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

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

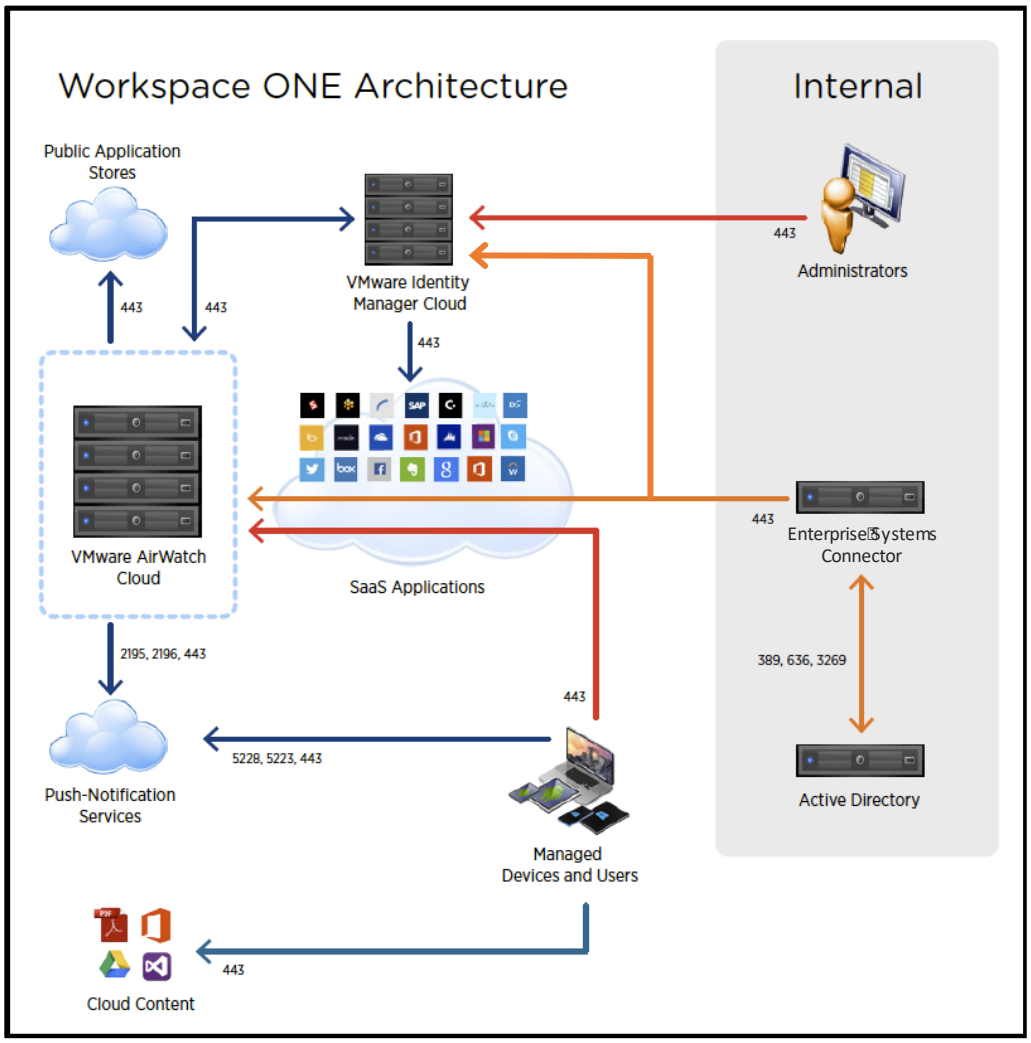
はじめに

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

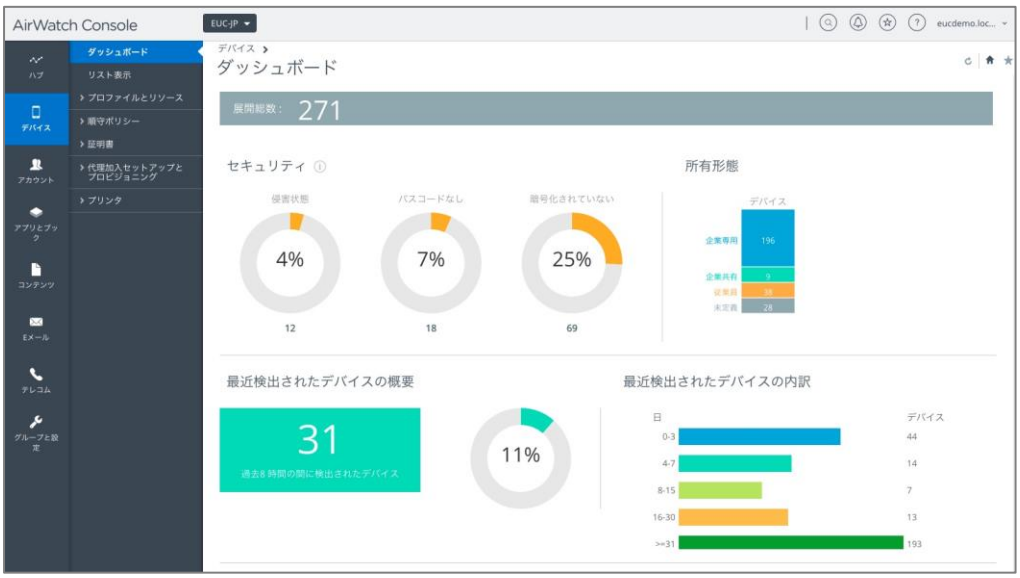
1.2 各コンポーネントのご紹介

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。

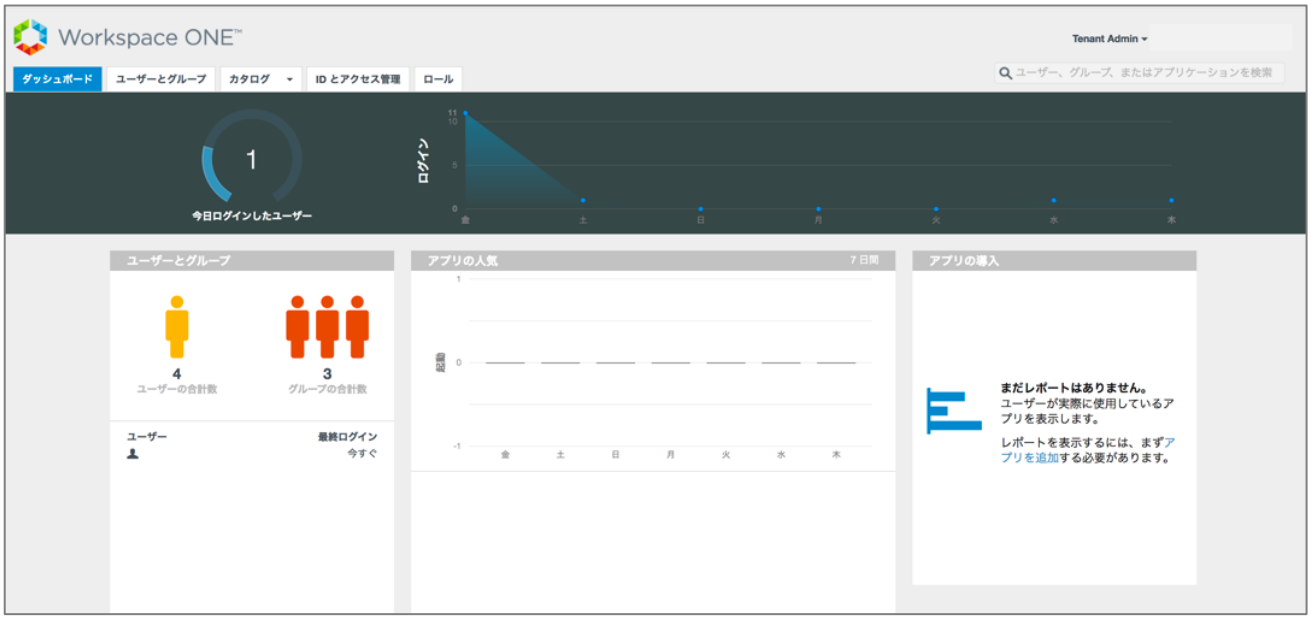
AirWatch ではこれらの機能を下図のような、包括的なコンソールである AirWatch Console を用いて、一元的に管理および運用を実施します。



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



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。

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。

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。

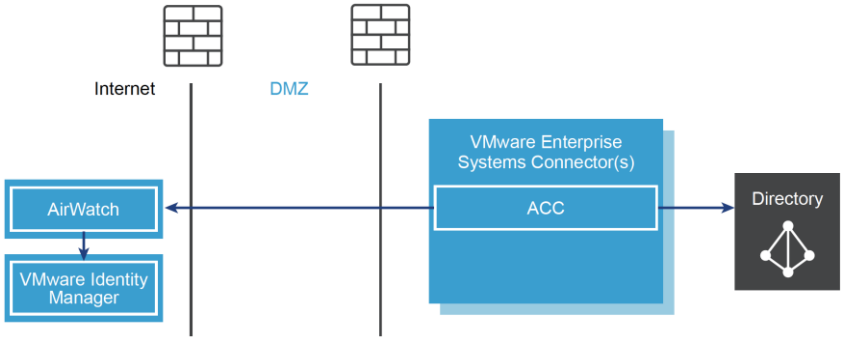
章	章題	目的
2	VMware Enterprise Systems Connector による環境の統合	VMware Identity Manager および AirWatch に対して企業内の Active Directory との連携を構成し、ユーザ管理を AD で一元管理する場合に実施します。
3	ディレクトリユーザを使用したパスワード認証の構成	ブラウザーベースでのアクセスや AirWatch で管理していないデバイスから、Active Directory の認証情報を使用した認証を構成する場合に実施します
4	iOS デバイス用モバイル SSO の構成	iOS デバイスからモバ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

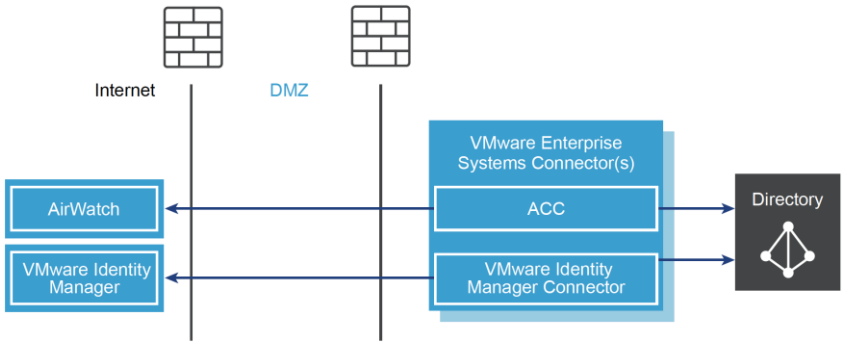
2.1 本章のゴール

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

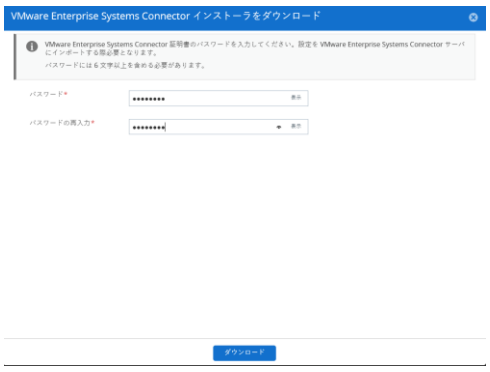
VMware Enterprise Systems Connector をインストールするための Windows マシンがあること。
サポートされる Windows 環境は以下の通り。

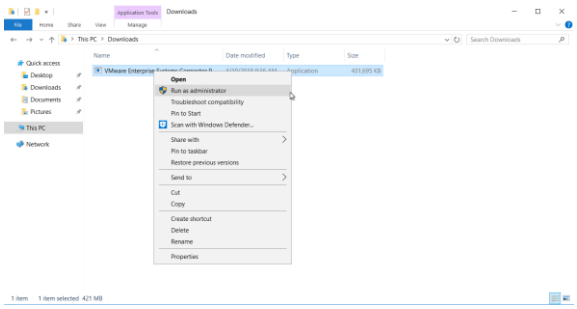
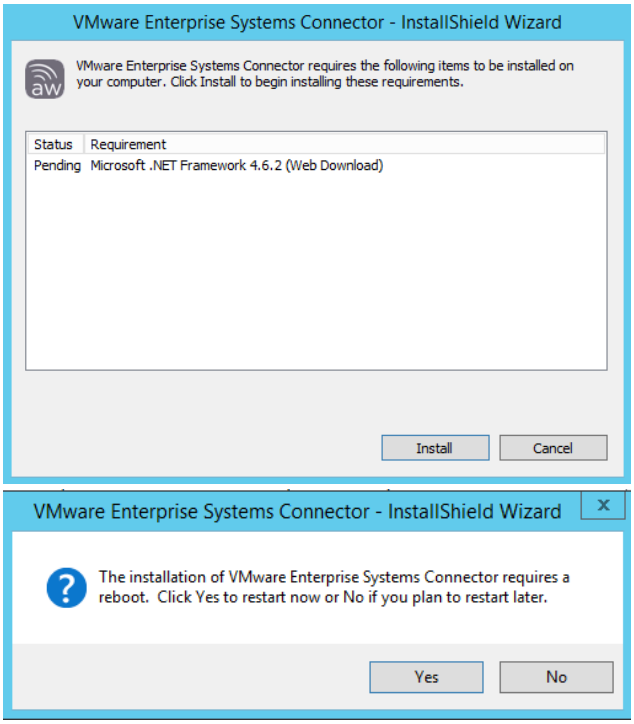
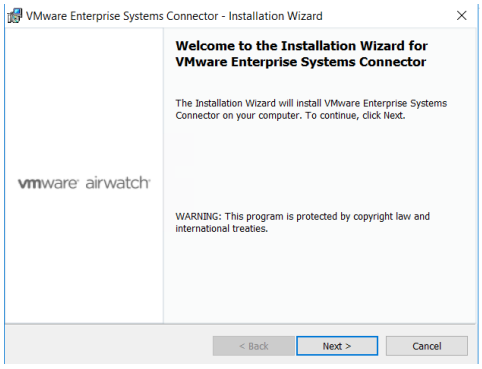
- Windows Server 2008R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- 連携対象の Active Directory ドメインに参加済み
- 英語版 OS を使用

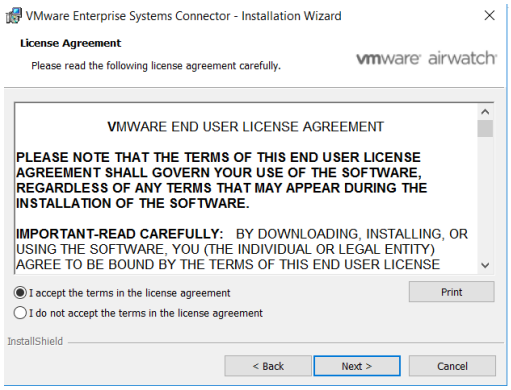
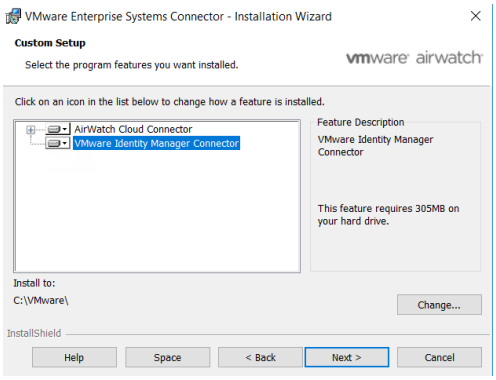
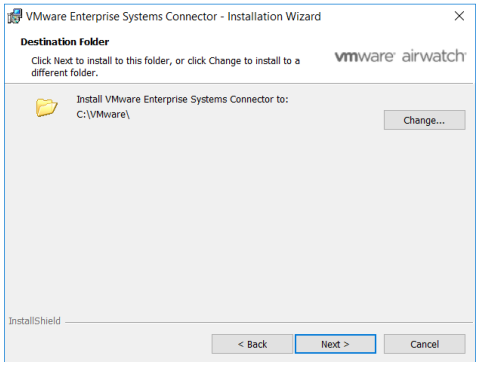
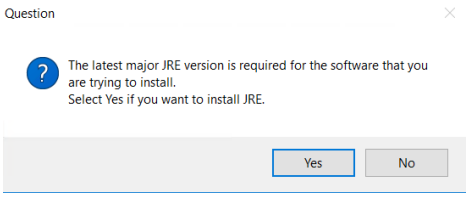
2.3 設定手順

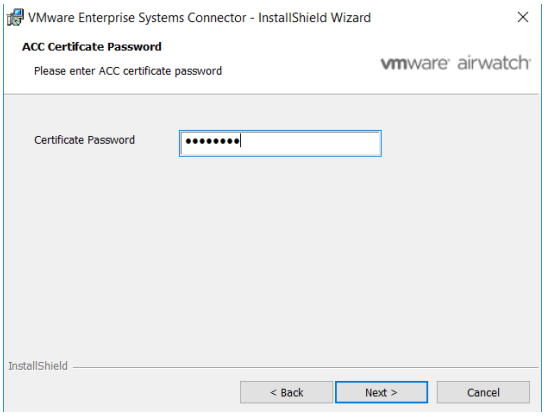
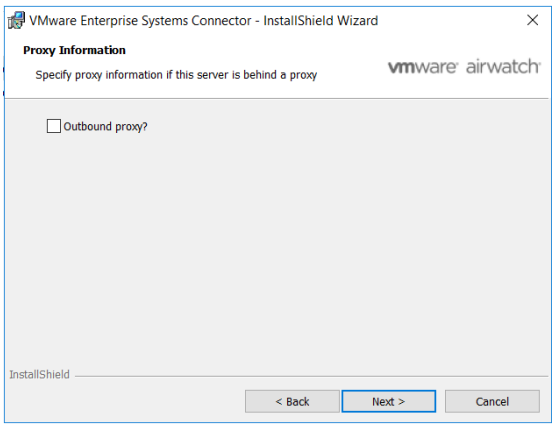
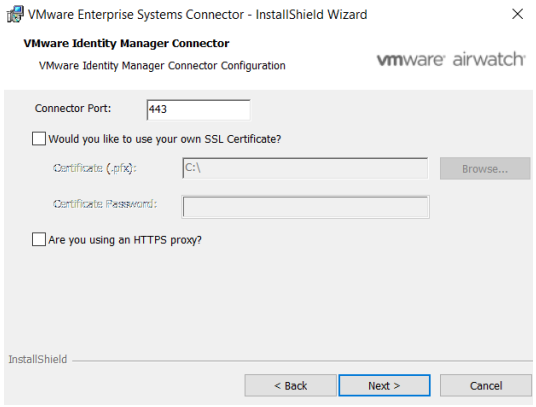
2.3.1 VMware Enterprise Systems Connector のインストールと設定

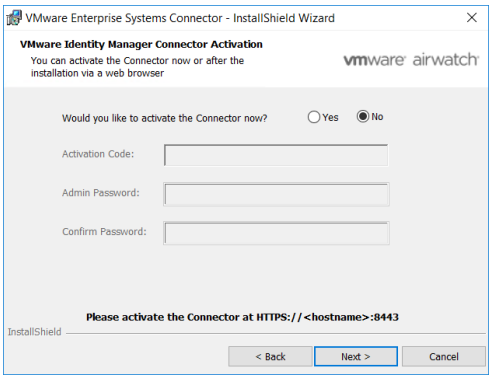
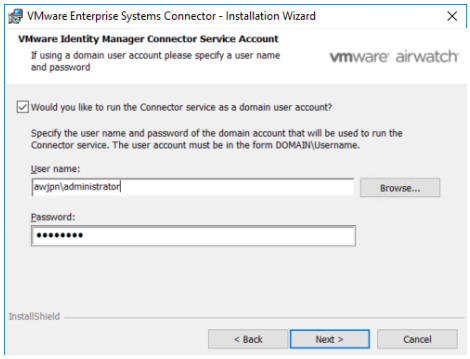
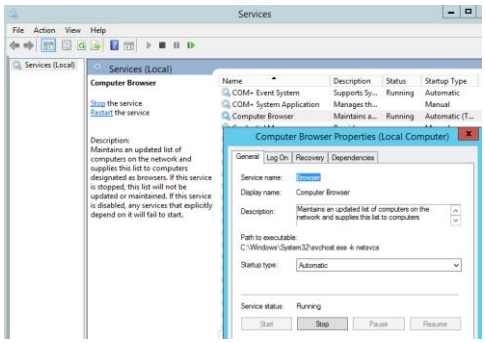
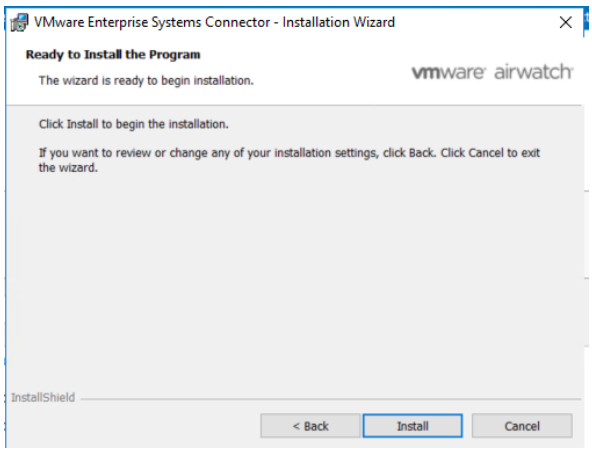
VMware Enterprise Systems Connector をインストールします。

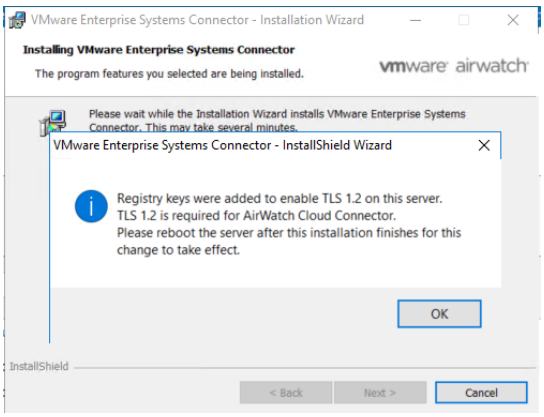
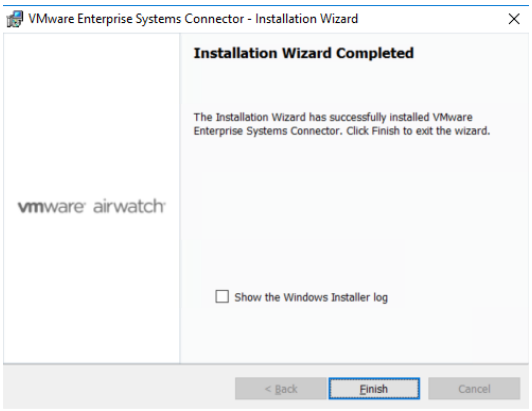
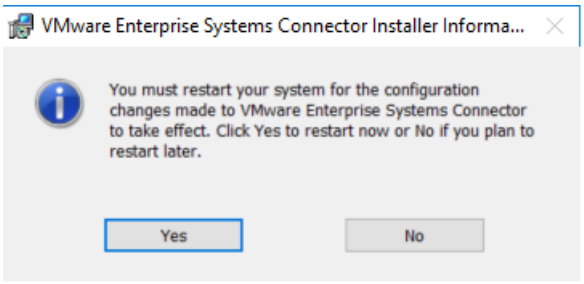
1. 	ESC のマシンからブラウザで AirWatch コンソールへログインし、[グループと設定 / すべての設定 / システム / エンタープライズ統合 / VMware Enterprise Systems Connector]の順にクリックします。
2. 	「現在の設定」でオーバーライドを選択し、[VMware Enterprise Systems Connector を有効化]にチェックを入れ、[保存]をクリックします。 その後、[VMware Enterprise Systems Connector インストーラをダウンロード]リンクをクリックします。
3. 	ダウンロード用のパス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

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。

7. 	使用許諾に同意し、[Next]をクリックします。
8. 	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。
9. 	インストール先フォルダを指定し、[Next]をクリックします。
10. 	JRE のインストールが求められたら、[Yes]をクリックします。

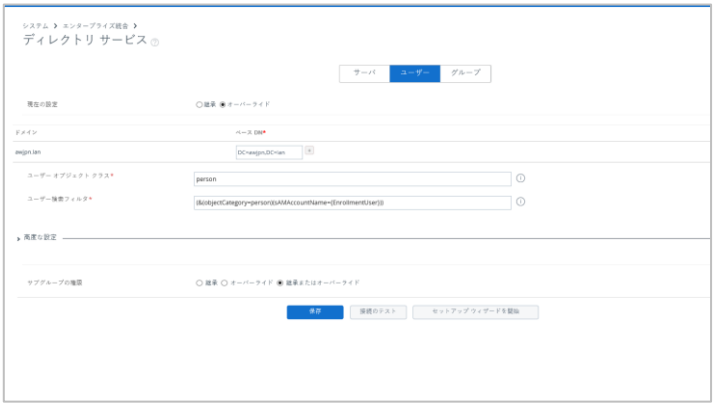
11.  	インストーラのダウンロード時に設定したパスワードを入力し、[Next]をクリックします。
12.  	[Next]をクリックします。 サーバが外部へ接続するのにプロキシを経由する場合は、プロキシの情報を入力します。 ＊ この画面で設定するプロキシは ACC コンポーネント用の設定になります。プロキシを使用する場合には次の画面で VIDM Connector コンポーネント用のプロキシ設定も実施してください。
13.  	[Would you like to use your own SSL Certificate?]のチェックを外し、[Next]をクリックします。 ＊ この画面で設定するプロキシは 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。

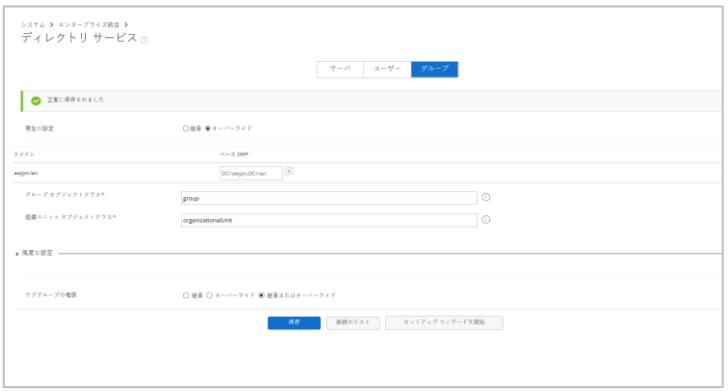
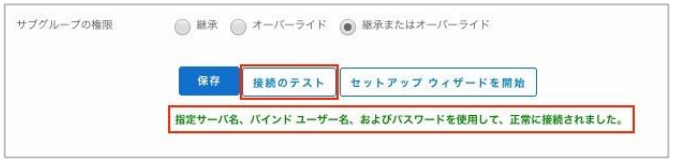
14.  	ここではチェックを入れずに[Next]をクリックします。
15.   	サービスを起動するためのドメインアカウントを手入力します。 認証に問題がない場合、Install に進めます。 （注）Windows Server 2016 では Computer Browser サービスが存在しないため、ドメインアカウントは手入力する必要があります。 Windows Server 2012 R2 以前のバージョンでは、[Browse]をクリックし、参照することが可能です。ただし、認証に失敗する場合は以下を確認して下さい。 ・ESC サーバー上で Computer Browser サービスが有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。

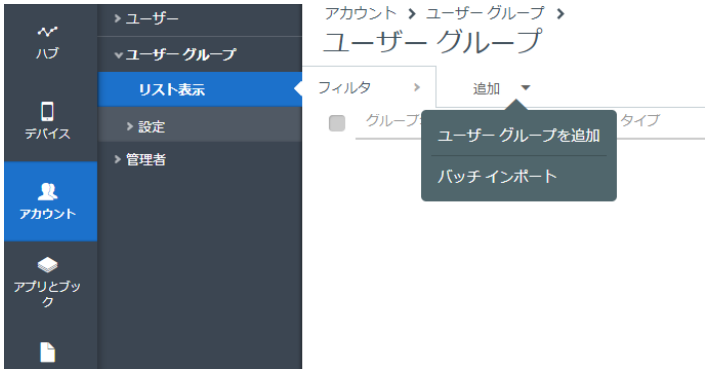
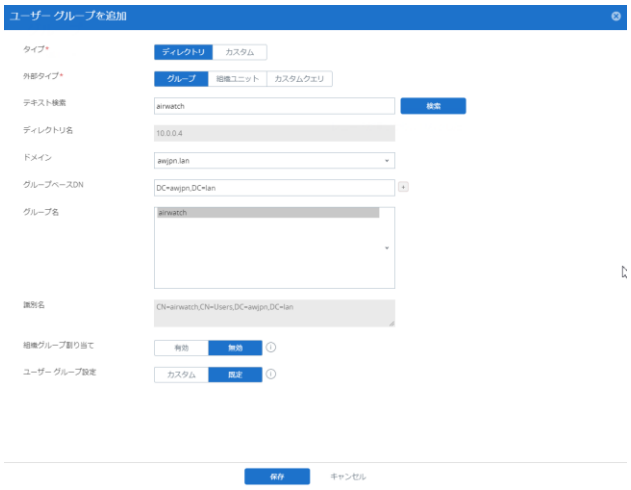
2.3.2 AirWatch と Active Directory の連携設定

VMware Enterprise Systems Connector 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 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。

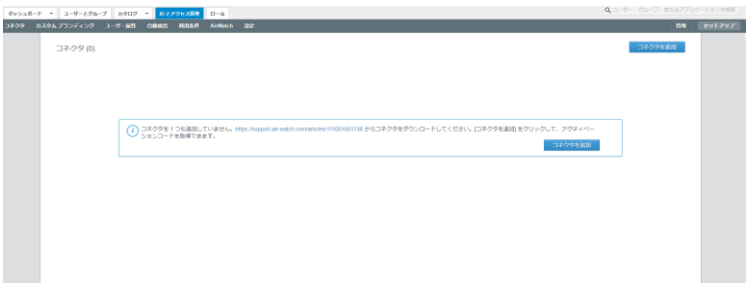
3.   	画面上部で[グループ]タブをクリックし、ベース DN を設定します。ベース DN は [+]ボタンをクリックすることで参照できます。 設定完了後、 [保存]をクリックし、エラーなく保存できることを確認します。 [接続のテスト]をクリックし、AD との接続に問題ないことを確認します。

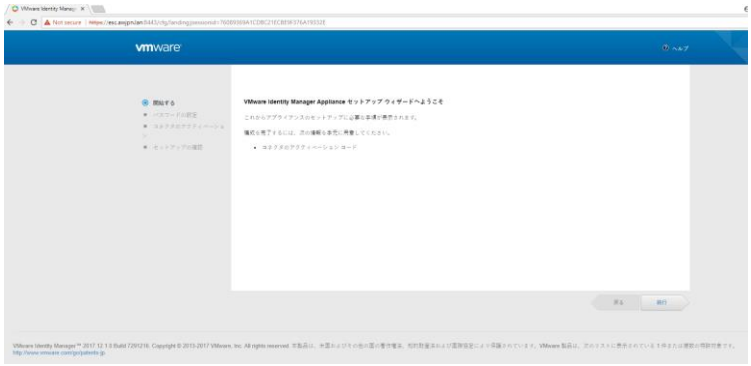
AD との連携が正しくできていることを確認するために、AirWatch へ AD 上のグループとユーザーを登録します。（事前に AD 上にグループを作成しユーザーを追加してください。）

4. 	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。
5. 	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：<*https://**xxx**.vmwareidentity.asia*> （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.   	[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。

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

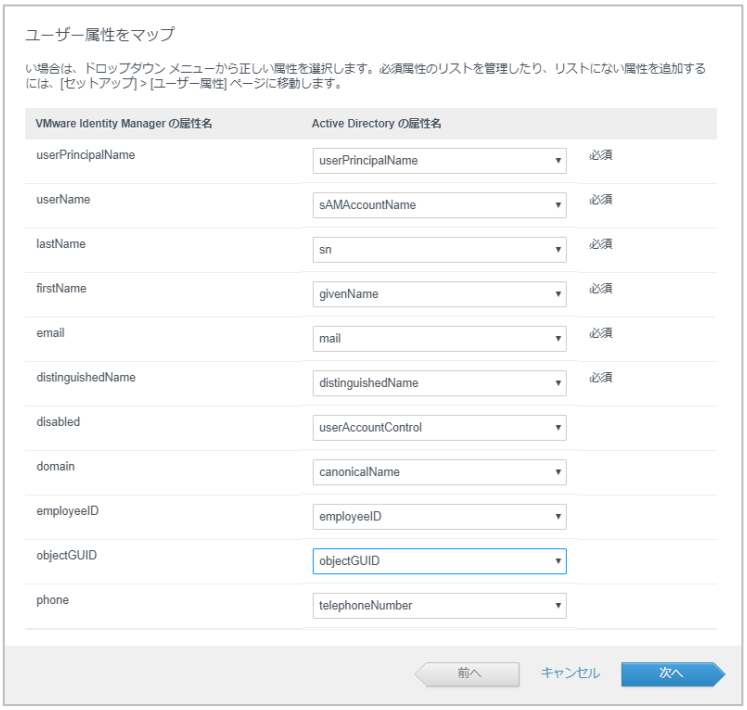
Identity Manager と Active Directory の連携設定を行います。

1.  	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 *userPricipalName* と *distinguishedName* 属性を必須に設定します。
2.  	[使用するその他の属性を追加]に[*objectGUID*]属性を追加します。 保存をクリックします。
3.  	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。 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。

<table>
<tr>
<td>4.
 
</td>
<td>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</td>
</tr>
<tr>
<td>5.
 
</td>
<td>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。</td>
</tr>
</table>

6.



[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.

[+]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.  	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.  	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. 	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。
14.  	[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。

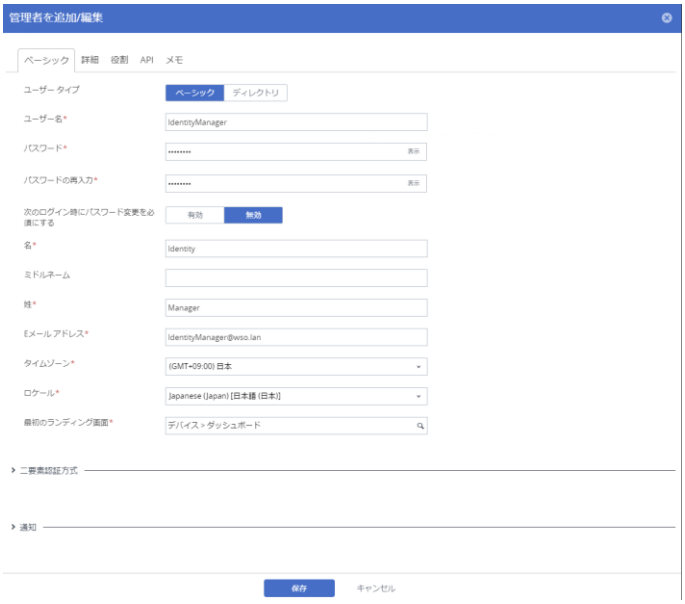
1. 	Identity Manager の管理コンソールへアクセスし、[ID とアクセス管理 / 管理 / ID プロバイダ]の順にクリックします。 タイプが組み込みの ID プロバイダ名をクリックします。本書では[System Identity Provider]です。
2. 	以下の設定をします。（次項に続く） ユーザー：システムディレクトリからチェックを外し、ドメインを選択 コネクタ：設定したコネクタをドロップダウンリストから選択し、[コネクタを追加]をクリック
3. 	以下の設定をし、[保存]をクリックします。 コネクタ認証方法：パスワード（クラウドデプロイ）にチェック 以上でアウトバウンドモードの設定は完了です。

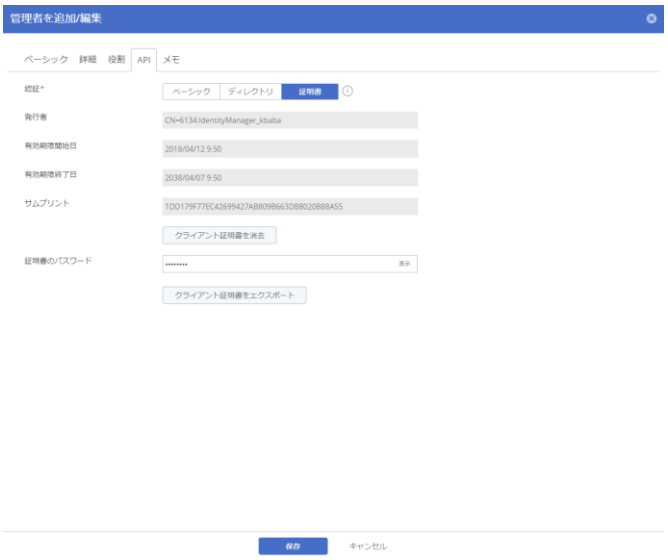
2.3.6 AirWatch と VMware Identity Manager の統合

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. 	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[*Identity Manager Admin*]、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[*Identity Manager User*]、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. 	[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.  	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。

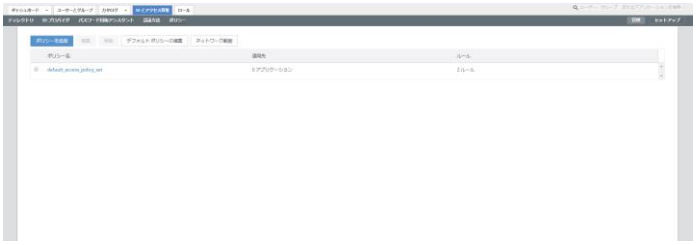
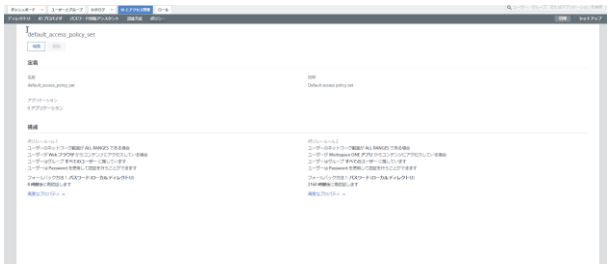
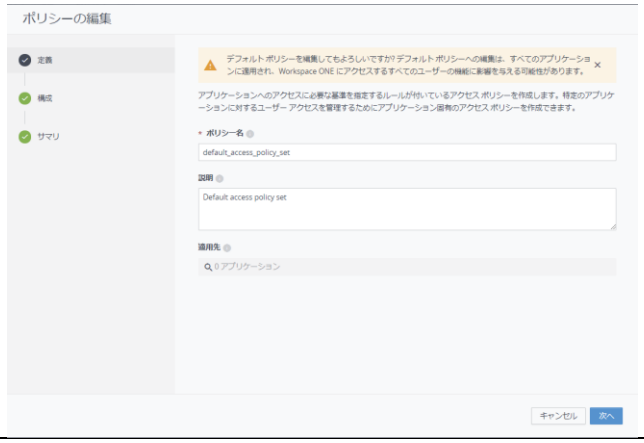
10.  	続いて以下の設定を行います。 統合カタログ：有効 [保存]を実行。

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

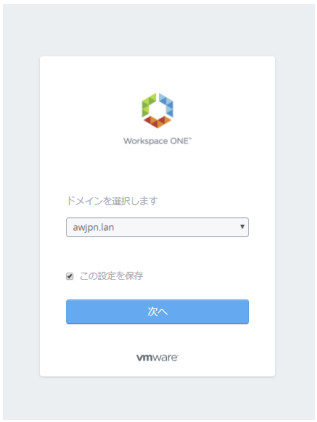
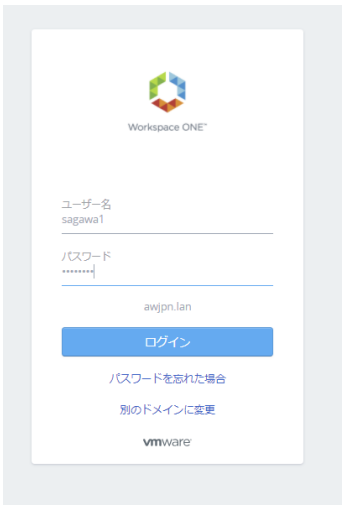
3.1 本章のゴール

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

1. 	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. 	[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[次へ]をクリックします。

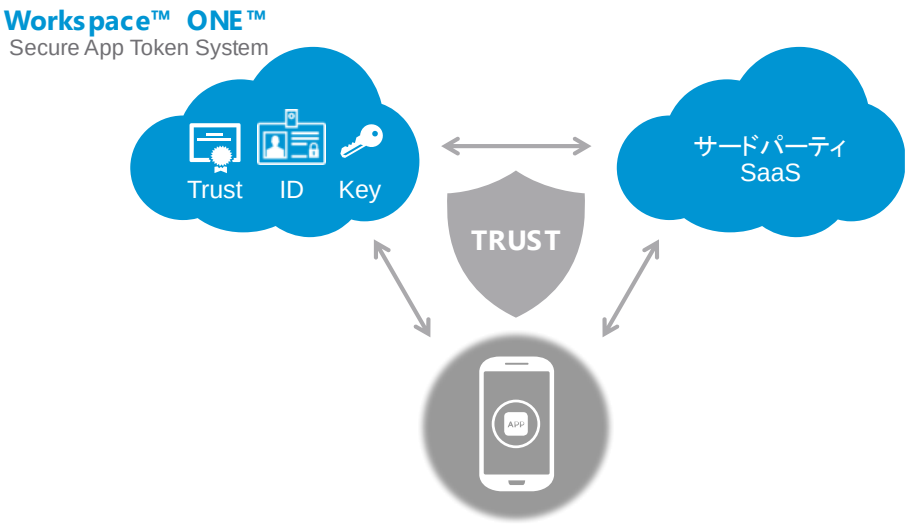
4. 	ポリシーの編集画面の構成タブで、[ポリシールールを追加]をクリックします。
5. 	以下の設定を行い[OK]をクリックします。 ・[ユーザーのネットワーク範囲が次の場合]：ALL RANGES ・[およびユーザーのコンテンツアクセス元が次の場合]：Web ブラウザ ・[次に、以下の方法を使用して認証することができます]：パスワード (クラウドデプロイ) [保存] をクリックします。
6. 	ポリシールールが追加されたことを確認します。 すでにルールが存在している場合は、作成したポリシールールを最上部にドラッグアンドドロップします。 [次へ]をクリックします。

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

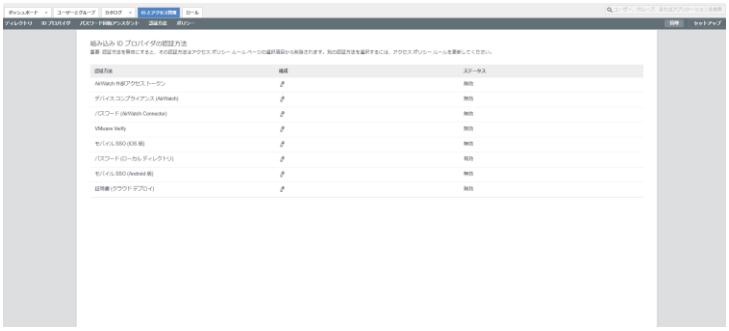
本章では、iOS デバイス用にモバイル SSO を構成します。モバイル SSO は Secure Application Token System(SATS)と呼ばれる証明書ベースの認証方式を使用することで、ユーザは認証情報の入力をすることなく各種 WEB アプリケーションやデバイスにインストールされたアプリケーションに SSO が可能となります。
iOS デバイス用のモバイル SSO では Kerberos 認証を使用しており、AirWatch からデバイスに配布されるシングルサインオンプロファイルによって制御されます。



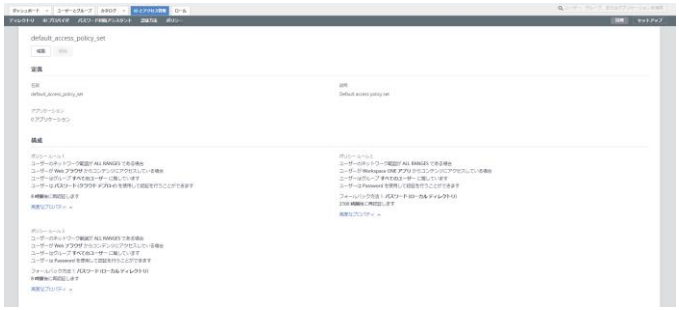
4.2 設定手順

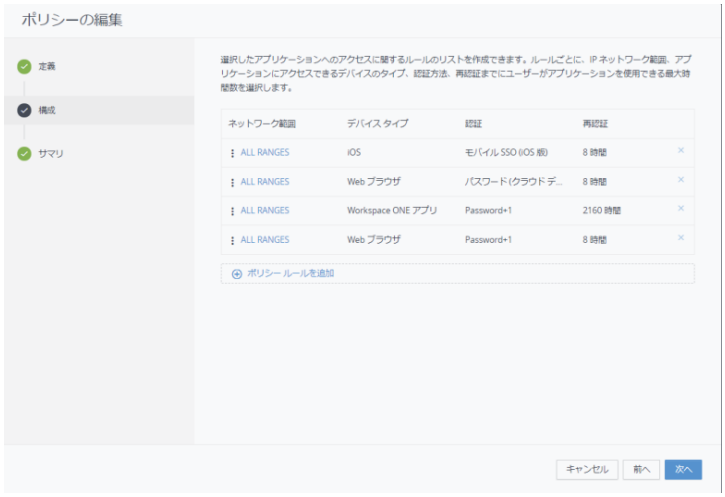
はじめに iOS モバイル SSO 用の認証アダプタを構成します。

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。

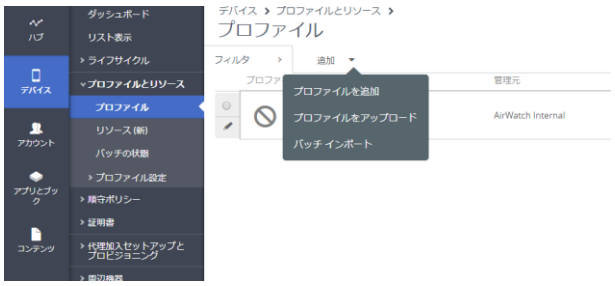
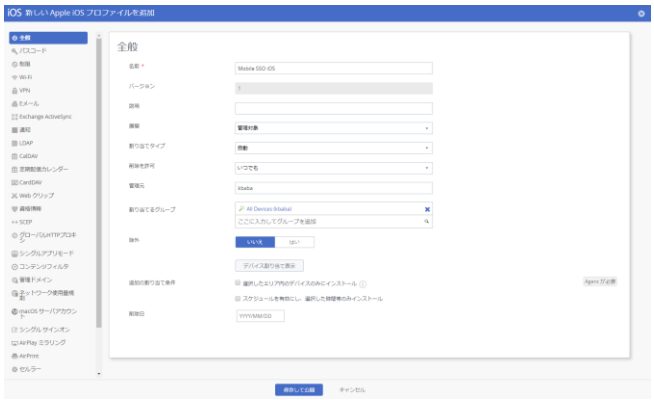
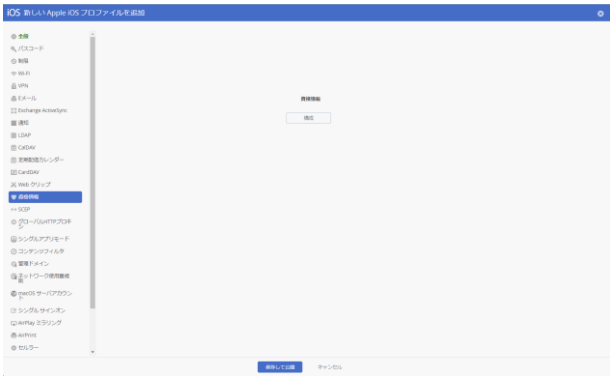
2.  	証明書の内容が表示されるので、 [エクスポート] をクリックし証明書をダウンロードします。
3. 	VMware Identity Manager コンソールで[ID とアクセス管理 / 管理 / 認証方法]を開く。 [モバイル SSO (iOS)]行の構成ボタンを押す 。
4.  	[KDC 認証を有効にする]にチェックを入れ有効化。 ルートおよび中間 CA 証明書 で [ファイルを選択] ボタンをクリックします。 ステップ 2 でダウンロードした証明書を選択してアップロードし、[OK]をクリックします。

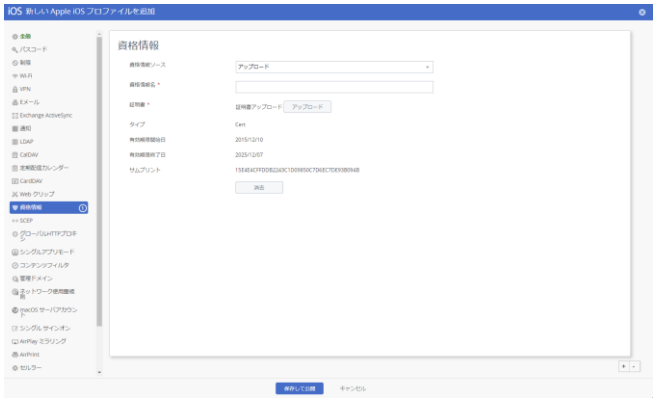
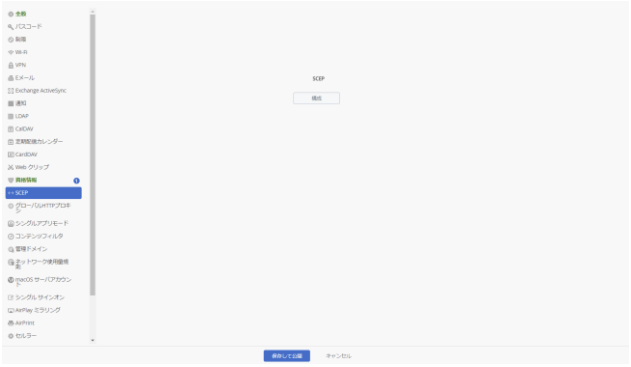
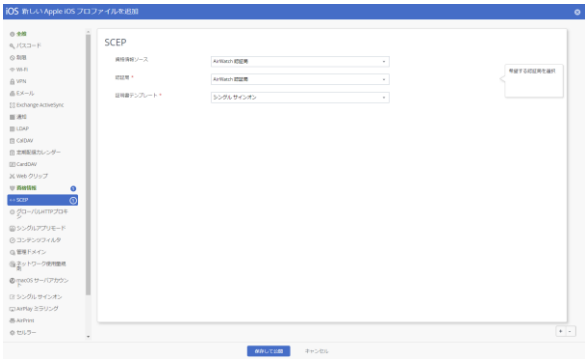
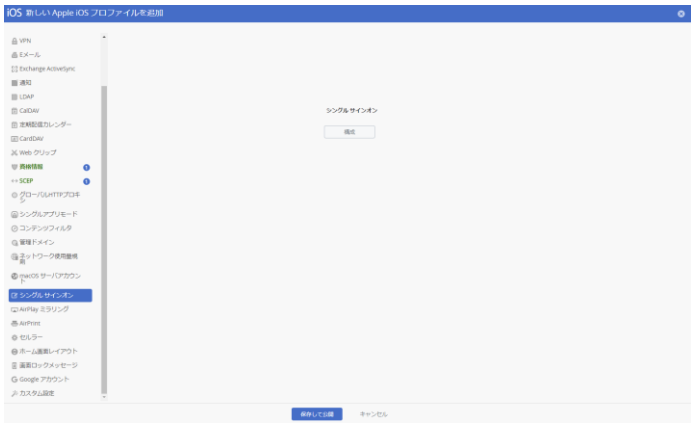
5.  	[保存]ボタンをクリックします。
6. 	VMware Identity Manager コンソールで[ID とアクセス管理 / 管理 / ID プロバイダ]を開きます。 [System Identity Provider]をクリックします。ない場合は、タイプが組み込みの ID プロバイダ名をクリックしてください。
7. 	認証方法で、[モバイル SSO (iOS)]行の[認証方法を関連付ける]にチェックを入れます。 [証明書をダウンロード]をクリックし、KDC 証明書をダウンロードします。 [保存]ボタンをクリックします。

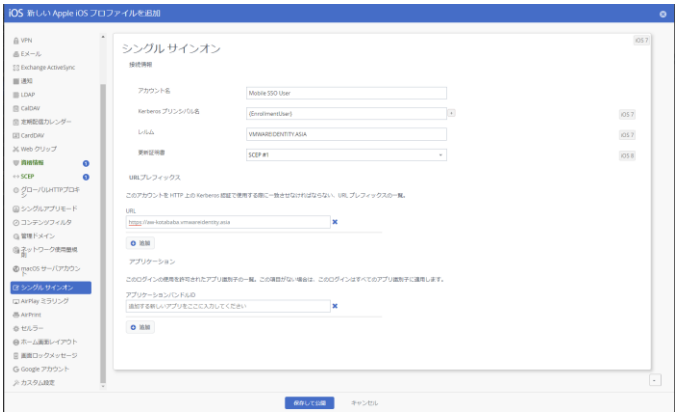
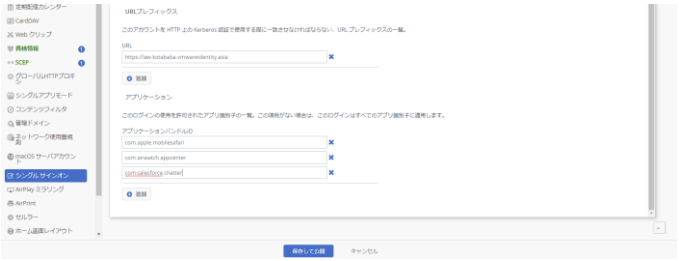
8. 	VMware Identity Manager コンソールで[ID とアクセス管理 / 管理 / ポリシー]を開き、[default_access_policy_set]をクリックします。
9.  	編集をクリックし、手順 3.2 と同様に、ポリシールールを追加します。
10. 	以下の設定を行い[保存]をクリックします。 ・[ユーザーのネットワーク範囲が次の場合] : ALL RANGES ・[およびユーザーのコンテンツアクセス元が次の場合] : iOS ・[次に、以下の方法を使用して認証することができます] : モバイル SSO (iOS 版)

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。

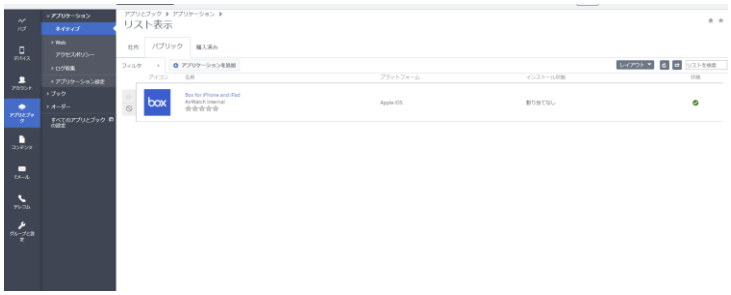
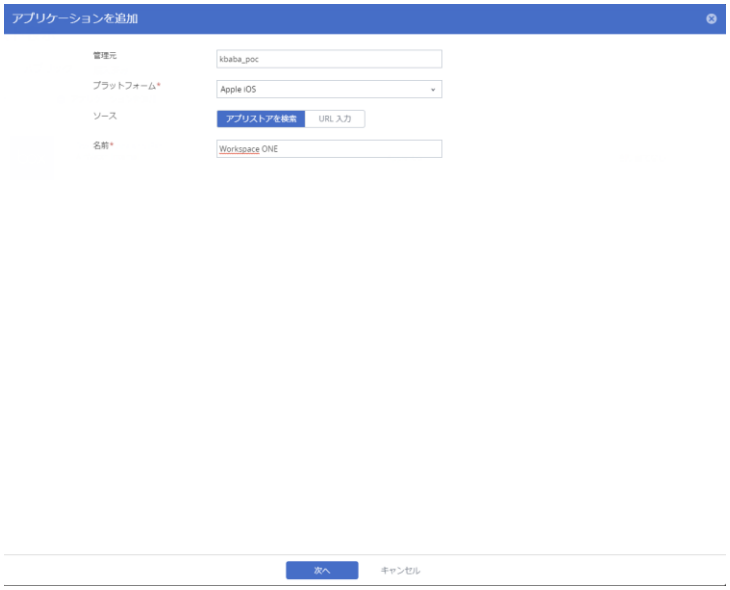
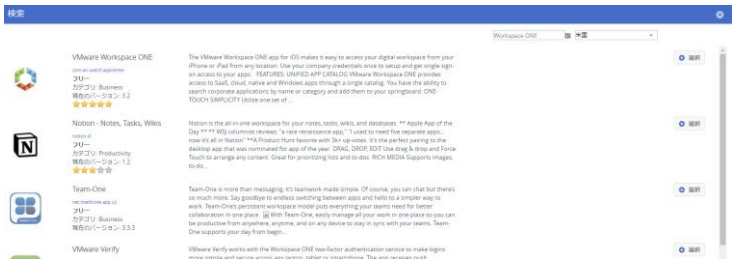
つづいて AirWatch のデバイスポリシーを使用してシングルサインオン構成をデバイスに配布します。

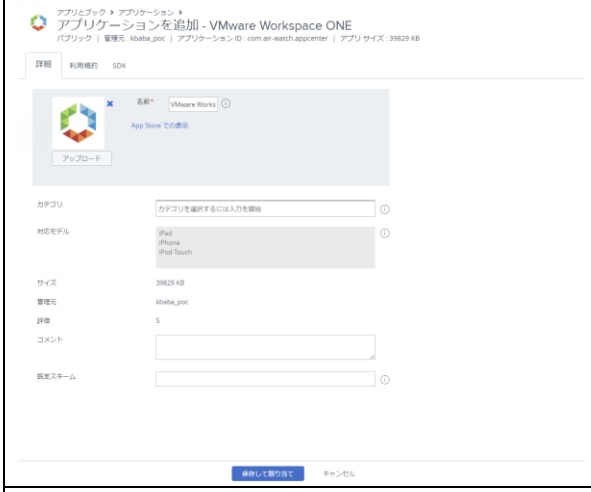
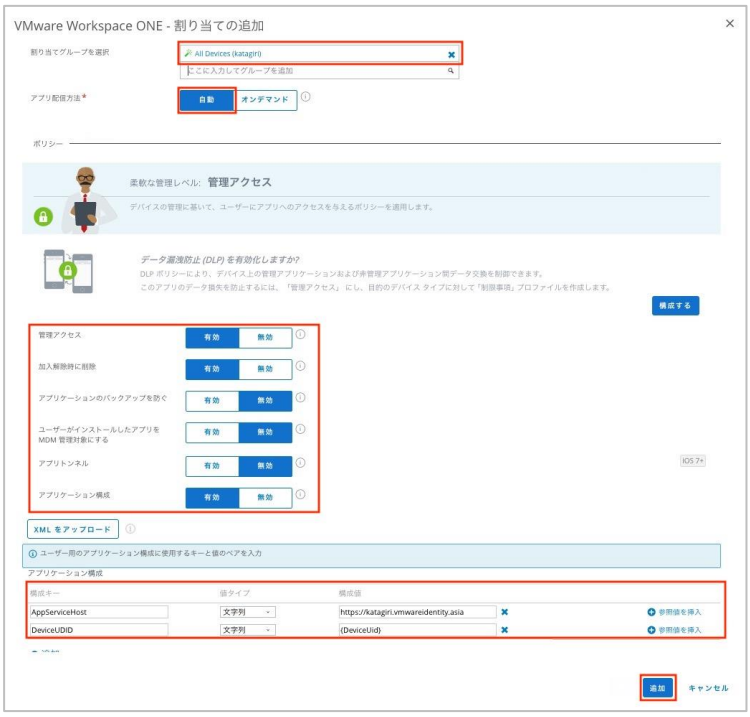
13. 	AirWatch コンソールで[デバイス / プロファイルとリソース / プロファイル]を開き、[追加 / プロファイルを追加]をクリックします。
14. 	[iOS]をクリックします。
15. 	[全般]ペイロードで以下を設定します。 名前：Mobile SSO iOS 割り当てるグループ：All Devices(テナント名)
16. 	[資格情報]ペイロードをクリックし、[構成]をクリックします。

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。

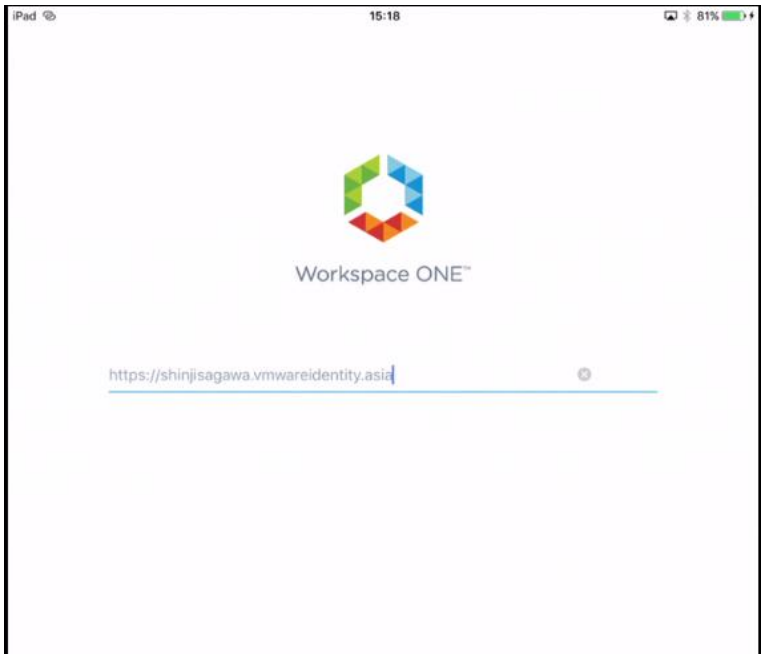
23.  	AirWatch コンソールで[アプリとブック / アプリケーション / ネイティブ / パブリック] を開き、[アプリケーションを追加]をクリックします。
24.  	以下のとおり設定を行い、[次へ]をクリックします。 プラットフォーム：Apple iOS ソース：アプリストアを検索 名前：Workspace ONE
25.  	VMware Workspace ONE の横の[選択]をクリックします。

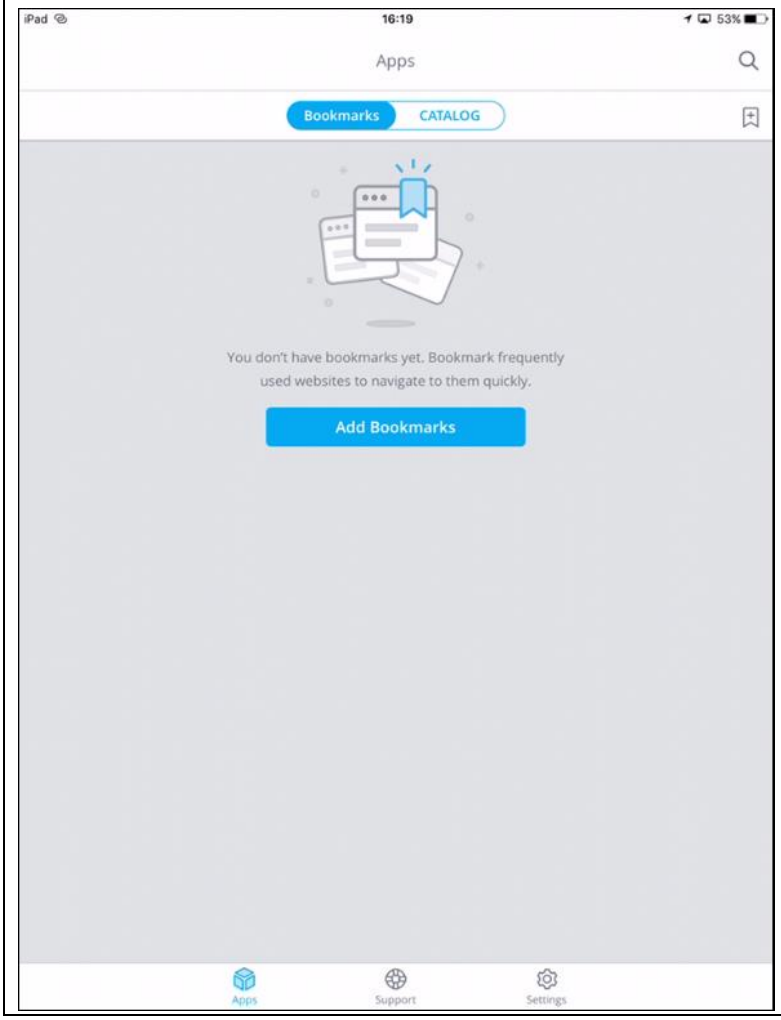
26. 	[保存して割り当て]をクリックします。
27.  	[割り当ての追加]をクリックします。 以下の設定を行います。 割り当てグループを選択：All Devices(テナント名) アプリ配信方法：自動 管理アクセス：有効 加入解除時に削除：有効 アプリケーション構成：有効 以下の 2 行を記述する。 構成キー：AppServiceHost 値のタイプ：文字列 構成値： https://<テナント>.vmwareidentity.asia 構成キー：DeviceUDID 値のタイプ：文字列 構成値：{DeviceUid} [追加]をクリックします。

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。

1.   	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。 （ https://<テナント>.vmwareidentity.asia ）
2.  	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。

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。
4.  	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。
5.  	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。
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。

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

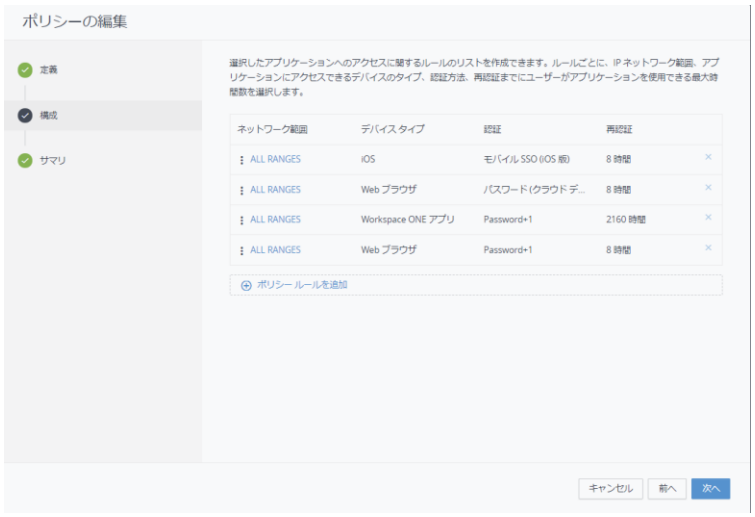
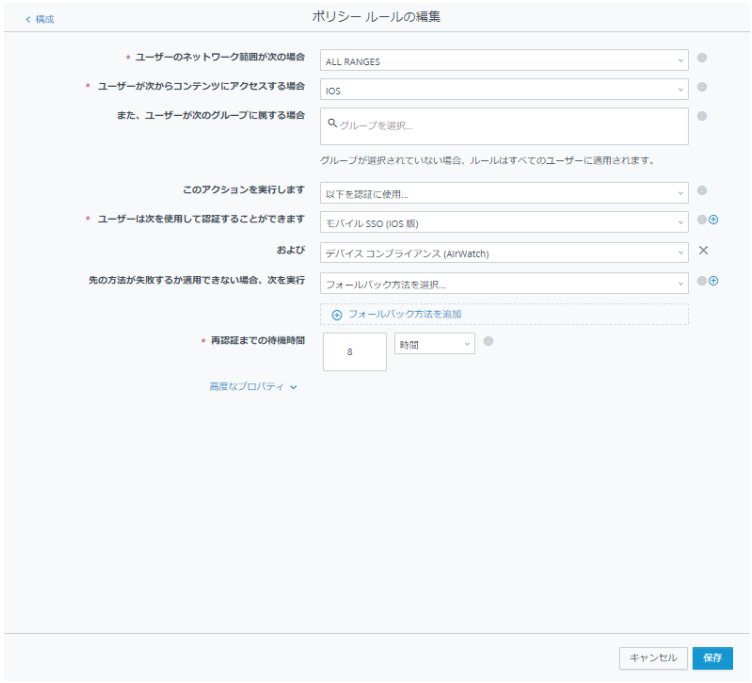
5.1 本章のゴール

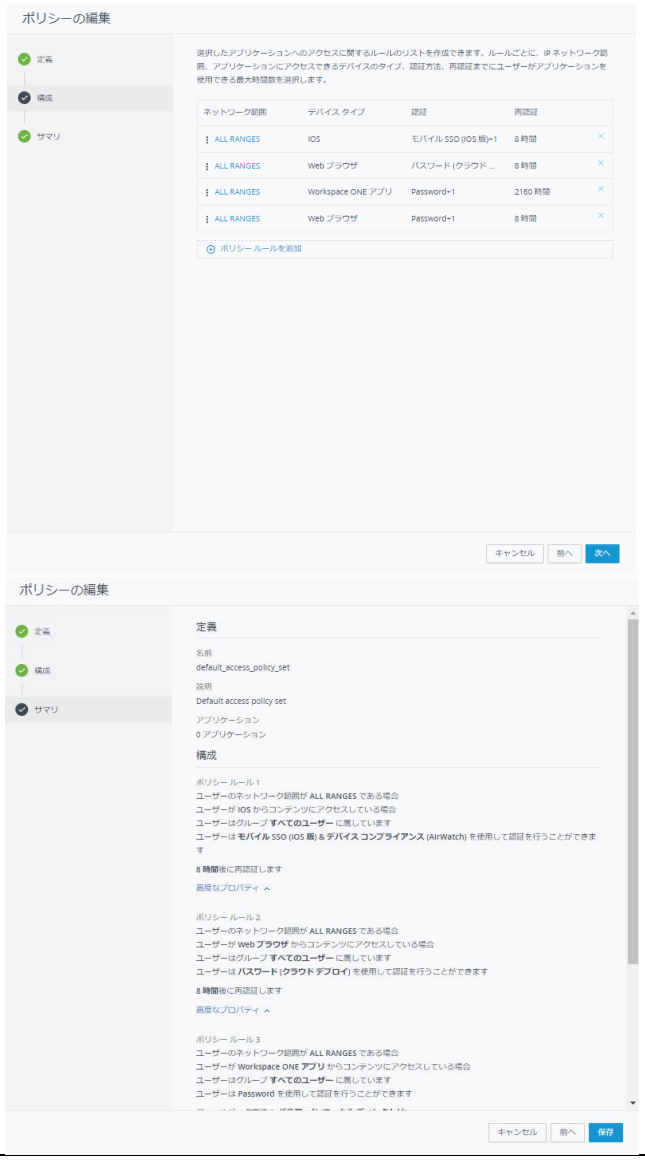
本章では AirWatch のデバイスコンプライアンスのステータスを認証に使用するデバイスコンプライアンス認証を構成します。
この機能を使用することで、デバイスが企業の設定したセキュリティ規準に準拠しているかどうかを評価した上での認証可否判断や、企業が使用を認めていない管理外デバイスからのアクセスを遮断するなどの要件に対応することができるようになります。
本章の手順では、前項までで構成した Workspace ONE のポータルへの認証時に使用している iOS 用モバイル SSO 認証にデバイスコンプライアンス認証を追加します。

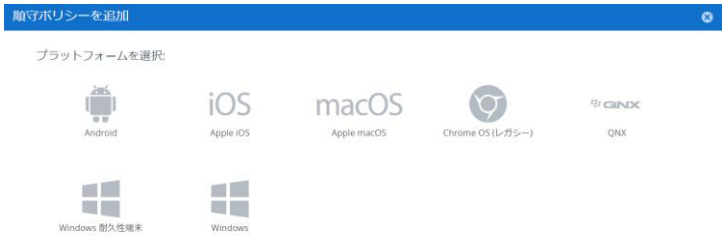
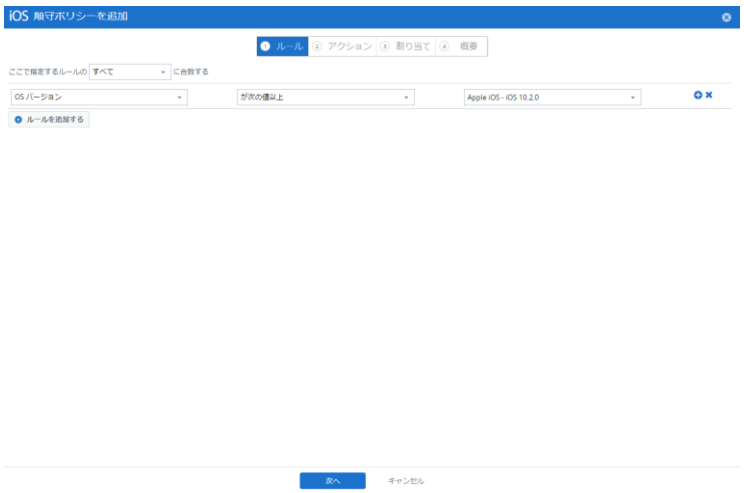
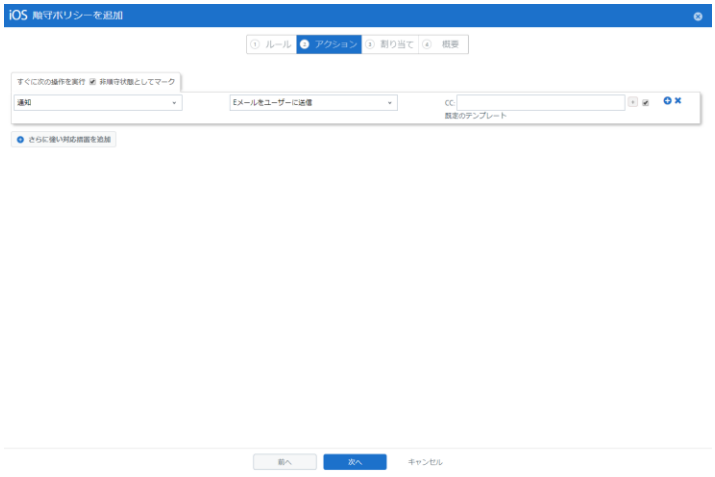
5.2 設定手順

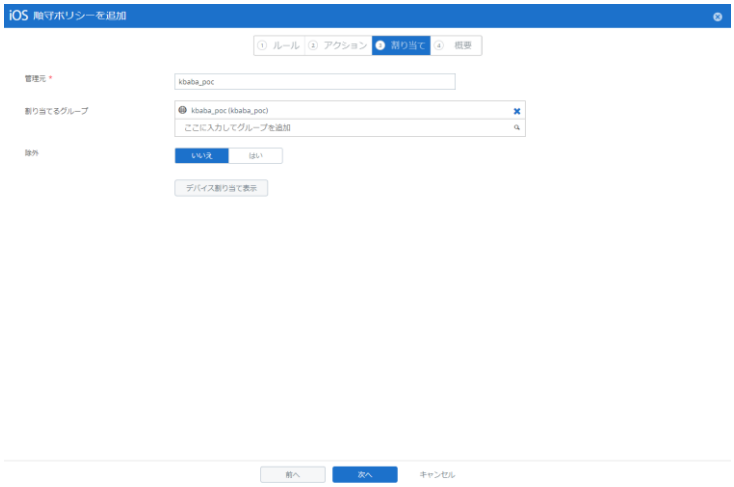
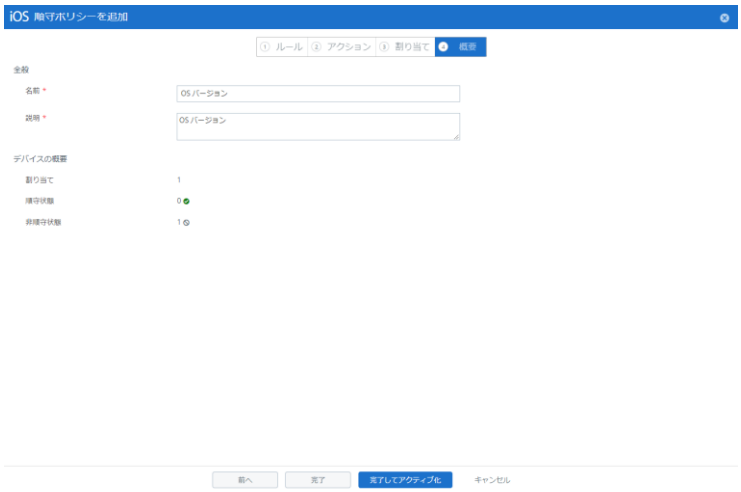
前項までに構成した iOS 用モバイル SSO 認証にデバイスコンプライアンス認証を追加構成します。

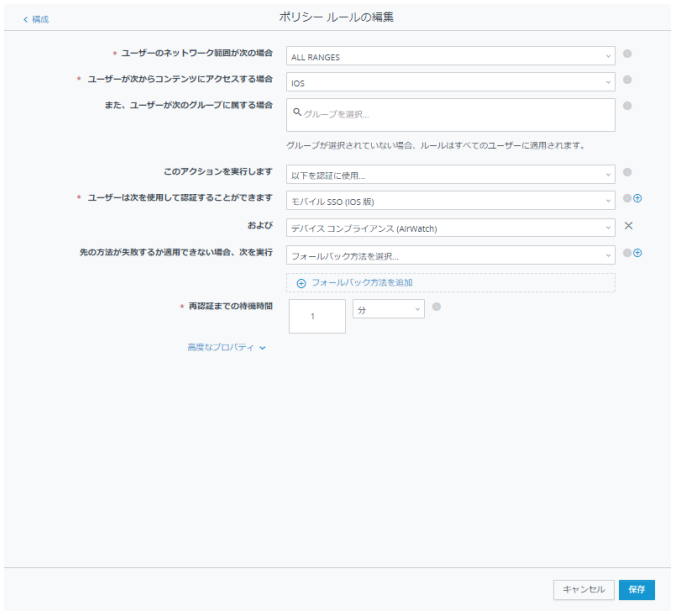
1.  	VMware Identity Manager コンソールで[ID とアクセス管理 / セットアップ / AirWatch]を開きます。 以下の設定を行い、[保存]をクリックします。 コンプライアンスチェック：有効
2.  	[ID とアクセス管理 / 管理 / ID プロバイダ]を開きます。[Sytem Identity Provider] を選択し、認証方法で[デバイスコンプライアンス (Airwatch)]にチェックを入れ、[保存]をクリックします。

2.  	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.  	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す]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。

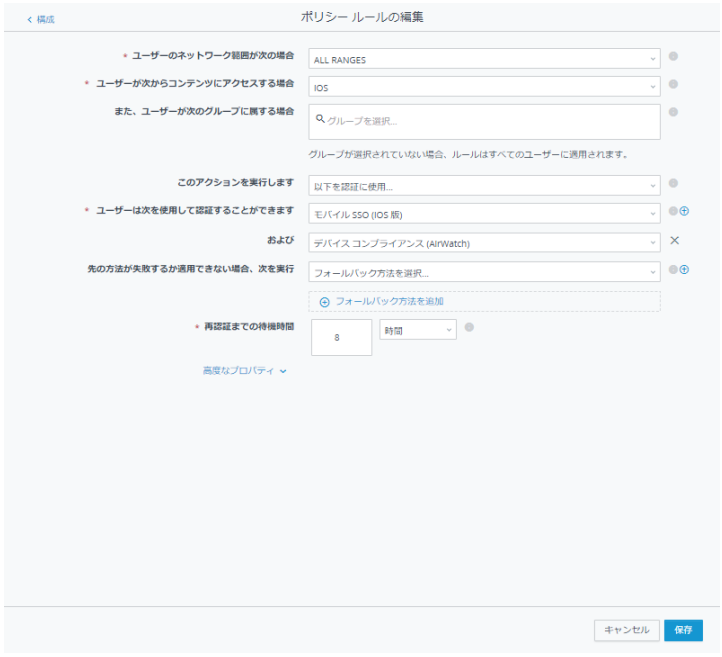
4. 	[次へ] → [保存]ボタンをクリックし、ポリシーの編集を完了します。
5. 	テストの為に企業が設定したセキュリティ基準を満たしていないデバイスの状態（非順守状態）を作成します。ここでは iOS が最新の場合は非順守状態という趣旨の順守ポリシーを構成しています。 AirWatch コンソールで[デバイス / 順守ポリシー / リスト表示] 開き、[追加]をクリックします。

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

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。 Idenity 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.



テストの為に行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

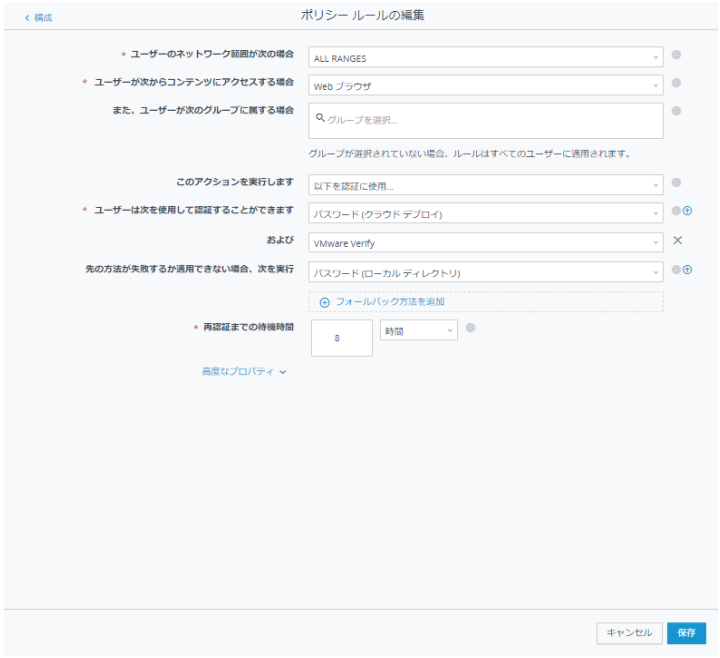
Workspace ONE に含まれる多要素認証機能である VMware Verify を構成します。本章では、ブラウザから Workspace ONE にアクセスした場合に、Active Directory のユーザ名とパスワードに加え、VMware Verify を使用した 2 要素認証を実施するように構成します。

6.2 設定手順

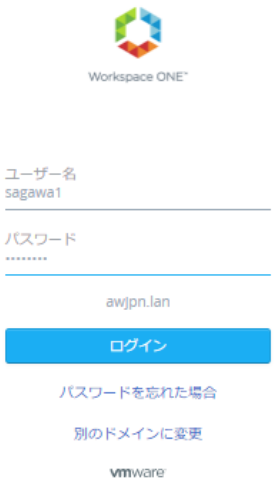
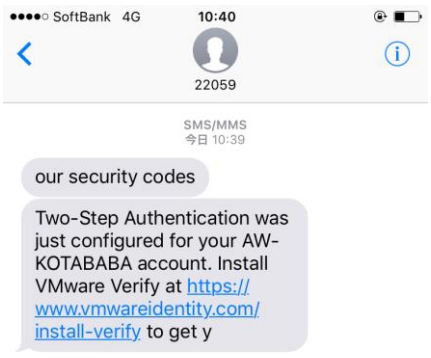
VMware Verify を有効化し、認証ポリシーに VMware Verify を組み込みます。

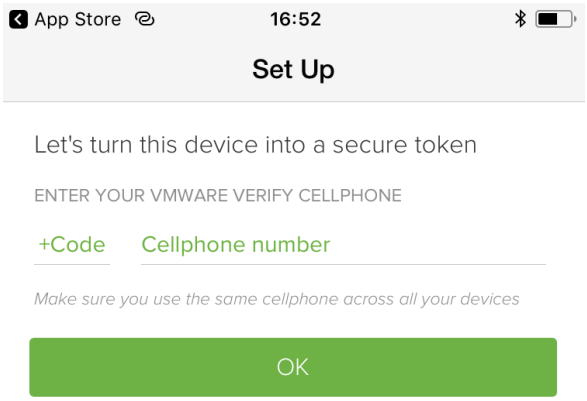
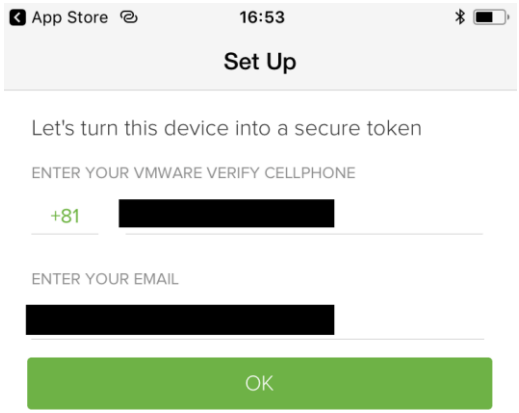
1.  	VMware Identity Manager コンソールで [ID とアクセス管理 / 管理 / 認証方法]を開きます。 [VMware Verify] 行の構成ボタンをクリックします。
2.  	[VMware Verify を有効化する]にチェックを入れ、[保存]ボタンをクリックします。

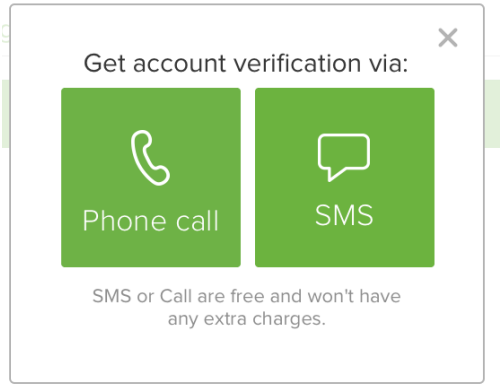
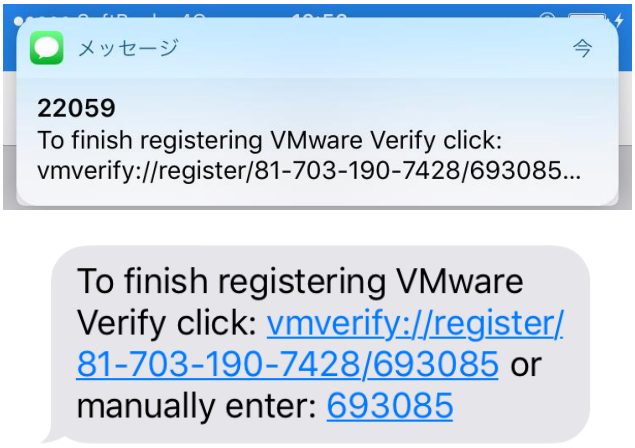
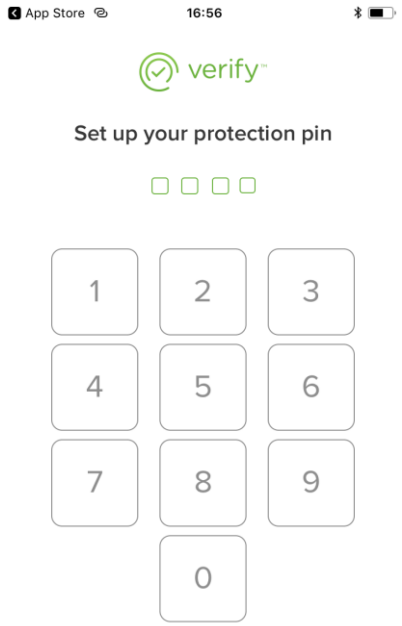
3.  	VMware Identity Manager コンソールで[ID とアクセス管理 / 管理 / ID プロバイダ]を開き、[System Identity Provider]をクリックします。
4.  	認証方法で、VMware Verify が有効になっていることを確認します。有効になっていない場合は、[認証方法を関連付ける]のチェックを有効にし、[保存]をクリックします。
5.  	VMware Identity Manager コンソールで[ID とアクセス管理 / 管理 / ポリシー]を開き、[default_access_policy_set]をクリックします。
6.  	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。

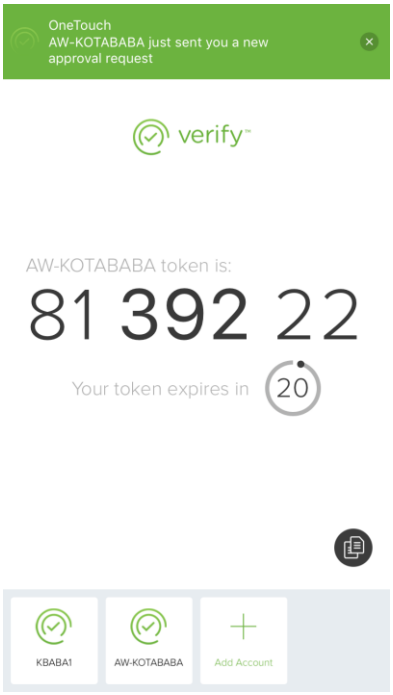
7. 	以下の設定を行い、[保存]をクリックします。 ・ユーザーのネットワーク範囲が次の場合： すべての範囲 ・また、ユーザーのコンテンツ アクセス元が次の場合： Web ブラウザ ・ユーザーは次を使用して認証することができます： パスワード（クラウドデプロイ） および：VMware Verify ・先の方法が失敗するか適用できない場合は、次を実行： パスワード（ローカルディレクトリ）
8. 	[保存]をクリックし、ポリシーの編集を完了します。

VMware Verify アプリのセットアップを実施します。

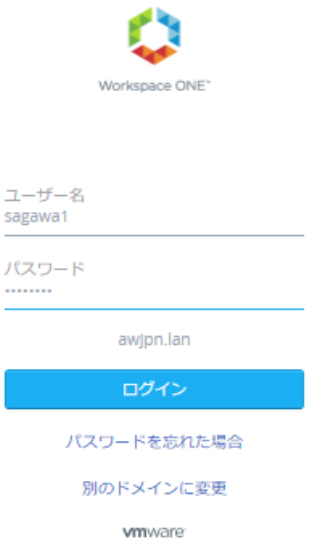
9. 	PC からブラウザで Workspace ONE のポータルにアクセスし、AD のユーザーでログインをします。
10. 	（はじめて VMware Verifiy を使用するアカウントの場合） 多要素認証に使用するスマートフォンの電話番号を入力して[ログイン]ボタンをクリックします。 TIP： 国内通話用の最初の[0]を省く必要はありません。 例　07011112222 を+81 7011112222 の形式で入力する必要はありません。
11. 	スマートフォン上の作業 指定したスマートフォンに VMware Verify をインストールするためのリンクが SMS で届くので開きます。

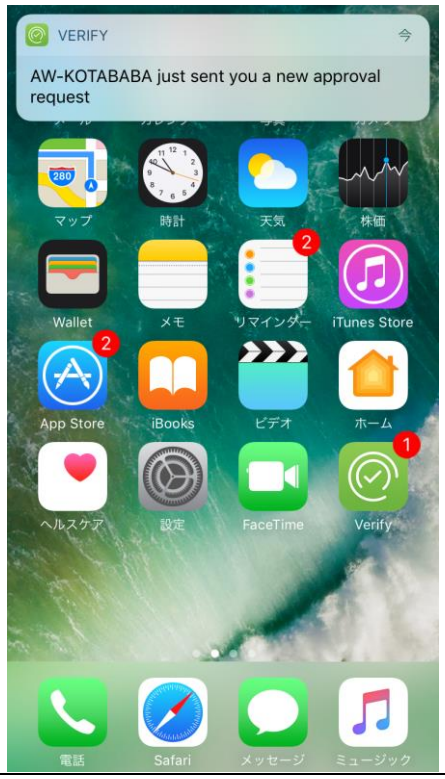
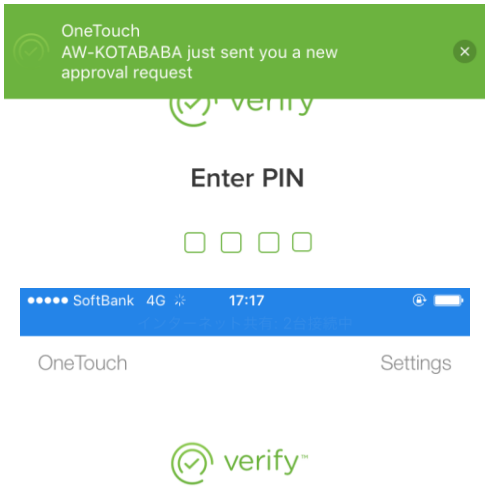
12. 	スマートフォン上の作業 指示に従ってインストールを実施します。
13. 	スマートフォン上の作業 VMware Verify アプリを起動します。 電話番号を入力します。
14. 	スマートフォン上の作業 E メールアドレスの入力欄が出てきた場合には、E メールアドレスを入力します。 [OK]ボタンをタップします。

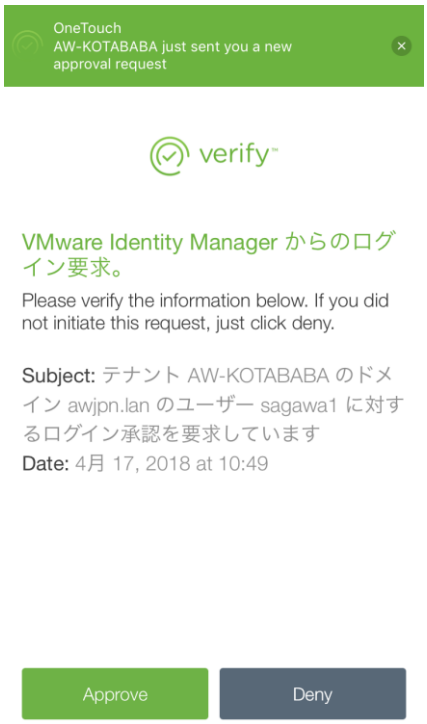
15.  	スマートフォン上の作業 [SMS]を選択します。
16.  	スマートフォン上の作業 VMware Verify をアクティベーションするためのリンクが SMS で届くので開きます。
17.  	スマートフォン上の作業 VMware Verify を保護するための PIN を設定します。

18. 	スマートフォン上の作業 トークンが表示されることを確認します。
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。
20. 	Workspace ONE へのブラウザからのログインが設定できました。 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]をクリックします。
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。
24. 	認証が VMware Verify 待機状態になることを確認します。

25. 	スマートフォン上の作業 VMware Verify に認証要求の通知が届くので VMware Verify を起動します。
26. 	スマートフォン上の作業 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。
27. 	スマートフォン上の作業 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。

28.  	スマートフォン上の作業 認証要求を開きます。
29.  	スマートフォン上の作業 認証要求の内容を確認し[Approve]ボタンで承認します。
30.  	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。 以上で VMware Verify を用いた 2 要素認証は完了です。

7 認証設定の最適化

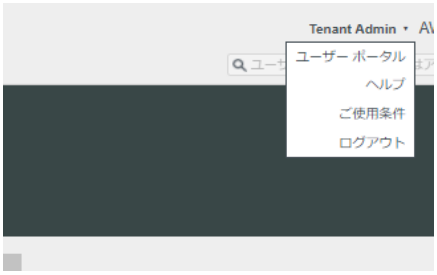
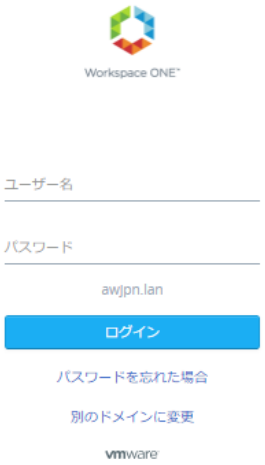
7.1 本章のゴール

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

1. 	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。
2. 	以下の設定を行い、[保存]をクリックします。 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**オフ** 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**オフ** 残りの設定はそのままにします。

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、[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. 	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. 	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

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

ヴイエムウェア株式会社