なワイプ、地理位置情報が含まれます。
- 顧客が実際のデバイスの管理を必要としながら、MDX ポリシーを必要としない場合。
- ユーザーはモバイルデバイス上のネイティブメールクライアントへのメールの配信のみが必要で、Exchange ActiveSync やクライアントアクセスサーバーにはすでに外部からアクセス可能な場合。このユースケースでは、MDM を使用してメールの配信を設定できます。
- ネイティブエンタープライズアプリ（非 MDX）、パブリックアプリストアアプリ、またはパブリックストアから配信された MDX アプリを展開する場合。MDM ソリューションだけでは、デバイス上のアプリ間の機密情報の漏洩を防止できない可能性があることを考慮してください。データ漏洩は、Office 365 アプリでのコピー＆ペースト操作や名前を付けて保存操作で発生する可能性があります。

モバイルアプリケーション管理（**MAM**）

MAM はアプリデータを保護し、アプリデータ共有を制御できるようにします。また、個人データとは別に企業のデータやリソースの管理も可能です。Citrix Endpoint Management が MAM に設定されていると、MDX 対応のモバイルアプリを使用して、アプリごとのコンテナ化と制御を提供できます。

MDX ポリシーを活用することにより、Citrix Endpoint Management はネットワークアクセス（マイクロ VPN など）、アプリとデバイスのやり取り、およびアプリへのアクセスをアプリレベルで制御します。

デバイスは管理されませんが企業データの保護は維持されるため、多くの場合 MAM は私的デバイス活用（BYO）に適しています。MDX には、MDM 制御を必要としない MAM のみのポリシーが多数あります。

MAM モードでは、Citrix 業務用モバイルアプリもサポートされます。このサポートには以下が含まれます：

- Citrix Secure Mail へのメールの安全な配信
- 保護対象の Citrix 業務用モバイルアプリ間でのデータ共有
- Citrix Files の安全なデータストレージ

詳しくは、「業務用モバイルアプリ」を参照してください。

多くの場合、MAM は次の例に適しています。

- アプリレベルで管理されている MDX アプリなどのモバイルアプリを配信する。
- システムレベルでデバイスを管理する必要がない。

MDM + MAM

Citrix Endpoint Management では、ユーザーがデバイス管理をオプトアウトできるかどうかを指定できます。この柔軟性は、複数のユースケースが混在する環境で役立ちます。これらの環境では、MAM リソースへのアクセスで、MDM ポリシーに基づいたデバイスの管理が必要な場合があります。

多くの場合、MDM + MAM は次の例に適しています。

- MDM と MAM の両方が必要なユースケースが 1 つだけある。MAM リソースにアクセスするために MDM が必要である。
- MDM が必要なユースケースもあるが、そうでないユースケースもある。
- MAM が必要なユースケースもあるが、そうでないユースケースもある。

デバイス管理と **MDM** 登録

Citrix Endpoint Management Enterprise 環境には、MAM リソースへのアクセスを許可する MDM ポリシーによるデバイス管理が必要なケースなど、複数のユースケースが混在している場合があります。

Citrix 業務用モバイルアプリをユーザーに展開する前に、ユースケースを十分に評価し、MDM 登録を必須にするかどうかを決定してください。MDM 登録の必要性を後で変更すると、ユーザーがデバイスを再登録しなければならない場合もあります。詳しくは、「登録プロファイル」を参照してください。

登録と NetScaler Gateway については、「NetScaler Gateway および Citrix ADC との統合」を参照してください。

次に、MDM 登録を必要とする場合のメリットとデメリットを（緩和策とともに）示します。

MDM 登録をオプションとする場合

長所

- ユーザーはデバイスを MDM 管理下に置くことなく、MAM リソースにアクセスできる。このオプションは、ユーザーへの導入を増やすことができます。
- MAM リソースへのアクセスを保護し、企業データを保護できる。
- アプリのパスコードなどの MDX ポリシーで、各 MDX アプリのアプリアクセスを制御できる。
- Citrix PIN と合わせて NetScaler Gateway、Citrix Endpoint Management、およびアプリケーションごとのタイムアウトを構成することで、セキュリティが高まる。

- MDM アクションはデバイスには適用されませんが、一部の MDX ポリシーを MAM アクセスを拒否するのに使用できます。この拒否は、ジェイルブレイクデバイスまたは Root 化済みデバイスなどのシステム設定に基づいて行われます。
- ユーザーは初回使用時に、MDM を使用してデバイスを登録するかどうかを選択できます。

短所

- MAM リソースを MDM に登録されていないデバイスで使用できる。
- MDM のポリシーとアクションを、MDM に登録されているデバイスでしか使用できない。

緩和オプション

- コンプライアンスに違反した場合はユーザーが責任を負うという企業の契約条件に対して、本人の同意を得ます。管理者に「管理されないデバイス」を監視させます。
- アプリケーションタイマーを使用して、アプリケーションアクセスとセキュリティを管理します。タイムアウト値を小さくするとセキュリティは向上しますが、ユーザーエクスペリエンスに影響する場合があります。

MDM 登録を必要とする場合

長所

- MAM リソースへのアクセスを MDM が管理するデバイスのみに制限できる。
- MDM のポリシーとアクションを、必要に応じて環境内のすべてのデバイスに適用できる。
- ユーザーがデバイス登録をオプトアウトすることはできない。

短所

- すべてのユーザーを MDM に登録する必要がある。
- 個人用デバイスの企業管理に反対するユーザーへの導入が減る可能性がある。

緩和オプション

- デバイス上での Citrix Endpoint Management の実際の管理対象や、管理者がどの情報にアクセスできるかについてユーザーに説明する。

デバイスの要件

November 29, 2023

展開で検討すべき重要なポイントは、展開を計画するデバイスセットです。iOS、Android、および Windows プラットフォームでは、多くの選択肢があります。Citrix Endpoint Management でサポートされるデバイスについて詳しくは、「サポート対象のデバイスプラットフォーム」を参照してください。

独自のデバイス（Bring Your Own Devive：BYOD）環境では、サポート対象のプラットフォームを混在させることができます。ただし、登録可能なデバイスについてユーザーに通知するときは、サポート対象のデバイスプラットフォームの記事に記載されている制限事項を考慮してください。ご使用の環境で 1 台または 2 台のデバイスだけを許可する場合でも、Citrix Endpoint Management は iOS、Android、および Windows デバイスで機能が若干異なります。各プラットフォームで異なる機能セットを使用できます。

また、すべてのアプリが、タブレットとスマートフォン両方のフォームファクタを対象とした設計になっているわけではありません。広範囲に変更を加える前にアプリをテストして、アプリを展開するデバイスの画面に合わせるようにしてください。

登録要素を検討することもできます。Apple と Google ではエンタープライズ登録プログラムを提供しています。Apple Deployment ProgramやGoogle Android Enterpriseを通じて、あらかじめ従業員用に設定されたデバイスを購入できます。

登録の詳細については、「User enrollment options（ユーザー登録オプション）」を参照してください。

セキュリティとユーザーエクスペリエンス

March 15, 2024

すべての組織にとってセキュリティは重要ですが、その一方でセキュリティとユーザーエクスペリエンスのバランスをとる必要があります。たとえば、ユーザーにとって使いにくいセキュリティが厳しい環境があります。また、ユーザーにとって使いやすいものの、アクセス制御が厳しくない環境もあります。この仮想ハンドブックの他のセクションでは、セキュリティ機能について詳しく説明します。この記事では、一般的なセキュリティ上の問題と、Citrix Endpoint Management で使用できるセキュリティオプションの概要を説明します。

各ユースケースで留意する重要な考慮事項は次のとおりです：

- 特定のアプリ、デバイス全体、またはその両方を保護しますか。
- どのような方法でユーザーの ID が認証されるようにしますか。LDAP、証明書ベースの認証、またはこの 2 つの組み合わせを使用しますか。
- ユーザーのセッションがタイムアウトするまでどのくらいの期間を設定しますか。バックグラウンドサービス、Citrix ADC、およびオフラインでのアプリへのアクセスでは、タイムアウト値が異なることに留意してください。

- ユーザーがデバイスレベルのパスコードやアプリレベルのパスコードを設定するようにしますか。サインインの試行を何回許可しますか? MAM で実装できるアプリごとの追加の認証要件と、ユーザーによってこれがどのように受け止められるかに留意してください。
- ユーザーに対して、他にどのような制限を加えますか。Siri などのクラウドサービスへのアクセスをユーザーに許可しますか。使用できるそれぞれのアプリで、ユーザーができること、およびできないことは何ですか。オフィス内にいるときに携帯データ通信プランが消費されるのを防ぐために、企業のネットワーク（Wi-Fi）ポリシーを導入する必要がありますか。

アプリかデバイスか

最初に考慮すべき点の 1 つは、次のどの範囲でセキュリティを確保するかです:

- 特定のアプリのみ（モバイルアプリ管理、または MAM）
- デバイス全体（モバイルデバイス管理、または MDM）。
- MDM + MAM

一般に、デバイスレベルの制御が不要な場合は、モバイルアプリを管理すれば十分です。これは特に、BYOD（Bring Your Own Device）がサポートされている組織に当てはまります。

Citrix Endpoint Management の管理対象外デバイスを持つユーザーは、アプリストアからアプリをインストールできます。選択的ワイプや完全なワイプなどのデバイスレベルの制御ではなく、アプリポリシーに従ってアプリへのアクセスを制御します。設定した値によっては、ポリシーにより、デバイスは Citrix Endpoint Management を定期的にチェックし、アプリの実行が引き続き許可されていることを確認するように求められます。

MDM を使用すると、デバイス上のすべてのソフトウェアのインベントリを取得する機能など、デバイス全体をセキュリティ保護できます。デバイスがジェイルブレイクされているか Root 化されている場合、安全でないソフトウェアがインストールされている場合に、登録を阻止することができます。ただし、このレベルで制御すると、ユーザーは自分が使用する個人用デバイスに対してこのような権限を許可することに慎重になるため、登録率が低下する可能性があります。

認証

認証は、ユーザーエクスペリエンスの重要な部分を占めています。既に Active Directory を実行している組織では、Active Directory を使用することが、ユーザーをシステムにアクセスさせる最も簡単な方法です。

そのほかに、認証におけるユーザーエクスペリエンスで重要な要素となるのがタイムアウトです。環境のセキュリティレベルが高い場合、ユーザーはシステムにアクセスするたびにサインインが必要なことがあります。このオプションは、組織やユースケースによっては理想的ではないことがあります。

ユーザーエントロピー

セキュリティを強化するために、ユーザーエントロピー と呼ばれる機能を有効にすることができます。Citrix Secure Hub や他のアプリでは、パスワード、PIN、および証明書などの共通データを共有することで、すべてが適正に機能するようになっています。この情報は、Citrix Secure Hub 内の汎用コンテナに保存されます。［シークレットの暗号化］オプションでユーザーエントロピーを有効にすると、Citrix Endpoint Management は UserEntropy という名前のコンテナを作成し、汎用コンテナからこの新しいコンテナに情報を移動させます。Citrix Secure Hub や他のアプリがこのデータにアクセスするには、ユーザーはパスワードまたは PIN を入力する必要があります。

ユーザーエントロピーを有効にすると、複数の場所で認証が強化されます。その結果、アプリが UserEntropy コンテナ内の共有データ（パスワード、PIN、証明書）にアクセスするたびに、ユーザーが認証する必要があります。

ユーザーエントロピーについては、「MDX Toolkit について」を参照してください。ユーザーエントロピーをオンにする場合は、関連する設定項目を ［クライアントプロパティ］ で見つけることができます。

ポリシー

MDX ポリシーと MDM ポリシーは、組織に大きな柔軟性をもたらす一方で、ユーザーが制限される場合もあります。状況によってはこの制限が必要な場合もありますが、ポリシーによってシステムが使用できなくなることもあります。たとえば、外部に機密データが送信される可能性のある、Siri や iCloud などのクラウドアプリケーションへのアクセスを禁止する必要がある場合、これらのサービスへのアクセスを禁止するポリシーを設定できますが、このようなポリシーによって意図しない結果がもたらされる可能性もあることに注意してください。たとえば、iOS キーボードマイクはクラウドへのアクセスが必要なことに注意してください。

アプリ

エンタープライズモビリティ管理（EMM：Enterprise Mobility Management）は、モバイルデバイス管理（MDM：Mobile Device Management）とモバイルアプリケーション管理（MAM：Mobile Application Management）に分けられます。MDM を利用するとモバイルデバイスを保護し、制御できる一方、MAM ではアプリケーションの配信と管理を簡単に行えます。BYOD（Bring Your Own Device）の導入率が増加した場合、一般的には、以下の実行に役立つ Citrix Endpoint Management などの MAM ソリューションを実装します：

- アプリ配信
- ソフトウェアライセンス
- 構成
- アプリのライフサイクル管理

Citrix Endpoint Management を使用すると、データの漏洩などのセキュリティ上の脅威を防ぐように特定の MAM ポリシーと VPN 設定を構成し、こうしたアプリの保護をさらに強化できます。Citrix Endpoint Management は柔軟性に優れているため、組織は同一の環境内に MDM と MAM の両方の機能を混在させることができます。

Citrix Endpoint Management は、モバイルデバイスへのアプリ配信機能に加えて、MDX テクノロジによるアプリのコンテナ化機能も備えています。MDX では、プラットフォームが提供するデバイスレベルの暗号化とは別の暗号化によってアプリを保護します。アプリをワイプまたはロックできます。ポリシーベースで詳細に制御できます。独立系ソフトウェアベンダー（ISV：Independent Software Vendor）では、Mobile Apps SDK を使用してこうした制御を行うことができます。

企業の環境では、ユーザーは職務の助けとしてさまざまなモバイルアプリを利用しています。こうしたアプリには、パブリックアプリストアのアプリや社内アプリ、ネイティブアプリも含まれます。Citrix Endpoint Management では、これらのアプリを次のように分類しています：

パブリックアプリ：これらのアプリには、Apple App Store や Google Play などのパブリックアプリストアで無料または有料で提供されているアプリが含まれます。組織外のベンダーの多くは、パブリックアプリストアで自社のアプリを公開しています。こうすることで、ベンダーの顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズによっては、組織内でパブリックアプリが数多く使用される場合があります。こうしたアプリには、GoToMeeting、Salesforce、EpicCare などがあります。

Citrix では、パブリックアプリストアからアプリバイナリを直接ダウンロードすることおよび、こうしたバイナリを社内配布用に MDX Toolkit でラップすることはサポートしていません。MDX 対応サードパーティアプリケーションをラップするには、アプリベンダーに連絡してアプリのバイナリを入手します。MDX Toolkit を使用してバイナリをラップするか、MAM SDK をバイナリと統合できます。

社内アプリ：多くの組織には社内開発者がおり、特定の機能を備え、組織内で独自に開発および配布されるアプリを作成しています。組織によっては、ISV から提供されるアプリを導入している場合もあります。こうしたアプリは、ネイティブアプリとして展開するか、Citrix Endpoint Management などの MAM ソリューションを使用してコンテナ化できます。たとえば、医療機関で、医師が患者の情報をモバイルデバイスで確認できる社内アプリを作成したとします。さらに、アプリを MAM SDK 対応にするまたは MDM ラップすることで、患者の情報を保護するとともに、バックエンドの患者データベースサーバーへの VPN アクセスを有効化できます。

Web アプリおよび **SaaS** アプリ：これらのアプリには、内部ネットワークからアクセスするアプリ（Web アプリ）やパブリックネットワーク経由でアクセスするアプリ（SaaS）が含まれます。Citrix Endpoint Management では、さまざまなアプリコネクタを使用して、カスタムの Web アプリおよび SaaS アプリを作成することもできます。これらのアプリコネクタを利用することで、既存の Web アプリへのシングルサインオン（SSO：Single Sign-On）を簡単に行えます。詳しくは、「アプリコネクタの種類」を参照してください。たとえば、Google Apps 向けのセキュリティアサーションマークアップランゲージ（SAML：Security Assertion Markup Language）を基にした、SSO 用の Google Apps SAML を使用できます。

業務用モバイルアプリ：業務用モバイルアプリは Citrix が開発したアプリであり、Citrix Endpoint Management ライセンスに含まれています。詳しくは、「業務用モバイルアプリについて」を参照してください。Citrix は、それ以外にもビジネス対応アプリを提供しています。ISV は、Mobile Apps SDK を使用してビジネス対応アプリを開発しています。

HDX アプリ： HDX アプリは StoreFront で公開される、Windows でホストされたアプリです。Citrix Virtual Apps and Desktops 環境を使用している場合、こうしたアプリを Citrix Endpoint Management に統合し、登録済みユーザーに公開することができます。

基になる構成およびアーキテクチャは、Citrix Endpoint Management で展開および管理するモバイルアプリの種類によって異なります。たとえば、1 つのアプリを権限レベルの異なる複数のユーザーグループが使用する場合、別々のデリバリーグループを作成して、このアプリを 2 つのバージョンで展開する必要があります。さらに、ユーザーデバイスでのポリシーの不一致を避けるため、ユーザーグループのメンバーシップが相互に排他的であることを確認します。

iOS アプリケーションのライセンスは、Apple の一括購入で管理することもできます。このオプションでは、Apple の一括購入プログラムに登録する必要があります。また、一括購入設定を構成するには、Citrix Endpoint Management コンソールを使用する必要があります。この構成によって、一括購入ライセンスでアプリを配信できるようになります。ユースケースは多様であるため、Citrix Endpoint Management 環境を実装する前に、MAM 戦略を評価し計画することが重要です。MAM 戦略の計画は、次の事柄を定義することから始めることをお勧めします。

アプリの種類：サポートするアプリの種類を一覧にします。次に、パブリックアプリ、ネイティブアプリ、Citrix 業務用モバイルアプリ、Web アプリ、社内アプリ、ISV アプリなどに分類します。また、iOS や Android などのデバイスプラットフォームごとにもアプリを分類します。このように分類することで、アプリの種類ごとに必要な Citrix Endpoint Management 設定を調整しやすくなります。たとえば、一部のアプリはラップの対象から除外することがあります。また、アプリによってはほかのアプリとのやり取りのために、Mobile Apps SDK を使用して特殊な API を有効化する必要があります。

ネットワーク要件：アプリには、適切に設定した明確なネットワークアクセス要件を構成します。たとえば、VPN 経由で内部ネットワークにアクセスする必要があるアプリもあれば、DMZ 経由でアクセスをルーティングするためにインターネットアクセスが必要なアプリもあります。こうしたアプリが必要なネットワークに接続できるようにするには、さまざまな設定を適切に構成しなければなりません。アプリごとのネットワーク要件を定義して、アーキテクチャに関する決定を事前に確定します。この作業により、導入プロセス全体が合理化されます。

セキュリティ要件：個々またはすべてのアプリに適用されるセキュリティ要件を定義します。MDX ポリシーなどの設定は、個々のアプリに適用されます。セッションと認証の設定はすべてのアプリに適用されます。一部のアプリには、特定の暗号化、コンテナ化、ラッピング、認証、ジオフェンシング、パスコード、またはデータ共有の要件があります。展開を簡単に行うために、こうした要件の概要を事前に定めます。

展開の要件：公開したアプリを適合したユーザーのみがダウンロードできるように、ポリシーベースの展開を使用する必要のある場合があります。たとえば、特定のアプリで次の要件を適用できます：

- デバイスのプラットフォームベースの暗号化が有効になっている
- デバイスが管理されている
- デバイスがオペレーティングシステムの最小バージョンに対応している
- 特定のアプリはコーポレートユーザーのみが使用可能

適切な展開ルールまたはアクションを構成できるように、こうした要件の概要を事前に定めます。

ライセンス要件：アプリ関連のライセンス要件を記録します。こうした記録により、ライセンスの使用状況を効率的に管理できるとともに、Citrix Endpoint Management で特定のライセンス管理支援機能を構成する必要があるかを判断できます。たとえば、無料または有料の iOS アプリを展開した場合、Apple によりユーザーに Apple Store

アカウントへのサインインが求められ、アプリにライセンス要件が適用されます。こうしたアプリは、Apple の一括購入に登録することで、Citrix Endpoint Management 経由で配信および管理できます。一括購入を利用することで、ユーザーは各自の Apple Store アカウントにサインインすることなくアプリをダウンロードできるようになります。さらに、Samsung Knox などのツールには、機能を展開する前に履行する必要のある特殊なライセンス要件が備わっています。

許可リストと禁止リストの要件：ユーザーがアプリをインストールまたは使用するのを阻止できます。デバイスがコンプライアンス違反になるアプリの許可リストを作成します。次に、デバイスが非準拠になったときにトリガーするポリシーを設定します。一方で、使用が容認されるアプリが、なんらかの理由で禁止リストに該当する可能性もあります。このような場合には、許可リストにそのアプリを追加し、アプリは使用してもよいが必須ではないと示すことができます。また、新しいデバイスにあらかじめインストールされているアプリの中には、オペレーティングシステムには含まれていないものの一般的に使用されているアプリもあります。こうしたアプリは、禁止リストの方針に抵触する可能性があります。

アプリの使用例

ある医療機関が、モバイルアプリ向けの MAM ソリューションとして Citrix Endpoint Management を導入する予定を立てました。モバイルアプリは、コーポレートユーザーおよび BYOD ユーザーに配信されます。IT 部門は、次のアプリを配信および管理することを決定しました。

- 業務用モバイルアプリ： Citrix が提供する iOS アプリおよび Android アプリ。
- **Citrix Files**：共有データにアクセスし、ファイルを共有、同期、編集するためのアプリ。

パブリックアプリストア

- **Citrix Secure Hub**：すべてのモバイルデバイスで Citrix Endpoint Management との通信に使用するクライアント。IT 部門では、Citrix Secure Hub クライアントを経由してセキュリティ設定、構成、およびモバイルアプリをモバイルデバイスにプッシュします。Android デバイスおよび iOS デバイスは、Citrix Secure Hub 経由で Citrix Endpoint Management に登録されます。
- **Citrix Workspace** アプリ： Citrix Virtual Apps でホストされているモバイルデバイスアプリ上で開くことのできるモバイルアプリ。
- **GoToMeeting**：ほかのコンピューターユーザー、顧客、クライアント、同僚とインターネット経由でリアルタイムに話し合うことができる、オンライン会議、デスクトップ共有、ビデオ会議用クライアント。
- **Salesforce1**：モバイルデバイスから Salesforce へのアクセスを可能にし、あらゆる Salesforce ユーザーが統一されたエクスペリエンスで Chatter、CRM、カスタムアプリ、およびビジネスプロセスを利用できるようにするモバイルアプリ。
- **RSA SecurID**： 2 要素認証用のソフトウェアベーストークン。
- **EpicCare** アプリ：医療従事者がモバイルデバイスで患者のカルテおよびリスト、スケジュールに安全にアクセスし、メッセージを通信できるようにするアプリ。
  - **Haiku**： iPhone および Android スマートフォン向けのモバイルアプリ。

  - **Canto**: iPad 用モバイルアプリ
  - **Rover**: iPhone および iPad 用のモバイルアプリ。

HDX: Citrix Virtual Apps は HDX アプリを Citrix Workspace に配信します。

- **Epic Hyperspace**: 電子カルテ管理用の Epic のクライアントアプリケーション。

ISV

- **Vocera**: iPhone や Android スマートフォンで時間や場所を問わず Vocera 音声技術を利用できるようにする、HIPAA に準拠したボイスオーバー IP およびメッセージ用モバイルアプリ。

社内アプリ

- **HCMail**: 暗号化されたメッセージを作成し、内部メールサーバー上のアドレス帳を検索して、暗号化されたメッセージをメールクライアントで連絡先へ送信できるアプリ。

社内 **Web** アプリ

- **PatientRounding**: 複数の部署で患者の健康情報の記録に使用する Web アプリケーション。
- **Outlook Web Access**: Web ブラウザー経由でメールにアクセスできるようになります。
- **SharePoint**: 組織全体でのファイルおよびデータの共有に使用します。

次の表に、MAM の構成に必要な基本情報を示します。

アプリ名	アプリの種類	MDX によるラップ	iOS	Android
Citrix Secure Mail	業務用モバイルアプリ	バージョン 10.4.1 以降では ×	はい	はい
Citrix Secure Web	業務用モバイルアプリ	バージョン 10.4.1 以降では ×	はい	はい
Citrix Files	業務用モバイルアプリ	バージョン 10.4.1 以降では ×	はい	はい
Citrix Secure Hub	パブリックアプリ	-	はい	はい
Citrix Workspace アプリ	パブリックアプリ	-	はい	はい
GoToMeeting	パブリックアプリ	-	はい	はい
SalesForce1	パブリックアプリ	-	はい	はい
RSA SecurID	パブリックアプリ	-	はい	はい
Epic Haiku	パブリックアプリ	-	はい	はい
Epic Canto	パブリックアプリ	-	はい	いいえ

アプリ名	アプリの種類	MDX によるラップ	iOS	Android
Epic Rover	パブリックアプリ	-	はい	いいえ
Epic Hyperspace	HDX アプリ	-	はい	はい
Vocera	ISV アプリ	はい	はい	はい
HCMail	社内アプリ	はい	はい	はい
PatientRounding	Web アプリ	-	はい	はい
Outlook Web Access	Web アプリ	-	はい	はい
SharePoint	Web アプリ	-	はい	はい

次の表に、Citrix Endpoint Management での MAM ポリシー構成の参考要件を示します。

アプリ名	VPN の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	デバイスのプラットフォームベースの暗号化
Citrix Secure Mail	Y	選択的に許可	許可	不要
Citrix Secure Web	Y	許可	許可	不要
Citrix Files	Y	許可	許可	不要
Citrix Secure Hub	Y	-	-	-
Citrix Workspace アプリ	Y	-	-	-
GoToMeeting	N	-	-	-
SalesForce1	N	-	-	-
RSA SecurID	N	-	-	-
Epic Haiku	Y	-	-	-
Epic Canto	Y	-	-	-
Epic Rover	Y	-	-	-
Epic Hyperspace	Y	-	-	-
Vocera	Y	禁止	禁止	不要
HCMail	Y	禁止	禁止	必須
PatientRounding	Y	-	-	必須

アプリ名	VPN の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	デバイスのプラットフォームベースの暗号化
Outlook Web Access	Y	-	-	不要
SharePoint	Y	-	-	不要

アプリ名	プロキシのフィルタリング	ライセンス	ジオフェンシング	Mobile Apps SDK	オペレーティングシステムの最小バージョン
Citrix Secure Mail	必須	-	選択的に必須化	-	適用する
Citrix Secure Web	必須	-	不要	-	適用する
Secure Notes	必須	-	不要	-	適用する
Citrix Files	必須	-	不要	-	適用する
Citrix Secure Hub	不要	一括購入	不要	-	適用しない
Citrix Workspace アプリ	不要	一括購入	不要	-	適用しない
GoToMeeting	不要	一括購入	不要	-	適用しない
SalesForce1	不要	一括購入	不要	-	適用しない
RSA SecurID	不要	一括購入	不要	-	適用しない
Epic Haiku	不要	一括購入	不要	-	適用しない
Epic Canto	不要	一括購入	不要	-	適用しない
Epic Rover	不要	一括購入	不要	-	適用しない
Epic Hyperspace	不要	-	不要	-	適用しない
Vocera	必須	-	必須	必須	適用する
HCMail	必須	-	必須	必須	適用する
PatientRounding	必須	-	不要	-	適用しない
Outlook Web Access	必須	-	不要	-	適用しない

アプリ名	プロキシのフィルタリング	ライセンス	ジオフェンシング	Mobile Apps SDK	オペレーティングシステムの最小バージョン
SharePoint	必須	-	不要	-	適用しない

ユーザーコミュニティ

すべての組織は、異なる機能的役割を持つ多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーのデバイスを通して提供されるさまざまなリソースを使用して、さまざまなタスクを実行しオフィス機能を果たします。ユーザーは、提供されたモバイルデバイスを使用して、自宅やリモートオフィスで作業する場合もあります。また、特定のセキュリティコンプライアンスルールの対象となるツールへのアクセスが許可された個人のモバイルデバイスを使用する場合もあります。

職務でモバイルデバイスを使用するユーザーコミュニティが増えるにつれ、データ漏洩を防止するために、エンタープライズモビリティ管理（EMM）が非常に重要になります。EMM は、組織のセキュリティ制限を実施するためにも重要です。効率的で高度なモバイルデバイス管理を実現するために、ユーザーコミュニティを分類することができます。そうすることにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーを適切なユーザーに適用できます。

次の例は、医療機関のユーザーコミュニティにおける EMM 向けの分類方法を示したものです。

ユーザーコミュニティの使用例

この医療機関の例では、ネットワークやアフィリエイトの従業員、ボランティアなどの複数のユーザーに技術リソースやアクセスを提供します。この組織は EMM ソリューションを非幹部ユーザーのみに展開することを選択しました。

この医療機関のユーザー役割と機能は、医療、医療以外、契約社員などのサブグループに分けられます。指定されたユーザーが企業のモバイルデバイスを受け取ります。その他のユーザーは個人のデバイスから限られた企業リソースにアクセスできます。適切なレベルのセキュリティ制限を実施し、データ漏洩を防止するために、この組織では、登録された各デバイスを企業の IT 部門が管理することに決定しました。これらのデバイスには、企業所有のデバイスまたはユーザー所有のデバイス（BYOD）の両方があります。また、ユーザーが登録できるデバイスは 1 台のみです。

以下のセクションでは、各サブグループの役割と機能の概要について説明します。

医療

- 看護師
- 医師（医師、外科医など）
- スペシャリスト（栄養士、麻酔医、放射線科医、心臓病専門医、がん専門医など）
- 外部の医師（外来の医師とリモートオフィスで作業するオフィスワーカー）

- 在宅医療サービス（患者の往診で医療サービスを行うオフィスワーカーとモバイルワーカー）
- 研究スペシャリスト（医薬における問題解決のための臨床研究を行う 6 つの研究機関のナレッジワーカーとパワーユーザー）
- 教育と訓練（教育と訓練に従事する看護師、医師、スペシャリスト）

医療以外

- 共通サービス（人事、給与、財務、サプライチェーンサービスなどのさまざまなバックオフィス機能を果たすオフィスワーカー）
- 医療サービス（管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、総合的健康管理、患者アクセスソリューション、収益サイクルソリューションなどの、さまざまな医療管理、管理サービス、ビジネスプロセスソリューションをプロバイダーに提供するオフィスワーカー）
- サポートサービス（福利厚生管理、医療の統合、コミュニケーション、報酬および業績管理、施設および土地サービス、ヒューマンリソーステックシステム、情報サービス、内部監査およびプロセス改善など、医療以外のさまざまな機能を果たすオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するさまざまな機能を果たすオフィスワーカーとモバイルワーカー）

契約社員

- メーカーやベンダーのパートナー（オンサイト、またはサイト間 VPN 経由でリモート接続された、医療以外のさまざまなサポート機能を提供する人々）

上記の情報に基づいて、この医療機関では以下のエンティティを作成しました。Citrix Endpoint Management のデリバリーグループについて詳しくは、「リソースの展開」を参照してください。

Active Directory 組織単位（**OU**）とグループ　**OU =** Citrix Endpoint Management リソースの場合:

- OU = 医療; グループ =
  - XM-看護師
  - XM-医師
  - XM-スペシャリスト
  - XM-外部の医師
  - XM-在宅医療サービス
  - XM-研究スペシャリスト
  - XM-教育と訓練
- OU = 医療以外; グループ =
  - XM-共通サービス
  - XM-医療サービス
  - XM-サポートサービス
  - XM-慈善プログラム

Citrix Endpoint Management のローカルユーザーとグループ　グループ = 契約社員、ユーザー =

- ベンダー 1
- ベンダー 2
- ベンダー 3
- …ベンダー 10

Citrix Endpoint Management のデリバリーグループ

- 医療-看護師
- 医療-医師
- 医療-スペシャリスト
- 医療-外部の医師
- 医療-在宅医療サービス
- 医療-研究スペシャリスト
- 医療-教育と訓練
- 医療以外-共通サービス
- 医療以外-医療サービス
- 医療以外-サポートサービス
- 医療以外-慈善プログラム

デリバリーグループとユーザーグループのマッピング

Active Directory グループ	Citrix Endpoint Management のデリバリーグループ
XM-看護師	医療-看護師
XM-医師	医療-医師
XM-スペシャリスト	医療-スペシャリスト
XM-外部の医師	医療-外部の医師
XM-在宅医療サービス	医療-在宅医療サービス
XM-研究スペシャリスト	医療-研究スペシャリスト
XM-教育と訓練	医療-教育と訓練
XM-共通サービス	医療以外-共通サービス
XM-医療サービス	医療以外-医療サービス
XM-サポートサービス	医療以外-サポートサービス
XM-慈善プログラム	医療以外-慈善プログラム

デリバリーグループとリソースのマッピング　次の表は、この使用例で各デリバリーグループに割り当てられたリソースを示しています。最初の表は、モバイルアプリの割り当てを示しています。2 番目の表はパブリックアプリ、HDX アプリ、デバイス管理リソースを示しています。

Citrix Endpoint Management のデリバリーグループ	Citrix モバイルアプリ	パブリックモバイルアプリ	HDX モバイルアプリ
医療-看護師	X		
医療-医師			
医療-スペシャリスト			
医療-外部の医師	X		
医療-在宅医療サービス	X		
医療-研究スペシャリスト	X		
医療-教育と訓練		X	X
医療以外-共通サービス		X	X
医療以外-医療サービス		X	X
医療以外-サポートサービス	X	X	X
医療以外-慈善プログラム	X	X	X
契約社員	X	X	X

Citrix Endpoint Management のデリバリーグループ	パブリックアプリ: RSA SecurID	パブリックアプリ: EpicCare Haiku	HDX アプリ: Epic Hyperspace	パスコードポリシー	デバイスの制限	自動化された操作	ネットワークポリシー
医療-看護師							X
医療-医師					X		
医療-スペシャリスト							
医療-外部の医師							

Citrix Endpoint Management のデリバリーグループ	パブリックアプリ：RSA SecurID	パブリックアプリ：EpicCare Haiku	HDX アプリ：Epic Hyperspace	パスコードポリシー	デバイスの制限	自動化された操作	ネットワークポリシー
医療-在宅医療サービス							
医療-研究スペシャリスト							
医療-教育と訓練		X	X				
医療以外-共通サービス		X	X				
医療以外-医療サービス		X	X				
医療以外-サポートサービス		X	X				

注意事項と考慮事項

- Citrix Endpoint Management は、初期構成時に「すべてのユーザー」というデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしないと、すべての Active Directory ユーザーに Citrix Endpoint Management への登録権限が付与されます。
- Citrix Endpoint Management は、LDAP サーバーとの動的接続により Active Directory のユーザーとグループをオンデマンドで同期します。
- ユーザーが Citrix Endpoint Management にマップされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが複数のグループのメンバーである場合、Citrix Endpoint Management は、ユーザーを Citrix Endpoint Management にマップされているグループにのみ分類します。

セキュリティ要件

Citrix Endpoint Management 環境を展開する場合、セキュリティ上のさまざまな点を考慮する必要が生じてきます。さまざまな部分や設定が連動しています。このため、許容できる保護レベルを確保するためにどこから始めたらいいのか、または何を選択すべきかがわからない場合があります。これらの選択を簡単にするために、次の表では、「高」、「より高い」、および「最高」のセキュリティの推奨事項を示しています。

セキュリティの問題だけでは、MAM、MDM+MAM とオプションの MDM、または MDM+MAM と必須の MDM のいずれのモードでデバイスを登録するかを決定することはできません。管理モードを選択する前に、ユースケースの要件を確認して、セキュリティの問題を軽減できるかどうかを判断することが重要です。

高：この設定を使用すると、ほとんどの組織で許容可能な基本レベルのセキュリティを維持しながら、最適なユーザーエクスペリエンスを実現できます。

より高い：この設定では、セキュリティとユーザービリティ間でよりバランスがとれています。

最高：この推奨事項に従うと、高いレベルのセキュリティが実現しますが、ユーザービリティとユーザーへの導入が犠牲になります。

管理モードのセキュリティに関する考慮事項

次の表は、各セキュリティレベルでの管理モードを示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
MAM、MDM+MAM	MDM + MAM	MDM + MAM

注：

- 使用例によっては、MAM のみの展開でセキュリティ要件を満たし、優れたユーザーエクスペリエンスを提供できる場合もあります。
- アプリのコンテナ化のみでビジネスとセキュリティ上のすべての要件が満たされる BYOD のような使用例では、MAM のみモードをお勧めします。
- 高セキュリティ環境（および企業がデバイスを支給）の場合、利用可能なすべてのセキュリティ機能を利用するために MDM + MAM をお勧めします。

Citrix ADC と **NetScaler Gateway** のセキュリティに関する考慮事項

次の表は、各セキュリティレベルの Citrix ADC および NetScaler Gateway の推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
Citrix ADC は推奨。NetScaler Gateway は MAM と MDM+MAM に必須	Citrix Endpoint Management が DMZ 内にある場合は、SSL ブリッジを使用した標準の NetScaler for XenMobile ウィザード構成。	エンドツーエンド暗号化による SSL オフロード

注:

- Citrix Endpoint Management サーバーを NAT や既存のサードパーティ製プロキシ、またはロードバランサー経由でインターネットに公開することは、MDM のオプションになります。ただしこの場合、SSL トラフィックは Citrix Endpoint Management サーバー上で終端するため、セキュリティ上のリスクが発生する可能性があります。
- 高度なセキュリティ環境を実現するには、通常 NetScaler Gateway とデフォルトの Citrix Endpoint Management 構成の組み合わせがセキュリティ要件を満たしているか、それ以上の条件を備えている必要があります。
- 最高水準のセキュリティが求められる MDM 登録を実現するには、SSL の終端を NetScaler Gateway にすることで、エンドツーエンドの SSL 暗号化を維持しながら境界でトラフィックを検査できます。
- SSL/TLS 暗号を定義するオプション。
- 詳しくは、「NetScaler Gateway および Citrix ADC との統合」を参照してください。

登録のセキュリティに関する考慮事項

次の表は、各セキュリティレベルの Citrix ADC および NetScaler Gateway の推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。	招待のみの登録セキュリティモード。Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。	デバイス ID に関連付けられた登録セキュリティモード。Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。

> 注:
>
> - 事前定義された Active Directory グループ内のユーザーのみに登録を制限することをお勧めします。そのためには、組み込みのすべてのユーザーデリバリーグループを無効にする必要があります。
> - 登録招待状を使用すると、招待状を持つユーザーだけが登録できるように制限できます。登録招待状は、Windows デバイスでは利用できません。
> - 2 要素認証ソリューションとしてワンタイム PIN（OTP）による登録招待状を使用し、ユーザーが登録で

> きるデバイス数を制御できます（OTP の招待状は Windows デバイスでは利用できません）。

デバイスのパスコードのセキュリティに関する考慮事項

次の表は、各セキュリティレベルでのデバイスのパスコードの推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
推奨。デバイスレベルの暗号化には高いセキュリティが必要です。MDM で適用できます。MDX ポリシー、非準拠のデバイスの動作を使用して、MAM のみで必要な設定にすることができます。	MDM、MAM、または MDM+MAM ポリシーを使用して適用されます。	MDM および MDX ポリシーを使用して適用されます。MDM の複雑なパスコードポリシー。

> 注:
>
> - デバイスのパスコードを使用することをお勧めします。
> - MDM ポリシーを使用してデバイスのパスコードを適用できます。
> - MDX ポリシーを使用して、管理対象アプリを使用するためのデバイスのパスコードを必須にすることができます（BYOD の使用例など）。
> - MDM+MAM 登録では、セキュリティを強化するために MDM と MDX のポリシーオプションを組み合わせることをお勧めします。
> - セキュリティ要件が最も高い環境では、複雑なパスコードポリシーを構成し、MDM でこのポリシーを適用できます。デバイスがパスコードポリシーに準拠していない場合は、管理者に通知したり、デバイスの選択的またはフルワイプを発行したりする自動アクションを構成できます。

アプリ

March 15, 2024

エンタープライズモビリティ管理（EMM：Enterprise Mobility Management）は、モバイルデバイス管理（MDM：Mobile Device Management）とモバイルアプリケーション管理（MAM：Mobile Application Management）に分けられます。MDM を利用するとモバイルデバイスを保護し、制御できる一方、MAM ではアプリケーションの配信と管理を簡単に行えます。BYOD（Bring Your Own Device）の導入率が増加した場合、一般的には、Citrix Endpoint Management などの MAM ソリューションを実装します。Citrix Endpoint Management はアプリケーション配信、ソフトウェアライセンス、構成、アプリケーションライフサイクル管理を支援します。ユーザーに MDM 管理を選択することを要求または許可することもできます。

Citrix Endpoint Management では、データの漏洩などのセキュリティ上の脅威を防ぐように MAM ポリシーと VPN 設定を構成し、アプリを保護します。組織は、MAM-only または MDM+MAM モードで柔軟にデバイスを登録できます。

Citrix Endpoint Management は、モバイルデバイスへのアプリ配信機能に加えて、MDX テクノロジによるアプリのコンテナ化機能も備えています。アプリはポリシーベースで詳細に制御できます。独立系ソフトウェアベンダー（ISV：Independent Software Vendor）では、Mobile Apps SDK を使用してこうした制御を行うことができます。

企業の環境では、ユーザーは職務の助けとしてさまざまなモバイルアプリを利用しています。こうしたアプリには、パブリックアプリストアのアプリや社内アプリ、ネイティブアプリも含まれます。Citrix Endpoint Management では、これらのアプリを次のように分類しています：

- パブリックアプリ：これらのアプリには、Apple App Store や Google Play などのパブリックアプリストアで無料または有料で提供されているアプリが含まれます。組織外のベンダーの多くは、パブリックアプリストアで自社のアプリを公開しています。こうすることで、ベンダーの顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズによっては、組織内でパブリックアプリが数多く使用される場合があります。こうしたアプリには、GoToMeeting、Salesforce、EpicCare などがあります。
  - **MAM SDK** を使用する場合：アプリベンダーからアプリのバイナリを入手します。その後、MAM SDK をアプリに統合します。
  - **MDX Toolkit** を使用する場合： Citrix では、パブリックアプリストアからアプリバイナリを直接ダウンロードすること、およびこうしたバイナリを社内配布用に MDX Toolkit でラップすることはサポートしていません。サードパーティのアプリケーションをラップするには、そのアプリのベンダーと協力してアプリのバイナリを入手します。その後、MDX Toolkit を使用してバイナリをラップすることができます。
- 社内アプリ：多くの組織には社内開発者がおり、特定の機能を備え、組織内で独自に開発および配布されるアプリを作成しています。組織によっては、ISV から提供されるアプリを導入している場合もあります。こうしたアプリは、ネイティブアプリとして展開するか、Citrix Endpoint Management などの MAM ソリューションを使用してコンテナ化できます。

  たとえば、医療機関で、モバイルデバイスで医師が患者の情報を確認できる社内アプリを作成したとします。さらに、患者の情報を保護するとともに、以下のいずれかを使用して患者データベースへの VPN アクセスを有効化できます：
  - MAM SDK
  - MDX Toolkit
- **Web** アプリおよび **SaaS** アプリ：これらのアプリには、内部ネットワークからアクセスするアプリ（Web アプリ）やパブリックネットワーク経由でアクセスするアプリ（SaaS）が含まれます。Citrix Endpoint Management では、さまざまなアプリコネクタを使用して、カスタムの Web アプリおよび SaaS アプリを作成することもできます。これらのアプリコネクタを利用することで、既存の Web アプリへのシングルサインオン（SSO：Single Sign-On）を簡単に行えます。詳しくは、「アプリコネクタの種類」を参照してくださ

い。たとえば、Google Apps 向けのセキュリティアサーションマークアップランゲージ（SAML：Security Assertion Markup Language）を基にした、SSO 用の Google Apps SAML を使用できます。

- 業務用モバイルアプリ：業務用モバイルアプリは Citrix が開発したアプリであり、Citrix Endpoint Management ライセンスに含まれています。詳しくは、「業務用モバイルアプリについて」を参照してください。Citrix では、ISV が Mobile Apps SDK を使用して開発したビジネス対応アプリも提供しています。
- **HDX** アプリ： HDX アプリは StoreFront で公開される、Windows でホストされたアプリです。Citrix Virtual Apps and Desktops と Citrix Workspace を使用する場合、登録ユーザーは HDX アプリを利用できます。

基になる構成は、Citrix Endpoint Management で展開および管理するモバイルアプリの種類によって異なります。たとえば、1 つのアプリを権限レベルの異なる複数のユーザーグループが使用する場合、別々のデリバリーグループを作成して、このアプリを 2 つのバージョンで展開する必要があります。さらに、ユーザーデバイスでのポリシーの不一致を避けるため、ユーザーグループのメンバーシップが相互に排他的であることを確認する必要があります。

iOS アプリケーションのライセンスは、Apple の一括購入で管理することもできます。この方法を使用するには、Citrix Endpoint Management コンソールで一括購入プログラムを登録し、一括購入の設定を構成する必要があります。この構成によって、一括購入ライセンスでアプリを配信できるようになります。ユースケースは多様であるため、Citrix Endpoint Management 環境を実装する前に、MAM 戦略を評価し計画することが重要です。MAM 戦略の計画は、次の事柄を定義することから始めることをお勧めします。

- アプリの種類：パブリックアプリ、ネイティブアプリ、Web アプリ、社内アプリ、ISV アプリなど、サポート予定のアプリの種類をリストアップして分類します。また、iOS や Android などのデバイスプラットフォームごとにもアプリを分類します。このように分類することで、アプリの種類ごとに必要な Citrix Endpoint Management の設定を調整しやすくなります。たとえば、一部のアプリでは、ほかのアプリとのやりとりのための特別な API を有効にするために、Mobile Apps SDK の使用が必要となる場合があります。
- ネットワーク要件：特定のネットワークアクセス要件のあるアプリの設定を構成します。たとえば、VPN 経由で内部ネットワークにアクセスする必要があるアプリもあれば、DMZ 経由でアクセスをルーティングするためにインターネットアクセスが必要なアプリもあります。こうしたアプリが必要なネットワークに接続できるようにするには、さまざまな設定を適切に構成しなければなりません。アプリごとのネットワーク要件を定義することで、アーキテクチャに関する決定事項を早期に確定し、実装プロセス全体の効率を高めることができます。
- セキュリティ要件：個々またはすべてのアプリに適用されるセキュリティ要件を定義できます。
  - MDX ポリシーなどの設定は、個々のアプリに適用されます
  - セッションと認証の設定はすべてのアプリに適用されます
  - 一部のアプリには、特定のコンテナ化、MDX、認証、ジオフェンシング、パスコード、またはデータ共有の要件があります。

  展開を簡単に行うために、こうした要件の概要を事前に定めます。Citrix Endpoint Management のセキュリティの詳細については、「セキュリティとユーザーエクスペリエンス」を参照してください。

- 展開の要件：公開したアプリを適合したユーザーのみがダウンロードできるように、ポリシーベースの展開を使用する必要のある場合があります。たとえば、特定のアプリについて、デバイスが管理対象であること、またはデバイスがオペレーティングシステムの最小バージョンを満たしていることを必須にできます。また、特定のアプリをコーポレートユーザーだけに利用可能にする必要のある場合もあります。適切な展開ルールまたはアクションを構成できるように、こうした要件の概要を事前に定めます。
- ライセンス要件：アプリ関連のライセンス要件の記録を維持します。こうした記録により、ライセンスの使用状況を効率的に管理できるとともに、Citrix Endpoint Management で特定のライセンス管理支援機能を構成するかを判断できます。たとえば、無料または有料の iOS アプリを展開した場合、Apple がアプリにライセンス要件を適用します。その結果、ユーザーは Apple Store アカウントへのサインインが必要となります。

  ただし、Apple の一括購入に登録することで、Citrix Endpoint Management を使用してこれらのアプリを配信および管理できます。一括購入を利用することで、ユーザーは各自の Apple App Store アカウントにサインインすることなくアプリをダウンロードできるようになります。

  一部のプラットフォームには、機能を展開する前に履行する必要のある特別なライセンス要件があります。
- 許可リストと禁止リストの要件：ユーザーにインストールや使用を禁止する必要のあるアプリを指定できます。禁止リストを作成することで、コンプライアンス違反イベントを定義します。次に、イベントが発生したときに起動するようにポリシーを設定できます。一方で、使用が容認されるアプリが、なんらかの理由で禁止リストに該当する可能性もあります。このような場合には、許可リストにそのアプリを追加し、アプリは使用してもよいが必須ではないと示すことができます。また、新しいデバイスにあらかじめインストールされているアプリの中には、オペレーティングシステムには含まれていないものの一般的に使用されているアプリもあります。こうしたアプリは、禁止リストの方針に抵触する可能性があります。

使用例

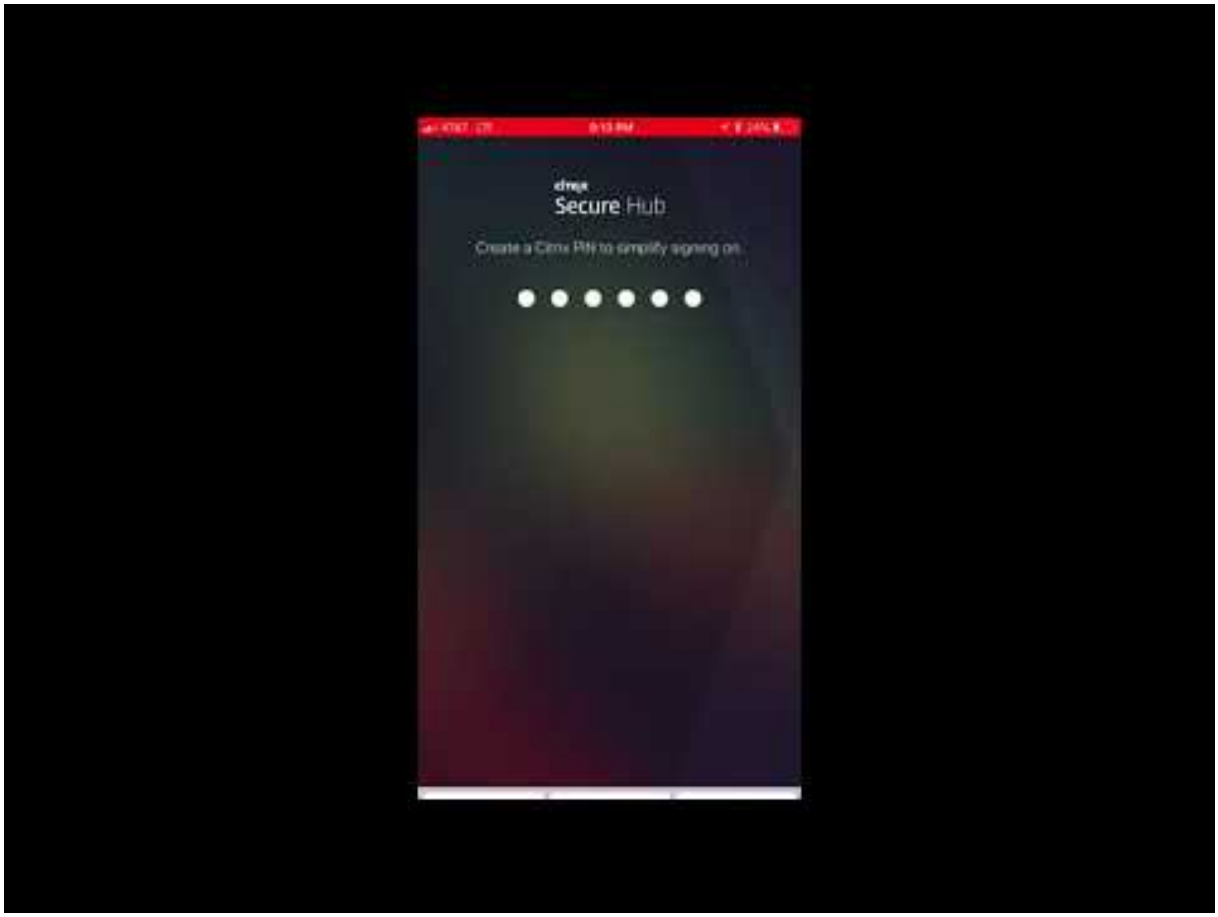
ある医療機関が、モバイルアプリ向けの MAM ソリューションとして Citrix Endpoint Management を導入する予定を立てました。モバイルアプリは、コーポレートユーザーおよび BYOD ユーザーに配信されます。IT 部門は、次のアプリを配信および管理することを決定しました。

業務用モバイルアプリ： Citrix が提供する iOS アプリおよび Android アプリ。詳しくは、「業務用モバイルアプリ」を参照してください。

Citrix Secure Hub： Citrix Endpoint Management 10.18.14 より前のバージョンを使用しているお客様の場合、セキュリティ設定、構成、モバイルアプリを Citrix Secure Hub を使用してモバイルデバイスにプッシュします。Android デバイスおよび iOS デバイスは、Citrix Secure Hub 経由で Citrix Endpoint Management に登録されます。

Citrix Endpoint Management 10.18.14 からの新規のお客様の場合、Citrix Secure Hub で Workspace アプリストアを使用できます。Citrix Secure Hub を開いても、Citrix 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。

以下は、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たビデオです。



Citrix Workspace アプリ： Citrix Workspace アプリには、既存の Citrix Receiver テクノロジ、Citrix Secure Hub、Citrix Workspace クライアントテクノロジが組み込まれています。Citrix Workspace アプリはコンテキストに応じた統合エクスペリエンスを提供します。

GoToMeeting：ほかのコンピューターユーザー、顧客、クライアント、同僚とインターネット経由でリアルタイムに話し合うことができる、オンライン会議、デスクトップ共有、ビデオ会議用クライアント。

Salesforce1：モバイルデバイスから Salesforce へのアクセスを可能にし、あらゆる Salesforce ユーザーが統一されたエクスペリエンスで Chatter、CRM、カスタムアプリ、およびビジネスプロセスを利用できるようにするモバイルアプリ。

RSA SecurID： 2 要素認証用のソフトウェアベーストークン。

EpicCare アプリ：医療従事者がモバイルデバイスで患者のカルテおよびリスト、スケジュールに安全にアクセスし、メッセージを通信できるようにするアプリ。

Haiku： iPhone および Android スマートフォン向けのモバイルアプリ。

Canto： iPad 用モバイルアプリ

Rover： iPhone および iPad 用のモバイルアプリ。

HDX：これらのアプリは、Citrix Workspace の Citrix Virtual Apps 経由で配信されます。

- **Epic Hyperspace**：電子カルテ管理用の Epic のクライアントアプリケーション。

ISV:

- **Vocera**： iPhone や Android スマートフォンで時間や場所を問わず Vocera 音声技術を利用できるようにする、HIPAA に準拠したボイスオーバー IP およびメッセージ用モバイルアプリ。

社内アプリ:

- **HCMail**：暗号化されたメッセージを作成し、内部メールサーバー上のアドレス帳を検索して、暗号化されたメッセージをメールクライアントで連絡先へ送信できるアプリ。

社内 **Web** アプリ:

- **PatientRounding**：複数の部署で患者の健康情報の記録に使用する Web アプリケーション。
- **Outlook Web Access**： Web ブラウザー経由でメールにアクセスできるようになります。
- **SharePoint**：組織全体でのファイルおよびデータの共有に使用します。

次の表に、MAM の構成に必要な基本情報を示します。

アプリ名	アプリの種類	**MDX** 対応	**iOS**	**Android**
Citrix Secure Mail	業務用モバイルアプリ	いいえ	はい	はい
Citrix Secure Web	業務用モバイルアプリ	いいえ	はい	はい
Citrix Files	業務用モバイルアプリ	いいえ	はい	はい
Citrix Secure Hub	パブリックアプリ	-	はい	はい
Citrix Workspace アプリ	パブリックアプリ	-	はい	はい
GoToMeeting	パブリックアプリ	-	はい	はい
SalesForce1	パブリックアプリ	-	はい	はい
RSA SecurID	パブリックアプリ	-	はい	はい
Epic Haiku	パブリックアプリ	-	はい	はい
Epic Canto	パブリックアプリ	-	はい	いいえ
Epic Rover	パブリックアプリ	-	はい	いいえ
Epic Hyperspace	HDX アプリ	-	はい	はい
Vocera	ISV アプリ	はい	はい	はい
HCMail	社内アプリ	はい	はい	はい

アプリ名	アプリの種類	**MDX** 対応	**iOS**	**Android**
PatientRounding	Web アプリ	-	はい	はい
Outlook Web Access	Web アプリ	-	はい	はい
SharePoint	Web アプリ	-	はい	はい

次の表に、Citrix Endpoint Management での MAM ポリシーの構成の参考要件を示します。

アプリ名	**VPN** の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	プロキシのフィルタリング	ライセンス	ジオフェンシング	**Mobile Apps SDK**	オペレーティングシステムの最小バージョン
Citrix Secure Mail	Y	選択的に許可	許可	必須	-	選択的に必須化	-	適用する
Citrix Secure Web	Y	許可	許可	必須	-	不要	-	適用する
Citrix Files	Y	許可	許可	必須	-	不要	-	適用する
Citrix Secure Hub	Y	-	-	不要	一括購入	不要	-	適用しない
Citrix Work-space アプリ	Y	-	-	不要	一括購入	不要	-	適用しない
GoToMeeting	N	-	-	不要	一括購入	不要	-	適用しない
SalesForce1	N	-	-	不要	一括購入	不要	-	適用しない
RSA SecurID	N	-	-	不要	一括購入	不要	-	適用しない
Epic Haiku	Y	-	-	不要	一括購入	不要	-	適用しない
Epic Canto	Y	-	-	不要	一括購入	不要	-	適用しない

アプリ名	**VPN** の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	プロキシのフィルタリング	ライセンス	ジオフェンシング	**Mobile Apps SDK**	オペレーティングシステムの最小バージョン
Epic Rover	Y	-	-	不要	一括購入	不要	-	適用しない
Epic Hyper-space	Y	-	-	不要	-	不要	-	適用しない
Vocera	Y	禁止	禁止	必須	-	必須	必須	適用する
HCMail	Y	禁止	禁止	必須	-	必須	必須	適用する
PatientRounding	Y	-	-	必須	-	不要	-	適用しない
Outlook Web Access	Y	-	-	必須	-	不要	-	適用しない
SharePoint	Y	-	-	必須	-	不要	-	適用しない

ユーザーコミュニティ

March 15, 2024

すべての組織は、異なる機能的役割を持つ多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーのモバイルデバイスを通して提供されるさまざまなリソースを使用して、さまざまなタスクを実行しオフィス機能を果たします。ユーザーは、提供されたモバイルデバイスを使用して、自宅やリモートオフィスで作業する場合もあります。また、特定のセキュリティコンプライアンスルールの対象となるツールへのアクセスが許可された個人のモバイルデバイスを使用する場合もあります。

モバイルデバイスを使用するユーザーコミュニティが増えるにつれ、データ漏洩を防止し、組織のセキュリティ制限を実施するために、エンタープライズモビリティ管理（EMM）が非常に重要になります。効率的で高度なモバイルデバイス管理を実現するために、ユーザーコミュニティを分類することができます。そうすることにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーを適切なユーザーに適用できます。

ユーザーコミュニティを分類するには、次のコンポーネントを使用できます:

- Active Directory 組織単位（OU）とグループ

特定の Active Directory セキュリティグループに追加されたユーザーは、ポリシーと、アプリなどのリソースを受け取ることができます。Active Directory セキュリティグループからユーザーを削除すると、以前に許可された Citrix Endpoint Management リソースへのアクセスが削除されます。

- Citrix Endpoint Management のローカルユーザーとグループ

  Active Directory にアカウントを持たないユーザーの場合は、ローカルの Citrix Endpoint Management ユーザーとしてユーザーを作成できます。ローカルユーザーをデリバリーグループに追加し、Active Directory ユーザーと同じ方法でリソースをプロビジョニングできます。

- Citrix Endpoint Management のデリバリーグループ

  権限レベルの異なるユーザーからなる複数のグループが 1 つのアプリを使用する場合は、個別のデリバリーグループの作成が必要になる場合があります。個別のデリバリーグループを使用する場合、同じアプリの 2 つの異なるバージョンを展開できます。デバイスポリシーを作成する前にデリバリーグループを作成することが推奨されます。

- デリバリーグループとユーザーグループのマッピング

  デリバリーグループと Active Directory グループのマッピングは、1 対 1 または 1 対多のいずれでもかまいません。基本のポリシーとアプリを 1 対多のデリバリーグループマッピングに割り当てます。機能に固有のポリシーとアプリを 1 対 1 のデリバリーグループマッピングに割り当てます。

- アプリのデリバリーグループとリソースのマッピング

  特定のアプリを各デリバリーグループに割り当てます。

- MDM リソースのデリバリーグループとリソースのマッピング

  アプリと特定のデバイス管理リソースを各デリバリーグループに割り当てます。たとえば、アプリの種類（パブリック、HDX など）、アプリの種類別の特定のアプリ、リソース（デバイスポリシーや自動アクションなど）を任意に組み合わせてデリバリーグループを設定します。

次の例は、医療機関のユーザーコミュニティにおける EMM 向けの分類方法を示したものです。

使用例

この医療機関の例では、ネットワークやアフィリエイトの従業員、ボランティアなどの複数のユーザーに技術リソースやアクセスを提供します。この組織は EMM ソリューションを非幹部ユーザーのみに展開することを選択しました。

この医療機関のユーザー役割と機能は、医療、医療以外、契約社員などのサブグループに分けられます。指定されたグループのユーザーが企業のモバイルデバイスを受け取ります。その他のユーザーは個人のデバイス（BYOD）から限られた企業リソースにアクセスできます。適切なレベルのセキュリティ制限を実施し、データ漏洩を防止するために、この組織では、登録された各デバイスを企業の IT 部門が管理することに決定しました。また、ユーザーが登録できるデバイスは 1 台のみです。

以下のセクションでは、各サブグループの役割と機能の概要について説明します。

医療

- 看護師
- 医師（医師、外科医など）
- スペシャリスト（栄養士、麻酔医、放射線科医、心臓病専門医、がん専門医など）
- 外部の医師（外来の医師とリモートオフィスで作業するオフィスワーカー）
- 在宅医療サービス（患者の往診で医療サービスを行うオフィスワーカーとモバイルワーカー）
- 研究スペシャリスト（医薬における問題解決のための臨床研究を行う 6 つの研究機関のナレッジワーカーとパワーユーザー）
- 教育と訓練（教育と訓練に従事する看護師、医師、スペシャリスト）

医療以外

- 共通サービス（人事、給与、財務、サプライチェーンサービスなどのさまざまなバックオフィス機能を果たすオフィスワーカー）
- 医療サービス（管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、総合的健康管理、患者アクセスソリューション、収益サイクルソリューションなどの、さまざまな医療管理、管理サービス、ビジネスプロセスソリューションをプロバイダーに提供するオフィスワーカー）
- サポートサービス（福利厚生管理、医療の統合、コミュニケーション、報酬および業績管理、施設および土地サービス、ヒューマンリソーステックシステム、情報サービス、内部監査およびプロセス改善など、医療以外のさまざまな機能を果たすオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するさまざまな機能を果たすオフィスワーカーとモバイルワーカー）

契約社員

- メーカーやベンダーのパートナー（オンサイト、またはサイト間 VPN 経由でリモート接続された、医療以外のさまざまなサポート機能を提供する人々）

上記の情報に基づいて、この医療機関では以下のエンティティを作成しました。Citrix Endpoint Management のデリバリーグループの詳細については、Citrix Endpoint Management 製品ドキュメントの「リソースの展開」を参照してください。

Active Directory 組織単位（**OU**）とグループ

OU = Citrix Endpoint Management リソース

- OU = 医療; グループ =
  - XM-看護師
  - XM-医師

  - XM-スペシャリスト
  - XM-外部の医師
  - XM-在宅医療サービス
  - XM-研究スペシャリスト
  - XM-教育と訓練

- OU = 医療以外; グループ =

  - XM-共通サービス
  - XM-医療サービス
  - XM-サポートサービス
  - XM-慈善プログラム

Citrix Endpoint Management のローカルユーザーとグループ

グループ = 契約社員、ユーザー =

- ベンダー 1
- ベンダー 2
- ベンダー 3
- …ベンダー 10

Citrix Endpoint Management のデリバリーグループ

- 医療-看護師
- 医療-医師
- 医療-スペシャリスト
- 医療-外部の医師
- 医療-在宅医療サービス
- 医療-研究スペシャリスト
- 医療-教育と訓練
- 医療以外-共通サービス
- 医療以外-医療サービス
- 医療以外-サポートサービス
- 医療以外-慈善プログラム

デリバリーグループとユーザーグループのマッピング

Active Directory グループ	Citrix Endpoint Management のデリバリーグループ
XM-看護師	医療-看護師
XM-医師	医療-医師
XM-スペシャリスト	医療-スペシャリスト
XM-外部の医師	医療-外部の医師
XM-在宅医療サービス	医療-在宅医療サービス
XM-研究スペシャリスト	医療-研究スペシャリスト
XM-教育と訓練	医療-教育と訓練
XM-共通サービス	医療以外-共通サービス
XM-医療サービス	医療以外-医療サービス
XM-サポートサービス	医療以外-サポートサービス
XM-慈善プログラム	医療以外-慈善プログラム

アプリのデリバリーグループとリソースのマッピング

	Secure Mail	Secure Web	Citrix Files	Workspace アプリ	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
医療-看護師	X	X	X					
医療-医師								
医療-スペシャリスト								
医療-外部の医師	X		X					
医療-在宅医療サービス	X		X					
医療-研究スペシャリスト	X		X					
医療-教育と訓練							X	X

	Secure Mail	Secure Web	Citrix Files	Workspace アプリ	SalesForce1	RSA SecurID	EpicCare Haiku	Epic Hyper-space
医療以外-共通サービス							X	X
医療以外-医療サービス							X	X
医療以外-サポートサービス	X		X				X	X
医療以外-慈善プログラム	X		X				X	X
契約社員	X		X	X	X		X	X

MDM リソースのデリバリーグループとリソースのマッピング

	MDM：パスコードポリシー	MDM：デバイスの制限事項	MDM：自動化された操作	MDM：ネットワークポリシー
医療-看護師				X
医療-医師		X		
医療-スペシャリスト				
医療-外部の医師				
医療-在宅医療サービス				
医療-研究スペシャリスト				
医療-教育と訓練				
医療以外-共通サービス				
医療以外-医療サービス				

	MDM：パスコードポリシー	MDM：デバイスの制限事項	MDM：自動化された操作	MDM：ネットワークポリシー
医療以外-サポートサービス				
医療以外-慈善プログラム				
契約社員				X

注意事項と考慮事項

- Citrix Endpoint Management は、初期構成時に「すべてのユーザー」というデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしないと、すべての Active Directory ユーザーに Citrix Endpoint Management への登録権限が付与されます。
- Citrix Endpoint Management は、LDAP サーバーとの動的接続により Active Directory のユーザーとグループをオンデマンドで同期します。
- ユーザーが Citrix Endpoint Management にマップされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが複数のグループのメンバーである場合、Citrix Endpoint Management は、ユーザーを Citrix Endpoint Management にマップされているグループにのみ分類します。

メール戦略

March 15, 2024

モバイルデバイスからメールに安全にアクセスできるようにすることは、組織のモビリティ管理の取り組みを推進するうえで主要な要因の 1 つです。適切なメール戦略を決定することは、Citrix Endpoint Management 設計の鍵となる要素です。Citrix Endpoint Management では、セキュリティ、ユーザーエクスペリエンス、および統合の要件に基づいて、さまざまなユースケースに対応するためのオプションを提供しています。この記事では、クライアントの選択からメールのトラフィックフローまで、最適なソリューションを選択するための典型的な設計決定プロセスと考慮事項について説明します。

メールクライアントの選択

通常、クライアントの選択は、メール戦略の設計全体において最初に実行すべき項目です。Citrix Secure Mail、特定のモバイルプラットフォームのオペレーティングシステムに含まれるネイティブメール、またはパブリックアプリストアを通じて利用できる他のサードパーティクライアントから選択できます。必要に応じて、単一の（標準）クライアントを使用したり、クライアントの組み合わせを使用したりして、ユーザーコミュニティをサポートできます。

次の表に、使用可能なさまざまなクライアントオプションで設計上考慮すべき事項を示します：

トピック	**Citrix Secure Mail**	ネイティブ（**iOS Mail** など）	サードパーティのメールクライアント
構成	MDX ポリシーによって構成された Exchange アカウントプロファイル。	MDM ポリシーによって構成された Exchange アカウントプロファイル。Android のサポートは次に限定されます：Android Enterprise。他のすべてのクライアントはサードパーティのクライアントと見なされます。	一般に、ユーザーが手動で構成する必要があります。
セキュリティ	これ自体がセキュアに設計されており、最高のセキュリティを提供します。データ暗号化レベルが強化された MDX ポリシーを使用します。Citrix Secure Mail は、MDX ポリシーによって完全に管理されているアプリです。Citrix PIN により、認証が強化されています。	ベンダーおよびアプリの機能セットに基づきます。より高いセキュリティを提供します。デバイスの暗号化設定を使用します。アプリへのアクセスでデバイスレベルの認証に依存します。	ベンダーおよびアプリの機能セットに基づきます。高いセキュリティを提供します。
統合	デフォルトで管理対象（MDX）アプリの操作を許可します。Citrix Secure Web で Web URL を開きます。Citrix Files にファイルを保存し、Citrix Files からファイルを添付します。GoToMeeting への直接参加およびダイヤルイン。	デフォルトでは、他の非管理対象（非 MDX）アプリのみ操作できます。	デフォルトでは、他の非管理対象（非 MDX）アプリのみ操作できます。

展開/ライセンス	MDM を通じて、パブリックアプリストアから直接 Citrix Secure Mail をプッシュできます。Citrix Endpoint Management の Advanced および Enterprise Edition のライセンスに含まれています。	クライアントアプリは、プラットフォームのオペレーティングシステムに含まれています。追加のライセンス要件はありません。	エンタープライズアプリとして MDM 経由で、またはパブリックアプリストアから直接、プッシュできます。アプリベンダーに基づき、関連ライセンスモデル/コスト。
サポート	クライアントおよび EMM ソリューションを提供する単一ベンダーのサポート（Citrix）。Citrix Secure Hub/アプリのデバッグログ機能にサポートの連絡先情報が埋め込まれています。サポートするクライアントは 1 つです。	ベンダーによって定義されたサポート（Apple/Google）。デバイスのプラットフォームに基づいて異なるクライアントをサポートする必要がある場合があります。	ベンダーによって定義されたサポート。サードパーティのクライアントがすべての管理対象デバイスプラットフォームでサポートされていることを前提に、1 つのクライアントをサポートします。

メールのトラフィックフローとフィルタリングに関する考慮事項

ここでは、Citrix Endpoint Management のコンテキストでのメール（ActiveSync）のトラフィックフローに関する 3 つの主要なシナリオと設計上の考慮事項について説明します。

シナリオ **1**：インターネットに接続された **Exchange**

外部クライアントをサポートする環境では、通常、Exchange ActiveSync サービスがインターネットに接続されています。モバイルの ActiveSync クライアントは、この外部に対するパスを通じて、リバースプロキシ（NetScaler Gateway など）またはエッジサーバーを介して接続します。このオプションは、ネイティブまたはサードパーティのメールクライアントを使用する場合に必要です。このため、このシナリオではこれらのクライアントが一般的な選択になります。また、一般的な方法ではありませんが、このシナリオで Citrix Secure Mail クライアントを使用することもできます。これにより、MDX ポリシーの使用とアプリの管理によって提供されるセキュリティ機能のメリットが得られます。

シナリオ **2**：**NetScaler Gateway** 経由のトンネリング（マイクロ **VPN** および **STA**）

Citrix Secure Mail の Micro VPN 機能により、Citrix Secure Mail クライアントを使用する場合はこのシナリオがデフォルトになります。この場合、Citrix Secure Mail クライアントは、NetScaler Gateway Gateway 経由で ActiveSync へのセキュリティで保護された接続を確立します。本質的に、Citrix Secure Mail は、内部ネットワークから ActiveSync に直接接続するクライアントと考えることができます。通常 Citrix のお客様は、最適なモバイル ActiveSync クライアントとして Citrix Secure Mail を標準に決定します。この決定は、1 つ目のシナリオで説明したように、インターネットに接続された Exchange Server 上で、ActiveSync サービスがインターネットに接続されないようにする取り組みの一部です。

マイクロ VPN 機能を使用できるのは、MAM SDK 対応アプリまたは MDX でラップされたアプリのみです。MDX ラッピングを使用する場合、このシナリオはネイティブクライアントには適用されません。MDX Toolkit を使用してサードパーティのクライアントをラップすることは可能ですが、この方法は一般的ではありません。ネイティブまたはサードパーティのクライアントにトンネルを介したアクセスを許可するためにデバイスレベルの VPN クライアントを使用することは煩雑であり、実行可能なソリューションではないことが実証されています。

シナリオ **3**：クラウドでホストされた **Exchange** サービス

クラウドでホストされた Exchange サービス（Microsoft Office 365 など）の普及が進んでいます。ActiveSync サービスもインターネットに接続しているため、Citrix Endpoint Management のコンテキストでは、このシナリオは 1 つ目のシナリオと同じように扱うことができます。この場合、クラウドサービスプロバイダーの要件によってクライアントの選択が決まります。一般的にこの選択には、Citrix Secure Mail や他のネイティブクライアントまたはサードパーティクライアントなど、ほとんどの ActiveSync クライアントのサポートが含まれます。

このシナリオでは、Citrix Endpoint Management は次の 3 つの領域で価値を付加できます：

- MDX ポリシーを含むクライアントと Citrix Secure Mail によるアプリの管理
- サポートされているネイティブメールクライアントでの MDM ポリシーを使用したクライアント構成
- Citrix Endpoint Management コネクタ：Exchange ActiveSync 用を使用した ActiveSync のフィルターオプション

メールトラフィックのフィルタリングに関する考慮事項

インターネットに接続している大半のサービスと同様に、パスを保護し、承認されたアクセスに対してフィルターを提供する必要があります。Citrix Endpoint Management ソリューションには、ネイティブクライアントとサードパーティクライアントに ActiveSync のフィルタリング機能を提供するために特別に設計された 2 つのコンポーネント：NetScaler Gateway コネクタ：Exchange ActiveSync 用、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用。

NetScaler Gateway コネクタ：**Exchange ActiveSync** 用

NetScaler Gateway コネクタ：Exchange ActiveSync 用は、ActiveSync トラフィックのプロキシとして NetScaler Gateway を使用して、境界で ActiveSync フィルタリングを提供します。その結果、フィルタリングコンポーネントはメールトラフィックフローのパスの一部として、メールが環境に出入りするときにインターセプトします。Exchange ActiveSync 用コネクタは、NetScaler Gateway と Citrix Endpoint Management の間の仲介役を果たします。デバイスが NetScaler Gateway 上の ActiveSync 仮想サーバーを介して Exchange と通信する場合、NetScaler Gateway は Exchange ActiveSync 用コネクタサービスに対して HTTP コールアウトを実行します。このサービスは、Citrix Endpoint Management を使用してデバイスの状態を確認します。Exchange ActiveSync 用コネクタは NetScaler Gateway に応答し、デバイスの状態に基づいて接続を許可または拒否します。また、ユーザー、エージェント、デバイスの種類や ID に基づいてアクセスをフィルターするように静的規則を構成することもできます。

この設定では、不正なアクセスを防ぐためにセキュリティレイヤーを追加して、Exchange ActiveSync サービスのインターネットへの接続を許可します。設計上の考慮事項は次のとおりです：

- **Windows Server**： Exchange ActiveSync コンポーネント用コネクタには Windows Server が必要です。
- フィルター規則のセット： Exchange ActiveSync 用コネクタは、ユーザー情報ではなくデバイスの状態と情報に基づいてフィルターするように設計されています。ユーザー ID でフィルターするように静的規則を構成することもできますが、たとえば Active Directory グループのメンバーシップに基づいてフィルターするオプションはありません。Active Directory グループのフィルターが必要な場合は、代わりに Citrix Endpoint Management コネクタ：Exchange ActiveSync 用を使用できます。
- **NetScaler Gateway** のスケーラビリティ： NetScaler Gateway を介した ActiveSync トラフィックのプロキシ要件を考慮すると、すべての ActiveSync SSL 接続によって追加されたワークロードをサポートするには、NetScaler Gateway インスタンスの適切なサイズ設定が不可欠です。
- **NetScaler Gateway** 統合キャッシュ： NetScaler Gateway 上の Exchange ActiveSync 用コネクタの構成では、統合キャッシュ機能を使用してコネクタからの応答をキャッシュします。この構成により、NetScaler Gateway では、特定のセッション内のすべての ActiveSync トランザクションに対してコネクタに要求を発行する必要がありません。適切なパフォーマンスとスケーラビリティを実現するにはこの構成も不可欠です。統合キャッシュは、NetScaler Gateway Platinum Edition で利用できます。
- カスタムのフィルターポリシー： カスタムの NetScaler Gateway ポリシーを作成して、特定の ActiveSync クライアントを標準のネイティブモバイルクライアント以外に制限する必要がある場合があります。この構成では、ActiveSync HTTP 要求と NetScaler Gateway のレスポンダーポリシーの作成に関する知識が必要です。
- **Citrix Secure Mail** クライアント： Citrix Secure Mail には、境界でのフィルターが不要なマイクロ VPN 機能が組み込まれています。一般に、Citrix Secure Mail クライアントは、NetScaler Gateway Gateway を介して接続されている場合、内部の（信頼できる）ActiveSync クライアントとして扱われます。ネイティブおよびサードパーティクライアント（Exchange ActiveSync 用コネクタを使用）、および Citrix Secure Mail クライアントのサポートが必要な場合：Citrix Secure Mail のトラフィックが、コネクタで使用される NetScaler Gateway 仮想サーバー経由でフローしないようにすることをお勧めします。これを実行するに

は、トラフィックが DNS 経由でフローし、コネクタポリシーが Citrix Secure Mail クライアントに影響を与えないようにします。

Citrix Endpoint Management 展開の NetScaler Gateway コネクタ：Exchange ActiveSync 用の図については、「アーキテクチャ」を参照してください。

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用

Citrix Endpoint Management コネクタ：Exchange ActiveSync 用は、Exchange サービスレベルで ActiveSync フィルターを提供する Citrix Endpoint Management コンポーネントです。つまり、メールが Citrix Endpoint Management 環境に到達した時ではなく、Exchange サービスに到達した後にのみフィルタリングが行われます。Mail Manager は、PowerShell を使用して Exchange ActiveSync にデバイスパートナーシップ情報のクエリを実行し、デバイスの隔離操作を通じてアクセスを制御します。これらのアクションは、Citrix Endpoint Management コネクタ：Exchange ActiveSync 用の規則条件に基づいて、デバイスを検疫に出し入れします。

NetScaler Gateway コネクタ：Exchange ActiveSync 用と同様に、Exchange ActiveSync 用コネクタでは Citrix Endpoint Management を使用してデバイスの状態を確認し、デバイスのコンプライアンスに基づいてアクセスをフィルターします。また、デバイスの種類や ID、エージェントのバージョン、Active Directory グループのメンバーシップに基づいてアクセスをフィルターするように静的規則を構成することもできます。

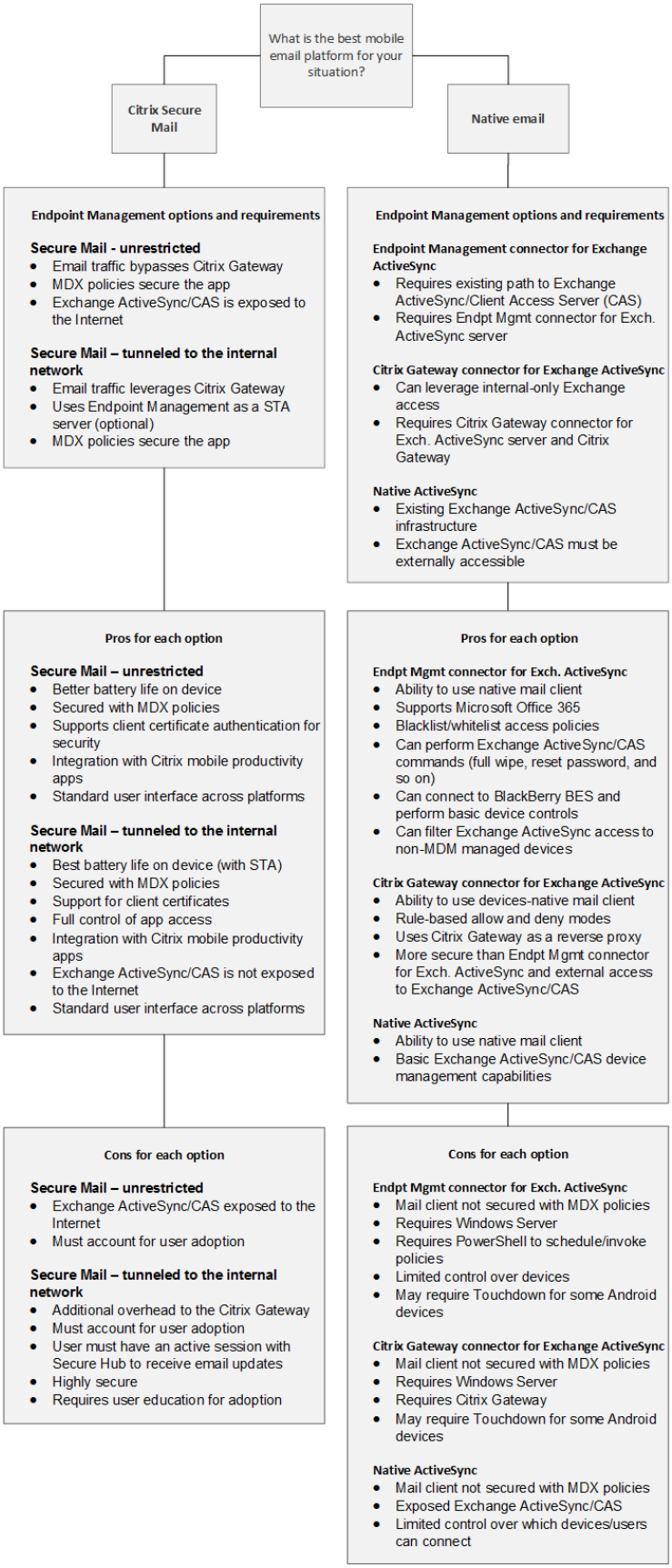
このソリューションでは、NetScaler Gateway を使用する必要はありません。既存の ActiveSync トラフィックのルーティングに変更を加えることなく、Exchange ActiveSync 用コネクタを展開できます。設計上の考慮事項は次のとおりです：

- **Windows Server**：Exchange ActiveSync 用コネクタには Windows Server の展開が必要です。
- フィルター規則のセット：NetScaler Gateway コネクタ：Exchange ActiveSync 用と同様に、Exchange ActiveSync 用コネクタには、デバイスの状態を評価するためのフィルター規則が含まれています。さらに、Exchange ActiveSync 用コネクタは、Active Directory グループのメンバーシップに基づいてフィルターする静的規則をサポートしています。
- **Exchange** の統合：Exchange ActiveSync 用コネクタでは、ActiveSync の役割をホストしている Exchange クライアントアクセスサーバー（CAS）に直接アクセスし、デバイスの隔離操作を制御する必要があります。環境アーキテクチャとセキュリティ状況によっては、この要件により課題がもたらされる可能性があります。この技術要件を前もって評価することが重要です。
- 他の **ActiveSync** クライアント：Exchange ActiveSync 用コネクタは ActiveSync サービスレベルでフィルターするため、Citrix Endpoint Management 環境外の他の ActiveSync クライアントについて考慮します。Exchange ActiveSync 用コネクタの静的規則を構成して、他の ActiveSync クライアントへの意図しない影響を防ぐことができます。
- 拡張された **Exchange** 機能： Exchange ActiveSync との直接統合により、Exchange ActiveSync 用コネクタは、モバイルデバイス上で Exchange ActiveSync のワイプを実行する機能を Citrix Endpoint Management に提供します。また Exchange ActiveSync 用コネクタでは、Citrix Endpoint Management が Blackberry デバイスに関する情報にアクセスしたり、その他の制御操作を実行することを許可します。

Citrix Endpoint Management 展開の Citrix Endpoint Management コネクタ：Exchange ActiveSync 用の図については、「アーキテクチャ」を参照してください。

電子メールプラットフォーム決定木

次の図は、Citrix Endpoint Management の展開でネイティブメールまたは Citrix Secure Mail のソリューションを使用する場合のメリットとデメリットを理解するのに役立ちます。選択ごとに、サーバー、ネットワーク、およびデータベースにアクセスするための Citrix Endpoint Management の関連オプションと要件がまとめられています。メリットとデメリットには、セキュリティ、ポリシー、およびユーザーインターフェイスの考慮事項に関する詳細が含まれています。



Citrix Endpoint Management の統合

March 15, 2024

この記事では、Citrix Endpoint Management を既存のネットワークおよびソリューションと統合する方法を計画するときに考慮すべき点について説明します。たとえば、Citrix Virtual Apps and Desktops 用の NetScaler Gateway を既に使用している場合は、次の点を考慮します:

- 既存の NetScaler Gateway インスタンス、または専用の新しいインスタンスを使用する必要がありますか。
- StoreFront で公開済みの HDX アプリを Citrix Endpoint Management と統合しますか。
- Citrix Files を Citrix Endpoint Management と併用しますか。
- Citrix Endpoint Management に統合するネットワークアクセス制御のソリューションがありますか。

NetScaler Gateway

NetScaler Gateway は、Citrix Endpoint Management の必須コンポーネントです。NetScaler Gateway は、すべての企業リソースにアクセスするためのマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

既存の NetScaler Gateway インスタンスを使用することも、Citrix Endpoint Management 用に新しいインスタンスを設定することもできます。以下のセクションでは、既存、または新規の専用の NetScaler Gateway インスタンスを使用する長所と短所について説明します。

Citrix Endpoint Management 用に作成済みの NetScaler Gateway VIP を使用した共有 NetScaler Gateway MPX

長所:

- Citrix のすべてのリモート接続（Citrix Virtual Apps、完全 VPN、およびクライアントレス VPN）に共通の NetScaler Gateway インスタンスを使用します。
- 証明書の認証や DNS、LDAP、NTP などのサービスへのアクセスに、NetScaler Gateway の既存の構成を使用します。
- 単一の NetScaler Gateway プラットフォームライセンスを使用します。

短所:

- 同じ NetScaler Gateway で 2 つの異なるユースケースを処理する場合は、スケールの計画が難しくなります。
- Citrix Virtual Apps のユースケースに特定のバージョンの NetScaler Gateway が必要になる場合があります。このような特定のバージョンには、Citrix Endpoint Management の既知の問題がある場合があります。または、Citrix Endpoint Management に、NetScaler Gateway のこのバージョンに関する既知の問題がある場合があります。

- NetScaler Gateway がある場合は、Citrix Endpoint Management 用の NetScaler Gateway 構成を作成するために、NetScaler Gateway for XenMobile ウィザードを再度実行することはできません。
- Platinum ライセンスが NetScaler Gateway 11.1 以降で使用されている場合を除き、NetScaler Gateway にインストールされ、VPN 接続に必要なユーザーアクセスライセンスはプールされます。これらのライセンスはすべての NetScaler Gateway 仮想サーバーで使用可能であるため、Citrix Endpoint Management 以外のサービスによって消費される可能性があります。

専用の **NetScaler Gateway VPX/MPX** インスタンス

長所:

専用の NetScaler Gateway インスタンスを使用することをお勧めします。

- スケールの計画が容易になるほか、既にリソースの制約がある可能性のある NetScaler Gateway インスタンスから Citrix Endpoint Management のトラフィックが分離されます。
- Citrix Endpoint Management と Citrix Virtual Apps で必要な NetScaler Gateway ソフトウェアのバージョンが異なる事態を回避できます。通常は、Citrix Endpoint Management と互換性のある最新の NetScaler Gateway バージョンおよびビルドを使用することをお勧めします。
- 組み込みの NetScaler Gateway for XenMobile ウィザードを使用して、Citrix Endpoint Management 用に NetScaler Gateway を構成できます。
- サービスの仮想的および物理的な分離。

短所:

- Citrix Endpoint Management の構成をサポートするために、NetScaler Gateway で追加のサービスを設定する必要があります。
- 別の NetScaler Gateway プラットフォームライセンスが必要です。NetScaler Gateway Gateway の NetScaler Gateway インスタンスごとにライセンスを取得します。

Citrix Endpoint Management 管理モード用の NetScaler Gateway と Citrix ADC の統合で考慮すべき点については、「NetScaler Gateway および Citrix ADC との統合」を参照してください。

StoreFront

Citrix Virtual Apps and Desktops 環境の場合は、StoreFront を使用して HDX アプリケーションを Citrix Endpoint Management と統合できます。HDX アプリを Citrix Endpoint Management と統合すると次のような効果があります:

- Citrix Endpoint Management に登録されているユーザーがこれらのアプリを利用できます。
- これらのアプリが、アプリストアに他のモバイルアプリとともに表示されます。
- Citrix Endpoint Management は、StoreFront で Citrix Receiver を使用します。

- Citrix Workspace アプリがデバイスにインストールされると、HDX アプリではこのアプリが使用されるようになります。

StoreFront には、StoreFront インスタンスごとに 1 つのサービスサイトの制限があります。複数のストアがあり、他の実稼働環境での使用から分離する必要があるとします。その場合は、通常、Citrix Endpoint Management 用に新しい StoreFront インスタンスとサービスサイトを検討することをお勧めします。

考慮事項は次のとおりです:

- StoreFront では認証要件が異なりますか。StoreFront サービスサイトでは、ログオンに Active Directory 資格情報が必要です。証明書ベースの認証のみを使用している場合、同じ NetScaler Gateway を使用して Citrix Endpoint Management 経由でアプリケーションを列挙することはできません。
- 同じストアを使用しますか。それともストアを作成しますか。
- 同じ StoreFront サーバーを使用しますか。それとも別の StoreFront サーバーを使用しますか。

以下のセクションでは、Citrix Workspace と Citrix 業務用モバイルアプリで StoreFront を個別に使用する場合と組み合わせて使用する場合の、メリットとデメリットについて説明します。

既存の **StoreFront** インスタンスを **Citrix Endpoint Management** と統合する

長所:

- 同じストア:HDX アクセスに同じ NetScaler Gateway VIP を使用する場合、Citrix Endpoint Management では StoreFront の追加構成が不要になります。同じストアを使用し、Citrix Workspace には新しい NetScaler Gateway VIP へアクセスするように指示するとします。その場合は、StoreFront に適切な NetScaler Gateway 構成を追加します。
- 同じ StoreFront サーバー: StoreFront の既存のインストールと構成を使用します。

短所:

- 同じストア: Citrix Virtual Apps and Desktops のワークロードをサポートするように StoreFront を再構成すると、Citrix Endpoint Management に悪影響が及ぶ可能性があります。
- 同じ StoreFront サーバー: 大規模な環境では、Citrix Endpoint Management がアプリの列挙と起動で Citrix Receiver を使用することにより、負荷が余計にかかる点を考慮する必要があります。

Citrix Endpoint Management との統合に新しい専用の **StoreFront** インスタンスを使用する

長所:

- 新しいストア: Citrix Endpoint Management で使用する StoreFront ストアの構成を変更しても、Virtual Apps and Desktops の既存のワークロードには影響しません。
- 新しい StoreFront サーバー: サーバー構成の変更は、Virtual Apps and Desktops のワークフローに影響しません。さらに、Citrix Endpoint Management がアプリの列挙と起動で Citrix Receiver を使用することによるもの以外の負荷は、スケーラビリティに影響しません。

短所:

- 新しいストア: StoreFront ストアの構成。
- 新しい StoreFront サーバー: StoreFront の新規のインストールと構成が必要です。

詳しくは、「アプリストア経由の Citrix Virtual Apps and Desktops」を参照してください。

ShareFile と Citrix Files

ShareFile を使用すると、ドキュメントを簡単かつセキュアに交換したり、メールで大容量のドキュメントを送信したり、サードパーティへのドキュメント転送をセキュアに処理することができます。Citrix Files アプリを使用すると、ユーザーは任意のデバイスからすべてのデータにアクセスして同期することができます。Citrix Files を使用すると、ユーザーは組織内外のユーザーとデータを安全に共有できます。

Citrix Endpoint Management により、Citrix Files に次の機能が提供されます:

- 業務用モバイルアプリユーザーのシングルサインオン認証。
- Active Directory ベースのユーザーアカウントのプロビジョニング。
- 包括的なアクセス制御ポリシー。

モバイルユーザーに完全な Enterprise アカウント機能セットのメリットをもたらすことができます。

または、ストレージゾーンコネクタとのみ統合するように Citrix Endpoint Management を構成することもできます。ストレージゾーンコネクタを介して、Citrix Files は以下へのアクセスを提供します:

- ドキュメントとフォルダー
- ネットワークファイル共有
- SharePoint サイトの場合: サイトコレクションとドキュメントライブラリ。

接続したファイル共有には、Citrix Virtual Apps and Desktops 環境で使用されるのと同じネットワークのホームドライブを含めることができます。Enterprise アカウントまたはストレージゾーンコネクタとの統合は、Citrix Endpoint Management コンソールを使用して構成します。詳しくは、「Citrix Files for Citrix Endpoint Management」を参照してください。

次のセクションでは、Citrix Files の設計を決定するときに確認すべき質問項目について説明します。

Citrix Files またはストレージゾーンコネクタのみとの統合

確認すべき質問項目:

- Citrix 管理のストレージゾーンにデータを保存する必要がありますか。
- ユーザーにファイルの共有および同期の機能を提供しますか。
- Citrix Files Web サイト上のファイルにユーザーがアクセスできるようにしますか。またはモバイルデバイスから Office 365 のコンテンツおよび個人向けクラウドコネクタにアクセスできるようにしますか。

設計の決定:

- 上記の質問のいずれかの回答が「はい」の場合は、Enterprise アカウントと統合します。
- ストレージゾーンコネクタのみと統合すると、iOS ユーザーは、SharePoint サイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。この構成では、Citrix Files サブドメインの設定や Citrix Files に対するユーザーのプロビジョニング、Citrix Files データのホストが不要になります。Citrix Endpoint Management とストレージゾーンコネクタの併用は、社内ネットワーク外へのユーザー情報漏洩に対するセキュリティ規制に適合したものです。

Storage Zone Controller サーバーの場所

確認すべき質問項目:

- オンプレミスのストレージや機能（ストレージゾーンコネクタなど）が必要ですか。
- Citrix Files のオンプレミス機能を使用する場合、Storage Zone Controller はネットワーク内のどこに配置されますか。

設計の決定:

- Citrix Files クラウド、オンプレミスのシングルテナントストレージシステム、またはサポートされているサードパーティのクラウドストレージに、Storage Zone Controller サーバーを配置するかどうかを決定します。
- Storage Zone Controller は、Citrix Files コントロールプレーンと通信するためにインターネットアクセスが必要です。直接アクセスや NAT および PAT の構成を含む、いくつかの方法で接続できます。

ストレージゾーンコネクタ

確認すべき質問項目:

- CIFS 共有パスは何ですか。
- SharePoint の URL は何ですか。

設計の決定:

- オンプレミスの Storage Zone Controller がこれらの場所にアクセスする必要があるかどうかを判断します。
- StorageZone コネクタは、ファイルリポジトリ、CIFS 共有、SharePoint などの内部リソースと通信するため、StorageZone コントローラーは、DMZ ファイアウォールの内側にあり、NetScaler Gateway が前に置かれた内部ネットワークに配置することをお勧めします。

SAML と **Citrix Endpoint Management** の統合

確認すべき質問項目:

- Citrix Files に Active Directory 認証が必要ですか。
- Citrix Endpoint Management で Citrix Files アプリを初めて使用するときに SSO を必須にしますか。
- 現在の環境に標準の IdP はありますか。
- いくつのドメインで SAML を使用する必要がありますか。
- Active Directory ユーザーに複数のメールエイリアスがありますか。
- Active Directory ドメインの移行が進行中、または近日中に予定されていますか。

設計の決定:

Citrix Files の認証メカニズムとして SAML の使用を選択できます。認証オプションは次のとおりです:

- SAML の ID プロバイダー（IdP）として Citrix Endpoint Management サーバーを使用します。

  このオプションは、優れたユーザーエクスペリエンスを提供し、Citrix Files アカウントの作成を自動化し、モバイルアプリの SSO 機能を有効にすることができます。

  Citrix Endpoint Management サーバーはこのプロセスのために強化されているため、Active Directory の同期は不要です。

  ユーザープロビジョニングに Citrix Files User Management Tool を使用します。

- サポートされているサードパーティベンダーを SAML の IdP として使用します。

  既存のサポートされている IdP があり、モバイルアプリの SSO 機能が不要な場合は、このオプションが最適です。また、このオプションでは、アカウントのプロビジョニングに Citrix Files User Management Tool を使用する必要があります。

  サードパーティの IdP ソリューション（ADFS など）を使用すると、Windows クライアント側にも SSO 機能が提供される場合があります。Citrix Files の SAML IdP を選択する前に、ユースケースを評価するようにします。

- または、両方のユースケースを満たす方法については、「デュアル ID プロバイダーの場合の ShareFile シングルサインオン構成ガイド」を参照してください。

モバイルアプリ

確認すべき質問項目:

- どの Citrix Files モバイルアプリ（パブリック、MDM、MDX）を使用する予定ですか。

設計の決定:

- Citrix 業務用モバイルアプリは Apple App Store や Google Play ストアから配信できます。パブリックアプリストアからの配信では、Citrix ダウンロードページからラップされたアプリを入手します。
- セキュリティ要件が低くコンテナ化が不要の場合、パブリックの Citrix Files アプリは適切でない可能性があります。
- 詳しくは、「アプリ」と「Citrix Files for Citrix Endpoint Management」を参照してください。

セキュリティ、ポリシー、およびアクセス制御

確認すべき質問項目:

- デスクトップ、Web、およびモバイルユーザーにはどのような制限が必要ですか。
- ユーザーに対する標準的なアクセス制御をどのような設定にしますか。
- どのようなファイル保持ポリシーを使用する予定ですか。

設計の決定:

- Citrix Files を使用すると、従業員の権限を管理できます。詳しくは、「従業員の権限」を参照してください。
- 一部の Citrix Files のデバイスセキュリティ設定と MDX ポリシーは、同じ機能を制御します。そのような場合は Citrix Endpoint Management のポリシーが優先され、次に Citrix Files のデバイスセキュリティ設定が適用されます。例: 外部アプリを Citrix Files で無効にし、Citrix Endpoint Management では有効にすると、Citrix Files ではこの外部アプリが無効になります。Citrix Endpoint Management では PIN とパスコードが不要、Citrix Files アプリでは PIN とパスコードが必要なようにアプリを構成できます。

標準 **StorageZone** と制限付き **StorageZone**

確認すべき質問項目:

- 制限付きストレージゾーンが必要ですか。

設計の決定:

- 標準ストレージゾーンは機密性の低いデータを対象としており、従業員は非従業員とデータを共有できます。このオプションは、ドメイン外でデータを共有するワークフローをサポートします。
- 制限付きストレージゾーンでは機密データが保護され、認証されたドメインユーザーのみが、ゾーンに格納されたデータにアクセスできます。

アクセス制御

企業はネットワーク内外のモバイルデバイスを管理できます。Citrix Endpoint Management などのエンタープライズモビリティ管理ソリューションは、場所に関係なくモバイルデバイスのセキュリティと制御を提供することに優れていますが、ネットワークアクセス制御（NAC）ソリューションと組み合わせると、ネットワーク内部のデバイスに対する QoS を向上させ、よりきめ細かい制御を行うことができます。この組み合わせにより、NAC ソリューションを通じて Citrix Endpoint Management のデバイスセキュリティ評価を強化できます。NAC ソリューションは Citrix Endpoint Management のセキュリティ評価を使用して、認証の決定を効率的に処理することができます。

次のいずれかのソリューションを使用して、NAC ポリシーを適用できます:

- NetScaler Gateway

- ForeScout

他の NAC ソリューションとの統合は保証されていません。

Citrix Endpoint Management と NAC ソリューションを統合する利点は次のとおりです:

- 社内ネットワーク上のすべてのエンドポイントのセキュリティ、コンプライアンス、制御の強化。
- NAC ソリューションでは、次のことが可能です:
  - ネットワークに接続しようとするデバイスを瞬時に検出します。
  - Citrix Endpoint Management にデバイス属性を照会します。
  - このデバイス情報を使用して、デバイスを許可、禁止、制限、またはリダイレクトするかどうかを決定します。これらの決定は、適用されるセキュリティポリシーによって異なります。
- NAC ソリューションでは、IT 管理者に非管理デバイスと非準拠デバイスのビューを提供します。

Citrix Endpoint Management でサポートされている NAC 準拠フィルターの説明と構成の概要については、「ネットワークアクセス制御」を参照してください。

NetScaler Gateway および Citrix ADC との統合

March 15, 2024

Citrix Endpoint Management と統合すると、NetScaler Gateway を経由して MAM（Mobile Application Management：モバイルアプリケーション管理）デバイス用の内部ネットワークにアクセスできる認証メカニズムを、リモートデバイスで利用できるようになります。この統合を利用すると、Citrix 業務用モバイルアプリはマイクロ VPN を介して、イントラネット内にある社内サーバーにアクセスすることができます。Citrix Endpoint Management により、デバイス上のアプリから NetScaler Gateway への Micro VPN が作成されます。NetScaler Gateway は、すべての企業リソースにアクセスするためのマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

ユーザーが MDM 登録をオプトアウトすると、デバイスは登録に NetScaler Gateway の完全修飾ドメイン名を使用します。

Citrix ADC の負荷分散は Citrix Cloud Operations が管理します。

設計の決定

以下のセクションでは、NetScaler Gateway と Citrix Endpoint Management との統合を計画するときに検討すべき、多くの設計上の決定事項についてまとめています。

証明書

決定の詳細:

- 登録や Citrix Endpoint Management 環境へのアクセスに高度なセキュリティが必要か
- LDAP は選択しないか

設計ガイド:

Citrix Endpoint Management のデフォルト構成は、ユーザー名とパスワードによる認証です。登録および Citrix Endpoint Management 環境へのアクセスのセキュリティを強化するには、証明書ベースの認証の使用を考慮してください。LDAP で 2 要素認証の証明書を使用すると、RSA サーバーを必要とせずに高度なセキュリティを提供できます。

LDAP やスマートカードの使用または同様の方法を許可しない場合、証明書を構成すると Citrix Endpoint Management にスマートカードを提示できます。ユーザーはそれにより、Citrix Endpoint Management が生成する一意の PIN を使用して登録できます。ユーザーがアクセス権を獲得すると、Citrix Endpoint Management は、Citrix Endpoint Management 環境に認証するために後で使用される証明書を作成して展開します。

Citrix Endpoint Management は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートしています。Microsoft CA を構成済みの場合、Citrix Endpoint Management は NetScaler Gateway を使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、NetScaler Gateway 証明書失効一覧（CRL）設定（[**Enable CRL Auto Refresh**]）を構成する必要があるかどうか検討します。この手順を使用すると、MAM のみで登録したデバイスのユーザーがデバイス上の既存の証明書を使用して認証できなくなります。ユーザー証明書は失効後もユーザーが自由に生成できるため、Citrix Endpoint Management は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

専用または共有の **NetScaler Gateway VIP** アドレス

決定の詳細:

- 現在、Citrix Virtual Apps and Desktops 用の NetScaler Gateway を使用しているか
- Citrix Endpoint Management で Citrix Virtual Apps and Desktops と同じ NetScaler Gateway を利用するか
- 両方のトラフィックフローの認証要件は何か

設計ガイド:

Citrix 環境に Citrix Endpoint Management と、Virtual Apps and Desktops が含まれている場合は、両方で同じ NetScaler Gateway 仮想サーバーを使用できます。バージョンによる競合が起きたり環境が孤立したりする可能性があるため、NetScaler Gateway は、それぞれの Citrix Endpoint Management 環境専用にすることをお勧めします。

LDAP 認証を使用する場合、Citrix Secure Hub は同じ NetScaler Gateway で問題なく認証できます。証明書ベースの認証を使用する場合、Citrix Endpoint Management は MDX コンテナ内の証明書をプッシュし、Citrix Secure Hub はその証明書を使用して NetScaler Gateway で認証します。

2 台の NetScaler Gateway VIP で同じ FQDN を使用できる、以下の回避策を検討することもできます。同じ IP アドレスで 2 つの NetScaler Gateway VIP を作成できます。Citrix Secure Hub 用の IP には標準の 443 ポートを使用し、（Citrix Workspace アプリを展開する）Citrix Virtual Apps and Desktops 用の IP にはポート 444 を使用します。こうすることで、1 つの FQDN が同じ IP アドレスに解決されます。この方法ではデフォルトのポート 443 ではなく、ポート 444 に ICA ファイルを返すよう StoreFront を構成する必要がある場合があります。この回避策では、ユーザーはポート番号を入力する必要はありません。

NetScaler Gateway のタイムアウト

決定の詳細：

- Citrix Endpoint Management のトラフィックに対する NetScaler Gateway のタイムアウトをどのように構成するか

設計ガイド：

NetScaler Gateway Gateway には、セッションタイムアウトと強制タイムアウトの設定があります。詳細については、「推奨構成」を参照してください。バックグラウンドサービス、NetScaler Gateway、およびオフラインでのアプリケーションへのアクセスでは、タイムアウト値が異なることに留意してください。

登録 **FQDN**

> 重要：
>
> 登録 FQDN を変更するには、新しい SQL Server データベースと Citrix Endpoint Management サーバーを再構築する必要があります。

Citrix Secure Web のトラフィック

決定の詳細：

- Citrix Secure Web を内部の Web ブラウジングのみに制限するか
- 内部と外部両方の Web ブラウジングで Citrix Secure Web を有効にするか。

設計ガイド：

Citrix Secure Web を内部での Web 閲覧のみに使用する予定の場合、NetScaler Gateway の構成は単純です。ただし、デフォルトで Citrix Secure Web がすべての内部サイトにアクセスできない場合は、ファイアウォールとプロキシサーバーを構成する必要がある可能性があります。

内部および外部のブラウジングに Citrix Secure Web を使用する予定の場合は、サブネット IP アドレスに送信方向のインターネットアクセスを許可する必要があります。一般的に、IT 部門は（MDX コンテナを使用する）登録済みデバイスを社内ネットワークの延長とみなします。そのため通常、IT 部門は Citrix Secure Web 接続を NetScaler Gateway に戻し、プロキシサーバーを経由させてからインターネットに接続することを望みます。デフォルトでは、Citrix Secure Web アクセスは内部ネットワークにトンネルされます。Citrix Secure Web ではすべてのネットワークアクセスにおいて、アプリケーションごとの VPN トンネルを使用して内部ネットワークに戻ってくるということであり、NetScaler Gateway では分割トンネリング設定を使用します。

Citrix Secure Web 接続の詳細については、「ユーザー接続の構成」を参照してください。

Citrix Secure Mail のプッシュ通知

決定の詳細：

- プッシュ通知を使用するか

iOS 向け設計ガイド：

NetScaler Gateway 構成に Citrix Secure Ticket Authority（STA）が含まれていて分割トンネリングがオフの場合、NetScaler Gateway は Citrix Secure Mail から次の Citrix リスナーサービス URL へのトラフィックを許可する必要があります。これらの URL は、Citrix Secure Mail for iOS のプッシュ通知で指定されます。

Android 向け設計ガイド：

Firebase Cloud Messaging（FCM）を使用して、Android デバイスが Citrix Endpoint Management に接続するタイミングと方法を制御します。FCM 構成では、セキュリティアクションや展開コマンドによって、ユーザーに Citrix Endpoint Management サーバーへの再接続を求めるプッシュ通知が Citrix Secure Hub に送信されます。

HDX の **STA**

決定の詳細：

- HDX アプリケーションのアクセスを統合する場合にどんな STA を使用するか

設計ガイド：

HDX の STA は StoreFront の STA と一致する必要があり、Virtual Apps and Desktops サイトで有効である必要があります。

Citrix Files と **ShareFile**

決定の詳細：

- 環境で Storage Zone Controller を使用するか
- どの Citrix Files VIP アドレス URL を使用するか

設計ガイド:

ご使用の環境に Storage Zone Controller を含める場合は、必ず以下を正しく構成してください:

- Citrix Files コンテンツスイッチ VIP（Citrix Files コントロールプレーンで Storage Zone Controller サーバーとの通信に使用）
- Citrix Files 負荷分散 VIP
- 必要なすべてのポリシーとプロファイル

詳しくは、Storage Zone Controllerのドキュメントを参照してください。

SAML ID プロバイダー

決定の詳細:

- Citrix Files に SAML が必要な場合、Citrix Endpoint Management を SAML ID プロバイダーとして使用するか

設計ガイド:

ベストプラクティスとして、Citrix Files を Citrix Endpoint Management と統合することをお勧めします。この方法は、SAML ベースのフェデレーションを構成するより簡単です。Citrix Endpoint Management により、Citrix Files に次の機能が提供されます:

- Citrix 業務用モバイルアプリユーザーのシングルサインオン（SSO）認証
- Active Directory ベースのユーザーアカウントのプロビジョニング
- 包括的なアクセス制御ポリシー。

Citrix Endpoint Management コンソールを使用して Citrix Files を構成したり、サービスレベルやライセンスの使用状況を監視したりできます。

次の 2 種類の Citrix Files クライアントがあります: Citrix Files for Citrix Endpoint Management クライアント（別名、ラップされた Citrix Files）、Citrix Files モバイルクライアント（別名、ラップされていない Citrix Files）。違いを理解するには、「Citrix Files for Citrix Endpoint Management クライアントと Citrix Files モバイルクライアントの違い」を参照してください。

SAML を使用して以下への SSO アクセスを提供するよう、Citrix Endpoint Management と Citrix Files を構成できます:

- MAM SDK 対応か、MDX Toolkit を使用してラップされた Citrix Files アプリ
- ラップされていない Citrix Files クライアント（Web サイト、Outlook Plug-in、同期クライアントなど）

Citrix Endpoint Management を Citrix Files 用の SAML ID プロバイダーとして使用する場合は、設定が適切であることを確認してください。詳しくは、「Citrix Files での SAML によるシングルサインオン」を参照してください。

ShareConnect での直接接続

決定の詳細:

- ユーザーが直接接続を利用して、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か

設計ガイド:

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。直接接続の場合、Citrix Endpoint Management は NetScaler 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。構成の詳細については、「ShareConnect」を参照してください。

各管理モードの登録 **FQDN**

管理モード	登録 FQDN
MDM ＋ MAM と必須の MDM 登録	Citrix Endpoint Management サーバー FQDN
MDM ＋ MAM とオプションの MDM 登録	Citrix Endpoint Management サーバー FQDN または NetScaler Gateway FQDN
MAM のみ	Citrix Endpoint Management サーバー FQDN
MAM のみ（レガシー）	NetScaler Gateway の FQDN

環境のまとめ

テスト環境、開発環境、および実稼働環境などの複数の Citrix Endpoint Management インスタンスがある場合は、追加の環境用に手動で NetScaler Gateway を構成する必要があります。作業環境がある場合は、Citrix Endpoint Management 用に手動で NetScaler Gateway を構成する前に、設定を書き留めておいてください。

重要な決定となるのは、Citrix Endpoint Management サーバーとの通信に HTTPS を使用するか、あるいは HTTP を使用するかという点です。HTTPS の場合は NetScaler Gateway と Citrix Endpoint Management との間のトラフィックが暗号化されるため、安全なバックエンド通信が可能です。再暗号化は Citrix Endpoint Management サーバーのパフォーマンスに影響します。HTTP を使用すると、Citrix Endpoint Management サーバーのパフォーマンスが向上します。NetScaler Gateway と Citrix Endpoint Management 間のトラフィッ

クは暗号化されていません。以下の表に、NetScaler Gateway および Citrix Endpoint Management の HTTP および HTTPS ポートの要件を示します。

HTTPS

Citrix では通常、NetScaler Gateway MDM 仮想サーバー構成用の SSL ブリッジをお勧めしています。MDM 仮想サーバーで NetScaler Gateway SSL オフロードを使用する場合、Citrix Endpoint Management はバックエンドサービスとしてポート 80 のみをサポートします。

管理モード	NetScaler Gateway の負荷分散手法	SSL 再暗号化	Citrix Endpoint Management サーバーポート
MAM	SSL オフロード	有効	8443
MDM + MAM	MDM：SSL ブリッジ	-	443, 8443
MDM + MAM	MAM：SSL オフロード	有効	8443

HTTP

管理モード	NetScaler Gateway の負荷分散手法	SSL 再暗号化	Citrix Endpoint Management サーバーポート
MAM	SSL オフロード	有効	8443
MDM + MAM	MDM：SSL オフロード	未サポート	80
MDM + MAM	MAM：SSL オフロード	有効	8443

Citrix Endpoint Management 環境での NetScaler Gateway の図については、「アーキテクチャ」を参照してください。

MDX アプリの SSO とプロキシの考慮事項

March 15, 2024

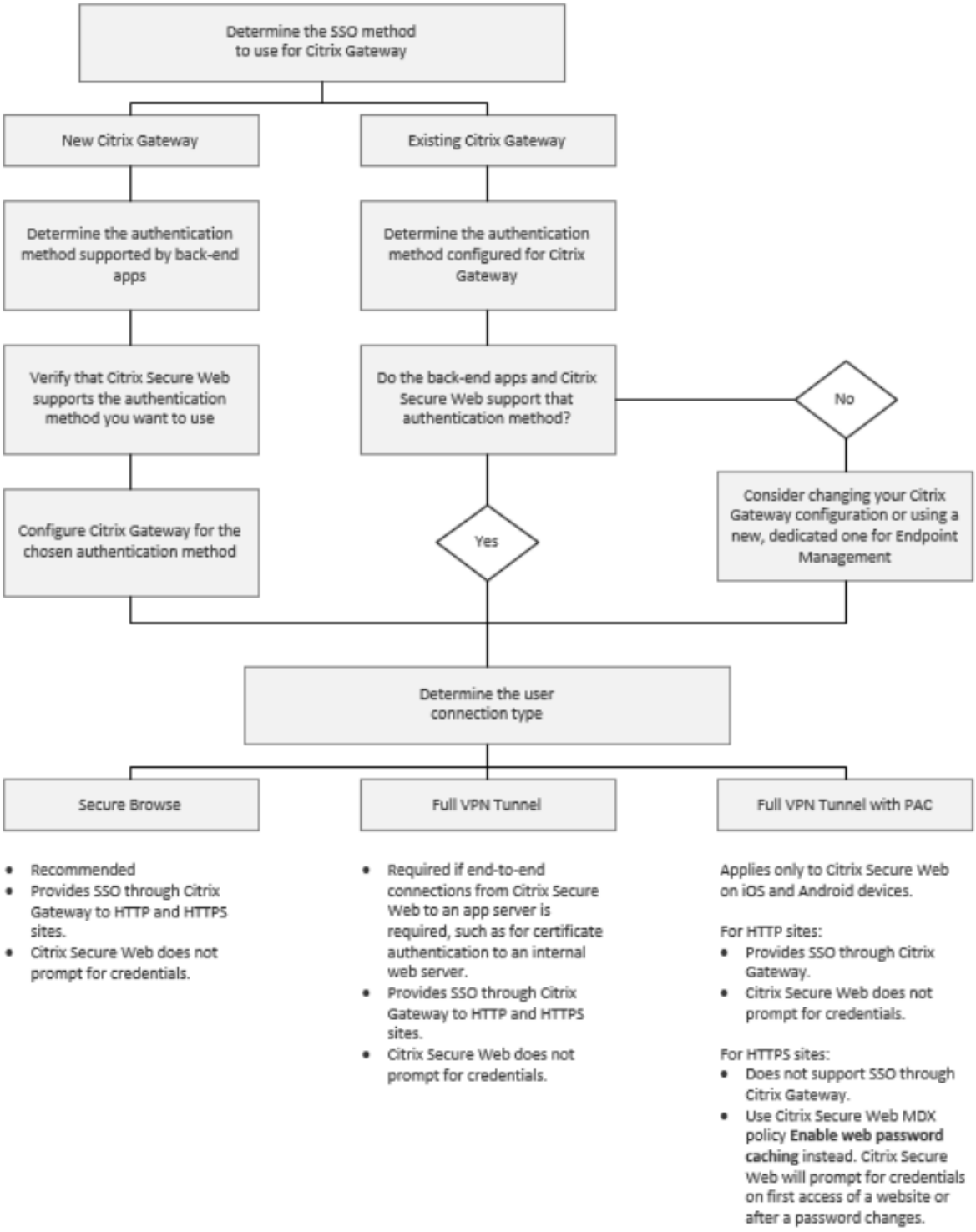
Citrix Endpoint Management と NetScaler Gateway の統合により、ユーザーにバックエンドのすべての HTTP/HTTPS リソースへのシングルサインオン（SSO）を提供することができます。SSO 認証の要件に応じて、

MDX アプリへのユーザー接続を、クライアントレス VPN の一種である Secure Browse（トンネル - Web SSO）を使用するように構成できます。

> 重要:
>
> iOS および Android デバイスの完全 VPN トンネル展開で、Proxy Automatic Configuration（PAC）ファイルのサポートが廃止されました。詳しくは、「廃止」を参照してください。

お客様の環境において SSO を提供する最善の方法が NetScaler Gateway でない場合は、ポリシーベースのローカルパスワードキャッシュを使用して MDX アプリをセットアップできます。この記事では、Citrix Secure Web に焦点を当てて、さまざまな SSO とプロキシのオプションについて説明します。この概念は他の MDX アプリにも適用されます。

次のフローチャートは、SSO とユーザー接続の決定フローをまとめたものです。



NetScaler Gateway 認証方法

ここでは、NetScaler Gateway でサポートされる認証方法について一般的な情報を説明します。

SAML 認証

SAML（Security Assertion Markup Language）を使用するように NetScaler Gateway を構成すると、ユーザーはシングルサインオンの SAML プロトコルをサポートする Web アプリに接続できます。NetScaler Gateway では、SAML Web アプリに対して ID プロバイダー（IdP）を使用したシングルサインオンがサポートされます。

必要な構成：

- NetScaler Gateway のトラフィックプロファイルで SAML SSO を構成します。
- 要求されたサービスの SAML Idp を構成します。

NTLM 認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler Gateway は NTLM 認証を自動的に実行します。

必要な構成：

- NetScaler Gateway のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

Kerberos 偽装

Citrix Endpoint Management では、Citrix Secure Web についてのみ Kerberos をサポートします。Kerberos SSO を使用するように NetScaler Gateway を構成すると、NetScaler Gateway ではユーザーパスワードを使用できる場合に偽装が使用されます。偽装とは、NetScaler Gateway がユーザーの資格情報を使用して、Citrix Secure Web などのサービスにアクセスするために必要なチケットを取得することです。

必要な構成：

- NetScaler Gateway の`Worx`セッションポリシーを構成して、接続から Kerberos レルムを識別できるようにします。
- NetScaler Gateway で Kerberos 制約付き委任（KCD）アカウントを構成します。このアカウントをパスワードなしで構成し、Citrix Endpoint Management ゲートウェイのトラフィックポリシーにバインドします。
- 上記およびその他の構成の詳細については、Citrix ブログ：WorxWeb and Kerberos Impersonation SSO を参照してください。

Kerberos の制約付き委任

Citrix Endpoint Management では、Citrix Secure Web についてのみ Kerberos をサポートします。Kerberos SSO を使用するように NetScaler Gateway を構成すると、NetScaler Gateway ではユーザーパスワードを使用できない場合に制約付き委任が使用されます。

制約付き委任では、NetScaler Gateway は指定された管理者アカウントを使用して、ユーザーとサービスに代わってチケットを取得します。

必要な構成:

- 必要な権限と NetScaler Gateway の KCD アカウントを使用して、Active Directory に KCD アカウントを構成します。
- NetScaler Gateway のトラフィックプロファイルで SSO を有効にします。
- Kerberos 認証用のバックエンド Web サイトを構成します。

フォーム入力認証

フォームベースのシングルサインオンを使用するように NetScaler Gateway を構成すると、ユーザーは一度ログオンするだけで、ネットワーク内の保護されたすべてのアプリにアクセスできます。この認証方法は、トンネル - Web SSO モードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gateway のトラフィックプロファイルでフォームベースの SSO を構成します。

ダイジェスト **HTTP** 認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler Gateway はダイジェスト HTTP 認証を自動的に実行します。この認証方法は、トンネル - Web SSO モードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gateway のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

HTTP 基本認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler Gateway は HTTP 基本認証を自動的に実行します。この認証方法は、トンネル - Web SSO モードを使用するアプリに適用されます。

必要な構成:

- NetScaler Gateway のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

セキュアトンネル **- Web SSO**

以下のセクションでは、Citrix Secure Web のユーザー接続の種類がトンネル **- Web SSO** について説明します。

内部ネットワークをトンネルする接続は、さまざまなクライアントレス VPN を使用できます。これはトンネル - Web SSO と呼ばれています。トンネル - Web SSO は、Citrix Secure Web の ［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。シングルサインオン（SSO）を必要とする接続に対しては、［トンネル-Web SSO］が推奨されます。

トンネル-Web SSO モードの場合、NetScaler Gateway は HTTPS セッションを次の 2 つの部分に分割します：

- クライアントから NetScaler Gateway まで
- NetScaler Gateway からバックエンドリソースサーバーまで。

このようにして、クライアントとサーバー間のすべてのトランザクションを把握することにより、NetScaler Gateway で SSO が提供できるようになります。

また、トンネル-Web SSO モードで使用される場合に Citrix Secure Web に対してプロキシサーバーを構成できます。詳しくは、ブログ「Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode」を参照してください。

> 注：
>
> Citrix は、PAC を使用した完全 VPN トンネルの廃止を発表しました。「廃止」を参照してください。

Citrix Endpoint Management は NetScaler Gateway が指定するプロキシ認証をサポートします。PAC ファイルには、指定の URL にアクセスするために Web ブラウザーがどのようにプロキシを選択するかを定義する規則が含まれます。PAC ファイル規則は、内部および外部の両サイトの処理を指定できます。Citrix Secure Web は PAC ファイル規則を解析し、プロキシサーバー情報を NetScaler Gateway に送信します。NetScaler Gateway は PAC ファイルまたはプロキシサーバーを認識しません。

HTTPS Web サイトへの認証の場合：Citrix Secure Web の MDX ポリシーである ［**Web** パスワードのキャッシュを有効化］により、MDX を介するプロキシサーバーへの SSO を Citrix Secure Web が認証して提供するようにできます。

NetScaler Gateway 分割トンネリング

SSO とプロキシの構成を計画するときは、NetScaler Gateway 分割トンネリングを使用するかどうかも決める必要があります。NetScaler Gateway 分割トンネリングは、必要な場合にのみ使用することをお勧めします。ここでは、分割トンネリングのしくみの概要を説明します：NetScaler Gateway では、ルーティングテーブルに基づいてトラフィックパスが決定されます。NetScaler Gateway 分割トンネリングがオンの場合、Citrix Secure Hub は内部（保護された）ネットワークのトラフィックとインターネットのトラフィックを区別します。Citrix Secure Hub は、DNS サフィックスとイントラネットアプリケーションに基づいてこの決定を行います。次に Citrix Secure Hub は、VPN トンネルを使用して内部ネットワークのトラフィックのみをトンネル処理します。NetScaler Gateway 分割トンネリングがオフの場合、すべてのトラフィックが VPN トンネルを経由します。

セキュリティ上の理由からすべてのトラフィックを監視する必要がある場合は、NetScaler Gateway 分割トンネリングをオフにします。これにより、すべてのトラフィックが VPN トンネルを経由します。

また NetScaler Gateway には、マイクロ VPN を使用したリバース分割トンネルモードもあります。この構成では、NetScaler Gateway にトンネル処理されない、除外対象の IP アドレス一覧がサポートされます。これらのアドレスは、代わりにデバイスのインターネット接続を使用して送信されます。リバース分割トンネリングについて詳しくは、NetScaler Gateway のドキュメントを参照してください。

Citrix Endpoint Management には、リバース分割トンネルの除外対象一覧が含まれています。特定の Web サイトを NetScaler Gateway 経由でトンネリングしない場合：代わりに LAN を使用して接続する完全修飾ドメイン名（FQDN）または DNS サフィックスのコンマ区切りの一覧を追加します。この一覧は、NetScaler Gateway がリバース分割トンネリング用に構成された、トンネル-Web SSO モードにのみ適用されます。

認証

March 15, 2024

Citrix Endpoint Management 環境で認証の構成方法を決定する場合、いくつかの点を考慮する必要があります。このセクションでは、認証に影響するさまざまな要素について説明します：

- 認証に関係する主な MDX ポリシー、Citrix Endpoint Management クライアントプロパティ、NetScaler Gateway の設定。
- これらのポリシー、クライアントプロパティ、および設定の関連性。
- それぞれの選択肢の代償。

また、セキュリティを強化する上で推奨される 3 つの構成例も紹介します。

大まかに言えば、セキュリティを強化するほどユーザーはより頻繁に認証を行わなければならなくなるため、最適なユーザーエクスペリエンスから遠ざかることになります。こうした問題のバランスをとる方法は、組織のニーズと優先事項によって異なります。3 つの推奨設定を確認し、さまざまな認証オプションの相互作用を把握してください。

認証モード

オンライン認証：ユーザーは Citrix Endpoint Management ネットワークに接続できます。インターネット接続が必要になります。

オフライン認証：デバイスで認証を行います。ユーザーは、セキュリティで保護された資格情報コンテナのロックを解除して、ダウンロード済みのメール、キャッシュされた Web サイト、メモなどにオフラインでアクセスできます。

認証方法

単一要素　**LDAP**：Citrix Endpoint Management では、LDAP（Lightweight Directory Access Protocol）に準拠している 1 つまたは複数のディレクトリへの接続を構成することができます。この方法は、企業環境でシングル

サインオン（SSO：Single Sign-On）を実現するためによく使用されています。Citrix PIN と Active Directory のパスワードキャッシュを合わせて使用することにして、LDAP でのユーザーエクスペリエンスを向上させることができます。同時に、登録、パスワードの有効期限、およびアカウントのロックアウト時に、複雑なパスワードによるセキュリティを提供できます。

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。

クライアント証明書： Citrix Endpoint Management を業界標準の証明機関と統合し、証明書を唯一のオンライン認証方法として使用できます。Citrix Endpoint Management では、ワンタイムパスワード、招待 URL、LDAP 資格情報のいずれかが要求されるユーザー登録を行った後に、この証明書が提供されます。クライアント証明書をプライマリ認証方法とする場合、クライアント証明書のみの環境では、デバイスで証明書を保護するために Citrix PIN が必要になります。

Citrix Endpoint Management は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートしています。Microsoft CA を構成済みの場合、Citrix Endpoint Management は NetScaler Gateway を使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、NetScaler Gateway 証明書失効一覧（CRL）設定（[Enable CRL Auto Refresh]）を構成する必要があるかどうか検討します。この手順を使用すると、MAM のみで登録したデバイスがそのデバイス上の既存の証明書を使用して認証できなくなります。ユーザー証明書は失効後もユーザーが自由に生成できるため、Citrix Endpoint Management は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

証明書ベースの認証、またはデバイスの証明書の発行でエンタープライズ証明機関（CA：Certificate Authority）を利用する場合に必要な展開環境を示した図については、「アーキテクチャ」を参照してください。

2 要素認証　**LDAP** ＋クライアント証明書：この構成は、Citrix Endpoint Management のセキュリティとユーザーエクスペリエンスの最適な組み合わせです。LDAP 認証とクライアント証明書認証の両方を使用する：

- NetScaler Gateway の 2 要素認証で提供されるセキュリティと共に SSO の最高の可能性を引き出します。
- ユーザーの知識（Active Directory パスワード）と所有物（デバイス上のクライアント証明書）によるセキュリティを実現します。

Citrix Secure Mail は自動的に構成され、クライアント証明書認証によるシームレスな初回のユーザーエクスペリエンスを提供します。この機能には、正しく構成された Exchange クライアントアクセスサーバー環境が必要です。

ユーザービリティを最適にするために、LDAP とクライアント証明書認証を Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。

LDAP ＋トークン：この構成では、RADIUS プロトコルを使用して、従来の LDAP 資格情報の構成とワンタイムパスワードを組み合わせることができます。ユーザービリティを最適にするために、このオプションを Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。

認証の重要なポリシー、設定、およびクライアントプロパティ

後に示す 3 つの推奨構成では、次のポリシー、設定、およびクライアントプロパティを利用します。

MDX ポリシー

アプリのパスコード：［オン］の場合、アプリを起動する時、または一定期間操作を行わなかった後で再開する時に、アプリのロック解除のために Citrix PIN またはパスコードが求められます。デフォルトは ［オン］です。

すべてのアプリに対して無操作タイマーを構成するには、Citrix Endpoint Management コンソールの ［設定］タブの ［クライアントプロパティ］で、INACTIVITY_TIMER 値を分単位で設定します。デフォルトは 15 分です。無通信タイマーを無効にして、PIN またはパスコードを要求するプロンプトがアプリの起動時のみに表示されるようにするには、この値をゼロに設定します。

Micro VPN セッションを必須とする：［オン］の場合、デバイス上のアプリにアクセスするために、エンタープライズネットワークおよびアクティブなセッションへ接続する必要があります。［オフ］の場合、デバイス上のアプリにアクセスするために、アクティブなセッションに接続する必要はありません。デフォルトは ［オフ］です。

最大オフライン期間（時間）： Citrix Endpoint Management がアプリ権利の再確認とポリシー更新を行わずにアプリを実行できる最大期間を定義します。以下の条件が満たされると、iOS アプリはユーザーの操作がなくても、MDX アプリの新しいポリシーを Citrix Endpoint Management から取得します：

- 最大オフライン期間が設定されています。
- Citrix Secure Hub for iOS に、有効な NetScaler Gateway トークンがあります。

Citrix Secure Hub に有効な NetScaler Gateway トークンがない場合、アプリポリシーを更新するにはユーザーが Citrix Secure Hub で認証する必要があります。非アクティブな NetScaler Gateway セッション、または強制的なセッションタイムアウトポリシーにより、NetScaler Gateway トークンが無効になることがあります。Citrix Secure Hub に再度サインインすると、アプリの実行を続けることができます。

期間が終了する 30 分前、15 分前、5 分前に、サインオンするようユーザーに警告メッセージが表示されます。期間終了後は、ユーザーがサインインするまでアプリはロックされます。デフォルトは **72** 時間（**3** 日）です。最短の期間は 1 時間です。

> 注：
>
> ユーザーの移動が頻繁であり国際ローミングを使用するシナリオでは、デフォルトの 72 時間（3 日）では時間が足りない場合があることに注意してください。

バックグラウンドサービスチケットの有効期間：バックグラウンドネットワークサービスチケットの有効状態が維持される期間。NetScaler Gateway を介して Citrix Secure Mail が ActiveSync を実行する Exchange Server に接続する場合、Citrix Endpoint Management がトークンを発行します。Citrix Secure Mail は、このトークンを使用して内部 Exchange Server に接続します。このプロパティ設定により、認証のために新しいトークンおよび Exchange Server への接続を要求することなく Citrix Secure Mail がトークンを使用できる期間が決まります。有効期限が切れた場合は、ユーザーは再度ログオンして新しいトークンを生成する必要があります。デフォルトは **168** 時間（**7** 日間）です。この有効期間が切れると、メール通知は行われなくなります。

Micro VPN セッションを必須とするまでの猶予期間：オンラインセッションが検証されるまでにオフラインでアプリを使用できる分数を指定します。デフォルトは **0**（猶予期間なし）です。

認証ポリシーの詳細については、次を参照してください：

- MAM SDK を使用する場合：MAM SDK の概要
- MDX Toolkit を使用する場合：「iOS の Citrix Endpoint Management MDX ポリシー」および「Android の Citrix Endpoint Management MDX ポリシー」

Citrix Endpoint Management クライアントプロパティ

> 注：
>
> クライアントプロパティは、Citrix Endpoint Management に接続するすべてのデバイスに適用されるグローバル設定です。

Citrix PIN：サインインを簡略化する場合は、Citrix PIN を有効にします。PIN を使用する場合、ユーザーは他の資格情報（Active Directory のユーザー名やパスワードなど）を繰り返し入力する必要はありません。Citrix PIN は単独のスタンドアロンのオフライン認証として設定できるほか、Active Directory のパスワードキャッシュと組み合わせて認証を効率化し、ユーザビリティを最適化することもできます。Citrix PIN の構成は、Citrix 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］で行うことができます。

以下に、いくつかの重要なプロパティの概要を示します。詳しくは、「クライアントプロパティ」を参照してください。

ENABLE_PASSCODE_AUTH

表示名： Enable Citrix PIN Authentication

このキーを使用すると、Citrix PIN 機能を有効にできます。ユーザーは、Citrix PIN またはパスコードにより、Active Directory パスワードの代わりに使用する PIN を定義するように求められます。**ENABLE_PASSWORD_CACHING** を有効にしているか、Citrix Endpoint Management で証明書認証を使用している場合は、この設定を有効にします。

設定可能な値： **true** または **false**

デフォルト値： **false**

ENABLE_PASSWORD_CACHING

表示名： Enable User Password Caching

このキーを使用すると、ユーザーの Active Directory パスワードをモバイルデバイス上でローカルにキャッシュできます。このキーを true に設定すると、ユーザーは Citrix PIN またはパスコードを設定するように求められます。このキーを true に設定する場合は、**ENABLE_PASSCODE_AUTH** キーを **true** に設定する必要があります。

設定可能な値： **true** または **false**

デフォルト値： **false**

PASSCODE_STRENGTH

表示名： PIN Strength Requirement

このキーでは、Citrix PIN またはパスコードの強度を定義します。この設定を変更すると、ユーザーは次回認証を求められたときに、新しい Citrix PIN またはパスコードを設定するように求められます。

設定可能な値: **Low**、**Medium**、**Strong**

デフォルト値: **Medium**

INACTIVITY_TIMER

表示名: Inactivity Timer

このキーでは、ユーザーがデバイスの操作を行わなくなってから、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］設定を ［オン］に設定する必要があります。［アプリのパスコード］設定を ［オフ］に設定すると、ユーザーは完全認証を実行するよう Citrix Secure Hub に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。デフォルトは 15 分です。

ENABLE_TOUCH_ID_AUTH

表示名: Enable Touch ID Authentication

オフライン認証での指紋リーダー（iOS のみ搭載）の使用を許可します。オンライン認証でも、プライマリ認証方法が求められます。

ENCRYPT_SECRETS_USING_PASSCODE

表示名: Encrypt secrets using Passcode

このキーでは、機密データをプラットフォームベースのネイティブな格納場所（iOS キーチェーンなど）ではなく、モバイルデバイスの Secret Vault に格納できます。この構成キーにより、重要な成果物を強力に暗号化できますが、ユーザーエントロピー（ユーザーだけが知る、ユーザーが生成したランダムな PIN コード）も追加されます。

設定可能な値: **true** または **false**

デフォルト値: **false**

NetScaler Gateway の設定

Session time-out: この設定を有効にすると、指定期間にわたって NetScaler Gateway でネットワークアクティビティが検出されない場合、NetScaler Gateway によりセッションが切断されます。この設定は、NetScaler Gateway Plug-in、Citrix Secure Hub、または Web ブラウザーを使用して接続するユーザーに適用されます。デフォルトは **1440** 分です。値を 0 にすると、設定は無効になります。

Forced time-out: この設定を有効にした場合、タイムアウト時間が経過すると、ユーザーの操作内容にかかわらず NetScaler Gateway によりセッションが切断されます。タイムアウト時間が経過した場合、ユーザーが切断を中止することはできません。この設定は、NetScaler Gateway Plug-in、Citrix Secure Hub、または Web ブラウザーを使用して接続するユーザーに適用されます。Citrix Secure Mail で STA（特別な NetScaler Gateway モード）を使用している場合、この設定は Citrix Secure Mail のセッションには適用されません。デフォルトの値は空であるため、アクティビティが行われれば、セッションは延長されます。

NetScaler Gateway のタイムアウト設定について詳しくは、NetScaler Gateway のドキュメントを参照してください。

ユーザーにデバイスで資格情報を入力して Citrix Endpoint Management の認証を行うように求めるシナリオについては、「認証を求められるシナリオ」を参照してください。

デフォルトの構成設定

これらの設定は、以下によって提供されるデフォルトです:

- NetScaler for XenMobile ウィザード
- MAM SDK または MDX Toolkit
- Citrix Endpoint Management コンソール

設定	設定が見つかる場所	デフォルト設定
セッションのタイムアウト	NetScaler Gateway	1,440 分
強制的なタイムアウト	NetScaler Gateway	値なし（オフ）
最大オフライン期間	MDX ポリシー	72 時間
バックグラウンドサービスチケットの有効期間	MDX ポリシー	168 時間（7 日）
マイクロ VPN セッションを必須とする	MDX ポリシー	オフ
Micro VPN セッションを必須とするまでの猶予期間	MDX ポリシー	0
アプリのパスコード	MDX ポリシー	On
Encrypt secrets using passcode	Citrix Endpoint Management クライアントプロパティ	false
Enable Citrix PIN Authentication	Citrix Endpoint Management クライアントプロパティ	false
PIN Strength Requirement	Citrix Endpoint Management クライアントプロパティ	中
PIN の種類	Citrix Endpoint Management クライアントプロパティ	Numeric
Enable User Password Caching	Citrix Endpoint Management クライアントプロパティ	false
Inactivity Timer	Citrix Endpoint Management クライアントプロパティ	15
Enable Touch ID Authentication	Citrix Endpoint Management クライアントプロパティ	false

推奨構成

このセクションでは、セキュリティが最も弱く最適なユーザーエクスペリエンスが得られる構成から、セキュリティが最高レベルでユーザーに操作が求められる頻度が最も多い構成まで、3 種類の Citrix Endpoint Management の構成例を示します。お客様自身の構成配置のスケールを決定する際は、これらの例を参考にしてください。これらの設定を変更する場合、他の設定の変更も必要になる可能性があります。たとえば、最大オフライン期間は、セッションのタイムアウト期間より長くすることはできません。

最高のセキュリティ

この構成ではセキュリティのレベルは最高になりますが、ユーザビリティが大きく損なわれます。

設定	設定が見つかる場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	1440	ユーザーは、オンライン認証が求められた時（24 時間ごと）にのみ、Citrix Secure Hub の資格情報を入力します。
強制的なタイムアウト	NetScaler Gateway	値なし	アクティビティが行われれば、セッションは延長されます。
最大オフライン期間	MDX ポリシー	23	毎日ポリシーを更新するように求めます。

バックグラウンドサービスチケットの有効期間	MDX ポリシー	72 時間	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Citrix Secure Mail では、STA タイムアウト期限をセッションのタイムアウト期限よりも長くすると、メール通知が停止されてしまう事態を回避できます。この場合、セッションの有効期限が切れる前にアプリを開かなかった場合、Citrix Secure Mail はユーザーに確認を求めません。
マイクロ VPN セッションを必須とする	MDX ポリシー	オフ	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを提供します。
Micro VPN セッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[Micro VPN セッションを必須とする］を有効にする場合）。
アプリのパスコード	MDX ポリシー	On	アプリケーションのパスコードを求めます。
Encrypt secrets using passcode	Citrix Endpoint Management クライアントプロパティ	true	ユーザーエントロピーで設定されたキーにより資格情報コンテナを保護します。
Enable Citrix PIN Authentication	Citrix Endpoint Management クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。
PIN Strength Requirement	Citrix Endpoint Management クライアントプロパティ	Strong	パスワードの複雑さに関する高レベルの要件を適用します。
PIN の種類	Citrix Endpoint Management クライアントプロパティ	Alphanumeric	PIN は英数字の文字列になります。

Enable Password Caching	Citrix Endpoint Management クライアントプロパティ	false	Active Directory のパスワードはキャッシュされず、Citrix PIN を使用してオフライン認証を行います。
Inactivity Timer	Citrix Endpoint Management クライアントプロパティ	15	ユーザーがこの期間にわたり MDX アプリまたは Citrix Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	Citrix Endpoint Management クライアントプロパティ	false	iOS でのオフライン認証のユースケースで、Touch ID を無効にします。

より高いセキュリティ

この構成は中間的なアプローチであり、ユーザーに認証を求める頻度を増やし（7 日ごとではなく最長で 3 日ごと）、セキュリティを強化しています。認証回数を増やしたことでコンテナはより頻繁にロックされるようになり、デバイスが使用されていないときのデータにセキュリティを提供できます。

設定	設定が見つかる場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	4320	ユーザーは、オンライン認証が求められた時（3 日ごと）にのみ、Citrix Secure Hub の資格情報を入力します。
強制的なタイムアウト	NetScaler Gateway	値なし	アクティビティが行われれば、セッションは延長されます。

最大オフライン期間	MDX ポリシー	71	3 日ごとにポリシーを更新するように求めます。1 時間短くしているのは、セッションタイムアウトより前に更新を行わせるようにするためです。
バックグラウンドサービスチケットの有効期間	MDX ポリシー	168 時間	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Citrix Secure Mail では、STA のタイムアウト期限をセッションのタイムアウト期限よりも長くすると、ユーザーに確認を求めることなくメール通知が停止されてしまう事態を回避できます。
マイクロ VPN セッションを必須とする	MDX ポリシー	オフ	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを提供します。
Micro VPN セッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[Micro VPN セッションを必須とする］を有効にする場合）。
アプリのパスコード	MDX ポリシー	On	アプリケーションのパスコードを求めます。
Encrypt secrets using passcode	Citrix Endpoint Management クライアントプロパティ	false	ユーザーエントロピーを要求せずに、資格情報コンテナを暗号化します。
Enable Citrix PIN Authentication	Citrix Endpoint Management クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。
PIN Strength Requirement	Citrix Endpoint Management クライアントプロパティ	中	中レベルのパスワードの複雑さ規則を適用します。

PIN の種類	Citrix Endpoint Management クライアントプロパティ	Numeric	PIN は数列になります。
Enable Password Caching	Citrix Endpoint Management クライアントプロパティ	true	ユーザー PIN により、Active Directory のパスワードをキャッシュ化して保護します。
Inactivity Timer	Citrix Endpoint Management クライアントプロパティ	30	ユーザーがこの期間にわたり MDX アプリまたは Citrix Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	Citrix Endpoint Management クライアントプロパティ	true	iOS でのオフライン認証のユースケース向けに、Touch ID を有効にします。

高セキュリティ

この構成はユーザーが最も使いやすいものであり、セキュリティは基本レベルになります。

設定	設定が見つかる場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	10080	ユーザーは、オンライン認証が求められた時（7 日ごと）にのみ、Citrix Secure Hub の資格情報を入力します。
強制的なタイムアウト	NetScaler Gateway	値なし	アクティビティが行われれば、セッションは延長されます。

最大オフライン期間	MDX ポリシー	167	毎週（7 日ごと）にポリシーを更新するように求めます。1 時間短くしているのは、セッションタイムアウトより前に更新を行わせるようにするためです。
バックグラウンドサービスチケットの有効期間	MDX ポリシー	240	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Citrix Secure Mail では、STA タイムアウト期限をセッションのタイムアウト期限よりも長くすると、メール通知が停止されてしまう事態を回避できます。この場合、セッションの有効期限が切れる前にアプリを開かなかった場合、Citrix Secure Mail はユーザーに確認を求めません。
マイクロ VPN セッションを必須とする	MDX ポリシー	オフ	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを提供します。
Micro VPN セッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[Micro VPN セッションを必須とする］を有効にする場合)。
アプリのパスコード	MDX ポリシー	On	アプリケーションのパスコードを求めます。
Encrypt secrets using passcode	Citrix Endpoint Management クライアントプロパティ	false	ユーザーエントロピーを要求せずに、資格情報コンテナを暗号化します。
Enable Citrix PIN Authentication	Citrix Endpoint Management クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。

PIN Strength Requirement	Citrix Endpoint Management クライアントプロパティ	低	パスワードの複雑さに関する要件を適用しません。
PIN の種類	Citrix Endpoint Management クライアントプロパティ	Numeric	PIN は数列になります。
Enable Password Caching	Citrix Endpoint Management クライアントプロパティ	true	ユーザー PIN により、Active Directory のパスワードをキャッシュ化して保護します。
Inactivity Timer	Citrix Endpoint Management クライアントプロパティ	90	ユーザーがこの期間にわたり MDX アプリまたは Citrix Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	Citrix Endpoint Management クライアントプロパティ	true	iOS でのオフライン認証のユースケース向けに、Touch ID を有効にします。

高レベルな認証を使用する

一部のアプリでは、高度な認証が必要な場合があります。たとえば、トークンや短い間隔のセッションタイムアウトといった 2 番目の認証要素などです。こうした認証方法は、MDX ポリシーで制御します。この方法では、認証方法を制御するために別個の（同一または別の NetScaler Gateway アプライアンス上の）仮想サーバーも必要になります。

設定	設定が見つかる場所	推奨設定	動作への影響
代替 NetScaler Gateway	MDX ポリシー	セカンダリ NetScaler Gateway アプライアンスの FQDN とポートを必須にする。	セカンダリ NetScaler Gateway アプライアンスの認証ポリシーおよびセッションポリシーによって制御する、より強固な認証が可能になります。

代替 NetScaler Gateway を使用するアプリをユーザーが開くと、他のすべてのアプリは、内部ネットワークとの通

信にその NetScaler Gateway インスタンスを使用します。セキュリティが強化された NetScaler Gateway インスタンスのセッションがタイムアウトした場合、セキュリティの弱い NetScaler Gateway インスタンスに切り替わるだけです。

［**Micro VPN** セッションを必須とする］の使用

Citrix Secure Web などの特定のアプリケーションでは、ユーザーのセッションが認証されているときにのみ、ユーザーがアプリを実行するようにできます。このポリシーではこうした設定を適用し、ユーザーが作業を完了できるように猶予期間を設けます。

設定	設定が見つかる場所	推奨設定	動作への影響
マイクロ VPN セッションを必須とする	MDX ポリシー	On	デバイスがオンラインで、有効な認証トークンを持っていることを必須にします。
Micro VPN セッションを必須とするまでの猶予期間	MDX ポリシー	15	ユーザーがアプリを使用できなくなるまでに 15 分間の猶予期間を設けます

サーバープロパティ

March 15, 2024

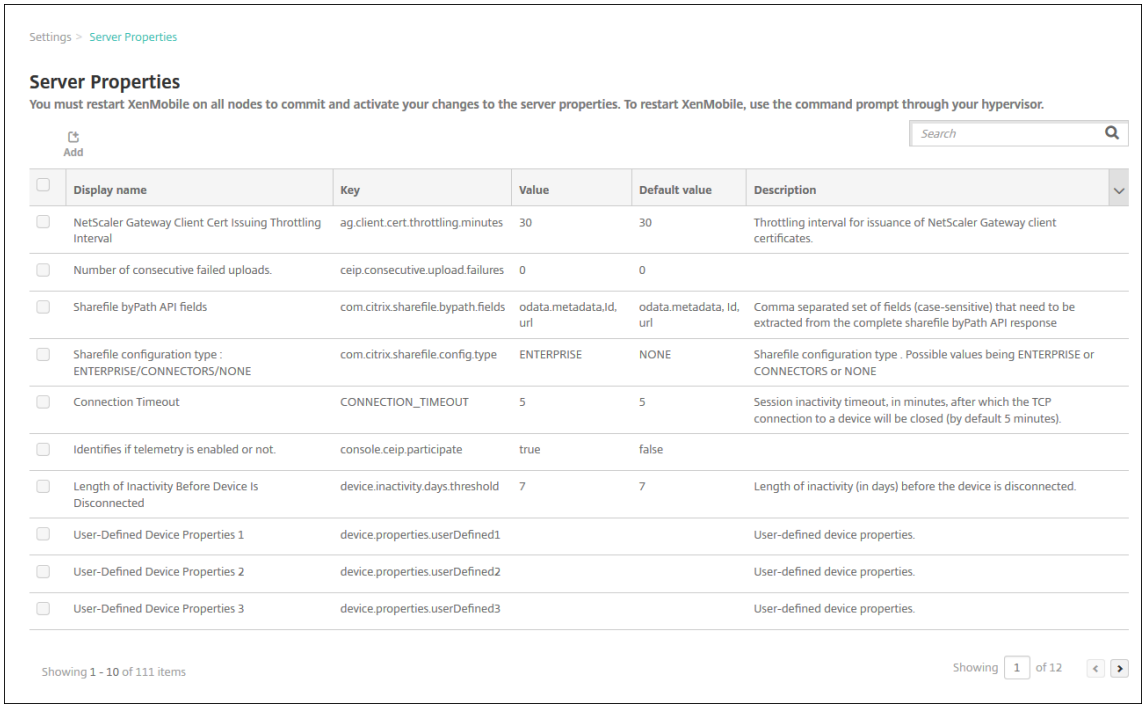
サーバープロパティは、Citrix Endpoint Management インスタンス全体の動作、ユーザー、およびデバイスに適用されるグローバルプロパティです。使用する環境で、この記事で取り上げたサーバープロパティを評価していただくことをお勧めします。他のサーバーのプロパティを変更する前には、Citrix にご相談ください。

サーバーのプロパティを更新するには、［設定］**>**［サーバープロパティ］の順に選択します。

サーバープロパティを追加、編集、または削除するには

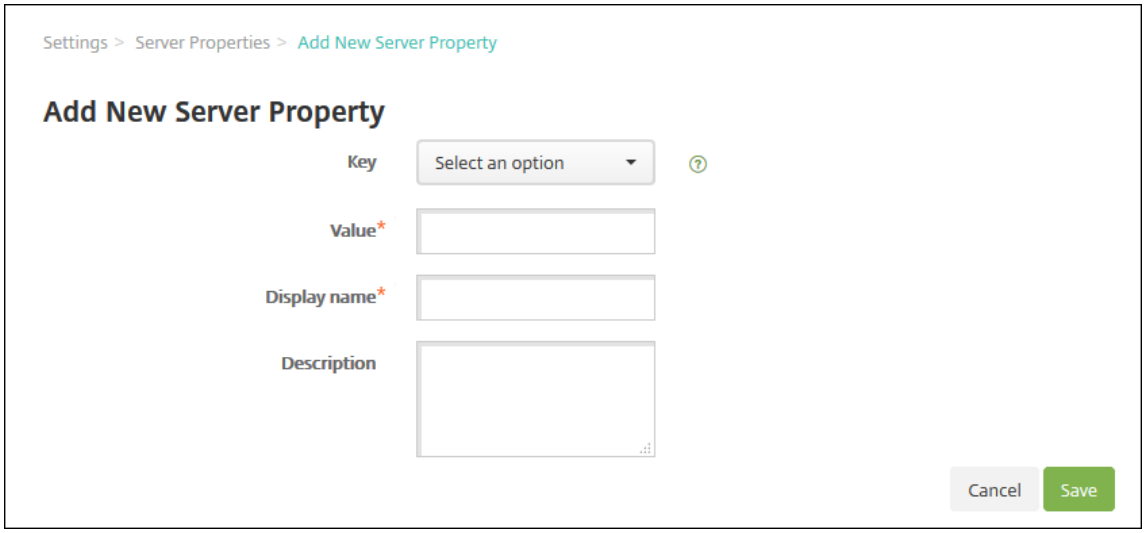
Citrix Endpoint Management で、サーバーにプロパティを適用できます。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［サーバー］の下の ［サーバープロパティ］をクリックします。［サーバープロパティ］ページが開きます。このページでは、サーバープロパティを追加、編集、または削除できます。



サーバープロパティを追加するには

1. ［追加］をクリックします。［新しいサーバープロパティの追加］ページが開きます。



2. 次の設定を構成します：

   - キー：一覧から、適切なキーを選択します。キーでは大文字と小文字が区別されます。プロパティ値を編集したり特殊キーを要求するには、Citrix サポートに連絡してください。
   - 値：選択したキーに応じて値を入力します。
   - 表示名：［サーバープロパティ］の表に表示される、新しいプロパティ値の名前を入力します。
   - 説明：任意で、新しいサーバープロパティの説明を入力します。

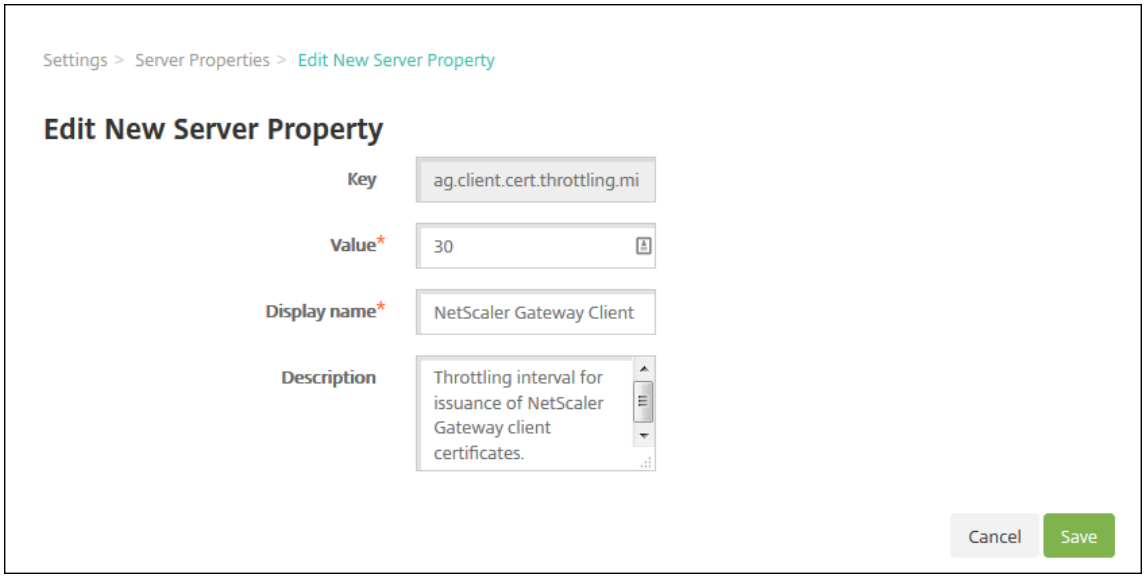
3. ［保存］をクリックします。

サーバープロパティを編集するには

1. ［サーバープロパティ］の表で、編集するサーバープロパティを選択します。

   サーバープロパティの横にあるチェックボックスをオンにすると、サーバープロパティ一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを開きます。

2. ［編集］をクリックします。［新しいサーバープロパティの編集］ページが開きます。



3. 必要に応じて以下の情報を変更します。

   - キー：このフィールドは変更できません。
   - 値：プロパティの値です。
   - 表示名：プロパティの名前です。
   - 説明：プロパティの説明です。

4. ［保存］をクリックして変更を保存するか、［キャンセル］をクリックしてプロパティを変更せずそのままにします。

サーバープロパティを削除するには

1. ［サーバープロパティ］の表で、削除するサーバープロパティを選択します。
2. ［削除］をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］をクリックします。

サーバープロパティ定義

管理対象 **Google Play** ストアにおけるすべてのアプリへのアクセス

- **true** の場合、Citrix Endpoint Management によってパブリック Google Play ストアのすべてのアプリに管理対象 Google Play ストアからアクセスできるようになります。制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。デフォルトは **false** です。

常にデバイスを追加

- **true** の場合、登録に失敗しても、Citrix Endpoint Management はデバイスを Citrix Endpoint Management コンソールに追加します。そのため、登録しようとしたデバイスを確認できます。デフォルトは **false** です。

AG クライアント証明書の発行調整間隔

- 証明書の作成の猶予期間です。この間隔により、Citrix Endpoint Management で短時間にデバイスの証明書が複数作成されることを防ぎます。この値は変更しないでください。デフォルトは **30** 分です。

指定された期間非アクティブとマークされたデバイスの削除を許可

- **true** の場合、指定された時間（日）非アクティブであったデバイスが Citrix Endpoint Management から削除されます。アクティビティの期間は、「**CEM** から自動的に削除される前にデバイスが非アクティブにしておくことができる時間の長さ」サーバープロパティにより設定されます。デフォルトは **true** です。このプロパティの値を変更するには、Citrix の担当者にお問い合わせください。

Audit Logger

- **False** の場合、ユーザーインターフェイス（UI）イベントはログに記録されません。デフォルトは **False** です。

Root 化された **Android** とジェイルブレイクされた **iOS** デバイスの登録をブロック

このプロパティが **true** の場合、Citrix Endpoint Management はルート化された Android デバイスおよびジェイルブレイクされた iOS デバイスの登録をブロックします。推奨の設定は、すべてのセキュリティレベルに対して **true** です。デフォルトは **true** です。

cdn.s3.retry.interval および **cdn.s3.max.retry**

`cdn.s3.retry.interval`と`cdn.s3.max.retry`のサーバープロパティを連携させて、すべてのmacOS PKG ファイルをアップロードする制限時間を設定できます。デフォルトでは、Citrix Endpoint Management によりファイルのアップロード時間が 100 秒に制限されています。ファイルのアップロードがその制限を超えると、アップロードは失敗します。デフォルトを変更するには、`cdn.s3.retry.interval`キーと`cdn.s3.max.retry`キーを次のように構成します:

- `cdn.s3.retry.interval`。ファイルのアップロードが正常に完了したかどうかを、Citrix Endpoint Management が確認する間隔をミリ秒単位で定義できます。デフォルトは`10000`です。
- `cdn.s3.max.retry`。アップロードが失敗するまでの検証再試行の最大回数を定義できます。デフォルトは`10`です。

2 つのキーが連携して、ファイルのアップロード時間を制限します。デフォルトでは、制限時間は 100 秒です (10000*10 ミリ秒)。

証明書の書き換え（秒数）

- 証明書の有効期限が切れる前に、Citrix Endpoint Management が証明書の更新を開始する秒数です。たとえば、証明書が 12 月 30 日に期限切れになる予定でこのプロパティが 30 日に設定されている場合、デバイスが 12 月 1 日から 12 月 30 日の間に接続すると Citrix Endpoint Management は証明書の更新を試みます。デフォルトは **2592000** 秒（30 日間）です。

接続タイムアウト

- 無操作状態でセッションがタイムアウトになるまでの期間（分単位）です。この期間を過ぎると、Citrix Endpoint Management はデバイスへの TCP 接続を閉じます。セッションは開いたままです。Android デバイスに適用されます。デフォルトは **5** 分です。

デフォルトの展開チャネル

- Citrix Endpoint Management でのデバイスへのリソースの展開: ユーザーレベル (**DEFAULT_TO_USER** ）とデバイスレベルのどちらで行うかを指定します。デフォルトは **DEFAULT_TO_DEVICE** です。

モバイルサービスプロバイダーの廃止

- Blackberry およびその他の Exchange ActiveSync デバイスのクエリに使用されるモバイルサービスプロバイダーインターフェイスのサポートは廃止されます。有効になっている間、モバイルサービスプロバイダーインターフェイスはコンソールから非表示になります。デフォルト値は **true** です。

デバイスのタグ付け

- enable.device.taggingを **true** に設定すると、Citrix Endpoint Management はデバイスタイプごとにデバイスに自動的にタグを付けます。デバイスタグを使用して、ポリシーとアプリを展開したり、デリバリーグループを構成したりできます。Citrix Endpoint Management は、次のデバイスにタグを適用します:
  - BYOD タグ
    - iOS ユーザー登録
    - Android Enterprise の仕事用プロファイル
  - 企業タグ
    - Android Enterprise の完全に管理された企業デバイス
    - 一括登録
      - Apple Business Manager デバイス
      - Apple School Manager デバイス
      - Windows AutoPilot デバイス
      - Android Enterprise の一括登録

ホスト名の検証を無効化

- デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証に失敗すると、サーバーログに次のようなエラーが記録されます:「一括購入サーバーに接続できません: ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」。ホスト名の認証によって展開が損なわれる場合は、このプロパティを **true** に変更します。デフォルトは **false** です。

SSL サーバーの検証を無効にする

- **True** の場合、以下の条件がすべて満たされると SSL サーバー証明書の検証が無効になります。
  - Citrix Endpoint Management で証明書ベースの認証を有効にしている
  - 証明書発行者に Microsoft CA サーバーを指定している
  - ルート Citrix Endpoint Management に信頼されていない内部 CA により証明書に署名している

  デフォルトは **True** です。

Enable Crash Reporting

- **true** の場合、Citrix Secure Hub for iOS および Android での問題のトラブルシューティングを目的として、Citrix によりクラッシュレポートと診断情報が収集されます。**false** の場合、データは収集されません。デフォルト値は、**true** です。

診断のための **Hibernate** 統計ログの有効化/無効化

- **True** にすると、アプリケーションパフォーマンスの問題のトラブルシューティングを支援する、Hibernate による診断統計ログが有効になります。Hibernate は、Microsoft SQL Server への Citrix Endpoint Management の接続のために使用されるコンポーネントです。ログはアプリケーションのパフォーマンスに影響を及ぼすため、デフォルトでは無効になっています。膨大なログファイルが作成されるのを避けるため、ログを有効にするのは短期間だけにしてください。Citrix Endpoint Management は、/opt/sas/logs/hibernate_stats.log にログを書き込みます。デフォルトは **False** です。

Enable macOS OTAE

- **false** の場合、macOS デバイス用の登録リンクの使用が禁止され、macOS ユーザーの登録方法が登録招待状のみに制限されます。デフォルトは **true** です。

通知トリガーの有効化

- Citrix Secure Hub クライアントの通知を有効または無効にします。値 **true** を指定すると、通知が有効になります。デフォルトは **true** です。

許可および拒否された **ActiveSync** ユーザーの完全な抽出

- Citrix Endpoint Management が許可および禁止された ActiveSync ユーザーの完全な一覧（ベースライン）を抽出する間隔（秒単位）です。デフォルトは **28800** 秒です。

テレメトリが有効かを特定する

- テレメトリが有効かを特定します。テレメトリは、カスタマーエクスペリエンス向上プログラム（CEIP）とも呼ばれます。Citrix Endpoint Management のインストールまたはアップグレード時に CEIP にオプトインすることができます。Citrix Endpoint Management が連続して 15 回アップロードを失敗した場合、利用統計情報は無効になります。デフォルトは **false** です。

無操作状態によるタイムアウト **(**分**)**

- 非アクティブなユーザーが Citrix Endpoint Management からログアウトされるまでの分数です。ユーザーが Citrix Endpoint Management のパブリック API を使用し、Citrix Endpoint Management コンソールやサードパーティ製アプリにアクセスしておく必要があります。タイムアウト値が **0** の場合、非アクティブなユーザーはログインしたままになります。API にアクセスするサードパーティのアプリは、通常はログインしたままにする必要があります。デフォルト値は **5** です。

- サーバープロパティ **Web** サービスのタイムアウトの種類が **INACTIVITY_TIMEOUT** に設定されている場合：このプロパティで、次の条件を満たす非アクティブな管理者が Citrix Endpoint Management からログアウトされるまでの分数を指定します：
  - REST サービス用のパブリック API を使用して Citrix Endpoint Management コンソールにアクセスした
  - REST サービス用のパブリック API を使用してサードパーティアプリにアクセスした。タイムアウト値が **0** の場合、非アクティブなユーザーはログインしたままになります。

include.device.properties.during.search

- デバイス検索にすべてのデバイスプロパティを含めます。デフォルトは **Off** で、速やかに検索を行うために、検索範囲を次のデバイスプロパティに制限します：
  - シリアル番号
  - IMEI
  - Wi-Fi MAC アドレス
  - Bluetooth MAC アドレス
  - Active Sync ID
  - ユーザー名

  このプロパティが **On** の場合、デバイスの検索に時間がかかることがあります。

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- オフラインの iOS デバイスまたは macOS デバイスを到達不可とみなすまでの日数を指定します。iOS または macOS デバイスが指定された制限に達すると、Citrix Endpoint Management への確認が停止されます。どちらのプロパティもデフォルトは **45** 日間です。

iOS デバイス管理登録：必要な場合ルート **CA** をインストールする

- すべての Citrix Endpoint Management 環境でサーバープロパティ **ios.mdm.enrollment.installRootCaIfRequire** が **False** に設定されます。Citrix Endpoint Management は信頼された公的機関の証明書チェーンを使用するため、ルート CA をデバイスにプッシュする必要はありません。（このプロパティは、オンプレミス環境でのみ使用されます）。

iOS デバイス管理登録：最後の手順の遅延

- デバイスの登録中、このプロパティの値は MDM プロファイルのインストールからデバイスでエージェントを開始するまでの待機時間を指定します。このプロパティは、ネットワークの遅延または速度の問題がある場合

にのみ編集することをお勧めします。編集する場合は、5000 ミリ秒（5 秒）を超える値を設定しないでください。デフォルトは **1000** ミリ秒（1 秒）です。

iOS デバイス管理：**ID** デリバリーモード

- Citrix Endpoint Management は、**SCEP**（セキュリティ上推奨される）または **PKCS12** を使用して MDM 証明書をデバイスに配布するかを指定します。PKCS12 モードの場合、サーバーでキーペアが生成され、ネゴシエーションは実行されません。デフォルトは **SCEP** です。

iOS デバイス管理：**ID** キーサイズ

- MDM ID、iOS プロファイルサービス、Citrix Endpoint Management iOS エージェント ID の秘密キーのサイズを定義します。デフォルトは **2048** です。

iOS デバイス管理：**ID** 更新日数

- 証明書の有効期限が切れる前に、Citrix Endpoint Management が証明書の更新を開始する秒数を指定します。たとえば、証明書が 10 日後に期限切れになり、このプロパティが **10** 日間に設定されている場合、デバイスが期限切れの 9 日前に接続すると Citrix Endpoint Management は新しい証明書を発行します。デフォルトは **30** 日間です。

iOS MDM APNS 秘密キーのパスワード

- このプロパティには、Citrix Endpoint Management が Apple サーバーに通知をプッシュするために必要な APNs パスワードが含まれます。

デバイスが切断されるまでの非アクティブ期間

- デバイスが Citrix Endpoint Management から切断されるまで非アクティブ状態（最後の認証を含む）でいられる期間を指定します。デフォルトは **7** 日間です。

CEM から自動的に削除される前にデバイスが非アクティブにしておくことができる時間の長さ

- Citrix Endpoint Management から自動的に削除される前にデバイスが非アクティブにしておくことができる時間の長さ（日）。最短は **14** 日で、デフォルトは **30** 日です。このプロパティを有効にするには、［指定された期間非アクティブとマークされたデバイスの削除を許可］サーバープロパティを **true** に設定する必要があります。

local.user.account.lockout.time

- ロックアウト制限を超えたあとにユーザーが待機する必要がある分数を指定します。指定できる値は 0〜999 です。デフォルトは **30** 分です。

local.user.account.lockout.limit

- ユーザーごとの連続する無効なログイン試行の上限回数を指定します。指定できる値は 0〜999 です。デフォルト値は **6** に設定されています。

mac.dep.admin.passwd.rotate

このサーバープロパティを使用すると、Apple Deployment Program を通じて登録された macOS デバイスの管理者パスワードのローテーション間隔を構成できます。Citrix Endpoint Management は、管理者アカウントのパスワードをローテーションするかどうかを毎日チェックします。デフォルトでは、Citrix Endpoint Management は 10,080 分（7 日）ごとにパスワードをローテーションします。この`mac.dep.admin.passwd.rotate`キーは次のように構成します：

- 値：管理者定義
  Citrix Endpoint Management がパスワードをローテーションする間隔（分単位）。360（6 時間）以上の値を入力します。Citrix Endpoint Management は、360 より小さい値を無視し、代わりに 360 分（6 時間）ごとにパスワードをローテーションします。
- 表示名：管理者定義
- 説明：管理者定義

MAM のみのデバイスの最大値

- このカスタムキーでは、各ユーザーが登録可能な MAM のみデバイスの数を制限します。このキーは次のように構成します。値を **0** にすると、デバイスを無制限に登録できます。
- キー = **number.of.mam.devices.per.user**
- 値 = **5**
- 表示名 = **MAM** のみのデバイスの最大値
- 説明 = 各ユーザーが登録できる **MAM** デバイスの数を制限します。

MaxNumberOfWorker

- 多数の一括購入ライセンスをインポートするときに使用するスレッド数です。デフォルトは **3** です。さらに最適化が必要な場合は、スレッド数を増やすことができます。ただし、スレッド数を大きくすると、CPU 使用率が高くなります。

NetScaler Gateway（**NetScaler Gateway**）シングルサインオン

- **False** の場合、NetScaler Gateway から Citrix Endpoint Management へのシングルサインオン実行中に Citrix Endpoint Management コールバック機能が無効にされます。コールバック機能は、NetScaler Gateway の構成でコールバック URL が設定されている場合に NetScaler Gateway のセッション ID の検証に使用されます。デフォルトは **False** です。

連続して失敗したアップロードの数

- カスタマーエクスペリエンス向上プログラム（CEIP）アップロード中の連続失敗回数を表示します。アップロードが失敗した場合、Citrix Endpoint Management がこの値を増やします。アップロードが 15 回失敗すると、Citrix Endpoint Management によって CEIP（利用統計情報）が無効化されます。詳しくは、サーバープロパティの「テレメトリが有効かを特定する」を参照してください。アップロードが成功した場合、Citrix Endpoint Management によってこの値は **0** にリセットされます。

デバイスごとのユーザーの数

- モバイルデバイス管理（MDM：Mobile Device Management）に同じデバイスを登録できるユーザーの最大数。値 **0** は、無制限の数のユーザーが同じデバイスを登録できることを意味します。デフォルトは **0** です。

optional.user.identity.attributes

- このサーバープロパティを使用すると、オプションの Active Directory ユーザー属性をカスタマイズできます。

  カスタムキーを作成し、［値］フィールドでユーザー属性を編集して、Citrix Endpoint Management がユーザーアカウントを作成するためにアクセスできる属性を定義します。詳しくは、「ユーザープロパティのカスタマイズ」を参照してください。

  - キー：カスタムキー
  - キー：**optional.user.identity.attributes**
  - 値：**commonName**、**firstName**、**lastName**、**displayName**、**streetAddress**、**city**、**state**、**country**、**workPhone**、**homePhone**、**mobilePhone**、**company**、**department**、**description**、**employeeID**、**faxNumber**、**initials**、**ipPhone**、**manager**、**homePostalAddress**、**otherMobile**、**pager**、**physicalDeliveryOfficeName**、**postalCode**、**postOfficeBox**、**title**、**organization**、**preferredLanguage**
  - 表示名：**optional.user.identity.attributes**
  - 説明：オプションの **Active Directory** ユーザー属性

macOS および **iOS/iPadOS** 登録プロファイルの組織名

- `apple.mdm.enrollment.profile.organization.name`に入力する値は、登録プロファイルを提供する組織の名前に対応しています。この名前は、ユーザーがデバイスを Citrix Endpoint Management に登録する際に表示されます。表示されるデフォルト名は **Citrix Workspace** です。

許可および拒否されたユーザーの増分変更の抽出

- ActiveSync デバイスの差分を取得する PowerShell コマンドを実行するときに、Citrix Endpoint Management がドメインからの応答を待機する秒数です。デフォルトは **60** 秒です。

Microsoft 認証サーバーへの読み取りタイムアウト

- 読み取りを実行する場合、Citrix Endpoint Management が証明書サーバーからの応答を待つ秒数です。証明書サーバーの接続速度が遅く、トラフィックが多い場合、この値を 60 秒以上にすることができます。証明書サーバーが 120 秒経っても応答しない場合は、保守が必要です。デフォルトは **15000** ミリ秒（15 秒）です。

REST Web サービス

- REST Web サービスを有効化します。デフォルトは **true** です。

指定されたサイズのチャンクでデバイス情報を取得する

- この値は、デバイスのエクスポート中のマルチスレッド処理で内部的に使用されます。この値を大きくすると、単一のスレッドで解析できるデバイス数が増加します。この値を小さくすると、デバイスをフェッチするスレッド数が増加します。この値を小さくすると、エクスポートおよびデバイスリストのフェッチのパフォーマンスが向上する可能性がありますが、利用可能なメモリが減少する可能性もあります。デフォルトは **1000** です。

shp.console.enable

- **False** の場合、Self Help Portal へのアクセスが禁止されます。ポート 4443 でポータルに移動すると、「アクセスが拒否されました」というメッセージが表示されます。**True** の場合、ポート 443 で Self Help Portal にアクセスできます。

  デフォルトは **False** です。

enable.new.shp

- **False** の場合、ユーザーは Self Help Portal からデバイスを有効にできません。**True** の場合、ユーザーは Self Help Portal からデバイスを有効にできます。

  BitLocker 回復キー機能では、このプロパティを **False** に設定し、`shp.console.enable`プロパティを **True** に設定する必要があります。

  デフォルトは **False** です。

セッションログのクリーンアップ **(**日**)**

- Citrix Endpoint Management にセッションログが保持される日数です。デフォルトは **7** です。

ShareFile の構成の種類

- Citrix Files のストレージの種類を指定します。［エンタープライズ］では、Citrix Files Enterprise モードが有効になります。［コネクタ］では、アクセス先が Citrix Endpoint Management コンソールで作成したストレージゾーンコネクタのみに制限されます。デフォルトは ［なし］で、［構成］**>** ［**Citrix Files**］画面の初期表示が表示されます。この画面では、Citrix Files Enterprise とコネクタの選択を行います。デフォルトは［なし］です。

静的タイムアウト **(**分**)**

- **WebServices timeout type** サーバープロパティが **STATIC_TIMEOUT** に設定されている場合：このプロパティで、管理者が次のいずれかの操作を行った後に Citrix Endpoint Management からログアウトされるまでの分数を指定します：

  - REST サービス用のパブリック API を使用して Citrix Endpoint Management コンソールにアクセスする。
  - REST サービス用のパブリック API を使用してサードパーティアプリにアクセスする。

  デフォルトは **60** です。

エージェントメッセージの無効化をトリガーする

- Citrix Secure Hub クライアントのメッセージを有効または無効にします。値を **false** に設定すると、メッセージが有効になります。デフォルトは **true** です。

エージェントのサウンドの無効化をトリガーする

- Citrix Secure Hub クライアントのサウンドを有効または無効にします。値を **false** に設定すると、サウンドが有効になります。デフォルトは **true** です。

認証されていない **Android** デバイス用アプリのダウンロード

- **True** の場合、セルフホストされたアプリを、Android Enterprise を実行している Android デバイスにダウンロードできます。このプロパティは、Google Play Store で静的にダウンロード URL を提供する Android Enterprise オプションが有効になっている場合に Citrix Endpoint Management で必要となります。この場合、ダウンロード URL に認証トークンを含む（**XAM One-Time Ticket** サーバープロパティによって定義された）ワンタイムチケットを含めることはできません。デフォルトは **False** です。

認証されていない **Windows** デバイス用アプリのダウンロード

- ワンタイムチケットが検証されない古い Citrix Secure Hub バージョンでのみ使用されます。**False** の場合、Citrix Endpoint Management から Windows デバイスに、未認証のアプリをダウンロードできます。デフォルトは **False** です。

ActiveSync ID を使用して **ActiveSync** デバイスをワイプする

- **true** の場合、Exchange ActiveSync 用 Citrix Endpoint Management コネクタは、ActiveSync 識別子を **asWipeDevice** メソッドの引数として使用します。デフォルトは **false** です。

Exchange のみのユーザー

- **true** の場合、Exchange ActiveSync ユーザーに対するユーザー認証を無効化します。デフォルトは **false** です。

一括購入の基準間隔

- Citrix Endpoint Management が一括購入ライセンスを Apple から再インポートする最小間隔です。ライセンス情報を更新することにより、Citrix Endpoint Management にすべての変更が反映されます（一括購入でインポートされたアプリを手動で削除した場合など）。デフォルトで、Citrix Endpoint Management は一括購入ライセンスの基準を最低 **1440** 分ごとに更新します。
  - 多数の一括購入ライセンスをインストールしている場合（たとえば、50,000 個以上）、基準間隔を広げてライセンスをインポートする頻度とオーバーヘッドを減らすことをお勧めします。

  - Apple からの頻繁な一括購入ライセンス変更が予想される場合は、変更に対して Citrix Endpoint Management が最新状態を維持できるよう、この値を下げることをお勧めします。
  - 2 つのベースライン間の最小間隔は 60 分です。また、Citrix Endpoint Management は 60 分ごとに差分インポートを実行して前回のインポートからの変更を取得します。このため、一括購入の基準間隔が 60 分の場合、基準間の間隔は最大 119 分開く可能性があります。

WebServices Timeout Type

- パブリック API から取得する認証トークンが期限切れになる方法を指定します。
  - **STATIC_TIMEOUT** の場合：サーバープロパティ ［静的タイムアウト（分）］の値に基づき、Citrix Endpoint Management はトークンを期限切れと見なします。
  - **INACTIVITY_TIMEOUT** の場合：サーバープロパティ ［無操作状態によるタイムアウト（分）］の値に基づき、Citrix Endpoint Management はトークンを期限切れと見なします。デフォルトは **STATIC_TIMEOUT** です。

Windows タブレット **MDM** 証明書の延長検証（**5** 年）

- Windows タブレットで MDM から発行されたデバイス証明書の有効期限です。デバイスは、デバイス管理中はデバイス証明書を使用して MDM サーバーへの認証を行います。**true** の場合、有効期限は 5 年間になります。**false** の場合、有効期限は 2 年間になります。デフォルトは **true** です。

Windows WNS Channel - Number of Days Before Renewal

- ChannelURI の更新間隔。デフォルトは **10** 日間です。

Windows WNS Heartbeat Interval

- Citrix Endpoint Management で 3 分ごとのデバイスへの接続を 5 回行った後に再びデバイスへ接続するまでの待機時間です。デフォルトは **6** 時間です。

XAM ワンタイムチケット

- アプリをダウンロードするときのワンタイム認証トークン（OTT：One-Time Authentication Token）の有効時間（ミリ秒）です。このプロパティは、認証されていない **Android** デバイス用アプリのダウンロードプロパティおよび認証されていない **Windows** デバイス用アプリのダウンロードプロパティとともに使用されます。これらのプロパティにより、未認証アプリのダウンロードを許可するかどうかを指定します。デフォルトは **3600000** です。

Citrix Endpoint Management MDM Self Help Portal コンソールの最大非アクティブ間隔（分）

- このプロパティ名には、Citrix Endpoint Management の古いバージョンが反映されます。このプロパティは、Citrix Endpoint Management コンソールの最大非アクティブ間隔を制御します。この間隔は、非アクティブなユーザーが Citrix Endpoint Management コンソールからログアウトされるまでの分数です。タイムアウトが **0** の場合、非アクティブなユーザーはログインしたままになります。デフォルトは **30** です。

デバイスポリシーとアプリポリシー

March 15, 2024

Citrix Endpoint Management にデバイスポリシーとアプリポリシーを適用すると、次のような要素間のバランスを最適化できます:

- 企業セキュリティ
- 企業データおよび資産の保護
- ユーザーのプライバシー
- 生産的で好ましいユーザーエクスペリエンス

これらの要素間の最適なバランスはさまざまです。たとえば、金融などの高度に規制されている組織では、ユーザーの生産性が重視される教育や小売りなどの業界よりも厳格なセキュリティ管理が求められます。

ユーザーの ID、デバイス、場所、および接続タイプに基づいてポリシーを集中的に管理および構成し、企業コンテンツが悪用されるのを抑制できます。デバイスを紛失または盗まれた場合、ビジネスアプリケーションとデータをリモートで無効にしたり、ロックやワイプを行ったりできます。総合的に見ると、従業員の満足度と生産性を向上させると同時に、セキュリティと管理者によるコントロールを保証するソリューションということになります。

この記事ではセキュリティに関連する多くのデバイスポリシーとアプリポリシーに焦点を当てます。

セキュリティリスクに対処するポリシー

Citrix Endpoint Management のデバイスポリシーとアプリポリシーは、次のようなセキュリティリスクを引き起こす可能性のある、さまざまな状況に対応しています:

- 信頼できないデバイスや予期しない場所からアプリやデータにアクセスしようとする場合
- ユーザーがデバイス間でデータを渡す場合
- 権限のないユーザーがデータにアクセスしようとした場合
- 退社したユーザーが独自のデバイス（Bring Your Own Device：BYOD）を使用した場合
- デバイスを紛失した場合
- ユーザーが常に安全にネットワークにアクセスする必要がある場合
- ユーザーが自分でデバイスを管理していて、仕事用のデータと個人用のデータを分ける必要がある場合

- デバイスがアイドル状態で、ユーザーの資格情報の検証が再度必要な場合
- 機密コンテンツをコピーして、保護されていないメールシステムに貼り付ける場合
- 個人用アカウントと企業アカウントの両方があり、機密データが保存されているデバイスでメールの添付ファイルまたは Web リンクを受信した場合

企業データの保護においては、こうした事態が懸念される場面は主に 2 つあります。具体的にはデータが次のような状態にあるときです。

- 保存されている
- 転送している

Citrix Endpoint Management による保存データの保護

モバイルデバイスに格納されているデータは、保存データと呼ばれます。Citrix Endpoint Management は、iOS および Android プラットフォームによって提供されるデバイス暗号化を使用します。Citrix Endpoint Management は、Citrix MAM SDK によって利用できるコンプライアンスチェックなどの機能でプラットフォームベースの暗号化を補完します。

Citrix Endpoint Management のモバイルアプリケーション管理（MAM：Mobile Application Management）機能を利用すると、Citrix 業務用モバイルアプリ、MDX 対応アプリ、およびそれらに関連付けられたデータに対する完全な管理、セキュリティ、および制御を実現できます。

Mobile Apps SDK は、Citrix MDX アプリコンテナ技術の使用によって Citrix Endpoint Management 展開環境のアプリを有効にします。コンテナ技術はユーザーデバイス上の企業アプリとデータを個人用アプリとデータから分離します。これにより、包括的なポリシーベースの制御に基づいて、カスタム開発したモバイルアプリやサードパーティ製のモバイルアプリ、BYO モバイルアプリをすべて保護することができます。

Citrix Endpoint Management には、アプリレベルの暗号化も含まれています。Citrix Endpoint Management はデバイスのパスコードを必要とせずに、MDX 対応アプリ内に保存されたデータを単独で暗号化します。ポリシーを適用するためにデバイスを管理する必要もありません。

- iOS デバイスの場合、Citrix Endpoint Management は、FIPS で検証された強力な暗号化サービスとキーチェーンなどのライブラリを使用します。
- OpenSSL は、さまざまなデバイスプラットフォーム用の FIPS 検証済みモジュールを提供します。OpenSSL は、移行中のデータと、デバイスの管理と登録に必要な証明書をさらに保護します。
- Citrix Endpoint Management は、MAM SDK の共有コンテナ API を使用して、同じキーチェーンアクセスグループを持つアプリ間で管理対象コンテンツを共有します。たとえば、登録されたアプリを介してユーザー証明書を共有できるため、アプリはセキュアなコンテナから証明書を取得できます。
- Citrix Endpoint Management は、プラットフォームによって提供されるデバイス暗号化を使用します。
- アプリレベルの Citrix Endpoint Management MAM コントロールは、コンプライアンスチェックを実行して、アプリの起動時にデバイスの暗号化が有効になっていることを検証します。

Citrix Endpoint Management による転送データの保護

ユーザーのモバイルデバイスと内部ネットワークとの間を移動するデータは、転送データと呼ばれます。MDX アプリコンテナ技術は、内部ネットワークに対するアプリケーション専用の VPN アクセスを、NetScaler Gateway を介して提供します。

従業員がモバイルデバイスからセキュアなエンタープライズネットワーク上の次のリソースにアクセスしようとする状況を想定します:

- 企業のメールサーバー
- 企業イントラネットでホストされている SSL 対応の Web アプリケーション
- ファイルサーバーまたは Microsoft SharePoint に保存されているドキュメント

MDX を使用すると、アプリケーション専用のマイクロ VPN を介して、モバイルデバイスからこれらすべての企業リソースにアクセスできます。各デバイスに専用のマイクロ VPN トンネルが用意されます。

マイクロ VPN 機能により、信頼できないモバイルデバイスのセキュリティを脅かす可能性がある、デバイス全体での VPN は不要になります。そのため、内部ネットワークがマルウェアや企業システム全体に感染する可能性のある攻撃にさらされることはありません。企業のモバイルアプリと個人用のモバイルアプリを、1 つのデバイス上で共存させることができます。

セキュリティレベルをさらに強化するために、代替 NetScaler Gateway ポリシーを使用して MDX 対応アプリを構成することができます。これは認証およびアプリとのマイクロ VPN セッションに使用します。代替 NetScaler Gateway を［マイクロ VPN セッション必須とする］ポリシーと組み合わせて使用し、アプリを指定のゲートウェイで再認証するようにできます。通常、このようなゲートウェイには、別の（確実性の高い）認証要件およびトラフィック管理ポリシーが割り当てられています。

セキュリティ機能に加え、マイクロ VPN 機能も圧縮アルゴリズムなどのデータ最適化テクノロジを提供します。圧縮アルゴリズムによって、次のことが保証されます:

- 最小限のデータのみが転送される
- 転送は可能な限り最短時間で行われる。スピードはユーザーエクスペリエンスを向上させるため、モバイルデバイスの導入を成功させる重要な要因です。

次のような場合は、デバイスポリシーを定期的に再評価します:

- デバイスのオペレーティングシステムの更新がリリースされたことで、Citrix Endpoint Management の新しいバージョンに新しいポリシーまたは更新されたポリシーが含まれる場合
- デバイスの種類を追加する場合:

  多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、iOS、Android、Windows デバイスの間で異なるほか、Android デバイスの製造元によっても違いがある場合があります。

- Citrix Endpoint Management の運用を、企業の新しいセキュリティポリシーやコンプライアンス規制など、企業や業界の変化に対して継続的に同期させる場合

- 新しいバージョンの MAM SDK に新しいポリシーまたは更新されたポリシーが含まれている場合
- アプリを追加または更新する場合
- アプリや要件が新しくなった結果、ユーザー用に新しいワークフローを統合する必要がある場合

アプリポリシーとユースケースのシナリオ

Citrix Secure Hub で利用可能なアプリを選択できますが、それらのアプリが Citrix Endpoint Management とやり取りする方法を定義しなくてはならない場合もあります。次の場合に、アプリポリシーを使用します:

- 一定の期間が経過した後にユーザーを認証できるようにする場合。
- ユーザーに自分の情報へのオフラインアクセスを提供する場合。

次のセクションでは、いくつかのポリシーと使用例について説明します。

- MAM SDK を使用して iOS アプリや Android アプリに統合できるサードパーティポリシーの一覧については、「MAM SDK の概要」を参照してください。
- プラットフォームごとの MDX ポリシーの一覧については、「MDX ポリシーの概要」を参照してください。

認証ポリシー

- デバイスのパスコード

  このポリシーを使用する理由：デバイスのパスコードポリシーを有効にして、デバイスのデバイスパスコードが有効になっている場合にのみ、ユーザーが MDX アプリにアクセスできるようにします。この機能によってデバイスレベルでの iOS 暗号化が保証されます。

  ユーザーの例：このポリシーを有効にすると、iOS デバイスでパスコードを設定しない限りは、MDX アプリにアクセスできないようになります。

- アプリのパスコード

  このポリシーを使用する理由：アプリのパスコードポリシーを有効にすると、Citrix Secure Hub で管理対象アプリを認証しない限りは、アプリを開いてデータにアクセスできないようになります。Citrix Endpoint Management コンソールで、［設定］**>**［クライアントプロパティ］で 構成する内容に応じて、ユーザーは Active Directory のパスワード、Citrix PIN、または iOS TouchID で認証できます。クライアントのプロパティで非アクティブタイマーを設定すると、タイマーが切れるまでの間に Citrix Secure Hub が管理対象アプリの再認証をユーザーに求めないようにすることができます。

  アプリのパスコードは、デバイスのパスコードとは異なります。デバイスパスコードポリシーがデバイスにプッシュされると、Citrix Secure Hub はユーザーにパスコードまたは PIN の構成を要求します。ユーザーがデバイスの電源をオンにしたとき、または無通信タイマーが期限切れになったときに、デバイスのロックを解除する必要があります。詳しくは、Citrix Endpoint Management でのユーザー認証についての記事を参照してください。

ユーザーの例：デバイス上で Citrix Secure Web アプリケーションを開くときに非アクティブ期間が過ぎていると、Citrix PIN を入力しない限りは Web サイトを参照できなくなります。

- マイクロ **VPN** セッションを必須とする

  このポリシーを使用する理由：アプリケーションの実行に Web アプリ（Web サービス）へのアクセスが必要な場合は、このポリシーを有効にします。Citrix Endpoint Management は、アプリを使用する前に、エンタープライズネットワークに接続するか、アクティブなセッションがあることを確認するようユーザーに要求します。

  ユーザーの例：［マイクロ VPN セッションを必須とする］ポリシーが有効になっている MDX アプリをユーザーが開こうとすると、ネットワークに接続しない限り、アプリを使用できなくなります。接続には、携帯ネットワークまたは Wi-Fi サービスを使用する必要があります。

- 最大オフライン期間

  このポリシーを使用する理由：このポリシーを追加のセキュリティオプションとして使用します。このポリシーでは、指定した期間にわたってアプリをオフラインで実行するユーザーが、アプリのユーザー権を再確認し、ポリシーを更新することが必要になります。

  ユーザーの例：最大オフライン期間を適用した MDX アプリを構成すると、オフラインタイマー期間が終了するまでの間、ユーザーはオフラインでアプリを開いて使用できます。期間が終了した時点で、ユーザーは携帯電話または Wi-Fi サービス経由でネットワークに接続し、プロンプトが表示されたら再認証する必要があります。

その他のアクセスポリシー

- アプリ更新猶予期間 **(**時間**)**

  このポリシーを使用する理由：アプリ更新猶予期間とは、アプリストアにリリースされている新しいバージョンのアプリを更新するまでの間、ユーザーが利用できる時間です。猶予期間が終了した時点で、ユーザーはアプリを更新しない限り、アプリ内のデータにアクセスできなくなります。この値を設定する場合には、モバイルワーカーのニーズ、特に海外旅行で長期間オフラインの状態になる可能性があるユーザーのニーズを考慮してください。

  ユーザーの例：アプリストアに新しいバージョンの Citrix Secure Mail をロードしてから、アプリ更新猶予期間を 6 時間に設定します。Citrix Secure Hub ユーザーが 6 時間を超えても Citrix Secure Mail をアップグレードしないと、アプリストアにルーティングされます。

- アクティブなポーリング周期 **(**分**)**

  このポリシーを使用する理由：アクティブなポーリング周期とは、Citrix Endpoint Management がアプリの App Lock や App Wipe などのセキュリティアクションを実行するタイミングをチェックする間隔のことです。

  ユーザーの例：アクティブなポーリング期間ポリシーを 60 分に設定した場合、App Lock コマンドを送信すると、最後のポーリングが行われてから 60 分以内にロックが発生します。

非準拠デバイスの動作ポリシー

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

アプリ相互作用ポリシー

これらのポリシーを使用する理由：アプリ相互作用ポリシーを使用して、MDX アプリからデバイス上の他のアプリへのドキュメントおよびデータの流れを制御します。たとえば、ユーザーが以下を実行できないようにします：

- コンテナの外の個人アプリにデータを移動する
- コンテナの外からコンテナ化されたアプリにデータを貼り付ける

ユーザーの例：アプリ相互作用ポリシーを［制限］に設定すると、ユーザーは Citrix Secure Mail から Citrix Secure Web にテキストをコピーできます。コンテナの外にある個人の Safari や Chrome ブラウザーにそのデータをコピーすることはできません。また、添付ドキュメントを Citrix Secure Mail から Citrix Files または QuickEdit で開くことができます。ユーザーは、添付されたドキュメントをコンテナの外にある自分の個人用ファイル表示アプリで開くことはできません。

アプリ制限ポリシー

これらのポリシーを使用する理由：アプリ制限ポリシーは、MDX アプリが開いている間にユーザーがアプリからアクセスできる機能を制御するために使用します。この制限により、アプリの実行中に悪意のある行為が発生しないようにすることができます。アプリ制限ポリシーは、iOS と Android でわずかに異なります。たとえば iOS では、MDX アプリの実行中に iCloud へのアクセスをブロックできます。Android では、MDX アプリの実行中に近距離無線通信（NFC）の使用を停止できます。

ユーザーの例：アプリ制限ポリシーを有効にして MDX アプリでの iOS の音声入力をブロックすると、ユーザーは MDX アプリの実行中に、iOS キーボードの音声入力機能を使用できなくなります。そのため、ユーザーの音声入力データが、セキュリティで保護されていないサードパーティのクラウド音声入力サービスに渡されることはありません。ユーザーがコンテナの外で個人のアプリを開いた場合、ユーザーが個人的な通信手段として使用する音声入力のオプションは、変わらず利用できます。

アプリのネットワークアクセスポリシー

これらのポリシーを使用する理由：アプリのネットワークアクセスポリシーは、デバイスのコンテナ内の MDX アプリから社内ネットワークにあるデータへのアクセスを提供するために使用します。トンネル-Web SSO オプションでは、HTTP トラフィックおよび HTTPS トラフィックのトンネリングのみが許可されます。このオプションは、HTTP および HTTPS トラフィックと PKINIT 認証にシングルサインオン（SSO）を提供します。

ユーザーの例：トンネリングが有効になっている MDX アプリをユーザーが開くと、Web ブラウザーがイントラネットサイトを開きます。ユーザーが VPN を開始する必要はありません。アプリは、マイクロ VPN 技術を使用して内部サイトに自動的にアクセスします。

アプリの地理位置情報およびジオフェンシングポリシー

これらのポリシーを使用する理由：アプリの地理位置情報およびジオフェンシングを制御するポリシーには、中心点経度、中心点緯度、および RADIUS が含まれます。これらのポリシーの対象には、特定の地理的領域にある MDX アプリのデータに対するアクセスが含まれます。このポリシーでは緯度および経度座標の半径によって地理的エリアを定義します。定義された半径外にあるアプリをユーザーが使用しようとしても、アプリはロックされたままで、アプリデータにはアクセスできません。

ユーザーの例：ユーザーが自分の職場がある場所にいる間は M&A のデータにアクセスできますが、オフィスの外に移動すると、この機微なデータにアクセスできなくなります。

Citrix Secure Mail アプリポリシー

- バックグラウンドネットワークサービス

  このポリシーを使用する理由： Citrix Secure Mail のバックグラウンドネットワークサービスは、Citrix Secure Ticket Authority（STA）を利用します。これは、事実上 NetScaler Gateway 経由で接続する SOCKS5 プロキシです。STA は長時間の接続をサポートしており、マイクロ VPN に比べてバッテリー寿命が長くなります。そのため、STA は常に接続しておくメールに最適です。Citrix Secure Mail ではこれらの設定を構成することをお勧めします。NetScaler for XenMobile ウィザードでは、Citrix Secure Mail の STA が自動的に設定されます。

  ユーザーの例： STA が有効になっていないときに Android ユーザーが Citrix Secure Mail を開くと、VPN を開くように求められ、デバイス上で開かれたまま維持されます。STA が有効になっているときに Android ユーザーが Citrix Secure Mail を開くと、Citrix Secure Mail は VPN を必要とせずシームレスに接続されます。

- デフォルトの同期間隔

  このポリシーを使用する理由：この設定では、ユーザーが Citrix Secure Mail に初めてアクセスしたときに、メールが Citrix Secure Mail と同期する既定の日数を指定します。メールの 2 週間は 3 日間よりも同期に時間がかかります。同期するデータが増えると、ユーザーのセットアッププロセスが長くなります。

  ユーザーの例：ユーザーが最初に Citrix Secure Mail を設定したときのデフォルトの同期間隔が 3 日に設定されているとします。ユーザーは、過去 3 日間に受信した受信トレイ内の任意のメールを表示できます。4 日以上経過したメールを見たい場合は、検索することができます。そうすることでサーバーに保存されている古いメールが Citrix Secure Mail に表示されます。Citrix Secure Mail のインストール後に、ユーザーはそれぞれのニーズに合わせてこの設定を変更できます。

デバイスポリシーとユースケースの動作

Citrix Endpoint Management がデバイスをどのように管理するかは、デバイスポリシー（MDM ポリシーとも呼ばれます）によって決まります。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。以下の一覧ではデバイスポリシーの一部と、その使用方法について説明します。すべてのデバイスポリシーの一覧については、「デバイスポリシー」を参照してください。

- アプリインベントリポリシー

  このポリシーを使用する理由：ユーザーがインストールしたアプリを表示するには、アプリインベントリポリシーをデバイスに展開します。ポリシーを展開しない場合、ユーザーがアプリストアからインストールしたアプリのみが表示され、個人的にインストールしたアプリは表示されません。特定のアプリが企業デバイスで実行されないようにするには、このポリシーを使用します。

  ユーザーの例： MDM 管理デバイスを使用するユーザーがこの機能を無効にすることはできません。ユーザーが個人的にインストールしたアプリケーションは、Citrix Endpoint Management 管理者に表示されます。

- アプリのロックポリシー

  このポリシーを使用する理由： Android 用のアプリのロックポリシーを使用すると、アプリを許可リストまたは禁止リストに追加できます。たとえば、許可されたアプリの場合、キオスクデバイスを構成できます。ユーザーがインストールできるアプリが制限されるため、通常は企業所有のデバイスにのみアプリのロックポリシーを展開します。上書きパスワードを設定すると、ブロックされているアプリにユーザーがアクセスできます。

  ユーザー例： Angry Birds アプリをブロックするというアプリのロックポリシーを展開するとします。ユーザーは Google Play から Angry Birds アプリをインストールできますが、アプリを開くと管理者がアプリをブロックした旨のメッセージが表示されます。

- 接続のスケジューリングポリシー

  このポリシーを使用する理由：接続のスケジューリングポリシーは Windows Mobile デバイスが MDM 管理、アプリのプッシュ、およびポリシーの展開を行うために Citrix Endpoint Management に接続できるようにします。Android および Android Enterprise デバイスの場合、Google の Firebase Cloud Messaging（FCM）を使用します。FCM は Citrix Endpoint Management への接続を制御します。スケジューリングオプションは次のとおりです：

  - しない：手動で接続します。ユーザーがデバイス上の Citrix Endpoint Management から接続を開始する必要があります。デバイスにセキュリティポリシーを展開できなくなるため、実稼働環境ではこのオプションはお勧めしません。このオプションを選択すると、ユーザーに新規アプリやポリシーが配信されなくなります。デフォルトでは、［しない］オプションは有効になっています。
  - 毎：指定された間隔で接続します。ロックやワイプなどのセキュリティポリシーを送信すると、このポリシーは次回デバイスが接続されたときに Citrix Endpoint Management によって処理されます。
  - スケジュールを定義： Citrix Endpoint Management は、ネットワーク接続が失われるとユーザーデバイスを Citrix Endpoint Management サーバーに再接続しようとします。また、指定した期間にわたり、定期的にコントロールパケットを送信することで接続を監視します。

ユーザーの例：登録されたデバイスにパスコードポリシーを展開する場合。スケジューリングポリシーを利用することで、デバイスは一定の間隔でサーバーに接続し、新しいポリシーを収集できます。

- 資格情報ポリシー

  このポリシーを使用する理由：多くはネットワークポリシーとともに使用され、この資格情報ポリシーを利用することで、証明書による認証が必要な内部リソースの認証に使用する証明書を展開できます。

  ユーザーの例：デバイスにワイヤレスネットワークを構成するネットワークポリシーを展開します。Wi-Fi ネットワークには認証用の証明書が必要です。資格情報ポリシーが証明書を展開すると、証明書はオペレーティングシステムのキーストアに格納されます。それによりユーザーは、内部リソースに接続したときに証明書を選択できます。

- **Exchange** ポリシー

  このポリシーを使用する理由： Citrix Endpoint Management には、Microsoft Exchange ActiveSync のメールを配信する 2 つのオプションがあります。

  - **Citrix Secure Mail** アプリ：パブリックアプリストアまたはアプリストアから配布する Citrix Secure Mail アプリを使用してメールを配信します。
  - ネイティブメールアプリ：デバイス上のネイティブメールクライアントで ActiveSync メールを有効にできます。Active Directory 属性からマクロでユーザーデータを取得して入力できます。`${ user.username }`ならユーザー名、`${ user.domain }`ならユーザードメインのように、ユーザーデータを入力できます。

  ユーザーの例： Exchange ポリシーをプッシュすると、Exchange Server の詳細がデバイスに送信されます。次に Citrix Secure Hub はユーザーに認証を求め、メールの同期を開始します。

- 場所ポリシー

  このポリシーを使用する理由：場所ポリシーでは、デバイスの GPS が Citrix Secure Hub で有効になっている場合に、地図上でそのデバイスの場所を検出できます。このポリシーを展開し、Citrix Endpoint Management から locate コマンドを送信すると、デバイスは場所の座標を返します。

  ユーザーの例：場所ポリシーが展開され、GPS がデバイスで有効になっている場合にユーザーがデバイスを紛失したときは、Citrix Endpoint Management Self Help Portal にログオンして［検索］オプションを選択すると、デバイスの場所を地図上に表示できます。ユーザーは、Citrix Secure Hub に位置情報サービスの使用を許可するかを選択します。ユーザーがデバイスを自分で登録した場合に、位置情報サービスの使用を強制することはできません。このポリシーを使用するときにもう 1 つ考慮すべき事項は、バッテリー寿命への影響です。

- パスコードポリシー

  このポリシーを使用する理由：パスコードポリシーを使用すると、管理対象デバイスに PIN コードまたはパスワードを適用できます。このパスコードポリシーでは、デバイス上でパスコードの複雑さやタイムアウトを設定できます。

ユーザー例：パスコードポリシーを管理対象デバイスに展開すると、Citrix Secure Hub はユーザーにパスコードまたは PIN の構成を要求します。起動時、または無通信タイマーの期限が切れたときに、パスコードまたは PIN によってユーザーはデバイスにアクセスできます。

- プロファイル削除ポリシー

  このポリシーを使用する理由：ユーザーのグループにポリシーを展開した後で、そのポリシーをユーザーのサブセットから削除する必要があるとします。プロファイル削除ポリシーを作成することで、選択したユーザーのポリシーを削除できます。次に、展開規則を使用して、指定したユーザーのみにプロファイル削除ポリシーを展開します。

  ユーザーの例：プロファイル削除ポリシーをユーザーデバイスに展開すると、ユーザーは変更に気付かない可能性があります。たとえば、デバイスカメラを無効にする制限がプロファイル削除ポリシーによって削除された場合、ユーザーにはその変更は表示されません。ユーザーエクスペリエンスに影響を及ぼす変更については、ユーザーに通知することを検討してください。

- 制限ポリシー

  このポリシーを使用する理由：制限ポリシーによって、管理対象デバイスの機能をロックダウンおよび制御するさまざまなオプションを使用できます。サポートされているデバイスに対して、何百もの制限オプションを有効にできます。制限オプションの例：デバイスでのカメラやマイクの無効化、ローミング規則の適用、アプリストアのようなサードパーティサービスへのアクセスの適用。

  ユーザーの例： iOS デバイスに制限を展開すると、ユーザーは iCloud または Apple App Store にアクセスできなくなることがあります。

- 契約条件ポリシー

  このポリシーを使用する理由：デバイスを管理することの法的な意味を、ユーザーに知らせる必要がある場合があります。また、企業データをデバイスにプッシュするときの、セキュリティ上のリスクをユーザーに認識させる場合もあります。契約条件文書では、ユーザー登録の前に規則および通知を公開できます。

  ユーザーの例：登録処理中に契約条件の情報をユーザーに表示します。指定された条件の受け入れを拒否した場合、登録処理は終了し、ユーザーは企業データにアクセスすることはできません。レポートを生成して HR/法務/コンプライアンスチームに提供し、条件を了承または拒否した対象者を確認できます。

- **VPN** ポリシー

  このポリシーを使用する理由： VPN ポリシーは、古い VPN ゲートウェイ技術を使用するバックエンドシステムへのアクセスを提供するために使用します。このポリシーではさまざまな VPN プロバイダー（Cisco AnyConnect、Juniper、Citrix VPN）がサポートされています。また、このポリシーを CA にリンクして、オンデマンドで VPN を有効にできます（VPN ゲートウェイがこのオプションをサポートしている場合）。

  ユーザーの例： VPN ポリシーを有効にすると、ユーザーのデバイスは、ユーザーが内部ドメインにアクセスしたときに VPN 接続を開きます。

- **Web** クリップポリシー

このポリシーを使用する理由：Web クリップポリシーは、Web サイトが直接開かれるアイコンをデバイスにプッシュする場合に使用します。Web クリップには Web サイトへのリンクが含まれており、カスタムアイコンを加えることができます。デバイス上では、Web クリップはアプリのアイコンのように見えます。

ユーザーの例：ユーザーが Web クリップアイコンをクリックしてインターネットのサイトを開き、必要なサービスにアクセスできます。Web リンクを使用する方が、Web ブラウザーアプリを開いてリンクアドレスを入力するよりも便利です。

- ネットワークポリシー

  このポリシーを使用する理由：ネットワークポリシーを使用すると、SSID、認証データ、および設定データなどの Wi-Fi ネットワークの詳細を管理対象デバイスに展開できます。

  ユーザーの例：ネットワークポリシーを展開すると、デバイスが自動的に Wi-Fi ネットワークに接続してユーザー認証を行うことで、ユーザーがネットワークにアクセスできるようになります。

- **Endpoint Management Store** ポリシー

  このポリシーを使用する理由：このアプリストアは、ユーザーが必要とするすべての企業アプリとデータリソースを、管理者が公開できる一元化されたアプリストアです。管理者は、次の項目を追加できます：

  - Web アプリ、SaaS アプリ、MAM SDK 対応アプリ、または MDX でラップされたアプリ
  - Citrix 業務用モバイルアプリ
  - .ipa または.apk ファイルなどのネイティブモバイルアプリ
  - Apple App Store アプリと Google Play アプリ
  - Web リンク
  - Citrix StoreFront を使用して公開された Citrix Virtual Apps

  ユーザーの例：デバイスを Citrix Endpoint Management に登録すると、ユーザーは Citrix Secure Hub アプリを通じてアプリストアにアクセスし、利用できるすべての企業アプリとサービスを表示できます。ユーザーはアプリをクリックすると、インストール、データへのアクセス、アプリの評価とレビュー、アプリストアからのアプリの更新プログラムのダウンロードを実行できます。

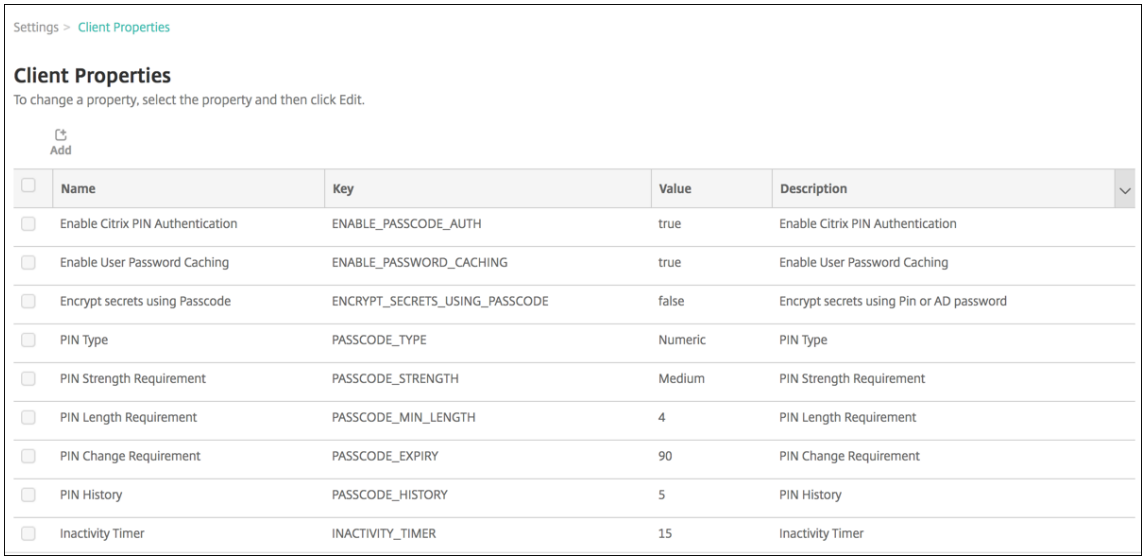
クライアントプロパティ

March 15, 2024

クライアントプロパティには、ユーザーのデバイスの Citrix Secure Hub に直接提供される情報が含まれています。これらのプロパティを使用して、Citrix PIN などの詳細設定を構成することができます。クライアントプロパティは Citrix サポートから取得します。

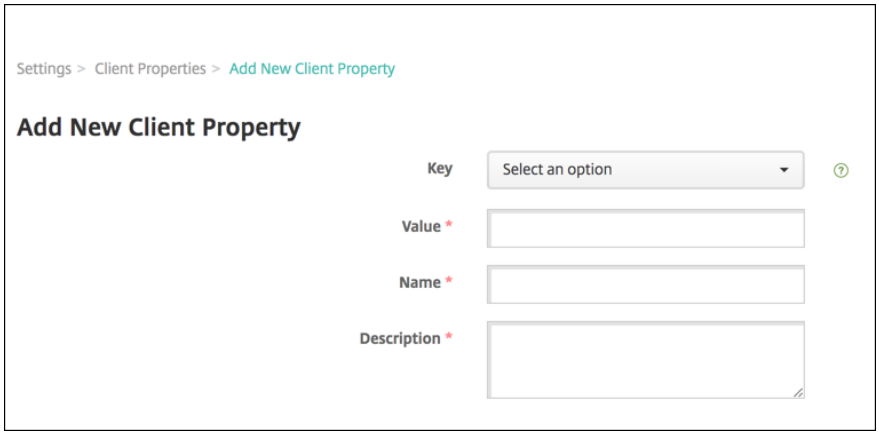
クライアントプロパティは、Citrix Secure Hub のリリースごとに変更されるほか、クライアントアプリのリリースで変更されることもあります。一般的に構成されたクライアントプロパティについて詳しくは、「クライアントプロパティリファレンス」を参照してください。

1. Citrix Endpoint Management コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［クライアント］の下の ［クライアントプロパティ］をクリックします。［クライアントプロパティ］ページが開きます。このページでは、クライアントプロパティを追加、編集、または削除できます。



クライアントプロパティを追加するには

1. ［追加］をクリックします。［新しいクライアントプロパティの追加］ページが開きます。



2. 次の設定を構成します：

   - キー：ドロップダウンリストから、追加するプロパティキーを選択します。重要：設定を更新する前に、Citrix サポートにご連絡ください。特殊キーを要求できます。
   - 値：選択したプロパティの値です。
   - 名前：プロパティの名前です。
   - 説明：プロパティの説明です。

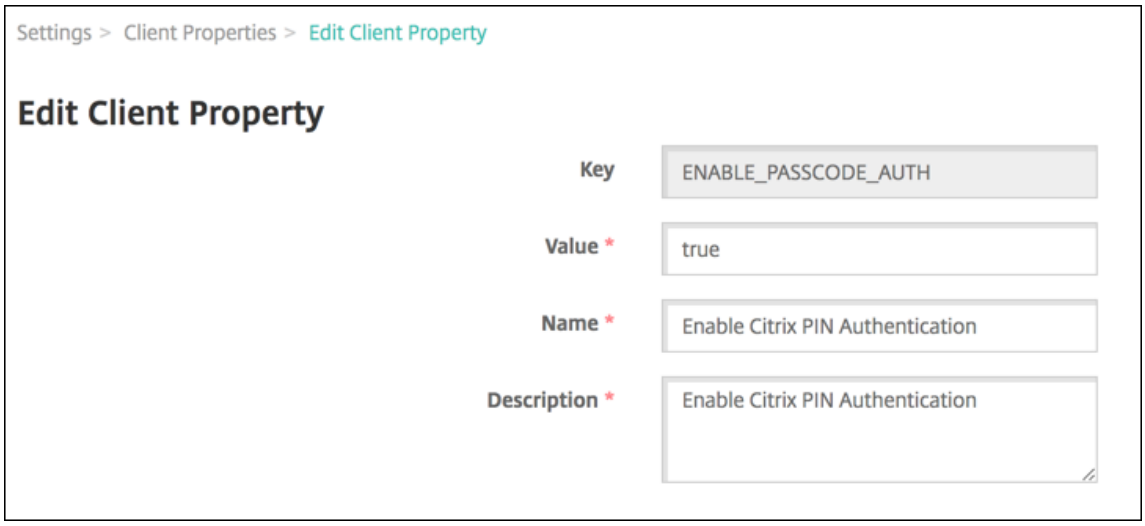
3. ［保存］をクリックします。

クライアントプロパティを編集するには

1. ［クライアントプロパティ］の表で、編集するクライアントプロパティを選択します。

   クライアントプロパティの横にあるチェックボックスをオンにすると、クライアントプロパティ一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを開きます。

2. ［編集］をクリックします。［クライアントプロパティの編集］ページが開きます。



3. 必要に応じて以下の情報を変更します。

   - キー：このフィールドは変更できません。
   - 値：プロパティの値です。
   - 名前：プロパティの名前です。
   - 説明：プロパティの説明です。

4. ［保存］をクリックして変更を保存するか、［キャンセル］をクリックしてプロパティを変更せずそのままにします。

クライアントプロパティを削除するには

1. ［**Client Properties**］の表で、削除するクライアントプロパティを選択します。

   各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。

2. ［削除］をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］をクリックします。

クライアントプロパティリファレンス

以下に、Citrix Endpoint Management の定義済みクライアントプロパティとそのデフォルトの設定を示します:

- **ALLOW_CLIENTSIDE_PROXY**
  - 表示名: ALLOW_CLIENTSIDE_PROXY
  - ユーザーが iOS 電話で構成したプロキシを使用する必要がある場合は、このカスタムポリシーをデフォルトの **true** に設定したままにします。

    一部のユーザーは既に、デバイスの ［設定］ **>** ［**Wi-Fi**］ **>** ［プロキシの構成］ でプロキシを構成しています。これらのユーザーに対して Citrix Secure Hub が開かない場合は、次のいずれかの操作を実行してもらいます:

    * デバイスからプロキシ構成を削除してから、Citrix Secure Hub を再起動する。
    * デバイスを別の Wi-Fi ネットワークに接続する。Citrix Secure Hub が再認証されると、**ALLOW_CLIENTSIDE_PROXY** プロパティを取得して開きます。
  - **ALLOW_CLIENTSIDE_PROXY** が **false** で、ユーザーがデバイス上でプロキシを構成している場合、Citrix Endpoint Management はプロキシを検出します。ただし、Citrix Secure Hub はプロキシを使用せず、エラーメッセージを表示します。プロキシが有効になっているアクセスポイントまたはルーターにデバイスが接続している場合、Citrix Endpoint Management はプロキシを検出しません。安全性を最大限に高めるためには、証明書ピン留め機能を使用することをお勧めします。Citrix Secure Hub での証明書ピン留め機能の有効化については、「証明書ピン留め」を参照してください。
  - このカスタムクライアントポリシーを構成するには、［設定］ **>** ［クライアントプロパティ］ の順に選択し、カスタムキー **ALLOW_CLIENTSIDE_PROXY** を追加して、［値］ を設定します。
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 表示名: MDX Container Self-Destruct Period
  - 非アクティブな状態で指定の日数を経過すると、自動削除機能により、Citrix Secure Hub および管理対象アプリにアクセスできなくなります。指定の期間を過ぎると、アプリを使用できなくなります。データのワイプでは、各インストール済みアプリのアプリデータ（アプリキャッシュ、ユーザーデータなど）が消去されます。

    非アクティブ状態とは、サーバーが一定期間、ユーザーの検証をするための認証要求を受け取っていない状態です。このプロパティが 30 日であるとします。ユーザーがアプリを 30 日を超えて使用しない状況が続くと、このポリシーが適用されます。

    このグローバルセキュリティポリシーは、既存のアプリのロックポリシーおよびワイプポリシーの機能拡張であり、iOS および Android のプラットフォームに適用されます。
  - このグローバルポリシーを構成するには、［設定］ **>** ［クライアントプロパティ］ の順に選択し、カスタムキー **CONTAINER_SELF_DESTRUCT_PERIOD** を追加します。

  - 値：日数

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 表示名：Send device logs to IT help desk
  - このプロパティで、IT ヘルプデスクへのログ送信機能を有効または無効にします。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**

- **DISABLE_LOGGING**
  - 表示名：Disable Logging
  - このプロパティを使用して、ユーザーが各自のデバイスからログを収集してアップロードすることを防ぎます。このプロパティで、Citrix Secure Hub およびすべてのインストール済み MDX アプリのログを無効にします。ユーザーが［サポート］ページから任意のアプリのログを送信することはできません。メール作成ダイアログボックスは開きますが、ログは添付されません。ログが無効になっているというメッセージが表示されます。またこの設定により、Citrix Endpoint Management コンソールで Citrix Secure Hub と MDX アプリのログ設定が更新されるのを防ぎます。

    このプロパティを **true** に設定すると、Citrix Secure Hub によって ［アプリケーションログのブロック］が **true** に設定されます。これによって、新しいポリシーが適用されたときに MDX アプリのログが停止します。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**（ロギングは有効です）

- **ENABLE_CRASH_REPORTING**
  - 表示名：Enable Crash Reporting
  - **true** の場合、Citrix Secure Hub for iOS および Android での問題のトラブルシューティングを目的として、Citrix によりクラッシュレポートと診断情報が収集されます。**false** の場合、データは収集されません。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**true**

- **ENABLE_CREDENTIAL_STORE**
  - 表示名：Enable Credential Store
  - 資格情報ストアを有効にすると、Android および iOS のユーザーは、Citrix 業務用モバイルアプリにアクセスする場合にパスワードを１度入力するだけで済むようになります。Citrix PIN を有効にするかどうかに関係なく、資格情報ストアを使用できます。Citrix PIN を有効にしないと、ユーザーは Active Directory のパスワードを入力します。Citrix Endpoint Management が資格情報ストアで Active Directory のパスワードの使用をサポートしているのは、Citrix Secure Hub とパブリックストアアプリに対してのみです。資格情報ストアで Active Directory のパスワードを使用する場合、Citrix Endpoint Management では PKI 認証はサポートされません。

- Citrix Secure Mail での自動登録では、このプロパティを **true** に設定する必要があります。
- このカスタムクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］の順に選択し、カスタムキー **ENABLE_CREDENTIAL_STORE** を追加して、［値］を **true** に設定します。

- **ENABLE_PASSCODE_AUTH**
  - 表示名：Enable Citrix PIN Authentication
  - このプロパティを使用すると、Citrix PIN 機能を有効にできます。ユーザーは、Citrix PIN またはパスコードにより、Active Directory パスワードの代わりに使用する PIN を定義するように求められます。ENABLE_PASSWORD_CACHING が有効になっているとき、または Citrix Endpoint Management で証明書認証を使用しているときは、この設定が自動的に有効になります。

    オフライン認証では、Citrix PIN がローカルで検証されて、要求したアプリやコンテンツへのアクセスがユーザーに許可されます。オンライン認証では、Citrix PIN またはパスコードによって Active Directory パスワードまたは証明書のロックが解除され、Citrix Endpoint Management との認証を実行するために送信されます。

    ENABLE_PASSCODE_AUTH が true で ENABLE_PASSWORD_CACHING が false の場合、Citrix Secure Hub でパスワードが保存されないため、オンライン認証では常にパスワードの入力が求められます。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**

- **ENABLE_PASSWORD_CACHING**
  - 表示名：Enable User Password Caching
  - このプロパティによって、Active Directory パスワードをモバイルデバイス上にローカルにキャッシュできます。このプロパティを **true** に設定する場合、**ENABLE_PASSCODE_AUTH** プロパティを **true** に設定する必要があります。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。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**

- **ENABLE_TOUCH_ID_AUTH**
  - 表示名：Enable Touch ID Authentication
  - Touch ID 認証をサポートするデバイスの場合、このプロパティでデバイスの Touch ID 認証を有効または無効にします。要件：

    ユーザーデバイスでは、Citrix PIN または LDAP を有効にする必要があります。LDAP 認証がオフの場合（証明書による認証が使用されている場合など）、ユーザーは Citrix PIN を設定する必要があります。この場合、クライアントプロパティの **ENABLE_PASSCODE_AUTH** が **false** であっても、Citrix Endpoint Management に Citrix PIN が必要になります。

ENABLE_PASSCODE_AUTH を **false** に設定します。これによって、ユーザーがアプリを起動したとき、Touch ID の使用を促すメッセージが表示されます。

- 設定可能な値：**true** または **false**
- デフォルト値：**false**

- **ENABLE_WORXHOME_CEIP**
  - 表示名：Enable Citrix Secure Hub CEIP
  - このプロパティにより、カスタマーエクスペリエンス向上プログラムがオンになります。この機能により、構成および使用データが定期的に、匿名で Citrix に送信されます。このデータは、Citrix Endpoint Management の品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。
  - 値：**true** または **false**
  - デフォルト値：**false**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 表示名：Encrypt secrets using Passcode
  - このプロパティでは、機密データをプラットフォームベースのネイティブな格納場所（iOS キーチェーンなど）ではなく、デバイスの Secret Vault に格納します。このプロパティにより、重要なデータの強力な暗号化が可能になるとともにユーザーエントロピーが追加されます。ユーザーエントロピーは、ユーザーが生成した、ユーザーしか知らないランダムな PIN コードです。

    ユーザーデバイスのセキュリティを強化するために、このプロパティを有効にすることをお勧めします。これによって、Citrix PIN の認証メッセージが増えます。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**

- **INACTIVITY_TIMER**
  - 表示名：Inactivity Timer
  - このプロパティで、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］設定を［オン］に設定します。［アプリのパスコード］設定を［オフ］に設定すると、ユーザーは完全認証を実行するよう Citrix Secure Hub に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。

    iOS では、Inactivity Timer は MDX アプリと MDX 以外のアプリの Citrix Secure Hub へのアクセスにも対応します。
  - 設定可能な値：正の整数
  - デフォルト値：**15**（分）

- **ON_FAILURE_USE_EMAIL**
  - 表示名：On failure Use Email to Send device logs to IT help desk
  - このプロパティで、メールを使用して IT にデバイスログを送信する機能を有効または無効にします。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**true**
- **PASSCODE_EXPIRY**
  - 表示名：PIN Change Requirement
  - このプロパティで、Citrix PIN またはパスコードが有効な期間を定義します。この期間を過ぎると、ユーザーは Citrix PIN またはパスコードを変更する必要があります。この設定を変更すると、現在の Citrix PIN またはパスコードの有効期限が切れた場合のみ、新しい値が設定されます。
  - 設定可能な値：**1** から **99** までの間を推奨。PIN をリセットする必要がないようにするためには、大きな値に設定してください（例：100,000,000,000）。有効期限を 1 から 99 日の間で設定し、その期間中に大きな値に変更した場合、PIN は最初に設定した期間の最終日に満期になり、満期がその後に設定されることはありません。
  - デフォルト値：**90**（日）
- **PASSCODE_HISTORY**
  - 表示名：PIN History
  - このプロパティでは、使用済みであり、Citrix PIN またはパスコードの変更時にユーザーが再使用できない Citrix PIN またはパスコードの個数を定義します。この設定を変更すると、ユーザーが Citrix PIN またはパスコードを次回再設定したときに新しい値が設定されます。
  - 設定可能な値：**1** から **99** までの間
  - デフォルト値：**5**
- **PASSCODE_MAX_ATTEMPTS**
  - 表示名：PIN Attempts
  - このプロパティで、完全認証が必要になる前に、ユーザーが誤った Citrix PIN またはパスコードを入力できる回数を定義します。完全認証に成功した後で、ユーザーは Citrix PIN またはパスコードを作成するように求められます。
  - 設定可能な値：正の整数
  - デフォルト値：**15**
- **PASSCODE_MIN_LENGTH**
  - 表示名：PIN Length Requirement
  - このプロパティは、Citrix PIN の最小文字数を定義します。
  - 設定可能な値：**4**～**10**
  - デフォルト値：**6**
- **PASSCODE_STRENGTH**

- 表示名：PIN Strength Requirement
- このプロパティで、Citrix PIN またはパスコードの強度を定義します。この設定を変更すると、ユーザーは、次回認証を求められたときに、Citrix PIN またはパスコードを作成するように求められます。
- 設定可能な値：**Low**、**Medium**、**High**、**Strong**
- デフォルト値：**Medium**
- PASSCODE_TYPE 設定に基づいた、各強度設定のパスワード規則は次のとおりです。

数字パスコードの規則は以下のとおりです。

パスコードの強度	数字パスコードの規則	許可	許可しない
低	すべての数字を任意の順序で使用できます	444444、123456、654321	
Medium（デフォルト設定）	すべての番号を同じにしたり連番にしたりすることはできません。	444333、124567、136790、555556、788888	444444、123456、654321
High	隣接する数字を同じにすることはできません。	123512、134134、132312、131313、987456	080080、112233、135579、987745、919199
Strong	同じ数字を 3 回以上使用しない。3 つ以上の連番を続けて使用しない。3 つ以上の連番を逆の順序で使用しない。	102983、085085、824673、132312	132132、131313、902030

英数字パスコードの規則は以下のとおりです。

パスコードの強度	英数字パスコードの規則	許可	許可しない
低	1 つ以上の数字と 1 つ以上の文字が含まれている必要があります	aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa	AAAaaa、aaaaaa、abcdef
Medium（デフォルト設定）	パスコード強度「低」の規則に加えて、文字およびすべての数字を同じにすることはできません。連続した文字および連続した数字は使用できません。	aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1 #、Ab123~	aaaa11、aa11aa、または aaa111; abcd12、bcd123、123abc、xy1234、xyz345、または cba123
High	1 つ以上の大文字、および 1 つ以上の小文字を含めます。	Abcd12、jkrtA2、23Bc#、AbCd	abcd12、DFGH2

パスコードの強度	英数字パスコードの規則	許可	許可しない
Strong	1 つ以上の数字、1 つ以上の特殊記号、1 つ以上の大文字、および 1 つ以上の小文字を含めます。	Abcd1 #、Ab123~、xY12 # 3、Car12 #、AAbc1 #	abcd12、Abcd12、dfgh12、jkrtA2

- **PASSCODE_TYPE**
  - 表示名：PIN Type
  - このプロパティで、数字の Citrix PIN または英数字パスコードのいずれをユーザーが定義できるようにするのかを定義します。［**Numeric**］を選択した場合、ユーザーは数字のみを使用できます（Citrix PIN）。［**Alphanumeric**］を選択した場合、ユーザーは文字と数字の組み合わせを使用できます（パスコード）。

    この設定を変更すると、ユーザーは、次回認証を求められたときに、新しい Citrix PIN またはパスコードを設定する必要があります。
  - 設定可能な値：**Numeric** または **Alphanumeric**
  - デフォルト値：**Numeric**
- **REFRESHINTERVAL**
  - 表示名：REFRESHINTERVAL
  - デフォルトでは、Citrix Endpoint Management は AutoDiscovery Server（ADS）のピン留め済み証明書に対して 3 日ごとに ping を実行します。更新時間を変更するには、［設定］**>**［クライアントプロパティ］でカスタムキー **REFRESHINTERVAL** を追加して、［値］を時間数に設定します。
  - デフォルト値：**72** 時間（3 日）
- **SEND_LDAP_ATTRIBUTES**
  - Android、iOS、または macOS デバイスを MAM-only で展開している場合、電子メール資格情報で Citrix Secure Hub に登録したユーザーが Citrix Secure Mail に自動的に登録されるように Citrix Endpoint Management を構成できます。これにより、ユーザーが追加の情報を入力したり、Citrix Secure Mail に登録するための追加の手順を実行する手間が省かれます。
  - このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］の順に選択し、カスタムキー **SEND_LDAP_ATTRIBUTES** を追加して、［値］を以下のように設定します。
  - 値:`userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme =${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
  - MDM ポリシーと同様、属性値はマクロとして指定されます。

- このプロパティのアカウントサービスレスポンスのサンプルを以下に示します。

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName
  =eng1,displayName=user\,test1,email=user@site.com\,user@site.
  com"name="SEND_LDAP_ATTRIBUTES"/>
  ```

- このプロパティでは、Citrix Endpoint Management はコンマ文字を文字列の終わりとして扱います。そのため、属性値にコンマが含まれる場合は、コンマの前にバックスラッシュを置きます。バックスラッシュは、含まれているコンマがクライアントによって属性値の末尾と解釈されるのを防ぎます。バックスラッシュ文字は「"\\"」と表します。

- **HIDE_THREE_FINGER_TAP_MENU**

  - このプロパティが設定されていないか、または **false** に設定されている場合、ユーザーはデバイスで 3 本指タップすることで隠し機能メニューにアクセスできます。隠し機能メニューによって、アプリケーションデータをリセットできます。このプロパティを **true** に設定すると、ユーザーは隠し機能メニューにアクセスできなくなります。
  - このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］の順に選択し、カスタムキー **HIDE_THREE_FINGER_TAP_MENU** を追加して、［値］を設定します。

- **TUNNEL_EXCLUDE_DOMAINS**

  - 表示名：Tunnel Exclude Domains
  - デフォルトでは、MDX は、Mobile Apps SDK およびアプリが各種機能で使用する一部のサービスエンドポイントを、Micro VPN トンネルから除外します。たとえば、このようなエンドポイントには、社内ネットワークを経由する必要がない、Google Analytics、Citrix Cloud サービス、Active Directory サービスなどのサービスが含まれます。このクライアントプロパティを使用して、除外対象ドメインのデフォルトの一覧を上書きします。
  - このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］の順に選択し、カスタムキー **TUNNEL_EXCLUDE_DOMAINS** を追加して、［値］を設定します。
  - 値：デフォルトの一覧をトンネルから除外するドメインで置き換えるには、ドメインサフィックスのコンマ区切りの一覧を入力します。すべてのドメインをトンネルに含めるには、「**none**」と入力します。デフォルトは：

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,
    cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics
    .com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.
    com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.
    com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.
    com,ssl.google-analytics.com,stream.launchdarkly.com
    ```

以下に、Citrix Endpoint Management のクライアントプロパティを示します：

ENABLE_MAM_NFACTOR_SSO:

- このプロパティを使用すると、NetScaler Gateway で高度な認証ポリシーを使用している場合、MAM の登録中または Secure Hub へのログイン中に MAM nFactor SSO を有効または無効にすることができます。値が **true** に設定されている場合、MAM の登録中または Secure Hub へのログイン中に MAM nFactor SSO が有効になります。
- このプロパティを構成するには、［設定］**>**［クライアントプロパティ］に移動し、［追加］をクリックします。［キー］ドロップダウンメニューで ［カスタム キー］を選択し、必要に応じて次の情報を更新します:
  - キー - ENABLE_MAM_NFACTOR_SSO
  - 値 - true or false
  - 名前 - ENABLE_MAM_NFACTOR_SSO
  - 説明 - 関連する説明を追加します

ユーザー登録オプション

March 15, 2024

ユーザーが iOS デバイスを Citrix Endpoint Management に追加できるようにする方法は数多くあります。詳細を検討する前に、どのデバイスを MDM+MAM、MDM、または MAM のいずれで登録するかを決定する必要があります。管理モードについて詳しくは、「管理モード」を参照してください。

最も高いレベルには、次の 4 つの登録オプションがあります。

- 登録招待状: ユーザーに登録招待状や招待 URL を送信します。登録招待状および URL は、Windows デバイスでは利用できません。
- **Self Help Portal**: ユーザーがアクセスするポータルを設定します。このポータルでは Citrix Secure Hub をダウンロードしたり、登録を要求したり、デバイス情報を表示したりできます。
- 手動登録: システムが起動していて登録可能であることをユーザーに知らせるメール、ハンドブック、その他の通信を送信します。ユーザーは Citrix Secure Hub をダウンロードし、デバイスを手動で登録します。
- エンタープライズ: デバイス登録のもう 1 つの選択肢は、Apple Deployment Program と Google Android Enterprise による登録です。これらの各プログラムを通して、従業員が使用する準備が整った事前設定済みデバイスを購入できます。詳しくは、Apple サポートの Apple Deployment Program の記事、およびAndroid Enterprise Web サイトにある Google Android Enterprise のドキュメントを参照してください。

登録招待状

iOS、macOS、Android Enterprise、または従来の Android デバイスを使用するユーザーに登録招待状メールを送信できます。登録招待状は、Windows デバイスでは利用できません。

また、iOS、macOS、Android Enterprise、Android、Windows デバイスを使用するユーザーに、SMTP を使用してインストールリンクを送信することもできます。詳しくは、「デバイスの登録」を参照してください。

登録招待状による方法を選択した場合、次のことができます:

- 登録セキュリティモードとして、[招待 **URL**]、[招待 **URL** および **PIN**]、または [招待 **URL** およびパスワード] のいずれかを選択できます。
- モードを任意に組み合わせて使用できます。
- Citrix Endpoint Management の [設定] ページからモードを有効にしたり無効にしたりできます。

各登録セキュリティモードについては、「登録セキュリティモードを構成する」を参照してください。

招待状は多くの目的にかないます。招待状の最も一般的な使用方法は、システムが利用でき、登録可能であることをユーザーに通知することです。招待 URL は一意的なものです。ユーザーが招待 URL を使用すると、その URL は 2 度と使用できなくなります。このプロパティを使用して、システムに登録するユーザーやデバイスを制限できます。

登録プロファイルを構成すると、特定のユーザーが登録できるデバイスの数を Active Directory のグループに基づいて制御できます。たとえば、財務部門でユーザーごとに 1 つのデバイスしか許可しないことができます。

特定の登録オプションを選ぶことで発生する追加コストや潜在的な危険に注意してください。SMTP を使用して招待状を送信するには、追加のインフラストラクチャが必要です。詳しくは、「通知」を参照してください。

また、招待状をメールで送信する場合は、ユーザーが Citrix Secure Hub 以外のメールにアクセスする方法があることを確認してください。MDM 登録用の Active Directory パスワードの代わりに、ワンタイムパスワード（OTP）登録セキュリティモードを使用できます。

Self-Help Portal

Self Help Potal には、管理者が Citrix Endpoint Management コンソールにアクセスする場合と同じ URL からアクセスできます。エンドユーザーには、管理コンソールではなく Self Help Portal が表示されます。ユーザーは、Self-Help Portal で Citrix Secure Hub をダウンロードし、登録を要求し、デバイス情報を表示できます。

ポータルを設定するには、[設定] **>** [サーバープロパティ] の順に選択します:

- `shp.console.enable`: **True** に設定すると、Self-Help Portal にアクセスできます。
- `enable.new.shp`: **True** に設定すると、ユーザーは Self Help Portal からデバイスを有効にできます。

手動登録

手動登録では、ユーザーは AutoDiscovery またはサーバー情報の入力によって Citrix Endpoint Management に接続します。AutoDiscovery を利用する場合、ユーザーはメールアドレス、またはユーザープリンシパル名形式の Active Directory 資格情報のみを使用してログオンします。AutoDiscovery を利用しない場合、サーバーアドレスと Active Directory の資格情報を入力する必要があります。AutoDiscovery のセットアップについて詳しくは、「Citrix Endpoint Management AutoDiscovery サービスのセットアップ」を参照してください。

手動登録は、さまざまな方法で簡単に行うことができます。ガイドを作成してユーザーに配布し、自身で登録してもらうことができます。IT 部門に依頼して、特定の時間枠でユーザーのグループを手動で登録してもらうこともできます。または、ユーザーが資格情報やサーバー情報を入力する必要がある同様の方法を利用することもできます。

ユーザーオンボーディング

環境を設定したら、どのようにしてユーザーを環境に取り込むかを決定する必要があります。この記事の前のセクションで、ユーザー登録セキュリティモードの詳細について説明しています。このセクションでは、ユーザーにアプローチする方法について説明します。

オープン登録か選択的招待か

ユーザーのオンボーディング時には、次の 2 つの基本的な方法で登録を許可できます:

- オープン登録。デフォルトでは、LDAP 資格情報と Citrix Endpoint Management 環境の情報を持つユーザーが登録できます。
- 制限付きの登録。招待状を持つユーザーのみが登録できるようにして、ユーザー数を制限できます。さらに、Active Directory グループごとにオープン登録を制限することもできます。

招待状による方法を使用すると、ユーザーが登録できるデバイスの数を制限することもできます。ほとんどの場合、オープン登録を適用できますが、考慮すべき点がいくつかあります。

- MAM 登録の場合は、Active Directory グループメンバーシップを通して簡単にオープン登録を制限できます。
- MDM 登録の場合は、Active Directory グループメンバーシップに基づいて登録できるデバイスの数を制限できます。環境内で企業デバイスのみを許可する場合、この制限は通常、問題ではありません。ただし、環境内のデバイス数を制限する BYOD ワークプレースでは、この方法を検討することをお勧めします。

選択的招待は通常、必要な作業がオープン登録よりも少し多いため、オープン登録ほど頻繁に行われません。ユーザーが自分のデバイスを環境に登録するには、各ユーザーに固有の招待状を送信する必要があります。登録招待状を送信する方法については、「登録招待の送信」を参照してください。

環境に登録する各ユーザーまたはグループには、招待を送信します。組織の規模によっては、このプロセスに時間がかかる場合があります。Active Directory グループを使用して一括して招待状を作成することも可能ですが、この方法は間をおいて何度も行う必要があります。

ユーザーとの最初の連絡

オープン登録を使用するか選択的招待を使用するかを決定し、それらの環境を設定したら、ユーザーに登録オプションを知らせる必要があります。

選択的招待の方法を使用する場合は、電子メールメッセージが対応に含まれます。オープン登録の場合も、Citrix Endpoint Management コンソールからメールを送信できます。詳しくは、「登録招待の送信」を参照してください。

どちらの場合も、メール用の SMTP サーバーが必要となります。これらのサーバーは、決定の際に追加費用として考慮すべき場合があります。新規ユーザーが情報にアクセスする方法を検討してください。すべてのユーザーが Citrix Endpoint Management からメールにアクセスする場合には、招待メールの送信が問題になります。

オープン登録環境では、Citrix Endpoint Management 以外の方法で送信することもできます。その場合は、関連する情報をすべて含めるよう注意してください。Citrix Secure Hub アプリを入手できる場所や登録に使用する方法をユーザーに伝えます。検出を無効にしている場合は、Citrix Endpoint Management サーバーのアドレスも伝える必要があります。AutoDiscovery の設定の詳細については、「Citrix Endpoint Management AutoDiscovery サービスのセットアップ」を参照してください。

アプリのプロビジョニングとプロビジョニング解除

March 15, 2024

アプリケーションのプロビジョニングの中心は、モバイルアプリのライフサイクル管理です：Citrix Endpoint Management 環境内でのモバイルアプリの準備、構成、配信、管理を行います。場合によっては、プロビジョニングプロセスの一環としてアプリケーションコードの開発や変更も行います。Citrix Endpoint Management には、アプリのプロビジョニングに使用できるさまざまなツールとプロセスが用意されています。

アプリのプロビジョニングに関するこの記事を読む前に、アプリおよびユーザーコミュニティについて読むことをお勧めします。組織でユーザーに提供する予定のアプリの種類を確定したら、アプリをライフサイクル全体にわたって管理するプロセスの概要を策定できるようになります。

アプリのプロビジョニングプロセスを定める際には、次の点を考慮してください。

- アプリのプロファイリング：最初は組織のアプリの数が限られているかもしれません。しかし、ユーザーへの普及率が増加し環境が拡大されるにつれて、管理するアプリの数が急増する可能性があります。アプリのプロビジョニングを簡単に管理できるように、初めからアプリのプロファイルを明確に定義する必要があります。アプリのプロファイリングを行うことにより、非技術的な観点から、アプリを論理的なグループに分類できます。たとえば、次の要素に基づいてアプリのプロファイルを作成します。
  - バージョン：追跡用のアプリのバージョン
  - インスタンス：ユーザー集団別に、異なるアクセスレベルなどを設定してインスタンスを複数展開
  - プラットフォーム：iOS、Android、または Windows
  - 対象ユーザー：標準ユーザー、部署、経営幹部
  - 所有権：アプリを所有する部門
  - 種類：MDX、パブリック、Web および SaaS、または Web リンク
  - アップグレードサイクル：アプリをアップグレードする頻度

  - ライセンス：ライセンス要件と所有権
  - MAM SDK または MDX ポリシー：モバイルアプリへの MDX 機能の適用
  - ネットワークアクセス：シングルサインオンによる HTTP および HTTPS トラフィックのトンネリング（トンネル-Web SSO）などのアクセスの種類。

例：

要素	Citrix Secure Mail	メール	社内	Epic Rover
バージョン	10.1	10.1	X.x	X.x
インスタンス	VIP	医師	医療	医療
プラットフォーム	iOS	iOS	iOS	iOS
対象ユーザー	VIP ユーザー	医師	臨床ユーザー	臨床ユーザー
所有権	IT 部門	IT 部門	IT 部門	IT 部門
種類	MDX	MDX	ネイティブ	パブリック
アップグレードサイクル	四半期単位	四半期単位	年単位	-
ライセンス	-	-	-	一括購入
MDX ポリシー	はい	はい	はい	いいえ
ネットワークアクセス	VPN	VPN	VPN	パブリック

- アプリのバージョン管理：アプリのバージョンの管理および追跡は、プロビジョニングプロセスの重要な要素です。通常、ユーザーがバージョン管理を意識することはありません。ユーザーは、アプリの新しいバージョンがダウンロード可能になったときに通知を受け取るだけです。管理者の観点では、実稼働サイトに影響を与えないために、実稼働環境以外でアプリの各バージョンのレビューおよびテストを行うことも重要です。

  また、特定のアップグレードが必要かどうかを評価することも重要です。通常、アプリのアップグレードには、特定のバグへの修正などのマイナーアップグレードと、大幅な変更が加えられたメジャーリリースの 2 種類があります。いずれの場合も、アプリのリリースノートを慎重に確認し、アップグレードが必要かどうかを評価してください。

- アプリ開発：開発したモバイルアプリに MAM SDK を統合すると、それらのアプリに MDX 機能が適用されます。「MAM SDK の概要」を参照してください。

  MAM SDK は、2023 年 7 月に廃止予定の MDX Toolkit に代わる機能です。アプリのラッピングについては、MDX Toolkitを参照してください。ラップされたアプリのアプリプロビジョニングプロセスは、標準的なラップされていないアプリのプロビジョニングプロセスとは異なります。

- アプリのセキュリティ：プロビジョニングプロセスの一環として、個々のアプリまたはアプリプロファイルのセキュリティ要件を定義します。アプリを展開する前に、セキュリティ要件を特定の MDM または MAM ポリ

シーにマッピングできます。こうした準備により、アプリケーションをより簡単に、すばやく展開できます。例：

  - 特定のアプリを異なる方法で展開できます。
  - Citrix Endpoint Management 環境でアーキテクチャの変更を加えることができます。こうした変更では、アプリによって必要なセキュリティコンプライアンスの種類が異なります。たとえば、特定のアプリでは、エンドツーエンドの SSL 暗号化またはジオフェンシングが必要になる場合があります。

- アプリの配信： Citrix Endpoint Management では、アプリを MDM アプリまたは MAM アプリとして配信できます。MDM アプリはアプリストアに表示されます。ストアを使用することで、パブリックアプリまたはネイティブアプリをユーザーに簡単に配信できます。デバイスレベルの制限を強制する以外には、アプリの制御は必要ありません。ただし、MAM を使用したアプリの配信では、アプリの配信およびアプリ自体を完全に制御できます。一般的には、MAM を使用したアプリの配信をお勧めします。
- アプリケーションのメンテナンス：
  - 初期監査の実施：実稼働環境に存在するアプリのバージョン、および最新のアップグレードサイクルを把握しておきます。アップグレードが必要になった特定の機能やバグの修正を記録します。
  - ベースラインの確立：アプリごとに、最新の安定リリースのリストを維持します。アップグレード後に予期しない問題が発生した場合のために、以前のバージョンに戻す準備をしておきます。ロールバック計画を作成します。実稼働環境に展開する前に、テスト環境でアプリのアップグレードをテストします。可能であれば、まず一部の実稼働環境のユーザーにアップグレードを展開してから、ユーザーベース全体に展開します。
  - Citrix のソフトウェアのアップデート通知およびサードパーティソフトウェアベンダーの通知の購読：アプリの最新リリースに関する最新の情報を常に把握するために重要です。早期アクセスリリース（EAR）ビルドを事前に入手し、テストできる場合もあります。
  - ユーザーへの通知の方針の作成：アプリのアップグレードが利用可能になった場合のユーザーへの通知方法を定めます。展開前に、ユーザーにトレーニングを提供してください。アプリの更新前に、複数の通知の送信を検討してください。アプリによっては、メールでの通知や Web サイトでの通知が最適な場合もあります。

アプリのライフサイクル管理には、アプリの初期展開から廃棄までのライフサイクル全体が含まれます。アプリのライフサイクルには、次の段階があります：

1. 仕様要件：ビジネスケースとユーザー要件から着手します。
2. 開発：アプリがビジネスニーズを満たしていることを検証します。
3. テスト：テストユーザー、問題、バグを特定します。
4. 展開：実稼働環境のユーザーにアプリを展開します。
5. メンテナンス：アプリのバージョンを更新します。実稼働環境でアプリを更新する前に、テスト環境にアプリを展開します。

ダッシュボードベースの操作

March 15, 2024

Citrix Endpoint Management コンソールのダッシュボードにアクセスすると、情報を一目で確認することができます。この情報を使用して、ウィジェットで問題や成功を速やかに確認できます。

ダッシュボードは、Citrix Endpoint Management コンソールに最初にサインオンすると表示される画面です。コンソールの別の場所からダッシュボードにアクセスするには、［分析］をクリックします。ページのレイアウトを編集したり表示されるウィジェットを編集するには、ダッシュボードの ［カスタマイズ］をクリックします。

- マイダッシュボード：最大 4 つのダッシュボードを保存できます。ダッシュボードを個別に編集し、保存したダッシュボードを選択してそれぞれを表示することができます。
- レイアウトスタイル：この行では、ダッシュボードに表示するウィジェットの数とレイアウトを選択することができます。
- ウィジェット選択：ダッシュボードに表示する情報を選択することができます。
  - 通知：左側の数字の上のチェックボックスをオンにして、ウィジェットの上に通知バーを追加します。このバーには、準拠デバイス数、非アクティブデバイス数、24 時間以内にワイプまたは登録されたデバイス数が表示されます。
  - プラットフォームごとのデバイス：プラットフォームごとの管理対象デバイス数と管理対象外デバイス数が表示されます。
  - キャリアごとのデバイス：キャリアごとの管理対象デバイス数と管理対象外デバイス数が表示されます。各バーをクリックすると、プラットフォームごとの内訳が表示されます。
  - プラットフォームにより管理されているデバイス：プラットフォームごとの管理対象デバイス数が表示されます。
  - プラットフォームにより管理されていないデバイス：プラットフォームごとの管理対象外デバイス数が表示されます。このグラフに表示されるデバイスにはエージェントがインストールされている場合がありますが、特権が失効またはワイプされています。
  - **ActiveSync** ゲートウェイ状態ごとのデバイス： ActiveSync ゲートウェイの状態ごとにグループ化されたデバイス数が表示されます。この情報では拒否、許可、または不明の状態が表示されます。各バーをクリックするとプラットフォームごとの内訳が表示されます。
  - 所有権ごとのデバイス：所有権の状態ごとにグループ化されたデバイス数が表示されます。この情報ではコーポレート所有、従業員所有、または不明の所有権状態が表示されます。
  - 失敗したデリバリーグループ展開：失敗した展開の合計数がパッケージごとに表示されます。展開に失敗したパッケージのみが表示されます。
  - ブロックされた理由ごとのデバイス： ActiveSync でブロックされたデバイス数が表示されます。
  - インストール済みアプリ：このウィジェットを使用して、アプリ名を入力すると、グラフにはそのアプリに関する情報が表示されます。
  - 一括購入アプリライセンス使用状況： Apple の一括購入アプリのライセンス使用状況に関する統計データが表示されます。

使用例

環境の監視におけるダッシュボードウィジェットの多彩な活用法の一例を次に示します。

- Citrix 業務用モバイルアプリを展開したところ、業務用モバイルアプリをデバイスにインストールできないというサポートチケットを受け取りました。［コンプライアンス外デバイス］ウィジェットおよび ［インストール済みアプリ］ウィジェットを使用して、Citrix 業務用モバイルアプリがインストールされていないデバイスを確認します。
- 非アクティブなデバイスを環境から削除してライセンスを解放できるように、こうしたデバイスを監視するとします。こうした統計情報を把握するには、［非アクティブ デバイス］ウィジェットを使用します。
- データが正しく同期されないというサポートチケットを受け取りました。［**ActiveSync** ゲートウェイ状態ごとのデバイス］ウィジェットおよび ［ブロックされた理由ごとのデバイス］ウィジェットを使用すると、この問題に ActiveSync が関連しているかどうかを特定できます。

レポート

環境のセットアップおよびユーザーの登録後、レポートを実行すると環境に関する情報を確認できます。Citrix Endpoint Management には、実際の環境でのデバイスの動作状況を把握するためのレポートが多数組み込まれています。詳しくは、「レポート」を参照してください。

役割ベースのアクセス制御と **Citrix Endpoint Management** のサポート

March 15, 2024

Citrix Endpoint Management では、役割ベースのアクセス制御（RBAC）を使用して、Citrix Endpoint Management コンソール、Self Help Portal、パブリック API などの Citrix Endpoint Management システム機能へのユーザーアクセスとグループアクセスを制限します。この記事では、Citrix Endpoint Management に組み込まれた役割について説明し、RBAC を活用した Citrix Endpoint Management のサポートモデルを決定するための考慮事項について説明します。

組み込みの役割

次の組み込みの役割に付与されたアクセス権を変更したり、役割を追加したりできます。各役割とそのデフォルト設定に関連したすべてのアクセス権と機能権限については、『Role-Based Access Control Defaults（役割ベースのアクセス制御の初期設定）』をダウンロードしてください。各機能の定義については、「RBAC を使用した役割の構成」を参照してください。

Admin の役割

付与されるデフォルトのアクセス権:

- システムへのフルアクセス。ただし、Self Help Portal は除きます。
- デフォルトでは、管理者は接続の確認やサポートバンドルの作成などの一部のサポートタスクを実行できます。

注意事項:

- 管理者の一部または全員が Self Help Portal にアクセスする必要がありますか。管理者の役割を編集するか、管理者の役割を追加できます。
- 一部の管理者または管理者グループのアクセスをさらに制限するには、管理者テンプレートに基づいて役割を追加し、権限を編集します。

ユーザー

付与されるデフォルトのアクセス権:

- Self Help Portal へのアクセス権。認証済みユーザーは登録リンクを生成できます。これらのリンクを使用して、デバイスを登録したり、登録招待状を自己送信したりできます。
- Citrix Endpoint Management コンソールへの制限付きアクセス権:デバイス機能(デバイスのワイプやロック/ロック解除、コンテナのロック/ロック解除、場所の参照と地理的制限の設定、デバイスの呼び出し、コンテナパスワードのリセットなど)、登録招待状の追加、削除、送信を行うことができます。

注意事項:

- ユーザー役割を使用すると、ユーザーは自分のことは自分自身でできるようになります。
- 共有デバイスをサポートするには、共有デバイス登録用のユーザー役割を作成します。

Citrix Endpoint Management サポートモデルに関する考慮事項

採用可能なサポートモデルは多様で、レベル 1 とレベル 2 のサポートをサードパーティが担当し、レベル 3 とレベル 4 のサポートは従業員が担当するような場合があります。サポート負荷をどのように分散させるかに関わらず、このセクションで説明する考慮事項で、ご利用の Citrix Endpoint Management 環境とユーザーベースに固有の点に留意してください。

ユーザーは企業所有のデバイスを持っていますか、**BYO** デバイスを持っていますか?
サポートに影響する第一の問題は、Citrix Endpoint Management 環境でユーザーデバイスを所有しているのが誰なのかということです。ユーザーが企業所有のデバイスを持っている場合は、デバイスをロックダウンする方法として、サポートのレベルを下げることが考えられます。その場合、デバイスの問題と使用方法に関してユーザーを支援するヘルプデスクを提供することができます。サポートが必要なデバイスのタイプに応じて、ヘルプデスクの RBAC デバイスプロビジョニングとサポートの役割をどのようにするかを検討してください。

ユーザーが BYO デバイスを持っている場合、組織ではデバイスサポートの独自の情報源をユーザー自身が探すよう期待することが考えられます。そのような場合、組織が提供するサポートは、Citrix Endpoint Management 固有の問題に対応する管理者の役割のようなものになります。

デスクトップのサポートモデルはどのようなものですか?
デスクトップのサポートモデルが他の企業所有デバイスに適しているかどうかを検討します。同じサポート組織を利用できますか? どのような追加のトレーニングが必要ですか?

Citrix Endpoint Management Self Help Portal へのアクセス権をユーザーに付与しますか?
Citrix Endpoint Management へのアクセス権をユーザーに付与するのは好ましくないとする組織もありますが、ユーザーに自己サポートの能力を与えると、サポート組織の負荷を軽減できます。RBAC のデフォルトのユーザー役割に、付与したくない権限が含まれる場合、付与したい権限のみを含む新しい役割を作成することを検討してください。要件を満たすのに必要な数の役割を作成できます。

Citrix のサポートプロセス

March 15, 2024

Citrix 製品に関する問題の解決には、Citrix Technical Support Services を利用できます。このサポートグループでは、回避策と解決策を提示しているほか、開発チームと連携してソリューションの提供も行っています。

Citrix Consulting Services と Citrix Education Services では、製品のトレーニング、製品の使用や構成、インストール、環境設計およびアーキテクチャに関連する支援をそれぞれご用意しています。

Citrix Consulting Services では、以下のような Citrix 製品に関連するプロジェクトのサポートを行っています:

- 概念実証
- 経済効果の評価
- インフラストラクチャのヘルスチェック
- 設計要件の分析
- アーキテクチャ設計の検証
- 統合
- 運用プロセスの開発

Citrix Education Services では、Citrix の仮想化、クラウド、ネットワーキング技術に関する最高レベルの IT トレーニングと認定試験を提供しています。

サポートケースを作成する前に、Citrix のセルフヘルプリソースと推奨事項を十分に活用することをお勧めします。たとえば、Citrix の技術専門家が作成した記事や掲示板にアクセスしたり、Citrix のソリューションおよびテクノロジに関する製品ドキュメントを参照したり、Citrix の役員、製品チーム、技術専門家からの率直な意見を読んだりすることができます。それぞれ、Knowledge Center、製品ドキュメント、ブログのページを参照してください。

よりインタラクティブな支援が必要な場合には、各種ディスカッションフォーラムに参加してください。他のユーザーに質問をして現実に即した答えを得たり、ユーザーグループや分科会でアイデア、意見、技術情報、ベストプラク

ティスを共有したりすることができます。また、Citrix サポートのソーシャルネットワーキングサイト経由で Citrix サポートのエンジニアと対話することもできます。Support ForumsおよびCitrix Communityの各ページを参照してください。

また、トレーニングおよび認定コースを受けて、スキルを磨くことも可能です。「Citrix Education」を参照してください。

Citrix Insight Services では、Citrix 環境向けにシンプルなトラブルシューティングプラットフォームとヘルスチェッカーをオンラインで提供しています。Citrix Endpoint Management、Citrix Virtual Apps and Desktops、Citrix Hypervisor、NetScaler Gateway で利用できます。分析ツールのページを参照してください。

テクニカルサポートを受けるには、電話か Web 経由でサポートケースを作成します。重要度が低および中程度の問題には Web で、重要度の高い問題の場合は電話でご連絡ください。Citrix Endpoint Management の問題に対するサポート対応については、「Citrix サポートサービス」を参照してください。

Citrix Services には、Citrix ソリューションを長年にわたり提供してきた経験を持ち、高度なトレーニングを受けた総合担当者として、テクニカルリレーションシップマネージャーも在籍しています。Citrix Services の提供サービスとメリットについて詳しくは、『Citrix Worldwide Services Guide』を参照してください。

Citrix Endpoint Management でのグループ登録招待状の送信

November 29, 2023

Author:
John Bartel III

Citrix Endpoint Management でグループおよびネストされたグループに登録招待状を送信できます。登録招待状は、Windows デバイスでは利用できません。

グループ招待状を設定するときは、1 つまたは複数のデバイスプラットフォームを指定できます。企業所有のデバイスと従業員が所有するデバイスを区別できるように、デバイスにタグを付けることもできます。次に、ユーザーデバイスの認証の種類を設定します。

> 注:
>
> カスタム通知テンプレートを使用する予定の場合は、登録セキュリティモードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「通知テンプレートの作成と更新」を参照してください。

ユーザーアカウント、役割、および登録セキュリティモードと招待状の基本的な構成について詳しくは、「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。

一般的な手順

1. Citrix Endpoint Management コンソールで、［管理］**>**［登録招待］に移動します。
2. 画面の左上にある ［追加］をクリックし、［招待の追加］をクリックします。
3. ［宛先］メニューの ［グループ］をクリックします。

   このステップでは、1 つまたは複数のプラットフォームを選択できます。社内に異なるオペレーティングシステムプラットフォームが混在している場合は、すべてのプラットフォームを選択します。特定のプラットフォームを使用するユーザーがいないことがわかっている場合は、そのプラットフォームの選択をオフにします。
4. 招待プロセス中にデバイスにタグを付けるように選択できます。［コーポレート］または ［従業員］を選択します。

   タグ付けにより、企業所有のデバイスと従業員所有のデバイスを簡単に区別することができます。
5. ［ドメイン］一覧で、グループが存在するドメインを選択します。
6. ［グループ］一覧で、招待状を送信する Active Directory グループを選択します。
7. ［登録モード］では、ユーザーに対する登録セキュリティの種類を設定できます。

   - ユーザー名およびパスワード
   - 高セキュリティ
   - 招待 URL
   - 招待 URL および PIN
   - 招待 URL およびパスワード
   - 2 要素
   - ユーザー名および PIN

   > 注:
   >
   > 高セキュリティ登録セキュリティモードは廃止されました。登録招待状を送信するには、登録セキュリティモードとして、［招待 **URL**］、［招待 **URL** および **PIN**］、または ［招待 **URL** およびパスワード］のいずれかのみを使用できます。［ユーザー名およびパスワード］、［**2** 要素］、［ユーザー名および **PIN**］のいずれかで登録するデバイスの場合、Citrix Secure Hub をダウンロードして資格情報を手動で入力する必要があります。

8. エージェントダウンロード、登録用 **URL**、登録 **PIN**、および 登録確認用 テンプレートでは、過去に作成したカスタムの通知テンプレートを選択します。または、一覧に記載されているデフォルトを選択します。

   これらの通知テンプレートでは、Citrix Endpoint Management 内で構成した SMTP サーバー設定を使用します。続行する前にまず SMTP 情報を設定してください。

   > 注:

> ［有効期限］および ［最大試行数］のオプションは、選択した ［登録モード］オプションに基づいて変更されます。ユーザーはこれらのオプションを変更できません。

9. ［招待状を送信］で［オン］を選択し、［保存］および［送信］をクリックしてプロセスを完了します。

ネストされたグループのサポート

ネストされたグループを使用して招待状を送信できます。通常、ネストされたグループは、同じ権限を持つグループが互いにバインドされている大規模な環境で使用されます。

［設定］**>** ［**LDAP**］に移動し、［ネストされたグループをサポートする］オプションを有効にします。

トラブルシューティングと既知の制限事項

問題： Active Directory グループから削除したユーザーにも招待状が送信されます。

解決策： Active Directory 環境の規模によっては、変更がすべてのサーバーに反映されるまでに最大 6 時間かかることがあります。ユーザーまたはネストされたグループが最近削除された場合、Citrix Endpoint Management では引き続きこのユーザーがグループの一部と見なされる可能性があります。

このため、ユーザーに別のグループへの招待状を送信する前に、最大 6 時間待つことをお勧めします。

Citrix Secure Mail のプッシュ通知用に **EWS** で証明書ベースの認証を構成する

March 15, 2024

Citrix Secure Mail のプッシュ通知が機能するには、次の操作を実行する必要があります：

- Exchange Server を証明書ベースの認証用に構成します。証明書ベースの認証で Citrix Secure Hub を Citrix Endpoint Management に登録する場合には、この要件が特に必要です。
- Exchange メールサーバーの Active Sync および Exchange Web サービス（EWS）仮想ディレクトリで、証明書ベースの認証を構成します。

これらの構成を完了しないと、Citrix Secure Mail のプッシュ通知へのサブスクリプションが失敗するほか、Citrix Secure Mail でバッジの更新が行われません。

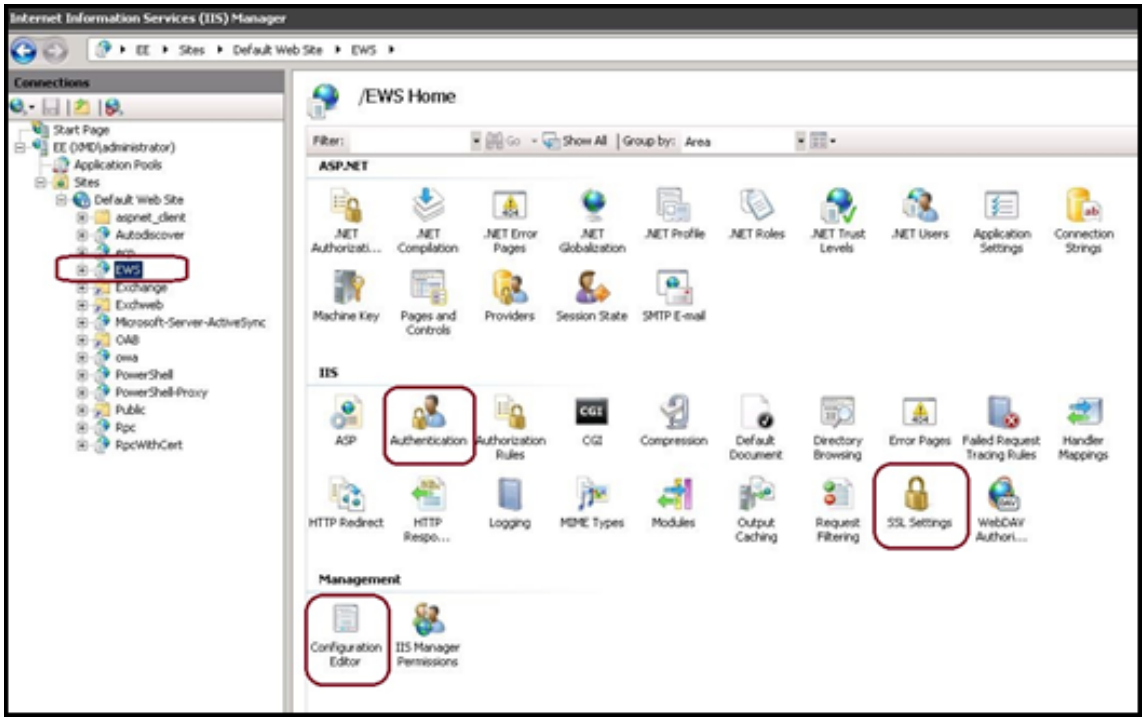
この記事では、証明書ベースの認証を構成する手順について説明します。この構成は、特に Exchange Server の EWS 仮想ディレクトリに対するものです。

構成を開始するには、次の手順を実行します：

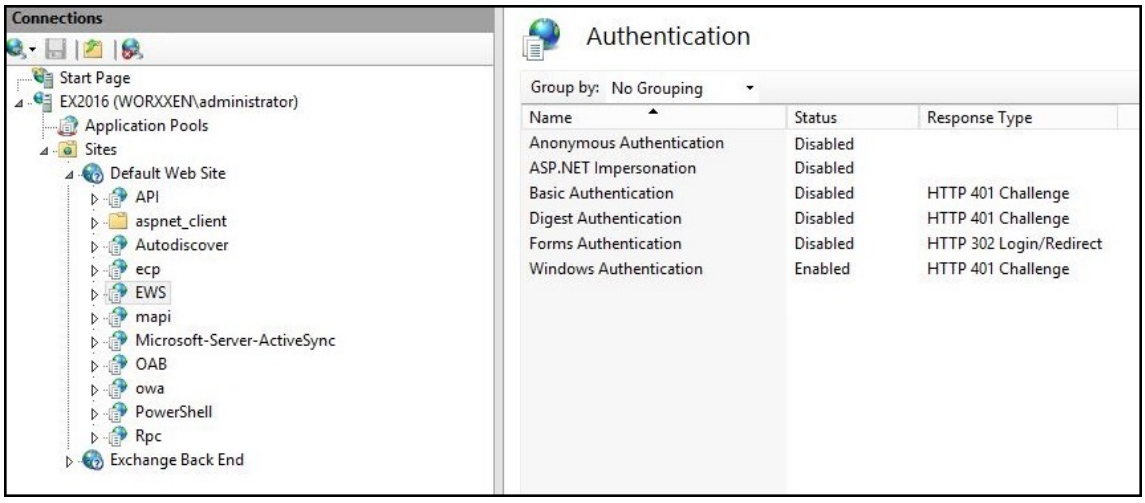
1. EWS 仮想ディレクトリがインストールされているサーバーにログオンします。

2. IIS マネージャーコンソールを開きます。
3. ［既定の **Web** サイト］で、［EWS 仮想ディレクトリ］をクリックします。

   認証、SSL、構成エディターのスナップインは、IIS マネージャーコンソールの右側にあります



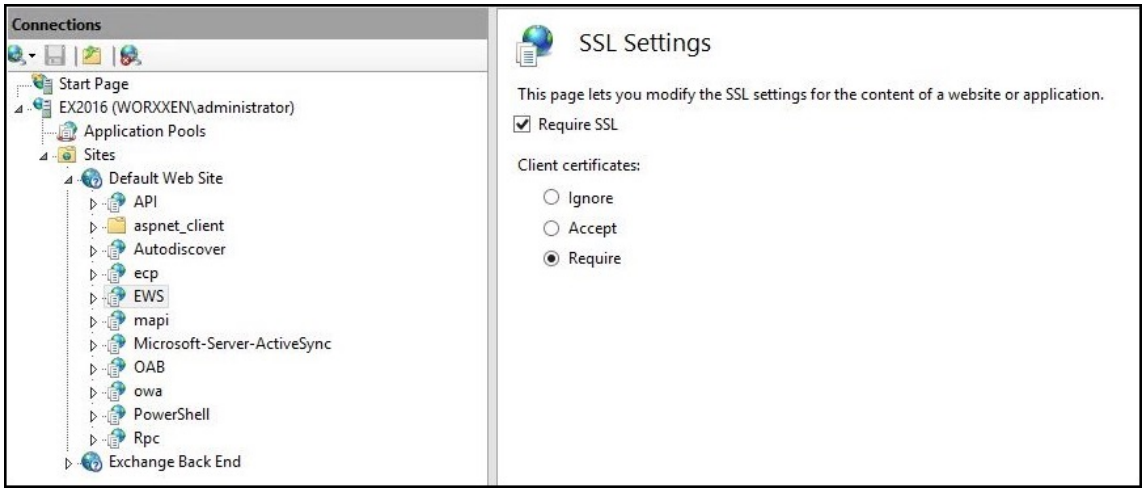
4. 次の図に示すように、EWS の 認証 設定が構成されていることを確認します。



5. EWS 仮想ディレクトリの **SSL** 設定 を構成します。

   a) ［**SSL** を必要とする］チェックボックスをオンにします。

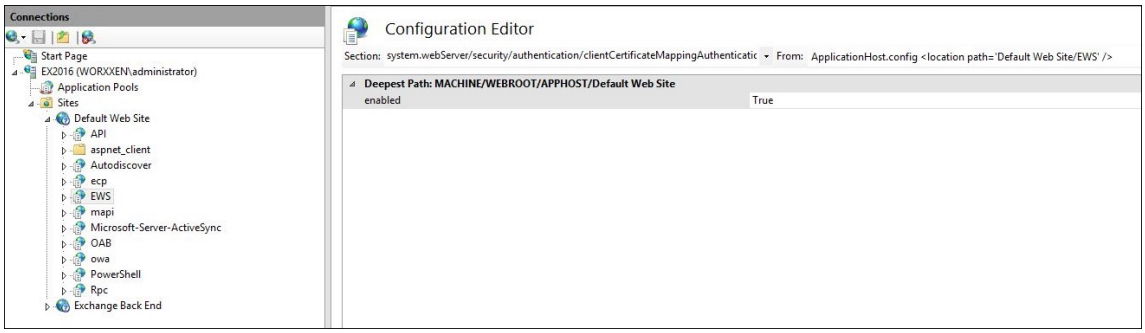
   b) ［クライアント証明書］で、［必須］をクリックします。または、他の EWS メールクライアントが Exchange Server の認証にユーザー名およびパスワードを使用する場合、［承認］をクリックします。



6. 構成エディターをクリックします。[**Section**] ドロップダウンリストの次のセクションに移動します:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. [有効] の値を **True** に設定します。



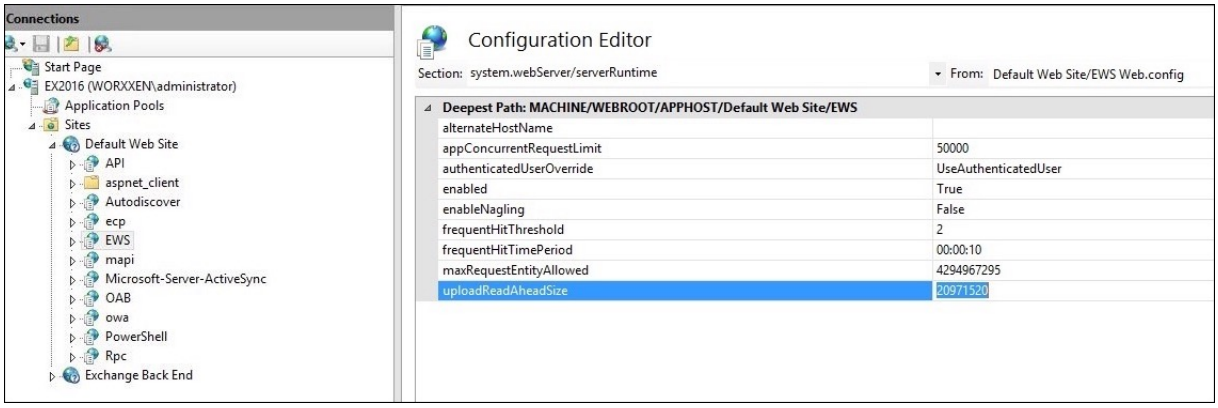
8. 構成エディターをクリックします。[**Section**] ドロップダウンリストの次のセクションに移動します:

   - **system.webServer/serverRuntime**

9. [**uploadReadAheadSize**] の値を **10485760**（10 MB）または **20971520**（20 MB）に設定するか、組織で必要な値に設定します。

   > 重要:
   >
   > この値が正しく設定されないと、EWS プッシュ通知のサブスクライブ時に証明書ベースの認証が失敗し、エラーコード 413 が発生する可能性があります。
   >
   > この値を「**0**」に設定しないでください。

詳しくは、Microsoft 社の記事「Microsoft IIS server runtime」を参照してください。



iOS のプッシュ通知に関連した Citrix Secure Mail の問題のトラブルシューティングについては、Citrix Support Knowledge Center の記事 を参照してください。

関連情報

Citrix Secure Mail for iOS のプッシュ通知

オンプレミスのデバイス正常性構成証明（**DHA**）サーバーの構成

March 15, 2024

オンプレミスの Windows サーバーから、Windows 10 および Windows 11 モバイルデバイスのデバイス正常性構成証明（DHA）を有効化できます。オンプレミスで DHA を有効にするには、まず DHA サーバーを構成します。

DHA サーバーを構成したら、Citrix Endpoint Management ポリシーを作成してオンプレミスの DHA サービスを有効にします。詳細については、「デバイス正常性構成証明デバイスポリシー」を参照してください。

DHA サーバーの前提条件

- Windows Server の Technical Preview 5 以降が［デスクトップエクスペリエンス］のインストールオプションを使用してインストールされ、実行されているサーバー。
- 1 台以上の Windows 10 および Windows 11 クライアントデバイス。これらのデバイスには、最新バージョンの Windows を実行する TPM 1.2 または 2.0 が搭載されている必要があります。
- 以下の証明書:
  - **DHA SSL** 証明書: エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 SSL 証明書です。この証明書は、次のような DHA データ通信を保護します:
    - サーバー間（DHA サービスおよび MDM サーバー）通信

    - サーバーからクライアント（DHA サービスおよび Windows 10 および Windows 11 デバイス）への通信
  - **DHA** 署名証明書：エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 証明書です。DHA サービスでは、この証明書を使用してデジタル署名を行います。
  - **DHA** 暗号化証明書：エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 SSL 証明書です。DHA サービスでは、この証明書を暗号化にも使用します。

- 次のいずれかの証明書検証モードを選択します。
  - **EKCert**： EKCert 検証モードは、インターネットに接続されていない組織のデバイス向けに最適化されています。EKCert 検証モードで実行されている DHA サービスに接続する場合、デバイスはインターネットに直接アクセスすることはありません。
  - **AIKCert**： AIKCert 検証モードは、インターネットにアクセス可能な運用環境向けに最適化されています。AIKCert 検証モードで実行されている DHA サービスに接続する場合、デバイスはインターネットに直接アクセスする必要があり、Microsoft から AIK 証明書を取得できます。

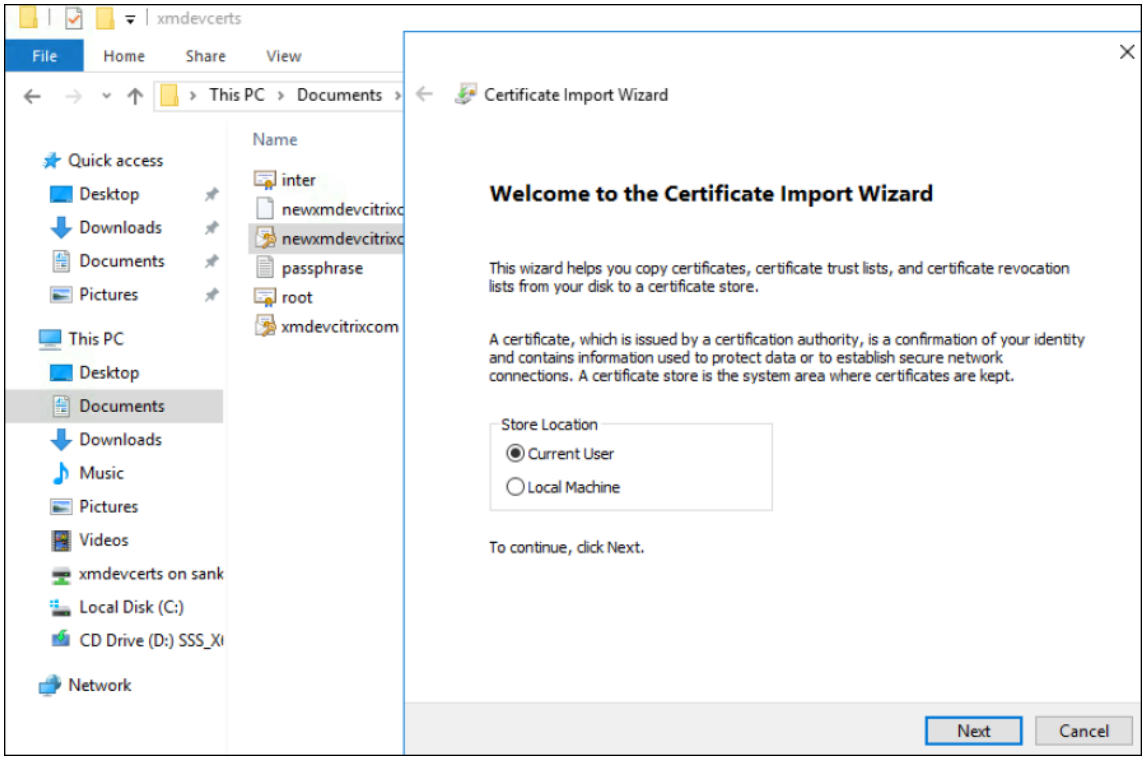
Windows サーバーに **DHA** サーバーの役割を追加する

1. Windows サーバーで、サーバーマネージャーがまだ開かれていない場合は、[スタート]、[サーバーマネージャー] の順にクリックします。
2. [役割と機能の追加] をクリックします。
3. [始める前に] ページで [次へ] をクリックします。
4. [インストールの種類の選択] ページで、[役割ベースまたは機能ベースのインストール] をクリックして、[次へ] をクリックします。
5. [対象サーバーの選択] ページで、[サーバープールからサーバーを選択] をクリックして、[次へ] をクリックします。
6. [サーバーの役割の選択] ページで、[デバイス正常性構成証明] チェックボックスをオンにします。
7. オプション：[機能の追加] をクリックして、その他の必要な役割サービスと機能をインストールします。
8. [次へ] をクリックします。
9. [機能の選択] ページで、[次へ] をクリックします。
10. [**Web** サーバーの役割（**IIS**）] ページで、[次へ] をクリックします。
11. [役割サービスの選択] ページで、[次へ] をクリックします。
12. [デバイス正常性構成証明サービス] ページで、[次へ] をクリックします。
13. [インストールオプションの確認] ページで、[インストール] をクリックします。
14. インストールが完了したら、[閉じる] をクリックします。

サーバーの証明書ストアに **SSL** 証明書を追加する

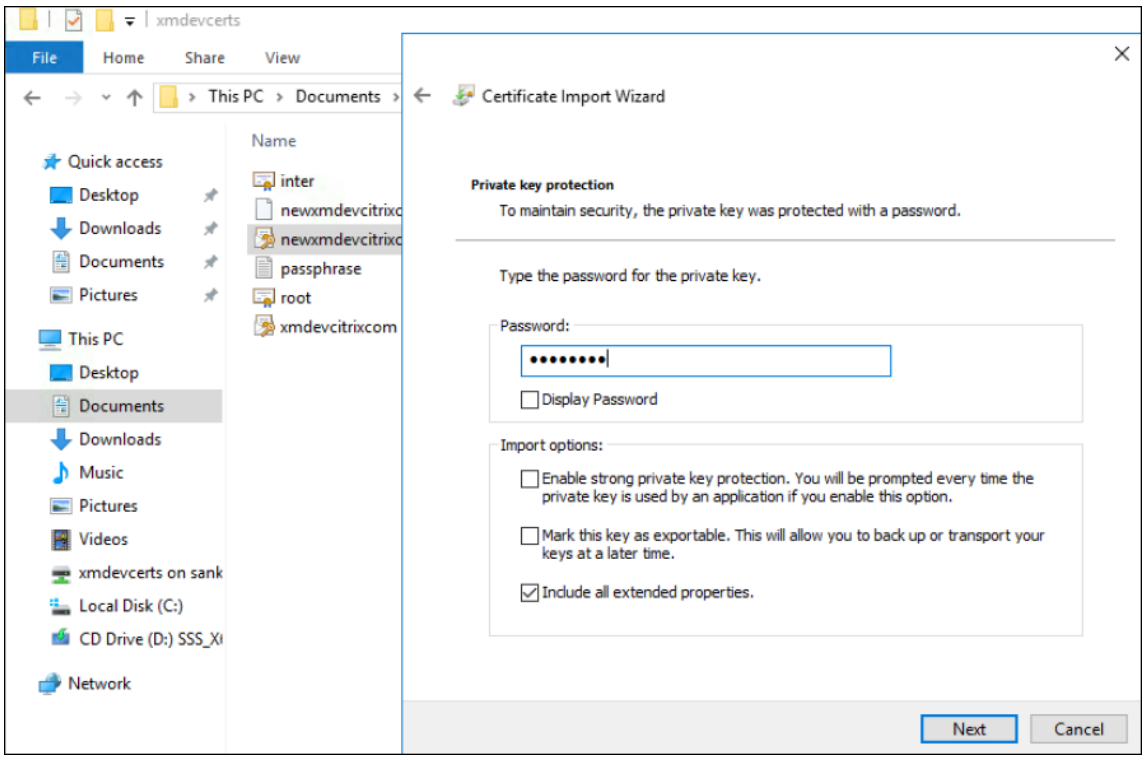
1. SSL 証明書ファイルの場所に移動して選択します。

2. 保存場所として ［現在のユーザー］を選択し、［次へ］をクリックします。

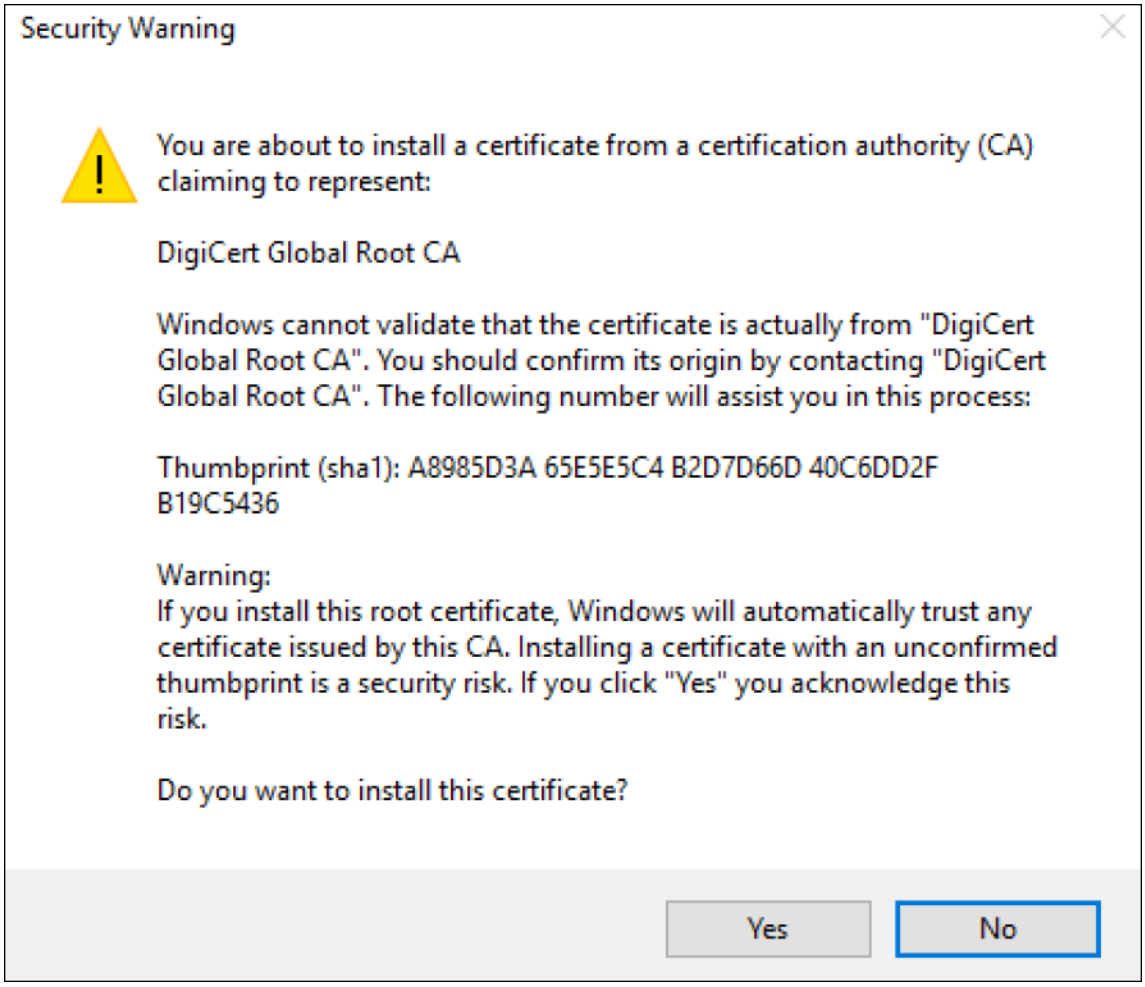


3. 秘密キーのパスワードを入力します。

4. ［すべての拡張プロパティを含める］インポートオプションが選択されていることを確認します。［次へ］をクリックします。



5. 以下のウィンドウが表示されたら、［はい］をクリックします。



6. 証明書がインストールされたことを確認します。

   a) ［コマンド プロンプト］ウィンドウを開きます。

   b) 「mmc」と入力して **Enter** キーを押します。ローカルマシンのストア内の証明書を表示するには、管理者の役割に属している必要があります。

   c) ［ファイル］メニューで、［スナップインの追加と削除］をクリックします。

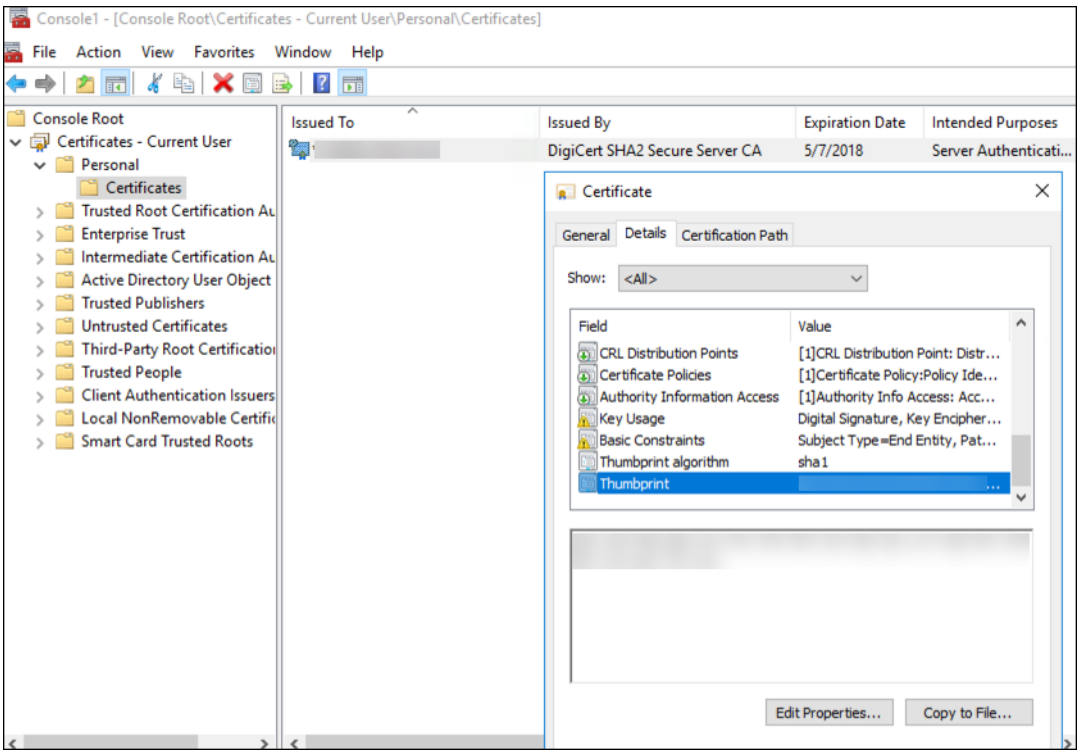
   d) ［追加］をクリックします。

   e) ［スタンドアロンスナップインの追加］ダイアログボックスで、［証明書］を選択します。

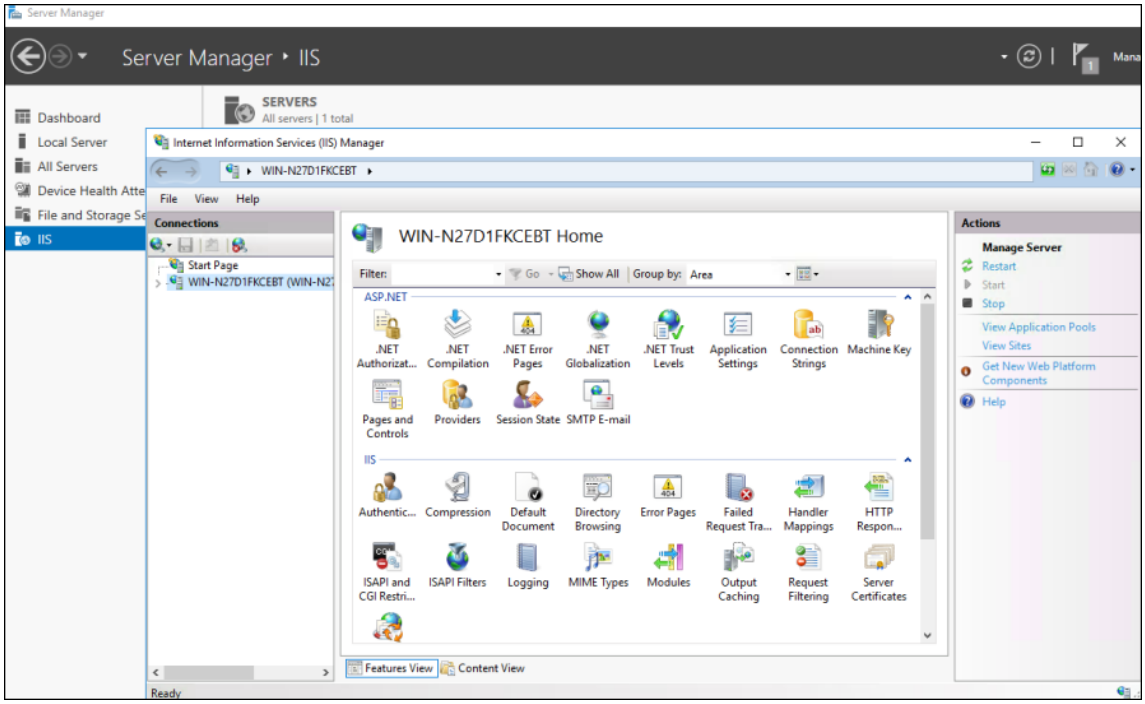
   f) ［追加］をクリックします。

   g) ［証明書スナップイン］ダイアログボックスで、［ユーザーアカウント］を選択します。（サービスアカウント所有者としてログインしている場合は、［サービスアカウント］を選択します。）

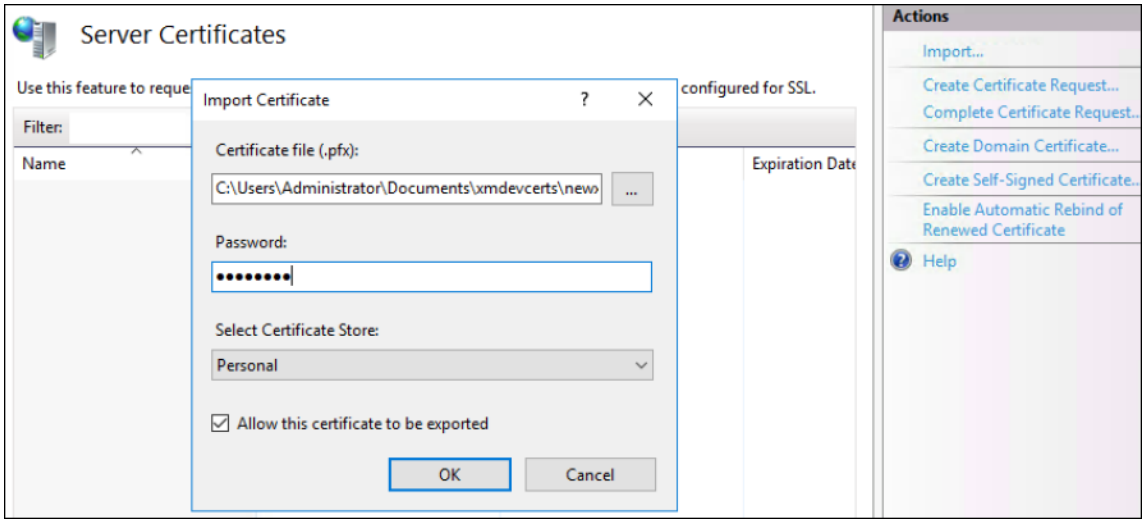
   h) ［コンピュータの選択］ダイアログボックスで、［完了］をクリックします。



7. [サーバーマネージャ] > [**IIS**] の順に選択し、アイコンの一覧で [サーバー証明書] を選択します。

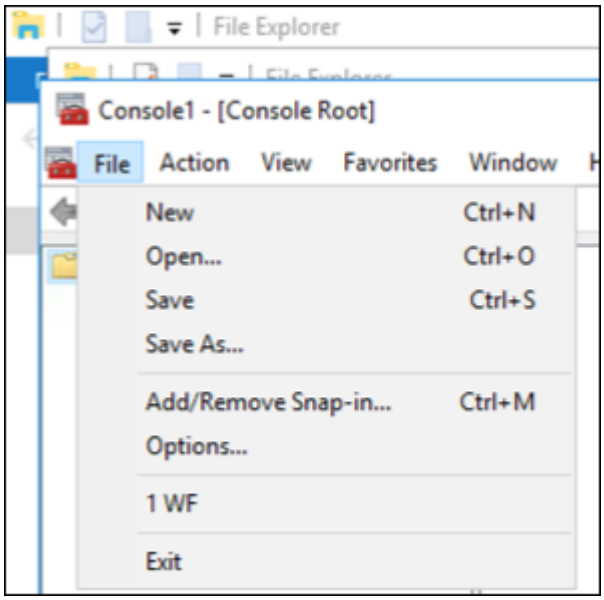


8. [アクション] メニューで [インポート…] を選択して、SSL 証明書をインポートします。

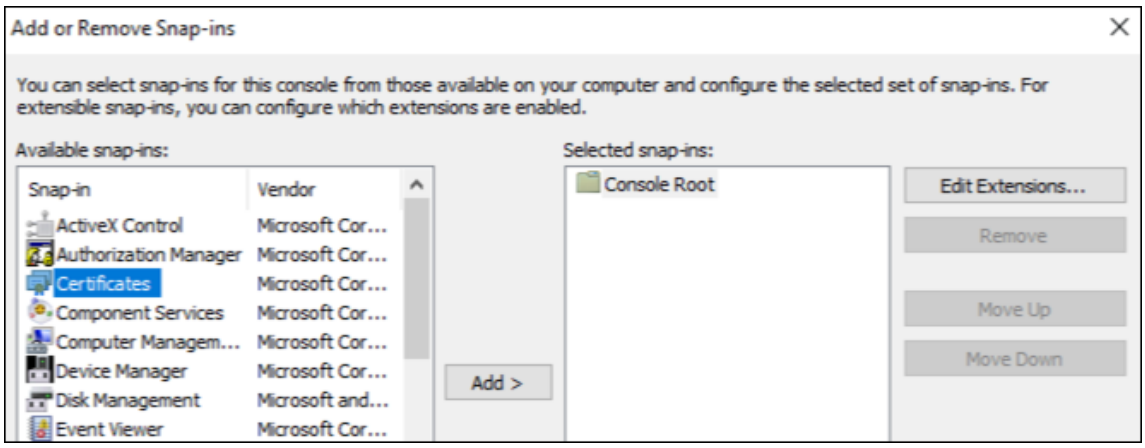


証明書の拇印を取得して保存する

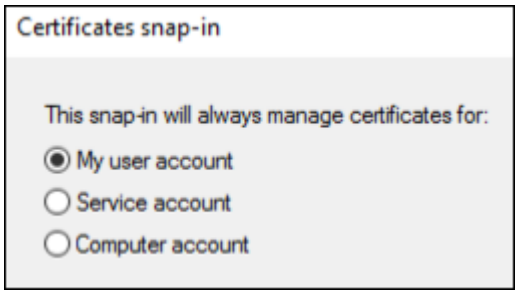
1. ファイルエクスプローラーの検索バーに「mmc」と入力します。
2. ［コンソールルート］ウィンドウで、［ファイル］**>**［スナップインの追加と削除］の順にクリックします。



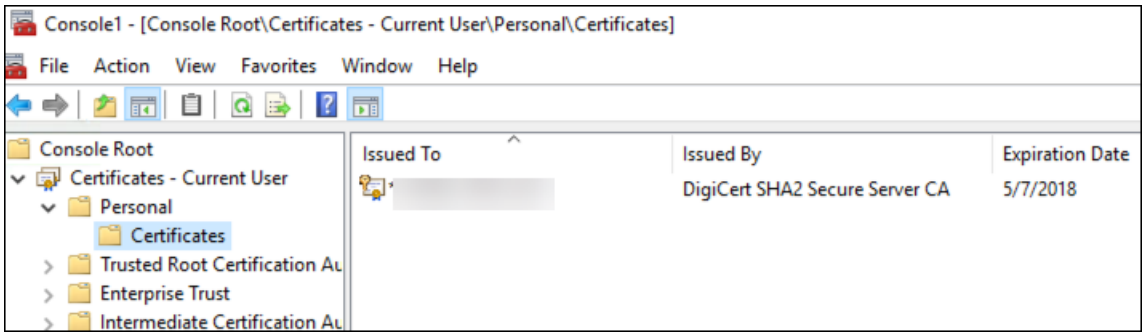
3. ［利用できるスナップイン］で［証明書］を選択し、［選択されたスナップイン］に追加します。



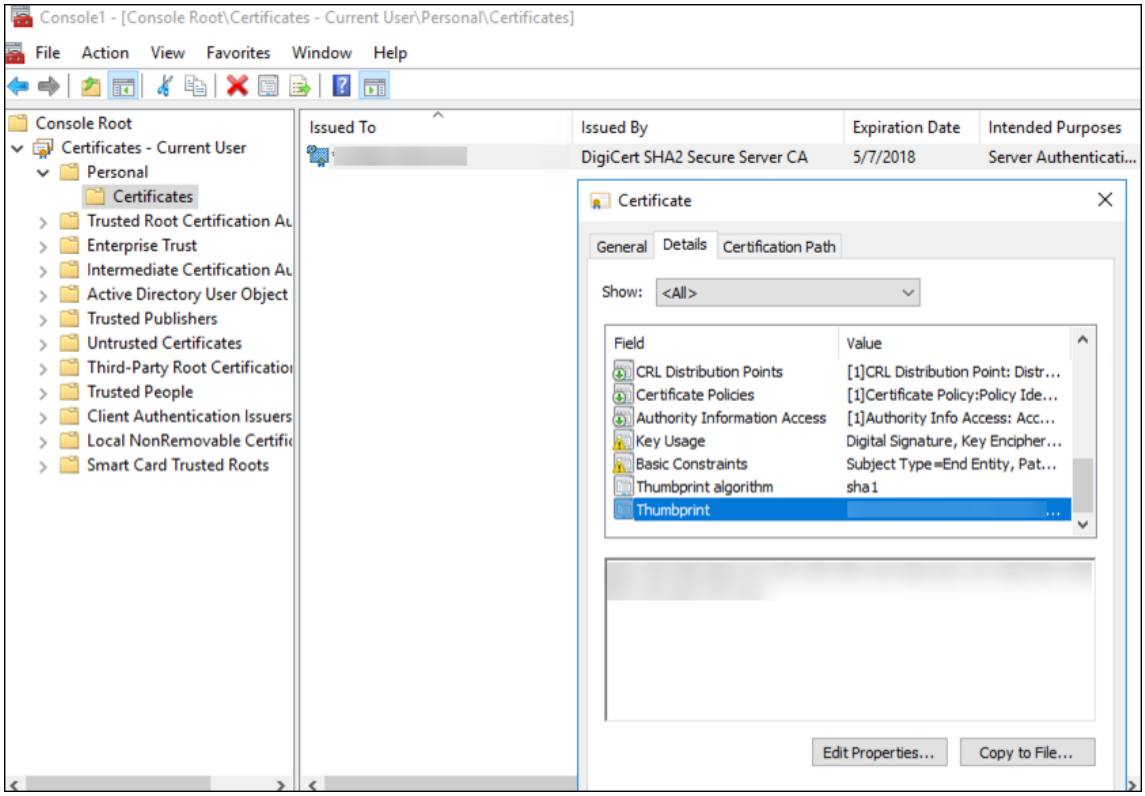
4. [ユーザーアカウント] を選択します。



5. 証明書を選択し、[**OK**] をクリックします。



6. 証明書をダブルクリックして、[詳細] タブをクリックします。下方向にスクロールして、証明書の拇印を表示します。



7. 拇印をファイルにコピーします。PowerShell コマンドで拇印を使用する場合は、スペースを削除します。

署名証明書と暗号化証明書をインストールする

以下の PowerShell コマンドを Windows サーバーで実行して、署名証明書と暗号化証明書をインストールします。

プレースホルダー ReplaceWithThumbprint を置き換えて、下に示すように二重引用符で囲みます。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
    $keyname icacls $keypath /grant IIS_IUSRS`:R

<!--NeedCopy-->
```

TPM ルート証明書を抽出し、信頼できる証明書パッケージをインストールする

以下のコマンドを Windows サーバーで実行します。


```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

DHA サービスを構成する

Windows サーバー上で次のコマンドを実行して、DHA サービスを構成します。

プレースホルダー ReplaceWithThumbprint を置き換えます。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

以下のコマンドを Windows サーバーで実行して、DHA サービスの証明書チェーンポリシーを設定します。

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

以下のようにプロンプトに回答します:

```
  Confirm

    Are you sure you want to perform this action?

    Performing the operation "Install-DeviceHealthAttestation" on
       target "[Machine Name]".

    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
       Help (default is "Y"): A

    Adding SSL binding to website 'Default Web Site'.

    Add SSL binding?

```



```
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
           Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
           inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
           .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
44  <!--NeedCopy-->
```

構成を確認する

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーで次のコマンドを実行します。

```
Get-DHASActiveSigningCertificate
```

証明書がアクティブな場合、証明書の種類（署名）と拇印が表示されます。

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーで次のコマンドを実行します。

プレースホルダー ReplaceWithThumbprint を置き換えて、下に示すように二重引用符で囲みます。

```
1  Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
       -Force
```



```
2
3 Get-DHASActiveEncryptionCertificate
4 <!--NeedCopy-->
```

証明書がアクティブな場合、拇印が表示されます。

最終チェックを行うには、次の URL にアクセスします:

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1
```

DHA サービスが実行されている場合は、「メソッドは許可されていません」と表示されます。