datacontrol

Workspace ONE UEM 9.4 / 9.5
AirWatch 9.3
アップデート

2018年8月10日

株式会社データコントロール

製品の名称変更

VMware AirWatch は Workspace ONE Unified Endpoint Management (UEM) という名称になります。名称の変更に伴いコンソールの名称も変更されます。

v9.3 まで
VMware AirWatch Console

変更

v9.4 から
Workspace ONE UEM Console

コンソールの主な変更点

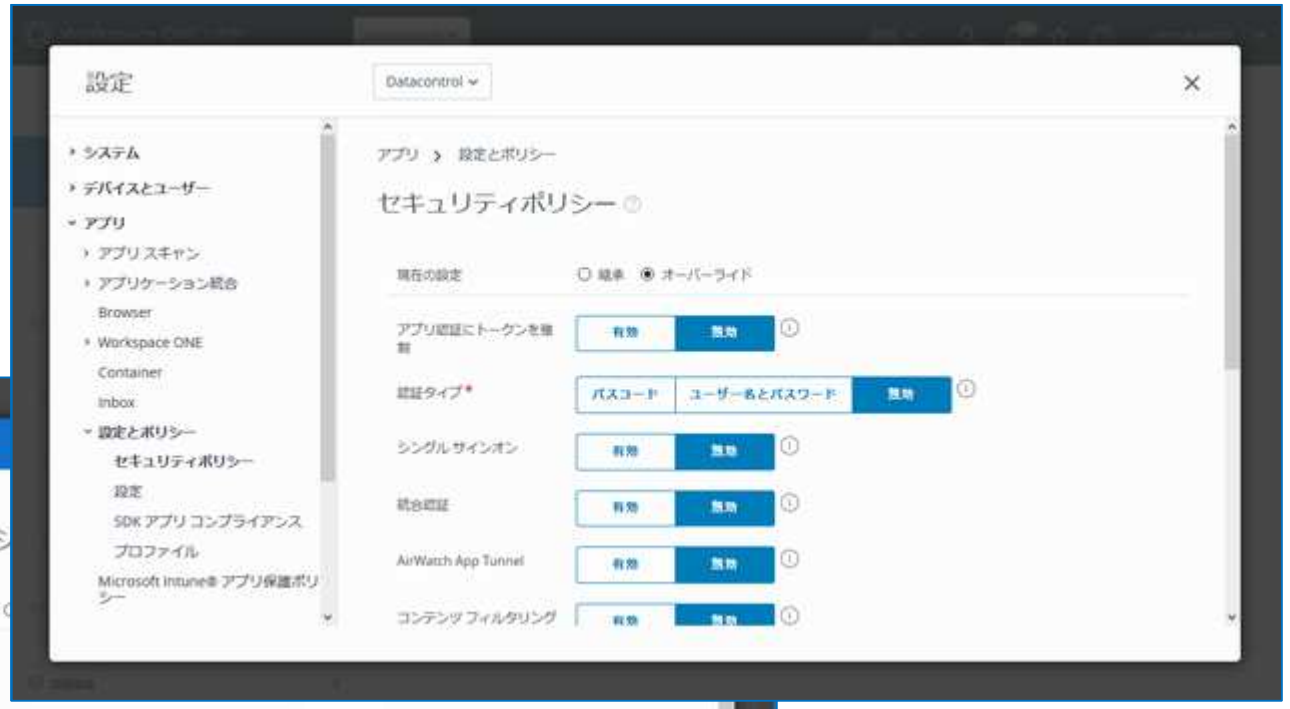
ロゴ、カラー等のブランディングが変更されます。メイン、サブメニューの表記や配列に変更はございませんので、従来通りの運用が可能です。

v9.4 Console

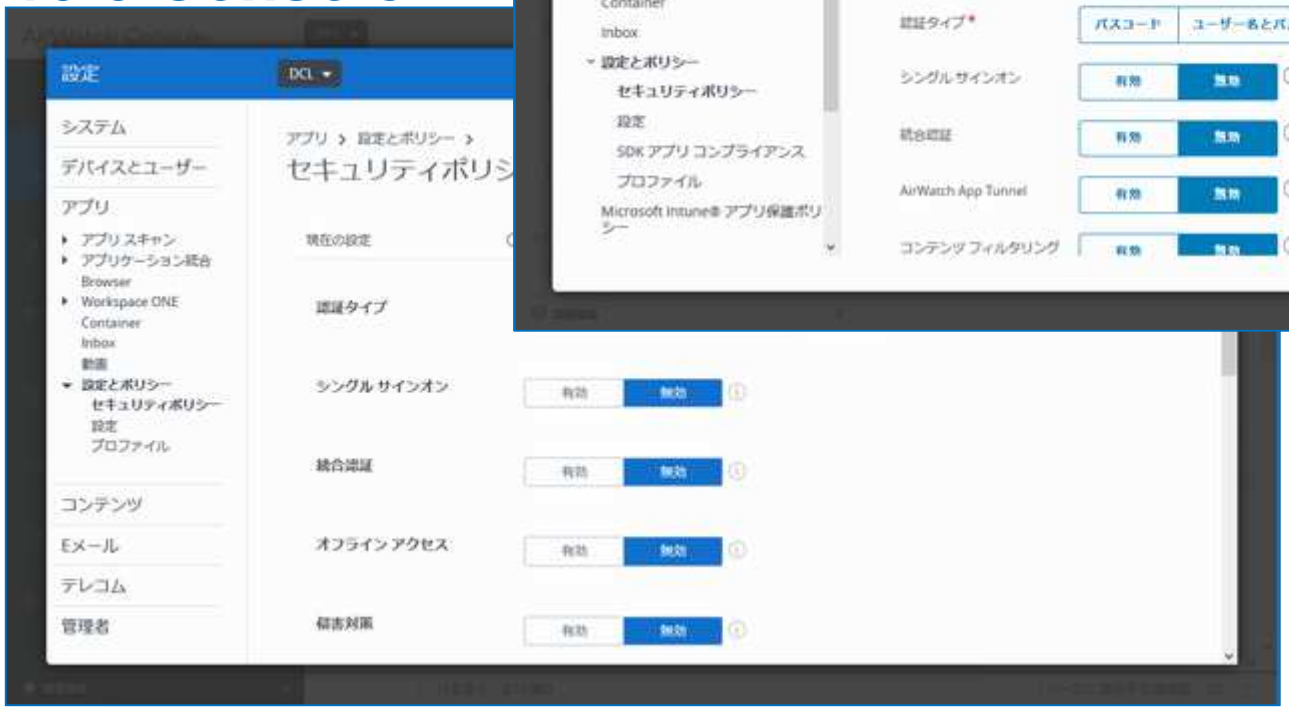
v9.3 Console

[設定] 画面における選択ボタンや入力フォームのデザイン変更されておりますが、既存の設定内容に変更はございません。

v9.4 Console



v9.3 Console



お客様へのお願い

Workspace ONE UEMへアップグレード実施後、Workspace ONE UEM コンソールにブラウザでアクセスすると意図しない表示になる場合があります。

初回Workspace ONE UEM コンソールにアクセスする際、ご利用いただいているブラウザのキャッシュを削除いただけますよう、お願いいたします。

- Chrome ブラウザでの手順

[Chrome menu] > [設定] > [詳細設定] > [プライバシーとセキュリティ]
[閲覧履歴データを消去する]
閲覧履歴、Cookie、キャッシュなどを削除します

[キャッシュされた画像とファイル] を選択して [データを消去] クリックします

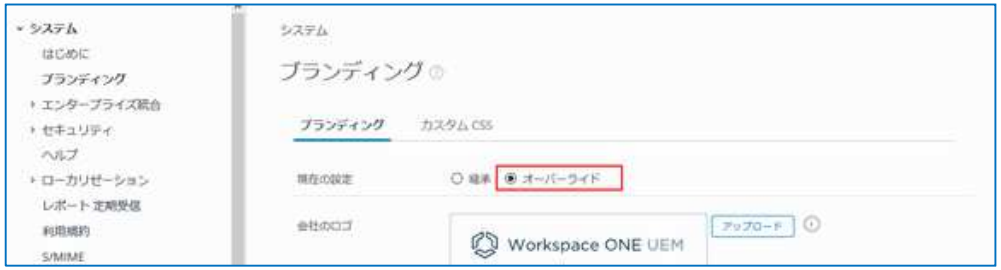
Workspace ONE UEM のロゴ

Workspace ONE UEMへアップグレード実施後、Workspace ONE UEM のロゴが見にくい事象が発生する場合があります。

事象が発生いたしましたら、下記の手順で設定変更をお願いいたします。

➢ 手順

[グループと設定] > [すべての設定] > [システム] > [ブランディング]
現在の設定　◉ オーバーライドを選択して、下段 [保存] をクリックします

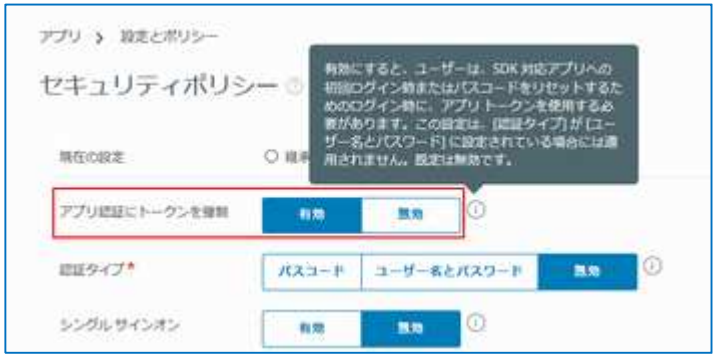


設定変更後、ログアウト-ログインを行ってください

SDKの機能追加

ユーザー名とパスワードを使用したパスコードのリセットを許可せずに、[アプリ認証にトークンを強制]という新しいオプションを使用して、パスコードを忘れた場合の手順を強制的に適用します。 [v9.4]

[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]



SDKで構築されたアプリケーション用のサードパーティ製キーボードの使用を制御できるようになりました。 [v9.3]

[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]

SDKの機能追加

デフォルトの SDK プロファイルである [**オフライン アクセス**] と[**侵害対策**] の場所を、[**セキュリティ ポリシー**] から、[**SDK アプリ コンプライアンス**] に移動しました。この画面の設定を使用することで管理者は、MDM プロファイルがインストールされていないデバイスであっても、SDK 対応アプリを通じてコンプライアンス機能を適用できます。 [v9.4]

[グループと設定] > [すべての設定] > [アプリ] > [設定とポリシー] > [SDKアプリ コンプライアンス]

Content Locker システム設定のオプション変更

VMware Content Locker、VMware Browser、および、VMware Boxer は、Workspace ONE (AirWatch) に加入していない管理外デバイスであっても利用することができるアプリケーションです。[v9.3]

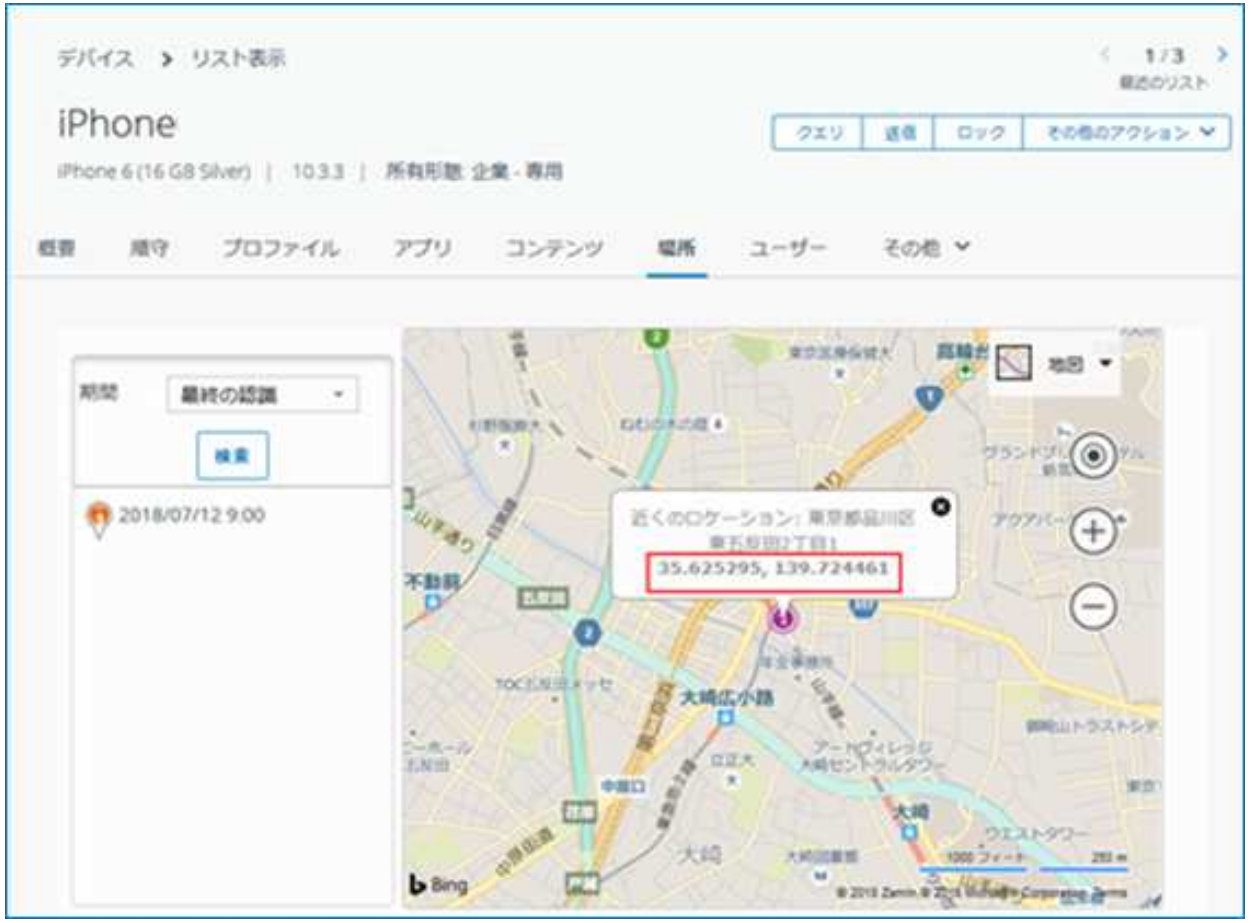
[グループと設定] > [すべての設定] > [コンテンツ] > [アプリケーション] > [Content Locker]

管理デバイスのみアプリを利用する場合は [有効] に設定します。

管理外デバイスでも利用できるようにする場合は [無効] に設定します。

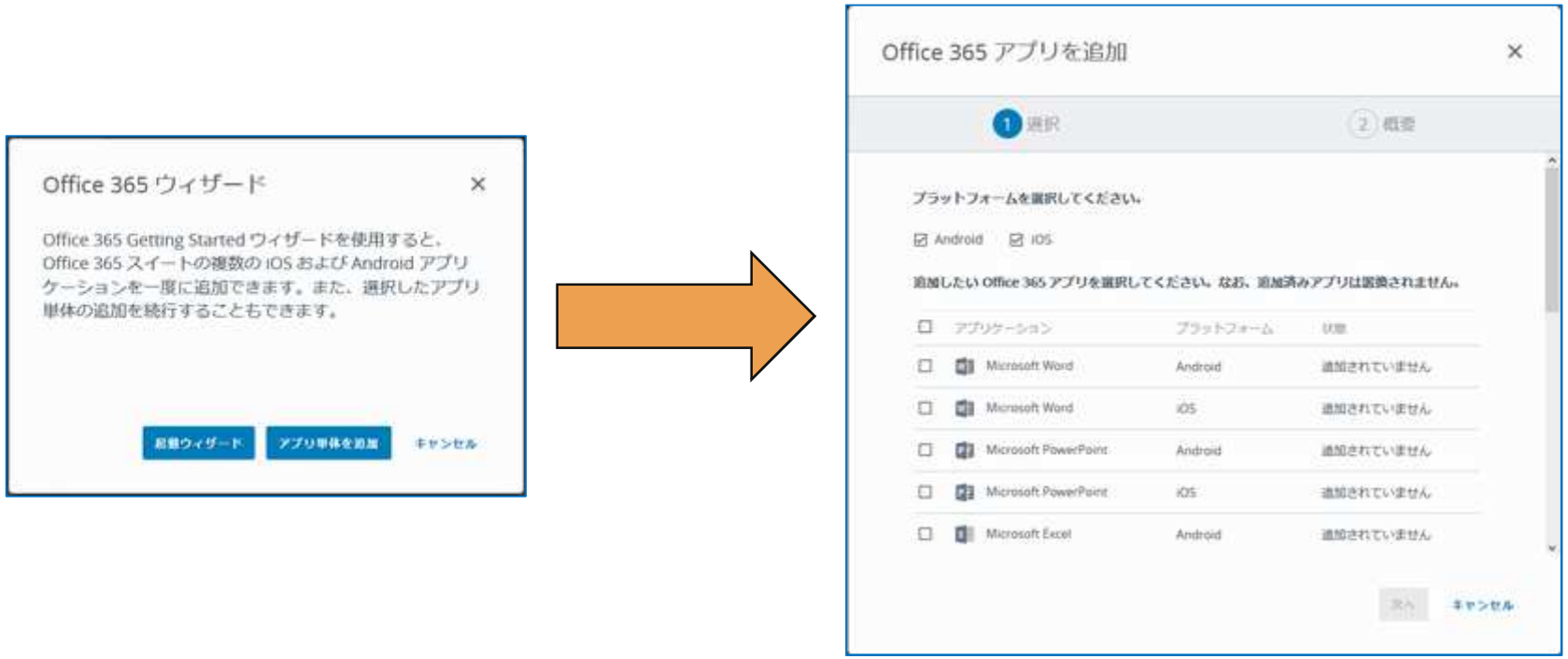
位置情報

[デバイス詳細] 画面 [場所]タブのBingマップ上の位置ピップにポインタを置くと、緯度と経度の座標がポップアップウィンドウに表示されます。 [v9.3]



Office 365 アプリ一括追加

Office 365 アプリの設定時に、複数の Office 365 アプリを一度に追加できる Office 365 アプリ ウィザード機能が追加されました。[v9.4]



Microsoft Intune® アプリ保護ポリシーとの連携

Workspace ONE (AirWatch) コンソールから Microsoft intune® のアプリ保護ポリシー設定が行える連携機能が追加されました。 Microsoft intune® のアプリ保護ポリシーとは、企業のデータを保護し、データ損失を防ぐために役立ちます。詳細は Microsoft社のドキュメントサイトをご参照ください。[v9.3, v9.4]

https://docs.microsoft.com/ja-jp/intune/app-protection-policy

[グループと設定] > [すべての設定] > [アプリ] > [Microsoft intune® のアプリ保護ポリシー]

※Microsoft社との契約により、Office365 および Microsoft Intune® のライセンスが必要になる場合があります。

Microsoft intune® アプリ保護ポリシーの種類

データ再配置設定

アクセス設定

iOS設定

Android設定

Google、Android デバイス管理機能のサポート縮小を発表

デバイス管理機能と Android Enterprise の今後

Android デバイスに対するこれまでの EMM モデルでは、VMware AirWatch Agent は Android デバイスの「デバイス管理アプリ」(デバイス管理者) として機能します。これは Android OS の要件として、Agent が EMM API にアクセスするために必要な権限です。そして Android L からは、Android Enterprise (旧名称は「Android for Work」) を使用する新しい EMM モデルが利用可能になっています。この新しいモデルでは、すべての Android OEM デバイスで利用可能な標準の管理 API 群、パブリック アプリのサイレント インストール、ビジネス向け Play ストアを利用した効率的なアプリケーション管理、BYOD ユース ケースでの個人用データと仕事用データの分離など、さまざまなメリットが得られます。

Android Enterprise の普及を促すため、Google 社は最近のアナウンスで、将来の Android OS バージョンにおいて従来のデバイス管理機能による EMM モデルのサポートを段階的に縮小することを表明しました。Android O ではデバイス管理機能モデルと Android Enterprise モデルの両方が完全なサポートの対象ですが、Android P ではデバイス管理 API は (機能はするものの) サポート対象外となる予定です。さらに Android Q のリリースで、デバイス管理機能モデルは完全に廃止され、Android Enterprise だけがサポート対象となります。

Workspace ONE (AirWatch) 環境では、特にことわりがない限り、従来のデバイス管理機能による EMM モデルも引き続きサポート対象です。デバイス管理機能モデルで管理されているデバイスは、OS をデバイス管理機能をサポートしていないバージョンにアップグレードしない限り、管理対象外になることも加入解除されることもありません。

お客様へのお願い

現在利用可能な Android バージョンのうち Android L ～ Android O はデバイス管理機能と Android Enterprise の両方の EMM モデルを完全にサポートしているため、現時点ですぐに実施していただく必要があるアクションはありませんが、2018年8月　Android 9 Pie がリリースされます。 Google 社および VMware はデバイス管理機能モデルを使用している企業/組織に対し、最終的には管理対象の Android デバイスをすべて Android Enterprise モデルに移行するよう、計画し始めていただくことを推奨します。この移行においては、考慮すべき重要なポイントが 2 つあります。

1. Workspace ONE (AirWatch) 環境で Android Enterprise を有効にした場合、現在デバイス管理機能モデルで加入しているデバイスが Android Enterprise モデルに移行するには再加入が必要になります。また、「Work Profile」と「Work Managed」の 2 つの加入モード、ならびにそれぞれのモードへの各種加入方法を評価し、貴社のユース ケースに最も適した加入モードと加入方法を決めていただく必要もあります。
2. Android Enterprise を使用するデバイスでは、AirWatch Agent は Android Enterprise API にしかアクセスできないため、OEM 固有の API により提供されている機能はサポートされなくなる場合もあります。これは、Workspace ONE (AirWatch) コンソールからプロファイルを使って設定している機能の一部が利用できなくなることを意味します。

Androidの名称変更

Android Enterprise (旧称 Android for Work) は、企業での Android デバイス導入を促進するため、2015 年に発表されました。それ以来、Google ではほとんどの Android デバイスで使用可能な機能を Android Enterprise に実装してきました。UEM コンソール リリース v9.4 以降、Workspace ONE UEM では、簡素化された命名規則を採用しています。**Android for Work** は **Android** に名称変更され、新規加入時のデフォルトの加入方法になっています。従来の Android プラットフォームは、今後は **Android (Legacy)** と呼ばれます。[v9.4]

【参考情報】Android OSのサポートバージョン

	Andorid 8 Oreo -	Android 9 Pie	Android 10 Q
Android API (従来)	サポート対象	機能はするが対象外	完全に廃止
Android Enterprise	サポート対象	サポート対象	サポート対象

Android Enterprise 設定

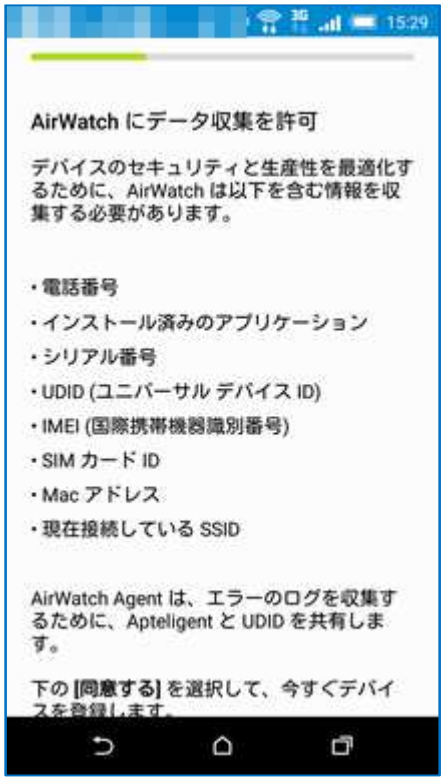
Workspace ONE UEM (AirWatch) コンソールには、Workspace ONE (AirWatch) に加入するための新しい Android EMM 登録画面が提供されました。これを使用して迅速にセットアップできます。[v9.4]

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Android] > [Android EMM 登録]

個人データ収集に関するユーザーの承諾

Android デバイスの加入時に、AirWatch によるユーザー データの許可を求める新しいアクセス許可画面がユーザーに表示されます。収集されたデータは、デバイスのセキュリティと生産性を最適化するために利用されます。収集される情報には、次の内容が含まれます。[v9.4]

- 電話番号
- インストール済みのアプリケーション
- シリアル番号
- UDID（ユニバーサル デバイス識別子）
- IMEI（国際移動体装置識別番号）
- SIM カード識別子
- MAC アドレス
- 接続している SSID



デバイスの QR コード加入における Wi-Fi 設定の追加

QR コードを使用した Android 仕事用管理対象デバイス(Work Managed)の加入で、管理者が Wi-Fi 認証情報を QR コードに含めることが可能になりました。QR コード プロビジョニングにより、NFC や NFC バンプをサポートしていないデバイスの加入が容易になります。管理者が Wi-Fi 認証情報を入力できるため、ユーザーはデバイスの Wi-Fi 接続を手動で行う必要がありません。[v9.4]

Workspace ONE (AirWatch) に加入する為の情報に加えて、Wi-Fi設定を付与してデバイスに読み込ませます

重要: この加入フローは、管理対象のGoogle Play ユーザーおよび管理対象Google ドメインユーザーが使用可能です。この加入フローは、Android 7.0 以降のデバイスでサポートされています。

Android プレリリース バージョンの展開

Android でのプレリリース バージョンの展開の機能が追加されました。

管理者は、アプリの本番バージョンをすべてのユーザーにプッシュする前に、アプリのアルファ バージョンまたはベータ バージョンをプッシュするかどうかを決定できるようになりました。Google Play を通じて公開したアルファ バージョンおよびベータ バージョンを、Android デバイス上の管理された Play ストアを通じて割り当ておよび提供できるようになりました。アプリケーションを割り当てるときに、新しいフィールドである [プレリリース バージョン] を使用して、アプリのバージョンを選択できます。アルファまたはベータを選択しないと、アプリの本番バージョンがすべてのデバイスに自動的にプッシュされます。[v9.5]

Android版VMware AirWatch の最小チェックイン間隔の更新

Android 版 VMware AirWatch Agent のチェックイン間隔の最小値が更新されました。最小サンプル値は、30 分からになります。Android 版 VMware AirWatch Agent の [プロファイルを更新] オプションに、6 時間と 10 時間の間隔が含められました。[v9.5]

iOS ソフトウェア遅延

OSレベルのソフトウェア遅延の制限により、指定した日数(1日～90日)の間、エンドユーザーのiOSデバイスに表示されている[設定] > [一般] > [ソフトウェアアップデート]から、OSを更新する際の強制的な遅延を実行できます。(iOS 11.3+管理対象デバイス)
[v9.3]

[デバイス] > [プロファイルとリソース] > [プロファイル]　iOSデバイス用構成プロファイル

iOS版VMware AirWatch の最小チェックイン間隔の更新

iOS版 VMware AirWatch Agent のチェックイン間隔の最小値が更新されました。最小サンプル値は、1 時間からになります。[v9.5]

Mac OS PerApp VPN サポート

Mac OSにおける、アプリベーストンネルが利用できるように機能が追加されました。[v9.4]

Apple Device Enrollment Program (DEP)

DEP 加入プロファイルにおける Apple 設定アシスタントのワークフローの 3 つの新しいスキップ オプションが追加されました。[v9.4]

[iCloud のドキュメントとデスクトップ]
[この Apple TV はどこですか]
[プライバシー]

Apple Volume Purchase Program (VPP)

VPP ロケーション トークンのロケーション名が Workspace ONE UEM (AirWatch) コンソールで表示されます。[v9.5]

※本機能は Apple Business Manager を利用する必要があります。
【参考サイト】
https://support.apple.com/ja-jp/HT208817

Windows 10 / コマンドプロセッサの改善

- コマンド プロセッサでは、応答待ちのコマンド キューを無期限に保持するのではなく、デバイスからの応答（成功または失敗）を受信しないとコマンドをキューから消去するようになりました。[v9.4]

- コマンド プロセッサは、アクティブな加入ユーザーが Windows デバイスにログインしていない場合でも、デバイス コンテキストに応じたコマンドを実行します。以前のバージョンでは、アクティブな加入ユーザーが Windows デバイスにログインしていないとコマンドを実行されませんでした。この動作に改善を加え、デバイス コンテキストのコマンドはすべて、ユーザーが Windows にログインしていなくても正しく実行されます。ユーザー コンテキストのコマンドは、ユーザーがログインするまで実行を待機します。[v9.4]

複数ユーザーで Windows 10 を利用していても、Workspace ONE (AirWatch) で管理することが可能となりました。

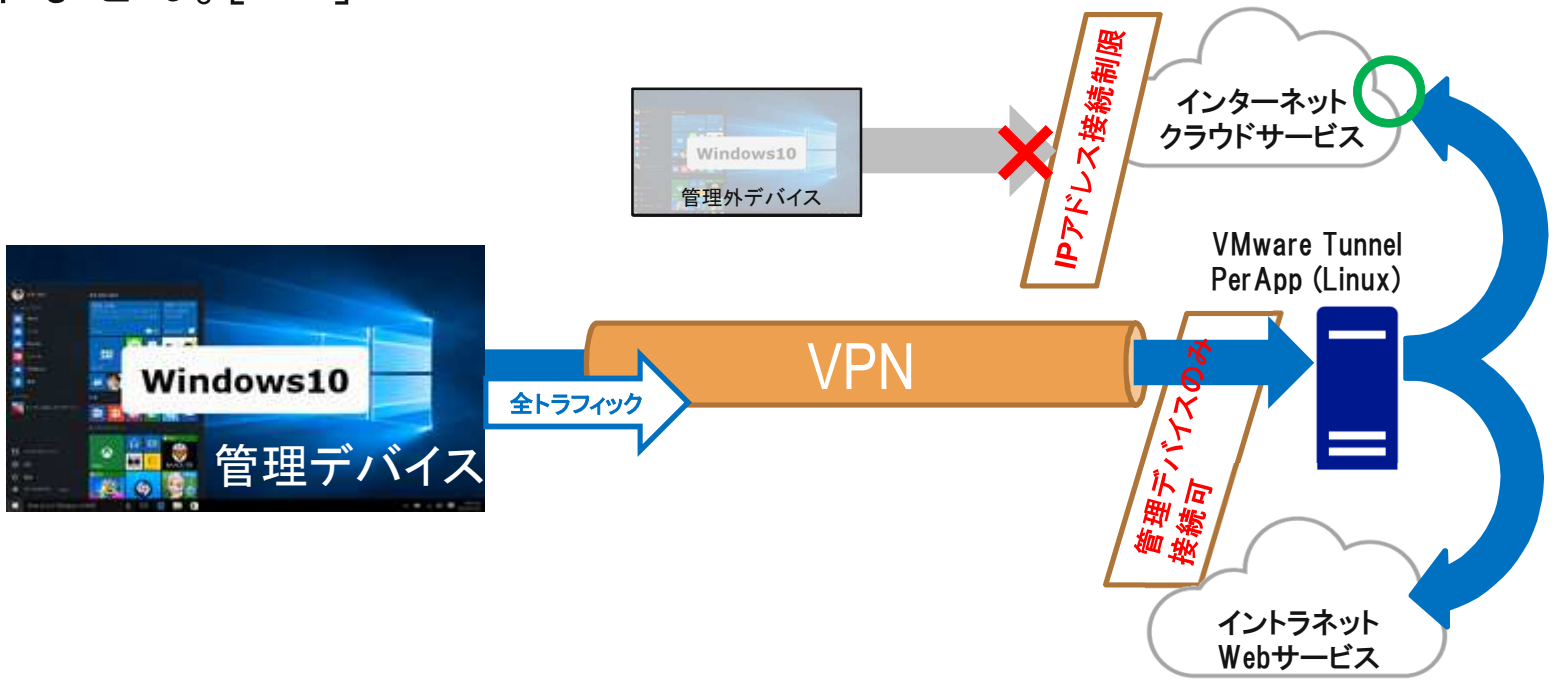
Windows 10 / 強化されたWindows Update管理プロファイル

Windows Updateプロファイルに新機能が追加されました。AirWatchは現在、マイクロソフトのアップデートブランチをサポートしています。その他の拡張機能には、配信最適化ネットワーク、メモリ、およびディスクスペースの設定、遅延アップデートのデュアルスキャン設定、自動再起動の設定などがあります。[v9.3]

Windows 10 / VMware Tunnel 通信のロックダウン

VMware Tunnel では、Windows 10 デバイスのすべてのデバイス トラフィックを VMware Tunnel にロックダウンする機能がサポートされました。

この機能を使用すると、デバイスは、トンネル接続以外の経路で外部と通信することができなくなります。ユーザーは常にトンネル接続を使用するように強制され、すべてのトラフィックが必ず VMware Tunnel を通過するようになります。デバイスがトンネル接続を使用できない場合、デバイスからトラフィックは送信されません。[v9.4]



Secure Email Gateway

- SEG (V2) で、Google のメール サーバがサポートされました。必要に応じて、自動パスワード プロビジョニング機能を有効または無効にできます。[v9.4]

- Secure Email Gateway V2 (SEG) での、E メール通知サービス (ENS) の機能が追加されます。VMware Boxer の E メール通知サービス (ENS) で使用される Exchange Web サービス (EWS) トラフィックに対し、SEG にて認証および順守の機能が提供されるようになりました。クラウドおよびオンプレミス展開用の ENS と、Kerberos の制約付き委任 (KCD) を使用した Exchange 証明書ベース認証 (CBA) がサポートされました。[v9.5]

クラシック Secure Email Gateway (SEG V1) インストーラのジェネラル サポート終了

VMware社 は 2019 年 5 月 5 日をもってクラシック Secure Email Gateway (SEG) インストーラのジェネラル サポートを終了いたします。

2018 年 12 月 24 日以降、クラシック SEG インストーラは Resource ポータルから削除される予定です。

お客様へのお願い

現在、クラシック SEG をご利用のすべてのお客様は、このジェネラル サポート終了までに SEG V2 に移行していただくようお願いいたします。

※クラシック Secure Email Gateway:

Microsoft Internet Information Services (IIS) と Microsoft . NET Framework をベースに稼働するゲートウェイサーバです。

Workspace ONE UEM (AirWatch) 9.5　リリーススケジュール

弊社提供のAirWatch SaaSは下記日程でアップグレードを
実施する予定です。

作業内容:
　Workspace ONE UEM (AirWatch) 9.5 へのアップグレード作業

日程:
　2018年8月29日 午後 11時～

ありがとうございました。