



Workspace ONE PoC ガイド Chapter 1

スタート編

V 2.2



ヴイエムウェア株式会社





Table of Contents

1	Wo	orkspace ONE PoC 環境	5
	1.1	システム構成	5
	1.2	各コンポーネントのご紹介	7
	1.2	2.1 AirWatch	7
	1.2	2.2 VMware Idenitity Manager	3
	1.3	環境の準備と留意点	3
	1.4	各章の目的	9
2	٧M	1ware Enterprise Systems Connector による環境の統合10)
	2.1	本章のゴール10	C
	2.2	前提条件1(C
	2.3	設定手順1	1
	2.3	3.1 VMware Enterprise Systems Connector のインストールと設定21	1
	2.3	8.2 AirWatch と Active Directory の連携設定1	7
	2.3	8.3 Identity Manager と VMware Enterprise Systems Connector の連携設定)
	2.3	3.4 Identity Manager と Active Directory の連携設定22	2
	2.3	3.5 Identity Manager 上でのアウトバウンドモードの設定	7
	2.3	3.6 AirWatch と VMware Identity Manager の統合	3
3	ディ	ィレクトリユーザを使用したパスワード認証の構成32	2
	3.1	本章のゴール	2
	3.2	設定手順	2
4	iOs	S デバイス用モバイル SSO の構成	5
	4.1	本章のゴール	5
	4.2	設定手順	5
	4.3	iOS デバイスで動作確認	5
5	ディ	バイスコンプライアンス認証の構成 45	z
	5.1	本章のゴール	3
	5.2	24年14月11日11日11日11日11日11日11日11日11日11日11日11日11日	R
~			
6	MA V	1Ware Verify を使用した多要素認証の構成55	>
	6.1	本草の」ール	2 -
	6.2	設走于順	2
7	初日	証設定の最適化	5
	7.1	本章のゴール6!	5
	7.2	設定手順	5
8	ΓA	APPENDIX] 参考情報	7
-	8.1	製品ドキュメント	7
	8.2	各種ガイド	7
	8.3	その他	7



更新履歴

バージョン	更新日	更新者	内容
1.0	2017.04.12	Tomonori Takaki Shinji Sagawa	新規作成
1.1	2017.04.13	Tomonori Takaki	各種手順の修正
2.0	2017.06.02	Tomonori Takaki Shinji Sagawa	Workspace ONE 9.1 へ対応 -VMware Enterprise Systems Connector -Workspace ONE App for iOS V3 -VMware Verify シナリオ変更
2.1	2017.06.07	Shinji Sagawa	第7章 認証設定の最適化追加
2.2	2018.04.27	Kota Baba	vIDM, Airwatch のバージョンアップに伴う各種手順 修正およびスクリーンショットの撮り直し



はじめに

本書は VMware が提供する正式な製品マニュアルではなく、フリートライアルや PoC に使用いただくた めの参考資料です。また、VMware Identity Managerの操作や設定方法を中心に記載しており、AirWatch 自体の基本的な操作や設定方法は簡略化している部分がありますので「AirWatch フリートライアルガ イド」シリーズも併せてご確認ください。

内容は適宜変更や更新される可能性があり、かつ記載内容およびその動作を保証するものではございま せん。



1 Workspace ONE PoC 環境

1.1 システム構成

Workspace ONE の一般的な Cloud デプロイメントでは企業内の Active Directory と VMware Enterprise Systems Connector を介して連携し、AirWatch と VMware Idenitity Manager は REST API を使用して連携を構成します。



Workspace ONE 概要構成とポート要件



1.2 各コンポーネントのご紹介

1.2.1 AirWatch

VMware が提供している EMM で、モバイルデバイスを"活用"するために必要な機能を取りそろえた製品となります。一般的な MDM に加えて、下表の機能が利用できます。

機能	アプリケー ション名	詳細
利用アプリケーション のコントロール	AppCatalog	App Store や Google Play 上で公開されているアプリケー ションを直接インストールさせるのではなく、管理者が許可 したアプリケーションのみを利用できる状態にしておいた り、プッシュで端末にアプリを配信することが可能です。
社内データへの アクセス	Content Locker	PDF やオフィス系のデータ、写真、動画といった様々なコ ンテンツを、暗号化/コピペ禁止/他のアプリへのデータ引き 渡し禁止、等のセキュリティを掛けた状態で、デバイスに配 信することができます。
企業メールの利用	Boxer	データを暗号化したり、本文のコピペを制御したり、添付フ ァイルを Contents Locker にしか渡せないように制御する 等、セキュアなメール利用が可能です。
社内システムへの アクセス	Secure Browser	面倒な VPN 接続やパスワード入力を実施することなく、社 内の Web システムにワンタッチでアクセスできます。

AirWatch ではこれらの機能を下図のような、包括的なコンソールである AirWatch Console を用いて、一元的に管理および運用を実施します。







1.2.2 VMware Idenitity Manager

VMware の提供する IDaaS 製品で、下記の機能を提供します。

- 業務で利用するアプリケーションのポータル機能
- アプリケーションへのシングルサインオン
- 様々な認証方式をサポート
- その他の VMware 製品との密な連携

🛟 Workspace ONE [™]		Tenant Admin -
ダッシュポード ユーザーとグループ カタログ ▼ ID とアクセス管理	□- <i>\</i>	Q ユーザー、グループ、またはアプリケーションを検索
1 9809121k2-9-		* * *
ユーザーとグループ	アプリの人気 7日間 1	アプリの導入
4 ユーザーの合計数 グルーフの合計数		まだレポートはありません。 ユーザーが実際に使用しているア
ユーザー 最終ログイン 上 今すぐ		ノリを表示します。 レポートを表示するには、まずア プリを追加する必要があります。

1.3 環境の準備と留意点

- AirWatch Blue/Yellow エディションもしくは Workspace ONE Advanced エディションに含ま れる AirWatch SaaS テナントおよび VMware Identity Managaer SaaS テナント。
- AirWatch の VMware Identity Manager 連携設定はディレクトリサービスを構成している組織 グループで実施する必要があります。
- 特段の記載が無い限り AirWatch 管理コンソール上の設定は貴社テナントの最上位の組織グループ (Customer OG もしくは Company OG と呼ばれる組織グループ)で実施してください。

AirWatch SaaS および VMware Identity Manager SaaS を お持ちでない場合は、必要に応じて AirWatch フリートライアル	30日間の 開始する) <mark>フリ</mark> ー	・トライアノ	しを
(<u>http://www.air-watch.com/lp/ja/free-trial/</u>)をお申し込み <ださい。	名 全葉メールアドレ	2	姓	
フリートライアルの申し込み方法やフリートライアル中の	役職			
支術的なお問い合わせは、御社担当営業までご連絡ください。	電話		郵便番号	
	業界	~	固	~
	興味のある	5 ソリュ-	ーションを選	択∙
	◎ モビリティ	イ管理 V#回作業		
	 ☑ JJFJ ☑ Identity Ma 	ノ共向TF未 anagement		



1.4 各章の目的

各章はそれぞれが目的のために完結する手順となっているため、構成が必要な章の内容を下表にて確認 いただき、実施のほどお願いいたします。

章	章題	目的
2	VMware Enterprise Systems Connector による環境の統合	VMware Identity Manager および AirWatch に対して 企業内の Active Directory との連携を構成し、ユーザ 管理を AD で一元管理する場合に実施します。
3	ディレクトリユーザを使用したパ スワード認証の構成	ブラウザーベースでのアクセスや AirWatch で管理し ていないデバイスから、Active Directory の認証情報 を使用した認証を構成する場合に実施します
4	iOS デバイス用モバイル SSO の構成	iOS デバイスからモバイル SSO を利用し、アプリケー ションへのシングルサインオンを構成する場合に実施 します。
5	デバイスコンプライアンス認証の 構成	管理下のデバイスが企業の設定したセキュリティ規準 に準拠しているかどうかを評価した上での認証可否判 断や、企業が使用を認めていない管理外デバイスから のアクセスを遮断するなどの要件である、デバイスコ ンプライアンスを構成する場合に実施します。
6	VMware Verify を使用した多要素 認証の構成	Workspace ONE に含まれる多要素認証機能である VMware Verifyを構成する場合に実施します。
7	認証設定の最適化	VMware Identity Manager へ管理者アカウントでロ グインできるように構成する場合に実施します。



2 VMware Enterprise Systems Connector による環境の統合

2.1 本章のゴール

Workspace ONE 9.1 以降で提供される VMware Enterprise Systems Connector は、従来の AirWatch Cloud Connector と VMware Identity Manager Connector の機能が統合されています。本 章では、VMware Enterprise Systems Connector をインストールし、VMware Identity Manager お よび AirWatch に対して企業内の Active Directory との連携を構成します。



Workspace ONE 9.1 以降の構成



2.2 前提条件

VMware Enterprise Systems Connector をインストールするための Windows マシンがあること。 サポートされる Windows 環境は以下の通り。

- Windows Server 2008R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- 連携対象の Active Directory ドメインに参加済み
- 英語版 OS を使用



2.3 設定手順

2.3.1 VMware Enterprise Systems Connector のインストールと設定

1. ESC のマシンからブラウザで AirWatch コンソー ルヘログインし、[グループと設定 / すべての設定 システム 「はじめに」 プランディング - エンタープライズ統合 エンタープライズ統合 サービス 版証明 VMacare システム > エンタープライズ総合 > VMware Enterprise Systems Connector (/ システム / エンタープライズ統合 / VMware ● エンターブライズ統会の機能性がアップグレードされました Enterprise Systems Connector]の順にクリック 今後、花参サービスはMaan Emerges Speece Connector そ長って使きたち、Maana Tumoi の使きたちキュアな漫画チャンはホッパイスからな使い、コンスパフトささらも ストビマシオテ、「Chargena Integration Association 100 そこれとしていたり世界する。それの100 花をきんかいの中にの手切いのConnector EMPL くんだい、使きをやすることによう、USLは数字に気からたます。155 に数字であからやサービスは、ESをホテルとていたサーバに Closed Connector ダインストールされらます。または ES が発展室的会 れるとで見ていたい。 VMware Enterprise Systems Connector ディレクトリ アービ ディレクトリ アービ Eメール (SMTP) VMware Tunnei ビアアービア サードパーティ 製プロ キシ します。 設定を移行する 今後このメッセージを表示しない キン SMS プルサービスインス トーフ 現在の設定 ●単年 〇オーバーライド ト Syslog 助画 CDN VMware Enterprise Systems Connector リモート管理
 VMware Identity Manager
 セキュリティ ヘルプ
 ローカリゼーション
 レポート 定請受信 利用規約 エンタープライズコンボーネントへのセキュアな接続を有効化します ○ 継承のみ ○ オーバーライドのみ ● 継承主たはオーバーライド サブダループの構図・ S/MIME , 高度な設定 2. 「現在の設定」でオーバーライドを選択し、 [VMware Enterprise Systems Connector を有効 🥏 正常に保存されました 「はじめに」 プランディング ・**エンタープライズ統合** エンタープライズ統合 サービス 全般 高度な設定 化]にチェックを入れ、[保存]をクリックします。 〇単条 ●オーバーライド 81至応
 VMAuser Enterprise Systems Connector ディレクトリラービス
 Eメール(SATP)
 VMause Tunnel ビアラービア
 Fバーティ数プロ キシ
 SMS ブル サービス インス トーラー 2 VMware Enterprise Systems Connector を有効化 イズコンボーネントへのセキュアな接続を有効化します。 その後、[VMware Enterprise Systems Connector 白動更新を有効化 □ 自動更新を有効化することにより、対応する ArWatch コンソールのインスタ シスを新しいバージョンにアップグレードした後、責社サーバにインストール キャル Maure Enternice Systems Connector をシールレスに更新できます。 インストーラをダウンロード]リンクをクリックし Syslog 動面 CDN 「モート管理 ます。 VMware Enterprise Systems Connector インストーラをダウンロード 古 構成方法の評判は、IVMware Enterprise Systems Connector ガイド1を参照してください。 サブグループの爆放・ ○ 肥呆のみ ○ オーバーライドのみ ● 肥早またはオーバーライド S/MIME 英度な設定 保存 接続のテスト 3. ダウンロード用のパスワードを入力し、[ダウンロ ード]をクリックします。 are Enterprise Systems Connector 証明書のバスワードを入力してください。設定を VMW ンボードする際必要となります。 ワードには 6 文字以上を食める必要があります。 0 #.÷ ペスワードの再入力・ . 82 ダウンロード

VMware Enterprise Systems Connector をインストールします。



4.		ダウンロードしたファイルを実行します。
	P I + Application Track Describes	
	None Start Matage ✓ ← → ∞ ∱ ThtSP, > Desricods ✓ Ø	
	Curch secrets Mame Date modified Type Size Size Middate (https://www.file.org/curched.ac.ac.ac.ac.ac.ac.ac.ac.ac.ac.ac.ac.ac.	
	Develoads P Open Downloads P Open Downloads P Downloads P	
	Pictures Proto Start Proto Start Traing Traing traing	
	Network Share with Network Proto taskbar	
	nestore previous vestions Sand to	
	Cate Copy Categories	
	Delete Rename	
	Properties	
	1 item 1 item selected 421 MB	
F		
J.		(.NEI Framework のインストールを求められ
	VMware Enterprise Systems Connector - InstallShield Wizard	た場合は) [Install] をクリックし、 .NET
	Mware Enterprise Systems Connector requires the following items to be installed on	Framework のインストールを行います。インスト
	your computer. Click Install to begin installing these requirements.	
	Status Requirement	クし円起動しより。
	Pending Microsoft .NET Framework 4.6.2 (Web Download)	
	Install Cancel	
	VMware Enterprise Systems Connector - InstallShield Wizard X	
	reboot. Click Yes to restart now or No if you plan to restart later.	
	Yes No	
6.		再起動後、インストールウィザードが起動します。
	A Marine Estimate Contains Consister Installation Weiner	
	Welcome to the Installation Wizard for VMware Enterprise Systems Connector	
	The Installation Wizard will Install Mikuran Extension Sustance	
	Connector on your computer. To continue, click Next.	
	vm ware: airwatch	
	WARNING: This program is protected by copyright law and	
	international treaties.	
	< Back Next > Cancel	





7		
/.		使用計話に回息し、[Next]をクリックします。
I	Wware Enterprise Systems Connector - Installation Wizard X	
-	Please read the following license agreement carefully.	
	VMWARE END USER LICENSE AGREEMENT	
	PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.	
	IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE V	
	I accept the terms in the license agreement Print I do not accept the terms in the license agreement Installiched	
	< Back Next > Cancel	
8.		AirWatch Cloud Connector
-	R VMware Enterprise Systems Connector - Installation Wizard	VMwaro Idontity Managor Connector
	Custom Setup	
	Select the program features you want installed.	の両コンボーネントをインストール対象にし、
	Click on an icon in the list below to change how a feature is installed.	[Next]をクリックします。
	B	
	VMware Identity Manager Connector Connector Connector	
	This feature requires 305MB on your band drive	
	you have are.	
	Install to: C:\VMware\ Channe	
	InstallShield	
	Help Space < Back	
9.		インストール先フォルダを指定し、[Next]をクリッ
-	Whware Enterprise Systems Connector - Installation Wizard X	
	Destination Folder	クします。
	Click Next to install to this folder, or click Change to install to a different folder.	
	Install VMware Enterprise Systems Connector to:	
	C:\VMware\ Change	
	InstallShield	
	< Back Next > Cancel	
10.		IRF のインストールが求められたら、「Yes1をクリ
-0.	Question X	
		ックします。
	The latest major JRE version is required for the software that you	
	are trying to install.	
	Yes No	



11. VMware Enterprise Systems Connector - InstallShield Wizard × ACC Certificate Password vmrware: airwatch Please enter ACC certificate password Certificate Password Certificate Password Accel	インストーラのダウンロード時に設定したパスワ ードを入力し、[Next]をクリックします。
12. VMware Enterprise Systems Connector - InstallShield Wizard × Proxy Information Specify proxy information if this server is behind a proxy Outbound proxy? InstallShield InstallSh	 [Next]をクリックします。 サーバが外部へ接続するのにプロキシを経由する 場合は、プロキシの情報を入力します。 * この画面で設定するプロキシは ACC コンポーネ ント用の設定になります。プロキシを使用する 場合には次の画面で VIDM Connector コンポー ネント用のプロキシ設定も実施してください。
13. Image: Conector - InstallShield Wizard X VMware Identity Manager Connector - InstallShield Wizard X VMware Identity Manager Connector Configuration vmware airwatchr Connector Port: 443 Would you like to use your own SSL Certificate? Browse Oartificate (pfx): C:\ Oartificate % page an HTTPS prox? InstallShield InstallShield	[Would you like to use your own SSL Certificate?]のチェックを外し、[Next]をクリック します。 * この画面で設定するプロキシは VIDM Connector コンポーネント用の設定になりま す。プロキシを使用する場合には前の画面での ACC コンポーネント用のプロキシ設定も実施し てください。



14.	ここではチェックを入れずに[Next]をクリックし
Jett Image: Connector - InstallShield Wizard Viscare Enterprise Systems Connector Activation Viscare Enterprise Systems Connector Activation Viscare Enterprise Systems Connector New or effer the Viscare Enterprise Systems Connector new or effer the Would you like to activate the Connector now? Ves Admin Password: Confirm Password: InstallShield	ここではチェックを入れすに[Next]をクリックし ます。
<complex-block></complex-block>	サービスを起動するためのドメインアカウントを 手入力します。 認証に問題がない場合、Install に進めます。 (注) Windows Server 2016 では Computer Browser サービスが存在しないため、ドメインア カウントは手入力する必要があります。 Windows Server 2012 R2 以前のバージョンで は、[Browse]をクリックし、参照することが可能 です。ただし、認証に失敗する場合は以下を確認し て下さい。 ・ESC サーバー上で Computer Browser サービ スが有効になっていること ・Computer Browser サービスが通信できるよう にファイアウォールが構成されていること
16. VMware Enterprise Systems Connector - Installation Wizard Acady to Install the Program The wizard is ready to begin installation. Click Install to begin the installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. InstallShield Acade Acade Acade Acade Acade Acade Acade Acade Acade Acade Acade Acade Acade Acade Acad	[Install]をクリックし、インストールを実施しま す。 (インストールには環境により 7 分程度の時間を 要します。)



17.		TLS 1.2 を有効化する旨の警告が表示されます。
	💕 VMware Enterprise Systems Connector - Installation Wizard — 🛛 🛛 🗙	
	Installing VMware Enterprise Systems Connector	
	The program features you selected are being installed.	
	Please wait while the Installation Wizard installs VMware Enterprise Systems Connector. This may take several minutes. WMware Enterprise Systems Connector - InstallShield Wizard	
	Registry keys were added to enable TLS 1.2 on this server. TLS 1.2 is required for AirWatch Cloud Connector.	
	Please reboot the server after this installation finishes for this change to take effect.	
	OK	
	InstallShield < Back Nevt >Cancel	
	< JULA IPEAL* Concer	
18.		[Finish] をクリックします。
	🛃 VMware Enterprise Systems Connector - Installation Wizard 🛛 🗙	これでインストールは完了です。
	Installation Wizard Completed	
	The Installation Wizard has successfully installed VMware	
	Enterprise Systems Connector. Click Finish to exit the wizard.	
	vm ware: airwatch:	
	Show the Windows Installer log	
	< Back Finish Cancel	
	- Noru Fuer center	
19.		インストール完了後、再起動を求められるので、
		「Yes] をクリックし再起動をします。
	😹 VMware Enterprise Systems Connector Installer Informa $ imes$	
	changes made to VMware Enterprise Systems Connector	
	to take effect. Click Yes to restart now or No if you plan to restart later.	
	Yes No	
1		



2.3.2 AirWatch と Active Directory の連携設定

VMware Enterprise Systems Connector の中の ACC の機能で、AirWatch と AD を連携させます。

1.			AirWatch コンソールヘログインし、[グループと設
1.	メステム > エンタープライズ8 ディレクトリサービス	Explosion in Contract And Annual Contract	AirWatch コンソールヘログインし、[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 / ディレクトリサービス]の順にクリックします。「ウィザードをスキップして手動で構成」を選択後、以下の項目の設定を行います。各項目はそれぞれの環境にあったものを入力してください。 ディレクトリタイプ:Active Directoryサーバ:ADのホスト名(FQDN 形式) 暗号化:なし ポート:389
ービス 認証局 VMware Enterprise Systems Connector ディレクトリ サービス	現在の設定	サーバ ユーザー グループ	プロトコルバージョン:3 サービスアカウントの資格情報を使用:無効
 Eメール (SMTP) VMware Tunnel ビアツービア サードパーティ製プロキシ 	LDAP ディレクトリタイプ*	Active Directory ·	バインド認証タイプ:GSS-NEGOTIATE
SMS ブルサービスインスト ーラ Syslog	DNS SRV サ−/<*	有効 <u>無効</u> ① add1.awtoriJan	バインドユーザー名:ドメインユーザー名
動画 CDN リモート管理 VMware Identity Manager	暗号化タイプ*		
 ヘルプ ローカリゼーション レポート 定期受信 利用規約 	プロトコル パージョン* サービス アカウントの東線感報		
S/MIME ▶ 高度な設定 デバイスとユーザー	5-こくアガランドの員俗情報 を使用 バインド認証タイプ*	有効 無効 ① 夏名 ベーシック ダイジェスト Kerberos NTLM GSS-NEGOTIATE	0
コンテンツ アプリ	パインド ユーザー名 パインド パスワードを消去	administrator O	
Eメール テレコム	バインド パスワード	① 示療 カーゼ マト×3	
管理者 インストール		awgnlan るd01.awgnlan ・ ドメインを追加	
2.			」
^{システム} キンタープライズ戦会 ディレクトリ サーヒ	> Zス ⊕	7-11 2-12 84-7	DN を設定します。 ベース DN は [+]ボタンをクリ ックすることで参照できます。
<u>7 − 7 − 7 − 7 − 7 − 7 − 7 − 7 − 7 − 7 −</u>			
Fメイン awign lan ユーザー オブジェクト クラス・	r4−72.084● DC=sas(pn,DC=is	n 8	
ユーザー検索フィルタキ	person BiobjectCategory~person0sA	MAccountiume-(involmentive/)	
> 内法な設定 サブグループの確認	○ 龍条 ○ オーバーライド ●	● 単発またはオーバーライド	
		80 SH(07A) 0+17+7047-1988	

3. \$\$272; \$29-79(788; \$\$7400000000000000000000000000000000000		画面上部で[グループ]タブをクリックし、ベース DN を設定します。ベース DN は [+]ボタンをクリ
 正常に目行されました 現在の設定 アメイン メタクロの 	9-rt a=9- 26-7 OR8 € 8-r-1-9 < F -r-5.00 ⁴ (compactors 0)	9099ることで参照できより。 設定元 1後、 [味 存]をクリックし、エラーなく保存できることを確 認します。
アルーブイブジッションフラス* 技術ニーットイブジッションフス* ・ 高度に設定 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	0 RB 0 0 0 RB 0 0 0 RB 0 0	[接続のテスト]をクリックし、AD との接続に問題 ないことを確認します。
サブグループの権限	◎ ■承 ◎ オーバーライド ⑧ 趣承またはオーバーライド	
	 保存 接続のテスト セットアップ ウィザードを開始 指定サーバ名、バインドユーザー名、およびパスワードを使用して、正常に接続されました。 	



AD との連携が正しくできていることを確認するために、AirWatch へ AD 上のグループとユーザーを登録します。(事前に AD 上にグループを作成しユーザーを追加してください。)

4. * ユーザー * ユーザー グループ * ユーザー グループ * コーザー グループ * ジェーザー グループ * ジェーザー グループ * ジェーザー グループ * ジェーザー グループ * ユーザー グループ * コーザー グループ	AirWatch コンソールヘログインし、[アカウント / ユーザーグループ/ リスト表示]の順にクリック し、追加メニューから[ユーザーグループを追加]を クリックします。
Joint Joint	以下のように設定をし、[ユーザーを確認]をクリッ クします。 タイプ:ディレクトリ テキスト検索:AD上のグループ名 ドメイン、グループベース DN が入力されていない 場合は入力 設定が正しければ、グループの情報を取得できま す。[保存]をクリックしてグループ登録を完了し ます。
6.	[アカウント / ユーザーグループ/ リスト表示]の 順にクリックし、リスト上にグループが登録されて いることを確認します。 [アカウント / ユーザー/ リスト表示]の順にクリ ックし、リスト上にグループ内のユーザーが登録さ れていることを確認します。



2.3.3 Identity Manager と VMware Enterprise Systems Connector の連携設定

SaaS 上の Identity Manager とインストールした ESC を連携させる設定を行います。

1.	Identity Manager の管理コンソールへアクセスし ます。 URL: < <i>https://xxx.vmwareidentity.asia></i> (注) xxx の箇所には事前に払い出された Identity Manager のテナント名が入ります。 ユーザー名/パスワードを入力し、[ログイン] をク リックします。
2. 1909 ANA/22012 - 9 - 21 - 9 - 21 - 9 - 21 - 9 - 21 - 9 - 21 - 9 - 21 - 9 - 21 - 9 - 9 - 9 - 9 - 9 - 9 - 9 - 9 - 9 -	 [ID とアクセス管理 / セットアップ / コネクタ] の順にクリックします。 その後、[コネクタを追加]をクリックします。 コネクタ ID 名に任意の値を入れ、[アクティベーションコードを生成]をクリックします。 コネクタのアクティベーションコードが生成されたらその値をコピーしておきます。
 コネクタを追加 コネクタを追加 コネクタの間の通信を確立するために使用されます。アクティベーションコードをコピーしてコネクタのアクティベーションコードはサービスとコ ネクタの間の通信を確立するために使用されます。アクティベーションコードをコピーしてコネクタのセットアップに適用します。 コネクタのアクティベーションコードをコピーしてコネクタのアクティベーションコードのコードをコピーして加り付けます ロネクタのアクティベーションコードをコピーして施り付けます 	









2.3.4 Identity Manager と Active Directoryの連携設定

Identity Manager と Active Directory の連携設定を行います。

1.				VMware Identity Manager コンソールで、「ID と
	ユーザー属性 デフォルト最低	ユーザーがディレクトリと同時化するとき、また	はローカルユーザーが作成されるときに使用する	アクセス / セットアップ / ユーザー属性]を開き、 デフォルト属性の userPricipalName と distinguishedName 属性を必須に設定します。
		属性を選択します。これらの属性は「ディレクト	リ」ページで確認することができます。	
		disabled	82'5R	
		distinguishedName	~	
		domain		
		email	~	
		employeeID		
		firstName	✓	
		lastName	~	
		phone		
		userName	✓	
		userPrincipalName	~	
2.				[使用するその他の属性を追加]に[objectGUID]
	使用するその他の属性を追 他の属性を	ディレクトリに同期します。ディレクトリの属性ペ	ージに移動して、これらの属性をマッ	属性を追加します。
	201 7 0 0 7 8			
	属性 objectG	DIU	+ × +	
				保存をクリックします。
	保存			
3.				Identity Managerの管理コンソールで、「ID とア
			Q.ユーザー、グルーブ、またはアプリケーションを総定	/ クセス管理 / 管理 / ディレクトリ]の順にクリッ
746	#FF: ユーラー2238-7 3909 - ロ2230004 ロール トリ ID プロボイダ パスワード開始からスタット 読む方法 ポリシー ディールマントレノ(1)		54 2402593	
	ディレクトリ8 タイプ	ГАЛЭ НИЙЛЬЭЛ-Э НИЙЛЬЭ	LCAPINIA 経由の Active Directory を追加 LCAP ディレクトリを追加	
	システムディレクトリ ローカルディレクトリ	1 0 1	ローカルユーザーディレクトリモ油加	Cope (アイレッイ シビビ加 / LDA / IWA 相当の Active Directory を追加 を クリックします
				Active Directory and mile 9990 as 9.



X	

4.			以下のように設定をし、[接続をテスト]をクリック
ディレクトリを追加			します。接続のテストに成功したら、[保存して次 へ]をクリックします。
ディレクトリ名	AWJPN		
	 LDAP 経由の Active 	Directory	
	Active Directory ((R)	合 Windows 認証)	ディレクトリの同期と認証
ディレクトリの同期と 認証	Active Directory から VM 択します。	lware Identity Manager ディレクトリヘユーザーを同期するコネクタを	同期コネクタ:設定したコネクタを選択
	同期コネクタ	esc.awjpn.lan 🔻	
	認証	このコネクタで認証も実行しますか?	ディレクトリ検索属性:sAMAccountName
		⊕ はい →	サーバーの場所:チェック
		0 L)L\Z	「バインドコーザーの詳細
	ティレクトリ検索問任*	sAMAccountName V	
		ユーザー名を含むアカウント間性を入力します。	ベース DN: アカワント検索を開始する DN
サーバの場所	DNS サービス ロケーシ は、このチェックボック ク ボックスを選択解除し	コン (SRV) レコードを使用して Active Directory ドメインを特定する/ スをオンにします。DNS SRV ルックアップを使用しない場合は、チ 、 Active Directory サーバホスト名と水ート番号を入力します。	バインド DN: アカウントの DN バインド DN パスワード: パスワード
	🖌 このディレクトリ は	: DNS サービス ロケーションをサポートします	
証明書	Active Directory で STAR CA 証明書を指定します。 いきます。各証明書が P 行が区切られていること	RTTLS 暗号化が必要な場合は、以下のチェックボックスを選択してル ルート CA 証明費が複数ある場合、すべての証明費を 1 つずつ追加 EM 形式であり、「BEGIN CERTIFICATE」と「END CERTIFICATE」 を確認してください。	
	このディレクトリに	は STARTTLS を使用するすべての投続が必要	
バインド ユーザーの詳 細	[ベース DN] フィールド(OU=myUnit,DC=myCorp アカウントを入力します す。	こ、アカウント検索を開始する識別名 (DN) を入力します。たとえば、 J.DC=com です。 FLインド DNJ フィールドには、ユーザーを検索でき 、たとえば、 CN=user1.CN=Users.OU=myUnit.DC=myCorp.DC=com	5 T
	N=X DN	cn=users,do=awjpn,do=lan	
	バインドロN*	cn=administrator,cn=users,dc=awjpn,dc=lan	
	バインドロNバスワー		
		Active Directory のバインド アカウント パスワードを入力します。	
		キャンセル 保存して次へ	
5.			連携させるドメイン情報が表示されていることを
ドメインを選択			確認し、[次へ]をクリックします。
LDAP 終由で Active Direct	ory を追加する場合、ドメイ ^ト	ノは自動的に選択されて下記に表示されます (チェックマーク付き).	
「メイン	*; CENT 2018 112412	- 100-1000-00-0001-001-001-00-0(1 10-00-00-00-00(1 エンススニン12旦)。	
awjpn.lan (AWJPN)			
×			-



ユーザー属性をマップ い場合は、ドロップダウンメニューから正しい喋性 には、[セットアップ]>[ユーザー蛋性] ページに移動 VMware Identity Manager の最性名 userPrincipalName userName lastName firstName email distinguishedName disabled domain employeeID	を選択します。必須喝性のリストを管理した わします。 Active Directory の雇性名 UserPrincipalName SAMAccountName Sn givenName mail distingulshedName UserAccountControl	 D、リストにない属性を追加する 必須 	に[objectGUID]を選択します。 [次へ]をクリックします。
場合は、ドロップダウン メニューから正しい 厚性 は、[セットアップ]> [ユーザー屋性] ページに移動 VMware Identity Manager の雇性名 userPrincipalName lastName firstName email distinguishedName disabled domain employeeID	を選択します。必須罵性のリストを管理したけ します。 Active Directory の届性名 userPrincipalName sAMAccountName sn givenName mail distinguishedName userAccountControl	 D、リストにない属性を追加する 必須 	[次へ]をクリックします。
VMware Identity Manager の定性名 userPrincipalName lastName lastName email distinguishedName disabled domain employeeID	Active Directory Ø 2014 243 UserPrincipalName SAMAccountName sn givenName mail distinguishedName UserAccountControl	 必須 	[次へ]をクリックします。
userPrincipalName userName astName irstName amail distinguishedName disabled amain amployeeID	userPrincipalName sAMAccountName sn givenName mail distinguishedName userAccountControl	 必須 	[次へ]をクリックします。
iserName astName irstName irstName iistinguishedName iisabled iomain imployeeID	sAMAccountName sn givenName mail distinguishedName userAccountControl	 · 必須 	
astName irstName irstName iistinguishedName iisabled iomain imployeeID	sn givenName mail distinguishedName userAccountControl	 必須 必須 必須 必須 必須 必須 必須 	
irstName mail listinguishedName lisabled lomain mployeeID	givenName mail distinguishedName userAccountControl	 必須 必須 必須 必須 	
mail istinguishedName isabled omain mployeeID	mail distinguishedName userAccountControl	▼ 必須	
istinguishedName isabled omain mployeeID	distinguishedName	▼ 必須	
sabled main mployeeID	userAccountControl		
omain mployeeID		•	
mployeeID	canonicalName	¥	
	employeeID	Ŧ	
bjectGUID	objectGUID	v	
hone	telenhoneNumher	•	
	前へ	キャンセル 次へ	
同期するグループを進択します。例: CN=us	sers.DC=example.DC=company.DC=com。ディレク	トリと同期する Active Directory	ます。
グループを選択します。グループを選択すると、 の使用資格がグループに付与されると同期されま	・グループ名がすぐに同期されます。 これらのグルー ます。	プのメンバーシップは、リソース	
✔ ネストされたグループ メンバーを同期			
		<i></i> <i>⇒</i>	ここでは AD 上に作成した 「airwatch」 という
グループ DN を指定 cn=aiowatch cn=users dc=awion dc=lan	すべてを 同期するグループ	⊳ +	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。
グループ DN を指定 cn=airwatch_cn=users_dc=awjpn_dc=lan	すべてを 同期するグループ 0/1 源代	₩ + × +	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ
グループ DN を指定 cn=airwatch,cn=users,dc=awjpn,dc=lan グループ DN	すべてを 同期するグループ 0/1 マップされたグループ	↓ ★ +	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし
グループ DN を指定 cn=airwatch,cn=users,dc=awjpn,dc=lan グループ DN	すべてを 同期するグループ 0/1 回訳 マップされたグループ	₩ + ★ +	ここでは AD 上に作成した 「airwatch」 というな ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。
グループ DN を指定 cn=airwatch,cn=users,dc=awijon,dc=lan グループ DN	すべてを 同期するグループ 0/1 第代 マップされたグループ	↓ + ★ +	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい
クループ DN を指定 cn=ainwatch,cn=users,dc=awjpn,dc=lan クループ DN の限するグループ DN を入力します。例 CN=use グループを選択します。グループを選択すると、 の使用資格がヴループに付与されると同時されま	すべてを 阿期するグループ 0/1 回訳 マップされたグループ ers_DC=example_DC=conn,ディレクト グループをがすぐに同時されます。これらのグルー? ぼす。	↓ ★ + × + 「Uと同期する Active Directory プのメンバーシップは、リソース	ここでは AD 上に作成した 「airwatch」というな ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。
グループ DN を指定 cn=airwatch,cn=users,dc=awjpn,dc=lan クループ DN の順するグループ DN を入力します。例 CN=use グループを選択すると、 の使用資格がグループに付与されると同時されま 1 グループが見つかりました:cn=airwatch,cn=use バループが見つかりました:cn=airwatch,cn=use	すべてを< 同期するグループ 0/1 回用 マップされたグループ ars.DC=sxample.DC=company.DC=com, ディレクト グループをがすぐに同時されます。これらのグルージ ers.dc=avijn.dc=lan	 ・ ・	ここでは AD 上に作成した 「airwatch」 というな ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。
クループ DN を指定 cn=ainwatch,cn=users,dc=awjpn,dc=lan クループ DN 同時するグループ DN を入力します。例 CN=use グループを選択します。グループを選択すると、 の使用資格がグループに付与されると同時されま 1 グループが見つかりました: cn=ainwatch,cn=use グループを検索	すべてを 阿期するグループ 0/1 回訳 マップされたグループ ers,DC=example,DC=company,DC=com, ディレクト グループ名がすぐに同期されます。これらのグルー: ers,dc=avjpn,dc=lan	↓ ★ + →リと問題する Active Directory プのメンバーシップは、リソース	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリック(す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。
グループ DN を指定 cn=airwatch, cn=users, dc=awjpn, dc=lan グループ DN	すべてを 同期するグループ 0/1 マップされたグループ	₩ + ★ +	ここでは AD 上に作成した 「airwatch」といき ープの DN を指定しています。 [グループの検索]をクリックし、対象のグル- 表示された後、[選択」をクリックします。
クループ DN を指定 cn=aitwatch.cn=users,dc=awjpn,dc=lan クループ DN 回照す <u>る</u> グループ DN を入力します。例 CN=use	すべてを 阿期するグループ 0/1 回訳 マップされたグループ es_DC=example_DC=company,DC=com, ディレクト	↓ ★ + ↓ ↓と問題する Active Directory	ここでは AD 上に作成した 「airwatch」 という? ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい
グループ DN を指定 Cn=airwatch,cn=users,dc=awjpn,dc=lan グループ DN 同時するグループ DN を入力します。例 CN=use グループを選択します。グループを選択すると、 の使用負化グループでは与れると同時されま 1 グループが見つかりました。cocabustch arguments	すべてを 阿期するグループ 0/1 回訳 マップされたグループ ers.DC=example.DC=company.DC=com, ディレクト グループをがすくに同期されます。これらのグルー; す。	↓ ★ + →リと同時する Active Directory プのメンバーシップは、リソース	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。
クループ DN を指定 cn=airwatch,cn=users,dc=awjpn,dc=lan クループ DN の限可 5 クリープ DN を入力します。例 CN=use クリープを避けします。クリープを選択すると、 の使用資格がグループに付与されると同時されま 1 グリープが見つかりました: cn=airwatch,cn=use グリープを検索	すべてを 阿期するグループ 0/1 回訳 マップされたグループ ers.DC=example.DC=company.DC=com, ディレクト グループ名がすぐに同期されます。これらのグルー? ers.dc=avipn.dc=lan	↓ ★ + ↓と同期する Active Directory プのメンバーシップは、リソース	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリックし す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。
クループ DN を指定 cn=ainwatch,cn=users,dc=awjpn,dc=lan クループ DN の開するグループ DN を入力します。例 CN=use グループを選択します。グループを選択すると、 の使用資格がグループに付与されると同期されま 1 グループが見つかりました; cn=ainwatch,cn=use グループを検索	すべてを 阿期するグループ 0/1 回用 マップされたグループ ers.DC=example.DC=company.DC=com, ディレクト グループ名がすぐに同期されます。これらのグルー? ers.dc=awjon.dc=lan	↓ ★ + -リと同時する Active Directory プのメンバーシップは、リソース	ここでは AD 上に作成した 「airwatch」 という ープの DN を指定しています。 [グループの検索]をクリックし、対象のグループ 表示された後、[選択] をクリックします。 対象のグループにチェックし、保存をクリック(す。 同期するグループが 1/1 となり、選択されてい ことを確認したら[次へ]をクリックします。



に進めます。
に進めより。
福を亦再し.
柳之友丈し、
-ザーはまだ
クすること



11. ディレクトリタ) ディレクトリ () ディレクトリタ やび ドメイン NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウスト-ブ NEKAウストーブ トン・シート 5.335ムディレクトリ ローク55 ディレクトリ 1 0 1 AKSN LDVP REDCASed Dealay 1 1 0 2016641113449	同期が完了すると、最終同期の時刻および緑のチェ ックが表示されます。 このタイミングでは、グループ内のユーザーはまだ 登録されていません。したがって、同期済みユーザ ーは0となります。
12.	[ユーザーとグループ / グループ]の順にクリック します。同期したグループをクリックします。
13.	[ユーザー]を選択し、[更新して同期ステータスを 表示]の更新をクリックします。
Image:	[ID とアクセス管理 / 管理 / ディレクトリ]をク リックし、同期済みユーザー数が 1 となっている ことが確認できました。 [ユーザーとグループ / ユーザー]をクリックし、 同様にグループ内のユーザーが登録されているこ とが確認できます。
ユーザー 6.7 エーザー 10 ドネイン ダイレクトリ 100 mark hordy E228年 グルー スター 2ス ユーザー 6 ユーザー 6 ドネイン ダイレクトリ NA ALL UERS R1 A dome hordy E228年 9 ALL UERS R1 A sequent Shire) sequent appendix AUUPEN 4-017201027428 anvestingSequentian, ALL UEES 1918	

mware[®]



2.3.5 Identity Manager 上でのアウトバウンドモードの設定

Identity Manager 上でアウトバウンドモード (ESC に固定グローバルアドレスを付与する必要がない構成)の設定を行います。

1. ************************************	20000 0.6 2000 2000 2000 2000 2000 2000 2000 200	2 2	Identity Manager の管理コンソールへアクセス し、[ID とアクセス管理 / 管理 / ID プロバイダ] の順にクリックします。 タイプが組み込みの ID プロバイダ名をクリックし ます。本書では[System Identity Provider]です。
2. (IPP UZHI CRS Deptem loanty Provider 9 (7) IBNUH Zy-92 (BD IPP CRS Provider 9 (SP 200)	10 プロルイタ& ユーザー ネットワーク 回転方法 コネクタ	System Identity Provider Colors Baller, Callage Callage, La To U, X, Ic. to Sa Milling Raser, Lo N-U Joo Baller, La To U, X, Ic. to Sa Milling Raser, Lo N-U Joo Baller, La To U, X, Ic. to Sa Milling Raser, La To U, X, Ic. t	以下の設定をします。(次項に続く) ユーザー:システムディレクトリからチェックを外 し、ドメインを選択 コネクタ:設定したコネクタをドロップダウンリス トから選択し、[コネクタを追加]をクリック
3. 	✓ ESC_AWJPN (esc.awj コネクタを追加	pn.lan) ★ 高可用性 (HA) のために追加のコネクタを選択できます。(コネクタを追加) ペ ージでコネクタのアクティベーションコードを作成して、コネクタをセットア ップし、この ID プロノイダ用にそのコネクタを選択してください。 重要、高可用性を確保するには、各コネクタに同じ認証方法が設定されている 必要があります。	以下の設定をし、[保存]をクリックします。 コネクタ認証方法:パスワード(クラウドデプロイ) にチェック 以上でアウトバウンドモードの設定は完了です。
コネクタ認識方法 KDC 証明書のエクスポー ト	認証方法 パスワード (クラウドラ ロイ) 証明書をダウンロード モバイルデバイス管理プロ	23延方法を関連付ける デプ	
	す。 <i>保持</i> キャンセ	וו	



2.3.6 AirWatch と VMware Identity Manager の統合

AirWatch と VMware Identity Manager の間での REST API 連携を構成します。API 連携することでユ ーザ情報の同期だけでなくアプリケーションカタログの統合やデバイスコンプライアンス認証などが構 成可能となります。

はじめに AirWatch 上に REST API 連携の設定を追加します。

1. SURA Laca: 2.5070 2.50707 2.507	DSD-1 HRURE 3 A* 3 EST API 0	 AirWatch コンソールで[グループと設定 / すべての 設定 / システム / 高度な設定 / API / REST API]を 開きます。 [API アクセスを有効化]を有効に設定します。 API キーを追加します。 サービス名に[<i>Identity Manager Admin</i>]、アカウ ントタイプに[管理者]、API キーは自動生成のもの をそのまま使用してください。
		(API キーをメモ帳などにコピーします。)
2		API キーを追加します。 サービス名に[<i>Identity Manager User</i>]、アカウン トタイプに[加入ユーザー]、API キーは自動生成の ものをそのまま使用してください。 (API キーをメモ帳などにコピーします。) 完了後、[保存]をウリックします。
3.	 > ユーザー > ユーザー グループ > ローザー グループ > 空間者 > フィルタ → ● 追加 ● ① バッチィンボート フィルタ → ○ ゴッチィンボート ローザー 管理者グループ 管理者グループ 管理者グループ 管理者グループ 管理者交遍加 ●時的な管理者を追加 	[アカウント / 管理者 / リスト表示]を開き、[追加 / 管理者を追加]をクリックします。



4.	ユーザ名に[IdentityManager]、その他の必須項目
管理者を追加/編集 🛛 🔘	を仕息に設定します。
ペーシック 詳細 役割 API メモ	
ユーザータイプ ペーシック ディレクトリ	
⊥− <i>J</i> − <i>E</i> * IdenctγManager	Tip :
	共有 SaaS をご利用の場合は、すでに別テナントにて
	"IdentityManager"や"IdentityManager1"などが使
2002ゲンタにパイノートな天宅の 有助 無効	用されている場合があります。こちらは管理上の名前
% * Identity	バマオので任音の右の (IdentityManager テナント
N COPPE AN INC.	
EX=)/J7FLZ* IdentifyAnater@wso.ian	名)などを指定してくたさい。
タイムゾーン* (GMT-09:00)日本	
ロケール* [apanese (apan)(日本語 (日本1) *	
最初のランディング画面* デバイス > ダッシュボード Q	
> 二表面如此力式.	
> 通知	
保行 キャンセル	
	[役割]タフに移動します。
管理者を追加/編集 😜	
ペーシック 評細 役割 API メモ	組織グループに最上位の組織グループを選択します。
● 総務を追加 ● 総務を追加 パスコード	役割に[Console Administrator]もしくは
ktuda Q. Console Administrator Q.	「AirWatch Administrator]を選択します。
6.	[API]タブに移動します。
管理者を追加編集 🛛 🔘	
ペーシック 拝場 役割 API メモ	「 証明書]を選択します。
	証明書田のパフロードを設定します
E研細の/(スワード	
	[保仔]を美行します。
	- セキュリティ暗証悉号が求められた堪合け - 事前に設
制限された操作 - 制限されている管理者パスワード変更アクション 〇	こう エラク うら 日本 日本 ラガス ひつう し この 日本 () 手がに し 定した 暗証番号を入力します。
制限された操作・制限されている管理者パスワード委更アクション 調度されている管理者パスワード委更アクション	定した暗証番号を入力します。
制限された操作・制限されている管理者パスワード変更アクション 制限されている管理者パスワード変更アクション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 番号を入力して結行してください。	定した暗証番号を入力します。
制限された場件・制限されている管理者パスワード変更アクション 制限されている管理者パスワード変更アクション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 番号を入力して統行してください。 6 8 8 8	定した暗証番号を入力します。
副限された場件・動限されている管理者パズワード変更アクション ■開設されている管理者パズワード変更アクション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 番号を入力して移行してください。 6 5	定した暗証番号を入力します。
副限された場件・制限されている管理者パスワード変更アクション 制限されている管理者パスワード変更アクション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端証 番号を入力して統行してください。 ① 8 8 ドメールアドレス メイン電影響	定した暗証番号を入力します。
副限された場件・動限されている管理者パスワード変更アクション 制限されている管理者パスワード変更アクション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 番号を入力して統行してください。 ○ を 提 ビールフドレス メイン電話時 セキュリティ暗証番号:	定した暗証番号を入力します。
	定した暗証番号を入力します。
図記された場件・細胞されている管理者パスワード変更アクション MRごされたいる管理者パスワード変更アクション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端証 番号を入力して統行してください。 6 8 1	定した暗証番号を入力します。
■限されている管理者パスワード変更アクション必要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端証 着きを入力して続けしてください。 ① を と、ルンドレス メイン電話時 セキュリティ解証[音号: ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	定した暗証番号を入力します。
	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで聞きます
	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。
	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。
MR2はれている管理者パスワード変更アクション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端証 書きを入力して続けしてください。 ① g g	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。
創業された場件・場構されている管理時パスワードを使アクション/見使を供行しようとしています。以下のすべての情報を確認したからセキュリティ確認 書きと入して体行してください。 () #	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。
WRATICLE Refit - UMRLATICLUS 管理的/CCO - Fegur POSelo / Communication - Control - Communication - Control	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。
Watch Leget 1, Cup - Keep Popsa > Alge explosible Cup is a kino port confide effective or the set of	定した暗証番号を入力します。 編集アイコンをクリックし、作成したユーザを再度編 集モードで開きます。



8.			[API]タブを開きます。
管理	曾理者を追加/編集 		
/	ペーシック 詳細 役割 API	XŦ	ユーザ作成時に設定した証明書のパスワードを入力し
1	認証*	ペーシック ディレクトリ 調算者 ①	て、[クライアント証明書をエクスポート]を実行し
9	発行者	Ol-6134.IdentityManager_kbaba	ます。
*	有効期限開始日	2018/04/12.9.50	(証明書のダウンロードが閉始されます)
*	有効期限終了日	2038/04/07 9:50	(証明書のタワンロートが開始されます。) [保存]を実行します。
t	サムプリント	1DD179F77EC42699427AB809B663DB8020B88A55	
		クライアント証明書を消去	
1	臣明書のパスワード		
		クライアント証明書をエクスポート	
		<i>離れ</i> キャンセル	

つづいて VMware Identity Manager 上で API 連携設定を追加します。

AirWatch AirWatch の構成	AirWatch を VMware Id 設定を構成したら。[6年 ションを有効にできた] AirWatch API URL* AirWatch API 証明書* 証明書/(スワード* AirWatch 管理用の API キー* AirWatch 管理用の API キー* AirWatch グルーブ ID* ドメインを複数の組織 グループにマップ	ntly Manager と逆病するよう ArWatch 設定を構成します。 1 をクリックします。それから ArWatch ごその他の包括オブ * https://as138.awmdm.com/ ArWatch API の URL を入力します。 道明書をアップロード 証明書の詳細を表示 API コールに使用する ArWatch .p12 証明書をアップロード はま。 	 アクセス管理 / セットアップ / AirWatch]を き、以下の設定を行い[保存]をクリックします AirWatch の構成 AirWatch API URL : AirWatch 環境の AP –バのアドレスを入力。 CN504 の場合 : https://as504.awmdm AirWatch API 証明書 : 前項目で作成した調書をアップロードし証明書のパスワードを力。 AirWatch 管理用の API キー :
建金有点口灯	保存		Identity Manager Admin の API キーを入
統合カタロク	 (※合力タログに組み入れま ③ 有効 ◎ 無効 (※存 	く、ArWeaton パンロンロンビュンヨンセットアップを読 す	・AirWatch 登録ユーサー用の API キー: <i>Identity Manager User</i> の API キーを入力
コンプライアンス チェ ック	 コンプライアンスチェッ< 管理対象デバイスが進行 ● 有効 [®] 無効 保存 	v夕を有効にして、AirWatch のコンプライアンス ポリシーを しているか確認します。	・AirWatch グループ ID:利用中の AirWatc 最上位組織グループのグループ ID を入力。
			「保存」を実行。





		続いて以下の設定を行います。
	<i>filti</i>	統合カタログ・有効
統合カタログ	統合カタログを有効にして、AirWatch カタログのアプリケーション セットアップを統合カタログに 組み入れます	
	● 有効 ◎ 無効	「 保存 〕を実行。
	發行	
コンプライアンスチェック	コンプライアンスチェックを有効にして、AirWatch のコンプライアンスポリシーを管理対象テバ イズが潜守しているが確認します。	
	◎ 有劝 ● 無効	
	保存	
AirWatch によるユーザー	ArWatch によるユーザーのパスワード問題を有効にします。	
OU (X)-Fishe	◎ 有効 ● 無効	
	發行	
AirWatch によるユーザー の外部アクセス トークン沼	AnWatch によるユーザーの外部アクセス トークン統語を有効にします。	
a a	◎ 有効 ● 無効	
	6477	



3 ディレクトリユーザを使用したパスワード認証の構成

3.1 本章のゴール

本章では、Active Directory の認証情報を使用した認証(Active Directory のユーザ ID およびパスワードを入力する認証)を構成します。この認証タイプは主にブラウザーベースでのアクセスや AirWatch で管理していないデバイスでの認証などに使用されます。

3.2 設定手順

1.	Int Interference	VMware Identity Manager コンソールで[ID と アクセス管理 / 管理 / ポリシー]を開き、 [default_access_policy_set]をクリックしま す。
2.	Ale na su de la constante INTE Managementaria Managementari	[編集]をクリックします。
3.		ポリシーの編集画面の定義タブで、そのまま[次
ポリシーの編集 ② 2章 ③ wa ③ サマリ	TORN-FMUS-ENERGY CEC25UrCTSD1973n/L+MUS-AONERS: FACOD7UD-20 × LERRACH, WANKAGO OK C270UZ78974C02-UF-OMECEWE924839880/90127, WZ 2019-523-AD794UZ48898858731UFMA: (1-43794UZ, 4902-54802, 157, 4800750) 2019-2012832-UF-9794UZ488985730-UF-WAN:-EHROLFS, 4800750 2019-2012832-UF-9794UZ488985730-UF-WAN:-EHROLFS, 4800750 eHrolt Access pologise EMR ● Q17709-505	へ]をクリックします。
	キャンセル 次へ	







4.		サマリタブで[保存]をクリックします。
ポリシーの編集		
📀 28	定義	
	名用 default access policy set	
9 max	20月 Default access policy set	
S 120	アプリケーション 0 アプリケーション	
	構成	
	ポリシー・バール・1 ユーザーのネットワーク細胞が ALL RANGES である場合	
	ユーザーが Web プラウザ からコンテンツにアクセスしている場合 ユーザーはグループ すべてのユーザー に思しています	
	ユージーはアメジェト (ジラント・テンドイ)を安用して18日を行うことかできます 各時間後に間応証します	
	ポリシールールコ ユーザーのネットワーク範囲が ALL RANGES である場合 ユーザーが Workspace ONE アプリ からコンテンツにアクセスしている場合	
	ユーザーはグループ すべてのユーザー に関しています ユーザーは Password を使用して和話を行うことができます	
	フォール(シク方法): パスワード(ローカルディレクトリ) 2448 addmin_mitres(1,4) オ *	
	4+>20/ 8A 60	
5.		任意のブラウザで Workspace ONE のポータルに
		アクセスします。
		(https://<テナント>.vmwareidentity.asia)
	Workspace ONE"	フルタワンメニューで設定した Active Directory
		ドメインを選択し[次へ]ボタンをクリックしま
	ドメインを選択します]
	awjpn Jan 🔻	
	<u>次</u> へ	
	vmware:	
6.		Active Directory のユーザ名とパスワードを入力
		して[ログイン]ボタンをクリックします。
	0	
	Workspace ONE"	
	Workspace ONE"	
	Workspace ONE"	
	Workspace ONE" ユーザー名 sagawa1	
	шонкрасе ОКЕ" <u>2-17-8</u> <u>зарама1</u> /(777- Б	
	Z−tf-& sagawa1 JC7.27 - K	
	ユーザー名 sagawa1 バスフード 	
	エーザー名 sagawa1 アCRフード 	
	ビジート コーザー名 sagawa1 アスワートド 	
	レビデン シンティン・シントン シンティン・シントン シントン・シントン・シントン・シントン・シントン・シントン・シントン・シントン	
	レビステレビ レビットロック シント・	
	レビアレント ユーザー名 agawa1 ノフワートド 	
	レビアレン Control Contro	
7	レビード ユーザー名 agawa1 ノバスワートド 	
7.	レビード A agawa1 アスワード Avijnlan ログイン パスワードを忘れた場合 別のドメインに変更	Workspace ONE のポータルへ AD のアカウント
7.	していていたいでは、 していていたいでは、 たいで たいで たいでは、 たいでは、 たいで たいで たいで たいで たいで たいで たいで たいで	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	していたいではないではないではないではないではないではないではないではないではないではな	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	していていたいではないではないではないではないではないではないではないではないではないではな	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	стори Contracting the contr	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	exact exact exa	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.		Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	example a constraint of the second seco	Workspace ONE のポータルへ AD のアカウント でログインができました。
7.	exact a sequence of the sequence o	Workspace ONE のポータルへ AD のアカウント でログインができました。
7 .	exact set of the set	Workspace ONE のポータルへ AD のアカウント でログインができました。





4 iOS デバイス用モバイル SSO の構成

4.1 本章のゴール

本章では、iOS デバイス用にモバイル SSO を構成します。モバイル SSO は Secure Application Token System(SATS)と呼ばれる証明書ベースの認証方式を使用することで、ユーザは認証情報の入力をする ことなく各種 WEB アプリケーションやデバイスにインストールされたアプリケーションに SSO が可能 となります。

iOS デバイス用のモバイル SSO では Kerberos 認証を使用しており、AirWatch からデバイスに配布さ れるシングルサインオンプロファイルによって制御されます。



4.2 設定手順

はじめに iOS モバイル SSO 用の認証アダプタを構成します。

1.		AirWatch コンソールで[グループと設定 / すべ
 > システム はじめに ブランディング > エンタープライズ統合 エンタープライズ統合サービス 変更局 ViAware Enterprise Systems Connector ディレクトリウービス 	システム > エンタープライズ統合 VMware Identity Manager ③ サーバ この編成グループにあるディレクトリを VMware Identity Manager と同時させることができます。これにより、VMware Identity Mic. この編成グループでたあるディレクトリを VMware Identity Manager と同時させることができます。これにより、VMware Identity Mic. この構成プループを支払	ての設定 / エンタプライズ統合 / VMware Identity Manager / 構成] を開く。 証明書から[有効化] をクリックします。
Eメール(SMTP) ・VbWare Tunnel ビアツービア サードパーティ製プロキシ SMS フルサービスインストーラ Syslog 動画 CDN リモート管理 ・VbWare Identity Manager 構成 アクセス管理	証明書 ArWeach 証明書プロビジョニングが Whare Identity Manager とモバイルシングルサインオンとともに使用できるようにします。 アダプタとの信頼を確立できるようにします。 育会化	



٦.			
Ζ.	-		証明書の内谷が表示されるので、 [エクスホート]
システム 「自じめに」 ブランティング ・エンタープライズ総合 エンタープライズ総合	システム)エンター VMware Ide	-79-(786 ≥ Intity Manager ©	をクリックし証明書をダウンロードします。
 2018日、 VMonre Foreprice Systems Convictor ディレクトリサービス じメールCMTPy VMonre Tarnel ビアワービア サードバーティロアコ キシ 	サーバ ――― この感染グループにま 愛があります。 「構成	まだいとういうは Novem Novem と 2011年まごとだされます。 このこうた、 Novem Novem Diagram TERNOF いうい 2018年10月できます。この公認定であるであるに、 この第ログループビディンクトンパルは主要者すると やういき者である。 後回し、後日記ではないてない、 メンジアグラムをならう 1000 イングリンジの研究できることができます。	
SMS ブルサービスインス トーラ Syslog	E98番	とジョニングゲ Vikuan Gento Vikuage とモドイバルングルダインオンとともに発見さきままってします。 このページの意外を回答者主なスポートして、Vikuan Gento Vikuager 回回アダプタとの意味を知定できるようにします。	
新聞 CDN リモート電理 * VMware identity Manager	1216.00	947 Ps. Richard 2160/11	
構成 アクセス管理 ・ セキュリアイ ヘルプ		म्रावा साम्राज्यम् 2016/04/13 77व	
 ローカリゼーション レポート 定期受信 利取扱的 		サムプリン - 54417C7864065G7#23850742388784234897051 ト	
- 第世な記念 - 第世な記念		±2008-+	
デバイスとユーザ			
3.			VMware Identity Manager コンソールで[IDと
97538-F = 3-9-296-3 7469FU DJ0869 1033	「 カタログ ・ 10 & 7 ク ード時間のPSスタント 2020	ana 0-5 0,2-5 - 50-7 30,2757-53788 8. б77-	アクセス管理 / 管理 / 認証方法]を開く。
1	Bみ込み ID プロバイダの I要 認証が出た見用にすると、3	構成力力法 この認力がありからなスポンシー ルール・アンロ連邦事業が必要用であたます。別の認知力を全面行するには、アクセスポンシー ルールを算用してください。	
	回転方法 ArWath 予想アクセストーク	## λ7=9λ · ·/· ·/·	
	デバイスコンプライアンス (A	man) / M0	[モバイル SSO (iOS)]行の構成ホタンを押す 。
	Villaam Verly		
	イスワード(ローカルディレク	р и и и и и и и и и и и и и и и и и и и	
	モバイル 550 (Android 勝) 巨球曲 (クラウド デブロイ)	2 80	
4.			[KDC 認証を有効にする]にチェックを入れ有効
			化。
KdcKerber	osAuthAda	apter	
KDC 認証を有効	効にする	✓	
		Kerberos をサポートするデバイスを使用したユーザー ログインを有効にします。	ルートおよび中間 CA 証明書 で [ファイルを選
11114		VMWAREIDENTITY.ASIA	択] ボタンをクリックします。
		このアダプタを使用した認証の実行に使用されるキー配布センター(KDC)のID。	
ルートおよび中 書	Þ뭼 CA 証明	ファイルを選択	
		連結 PEM ファイルを含む DER および PEM 形式の複数のルートおよび中間 CA 証明書をアップロードします。	ステップ2でタウンロードした証明書を選択して
アップロードさ	された CA 証	ファイルが選択されていません	アップロードし、[OK]をクリックします。
	ーする		
OC3F -E-HAM	290	」 証明書のオンライン証明書ステータス プロトコル (OCSP) チェックを有効にします。AirWatch CA などの OCSP	
		をサポートしない認証局には OCSP を選択しないでください。	
OCSP Nonce	を达信りる	ターCSP 要求に Nonce を含めることで、 レスポンス リブレイ 立般から履進します。	
OCSP レスポン	ンダの署名証	ファイルを選択	
明書			
OCSP レスポン	ッダの署名証	OUSP レスパンスへの差石に使用する証明音をアックロードします。 ファイルが選択されていません	
明書サプジェク	ト DN		
キャンセルメ	ッセージ		
		ユーザーの認証中に表示されるログインメッセージをカスタマイズします。	
キャンセル リン する	ンクを有効に		
		[キャンセル] を有効にすると、ユーザーはログイン ページで [キャンセル] をクリックして Kerberos 認証を停止	
エンタープライ	イズデバイス		
管理サーバのし	JRL		
		キャンセル 保存	
		認証アダプタの更新	
		ノアイルを確認およひアッフロートするには、[OK] をク リック してください。	
		5-12-1711. OK	





8.	Image: Control of the second	VMware Identity Manager コンソールで[ID と アクセス管理 / 管理 / ポリシー]を開き、 [default_access_policy_set]をクリックしま す。
9.		編集をクリックし、手順 3.2 と同様に、ポリシー
91048-1 + 3-9-428-7 8907 + 44270578 0-6 7-45910 0570577 7005180753951 2076 805	 A. Star for all highly defined and starting of the start of the start	ルールを追加します。
default_access_policy_set		
228 EX ideal_icent_play_ve	ant Default access particip rea	
775年-542 07795-565 発電		
ポント・レード コーダーシャントワークを取りたしてアンジスプログロントを使き コーダーゼ やみ プログロ からしてアンジスプログロントを使き コーダーゼ やみ プログロ からしたし いました いまし オーダール スロン・ドウンター かんか とをかたし いました かたらから を使うたいため	All μ = 4×3 Δ = 4×30 ± 100 ±	
(1)しーレーム3 11:4 ⁻¹ -0 ¹ -0		
ポリシーの編集		
28	単沢したアプリケーションへのアクセスに加するルールのリストを特成できます。ルールごとに、ドネットワーク範囲、アプ リケーションにアクセスできるデバイスのタイプ、認証力法、再認証表でにユーザーがアプリケーションを使用できる最大時 感音を選択した。	
(4) 構成	ネットワーク範囲 デバイスタイプ 認証 再認証	
🖉 ਸੁਣਮ	ALLRANGES Web プラウザ パスワード(クラウドデ 8時間 × ************************************	
	: NLI RAVINES INVORSIDATE VICE 7275 FIRSTWORTE 1 2100 Html ** : ALL RANCES Web プラウザ Password+1 8 時間 **	
	 (6) ポリシールールを追加 	
	キャンセル 個へ 第へ	
10.		以下の設定を行い[保存]をクリックします。
< 構成	ポリシールールを追加	
* ユーザーのネット	マーク編明が彼の場合 ALL RANGES 🗸 🔍	・[ユーザーのネットワーク範囲が次の場合]:
 ユーザーが次からコンテン また、ユーザーが次の 	29%79/tz758@d 105 v	ALL RANGES
	ペクルーフを選択 グループが継択されていない場合、ルールはすべてのユーザーに運用されます。	
この) - ユーザーは安泰州田にア ¹	ダクションを実行します 以下を認証に使用	・[およびユーザーのコンテンツアクセス元が次の
先の方法が失敗するが適用で	th/1/1/2 SUUUS 100 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	場合]:iOS
	④ フォール/シク方法を追加 PASEまでの時期時間 時間 ●	・「次に 以下の古法を庙田」ア羽証オスマレギズ
		・[次に、以下の方法を使用して認証することがで きます]・モバイル SSO (iOS 版)
	キャンセル αカ	





11.							作成したポリシールールを最上部にドラッグアン
ポリ	シーの編集						ドドロップします。[次へ]をクリックします。
🥑 定義	8	違択したアプリケーション^ リケーションにアクセスでき 閣数を違択します。	、のアクセスに願するルールのリン きるデバイスのタイプ、認証方法、	ストを作成できます。ルールご 、再認証までにユーザーがアプ	とに、IP ネットワー リケーションを使用	-ク範囲、アプ できる最大時	TIP :
⊘ 横剑	R	ネットワーク範囲	デバイスタイプ	872E	再認証		ポリシールールは上段のものが優先されます。 複
। I I I I I I I I I I I I I I I I I I I	Ų۶	ALL RANGES	IOS	モバイル SSO (IOS 版)	8 時間	×	教の認証ポリシーを構成している場合は要件に合
		ALL RANGES	Web ブラウザ	バスワード(クラウドデ	8 時間	×	
		ALL RANGES	Workspace ONE アプリ	Password+1	2160 時間	×	わせて優大度を調整し、適切なホリンールールを
		ALL RANGES	Web ブラウザ	Password+1	8 時間	×	構成してください。
		● ポリシー ルールを追	ta				
12.				[キャンセル 着	× ×	[保存] をクリックします。
	ポリシーの編集						
	🥝 注幕	定義					
	O 1810	名相 default_access_policy_set					
	Ĩ.	28배 Default access policy set					
	0 טעדע	アプリケーション 0 アプリケーション					
		構成					
		ポリシールールト コーザーがの5 かうつう コーザーよりの5 かうつう コーザーは でんてあ 550 ポリシールール2 コーザーは でんてみ 550 ポリシールール2 コーザースタットラークコ コーザースタットラーク コーザーは パンマット (ク 6 時間に「同辺正します 8 時間に「同辺正します	国がALENNAG5である場合 シジニアジセスしている場合 ロンザーに買いています の05 節を使用して詳細を行うことが 調加がALENNAG5である場合 からコンテンジニアクセスしているす の3 コンテンジニアクセスしているす の3 コンテンジニアクセスしているます	「できます 商店 フラごことができます			
				キ ヤ:	地に前へ	6844	



つづいて A	AirWatch	のデバイスポ	リシーを	使用してシン	·グルサインオン構成をデバイスに配布します。
13. У 3925 У 3925 У 3925 У 3925 У 3927 У 3977 У 3977	aボード デバプ 新示 フィル サイクル フィル マイルとリソース マイルとリソース マイル マイルとリンース (第) ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	イス > プロファイルとリソース > コファイル タ 、 追加 ・ プロファイル プロファイルを追加 プロファイルを追加 プロファイルをアップロー パッチィンボート	管理元 - F AirWa	: ch Internal	AirWatch コンソールで[デバイス / プロファイルとリソ ース / プロファイル]を開き、[追加 / プロファイルを追 加]をクリックします。
14.					[iOS]をクリックします。
フロファイルを追加					
7591774-688	iOS	macOS	tvOS		
	ADDIN KO		Appu rico	Buckberry	
BlackBerry 10	Tizen	Windows 超久控制化	Windows	Chrome CS ((,/)>)	
15.					[全般]ペイロードで以下を設定します。
iOS WYUUN Apple iOS フロ	コファイルを追加			0	
● ±秋 ④,/C□−ド ④剤陽	全般				名前: Mobile SSO iOS
中WER 曲 VPN 曲でメール	/(-582	1			割り当てるグループ: All Devices(テナント名)
El Exchange ActiveSync 画道和 回しにAR	88	軍項北急			
回 CalDAV 回 ZARDAV 回 定時配載カレンダー	制造したり	市場 いつでち	*		
 Web クリップ 単 前均体理 12 2010 	軍車た 割り当てるグループ	Raba	*		
↔ SCP © グローバ5xHTPプロギ © シングルフプリモード	1875	ことに入力してクループを追加 いいえ はい	5 <u>4</u>		
○ コンデンジフィルタ Q 管理ドメイン D 2 × トロークは空間相	遺物の割り当て条件	デバイス部り当て表示 ■ 離死したエリア内のデバイスのかにインストール ①		Again 11 DM	
の marcos サーバクカウン に シングルサインオン	Wites	目 スケジュールを有効にし、違民した時間等のみインストール YYYYYMM00			
G AirRay ミラリング 毎 AirPrint					
		都参して公開 キャンセル			
16.					[資格情報]ペイロードをクリックし、[構成]をクリックし
IOS WILLIN Apple IOS	フロファイルを追加			•	ます。
0,1/3⊐−F © NR					
島 VPN 画 Eメール 11 Exchance ActiveSers		19.00.00			
III III III III III III III III III II		機成			
ー ② 泡用和加速カレンダー 団 CardDAr 当: Web グリップ					
● おかれを ++ SCEP のグローノしんTEPプロを	·				
 ⇒>>グルアプリモード ⊘ コンテンジフィルタ 					
 会 管理ドメイン 会 ポットワーク市和要点 会 rac05 サーバアカウン 					
ト ロシングルサインオン 口 AitFlay ミラリング					
 ● セレラー 		886.0008 345.000.			





vmware[®]







Workspace ONE App for iOS を構成します。

23.	700-5435 またまで 770-5435 770-5435 770-5438 770-5458	7719-543 3 20 8.3.6 56 7275-54-548 56 7275-54-548 56 7275-54 56 7275-54 57 7275-57 57 7275-54 57 7275-54 7275-575-575-575-575-575-575-575-575-575	8 8 -337-08 Bisettu •	AirWatch コンソールで[アプリとブック / アプ リケーション / ネイティブ / パブリック] を開 き、[アプリケーションを追加]をクリックします。
24.				以下のとおり設定を行い、[次へ]をクリックしま
アプリケ	ーションを追加		0	す。
	管理元	kbaba_poc		
	ブラットフォーム*	Apple IOS v		プラットフォーム:Apple iOS
	2-人	アプリストアを映着 URL 入力 Workspace ONE		 ソース : アプリストアを検索
				名前:Workspace ONE
		次八 年92世纪		
25.				VMware Workspace ONE の横の[選択]をクリッ
検索			Norkepace ONE III HIL	クします。
0	VMware Workspace ONE concessed agrows フリー・ カテゴリ: Business 現在のバーション32 家家家家	The Vibeas Winkspace ONE gas for COT makes te any tax across your digat interstates times your hitmans or Anifer any instruction. Usey your present presentation to strate and gas range in gas and across the your arrays. "REATING UNKERS DAY CORDUCT Makes' Winkspace ONE provide sector compare acceleration to be more acceleration of acceleration of the sector compare acceleration to be more acceleration and additional to our springbared. ONE 10001 SMPLCITY labels one set of	0 80	
N	Notion - Notes, Tasks, Wiles フリー カアゴリ: Productivity 戦略のパージョン:1.2 音音音音音	resons are all in-one workspace for your netex, cask, while, and databases. ¹⁴ Apple App of the Day **** V80 provides reviews: "are remoistence app", "sub-to meet for spaceres apps, near 4.4 in Instant" **A Youth Their Kenner with Ski oponesis. It is the perfect pairing to the database paper traverse momental for oper of the your DABA CORE DTL to an upp & equar Sforia Touchs to arrange any contact. Great for prioritizing test and to due. RCM MEDAK Supports images, to due.	O RR	
	Team-One reconstruction app v2 フリー カテコリン Business	Team-One is more than messaging it's teamwork made simple. Of course, you can that hat there is so much more. Say possible teambers searching between apps and help to a simpler way to work. Team-One you provide a course mode post everyting put seam meets the bears relationstation is one place. Write them One wells manage all your and in one place to post on the seam states. Team one states will write them One wells manage all you main in one place to post one be another than the manahese another and one and one state (seam states in seam of the means. Team-	0.107	
	場合のパージョン333 VMware Vertly	Description provide from tages, and the second seco	0 m	



26.	[保存して割り当て]をクリックします。
シンジンジンジンジンジンジンジンジンジンジンジンジンジンジンジンジンジンジンジ	
IFIB XUBBUT SOK	
K 5.6° Weber Works ○ App form CollBit	
Py2t-#	
カデゴリ カデゴリを細叶するには入力を統領 ①	
MSモデル (Pad ()) (Phone (Pd Bach	
9×7 39429+00	
Water Mondays	
27.	[目り当ての追加]をクリックします。
VMware Workspace ONE - 割り当てを更新 🔹	以下の設定を行います。
割り当て 除外 デバイスは、次の場応に第ついてアプリを受信します。	
デバイズが全部のグループに対応している場合。 低れ度が会も高い(0)が最高低れ度) グループのボリシーを支張します。 ① 割り合ての始始	割り当てグループを選択:All Devices(テナント名)
24回 単元田 アンリム協力法 軍用別後のシクセス 加入転用時に相当 アンリターションのハックアップを含く VPNアクセス 構成を法成する 軍権を代す	アプリ配信方法:自動
レコードが見つかりませんでした	 管理アクヤス・有効
VMware Workspace ONE - 割り当ての追加 ×	アノリケーション構成: 有効
m / a い / A い Bokes (stagg) とこに入力してグループを活動	以下の2行を記述する。
7796億万法* 自動 オンデマンド ()	構成キー:AppServiceHost
#U9	値のタイプ:文字列
★取る管理レベル: 管理・クロス デバイスの管理に基いて、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。	構成値:
データ憲法防止 (DLP) を有効化しますか?	https://<テナント>.vmwareidentity.asia
11日アクセス. 有助 無助 ①	
アプリケーションの(シクアップを除く 有効 気泡 () ユーザーがインストールしたアプリを 有効 気泡 ()	値のタイノ:文子列
MOM 世間対象にする アプリトンネル 有効 素加 〇 05570	構成值:{DeviceUid}
アプリケーション現成 戦後 戦後 〇〇	
XMLをアップロード ① ① ニーザー用のアブリクーション構成に労用するキーと協めペアを入力	[追加]をクリックします。
アプリケーション構成 構成キー 道クイブ 構成道	
AppServiceHost 文字列 ・ https://stagir/umwaredentity.ssia X O 参照像を得入 DexiceUDD 文字列 ・ (DexiceUd) X O 参照像を得入	
2日 キャンセル	





4.3 iOS デバイスで動作確認

iOS デバイスを使用して動作確認をします。

* この手順は当該 iOS デバイスが AirWatch に正常に管理されている状態(加入状態)を前提としております。iOS デバイスが加入状態でない場合は加入操作の完了後に実施してください。





3.		iOS デバイスで Workspace ONE App を起動しま す。
		アプリ配信方法を自動に設定しているため、 AirWatch から自動でインストールされます。
	Workspace	
4.	15:18 🗔 🖗 81	VMware Identity ManagerのURLが自動的に設 定されていることを確認し、[Enter]をタップしま す。
	Workspace ONE"	
	https://shinjisagawa.vmwareidentity.asia	
5.	S S Workspace ONE	モバイル SSO により、認証情報の入力をすることなくログイン処理が行われることを確認します。
	ログインしています 資格情報を認証しようとしています。	
	vmware:	
6.		[入力]をクリックします。Workspace ONE アプ リでも同様にモバイル SSO でログインできること が確認できました。
	ワークスペースが準備できました。 入力	







5 デバイスコンプライアンス認証の構成

5.1 本章のゴール

本章では AirWatch のデバイスコンプライアンスのステータスを認証に使用するデバイスコンプライア ンス認証を構成します。

この機能を使用することで、デバイスが企業の設定したセキュリティ規準に準拠しているかどうかを評価した上での認証可否判断や、企業が使用を認めていない管理外デバイスからのアクセスを遮断するなどの要件に対応することができるようになります。

本章の手順では、前項までで構成した Workspace ONE のポータルへの認証時に使用している iOS 用モ バイル SSO 認証にデバイスコンプライアンス認証を追加します。

5.2 設定手順

前項までに構成した iOS 用モバイル SSO 認証にデバイスコンプライアンス認証を追加構成します。

1. 1990;	利用条件 AirWatch	識定 保存			VMware Identity Manager コンソールで[ID と アクセス管理 / セットアップ / AirWatch]を開 きます。	
	統合カタログ	統合カタログを有効にして 組み入れます ● 有効 ◎ 無効	こ、AirWatch カタログのアプリケーシ	ヨン セットアップを読合カタログに		以下の設定を行い、[保存]をクリックします。 コンプライアンスチェック:有効
	コンプライアンス チェック	コンプライアンス チェッイ イスが適守しているか確認 ③ 有効 ◎ 無効 保存	フを有効にして、AirWatch のコンブラ します。	イアンスポリシーを管理対象デバ		
	AirWatch によるユーザー のパスワード課題	AirWatch によるユーザーの © 有効 ® 無効 保存	D/ (スワード認証を有効にします。			
2.						[ID とアクセス管理 / 管理 / ID プロバイダ]を
	↓ IdP リスト) に戻る	ID プロバイダ名	System Identity Provider			開きます。[Sytem Identity Provider] を選択し、
	System Identity Provider タイプ: 組み込み	ユーザー	この IdP を使用して認証できるユーザーを選択 クトリから選択します。 システム ディレクトリ W AWJPN	します。以下のリストにある利用可能なディレ		認証方法で[デバイスコンプライアンス
	ステータス: 行効 IdP を無効化 商 IdP を用除	ネットワーク	この IdP にアクセスできるネットワークを選択 選択します。	します。次の利用可能なネットワーク範囲から		(Airwatch)]にチェックを入れ、[保存]をクリック
		課証方法	● すべての範囲 IdP がユーザー認証に使用する認証方式を選択し	ノます。 		します。
		27/9	第27方法 デバイス コンプライアンス (ArWatch) モバイル SSO (OS 部) パスワード (ローカルディレクトリ) ESC_AWJFN (secanignian) × 132/25年340 高田町5 (AU, DF)4	認証が強を関連的なる ダ ダ ・ ・ に したのつえつクタ 当時できます。 につみつタ		
			を追加(ハージでコネ て、コネクタをゼッ) タを選択してください 重要:高可用性を確保 れているめ巻があり!	いクタのアクティベーションコードを作成し トアップし、このIDプロバイダ用にそのコネク 」、 !するには、各コネクタに同じ認証方法が協定さ ます。		
		コネクタ認証方法	講証方法 バスワード (クラウ ド <i>デブ</i> ロイ)	認証方法を関連付ける ▼		
		KDC 証明書のエクスポ ート	証明書をダウンロード モバイルデバイス管理プロファイルで使用する ボートします。	ための KDC サーバのルート証明書をエクス		
			保存 キャンセル			











6.	[iOS]をクリックします。
順守ボリシーを追加 ◎	
ブラットフォームを選択	
Addroid Apple KOS Apple macOS Chrome OS (L/JS) QRX	
Windows 耐久性應未 Windows	
7. iOS Mマホリシーを追加 ● ルール @ アクション (① 割り出て (④ 概要)	OS バージョンが、iOS 10.2.0 以上だった場合 に、非順守状態となるポリシーを構成します。
ここで相差するルールの「下べて ・」に合致する	
05パーラロン 方向の間以上 ・ Apple K05・05 10 2.0 ・ O X 0 ルールを注加する ・ ・ ・ ・ ● ・ ● ・ ● <td></td>	
取べ キャンセル	
8.	[次へ]をクリックします。
iOS METボリシーを追加	
() ルール ● アクション ③ 割り当て () 概要	
Tぐに尻の線行を取け後 用線付加としてマーク 編約 ・ EA-ハをユーザーに設備 ・ CC 10 歳	
取定のデンプレート 0 たらに含い400の面積を約66	
80 80 40205	



9.	以下の設定を行い、[次へ]をクリックします。
iOS 順守ポリシーを追加 📀	
① ルール ④ アウション ● 群り当て ④ 概要	割り当てるグループ : All Devices(ssagawa)
图理元 * Kbala_ox	
副り当てるグループ	
ここに入力してクループを通知	
新へ あへ キャンセル	
10	
10.	[完了してアクティフ化]をクリックします。
iOS 順守ホリシーを追加 ©	
① ルール ③ アクション ③ 割り当て 🔹 感受	
11.10 名称 OS /(-ジョン	
2015 /(-ジョン	
デバイスの概要	
副り当て 1	
順守状態 0 ● 非順守状態 1 ◎	
第八 第7 第7しておりディン化 キャンセル	
11	
	ナヘトに () アイ・マント () アイト () 「「「」」 () アイ・マント (
パブ リスト表示 Sagawa1 iPhone iOS 11.2.5 G5MN	ことを確認します。
「IPPone 6 (16 GB Space Grey) 11.2.5 所有形態: 未定義	
7カウント O CVI3 EN ✓ ANISOURI3 - 31 分別 ○ GR書	
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
デバイス改定 □ コンデンツ ご 営理元 MDM ユーザー名	
 「iPhone を探す」が有効です sagawal 	
	1







1/							ニフトの海に行った乳完たこに同します
14.							ナストの為に行うに設定を元に戻します。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
~	ダッシュボード	デバイス > 順行	ボリシー >				
ハプ	リスト表示		1/				AirWatch 管理コンソール上で、作成した順守ポリ
	* ライフサイクル	V 102704					シーの緑色の隣のアイコンをクリックし、無効に
	→ プロファイルとリソース	有効	名前		説明		
! アカウント	▽順守ポリシー	••	OS バージョン		くEジーフ 20		
•	リスト教示	項目 1-1 / 1					
アプリとブック							Identity Manager で設定した再認証までの待機時
	割り当てグループ →						
コンテンツ	> 證明書						間を8時間に戻します。
< 構成			ポリシー ル・	ールの編集			
	* コーザーのネット	ワーク範囲が次の場合					
	* ユーザーが次からコンテン	ツにアクセスする場合	ALL RANGES				
	また、ユーザーが次の	グループに属する場合			•		
			~ 5/0-52	2897			
	707	カシート 右来仁(中才	グループが選択	されていない場合、ルールはす	べてのユーザーに適用されます。		
	 このデ ・ コーザーは次を使用して認 	ジンヨンを夹付します	以下を認証に使用			- ●	
	1 9 1001200000	および	モバイル SSO	(IOS 版)			
	先の方法が失敗するか適用で	きない場合、次を実行	テハイス コンフライアンス (AirWatch)				
			⊕ 7 <i>x</i> − <i>l</i>	バック方法を追加			
		再認証までの待機時間		時間 🗸 💿			
			8				
		高度なプロパティ 🗸					
					キャンセル	保存	

mware[®]



6 VMware Verify を使用した多要素認証の構成

6.1 本章のゴール

Workspace ONE に含まれる多要素認証機能である VMware Verify を構成します。本章では、ブラウザから Workspace ONE にアクセスした場合に、Active Directory のユーザ名とパスワードに加え、 VMware Verify を使用した2要素認証を実施するように構成します。

6.2 設定手順

VMware Verify を有効化し、認証ポリシーに VMware Verify を組み込みます。

1. ロール 地の込み D プロバイダの認識方法 語の日本日本 たん 人の日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本日本	V- 1-1 Provide the state for the		VMware Identity Manager コンソールで [ID とアクセス管理 / 管理 / 認証方法]を 開きます。
■第1882月出せ無知らすらこ。その882月出4アクセスホー 四級方法	「	32-92	
AirWatch 外部アクセス トークン	0	103	
デバイス コンプライアンス (AirWatch)	0	有印	- [VMware Verify] 行の構成ボタンをクリッ
パスワード (AirWatch Connector)	0	363	
Villware Verify	0	8.0	クします。
モバイル SSO (OS 版)	0	有30	
バスワード (ローカル ディレクトリ)	0	450	
		80	
2.			 [VMware Verifyを有効化する]にチェックを
MFAAdapi	ler		入れ、[保存]ボタンをクリックします。
VMware Ver にする	rify を有効 🖌		
		キャンセル 保存	



3.					VMware Identity Manager コンソールで[ID
					とアクセス管理 / 管理 / ID プロバイダ]を開
ID フロバイダ (3)				10 기미가귀 위험	き、[System Identity Provider]をクリックし
ID プロバイダ名 System Identity Provider	認証方式 ディレクトリ モバイル SSO (OS IØ) AWJPN	ネットワーク範囲	コネクタ タイフ esc.awion.lan 組みに	ステータスカ 行効	ます。
	デバイス コンプライアンス (AirWebh) バスワード (クラウド デプロ				
	イ) バスワード (ローカル ディレク トリ)				
Buit-In	バスワード (ローカルディレク システムディレク トリ)	ų.	esc.awjpn.lan 組み2	み 有効	
Workspace/DP1149	Password AWJPN	すべての範囲	esc.awjpn.lan Identit	y Manager Ŧ538	
4.					認証方法で、VMware Verify が有効になってい
<[IdP リスト] に戻る	5				ることを確認します。有効になっていない場合
	ID プロバイダ名	System Identity Provider			
	ユーザー	この IdP を使用して認証できるユーザー クトリから選択します。	を選択します。以下のリストにある	利用可能なディレ	
System Identity Pro	vider	■ システムディレクトリ			にし、[保存]をクリックします。
タイプ : 組み込み ステータス: 有効		awjpn			
IdP を無効化	ネットワーク	この IdP にアクセスできるネットワーク 選択します。	を選択します。次の利用可能なネッ	トワーク範囲から	
a IdP を削除		✓ すべての範囲			
	認証方法	IdP がユーザー認証に使用する認証方式	を選択します。		
		認証方法	認証方法を関連付ける		
		VMware Verify	· ·		
		モバイル SSO (iOS 版)	~		
		パスワード (ローカル ディレクトリ)	~		
	コネクタ	ESC AWJPN (esc.awjpn.lan) 🗙			
		コネクタを追加 高可用性 (HA を追加) ペー3) のために追加のコネクタを選択でき ジでコネクタのアクティベーション	fます。[コネクタ コードを作成し	
		て、コネクタ タを選択して	をセットアップし、この ID プロバー ください。	ダ用にそのコネク	
		重要:高可用! れている必要	5を確保するには、各コネクタに同じ があります。	認証方法が設定さ	
	コネクタ認証方法	認証方法	認証方法を関連付ける		
		バスワード (クラウ ド デプロイ)	~		
		THE PART OF LE			
	KDC 証明書のエクスホ ート	証明書をタワンロート モバイル デバイス管理プロファイルで使 ポートします。	用するための KDC サーバのルート	正明書をエクス	
		保存キャンセル			
F					
5.					VMware Identity Manager $\Box 29 - 70 \text{Cl ID}$
タッシュホード ユーザーとクルーフ カク ディレクトリ IDプロパイダ パスワート回義アS	07 0270年2月1日 ロール 3239ント 田田方油 ポリシー				■■ とアクセス管理 / 管理 / ポリシー]を開き、
ポリシーを追加 10% 10% ポリシー名	デフォルト ポリシーの編集 キットワーク研究	3.02		22.	[default_access_policy_set]をクリックしま
default_access_policy_set		0 アプリケーション		436-36	ਰ.
-					
6.					手順 3.2 と同様に、ポリシールールの編集で構
ポリシーの編集					成々ブキで進み、デバイフタイプが[Web ブラ
🕑 定義	選択したアプリケ- 囲、アプリケーショ	- ションへのアクセスに関するルール a ンにアクセスできるデバイスのタイ	のリストを作成できます。ルー プ、認証方法、再認証までにユ	ルごとに、IP ネットワーク範 .ーザーがアプリケーションを	リサ」になっている列の認証方法のリンクをクリ
	使用できる最大時間	司数を選択します。			ックします。デバイスタイプが Web ブラウザ
✓ 構成	ネットワーク範囲	町 デバイスタイプ	認証	再認証	のものがない場合はポリシールールを追加して
ן אב ה ה	: ALL RANGES	105	モバイル SSO (IOS 版)+1	8時間 ×	
		105		• ****	
	: ALL RANGES	Web 2 2 2 2 2		o vojio)	
	ALL RANGES	Workspace ONE アプリ	Password+1	2160 #glil) ×	
	E ALL RANGES	Web ブラウザ	Password+1	8時間 ×	
	⊕ ポリシール	ールを追加			



VMware Verify アプリのセットアップを実施します。

9.	レビン レンド マンド マンド マンド マンド マンド マンド マンド マンド マンド マ	PC からブラウザで Workspace ONE のポータル にアクセスし、AD のユーザーでログインをしま す。
10.	ごのの認証には VMware Verify が必要です。開始するには電話 素考を入力してください。 (国コード) (国コード) 電話 器局 (国コード) 電話 器局 (国コード)	 (はじめて VMware Verifiy を使用するアカウントの場合) 多要素認証に使用するスマートフォンの電話番号を入力して[ログイン]ボタンをクリックします。 TIP: 国内通話用の最初の[0]を省く必要はありません。 例 07011112222を+817011112222の形式で入力する必要はありません。
11.	••••• SoftBank 4G C 10:40 C 2059 C 10:20 C	スマートフォン上の作業 指定したスマートフォンに VMware Verify をイン ストールするためのリンクが SMS で届くので開き ます。

18.	スマートフォン上の作業
OneTouch AW-KOTABABA just sent you a new × approval request	トークンが表示されることを確認します。
⊘ verify ⁻	
AW-KOTABABA token is: 81 392 22 Your token expires in	
KBABAI Account	
19.	ブラウザへ戻り、VMware Verify アプリに表示さ れているトークンを入力し、[ログイン]をクリ ックします。
Workspace ONE"	
アクションが必要: VMware Verify からトークンを コピーしてログインしてください	
8139222	
ログイン Minuare Martin に開始がある語今	
SMS でログイン	
vmware:	
20.	Workspace ONE へのブラウザからのログインが 設定できました。
すべてのアプリ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	これにより、ブラウザからアクセスする場合は、 VMware Verify を用いて2要素認証するように構 成することができました。

初回セットアップ完了後の動作を確認します。

22.			画面右上のユーザーをクリックし、[ログアウト]を
O Workspace ONE"	Q 桃果	sagawa1 strinji ~ za#*	クリックします。
すべてのアプリ	:4	ログアウト	
	まだアプリが割り当てられていないようです。まちなく割り当てられますので、後でご種	認ください。	
23.			もう一度、AD のアカウント情報を入力し、[ログイ
			ン]をクリックします。
	Workspace ONE"		
	ユーザー名 sagawa 1		
	パスワード		
	awjpn.lan		
	ログイン		
	パスワードを忘れた場合	,	
	別のドメインに変更		
	vm ware:		
24.			認証が VMware Verify 待機状態になることを確認
			します。
	()		
	Workspace ONE"		
	アクションが必要:		
	VM ware Verify アプリを確認し て認証要求を承認してくださ		
	ふ物た体操しています		
	小師で行城しています…		
	要求を受信しなかった場合		
	ここをクリック		
	vmware:		

28.	スマートフォン上の作業
(VMware Identity Manager からのログイン 24s ago 要求。 Expires in 23h	認証要求を開きます。
29.	
OneTouch AW-KOTABABA just sent you a new approval request	認証要求の内容を確認し[Approve]ボタンで承認します。
⊘ verify~	
VMware Identity Manager からのログ イン要求。Please verify the information below. If you did not initiate this request, just click deny.Subject: テナント AW-KOTABABA のドメ イン awjpn.lan のユーザー sagawa1 に対す るログイン承認を要求していますDate: 4月 17, 2018 at 10:49	
30.	ブラウザからの Workspace ONE へのログインが
🗘 Workspace ONE* 🔍 🕸 👔 Lagenal strop 🗸	完了することが確認できました。
すべてのアプリ またアプリが知り用てられていないようです。まらなく用り用てられますので、他でご発展くだらい、	以上で VMware Verify を用いた 2 要素認証は完了 です。

Mware[®]

7 認証設定の最適化

7.1 本章のゴール

前章までの設定をの影響で、管理アカウントでログインができなくなっている場合があります。その場合は、以下の URL ヘアクセスすることで、管理者アカウントでのログインが可能です。 https://<テナント>.vmwareidentity.asia/SAAS/login/0

管理コンソールへのアクセスは上記 URL を用いても問題ありませんが、本章では、上記 URL を利用せずとも、管理者アカウントでログインできるように設定を行います。

7.2 設定手順

1								VMware Identity Manager コンソールで[ID と
	ロゴロバイダ (3)						ロブロバイダを追加	アクセス管理 / 管理 / ID プロバイダ 1を聞き
	050000							
	ロブロバイダ名	認証方式	ディレクトリ	ネットワーク範囲	コネクタ	タイプ	ステータス	[System Identity Provider]をクリックします。
	System Identity Provider	モバイル SSO (IOS 版) デバイス コングライアン (AirWatch) ノ(スワード (クラウド デ) イ) VMasre Veify ノ(スワード (ローカルディ トリ)	AWJPN ス プロ ィレク	すべての範囲	esc.awjon.lan	88.012.01	4138	
	Bulbin	バスワード (ローカルデ・ トリ)	ィレク システムディレクト	v.	esc.aejon.lan	相迎运动	有効	
	WorkspaceIDP1149	Password	AWJPN	すべての範囲	esc.awjon.lan	Identity Manager	4650	
2								以下の設定を行い、[保存]をクリックします。
	✓[IdP リスト] に戻	õ	ID プロバイダ名	Built_in_AWJPN			נ	 ID プロバイダ名:Buit-in ドメイン名 へ変更
			ユーザー	この IdP を使用して認証できるコ クトリから選択します。	Lーザーを選択します。以下	のリストにある利用可能なデー	rν	ユーザー:
	Built_in_AWJPN タイプ: 組み込み	ネットワーク	システムディレクトリ AWJPN				[システムディレクトリ]のチェックを オフ	
	(dP を無効化)		この kdP にアクセスできるネット 遊択します。 	・ワークを選択します。次の	利用可能なネットワーク範囲が	15	認証方法:パスワード(ローカルディレクトリ)	
	H ICH ISING			▲ すべての範囲 はP がユーザー認証に使用する認証方式を追訳します。				のチェックを オフ
			認証方法					
				認証方法	認証方法を	関連付ける		
				デバイス コンプライアンス (Ai	rWatch)	r		残りの設定はそのままにします。
				VMware Verify	~	•		
				モバイル SSO (IOS 版)	·			
				7000-100-1009-1009	(*3)			
			コネクタ	ESC_AWJPN (esc.awjpn.lar	n) 🗙			
				コネクタを追加 高可用 を追加 て、コ タを追 タを追	性(HA)のために追加のコネ] ページでコネクタのアクラ コネクタをセットアップし、 明してください、	ネクタを選択できます。[コネク ティベーション コードを作成し この ID プロバイダ用にそのコ	79 , ネク	
				重要: i れてい	高可用性を確保するには、き いる必要があります。	8コネクタに同じ認証方法が説	定さ	
			コネクタ認証方法	認証方法	認証方法を関	睡付ける		
				バスワード (クラウ ド デプロイ)	~			
			KDC 証明書のエクスポ ート	証明書をダウンロード モバイル デバイス管理プロファ~ ポートします。	イルで使用するための KDC	サーバのルート証明書をエクス		
				発行 キャンセル				
1								

3.								VMware Identity Manager コンソールで[ID と
וס לים יכ מו שאת	コ/(イダ (3) ロバイダ8 Jn_AWJPN	認証方式 モリ(イル SSO (IOS 順) デバイス コンプライアン3 (ArWatch)	ディレクトリ AWJPN	ネットワーク範囲 すべての部例	コネクタ esc.aejpn.lan	タイプ 組か込み	ロプロバイダを起 サードパーティ IDP 1 Workspace IDP を作成 組み込み IDP を作成	アクセス管理 / 管理 / ID プロバイダ]を開き、 「Contral print 「ID プロバイダを追加 / 組み込み IDP を作成]の 順にクリックします。
Bull-	in space(DP_1149	1000 = ド(250 トラン イ) Vitiware Verity パステード (ローカル ディ トリ) Passaord	ロ レク システムディレクトリ ANLEN	すべての範囲	esc axign, lan esc axign, lan	HEP-23-P Idently Manager	403 463	
4.	(par リスト にむ していたいたいでは、 タイプ、細からか ステータス: 不明	romain	D プロバイダ名 ユーザー ネットワーク 描記力法 KDC 証明素のエクスポ 	Built_m_SystemDomain この いP を使用して認識でき クトリから送訳します。 ・ <	るユーザーを選択します。 ットワークを選択します。 の認知方式を選択します。 (ArWatch) レクトリ)	以下のリストにある利用 次の利用可能なネットワー フ <u>はを関連付ける</u> □ □ マ × RDC サーノ(の)レート証明	「「能なディレ ーク部門から	以下の設定を行い、[追加]をクリックします。 ID プロバイダ名:Built-in_SystemDomain ユーザー:システムディレクトリを選択 ネットワーク:すべての範囲を選択 認証方:パスワード(ローカルディレクトリ)を 選択
5.				۵ ٦	Tenant A ユーザーホ ご使 ログ	dmin・A\ ータル ータル 加え 用条件 アウト		VMware Identity Manager 管理コンソールから ログアウトします。
6.				Workspace ONE*				 VMware Identity Manager 管理コンソールヘア クセスし、管理者アカウントでログインできるこ とを確認します。 同様にドメインアカウントでもログインできるこ とを確認してください。
			2-5-: 120- 1	8 awjpn.lan ログイン (スワードを忘れた) 別のドメインに変 vmware	場合更			以上で設定は完了です。これにより https://<テナント>.vmwareidentity.asia/ ヘアクセスすれば、管理者、ドメインユーザーど ちらもログインできるように構成ができました。

8 [APPENDIX] 参考情報

8.1 製品ドキュメント

VMware Identity Manager 製品ドキュメント http://www.vmware.com/jp/support/support-resources/pubs/identitymanager-pubs.html

VMware Identity Manager Integration Documentation (各種 SaaS とのインテグレーションガイド) https://www.vmware.com/support/pubs/vidm_webapp_sso.html

AirWatch 製品ドキュメント https://resources.air-watch.com

8.2 各種ガイド

Reviewer's guide for cloud-based VMware Workspace ONE http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-workspace-one-airwatchidentity-manager-reviewers-guide.pdf

Workspace ONE PoC Guide https://resources.air-watch.com/view/t5b49gbkrvglm8jmq565/en

AirWatch フリートライアルガイド スタート編 https://www.slideshare.net/HamamatsuMobile/vmware-airwatch-fee-trial-guide-jp-chapter-1-v20-73517273

AirWatch フリートライアルガイド ゲートウェイ連携編 https://www.slideshare.net/HamamatsuMobile/vmware-airwatch-fee-trial-guide-jp-chapter-2-v21-73517348

8.3 その他

浜松町モバイル愛好会 SlideShare https://www.slideshare.net/HamamatsuMobile/presentations

浜松町モバイル愛好会 YouTube (各種デモ動画) https://www.youtube.com/channel/UCVMfQCwJaNRl1tWyw8EZTTQ

ヴイエムウェア株式会社