Workspace ONE UEM 管理コンソールガイド(入門編)

Workspace ONE UEM 2109 WebUI ベース

2022 年 1 月 21 日 株式会社ウィザース

Copyright(C) 2022 WiZaaS Co., Ltd. Rights Reserved.

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2月26日	第二版発行
3.00	2014年7月31日	第三版発行
4.00	2014年12月31日	第四版発行
5.00	2015年7月31日	第五版発行
6.00	2016年1月20日	第六版発行
6.01	2016年3月8日	第六版更新
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	第九版発行
10.0	2018年6月20日	第十版発行 AirWatch Ver9.2 対応
11.0	2018年8月21日	第十一版発行 Workspace ONE UEM Ver9.5 対応
12.0	2019年1月18日	第十二版発行 Workspace ONE UEM Ver18.11 対応
13.0	2019年11月1日	第十二版発行 Workspace ONE UEM 1909 版
14.0	2020年7月7日	第十二版発行 Workspace ONE UEM 1909 Web UI ベース版
15.0	2020年12月25日	第十三版発行 Workspace ONE UEM 2011 Web UI ベース版
16.0	2022年1月21日	第十四版発行 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。

1		本書	青について	. 1
2		本書	言での操作の流れ	. 2
3		ご利	リ用にあたっての準備	. 3
4		Worl	kspace ONE UEM 管理コンソールヘログインする	. 5
	4.	1.	初回ログイン	. 5
	4.	2.	2 回目以降のログイン	. 8
5		API	Ns の登録-iOS	. 9
	5.	1.	証明書要求をダウンロードする	. 9
	5.	2.	APCP で証明書を作成する	11
	5.	3.	Workspace ONE UEM 管理コンソールで証明書を登録する	14
6		ディ	イスの所有形態	17
	6.	1.	既定のデバイス所有形態を設定する	17
7		그-	-ザー登録	19
	7.	1.	ユーザーを追加	19
8		Woi	rkspace ONE SDK プロファイルの設定-iOS	21
	8.	1.	Workspace ONE Intelligent Hub	22
	8.	2.	Workspace ONE Web	23
	8.	3.	Workspace ONE Content	24
9		ディ	バイスで加入処理を実行	26
	9.	1.	サーバ詳細情報の入力から加入を行う	27
	9.	2.	QR コード付きのメール送信から加入を行う	33
		9. 2.	.1. デバイスの追加を E メールで通知する	33
		9. 2.	.2. QR コードを読み取り加入をする	35
1	0	7	デバイスの状態確認とリモート操作	37
	10).1.	ダッシュボード - デバイスの加入状況を確認する	37
	10).2.	デバイスリスト - デバイスの情報を確認する	38
	10).3.	デバイスをリモート操作する	39
		10. 3	3.1. デバイスをロック	40
		10. 3	3.2. 企業情報ワイプ	42
		10. 3	3.3. デバイスワイプ	43
1	1	シ	ィステム構成	44
	11	.1.	デバイスワイプの設定	44
	11	.2.	制限された操作の設定	45
1	2	尚	を社サポート	47

目 次

| 本書について

Workspace ONE UEM の SaaS を初めて操作される方を対象に、下記手順について説明しています。

- ・Workspace ONE UEM へのログイン
- ・ユーザー登録
- ・デバイスの状態確認とリモート操作

上記に無い SaaSの操作手順については、次の2つのガイドをご参照ください。

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

Workspace ONE UEM 管理コンソールガイド(機能編)

- ・機能別ガイドの概略
- ・システム設定
- ・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

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 本書での操作の流れ

本書は下記図のように操作の流れを説明しております。



APCP : Apple Push Certificates Portal (Apple 社のサイト) APNs : Apple Push Notification Service (iOS デバイスへ情報を送るサービス)

ご利用にあたっての準備 3

Workspace ONE UEM の利用開始にあたって、以下を準備してください。

✓ Apple ID

・既存アカウントの流用は避け、Workspace ONE UEM 専用の Apple ID をご用意ください。 既に他の MDM などで iOS デバイスの管理を行っている場合は、同じ Apple ID を利用して 利用を開始することができます。同じ Apple ID を利用する場合は、複数の APNs 証明書の 取得が可能となる為、APNs 証明書更新時に注意が必要です。

・iOS 以外のデバイス使用時は、必要ありません。

✓ VMware Workspace ONE SaaS 確認書

・Workspace ONE UEM 管理コンソールの初回ログイン時やデバイスを Workspace ONE UEM (AirWatch)に加入させる時に必要な情報が記載されています。

- ✓ Workspace ONE UEM 管理者アカウント アクティベーション メール
 - ・お申込みいただいた管理者様 E メールアドレスに件名「Workspace ONE UEM 管理者アカウ ント アクティベーション」のメールが届きます。管理者アカウントパスワード変更のリン ク URL が記載されています。
- ✓ Workspace ONE UEM 管理コンソール用 PC
 - ・以下の Web ブラウザ (いずれか)を利用して Workspace ONE UEM 管理コンソールを操作し ます。

Chrome Firefox Microsoft Edge Safari(Mac版)

- ・最新バージョンの 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。 特に IE は後述「5 APNs の登録」で問題となる為、使用しないでください。

✓ 管理対象デバイス

- ・Workspace ONE UEM で管理予定のモバイルデバイスです。
- ・旧デバイスの場合、デバイスでご利用予定のWorkspace ONE プロダクト(アプリケーショ ン)より、以下の対応表で使用可否をご確認ください。

iOS & iPadOS	2022 年 1 月 21 日現在
Workspace ONE(AirWatch)プロダクト	サポートiOS Version
MDM 機能サポート	iOS 13.0+
VMware Workspace ONE Intelligent Hub	iOS 13.0+
VMware Workspace ONE Boxer	iOS 13.0+
VMware Workspace ONE Web	iOS 13.0+
VMware Workspace ONE Content	iOS 12.2+**
VMware Workspace ONE Tunnel	iOS 12.2+*

- ※ iOSバージョンがリリースされると、3世代前iOSバージョンのサポートは終了します。例、iOS 16 がリリースされると、VMware Workspace ONE アプリケーションの 次のリリースバージョンではiOS 13のサポートが廃止される予定です。
- ※利用可能なバージョンのアプリは以前のiOSバージョンのデバイス上でこれまでど おり機能しますが、より新しいバージョンで導入された機能やバグ修正はご利用い ただけません。

Android	2022 年 1 月 21 日現在
Workspace ONE(AirWatch)プロダクト	サポート Android Version
VMware Workspace ONE Intelligent Hub	Android 5.0+
VMware Workspace ONE Boxer	Android 9.0+
VMware Workspace ONE Web	Android 8.0+
VMware Workspace ONE Content	Android 8.0+
VMware Workspace ONE Tunnel	Android 8.0+

- ※ Androidバージョンがリリースされると、4世代前iOSバージョンのサポートは終了 します。例、Android 13 がリリースされると、VMware Workspace ONE アプリケー ションの次のリリースバージョンではAndroid 9のサポートが廃止される予定で す。
- ※新しいOSバージョンでのみ使用可能なAPIに依存する可能性があるため、古いOSバ ージョンではすべての製品機能が使用できるわけではありません。さらに、一部の 製品機能はサードパーティのライブラリに依存します。

4 Workspace ONE UEM 管理コンソールヘログインする

PC で Web ブラウザを起動し、Workspace ONE UEM 管理コントールにログインします。

4.1. 初回ログイン

1) Workspace ONE UEM 管理者アカウント アクティベーション メールに記載されているパスワ ードのリセットリンクをクリックします。

vm ware [.]		
	Workapace Of ECEN 管理者がカウント アクティペーション - 2019/110	
Support W	case.	
Wortspace 聖禮書⇒>	OLE UEM 管理者アカウントが存成され、次の直接資源を使用して Workstake One UEM ゾールにログインできるようになり呈した	
Winay 7 - H J129 Read	***** OF#FUEW 智理書コンジール http: - を - ドのリセット リンク / **** - とにまっけで5550/URD	
1009	- ドカリセット リンクの東部局部, 11:32018 11:18:29 AM	
次の管理者	複製へのアクセスが排引されました	
	and the second se	
実験がある	場合は、在内のボヘルプデスクに影聴い合わせください。batedriftsumeary.com	
戦月 Workspace	CARE OEM	
.0	yylgh 8 31/9 Wham, Hc. Al-Ights Inne-Hot.: 1118 Pannana Cenar Weat, Suite 103 Aberts, G# 2008	

重要

パスワードのリセット リンクの有効期限は48時間(2日間)です。有効期限が過ぎた場合は、弊社サポートまでお問い合せください。

2) Workspace ONE UEM 管理コントールのパスワード変更の画面が表示されます。新しいパスワー ドを入力し、送信をクリックします。

Works	pace ONE*	UEM
#UUU00-1		
/1217-KORD	33	
<u>0</u>		

3) Workspace ONE UEM 管理コントールのログイン画面が表示されます。画面のユーザー名とパス ワードに対し、VMware Workspace ONE SaaS 確認書に記載のアカウントと設定したパスワー ドを入力し、ログインをクリックします。

Workspace ONE ⁺ UEM	Workspace ONE" UEM
3-5-8	ವ− ೮− 8
0.28	0.28
	1
	0242
WA DAVERDURD	語のユーザーとしてロタイン
ログインできない場合	132:43-72:4332000月

4) VMware Cloud Service 製品のサービス利用規約 (TOS) が表示されます。[承諾] をクリッ クします。

vm ware	<u>-</u> 2°			
	VMware Clo	ud Service Offe	arings	-
	TERM	S OF SERVICE		
Last updated: 13 Septem	ber 2019			
By using a Service Offe ('Terms of Service'), "Agreement". If you do must not use the Servic applicable, your Users) the authority to bind that the billing address for y company organized ann the United States. Capi of Service and in Section these Terms of Service	ring, you agree to be by and by the Service not agree to these Term ce Offering. "You" mean If you are entering into at entity. "VMware", "we our Order is in the Unite d existing under the laws talized terms used in thio on 14 ("Definitions"). Se	ound by these tern Offering Docume ns of Service or to s you individually the Agreement fo ", or "us" means " ad States, or VMw s of Ireland, if the ese Terms of Serviction references i	ms of service betwee entation, which toge any other portion o or the entity that yo or an entity, you repu- VMware, Inc., a Del- vare International Ur billing address for y- vice are defined thro n this document are	en you and VMware ther constitute the the Agreement you u represent (and, as esent that you have aware corporation, if thimited Company, a our Order is outside ughout these Terms to the provisions of

5) **セキュリティ設定**の画面が表示されます。下記の必須項目①~③を設定し、[保存] をクリッ クします。項目名の後に*****がついているものは入力必須項目です。

重要

他の管理者アカウントからパスワードの変更が行えません。パスワード回復の質問と 回答がわからなくなると、管理コンソールにログインが行えなくなりますので、ご注 意ください。

セキュリティ設定
 ・ ・ はけるにはプロファイルを完了してください パスワード回復用の質問を1つ設定する必要があります ・ ・ ・
パスワード
パスワード リセット
パスワード回復用の質問1
バスワード回復用の質 あなたの子供時代のあだ名は何でしたか? 🗸
バスワード回復用の回 答* 2 2
バスワード回復用の回答 を再入力*
セキュリティ暗証番号 ――――――――――――――――――――――――――――――――――――
4 桁のセキュリティ PIN を入力する必要があります。これは、一部の制限されているアクションのコンソールで必要 です (承認された管理者がシステム セキュリティ設定で構成)。
セキュリティ暗証番号* 恵示 3
セキュリティ 暗証番号を 再確認★

必須項目		設定
	パスワード回復用の質問	パスワード回復時に求められる質問を選択しま す。
2	パスワード回復用の回答	上記①で選択した質問に対する回答を設定しま す。
3	セキュリティ暗証番号	デバイスをWorkspace ONE UEM へ加入する前の状態へ戻す"企業情報ワイプ"等の操作で入力を求められる4ケタの数字を設定します。



6) ログインが完了すると、Workspace ONE UEM 管理コンソール画面が表示されます。

4.2. 2回目以降のログイン

2回目以降は、上記「4.1 初回ログイン」の 3)のログイン画面になります。管理者アカウントと パスワードを入力すると、Workspace ONE UEM 管理コンソール画面が表示されます。

5 APNs の登録-iOS

iOS デバイスを管理するためには、APNs への事前登録が必要となります。 次の手順で証明書を作成し登録します。

- Workspace ONE UEM 管理コンソールから証明書要求をダウンロードする。
 → 5.1. 証明書要求をダウンロードする
- ② APCP で証明書を作成する。
 - → 5.2. APCP で証明書を作成する
- ③ 作成した証明書を Workspace ONE UEM 管理コンソールで登録する。
 - → 5.3. Workspace ONE UEM 管理コンソールで証明書を登録する

参考

iOS デバイスを利用しない場合、以降の操作(APNsの登録)は不要です。 次章の**ユーザー登録**へ進んでください。

5.1. 証明書要求をダウンロードする

1) [デバイス] > [デバイス設定] > [デバイスとユーザー] > [Apple] > [MDMの APNs]をクリックしま す。

> システム	デバイスとユーザー
 ▼ デバイスとユーザー > 全般 	Apple 🖉
> Android	MDM の APNs
~ Apple	Apple iOS
MDM の APNs	Apple macOS
Apple iOS	AppleCare
> Apple macOS	自動加入

2) [新しい証明書を作成] をクリックします。

• * ***	₩/JJJ2EIL-tf-) Apple
- デバイスとユーザー ・ 全般	MDM Ø APNs
Android Apple MDM d0 APNs Apple (05)	Apple デバイスを管理するためには、Apple のブッシュ通知サービス (APNs) 証明書が必要です。 新しい証明書の作成には 「新しい証明書を主成」 をグリックしてください。
・Apple macOS AppleCare 自動加入 デバイス加入プログラム	APNs 証明書がすでにある場合は、下の「版存の証明書をアップロード」ボタンを使用するとアップロードできます。 置しい証明者を1点

[MDM 用の APNs] をクリック後に、次の画面が表示される場合があります。この場合は、 [消去] をクリックし、[セキュリティ暗証番号] を入力すると、上記と同じ画面が表示されま す。

NDM 03 APNS 🗇		
Minnez	○ 総務 ● オーバーライド	
紅明樹 -	12回線アップロード	
947	Pri	
発行 列	C+U/L, C1+A459:37819425;<8534360;8177/81183;27508; OID D 9:23421920100 1011.1+com.apple.mgmt8:Februal.5781942c<863-4960;8177/81193c21008	
RITE	C+LIS, C+Apple Inc., CO+Apple Certification Authority, CH+Apple Application Integration 2. Certification Authority	
制改和国政地区	2019/10/04	
ROABH75	2020/10/54	
サムプリント	344559/7053468830X592FFFF3484224473525F76	
AppletD	กมากลังเตาวิชีชิฐกาลใ.((m	
HTTN2 上のデスト (新聞	MILOFRE O	
サフタループの構築・	③ 880.0 ⊕ π-/1-511000 € 88825121-/1-511	
		-

3) [MDM_APNsRequest.plist] をクリックして、AirWatch 証明書要求 をダウンロードしま



ご利用のブラウザのファイルダウンロードの操作で、MDM_APNsRequest.plist を(任意のフ ォルダへ)保存します。

5.2. APCP で証明書を作成する

1) [Apple のサイトを開く] をクリックすると、Apple サインインの画面が表示されます。



重要 APCP を表示する際、Internet Explorer は使用しないでください!問題が生じること があります。 APCP を表示する際、管理コンソールの画面は閉じないでください。管理コンソールの 画面を閉じた場合は、APNs の登録に失敗するケースがあります。

2) Apple ID の資格情報(パスワード,二要素認証)を利用して [サインイン] を行います。

Apple IDを使ってサインイン	
	2ファクタ認証
//27−F ④	
Apple IDをプラウザに保存	確認コードを含むテキストメッセージをご利用のデバイスに送信し』 した。続けるにはコードを入力してください。
Apple IDまたはパスワードをあ忘れですか? Apple IDをお持ちでないですか? 作道はこちら >	確認コードを受信していませんか?

参考

上記画面が表示されない場合(エラー、その他のメッセージが表示される)は、時間をおいて再度お試しください。エラーが続く場合、下記いずれかへご連絡ください。

・弊社サポート

・Apple 社サポート

3) ログイン後、[Create a Certificate] をクリックします。



4) 内容を確認の上、同意の**チェック**をして[Accept] をクリックします。

Terms of Use	
PLEASE READ THE FOLLOWING LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE CERTIFICATES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOUR COMPANY/ORGANIZATION AND APPLE.	
IDM Certificate Agreement	
tor companies deproying moune device management for IOS and/or OS A products)	
our company, organization or educational institution would like to use the MDM Certificates (as defined ielow) to enable You to either deploy a third-party commercial, enterprise server software product for mo levice management of IOS and/or OS X products, or deploy Your own internal mobile device manageme OS and/or OSX products within Your company, organization or educational institution. Apple is willing to you a limited license to use the MDM Certificates as permitted herein on the terms and conditions set for ins Agreement.	bile nt for grant th in
. Accepting this Agreement; Definitions	
.1 Acceptance n order to use the MDM Certificates and related services. You must first agree to this License Agreement (or do not or cannot agree to this License Agreement, You are not permitted to use the MDM Certificates elated services. Do not download or use the MDM Certificates or any related services in that case.	t. If or
I have read and agree to these terms and conditions.	
Printable Version >	
Decline	

5) [参照...] をクリックして、「5.1. 証明書要求をダウンロードする」のステップ3で保存した 証明書要求のファイル (MDM_APNsRequest.plist)を選択します。

pload your Certificate Sign	ning Request signed by your third-party server
endor to create a new pus	h certificate.
lates	
Smoot	
※1byte 文	字でメモが入力できます
endor-Signed Certificate 5	iigning Requirat
※1byte 文	字でメモが入力できます
endor-Signed Certificate 5	ligning Request
ファイルを選択	れていません
※1byte 文	字でメモが入力できます
endor-Signed Certificate S	ligning Request
ファイルを運行	れていません

6) [Upload] をクリックして、証明書要求のファイルをアップロードします。

Create a New Push Certificate
Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.
Notes
Support
Vendor-Signed Certificate Signing Request
参照 MDM_APNsRequest.plist
Cancel Upload

7) 要求が承認されると、確認画面が表示され[Download] をクリックします。

Confirmation 🥑	
You have successfully created a n	ew push certificate with the following information:
Service	Mobile Device Management
Vendor	AirWatch
Expiration Date	Apr 10, 2019
Manage Certi	ficates Download

ご利用のブラウザのファイルダウンロードの操作で、MDM_AirWatch_Certificate.pem を(任 意のフォルダへ)保存します。

Workspace ONE UEM 管理コンソールへ戻ります。

参考

クリック後にエラーで保存ができなかった場合

Apple のサイトに行く際、Workspace ONE UEM の管理コンソールを閉じてしまった場合 は、

再度「5.1.証明書要求をダウンロードする」からやり直してください。

5.3. Workspace ONE UEM 管理コンソールで証明書を登録する

1) Workspace ONE UEM 管理コンソールに戻り、[次へ] をクリックします。

デバイスとユーザー > Apple	
MDM の APNs ⑦	
ステップ1 ステップ2 署名を要求 要求を完了	
Apple の証明書ボータルで APNs 証明書を作成し、ここに戻ってアップロードします。この証明書を作成するには、以下(1. AirWatch 証明書要求 (MDM_APNsRequest.plist) 2. 企業の Apple ID。AirWatch は、モバイル デバイス管理専用の Apple ID を作成することを推奨します。Apple ID を作 APPLE のサイトを開く	Dアイテムが必要です。(説明) 成してください。(ここをクリック)
次へ キャンセル	

2) **[アップロード]** をクリックして「5.2. APCP で証明書を作成する」でダウンロード(保存)した MDM_AirWatch_Certificate.pem をアップロードします。

デバイスとユーザー 🕻 Apple	
MDM の APNs ②	
ステップ 1 ステップ 2 署名を要求 要求を完了	
Apple からの応答をアップロー	ドしてください。ファイル名は 「MDM_AirWatch_Certificate.pem」 としてください。
Apple社発行のAirWatchMDM証明 書(.pem)	<i>アップロード</i>
AppleID *	
	戻る 保存 キャンセル

[参照] をクリックしてファイルを指定し、[保存] をクリックします。

追加	×	追加	×
ファイルを選択 提択…ません	6.	「ファイルを選択」MOM perm	
a	存 キャンセル	&#</td><td>i>teak</td></tr></tbody></table>	

3) APCP で指定した Apple ID を入力して、[保存] をクリックします。

デバイスとユーザー 〉 Apple	
MDM の APNs ②	
ステップ 1 ステップ 2 署名を要求 要求を完了	
Apple からの応答をアップロー	ドしてください。ファイル名は「MDM_AirWatch_Certificate.pem」 としてください。
Apple社発行のAirWatchMDM証明 書(.pem)	MDM_AirWatch_Certificate.pem アップロード
AppleID *	tae ≡_■B@gmail.com
	戻る 保存 キャンセル

- 4) 4桁の[**セキュリティ暗証番号]** を入力します。
 - セキュリティ暗証番号とは、「4.1 初回ログイン」5)で設定した4桁の数字です。

制限された操作	- APNs 証明書の変更	×
APNs 証明書の変更 ティ暗証番号を入	Đ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 カして統行してください。	.U
AirWatch は APNs 証明書 書に対する変更を続行す なくなります。	を使用することにより、Apple デバイスと遠信できます。この組織グループでアップロードされた現在の) ると、証明書内に異なるトピック値がある場合、AirWatch は、現在加入しているすべてのデバイスと通信	正明 でき
この操作を元に戻すこと	はできません。また、AirWatch がごれらのデバイスを再度管理するには、再加入させる必要があります。	
証明書アップロード		
タイプ	Cert	
有効期限開始日	2018/06 04	
有効期限終了日	2019/###~	
サムプリント	0ED5	
	セキュリティ暗証 番号:	
	セキュリティ暗証番号をお忘れですか?	
	49 4	セル

5) 正常に保存が行われると以下の画面表示になりますので、[サブグループの権限] が [継承または オーバーライド] になっていることを確認します。

◎ 正常に保存されま	した
現在の設定	○ 起素 ● オーバーライド
王明鼎 *	証明書アップロード
タイプ	Pfx
発行先	C+US, CN+APSP OID.0.9.2342.19200300.100.1.1+com.apple.mgmt.External
発行者	C-US, O-Apple Inc., OU-Apple Certification Authority, CN-Apple Application Integration 2 Certification Authority
有効期限開始日	2020/12/24
有効期感終了日	2021/12/24
サムプリント	
ppleiD	rise salada ti diterga dana san
1779/2 上のテスト盛続	「推験のデスト」

重要

証明書をアップロードして保存後、サブグループの許可がオーバーライドのみにチェ ックされている場合があります。この場合、下位の組織グループは APNs が継承されま せん。

下位の組織グループに所属する iOS デバイスがある場合は、必ず継承またはオーバー ライドで保存してください。

6 デバイスの所有形態

Workspace ONE UEM では、デバイスの所有形態を指定することにより、構成プロファイルの配 布やアプリケーションの展開を柔軟に行う事ができます。また、デバイスの情報収集やデバイス に対するコマンド実行の可否を設定するプライバシー設定と密接に関係しています。デバイス加 入時にデバイスの所有形態を指定しない場合は、[未定義]のデバイスとして加入することとな り、プライバシー設定によっては意図しない動作になる場合があります。この為、デバイス加入 時にデバイスの所有形態が自動的に[企業 - 専用]などになる設定を予め行う事を推奨しておりま す。

プライバシー設定については「11.1 デバイスワイプの設定」をご参照ください。

6.1. 既定のデバイス所有形態を設定する

1) [**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]** をクリックしま す。



2) [グループ化]タブをクリックし、[現在の設定]を [オーバーライド]に変更します。

□入 ◎					
認証 管理モー	下 利用規約	グループ化	制限	オプションのメッセージ	カスタマイ
現在の設定	○ 縦条 💽 オーバ・	-945			
グループ 10 割り当てモード	● 既定 〇 ユーザ	ーがグループ 叩 を避け	やするようプロ:	レプト表示する	
The state of the second					
() ユーサー クルーフに基づき日	動選択				
() ユーサー クループに基づき日 既定	動運行				
↓ ユーワークルーフに基づき目 既定 既定のデバイス所有形態*	1動選5で 【なし		ೆರ		
 ユーワークルーフに基づき目 既定 既定のデバイス所有形態* 既定の役割* 	動量的 なし フル アクセス		÷		

- 3) [既定のデバイス所有形態]の欄をクリック(プルダウン)してデバイスの所有形態を選択しま す。
 - [企業 専用]: 会社支給の個人利用のデバイス[企業 共有]: 会社支給の共用のデバイス[従業員所有]: 従業員が所有するデバイス (BYOD)

画面下 [保存] をクリックして設定を保存します。

裁定	
国産のデバイス所有形態。	au -
私主の時期 *	なし 企業・専用 企業・共有
非アクティブユーザーに対す る設定アクション *	这族員所有 (ACCOUNT
ユーザー グループ 同期	
Workspace ONE におしてユ ーザー グループをリアルタイ 広岡崎	1330 (1)
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助化	
サブグループの権限*	○ 暗手のみ ○ オーバーライドのみ ● 様手またはオーバーライド
	4 #

7 ユーザー登録

デバイスを管理するために、**デバイスの使用者であるユーザー**をデバイスより先に登録する必要が あります。

7	1	┐―ザ―を追加	
1.		エフで追加	

1) [**アカウント**] > [リスト表示]をクリックします。

₩ €=⊅	ユーザー リスト表示	~	^{アカウント} > ユーザー リスト表示				â ★
 デバイス	役割 加入状態	→	フィルタ >> 「追加 💙		レイアウト 🗸		食索
	バッチの状態		────────────────────────────────────	加入組織グループ	ユーザー グループ	デバイス	状態
答 アカウント	ユーザー設定 ユーザー グループ	>					
!!!! アプリとブック	管理者	>		レコードが見つかりき	ませんでした		

2) 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、[ユーザーを追加] をクリックしま す。

アカウント > ユー!	ザー	
リスト表示		
フィルタ »	追加 🖌	
一般情報	ユーザーを追加	加入組織グループ
	バッチ インポート	

ユーザーを追加/編集の画面が表示されます。

必須項目を入力して[保存]をクリックします。
 項目名の後に「*」がついているものは必須項目です。

ーザーを追加/編	集			
全般 高度な設定				
セキュリティ タイプ*	ペーシック ディレ	クトリ		
ユーザー名 *				
パスワード*		表	Ē	
パスワードの再入力*		表;	Ā	
氏名*	名	ミドルネーム	姓	
表示名				
Eメールアドレス*				
Eメール アドレス* Eメールのユーザー名 ドメイン				
Eメール アドレス [★] Eメールのユーザー名 ドメイン 電話番号	 電話即号			
Eメール アドレス * Eメールのユーザー名 ドメイン 電話番号	 电話許号 质带電話			
Eメール アドレス* Eメールのユーザー名 ドメイン 電話番号	 尾話曲号 現州電話			
Eメール アドレス * Eメールのユーザー名 ドメイン 電話番号 > 加入	 电武器号 质带電話			
Eメール アドレス* Eメールのユーザー名 ドメイン 電話番号 > 加入	 電話曲号 			
Eメール アドレス* Eメールのユーザー名 ドメイン 電話番号 > 加入				
Eメール アドレス* Eメールのユーザー名 ドメイン 電話番号 > 加入				

[加入]、[通知]をクリックすると各設定内容が展開されますので、必要であれば設定を変更します。

1入組織グループ*	support	Q	
1加の組織グループにユー 「ーが加入することを許可	有効 無効		
1-ザー役割*	フル アクセス		
Lーザー役割* 通知	フル アクセス なし Eメール		

4) リスト表示でユーザが追加されている事を確認します。

アカウント > ユーザー リスト表示					# *
フィルタ » <u>追加</u> 一般情報	連絡先情報	加入組織グループ	レイアウト マ C E ユーザー グループ	リストを検索 デバイス	状態
User01 01 User		support	0	0	 ● 有効

20 Copyright(C) 2022 WiZaaS Co., Ltd. Rights Reserved.

8 Workspace ONE SDK プロファイルの設定-iOS

以下の Workspace ONE アプリケーションを iOS デバイスで使用する場合、Workspace ONE SDK プロファイル (アプリケーションプロファイル) の設定が必要になります。

Workspace ONE Intelligent Hub

Workspace ONE UEM のデバイス管理機能、Hub サービス機能、および、デバイス加入アシストに対応するアプリケーション

Workspace ONE Web

Workspace ONE UEM の管理・セキュリティ機能に対応するブラウザ

Workspace ONE Content

Workspace ONE UEM のコンテンツ管理機能に対応するコンテンツ参照アプリケーション iOS デバイスを使用する場合、以下の画面で設定するセキュリティポリシーは、以下の項の記載の Workspace ONE SDK プロファイルの設定を行う事で、これらアプリケーションに適用されるように なります。

[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]

> >2227	アプリ > 国産とポリシー	
・ デバイスとユーザー	セキュリティボリシー ③	
・アプリ ・アプリスキャン Workspace ONE Web	現在の設定 〇 柱末 ● オーバーフィド	
Workspace ONE Container	77UEEEE9283 NR III	
 設定とポリシー セキュリティポリシー 	EEE947* 2-9-82/129-8 . ()	
設定 50% アブリ コンブライアンス	94679) 4 (MM +)	
プロファイル	10万共助国新加上版* 4 · ①	
microsoft inturies 77 (1988)	パイオメトリックモード 和治 島助 〇	
EX-M	5>7/L#4345 88 0	
テレコム	1987 1997 1997 1997 1997 1997 1997 1997	
	#754>P9tta #8 55	
	· 供酒材常 · · · · · · · · · · · · · · · · · · ·	
	AirWatch App Tunnel NS Es 🗇	
	コンテンツ フィルタリング 🔒 🗂 🕕	
	547=>3 ## ## ①	
	F-9W8002 ##	
	ネットフークアクセスコ 4% Bn () ントロール	
	サブダループの構築・ 〇 絵木のみ 〇 ホーバーライドのみ 🌘 絵楽書だはオーバーライド	
		42.17r

セキュリティポリシーは、上記アプリ利用時に利用者に求める認証の方法や各アプリの機能制約 を集めた設定です。

8.1. Workspace ONE Intelligent Hub

 [デバイス] > [デバイス設定] をクリックし、表示された設定画面右側に表示される [デバイスとユ -ザ-] > [Apple] > [Apple iOS] > [Intelligent Hub 設定] をクリックします。

🖄 Works	pace ONE UEM		設定	WS01811
₩ €=9	ダッシュホード		> システム → デバイスとユーザー	デバイスとユーザー > Apple
 デバイス	ライフサイクル プロファイルとリソース	>	> 全般 > Android ~ Apple	Apple IOS ⑦ アプリケーションの APNs Intelligent Hub 設定
答 アカウント	順守ホリシー 証明書 プロビジョニング	> > >	MDM の APNs Y Apple IOS アプリケーションの APNs	管理設定
詳 アプリとブック	デバイス設定		Intelligent Hub 股定 管理設定	

[SDK プロファイル] が iOS Default Settings@Global で設定されている事を確認します。
 設定されてない場合、[現在の設定] を[オーバーライド] に変更して、[SDK プロファイル] を iOS Default Settings@Global にし、[保存] をクリックします。

全般	810		
現在の設定	088 * //-54F		
282			
intelligent Hub の加入解除 オプションを解効化			
バックグラウンド アプリの 更新			1057
エリア			
位置调枪データを収集			
iBeacon エリアを検出する	00		
テレコム			
ゼルラー データ使用量増減 を収集	23		
セルフサービス設定			
セルフサービス有効化	0		
SDKプロファイル			
SDKプロファイルiレガシ ー!	an.	*	
SDKプロファイル	IOS Default Settings @ Global	×	

8.2. Workspace ONE Web

 [グループと設定] > [すべての設定] をクリックし、表示された設定画面右側に表示される [アプ リ] > [Workspace ONE Web] をクリックします。



[Workspace ONE Webの設定] をクリックし、[アプリのプロファイル] が[既定] である事を確認します。

この設定でない場合、[現在の設定]を[オーバーライド]に変更後、[アプリのプロファイル]を[既定] に変更し、[保存]をクリックします。

The second second second	設定 ブックマーク	通知	
現在の設定	○報理 ●オーバーライド		
設定とポリシー			
アイル	17 JA94	U.	
() Workspace ONE Web	は以下の画面で定義されるデファ	ルトのアプリケーション設定と	ポリジーを使用します
ヤキュリティポリシー	と設定		
ゼキュリティポリシー	-と設定		
セキュリティポリシー	-CRE		
ゼキュリティポリシー	- と改正 		
ゼキュリティポリシー	-2192		
セキュリティポリシー	-287		
ゼキュリティポリシー 利用規約 心要とする利用規約	282 80		

3) [通知] をクリックし、[アプリケーション名] が VMware Browser@Global である事を確認しま す。

この設定でない場合、[現在の設定] を[オーバーライド] に変更後、[アプリケーション名]を VMware Browser@Global に変更し、[保存] をクリックします。_____

現在改設定	○総承 ●オーバーライド
通知 ()05 のみ)	
アプリケーションタイプ*	• ○ステム 日内
アプリケーション名*	VMware Browsen@Global =
/(>F/piD*	com alt-match salcure browthat

8.3. Workspace ONE Content

 [グループと設定] > [すべての設定] をクリックし、表示された設定画面右側に表示される [コン テンツ] > [アプリケーション] > [Workspace ONE Content アプリ]をクリックします。

設定	An and a second	
 > システム > デバイスとユーザー > アプリ * コンテンツ * アプリ Workspace ONE Content アプ 	コンテンツ アプリ ① Workspace ONE Content アプリ	

2) 以下の設定である事を確認します。

[設定とポリシー] - [アプリのプロファイル]: [既定] [通知] - [アプリケーション名]: VMware

VMware Content Locker@Global

上記設定でない場合、[現在の設定]を[オーバーライド]に変更後、上記設定に変更し、[保存] をクリックします。

現在の設定	○ 超素 ● オーバーライド	
8定とポリシー		
アプリターションプロファイ ル	ES 73.94	
Content (#ULFO) ALC 2	■ 数字れる設定設定のアプリケーション設定とポリシーを使用します ●	

アプリケーションタイプ・	システム 社内			
アプリケーション名・	VMware Content Locker@Global ~]		
バンドル10*	com an watch content locker	l.		
バッジカウント・	アップデートのみ (ダウンロードされたコンテンツ用)	86	SL	
er e				
ブクループの権限	〇 地承のみ 〇 オーバーライドのみ	-9415		

9 デバイスで加入処理を実行

デバイスから Workspace ONE UEM への加入処理を行い、このデバイスを Workspace ONE UEM で管理 できるようにします。

- 1) 加入処理は、Workspace ONE Intelligent Hub アプリを利用し、以下からインストールしま す。
 - iOS: App Store
 - Android: Google play
- Workspace ONE Intelligent Hub を起動します。
 本書では、iOS の加入処理方法を説明させていただきます。
 未加入時は、以下のように「メールアドレス」または「サーバアドレス」を入力する欄と、
 「QR コード」が表示されます。
 加入時認証方法によって、以下のように入力します。

E メールアドレス…[メール アドレスまたはサーバ]欄に入力 サーバアドレス…[メール アドレスまたはサーバ]欄に入力

QR コード…「QR コード」をタップしQR コードを読込

٥
メール アドレスまたはサーバ
闘 QR ユード
**

3) 各認証方法による操作は、以下で説明します。

サーバ詳細

7.1 サーバ詳細情報の入力から加入を行う OR コード

7.2. QR コード付きのメール送信から加入を行う

また、上記の操作は iOS デバイスの例で説明します。

Eメールアドレスについては、別紙「メールアドレスを利用したデバイス登録方法について」を ご参照ください。

9.1. サーバ詳細情報の入力から加入を行う

認証に必要な情報を全て手入力で行い、加入を行う方法です。

1) [メール アドレスまたはサーバ] に VMware Workspace ONE SaaS 確認書に記載のデバイスサービス URL を入力して、[次へ]をタップします。

	QR I	⊐ <i>−</i> ド		
	 次^		 	

2) [グループ ID] にグループ ID を入力して、[次へ]をタップします。



参考

グループ ID は組織グループを識別する為の ID です。Workspace ONE UEM 管理コンソール画面右 上の組織グループ表示にマウスポインタを重ねるとグループ ID を確認する事が出来ます。



3) 6. ユーザー登録で設定したユーザー名とパスワードを入力して、[次へ]をタップします。

<										
wso1811-user										
L				次へ		-		Į.		
۹ v	V	e		t J	<u> </u>		i c	р		
а	s	d	f	g	h	j	k	1		
Ŷ	z	x	С	V	b	n	m	$\langle \times$		
123	3		:	space	;		(Go		

4) 加入後の機能説明が表示されます [次へ]をタップします。タップすると Safari に遷移します。

0	収集しない	収集できる
9	メッセージ テキストメッセージを	プライベートのままにします。
◙	個人 E メール 所有のアカウントはす^	(てプライベートです。
	個人の写真 写真を簡約したり、写訳	(にアクセスしたりはしません。
	個人の写真 写真を感納したり、写算	(にアクセスしたりはしません。

5) 構成プロファイルダウンロード許可のポップアップに対して[許可] をタップします。構成プロファイルダウンロード後、[閉じる] をタップします。



6) 手動で iOS デバイスの[設定]を開きます。[プロファイルがダウンロードされました]をタップすると、 ダウンロードした構成プロファイルが表示されます。[インストール] をタップします。



7) デバイスにパスコードが設定されている場合、インストール実行前にパスコード入力を求め られます。[インストール] をタップします。

15:09		.ul 🗢 💼		17:29	.al 🗢 💼
	パスコードを入力				プロファイルのインストール
					加入 Workspace
					E Nawmani.com NEERA ✓
	バスコードを入力		>		・デバイス上の仕事用アプリケーションおよびワービス を管理およびアクティブ化する際に使用する、デバイ
	0000				ス世紀プロファイルです。 1 デバイス教師チャレンジ
				1730	
					インストール
					キャンセル

8) モバイルデバイス管理になる警告表示に対し[**インストール**] をタップし、続けて表示されるポ ップアップに対し[信頼] をタップします。



9) プロファイルのイントール完了の画面の[完了] をタップし、続けて表示される画面のポップ アップに対し、[開く] をタップします。



10) 手動で Workspace ONE Intelligent Hub アプリを開きます。加入完了の画面が表示されます ので、[完了] をタップします。



11) プライバシーの同意画面で[理解しました]を選択し、次のデータ共有の同意画面で [同意します] または[今はしない]を選択します。



データ共有の同意は任意です。どちらを選択しても問題ありません。

【認証設定あり】 Workspace ONE Intelligent Hub アプリの利用に対する認証画面が表示され、 認証に必要な情報を正しく入力すると、プライバシーの同意画面が表示されます。

		<				1.3							プライバシー
く パスコードを作成				<i>.</i> ,	パスコ	-1	۲¢	再入	カ				
パスコード			パス										当社では、ユーザーの皆様のプライバシーを重
パスコードのガイドライン	····>			2	(スコ	- F0	のガイ	ドライ	×			>	視しています。 VMware Workspee ONE は、作業データあよびアプリケー ションへの空会なアクセスを選択するために情報を収集しま す。最適点パフォーマンス、セキュリティ、およびサポートを 提供するために Workspace ONE および Hub によって収集さ れるデータの振発は以下をご確認ください、Workspace ONE によって収集された情報をお客様の企業的どのように扱うかに ついては、お客様の企業の知道者にお問い合わせください。
		1	2	3	4	5	6	7	8	9	0		デパイスの加入を解除してこのアプリへのアクセスを中止する 方法については、企業の IT 管理者にお問い合わせください。
		-	1	:	;	()	¥	&	@	"		データ収集寺 けいり
次へ		#+=			,		?	1	,		\otimes		・ 、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、
		1	ABC			sp	ace			Ne	xt		理解しました

上記左画面は、セキュリティポリシーの設定にある[認証タイプ] が[パスコード] の場合の例で す。[認証タイプ] が[無効] の場合は、表示されません。

9.2. QRコード付きのメール送信から加入を行う

Workspace ONE Intelligent Hub の加入処理で最初に行うサーバ詳細情報の入力をQR コードで行う方法です。

これ以降の手順は7.1 サーバ詳細情報の入力から加入を行うと同じです。

QR コードは、管理コントールから送信される以下の「Workspace ONE UEM デバイスアクティブ 化」のメール本文に貼りつけられています。



9.2.1. デバイスの追加を E メールで通知する

管理コンソールの操作で、デバイス利用者にメール「Workspace ONE UEM デバイスアクティブ

化」を送信します。

1) [アカウント] > [ユーザー] > [リスト表示] で該当ユーザーをクリックします。



2) 画面右上の[デバイスを追加] をクリックします。

マン モニタ	ユーザー	~	アカウント 🔰 ユーザー	く 1/1 > 最近のリスト
п	リスト表示		wso user	ニバイフを追加 毎年 ろの他 ¥
デバイス	詳細表示		wso1811-user sorcerycojp+wso1811user@gmail.com	() (() () () () () () () () () () () ()
ഹാ	役割			
で アカウント	加入状態	\rightarrow	概要 利用規約 イベントログ 共有デバイスログ	

3) [メッセージタイプ] を[Eメール] に設定し、デバイス利用者宛の Eメールアドレスを[宛先アドレス] に設定し、[保存] をクリックします。

デバイスを追加		×
General		
フレンドリ名	wso1811-user デバイス	
組織グループ	WSO1811	
デバイス所有形態タ イプ *	企業 - 専用 🔹	
プラットフォーム <mark>*</mark>	任意	
	□ デバイス情報の高度なオプションを表示	
Message		-
メッセージ タイプ *	なし Eメール SMS	
宛先アドレス *	sancerycago-wood #11 usersygmatic.com	
メッセージ <i>テン</i> プ レート	Device Activation (HTML)@Global × メッセージのプレビュー	
व .	メッセージ テンプレートはメッセージ テンプレートページで構成できま	
テンプレートが表示され	ここをクリックすると、新しいウィンドウまたはタブが開き、メッセージ 1ます。 c ^a	
	保存 キャンセ	zılı

保存が正常に行われると、デバイス利用者にメール「Workspace ONE UEM デバイスアクティブ化」 が送られます。 9.2.2. QR コードを読み取り加入をする

メール「Workspace ONE UEM デバイスアクティブ化」にある QR コードを準備(PC に画面表示、印刷)し、加入するデバイスで Workspace ONE Intelligent Hub アプリを起動し以下を行います。

1) [QR ⊐−ド] をタップします。



2) デバイスでカメラが起動し、QR コードの読み取りが開始されるので、メール「Workspace ONE UEM デバイスアクティブ化」にある QR コードを読み取らせます。



4) QR コードの読み取りに成功すると、ユーザー資格情報の入力を求める画面が表示されます。 これ以降は「8.1. サーバ詳細情報の入力から加入を行う」3)~12)と同じ操作で、加入を行 います。

×									
	cn1.c	lcl-m	ıdm.c	om				0	
				次	^				
1	2	3	4	5	6	7	8	9	0
-	1	:	;	()	¥	&	@	"
#+=			,		?	!	'		$\langle \times \rangle$
ABC		•)		space	e		Go	,

10デバイスの状態確認とリモート操作

デバイスを加入すると、Workspace ONE UEM 管理コンソールから加入デバイスに対し、以降の項 で記載するデバイスのステータス確認、リモート操作が可能になります。

10.1. ダッシュボード - デバイスの加入状況を確認する

[デバイス] > [ダッシュボード] をクリックすると、加入済みデバイスのセキュリティや所有形態、プ ラットフォーム内訳などの統計が視覚的に確認できます。



表示対象は、画面で選択されている組織グループ(以下)と配下のサブ組織グループに加入して いるデバイスです。

🖏 Works	pace ONE UEM		WSO1811
	ダッシュボード		デバイス
	リスト表示		ダッシ
	ライフサイクル	>	
27.114	プロファイルとリソース	>	展開総数
e e	順守ポリシー	>	

10.2. デバイスリスト - デバイスの情報を確認する

1) [デバイス] > [リスト表示] をクリックすると、各デバイスの概要情報がリスト表示されます。

のない			1444
フィルタ 》 ③ デバイスを追加			ト マ リストを検察
■ 最终接线時間 ▲ 一般情報		プラットフォーム	ಷ-೮- ಕ
	55 13 2 0 JF8K 象 企業 - 興用	Apple IOS IPad 6th Gen (32 GB Silver) 13 2.0	hana@wizaas.com hana Hana Urashima
- IS ···································	ald Android 8.0.0 C476 象(企業 - 専用	Android 8.0.0	wizaas.com

加入解除状態のデバイス(以前加入していたデバイス)も表示されます。

3) 更に、リストされているデバイス(行)をクリックすると、このデバイスの詳細が表示 されます。

コートキー		
		7775-5 V UT558*
■ 最終2888時間 ▲ 一般消除	75×1-74-6	2-4-
Phone Total Tota	Apple iOS iPhone X (64 G8 Space Gray) 14.3.0	randalari Maria - Maria Maria Materia
Finite THE C Void o State Person Finite THE C Void o State Person Finite Person UEM 管理対象 企業・専用	el チスクトップ N II TINES MOTO Windows デスクトップ Vostro 3458 10.0.19042	rina takaha disebut penanan zoni Prana 1983 tu Mari terenak
ボイイス > リスト第巻 Phone-11年2月 - 11年2日 - 万利切断 企業- 和 時年 プロファイル アプリ 良新 の デバイスに参加に発き 0 087825 - していてきた	新聞 コンダンツ 位置清明 ユーザー その他 ~ 10.35A 20.75724 () #/16261	(1/7) 第四日の以上 「クエリ」 自然 「ロック」 その他のグクション マ
a セキュリティ	▲ ユーザー信報	ロ デバイス情報
 ✓ UIMCよる目間 ● IDFORE 金属TT がなめです ● アグティベーション DFク作用 ● Ocot のパックアップ 取為 ▲ 取扱UT(スコード ▲ デークが超升めりまけん 	2−9−5; decourteres; SR framinanos I X−20 reconstratered beginner com	田島セグリーブ 「「「「「」」」」 メスペート・クリーブ メンタート・クリーブ メンタート・クリーブ ストロー・「」 メンタート・クリーブ そのたち、「」 本日のたち、「」 二 本日のたち、「」 二 本日のたち、「」 二 二 二 二 二 二 二 二 二 二 二 二 二
◆ 利用可能な OS アップデート なし		18006 UDID 1819 - 1910 - 1919 - 1919 - 1919 - 1919 - 1919 - 1919 - 1919 - 1919 - 1919 - 1910 - 1910 - 1919 - 1919 - 1919 - 1910 - 1919 - 1910
第 アプリ ✓ 1/1 インストール原数 00 80572 00 8257259729	 C コンテンツ 0/0 インストール浜か 00 埋きパトロンテング 00 埋きパトリクエンデング 同り当てられたコンテングはありません コンテング世界ページを変更 	■ 電源活動 パッテリ想染中 ストレーン写動 気いるフレーインタ(50)(84,8%) 物理メモリ 2.5(6)(7)レーイン5(6)(83,1%) パッテリ知識 何を、 ネットワークテザリング オフ
医 証明書	@ ネットワーク	
インストール液み 回時間失功能証 (<60日前) の 期間状況の証明書 の 期間状況の証明書	 ショムカード状態工業 ローミング中ではありません データローこング助防 	

10.3. デバイスをリモート操作する

デバイスの詳細表示の右上にあるボタン(コマンド)で、デバイスに対してリモート操作をする ことができます。

デバイス > リスト表示	1	2	3	< 1/7 > 最近のリスト
iPhone-	クエリ	送信	ロック	その他のアクション 🗸
iPhone X (64 GB Space Gray) 14.3.0 所有形態: 企業 - 専用				
			バスコ デバ アプ 電理 管理 デバ eSM	- ドを消去 イス (4) リトークン生成 第冊ワイプ (5) 設定 イス ワイプ (6) 1 な更新

ここでは、デバイスの管理で必要になる以下の基本操作を説明します。

基本操作

	操作	説明
		このデバイスに対し、Workspace ONE UEM SaaS ヘデバイ
U	[עבע]	ス情報を送信するよう要求します。
		このデバイスに対し、メッセージを送信します。
2	[送信]	[メッセージタイプ] は[Eメール] または[プッシュ通知] を選択
		できます。([SMS] は未対応)
		このデバイスをロックします。
3	③ [ロック]	詳しくは「9.3.1. デバイスをロックする」をご参照く
		ださい。
a	[その他のアクション] >	このデバイスのパスワードを消去します。
Ð	[パスワードを消去 – デバイス]	
		このデバイスを Workspace ONE UEM へ加入する前の状態
ß	[その他のアクション] > 「管理 本業情報情報ロノ	へ戻します。
		詳しくは「 9.3.2 企業情報情報ワイプ 」をご参照くださ
	7]	<i>د</i> ر.
	[その他のアクション] >	このデバイスを工場出荷状態に初期化します。
	[管理 – デバイスワイプ]	詳しくは「 9.3.3 デバイスワイプ 」をご参照ください。

参考

[Dック] [パスワードを消去 - デバイス] [管理 - デバイスワイプ] が表示されない場合は、「10.1 コマンドの設定」で記載の設定をご確認ください。

10.3.1. デバイスをロック	
デバイス紛失の際に、ロックする事ができます。	
1) [ロック] をクリックします。	

デバイス > リスト表示	く 2/5 》 最近のリスト
wso1909 iPhone iOS 13.2.0 JCLK	クエリ 送信 ロック その他のアクション・マー
iPhone X (64 G8 Space Gray) 13.2.0 所有形態 企業 - 専用	

2) iOS の場合は以下の画面が表示され、ロック画面にメッセージと電話番号(拾得時の連絡 先)を表示させる事ができます。([メッセージテンプレート]を[カスタムメッセージ]にした場合)

テ	バイスをロック	ク	×
	カスタムメッセージを送 フィールドの最大文字数	st信するには、パスコードがデバイス上に存在している必要がありま は、256 文字以内にする必要があります。	ミす。 メッセージ
	メッセージテンプレー ト	カスタムメッセージ メッセージはありません	
	メッセージ	Support Desk	
	電話番号	03-12xx-xx34	
			送信 キャンセル

[送信]をクリックすると、以下の画面でロックされます。



3) Androidの場合は、通常のロック画面でロックされます。

1)の[**ロック**] 後に表示される以下のダイアログに対し、[**OK**] をクリックすると、デバイスが ロックされます。

5.awmdm.jp の内? スのロックを要求します!	9		_
		OK	44540
5.awmdm.jp ወሶነት			
スがロックされました			

10.3.2. 企業情報ワイプ デバイスを加入する前の状態に戻します。これにより Workspace ONE UEM で設定したアプリケー ションやプロファイルを含む全ての管理企業リソースが削除されます。 この操作を戻すためには、Workspace ONE(AirWatch)への再加入が必要になります。

1) [その他のアクション] > [管理 - 企業情報ワイプ] をクリックします。

	単位のジスト
wso1909 iPhone iOS 13.2.0 JCLK	クエリ 送信 ロック その色のアクション 🗸
iPhone X (64 G8 Space Gray) 13.2.0 所有形態 企業 - 専用	

2) 初回ログインで登録したセキュリティ暗証番号を入力します。中止したい場合は、[キャンセル] をクリックします。

SERVER SEA MORNING	887-06877-77-582, 2027-668809872-74880872-7 C#LE7.
00002007220	ままず、周囲 konoch によるテンドス国際なる新な場合。同時入方は新になります。 (…)Mark
Protect-p	- mag
	And Colors And and And and And And
1.0.0	
-	
a service and	
8-1-7+205 375	150
12-6	A service and appendix of
\$52FL	Andrea
8821-7	Argentan
muxing.	D
н 345-7×272 385 81055 9825-7 892352	Tanun Tan Konnandiliphiran Angenan D C-54. Non7D27 / Achimen Statum Falses Anne F/- Exter.
20173-120×1 123/F2-9-08	
10173-17-04 10172-17-08	

セキリティ暗証番号を最大回数以上間違えると、ログアウトします。最大回数については 「10.2 制限事項の設定」をご参照ください。

10.3.3. デバイスワイプ

デバイスを初期化して工場出荷状態に戻します。

1) [その他のアクション] > [管理 - デバイスワイプ] をクリックします。

デバイス > リスト表示	< 2/5 》 単近のリスト
wso1909 iPhone iOS 13.2.0 JCLK	クエリ 送信 ロック その色のアクション Y
(Phone X (64 G8 Space Gray) 13.2.0 所有形態 企業 - 専用	I
	デバイスワイプ
参考	

デバイスワイプのメニューが表示されない場合、プライバシー設定でデバイスへの操作 が制限されている可能性があります。「10.1 デバイスワイプの設定」にて確認・設定変 更の上ご利用ください。

2) 初回ログインで登録したセキュリティ暗証番号を入力するとデバイスワイプが実行されま す。中止したい場合は、[キャンセル] をクリックします。

デバイスウイブルアムでの 出物時の状態に使します。 せんのてご絵色の上、特別	クプリ、データ、ミメール、プロファイムおよび VCM MMIの利用し、デディスまごは 2016年5月5日巻、すべてのユーザー個人資料も含まれます。この知道はつに見せま してくてきい。	
フレンドリカ	Users-1100 [Provide (73.14.) ((())	
⊐-#-€	m++-1411	
2/10/4	1. A. T.	
	Are .	
プラントフォーム	Apple	
12	Tatanan .	
オペレーディング シ ステム	1231)	
$\mathbb{E}^{\ell} \gg - \ell \mathbb{E}$	na anna geograd an	
素がモデル	White	
相称ジループ	Augustus.	
7-9750080	Q	
プロネシミティ むり トアップを開止	D	
0710728084 0710728084 0710728088	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

セキリティ暗証番号を最大回数以上間違えると、ログアウトします。最大回数については 「10.2 制限事項の設定」をご参照ください。

11システム構成

11.1. デバイスワイプの設定

デバイスの所有形態により、ロックやワイプなどのデバイスに対する操作を制限することができ ます。デバイスワイプの操作が行えない場合は、デバイスの所有形態と以下の設定をご確認くだ さい。

 [デバイス] > [デバイス設定] をクリックし、[設定] 画面の[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。



2) [現在の設定] を[オーバーライド] にします。

設定	
> システム > デバイスとユーザー > 全額	デバイスとユーザー > 金約 プライバシー ◎
加入 フレンドリ名 表現フィールド	② 分析や個人情報など、この製品で収集されるさまざまなタイプのデータについては、VMwweのプライバシーボリシーざを参照してください。
メッセージ テンプレート 通知	現在の設定 〇 坦季 🔘 オーバーライド

3) [コマンド - デバイスワイプ]に設定されている、各デバイス所有形態に対する許可を確認します。 [〇許可しない]が設定されていると、デバイスに対する操作でコマンド未表示になります。 設定変更は、マウスポインタを各設定箇所に合せて設定ボタンを表示させます。

(m) 1+0	-idit CIF4	D.		
	企業一期用	追踪 共務	经规则 利用	割り当てなし
コマンド				
デバイスフィブ	۲		0	0
デバイス パスユードをクリア ロック/シャットダウン/高級	FK128 🛞		0	0

4) 設定変更した場合は、[保存]をクリックします。

ユーザーフレンドリなプライ	パシー通知			
ユーザーフレンドリなプラ イバシー道知を有効化する	45.73	8:0		
サブクループの権限。	О КАЛЭ	0.7-/(-34K0A	● 総束またはオーバーライド	
				<i>au</i>

11.2. 制限された操作の設定

デバイス削除やアカウント削除などの操作に、パスワードによる保護処理を適用することができます。

 [デバイス] > [デバイス設定] をクリックし、[設定] 画面の[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) [パスワード保護処理] の各項目に対し、 [有効] にすると、実行時にセキュリティ暗証番号の 入力を求められるようになります。

極の設定	○ 昭承 ● オーバーライド	
/スワード保護処理 ――		
O MERBRESS, MI	種の先了有に、智覚者にセキュリティ福祉毎号の入力を求める東面が表示されます。	
管理書アカウント制錬	630 8 .0	
管理者/1スワード変更	8.00 B.00	
AirWatch Cloud Connector の証明書を再生成する	e 620 200	
APNIS 証明書の変更	(10) Em	
アプリケーションを削除す る/非アクティブにする/低端 する	41.90 21.5 0	
	• • • • • • • • • • • • • • • • • • •	

BIOS バスワードのリセット を強制	有効 25%
暗証番号の試行回数上限★	3

また、セキュリティ暗号番号入力ミスによるログアウトまでの試行回数の設定も行えます。

3) [保存] をクリックします。

デバイスの再起動	和效 30 30
シャットダウン	有1.25 25 28
サブクループの権略	○ 総乗のみ ○ オーバーライドのみ ● 総集またはオーバーライド

12弊社サポート

株式会社ウィザース Workspace ONE サポートデスク

E-Mail wso-support@wizaas.co.jp

TEL 03-3633-4833

重要

お問い合せの際、お客様へ発行させていただいた[VMware Workspace ONE SaaS 確認書]に記載の ライセンス管理番号を確認させていただいております。 Workspace ONE UEM 管理コンソールガイド(入門編)

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。