

AirWatch 8.4 アップデート

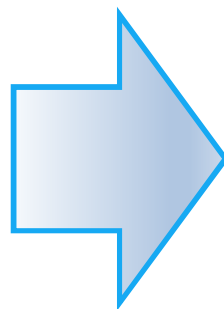
2016年11月16日
株式会社データコントロール

iOS MDMプロファイルの表記変更

<変更点>

iOSデバイスにおけるMDMプロファイルの表記が変更されます。

AW 8.3



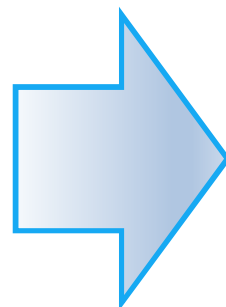
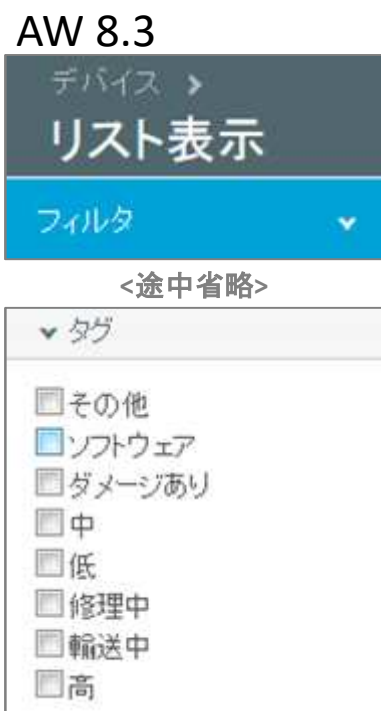
AW 8.4



デバイスリストのフィルタ

<変更点>

- ・フィルタ機能の[タグ]のチェックボックスを検索テキストボックスに置き換え、操作性を向上しました。
- ・フィルタ機能の[ユーザーグループ]の自動入力機能が最適化され、操作性を向上しました。



デバイス管理 加入機能

<追加機能>

- ・組織グループにおける、加入可能なデバイスの台数を制限する機能が追加されました。加入台数を制限は、設定を行った組織グループとその下位の組織グループに適用されます。

The screenshot shows the VMware AirWatch Datacontrol console interface. The left sidebar contains a navigation menu with categories like 'システム' (System), 'デバイスとユーザー' (Devices and Users), 'アプリ' (Apps), and 'コンテンツ' (Content). Under 'デバイスとユーザー', the '全般' (General) section is expanded, showing options like '加入' (Join), 'フレンドリ名' (Friendly Name), '参照フィールド' (Reference Fields), 'メッセージテンプレート' (Message Templates), '通知' (Notifications), 'プライバシー' (Privacy), '共有デバイス' (Shared Devices), and '高度な設定' (Advanced Settings). The main content area is titled 'デバイスとユーザー / 全般 / 加入' and has several tabs: '認証' (Authentication), '利用規約' (Terms of Use), 'グループ化' (Grouping), '制限事項' (Restrictions), 'プロンプト表示 (オプション)' (Prompt Display (Optional)), and 'カスタマイズ' (Customization). The '制限事項' tab is active. Below the tabs, there are radio buttons for '現在の設定' (Current Settings) with options '継承' (Inherit) and '上書き' (Override). The '加入制限' (Join Limit) section is highlighted with a red dashed box. It contains a 'ユーザーアクセスコントロール' (User Access Control) section with two checkboxes: '加入を既知のユーザーのみに制限' (Restrict to known users only) and '加入を構成済みのグループのみに制限' (Restrict to configured groups only). Below these is a text box with the description: 'この組織グループとその下のサブグループへの加入デバイス数に上限を設定します。' (Set a limit on the number of devices that can join this organization group and its subgroups). To the right of this text are '有効' (Enabled) and '無効' (Disabled) buttons. At the bottom, there is a 'デバイス数上限を入力' (Enter device count limit) field with the value '10'.

ディレクトリサービスとユーザ管理

<追加機能>

- ・SAML認証を、管理者のみ、ユーザのみ、および、管理者とユーザに許可する機能が追加されました。この機能によりSAML認証を柔軟に対応することが可能となりました。

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 グループ

<途中省略>

AZURE ACTIVE DIRECTORY

<途中省略>

認証に SAML を使用 有効 無効

以下のユーザーに対し SAML 認証を有効化: * 管理者 ユーザー 双方 i

新しい SAML 認証エンドポイントを使用する 有効 無効 i

Androidデバイス 順守ポリシー

<追加機能>

- ・Androidデバイスに適用される順守ポリシーにおいて、Androidデバイス属性であるセキュリティパッチバージョンを仕様する機能が追加されました。

順守ポリシーを追加

1 ルール 2 アクション 3 割り当て 4 概要

ここで指定するルール すべて に合致する

セキュリティパッチのバージョン が次の日付より前 YYYY/MM/DD 0:00

10月 2016

月	火	水	木	金	土	日
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

ルールを追加する

キャンセル 次へ

レポート機能 機能削除

<機能削除>

・レポート出力からPDFとExcel形式のサポートが削除されました。新規レポートにはPDFとExcel形式が利用できませんのでご注意ください。

※既存の定期配信は編集を行わない限り、PDF、Excelのように機能しますが、一旦編集すると、CSV形式に変更されます。

・エラーの状態またはアクティブでない状態の定期配信を編集し、エラーを修正し、再保存する機能を追加しました。

AW 8.3

デバイス インベントリ概要

組織グループ ✕
ここに入力して新しいグループを追加

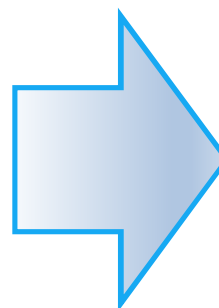
すべて選択

休止状態の閾値 (分)*

レポート形式を選択



ダウンロード PDF形式でプレビュー キャンセル



AW 8.4

デバイス インベントリ概要

組織グループ ✕
ここに入力して新しいグループを追加

すべて選択

休止状態の閾値 (分)*

レポート形式

スプレッドシート (コンマ区切り値)

サンプルレポート

ダウンロード キャンセル

プライバシー設定

<追加機能>

・デバイスの所有形態における、デバイスパスコード消去/デバイスロックが選択できるようプライバシー設定に機能が追加されました。

※デフォルト設定は従業員所有(BYOD向け)のみOFFとなります。

	企業-専用	企業-共有	従業員所有	割り当てなし
コマンド				
デバイスワイプ	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
デバイスパスコード消去/デバイスロック	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
ファイルマネージャへのアクセス *	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
リモート操作 *	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
レジストリ マネージャ **	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

* AndroidとWinMoデバイスにのみ適用
** WinMo デバイスのみに適用

プライバシー設定のセキュリティ

<追加機能>

・プライバシー設定を変更後保存する際、管理者のセキュリティ暗証番号の入力が必要になりました。

※デフォルト設定は有効ですが、無効に設定することが可能です。

制限された操作 - プライバシー設定を変更する

プライバシー設定を変更する処理を実行しようとしています。以下のすべての情報を確認してからセキュリティ暗証番号を入力して続行してください。 ⓘ

プライバシー設定が更新されると、収集され保管される個人データやデバイス上で実行される操作も変更される場合があります。さらに、「ユーザーフレンドリーなプライバシー通知」割り当てが変更された場合には、インストールまたは削除のためにウェブクリッププロファイルがキューに登録される場合があります。

セキュリティ暗証番号を入力

[セキュリティ暗証番号をお忘れですか？](#)

キャンセル

AirWatch 8.4 & iOS 10追加機能①

<追加機能> [監視対象]のみ

- ・Bluetoothの設定変更を許可/拒否の設定を行うU/Iが追加されました。



AirWatch 8.4 & iOS 10追加機能②

<追加機能>

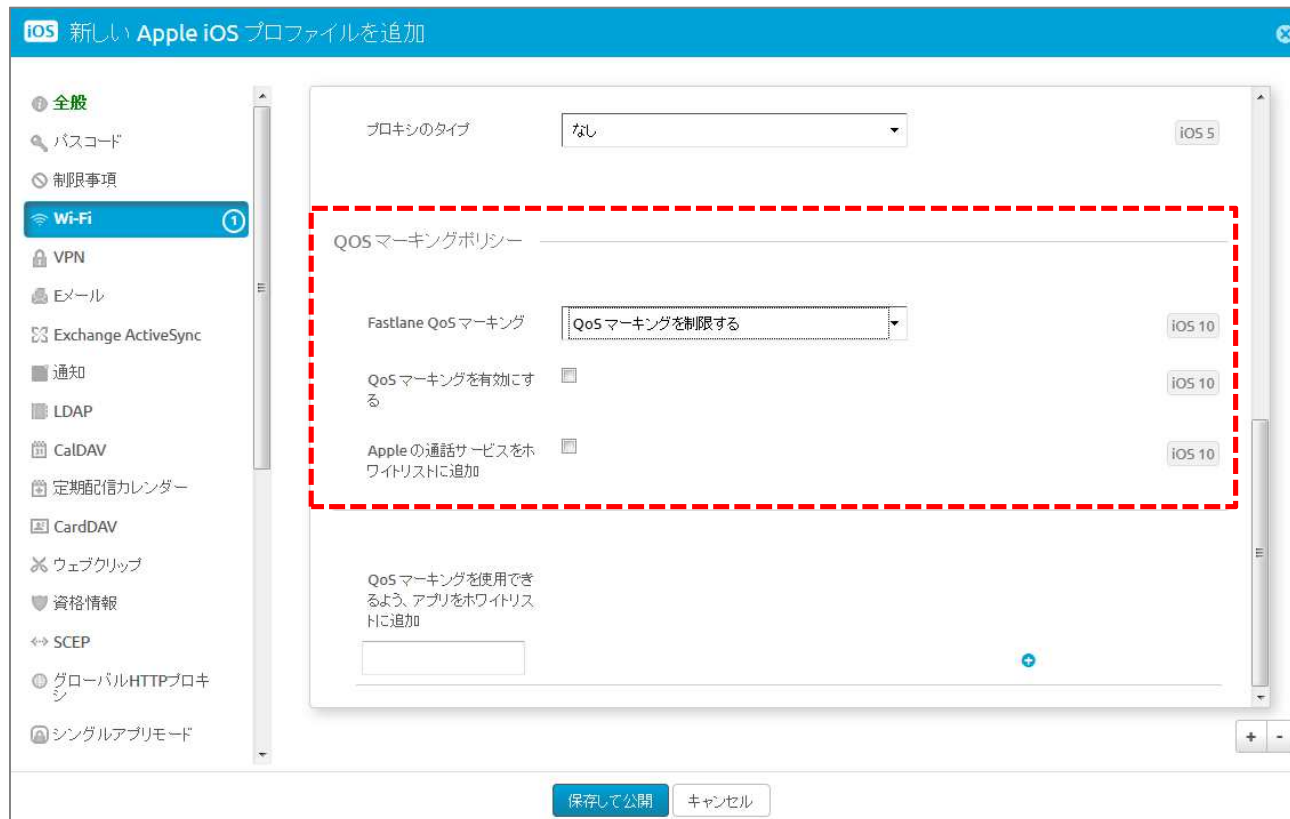
- ・iOSネイティブメーラーに対する構成プロファイル/ActiveSyncの設定に、デフォルトで利用する音声通話アプリ(Skye for Businessなど)が指定できる設定のU/Iが追加されました。



AirWatch 8.4 & iOS 10追加機能③

<追加機能>

- ・構成プロファイル/Wi-Fiの設定に、QoSマーキングポリシー(優先制御)が指定できる設定のU/Iが追加されました。



テレコムアプリケーションの向上

<機能修正>

- ・Androidデバイスにおけるテレコム情報を収集するサービスアプリケーションの安定性と信頼性の向上を行いました。

デバイスとユーザー / Android / サービス アプリケーション ⓘ

現在の設定 継承 上書き

サービスアプリを必須にする

Play ストアからサービスアプリをプッシュする

常に最新バージョンのテレコムサンプラーを使用

テレコムサンプラーバージョン

常に最新バージョンの AirWatch Launcher を使用する

AirWatch Launcher バージョン

サブグループの許可* 継承のみ 上書きのみ 継承または上書き

保存

McAfee Web Gatewayとの連携

<機能追加>

・ICAP プロキシ経由のコンテンツマルウェア検知を実行する機能を実装、さらにICAP プロバイダ(McAfee Web Gateway) との連携を追加しました。

企業リポジトリにコンテンツをアップロード、ダウンロードする前に、マルウェアのスキンの機能が拡張されました。

Content Gateway 構成

ICAP プロキシ構成

貴社の企業リポジトリにコンテンツをアップロードしたりコンテンツをダウンロードする前に、マルウェアが含まれていないか AirWatch ICAP プロキシを構成してスキャンします。

ICAP リクエストスキャン 有効 無効 ⓘ

ICAP リクエストアドレス * ⓘ

ICAP リクエストポート *

ICAP 応答スキャン 有効 無効 ⓘ

ICAP 応答アドレス * ⓘ

ICAP 応答ポート *

※McAfee Web Gateway v7.5.2.7.0 以降がサポートされています。

Apple iOSデバイスのサポートについて

VMware AirWatchより、Apple iOSデバイスのサポートバージョンのお知らせとなります。Apple社のiOS 10リリースによりAirWatchのサポートバージョンは下記となります。

AirWatch プロダクト	サポート iOS Version
AirWatch アプリケーション Browser, Content Locker, Inboxなど	iOS 9+ (iOS 9以上)
AirWatch Agent / Container	iOS 8+ (iOS 8以上)
AirWatchのMDM機能サポート	iOS 7+ (iOS 7以上)

AirWatch 8.4 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: AirWatch 8.4へのアップグレード作業
日程: 2016年11月17日 午前 0時～

ありがとうございました。

※VMware各種ロゴはVMware, Inc.の商標または登録商標です。