

Workspace ONE UEM 1811アップデート

2019/3/5
株式会社ウィザース

目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM
8. その他

目次

1. **Workspace ONE UEM 管理者パスワード**
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Workspace ONE UEM 管理者パスワードのセキュリティ強化

2018年はソリューション名称とバージョン表記が変更されました。

- 2018年3月: ソリューション名称が Workspace ONE に変更されました。 **9.4**
- 2018年10月: コンソールリリースのバージョン表記に新しい形式が採用されました。 **1810**
従来のメジャー リリース番号とマイナー リリース番号をドットで繋いだ形式 (major.minor) のバージョン番号表記を廃止し、リリース年とリリース月を列記した形式 (YYMM) に移行しました。

いくつかの新バージョンリリースでは、ベーシック管理者のパスワードセキュリティ強化の行われました。

本章では、ベーシック管理者のパスワードセキュリティ強化についてご案内させていただきます。

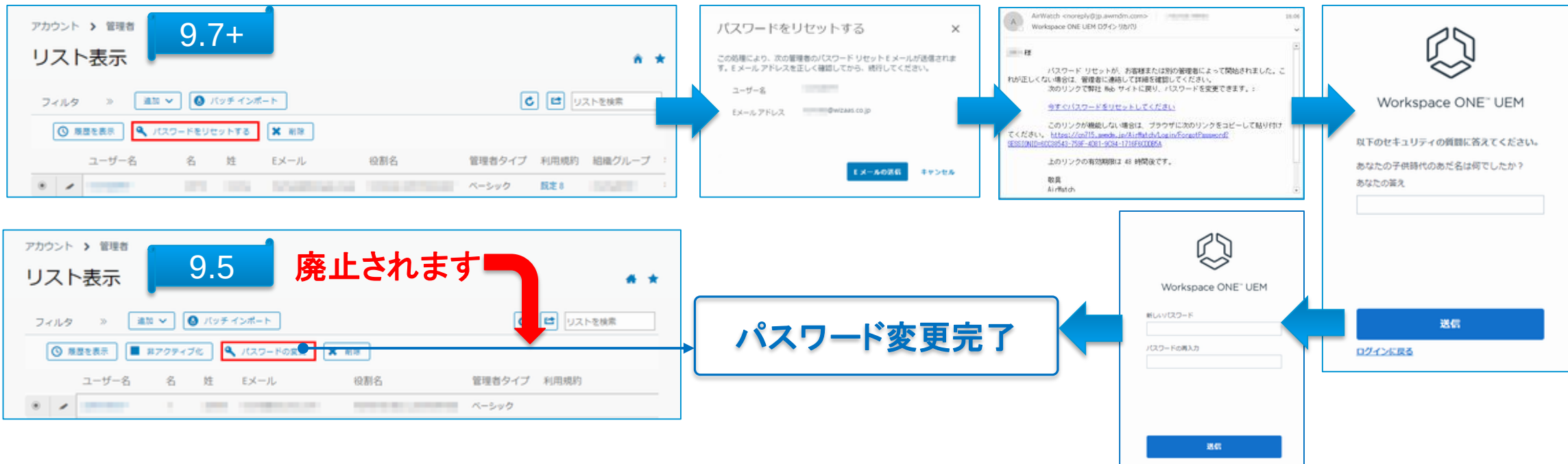
※ベーシック管理者(以下管理者): Workspace ONE UEM で管理されている管理者アカウントです。Active Directory と連携している管理者とは異なります。

管理者のパスワード変更機能からパスワードリセット機能へ

管理者向けの UEM Console セキュリティが強化され、[パスワードの変更] オプションが削除されて [パスワードをリセットする] ソリューションに置き換わりました。 **9.7**

[パスワードをリセットする] 機能とは、管理者の E メールアドレス宛にパスワードをリセットするための E メールが送信されます。 **管理者アカウント初回ログイン時にセットアップされたパスワード回復用の質問に回答することで、管理者の身元が認証されます。**

上記機能変更により、管理者が他の管理者のパスワード変更を行うことが出来なくなりました。



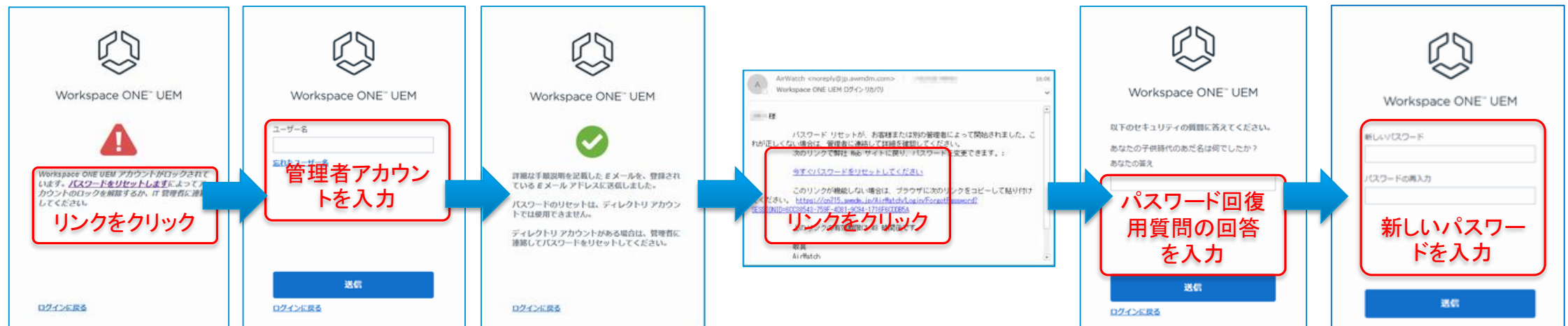
管理者ロックアウト機能の変更

管理者のロックアウトの期限を廃止しました。この為、一度ロックアウトした管理者は他の管理者から [パスワードをリセットする] を実行し、パスワードリセットの E メール通知を受信するか、ログイン画面からパスワードリセットの E メール通知を受信する必要があります。ロックアウトが解除されるのを待っての再試行は行えないのでご注意ください。 1810

管理者のロックアウト

- ・ 管理者のパスワードを誤った入力を 5 回入力 (cn1.dcl-mdm.com の場合)
- ・ パスワード回復用質問に誤った回答を 3 回入力

管理者セルフパスワードリカバリの流れ



他の管理者パスワードのセキュリティについて

「管理者アカウントがロックされました」と「管理者アカウントがロック解除されました」という 2 つの新しいイベントが、コンソール イベント ログに追加されました。 1811

管理者がロックアウトされてしまった際のトラブルシューティングとしてご活用ください。



日付の範囲	重要度	日付と時刻	管理者アカウント	モジュール	カテゴリ	イベント名	イベントデータ
今日	お知らせ	2019/02/25 14:59		管理	ログイン	管理者アカウントがロック解除されました	
	お知らせ	2019/02/25 14:54		管理	ログイン	管理者アカウントがロックされました	

Workspace ONE UEM ログイン画面にて、CAPTCHA が要求されなくなりました。 9.7

廃止されます



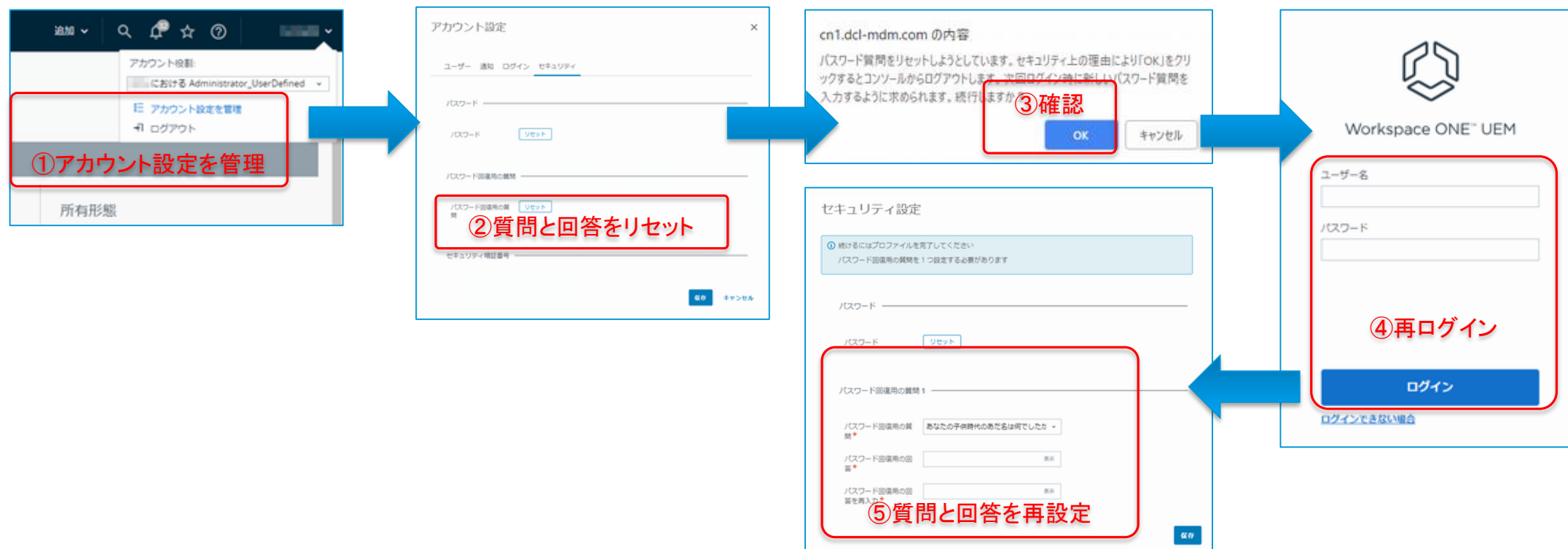
※CAPTCHA: Completely-Automated-Public-Turing-Test to tell Computers and Humans Apart (コンピュータと人間を区別する完全に自動化された公開チューリングテスト) を略したものです。

お客様へのお願い

管理者のパスワードセキュリティ強化により、他の管理者によるパスワードの変更が行えなくなりました。弊社サポートにご依頼をいただいても管理者のパスワードの変更は行えません。

お客様におかれましては、今一度、パスワード回復用質問と回答を見直していただけますよう、何卒よろしくお願いいたします。また、管理者に設定されている E メールアドレスが受信可能であることを今一度ご確認くださいませよう、何卒よろしくお願いいたします。

パスワード回復用質問と回答の変更の流れ



目次

1. Workspace ONE UEM 管理者パスワード
2. **Workspace ONE Intelligent Hub の新機能**
3. Workspace ONE Intelligent
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Workspace ONE Intelligent Hub の新機能

Workspace ONE UEM 1811 リリースに伴い Workspace ONE Intelligent Hub の新機能が利用できるようになります。Workspace ONE Intelligent Hub は大きく分けると3段階の利用方法がございますので、Step 1 ~ Step 3 に分けてご案内させていただきます。

Step 1 Workspace ONE UEM 9.5

機能: [デバイス管理]

Step 2 Workspace ONE UEM 1810~ + VMware Identity Manager

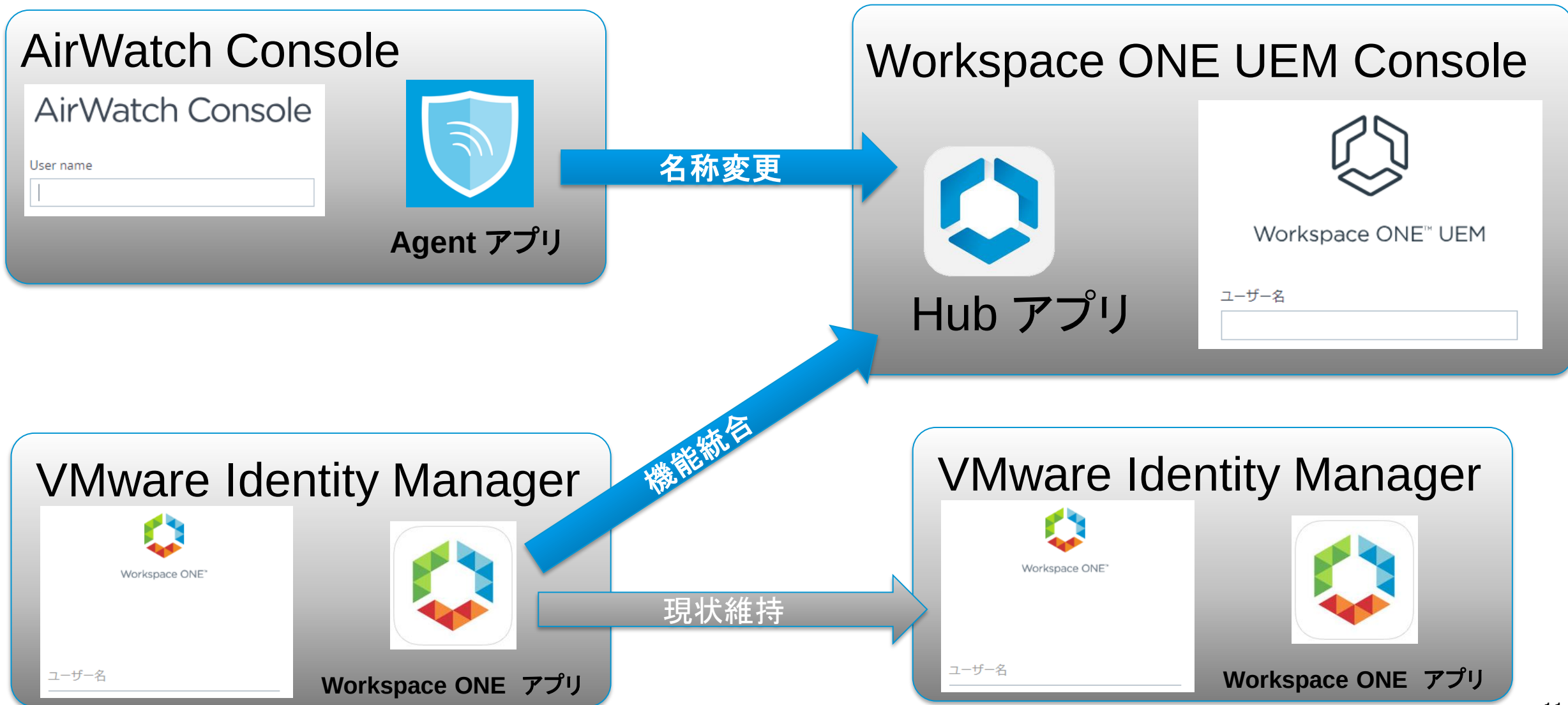
機能: [デバイス管理], [**ホーム画面**], [**WSO UEM Catalog**]

Step 3 Workspace ONE UEM 1810~ + VMware Identity Manager + Active Directory

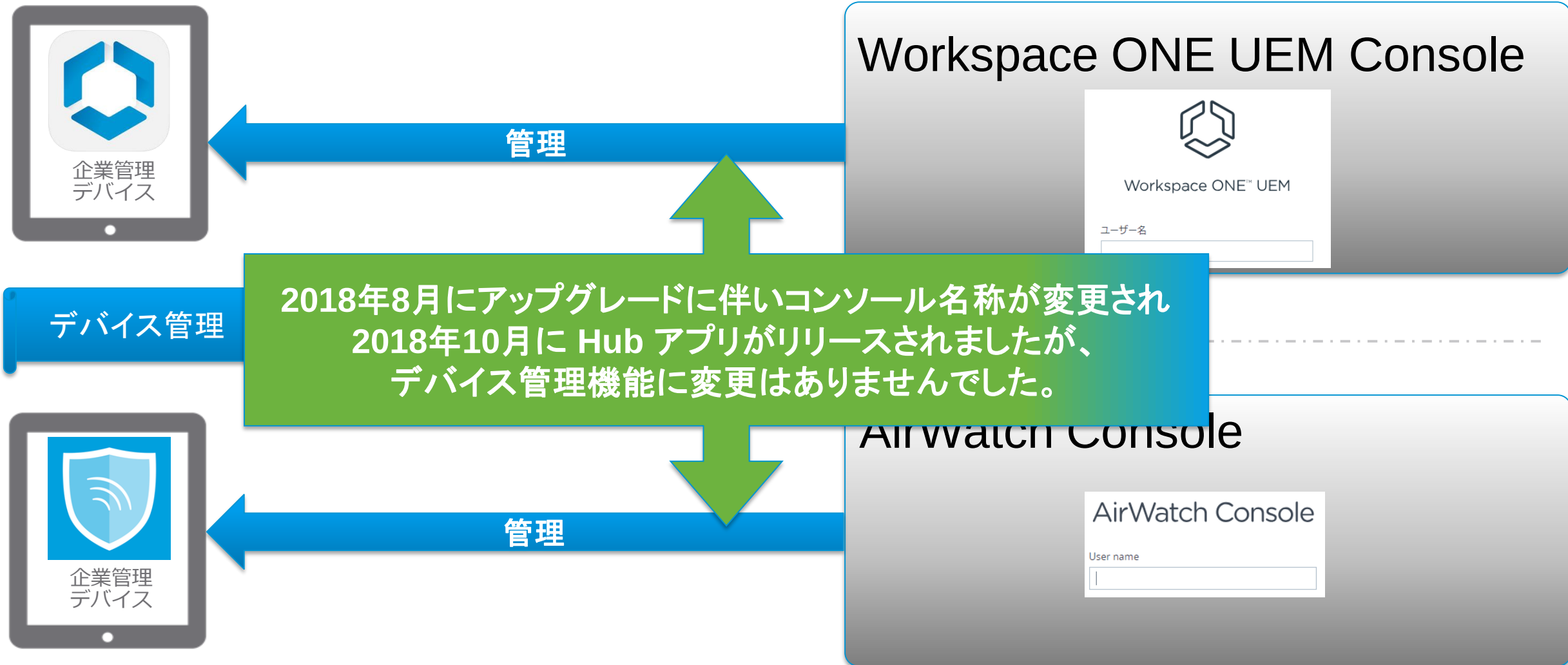
機能: [デバイス管理], [ホーム画面], [WSO UEM Catalog], [**SSO**]

Workspace ONE Intelligent Hub アプリとは
2018年10月 VMware 社よりリリースされた AirWatch Agent アプリの後継となるアプリです。

【参考】 ソリューション名称とアプリ名称の変更について

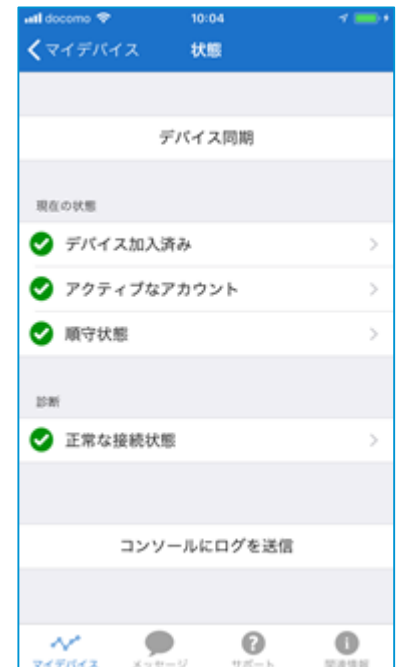


Step 1 Workspace ONE UEM 単体



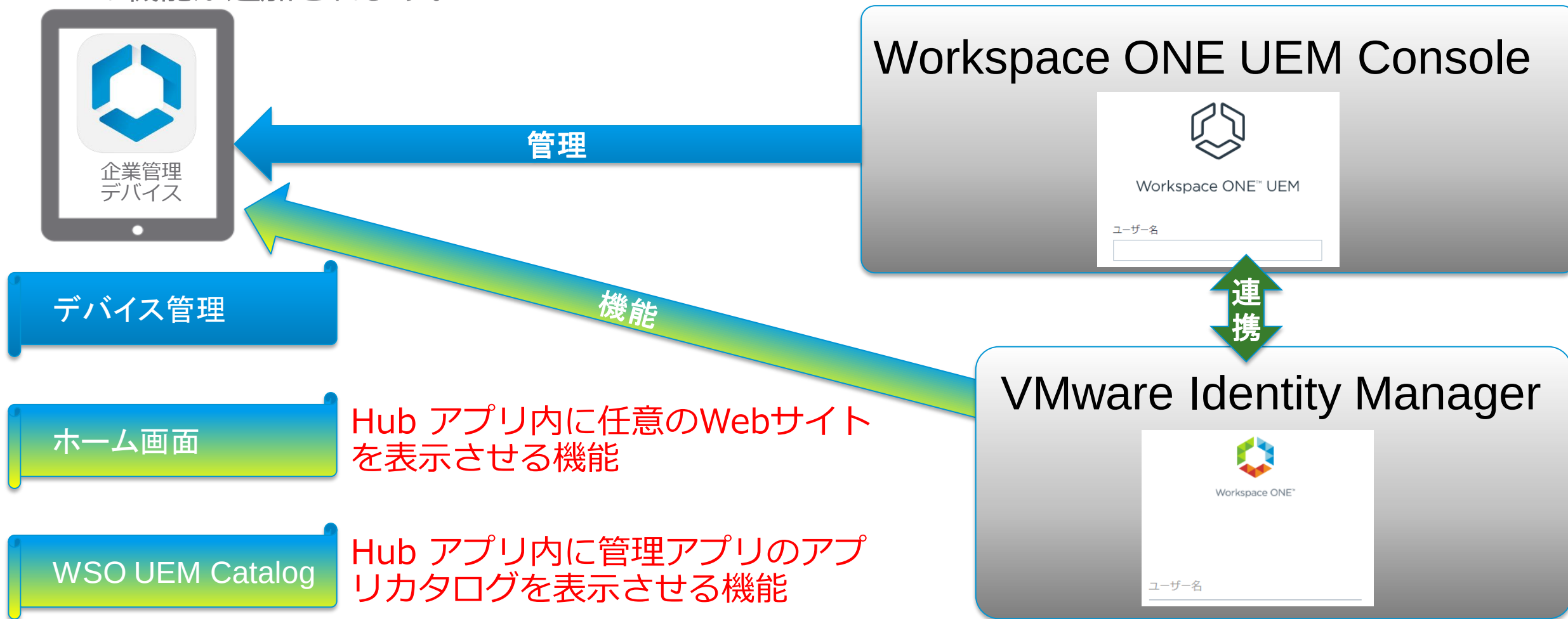
Step 1 Intelligent Hub vs AirWatch Agent

Workspace ONE Intelligent Hub と AirWatch Agent の画面比較となります。
デバイス管理機能に違いはありません。



Step 2 Workspace ONE UEM + VMware Identity Manager

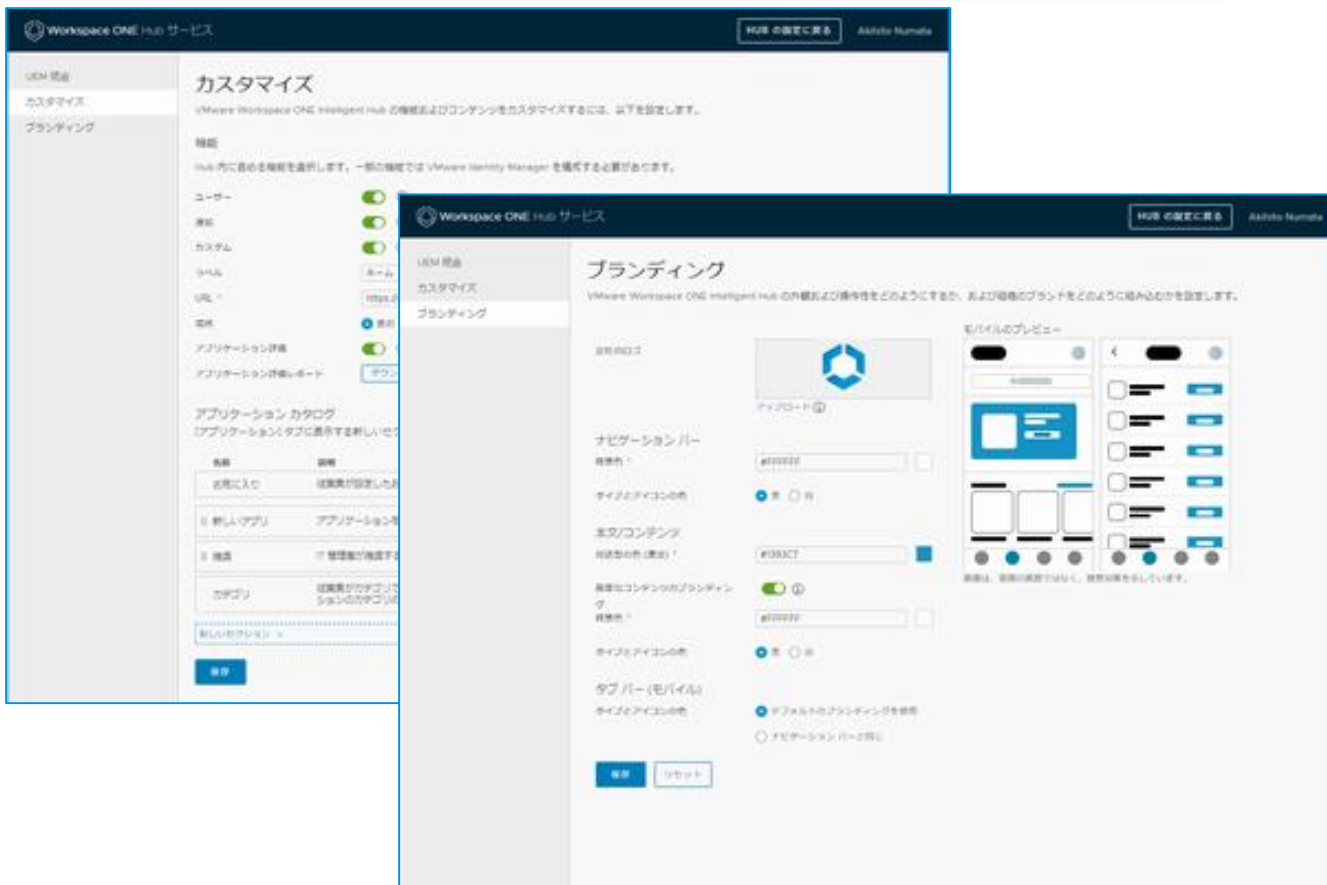
VMware Identity Manager と連携させることにより、Workspace ONE Intelligent Hub に二つの機能が追加されます。



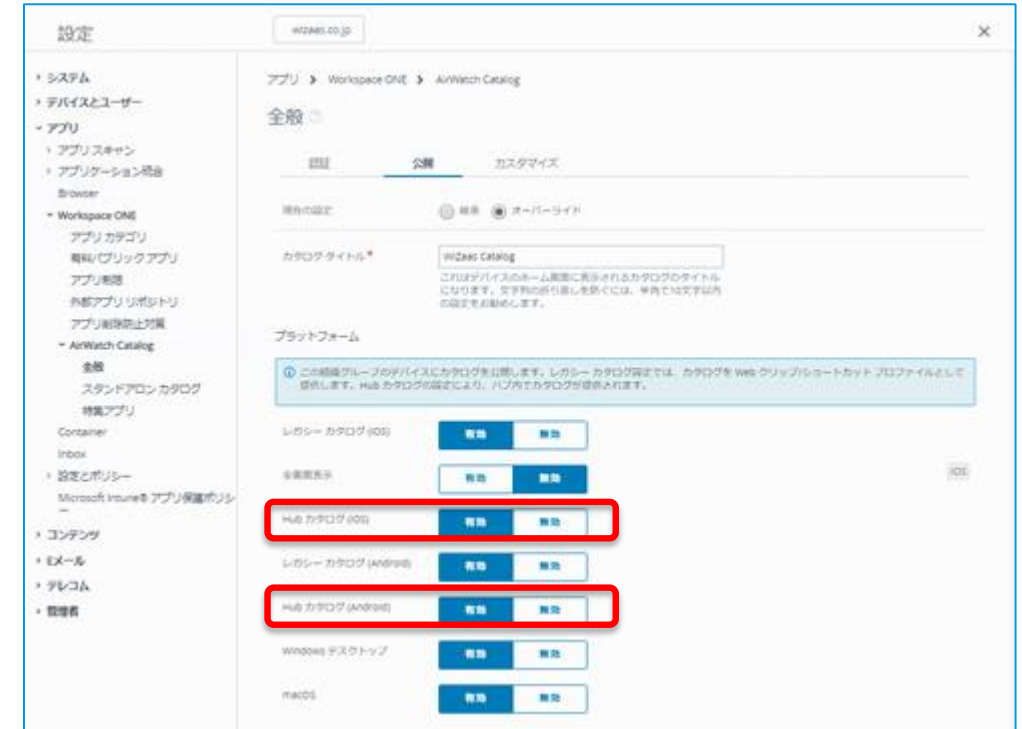
Step 2 Intelligent Hub の基本設定

Intelligent Hub のカスタマイズは VMware Identity Manager コンソールで行います。
Intelligent Hub 内アプリカタログの オン/オフ は Workspace ONE UEM コンソールで行います。

VMware Identity Manager コンソール



Workspace ONE UEM コンソール



Workspace ONE UEM コンソールからリダイレクトされます

Step 2 Intelligent Hub

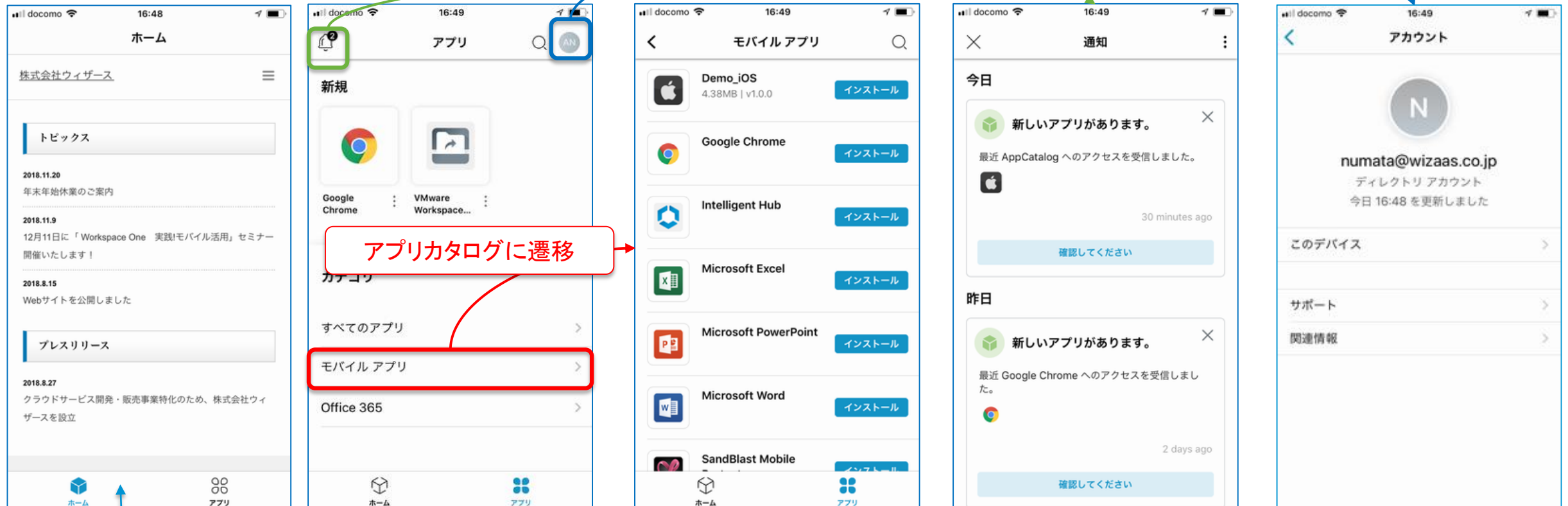
ホーム画面

WSO UEM Catalog

デバイス管理画面に遷移

通知画面に遷移

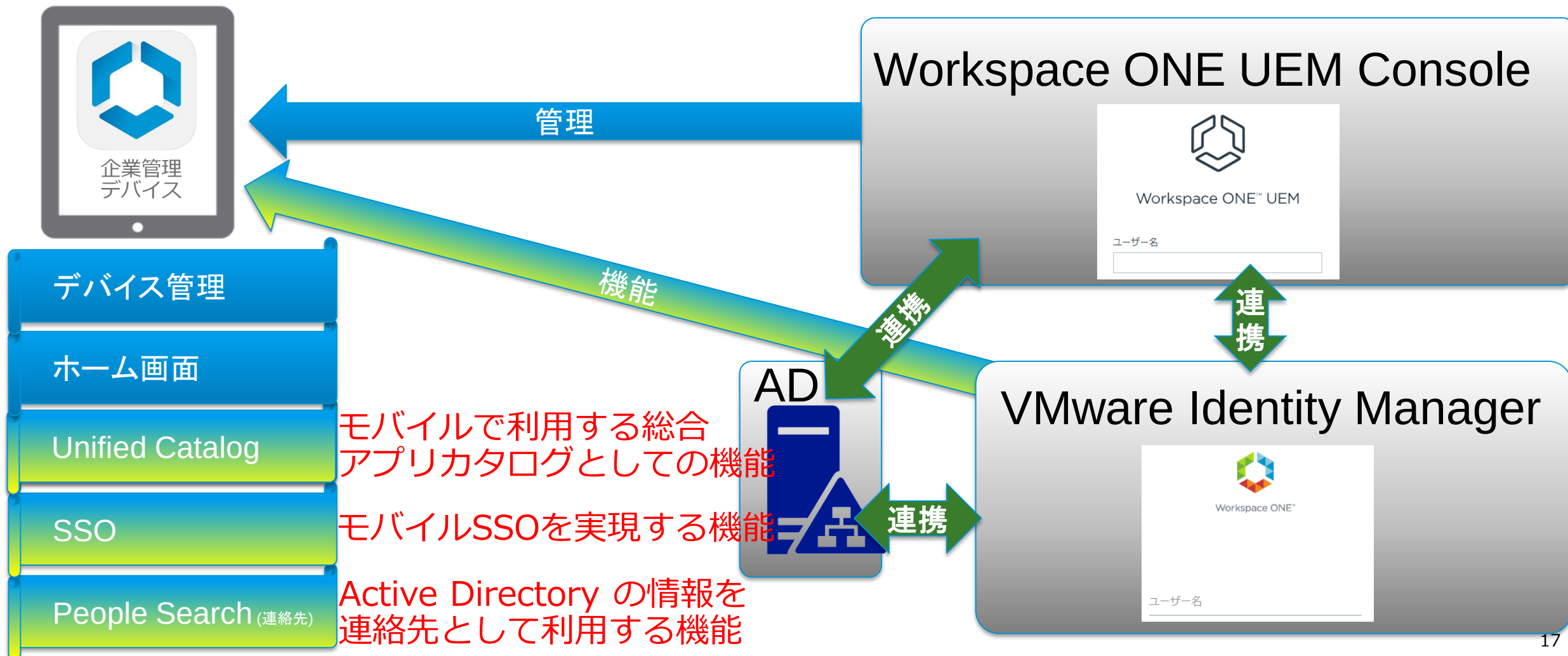
アプリカタログに遷移



VPN接続を利用してイントラWebサイトの表示も可能です。

Step 3 Workspace ONE UEM + vIDM + Active Directory

Active Directory を連携させることにより、Workspace ONE Intelligent Hub にさらに三つの機能が追加されます。

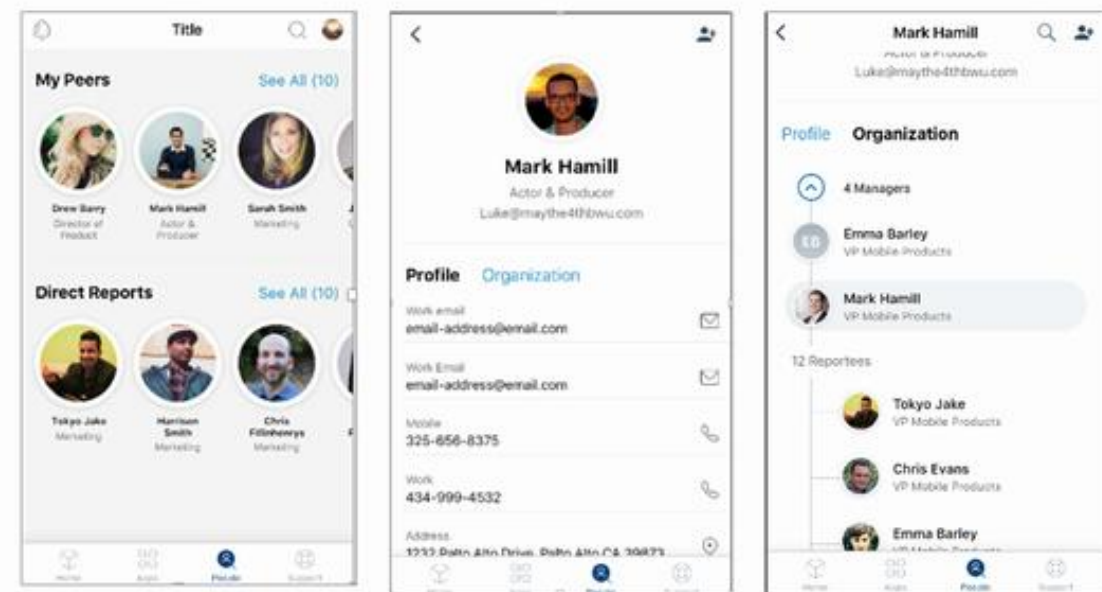


Step 3 Intelligent Hub

Unified Catalog



People Search (連絡先)



【参考】Workspace ONE アプリケーション

Workspace ONE



Intelligent Hub



Content



Web



Boxer



Tunnel

VMware (AirWatch)



AirWatch Agent



Content Locker



Browser



Boxer



Tunnel

目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. **Workspace ONE Intelligence**
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Workspace ONE Intelligence 構成

Workspace ONE Intelligence は可視化ツールです。

➤ダッシュボード (プロダクトライセンス)

ダッシュボードには様々なデータをグラフ化したものや数値化したものがウィジェット形式で並びます。このウィジェットは管理者のかたが見やすく、そして、管理しやすいように自由にカスタマイズすることができます。

➤自動化 (プロダクトライセンス)

モバイルデバイス順守違反や脆弱なデバイスを検知するなどのイベントが発生した際、SNSを利用したユーザー、管理者への通知、および、ヘルプデスクシステムへのインシデント通知などを自動化することができます。

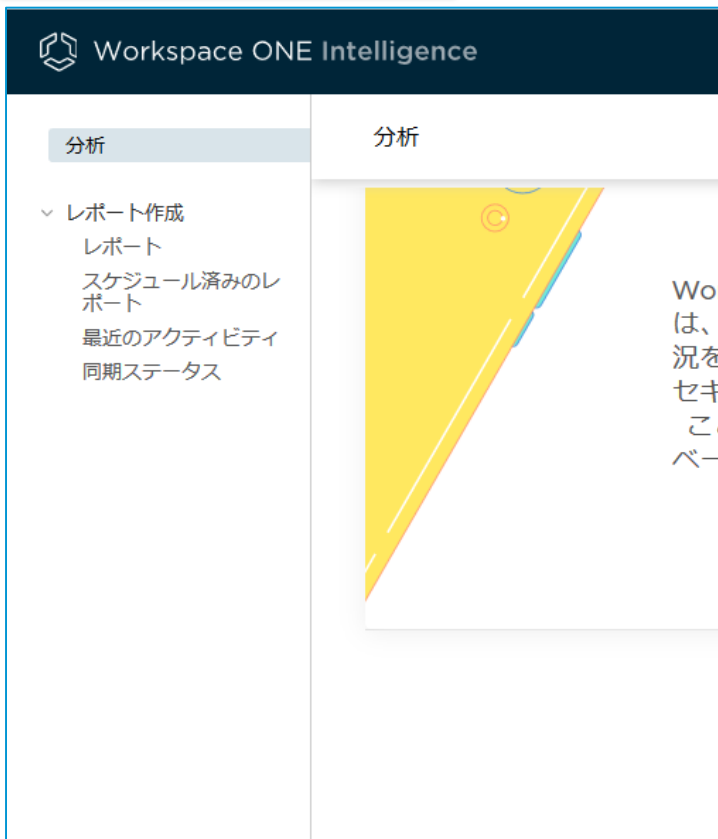
➤レポート (無償提供)

管理者にとって必要な情報のみを抽出したレポートをカスタマイズすることができます。
不必要な情報がプリセットされたレポートの編集が不要となります。

Workspace ONE Intelligence 画面

Workspace ONE Intelligence はプロダクトライセンスが必要です。
また、30日間のトライアルが可能となっております。

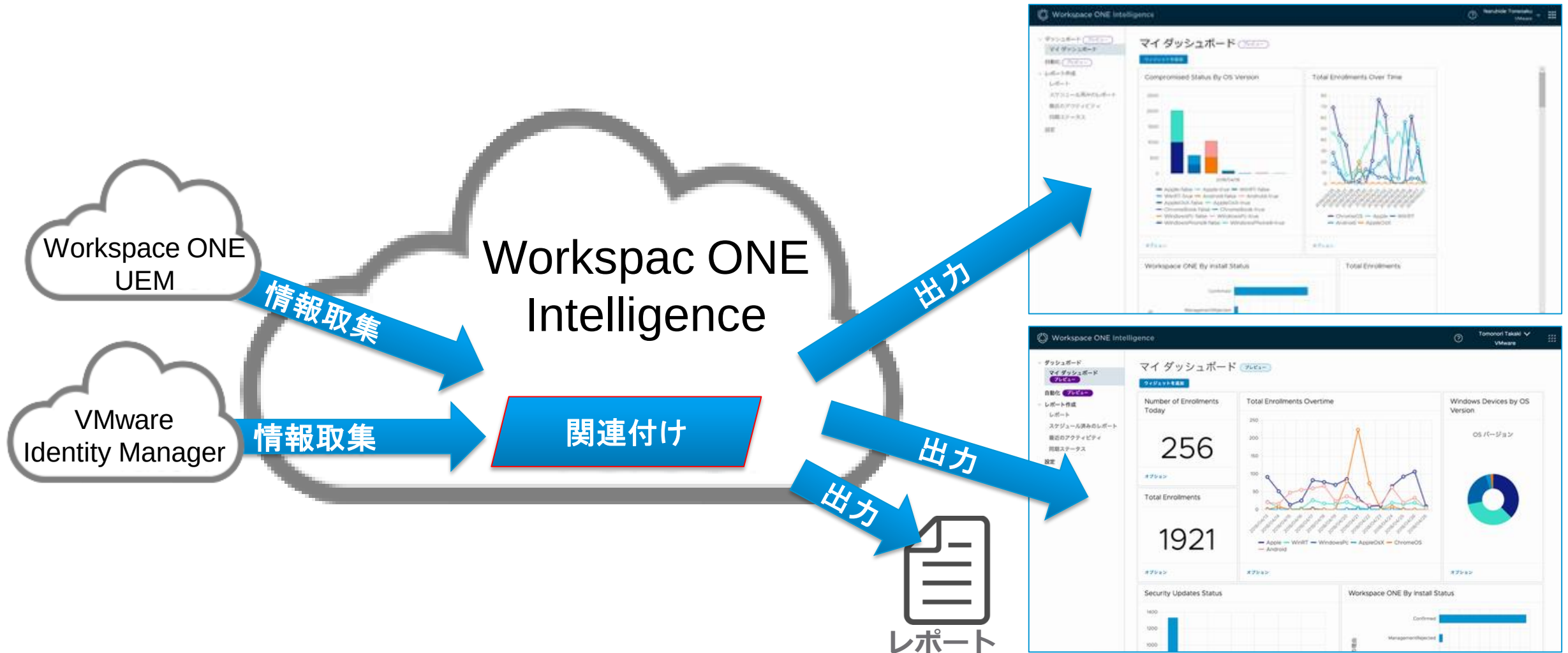
ライセンスなし



ライセンスあり (トライアル)

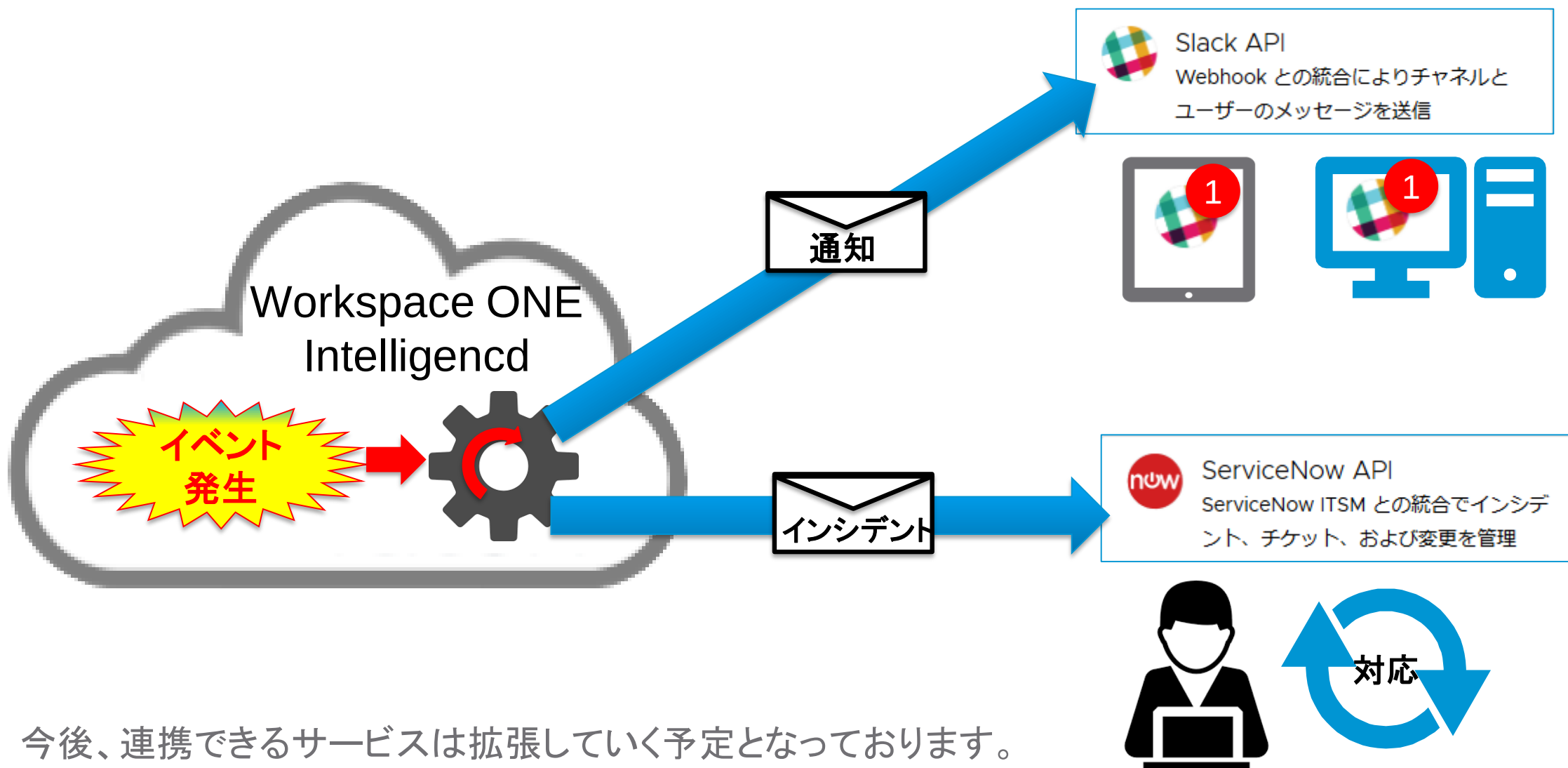


収集した情報を可視化



今後、情報収集できるサービスは拡張していく予定となっております。

そしてアクション実行までを自動化



今後、連携できるサービスは拡張していく予定となっております。

IT管理者の悩み事

下記のような課題に

- 会社支給のスマートフォンが実際に活用されているかわからない
- 導入したクラウドサービスが実際に活用されているかわからない
- 旧機種から新機種への移行が捗らない
- モバイルデバイスのコンプライアンスが徹底できない

視覚的に解決できます！

Workspace ONE Intelligence

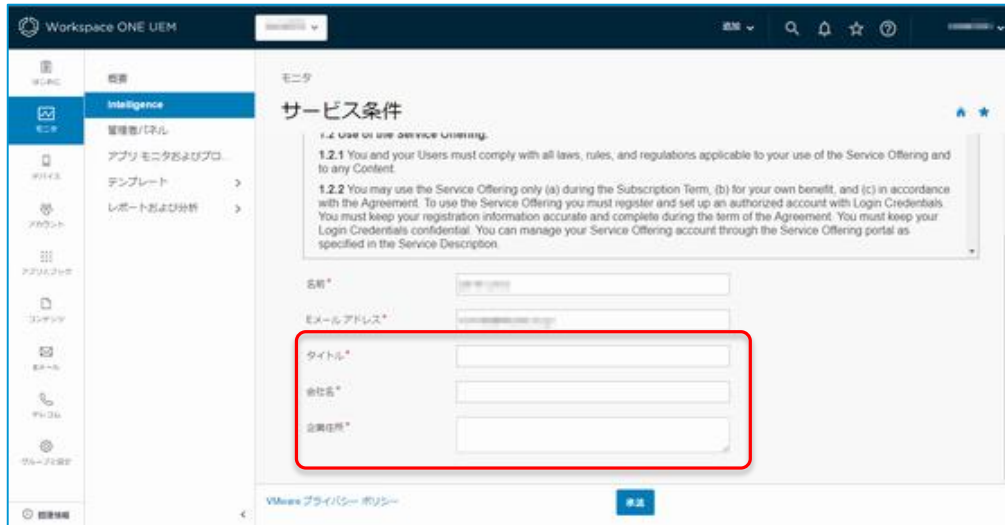
Workspace ONE Intelligence 利用開始まで



- ① Workspace ONE UEM コンソール
[モニタ] > [Intelligence] をクリックします。
[使用を開始する] をクリックします。



- ② Intelligence メニュー内
[起動] にチェックを入れます。
[次へ] をクリックします。
※2回目以降のアクセスは左図となります。



- ③ Workspace ONE Intelligence 利用規約
サービス条件 を一読します。
必須事項を入力します。
[次へ] をクリックします。



- ④ トライアル開始の案内
説明文を一読します。
[30日間のトライアルを開始] をクリックします。



⑤ 無償トライアルの使用、または、未使用

トライアルを開始する場合は必須事項を入力し、**[承諾]** をクリックします。

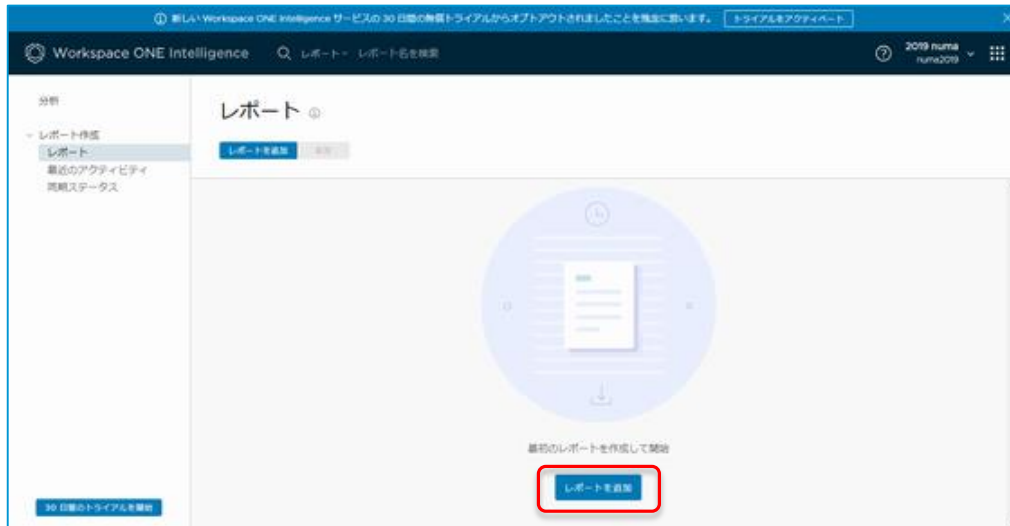
トライアルを開始しない場合は(レポート機能のみ)**[使用しない]** をクリックします。



⑥ Intelligencd (レポート機能のみ)

Workspace ONE Intelligence コンソールに遷移します。

※Workspace ONE UEM とは URL が異なります。

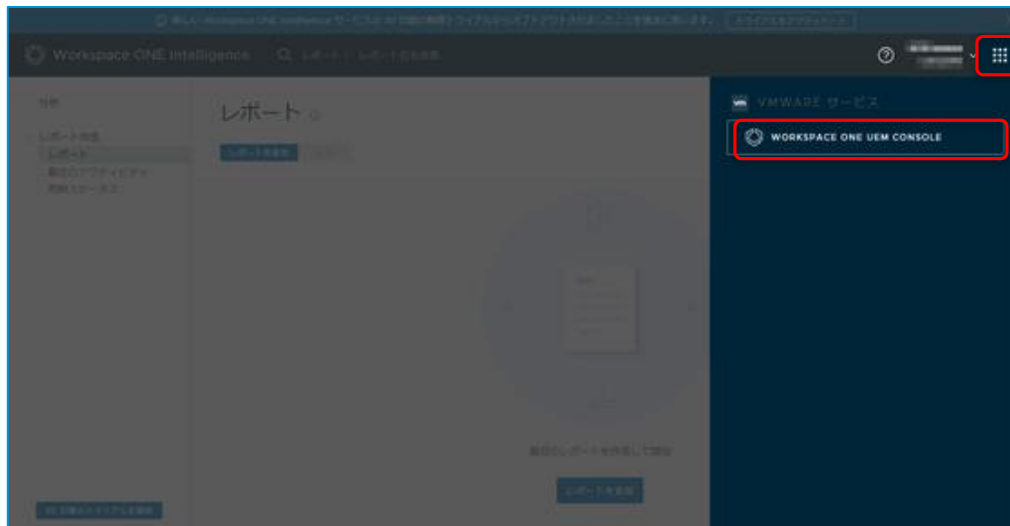


⑦ レポートの追加

[レポート作成] > [レポート] をクリックします。

[レポートの追加] をクリックします。

レポート作成のウィザードに従って、レポートを作成します。



⑧ Workspace ONE UEM コンソールへ

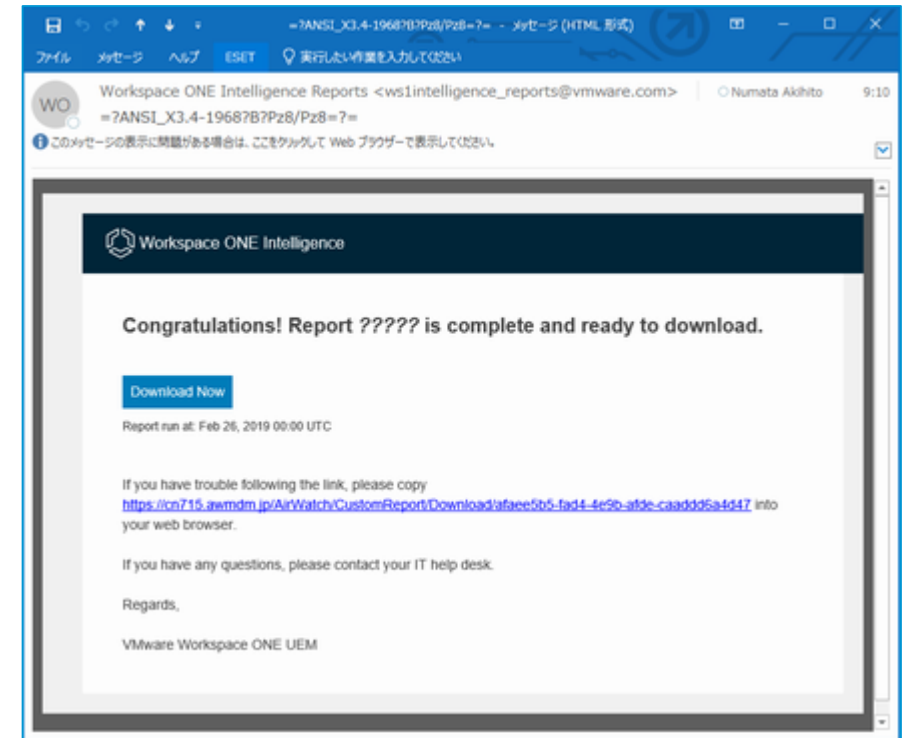
画面右上隅のメニューボタンをクリックします。

Workspace ONE UEM Console をクリックすると Workspace ONE UEM Console へ画面が遷移します。

Workspace ONE Intelligence の注意点

Workspace ONE Intelligence コンソール上の日本語表記に問題はありませんでした。しかしながら、レポートの名称などレポート通知メール本文に反映される文字列が 2byte 文字である場合に、受信したレポート通知メールの文字化けが発生します。(2019年2月26日現在)

可能な限り、Workspace ONE Intelligence コンソールでの設定は 1byte 文字でご利用いただくことをお勧めします。



Workspace ONE UEM のレポート機能は将来廃止予定

従来のレポート機能は将来廃止される予定となっております。
廃止時期は未定です。(2019年2月26日現在)

The screenshot displays the Workspace ONE UEM console interface. The left sidebar contains navigation icons for Hub, Devices, Accounts, Applications and Books, Content, Email, Telecom, and Groups and Settings. The main content area is titled 'Hub > Reports and Analysis > Reports'. It shows a 'List View' (リスト表示) of reports. A table lists various reports with columns for Name (名前), Category (カテゴリ), and Description (説明). The reports include 'New' (新規) status for items like 'Administrator Login History', 'Administrator User Roles', 'Device-specific Application Details', 'Device-specific Blacklist Application Details', 'Certificate Expiry Notification', 'Device-specific Content Details', 'Active Device Count', and 'Active Device Count by User'. The bottom of the page shows pagination information: '1 - 50を表示 / 全128項目' and '1 ページに表示する項目数: 50'.

名前	カテゴリ	説明
新規 管理者のログイン履歴	ユーザー管理	選択された日付範囲における管
新規 管理者ユーザーの役割	ユーザー管理	すべての管理者ユーザーとその
新規 デバイスごとのアプリ詳細情報	アプリケーション	デバイスをアプリケーションの
新規 デバイスごとの、ブラックリスト登録アプリまたはホワイトリスト未登録アプリの詳細情報	アプリケーション	デバイス上のブラックリスト登
新規 証明書失効間近	デバイスのインベントリ	証明書が関連付けられているデ
新規 デバイスごとのコンテンツ詳細情報	コンテンツ	デバイスおよびコンテンツ詳細
新規 アクティブなデバイスの台数	デバイスのインベントリ	過去 30 日間に使用されたデバ
新規 ユーザーごとのアクティブなデバイスの台数	デバイスのインベントリ	ユーザーが過去 30 日以内に開

目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. **Android デバイス**
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Android デバイス 構成プロファイルの改善

Work 管理対象デバイス (device owner mode) と Work プロファイルにおける制限事項の操作性を向上しました。この向上により、Androidデバイス管理機能を柔軟に制御できるようになりました。

1811

新しい Android プロファイルを追加

全般
パスコード
Chrome ブラウザ設定
制限
Exchange ActiveSync
自動更新
資格情報
アプリケーション制御
プロキシ設定
システム更新
Wi-Fi
VPN
権限
シングルアプリモード
Launcher
エンタープライズ工場出荷状態リセット保護
カスタム設定

制限

Work プロファイルの設定を構成して、業務専用アプリケーションでポリシーを管理し、デバイス全体にポリシーを適用するように、Work 管理対象デバイス設定を構成します。会社所有の個人対応デバイスには、Work プロファイルと Work 管理対象デバイス設定の両方の構成が適用されます。

デバイス機能

	Work 管理対象デバイス	Work プロファイル
工場出荷状態リセットを許可	☒	☐
スクリーンキャプチャを許可	☒	☒
Google アカウントの追加を許可する	☐	☐
Android Work アカウントの削除を許可する	☒	☐
発信通話を許可する	☒	☐
SMSの送受信を許可する	☒	☐
資格情報の変更を許可する	☒	☐
すべてのキーガード機能を許可する	☒	☐
キーガード使用中、カメラを許可する	☒	☐
キーガード使用中、通知を許可する	☒	☐

9.5

追加

工場出荷状態リセットを許可 ☒
スクリーンキャプチャを許可 ☒
Google アカウントの追加を許可 ☐
Android Work アカウントの削除を許可 ☒
発信通話を許可 ☒
SMSの送受信を許可 ☒
資格情報の変更を許可 ☒
すべてのキーガード機能を許可 ☒
キーガード使用中、カメラを許可 ☒
キーガード使用中、通知を許可 ☒

Work Managed Device
Work Managed Device/Work Profile
Work Managed Device/Work Profile
Work Managed Device
Work Managed Device
Work Managed Device
Work Managed Device
Work Managed Device
Work Managed Device
Work Managed Device
Work Managed Device

Android デバイスの追加機能

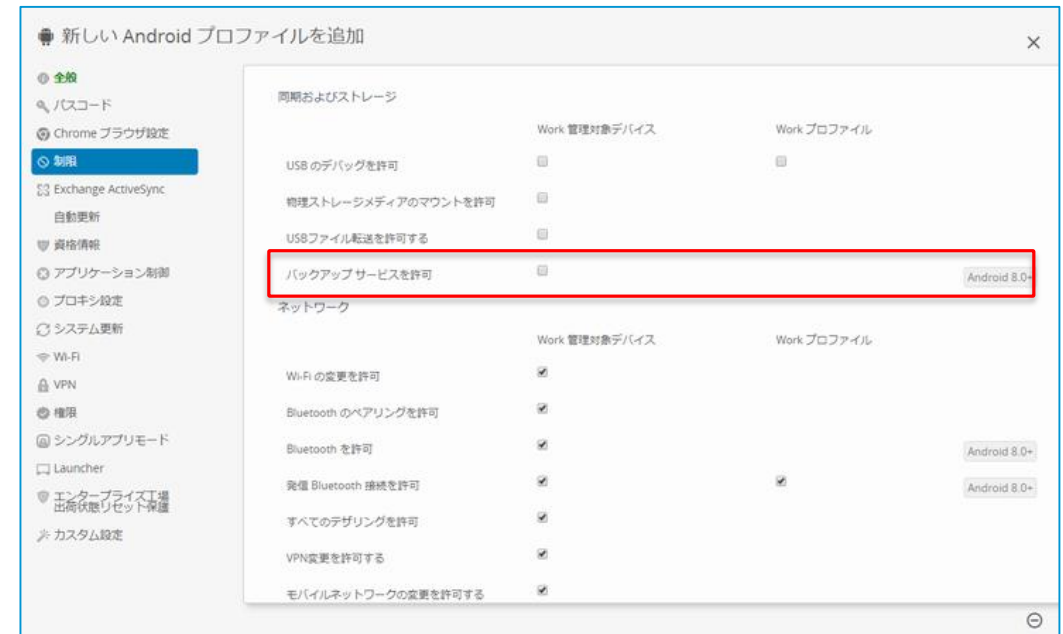
1811

- Wi-Fi プロファイルに [プロキシ] セクションが追加されました。
Android 8.0 以上



1811

- 制限プロファイルに [バックアップ サービスを許可] が追加されました。Android 8.0 以上
Googleアカウントへのバックアップを制限します。



1811

➤ 制限プロファイルに Bluetooth 関連の制限事項が追加されました。Android 8.0 以上

- Bluetooth ペアリングの制御
- Bluetooth 送信接続の制御



1811

➤ 制限プロファイルにシステム UI の制限事項が追加されました。

システム UI（トースト、アクティビティ、アラート、エラー、オーバーレイ）を防止できるようになり、デバイス上で不要なウィンドウが開くのを防止できます。



1811

➤ 構成プロファイルにパブリックアプリ更新の機能が追加されました。

- ・ 自動更新の実施
- ・ 指定した時間にのみ自動更新の実施



1811

➤ デバイス詳細画面に [保留中のシステム更新] というセクションが追加されました。
Android 8.0 以上

デバイスの使用可能な更新や最新の更新に関する情報が表示されます。



➤ バイオメトリック認証の追加 9.6

Workspace ONE アプリ (Hub, Web など) のロック解除に指紋認証などのバイオメトリック認証が利用できるように機能が追加されました。

バースコード最少文字数: 4

バースコードの有効期間(日)*: 0

バースコード履歴*: 0

バイオメトリックモード*: 有効 無効 ⓘ

[iOS] の表記が無くなりました

➤ 周辺機器の接続をログに記録する機能 9.6

デバイスに Bluetooth または USB で周辺機器を接続するたびに、Workspace ONE UEM Console がイベントを Syslog サーバーへログとして送信します。

※企業ネットワークの Syslog サーバーへ送信する場合には、別途 ACC (AirWatch Cloud Connector) が必要になります。

疑わしいアクティビティのログ

① 疑わしいアクティビティに対してログ設定を有効にすると、Bluetooth ヘッドセットと USB 充電を除くすべての Bluetooth および USB 接続がデバイスでログに記録されます。疑わしいアクティビティのログにアクセスするには、Syslog 設定が正しく構成されている必要があります [こちら](#)。

Bluetooth 接続: 有効 無効 Android 4.3+

USB 接続: 有効 無効

➤ SafetyNet Attestation API 機能追加 1810

SafetyNet Attestation API を利用してアプリが実行されている Android デバイスのセキュリティと互換性を評価できる機能が追加されました。この API を利用することにより Root 化をはじめ OS 改ざんなどを検知することが可能となりアプリを動作させる環境のセキュリティチェックが可能となります。

1810 では SafetyNet Attestation API を有効にするためには、WSO SDK のカスタム設定から手入力で行う必要がありました。1811 で改善されました。

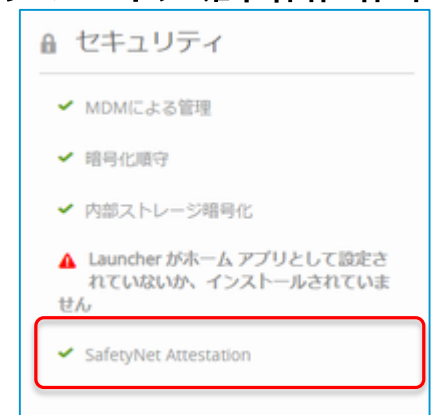
➤ SafetyNet Attestation API 用コンソールUI 追加 1811

SafetyNet アプリの検証 (SafetyNet Attestation API) 有効無効の機能がコンソールに追加されました。

コンソール設定画面



デバイス詳細画面



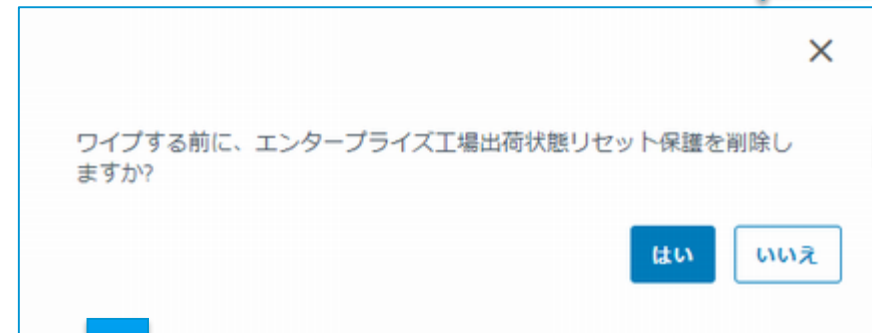
- エンタープライズ工場出荷状態リセット保護
エンタープライズ工場出荷状態リセット保護の構成プロファイルを利用することにより、Android デバイスの Device Protection (端末保護機能) の解除が行える機能が追加されました。Android 7.0 以上 + Work管理デバイス

退職する社員が利用していたデバイスの初期化などに役立ちます。

エンタープライズ工場出荷状態リセット保護 9.6



デバイスワイプコマンド実行時の確認 1810



デバイスワイプコマンド実行時



目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Apple iOS デバイス管理に関する改善

9.7

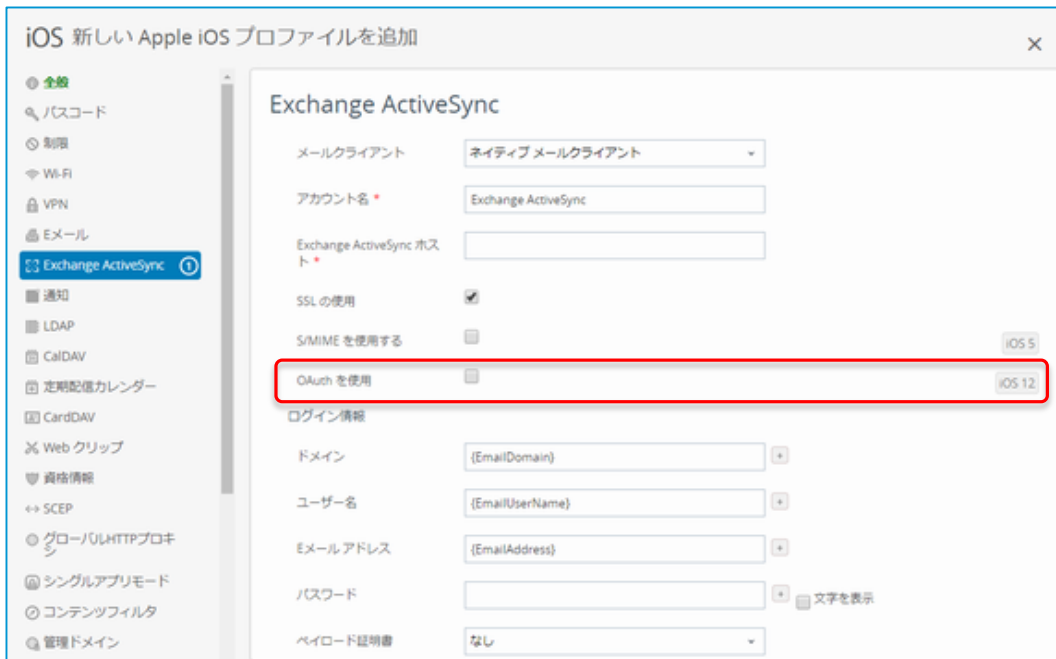
Apple iOS デバイス へのプロファイルの発行処理の効率が向上しました。この向上により、大規模に割り当てる際のプロファイルの発行処理が改善されました。

iOS デバイスの追加機能

9.7

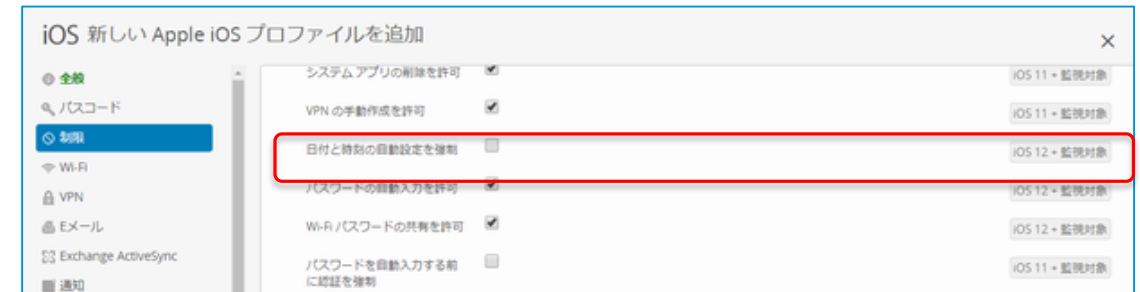
- Exchange ActiveSync プロファイルに [OAuthを使用] の項目が追加されました。iOS 12 以上

iOS 12 のネイティブ メール Exchange 接続で OAuth 認証の指定が可能となります。



9.7

- [日付と時刻] の [自動設定] 機能の制御が追加されました。iOS 12 以上 + 監視対象

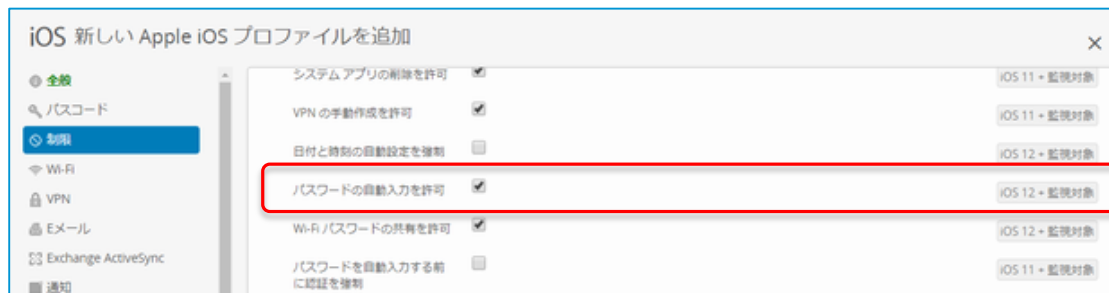


iOS デバイス側

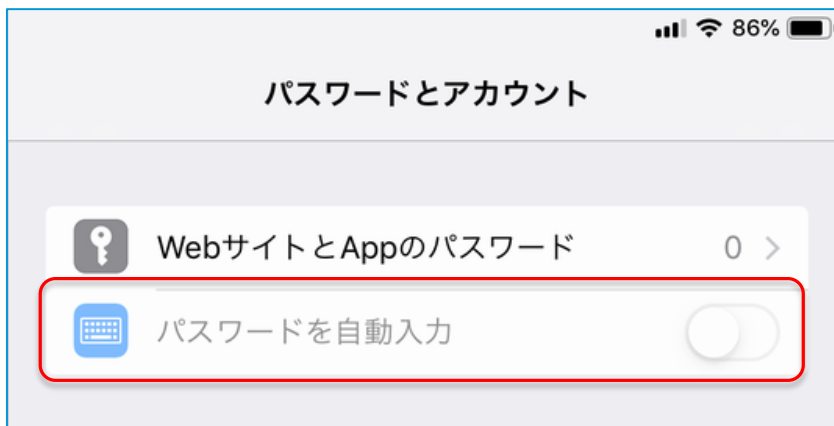


9.7

- [パスワードとアカウント] の [パスワード自動入力] 機能の制御が追加されました。
iOS 12 以上 + 監視対象

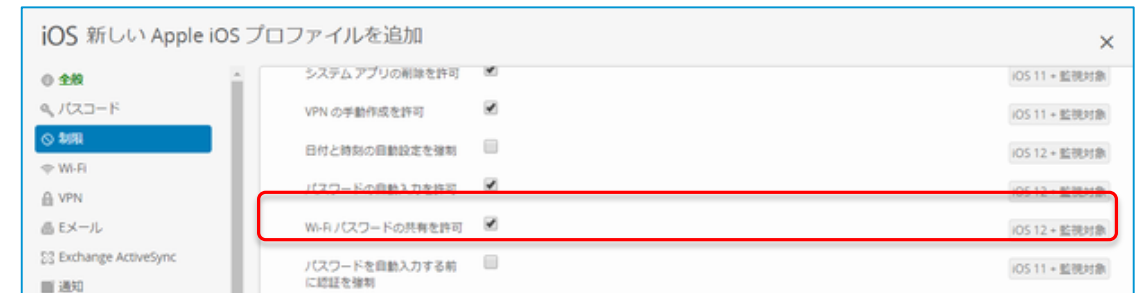


iOS デバイス側



9.7

- Wi-Fi パスワードの共有機能の制御が追加されました。iOS 12 以上 + 監視対象



9.7

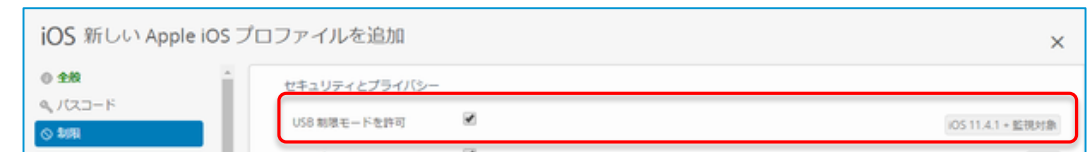
- 管理、非管理アプリの連絡先に関する制限事項が追加されました。iOS 12 以上
 - 管理対象 App が管理対象外の連絡先を編集することを許可
 - 管理対象外 App が管理対象の連絡先を読み込むことを許可

管理アプリ、非管理アプリにおける Open-in 制御と同様に連絡先についても管理アプリ、非管理アプリで制御が可能になります。



9.6

- [Touch ID とパスワード] の [USBアクセサリ] 機能の制御が追加されました。
iOS 11.4 以上 + 監視対象



iOS デバイス側



9.7

- おやすみモードがオンの場合でも、アプリの通知を重大な通知とする機能が追加されました。iOS 12 以上 + 監視対象

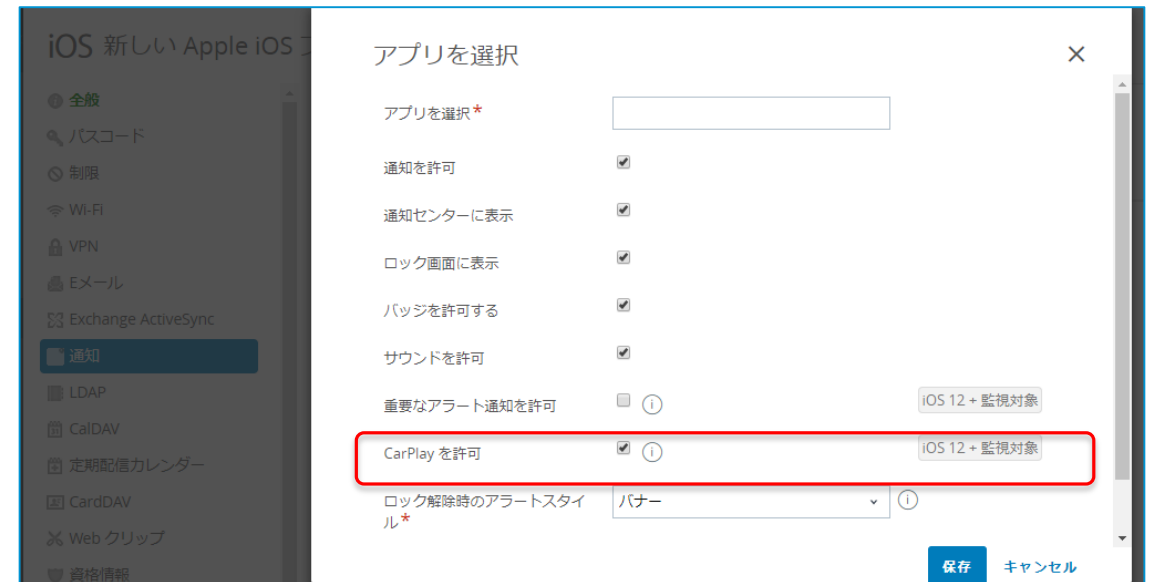
本設定はアプリ毎に行われ、アプリに通知があった際、サウンド付きで通知されます。



9.7

- デバイスが CarPlay を利用している際に、アプリの通知を表示させない機能が追加されました。iOS 12 以上 + 監視対象

本設定はアプリ毎に行われます。



デバイスワイプ時の機能追加

➤ セルラーデータの保持 9.7

デバイスワイプ実行後、当該デバイスのSIM データプランを管理コンソールに残す事が可能になりました。当該デバイスを工場出荷状態から再度加入を行っても、SIM データプランを引き継ぐ事が可能となりました。

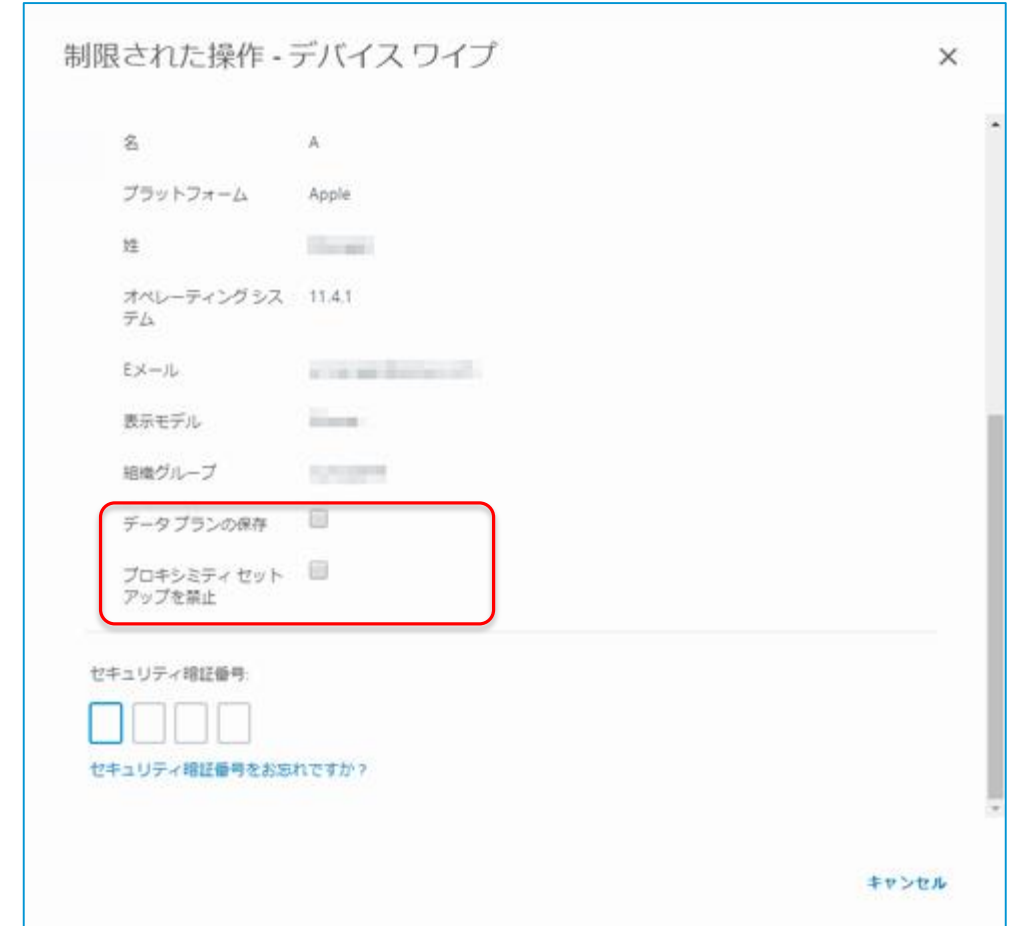
iOS 11 以上

➤ クイックスタートのスキップ 9.7

デバイスワイプ実行後、当該デバイスのセットアップ アシスタントで [クイックスタート (Proximity Setup)] を] 画面をスキップする機能が追加されました。

iOS 11.3 以上

デバイス利用者によるクイックスタートを制限することが可能です。



➤ 管理設定に Bluetooth の設定が追加されました

9.6

音声通話ローミング、データ ローミング、パーソナル ホットスポットと同様に、Bluetooth を有効 | 無効 にすることができます。

管理設定 画面

デバイスとユーザー > Apple > Apple iOS

管理設定 ⓘ

現在の設定 ☐ 継承 ☒ オーバーライド

既定の管理設定

既定の設定を次のアイテムに対して使用する ☐ 企業 - 専用 ☐ 企業 - 共有 ☐ 従業員所有 ☐ 不明

音声通話ローミング	☒	iOS 5
データローミング	☒	iOS 5
パーソナルホットスポット	☒	iOS 7
アクティベーションロック	☒	iOS 7 + 監視対象
Bluetooth	☒	iOS 11.3 + 監視対象

管理設定コマンド実行 画面

管理設定 ×

Bluetooth	☒ 有効化 ☐ 無効化
音声通話ローミング	☒ 有効化 ☐ 無効化
データローミング	☒ 有効化 ☐ 無効化
パーソナルホットスポット	☒ 有効化 ☐ 無効化
アクティベーションロックを許可	☒ 有効化 ☐ 無効化 ⓘ

➤ iOS DEPデバイス用のスキップ設定 9.6

DEP デバイスのセットアップアシスタントで、3 つのスキップ項目が追加されました。

iMessage と FaceTime

ソフトウェア アップデート

スクリーン タイム

プロファイルの編集

ホーム ボタンの反応	スキップ	スキップしない	①	iOS Only
タップしてセットアップ	スキップ	スキップしない	①	tvOS Only
スクリーンセーバー	スキップ	スキップしない	①	tvOS Only
キーボード	スキップ	スキップしない	①	iOS Only
チュートリアル	スキップ	スキップしない	①	iOS Only
Apple Watch の移行	スキップ	スキップしない	①	iOS Only
iMessage と FaceTime	スキップ	スキップしない	①	iOS Only
ソフトウェアアップデート	スキップ	スキップしない	①	iOS Only
スクリーンタイム	スキップ	スキップしない	①	iOS Only
SIM セットアップ	スキップ	スキップしない	①	iOS Only

保存 キャンセル

目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
- 6. Windows 10 デバイス**
7. Workspace ONE UEM コンソール
8. その他

Windows 10 デバイスの追加機能

1811

- 構成プロファイルに [プロキシ] が追加されました。 1803 以上

Windows OS に対して、プロキシサーバーの設定が行えるようになります。



1810

- 構成プロファイルの[Windows 更新プログラム]に機能が追加されました。

[自動承認された更新プログラム] 機能に、[機能更新プログラム] と [ドライバ] が追加されました。

この機能追加により、機能更新プログラムとドライバのダウンロードを自動承認できます。



1810

- 構成プロファイルに [キオスク] が追加されました。1709 以上

独自のカスタム XML を使用するか (1709+)、付属のデザイナ を使用して (1803+)、マルチアプリ キオスク デバイスにカスタマイズすることが可能となります。



9.7

- BitLocker の強制が改善されました。

BitLocker 暗号化の実施によって、デバイスをアップグレードまたはワイプするときに問題がありましたが、改善を行いました。リアルタイム実施を無効にすることができるようになった為、BitLocker 暗号化の問題が発生することなく、Windows デバイスをアップグレードできます。



➤ 位置情報サービスの機能変更 1811

Windows デスクトップ デバイスの GPS サポートを強化しました。Microsoft Store から配布されている AirWatch Agent ではなく OMA DM を通じて位置情報データを取得するように機能が変更しました。

➤ デバイスワイプのレベルオプション追加 1811

デバイス ワイプのレベルを選択できるように、[デバイス ワイプ] コマンドを強化しました。従来のデバイス ワイプに加え、ユーザーが回避できない [保護対象のワイプ] を実行できるようになりました。さらに、プロビジョニング データをバックアップしてデバイスのワイプ後に再適用する [ワイプとプロビジョニング データの保持] アクションを実行することもできます。

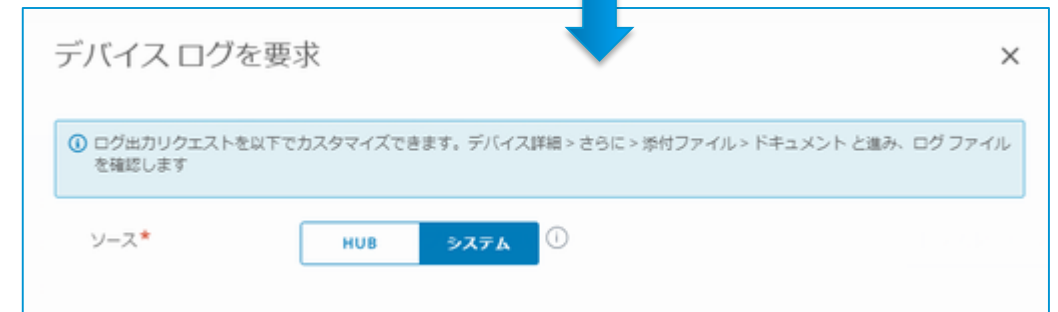


➤ 管理コマンドの追加 1811

[デバイス詳細] 画面のアクション メニューに、デバイスをリモートで再起動できる [デバイスの再起動] ボタンが追加されました。この機能はデバイスを Workspace ONE UEM に加入させたままで工場出荷時の設定にリセットできる機能です。

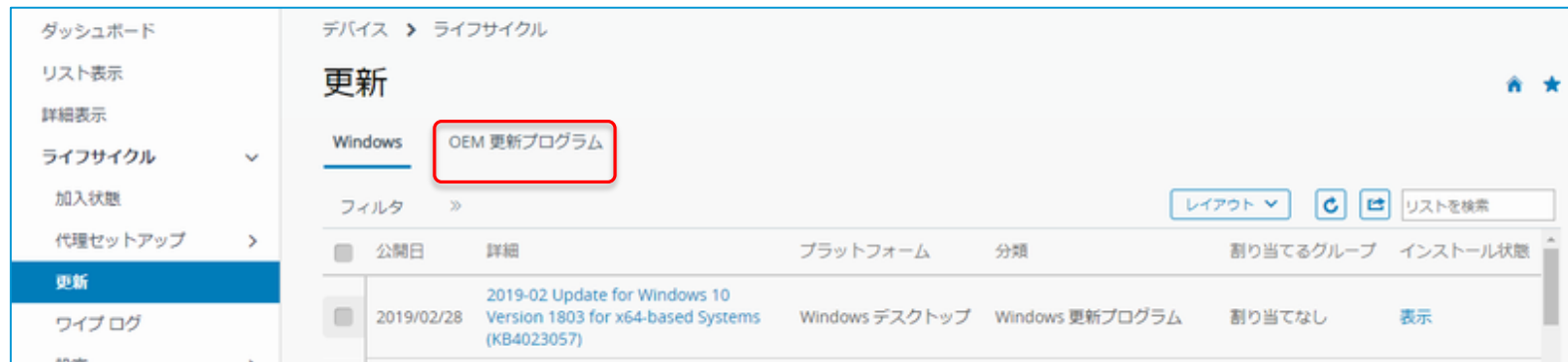
➤ ログ収集機能の追加 1811

トラブルシューティングやサポートの提供のためにデバイスからのデバイスの詳細ログを要求できるように、機能を追加しました。



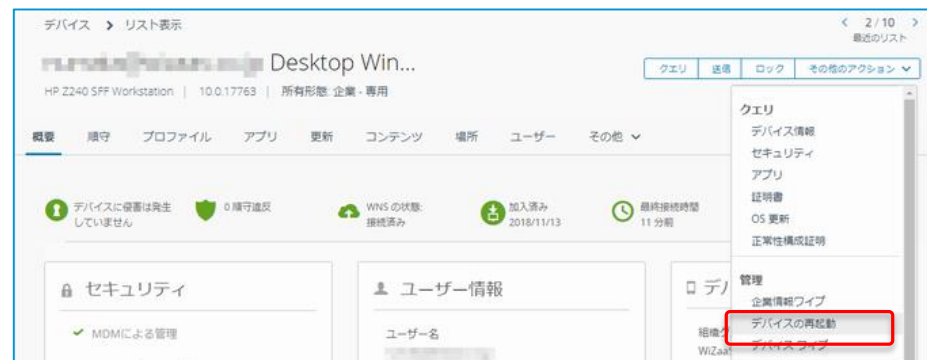
➤ [OEM 更新プログラム] 表示リストの追加 9.6

展開済みの OEM 更新プログラムがすべて表示されるようになりました。この画面では、オーディオドライバ、チップセットドライバ、BIOS 更新プログラムなどの種類別に更新プログラムをフィルタリングできます。



➤ 管理コマンドの追加 9.6

[デバイス詳細] 画面のアクションメニューに、デバイスをリモートで再起動できる [企業情報リセット] ボタンが追加されました。



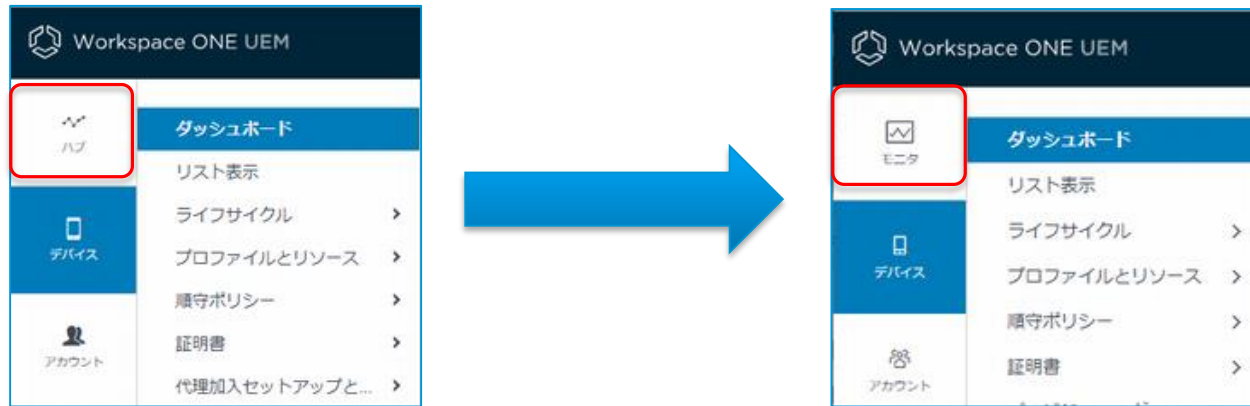
目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. **Workspace ONE UEM コンソール**
8. その他

Workspace ONE UEM コンソールの変更

➤ コンソール画面のメニュー表記の変更 1810

UEM コンソール画面の [ハブ] メニューが [モニタ] という名前に変更されます。



➤ AirWatch Cloud Connector の変更 1810

- ・システム設定画面では、[VMware Enterprise Systems Connector] が [Cloud Connector] に変更されます。
- ・VMware AirWatch Cloud Connector および VMware Identity Manager Connector のインストーラーが個別に提供されるように変更されます。
 - VMware AirWatch Cloud Connector: Workspace ONE UEM コンソールからダウンロードします。
 - VMware Identity Manager Connector: お客様がご利用いただいているVMware社のアカウント情報によりインストーラーの入手方法が異なりますので、インストーラーが必要なお客様は弊社サポート窓口へお問合せください。

➤ WSO SDK のメニューの変更 9.7

既定の SDK プロファイルの [侵害対策] と [オフライン アクセス] は [セキュリティ ポリシー] ページに移動されます。

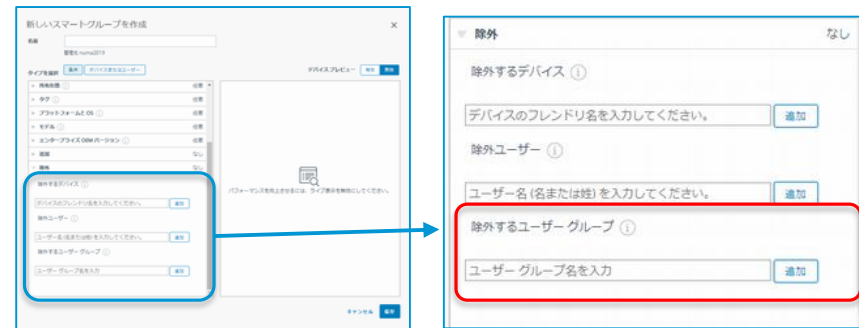


※AirWatch 9.3 の場所に戻ります。

Workspace ONE UEM コンソール機能追加

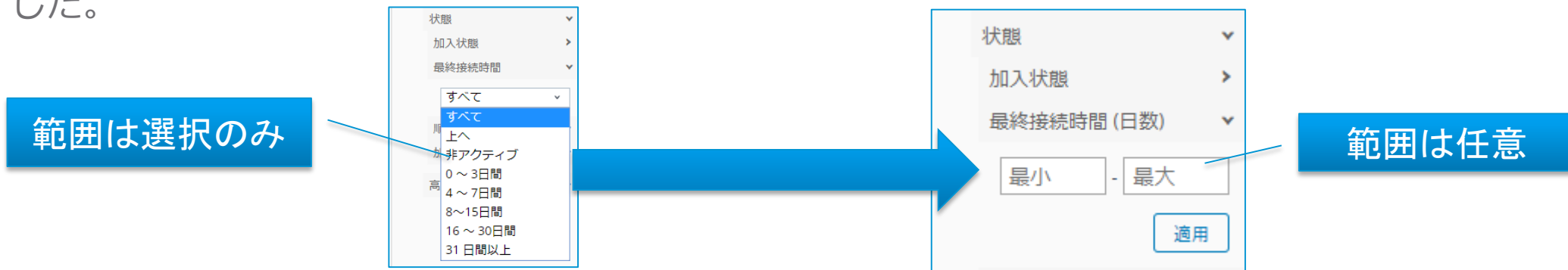
▶ スマートグループの機能強化 9.7

より柔軟なグループ分けを行えるようスマートグループにユーザーグループの除外設定が行えるよう機能が追加されました。



▶ デバイスリスト表示のフィルタリング機能強化 9.7

[最終接続時間]のフィルタリング機能に日数を指定してフィルタリングが行えるよう機能が追加されました。



▶ VMware Tunnel デバイス トラフィックの機能強化 9.7

すべての子組織グループで [デバイス トラフィック規則] 設定を継承するかオーバーライドするかを選択できるよう機能が追加されました。

システム > エンタープライズ統合 > VMware Tunnel

ネットワーク トラフィック規則

デバイス トラフィック規則 サーバ トラフィック規則

現在の設定 ☒ 継承 ☐ オーバーライド

VMware Tunnel を使用してネットワーク トラフィックをトンネル、ブロック、またはバイパスする規則を追加してください。

注: これらの規則は、Android デバイスおよび iOS デバイス向け VMware Tunnel の「アプリベース トンネル」コンポーネントのみに適用されます (iOS の場合は、App Store で入手できる VMware Tunnel クライアント アプリを使用してください)。モバイル デバイスにインストールされた VMware Tunnel アプリは、このページで指定した規則に従って、ネットワーク トラフィックをトンネル、ブロック、またはバイパスします。さらに、ネットワーク トラフィックを貴社ネットワークで構成されたカスタム Web プロキシにルーティングするオプションもあります。

ランク	アプリケーション	アクション	送信先ポート名
ランク 1	Safari 以外のすべてのフラグ付きアプリ	Tunnel	

保存

▶ デバイス リスト表示画面の改善 9.6

[アセット番号] 列で並べ替えるためのオプションを削除したことで、デバイス リスト表示画面のパフォーマンスが向上しました。

➤ SAML 認証の有効化機能の追加 9.6

v9.5 では、管理者/ユーザーの一方だけに対しても、その両方に対しても SAML 認証を有効にすることができました。V9.6 から管理者、加入、セルフ サービス ポータルのそれぞれに対して SAML 認証を使用するかどうかを選択できるようになりました。この機能追加により、セルフサービスポータルに対して SAML 認証を有効にし、デバイス加入には有効にしない、柔軟な構成が可能となります。

システム > エンタープライズ統合

ディレクトリ サービス ⓘ

サーバ ユーザー

現在の設定 ☐ 継承 ☒ オーバーライド

LDAP

ディレクトリタイプ* なし ⓘ

ID サービスに Azure AD を使用

認証に SAML を使用

以下のユーザーに対し SAML 認証を有効化* ⓘ

新しい SAML 認証エンドポイントを使用 ⓘ

v9.5

システム > エンタープライズ統合

ディレクトリ サービス ⓘ

サーバ ユーザー

現在の設定 ☐ 継承 ☒ オーバーライド

LDAP

ディレクトリタイプ* なし ⓘ

ID サービスに Azure AD を使用

認証に SAML を使用

以下のユーザーに対し SAML 認証を有効化* ☐ 管理者 ⓘ ☒ 加入 ☒ セルフ サービス ポータル ⓘ

新しい SAML 認証エンドポイントを使用 ⓘ

➤ セルフサービス ポータル内のセキュリティ対策を強化 9.6

トークンを使用して加入するアカウントのみを対象とした、次のセキュリティ機能がセルフサービスポータルに実装されました。

- [デバイスを追加] 画面と [アカウント] 画面の [E メール アドレス] フィールドおよび [電話番号] フィールドが読み取り専用になりました。
- [加入メッセージを表示する] の基本アクションは利用できなくなりました。
- [加入メッセージを再送信する] の基本アクション フォームには、読み取り専用のメール アドレス テキストボックスと電話番号テキスト ボックスが表示されます。

デバイスを登録する

フレンドリ名*

プラットフォーム* 選択してください

モデル 選択してください

OS 選択してください

デバイス所有形態* なし

メッセージタイプ* なし Eメール SMS QRコード

Eメール アドレス* <<< 読み取り専用

トークンベースの加入が有効になっている場合は、セキュリティを強化するために、ユーザー アカウントで指定されているメール アドレスに加入の詳細が送信されます。

メッセージテンプレート非表示

アカウント

概要 S/MIME 利用規約 アプリ

グループ ID

ユーザー名

名*

ミドルネーム

姓*

電話番号 <<< 読み取り専用

Eメール アドレス* <<< 読み取り専用

Eメールのユーザー名

保存 キャンセル

加入メッセージを再送信する

 加入保留中

メッセージタイプ* Eメール SMS QRコード

電話番号* <<< 読み取り専用

トークンベースの加入が有効になっている場合は、セキュリティを強化するために、ユーザー アカウントで指定されている電話番号に加入の詳細が送信されます。

加入メッセージを再送信する

 加入保留中

メッセージタイプ* Eメール SMS QRコード

Eメール アドレス* <<< 読み取り専用

トークンベースの加入が有効になっている場合は、セキュリティを強化するために、ユーザー アカウントで指定されているメール アドレスに加入の詳細が送信されます。

VMware 社の取り組み

VMware 社は、お客様のご意見、ご要望が重要であると考えています。お客様の声に適切にお応えできるように、フィードバック（オプション）の収集にさらに力を注いでいます。VMware 社がより深くお客様を理解し、そのニーズに基づいて製品を改良するためのシステムとなっております。

ご協力の程、よろしくお願いいたします。



フィードバックを共有

お客様の経験を評価して、当社にフィードバックをお送りください。お客様のアカウントに関して当社が保有しているその他の情報があればあわせて活用して、問題を修正し、製品およびサービスを改善し、お客様に推奨事項をご提供するために役立てさせていただきます。お客様がご連絡先情報を当社にすでにご提供いただいている場合、お客様のご連絡先情報は、お客様のフィードバックについて、VMware がお客様をフォローアップする目的でのみ使用されます。

Workspace ONE UEM にはどの程度満足していますか。

非常に 不満 1 2 3 4 5 6 7 非常に 満足

他に、"Workspace ONE UEM に関するフィードバックはありますか。ご意見をお聞かせください。

お客様ご自身の責任において、フィードバックに機密情報、部外秘情報、または個人情報が確実に含まれないようにしてください。このフォームは、Workspace ONE UEM に関するフィードバックのみを対象としています。サポートが必要な場合や、お問い合わせの際には、サポート センターまでご連絡ください。

詳細については、VMware のプライバシー通知 (<https://www.vmware.com/help/privacy.html>) をご覧ください。

終了

エラー メッセージの改善により、発生した問題の原因をより適切に通知できるようになりました。 1811

物事が思いどおりに進まないでフラストレーションが溜まるものです。VMware はお客様のフラストレーションを軽減できるように、エラー メッセージの改善に取り組んでいます。



目次

1. Workspace ONE UEM 管理者パスワード
2. Workspace ONE Intelligent Hub の新機能
3. Workspace ONE Intelligence
4. Android デバイス
5. iOS デバイス
6. Windows 10 デバイス
7. Workspace ONE UEM コンソール
8. その他

Android Enterprise デバイスの加入識別子の変更

概要

Android Enterprise に完全管理対象デバイスを加入する一般的な方法のひとつに、Google 社の DPC 識別子の利用があります。これにより、適切な EMM が自動的にプロビジョニングされます。現在、この識別子は「**afw#airwatch**」ですが、2019 年 4 月 2 日より、新しいものに変更されます。新しい識別子は、Workspace ONE UEM でデバイス管理に使用されるアプリの新名称である Workspace ONE Intelligent Hub に合わせて、「**afw#hub**」になります。

影響の範囲

すでに加入済みのデバイスへの影響はありません。

Google 社によって識別子が「**afw#hub**」へ変更された後に、従来の識別子である「**afw#airwatch**」を使用して新たにデバイスを加入しようとする、識別子を判別できずエラーが返されます。4 月 2 日以降、DPC 識別子を利用しての新規加入には「**afw#hub**」を使用する必要があります。エンドユーザー向けにメッセージやドキュメントを作成している場合は、どの識別子をいつ使用するかを通知するためにそれらを更新する必要があります。

Apple VPP アプリの割り当て数の削減（予定）

概要

Apple Business Manager (旧 VPP) との統合により、Workspace ONE UEM コンソールの、特定のスマート グループへの「ライセンス割り当て」オプションが削除されます。ただし、この変更によって機能が失われるわけではありません。管理者やユーザーに対して想定される唯一の影響は、アプリのライセンス割り当て数を対応するスマート グループのデバイス数より少なく設定していても、展開モードが自動インストールになっていると、当該変更後はアプリがライセンス割り当て数を超過してインストールされるようになることです。これを回避するには、保留中のライセンス割り当て数を増やすか、展開モードをオンデマンドに設定してください。



削除予定

背景

Apple Business Manager と場所ベース トークンのリリースで、Apple 社は各アプリに必要なライセンスを場所ベース トークンに割り当てる機能を導入しました。また、このリリースには割り当てたライセンスを、ある場所ベース トークンから他の場所ベース トークンに再割り当てする機能も含まれています。これらの機能を活用してライセンス アカウントとライセンス割り当ての管理を簡素化することにより、より簡単な操作性、より良いパフォーマンス、複雑さの軽減を実現するため、将来の Workspace ONE UEM リリースで特定のスマート グループへのライセンス割り当てフィールドを削除する予定です。

影響の範囲

この変更に関連する影響はひとつだけです。現在ライセンス割り当て数が、スマート グループのデバイス数より少なく設定されているアプリの場合（例：100 台のデバイスを含むスマート グループに 200 ライセンスを有するアプリが割り当てられているが、ライセンス割り当て数は 50 のみの場合）、展開モードが自動に設定されていると、当該変更後はライセンス割り当て数を超過して残りのデバイスにアプリがインストールされるようになります。2019 年に予定されている変更について管理者の方にお知らせしています。今後、ライセンスの割り当てが不要となる新しいユーザー操作性の詳細についてお知らせしてまいります。

サポート終了のお知らせ

サポート終了サービス

- Windows デスクトップ用 VMware Content Locker Outlook アドイン
- Windows デスクトップ用 VMware Content Locker
 - ※ UEM Console からダウンロードした VMware Content Locker が対象になります。

サポート終了期日

2018年4月1日

お客様への影響

- Windows デスクトップ用 VMware Content Locker Outlook アドイン

現在VMware Content Locker Outlookアドインを利用しているすべてのお客様は、一般サポート期間が終了する前に、Outlookアドインを必要とするワークフローの移行オプションをご検討ください。
- Windows デスクトップ用 VMware Content Locker

Microsoft Store から入手可能な VMware Content Locker は引き続きサポートされます。ご利用のお客様は Microsoft Store から VMware Content Locker 入手と移行を行う事をご検討ください。

Workspace Gate サービスのご紹介

株式会社ウィザースでは Workspace ONE ゲートウェイサーバーのクラウド構築・運用をサポートするサービスをご提供しています。

サービス概要

「Workspace ONE(AirWatch)を短期間でスムーズに導入したい」、「Office365などのクラウドサービスと連携させたいが設定方法がわからない」など導入構築時の悩みや、「Workspace ONE(AirWatch)運用の相談窓口がほしい」などの困りごとはありませんか？

「Workspace Gate構築/Workspace Gate運用サービス」は、弊社が長年培ってきたノウハウを生かして、ゲートウェイ構築と運用にまつわる悩みを解消いたします。

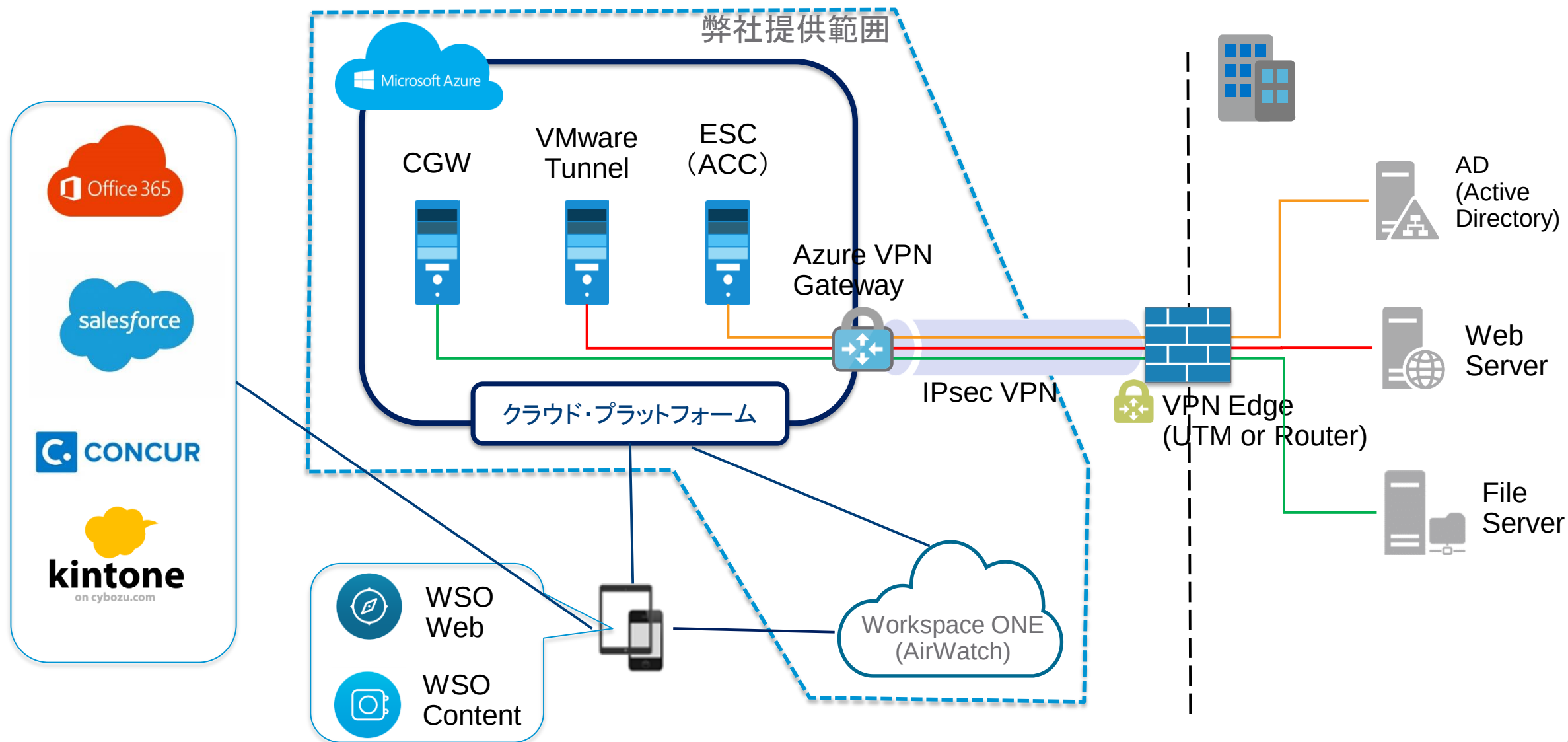
Workspace Gate構築サービス/Workspace Gate運用サービス

社内システムとの連携に必要なオンプレミスのゲートウェイサーバー

- Secure Email Gateway(SEG)
- Cloud Connector & vIDM Connector
- VMware Tunnel
- Content Gateway(CGW)

をAzure/AWSなどのSaaSでご提供いたします。設計・構築から運用までワンストップでご提供します。社内にオンプレミスサーバーを増やしたくないお客様に最適です。

Workspace Gate サービスの概念図



Workspace ONE UEM 1811 リリーススケジュール

弊社提供の VMware Workspace ONE UEM 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 1811 へのアップグレード作業

日程:

2019年3月14日 午後 11時～

ありがとうございました

WiZaaS

※各社各種ロゴは各社の商標または登録商標です。