VMware Identity Manager による VMware Workspace ONE の展開ガイド

2018 年 9 月

VMware Workspace ONE

vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。
https://docs.vmware.com/jp/
VMware の Web サイトでは、最新の製品アップデートを提供しています。
本書に関するご意見、ご要望をお寄せください。フィードバック送信先：
docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

内容

VMware Workspace ONE の展開について

VMware Identity Manager による『VMware Workspace™ ONE™ の展開ガイド』には、AirWatch で VMware Identity Manager™ と VMware Workspace ONE UEM™ を統合し、Workspace ONE、Workspace ONE UEM におけるデバイス管理、そして VMware Workspace ONE に、アプリケーションのカタログとしてシングル サインオン機能を導入するための情報が記載されています。

Workspace ONE UEM と VMware Identity Manager を統合すると、Workspace ONE UEM に登録されたデバイスを持つユーザーは、複数のパスワードを入力することなく、自分の有効になっているアプリケーションに安全にログインできます。

対象者

この情報は、Workspace ONE UEM サービスと VMware Identity Manager サービスの両方に精通する管理者を対象としています。

2018 年 9 月のリリースは、VMware Identity Manager Cloud 2018 年 9 月、VMware Identity Manager 3.3、Workspace ONE UEM 9.7 に適用されます。

Workspace ONE の概要

1

VMware Workspace® ONE® は、iOS、Android、および Windows 10 の各デバイス上でアプリケーションを提供および管理する、セキュリティで保護されたプラットフォームです。ID、アプリケーション、およびエンタープライズ モビリティ管理は、Workspace ONE プラットフォームに統合されます。

VMware Workspace ONE UEM® および VMware Identity Manager™ は、アプリケーションおよびモバイル アクセス管理サービスの Workspace ONE カタログを提供するために統合されます。

VMware Identity Manager サービスは、自分のリソースにシングル サインオンするユーザーの認証を含む ID 関連コンポーネントを提供します。ネットワークとこれらのリソースへのアクセスを制御するための認証に関連する一連のポリシーを作成します。

Workspace ONE UEM サービスは、デバイスの登録、アプリケーションの配布、およびコンプライアンス チェック ツールを提供し、リモート アクセス デバイスが企業のセキュリティ基準を満たしていることを確認します。Workspace ONE UEM に登録されたデバイスのユーザーは、複数のパスワードを入力することなく、有効なアプリケーションに安全にログインできます。

この章には、次のトピックが含まれています。

Workspace ONE アーキテクチャの概要

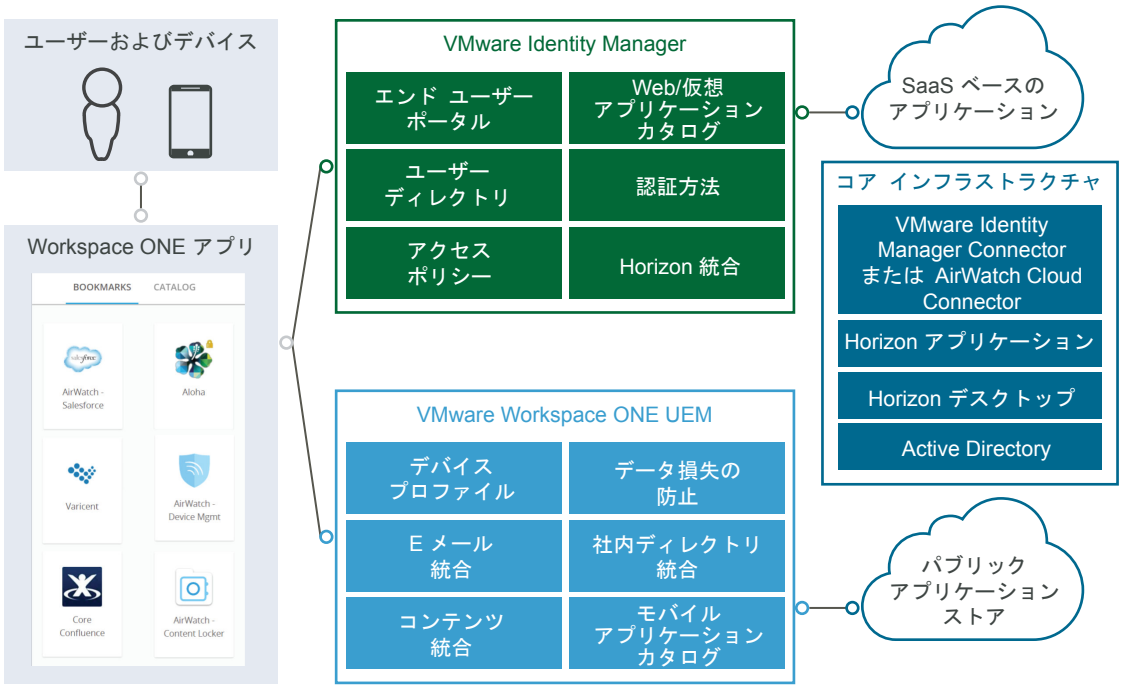
Workspace ONE は、統合カタログから管理されるクラウド、モバイル、Windows アプリケーションへの安全なアクセスをユーザーに提供します。デバイス アクセスの場合、Workspace ONE ネイティブ アプリケーションは iOS、Android、および Windows 10 デバイスから使用できます。

Workspace ONE が展開された場合、次の VMware Identity Manager サービスと Workspace ONE UEM サービスを実装する必要があります。

- VMware Identity Manager Connector コンポーネントまたは AirWatch Cloud Connector (ACC) コンポーネントを構成できます。
- 会社のユーザーとグループを Active Directory から Workspace ONE サービスに同期するための、Active Directory の VMware Identity Manager との統合、または Workspace ONE UEM Cloud Connector との統合。

- VMware Identity Manager を Workspace ONE UEM API キーおよび管理者ルート証明書と一緒に構成し、Workspace ONE UEM を介して Workspace ONE カタログ、コンプライアンス チェック、ユーザー パスワード認証を有効にします。

図 1-1. Workspace ONE のアーキテクチャ概要



要件

Workspace ONE のシステム要件は次のとおりです。

表 1-1. Workspace ONE のシステム要件

Workspace ONE の要件	詳細
Active Directory	Windows 2008 および 2008 Server R2 Windows 2012 および 2012 Server R2
VMware Identity Manager および Workspace ONE コンソールにアクセスするための Web ブラウザ	Windows 用 Internet Explorer 11 Google Chrome 4.0 以降 Mozilla Firefox 40 以降 Safari 6.2.8 以降
VMware Identity Manager Connector または AirWatch Cloud Connector がインストールされていること。	Windows Server 2008 R2 Windows Server 2012 または 2012 R2 .NET Framework 4.6.2 VMware Identity Manager Connector のインストールについての詳細情報は、VMware Identity Manager ドキュメント センター を参照してください。AirWatch Cloud Connector のインストールについての詳細情報は、Workspace ONE UEM ドキュメント センター を参照してください。

Workspace ONE の機能の詳細

Workspace ONE の主要な特徴を以下に示します。

ネイティブ モバイル Workspace ONE アプリケーション

ユーザーは、モバイル デバイスで Workspace ONE アプリケーションをインストールし、社内アプリケーション、クラウド アプリケーション、およびモバイル アプリケーションへのシングル サインオン (SSO) アクセス用の会社の認証情報を使用できます。

Web、Horizon、および Citrix リソース用のセルフ サービス アプリケーション カタログ

Workspace ONE は、統合カタログを使用したクラウド、モバイル、Windows アプリケーションへのアクセスをユーザーに提供します。カタログには、VMware Identity Manager および VMware Workspace ONE UEM に公開されるアプリケーションが含まれます。サポートされているアプリケーションのタイプには、社内 Web、SaaS、ネイティブ モバイル、社内開発モバイル、レガシーおよび最新の Windows、Horizon 7、VMware Horizon Cloud Service™、Citrix が公開したもの、および ThinApp パッケージが含まれます。アプリケーション ストアには、仮想化されたデスクトップも含まれます。

シングル サインオンでの Web および仮想アプリケーションの起動

Workspace ONE はモバイル アプリケーションへのモバイル シングル サインオン (SSO)、ワンタッチ ログインの実装を提供します。モバイル SSO は、Android、iOS、および Windows 10 デバイスで利用可能です。

デバイス コンプライアンスでの条件付きアクセス

Workspace ONE を使用すると、ネットワーク範囲、プラットフォーム、および認証のためのアプリケーション固有の基準に基づいて、条件付きアクセスを強制的に適用できます。デバイスは、アプリケーションへのアクセスを許可する前に、セキュリティ ルールへの遵守を証明する必要があります。VMware Identity Manager には、ユーザーがデバイスからログインする際に、Workspace ONE UEM サーバを確認してデバイスのコンプライアンスの状態を確認するよう構成できるアクセス ポリシー オプションが組み込まれています。

多要素認証

Workspace ONE は、VMware Verify アプリケーションを介して多要素認証を提供します。ユーザーが Workspace ONE カタログまたは強力な認証を必要とする任意のアプリケーションにアクセスしようとすると、VMware Verify はユーザーの電話に通知を送信します。Workspace ONE へのアクセスの試行を確認するには、ユーザーは同意をスワイプしてアプリケーションにアクセスする必要があります。

アダプティブ管理

基本的なレベルのセキュリティを必要とするアプリケーションの場合、ユーザーは Workspace ONE UEM Mobile Device Management™ に自分のデバイスを登録する必要はありません。ユーザーは、Workspace ONE モバイル アプリケーションをダウンロードし、目的のアプリケーションをインストールすることを選択できます。高レベルのセキュリティを必要とするアプリケーションの場合、ユーザーは Workspace ONE UEM に Workspace ONE モバイル アプリケーションから直接自分のデバイスを登録できます。

Workspace ONE「はじめに」ウィザード

Workspace ONE「はじめに」ウィザードを使用すると、Workspace ONE UEM サービスおよび VMware Identity Manager サービスを統合し、Workspace ONE 環境を作成するための多数の構成手順を実行できます。

「はじめに」ウィザードは、個々の設定を構成または編集する機能に置き換わるものではありませんが、ほとんどのユーザーの初期セットアップを大幅に自動化します。

Workspace ONE「はじめに」ウィザードは、次の設定のために使用できます。

- Enterprise Connector とディレクトリ。このウィザードでは、VMware Enterprise System Connector を設定し、Workspace ONE UEM Cloud Connector からの Active Directory 接続を構成し、ユーザーとグループを会社のディレクトリからインポートするための手順を実行します。Enterprise Connector の設定方法については、『VMware Workspace ONE Quick Configuration Guide』を参照してください。
- 自動検出。ウィザードを実行し、エンド ユーザーが Workspace ONE アプリケーションを介してアプリケーション ポータルに簡単にアクセスできるように、自動検出サービスにメール ドメインを登録します。その後、エンド ユーザーは、組織の URL の代わりにメール アドレスを入力できます。
- Workspace ONE カタログ。Workspace ONE カタログ ウィザードでは、Workspace ONE カタログを設定する手順を実行します。Workspace ONE のカスタム ブランディング手順は、会社のブランドの情報を Workspace ONE カタログおよびアプリケーションに追加するためにも使用できます。Workspace ONE カタログの設定方法については、『VMware Workspace ONE Quick Configuration Guide』を参照してください。
- アダプティブ管理。アダプティブ管理を設定し、ユーザーのデバイスへのプロファイルのインストールを要求することによって、特定のアプリケーションを制限します。プロファイルによって、会社のアプリケーションやデータを必要に応じて削除できます。アプリ ストアからアプリケーションを手動でダウンロードすることで、パブリック アプリケーションが管理対象になる、または独立して使用されることを要求することもできます。

「はじめに」ウィザードは、競合する可能性のある既存の構成がすでに Workspace ONE UEM サービスまたは VMware Identity Manager サービスで有効な場合、警告できます。これが発生した場合、または「はじめに」ウィザードの手順が一部のみ完了した場合、機能を手動で構成できます。このガイドを使用し、Workspace ONE UEM サービスおよび VMware Identity Manager サービスを Workspace ONE 用に手動で構成します。

Workspace ONE UEM の VMware Identity Manager との統合

2

ユーザーのシングル サインオンと ID 管理のために VMware Identity Manager サービスを使用するデバイスで Workspace ONE UEM モバイル管理サービスを設定するには、サービスを統合する必要があります。

Workspace ONE UEM と VMware Identity Manager を統合すると、Workspace ONE UEM に登録されたデバイスのユーザーは、複数のパスワードを入力することなく、Workspace ONE にログインして自分の有効になっているアプリケーションに安全にアクセスできます。

Workspace ONE「はじめに」ウィザードを使用すると、Workspace ONE UEM および VMware Identity Manager を統合するための多数の構成手順を実行できます。Workspace ONE ウィザードの実行については、『VMware Workspace ONE Quick Configuration Guide』を参照してください。

この章には、次のトピックが含まれています。

Workspace ONE UEM コンソールからの統合の設定

VMware Identity Manager サービスと統合するには、Workspace ONE UEM コンソールで以下の内容を設定します。

- VMware Identity Manager サービスとの通信用の Rest API 管理キー
- VMware Identity Manager が構成されているのと同じ組織グループに作成された AirWatch Cloud Connector パスワード認証に対する REST 登録ユーザー API キー
- VMware Identity Manager の API 管理アカウント、および VMware Identity Manager コンソールで Workspace ONE UEM からエクスポートされ AirWatch 設定に追加された管理認証証明書

Workspace ONE UEM での REST API キーの作成

VMware Identity Manager を Workspace ONE UEM と統合するには、Workspace ONE UEM コンソールで REST 管理者 API アクセスと登録ユーザー アクセスを有効にする必要があります。API アクセスを有効にすると、API キーが生成されます。

手順

1 Workspace ONE UEM コンソールで、[グローバル] > [カスタマレベルの組織グループ] を選択して、[グループと設定] > [すべての設定] > [システム] > [詳細] > [API] > [REST API] の順に移動します。

2 [全般] タブで、[追加] をクリックし、VMware Identity Manager サービスで使用する API キーを生成します。アカウントのタイプは [管理者] になります。

一意のサービス名を入力します。「**AirWatchAPI for IDM**」などの説明を追加します。

3 登録ユーザー API キーを生成するには、再度 [追加] をクリックします。

4 [アカウント タイプ] ドロップダウン メニューで、[加入ユーザー] を選択します。

一意のサービス名を入力します。「**UserAPI for IDM**」などの説明を追加します。

5 2 つの API キーをコピーしてファイルに保存します。

これらのキーは、VMware Identity Manager コンソールで Workspace ONE UEM (AirWatch) を設定するときに追加します。

6 [保存] をクリックします。

VMware Workspace ONE UEM 管理者ルート証明書のエクスポート

管理者用の API キーを作成したら、Workspace ONE UEM コンソールで、管理者アカウントを追加して証明書認証をセットアップします。

REST API 証明書ベースの認証では、Workspace ONE UEM コンソールでユーザー レベルの証明書が生成されます。使用する証明書は、Workspace ONE UEM 管理者ルート証明書から生成された自己署名 Workspace ONE UEM 証明書です。

前提条件

Workspace ONE UEM REST 管理者用 API キーを作成します。

手順

1 Workspace ONE UEM コンソールで、[グローバル] > [カスタマレベルの組織グループ] の順に選択し、[アカウント] > [管理者] > [リスト表示] の順に移動します。

2 [追加] - [管理者を追加] をクリックします。

3 [ベーシック] タブで、証明書の管理者のユーザー名とパスワードを必要なテキスト ボックスに入力します。

4 [ロール] タブを選択し、現在の組織グループを選択し、2 番目のテキスト ボックスをクリックして、[AirWatch 管理者] を選択します。

5 [API] タブを選択し、[認証] テキスト ボックスで [証明書] を選択します。

6 証明書のパスワードを入力します。このパスワードは、[ベーシック] タブで管理者用に入力したものと同じパスワードです。

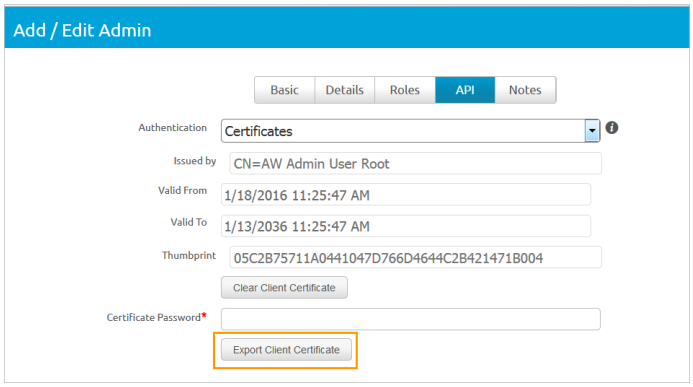
7 [保存] をクリックします。

新しい管理者アカウントとクライアント証明書が作成されます。

8 [リスト表示] ページで、作成した管理者を選択し、[API] タブを再度開きます。

証明書のページには証明書に関する情報が表示されます。

9 設定したパスワードを [証明書パスワード] テキスト ボックスに入力し、[クライアント証明書をエクスポート] をクリックしてファイルを保存します。



クライアント証明書が .p12 ファイル形式として保存されます。

次のステップ

VMware Identity Manager コンソールで Workspace ONE UEM URL を設定します。

VMware Identity Manager での Workspace ONE UEM インスタンスの設定

Workspace ONE UEM コンソールで設定した後、VMware Identity Manager コンソールの [ID とアクセス管理] ページで、Workspace ONE UEM URL、API キー値、および証明書を入力します。Workspace ONE UEM を設定後、Workspace ONE で使用できる機能オプションを有効にすることができます。

VMware Identity Manager への Workspace ONE UEM 設定の追加

VMware Identity Manager で Workspace ONE UEM 設定を構成し、VMware Identity Manager に Workspace ONE UEM を統合して、Workspace ONE UEM 機能の統合オプションを有効にします。Workspace ONE UEM API キーおよび証明書は、Workspace ONE UEM を使用した VMware Identity Manager 認証用に追加されます。

[]

前提条件

- 管理者が Workspace ONE UEM コンソールにログインするための Workspace ONE UEM サーバの URL。
- 統合のセットアップを目的として、VMware Identity Manager から Workspace ONE UEM サーバへの API 要求に使用する、Workspace ONE UEM 管理者用の API キー。
- API コールに使用する Workspace ONE UEM 証明書ファイルと証明書のパスワード。証明書ファイルは .p12 のファイル形式でなければなりません。

- Workspace ONE UEM 登録ユーザー API キー。
- テナントの Workspace ONE UEM グループ ID（Workspace ONE UEM のテナント ID）。

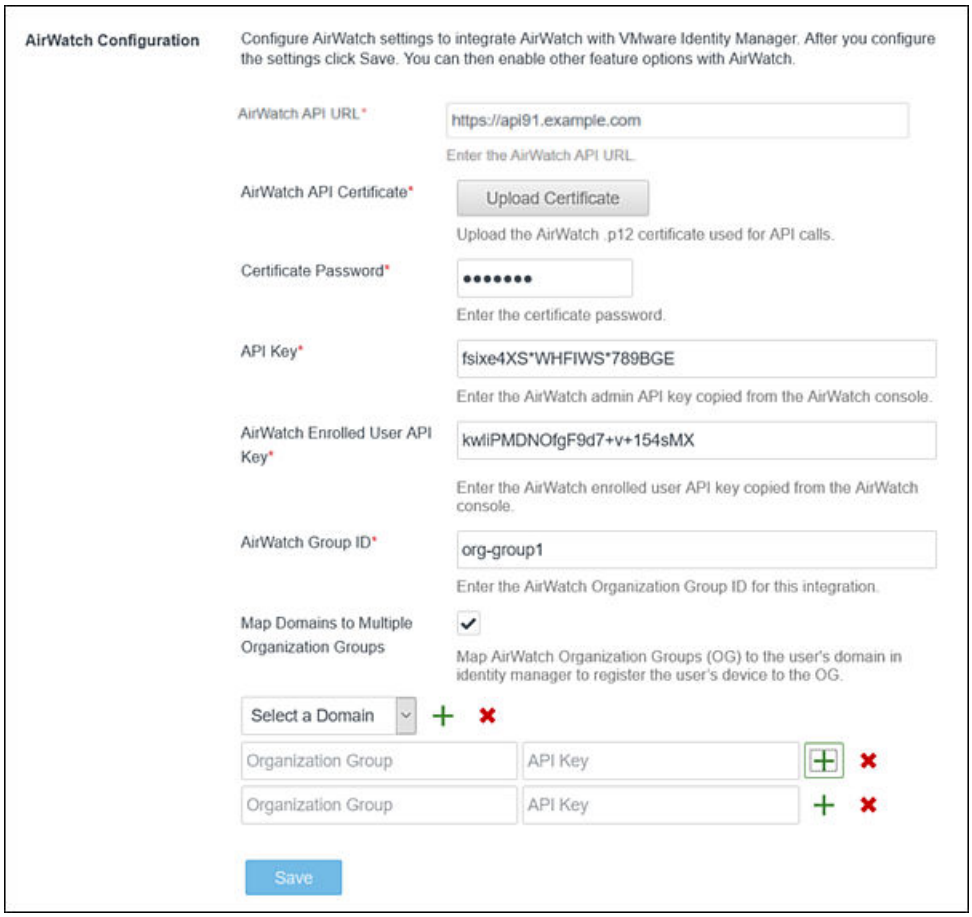
手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [AirWatch] の順にクリックします。

2 次のフィールドに Workspace ONE UEM 統合設定を入力します。

フィールド	説明
AirWatch API の URL	Workspace ONE UEM の URL を入力します。たとえば、`https://myco.ws1uem.com` のように入力します。
AirWatch API の証明書	API コールに使用する証明書ファイルをアップロードします。
証明書のパスワード	証明書のパスワードを入力します。
AirWatch 管理者用の API キー	管理者用の API キー値を入力します。API キー値の例：`FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
AirWatch 登録ユーザー用の API キー	登録ユーザー API キー値を入力します。
AirWatch グループ ID	API キーと管理者アカウントが作成された組織グループの Workspace ONE UEM グループ ID を入力します。

3 [保存] をクリックします。



次のステップ

[Workspace ONE カタログ] 機能オプションを有効にして、Workspace ONE UEM カタログでセットアップされたアプリケーションを Workspace ONE カタログにマージします。

- [コンプライアンス チェック] を有効にして、Workspace ONE UEM のコンプライアンス ポリシーを Workspace ONE UEM で管理されているデバイスが遵守しているか確認します。

「Workspace ONE UEM で管理されているデバイスのコンプライアンス チェックの有効化」を参照してください。

Workspace ONE UEM での複数の組織グループへの VMware Identity Manager ドメインのマッピング

Workspace ONE UEM でユーザーおよびデバイスを設定するときに、Workspace ONE UEM は組織グループ (OG) を使用し、ユーザーを編成してグループ化し、権限を確立します。Workspace ONE UEM が VMware Identity Manager と連携すると、管理および登録ユーザーの REST API キーは、[カスタマ] タイプの Workspace ONE UEM 組織グループでのみ構成できます。

マルチテナント用に構成された Workspace ONE UEM の環境では、ユーザーおよびデバイス用に多くの組織グループが作成されます。デバイスが組織グループに登録できるようになります。組織グループは、マルチテナント環境の固有の構成で設定できます。たとえば地域別、部門別、使用事例別の組織グループです。

VMware Identity Manager で設定したドメインを Workspace ONE UEM の特定の組織グループにリンクすると、Workspace ONE を介してデバイス登録を管理できます。ユーザーが Workspace ONE にログインすると、VMware Identity Manager 内でデバイスの登録のイベントがトリガされます。デバイスの登録中、ユーザーおよびデバイスの組み合わせに資格が付与された任意のアプリケーションを取得するための要求が Workspace ONE UEM に送信されます。

デバイス組織グループは、Workspace ONE UEM が VMware Identity Manager と統合されるときに特定される必要があります。そうすることで、Identity Manager がユーザーを見つけ、適切な組織グループにデバイスを正常に登録できるようになります。

VMware Identity Manager サービスで Workspace ONE UEM を設定するときは、ドメインに複数の OG をマッピングするために、デバイスの組織グループ ID および API キーを入力できます。ユーザーが自分のデバイスから Workspace ONE にログインすると、ユーザーのレコードが検証され、そのデバイスが Workspace ONE UEM の適切な組織グループに登録されます。

複数の組織グループを構成する方法の詳細については、「複数の Workspace ONE UEM 組織グループを設定するための展開戦略」を参照してください。

注: Workspace ONE UEM が VMware Identity Manager に統合され、複数の Workspace ONE UEM 組織グループが構成されている場合、[Active Directory グローバル カタログ] オプションを VMware Identity Manager サービスで使用するように構成することはできません。

Workspace ONE UEM 用の Workspace ONE カタログの有効化

Workspace ONE UEM インスタンスを使用して VMware Identity Manager を構成するときに、Workspace ONE カタログを有効にして Workspace ONE UEM カタログからのアプリケーションを含めることができます。エンドユーザーは、使用資格が付与されたすべてのアプリケーションを Workspace ONE ポータルで確認できます。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [AirWatch] の順にクリックし、[Workspace ONE カタログ] セクションに移動します。

2 AirWatch カタログのアプリケーションを Identity Manager カタログのアプリケーションに含めるには、[IDM から取得] と [AirWatch から取得] の両方を有効にします。

VMware Identity Manager サービスが構成されていないモバイル デバイスで Workspace ONE カタログを使用する場合は、[AirWatch から取得] のみを選択してください。

デフォルトでは、[IDM から取得] が有効になっています。

3 [保存] をクリックします。

次のステップ

Workspace ONE UEM エンド ユーザーに、カタログへアクセスする方法や、Workspace ONE ポータルの表示方法について通知します。

Workspace ONE UEM で管理されているデバイスのコンプライアンス チェックの有効化

ユーザーがデバイスを登録する場合、コンプライアンスを評価するために使用されるデータを含むサンプルがスケジュールに従って送信されます。このサンプル データの評価により、デバイスが Workspace ONE UEM (UEM) コンソールの管理者によって設定されたコンプライアンス ルールを遵守していることを確認できます。デバイスがコンプライアンス ルールを遵守していない場合、UEM コンソールで構成されたアクションが実行されます。

VMware Identity Manager サービスには、ユーザーがデバイスからログインする際に、Workspace ONE UEM サーバを確認してデバイスのコンプライアンスの状態を確認するよう構成できるアクセス ポリシー オプションが組み込まれています。デバイスがコンプライアンス ルールに遵守されなくなった場合、コンプライアンス チェックにより、ユーザーがアプリケーションにログインしたり、Workspace ONE ポータルに対してシングル サインオンを使用したりすることを確実に防ぐことができます。デバイスで再度コンプライアンス ルールが遵守されるようになったら、再びログインできるようになります。

デバイスが危険にさらされている場合、Workspace ONE アプリケーションが自動的にログアウトし、アプリケーションへのアクセスをブロックします。デバイスがアダプティブ管理によって登録された場合、UEM コンソールを介して発行されたエンタープライズ WIPE コマンドにより、デバイスの登録が解除され、管理対象アプリケーションがデバイスから削除されます。管理対象外のアプリケーションは削除されません。

Workspace ONE UEM コンプライアンス ポリシーの詳細については、「VMware Workspace ONE UEM ドキュメント」ページの『VMware Workspace ONE UEM Mobile Device Management Guide』を参照してください。

Workspace ONE UEM によるユーザーのパスワード認証の有効化

AirWatch Cloud Connector で認証を実装するには、Workspace ONE UEM によるパスワード認証機能を有効にする必要があります。

前提条件

- Workspace ONE UEM が VMware Identity Manager で構成されていること。

- AirWatch Cloud Connector がインストールされアクティブであること。
- Workspace ONE UEM ディレクトリ サービスが Active Directory と統合されていること。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [AirWatch] の順にクリックします。

2 [AirWatch によるユーザーのパスワード認証] セクションで、[有効] を選択します。

3 [保存] をクリックします。

次のステップ

AirWatch Cloud Connector 認証の使用方法については、「AirWatch Cloud Connector での認証の実装」を参照してください。

コンプライアンス チェック ルールの構成

コンプライアンス チェックを有効にしたら、Workspace ONE UEM で管理されているデバイスに対して認証とデバイス コンプライアンスの確認を求めるアクセス ポリシー ルールを作成します。

コンプライアンス チェック ポリシー ルールは、iOS 版モバイル SSO、Android 版モバイル SSO、および証明書のクラウド デプロイによる認証チェーンで動作します。ルールを構成するときは、使用する認証方法はデバイスのコンプライアンス方法の前に配置する必要があります。

前提条件

認証方法が設定され、組み込み ID プロバイダに関連付けられていること。

[VMware Identity Manager AirWatch] ページでコンプライアンス チェックが有効になっていること。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[管理] - [ポリシー] の順に選択します。

2 [デフォルト ポリシーの編集] をクリックします。

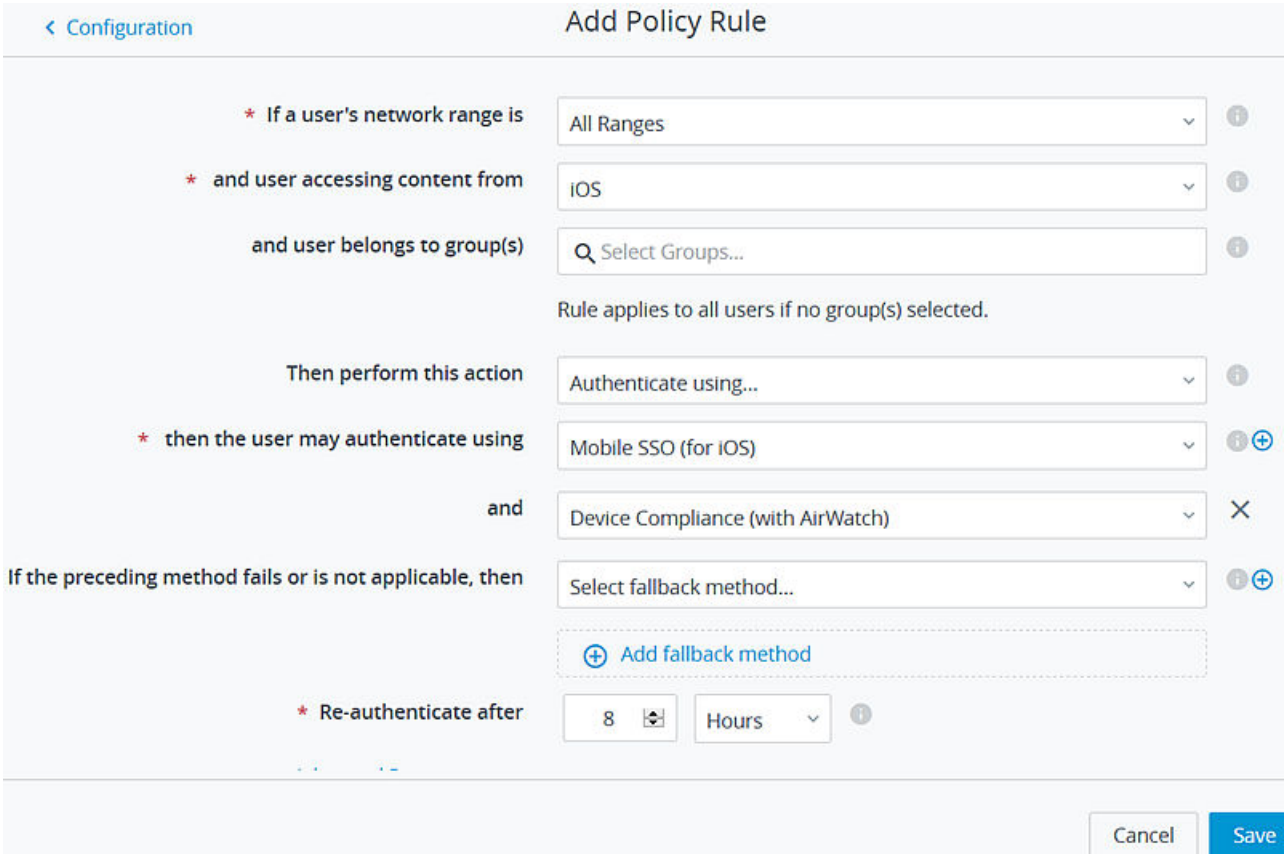
3 [次へ] をクリックします。

4 [ポリシー ルールの追加] をクリックしてルールを追加するか、編集するルールを選択します。

オプション	説明
ユーザーのネットワーク範囲が次の場合	ネットワーク範囲が正しいことを確認します。ルールを追加する場合は、ネットワーク範囲を選択します。
ユーザーが次からコンテンツにアクセスする場合	モバイル デバイスのタイプを選択します。
また、ユーザーが次のグループに属する場合	このアクセス ルールが特定のグループに適用される場合は、検索ボックスでグループを検索します。 グループが選択されていない場合、アクセス ポリシーはすべてのユーザーに適用されます。
このアクションを実行します	[以下を認証に使用...] を選択します。

オプション	説明
ユーザーは次を使用して認証することができます	適用するモバイル デバイスの認証方法を選択します。 [+] をクリックし、ドロップダウン メニューで [デバイス コンプライアンス (AirWatch)] を選択します。
先の方法が失敗するか適用できない場合、次を実行	必要に応じて、フォールバック認証方法を構成します。
再認証までの待機時間	ユーザーによる再認証が必要となるまでのセッション長さを選択します。

5 [保存] をクリックします。



Workspace ONE UEM のアップグレード後の VMware Identity Manager の更新

Workspace ONE UEM を新しいバージョンにアップグレードする場合は、VMware Identity Manager コンソールで AirWatch の構成ページの [Workspace ONE カタログ] と [ユーザー パスワード認証] オプションを更新する必要があります。

Workspace ONE UEM をアップグレードした後にこれらのオプションを保存すると、VMware Identity Manager サービスの AirWatch 設定が、新しいバージョンの Workspace ONE UEM によって更新されます。

手順

1 Workspace ONE UEM をアップグレードした後、VMware Identity Manager コンソールにログインします。

2 [ID とアクセス管理] タブで、[セットアップ] - [AirWatch] の順にクリックします。

3 [Workspace ONE カタログ] セクションが表示されるまでページを下方にスクロールして、[保存] をクリックします。

4 [AirWatch によるユーザーのパスワード認証] セクションが表示されるまで下方にスクロールして、[保存] をクリックします。

Workspace ONE UEM 構成は、VMware Identity Manager サービスの新しいバージョンで更新されます。

AirWatch Cloud Connector での認証の実装

VMware Enterprise Systems Connector の AirWatch Cloud Connector (ACC) コンポーネントは、Workspace ONE でユーザー パスワード認証のために VMware Identity Manager と統合されます。

注: ACC をインストールし、Workspace ONE UEM で ACC コンポーネントを構成します。AirWatch Cloud Connector のインストールと構成については、『VMware Enterprise Systems Connector のインストールと構成』ガイドを参照してください。ACC をインストールして構成したら、Workspace ONE UEM ディレクトリ サービスを Active Directory に統合します。ディレクトリ サービスを有効にする方法については、『VMware Workspace ONE UEM ディレクトリ サービス ガイド』を参照してください。

Workspace ONE の AirWatch Cloud Connector 認証を実装するため、VMware Identity Manager コンソールでは、パスワード (Workspace ONE UEM Connector) 認証方法が組み込み ID プロバイダに関連付けられています。

ジャストインタイム サポートを Workspace ONE UEM で有効にし、ユーザーが初めてログインしたときに、新しいユーザーを VMware Identity Manager ディレクトリに追加できます。ジャストインタイム サポートが有効になると、ユーザーは Workspace ONE にアクセスするために Workspace ONE UEM サーバからの次のスケジュール設定された同期を待つ必要はありません。代わりに、新しいユーザーは、iOS や Android デバイス、またはデスクトップ コンピュータから Workspace ONE ポータルにログインし、Active Directory のユーザー名とパスワードを入力します。VMware Identity Manager サービスは、AirWatch Cloud Connector を介して Active Directory の認証情報を認証し、ユーザー プロファイルをディレクトリに追加します。

認証方法を組み込み ID プロバイダで関連付けたら、この認証方法に適用するアクセス ポリシーを作成します。

注: ユーザー名とパスワードの認証は、AirWatch Cloud Connector 環境に統合されます。その他の VMware Identity Manager でサポートされている認証方法を使用してユーザーを認証するには、VMware Identity Manager コネクタを構成する必要があります。

ユーザー属性マッピングの管理

Workspace ONE UEM ディレクトリと VMware Identity Manager ディレクトリ間のユーザー属性マッピングを構成できます。

VMware Identity Manager, の [ID とアクセス管理] タブの [ユーザー属性] ページには、Workspace ONE UEM ディレクトリ属性にマッピングされるデフォルトのディレクトリ属性が一覧表示されます。必須の属性には、アスタリスクが付けられています。プロファイルで必須の属性が指定されていないユーザーは、VMware Identity Manager サービスで同期されません。

表 2-1. デフォルトの Workspace ONE UEM ディレクトリ属性のマッピング

VMware Identity Manager ユーザー属性名	Workspace ONE UEM ユーザー属性へのデフォルトのマッピング
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	ドメイン
disabled (external user disabled)	disabled
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Email*
userName	username*

Workspace ONE UEM ディレクトリから VMware Identity Manager ディレクトリへのユーザーとグループの同期

Workspace ONE UEM コンソールで VMware Identity Manager を設定し、Workspace ONE UEM ディレクトリの組織グループ インスタンスと VMware Identity Manager 間の接続を確立します。この接続は、VMware Identity Manager サービスで作成されたディレクトリにユーザーとグループを同期するために使用されます。

ユーザーとグループは、最初に手動で VMware Identity Manager ディレクトリに同期されます。Workspace ONE UEM 同期スケジュールは、ユーザーとグループを VMware Identity Manager ディレクトリといつ同期させるかを決定します。

ユーザーまたはグループが Workspace ONE UEM サーバで追加または削除されると、変更はすぐに VMware Identity Manager サービスに反映されます。

前提条件

- VMware Identity Manager のローカル管理者名とパスワード。
- Workspace ONE UEM ディレクトリからマッピングする属性値を特定します。「ユーザー属性マッピングの管理」を参照してください。

手順

1 Workspace ONE UEM コンソールで、[グループと設定] > [すべての設定] ページの [グローバル] > [カスタマレベルの組織グループ] を選択して、[システム] - [エンタープライズ統合] > [VMware Identity Manager] の順に移動します。

2 [サーバ] セクションで [構成] をクリックします。

> 注: [構成] ボタンは、同じ組織グループにディレクトリ サービスも構成されている場合にのみ使用できます。[構成] ボタンが表示されない場合は、正しい組織グループを選択していません。組織グループは、[グローバル] ドロップダウン メニューで変更できます。

3 VMware Identity Manager 設定を入力します。

オプション	説明
URL	テナント VMware URL を入力します。たとえば、`https://myco.identitymanager.com` となります。
管理者ユーザー名	VMware Identity Manager のローカル管理者ユーザー名を入力します。
管理者パスワード	VMware Identity Manager のローカル管理者ユーザーのパスワードを入力します。

4 [次へ] をクリックします。

5 カスタム マッピングを有効にして、Workspace ONE UEM から VMware Identity Manager サービスへのユーザー属性マッピングを構成します。

6 [接続をテスト] をクリックして、設定が正しいことを検証します。

7 [今すぐ同期] をクリックして、すべてのユーザーとグループを VMware Identity Manager サービスに手動で同期します。

注: システム負荷の制御のため、手動同期は前回の同期から 4 時間経過しないと実行できません。

VMware Identity Manager サービスに Workspace ONE UEM ディレクトリが作成され、ユーザーとグループが VMware Identity Manager のディレクトリに同期されます。

次のステップ

VMware Identity Manager コンソールの [ユーザーとグループ] タブで、ユーザーとグループの名前が同期されていることを確認します。

Workspace ONE UEM に対するパスワード認証の構成を管理する

Workspace ONE UEM をインストールし、VMware Identity Manager サービスを追加した際にセットアップされたパスワード (AirWatch Connector) 構成を確認し、管理できます。

パスワード (AirWatch Connector) 認証方法は、[ID とアクセス管理] > [認証方法] ページで管理され、[ID プロバイダ] ページの組み込み ID プロバイダに関連付けられます。

重要: AirWatch Cloud Connector ソフトウェアがアップグレードされたら、VMware Identity Manager コンソールの [AirWatch] ページで Workspace ONE UEM の設定を更新してください。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[認証方法] を選択します。

2 [パスワード (AirWatch Connector)] の [構成] 列で鉛筆アイコンをクリックします。

3 以下の構成を確認します。

オプション	説明
AirWatch パスワード認証を有効にする	このチェック ボックスにより、Workspace ONE UEM パスワード認証が有効になります。
AirWatch 管理コンソール URL	Workspace ONE UEM URL があらかじめ入力されています。

オプション	説明
AirWatch API キー	Workspace ONE UEM 管理用の API キーがあらかじめ入力されています。
認証に使用する証明書	Workspace ONE UEM Cloud Connector の証明書があらかじめ入力されています。
証明書のパスワード	Workspace ONE UEM Cloud Connector の証明書のパスワードがあらかじめ入力されています。
AirWatch グループ ID	組織グループ ID があらかじめ入力されています。
許可されている認証試行回数	Workspace ONE UEM パスワードを認証に使用するときのログイン試行の最大失敗回数。失敗したログインの回数がこの値に達すると、以降のログインは許可されません。このオプションが設定されている場合、VMware Identity Manager サービスはフォールバック認証方法の使用を試みます。デフォルトは、5 回です。
JIT を有効化	JIT が有効になっていない場合、ユーザーが初めてログインする際に、VMware Identity Manager サービスで動的にジャストインタイム プロビジョニングを有効にするには、このチェック ボックスを選択します。

4 [保存] をクリックします。

組み込み ID プロバイダの構成

複数の組み込み ID プロバイダを構成し、[ID とアクセス管理] > [認証方法] ページで構成した認証方法を関連付けることができます。

手順

1 [ID とアクセス管理] タブで、[管理] - [ID プロバイダ] の順に移動します。

2 [ID プロバイダを追加] をクリックして、[組み込み IDP を作成] を選択します。

オプション	説明
ID プロバイダ名	この組み込み ID プロバイダ インスタンスの名前を入力します。
ユーザー	認証するユーザーを選択します。構成されたディレクトリがリストされます。
ネットワーク	サービスに構成されている既存のネットワーク範囲が表示されます。各ユーザーの IP アドレスに基づいて、認証時に ID プロバイダ インスタンスが使用するネットワーク範囲を選択します。
認証方法	サービスで構成されている認証方法が表示されます。この組み込み ID プロバイダに関連付ける認証方法のチェック ボックスを選択します。 [デバイス コンプライアンス (Workspace ONE UEM)] と [パスワード (AirWatch Connector)] オプションについては、[AirWatch の構成] ページで有効になっていることを確認してください。

3 [追加] をクリックします。

次のステップ

デフォルトのアクセス ポリシー ルールを設定して、認証ポリシーをルールに追加します。「コンプライアンス チェック ルールの構成」を参照してください。

Workspace ONE UEM により管理された iOS デバイス向けのモバイル シングル サインオン認証の実装

3

iOS デバイス認証の場合、VMware Identity Manager は VMware Identity Manager サービスに組み込まれた ID プロバイダを使用してモバイル SSO 認証へのアクセスを提供します。

iOS デバイスのためのこの認証方法は、コネクタまたはサードパーティのシステムを使用しないキー配布センター (KDC) を使用します。Kerberos 認証によって、ドメインに正常にログインしたユーザーは、認証を再度行わずに Workspace ONE アプリケーション ポータルにアクセスできます。

この章には、次のトピックが含まれています。

iOS 版モバイル SSO を構成するための実装の概要

Workspace ONE UEM により管理された iOS 9 以降のデバイスのモバイル SSO 認証の実装では次の構成手順が必要です。

- iOS 版モバイル SSO を構成するための発行元証明書をダウンロードします。
  - Active Directory の証明書サービスを使用している場合は、Active Directory の証明書サービスで Kerberos 証明書配布用の認証局テンプレートを構成します。次に、Active Directory 認証局を使用するように Workspace ONE UEM を構成します。Workspace ONE UEM コンソールで証明書テンプレートを追加します。iOS 版モバイル SSO を構成するための発行元証明書をダウンロードします。
  - Workspace ONE UEM 認証局を使用している場合は、証明書を VMware Identity Manager の統合ページで有効にします。iOS 版モバイル SSO を構成するための発行元証明書をダウンロードします。

- 使用するキー配布センター (KDC) を確立します。
- Workspace ONE UEM コンソールで、iOS デバイス プロファイルを構成し、シングル サインオンを有効にします。
- iOS 版モバイル SSO 認証方法を構成します。
- VMware Identity Manager コンソールで、組み込みの ID プロバイダを構成し、iOS 版モバイル SSO 認証を関連付けます。

Workspace ONE UEM での Active Directory 認証局の構成

Workspace ONE UEM が管理する iOS 9 モバイル デバイスにシングル サインオン認証を設定するため、Active Directory と Workspace ONE UEM 間の信頼関係を確立し、VMware Identity Manager で iOS 版モバイル SSO 認証方法を有効にできます。

Active Directory 証明書サービスで Kerberos 証明書を配布するように認証局と証明書テンプレートを構成した後、Workspace ONE UEM で認証に使用する証明書を要求し、Workspace ONE UEM コンソールに認証局を追加できるようにします。

手順

1 Workspace ONE UEM コンソールのメイン メニューで、[デバイス] > [証明書] > [認証局] の順に移動します。

2 [追加] をクリックします。

3 認証局ページで以下を設定します。

注: このフォームの入力を始める前に、権限のタイプとして Microsoft AD CS が選択されていることを確認してください。

オプション	説明
名前	新しい認証局の名前を入力します。
認証局の種類	[Microsoft ADCS] が選択されていることを確認してください。
プロトコル	プロトコルとして [ADCS] を選択します。
サーバのホスト名	サーバの URL を入力します。ホスト名を `https://{servername.com}/certsrv.adcs/` の形式で入力します。サイトは、サイトのセットアップ方法に応じて http または https となります。URL の最後には、 `/` を含める必要があります。 注: URL のテスト時に接続が失敗した場合、アドレスから http:// または https:// を削除し、接続を再度テストします。
認証局名	ADCS エンド ポイントの接続先である認証局の名前を入力します。この名前は、認証局サーバで認証局アプリケーションを起動することで確認できます。
認証	[サービス アカウント] が選択されていることを確認してください。
ユーザー名とパスワード	Workspace ONE UEM で証明書を要求および発行するためのアクセス権が付与された、AD CS 管理者アカウントのユーザー名とパスワードを入力します。

4 [保存] をクリックします。

次のステップ

Workspace ONE UEM で証明書テンプレートを構成します。

Active Directory 認証局を使用するための Workspace ONE UEM の構成

認証局テンプレートは、Kerberos 証明書の配布用に適切に構成する必要があります。Active Directory 証明書サービス (AD CS) では、既存の Kerberos 認証テンプレートを複製し、iOS Kerberos 認証の新しい認証局テンプレートを構成できます。

AD CS の Kerberos 認証テンプレートを複製する際は、[新しいテンプレートのプロパティ] ダイアログ ボックスで、以下の情報を構成する必要があります。

図 3-1. Active Directory 証明書サービスの [新しいテンプレートのプロパティ] ダイアログ ボックス

- [全般] タブ。テンプレート表示名とテンプレート名を入力します。たとえば、iOSKerberos のように入力します。これは、証明書テンプレート スナップイン、証明書スナップイン、および証明機関スナップインで表示される表示名です。
- [要求処理] タブ。[秘密キーのエクスポートを許可する] を有効にします。
- [サブジェクト名] タブ。[要求に含まれる] ラジオ ボタンを選択します。Workspace ONE UEM が証明書を要求する場合、サブジェクト名が Workspace ONE UEM によって提供されます。
- [拡張] タブ。アプリケーション ポリシーを定義します。
  - [アプリケーション ポリシー] を選択し、[編集] をクリックして新しいアプリケーション ポリシーを追加します。このポリシーに Kerberos Client Authentication という名前を付けます。
  - 1.3.6.1.5.2.3.4 というオブジェクト識別子 (OID) を追加します。これは変更しないでください。
  - [アプリケーション ポリシーの説明] リストで、表示されている Kerberos Client Authentication ポリシーおよびスマート カード認証ポリシー以外のすべてのポリシーを削除します。
- [セキュリティ] タブ。証明書を使用できるユーザーのリストに、Workspace ONE UEM アカウントを追加します。アカウントに権限を設定します。セキュリティ プリンシパルには、証明書テンプレートのアクセス許可を含む証明書テンプレートのすべての属性を変更できるように、フル コントロールを設定します。または、組織の要件に従って権限を設定します。

変更を保存します。このテンプレートを、Active Directory 認証局で使用するテンプレートのリストに追加します。

Workspace ONE UEM で認証局を構成し、証明書テンプレートを追加します。

Workspace ONE UEM での証明書テンプレートの追加

ユーザーの証明書を生成するために使用する、認証局を関連付けた証明書テンプレートを追加します。

前提条件

Workspace ONE UEM で認証局を構成します。

手順

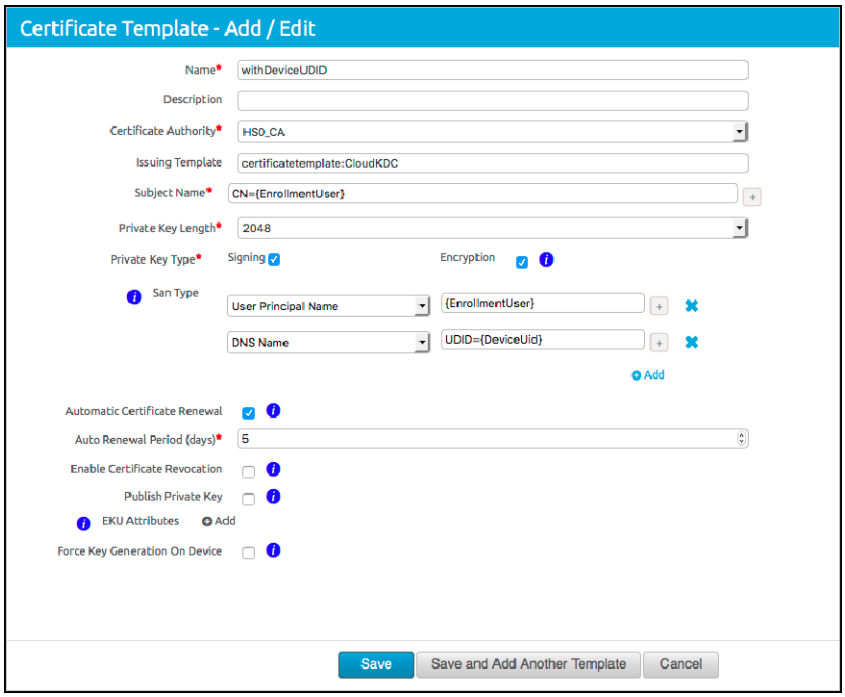
1 Workspace ONE UEM コンソールで、[システム] > [エンタープライズ統合] > [認証局] に移動します。

2 [要求テンプレート] タブを選択し、[追加] をクリックします。

3 証明書テンプレートのページで以下を構成します。

オプション	説明
名前	Workspace ONE UEM の新しい要求テンプレートの名前を入力します。
認証局	ドロップダウン メニューで、作成した認証局を選択します。
発行するテンプレート	Microsoft CA 証明書テンプレート名を、AD CS で作成したとおりに入力します。たとえば、**`iOSKerberos`** のように入力します。
サブジェクト名	テンプレートのサブジェクト名を入力します。+ をクリックして、リストからルックアップ値を選択することができます。テキスト ボックスで、[CN =]の後に値が入力されていることを確認します。ルックアップ タイプに DeviceUid を選択した場合、値の後に半角コロン (:) を入力し、リストからルックアップ値を選択します。たとえば、[CN = {deviceuid}: {lookupvalue}] のようになります。ここで {} テキスト ボックスは Workspace ONE UEM のルックアップ値です。必ずコロン (:) を含めるようにしてください。このテキスト ボックスに入力するテキストは証明書のサブジェクトで、これにより証明書を受信した人やデバイスを判断することができます。
プライベート キー（秘密鍵）の長さ	プライベート キーの長さは、AD CS で使用する証明書テンプレートの設定と一致します。通常は、2048 です。
プライベート キーのタイプ	[署名]および[暗号化] のチェック ボックスをオンにします。
SAN タイプ	[+ 追加] をクリックします。代替識別名には、[ユーザー プリンシパル名] を選択します。値は **`{EnrollmentUser}`** にする必要があります。 デバイス コンプライアンス チェックが Kerberos 認証で構成されていて、サブジェクト名のルックアップ値として DeviceUid を構成しなかった場合、2 つ目の SAN タイプを追加して、デバイスの一意の識別子 (UDID) を含めます。SAN タイプの [DNS 名]を選択します。値は [UDID={DeviceUid}] にする必要があります。
証明書の自動更新	このチェック ボックスをオンにすると、このテンプレートを使用する証明書は、有効期限が切れる前に自動的に更新されます。
自動更新期間 (日)	自動更新期間を日数で指定します。
証明書の取り消しを有効化	チェック ボックスをオンにすると、該当するデバイスが登録解除された場合や削除された場合、または該当するプロファイルが削除された場合に、証明書が自動的に失効します。
プライベート キーの公開	プライベート キーを公開するには、このチェック ボックスを選択します。
プライベート キーの送信先	[ディレクトリ サービス] または [カスタム Web サービス] のいずれか

4 [保存] をクリックします。



次のステップ

VMware Identity Provider コンソールで、組み込み ID プロバイダに iOS 版モバイル SSO 認証方法を設定します。

Kerberos 認証用の Workspace ONE UEM 認証局の使用

Active Directory 認証局の代わりに Workspace ONE UEM 認証局を使用して、Workspace ONE UEM で管理される iOS 9 モバイル デバイスに対し、組み込みの Kerberos 認証を使用するシングル サインオンをセットアップできます。Workspace ONE UEM 認証局を Workspace ONE UEM コンソールで有効にして、VMware Identity Manager サービスで使用する CA 発行者証明書をエクスポートできます。

Workspace ONE UEM 認証局は Simple Certificate Enrollment Protocol (SCEP) に準拠するように設計されており、SCEP をサポートする Workspace ONE UEM 管理デバイスで使用されます。VMware Identity Manager と Workspace ONE UEM の統合では、Workspace ONE UEM 認証局を使用して証明書をプロファイルの一部として iOS 9 モバイル デバイスに発行します。

Workspace ONE UEM 認証局の発行者ルート証明書は、OCSP の署名証明書でもあります。

Workspace ONE UEM 認証局を有効にしてエクスポート

Workspace ONE UEM で VMware Identity Manager が有効になっている場合は、Workspace ONE UEM 発行者ルート証明書を生成してエクスポートし、管理対象となる iOS 9 モバイル デバイスの iOS 版モバイル SSO 認証で使用できます。

手順

1 Workspace ONE UEM コンソールで、[システム] - [エンタープライズ統合] > [VMware Identity Manager] の順に移動します。

Workspace ONE UEM 認証局を有効にするには、組織グループ タイプが [カスタマ] である必要があります。

ヒント: グループ タイプを表示または変更するには、[グループと設定] > [グループ] - [組織グループ] > [組織グループ詳細] の順に移動します。

2 [構成] をクリックします。

3 [証明書] セクションで、[有効] をクリックします。

このページに、発行者ルート証明書の情報が表示されます。

4 [エクスポート] をクリックしてファイルを保存します。

次のステップ

VMware Identity Manager コンソールで、組み込みの ID プロバイダに Kerberos 認証を構成し、認証局発行者証明書を追加します。

iOS デバイスから認証するためのキー配布センターの使用

iOS デバイスの場合は、サービスを Kerberos と統合します。Kerberos 認証によって、ドメインに正常にログインしたユーザーは、認証を再度行わずにアプリケーション ポータルにアクセスできます。iOS デバイスのためのこの認証方法は、コネクタまたはサードパーティのシステムを使用しないキー配布センター (KDC) を使用します。

VMware Identity Manager クラウドのテナントは、KDC を管理または構成する必要はありません。

オンプレミス展開では、2 つの KDC オプションが利用可能です。

- 組み込み KDC。組み込み KDC を使用する場合は、アプライアンス上で KDC を初期化し、パブリック DNS エントリを作成して Kerberos クライアントが KDC を検出できるようにする必要があります。組み込み KDC を有効にする方法の詳細については、『VMware Identity Manager 管理ガイド』を参照してください。
- VMware Identity Manager クラウド ホスト型サービスとしての KDC。クラウドで KDC を使用する場合は、iOS 認証アダプタ ページで適切なレルム名を選択する必要があります。

注: VMware Identity Manager がインストールされており、Windows 環境で Workspace ONE UEM が構成されている場合、VMware Identity Manager クラウドでホストされている KDC サービスを使用するように iOS モバイルの認証方法を構成する必要があります。

クラウド ホスト型 KDC サービスの使用

iOS 版モバイル SSO での Kerberos 認証の使用をサポートするため、VMware Identity Manager はクラウド ホスト型 KDC サービスを提供します。

Workspace ONE UEM を使用して Windows 環境に VMware Identity Manager サービスを展開する場合は、クラウドでホストされている KDC サービスを使用する必要があります。

VMware Identity Manager アプライアンスで管理されている KDC を使用するには、『VMware Identity Manager のインストールと構成ガイド』の「iOS デバイスで Kerberos 認証を使用するための準備」を参照してください。

iOS 版モバイル SSO 認証を構成する場合は、クラウド ホスト型 KDC サービスのレルム名を設定します。レルムは、認証データを保持する管理エンティティの名前です。[保存] をクリックすると、VMware Identity Manager サービスがクラウド ホスト型 KDC サービスに登録されます。KDC サービスに保存されるデータは、iOS 版モバイル SSO 認証方法の構成によって決まります。これには、CA 証明書、OCSP 署名証明書、および OCSP 要求設定の詳細が含まれます。

ログ記録はクラウド サービスに保存されます。ログ記録の個人識別情報 (PII) には、ユーザー プロファイルの Kerberos プリンシパル名、サブジェクト DN と UPN および E メール SAN の値、ユーザーの証明書のデバイス ID、およびユーザーがアクセスしている IDM サービスの FQDN が含まれます。

クラウド ホスト型 KDC サービスを使用するには、VMware Identity Manager を次のように構成する必要があります。

- VMware Identity Manager サービスの FQDN はインターネット経由でアクセスできる必要があります。VMware Identity Manager で使用される SSL/TLS 証明書は公的に署名されている必要があります。
- 送信要求/応答ポート 88 (UDP) とポート 443 (HTTPS/TCP) は、VMware Identity Manager サービスからアクセスできる必要があります。
- OCSP を有効にする場合、OCSP レスポンダはインターネット経由でアクセスできる必要があります。

iOS 版モバイル SSO 認証の設定

VMware Identity Manager コンソールの [認証方法] ページから iOS 版モバイル SSO 認証方法を設定します。組み込み ID プロバイダで使用するモバイル SSO（iOS 版）認証方法を選択します。

前提条件

- Workspace ONE UEM テナントでユーザーへの証明書発行に使用する認証局の PEM または DER ファイル
- 取り消し確認用の OCSP レスポンダの署名証明書
- KDC サービスの場合は、KDC サービスのレルム名を選択します。組み込み KDC サービスを使用している場合は、KDC を初期化する必要があります。組み込み KDC の詳細については、『VMware Identity Manager のインストールと構成』を参照してください。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[管理] - [認証方法] に移動します。

2 [モバイル SSO (iOS 版)]の [構成] 列で鉛筆アイコンをクリックします。

3 Kerberos 認証方法を構成します。

オプション	説明
KDC 認証を有効にする	このチェック ボックスをオンにすると、Kerberos 認証をサポートする iOS デバイスを使用して、ユーザーがログインできるようになります。
レルム	クラウド内にテナントを展開する場合、レルムの値は読み取り専用です。表示されるレルム名は、テナントの Identity Manager レルム名です。 オンプレミスの展開で、クラウド ホスト型の KDC を使用している場合は、提供されている定義済みでサポート対象のレルム名を入力します。このパラメータのテキストはすべて大文字で入力する必要があります。たとえば、OP.VMWAREIDENTITY.COM のようになります。組み込み KDC を使用している場合は、KDC を初期化したときに設定したレルム名が表示されます。
ルートおよび中間 CA 証明書	認証局の発行者証明書ファイルをアップロードします。ファイル形式には PEM または DER のいずれかを使用できます。
アップロードされた CA 証明書サブジェクト DN	アップロードされた証明書ファイルの内容が表示されます。複数のファイルをアップロードすることができ、アップロードに含まれるすべての証明書がリストに追加されます。
OCSP の有効化	証明書検証プロトコルとして Online Certificate Status Protocol (OCSP) を使用して、証明書の失効ステータスを取得するには、このチェック ボックスをオンにします。
OCSP Nonce を送信する	応答時に、OCSP 要求の一意の ID を送信する場合は、このチェック ボックスをオンにします。
OCSP レスポンダの署名証明書	レスポンダの OCSP 証明書をアップロードします。 Workspace ONE UEM 認証局を使用しているときは、発行者証明書が OCSP 証明書として使用されます。この場合も同様に Workspace ONE UEM 証明書をアップロードします。
OCSP レスポンダの署名証明書サブジェクト DN	アップロードされた OCSP 証明書ファイルが表示されます。
キャンセル メッセージ	認証が長時間におよぶ場合に表示するカスタムのログイン メッセージを作成します。カスタム メッセージを作成しない場合、デフォルトのメッセージは「`Attempting to authenticate your credentials`」になります。
リンクのキャンセルを有効にする	認証が長時間に及ぶ場合に、ユーザーが [キャンセル] をクリックして認証を停止し、ログインをキャンセルできます。 キャンセル リンクを有効にすると、表示される認証エラー メッセージの最後に「キャンセル」という文字が表示されます。
エンタープライズ デバイス管理サーバの URL	デバイスがモバイル デバイス管理 (MDM) 用の Workspace ONE UEM に登録されていないためにアクセスが拒否される場合は、MDM サーバの URL を入力してユーザーをリダイレクトします。この URL は、認証失敗のエラー メッセージに表示されます。ここに URL を入力しない場合、一般的なアクセス拒否のメッセージが表示されます。

4 [保存] をクリックします。

次のステップ

- 組み込み ID プロバイダのモバイル SSO (iOS 版) 認証方法を関連付けます。

iOS 版モバイル SSO 認証用の組み込み ID プロバイダの設定

組み込み ID プロバイダを設定し、[ID とアクセス管理] > [認証方法] ページで設定した iOS 版モバイル SSO 認証方法を関連付けることができます。

前提条件

[認証方法] ページで設定されている iOS 版モバイル SSO 認証。

手順

1 [ID とアクセス管理] タブで、[管理] - [ID プロバイダ] の順に移動します。

2 [ID プロバイダを追加] をクリックして、[組み込み IDP を作成] を選択します。

オプション	説明
ID プロバイダ名	この組み込み ID プロバイダ インスタンスの名前を入力します。
ユーザー	認証するユーザーを選択します。構成されたディレクトリがリストされます。
ネットワーク	サービスに構成されている既存のネットワーク範囲が表示されます。各ユーザーの IP アドレスに基づいて、認証時に ID プロバイダ インスタンスが使用するネットワーク範囲を選択します。
認証方法	サービスで構成されている認証方法が表示されます。この組み込み ID プロバイダに関連付ける iOS 版認証方法のチェック ボックスを選択します。その他のすべての認証方法を追加します。 デバイス コンプライアンス (Workspace ONE UEM) とパスワード（Workspace ONE UEM コネクタ）については、[Workspace ONE UEM の構成] ページでオプションが有効になっていることを確認してください。

3 [KDC 証明書のエクスポート] セクションで、[証明書をダウンロード] をクリックします。この証明書を、Workspace ONE UEM コンソールからアクセス可能なファイルに保存します。

この証明書は、Workspace ONE UEM で iOS デバイス プロファイルを設定するときにアップロードします。

4 [追加] をクリックします。

次のステップ

- iOS デバイスの Kerberos 認証用にデフォルトのアクセス ポリシー ルールを構成します。この認証方法が、ルール内で最初の認証方法となるようにセットアップします。
- Workspace ONE UEM コンソールに移動し、Workspace ONE UEM で iOS デバイス プロファイルを設定して、VMware Identity Manager から KDC サーバ証明書の発行者証明書を追加します。

Active Directory 認証局と証明書テンプレートを使用した Workspace ONE UEM での Apple iOS プロファイルの構成

ID プロバイダの設定をデバイスにプッシュするため、Workspace ONE UEM で Apple iOS デバイス プロファイルを作成して展開します。このプロファイルには、デバイスを VMware の ID プロバイダに接続するために必要な情報と、デバイスが認証に使用する証明書が含まれます。シングル サインオンを有効にすると、アプリケーションごとに認証することなくシームレスにアクセスできます。

前提条件

- VMware Identity Manager で構成されている iOS 版モバイル SSO。
- Workspace ONE UEM 管理者コンソールからアクセス可能なコンピュータに格納された、iOS Kerberos の認証局ファイル。
- Workspace ONE UEM で適切に構成されている認証局と証明書テンプレート。
- iOS デバイスの iOS 版モバイル SSO 認証を使用する URL とアプリケーション バンドル ID のリスト。

手順

1 Workspace ONE UEM コンソールで、[デバイス] > [プロファイルとリソース] > [プロファイル] の順に移動します。

2 [追加] - [プロファイルの追加] を選択し、[Apple iOS] を選択します。

3 **iOSKerberos** という名前を入力して、[全般] の設定を構成します。

4 左側のナビゲーション ペインで、[資格情報] - [構成] の順に選択して認証情報を構成します。

オプション	説明
認証情報ソース	ドロップダウン メニューから [定義済み認証局] を選択します。
認証局	ドロップダウン メニューのリストから認証局を選択します。
証明書テンプレート	ドロップダウン メニューから、認証局を参照する要求テンプレートを選択します。これは、Workspace ONE UEM の「証明書テンプレートの追加」で作成された証明書テンプレートです。

5 ページの右下隅にある [+] をもう一度クリックし、2 つ目の認証情報を作成します。

6 [資格情報ソース] ドロップダウン メニューで、[アップロード] を選択します。

7 認証情報名を入力します。

8 [アップロード] をクリックして、[ID とアクセス管理] > [管理] > [ID プロバイダ] > [組み込みの ID プロバイダ] ページからダウンロードされた KDC サーバ ルート証明書をアップロードします。

9 左側のナビゲーション ペインで、[シングル サインオン] を選択して、[構成] をクリックします。

10 接続情報を入力します。

オプション	説明
アカウント名	**Kerberos** と入力します。
Kerberos プリンシパル名	[+] をクリックして [{EnrollmentUser}] を選択します。
レルム	クラウドにテナントを展開する場合、テナントに Identity Manager レルム名を入力します。このパラメータのテキストは大文字で記入する必要があります。たとえば、**VMWAREIDENTITY.COM** のように記入します。 オンプレミス展開では、VMware Identity Manager アプライアンスで KDC を初期化したときに使用したレルム名を入力します。たとえば、**EXAMPLE.COM** です。
更新証明書	ドロップダウン メニューから [証明書 #1] を選択します。これは認証情報で最初に構成された Active Directory CA 証明書です。

オプション	説明
URL プレフィックス	このアカウントを使用するために、HTTP 経由の Kerberos 認証用に一致する必要のある URL プリフィックスを入力します。 クラウドにテナントを展開する場合、VMware Identity Manager サーバ URL を `https://<tenant>.vmwareidentity.<region>` のように入力します。 ンプレミス展開では、VMware Identity Manager サーバ URL を `https://myco.example.com` のように入力します。
アプリケーション	このサインオンで使用を許可する一連のアプリケーション ID を入力します。iOS の組み込みの Safari ブラウザを使用してシングル サインオンを実行するには、`com.apple.mobilesafari` のように最初のアプリケーション バンドル ID を入力します。その後続けてアプリケーション バンドル ID を入力します。これらのアプリケーションは、SAML 認証をサポートしている必要があります。

11 [保存して公開] をクリックします。

次のステップ

スマート グループにデバイス プロファイルを割り当てます。スマート グループは、どのプラットフォーム デバイス、およびユーザーが割り当てられたアプリケーション、ブック、遵守ポリシー、デバイス プロファイル、またはプロビジョニングを受信するかを決定するカスタマイズ可能なグループです。

Workspace ONE UEM での Workspace ONE UEM 認証局を使用した Apple iOS プロファイルの構成

ID プロバイダの設定をデバイスにプッシュするため、Workspace ONE UEM で Apple iOS デバイス プロファイルを作成して展開します。このプロファイルには、デバイスを VMware の ID プロバイダに接続するために必要な情報と、デバイスが認証に使用する証明書が含まれます。

前提条件

- VMware Identity Manager で構成されている組み込みの Kerberos。
- Workspace ONE UEM コンソールからアクセス可能なコンピュータに保存された VMware Identity Manager KDC サーバのルート証明書ファイル。
- 有効になっており、Workspace ONE UEM コンソールの [システム] > [エンタープライズ統合] > [VMware Identity Manager] ページからダウンロードした証明書。
- iOS デバイスの組み込みの Kerberos 認証を使用する URL とアプリケーション バンドル ID のリスト。

手順

1 Workspace ONE UEM コンソールで、[デバイス] > [プロファイルとリソース] > [プロファイル] > [プロファイルの追加] の順に移動し、[Apple iOS] を選択します。

2 プロファイルの [全般] 設定を構成し、デバイスの名前として **`iOSKerberos`** と入力します。

3 左側のナビゲーション ペインで、[SCEP] - [構成] の順に選択して認証情報を構成します。

オプション	説明
認証情報ソース	ドロップダウン メニューから [AirWatch 認証局] を選択します。
認証局	ドロップダウン メニューから [AirWatch 認証局] を選択します。
証明書テンプレート	[シングル サインオン] を選択して、AirWatch 認証局が発行する証明書のタイプを設定します。

4 [資格情報] > [構成] をクリックして、2 番目の証明書を作成します。

5 [資格情報ソース] ドロップダウン メニューで、[アップロード] を選択します。

6 iOS Kerberos 認証情報名を入力します。

7 [アップロード] をクリックして、[ID とアクセス管理] > [管理] > [ID プロバイダ] > [組み込みの ID プロバイダ] ページからダウンロードされた VMware Identity Manager KDC サーバ ルート証明書をアップロードします。

8 左側のナビゲーション ペインで、[シングル サインオン] を選択します。

9 接続情報を入力します。

オプション	説明
アカウント名	**Kerberos** と入力します。
Kerberos プリンシパル名	[+] をクリックして [{EnrollmentUser}] を選択します。
レルム	テナントをクラウドに展開する場合、テナントに VMware Identity Manager レルム名を入力します。このパラメータのテキストは大文字で記入する必要があります。たとえば、**VMWAREIDENTITY.COM** のように記入します。 オンプレミス展開では、VMware Identity Manager マシンで KDC を初期化したときに使用したレルム名を入力します。例：**EXAMPLE.COM**
更新証明書	iOS 8 以降のデバイスでは、ユーザーのシングル サインオン セッションの有効期限が切れた場合に、ユーザーの操作を必要とせずに、ユーザーを自動的に再認証するために使用する証明書を選択します。
URL プレフィックス	このアカウントを使用するために、HTTP 経由の Kerberos 認証用に一致する必要のある URL プリフィックスを入力します。 クラウドにテナントを展開する場合、VMware Identity Manager サーバ URL を **https://<tenant>.vmwareidentity のように入力します。<region>** オンプレミス展開では、VMware Identity Manager サーバ URL を **https://myco.example.com** のように入力します。
アプリケーション	このログインで使用を許可する一連のアプリケーション ID を入力します。iOS の組み込みの Safari ブラウザを使用してシングル サインオンを実行するには、**com.apple.mobilesafari** のように最初のアプリケーション バンドル ID を入力します。その後続けてアプリケーション バンドル ID を入力します。これらのアプリケーションは、SAML 認証をサポートしている必要があります。

10 [保存して公開] をクリックします。

iOS プロファイルがユーザーのデバイスに正常にプッシュされたら、ユーザーは組み込みの Kerberos 認証方法を使用して、認証情報を入力することなく VMware Identity Manager にログインできます。

次のステップ

スマート グループにデバイス プロファイルを割り当てます。スマート グループは、どのプラットフォーム デバイス、およびユーザーが割り当てられたアプリケーション、ブック、遵守ポリシー、デバイス プロファイル、またはプロビジョニングを受信するかを決定するカスタマイズ可能なグループです。

Workspace ONE UEM デバイス プロファイルの割り当て

デバイス プロファイルの作成後、スマート グループにプロファイルを割り当てます。

スマート グループは、どのプラットフォーム デバイス、およびユーザーが割り当てられたアプリケーション、遵守ポリシー、デバイス プロファイル、またはプロビジョニングを受信するかを決定するカスタマイズ可能なグループです。『Workspace ONE UEM Mobile Device Management ガイド』を参照してください。

手順

1 Workspace ONE UEM コンソールで、[デバイス] - [プロファイルとリソース] > [プロファイル] の順に移動します。

2 スマート グループに割り当てるデバイス プロファイルを選択します。

3 [全般] タブで、[割り当てるグループ] テキスト ボックスをクリックし、[割り当てグループを作成] を選択します。

4 [新しいスマートグループを作成] ページで、スマート グループの名前を入力します。

5 [プラットフォームと OS] を選択し、ドロップダウン メニューから正しいオペレーティング システムとバージョンを選択します。

6 [保存して公開] をクリックします。

スマート グループをデバイス オプションに割り当てると、ユーザーは Workspace ONE にログインし、カタログからアプリケーションにアクセスできるようになります。

管理された Android デバイス向けのモバイル シングル サインオン認証の実装

4

Android 版モバイル シングル サインオン (SSO) は、Workspace ONE UEM により管理される Android デバイス向けの証明書による認証方法の実装です。モバイル SSO により、ユーザーは自分のデバイスにログインし、パスワードを再入力せずに Workspace ONE アプリケーションに安全にアクセスできます。

VMware Tunnel® モバイル アプリが Android デバイスにインストールされ、認証フローに証明書とデバイス ID 情報が追加されます。Workspace ONE UEM Console の Tunnel 設定では認証のために VMware Identity Manager サービスにアクセスするように構成されており、このサービスは認証のためにデバイスから証明書を取得します。

Workspace ONE UEM Console で、次の設定も行います。

- Android VPN プロファイル。このプロファイルは Android 向けのアプリケーション単位のトンネル機能を有効にするために使用します。
- Workspace ONE UEM Console からアプリケーションのトンネル機能を使用する各アプリケーションの VPN を有効にします。
- アプリケーション単位の VPN に対して構成されるすべてのアプリケーション、プロキシ サーバの詳細、および VMware Identity Manager URL のリストを含むネットワーク トラフィック ルールを作成します。

オンプレミスの VMware Identity Manager サービスを使用して Android 版モバイル SSO を実装する場合は、VMware Identity Manager マシンで証明書プロキシ サービスを構成します。証明書プロキシ サービスを構成したら、VMware Identity Manager コンソールから VMware Identity Manager の組み込み ID プロバイダに証明書認証を設定できます。

クラウドの VMware Identity Manager サービスを使用して Android 版モバイル SSO を実装する場合は、VMware Identity Manager コンソールから VMware Identity Manager の組み込み ID プロバイダに証明書認証を設定できます。ユーザーのために証明書プロキシ サービスが管理されます。

Android 版のモバイル SSO の設定の詳細については、Workspace ONE ドキュメント センターのドキュメント『Android Mobile Single Sign-on to VMware Workspace One』を参照してください。

サポートされている Android デバイス

Android 5.1 以降がサポートされます。

Android デバイスからアクセスするアプリケーションは、SAML またはシングル サインオンのための別のフェデレーション規格をサポートしている必要があります。

Workspace ONE アプリケーションを使用した直接加入

5

Workspace ONE を使用した直接加入では、ユーザーは Workspace ONE アプリケーションのリソースにアクセスする前にデバイス加入を実行する必要があります。

Workspace ONE アプリケーションを使用した直接加入では、すべてのユーザーに対して、適切なアプリケーションストアに移動して Workspace ONE アプリケーションをダウンロードし、メール アドレスを入力して、プロンプトに従ってデバイス上で Workspace ONE の使用を開始するように指示できます。

サポート対象デバイス

- Apple iOS 9.0 以降
- Android Enterprise（旧称 Android for Work）5.1 以降
- Android Legacy 4.1 以降

  Android Legacy デバイスとは、Android Enterprise に対応していない Android デバイス、または Android Enterprise に対応した、Android Enterprise が有効になっていない Workspace ONE UEM インスタンスに接続しているデバイスです。

この章には、次のトピックが含まれています。

- Workspace ONE の直接加入を有効にする
- Workspace ONE を使用して Workspace ONE UEM に直接加入する場合のユーザー エクスペリエンス

Workspace ONE の直接加入を有効にする

Workspace ONE でのデバイスの直接加入は、Workspace ONE UEM コンソール上の組織グループ (OG) の [加入] > [制限] ページで有効にします。

Workspace ONE の直接加入を有効にすると、初めてログインする資格のあるデバイスが直接加入されます。直接加入の対象とならないデバイスには、Workspace ONE 登録済みの状態でのモバイル アプリケーション管理専用アクセスが許可されます。

手順

1 Workspace ONE UEM コンソールで、Workspace ONE の直接加入を有効にする組織グループを選択します。

2 [グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [加入] に移動し、[制限] タブを選択します。

3 [現在の設定] では、必要に応じて [上書き] を選択します。

4 [Workspace ONE の管理要件] にスクロールし、構成オプションを選択します。

設定	説明
[Workspace ONE には MDM が必要]	有効にすると、資格のあるデバイスとユーザーは Workspace ONE にログイン後すぐに加入するように要求されます。
[割り当てられるユーザー グループ]	[すべてのユーザー] がデフォルトのユーザー グループです。直接加入プロセスに含める特定のユーザー グループを選択できます。
[iOS]	iOS デバイスを含めることを許可します。無効にすると、iOS デバイスを直接加入する資格は与えられません。無効の場合でも、管理されていない状態で Workspace ONE UEM にデバイスを登録できます。
[Android Legacy]	Android Legacy デバイスを含めることを許可します。無効にすると、Android Legacy デバイスを直接加入する資格は与えられません。無効の場合でも、管理されていない状態で Workspace ONE UEM にデバイスを登録できます。
[Android Enterprise]	Android Enterprise デバイスを含めることを許可します。無効にすると、Android Enterprise デバイスを直接加入する資格は与えられません。無効の場合でも、管理されていない状態で Workspace ONE UEM にデバイスを登録できます。

5 [保存] をクリックします。

6 Workspace ONE でサポートされる加入オプションを使用して加入タブの設定を続けます。「Workspace ONE 直接加入の構成オプション」を参照してください。

Workspace ONE の直接加入の設定の詳細については、『VMware AirWatch Mobile Device Management Guide』の「デバイス加入」の章を参照してください。

Workspace ONE 直接加入の構成オプション

Workspace ONE UEM コンソールで Workspace ONE 直接加入を設定します。[グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [加入] に移動します。[Workspace ONE デバイス加入オプションの表] には、設定可能なメニュー項目がリストされています。

加入設定ページでは、デバイスとユーザー加入に関連するオプションを設定できます。ページは、以下で説明するタブに分割されます。デバイス加入の設定の詳細については、『VMware Workspace ONE UEM Mobile Device Management Guide』を参照してください。

図 5-1. Workspace ONE UEM コンソールの登録ページ

表 5-1. Workspace ONE 直接加入で設定可能なメニュー項目

[加入] タブ	Workspace ONE への直接加入で設定可能なメニュー項目
[認証]	ディレクトリ ユーザーがサポートされます。 また、SAML および Active Directory ユーザーが「オンザフライ」でサポートされます。LDAP なしの SAML ユーザーは、最初のログイン時に Workspace ONE UEM にユーザー レコードが存在する場合にサポートされます。 デバイス加入モードでは、[オープン加入] のみがサポートされます。[登録済みデバイスのみ] はサポートされていません。
[利用条件]	利用条件を作成し、ユーザーが直接加入プロセスを進める前にその利用条件に同意するように要求することができます。
[グループ化]	すべてのグループ化メニュー オプションは、Workspace ONE 直接加入と互換性があります。 デフォルトでは、[Workspace ONE のユーザー グループをリアルタイムで同期] が有効です。デバイスを加入させるときに、Workspace ONE UEM は Active Directory をリアルタイムで呼び出し、ユーザーのユーザー グループを同期します。Workspace ONE UEM にユーザーが存在しない場合、Workspace ONE UEM コンソールは最初にリアルタイムでユーザーを同期し、続いてユーザー グループを同期します。この機能が有効でない場合、Workspace ONE UEM コンソールは、ユーザー グループを同期しません。 注: この機能は CPU に負担がかかります。ユーザー グループが頻繁に変更されていない場合、またはユーザー グループがすでに Workspace ONE UEM に存在する場合は、パフォーマンスを向上させるためにこの設定を無効にして、Workspace ONE アプリケーションの起動時の遅延時間の問題を回避します。 「複数の Workspace ONE UEM 組織グループを設定するための展開戦略」の「デバイスを正しい組織グループに配置する」セクションを参照してください。
[制限]	■ [ユーザー アクセスの管理] では、[加入を既知のユーザーに制限] と [加入を構成済みのグループに制限] の両方を選択できます。 ■ デバイス数の上限がサポートされます。 ■ [ポリシー設定] は部分的にサポートされます。 ■ [許可された所有形態タイプ]。Workspace ONE は、「従業員所有」および「企業-専用」のみをプロンプト表示します。 注: 「コンテナを許可」加入タイプはサポートされません。
[オプションのプロンプト表示]	有効にすることができる 2 つのオプションのプロンプト表示は、[所有形態タイプのプロンプト表示] と [デバイス アセット番号のプロンプト表示を有効化] です。アセット番号の入力は、所有形態タイプが「企業所有」の場合にのみ要求されます。
[カスタマイズ]	[カスタマイズ] メニュー オプションがサポートされています。 ■ 加入後のランディング URL（iOS のみ） ■ MDM プロファイル メッセージ（iOS のみ） ■ カスタム MDM アプリケーションを使用する [各プラットフォームの専用メッセージテンプレートを使用する] を有効にすることができますが、特定の Workspace ONE メッセージ テンプレートは Workspace ONE 3.2 では使用できません。

Workspace ONE を使用して Workspace ONE UEM に直接加入する場合のユーザー エクスペリエンス

Workspace ONE を使用してモバイル デバイス管理を実装する場合、ユーザーは Workspace ONE アプリケーションをダウンロードし、Workspace ONE UEM を使用して認証し、デバイスを加入させます。デバイスを加入した後、ユーザーは Workspace ONE を使用して、資格のあるリソースをすぐに追加して使用できます。

Workspace ONE を使用してデバイスを加入させるときにユーザーが実行するプロセスは、iOS と Android Enterprise のどちらのデバイスでも同じです。Android Legacy の加入の場合、加入のために AirWatch Agent にリダイレクトされます。AirWatch Agent は、加入が完了すると自動的にコントロールを Workspace ONE に戻します。ユーザーは、これらの異なるケースでそれぞれ Workspace ONE にアクセスできます。

iOS デバイスでの Workspace ONE を使用した直接加入

Workspace ONE アプリケーションを Apple App Store からダウンロードしてインストールし、実行するようにユーザーに指示します。

手順

1 ユーザーはアプリケーションを開き、サーバの URL とメール アドレスを入力し、環境の設定に従って認証を実行します。

2 [企業により追加のセットアップが要求されています] 画面が表示されます。

図 5-2. デバイス加入の設定の通知

3 利用条件が設定されている場合、ユーザーは先に進む前にその利用条件に同意するように求められます。

4 デバイスの所有形態タイプを表示してデバイス アセット番号を要求するオプションのプロンプト表示を設定すると、この情報が表示されます。

図 5-3. デバイスの所有形態の選択

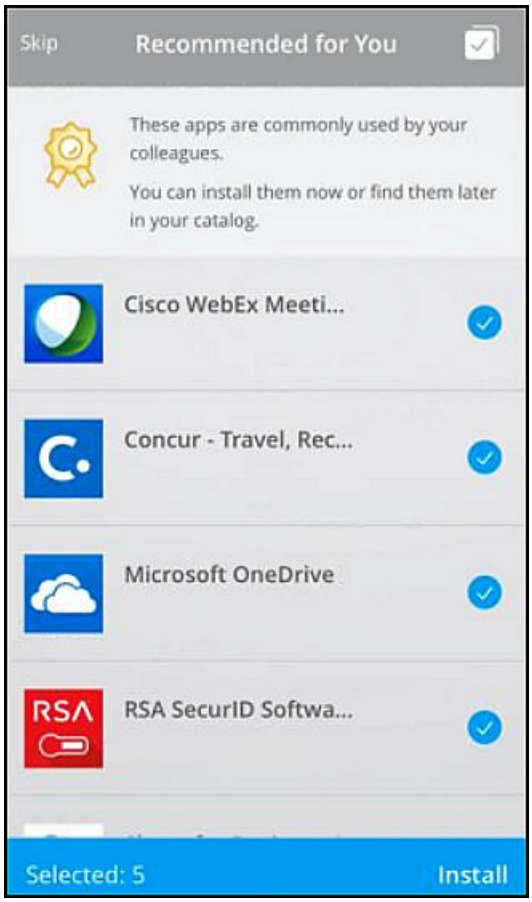
5 Safari が開き、ユーザーは [許可] をクリックして [設定] ページを開きます。

図 5-4. 構成プロファイルの設定を許可

ワークスペース サービスと構成プロファイルはデバイス上で設定されます。

これで、デバイスが Workspace ONE UEM に加入し、Workspace ONE が起動します。[推奨されるアプリ] 画面が表示されます。

図 5-5. [推奨されるアプリケーション] 画面



6 ユーザーは、インストールするアプリケーションを選択することも、この手順をスキップすることもできます。

これで、デバイスは Workspace ONE UEM MDM によって管理されます。推奨されるアプリケーションをインストールするように選択すると、ユーザーはそれらのアプリケーションのプッシュ通知を受信するようになります。

Android Enterprise デバイスでの Workspace ONE を使用した直接加入

Workspace ONE アプリケーションを Google App Store またはリポジトリからダウンロードしてインストールし、実行するようにユーザーに指示します。

手順

1 ユーザーはサーバの URL とメール アドレスを入力し、環境の設定に従って認証を実行します。

2 [企業により追加のセットアップが要求されています] 画面が表示されます。ユーザーは [続行] をクリックします。

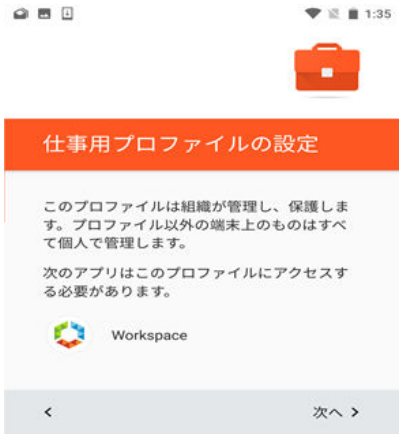
図 5-6. デバイス加入の設定の通知

3 利用条件が設定されている場合、ユーザーは先に進む前にその利用条件に同意するように求められます。

4 デバイスの所有形態タイプを表示してデバイス アセット番号を要求するオプションのプロンプト表示を設定すると、この情報が表示されます。

5 ワークスペース サービスと仕事用プロファイルはデバイス上で設定されます。

図 5-7. 仕事用プロファイルの通知の設定

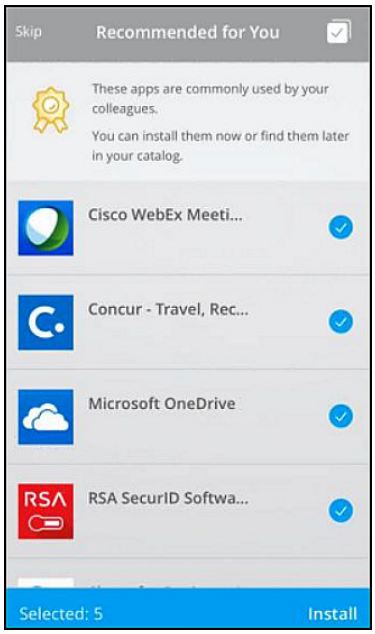


ユーザーは、この仕事用プロファイルでのデバイス管理の制御についてのメッセージを確認し、[OK] をクリックします。

Workspace ONE アプリケーションがインストールされ、Android Work アカウントが登録されます。

6 これで、デバイスが Workspace ONE UEM に加入し、Workspace ONE が起動します。[推奨されるアプリ] 画面が表示されます。

図 5-8. [推奨されるアプリケーション] 画面



7 ユーザーは、インストールするアプリケーションを選択することも、この手順をスキップすることもできます。

これで、デバイスは Workspace ONE UEM MDM によって管理されます。推奨されるアプリケーションをインストールするように選択すると、バッジつきの Android Enterprise ブリーフケース アイコンが表示されてそれらのアプリケーションのインストールが開始します。

レガシーの Android デバイスのデバイスの加入

Android Legacy デバイスのデバイス加入の場合、加入のために AirWatch Agent にリダイレクトされます。AirWatch Agent は、加入が完了すると自動的にコントロールを Workspace ONE に戻します。

ユーザーがアプリケーション ストアに移動して Workspace ONE をダウンロードするよう指示されます。

手順

1 ユーザーはアプリケーションを開き、サーバの URL またはメール アドレスを入力し、ログインするユーザー名とパスワードを入力します。

この時点で、Workspace ONE アプリケーションはデバイスが Android Enterprise で有効になっていないこと、および Workspace ONE のリソースにアクセスするためにデバイスを直接加入させる必要があるかどうかを検出できます。

2 [企業により追加のセットアップが要求されています] 画面が表示され、ユーザーが [続行] をクリックすると、ユーザーが Google Play Store の AirWatch Agent アプリケーションにリダイレクトされます。

図 5-9. AirWatch Agent アプリケーションのダウンロード リクエスト

3 ユーザーが AirWatch Agent アプリケーションをダウンロードします。

注: AirWatch Agent アプリケーションがすでにデバイスにインストールされている場合、Workspace ONE は自動的にアプリケーションを起動します。ユーザーはアプリケーション ストアにリダイレクトされません。

Workspace ONE のために入力された認証の詳細は AirWatch Agent アプリケーションに渡されたため、ユーザーはこの情報を再入力しません。

AirWatch Agent アプリケーションが起動されます。AirWatch Agent へのデバイス加入中に、ユーザーは所有形態のタイプを選択し、デバイスのアセット番号を（設定されている場合）入力します。

4 [Agent が電話通話を実行および管理することを許可します] が表示されたら、ユーザーは [許可] をクリックします。

AirWatch Agent は加入を検証し、ユーザーを認証して、このデバイスの AirWatch に権限を付与します。

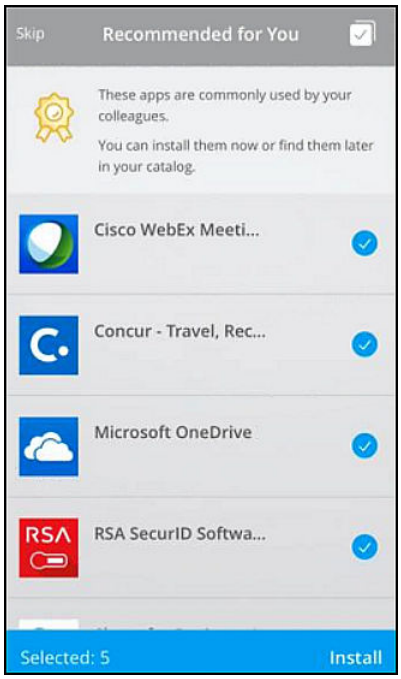
5 [デバイス管理アプリケーションをアクティブ化しますか?] 画面が表示されたら、ユーザーは [このデバイス管理アプリケーションをアクティブ化] をクリックします。

図 5-10. デバイス管理アプリケーションのアクティブ化

6 ユーザーは、さまざまなデバイス機能にアクセスするための権限を付与するように求められます。

これで、デバイスが Workspace ONE UEM に加入し、Workspace ONE が起動します。[推奨されるアプリケーション] 画面が表示されます。

図 5-11. [推奨されるアプリケーション] 画面



7　ユーザーは、インストールするアプリケーションを選択することも、この手順をスキップすることもできます。

これで、デバイスは Workspace ONE UEM MDM によって管理されます。推奨されるアプリケーションをインストールするように選択すると、ユーザーはそれらのアプリケーションの通知を受信するようになります。

Apple デバイス登録プログラムの統合をサポートする Workspace ONE の適用

6

Apple Device Enrollment Program (DEP) は、お客様がユーザー認証に SAML を使用するシナリオをサポートしていません。ただし、Workspace ONE には、このようなユースケースをサポートする独自の方法が実装されています。

Workspace ONE UEM デバイスのステージングを通じて、管理者はデバイスを複数デバイスのステージング ユーザーに割り当て、Workspace ONE アプリケーションにログインするときに Workspace ONE でデバイスに適切なユーザーを再度割り当てることができます。

ステージング ユーザー加入の一部として、Workspace ONE アプリケーションをデバイスにインストールする必要があります。ユーザーが初めて Workspace ONE にログインする場合、Workspace ONE は設定された SAML プロバイダを介してユーザーを認証します。ユーザーが認証されると、デバイスの所有形態がマルチデバイスのステージング ユーザーから認証されたディレクトリ ユーザーに切り替えられます。

前提条件

ユーザーが Workspace ONE アプリケーションにログインするときに、ディレクトリ ユーザーが Workspace ONE UEM に存在している必要があります。必要に応じて CSV を使用してユーザーを事前に一括でロードすることも、次の API を適用してユーザーを生成することもできます。

注: [セキュリティ タイプ] の値はディレクトリと同一である必要があります。

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

Workspace ONE で DEP 統合をサポートするためのフロー

Workspace ONE を使用して Apple デバイス登録プログラムのサポートを実装するには、以下のタスクを実行する必要があります。

- iOS デバイスに Workspace ONE アプリケーションをインストールします。
- Workspace ONE UEM コンソールにおける次のステージング構成に、ステージング ユーザーが存在することを確認します。
  a [アカウント] > [ユーザー] > [リスト ビュー] に移動して、編集するデバイス ステージングを有効にするユーザー アカウントを選択します。
  b [ユーザを追加/編集] ページで、[高度な設定] タブを選択します。[ステージング] セクションにスクロールし、[デバイスのステージング] と [マルチユーザー デバイス] を有効にします。

図 6-1. Workspace ONE UEM でのマルチユーザー デバイスの設定

- Apple DEP ポータルのステージング ユーザーにデバイスを割り当て、デバイスをエンド ユーザーに提供します。

  Apple デバイス登録プログラムの詳細については、Apple デバイス登録 ガイドを参照してください。

統合の仕組み

ユーザーが初めてデバイスをオンにする場合、デバイスが加入させられて、マルチデバイスのステージング ユーザーに割り当てられます。ユーザーが、使用可能な Workspace ONE アプリケーションをホーム画面で起動してログインします。Workspace ONE は設定された SAML プロバイダを使用してユーザーを認証します。

ユーザーが認証されると、デバイスの所有形態がマルチデバイスのステージング ユーザーから認証されたディレクトリ ユーザーに切り替えられます。認証されたユーザーに割り当てられたアプリケーション、プロファイル、およびリソースがデバイスにプッシュされます。

注: デバイスの組織グループは変更されません。この機能は、Workspace ONE UEM コンソールの [登録設定] セクションにあるユーザー グループ マッピング、またはドロップダウン メニューに基づく手動のユーザー選択をサポートしていません。

VMware Workspace ONE モバイル アプリケーションの展開

7

VMware Workspace ONE アプリケーションがモバイル デバイスにインストールされているとき、ユーザーは使用が許可されているリソースにアクセスできます。

ユーザーは、自分の ID が VMware Identity Manager で管理されている場合は、シングル サインオン機能を使用して、資格が付与されたアプリケーションにアクセスできます。ユーザーは、他のアプリケーションを追加できるアプリケーション カタログにもアクセスできます。

Workspace ONE アプリケーションのインターフェイスは、スマートフォン、タブレット、またはデスクトップ コンピュータで同じように操作でき、類似するオプションを利用できます。

デバイスがモバイル デバイス管理 (MDM) に登録されている場合、Workspace ONE アプリケーションを管理対象アプリケーションとしてプッシュすることができます。

この章には、次のトピックが含まれています。

- Workspace ONE のためのパブリック アプリケーションおよび社内アプリケーション用の Workspace ONE UEM でのデバイス管理オプション
- アプリケーションへのアクセスの管理
- Workspace ONE カタログにアクセスするための利用条件の要求
- Workspace ONE アプリケーションの入手と配布
- 自動検出用のメール ドメインの登録
- セッション認証設定
- 複数の Workspace ONE UEM 組織グループを設定するための展開戦略

Workspace ONE のためのパブリック アプリケーションおよび社内アプリケーション用の Workspace ONE UEM でのデバイス管理オプション

デバイス管理ステータスに基づいて、パブリック アプリケーションおよび社内アプリケーションを展開するように構成できます。任意のデバイスが、オープン アクセスとして構成されているアプリケーションにアクセスできます。ワークスペース サービスまたはエージェントの登録を介して有効にすることで、権限が付与されたデバイスのみが、管理されたアクセス用に構成されたアプリケーションにアクセスできます。

この表で、管理対象および非管理対象の両方のシナリオの機能について説明します。

アクセスの種類	機能	説明	推奨される使用方法
オープン アクセス（非管理対象）	■ Web、Horizon、および Citrix リソース用のセルフ サービス アプリケーション カタログ ■ シングル サインオン (SSO) での Web/仮想の起動 ■ Touch ID/PIN アプリケーション保護 ■ デバイス ジェイルブレイク検出 ■ 認証ポリシーおよびデバイスのブロックを含む、VMware Identity Manager の条件付きアクセスのサポート ■ ネイティブ アプリケーション アクセス ■ 社内アプリケーションおよび SDK アプリケーションの配布	ユーザーは、自分のデバイスにアクセスするための管理者権限を与えなくても、自分のデバイス上のリソースにアクセスします。 オープン アクセスを持つアプリケーションは、アプリケーションの管理対象ステータスに関係なく、デバイスから使用できます。ネイティブ アプリケーションがオープン アクセスに設定されているときは、管理者がそれらをシステム的に削除することはできません。	■ 昇格したセキュリティ権限なしで、ログイン時にすぐにエンドユーザーにアプリケーションへのアクセスを提供します。 ■ アプリケーションをインストールする必要なく、アプリケーションの使用を推奨します。ユーザーは自分がそうしたいときに自分のデバイスにアプリケーションをインストールできます。 ■ アプリケーションには、企業の機密データは含めず、保護された社内リソースにアクセスしないようにします。 ■ Workspace ONE UEM MDM プロファイルなしで、補助の担当者にアプリケーションを配布する目的で使用します。
管理対象アクセス	■ Web、Horizon、および Citrix リソース用のセルフ サービス アプリケーション カタログ ■ シングル サインオン (SSO) での Web/仮想の起動 ■ Touch ID/PIN アプリケーション保護 ■ デバイス ジェイルブレイク検出 ■ 認証ポリシーおよびデバイスのブロックを含む、VMware Identity Manager の条件付きアクセスのサポート ■ ネイティブ アプリケーションの管理対象およびダイレクトのインストール ■ 内部アプリケーションおよび SDK アプリケーションの管理 ■ アプリケーション構成のサポート ■ アプリごとの VPN ■ SAML 対応のネイティブ アプリケーション用ワンタッチ SSO ■ デバイス プロファイル ■ Workspace ONE UEM コンプライアンス エンジン	ユーザーは、自分のデバイスにアクセスするための管理者権限を与えるため、自分のデバイスに管理プロファイルをインストールします。 管理対象アクセスを持つアプリケーションは、Workspace ONE UEM が管理するデバイスから使用できます。 Workspace ONE UEM がデバイスを管理していない場合は、Workspace ONE はデバイス上のユーザーに Workspace ONE UEM への登録を求めます。デバイスが登録されている場合、ユーザーはデバイスを使用して、Workspace ONE を介してアプリケーションにアクセスできます。	■ ユーザーが組織を離れた、またはデバイスを失くしたときに、デバイスから社内機密データを削除する目的で使用します。 ■ アプリケーションがイントラネットにアクセスするときに、認証し、内部バックエンド リソースと安全に通信するためにアプリケーション トンネリングを必要とします。 ■ アプリケーションのシングル サインオンを有効にします。 ■ アプリケーションのユーザーの導入とインストールのステータスを追跡します。 ■ 登録時に自動的にアプリケーションを展開します。

社内アプリケーション用の管理対象アクセス オプションを構成する場所、または Workspace ONE を介して展開のためにパブリック アプリケーションを追加する方法については、『Workspace ONE UEM モバイル アプリケーション管理ガイド』を参照してください。

オープンおよび管理対象アクセスのサポートされているプラットフォーム

プラットフォームに基づく社内およびパブリック アプリケーション用のアクセスの種類を構成します。

	管理対象アクセス	オープン アクセス
社内アプリケーション		
Android	X	X
iOS	X	X
Windows 10 デスクトップ	X	-
Windows 10 電話	X	-
パブリック アプリケーション		
Android	X	X
iOS	X	X
Windows 10 デスクトップ	-	X
Windows 10 電話	-	X

アプリケーションへのアクセスの管理

1 人のユーザーは、ネイティブ アプリケーションへのオープンまたは管理対象のアクセスの混合に資格が付与される場合があります。このアダプティブ管理方法によって、管理を必要とせずに、エンド ユーザーにオープン アクセス アプリケーションの使用を許可できます。ユーザーが管理を必要とするネイティブ アプリケーションを要求すると、アダプティブ管理は、そのネイティブ アプリケーションの管理に必要な追加のセキュリティとコントロールを提供します。

アプリケーションが管理対象の場合、ユーザーは Workspace サービスを有効にして、管理対象アプリケーションをインストールして使用する必要があります。Workspace ONE UEM コンソールでアプリケーションをアップロードすると、そのアプリケーションの構成に基づいて、オープンまたは管理対象のいずれかとしてアクセスの状態が表示されます。たとえば、[アプリケーション構成の送信]オプションが選択されている場合、アプリケーションは管理を要求するように設定されます。

カタログで、管理が必要なアプリケーションを未管理状態で表示すると、星印のアイコンが表示されます。アプリケーションを使用するには、ユーザーはアダプティブ管理プロセスを介して Workspace サービスを有効にする必要があります。ユーザーが、星印のアイコンが表示されたアプリケーションをダウンロードしようとすると、ワークスペース サービスを有効にすることを確認するメッセージがユーザーに表示されます。プライバシー通知リンクをクリックして、アダプティブ管理プロセスの続行を選択した場合の個人情報に対するプライバシーの影響を確認することができます。プライバシー通知は、登録先の Workspace ONE UEM 環境から自動的に設定をプルします。プライバシー設定情報を確認した後、ユーザーは Workspace サービスの有効化に進むか、引き返して、デバイス上で Workspace ONE アプリケーションを非管理対象として使用し続けるかのいずれかを選択できます。ユーザーが Workspace サービスを有効にするときに、すべての管理対象アプリケーションから星印のアイコンが消えます。

管理対象デバイスでのアクセスの削除

ユーザーは、アカウントの削除オプションを通じて、管理対象デバイス上で Workspace ONE アプリケーションを無効にできます。アカウントを削除すると、デバイスで企業情報ワイプが実行され、これにより企業アクセスが削除され、ユーザーはログイン画面に戻ります。管理者は、企業情報ワイプを Workspace ONE UEM コンソールから実行し、Workspace ONE サービスを無効にできます。

管理対象デバイスでアカウントの削除アクションを実行すると、Workspace ONE アプリケーションを介して付与されたアクセス権限が取り消され、Workspace ONE UEM からデバイスが登録解除されます。管理が必要なアプリケーションはデバイスから削除され、Boxer、Browser、Content Locker などの Workspace ONE UEM の生産性向上のためのアプリケーションへのアクセス権限が失効します。

Workspace ONE カタログにアクセスするための利用条件の要求

組織自身の Workspace ONE 利用条件を作成し、エンド ユーザーが Workspace ONE を使用する前にこの利用条件に同意するようにすることができます。

ユーザーが Workspace ONE にログインした後、利用条件が表示されます。ユーザーは、Workspace ONE カタログに進む前に利用条件に同意する必要があります。

利用条件機能には、次の設定オプションが含まれます。

- 既存の利用条件のバージョンの作成。
- 利用条件の編集。
- デバイス タイプに基づいて表示できる複数の利用条件の作成。
- 利用条件の言語固有のコピーの作成。

設定する利用条件ポリシーは、[ID とアクセス管理] タブにリストされます。利用条件ポリシーを編集して既存のポリシーを修正したり、ポリシーの新しいバージョンを作成することができます。新しいバージョンの利用条件を追加すると、既存の利用条件が置き換えられます。ポリシーを編集しても、利用条件は変更されません。

利用条件ページでは、利用条件に同意したユーザーまたは拒否したユーザーの数を表示できます。同意した数または拒否した数をクリックすると、該当のユーザーとその状態のリストが表示されます。

利用条件の設定と有効化

[利用条件] ページに利用条件ポリシーを追加し、使用パラメータを設定します。利用条件が追加されたら、[利用条件] オプションを有効にします。ユーザーが Workspace ONE にログインするときは、カタログにアクセスするために利用条件に同意する必要があります。

前提条件

利用条件ポリシーのテキストは、利用条件の内容テキスト ボックスにコピーして貼り付けるため HTML で作成されています。利用条件は、英語、ドイツ語、スペイン語、フランス語、イタリア語、オランダ語で追加できます。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [利用条件] を選択します。

2 [利用条件を追加] をクリックします。

3 利用条件のわかりやすい名前を入力します。

4 利用条件ポリシーがすべてのユーザーを対象にする場合は、[任意] を選択します。デバイス タイプ別に利用条件ポリシーを使用するには、[選択したデバイスのプラットフォーム] を選択し、この利用条件ポリシーを表示するデバイス タイプを選択します。

5 デフォルトでは、最初に表示される利用条件の言語は、ブラウザの言語設定に基づいて選択されます。テキスト ボックスにデフォルトの言語の利用条件の内容を入力します。

6 [保存] をクリックします。

利用条件ポリシーを別の言語で追加するには、[言語を追加] をクリックして別の言語を選択します。利用条件の内容テキスト ボックスが更新され、テキスト ボックスにテキストを追加できるようになります。

言語名をドラッグして、利用条件が表示される順序を指定できます。

7 利用条件の使用を開始するには、表示されるページで [利用条件を有効にする] をクリックします。

次のステップ

利用条件に対して特定のデバイス タイプを選択した場合は、そのデバイス タイプの追加の利用条件を作成することができます。

利用条件への同意状況の表示

[ID とアクセス管理] > [利用条件] ページにリストされた利用条件ポリシーには、ポリシーに同意したユーザーまたは拒否したユーザーの数が表示されます。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [利用条件] を選択します。

2 [同意/拒否] 列で、左側の「同意」の数または右側の「拒否」の数をクリックします。

ステータスのページには、実行したアクション（同意または拒否、ユーザー名付き）、デバイス ID、表示したポリシーのバージョン、使用したプラットフォーム、および日付が表示されます。

3 ビューを閉じるには、[キャンセル] をクリックします。

Workspace ONE アプリケーションの入手と配布

ユーザーがデバイス アプリ ストアから VMware Workspace ONE アプリケーションをダウンロードするか、管理者が Workspace ONE UEM を構成して Workspace ONE アプリケーションを管理対象アプリケーションとしてデバイスにプッシュすることができます。

Workspace ONE アプリケーションを Workspace ONE UEM コンソールから組織内の特定のグループおよびユーザーに展開します。ユーザーがデバイス上で Workspace ONE アプリケーションにログインした後、資格付与された Web および SaaS アプリケーションにアクセスすることができます。

次の手順では、Workspace ONE UEM コンソールから Workspace ONE モバイル アプリケーションを管理対象アプリケーションとしてプッシュします。アプリケーションをプッシュするために、Workspace ONE「はじめに」ウィザードを実行することもできます。

注: Workspace ONE UEM で管理対象アプリケーションを構成する方法の詳細については、リソース ポータル (https://resources.air-watch.com) から入手可能な『VMware Workspace ONE UEM モバイル アプリケーション管理 (MAM) ガイド』を参照してください。

前提条件

Workspace ONE モバイル アプリケーションを Workspace ONE UEM コンソールからプッシュするよう計画している場合、アプリケーションの使用資格が付与されたエンド ユーザーのスマート グループを準備します。

手順

1 Workspace ONE UEM コンソールで、[アプリケーションとブック] - [アプリケーション] > [リスト ビュー] - [公開] の順に移動して、[アプリケーションを追加] を選択します。

2 プラットフォームを iOS、Android、または Windows から選択します。

3 [アプリ ストアを検索] を選択し、[名前] テキスト ボックスに、アプリケーション ストアで VMware Workspace ONE を検索するためのキーワードとして「**Workspace ONE**」を入力します。

4 [次へ] を選択し、[選択] を使用して、アプリケーション ストアの検索ページから Workspace ONE アプリケーションをアップロードします。

5 次のタブ設定で、Workspace ONE ユーザーの割り当てとデプロイのオプションを構成します。

タブ	説明
情報	サポートされるデバイス モデル、評価、およびカテゴリなどに関する情報を入力および表示します。
割り当て	Workspace ONE モバイル アプリケーションを、デバイス上でアプリケーションを使用することができるエンド ユーザーのスマート グループに割り当てます。
展開	該当する場合は、可用性と高度なエンタープライズ モビリティ管理 (EMM) 機能を構成します。 管理対象アプリケーションを自動的に構成するには、[アプリケーション構成を送信] を有効にして、エンタープライズ用アプリケーション構成 (ACE) のキー値のペアを入力します。「エンタープライズ キーと値のペアに関する Workspace ONE UEM アプリケーションの構成」を参照してください。
利用条件	(オプション) Workspace ONE アプリケーションを使用するための [利用条件] を有効にします。

6 [保存と公開] を選択して、ユーザーがアプリケーションを利用できるようにします。

サポートされている各プラットフォームでこれらの手順を完了します。

エンタープライズ キーと値のペアに関する Workspace ONE UEM アプリケーションの構成

Workspace ONE UEM で管理対象アプリケーションとして Workspace ONE アプリケーションを展開し、[アプリケーション構成の送信] を有効にして、Workspace ONE UEM コンソールから Workspace ONE アプリケーションをプッシュします。これにより、ユーザーが Workspace ONE アプリケーションをインストールおよび起動する際に適用される、Workspace ONE 設定を事前に構成できます。

Workspace ONE アプリケーションが管理対象のモバイル アプリケーションとして Workspace ONE UEM コンソールにアップロードされるときに、VMware Workspace ONE Server の URL、デバイスの UID 値、および Android デバイスの証明書認証の要件を構成できます。

表 7-1. Workspace ONE UEM コンソールの Workspace ONE 管理対象デバイスの構成オプション

プラットフォーム	構成キー	値のタイプ	構成値	説明
すべて	`AppServiceHost`	文字列	<**VMware Workspace ONE Server の URL**>	デバイスで VMware Workspace ONE のサーバ URL を構成します。
iOS	`deviceUDID`	文字列	**{DeviceUid}** デバイス UID 値を入力します。 [ルックアップ値の挿入] 機能は使用しないでください。	VMware Identity Manager 環境への認証に使用されるデバイスを追跡します。

表 7-1. Workspace ONE UEM コンソールの Workspace ONE 管理対象デバイスの構成オプション (続き)

プラットフォーム	構成キー	値のタイプ	構成値	説明
iOS	`SkipDiscoveryScreen`	Boolean	**`true`**	Workspace ONE アプリケーションのバージョン 3.1 以降では、SkipDiscoveryScreen 構成キーが構成できます。 True に設定すると、Workspace ONE は、メール アドレス/サーバの URL の画面を通過しようとします。`AppServiceHost` 構成キーと一緒に使用した場合、ユーザーは認証画面にすぐに移動します。モバイル SSO も使用されている場合、管理者は、エンド ユーザーが Workspace ONE を起動することで Workspace ONE アプリケーションのロードが即時に開始されるようにし、シームレスな経験を提供できます。
Android および iOS	`RemoveAccountSignOut`	整数	0 - [アカウントの削除] オプションを表示 1 - [アカウントの削除] オプションを表示しない 値が設定されていない場合は、[アカウントの削除] オプションが表示されます。	値を 1 に設定すると、[アカウントの削除] オプションはユーザーの [Workspace ONE 設定] ページに表示されません。ユーザーは、自分のデバイスから Workspace ONE アカウントを削除できません。 この値が 0 に設定されている場合、または値が設定されていない場合は、[アカウントの削除] オプションが表示されます。ユーザーが [アカウントの削除] をクリックすると、Workspace ONE UEM はデバイスのエンタープライズ ワイプを実行し、Workspace ONE UEM からデバイスを登録解除します。

自動検出用のメール ドメインの登録

エンド ユーザーが Workspace ONE アプリケーションを介してアプリケーション ポータルに簡単にアクセスできるように、自動検出サービスにメール ドメインを登録できます。エンド ユーザーは、組織の URL の代わりにメール アドレスを入力します。

組織のメール ドメインが自動検出に登録されている場合、エンド ユーザーはログイン ページにメール アドレスだけを入力してアプリケーション ポータルにアクセスできます。たとえば、**username@myco.com** と入力します。

自動検出を使用しない場合、エンド ユーザーは初めて Workspace One アプリケーションを開くときに、完全な組織 URL を指定する必要があります。たとえば、**myco.vmwareidentity.com** と入力します。

VMware Identity Manager での自動検出の設定

ドメインを登録するには、VMware Identity Manager コンソールの [自動検出] ページでメール ドメインとメール アドレスを入力します。

アクティベーショントークンが記載されたメール メッセージがドメインのメール アドレスに送信されます。ドメインの登録を有効にするには、[自動検出] ページでトークンを入力し、登録したドメインが自分のドメインであることを確認します。

注: オンプレミスに展開されている VMware Identity Manager の自動検出を設定するには、ローカル管理者として VMware Identity Manager コンソールにログインする必要があります。Workspace ONE UEM Web サイト (https://secure.air-watch.com/register) で作成した Workspace ONE UEM の ID とパスワードを入力します。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [自動検出] の順にクリックします。

2 (オンプレミスの展開環境のみ)。Workspace ONE UEM の自動検出 URL を構成します。

オプション	説明
自動検出 URL	https://discovery.awmdm.com として URL を入力します。
AirWatch ID	Workspace ONE UEM で登録したメール アドレスを入力して、Web サイトにログインします。
パスワード	Workspace ONE UEM アカウントに関連付けられているパスワードを入力します。

3 [メール ドメイン] テキスト ボックスに、登録する組織のメール ドメインを入力します。

4 [メール アドレスの確認] テキスト ボックスに、そのメール ドメインの、検証トークンを受信するメール アドレスを入力します。

5 [OK] をクリックします。

このメール ドメインの登録ステータスが [保留] とマークされます。保留中のメール ドメインは一度に 1 つしか追加することができません。

6 E メールに移動し、メッセージに記載されているアクティベーション トークンをコピーします。

7 [ID とアクセス管理] - [自動検出] ページに戻り、[アクティベーション トークン] テキスト ボックスにトークンを貼り付けます。

8 [検証] をクリックしてドメインを登録します。

メール ドメインが登録され、[自動検出] ページの登録済みのメール ドメインのリストに追加されます。

これで、エンド ユーザーは Workspace ONE アプリケーションでメール アドレスを入力してアプリケーション ポータルにアクセスできるようになりました。

次のステップ

複数のメール ドメインがある場合、別のメール ドメインを追加して登録します。

セッション認証設定

VMware Identity Manager サービスには、VMware Identity Manager リソースへのユーザー アクセスを制御するデフォルトのアクセス ポリシーが含まれます。

ポリシー ルールで構成される認証セッションの長さは、ユーザーがアプリケーション ランチャ ページ アクセスするか、または特定の Web アプリケーションを起動した前回の認証イベント以来の最長時間を決定します。デフォルト設定は、8 時間です。ユーザーが認証した後の 8 時間は、Web アプリケーションを起動でき、別の認証イベントを開始すると、この時間が延長されます。

VMware Identity Manager 管理コンソールの [ID とアクセス管理] タブから [管理] > [ポリシー] にアクセスして、デフォルトのポリシーを編集して、セッションの長さを変更できます。『VMware Identity Manager 管理ガイド』の「アクセス ポリシーの管理」を参照してください。

Workspace ONE UEM で管理されているデバイスのコンプライアンス チェックの有効化

ユーザーがデバイスを登録する場合、コンプライアンスを評価するために使用されるデータを含むサンプルがスケジュールに従って送信されます。このサンプル データの評価により、デバイスが Workspace ONE UEM (UEM) コンソールの管理者によって設定されたコンプライアンス ルールを遵守していることを確認できます。デバイスがコンプライアンス ルールを遵守していない場合、UEM コンソールで構成されたアクションが実行されます。

VMware Identity Manager サービスには、ユーザーがデバイスからログインする際に、Workspace ONE UEM サーバを確認してデバイスのコンプライアンスの状態を確認するよう構成できるアクセス ポリシー オプションが組み込まれています。デバイスがコンプライアンス ルールに遵守されなくなった場合、コンプライアンス チェックにより、ユーザーがアプリケーションにログインしたり、Workspace ONE ポータルに対してシングル サインオンを使用したりすることを確実に防ぐことができます。デバイスで再度コンプライアンス ルールが遵守されるようになったら、再びログインできるようになります。

デバイスが危険にさらされている場合、Workspace ONE アプリケーションが自動的にログアウトし、アプリケーションへのアクセスをブロックします。デバイスがアダプティブ管理によって登録された場合、UEM コンソールを介して発行されたエンタープライズ WIPE コマンドにより、デバイスの登録が解除され、管理対象アプリケーションがデバイスから削除されます。管理対象外のアプリケーションは削除されません。

Workspace ONE UEM コンプライアンス ポリシーの詳細については、「VMware Workspace ONE UEM ドキュメント」ページの『VMware Workspace ONE UEM Mobile Device Management Guide』を参照してください。

複数の Workspace ONE UEM 組織グループを設定するための展開戦略

Workspace ONE UEM は組織グループを使用してユーザーを識別し、アクセス許可を確立します。
Workspace ONE UEM が VMware Identity Manager と連携すると、管理および登録ユーザーの REST API キーは、顧客と呼ばれる Workspace ONE UEM 組織グループ タイプで構成されます。

ユーザーがデバイスから Workspace ONE にログインすると、VMware Identity Manager 内でデバイスの登録のイベントがトリガされます。ユーザーおよびデバイスの組み合わせに資格が付与された任意のアプリケーションを取得するための要求が Workspace ONE UEM に送信されます。Workspace ONE UEM 内でユーザーを特定し、適切な組織グループにデバイスを配置するための要求が REST API を使用して送信されます。

組織グループを管理するには、VMware Identity Manager で 2 つのオプションを構成できます。

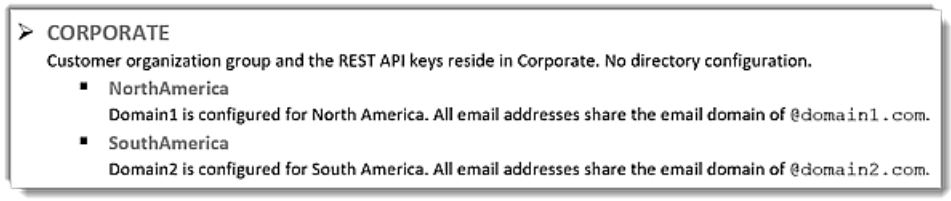
- Workspace ONE UEM 自動検出を有効にします。
- Workspace ONE UEM 組織グループを VMware Identity Manager サービス内のドメインにマップします。

これらの 2 つのオプションのどちらも構成されていない場合、Workspace ONE は REST API キーが作成された組織グループでユーザーを特定しようとします。これは、顧客グループです。

Workspace ONE UEM 自動検出の使用

顧客組織グループへの子グループで 1 つのディレクトリが構成されるとき、または一意の E メール ドメインを使用して顧客グループの下に複数のディレクトリが構成されるときに、自動検出を設定します。

図 7-1. 例 1



例 1 では、自動検出のために組織の E メール ドメインが登録されます。ユーザーは、Workspace ONE ログイン ページに自分のメール アドレスのみを入力します。

この例では、NorthAmerica ドメインのユーザーが Workspace ONE にログインするときに、完全なメール アドレスを user1@domain1.com として入力します。アプリケーションはドメインを検索し、NorthAmerica 組織グループ内にユーザーが存在するか、またはディレクトリ呼び出しを使用してユーザーを作成できるかを確認します。デバイスを登録できます。

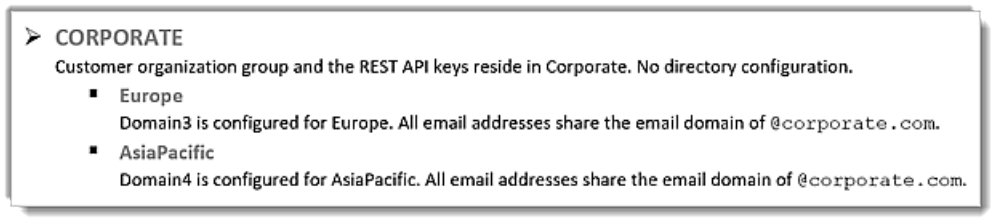
VMware Identity Manager ドメインへの Workspace ONE UEM 組織グループ マッピングの使用

同じ E メール ドメインを使用して複数のディレクトリが構成されている場合、VMware Identity Manager サービスと Workspace ONE UEM 組織グループのマッピングを構成します。VMware Identity Manager コンソールの AirWatch 構成ページで [ドメインを複数の組織グループにマップ] を有効にします。

[ドメインを複数の組織グループにマップ] オプションを有効にすると、VMware Identity Manager で構成されているドメインを Workspace ONE UEM 組織グループ ID にマッピングできます。管理者 REST API キーも要求されます。

例 2 では、2 つのドメインが別々の組織グループにマッピングされます。管理者 REST API キーが要求されます。同じ管理 REST API キーが両方の組織グループ ID に使用されます。

図 7-2. 例 2



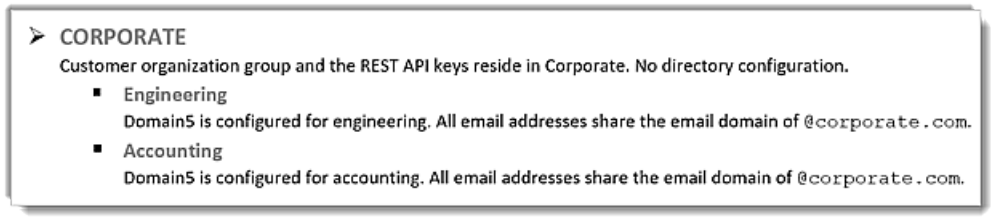
VMware Identity Manager コンソールの AirWatch 構成 ページで、各ドメインの固有の Workspace ONE UEM 組織グループ ID を構成します。

図 7-3. 例 2 組織グループの構成

この構成では、ユーザーが自分のデバイスから Workspace ONE にログインすると、デバイス登録要求は組織グループ Europe 内の Domain3 のユーザーと、組織グループ AsiaPacific 内の Domain4 のユーザーを見つけようとします。

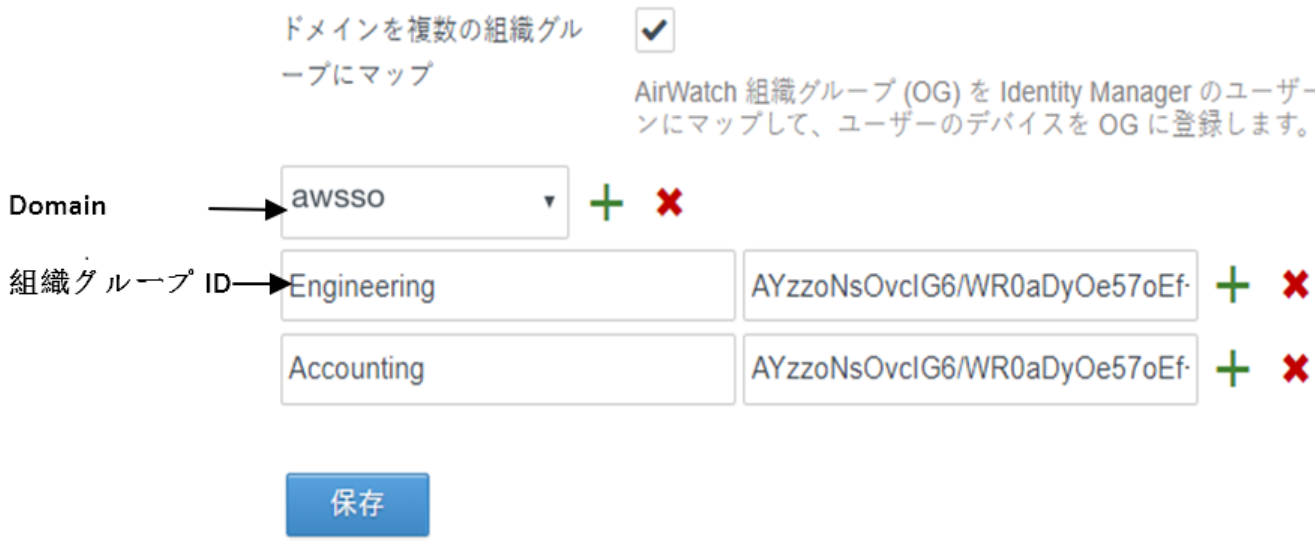
例 3 では、1 つのドメインが複数の Workspace ONE UEM 組織グループにマッピングされます。両方のディレクトリが E メール ドメインを共有します。ドメインは、同じ Workspace ONE UEM 組織グループをポイントします。

図 7-4. 例 3



この構成では、ユーザーが Workspace ONE にログインすると、アプリケーションは、どのグループに登録するかの選択をユーザーに要求します。この例では、ユーザーは Engineering または Accounting のいずれかを選択できます。

図 7-5. ディレクトリが同じドメインを共有する組織グループ



正しい組織グループへのデバイスの配置

ユーザー レコードが正常に配置されると、デバイスが適切な組織グループに追加されます。Workspace ONE UEM 登録設定の [グループ ID 割り当てモード] によって、デバイスを配置する組織グループが決まります。この設定は、Workspace ONE UEM Console の [システム設定] > [デバイスとユーザー] > [全般] > [加入] > [グループ化] ページで行います。

図 7-6. デバイスの Workspace ONE UEM グループの登録

例 4 では、すべてのユーザーは、Corporate 組織グループ レベルにあります。

図 7-7. 例 4

デバイスの配置は、Corporate 組織グループでのグループ ID 割り当てモード用に選択した構成に依存します。

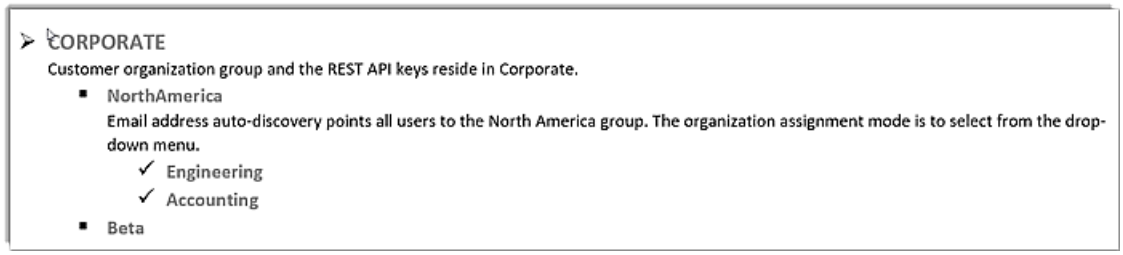
- [デフォルト] が選択されている場合、デバイスはユーザーが配置されているのと同じグループに配置されます。例 4 では、デバイスは Corporate グループに配置されます。
- [ユーザーがグループ ID を選択するようプロンプト表示する] が選択されている場合、自分のデバイスを登録するグループを選択するようユーザーに求められます。例 4 では、Workspace ONE アプリケーション内に Engineering と Accounting がオプションとして設けられたドロップダウン メニューがユーザーに表示されます。
- [ユーザー グループに基づき自動選択] が選択されている場合、デバイスは、ユーザー グループ割り当てと、Workspace ONE UEM コンソールの対応するマッピングに基づいて、Engineering または Accounting のいずれかに配置されます。

非表示グループの概念について

例 4 では、ユーザーに登録元の組織グループの選択が要求されるときに、ユーザーは Workspace ONE アプリケーションから提供されたリストに含まれていないグループ ID の値も入力できます。これが非表示グループの概念です。

例 5 では、Corporate 組織グループ構造に North America と Beta が Corporate の下のグループとして構成されています。

図 7-8. 例 5



例 5 では、ユーザーは Workspace ONE にメール アドレスを入力します。認証後、ユーザーに選択肢として Engineering と Accounting が表示されたリストが示されます。Beta は表示されるオプションではありません。ユーザーが組織グループ ID を把握している場合、グループの選択テキスト ボックスに手動で Beta を入力することで、自分のデバイスを Beta に正常に登録できます。

Workspace ONE ポータルでの作業

8

Workspace ONE アプリケーションがデバイスにインストールされると、ユーザーは Workspace ONE にログインして、ユーザーの組織が有効にしているアプリケーションのカタログに安全にアクセスできるようになります。アプリケーションにシングル サインオンを構成すると、アプリケーションを起動するときにユーザーはログイン認証情報を再度入力する必要がありません。

Workspace ONE のユーザー インターフェイスは、スマートフォン、タブレット、およびデスクトップで同じように使用できます。Workspace ONE の [カタログ] ページには、Workspace ONE にプッシュされたリソースが表示されます。ユーザーは、タップまたはクリックし、アプリケーションを検索、追加、ブックマーク、および更新できます。アプリケーションを右クリックして [ブックマーク済み] ページから削除でき、[カタログ] ページに移動して、使用資格が付与されたリソースを追加できます。

この章には、次のトピックが含まれています。

- Workspace ONE 内でのアプリケーションの操作
- Workspace ONE アプリケーションのパスコードの設定
- iOS デバイスでのアプリ レベルのパスコード
- ネイティブ アプリケーションの追加
- ユーザー認証のための VMware Verify の使用
- Workspace ONE ユーザーへのアラートの送信
- Android デバイス版 Workspace ONE の操作

Workspace ONE 内でのアプリケーションの操作

Workspace ONE ユーザー ポータルは、[カタログ] タブと [ブックマーク] タブで構成されています。ユーザーが最初に Workspace ONE ポータルにログインするとき、[ブックマーク] タブが空の場合は [カタログ] タブが表示されます。

最初の起動後に、ユーザーは前回アクセスしたタブに直接移動します。ユーザーが [カタログ] タブから起動することを好む場合、カタログ ビューを使用できます。

Workspace ONE ポータルでは [カタログ] タブまたは [ブックマーク] タブのいずれかを非表示にし、ユーザー固有の要件に合わせて使いやすくすることができます。ポータルの設定は、VMware Identity Manager コンソールの [カタログ] > [設定] > [ユーザー ポータルの設定] ページで変更できます。

図 8-1. [ブックマーク] ページの初期ビュー

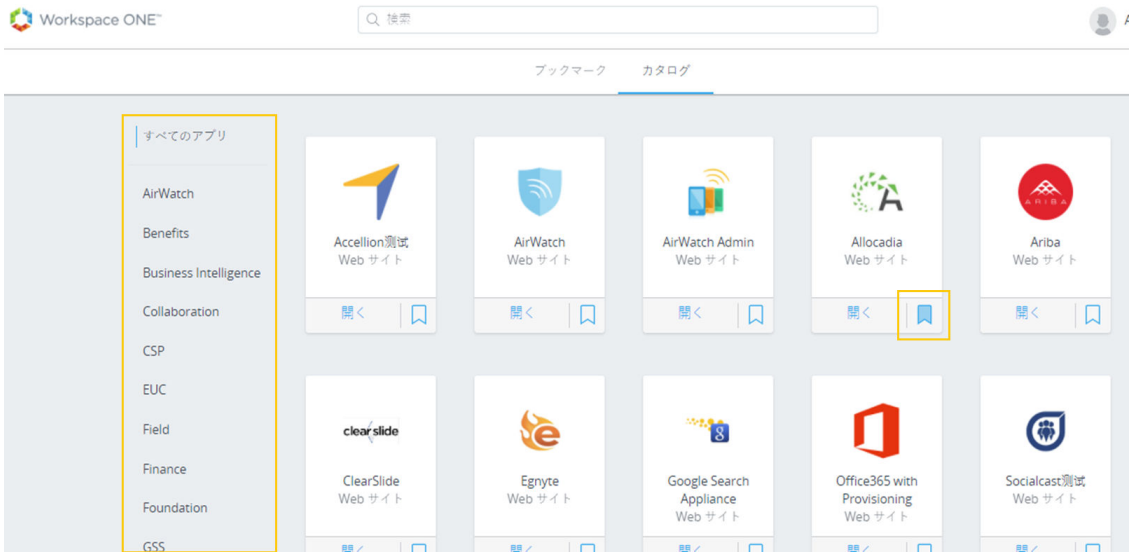
カタログから、ユーザーは自分に使用資格が付与されている Web、モバイル、および仮想アプリケーションをインストールできます。Web アプリケーションおよび仮想アプリケーションは、Workspace ONE アプリケーションのカタログ ページまたはブックマーク ページから直接開くことができます。

iOS や Android などのネイティブ アプリケーションは、Workspace ONE ページからブックマークまたは起動することができません。これらのアプリケーションは、iOS または Android のスプリングボードから起動されます。

[カタログ] ページでは、アプリケーションを論理カテゴリに整理することで、必要なリソースをユーザーが簡単に特定することができます。デフォルトでは、「推奨」というカテゴリが表示されます。アプリケーションを「推奨」に分類すると、[ブックマーク タブに推奨されるアプリケーションを表示] を有効にして、[ブックマーク] ページに推奨アプリケーションを自動入力することができます。

この構成によって、Workspace ONE ポータルに最初にログインしたときに、ユーザーは推奨アプリケーションに迅速にアクセスできます。

図 8-2. Workspace ONE の [カタログ] ページ



注: モバイル アプリケーションは、デスクトップ ブラウザからは使用できません。

ユーザーは、次のように Web アプリケーションを起動できます。

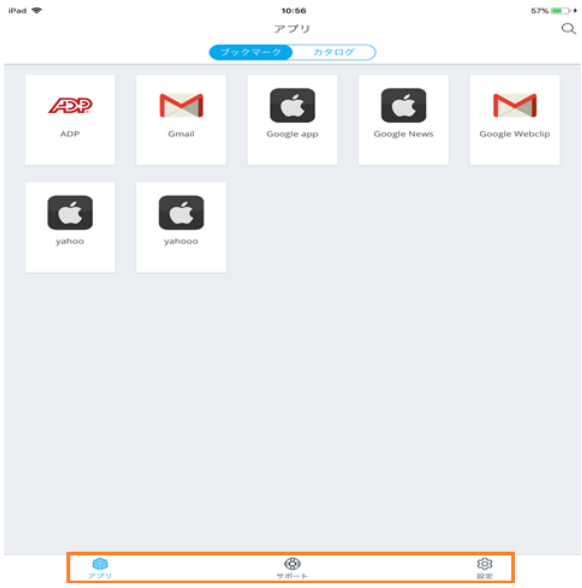
- [ブックマーク] タブから。ユーザーは、アプリケーションを起動するためのアプリケーションのアイコンをクリックします。
- [カタログ] タブから。ユーザーは、アプリケーションを開くための、矢印のアイコンが付いたボックスをクリックします。
- Workspace ONE 内における Spotlight 検索または検索から。iOS デバイスの Spotlight 検索では、ユーザーは、リストからアプリケーションのアイコンを選択します。Workspace ONE 検索から、ユーザーはアプリケーションを開くための、矢印のアイコンが付いたボックスをクリックします。

ユーザーは、自分の名前の横にあるドロップダウン矢印から Workspace ONE 設定にアクセスできます。

- アカウント。ユーザーの名前、ユーザー名、およびメール アドレスなど、ユーザーのプロファイル情報です。
- デバイス。Workspace ONE アプリケーションにログインしたデバイスのリストと、その最終ログイン日時です。
- アプリケーションのヒント。ユーザーのデバイスから Workspace ONE に移動する方法に関するヒントです。
- 関連情報。Workspace ONE の著作権、特許、およびライセンス情報です。
- 基本設定。Horizon リモート アプリケーションがアクセスされたときに、アプリケーションを Horizon Client から、またはブラウザからのどちらから表示するかのデフォルトの起動設定です。

ユーザーは、自分のアプリケーション ポータルにログインするために、デバイスの Workspace ONE アプリケーション アイコンをタップします。それらがブックマークされたアプリケーションの場合、[ブックマーク] ページが表示されます。デバイスの Workspace ONE アプリケーションには、サポートおよび設定へのリンクが含まれています。

図 8-3. Workspace ONE ポータルのデバイスの表示



- [サポート] ページには、[デバイス] と [レポートを送信] へのリンクが含まれています。[デバイス] ページには、デバイスに前回ログインしたときの状態が表示されます。[レポートを送信] では、診断情報やその他のフィードバックを送信する方法がユーザーに提供されます。ユーザーは、この機能を自分のデバイス設定でオフまたはオンにできます。

- [設定] ページには、Workspace ONE アプリケーションのバージョンと VMware Workspace のプライバシー ポリシーが表示されます。ユーザーは、Workspace ONE アプリケーションからログアウトするためのアカウントを [設定] ページから削除できます。

Workspace ONE での検索の使用

ユーザーは、Workspace ONE で検索を使用して、名前やカテゴリでアプリケーションを検索できます。

ユーザーは、検索テキスト ボックスに、入力ディスプレイと一致するアプリケーションを入力します。

図 8-4. 結果を示す検索

ユーザーは、検索結果から Web アプリケーションを起動するか、ネイティブ アプリケーションを直接ダウンロードできます。

iOS デバイスで、ユーザーは Workspace ONE ポータル内にあるアプリケーションを検索するために Spotlight を使用できます。iOS デバイスのホーム画面から、画面に指をタッチし、下にドラッグして Spotlight 検索フィールドを表示します。Workspace ONE ポータル内にあるアプリケーション名を入力すると、Workspace ONE が開き、アプリケーションが起動します。

iOS デバイスから問題をレポートするユーザーの支援

iOS デバイスの場合は、iOS アプリケーション開発者にログを送信するために、Rage Shake 機能を使用できます。

ユーザーが自分のデバイスをシェイクし、デバイスが現在の状態をログに記録します。詳細をデフォルトで Workspace ONE アプリケーション開発者に E メール メッセージで送信します。ユーザーは、別のメール アドレスを手動で入力し、別のアドレスに情報を送信できます。

ユーザーは、「シェイクでフィードバックを送信」機能を自分のデバイスの [設定] > [ワークスペース] ページから有効にできます。ユーザーは Workspace ONE ポータルの任意の画面から Rage Shake を使用し、レポートを送信します。

図 8-5. 「シェイクでフィードバックを送信」機能を有効にします。

iOS デバイスが**このデバイスが別のユーザーまたは環境に登録されている**ことを示すエラー メッセージを受信すると、デバイスのローカルに格納されているすべてのアプリケーション データをクリアするための手動でのアプリケーション リセット オプションを使用できます。

Workspace ONE アプリケーションのパスコードの設定

ユーザーは、デバイスでロックアウト パスコード機能を有効にする必要があります。有効でない場合、Workspace ONE アプリケーションの初回起動時にパスコードを作成するように求められます。このパスコードは、ユーザーがデバイスから Workspace ONE にアクセスするときに毎回入力されます。

パスコード機能を使用しない場合、ユーザーは Workspace ONE アプリケーションにアクセスする前にパスコードをセットアップするよう求められます。パスコードが設定される場所は、プラットフォームによって異なります。Android デバイスでは、パスコードはアプリケーション レベルで設定されます。Windows デスクトップ デバイスおよび Workspace ONE 3.2 以前を使用している iOS デバイスの場合、パスコードはデバイス レベルで設定されます。

注: iOS デバイスおよび Android デバイスは、Touch ID 指紋認証機能もサポートします。

Workspace ONE は、デバイスに関する潜在的なセキュリティの問題を検出できます。ユーザーがデバイス上でパスコードを無効にすると、次回 Workspace ONE アプリケーションにアクセスするときに、Workspace ONE にアクセスする前にパスコードを設定するように求められます。アプリケーション レベルのパスコードが有効な場合、エンド ユーザーはアプリケーション レベルのパスコードを無効にできません。

iOS デバイスでのアプリ レベルのパスコード

最小の 4 桁のデバイス パスコードよりも複雑なパスコードを作成できます。アプリ レベルのパスコードは、VMware Boxer などの他の生産性向上アプリと共有できます。

Workspace ONE UEM コンソール内のアプリのローカル パスコード要件を指定します。[グループと設定] > [すべての設定] > [アプリ] > [設定とポリシー] > [セキュリティ ポリシー] > [認証タイプ] に移動します。

パスコード認証が構成されている場合、他の生産性向上アプリが存在しない場合はアプリ レベルのパスコードを設定するよう求められます。または、他の生産性向上アプリとの共有パスコードを入力するよう求められます。

パスコード認証が構成されていない場合は、iOS デバイスでのデバイス パスコードが必要です。

ネイティブ アプリケーションの追加

ネイティブ アプリケーションは、特定のモバイル デバイス向けに開発されたアプリケーション プログラムです。Workspace ONE UEM での使用資格が付与されたネイティブ アプリケーションは、Workspace ONE の [カタログ] ページから表示できます。たとえば、iOS デバイスからカタログを表示する場合は、ユーザーに使用資格が付与された iOS アプリケーションのみが表示されます。

[カタログ] ページで [インストール] をタップすると、アプリケーションをデバイスにインストールできます。[インストール] をタップするとポップアップが表示されるので、次の処理を確認できます。表示される情報は、アプリケーションのタイプとプラットフォームによって異なります。鍵のアイコンが表示されるアプリケーションの場合、デバイスが Workspace ONE UEM によって管理されている必要があります。エンド ユーザーが鍵のアイコンの付いたアプリケーションをダウンロードしようとすると、「`Installation of this app requires enablement of Workspace Services`」というメッセージを受け取ります。

ユーザー認証のための VMware Verify の使用

VMware Verify サービスを、デバイスから Workspace ONE にログインするための 2 要素認証の 2 番目の認証方法として有効にした場合、ユーザーはデバイス アプリケーション ストアから VMware Verify アプリケーションをダウンロードする必要があります。

ユーザーが初めて Workspace ONE アプリケーションにログインするとき、ユーザー名とパスワードを入力するよう求められます。ユーザー名とパスワードが検証されると、ユーザーは VMware Verify サービスに登録するデバイスの電話番号を入力するよう求められます。

[登録] をクリックすると、デバイスの電話番号が VMware Verify サービスに登録されます。VMware Verify アプリケーションがダウンロードされていない場合、アプリケーションをダウンロードするよう求められます。

アプリケーションがインストールされると、ユーザーは、前回と同じ電話番号を入力し、ワンタイム登録コードを受け取るための通知方法を選択するよう求められます。登録コードは登録 PIN ページに登録されます。

デバイスの電話番号が登録されると、ユーザーは VMware Verify アプリケーションに表示される時間ベースのワンタイム パスコードを使用して Workspace ONE にログインすることができます。パスコードは、デバイス上で生成され、常に変化する一意の番号です。

ユーザーは複数のデバイスを登録することができます。VMware Verify パスコードは、登録済みの各デバイスに自動的に同期されます。

Workspace ONE ユーザーへのアラートの送信

管理者は、次回のシステムのダウンタイム、コンプライアンス ステータスを Workspace ONE ユーザーに通知して、アクションをリクエストしたり、アラートを送信したりできます。Workspace ONE UEM コンソールを介して通知が送信されます。

ユーザーはデバイスからの通知の受信方法を管理します。

Android デバイス版 Workspace ONE の操作

Android Workspace ONE アプリケーションを介して、アプリケーションの次のタイプを有効にできます。

- Web アプリケーション
- VMware Identity Manager サービスで有効になっているリモート アプリケーション。たとえば、Horizon 仮想アプリケーション、Citrix XenApp、ThinApp です。
- 管理対象および非管理対象の両方のネイティブ アプリケーション。ネイティブ アプリケーションは、Android プラットフォーム用に開発された Android アプリケーションです。これには 2 つのタイプがあります。
  - Google Play ストアから配布されるパブリック アプリケーション。
  - Workspace ONE UEM からプライベートで配布されており、Google Play ストアから入手できない社内アプリケーション。

  Web アプリケーションはブラウザで開きます。ユーザーは、VMware Horizon Client、または Citrix Receiver のいずれかを介して仮想アプリケーションにアクセスできます。

Android デバイスからの Workspace ONE アプリケーションの登録

有効なサーバ URL および認証情報で Workspace ONE アプリケーションにログインすることで、ユーザーは Workspace ONE 統合カタログにアクセスできるようになります。統合カタログで、ユーザーに割り当てられているすべてのアプリケーションが表示されます。

アプリケーションにアクセスするには Workspace ONE アプリケーションにユーザーを登録する必要があります。Workspace ONE に登録された状態では、ユーザーは VMware Identity Manager、Workspace ONE UEM 業務アプリケーション、および管理なしの SDK アプリケーションを介して有効になっている Web アプリケーションおよび仮想アプリケーションを使用できます。

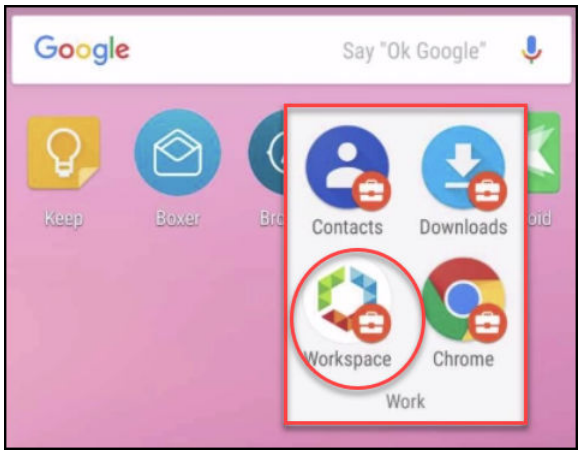
注: SDK アプリケーションは Workspace ONE UEM SDK を使用してコンテナ化および管理され、デバイスが管理される必要はありません。

ユーザーはアダプティブ管理を開始できます。これにより、デバイスで Android for Work が有効になり、プロファイル、ポリシー、およびデバイス用のアプリケーション配布の向上が可能になります。

Workspace ONE での Android for Work の管理

デバイスで Android for Work を有効にすると、オペレーティング システム レベルで仕事用データから個人用データを分離します。Android for Work は仕事用アプリケーションと個人用アプリケーションとの間の明確な分離を作成します。Android for Work は、個別の Android 仕事用バッジを使用して仕事用アプリケーションを作成します。

図 8-6. Android for Work のコンテンツ



管理者は、アプリケーションにアクセスできるようにする前に、デバイスが管理対象になることを要求するカタログ内のアプリケーションを決定します。管理を要求するカタログ内のアプリケーションには、[ダウンロード] ボタンの横に個別の星印が表示されます。

ユーザーがこれらのアプリケーションのいずれかをダウンロードしようとすると、そのアプリケーションはデバイスが管理対象であることを求めているとのメッセージが表示されます。デバイス管理の機能と利点を説明する画面が表示されます。

図 8-7. ワークスペース サービスの概要ページ

ユーザーが Android for Work の管理を有効にすることに同意すると、管理を設定するための手順がユーザーに表示されます。デバイスが管理対象になると、デバイスに Android for Work コンテナが作成されます。

Workspace ONE カタログの使用

9

Workspace ONE UEM と VMware Identity Manager を統合した場合、Workspace ONE アプリケーション カタログは、ユーザーに使用資格を付与できるすべてのリソースのリポジトリになります。ユーザーは、アプリケーションのために確立する設定に基づいて、Workspace ONE カタログ内で管理者が管理する企業アプリケーションにアクセスできます。

クラウド、モバイル、および Windows アプリケーションに、カタログからアクセスできます。社内開発またはアプリケーション ストアで公開しているネイティブ アプリケーションを、Workspace ONE ポータルからエンド ユーザーに提供できます。

Workspace ONE の [カタログ] ページで次のタスクを実行できます。

- 新規リソースのカタログへの追加
- 現在ユーザーに使用資格を付与できるリソースの表示
- カタログ内の各リソースについての情報へのアクセス

一部の Web アプリケーションは [カタログ] ページからユーザーのカタログに直接追加できます。他のリソース タイプでは、管理コンソール以外での操作が必要になります。リソースのセットアップに関する情報については、『VMware Identity Manager でのリソースのセットアップ』ガイドを参照してください。

カタログでのリソースの管理

特定のリソースの使用資格をユーザーに付与できるようにするには、そのリソースをカタログに格納する必要があります。リソースをカタログに格納する場合に使用する方法は、リソースのタイプによって異なります。

ユーザーへの資格付与と配布のためにカタログ内で定義できるリソース タイプは、Web アプリケーション、VMware ThinApp パッケージとしてキャプチャされる Windows アプリケーション、Horizon Client デスクトップ プールおよび Horizon 仮想アプリケーション、または Citrix ベース アプリケーションです。

Horizon Client デスクトップ プールおよびアプリケーション プール、Citrix 公開リソース、または ThinApp パッケージ アプリケーションを統合して有効にするには、[カタログ] タブのドロップダウン メニューにある仮想アプリケーションのコレクション機能を使用します。

これらのリソースの情報、要件、インストールおよび構成については、VMware Identity Manager を参照してください。

組織のカタログへの Web アプリケーションの追加

Web アプリケーションをカタログに追加するには、クラウド アプリケーション カタログから選択するか、新しい Web アプリケーションを作成します。

クラウド アプリケーション カタログには、一般に使用されるエンタープライズ Web アプリケーションが含まれています。これらのアプリケーションは部分的に構成されていて、アプリケーション レコードを完成させるには追加情報を提供する必要があります。また、Web アプリケーションのアカウント担当者と連携して、その他の必要なセットアップが必要な場合があります。

クラウド アプリケーション カタログの多くのアプリケーションは、SAML 2.0 または SAML 1.1 を使用して認証および承認データを交換し、Workspace ONE から Web アプリケーションへのシングル サインオンを有効にします。

アプリケーションを作成するときには、アプリケーションのすべての構成情報を入力する必要があります。構成は、追加するアプリケーションの種類によって異なります。フェデレーション プロトコルを使用しないアプリケーションの場合は、ターゲット URL のみが必要です。

VMware Identity Manager のアプリケーション ソースとして構成したサードパーティの ID プロバイダのアプリケーションは、新しいアプリケーションとして追加されます。

アプリケーションを追加するときには、アプリケーションへのユーザー アクセスを制御するアクセス ポリシーも選択します。デフォルトのアクセス ポリシーを使用できますが、[ID とアクセス管理] > [管理] > [ポリシー] ページから新しいポリシーを作成することもできます。アクセス ポリシーの詳細については、『VMware Identity Manager の管理』を参照してください。

カテゴリへのリソースのグループ化

Workspace ONE ポータルで必要なリソースをユーザーが簡単に突き止めることができるように、リソースを論理的なカテゴリに編成できます。

カテゴリを作成するときには、組織の構造、リソースのジョブ機能、リソースのタイプについて考慮します。リソースには複数のカテゴリを割り当てることができます。たとえば、販売員というカテゴリと営業担当リソースという別のカテゴリを作成することができます。カタログ内のすべての営業リソースに、販売員を割り当てます。また、営業担当リソースを、販売員のみと共有する特定の営業リソースに割り当てます。

カテゴリを作成した後、そのカテゴリをカタログ内の任意のリソースに適用できます。同じリソースに複数のカテゴリを適用できます。

ユーザーが自分の Workspace ONE ポータルにログインすると、ユーザーのビュー用に有効にされたカテゴリが表示されます。

『VMware Identity Manager 管理ガイド』でカタログの管理について参照してください。

VMware Identity Manager サービスのカスタム ブランディング

10

VMware Identity Manager コンソール、ユーザーおよび管理者のログイン画面、Workspace ONE アプリケーション ポータルの Web ビュー、モバイル デバイス上の Workspace ONE アプリケーションの Web ビューで表示される、ロゴ、フォント、および背景をカスタマイズできます。

カスタマイズ ツールを使用して、企業の配色、ロゴ、およびデザインや操作性を変更することができます。

この章には、次のトピックが含まれています。

VMware Identity Manager サービスのブランディングのカスタマイズ

管理コンソールおよびユーザー ポータルに、会社名、製品名、アドレス バー用のお気に入りアイコンを追加できます。また、ログイン ページをカスタマイズして、会社の配色やロゴ デザインに合うように背景色を設定することもできます。

手順

1 VMware Identity Manager コンソールの [ID とアクセス管理] タブで、[セットアップ] - [カスタム ブランディング] を選択します。

2 必要に応じて、フォーム内の次の設定を編集します。

[フォーム] フィールド	説明
	[名前とロゴ] タブ
会社名	会社名は、デスクトップ デバイスとモバイル デバイスの両方に適用されます。ブラウザのタブに表示されるタイトルとして会社名を追加できます。 既存の会社名の上に新しい会社名を入力して、名前を変更します。
製品名	製品名は、デスクトップ デバイスとモバイル デバイスの両方に適用されます。ブラウザのタブで会社名に続いて製品名が表示されます。
お気に入りアイコン	お気に入りアイコンは、ブラウザのアドレス バーに表示される、URL に関連付けられるアイコンです。 お気に入りアイコンの最大サイズは 16 × 16 px です。有効なフォーマットは JPEG、PNG、GIF、または ICO です。 [アップロード] をクリックし、新しいイメージをアップロードして現在のお気に入りアイコンを置き換えます。変更の確認を求めるメッセージが表示されます。変更は直ちに実行されます。
	[ログイン画面] タブ

[フォーム] フィールド	説明
ロゴ	[アップロード] をクリックし、新しいロゴをアップロードしてログイン画面の現在のロゴを置き換えます。[確認] をクリックすると、直ちに変更が行われます。 アップロードするイメージの推奨最小サイズは、350 x 100 ピクセルです。350 x 100 ピクセルより大きいイメージをアップロードすると、イメージは 350 x 100 ピクセルのサイズに合わせて調整されます。有効なフォーマットは JPEG、PNG、または GIF です。
背景の色	ログイン画面の背景に表示される色。 既存の色コードの上に 6 桁の 16 進数の色コードを入力して、背景の色を変更します。
ボックスの背景色	ログイン画面のボックスの色はカスタマイズできます。 既存の色コードの上に 6 桁の 16 進数の色コードを入力します。
ログイン ボタンの背景色	ログイン ボタンの色はカスタマイズできます。 既存の色コードの上に 6 桁の 16 進数の色コードを入力します。
ログイン ボタンのテキストの色	ログイン ボタンに表示されるテキストの色はカスタマイズできます。 既存の色コードの上に 6 桁の 16 進数の色コードを入力します。

ログイン画面をカスタマイズするときは、プレビュー ペインで変更を確認してから、変更を保存できます。

3 [保存] をクリックします。

VMware Identity Manager コンソールとログイン ページのカスタム ブランディングを更新して [保存] をクリックすると、5 分以内に更新内容が適用されます。

次のステップ

各種インターフェイスでブランディングの変更の見栄えを確認します。

エンド ユーザーの Workspace ONE ポータルと、モバイルおよびタブレット ビューの見栄えを更新します。「ユーザー ポータルのブランディングのカスタマイズ」を参照してください。

ユーザー ポータルのブランディングのカスタマイズ

ロゴの追加、背景色の変更、および画像の追加によって Workspace ONE ポータルをカスタマイズできます。

手順

1 VMware Identity Manager コンソールの [カタログ] タブで、[設定] - [ユーザー ポータル ブランディング] を選択します。

2 必要に応じて、フォーム内の設定を編集します。

フォーム項目	説明
ロゴ	VMware Identity Manager コンソール、および Workspace ONE ポータルの Web ページの上部に、バナーとして題字のロゴを追加します。 イメージの最大サイズは 220 × 40 px です。有効なフォーマットは JPEG、PNG または GIF です。
	ポータル
題字の背景色	既存の色コードの上に 6 桁の 16 進数の色コードを入力して、題字の背景色を変更します。新しい色コードを入力すると、アプリケーション ポータルのプレビュー画面に表示される背景色が変わります。
題字の文字の色	既存の色コードの上に 6 桁の 16 進数の色コードを入力して、題字として表示される文字の色を変更します。

フォーム項目	説明
背景の色	Web ポータル画面の背景に表示される色。 既存の色コードの上に新しい 6 桁の 16 進数の色コードを入力して、背景色を変更します。新しい色コードを入力すると、アプリケーション ポータルのプレビュー画面に表示される背景色が変わります。 背景色を強調するには [背景ハイライト] を選択します。[背景ハイライト] が有効になっている場合、複数の背景イメージをサポートするブラウザでは、[ランチャ] および [カタログ] ページにオーバーレイが表示されます。 背景色にあらかじめデザインされた三角形パターンを設定するには [背景パターン] を選択します。
アイコンの背景色	6 桁の 16 進数の色コードを入力して、アプリケーション アイコンを囲んでいる背景色ボックスを変更します。
アイコンの背景の不透明度	透明度を設定するには、バーでスライダを移動します。
名前とアイコンの色	アプリケーション ポータル ページのアイコンの下に表示される名前について、テキストの色を選択できます。 既存の色コードの上に 16 進数の色コードを入力して、フォントの色を変更します。
レタリング効果	Workspace ONE ポータルの画面のテキストに使用するレタリングの種類を選択します。
背景ハイライト	有効にすると、複数の背景イメージをサポートするブラウザでは背景オーバーレイがブックマークおよびカタログ ページに表示されます。
背景パターン	有効にすると、複数の背景イメージをサポートするブラウザでは背景オーバーレイがブックマークおよびカタログ ページに表示されます。
イメージ（オプション）	色の代わりにイメージをアプリケーション ポータル画面の背景に追加するには、イメージをアップロードします。

3 [保存] をクリックします。

ユーザー ポータルのカスタム ブランディングは 24 時間ごとに更新されます。より早く変更をプッシュするには、管理者として新しいタブを開いて次の URL を入力し、myco.example.com 部分をお使いのドメイン名に置き換えます。 `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`

次のステップ

各種インターフェイスでブランディングの変更の見栄えを確認します。

その他のドキュメントへのアクセス 11

Workspace ONE を設定するときは、VMware Identity Manager と VMware Workspace ONE UEM の両方のドキュメントを参照する必要があります。

こうしたドキュメント センターには、その他のドキュメントもあります。

- VMware Workspace ONE
- VMware Workspace ONE UEM
- VMware Identity Manager