

# Workspace ONE UEM 1909 リリースハイライト

2019/10/28  
株式会社ウィザース

## WS1 UEM Console / ログイン画面

管理者は、ユーザー名とパスワードをブラウザ キャッシュに保存して、以降のログインで使用できるような管理者エクスペリエンスを向上させました。



Workspace ONE™ UEM

ユーザー名  
administrator@wizaas.co.jp

記憶

次へ

[ログインできない場合](#)

# WS1 UEM Console / デバイス情報

デバイス詳細画面セキュリティ欄に記載されている「MDMによる管理」が「UEMによる管理」に変更されました。変更対象となるデバイスは Intelligent Hub アプリがインストールされており初期設定が完了しているデバイスとなります。

Hub アプリインストール済みデバイス



デバイス > リスト表示

hana iPad iOS 13.1.1 JF8K

iPad 6th Gen (32 GB Silver) | 13.1.1 | 所有形態: 企業 - 専用

概要 順守 プロファイル アプリ コンテンツ 位置情報 ユーザー その他

デバイスに侵害は発生していません 0 順守違反 加入済み 2019/10/04 最終接続時間 2秒前

**セキュリティ**

- ✓ UEMによる管理
- 監視対象
- 「iPhoneを探す」が有効です
- アクティベーションロック無効
- iCloudのバックアップ有効

**ユーザー情報**

ユーザー名  
hana

名前  
[redacted]

Eメール  
hana@wizaas.com

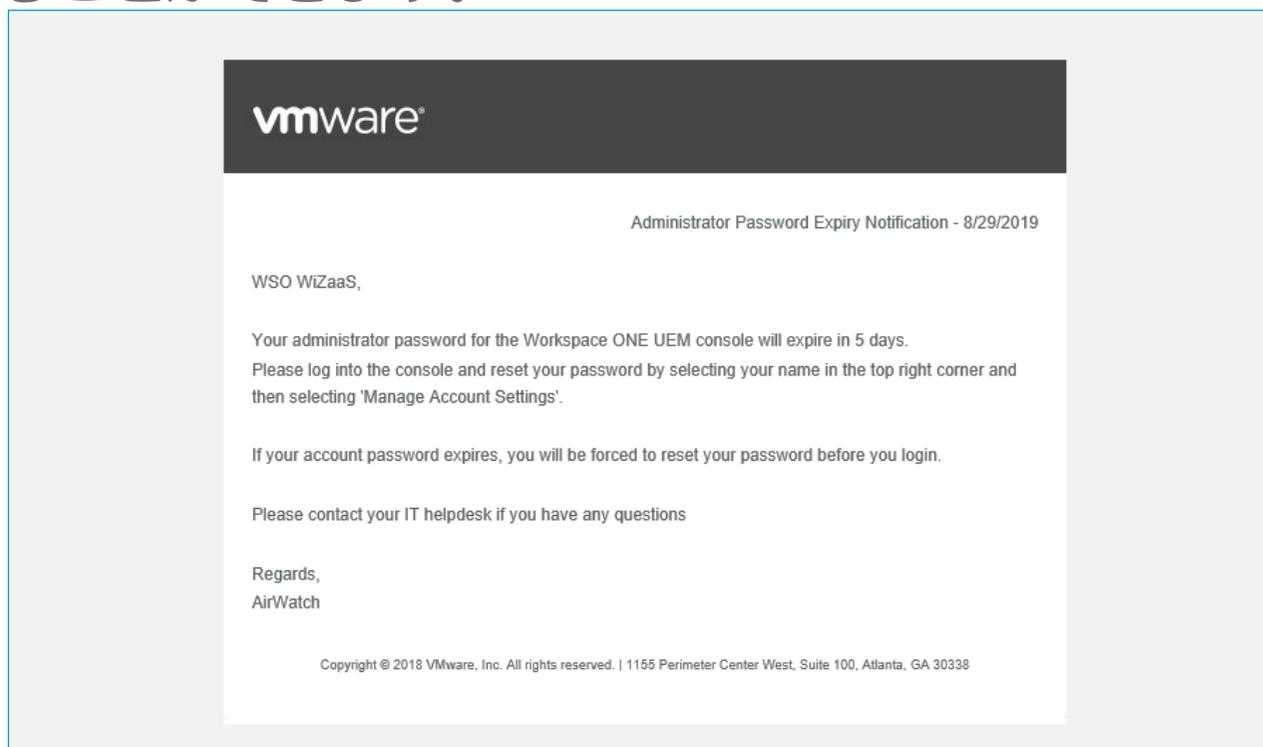
# WS1 UEM Console / マイサービス

右メニューボタンより、設定を行った Workspace ONE サービスへの切り替えメニューが追加されました。



# WS1 UEM Console / 管理者アカウント

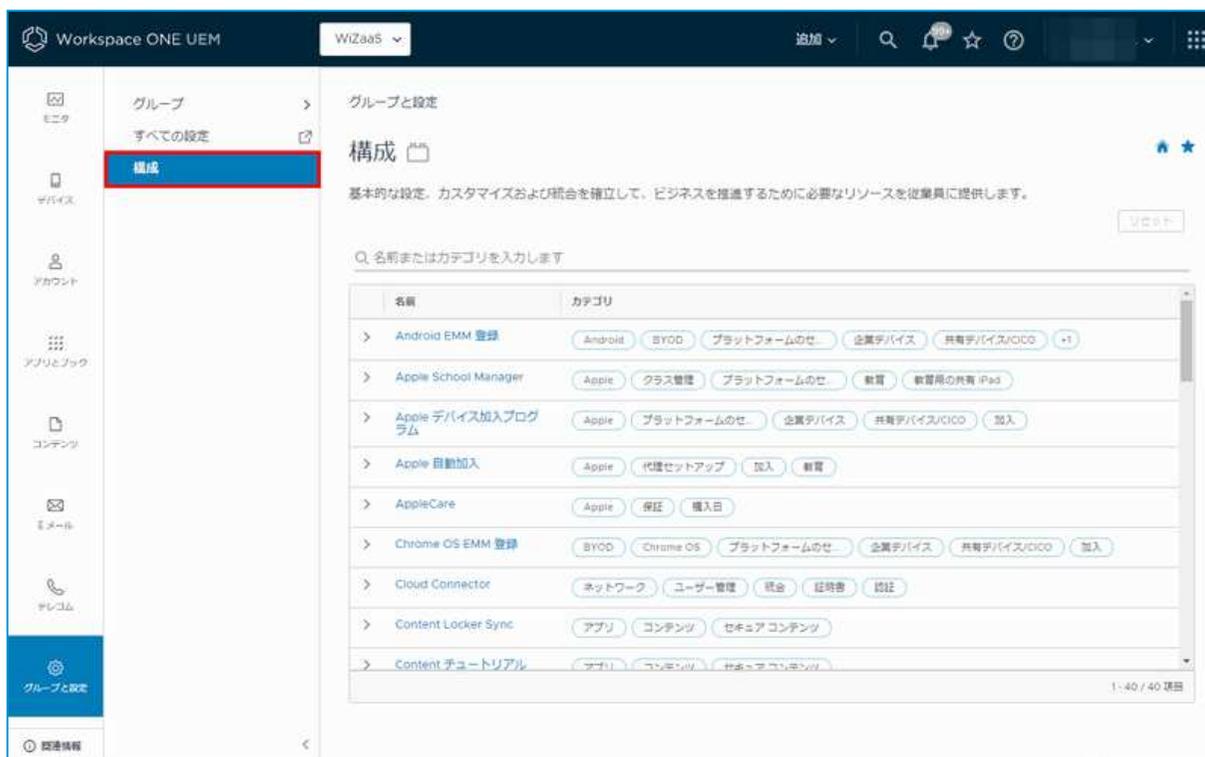
管理者アカウントのパスワードの有効期限が切れる 5 日前に管理者宛てに E メールを送信する機能が追加されました。管理者はパスワードの有効期限が切れるタイミングを把握することができます。



※共有環境の Workspace ONE UEM は 5日という既定値の変更は行えません。

# WS1 UEM Console / 構成

サブメニューに「構成」が追加されました。「すべての設定」メニューの要素が一か所に集約して提供されており、アクセスおよびアクションがより行いやすくなっています。また、タグベースのより直感的な検索機能で、必要なコンポーネントをすばやく簡単に見つけることができます。



Workspace ONE UEM console screenshot showing the '構成' (Configuration) menu item highlighted in the left sidebar. The main content area displays a list of configuration items with their names and categories.

名前	カテゴリ
> Android EMM 登録	Android BYOD プラットフォームのせ 企業デバイス 共有デバイス/CICO +1
> Apple School Manager	Apple クラス管理 プラットフォームのせ 教育 教育用の共有 iPad
> Apple デバイス加入プログラム	Apple プラットフォームのせ 企業デバイス 共有デバイス/CICO 加入
> Apple 自動加入	Apple 代理セットアップ 加入 教育
> AppleCare	Apple 保証 購入日
> Chrome OS EMM 登録	BYOD Chrome OS プラットフォームのせ 企業デバイス 共有デバイス/CICO 加入
> Cloud Connector	ネットワーク ユーザー管理 統合 証明書 認証
> Content Locker Sync	アプリ コンテンツ セキュアコンテンツ
> Content チュートリアル	アプリ コンテンツ セキュアコンテンツ

# WS1 UEM Console / グローバル検索

グローバル検索結果から [設定] タブが削除され、これにより検索速度が向上します。



# WS1 UEM Console / メッセージテンプレート

新しいシステムでは、管理者がメッセージテンプレートを使用すると、アクティブな言語のテンプレートのみが表示されます。

デバイスとユーザー > 全般

メッセージテンプレート

フィルタ    リストを検索

名前	カテゴリ	タイプ	モード	説明
① デバイス アクティベーション (HTML)	加入	MDM デバイス アクティベーション	システム	デバイスを加入できることをユーザーに通知
② ユーザー アクティベーション (HTML)	加入	ユーザー アクティベーション	システム	EMM ユーザーとして追加されてデバイスの
③ アプリケーション購入 (HTML)	アプリケーション	購入済アプリ	システム	ユーザーに代わってアプリケーションが購
④ デバイスの登録解除 (HTML)	加入	デバイスの登録解除	システム	デバイスが加入解除され、すべての組織
⑤ 順守違反ユーザー通知 (HTML)	順守	順守違反ユーザー通知	システム	順守違反ユーザー通知 (HTML)
⑥ 順守状態チェックの要求 (HTML)	順守	順守状態チェックの要求	システム	デバイスの返却と侵害状態スキャンを許可
⑦ 利用規約通知 (HTML)	利用規約	利用規約通知	システム	利用規約が追加または更新されたため、通
⑧ アプリケーション通知 (HTML)	アプリケーション	アプリケーション通知	システム	アプリ カタログで新しいアプリケーション
⑨ アプリ利用規約 - 最終通知 (HTML)	アプリケーション	アプリケーション利用規約最終通知	システム	アプリケーションの更新または追加された
⑩ MAM 管理者 - 新規ユーザー アクティベーションを開始 (HTML)	加入	MAM管理者 - 新規ユーザー アクティベーションを開始	システム	管理者が、MAM 加入のために構成した組
⑪ MAM ユーザー - 新規ユーザー アクティベーションを開始 (HTML)	加入	MAM新規ユーザー アクティベーション	システム	ユーザーが、MAM 加入のために構成した
⑫ App Catalog トークン通知 (HTML)	アプリケーション	App Catalog トークン通知	システム	アプリ カタログに最初にアクセスするとき
⑬ SDK に対するアプリケーション ログ通知 (HTML)	アプリケーション	アプリケーションログ通知	システム	SDK 対応アプリケーションでクラッシュロ
⑭ E メールドメイン登録 (HTML)	加入	メールドメイン登録	システム	簡単にメールドメインを追加して使用する E

項目 1 - 47/47

1 ページに表示する項目数: 50

# WS1 UEM Console / Legacy Android 移行

Legacy Android 管理(旧来の Android 管理)上のデバイスを Work プロファイルに移動するための、プログラムによる移行ワークフローが追加されました。Legacy Android 環境から Android Enterprise (旧 Android for Work) に移行すると、すべての OEM デバイスの制御と一貫性が向上します。

The screenshot displays the 'Legacy Android 移行' (Legacy Android Migration) page in the VMware UEM console. The page is titled 'デバイス > ライフサイクル' (Devices > Lifecycle) and 'Legacy Android 移行'. It features a main heading 'Legacy Android 管理の作業プロファイルへの移行および監視が一層簡単になりました。' (Migration and monitoring of Legacy Android management work profiles is now even simpler.) and a sub-heading '新しい移行を今すぐセットアップします。' (Set up the new migration now.). A '新しい移行' (New Migration) button is visible. Below this, there are three columns of information:

- 一貫性のある制御と一貫性** (Consistent control and consistency): 'すべての機能が各 OEM デバイスで同じように動作することを保証します。' (We guarantee that all features will operate the same way on all OEM devices.)
- Google Play ストアでアプリを管理** (Manage apps on Google Play Store): '従業員に、より信頼性の高い統合されたアプリエクスペリエンスを提供します。' (We provide employees with a more reliable, integrated app experience.)
- 業務アプリと個人アプリを分けて管理し、安全を確保** (Separate management of business and personal apps, ensuring security): '業務アプリとそのデータは個人アプリとは分けて保存、管理されるため、完全なデバイス削除は不要です。' (Business apps and their data are stored and managed separately from personal apps, so a full device wipe is not required.)

Below these columns, there are three sections under the heading '予期される事項' (Expected items):

- 一貫したデバイス管理** (Consistent device management): 'シガシー管理は、移行が完了するまで維持されます。' (Seamless management is maintained until migration is complete.)
- 既存のデバイスに影響はありません** (No impact on existing devices): '移行されていないデバイスは、影響を受けません。' (Devices not being migrated are unaffected.)
- 進行状況を追跡してアクションを実行** (Track progress and take action): '各デバイスの状態が、完了、処理中、取り当て済みのいずれかを確認してください。' (Check the status of each device as completed, in progress, or assigned.)

# WS1 UEM Console / デバイス タグ

デバイス タグの色とタイプのオプションは、コンソールから削除されました。  
複数のデバイスからデバイス タグを同時に割り当て解除できるようになりました。



# WS1 UEM Console / ディレクトリサービス

ディレクトリサービスのセットアップ時に、ディレクトリユーザーおよびユーザーグループとその属性を検証できるようになりました。誤ったディレクトリサービスのセットアップによって発生する不適切な構成を回避するために有効です。

### 接続のテスト

サーバ

ドメイン 状態

wizaas.com

もう一度テストする

ユーザー グループ

ドメイン wizaas.com

ユーザー名

ユーザーを確認

キャンセル

VMware Identity Manager の名称が Workspace ONE Access に変わりました。

Workspace ONE Access 環境をご利用されているお客様は、URLと管理者資格情報を入力するだけで、Hub サービスを簡単にアクティブ化できるようになりました。また、Workspace ONE Access 環境をご利用されていないお客様でも、リクエストウィザードに従い操作するだけで、Hub サービスを簡単にアクティブ化できるようになりました。

The image displays a series of overlapping screenshots from the VMware Identity Manager console, illustrating the process of activating the Hub Service. The steps shown are:

- グループと設定 (Group and Settings):** Shows the 'Intelligent Hub' and 'Hub サービス (Hub Service)' sections. A blue arrow points to the 'Hub サービス' section.
- サービス条件 (Service Conditions):** A dialog box titled 'クラウドテナントのリクエスト (Request Cloud Tenant)' with steps: 1. サービス条件 (Service Conditions), 2. 管理者の詳細 (Administrator Details), 3. データセンターの場所を選択 (Select Data Center Location), 4. クラウドテナントのリクエスト (Request Cloud Tenant).
- 管理者の詳細 (Administrator Details):** A dialog box for entering administrator information.
- データセンターの場所を選択 (Select Data Center Location):** A dialog box for selecting a data center location.
- クラウドテナントのリクエスト (Request Cloud Tenant):** A dialog box for selecting a cloud tenant.
- テナント名 (Tenant Name):** A dialog box for entering the tenant name.
- グループと設定 (Group and Settings):** The final configuration page for the Hub Service. A red box highlights the 'Hub サービス URL (Hub Service URL)' field, which contains the URL: `https://[tenant-name].vmwareidentity.com`.

自動的にWS1 Access 環境がデプロイされ、WS1 UEM 環境と連携します。12

# WS1 UEM Console / リスト エクスポート

リストビューを XLSX ファイルとしてエクスポートできる機能が追加されました。  
従来の CSV ファイルとしてのエクスポートも有効です。

The screenshot displays the VMware Workspace ONE UEM console interface. The left sidebar shows navigation options like 'ダッシュボード' (Dashboard), 'リスト表示' (List View), 'デバイス更新' (Device Updates), etc. The main content area is titled 'デバイス リスト表示' (Devices List View). At the top right of the main area, there is an 'エクスポート' (Export) dropdown menu, which is currently open, showing 'CSV' and 'XLSX' options. Below the menu is a table of devices. The table has columns for '最終接続時間' (Last connection time), '一般情報' (General information), 'プラットフォーム' (Platform), and 'ユーザー' (User). The table contains three rows of device information.

最終接続時間	一般情報	プラットフォーム	ユーザー
2分	WiZaaS / wizaas.co.jp UEM 管理対象   企業 - 専用	Apple iOS iPad 6th Gen ... 13.1.0	
39分	WiZaaS / wizaas.co.jp UEM 管理対象   企業 - 専用	Android docomo SO-0... 8.0.0	
39分	WiZaaS / wizaas.co.jp MDM   企業 - 専用	Windows デ... HP Z240 SFF ... 10.0.18362	

# WS1 UEM Console / デバイス情報

デバイス詳細およびデバイス リスト表示に、パブリック IP アドレスという新しいデバイス識別子が追加されました。管理しているデバイスが利用しているパブリック IP アドレスの確認が行えます。

リスト表示

フィルタ >> [デバイスを追加](#) [レイアウト](#) [リフレッシュ](#) [エクスポート](#) [リストを検索](#)

	プラットフォーム	OS	モデル	管理	現在のキャリア	パブリック IP アドレス
<input type="checkbox"/>	Android	8.0.0	docomo SO-03j	UEM 管理対象	NTT DOCOMO	1 . 2
<input type="checkbox"/>	Windows デスクトップ	10.0.18362	HP Z240 SFF Workstation	MDM	不明	61 . 5
<input type="checkbox"/>	Windows デスクトップ	10.0.17763	HP Z240 SFF Workstation	MDM	不明	61 . 5
<input type="checkbox"/>	Android	7.1.1	google Nexus 6	UEM 管理対象	不明	61 . 5
<input type="checkbox"/>	Apple iOS	13.1.0	iPad 6th Gen (32 GB Silver)	UEM 管理対象	不明	61 . 5
<input type="checkbox"/>	Apple iOS	12.4.1	iPhone 7	UEM 管理対象	NTT DOCOMO	1 . 222
<input type="checkbox"/>	Apple iOS	12.4.1	iPhone X (64 GB Space Gr...	MDM	NTT DOCOMO	1 . 100
<input type="checkbox"/>	Windows デスクトップ	10.0.18362	CFR26-2	MDM	不明	61 . 5
<input type="checkbox"/>	Windows デスクトップ	10.0.17763	CFR26-2	MDM	NTT DOCOMO	61 . 5
<input type="checkbox"/>	Apple iOS	12.4.1	iPhone Xs (256 GB Gold)	UEM 管理対象	プライベート	プライベート
<input type="checkbox"/>	Apple iOS	12.2.0	iPad Air 2 (16 GB Gold)	UEM 管理対象	不明	126 . 47

※パブリック IP アドレス情報の収集は、[プライバシー] 設定で行えます。

# WS1 UEM Console / スマートグループ

スマートグループ作成時に使用できる便利なカテゴリ [管理タイプ] と [加入カテゴリ] が加わりました。フィルタ条件がさらにスマートに分類できます。

新しいスマートグループを作成

名前

管理元

タイプを選択

デバイスプレビュー

管理タイプ

任意

選択

MDM 加入済み

アプリケーション管理

加入カテゴリ

任意

選択

Apple - DEP 加入済み

Apple - ユーザーによって承認された MDM に加入しました

Apple - 監視対象

Apple - EDU 共有 iPad モード

Android (Legacy)

Android Enterprise

追加

除外

パフォーマンスを向上させるには、ライブ表示を無効にしてください。

# WS1 UEM Console / WS1 Access

ベーシックユーザーの同期を有効にして、ローカルユーザーを Workspace ONE Access (VMware Identity Manager) のローカル UEM ディレクトリに同期する機能が追加されました。ユーザーを同期することにより Workspace ONE Intelligent Hub アプリを使用してリソースへのシングルサインオン アクセスを行えます。

システム > エンタープライズ統合

### VMware Identity Manager

サーバ \_\_\_\_\_

ユーザー、デバイス、およびハイブリッドクラウド間の信頼を確立し、シームレスなユーザー エクスペリエンスと、Web、ネイティブ、仮想アプリによる統合されたアプリ カタログへの強力な条件付きアクセスを実現します。

URL

管理者ユーザー名

Active Directory Basic  有効  無効

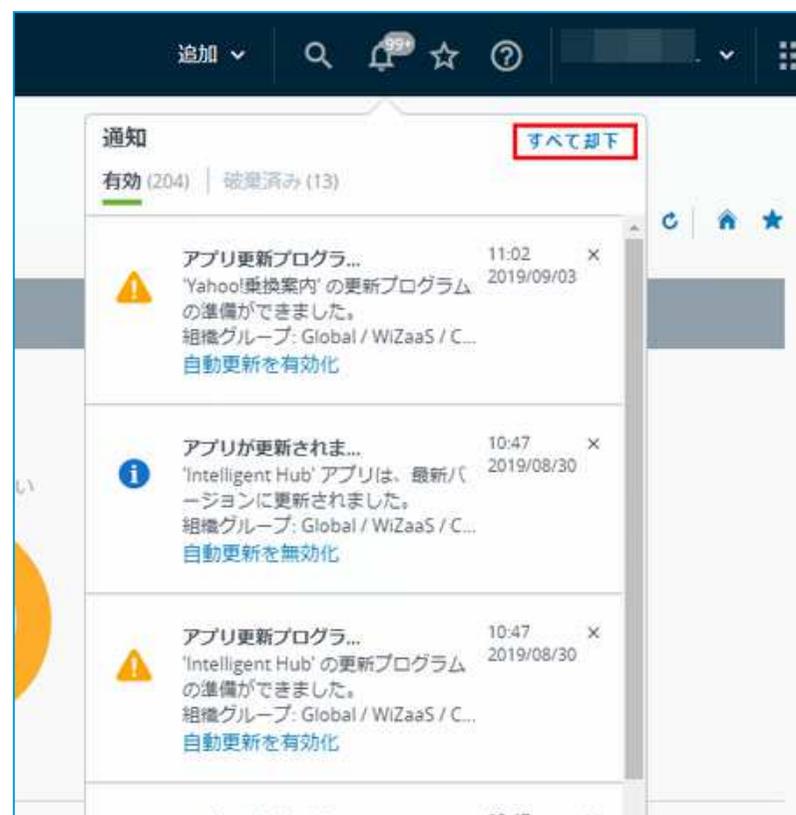
**ベーシックユーザーの同期**  有効化

ローカルベーシックユーザーの同期では、IDMでWorkspace ONE UEMベーシックユーザーを使用できます。有効にした場合、ローカルベーシックユーザーの同期は無効にできません。

このアクション ボタンを使用して、自動生成された UEM API キーを使用するように Workspace ONE IDM-UEM の構成を更新します

## WS1 UEM Console / コンソール通知

すべてのコンソール通知を 1 つのボタンでクリアする機能が追加されました。すべてのアクティブな通知を破棄して、破棄済み通知一覧に送ることができます。



# WS1 Intelligence / WS1 Sensors / Windows 10

1905

Windows 10 デバイスの、ハードウェア、OS、などの情報を追跡するために、Workspace ONE Sensors をリリースいたしました。今後は特定の属性に対するセンサーを作成し、ダッシュボードやカスタマイズ レポートに視覚化して、Workspace ONE Intelligenceに表示できるようになります。

The screenshot displays the Workspace ONE Intelligence interface. On the left, the 'Workspace ONE UEM' navigation pane is visible, with 'デバイス' (Devices) selected. The main area shows the 'センサー' (Sensors) configuration page, where a 'cpu\_info\_01' sensor is being configured. A 'レポート' (Report) section is also visible, showing a 'Windows 10 Inventory: 概要' report. The report preview shows a table with 6 records.

pc_vendor	cpu_info_01	cpu_info_02	device_guid
HP	Intel64 Family 6 Model 94 Stepping 3	Intel(R) Xeon(R) CPU E3-1225 v5 @ 3.30GHz	db6105f1-94c5-4de8-8876-bb4...
LENOVO	AMD64 Family 21 Model 112 Stepping 0	AMD A4-9125 RADEON R3, 4 COMPUTE CORES 2C+2G	21a2528b-0547-4c6c-98df-12ad...
LENOVO	AMD64 Family 21 Model 112 Stepping 0	AMD A4-9125 RADEON R3, 4 COMPUTE CORES 2C+2G	57d3ba9f-22a0-4b57-b3c4-123...
HP	Intel64 Family 6 Model 94 Stepping 3	Intel(R) Xeon(R) CPU E3-1225 v5 @ 3.30GHz	#3d3944b-9c30-4500-898c-67...
Panasonic Corporation	Intel64 Family 6 Model 142 Stepping 9	Intel(R) Core(TM) i5-7Y57 CPU @ 1.20GHz	#f09606d-262d-4209-be7a-24...
Panasonic Corporation	Intel64 Family 6 Model 142 Stepping 9	Intel(R) Core(TM) i5-7Y57 CPU @ 1.20GHz	87dc379e-1afb-4d97-98ff-9c56...

WS1 Intelligence で Windows 10 デバイスの情報を視覚化

WS1 UEM で Windows 10 デバイスの情報を取得

# WS1 UEM MAM / Tunnel

Tunnel (PerApp VPN) 設定の展開と管理を簡素化するため、新しい管理者エクスペリエンスに変更いたしました。エクスペリエンスを開始するには、[グループと設定] > [構成] > [Tunnel] の順に選択してください。

VMware Tunnel (PerApp VPN)メニューと VMware Tunnel プロキシメニューが分離しました

クリックすると刷新された画面が表示されます

システム

エンタープライズ統合 ①

エンタープライズ統合サービス

認証局

Content Gateway

Cloud Connector

ディレクトリサービス

Eメール (SMTP)

VMware Tunnel

VMware Tunnel プロキシ

ピアツーピア

サードパーティ製プロキシ

ブルサービス インストーラ

SMS

Syslog

VMware Identity Manager

### Tunnel 構成

基本的な Tunnel アーキテクチャを構成して、環境内の接続性と信頼性を確立します。

編集 再動化 XML をダウンロード 接続のテスト 削除 ① インストーラをダウンロード

展開の詳細 Basic

展開の種類  ベーシック  カスケード ①

ホスト名 \*

ポート \* 8443

> サーバ認証	AirWatch
> クライアント認証	AirWatch
> ネットワーク	Disabled
> ログ収集	Disabled

デバイストラフィック規則

規則の総数 0

アプリ アクション

他のすべてのアプリケーション

サーバトラフィック規則

送信プロキシ

サーバトラフィック規則

# WS1 UEM MCM / 一括削除

管理コンテンツ リスト表示から複数のファイルを選択して、同時に削除できる機能が追加されました。

The screenshot shows the 'Content Locker' interface in VMware Workspace ONE UEM MCM. The page title is 'リスト表示' (List Display). Below the title, there are tabs for 'AirWatch 管理' and '企業ファイルサーバ'. A filter bar shows 'コンテンツを追加' (Add Content) and '使用中のストレージ' (Storage in Use) with a progress bar at 4.68. There are buttons for 'レイアウト' (Layout), 'リセット' (Reset), 'エクスポート' (Export), and 'リストを検索' (Search List). A dropdown menu 'その他のアクション' (Other Actions) is open, showing a '管理' (Manage) menu with a '削除' (Delete) option highlighted in a red box. The main table lists content items with columns for '管理' (Manage), '企業/従/共' (Company/Standard/Common), '管理元' (Source), '有効日' (Valid Date), 'ダウンロードタイプ' (Download Type), '編集者' (Editor), and 'インストール状態' (Install Status).

管理	企業/従/共	管理元	有効日	ダウンロードタイプ	編集者	インストール状態
削除	N/A	wizaas.co.jp	2018/12/21 0:00	オンデマンド		1 11
	N/A	wizaas.co.jp	2019/06/03 0:00	オンデマンド		1 11
	C	wizaas.co.jp	2019/05/24 0:00	オンデマンド		1 10
	N/A	wizaas.co.jp	2019/06/03 0:00	オンデマンド		0 11

# Apple iOS / MDM管理対象アプリ

デバイス利用者が App Store 経由などでアプリを管理対象外としてインストール済みの場合、かつ [ユーザーがインストールしたアプリを MDM 管理対象にする] 設定が有効になっている場合、[アプリ配信方法] が自動かオンデマンドかにかかわらず、コンソールはアプリを自動的に管理対象に変換するようになります。



アプリ配信方法	アプリの動作	
	UEMアップデート前	UEMアップデート後
自動	[自動インストール設定] 自動的に管理対象に変換	[自動インストール設定] 自動的に管理対象に変換
オンデマンド	[オンデマンドインストール設定] 手動で管理対象に変換	[オンデマンドインストール設定] <b>自動的に管理対象に変換</b>

【お願い】 UEM アップグレード後、監視対象外 iOS デバイスには管理アプリに関するプロンプトが表示される。このプロンプトについて、あらかじめデバイス利用者への注意喚起を行う事をお勧めいたします。

# Apple iOS / ワイプコマンド

アクティベーションロック対応 iOS デバイスの企業情報ワイプまたはデバイスワイプの現在のステータスについて正確なフィードバックを収集する機能が追加されました。管理者にとって、アクティベーションロック対応 iOS デバイスのワイプはさらに分かりやすく、削除はさらに効率よく実行できるようになりました。

リスト表示

フィルタ + デバイスを追加 レイアウト エクスポート リストを検索

最終接続時間	一般情報	プラットフォーム	ユーザー	タグ	加入	順守状態
6分	iPhone iOS 12.4.0 JCLK / Internal Testing / UEM 管理対象   企業 - 専用	Apple iOS iPhone X (64 ... 12.4.0			加入済み	順守状態
3分	iPhone iOS 12.4.0 JCLK / Internal Testing / UEM 管理対象   企業 - 専用	Apple iOS iPhone X (64 ... 12.4.0			ワイプが開始されました	順守状態
1秒	iPhone iOS 12.4.0 JCLK / Internal Testing / UEM 管理対象   企業 - 専用	Apple iOS iPhone X (64 ... 12.4.0			加入解除	情報なし

# Apple iOS / 構成プロファイル

iOS 13 の実装の変更に伴い、下記の制限が監視対象の iOS 13 デバイス以降で利用可能になります。

- ・iTunes
- ・Safari
- ・カメラ
- ・FaceTime
- ・不適切な単語フィルタ
- ・iCloud へのバックアップ
- ・iCloud とのドキュメントの同期
- ・iCloud とのキーチェーン同期
- ・Game Center での友人の追加
- ・Game Center でのマルチプレイヤー ゲーム

【コンソール表示の一例】



上記の制限 / プロファイルがすでに適用されている監視対象外デバイスを iOS 13 にアップグレードした場合、制限 / プロファイルはこれまでどおり機能する点にご注意してください。ただし、これらの制限 / プロファイルを削除または更新すると無効になります。また、これらの既存の制限 / プロファイルは新規加入した監視対象外デバイスの iOS 13 デバイスには適用されません。

# Apple iOS / 構成プロファイル

iOS 13 から Per-App VPN に、メール、カレンダー、および連絡先のドメインがサポートされました。Apple iOS 機能追加に伴い構成プロファイル / VPN にメール、カレンダー、および連絡先の UI が追加されました。

iOS 新しい Apple iOS プロファイルを追加

ペイロードの検索

全般  
パスコード  
制限  
Wi-Fi  
VPN ①  
E メール  
Exchange ActiveSync  
通知  
LDAP  
CalDAV  
定期配信カレンダー  
CardDAV  
Web クリップ  
資格情報  
SCEP  
グローバル HTTP プロキシ  
シングルアプリモード  
コンテンツフィルタ  
管理ドメイン

接続タイプ \* Workspace ONE Tunnel

サーバ \* TCP://uag.wizaas.com:8443

アプリベース VPN 規則  1057

VMware Tunnel を有効化  ①

プロバイダタイプ AppProxy

Safari ドメイン

メール ドメイン

連絡先ドメイン

カレンダー ドメイン

保存して公開 キャンセル

# Apple iOS / 構成プロファイル

iOS 13 から追加された機能制限の UI が追加されました。(監視対象)

- Wi-Fiのオン/オフ切替制限
- QuickPathキーボード利用制限
- USBドライブへのアクセス制限



# Apple iOS / 構成プロファイル

ネットワーク使用量規則ペイロードに新たな項目が追加されました。デバイスの物理 SIM カードと eSIM カードの Wi-Fi アシスト機能のセットアップが可能となりました。

iOS 新しい Apple iOS プロファイルを追加

ペイロードの検索

- CardDAV
- Web クリップ
- 資格情報
- SCEP
- グローバル HTTP プロキシ
- シングルアプリモード
- コンテンツフィルタ
- 管理ドメイン
- ネットワーク使用量規則**
- macOS サーバアカウント
- シングルサインオン
- AirPlay ミラーリング
- AirPrint
- セラー
- ホーム画面レイアウト
- 画面ロックメッセージ
- Google アカウント
- カスタム設定

### ネットワーク使用量規則

アプリ使用量規則

管理アプリのセルラーデータネットワークの使用方法を指定する iOS 9 + Supervised

アプリケーション識別子	セルラーデータを許可	ローミング中のデータ使用	
<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✕

+ 追加

### SIM 使用量規則

SIM のセルラーデータ ネットワークの使用方法を指定 iOS 13 + Supervised

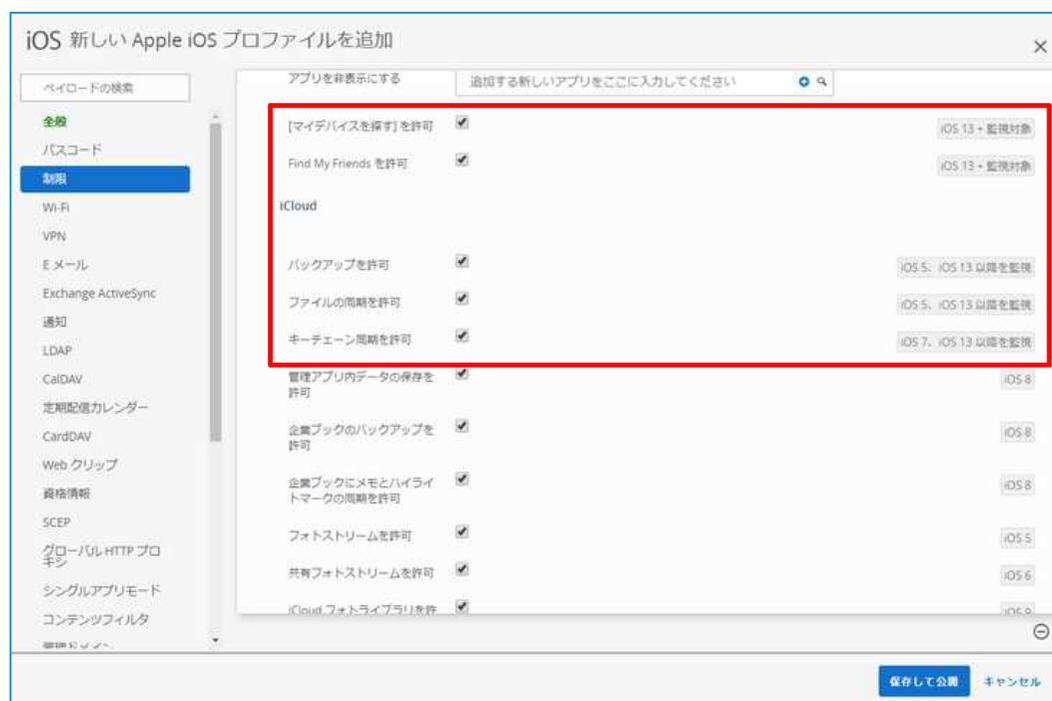
ICCID	Wi-Fi アシスト	
<input type="text"/>	設定	✕

+ 追加

保存して公開 キャンセル

# Apple iOS / 構成プロファイル

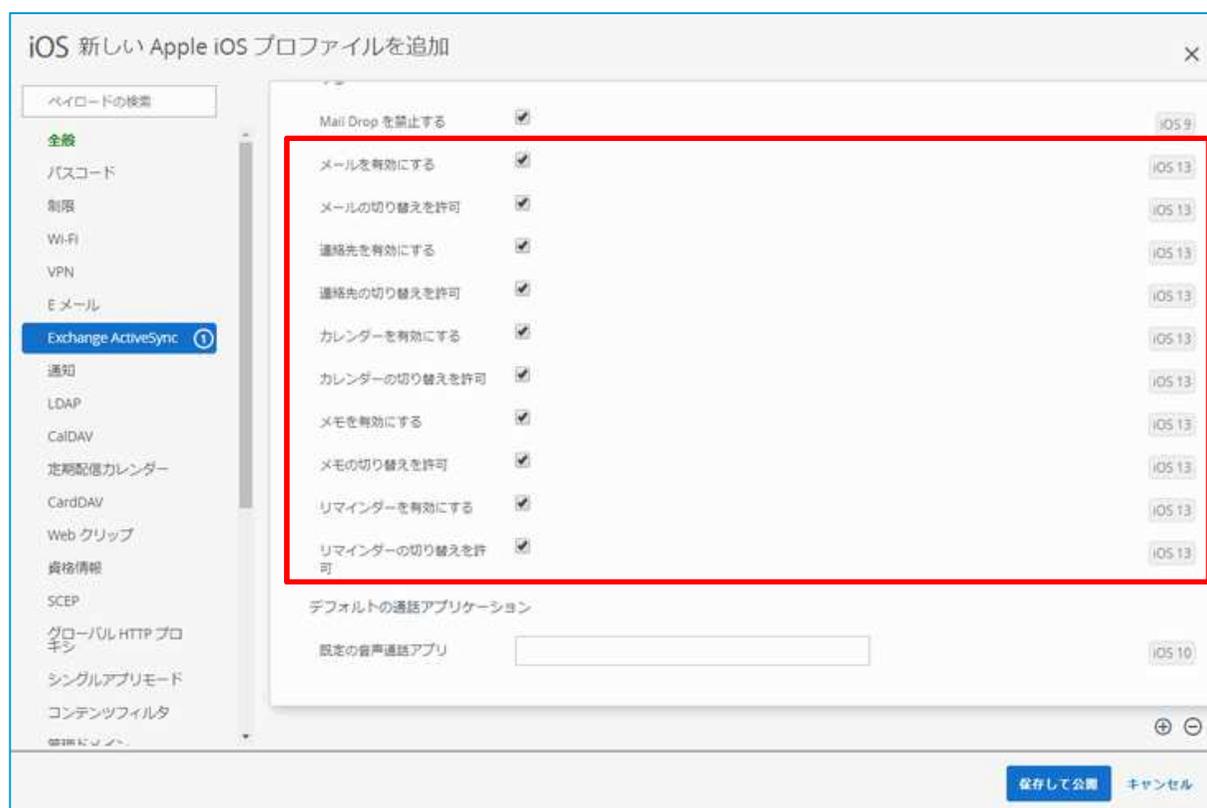
iOS 13 デバイスの新しい制限事項ペイロードが追加されました。Wi-Fi の切り替え、QuickPath キーボード、友達を探す、デバイスの検索を防止することが可能となりました。また、カメラ、Safari、iCloud バックアップ、明示的なコンテンツの制限など、監視を必要とする既存のオプションも複数追加されました。



※上記スクリーンショットは iOS 13 で追加、変更された制限事項の一例となります。

# Apple iOS / 構成プロファイル

iOS ネイティブメーラーにおける メール、連絡先、カレンダー、リマインダ、メモアプリの、ユーザーによる個別の切り替えを操作不可とする機能がExchange ActiveSync ペイロードに追加されました。



# Apple iOS / 構成プロファイル

iOS デバイスの制限プロファイルに [eSIM の変更を許可] 機能が追加されました。監視対象の iOS デバイスで、eSIM 構成をユーザーがセットアップまたは編集できないようにすることができます。



# Apple iOS / 構成プロファイル

ユーザーがパーソナルホットスポット設定を変更しないように制限機能が追加されました。iOS 12.2 [監視デバイス] 以降のデバイスで Siri がデータをログ収集してサーバに返すのを防止できるようになりました。



# Apple iOS / multiple SIM

新しいデュアル SIM サポートで物理 SIM と eSIM の両方について情報が確認できるよう機能が追加されました。

デバイス > リスト表示

iPhone iOS 12.4.1

iPhone X (64 GB Space Gray) | 12.4.1 | 所有形態: 企業 - 専用

概要 障害 トラブルシューティング アプリ コンテンツ 位置情報 ユーザー ネットワーク

セッティング

	SIM カード 1	SIM カード 2
状態	有効	有効
電話番号	080	080
ローミング設定 (音声/データ)	偽 / 偽	偽 / 偽
パーソナルホットスポット	無効	無効
IP アドレス	0.0.0.0	0.0.0.0
パブリック IP アドレス	1.72.7.100	1.72.7.100
オペレータ/キャリア	NTT DOCOMO	NTT DOCOMO
セルラー テクノロジー	高方	高方
IMEI	3	3
現在の SIM	eSIM	eSIM
許可された SIM		
キャリアバージョン	36.0.1	36.0.1
モデム ファームウェア		
現在の MCC/MNC	440 / 10	440 / 10
SIM MCC/MNC	/ 10	/ 10
データ優先	真	真
音声優先	情報なし	情報なし
ラベル	USER_LABEL_PRIMARY	USER_LABEL_PRIMARY
ラベル ID		
スロット	CTSUBSCRIPTIONSLOTONE	CTSUBSCRIPTIONSLOTONE

# Apple iOS / DEP

Apple 社は iOS 13 から設定アシスタント画面に至る前の加入プロセス中に、MDM で用意した Web ページ URL を表示することができるよう機能を追加しました。Workspace ONE UEM では、デバイス加入プログラム- ②認証「カスタム加入」で対応いたしました。「カスタム加入」オンにすることにより、カスタム利用規約やその他の必要なオプションを表示することが可能となりました。



2019年10月25日現在(Ws1 UEM v19.9.0.1)「カスタム加入」をオンにしてデバイスを加入させると、正常に加入できない事象を確認しております。「カスタム加入」をご利用を検討されるお客様においては本機能を検証いただいたうえで、導入のご検討をいただけますよう、お願い申し上げます。

# Apple iOS / DEP

iOS 13 デバイスの新セットアップ アシスタント画面のスキップ項目が追加されました。



# Android / コマンド

Android 8.0 以降を実行している Work Profile デバイスで、Work パスコード消去と Work パスコードのリセットの各コマンドを選択できるようになりました。Work パスコードの消去を実行すると、デバイス上の Work セキュリティ チャレンジが削除され、Work パスコードのリセットプロンプトが表示されて、新しいパスコードの入力が求められます。



消去、変更



# Android / パブリックアプリ その1

Android 向けパブリックアプリの割り当て設定を簡素化するため、新しい管理者エクスペリエンスに変更いたしました。

Salesforce - 割り当てを更新

割り当て 除外

デバイスは、次の構成に基づいてアプリケーションを受信します。  
デバイスが複数のグループに所属している場合、優先度が最も高い (0 が最高優先度) グループのポリシーを受信します。

割り当ての追加 編集 削除 上に移動 下に移動

	名前	優先度	アプリ配信方法	管理対象のアクセス	VPNアクセス	構成を送信する
<input type="radio"/>	All Devices	0	オンデマンド	<input type="radio"/> 無効	<input type="radio"/> 無効	<input type="radio"/> 無効

Salesforce - 割り当ての追加

割り当てグループ \*

アプリ配信方法 \*

柔軟な管理レベル: オープンアクセス  
最低限の管理で、ユーザーにアプリへのオープンアクセスを与えるポリシーを適用します。

データ漏洩防止 構成  
DLP ポリシーにより、デバイス上の管理アプリケーションおよび非管理アプリケーション間データ交換を制御できます。このアプリケーションのデータ損失を防止するには、「管理対象のアクセス」にし、目的のデバイスタイプに対して「無効」プロファイルを作成します。

管理対象のアクセス

アプリトネル

プレリリースバージョン \* なし

アプリケーション構成 構成

キャンセル 追加

# Android / パブリックアプリ その2

App Config に対応したパブリックアプリのアプリ構成を読み込む機能が追加されました。App Config に対応のアプリ構成の設定がよりわかりやすくなりました。

The screenshot displays the 'Salesforce - アプリケーション構成' (Salesforce - Application Configuration) dialog box. The dialog is divided into two main sections. The left section contains a search bar and a list of configuration items, with the '構成' (Configure) button highlighted in a red box. The right section contains a list of configuration items with their respective values and controls.

Configuration Item	Value / Control
AppServiceHosts	_____ ⓘ
AppServiceHostLabels	_____ ⓘ
ManagedAppOAuthID	_____ ⓘ
ManagedAppCallbackURL	_____ ⓘ
RequireCertAuth	無効化 ⓘ
ManagedAppCertAlias	_____ ⓘ
OnlyShowAuthorizedHosts	無効化 ⓘ
IDPAppURLScheme	_____ ⓘ

# Android / 構成プロファイル

Android デバイスのパスコード プロファイルが強化されました。この強化によりネイティブ機能のサポートが改善されます。

- デバイスの業務使用と個人使用で別のパスコードの設定が可能
- パスワード有効期限の最大日数が 180 日から 9999 日へ変更
- 各種バイOMETRICS パスコード オプションの追加 (Android 9)

新しい Android プロファイルを追加

パスワード

Work パスコード

Work パスコードポリシーを有効化

パスワードの長さ \* 4

パスワードのコンテンツ \* 数字

実行失敗回数の上限 --

パスワードの有効期限 9999

パスワードの種類

デバイスロック タイムアウト (分)

ワンロックを許可

バイOMETRICS オプションを許可

顔認識センサーを許可

顔スキャンを許可

虹彩スキャンを許可

デバイスパスワード

Work プロファイルを使って追加したデバイスのパスワード ポリシーを使用します。このパスワードは、デバイスをロック解除する際に入力する必要があります。業務用パスワードが適用されている場合でも適用できます。Work 管理デバイスには、このパスワード ポリシーが適用されません。

デバイスパスワードポリシーを有効化

# Android / 構成プロファイル

Android デバイスに [カスタムメッセージ] プロファイルでメッセージを配信する機能が追加されました。

**新しい Android プロファイルを追加**

ペイロードの検索

全般

パスワード

Chrome ブラウザ設定

制限

Exchange ActiveSync

パブリック アプリ自動更新

資格情報

**カスタムメッセージ**

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

**カスタム メッセージ**

ロック画面メッセージを設定  有効  無効 Android 7.0+ Work Managed Device

ロックされているときのデバイス画面に、メッセージが表示されます。デバイスの紛失時または盗難時に役立ちます。

ブロックされた設定のメッセージを設定  有効  無効 Android 7.0+ Work Profile/Work Managed Device

ブロックされた設定または機能をユーザーがクリックしたときに、サポートメッセージを表示して、その機能にアクセスできない理由を簡単に説明できます。

設定でユーザーに表示するメッセージを設定  有効  無効 Android 7.0+ Work Profile/Work Managed Device

ユーザーは、このメッセージをデバイスの [設定] > [セキュリティ] > [デバイス] で表示できます。

保存して公開 キャンセル

15:38

この端末は超額によって管理されています  
急速充電中 (完了まで2 時間)

アカウントの追加

Duo プレビュー

Google

操作が許可されていません

ブロックされた設定または機能をユーザーがクリックしたときに、サポートメッセージを表示して、その機能にアクセスできない理由を簡単に説明できます。

詳細

OK

# Android / Firebase Cloud Messaging

Google の Firebase Cloud Messaging (FCM) サービスのサポートを追加しました。Android デバイスの通信については、Firebase Messaging 実装が Google Cloud Messaging の代わりとなります。



※従来通り、AWCM (AirWatch Cloud Messaging) をメッセージングサービスとしてご利用できます。

# Android / Work 管理対象デバイス

Work 管理対象デバイス (Work Managed Device) の企業情報ワイプ デバイス コマンドが削除され、サポートされなくなりました。  
管理者はデバイス ワイプ コマンドを使用して、デバイスで工場出荷時状態リセットを行ってください。



# Android / Office 365 アプリ

Office 365 の「はじめに」のウィザードで、Android Enterprise 向けの Office 365 アプリを自動的に承認できる機能が追加されました。

### Office 365 アプリを追加

1 選択 2 概要

プラットフォームを選択してください。

Android  iOS

追加したい Office 365 アプリを選択してください。なお、追加済みアプリは置換されません。

**Android アプリおよび関連するすべての権限は、Google Play ストアアカウントで自動的に承認および更新されます。**

また、パブリックアプリ画面からアプリを追加して、権限の表示と手動での承認を行うこともできます。

アプリケーション	プラットフォーム	状態
<input checked="" type="checkbox"/> Microsoft Word	Android	追加済
<input checked="" type="checkbox"/> Microsoft PowerPoint	Android	追加済
<input checked="" type="checkbox"/> Microsoft Excel	Android	追加済
<input checked="" type="checkbox"/> Microsoft Outlook	Android	追加されていません
<input checked="" type="checkbox"/> Microsoft OneNote	Android	追加されていません
<input type="checkbox"/> Microsoft SharePoint	Android	追加されていません
<input type="checkbox"/> Microsoft OneDrive	Android	追加されていません

次へ キャンセル

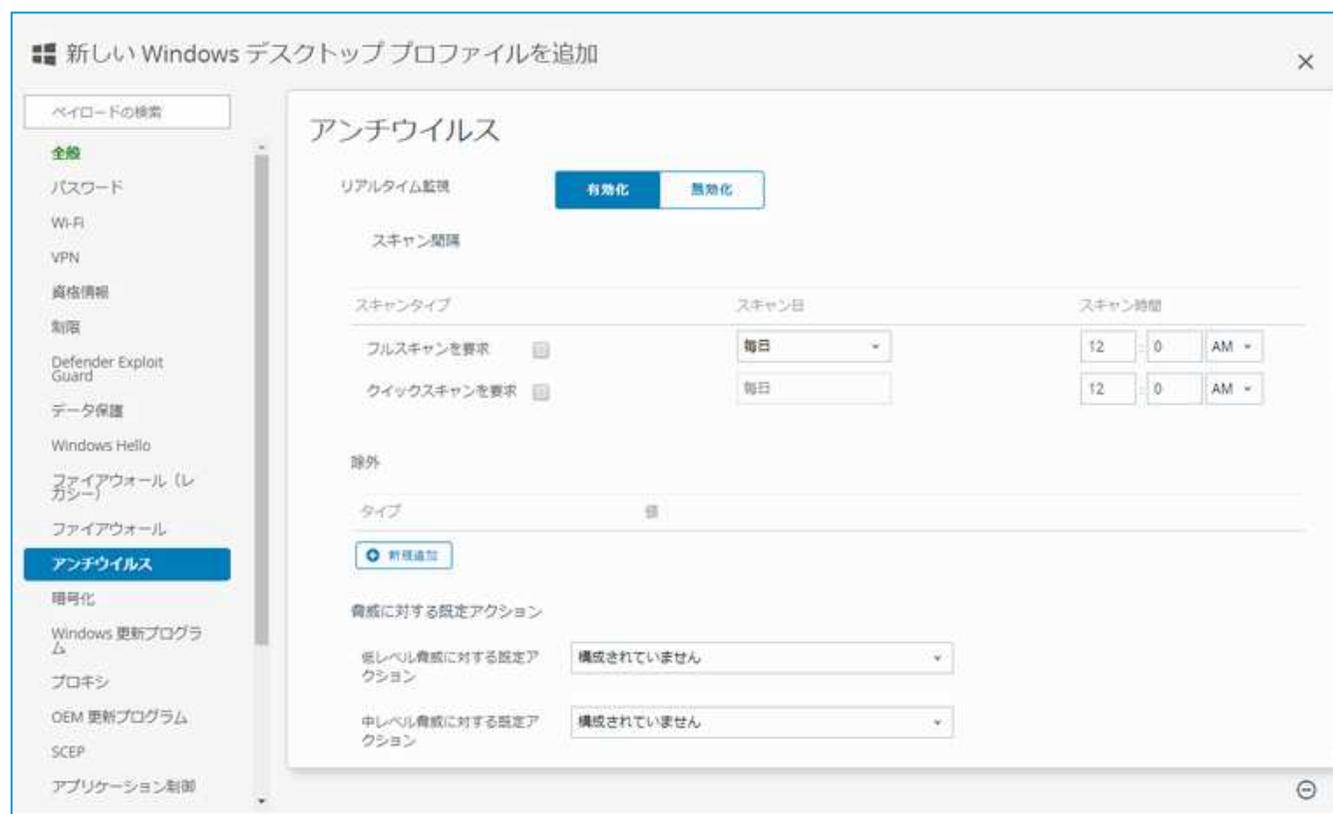
# Windows 10 / ベースライン

Windows 10 デバイスを業界のベスト プラクティス設定にしておくために、ベースライン機能があらたに追加されました。ベースラインにより、デバイスをセキュアな状態に保ち、CIS ベンチマークなどの業界標準に適合させることができます。

The screenshot displays the Workspace ONE UEM console interface. The top navigation bar shows 'Workspace ONE UEM' and the user 'WiZaaS / wizaas.co.jp'. The left sidebar contains navigation options such as 'はじめに', 'モニタ', 'デバイス', 'アカウント', and 'アプリとブック'. The main content area is titled 'デバイス > プロファイルとリソース' and 'ベースライン'. A modal window titled '新しいベースライン' is open, showing a list of steps: 1. 全般, 2. ベースラインの選択 (highlighted), 3. カスタマイズ, 4. ポリシーを追加, 5. 概要. The 'ベースラインの選択' step is active, displaying a selection screen with the instruction '事前構成されているベースラインとバージョンを選択します。'. Three options are visible: 'Windows 10 Security Baseline' (version 1709), 'CIS Windows 10 Benchmarks' (version 1709, L1), and 'カスタム ベースライン' with an 'アップロード' button.

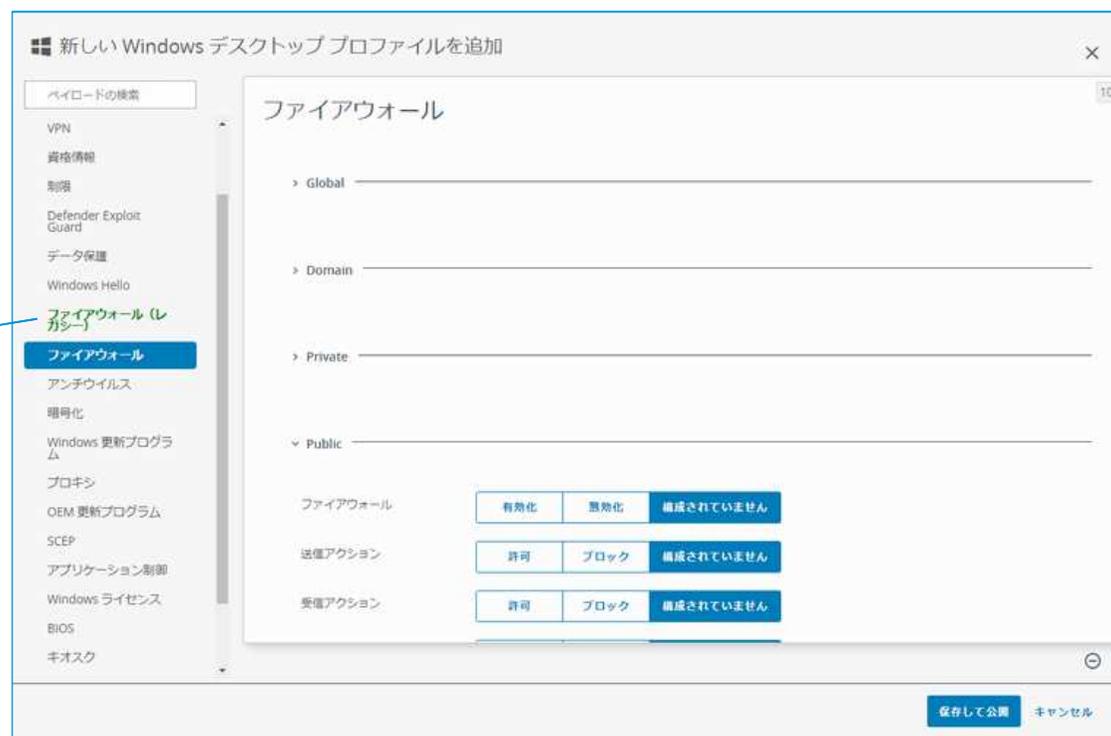
# Windows 10 / Anti-Virus

Windows 10 デバイス用ウイルス対策プロファイルが更新されてエージェントアプリ (Intelligent Hub) が不要になりました。そのため、Windows 10 デバイスを Windows Defender でより簡単に保護できるようになりました。



# Windows 10 / 構成プロファイル

Windows ファイアウォールの構成プロファイルが機能追加され、ドメイン接続、パブリック接続、およびプライベート接続に対して異なる動作を構成できるようになりました。また、独自のカスタム ファイアウォールルールを追加することもできます。



従来の設定は、ファイアウォール(レガシー)に変更されました。すでに設定済みの場合でも、引き続き当該設定は有効です。

※要件: Windows 10 1709 以上

# Windows 10 / 構成プロファイル

Windows 10 デバイスのプロファイルに [個人用設定] 機能が追加されました。デバイスの背景とロック画面の画像、およびスタートメニュー ポリシーを制御します。また、スタート画面のレイアウトの XML ファイルでアップロードできます。この XML ファイルは、既定のスタートメニューのレイアウトを上書きして、デバイス利用者による変更を制御します。



※要件: Windows 10 1703 以上

WiZaaS Co.,Ltd. ©2019 All Rights Reserved.

# Windows 10 / Dell Provisioning

テンプレートを使用すると、アプリを含むプロビジョニングパッケージの設定を構成し、後で使用できるように設定を保存する機能が追加されました。また、既存のプロビジョニングパッケージを [編集] および [削除] する機能も追加されました。



【注意】 1904 以降へのアップグレード時に既存の PPKG がある場合、その PPKG は、新しいワークフローをサポートしていないため削除されますのでご注意ください。また、既存の PPKG の再作成が必要になりますので、既存の設定内容を記録しておくことをお勧めいたします。

# Windows 10 / Catalog

社内アプリまたはパブリック アプリを割り当てるときに、[App Catalog に表示] オプションを使用して、展開したいがカタログでは公開したくないファイルを非表示にすることができます。

7-Zip 19.00 (x64 edition) - 割り当ての追加

割り当てグループを選択

アプリ配信方法 \*

App Catalog に表示   ①

展開の開始日: \*

現在のタイムゾーン: (GMT+09:00) Japan

ポリシー

柔軟な管理レベル: 管理対象のアクセス

デバイスの管理に基づいて、ユーザーにアプリへのアクセスを与えるポリシーを適用します。

## ゲートウェイサーバーのサポート終了について

- Workspace ONE UEM バージョン 1811 の際に構築、更新を行ったお客様
  - AirWatch Cloud Connector (ACC)
  - VMware Tunnel
  - Secure Email Gateway (SEG)サポート終了日: 2020年 6月 20日
  
- UAG (Unified Access Gateway ) をご利用のお客様  
お客様がご利用いただいている UAG バージョンと WS1 UEM 1811 の相互運用マトリックスをご確認いただけますようお願いいたします。

[https://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php#interop&382=&326=&hideEmpty=false&hideUnsupported=false](https://www.vmware.com/resources/compatibility/sim/interop_matrix.php#interop&382=&326=&hideEmpty=false&hideUnsupported=false)

サポート終了までに、アップグレードのご検討をいただけますようお願いいたします。

## Apple VPP & DEP サービス終了について

Device Enrollment Program (DEP) と Volume Purchase Program (VPP) の機能は、Apple School Manager または Apple Business Manager に統合され新たなサービスとして提供されます。

DEP および VPP のサービスは **2019年 12月 1日**に終了いたしますので、Apple School Manager または Apple Business Manager へのアップグレードを行ってください。

<https://support.apple.com/ja-jp/HT209617>

# Workspace ONE UEM 1909 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 1909 へのアップグレード作業

日程:

2019年11月12日 午前 0時 ~ 午前 4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。