

Workspace ONE UEM 管理コンソールガイド(機能編)

Workspace ONE UEM 2109 Web UI ベース

2022 年 1 月 21 日
株式会社ウィザース

改訂履歴

ver.	発行日	改訂履歴
1.00	2013 年 11 月 20 日	初版発行
2.00	2014 年 4 月 1 日	第二版発行
3.00	2014 年 10 月 16 日	第三版発行
4.00	2015 年 1 月 7 日	第四版発行
5.00	2015 年 8 月 12 日	第五版発行
6.00	2016 年 1 月 14 日	第六版発行 (Ver8.2 対応)
7.00	2016 年 7 月 19 日	第七版発行
8.00	2016 年 10 月 1 日	第八版発行
8.01	2016 年 11 月 16 日	第八版更新
9.00	2017 年 4 月 24 日	第九版更新
10.00	2018 年 7 月 12 日	第十版発行 (Ver9.2 対応)
11.0	2018 年 8 月 28 日	第十一版発行 Workspace ONE UEM Ver9.5 対応
12.0	2019 年 1 月 25 日	第十二版発行 Workspace ONE UEM Ver18.11 対応
13.0	2019 年 11 月 7 日	第十三版発行 Workspace ONE UEM 1909 版
14.0	2020 年 7 月 8 日	第十四版発行 Workspace ONE UEM 2005 Web UI ベース版
15.0	2021 年 1 月 14 日	第十五版発行 Workspace ONE UEM 2011 Web UI ベース版
16.0	2022 年 1 月 21 日	第十六版発行 Workspace ONE UEM 2109 Web UI ベース版

※ バージョン 9.4 より、コンソールの名称が“AirWatch Console”から“Workspace ONE UEM Console”に変更されました。

目 次

1	本書について	1
2	ご利用にあたっての準備	2
3	機能別ガイドの概略	3
3.1	システム構成	3
3.2	アプリケーションの管理	3
3.3	順守ポリシーの管理	3
3.4	レポートの管理	3
4	システム構成	4
4.1	システム	4
4.1.1	ブランディング	4
4.1.2	エンタープライズ統合	6
4.1.3	セキュリティ	7
4.1.4	利用規約	8
4.2	デバイスとユーザー	9
4.2.1	全般	9
4.2.2	Android	13
4.2.3	Apple	16
4.3	アプリ	20
4.3.1	Workspace ONE Web	20
4.4	コンテンツ	22
5	アプリケーションの管理	23
5.1	社内・パブリックのアプリケーション	23
5.2	パブリックアプリケーションの配布	23
5.3	社内アプリケーションの配布	28
5.4	インストール状態の確認、コマンド送信	33
5.5	配布アプリケーションに対する操作	34
6	デバイスの順守管理	35
6.1	デバイスの順守(順守ポリシー)	35
6.2	アプリのインストールの制限	36
6.2.1	アプリグループの設定	36
6.2.2	順守ポリシー設定	38
6.3	JailBreak/Root Kit されたデバイスの順守ポリシー設定	42
7	レポートの管理	45
7.1	レポートの取得	45
7.2	レポートの定期取得	46
7.3	レポートの操作	48

1 本書について

本書はユーザーとデバイスの登録、ユーザーの管理、プロファイルの作成を経験された管理者の方向けに、下記の5つの項目について説明しています。

- ・ 機能別ガイドの概略
- ・ システム構成
- ・ アプリケーションの管理
- ・ コンプライアンスの管理
- ・ レポートの管理

本書以外、Workspace ONE UEM 管理コンソールガイドには、次の2つがあります。

Workspace ONE UEM 管理コンソールガイド(入門編)

- ・ Workspace ONE UEM へのログイン
- ・ ユーザー登録
- ・ ダッシュボードの表示
- ・ ※ユーザーとデバイスの登録をされていない方はご参照ください。

Workspace ONE UEM 管理コンソールガイド(初級編)

- ・ ユーザー管理
- ・ デバイス操作
- ・ プロファイル

デバイス*の操作についてのガイドは、以下のようになっています。

かんたんセットアップガイド_Android 編

かんたんセットアップガイド_iOS 編

*デバイス： Android のスマートフォンとタブレット、iPhone、iPad、iPod touch

*iOS デバイス： iPhone、iPad、iPod touch

2 ご利用にあたっての準備

本書にあります手順を実行する前に、以下のものを準備してください。

Web ブラウザを利用可能なコンソール用 PC

管理対象となるデバイス

利用可能な Web ブラウザ

- Firefox
 - Chrome
 - Microsoft Edge
 - Safari (Mac 版)
- ・ 最新 Ver の Web ブラウザのご使用を推奨しております。
 - ・ 上記以外では、表示不良や操作が出来ない等の問題が発生する事があります。

3 機能別ガイドの概略

以下は本書に記載されている機能についての説明です。

3.1 システム構成

管理コンソールのカスタマイズや、エンタープライズ統合の設定、VMWare Intelligent Hub、Workspace ONE Web や Content 等の Workspace ONE SDK を利用しているアプリケーションの設定を行います。

3.2 アプリケーションの管理

デバイスへのアプリ配信について、設定・管理する機能です。アプリは次の二つに分類されます。

- ・ 内部アプリケーション

自社で開発され自社用に公開し、App Store、Google Play に対し非公開

- ・ 公共アプリケーション

App Store、Google Play で公開

3.3 順守ポリシーの管理

管理者が指定したセキュリティ設定をデバイスが遵守しているか管理する機能です。

3.4 レポートの管理

デバイスのステータス、構成、ユーザー情報等を収集し、レポートを作成する機能です。

4 システム構成

4.1 システム

4.1.1 ブランディング

管理画面のヘッダー部分にあるアイコンを変更する事が可能です。

- 1) [グループと設定] > [すべての設定]をクリックします。



- 2) [システム] > [ブランディング] をクリック後、[現在の設定]を[オーバーライド]にして [アップロード]をクリックします。

メインロゴにオリジナルの画像ファイルをアップロード可能です。またロゴには外部 URL を設定する事が可能です。



3) [参照]をクリックし、画像ファイルを選択して[保存]をクリックします。



4) 画面下部の[保存]をクリックします。

3)で選択した画像が画面に表示されます。

[企業 Web サイトの URL]にアドレスを入力すると、ロゴのクリック時入力したリンク先へ移動することができます。

変更前



変更後



4.1.2 エンタープライズ統合

➤ E メール (SMTP)

SaaS 環境の初期設定では VMware 社がクラウド環境で管理しているメールサーバが登録され、そのサーバから E メールが送信されます。SaaS 環境をご利用のお客様がお客様の既存のメールサーバを経由させるためにはお客様の社内に ACC サーバの構築が必要です。

そして、御社の E メールサーバアドレス、送信者名、送信者の E メールアドレスなどを指定する事で、下記の場合に御社のメールサーバを利用してメールが送信されます。

- E メールによるデバイスの登録
- デバイスダッシュボードからデバイスへの E メール送信

[グループと設定] > [すべての設定] > [システム] > [エンタープライズ統合] > [E メール (SMTP)] をクリックします。

1) 必要な項目を入力します。

項目名の後に「*」がついているものは必須項目です。

システム > エンタープライズ統合

Eメール (SMTP)

現在の設定 ☒ 結果 ☐ オーバーライド

1 サーバ*

2 ポート*

3 タイムアウト (秒)*

4 送信者名

5 送信者のEメール・アドレス*

サブグループの権限* ☐ 結果のみ ☐ オーバーライドのみ ☒ 結果またはオーバーライド

保存

①	サーバ	E メール (SMTP) サーバのアドレスを入力します。
②	ポート	E メール (SMTP) サーバのポート番号を入力します。
③	タイムアウト (秒)	タイムアウト値を入力します。
④	送信者名	Eメールの送信社名を入力します。
⑤	送信者の E メールアドレス	送信者の E メールアドレスを入力します。

4.1.3 セキュリティ

➤ 制限された操作

制限された処理の項目を有効にして保存すると、有効にした項目の動作を行う際に管理者用のセキュリティ暗証番号の入力を求められます。これは、最初にログインしたときに設定する4桁の暗証番号です。また、暗証番号試行の最大回数を設定する事で、設定回数以上間違えると、強制的にログアウトさせる事が可能です。また、一部の項目では、慎重に行う作業の為にメモを要求する項目があり有効化させる事が可能です。本設定は一番上位の組織グループとなる、カスタマー組織グループのみ有効です。

※セキュリティ暗証番号について、Workspace ONE UEM 管理コンソールガイド(入門編)「4.1 初回ログイン」をご参照下さい。

- 1) [グループと設定] > [すべての設定] > [システム] > [セキュリティ] > [制限された操作]をクリックします。
- 2) [暗証番号の試行回数上限]を設定して[保存]をクリックします。

[図一部省略]

4.1.4 利用規約

使用上の条件・注意等についての規約文を作成します。利用規約はコンソール、アプリケーションの2種類を作成する事が可能です。コンソールの利用規約は管理者アカウントで管理コンソールに初回ログインした際に表示されます。アプリケーションの利用規約はアプリケーションがデバイスにインストールされる際に表示されます。

- 1) [グループと設定] > [すべての設定] > [システム] > [利用規約]をクリックします。
- 2) [利用規約を追加]をクリックします。



- 3) 必要な項目を入力して[保存]をクリックします。

①	名前	利用規約の名前を入力します。
②	タイプ	コンソールかアプリケーションを選択します。
③	言語の選択	日本語以外に英語が選択可能です。英語を選択する場合は[+ 追加]をクリックして英語を追加します。
④	利用規約本文	利用規約の本文を入力します。

4.2 デバイスとユーザー

4.2.1 全般

デバイスを Workspace ONE UEM に加入する際のルールや加入後のデバイス情報の収集やコマンドの許可の設定等を行います。

ここでは主要な設定について記載します。

➤ 加入

[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]をクリックし、[グループ化]タブをクリックにします。

デバイスとユーザー > 全般

加入

認証 管理モード 利用規約 **グループ化** 制限 オプションのメッセージング カスタマイズ

現在の設定 ☐ 継承 ☒ オーバーライド

グループID割り当てモード * ☒ 既定 ☐ 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 ☐ ユーザーグループに基づき自動選択

設定

① 既定のデバイス所有形態 * 企業 - 専用

② 既定の役割 * フルアクセス

非アクティブユーザーに対する設定アクション * 加入状態デバイスの企業情報をフィードバック

ユーザーグループ同期

Workspace ONE に対してユーザーグループをリアルタイム同期 ☒ 有効 ☐ 無効 ③

ユーザー役割のマッピング

ディレクトリのグループベースのマッピングを有効化 ☐

サブグループの権限 * ☐ 継承のみ ☐ オーバーライドのみ ☒ 継承またはオーバーライド

保存

①	既定のデバイス形態 *	デバイス加入時の所有形態のデフォルト設定。
②	既定の役割 *	ユーザーに割り当てる役割のデフォルト設定。 この役割はセルフポータルサイト (SSP) 利用時に適用されます。

➤ フレンドリ名

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [フレンドリ名]をクリックします。

①	カスタム フレンドリ名を有効化	有効にすると、加入時のフレンドリ名はカスタムフレンドリ名が適用されます。
②	カスタムフレンドリ名	文字列と参照値({}表記)で設定。 参照値は[+]をクリックして確認してください。
③	デバイス名をフレンドリ名に設定	有効にすると、加入時の監視モードの iOS デバイスのフレンドリ名はデバイス名が適用されます。

➤ プライバシー

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [プライバシー]をクリックします。

設定

システム

デバイスとユーザー

全般

フレンドリ名

参照フィールド

メッセージテンプレート

通知

プライバシー

パスワード

共有デバイス

高度な設定

Android

Apple

QNX

Chrome OS

Windows

周辺機器

高度な設定

デバイスとユーザー > 全般

プライバシー

①

②

③

位置情報

	企業・商用	企業・共有	従業員所有	許可されてなし
GPS データ	●	●	○	○
Bluetooth データ	○	○	○	○
USB データ	○	○	○	○

テレコム

	企業・商用	企業・共有	従業員所有	許可されてなし
ダイヤルコード	●	●	●	●
ローミング状態	●	●	●	●
セルラーデータ使用量	●	●	●	●
通話使用	●	●	●	●
SMS 使用量	●	●	●	●
デバイス電話番号	●	●	○	○

アプリ

	企業・商用	企業・共有	従業員所有	許可されてなし
後入アプリケーション	●	●	○	○
Android 5.0 アプリケーション	○	○	○	○

プロフィール

	企業・商用	企業・共有	従業員所有	許可されてなし
登録されていないプロフィール	●	●	○	○

ネットワーク

	企業・商用	企業・共有	従業員所有	許可されてなし
パブリックIPアドレス	●	●	○	○

コマンド

	企業・商用	企業・共有	従業員所有	許可されてなし
デバイスワイプ	●	●	○	○
デバイスパスワードをクリア/デバイスをロック/シャットダウン/再起動	●	●	○	○
リモート操作	●	●	○	○
デバイスログを要求	●	●	○	○

ユーザー情報

名*

姓*

電話番号*

Eメール アカウント*

ユーザー名*

好きな色

好きなモード

ユーザーフレンドリなプライバシー通知

ユーザーフレンドリなプライバシー通知を有効にする

サブグループの権限*

結果のみ

オーバーライドのみ

結果またはオーバーライド

保存

①	GPS テレコム アプリケーション プロファイル ネットワーク	Workspace ONE UEM が行うデバイス情報の収集について、それぞれの情報に対して、デバイスの所有形態毎に設定。 マウスポインタを設定箇所に移動して設定します (③)
②	コマンド	Workspace ONE UEM からデバイスへのコマンド実行について、それぞれのコマンドに対して、デバイスの所有形態毎に設定。

重要

加入しているデバイスの所有形態を変更して設定を適用させる場合、**デバイスの再加入**が必要です。
また所有形態を変更していない加入中のデバイスで設定と整合しない場合、**デバイスの再加入**をお試しください。

➤ パスワード

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [全般] > [パスワード]をクリックします。

①	加入ユーザーのパスワード設定を有効化	有効にすると、パスワードのポリシー設定が可能です。
②	適用されたパスワードの履歴 *	再使用できない旧パスワードの数を設定。
③	パスワードの最小文字数 * パスワードの複雑度 *	パスワードの設定条件を設定。

4.2.2 Android

Android に関する設定を行います。

ここでは主要な設定について記載します。

➤ Android EMM 登録

managed Google Play 対応する為の設定を行います。旧来の Google Play ストアによるアプリの検索/追加の操作は Google 社により実施された Google Play ストア UI の変更により行えません。

初期設定に関しては、以下をご参照ください。

「Workspace ONE Android ガイド(入門編)」 3 Android 初期設定

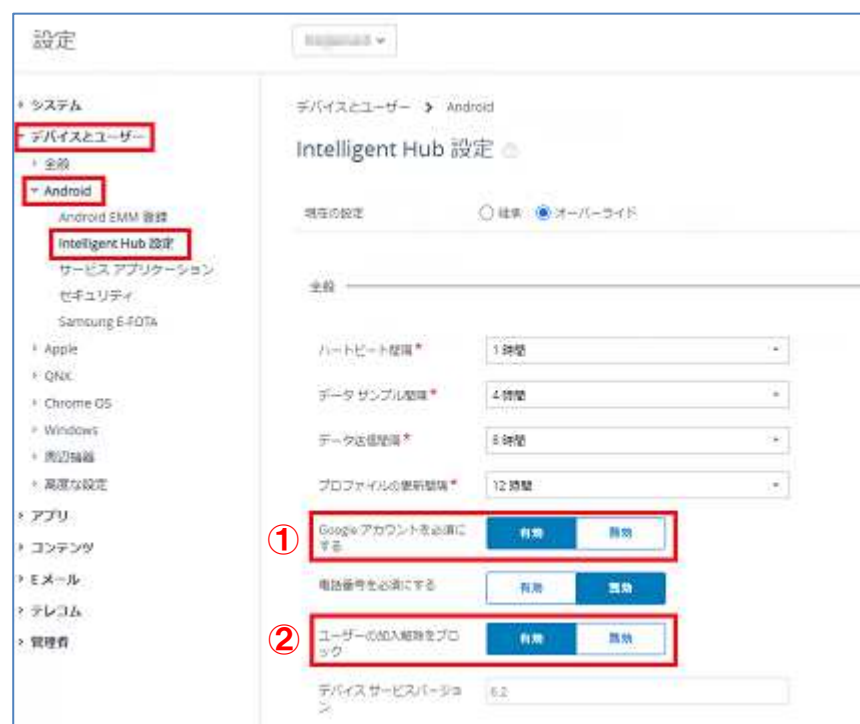
[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Android] > [Android EMM 登録]



➤ Intelligent Hub 設定

Android 版 intelligent Hub アプリの動作に関する設定です。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Android] > [Intelligent Hub 設定]をクリックします。



位置情報

位置情報データを収集

有効

無効

③

テレコム

通信ログを有効化

有効

無効

SMS ログを有効化

有効

無効

セルラーデータの送信を有効化

有効

無効

④

AirWatch Cloud Messaging (AWCM)

AWCM を FCM の代わりにプッシュ通知サービスとして使用

有効

無効

⑤

S&K プロファイル

S&K プロファイル

Android Default Settings @ Global

サブグループの権限

☐ 読者のみ
☐ オーバーライドのみ
☒ 読者またはオーバーライド

保存

①	Google アカウントを必須にする	デバイス加入時にデバイスのGoogleアカウント設定を必須とします。
②	ユーザーの加入解除をブロック	デバイス利用者の加入解除操作を制限します。
③	位置情報	デバイスの位置情報サービスを収集する場合、この項目を有効にし、デバイスの所有形態に対する GPS データの収集を有効にします。（「4.2.1 全般」プライバシー参照）
④	テレコム	デバイスのテレコム情報を収集する場合、この項目を有効にし、デバイスの所有形態に対するテレコム情報の収集を有効にします。（「4.2.1 全般」プライバシー参照）
⑤	AirWatch Cloud Messaging (AWCM)	Android デバイスのメッセージングサーバーを選択します。[有効]を選択すると AWCM が利用されます。

➤ サービスアプリケーション

特定のメーカー／モデルで対応する制御やテレコム情報の参照、ランチャーの利用時に設定します。
[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Android] > [サービスアプリケーション]をクリックします。



①	サービスアプリを必須にする	プロファイルのデバイス制御設定で、対応デバイスの表示のある項目が含まれる場合、これを有効にします。各制御項目とデバイスとの対応については、メーカーマニュアル「VMware Workspace ONE Android プラットフォームガイド 付録：Android機能のマトリックス」をご参照ください。
②	常に最新バージョンのテレコムサンプラーを使用	テレコム情報を利用する時に設定します。
③	常に最新バージョンの AirWatch Launcher を使用	ランチャーを利用する時に設定します。

4.2.3 Apple

iOS に関する設定を行います。

ここでは主要な設定について記載します。

➤ [Apple iOS] > [Agent 設定]

iOS 版 Intelligent Hub アプリの動作に関する設定です。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Apple] > [Apple iOS] > [Intelligent Hub 設定]をクリックします。

デバイスとユーザー > Apple > Apple iOS

Intelligent Hub 設定

全般 通知

現在の設定 継承 オーバーライド

全般

① Intelligent Hub の加入解除オプションを無効化 ☒

② バックグラウンドアプリの更新 ☐ iOS 7

エリア

③ 位置情報データを収集 ☒ ⓘ

iBeacon エリアを検知する ☐ ⓘ

テレコム

④ セルラーデータ使用量情報を収集 ☒

セルフサービス

セルフサービス有効化 ☒ ⓘ

SDK プロファイル

SDK プロファイル (レガシー) なし

⑤ SDK プロファイル V2 iOS Default Settings @ Global

サブグループの権限* 継承のみ オーバーライドのみ 継承またはオーバーライド

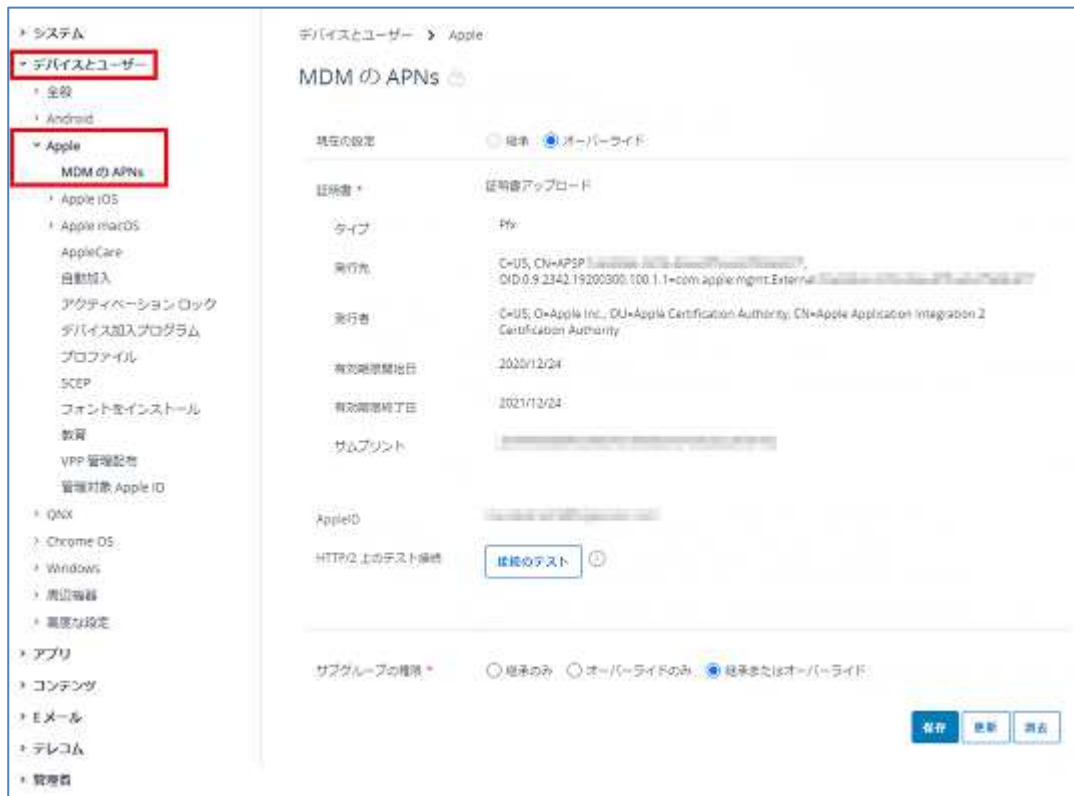
保存

①	Intelligent Hubの加入オプションを無効化	Intelligent Hub アプリの操作で加入解除を禁止する場合、この項目を有効にします。
②	バックグラウンドアプリの更新	バックグラウンド動作の Intelligent Hub が行う Workspace ONE UEM へのデバイスの状態やデータの通知に対する設定変更する場合、この項を有効にします。
③	位置データを収集	デバイスの位置情報サービス情報を収集する場合、この項目を有効にし、デバイスの所有形態に対する位置情報サービス情報の収集を有効にします。（「4.2.1 全般」プライバシー 参照）
④	セルラーデータ使用量情報を収集	セルラー通信情報を収集する場合、この項目を有効にし、デバイスの所有形態に対するテレコムの各情報収集を有効にします。（「4.2.1 全般」プライバシー 参照）
⑤	SDK プロファイル V2	[iOS Default Settings@Global]を設定します。

➤ MDM の APNs

APNs に関する設定です。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Apple] > [MDM の APNs]をクリックします。



以下をご参照ください。

「Workspace ONE UEM 管理コンソールガイド(入門編)」

5 APNs の登録-iOS

「Workspace ONE APNs 更新ガイド」

3 APNs 更新作業

➤ 自動加入

Apple Configurator による Workspace ONE の加入までのデバイス初期設定（キッティング）を行う時に設定します。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Apple] > [自動加入]をクリックします。



以下をご参照ください。

「Workspace ONE Apple Configurator2 統合ガイド」

4 Workspace ONE UEM コンソールによる準備

➤ デバイス加入プログラム

DEP (Device Enrollment Program) による Workspace ONE の加入までのデバイス初期設定（キッティング）を行う時に設定します。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Apple] > [デバイス加入プログラム]をクリックします。



以下をご参照ください。

「Workspace ONE DEP(Device Enrollment Program)統合ガイド」

5 DEP へのデバイス登録

➤ VPP 管理配布

VPP(Volume Purchase Program)により一括購入したアプリの配布を行う時に設定します。

[グループと設定] > [すべての設定] > [デバイスとユーザー] > [Apple] > [VPP 管理配布]をクリックします。



以下をご参照ください。

「Workspace ONE Apple VPP 管理ガイド」

3. Workspace ONE UEM コンソールによる操作

4.3 アプリ

デバイスで使用する VMware Workspace ONE アプリケーションに関する設定を行います。

4.3.1 Workspace ONE Web

➤ ブラウザ設定

[グループと設定] > [すべての設定] > [アプリ] > [Workspace ONE Web] をクリックし、[ブラウザ設定]タブをクリックします。

Workspace ONE Web の設定

Workspace ONE Web の設定

設定とポリシー

設定とポリシー

全般

モード

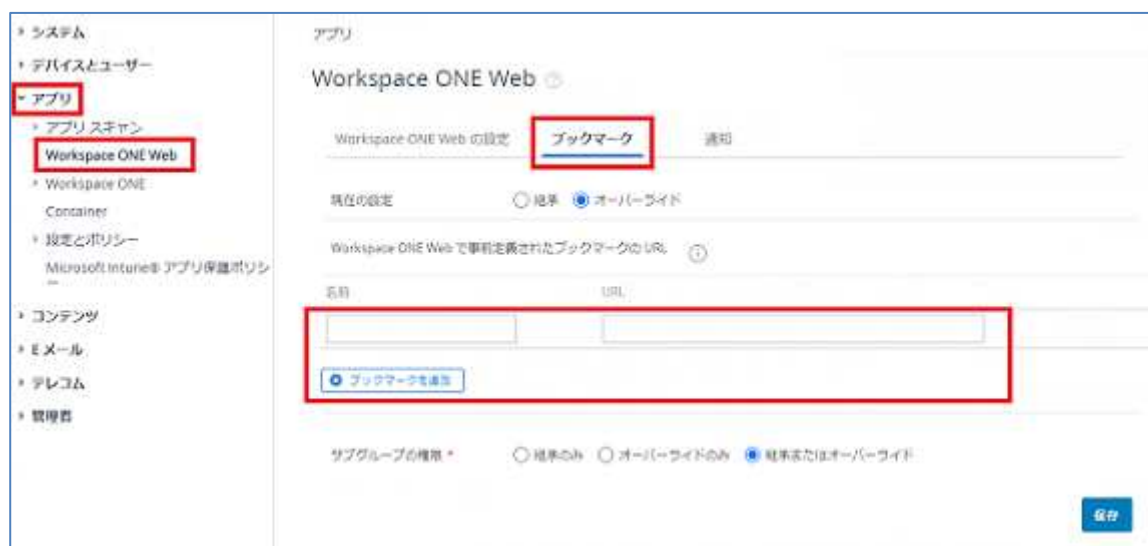
利用規約

保存

①	設定とポリシー	セキュリティポリシーを設定します。 [既定]にすると [設定とポリシー]の設定を適用します。 [カスタム]にすると この画面に表示されるカスタムの設定を適用します。
②	全般	Cookie やキャッシュなど、ブラウザの動作に対する設定をします。
③	モード	操作を URL ページ参照のみに制限するキオスクモードの設定、ホーム画面設定、許可/禁止サイトへのアクセスの設定をします。
④	利用規約	必要に応じ、[システム] > [利用規約]で利用規約（[タイプ]=アプリケーション）を作成して、ここに設定します。

➤ ブックマーク

[グループと設定] > [すべての設定] > [アプリ] > [Workspace ONE Web] をクリックし、[ブックマーク]タブをクリックします。



[ブックマークを追加]をクリックし、追加されたブックマークの[名前]と[URL]の設定行にブックマークを追加します。

4.4 コンテンツ

デバイスで使用する Content の設定を行います。

[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] をクリックします。

Workspace ONE Content アプリ

現在の設定: ☐ 継承 ☒ オーバーライド

① 設定とポリシー

アプリケーションプロファイル: ⓘ

② 全般

コンテンツを新規として表示する日数*: 35

Content, Boxes, および Web からの追加をブロック:

管理コンテンツのリポジトリ名の変更:

ハイパーリンクを許可:

インターネットリンクを開くアプリ*:

ローカルストレージ:

アップロードを Web のみに制限:

③ 利用規約

Content は下記のフィールドで選択された利用規約を表示します。[システム] > [利用規約] と進んで独自の利用規約を作成することができます

必要とする利用規約*:

通知

プラットフォーム: ☒ Apple ☐ Android ☐ Windows デスクトップ

アプリケーションタイプ*:

アプリケーション名*: VMware Content Locker@Global

バンドル ID*: com.vmware.watch.content.locker

バックアップ*:

サブグループの権限: ☐ 継承のみ ☐ オーバーライドのみ ☒ 継承またはオーバーライド

①	設定とポリシー	セキュリティポリシーを設定します。 [既定]にすると [設定とポリシー]の設定を適用します。 [カスタム]にすると この画面に表示されるカスタムを設定を適用します。
②	全般	Content の機能や動作に対する設定をします。
③	利用規約	必要に応じ、[システム] > [利用規約]で利用規約 ([タイプ]=アプリケーション)を作成して、ここに設定します。

5 アプリケーションの管理

5.1 社内・パブリックのアプリケーション

管理者は Workspace ONE UEM のアプリケーション機能を利用して、対象組織グループの全デバイスへアプリケーションを配布できます。アプリケーションは次の2つに分類されます。

社内（自社で開発したアプリのみ使用）アプリケーション

パブリック（App Store、Google Play、MicrosoftStore で公開）アプリケーション

iOS デバイスの社内アプリケーションの配布には Apple Developer Enterprise Program に参加する必要がありますので、以下の Apple 社のサイトにてご確認ください。

<https://developer.apple.com/jp/programs/enterprise/>

5.2 パブリックアプリケーションの配布

1) [アプリとブック] > [パブリック]タブをクリックし、[アプリケーションを追加] ボタンをクリックします。



2) アプリケーションの情報を入力し、[次へ]をクリックします。

アプリケーションを追加

管理元

support

①

プラットフォーム*

Apple iOS

②

ソース

アプリストアを検索

URL 入力

③

名前*

vmware|

④

次へ

キャンセル

①	管理元	組織グループが表示されます。
②	プラットフォーム*	アプリケーションのプラットフォームを選択します。
③	ソース	[アプリストアを検索]を選択します。
④	名前*	アプリストアで検索する検索キーを設定します。

3) Apple iOS の場合は、[国]が米国での結果が表示されますので、日本に変更後、追加するアプリケーションに対し[選択]ボタンをクリックします。



Android の場合、追加するアプリをクリック後、[承認]をクリックします。承認のダイアログ表示で [承認] をクリックし、[このアプリから新しい権限をリクエストされたときにアプリの承認を維持します。] を選択し、[保存] をクリックします。



4) [保存して割り当て]をクリックします。

The screenshot shows the 'Add Application - Web - Workspace ONE' interface. At the bottom right, the button '保存して割り当て' (Save and Assign) is highlighted with a red rectangular box. Other visible elements include the application name 'Web - Workspace ONE', a category selection field, and various device compatibility filters.

5) 新規アプリの追加時には割り当て画面が表示されます。このアプリケーションの配布についての設定を行います。次に[制限]をクリックします。

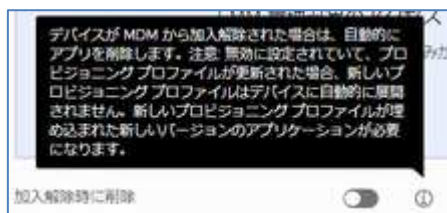
The screenshot displays the 'Web - Workspace ONE - 割り当て' (Assignment) screen. The '配布' (Distribution) tab is selected on the left. Three fields are highlighted with red boxes and numbered: ① '名前' (Name) field, ② '割り当てグループ' (Assignment Group) field, and ③ 'アプリ配信方法' (Application Distribution Method) field, which shows 'オンデマンド' (On-demand) selected.

①	名前	割り当ての名称を入力します。
②	割り当てグループ	該当デバイスを組織グループまたはスマートグループで指定します。
③	アプリ配信方法	[自動] 該当デバイスに対して一括配信。 Workspace ONE UEM 側で未インストール状態と判断されたデバイスに対してインストールのコマンドが発行されます。 [オンデマンド] 管理コンソールの操作でデバイスを選択してインストール、もしくはデバイス側で AppCatalog によるインストールします。

6) このアプリケーションのインストールやアクセスに対する設定を行い、[作成]をクリックします。



④	管理対象アクセス	管理デバイスに対してアプリのインストールを行う際、制限などのポリシーが適用されます。管理対象アクセスの設定は、他のポリシーを有効にすると自動的に有効に設定されます。
⑤	ポリシー	インストールの管理、データ漏洩、アクセスなどのコントロールを設定。各項目については、バルーン表示（下図）でご確認ください。



【参考】 Tunnel（PerApp VPN）用プロファイルの適用設定例



- 7) 追加した割り当てがリストされます。[割り当ての追加]で別のデバイスグループに割り当てを追加する事も可能です。
- [保存]をクリックすると、対象のデバイスがリスト表示されますので、[公開]をクリックして適用します。

Web - Workspace ONE - 割り当て

詳細
プラットフォーム: App® 状態: 有効

割り当て 操作

デバイスは、以下の構成に基づいてアプリケーションを受け取ります。複数の割り当てがあるデバイスは、優先度の順番によってポリシーを受け取ります。1つの割り当ての優先度を調整すると、他の割り当ての優先度が自動的に再指定されます。編集する割り当てを選択してください。新しい割り当てを追加すると、リストの一番下に新しいルールが作成されます。

割り当ての追加

優先度	割り当て名	状態	スマートグループ	アプリ配信方法	EMM 管理対象のデバイス
1	All Device	有効	1	オンデマンド	有効

1ページに表示する項目数: 5 項目 1-1/1

キャンセル 保存

Web - Workspace ONE - 割り当てデバイスプレビュー

割り当て状態: すべて リストを複製

割り当て状態	プラットフォーム	ユーザー	プラットフォーム	組織グループ
追加済	iPhone iOS 11.5.1 (CLK)		App®	

1ページに表示する項目数: 20 項目 1-1/1

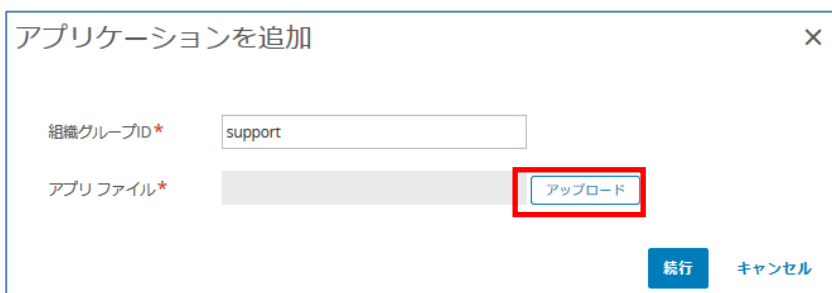
キャンセル 公開

5.3 社内アプリケーションの配布

- 1) [アプリとブック] > [社内]タブをクリックし、マウスポインタを[追加]に移動してサブメニューを表示し、[アプリケーション ファイル] をクリックします。



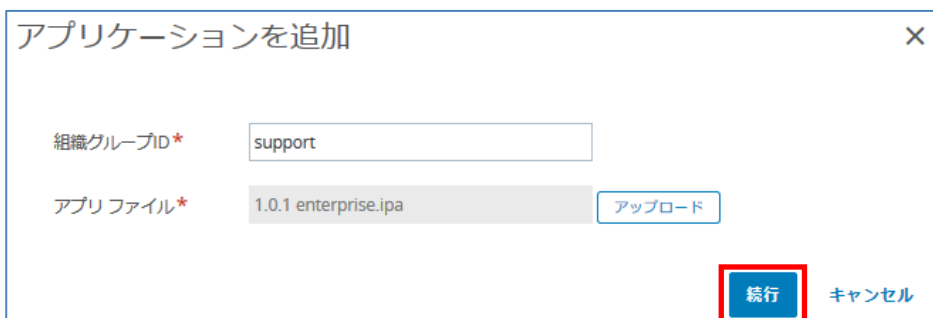
- 2) 管理元で組織グループを選択して、[アップロード]をクリックします。



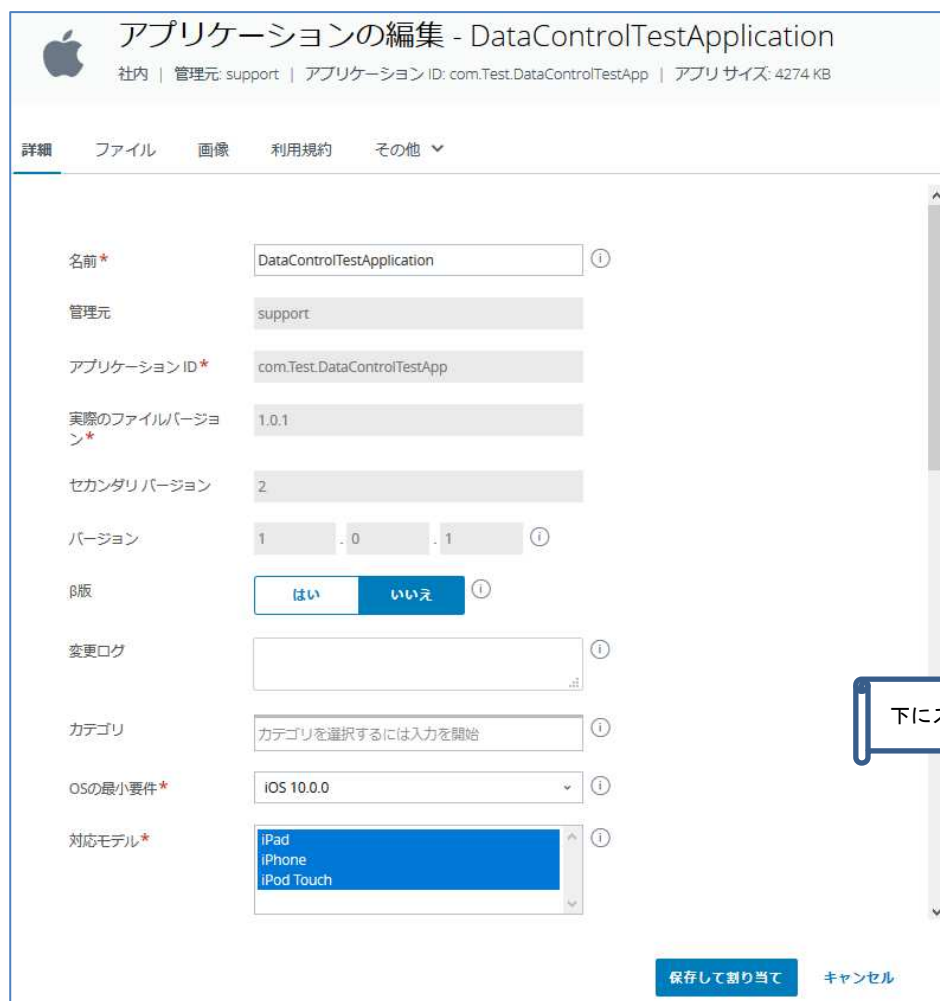
- 3) [ファイルを選択]をクリックしファイルを選択後、[保存]をクリックします。
※保存出来るのはファイル拡張子が【ipa】(iOS 用)か【apk】(Android 用)のアプリファイルのみです。



- 4) [続行]をクリックします。



5) アプリケーションの詳細表示を確認します。



アプリケーションの編集 - DataControlTestApplication

社内 | 管理元: support | アプリケーション ID: com.Test.DataControlTestApp | アプリサイズ: 4274 KB

詳細 ファイル 画像 利用規約 その他

名前 * DataControlTestApplication ⓘ

管理元 support

アプリケーション ID * com.Test.DataControlTestApp

実際のファイルバージョン * 1.0.1

セカンダリバージョン 2

バージョン 1 . 0 . 1 ⓘ

β版 はい いいえ ⓘ

変更ログ ⓘ

カテゴリ カテゴリを選択するには入力を開始 ⓘ

OSの最小要件 * iOS 10.0.0 ⓘ

対応モデル * iPad iPhone iPod Touch ⓘ

保存して割り当て キャンセル

下にスクロールできます。

必須設定(確認)項目

名前 *	アプリケーションから自動で取得します。
アプリケーション ID *	アプリケーションから自動で取得します。
実際のファイルバージョン *	アプリケーションから自動で取得します。
OSの最小要件 *	アプリケーションから自動で取得します。アプリケーションで設定されていない場合は、手動で設定する必要があります。
対応モデル *	アプリケーションから自動で取得します。

6) [ファイル]タブをクリックし、設定を確認して[保存して割り当て]をクリックします。

※この項目は iOS アプリケーションを登録する場合に行います

アプリケーションの編集 - DataControlTestApplication
社内 | 管理元: support | アプリケーション ID: com.Test.DataControlTestApp | アプリ サイズ: 4274 KB

詳細 **ファイル** 画像 利用規約 その他 ▾

アプリ ファイル* 1.0.1 enterprise.ipa

プロビジョニングプロファイル* DataControlTestAppPro 変更 ①

アプリケーションは APNs をサポート ☐ はい ☒ いいえ ②

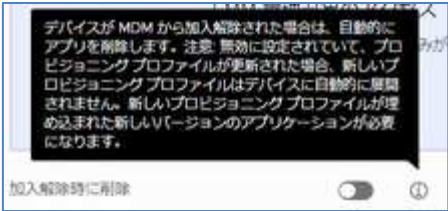
保存して割り当て キャンセル

①	プロビジョニングプロファイル *	アプリファイルに組み込まれている場合、プロビジョニングプロファイルが表示されます。 アプリファイルがプロビジョニングプロファイル情報を持っていない場合、別途アップロードが必要となります。プロビジョニングプロファイルは iOS の社内アプリケーションでは必須で、アプリの提供元の信頼性を iOS が判断する時に使われます。 有効期限は 1 年です。期限に近づくとボタンが[更新]に変わり[失効日]が表示されますので、更新を行ってください。
②	アプリケーションは APNs をサポート	Workspace ONE UEM から開発したアプリに対してメッセージを送る等の APNs 機能を利用する場合に設定します。 開発したアプリが APNs をサポートしている場合は、[はい]を選択し、アプリケーションの APNs 証明書をアップロードしてください。

- 7) 新規アプリの追加時には割り当て画面が表示されます。このアプリケーションの配布についての設定を行います。次に[制限]をクリックします。

①	名前	割り当ての名称を入力します。
②	割り当てグループ	該当デバイスを組織グループまたはスマートグループで指定。
③	展開の時間	展開を開始する日時を設定。
④	アプリ配信方法	[自動] 該当デバイスに対して一括配信。 Workspace ONE UEM 側で未インストール状態と判断されたデバイスに対してインストールのコマンドが発行されます。 [オンデマンド] 管理コンソールの操作でデバイスを選択してインストール、もしくはデバイス側で AppCatalog によるインストール。

- 8) このアプリケーションのインストールやアクセスに対する設定を行い、[作成]をクリックします。

⑤	管理対象アクセス	管理デバイスに対してアプリのインストールを行う際、制限などのポリシーが適用されます。管理対象アクセスの設定は、他のポリシーを有効にすると自動的に有効に設定されます。
⑥	ポリシー	インストールの管理、データ漏洩、アクセスなどのコントロールを設定。各項目については、バルーン表示（下図）でご確認ください。 

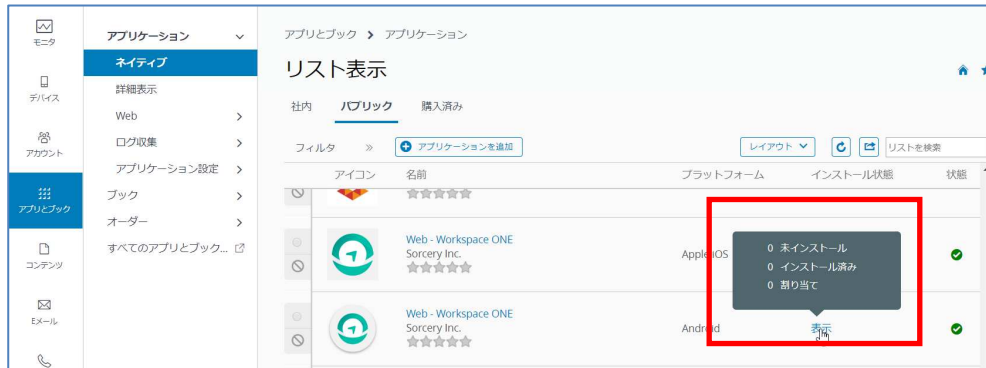
- 9) 追加した割り当てがリストされます。[割り当ての追加]で別のデバイスグループに割り当てを追加する事も可能です。

[保存]をクリックすると、対象のデバイスがリスト表示されますので、[公開]をクリックして適用します。



5.4 インストール状態の確認、コマンド送信

- 1) デバイスのインストール状態は、アプリケーションリスト表示（[アプリとブック] > [パブリック]タブや[社内]タブをクリック）で、該当アプリの[インストール状態]の[表示]をクリックし、目的の状態（フィルタ）を選択します。



- 2) 選択したフィルタで、アプリケーションの[詳細表示] > [デバイス]タブの表示になります。



- 3) この画面で、デバイスを選択すると（リスト左の口をクリック）、コマンドボタンが表示され、デバイスに対してコマンド実行が可能です。



クエリ	デバイスにクエリを送信し、現在のアプリケーション情報を取得します。
送信	メッセージを送信し、アプリケーションのインストールを促します。
インストール	デバイスに対してプッシュモードでインストールを行います。
削除	デバイスからアプリケーションを削除します。
トンネル構成の同期	デバイスに対して、Tunnel 構成（VPN プロファイル）の同期を行います。

5.5 配布アプリケーションに対する操作

- 1) デバイスに配布設定したアプリに対する操作は、アプリケーションリスト表示（[アプリとブック] > [パブリック]や[社内]タブ）で該当アプリの列をクリックにより、詳細表示で行います。



編集	アプリ編集画面を表示します。
割り当て	デバイスの割当ての追加/編集/削除を行う画面を表示します。
その他	
管理:非アクティブ化/アクティブ化	デバイスへの割当ての適用を無効化（非アクティブ化）/有効化（アクティブ化）します。
管理: アプリケーション構成を送信	設定したアプリケーション構成を再送信します。
管理:回収 ※社内アプリケーション	アプリケーションのステータスを「回収済み」へ設定し、デバイスからアプリケーションを回収（削除）します。
表示:ユーザー評価	ユーザー評価の画面を表示します。
表示:イベント	デバイスとコンソールイベントを表示します。
削除:アプリケーションを削除	このアプリの配布設定を削除します。
バージョン:バージョン追加 ※社内アプリケーション	アプリケーションの最新バージョンを追加します。 「以前のバージョンを回収」のオプションをチェック時は、デバイスの古いバージョンが新しいバージョンに差替えられます。
バージョン:他のバージョン ※社内アプリケーション	選択したアプリケーション以外のバージョン情報を表示します。

6 デバイスの順守管理

6.1 デバイスの順守(順守ポリシー)

デバイスが企業の運用ポリシーに準拠して運用されているかを管理することができます。

運用ポリシーは、ポリシーのルールにて準拠/非準拠の判断を行い、非準拠のデバイスに対しては、さまざまなアクションを行い企業の運用ポリシーに準拠させる事が行えます。

◆ルール

- ・ Jail Brake / root 化の有無
- ・ デバイス最終検出 (Workspace ONE UEM との最後の通信) の有無
- ・ パスコードの設定の有無
- ・ OS バージョン
- ・ SIM カードの変更の有無
- ・ アプリケーションリスト (ブラックリスト、ホワイトリストなど) の有無など

◆アクション

アプリケーション

- ・ 管理アプリケーションの削除、インストール拒否

コマンド

- ・ チェックイン要求 (Workspace ONE UEM への通信要求)
- ・ 企業情報ワイプ (Workspace ONE UEM 管理情報の削除)
- ・ ローミング設定の変更

通知

- ・ E メール通知 (ユーザーまたは管理者)
- ・ Push 通知

プロファイル

- ・ 構成プロファイルの削除、インストール拒否

6.2 アプリのインストールの制限

ここでは、アプリケーションに関する順守ポリシーの設定を説明します。

アプリグループには下記の3種類のタイプがあります。

ホワイトリスト：

ホワイトリストに登録したアプリケーション以外のアプリケーションをインストールした際にアクションを発動させます。

ブラックリスト：

ブラックリストに登録したアプリケーションをインストールした際にアクションを発動させます。

必須：

必ずインストールしなければならないアプリケーションがインストールされていない際にアクションを発動させます。

6.2.1 アプリグループの設定

- 1) [アプリとブック] > [アプリケーション設定] > [アプリグループ] をクリック後、[グループを追加] をクリックします。



- 2) [タイプ]、[プラットフォーム]、[名前]を設定し、[アプリケーションの追加]をクリックします。
(タイプとプラットフォームが未選択の場合はアプリケーションの追加が表示されません)



- 3) [アプリケーション名]に検索キーを入力し、検索を行います。(虫眼鏡アイコンをクリック)
検索結果から該当のアプリケーションに対し[選択]をクリックします。

アプリケーショングループを追加

リスト 割り当て

△ 個人アプリケーション プライバシー ポリシーでは、組織内の少なくとも1つの組織グループで、少なくとも1つのデバイスが収集しないように設定されています。これらのデバイスの個人アプリケーションのアプリケーショングループに紐付けられている許可ポリシーとアプリケーション制限プロファイルは、適用されません。

タイプ* プラットフォーム* 名前*

ホワイトリスト Apple iOS

アプリケーションを追加

アプリケーション名* アプリケーションID*

workspace one web

検索: workspace one web

Web - Workspace ONE
com.air-watch.secure.browser
フリー
カテゴリ: Business
現在のバージョン: 7.15
開発者: Kana

インターネット、インターネット、Web アプリのいずれも通常のセットアップにブラウジングできます。Workspace ONE Web を使用する際は、外出先から会社の社内ネットワーク サイトにすばやくアクセスできます。VPN に手動で接続する必要はありません。**会社のサイトやインターネットにすばやくアクセス** VPN を手動で設定することなく、通常の Web サイトやインターネットにすばやく簡単にアクセスできます。**すべてのブックマークを1つの場所にある** 会社は、ユーザーが簡単にアクセスできるように、ユーザーのアプリにブックマークをプッシュできます。ユーザーはブックマークを編集、削除したり、目で追加したりできます。ブックマークを見つけるのに苦労していますが、下のアクション グリッドをタップして、[ブックマーク] をタップしてください。 **QR コードをすばやくスキャン** QR コードをスキャンする必要がありますが、ブラウザの URL アドレス バーに移動し、右側のコードをタップして、カメラへのアクセスを有効にすれば、すぐにデバイスでスキャンできます。

選択

- 4) 上記 3) の操作を繰り返し、該当する全てのアプリケーションの追加後に、[次へ]をクリックします。

アプリケーショングループを追加

リスト 割り当て

△ 個人アプリケーション プライバシー ポリシーでは、組織内の少なくとも1つの組織グループで、少なくとも1つのデバイスが収集しないように設定されています。これらのデバイスの個人アプリケーションのアプリケーショングループに紐付けられている許可ポリシーとアプリケーション制限プロファイルは、適用されません。

タイプ* プラットフォーム* 名前*

ホワイトリスト Apple iOS

アプリケーションを追加

アプリケーション名* アプリケーションID*

Web - Workspace ONE com.air-watch.secure.b

Content - Workspace O com.air-watch.content

Vivante Tunnel com.vivante.xio-tunnel

次へ キャンセル

5) [②割り当て]の各項目を設定し[完了]をクリックします。

アプリケーショングループを追加

① リスト ② 割り当て

△ 個人アプリケーション プライバシー ポリシーでは、権限が少なくとも1つの組織グループで、少なくとも1つのデバイスが
の属しないに設定されています。これらのデバイスの個人アプリケーションのアプリケーション グループに属付けされてい
るポリシーとアプリケーション制御プロファイルは、適用されません。

説明

① デバイス所有形態 任意

② モデル 任意

③ オペレーティングシステム 任意

④ 管理元

⑤ 組織グループ

⑥ ユーザーグループ

完了 キャンセル

①	デバイス所有形態	デバイス所有形態を選択します。
②	モデル	デバイスモデルを選択します。
③	オペレーションシステム	OS のバージョンを選択します。
④	管理元	アプリを管理する組織グループを選択します。
⑤	組織グループ	適用する組織グループを選択します。
⑥	ユーザーグループ	適用するユーザーグループを選択します。

6. 2. 2 順守ポリシー設定

アプリグループを元に順守ポリシーを作成します。

ここでは前項で作成したホワイトリストを使用してご説明します。

1) [デバイス] > [順守ポリシー] > [リスト表示] をクリック後、[追加]をクリックします。

デバイス > 順守ポリシー

リスト表示

追加

- 2) 作成する順守ポリシーに対応するプラットフォームを選択します。(ここでは iOS を選択します)



- 3) 画面[順守ポリシーを追加]の[① ルール]で、一番左のプルダウンリストを[アプリケーションリスト]にします。(ホワイトリストを使用する場合)



- 4) 作成したアプリグループを基に順守条件を選択して[次へ]をクリックします。
ここでは、「ホワイトリストにないアプリが含まれている」を選択します。



- 5) 画面[② アクション]でデバイスが画面[① ルール]で設定の状態に合致した時のアクションを設定して[次へ]をクリックします。

iOS 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

すぐに次の操作を実行 ☒ 非順守状態としてマーク

通知
アプリケーション
コマンド
Eメール
通知
プロフィール

Eメールをユーザーに送信

CC:

☒ 既定のテンプレート

前へ 次へ キャンセル

ここでは、デバイスが非順守の状態になった時に対象ユーザーにメールで通知する設定です。対象ユーザー以外にも通知する場合はCCに該当メールアドレスを設定します。

- 6) 画面[③ 割り当て]で[スマートグループ]に組織グループまたはスマートグループを設定し、[次へ]をクリックします。

iOS 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

管理先:

スマートグループ:

いいえ はい

デバイス割り当て実行

前へ 次へ キャンセル

7) 最後に[名前]と[説明]を入力し、[アクティブ化する]をクリックします。

※[完了]でも設定完了をすることができますが、設定したポリシーはアクティブ状態ではない為、設定を有効にする場合は手動でアクティブ状態へ変更する必要があります。

6.3 JailBreak/Root Kit されたデバイスの順守ポリシー設定

iOS の JailBreak と、Android の Root Kit されたデバイスの検知、検知されたデバイスへの対処の一例を説明します。

1) [デバイス] > [順守ポリシー] > [リスト表示] をクリック後、[追加]をクリックします。



2) 作成する順守ポリシーに対応するプラットフォームを選択します。(ここでは iOS を選択します)。



3) 画面[①ルール]で[侵害状況]、[侵害状態である]にし、[次へ]をクリックします。



- 4) 画面[② アクション]で侵害状態（JailBreak、Root Kit 化されている事を検知した場合）のデバイスに対するアクションを設定して[次へ]をクリックします。

iOS 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

すぐに次の操作を実行 ☒ 非順守状態としてマーク

通知 ▼

- プッシュ通知をデバイスに送信
- メールをユーザーに送信
- SMS をデバイスに送信
- プッシュ通知をデバイスに送信
- メールを管理者に送信

さらに強い対応処置を追加

既定のテンプレート

前へ 次へ キャンセル

[さらに強い対応処置を追加]をクリックすると、項目が追加され対応処置を増やすことができます。

- 5) 画面[③ 割り当て]で[割り当てるグループ]に組織グループまたはスマートグループを設定し、[次へ]をクリックします。

iOS 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

管理元 * support

割り当てるグループ

- iOSデバイス (support)
- ここに入力してグループを追加

除外

いいえ はい

デバイス割り当て表示

前へ 次へ キャンセル

6) [名前]と[説明]を入力後、[完了してアクティブ化する]をクリックします。

iOS 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

全般

名前 *

侵害状態

説明 *

iOS JailBreak検知

デバイスの概要

割り当て

2

順守状態

2

非順守状態

0

前へ

完了

完了してアクティブ化

キャンセル

※完了でも設定完了をすることができますが、設定したポリシーはアクティブ状態ではない為、設定を有効にする場合は手動でアクティブ状態へ変更する必要があります。

7 レポートの管理

デバイスのステータス、構成、ユーザー情報等についてのレポートを CSV ファイルで取得する事ができ、定期的に取得する事も可能です。

7.1 レポートの取得

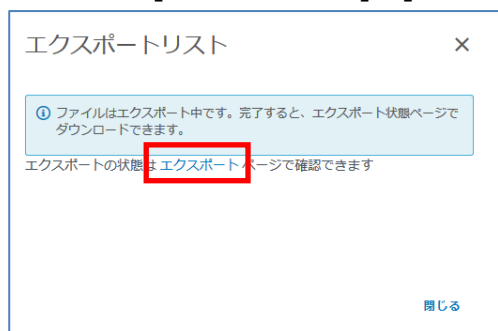
- 1) [モニタ] > [レポートおよび分析] > [レポート] > [リスト表示]をクリックして、レポートの一覧を表示させます。



- 2) レポートの[名前]をクリックし、レポートの取得条件を設定して[実行]をクリックします。



- 3) ダイアログ[エクスポートリスト]の[エクスポートページで確認できます]をクリッククリックします。



- 4) 遷移した[ハブ] > [レポートおよび分析] > [エクスポート]の画面で、実行したレポートの状態表示の[完了]をクリックします。すると、ブラウザの機能によるレポートファイルのダウンロードが行われます。



- 5) ブラウザの機能でレポートファイルがダウンロードされます。

7.2 レポートの定期取得

定期的にレポートを取得し、管理者にメール通知する事が行えます。

- 1) レポートのリスト表示([ハブ] > [レポートおよび分析] > [レポート] > [リスト表示])からレポートを選択(名前左の○をクリック)で表示される、[レポートのサブスクリプション]ボタンをクリックします。



- 2) 画面[①パラメータ]でレポートの取得条件を設定し、[次へ] をクリックします。



- 3) [②スケジュール]でレポート取得の通知や実施条件を設定し、[保存] をクリックします。

①	送信元	定期受信のメール送信元として、管理コンソールにログインしたアカウントのメールアドレスが設定されます。
②	送信先	指定した管理者アカウントのメールアドレスに定期受信のメールが送信されます。
③	繰り返し 日付/時刻/曜日 繰り返しを終了	定期受信に対し、実施サイクル、実施タイミング、終了日について設定します。
④	タイトル メッセージ	定期受信のメールのタイトルとメッセージを設定します。

- 4) レポート取得後に送信されるメールの以下のリンクをクリックすると、ブラウザの管理コンソール画面（ログイン操作が必要）に遷移し、レポートファイルがダウンロードされます。

Report is available for download, please click below link to download the report.

[Application Details by Device](#)

なおご利用のブラウザは、Workspace ONE SaaS(<https://cn1.dcl-mdm.com>)のポップアップを許可する設定にする必要があります。

7.3 レポートの操作

- 1) 設定した定期取得のレポートを確認する時は、[ハブ] > [レポートおよび分析] > [レポート] > [定期受信]をクリックします。

削除する時はレポートの名前左の[○]をクリックし、[定期配信削除]をクリックします。①

編集する時はレポートの[名前]をクリック、または名前左の[ペンアイコン]をクリックします。②



- 2) これまで取得したレポートは、[ハブ] > [レポートおよび分析] > [レポート] > [リスト表示] をクリックし、[最近のレポート]タブをクリックします。①

頻繁に取得するレポートは、名前左の[○]をクリックし、[マイレポートに追加] をクリックして、[マイレポート]タブに追加する事ができます。②



Workspace ONE UEM 管理コンソールガイド(機能編)

Workspace ONE UEM 2109 Web UI ベース

ver. 16.00 2022 年 1 月 21 日

ご注意事項

- この文書に記載された製品の仕様ならびに動作に関しては、各社ともにこれらを予告なく改変する場合があります。
- 本文中にあるシステム名、製品名、およびロゴ等は各社の商標または登録商標です。