Gestion des terminaux iOS

VMware Workspace ONE UEM

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

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

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

Présentation de la gestion des terminaux iOS

1

Workspace ONE UEM powered by AirWatch met à votre disposition un ensemble fiable de solutions de gestion de la mobilité pour enrôler, sécuriser, configurer et gérer les terminaux iOS dans votre déploiement.

Grâce à la Workspace ONE UEM Console, vous pouvez :

- Gérer l'intégralité du cycle de vie des terminaux appartenant à l'entreprise comme aux employés.
- Permettre aux utilisateurs d'effectuer des tâches par eux-mêmes, y compris l'enrôlement par l'intermédiaire du portail en libre-service (SSP).
- Garantir que les terminaux sont conformes et sécurisés en attribuant des profils à des groupes et des individus spécifiques de votre organisation.
- Intégrer n'importe quelle application d'entreprise existante avec le kit de développement de logiciel (SDK) de Workspace ONE UEM.
- Utiliser les outils de génération d'états et un tableau de bord personnalisable qui offre de nombreuses possibilités de recherche pour la maintenance et la gestion quotidiennes de votre parc de terminaux.

Terminaux iOS pris en charge

Workspace ONE UEM prend en charge les terminaux iPhone, iPad et iPod Touche exécutant iOS v.5.0 et ultérieures. Certaines fonctionnalités Workspace ONE UEM et iOS nécessitent des versions ultérieures du logiciel. Ces prérequis supplémentaires sont indiqués dans la documentation si nécessaire.

Ce chapitre contient les rubriques suivantes :

Prérequis des tâches d'administration iOS

Vous avez besoin des informations suivantes pour effectuer un grand nombre de tâches. Compilez ces informations avant de continuer.

- **UEM Console** – Accédez à UEM Console avec des droits d'administrateur afin de pouvoir créer des profils et des politiques, et gérer des terminaux dans l'environnement Workspace ONE UEM.
- **Identifiants** – Le nom d'utilisateur et le mot de passe permettent d'accéder à l'environnement UEM Console. Vous pouvez utiliser vos identifiants de services d'annuaire ou en définir d'autres dans UEM Console.
- **Certificat de service de notification Push d'Apple (APNs)** – Ce certificat est émis pour autoriser l'utilisation des services de messagerie Cloud d'Apple par votre organisation.

Aperçu de l'enrôlement des terminaux iOS

2

Vous devez enrôler chaque terminal du déploiement de l'organisation dans l'environnement de celle-ci avant qu'il puisse communiquer avec Workspace ONE UEM et accéder aux fonctionnalités et contenus internes à l'aide de la Gestion de terminaux mobiles (MDM). Les terminaux iOS s'enrôlent à l'aide de la fonctionnalité MDM intégrée à l'OS natif.

Conditions requises en matière d'enrôlement

Pour enrôler un terminal iOS, vous ou vos utilisateurs devez collecter des informations spécifiques. Les informations dont les utilisateurs ont besoin varient selon que vous avez associé ou non un domaine de messagerie à l'environnement dans le cadre de la détection automatique.

Associer un domaine de messagerie à votre environnement implique que les utilisateurs saisissent leur adresse e-mail et leurs identifiants (et parfois sélectionnent un ID de groupe dans la liste) pour terminer l'enrôlement. Ce choix simplifie l'enrôlement, car les utilisateurs connaissent vraisemblablement ces informations.

Si vous n'installez pas de domaine de messagerie pour l'enrôlement, les utilisateurs sont également invités à indiquer l'URL d'enrôlement et l'ID de groupe que les administrateurs doivent leur fournir.

Pour plus d'informations sur les conditions requises en matière d'enrôlement, reportez-vous à la section Conditions requises en matière d'enrôlement de terminaux iOS.

Enrôlement d'un seul terminal

Les fonctionnalités de gestion des terminaux disponibles pour les terminaux enrôlés dépendent du type d'enrôlement que vous choisissez. Workspace ONE UEM fournit une matrice comparant les fonctions prises en charge pour les enrôlements basés sur le Hub et sans agent. Utilisez cette matrice pour déterminer le type d'enrôlement qui correspond aux besoins de votre organisation.

Pour plus d'informations sur la matrice de comparaison des inscriptions basées sur le Hub et celles basés sur le navigateur, consultez la section Fonctionnalités basées sur le type d'enrôlement pour terminaux iOS.

Enrôlement basé sur le Hub

Le processus d'enrôlement basé sur le Hub établit une connexion entre les terminaux iOS et votre environnement Workspace ONE UEM via l'application Workspace ONE Intelligent Hub. L'application Workspace ONE Intelligent Hub facilite l'enrôlement des terminaux et permet la gestion et l'accès en temps réel aux informations concernant le terminal. L'enrôlement basé sur le Hub est préférable pour les déploiements pour lesquels les utilisateurs disposent d'un identifiant Apple, grâce auquel ils doivent télécharger Workspace ONE Intelligent Hub sur l'App Store.

Pour plus d'informations sur l'enrôlement basé sur le Hub, consultez la section Workspace ONE Intelligent Hub pour iOS et Enrôler un terminal iOS auprès de Workspace ONE Intelligent Hub.

Enrôlement basé sur un navigateur

Vous pouvez également enrôler des terminaux sur le Web, à l'aide du navigateur Safari intégré aux terminaux iOS. Cette approche est idéale pour les déploiements pour lesquels les utilisateurs ne disposent pas d'identifiant Apple pour télécharger Workspace ONE Intelligent Hub.

Pour plus d'informations sur l'enrôlement basé sur un navigateur, reportez-vous à la section Enrôler un terminal iOS avec le navigateur Safari.

Enrôlement des terminaux par lots

En fonction de votre type de déploiement et du modèle des terminaux, vous pouvez choisir d'enrôler des terminaux par lots. Workspace ONE UEM fournit des fonctionnalités d'inscription par lots à l'aide d'Apple Configurator 2 et du programme d'inscription des terminaux (DEP) d'Apple Business Manager.

Enrôlement par lots avec Apple Configurator 2

Workspace ONE UEM aide les entreprises à tirer profit des fonctionnalités exclusives de configuration offertes par Apple Configurator 2 comme le respect de la version d'iOS et le blocage complet des sauvegardes. Vous pouvez enrôler des terminaux par lots à l'aide d'Apple Configurator 2 sur un ordinateur macOS afin de configurer et de déployer des terminaux iOS.

Pour plus d'informations sur l'utilisation d'Apple Configurator pour l'enrôlement par lots, reportez-vous à la section Enrôlement par lots de terminaux iOS à l'aide d'Apple Configurator.

Enrôlement par lots avec le programme d'inscription des appareils d'Apple

Déployer un enrôlement par lots à l'aide du programme d'inscription des appareils (DEP) d'Apple vous permet d'installer un profil MDM non supprimable sur un terminal, ce qui empêche les utilisateurs de supprimer le profil sur leur terminal. Vous pouvez également provisionner des terminaux en mode supervisé pour accéder à des paramètres de configuration et de sécurité supplémentaires.

Pour plus d'informations sur l'inscription avec Apple Business Manager, reportez-vous à la section Inscription des terminaux à l'aide du programme d'inscription des terminaux (DEP) d'Apple Business Manager.

Ce chapitre contient les rubriques suivantes :

- Conditions requises en matière d'enrôlement de terminaux iOS
- Fonctionnalités basées sur le type d'enrôlement pour terminaux iOS
- Enrôler un terminal iOS auprès de Workspace ONE Intelligent Hub
- Enrôler un terminal iOS avec le navigateur Safari
- Enrôlement par lots de terminaux iOS à l'aide d'Apple Configurator
- Inscription des terminaux à l'aide du programme d'inscription des terminaux (DEP) d'Apple Business Manager
- Enrôlement de l'utilisateur

Conditions requises en matière d'enrôlement de terminaux iOS

Pour enrôler un terminal iOS, vous (ou vos utilisateurs finaux) avez besoin d'informations qui varient selon que vous avez associé ou non un domaine de messagerie à l'environnement dans le cadre de la détection automatique.

Si un domaine de messagerie est associé à votre environnement, les utilisateurs ont besoin des informations suivantes :

- **Adresse e-mail** – Il s'agit de l'adresse e-mail associée à votre entreprise. Exemple : JohnDoe@acme.com.
- **Code QR** – Les utilisateurs peuvent lire un code QR généré depuis UEM Console et qu'ils reçoivent par e-mail.
- **Identifiant Apple** – Cet identifiant Apple est requis pour chaque utilisateur procédant à l'enrôlement basé sur le Hub.

Si un domaine de messagerie n'est pas associé à votre environnement :

Si un domaine n'est pas associé à un environnement, les utilisateurs doivent saisir leur adresse e-mail. Puisque l'auto-détection n'est pas activée, les utilisateurs doivent fournir les informations suivantes :

- **URL d'enrôlement** – Propre à l'environnement d'enrôlement de l'entreprise, cette URL dirige l'utilisateur directement vers l'écran d'enrôlement. Par exemple, **https://<nom de l'environnement > .com/enroll**.
- **ID de groupe** – Cet ID de groupe associe le terminal d'un utilisateur à son rôle dans l'entreprise et est défini dans UEM Console pour un groupe organisationnel donné. Pointez vers le menu déroulant du groupe d'organisations pour voir l'ID du groupe actuel.
- **Identifiant Apple** – Cet identifiant Apple est requis pour chaque utilisateur procédant à l'enrôlement basé sur le Hub.

Fonctionnalités basées sur le type d'enrôlement pour terminaux iOS

La matrice suivante répertorie les fonctions prises en charge pour les enrôlements basés sur le Hub et sans agent. Utilisez cette matrice pour déterminer le type d'enrôlement qui correspond aux besoins de votre organisation.

Fonctionnalité	Basé sur le Hub	Sans Agent
Enrôlement		
Identifiant Apple obligatoire	Requis	Facultatif
Acceptation obligatoire du CLUF/des conditions d'utilisation	Oui	Oui
Intégration Active Directory/LDAP/SAML	Oui	Oui
Authentification forte	Oui	Oui
Prise en charge BYOD	Oui	Oui
Prise en charge de l'inscription intermédiaire du terminal	Oui[9]	Oui
Personnalisation d'apparence	Partielle	Oui
Gestion des profils de configuration		
Affichage et gestion des profils	Oui	Oui
Paramètres de sécurité (chiffrement des données, politique de mot de passe, etc.)	Oui	Oui
Restrictions du terminal	Oui	Oui
Gestion des certificats	Oui	Oui
Gestion des e-mails et d'Exchange ActiveSync	Oui	Oui
Données du terminal		
Informations du terminal (modèle, numéro de série, numéro IMEI, etc.)	Oui	Oui

Fonctionnalité	Basé sur le Hub	Sans Agent
Suivi GPS	Oui	Non
Numéro de téléphone	Oui	Oui
Informations de mémoire	Oui	Oui
Informations sur la batterie	Oui	Oui
UDID	Oui	Oui
Détection de la compromission des terminaux (jailbreak)	Oui	Oui†
Statut de verrouillage d'activation	Oui	Oui
Statut Localiser mon iPhone	Oui	Oui
Statut Sauvegarde iCloud	Oui	Oui
Heure de la dernière sauvegarde	Oui	Oui
Informations sur le réseau		
Informations cellulaires (MCC/MNC, informations sur la carte SIM, etc.)	Oui	Oui
Informations sur l'itinérance des télécommunications	Oui	Oui
Informations sur l'utilisation des télécommunications	Oui	Oui†
Adresse IP	Oui	Oui†
Adresse MAC Bluetooth	Oui	Oui
Adresse MAC Wi-Fi	Oui	Oui
Commandes de gestion		
Réinitialisation complète du terminal	Oui	Oui
Effacement du contenu d'entreprise	Oui	Oui
Verrouillage du terminal	Oui	Oui
Effacement du code d'accès	Oui	Oui
Envoi d'e-mails	Oui	Oui
Envoi de SMS	Oui	Oui
Envoi de notifications Push via le service APNS	Oui	Oui†
Affichage à distance	Oui	Non
Définir le nom du terminal	Oui	Oui
Effacer le code d'accès de restrictions	Oui	Oui
Gestion d'applications		
Affichage et gestion des applications	Oui	Oui
Programme d'achats en volume (VPP)	Oui	Oui
Liste d'applications	Oui	Oui
Badge numérique pour les mises à jour d'application	Oui	Oui†
Gestion de contenu		
Gestion de contenu	Oui*	Oui*

º L'utilisateur doit transférer les achats lors de la première synchronisation.

† L'application intégrée Workspace ONE UEM SDK doit être présente sur le terminal.

* L'application VMware Content Locker doit être téléchargée depuis iTunes.

Enrôler un terminal iOS auprès de Workspace ONE Intelligent Hub

Le processus d'enrôlement basé sur le Hub établit une connexion entre un terminal iOS et votre environnement Workspace ONE UEM. L'application Workspace ONE Intelligent Hub facilite l'enrôlement des terminaux et permet la gestion et l'accès en temps réel aux informations concernant le terminal.

Si vous souhaitez bénéficier pleinement des fonctionnalités de Workspace ONE Intelligent Hub tout en permettant le processus d'enrôlement Web, vous pouvez permettre aux utilisateurs de s'enrôler via Workspace ONE Intelligent Hub. Ce paramètre empêche les utilisateurs de s'enrôler s'ils n'ont pas téléchargé Workspace ONE Intelligent Hub.

Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement > Authentification**, puis sélectionnez **Exiger l'enrôlement basé sur le Hub pour les terminaux iOS**.

Pour enrôler un terminal iOS avec Workspace ONE Intelligent Hub, procédez comme suit :

Procédure

1. Accédez à **getwsone.com** depuis le navigateur Safari. Workspace ONE UEM invite automatiquement l'utilisateur final à se rendre sur l'App Store pour télécharger l'application Workspace ONE Intelligent Hub. Suivez les messages liés au téléchargement. Remarque : un identifiant Apple est nécessaire pour télécharger Workspace ONE Intelligent Hub sur l'iTunes Store.
2. Sélectionnez l'application Workspace ONE Intelligent Hub, puis choisissez l'une des méthodes d'authentification suivantes :
   a. **Adresse e-mail** – Sélectionnez la détection automatique si elle est configurée dans votre environnement. En outre, vous pourrez être invité à sélectionner un groupe dans le menu déroulant.
   b. **Détails du serveur** – Sélectionnez cette option pour effectuer l'enrôlement à l'aide de l'URL du serveur. L'URL du serveur est l'emplacement réseau de l'instance Workspace ONE UEM de votre organisation et de l'identifiant du groupe associé à votre terminal.
   c. **Code QR** – Sélectionnez cette option et utilisez le terminal pour lire le code QR reçu par e-mail ou via l'onglet Assistance.

3 Entrez les informations d'identification ; il peut s'agir d'un **Nom d'utilisateur** et d'un **Mot de passe**, ou d'un **Jeton** ou d'une combinaison des deux qui permettent d'authentifier le terminal.

   a Si vous saisissez les informations d'identification de manière incorrecte, un code Captcha s'affiche. Saisissez le code Captcha affiché pour terminer l'authentification.

4 Terminez le processus suivant conformément aux indications de l'administrateur. Sélectionnez **Suivant** après avoir rempli chaque page.

   a Sélectionnez le type de **Propriété du terminal**, le cas échéant.

   b Acceptez les **Conditions d'utilisation** de votre organisation, le cas échéant.

   c Saisissez le **Numéro d'actif**, le cas échéant.

5 Sélectionnez **Suivant** après avoir examiné les informations de collecte de confidentialité.

6 Une fois redirigé vers le webview Safari, vous êtes invité à télécharger le profil MDM. Le message suivant s'affiche :

   ce site Web tente de télécharger un fichier de configuration. Voulez-vous l'y autoriser ?

7 Appuyez sur **Autoriser**, puis à la fin du téléchargement, appuyez sur **Fermer**.

   a Pour les terminaux iOS 12.2 et les versions ultérieures, appuyez sur **Continuer** et ouvrez le Hub pour suivre les instructions d'installation du profil MDM. Ensuite, acceptez le message d'avertissement MDM en sélectionnant **Installer**.

   b Pour les terminaux dont l'iOS est antérieur à 12.2, installez le profil MDM lorsque vous y êtes invité et acceptez le message d'avertissement MDM en sélectionnant **Installer**.

8 Sélectionnez **Autoriser** pour télécharger le profil MDM.

9 Installez le profil MDM. Acceptez toutes les invites concernant l'approbation, le cas échéant.

10 Une fois le profil MDM installé, revenez au Hub.

11 Sélectionnez **Terminer** pour terminer l'enrôlement. Le message de réussite s'affiche. L'enrôlement dans Workspace ONE UEM est maintenant terminé.

   a Si vous y êtes invité, configurez un **code d'accès** ou saisissez d'autres identifiants pour les terminaux partagés. Pour configurer un code d'accès, connectez-vous au portail en libre-service et suivez les instructions.

   b Vous pouvez éventuellement sélectionner **Ouvrir** pour consulter les détails Workspace ONE Intelligent Hub.

Enrôler un terminal iOS avec le navigateur Safari

Vous pouvez enrôler des terminaux sur le Web, à l'aide du navigateur Safari intégré aux terminaux iOS. Cette approche est idéale pour les déploiements pour lesquels les utilisateurs ne disposent pas d'identifiant Apple pour télécharger Workspace ONE Intelligent Hub.

Pour enrôler un terminal iOS à l'aide d'un processus d'enrôlement basé sur le Web, procédez comme suit :

Procédure

1 Ouvrez le navigateur Safari sur le terminal iOS.

2 Naviguez vers **https://<Environment_URL>.com/enroll**.

3 Sélectionnez **ID de groupe** ou votre **Adresse e-mail** (si la détection automatique est configurée pour votre environnement) pour enrôler votre terminal iOS. Sélectionnez **Suivant**.

4 Entrez les informations d'identification ; il peut s'agir d'un **Nom d'utilisateur** et d'un **Mot de passe**, ou d'un **Jeton** ou d'une combinaison des deux qui permettent d'authentifier le terminal.

   a Si vous saisissez les informations d'identification de manière incorrecte, un code Captcha s'affiche. Saisissez le code Captcha affiché pour terminer l'authentification.

5 Terminez le processus suivant conformément aux indications de l'administrateur. Sélectionnez **Suivant** après avoir rempli chaque page.

   a Sélectionnez le type de **Propriété du terminal**, le cas échéant.

   b Saisissez le **Numéro d'actif**, le cas échéant.

   c Acceptez les **Conditions d'utilisation** de votre organisation, le cas échéant.

6 Lorsque vous y êtes invité, téléchargez le profil MDM. Le message suivant s'affiche :

   ce site Web tente de télécharger un fichier de configuration. Voulez-vous l'y autoriser ?

7 Appuyez sur **Autoriser**, puis à la fin du téléchargement, appuyez sur **Fermer**.

   Vous avez installé le profil. Vous pouvez afficher le profil dans les **Paramètres** et poursuivre l'installation.

8 Téléchargez et installez le profil MDM. Acceptez toutes les invites concernant l'approbation, le cas échéant.

   - Pour les terminaux dont l'iOS est antérieur à 12.2, installez le profil MDM lorsque vous y êtes invité et acceptez le message d'avertissement MDM en sélectionnant **Installer**.
   - Pour les terminaux iOS 12.2 et ultérieur, suivez les instructions pour installer le profil MDM et acceptez le message d'avertissement MDM en sélectionnant **Installer**.

Note Vous pouvez également effectuer un enrôlement sans agent, sans utiliser Workspace ONE Intelligent Hub pour l'enrôlement basé sur le Web. Pour effectuer un enrôlement sans agent, accédez à **Groupes et paramètres > Tous les paramètres > Périphériques et utilisateurs > Général** et assurez-vous que la case **Exiger l'enrôlement basé sur le Hub pour les terminaux iOS** n'est pas cochée.

Enrôlement par lots de terminaux iOS à l'aide d'Apple Configurator

Vous pouvez enrôler des terminaux par lots à l'aide d'Apple Configurator sur un ordinateur macOS afin de configurer et de déployer des terminaux iOS. En intégrant Apple Configurator à Workspace ONE UEM, vous pouvez bénéficier d'une bonne visibilité sur la gestion des terminaux, d'une prévention de sauvegarde complète et d'une gestion du cycle de vie continue au-delà de la configuration initiale.

Grâce à Apple Configurator, vous pouvez :

- Préparer une « image » de sauvegarde centrale unique pour configurer les terminaux de manière cohérente et par lots ;
- Installer le profil Workspace ONE UEM MDM en tant qu'élément de la configuration pour enrôler et gérer les terminaux ;
- Attribuer des terminaux à des utilisateurs spécifiques en ajoutant les détails propres aux terminaux, comme le numéro de série ou IMEI, au terminal enregistré d'un utilisateur dans UEM Console avant de l'enrôler avec Apple Configurator ;
- Configurer et mettre à jour les paramètres et les applications des terminaux professionnels à distance dans Workspace ONE UEM.

Pour savoir comment utiliser Apple Configurator avec Workspace ONE UEM ou pour plus d'informations, reportez-vous au document **VMware Workspace ONE UEM pour l'intégration avec Apple Configurator**.

Inscription des terminaux à l'aide du programme d'inscription des terminaux (DEP) d'Apple Business Manager

Le programme d'enrôlement des terminaux optimise les avantages des terminaux Apple enrôlés dans la Gestion de terminaux mobiles (MDM).

Grâce à DEP, vous pouvez réaliser les actions suivantes.

- Installer un profil MDM non supprimable afin d'empêcher les utilisateurs finaux de l'effacer.
- Déployer des terminaux en mode Supervisé (iOS uniquement). Les terminaux en mode supervisé peuvent accéder à des paramètres de configuration et de sécurité supplémentaires.
- Appliquer un enrôlement pour tous utilisateurs finaux.
- Répondre aux besoins de votre entreprise en personnalisant et en simplifiant le processus d'enrôlement.
- Empêcher la sauvegarde dans iCloud en désactivant l'option autorisant les utilisateurs à se connecter avec un identifiant Apple lors de la génération d'un profil DEP.
- Forcer les mises à jour iOS pour tous les utilisateurs.

Pour plus d'informations, voir les rubriques suivantes :

- Apple Business Manager : programme d'inscription des terminaux dans la *Présentation d'Apple Business Manager*.
- Le portail Assistance aux entreprises d'Apple.
- Le guide Device Enrollment Program d'Apple ou contactez votre représentant Apple.

Enrôlement de l'utilisateur

L'enrôlement de l'utilisateur est une nouvelle méthode d'enrôlement utilisée pour les terminaux iOS 13 ou versions ultérieures, qui vous permet de gérer efficacement les paramètres, les applications et les données d'entreprise tout en protégeant la confidentialité des utilisateurs et leurs données personnelles. L'enrôlement de l'utilisateur vous autorise à installer des applications, à configurer des profils et à envoyer des commandes uniquement à un conteneur d'utilisateurs géré sur le terminal plutôt qu'à l'ensemble du terminal.

Il s'appuie sur l'utilisation de MDM, qui fournit un contexte utilisateur ou « identifiant Apple géré » dans le profil MDM installé sur le terminal au moment de l'enrôlement. Le contexte utilisateur ordonne au terminal de demander à l'utilisateur de renseigner ses informations d'identification Apple gérées pour installer le profil MDM. Après l'enrôlement, un volume APFS (Apple File System) spécifique est créé pour les données gérées. Les données contenues dans le volume personnel ne sont pas accessibles depuis le volume géré, ce qui préserve la confidentialité des données utilisateur.

La création du nouveau volume géré de données empêche l'exécution de plusieurs fonctionnalités de gestion existantes pour des raisons de confidentialité. Par exemple, si une application est installée manuellement par l'utilisateur à partir de l'App Store, cette application est considérée comme personnelle et ne peut donc pas être gérée par MDM. Ces applications installées par l'utilisateur doivent d'abord être désinstallées, puis réinstallées par Workspace ONE UEM pour pouvoir être gérées.

C'est pourquoi Workspace ONE n'autorise pas l'exécution de l'enrôlement de l'utilisateur via l'application Intelligent Hub. Si Intelligent Hub a déjà été installé par l'utilisateur, désinstallez puis réinstallez le Hub via MDM afin que les autres applications activées par Workspace ONE SDK puissent accéder aux données de l'application.

Paramètres d'enrôlement utilisateur

Pour activer l'option d'enrôlement de l'utilisateur pour les terminaux iOS, rendez-vous sur la page Paramètres d'enrôlement de Workspace ONE UEM Console (**Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement**). L'activation de cette option permet aux terminaux iOS 13 ou versions ultérieures pris en charge de s'enrôler dans le groupe organisationnel à l'aide de la méthode d'enrôlement utilisateur d'Apple. L'enrôlement de l'utilisateur utilise l'identifiant Apple géré des utilisateurs plutôt que le nom de l'utilisateur d'enrôlement pour identifier l'utilisateur enrôlé par le terminal. L'identifiant Apple géré doit correspondre à l'adresse e-mail d'un utilisateur dans Workspace ONE UEM.

Enrôler un terminal iOS via l'enrôlement utilisateur

Enrôlez un terminal iOS 13 ou versions ultérieures à l'aide de l'identifiant Apple géré dans une instance Apple Business Manager fédérée à Azure AD. Un terminal avec enrôlement de l'utilisateur améliore la confidentialité pour les utilisateurs en séparant les données gérées des données personnelles et en fournissant des fonctionnalités de gestion essentielles, telles que l'installation d'applications, la configuration de Wi-Fi et les exigences de code secret.

Pour enrôler un terminal iOS :

Conditions préalables

Assurez-vous que vous remplissez les conditions préalables suivantes avant d'exécuter l'enrôlement de l'utilisateur :

- Apple Business Manager avec fédération à Azure AD
- Azure AD
- Terminal iOS 13 ou version ultérieure non surveillé
- Un utilisateur d'enrôlement avec une adresse e-mail qui correspond précisément à un identifiant Apple géré dans Apple Business Manager.

Procédure

1. Ouvrez le navigateur Safari sur votre terminal iOS 13 ou version ultérieure et accédez à l'URL d'enrôlement utilisateur de votre environnement. L'URL est le nom d'hôte des services de votre terminal ajouté au chemin d'accès `/enroll/user`.

   Par exemple :

   ```
   https://ds22.awmdm.com/enroll/user
   ```

2. Entrez l'adresse e-mail de l'utilisateur d'enrôlement correspondant à un identifiant Apple géré.

   Vous pouvez également saisir l'ID de groupe d'un groupe organisationnel au niveau ou en dessous du groupe organisationnel de l'utilisateur d'enrôlement. Sinon, le groupe organisationnel d'enrôlement de l'utilisateur est utilisé.

3. Confirmez le téléchargement du profil MDM d'enrôlement utilisateur.
4. Accédez à **Paramètres** dans l'application, puis sélectionnez **Enrôler dans {votre société}**.
5. Acceptez les invites qui vous redirigeront vers Azure AD pour les invites d'authentification et d'accès conditionnel.

   Le type et le nombre d'invites dépendent de la configuration d'Azure AD, du type d'utilisateur, du terminal ou de l'organisation.

Résultats

L'exécution l'enrôlement utilisateur est maintenant terminée. Le terminal commence à recevoir les commandes de la console UEM.

Gestion des applications sur les terminaux avec enrôlement de l'utilisateur

Les applications installées par Workspace ONE UEM sur les terminaux avec enrôlement de l'utilisateur sont gérées et associées à l'identifiant Apple géré utilisé pour enrôler le terminal. Toute application installée par l'utilisateur via l'App Store est associée à l'identifiant Apple personnel de l'utilisateur et ne peut pas être gérée.

Étant donné que l'enrôlement de l'utilisateur doit associer l'application gérée à un identifiant Apple géré, seule la distribution gérée avec des licences d'utilisateur achetées dans Apple Business Manager est prise en charge. Par exemple, les applications attribuées via l'onglet **Public** sous la page **Ressources > Applications** de la console UEM ne sont pas prises en charge sur les terminaux avec enrôlement de l'utilisateur. Les licences d'utilisateur sont gérées de la même façon dans le cadre de l'enrôlement de l'utilisateur et de l'enrôlement du terminal. Une fois l'application attribuée à un terminal avec enrôlement de l'utilisateur, une licence VPP est attribuée à l'identifiant Apple géré associé au terminal, après quoi l'application est installée.

Pour plus d'informations, consultez la section *Managed Distribution by Apple IDs* du guide *Integration with Apple Business Manager*.

Profils du terminal

3

Les profils sont votre principal moyen de gestion des terminaux. Configurez les profils pour que vos terminaux iOS restent sécurisés et configurés dans vos paramètres privilégiés. Considérez les profils de sécurité comme des paramètres facilitant l'application des procédures de l'entreprise, lorsqu'ils sont combinés à des politiques de conformité. Ils contiennent les paramètres, les configurations et les restrictions que vous souhaitez appliquer aux terminaux.

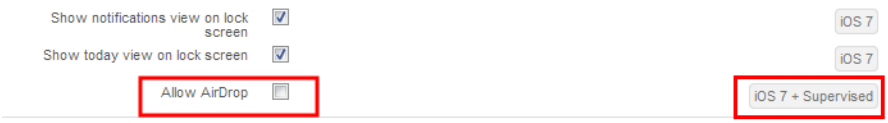
Un profil est composé des paramètres de profil généraux et d'une section de configuration spécifique. Les profils fonctionnent mieux lorsqu'ils ne contiennent qu'une seule section de configuration.

Les profils iOS s'appliquent sur un terminal au niveau de l'utilisateur ou du terminal. Lors de la création de profils iOS, sélectionnez le niveau auquel s'applique le profil. Certains profils peuvent uniquement s'appliquer au niveau utilisateur ou au niveau terminal.

Exigence de mode Supervisé pour les profils

Vous pouvez déployer certains ou tous vos terminaux iOS en **mode Supervisé**. Le mode Supervisé est un paramètre de niveau terminal qui fournit aux administrateurs des fonctionnalités et des restrictions sur la gestion avancée.

Certains paramètres de profil sont disponibles uniquement pour les terminaux supervisés. Un paramètre supervisé est repéré à l'aide d'une icône affichée à droite, qui indique la configuration requise minimale iOS nécessaire à son application.



Par exemple, vous pouvez empêcher les utilisateurs d'utiliser AirDrop pour partager des fichiers avec d'autres ordinateurs macOS et terminaux iOS en désélectionnant la case en regard de l'option **Autoriser AirDrop**. L'icône **iOS 7 + mode Supervisé** indique que seuls les terminaux exécutant iOS 7 et configurés en mode Supervisé via Apple Configurator sont concernés par cette restriction.Pour plus d'informations, reportez-vous aux guides **Intégration avec Apple Configurator** ou **Apple Business Manager**. Pour voir la liste complète des exigences relatives à la configuration iOS requise et des options de supervision, consultez l'Chapitre 10 Matrice des fonctionnalités iOS : comparaison Supervisé et Non supervisé

Accès aux terminaux

Certains profils de terminal configurent les paramètres d'accès à un terminal iOS. Utilisez ces paramètres pour veiller à ce que l'accès à un terminal est uniquement limité aux utilisateurs autorisés.

Voici certains exemples de profils d'accès à un terminal :

- Sécuriser un terminal à l'aide d'un profil Mot de passe. Pour plus d'informations, consultez la section Configurer un profil de code d'accès sur le terminal
- Limiter le terminal à une seule application à l'aide d'un profil Mode d'application unique. Pour plus d'informations, consultez la section Configurer un profil Mode d’application unique.

Sécurité des terminaux

Veillez à assurer la sécurité de vos terminaux iOS via les profils de terminaux. Ceux-ci permettent de configurer les fonctionnalités de sécurité iOS natives ou les paramètres de sécurité de l'entreprise sur un terminal via Workspace ONE UEM.

Voici certains exemples de profils de sécurité à un terminal :

- Utiliser un profil Wi-Fi pour se connecter à des terminaux enrôlés à votre Wi-Fi d'entreprise sans envoyer d'identifiants réseaux aux utilisateurs. Pour plus d'informations, consultez la section Configurer un profil Wi-Fi.
- Mettez en place des certificats numériques pour protéger vos actifs professionnels. Pour plus d'informations, consultez la section Configurer un profil Identifiants/SCEP.
- Garantir l'accès aux ressources internes pour vos terminaux grâce au profil VPN. Pour plus d'informations, consultez la section Configurer un profil VPN (Virtual Private Network).

Configuration des terminaux

Configurez les divers paramètres de vos terminaux iOS à l'aide des profils de configuration. Ces profils permettent de configurer les paramètres des terminaux afin de répondre aux besoins spécifiques de l'entreprise.

Voici certains exemples de profils de configuration de terminaux :

- Configurer une compte Exchange sur un terminal à l'aide d'un profil Exchange ActiveSync. Pour plus d'informations, consultez la section Configurer un profil de messagerie EAS pour le client de messagerie natif.
- Placez sur liste blanche un ensemble spécifique de terminaux destinés à recevoir des privilèges de diffusion Apple TV avec le profil AirPlay. Pour plus d'informations, consultez la section Configurer un profil de liste blanche AirPlay.
- Veillez à ce que les terminaux soient à jour avec le profil de mises à jour iOS. Pour plus d'informations, consultez la section Gestion des mises à jour d'OS.

Ce chapitre contient les rubriques suivantes :

Profils du code secret du terminal

Les profils de code d'accès de terminal sécurisent les terminaux iOS et leur contenu. Configurez le niveau de sécurité en fonction des besoins de vos utilisateurs.

Choisissez des options strictes pour les employés ayant une forte visibilité et des options plus souples pour les autres terminaux ou pour les employés faisant partie d'un programme permettant d'utiliser des terminaux personnels. En outre, lorsqu'un code d'accès est défini sur un terminal iOS, il fournit le chiffrement matériel du terminal et crée également un indicateur de terminal **Protection des données activée** dans l'onglet **Sécurité** de la page **Détails du terminal**.

Créez un code d'accès et configurez les options suivantes :

- **Complexité** – Utilisez des valeurs simples pour un accès rapide ou des codes d'accès alphanumériques pour une sécurité renforcée. Vous pouvez également exiger un nombre minimum de caractères complexes (@, #, &, !, ?) dans le code d'accès. Par exemple, vous pouvez exiger des utilisateurs ayant accès à du contenu sensible qu'ils utilisent des codes d'accès plus stricts.
- **Nombre maximum de tentatives infructueuses** – Empêchez tout accès non autorisé en réinitialisant ou en verrouillant le terminal après un nombre déterminé de tentatives. Cette option fonctionne bien pour les terminaux appartenant à l'entreprise, mais pas avec les terminaux appartenant aux employés dans un programme BYOD. Par exemple, si un terminal a une limite de cinq tentatives infructueuses de saisie du code d'accès et qu'un utilisateur a entré un code d'accès erroné cinq fois d'affilée, le terminal effectue automatiquement une réinitialisation complète. Si le simple verrouillage du terminal est préférable, définissez cette option sur **Aucun**, ce qui signifie que le nombre de tentatives de saisie du code d'accès est illimité.
- **Durée de vie maximale du code d'accès** – Imposez le renouvellement des codes d'accès à intervalles réguliers. Les codes d'accès modifiés fréquemment sont moins vulnérables aux tentatives d'accès des utilisateurs non autorisés.
- **Verrouillage automatique (min)** – Verrouille le terminal automatiquement après une période définie. Ce verrouillage garantit que le contenu du terminal n'est pas compromis si un utilisateur laisse accidentellement son téléphone sans surveillance.

Configurer un profil de code d'accès sur le terminal

Les profils de code d'accès de terminal sécurisent les terminaux iOS et leur contenu. Configurez plusieurs paramètres dans le cadre d'une section de configuration Code d'accès afin d'appliquer des codes d'accès de terminal en fonction des besoins des utilisateurs.

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **Code d'accès** dans la liste.

4 Configurez les paramètres **Code d'accès** :

Paramètre	Description
Exiger un code d'accès sur le terminal	Active la protection par code d'accès obligatoire.
Valeurs simples autorisées	Autorisez l'utilisateur à appliquer un code d'accès numérique simple.
Exiger une valeur alphanumérique	Empêchez l'utilisateur d'utiliser des espaces ou des caractères non alphanumériques dans le code d'accès.
longueur min. du code d'accès	Sélectionnez le nombre minimum de caractères requis pour le code d'accès.
Nombre minimum de caractères complexes	Sélectionnez le nombre minimum de caractères complexes (#, $,!, @) requis pour un code d'accès.
Durée de vie maximale du code d'accès (en jours)	Sélectionnez le nombre maximum de jours durant lequel le code d'accès restera actif.
Verrouillage automatique (en min)	Sélectionnez la durée pendant laquelle le terminal peut être en veille avant le blocage automatique de l'écran.
historique du code d'accès	Sélectionnez le nombre de codes d'accès à stocker dans l'historique qu'un utilisateur ne peut pas répéter.
Période de grâce avant verrouillage du terminal (min)	Sélectionnez la durée d'inactivité (en minutes) d'un terminal avant son verrouillage par le système et après laquelle l'utilisateur doit ressaisir son code d'accès.
Nombre maximum de tentatives infructueuses	Sélectionnez le nombre de tentatives autorisées. Si l'utilisateur entre un code d'accès incorrect le nombre de fois indiqué, le terminal effectue une réinitialisation sur les valeurs usine.

5 Cliquez sur **Enregistrer et publier**.

Profils de restriction du terminal

Profils de restriction – Limitent la façon dont les employés peuvent utiliser leurs terminaux iOS et permettent aux administrateurs de verrouiller la fonctionnalité native des terminaux iOS et de mettre en œuvre un système de prévention contre la perte des données.

Remarque : certaines options de restriction de la page des profils **Restrictions** sont accompagnées d'une icône qui indique la configuration iOS minimale requise pour pouvoir appliquer la restriction. Par exemple, l'icône **iOS 7 + mode Supervisé** située à côté de la case à cocher **Autoriser AirDrop** signifie que seuls les terminaux s'exécutant sous iOS 7, définis pour s'exécuter en mode Supervisé et utilisant Importer un profil Apple Configurator signé dans UEM Console ou le Inscription des terminaux à l'aide du programme d'inscription des terminaux (DEP) d'Apple Business Manager d'Apple sont concernés par cette restriction.

Les instructions détaillées indiquées ici répertorient quelques exemples fonctionnels des paramètres que vous pouvez limiter. Pour voir la liste complète des exigences en matière de version iOS et de mode Supervisé, consultez l'Chapitre 10 Matrice des fonctionnalités iOS : comparaison Supervisé et Non supervisé.

Configurations des profils de restriction

Un profil de restriction peut être personnalisé pour contrôler les applications, le matériel et les fonctionnalités accessibles par les utilisateurs. Utilisez ces restrictions pour améliorer la productivité, protéger les utilisateurs et les terminaux, et séparer les données personnelles et les données d'entreprise.

Pour configurer un profil de restrictions, consultez la section Configurer un profil de restriction sur le terminal.

Les restrictions suivantes constituent une liste représentative, mais pas exhaustive, des options.

Restrictions d'OS

Restrictions de retard du logiciel au niveau du système d'exploitation qui vous permettent de masquer les mises à jour iOS aux utilisateurs finaux pendant un nombre de jours spécifié.

Paramètres	Description
Retarder les mises à jour (jours)	Activez cette option et indiquez le nombre de jours pendant lesquels différer la mise à jour logicielle. Nombre de jours allant de 1 à 90. (Terminaux supervisés iOS 11.3 et versions ultérieures). Le nombre de jours indique le laps de temps après le lancement de la mise à jour logicielle et pas après l'heure de l'installation du profil.

Restrictions concernant la fonctionnalité des terminaux

Les restrictions au niveau du terminal peuvent désactiver les fonctionnalités importantes comme l'appareil photo, FaceTime, Siri et les achats au sein des applications pour améliorer la productivité et la sécurité.

- Empêchez les utilisateurs de modifier les paramètres Bluetooth du terminal. (iOS 10 et versions ultérieures).
- Bloquez les captures d'écran du terminal afin de préserver la confidentialité du contenu professionnel du terminal.
- Désactivez Siri lorsque le terminal est verrouillé afin d'empêcher l'accès aux e-mails, au téléphone et aux notes sans le code d'accès sécurisé (iOS 7 et versions ultérieures).

  Par défaut, les utilisateurs peuvent maintenir le bouton d'**accueil** enfoncé et utiliser Siri, même lorsque le terminal est verrouillé. Cette option permet aux utilisateurs non autorisés d'accéder aux informations sensibles et d'effectuer des actions sur un terminal qui n'est pas le leur. Si votre entreprise a des exigences strictes en matière de sécurité, vous pouvez déployer un profil **Restrictions** qui empêche l'utilisation de Siri lorsqu'un terminal est verrouillé.
- Empêchez la synchronisation automatique lors de l'itinérance afin de réduire les surcoûts liés aux données.

- Empêchez le déverrouillage du terminal par Touch ID (iOS 7 et versions ultérieures).
- Empêchez les utilisateurs finaux de modifier le paramètre de point d'accès personnel sur le terminal (iOS 12.2 et versions ultérieures, mode Supervisé). Si la restriction est activée ou désactivée dans le profil, vous pouvez remplacer le paramètre de point d'accès personnel à l'aide de la commande de paramètres gérés de point d'accès personnel.
- Limitez la demande de journalisation de l'utilisateur final sur les serveurs Siri. Lorsque la restriction est désactivée, Siri ne journalise pas les données de journalisation de l'utilisateur final sur le serveur.
- Empêchez les utilisateurs finaux d'activer ou de désactiver le Wi-Fi dans les paramètres ou le centre de contrôle du terminal (même en cas d'activation ou désactivation du mode avion) en activant l'option **Forcer l'activation du Wi-Fi** sur la console UEM (iOS 10.3 et versions ultérieures).
- Désactivez **Accès aux fichiers des lecteurs réseau** pour empêcher les utilisateurs de se connecter aux lecteurs réseau dans l'application Fichiers (iOS 10.3 et versions ultérieures).

Principales restrictions relatives à un terminal iOS 8

- Désactivez le transfert qui peut être utilisé pour démarrer une activité sur un terminal, localiser d'autres terminaux et reprendre des activités sur des applications partagées.
- Désactivez les résultats des recherches Internet dans Spotlight. Cette restriction empêche l'affichage des sites Web suggérés lorsque la recherche est effectuée à l'aide de Spotlight. (iOS 8 et versions ultérieures, mode Supervisé)
- Désactivez la configuration du paramètre Restrictions. Cette autorisation permet aux administrateurs de remplacer la configuration des restrictions personnelles par l'intermédiaire du menu Paramètres du terminal (iOS 8 et versions ultérieures, mode Supervisé).
- Empêchez l'utilisateur d'effacer tout le contenu et les paramètres sur le terminal. Cette restriction empêche les utilisateurs d'effacer et de désenrôler le terminal (iOS 8 et versions ultérieures, mode Supervisé).
- Désactivez le stockage local des données en sauvegardant des applications gérées avec iCloud.
- Désactivez la sauvegarde des livres d'entreprise avec iCloud.
- Empêchez les utilisateurs de synchroniser des notes et des favoris dans les livres professionnels avec iCloud.
- Désactivez l'ajout ou la suppression des informations existantes sur Touch ID (iOS 8.1.3 et versions ultérieures, mode Supervisé).
- Désactivez les podcasts. Cette restriction empêche l'accès à l'application de podcast d'Apple (mode Supervisé uniquement).

Principales restrictions relatives à un terminal iOS 9

- Désactivez la modification des codes d'accès afin d'empêcher l'ajout, la modification ou la suppression d'un code d'accès de terminal (mode Supervisé uniquement).
- Masquez l'App Store. Cette restriction désactive l'App Store et supprime l'icône de l'écran d'accueil. Les utilisateurs peuvent encore utiliser MDM pour installer ou mettre à jour leurs applications, ce qui donne à l'administrateur un contrôle complet sur les applications (mode Supervisé uniquement).
- Désactivez les téléchargements automatiques d'applications. Cette restriction empêche la synchronisation automatique des applications achetées sur d'autres terminaux. Elle n'a pas d'incidence sur les mises à jour des applications existantes (mode Supervisé uniquement).
- Désactivez la modification du nom des terminaux. Cette restriction empêche les utilisateurs de changer le nom des terminaux. Il est conseillé d'appliquer cette restriction pour les déploiements de terminaux partagés et préenrôlés (mode Supervisé uniquement).
- Désactivez la modification du fond d'écran. Cette restriction empêche les utilisateurs de changer le fond d'écran des terminaux (mode Supervisé uniquement).
- Désactivez AirDrop comme destination de dépôt non gérée afin d'empêcher les utilisateurs d'envoyer à AirDrop des données d'entreprise ou des pièces jointes depuis une application gérée. Cette restriction nécessite également la restriction en matière de fonctionnalité « Ouvrir dans » gérée d'Apple.
- Désactivez les raccourcis clavier afin d'empêcher les utilisateurs de créer et d'utiliser des raccourcis clavier (mode Supervisé uniquement).
- Désactivez News afin d'empêcher l'accès à l'application News d'Apple (mode Supervisé uniquement).
- Désactivez la bibliothèque iCloud iPhoto. Cette restriction empêche le stockage local des photos qui ne sont pas totalement téléchargées depuis la bibliothèque.
- Désactivez la fiabilité des applications d'entreprise externes afin d'empêcher les utilisateurs d'installer des applications non gérées, signées par l'entreprise et non fiables. Les applications d'entreprise gérées en interne sont implicitement fiables.
- Désactivez l'enregistrement vidéo en interdisant la capture d'écran afin d'empêcher les utilisateurs d'effectuer des captures de l'écran des terminaux.
- Désactivez le service Music qui empêche l'installation de l'application Music (iOS 8.3.3 et versions ultérieures, mode Supervisé uniquement).

Principales restrictions relatives à un terminal iOS 9.3

- Désactivez le service iTunes Radio qui empêche l'installation d'iTunes Radio. Si Apple Music n'est pas restreint, le service Radio s'affiche dans l'application Apple Music (mode Supervisé uniquement).

Principales restrictions relatives à un terminal watchOS

- Désactivez le couplage Apple Watch qui dissocie et efface toute Apple Watch couplée (iOS 9 et versions ultérieures, mode Supervisé).
- Appliquez la détection du poignet qui verrouille l'Apple Watch lorsqu'elle n'est pas portée.

Restrictions de niveau application

Les restrictions de niveau application désactivent certaines applications telles que YouTube, iTunes et Safari, ou certaines de leurs fonctionnalités, afin d'appliquer les politiques d'utilisation de l'entreprise. Les restrictions disponibles sont les suivantes :

- Désactivez le remplissage automatique afin que les informations confidentielles ne soient pas insérées automatiquement dans certains formulaires.
- Activez la fonction d'avertissement en cas de fraude pour forcer Safari à afficher un avertissement lorsque les utilisateurs visitent des sites Internet susceptibles d'être des sites d'hameçonnage.
- Contrôlez l'acceptation des cookies dans Safari. Vous pouvez configurer Safari pour qu'il n'accepte aucun cookie ou uniquement ceux de sites spécifiques.
- Bloquez l'accès au Game Center et aux jeux multijoueurs afin d'appliquer les politiques professionnelles pour l'utilisation du terminal pendant les heures de bureau.
- Activez ou désactivez les applications individuelles, natives et autres en les ajoutant à la section **Afficher les applications** ou **Masquer les applications**. Cette restriction vous permet d'afficher ou de masquer des applications en fonction des besoins (pour iOS 9.3 et versions ultérieures, mode Supervisé uniquement).
  - Pour la mise sur liste blanche des raccourcis Internet, ajoutez l'ID de bundle **com.apple.webapp** à la zone de texte **Afficher les applications**.

Restrictions concernant iCloud

Pour les terminaux exécutant iOS 7 ou versions ultérieures, les utilisateurs peuvent stocker, sauvegarder ou synchroniser les données de leurs terminaux dans iCloud, l'ensemble de serveurs Apple. Ces données comprennent les photos, vidéos, paramètres du terminal, données d'application, messages, documents, etc. Afin de s'adapter aux besoins de votre entreprise, Workspace ONE UEM établit des restrictions pour les terminaux iOS 7 et versions ultérieures qui peuvent désactiver iCloud ou la fonctionnalité iCloud en fonction des besoins.

Le contenu Exchange ActiveSync (e-mails, contacts, calendriers, tâches) et tous les autres profils de déploiement mobile ne sont pas synchronisés vers l'instance iCloud d'un utilisateur.

Exigences en matière d'administration	Restriction	Paramètre désactivé sur le terminal
Restreindre la configuration iCloud (restriction de fonctionnalité des terminaux)		
Restreindre la possibilité de connexion à iCloud et de configuration des paramètres iCloud	Autoriser les modifications de comptes (supervision obligatoire)	Désactive l'option iCloud dans les paramètres de terminal (iOS 7 et versions ultérieures, mode Supervisé) Cette restriction empêche également la modification des autres comptes, par exemple le compte de messagerie, dans les paramètres du terminal.
Gestion iCloud (restrictions iCloud granulaires)		
Empêchez les utilisateurs de sauvegarder des données dans iCloud	Autoriser la sauvegarde	Désactive l'option Sauvegarde dans les paramètres iCloud (iOS 7)
Empêche les utilisateurs de stocker des documents et des données à iCloud Drive	Autoriser la synchronisation de documents	Supprime l'option iCloud Drive dans les paramètres iCloud (iOS 7)
Empêche les utilisateurs de stocker dans iCloud leur mot de passe et les informations de leur carte de crédit	Autoriser la synchronisation du trousseau	Supprime l'option Trousseau dans les paramètres iCloud (iOS 7)
Empêche les utilisateurs d'applications gérées de stocker des documents dans iCloud	Autoriser les applications gérées à stocker les données	Désactive les applications gérées et les empêche de stocker des documents dans iCloud Drive (iOS 8)
Empêcher les utilisateurs de sauvegarder des livres d'entreprise dans iCloud	Autoriser la sauvegarde de livres professionnels	Désactive les livres gérés et empêche leur sauvegarde dans iCloud ou iTunes (iOS 8)
Empêche la synchronisation des livres d'entreprise, notes et favoris	Autoriser la synchronisation des notes, des favoris et des livres professionnels	Désactive les notes et les favoris pour les livres professionnels dans iBooks (iOS 8)
Empêche les utilisateurs de synchroniser des photos dans iCloud	Autoriser le flux de photos et Autoriser le flux de photos partagé	Supprime l'option Photos dans les paramètres iCloud (iOS 7)
Empêche automatiquement l'importation de nouvelles photos et leur envoi dans les terminaux iCloud	Autoriser le flux de photos partagé	Désactive Mon flux de photos dans Photos, dans les paramètres iCloud (iOS 7)

Les sauvegardes iCloud n'ont lieu que si :

- Aucune restriction des sauvegardes iCloud n'est en place ;
- Le paramètre de basculement vers iCloud est activé dans **Réglages > iCloud > Sauvegarde sur le terminal**.
- Le Wi-Fi est activé ;
- le terminal est branché sur une source d'alimentation et verrouillé.

Restrictions en matière de sécurité et de confidentialité

Les restrictions liées à la sécurité et à la confidentialité empêchent les utilisateurs d'effectuer certaines actions susceptibles de violer la politique professionnelle ou de compromettre le terminal d'une autre façon. Les restrictions disponibles sont les suivantes :

- Empêcher les utilisateurs des terminaux iOS 11.4.1 et versions ultérieures d'entrer le code d'accès pour se connecter initialement ou pour rester connectés aux accessoires USB alors que le terminal est verrouillé.
- Empêcher les utilisateurs de faire confiance aux applications d'entreprise non gérées.
- Empêcher la saisie de force d'un mot de passe pour l'iTunes Store.
- Empêcher les données de diagnostic qui incluent les informations de localisation et les données d'utilisation à envoyer à Apple pour les aider à améliorer le logiciel iOS.
- Empêcher les utilisateurs d'accepter des certificats TLS non approuvés de manière à ce qu'ils ne puissent pas accéder aux sites Web avec des certificats SSL non valides. Si vous autorisez les certificats TLS non approuvés, les utilisateurs sont informés de la présence de certificats non valides, mais peuvent continuer s'ils le souhaitent.
- Empêcher la mise à jour des infrastructures de clés publiques (PKI) à distance.
- Forcer le chiffrement des sauvegardes. Les sauvegardes chiffrées garantissent que toutes les informations personnelles comme les mots de passe des comptes de messagerie ou les informations de contact sont chiffrées lors de la sauvegarde et du stockage sur les terminaux.
- Empêcher le couplage avec des hôtes différents de l'Apple Configurator.
- Empêcher les terminaux iOS 10.3 et versions ultérieures de se connecter à des réseaux inconnus ou malveillants. Les terminaux activés avec cette restriction ne peuvent se connecter qu'aux réseaux Wi-Fi gérés. Sélectionnez **Forcer la mise sur liste blanche** du Wi-Fi pour appliquer cette restriction.

Restrictions en matière de contenu multimédia

Les restrictions basées sur les notations bloquent l'accès à certains contenus en fonction de leur notation, gérée par région. Les restrictions disponibles sont les suivantes :

- Restreignez l'accès au contenu pour adultes sur des terminaux professionnels dans le cadre de la politique d'entreprise.
- Bloquez l'accès aux applications réservées aux personnes majeures pendant les heures de bureau normales.
- Bloquez l'accès à du contenu iBook inapproprié ou explicite sur les terminaux professionnels.

Configurer un profil de restriction sur le terminal

Profils de restriction – Limitent la façon dont les employés utilisent leurs terminaux iOS et permettent aux administrateurs de verrouiller la fonctionnalité native des terminaux iOS et de mettre en œuvre un système de prévention contre la perte des données.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Restrictions** dans la liste. Vous pouvez inclure plusieurs restrictions dans la même section de configuration.

4 Configurez les paramètres de **Restrictions**. Pour plus d'informations, consultez la section Configurations des profils de restriction.

5 Cliquez sur **Enregistrer et publier**.

Configurer un profil Wi-Fi

La configuration d'un profil Wi-Fi permet aux terminaux de se connecter aux réseaux d'entreprise, même s'ils sont masqués, chiffrés ou protégés par mot de passe. Cette section de configuration est utile pour les utilisateurs qui voyagent et utilisent leur propre réseau sans fil, ou pour les utilisateurs qui se trouvent dans un bureau dans lequel ils peuvent connecter leur terminal automatiquement à un réseau sans fil sur site.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Wi-Fi** dans la liste.

4 Configurez les paramètres du **Wi-Fi**.

Paramètre	Description
Identifiant SSID	Saisissez nom du réseau auquel le terminal se connecte.
Réseau masqué	Saisissez une connexion à un réseau qui n'est pas ouvert ou qui n'émet aucune donnée.
Rejoindre automatiquement	Déterminez si le terminal se connecte automatiquement au réseau lors du démarrage du terminal. Le terminal conserve une connexion active jusqu'au redémarrage du terminal ou jusqu'à la sélection manuelle d'une autre connexion.
Type de sécurité	Sélectionnez le type de protocole d'accès à utiliser. Saisissez le **Mot de passe** ou sélectionnez les **Protocoles** qui s'appliquent à votre réseau Wi-Fi.
Protocoles	Choisissez les protocoles d'accès réseau. ■ Cette option apparaît lorsque **Wi-Fi** et **Type de sécurité** sont définis sur l'un des paramètres **Entreprise**. Cette option s'affiche également lorsque **Ethernet** est sélectionné.

Paramètre	Description
Point d'accès Wi-Fi 2.0	Active la fonctionnalité Point d'accès Wi-Fi 2.0 et n'est disponible que pour les terminaux iOS 7 et versions ultérieures. Le point d'accès 2.0 est un type d'accès Wi-Fi public qui permet aux terminaux de s'identifier et de se connecter facilement au meilleur point d'accès disponible. Les forfaits des fournisseurs doivent prendre en charge les points d'accès 2.0 pour que cette option fonctionne correctement.
Nom de domaine	Saisissez le nom du domaine du fournisseur de service du Passpoint.
Autorise la connexion aux réseaux Passpoint des partenaires d'itinérance	Activez l'itinérance vers les réseaux Passpoint partenaires.
Nom de l'opérateur affiché	Saisissez le nom du fournisseur de services du point d'accès Wi-Fi.
ID d'organisation du consortium en itinérance	Saisissez les identifiants de l'organisation du consortium en itinérance.
ID d'accès réseau	Saisissez les noms de domaine d'ID d'accès au réseau.
MCC/MNC	Saisissez la configuration Mobile country code/Mobile network code, sous la forme d'un nombre à 6 chiffres.
Authentification	Configurez les paramètres d'**authentification** qui varient selon le protocole.
Nom d'utilisateur	Saisissez un nom d'utilisateur pour le compte.
Mot de passe par connexion de l'utilisateur	Demandez le mot de passe lors de la connexion et envoyez-le avec l'authentification.
Mot de passe	Entrez le mot de passe pour la connexion.
Certificat d'identité	Sélectionnez le certificat pour l'authentification.
Identité externe	Sélectionnez la méthode d'authentification externe.
Version TLS minimale	Sélectionnez la version TLS minimale (1.0, 1.1 et 1.2). Si aucune valeur n'est sélectionnée, la version TLS minimale est définie par défaut sur 1.0. **Note** et les versions TLS maximales peuvent uniquement être configurées pour les types de protocole TLS, TTLS, EAP-Fast et PEAP.
Version TLS maximale	Sélectionnez la version TLS maximale (1.0, 1.1 et 1.2). Si aucune valeur n'est sélectionnée, la version TLS maximale est définie par défaut sur 1.2.
Certificats approuvés	Il s'agit des certificats de serveurs fiables pour votre réseau Wi-Fi.
Noms des certificats de serveurs approuvés	Entrez les noms des certificats de serveur approuvés.
Autoriser les exceptions de fiabilité	Autorisez les utilisateurs à prendre des décisions avisées.

5 Configurez les paramètres **Proxy** pour les types de proxy **Manuel** ou **Auto**.

6 Si vous utilisez une infrastructure Cisco, configurez la Politique de marquage QoS (terminaux iOS v11 et versions ultérieures).

Paramètre	Description
Marquage QoS pour Fastlane	Sélectionnez la configuration de marquage requise.
Activer le marquage QoS	Sélectionnez cette option pour choisir les applications concernées par les attributions de données prioritaires.
Autoriser les services d'appels d'Apple	Sélectionnez cette option pour ajouter les services d'appel Wifi d'Apple à votre liste blanche de QoS.
Autoriser des application à utiliser le marquage QoS	Recherchez les applications concernées par les attributions de données prioritaires et ajoutez-les.

7 (Facultatif) Configurez le **portail Captivate** pour le contourner.

8 Sélectionnez **Enregistrer et publier** lorsque vous avez terminé d'envoyer le profil aux terminaux.

Configurer un profil VPN (Virtual Private Network)

Les réseaux privés virtuels (VPN) fournissent aux terminaux un tunnel sécurisé et chiffré pour accéder aux ressources internes. Les profils VPN permettent à chaque terminal de fonctionner comme s'il était connecté sur un réseau sur site. La configuration d'un profil VPN assure aux utilisateurs finaux un accès facile aux e-mails, aux fichiers et au contenu.

Procédure

1 Accédez à **Ressources > Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **VPN**.

4 Configurez les informations de **connexion** :

Les paramètres que vous voyez peuvent varier en fonction du **Type de connexion** que vous choisissez. Pour plus d'informations sur l'utilisation de Forcepoint ou Blue Coat pour filtrer le contenu, reportez-vous aux sections Configurer un profil de filtrage de contenu Forcepoint et Configurer un profil de filtrage de contenu Blue Coat.

Paramètres	Description
Nom de la connexion	Saisissez le nom affiché de la connexion à afficher sur le terminal.
Type de connexion	Utilisez le menu déroulant pour sélectionner la méthode de connexion réseau.
Serveur	Saisissez le nom d'hôte ou l'adresse IP du serveur utilisé pour la connexion.
Compte	Saisissez le nom du compte VPN.
Envoyer tout le trafic	Permet de forcer l'ensemble du trafic à travers le réseau spécifié.

Paramètres	Description
Déconnexion en cas d'inactivité	Autorisez le VPN à se déconnecter automatiquement après une certaine durée. La prise en charge de cette valeur dépend du fournisseur VPN.
Se connecter automatiquement	Sélectionnez cette option pour autoriser le VPN à se connecter automatiquement aux domaines suivants. Cette option s'affiche lorsque l'option **Règles du VPN par application** est sélectionnée. ■ Domaines pour Safari ■ Domaines de messagerie ■ Domaines de contacts ■ Domaines de calendrier
Type de fournisseur	Sélectionnez le type de service VPN. Si le type de service VPN est un proxy d'application, le service VPN achemine le trafic au niveau de l'application. S'il s'agit d'un tunnel de paquets, le service VPN achemine le trafic au niveau de la couche IP.
Règles du VPN par application	Active le VPN par application pour les terminaux. Pour plus d'informations, consultez la section Configurer un profil VPN par application.
Authentification	Sélectionnez la méthode d'authentification des utilisateurs finaux. Suivez les indications qui s'affichent pour importer un **Certificat d'identité** ou saisissez un **Mot de passe** ou la clé **Secret partagé** à fournir pour donner aux utilisateurs l'accès VPN.
Activer le VPN à la demande	Activez le VPN à la demande afin d'utiliser des certificats pour établir automatiquement des connexions VPN à l'aide des informations de la section Configurer un profil VPN par application de ce guide.
Proxy	Sélectionnez le type de proxy **Manuel** ou **Automatique** à configurer avec cette connexion VPN.
Serveur	Saisissez l'URL du serveur proxy.
Port	Saisissez le port utilisé pour communiquer avec le proxy.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour vous connecter au serveur proxy.
Mot de passe	Saisissez le mot de passe pour vous authentifier.
Clés du fournisseur	Sélectionnez cette option pour créer des clés personnalisés à ajouter au dictionnaire de configuration du fournisseur.
Clé	Saisissez la clé spécifique fournie par le fournisseur.
Valeur	Saisissez la valeur VPN pour chaque clé.
Exclure les réseaux locaux	Activez cette option pour inclure tous les réseaux afin d'acheminer le trafic réseau en dehors du VPN.
Inclure tous les réseaux	Activez cette option pour inclure tous les réseaux afin d'acheminer le trafic réseau via le VPN.

Note Si vous avez choisi le type IKEv2, vous êtes autorisé à entrer la version TLS minimale et maximale pour la connexion VPN, à condition que vous ayez coché la case **Activer EAP** avant d'entrer la version TLS.

5 Cliquez sur **Enregistrer et publier**. Les utilisateurs ont désormais accès aux sites autorisés.

Configurer un profil de filtrage de contenu Forcepoint

L'intégration de Workspace ONE UEM à Forcepoint vous permet d'utiliser vos catégories de filtrage de contenu existantes dans Forcepoint et de les appliquer aux terminaux que vous gérez dans UEM Console.

Autorisez ou bloquez l'accès à des sites Web en fonction des sites Web que vous configurez dans Forcepoint, puis déployez une section de configuration VPN pour forcer les terminaux à respecter ces règles. Les utilisateurs de l'annuaire enrôlés dans Workspace ONE UEM sont validés via Forcepoint pour déterminer les règles de filtrage de contenu à appliquer selon l'utilisateur final.

Vous pouvez appliquer le filtrage de contenu avec Forcepoint de l'une des deux manières suivantes.

- Utilisez le profil **VPN** en fonction des descriptions de cette section. La mise en place d'un filtrage du contenu à l'aide du profil VPN peut s'appliquer à l'ensemble du trafic Web utilisant d'autres navigateurs que VMware Browser.
- Configurez la page **Paramètres et politiques** qui s'applique à l'ensemble du trafic Web utilisant d'autres navigateurs que VMware Browser. Pour obtenir des instructions sur la configuration de **Paramètres et politiques**, consultez le **Guide VMware Browser**.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter**. Sélectionnez **Apple iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **VPN**.
4. Sélectionnez **Websense (Forcepoint)** comme **Type de connexion**.
5. Configurez les informations de C**onnexion** :

Paramètres	Description
Nom de la connexion	Saisissez le nom de la connexion à afficher.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour vous connecter au serveur proxy.
Mot de passe	Saisissez le mot de passe pour la connexion.

6. (Facultatif) Vous pouvez également sélectionner **Test de la connexion**.
7. Définissez les paramètres **Configurations du fournisseur**.

Paramètre	Description
Clés du fournisseur	Créez des clés personnalisées à ajouter au dictionnaire de configuration du fournisseur.
Clé	Saisissez la clé spécifique fournie par le fournisseur.
Valeur	Saisissez la valeur VPN pour chaque clé.

8 Cliquez sur **Enregistrer et publier**. Les utilisateurs basés sur l'annuaire peuvent désormais accéder aux sites autorisés selon vos catégories Forcepoint.

Configurer un profil de filtrage de contenu Blue Coat

L'intégration Workspace ONE UEM avec Blue Coat vous permet d'utiliser dans Blue Coat les règles de filtrage de contenu existantes.

Autorisez ou bloquez l'accès à des sites web selon les règles que vous configurez dans Blue Coat, puis déployez une section de configuration VPN pour forcer les terminaux à respecter ces règles.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base > Profils > Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **VPN**.

4 Sélectionnez **Blue Coat** en tant que **Type de connexion**.

Paramètre	Description
ID Blue Coat du client	Accédez à cette valeur en vous connectant au site Web de Blue Coat et en accédant à la section API Tokens & Keys, dans laquelle vous pouvez ajouter un partenaire MDM et obtenir l'identifiant. Contactez Blue Coat pour plus d'informations ou pour obtenir de l'aide.
VPN par application	Activez le VPN par application (facultatif). Pour plus d'informations, consultez la section Configurer un profil VPN par application.

5 Vous pouvez également sélectionner **Test de la connexion** si vous le souhaitez.

6 Configurez **Configurations du fournisseur** :

Paramètre	Description
Clés du fournisseur	Sélectionnez cette option pour créer des clés personnalisées à ajouter au dictionnaire de configuration du fournisseur.
Clé	Saisissez la clé spécifique fournie par le fournisseur.
Valeur	Saisissez la valeur VPN pour chaque clé.

7 Cliquez sur **Enregistrer et publier**. Les utilisateurs ont désormais accès aux sites autorisés en fonction de vos règles de filtrage de contenu Blue Coat.

Configurer un profil VPN à la demande

Le VPN à la demande est le processus d'établissement automatique d'une connexion VPN pour des domaines spécifiques. Pour une meilleure sécurité et une plus grande facilité d'utilisation, le VPN à la demande utilise, pour l'authentification, des certificats au lieu des codes d'accès simples.

Conditions préalables

Assurez-vous que votre autorité de certification et les modèles de certificat dans Workspace ONE UEM sont convenablement configurés pour la distribution des certificats. Rendez l'application VPN tierce de votre choix disponible pour les utilisateurs en l'envoyant vers les terminaux ou en la recommandant dans votre catalogue d'applications d'entreprise.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter**, puis sélectionnez **iOS**.
2. Sélectionnez la section de configuration **VPN** dans la liste.
3. Configurez votre Configurer un profil VPN (Virtual Private Network) en conséquence.
4. Sélectionnez **Certificat** dans le menu déroulant **Authentification de l'utilisateur**. Naviguez vers la section de configuration **Identifiants**.
   a. Dans le menu déroulant **Source des identifiants**, sélectionnez **Autorité de certification définie**.
   b. Sélectionnez l'**Autorité de certification** et le **Modèle de certificat** dans les menus déroulants correspondants.
   c. Revenez à la section de configuration **VPN**.
5. Sélectionnez le **Certificat d'identité** tel qu'il est indiqué dans la section de configuration **Identifiants** si vous appliquez une authentification de certificat au profil VPN.
6. Cochez la case **Activer le VPN à la demande**.
7. Configurez l'option **Utiliser les nouvelles clés à la demande (iOS 7)** pour activer une connexion VPN lorsque les utilisateurs accèdent à l'un des domaines spécifiés :

Paramètre	Description
Utiliser de nouvelles clés à la demande (iOS 7 et versions ultérieures)	Sélectionnez cette option pour utiliser la nouvelle syntaxe qui permet d'indiquer des règles VPN plus granulaires.
Règle à la demande/Action	Choisissez une **Action** pour définir le comportement VPN à appliquer à la connexion VPN en fonction des critères définis. Si le critère est vrai, l'action spécifiée se produit. ■ **Évaluer la connexion** : établit automatiquement la connexion au tunnel VPN en fonction des paramètres réseau et des caractéristiques de chaque connexion. L'évaluation se produit chaque fois que le VPN se connecte à un site Web. ■ **Connecter** : établit automatiquement la connexion au tunnel VPN lors de la nouvelle tentative de connexion au réseau si les critères réseau sont satisfaits. ■ **Déconnecter** : désactive automatiquement la connexion au tunnel VPN et ne se reconnecte pas à la demande si les critères réseau sont satisfaits. ■ **Ignorer** : quitte la connexion VPN existante, mais ne se reconnecte pas à la demande si les critères réseau sont satisfaits.

Paramètre	Description
Paramètre d'action	Configurez les **Paramètres d'action** pour que les domaines spécifiés déclenchent une tentative de connexion VPN en cas d'échec de la résolution des noms de domaine, par exemple lorsque le serveur DNS indique qu'il ne parvient pas à résoudre le domaine, répond par une redirection vers un autre serveur ou ne parvient pas à répondre (expiration). Si vous choisissez **Évaluer la connexion**, ces options sont les suivantes : ■ Choisissez **Connecter si besoin/Ne jamais connecter** et saisissez des informations supplémentaires : ■ **Domaines** – Saisissez les domaines pour lesquels cette évolution s'applique. ■ **Analyse de l'URL** – Saisissez une URL HTTP ou, de préférence, HTTPS à analyser à l'aide d'une requête GET. Si le nom d'hôte de l'URL ne peut pas être résolu, si le serveur est inaccessible ou ne répond pas avec un code de statut 200 HTTP, une connexion VPN est établie en réponse. ■ **Serveurs DNS** – Saisissez une série d'adresses IP de serveur DNS à utiliser pour la résolution des domaines spécifiés. Ces serveurs ne doivent pas nécessairement faire partir de la configuration réseau actuelle du terminal. Si ces serveurs DNS ne sont pas accessibles, une connexion VPN est établie en réponse. Il doit s'agir de serveurs DNS internes ou de serveurs DNS externes approuvés. (facultatif)
Critères/Valeur pour le paramètre	■ **Correspondance des interfaces** – Sélectionnez le type de connexion qui correspond à l'adaptateur actuel du réseau du terminal. Les valeurs disponibles sont **Tout**, **Wifi**, **Ethernet** et **Cellulaire**. ■ **Détection de l'URL** – Saisissez l'URL spécifiée pour que les critères soient satisfaits. Lorsque les critères sont satisfaits, un code de statut 200 HTTP est renvoyé. Ce format inclut le protocole (https). ■ **Correspondance SSID** – Saisissez l'ID réseau actuel du terminal. Pour que les critères soient satisfaits, l'ID doit correspondre à au moins l'une des valeurs de la plage. ■ Utilisez l'icône **+** pour entrer plusieurs SSID si nécessaire. ■ **Correspondance de domaines DSN** – Saisissez le domaine de recherche du réseau actuel du terminal. Vous pouvez utiliser un caractère générique (*.exemple.com). ■ **Correspondance d'adresses DNS** – Saisissez l'adresse DNS qui correspond à l'adresse IP du serveur DNS actuel du terminal. Pour que les critères soient satisfaits, toutes les adresses IP répertoriées du terminal doivent être entrées. Vous pouvez effectuer la mise en correspondance avec un seul caractère générique (17.*).

8 Vous pouvez également choisir l'option existante **VPN à la demande** :

Paramètre	Description
Domaine ou hôte	Action à la demande ■ **Établir si nécessaire** ou **Toujours établir** – Établit une connexion VPN uniquement si la page indiquée n'est pas accessible directement. ■ **Ne jamais établir** – N'établit pas de connexion VPN pour les adresses correspondant au domaine indiqué. Cependant, si un VPN est déjà actif, celui-ci peut être utilisé.

9 Utilisez l'icône **+** pour ajouter d'autres **Règles** et **Paramètres d'action** si nécessaire.

10 Choisissez un type de **Proxy** :

Paramètre	Description
Proxy	Sélectionnez le type de proxy M**anuel** ou A**utomatique** pour configurer cette connexion VPN.
Serveur	Saisissez l'URL du serveur proxy.
Port	Saisissez le port utilisé pour communiquer avec le proxy.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour vous connecter au serveur proxy.
Mot de passe	Saisissez le mot de passe pour vous authentifier.

11 Effectuez les **Configurations du fournisseur**. Ces valeurs sont propres à chaque fournisseur VPN.

Paramètre	Description
Clés du fournisseur	Sélectionnez cette option pour créer des clés personnalisées à ajouter au dictionnaire de configuration du fournisseur.
Clé	Saisissez la clé spécifique fournie par le fournisseur.
Valeur	Saisissez la valeur VPN pour chaque clé.

12 Cliquez sur **Enregistrer et publier**. Une fois le profil installé sur le terminal d'un utilisateur, une invite de connexion via le VPN s'affiche automatiquement dès que l'utilisateur navigue vers un site concerné, comme SharePoint.

Configurer un profil VPN par application

Pour les terminaux iOS 7 et versions ultérieures, vous pouvez obliger certaines applications à se connecter via votre VPN d'entreprise. Votre fournisseur VPN doit prendre en charge cette fonctionnalité et vous devez publier les applications en tant qu'applications gérées.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base > Profils> Ajouter** et sélectionnez **iOS**.

2 Sélectionnez la section de configuration **VPN** dans la liste.

3 Configurez votre Configurer un profil VPN (Virtual Private Network) en conséquence.

4 Cliquez sur **VPN par application** afin de générer un UUID de VPN pour les paramètres du profil VPN. L'UUID de VPN est un identifiant unique propre à cette configuration de VPN spécifique.

5 Sélectionnez **Se connecter automatiquement** pour afficher les zones de texte des **Domaines pour Safari** ; ces sites internes déclenchent une connexion VPN automatique.

6 Choisissez un **Type de fournisseur** afin de déterminer le mode de transmission du trafic par tunnel, par l'intermédiaire d'une couche d'applications ou d'une couche IP.

7 Cliquez sur **Enregistrer et publier**.

Si cet enregistrement a été réalisé en tant que mise à jour d'un profil VPN existant, les applications et terminaux existants utilisant actuellement le profil sont mis à jour. Les terminaux et applications n'utilisant aucun UUID de VPN sont également mis à jour pour utiliser le profil VPN.

Configurer des applications publiques pour utiliser le profil par application

Après avoir créé un profil de tunnel par application, vous pouvez l'attribuer à des applications spécifiques dans l'écran de configuration des applications. Cela indique à cette application qu'elle doit utiliser le profil VPN défini lors de l'établissement de connexions.

Procédure

1 Accédez à **Ressources > Applications > Natives**.

2 Cliquez sur l'onglet **Publics/Publiques**.

3 Sélectionnez **Ajouter une application** pour ajouter une application ou **Modifier** pour modifier une application existante.

4 Sous l'onglet Déploiement, sélectionnez **Utiliser le VPN** et sélectionnez le profil que vous avez créé.

5 Sélectionnez **Enregistrer** et publiez vos modifications.

Étape suivante

Pour plus d'informations sur l'ajout ou la modification d'applications, reportez-vous au guide **Gestion des applications mobiles**.

Configurer des applications internes pour utiliser le profil par application

Après avoir créé un profil de tunnel par application, vous pouvez l'attribuer à des applications spécifiques dans l'écran de configuration des applications. Cela indique à cette application qu'elle doit utiliser le profil VPN défini lors de l'établissement de connexions.

Procédure

1 Accédez à **Ressources > Applications > Natives**.

2 Sélectionnez l'onglet **Interne**.

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

4 Sélectionnez **Enregistrer et attribuer** pour accéder à la page Attribution.

5 Sélectionnez **Ajouter une attribution**, puis **Profil VPN par application** dans la section **Avancé**.

6 **Enregistrez et publiez** l'application.

Étape suivante

Pour plus d'informations sur l'ajout ou la modification d'applications, consultez le guide **Gestion des applications mobiles**, disponible dans la documentation de VMware AirWatch

Configurer un profil de compte de messagerie

Configurez un profil de messagerie pour les terminaux iOS afin de configurer les paramètres de messagerie sur le terminal.

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **E-mail**.
4. Configurez les paramètres de compte de messagerie :

Paramètres	Descriptions
Description du compte	Saisissez une courte description du compte de messagerie.
Type de compte	Utilisez le menu déroulant pour sélectionner IMAP ou POP.
Préfixe du chemin d'accès	Saisissez le nom du dossier racine pour le compte de messagerie (IMAP uniquement).
Nom affiché de l'utilisateur	Saisissez le nom de l'utilisateur.
Adresse e-mail	Saisissez l'adresse e-mail du compte de messagerie.
Empêcher le déplacement des messages	Sélectionnez cette option pour empêcher l'utilisateur de transférer des e-mails ou de les ouvrir dans des applications tierces.
Empêcher la synchronisation des adresses récentes	Sélectionnez cette option pour empêcher l'utilisateur de synchroniser ses contacts dans le terminal personnel.
Empêcher l'utilisation dans des applications tierces	Sélectionnez cette option pour empêcher les utilisateurs de déplacer les e-mails d'entreprise dans d'autres clients de messagerie.
Empêcher le dépôt d'e-mails	Sélectionnez cette option pour empêcher les utilisateurs d'utiliser la fonctionnalité de dépôt d'e-mails d'Apple.
Utiliser S/MIME	Sélectionnez cette option pour utiliser d'autres certificats de chiffrement.
Nom d'hôte	Saisissez le nom du serveur de messagerie.
Port	Indiquez le numéro du port affecté au trafic de messagerie entrant.
Nom d'utilisateur	Saisissez le nom d'utilisateur du compte de messagerie.
Type d'authentification	Utilisez le menu déroulant pour sélectionner le mode d'authentification du détenteur du compte de messagerie.
Mot de passe	Saisissez le mot de passe requis pour authentifier l'utilisateur final.
Utiliser le SSL	Sélectionnez cette option afin d'activer l'utilisation de SSL (Secure Socket Layer) pour le trafic entrant.

Paramètres	Descriptions
Nom d'hôte	Saisissez le nom du serveur de messagerie.
Port	Indiquez le numéro du port affecté au trafic de messagerie sortant.
Nom d'utilisateur	Saisissez le nom d'utilisateur du compte de messagerie.
Type d'authentification	Utilisez le menu déroulant pour sélectionner le mode d'authentification du détenteur du compte de messagerie.
Mot de passe sortant identique au mot de passe entrant	Sélectionnez cette option pour remplir automatiquement la zone de texte du mot de passe.
Mot de passe	Saisissez le mot de passe requis pour authentifier l'utilisateur final.
Utiliser le SSL	Sélectionnez cette option afin d'activer l'utilisation de SSL (Secure Socket Layer) pour le trafic sortant.

Messagerie Exchange ActiveSync (EAS) pour les terminaux iOS

Le protocole standard conçu pour la synchronisation des e-mails sur les terminaux mobiles s'appelle **Exchange ActiveSync (EAS)**. Grâce aux profils EAS, vous pouvez configurer les terminaux à distance afin qu'ils se connectent à votre serveur de messagerie pour synchroniser les e-mails, les calendriers et les contacts.

Le profil EAS utilise les informations de chaque utilisateur, comme le nom d'utilisateur, l'adresse e-mail et le mot de passe. Si vous intégrez Workspace ONE UEM aux services Active Directory, ces informations utilisateur sont remplies automatiquement et peuvent être indiquées dans le profil EAS par l'utilisation de valeurs de recherche.

Création d'un profil EAS générique pour plusieurs utilisateurs

Avant de créer un profil EAS qui permettra aux terminaux de récupérer automatiquement des données depuis le serveur de messagerie, vous devez d'abord vous assurer que les utilisateurs disposent des informations nécessaires dans les données de leur compte utilisateur. Pour les **utilisateurs de l'annuaire** ou bien pour ceux qui s'enrôlent avec leurs identifiants d'annuaire comme Active Directory, les informations seront automatiquement saisies pendant l'enrôlement. Toutefois, pour les **utilisateurs basiques**, ces informations ne sont pas fournies automatiquement et doivent être renseignées via l'une des deux méthodes suivantes :

- Vous pouvez modifier les données de chaque utilisateur, et renseigner les champs **Adresse e-mail** et **Nom d'utilisateur de messagerie**.
- Pour inviter les utilisateurs à saisir ces informations au cours de l'enrôlement, naviguez vers **Terminaux > Paramètres des terminaux > Général > Enrôlement**, puis sous l'onglet **Invite facultative**, cochez la case **Activer la demande de l'e-mail d'enrôlement**.

Configurer un profil de messagerie EAS pour le client de messagerie natif

Créez un profil de configuration des e-mails pour le client de messagerie natif sur des terminaux iOS.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter.** Sélectionnez **Apple iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **Exchange ActiveSync**.
4. Sélectionnez **Client de messagerie natif** en tant que **Client de messagerie**. Complétez la zone de texte **Nom du compte** avec la description de ce compte de messagerie. Remplissez le champ **Hôte Exchange ActiveSync** avec l'URL externe du serveur ActiveSync de votre entreprise.

   Le serveur ActiveSync peut être n'importe quel serveur de messagerie utilisant le protocole ActiveSync, comme IBM Notes Traveler, Novell Data Synchronizer et Microsoft Exchange. Dans le cas des déploiements Secure Email Gateway (SEG), utilisez l'URL de la SEG et non l'URL du serveur de messagerie.
5. Cochez la case **Utiliser SSL** afin d'activer l'utilisation de SSL (Secure Socket Layer) pour le trafic de messagerie entrant.
6. Cochez la case **S/MIME** pour utiliser d'autres certificats de chiffrement. Avant d'activer cette option, vérifiez que vous avez importé les certificats nécessaires dans les paramètres de profil **Identifiants**.
   a. Sélectionnez le **certificat S/MIME** pour signer les messages des e-mails.
   b. Sélectionnez le **certificat de chiffrement S/MIME** pour signer et chiffrer les messages des e-mails.
   c. Activez l'option **Par message** pour permettre aux utilisateurs de choisir les messages qu'ils souhaitent signer et chiffrer en utilisant le client de messagerie natif iOS (iOS 8 et versions ultérieures supervisées uniquement).
7. Cochez la case **Utiliser OAuth** pour inclure la connexion et l'URL du jeton.
   a. **URL de connexion à OAuth** : entrez l'URL de connexion à OAuth.
   b. **URL du jeton OAuth** : entrez l'URL du jeton OAuth.
8. Remplissez les **Informations de connexion** (**Nom de domaine, Nom d'utilisateur et Adresse e-mail**) à l'aide des valeurs de recherche. Les valeurs de recherche viennent directement de l'enregistrement du compte utilisateur. Pour utiliser les valeurs de recherche {EmailUserName} et {EmailDomain}, assurez-vous que les comptes utilisateur Workspace ONE UEM disposent d'une adresse e-mail et d'un nom d'utilisateur de messagerie définis.

9 Laissez le champ **Mot de passe** vide pour demander à l'utilisateur de saisir son propre mot de passe.

10 Sélectionnez **Certificat de section de configuration** pour définir un certificat pour l'authentification basée sur les certificats une fois que le certificat est ajouté à la section de configuration **Identifiants**.

11 Configurez les **paramètres et sécurité** facultatifs suivants, si nécessaire :

a **Synchronisation des e-mails depuis** – Télécharge le nombre de messages défini. Notez qu'une longue période de temps entrainera une consommation des données plus importante lors du téléchargement des messages.

b **Empêcher le déplacement des messages** – Désactive le déplacement des e-mails depuis une boîte e-mail Exchange vers une autre boîte e-mail du terminal.

c **Empêcher l'utilisation dans des applications tierces** – Interdit les autres applications d'utiliser la boîte aux lettres Exchange pour envoyer des messages.

d **Empêcher la synchronisation des adresses récentes** – Désactive les suggestions de contacts lors de l'envoi d'e-mails dans Exchange.

e **Empêcher le dépôt d'e-mails** – Désactive la fonctionnalité de dépôt de courrier d'Apple.

f (iOS 13) **Activer la messagerie** – Active la configuration d'une application de messagerie distincte pour le compte Exchange.

g (iOS 13) **Autoriser le basculement de la messagerie** – Si désactivé, empêche l'utilisateur d'activer ou de désactiver la messagerie.

h (iOS 13) **Activer les contacts** – Active la configuration d'une application de contacts distincte pour le compte Exchange.

i (iOS 13) **Autoriser le basculement des contacts** – Si désactivé, empêche l'utilisateur d'activer ou de désactiver les contacts.

j (iOS 13) **Activer les calendriers** – Active la configuration d'une application de calendrier distincte pour le compte Exchange.

k (iOS 13) **Autoriser le basculement des calendriers** – Si désactivé, empêche l'utilisateur d'activer ou de désactiver les calendriers.

l **Activer les notes** – Active la configuration d'une application de notes distincte pour le compte Exchange.

m (iOS 13) **Autoriser le basculement des notes** – Si désactivé, empêche l'utilisateur d'activer ou de désactiver les notes.

n (iOS 13) **Activer les rappels** – Active la configuration d'une application de rappels distincte pour le compte Exchange

o (iOS 13) **Autoriser le basculement des rappels** – Si désactivé, empêche l'utilisateur d'activer ou de désactiver les rappels.

12 Attribuez une **Application d'appel audio par défaut** que votre compte EAS natif utilisera pour passer des appels lorsque vous sélectionnerez un numéro de téléphone dans un e-mail.

13 Sélectionnez **Enregistrer et publier** pour envoyer le profil vers les terminaux disponibles.

Configurer un profil de notifications

Utilisez ce profil afin d'autoriser des applications spécifiques à apparaître dans l'écran d'accueil lorsqu'il est verrouillé.

Contrôlez le moment et l'endroit d'affichage des notifications. Ce profil s'applique aux terminaux iOS 9.3 + mode Supervisé.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Affichage en liste** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Notifications** dans la liste.

4 Choisissez **Sélectionner l'application.** Une nouvelle fenêtre s'affiche.

Paramètre	Description
Sélectionner l'application	Choisissez l'application que vous souhaitez configurer.
Autoriser les notifications	Sélectionnez cette option si vous souhaitez autoriser des notifications.
Afficher dans le centre de notifications	Sélectionnez cette option si vous souhaitez autoriser les notifications à s'afficher dans le centre de notifications.
Afficher sur l'écran de verrouillage	Sélectionnez cette option si vous souhaitez autoriser les notifications à s'afficher dans l'écran de verrouillage.
Autoriser le son	Sélectionnez cette option si vous souhaitez autoriser l'émission d'un son avec la notification.
Autoriser la création de badges	Sélectionnez cette option si vous souhaitez autoriser l'affichage des badges dans l'icône d'application.
Type d'alerte quand le terminal est déverrouillé	Choisissez le style de notification lorsque le terminal est déverrouillé : ■ **Bannière** – Une bannière s'affiche en travers de l'écran d'accueil pour alerter l'utilisateur. ■ **Alerte modale** – Une fenêtre s'affiche sur l'écran d'accueil. L'utilisateur doit interagir avec la fenêtre avant de continuer.

5 Sélectionnez **Enregistrer** pour envoyer la section de configuration au terminal.

Configurer un profil de paramètres LDAP

Configurez un profil LDAP afin d'autoriser les utilisateurs à accéder aux informations sur les répertoires LDAPv3 de votre entreprise et à les intégrer.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS.**

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **LDAP**.

4 Configurez les paramètres LDAP :

Paramètre	Description
Description du compte	Saisissez une courte description du compte LDAP.
Nom d'hôte du compte	Saisissez/Affichez le nom du serveur pour l'utilisation d'Active Directory.
Nom d'utilisateur du compte	Saisissez le nom d'utilisateur pour le compte Active Directory.
Mot de passe du compte	Saisissez le mot de passe pour le compte Active Directory.
Utiliser le SSL	Cochez cette case pour activer l'utilisation de la sécurité SSL (Secure Socket Layer).
Paramètres de recherche	Entrez les paramètres des recherches Active Directory effectuées depuis le terminal.

5 Sélectionnez **Enregistrer et publier**.

Configurer un profil CalDAV ou CardDAV

Déployez un profil CalDAV ou CardDAV afin d'autoriser les utilisateurs à synchroniser respectivement les éléments de calendrier et les contacts de l'entreprise.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **CalDAV ou CardDAV**.

4 Configurez les paramètres **CalDAV** ou **CardDAV**, notamment :

Paramètre	Description
Description du compte	Saisissez une courte description du compte.
Nom d'hôte du compte	Saisissez/Affichez le nom du serveur pour l'utilisation de CalDAV.
Port	Saisissez le numéro du port attribué pour la communication avec le serveur CalDAV.
URL principale	Saisissez l'emplacement Web du serveur CalDAV.
Nom d'utilisateur du compte	Saisissez le nom d'utilisateur pour le compte Active Directory.

Paramètre	Description
Mot de passe du compte	Saisissez le mot de passe pour le compte Active Directory.
Utiliser le SSL	Sélectionnez cette option pour activer l'utilisation de la sécurité SSL (Secure Socket Layer).

5 Sélectionnez **Enregistrer et publier**.

Configurer un profil d'abonnements aux calendriers

Envoyez à vos terminaux iOS des abonnements aux calendriers à l'aide de l'application de calendrier native dans macOS en configurant cette section de configuration.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Abonnements aux calendriers**.

4 Configurez les paramètres de calendrier :

Paramètre	Description
Description	Saisissez une courte description des abonnements aux calendriers.
URL	Saisissez l'URL du calendrier auquel vous vous inscrivez.
Nom d'utilisateur	Saisissez le nom de l'utilisateur à des fins d'authentification.
Mot de passe	Saisissez le mot de passe à des fins d'authentification.
Utiliser le SSL	Cochez cette case pour envoyer tout le trafic par SSL.

5 Sélectionnez **Enregistrer et publier**.

Configurer un profil Raccourcis Internet

Les raccourcis Internet sont des signets que vous pouvez envoyer vers les terminaux et qui s'afficheront comme des icônes sur l'écran d'accueil du terminal ou dans votre catalogue d'applications.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Raccourcis Internet** dans la liste.

4 Configurez les paramètres **Raccourcis Internet** :

Paramètre	Description
Libellé	Saisissez le texte affiché sous l'icône du raccourci Internet sur le terminal d'un utilisateur. Par exemple : « Portail en libre-service d'AirWatch ».
URL	Saisissez l'URL du raccourci Internet qui s'affiche. Voici quelques exemples de pages Workspace ONE UEM : ■ Pour le SSP, utilisez : https://<Airwatch Environment>/mydevice/ ■ Pour le catalogue d'applications, utilisez : https://<Environment>/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform} ■ Pour le catalogue de livres, utilisez : https://<Environment>/Catalog/BookCatalog?uid={DeviceUUID}
Supprimable	Autorisez les utilisateurs des terminaux à utiliser la fonctionnalité d'appui long pour supprimer des raccourcis internet.
Icône	Sélectionnez cette option pour l'importation comme icône de raccourci Internet. Importez une icône personnalisée, au format .gif, .jpg ou .png, pour l'application. Pour de meilleurs résultats, choisissez une image carrée de 400 pixels maximum de côté et de moins d'1 Mo lorsqu'elle n'est pas compressée. L'image sera automatiquement ajustée et rognée, puis convertie au format png. Les icônes des raccourcis Internet mesurent 104 x 104 pixels pour les terminaux dotés d'un écran Retina ou 57 x 57 pixels pour tous les autres terminaux.
Icône précomposée	Sélectionnez cette option pour afficher l'icône sans effets visuels.
Plein écran	Sélectionnez cette option pour exécuter la page Web en mode plein écran.

5 Cliquez sur **Enregistrer et publier**.

Configurer un profil Identifiants/SCEP

Même si vous protégez votre messagerie, votre Wi-Fi, votre VPN et vos autres connexions d'entreprise à l'aide de codes d'accès et d'autres restrictions, votre infrastructure peut rester vulnérable aux attaques par force brute et par dictionnaire, ainsi qu'aux erreurs humaines. Pour une sécurité renforcée, vous pouvez mettre en place des certificats numériques qui protégeront vos actifs professionnels.

Pour attribuer des certificats, vous devez d'abord définir une autorité de certification. Configurez ensuite une section de configuration **Identifiants** avec votre section de configuration **Exchange ActiveSync (EAS)**, **Wi-Fi** ou **VPN**. Chacune de ces sections de configuration dispose de paramètres permettant d'associer l'autorité de certification définie dans la section de configuration **Identifiants**.

Pour envoyer des certificats vers des terminaux, vous devez configurer une section de configuration **Identifiants** ou **SCEP** dans le cadre des profils que vous avez créés pour les paramètres EAS, Wi-Fi et VPN. Suivez les instructions ci-dessous pour un profil activé par certificat :

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **iOS** dans la liste des plateformes.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **EAS**, **Wi-Fi** ou **VPN** à configurer. Complétez les informations nécessaires, en fonction de la section de configuration que vous avez sélectionnée.
4. Sélectionnez la section de configuration **Identifiants** (ou **SCEP**).
5. Choisissez une option du menu **Source des identifiants** :
   a. Choisissez d'**importer** un certificat et saisissez le **nom du certificat**.
   b. Choisissez **Autorité de certification définie** et sélectionnez les options **Autorité de certification** et **Modèle de certificat** appropriées.
   c. Choisissez **Certificat utilisateur** et l'utilisation prévue du certificat **S/MIME**.
   d. Choisissez la valeur **Identifiants dérivés** et sélectionnez l'**utilisation de la clé** appropriée selon la manière dont le certificat est utilisé. Voici les options d'utilisation de la clé disponibles : **Authentification**, **Signature** et **Chiffrement**.
6. Revenez à la section de configuration **EAS**, **Wi-Fi** ou **VPN** précédente.
7. Spécifiez le Certificat d'identité dans la section de configuration :
   a. **EAS** – Sélectionnez le **Certificat de section de configuration** dans Informations de connexion.
   b. **Wi-Fi** – Sélectionnez un **Type de sécurité** compatible (WEP d'entreprise, WPA/WPA2 d'entreprise ou Tous [professionnels]) et sélectionnez le **Certificat d'identité** dans la section Authentification.
   c. **VPN** – Sélectionnez un **Type de connexion** compatible (par exemple, CISCO AnyConnect, F5 SSL) et sélectionnez **Certificat** dans la liste déroulante Authentification de l'utilisateur. Sélectionnez **Certificat d'identité**.
8. Revenez à la section de configuration **Identifiants** (ou **SCEP**).
9. Configurez les paramètres restants, puis sélectionnez **Enregistrer et publier**.

Configurer un profil de proxy HTTP global

Configurez un proxy HTTP global qui dirige tout le trafic HTTP des terminaux iOS 7 (et versions ultérieures) supervisés vers un serveur proxy défini. Par exemple, une école peut définir un proxy global pour s'assurer que l'ensemble de la navigation Internet passe par son filtre de contenu Web.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez dans la liste la section de configuration **Proxy HTTP global**.

4 Configurez les paramètres du proxy :

Paramètre	Description
Type de proxy	Choisissez **Auto** ou **Manuel** comme configuration du proxy.
Serveur proxy	Saisissez l'URL du serveur proxy. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Manuel**.
Port du serveur proxy	Saisissez le port utilisé pour communiquer avec le proxy. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Manuel**.
Nom d'utilisateur/Mot de passe du proxy	Si le proxy nécessite des identifiants, vous pouvez utiliser des valeurs de recherche pour définir la méthode d'authentification. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Manuel**.
Autoriser le contournement du proxy pour accéder aux réseaux captifs	Cochez cette case pour permettre au terminal de contourner les paramètres du proxy afin d'accéder à un réseau connu. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Manuel**.
URL du fichier PAC du proxy	Entrez l'URL du fichier PAC du proxy pour appliquer automatiquement ses paramètres. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Auto**.
Autoriser la connexion directe si le PAC est inaccessible	Sélectionnez cette option pour permettre aux terminaux iOS de contourner le serveur proxy si le fichier PAC est inaccessible. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Auto**.
Autoriser le contournement du proxy pour accéder aux réseaux captifs	Cochez cette case pour permettre au terminal de contourner les paramètres du proxy afin d'accéder à un réseau connu. Cette zone de texte s'affiche lorsque le **Type de proxy** est défini sur **Auto**.

5 Cliquez sur **Enregistrer et publier**.

Configurer un profil Mode d’application unique

Utilisez le mode d'application unique pour provisionner des terminaux afin qu'ils ne puissent accéder qu'à une seule application de leur choix. Le mode d'application unique désactive le bouton d'accueil et force le terminal à démarrer directement dans l'application souhaitée si l'utilisateur tente un redémarrage manuel.

Conditions préalables

Cette fonctionnalité permet de s'assurer que le terminal n'est pas utilisé pour quoi que ce soit en dehors de l'application définie et qu'il n'a aucun moyen d'accéder à d'autres applications indésirables, aux paramètres du terminal ou à un navigateur Internet. Cette fonctionnalité est utile pour les restaurants et les magasins de vente au détail. Pour le secteur de l'éducation, les élèves peuvent utiliser des terminaux dont l'accès est verrouillé sur un seul jeu, eBook ou exercice.

- Un terminal iOS 7 ou version ultérieure configuré en mode Supervisé. (La version iOS 7, ou une version ultérieure, est requise pour des options supplémentaires et le mode d'application unique autonome.)

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** >**Profils** > **Ajouter.** Sélectionnez **Apple iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **Mode d'application unique**.
4. Configurez les paramètres du mode d'application unique :

Paramètre	Description
Type de filtre	Choisissez un filtre, **Limiter le terminal à une seule application** ou **Applications autorisées pour le mode autonome d'application unique** : ■ **Limiter le terminal à une seule application** – Verrouillez les terminaux dans une seule application publique, interne, achetée ou native, jusqu'à ce que le profil contenant cette section de configuration soit supprimé. Le bouton d'accueil est désactivé et le terminal démarre toujours sur l'application indiquée, après une mise en veille ou un redémarrage. ■ **Applications autorisées pour le mode autonome d'application unique** – Autorisez les applications en liste blanche à déclencher un mode d'application unique en fonction d'un événement qui contrôle le moment d'activation et de désactivation du mode d'application unique sur le terminal. Cette action se produit dans l'application proprement dite, conformément aux indications du développeur de l'application.
ID de l'offre groupée d'applications	Saisissez l'ID de l'offre groupée ou sélectionnez-en un dans le menu déroulant. L'ID de l'offre groupée apparaît dans le menu déroulant une fois que l'application est importée dans UEM Console. Par exemple : **com.air-watch.secure.browser**.
Paramètres facultatifs	Choisissez des paramètres facultatifs pour les terminaux iOS 7 et versions ultérieures supervisés.

5. Cliquez sur **Enregistrer et publier**. Chaque terminal équipé de ce profil passe en mode d'application unique.

Redémarrer un terminal fonctionnant en mode d'application unique

La procédure de réinitialisation matérielle est utilisée pour redémarrer un terminal fonctionnant en mode d'application unique.

Procédure

1 Appuyez simultanément sur le bouton d'accueil et le bouton de mise en veille et maintenez-les enfoncés.

2 Maintenez ces boutons enfoncés jusqu'à ce que le terminal s'éteigne et redémarre.

3 Relâchez-les lorsque le logo Apple argenté apparaît. Le terminal peut mettre quelques minutes à charger l'écran d'accueil depuis la page du logo Apple.

Quitter le mode d'application unique sur les terminaux iOS

Les utilisateurs ne peuvent pas quitter l'application lorsque le mode d'application unique est activé. Workspace ONE UEM fournit deux options permettant de quitter le mode d'application unique, en fonction du mode d'application unique que vous activez.

Vous pouvez désactiver temporairement le mode d'application unique si vous souhaitez mettre à jour l'application en question vers une nouvelle version. Suivez les instructions ci-dessous, installez la nouvelle version de l'application et réactivez le mode d'application unique.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils**. Dans la ligne du profil Mode d'application unique, sélectionnez l'icône **Voir les terminaux**.

2 En regard du terminal pour lequel vous souhaitez supprimer ce paramètre, sélectionnez **Supprimer le profil**.

3 Mettez l'application à jour vers la version souhaitée.

4 Réinstallez le profil en suivant les étapes de la section Configurer un profil Mode d'application unique.

Autoriser l'administrateur des terminaux à quitter le mode d'application unique depuis le terminal

Vous pouvez autoriser un administrateur à quitter le mode d'application unique à l'aide d'un code d'accès sur le terminal proprement dit. Cette option n'est disponible que si vous activez le mode d'application unique en tant que **Type de filtre** pour le profil du mode d'application unique.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter.** Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Mode d'application unique**.

4 Après avoir sélectionné l'option **Applications autorisées pour le mode autonome d'application unique**, saisissez l'ID de bundle d'une application qui prend en charge le mode autonome d'application unique sous **Applications autorisées**.

5 Sélectionnez **Enregistrer et publier** pour envoyer le profil aux terminaux attribués.

6 Accédez à **Ressources** > **Applications** > **Natives** > **Publiques** pour les applications publiques ou à **Ressources** > **Applications** > **Natives** > **Achetées** pour les applications gérées au moyen de VPP.

7 Localisez l'application prise en charge pour le mode autonome d'application unique et sélectionnez l'**icône Modifier l'attribution**. La fenêtre Modifier l'application s'affiche.

8 Sélectionnez l'onglet **Attribution** et ouvrez la section **Politiques**.

9 Sélectionnez **Activé** pour **Envoyer la configuration de l'application**, saisissez **AdminPasscode** en tant que **Clé de configuration**, puis définissez le **Type de valeur** sur **Chaîne**.

10 Saisissez le code d'accès qu'utilisent les administrateurs pour quitter le mode d'application unique en tant que **Valeur de configuration**. La valeur peut être numérique ou alphanumérique. Sélectionnez **Ajouter**.

11 Sélectionnez **Enregistrer et publier** pour envoyer la configuration d'application.

Configurer un profil de filtrage de contenu Web

Vous pouvez autoriser ou empêcher les utilisateurs d'accéder à certaines URL depuis un navigateur Web en configurant une section de configuration Filtre de contenu Web appliquée aux terminaux. Toutes les URL doivent commencer par http:// ou https://. Si nécessaire, vous devez créer des entrées séparées pour les versions HTTP et HTTPS d'une même URL. La section de configuration Filtre de contenu Web n'est applicable qu'à des terminaux iOS 7 (et versions ultérieures) supervisés.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter.** Sélectionnez **iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Filtre du contenu**.

4 Sélectionnez le menu déroulant **Type de filtre** :

   a Intégré : Autoriser les sites Web

   b Intégré : Refuser les sites Web

   c Plug-ins

Intégré : Autoriser les sites Web

Configurez une liste blanche d'URL afin d'autoriser les utilisateurs à accéder uniquement aux sites Web spécifiques figurant sur la liste et les empêcher d'accéder à d'autres sites Web.

Procédure

1 Sélectionnez **Intégré : Autoriser les URL** dans le menu déroulant **Type de filtre** pour choisir les plug-ins qui sont accessibles.

2 Sélectionnez **Ajouter** et configurez la liste des sites Web autorisés :

Paramètre	Description
URL autorisées	URL d'un site figurant dans la liste blanche.
Titre	Titre du signet.
Chemin d'accès au signet	Dossier dans lequel le signet sera ajouté dans Safari.

Intégré : Refuser les sites Web

Configurez une liste noire d'URL afin d'empêcher les utilisateurs d'accéder aux sites Web spécifiés. Toutefois, tous les autres sites Web restent disponibles pour les utilisateurs. Par ailleurs, les sites Web comportant des grossièretés sont exclus, sauf si une exception est autorisée.

Procédure

- Sélectionnez **Intégré : Refuser les URL** dans le menu déroulant **Type de filtre** et configurez les sites Web mis en liste noire :

Paramètre	Description
URL sur liste noire	Saisissez des **URL sur liste noire** en les séparant par un retour à la ligne, un espace ou une virgule.
Filtrer automatiquement les sites Web inappropriés	Sélectionnez cette option pour exclure les sites Web pour adultes.
Chemin d'accès au signet	Saisissez le chemin d'accès au dossier dans lequel le signet est ajouté dans Safari.
URL autorisées	Saisissez les sites Web qui peuvent être autorisés en tant qu'exceptions au filtre automatique.

Plug-ins

Cette section de configuration vous permet d'intégrer dans Safari un plug-in tiers de filtrage de contenu Web.

Si vous souhaitez intégrer spécifiquement des filtres de contenu Configurer un profil de filtrage de contenu Forcepoint ou Configurer un profil de filtrage de contenu Blue Coat, consultez les sections correspondantes de ce guide.

Procédure

1 Sélectionnez **Plug-in** dans le menu déroulant **Type de filtre** pour choisir les plug-ins qui sont accessibles. Vous devez activer les besoins en trafic Webkit ou Socket pour que la section de configuration fonctionne.

Paramètre	Description
Nom du filtre	Saisissez le nom du filtre qui s'affiche sur le terminal.
Identifiant	Saisissez l'ID d'offre groupée de l'identifiant du plug-in qui fournit un service de filtrage.
Adresse de service	Saisissez le nom d'hôte, l'adresse IP ou l'URL du service.
Groupe	Choisissez la chaîne d'organisation transmise au plug-in tiers.
Filtrer le trafic WebKit	Sélectionnez cette option pour choisir si vous souhaitez filtrer le trafic Webkit.
Filtrage du trafic Socket	Sélectionnez cette option pour choisir si vous souhaitez filtrer le trafic Socket.

2 Configurez les informations d'**Authentification** :

Paramètre	Description
Nom d'utilisateur	Utilisez les valeurs de recherche pour qu'elles se remplissent automatiquement depuis l'enregistrement de compte utilisateur. Vérifiez qu'une adresse e-mail et un nom d'utilisateur e-mail sont définis pour les comptes utilisateur Workspace ONE UEM.
Mot de passe	Saisissez le mot de passe de ce compte.
Certificat de section de configuration	Choisissez le certificat d'authentification.

3 Ajoutez des **Données personnalisées** qui incluent les clés requises par le service de filtrage tiers. Ces informations intègrent le dictionnaire de configuration du fournisseur.

4 Cliquez sur **Enregistrer et publier**.

Configurer un profil de domaines gérés

Les domaines gérés sont une autre méthode par laquelle Workspace ONE UEM améliore la fonctionnalité de sécurité « Ouvrir dans » d'Apple sur les terminaux iOS 8. L'utilisation de la fonctionnalité de sécurité d'ouverture « Ouvrir dans » avec des domaines gérés vous permet de protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir les documents téléchargés depuis les domaines de l'entreprise à l'aide de Safari.

Spécifiez les URL ou les sous-domaines pour gérer la méthode d'ouverture des documents, des pièces jointes et des téléchargements. Par ailleurs, dans les domaines de messagerie gérés, un indicateur d'avertissement en couleur peut être affiché dans les e-mails envoyés à des domaines non gérés. Ces outils permettent aux utilisateurs de déterminer les documents qui peuvent être ouverts avec des applications de l'entreprise, ainsi que ceux qui sont personnels et peuvent être ouverts dans des applications personnelles.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Affichage en liste** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Domaines gérés** dans la liste.

Paramètre	Description
Domaines de messagerie gérés	Entrez des domaines pour spécifier les adresses e-mail qui sont des domaines d'entreprise. Par exemple : **exchange.acme.com**. Les e-mails envoyés aux adresses non indiquées ici sont mis en surbrillance dans l'application de messagerie afin d'indiquer que l'adresse ne fait pas partie du domaine de l'entreprise.
Domaines Web gérés	Entrez les domaines afin de choisir les URL ou les sous-domaines spécifiques qui peuvent être considérés comme étant gérés. Par exemple : **sharepoint.acme.com**. Tous les documents ou pièces jointes provenant de ces domaines sont considérés comme étant gérés.
Domaines de mot de passe Safari	Saisissez le mot de passe des domaines que Safari doit enregistrer. Cette option s'applique uniquement aux terminaux surveillés.

4 Cliquez sur **Enregistrer et publier**.

Configurer un profil de règles d'utilisation du réseau

Configurez des règles d'utilisation du réseau pour contrôler les applications et les cartes SIM qui peuvent accéder aux données en fonction du type de connexion réseau ou lorsque le terminal est en itinérance. Cette fonctionnalité permet aux administrateurs d'apporter leur aide dans la gestion des charges de données lorsque les employés utilisent les terminaux pour leur travail. Utilisez les contrôles granulaires pour appliquer différentes règles aux terminaux et aux cartes SIM si nécessaire.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Affichage en liste** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Règles d'usage du réseau** dans la liste.

4 Sous Règles d'utilisation de l'application, saisissez l'**Identifiant d'application** de toutes les applications publiques, internes ou achetées.

5 Activez **Autoriser les données cellulaires** et **Utilisation des données en itinérance**. Les deux options sont sélectionnées par défaut.

6 Sous Règles d'utilisation de la carte SIM, fournissez les **ICCID** des cartes SIM (cartes physiques et eSIM) et spécifiez le type de capacité d'**Assistance Wi-Fi**, à savoir **Par défaut** ou **Données mobiles illimitées**.

7 Cliquez sur **Enregistrer et publier**.

Configurer un profil de compte serveur macOS

Ajoutez un compte serveur macOS directement depuis UEM Console afin de gérer votre infrastructure MDM. Utilisez cette option afin de fournir les identifiants visant à autoriser les utilisateurs à accéder au partage de fichiers sur macOS.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Compte serveur macOS** dans la liste.

Paramètre	Description
Description du compte	Saisissez le nom affiché du compte.
Nom d'hôte	Saisissez l'adresse du serveur.
Nom d'utilisateur	Saisissez le nom de connexion de l'utilisateur.
Mot de passe	Saisissez le mot de passe de l'utilisateur.
Port	Désigne le numéro de port à utiliser pour contacter le serveur.

4 Cliquez sur **Enregistrer et publier**.

Configurer un profil d'authentification unique

Activez l’authentification unique pour les applications d’entreprise afin d’autoriser un accès simple, sans authentification requise à chaque application. Envoyez ce profil pour authentifier les utilisateurs par l'intermédiaire de l'authentification Kerberos au lieu du stockage de mots de passe sur les terminaux. Pour plus d'informations sur les paramètres d'authentification unique, reportez-vous au **Guide VMware Workspace ONE UEM de gestion des applications mobiles**.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** et sélectionnez **Apple iOS.**

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Authentification unique**.

4 Entrez les **Informations de connexion** :

Paramètre	Description
Nom du compte	Saisissez le nom qui apparaîtra sur le terminal.
Nom principal pour Kerberos	Saisissez le nom principal pour Kerberos.
Domaine	Saisissez le domaine Kerberos. Ce paramètre doit être indiqué entièrement en majuscules.
Certificat de renouvellement	Sur les terminaux iOS 8 et versions ultérieures, sélectionnez le certificat utilisé pour réauthentifier l'utilisateur automatiquement, sans aucune interaction de sa part, à l'expiration de la session d'authentification unique. Configurez un certificat de renouvellement (par exemple, .pfx) à l'aide de la section de configuration Configurer un profil Identifiants/SCEP.

5 Saisissez les **préfixes d'URL** pour lesquels utiliser ce compte pour l'authentification Kerberos via HTTP. Par exemple : **http://sharepoint.acme.com/**. Si ce champ est laissé vide, le compte sera utilisé pour toutes les URL HTTP et HTTPS.

6 Saisissez l'**ID de l'offre groupée d'applications** ou sélectionnez-en un dans le menu déroulant. L'ID de l'offre groupée apparaît dans le menu déroulant une fois que l'application est importée dans UEM Console. Par exemple : **com.air-watch.secure.browser**. Les applications spécifiées doivent prendre en charge l'authentification Kerberos.

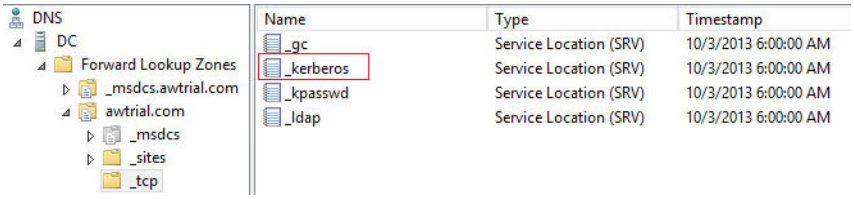
7 Cliquez sur **Enregistrer et publier**.

Exemple

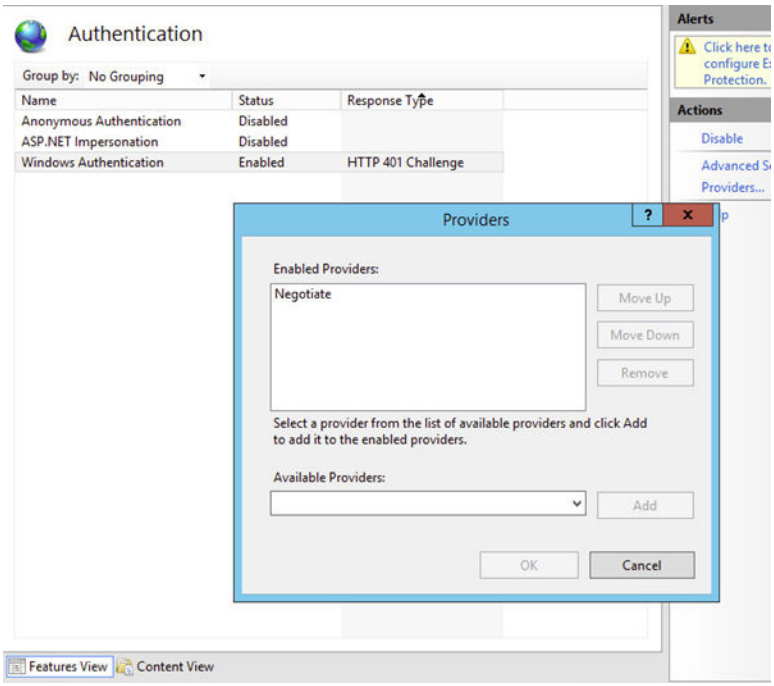
Dans l'exemple d'un navigateur Web, lorsque les utilisateurs accèdent à un site Web spécifié dans la section de configuration, ils sont invités à saisir le mot de passe de leur compte de domaine. Par la suite, ils n'ont plus à ressaisir les identifiants pour accéder à l'un des sites Web spécifiés dans la section de configuration.

Note

- Avec l'authentification Kerberos, les terminaux doivent être connectés au réseau d'entreprise (par Wi-Fi ou VPN d'entreprise).
- Le serveur DNS doit avoir un enregistrement des services Kerberos (serveur KDC).



- L'application sur le terminal mobile et le site Web doivent tous deux prendre en charge l'authentification Kerberos/Negotiate.



Configurer un profil d'extension SSO

Pour configurer une application sur un terminal afin d'effectuer une authentification unique (SSO) avec l'extension Kerberos, configurez le profil d'extension SSO. Le profil d'extension SSO évite aux utilisateurs d'avoir à renseigner leur nom d'utilisateur et leur mot de passe pour accéder à des URL spécifiques. Ce profil s'applique uniquement aux terminaux iOS 13 et versions ultérieures.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter** > **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la charge utile **Extension SSO**.

4 Configurez les paramètres du profil.

Paramètre	Description
Type d'extension	Sélectionnez le type d'extension SSO de l'application. Si vous choisissez le type Générique, indiquez dans le champ **Identifiant d'extension** l'ID de bundle de l'extension d'application qui exécute la SSO pour les URL spécifiées. Si vous sélectionnez Kerberos, spécifiez les domaines Active Directory.
Type	Sélectionnez Informations d'identification ou Redirection comme type d'extension. L'extension Informations d'identification est utilisée pour l'authentification par stimulation/réponse. L'extension Redirection prend en charge les authentifications OpenID Connect, OAuth et SAML.
Identifiant d'équipe	Entrez l'identifiant d'équipe de l'extension d'application qui exécute la SSO pour les URL spécifiées.
URL	Entrez un ou plusieurs préfixes d'URL de fournisseurs d'identité dans lesquels l'extension d'application exécute la SSO.
Paramètres supplémentaires	Entrez les paramètres supplémentaires du profil dans le code XML qui est ajouté au nœud ExtensionData.
Domaine Active Directory	Cette option s'affiche uniquement si Kerberos est sélectionné comme type d'extension. Entrez le nom du domaine Kerberos.
Domaines	Entrez les noms d'hôte ou les noms de domaine pouvant être authentifiés via l'extension d'application.
Utiliser la détection automatique de site	Activez cette option pour que l'extension Kerberos utilise automatiquement LDAP et DNS pour déterminer le nom du site Active Directory.
Autoriser la connexion automatique	Activez cette option pour permettre l'enregistrement des mots de passe dans le trousseau d'accès.
Demander un ID utilisateur tactile ou un mot de passe	Activez cette option pour permettre à l'utilisateur de fournir un ID tactile, un ID de reconnaissance faciale ou un code secret pour accéder à l'entrée du trousseau d'accès.
Certificat	Sélectionnez le certificat à transférer au terminal qui se trouve dans le même profil MDM.
ID de bundle autorisés	Entrez une liste d'ID de bundle d'applications pour autoriser l'accès au ticket d'attribution de ticket (TGT) de Kerberos.

5 Sélectionnez **Enregistrer et publier**.

Configurer un profil de liste blanche AirPlay

La configuration de la section de configuration AirPlay vous permet de placer sur liste blanche un ensemble spécifique de terminaux destinés à recevoir des privilèges de diffusion selon l'ID du terminal. Par ailleurs, si l'accès à l'écran de votre terminal Apple TV est protégé par mot de passe, présaisissez le mot de passe pour établir une connexion réussie sans révéler le code PIN aux tiers non autorisés.

Cette section de configuration fonctionnera même si vous n'enrôlez pas vos terminaux Apple TV avec Workspace ONE UEM. Pour plus d'informations sur les capacités de tvOS, reportez-vous au guide **tvOS Management** .

Note la mise en liste blanche d'AirPlay n'est actuellement disponible que sur les terminaux iOS 7 et iOS 8 supervisés.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Choisissez **Apple iOS** dans la liste des plateformes.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez l'onglet de la section de configuration **Mise en miroir AirPlay**.

4 Configurez les paramètres **Mots de passe** pour les terminaux iOS 7 et **Listes blanches** pour les terminaux iOS 7 supervisés :

Paramètre	Description
Nom du terminal	Entrez le nom du terminal de la destination AirPlay.
Mot de passe	Saisissez le mot de passe de la destination AirPlay. Sélectionnez **Ajouter** pour inclure d'autres terminaux mis en liste blanche.
Nom d'affichage	Saisissez le nom affiché de la destination. Le nom doit correspondre à celui du terminal tvOS et est sensible à la casse. Le nom du terminal est disponible dans les paramètres du terminal tvOS. (iOS 7 + mode Supervisé)
ID du terminal	Saisissez l'ID du terminal (incluez l'adresse MAC ou l'adresse Ethernet au format XX:XX:XX:XX:XX:XX) pour l'affichage de destination. Sélectionnez **Ajouter** pour inclure d'autres terminaux mis en liste blanche. (iOS 7 + mode Supervisé)

5 Maintenant que la liste blanche de destination d'AirPlay est établie pour les terminaux iOS 7 supervisés, utilisez le panneau de configuration du terminal pour activer ou désactiver AirPlay manuellement :

   a Naviguez vers **Terminaux > Affichage en liste** et localisez le terminal auquel AirPlay est destiné, puis sélectionnez le nom convivial du terminal.

   b Sélectionnez **Support**, puis **Démarrer Airplay** dans la liste des options de support.

c Choisissez la **Destination** créée dans le profil AirPlay, saisissez le **Mot de passe** si nécessaire, puis sélectionnez la **Durée de l'analyse**. Vous pouvez également sélectionner **Personnaliser** dans la liste Destination afin de créer une destination personnalisée pour ce terminal particulier.

d Sélectionnez **Enregistrer** et acceptez l'invite d'activation d'AirPlay.

6 Pour désactiver AirPlay manuellement sur le terminal, revenez au panneau de configuration du terminal, puis sélectionnez **Support** et **Arrêter AirPlay**.

Configurer le profil AirPrint

Configurez une section de configuration AirPrint pour les terminaux Apple pour autoriser les ordinateurs à détecter automatiquement une imprimante AirPrint, même si le terminal se situe sur un autre sous-réseau que l'imprimante AirPrint.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Affichage en liste** > **Ajouter** et ajoutez la plateforme appropriée. Si vous sélectionnez Apple macOS, indiquez si ce profil s'applique uniquement à l'utilisateur d'enrôlement sur le terminal (**Profil d'utilisateur**) ou à l'intégralité du terminal (**Profils du terminal**).

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez l'onglet de la section de configuration **AirPrint**.

Paramètre	Description
Adresse IP	Saisissez l'adresse IP (XXX.XXX.XXX.XXX).
Chemin d'accès à la ressource	Saisissez le chemin d'accès à la ressource (ipp/printer or printers/Canon_MG5300_series) associé à l'imprimante AirPrint. Pour trouver le chemin d'accès à la ressource et les informations d'adresse IP d'une imprimante, reportez-vous à la section Récupérer les informations de l'imprimante AirPrint.

4 Cliquez sur **Enregistrer et publier**.

Récupérer les informations de l'imprimante AirPrint

Pour connaître les informations de l'imprimante AirPrint, telles que l'adresse IP et le chemin d'accès aux ressources, suivez la procédure décrite dans cette section.

1 Connectez un terminal iOS au réseau local (sous-réseau) sur lequel se trouvent les imprimantes AirPrint.

2 Ouvrez la fenêtre Terminal (située dans /Applications/Utilitaires/), entrez la commande suivante, puis appuyez sur Retour.

```
ippfind
```

Note Notez les informations de l'imprimante qui sont extraites via la commande. La première partie est le nom de votre imprimante et la dernière partie est le chemin de la ressource.

```
ipp://myprinter.local.:XXX/ipp/portX
```

3 Pour obtenir l'adresse IP, entrez la commande suivante et le nom de votre imprimante.

```
ping myprinter.local.
```

Note Notez les informations de l'adresse IP qui sont extraites via la commande.

```
PING myprinter.local (XX.XX.XX.XX)
```

4 Entrez l'adresse IP (XX.XX.XX.XX) et le chemin de ressource (/ipp/portX) obtenus à partir des étapes 2 et 3 dans les paramètres de charge utile AirPrint.

Configurer un profil de paramètres cellulaires

Configurez une section de configuration Cellulaire pour configurer les paramètres de réseau cellulaire sur les terminaux et déterminez la manière dont le terminal accède au réseau de données cellulaires de l'opérateur.

Envoyez cette section de configuration afin d'utiliser un autre APN depuis le point par défaut. Si les paramètres APN sont incorrects, vous risquez de perdre des fonctionnalités ; vous devez donc vous procurer les paramètres APN corrects auprès de l'opérateur. Pour plus d'informations sur les paramètres cellulaires, consultez cet article de la base de connaissances Apple.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Choisissez une section de configuration **Cellulaire** pour les terminaux iOS 7 et versions ultérieures.

4 Configurez les paramètres de la section de configuration Cellulaire.

Paramètre	Description
Nom du point d'accès (APN)	Saisissez l'APN fourni par votre opérateur (par exemple, come.moto.cellular).
Type d'authentification	Sélectionnez le protocole d'authentification.

Paramètre	Description
Nom d'utilisateur du point d'accès	Saisissez le nom d'utilisateur utilisé pour l'authentification.
Mot de passe du point d'accès APN	Saisissez le mot de passe APN utilisé pour l'authentification.
Nom du point d'accès	Saisissez l'APN fourni par votre opérateur (par exemple, come.moto.cellular).
Nom d'utilisateur du point d'accès	Saisissez le nom d'utilisateur utilisé pour l'authentification.
Type d'authentification	Sélectionnez le protocole d'authentification.
Mot de passe	Saisissez le mot de passe APN utilisé pour l'authentification.
Serveur proxy	Saisissez les détails du serveur proxy.
Port du serveur proxy	Indiquez le port du serveur proxy pour tout le trafic. Sélectionnez **Ajouter** pour continuer ce processus.

5 Sélectionnez **Enregistrer et publier**.

Configurer un profil de mise en page de l'écran d'accueil (iOS Mode supervisé)

Utilisez cette section de configuration pour personnaliser l'écran d'accueil. L'activation de cette fonctionnalité vous permet de regrouper des applications en fonction des besoins de votre organisation.

Lorsque la section de configuration est envoyée au terminal, l'écran d'accueil est verrouillé et les utilisateurs ne peuvent pas modifier votre configuration personnalisée. Cette section de configuration s'applique aux terminaux iOS 9.3 + mode Supervisé.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Affichage en liste** > **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Sélectionnez la section de configuration **Mise en page de l'écran d'accueil** dans la liste.

Paramètre	Description
Dock	Choisissez les applications que vous souhaitez voir apparaître dans le Dock.
Page	Choisissez les applications que vous souhaitez ajouter au terminal. Vous pouvez également ajouter d'autres pages pour d'autres groupes d'applications.
Ajouter un dossier	Configurez un nouveau dossier pour l'ajouter à l'écran du terminal sur la page sélectionnée. ■ Utilisez l'**icône représentant un crayon** qui se trouve dans la barre grise pour créer ou modifier le nom du dossier.

4 Sélectionnez **Ajouter une page** pour ajouter d'autres pages au terminal si nécessaire.

5 Sélectionnez **Enregistrer et publier** pour envoyer le profil aux terminaux.

Créer un profil de message d'écran de verrouillage

Personnalisez l'écran de verrouillage des terminaux de vos utilisateurs finaux avec des informations qui peuvent vous aider à récupérer des terminaux perdus.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** et sélectionnez **Ajouter**. Sélectionnez **Apple iOS**.

2 Configurez les **paramètres généraux** du profil.

3 Configurez le message de l'écran de verrouillage :

Paramètre	Description
Message « En cas de perte, rapportez-moi à »	Affiche un nom ou une organisation à qui renvoyer un terminal trouvé. Ce champ accepte les valeurs de recherche.
Informations de l'étiquette du composant	Affiche les informations de l'étiquette d'inventaire du terminal sur son écran de verrouillage. Cette étiquette d'inventaire peut dupliquer ou remplacer une étiquette d'inventaire physique attachée au terminal. Ce champ accepte les valeurs de recherche.

4 Cliquez sur **Enregistrer et publier**.

Configurer un profil de support de compte Google (iOS)

Autoriser un utilisateur à utiliser son compte Google sur l'application de messagerie native sur le terminal iOS. Ajoutez un compte Google directement depuis UEM Console.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**. Sélectionnez la plateforme **Apple iOS**.

2 Configurez les paramètres du profil de l'onglet **Général**.

3 Configurez les informations du compte utilisateur :

Paramètre	Description
Nom du compte	Nom d'utilisateur complet du compte Google. Il s'agit du nom d'utilisateur qui apparaît lorsque vous envoyez un e-mail.
Description du compte	Description du compte Google qui s'affiche dans Messagerie et Paramètres.
Adresse e-mail	Adresse e-mail Google complète du compte.
Application d'appel audio par défaut	Recherchez et sélectionnez une application qui deviendra l'application par défaut pour passer des appels depuis le compte Google configuré.

4 Cliquez sur **Enregistrer et publier**.

Configurer un profil de paramètres personnalisés

La section de configuration **Paramètres personnalisés** peut être utilisée lorsqu'Apple lance une nouvelle fonctionnalité iOS que Workspace ONE UEM ne prend actuellement pas en charge dans les sections de configuration natives. Si vous ne souhaitez pas attendre la dernière version de Workspace ONE UEM pour contrôler ces paramètres, utilisez la section de configuration **Paramètres personnalisés** et le code XML afin d'activer ou de désactiver certains paramètres manuellement.

Conditions préalables

- Vous souhaiterez peut-être effectuer une copie de votre profil et l'enregistrer dans un groupe organisationnel « test », pour éviter d'affecter les utilisateurs tant que vous n'êtes pas prêt à enregistrer et publier.
- N'attribuez pas de profil à un Smart Group, car cela peut produire une valeur chiffrée lors de l'affichage du XML.

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter** > **Ajouter un profil** > **iOS**.
2. Configurez les paramètres du profil de l'onglet **Général**.
3. Configurez les sections de configuration appropriées (Restrictions ou Code d'accès, par exemple).
4. Sélectionnez **Enregistrer et publier**.

   Note Assurez-vous que le profil créé au cours des étapes 1 à 4 n'est attribué à aucun Smart Group. Dans le cas contraire, les données peuvent être chiffrées lors de l'affichage du XML.

5. Revenez à la page Profils et sélectionnez un profil à l'aide du bouton radio en regard du nom du profil. Les options de menu s'affichent au-dessus de la liste.
6. Sélectionnez **</> XML** dans les options de menu. La fenêtre **Consulter le XML du profil** s'affiche.
7. Trouvez et copiez la section délimitée par <dict> ... </dict>, que vous avez préalablement configurée (par exemple, Restrictions ou Code d'accès). Ce texte contient un type de configuration identifiant l'objectif, par exemple les restrictions. Vous devez copier un contenu de dictionnaire unique dans PayloadContent, comme indiqué dans l'exemple.

```
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>safariAcceptCookies</key>
        <real>2</real>
        <key>safariAllowAutoFill</key>
```

```
        <true />
        <key>PayloadDisplayName</key>
        <string>Restrictions</string>
        <key>PayloadDescription</key>
        <string>RestrictionSettings</string>
        <key>PayloadIdentifier</key>
        <string>745714ad-e006-463d-8bc1-495fc99809d5.Restrictions</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadType</key>
        <string>com.apple.applicationaccess</string>
        <key>PayloadUUID</key>
        <string>9dd56416-dc94-4904-b60a-5518ae05ccde</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
      </dict>
    </array>
    <key>PayloadDescription</key>
    <string></string>
    <key>PayloadDisplayName</key>
    <string>Block Camera/V_1</string>
    <key>PayloadIdentifier</key>
    <string>745714ad-e006-463d-8bc1-495fc99809d5</string>
    <key>PayloadOrganization</key>
    <string></string>
    <key>PayloadRemovalDisallowed</key>
    <false />
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>86a02489-58ff-44ff-8cd0-faad7942f64a</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
  </dict>
</plist>
```

Pour obtenir plus d'exemples et d'informations sur le code XML, reportez-vous à l'article de notre base de connaissances : https://support.workspaceone.com/articles/115012790248.

8 Si vous voyez du texte chiffré entre les balises dict dans la fenêtre XML, vous pouvez générer le texte déchiffré en modifiant les paramètres sur la page Profils. Pour ce faire :

   a Accédez à **Groupe et paramètres** > **Tous les paramètres** > **Terminaux** > **Utilisateurs** > **Apple** > **Profils**.

   b Remplacez l'option paramètres personnalisés.

   c Désactivez l'option Chiffrer les profils, puis enregistrez.

9 Revenez au profil **Paramètres personnalisés** et collez le XML que vous avez copié dans la zone de texte. Le code XML doit contenir un bloc de code complet, délimité par <dict> et </dict>.

10 Supprimez la section de configuration que vous aviez configurée à l'origine en sélectionnant la section de configuration de base, par exemple, Restrictions ou Code d'accès, et en sélectionnant sur le bouton moins (-) en bas de la page. Vous pouvez maintenant améliorer le profil en ajoutant du code XML personnalisé pour les nouvelles fonctionnalités.

11 Sélectionnez **Enregistrer et publier**.

politiques de conformité

4

Le moteur de conformité est un outil automatisé de Workspace ONE UEM powered by AirWatch qui garantit que tous les terminaux respectent vos stratégies. Ces politiques peuvent inclure des paramètres de sécurité basiques comme un code d'accès et une période minimale de verrouillage du terminal.

Pour certaines plateformes, vous pouvez également décider de définir et de mettre en œuvre certaines précautions. Ces précautions incluent le respect des exigences de complexité du mot de passe, la mise en liste noire de certaines applications et l'exigence d'un intervalle d'enregistrement pour s'assurer que les terminaux sont sécurisés et en contact avec Workspace ONE UEM. Après avoir déterminé que les terminaux ne sont pas conformes, le moteur de conformité avertit l'utilisateur pour qu'il résolve les erreurs de conformité et évite une action disciplinaire sur le terminal. Par exemple, le moteur de conformité peut envoyer un message à l'utilisateur pour l'informer que son terminal n'est pas conforme.

En outre, les terminaux qui ne sont pas conformes ne peuvent pas recevoir de profils de terminal ni posséder d'applications installées. Si les corrections ne sont pas apportées dans l'intervalle de temps spécifié, le terminal perd accès à certains contenus et fonctionnalités que vous avez définis. Les politiques de conformité et actions disponibles varient selon la plateforme.

Pour plus d'informations sur les stratégies de conformité, notamment sur les stratégies et les actions prises en charge par une plate-forme spécifique, consultez la documentation sur les **terminaux de gestion**, disponible sur docs.vmware.com.

Applications pour iOS

5

Combinez les fonctionnalités de Workspace ONE UEM MDM avec les applications Workspace ONE UEM pour davantage de sécurité et de performances. Gérez facilement les applications Workspace ONE UEM dans toute leur durée de vie sur les terminaux personnels des employés, ceux appartenant à l'entreprise, ainsi que les terminaux partagés depuis UEM Console.

Avec les applications Workspace ONE UEM, vos utilisateurs finaux et vous-mêmes pouvez :

- Explorer l'application VMware Workspace ONE Content pour synchroniser un dossier de contenu personnel.
- Configurer VMware Workspace ONE Web pour sécuriser les recherches sur Internet.
- Activer VMware Workspace ONE Boxer pour configurer la messagerie.
- Utiliser AirWatch Container comme solution alternative à MDM en séparant les données professionnelles et personnelles sur les terminaux tout en respectant la confidentialité des employés.

Pour plus d'informations sur la gestion des applications, reportez-vous au **Guide de gestion des applications mobiles**.

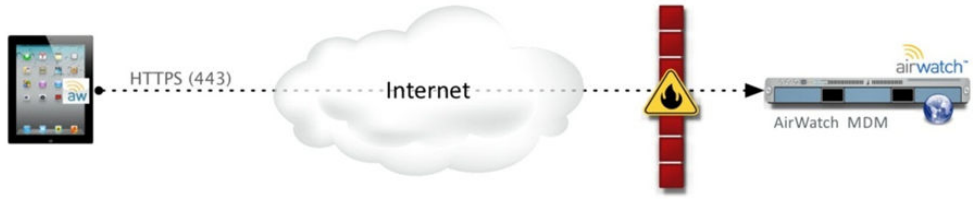
Ce chapitre contient les rubriques suivantes :

Workspace ONE Intelligent Hub pour iOS

Workspace ONE Intelligent Hub pour iOS collecte des informations sur les terminaux gérés et les fournit à UEM Console. Ces informations pouvant contenir des données sensibles,

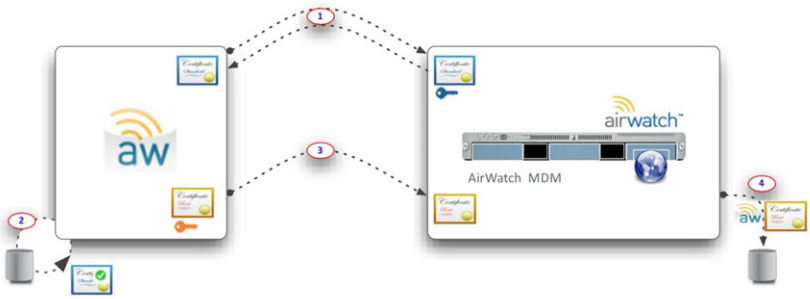
Workspace ONE UEM prend des mesures importantes afin que ces informations soient chiffrées et soient issues d'une source fiable.

Workspace ONE UEM utilise une paire de certificats unique pour signer et chiffrer toutes les communications entre Workspace ONE Intelligent Hub pour iOS et le serveur. Ces certificats permettent également au serveur de vérifier l'identité et l'authenticité de chaque terminal enrôlé dans Workspace ONE UEM. Cet aperçu présente en détail les avantages et les obligations de ces deux modes de renforcement de la sécurité.



Présentation de l'échange de certificats

Avant tout transfert de données, l'application Workspace ONE Intelligent Hub et le serveur s'échangent des certificats personnalisés. Cette relation est établie lorsque Workspace ONE Intelligent Hub pour iOS se connecte au serveur Workspace ONE UEM pour la première fois pendant l'enrôlement.



1 Workspace ONE Intelligent Hub pour iOS communique avec le serveur Workspace ONE UEM pour obtenir une clé publique de certificat du serveur. Workspace ONE Intelligent Hub pour iOS et le serveur Workspace ONE UEM font confiance à la clé publique du certificat racine Workspace ONE UEM qui vérifie l'authenticité de tous les certificats impliqués dans l'échange d'enrôlement.

2 Workspace ONE Intelligent Hub pour iOS valide le certificat du serveur en fonction du certificat de l'autorité de certification racine Workspace ONE UEM.

3 Workspace ONE Intelligent Hub pour iOS envoie une clé publique de certificat unique au serveur Workspace ONE UEM.

4 Le serveur Workspace ONE UEM associe le certificat de Workspace ONE Intelligent Hub à ce terminal dans la base de données.

Sécurisation des données en transit

À partir de l'échange initial des certificats, toutes les données envoyées à UEM Console sont chiffrées. Le tableau suivant indique les deux certificats concernés, ainsi que leur responsabilité dans la transaction.

	Certificat du Hub	Certificat serveur
Workspace ONE Intelligent Hub	Signature des données	Chiffrement des données
Serveur Workspace ONE UEM	Vérification de l'origine des données	Déchiffrement des données

API et fonctionnalité des applications

Workspace ONE UEM utilise deux catégories d'API sur les terminaux iOS pour les fonctionnalités de gestion et de suivi :

- Les **API MDM à distance (OTA)** sont activées lors du processus d'enrôlement, avec ou sans utilisation de Workspace ONE Intelligent Hub pour iOS.
- Les **API iOS SDK natives** sont disponibles pour toutes les applications tierces, notamment Workspace ONE Intelligent Hub et toute autre application utilisant le kit de développement de logiciel (SDK) Workspace ONE UEM.

Workspace ONE Intelligent Hub pour iOS agit comme courtier et s'intègre avec la couche d'API iOS SDK native de gestion. Lorsqu'ils utilisent Workspace ONE Intelligent Hub pour iOS avec Workspace ONE UEM SDK pour iOS, les administrateurs peuvent bénéficier pour les applications de fonctionnalités MDM plus nombreuses que dans la couche d'API MDM à distance.

Configurer les paramètres Workspace ONE Intelligent Hub pour les terminaux iOS

Vous pouvez personnaliser les paramètres Workspace ONE Intelligent Hub dans UEM Console. Par exemple, définissez un profil SDK à utiliser avec Workspace ONE Intelligent Hub pour exploiter la fonctionnalité de Workspace ONE UEM.

Procédure

1 Accédez à **Terminaux > Paramètres des terminaux > Apple > Apple iOS > Paramètres du Hub**.

2 Configurez les paramètres suivants pour Workspace ONE Intelligent Hub :

Tableau 5-1. Généralités

Paramètre	Description
Désactiver le désenrôlement dans le Hub	Ce paramètre empêche l'utilisateur de se désenrôler de Workspace ONE UEM MDM à l'aide de Workspace ONE Intelligent Hub. Ce paramètre n'est disponible que dans Workspace ONE Intelligent Hub 4.9.2 et versions ultérieures.
Actualisation d'application en tâche de fond	Ce paramètre indique à Workspace ONE Intelligent Hub la période maximale autorisée pour actualiser le contenu de l'application. Certaines applications s'exécutent pendant une courte période avant d'atteindre l'état Suspendu. Avec la fonctionnalité Actualisation d'application en tâche de fond dans iOS, l'application sort d'elle-même de cet état Suspendu. Pendant cette actualisation, Workspace ONE Intelligent Hub signale à UEM Console des informations telles que la détection de l'état de compromission, les détails sur le matériel, le GPS, iBeacon et les données sur les télécommunications. La fréquence à laquelle Workspace ONE Intelligent Hub s'actualise est contrôlée par le système d'exploitation et ne se produit que pendant des périodes efficaces, par exemple lorsque le terminal est branché sur secteur ou est connecté sur un réseau Wi-Fi, ou encore en fonction de la fréquence d'utilisation. Pour bénéficier de la fonctionnalité Actualisation d'application en tâche de fond, vous devez activer ce paramètre dans UEM Console. Par ailleurs, Workspace ONE Intelligent Hub ne peut pas être supprimé sur le terminal, et la fonctionnalité Actualisation d'application en tâche de fond doit également être activée sur le terminal pour Workspace ONE Intelligent Hub, sous **Paramètres > Général > Actualisation d'application en tâche de fond**.
Minimum de l'intervalle d'actualisation	Sélectionnez la durée minimale qui doit s'écouler avant que le terminal tente d'actualiser le contenu de l'application.
Transmettre uniquement par Wi-Fi	Activez l'actualisation en tâche de fond pour qu'elle se produise uniquement avec des connexions Wi-Fi.

3 Personnalisez les configurations supplémentaires de Workspace ONE Intelligent Hub dans la page **Paramètres et politiques** d'UEM Console pour Activation de codes d'accès SSO au niveau des applications dans ce guide.

Étape suivante

Pour plus d'informations sur l'accès hors ligne, la personnalisation et d'autres paramètres et politiques, consultez le **guide VMware AirWatch de gestion des applications mobiles** .

Application mobile Workspace ONE Intelligent Hub pour iOS

Après l'enrôlement de Workspace ONE Intelligent Hub, l'application affiche un écran **Mon terminal** par défaut. Vous voyez ici des informations en temps réel concernant votre terminal, sa synchronisation et son réenrôlement, ainsi que les messages envoyés depuis UEM Console.

Dans UEM Console, la case **Self-service activé** doit être cochée dans **Paramètres du Hub** pour permettre l'affichage de toutes les informations sur les statuts.

Note si l'option **Désactiver le désenrôlement du Hub** n'est pas cochée dans **Paramètres du Hub**, sélectionnez **Désenrôler le terminal** avant d'effectuer le réenrôlement avec Workspace ONE Intelligent Hub v4.9.2.

Fonctionnalité Mon terminal

- Appuyez sur la menu **Statut** pour afficher les différents statuts et options de diagnostic en libre-service :
  - **Synchroniser le terminal** – Appuyez sur cette action pour envoyer une requête de resynchronisation du terminal avec UEM Console.
  - **Statut actuel** – Utilisez les menus pour trouver les informations concernant l'enrôlement et le réenrôlement du terminal, l'affichage des comptes, ainsi que la conformité.
  - **Diagnostics** – Utilisez ces menus pour tester la connectivité, afficher l'accès Internet, les problèmes de connectivité et les informations serveur, ainsi que pour afficher et envoyer des journaux du Hub et du terminal.
- Appuyez sur le menu **Détails du terminal** pour afficher différentes options de statut :
  - **Réseau** – Affichez les adaptateurs réseau et les adresses IP.
  - **Avancé** – Utilisez ces menus pour trouver des informations sur la batterie, la mémoire et l'espace disque du terminal.
  - **Localisation** – Affichez les coordonnées GPS de votre terminal pour la période actuelle et les périodes précédentes
  - **iBeacon** – Affichez le nom de la région iBeacon. Si l'iBeacon est configuré, mais que les données de localisation ne le sont pas, le terminal affiche uniquement la zone iBeacon. Si l'iBeacon et les données de localisation sont activés, le terminal affiche la zone iBeacon et l'associe à la localisation sur le terminal.
- Utilisez le **Dock** au bas de l'écran pour trouver d'autres informations, notamment :
  - **Messages** – Lisez les notifications d'UEM Console. Par exemple, vous pouvez recevoir des notifications dans le centre de messages pour procéder à une vérification de conformité obligatoire afin de s'assurer que votre terminal peut être géré sans problèmes.
  - **À propos** – Trouvez des informations juridiques et sur l'application Workspace ONE Intelligent Hub.

VMware Workspace ONE Content

VMware Workspace ONE Content est une application qui permet à vos utilisateurs finaux d'accéder à des contenus importants sur leurs terminaux, tout en assurant la sécurité des fichiers de l'entreprise.

Depuis VMware Workspace ONE Content, les utilisateurs peuvent accéder au contenu que vous importez dans UEM Console, du contenu de référentiels d'entreprise synchronisés ou leur propre contenu personnel.

Utilisez UEM Console pour ajouter du contenu, synchroniser des référentiels et configurer les actions à disposition des utilisateurs pour le contenu ouvert dans l'application. Ces configurations empêchent de copier, de partager ou d'enregistrer du contenu sans autorisation.

Pour plus d'informations sur MCM et la configuration de VMware Workspace ONE Content, reportez-vous au **Guide VMware Workspace ONE UEM de gestion de contenu mobile**.

VMware Workspace ONE Web

VMware Workspace ONE Web est une application qui constitue une solution alternative gérable et sécurisée aux navigateurs Web natifs. Vous pouvez sécuriser l'expérience de navigation au niveau des applications, des tunnels et des sites Web.

Vous pouvez configurer l'application Workspace ONE Web pour qu'elle corresponde aux besoins de l'entreprise en limitant l'accès aux sites Web et en fournissant un portail Internet sécurisé pour les terminaux mobiles de point de vente. Offrez aux utilisateurs une expérience de navigation standard, avec prise en charge de la navigation multi-onglets et les boîtes de dialogue Javascript. Pour une sécurité maximale sur vos terminaux Android et iOS, il est recommandé de déployer Workspace ONE Web avec un profil de restrictions qui bloque le navigateur natif.

Pour savoir comment préparer et configurer Workspace ONE Web pour le déploiement, reportez-vous au **Guide d'administration Web VMware Workspace ONE Web**.

VMware Workspace ONE Boxer

VMware Workspace ONE Boxer est une application de messagerie offrant une productivité mobile centrée sur le consommateur et dotée d'une sécurité professionnelle sous forme de chiffrement AES 256 bits. Cette application sépare les données personnelles et professionnelles, offrant ainsi un accès simple aux contacts, au calendrier et à la messagerie d'entreprise, à la fois sur les terminaux personnels et professionnels.

Workspace ONE Boxer permet aux utilisateurs de configurer l'application pour répondre à leurs besoins grâce à des fonctionnalités personnalisables comme le glisser, les avatars de contact, les dossiers intelligents et les préférences de couleurs du compte. En regroupant la messagerie, le calendrier et les contacts dans une seule application, la solution offre une expérience utilisateur intuitive qui répond aux principes de conception native sur les terminaux.

Pour plus d'informations sur VMware Workspace ONE Boxer, reportez-vous au *Guide d'administration Workspace ONE BoxerVMware*.

AirWatch Container pour iOS

AirWatch Container offre une approche flexible de la gestion de terminaux personnels (BYOD, Bring Your Own Device) via le déploiement d'un espace de travail sécurisé sur les terminaux personnels. Les entreprises peuvent distribuer des applications internes et Workspace ONE UEM vers AirWatch Container afin que leurs employés puissent les utiliser sur leurs terminaux mobiles.

Les applications sont visibles dans et hors AirWatch Container, mais les applications d'entreprise sont sécurisées via une infrastructure SDK et un code d'accès au conteneur identiques pour toutes. Ces applications peuvent interagir de manière transparente avec l'authentification unique et se connecter sans risques à Internet via un VPN de tunnel pour application.

Pour plus d'informations sur AirWatch Container, consultez le **guide de l'administrateur VMware AirWatch Container**.

Activation de codes d'accès SSO au niveau des applications

L'authentification unique (SSO, Single Sign-On) permet aux utilisateurs finaux d'accéder aux applications Workspace ONE UEM, les applications encapsulées et les applications créées avec le SDK sans devoir renseigner les identifiants de connexion pour chaque application. En utilisant Workspace ONE Intelligent Hub ou AirWatch Container comme « application broker », les utilisateurs finaux s'authentifient une fois par session à l'aide de leurs identifiants habituels ou d'un code d'accès SSO.

Activez la fonction SSO comme une **politique de sécurité** configurée pour être attribuée à toutes les applications Workspace ONE UEM, les applications encapsulées et les applications créées avec le SDK utilisant un profil SDK par défaut.

Procédure

1. Naviguez vers **Groupes et paramètres > Tous les paramètres > Applications > Paramètres et politiques > Politiques de sécurité**.
2. **Activez** l'**authentification unique** pour permettre aux utilisateurs finaux d'accéder à toutes les applications Workspace ONE UEM et de maintenir la connexion.
3. (Facultatif) Si vous le souhaitez, **définissez le type d'authentification** sur **Code d'accès** et le **mode de code d'accès** sur **Numérique** ou **Alphanumérique** pour exiger un code d'accès SSO sur le terminal. Si vous activez l'authentification unique, mais pas le type d'authentification, les utilisateurs finaux s'authentifient avec leurs identifiants habituels (compte Workspace ONE UEM ou services d'annuaire) et aucun code d'accès SSO n'est généré.

Résultats

Lorsqu'un utilisateur s'authentifie avec une application à authentification unique, une session SSO s'ouvre. La session reste active jusqu'à ce que le **délai d'expiration** défini dans le profil SDK soit atteint ou que l'utilisateur verrouille manuellement l'application.

Aperçu d'Apple Configurator

Workspace ONE UEM s'intègre à Apple Configurator pour vous permettre de superviser et de gérer les déploiements de terminaux Apple iOS. Les administrateurs peuvent créer des profils de configuration, importer des profils existants depuis l'utilitaire de configuration iPhone, installer des versions de système d'exploitation spécifiques et appliquer des politiques de sécurité pour les terminaux iOS.

Installez et exécutez Apple Configurator 2 depuis un ordinateur portable macOS pour l'intégrer avec Workspace ONE UEM Console afin de superviser et de configurer un ou plusieurs terminaux simultanément.

- Installez le profil Workspace ONE UEM MDM en tant qu'élément de la configuration pour enrôler les terminaux en mode silencieux.
- Supervisez des terminaux dédiés à une activité et partagés entre plusieurs utilisateurs.
- Créez des profils de configuration afin de changer les paramètres de terminal pour les réseaux Wi-Fi, la préconfiguration des paramètres de messagerie et de Microsoft Exchange, etc.
- Distribuez des applications publiques sans saisir d'identifiant Apple sur le terminal.
- Créez des blueprints pour automatiser la gestion des terminaux. Utilisez des blueprints comme modèles pour configurer des profils et des applications, puis les envoyer rapidement aux terminaux.
- Ajoutez une fonctionnalité de supervision aux terminaux et bénéficiez d'autres fonctionnalités de gestion, notamment l'affichage ou le masquage d'applications, la modification du nom des terminaux, du fond d'écran, des codes d'accès, des raccourcis clavier, etc.
- Sauvegardez les paramètres utilisateur et les données d'application, notamment les données créées par un nouvel utilisateur à l'aide de Configurator.

Apple Configurator 2 fonctionne également avec le programme DEP (Device Enrollment Program) d'Apple pour automatiser l'enrôlement MDM (Mobile Device Management) et le programme d'achat en volume (VPP) en attribuant aux terminaux des applications sous licence gérées.

Pour obtenir la liste complète des fonctions et fonctionnalités disponibles pour les terminaux supervisés et non supervisés, consultez l'Chapitre 10 Matrice des fonctionnalités iOS : comparaison Supervisé et Non supervisé.

Pour plus d'informations sur l'inscription de terminaux iOS avec Apple Configurator, consultez les manuels Enrôlement par lots de terminaux iOS à l'aide d'Apple Configurator et **Integration with Apple Configurator Guide**.

Importer un profil Apple Configurator signé dans UEM Console

Vous pouvez exporter un profil signé depuis Apple Configurator (ou IPCU) directement vers UEM Console.

Procédure

1. Configurez les paramètres de gestion et de supervision dans Apple Configurator (ou IPCU).
2. Exportez et enregistrez le profil nouvellement créé dans un emplacement facilement accessible sur votre ordinateur.
3. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** dans UEM Console et sélectionnez **Charger**.

4 Complétez le champ **Géré(e) par** et sélectionnez **Importer** pour sélectionner le profil exporté depuis Apple Configurator (ou IPCU). Cliquez sur **Continuer**.

5 Saisissez la description générale du profil, notamment le nom, la description et les groupes organisationnels attribués.

6 Cliquez sur **Enregistrer et publier** pour envoyer le profil vers tous les terminaux attribués.

Configurations de terminal iOS 6

Workspace ONE UEM vous aide à configurer les éléments essentiels permettant de gérer l'expérience des terminaux de vos utilisateurs afin de répondre aux objectifs de votre entreprise. La fonctionnalité détaillée dans cette section fournit des détails granulaires de l'interface et de l'expérience de vos terminaux gérés.

Ces configurations sont majoritairement disponibles uniquement avec certains types de déploiements, par exemple les déploiements Apple DEP ou Apple School Manager.

Ce chapitre contient les rubriques suivantes :

Modèles d'entreprise Apple

Choisissez les modèles d'entreprise pour accélérer votre déploiement.

Les modèles d'industrie Apple regroupent automatiquement les applications mobiles et profils recommandés, ainsi que les politiques de conformité de manière à ce qu'ils puissent être envoyés simultanément au groupe organisationnel requis.

- Les modèles d'entreprise disponibles dans UEM Console v8.2.2 comprennent les secteurs de la santé et de la vente.

- Les modèles d'entreprise disponibles dans UEM Console v8.3 et versions ultérieures comprennent les secteurs de la santé, de la vente, de l'éducation, de l'hôtellerie/restauration et des services sur site.

Types de modèles

Utilisez le tableau suivant pour déterminer le type de modèle et l'initiative qui décrivent le mieux le type de configuration mobile dont vous avez besoin. Chaque modèle inclut des applications recommandées et des politiques de sécurité en fonction des normes du secteur de la recherche et des meilleures pratiques.

Secteur d'activité	Initiative	Description
Santé	Collaboration clinique	Envoyez au personnel médical et aux patients des communications en temps opportun afin de garantir les meilleurs soins, sans aucun compromis sur la sécurité. (UEM Console v8.2.2 et versions ultérieures)
Flux de travail médicaux mobiles	Permettez aux médecins, infirmières, pharmaciens et autres personnels d'utiliser des communications en temps réel afin de prodiguer des soins aux patients si ces derniers sont à leur domicile ou se trouvent dans une autre structure médicale. (UEM Console v8.2.2 et versions ultérieures)	
Soins apportés aux patients	Augmentez les résultats médicaux et la satisfaction des patients en utilisant des iPad et des applications mobiles afin d'améliorer l'expérience des patients. (UEM Console v8.2.2 et versions ultérieures)	
Éducation	Classe numérique	Utilisez des iPad et des applications mobiles pour communiquer avec les enseignants, les étudiants et les parents au sujet des travaux, du comportement des étudiants, etc. (UEM Console v8.3 et versions ultérieures)
Rendre l'apprentissage agréable	Stimulez l'intérêt des étudiants grâce à l'apprentissage et à la collaboration numériques. (UEM Console v8.3 et versions ultérieures)	
Caisse enregistreuse mobile	Autorisez les employés à servir de point de vente où qu'ils se trouvent, dans une librairie ou dans un bureau administratif par exemple. (UEM Console v8.3 et versions ultérieures)	
Hôtellerie/ Restauration	Expérience des hôtes	Créez pour vos hôtes des expériences mémorables qui les fidéliseront en leur permettant de planifier leurs propres services, de rechercher des attractions ou d'échanger des bons de réduction pour leur fidélité. (UEM Console v8.3 et versions ultérieures)

Secteur d'activité	Initiative	Description
Gestion d'hôtels	Gérez les réservations, suivez les plannings du personnel, les responsabilités de chaque équipe et les demandes spéciales en temps réel. (UEM Console v8.3 et versions ultérieures)	
Paiement mobile	Intégrez des solutions de paiement mobile dans des systèmes de point de vente afin que les clients puissent bénéficier de méthodes de paiement rapides ou autorisez les employés à servir de points de vente dès que nécessaire. (UEM Console v8.3 et versions ultérieures)	
Vente détail	Expérience mobile en magasin	Servez des clients, où qu'ils se trouvent dans le magasin, en parcourant des produits, en fournissant des informations sur les produits, en vérifiant un prix ou en effectuant une vente. (UEM Console v8.3 et versions ultérieures)
Caisse enregistreuse mobile	Créez des points de vente mobiles et libérez de l'espace pour les marchandises. (UEM Console v8.2.2 et versions ultérieures)	
Responsables de magasin	Donnez aux responsables la liberté de travailler sur des rapports, des plannings d'employés et la paie, où qu'ils se trouvent dans le magasin. (UEM Console v8.2.2 et versions ultérieures)	
Services sur site	Employé sur site	Augmentez l'efficacité des représentants commerciaux, des techniciens de maintenance et d'autres catégories de personnel afin de fournir aux clients des services dématérialisés améliorés et des données en temps réel. (UEM Console v8.3 et versions ultérieures)
Responsable sur site	Fournissez aux responsables des plannings dynamiques et des fonctionnalités de génération de rapport en temps réel afin de leur permettre de communiquer avec les employés, d'identifier les emplacements, de modifier les plannings et d'attribuer des tâches. (UEM Console v8.3 et versions ultérieures)	

Utilisation de profils et de politiques de conformité pour les modèles d'entreprise

- **Profils –** La capacité d'ajouter ou de modifier des profils est prise en charge dans UEM Console depuis la page **Affichage en liste** uniquement. Les modifications apportées à la page **Affichage en liste** ne sont pas reflétées dans l'IU du modèle d'entreprise, dans **Hub**.

- **Politiques de conformité –** La seule politique de conformité pouvant être affichée dans les modèles d'entreprise a le statut Compromis dans UEM Console 8.2.2 et versions ultérieures. Semblable aux profils, la capacité d'ajouter ou de modifier des politiques de conformité est prise en charge dans la page **Affichage en liste** uniquement. Les modifications apportées à la page **Affichage en liste** ne sont pas reflétées dans l'IU du modèle d'entreprise, dans **Hub**.

Pour plus d'informations sur la configuration de profils et de stratégies de conformité, reportez-vous au **Guide VMware Workspace ONE UEM de gestion des terminaux mobiles**, disponible dans Ressources Workspace ONE UEM.

Créer un modèle d'entreprise Apple

Configurez des paramètres propres à une initiative à l'aide d'un modèle. Créez ensuite un modèle Soins apportés aux patients à envoyer aux patients. Par exemple, vous pouvez créer un modèle Collaboration clinique à envoyer à un groupe de médecins et à un groupe d'infirmières.

Conditions préalables

Il est conseillé de créer vos groupes d'utilisateurs avant de commencer ce processus.

Procédure

1. Naviguez vers **Hub > Modèles d'entreprise > Affichage en liste > Ajouter un modèle**. Une fenêtre **Ajouter un modèle** s'affiche.
2. Sélectionnez la catégorie de secteur d'activité approprié. Une fenêtre **Prise en charge des modèles d'entreprise** s'affiche.
   a. Si vous souhaitez sélectionner un autre secteur d'activité et d'autres initiatives, sélectionnez **Choisir un autre secteur d'activité** au bas de la fenêtre pour remplacer le secteur actuel si nécessaire.
3. Choisissez l'initiative à configurer et sélectionnez **Configuration**.
4. Sélectionnez **Suivant** après avoir examiné l'aperçu du modèle. Dans la nouvelle fenêtre qui s'affiche, vous pouvez personnaliser le modèle.
5. Définissez le **Nom convivial** qui s'affiche dans UEM Console.

6 Choisissez les **Applications** à envoyer à vos utilisateurs en les sélectionnant et désélectionnant. Par défaut, toutes les applications sont recommandées et présélectionnées. Vous pouvez également sélectionner **Ajouter une application** afin de rechercher l'App Store pour les applications publiques ou d'importer les applications internes.

   a Choisissez **Plus d'options** pour envoyer l'application en mode **Auto** ou **À la demande**, et créez une **Configuration de l'application** personnalisée afin de saisir les paires de valeurs de clé.

   si vous choisissez le modèle Expérience de la mobilité en magasins et sélectionnez VMware Browser en mode d'application unique, configurez l'URL avant d'envoyer le modèle aux terminaux en naviguant vers **Groupes et paramètres > Tous les paramètres > Applications > Navigateur > Mode > URL de la page d'accueil**. Ces terminaux doivent être configurés en mode Supervisé.

7 Examinez les **Politiques** qui s'appliquent au modèle sélectionné.

8 Attribuez des **Utilisateurs** ou des groupes d'utilisateurs pour le déploiement, ou créez des utilisateurs. Les Services d'annuaire doivent déjà être configurés pour que vous puissiez ajouter des utilisateurs d'annuaire. Si un nouvel utilisateur ou un nouveau groupe est créé, il apparaît dans la page **Comptes > Affichage en liste** dans UEM Console, même si le modèle d'entreprise n'est pas encore déployé.

9 Sélectionnez **Suivant** après avoir confirmé vos sélections.

10 Sélectionnez **Publier**. Le nouveau modèle crée un groupe intelligent auquel tous les profils, applications, politiques, utilisateurs et groupes d'utilisateurs sont attribués. Le nouveau modèle apparaît désormais dans **Modèles d'entreprise > Affichage en liste**.

   l est conseillé d'attribuer un modèle à un groupe de terminaux afin qu'une seule initiative soit attribuée à chaque terminal. Toutefois, si vous attribuez deux modèles à un même groupe, toutes les applications des deux modèles s'installent et les politiques les plus restrictives sont envoyées au terminal.

Modifier les listes d'application dans les modèles d'entreprise Apple

Vous pouvez personnaliser les modèles d'entreprise que vous créez avec un déploiement d'applications et des configurations spécifiques.

Procédure

1 Supprimez rapidement une application publique et envoyez immédiatement aux utilisateurs la liste d'applications mise à jour.

   a Naviguez vers **Hub > Modèles d'entreprise > Affichage en liste**.

   b Sélectionnez le **bouton représentant un crayon** ou le nom du modèle pour modifier le modèle.

   c Désélectionnez l'application. La coche qui se trouve dans l'angle disparaît.

   d Sélectionnez **Suivant > Publier** pour enregistrer et republier le modèle.

2 Importez une nouvelle version d'une application interne après avoir supprimé l'ancienne version.

   a Sélectionnez le **bouton représentant un crayon** ou le lien permettant de modifier le modèle.

   b Sélectionnez **Plus d'options**. Une icône de corbeille apparaît dans l'application interne.

   c Sélectionnez **Supprimer** et suivez le message vous invitant à supprimer l'application de la liste.

   d Sélectionnez **Ajouter une application** pour importer l'application mise à jour.

   e Sélectionnez **Suivant > Publier** pour enregistrer et republier le modèle avec la nouvelle version d'application.

   Il est conseillé de modifier les applications uniquement dans le modèle d'entreprise. Toutefois, les applications peuvent également être modifiées depuis **Ressources > Applications > Natives** dans UEM Console. Les modifications apportées aux applications dans la page Affichage en liste natif ne sont pas reflétées dans l'IU du modèle d'entreprise.

Supprimer un modèle d'entreprise Apple

Vous ne pouvez modifier et supprimer des modèles qu'au niveau actuel ou du groupe organisationnel parent. Vous pouvez consulter les modèles créés à un groupe d'organisation supérieur, mais pas les modifier ni les supprimer.

Procédure

1 Naviguez vers **Hub > Modèles d'entreprise > Affichage en liste**.

2 Sélectionnez le **bouton radio**. Un bouton **Supprimer** apparaît en haut de la liste.

3 Sélectionnez **Supprimer** et suivez les messages à l'écran pour supprimer le modèle. La suppression d'un modèle supprime également les applications et politiques correspondantes des terminaux attribués.

   La suppression d'un modèle ne supprime pas l'application dans **Applications > Native** ou ne retire pas le Smart Group de **Groupes > Affichage en liste**.

Aperçu d'Apple iBeacon

Apple iBeacon avec Workspace ONE Intelligent Hub 5.1 (et versions ultérieures) vous permet de gérer la localisation des terminaux. Grâce à la fonctionnalité BLE (Bluetooth Low Energy), les iBeacon fournissent une méthode de suivi des terminaux plus efficace que la géo-barrière.

La fonctionnalité Bluetooth Low Energy n'épuise pas la batterie d'un terminal, si bien que vous pouvez établir des iBeacon pour observer simultanément plusieurs régions et, par conséquent, bénéficier d'une surveillance plus précise. Cette fonctionnalité offre également une plus grande confidentialité pour les utilisateurs, car les terminaux ne sont suivis que lorsqu'ils entrent dans des localisations spécifiques, ou les quittent, au lieu d'être surveillés en permanence.

Après avoir configuré un iBeacon tiers, configurez l'iBeacon dans UEM Console. Créez ensuite les zones iBeacon à surveiller. Pour finir, envoyez les profils avec fonctionnalité iBeacon afin de gérer les iBeacon dans les régions configurées à l'aide de Workspace ONE Intelligent Hub. Détectez si le terminal entre dans ces régions et utilise les journaux d'événements pour rechercher des modifications dans les plages iBeacon.

Prérequis pour iBeacon

- Workspace ONE UEM Console v8.1 et versions ultérieures
- iBeacon d'un fournisseur tiers
- Workspace ONE Intelligent Hub 5.1 et versions ultérieures pour iOS
- Les services de localisation doivent être activés sur le terminal.
- La fonctionnalité Bluetooth doit être activée.
- iPhone 4S et versions ultérieures, iPad mini et versions ultérieures, iPad 3e génération et versions ultérieures, iPod touch 5e génération et versions ultérieures

Détails des opérations iBeacon

- Un maximum de 20 régions, y compris les géo-barrières et les groupes iBeacon peut être attribué au terminal. Il s'agit de la quantité maximale autorisée par Apple. Un nombre élevé de groupes iBeacon attribués au terminal augmente la consommation de la batterie sur le terminal.
- Workspace ONE Intelligent Hub surveille uniquement les iBeacon. Il n'utilise pas la technique de détection qui détermine la proximité du terminal au transmetteur iBeacon.
- Si Workspace ONE Intelligent Hub est fermé avant qu'un terminal ne quitte le groupe iBeacon, le terminal n'est détecté qu'au nouveau lancement de Workspace ONE Intelligent Hub.

Activer iBeacon pour des terminaux iOS

Pour configurer iBeacon, activez d'abord Workspace ONE Intelligent Hub afin qu'il détecte les groupes iBeacon qui reçoivent des diffusions. Ajoutez ensuite un ensemble de groupes iBeacon pour le terminal à surveiller.

Procédure

1. Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Apple > Apple iOS > Paramètres du Hub**.
2. Accédez à **Zone**, puis sélectionnez **Détecter la zone iBeacon** afin d'activer un iBeacon pour le groupe organisationnel.
3. Cliquez sur **Enregistrer**.
4. Accédez à **Ressources** > **Profils et lignes de base** > **Paramètres** > **Zones**.

5 Sélectionnez **Ajouter > Groupe iBeacon**. Choisissez **Ajouter > Ajouter un profil** ou **Modifier** un profil existant à l'aide du bouton crayon qui se trouve dans la partie gauche du profil. Une fenêtre de profil **Général** s'affiche.

6 Configurez les paramètres **Groupe iBeacon**.

Paramètre	Description
Nom de groupe	Saisissez le nom du groupe iBeacon spécifique.
Nom iBeacon	Saisissez le nom de l'iBeacon.
UUID	Saisissez un identifiant unique pour le déploiement iBeacon à partager.
Valeur majeure	Entrez un identifiant pour subdiviser la zone de l'iBeacon.
Valeur mineure	Entrez un identifiant supplémentaire pour subdiviser la zone de l'iBeacon.

7 Cliquez sur **Enregistrer**. Revenez à **Zone**, puis modifiez et supprimez des groupes iBeacon si nécessaire à l'aide des boutons de menu situés à gauche.

Attribuer des groupes iBeacon à des profils de terminaux

Une fois le groupe iBeacon établi, vous pouvez l'attribué à un profil de terminal. Ce profil est alors installé sur le terminal lorsque ce dernier entre dans le groupe iBeacon et il est supprimé de ce groupe lorsqu'il en sorti.

Procédure

1 Accédez à **Ressources** > **Profils et lignes de base** > **Profils**. Choisissez **Ajouter** > **Ajouter un profil** ou **Modifier** un profil existant à l'aide du bouton crayon qui se trouve dans la partie gauche du profil. Une fenêtre de profil **Général** s'affiche.

2 Naviguez vers **Critères d'attribution supplémentaires** dans le profil **Général**.

3 Sélectionnez **Installer uniquement sur les terminaux à l'intérieur des zones sélectionnées**, puis l'iBeacon dans **Zone de géo-barrière attribuée**.

4 Continuez à configurer la section de configuration en fonction de vos besoins.

5 Cliquez sur **Enregistrer et publier**. Vous pouvez désormais gérer les terminaux dans le groupe iBeacon avec Workspace ONE Intelligent Hub.

Ajouter des politiques de conformité pour les groupes iBeacon

Une fois le groupe d'Once iBeacon établi, ajoutez des politiques de conformité afin d'appliquer des actions sur le terminal lorsqu'il entre dans le groupe iBeacon ou lorsqu'il quitte ce groupe.

Procédure

1 Naviguez vers **Terminaux > Politiques de conformité > Affichage en liste** et sélectionnez **Ajouter**, puis **Apple iOS**.

2 Choisissez **N'importe quelle règle** ou **Toutes les règles** pour effectuer la mise en correspondance.

3 Sélectionnez **Zone iBeacon** et choisissez **compris/non compris**, ainsi que le groupe iBeacon, puis sélectionnez **Suivant**.

4 Choisissez l'onglet **Actions** et sélectionnez les actions qui peuvent survenir dans le groupe iBeacon. Pour obtenir des informations détaillées sur les actions applicables sur Apple iOS, reportez-vous à la section *Action des stratégies de conformité par plateforme* de la documentation *Gestion des terminaux*.

5 Sélectionnez **Terminer et activer** lorsque vous avez terminé la configuration de la politique de conformité. Vérifiez que la politique est disponible dans la page Détails du terminal dans UEM Console.

Aperçu du verrouillage d'activation

Le verrouillage d'activation est une fonction de sécurité pour les terminaux exécutant iOS 7 et les versions ultérieures qui utilise la fonctionnalité Localiser mon iPhone d'Apple. Cette fonction rend difficile, pour une personne non autorisée, l'utilisation d'un terminal perdu ou volé.

Lorsque le verrouillage d'activation est activé, l'identifiant Apple et le mot de passe de l'utilisateur sont en effet nécessaires pour déverrouiller un terminal, même si les données du terminal ont été effacées ou si le terminal a été réinitialisé sur les valeurs d'usine, y compris par le mode DFU (Device Firmware Update). Pour plus d'informations sur le verrouillage d'activation pour iOS, veuillez lire l'article de l'assistance Apple Verrouillage d'activation de la fonctionnalité Localiser mon iPhone.

Conditions prérequises

Pour utiliser la fonction Verrouillage d'activation, les terminaux disposer des éléments suivants :

- Un identifiant Apple et un mot de passe valides attribués
- Fonction Localiser mon iPhone activée

Verrouillage d'activation pour terminaux supervisés et non supervisés

Les possibilités de gestion des terminaux sur lesquels le verrouillage d'activation a été activé varient selon le statut des terminaux : supervisés ou non supervisés. Le tableau suivant met en avant les différences :

Non supervisé	Supervisé
■ L'utilisateur final doit activer le paramètre Localiser mon iPhone ■ L'administrateur peut vérifier si le verrouillage d'activation est activé sur un terminal particulier. ■ L'administrateur doit accepter une notification lors de l'exécution de la commande de réinitialisation. Elle vous avertit qu'un terminal sur lequel le verrouillage d'activation est activé ne peut être réactivé qu'avec l'identifiant Apple et le mot de passe d'origine.*	■ L'administrateur peut activer le verrouillage d'activation. Cela aura pour effet d'activer automatiquement le paramètre Localiser mon iPhone. ■ L'administrateur peut vérifier si le verrouillage d'activation est activé sur un terminal particulier. ■ L'administrateur peut désactiver le verrouillage d'activation à l'aide de l'une des trois méthodes.

*Pour apprendre comment supprimer l'identifiant Apple d'un précédent utilisateur afin de réactiver le terminal, veuillez lire l'article de l'assistance Apple Désactivation de l'option Verrouillage d'activation liée au service Localiser mon iPhone.

Activer le verrouillage d'activation pour les terminaux iOS

Pour les terminaux supervisés qui exécutent iOS 7 ou une version ultérieure, vous pouvez configurer le verrouillage d'activation et forcer son activation.

Procédure

1 Naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Apple > Apple iOS > Paramètres gérés**.

2 Sélectionnez le paramètre **Verrouillage d'activation**.

3 Cliquez sur **Enregistrer**.

Affichage du statut de verrouillage d'activation

Pour les terminaux supervisés et non supervisés exécutant iOS 7 ou une version ultérieure, vous pouvez vérifier si le verrouillage d'activation est activé sur le terminal.

Procédure

1 Accédez à **Terminaux > Affichage en liste**.

2 Sélectionnez un terminal iOS.

Résultats

Dans la section Sécurité, vous pouvez voir si le verrouillage d'activation est activé ou désactivé.

Désactiver le verrouillage d'activation sur les terminaux iOS

Pour les terminaux supervisés exécutant iOS 7 ou une version ultérieure, vous pouvez désactiver le verrouillage d'activation à l'aide de l'une des trois méthodes suivantes.

Procédure

1 Utiliser la commande Supprimer le verrouillage d'activation

2 Entrez un code de contournement du verrouillage d'activation directement sur le terminal.

3 Effectuez une commande d'effacement du contenu du terminal et sélectionnez une option pour supprimer le verrouillage d'activation.

Utilisation de la commande Supprimer le verrouillage d'activation

Grâce à la commande Supprimer le verrouillage d'activation, vous pouvez supprimer le verrou d'activation sur un terminal sans réinitialiser le terminal. Cette commande est utile si vous connaissez l'emplacement du terminal et ne souhaitez pas effacer complètement son contenu pour supprimer le verrouillage.

Cette commande fonctionne également si le terminal est désenrôlé de Workspace ONE UEM MDM.

Procédure

1 Naviguez vers **Terminaux > Affichage en liste**.

2 Sélectionnez un terminal iOS.

3 La page Détails du terminal s'affiche. Sélectionnez le menu déroulant **Plus** pour voir la liste des commandes à distance disponibles.

4 Sélectionnez **Supprimer le verrouillage d'activation**.

5 Sélectionnez **Désactiver**.

Saisir un code de contournement du verrou d'activation

La saisie d'un code de contournement du verrouillage d'activation peut être utile si le terminal a été désenrôlé de Workspace ONE UEM MDM et que vous n'avez aucun moyen d'exécuter la commande Supprimer le verrouillage d'activation ou une réinitialisation du terminal.

Procédure

1 Naviguez vers **Terminaux > Affichage en liste**.

2 Sélectionnez un terminal iOS. La page Détails des terminaux s'affiche.

3 Sélectionnez le menu déroulant **Plus** pour voir la liste des commandes à distance disponibles.

4 Sélectionnez **Supprimer le verrouillage d'activation**. Le code de contournement du verrou d'activation s'affiche à l'écran.

Étape suivante

Réactiver le terminal après sa réinitialisation à l'aide de MDM. Lorsque vous accédez au panneau Activer l'iPhone de l'assistant de configuration, saisissez le code de contournement comme mot de passe de verrouillage d'activation et ne remplissez pas la zone de texte Identifiant Apple.

Exécution d'une commande de réinitialisation du terminal

Lors de l'exécution de la commande de réinitialisation du terminal, vous pouvez également supprimer le code d'activation sur un terminal.

Procédure

1 Naviguez vers **Terminaux > Affichage en liste**.

2 Sélectionnez un terminal iOS. La page Détails des terminaux s'affiche.

3 Sélectionnez le menu déroulant **Plus** pour voir la liste des commandes à distance disponibles.

4 Sélectionnez **Réinitialisation du terminal**. La page Réinitialisation du terminal s'affiche.

5 Sélectionnez **Supprimer le verrouillage d'activation**. Saisissez votre **code PIN de sécurité** : le terminal est réinitialisé.

Verrouillage d'activation - Matrice de workflow de commande d'effacement

La matrice suivante montre le workflow permettant de vérifier le code de contournement du verrouillage d'activation avant d'émettre la commande d'effacement depuis la console UEM vers le terminal. La vérification du code de contournement peut être lancée à partir de la page Affichage en liste des terminaux ou de la page Détails du terminal.

Tableau 6-1. Matrice de vérification du code de contournement du verrouillage d'activation

Commande	**Workflow du code de contournement du verrouillage d'activation**	
	Affichage en liste des terminaux	**Page Détails du terminal**
Réinitialisation de terminaux	Non applicable	1 Envoie une requête au terminal pour extraire le code de contournement du verrouillage d'activation. 2 Le terminal est marqué comme **Effacement initialisé du terminal** dans la console UEM. 3 Si la protection contre l'effacement est désactivée sur le terminal, ce dernier répond avec le code de contournement à la console UEM. 4 La console UEM envoie la commande d'effacement du terminal à ce dernier. 5 Le terminal répond avec le message d'effacement réussi à la console UEM. 6 Le terminal est marqué comme **Désenrôlé** dans la console UEM.
Effacement des données d'entreprise	1 Envoie une requête au terminal pour extraire le code de contournement du verrouillage d'activation. 2 Le terminal est marqué comme **Effacement des données professionnelles initialisé** dans la console UEM. 3 Si la protection contre l'effacement est désactivée sur le terminal, ce dernier répond avec le code de contournement à la console UEM. 4 La console UEM envoie la commande d'effacement des données professionnelles au terminal. 5 Le terminal répond avec le message d'effacement réussi à la console UEM. 6 Le terminal est marqué comme **Désenrôlé** dans la console UEM.	1 Envoie une requête au terminal pour extraire le code de contournement du verrouillage d'activation. 2 Le terminal est marqué comme **Effacement des données professionnelles initialisé** dans la console UEM. 3 Si la protection contre l'effacement est désactivée sur le terminal, ce dernier répond avec le code de contournement à la console UEM. 4 La console UEM envoie la commande d'effacement des données professionnelles au terminal. 5 Le terminal répond avec le message d'effacement réussi à la console UEM. 6 Le terminal est marqué comme **Désenrôlé** dans la console UEM.

Requête AirPlay pour un terminal iOS

Grâce à la commande AirPlay, les administrateurs peuvent diffuser en miroir l'écran d'un ordinateur macOS sur un tvOS, sur le même sous-réseau que celui du terminal iOS 7 et versions ultérieures de l'utilisateur.

Si un utilisateur a besoin d'aide, il vous suffit d'envoyer au terminal une demande AirPlay depuis UEM Console afin de partager votre écran sur le terminal de cet utilisateur.

Procédure

1. Naviguez vers **Terminaux > Affichage en liste > Sélectionner un terminal > Support > Plus > Démarrer AirPlay.** Une fenêtre **AirPlay** s'affiche.
2. Sélectionnez **Ajouter une destination** pour commencer à ajouter des destinations à afficher. La fenêtre **Ajouter une nouvelle destination AirPlay** apparaît.
3. Entrez le **Nom de destination**, c'est-à-dire le nom convivial du terminal.
4. Entrez l'**Adresse de destination**, c'est-à-dire l'adresse MAC du terminal à afficher.
5. Entrez le **Mot de passe** de la destination.
6. Déterminez la **Durée de l'analyse**, c'est-à-dire la durée de recherche de la destination par le terminal. La valeur par défaut est de 30 secondes.
7. Cochez la case **Définir par défaut** pour que la destination actuelle soit la destination par défaut. Lors de l'utilisation suivante d'AirPlay, la destination par défaut apparaît dans le menu **Nom de destination**. Elle n'a pas besoin d'être ressaisie.
8. Sélectionnez **Enregistrer et démarrer** pour envoyer la demande AirPlay au terminal.
   a. Cette destination est enregistrée pour la demande suivante dans le menu déroulant **Nom de destination**.
9. Pour **Arrêter AirPlay** sur les terminaux iOS 7 et versions ultérieures supervisés, revenez à UEM Console. Accédez à **Terminaux > Affichage en liste > Sélectionner un terminal > Support > Plus > Arrêter AirPlay.**
10. Pour **Modifier la destination AirPlay**
    a. Naviguez vers **Terminaux > Affichage en liste > Sélectionner un terminal > Support > PlusAir > Play.** Une fenêtre **AirPlay** s'affiche.
    b. Choisissez la **Destination des terminaux** à modifier dans le menu déroulant.
    c. Sélectionnez **Modifier** pour commencer à modifier les paramètres de destination. La fenêtre **Modifier une destination AirPlay** apparaît.
    d. Sélectionnez **Enregistrer et démarrer** pour envoyer la demande AirPlay au terminal.

Affichage à distance

Avec la fonction Affichage à distance, les administrateurs peuvent facilement aider à la résolution des problèmes en affichant le terminal d'un utilisateur final géré par MDM depuis l'instance d'UEM Console qui est intégrée dans le système partenaire. L'intégration du système partenaire avec UEM Console offre une suite complète de gestion à distance dotée de capacités d'affichage à distance.

Pour plus d'informations sur la configuration et l'intégration des services de gestion à distance à l'aide du système partenaire et d'UEM Console, reportez-vous au **Guide VMware AirWatch de gestion à distance avancée** que vous trouverez sur docs.vmware.com.

Prérequis pour lancer une session d'affichage à distance

- Instance d'UEM Console provisionnée avec le nom d'hôte partenaire adéquat et tous les certificats requis.
- Terminaux d'utilisateur final enregistrés auprès du partenaire par Workspace ONE Intelligent Hub.

Configuration requise pour l'affichage à distance de terminaux

- Les terminaux doivent avoir l'application Workspace ONE Intelligent Hub 5.8 ou version ultérieure installée et au premier plan lorsque vous essayez de lancer un affichage à distance.
- L'exécution de la commande **Démarrer l'affichage à distance** nécessite des terminaux iOS 11 et versions ultérieures.
- Pour exécuter la commande **Arrêter l'affichage à distance**, les administrateurs ont besoin de terminaux iOS 11 et versions ultérieures en mode Supervisé. Cette commande s'affiche sur la console partenaire.

Configurer UEM Console avec l'affichage à distance

Pour les déploiements sur site, provisionnez les URL de site avec le nom d'hôte approprié pour le système partenaire au niveau du groupe organisationnel Global sur la page URL de site.

Procédure

1 Accédez à **Groupes et paramètres > Tous les paramètres > Système > Avancé > URL de site**.

2 Dans la section **Workspace ONE Assist**, configurez les paramètres Gestion à distance.

Paramètres	Description
Nom d'hôte de connexion à la console	Entrez le nom de domaine qualifié (FQDN) du serveur de gestion à distance plus « /t10 ». Par exemple : `https://rmstage01.awmdm.com/t10`
Nom d'hôte de connexion au terminal	Entrez le FQDN du serveur ARM. Par exemple : `https://rmstage01.awmdm.com` Le nom d'hôte du terminal est la seule URL utilisée pour l'inscription du terminal. Il est envoyé à tous les terminaux du groupe organisationnel lorsque le partenaire est provisionné.

3 Cliquez sur **Enregistrer**.

Lorsque la page URL de site est enregistrée, l'URL du site ainsi que les données suivantes sont transférées vers le profil de paramètres de Workspace ONE Intelligent Hub. Les terminaux déjà enrôlés auprès de Workspace ONE Intelligent Hub commencent à récupérer le profil de paramètres du Hub mis à jour.

- **Nom d'hôte du terminal** – Nom d'hôte du terminal à contacter lorsqu'une session d'affichage à distance est lancée à partir d'UEM Console.
- **Nom de l'environnement** – Nom d'environnement permettant au partenaire de placer le terminal dans le bon groupe organisationnel lorsque le terminal le contacte pour l'affichage à distance.

Configurer les terminaux des utilisateurs finaux

Maintenant que la console est configurée, vous devez installer le Hub propre à iOS sur les terminaux afin qu'ils puissent être gérés à distance.

Procédure

1 Consultez la page my Workspace ONE™ qui répertorie tous les agents de terminal. (https://my.workspaceone.com/products/AirWatch-Agent).

2 Téléchargez Workspace ONE Intelligent Hub pour iOS sur l'App Store pour votre déploiement.

Pour plus d'informations sur la gestion des applications, consultez le **Guide de gestion des applications mobiles** disponible dans la documentation de VMware AirWatch.

3 Personnalisez le centre de contrôle pour initier la diffusion de l'écran :

a Accédez à **Paramètres > Centre de contrôle > Personnaliser les contrôles**.

b Ajoutez **Enregistrement d'écran**.

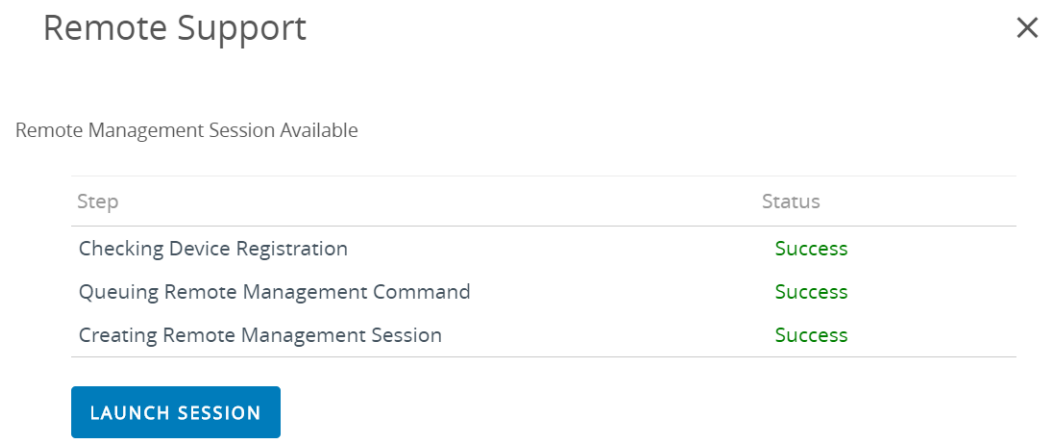
Démarrer une session d'affichage à distance

Utilisez la session d'affichage à distance pour aider facilement au dépannage en affichant le terminal de l'utilisateur final depuis UEM Console.

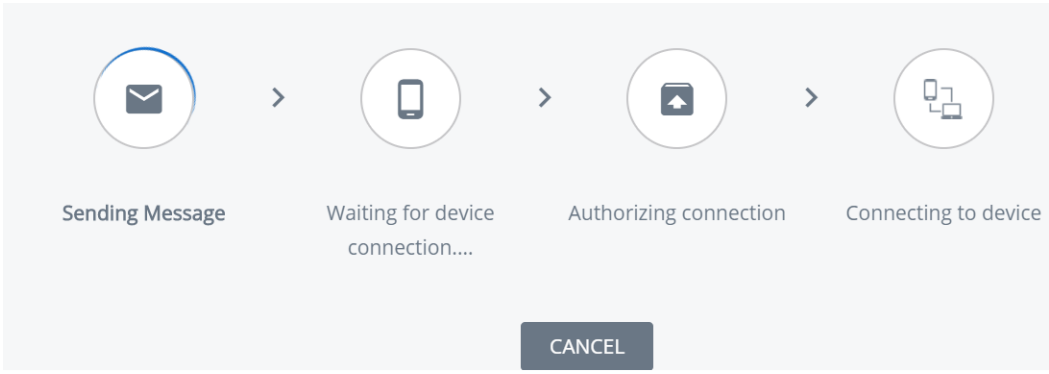
Procédure

1 Naviguez vers **Terminaux > Affichage en liste > Sélectionner un terminal > Plus d'actions > Support > Démarrer l'affichage à distance**

La fenêtre **Assistance à distance** s'affiche. UEM Console vérifie les capacités du terminal avant d'initier la diffusion. Parallèlement, une notification Push est envoyée vers le terminal de l'utilisateur final via Workspace ONE Intelligent Hub afin de lancer la diffusion. L'utilisateur doit accéder au centre de contrôle des terminaux et forcer l'enregistrement de l'écran. Sélectionnez **Diffusion Hub > Démarrer la diffusion** pour lancer la diffusion de l'écran du terminal. Le terminal commence à capturer l'interface utilisateur et la partage avec Workspace ONE Intelligent Hub qui est, à son tour, associé au serveur de gestion à distance avancé.



2 Dans la fenêtre d'assistance à distance, sélectionnez **Lancer la session** pour initier la session d'affichage à distance. Une fois que la connexion est établie, le client de gestion à distance s'ouvre sur la console, et l'écran du terminal en miroir s'affiche.



Note UEM Console affiche un code PIN à quatre chiffres que le client doit entrer sur son terminal. Le client obtient ainsi l'autorisation de gérer son terminal à distance.

3 Si nécessaire, sélectionnez **Annuler** pour terminer la session.

Configurer les paramètres gérés pour les terminaux iOS

La page Paramètres gérés d'UEM Console vous permettent de configurer des paramètres supplémentaires concernant Workspace ONE Intelligent Hub et la gestion des terminaux iOS.

Procédure

1 Naviguez vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Apple > Apple iOS > Paramètres gérés > Paramètres gérés par défaut**.

2 Configurez les terminaux auxquels les paramètres sont appliqués en fonction du type de propriété : professionnel, partagé, personnel ou inconnu.

3 Activez ou désactivez :

   a Itinérance vocale (iOS 5 et versions ultérieures)

   b Données en itinérance (iOS 5 et versions ultérieures)

   c Point d'accès personnel (iOS 7)

   d Verrouillage d'activation (iOS 7, supervisé)

   e (iOS 11.3 et versions ultérieures, supervisé)

4 Sélectionnez **Enregistrer** pour sauvegarder les paramètres sur les terminaux du groupe organisationnel sélectionné.

Remplacer les paramètres d'itinérance par défaut (iOS)

Remplacez les paramètres par défaut afin de modifier les autorisations d'itinérance pour un terminal iOS.

La modification des paramètres pour gérer le statut d'itinérance ne requiert pas de restriction permanente.

Procédure

1 Naviguez vers **Terminaux** > **Affichage en liste**. Filtrez le contenu par **Plateforme** pour localiser le terminal souhaité. Sélectionnez son **Nom convivial** pour ouvrir le panneau de configuration du terminal.

2 Sélectionnez **PlusParamètres gérés**.

3 Sélectionnez le bouton radio **Activer** ou **Désactiver** pour remplacer les paramètres **Itinérance vocale autorisée**, **Autoriser les données en itinérance** et **Point d'accès personnel autorisé** actuels. Cliquez sur **Enregistrer**.

Définir un fond d'écran par défaut

Définissez une image par défaut de l'écran de verrouillage ou de l'écran d'accueil pour les terminaux iOS 7 Supervisés qui corresponde aux politiques de marque de votre entreprise.

Procédure

1. Naviguez vers **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Apple > Apple iOS > Paramètres gérés**. Accédez à la section Fond d'écran par défaut.
2. Importez une **Image de l'écran de verrouillage** ou une **Image de l'écran d'accueil**.
3. Cliquez sur **Enregistrer**.

Définir les informations par défaut de l'organisation

Configurez des informations organisationnelles personnalisées pour les invites MDM pour les terminaux iOS 7 et versions ultérieures.

Procédure

1. Naviguez vers **Terminaux > Paramètres de terminal > Apple > Apple iOS > Paramètres gérés** et rendez-vous à la section **Informations de l'entreprise par défaut**, en bas de la page.
2. Saisissez les informations relatives à votre organisation, notamment son nom, son numéro de téléphone et son e-mail.
3. Cliquez sur **Enregistrer**.

Installer des polices sur les terminaux iOS

Disponible pour les terminaux macOS Yosemite et pour ceux exécutant iOS 7 et versions ultérieures, UEM Console offre un moyen d'importer des polices et de les installer sur les terminaux. L'installation de polices spécifiques permet aux utilisateurs d'afficher et de lire du texte qui n'est traditionnellement pas pris en charge.

Les types de fichiers de police compatibles sont les formats .ttf ou .otf. Vous pouvez installer autant de polices que vous le souhaitez sur les terminaux et pouvez également supprimer des polices à tout moment.

Procédure

- Pour installer et déployer des polices :
  a. Accédez à **Terminaux > Paramètres des terminaux > Apple > Installer des polices de caractères**.
  b. Glissez-déposez un type de fichier de polices pris en charge (`.ttf` ou `.otf`) sur l'écran.
  c. Localisez le fichier de police et sélectionnez **Enregistrer** pour envoyer la police vers tous les terminaux iOS enrôlés dans le groupe organisationnel en cours.

Marquage QoS Cisco pour applications iOS

Apple et Cisco se sont associés pour offrir une meilleure expérience vocale et dans les applications pour les terminaux iOS sur réseaux d'entreprise par l'intermédiaire du réseau Fast Lane QoS de Cisco. Workspace ONE UEM vous permet de sélectionner des applications audio et vidéo pour recevoir les attributions de données prioritaires.

Avec Workspace ONE UEM MDM, les clients disposant de l'infrastructure Cisco peuvent :

- Activer ou désactiver l'utilisation du réseau Fast Lance QoS de Cisco
- Mettre en liste blanche des applications afin de tirer profit du marquage L2 et L3
- Permettre le trafic audio et vidéo pour les services intégrés tels que les appels FaceTime et Wi-Fi pour le marquage L2 et L3 du trafic envoyé au réseau Wi-Fi

Pour configurer le marquage QoS Cisco sur les applications, consultez la section Configurer un profil Wi-Fi.

Apple Push Notification Service (APNs) 7

Apple Push Notification Service (APNs) est le protocole MDM créé par Apple pour gérer ses terminaux. Le fournisseur MDM doit disposer d'un certificat APNs valide configuré et il achemine toutes les commandes via les serveurs de messagerie Cloud centraux d'Apple.

Le lancement d'une commande APNs entraîne les étapes suivantes :

- Lorsqu'un terminal iOS est inscrit, un jeton APNs est généré et connecté à un terminal spécifique. Le jeton généré est connu à la fois de Workspace ONE UEM console et des serveurs APNs.
- Une fois inscrit, un terminal présente toujours une connexion active aux serveurs APNs d'Apple (à condition que la connectivité le permette).
- Lorsqu'une commande est lancée dans UEM console (telle qu'une commande Push de profil ou une commande de verrouillage du terminal), les étapes suivantes se produisent :
  - Une entrée est stockée dans la file d'attente de commandes du terminal dans la base de données UEM. L'entrée contient un ID spécifique associé au type de commande lancée.
  - Le serveur UEM (les services de console ou de terminal, selon l'emplacement de la commande) atteint les serveurs APNs avec le jeton APNs lié à ce terminal spécifique.
- Le serveur APNs valide le jeton et informe le terminal pour qu'il se connecte au serveur MDM afin de recevoir une commande.
- Le terminal se connecte au serveur des services des terminaux. Lors de l'établissement de cette connexion, le terminal reçoit toutes les commandes en attente de la file d'attente de commandes du terminal.

Certificat Apple Push Notification Service (APNs)

Pour gérer des terminaux iOS, vous devez d'abord obtenir un certificat de service de notifications Push d'Apple (APNs). Un certificat APNs permet à la console UEM de communiquer en toute sécurité avec les terminaux Apple. Il permet également le renvoi d'informations à cette console.

D'après l'Enterprise Developer Program d'Apple, la validité d'un certificat APNs est d'un an, après quoi il doit être renouvelé. UEM console envoie des rappels par l'intermédiaire de notifications au fur et à mesure que la date d'expiration approche. Votre certificat actuel est révoqué lorsque vous effectuez un renouvellement depuis le portail de développement d'Apple, ce qui empêche la gestion des terminaux jusqu'à l'importation du nouveau certificat. Prévoyez d'importer votre certificat aussitôt après l'avoir renouvelé. Envisagez l'utilisation d'un certificat différent pour chaque environnement si vous utilisez des environnements de production et de test distincts.

Ce chapitre contient les rubriques suivantes :

Workflow Apple Push Notification Service

Familiarisez-vous avec le workflow backend d'Apple Push Notification Service avant de lancer la gestion MDM sur les terminaux Apple.

Procédure

1. L'administrateur système exécute à distance des actions MDM comme le verrouillage du terminal, l'effacement du code secret du terminal, la réinitialisation du terminal et l'interruption de MDM à partir d'UEM console.

   Une notification sera mise en file d'attente dans **FastLaneAPNsOutBound**, qui est récupérée par **Workspace ONE Messaging Service** et envoyée au serveur APNs. Ensuite, une commande est mise en file d'attente dans **AWEventLog**, puis est récupérée par le service **EntityChangeQueueMonitor**. Ce service met en file d'attente la commande sur le serveur de base de données Workspace ONE.
2. Le terminal dispose toujours d'une connexion active à APNs. Toutes les communications vers APNs sont entrantes et sont constamment vérifiées avec APNs. Les serveurs informent le terminal lorsqu'une commande est en attente pour le terminal par MDM.
3. Une fois que le terminal reçoit la notification Push, il se connecte au serveur de services des terminaux Workspace ONE.
4. Le serveur de services des terminaux vérifie si une commande est mise en file d'attente pour ce terminal donné (basé sur DeviceID) sur le serveur de base de données Workspace ONE.
5. Le serveur de services des terminaux extrait la commande, déjà mise en file d'attente pour ce terminal, à partir du serveur de base de données Workspace ONE.
6. Les services des terminaux génèrent un fichier XML et l'envoient au terminal. MDM Agent native (profil MDM installé sur le terminal) exécute ensuite l'action requise sur le terminal.

Gestion des terminaux

8

Une fois vos terminaux enrôlés et configurés, gérez-les depuis Workspace ONE™ UEM Console. Les outils et fonctionnalités vous permettent de garder un œil sur vos terminaux et exécuter des commandes administratives à distance.

Vous pouvez gérer tous vos terminaux dans UEM Console. Le tableau de bord offre des possibilités de recherche et de personnalisation pour filtrer et trouver des terminaux spécifiques. Cette fonctionnalité facilite la réalisation de fonctions administratives sur un ensemble défini de terminaux. L'affichage en liste des terminaux répertorie tous les terminaux enrôlés dans votre environnement Workspace ONE UEM ainsi que leur statut. La page **Détails du terminal** fournit des informations spécifiques du terminal tels que les profils, les applications, la version de Workspace ONE Intelligent Hub et toute version de service OEM applicable actuellement installés sur le terminal. Vous pouvez également effectuer des actions à distance sur le terminal qui sont propres à la plateforme, à partir de la page Détails du terminal.

Ce chapitre contient les rubriques suivantes :

Tableau de bord des terminaux

Durant le processus d'enrôlement, vous pouvez gérer les terminaux depuis le **Tableau de bord des terminaux** dans Workspace ONE UEM powered by AirWatch.

Le **tableau de bord des terminaux** fournit une vue détaillée de votre flotte complète de terminaux mobiles et vous permet d'agir rapidement sur chaque terminal.

Affichez des représentations graphiques d'informations pertinentes sur les terminaux de votre flotte, telles que le type de propriété, les statistiques de conformité et la répartition par plateforme et OS. Vous pouvez accéder rapidement à chaque ensemble de terminaux dans les catégories présentées en cliquant sur l'une des vues de données disponibles dans le **tableau de bord des terminaux**.

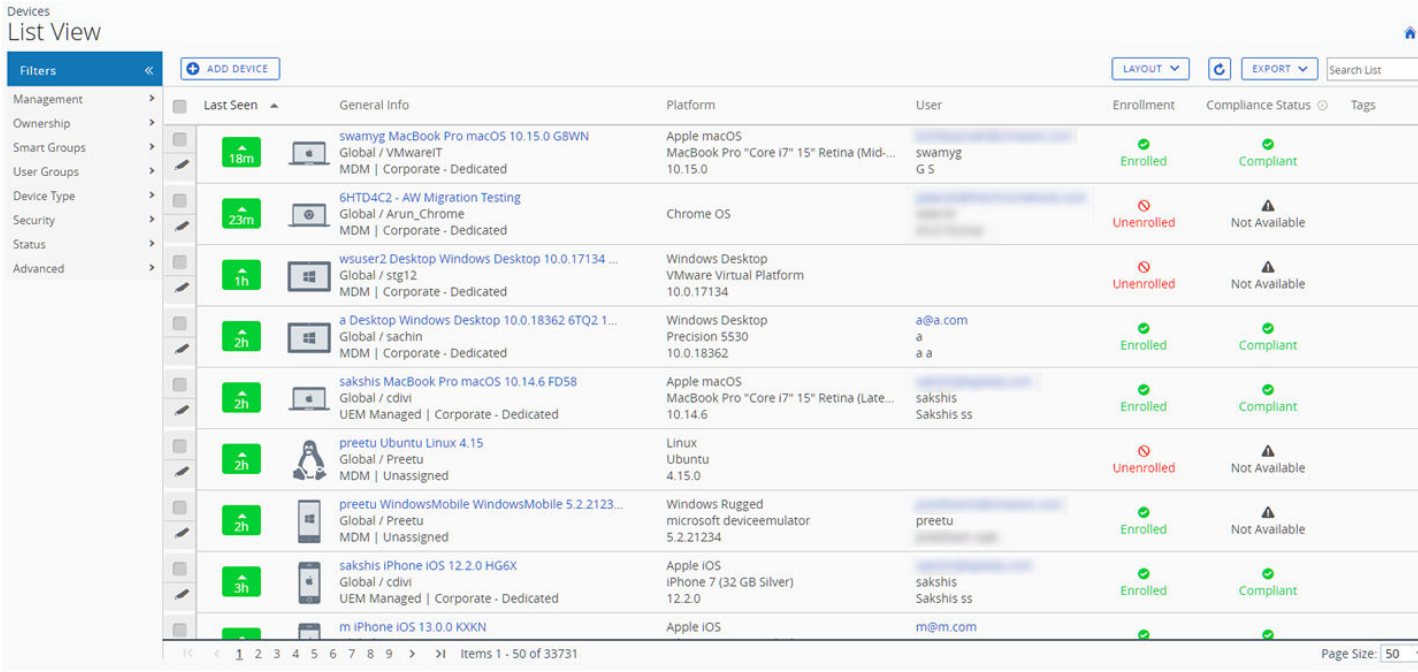
À partir de cet **affichage en liste**, vous pouvez effectuer des actions administratives : envoyer un message, verrouiller ou supprimer des terminaux et modifier les groupes associés à un terminal.

- **Sécurité** – Affichez les causes principales de problèmes de sécurité dans votre flotte de terminaux. La sélection de l'un des graphiques en anneau affiche une **liste de terminaux** filtrés qui sont concernés par le problème de sécurité sélectionné. Si elle est prise en charge par la plateforme, vous pouvez configurer une stratégie de conformité pour entreprendre des actions sur ces terminaux.
  - **Compromis** –Nombre et pourcentage de terminaux compromis (craqués) dans votre déploiement.
  - **Sans code d'accès** – Nombre et pourcentage de terminaux sans code d'accès configuré pour la sécurité.
  - **Non chiffré** – Nombre et pourcentage de terminaux non chiffrés. Ce chiffre exclut le chiffrement de la carte SD Android. Seuls les terminaux Android sans chiffrement de disque figurent dans le graphique.

  Type de propriété – Affichez le nombre total de terminaux pour chaque catégorie de propriété. La sélection de l'un des histogrammes affiche une **liste de terminaux** filtrés par le type de propriété sélectionné.
- **Aperçu/Répartition des derniers terminaux** – Affichez le nombre et le pourcentage de terminaux qui ont récemment communiqué avec le serveur Workspace ONE UEM MDM. Par exemple, si plusieurs terminaux n'ont pas été vus pendant plus de 30 jours, sélectionnez le graphique à barres correspondant pour n'afficher que ces terminaux. Vous pouvez ensuite sélectionner tous ces terminaux filtrés et leur envoyer une commande de requête pour que les terminaux puissent s'archiver.
- **Plateformes** – Affichez le nombre total de terminaux pour chaque catégorie de plateforme. La sélection de l'un des graphiques affiche une **liste de terminaux** filtrés par la plateforme sélectionnée.
- **Enrôlement** – Affichez le nombre total de terminaux pour chaque catégorie d'enrôlement. La sélection de l'un des graphiques affiche une **liste de terminaux** filtrés par le statut d'enrôlement sélectionné.
- **Répartition des systèmes d'exploitation** – Affichez les terminaux de votre flotte par système d'exploitation. Il existe des diagrammes distincts pour chaque système d'exploitation pris en charge. La sélection de l'un des graphiques affiche une **liste de terminaux** filtrés par version d'OS sélectionnée.

Affichage en liste des terminaux

Utilisez l'affichage en liste des terminaux dans Workspace ONE UEM powered by AirWatch pour afficher une liste complète des terminaux du groupe organisationnel actuellement sélectionné.



La colonne **Dernière connexion** affiche un indicateur signalant le nombre de minutes écoulées depuis que le terminal s'est connecté pour la dernière fois. L'indicateur est rouge ou vert, selon la durée pendant laquelle le terminal est inactif. La valeur par défaut est de 480 minutes (8 heures), mais vous pouvez définir une valeur personnalisée en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Avancé** et en modifiant la valeur de **Délai d'expiration d'inactivité du terminal (en min)**.

Choisissez un nom convivial de terminal dans la colonne **Informations générales** à tout moment pour ouvrir la page de détails du terminal concerné. Un **nom convivial** est l'étiquette que vous attribuez à un terminal pour vous aider à le différencier des terminaux de la même marque et du même modèle.

Triez par colonne et configurez les filtres d'informations pour vérifier les activités selon des informations précises. Par exemple, triez la colonne **Statut de conformité** pour n'afficher que les terminaux actuellement non conformes et cibler uniquement ces terminaux. Effectuez une recherche parmi les terminaux par nom convivial ou nom d'utilisateur pour isoler un terminal ou un utilisateur.

Personnalisez l'aperçu de l'affichage en liste des terminaux

Affichez la liste complète des colonnes visibles dans l'affichage **Liste des terminaux** en sélectionnant le bouton **Mise en page** et en choisissant **Personnalisé**. Cet affichage vous permet d'afficher ou de masquer les colonnes Liste des terminaux à votre convenance.

Vous pouvez aussi appliquer vos colonnes personnalisées à tous les administrateurs au niveau du groupe organisationnel actuel ou en dessous de celui-ci. Par exemple, vous pouvez masquer le « Numéro d'actif » depuis les affichages en **Liste des terminaux** du groupe organisationnel actuel et de tous les sous-groupes organisationnels.

Une fois vos personnalisations terminées, cliquez sur le bouton **Accepter** pour enregistrer vos préférences et appliquer ce nouvel affichage de la colonne. Vous pouvez revenir aux paramètres du bouton **Mise en page** à tout moment pour modifier vos préférences d'affichage de la colonne.

Certaines des colonnes de mise en page personnalisées de l'affichage en liste des terminaux incluent les éléments suivants.

- Android Management
- SSID (identifiant SSID ou nom de réseau Wi-Fi)
- Adresse MAC Wi-Fi
- Adresse IP Wi-Fi
- Adresse IP publique

Exporter l'affichage en liste

Sélectionnez le bouton **Exporter** pour enregistrer un fichier .xlsx ou .csv (valeurs séparées par des virgules) de l'intégralité de l'**Affichage en liste du terminal** qui peut ensuite être ouvert et analysé dans MS Excel. Si un filtre est appliqué à l'**Affichage en liste du terminal**, la liste exportée sera également filtrée.

Recherche dans l'affichage en liste des terminaux

Vous pouvez rechercher un terminal pour accéder rapidement à ses informations et entreprendre une action à distance sur celui-ci.

Pour effectuer une recherche, accédez à **Terminaux > Affichage en liste**, cliquez sur la barre **Rechercher dans la liste** et saisissez le nom d'utilisateur, le nom convivial ou un autre élément d'identification du terminal. Cette action est alors lancée sur la totalité des terminaux selon vos paramètres, au niveau du groupe organisationnel actuel et de tous les sous-groupes.

Cluster de boutons d'action d'affichage en liste du terminal

Avec un ou plusieurs terminaux sélectionnés dans l'Affichage en liste des terminaux, vous pouvez effectuer des actions courantes avec le cluster de boutons d'action, notamment Interroger, Envoyer [Message], Verrouiller et d'autres actions accessibles via le bouton **Plus d'actions**.

La disponibilité des actions sur les terminaux varie selon la plateforme, le fabricant du terminal, le modèle, l'état d'enrôlement ainsi que de la configuration spécifique de votre Workspace ONE UEM Console.

Assistance à distance

Vous pouvez démarrer une session **Assistance à distance** sur un seul terminal éligible, ce qui vous permet d'afficher à distance l'écran et de contrôler le terminal. Cette fonctionnalité est idéale pour le dépannage et l'exécution de configurations avancées sur les terminaux de votre flotte.

Pour utiliser cette fonctionnalité, vous devez respecter les exigences suivantes :

- Vous devez posséder une licence valide pour Workspace ONE assistance.
- Vous devez être un administrateur avec un rôle attribué qui inclut les autorisations Assist appropriées.
- L'application Assist doit être installée sur le terminal.
- Plateformes de terminaux prises en charge :
  - Android
  - iOS
  - macOS
  - Windows 10
  - Windows Mobile

Cochez la case à gauche d'un terminal éligible dans l'**Affichage en liste des terminaux** et le bouton **Assistance à distance** s'affiche. Appuyez sur ce bouton pour initier une session d'assistance à distance.

Pour plus d'informations, reportez-vous au guide **Workspace ONE Assist**, disponible sur docs.vmware.com .

Utilisation de la page de détails des terminaux pour terminaux iOS

Utilisez la page Détails du terminal pour suivre les informations détaillées du terminal et accéder rapidement aux actions de gestion des utilisateurs et des terminaux.

Vous pouvez accéder à la page des détails du terminal en cliquant sur le nom convivial d'un terminal depuis la page **Affichage en liste**, depuis l'un des tableaux de bord disponibles ou en utilisant n'importe quel outil de recherche proposé dans UEM console.

Afficher les informations du terminal

Utilisez le menu Détails du terminal pour accéder aux informations spécifiques du terminal :

- **Résumé** – Affichez les statistiques générales telles que :
  - Politique
  - Statut de l'enrôlement

- Dernière connexion
- Plateforme/modèle/système d'exploitation
- menaces
- de supervision
- Verrouillage d'activation
- Localiser mon iPhone
- Sauvegarde iCloud (utilisez la souris pour passer le curseur sur le statut de la sauvegarde iCloud pour voir le statut de la dernière sauvegarde)
- Protection des données
- Chiffrement
- Contacts
- Groupe organisationnel et Smart Group
- Numéro de téléphone (pour les terminaux, tels que iPhone XS, XR ou XS Max prenant en charge plusieurs cartes SIM y compris eSIM, affiche les numéros de téléphone de toutes les SIM associées au terminal)
- Numéro de série, UDID et numéro d'actif
- État de l'alimentation
- Capacité de stockage
- Mises à jour du système d'exploitation disponibles (terminaux iOS 11 et versions ultérieures)
- Mémoire physique et mémoire virtuelle et informations de garantie

Si les informations Global Service Exchange d'Apple sont accessibles, sélectionnez le lien de garantie pour voir la date de la dernière mise à jour du statut. Utilisez ensuite le bouton **Actualiser** pour recevoir les dernières informations.

- La réinitialisation des paramètres d'entreprise ou d'usine demande un code de contournement du verrouillage d'activation, puis elle passe en mode de réinitialisation en attente sur les terminaux **supervisés**.
- Remarque : si l'option Verrouillage d'activation de la fonction Localiser mon iPhone est activée sur les terminaux iOS 7 (et versions ultérieures), un avertissement s'affichera lors de l'exécution de la commande de réinitialisation sur un terminal **non supervisé**, vous informant qu'un terminal ayant activé le verrouillage d'activation ne peut être réactivé qu'avec l'identifiant Apple et le mot de passe d'origine. Ceci s'applique également lorsque vous procédez à une réinitialisation complète du terminal. Pour plus d'informations, consultez la section Aperçu du verrouillage d'activation .

- **Conformité** – Affichez le statut, le nom de la politique, les dates de la dernière et de la prochaine vérification de conformité, ainsi que les actions déjà entreprises sur le terminal.

- **Profils** – Affichez tous les profils MDM actuellement installés sur le terminal.
- **Applications** – Affichez le statut, le nom et le type de l'application (qu'elle soit publique ou interne), sa version et son identifiant, ainsi que sa taille. Pour les terminaux iOS 11. et versions ultérieures, UEM Console affiche les mises à jour disponibles pour l'application (si la version installée est la plus récente ou si une mise à jour est disponible) et la source de l'application (si elle est installée par le biais de l'App Store, distribuée en version bêta, signée ad hoc par un compte d'entreprise ou gérée à l'aide d'une licence VPP basée sur un terminal).

  Note En raison de la manière dont l'état de l'application est signalé sur les terminaux iOS, une application n'obtient le statut **Installé** qu'une fois que le processus d'installation est entièrement terminé. Cela signifie que lorsque Workspace ONE UEM Console interroge le terminal pour son exemple de liste d'applications, et si l'application est toujours en téléchargement, l'application renvoie l'état Installation. Lors d'une installation réussie de l'application, le terminal renvoie l'état de l'application comme **Installé**, qui est marqué de la même manière dans Workspace ONE UEM Console.

- **Mises à jour** – Affichez les mises à jour iOS disponibles pour le terminal, notamment la version du système d'exploitation, la clé de produit, la version de la build, la dernière mise à jour, le pourcentage de téléchargement et l'état de progression.
- **Contenu** – Affichez le statut, le type, le nom, la priorité, le déploiement, la dernière mise à jour, l'heure et la date d'affichage, et utilisez la barre d'outils pour entreprendre des actions d'administration (installer ou supprimer du contenu).
- **Localisation** – Affichez la localisation actuelle d'un terminal ou son historique de localisation.
- **Utilisateur** – Accédez aux détails concernant l'utilisateur d'un terminal et le statut des autres terminaux enrôlés pour cet utilisateur.

Pour accéder aux onglets du menu ci-dessous, cliquez sur **Plus** sous la page principale Détails du terminal :

- **Réseau** – Affichez le statut actuel du réseau (cellulaire, Wi-Fi, Bluetooth) d'un terminal. Pour les terminaux iOS 12.1 et versions ultérieures tels que iPhone XS, XR ou XS Max prenant en charge plusieurs cartes SIM et eSIM, vous pouvez afficher et suivre l'état du réseau des SIM sur UEM console.
- **Sécurité** – Affichez le statut de sécurité actuel d'un terminal, en fonction des paramètres de sécurité.
- **Restrictions** – Afficher les types de restrictions qui s'appliquent au terminal.
- **Télécoms** – Affichez le nombre d'appels, de messages, et la quantité de données envoyés et reçus pour ce terminal.
- **Remarques** – Visualisez et ajoutez des remarques concernant le terminal. Par exemple, indiquez son statut d'expédition ou si le terminal est en réparation ou hors service.
- **Certificats** – Identifiez les certificats des terminaux par nom et émetteur. Cet onglet fournit aussi des informations sur l'expiration des certificats.

- **Conditions d'utilisation** – Affichez la liste des contrats de licence utilisateur final (EULA) qui ont été acceptés lors de l'enrôlement du terminal.
- **Alertes** – Affichez toutes les alertes associées au terminal.
- **Livres** – Affichez toutes les livres internes du terminal.
- **Journal du terminal partagé** – Affichez l'historique du terminal partagé, notamment les dernières connexions et déconnexions et le statut.
- **Restrictions** – Affichez toutes les restrictions appliquées au terminal. Cet onglet affiche également des restrictions par terminal, application, note et code d'accès.
- **Historique du statut** – Affichez l'historique du statut d'enrôlement du terminal.
- **Journalisation ciblée** – Affichez les journaux de la console, du catalogue, des services de terminaux, de la gestion des terminaux et du portail en libre-service. Vous devez activer la journalisation ciblée dans les paramètres. Un lien est prévu à cet effet. Vous devez ensuite sélectionner le bouton **Créer un nouveau journal** et choisir la durée de la collecte du journal.
- **Dépannage** – Affichez les données de consignation **Journal des événements** et **Commandes**. Cette page propose des fonctions d'exportation et de recherche, vous permettant d'effectuer des recherches et des analyses ciblées.
  - **Journal des événements** – Affichez les informations détaillées de débogage et les check-ins sur le serveur, en les **filtrant** notamment par **type de groupe d'événements**, **période**, **gravité**, **module** et **catégorie**.

    Dans la liste **Journal des événements**, la colonne **Données de l'événement** pourrait afficher des liens hypertextes pointant vers une page contenant encore plus d'informations relatives à l'événement. Cette information vous permet d'effectuer un dépannage avancé pour, par exemple, déterminer pourquoi un profil ne peut pas être installé.
  - **Commandes** – Affichez une liste détaillées des commandes terminées et en attente, envoyées au terminal. Contient un **filtre** qui vous permet de trier les commandes par **catégorie**, **statut** et **commande** spécifique.
- **Pièces jointes** – Utilisez cet espace de stockage sur le serveur pour les captures d'écran, les documents, les journaux d'affichage Hub envoyés par Intelligent Hub et les liens destinés au dépannage et à d'autres fins sans occuper de l'espace sur le terminal.

Commandes à distance

Le menu déroulant **Plus d'actions** de la page Détails du terminal vous permet d'effectuer des actions à distance sur le terminal sélectionné. Voici les informations détaillées concernant chaque commande à distance : Les actions répertoriées ci-dessous varient selon différents facteurs, tels que la plateforme du terminal, les paramètres d'UEM Console et le statut d'enrôlement.

- **Envoyer une requête à tous les terminaux** – Envoyez une commande de requête au terminal pour recevoir une liste des applications (dont Workspace ONE Intelligent Hub, le cas échéant), des livres, des certificats, des informations sur le terminal, des profils et des mesures de sécurité installés.
- **Informations sur le terminal (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir des informations telles que le nom convivial, la plate-forme, le modèle, le groupe organisationnel, la version du système d'exploitation et le statut de propriété.
- **Sécurité (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des mesures de sécurité actives (gestionnaire de terminal, chiffrement, code secret, certificats, etc.).
- **Profils (Requête)** – Envoyez une requête MDM au terminal pour recevoir une liste des profils de terminaux installés.
- **Applications (Requête)** – Envoyez une commande de requête MDM au terminal pour recevoir la liste des applications installées.
- **Certificats (Requête)** – Envoyez une requête MDM au terminal pour recevoir une liste des certificats installés.
- **Supprimer le code secret (Paramètres de restriction)** – La commande Supprimer le code secret supprime le code secret du terminal. Le terminal doit être supervisé.
- **Liste d'utilisateurs (Requête)** – Envoyez une commande de requête au terminal pour qu'il vous renvoie la liste des utilisateurs qui se sont connectés à ce terminal (terminaux partagés uniquement).
- **Verrouiller le terminal** – Envoyez une commande MDM pour verrouiller un terminal sélectionné, le rendant inutilisable jusqu'à ce qu'il soit déverrouillé.
- **Verrouiller la SSO** – Empêchez l'utilisateur du terminal d'utiliser Workspace ONE UEM Container et toutes les applications correspondantes.
- **Effacement des données professionnelles** – Effacez les données professionnelles du terminal pour le désenrôler et supprimer toutes ses ressources professionnelles gérées, y compris les

applications et les profils. Cette action ne peut pas être annulée. De plus, le réenrôlement est nécessaire pour que Workspace ONE UEM gère de nouveau ce terminal. Cette action comprend différentes options pour empêcher un futur réenrôlement et une zone de texte **Description de la note** vous permettant d'ajouter des informations sur l'action.

  - L'effacement des données professionnelles n'est pas pris en charge sur les terminaux joints au domaine Cloud.

- **Mises à jour iOS** – Sélectionnez des terminaux indépendamment ou par lots pour envoyer des mises à jour aux terminaux enrôlés à l'aide d'Apple Business Manager.
- **Paramètres gérés** – Activez ou désactivez l'itinérance des appels et des données, ainsi que les points d'accès personnels.
- **Réinitialisation du terminal** – Envoyez une commande MDM pour effacer toutes les données et le système d'exploitation d'un terminal. Le terminal est placé dans un état où une partition de récupération sera nécessaire pour réinstaller le système d'exploitation. Cette action est irréversible. La partition de récupération n'est nécessaire que sur les terminaux Mac et non sur les terminaux iOS.
  - Considérations relatives à la réinitialisation de terminal iOS
    - Pour les terminaux iOS 11 et versions antérieures, la commande de réinitialisation du terminal effacerait également les données de la carte SIM Apple associée.
    - Pour les terminaux iOS 11 et versions ultérieures, vous pouvez conserver le forfait de données de la carte SIM Apple (si disponible sur le terminal). Pour ce faire, cochez la case **Conserver le plan de données** sur la page Effacement du contenu du terminal avant d'exécuter la commande d'effacement du contenu du terminal.
    - Pour les terminaux iOS 11.3 et versions ultérieures, vous disposez d'une option à activer ou désactiver pour ignorer l'écran **Configuration de la proximité** lors de l'exécution de la commande d'effacement du contenu du terminal. Lorsque l'option est activée, l'écran Configuration de la proximité est ignoré dans l'Assistant de configuration, empêchant ainsi l'utilisateur du terminal de voir l'option Configuration de la proximité.

Pour plus d'informations sur la résolution des problèmes liés à la réinitialisation des terminaux, aux autorisations connexes et au moment où les actions de réinitialisation apparaissent dans UEM Console, reportez-vous à l'article suivant de la base de connaissances Workspace ONE UEM https://support.workspaceone.com/articles/115012396488.

- **Planifier des mises à jour d'iOS** – Envoyez une mise à jour iOS à un terminal non enrôlé par DEP. Pour plus d'informations, reportez-vous à la section Gestion des mises à jour d'OS.
- **Actualiser eSIM** – Envoyez une requête à une URL du serveur eSIM de l'opérateur pour actualiser les profils de forfait mobile eSIM actifs sur le terminal.
- **Envoyer un message** – Envoyez un message à l'utilisateur du terminal sélectionné. Choisissez entre **E-mail**, **Notification Push** (via AirWatch Cloud Messaging) et **SMS**. La notification Push requiert des applications Airwatch telles que Hub, Boxer, etc. qui doivent avoir été déployées au moins une fois.
- **Rechercher un terminal** – Envoyez un message texte à l'application Workspace ONE UEM applicable et un bip sonore destiné à aider l'utilisateur à localiser un terminal égaré. Les options de bips sonores comprennent la configuration du nombre de lectures du bip et l'intervalle entre chaque lecture, en secondes.
- **Demander le check-in du terminal** – Demandez au terminal sélectionné d'effectuer son check-in dans UEM Console et de mettre à jour le statut de la colonne **Dernière**. Cette action réinitialise également l'enrôlement du terminal sur l'utilisateur de préenrôlement.
- **Synchroniser le terminal** – Synchronisez le terminal sélectionné avec UEM Console, en actualisant son statut de **Dernière connexion**.
- **Affichage à distance** – Activez un flux actif des données sortantes du terminal vers une destination de votre choix, ce qui vous permet d'afficher ce que l'utilisateur voit lorsqu'il utilise son terminal. Les paramètres de destination comprennent l'adresse IP, le port, le port audio, le mot de passe et le temps d'analyse.
- **Modifier le groupe organisationnel** – Remplacez le groupe organisationnel d'origine du terminal par un autre groupe organisationnel existant. Comprend une option pour sélectionner un groupe organisationnel statique ou dynamique.
  - Si vous souhaitez modifier le groupe organisationnel de plusieurs terminaux à la fois, vous devez sélectionner des terminaux pour effectuer une action en masse à l'aide de la méthode de sélection de bloc (en utilisant la touche Maj) au lieu de sélectionner la case principale (en regard de l'en-tête de la colonne Dernière connexion visible dans la vue de la liste des terminaux).
- **Ajouter une balise** – Attribuez une balise personnalisable à un terminal, pour pouvoir l'identifier au sein de la flotte.
- **Modifier le terminal** – Modifiez les informations du terminal, telles que le **nom convivial**, le **numéro d'actif**, le type de **propriété**, le type de **groupe**, la **catégorie**.
- **Supprimer le terminal** – Supprimez et annulez l'inscription d'un terminal depuis la console. Envoie la commande d'effacement des données professionnelles au terminal qui est effacé

lors de l'archivage suivant et marque le terminal comme **Suppression en cours** sur la console. Si la protection contre l'effacement est désactivée sur le terminal, la commande émise effectue immédiatement un effacement des données professionnelles et supprime la représentation du terminal dans la console.

- **Désactiver le verrou d'activation** – Désactivez le verrou d'activation sur un terminal iOS. Si le verrou d'activation est activé, l'utilisateur doit disposer d'un identifiant Apple et d'un mot de passe avant de pouvoir utiliser les fonctions suivantes : Localiser mon iPhone, Réinitialiser le terminal avec les paramètres usine et Réactiver pour utiliser le terminal.
- **Terminal configuré** – Envoyez cette commande si un terminal est bloqué dans l'état En attente de configuration.
- **Activer/Désactiver le mode Perdu** – Utilisez cette fonctionnalité pour verrouiller un terminal et envoyer un message, un numéro de téléphone ou un SMS à l'écran verrouillé. L'utilisateur final du terminal ne peut pas désactiver le mode Perdu. Lorsqu'un administrateur désactive le mode Perdu, le terminal rétablit la fonctionnalité normale. Les utilisateurs reçoivent un message qui leur indique que l'emplacement du terminal a été partagé. (iOS 9.3 + mode Supervisé)
  - **Demander la localisation du terminal** – Envoyez une requête au terminal lorsqu'il est en mode Perdu et utilisez l'onglet Localisation pour le trouver. (iOS 9.3 + mode Supervisé)
- **Déconnecter l'utilisateur** – Déconnectez l'utilisateur actuel du terminal si nécessaire.

Créer et déployer une commande personnalisée sur un terminal géré

Workspace ONE UEM permet aux administrateurs de déployer une commande XML personnalisée sur des terminaux Apple gérés. Les commandes personnalisées permettent un contrôle plus granulaire sur vos terminaux.

Utilisez les commandes personnalisées pour prendre en charge des actions sur les terminaux que UEM Console ne prend actuellement pas en charge. N'utilisez pas les commandes personnalisées pour envoyer des commandes qui existent déjà dans UEM Console sous forme d'actions sur les terminaux. Des exemples de code XML que vous pouvez déployer en tant que commandes personnalisées sont disponibles dans la base de connaissances Workspace ONE UEM à l'adresse : https://kb.vmware.com/s/article/2960669.

Important des commandes incorrectement formulées ou non prises en charge peuvent avoir un impact sur l'utilisation et les performances des terminaux gérés. Testez la commande sur un seul terminal avant d'émettre des commandes par lots.

Procédure

1. Dans UEM Console, naviguez vers **Terminaux > Affichage en liste**.
2. Sélectionnez un ou plusieurs terminaux macOS ou iOS à l'aide des cases à cocher dans la colonne de gauche.

3 Sélectionnez la liste déroulante **Plus d'actions**, puis cliquez sur **Commandes personnalisées**. La boîte de dialogue Commandes personnalisées s'affiche.

4 Entrez le code XML de l'action que vous souhaitez déployer, puis sélectionnez **Envoyer** pour déployer la commande sur les terminaux.

   Recherchez des exemples de code XML pour commandes personnalisées dans la base de connaissances Workspace ONE UEM à l'adresse : https://kb.vmware.com/s/article/2960669.

   Si la commande personnalisée ne s'exécute pas correctement, supprimez-la en naviguant vers **Terminaux > Affichage en liste**. Sélectionnez le terminal auquel vous avez attribué la commande personnalisée. Dans l'écran **Détails du terminal**, sélectionnez **En savoir plus > Dépannage > Commandes**. Sélectionnez la commande à supprimer, puis cliquez sur **Supprimer**. L'option Supprimer est uniquement disponible pour les commandes personnalisées dotées d'un statut En attente.

Gestion des mises à jour d'OS

Avec le système de gestion des mises à jour du système d'exploitation, les administrateurs peuvent bloquer et exiger des mises à jour iOS sur leurs terminaux iOS supervisés afin de conserver tous les terminaux sur une version iOS commune pour une expérience de gestion cohérente. La maintenance du système d'exploitation garantit que les problèmes de sécurité du terminal sont traités avec des mises à jour iOS mineures et que les terminaux sont toujours à jour.

La gestion des mises à jour du système d'exploitation offre une solution idéale pour les administrateurs pour :

- Empêcher les terminaux d'utilisateurs finaux de détecter de nouvelles mises à jour iOS publiées par Apple. Pour plus d'informations sur la configuration du profil de restriction visant à bloquer les utilisateurs finaux, consultez Configurations des profils de restriction.
- Obtenez des informations sur les correctifs/mises à jour actuellement disponibles pour les terminaux.
- Publiez les mises à jour iOS sur les terminaux des utilisateurs finaux.

Fonctionnalités de gestion des mises à jour iOS

Les principales fonctionnalités disponibles sont :

- **Bloquer la mise à jour** – Configurer le terminal pour qu'il ne détecte aucune mise à jour pendant 90 jours au maximum à partir de la date de publication de la mise à jour par Apple. Pour plus d'informations sur la configuration du profil de restriction afin de bloquer les mises à jour, reportez-vous à Configurations des profils de restriction
- **Répertorier les mises à jour disponibles** – Répertorier toutes les mises à jour disponibles publiées par Apple et répertorier les terminaux admissibles pour les mises à jour respectives.
- **Action de mise à jour du système d'exploitation** – Définir l'action de mise à jour du système d'exploitation : télécharger uniquement, installer uniquement ou télécharger et installer immédiatement.

- **Surveillance** – Afficher l'état d'une mise à jour du système d'exploitation sur les terminaux attribués.

Conditions préalables à la gestion des mises à jour iOS

Assurez-vous de remplir les conditions minimales requises qui sont expliquées dans cette section avant de lancer la gestion des mises à jour du système d'exploitation sur les terminaux gérés à partir de UEM console.

Terminaux pris en charge

- iOS 11.3 et versions ultérieures en mode supervisé
- Le terminal doit disposer d'une batterie à au moins 50 %

Configurations réseau requises

Pour plus d'informations sur l'architecture réseau et ses exigences, reportez-vous au *guide d'architecture recommandée*.

Afficher les mises à jour iOS disponibles

Affichez le snapshot de la liste des dernières mises à jour iOS ou des mises à jour iOS actives publiées par Apple pour tous les terminaux gérés et autorisés.

Accédez à la page **Ressources** > **Mises à jour du terminal** > **iOS** pour afficher les mises à jour disponibles du système d'exploitation et d'autres détails, notamment :

- **Mise à jour** – Nom de la mise à jour.
- **Version** – Version de la mise à jour.
- **Date de publication** – Date de publication de la mise à jour.
- **Date d'expiration** – Date à laquelle la mise à jour expire.
- **État de mise à jour** – État de la mise à jour iOS, mise à disposition ou non par Apple.
- **Attributions** – Nombre d'attributions appliquées à une mise à jour.
- **État de l'attribution** – État des attributions appliquées à la mise à jour : Attribué, Non attribué ou Suspendu.

Note La liste des détails de la mise à jour iOS est fournie par Apple et obtenue à l'aide de la tâche du planificateur Sync Device Updates à l'intervalle spécifié ; la tâche s'exécute toutes les 6 à 24 heures pour extraire les données des serveurs d'Apple.

Sélectionnez une mise à jour du système d'exploitation sur la page **Mises à jour du terminal** > **iOS** pour afficher des informations supplémentaires. La section Détails affiche les détails de la mise à jour du système d'exploitation (comme les détails de la version, les terminaux pris en charge, etc.). Les graphiques sous la section Détails affichent :

- **Disponibilité du terminal** – Fournit des informations relatives à la mise à jour et aux terminaux enrôlés au niveau du groupe organisationnel et au-dessous. Cela inclut les terminaux autorisés à recevoir la mise à jour, les terminaux qui ne sont pas autorisés à recevoir la mise à jour (p. ex. terminal non surveillé, matériel incompatible, etc.), les terminaux qui ont une version plus récente ou les terminaux qui ont déjà la version sélectionnée.
- **État du terminal** – Fournit des informations sur l'état de la mise à jour iOS sur les terminaux autorisés attribués. Cela inclut les terminaux qui ont téléchargé la mise à jour, installé la mise à jour ou dont la mise à jour a échoué avec le code d'erreur indiqué.
- **Terminaux** – Le tableau indique l'état de la mise à jour iOS sur les terminaux autorisés et non autorisés inclus dans une attribution.

Les mises à jour des terminaux sont attribuées à l'aide de Smart Groups et de paramètres de déploiement préférés en sélectionnant **Gérer les attributions**. Pour plus d'informations sur les attributions, reportez-vous à la page Attribuer et publier des mises à jour iOS.

Attribuer et publier des mises à jour iOS

Pour déployer une mise à jour du système d'exploitation, attribuez un ou plusieurs Smart Groups à une mise à jour iOS et procédez à la publication sur le terminal.

Pour attribuer des Smart Groups et déployer les mises à jour iOS :

Procédure

1. Accédez à la page **Ressources** > **Mises à jour du terminal** > **iOS**.
2. Sélectionnez une mise à jour iOS en sélectionnant la case d'option correspondante. L'option **Gérer les attributions** s'affiche en haut de la page.
3. Sélectionnez **Gérer les attributions** pour afficher la page d'attribution.
4. Sélectionnez **Nouvelle attribution** sous la section **Attribution**. La page **Ajouter une attribution** s'affiche.
5. Dans l'onglet **Définition**, entrez le nom de l'attribution et sélectionnez un ou plusieurs Smart Groups. Sélectionnez **Suivant**.

6 Dans l'onglet **Déploiement**, entrez la date et l'heure de début du déploiement, puis sélectionnez une méthode de déploiement. Voici les méthodes de déploiement disponibles :

Méthode	Description
Télécharger et installer	La mise à jour iOS est téléchargée et installée sur le terminal.
Télécharger uniquement	La mise à jour iOS est uniquement téléchargée, elle n'est pas installée sur le terminal.
Installer uniquement	Les mises à jour iOS sont installées sur le terminal uniquement si elles sont déjà téléchargées via MDM ou manuellement.

7 Dans l'onglet **Notification**, activez ou désactivez la notification pour l'état de téléchargement réussi ou d'installation réussie et entrez le texte de notification dans le champ **Notification Push**.

8 Sélectionnez **Enregistrer** pour publier la mise à jour iOS.

Résultats

L'attribution est enregistrée pour la mise à jour iOS sélectionnée dans la console UEM, et tous les terminaux autorisés et attribués qui effectuent un check-in reçoivent la mise à jour de la version iOS spécifiée. L'état de la mise à jour iOS passe à Attribué et l'état des terminaux attribués peut être surveillé sur la page Détails de la mise à jour.

Note Ces paramètres peuvent être modifiés à tout moment après la publication de la mise à jour.

Si des terminaux ont plusieurs attributions de mise à jour iOS, les paramètres de déploiement et la version d'iOS seront évalués avec la priorité suivante :

1 Version iOS la plus récente (p. ex. iOS 13.3 est prioritaire sur iOS 13.1).

2 Attribution la plus proche au niveau ou au-dessus du groupe d'organisation dans lequel le terminal est enrôlé (p. ex. si un terminal est enrôlé dans un groupe d'organisation enfant, le terminal prendra l'attribution au niveau du groupe d'organisation enfant plutôt qu'à n'importe quel niveau parent. Cela suppose que les attributions concernent la même version d'iOS).

3 Priorité la plus élevée dans l'attribution sélectionnée en fonction des deux premiers critères avec une priorité ascendante (p. ex. la priorité 1 est supérieure à la priorité 2).

Suspendre et reprendre les mises à jour iOS

En tant qu'administrateur, vous pouvez même suspendre toute mise à jour qui a été attribuée. Cela bloque les mises à jour qui n'ont pas été envoyées aux terminaux iOS aussi longtemps que la suspension de la mise à jour n'est pas annulée.

Pour suspendre une mise à jour iOS :

Procédure

1 Accédez à la page **Ressources** > **Mises à jour du terminal** > **iOS**.

2 Sélectionnez une mise à jour iOS attribuée.

3 Sélectionnez l'option **SUSPENDRE** en haut de la page.

Note La suspension n'arrête pas les mises à jour qui ont déjà été traitées sur le terminal, par exemple si le téléchargement de la mise à jour a déjà débuté. La suspension empêche uniquement les futurs téléchargements de la mise à jour.

Surveiller les attributions de mise à jour iOS

Après l'attribution et la publication de mises à jour iOS sur des terminaux, l'étape suivante consiste à surveiller leur déploiement.

Pour voir l'état d'un déploiement, sélectionnez une mise à jour iOS sur la page **Ressources** > **Mises à jour du terminal** > **iOS** pour afficher des informations supplémentaires. La section Détails affiche les détails de la mise à jour iOS (comme les détails de la version, les terminaux pris en charge, etc.). Les graphiques situés sous la section Détails sont destinés à l'exécution d'actions sur les terminaux attribués et à leur surveillance. Ces graphiques affichent :

- **Disponibilité du terminal** – Fournit des informations relatives à la mise à jour et aux terminaux enrôlés au niveau du groupe organisationnel et au-dessous. Cela inclut les terminaux autorisés à recevoir la mise à jour, les terminaux qui ne sont pas autorisés à recevoir la mise à jour (p. ex. terminal non surveillé, matériel incompatible, etc.), les terminaux qui ont une version plus récente ou les terminaux qui ont déjà la version sélectionnée.
- **État du terminal** – Fournit des informations sur l'état de la mise à jour iOS sur les terminaux autorisés attribués. Cela inclut les terminaux qui ont téléchargé la mise à jour, installé la mise à jour ou dont la mise à jour a échoué avec le code d'erreur indiqué.
- **Terminaux** – Le tableau indique l'état de la mise à jour iOS sur les terminaux autorisés et non autorisés inclus dans une attribution. Les valeurs de ce tableau sont :

Valeurs	Description
Dernière connexion	Date et heure de la dernière communication du terminal avec Workspace ONE UEM.
Nom du terminal	Nom convivial du terminal.
Utilisateur	Prénom et nom de l'utilisateur d'enrôlement attribué au terminal.
État	État le plus récent reçu pour la mise à jour de cette version d'iOS.
Motif	Contexte supplémentaire de l'état d'une mise à jour qui a échoué.
Nouvelle tentative	Estimation de la date à laquelle le système retentera d'envoyer la mise à jour au terminal lorsque celle-ci a échoué. Cette nouvelle tentative peut se produire avant la date et l'heure indiquées.

Le tableau est également utilisé pour effectuer des actions sur les terminaux pour la mise à jour sélectionnée. Les actions sont :

- **Interrogation** – Demander les dernières informations du terminal associé à la mise à jour iOS.
- **Remplacement** – Déclencher une commande de téléchargement et/ou d'installation pour le terminal. Cette commande ignore les attributions effectuées précédemment pour le terminal.

Gérer les mises à jour iOS pour des terminaux individuels

La gestion des mises à jour iOS peut être réalisée au niveau d'un terminal individuel pour une approche plus directe afin de s'assurer que les dernières mises à jour et leurs fonctionnalités sont appliquées sur un terminal géré. Ces mises à jour peuvent être déployées et surveillées pour un terminal individuel en accédant à **Terminaux > Affichage en liste > Sélectionner le terminal > Mises à jour**.

Publier les mises à jour iOS pour un terminal

Pour publier une mise à jour spécifique sur un terminal sélectionné :

1 Sélectionnez l'onglet **Mises à jour** pour afficher le snapshot des détails des mises à jour du système d'exploitation disponibles.

2 Sélectionnez un nom de mise à jour du système d'exploitation, puis sélectionnez **Publier**. La page **Mise à jour** s'affiche.

3 Sélectionnez la **Méthode d'installation du terminal** souhaitée.

Note L'option **Télécharger/Installer** pour les attributions de mise à jour effectue des opérations de téléchargement ou d'installation en fonction de l'état de la mise à jour du système d'exploitation sur le terminal.

Si la mise à jour du système d'exploitation a déjà été téléchargée, la commande l'installe. Cependant, si la mise à jour du système d'exploitation n'a pas encore été téléchargée, la commande lance un téléchargement. Exécutez de nouveau la commande une fois le téléchargement terminé pour déclencher l'installation.

4 Sélectionnez **Envoyer** pour publier la mise à jour du système d'exploitation sur le terminal.

5 Sélectionnez **Rechercher l'avancement de la mise à jour** pour interroger le dernier état de la mise à jour.

Note Cela n'a aucune incidence sur les mises à jour iOS attribuées au terminal. Toutes les attributions continueront à être publiées sur les terminaux jusqu'à ce qu'elles soient égales ou supérieures à la version iOS attribuée.

Suivre l'état des mises à jour iOS

L'état des mises à jour iOS ne s'affiche pas tant que vous n'avez pas planifié une mise à jour à partir de UEM console, que ce soit une publication manuelle ou l'attribution d'une mise à jour au terminal. Si une mise à jour est téléchargée manuellement sur un terminal iOS, l'état de cette mise à jour n'apparaîtra pas dans la vue en liste **Mises à jour**. Dès que l'administrateur planifie la mise à jour, l'état sur la console est réactualisé. Si une mise à jour est installée manuellement, elle apparaît dans le résumé des détails du terminal.

Résolution des problèmes

Toutes les commandes et réponses peuvent être visualisées dans les données d'événement en accédant à l'onglet **Détails du terminal** → **Plus** → **Dépannage**.

Reporter les mises à jour iOS

Les administrateurs peuvent retarder les mises à jour iOS jusqu'à 90 jours après la publication de la mise à jour par Apple à l'aide d'un profil de configuration.

Pour reporter une mise à jour iOS :

Procédure

1. Accédez à **Ressources** > **Profils et lignes de base** > **Profils** > **Ajouter**.
2. Sélectionnez **Apple** > **iOS** et configurez les paramètres **Restrictions**.
3. Sélectionnez **Retarder les mises à jour (jours)** dans la sous-section **Restrictions des mises à jour du système d'exploitation**.
4. Restreignez les mises à jour et indiquez le nombre de jours pendant lesquels différer la mise à jour logicielle. Nombre de jours allant de 1 à 90. Le nombre de jours indique le laps de temps après le lancement de la mise à jour logicielle, et non après l'heure de l'installation du profil.

Définir le nom du terminal pour un terminal iOS supervisé

Définissez automatiquement ou manuellement un nom de terminal iOS 8 + mode Supervisé pour qu'il corresponde au nom convivial dans UEM Console. Cette fonctionnalité est utile lors du suivi des actifs depuis le terminal proprement dit. Le nom du terminal s'affiche lorsque le terminal est connecté à iTunes et il peut être modifié, dans iTunes également.

Procédure

1. Naviguez vers **Groupes et paramètres > Tous les paramètres > Général > Terminaux et utilisateurs > Nom convivial**.
2. Sélectionnez l'option **Activer le nom convivial pour Smartphone personnalisé** pour définir le nom du terminal en tant que nom convivial.
3. Indiquez le **Format du nom convivial pour Smartphone** en entrant les informations concernant l'utilisateur d'enrôlement, le modèle du terminal et le système d'exploitation du terminal.

4 Sélectionnez le paramètre **Définir le nom convivial comme nom du terminal** pour définir ce nom en tant que nom de terminal et le faire correspondre au nom convivial.

5 Sélectionnez **Enregistrer** pour mettre le nom à jour.

AppleCare GSX

Apple Global Service Exchange (GSX) permet aux administrateurs de rechercher directement depuis UEM Console des informations détaillées sur les terminaux, telles que le nom de leur modèle d'affichage, la date de leur achat et leur statut de garantie.

Si l'un des terminaux d'un groupe d'organisations n'a pas de nom de modèle d'affichage, un programmateur horaire s'exécute périodiquement pour rechercher et mettre à jour ces noms à l'aide des informations de GSX qui ont été configurées pour les terminaux au niveau de ce groupe organisationnel.

Seuls les employés Apple autorisés ou les organisations inscrites au programme de compte libre-service d'Apple peuvent accéder aux informations GSX.

Créer un compte GSX

Avant de pouvoir intégrer votre déploiement, vous devez créer un compte Apple GSX. Pour demander un compte GSX, vous devez avoir un contrat de service avec Apple. Contactez votre responsable de compte Apple pour en savoir plus sur GSX.

Pour faire une demande de compte GSX, visitez le site http://www.apple.com/support/programs/ssa/.

Obtenir un certificat Apple pour intégrer AppleCare GSX

Pour intégrer AppleCare GSX avec un déploiement Workspace ONE UEM, vous devez obtenir au préalable des certificats Apple et les convertir au format .p12.

Pour plus d'informations, consultez Obtenir un certificat Apple pour intégrer AppleCare GSX.

Configurer AppleCare dans UEM Console

Une fois que vous avez obtenu un certificat Apple et que vous l'avez configuré, vous devez l'importer dans UEM Console et configurer l'instance AppleCare.

Pour plus d'informations, consultez la section Configurer AppleCare GSX dans UEM Console.

Obtenir un certificat Apple pour intégrer AppleCare GSX

Pour intégrer AppleCare GSX avec un déploiement Workspace ONE UEM, vous devez obtenir au préalable un certificat Apple et les convertir au format .p12.

Procédure

1 Générez une demande de signature de certificat (CSR) à l'aide d'OpenSSL ou de Java Keytool.

2 Envoyez la demande de signature de certificat et les informations de compte GSX à Apple pour recevoir les certificats Apple (fichiers .pem).

   a Numéro de compte GSX Sold-To

   b Nom du contact informatique principal

   c Adresse de messagerie du contact informatique principal

   d Numéro de téléphone du contact informatique principal

   e Adresse IP statique sortante du serveur qui envoie des demandes à GSX Production

      Si l'environnement est hébergé sur AW SaaS, reportez-vous à l'article https://support.air-watch.com/articles/115001662168 pour l'adresse IP. Si la plage d'adresses IP de l'environnement n'est pas répertoriée, veuillez créer un ticket de support afin que notre équipe des opérations réseau vous en fournisse une.

      Apple génère le certificat Apple (.pem) et renvoie un certificat signé et un certificat de chaîne. Pour en faciliter l'utilisation, renommez les fichiers « cert.pem » et « chain.pem » afin de les utiliser dans des étapes ultérieures.

      Vous pouvez également recevoir le fichier « issuer » qui n'est pas nécessaire pour ce processus.

3 Convertissez les certificats Apple au format .p12.

   a Créez un fichier .p12 à l'aide de la clé privée et des certificats Apple en exécutant la commande suivante :`sudo openssl pkcs12 –export –inkey privatekey.pem –in cert.pem –certfile chain.pem –out GSX_Cert.p12`

   b Le certificat est enregistré en tant que fichier .p12 à l'emplacement que vous spécifiez.

      Si vous ne spécifiez pas de chemin lors de l'exécution de la commande de conversion, le fichier est enregistré dans votre répertoire de travail.

Configurer AppleCare GSX dans UEM Console

Une fois que vous avez obtenu un certificat Apple et que vous l'avez configuré, vous devez l'importer dans UEM Console et configurer l'instance AppleCare.

Procédure

1 Naviguez vers **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Apple > AppleCare**.

   Pour configurer une connexion GSX avec UEM Console, vous devez disposer d'un compte GSX doté du niveau d'accès gestionnaire, d'un accès aux services Web ainsi que d'un accès aux informations de couverture et de garantie.

2 Entrez les **paramètres GSX** notamment :

Paramètre	Action
ID de l'utilisateur GSX	Entrez l'ID de l'utilisateur du compte.
Mot de passe GSX	Entrez le mot de passe de compte.
Numéro de compte de l'acquéreur	Entrez le numéro de compte de service à dix chiffres. Vous trouverez ce numéro de compte dans le portail GSX au bas de la page Web.
Fuseau horaire	Utilisez le menu déroulant pour sélectionner le fuseau horaire approprié.
Langue	Utilisez le menu déroulant pour choisir la langue.

3 Sélectionnez **Enregistrer** pour terminer l'intégration avec AppleCare.

4 Naviguez vers **Affichage en liste**, sélectionnez un terminal et utilisez le menu **Plus** pour rechercher les informations **AppleCare** dans UEM Console.

5 Accédez à **Comptes** > **Administrateurs** et récupérez les informations de la section **Détails**.

6 Sur la page **Ajouter/modifier l'administrateur** , ajoutez l'ID d'utilisateur GSX et cliquez sur **ENREGISTRER**.

Vous pouvez maintenant effectuer des appels API GSX.

Terminaux partagés

9

La fonctionnalité de terminaux partagés/multi-utilisateurs de Workspace ONE UEM powered by AirWatch garantit la sécurité et l'authentification pour chaque utilisateur final. De plus, les terminaux partagés permettent uniquement à certains utilisateurs finaux d'accéder à des informations sensibles.

L'attribution d'un terminal à chaque employé peut être coûteux pour certaines organisations. Grâce à Workspace ONE UEM powered by AirWatch, vous pouvez faire en sorte que les utilisateurs partagent des terminaux mobiles en mettant en place une configuration fixe commune à tous les utilisateurs ou en définissant des paramètres de configuration propres à chaque utilisateur.

Lorsque vous gérez des terminaux partagés, vous devez d'abord les provisionner avec les paramètres et restrictions applicables avant le déploiement aux utilisateurs finaux. Une fois les terminaux déployés, Workspace ONE UEM utilise un processus de connexion ou de déconnexion propre aux terminaux partagés, qui permet aux utilisateurs finaux de se connecter en saisissant simplement leurs identifiants dédiés ou de services d'annuaire. Le rôle de l'utilisateur final détermine son niveau d'accès aux ressources de l'entreprise, notamment au contenu, aux fonctions et aux applications. Ce rôle garantit la configuration automatique des fonctions et des ressources disponibles après la connexion de l'utilisateur.

Les fonctions de connexion ou de déconnexion sont contenues dans Workspace ONE Intelligent Hub. L'auto-confinement garantit que le statut d'enrôlement n'est jamais affecté et que le terminal est géré (qu'il soit en cours d'utilisation ou non).

Les fonctionnalités de terminaux partagés sont également disponibles en mode natif sur les iPad Apple intégrés à Apple Business Manager. Cette fonctionnalité appelée iPad partagés pour les entreprises utilise l'identifiant Apple géré par l'utilisateur pour la connexion, mais elle n'est pas disponible pour la connexion et la déconnexion dans Workspace ONE Intelligent Hub. Pour en savoir plus sur la configuration des iPad partagés pour les entreprises avec Apple Business Manager et comment obtenir cette fonctionnalité, reportez-vous à la section **iPad partagés pour les entreprises** dans le guide *Présentation d'Apple Business Manager* disponible sur docs.vmware.com.

Fonctionnalités de terminaux partagés

Il existe des fonctionnalités de base quant à la sécurité des terminaux partagés entre plusieurs utilisateurs. Ces fonctionnalités offrent de bonnes raisons pour considérer les terminaux partagés comme solution rentable afin de tirer le meilleur parti de la mobilité d'entreprise.

Fonctionnalité

- Personnalisez l'expérience de chaque utilisateur final sans perdre les paramètres de l'entreprise.
- La connexion à un terminal entraîne sa configuration avec l'accès d'entreprise et des paramètres, des applications et du contenu spécifiques en fonction du rôle et du groupe organisationnel de l'utilisateur.
- Autorisez un processus de connexion/déconnexion qui est contenu dans Workspace ONE Intelligent Hub ou Workspace ONE Access.
- Une fois l'utilisateur final déconnecté du terminal, les paramètres de configuration de cette session sont effacés. Un autre utilisateur final peut alors se connecter au terminal.

Sécurité

- Provisionnez les terminaux avec les paramètres du terminal partagé avant de fournir les terminaux aux utilisateurs.
- Connectez et déconnectez les terminaux sans affecter l'enrôlement dans Workspace ONE UEM.
- Authentifiez les utilisateurs lors de la connexion avec les identifiants Workspace ONE UEM dédiés ou les identifiants des services d'annuaire.
- Authentifiez les utilisateurs finaux à l'aide de Workspace ONE Access.
- Gérez les terminaux même si un terminal n'est pas connecté.

Plateformes qui prennent en charge les terminaux partagés

Les terminaux suivants prennent en charge la fonctionnalité de terminaux partagés/multi-utilisateurs.

- Android 4.3 ou versions ultérieures
- Terminaux iOS avec Workspace ONE Intelligent Hub 4.2 ou versions ultérieures.
  - Pour plus d'informations sur la connexion et la déconnexion des terminaux iOS partagés, consultez la rubrique *Connexion et déconnexion des terminaux iOS partagés* dans le **guide pour la plateforme iOS**, disponible sur docs.vmware.com.
- Terminaux MacOS avec Workspace ONE Intelligent Hub 2.1 ou versions ultérieures.

Ce chapitre contient les rubriques suivantes :

Définir la hiérarchie des terminaux partagés

Bien que cela soit strictement facultatif, la création d'un groupe organisationnel (GO) spécifique aux terminaux partagés offre de nombreux avantages en raison des paramètres de locataires multiples et de terminaux hérités.

Si votre flotte comporte un grand nombre de terminaux partagés et que vous souhaitez les gérer à l'écart des terminaux à utilisateur unique, vous pouvez rendre un groupe organisationnel spécifique à un terminal partagé. La création d'une hiérarchie de terminaux partagés dans la structure de groupes organisationnels est facultative. Les fonctionnalités comme les Smart Groups et les groupes d'utilisateurs vous permettent de ne pas vous reposer exclusivement sur la conception de la hiérarchie de groupes organisationnels pour simplifier la gestion des terminaux.

Toutefois, la mise en œuvre d'un groupe organisationnel de terminaux partagés (ou de groupes organisationnels imbriqués) simplifie la gestion des terminaux en vous permettant de normaliser la fonctionnalité des terminaux via des profils, des politiques et l'héritage des terminaux sans la capacité supplémentaire de traitement requise par un Smart Group ou un groupe d'utilisateurs.

Procédure

1. Accédez à **Groupes et paramètres > Groupes > Groupes organisationnels > Détails du groupe organisationnel**.

   Vous verrez alors un groupe organisationnel représentant votre entreprise.
2. Vérifiez que les **détails du groupe organisationnel** affichés sont corrects, puis utilisez les paramètres disponibles pour apporter des modifications, si nécessaire. Si vous effectuez des modifications, cliquez sur **Enregistrer**.
3. Cliquez sur **Ajouter un sous-groupe organisationnel**.

4 Saisissez les informations suivantes pour le premier groupe organisationnel créé sous le groupe racine :

Paramètre	Description
Nom	Saisissez un nom pour le sous-groupe organisationnel à afficher. Utilisez des caractères alphanumériques uniquement. N'utilisez pas de caractères spéciaux.
ID de groupe	Saisissez un identifiant pour le groupe organisationnel que l'utilisateur final utilisera pour connecter son terminal. Les ID de groupe sont utilisés lors de l'enrôlement pour rassembler les terminaux dans le bon groupe organisationnel. Assurez-vous que les utilisateurs qui partagent des terminaux reçoivent l'**ID de groupe**, celui-ci pouvant être exigé pour la connexion du terminal, en fonction des paramètres de terminal partagé. Si vous n'êtes pas dans un environnement sur site, l'ID de groupe identifie votre groupe organisationnel dans tout l'environnement SaaS partagé. Pour cette raison, tous les ID de groupe doivent posséder un nom unique.
Type	Sélectionnez le type de groupe organisationnel préconfiguré qui reflète la catégorie du sous-groupe organisationnel.
Pays	Sélectionnez le pays où le groupe organisationnel est basé.
Paramètres régionaux	Choisissez une langue pour le pays sélectionné.
Secteur d'activité du client	Ce paramètre est uniquement disponible lorsque le **type** est « Client ». Sélectionnez dans la liste de secteurs d'activité des clients.
Fuseau horaire	Sélectionnez le fuseau horaire pour l'emplacement du groupe organisationnel.

5 Établissez votre structure hiérarchique professionnelle en créant plus de groupes et sous-groupes organisationnels de la même manière.

   a Si vous configurez un **groupe organisationnel défini**, assurez-vous de créer ce groupe organisationnel pour permettre aux utilisateurs finaux de se connecter/déconnecter.

   b Si vous activez l'option **Demander à l'utilisateur de saisir le groupe organisationnel**, assurez-vous d'avoir créé les différents groupes organisationnels requis pour permettre la connexion/déconnexion en fonction des rôles de l'utilisateur final. Pour plus d'informations, consultez la section Configurer les terminaux partagés.

6 Cliquez sur **Enregistrer**.

Configurer les terminaux partagés

Le préenrôlement multi-utilisateurs est semblable au préenrôlement d'utilisateur unique, mais permet à un administrateur informatique de provisionner des terminaux destinés à être partagés par plusieurs utilisateurs.

Procédure

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Terminal partagé**.

2 Cliquez sur **Remplacer** et complétez la section **Regroupement**.

Paramètre	Description
Mode d'attribution de groupe	Vous pouvez configurer les terminaux de trois façons : ■ Sélectionnez **Demander à l'utilisateur de saisir le groupe organisationnel** pour que l'utilisateur final saisisse un ID de groupe organisationnel à chaque ouverture de session. Cette méthode vous offre la flexibilité d'accorder un accès aux paramètres, aux applications et au contenu du groupe organisationnel saisi. Avec cette approche, l'utilisateur final n'est pas limité à l'accès exclusif des paramètres, des applications et du contenu du groupe organisationnel dans lequel il est enrôlé. ■ Sélectionnez **Groupe organisationnel défini** pour limiter vos terminaux gérés aux paramètres et contenu d'un seul groupe organisationnel. Tous les utilisateurs qui se connectent à un terminal ont accès aux mêmes paramètres, aux mêmes applications et au même contenu. Cette méthode peut être avantageuse pour les points de vente où les employés utilisent des terminaux partagés pour réaliser les mêmes opérations, telles qu'un contrôle de stock. ■ Sélectionnez **Groupe organisationnel du groupe d'utilisateurs** pour activer les fonctions basées sur les groupes d'utilisateurs et les groupes organisationnels de la hiérarchie. Lorsqu'un utilisateur final se connecte à un terminal, les paramètres, applications et contenu auxquels il a accès dépendent de son rôle au sein de la hiérarchie. Prenons, par exemple, un utilisateur membre du groupe d'utilisateurs « Vente », lui-même associé au groupe organisationnel « Accès standard ». Lorsque cet utilisateur se connecte au terminal, ce dernier est configuré avec les paramètres, les applications et le contenu associés au groupe organisationnel « Accès standard ». Vous pouvez associer des groupes d'utilisateurs à des groupes organisationnels dans UEM Console. Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement**. Cliquez sur l'onglet **Regroupement** et renseignez les champs requis.
Inviter à lire et accepter les conditions d'utilisation	Invite les utilisateurs finaux à accepter vos **Conditions d'utilisation** avant qu'ils n'ouvrent une session sur un terminal.

3 Complétez la section **Sécurité**.

Paramètre	Description
Exiger le code d'accès du terminal partagé	Obligez les utilisateurs à créer un code d'accès au terminal partagé dans le portail en libre-service pour pouvoir se connecter au terminal. Ce code d'accès est différent du code d'accès SSO ou du code d'accès au niveau du terminal.
Exiger des caractères spéciaux	Exigez l'utilisation de caractères spéciaux dans le code d'accès au terminal partagé, y compris des caractères tels que @, %, &, etc.
Longueur minimum du code d'accès des terminaux partagés	Définissez le nombre minimal de caractères du code d'accès partagé.
Délai d'expiration du code d'accès du terminal partagé (en jours)	Définissez la durée (en jours) après laquelle le code d'accès partagé expire.

Paramètre	Description
Conserver le code d'accès d'un terminal partagé pendant au moins (jours)	Définissez la durée minimale (en jours) durant laquelle le code d'accès au terminal partagé devra être modifié.
Inviter les utilisateurs à changer le code d'accès de leurs terminaux partagés x (jours) avant son expiration	**(Pour terminaux iOS uniquement)** Définissez, en nombre de jours avant l'expiration, le moment où l'utilisateur reçoit un rappel lui indiquant de changer son code d'accès au terminal partagé. Pour de meilleurs résultats, définissez une valeur inférieure à la différence entre l'heure d'expiration et la durée minimale pendant laquelle vous pouvez conserver le code secret de terminal partagé.
historique du code d'accès	Définissez le nombre de codes d'accès enregistrés dans le système afin de renforcer la sécurité de l'environnement en évitant que l'utilisateur ne réutilise un ancien code d'accès.
Déconnexion automatique	Configurez la déconnexion automatique après une période définie.
Déconnexion automatique après	Définissez le laps de temps avant l'activation de la fonction de **déconnexion automatique** en **minutes**, **heures** ou **jours**.
Mode Application unique iOS	Cochez cette case pour configurer le mode application unique, qui verrouille le terminal dans une application unique lorsqu'un utilisateur s'y connecte. Pour exporter un terminal iOS en mode d'application unique, les utilisateurs se connectent à l'aide de leurs identifiants. Lorsque le terminal est de nouveau importé, il repasse en mode d'application unique. L'activation du mode Application unique désactive également le bouton d'accueil sur le terminal. **Note** Le mode d'application unique ne s'applique qu'aux terminaux iOS supervisés.

4 Configurez les **Paramètres de déconnexion**, le cas échéant.

Paramètre	Description
Effacez les données d'application Android	Effacez les données d'application lorsque l'utilisateur se déconnecte d'un terminal partagé (check in).
Réinstaller des applications Android	Utilisez le menu déroulant pour choisir de toujours réinstaller l'application entre les utilisateurs ou de ne jamais réinstaller l'application entre les utilisateurs. Pour les déploiements Android (hérité), vous pouvez choisir de réinstaller l'application si le hub ne peut pas effacer les données d'application entre les utilisateurs.
Effacer le code secret Android du terminal	Ce paramètre permet de contrôler que le code secret actuel du terminal Android est effacé lorsque l'utilisateur se déconnecte (connexion) d'un terminal partagé par plusieurs utilisateurs.
Effacer le code secret iOS du terminal	Ce paramètre permet de contrôler que le code secret actuel du terminal iOS est effacé lorsque l'utilisateur se déconnecte (connexion) d'un terminal partagé par plusieurs utilisateurs.

5 Cliquez sur **Enregistrer**.

Étape suivante

Pour des informations spécifiques sur le provisionnement de terminaux pour le préenrôlement de terminaux à utilisateur unique et à plusieurs utilisateurs, reportez-vous aux rubriques Préenrôler un terminal à utilisateur unique et Préenrôler un terminal à plusieurs utilisateurs.

Se connecter et se déconnecter des terminaux iOS partagés

Vous pouvez vous connecter à un terminal iOS partagé par plusieurs utilisateurs et vous en déconnecter.

Procédure

1 Exécutez Workspace ONE Intelligent Hub sur le terminal.

2 Saisissez les identifiants de l'utilisateur.

Si le terminal est déjà connecté à Workspace ONE Intelligent Hub, les utilisateurs sont invités à saisir un code d'accès SSO. Si le terminal n'est pas connecté, les utilisateurs sont invités à saisir un nom d'utilisateur et un mot de passe. Les profils attribués à chaque utilisateur sont déployés en fonction du Smart Group et des associations de groupes d'utilisateurs.

Note si l'option **Demander à l'utilisateur de saisir le groupe organisationnel** est activée, l'utilisateur doit saisir un **ID de groupe** pour ouvrir une session sur un terminal.

3 Sélectionnez **Connexion** et acceptez les **Conditions d'utilisation**.

Note s'ils sont invités à fournir un code d'accès, les utilisateurs peuvent en créer un dans le portail en libre-service. Ces codes d'accès ont une date d'expiration. À l'approche de cette date d'expiration, Workspace ONE Intelligent Hub invite les utilisateurs à changer leur code d'accès sur le terminal. Si les utilisateurs ne changent pas leur code d'accès avant son expiration, ils doivent retourner sur le portail en libre-service pour en créer un autre.

Étape suivante

Pour vous déconnecter d'un terminal iOS, exécutez Workspace ONE Intelligent Hub et sélectionnez **Déconnexion** en bas.

Matrice des fonctionnalités iOS : comparaison Supervisé et Non supervisé

10

Le tableau suivant montre toutes les fonctionnalités de profil iOS disponibles que vous pouvez contrôler via UEM Console, ainsi que les versions système minimum applicables.

Fonctionnalité	Supervision non obligatoire	Supervision obligatoire	Notes sur l'OS
Code d'accès			
Paramètres du code d'accès	✓		-
Wi-Fi			
Paramètres Wi-Fi	✓		-
Rejoindre automatiquement	✓		iOS 7
Paramètres de point d'accès Wi-Fi 2.0	✓		iOS 7
Paramètres du proxy	✓		iOS 7
Politique de marquage QOS	✓		iOS 10
VPN			
Paramètres du VPN	✓		-
VPN par application	✓		iOS 7
Connexion automatique	✓		iOS 7
E-mail			
Paramètres des e-mails	✓		-
Empêcher le déplacement des messages	✓		iOS 7
Désactiver la synchronisation des contacts récents	✓		iOS 7
Empêcher l'utilisation dans des applications tierces	✓		iOS 7
Utiliser S/MIME	✓		iOS 7
Exchange ActiveSync			
Paramètres EAS	✓		-
Utiliser S/MIME	✓		iOS 7
S/MIME par message	✓		iOS 8
Empêcher le déplacement des messages	✓		iOS 7

Fonctionnalité	Supervision non obligatoire	Supervision obligatoire	Notes sur l'OS
Empêcher l'utilisation dans des applications tierces	✓		iOS 7
Désactiver la synchronisation des contacts récents	✓		iOS 7
Empêcher le dépôt d'e-mails	✓		iOS 9
Application d'appel par défaut	✓		iOS 10
LDAP			
Paramètres LDAP	✓		-
CalDAV			
Paramètres CalDAV	✓		-
Abonnements calendriers			
Paramètres des abonnements aux calendriers	✓		-
CardDAV			
Paramètres CardDAV	✓		-
Raccourcis Internet			
Paramètres des raccourcis Internet	✓		-
Identifiants			
Paramètres des certificats d'identifiants	✓		-
SCEP			
Paramètres SCEP pour l'autorité de certification	✓		-
Proxy HTTP global			
Paramètres du proxy HTTP global		✓	iOS 7
Mode Application unique			
Mode Application unique – Verrouillage du terminal dans une seule application		✓	iOS 7
Paramètres facultatifs pour le « verrouillage du terminal dans une seule application »		✓	iOS 7
Mode d'application unique autonome		✓	iOS 7
Filtre du contenu Web			
Paramètres du filtre du contenu Web (liste blanche, liste noire, URL autorisées)		✓	iOS 7
Filtrage de contenu Web avec fournisseur tiers		✓	iOS 8
Domaines gérés			
Domaines de messagerie gérés	✓		iOS 8

Fonctionnalité	Supervision non obligatoire	Supervision obligatoire	Notes sur l'OS
Domaines Web gérés	✓		iOS 8
Domaines de mot de passe Safari gérés	✓		iOS 9.3
Règles d'utilisation du réseau			
Règles d'utilisation du réseau	✓		iOS 9
Comptes serveur macOS			
Comptes serveur macOS	✓		iOS 9
Authentification unique			
Paramètres d'authentification unique avec authentification Kerberos	✓		iOS 7
Paramètres d'authentification unique avec certificats de renouvellement	✓		iOS 8
AirPrint			
Paramètres de destination AirPrint	✓		iOS 7
Mise en miroir AirPlay			
Paramètres de destination AirPlay (liste blanche)		✓	iOS 7
Mots de passe AirPlay	✓		
Point d'accès			
Paramètres de point d'accès avancés	✓		
Paramètres d'installation d'application			
Installation silencieuse d'applications		✓ +VPP	
Contrôler les paramètres mobiles			
Itinérance vocale	✓	✓	iOS 7
Données en itinérance	✓	✓	iOS 7
Point d'accès personnel	✓	✓	iOS 7
Paramètres de fond d'écran			
Définir une image d'écran de verrouillage		✓	iOS 7
Définir le message de l'écran de verrouillage		✓	iOS 9.3 et versions ultérieures
Définir une image d'écran d'accueil		✓	iOS 7
Définir la disposition de l'écran d'accueil		✓	iOS 9.3 et versions ultérieures
Notifications			
Paramètres de notification		✓	iOS 9.3 et versions ultérieures
Requêtes et commandes			

Fonctionnalité	Supervision non obligatoire	Supervision obligatoire	Notes sur l'OS
Statut supervisé	✓		iOS 7
Statut du point d'accès personnel	✓		iOS 7
Supprimer le verrouillage d'activation		✓	iOS 7
Effacer le code d'accès de restrictions		✓	iOS 8
Configurer les mises à jour iOS		✓	iOS 9 Avant iOS 10.3, DEP est également requis
Reporter les mises à jour iOS		✓	(iOS 11.3 et versions ultérieures)
Messagerie électronique et polices personnalisées			
Installation de polices personnalisées	✓		iOS 7
Messages d'enrôlement personnalisés	✓		iOS 7
Invites MDM personnalisées	✓		iOS 7
Avertissement de verrouillage d'activation	✓		iOS 7