Guide de déploiement de VMware Workspace ONE (sur sites)

Mai 2018
VMware Workspace ONE
VMware Identity Manager 3.2
VMware AirWatch 9.3

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

https://docs.vmware.com/fr/

N’hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l’adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos du déploiement de VMware Workspace ONE

Le Guide de déploiement de VMware Workspace™ ONE™ fournit des informations sur l'intégration de VMware Identity Manager™ et de VMware AirWatch® pour fournir l'authentification unique à Workspace ONE, la gestion des périphériques dans AirWatch et VMware Workspace ONE sous forme de catalogue d'applications.

Lorsqu'AirWatch et VMware Identity Manager sont intégrés, les utilisateurs avec des périphériques AirWatch inscrits peuvent se connecter à leurs applications activées en toute sécurité sans entrer plusieurs mots de passe.

Public concerné

Ces informations sont conçues pour les administrateurs qui connaissent bien les services AirWatch et VMware Identity Manager.

Introduction à Workspace ONE

1

VMware Workspace® ONE® est une plate-forme d'entreprise sécurisée qui fournit et gère les applications sur les périphériques iOS, Android et Windows 10. La gestion des identités, des applications et de la mobilité d'entreprise est intégrée à la plate-forme Workspace ONE.

VMware AirWatch® et VMware Identity Manager™ sont intégrés afin que vous bénéficiiez du catalogue des applications et des services de gestion d'accès mobile de Workspace ONE.

Les services VMware Identity Manager fournissent les composants liés à l'identité, y compris l'authentification pour les utilisateurs qui utilisent l'authentification unique pour se connecter à leurs ressources. Vous créez un ensemble de stratégies qui se rapportent à la mise en réseau et à l'authentification pour contrôler l'accès à ces ressources.

Les services AirWatch fournissent des outils d'inscription de périphérique, de distribution d'application et de vérification de la conformité pour vous assurer que les périphériques d'accès distant répondent aux normes de sécurité de l'entreprise. Les utilisateurs des périphériques inscrits AirWatch peuvent se connecter à leurs applications activées en toute sécurité sans entrer plusieurs mots de passe.

Ce chapitre aborde les rubriques suivantes :

Présentation de l’architecture Workspace ONE

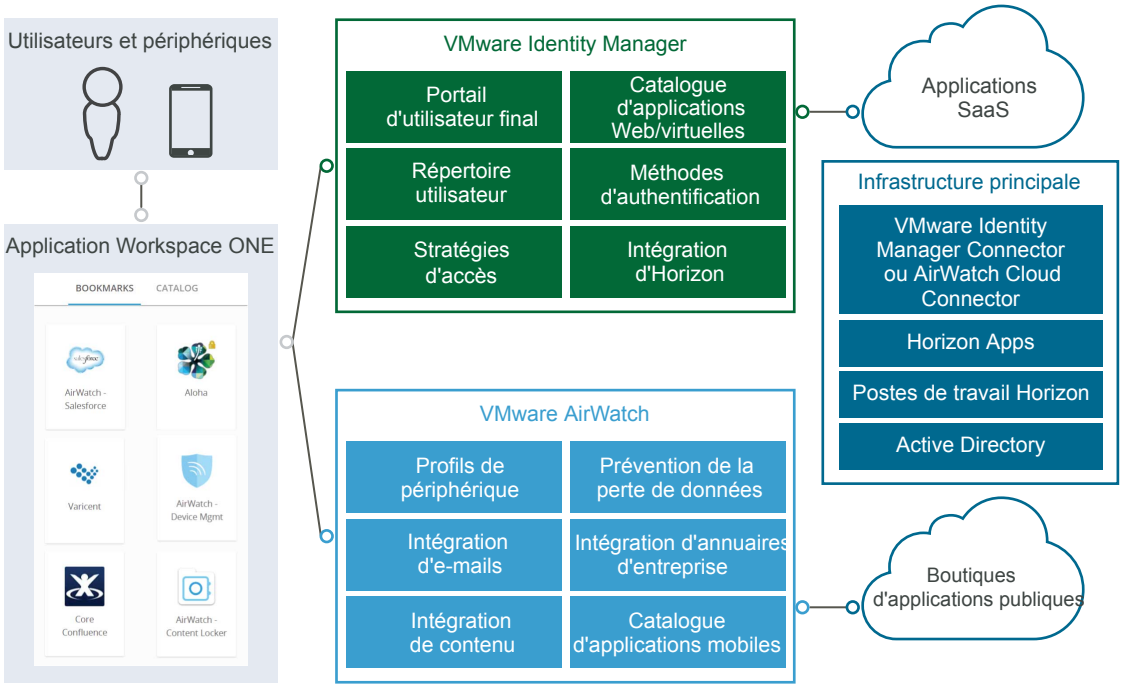
Workspace ONE fournit aux utilisateurs un accès sécurisé aux applications Cloud, mobiles et Windows gérées à partir d'un catalogue unifié. Pour accéder au périphérique, l'application native Workspace ONE est disponible pour les périphériques iOS, Android et Windows 10.

Lorsque Workspace ONE est déployé, les services VMware Identity Manager et AirWatch suivants doivent être implémentés.

- VMware Enterprise Systems Connector installé et configuré. Vous pouvez configurer le composant VMware Identity Manager Connector ou le composant AirWatch Cloud Connector (ACC).

- Intégration d'Active Directory de votre entreprise à VMware Identity Manager ou AirWatch Cloud Connector pour synchroniser les utilisateurs et les groupes d'Active Directory avec le service Workspace ONE.
- Configurez VMware Identity Manager avec des clés d'API AirWatch et le certificat racine administrateur, puis activez le catalogue unifié, la vérification de la conformité et l'authentification par mot de passe utilisateur via AirWatch.

Figure 1-1. Présentation de l'architecture Workspace ONE



Configuration requise

La configuration système requise de Workspace ONE est indiquée ci-dessous.

Tableau 1-1. Configuration système requise de Workspace ONE

Configuration requise de Workspace ONE	Détails
Active Directory	Windows Server 2008 et 2008 R2 Windows Server 2012 et 2012 R2
Navigateur Web pour accéder à la console d'administration de VMware Identity Manager et d'AirWatch	Internet Explorer 11 pour Windows Google Chrome 4.0 et versions ultérieures Mozilla Firefox 40 et versions ultérieures Safari 6.2.8 et versions ultérieures
VMware Enterprise Connector, avec VMware Identity Manager Connector ou AirWatch Cloud Connector installé.	Windows Server 2008 R2 Windows Server 2012 ou 2012 R2 .NET Framework 4.6.2 Consultez le guide d'installation et de configuration de VMware Enterprise Systems Connector pour déployer les connecteurs.

Détails de la fonctionnalité Workspace ONE

Les principales fonctionnalités dans Workspace ONE sont décrites ci-dessous.

Applications Workspace ONE mobiles natives

Les utilisateurs peuvent installer l'application Workspace ONE sur un périphérique mobile et utiliser les informations d'identification d'entreprise pour accéder avec l'authentification unique aux applications d'entreprise, Cloud et mobiles.

Catalogue d'applications en libre-service pour ressources Web, Horizon et Citrix

Workspace ONE fournit aux utilisateurs un accès aux applications Cloud, mobiles et Windows à l'aide d'un catalogue unifié. Le catalogue contient des applications publiées dans VMware Identity Manager et VMware AirWatch. Les types d'applications pris en charge incluent les applications Web internes, SaaS, mobiles natives, mobiles développées en interne, Windows héritées et modernes, Horizon 7, VMware Horizon Cloud Service™, publiées Citrix, ainsi que des modules ThinApp. La boutique d'applications contient également des postes de travail virtualisés.

Lancer des applications Web et virtuelles avec l'authentification unique

Workspace ONE fournit l'authentification unique mobile, une implémentation de connexion mono-touche aux applications mobiles. Mobile SSO est disponible pour les périphériques Android, iOS et Windows 10.

Accès conditionnel avec la conformité des périphériques

Avec Workspace ONE, vous pouvez appliquer un accès conditionnel en fonction de la plage réseau, de la plate-forme et de critères spécifiques à l'application pour l'authentification. Un périphérique doit prouver sa conformité aux règles de sécurité avant d'autoriser l'accès à une application. VMware Identity Manager inclut une option de stratégie d'accès pouvant être configurée afin de vérifier l'état de conformité du périphérique sur le serveur AirWatch lorsque des utilisateurs se connectent à partir du périphérique.

Authentification multifacteur

Workspace ONE fournit une authentification multifacteur via l'application VMware Verify. Lorsqu'un utilisateur tente d'accéder au catalogue Workspace ONE ou à n'importe quelle application nécessitant une authentification forte, VMware Verify envoie une notification sur le téléphone de l'utilisateur. Pour consulter les tentatives d'accès à Workspace ONE, l'utilisateur doit balayer Accepter pour accéder à l'application.

Gestion adaptative

Pour les applications qui requièrent uniquement un niveau de base de sécurité, les utilisateurs n'ont pas à inscrire leur périphérique dans AirWatch Mobile Device Management™. Les utilisateurs peuvent télécharger l'application mobile Workspace ONE et sélectionner les applications qu'ils souhaitent installer. Pour connaître les applications qui requièrent un niveau plus élevé de sécurité, les utilisateurs peuvent inscrire leur périphérique dans AirWatch directement à partir de l'application mobile Workspace ONE.

Démarrage avec l'assistant Workspace ONE

Vous pouvez utiliser l'assistant Démarrage Workspace ONE pour vous guider à travers plusieurs étapes de configuration pour intégrer des services AirWatch et VMware Identity Manager afin de créer l'environnement Workspace ONE.

L'assistant Démarrage ne remplace pas la possibilité de configurer ou de modifier n'importe quel paramètre individuel, mais automatise considérablement la configuration initiale pour la plupart des clients.

L'assistant Démarrage Workspace ONE peut être utilisé pour configurer ce qui suit.

- Enterprise Connector & Directory. L'assistant vous guide à travers les étapes de configuration de VMware Enterprise System Connector et de configuration de la connexion Active Directory depuis AirWatch Cloud Connector afin d'importer des utilisateurs et des groupes à partir du répertoire de votre entreprise. Consultez le guide de configuration rapide de VMware Workspace ONE pour vous aider à configurer Enterprise Connector.
- Découverte automatique. Exécutez l'assistant pour enregistrer votre domaine de messagerie dans le service de découverte automatique afin de faciliter l'accès des utilisateurs finaux à leur portail d'applications via l'application Workspace ONE. Les utilisateurs finaux entrent ensuite leur adresse e-mail au lieu de l'URL de l'organisation.
- Catalogue Workspace ONE. L'assistant Catalogue Workspace ONE vous guide à travers les étapes de configuration du catalogue Workspace ONE. Vous pouvez également utiliser l'étape de marque personnalisée de Workspace ONE pour ajouter des informations de marque de votre entreprise au catalogue Workspace ONE et à l'application. Consultez le guide de configuration rapide de VMware Workspace ONE pour vous aider à configurer le Catalogue Workspace ONE.
- Gestion adaptative. Configurez la gestion adaptative pour limiter certaines applications en exigeant qu'un profil soit installé sur les périphériques de l'utilisateur. Le profil s'assure que les données et les applications d'entreprise peuvent être supprimées si nécessaire. Vous pouvez également choisir d'exiger que les applications publiques soient gérées ou utilisées indépendamment en les téléchargeant manuellement depuis la boutique d'applications.

L'assistant Démarrage peut vous alerter si des configurations existantes potentiellement en conflit sont déjà activées dans AirWatch ou dans les services VMware Identity Manager. Si cela se produit, ou si l'assistant Démarrage n'exécute que partiellement les étapes, les fonctionnalités peuvent être configurées manuellement. Utilisez ce guide pour configurer les services AirWatch et VMware Identity Manager manuellement pour Workspace ONE.

Intégration d' AirWatch à VMware Identity Manager

2

Pour configurer les services de gestion mobile AirWatch pour les périphériques mettant en œuvre des services VMware Identity Manager pour la gestion de l'authentification unique et des identités des utilisateurs, vous devez intégrer les services.

Lorsqu'AirWatch et VMware Identity Manager sont intégrés, les utilisateurs des périphériques AirWatch inscrits peuvent se connecter à Workspace ONE pour accéder à leurs applications activées en toute sécurité sans entrer plusieurs mots de passe.

L'assistant Démarrage de Workspace ONE peut vous guider à travers les nombreuses étapes de configuration pour intégrer AirWatch et VMware Identity Manager. Consultez le guide de configuration rapide de VMware Workspace ONE pour exécuter les assistants Workspace ONE.

Ce chapitre aborde les rubriques suivantes :

Configurer l’intégration à partir de la console d’administration d’AirWatch

Pour intégrer les services VMware Identity Manager, configurez ces paramètres dans la console d’administration d'AirWatch.

- La clé d'administration API REST pour la communication avec le service VMware Identity Manager
- La clé API d'utilisateur inscrit REST pour l’authentification par mot de passe AirWatch Cloud Connector qui est créée dans le groupe d’organisation sur lequel VMware Identity Manager est configuré.

- Un compte d'administration API pour VMware Identity Manager et le certificat d'authentification d'administration qui est exporté depuis AirWatch et ajouté aux paramètres d'AirWatch dans la console d'administration VMware Identity Manager.

Créer des clés API REST dans AirWatch

L'accès API d'administration REST et l'accès des utilisateurs inscrits doivent être activés dans la console d'administration d'AirWatch pour intégrer VMware Identity Manager à AirWatch. Lorsque vous activez l'accès API, une clé API est générée.

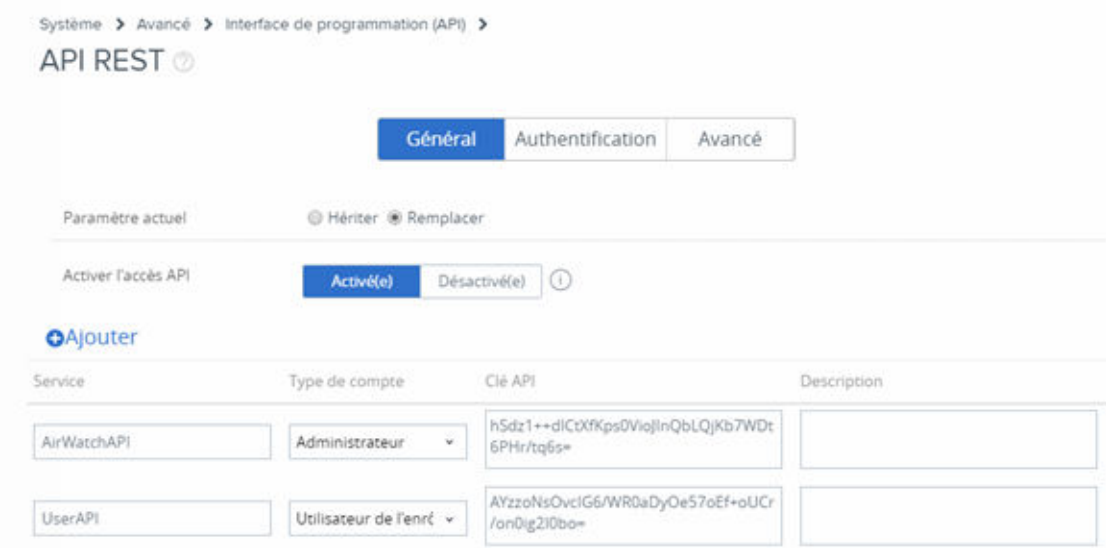
Procédure

1. Dans la console d'administration d'AirWatch, sélectionnez le groupe d'organisation de niveau Global > Client et accédez à **Groupes et paramètres > Tous les paramètres > Système > Avancé > API > API REST**.
2. Dans l'onglet Général, cliquez sur **Ajouter** pour générer la clé API à utiliser dans le service VMware Identity Manager. Le type de compte doit être Administrateur.

   Fournissez un nom de service unique. Ajoutez une description, telle que **`AirWatchAPI pour IDM`**.
3. Pour générer la clé API d'utilisateur inscrit, cliquez de nouveau sur **Ajouter**.
4. Dans le menu déroulant Type de compte, sélectionnez **Utilisateur de l'enrôlement**.

   Fournissez un nom de service unique. Ajoutez une description, telle que **`UserAPI pour IDM`**.
5. Copiez les deux clés API et enregistrez les clés dans un fichier.

   Vous ajoutez ces clés lorsque vous configurez AirWatch dans la console d'administration de VMware Identity Manager.



6. Cliquez sur **Enregistrer**.

Exporter le certificat racine d'un administrateur VMware AirWatch

Une fois la clé API d'administration créée, vous ajoutez un compte d'administrateur et configurez l'authentification par certificat dans la console d'administration d'AirWatch.

Pour l'authentification par certificat API REST, un certificat de niveau utilisateur est généré à partir de la console d'administration d'AirWatch. Le certificat utilisé est un certificat AirWatch auto-signé généré à partir du certificat racine d'administration AirWatch.

Prérequis

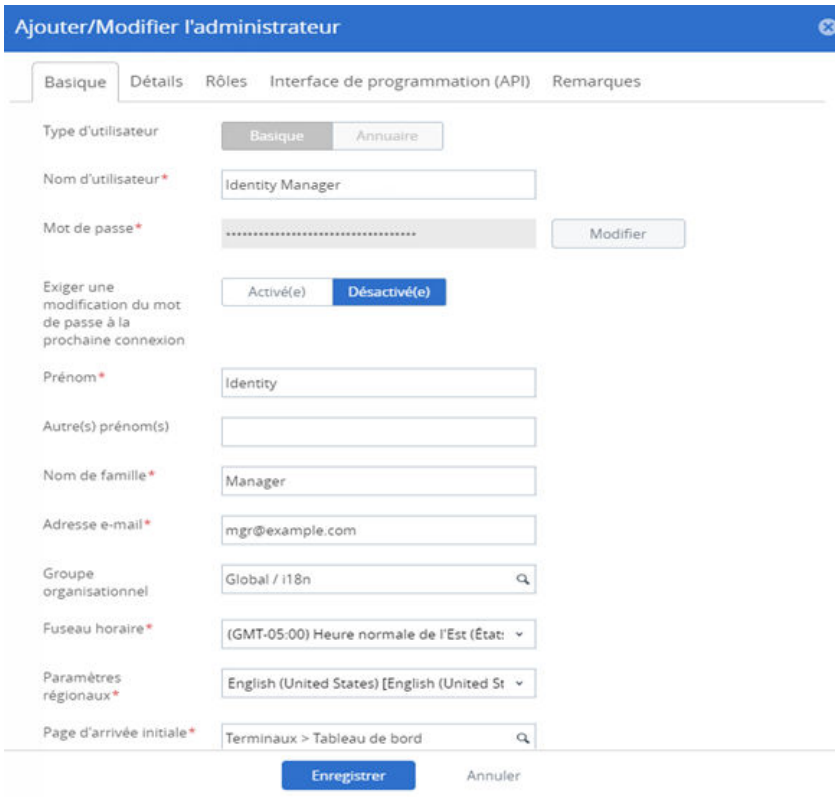
La clé API d'administration REST AirWatch est créée.

Procédure

1 Dans la console d'administration d'AirWatch, sélectionnez le groupe d'organisation de niveau Global > Client et accédez à **Comptes > Administrateurs > Vue Liste**.

2 Cliquez sur **Ajouter > Ajouter un administrateur**.

3 Dans l'onglet Standard, entrez le nom d'utilisateur et le mot de passe de l'administrateur de certificat dans les zones de texte requises.



4 Sélectionnez l'onglet Rôles, choisissez le groupe d'organisation actuel, cliquez sur la deuxième zone de texte et sélectionnez **Administrateur AirWatch**.

5 Sélectionnez l'onglet API et, dans la zone de texte Authentification, sélectionnez **Certificats**.

6 Entrez le mot de passe du certificat. Le mot de passe est le même que celui entré pour l'administrateur dans l'onglet Standard.

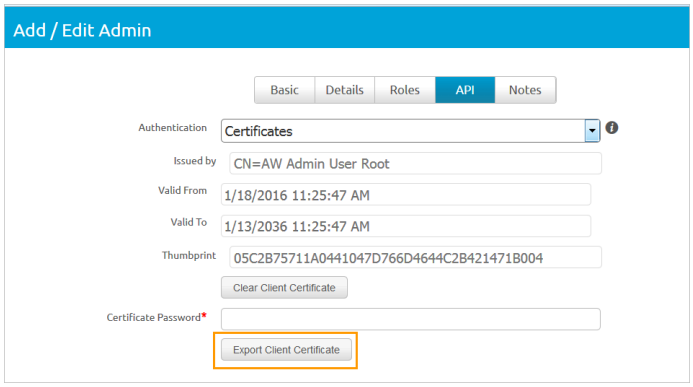
7 Cliquez sur **Enregistrer**.

Le nouveau compte d'administrateur et le certificat client sont créés.

8 Sur la page Vue Liste, sélectionnez l'administrateur que vous avez créé et ouvrez de nouveau l'onglet API.

La page des certificats affiche des informations sur le certificat.

9 Entrez le mot de passe que vous avez défini dans la zone de texte Mot de passe du certificat, cliquez sur **Exporter le certificat client** et enregistrez le fichier.



Le certificat client est enregistré sous un fichier de type .p12.

Suivant

Configurez vos paramètres d'URL AirWatch dans la console d'administration de VMware Identity Manager.

Configuration d'une instance d'AirWatch dans VMware Identity Manager

Après avoir configuré les paramètres dans la console d'administration d'AirWatch, sur la page Identité et gestion de l'accès de la console d'administration de VMware Identity Manager, vous entrez l'URL d'AirWatch, les valeurs de clé API et le certificat. Une fois les paramètres d'AirWatch configurés, vous pouvez activer les options de fonctionnalité disponibles pour Workspace ONE.

Ajouter des paramètres AirWatch dans la console d'administration de VMware Identity Manager

Configurez les paramètres AirWatch dans la console d'administration de VMware Identity Manager pour intégrer AirWatch à VMware Identity Manager.

Vous pouvez lier des domaines configurés dans VMware Identity Manager à des groupes d'organisation spécifiques dans AirWatch afin de faciliter l'enregistrement du périphérique dans AirWatch. Voir Mappage de domaines VMware Identity Manager à plusieurs groupes d'organisation.

Prérequis

- URL du serveur AirWatch que l'administrateur utilise pour se connecter à la console d'administration d'AirWatch.
- Clé API d'administration AirWatch utilisée pour faire des demandes API depuis VMware Identity Manager au serveur AirWatch afin de configurer l'intégration.
- Fichier de certificat AirWatch utilisé pour passer des appels API et mot de passe du certificat. Le fichier de certificat doit être au format .p12.
- Clé API d'utilisateur inscrit AirWatch.
- ID de groupe AirWatch de votre locataire, qui est l'identifiant du locataire dans AirWatch.

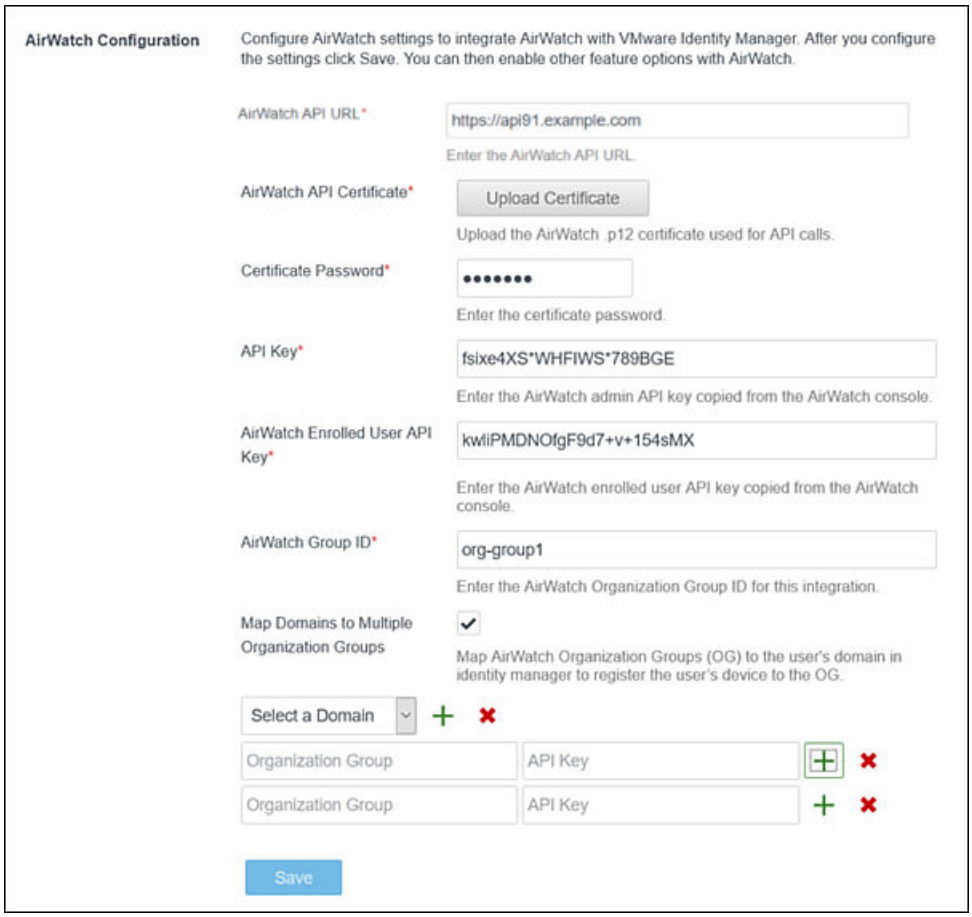
Procédure

1. Dans l'onglet Identité et gestion de l'accès de la console d'administration de VMware Identity Manager, cliquez sur **Configuration > AirWatch**.
2. Entrez les paramètres d'intégration d'AirWatch dans les champs suivants.

Champ	Description
URL API d'AirWatch	Entrez l'URL API d'AirWatch. Par exemple, `https://api91.example.com`
Certificat API AirWatch	Téléchargez le fichier de certificat utilisé pour passer des appels API.
Mot de passe du certificat	Entrez le mot de passe du certificat.
Clé API d'administration AirWatch	Entrez la valeur de clé API d'administration. Exemple de valeur de clé API `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
Clé API d'utilisateur inscrit AirWatch	Entrez la valeur de clé API d'utilisateur inscrit.
ID de groupe AirWatch	Entrez l'ID de groupe AirWatch pour le groupe d'organisation dans lequel la clé API et le compte d'administrateur ont été créés.

3. Pour mapper des domaines à plusieurs groupes d’organisation, sélectionnez la case à cocher **Mapper les domaines sur plusieurs groupes d’organisation**.
   a. Sélectionnez le domaine à mapper dans le menu déroulant et saisissez l'ID du groupe d'organisation et la clé API d'administration pour ce groupe dans les zones de texte.
   b. Cliquez sur **+** afin de mapper des groupes d'organisation supplémentaires au domaine.
   c. Pour mapper un autre domaine, cliquez sur **+** à côté du menu déroulant.

4 Cliquez sur **Enregistrer**.



Suivant

- Activez l'option de la fonctionnalité Catalogue unifié pour fusionner des applications configurées dans le catalogue AirWatch avec le catalogue unifié.
- Activez la vérification de la conformité pour vérifier que les périphériques gérés par AirWatch respectent les stratégies de conformité d'AirWatch.

Mappage de domaines VMware Identity Manager à plusieurs groupes d'organisation dans AirWatch

Lors de la configuration d'utilisateurs et de périphériques dans AirWatch, AirWatch utilise des groupes organisationnels pour organiser et regrouper les utilisateurs et pour définir des autorisations. Lorsqu'AirWatch est intégré à VMware Identity Manager, les clés REST API de l'utilisateur d'administration et d'inscription peuvent uniquement être configurées sur le groupe organisationnel AirWatch de type Client.

Dans les environnements AirWatch configurés pour l'architecture mutualisée, un grand nombre de groupes organisationnels est créé pour les utilisateurs et les périphériques. Les périphériques sont enregistrés ou inscrits dans un groupe organisationnel. Les groupes organisationnels peuvent être configurés dans des configurations uniques dans un environnement d'architecture mutualisée. Par exemple, groupes organisationnels par zones géographiques, services ou cas d'utilisation distincts.

Vous pouvez lier des domaines configurés dans VMware Identity Manager à des groupes organisationnels spécifiques dans AirWatch afin de gérer l'enregistrement du périphérique via Workspace ONE. Lorsque les utilisateurs se connectent à Workspace ONE, un événement d'enregistrement de périphérique est déclenché dans VMware Identity Manager. Lors de l'enregistrement du périphérique, une demande est envoyée à AirWatch pour extraire toutes les applications auxquelles la combinaison utilisateur/périphérique est autorisée à accéder.

Les groupes organisationnels de périphérique doivent être identifiés lorsqu'AirWatch est intégré à VMware Identity Manager afin que le gestionnaire d'identité puisse localiser l'utilisateur et enregistrer correctement le périphérique dans le groupe organisationnel approprié.

Lorsque vous configurez les paramètres d'AirWatch dans le service VMware Identity Manager, vous pouvez saisir l'ID de groupe organisationnel de périphérique et les clés de l'API pour mapper plusieurs groupes organisationnels à un domaine. Lorsque les utilisateurs se connectent à Workspace ONE à partir de leurs périphériques, les enregistrements des utilisateurs sont vérifiés et le périphérique est enregistré sur le groupe organisationnel approprié dans AirWatch.

Pour plus d'informations sur la configuration de plusieurs groupes organisationnels, reportez-vous à la section Stratégies de déploiement de la configuration de plusieurs groupes organisationnels AirWatch.

Remarque Lorsqu'AirWatch est intégré à VMware Identity Manager et que plusieurs groupes organisationnels AirWatch sont configurés, l'option Catalogue global d'Active Directory ne peut pas être configurée pour être utilisée avec le service VMware Identity Manager.

Activer le catalogue Workspace ONE pour AirWatch

Lorsque vous configurez VMware Identity Manager avec votre instance AirWatch, vous pouvez activer le catalogue Workspace ONE. Les utilisateurs finaux voient toutes les applications auxquelles ils peuvent accéder à partir du portail Workspace ONE.

Procédure

1. Dans l'onglet Identité et gestion de l'accès de la console d'administration, cliquez sur **Configuration > AirWatch**.
2. Dans la section Catalogue unifié de cette page, sélectionnez **Activer**.
3. Cliquez sur **Enregistrer**.

Suivant

Indiquez aux utilisateurs finaux d’AirWatch comment accéder au catalogue unifié et voir leur portail Workspace ONE.

Activation de la vérification de la conformité pour les périphériques gérés par AirWatch

Lorsque les utilisateurs inscrivent leurs périphériques, des exemples contenant des données utilisées pour évaluer la conformité sont envoyés selon un calendrier établi. L'évaluation de ces exemples de données garantit que le périphérique répond aux règles de conformité définies par l'administrateur dans la console AirWatch. Si le périphérique n'est plus conforme, les mesures correspondantes configurées dans la console AirWatch sont prises.

Le service VMware Identity Manager inclut une option de stratégie d'accès pouvant être configurée de manière à vérifier l'état de conformité du périphérique sur le serveur AirWatch lorsque des utilisateurs se connectent à partir du périphérique. La vérification de la conformité garantit que les utilisateurs ne peuvent pas se connecter à une application ou utiliser l'authentification unique sur le portail Workspace ONE si le périphérique devient non conforme. Une fois le périphérique de nouveau conforme, il est possible de se connecter.

L'application Workspace ONE se déconnecte automatiquement et bloque l'accès aux applications si le périphérique est compromis. Si le périphérique a été inscrit via la gestion adaptative, une commande de nettoyage d'entreprise émise via la console d'AirWatch désinscrit le périphérique et supprime les applications gérées à partir du périphérique. Les applications non gérées ne sont pas supprimées.

Pour plus d'informations sur les stratégies de conformité d'AirWatch, consultez le Guide de gestion des périphériques mobiles VMware AirWatch, disponible sur le site Web des ressources d'AirWatch.

Autoriser l'authentification du mot de passe de l'utilisateur via AirWatch

Pour implémenter l'authentification avec AirWatch Cloud Connector, vous devez activer le mot de passe d'authentification via la fonctionnalité AirWatch.

Prérequis

- AirWatch configuré dans VMware Identity Manager.
- AirWatch Cloud Connector installé et activé.
- Services d'annuaire AirWatch intégrés à Active Directory.

Procédure

1. Dans l'onglet Identité et gestion de l'accès de la console d'administration, cliquez sur **Configuration > AirWatch**.
2. Dans la section Authentification par mot de passe utilisateur via AirWatch, sélectionnez **Activer**.
3. Cliquez sur **Enregistrer**.

Suivant

Reportez-vous à la section Implémentation de l'authentification avec AirWatch Cloud Connector pour utiliser l’authentification AirWatch Cloud Connector.

Configurer une règle de stratégie d’accès

Pour fournir un accès sécurisé au portail Workspace ONE des utilisateurs et lancer des applications Web et de poste de travail, vous configurez des stratégies d'accès. Les stratégies d'accès incluent des règles qui spécifient les critères devant être satisfaits afin de pouvoir vous connecter et utiliser vos ressources.

Vous devez modifier les règles de stratégie par défaut pour sélectionner les méthodes d’authentification que vous avez configurées. Une règle de stratégie peut être configurée pour authentifier des utilisateurs en fonction de conditions, telles que le réseau, le type de périphérique, l'état d'inscription et de conformité du périphérique AirWatch ou l'application en cours d'accès. Une règle de stratégie peut également être configurée pour refuser l'accès à des utilisateurs par plage réseau et type de dispositif. Vous pouvez ajouter des groupes à une stratégie pour gérer l'authentification pour des groupes spécifiques.

Lorsque la vérification de la conformité est activée, vous créez une règle de stratégie d'accès qui requiert l'authentification et la vérification de la conformité des périphériques gérés par AirWatch.

La règle de stratégie de vérification de la conformité fonctionne dans une chaîne d'authentification avec Mobile SSO pour iOS, Mobile SSO pour Android et le déploiement de Cloud de certificat. La méthode d'authentification à utiliser doit précéder l'option de conformité des périphériques dans la configuration de la règle de stratégie.

Prérequis

Méthodes d’authentification configurées et associées à un fournisseur d’identité intégré.

Vérification de la conformité activée sur la page AirWatch de VMware Identity Manager.

Procédure

1. Sur l'onglet Gestion des identités et des accès de la console d'administration, sélectionnez **Gérer > Stratégies**.
2. Cliquez sur **Modifier la stratégie par défaut**.
3. Cliquez sur **Suivant**.
4. Cliquez sur **Ajouter une règle de stratégie** pour ajouter une règle ou sélectionnez une règle à modifier.

   La page Ajouter une règle de stratégie s'affiche.

   a. Sélectionnez la plage réseau pour appliquer cette règle.

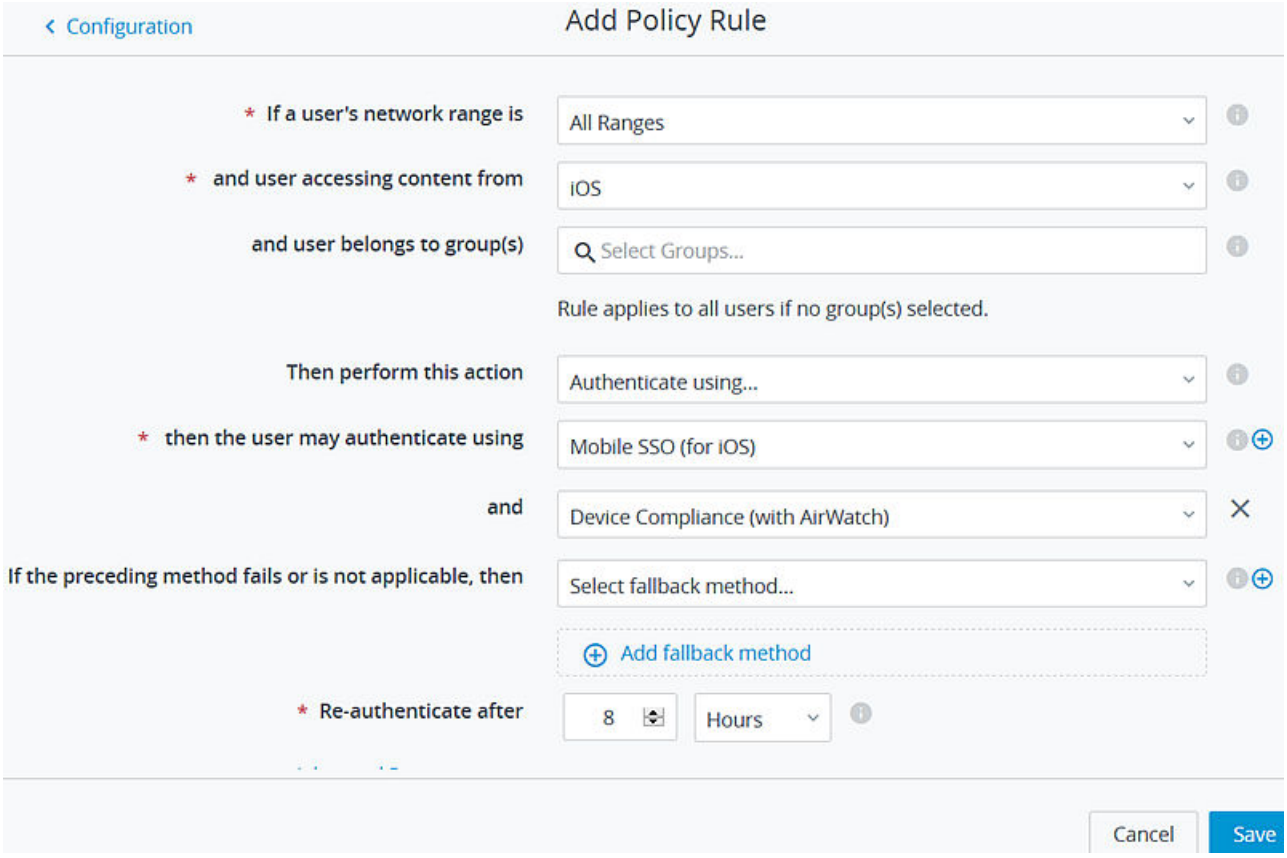
   b. Dans le menu déroulant **et que l'utilisateur accède à du contenu provenant de**, sélectionnez le type de périphérique mobile.

   c. Dans le menu déroulant **alors l'utilisateur peut s'authentifier selon**, sélectionnez la méthode d'authentification à utiliser.

d Cliquez sur **+** pour sélectionner **Conformité des périphériques (avec AirWatch)**

e Cliquez sur **Enregistrer**.

5 Cliquez sur **Enregistrer**.



Mise à jour de VMware Identity Manager après la mise à niveau d'AirWatch

Lorsque vous effectuez la mise à niveau d'AirWatch vers une nouvelle version, vous devez mettre à jour les options Catalogue unifié et Authentification par mot de passe utilisateur sur la page de configuration d'AirWatch dans la console d'administration de VMware Identity Manager.

Lorsque vous enregistrez ces options après la mise à niveau d'AirWatch, les paramètres d'AirWatch dans le service VMware Identity Manager sont mis à jour avec la nouvelle version d'AirWatch.

Procédure

1 Après la mise à niveau d'AirWatch, connectez-vous à la console d'administration de VMware Identity Manager.

2 Dans l'onglet Identité et gestion de l'accès, cliquez sur **Configuration > AirWatch**.

3 Faites défiler la page jusqu'à la section **Catalogue unifié** et cliquez sur **Enregistrer**.

4 Faites défiler jusqu'à la section **Authentification par mot de passe utilisateur via AirWatch** et cliquez sur **Enregistrer**.

La configuration d'AirWatch est mise à jour avec la nouvelle version dans le service VMware Identity Manager.

Implémentation de l'authentification avec AirWatch Cloud Connector

Le composant AirWatch Cloud Connector (ACC) de VMware Enterprise Systems Connector est intégré à VMware Identity Manager pour l'authentification par mot de passe utilisateur dans Workspace ONE.

Remarque Vous installez ACC et configurez le composant ACC dans AirWatch. Consultez le guide d'installation et de configuration de VMware Enterprise Systems Connector pour plus d'informations sur l'installation et la configuration d'AirWatch Cloud Connector. Une fois ACC installé et configuré, vous intégrez les services d'annuaire AirWatch à Active Directory. Consultez le guide des services d'annuaire de VMware AirWatch pour la procédure d'activation des services d'annuaire.

Pour implémenter l'authentification AirWatch Cloud Connector pour Workspace ONE, dans la console d'administration de VMware Identity Manager, la méthode d'authentification par mot de passe (AirWatch Connector) est associée à un fournisseur d'identité intégré.

Vous pouvez activer le support juste-à-temps dans AirWatch pour ajouter les nouveaux utilisateurs à l'annuaire VMware Identity Manager lorsque des utilisateurs se connectent pour la première fois. Lorsque la prise en charge juste-à-temps est activée, les utilisateurs n'ont pas besoin d'attendre la prochaine synchronisation planifiée à partir du serveur AirWatch pour accéder à Workspace ONE. Les nouveaux utilisateurs se connectent à leur portail Workspace ONE, depuis un périphérique iOS ou Android ou depuis leur ordinateur, puis entrent leur nom d'utilisateur et leur mot de passe Active Directory. Le service VMware Identity Manager authentifie les informations d'identification Active Directory via AirWatch Cloud Connector et ajoute le profil utilisateur au répertoire.

Une fois les méthodes d'authentification associées dans les fournisseurs d'identité, vous devez créer des stratégies d'accès à appliquer à ces méthodes.

Remarque L'authentification par nom d'utilisateur et mot de passe est intégrée dans le déploiement d'AirWatch Cloud Connector. Pour authentifier les utilisateurs à l'aide d'autres méthodes d'authentification prises en charge par VMware Identity Manager, le connecteur VMware Identity Manager doit être configuré.

Gestion du mappage d'attributs utilisateur

Vous pouvez configurer le mappage d'attribut utilisateur entre l'annuaire AirWatch et l'annuaire VMware Identity Manager.

La page des attributs utilisateur dans l'onglet VMware Identity Manager, Identity & Access Management répertorie les attributs d'annuaire par défaut qui sont mappés aux attributs de l'annuaire AirWatch. Les attributs obligatoires sont signalés par un astérisque. Les utilisateurs pour qui il manque un attribut obligatoire dans le profil ne sont pas synchronisés avec le service VMware Identity Manager.

Tableau 2-1. Mappage d'attributs d'annuaire AirWatch par défaut

Nom de l'attribut utilisateur de VMware Identity Manager	Mappage par défaut avec l'attribut utilisateur AirWatch
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domaine	Contrôleur
disabled (utilisateur externe désactivé)	disabled
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Email*
userName	username*

Synchroniser des utilisateurs et des groupes entre l'annuaire AirWatch Directory et VMware Identity Directory

Configurez les paramètres de VMware Identity Manager dans la console d'administration d'AirWatch pour établir une connexion entre votre instance du groupe d'organisation du répertoire AirWatch et VMware Identity Manager. Cette connexion est utilisée pour synchroniser des utilisateurs et des groupes avec un répertoire créé dans le service VMware Identity Manager.

Les utilisateurs et les groupes commencent par synchroniser le répertoire VMware Identity Manager manuellement. Le planning de synchronisation d'AirWatch détermine à quel moment les utilisateurs et les groupes se synchronisent avec le répertoire VMware Identity Manager.

Lorsqu'un utilisateur ou un groupe est ajouté ou supprimé sur le serveur AirWatch, la modification est immédiatement reflétée sur le service VMware Identity Manager.

Prérequis

- Nom et mot de passe d'administrateur local de VMware Identity Manager.
- Identifiez des valeurs d'attribut à mapper depuis le répertoire AirWatch. Voir Gestion du mappage d'attributs utilisateur.

Procédure

1 Dans la console d'administration d'AirWatch, sur la page Groupes et paramètres, Tous les paramètres, sélectionnez le groupe d'organisation de niveau Global > Client et accédez à **Système > Intégration d'entreprise** >**VMware Identity Manager**.

2 Dans la section Serveur, cliquez sur **Configurer**.

Remarque Le bouton de configuration n'est disponible que lorsque le service de répertoire est également configuré pour le même groupe d'organisation. Si le bouton Configurer n'est pas visible, vous ne vous trouvez pas dans le bon groupe d'organisation. Vous pouvez modifier le groupe d'organisation dans le menu déroulant Global.

3 Entrez les paramètres de VMware Identity Manager.

Option	Description
URL	Entrez l'URL VMware de votre locataire. Par exemple, `https://myco.identitymanager.com`.
Nom d'utilisateur de l'administrateur	Entrez le nom d'utilisateur Admin local de VMware Identity Manager.
Mot de passe de l'administrateur	Entrez le mot de passe de l'utilisateur Admin local de VMware Identity Manager.

4 Cliquez sur **Suivant**.

5 Activez le mappage personnalisé pour configurer le mappage d'attributs utilisateur entre AirWatch et le service VMware Identity Manager.

6 Cliquez sur **Tester la connexion** pour vérifier que les paramètres sont corrects.

7 Cliquez sur **Synchroniser maintenant** pour synchroniser manuellement tous les utilisateurs et les groupes avec le service VMware Identity Manager.

Remarque Pour contrôler la charge système, la synchronisation manuelle ne peut être effectuée que quatre heures après une précédente synchronisation.

Un annuaire AirWatch est créé dans le service VMware Identity Manager et les utilisateurs et les groupes sont synchronisés avec un annuaire dans VMware Identity Manager.

Suivant

Examinez l'onglet Utilisateurs et groupes dans la console d'administration de VMware Identity Manager pour vérifier que les noms d'utilisateur et de groupe sont synchronisés.

Gestion de la configuration de l'authentification par mot de passe sur AirWatch

Vous pouvez vérifier et gérer la configuration du mot de passe (AirWatch Connector) qui a été configurée lorsque vous avez installé AirWatch et ajouté le service VMware Identity Manager.

La méthode d'authentification par mot de passe (AirWatch Connector) est gérée à partir de la page Gestion des identités et des accès > Méthodes d'authentification et est associée au fournisseur d'identité intégré de la page Fournisseurs d'identité.

Important Lors d'une mise à niveau du logiciel AirWatch Cloud Connector, veillez à mettre à jour la configuration AirWatch de VMware Identity Manager dans la page AirWatch de la console d'administration de VMware Identity Manager.

Procédure

1 Pour consulter et gérer la configuration, dans l'onglet Gestion des identités et des accès, sélectionnez **Méthodes d'authentification**.

2 Dans la colonne Configurer de **Mot de passe (AirWatch Connector)**, cliquez sur l'icône en forme de crayon.

3 Vérifiez la configuration.

Option	Description
Activer l'authentification par mot de passe AirWatch	Cette case à cocher active l'authentification par mot de passe AirWatch.
URL de la console d'administration d'AirWatch	Pré-remplie avec l'URL d'AirWatch.
Clé API AirWatch	Pré-remplie avec la clé API d'administration AirWatch.
Certificat utilisé pour l'authentification	Pré-remplie avec le certificat d'AirWatch Cloud Connector.
Mot de passe du certificat	Pré-remplie avec le mot de passe du certificat d'AirWatch Cloud Connector.
ID de groupe AirWatch	Pré-remplie avec l'ID du groupe d'organisation.
Nombre de tentatives d'authentification autorisées	Le nombre maximum de tentatives de connexion échouées lors de l'utilisation de l'authentification par mot de passe AirWatch. Plus aucune connexion n'est autorisée une fois que ce nombre maximal de tentatives de connexion échouées est atteint. Le service VMware Identity Manager tente d'utiliser la méthode d'authentification de secours si elle est configurée. La valeur par défaut est de cinq tentatives.
JIT activé	Si JIT n'est pas activé, cochez cette case pour activer le provisionnement juste-à-temps d'utilisateurs dans le service VMware Identity Manager dynamiquement lorsqu'ils se connectent pour la première fois.

4 Cliquez sur **Enregistrer**.

Configurer des fournisseurs d'identité intégrés

Vous pouvez configurer plusieurs fournisseurs d'identité intégrés et associer des méthodes d'authentification qui ont été configurées sur la page Gérer > Méthodes d'authentification de l'onglet Identité et gestion de l'accès.

Procédure

1 Dans l'onglet Identité et gestion de l'accès, accédez à **Gérer > Fournisseurs d'identité**.

2 Cliquez sur **Ajouter un fournisseur d'identité**, puis sélectionnez **Créer un IDP intégré**.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance du fournisseur d'identité intégré.
Utilisateurs	Sélectionner des utilisateurs pour l'authentification. Les annuaires configurés sont répertoriés.

Option	Description
Réseau	Les plages réseau existantes configurées dans le service sont répertoriées. Sélectionnez les plages réseau des utilisateurs en fonction des adresses IP que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.
Méthodes d'authentification	Les méthodes d'authentification qui sont configurées sur le service sont affichées. Cochez la case des méthodes d'authentification à associer à ce fournisseur d'identité intégré. Pour Conformité des périphériques (avec AirWatch) et Mot de passe (AirWatch Connector), vérifiez que l'option est activée sur la page de configuration d'AirWatch.

3 Cliquez sur **Ajouter**.

Suivant

Configurez la règle de stratégie d’accès par défaut pour ajouter la stratégie d’authentification à la règle. Voir Configurer une règle de stratégie d’accès

Implémentation de l'authentification unique mobile pour des périphériques iOS gérés par AirWatch

3

Pour l'authentification des périphériques iOS, VMware Identity Manager utilise un fournisseur d'identité intégré au service VMware Identity Manager pour fournir l'accès à l'authentification Mobile SSO.

Cette méthode d'authentification pour les périphériques iOS utilise un centre de distribution de clés (KDC) sans utiliser un connecteur ou un système tiers. L'authentification Kerberos permet aux utilisateurs correctement connectés à leur domaine d'accéder à leur portail d'applications Workspace ONE sans devoir saisir de nouveau leurs informations d'identification.

Ce chapitre aborde les rubriques suivantes :

Présentation de l'implémentation pour configurer Mobile SSO pour iOS

L'implémentation de l'authentification Mobile SSO pour périphériques iOS 9 ou version ultérieure gérés par AirWatch nécessite les étapes de configuration suivantes.

- Téléchargez le certificat de l'émetteur pour configurer Mobile SSO pour iOS
  - Si vous utilisez des services de certificats Active Directory, configurez un modèle d'autorité de certification pour la distribution de certificats Kerberos dans les services de certificats Active Directory. Ensuite, configurez AirWatch pour qu'il utilise l'autorité de certification Active Directory. Ajoutez le modèle de certificat dans la console d'administration d'AirWatch. Téléchargez le certificat de l'émetteur pour configurer Mobile SSO pour iOS.

  - Si vous utilisez une autorité de certification AirWatch, activez Certificats sur la page Intégrations de VMware Identity Manager. Téléchargez le certificat de l'émetteur pour configurer Mobile SSO pour iOS.
- Établissez le centre de distribution de clés (KDC) à utiliser.
- Configurez le profil de périphérique iOS et activez l'authentification unique dans la console d'administration d'AirWatch.
- Configurez la méthode d’authentification Mobile SSO (iOS)
- Configurez le fournisseur d'identité intégré et associez l'authentification Mobile SSO pour iOS dans la console d'administration de VMware Identity Manager.

Configurer une autorité de certification Active Directory dans AirWatch

Pour configurer l'authentification unique sur des périphériques mobiles iOS 9 gérés par AirWatch, vous pouvez établir une relation de confiance entre Active Directory et AirWatch et activer la méthode d'authentification Mobile SSO pour iOS dans VMware Identity Manager.

Après avoir configuré le modèle d'autorité de certification et le modèle de certificat pour la distribution de certificats Kerberos dans les services de certificats Active Directory, activez AirWatch pour demander le certificat utilisé pour l'authentification et ajouter l'autorité de certification à la console d'administration d'AirWatch.

Procédure

1 Dans le menu principal de la console d'administration d'AirWatch, accédez à **Périphériques > Certificats > Autorités de certification**.

2 Cliquez sur **Ajouter**.

3 Configurez ce qui suit sur la page Autorité de certification.

Remarque Vérifiez que Microsoft AD CS est sélectionné comme type d'autorité avant de commencer à remplir ce formulaire.

Option	Description
Nom	Entrez un nom pour la nouvelle autorité de certification.
Type d'autorité	Vérifiez que **Microsoft ADCS** est sélectionné.
Protocole	Sélectionnez **ADCS** comme protocole.
Nom d'hôte de serveur	Entrez l'URL du serveur. Entrez le nom d'hôte au format `https://{servername.com}/certsrv.adcs/`. Le site peut être http ou https, en fonction de la configuration du site. L'URL doit inclure la `/` de fin. **Remarque** Si la connexion échoue lorsque vous testez l'URL, supprimez la partie http:// ou https:// de l'adresse et testez de nouveau la connexion.

Option	Description
Nom d'autorité	Entrez le nom de l'autorité de certification à laquelle le point de terminaison ADCS est connecté. Vous pouvez voir ce nom en lançant l'application Autorité de certification sur le serveur d'autorité de certification.
Authentification	Vérifiez que **Compte de service** est sélectionné.
Nom d'utilisateur et mot de passe	Entrez le nom d'utilisateur et le mot de passe du compte d'administrateur AD CS avec un accès suffisant pour autoriser AirWatch à demander et émettre des certificats.

4 Cliquez sur **Enregistrer**.

Suivant

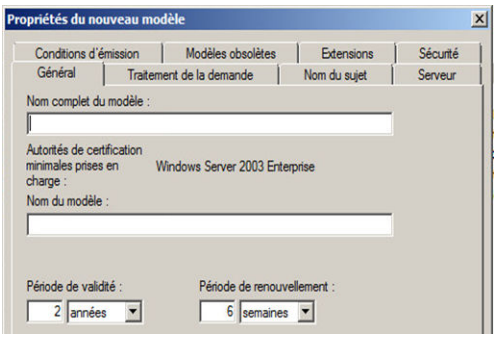
Configurez le modèle de certificat dans AirWatch.

Configuration d'AirWatch pour qu'il utilise l'autorité de certification Active Directory

Votre modèle d'autorité de certification doit être correctement configuré pour la distribution de certificats Kerberos. Dans les services de certificats Active Directory (AD CS), vous pouvez dupliquer le modèle Authentification Kerberos existant pour configurer un nouveau modèle d'autorité de certification pour l'authentification Kerberos iOS.

Lorsque vous dupliquez le modèle Authentification Kerberos depuis AD CS, vous devez configurer les informations suivantes dans la boîte de dialogue Propriétés du nouveau modèle.

Figure 3-1. Boîte de dialogue Propriétés du nouveau modèle des services de certificats Active Directory



- Onglet **Général**. Entrez le nom complet du modèle et le nom du modèle. Par exemple iOSKerberos. Il s'agit du nom complet indiqué dans les composants logiciels enfichables Modèles de certificat, Certificats et Autorité de certification.
- Onglet **Traitement de la demande**. Activez **Autoriser l'exportation de la clé privée**.
- Onglet **Nom du sujet**. Activez le bouton radio **Fournir dans la demande**. Le nom du sujet est fourni par AirWatch lorsqu'il demande le certificat.
- Onglet **Extensions**. Définissez les stratégies d'application.
  - Sélectionnez Stratégies d'application et cliquez sur Modifier pour ajouter une nouvelle stratégie d'application. Nommez cette stratégie Authentification client Kerberos.

- Ajoutez l'identificateur d'objet (OID) comme suit : 1.3.6.1.5.2.3.4. Ne le modifiez pas.
- Dans la liste Description des stratégies d'application, supprimez toutes les stratégies répertoriées, sauf les stratégies Authentification client Kerberos et Authentification par carte à puce.

- Onglet **Sécurité**. Ajoutez le compte AirWatch à la liste d'utilisateurs pouvant utiliser le certificat. Définissez les autorisations du compte. Définissez Contrôle total pour autoriser le principal de sécurité à modifier tous les attributs d'un modèle de certificat, notamment les autorisations du modèle de certificat. Autrement, définissez les autorisations en fonction des exigences de votre entreprise.

Enregistrez les modifications. Ajoutez le modèle à la liste des modèles utilisés par l'autorité de certification Active Directory.

Dans AirWatch, configurez l'autorité de certification et ajoutez le modèle de certificat.

Ajouter un modèle de certificat dans AirWatch

Vous ajoutez le modèle de certificat qui associe l'autorité de certification utilisée pour générer le certificat de l'utilisateur.

Prérequis

Configurez l'autorité de certification dans AirWatch.

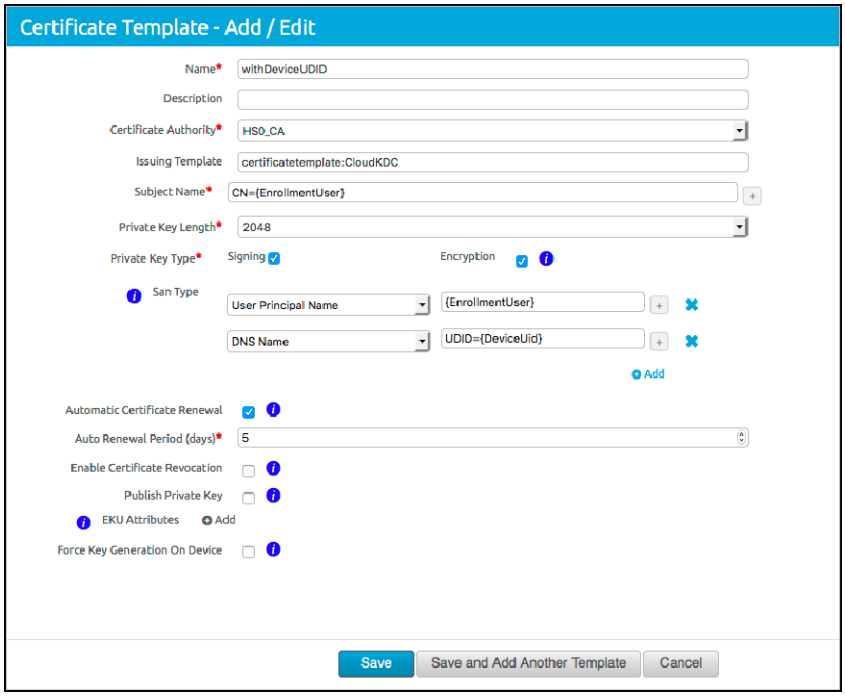
Procédure

1. Dans la console d'administration d'AirWatch, accédez à **Système > Intégration d'entreprise > Autorités de certification**.
2. Sélectionnez l'onglet **Modèle de demande** et cliquez sur **Ajouter**.
3. Configurez ce qui suit sur la page du modèle de certificat.

Option	Description
Nom	Entrez le nom du nouveau modèle de demande dans AirWatch.
Autorité de certification	Dans le menu déroulant, sélectionnez l'autorité de certification qui a été créée.
Modèle d'émission	Entrez le nom du modèle de certificat d'autorité de certification Microsoft exactement comme vous l'avez créé dans AD CS. Par exemple, `iOSKerberos`.
Nom du sujet	Après **CN=**, entrez `{EnrollmentUser}`, où la zone de texte {} est la valeur de recherche d'AirWatch. Le texte entré ici est le sujet du certificat, qui peut être utilisé pour déterminer qui a reçu le certificat.
Longueur de clé privée	Cette longueur de clé privée correspond au paramètre sur le modèle de certificat utilisé par AD CS. En général, elle est de 2 048.
Type de clé privée	Cochez la case **Signature et chiffrement**.
Type d'autre nom du sujet	Pour l'autre nom du sujet, sélectionnez **Nom principal de l'utilisateur**. La valeur doit être `{EnrollmentUser}`. Si la vérification de la conformité du périphérique est configurée avec l'authentification Kerberos, vous devez définir un deuxième type d'autre nom du sujet pour inclure l'UDID. Sélectionnez le type d'autre nom du sujet **DNS**. La valeur doit être **UDID={DeviceUid}**.

Option	Description
Renouvellement automatique des certificats	Cochez la case pour que les certificats utilisant ce modèle soient renouvelés automatiquement avant leur date d'expiration.
Période de renouvellement automatique (jours)	Spécifiez le renouvellement automatique en jours.
Activer la révocation de certificat	Cochez la case pour que les certificats soient automatiquement révoqués lorsque des périphériques applicables sont désinscrits ou supprimés, ou si le profil applicable est supprimé.
Publier la clé privée	Cochez cette case pour publier la clé privée.
Destination de la clé privée	Service de répertoire ou Service Web personnalisé

4 Cliquez sur **Enregistrer**.



Suivant

Dans la console d'administration du fournisseur d'identité, configurez le fournisseur d'identité intégré avec la méthode d'authentification Mobile SSO pour iOS.

Utilisation de l'autorité de certification AirWatch pour l'authentification Kerberos

Vous pouvez utiliser l'autorité de certification AirWatch au lieu de l'autorité de certification Active Directory pour configurer l'authentification unique avec l'authentification Kerberos intégré sur des périphériques mobiles iOS 9 gérés par AirWatch. Vous pouvez activer l'autorité de certification AirWatch dans la console d'administration d'AirWatch et exporter le certificat de l'émetteur de l'autorité de certification afin de l'utiliser dans le service VMware Identity Manager.

L'autorité de certification AirWatch est conçue pour suivre le protocole d'inscription du certificat simple (SCEP) et est utilisée avec des périphériques gérés par AirWatch qui prennent en charge SCEP. L'intégration de VMware Identity Manager à AirWatch utilise l'autorité de certification AirWatch pour émettre des certificats sur des périphériques mobiles iOS 9 dans le cadre du profil.

Le certificat racine de l'émetteur de l'autorité de certification AirWatch est également le certificat de signature OCSP.

Activer et exporter l'autorité de certification AirWatch

Lorsque VMware Identity Manager est activé dans AirWatch, vous pouvez générer le certificat racine de l'émetteur AirWatch et exporter le certificat pour l'utiliser avec l'authentification Mobile SSO pour iOS sur des périphériques mobiles iOS 9.

Procédure

1. Dans la console d'administration d'AirWatch, accédez à **Système > Intégration d'entreprise** > **VMware Identity Manager**.
2. Pour activer l'autorité de certification AirWatch, le type de groupe d'organisation doit être Client.

Conseil Pour afficher ou modifier le type de groupe, accédez à Groupes et paramètres, **Groupes > Groupes organisationnels**> **Détails du groupe organisationnel**.

3. Dans la section CERTIFICAT, cliquez sur **Activer**.

   La page affiche les détails du certificat racine de l'émetteur.
4. Cliquez sur **Exporter** et enregistrez le fichier.

Suivant

Dans la console d'administration de VMware Identity Manager, configurez l'authentification Kerberos dans le fournisseur d'identité intégré et ajoutez le certificat de l'émetteur de l'autorité de certification.

Utilisation d'un centre de distribution de clés pour l'authentification à partir de périphériques iOS

Pour le périphérique iOS, vous intégrez le service avec Kerberos. L'authentification Kerberos permet aux utilisateurs correctement connectés à leur domaine d'accéder à leur portail d'applications sans devoir saisir de nouveau leurs informations d'identification. Cette méthode d'authentification pour les périphériques iOS utilise un centre de distribution de clés (KDC) sans utiliser de connecteur ou de système tiers.

Les locataires de Cloud VMware Identity Manager n'ont pas besoin de gérer ni de configurer le KDC.

Pour les déploiements sur site, deux options de service KDC sont disponibles.

- KDC intégré. Le KDC intégré nécessite l'initialisation du KDC sur le dispositif et la création d'entrées DNS publiques afin de permettre aux clients Kerberos de trouver le KDC. Pour plus d'informations sur l'activation de KDC intégré, consultez le guide d'administration de VMware Identity Manager.

- KDC comme un service hébergé cloud VMware Identity Manager. L'utilisation de KDC dans le cloud nécessite de sélectionner le nom de domaine approprié dans la page adaptateur d'authentification iOS.

Remarque Lorsque VMware Identity Manager est installé et configuré avec AirWatch dans un environnement Windows, la méthode d'authentification Mobile pour iOS doit être configurée pour utiliser le service KDC hébergé sur le Cloud VMware Identity Manager.

Utilisation du service de cloud hébergé KDC

Pour prendre en charge l'utilisation d'authentification Kerberos pour Mobile SSO pour iOS, VMware Identity Manager fournit un service de cloud hébergé KDC.

Le service KDC hébergé dans le cloud doit être utilisé lorsque le service VMware Identity Manager est déployé avec AirWatch dans un environnement Windows.

Pour utiliser le KDC géré dans le dispositif VMware Identity Manager, reportez-vous à la Préparation pour utiliser l'authentification Kerberos sur les périphériques iOS dans le Guide de configuration et d'installation de VMware Identity Manager.

Lorsque vous configurez l'authentification Mobile SSO pour iOS, vous configurez le nom de domaine pour le service cloud hébergé KDC. Le domaine est le nom de l'entité administrative qui conserve des données d'authentification. Lorsque vous cliquez sur Enregistrer, le service VMware Identity Manager est enregistré avec le service cloud hébergé KDC. Les données stockées dans le service KDC sont basées sur la configuration de la méthode d'authentification Mobile SSO pour iOS, ce qui inclut le certificat d'autorité de certification, le certificat de signature OCSP et les détails de configuration de demande OCSP. Aucune autre information spécifique à l'utilisateur n'est stockée dans le service de cloud.

Les enregistrements de journalisation sont stockées dans le service cloud. Les informations identifiables personnellement (IPI) dans les enregistrements de journalisation incluent le nom principal Kerberos du profil utilisateur, les valeurs d'objet ND et UPN et E-mail SAN, le périphérique ID du certificat de l'utilisateur et le nom de domaine complet du service IDM auquel accède l'utilisateur.

Pour utiliser le service cloud hébergé KDC, VMware Identity Manager doit être configuré comme suit.

- Le nom de domaine complet du service VMware Identity Manager doit être accessible depuis Internet. Le certificat SSL/TLS utilisé par VMware Identity Manager doit être signé publiquement.
- Une demande/réponse du port 88 (UDP) et du port 443 (HTTPS/TCP) sortants doivent être accessibles depuis le service VMware Identity Manager.
- Si vous activez OCSP, le répondeur OCSP doit être accessible depuis Internet.

Configurer l'authentification Mobile SSO pour iOS

Vous configurez la méthode d'authentification Mobile SSO pour iOS à partir de la page Méthodes d'authentification dans la console d'administration. Sélectionnez la méthode d'authentification Mobile SSO (pour iOS) à utiliser dans le fournisseur d'identité intégré.

Prérequis

- Fichier PEM ou DER de l'autorité de certification utilisé pour émettre des certificats pour les utilisateurs dans le locataire AirWatch.
- Pour la vérification de révocation, certificat de signature du répondeur OCSP.
- Pour le service KDC, sélectionnez, le nom de domaine du service KDC. Si vous utilisez le service KDC intégré, le centre de distribution de clés (KDC) doit être initialisé. Reportez-vous à la section Installation et configuration de VMware Identity Manager pour voir les détails du KDC intégré.

Procédure

1. Dans l'onglet Identité et gestion de l'accès, accédez à **Gérer > Méthodes d'authentification**.
2. Dans la colonne Configurer de **Mobile SSO (pour iOS)**, cliquez sur l'icône.
3. Configurez la méthode d'authentification Kerberos.

Option	Description
Activer l'authentification KDC	Cochez cette case pour autoriser les utilisateurs à s'authentifier à l'aide de périphériques iOS prenant en charge l'authentification Kerberos.
Domaine	Si vous utilisez le cloud hébergé KDC, entrez le nom de domaine prédéfini pris en charge qui vous est fourni. Dans ce paramètre, le texte doit être saisi en lettres majuscules. Par exemple, OP.VMWAREIDENTITY.COM Si vous utilisez le KDC intégré, le nom de domaine que vous avez configuré lorsque vous avez initialisé le KDC s'affiche. La valeur de domaine est en lecture seule. Le domaine entré ici est le nom de domaine du fournisseur d'identité pour votre locataire.
Certificat d'autorité de certification racine et intermédiaire	Téléchargez le fichier de certificat de l'émetteur de l'autorité de certification. Le format de fichier peut être PEM ou DER.
Noms uniques de sujet du certificat d'autorité de certification téléchargés	Le contenu du fichier de certificat téléchargé s'affiche ici. Il est possible de télécharger plusieurs fichiers et tous les certificats inclus sont ajoutés à la liste.
Activer OCSP	Cochez la case pour utiliser le protocole de validation des certificats OCSP (Online Certificate Status Protocol) afin d'obtenir le statut de révocation d'un certificat.
Envoi de nonce OCSP	Cochez cette case si vous souhaitez que l'identificateur unique de la requête OCSP soit envoyé dans la réponse.
Certificat de signature du répondeur OCSP	Téléchargez le certificat OCSP du répondeur. Lorsque vous utilisez l'autorité de certification AirWatch, le certificat de l'émetteur est utilisé comme certificat OCSP. Téléchargez le certificat AirWatch ici également.
Nom unique de sujet du certificat de signature du répondeur OCSP	Le fichier de certificat OCSP téléchargé est répertorié ici.
Message Annuler	Créez un message de connexion personnalisé qui s'affiche lorsque l'authentification prend trop de temps. Si vous ne créez pas de message personnalisé, le message par défaut est `Attempting to authenticate your credentials`.

Option	Description
Activer le lien d'annulation	Lorsque l'authentification prend trop de temps, permettez aux utilisateurs de cliquer sur Annuler pour arrêter la tentative d'authentification et annuler la connexion. Lorsque le lien Annuler est activé, Annuler apparaît à la fin du message d'erreur d'authentification qui s'affiche.
URL du serveur de gestion des périphériques de l'entreprise	Entrez l'URL du serveur Mobile Device Management (MDM) pour rediriger les utilisateurs lorsque l'accès est refusé, car le périphérique n'est pas inscrit dans AirWatch pour la gestion MDM. Cette URL s'affiche dans le message d'erreur d'échec d'authentification. Si vous n'entrez pas une URL ici, le message générique Accès refusé s'affiche.

4 Cliquez sur **Enregistrer**.

Suivant

- Associez la méthode d'authentification Mobile SSO (pour iOS) dans le fournisseur d'identité intégré.
- Configurez la règle de stratégie d'accès par défaut pour l'authentification Kerberos pour les périphériques iOS. Vérifiez que cette méthode d'authentification est la première configurée dans la règle.
- Allez dans la console d'administration d'AirWatch et configurez le profil de périphérique iOS dans AirWatch, puis ajoutez le certificat de l'émetteur de certificat du serveur KDC à partir de VMware Identity Manager.

Configurer un fournisseur d'identité intégré pour l'authentification Mobile SSO pour iOS

Vous configurez le fournisseur d'identité intégré et associez la méthode d'authentification Mobile SSO pour iOS qui a été configurée sur la page Gérer > Méthodes d'authentification de l'onglet Identité et gestion de l'accès.

Prérequis

Authentification Mobile SSO (pour iOS) configurée sur la page Méthodes d'authentification.

Procédure

1 Dans l'onglet Identité et gestion de l'accès, accédez à **Gérer > Fournisseurs d'identité**.

2 Cliquez sur **Ajouter un fournisseur d'identité**, puis sélectionnez **Créer un IDP intégré**.

Option	Description
Nom du fournisseur d'identité	Entrez un nom pour cette instance du fournisseur d'identité intégré.
Utilisateurs	Sélectionner des utilisateurs pour l'authentification. Les annuaires configurés sont répertoriés.

Option	Description
Réseau	Les plages réseau existantes configurées dans le service sont répertoriées. Sélectionnez les plages réseau des utilisateurs en fonction des adresses IP que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.
Méthodes d'authentification	Les méthodes d'authentification qui sont configurées sur le service sont affichées. Cochez la case de la méthode d'authentification iOS à associer à ce fournisseur d'identité intégré. Ajoutez d'autres méthodes d'authentification. Pour Conformité des périphériques (avec AirWatch) et Mot de passe (AirWatch Connector), vérifiez que l'option est activée sur la page de configuration d'AirWatch.

3 Dans la section Exportation de certificat KDC, cliquez sur **Télécharger le certificat**. Enregistrez ce certificat dans un fichier accessible depuis la console d'administration d'AirWatch.

   Vous téléchargez ce certificat lorsque vous configurez le profil de périphérique iOS dans AirWatch.

4 Cliquez sur **Ajouter**.

Suivant

- Configurez la règle de stratégie d'accès par défaut pour l'authentification Kerberos pour les périphériques iOS. Vérifiez que cette méthode d'authentification est la première configurée dans la règle.
- Allez dans la console d'administration d'AirWatch et configurez le profil de périphérique iOS dans AirWatch, puis ajoutez le certificat de l'émetteur de certificat du serveur KDC à partir de VMware Identity Manager.

Configurer le profil Apple iOS dans AirWatch à l'aide de l'autorité de certification et du modèle de certificat Active Directory

Créez et déployez le profil de périphérique Apple iOS dans AirWatch afin de transférer les paramètres du fournisseur d'identité au périphérique. Ce profil contient les informations nécessaires pour que le périphérique se connecte au fournisseur d'identité VMware et le certificat que le périphérique a utilisé pour s'authentifier. Activez l'authentification unique pour autoriser l'accès transparent sans que l'authentification soit requise dans chaque application.

Prérequis

- Mobile SSO pour iOS est configuré dans VMware Identity Manager.
- Fichier d'autorité de certification Kerberos iOS enregistré sur un ordinateur accessible depuis la console d'administration d'AirWatch.
- L'autorité de certification et le modèle de certificat sont correctement configurés dans AirWatch.
- Liste d'URL et d'ID de bundle d'application qui utilisent l'authentification Mobile SSO pour iOS sur des périphériques iOS.

Procédure

1. Dans la console d'administration d'AirWatch, accédez à **Périphériques > Profils et ressources > Profils**.
2. Sélectionnez **Ajouter > Ajouter un profil** et sélectionnez **Apple iOS**.
3. Entrez le nom **`iOSKerberos`** et configurez les paramètres **Général**.
4. Dans le volet de navigation de gauche, sélectionnez **Informations d'identification > Configurer** pour configurer les informations d'identification.

Option	Description
Source des informations d'identification	Sélectionnez **Autorité de certification définie** dans le menu déroulant.
Autorité de certification	Sélectionnez l'autorité de certification dans la liste du menu déroulant.
Modèle de certificat	Sélectionnez le modèle de demande qui fait référence à l'autorité de certification dans le menu déroulant. Il s'agit du modèle de certificat créé dans Ajout du modèle de certificat dans AirWatch.

5. Cliquez de nouveau sur **+** dans l'angle inférieur droit de la page et créez un second lot d'informations d'identification.
6. Dans le menu déroulant **Source des informations d'identification**, sélectionnez **Télécharger**.
7. Entrez un nom d'informations d'identification.
8. Cliquez sur **Télécharger** pour télécharger le certificat racine du serveur KDC qui est téléchargé depuis la page Identité et gestion de l'accès > Gérer > Fournisseurs d'identité > Fournisseur d'identité intégré.
9. Dans le volet de navigation de gauche, sélectionnez **Authentification unique** et cliquez sur **Configurer**.
10. Entrez les informations de connexion.

Option	Description
Nom de compte	Entrez **`Kerberos`**.
Nom principal Kerberos	Cliquez sur **+** et sélectionnez **{EnrollmentUser}**.
Domaine	Entrez le nom de domaine Identity Manager de votre locataire. Le texte dans ce paramètre doit être en majuscules. Pour le nom de domaine, vous avez le choix entre **`VMWAREIDENTITY.COM`**, **`VMWAREIDENTITY.EU`** et **`VMWAREIDENTITY.ASIA`**. Entrez le nom de domaine que vous avez utilisé lorsque vous avez initialisé KDC dans le dispositif VMware Identity Manager. Par exemple : EXAMPLE.COM
Renouvellement de certificat	Sélectionnez **Certificate#1** dans le menu déroulant. Il s'agit du certificat d'autorité de certification Active Directory qui a été configuré en premier avec des informations d'identification.

Option	Description
Préfixes d'URL	Entrez les préfixes d'URL qui doivent correspondre pour utiliser ce compte pour l'authentification Kerberos sur HTTP. Entrez l'URL du serveur VMware Identity Manager sous la forme `https://myco.example.com`. Entrez l'URL du serveur VMware Identity Manager sous la forme `https://<tenant>.vmwareidentity.<region>`.
Applications	Entrez la liste des identités d'application qui sont autorisées à utiliser cette connexion. Pour exécuter l'authentification unique à l'aide du navigateur Safari intégré d'iOS, entrez le premier ID de bundle d'application sous la forme `com.apple.mobilesafari`. Entrez les ID de bundle d'application suivants. Les applications répertoriées doivent prendre en charge l'authentification SAML.

11 Cliquez sur **Enregistrer et publier**.

Suivant

Attribuez le profil de périphérique à un groupe intelligent. Les groupes intelligents sont des groupes personnalisables qui déterminent les périphériques de plate-forme, et les utilisateurs reçoivent une application attribuée, un livre, une stratégie de conformité, un profil de périphérique ou un provisionnement.

Configurer le profil Apple iOS dans AirWatch à l'aide de l'autorité de certification AirWatch

Créez et déployez le profil de périphérique Apple iOS dans AirWatch afin de transférer les paramètres du fournisseur d'identité au périphérique. Ce profil contient les informations nécessaires pour que le périphérique se connecte au fournisseur d'identité VMware et le certificat que le périphérique utilise pour s'authentifier.

Prérequis

- Kerberos intégré configuré dans VMware Identity Manager.
- Fichier de certificat racine du serveur KDC VMware Identity Manager enregistré sur un ordinateur accessible depuis la console d'administration d'AirWatch.
- Certificat activé et téléchargé depuis la console d’administration d'AirWatch page Système > Intégration d'entreprise > VMware Identity Manager.
- Liste d'URL et d'ID de bundle d'application qui utilisent l'authentification Kerberos intégré sur des périphériques iOS.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Périphériques > Profils et ressources > Profil > Ajouter un profil** et sélectionnez **Apple iOS**.

2 Configurez les paramètres **Général** du profil et entrez le nom du périphérique **`iOSKerberos`**.

3 Dans le volet de navigation de gauche, sélectionnez **SCEP > Configurer** pour configurer les informations d'identification.

Option	Description
Source des informations d'identification	Sélectionnez **Autorité de certification AirWatch** dans le menu déroulant.
Autorité de certification	Sélectionnez **Autorité de certification AirWatch** dans le menu déroulant.
Modèle de certificat	Sélectionnez **Authentification unique** pour définir le type de certificat émis par l'autorité de certification AirWatch.

4 Cliquez sur **Informations d'identification > Configurer** et créez d'autres informations d'identification.

5 Dans le menu déroulant **Source des informations d'identification**, sélectionnez **Télécharger**.

6 Entrez le nom des informations d'identification Kerberos iOS.

7 Cliquez sur **Télécharger** pour télécharger le certificat racine du serveur KDC VMware Identity Manager qui est téléchargé depuis la page Identité et gestion de l'accès > Gérer > Fournisseurs d'identité > Fournisseur d'identité intégré.

8 Dans le volet de navigation de gauche, sélectionnez **Authentification unique**.

9 Entrez les informations de connexion.

Option	Description
Nom de compte	Entrez `Kerberos`.
Nom principal Kerberos	Cliquez sur **+** et sélectionnez **{EnrollmentUser}**.
Domaine	Entrez le nom de domaine Identity Manager de votre locataire. Le texte dans ce paramètre doit être en majuscules. Pour le nom de domaine, vous avez le choix entre `VMWAREIDENTITY.COM`, `VMWAREIDENTITY.EU` et `VMWAREIDENTITY.ASIA`. Entrez le nom de domaine que vous avez utilisé lorsque vous avez initialisé KDC dans le dispositif VMware Identity Manager. Par exemple, `EXAMPLE.COM`.
Renouvellement de certificat	Sur les périphériques iOS 8 et versions ultérieures, sélectionnez le certificat utilisé pour réauthentifier l'utilisateur automatiquement sans interaction de sa part lorsque sa session d'authentification unique expire.
Préfixes d'URL	Entrez les préfixes d'URL qui doivent correspondre pour utiliser ce compte pour l'authentification Kerberos sur HTTP. Entrez l'URL du serveur VMware Identity Manager sous la forme `https://myco.example.com`. Entrez l'URL du serveur VMware Identity Manager sous la forme `https://<tenant>.vmwareidentity.<région>`.
Applications	Entrez la liste des identités d'application qui sont autorisées à utiliser cette connexion. Pour exécuter l'authentification unique à l'aide du navigateur Safari intégré d'iOS, entrez le premier ID de bundle d'application sous la forme `com.apple.mobilesafari`. Entrez les ID de bundle d'application suivants. Les applications répertoriées doivent prendre en charge l'authentification SAML.

10 Cliquez sur **Enregistrer et publier**.

Lorsque le profil iOS est correctement transféré aux périphériques des utilisateurs, ces derniers peuvent se connecter à VMware Identity Manager à l'aide de la méthode d'authentification Kerberos intégrée sans entrer leurs informations d'identification.

Suivant

Attribuez le profil de périphérique à un groupe intelligent. Les groupes intelligents sont des groupes personnalisables qui déterminent les périphériques de plate-forme, et les utilisateurs reçoivent une application attribuée, un livre, une stratégie de conformité, un profil de périphérique ou un provisionnement.

Attribuer un profil de périphérique AirWatch

Après avoir créé un profil de périphérique, vous attribuez le profil à un groupe intelligent.

Les groupes intelligents sont des groupes personnalisables qui déterminent les périphériques de plate-forme, et les utilisateurs reçoivent une application attribuée, une stratégie de conformité, un profil de périphérique ou un provisionnement. Consultez le guide de gestion des périphériques mobiles AirWatch.

Procédure

1. Dans la console d'administration d'AirWatch, accédez à **Périphériques > Profils et ressourcesProfils**.
2. Sélectionnez le profil de périphérique que vous souhaitez attribuer au groupe intelligent.
3. Dans l’onglet Général, cliquez sur la zone de texte **Groupes attribués** et sélectionnez **Créer un groupe d'attribution**.
4. Sur la page Créer un groupe intelligent, entrez le nom du groupe intelligent.
5. Sélectionnez **Plate-forme et système d'exploitation** et sélectionnez le système d'exploitation et la version corrects dans les menus déroulants.
6. Cliquez sur **Enregistrer et publier**.

Une fois que vous attribuez un groupe intelligent à l'option de périphérique, les utilisateurs peuvent se connecter à Workspace ONE et accéder aux applications à partir du catalogue.

Implémentation de l'authentification unique mobile pour des périphériques Android gérés par AirWatch

4

Mobile SSO pour Android est une implémentation de la méthode d'authentification de certificat pour les périphériques Android gérés par AirWatch.

L'application mobile VMware Tunnel est installée sur le périphérique Android. Le client VMware Tunnel est configuré pour accéder au service VMware Identity Manager à des fins d'authentification. Le client tunnel utilise le certificat client pour établir une session SSL authentifiée mutuelle et le service VMware Identity Manager récupère le certificat client à des fins d'authentification.

Remarque L'authentification Mobile SSO pour Android est prise en charge pour les périphériques Android 4.4 et versions ultérieures.

Authentification unique mobile sans accès VPN

L'authentification unique mobile pour périphériques Android peut être configurée pour contourner le serveur Tunnel lorsque l'accès VPN n'est pas requis. L'implémentation de l'authentification Mobile SSO pour Android sans utiliser de VPN utilise les mêmes pages de configuration que celles utilisées pour configurer VMware Tunnel. Comme vous n'installez pas le serveur Tunnel, vous n'entrez pas le nom d'hôte et le port du serveur VMware Tunnel. Vous configurez toujours un profil à l'aide du formulaire de profil VMware Tunnel, mais le trafic n'est pas dirigé vers le serveur Tunnel. Le client Tunnel est utilisé uniquement pour l'authentification unique.

Dans la console d'administration d'AirWatch, vous configurez les paramètres suivants.

- Composant Tunnel par application dans VMware Tunnel. Cette configuration permet aux périphériques Android d'accéder à des applications internes et publiques gérées via le client d'application mobile VMware Tunnel.
- Profil Tunnel par application. Ce profil est utilisé pour activer les capacités de tunneling par application pour Android.
- Sur la page Règles de trafic réseau, comme le serveur Tunnel n'est pas configuré, vous sélectionnez Contournement pour qu'aucun trafic ne soit dirigé vers un serveur Tunnel.

Authentification Mobile SSO avec accès VPN

Lorsque l'application configurée pour l'authentification unique est également utilisée pour accéder à des ressources intranet derrière le pare-feu, configurez l'accès VPN et le serveur Tunnel. Lorsque l'authentification unique est configurée avec VPN, le client Tunnel peut en option diriger le trafic de l'application et les demandes de connexion via le serveur Tunnel. Au lieu de la configuration par défaut utilisée pour le client Tunnel dans la console en mode authentification unique, la configuration doit pointer vers le serveur Tunnel.

L'implémentation de l'authentification Mobile SSO pour Android pour les périphériques Android gérés par AirWatch requiert la configuration de VMware Tunnel dans la console d'administration d'AirWatch et l'installation du serveur VMware Tunnel pour que vous puissiez configurer Mobile SSO pour Android dans la console d'administration de VMware Identity Manager. Le service VMware Tunnel fournit l'accès VPN par application aux applications gérées par AirWatch. VMware Tunnel permet également de diriger le trafic proxy d'une application mobile vers VMware Identity Manager pour l'authentification unique.

Dans la console d'administration d'AirWatch, vous configurez les paramètres suivants.

- Composant Tunnel par application dans VMware Tunnel. Cette configuration permet aux périphériques Android d'accéder à des applications internes et publiques gérées via le client d'application mobile VMware Tunnel.

  Une fois les paramètres de Tunnel configurés dans la console d'administration, vous téléchargez le programme d'installation de VMware AirWatch Tunnel et exécutez l'installation du serveur VMware Tunnel.
- Profil VPN Android. Ce profil est utilisé pour activer les capacités de tunneling par application pour Android.
- Activez le VPN pour chaque application qui utilise la fonctionnalité Tunnel par application à partir de la console d'administration.
- Créez des règles de trafic de périphérique avec une liste de toutes les applications qui sont configurées pour VPN par application, les détails du serveur proxy et l'URL de VMware Identity Manager.

Pour voir des informations détaillées sur l'installation et la configuration de VMware Tunnel, consultez le guide VMware Tunnel sur le site Web AirWatch Resources.

Ce chapitre aborde les rubriques suivantes :

- Configurer des règles de trafic dans AirWatch
- Configurer l'authentification Mobile SSO pour iOS dans le fournisseur d'identité intégré

Configurer l'authentification unique pour un périphérique Android dans la console d'administration d'AirWatch

Configurez l'authentification unique pour des périphériques Android afin de permettre aux utilisateurs de se connecter en toute sécurité à des applications d'entreprise, sans entrer leur mot de passe.

Pour configurer l'authentification unique pour des périphériques Android, vous n'avez pas besoin de configurer VMware Tunnel, mais vous configurez l'authentification unique avec la plupart des mêmes champs.

Prérequis

- Android 4.4 ou version ultérieure
- Les applications doivent prendre en charge SAML ou une autre norme de fédération prise en charge

Procédure

1. Dans la console d'administration d'AirWatch, accédez à **Système > Intégration d'entreprise > VMware Tunnel**.
2. La première fois que vous configurez VMware Tunnel, sélectionnez **Configurer** et suivez l'assistant de configuration. Sinon, sélectionnez **Remplacer** et cochez la case **Activer VMware Tunnel**. Ensuite, cliquez sur **Configurer**.
3. Sur la page Type de configuration, activez **Tunnel par application (Linux uniquement)**. Cliquez sur **Suivant**.

   Conservez **Basique** comme modèle de déploiement.
4. Sur la page Détails, entrez une valeur factice dans la zone de texte, car ce champ n'est pas requis pour la configuration de l'authentification unique. Cliquez sur **Suivant**.
5. Sur la page SSL, configurez le certificat SSL de tunneling par application. Pour utiliser un SSL public, cochez la case **Utiliser le certificat SSL public**. Cliquez sur **Suivant**.

   Le certificat racine de périphérique tunnel est généré automatiquement.

   Remarque Les certificats SAN ne sont pas pris en charge. Vérifiez que votre certificat est émis pour le nom d'hôte de serveur correspondant ou qu'il s'agit d'un certificat avec caractères génériques valide pour le domaine correspondant.

6 Sur la page Authentification, sélectionnez le type d'authentification de certificat à utiliser. Cliquez sur **Suivant**.

Option	Description
Valeur par défaut	Sélectionnez Par défaut pour utiliser les certificats émis par AirWatch.
Autorité de certification d'entreprise	Un menu déroulant répertoriant l'autorité de certification et le modèle de certificat que vous avez configurés dans AirWatch s'affiche. Vous pouvez également télécharger le certificat racine de votre autorité de certification.

Si vous sélectionnez Autorité de certification d'entreprise, vérifiez que le modèle d'autorité de certification contient le nom du sujet **CN=UDID**. Vous pouvez télécharger les certificats d'autorité de certification sur la page de configuration de VMware Tunnel.

7 Cliquez sur **Suivant**.

8 Sur la page Association de profil, associez un profil existant ou créez un profil VPN VMware Tunnel pour Android.

Si vous créez le profil à cette étape, vous devez toujours le publier. Consultez Configurer un profil Android dans AirWatch.

9 Examinez le résumé de votre configuration et cliquez sur **Enregistrer**.

Vous êtes dirigé vers la page de configuration des paramètres système.

Configurer des paramètres d'accès VPN de VMware Tunnel dans la console d'administration d' AirWatch

Vous activez le composant Tunnel par application dans les paramètres de VMware Tunnel afin de configurer la fonctionnalité de tunnelling par application pour les périphériques Android. Le tunneling par application permet à vos applications internes et publiques gérées d'accéder à vos ressources d'entreprise application par application.

Le VPN peut se connecter automatiquement lorsqu'une application spécifiée est lancée.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Système > Intégration d'entreprise > VMware Tunnel**.

2 La première fois que vous configurez VMware Tunnel, sélectionnez **Configuration** et suivez l'assistant de configuration. Dans le cas contraire, sélectionnez **Remplacer** et **Activer**. Ensuite, cliquez sur **Configurer**.

3 Sur la page Type de configuration, activez **Tunnel par application (Linux uniquement)**. Cliquez sur **Suivant**.

Conservez **Basique** comme modèle de déploiement.

4 Sur la page Détails, pour la configuration de tunneling par application, entrez le nom d'hôte et le port du serveur VMware Tunnel. Par exemple, entrez `tunnel.example.com`. Cliquez sur **Suivant**.

5 Sur la page SSL, configurez le certificat SSL de tunneling par application. Pour utiliser un SSL public, cochez la case **Utiliser le certificat SSL public**. Cliquez sur **Suivant**.

Le certificat racine de périphérique tunnel est généré automatiquement.

Remarque Les certificats SAN ne sont pas pris en charge. Vérifiez que votre certificat est émis pour le nom d'hôte de serveur correspondant ou qu'il s'agit d'un certificat avec caractères génériques valide pour le domaine correspondant.

6 Sur la page Authentification, sélectionnez le type d'authentification de certificat à utiliser. Cliquez sur **Suivant**.

Option	Description
Valeur par défaut	Sélectionnez Par défaut pour utiliser les certificats émis par AirWatch.
Autorité de certification d'entreprise	Un menu déroulant répertoriant l'autorité de certification et le modèle de certificat que vous avez configurés dans AirWatch s'affiche. Vous pouvez également télécharger le certificat racine de votre autorité de certification.

Si vous sélectionnez Autorité de certification d'entreprise, vérifiez que le modèle d'autorité de certification contient le nom du sujet **CN=<udid>:<string>**. Vous pouvez télécharger les certificats d'autorité de certification sur la page de configuration de VMware Tunnel.

Si la vérification de la conformité du périphérique est configurée pour Android, vérifiez que le modèle d'autorité de certification contient le nom du sujet CN={DeviceUid} ou définissez un type d'autre nom du sujet pour inclure l'UDID. Sélectionnez le type d'autre nom du sujet du nom DNS. La valeur doit être UDID={DeviceUid}.

7 Cliquez sur **Suivant**.

8 Sur la page Association de profil, associez un profil existant ou créez un profil VPN VMware Tunnel pour Android.

Si vous créez le profil à cette étape, vous devez toujours le publier. Consultez Configurer un profil Android dans AirWatch.

9 (Facultatif) Sur la page Divers, activez les journaux d'accès pour les composants Tunnel par application. Cliquez sur **Suivant**.

Vous devez activer ces journaux avant d'installer le serveur VMware Tunnel.

10 Examinez le résumé de votre configuration et cliquez sur **Enregistrer**.

Vous êtes dirigé vers la page de configuration des paramètres système.

11 Sélectionnez l'onglet **Général** et téléchargez le **dispositif virtuel Tunnel**.

Vous pouvez utiliser VMware Unified Access Gateway pour déployer le serveur Tunnel.

Suivant

Installez le serveur VMware Tunnel. Pour voir des instructions, consultez le guide VMware Tunnel sur le site Web AirWatch Resources.

Configurer le profil Tunnel par application pour Android

Une fois que vous avez configuré et installé le composant Tunnel par application de VMware Tunnel, vous pouvez configurer le profil VPN Android et ajouter une version au profil.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Périphériques > Profils > Ajouter un profil** et sélectionnez **Android** ou **Android for Work**.

2 Configurez les Paramètres généraux pour Android, si ce n'est pas déjà fait.

3 Dans la colonne de gauche, sélectionnez **VPN** et cliquez sur **Configurer**.

4 Renseignez les informations sur la connexion VPN.

Option	Description
Type de connexion	Sélectionnez **VMware Tunnel**.
Nom de la connexion	Entrer un nom pour cette connexion. Par exemple, **`Configuration AndroidSSO`**.
Serveur	L'URL du serveur VMware Tunnel est entrée automatiquement.
Règles VPN par application	Cochez la case **Règles VPN par application**.

5 Cliquez sur **Ajouter une version**.

6 Cliquez sur **Enregistrer et publier**.

Suivant

Activez le VPN par application pour les applications Android auxquelles vous pouvez accéder à l'aide de Mobile SSO pour Android. Voir Activer VPN par application pour les applications Android.

Attribuez le profil de périphérique à un groupe intelligent. Les groupes intelligents sont des groupes personnalisables qui déterminent les périphériques de plate-forme, et les utilisateurs reçoivent une application attribuée, un livre, une stratégie de conformité, un profil de périphérique ou un provisionnement. Voir Attribuer un profil de périphérique AirWatch.

Activer VPN par application pour les applications Android

Le paramètre Profil VPN par application est activé pour les applications Android auxquelles vous accédez avec Mobile SSO pour Android de VMware Identity Manager.

Prérequis

- VMware Tunnel configuré avec le composant Tunnel par application installé.
- Profil VPN Android créé.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Applications et livres > Applications > Mode Liste**.

2 Sélectionnez l'onglet Interne.

3 Sélectionnez **Ajouter une application** et ajoutez une application.

4 Cliquez sur **Enregistrer et attribuer**.

5 Sur la page Attribution, sélectionnez **Ajouter une attribution** et, dans la section Avancé du menu déroulant **Profil VPN par application**, sélectionnez le profil VPN Android que vous avez créé.

6 Cliquez sur **Enregistrer et publier**.

Activez le VPN par application pour les applications Android auxquelles vous accédez à l'aide de Mobile SSO pour Android. Pour plus d'informations sur l'ajout ou la modification d'applications, consultez le guide de gestion des applications mobiles VMware AirWatch, sur le site Web des ressources d'AirWatch.

Suivant

Créez les règles de trafic réseau. Voir Configurer des règles de trafic dans AirWatch.

Configurer des règles de trafic dans AirWatch

Configurez les règles de trafic réseau pour que le client VMware Tunnel dirige le trafic vers le proxy HTTPS pour les périphériques Android. Répertoriez les applications Android qui sont configurées avec l'option VPN par application sur les règles de trafic, puis configurez l'adresse du serveur proxy et le nom d'hôte de destination.

Configurez les règles de trafic de périphérique pour contrôler la manière dont les périphériques gèrent le trafic provenant d'applications spécifiées. Les règles de trafic de périphérique forcent l'application VMware Tunnel à envoyer le trafic via le tunnel, bloquent tout le trafic à destination des domaines spécifiés, ignorent le réseau interne pour accéder directement à Internet ou envoient le trafic vers un site proxy HTTPS.

Pour voir des informations détaillées sur la création de règles de trafic réseau, consultez le guide VMware Tunnel sur le site Web AirWatch Resources.

Prérequis

- Option VMware Tunnel configurée avec le composant Tunnel par application installé.
- Profil VPN Android créé.
- VPN par application activé pour chaque application Android ajoutée aux règles de trafic réseau.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Système > Intégration d'entreprise** > **VMware Tunnel > Règles de trafic réseau**.

2 Dans l'onglet **Règles de trafic de périphérique**, configurez les paramètres des règles de trafic de périphérique comme indiqué dans le Guide de VMware Tunnel. Configurez les paramètres suivants qui sont spécifiques à la configuration de Mobile SSO pour Android.

a Sélectionnez l'action par défaut.

Option	Description
Tunnel	Pour la configuration de VPN avec authentification unique sur Android, sélectionnez Tunnel comme action par défaut. Toutes les applications du périphérique configurées pour VPN par application envoient le trafic réseau via le tunnel.
Contournement	Pour l'authentification unique sur Android, sélectionnez **Contournement** comme action par défaut. **Important** Avec Contournement comme action par défaut, toutes les applications configurées pour VPN par application sur le périphérique contournent le tunnel et se connectent directement à Internet. Ainsi, aucun trafic n'est envoyé au serveur Tunnel lorsque le client Tunnel est utilisé uniquement pour l'authentification unique.

Pour l'authentification unique sur Android avec utilisation de VPN, sélectionnez **Contournement** comme action par défaut.

Important Avec Contournement comme action par défaut, toutes les applications configurées pour VPN par application sur le périphérique contournent le tunnel et se connectent directement à Internet. Ainsi, aucun trafic n'est envoyé au serveur Tunnel lorsque le client Tunnel est utilisé uniquement pour l'authentification unique.

b Dans la colonne Application, ajoutez les applications Android qui sont configurées avec le profil VPN par application.

c Pour les locataires hébergés dans le Cloud, dans la colonne Action, sélectionnez Proxy et spécifiez les informations du proxy HTTPS. Entrez **`certproxy.vmwareidentity.com:5262`**.

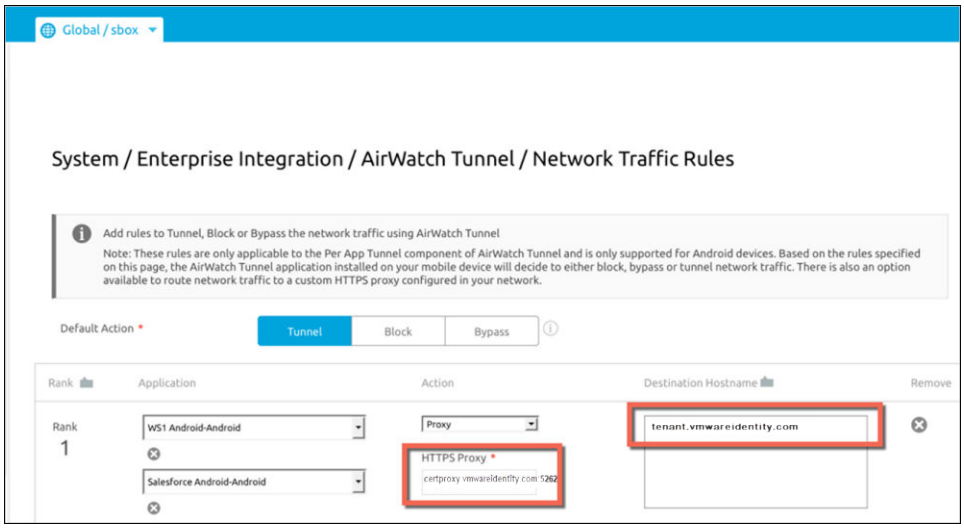
Dans la colonne Nom d'hôte de destination, entrez le nom d'hôte VMware Identity Manager de destination. Entrez **`<locataire>.vmwareidentitymanager.<région>`**. Les choix d'adresse sont : vmwareidentity.com, vmwareidentity.eu ou vmwareidentity.asia. Le client VMware Tunnel dirige le trafic vers le proxy HTTPS à partir du nom d'hôte VMware Identity Manager.

d Pour une utilisation sur site, dans la colonne Action, sélectionnez Proxy et spécifiez les informations du proxy HTTPS. Entrez le port et le nom d'hôte de VMware Identity Manager. Par exemple, **`login.example.com:5262`**.

Remarque Pour les déploiements sur site, si vous fournissez un accès externe à l'hôte VMware Identity Manager, le port de pare-feu 5262 doit être ouvert ou le trafic du port 5262 doit être traité par proxy via un proxy inverse dans la zone DMZ.

Dans la colonne Nom d'hôte de destination, entrez le nom d'hôte VMware Identity Manager de destination. Par exemple, **`myco.example.com`**. Le client VMware Tunnel dirige le trafic vers le proxy HTTPS à partir du nom d'hôte VMware Identity Manager.

3 Cliquez sur **Enregistrer**.



Suivant

Publiez ces règles. Une fois les règles publiées, le périphérique reçoit un profil VPN de mise à jour et l'application VMware Tunnel est configurée pour activer SSO.

Accédez à la console d'administration de VMware Identity Manager et configurez Mobile SSO pour Android sur la page du fournisseur d'identité intégré.

Configurer l'authentification Mobile SSO pour iOS dans le fournisseur d'identité intégré

Pour fournir l'authentification unique depuis des périphériques Android gérés par AirWatch, vous configurez l'authentification Mobile SSO pour Android dans le fournisseur d'identité intégré VMware Identity Manager.

Prérequis

- Obtenez les certificats racines et intermédiaires auprès de l'autorité de certification ayant signé les certificats présentés par vos utilisateurs.
- (Facultatif) Une liste des identificateurs d'objets (OID) des stratégies de certificat valides pour l'authentification par certificat.
- Pour le contrôle de la révocation, l'emplacement du fichier du CRL et l'URL du serveur OCSP.
- (Facultatif) L'emplacement du fichier de la signature du certificat de la réponse OCSP.

Procédure

1 Dans l'onglet Identité et gestion de l'accès de la console d'administration, sélectionnez **Gérer > Fournisseurs d'identité**.

2 Cliquez sur le fournisseur d'identité avec l'étiquette **Intégré**.

3 Vérifiez que la configuration Utilisateurs et réseau dans le fournisseur d'identité intégré est correcte.

Si ce n'est pas le cas, modifiez les sections Utilisateurs et réseau si nécessaire.

Remarque La plage réseau que vous utilisez dans la règle de stratégie pour Mobile SSO pour Android ne doit contenir que les adresses IP utilisées pour recevoir des demandes provenant du serveur proxy VMware Tunnel.

4 Dans la section Méthodes d'authentification, cliquez sur l'icône d'engrenage **Mobile SSO (pour périphériques Android)**.

5 Sur la page CertProxyAuthAdapter, configurez la méthode d'authentification.

Option	Description
Activer l'adaptateur de certificat	Cochez cette case pour activer Mobile SSO pour Android.
Certificat d'autorité de certification racine et intermédiaire	Sélectionnez les fichiers de certificat à télécharger. Il est possible de sélectionner plusieurs certificats d'autorité de certification racine et intermédiaire qui sont encodés. Le format de fichier peut être PEM ou DER.
Noms uniques de sujet du certificat d'autorité de certification téléchargés	Le contenu du fichier de certificat téléchargé s'affiche ici.
Utiliser une adresse e-mail s'il n'existe pas d'UPN dans le certificat	Si le nom principal de l'utilisateur (UPN) n'existe pas dans le certificat, cochez cette case pour utiliser l'attribut emailAddress comme extension Autre nom de l'objet afin de valider des comptes d'utilisateur.
Stratégies de certificat acceptées	Créez une liste d'identificateurs d'objet qui sont acceptés dans les extensions de stratégie de certificat. Entrez le numéro d'ID d'objet (OID) pour la stratégie d'émission de certificat. Cliquez sur **Ajouter une autre valeur** pour ajouter des OID supplémentaires.
Activer la révocation de certificat	Cochez cette case pour permettre le contrôle de la révocation des certificats. Cela empêche les utilisateurs avec des certificats d'utilisateur révoqués de s'authentifier.
Utiliser la CRL des certificats	Cochez cette case pour utiliser la liste de révocation de certificats (CRL) publiée par l'autorité de certification qui a émis les certificats afin de valider le statut d'un certificat, révoqué ou non révoqué.
Emplacement de la CRL	Entrez le chemin d'accès au fichier de serveur ou local depuis lequel la CRL peut être récupérée.
Autoriser la révocation OCSP	Cochez cette case pour utiliser le protocole de validation des certificats OCSP (Online Certificate Status Protocol) afin d'obtenir le statut de révocation d'un certificat.
Utiliser la CRL en cas de défaillance du protocole	Si vous configurez une CRL et OCSP, vous pouvez sélectionner cette zone pour basculer vers l'utilisation de la CRL si le contrôle OCSP n'est pas disponible.
Envoi de nonce OCSP	Cochez cette case si vous souhaitez que l'identificateur unique de la requête OCSP soit envoyé dans la réponse.
URL d'OCSP	Si vous avez activé la révocation OCSP, entrez l'adresse de serveur OCSP pour le contrôle de la révocation.
Certificat de signature du répondeur OCSP	Entrez le chemin d'accès au certificat OCSP du répondeur. Utilisez le format `/path/to/file.cer`

Option	Description
Activer le lien d'annulation	Lorsque l'authentification prend trop de temps, si ce lien est activé, les utilisateurs peuvent cliquer sur Annuler pour interrompre la tentative d'authentification et annuler la connexion.
Message Annuler	Créez un message personnalisé qui s'affiche lorsque l'authentification prend trop de temps. Si vous ne créez pas de message personnalisé, le message par défaut est `Attempting to authenticate your credentials`.

6 Cliquez sur **Enregistrer**.

7 Cliquez sur **Enregistrer** sur la page Fournisseur d'identité intégré.

Suivant

Configurez la règle de stratégie d'accès par défaut pour Mobile SSO pour Android.

Enrôlement direct dans AirWatch à l'aide de Workspace ONE

5

L'enrôlement direct via Workspace ONE oblige les utilisateurs à enrôler leurs terminaux pour pouvoir accéder aux ressources dans l'application Workspace ONE.

Lorsque l'enrôlement direct se fait via l'application Workspace ONE, vous pouvez obliger les utilisateurs à accéder à la boutique d'applications appropriée, à télécharger Workspace ONE, à saisir leur adresse e-mail et à suivre les invites pour commencer à utiliser Workspace ONE sur leurs terminaux.

Terminaux pris en charge

- Apple iOS 9.0 et versions ultérieures
- Android Enterprise (anciennement Android for Work) 4.1 et versions ultérieures
- Android Legacy 4.1 et versions ultérieures

  Un terminal Android Legacy est un terminal Android qui n'est pas compatible avec Android Enterprise, ou un terminal compatible avec Android Enterprise se connectant à une instance d'AirWatch sur laquelle Android Enterprise n'est pas activé.

Ce chapitre aborde les rubriques suivantes :

Activer Workspace ONE pour l'enrôlement direct

Vous activez l'enrôlement direct des terminaux via Workspace ONE à partir de la page Enrôlement > Restriction de la console d'administration AirWatch pour votre groupe organisationnel.

Lorsque Workspace ONE est activé pour l'enrôlement direct, les terminaux éligibles se connectant pour la première fois sont directement enrôlés. Les terminaux non éligibles à l'enrôlement direct n'ont le droit d'accéder qu'à la gestion des applications mobiles dans un état de Workspace ONE enregistré.

Procédure

1. Dans la console d'administration AirWatch, sélectionnez le groupe organisationnel pour activer l'enrôlement direct pour Workspace ONE.
2. Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et sélectionnez l'onglet **Restrictions**.

3 Pour les paramètres actuels, sélectionnez **Remplacer** si nécessaire.

4 Faites défiler jusqu'aux exigences de gestion requises pour Workspace ONE et sélectionnez les options de configuration.

Paramètre	Description
MDM requis pour Workspace ONE	Lorsque ce paramètre est activé, les terminaux éligibles et les utilisateurs sont invités à s'enrôler immédiatement lors de la connexion à Workspace ONE.
Groupe d'utilisateurs affecté	Le groupe d'utilisateurs par défaut est Tous les utilisateurs. Vous pouvez sélectionner un groupe d'utilisateurs spécifique à inclure dans le processus d'enrôlement direct.
iOS	Activez ce paramètre pour inclure des terminaux iOS. Les terminaux iOS ne sont pas éligibles pour l'enrôlement direct si ce paramètre est désactivé. Si ce paramètre est désactivé, les terminaux peuvent toujours s'enregistrer dans AirWatch dans un état non géré.
Android Legacy	Activez ce paramètre pour inclure des terminaux Android Legacy. Les terminaux Android Legacy ne sont pas éligibles pour l'enrôlement direct si ce paramètre est désactivé. Si ce paramètre est désactivé, les terminaux peuvent toujours s'enregistrer dans AirWatch dans un état non géré.
Android Enterprise	Activez ce paramètre pour inclure des terminaux Android Enterprise. Les terminaux Android Enterprise ne sont pas éligibles pour l'enrôlement direct si ce paramètre est désactivé. Si ce paramètre est désactivé, les terminaux peuvent toujours s'enregistrer dans AirWatch dans un état non géré.

5 Cliquez sur **Enregistrer**.

6 Continuez à configurer les onglets d'enrôlement avec les options d'enrôlement prises en charge pour Workspace ONE. Voir Options de configuration de l'enrôlement direct à Workspace ONE.

Pour plus d'informations sur la configuration de l'enrôlement direct pour Workspace ONE, consultez le guide VMware AirWatch Mobile Device Management Guide (Gestion des terminaux mobiles VMware AirWatch), chapitre Enrôlement des terminaux.

Options de configuration de l'enrôlement direct à Workspace ONE

Configurez l'enrôlement direct à l'aide de Workspace ONE dans la console d'administration AirWatch. Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs/Général/Enrôlement**. Le tableau Options d'enrôlement de terminaux Workspace ONE répertorie les éléments de menu qui peuvent être configurés.

La page Paramètres d'enrôlement permet de configurer les options liées à l'enrôlement des terminaux et des utilisateurs. La page est divisée en onglets décrits ci-dessous. Pour obtenir des informations détaillées sur la configuration de l'enrôlement des terminaux, consultez le guide VMware AirWatch Mobile Device Management (Gestion des terminaux mobiles VMware AirWatch).

Figure 5-1. Page Enrôlement de la console AirWatch

Tableau 5-1. Éléments de menu configurables pour l'enrôlement direct à Workspace ONE

Onglet Enrôlement	Éléments de menu configurables pour l'enrôlement direct à Workspace ONE
Authentification	Les utilisateurs d'annuaire sont pris en charge. En outre, les utilisateurs de SAML et d'Active Directory sont pris en charge « à la volée ». Les utilisateurs de SAML sans LDAP sont pris en charge lorsque l'enregistrement d'utilisateur existe dans AirWatch au moment de la connexion initiale. Pour Mode d'enrôlement des terminaux, seul **Enrôlement ouvert** est pris en charge. Terminaux enregistrés uniquement n'est pas pris en charge.
Conditions d'utilisation	Des conditions d'utilisation peuvent être créées afin d'obliger les utilisateurs à accepter les conditions d'utilisation pour pouvoir poursuivre le processus d'enrôlement direct.
Regroupement	Toutes les options de menu de regroupement sont compatibles avec l'enrôlement direct à Workspace ONE. L'option **Synchroniser les groupes d'utilisateurs en temps réel pour Workspace ONE** est activée par défaut. Lors de l'enrôlement d'un terminal, AirWatch effectue un appel en temps réel à Active Directory pour synchroniser les groupes d'utilisateurs. Si l'utilisateur n'existe pas dans AirWatch, la console AirWatch synchronise d'abord l'utilisateur puis les groupes d'utilisateurs en temps réel. Si cette fonctionnalité n'est pas activée, la console AirWatch ne synchronise pas les groupes d'utilisateurs. **Remarque** Cette fonctionnalité est gourmande en processeur. Si des groupes d'utilisateurs ne changent pas fréquemment, ou qu'ils existent déjà dans AirWatch, désactivez ce paramètre pour améliorer les performances et pour empêcher des problèmes de latence lors du lancement de l'application Workspace ONE. Consultez la section Placement de terminaux dans le bon groupe organisationnel dans Stratégies de déploiement de la configuration de plusieurs groupes organisationnels AirWatch.

Restrictions	■ Dans **Contrôle d'accès d'utilisateur**, vous pouvez sélectionner Limiter l'enrôlement aux utilisateurs connus et Limiter l'enrôlement aux groupes configurés.
	■ Une limite maximale du nombre de terminaux est prise en charge.
	■ **Paramètre de stratégie** est partiellement pris en charge.
	  ■ **Types de propriété autorisés**. Workspace ONE ne demande que pour Personnel et Professionnel.
	  Remarque Le type d'enrôlement Autorisation de conteneur n'est pas pris en charge.

Tableau 5-1. Éléments de menu configurables pour l'enrôlement direct à Workspace ONE (suite)

Onglet Enrôlement	Éléments de menu configurables pour l'enrôlement direct à Workspace ONE
Invite facultative	Les deux invites facultatives pouvant être activées sont **Demander le type de propriété** et **Activer la demande du numéro d'actif**. La demande du numéro d'actif ne s'affiche que lorsque le type de propriété est Professionnel.
Personnalisation	Options de menu de personnalisation prises en charge. ■ URL de la page d'accueil post-enrôlement (iOS uniquement) ■ Message de profil MDM (iOS uniquement) ■ Utiliser les applications MDM personnalisées Utiliser un modèle de message spécifique pour chaque plateforme peut être activé, mais des modèles de message de Workspace ONE spécifiques ne sont pas disponibles pour Workspace ONE 3.2.

Expérience utilisateur lors de l'enrôlement direct dans AirWatch avec Workspace ONE

Lorsque la gestion de terminaux mobiles est mise en œuvre via Workspace ONE, les utilisateurs téléchargent l'application Workspace ONE, s'authentifient avec AirWatch et enrôlent leur terminal. Une fois le terminal enrôlé, les utilisateurs peuvent utiliser Workspace ONE pour ajouter et utiliser immédiatement leurs ressources autorisées.

Le processus suivi par les utilisateurs lors de l'utilisation de Workspace ONE pour enrôler leurs terminaux est similaire pour les terminaux iOS et Android Enterprise. L'enrôlement Android Legacy est redirigé vers AirWatch Agent pour l'enrôlement. AirWatch Agent rend automatiquement le contrôle à Workspace ONE lorsque l'enrôlement est terminé. Les utilisateurs peuvent accéder à Workspace ONE dans chacune de ces variations.

Enrôlement direct via Workspace ONE sur des terminaux iOS

Obligez les utilisateurs à télécharger, installer et exécuter l'application Workspace ONE depuis l'Apple Store.

Procédure

1 Les utilisateurs ouvrent l'application, entrent l'URL de leur serveur et leur adresse e-mail et s'authentifient selon la configuration de leur environnement.

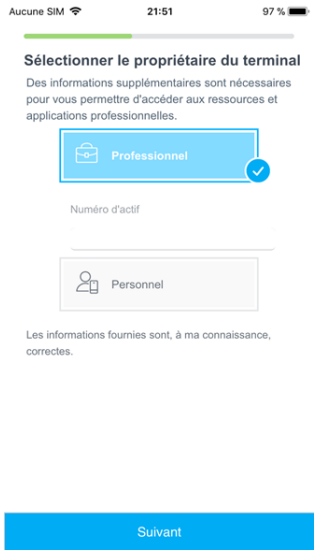
2 L'écran **Une configuration supplémentaire est requise par votre société** s'affiche.

Figure 5-2. Notification de la configuration de l'enrôlement des terminaux

3 Si des conditions d'utilisation sont configurées, les utilisateurs sont invités à accepter ces conditions d'utilisation avant de continuer.

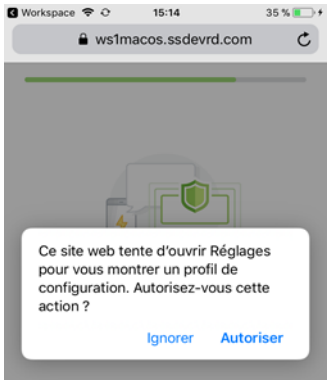
4 Si vous avez configuré des invites facultatives pour afficher le type de propriété et demander le numéro d'actif du terminal, ces informations s'affichent.

Figure 5-3. Sélection de la propriété du terminal



5 Safari est ouvert et les utilisateurs cliquent sur **Autoriser** pour ouvrir la page Paramètres.

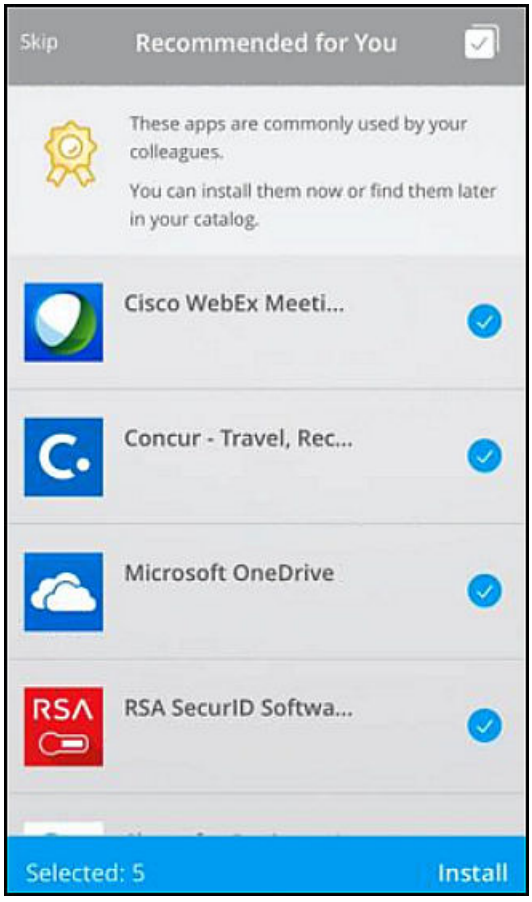
Figure 5-4. Autoriser les paramètres de profil de configuration



Les services d'espace de travail et le profil de configuration sont configurés sur le terminal.

Le terminal est maintenant enrôlé dans AirWatch et Workspace ONE est lancé. L'écran Recommandé pour vous s'affiche.

Figure 5-5. Écran Applications recommandées



6 Les utilisateurs peuvent sélectionner les applications qu'ils veulent installer ou bien ils peuvent ignorer cette étape pour l'instant.

Le terminal est maintenant géré par AirWatch MDM. Si des applications recommandées ont été sélectionnées pour être installées, les utilisateurs commencent à recevoir des notifications push pour ces applications.

Enrôlement direct à l'aide de Workspace ONE sur des terminaux Android Enterprise

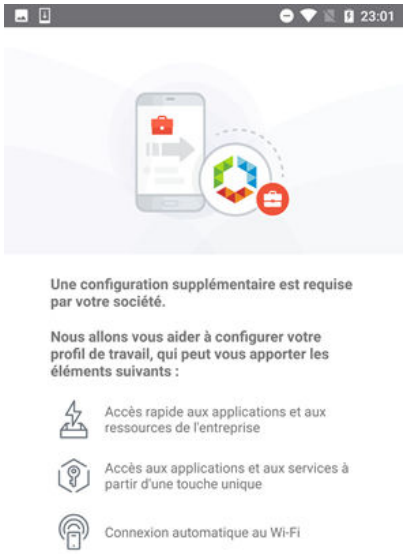
Obligez les utilisateurs à télécharger, installer et exécuter l'application Workspace ONE depuis le Google App Store ou le référentiel.

Procédure

1 Les utilisateurs entrent l'URL de leur serveur et leur adresse e-mail et s'authentifient selon la configuration de leur environnement.

2 L'écran **Une configuration supplémentaire est requise par votre société** s'affiche. L'utilisateur clique sur **Continuer**.

Figure 5-6. Notification de la configuration de l'enrôlement des terminaux

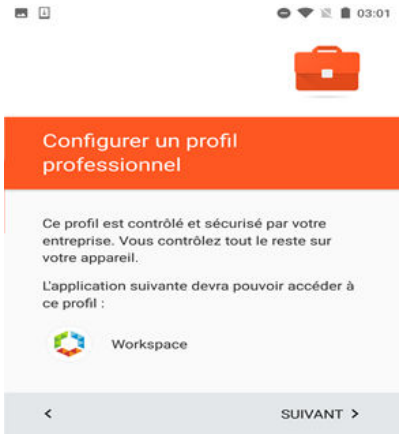


3 Si des conditions d'utilisation sont configurées, les utilisateurs sont invités à accepter ces conditions d'utilisation avant de continuer.

4 Si vous avez configuré des invites facultatives pour afficher le type de propriété et demander le numéro d'actif du terminal, ces informations s'affichent.

5 Les services d'espace de travail et le profil professionnel sont configurés sur le terminal.

Figure 5-7. Configurer la notification du profil professionnel

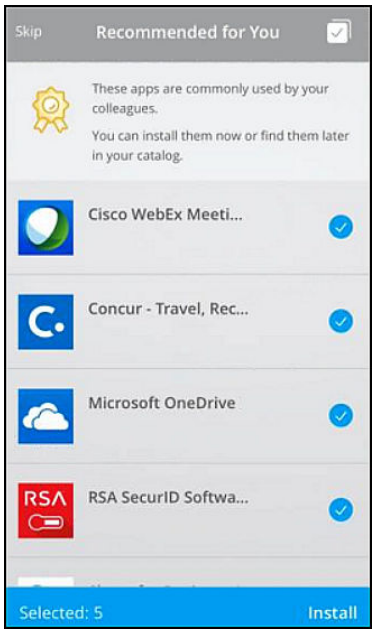


Les utilisateurs voient un message décrivant le contrôle de gestion du terminal avec ce profil professionnel et cliquent sur **OK**.

L'application Workspace ONE est installée et le compte professionnel Android est enregistré.

6 Le terminal est maintenant enrôlé dans AirWatch et Workspace ONE est lancé. L'écran Recommandé pour vous s'affiche.

Figure 5-8. Écran Applications recommandées



7 Les utilisateurs peuvent sélectionner les applications qu'ils veulent installer ou ignorer cette étape pour l'instant.

Le terminal est maintenant géré par AirWatch MDM. Si des applications recommandées ont été sélectionnées pour être installées, leur installation commencent avec une icône représentant un porte-documents Android Enterprise.

Enrôlement de terminaux Android Legacy

L'enrôlement de terminaux Android Legacy redirige vers AirWatch Agent pour l'enrôlement. AirWatch Agent rend automatiquement le contrôle à Workspace ONE lorsque l'enrôlement est terminé.

Demandez aux utilisateurs d'accéder à la boutique d'applications pour télécharger Workspace ONE.

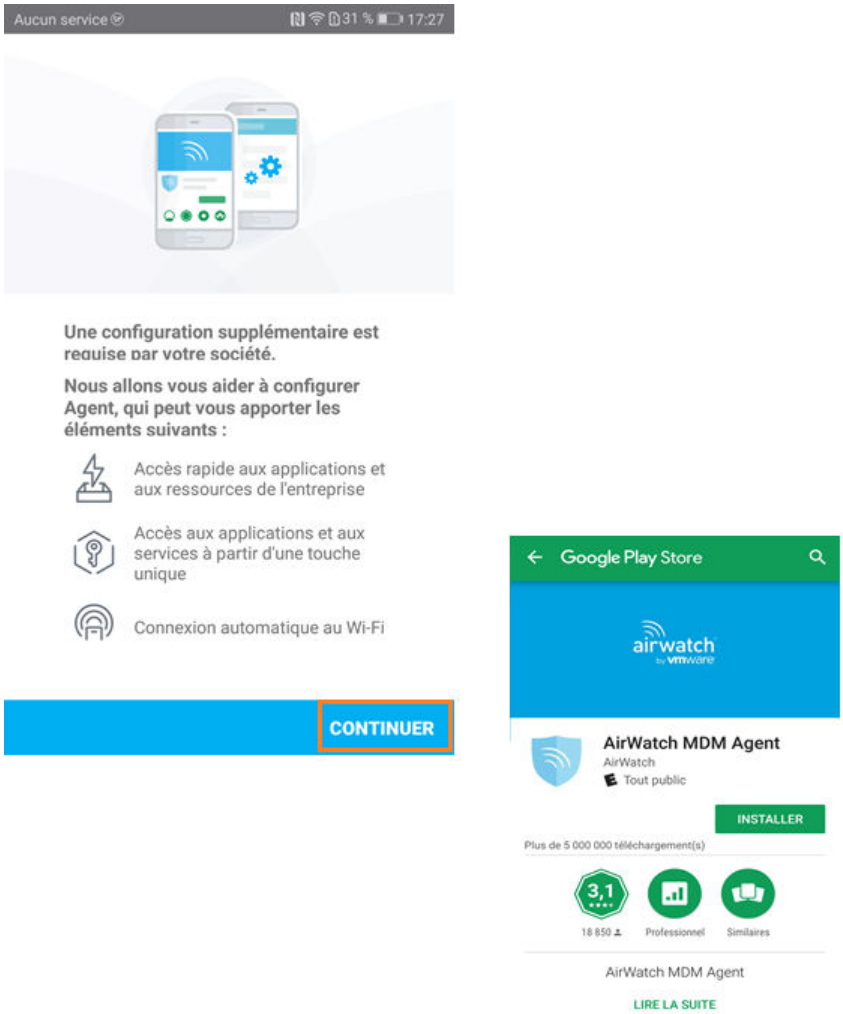
Procédure

1 Les utilisateurs ouvrent l'application, entrent l'URL de leur serveur ou leur adresse e-mail, puis saisissent leur nom d'utilisateur et leur mot de passe pour se connecter.

   À ce stade, l'application Workspace ONE peut détecter que le terminal n'est pas activé pour Android Enterprise et si le terminal requiert un enrôlement direct avant que les ressources sur Workspace ONE soient accessibles.

2 L'écran **Une configuration supplémentaire est requise par votre société** s'affiche et, lorsque les utilisateurs cliquent sur **Continuer**, ils sont redirigés vers l'application AirWatch Agent dans le Google Play Store.

Figure 5-9. Demande de téléchargement de l'application AirWatch Agent



3 Les utilisateurs téléchargent l'application AirWatch Agent.

Remarque Si l'application AirWatch Agent est déjà installée sur le terminal, Workspace ONE lance automatiquement l'application. Les utilisateurs ne sont pas redirigés vers l'App Store.

Les détails d'authentification qui ont été entrés pour Workspace ONE sont transmis à l'application AirWatch Agent afin que les utilisateurs n'aient pas à entrer de nouveau ces informations.

L'application AirWatch Agent est lancée. Pendant l'enrôlement du terminal avec AirWatch Agent, les utilisateurs sélectionnent le type de propriété et entrent le numéro d'actif, si configuré.

4 Lorsque **Autoriser Agent à passer et à gérer des appels téléphoniques** s'affiche, les utilisateurs cliquent sur **Autoriser**.

AirWatch Agent valide l'enrôlement, authentifie l'utilisateur et accorde des autorisations à AirWatch sur ce terminal.

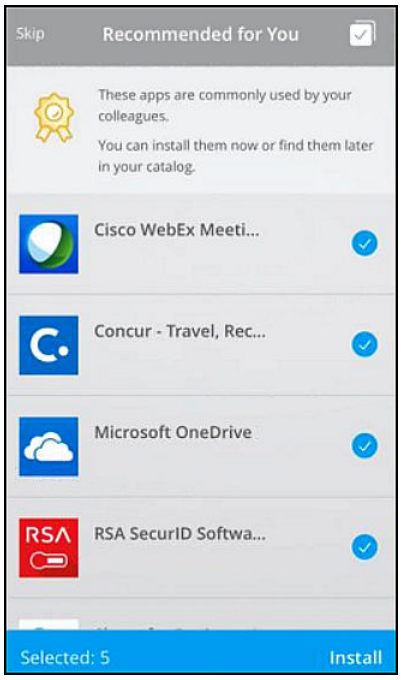
5 Lorsque l'écran **Activer l'application d'administration de terminal ?** s'affiche, les utilisateurs cliquent sur **Activer cette application d'administration de terminal**.

Figure 5-10. Activer l'application d'administration de terminal

6 Les utilisateurs sont invités à accorder une autorisation pour accéder aux diverses fonctionnalités du terminal.

Le terminal est maintenant enrôlé dans AirWatch et Workspace ONE est lancé. L'écran Applications recommandées s'affiche.

Figure 5-11. Écran Applications recommandées



7 Les utilisateurs peuvent sélectionner les applications qu'ils veulent installer ou ils peuvent ignorer cette étape pour l'instant.

Le terminal est maintenant géré par AirWatch MDM. Si des applications recommandées ont été sélectionnées pour être installées, les utilisateurs commencent à recevoir des notifications pour ces applications.

Exploitation de Workspace ONE pour prendre en charge l'intégration du Programme d'inscription des appareils Apple

6

Le Programme d'inscription des appareils (DEP) Apple ne prend pas en charge les scénarios dans lesquels un client utilise SAML pour l'authentification utilisateur. En revanche, Workspace ONE a implémenté une manière unique pour prendre en charge ce cas d'utilisation.

À travers le préenrôlement des terminaux AirWatch, les administrateurs peuvent attribuer le terminal à un utilisateur de préenrôlement de plusieurs terminaux et autoriser Workspace ONE à réattribuer le terminal à l'utilisateur approprié lorsqu'il se connecte à l'application Workspace ONE.

L'application Workspace ONE doit être installée sur le terminal dans le cadre de l'enrôlement d'utilisateur de préenrôlement. Lorsqu'un utilisateur se connecte à Workspace ONE pour la première fois, Workspace ONE l'authentifie via le fournisseur SAML configuré. Une fois que l'utilisateur est authentifié, la propriété du terminal passe de l'utilisateur de préenrôlement de plusieurs terminaux à l'utilisateur d'annuaire authentifié.

Conditions préalables

L'utilisateur d'annuaire doit exister dans AirWatch lorsqu'il se connecte à l'application Workspace ONE. Vous pouvez précharger des utilisateurs dans une charge en bloc via CSV ou appliquer l'API suivante pour générer des utilisateurs au besoin.

Remarque La valeur Type de sécurité doit être égale à l'annuaire.

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

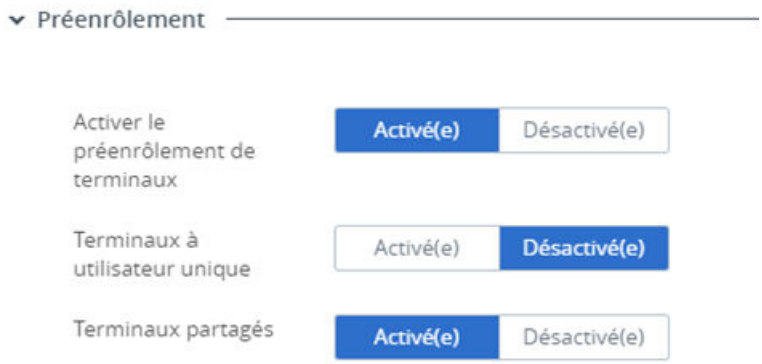
Flux pour la prise en charge de Workspace ONE de l'intégration du DEP

Les tâches suivantes doivent être effectuées pour implémenter la prise en charge du Programme d'inscription des appareils Apple à l'aide de Workspace ONE :

- Installez l'application Workspace ONE sur les terminaux iOS.
- Vérifiez l'existence d'un utilisateur de préenrôlement avec la configuration de préenrôlement suivante.
  a Accédez à **Comptes > Utilisateurs > Affichage en liste** et sélectionnez le compte d'utilisateur pour lequel vous voulez activer le préenrôlement des terminaux à modifier.

b Sur la page **Ajouter/Modifier l'utilisateur**, sélectionnez l'onglet **Avancé**. Faites défiler vers le bas jusqu'à la section **Préenrôlement** et activez **Préenrôlement d'un terminal** et **Terminaux partagés**.

Figure 6-1. Terminaux partagés définis dans AirWatch



- Attribuez le terminal à l'utilisateur de préenrôlement dans le portail du DEP Apple et fournissez le terminal à l'utilisateur final.

  Pour plus d'informations sur le Programme d'inscription des appareils Apple, consultez le Guide VMware AirWatch pour le Programme d'inscription des appareils Apple.

Fonctionnement de l'intégration

La première fois que l'utilisateur active le terminal, ce dernier est enrôlé et attribué à l'utilisateur de préenrôlement de plusieurs terminaux. L'utilisateur lance l'application Workspace ONE disponible sur l'écran d'accueil et se connecte. Workspace ONE authentifie l'utilisateur via le fournisseur SAML configuré.

Une fois que l'utilisateur est authentifié, la propriété du terminal passe de l'utilisateur de préenrôlement de plusieurs terminaux à l'utilisateur d'annuaire authentifié. Les applications, les profils et les ressources attribués à l'utilisateur authentifié sont envoyés au terminal.

Activation d'Out-of-Box Experience pour Workspace ONE sur des périphériques Dell Windows 10

7

Lorsque des utilisateurs reçoivent un nouveau périphérique Dell® Windows 10 avec un provisionnement Out-of-Box Experience (OOBE) activé dans le service de provisionnement AirWatch Windows 10, l'application Workspace ONE peut être configurée pour s'ouvrir automatiquement et fournir des applications au périphérique.

Pour fournir ce OOBE avec l'application Workspace ONE, vous devez activer la méthode d'authentification par jeton d'accès externe dans le cadre de l'intégration d'AirWatch. La méthode d'authentification est activée dans le fournisseur intégré et vous créez une règle de stratégie d'accès pour utiliser la méthode d'authentification par jeton d'accès externe.

Workspace ONE OOBE exécute l'application Workspace ONE sans demander aux utilisateurs d'entrer leurs informations d'identification de connexion une seconde fois. Si cette méthode d'authentification n'est pas activée, les utilisateurs doivent se connecter à Workspace ONE en plus de se connecter au périphérique lors du processus d'enregistrement de Windows.

Remarque Les autres services qui doivent être configurés pour OOBE dans les périphériques Dell Windows 10 incluent le service de provisionnement AirWatch pour Windows 10 et la fédération à Microsoft Azure Active Directory. Consultez Service de provisionnement de Windows 10 et Présentation de l'enrôlement de poste de travail Windows dans le Guide de la plateforme de poste de travail AirWatch Windows pour le provisionnement des détails de la configuration de service.

Ce chapitre aborde les rubriques suivantes :

Activer le jeton d'accès externe dans AirWatch

Pour activer Out-of-Box Experience Workspace ONE sur les périphériques Dell Windows 10, vous devez d'abord activer la méthode d'authentification par jeton d'accès externe sur la page de configuration d'AirWatch.

Procédure

1. Dans l'onglet Identité et gestion de l'accès de la console d'administration, cliquez sur **Configuration > AirWatch**.
2. Dans la section Authentification du jeton d'accès externe des utilisateurs via AirWatch, sélectionnez **Activer**.
3. Cliquez sur **Enregistrer**.

Suivant

Activez le jeton d'accès externe comme méthode d'authentification.

Activer un jeton d'accès externe comme méthode d'authentification

Dans VMware Identity Manager, la méthode d'authentification par jeton d'accès externe est unique à l'intégration d'AirWatch. Elle est requise pour l'authentification unique et pour le déclenchement d'Out-of-Box Experience dans Workspace ONE sur les périphériques Windows 10.

Prérequis

Lorsque vous utilisez l'authentification par jeton d'accès externe AirWatch, le composant AirWatch Cloud Connector de VMware Enterprise Systems Connector doit être déployé et configuré.

- Authentification par jeton d'accès externe activée sur la page AirWatch dans l'onglet Identité et gestion de l'accès.
- Service Microsoft Azure Active Directory configuré.
- Service de provisionnement AirWatch pour périphériques Windows 10 configuré.

La configuration du jeton d'accès externe est en lecture seule et repose sur la configuration d'AirWatch dans VMware Identity Manager. L'exception est le champ de durée de vie du jeton.

Procédure

1. Pour consulter et gérer la configuration, dans l'onglet Gestion des identités et des accès, sélectionnez **Méthodes d'authentification**.
2. Dans la colonne **Configurer** de **Jeton d'accès externe Airwatch**, cliquez sur l'icône en forme de crayon.
3. Vérifiez la configuration.

Option	Description
Activer le jeton d'accès externe Airwatch	Cette case est cochée sur la page AirWatch.
URL de la console d'administration d'AirWatch	Pré-remplie avec l'URL d'AirWatch.
Clé API AirWatch	Pré-remplie avec la clé API d'administration AirWatch.

Option	Description
Certificat utilisé pour l'authentification	Pré-remplie avec le certificat d'AirWatch Cloud Connector.
Mot de passe du certificat	Pré-remplie avec le mot de passe du certificat d'AirWatch Cloud Connector.
Durée de vie du jeton d'accès externe à AirWatch en secondes	Le jeton d'accès est utilisé pour vérifier l'authentification avec VMware Identity Manager. Les jetons d'accès ont une durée de vie limitée. La durée configurée est la durée maximale pendant laquelle le jeton d'accès est valide. La durée de vie du jeton est modifiable et définie par défaut sur 600 secondes, ce qui correspond à 10 minutes. Si le jeton d'accès expire, les utilisateurs sont invités à s'authentifier de nouveau dans l'application Workspace ONE.

4 Cliquez sur **Enregistrer**.

Suivant

Associez la méthode d'authentification par jeton d'accès externe AirWatch dans le fournisseur d'identité intégré. Voir Configurer des fournisseurs d'identité intégrés

Une fois le jeton d'accès externe AirWatch associé au fournisseur d'identité intégré, créez une règle de stratégie d'accès pour utiliser cette méthode d'authentification. Voir Créer une stratégie d'accès pour le processus Out-of-Box Experience Workspace ONE.

Associer une méthode d'authentification par jeton d'accès externe au fournisseur d'identité intégré

Lorsqu'un jeton d'accès externe est configuré comme méthode d'authentification, la méthode d'authentification est disponible dans le fournisseur d'identité intégré. Vous devez associer cette méthode d'authentification à un annuaire d'utilisateur dans le fournisseur d'identité intégré.

Prérequis

Jeton d'accès externe activé sur la page de configuration d'AirWatch.

Jeton d'accès externe activé comme méthode d'authentification.

Procédure

1 Dans l'onglet Identité et gestion de l'accès, accédez à **Gérer > Fournisseurs d'identité**.

2 Cliquez sur **Intégré** dans l'affichage en liste.

Option	Description
Utilisateurs	Les annuaires configurés sont répertoriés. Sélectionnez les annuaires d'utilisateur qui utilisent la méthode d'authentification par jeton d'accès externe.
Réseau	Les plages réseau existantes configurées dans le service sont répertoriées. Sélectionnez les plages réseau des utilisateurs en fonction des adresses IP que vous souhaitez rediriger vers cette instance de fournisseur d'identité à des fins d'authentification.
Méthodes d'authentification	Les méthodes d'authentification qui sont configurées sur le service sont affichées. Cochez la case **Jeton d'accès externe AirWatch**.

3 Cliquez sur **Enregistrer**.

Suivant

Configurez la règle de stratégie d'accès par défaut pour marquer la méthode d'authentification de jeton d'accès externe comme dernière méthode de recours dans la règle. Voir Créer une stratégie d'accès pour le processus Out-of-Box Experience Workspace ONE.

Accédez à la page Paramètres du catalogue afin de créer une page d'accueil de marque personnalisée et un message pour les utilisateurs qui se connectent à Workspace ONE dans le cadre de Windows 10 Out-Of-Box Experience. Voir Informations de marque personnalisées prêtes à l'emploi Workspace ONE pour Windows 10.

Créer une stratégie d'accès pour le processus Out-of-Box Experience Workspace ONE

Pour établir Out-of-Box Experience Workspace ONE après l'activation et l'ajout du jeton d'accès externe au fournisseur d'identité intégré, vous devez ajouter la méthode d'authentification par jeton d'accès externe à l'ensemble des stratégies d'accès par défaut.

Procédure

1 Sur l'onglet Gestion des identités et des accès de la console d'administration, sélectionnez **Gérer > Stratégies**.

2 Cliquez sur **Modifier la stratégie par défaut**, puis sur **Suivant**.

3 Sélectionnez la ligne qui répertorie l'**Application Workspace ONE** dans la colonne Type de périphérique.

Si la règle Application Workspace ONE n'est pas répertoriée, cliquez sur **Ajouter une règle de stratégie**.

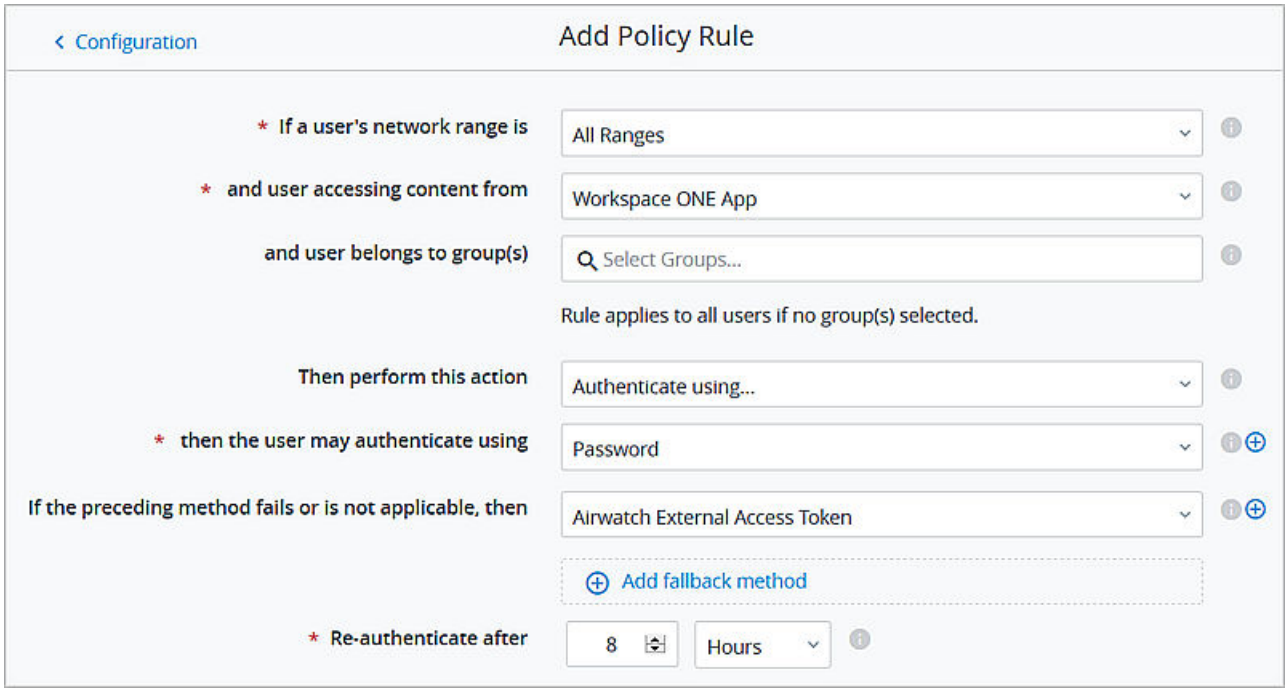
4 Sélectionnez les méthodes d'authentification à utiliser pour accéder au contenu depuis l'application Workspace ONE.

Répertoriez la méthode d'authentification par jeton d'accès externe comme dernière méthode de recours dans la règle. Lorsque le jeton d'accès externe est détecté dans la demande d'authentification, la méthode d'authentification est respectée. Les autres méthodes d'authentification répertoriées après le jeton d'accès externe ne sont pas détectées.

5 Cliquez sur **Suivant** pour examiner la configuration.

6 Cliquez sur **Enregistrer**.

Figure 7-1.



7 Sur la page Configuration, examinez l'ordre des règles dans la liste des règles. Si la règle Application Workspace ONE n'est pas la première de la liste de stratégies d'accès par défaut, faites glisser la règle pour qu'elle soit la première ligne de la liste.

   Application Workspace ONE doit être la première règle de la liste des règles de stratégie d'accès par défaut.

8 Cliquez sur **Suivant**.

9 Examinez la page Résumé et cliquez sur **Enregistrer**.

Informations de marque personnalisées prêtes à l'emploi Workspace ONE pour Windows 10

Lorsque le service de provisionnement de Windows 10 par VMware AirWatch est utilisé pour le provisionnement d'un nouveau périphérique Windows 10, des informations de marque personnalisées et un message de bienvenue peuvent être définis dans l'application Workspace ONE.

Lorsque les utilisateurs mettent sous tension leur nouvel ordinateur et qu'ils se connectent à l'aide de leurs informations d'identification pour la première fois, l'agent de provisionnement AirWatch s'assure que l'application Workspace ONE est disponible. Workspace ONE est lancé une fois que la configuration de Windows est entièrement terminée. Les utilisateurs voient un message de bienvenue personnalisé avec

les informations de marque de l'entreprise avant que le catalogue d'applications Workspace ONE s'ouvre. Pendant ce temps, si Afficher les applications recommandées dans l'onglet Signets est activé sur la page Catalogue > Paramètres > Configuration du portail de l'utilisateur, les applications recommandées sont téléchargées par Workspace ONE.

Remarque Consultez le *Guide de la plateforme de poste de travail Windows* pour plus d'informations sur le service de provisionnement de Windows 10 par AirWatch.

Procédure

1 Dans l'onglet Catalogues de la console d'administration, sélectionnez **Paramètres > Informations de marque du portail de l'utilisateur**.

2 Dans la section **Poste de travail Out-of-Box-Experience**, modifiez les paramètres pour personnaliser les pages d'enregistrement de Workspace ONE.

Élément de formulaire	Description
Logo de l'écran d'accueil	Ajoutez un logo qui sera centré en haut de l'écran d'accueil. La taille maximale de l'image est de 250 x 250 pixels. Le format est PNG.
Couleur d'arrière-plan de l'écran d'accueil	Couleur d'arrière-plan des écrans de démarrage et d'accueil. Saisissez un code couleur hexadécimal à six chiffres sur le code existant pour modifier la couleur d'arrière-plan. L'écran d'aperçu est mis à jour avec la nouvelle couleur.
Couleur du bouton Suivant de l'écran d'accueil	Saisissez un code couleur hexadécimal à six chiffres pour modifier la couleur d'arrière-plan du bouton Suivant qui s'affiche sur l'écran d'accueil.
Couleur de la police de l'écran d'accueil	Saisissez un code couleur hexadécimal à six chiffres pour modifier la couleur de police du bouton Suivant.
Message de bienvenue	Créer un message de bienvenue concernant l'utilisation de Workspace ONE qui s'affiche sur la page d'accueil.

3 Cliquez sur **Enregistrer**.

Déploiement de l'application mobile Workspace ONE de VMware

8

Lorsque l'application VMware Workspace ONE est installée sur des périphériques mobiles, les utilisateurs peuvent accéder aux ressources que vous les avez autorisés à utiliser.

Les utilisateurs peuvent accéder à leurs applications autorisées à l'aide de la fonctionnalité d'authentification unique lorsque leurs identités sont gérées avec VMware Identity Manager. Ils peuvent également accéder à un catalogue d'applications dans lequel ils peuvent ajouter d'autres applications.

L'interface de l'application Workspace ONE offre une expérience similaire et les mêmes options que n'importe quel smartphone, tablette ou ordinateur.

Si le périphérique est inscrit dans la gestion des périphériques mobiles (MDM), vous pouvez transférer l'application Workspace ONE en tant qu'application gérée.

Ce chapitre aborde les rubriques suivantes :

Options de gestion des périphériques dans AirWatch pour les applications publiques et internes de Workspace ONE

Vous pouvez choisir de déployer des applications publiques et internes en fonction de l'état de gestion des périphériques. N'importe quel périphérique peut accéder aux applications qui sont configurées avec un accès ouvert. Seuls les périphériques qui sont autorisés, en étant activés via les services Workspace ou via Inscription d'agent, peuvent accéder aux applications qui sont configurées pour un accès géré.

Le tableau décrit les capacités pour les périphériques gérés et non gérés.

Type d'accès	Fonctionnalités	Description	Utilisations suggérées
Accès ouvert (non géré)	■ Catalogue d'applications en libre-service pour ressources Web, Horizon et Citrix ■ Lancer Web/virtuel avec l'authentification unique (SSO) ■ Protection des applications par Touch ID/code PIN ■ Détection de déblocage de périphérique ■ Prise en charge de l'accès conditionnel de VMware Identity Manager, notamment des stratégies d'authentification et de blocage des périphériques. ■ Accès aux applications natives. ■ Distribution d'applications internes et d'applications SDK.	Les utilisateurs accèdent aux ressources sur leur périphérique sans accorder d'autorisation aux administrateurs pour accéder à leur périphérique. Les applications avec un accès ouvert sont disponibles pour les périphériques quel que soit leur état géré. Les administrateurs ne peuvent pas systématiquement supprimer les applications natives lorsqu'elles sont définies sur Accès ouvert.	■ Fournissez un accès aux applications aux utilisateurs finaux immédiatement lors de la connexion, sans autorisations de sécurité élevées. ■ Recommandez l'utilisation d'une application sans exiger que l'application soit installée. Les utilisateurs peuvent installer l'application sur leur périphérique lorsqu'ils le souhaitent. ■ Les applications ne contiennent pas de données d'entreprise sensibles et n'ont pas accès aux ressources d'entreprise protégées. ■ Pour distribuer des applications au personnel auxiliaire sans le profil AirWatch MDM.
Accès géré	■ Catalogue d'applications en libre-service pour ressources Web, Horizon et Citrix ■ Lancer Web/virtuel avec l'authentification unique (SSO) ■ Protection des applications par Touch ID/code PIN ■ Détection de déblocage de périphérique ■ Prise en charge de l'accès conditionnel de VMware Identity Manager, notamment des stratégies d'authentification et de blocage des périphériques. ■ Installation gérée et directe des applications natives ■ Gestion d'applications internes et d'applications SDK. ■ Prise en charge de la configuration de l'application ■ VPN par application	Les utilisateurs installent un profil de gestion sur leur périphérique pour accorder une autorisation aux administrateurs pour accéder à leur périphérique. Les applications avec un accès géré sont disponibles pour les périphériques gérés par AirWatch. Si AirWatch ne gère pas le périphérique, Workspace ONE invite l'utilisateur sur le périphérique à s'inscrire avec AirWatch. Si le périphérique est inscrit, l'utilisateur peut l'utiliser pour accéder à l'application via Workspace ONE.	■ Pour supprimer les données d'entreprise sensibles des périphériques lorsque les utilisateurs quittent l'organisation ou perdent leur périphérique. ■ Nécessite le tunneling d'application pour s'authentifier et communiquer en toute sécurité avec des ressources principales internes lorsque les applications accèdent à l'intranet. ■ Activez l'authentification unique pour les applications. ■ Suivez l'adoption des utilisateurs et l'état d'installation des applications. ■ Déployez l'application automatiquement lors de l'inscription.

Type d'accès	Fonctionnalités	Description	Utilisations suggérées
	■ SSO mono-touche pour applications natives avec SAML activé ■ Profils de périphérique ■ Moteur de conformité d'AirWatch		

Pour savoir où configurer les options d'accès géré pour les applications internes ou comment ajouter une application publique pour le déploiement via Workspace ONE, consultez le guide de gestion des applications mobiles AirWatch.

Plates-formes prises en charge pour l'accès ouvert et géré

Configurez le type d'accès pour les applications internes et publiques en fonction de la plate-forme.

	Accès géré	Accès ouvert
APPLICATIONS INTERNES		
Android	X	X
iOS	X	X
Poste de travail Windows 10	X	-
Windows 10 Phone	X	-
APPLICATIONS PUBLIQUES		
Android	X	X
iOS	X	X
Poste de travail Windows 10	-	X
Windows 10 Phone	-	X

Gestion de l'accès à des applications

Un seul utilisateur peut être autorisé à mélanger un accès ouvert ou géré à des applications natives. L'approche de gestion adaptative permet aux utilisateurs finaux d'utiliser des applications avec accès ouvert sans nécessiter de gestion. Lorsque les utilisateurs demandent une application native qui nécessite la gestion, la gestion adaptative fournit une sécurité et un contrôle supplémentaires nécessaires pour gérer cette application native.

Lorsque des applications sont gérées, les utilisateurs doivent activer les services Workspace pour installer et utiliser les applications gérées. Lorsque vous chargez une application dans la console d'administration d'AirWatch, l'état de l'accès s'affiche comme ouvert ou géré en fonction de la configuration de cette application. Par exemple, si l'option **Envoyer des configurations d'application** est sélectionnée, une application est réglée pour nécessiter la gestion.

Les applications qui doivent être gérées indiquent une icône d'étoile lorsqu'elles sont affichées dans un état non géré dans le catalogue. Les utilisateurs doivent choisir d'activer les services Workspace via le processus de gestion adaptative afin d'utiliser l'application. Lorsque les utilisateurs tentent de télécharger une application qui affiche une icône d'étoile, ils reçoivent un message leur demandant d'activer les services Workspace. Les utilisateurs peuvent cliquer sur un lien d'avis de confidentialité pour voir l'impact sur la confidentialité de leurs données personnelles s'ils choisissent de poursuivre le processus de gestion adaptative. L'avis de confidentialité extrait les paramètres de l'environnement AirWatch sur lequel ils sont sur le point de s'inscrire. Après avoir examiné les informations sur le paramètre de confidentialité, les utilisateurs peuvent poursuivre l'activation des services Workspace ou renoncer et continuer à utiliser l'application Workspace ONE non gérée sur leur périphérique. Lorsque les utilisateurs activent des services Workspace, l'icône d'étoile est supprimée de toutes les applications gérées.

Suppression de l'accès sur des périphériques gérés

Les utilisateurs peuvent désactiver l'application Workspace ONE sur leur périphérique géré via l'option Supprimer le compte. La suppression du compte exécute un effacement des données professionnelles sur le périphérique, une suppression de l'accès d'entreprise et un renvoi de l'utilisateur à l'écran de connexion. Les administrateurs peuvent effectuer un effacement des données professionnelles depuis la console d'administration d'AirWatch pour désactiver les services Workspace ONE.

L'exécution d'une action Supprimer un compte sur des périphériques gérés révoque l'accès accordé via l'application Workspace ONE et annule l'inscription du périphérique à partir d' AirWatch. Les applications qui devaient être gérées sont supprimées du périphérique et l'accès à des applications de productivité d'AirWatch, telles que Boxer, Browser et Content Locker, est révoqué.

Conditions d'utilisation pour accéder au catalogue Workspace ONE

Vous pouvez écrire les conditions d’utilisation Workspace ONE de votre organisation et vous assurer que l’utilisateur final les accepte avant d’utiliser Workspace ONE.

Les conditions d’utilisation s'affichent après que l’utilisateur ouvre une session dans Workspace ONE. Les utilisateurs doivent accepter les conditions d’utilisation avant de se rendre à leur catalogue Workspace ONE.

La fonctionnalité des conditions d'utilisation inclut les options de configuration suivantes.

- Créer des versions de conditions d’utilisation existantes.
- Modifier les conditions d'utilisation
- Créer plusieurs termes d’utilisation qui peuvent être affichées en fonction du type de périphérique.
- Créer des copies spécifiques de langues des conditions d’utilisation.

Les stratégies des conditions d'utilisation que vous configurez sont répertoriées dans l'onglet Gestion des identités et des accès. Vous pouvez modifier les stratégies des conditions d'utilisation pour corriger la stratégie existante ou créer une nouvelle version de la stratégie. L'ajout d'une nouvelle version des conditions d'utilisation remplace les conditions d'utilisation existantes. Modifier une stratégie ne traduit pas les conditions d'utilisation.

Vous pouvez afficher le nombre d'utilisateurs qui ont accepté ou refusé les conditions d'utilisation à partir des page de conditions d'utilisation. Cliquez soit sur le nombre accepté ou celui refusé afin de voir une liste d'utilisateurs et leur état.

Configurer et activer des conditions d'utilisation

Dans la page Conditions d'utilisation, vous ajoutez les conditions d'utilisation et configurez les paramètres de l'utilisation. Une fois que les conditions d'utilisation sont ajoutées, vous activez l'option Conditions d'utilisation. Lorsque les utilisateurs se connectent à Workspace ONE, ils doivent accepter les conditions d'utilisation pour accéder à leur catalogue.

Prérequis

Le texte de la stratégie des conditions d'utilisation au format HTML pour copier/coller dans la zone de texte du contenu des Conditions d'utilisation. Vous pouvez ajouter des conditions d'utilisation en Anglais, Allemand, Espagnol, Français, Italien et Néerlandais.

Procédure

1. Dans l'onglet Gestion des identités et des accès de la console d'administration, sélectionnez **Configuration > Conditions d'utilisation**.
2. Cliquez sur **Ajouter des conditions d'utilisation**.
3. Entrez un nom descriptif pour les conditions d'utilisation.
4. Sélectionnez **N'importe lequel**, si les conditions d'utilisation sont pour tous les utilisateurs. Pour utiliser des conditions de stratégies d'utilisation par type de périphérique, sélectionnez **Sélectionner des plates-formes de périphériques** et sélectionnez les types de périphérique qui affichent ces conditions de stratégie d'utilisation.
5. Par défaut, la langue des conditions d'utilisation qui s'affiche en premier correspond aux paramètres de préférence de langue du navigateur. Entrez le contenu des conditions d'utilisation pour la langue par défaut dans la zone de texte.
6. Cliquez sur **Enregistrer**.

   Pour ajouter des conditions d'utilisation dans une autre langue, cliquez sur **Ajouter une langue** et sélectionnez une autre langue. La zone de texte du contenu des conditions d'utilisation est actualisée et vous pouvez ajouter le texte dans la zone de texte.

   Vous pouvez faire glisser le nom de la langue afin d'établir l'ordre que les conditions d'utilisation ont affiché.

7 Pour commencer à utiliser les conditions d'utilisation, cliquez sur **Activer les conditions d'utilisation** sur la page qui s'affiche.

Suivant

Si vous avez sélectionné un type de périphérique spécifique pour les conditions d'utilisation, vous pouvez créer des conditions d'utilisation supplémentaires pour les autres types de périphérique.

Afficher le statut d'acceptation des conditions d'utilisation

Les stratégies des conditions d'utilisation répertoriées dans la page Gestion des identités et des accès > Conditions d'utilisation indique le nombre d'utilisateurs ayant accepté ou refusé la stratégie.

Procédure

1 Dans l'onglet Gestion des identités et des accès de la console d'administration, sélectionnez **Configuration > Conditions d'utilisation**.

2 Dans la colonne Accepté / Refusé, cliquez soit sur le nombre Accepté à gauche soit sur le nombre Refusé à droite.

Une page d'état affiche l'action effectuée, acceptée ou refusée, avec le nom d'utilisateur, ID de périphérique, version de la stratégie affichés, plate-forme utilisée et la date.

3 Cliquez sur **Annuler** pour fermer la fenêtre.

Obtention et distribution de l'application Workspace ONE

Les utilisateurs peuvent télécharger l'application VMware Workspace ONE depuis la boutique d'applications de leur périphérique ou les administrateurs peuvent configurer AirWatch pour transférer l'application Workspace ONE en tant qu'application gérée aux périphériques.

Vous déployez l'application Workspace ONE depuis la console d'administration d'AirWatch sur des groupes et des utilisateurs spécifiques dans votre organisation. Une fois les utilisateurs connectés à l'application Workspace ONE sur leurs périphériques, ils peuvent accéder à des applications Web et SaaS qui leur sont attribuées.

Les étapes suivantes consistent à faire de l'application mobile Workspace ONE une application gérée à partir de la console d'administration d'AirWatch. Vous pouvez également exécuter l'assistant Démarrage Workspace ONE pour transférer l'application.

Remarque Pour des informations détaillées sur la configuration d'applications gérées dans AirWatch, consultez le guide VMware AirWatch Mobile Application Management (MAM), disponible sur le portail de ressources à l'adresse https://resources.air-watch.com.

Prérequis

Si vous prévoyez de transférer l'application mobile Workspace ONE depuis la console d'administration d'AirWatch, préparez des groupes intelligents d'utilisateurs finaux auxquels est attribuée l'application.

Procédure

1 Dans la console d'administration d'AirWatch, accédez à **Applications et livres > Applications** > **Mode Liste > Public** et sélectionnez **Ajouter une application**.

2 Sélectionnez la plate-forme, iOS, Android ou Windows.

3 Sélectionnez **Rechercher dans la boutique d'applications** et, dans la zone de texte **Nom**, entrez `Workspace ONE` comme mot-clé pour trouver VMware Workspace ONE dans la boutique d'applications.

4 Choisissez **Suivant** et utilisez **Sélectionner** pour charger l'application Workspace ONE sur la page Résultats de la boutique d'applications.

5 Configurez les options d'attribution et de déploiement pour les utilisateurs Workspace ONE dans les paramètres d'onglet suivants.

Onglet	Description
Info	Entrez et affichez des informations sur les modèles, les classements et les catégories des périphériques pris en charge.
Attribution	Attribuez l'application mobile Workspace ONE à des groupes intelligents d'utilisateurs finaux qui peuvent utiliser l'application sur leur périphérique.
Déploiement	Configurez les fonctionnalités de disponibilité et de gestion avancée de la mobilité d'entreprise, si applicable. Pour configurer automatiquement des applications gérées, activez **Envoyer la configuration d'application** et entrez les paires valeur/clé Configuration d'application pour entreprise (ACE). Voir Configuration de l'application AirWatch pour des paires clé/valeur d'entreprise.
Conditions d'utilisation	(Facultatif) Activez **Conditions d'utilisation** pour l'utilisation de l'application Workspace ONE.

6 Sélectionnez **Enregistrer et publier** pour mettre l'application à disposition des utilisateurs.

Exécutez ces étapes pour chaque plate-forme prise en charge.

Configuration de l'application AirWatch pour des paires clé/valeur d'entreprise

Lorsque vous déployez l'application Workspace ONE en tant qu'application gérée dans AirWatch et que vous activez Envoyer des configurations d'application quand vous transférez l'application Workspace ONE depuis la console AirWatch, vous pouvez préconfigurer des paramètres de Workspace ONE qui s'appliquent lorsque des utilisateurs installent et démarrent l'application Workspace ONE.

Lorsque l'application Workspace ONE est chargée dans la console d'administration AirWatch en tant qu'application mobile gérée, vous pouvez configurer l'URL du serveur VMware Workspace ONE, la valeur UID du terminal et les conditions requises pour l'authentification de certificat dans les terminaux Android.

Tableau 8-1. Options de configuration de périphérique gérées par Workspace ONE dans la console d'administration d'AirWatch

Plate-forme	Clé de configuration	Type de valeur	Valeur de configuration	Explication
Tous	`AppServiceHost`	String	**<URL du serveur VMware Workspace ONE>**	Configure l'URL de serveur de VMware Workspace ONE sur les périphériques.
iOS	`deviceUDID`	String	**{DeviceUid}** Entrez la valeur UID du périphérique. N'utilisez pas la fonction Insérer une valeur de recherche.	Suit les périphériques utilisés pour s'authentifier sur l'environnement VMware Identity Manager.
iOS	`SkipDiscoveryScreen`	Booléen	**true**	À partir de la version 3.1 de l'application Workspace ONE, la clé de configuration SkipDiscoveryScreen peut être configurée. Lorsque cette valeur est définie sur True, Workspace ONE tente de passer l'écran d'adresse e-mail/URL de serveur. Lorsqu'elle est utilisée avec la clé de configuration `AppServiceHost`, les utilisateurs passent immédiatement à l'écran d'authentification. Si Mobile SSO est également utilisé, les administrateurs peuvent proposer aux utilisateurs finaux une expérience transparente par laquelle ils démarrent Workspace ONE et commencent immédiatement le chargement de leur application Workspace ONE.

Enregistrement de domaines de messagerie pour la découverte automatique

Vous pouvez enregistrer votre domaine de messagerie dans le service de découverte automatique dans VMware Identity Manager afin de faciliter l'accès des utilisateurs finaux à leur portail d'applications via l'application Workspace ONE. Les utilisateurs finaux entrent leur adresse e-mail au lieu de l'URL de l'organisation.

Lorsque le domaine de messagerie de l'organisation est enregistrée pour la découverte automatique, les utilisateurs finaux n'entrent que leur adresse e-mail sur la page de connexion pour accéder à leur portail d'applications. Par exemple, ils entrent **`username@myco.com`**.

Lorsque la découverte automatique n'est pas utilisée, la première fois que les utilisateurs finaux ouvrent l'application Workspace One, ils doivent fournir l'URL complète de l'organisation. Par exemple, ils entrent **`myco.vmwareidentity.com`**.

Configurer la découverte automatique dans VMware Identity Manager

Pour enregistrer un domaine, vous entrez votre domaine de messagerie et votre adresse e-mail sur la page Découverte automatique de la console d'administration de VMware Identity Manager.

Un message électronique avec un jeton d'activation est envoyé à votre adresse e-mail sur le domaine. Pour activer l'enregistrement de domaine, vous entrez le jeton sur la page Découverte automatique et vous vérifiez que le domaine que vous avez enregistré est le vôtre.

Remarque Pour configurer la découverte automatique pour des déploiements sur site de VMware Identity Manager, vous devez vous connecter à la console d'administration en tant qu'administrateur local. Entrez l'ID et le mot de passe d'AirWatch que vous avez créés sur le site Web d'AirWatch, https://secure.air-watch.com/register.

Procédure

1. Dans l'onglet Gestion des identités et des accès de la console d'administration, cliquez sur **Configuration > Découverte automatique**.
2. (Déploiements sur site uniquement). Configurez l'URL de la découverte automatique d'AirWatch.

Option	Description
URL de la découverte automatique	Entrez l'URL https://discovery.awmdm.com.
ID d'AirWatch	Entrez l'adresse e-mail que vous avez enregistrée avec AirWatch pour vous connecter à son site Web.
Mot de passe	Entrez le mot de passe associé au compte AirWatch.

3. Dans la zone de texte **Domaine de messagerie**, entrez le domaine de messagerie de votre organisation à enregistrer.

4 Dans la zone de texte **Adresse de messagerie de confirmation**, entrez une adresse e-mail sur ce domaine de messagerie pour recevoir le jeton de vérification.

5 Cliquez sur **OK**.

Cet enregistrement de domaine de messagerie a l'état En attente. Vous ne pouvez avoir qu'un seul domaine de messagerie en attente à la fois.

6 Accédez à l'e-mail et copiez le jeton d'activation qui se trouve dans le message.

7 Revenez à la page **Identité et gestion de l'accès > Découverte automatique** et collez le jeton dans la zone de texte Jeton d'activation.

8 Cliquez sur **Vérifier** pour enregistrer le domaine.

Le domaine de messagerie est enregistré et ajouté à la liste de domaines de messagerie enregistrés sur la page Découverte automatique.

Les utilisateurs finaux peuvent maintenant entrer leur adresse e-mail dans l'application Workspace ONE pour accéder à leur portail d'applications.

Suivant

Si vous possédez plusieurs domaines de messagerie, ajoutez les autres domaines à enregistrer.

Paramètre d'authentification de session

Le service VMware Identity Manager inclut une stratégie d'accès par défaut qui contrôle l'accès des utilisateurs à leurs ressources VMware Identity Manager.

La durée de la session d'authentification configurée dans les règles de stratégie détermine la période maximale dont disposent les utilisateurs depuis leur dernier événement d'authentification pour accéder à la page de leur lanceur d'applications ou pour lancer une application Web spécifique. La valeur par défaut est de huit heures. Une fois les utilisateurs authentifiés, ils disposent de huit heures pour lancer une application Web sauf s'ils initient un autre événement d'authentification qui allonge cette durée.

Vous pouvez modifier la stratégie par défaut pour modifier la durée de la session dans la console d'administration VMware Identity Manager, onglet Identité et gestion de l'accès, Gérer > Stratégies. Consultez le guide d'administration de VMware Identity Manager, Gestion des stratégies d'accès.

Activation de la vérification de la conformité pour les périphériques gérés par AirWatch

Lorsque les utilisateurs inscrivent leurs périphériques, des exemples contenant des données utilisées pour évaluer la conformité sont envoyés selon un calendrier établi. L'évaluation de ces exemples de données garantit que le périphérique répond aux règles de conformité définies par l'administrateur dans la console AirWatch. Si le périphérique n'est plus conforme, les mesures correspondantes configurées dans la console AirWatch sont prises.

Le service VMware Identity Manager inclut une option de stratégie d’accès pouvant être configurée de manière à vérifier l’état de conformité du périphérique sur le serveur AirWatch lorsque des utilisateurs se connectent à partir du périphérique. La vérification de la conformité garantit que les utilisateurs ne peuvent pas se connecter à une application ou utiliser l’authentification unique sur le portail Workspace ONE si le périphérique devient non conforme. Une fois le périphérique de nouveau conforme, il est possible de se connecter.

L'application Workspace ONE se déconnecte automatiquement et bloque l'accès aux applications si le périphérique est compromis. Si le périphérique a été inscrit via la gestion adaptative, une commande de nettoyage d'entreprise émise via la console d'AirWatch désinscrit le périphérique et supprime les applications gérées à partir du périphérique. Les applications non gérées ne sont pas supprimées.

Pour plus d'informations sur les stratégies de conformité d'AirWatch, consultez le Guide de gestion des périphériques mobiles VMware AirWatch, disponible sur le site Web des ressources d'AirWatch.

Stratégies de déploiement de la configuration de plusieurs groupes organisationnels AirWatch

AirWatch utilise des groupes organisationnels pour identifier les utilisateurs et établir des autorisations. Lorsqu'AirWatch est intégré à VMware Identity Manager, les clés REST API de l'utilisateur d'administration et d'inscription sont configurées sur le type de groupe organisationnel AirWatch appelé Client.

Lorsque les utilisateurs se connectent à Workspace ONE à partir d'un périphérique, un événement d'enregistrement de périphérique est déclenché dans VMware Identity Manager. Une demande est envoyée à AirWatch pour extraire toutes les applications auxquelles la combinaison utilisateur/périphérique est autorisée à accéder. La demande est envoyée à l'aide de REST API pour localiser l'utilisateur dans AirWatch et pour placer le périphérique dans le groupe organisationnel approprié.

Pour gérer les groupes organisationnels, deux options peuvent être configurées dans VMware Identity Manager.

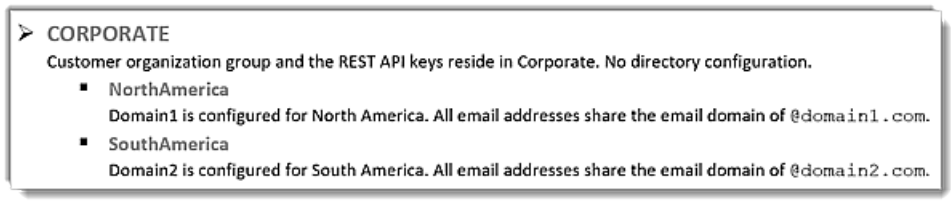
- Activez la découverte automatique d'AirWatch.
- Mappez des groupes organisationnels AirWatch à des domaines dans le service VMware Identity Manager.

Si aucune de ces deux options n'est configurée, Workspace ONE tente de localiser l'utilisateur dans le groupe organisationnel dans lequel la clé REST API est créée. Il s'agit du groupe Client.

Utilisation de la découverte automatique d′ AirWatch

Configurez la découverte automatique lorsqu'un répertoire unique est configuré dans un groupe enfant pour le groupe organisationnel Client, ou lorsque plusieurs répertoires sont configurés sous le groupe Client avec des domaines de messagerie uniques.

Figure 8-1. Exemple 1



Dans l'exemple 1, le domaine de messagerie de l'organisation est enregistré pour la découverte automatique. Les utilisateurs entrent uniquement leur adresse e-mail sur la page de connexion de Workspace ONE.

Dans cet exemple, lorsque les utilisateurs du domaine Amérique du Nord se connectent à Workspace ONE, ils entrent l'adresse e-mail complète sous la forme user1@domain1.com. L'application recherche le domaine et vérifie que l'utilisateur existe ou peut être créé avec un appel de répertoire dans le groupe organisationnel Amérique du Nord. Le périphérique peut être enregistré.

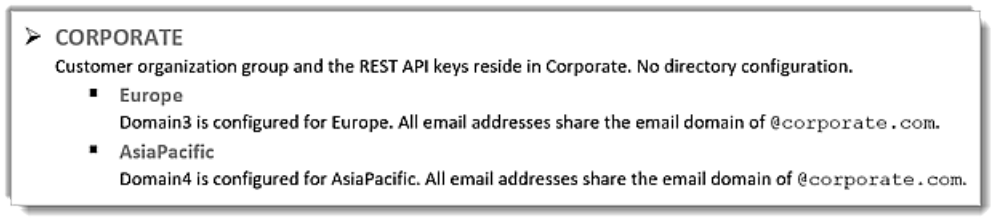
Utilisation du mappage de groupe organisationnel d' AirWatch à des domaines VMware Identity Manager

Configurez VMware Identity Manager pour le mappage de groupe organisationnel d'AirWatch lorsque plusieurs répertoires sont configurés avec le même domaine de messagerie. Vous activez **Mapper des domaines à plusieurs groupes organisationnels** sur la page de configuration d'AirWatch dans la console d’administration de VMware Identity Manager.

Lorsque l'option Mapper des domaines à plusieurs groupes organisationnels est activée, les domaines configurés dans VMware Identity Manager peuvent être mappés à des ID de groupe organisationnel d'AirWatch. La clé REST API d'administration est également requise.

Dans l'exemple 2, deux domaines sont mappés à des groupes organisationnels différents. Une clé REST API d'administration est requise. La même clé REST API d'administration est utilisée pour les deux ID de groupe organisationnel.

Figure 8-2. Exemple 2



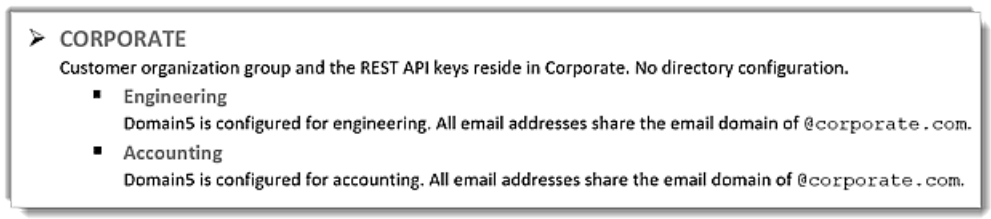
Sur la page de configuration d'AirWatch dans la console d’administration de VMware Identity Manager, configurez un ID de groupe organisationnel AirWatch spécifique pour chaque domaine.

Figure 8-3. Exemple 2 de configuration de groupe organisationnel

Avec cette configuration, lorsque les utilisateurs se connectent à Workspace ONE à partir de leur périphérique, la demande d'enregistrement de périphérique tente de localiser les utilisateurs du domaine Domain3 dans le groupe organisationnel Europe et les utilisateurs du domaine Domain4 dans le groupe organisationnel Asie Pacifique.

Dans l'exemple 3, un domaine est mappé à plusieurs groupes organisationnels AirWatch. Les deux répertoires partagent le domaine de messagerie. Le domaine pointe sur le même groupe organisationnel AirWatch.

Figure 8-4. Exemple 3



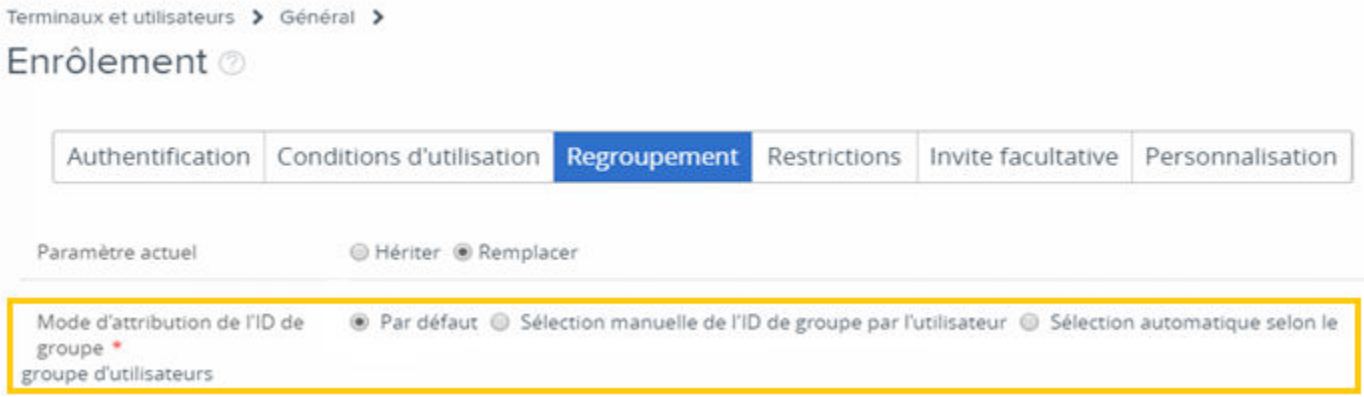
Dans cette configuration, lorsque les utilisateurs se connectent à Workspace ONE, l'application les invite à sélectionner le groupe auquel ils souhaitent s'enregistrer. Dans cet exemple, les utilisateurs peuvent sélectionner Ingénierie ou Comptabilité.

Figure 8-5. Groupes organisationnels dans lesquels les répertoires partagent le même domaine

Placement de périphériques dans le groupe organisationnel correct

Lorsqu'un enregistrement d'utilisateur est trouvé, le périphérique est ajouté au groupe organisationnel approprié. Le paramètre d'inscription d'AirWatch **Mode d'attribution d'ID de groupe** détermine le groupe organisationnel dans lequel placer le périphérique. Ce paramètre se trouve sur la page Paramètres système > Périphérique et utilisateurs > Général > Inscription > Regroupement.

Figure 8-6. Inscription de groupe AirWatch pour des périphériques



Dans l'exemple 4, tous les utilisateurs sont au niveau du groupe organisationnel Entreprise.

Figure 8-7. Exemple 4

Le placement du périphérique dépend de la configuration sélectionnée pour le mode d'attribution d'ID de groupe dans le groupe organisationnel Entreprise.

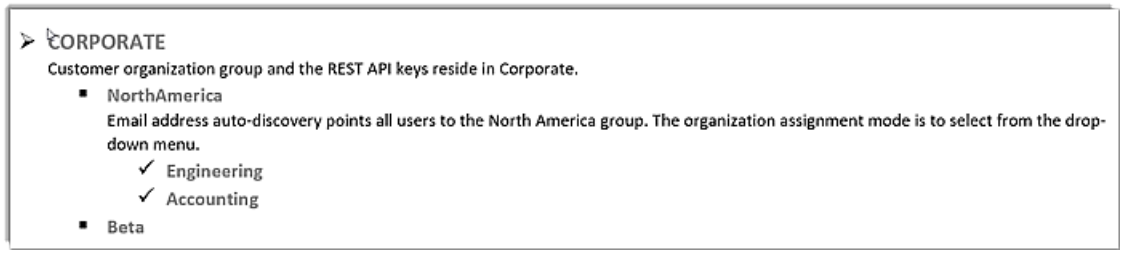
- Si la valeur par défaut est sélectionnée, le périphérique est placé dans le même groupe où se trouve l'utilisateur. Pour l'exemple 4, le périphérique est placé dans le groupe Entreprise.
- Si l'option Inviter l'utilisateur à sélectionner un ID de groupe est sélectionnée, les utilisateurs sont invités à sélectionner le groupe dans lequel enregistrer leur périphérique. Pour l'exemple 4, les utilisateurs voient un menu déroulant dans l'application Workspace ONE avec Ingénierie et Comptabilité comme options.
- Si l'option Automatiquement sélectionné en fonction du groupe d'utilisateurs est sélectionnée, les périphériques sont placés dans Ingénierie ou Comptabilité en fonction de leur attribution de groupe d'utilisateurs et du mappage correspondant dans la console d'administration d'AirWatch.

Comprendre le concept de groupe masqué

Dans l'exemple 4, lorsque les utilisateurs sont invités à sélectionner un groupe organisationnel à partir duquel enregistrer, ils peuvent également entrer une valeur d'ID de groupe qui ne se trouve pas dans la liste présentée dans l'application Workspace ONE. Il s'agit du concept de groupe masqué.

Dans l'exemple 5, dans la structure de groupe organisationnel Entreprise, Amérique du Nord et Bêta sont configurés comme groupes sous Entreprise.

Figure 8-8. Exemple 5



Dans l'exemple 5, les utilisateurs entrent leur adresse e-mail dans Workspace ONE. Après l'authentification, les utilisateurs voient une liste qui affiche Ingénierie et Comptabilité. Ils doivent choisir l'une de ces options. Bêta n'est pas une option qui s'affiche. Si les utilisateurs connaissent l'ID du groupe organisationnel, ils peuvent entrer manuellement Bêta dans la zone de texte de sélection de groupe et enregistrer correctement leur périphérique dans Bêta.

Utilisation du portail Workspace ONE

9

Lorsque l'application Workspace ONE est installée sur des périphériques, les utilisateurs peuvent se connecter à Workspace ONE pour accéder en toute sécurité à un catalogue d'applications que votre organisation a activé pour eux. Lorsque l'application est configurée avec l'authentification unique, les utilisateurs n'ont pas à entrer de nouveau leurs informations d'identification de connexion lorsqu'ils lancent l'application.

L'interface utilisateur de Workspace ONE fonctionne de la même façon sur les téléphones, les tablettes et les ordinateurs. La page Catalogue dans Workspace ONE affiche les ressources qui ont été transférées à Workspace ONE. Les utilisateurs peuvent effectuer une pression ou un clic pour rechercher, ajouter, mettre en signet et mettre à jour des applications. Ils peuvent faire un clic droit sur une application pour la supprimer de la page Mis en signet et accéder à la page Catalogue pour ajouter des ressources autorisées.

Ce chapitre aborde les rubriques suivantes :

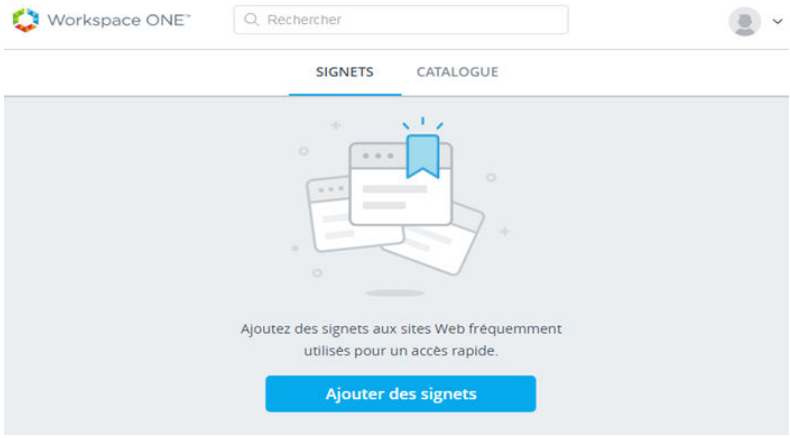
Utilisation d'applications dans Workspace ONE

Le portail utilisateur de Workspace ONE est composé d'un onglet Catalogue et d'un onglet Signets. La première fois que les utilisateurs se connectent à leur portail Workspace ONE, l'onglet Catalogue s'affiche si l'onglet Signets est vide.

Après le premier lancement, les utilisateurs sont dirigés directement vers le dernier onglet visité. Si les utilisateurs préfèrent que le lancement se fasse depuis l'onglet Catalogue, ils peuvent toujours utiliser la vue Catalogue.

Vous pouvez masquer l'onglet Catalogue ou Signets dans le portail Workspace ONE pour l'adapter à vos besoins. Vous pouvez modifier la configuration du portail sur la page Catalogue > Paramètres > Configuration du portail de l'utilisateur.

Figure 9-1. Vue initiale de la page Signets

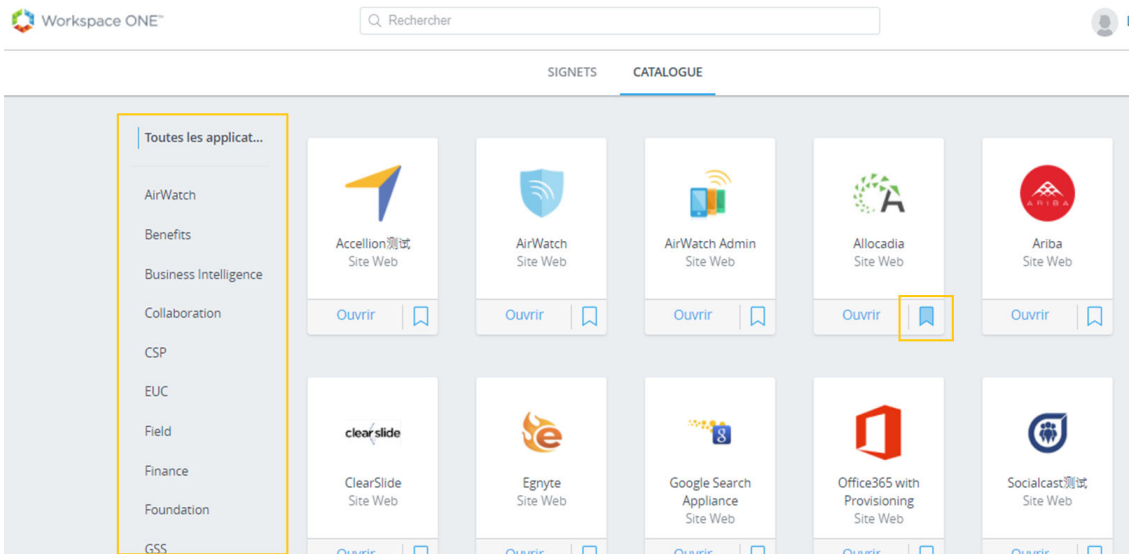


À partir du catalogue, les utilisateurs peuvent ouvrir ou installer des applications Web, mobiles et virtuelles qui leur sont attribuées. Si l'onglet Signets n'est pas masqué, les utilisateurs peuvent sélectionner l'icône de ruban afin de marquer l'application en tant que signet.

Dans les pages de catalogue, vous pouvez organiser les applications en catégories logiques, afin de faciliter la recherche des ressources dont les utilisateurs ont besoin. Par défaut, une catégorie, appelée Recommandé, est répertoriée. Lorsque vous classez des applications dans la catégorie Recommandé, vous pouvez activer l'option **Afficher les applications recommandées dans l'onglet Signets** pour préremplir la page Signets avec ces applications.

Avec cette configuration, les utilisateurs peuvent accéder immédiatement aux applications recommandées lorsqu'ils se connectent pour la première fois au portail Workspace ONE.

Figure 9-2. Page Catalogue de Workspace ONE



Remarque Les applications mobiles ne sont pas disponibles à partir des navigateurs de bureau.

Les utilisateurs peuvent lancer des applications Web comme suit.

- Depuis l'onglet Signets. Les utilisateurs cliquent sur l'icône de l'application pour la lancer.
- Depuis l'onglet Catalogue. Les utilisateurs cliquent sur la zone avec l'icône de flèche pour ouvrir l'application.
- Depuis Recherche Spotlight ou Recherche dans Workspace ONE. Depuis Recherche Spotlight sur des périphériques iOS, les utilisateurs sélectionnent l'icône de l'application dans la liste. Depuis la recherche Workspace ONE, les utilisateurs cliquent sur la zone avec l'icône de flèche pour ouvrir l'application.

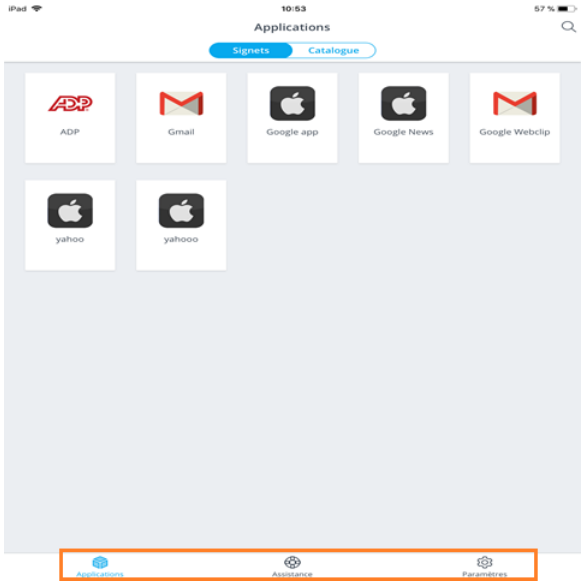
Pour lancer des applications natives installées, les utilisateurs cliquent sur l'icône de l'application dans le springboard iOS.

Les utilisateurs peuvent accéder aux paramètres de Workspace ONE à partir de la flèche déroulante en regard de leur nom.

- Compte. Informations de profil de l'utilisateur, y compris ses nom, nom d'utilisateur et adresse e-mail.
- Périphériques. Liste des périphériques qui se sont connectés à l'application Workspace ONE et dernières date et heure d'ouverture de session.
- Conseils pour l'application. Conseils sur la navigation dans Workspace ONE à partir du périphérique de l'utilisateur.
- À propos. Informations sur le copyright, les brevets et la licence de Workspace ONE.
- Préférences. Paramètres de lancement par défaut lorsque des applications distantes Horizon sont accessibles, que l'application soit affichée depuis Horizon Client ou depuis un navigateur.

Les utilisateurs appuient sur l'icône de l'application Workspace ONE sur leurs périphériques pour se connecter à leur portail d'applications. S'ils ont ajouté un signet à des applications, la page Signets s'affiche. L'application Workspace ONE sur les périphériques inclut des liens vers Support et Paramètres.

Figure 9-3. Vue des périphériques du portail Workspace ONE



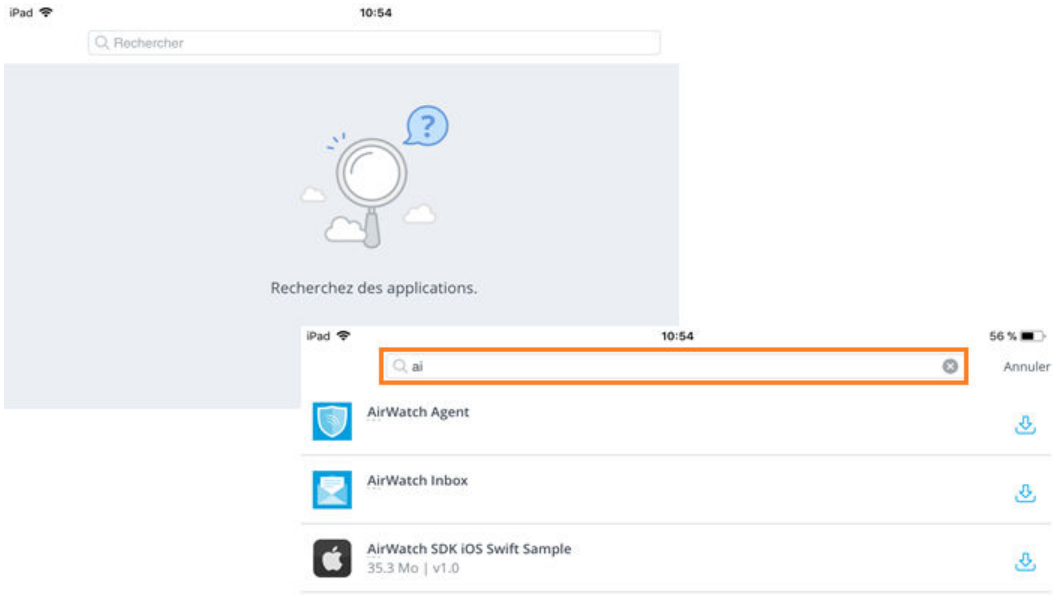
- La page Support comporte un lien vers Périphériques et vers Envoyer le rapport. La page Périphériques indique quand l'utilisateur s'est connecté pour la dernière fois au périphérique. Envoyer le rapport permet à l'utilisateur de vous envoyer des informations de diagnostic ou autres commentaires. Les utilisateurs peuvent activer ou désactiver cette fonctionnalité à partir des paramètres de leur périphérique.
- La page Paramètres affiche la version de l'application Workspace ONE et la déclaration de confidentialité de VMware Workspace. Les utilisateurs peuvent supprimer le compte à partir de la page Paramètres pour se déconnecter de l'application Workspace ONE.

Utilisation de la recherche dans Workspace ONE

Les utilisateurs peuvent utiliser la recherche dans Workspace ONE pour rechercher des applications par nom ou par catégorie.

À mesure que les utilisateurs tapent dans la zone de texte de recherche, les applications qui correspondent à l'entrée s'affichent.

Figure 9-4. Résultats de la recherche



Les utilisateurs peuvent lancer une application Web ou télécharger une application native directement depuis les résultats de la recherche

Sur les périphériques iOS, les utilisateurs peuvent utiliser Spotlight pour rechercher des applications qui se trouvent dans le portail Workspace ONE. À partir de l'écran d'accueil du périphérique iOS, les utilisateurs posent leur doigt sur l'écran et le font glisser vers le bas pour afficher le champ de recherche Spotlight. Lorsqu'ils entrent un nom d'application qui se trouve dans leur portail Workspace ONE, Workspace ONE s'ouvre et l'application est lancée.

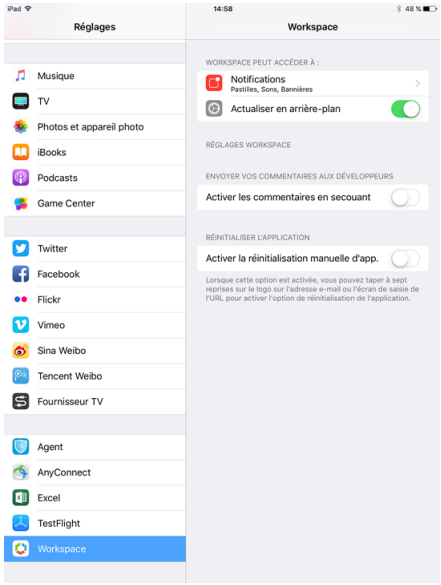
Aider les utilisateurs à signaler des problèmes depuis des périphériques iOS

Pour les périphériques iOS, la fonctionnalité Rage Shake peut être utilisée pour envoyer des journaux aux développeurs d'applications iOS.

Les utilisateurs agitent leur périphérique et le périphérique journalise son état actuel et envoie les détails dans un e-mail aux développeurs de l'application Workspace ONE par défaut. Les utilisateurs peuvent entrer manuellement une autre adresse e-mail pour envoyer les informations à une autre adresse.

Les utilisateurs peuvent activer la fonctionnalité Activer les commentaires sur secousse sur la page Paramètres > Workspace de leur périphérique. Les utilisateurs peuvent utiliser Rage Shake depuis n'importe quel écran du portail Workspace ONE pour envoyer un rapport.

Figure 9-5. Fonctionnalité Activer les commentaires sur secousse



Lorsqu'un périphérique iOS reçoit un message d'erreur semblable à `ce périphérique est enregistré avec un autre utilisateur ou environnement`, l'option Réinitialisation manuelle de l'application peut être utilisée pour effacer toutes les données d'application stockées localement sur le périphérique.

Définition de codes secrets pour l'application Workspace ONE

La fonctionnalité de code secret de verrouillage doit être activée sur les périphériques des utilisateurs. Si elle n'est pas activée, la première fois que l'application Workspace ONE est lancée, il est demandé aux utilisateurs de créer un code secret. Ce code secret est entré dès qu'un utilisateur accède à Workspace ONE depuis son périphérique.

Si la fonctionnalité de code secret n'est pas utilisée, les utilisateurs sont invités à configurer un code secret avant de pouvoir accéder à l'application Workspace ONE. Le niveau auquel est défini le code secret dépend de la plate-forme. Pour les périphériques Android, le code secret est défini au niveau de l'application. Pour les périphériques iOS et Windows, le code secret est défini au niveau du périphérique.

Remarque Les périphériques iOS et Android prennent également en charge la fonctionnalité de détection d'empreinte digitale Touch ID.

Workspace ONE peut détecter les problèmes de sécurité possibles sur les périphériques. Si des utilisateurs désactivent le code secret sur le périphérique, la prochaine fois qu'ils accèdent à l'application Workspace ONE, ils sont invités à définir un code secret avant de pouvoir accéder à Workspace ONE.

Ajout d'applications natives

Les applications natives sont des programmes d'application développés pour un périphérique mobile spécifique. Les utilisateurs peuvent voir leurs applications natives autorisées par AirWatch sur la page Catalogue de Workspace ONE. Par exemple, si un utilisateur voit le catalogue depuis un périphérique iOS, seules les applications iOS autorisées pour l'utilisateur sont affichées.

Sur la page Catalogue, les utilisateurs appuient sur Installer pour installer l'application sur leur périphérique. Après avoir appuyé sur Installer, une fenêtre contextuelle s'affiche pour indiquer aux utilisateurs les prochaines étapes. Les informations affichées dépendent du type d'application et de la plateforme. Les applications qui indiquent une icône de cadenas exigent que le périphérique soit géré par AirWatch. Lorsqu'un utilisateur final tente de télécharger une application avec une icône de cadenas, le message suivant s'affiche : `Installation of this app requires enablement of Workspace Services`.

Utilisation de VMware Verify pour l'authentification des utilisateurs

Lorsque le service VMware Verify est activé comme seconde méthode d'authentification pour l'authentification à deux facteurs pour se connecter à Workspace ONE à partir de leur périphérique, les utilisateurs doivent télécharger l'application VMware Verify depuis la boutique d'applications du périphérique.

La première fois que les utilisateurs se connectent à l'application Workspace ONE, il leur est demandé d'entrer leur nom d'utilisateur et leur mot de passe. Lorsque le nom d'utilisateur et le mot de passe sont vérifiés, les utilisateurs sont invités à entrer le numéro de téléphone de leur périphérique à inscrire dans le service VMware Verify.

Lorsqu'ils cliquent sur **Inscription**, le numéro de téléphone du périphérique est enregistré avec le service VMware Verify. S'ils n'ont pas téléchargé l'application VMware Verify, ils sont invités à le faire.

Lorsque l'application est installée, il est demandé aux utilisateurs d'entrer le même numéro de téléphone que celui entré précédemment et de sélectionner une méthode de notification pour recevoir un code d'enregistrement à usage unique. Le code d'enregistrement est entré sur la page Code PIN d'enregistrement.

Une fois le numéro de téléphone du périphérique enregistré, les utilisateurs peuvent utiliser un code secret à usage unique basé sur l’heure affiché dans l'application VMware Verify pour se connecter à Workspace ONE. Le code secret est un numéro unique généré sur le périphérique et qui change constamment.

Les utilisateurs peuvent enregistrer plusieurs périphériques. Le code secret VMware Verify est synchronisé automatiquement sur chaque périphérique enregistré.

Envoyer des alertes aux utilisateurs Workspace ONE

Les administrateurs peuvent signaler aux utilisateurs de Workspace ONE les arrêts système prévus, l'état de conformité, leur demander d'exécuter des actions ou leur envoyer des alertes. Une notification peut être envoyée via la console d'administration d'AirWatch. Elle peut être affichée sous la forme d'une notification de périphérique ou d'une notification dans l'application.

Utilisation de Workspace ONE pour les périphériques Android

Les types suivants d'applications peuvent être activés via l'application Workspace ONE Android.

- applications Web
- Applications distantes activées dans le service VMware Identity Manager. Par exemple, applications virtuelles Horizon, Citrix XenApp et ThinApp.
- Applications natives, à la fois gérées et non gérées. Les applications natives sont des applications Android développées pour la plate-forme Android. Deux types sont disponibles.
  - Applications publiques distribuées à partir de Google Play Store.
  - Applications internes distribuées en privé via AirWatch et non disponibles dans Google Play Store.

  Les applications Web s'ouvrent dans un navigateur. Les utilisateurs peuvent accéder aux applications virtuelles via VMware Horizon Client ou Citrix Receiver.

Enregistrement de Workspace ONE

Se connecter à Workspace ONE avec une URL de serveur et des informations d'identification valides permet aux utilisateurs d'accéder au catalogue unifié Workspace ONE. Dans le catalogue unifié, les utilisateurs peuvent afficher toutes les applications qui leur sont attribuées.

Les utilisateurs doivent enregistrer Workspace ONE pour accéder aux applications. Avec Workspace ONE enregistré, les utilisateurs peuvent utiliser des applications Web et virtuelles activées via VMware Identity Manager, des applications de productivité AirWatch et des applications SDK sans gestion.

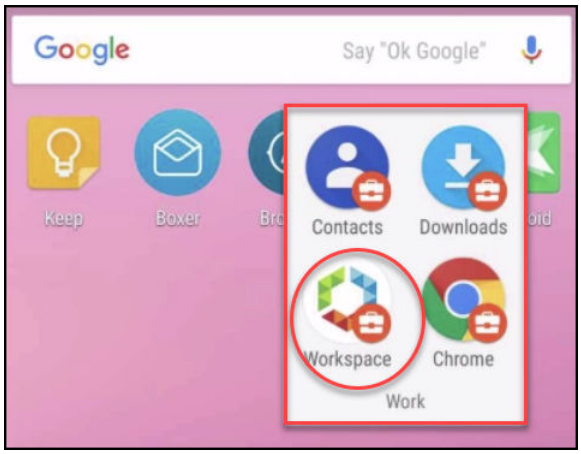
Remarque Les applications SDK sont en conteneur et gérées via le SDK AirWatch et elles ne requièrent pas que le périphérique soit géré.

Les utilisateurs peuvent lancer la gestion adaptative, ce qui active Android for Work sur le périphérique et autorise les profils, les stratégies et la distribution améliorée des applications pour le périphérique.

Gestion d'Android for Work avec Workspace ONE

L'activation d'Android for Work sur les périphériques sépare les données personnelles des données de travail au niveau du système d'exploitation. Android for Work crée une séparation nette entre les applications de travail et les applications personnelles. Android for Work crée les applications de travail avec un badge de travail Android distinct.

Figure 9-6. Contenu d'Android for Work



Les administrateurs déterminent quelles applications dans le catalogue requièrent qu'un périphérique soit géré avant que l'application puisse être consultée. Dans le catalogue, un symbole d'étoile distinct apparaît en regard du bouton de téléchargement des applications qui requièrent la gestion.

Lorsque les utilisateurs tentent de télécharger une de ces applications, ils reçoivent un message leur indiquant que l'application requiert que le périphérique soit géré. Un écran décrivant les fonctionnalités et les avantages de la gestion des périphériques s'affiche.

Figure 9-7. Page d'introduction des services Workspace

Lorsque les utilisateurs acceptent d'activer la gestion Android for Work, ils sont guidés tout au long du processus de configuration de la gestion. Une fois que le périphérique est géré, le conteneur d'Android for Work est créé sur le périphérique.

Utilisation du catalogue Workspace ONE

10

Lorsqu'AirWatch et VMware Identity Manager sont intégrés, le catalogue d'applications Workspace ONE est le référentiel de toutes les ressources que vous pouvez attribuer aux utilisateurs. Les utilisateurs peuvent accéder aux applications d'entreprise que vous gérez dans le catalogue Workspace ONE en fonction des paramètres que vous établissez pour l'application.

Les applications Cloud, mobiles et Windows sont accessibles à partir du catalogue. Les applications natives qui sont développées en interne ou disponibles publiquement dans des boutiques d'applications peuvent être mises à la disposition de vos utilisateurs finaux à partir du portail Workspace ONE.

Sur les pages Catalogue Workspace ONE, vous pouvez effectuer les tâches suivantes :

- Ajouter de nouvelles ressources à votre catalogue
- Visualiser les ressources auxquelles vous pouvez actuellement attribuer des utilisateurs
- Accéder aux informations sur chaque ressource de votre catalogue

Certaines applications Web peuvent être ajoutées directement à votre catalogue depuis les pages Catalogue. D'autres types de ressources nécessitent une action de votre part en dehors de la console d'administration. Consultez le guide Configuration des ressources de VMware Identity Manager pour plus d'informations sur la configuration des ressources.

Gestion des ressources dans le catalogue

Avant de pouvoir attribuer une ressource particulière à vos utilisateurs, vous devez doter votre catalogue de cette ressource. La méthode utilisée pour doter votre catalogue d'une ressource dépend du type de cette ressource.

Les types de ressources que vous pouvez définir dans votre catalogue pour l'octroi et la distribution aux utilisateurs sont les applications Web, les applications Windows capturées sous forme de modules VMware ThinApp, les pools de poste de travail Horizon Client et les applications virtuelles Horizon, ou les applications Citrix.

Pour intégrer et activer des pools de postes de travail et d'applications Horizon Client, des ressources publiées Citrix ou des applications modularisées ThinApp, vous utilisez la fonctionnalité Collection d'applications virtuelles dans le menu déroulant de l'onglet Catalogue.

Pour obtenir plus d'informations et connaître les conditions requises, la procédure d'installation et la configuration de ces ressources, reportez-vous à la section *Configuration des ressources dans VMware Identity Manager*.

Ajout d'applications Web au catalogue de votre organisation

Vous pouvez ajouter les applications Web de votre organisation à votre catalogue et rendre ces applications accessibles à vos utilisateurs et à vos groupes.

Vous pouvez doter votre catalogue d'applications Web directement sur la page Catalogue de la console d'administration. Lorsque vous cliquez sur une application Web affichée sur la page Catalogue, les informations sur cette application s'affichent. Depuis la page qui s'affiche, vous pouvez configurer l'application Web, par exemple fournir les attributs SAML appropriés pour configurer une connexion Single Sign-On entre VMware Identity Manager et l'application Web ciblée. Lorsque l'application Web est configurée, vous pouvez alors lui attribuer des utilisateurs et des groupes.

Lorsque vous ajoutez au catalogue une entrée pour une application Web, vous créez un enregistrement d'application et configurez l'adresse de l'application Web. Le service VMware Identity Manager utilise l'enregistrement d'application en tant que modèle pour établir une connexion sécurisée à l'application Web.

Les méthodes suivantes vous permettent d'ajouter des enregistrements d'applications Web à votre catalogue dans l'onglet Catalogue.

Méthode	Description
À partir du catalogue d'applications Cloud	Les types courants d'applications Web d'entreprise sont répertoriés dans le catalogue d'applications Cloud. Ces applications fédérées sont partiellement configurées. Vous devez renseigner le reste du formulaire de l'enregistrement d'application.
Créer un nouvel enregistrement	Vous pouvez ajouter à votre catalogue des applications Web qui ne sont pas répertoriées dans le catalogue d'applications Cloud. Les applications non fédérées sont créées en tant que nouvelles applications. Les enregistrements d’application pour ces applications Web sont plus génériques que ceux des applications du catalogue d’applications Cloud. Vous entrez les informations de description et de configuration de l'application pour créer l'enregistrement de l'application.
Importer un fichier ZIP ou JAR	Vous pouvez importer une application Web ayant été précédemment configurée dans le service. Cette méthode permet de transférer un déploiement de l'environnement de test à la production. Dans une telle situation, vous pouvez exporter une application Web depuis le déploiement de l'environnement de test sous forme de fichier ZIP. Vous pouvez ensuite importer le fichier ZIP dans le déploiement de production.

Après avoir ajouté des applications Web au catalogue, vous pouvez configurer les droits, les stratégies d'accès, la gestion des licences et les informations relatives au provisionnement.

Groupement des ressources en catégories

Il est possible d'organiser les ressources en catégories logiques, afin que les utilisateurs puissent localiser facilement la ressource dont ils ont besoin dans leur portail Workspace ONE.

Lorsque vous créez des catégories, tenez compte de la structure de votre organisation, de la fonction des ressources et du type de ressource. Une ressource peut correspondre à plusieurs catégories. Par exemple, vous pouvez créer une catégorie appelée Vendeur et une autre appelée Ressources commerciales. Attribuez Vendeur à toutes les ressources commerciales dans votre catalogue. De plus, attribuez Ressources commerciales aux ressources commerciales spécifiques qui sont partagées uniquement avec les vendeurs.

Une fois que vous avez créé une catégorie, vous pouvez l'appliquer à toute ressource du catalogue. Il est possible d'appliquer plusieurs catégories à une même ressource.

Lorsque les utilisateurs se connectent à leur portail Workspace ONE, ils voient les catégories que vous avez activées pour leur affichage.

Consultez le guide d'administration de VMware Identity Manager, Gestion du catalogue.

Informations de marque personnalisées pour les services VMware Identity Manager

11

Vous pouvez personnaliser les logos, les polices et l'arrière-plan qui s'affichent dans la console d'administration, les écrans de connexion de l'utilisateur et de l'administrateur, la vue Web du portail d'applications Workspace ONE et la vue Web de l'application Workspace ONE sur les périphériques mobiles.

Vous pouvez utiliser l'outil de personnalisation pour adopter l'apparence des couleurs, des logos et du design de votre entreprise.

Ce chapitre aborde les rubriques suivantes :

Personnaliser les informations de marque dans Service VMware Identity Manager

Vous pouvez ajouter le nom de votre entreprise, un nom de produit et une icône favorite à la barre d'adresses pour la console d'administration et le portail utilisateur. Vous pouvez également personnaliser la page de connexion pour définir des couleurs d'arrière-plan qui correspondent aux couleurs et au logo de votre entreprise.

Procédure

1. Dans l'onglet Gestion des identités et des accès de la console d'administration, sélectionnez **Configuration > Personnaliser les informations de marque**.
2. Modifiez les paramètres suivants du formulaire comme nécessaire.

Champ de formulaire	Description
	Onglet des noms et logos
Nom de l'entreprise	L'option Nom de l'entreprise s'applique aux postes de travail et aux périphériques mobiles. Vous pouvez ajouter le nom de votre entreprise comme titre qui apparaît dans l'onglet du navigateur. Saisissez un nom d'entreprise sur le nom existant pour le modifier.
Nom du produit	L'option Nom de l'entreprise s'applique aux postes de travail et aux périphériques mobiles. Le nom du produit apparaît après le nom d'entreprise dans l'onglet du navigateur.

Champ de formulaire	Description
Icône Favorite	Une icône favorite est une icône associée à une URL qui s'affiche dans la barre d'adresses du navigateur. La taille maximale de l'image d'icône favorite est de 16 x 16 pixels. Le format peut être JPEG, PNG, GIF ou ICO. Cliquez sur **Télécharger** pour télécharger une nouvelle image qui remplacera l'icône favorite actuelle. Un message vous demande de confirmer la modification. La modification est immédiate.
	Onglet de l'écran de connexion
Logo	Cliquez sur **Télécharger** pour télécharger un nouveau logo afin de remplacer le logo actuel dans les écrans d'ouverture de session. Lorsque vous cliquez sur **Confirmer**, la modification s'applique immédiatement. La taille de page minimale recommandée pour le téléchargement est de 350 x 100 px. Si vous téléchargez des images supérieures à 350 x 100 px, elles sont redimensionnées à la taille 350 x 100 px. Le format peut être JPEG, PNG ou GIF.
Couleur d'arrière-plan	Couleur d'arrière-plan de l'écran de connexion. Saisissez le code couleur hexadécimal à six chiffres sur le code existant pour changer la couleur d'arrière-plan.
Couleur d'arrière-plan de la case	La couleur de l'écran de connexion peut être personnalisée. Saisissez le code couleur hexadécimal à six chiffres sur le code existant.
Couleur d'arrière-plan du bouton de connexion	La couleur du bouton de connexion peut être personnalisée. Saisissez le code couleur hexadécimal à six chiffres sur le code existant.
Couleur de texte du bouton de connexion	La couleur du texte qui s'affiche sur le bouton de connexion peut être personnalisée. Saisissez le code couleur hexadécimal à six chiffres sur le code existant.

Lorsque vous personnalisez l'écran de connexion, vous pouvez voir vos modifications dans le volet Aperçu avant de les enregistrer.

3 Cliquez sur **Enregistrer**.

Les mises à jour des informations de marque sur la console d'administration et des pages de connexion sont appliquées dans un délai de cinq minutes après que vous avez cliqué sur Enregistrer.

Suivant

Vérifiez l'effet que produisent les modifications des informations de marque dans les diverses interfaces.

Mettez à jour l'apparence du portail Workspace ONE de l'utilisateur final et des vues Mobile et Tablette. Voir Personnaliser les informations de marque pour le portail de l'utilisateur

Personnaliser les informations de marque pour le portail de l'utilisateur

Vous pouvez ajouter un logo, modifier les couleurs d'arrière-plan et ajouter des images pour personnaliser le portail Workspace ONE.

Procédure

1 Dans l'onglet Catalogues de la console d'administration, sélectionnez **Paramètres > Informations de marque du portail de l'utilisateur**.

2 Modifiez les paramètres du formulaire comme nécessaire.

Élément de formulaire	Description
Logo	Ajoutez un logo d'en-tête à la bannière dans la partie supérieure de la console d'administration et des pages Web du portail Workspace ONE. La taille maximale de l'image est de 220 x 40 pixels. Le format peut être JPEG, PNG ou GIF.
	Portail
Couleur d'arrière-plan de l'en-tête	Saisissez un code couleur hexadécimal à six chiffres sur le code existant pour changer la couleur d'arrière-plan de l'en-tête. La couleur d'arrière-plan change dans l'écran d'aperçu du portail d'applications lorsque vous entrez un nouveau code couleur.
Couleur de texte de l'en-tête	Saisissez un code couleur hexadécimal à six chiffres sur le code existant pour changer la couleur du texte qui s'affiche dans l'en-tête.
Couleur d'arrière-plan	Couleur d'arrière-plan de l'écran du portail Web. Saisissez un nouveau code couleur hexadécimal à six chiffres sur le code existant pour changer la couleur d'arrière-plan. La couleur d'arrière-plan change dans l'écran d'aperçu du portail d'applications lorsque vous entrez un nouveau code couleur. Sélectionnez **Mise en surbrillance de l'arrière-plan** pour accentuer la couleur de l'arrière-plan. Si cette option est activée, les navigateurs prenant en charge plusieurs images d'arrière-plan affichent la superposition sur les pages du lanceur et du catalogue. Sélectionnez **Modèle d'arrière-plan** pour définir le modèle de triangle préconçu dans la couleur d'arrière-plan.
Couleur d'arrière-plan de l'icône	Saisissez un code de couleur hexadécimal à six chiffres pour modifier la palette de couleurs d'arrière-plan qui encadre les icônes d'application.
Opacité de l'arrière-plan de l'icône	Pour définir une transparence, déplacez le curseur sur la barre.
Nom et couleur des icônes	Vous pouvez sélectionner la couleur de texte des noms répertoriés sous les icônes sur les pages du portail d'applications. Saisissez un code de couleur hexadécimal sur le code existant pour modifier la couleur de la police.
Effet de lettrage	Sélectionnez le type de lettrage à utiliser pour le texte dans les écrans du portail Workspace ONE.
Arrière-plan éclairé	S'il est activé, pour les navigateurs qui prennent en charge plusieurs images d'arrière-plan, la superposition d'arrière-plan s'affiche sur les pages de signet et de catalogue.
Modèle d'arrière-plan	S'il est activé, pour les navigateurs qui prennent en charge plusieurs images d'arrière-plan, les superpositions d'arrière-plan s'affichent sur les pages de signet et de catalogue.
Image (en option)	Pour ajouter une image plutôt qu'une couleur à l'arrière-plan sur l'écran du portail des applications, téléchargez une image.

3 Cliquez sur **Enregistrer**.

Les mises à jour des informations de marque personnalisées sont actualisées toutes les 24 heures pour le portail de l'utilisateur. Pour appliquer les modifications plus tôt, en tant qu'administrateur, ouvrez un nouvel onglet et entrez cette URL, en remplaçant votre nom de domaine par myco.example.com. `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

Suivant

Vérifiez l’effet que produit les modifications des informations de marque dans les diverses interfaces.

Accès à d'autres documents

12

Lorsque vous configurez Workspace ONE, vous devrez peut-être consulter la documentation de VMware Identity Manager et de VMware AirWatch.

Pour voir une liste complète de la documentation d'AirWatch 9.2, accédez à https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm.

Pour voir une documentation générale d'AirWatch, vous pouvez accéder à AirWatch Resources sur my AirWatch et rechercher d'autres versions de la documentation.

Pour voir une documentation générale de VMware Identity Manager, vous pouvez accéder à https://docs.vmware.com/fr/VMware-Identity-Manager/index.html.