



# Workspace ONE

## PoC ガイド Chapter 1

### スタート編

V 2.2



VMware株式会社



## Table of Contents

<b>1</b>	<b>Workspace ONE PoC 環境</b> .....	<b>6</b>
1.1	システム構成 .....	6
1.2	各コンポーネントのご紹介 .....	7
1.2.1	AirWatch .....	7
1.2.2	VMware Identity Manager .....	8
1.3	環境の準備と留意点 .....	8
1.4	各章の目的 .....	9
<b>2</b>	<b>VMware Enterprise Systems Connector による環境の統合</b> .....	<b>10</b>
2.1	本章のゴール .....	10
2.2	前提条件 .....	10
2.3	設定手順 .....	11
2.3.1	VMware Enterprise Systems Connector のインストールと設定 .....	11
2.3.2	AirWatch と Active Directory の連携設定 .....	17
2.3.3	Identity Manager と VMware Enterprise Systems Connector の連携設定 .....	20
2.3.4	Identity Manager と Active Directory の連携設定 .....	22
2.3.5	Identity Manager 上でのアウトバウンドモードの設定 .....	27
2.3.6	AirWatch と VMware Identity Manager の統合 .....	28
<b>3</b>	<b>ディレクトリユーザを使用したパスワード認証の構成</b> .....	<b>32</b>
3.1	本章のゴール .....	32
3.2	設定手順 .....	32
<b>4</b>	<b>iOS デバイス用モバイル SSO の構成</b> .....	<b>35</b>
4.1	本章のゴール .....	35
4.2	設定手順 .....	35
4.3	iOS デバイスで動作確認 .....	45
<b>5</b>	<b>デバイスコンプライアンス認証の構成</b> .....	<b>48</b>
5.1	本章のゴール .....	48
5.2	設定手順 .....	48
<b>6</b>	<b>VMware Verify を使用した多要素認証の構成</b> .....	<b>55</b>
6.1	本章のゴール .....	55
6.2	設定手順 .....	55
<b>7</b>	<b>認証設定の最適化</b> .....	<b>65</b>
7.1	本章のゴール .....	65
7.2	設定手順 .....	65
<b>8</b>	<b>[ APPENDIX ] 参考情報</b> .....	<b>67</b>
8.1	製品ドキュメント .....	67
8.2	各種ガイド .....	67
8.3	その他 .....	67

## 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

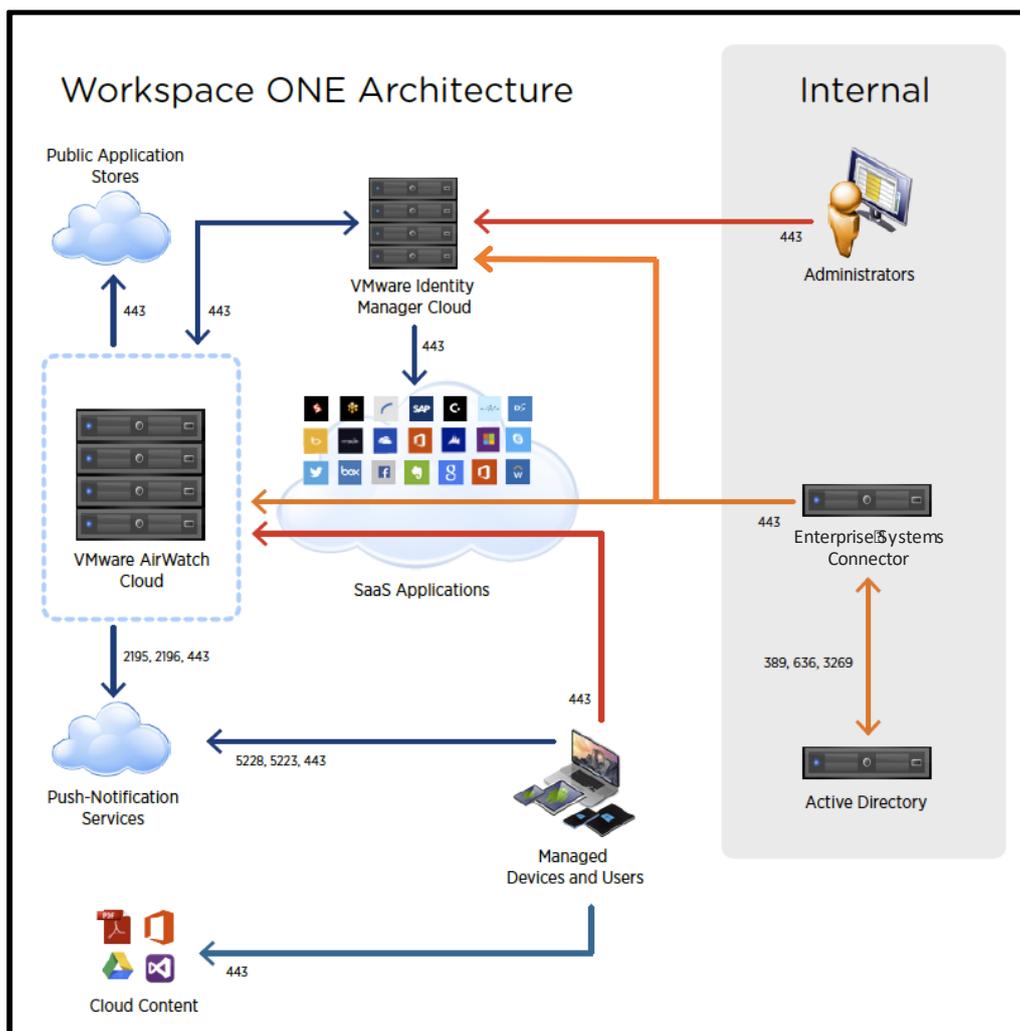
本書は VMware が提供する正式な製品マニュアルではなく、フリートライアルや PoC に使用いただくための参考資料です。また、VMware Identity Manager の操作や設定方法を中心に記載しており、AirWatch 自体の基本的な操作や設定方法は簡略化している部分がありますので「AirWatch フリートライアルガイド」シリーズも併せてご確認ください。

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

# 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 Identity 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



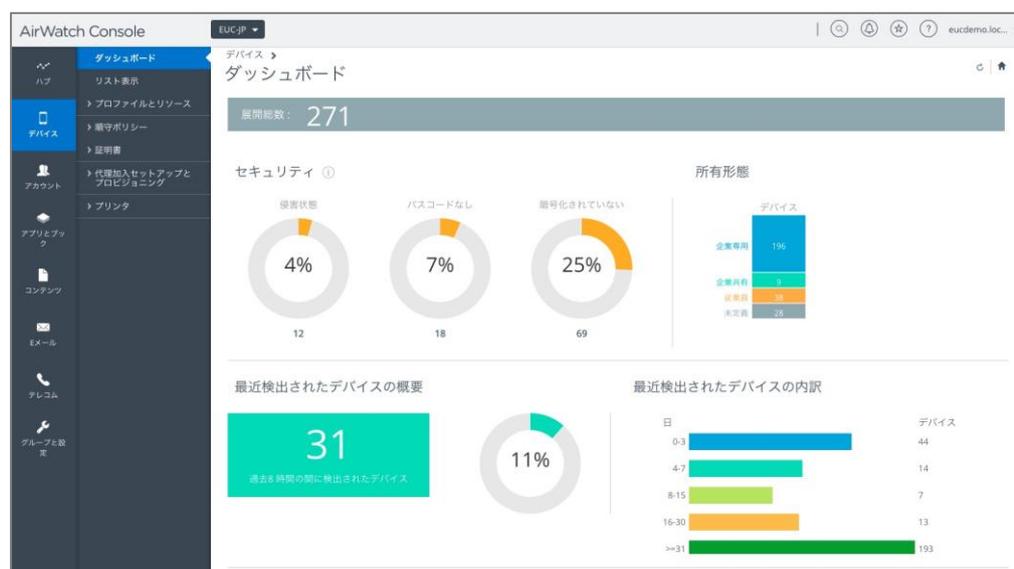
## 1.2 各コンポーネントのご紹介

### 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/コピー禁止/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、本文のコピーを制御したり、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。

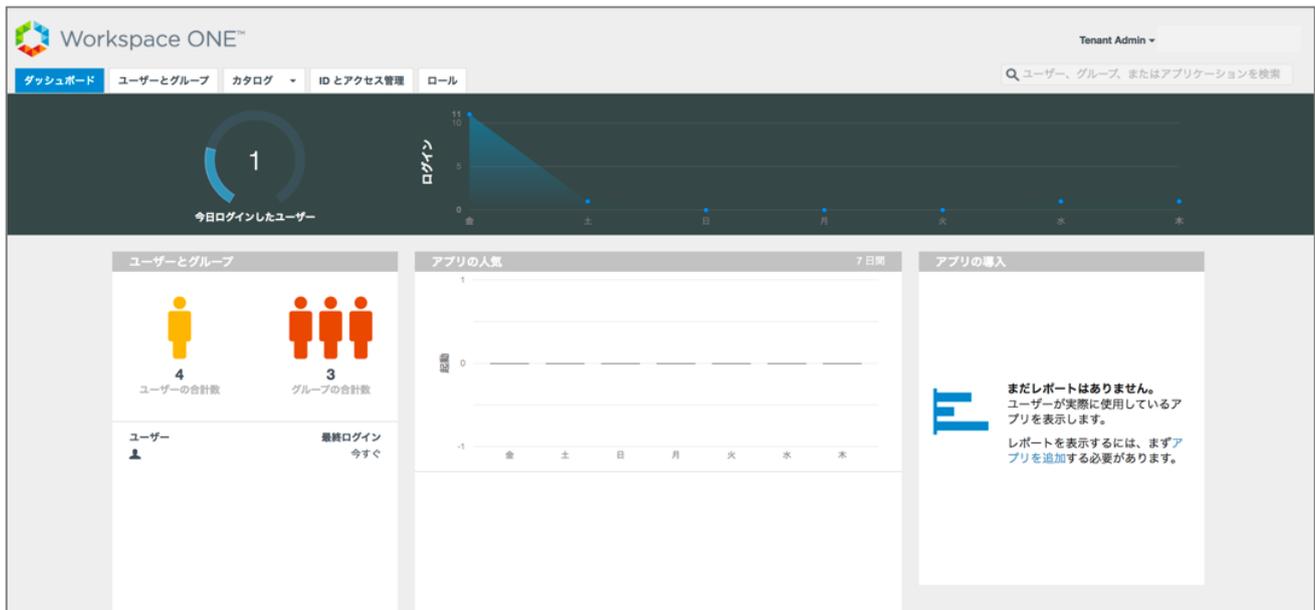
AirWatch ではこれらの機能を下図のような、包括的なコンソールである AirWatch Console を用いて、一元的に管理および運用を実施します。



## 1.2.2 VMware Identity 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



## 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 Manager 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。

### Tip :

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 (<http://www.air-watch.com/lp/ja/free-trial/>) をお申し込みください。

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技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。

30日間の **フリートライアル**を開始する

名	姓
企業メールアドレス	
役職	
電話	郵便番号
会社名	
業界	国

興味のあるソリューションを選択・

- モビリティ管理
- コンテンツ共同作業
- Identity Management



## 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。

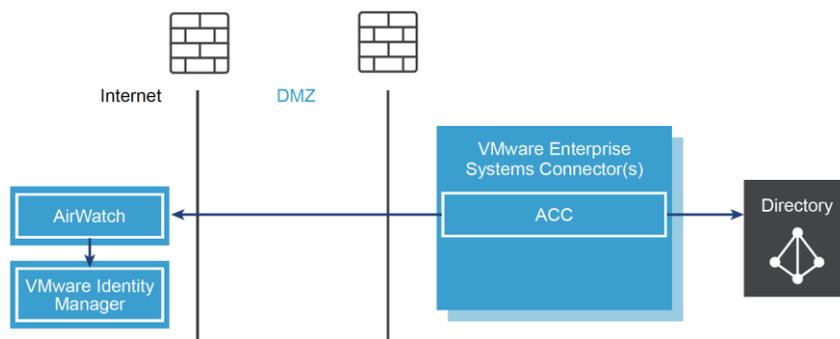
章	章題	目的
2	VMware Enterprise Systems Connector による環境の統合	VMware Identity Manager および AirWatch に対して企業内の Active Directory との連携を構成し、ユーザ管理を AD で一元管理する場合に実施します。
3	ディレクトリユーザを使用したパスワード認証の構成	ブラウザーベースでのアクセスや AirWatch で管理していないデバイスから、Active Directory の認証情報を使用した認証を構成する場合に実施します
4	iOS デバイス用モバイル SSO の構成	iOS デバイスからモバイル 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

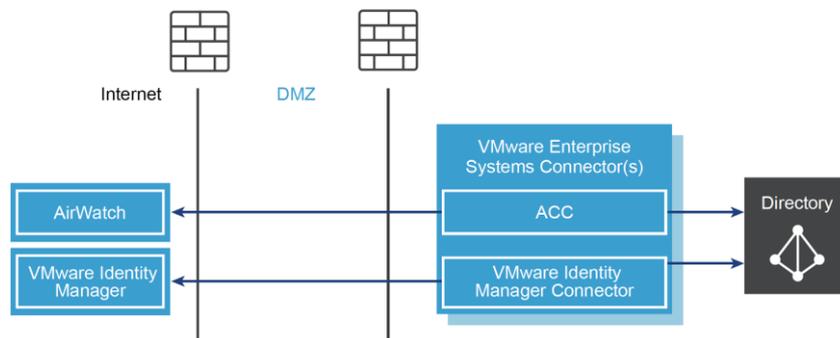
### 2.1 本章のゴール

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。

AirWatch 9.0 までの構成



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。

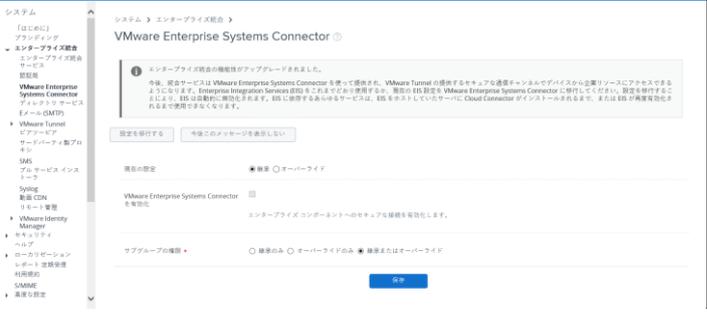
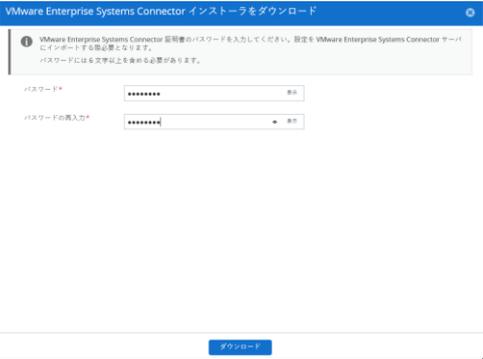
- Windows Server 2008R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- 連携対象の Active Directory ドメインに参加済み
- 英語版 OS を使用



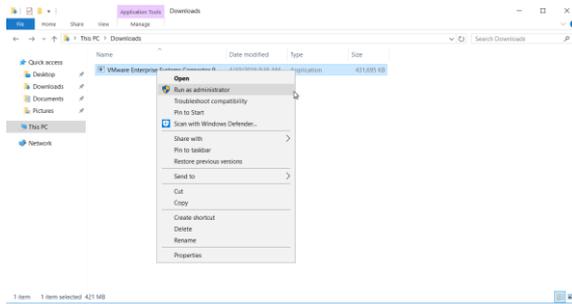
## 2.3 設定手順

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

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

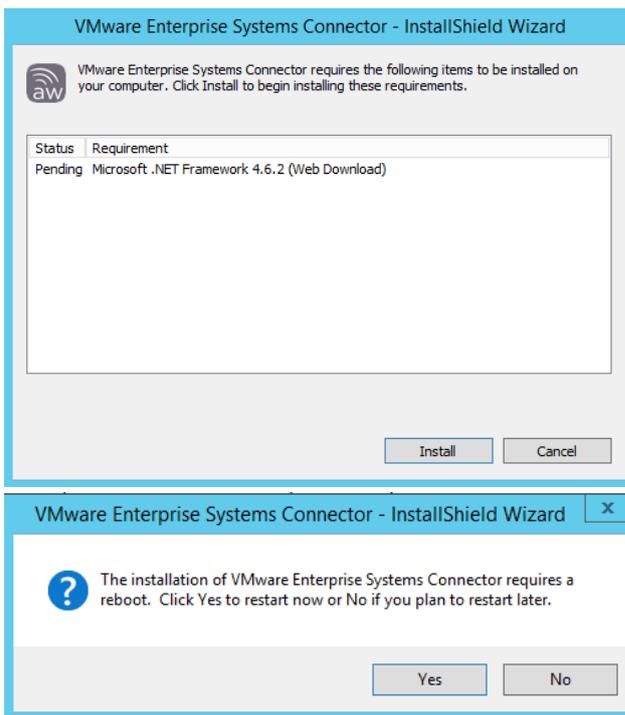
<p>1.</p> 	<p>ESC のマシンからブラウザで AirWatch コンソールへログインし、[グループと設定 / すべての設定 / システム / エンタープライズ統合 / VMware Enterprise Systems Connector]の順にクリックします。</p>
<p>2.</p> 	<p>「現在の設定」でオーバーライドを選択し、[VMware Enterprise Systems Connector を有効化]にチェックを入れ、[保存]をクリックします。</p> <p>その後、[VMware Enterprise Systems Connector インストーラをダウンロード]リンクをクリックします。</p>
<p>3.</p> 	<p>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。</p>

4.



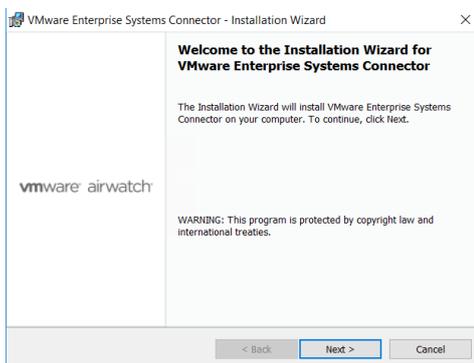
ダウンロードしたファイルを実行します。

5.



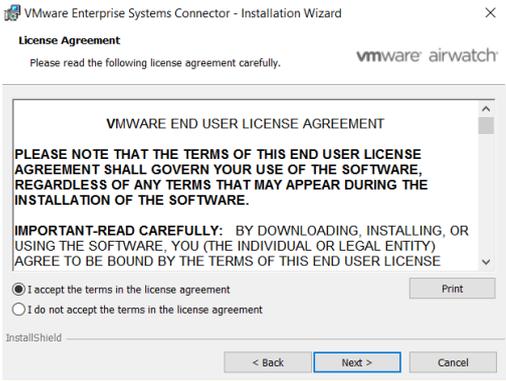
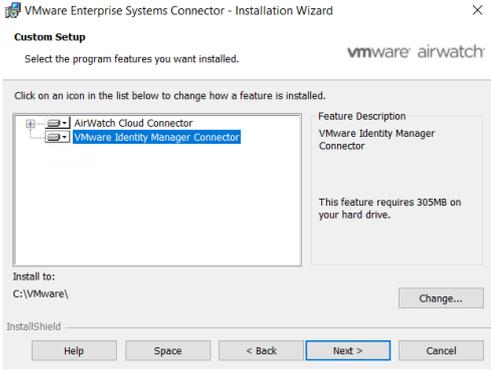
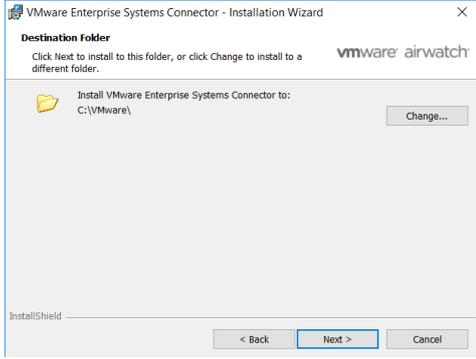
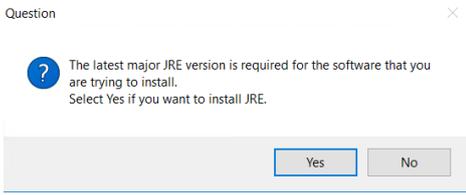
(.NET Framework のインストールを求められた場合は) [Install] をクリックし、.NET Framework のインストールを行います。インストール後、再起動を求められるので、[Yes] をクリックし再起動します。

6.

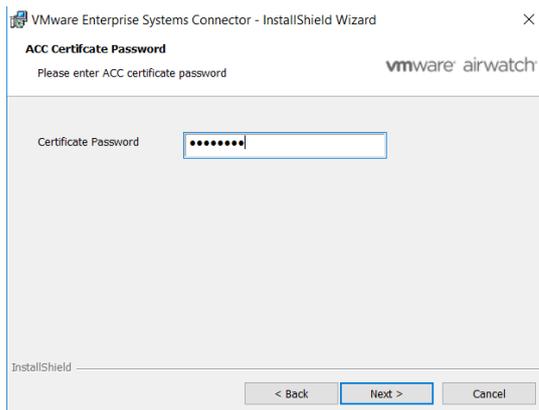


再起動後、インストールウィザードが起動します。[Next] をクリックします。



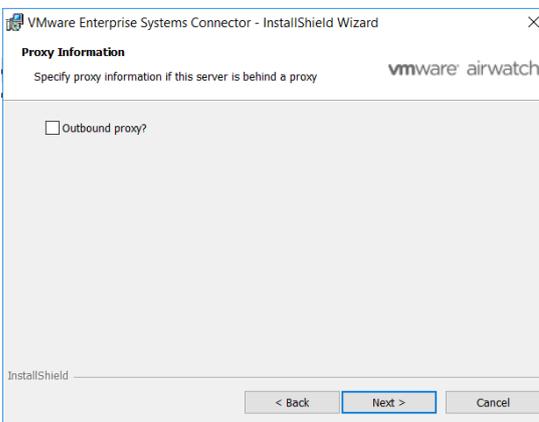
<p>7.</p> 	<p>使用許諾に同意し、[Next]をクリックします。</p>
<p>8.</p> 	<p>AirWatch Cloud Connector VMware Identity Manager Connector の両コンポーネントをインストール対象にし、 [Next]をクリックします。</p>
<p>9.</p> 	<p>インストール先フォルダを指定し、[Next]をクリックします。</p>
<p>10.</p> 	<p>JRE のインストールが求められたら、[Yes]をクリックします。</p>

11.



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。

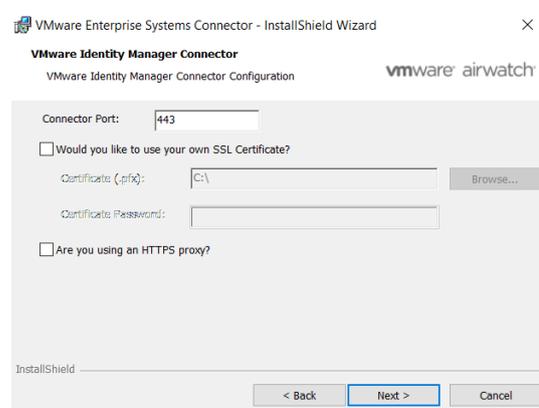
12.



[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.

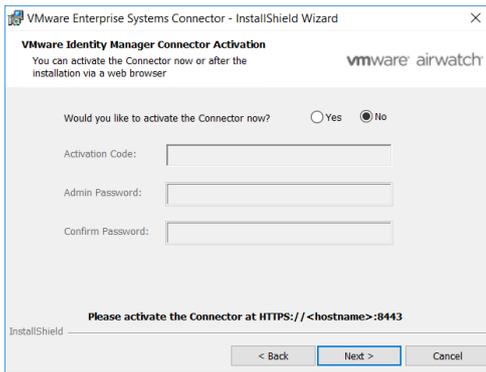


[Would you like to use your own SSL Certificate?]のチェックを外し、[Next]をクリックします。

\* 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。

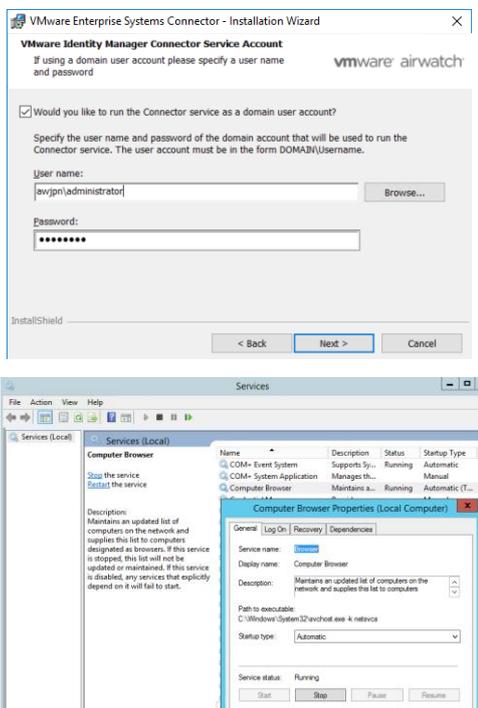


14.



ここではチェックを入れずに[Next]をクリックします。

15.



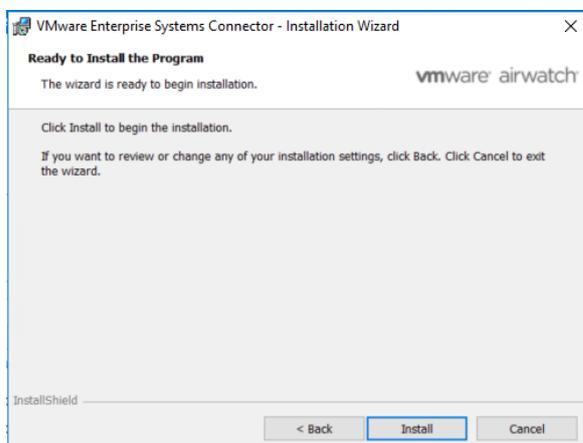
サービスを起動するためのドメインアカウントを手入力します。  
認証に問題がない場合、Install に進めます。

(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

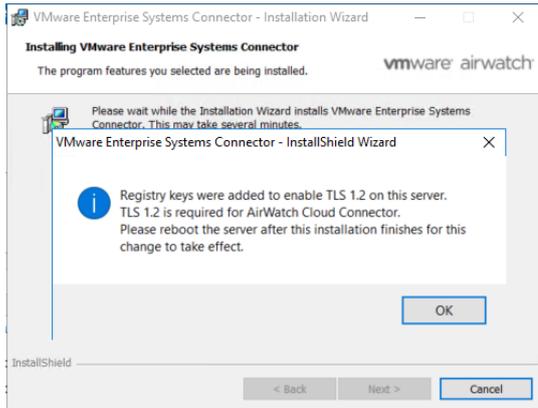
16.



[Install]をクリックし、インストールを実施します。

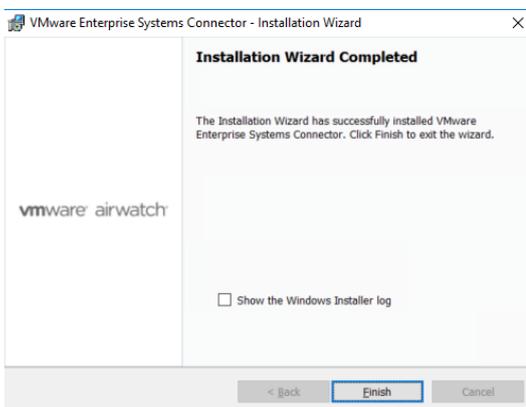
(インストールには環境により 7 分程度の時間を要します。)

17.



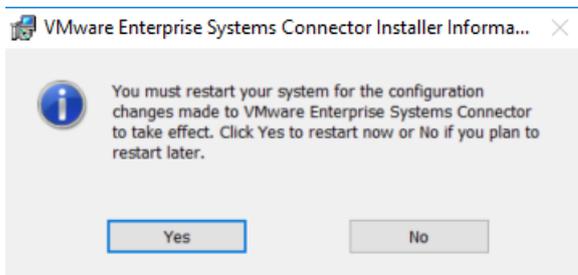
TLS 1.2 を有効化する旨の警告が表示されます。  
[OK] をクリックします。

18.



[Finish] をクリックします。  
これでインストールは完了です。

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。

## 2.3.2 AirWatch と Active Directory の連携設定

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

1.



AirWatch コンソールへログインし、[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

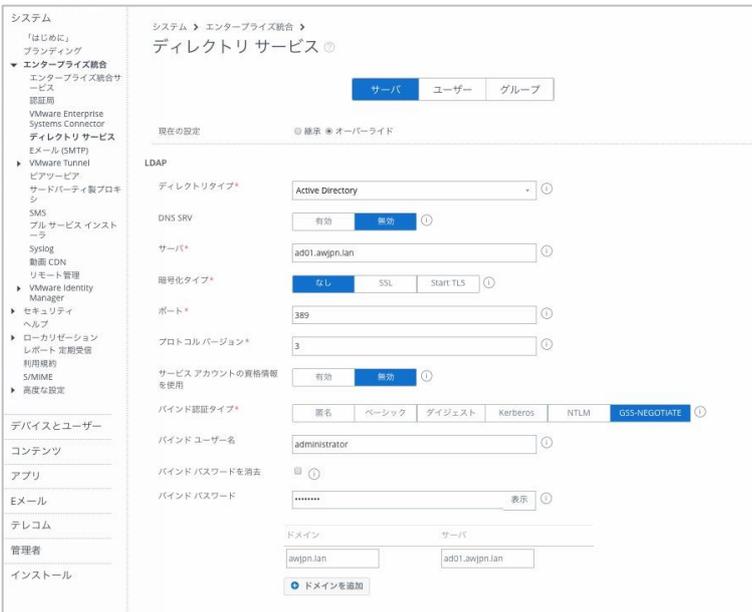
プロトコルバージョン : 3

サービスアカウントの資格情報を使用 : 無効

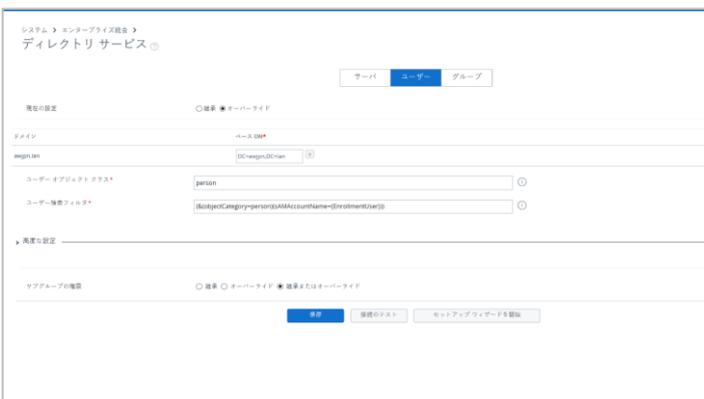
バインド認証タイプ : GSS-NEGOTIATE

バインドユーザー名 : ドメインユーザー名

バインドパスワード : パスワード



2.



画面上部で[ユーザー]タブをクリックし、ベース DN を設定します。ベース DN は [+]ボタンをクリックすることで参照できます。

## 3.

システム > モニタープレイス設定 > ディレクトリ サービス

サーバ ユーザー **グループ**

設定を確認する必要があります。

属性の指定  継承  オーバーライド

グループ名

ベース DN

グループオブジェクトクラス

継承ユニット オブジェクトクラス

サブグループの権限  継承  オーバーライド  継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

サブグループの権限  継承  オーバーライド  継承またはオーバーライド

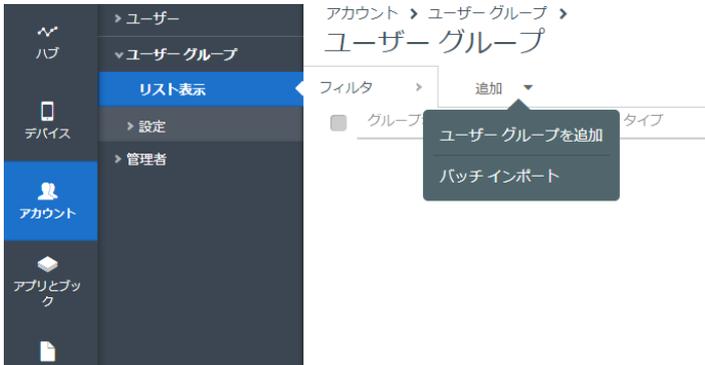
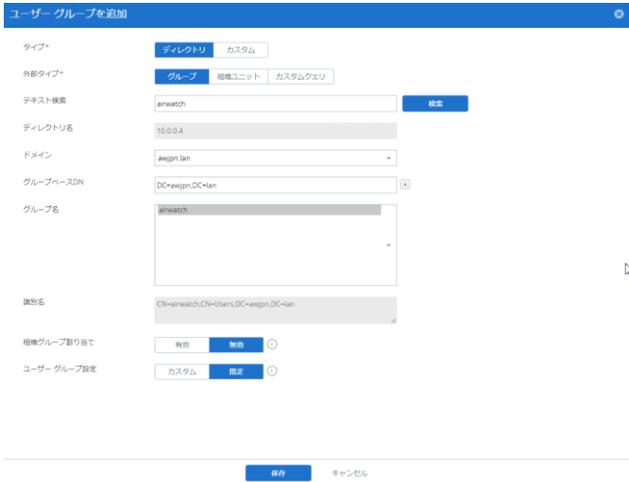
保存 接続のテスト セットアップ ウィザードを開始

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。

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 [+]ボタンをクリックすることで参照できます。設定完了後、[保存]をクリックし、エラーなく保存できることを確認します。

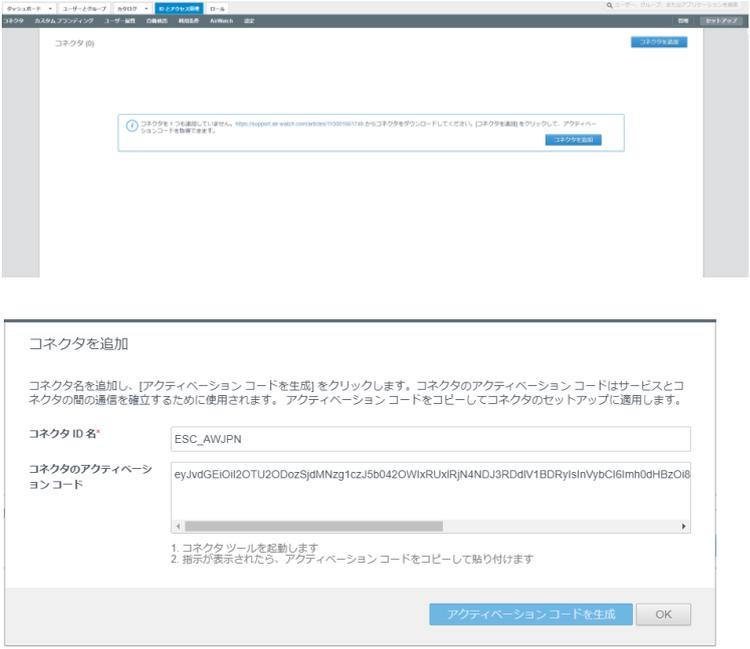
[接続のテスト]をクリックし、AD との接続に問題ないことを確認します。

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。)

<p>4.</p> 	<p>AirWatch コンソールへログインし、[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。</p>
<p>5.</p> 	<p>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。</p> <p>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</p> <p>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。</p>
<p>6.</p> 	<p>[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。</p> <p>[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。</p>

## 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。

<p>1.</p> 	<p>Identity Manager の管理コンソールへアクセスします。</p> <p>URL : &lt;https://xxx.vmwareidentity.asia&gt; (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。</p> <p>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。</p>
<p>2.</p> 	<p>[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。</p> <p>その後、[コネクタを追加]をクリックします。</p> <p>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。</p> <p>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。</p>



3.



ESC サーバー上でブラウザを起動し、以下の URL にアクセスし、[続行]をクリックします。

https://ESC サーバーの FQDN:8443

4.



管理者アカウント(admin)のパスワードを入力し、[続行]をクリックします。

5.



先ほどコピーしたアクティベーションコードをペーストします。

[続行]をクリックします。

6.



コネクタの設定が完了しました。

## 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。

<p>1.</p> 	<p>VMware Identity Manager コンソールで、[ID とアクセス / セットアップ / ユーザー属性]を開き、 デフォルト属性の <i>userPrincipalName</i> と <i>distinguishedName</i> 属性を必須に設定します。</p>
<p>2.</p> 	<p>[ 使用するその他の属性を追加 ]に[<i>objectGUID</i> ]属性を追加します。</p> <p>保存をクリックします。</p>
<p>3.</p> 	<p>Identity Manager の管理コンソールで、[ID とアクセス管理 / 管理 / ディレクトリ]の順にクリックします。</p> <p>その後、[ディレクトリを追加 / LDAP/IWA 経由の Active Directory を追加]をクリックします。</p>



4.

ディレクトリを追加

ディレクトリ名\*

LDAP 経由の Active Directory  
 Active Directory (統合 Windows 認証)

ディレクトリの同期と認証

Active Directory から VMware Identity Manager ディレクトリへユーザーを同期するコネクタを選択します。

同期コネクタ

認証 このコネクタで認証も実行しますか?  
 はい  
 いいえ

ディレクトリ検索属性\*

ユーザー名を含むアカウント属性を入力します。

サーバーの場所

DNS サービス ロケーション (SRV) レコードを使用して Active Directory ドメインを特定するには、このチェックボックスをオンにします。DNS SRV ルックアップを使用しない場合は、チェックボックスを選択解除し、Active Directory サーバホスト名とポート番号を入力します。

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 STARTTLS 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ート CA 証明書を指定します。ルート CA 証明書が複数ある場合、すべての証明書を 1 つずつ追加していきます。各証明書が PEM 形式であり、「BEGIN CERTIFICATE」と「END CERTIFICATE」で区切られていること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接続が必要

バインド ユーザーの詳細

【ベース DN】フィールドに、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、OU=myUnit,DC=myCorp,DC=room です。【バインド DN】フィールドには、ユーザーを検索できるアカウントを入力します。たとえば、CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=room です。

ベース DN\*

バインド DN\*

バインド DN パスワード

Active Directory のバインド アカウントパスワードを入力します。

以下のように設定をし、[接続をテスト]をクリックします。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：任意の名前を入力
- ディレクトリの同期と認証
  - 同期コネクタ：設定したコネクタを選択
  - 認証：はい
  - ディレクトリ検索属性：sAMAccountName
- サーバーの場所：チェック
- バインドユーザーの詳細
  - ベース DN：アカウント検索を開始する DN
  - 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

5.

ドメインを選択

LDAP 経由で Active Directory を追加する場合、ドメイン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)。

ドメイン

awjpn.lan (AWJPN)

連携させるドメイン情報が表示されていることを確認し、[次へ]をクリックします。

6.

ユーザー属性をマップ

いい場合は、ドロップダウンメニューから正しい属性を選択します。必須属性のリストを管理したり、リストにない属性を追加するには、[セットアップ] > [ユーザー属性] ページに移動します。

VMware Identity Manager の属性名	Active Directory の属性名	
userPrincipalName	userPrincipalName	必須
userName	sAMAccountName	必須
lastName	sn	必須
firstName	givenName	必須
email	mail	必須
distinguishedName	distinguishedName	必須
disabled	userAccountControl	
domain	canonicalName	
employeeID	employeeID	
objectGUID	objectGUID	
phone	telephoneNumber	

前へ
キャンセル
次へ

[ objectGUID ] 行の [ Active Directory の属性名 ] に [ objectGUID ] を選択します。

[次へ] をクリックします。

7.

同期するグループを選択します

同期するグループ DN を入力します。例: CN=users,DC=example,DC=company,DC=com。ディレクトリと同期する Active Directory グループを選択します。グループを選択すると、グループ名がすぐに同期されます。これらのグループのメンバーシップは、リソースの使用資格がグループに付与されると同期されます。

ネストされたグループメンバーを同期

グループ DN を指定	すべてを...	同期するグループ	
cn=airwatch,cn=users,dc=awjpn,dc=lan	<input type="checkbox"/>	0 / 1	選択 <span style="color: red;">✖</span> <span style="color: green;">+</span>

グループ DN	マップされたグループ

同期するグループ DN を入力します。例: CN=users,DC=example,DC=company,DC=com。ディレクトリと同期する Active Directory グループを選択します。グループを選択すると、グループ名がすぐに同期されます。これらのグループのメンバーシップは、リソースの使用資格がグループに付与されると同期されます。

1 グループが見つかりました: cn=airwatch,cn=users,dc=awjpn,dc=lan

グループを検索

<input checked="" type="checkbox"/> 名前	パス
<input checked="" type="checkbox"/> airwatch	CN=airwatch,CN=Users,DC=awjpn,DC=lan

同期するグループを選択します

同期するグループ DN を入力します。例: CN=users,DC=example,DC=company,DC=com。ディレクトリと同期する Active Directory グループを選択します。グループを選択すると、グループ名がすぐに同期されます。これらのグループのメンバーシップは、リソースの使用資格がグループに付与されると同期されます。

ネストされたグループメンバーを同期

グループ DN を指定	すべてを...	同期するグループ	
cn=airwatch,cn=users,dc=awjpn,dc=lan	<input type="checkbox"/>	1 / 1	選択 <span style="color: red;">✖</span> <span style="color: green;">+</span>

グループ DN	マップされたグループ
cn=airwatch,cn=users,dc=awjpn,dc=lan	CN=airwatch,CN=Users,DC=awjpn,DC=lan

[+] ボタンをクリックし、Identity Manager に同期するグループの設定を行い [次へ] をクリックします。

ここでは AD 上に作成した「airwatch」というグループの DN を指定しています。

[グループの検索] をクリックし、対象のグループが表示された後、[選択] をクリックします。

対象のグループにチェックし、保存をクリックします。

同期するグループが 1/1 となり、選択されていることを確認したら [次へ] をクリックします。



8. \_\_\_\_\_

同期するユーザーを選択

たとえば、CN=username,CN=users,DC=example,DC=company,DC=com など、同期するユーザー DN を入力します。DN 配下で見つかるすべてのユーザーも同期されます。同期から除外するユーザーを指定するには、除外フィルタを使用します。

ユーザー DN を指定 +

ユーザーを除外するフィルタ... +

Identity Manager に同期するユーザーの設定を行い[次へ]をクリックします。  
本書ではユーザー指定での登録はせずに進めます。

9. \_\_\_\_\_

設定の確認

選択したグループとユーザーをディレクトリへ同期する準備が整いました。変更が必要な場合は、同期を実行する前に修正してください。

	追加	削除	更新	
	0	0	0	ユーザー DN を編集
	1	0	0	グループ DN を編集

最初の同期の後、同期は毎週 1 回間隔で実行するようにスケジュール設定されます。同期間隔は今すぐ変更することも、後で [同期間隔] ページで変更することも可能です。 キャンセル 保存

同期間隔

日

時間  :

ヒント: 同期スケジュールはコネクタのタイムゾーンで実行されます。

キャンセル ディレクトリ同期

必要であれば、ディレクトリの同期間隔を変更し、[ディレクトリ同期]をクリックします。  
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。

10. \_\_\_\_\_

ディレクトリ名	タイプ	ドメイン	同期済みグループ	同期済みユー...	最終同期	アラート
システムディレクトリ	ローカルディレクトリ	1	0	1		
AWLPN	LDAP 経由の Active Dir...	1	0	0		<span>ページを更新して同期ステータスを表示</span>

ディレクトリの同期が開始されます。  
最新の状態は[ページを更新]をクリックすることで確認できます。

11.

ディレクトリ名	タイプ	ドメイン	同期済みグループ	同期済みユー...	最終同期	アラート
システムディレクトリ	ローカルディレクトリ	1	0	1		
ADFS	LDAP 経由の Active Directory	1	1	0	2018/04/13 13:04:09	<span style="color: green;">●</span> 更新済み

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.

グループ名	ドメイン	ディレクトリ	同期済みユー...
All USERS			1
awsadm@agpn.jp	agpn.jp	ADFS	同期されていません

[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.

このグループのユーザー  
awsadm@agpn.jp  
ドメイン: agpn.jp  
ディレクトリ: ADFS

このグループのユーザー  
このユーザーは同期されていません。  
詳しくはヘルプを参照してください。

[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。

14.

ディレクトリ名	タイプ	ドメイン	同期済みグループ	同期済みユー...	最終同期	アラート
システムディレクトリ	ローカルディレクトリ	1	0	1		
ADFS	LDAP 経由の Active Directory	1	1	1	2018/04/13 13:14:54	<span style="color: green;">●</span> 更新済み

ユーザー名	ユーザー ID	ドメイン	ディレクトリ	VMware Verify 電話番号	グループ	ステータス
Admin_Tenant	ksah@vmware.com	System Domain	システムディレクトリ	NA	ALL USERS	有効
awsadm@agpn.jp	awsadm1	agpn.jp	ADFS	+517021907428	awsadm@agpn.jp, ALL USE...	有効

[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。



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

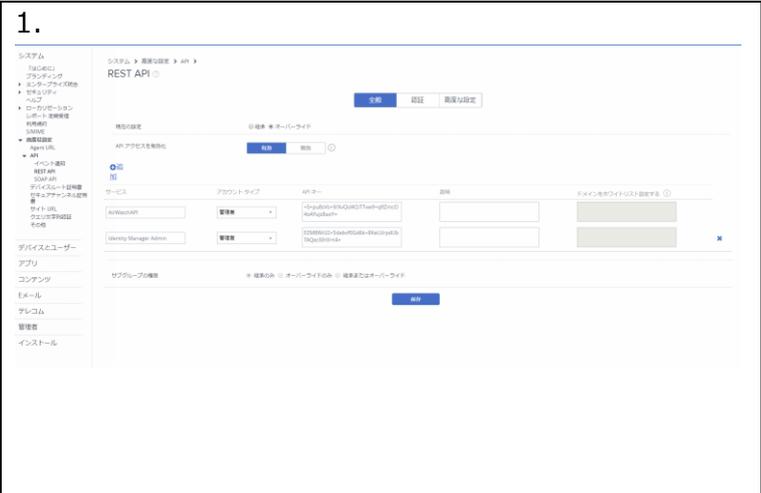
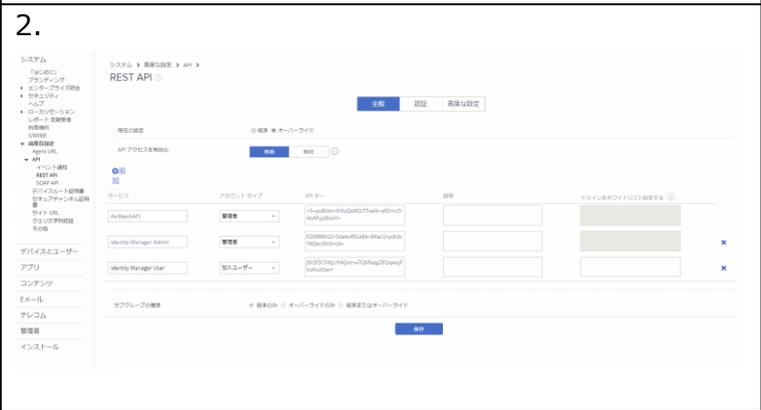
Identity Manager 上でアウトバウンドモード（ESC に固定グローバルアドレスを付与する必要がない構成）の設定を行います。

<p>1.</p> 	<p>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。</p>
<p>2.</p> 	<p>以下の設定をします。（次項に続く）</p> <p>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</p>
<p>3.</p> 	<p>以下の設定をし、[保存]をクリックします。</p> <p>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</p> <p>以上でアウトバウンドモードの設定は完了です。</p>

## 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。

<p>1.</p> 	<p>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。</p> <p>[API アクセスを有効化]を有効に設定します。</p> <p>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。</p> <p>(API キーをメモ帳などにコピーします。)</p>
<p>2.</p> 	<p>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。</p> <p>(API キーをメモ帳などにコピーします。)</p> <p>完了後、[保存]をウリックします。</p>
<p>3.</p> 	<p>[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。</p>



4.

ユーザ名に[ IdentityManager ]、その他の必須項目を任意に設定します。

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" などが使用されている場合があります。こちらは管理上の名前ですので任意のもの (IdentityManager\_テナント名) などを指定してください。

5.

[役割]タブに移動します。

組織グループに最上位の組織グループを選択します。役割に[ Console Administrator ]もしくは[ AirWatch Administrator ]を選択します。

6.

[API]タブに移動します。

[ 証明書 ]を選択します。  
証明書用のパスワードを設定します。  
[ 保存 ]を実行します。  
セキュリティ暗証番号が求められた場合は、事前に設定した暗証番号を入力します。

7.

名前	姓	Eメール	組織	管理タイプ	有効期限	組織グループ	状態
IdentityManager_kbaba	Manager	IdentityManager@vso.lan	Console Administrator	パスワード	有効	None	有効

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。

ユーザ作成時に設定した証明書のパスワードを入力して、[ クライアント証明書をエクスポート ]を実行します。  
(証明書のダウンロードが開始されます。)

[ 保存 ]を実行します。

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

9.

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、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 API サーバのアドレスを入力。  
CN504 の場合 : https://as504.awmdm.jp
- AirWatch API 証明書 : 前項目で作成した証明書をアップロードし証明書のパスワードを入力。
- AirWatch 管理用の API キー :  
*Identity Manager Admin* の API キーを入力。
- AirWatch 登録ユーザー用の API キー :  
*Identity Manager User* の API キーを入力。
- AirWatch グループ ID : 利用中の AirWatch の最上位組織グループのグループ ID を入力。

[ 保存 ]を実行。



10.

**保存**

---

**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**

---

**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デバイスが遵守しているか確認します。

有効  無効

**保存**

---

**AirWatch によるユーザーのパスワード認証** AirWatch によるユーザーの(スワード)認証を有効にします。

有効  無効

**保存**

---

**AirWatch によるユーザーの外部アクセス トークン認証** AirWatch によるユーザーの外部アクセス トークン認証を有効にします。

有効  無効

**保存**

続いて以下の設定を行います。

統合カタログ : 有効

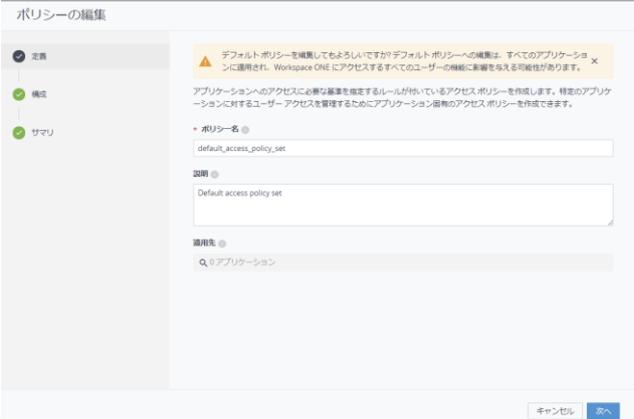
[ 保存 ] を実行。

## 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

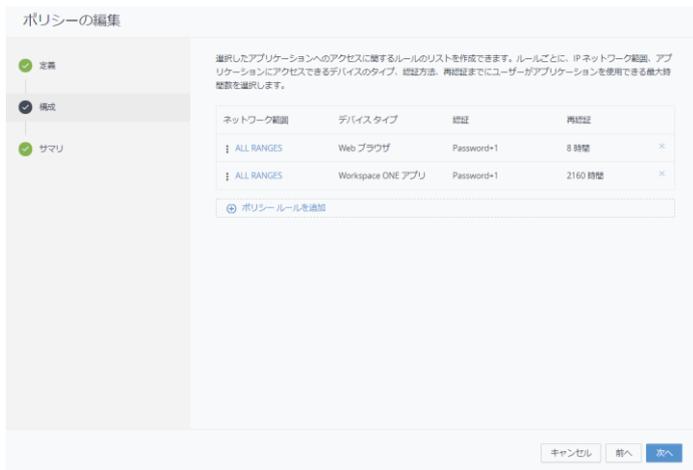
本章では、Active Directory の認証情報を使用した認証（Active Directory のユーザ ID およびパスワードを入力する認証）を構成します。この認証タイプは主にブラウザーベースでのアクセスや AirWatch で管理していないデバイスでの認証などに使用されます。

### 3.2 設定手順

<p>1.</p> 	<p>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。</p>
<p>2.</p> 	<p>[編集]をクリックします。</p>
<p>3.</p> 	<p>ポリシーの編集画面の定義タブで、そのまま[次へ]をクリックします。</p>



4.



ポリシーの編集画面の構成タブで、[ポリシールールを追加]をクリックします。

5.

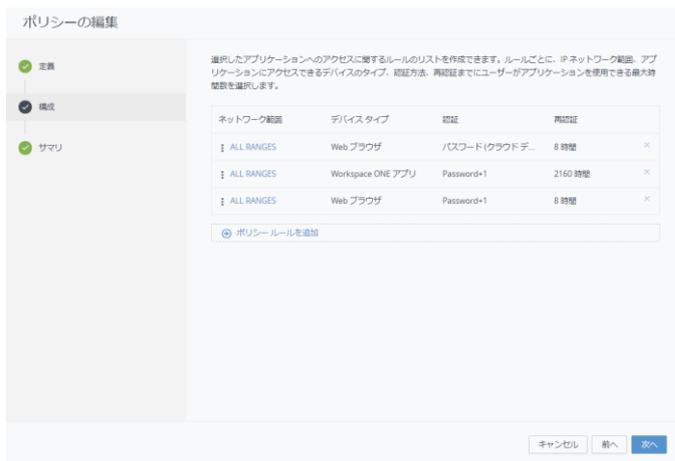


以下の設定を行い[OK]をクリックします。

- ・ [ユーザーのネットワーク範囲が次の場合] : ALL RANGES
- ・ [およびユーザーのコンテンツアクセス元が次の場合] : Web ブラウザ
- ・ [次に、以下の方法を使用して認証することができます] : パスワード (クラウドデプロイ)

[保存] をクリックします。

6.



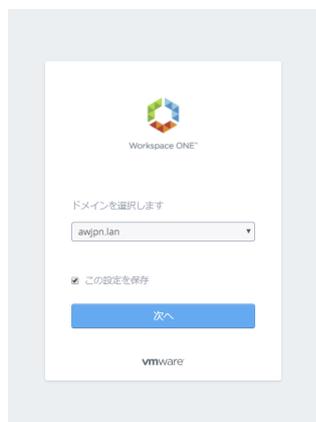
ポリシールールが追加されたことを確認します。すでにルールが存在している場合は、作成したポリシールールを最上部にドラッグアンドドロップします。  
[次へ]をクリックします。

4.



サマリタブで[保存]をクリックします。

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>)

プルダウ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す。

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。

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。

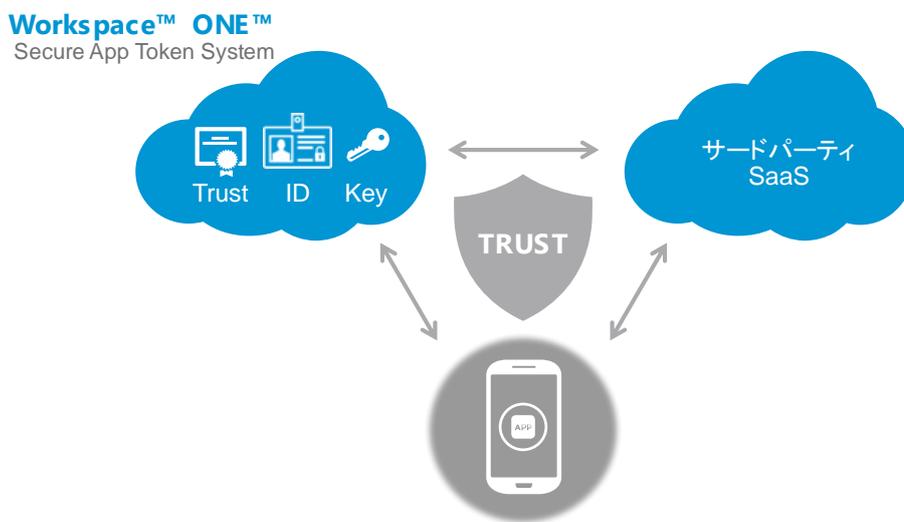


## 4 iOS デバイス用モバイル SSO の構成

### 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。

<p>1.</p>	<p>AirWatch コンソールで[グループと設定 / すべての設定 / エンタプライズ統合 / VMware Identity Manager / 構成] を開く。</p> <p>証明書から[有効化] をクリックします。</p>
-----------	--

2.



証明書の内容が表示されるので、 [エクスポート] をクリックし証明書をダウンロードします。

3.



VMware Identity Manager コンソールで[ ID とアクセス管理 / 管理 / 認証方法 ]を開く。  
[ モバイル SSO (iOS) ]行の構成ボタンを押す。

4.

KdcKerberosAuthAdapter

KDC 認証を有効にする  
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。

レルム:   
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。

ルートおよび中間 CA 証明書:   
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。

アップロードされた CA 証明書のサブジェクト DN:

OCSP を有効にする  
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 を送信する  
各 OCSP 要求に Nonce を含むことで、レスポンスのリプレイ攻撃から保護します。

OCSP レスポンスの署名証明書:   
OCSP レスポンスへの署名に使用する証明書をアップロードします。

OCSP レスポンスの署名証明書のサブジェクト 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。

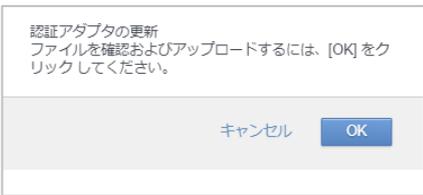
キャンセル リンクを有効にする  
[キャンセル] を有効にすると、ユーザーはログイン ページで [キャンセル] をクリックして Kerberos 認証を停止できるようになります。

エンタープライズデバイス管理サーバの URL:

[ KDC 認証を有効にする ] にチェックを入れ有効化。

ルートおよび中間 CA 証明書 で [ファイルを選択] ボタンをクリックします。

ステップ 2 でダウンロードした証明書を選択してアップロードし、[OK]をクリックします。



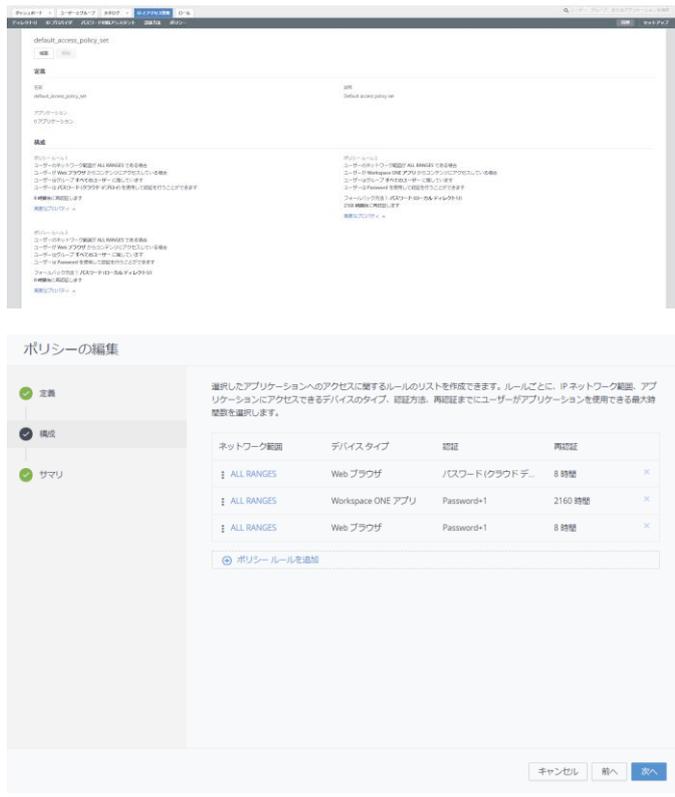


8.



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、ポリシールールを追加します。

10.

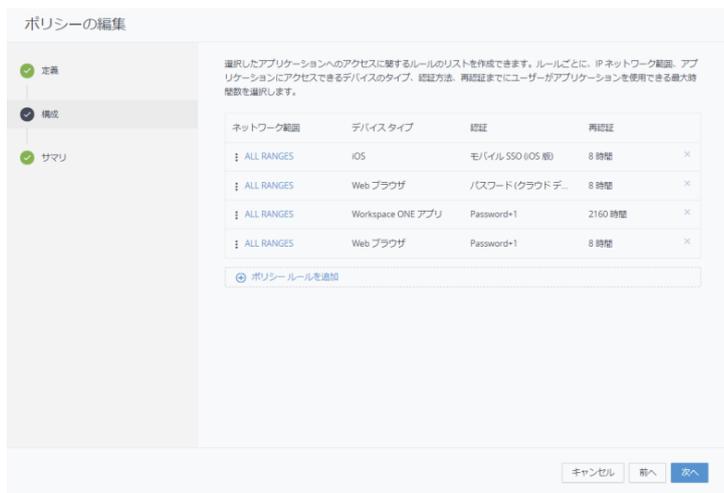


以下の設定を行い[保存]をクリックします。

- ・ [ユーザーのネットワーク範囲が次の場合] : ALL RANGES
- ・ [およびユーザーのコンテンツアクセス元が次の場合] : iOS
- ・ [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)



11.



作成したポリシールールを最上部にドラッグアンドドロップします。[次へ]をクリックします。

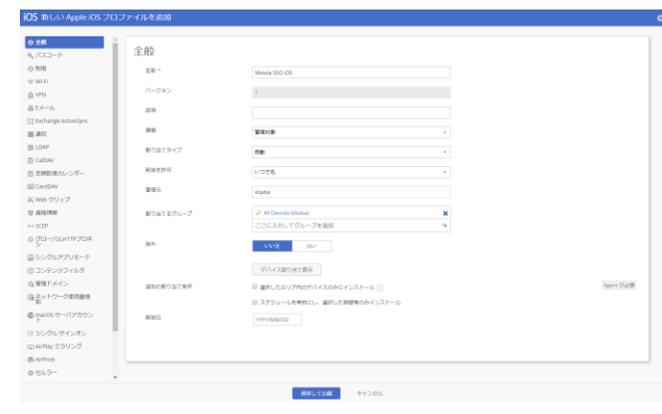
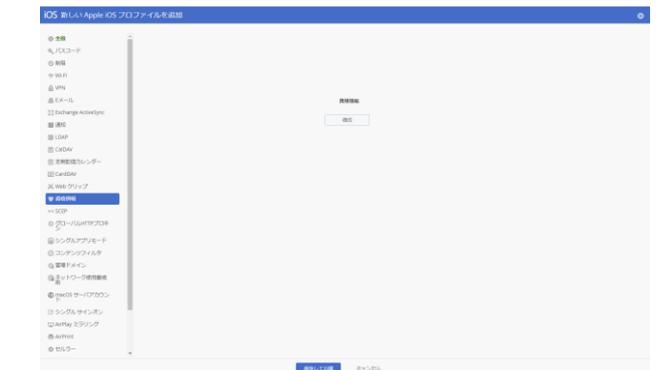
TIP :  
 ポリシールールは上段のものが優先されます。複数の認証ポリシーを構成している場合は要件に合わせて優先度を調整し、適切なポリシールールを構成してください。

12.



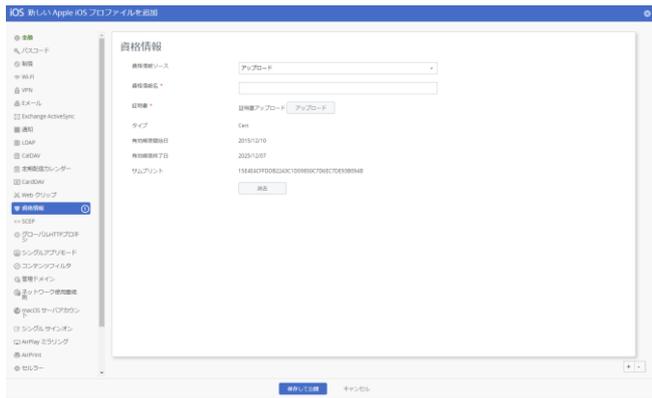
[保存] をクリックします。

つづいて 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。

<p>13.</p> 	<p>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。</p>
<p>14.</p> 	<p>[iOS]をクリックします。</p>
<p>15.</p> 	<p>[全般]ペイロードで以下を設定します。</p> <p>名前 : Mobile SSO iOS          割り当てるグループ : All Devices(テナント名)</p>
<p>16.</p> 	<p>[資格情報]ペイロードをクリックし、[構成]をクリックします。</p>



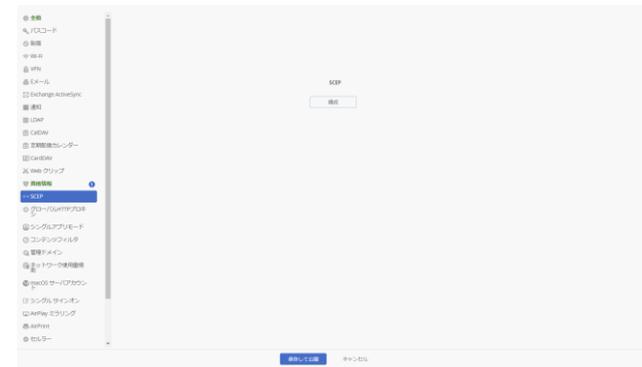
17.



[アップロード]をクリックし、ステップ7でダウンロードした KDC ルート証明書をアップロードします。

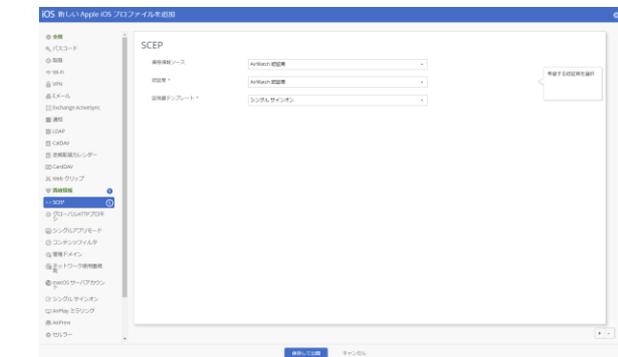
資格情報名に任意の名前を入力します。

18.



[SCEP]ペイロードをクリックし、[構成]をクリックします。

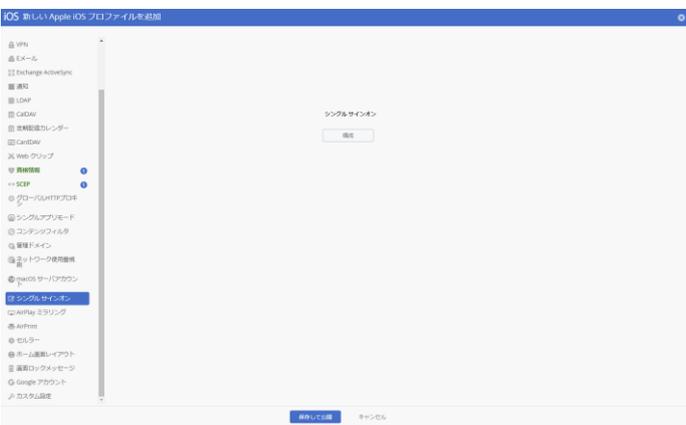
19.



以下のように設定を行います。

- 資格情報ソース : AirWatch 認証局
- 認証局 : AirWatch 認証局
- 証明書テンプレート : シングルサインオン

20.



[シングルサインオン]ペイロードをクリックし、[構成]をクリックします。

21.



以下のとおり設定を行います。

- 接続情報

アカウント名： <任意の管理名>

Kerberos プリンシパル名： {EnrollmentUser}を選択

レルム： VMWAREIDENTITY.ASIA

(VMware Identity Manager のドメイン名を記載)

更新証明書：“SCEP #1”を選択

- URL プレフィックス

URL： https://<テナント>.vmwareidentity.asia

22.



(続き) [シングルサインオン]ペイロードで以下のとおり設定します。

- アプリケーション

com.apple.mobilesafari

com.air-watch.appcenter

com.salesforce.chatter

TIP :

モバイル SSO の対象とするアプリケーションのアプリケーションバンドル ID を入力します。

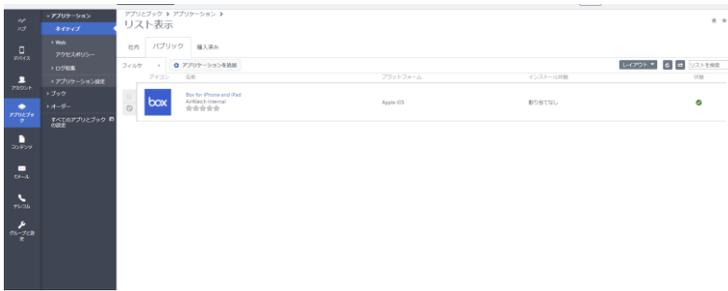
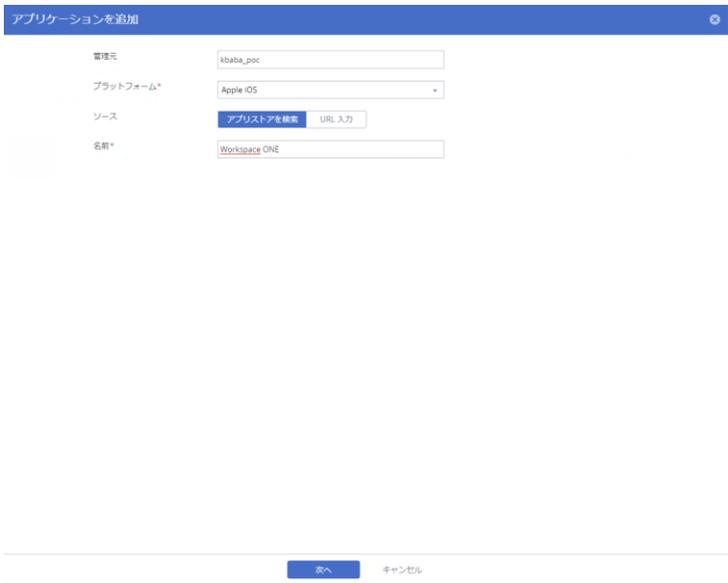
例： Safari でモバイル SSO 対象とする場合は Safari のアプリケーションバンドル ID (com.apple.mobilesafari) を入力します。

Workspace ONE App をモバイル SSO 対象とする場合は Workspace ONE App のアプリケーションバンドル ID (com.air-watch.appcenter) を入力します。

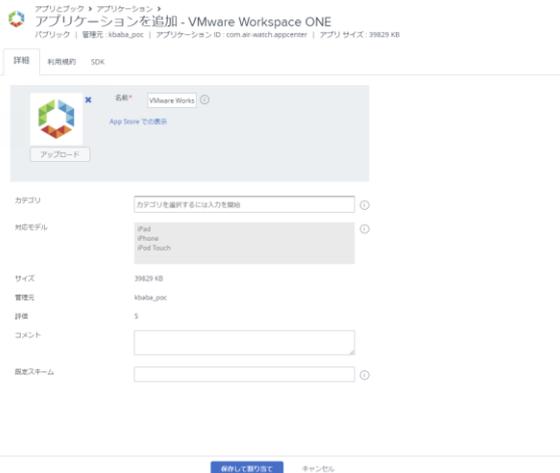
[保存して公開 / 公開]の順にクリックします。



## Workspace ONE App for iOS を構成します。

<p>23.</p> 	<p>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。</p>
<p>24.</p> 	<p>以下のとおり設定を行い、[次へ]をクリックします。</p> <p>プラットフォーム : Apple iOS          ソース : アプリストアを検索          名前 : Workspace ONE</p>
<p>25.</p> 	<p>VMware Workspace ONE の横の[選択]をクリックします。</p>

26.



[保存して割り当て]をクリックします。

27.



[割り当ての追加]をクリックします。

以下の設定を行います。

割り当てグループを選択: All Devices(テナント名)

アプリ配信方法: 自動

管理アクセス: 有効

加入解除時に削除: 有効

アプリケーション構成: 有効

以下の2行を記述する。

構成キー: AppServiceHost

値のタイプ: 文字列

構成値:

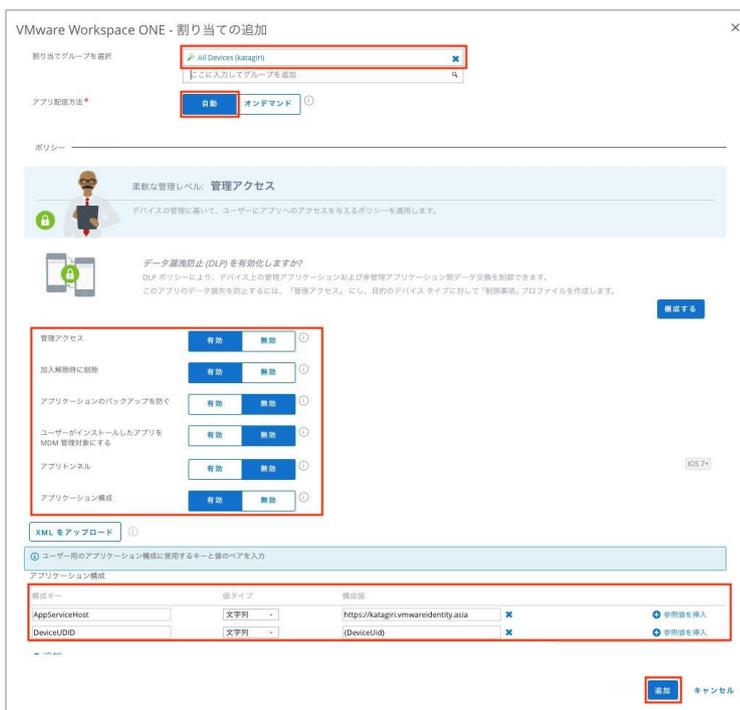
https://<テナント>.vmwareidentity.asia

構成キー: DeviceUDID

値のタイプ: 文字列

構成値: {DeviceUid}

[追加]をクリックします。

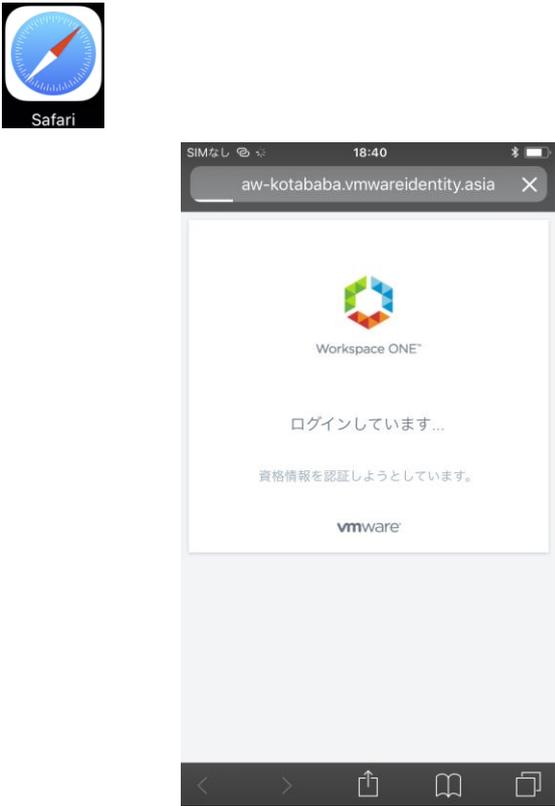


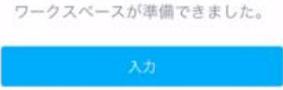


### 4.3 iOS デバイスで動作確認

iOS デバイスを使用して動作確認をします。

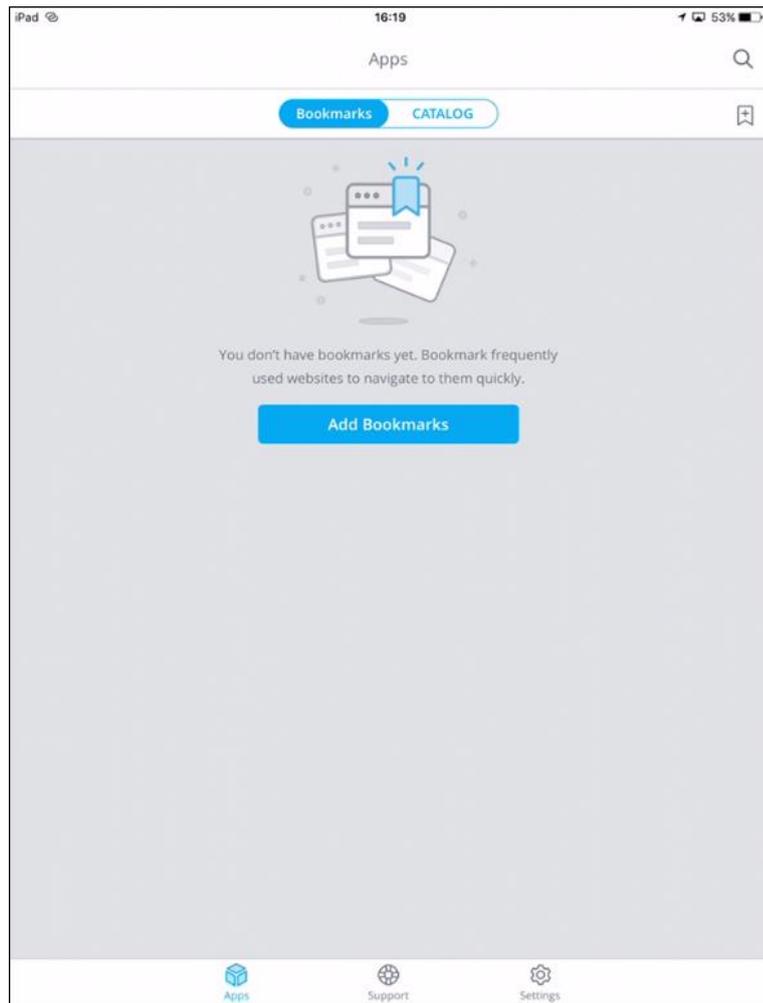
\* この手順は当該 iOS デバイスが AirWatch に正常に管理されている状態（加入状態）を前提としております。iOS デバイスが加入状態でない場合は加入操作の完了後に実施してください。

<p>1.</p> 	<p>iOS デバイスで Safari を使用して Workspace ONE のポータルにアクセスします。          ( <a href="https://&lt;テナント&gt;.vmwareidentity.asia">https://&lt;テナント&gt;.vmwareidentity.asia</a> )</p>
<p>2.</p> 	<p>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が完了し、Workspace ONE のポータルが開けることを確認します。</p>

<p>3.</p> 	<p>iOS デバイスで Workspace ONE App を起動します。</p> <p>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。</p>
<p>4.</p> 	<p>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。</p>
<p>5.</p> 	<p>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。</p>
<p>6.</p> 	<p>[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。</p>



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。

## 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。

<p>1.</p> 	<p>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。</p> <p>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</p>
<p>2.</p> 	<p>[ ID とアクセス管理 / 管理 / ID プロバイダ ]を開きます。[System Identity Provider] を選択し、認証方法で [デバイスコンプライアンス (Airwatch)]にチェックを入れ、[保存]をクリックします。</p>



2.

ポリシーの編集

定義

構成

サマリ

選択したアプリケーションへのアクセスに関するルールのリストを作成できます。ルールごとに、IP 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、認証方法、再認証までにユーザーがアプリケーションを使用できる最大時間数を選択します。

ネットワーク範囲	デバイスタイプ	認証	再認証
ALL RANGES	iOS	モバイル SSO (iOS 版)	8 時間
ALL RANGES	Web ブラウザ	パスワード(クラウドデ...	8 時間
ALL RANGES	Workspace ONE アプリ	Password+1	2160 時間
ALL RANGES	Web ブラウザ	Password+1	8 時間

ポリシールールを追加

キャンセル 前へ 次へ

VMware Identity Manager コンソールで[ ID とアクセス管理 / 管理 / ポリシー ]を開きます。

[ default\_access\_policy\_set ]を開きます。

手順 3.2 と同様に、ポリシールールの編集で構成タブまで進み、[モバイル SSO(iOS 版)]を編集します。

3.

ポリシー ルールの編集

ユーザーのネットワーク範囲が次の場合 ALL RANGES

ユーザーが次からコンテンツにアクセスする場合 iOS

また、ユーザーが次のグループに属する場合

グループを選択...

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。

このアクションを実行します

以下を認証に使用...

ユーザーは次を使用して認証することができます

モバイル SSO (iOS 版)

および

デバイスコンプライアンス (AirWatch)

先の方法が失敗するか適用できない場合、次を実行

フォールバック方法を選択...

フォールバック方法を追加

再認証までの待機時間

8 時間

高度なプロパティ

キャンセル 保存

以下の設定を行い、[OK]をクリックします。

[ユーザーは次を使用して認証することができません]行に追加の認証方法を追加するために[+]ボタンをクリックし、[デバイスコンプライアンス (AirWatch)]を選択します。

[保存]をクリックします。

4.

ポリシーの編集

定義

選択したアプリケーションへのアクセスに関するルールのリストを作成できます。ルールごとに、IP 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、認証方法、再認証までにユーザーがアプリケーションを使用できる最大時間を指定します。

ネットワーク範囲	デバイスタイプ	認証	再認証
ALL RANGES	iOS	モバイル SSO (iOS 版)+1	8 時間
ALL RANGES	Web ブラウザ	パスワード (クラウド ...)	8 時間
ALL RANGES	Workspace ONE アプリ	Password+1	2160 時間
ALL RANGES	Web ブラウザ	Password+1	8 時間

ポリシールールを追加

キャンセル 前へ 次へ

ポリシーの編集

定義

名前  
default\_access\_policy\_set

説明  
Default access policy set

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 1  
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 iOS 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** に属しています  
ユーザーは **モバイル SSO (iOS 版) & デバイスコンプライアンス (AirWatch)** を使用して認証を行うことができます  
8 時間後に再認証します  
高度なプロパティ

ポリシールール 2  
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 Web ブラウザ 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** に属しています  
ユーザーは **パスワード (クラウド デプロイ)** を使用して認証を行うことができます  
8 時間後に再認証します  
高度なプロパティ

ポリシールール 3  
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** に属しています  
ユーザーは **Password** を使用して認証を行うことができます

キャンセル 前へ 保存

[次へ] → [保存]ボタンをクリックし、ポリシーの編集を完了します。

5.

デバイス > 順守ポリシー > リスト表示

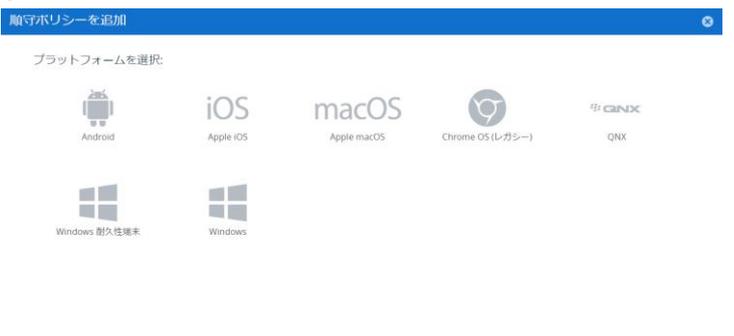
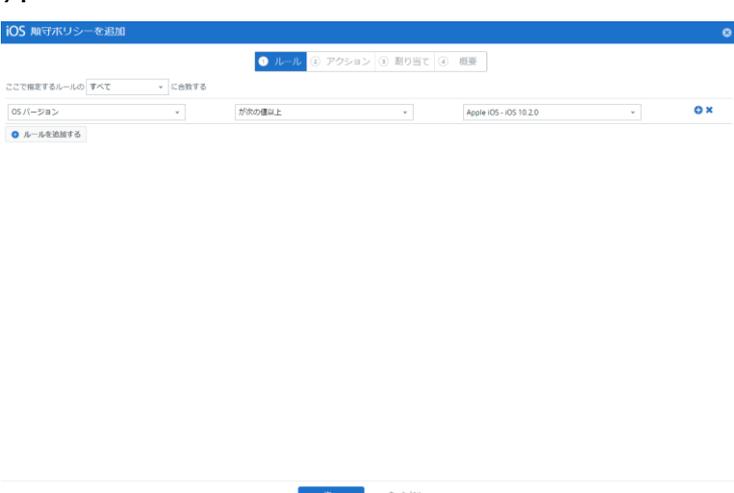
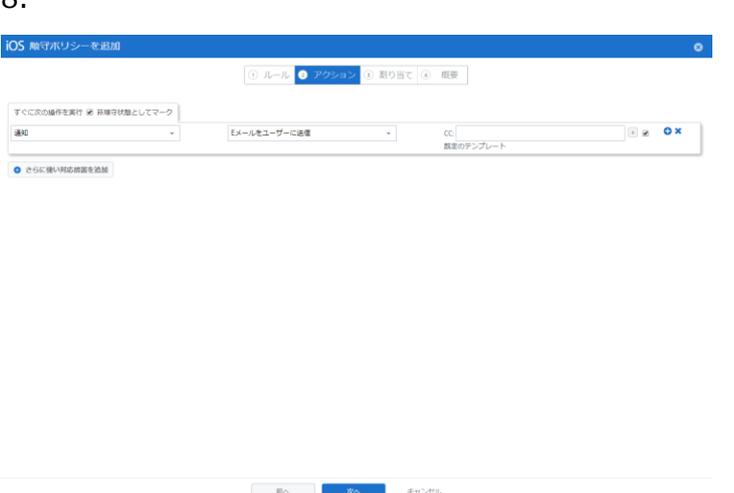
追加

有効	名前	説明	管理元
----	----	----	-----

レコー

テストの為に企業が設定したセキュリティ基準を満たしていないデバイスの状態（非順守状態）を作成します。ここでは iOS が最新の場合は非順守状態という趣旨の順守ポリシーを構成して

ます。AirWatch コンソールで[デバイス / 順守ポリシー / リスト表示] 開き、[追加]をクリックします。

<p>6.</p> 	<p>[iOS]をクリックします。</p>
<p>7.</p> 	<p>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。</p>
<p>8.</p> 	<p>[次へ]をクリックします。</p>

9.

以下の設定を行い、[次へ]をクリックします。

割り当てるグループ : All Devices(ssagawa)

10.

[完了してアクティブ化]をクリックします。

11.

テストに使用するデバイスが[ 順守違反 ]となることを確認します。



12.

テストの為に再認証までの時間を短縮します。  
Identity Manager の管理コンソールで、モバイル SSO を使用するポリシールールを編集します。

以下の設定を行い [OK / 保存]をクリックします。

再認証までの待機時間：1 分

13.



Safari を起動し、Identity Manager の URL へ接続し、ログインできなくなっていることを確認します。

以上で、AirWatch の管理状態を見てアクセス制御を行うデバイスコンプライアンスの機能確認ができました。

14.

デバイス > 順守ポリシー > リスト表示

追加

有効	名前	説明
●●	OSバージョン	OSバージョン

項目 1-1 / 1

構成 ポリシー ルールの編集

- ユーザーのネットワーク範囲が次の場合: ALL RANGES
- ユーザーが次からコンテンツにアクセスする場合: IOS
- また、ユーザーが次のグループに属する場合: グループを選択...

このアクションを実行します: 以下を認証に使用...  
モバイル SSO (iOS 版)

および: デバイスコンプライアンス (AirWatch)

先の方法が失敗するか適用できない場合、次を実行: フォールバック方法を選択...  
フォールバック方法を追加

再認証までの待機時間: 8 時間

高度なプロパティ

キャンセル 保存

テストの為にいった設定を元に戻します。

AirWatch 管理コンソール上で、作成した順守ポリシーの緑色の隣のアイコンをクリックし、無効にします。

Identity Manager で設定した再認証までの待機時間を 8 時間に戻します。



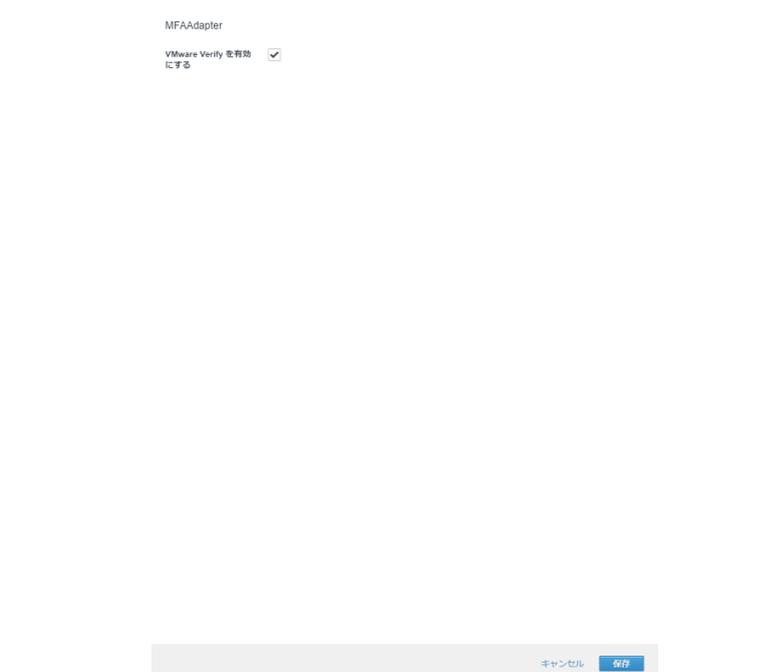
## 6 VMware Verify を使用した多要素認証の構成

### 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。

<p>1.</p>  <table border="1"> <thead> <tr> <th>認証方法</th> <th>構成</th> <th>ステータス</th> </tr> </thead> <tbody> <tr> <td>AuthNash 外部アクセス トークン</td> <td>?</td> <td>無効</td> </tr> <tr> <td>デバイス登録シリアル番号 (AuthNash)</td> <td>?</td> <td>無効</td> </tr> <tr> <td>パスワード (AuthNash Connector)</td> <td>?</td> <td>無効</td> </tr> <tr> <td>VMware Verify</td> <td>?</td> <td>無効</td> </tr> <tr> <td>モバイル SSO (iOS 版)</td> <td>?</td> <td>無効</td> </tr> <tr> <td>パスワード (ローカル ディレクトリ)</td> <td>?</td> <td>無効</td> </tr> <tr> <td>モバイル SSO (Android 版)</td> <td>?</td> <td>無効</td> </tr> <tr> <td>証明書 (クラウド デプロイ)</td> <td>?</td> <td>無効</td> </tr> </tbody> </table>	認証方法	構成	ステータス	AuthNash 外部アクセス トークン	?	無効	デバイス登録シリアル番号 (AuthNash)	?	無効	パスワード (AuthNash Connector)	?	無効	VMware Verify	?	無効	モバイル SSO (iOS 版)	?	無効	パスワード (ローカル ディレクトリ)	?	無効	モバイル SSO (Android 版)	?	無効	証明書 (クラウド デプロイ)	?	無効	<p>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。</p> <p>[ VMware Verify ] 行の構成ボタンをクリックします。</p>
認証方法	構成	ステータス																										
AuthNash 外部アクセス トークン	?	無効																										
デバイス登録シリアル番号 (AuthNash)	?	無効																										
パスワード (AuthNash Connector)	?	無効																										
VMware Verify	?	無効																										
モバイル SSO (iOS 版)	?	無効																										
パスワード (ローカル ディレクトリ)	?	無効																										
モバイル SSO (Android 版)	?	無効																										
証明書 (クラウド デプロイ)	?	無効																										
<p>2.</p>  <p>MFAAdapter</p> <p>VMware Verify を有効にする <input checked="" type="checkbox"/></p> <p>キャンセル 保存</p>	<p>[ VMware Verify を有効化する ] にチェックを入れ、[ 保存 ] ボタンをクリックします。</p>																											

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 ]を開き、[System Identity Provider]をクリックします。

4.



認証方法で、VMware Verify が有効になっていることを確認します。有効になっていない場合は、[認証方法を関連付ける]のチェックを有効にし、[保存]をクリックします。

5.



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。

6.



手順 3.2 と同様に、ポリシールールの編集で構成タブまで進み、デバイスタイプが[Web ブラウザ]になっている列の認証方法のリンクをクリックします。デバイスタイプが Web ブラウザのものがない場合はポリシールールを追加してください。



7.

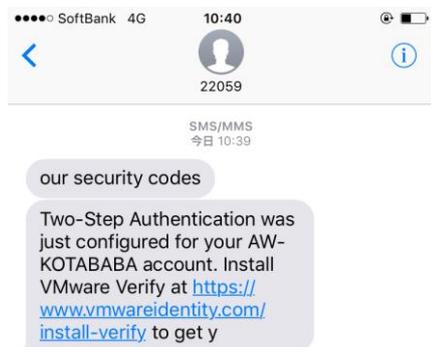
以下の設定を行い、[保存]をクリックします。

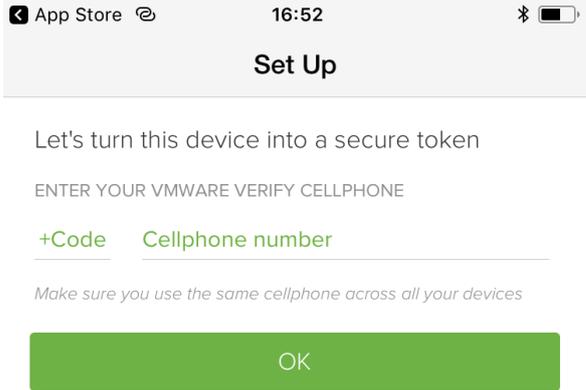
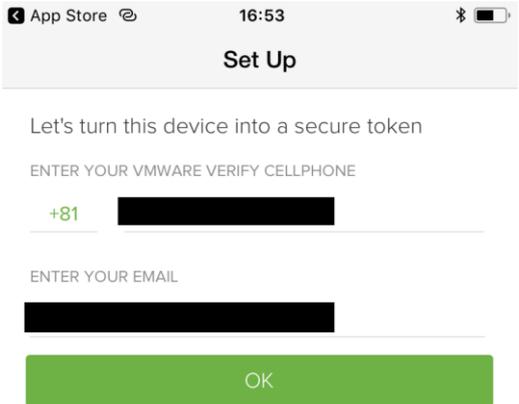
- ユーザーのネットワーク範囲が次の場合：  
すべての範囲
- また、ユーザーのコンテンツ アクセス元が次の場合：  
Web ブラウザ
- ユーザーは次を使用して認証することができます：  
パスワード (クラウドデプロイ)  
および：VMware Verify
- 先の方法が失敗するか適用できない場合は、  
次を実行：  
パスワード (ローカルディレクトリ)

8.

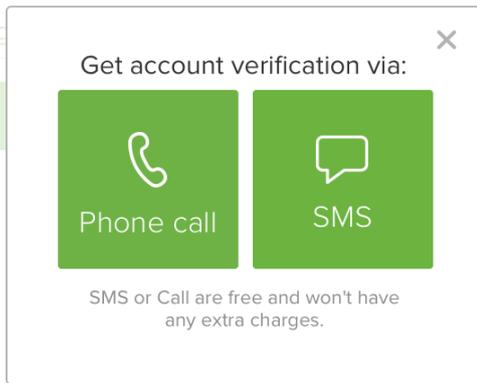
[保存]をクリックし、ポリシーの編集を完了します。

VMware Verify アプリのセットアップを実施します。

<p>9.</p> 	<p>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。</p>
<p>10.</p> 	<p>(はじめて VMware Verify 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。</p> <p>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+81 7011112222 の形式で入力する必要はありません。</p>
<p>11.</p> 	<p><u>スマートフォン上の作業</u></p> <p>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。</p>

<p>12.</p> 	<p><u>スマートフォン上の作業</u></p> <p>指示に従ってインストールを実施します。</p>
<p>13.</p> 	<p><u>スマートフォン上の作業</u></p> <p>VMware Verify アプリを起動します。</p> <p>電話番号を入力します。</p>
<p>14.</p> 	<p><u>スマートフォン上の作業</u></p> <p>E メールアドレスの入力欄が出てきた場合には、E メールアドレスを入力します。</p> <p>[ OK ]ボタンをタップします。</p>

15.



スマートフォン上の作業

[ SMS ]を選択します。

16.

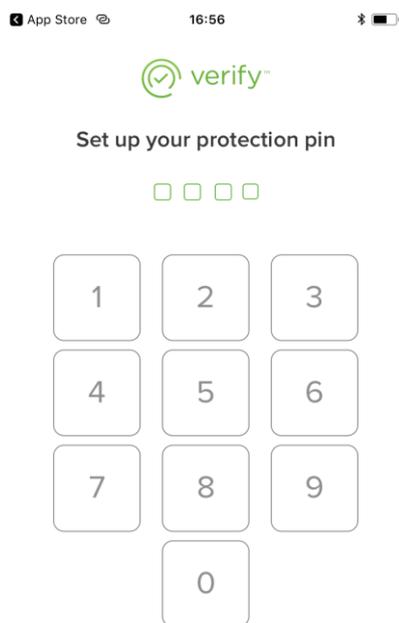


To finish registering VMware Verify click: [vmverify://register/81-703-190-7428/693085](https://vmverify://register/81-703-190-7428/693085) or manually enter: [693085](https://vmverify://register/81-703-190-7428/693085)

スマートフォン上の作業

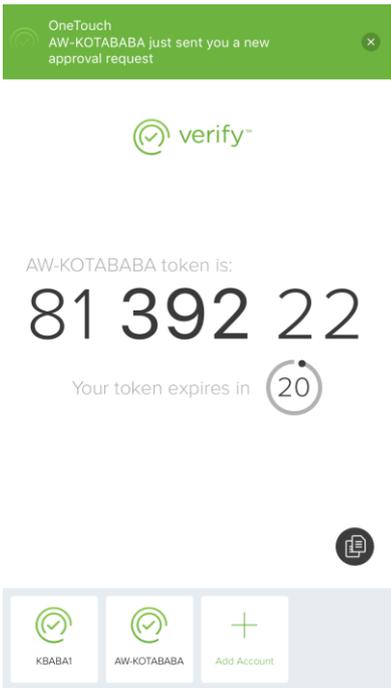
VMware Verify をアクティベーションするためのリンクが SMS で届くので開きます。

17.



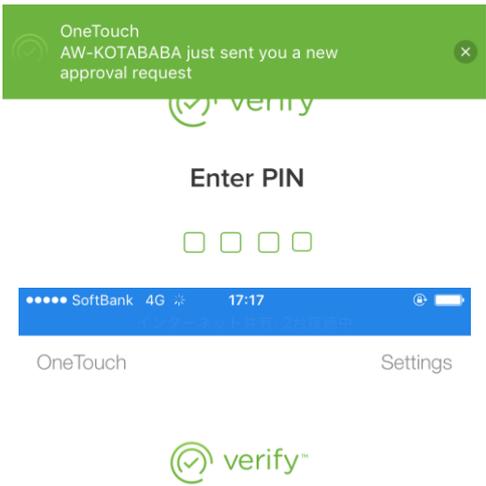
スマートフォン上の作業

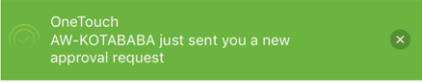
VMware Verify を保護するための PIN を設定します。

<p>18.</p>  <p>OneTouch AW-KOTABABA just sent you a new approval request</p> <p>verify</p> <p>AW-KOTABABA token is: <b>81 392 22</b></p> <p>Your token expires in 20</p> <p>KBABAI AW-KOTABABA Add Account</p>	<p>スマートフォン上の作業</p> <p>トークンが表示されることを確認します。</p>
<p>19.</p>  <p>Workspace ONE</p> <p>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</p> <p>8139222</p> <p>ログイン</p> <p>VMware Verify に問題がある場合</p> <p>SMS でログイン</p> <p>vmware</p>	<p>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。</p>
<p>20.</p>  <p>Workspace ONE</p> <p>すべてのアプリ</p> <p>まだアプリが更新されていないようです。まもなく更新されますので、後で確認ください。</p>	<p>Workspace ONE へのブラウザからのログインが設定できました。</p> <p>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。</p>

初回セットアップ完了後の動作を確認します。

<p>22.</p> 	<p>画面右上のユーザーをクリックし、[ログアウト]をクリックします。</p>
<p>23.</p> 	<p>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。</p>
<p>24.</p> 	<p>認証が VMware Verify 待機状態になることを確認します。</p>

<p>25.</p> 	<p><u>スマートフォン上の作業</u></p> <p>VMware Verify に認証要求の通知が届くので VMware Verify を起動します。</p>
<p>26.</p> 	<p><u>スマートフォン上の作業</u></p> <p>初回セットアップ時に設定した PIN もしくは Touch ID で VMware Verify のロックを解除します。</p>
<p>27.</p> 	<p><u>スマートフォン上の作業</u></p> <p>アプリ上部に表示される認証要求通知、もしくは [ OneTouch ] ボタンをタップします。</p>

<p>28.</p>  <p>VMware Identity Manager からのログイン要求。 24s ago</p> <p>Expires in 23h</p>	<p><u>スマートフォン上の作業</u></p> <p>認証要求を開きます。</p>
<p>29.</p>   <p>VMware Identity Manager からのログイン要求。</p> <p>Please verify the information below. If you did not initiate this request, just click deny.</p> <p><b>Subject:</b> 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</p> <p><b>Date:</b> 4月 17, 2018 at 10:49</p> <p>Approve Deny</p>	<p><u>スマートフォン上の作業</u></p> <p>認証要求の内容を確認し[ Approve ]ボタンで承認します。</p>
<p>30.</p> 	<p>ブラウザからの Workspace ONE へのログインが完了することが確認できました。</p> <p>以上で VMware Verify を用いた 2 要素認証は完了です。</p>

## 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 へ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

<p>1.</p> 	<p>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 ]を開き、[System Identity Provider]をクリックします。</p>
<p>2.</p> 	<p>以下の設定を行い、[保存]をクリックします。</p> <p>ID プロバイダ名 : Buit-in_ドメイン名 へ変更          ユーザー :          [システムディレクトリ]のチェックを<b>オフ</b>          認証方法 : パスワード (ローカルディレクトリ)のチェックを<b>オン</b></p> <p>残りの設定はそのままにします。</p>

3.

IDプロバイダ名	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
Built-in_AWJPN	モバイル SSO (OS 版) デバイスコンプライアンス (AirWatch) パスワード (クラウド デプロイ) VMware Verify	AWJPN	すべての範囲	aws.zajpn.lan	組み込み
Built-in	パスワード (ローカル ディレクトリ)	システム ディレクトリ		aws.zajpn.lan	組み込み
WorkspaceOP_1149	Password	AWJPN	すべての範囲	aws.zajpn.lan	Identity Manager

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 ]を開き、[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。

4.

IDプロバイダ名: Built\_in\_SystemDomain

ユーザー: この IDP を使用して認証できるユーザーを選択します。以下のリストにある利用可能なディレクトリから選択します。  
 システム ディレクトリ  
 AWJPN

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します。次の利用可能なネットワーク範囲から選択します。  
 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	認証方法を無効化する
デバイス コンプライアンス (AirWatch)	<input type="checkbox"/>
VMware Verify	<input type="checkbox"/>
モバイル SSO (OS 版)	<input type="checkbox"/>
パスワード (ローカル ディレクトリ)	<input checked="" type="checkbox"/>

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ための KDC サーバのルート証明書をエクスポートします。

追加 キャンセル

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.



VMware Identity Manager 管理コンソールからログアウトします。

6.

Workspace ONE®

ユーザー名 \_\_\_\_\_

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

vmware

VMware Identity Manager 管理コンソールへアクセスし、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。

以上で設定は完了です。これにより <https://<テナント>.vmwareidentity.asia/> へアクセスすれば、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](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-airwatch-identity-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/UCVMfQCwJaNRI1tWyw8EZTTQ>



VMware株式会社