Plateforme Android

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

Intégration de Workspace ONE UEM à Android

1

Workspace ONE UEM powered by AirWatch met à votre disposition un ensemble de solutions de gestion de la mobilité pour enrôler, sécuriser, configurer et gérer votre déploiement sur les terminaux Android. Workspace ONE UEM Console met à votre disposition plusieurs outils et fonctionnalités pour gérer le cycle de vie complet des terminaux de l'entreprise et des employés.

Le guide explique comment intégrer Workspace ONE UEM en tant que fournisseur EMM avec les terminaux Android.

Android Entreprise a été lancé en 2015 pour encourager l'adoption des terminaux Android par les entreprises. Depuis la version 9.4 de Workspace ONE UEM Console, Workspace ONE UEM a adopté la convention de dénomination simplifiée. Android for Work a été renommé Android ; il s'agit de la méthode de déploiement par défaut pour les nouveaux enrôlements. Ce guide explique cette méthode de déploiement. Si vous êtes déjà client Workspace ONE UEM, vous pouvez poursuivre votre déploiement Android en utilisant Android (hérité) pour gérer votre flotte de terminaux. Pour en savoir plus sur la gestion d'Android (hérité), consultez le Guide VMware AirWatch pour la plateforme Android (hérité).

Ce chapitre contient les rubriques suivantes :

Conditions requises pour l'utilisation d'Android avec Workspace ONE UEM

Avant le déploiement sur les terminaux Android, prenez connaissance des prérequis, des exigences concernant l'enrôlement, des documents d'accompagnement et des suggestions fournis par l'équipe de Workspace ONE UEM.

Systèmes d'exploitation pris en charge

Android 5.X.X (Lollipop)

Android 6.X.X

Android 7.X.X

Android 8.X.X

Android 9.X.X

Note L'application du service LG n'est plus prise en charge sur les terminaux LG exécutant Android 9 et les versions ultérieures avec des déploiements Android (hérités). Si vous utilisez des terminaux LG sur Android 9 ou version ultérieure à l'aide de la méthode d'enrôlement Android Hérité, envisagez une migration vers Android Enterprise.

Android 10.X.X

Android 11.X.X

Note Les clients bénéficieront d'un ensemble de fonctionnalités de protection de la confidentialité mis à jour lors de la mise à niveau d'un terminal enrôlé COPE d'Android 10 vers Android 11. Un résumé des fonctionnalités clés des terminaux COPE est disponible dans Présentation des modes des terminaux Android.

Note Si votre entreprise a besoin de plus de temps pour effectuer des tests, il existe deux options pour retarder la mise à niveau de vos terminaux vers Android 11. Voir Gérer les mises à jour système pour les terminaux Android.

Si vos terminaux ne prennent pas en charge l'intégration EMM de Google Play, reportez-vous au déploiement Android (hérité) ou utilisez la configuration de réseau AOSP/fermé.

Pour plus d'informations sur le réseau AOSP/fermé, reportez-vous à Présentation des modes des terminaux Android.

Android Go n'est pas pris en charge par Workspace ONE UEM.

Conditions requises en matière d'enrôlement

Tous les terminaux Android de votre déploiement d'entreprise doivent être enrôlés pour pouvoir communiquer avec Workspace ONE UEM et accéder au contenu et aux fonctionnalités internes. Avant d'enrôler votre terminal, vous devez fournir les informations suivantes.

Si un domaine de messagerie est associé à votre environnement – Si la détection automatique est utilisée :

- **Adresse e-mail** – Il s'agit de l'adresse e-mail professionnelle. Exemple : **JohnDoe@acme.com**.
- **Identifiants** – **Nom d'utilisateur** et **Mot de passe** qui vous permettent d'accéder à l'environnement Workspace ONE UEM. Vous pouvez utiliser vos identifiants de services d'annuaire ou en définir d'autres dans Workspace ONE UEM console.

Si un domaine de messagerie n'est pas associé à votre environnement – Si la détection automatique n'est pas utilisée :

Si un domaine de messagerie n'est pas associé à votre environnement, il vous sera demandé de saisir votre adresse e-mail. Puisque la détection automatique n'est pas activée, vous devrez ensuite fournir les informations suivantes :

- **ID de groupe** – Défini dans Workspace ONE UEM Console, l'ID de groupe associe le terminal au rôle dans l'entreprise.
- **Identifiants** – Nom d'utilisateur et mot de passe uniques qui vous permettent d'accéder à l'environnement AirWatch. Vous pouvez utiliser vos identifiants de services d'annuaire ou en définir d'autres dans Workspace ONE UEM console.

Pour télécharger le Workspace ONE Intelligent Hub et ensuite enrôler un terminal Android, vous devez effectuer l'une des opérations suivantes :

- Accédez à https://www.getwsone.com et suivez les invites.
- Accédez à Workspace ONE Intelligent Hub depuis Google Play Store

Configuration réseau requise pour Android

Les terminaux d'utilisateur final doivent pouvoir atteindre certains points de terminaison pour accéder aux applications et aux services. La configuration réseau requise pour Android est une liste de points de terminaison connus pour les versions actuelles et antérieures des API de gestion d'entreprise.

Pour atteindre tous les points de terminaison, vous devez utiliser une connexion directe. La connexion des terminaux derrière un proxy empêche la communication directe et entraîne l'échec de certaines fonctions.

Tableau 1-1. Règles de pare-feu pour les terminaux

Hôte de destination	Ports	Objectif
play.google.com,android.com,google-analytics.com,googleusercontent.com, *gstatic.com,*gvt1.com*,*ggpht.com,dl.google.com,dl-ssl.google.com, android.clients.google.com*,gvt2.com,*gvt3.com	TCP/443 TCP,UDP/5228-5230	Google Play et mises à jour gstatic.com, googleusercontent.com - contient du contenu généré par l'utilisateur (p.ex., icônes d'application dans le Store) *gvt1.com, *.ggpht, dl.google.com,dl-ssl.google.com,android.clients.google.com -Télécharger les applications et mises à jour, PlayStore APIs, gvt2.com et gvt3.com sont utilisés pour les diagnostics pour la surveillance de la connectivité de Play.
*.googleapis.com	TCP/443	API EMM/Google/PlayStore

Tableau 1-1. Règles de pare-feu pour les terminaux (suite)

Hôte de destination	Ports	Objectif
accounts.google.com, accounts.google.[pays]	TCP/443	Authentification pour les comptes.google.[pays], utilisez votre domaine de niveau supérieur local pour [pays]. Par exemple, pour l'Australie, utilisez accounts.google.com.au, et pour le Royaume-Uni, accounts.google.co.uk.
fcm.googleapis.com, fcm-xmpp.googleapis.com	TCP/443,5228-5230	Firebase Cloud Messaging (p.ex. communication Repérer mon terminal, EMM Console <-> DPC, configurations push)
pki.google.com, clients1.google.com	TCP/443	Vérifications de la liste de révocation des certificats pour les certificats émis par Google
clients2.google.com, clients3.google.com. clients4.google.com, clients5.google.com, clients6.google.com	TCP/443	Domaines partagés par divers services de backend Google, tels que le rapport d'incident, la synchronisation des signets Chrome, la synchronisation de l'heure (tlsdate) et bien d'autres encore
omahaproxy.appspot.com	TCP/443	Mises à jour Chrome
android.clients.google.com	TCP/443	URL de téléchargement CloudDPC utilisée dans le provisionnement NFC
connectivitycheck.android.com www.google.com	TCP/443	La vérification de la connectivité avant celle de CloudDPC V470 Android à partir de N MR1 nécessite que le lien https://www.google.com/generate_204 soit accessible, ou que le réseau WiFi concerné pointe vers un fichier PAC accessible. Elle est également requise pour les terminaux AOSP exécutant Android 7.0 ou versions ultérieures.
www.google.com, www.google.com/generate_204		Terminaux AOSP exécutant Android 7.0 ou versions ultérieures

Règles de pare-feu pour les Consoles

Si une console EMM est localisée sur site, les destinations ci-dessous doivent être accessibles depuis le réseau afin de créer une entreprise Google Play gérée et d'accéder à l'iFrame Google Play géré.

Ces exigences reflètent les exigences actuelles de Google Cloud et sont sujettes à modification.

Hôte de destination	Ports	Objectif
play.google.com, www.google.com	TCP/443	Réenrôler l'entreprise Google Play Store Play
fonts.googleapis.com*, .gstatic.com	TCP/443	iFrame JS, polices Google, contenu généré par l'utilisateur (p.ex., icônes d'application dans le Store)
accounts.youtube.com, accounts.google.com, accounts.google.com.*	TCP/443	Authentification de compte, authdomains de compte spécifiques à un pays
apis.google.com, ajax.googleapis.com	TCP/443	GCM, autres services Web Google et iFrame JS
clients1.google.com, payments.google.com, google.com	TCP/443	Approbation de l'application
ogs.google.com	TCP/443	Éléments de l'interface utilisateur iFrame
notifications.google.com	TCP/443	Notifications de poste de travail/ mobiles

Restrictions d'enrôlement pour Android

Les restrictions d'enrôlement vous permettent de provisionner l'enrôlement, comme restreindre l'enrôlement aux utilisateurs ou groupes d'utilisateurs connus, ou limiter le nombre de terminaux enrôlés autorisés.

Ces options sont disponibles en accédant à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Enrôlement** et en cliquant sur l'onglet **Restrictions**. Ceci permet de personnaliser les politiques de restriction de l'enrôlement par groupe organisationnel et par groupe d'utilisateurs.

Vous pouvez créer des restrictions d'enrôlement en fonction des éléments suivants :

- Fabricant et modèle Android, afin que seuls les terminaux Android approuvés soient enrôlés dans Workspace ONE UEM.

  Note Certains terminaux sont fabriqués par d'autres fournisseurs. Vous pouvez créer une stratégie avec le fabricant actuel du terminal pour que les stratégies entrent en vigueur. Voici quelques façons d'identifier le fabricant du terminal :

  - Accédez à la page **À propos** dans les paramètres du terminal.
  - Avec une commande adb : `adb shell getprop | grep "manufacturer"`.

- Mettez les terminaux sur liste noire ou blanche en indiquant leur UDID, IMEI et numéro de série.

  Note Lors de l'enrôlement de terminaux Android 10 ou version ultérieure en mode Profil professionnel, les terminaux sont maintenus dans un état d'attente jusqu'à ce qu'UEM console puisse récupérer l'IMEI ou le numéro de série sur les terminaux pour voir s'ils sont sur liste blanche ou noire. Tant que cette opération n'est pas vérifiée, le terminal ne sera pas entièrement enrôlé et aucune donnée de travail n'est envoyée avant la fin de l'enrôlement.

Pour plus d'informations, reportez-vous à la section Créer une politique de restriction d'enrôlement.

Termes clés pour Android

Ces termes clés associés à Android vous aideront à comprendre comment configurer et déployer les paramètres pour vos utilisateurs.

- **Profil professionnel** – Le mode Profil professionnel, également appelé Propriétaire du profil, permet de créer un conteneur dédié sur votre terminal pour les applications et les contenus professionnels uniquement. Le mode Profil professionnel permet aux organisations de gérer les données et les applications professionnelles, mais elles n'ont pas accès aux applications et aux données personnelles de l'utilisateur. Les applications Android sont signalées par une icône en forme de mallette pour pouvoir les distinguer des applications personnelles. Pour plus d'informations, reportez-vous à Présentation des modes des terminaux Android.
- **Terminaux gérés pour le travail** – Le mode Terminaux gérés pour le travail, également appelé mode Propriétaire du terminal ou mode entièrement géré, est étendu à l'ensemble du terminal. Le terminal n'est pas destiné à un usage personnel et les stratégies transférées par Workspace ONE Intelligent Hub s'appliquent à l'ensemble du terminal. Le mode Terminaux gérés pour le travail s'applique à un terminal qui démarre dans un état non provisionné. Par le biais d'un processus de provisionnement séparé, il installe et accorde à Workspace ONE Intelligent Hub le contrôle total de l'ensemble du terminal. Pour plus d'informations, reportez-vous à Présentation des modes des terminaux Android.
- **Terminaux professionnels et personnels (COPE)** – ce mode fait référence aux terminaux professionnels. Similaires à des terminaux gérés pour le travail, ils sont provisionnés avec un profil professionnel qui a recours à l'utilisation personnelle et professionnelle. Pour plus d'informations, consultez la rubrique Présentation des modes des terminaux Android
- **Compte Google géré** – Se réfère au compte Google inscrit sur le terminal utilisé pour Android et fournit la gestion des applications Android via le Google Play. Ce compte est géré par le domaine qui gère votre configuration Android.
- **Compte Google Play géré** : pour les organisations qui souhaitent configurer Android, mais qui ne disposent pas de comptes G Suite ou de comptes Google gérés.

- **Compte de service Google** – Le compte de service Google est un compte Google spécial utilisé par les applications pour accéder aux API Google recommandées pour les clients de G Suite.
- **Jeton EMM** – ID unique que Workspace ONE UEM utilise pour connecter Workspace ONE UEM Console au compte Google géré.
- **Domaine Google géré** – Domaine demandé pour l'activation d'Android, associé à votre entreprise.
- **Configuration du domaine Google** – Processus Google pour demander un domaine Google géré.
- **AirWatch Relay** – L'application Workspace ONE UEM permet aux administrateurs d'enrôler par lots des terminaux Android dans Workspace ONE UEM.
- **Bump NFC** : technologie de communication qui permet à des terminaux que l'on fait s'entrechoquer d'échanger des informations. Cette opération est effectuée lors de l'utilisation de l'application AirWatch Relay pour transmettre les informations du terminal parent au terminal enfant.
- **Réseau AOSP/fermé** : les réseaux Android Open Source Project ou fermés font référence aux terminaux Android sans Google Mobile Services (GMS) et aux environnements de console sans accès à Google.
- **Enrôlement basé sur l'utilisateur et sur le terminal** : choisissez si le compte Google sur le terminal doit être lié à chaque session d'enrôlement (basé sur le terminal) ou à chaque compte utilisateur d'enrôlement (basé sur l'utilisateur).
- **Cap and Grow** : Cap and Grow vous permet de continuer à utiliser votre déploiement de terminal actuel lorsque vous effectuez la transition d'Android (hérité) vers Android Enterprise. Tout nouveau déploiement de terminal peut être enrôlé dans Android Enterprise et géré avec des terminaux plus anciens. Pour plus d'informations, reportez-vous à Migration de l'administrateur du terminal Android (hérité).

Présentation des modes des terminaux Android

Les fonctions de gestion intégrées d'Android permettent aux administrateurs de gérer entièrement les terminaux utilisés exclusivement pour le travail.

Android propose plusieurs modes en fonction de la propriété du terminal en cours d'utilisation au sein de votre organisation :

- Le **Profil professionnel** : permet de créer un espace dédié sur le terminal pour les applications et les données professionnelles. Il s'agit du déploiement idéal pour les applications BYOD (Bring Your Own Device).

- **Terminaux gérés pour le travail** : permet à Workspace ONE UEM et aux administrateurs informatiques de contrôler totalement le terminal et d'appliquer un large éventail de contrôles de la stratégie non disponibles pour les profils professionnels, mais limite l'utilisation du terminal à un usage professionnel.
  - **Terminaux professionnels et personnels** : fait référence aux terminaux professionnels. À l'instar des terminaux gérés pour le travail, ils sont provisionnés avec un profil professionnel qui a recours à l'utilisation personnelle et professionnelle.
  - **Terminaux gérés pour le travail sans Google Play Services** : si vous utilisez Workspace ONE UEM sur des terminaux AOSP (Android Open Source Project) ou sur des terminaux non-GMS, ou que vous utilisez des réseaux fermés au sein de votre entreprise, vous pouvez enrôler vos terminaux Android à l'aide du flux d'enrôlement de terminaux gérés pour le travail sans Google Play Services.

Fonctionnalité du mode Profil professionnel

Les applications dans le mode Profil professionnel se différencient par une icône de porte-documents rouge. Appelées applications badgées, elles s'affichent dans un seul et même lanceur avec les applications personnelles de l'utilisateur. Par exemple, votre terminal affiche une icône personnelle pour Google Chrome et une icône distincte pour Work Chrome marquée avec le badge. L'utilisateur final peut penser qu'il s'agit de deux applications différentes. En fait, l'application n'est installée qu'une seule fois, mais les données professionnelles sont stockées séparément des données personnelles.

Workspace ONE Intelligent Hub est badgé et n'existe que dans l'espace de données Profil professionnel. Il n'existe aucun contrôle sur les applications personnelles, et Workspace ONE Intelligent Hub n'a pas accès aux informations personnelles.

Quelques applications système sont incluses par défaut dans le profil professionnel : Work Chrome, Google Play, Google Settings, Contacts et Camera, par exemple. Ces applications peuvent être masquées à l'aide d'un profil de restrictions.

Certains paramètres indiquent la séparation entre les configurations personnelles et professionnelles. Des configurations différentes s'affichent pour les paramètres suivants :

- **Identifiants** – Affiche les certificats d'entreprise pour l'authentification des utilisateurs sur les terminaux gérés.
- **Comptes** – Affiche le compte Google géré lié au profil professionnel.
- **Applications** – Répertorie toutes les applications installées sur le terminal.
- **Sécurité** – Affiche le statut de chiffrement du terminal.

Fonctionnement du mode Terminaux gérés pour le travail

Lorsque les terminaux sont enrôlés en mode Terminaux gérés pour le travail, un mode de propriété professionnelle réel est créé. Workspace ONE UEM contrôle l'intégralité du terminal, et il n'existe aucune séparation entre les données personnelles et professionnelles.

Les choses importantes à prendre en compte pour le mode Terminaux gérés pour le travail sont :

- L'écran d'accueil n'affiche pas les applications badgées comme dans le mode Profil professionnel.
- Les utilisateurs ont accès à différentes applications préchargées lorsque le terminal est activé. Les applications supplémentaires peuvent uniquement être approuvées et ajoutées via Workspace ONE UEM Console.
- Workspace ONE Intelligent Hub est défini comme administrateur du terminal dans les paramètres de sécurité. Il ne peut pas être désactivé.
- Le désenrôlement du terminal du mode Terminaux gérés pour le travail demande une réinitialisation du terminal aux paramètres d'usine.

Terminal géré pour le travail sans Google Play Services

Si vous utilisez Workspace ONE UEM sur des terminaux AOSP (Android Open Source Project) ou sur des terminaux non-GMS ou que vous utilisez des réseaux fermés au sein de votre entreprise, vous pouvez enrôler vos terminaux Android à l'aide du flux d'enrôlement de terminaux gérés pour le travail sans Google Play Services. Vous pouvez héberger des applications sur l'intranet de votre entreprise et utiliser des méthodes d'enrôlement spécifiques OEM pour le déploiement.

Vous devrez spécifier dans UEM Console que vous utilisez un réseau AOSP/fermé lors de l'enregistrement EMM Android. Pour plus d'informations, reportez-vous à Inscription EMM pour Android avec un compte Google Play géré.

Éléments à prendre en compte lors de l'utilisation d'un terminal géré pour le travail sans Google Play Services sur des déploiements de réseaux AOSP/fermés :

- Si vous avez déjà configuré Android dans un groupe organisationnel parent et que vous souhaitez déployer un réseau AOSP/fermé dans un groupe organisationnel enfant spécifique, l'administrateur UEM Console dispose d'une option pour spécifier que les enrôlements Out-Of-Box sur le groupe organisationnel enfant ne disposeront pas d'un compte Google géré. Pour plus d'informations, reportez-vous à Terminaux et utilisateurs/Android/Inscription EMM pour Android dans l'enregistrement EMM Android.
- Si vous déployez des terminaux à l'aide de Workspace ONE UEM 1907 et version antérieure, aucune configuration d'UEM console n'est requise.
- Si vous déployez des terminaux à l'aide de Workspace ONE UEM 1908 et versions ultérieures, vous devez configurer les paramètres sur la page Chapitre 2 Inscription pour Android avec Workspace ONE UEM.
- Les méthodes d'enrôlement prises en charge sont les suivantes :
  - Code QR
  - StageNow pour les terminaux Zebra
  - Honeywell Enterprise Provisioner pour les terminaux Honeywell

- L'enrôlement via l'identifiant VMware Workspace ONE Intelligent Hub n'est pas pris en charge sur les terminaux AOSP.
- Le profil de mise à jour automatique publique n'est pas pris en charge. Ce profil est spécifiquement destiné aux applications publiques et ne fonctionne pas sur les terminaux qui se trouvent sur des réseaux AOSP ou fermés.
- Le profil de protection contre la réinitialisation aux paramètres d'usine n'est pas pris en charge.
- Les applications internes (hébergées dans Workspace ONE UEM Console) se déploient de manière silencieuse sur les terminaux sur réseaux AOSP/fermés.
- Les terminaux gérés pour le travail enrôlés sans compte Google géré ne doivent pas être attribués à des applications publiques et ne doivent pas être pris en compte dans les calculs de terminaux attribués à des applications publiques.
- Version du système d'exploitation et exigences OEM pour les terminaux gérés pour le travail sans Google Play Services :
  - AOSP (non-GMS)
    - Zebra et Honeywell : ils doivent se trouver sur une version de système d'exploitation qui prend en charge l'enrôlement de StageNow ou Honeywell Enterprise Provisioner.
    - Autres OEM : non pris en charge sauf si OEM développe sa prise en charge via un client tel que StageNow ou en autorisant les utilisateurs à accéder à l'enrôlement par code QR.
  - Réseau fermé
    - Zebra et Honeywell : Android 7.0 et versions ultérieures ou ils doivent se trouver sur une version de système d'exploitation qui prend en charge StageNow (version 7 0 ou version ultérieure) ou sur l'enrôlement de Honeywell Enterprise Provisioner.
    - Autres OEM : Android 7.0 ou versions ultérieures, car l'enrôlement par code QR est la seule méthode prise en charge.

Mode Terminaux professionnels et personnels (COPE)

Lorsque les terminaux sont enrôlés à l'aide du mode COPE, vous contrôlez toujours l'intégralité du terminal. Le mode COPE vous procure une capacité unique : il vous permet d'appliquer deux ensembles distincts de politiques, telles que les restrictions, pour le terminal et au sein d'un profil de travail.

Le mode COPE est uniquement disponible sur les terminaux Android 8.0 et versions ultérieures. Si vous enrôlez des terminaux Android sous Android 8.0, le terminal s'enrôle automatiquement en tant que terminal entièrement géré.

Certaines mises en garde doivent être prises en compte concernant l'enrôlement des terminaux en mode COPE :

- Pour les nouveaux enrôlements avec Android 11, vous devez utiliser Workspace ONE Intelligent Hub 20.08 pour Android et Workspace ONE UEM console 2008. Pour obtenir des informations spécifiques, reportez-vous à Modifications apportées aux terminaux professionnels et personnels (COPE) dans Android 11.
- Le chiffrement basé sur le code PIN et l'authentification unique Workspace ONE UEM à l'aide du SDK ne sont pas pris en charge pour les terminaux professionnels et personnels. Un code d'accès professionnel peut être appliqué pour s'assurer que l'utilisation d'applications professionnelles nécessite l'utilisation d'un code d'accès.
- Le préenrôlement d'un utilisateur unique et le préenrôlement de plusieurs utilisateurs ne sont pas pris en charge pour les enrôlements COPE.
- Les applications internes (hébergées dans Workspace ONE UEM) et les applications publiques déployées sur les terminaux COPE sont affichées dans l'application Catalog du profil professionnel.
- Comme pour les enrôlements en mode Profil professionnel uniquement, les terminaux professionnels et personnels permettent aux utilisateurs de désactiver le profil professionnel (par exemple, si l'utilisateur est en congé). Lorsque le profil professionnel est désactivé, les applications professionnelles n'affichent plus de notifications et ne peuvent pas être lancées. L'état (activé ou désactivé) du profil professionnel est présenté à l'administrateur sur la page Détails du terminal. Lorsque le profil professionnel est désactivé, les informations les plus récentes sur les applications et le profil ne peuvent pas être extraites du profil professionnel.
- Workspace ONE Intelligent Hub existe dans les sections Entièrement géré et Profil professionnel du terminal professionnel et personnel. Puisqu'elles existent à la fois au sein du profil professionnel et en dehors de celui-ci, les politiques de gestion peuvent être appliquées au sein du profil professionnel et à tout le terminal. Toutefois, Workspace ONE Intelligent Hub n'est visible que dans le profil professionnel.
- Lorsque des notifications Push sont envoyées au terminal, Workspace ONE Intelligent Hub en dehors du profil professionnel est temporairement disponible pour permettre à l'utilisateur d'afficher les messages, garantissant ainsi qu'il reçoit les messages critiques, même si le profil professionnel est temporairement désactivé.
- Les profils attribués peuvent être affichés par le biais de Workspace ONE Intelligent Hub, dans le profil professionnel.
- Les politiques de conformité pour la gestion d'applications (telles que Bloquer/Supprimer des applications) sont uniquement prises en charge pour les applications dans le profil professionnel. Les applications peuvent être mises sur liste noire sur le terminal (en dehors du profil professionnel) en utilisant les profils de contrôle des applications.
- Un effacement des données professionnelles réinitialisera les terminaux professionnels et personnels aux paramètres d'usine.
- Le provisionnement de produit n'est pas pris en charge sur les inscriptions COPE.

- **Modifications propres à Android 11** :
  - Les applications internes (hébergées par Workspace ONE UEM) ne peuvent plus être transférées vers le côté personnel du terminal. Les applications internes (en tant qu'applications privées) et les applications publiques doivent être déployées uniquement avec le profil professionnel.
    - Les autres fonctionnalités, par exemple les règles de conformité reposant sur des applications internes, ne sont plus prises en charge.
  - La méthode d'enrôlement afw#hub n'est plus prise en charge.
    - Il est préférable d'utiliser l'enrôlement par code QR ou sans contact.
  - Si votre entreprise a besoin de plus de temps pour effectuer des tests, il existe deux options pour retarder la mise à niveau de vos terminaux vers Android 11. Voir Gérer les mises à jour système pour les terminaux Android.

    Pour obtenir des informations spécifiques, reportez-vous à Modifications apportées aux terminaux professionnels et personnels (COPE) dans Android 11.

Migration de l'administrateur du terminal Android (hérité)

L'administrateur du terminal est la méthode héritée d'enrôlement des terminaux Android avec Workspace ONE UEM console après l'introduction dans Android 5.0 des modes Terminaux gérés pour le travail et Profil professionnel d'Android. Les clients enrôlés dans Workspace ONE UEM à l'aide du déploiement Android (hérité) peuvent migrer vers Android Enterprise pour bénéficier de la fonctionnalité de terminal pour l'entreprise.

Cette section fournit des informations et les meilleures pratiques sur la façon de passer du déploiement Android (hérité) à Android Enterprise.

Google a abandonné certaines API d'administrateur de terminal en faveur de la fonctionnalité la plus récente, car l'administrateur des terminaux n'est pas apte à prendre en charge les besoins actuels de l'entreprise. Les clients Workspace ONE UEM peuvent adopter le mode Terminaux gérés pour le travail (idéal pour les terminaux d'entreprise), le mode Profil professionnel (idéal pour les déploiements de terminaux personnels BYOD) et le mode Terminaux professionnels et personnels (COPE) pour gérer leurs terminaux Android en migrant d'Android (hérité) vers Android Enterprise. Pour plus d'informations sur les modes de terminaux, reportez-vous à Présentation des modes des terminaux Android.

Avez-vous d'autres questions ? Consultez nos sections Questions fréquentes à propos de la migration Android (héritée) pour obtenir de l'aide.

Migration d'Android (hérité) vers Android Enterprise en mode géré par Work à l'aide de terminaux Android Zebra

Les terminaux Zebra exécutant Android 7 ou une version ultérieure et MXMF 7 ou version une ultérieure prennent en charge une migration d'Android (hérité) vers le mode géré par Work d'Android Enterprise. Les fonctionnalités de migration de ce flux incluent :

- La migration est effectuée à distance et en mode silencieux.
- Les terminaux ne se mettent pas hors tension, ne redémarre pas ou ne se réinitialisent pas pendant la migration, ce qui garantit que les données des applications restent intactes.
- La connectivité Wi-Fi est maintenue pendant la migration.
- Les produits qui ne contiennent pas de profils restent installés.
- La migration vers le mode réseau AOSP/fermé est entièrement prise en charge.

Pour commencer, reportez-vous à Migration vers l'enrôlement géré par Work à l'aide de l'outil de migration Android hérité.

Migrer d'Android (hérité) vers Android Enterprise avec des terminaux personnels (BYOD)

Workspace ONE UEM console fournit un processus transparent qui vous permet de migrer tous les terminaux Android (hérité) vers un Profil professionnel pour Android Enterprise. Les fonctionnalités de migration de la console UEM vous aident à vous assurer que :

- Votre administration héritée reste intacte jusqu'à ce que la migration soit terminée.
- Les terminaux non migrés ne sont jamais affectés.
- Identifiez les terminaux qui sont terminés, en cours et attribués.
- Créez des Smart Groups de pré-enrôlement ou de test pour vous assurer que tous les terminaux utilisateur migrent correctement avant de procéder à la migration complète de votre parc de terminaux.

Pour commencer, reportez-vous à Migration vers un profil professionnel depuis Android (hérité) à l'aide de l'outil de migration.

Migrer d'Android (hérité) vers Android Enterprise avec des terminaux d'entreprise

Vous pouvez migrer d'Android (hérité) vers Android Enterprise avec vos terminaux d'entreprise en mode Terminaux gérés pour le travail ou en mode Terminaux professionnels et personnels (COPE). Les options d'enrôlement et de migration varient selon le système d'exploitation Android, le type de terminal et si les terminaux ont accès aux services Google. Ce scénario est préférable pour la migration de terminaux Android non-Zebra.

Les options de migration et d'enrôlement sont les suivantes :

- Utiliser l'enrôlement entièrement géré pour les terminaux Android 8.0+. Pour commencer, reportez-vous à Migrer vers Android Enterprise à l'aide de l'enrôlement rationalisé
- Utiliser Knox Mobile Enrollment pour les terminaux Samsung Android 8.0+. Pour commencer, reportez-vous à la documentation Samsung Knox Mobile Enrollment.
- Suivez la stratégie Cap and Grow et continuez à utiliser vos terminaux Android actuels enrôlés via Android (hérité). Une stratégie Cap and Grow signifie que tout nouveau déploiement de terminal est automatiquement enrôlé dans Android Enterprise et géré simultanément avec les anciens déploiements (Android (hérité)) jusqu'à ce que votre organisation soit prête à déplacer tous les terminaux vers Android Enterprise.

Migrer d'Android (hérité) vers Android Enterprise sans les services Google

Si vous êtes actuellement enrôlé dans Workspace ONE UEM avec des terminaux Android déployés via Android (hérité) et que vous souhaitez basculer vers Android Enterprise sans les services Google, nous proposons une prise en charge de réseaux fermés pour les terminaux d'entreprise et l'enrôlement non géré pour terminaux personnels BYOD.

Si vous disposez d'un terminal qui n'a pas de connectivité réseau ou si le terminal peut se connecter à un réseau mais qu'il n'a pas de services Google (un terminal non GMS), vous pouvez enrôler ces terminaux dans Android Enterprise en mode Terminaux gérés pour le travail, puis transférer des applications internes et appliquer des stratégies avec des profils Android.

Si vous avez un terminal qui dispose d'une connectivité réseau mais qui a un accès restreint aux services Google, par exemple les terminaux en Chine, vous pouvez utiliser la prise en charge de réseaux fermés pour les terminaux d'entreprise. Pour les terminaux personnels (BYOD), vous pouvez utiliser le mode MAM uniquement basé sur SDK, appelé mode Enregistré, pour activer l'enrôlement non géré des terminaux Android.

Pour plus d'informations sur la prise en charge de réseaux fermés pour les terminaux d'entreprise, Reportez-vous à Terminaux et utilisateurs/Android/Enregistrement EMM Android pour configurer ces paramètres.

Pour configurer vos terminaux personnels (BYOD) sans les services Google, reportez-vous à Activer l'enrôlement non géré pour les terminaux Android pour connaître les étapes de l'enrôlement.

Impact sur les API

Google a abandonné certaines API d'administrateur de terminal en faveur de la fonctionnalité la plus récente, car l'administrateur des terminaux n'est pas apte à prendre en charge les besoins actuels de l'entreprise. Les API suivantes disponibles avec l'administrateur de terminal ne fonctionnent plus sur les terminaux exécutant Android 10 et versions ultérieures. Les terminaux restant sur Android 9.0 et versions antérieures ne sont pas affectés :

- USES_POLICY_DISABLE_CAMERA

- USES_POLICY_DISABLE_KEYGUARD_FEATURES
- USES_POLICY_EXPIRE_PASSWORD
- USES_POLICY_LIMIT_PASSWORD

Créer un Smart Group pour migrer d'Android (hérité) vers un profil professionnel Android

Les clients Workspace ONE UEM actuellement déployés sous Android (hérité) peuvent migrer vers le mode de profil professionnel Android pour gérer leurs terminaux Android. Ce cas d'utilisation vous guide à travers les étapes de création de Smart Groups, de création d'une nouvelle migration et de suivi de l'état de la migration.

Workspace ONE UEM Console fournit un processus transparent qui vous permet de créer des Smart Groups afin de migrer tous les terminaux Android (hérité) vers un déploiement de profil professionnel Android.

Conditions préalables

Avant de procéder à la migration, vous devrez créer des Smart Groups pour tous les terminaux à migrer. Vous pouvez créer des groupes distincts pour le préenrôlement d'un petit nombre de terminaux à des fins de test avant le déploiement sur tous vos terminaux.

Procédure

1. Sélectionnez le **Groupe organisationnel (GO)** auquel votre nouveau Smart Group s'appliquera et à partir duquel il sera géré. La sélection d'un GO est facultative.
2. Accédez à **Groupes et paramètres > Groupes > Groupes d'attribution**, puis cliquez sur **Ajouter un Smart Group**.
3. Saisissez un **nom** pour le Smart Group.
4. Configurez le type de Smart Group :
   - **Critères** : cette option fonctionne mieux pour les groupes comprenant un grand nombre de terminaux (plus de 500) qui reçoivent des mises à jour générales. Cette méthode fonctionne mieux, car les détails propres à ces groupes peuvent atteindre tous les points de terminaison de votre flotte mobile.
   - **Terminaux ou utilisateurs** : cette option fonctionne mieux pour les groupes comprenant un plus petit nombre de terminaux (500 ou moins) qui reçoivent des mises à jour ponctuelles, néanmoins importantes. Cette méthode fonctionne mieux, car vous pouvez sélectionner les membres du groupe à un niveau granulaire.

   Note Basculer entre les deux types de Smart Group efface toutes les entrées et sélections que vous avez pu faire.

   Au moins un terminal déployé en tant qu'Android (hérité) doit être sélectionné comme éligible pour la migration ou vous obtiendrez des erreurs lors de la configuration de la migration.

5 Cliquez sur **Enregistrer**.

Étape suivante

Une fois vos Smart Groups créés, vous pouvez parcourir les pré-requis pour commencer la migration.

Conditions préalables à la migration vers Android Enterprise pour la migration du profil Work Android (hérité)

Pour fournir une expérience utilisateur intuitive de la migration, cette page vous guide à travers une migration réussie. Ne pas exécuter ces étapes peut entraîner l'échec de la migration ou bloquer l'accès des utilisateurs à toutes les applications dont ils ont besoin.

Éligibilité du terminal

Le terminal doit être éligible pour la migration. Par exemple. Les terminaux Samsung sur lesquels Knox Container est activé ne peuvent pas être migrés.

Vérifiez l'éligibilité pour la migration en accédant à **Informations sur le terminal > Attributs personnalisés** et définissez l'attribut `sure migration.eligible` sur la valeur `True`.

Recréer des profils pour Android

Les profils Android Enterprise sont distincts des profils d'administrateur de terminal ou Android (hérité). Vous devez recréer des profils pour Android Enterprise. Ces profils peuvent être configurés après la fin de l'enregistrement d'Android Enterprise.

Sur les consoles UEM de version inférieure à la version 9.4.0, les profils Android Enterprise sont disponibles sous `Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android > Android for Work`.

Sur les consoles UEM 9.4.0 et versions ultérieures, les profils Android Enterprise sont disponibles sous `Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android`.

Note Si le profil Wi-Fi a été configuré pour votre déploiement Android (hérité), vous devez créer et attribuer un profil Wi-fi Android aux terminaux sélectionnés pour la migration avant d'en créer une.

Les profils de terminaux Android garantissent la bonne utilisation des terminaux, la protection des données sensibles et un bon fonctionnement de l'espace de travail. Les profils remplissent de nombreuses fonctions : ils permettent notamment de mettre en œuvre les règles et procédures internes, ou de configurer et de préparer des terminaux Android selon l'utilisation souhaitée.

Configurer la gestion d'applications

Une fois qu'une application a été ajoutée à Workspace ONE UEM console, elle peut être distribuée à l'administrateur de terminaux (enrôlements Android (hérité) et Android Enterprise). Si une application publique a été ajoutée à UEM Console avant l'enregistrement d'Android Enterprise, la section relative à la gestion des applications de ce guide vous aidera à configurer les paramètres pour qu'il n'y ait aucune interruption des attributions d'application existantes.

Les applications internes ne peuvent pas être gérées en mode de gestion des profils professionnels sous Android Enterprise. Pour faire en sorte que les applications internes soient disponibles pour les terminaux qui ont migré vers le mode de gestion des profils professionnels, vous devez charger l'application vers la console Google gérée en tant qu'application privée avant la migration.

Utilisez Workspace ONE UEM pour gérer le déploiement et la maintenance d'applications mobiles disponibles publiquement depuis Google Play Store. Assurez-vous que chaque application publique est approuvée pour votre organisation afin de garantir une migration transparente.

Vérifier les paramètres réseau

La configuration réseau requise pour Android est une liste de points de terminaison connus pour les versions actuelles et antérieures des API de gestion d'entreprise. Vérifiez vos paramètres réseau afin d'assurer une connexion entre Workspace ONE, Google Play Store et les terminaux Android. Pour plus d'informations, reportez-vous à Configuration réseau requise pour Android.

Gérer les applications publiques pour la migration Android (hérité)

Si une application publique a été ajoutée à UEM console avant la migration Android (hérité) et l'enregistrement Android d'entreprise, cette tâche vous aide à vérifier que toutes les applications sont importées après la migration.

Ces étapes vérifient simplement que la console UEM est informée que l'application a été approuvée sur la fonction Google Play gérée. Il est maintenant possible d'attribuer cette application à des enrôlements Android Enterprise une fois la migration terminée.

Procédure

1. Accédez à https://Play.google.com/work (connectez-vous avec le même compte Gmail utilisé pour configurer Android Enterprise), recherchez les applications et approuvez-les pour votre organisation.
2. Dans la console UEM, accédez à `Applications et livres > Natives > Publiques > Ajouter une application > Android > Importer depuis Play`.
3. Sélectionnez Importer une fois que la liste des applications approuvées s'affiche.

   Après la migration, le cache de l'application est effacé et les utilisateurs devront entrer de nouveau les informations d'identification.

Migration vers l'enrôlement géré par Work à l'aide de l'outil de migration Android hérité

Workspace ONE UEM console permet de migrer vos terminaux de l'administrateur du terminal ou Android (hérité) vers le mode géré par Work avec Android Enterprise avec l'outil de migration héritée.

L'outil de migration Android héritée vous permet de remplir toutes les conditions préalables, de sélectionner des Smart Groups et de charger les certificats de migration. Il fournit également un tableau de bord permettant d'afficher une page récapitulative des terminaux migrés, y compris l'état d'admissibilité et le motif des échecs ou réussites.

Note Ne mettez pas les terminaux hors tension pendant la migration.

Conditions préalables

Veillez à remplir les conditions préalables pour éviter l'échec de la migration ou le blocage de l'accès à toutes les applications dont les utilisateurs ont besoin. Pour plus d'informations sur les conditions préalables, consultez : Conditions préalables à la migration vers un terminal géré par Work à l'aide de l'outil de migration hérité.

Procédure

1 Accedez à **Terminaux > Cycle de vie > Migration Android héritée > Nouveau >** et sélectionnez **Géré par Work** dans la fenêtre **Sélectionner le type de migration**.

Sélectionnez

2 Remplissez les conditions préalables et sélectionnez **Suivant** pour passer au **Détails**, afin de sélectionner les Smart Groups que vous souhaitez migrer :

Paramètre	Description
Nom	Saisissez un nom convivial pour le groupe de migration.
Description	Saisissez une description détaillée du groupe de migration.
Smart Groups	Spécifiez les Smart Groups qui doivent recevoir la migration. Les Smart Groups doivent inclure des déploiements Android (hérité). Vous recevrez un message d'erreur si un Smart Group n'est pas éligible à la migration.
Certificat de migration	Sélectionnez le bouton **Télécharger** pour télécharger le certificat de migration de vos terminaux Zebra. Contactez l'assistance Zebra pour récupérer un certificat pour votre entreprise, ce qui est nécessaire du point de vue de la sécurité pour garantir l'intégrité de la migration.

3 Sélectionnez **Valider** pour récupérer le nombre de terminaux éligibles pour la migration.

La migration peut prendre plusieurs minutes.

Sur la page suivante, UEM console affiche la liste des terminaux éligibles. Pour poursuivre la migration, cliquez sur **Créer**.

Résultats

Une liste d'attributions de migration s'affiche. Vous pouvez cliquer sur chacune d'entre elles pour afficher des détails supplémentaires et vérifier l'état de la migration de chaque terminal.

Sur le terminal, Workspace ONE Intelligent Hub pour Android s'affiche et s'épingle sur l'écran d'accueil lors de la migration, puis supprime l'épinglage une fois la migration terminée.

Étape suivante

Reportez-vous à la Page Détails de la migration pour obtenir des informations supplémentaires.

Conditions préalables à la migration vers un terminal géré par Work à l'aide de l'outil de migration hérité

Pour fournir une expérience utilisateur intuitive de la migration, cette page vous guide à travers une migration réussie. Ne pas exécuter ces étapes peut entraîner l'échec de la migration ou bloquer l'accès des utilisateurs à toutes les applications dont ils ont besoin.

Configuration logicielle requise

- VMware Workspace ONE UEM 2006 ou version ultérieure
- Workspace ONE Intelligent Hub 20.05 pour Android et Zebra MX Service 4.8 pour Android.

Si vous utilisez des fichiers APF pour la mise à niveau ou l'enrôlement du Hub, la version de l'administrateur de terminaux Android (hérité), répertoriée comme DA, du fichier APF doit être utilisée pour l'enrôlement et la version gérée par Work (Android Enterprise), répertoriée comme DO, doit être utilisée pour la mise à niveau.

Device Requirements

Terminal Zebra exécutant Android 7 et les versions ultérieures et MXMF 7 et les versions ultérieures. Le terminal doit être enrôlé dans le mode Android hérité (administrateur de terminaux).

Comptes Google

Les comptes Google ne peuvent pas être présents sur le terminal, car cela entraîne l'échec de la migration. Supprimez tous les comptes Google avant la migration.

Certificat de migration

Contactez l'assistance Zebra pour récupérer un certificat pour votre entreprise, ce qui est nécessaire du point de vue de la sécurité pour garantir l'intégrité de la migration. En général, les certificats ont une durée de vie courte (30 à 90 jours). Le certificat doit être au format `.pem`.

Zebra peut demander les informations suivantes pour la génération de certificats :

- Application effectuant la migration : **Zebra MX Service**

- Application migrée vers le mode géré par Work : **Workspace ONE Intelligent Hub pour Android**
- nom du client

Enregistrement EMM Android

Configurez l'enregistrement EMM pour Android dans votre environnement pour activer l'enrôlement et la migration des terminaux vers Android Enterprise Pour plus d'informations, reportez-vous à Chapitre 2 Inscription pour Android avec Workspace ONE UEM.

Profils et produits

Les profils Android Enterprise sont distincts des profils d'administrateur de terminal ou Android (hérité). Vous devez recréer des profils pour Android Enterprise. Ces profils peuvent être configurés après la fin de l'enregistrement d'Android Enterprise.

Les profils devront être recréés sous Android et le produit contenant les profils hérités doit être modifié ou désactivé et remplacé.

Éligibilité à la migration

Deux nouveaux attributs personnalisés, `migration.do.eligible` et `migration.do.ineligibilityReason`, sont signalés à la console. Si `migration.do.eligible` est défini sur « Vrai », le terminal peut migrer. La console vérifie automatiquement cet attribut avant d'envoyer une commande de migration au terminal. Si la valeur est définie sur « Faux », vérifiez `migration.do.ineligibilityReason` pour obtenir des indications supplémentaires.

Smart Groups

Les migrations sont attribuées à des Smart Groups. Créez des groupes si nécessaire pour vos plans de migration.

Migration vers un profil professionnel depuis Android (hérité) à l'aide de l'outil de migration

Workspace ONE UEM console fournit un outil de migration qui vous permet de remplir toutes les conditions préalables, de sélectionner des Smart Groups et de configurer un message personnalisé pour les utilisateurs. Elle fournit également un tableau de bord permettant d'afficher une page récapitulative des terminaux migrés, y compris l'état d'admissibilité et la raison des échecs ou réussites.

Conditions préalables

Veillez à remplir les conditions préalables pour éviter l'échec de la migration ou le blocage de l'accès à toutes les applications dont les utilisateurs ont besoin. Pour plus d'informations sur les conditions préalables, consultez : Conditions préalables à la migration vers Android Enterprise pour la migration du profil Work Android (hérité) .

Procédure

1 Accédez à **Terminaux > Cycle de vie > Migration Android hérité** et sélectionnez **Nouvelle migration**.

2 Consultez les conditions préalables et sélectionnez **Suivant** pour passer à l'onglet **Détails**.

Détails	L'onglet Détails vous permet de sélectionner les Smart Groups que vous souhaitez migrer
Nom	Saisissez un nom convivial pour le groupe de migration.
Description	Saisissez une description détaillée du groupe de migration.
Smart Groups	Spécifiez les Smart Groups qui doivent recevoir la migration. Les Smart Groups doivent inclure des déploiements Android (hérité). Vous recevrez un message d'erreur si un Smart Group n'est pas éligible à la migration.
Message	Une fois que les collaborateurs ont choisi d'effectuer la mise à niveau vers Android Enterprise, ce message les informe de la migration et les invite à effectuer certaines actions pour continuer.

3 Sélectionnez **Valider**. Sélectionner Valider pour récupérer le nombre de terminaux éligibles pour la migration.

4 Sélectionnez **Continuer** une fois que tous les terminaux ont été validés pour la migration. Vous ne pouvez pas continuer tant qu'un Smart Group valide n'est pas sélectionné.

Une page **Résumé** affiche des détails tels que la liste des terminaux, l'éligibilité à la migration et la raison pour laquelle le terminal n'est pas éligible, lorsqu'il est appliqué.

5 Sélectionnez **Créer** pour créer la migration.

Une notification est envoyée aux terminaux éligibles dans les Smart Groups sélectionnés pour informer les utilisateurs de la migration et leur demander d'effectuer les actions nécessaires pour continuer. Vous pouvez suivre la progression sur la page Migration Android hérité. Depuis cette page, vous pouvez sélectionner les migrations dans la liste pour afficher la page Détails de la migration.

Note Lors d'une migration Android (hérité) vers Android Enterprise, en fonction du paramètre défini dans le planificateur, la commande de migration est automatiquement et instantanément envoyée pour la première taille de lot (300) de terminaux. Après les 300 premiers terminaux, les terminaux restants recevront la commande aux intervalles déterminés. Vous pouvez afficher les paramètres dans UEM Console sous **Administrateur > Planificateur**.

Étape suivante

Pour plus d'informations, consultez Page Détails de la migration

Migrer vers Android Enterprise à l'aide de l'enrôlement rationalisé

L'enrôlement rationalisé permet de configurer des terminaux Android en masse avec Workspace ONE UEM en tant que fournisseur EMM « out of the box » sans avoir à configurer manuellement chaque terminal. L'utilisation de l'enrôlement rationalisé avec votre migration Android (héritée) vous permet de mettre vos terminaux en mode entièrement géré avec facilité et de garantir que la migration est effectuée en toute sécurité.

TBD

Procédure

1. Configurez Workspace ONE UEM console en remplissant les conditions préalables pour la migration Android (héritée). Les étapes sont décrites Conditions préalables à la migration vers Android Enterprise pour la migration du profil Work Android (hérité) .
2. Effectuez l'enrôlement rationalisé pour ajouter vos terminaux dans le portail rationalisé. Pour commencer, reportez-vous à Enrôler un terminal Android à l'aide du portail Zero Touch
3. Effectuez un test et assurez-vous que le flux de migration fonctionne pour vos terminaux de test.

   Note Rappelez-vous qu'un profil Wi-Fi doit être créé pour que la migration aboutisse.
4. Envoyez une commande « Effacement du terminal » aux terminaux précédemment gérés sous Android (hérité).

Page Détails de la migration

Les pages **Détails de la migration** vous permettent de suivre la migration en fonction du groupe de migration, des détails, de l'état et de la liste des terminaux inclus dans la migration.

Affichage en liste de la migration Android hérité

L'affichage en liste de la migration Android hérité s'affiche automatiquement après la création d'une nouvelle page de migration. L'affichage en liste vous permet de voir en temps réel toutes les mises à jour de vos terminaux utilisateurs en cours de migration à l'aide de Workspace ONE UEM console. L'affichage en liste vous permet d'effectuer les opérations suivantes :

- Modifier des migrations spécifiques en sélectionnant la case d'option correspondant au nom convivial de migration souhaité. Vous pouvez mettre à jour la migration pour les nouveaux terminaux ajoutés au Smart Group en sélectionnant **Modifier**.
- Supprimer les groupes de migration qui empêchent les terminaux en file d'attente de migrer à partir d'Android hérité en retirant la notification persistante. Le profil professionnel Android n'est pas supprimé des terminaux qui ont déjà migré.
- Rechercher et réduire un terminal à l'aide de l'option Recherche.

Page Détails de la migration Android hérité

La page Détails de la migration est accessible en sélectionnant un nom convivial de migration dans l'affichage en liste des migrations Android hérité avec Workspace ONE UEM console pour vérifier l'état de la migration. Vous pouvez afficher une présentation graphique, l'état et la raison de l'échec ou de la réussite de la migration.

Utilisez la page Détails de la migration pour transférer le contrôle de la migration vers le terminal avec le bouton **Réessayer** si la migration échoue.

Personnalisez un message pour les terminaux du lot de migration à l'aide du bouton **Notifier**. Configurez le champ comme suit :

- **Type de message** : sélectionnez le type de message (e-mail, SMS ou Push) que Workspace ONE UEM utilise pour ce modèle.
- **Objet** : saisissez l'objet du message.
- **Corps du message** : saisissez le message à afficher par Workspace ONE UEM sur les terminaux des utilisateurs pour chaque type de message.

Questions fréquentes à propos de la migration Android (héritée)

Pour vous aider à mieux comprendre la migration Android (héritée), voici quelques questions fréquentes et les meilleures pratiques à appliquer pour réussir une migration.

Questions fréquentes

- **Lorsque j'active Android Enterprise dans un groupe organisationnel, cela a-t-il une incidence sur mes enrôlements d'administrateur de terminal existants ?**
  - Les enrôlements d'administrateur de terminal actuels restent enrôlés et reçoivent tous les profils et applications attribués. L'activation d'Android Enterprise n'affecte que les nouveaux enrôlements ; lorsqu'un nouveau terminal compatible Android Enterprise est enrôlé, il utilise Android Enterprise. Si un terminal n'est pas compatible Android Enterprise, il est enrôlé à l'aide de l'administrateur de terminaux.
- **L'administrateur de terminaux et Android Enterprise peuvent-ils cohabiter dans la même console UEM ?**
  - Les enrôlements d'administrateur de terminaux et les enrôlements d'Android Enterprise peuvent coexister dans le même groupe organisationnel. La gestion des profils est séparée, avec les enrôlements Android et Android (hérité) pour Android Enterprise d'un côté, et pour l'administrateur de terminaux de l'autre côté.

    En outre, avec UEM console v9.2.0+, il est possible de remplacer les enrôlements d'Android Enterprise pour des groupes d'organisation spécifiques, ou même de les limiter à des Smart Groups spécifiques.
- **Puis-je utiliser le provisionnement de produits avec Android Enterprise ?**
  - Le provisionnement de produit est pris en charge sur les terminaux entièrement gérés.

- **Des capacités de gestion spécifiques OEM sont-elles disponibles sur les terminaux enrôlés via Android Enterprise ?**
  - Des capacités de gestion spécifiques OEM sont possibles par l'intermédiaire de OEMConfig. Les OEM tels que Samsung et Zebra ont créé des applications publiques qui peuvent être ajoutées à Workspace ONE UEM console. Ces applications fournissent des paires clé-valeur de configuration d'application qui peuvent modifier les capacités du terminal.
- **Workspace ONE Assist fonctionne-t-il avec Android Enterprise ?**
  - Workspace ONE Assist est compatible avec toutes les options d'enrôlement d'Android Enterprise.
- **Les nouveaux clients peuvent-ils utiliser Android (hérité) ?**
  - Les nouveaux clients Workspace ONE UEM doivent configurer Android Enterprise pour déployer des terminaux Android.
  - Les clients existants peuvent désactiver et réactiver Android (hérité) comme ils le souhaitent.

Meilleures pratiques pour la migration Android (héritée)

Le meilleur moment pour la migration vers Android Enterprise dépend des besoins de votre entreprise, et le calendrier de la migration réelle dépend des cas d'utilisation de votre organisation. Voici quelques éléments à prendre en compte :

- Si vos terminaux actuels ne sont pas susceptibles de recevoir Android 10 ou si les mises à jour du système d'exploitation sont contrôlées par votre organisation, il n'est pas nécessaire de migrer ces terminaux. Vous pouvez déployer Android Enterprise pour les terminaux récemment achetés.
- Les terminaux personnels (BYOD) sont les plus vulnérables, car les utilisateurs finaux peuvent mettre à jour leurs terminaux vers le dernier système d'exploitation. Une migration d'administrateur de terminal vers un profil professionnel peut être effectuée à l'aide de la fonctionnalité de migration Android héritée dans Workspace ONE UEM console. Pour commencer, reportez-vous à Migration vers un profil professionnel depuis Android (hérité) à l'aide de l'outil de migration.

Inscription pour Android avec Workspace ONE UEM

2

Pour commencer à gérer les terminaux Android, vous devrez inscrire Workspace ONE UEM comme fournisseur de gestion de la mobilité d'entreprise (EMM, Enterprise Mobility Management) avec Google. La page de démarrage dans Workspace ONE UEM Console fournit une solution détaillée pour configurer les outils de gestion d'entreprise nécessaires pour sécuriser et gérer votre flotte de terminaux.

Il existe deux façons de configurer Android : en utilisant un compte Google Play géré (solution préférée) ou à l'aide d'un domaine Google géré (solution recommandée par Google pour les clients de la suite d'outils G Suite). Un compte Google Play géré est utilisé si votre entreprise n'utilise pas G Suite. Il permet plusieurs configurations d'Android au sein de votre organisation à l'aide d'un compte Google personnel. Workspace ONE UEM permet de gérer ce compte et ne nécessite aucune synchronisation Active Directory ni vérification Google.

La configuration d'Android à l'aide du domaine Google géré (G Suite) nécessite que votre entreprise configure un domaine Google. Elle doit également suivre une procédure de vérification pour prouver que vous possédez le domaine. Ce domaine peut uniquement être lié à un compte EMM vérifié. La configuration consiste notamment à créer un compte de service Google et à configurer Workspace ONE UEM en tant que fournisseur EMM. Pensez à créer un compte Google spécialement pour Android pour votre organisation afin d'éviter tout conflit avec des comptes Google existants.

Note Lorsque vous créez un compte Google pour le domaine Google géré, il est considéré comme le compte administrateur de votre domaine. Songez à ajouter des utilisateurs supplémentaires (comptes Google) pour vous aider à gérer les tâches dans le Google Play géré. Ajouter des comptes Google est utile en cas d'expiration du compte Google principal. S'il expire, vous pouvez toujours accéder au domaine Google géré et éviter les comportements indésirables.

Vous pouvez créer et attribuer des rôles pour votre domaine Google géré. Reportez-vous à la section Attribuer des rôles dans les entreprises.

Le compte de service Google est un compte Google spécial qui est utilisé par les applications pour accéder aux API Google. Il est obligatoire lors de la configuration d'Android à l'aide de la méthode de domaine Google géré pour votre entreprise. Les identifiants du compte de service Google sont automatiquement renseignés lors de la configuration des comptes Android si l'inscription est effectuée à l'aide d'un compte Google Play géré. Si vous rencontrez une erreur

lors de la configuration des comptes Android, effacez vos paramètres dans Workspace ONE UEM Console et réessayez. Vous pouvez également créer le compte manuellement. Pour les comptes Google, pensez à créer votre compte de service Google avant d'utiliser l'une ou l'autre méthode de configuration.

Pour modifier le compte Google ou apporter des modifications à vos paramètres d'administration, vous devez déconnecter le compte de Workspace ONE UEM Console.

Important La configuration d'Android inclut l'intégration d'outils tiers qui ne sont pas gérés par VMware. Les informations contenues dans ce guide concernant la console d'administration Google et Google Developer Console correspondent à la version disponible en janvier 2018. L'intégration avec un produit tiers n'est pas garantie et dépend du bon fonctionnement des solutions tierces.

Ce chapitre contient les rubriques suivantes :

Inscription EMM pour Android avec un compte Google Play géré

Workspace ONE UEM Console vous permet de suivre un processus de configuration simplifié pour relier UEM console à Google en tant que fournisseur EMM.

Conditions préalables

Si la page d'enregistrement Android EMM est bloquée, assurez-vous d'avoir activé les URL Google dans votre architecture réseau pour communiquer avec des points de terminaison internes et externes. Pour plus d'informations, reportez-vous à Configuration réseau requise pour Android.

Procédure

1. Accédez à **Démarrage > Workspace ONE > Enregistrement EMM Android**.
2. Sélectionnez **Configurer**. Vous êtes alors redirigé vers la page d'inscription EMM pour Android.
3. Sélectionnez **Inscrire avec Google**. Si vous êtes déjà connecté avec vos identifiants Google, vous êtes dirigé vers la page « Démarrer » de Google.

   Si votre organisation utilise plus d'un domaine, vous devrez enregistrer des domaines distincts.

   Pour plus d'informations sur AOSP ou sur l'utilisation sur un réseau fermé, reportez-vous à Présentation des modes des terminaux Android

4 Sélectionnez **Se connecter** si vous ne l'êtes pas déjà et entrez vos identifiants Google, puis sélectionnez **Démarrer**.

5 Saisissez le **nom de votre organisation**. Le champ fournisseur EMM (Enterprise Mobility Manager) se remplit automatiquement avec VMware Workspace ONE UEM.

6 Sélectionnez **Confirmer > Terminer l'inscription**. Vous êtes redirigé vers Workspace ONE Console et vos identifiants de connexion du compte de service Google sont automatiquement renseignés.

7 Sélectionnez **Enregistrer > Tester la connexion** pour vous assurer que le compte de service est correctement configuré et connecté.

Étape suivante

si vos paramètres dans UEM Console ont été effacés et que vous souhaitez procéder à l'inscription auprès de Google, un message s'affiche vous invitant à terminer la configuration. Vous êtes redirigé vers Workspace ONE UEM Console pour terminer la configuration.

Inscription EMM pour Android avec un domaine Google géré (clients G-Suite)

Vous devez effectuer plusieurs tâches manuelles, comme vérifier la propriété du domaine avec Google, obtenir un jeton EMM et créer un compte de service d'entreprise pour utiliser ce type de configuration.

Conditions préalables

Pour configurer votre compte avec un domaine Google géré, l'organisation doit configurer un domaine Google s'ils n'en utilisent pas déjà un.

Procédure

1 Accédez à **Démarrage > Workspace ONE > Enregistrement EMM Android**.

2 Sélectionnez **Inscrire** pour être redirigé vers l'assistant de configuration Android afin d'effectuer ces trois étapes :

   a Générer un jeton : obtenez votre jeton d'entreprise en inscrivant votre domaine d'entreprise auprès de Google.

   b Importer un jeton : entrez le jeton EMM dans l'Assistant de configuration Android.

   c Utilisateurs installés : configurez le mode de création des utilisateurs pour l'ensemble de votre entreprise.

3 Sélectionnez **Accéder à Google**. Vous êtes redirigé vers le site G Suite.

4 Inscrivez votre entreprise et vérifiez votre domaine.

Configurer un compte de service Google

Le compte de service Google est un compte Google spécial utilisé par les applications pour accéder aux API Google. Vous devez créer ce compte après avoir généré votre jeton EMM afin de pouvoir importer toutes les informations en même temps.

Procédure

1 Naviguez vers Google Cloud Platform – Google Developers Console.

2 Connectez-vous avec vos identifiants Google.

les identifiants Google de type Administrateur n'ont pas besoin d'être associés à votre domaine d'activité. Pensez à créer un compte Google spécialement pour Android pour votre organisation afin d'éviter tout conflit avec des comptes Google existants.

Note Envisagez d'ajouter des comptes supplémentaires de sorte que, si un compte expire pour cause d'inactivité, vous disposiez de comptes supplémentaires pour vous connecter et accéder à votre compte de service Google.

3 Utilisez le menu déroulant du menu Sélectionner un projet et sélectionnez **Nouveau projet**.

4 Entrez un **Nom de projet** pour créer votre projet API dans la fenêtre Nouveau projet. Pensez à utiliser Android EMM-NomSociété comme convention de dénomination.

5 Acceptez les conditions générales et sélectionnez **Créer**.

Votre projet est généré et Google Developer Console vous redirige vers la page API Manager.

6 Sélectionnez **Activer les API et les services** pour Android à partir du **Tableau de bord des API et des services**.

7 Recherchez et activez les API suivantes : **Google Play EMM** et **Admin SDK**.

Après avoir créé votre projet et activé les API, créez votre compte de service dans Google Developer's Console.

8 Naviguez vers **API et services > Identifiants > Créer des identifiants > Clé de compte de service > Nouveau compte de service**.

9 Définissez le **nom du compte de service** pour votre compte de service. Pensez à respecter la convention de dénomination Android et assurez-vous de noter le nom que vous choisissez car vous en aurez besoin dans les étapes suivantes.

10 Pour l'option **Rôle > Projet**, utilisez le menu déroulant pour sélectionner **Propriétaire**.

11 Sélectionnez le **Type de clé P12**.

12 Sélectionnez **Créer**. Le certificat d'identité est automatiquement créé et téléchargé sur votre disque local. assurez-vous d'enregistrer votre certificat d'identité et le mot de passe lorsque vous importez le certificat dans Workspace ONE UEM Console.

13 Sélectionnez **Gérer les comptes de service** dans la liste **Clés de compte de service** pour ouvrir la page Comptes de service.

14 Sélectionnez le bouton de menu (trois points verticaux) à côté de votre compte de service et sélectionnez **Modifier**.

15 Sélectionnez **Activer la délégation pour le domaine G Suite**.

16 Entrez un **nom de produit** afin de modifier les paramètres du domaine G Suite. Pensez à utiliser AndroidEMM-NomSociété comme convention de dénomination.

17 Cliquez sur **Enregistrer**.

18 Sélectionnez **ID View Client** dans le champ **Délégation pour le domaine**. Les détails de votre compte de service s'affichent. Vous devez alors quitter Developer Console et entrer vos identifiants de connexion dans la console d'administration Google.

Assurez-vous d'enregistrer votre ID client avant de quitter Developer's Console. Vous utiliserez également ces informations d'identification dans Workspace ONE UEM Console lorsque vous importez votre jeton EMM. Pour plus d'informations, reportez-vous à la section Importer un jeton EMM.

Étape suivante

Pour connaître les étapes de configuration de la console d'administration Google, consultez la section Configurer la console d'administration Google.

Configurer la console d'administration Google

La console d'administration Google permet aux administrateurs de gérer les services Google pour les utilisateurs d'une organisation. Workspace ONE UEM utilise la console d'administration Google pour l'intégration avec les systèmes d'exploitation Android et Chrome.

La page Gérer l'accès client des API vous permet de contrôler l'accès des applications internes personnalisées et des applications tierces aux API Google prises en charge (portées).

Procédure

1 Connectez-vous à la console d'administration Google et accédez à**Sécurité > Paramètres avancés > Gérer l'accès client des API**.

2 Remplissez les informations suivantes :

Paramètre	Description
Nom du client	Entrer l'ID client généré lors de la création de votre compte de service Google
Un ou plusieurs champs d'application de l'API	Copiez et collez les champs d'application de l'API Google suivants pour Android : **Android** : https://www.googleapis.com/auth/admin.directory.user

3 Sélectionnez **Autoriser**.

Générer un jeton EMM

Votre jeton EMM unique fait la liaison entre votre domaine pour la gestion Android et Workspace ONE UEM powered by AirWatch. Vous êtes dirigé vers le site de configuration de G Suite après avoir sélectionné **Accéder à Google** à partir de la tâche précédente.

La procédure décrite dans la tâche consiste à générer un jeton EMM pour un nouveau domaine. La tâche de génération du jeton EMM est différente selon que vous vous enregistrez avec un nouveau domaine ou un domaine existant.

Procédure

1. Remplissez les champs suivants :
   a. **À propos de vous** – Entrez vos coordonnées administratives.
   b. **À propos de votre entreprise** – Remplissez les informations sur votre entreprise.
   c. **Votre compte administrateur Google** – Créez un compte administrateur Google.
   d. **Finalisation** – Entrez les données de vérification de la sécurité.
2. Sélectionnez **Accepter et créer votre compte** après avoir lu et accepté les conditions définies par Google.
3. Suivez les invites suivantes pour **vérifier la propriété du domaine** et **vous connecter avec votre fournisseur**. Une fois les vérifications effectuées, celui-ci devient votre domaine Google géré.

   Pour vérifier la propriété du domaine, les options suivantes sont disponibles : **ajouter une balise meta à votre page d'accueil**, **ajouter un enregistrement d'hôte de domaine**ou **télécharger un fichier HTML sur votre site de domaine**. Configurez les paramètres des options disponibles.
4. Sélectionnez **Vérifier** pour continuer. Si ce processus réussit, la section **Connexion avec votre fournisseur** affiche votre jeton EMM. Ce jeton est valable 30 jours. si vous rencontrez des problèmes au cours de cette étape, reportez-vous au service d'assistance Google en utilisant le numéro et le code PIN unique figurant sur la liste.
5. Copiez le jeton EMM généré et sélectionnez **Terminer**.

Étape suivante

Workspace ONE UEM vous recommande de créer votre compte de service Google avant de retourner à Workspace ONE UEM console pour télécharger le jeton EMM, afin que vous puissiez importer toutes les informations d'identification en une seule fois.

Générer le jeton EMM pour le domaine existant

Votre jeton EMM unique fait la liaison entre votre domaine pour la gestion Android et Workspace ONE UEM powered by AirWatch. Pour le domaine existant, vous êtes dirigé vers la console d'administration Google pour générer le jeton EMM.

La procédure décrite dans la tâche consiste à générer un jeton EMM pour un domaine existant. La tâche de génération du jeton EMM est différente selon que vous vous enregistrez avec un nouveau domaine ou un domaine existant. Pour plus d'informations sur la génération d'un jeton EMM pour un nouveau domaine, voir Générer un jeton EMM.

Procédure

1 Connectez-vous à la console d'administration Google à l'aide de vos informations d'identification Google admin.

2 Accédez à **Sécurité > Fournisseur EMM géré pour Android** et sélectionnez **Générer le jeton EMM**.

3 Copiez et collez le jeton dans la console Workspace ONE UEM.

Étape suivante

Revenez à la console Workspace ONE UEM pour terminer l'enrôlement.

Importer un jeton EMM

Entrez les informations que vous avez obtenues de Google lors de l'enregistrement. Cela inclut le domaine enregistré, le jeton d'entreprise et l'adresse e-mail de l'administrateur Google que vous avez créés.

Vous pouvez également obtenir votre jeton d'entreprise en vous connectant à https://admin.google.com avec votre adresse e-mail d'administrateur Google dans **Sécurité→Gérer le fournisseur EMM pour Android**.

Procédure

1 Accédez à **Démarrage > Workspace ONE > Enregistrement EMM Android**. Si vous avez fermé la fenêtre ou si vous n'êtes pas automatiquement redirigé vers Workspace ONE UEM.

2 Sélectionnez **Enregistrer** pour être redirigé vers l'assistant de configuration Android.

3 Sélectionnez **Importer un jeton** à partir de l'assistant de configuration Android.

Cela est également appelé jeton d'entreprise.

4 Remplissez les champs suivants :

Paramètre	Description
Domaine	Domaine demandé pour l'activation d'Android, associé à votre entreprise. **Important** si votre domaine a déjà été inscrit auprès d'un autre fournisseur EMM, vous ne serez pas autorisé à télécharger un nouveau jeton EMM.
Jeton EMM d'entreprise	Jeton généré dans la console d'administration Google.
Adresse e-mail de l'administrateur Google	Il s'agit du compte d'administrateur utilisé pour l'enregistrement de domaine, la console de développeur Google et la console d'administration Google.

Paramètre	Description
ID client	ID client généré lors de la création de votre compte de service Google. Cet ID est récupéré à partir des **Paramètres de la console de développeur Google**.
Adresse de messagerie de compte de service Google	E-mail généré à partir de la création du compte de service Google. Cet ID est récupéré à partir des **Paramètres de la console de développeur Google**.
ID de certificat	Téléchargez le certificat P12 créé lors de la génération du compte de service Google. Nécessite un mot de passe. Cet ID est récupéré à partir des **Paramètres de la console de développeur Google**.

5 Sélectionnez **Suivant** pour définir les utilisateurs.

Utilisateurs installés

Les utilisateurs de votre entreprise utilisant Android ont tous besoin de disposer d'un compte Google pour se connecter à leurs terminaux. Cette dernière étape dans l'assistant d'inscription EMM Android vous permet de déterminer la méthode d'installation que vous préférez pour la création d'utilisateurs.

Vous avez deux options pour créer des utilisateurs sous Android :

- Autoriser Workspace ONE UEM à créer automatiquement des comptes Google lors de l'enrôlement.
- Créer des utilisateurs manuellement en se connectant à la console d'administration Google ou en utilisant l'outil Google Active Directory Sync (GADS).

Le format du nom d'utilisateur est nom_utilisateur@<votre_domaine_professionnel>.com.

Procédure

1 Activez l'une des options suivantes pour déterminer la manière dont les utilisateurs sont configurés :

   - Créer le compte Google pendant l'enrôlement à partir de l'adresse e-mail de l'utilisateur enrôlé.
   - Utiliser SAML pour l'authentification : activez SAML pour le processus d'enrôlement.
   - Utiliser SAML pour l'authentification du compte Google : pour utiliser cette méthode, configurez Single Sign-On en accédant à **Sécurité > Single Sign On** dans la console d'administration Google.

   Si la création automatique des utilisateurs n'est pas activée avec l'une des méthodes ci-dessus, Workspace ONE UEM console vous dirige vers la méthode alternative de création de comptes Google par l'outil Google Active Directory Sync ou la console d'administration Google.

2 Utilisez l'option **Tester la connexion** pour vérifier l'établissement de la communication avec Google.

   - **Accès à l'API Play** : garantit que l'API Google EMM est activée et que les applications peuvent être installées.
   - **Accès à l'API Directory** : garantit que l'API Admin SDK est activée et que les privilèges pour https://www.googleapis.com/auth/admin.directory.user sont autorisés sur la console d'administration Google.

3 Cliquez sur **Enregistrer**.

Création automatique des utilisateurs de l'enrôlement Android

VMware vous suggère de créer automatiquement des utilisateurs pour Android lors de l'inscription. L'assistant de configuration Android vous permet d'indiquer si vous voulez créer automatiquement des comptes d'utilisateur pendant l'enrôlement, et si oui, si vous souhaitez utiliser SAML pour authentifier les comptes. Si vous n'avez pas configuré SAML auparavant, l'assistant affichera un lien qui vous dirigera vers la configuration de vos paramètres.

Procédure

1 Répondez **Oui** à l'invite **Créer des comptes Google lors de l'enrôlement à partir des e-mails des utilisateurs enrôlés**.

2 Sélectionnez **Oui** pour **utiliser le point de terminaison SAML pour l'authentification des comptes**.

   Si vous n'avez pas configuré SAML, l'assistant vous demandera de configurer les paramètres d'authentification SAML.

3 Répondez **Oui** à l'invite **Utiliser SAML pour l'authentification du compte Google**, ce qui vous oblige à configurer l'authentification Single Sign-On dans la console d'administration Google.

4 Sélectionnez **Enregistrer** pour terminer la configuration d'Android.

Création manuelle des utilisateurs de l'enrôlement Android

Vous pouvez créer manuellement des comptes utilisateurs pour l'ensemble de votre entreprise en dehors de Workspace ONE UEM Console en utilisant l'outil Google Cloud Directory Sync (GCDS) ou la console d'administration Google. Pour accéder à la console d'administration Google, vous pouvez cliquer sur le lien fourni dans l'assistant de configuration. Vous devrez contacter Google pour en savoir plus sur l'utilisation de la console.

La méthode GCDS exige que vous utilisiez des paramètres similaires à ceux des services d'annuaire AirWatch. Accédez aux paramètres des services d'annuaire en naviguant vers **Groupes et paramètres ► Tous les paramètres ► Système ► Intégration d'entreprise ► Services d'annuaire**.

Vous pouvez accéder à l'outil GCDS en cliquant sur le lien affiché dans l'assistant de configuration ou en téléchargeant l'outil directement sur votre ordinateur à partir de la page d'assistance Google.

L'outil GDCS vous permet de créer manuellement en une seule fois des comptes Google pour tous les employés de votre entreprise. Les comptes sont créés en se synchronisant avec les informations stockées de vos services d'annuaire VMware Workspace ONE Directory.

Note les informations présentées ici sont à jour par rapport à la dernière version de GCDS v4.4.0 pour mars 2017.

Procédure

1 Sélectionnez le lien à partir de l'assistant de configuration ou téléchargez l'outil GDCS directement depuis Google.

2 Ouvrez l'outil à partir de votre bureau et sélectionnez les **Comptes utilisateur** et les **Groupes** à synchroniser.

3 Sélectionnez l'onglet **Configuration des applications Google** et entrez les informations suivantes :

   a Entrez le **nom du domaine principal**.

   b Sélectionnez cette option pour **remplacer les noms de domaine dans l'adresse e-mail LDAP (des utilisateurs et des groupes) par ce nom de domaine**. Cela permettra de s'assurer que toutes les adresses e-mail des utilisateurs correspondent au nom de domaine.

4 Sélectionnez le bouton **Autoriser maintenant**.

5 Suivez les étapes pour poursuivre le processus d'autorisation lorsque la boîte de dialogue **Autoriser la synchronisation de l'annuaire des applications Google** s'affiche.

   a Connectez-vous à votre compte administrateur Android.

   b Entrez le code de vérification reçu par e-mail.

   c Sélectionnez **Valider** pour confirmer ces paramètres.

6 Sélectionnez l'onglet **Configuration LDAP** pour entrer les paramètres de connexion afin de synchroniser les services d'annuaire AirWatch avec Google. Vous pouvez alors entrer les mêmes paramètres que ceux enregistrés dans les services d'annuaire AirWatch pour les synchroniser avec cet outil. Pour accéder à ces paramètres, naviguant vers **Groupes et paramètres ► Tous les paramètres ► Système ► Intégration d'entreprise ► Services d'annuaire**.

7 Sélectionnez **Test de la connexion.** Si la synchronisation a réussi, les comptes Active Directory liés et les comptes Google d'entreprise sont automatiquement créés dans Google.

   Vous serez redirigé vers l'assistant de configuration pour terminer la configuration.

Supprimer la liaison du domaine Workspace ONE UEM

Vous pouvez déconnecter le compte administrateur Android dans Workspace ONE UEM Console si vous avez besoin de modifier des comptes Google.

Procédure

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Android > Inscription EMM pour Android**.

2 Sélectionnez **Effacer les paramètres** sur la page d'inscription EMM pour Android.

Aperçu de l'inscription de terminaux Android

3

Tous les terminaux Android de votre déploiement d'entreprise doivent être enrôlés pour pouvoir communiquer avec Workspace ONE UEM Console et accéder au contenu et aux fonctionnalités internes.

Workspace ONE Intelligent Hub constitue une ressource unique pour enrôler le terminal et fournir les détails relatifs à la connexion et au terminal. L'enrôlement basé sur le Hub vous permet :

- d'authentifier les utilisateurs à l'aide d'une méthode basique ou des services d'annuaire, comme les services AD/LDAP/Domino, la norme SAML, des jetons ou des serveurs proxy ;
- d'inscrire des terminaux par lots ou de permettre aux utilisateurs de les inscrire eux-mêmes ;
- de définir des versions de système d'exploitation, des modèles approuvés, ainsi qu'un nombre maximum de terminaux par utilisateur.
- Authentifiez l'enrôlement à l'aide de Workspace ONE Access lors de l'enrôlement automatique.

Le déploiement d'Android (hérité) vous permet d'enrôler des terminaux Android avec Workspace ONE Intelligent Hub en tant qu'administrateur du terminal si vous avez refusé l'inscription Google. Pour inscrire des terminaux à l'aide du déploiement Android (hérité), reportez-vous à la section Aperçu de l'inscription Android (hérité) de la documentation relative à Workspace ONE Android (hérité).

Ce chapitre contient les rubriques suivantes :

Terminaux et utilisateurs/Android/Inscription EMM pour Android

Inscription EMM pour Android vous permet de configurer les différentes options d'intégration avec Android. Cette page utilise un assistant pour vous aider à configurer l'intégration des terminaux. Activez ces paramètres avant de commencer l'enrôlement.

Configuration

La page **Configuration** affiche les paramètres de la console d'administration Google et les paramètres de l'API Google une fois que l'inscription EMM pour Android a réussi.

Paramètres d'enrôlement

Paramètre	Description
Type d'enrôlement géré pour le travail (suite non-G uniquement)	Choisissez si les terminaux doivent être associés à l'utilisateur ou au terminal de l'enrôlement. Lors de l'utilisation d'applications payantes, **Basé sur l'utilisateur** est l'option privilégiée pour une allocation optimale des licences et pour la plupart des cas d'utilisation BYOD. Pour les scénarios où plusieurs utilisateurs peuvent être associés au terminal (comme Kiosques), il est préférable d'utiliser l'option **Basé sur le terminal**. Si vous utilisez un réseau fermé ou que vous ne pouvez pas communiquer avec Google Play, sélectionnez **Réseau AOSP/fermé**. Aucun compte Google n'est créé sur ces terminaux. La gestion des applications publiques via la fonction Google Play gérée n'est pas disponible à l'aide de l'enrôlement de réseau AOSP/fermé. Ce paramètre ne s'applique qu'aux terminaux enrôlés avec ce groupe organisationnel. L'organisation parente peut toujours avoir des terminaux sur l'enrôlement géré pour le travail à l'aide d'un compte Google. Dans certaines instances, vous pouvez enrôler des terminaux GMS et non-GMS dans le même groupe organisationnel sans avoir à créer plusieurs groupes organisationnels pour la gestion des terminaux. Si vous utilisez l'enrôlement du code QR pour ces terminaux, vous pouvez configurer l'assistant de configuration de l'enrôlement pour forcer l'enrôlement du réseau AOSP/fermé quel que soit le type d'enrôlement défini dans ce champ.
Enrôlements de terminaux entièrement gérés	Choisissez si les terminaux enrôlés utilisent le mode **Terminaux gérés pour le travail** ou **Terminaux professionnels et personnels (COPE)**. ■ Le **terminal géré pour le travail** est un terminal entièrement géré qui sera verrouillé. Il permettra aux employés d'accéder aux applications professionnelles uniquement et n'offrira aucun accès aux applications personnelles via le Google Play Store. ■ Le mode **Terminaux professionnels et personnels (COPE)** procure tous les avantages de la gestion complète des terminaux, mais les employés recevront un profil professionnel pour accéder aux applications d'entreprise et auront toujours accès à leur Google Play Store personnel à l'extérieur du profil professionnel. Ce type d'enrôlement est uniquement disponible sous Android 8.0 et versions ultérieures.
Message utilisateur Effacer le contenu d'entreprise du profil professionnel	Personnalisez un message toast à afficher sur les terminaux des utilisateurs lorsque vous avez supprimé du contenu d'entreprise à partir de la console UEM. Lorsque vous effectuez une opération d'effacement de contenu d'entreprise à partir de la page Détails du terminal, ce message est également généré. L'utilisateur n'a pas d'action à effectuer sur son terminal. Le message s'affiche une fois l'effacement du contenu d'entreprise terminé.

Pour plus d'informations sur les modes des terminaux Android, reportez-vous à la documentation *Présentation des modes des terminaux Android* du **guide de la plate-forme Android Workspace ONE UEM** disponible sur docs.vmware.com.

Restrictions d'enrôlement

Paramètre	Description
Définir la méthode d'enrôlement pour ce groupe organisationnel	Sélectionnez **Toujours utiliser Android**, **Toujours utiliser Android (hérité)** ou **Définir le groupe d'attributions qui utilise Android**. Si vous sélectionnez **Définir le groupe d'attributions qui utilise Android**, tous les terminaux non affectés utilisent par défaut Android (hérité).
Groupes d'attribution	Sélectionnez un Smart Group dans la liste déroulante. Lorsqu'un ou plusieurs Smart Groups sont sélectionnés, les terminaux ou les utilisateurs qui n'appartiennent pas à ces groupes passeront par l'enrôlement Android hérité (administrateur de terminaux). Les terminaux qui appartiennent au Smart Group s'enrôlent en mode Profil professionnel ou Terminaux gérés pour le travail en supposant qu'ils prennent en charge les modes d'enrôlement suivants.
Autoriser l'enrôlement de profils professionnel	Utilisez ce champ pour bloquer l'enrôlement de profiles professionnels pour les terminaux gérés dans le cadre d'un enrôlement COPE. Lorsque cette option est activée, les utilisateurs ne peuvent pas ajouter des terminaux personnels à ce groupe organisationnel.

Protection des terminaux Android

Android OS 5.1 et versions ultérieures comporte une fonction appelée Protection du terminal qui exige que les identifiants de connexion Google soient entrés avant et après la réinitialisation d'un terminal. Lorsqu'un terminal est prêt à être enrôlé en tant que Terminal géré pour le travail pour Android, il doit être réinitialisé sur les paramètres d'usine.

Pour que Workspace ONE Intelligent Hub puisse être installé au cours de l'enrôlement, tout compte Google existant doit être supprimé du terminal et l'écran de verrouillage sécurisé doit être désactivé afin d'éviter de déclencher la protection du terminal. L'utilisation du terminal à partir de l'état de réinitialisation sur les paramètres d'usine empêche également le nouvel utilisateur d'être verrouillé sur le terminal.

Si le propriétaire précédent a changé le mot de passe du compte Google, vous devez attendre trois jours avant de réinitialiser vos terminaux Android 5.1 (et versions ultérieures) pour l'enrôlement sauf si vous avez explicitement désactivé la protection des terminaux Android. Si vous réinitialisez l'un de vos terminaux Android avant la fin de ces trois jours et que vous tentez de vous connecter à ce terminal avec votre compte Google, vous recevrez un message d'erreur et vous ne serez pas autorisé à vous connecter au terminal avec un compte avant 72 heures après la réinitialisation du mot de passe.

Enrôlement par détection automatique

Workspace ONE UEM powered by AirWatch simplifie le processus d'enrôlement grâce à un système de détection automatique basé sur l'e-mail pour enrôler les terminaux dans des

environnements et des groupes organisationnels (OG). La détection automatique permet également aux utilisateurs de s'authentifier sur le portail en libre-service (SSP).

Note Afin d'activer la détection automatique pour les environnements sur site, assurez-vous que votre environnement peut communiquer avec les serveurs de détection automatique de Workspace ONE UEM.

Inscription pour l'enrôlement par détection automatique

Le serveur vérifie que le domaine d'e-mail a un nom unique et qu'il n'est pas déjà inscrit dans un autre groupe organisationnel de l'environnement. À cause de cette vérification du serveur, enregistrez votre domaine au niveau de votre plus haut groupe organisationnel.

La détection automatique est configurée automatiquement pour les nouveaux clients SaaS.

Configuration de l'enrôlement par détection automatique à partir d'un sous-groupe organisationnel

Vous pouvez configurer l'enrôlement à détection automatique depuis un sous-groupe organisationnel du groupe organisationnel d'enrôlement. Pour activer l'enrôlement de détection automatique de cette manière, vous devez demander aux utilisateurs de sélectionner un ID de groupe pendant l'enrôlement.

Forcez les utilisateurs à sélectionner un ID de groupe pendant les enrôlements.

Procédure

1. Accédez à **Terminaux > Paramètres des terminaux > Général > Enrôlement** et sélectionnez l'onglet **Regroupement**.
2. Sélectionnez **Sélection manuelle de l'ID de groupe par l'utilisateur**.
3. Cliquez sur **Enregistrer**.

Configuration de l'enrôlement par détection automatique à partir d'un groupe organisationnel parent

L'enrôlement par détection automatique simplifie le processus d'enrôlement des terminaux dans les environnements et groupes organisationnels auxquels ils sont destinés à l'aide des adresses e-mail des utilisateurs finaux.

Configurez un enrôlement de détection automatique depuis un groupe organisationnel parent en effectuant les opérations suivantes.

Procédure

1 Accédez à **Groupes et paramètres > Tous les paramètres > Administrateur > Services Cloud** et activez le paramètre **Détection automatique**. Saisissez l'adresse e-mail de connexion dans **ID AirWatch de détection automatique** et sélectionnez **Définir une identité**.

   a Si nécessaire, accédez à https://my.workspaceone.com/set-discovery-password afin de définir votre mot de passe pour le service de détection automatique. Une fois vous avez enregistré et sélectionné cliqué sur **Définir une identité**, le **jeton HMAC** s'affiche automatiquement. Cliquez sur **Tester la connexion** pour vous assurer que la connexion fonctionne.

2 Activez l'option **Épinglage de certificat de détection automatique** pour importer votre propre certificat et l'épingler à la fonction de détection automatique. Vous pouvez passer en revue les dates de validité et d'autres informations concernant les certificats existants, et utiliser les options **Remplacer** et **Supprimer** pour ces certificats.

3 Sélectionnez **Ajouter un certificat** ; les paramètres **Nom** et **Certificat** s'affichent. Saisissez le nom du certificat à importer, sélectionnez le bouton **Importer** et choisissez le certificat sur votre terminal.

4 Cliquez sur **Enregistrer** pour terminer la configuration de la détection automatique.

Étape suivante

Demandez aux utilisateurs finaux qui se sont enrôlés de sélectionner l'option d'adresse e-mail pour l'authentification au lieu de l'URL d'environnement et de l'ID de groupe. Lorsque les utilisateurs enrôlent des terminaux à l'aide de leur adresse e-mail, ils s'enrôlent dans le groupe indiqué dans le champ **Groupe organisationnel d'enrôlement** du compte utilisateur associé.

Configuration de l'enrôlement en mode Terminaux gérés pour le travail

Le mode Terminaux gérés pour le travail d'Android donne le contrôle de l'ensemble du terminal à Workspace ONE UEM. L'utilisation d'un terminal réinitialisé sur les paramètres d'usine permet de s'assurer qu'il n'est pas configuré pour un usage personnel.

Il existe plusieurs façons d'enrôler des terminaux gérés pour le travail :

- Par communication en champ proche (CCP) avec AirWatch Relay
- Avec un identifiant unique ou un code de jeton
- En scannant un code QR
- À l'aide de l'enrôlement sans contact

Les méthodes d'enrôlement que vous souhaitez utiliser dépendent de vos besoins professionnels. Vous ne pouvez pas enrôler des terminaux tant que vous n'avez pas terminé l'inscription du jeton EMM pour Android. Reportez-vous à la documentation Chapitre 2 Inscription pour Android avec Workspace ONE UEM pour terminer l'enregistrement.

Si les terminaux Android que vous utilisez se trouvent sur un réseau fermé, ne parviennent pas à communiquer avec Google Play ou exécutent Android 5.0 ou des versions antérieures, vous pouvez les enrôler à l'aide de l'enrôlement de terminaux gérés pour le travail pour la prise en charge du réseau AOSP/fermé. La gestion des applications publiques via la fonction Google Play gérée n'est pas disponible.

Enrôlement avec AirWatch Relay

AirWatch Relay est une application qui transmet les informations des terminaux parent à tous les terminaux enfant enrôlés dans Workspace ONE UEM avec Android.

Note AirWatch Relay n'est pas pris en charge dans Android 10.

Ce processus se fait par l'intermédiaire d'un transfert NFC et provisionne les terminaux enfants pour :

- Copiez le réseau Wi-Fi du terminal parent et les paramètres régionaux, notamment la date, l'heure et l'emplacement du terminal.
- Télécharger la dernière version de production de Workspace ONE Intelligent Hub pour Android.
- Installer en mode silencieux Workspace ONE Intelligent Hub en tant qu'administrateur du terminal.
- S'enrôler automatiquement dans Workspace ONE UEM.

AirWatch Relay vous permet d'enrôler tous les terminaux enfant par lots avant de les déployer auprès des utilisateurs finaux. Il évite ainsi aux utilisateurs finaux d'avoir à enrôler leurs propres terminaux. Tous les terminaux enfant doivent être en mode réinitialisation des paramètres d'usine et la fonction NFC doit être activée par défaut pour qu'ils soient enrôlés en tant que terminaux gérés pour le travail pour Android.

Le processus de transfert NFC dépend de l'OS Android. Les terminaux Android 6.0 (et versions ultérieures) exécutent un transfert pour connecter et enrôler les terminaux enfant en une seule étape. Les terminaux avec des versions OS Android entre v5.0 et v6.0 exécutent deux transferts NFC. Le premier transfert consiste à connecter le terminal enfant au réseau Wi-Fi et à appliquer les paramètres régionaux, notamment la date, l'heure et l'emplacement du terminal, et à télécharger Workspace ONE Intelligent Hub. Le deuxième transfert NFC consiste à enrôler tous les terminaux enfant avant de les déployer auprès des utilisateurs finaux.

Pour l'enrôlement d'AirWatch Relay, reportez-vous à la documentation Enrôler un terminal géré pour le travail avec AirWatch Relay.

Enrôlement avec l'identifiant Workspace ONE Intelligent Hub

La méthode d'enrôlement par identifiant Workspace ONE Intelligent Hub est une approche simplifiée pour l'enrôlement des terminaux Android 6.0 (et versions ultérieures) gérés pour le travail. Entrez un identifiant, ou valeur de hachage, unique sur un terminal réinitialisé sur les paramètres d'usine. Une fois l'identifiant saisi, l'enrôlement est automatisé, et Workspace ONE

Intelligent Hub est déployé. L'utilisateur doit uniquement entrer les détails du serveur, le nom d'utilisateur et le mot de passe. Pour l'enrôlement avec l'identifiant Workspace ONE Intelligent Hub, reportez-vous à la documentation Enrôler des terminaux Android à l'aide de l'identifiant VMware Workspace ONE Intelligent Hub.

Avec l'identifiant, vous pouvez également procéder à l'enrôlement pour l'utilisateur final grâce au préenrôlement de terminaux à utilisateur unique. Cette méthode est utile pour les administrateurs qui doivent configurer plusieurs terminaux pour une équipe ou pour des membres d'une équipe. Une telle méthode permet d'économiser temps et efforts lors de l'enrôlement des terminaux.

Pour plus d'informations sur le Préenrôlement d'utilisateur unique, reportez-vous à la section Préenrôlement d'utilisateur unique dans la documentation relative à la gestion de terminaux mobiles (MDM).

Enrôlement avec le code QR

Le provisionnement par code QR est un moyen facile d'enrôler une flotte de terminaux qui ne prennent pas en charge le NFC et le transfert NFC. Le code QR contient une section de configuration de paires clé-valeur avec toutes les informations nécessaires à l'enrôlement du terminal. Créez le code QR avant de commencer l'enrôlement. Vous pouvez utiliser n'importe quel générateur de code QR en ligne, comme Web Toolkit Online, pour créer votre code QR unique. Le code QR comprend l'URL du serveur et les informations d'ID de groupe. Vous pouvez également inclure le nom d'utilisateur et le mot de passe ou laisser l'utilisateur entrer ses identifiants de connexion.

Voici le format du texte à coller dans le générateur :

```
{"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/
com.airwatch.agent.DeviceAdministratorReceiver","android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE
_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=
\n","android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"https://getwsone.com/
mobileenrollment/airwatchagent.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,"android.app.extra.PROVISIONING_WIFI_SSID":
"Your_SSID","android.app.extra.PROVISIONING_WIFI_PASSWORD": "Password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"serverurl": "Server URL",
"gid": "Group ID",
"un":"Username",
"pw":"Password"}
```

Pour l'enrôlement par code QR, consultez la section Enrôlement des terminaux gérés pour le travail à l'aide d'un code QR.

Enrôlement à l'aide du portail Zero Touch (sans contact)

L'enrôlement sans contact permet de configurer tout de suite les terminaux Android 8.0 et versions ultérieures avec Workspace ONE UEM comme fournisseur EMM.

Si le terminal est connecté à Internet pendant sa configuration, Workspace ONE Intelligent Hub est automatiquement téléchargé, et les détails de l'enrôlement sont automatiquement transmis pour enrôler le terminal sans interaction de l'utilisateur. Vous pouvez gérer l'inscription rationalisée pour votre organisation à partir d'un portail en ligne de votre navigateur Web. Nous l'appelons le portail d'inscription rationalisée.

L'enrôlement sans contact est pris en charge par un nombre limité d'opérateurs mobiles et d'OEM. Les clients contactent leur opérateur pour s'assurer que le provisionnement sans contact est pris en charge. Pour en savoir plus sur les opérateurs et les terminaux pris en charge, consultez le site Web de Google.

Pour plus d'informations sur l'inscription rationalisée, reportez-vous à l'article de prise en charge Android.

Pour savoir comment utiliser l'enrôlement à l'aide du portail Zero Touch (sans contact), reportez-vous à la documentation Enrôler un terminal Android à l'aide du portail Zero Touch (sans contact)

Note l'enrôlement sans contact est uniquement pris en charge sur les terminaux Android 8.0 (Oreo).

Enrôlement de terminaux à l'aide de Workspace ONE Access

Workspace ONE Access fournit une authentification multifacteur, un accès conditionnel et une authentification Single Sign-On aux applications SaaS, Web et mobiles natives. Vous pouvez utiliser Workspace ONE Access pour authentifier des terminaux à la place de Workspace ONE Intelligent Hub. Une fois que vous avez activé Workspace ONE Access comme méthode d'authentification, vous pouvez utiliser des méthodes d'enrôlement automatique telles que le NFC, le code QR, l'enrôlement rationalisé et l'enrôlement Mobile Samsung Knox.

Enrôler un terminal géré pour le travail avec AirWatch Relay

L'enrôlement en mode Terminaux gérés pour le travail avec AirWatch Relay varie en fonction de la version de l'OS Android.

Note AirWatch Relay n'est pas pris en charge dans Android 10.

Si vous utilisez Android 6.0 et versions ultérieures, l'application AirWatch Relay propose une seule option de transfert NFC qui configure les paramètres d'enrôlement, du Wi-Fi et du provisionnement. Pour en savoir plus sur le provisionnement de terminaux gérés pour le travail avec AirWatch Relay sur les terminaux Android 6.0 et versions ultérieures, veuillez consulter la section Enrôlement d'un terminal Android avec AirWatch Relay pour Android 6.0 et versions ultérieures.

L'enrôlement en mode Terminaux gérés pour le travail pour les terminaux Android entre les versions 5.0 et 6.0 est effectué en deux transferts NFC. Le premier transfert configure les paramètres régionaux, le Wi-Fi et tous les paramètres avancés applicables à l'ensemble des terminaux de votre flotte. Le deuxième transfert configure les paramètres d'enrôlement et automatise le processus d'enrôlement. Consultez la section Enrôlement d'un terminal géré pour le travail avec AirWatch Relay pour Android 5.0 et Android 6.0.

Enrôlement d'un terminal Android avec AirWatch Relay pour Android 6.0 et versions ultérieures

Pour Android 6.0 et versions ultérieures, l'application AirWatch Relay offre une option de transfert unique qui configure les paramètres régionaux, le Wi-Fi, les paramètres de provisionnement et les paramètres d'enrôlement en un transfert unique.

Procédure

1. Téléchargez l'application AirWatch Relay depuis le Google Play Store sur le terminal parent et lancez l'application une fois l'installation terminée.
2. Passez en revue l'écran réservé aux administrateurs AirWatch et sélectionnez **Suivant** pour passer à l'assistant.

   Cet écran vous permettra d'afficher ou d'ignorer un assistant de configuration qui fournit une description de l'application et un tutoriel expliquant le transfert NFC.
3. Appuyez sur **Configurer** sur les terminaux à provisionner en un seul transfert (Android 6.0 et versions ultérieures).
4. Sur le terminal parent, définissez les paramètres suivants :

Paramètre	Description
Heure locale	Activez ce champ pour que le terminal soit automatiquement configuré avec l'heure locale.
Fuseau horaire	Sélectionnez le fuseau horaire.
Paramètres régionaux	Sélectionnez l'emplacement où votre terminal sera activé.
Réseau Wi-Fi	Indiquez le réseau Wi-Fi auquel le terminal se connectera.
Type de sécurité	Déterminez le type de chiffrement pour la connexion.
Mot de passe Wi-Fi	Entrez le mot de passe Wi-Fi.
Chiffrer le terminal	Désactivez cette option pour ignorer le chiffrement du terminal dans le cadre du provisionnement du terminal géré pour le travail.
Désactiver les applications système	Lorsqu'il est activé, Workspace ONE Intelligent Hub désactive les applications système lors de la configuration.
Serveur	Saisissez le nom d'hôte ou l'URL du serveur.
ID de groupe	Saisissez un identifiant pour le groupe organisationnel que l'utilisateur final utilisera pour y connecter son terminal.

Paramètre	Description
Nom d'utilisateur	Saisissez les identifiants de connexion de l'utilisateur pour lequel le terminal enfant sera enrôlé.
Mot de passe	Saisissez les identifiants de connexion de l'utilisateur pour lequel le terminal enfant sera enrôlé.

5 Appuyez sur **Prêt** sur le terminal parent.

6 Effectuez le transfert NFC en plaçant dos à dos le terminal parent et le terminal enfant. Le terminal enfant doit être en mode de réinitialisation sur les paramètres d'usine. Cela permet de s'assurer que le terminal n'est pas utilisé à des fins personnelles.

avant d'effectuer une réinitialisation sur les paramètres d'usine des terminaux enfant (si le terminal n'est pas neuf), désactivez l'écran de verrouillage et supprimez tout compte Google existant configuré sur le terminal. La protection du terminal est une fonctionnalité pour Android 5.1 et versions ultérieures qui nécessite d'entrer les identifiants de connexion du compte Google avant d'effectuer une réinitialisation aux paramètres d'usine. Si vous désactivez le verrouillage de l'écran et supprimez tout compte Google existant, vous ne serez pas invité à fournir des identifiants de connexion et l'enrôlement ne sera pas entravé.

7 Appuyez sur **Appuyer pour transférer** sur le terminal parent, les terminaux étant toujours dos à dos.

8 Appuyez sur **Chiffrer** sur le terminal enfant, les terminaux étant toujours dos à dos.

Cette étape s'applique uniquement si l'option **Chiffrer le terminal** n'est pas activée. Sinon, elle est automatiquement acceptée.

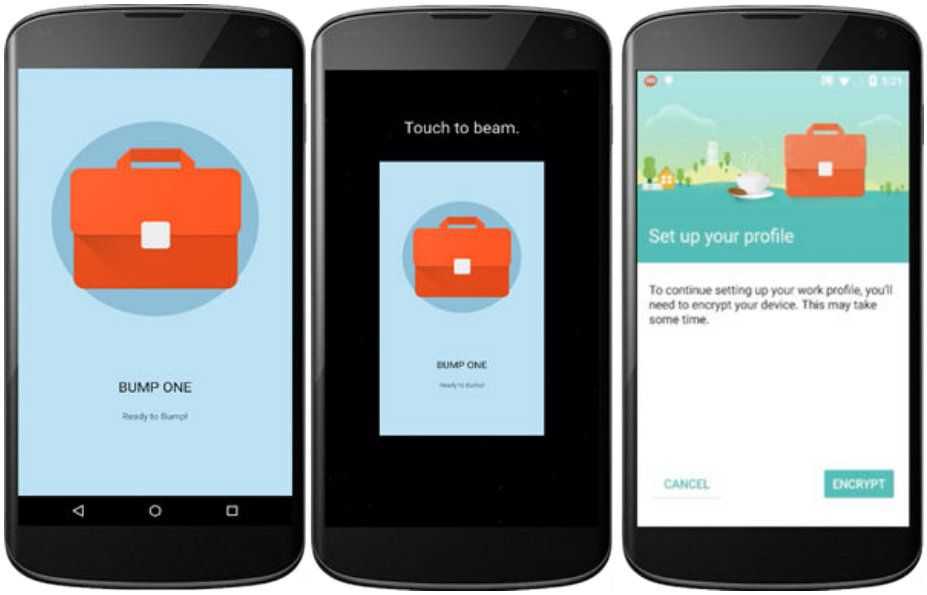
Le terminal enfant va automatiquement :

a Se connecter au réseau Wi-Fi défini dans l'application AirWatch Relay.

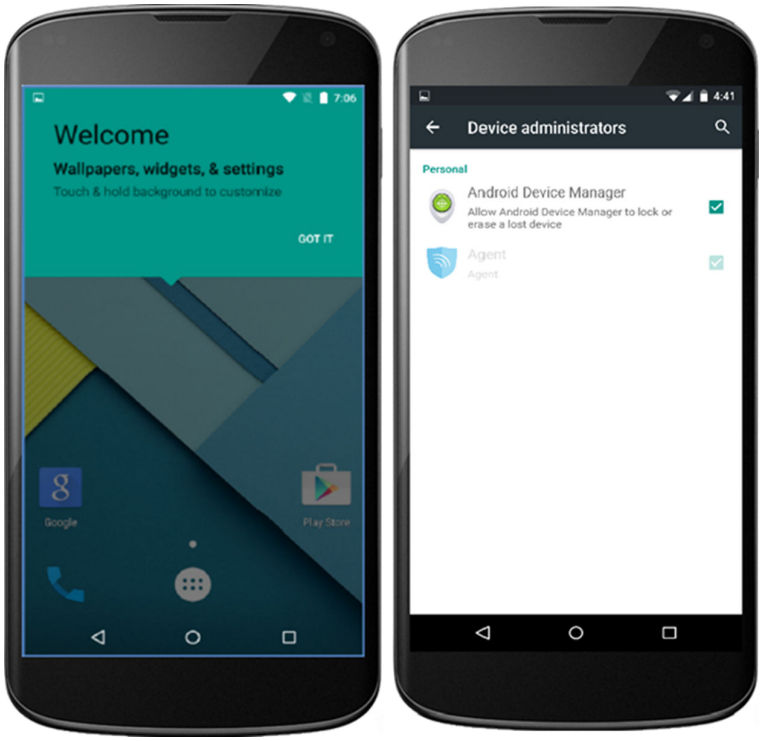
b Télécharger et installer silencieusement Workspace ONE Intelligent Hub.

c Définir Workspace ONE Intelligent Hub en tant qu'administrateur du terminal.

d Réinitialiser le terminal.



Après la réinitialisation du terminal enfant, le terminal est provisionné pour le mode Géré pour le travail. Un écran de bienvenue s'affiche sur votre terminal enfant. Pour vérifier cela sur le terminal enfant, accédez à **Paramètres du terminal > Sécurité > Administrateur du terminal** et regardez si Workspace ONE Intelligent Hub est énuméré comme administrateur du terminal. Les utilisateurs finaux ne pourront pas désactiver ce paramètre.



Vous remarquerez également sur l'écran d'accueil du terminal les applications pré-téléchargées autorisées. Toute autre application devra être approuvée par l'administrateur dans Workspace ONE UEM Console.

Si vous avez plusieurs terminaux à enrôler dans votre flotte de terminaux, répétez le transfert NFC sur chaque terminal enfant pour les provisionner en mode Terminaux gérés pour le travail.

Résultats

Si l'enrôlement a réussi, la page **Mon terminal** s'affiche sur le terminal enfant. Tous les profils et applications commencent à être automatiquement transférés vers le terminal. Répétez les étapes d'enrôlement pour chaque terminal devant être enrôlé dans votre flotte de terminaux.

Workspace ONE UEM Console indique le statut d'Android sur les terminaux des utilisateurs. Vous pouvez consulter la page **Vue détails** pour vérifier que le terminal enrôlé en mode géré pour le travail a réussi.

Enrôlement d'un terminal géré pour le travail avec AirWatch Relay pour Android 5.0 et Android 6.0

Pour Android v5.0 et Android v6.0, l'application AirWatch Relay propose une option de transfert NFC qui configure automatiquement les paramètres régionaux, le Wi-Fi, les paramètres de provisionnement et les paramètres d'inscription.

Procédure

1. Téléchargez l'application AirWatch Relay depuis le Google Play Store sur le terminal parent et lancez l'application une fois l'installation terminée.
2. Passez en revue l'écran réservé aux administrateurs AirWatch et sélectionnez **Suivant** pour passer à l'assistant.

   Cet écran vous permettra d'afficher ou d'ignorer un assistant de configuration qui fournit une description de l'application et un tutoriel expliquant le transfert NFC.
3. Appuyez sur **Configuration** sur l'option souhaitée pour **Provisionner les terminaux en 2 transferts (peut être exécutée sur les terminaux Android 5.0 à Android 6.0)**.

   Si vous utilisez Android 6.0 ou versions ultérieures, sélectionnez **Provisionnement de terminaux en un seul transfert (Android 6.0 ou versions ultérieures).** Pour obtenir les instructions pour les terminaux Android 6.0 et versions ultérieures, veuillez consulter la section Enrôlement d'un terminal Android avec AirWatch Relay pour Android 6.0 et versions ultérieures.
4. Sur le terminal parent, définissez les paramètres suivants :

Paramètre	Description
Heure locale	Activez ce champ pour que le terminal soit automatiquement configuré avec l'heure locale.
Fuseau horaire	Sélectionnez le fuseau horaire.
Paramètres régionaux	Sélectionnez l'emplacement où votre terminal sera activé.
Réseau Wi-Fi	Indiquez le réseau Wi-Fi auquel le terminal se connectera.
Type de sécurité	Déterminez le type de chiffrement pour la connexion.

Paramètre	Description
Mot de passe Wi-Fi	Entrez le mot de passe Wi-Fi.
Chiffrer le terminal	Activez ce champ pour indiquer que le chiffrement des terminaux peut être ignoré dans le cadre du provisionnement des terminaux gérés pour le travail.
Désactiver les applications système	Si ce champ est activé, Workspace ONE Intelligent Hub désactive les applications système pendant la configuration.

5 Appuyez sur **Prêt** sur le terminal parent pour effectuer le premier transfert.

6 Effectuez le premier transfert NFC en plaçant dos à dos le terminal parent et le terminal enfant. Le terminal enfant doit être en mode de réinitialisation sur les paramètres d'usine. Cela permet de s'assurer que le terminal n'est pas utilisé à des fins personnelles.

avant d'effectuer une réinitialisation sur les paramètres d'usine des terminaux enfant (si le terminal n'est pas neuf), désactivez l'écran de verrouillage et supprimez tout compte Google existant configuré sur le terminal. La protection du terminal est une fonctionnalité pour Android 5.1 qui nécessite d'entrer les identifiants de connexion du compte Google avant d'effectuer une réinitialisation sur les paramètres d'usine. Si vous désactivez le verrouillage de l'écran et supprimez tout compte Google existant, vous ne serez pas invité à fournir des identifiants de connexion et l'enrôlement ne sera pas entravé.

7 Appuyez sur **Appuyer pour transférer** sur le terminal parent, les terminaux étant toujours dos à dos.

8 Appuyez sur **Chiffrer** sur le terminal enfant, les terminaux étant toujours dos à dos.

Cette étape s'applique uniquement si **Chiffrer le terminal** n'est pas activé, sinon il sera automatiquement accepté.

Le terminal enfant va automatiquement :

- Se connecter au réseau Wi-Fi défini dans l'application AirWatch Relay.
- télécharger et installer silencieusement Workspace ONE Intelligent Hub ;
- définir Workspace ONE Intelligent Hub en tant qu'administrateur du terminal ;
- Réinitialiser le terminal.

Après la réinitialisation du terminal enfant, le terminal est provisionné pour le mode Géré pour le travail et le premier transfert est terminé. Un écran de bienvenue s'affiche sur votre terminal enfant. Pour vérifier cela sur le terminal enfant, accédez à **Paramètres du terminal > Sécurité > Administrateur du terminal** et regardez si Workspace ONE Intelligent Hub est énuméré comme administrateur du terminal. Les utilisateurs finaux ne pourront pas désactiver ce paramètre.

Vous remarquerez également sur l'écran d'accueil du terminal les applications pré-téléchargées autorisées. Toute autre application devra être approuvée par l'administrateur dans Workspace ONE UEM Console.

Si vous avez plusieurs terminaux à enrôler dans votre flotte de terminaux, répétez le transfert NFC sur chaque terminal enfant pour les provisionner en mode Terminaux gérés pour le travail. Si ce n'est pas le cas, passez à l'enrôlement.

Vous pouvez également enrôler manuellement les terminaux enfant et ignorer les étapes de deuxième transfert NFC expliquées ci-dessous. Vous devrez entrer manuellement les détails d'enrôlement sur chaque terminal. Pour des processus d'enrôlement supplémentaires, reportez-vous à la section Workflows d'enrôlement supplémentaires dans la documentation Gestion des terminaux mobiles (MDM).

9 Retournez à l'application AirWatch Relay, sur le terminal parent, puis appuyez sur **Enrôler**.

10 Définissez les paramètres d'enrôlement. Ces paramètres seront utilisés pour automatiser l'enrôlement des terminaux enfant.

Paramètre	Description
Serveur	Saisissez le nom d'hôte ou l'URL du serveur.
ID de groupe	Saisissez un identifiant pour le groupe organisationnel que l'utilisateur final utilisera pour y connecter son terminal.

11 Appuyez sur **Prêt**.

12 Effectuez le deuxième transfert NFC en plaçant dos à dos le terminal parent et le terminal enfant et appuyez sur **Appuyer pour transférer** sur le terminal enfant pour commencer l'enrôlement. Le deuxième transfert NFC doit être effectué après la fin de l'assistant de configuration. Attendez que l'assistant de configuration ait terminé et qu'il vous dirige vers la page d'accueil du terminal avant d'effectuer le deuxième transfert NFC pour configurer Workspace ONE Intelligent Hub.

13 Entrez les identifiants de connexion pour le compte Google professionnel lié à l'utilisateur. Un écran s'affiche et vous demande le mot de passe du compte Google. Si vous êtes inscrit en tant que compte Google Play géré, cet écran ne s'affiche pas.

14 Appuyez sur **Suivant** pour passer à la page **Mon terminal** (illustrée dans l'image ci-dessus).

Étape suivante

Si l'enrôlement a réussi, la page **Mon terminal** s'affiche sur le terminal enfant (voir ci-dessus). Tous les profils et applications commencent à être automatiquement transférés vers le terminal. Répétez les étapes d'enrôlement pour chaque terminal devant être enrôlé dans votre flotte de terminaux.

Enrôler des terminaux Android à l'aide de l'identifiant VMware Workspace ONE Intelligent Hub

Lors de l'inscription d'un terminal géré pour le travail et d'un terminal professionnel à accès personnel (COPE), l'utilisateur saisit un jeton d'identification spécifique à un DPC spécial lorsqu'il

est invité à ajouter un compte. Le jeton pour Workspace ONE UEM est « afw#hub » qui identifie automatiquement Workspace ONE UEM en tant que fournisseur EMM.

Important Ce flux d'inscription est uniquement pris en charge pour les terminaux Android 6.0 Marshmallow ou versions ultérieures.

Procédure

1. Appuyez sur **Démarrer** sur votre terminal réinitialisé sur les paramètres d'usine.
2. Sélectionnez votre réseau **Wi-Fi** et connectez-vous avec vos identifiants pour connecter le terminal.
3. Entrez l'identifiant « afw#hub » lorsque vous êtes invité à ajouter un compte Google. L'assistant de configuration ajoute un compte Google temporaire au terminal. Ce compte n'est utilisé que pour télécharger le DPC sur le Google Play Store et est supprimé à la fin.

   Si l'identifiant n'est pas saisi correctement, vous êtes invité à le saisir à nouveau.
4. Appuyez sur **Installer** pour commencer la configuration de Workspace ONE Intelligent Hub sur le terminal. Le Hub s'ouvrira automatiquement une fois l'installation terminée.
5. Choisissez la **méthode d'authentification** pour poursuivre l'enrôlement :
   a. Entrez **Adresse e-mail** si vous avez configuré la détection automatique. En outre, vous pouvez être invité à sélectionner votre ID de groupe dans une liste ou choisir **Détails du serveur** et entrer le serveur, l'ID de groupe et les informations d'identification de l'utilisateur.
   b. Choisissez **Code QR** si vous avez créé un code QR dans UEM Console.
6. Suivez les instructions des invites suivantes pour finaliser l'enrôlement.

   Note Vous pouvez consulter la page **Vue détails** pour vérifier que le terminal a été inscrit en mode géré pour le travail.

Enrôlement des terminaux gérés pour le travail à l'aide d'un code QR

La méthode d'enrôlement du code QR configure les modes Terminaux gérés pour le travail et Terminaux professionnels et personnels (COPE) en scannant un code QR généré avec l'assistant de configuration de l'enrôlement ou depuis n'importe quel générateur de code QR, tel que Web Toolkit Online.

Conditions préalables

Pour utiliser UEM console afin de créer le code QR, reportez-vous à l'assistant de configuration de l'enrôlement **(Terminaux > Cycle de vie > Préenrôlement > Affichage en liste > Configurer l'enrôlement)**. Pour plus d'informations sur l'assistant de configuration de l'enrôlement, reportez-vous à la section Génération d'un code QR à l'aide de l'assistant de configuration de l'enrôlement.

Important ce workflow d'enrôlement est disponible pour les utilisateurs Google Play et de domaine Google gérés. Ce workflow d'enrôlement est pris en charge sur les terminaux Android 7.0 et versions ultérieures.

Procédure

1 Mettez sous tension le dispositif de réinitialisation aux paramètres d'usine ou le terminal prêt à l'emploi. L'Assistant de configuration invite l'utilisateur à appuyer six fois sur l'écran d'accueil. Les pressions doivent être effectuées au même endroit de l'écran.

   a Pour les terminaux Android 8.0 et versions ultérieures, passez à l'étape 2 afin de télécharger le lecteur de codes QR.

   b Pour les terminaux Android 9.0 et versions ultérieures, la caméra s'ouvrira automatiquement lorsque vous aurez terminé les six étapes.

2 Connectez-vous au **Wi-Fi** pour que l'assistant de configuration télécharge automatiquement un lecteur de code QR. L'application de lecteur de code QR démarre automatiquement une fois l'installation terminée.

3 Scannez votre code QR. Pour les terminaux Android 9.0 et versions ultérieures, utilisez l'option Code QR sur la caméra pour scanner. Vous pouvez utiliser n'importe quel générateur de code QR en ligne, comme Web Toolkit Online, pour créer votre code QR unique. Pour plus d'informations, reportez-vous à Configuration de l'enrôlement en mode Terminaux gérés pour le travail.

Format texte du code QR	{"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.airwatch.androidagent/ com.airwatch.agent.DeviceAdministratorReceiver","android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8= \n","android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"https://getwsone.com/mobileenrollment/ airwatchagent.apk", "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,"android.app.extra.PROVISIONING_WIFI_SSID": "Your_SSID","android.app.extra.PROVISIONING_WIFI_PASSWORD": "Password", "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {"serverurl": "Server URL", "gid": "Group ID", "un":"Username", "pw":"Password"}}

4 L'assistant de configuration télécharge automatiquement Workspace ONE Intelligent Hub et configure automatiquement l'URL du serveur, l'ID de groupe, le nom d'utilisateur et le mot de passe spécifiés dans le code QR généré.

   Remarque : lorsque le serveur, l'ID de groupe, le nom d'utilisateur et le mot de passe sont tous inclus dans la configuration, le Hub ignore toutes les invites d'enrôlement supplémentaires.

5 Entrez les identifiants de l'utilisateur qui n'ont pas été configurés précédemment dans le code QR.

   Si l'enrôlement a réussi, la page **Mon terminal** s'affiche sur le terminal. Les profils et les applications commencent tous à être transférés automatiquement vers le terminal.

   Workspace ONE UEM Console indique le statut d'Android sur les terminaux des utilisateurs. Vous pouvez consulter la page **Vue détails** pour vérifier que le terminal enrôlé en mode géré pour le travail a réussi.

Génération d'un code QR à l'aide de l'assistant de configuration de l'enrôlement

Créez un code QR à scanner avec vos terminaux Android 7.0 ou versions ultérieures pour transférer le terminal rapidement. L'assistant simplifie le processus de configuration du préenrôlement.

Procédure

1 Accédez à **Terminaux > Cycle de vie > Préenrôlement > Affichage en liste > Android > Code QR** dans Workspace ONE UEM Console.

2 Connectez le terminal au **Wi-Fi** avant l'enrôlement en activant le curseur correspondant. Les options suivantes s'affichent :

Paramètre	Description
SSID	Entrez l'identifiant SSID, plus communément appelé le nom du réseau Wi-Fi.
Mot de passe	Entrez le mot de passe Wi-Fi pour le SSID saisi.

3 Sélectionnez **Suivant**.

4 Sélectionnez la version de Workspace ONE Intelligent Hub à transférer vers les terminaux durant le préenrôlement. La sélection par défaut est Utiliser la dernière version de Workspace ONE Intelligent Hub.

   Si Workspace ONE Intelligent Hubn'est pas ajouté, sélectionnez **Hébergé sur une URL externe** et entrez l'adresse dans la zone de texte **URL** pour pointer vers un package Workspace ONE Intelligent Hub hébergé en externe.

5 Sélectionnez **Suivant**.

6 Définissez les paramètres **Détails de l'enrôlement**. Pour utiliser l'authentification par jeton, laissez les deux options désactivées.

Paramètre	Description
Groupe organisationnel	Activez et sélectionnez le groupe organisationnel utilisé par le package de préenrôlement par code QR.
Nom d'utilisateur	Configurez les identifiants de connexion. Entrez le nom d'utilisateur du compte Workspace ONE UEM.
Mot de passe	Entrez le mot de passe correspondant.
Applications système	S'applique aux terminaux gérés pour le travail uniquement. Vous pouvez sélectionner **Activer** afin de conserver les applications système non critiques installées sur votre terminal géré pour le travail. Sélectionnez **Désactiver** pour supprimer ces applications.
Forcer l'enrôlement de réseau AOSP/fermé	Lorsque ce champ est activé, vous pouvez enrôler des terminaux GMS et non-GMS dans le même groupe organisationnel, quel que soit le type d'enrôlement de terminal géré pour le travail défini lors de l'enregistrement EMM Android. ■ Si l'indicateur est défini pour utiliser GMS et qu'UEM console est définie sur AOSP sur la page d'enregistrement EMM Android, le terminal utilisera l'indicateur d'UEM console et s'enrôlera sans compte Google. ■ Si l'indicateur est défini pour utiliser GMS et qu'UEM console est définie sur des comptes basés sur l'utilisateur ou sur des terminaux, Intelligent Hub tentera d'effectuer un flux d'enrôlement de GMS. Si le terminal est non-GMS, l'enrôlement échoue.

7 Sélectionnez **Suivant**.

8 La page **Résumé** vous permet de **télécharger le fichier** au format PDF. Sélectionnez **Afficher le PDF** pour obtenir un aperçu de vos sélections **Format de code QR**.

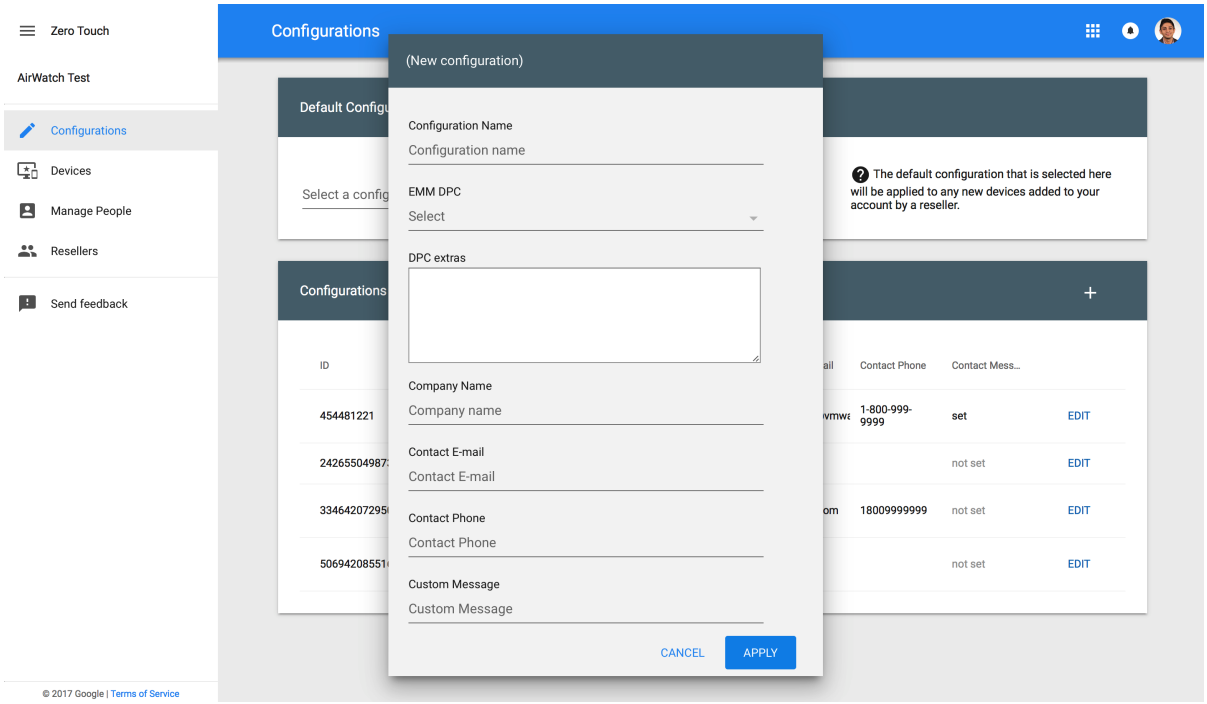
Enrôler un terminal Android à l'aide du portail Zero Touch (sans contact)

Dans le portail Zero Touch (sans contact), ajoutez les configurations d'enrôlement qui devraient être appliquées sur le terminal dès que Workspace ONE Intelligent Hub est téléchargé.

Note l'enrôlement sans contact est uniquement pris en charge sur les terminaux Android 8.0 (Oreo). Pour les terminaux Samsung, utilisez Knox Mobile Enrollment.

Procédure

1 Naviguez jusqu'à l'onglet **Configurations** et cliquez sur le signe **+**.



2 Saisissez les détails suivants pour l'enrôlement :

Paramètre	Description
Nom de la configuration	Saisissez le nom cette configuration.
EMM DPC	Sélectionnez Workspace ONE Intelligent Hub. Cela permet de s'assurer que Workspace ONE Intelligent Hub est téléchargé lors de la configuration avec les paramètres d'usine.

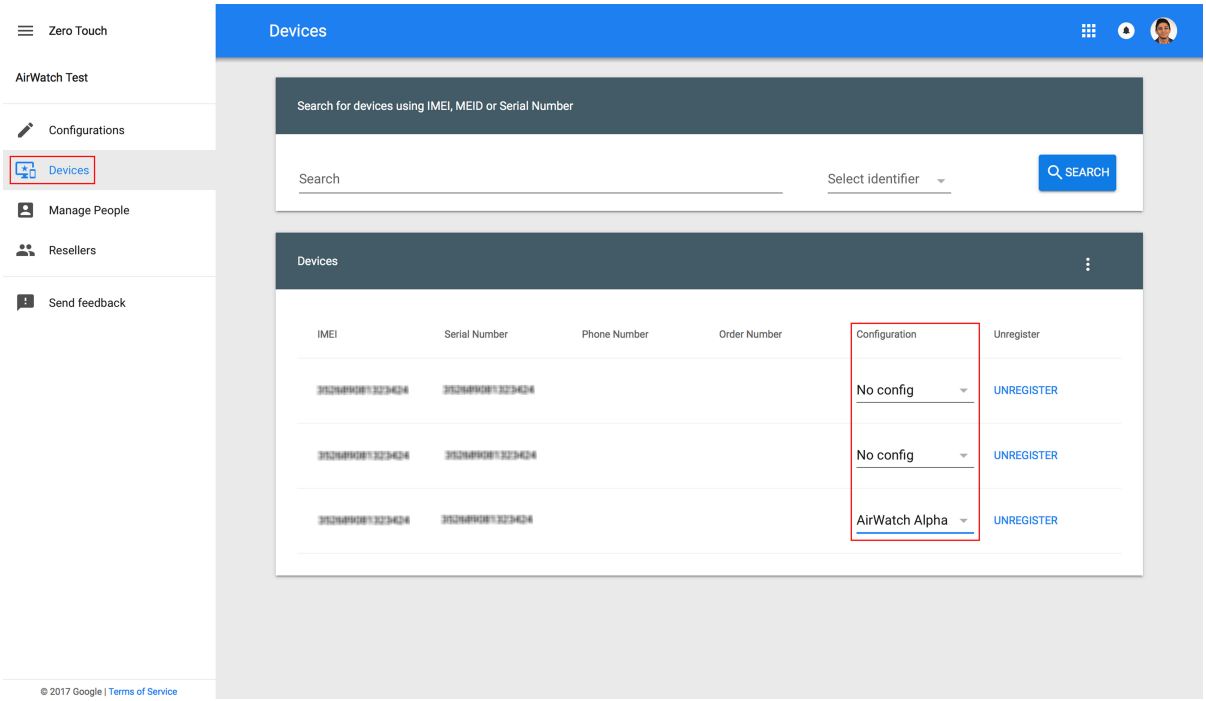
DPC supplémentaires	Entrez les identifiants d'enrôlement qui seront configurés dans Workspace ONE Intelligent Hub. Vous pouvez inclure l'URL du serveur de Workspace ONE UEM Console, l'ID de groupe, le nom d'utilisateur de l'enrôlement et le mot de passe.
	Terminal à provisionner pour l'utilisateur final :
	Dans ce scénario, excluez le nom d'utilisateur et le mot de passe. L'utilisateur est invité à les saisir lors de la configuration du terminal.
	`{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID"} }`
	Pour l'enrôlement sans contact :
	Ce scénario est recommandé si tous les terminaux sont préenrôlés pour un seul utilisateur ou si le nom d'utilisateur et le mot de passe d'enrôlement sont connus.
	`{ "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": { "serverurl": "https://airwatch.console.com", "gid": "groupID", "un":"username", "pw":"password" } }`

Paramètre	Description
Nom de l'entreprise	Saisissez le nom de votre organisation.
E-mail de contact	Entrez l'e-mail que les utilisateurs finaux doivent contacter s'ils rencontrent des problèmes.
Téléphone de contact	Entrez le numéro de téléphone que les utilisateurs finaux doivent appeler s'ils rencontrent des problèmes.
Message personnalisé	Entrez un message personnalisé à afficher aux utilisateurs finaux avant le téléchargement de Workspace ONE Intelligent Hub.

3 Sélectionnez **Appliquer**.

4 Attribuez des configurations sous l'onglet **Terminaux** en sélectionnant la configuration d'enrôlement qui doit être appliquée au terminal.

Renseignez-vous auprès de votre opérateur/fournisseur de terminaux pour récupérer l'IMEI et les numéros de série de vos terminaux.



Configuration de l'enrôlement de terminaux professionnels et personnels (COPE)

Le mode Terminaux professionnels et personnels (COPE) procure à Workspace ONE UEM un contrôle sur l'intégralité du terminal, tout en déployant un profil professionnel permettant à

l'utilisateur de s'en servir comme d'un terminal personnel. COPE est un hybride entre les modes Profil professionnel et Terminaux gérés pour le travail.

Note Android 8.0 ou version ultérieure est requis pour utiliser le déploiement COPE sur votre flotte de terminaux. Si vous tentez d'enrôler un terminal qui n'exécute pas Android 8.0, celui-ci est automatiquement enrôlé comme terminal géré pour le travail. Pour plus d'informations sur l'enrôlement de terminaux gérés pour le travail, consultez la section Configuration de l'enrôlement en mode Terminaux gérés pour le travail.

Il existe plusieurs façons d'enrôler des terminaux COPE :

- Par communication en champ proche (CCP) avec AirWatch Relay
- Avec un identifiant unique ou un code de jeton
- En scannant un code QR
- À l'aide de l'enrôlement sans contact
- Utiliser Knox Mobile Enrollment pour les terminaux Samsung. Vous pouvez trouver des informations dans la documentation Knox Mobile Enrollment.

Les méthodes d'enrôlement que vous souhaitez utiliser dépendent de vos besoins professionnels. Vous ne pouvez pas enrôler des terminaux tant que vous n'avez pas terminé l'inscription du jeton EMM pour Android. Reportez-vous à la documentation Chapitre 2 Inscription pour Android avec Workspace ONE UEM pour terminer l'enregistrement.

Enrôlement avec AirWatch Relay

AirWatch Relay est une application qui transmet les informations des terminaux parent à tous les terminaux enfant enrôlés dans Workspace ONE UEM avec Android. Ce processus se fait par le biais d'un transfert NFC et provisionne les terminaux enfant pour :

- Connectez le terminal parent pour copier le réseau Wi-Fi et appliquer les paramètres régionaux, notamment la date, l'heure et l'emplacement du terminal.
- Télécharger la dernière version de production de Workspace ONE Intelligent Hub pour Android.
- Installer en mode silencieux Workspace ONE Intelligent Hub en tant qu'administrateur du terminal.
- S'enrôler automatiquement dans Workspace ONE UEM.

AirWatch Relay vous permet d'enrôler tous les terminaux enfant par lots avant de les déployer auprès des utilisateurs finaux. Il évite ainsi aux utilisateurs finaux d'avoir à enrôler leurs propres terminaux. Tous les terminaux enfant doivent être en mode réinitialisation des paramètres d'usine et la fonction NFC doit être activée par défaut pour qu'ils soient enrôlés en tant que terminaux COPE.

Le processus de transfert NFC dépend de la version du système d'exploitation Android. Dans la mesure où le mode COPE est uniquement pris en charge sous Android 8.0 et versions ultérieures, l'enrôlement auprès de AirWatch Relay effectuera un seul transfert pour vous connecter et enrôler des terminaux enfant en une seule étape.

Pour l'enrôlement d'AirWatch Relay, reportez-vous à la documentation Enrôlement d'un terminal Android avec AirWatch Relay pour Android 6.0 et versions ultérieures

Enrôlement avec l'identifiant Workspace ONE Intelligent Hub

La méthode d'enrôlement avec l'identifiant Workspace ONE Intelligent Hub est une approche simplifiée pour l'enrôlement des terminaux COPE. Entrez un identifiant, ou valeur de hachage, unique sur un terminal réinitialisé sur les paramètres d'usine. Une fois l'identifiant saisi, l'enrôlement est automatisé, et Workspace ONE Intelligent Hub est déployé. L'utilisateur doit uniquement entrer les détails du serveur, le nom d'utilisateur et le mot de passe. Pour l'enrôlement avec l'identifiant Workspace ONE Intelligent Hub, reportez-vous à la documentation Enrôler des terminaux Android à l'aide de l'identifiant VMware Workspace ONE Intelligent Hub.

Enrôlement avec le code QR

Le provisionnement par code QR est un moyen facile d'enrôler une flotte de terminaux qui ne prennent pas en charge le NFC et le transfert NFC. Le code QR contient une section de configuration de paires clé-valeur avec toutes les informations nécessaires à l'enrôlement du terminal. Créez le code QR avant de commencer l'enrôlement. Vous pouvez générer le code QR à l'aide de l'assistant de configuration de l'enrôlement dans Workspace ONE UEM Console. Pour plus d'informations, reportez-vous à la section Génération d'un code QR à l'aide de l'assistant de configuration de l'enrôlement.

Le code QR comprend l'URL du serveur et les informations d'ID de groupe. Vous pouvez également inclure le nom d'utilisateur et le mot de passe ou laisser l'utilisateur entrer ses identifiants de connexion.

Voici le format du texte à coller dans le générateur de code QR :

```
{

"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://getwsone.com/mobileenrollment/airwatchagent.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
"android.app.extra.PROVISIONING_WIFI_SSID": "ssid",
"android.app.extra.PROVISIONING_WIFI_PASSWORD": "password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
"serverurl": "deviceservices.myserver.com",
"gid": "group_id",
```

```
"un":"username",
"pw":"password"
}
}
```

Pour l'enrôlement par code QR, consultez la section Enrôlement des terminaux gérés pour le travail à l'aide d'un code QR.

Enrôlement sans contact

L'enrôlement sans contact permet de configurer tout de suite les terminaux Android 8.0 et versions ultérieures avec Workspace ONE UEM comme fournisseur EMM.

Si le terminal est connecté à Internet pendant sa configuration, Workspace ONE Intelligent Hub est automatiquement téléchargé, et les détails de l'enrôlement sont automatiquement transmis pour enrôler le terminal sans interaction de l'utilisateur.

Voici certaines conditions préalables à prendre en compte :

L'enrôlement sans contact est uniquement pris en charge par un nombre limité d'opérateurs mobiles et d'OEM. Les clients doivent contacter leur opérateur pour s'assurer que le provisionnement sans contact est pris en charge. Pour en savoir plus sur les opérateurs et les terminaux pris en charge, consultez le site Web de Google.

Pour connaître les étapes de l'enrôlement Zero Touch, consultez la section Enrôler un terminal Android à l'aide du portail Zero Touch (sans contact).

Indicateurs d'enrôlement supplémentaires pris en charge pour l'enrôlement Android

Cette rubrique explique comment mettre en œuvre des indicateurs d'enrôlement supplémentaires à l'aide du code QR ou de l'enrôlement sur le portail Zero Touch.

Formatage

Dans l'exemple ci-dessous, les informations en **gras** indiquent les **Informations requises** lors de la mise en œuvre du code QR ou de l'enrôlement JSON.

Pour les valeurs facultatives, depuis `"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":`, entrez les identifiants d'enrôlement qui seront configurés dans le Workspace ONE Intelligent Hub. Vous pouvez inclure l'URL du serveur de Workspace ONE UEM Console, l'ID de groupe, le nom d'utilisateur de l'enrôlement et le mot de passe.

Là où apparaît `"VMwareSpecificflags":"EnterValue"`, reportez-vous aux indicateurs disponibles ci-dessous et utilisez la valeur correcte si nécessaire.

```
{
   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"com.airwatch.androidagent/
com.airwatch.agent.DeviceAdministratorReceiver",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7v
tW7i_o8=", "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"",
```

```
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION":"false",
   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{
      "serverurl":"",
      "gid":"",
      "un":"",
      "pw":"",
      "VMwareSpecificflags":"Value"
   }
}
```

Utiliser une authentification UEM

Si les utilisateurs souhaitent utiliser l'authentification UEM alors qu'ils sont sur Workspace ONE Access, ils doivent le notifier au moyen d'un nouveau code QR, qui est également utilisé dans le portail KME par le JSON personnalisé. Définissez la valeur booléenne en remplaçant la valeur « Booléen » par « vrai » ou « faux ».

```
"useUEMAuthentication":"Boolean"
```

URL de détection automatique locale

Définissez l'URL de détection automatique locale en remplaçant « Chaîne » dans l'exemple ci-dessous par une URL similaire à « www.monurldetectionautomatique.com ».

```
"localAutoDiscoveryUrl":"String"
```

Nombre de nouvelles tentatives de détection

Définissez le nombre de nouvelles tentatives de détection à l'aide d'une valeur entière. Par exemple, un nombre inférieur à 10. Voici, par exemple, comment entrer correctement cette valeur, en remplaçant « Valeur entière » par le nombre de votre choix.

```
"discoveryRetryCount":"Integer"
```

Intervalle de détection en secondes

Définissez l'intervalle avant nouvelle tentative de détection en secondes. Voici, par exemple, comment entrer correctement cette valeur, en remplaçant « Valeur entière » par le nombre de votre choix.

```
"discoveryIntervalInSeconds":"Integer"
```

Inscription AOSP

Autorisez le terminal à ignorer l'ajout d'un compte professionnel. Définissez la valeur booléenne en remplaçant la valeur « Booléen » par « vrai » ou « faux ».

```
"aospenrollment":"Boolean"
```

Nombre de nouvelles tentatives

Définissez le nombre de tentatives d'enrôlement automatique en cas d'échec. Envisagez d'utiliser une valeur inférieure à 10. Voici, par exemple, comment entrer correctement cette valeur, en remplaçant « Valeur entière » par le nombre de votre choix.

```
"retrycount":"Integer"
```

Autoriser la suppression de l'épinglage

Autorisez l'utilisateur à quitter le Hub lors de l'enrôlement. Définissez la valeur booléenne en remplaçant la valeur « Booléen » par « vrai » ou « faux ».

```
"allowUnpinning":"Boolean"
```

Enrôlement d'un terminal Android en mode Profil professionnel

Le processus d'enrôlement établit une connexion entre les terminaux Android et votre environnement AirWatch. Workspace ONE Intelligent Hub facilite l'enrôlement des terminaux et permet la gestion et l'accès en temps réel aux informations appropriées concernant le terminal.

Procédez comme suit pour installer Workspace ONE Intelligent Hub et authentifier les utilisateurs en fonction du workflow d'enrôlement.

Procédure

1. Téléchargez et installez Workspace ONE Intelligent Hub depuis le Google App Store.
2. Lancez Workspace ONE Intelligent Hub.
   a. Si vous avez configuré la détection automatique de la messagerie, Workspace ONE Intelligent Hub vous demande de saisir votre adresse e-mail. En outre, vous devrez peut-être sélectionner votre ID de groupe dans une liste.
   b. Si vous n'avez pas configuré la détection automatique de la messagerie, sélectionnez la méthode d'enrôlement désirée.
3. Entrez l'adresse e-mail ou l'URL d'inscription.
4. Saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis appuyez sur **Continuer**.
5. Acceptez les **conditions d'utilisation**.

6 Appuyez sur le bouton **Chiffrer** et acceptez les paramètres dans les invites suivantes. Workspace ONE Intelligent Hub se ferme une fois les paramètres de chiffrement acceptés. Appuyez sur la notification « **Chiffrement terminé** » pour revenir à Workspace ONE Intelligent Hub et poursuivre l'enrôlement.

   l'option de chiffrement du terminal dépend de sa version d'Android. Les terminaux sous Android Marshmallow sont chiffrés par défaut. Cette option ne s'affiche donc pas lors de l'enrôlement.

7 Appuyez sur **Configurer** pour configurer le profil professionnel qui sera associé au terminal.

8 Appuyez sur **OK** dans la Déclaration de confidentialité. Les autres écrans de l'enrôlement varient en fonction de la méthode de création des utilisateurs. Les paramètres d'entreprise de Workspace ONE UEM Console seront poussés vers le terminal. **Ceci termine l'enrôlement des terminaux pour les comptes Google Play gérés.**

9 Pour les comptes Google uniquement, appuyez sur **Démarrer** pour créer le profil professionnel et connecter le compte Google géré au terminal. Ces étapes varient en fonction de la méthode d'authentification : Pour procéder à l'enrôlement **Défini par l'utilisateur** :

   a Créez le mot de passe avec vos identifiants de connexion utilisateur et appuyez sur **Suivant**.

   b Entrez le **Mot de passe** du compte Google géré et appuyez sur **Suivant**.

10 Pour poursuivre avec **Directory Service Sync** :

   a Entrez votre **Mot de passe** et appuyez sur **Suivant**.

   b Sélectionnez **Continuer**.

   c Sélectionnez **Quitter**.

11 Pour suivre le workflow d'enrôlement **SAML** :

   a Entrez le **Nom d'utilisateur** et le **Mot de passe**, puis appuyez sur **Connexion**. L'utilisateur sera redirigé vers Workspace ONE Intelligent Hub.

Résultats

Si l'opération réussit, le profil professionnel est configuré pour le terminal, et la page des paramètres Workspace ONE Intelligent Hub est affichée. Le terminal est prêt à l'emploi conformément aux paramètres Android pour le profil professionnel.

Activation de l'enrôlement non géré pour les terminaux Android

Pour permettre à certains terminaux Android de s'enrôler à Workspace ONE UEM sans services Google, vous devez activer le mode Enregistré.

Les terminaux enrôlés via l'application Intelligent Hub sont gérés par MDM par défaut. Pour permettre à certains terminaux Android de s'enrôler sans gestion MDM, vous devez activer le mode non géré pour un Smart Group.

Les critères de sélection disponibles sont : la version du système d'exploitation, le type de propriété et le groupe d'utilisateurs.

Dans l'enrôlement non géré, les utilisateurs peuvent accéder aux applications qui nécessitent un niveau de sécurité de base. Lorsque des utilisateurs essaient d'accéder à une application qui nécessite d'être gérée, les utilisateurs sont guidés via le processus d'enrôlement dans MDM. Vous utilisez les stratégies d'application de gestion adaptative pour contrôler les niveaux de gestion des terminaux Android enrôlés sans gestion.

Procédure

1. Dans Workspace ONE UEM Console, sélectionnez le groupe organisationnel à activer avec l'enrôlement non géré et accédez à la page **Terminaux > Paramètres du terminal > Terminaux et utilisateurs > Général > Enrôlement > Mode de gestion**.
2. Dans les paramètres actuels, cliquez sur **Remplacer**.
3. Pour Android, sélectionnez **Activé**.
4. Dans Smart Groups, ajoutez le Smart Group qui est activé pour les enrôlements non gérés.
5. Cliquez sur **Enregistrer**.

Résultats

Les utilisateurs disposant de terminaux Android appartenant au Smart Group configuré bénéficient d'un accès non géré aux applications. Les utilisateurs peuvent utiliser l'application Workspace ONE Intelligent Hub pour accéder aux applications qui nécessitent un niveau de sécurité de base sans que le terminal ne soit enrôlé dans la gestion de terminaux mobiles Workspace ONE UEM.

Zebra Stage Now

Le client de préenrôlement Stage Now est la solution Android nouvelle génération de Zebra pour le préenrôlement des terminaux Zebra et leur préparation pour une utilisation en production.

Workspace ONE UEM prend en charge Stage Now avec les conditions et limitations suivantes.

Pour plus d'informations sur Zebra Mobility, reportez-vous à Zebra Mobility Extensions (MX) et Full MX Feature Matrix.

Si vous prévoyez d'enrôler des terminaux Zebra en mode Terminaux gérés pour le travail au moyen d'un code-barres Stage Now, procédez comme suit.

Conditions préalables

- Les terminaux Zebra doivent exécuter Android 7.0 avec MX version 7.1 ou ultérieure.

- Si vous souhaitez enrôler vos terminaux Zebra à l'aide d'un code-barres Stage Now, vous devez avoir chargé Intelligent Hub 8.2 pour Android ou version ultérieure sur la console en tant que module Workspace ONE Intelligent Hub.
- Les terminaux Zebra exécutant Android 6.0 et versions inférieures doivent continuer à utiliser Rapid Deployment comme client de préenrôlement par défaut.
- Seuls les serveurs relais en mode passif sont pris en charge. Les serveurs relais en mode actif ne sont pas pris en charge et ne fonctionnent pas avec le client Stage Now.
- Assurez-vous que le paramètre **URL Stage Now**, qui se trouve dans **Groupes et paramètres > Tous les paramètres > Système > Avancé > URL de sites**, est défini sur l'URL appropriée.
  - Si votre environnement sur site configure votre propre serveur Stage Now, inscrivez votre URL personnalisée dans ce champ.
  - Si votre environnement sur site ne configure pas votre propre serveur Stage Now, vous devez simplement ouvrir vos réseaux pour autoriser l'accès à l'URL répertoriée ici.
  - Les environnements SaaS n'ont pas besoin de modifier cette zone de texte.
- Il ne doit y avoir aucun compte Google présent sur le terminal lors d'une tentative d'enrôlement Stage Now en mode Terminaux gérés pour le travail.

Procédure

1. Utilisez le sélecteur de groupe organisationnel pour sélectionner celui que vous souhaitez configurer pour vos terminaux Android.
2. Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Android > Enregistrement EMM Android** et sélectionnez l'onglet **Restrictions d'inscription**.

3 Configurez les paramètres suivants :

Paramètre	Description
Paramètre actuel	Sélectionnez **Remplacer** pour appliquer les modifications au groupe organisationnel sélectionné à l'étape 1.
Définissez la méthode d'inscription pour ce groupe organisationnel	Ce paramètre détermine la manière dont ce groupe organisationnel traite les terminaux Android. Choisissez parmi les paramètres suivants : **Toujours utiliser Android** – Ce paramètre active le curseur Mode propriétaire du terminal sur l'écran Générer un code-barres Stage Now et le rend non modifiable. Cela force tous les terminaux Android enrôlés dans ce groupe organisationnel à être en mode propriétaire du terminal (ou mode Terminaux gérés pour le travail). **Toujours utiliser Android (hérité)** – Ce paramètre désactive le curseur Mode propriétaire du terminal sur l'écran Générer un code-barres Stage Now et le rend non modifiable. Cela force tous les terminaux Android enrôlés dans ce groupe organisationnel à être en mode d'administration du terminal. **Définir les groupes d'attribution qui utilisent Android** – Ce paramètre active le curseur Mode propriétaire du terminal sur l'écran Générer un code-barres Stage Now et le rend modifiable, ce qui vous permet de choisir d'enrôler des terminaux Android en mode propriétaire du terminal (mode Terminaux gérés pour le travail) ou en mode d'administration du terminal, en fonction des groupes d'attribution sélectionnés.

4 Demandez à votre utilisateur final d'effectuer les étapes suivantes pour enrôler son terminal :

a Démarrez le terminal dans un état « paramètres d'usine ».

b Assurez-vous qu'aucun compte Google n'est présent sur le terminal.

c Suivez les étapes de l'assistant de configuration ou scannez le code barres « ignorer l'assistant de configuration » fourni par Zebra.

d Ouvrez l'application Stage Now.

e Scannez le code barres.

Le terminal est automatiquement enrôlé en mode Terminaux gérés pour le travail.

Aperçu des profils Android

4

Les profils Android permettent de s'assurer de la bonne utilisation des terminaux et de la protection des données sensibles. Les profils remplissent de nombreuses fonctions : ils permettent notamment de mettre en œuvre les règles et procédures internes, ou de configurer et de préparer des terminaux Android selon l'utilisation souhaitée.

Profils Android ou Android (hérité)

Le déploiement de profils comporte deux types de profils Android : Android et Android (hérité). Sélectionnez l'option Profil Android si vous avez terminé l'enregistrement EMM Android. Si vous avez refusé l'inscription EMM, les profils Android (hérité) sont disponibles. Lorsque vous sélectionnez Android mais que vous n'avez pas procédé à l'inscription EMM pour Android, un message d'erreur s'affiche vous demandant d'aller sur la page des paramètres pour effectuer l'inscription EMM ou de procéder au déploiement du profil Android (hérité).

Pour passer en revue l'enregistrement EMM pour Android, reportez-vous à la documentation Chapitre 2 Inscription pour Android avec Workspace ONE UEM.

Mode Profil professionnel ou mode Terminaux gérés pour le travail

Un profil professionnel désigne un type d'administrateur spécial, conçu principalement pour un cas d'utilisation BYOD. Lorsque l'utilisateur dispose déjà d'un terminal personnel configuré avec son propre compte Google, l'enrôlement de Workspace ONE UEM crée un profil professionnel sur lequel il installe Workspace ONE Intelligent Hub.Workspace ONE UEM contrôle uniquement le profil professionnel. Les applications gérées sont installées dans le profil professionnel et disposent d'un badge de porte-documents orange pour se différencier des applications personnelles.

Le terminal géré pour le travail s'applique aux terminaux enrôlés à partir d'un état non provisionné (réinitialisation aux paramètres d'usine) et est recommandé pour les terminaux professionnels. Workspace ONE Intelligent Hub est installé pendant le processus de configuration et défini en tant que propriétaire du terminal, ce qui signifie que Workspace ONE UEM aura le contrôle de l'intégralité du terminal.

Les profils Android affichent les étiquettes suivantes : Profil professionnel et Terminaux gérés pour le travail.

Les options de profil avec l'étiquette Profil professionnel s'appliquent uniquement aux paramètres du Profil professionnel et aux applications, et n'affectent pas les applications ou paramètres personnels de l'utilisateur. Par exemple, certaines restrictions désactivent l'accès à l'appareil photo ou la capture d'écran. Ces restrictions affectent uniquement les applications avec le badge Android dans le Profil professionnel et n'ont pas d'impact sur les applications personnelles. Les options de profil configurées pour les Terminaux gérés pour le travail s'appliquent à l'intégralité du terminal. Chaque profil expliqué dans cette section indique le type de terminal affecté par le profil.

Accès aux terminaux

Certains profils de terminal configurent les paramètres d'accès à un terminal Android. 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 :

- Configurez un profil de code secret pour exiger un code secret pour l'ensemble du terminal (code secret du terminal) ou uniquement le Profil professionnel (code secret professionnel). Pour plus d'informations, reportez-vous à la documentation Profil de code d'accès (Android).
- Spécifier et contrôler comment, quand et où vos employés utilisent leur terminal. Pour plus d'informations, reportez-vous à la documentation Configuration de restrictions pour le terminal Android avec Workspace ONE UEM.

Sécurité des terminaux

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

- Accédez aux ressources internes telles que les e-mails, les fichiers et les contenus. Pour plus d'informations, reportez-vous à la documentation Configurer un VPN (Android).
- Entreprenez des actions administratives lorsqu'un utilisateur installe ou désinstalle certaines applications. Pour plus d'informations, reportez-vous à la documentation Contrôle des applications (Android).

Configuration des terminaux

Configurez les divers paramètres de vos terminaux Android 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.

- Connectez votre terminal automatiquement au réseau Wi-Fi interne. Pour plus d’informations, reportez-vous à Profil Wi-Fi (Android).

- Gérez comment sont contrôlées les notifications de mise à jour et les mises à jour réelles de l'OS Android. Pour plus d'informations, reportez-vous à la documentation Gérer les mises à jour système pour les terminaux Android.

Ce chapitre contient les rubriques suivantes :

Profil de code d'accès (Android)

Le profil Code secret vous permet de configurer un code secret au niveau du terminal ou un code secret qui s'applique uniquement au profil professionnel sur les terminaux Android.

Les politiques de code secret de profil professionnel s'appliquent uniquement aux applications professionnelles afin que les utilisateurs n'aient pas à saisir de mots de passe complexes chaque fois qu'ils déverrouillent leur terminal lorsqu'il est inscrit avec un profil professionnel. Le profil professionnel conserve les données des applications d'entreprise protégées et permet aux

utilisateurs finaux d'accéder aux applications et aux données personnelles comme bon leur semble. Pour les terminaux gérés pour le travail, cette politique de code d'accès s'applique au terminal. Le code d'accès professionnel est disponible sur Android 7.0 (Nougat) et versions ultérieures pour les terminaux enrôlés avec un profil professionnel.

Les politiques de code secret du terminal s'appliquent à l'ensemble du terminal (inscrit avec un profil professionnel ou géré pour le travail). Ce code d'accès doit être saisi chaque fois que le terminal est déverrouillé. Il peut être appliqué en plus du code d'accès professionnel.

Par défaut, lors de la création de nouveaux profils, seul le code secret professionnel est activé (le code secret du terminal est désactivé). L'administrateur doit activer manuellement le code d'accès du terminal.

Note Lorsque le profil avec code secret est présent sur le terminal et que l'utilisateur ne définit pas le code secret, aucune application ou aucun profil n'est transféré vers le terminal tant que celui-ci n'est pas conforme.

Appliquer les paramètres du code d'accès (Android)

Une politique de code d'accès exige de vos utilisateurs finaux qu'ils saisissent un code d'accès, fournissant ainsi un premier niveau de sécurité pour les données sensibles des terminaux.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil appropriés dans l'onglet **Général**.
3. Sélectionnez **Code d'accès** dans la liste de sections de configuration et configurez les paramètres de code d'accès :

Paramètres	Description
Activer la politique de code d'accès profesionnelle	Activez cette option pour appliquer les politiques de codes d'accès uniquement aux applications badgées par Android.
longueur min. du code d'accès	Assurez-vous que les codes d'accès sont suffisamment complexes en définissant un nombre minimal de caractères.

Paramètres	Description
Contenu du code d'accès	Assurez-vous que le contenu du code d'accès respecte vos exigences de sécurité en sélectionnant l'une des options suivantes : **Indifférent**, **Numérique**, **Alphanumérique**, **Alphabétique**, **Complexe**, **Numérique complexe** ou **Biométrique faible** dans le menu déroulant. 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. Un contenu de code d'accès à faible biométrie permet d'utiliser des méthodes de déverrouillage biométrique avec une sécurité réduite, telles que la reconnaissance faciale. **Important** Si le nombre minimal de caractères complexes dans le mot de passe est supérieur à 4, au moins un caractère en minuscule et un caractère en majuscule sont nécessaires (terminaux SAFE v5.2 uniquement).
Nombre maximum de tentatives infructueuses	Indiquez le nombre de tentatives autorisées avant la réinitialisation du terminal.
Durée de vie maximale du code d'accès (en jours)	Indiquez le nombre maximum de jours durant lequel le code d'accès restera actif.
Alerte de modification du code secret	Définit la durée restante avant l'expiration du code secret. L'utilisateur recevra une notification l'invitant à le modifier. Cette option est également disponible dans la stratégie de code secret du terminal. L'utilisateur est invité à modifier le code secret via l'invite sur son terminal, mais il n'est pas autorisé à y effectuer d'autres tâches. Vous pouvez configurer une stratégie de conformité ou utiliser les paramètres du Workspace ONE Intelligent Hub pour Android afin de créer et d'appliquer un code secret qui est à nouveau ajouté au terminal.
historique du code d'accès	Indiquez le nombre de changements de code d'accès requis avant qu'un ancien code ne puisse être réutilisé.
Plage d'expiration du verrouillage du terminal (en minutes)	Définit le délai d'inactivité avant que l'écran du terminal ne se verrouille.
Modification du code secret requise (en minutes)	Définit la durée après le déverrouillage d'un terminal via une authentification non forte (telle qu'une empreinte digitale ou une reconnaissance faciale) qui s'écoule avant qu'un code secret ne soit requis. Cette option est également disponible dans la stratégie de code secret du terminal.
Autoriser le verrouillage One	Désactivez cette option pour séparer le code secret du profil professionnel et du terminal **Note** S'applique aux profils professionnels des terminaux Android 9.0+ et aux terminaux COPE uniquement.
Autoriser les options biométriques	Activez cette option pour autoriser les méthodes de déverrouillage biométriques, telles que la reconnaissance faciale.
Autoriser le capteur d'empreinte	Activer ce paramètre pour permettre aux utilisateurs d'utiliser leurs empreintes digitales pour déverrouiller leurs terminaux. Désactivez cette option pour empêcher l'utilisation de l'empreinte digitale comme méthode d'authentification principale, et demandez à l'utilisateur d'entrer un mot de passe spécifié dans le profil.

Paramètres	Description
Autoriser la reconnaissance faciale	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode de déverrouillage facial. **Note** S'applique aux terminaux professionnels gérés Android 9.0+ uniquement.
Autoriser la reconnaissance d'iris	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode de reconnaissance d'iris. **Note** S'applique aux terminaux professionnels gérés Android 9.0+ uniquement.
Activer la politique de code d'accès aux terminaux	Appliquez les politiques de code d'accès pour le terminal enrôlé avec un profil professionnel. Ce code d'accès doit être saisi pour déverrouiller le terminal. Il peut être appliqué en plus du code d'accès professionnel. Pour les terminaux gérés pour le travail, cette politique de code d'accès est appliquée au terminal.
longueur min. du code d'accès	Assurez-vous que les codes d'accès sont suffisamment complexes en définissant un nombre minimal de caractères.
Définir le code secret initial	Activez cette fonction pour définir un code secret initial au niveau du terminal sur tous les terminaux déployés. Après le déploiement, il est possible de réinitialiser le code secret au niveau du terminal. **Note** S'applique aux terminaux professionnels gérés Android 7.0+ uniquement.
Contenu du code d'accès	Pour vous assurer que le contenu du code d'accès respecte vos exigences de sécurité, sélectionnez **Indifférent**, **Numérique**, **Alphanumérique**, **Alphabétique**,**Complexe** ou **Numérique complexe** dans le menu déroulant.
Nombre maximum de tentatives infructueuses	Indiquez le nombre de tentatives autorisées avant la réinitialisation du terminal.
Durée de vie maximale du code d'accès (en jours)	Indiquez le nombre maximum de jours durant lequel le code d'accès restera actif.
Alerte de modification du code secret	Définit la durée restante avant l'expiration du code secret. L'utilisateur recevra une notification l'invitant à le modifier.
historique du code d'accès	Indiquez le nombre de changements de code d'accès requis avant qu'un ancien code ne puisse être réutilisé.
Plage d'expiration du verrouillage du terminal (en minutes)	Définissez le temps d'inactivité avant le verrouillage automatique de l'écran du terminal.
Autoriser les options biométriques	Activez cette option pour autoriser les méthodes de déverrouillage biométriques, telles que la reconnaissance faciale.
Autoriser le déverrouillage par empreintes digitales	Autorisez le déverrouillage par empreinte digitale comme deuxième méthode d'authentification uniquement, et demandez à l'utilisateur de saisir un mot de passe spécifié dans le profil.
Autoriser la reconnaissance faciale	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode Déverrouillage facial sur le terminal Samsung. **Note** S'applique aux terminaux professionnels gérés Android 9.0+ uniquement.

Paramètres	Description
Autoriser la reconnaissance d'iris	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode Scanner d'iris sur le terminal Samsung. **Note** S'applique aux terminaux professionnels gérés Android 9.0+ uniquement.
Code d'accès visible	Activez ce paramètre pour afficher le code d'accès à l'écran, tel qu'il est saisi. Pour les terminaux Samsung. Nécessite que vous activiez les **Paramètres OEM** dans le profil **Général** et **Samsung** à partir de la liste déroulante **Sélectionner OEM**.
Exiger le chiffrement de la carte SD	Indiquez si la carte SD requiert un chiffrement. Pour les terminaux Samsung. Nécessite que vous activiez les **Paramètres OEM** dans le profil **Général** et **Samsung** à partir de la liste déroulante **Sélectionner OEM**.
Nombre maximum de caractères répétés	Pour empêcher vos utilisateurs finaux de saisir des codes d'accès répétitifs facilement piratables comme « 1111 », définissez un nombre maximum de caractères répétés. Pour les terminaux Samsung.

Les paramètres suivants s'appliquent si vous sélectionnez Complexe dans la zone de texte **Contenu du code d'accès**.

Paramètre	Description
Nombre minimum de lettres	Indiquez le nombre de lettres qui peuvent être incluses dans le code d'accès.
Nombre minimum de minuscules	Indiquez le nombre de lettres minuscules requises dans le code secret.
Nombre minimum de majuscules	Indiquez le nombre de lettres majuscules requises dans le code secret.
Nombre minimum de caractères non alphabétiques	Indiquez le nombre de caractères spéciaux requis dans le code secret.
Nombre minimum de chiffres	Indiquez le nombre de chiffres requis dans le code secret.
Nombre minimum de symboles	Indiquez le nombre de symboles requis dans le code secret.

Les paramètres suivants s'appliquent pour définir un code secret sur un terminal Samsung.

Ces paramètres s'affichent uniquement lorsque les **Paramètres OEM** dans les profils **Général** et **Samsung** à partir de la liste déroulante **Sélectionner OEM**.

sont activés.

Paramètre	Description
Code d'accès visible	Activez ce paramètre pour afficher le code d'accès à l'écran, tel qu'il est saisi.
Autoriser le déverrouillage par empreintes digitales	Autorisez le déverrouillage par empreinte digitale comme deuxième méthode d'authentification uniquement, et demandez à l'utilisateur de saisir un mot de passe spécifié dans le profil.
Exiger le chiffrement de la carte SD	Indiquez si la carte SD requiert un chiffrement.
Demander le code d'accès	Nécessite que l'utilisateur entre le code secret utilisé pour chiffrer la carte SD. Si la case n'est pas cochée, certains terminaux autorisent le chiffrement de la carte SD sans interaction de l'utilisateur.

Paramètre	Description
Nombre maximum de caractères répétés	Pour empêcher vos utilisateurs finaux de saisir des codes d'accès répétitifs facilement piratables comme « 1111 », définissez un nombre maximum de caractères répétés.
Longueur maximum des séquences numériques	Empêchez vos utilisateurs finaux de saisir un code d'accès sous forme d'une séquence numérique facilement piratable comme « 1234 ». Pour les terminaux Samsung.
Autoriser le scanner d'iris	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode Scanner d'iris sur le terminal Samsung.
Déverrouillage par reconnaissance faciale	Désactivez cette option pour empêcher la configuration ou la sélection de la méthode Déverrouillage facial sur le terminal Samsung.
Superposition de l'écran de verrouillage	Activez ce paramètre pour permettre aux administrateurs d'envoyer des informations qui s'afficheront sur l'écran de verrouillage des terminaux des utilisateurs finaux. ■ **Superposition d'images** – Importez des images à superposer à l'écran de verrouillage. Vous pouvez importer une image principale et une image secondaire, puis déterminer la position et la transparence de chacune. ■ **Informations sur l'entreprise** – Saisissez les informations sur l'entreprise à afficher sur l'écran de verrouillage. Ces informations peuvent servir en cas d'urgence, si le terminal est perdu ou signalé comme volé. Le paramètre de superposition sur l'écran de verrouillage s'applique uniquement aux terminaux SAFE 5.0 et versions ultérieures. Ce paramètre reste configuré sur le terminal durant son utilisation et ne pourra pas être modifié par l'utilisateur final. Pour plus d'informations sur les paramètres de superposition de l'écran de verrouillage, consultez la section Configurer la superposition de l'écran de verrouillage (Android)

4 Cliquez sur **Enregistrer et publier** pour attribuer le profil aux terminaux associés.

Configurer la superposition de l'écran de verrouillage (Android)

Dans le profil de code d'accès, l'option **Superposition de l'écran de verrouillage** vous permet de superposer des informations sur l'image de l'écran de verrouillage à l'intention de l'utilisateur final ou de la personne qui trouverait un terminal verrouillé. Superposition de l'écran de verrouillage fait partie du profil Code d'accès.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Sélectionnez **Android** ou **Android (Hérité)** en fonction de votre configuration d'enrôlement.

3 Configurez les paramètres de profil appropriés dans l'onglet **Général**.

La superposition de l'écran de verrouillage est une fonctionnalité native pour Android qui est disponible pour plusieurs licences OEM.

Les paramètres de la superposition de l'écran de verrouillage pour les profils **Android** s'affichent lorsque le champ **Paramètres OEM** est défini sur **Activé** et que Samsung est sélectionné dans le champ **Sélectionner l'OEM**. Le champ Paramètres OEM du profil général s'applique uniquement aux profils Android et non aux configurations Android (héritées).

4 Sélectionnez le profil **Code d'accès** dans la liste.

5 Activez l'option **Superposition de l'écran de verrouillage**.

6 Sélectionnez votre type de superposition désiré sur l'écran de verrouillage : **Superposition d'images** ou **Informations sur l'entreprise**.

7 Configurez les paramètres de superposition d'images.

Paramètre	Description
Type de superposition d'images	Sélectionnez **Image unique** ou **Plusieurs images** pour déterminer le nombre d'images à superposer.
Image principale	Importez un fichier image.
Position au premier plan de l'image principale en pourcentage	Déterminez la position de l'image au premier plan en indiquant une valeur comprise entre 0 et 90 %.
Position inférieure de l'image principale en pourcentage	Déterminez la position de l'image en arrière-plan en indiquant une valeur comprise entre 0 et 90 %.
Image secondaire	Importez une deuxième image si vous le souhaitez. Ce paramètre s'affiche uniquement si vous avez sélectionné l'option Plusieurs images, dans le champ **Type de superposition d'images**.
Position de l'image secondaire en pourcentage	Déterminez la position de l'image au premier plan en indiquant une valeur comprise entre 0 et 90 %. Ce paramètre s'affiche uniquement si vous avez sélectionné l'option Plusieurs images, dans le champ Type de superposition d'images.
Position inférieure de l'image secondaire en pourcentage	Déterminez la position de l'image en arrière-plan en indiquant une valeur comprise entre 0 et 90 %. Ce paramètre s'affiche uniquement si vous avez sélectionné l'option Plusieurs images, dans le champ Type de superposition d'images.
Image en filigrane	Déterminez la transparence de l'image en sélectionnant **Transparent** ou **Opaque**.

8 Configurez les paramètres des **Informations sur l'entreprise**.

Paramètre	Description
Nom de l'entreprise	Saisissez le nom de l'entreprise à afficher.
Logo de l'entreprise	Importez le logo de l'entreprise sous forme de fichier image.
Adresse de l'entreprise	Indiquez l'adresse de l'entreprise.
Numéro de téléphone de l'entreprise	Indiquez le numéro de téléphone de l'entreprise.
Image en filigrane	Déterminez la transparence de l'image en sélectionnant **Transparent** ou **Opaque**.

9 **Enregistrer et publier**.

Appliquer les paramètres du navigateur Chrome (Android)

Le profil Paramètres du navigateur Chrome vous aide à gérer les paramètres de l'application Work Chrome.

Chrome est le navigateur Web de Google. Chrome offre un certain nombre de fonctionnalités telles que la recherche, l'omnibox (une zone permettant de faire des recherches et de naviguer), le remplissage automatique, l'enregistrement des mots de passe et la connexion au compte Google pour accéder instantanément aux derniers onglets et recherches sur tous vos terminaux. L'application Work Chrome fonctionne de la même manière que la version personnelle de Chrome. La configuration de ce profil n'affectera pas l'application Chrome personnelle de l'utilisateur. Vous pouvez pousser ce profil avec une section de configuration VPN ou Identifiants +Wi-Fi séparée pour garantir que les utilisateurs finaux peuvent s'authentifier et se connecter à vos sites et systèmes internes. Cela permet de s'assurer que les utilisateurs utilisent l'application Work Chrome à des fins professionnelles.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Sélectionnez la section de configuration **Paramètres du navigateur Chrome** et configurez les paramètres comme vous le souhaitez.

4 Cliquez sur **Enregistrer et publier**.

Matrice des paramètres du navigateur Chrome (Android)

Le profil Paramètres du navigateur Chrome vous aide à gérer les paramètres de l'application Work Chrome. La configuration de ce profil n'affectera pas l'application Chrome personnelle de l'utilisateur. Vous pouvez pousser ce profil avec une section de configuration VPN ou Identifiants +Wi-Fi séparée pour garantir que les utilisateurs finaux peuvent s'authentifier et se connecter à vos sites et systèmes internes.

Cette matrice présente en détail les paramètres disponibles dans le profil du navigateur Chrome :

Tableau 4-1. Paramètres du navigateur Chrome Paramètres du profil

Paramètre	Description
Autoriser les cookies	Sélectionnez ce paramètre pour déterminer les paramètres de cookies du navigateur.
Autoriser les cookies sur ces sites	Spécifiez les URL autorisées à définir des cookies.
Bloquer les cookies sur ces sites	Spécifiez les URL non autorisés à définir des cookies.
Autoriser uniquement les cookies de session sur ces sites	Spécifiez les sites autorisés à définir des cookies uniquement pour la session.

Tableau 4-1. Paramètres du navigateur Chrome Paramètres du profil (suite)

Paramètre	Description
Autoriser les images	Sélectionnez ce paramètre pour déterminer les sites autorisés à afficher des images.
Autoriser les images sur ces sites	Spécifiez une liste d'URL autorisées à afficher des images.
Bloquer les images sur ces sites	Spécifiez une liste d'URL non autorisées à afficher des images.
Autoriser JavaScript	Sélectionnez les paramètres JavaScript du navigateur.
Autoriser Javascript sur ces sites	Spécifiez les sites autorisés à exécuter JavaScript.
Bloquer Javascript sur ces sites	Spécifiez les sites non autorisés à exécuter JavaScript.
Autoriser les fenêtres pop-up	Sélectionnez les paramètres de pop-up du navigateur.
Autoriser les pop-ups sur ces sites	Sélectionnez une option pour identifier les sites autorisés à ouvrir des fenêtres contextuelles.
Bloquer les pop-ups sur ces sites	Spécifiez les sites non autorisés à ouvrir des fenêtres pop-up.
Autoriser le suivi de la localisation	Déterminez si les sites Web sont autorisés à effectuer le suivi de l'emplacement physique des utilisateurs.
Mode proxy	Spécifiez le serveur proxy utilisé par Google Chrome et empêchez les utilisateurs de modifier les paramètres de proxy.
URL du serveur proxy	Spécifiez l'URL du serveur proxy.
URL du fichier PAC du proxy	Indiquez une URL pointant vers un fichier .pac du proxy.
Règles de contournement du proxy	Spécifiez les paramètres de proxy à contourner. Cette stratégie n'entre en vigueur que si vous avez sélectionné les paramètres de proxy manuels.
Forcer Google SafeSearch	Activez ce paramètre pour forcer les requêtes de recherche dans la recherche Web Google à effectuer avec SafeSearch.
Forcer le mode sécurisé de Youtube	Activez ce paramètre pour donner aux utilisateurs la possibilité de bloquer le contenu pour adulte.
Activer Touch to Search	Permet d'utiliser Touch to Search dans l'affichage du contenu de Google Chrome.
Activer le moteur de recherche par défaut	Spécifiez le moteur de recherche par défaut.
Nom du moteur de recherche par défaut	Spécifiez le nom du moteur de recherche par défaut.
Mot-clé du moteur de recherche par défaut	Spécifiez la recherche par mot-clé pour le moteur de recherche par défaut.
URL de recherche du moteur de recherche par défaut	Spécifiez l'URL du moteur de recherche utilisé lorsque vous effectuez une recherche par défaut.
URL suggérée du moteur de recherche par défaut	Spécifiez l'URL du moteur de recherche utilisé pour fournir des suggestions de recherche.

Tableau 4-1. Paramètres du navigateur Chrome Paramètres du profil (suite)

Paramètre	Description
URL instantanée du moteur de recherche par défaut	Spécifiez les moteurs de recherche par défaut lorsque l'utilisateur saisit des demandes de recherche.
Icône du moteur de recherche par défaut	Spécifiez l'URL de l'icône des favoris du moteur de recherche par défaut.
Encodages du moteur de recherche par défaut	Spécifiez les encodages de caractères pris en charge par le moteur de recherche. Les encodages sont des noms de page de code tels que UTF-8, GB2312 et ISO-8859-1. Si elle n'est pas définie, la valeur par défaut sera utilisé (UTF-8).
Liste d'URL alternatives pour le moteur de recherche par défaut	Spécifiez une liste d'URL alternatives qui peuvent être utilisées pour extraire des termes de recherche du moteur de recherche.
Clé de remplacement des termes de recherche	Entrez toutes les clés de remplacement des termes de recherche.
URL de l'image du moteur de recherche	Spécifiez l'URL du moteur de recherche utilisé pour permettre une recherche d'images.
URL du nouvel onglet	Spécifiez l'URL utilisée par un moteur de recherche pour fournir une page Nouvel onglet.
Paramètres de recherche d'URL POST	Spécifiez les paramètres utilisés lors de la recherche d'une URL avec POST.
Paramètres de recherche de suggestion POST	Spécifiez les paramètres utilisés lors d'une recherche d'images avec POST.
Paramètres de recherche d'image POST	Spécifiez les paramètres utilisés lors d'une recherche d'images avec POST.
Activer le gestionnaire de mots de passe	Activez l'enregistrement de mots de passe dans le gestionnaire de mot de passe.
Autoriser les autres pages d'erreur	Activez ce paramètre pour utiliser les autres pages d'erreur intégrées dans Google Chrome (tels que « Page non trouvée »).
Activez la saisie automatique	Activez ce paramètre pour permettre aux utilisateurs à renseigner automatiquement des formulaires Web en utilisant les informations stockées précédemment tels que les informations d'adresse ou de carte de crédit.
Activer l'impression	Activez ce paramètre pour autoriser l'impression dans Google Chrome.
Activer la fonction proxy de compression des données	Spécifiez l'une des options suivantes pour le proxy de compression des données : toujours activer, toujours désactiver. Le proxy de compression des données peut réduire l'utilisation des données cellulaires et accélérer la navigation Web mobile en utilisant des serveurs proxy hébergés par Google pour optimiser le contenu du site Web.

Tableau 4-1. Paramètres du navigateur Chrome Paramètres du profil (suite)

Paramètre	Description
Activer la navigation sécurisée	Activez ce paramètre pour activer la navigation sécurisée de Google Chrome.
Désactiver l'enregistrement de l'historique du navigateur	Activez ce paramètre pour désactiver l'enregistrement de l'historique du navigateur Google Chrome.
Empêcher de continuer après une alerte de navigation sécurisée	Activez ce paramètre pour empêcher les utilisateurs de continuer au-delà de la page d'avertissement de sites malveillants.
Désactiver le protocole SPDY	Désactive l'utilisation du protocole SPDY dans Google Chrome.
Activer la prédiction du réseau	Sélectionnez la prédiction du réseau dans Google Chrome.
Activer les fonctionnalités obsolètes de la plateforme Web pour une durée limitée	Spécifiez une liste de fonctionnalités de plateforme Web obsolètes pour les réactiver temporairement.
Forcer la recherche sécurisée	Activez ce paramètre pour activer la recherche sécurisée lors de l'utilisation du navigateur Web.
Disponibilité de la navigation privée	Spécifiez si un utilisateur peut ouvrir des pages en mode de navigation privée dand Google Chrome.
Autorise la connexion à Chromium	Activez ce paramètre pour forcer les utilisateurs Chrome à se connecter au navigateur s'ils se sont connectés à Gmail sur le Web.
Activer les suggestions de recherche	Activez les suggestions de recherche dans l'omnibox de Google Chrome.
Autoriser la traduction	Activez le service Google Traduction intégré à Google Chrome.
Active ou désactive la modification des signets	Activez ce paramètre pour autoriser l'ajout, la suppression ou la modification de signets.
Signets gérés	Spécifiez une liste de signets gérés.
Bloquer l'accès à une liste d'URL	Entrez des URL dans la liste noire pour empêcher l'utilisateur de charger des pages Web.
Exceptions à la liste d'URL bloquées	Entrez les URL des exceptions de la liste de blocage.
Version SSL minimale activée	Sélectionnez la version SSL minimale dans le menu déroulant.
Version SSL minimale à rétablir	Sélectionnez le version minimale de SSL à rétablir depuis le menu déroulant.

Configuration de restrictions pour le terminal Android avec Workspace ONE UEM

Les profils de restriction dans la console UEM verrouillent la fonctionnalité native des terminaux Android. Les restrictions et le comportement disponibles varient en fonction de l'enrôlement du terminal.

Le profil **Restrictions** affiche des étiquettes qui indiquent si la restriction sélectionnée s'applique au mode Profil professionnel, Terminaux gérés pour le travail ou aux deux. Cependant, pour les terminaux avec un Profil professionnel, elles n'affectent que les applications badgées par Android. Par exemple, lorsque vous configurez des restrictions pour le Profil professionnel, vous pouvez désactiver l'accès à l'application Camera professionnelle. Ceci affecte uniquement l'application Camera badgée par Android et non l'application Camera personnelle de l'utilisateur.

Note : quelques applications système sont incluses par défaut dans le profil professionnel : Work Chrome, Google Play, Google Settings, Contacts et Camera, par exemple. Ces applications peuvent être masquées à l'aide d'un profil de restrictions et n'affectent pas l'application Camera personnelle de l'utilisateur.

Restrictions sur l'utilisation de comptes Google non gérés

Il est possible que vous souhaitiez autoriser des personnes à ajouter des comptes Google non gérés ou personnels, par exemple, pour lire des mails personnels, mais que vous vouliez quand même empêcher le compte personnel d'installer des applications sur le terminal. Vous pouvez définir une liste de comptes que les personnes peuvent utiliser dans Google Play dans la Workspace ONE UEM console.

Configurer des restrictions pour les terminaux Android

Déployez une section de configuration Restrictions pour renforcer la sécurité sur des terminaux Android. Les sections de configuration Restrictions permettent de désactiver l'accès des utilisateurs aux fonctions du terminal pour veiller à ce que les terminaux ne soient pas altérés.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil de l'onglet **Général**.

3 Sélectionnez le profil **Restrictions** et configurez les paramètres :

Paramètres	Description
Fonctionnalités des terminaux	Les restrictions au niveau du terminal peuvent désactiver des fonctionnalités importantes des terminaux comme l'appareil photo, la capture d'écran et la réinitialisation aux paramètres d'usine, pour une productivité et une sécurité optimales. La désactivation de l'appareil photo évite par exemple que des documents sensibles ne soient photographiés et transmis à un tiers extérieur à l'entreprise. Le blocage des captures d'écran aide à préserver la confidentialité du contenu professionnel du terminal.
Win32	Les restrictions au niveau de l'application peuvent désactiver certaines applications comme YouTube et le navigateur natif, ce qui vous permet de garantir le respect des politiques d'utilisation des terminaux de l'entreprise.
Synchronisation et stockage	Contrôlez la manière dont les informations sont stockées sur les terminaux afin de maintenir un équilibre optimal entre productivité et sécurité. La désactivation des sauvegardes Google et USB permet par exemple de conserver les données mobiles professionnelles sur les terminaux gérés et hors de portée d'individus malveillants.
Réseau	Empêchez les terminaux d'accéder au Wi-Fi et aux connexions données pour vous assurer que les utilisateurs finaux ne consultent pas d'informations sensibles via une connexion non sécurisée.
Professionnel et personnel	Permet de définir l'accès et le partage des informations entre un conteneur personnel et un conteneur professionnel. Ces paramètres s'appliquent uniquement au mode Profil professionnel.
services de localisation	Configurez les paramètres du service de localisation uniquement pour les terminaux gérés pour le travail.
Samsung Knox	Configurez les restrictions spécifiquement pour les terminaux Android exécutant Samsung Knox. Cette section est disponible uniquement lorsque l'option **Paramètres OEM** du profil général est activée et que Samsung est sélectionné dans le champ **Sélectionner OEM**.

4 Sélectionnez **Enregistrer et publier** pour attribuer le profil aux terminaux associés.

Activer le profil Active Exchange Sync sur les terminaux Android

Workspace ONE UEM utilise le profil EAS (Exchange ActiveSync) sur les terminaux Android pour garantir une connexion sécurisée aux données internes (e-mails, calendriers et contacts) avec des clients de messagerie. Par exemple, les paramètres de messagerie EAS configurés pour le profil professionnel affectent toutes les applications de messagerie téléchargées à partir du catalogue Workspace ONE UEM avec l'icône badgée, mais ils n'affectent pas la messagerie personnelle de l'utilisateur.

Conditions préalables

Une fois que chaque utilisateur dispose d'une adresse e-mail et d'un nom d'utilisateur, vous pouvez créer un profil Exchange Active Sync.

Note Le profil Exchange Active Sync s'applique aux types de modes Profil professionnel et Terminaux gérés pour le travail.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil appropriés dans l'onglet **Général**.
3. Sélectionnez le profil **Exchange Active Sync** et configurez les paramètres suivants.

Paramètres	Description
Type de client de messagerie	Utilisez le menu déroulant pour sélectionner un client de messagerie qui est poussé vers les terminaux utilisateur.
Hôte	Indiquez l'URL externe du serveur ActiveSync de votre entreprise.
Type de serveur	Choisissez entre **Exchange** et **Lotus**.
Utiliser le SSL	Permet d'activer le chiffrement des données EAS.
Désactiver les contrôles de validation sur les certificats SSL	Permet d'activer les certifications SSL (Secure Socket Layer).
S/MIME	Activez cette option pour sélectionner un certificat S/MIME que vous associez en tant que certificat utilisateur dans la section de configuration **Identifiants**. ■ **Certificat de signature S/MIME** – Sélectionnez le certificat pour permettre la distribution de certificats S/MIME au client pour la signature des messages. ■ **Certificat S/MIME de chiffrement** – Sélectionnez le certificat pour permettre la distribution de certificats S/MIME au client pour le chiffrement des messages.
Domaine	Utilisez les valeurs de recherche pour sélectionner la valeur spécifique au terminal.
Nom d'utilisateur	Utilisez les valeurs de recherche pour sélectionner la valeur spécifique au terminal.
Adresse e-mail	Utilisez les valeurs de recherche pour sélectionner la valeur spécifique au terminal.
Mot de passe	Ne remplissez pas ce champ pour permettre aux utilisateurs finaux de définir leur propre mot de passe.
Certificat de connexion	Sélectionnez le certificat disponible dans le menu déroulant.
Signature par défaut	Indiquez une signature d'e-mail par défaut à afficher sur les nouveaux messages.

Paramètres	Description
Taille maximale des pièces jointes (Mo)	Entrez la taille maximale des pièces jointes que l'utilisateur est autorisé à envoyer.
Autoriser la synchronisation du calendrier et des contacts	Permet d'autoriser la synchronisation des contacts et du calendrier avec les terminaux.

4 Sélectionnez **Enregistrer et publier** pour attribuer le profil aux terminaux associés.

Profil de mise à jour automatique d'applications publiques (Android)

Le profil de mise à jour automatique d'applications publiques vous permet de configurer des mises à jour automatiques et de planifier des fenêtres de maintenance pour les applications Android publiques.

Le profil de mise à jour automatique d'application publique utilise les API Google pour envoyer des données de profil directement aux terminaux. Ce profil ne sera pas affiché dans Workspace ONE Intelligent Hub.

Pour configurer le profil de mise à jour automatique d'applications publiques :

Note Si un profil contient une charge utile de mise à jour d'application publique, il ne peut pas contenir d'autres charges utiles.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Configurez les paramètres de profil appropriés dans l'onglet Général. Ces paramètres déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.

3 Sélectionnez Mise à jour automatique d'applications publiques dans la liste de charges utiles et configurez les paramètres de mise à jour :

- Stratégie de mise à jour automatique des applications publiques : spécifiez à quel moment Google Play autorise la mise à jour automatique. Sélectionnez Autoriser l'utilisateur à configurer, Toujours mettre à jour automatiquement, Mettre à jour sur Wi-Fi uniquement ou Jamais de mise à jour automatique.

  La sélection par défaut est Autoriser l'utilisateur à configurer.

- Heure de début : définissez ce que les applications à l'heure locale au premier plan sont autorisées à mettre à jour automatiquement chaque jour. Sélectionnez une heure comprise entre 0h30 et 23h30.

  Note S'applique uniquement si les options **Procéder à la mise à jour en Wi-Fi uniquement** et **Toujours procéder à la mise à jour automatique** sont sélectionnées.

- Date de fin : définissez ce que les applications à l'heure locale au premier plan sont autorisées à mettre à jour automatiquement chaque jour. Sélectionnez une durée comprise entre 30 minutes et 24 heures.

  Note S'applique uniquement si les options Mettre à jour en Wi-Fi uniquement et Toujours procéder à la mise à jour automatique sont sélectionnées.

4 Sélectionnez Enregistrer et publier pour attribuer le profil aux terminaux associés.

Résultats

En fonction de la durée configurée, les applications ne se mettent à jour automatiquement qu'entre les heures de début et de fin indiquées. Par exemple, vous pouvez configurer des terminaux kiosque pour qu'ils se mettent à jour uniquement en dehors des heures ouvrables pour ne pas interrompre leur utilisation.

Informations d'identification (Android)

Pour une sécurité renforcée, vous pouvez mettre en place des certificats numériques qui protégeront vos actifs professionnels. Pour ce faire, vous devez d'abord définir une autorité de certification, puis configurer une section de configuration Identifiants avec votre section de configuration EAS (Exchange ActiveSync), Wi-Fi ou VPN.

Chacune section de configuration dispose de paramètres pour l'association d'une autorité de certification définie dans la section de configuration Identifiants. Les profils des identifiants déploient des certificats d'entreprise pour que les utilisateurs s'authentifient aux terminaux gérés. Les paramètres de ce profil varient en fonction du type de propriété du terminal. Le profil **Identifiants** s'applique aux types de mode Profil professionnel et Terminaux gérés pour le travail.

Les terminaux doivent disposer d'un code PIN de terminal configuré avant que Workspace ONE UEM puisse installer des certificats d'identité avec une clé privée.

Identifiants de déploiement (Android)

Les profils des identifiants déploient des certificats d'entreprise pour que les utilisateurs s'authentifient aux terminaux gérés. Les paramètres de ce profil varient en fonction du type de propriété du terminal. Le profil **Identifiants** s'appliquera aux types de mode Profil professionnel et Terminaux gérés pour le travail.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Sélectionnez le profil **Identifiants** et sélectionnez **Configurer**.

4 Dans le menu déroulant, sélectionnez **Importer** ou **Autorité de certification définie** pour la **Source du certificat**. Les options de profil restantes dépendent de la source. Si vous choisissez **Importer**, vous devez saisir un **nom d'identifiant** et importer un nouveau certificat. Si vous sélectionnez **Autorité de certification définie**, vous devez choisir une **autorité de certification** prédéfinie, ainsi qu'un **modèle** de certificat.

5 Cliquez sur **Enregistrer et publier**.

Création de messages personnalisés

Le profil de messages personnalisés vous permet de configurer des messages qui s'affichent sur l'écran d'accueil du terminal lorsque des informations importantes doivent être relayées à l'utilisateur.

Le profil de messages personnalisés vous permet de définir un message de verrouillage de l'écran, un message pour les paramètres bloqués ou un message que les utilisateurs peuvent afficher dans les paramètres de leur terminal.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Sélectionnez Android.

3 Configurez les paramètres de profil appropriés dans l'onglet Général.

4 Sélectionnez le profil de messages personnalisés et configurez les paramètres des messages :

Option	Description
Définir un message pour l'écran de verrouillage	Entrez un message à afficher sur l'écran d'accueil du terminal lorsque le terminal est verrouillé. Cette opération est utile pour qu'un terminal perdu ou volé affiche les informations de contact de l'utilisateur.
Définir un message pour les paramètres bloqués	Entrez le message à afficher lorsqu'un utilisateur tente d'effectuer des actions sur un terminal bloqué. Utilisez le message personnalisé pour expliquer pourquoi la fonctionnalité est bloquée.
Définir un message pour les utilisateurs à afficher dans les paramètres	Les utilisateurs peuvent vérifier ce paramètre dans Paramètres>Sécurité>Terminal.

5 Cliquez sur Enregistrer et publier pour attribuer le profil aux terminaux associés

Contrôle des applications (Android)

Le profil de contrôle des applications vous permet de mettre les applications sur liste noire et d'éviter de désinstaller des applications importantes. Alors que le moteur de conformité peut envoyer des alertes et effectue des actions administratives lorsqu'un utilisateur installe ou désinstalle certaines applications, le contrôle des applications empêche les utilisateurs de procéder à ces changements.

Il n'y a aucune option de mise sur liste blanche dans le profil de contrôle des applications Android, car par défaut, seules les applications approuvées par l'administrateur s'affichent dans le Play Store. Par exemple, vous pouvez envoyer automatiquement le navigateur de votre choix au terminal en tant qu'application gérée et l'ajouter aux applications requises du groupe d'applications. Cette configuration combinée avec l'activation de l'option Empêcher la désinstallation des applications requises dans le profil de contrôle des applications empêche la désinstallation du navigateur et d'autres applications requises configurées dans le groupe d'applications.

Pour plus d'informations sur les Groupes d'applications, consultez la documentation relative à la gestion des applications mobiles.

Configurer le contrôle des applications (Android)

Pour contrôler l'accès à l'application sur vos terminaux Android, créez un profil afin de placer sur liste noire, d'interdire, de désinstaller ou d'activer les applications système avec le profil Contrôle des applications.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil appropriés dans l'onglet **Général**.
3. Sélectionnez la section de configuration **Contrôle d'applications**.
4. Pour définir le niveau de contrôle de vos déploiements d'applications, configurez les paramètres suivants :

Paramètre	Description
Désactiver l'accès aux applications sur liste noire	Activez cette option pour désactiver l'accès aux applications qui sont sur liste noire, telle que définie dans les Groupes d'applications. Si cette option est activée, l'application n'est pas désinstallée du terminal.
Empêcher la désinstallation des applications requises	Activez cette option pour empêcher la désinstallation des applications requises définies dans les Groupes d'applications.
Activer les applications système	Activez cette option pour afficher les applications pré-installées telles qu'elles sont définies dans les applications placées sur liste blanche dans les Groupes d'applications. Pour les terminaux à accès privé d'entreprise, la case à cocher « Terminaux gérés pour le travail » s'applique au côté personnel et « Profil professionnel » s'applique au côté entreprise.

5. Cliquez sur **Enregistrer et publier**.

Configurer les paramètres proxy (Android)

Les paramètres de proxy sont configurés de sorte que tout le trafic réseau HTTP et HTTPS passe uniquement par ce proxy. Toutes les données personnelles et professionnelles sont alors filtrées via le profil de paramètres de proxy, ce qui renforce la sécurité des données.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil de l'onglet **Général**.
3. Sélectionnez le profil **Paramètres du proxy**.
4. Configurez les paramètres du proxy de la manière suivante :

Paramètre	Description
Mode proxy	Sélectionnez le type de proxy de votre choix.
URL de proxy PAC	Indiquez une URL pointant vers un fichier .pac du proxy.
Serveur proxy	Saisissez le nom d'hôte de l'adresse IP du serveur proxy.
Liste d'exclusions	Ajoutez des noms d'hôte pour les empêcher de passer par le proxy.

5. Cliquez sur **Enregistrer et publier**.

Gérer les mises à jour système pour les terminaux Android

Utilisez ce profil pour gérer la manière dont les mises à jour de terminaux Android sont gérées lorsque le terminal est inscrit dans Workspace ONE UEM.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil souhaités dans l'onglet **Général**.
3. Sélectionnez le profil **Mises à jour système**.

4 Utilisez le menu déroulant du champ **Mises à jour automatiques** pour sélectionner la politique de mise à jour.

Paramètre	Description
Mises à jour automatiques (Terminaux gérés pour le travail Android 6.0 et versions ultérieures)	■ **Installer automatiquement les mises à jour** : installez automatiquement les mises à jour lorsqu'elles sont disponibles. ■ **Différer les notifications de mise à jour** : différez toutes les mises à jour. Vous pouvez envoyer une politique qui bloque les mises à jour de l'OS pour une période maximale de 30 jours. ■ **Définir la fenêtre de mise à jour** : définissez une fenêtre d'heure quotidienne durant laquelle mettre à jour le terminal.
Périodes de blocage des mises à jour système annuelles (Terminaux gérés pour le travail Android 9.0 et versions ultérieures)	Les propriétaires de terminaux peuvent reporter les mises à jour système à distance (OTA) sur des terminaux pendant 90 jours maximum pour figer la version du système d'exploitation exécutée sur ces terminaux sur des périodes critiques (telles que les vacances). Le système applique une mémoire tampon de 60 jours après une période de blocage définie afin d'éviter de figer le terminal indéfiniment. Pendant une période de blocage : ■ Les terminaux ne reçoivent aucune notification sur les mises à jour à distance en attente. ■ Les terminaux n'installent pas de mises à jour à distance sur le système d'exploitation. ■ Les utilisateurs de terminaux ne peuvent pas vérifier manuellement les mises à jour à distance.
Période de gel	Utilisez ce champ pour définir des périodes de gel, en mois et en jours, lorsque les mises à jour ne peuvent pas être installées. Lorsque l'heure du terminal atteint l'une des périodes de gel, toutes les mises à jour système entrantes, y compris les correctifs de sécurité, sont bloquées et ne peuvent pas être installées. Chaque période de gel individuelle est autorisée à être d'au moins 90 jours et les périodes de gel adjacentes doivent être espacées d'au moins 60 jours.

5 Cliquez sur **Enregistrer et publier**.

Profil Wi-Fi (Android)

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.

Ce profil Wi-Fi peut s'avérer utile pour les utilisateurs finaux en déplacement dans des bureaux disposant de leur propre réseau sans fil ou pour configurer les terminaux automatiquement de sorte qu'ils se connectent au réseau sans fil approprié d'un site.

Lors du déploiement d'un profil Wi-Fi sur des terminaux sous Android 6.0 ou version ultérieure, si un utilisateur a déjà connecté son terminal à un réseau Wi-Fi manuellement, Workspace ONE UEM ne peut modifier la configuration Wi-Fi. Par exemple, si vous déployez le profil mis à jour sur les terminaux inscrits alors que le mot de passe Wi-Fi a été modifié, certains utilisateurs devront saisir le nouveau mot de passe manuellement sur leur terminal.

Configurer un accès Wi-Fi (Android)

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.

Procédure

1. Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.
2. Configurez les paramètres de profil de l'onglet **Général**.
3. Sélectionnez la section de configuration **Wi-Fi**.
4. Configurez les paramètres du **Wi-Fi** :

Paramètre>	Description
Identifiant SSID	Indiquez le nom du réseau auquel le terminal se connecte.
Réseau masqué	Indiquez si le réseau Wi-Fi est masqué.
Définir comme réseau actif	Indiquez si le terminal se connecte au réseau sans intervention de l'utilisateur final.
Type de sécurité	Indiquez le protocole d'accès utilisé et si des certificats sont requis. Selon le type de sécurité sélectionné, les champs requis ne seront pas les mêmes. Si l'option **Aucun, WEP, WPA/WPA 2 ou Tous (personnels)** est sélectionnée, le champ **Mot de passe** s'affiche. Si l'option **WPA/WPA 2 Enterprise** est sélectionnée, les champs Protocoles et Authentification s'affichent. ■ **Protocoles** ■■ Utiliser l'authentification à deux facteurs ■■ Type SFA ■ **Authentification** ■■ Identité ■■ Identité anonyme ■■ Nom d'utilisateur ■■ Mot de passe ■■ Certificat d'identité ■■ Certificat racine
Mot de passe	Saisissez les identifiants requis pour que le terminal puisse se connecter au réseau. Le champ de mot de passe s'affiche lorsque l'option **WEP, WPA/ WPA2, Tous (personnels) ou WPA/WPA2 Enterprise** est sélectionnée dans le champ **Type de sécurité**.
Inclure les paramètres de Fusion	Activez ce paramètre pour étendre les options Fusion aux adaptateurs Fusion pour terminaux Motorola. Les paramètres Fusion s'appliquent uniquement aux terminaux Motorola durcis. Pour plus d'informations sur le support VMware pour les terminaux Android durcis, consultez le **Guide des terminaux durcis Android**.
Configurer Fusion 802.11d	Définissez les paramètres Fusion 802.11d pour utiliser ce réseau.
Activer 802.11d	Activez ce paramètre pour utiliser la norme de réseau sans fil 802.11d dans des domaines réglementaires supplémentaires.

Paramètre>	Description
Configurer le code du pays	Définissez le **code du pays** à utiliser dans les spécifications 802.11d.
Configurer la bande RF	Choisissez la bande **2.4 GHz**, **5 GHz** ou les deux, avec les filtres de fréquence applicables.
Type de proxy	Configurez les paramètres du proxy Wi-Fi. **Note** Le VPN par application ne prend pas en charge la configuration automatique du proxy Wi-Fi.
Serveur proxy	Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
Port du serveur proxy	Indiquez le port du serveur proxy.
Liste d'exclusions	Saisissez les noms d'hôte à exclure du proxy. Les noms d'hôte indiqués ici ne seront pas routés via le proxy. Utilisez le caractère générique * pour le domaine, par exemple : *.air-watch.com ou *air-watch.com.

5 Cliquez sur **Enregistrer et publier**.

Configurer un VPN (Android)

Les réseaux privés virtuels (VPN) fournissent aux terminaux un tunnel sécurisé et chiffré pour accéder aux ressources internes, telles que la messagerie, les fichiers et le contenu professionnels. Les profils VPN permettent à chaque terminal de fonctionner comme s'il était connecté sur le réseau local.

Selon le type de connexion et la méthode d'authentification, utilisez des valeurs de recherche qui permettront de renseigner automatiquement le nom d'utilisateur, afin de rationaliser le processus de connexion.

Note Le profil VPN s'applique aux deux types de mode Profil professionnel et Terminaux gérés pour le travail.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Sélectionnez **VPN** pour modifier le profil.

4 Configurez les paramètres de **VPN**. Le tableau ci-dessous contient tous les paramètres que vous pouvez configurer selon le client VPN.

Paramètre	Description
Type de connexion	Choisissez le protocole utilisé pour faciliter les sessions VPN. Chaque type de connexion nécessite que le client VPN respectif soit installé sur le terminal pour déployer le profil VPN. Ces applications doivent être attribuées à des utilisateurs et publiées en tant qu'applications publiques.
Nom de la connexion	Saisissez le nom de la connexion attribuée créée par le profil.
Serveur	Saisissez le nom ou l'adresse du serveur utilisé pour les connexions VPN.
Compte	Entrez le compte utilisateur pour l'authentification de la connexion.
VPN toujours actif	Activez cette option pour forcer tout le trafic provenant des applications professionnelles à passer par le VPN.
Activer	Permet d'activer le VPN après l'application du profil au terminal.
Règles du VPN par application	Le VPN par application vous permet de configurer des règles de trafic VPN pour certaines applications spécifiques. Cette zone de texte s'affiche uniquement pour les fournisseurs de VPN pris en charge. **Note** Le VPN par application ne prend pas en charge la configuration automatique du proxy Wi-Fi.
Protocole	Sélectionnez le protocole d'authentification à utiliser avec le VPN. Disponible lorsque Cisco AnyConnect est sélectionné dans Type de connexion.
Nom d'utilisateur	Entrez le nom d'utilisateur. Disponible lorsque Cisco AnyConnect est sélectionné dans Type de connexion.
Authentification utilisateur	Choisissez la méthode requise pour authentifier la session VPN.
Mot de passe	Indiquez les identifiants requis pour l'accès de l'utilisateur final au VPN.
Certificat client	Utilisez le menu déroulant pour sélectionner le certificat client. Ceux-ci sont configurés dans les profils Identifiants de déploiement (Android).
Révocation des certificats	Permet d'activer la révocation des certificats.
Profil AnyConnect	Entrez le nom du profil AnyConnect.
Mode FIPS	Permet d'activer le mode FIPS.
Mode restreint	Permet d'activer le mode Strict.
Clés du fournisseur	Permet de 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.
Certificat d'identité	Sélectionnez le certificat d'identité à utiliser pour la connexion VPN. Disponible lorsque Workspace ONE Tunnel est sélectionné dans Type de connexion.

5 Cliquez sur **Enregistrer et publier**.

Configuration d'une règle de VPN par application (Android)

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.

Note Le VPN par application ne prend pas en charge la configuration automatique du proxy Wi-Fi.

Procédure

1. Accédez à**Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android**.
2. Sélectionnez **Android** pour configurer les paramètres.
3. Sélectionnez la section de configuration **VPN** dans la liste.
4. Sélectionnez votre fournisseur VPN dans le champ **Type de connexion**.
5. Configurez votre profil VPN.
6. Sélectionnez **Règles de VPN par application** pour pouvoir associer le profil VPN aux applications souhaitées. Pour les clients Workspace ONE Tunnel, cette option est activée par défaut. Une fois la case cochée, ce profil peut être sélectionné dans la liste déroulante des profils de tunnel par application sur la page d'attribution de l'application.
7. Cliquez sur **Enregistrer et publier**.

   Si les règles de VPN par application sont activées en tant que mise à jour d'un profil VPN existant, les terminaux/applications qui utilisaient auparavant la connexion VPN sont affectés. La connexion VPN qui acheminait précédemment tout le trafic d'applications est déconnectée et le VPN ne s'applique qu'aux applications associées au profil mis à jour.

Étape suivante

Pour configurer des applications publiques afin d'utiliser le profil VPN par application, reportez-vous à la section Ajout d'applications publiques pour Android dans la Gestion des applications pour la publication Android.

Définir des autorisations (Android)

Workspace ONE UEM console permet à l'administrateur d'afficher une liste de toutes les autorisations qu'une application utilise et de définir l'action par défaut au moment de l'exécution de l'application. Le profil Autorisations est disponible sur les terminaux Android 6.0 et versions ultérieures utilisant les modes Terminaux gérés pour le travail et Profil professionnel.

Vous pouvez définir des politiques d'autorisation pour chaque application Android. Les dernières autorisations sont récupérées lors de la configuration de chaque application au niveau individuel.

Note Toutes les autorisations utilisées par une application sont répertoriées lorsque vous sélectionnez l'application dans la liste Exceptions. Toutefois, les stratégies d'autorisation de Workspace ONE UEM ne s'appliquent qu'aux autorisations considérées comme dangereuses par Google. Les autorisations dangereuses concernent les opérations où l'application demande des données qui incluent les informations personnelles de l'utilisateur ou qui pourraient potentiellement affecter les données stockées par l'utilisateur. Pour plus d'informations, veuillez consulter le site Web Android Developer.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Configurez les paramètres Autorisations, notamment :

Paramètres	Description
Politique d'autorisation	Choisissez si vous souhaitez **demander l'autorisation à l'utilisateur**, **accorder toutes les autorisations** ou **refuser toutes les autorisations** pour toutes les applications professionnelles.
Exceptions	Recherchez les applications qui ont déjà été ajoutées dans AirWatch (applications Android approuvées uniquement) et faites une exception à la politique d'autorisation pour l'application.

4 Cliquez sur **Enregistrer et publier** pour attribuer le profil aux terminaux associés.

Configurer le mode Application unique (Android)

Le mode Application unique vous permet d'utiliser les terminaux Android avec une seule finalité telle que le mode kiosque en ajoutant sur la liste blanche les applications internes et publiques prises en charge.

Note pour plus d'informations sur les applications prises en charge, consultez le lien dans le profil de Mode d'application unique dans Workspace ONE UEM Console qui vous renvoie vers le site Google Code pour des spécificités.

Pour une utilisation optimale du mode Application unique et des meilleures pratiques, reportez-vous à la section Meilleures pratiques pour le mode Application unique (Android).

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Configurez les paramètres Mode d'application unique :

Paramètres	Description
Applications sur liste blanche	Sélectionnez l'application de votre choix pour verrouiller le terminal en mode Application unique.

Meilleures pratiques pour le mode Application unique (Android)

Pensez à appliquer ces politiques et restrictions afin d'assurer la meilleure expérience et la meilleure maintenance pour votre application à finalité unique en utilisant les politiques du mode Application unique. Ces recommandations sont utiles si vous déployez un profil du mode Application unique pour les terminaux dans des cas d'utilisation de type kiosque et affichage numérique pour lesquels un utilisateur final n'est pas associé au terminal.

Créez un profil « Restrictions » et configurez les éléments suivants dans le profil :

- Désactivez les options suivantes sous **Fonctionnalités du terminal** :
  - **Barre d'état autorisée** – Permet une expérience immersive lorsque le terminal est verrouillé dans une seule application.
  - **Autoriser Keyguard** – Permet d'empêcher le verrouillage du terminal.
- Activez les options suivantes sous **Fonctionnalités du terminal** :
  - Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur CA.
  - Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur USB.
  - Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur sans fil.

  Ces options permettent de s'assurer que l'écran du terminal est toujours actif.

Déployez le profil Politique de mise à jour système pour vous assurer que le terminal reçoit les dernières corrections avec un minimum d'intervention manuelle.

Définir la date/heure Android

Définissez la date, l'heure et le format d'affichage pour que votre flotte utilise le format régional approprié.

Ce profil est disponible lorsque l'option **Paramètres OEM** est activée et que le champ **Sélectionner OEM** est défini sur **Samsung** dans les paramètres du profil général.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Cliquez sur **Terminal** pour déployer votre profil sur un terminal.

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

Note Le profil **Date/Heure** s'affiche uniquement lorsque le champ **Paramètres OEM** est défini sur **Activé**.

4 Sélectionnez la section de configuration **Date/heure**.

5 Configurez les paramètres de date/heure :

Paramètre	Description
Format de la date	Modifiez l'ordre d'affichage du **Mois**, du **Jour** et de l'**Année**.
Format de l'heure	Choisissez le format **12** ou **24 heures**.
Date/heure	Définissez la source de données que vos terminaux consultent pour les paramètres de date et d'heure : ■ **Automatique** – Définit la date et l'heure à partir des paramètres natifs des terminaux. ■ **Heure du serveur** – Définit l'heure à partir de l'heure du serveur de Workspace ONE UEM Console. ■■ **Définir le fuseau horaire** – Précisez le fuseau horaire. ■ **URL HTTP** – Définit l'heure à partir d'une URL. Vous pouvez utiliser n'importe quelle URL, par exemple www.google.com. ■■ **URL** – Indiquez le site web utilisé pour la date et l'heure, ■■ **Activer la synchronisation périodique** – Permet au terminal de vérifier la date et l'heure à intervalles réguliers (en jours). ■■ **Définir le fuseau horaire** – Précisez le fuseau horaire. ■ **Serveur SNTP** ■■ **URL** – Indiquez le site web utilisé pour la date et l'heure, Vous pouvez entrer time.nist.gov par exemple. ■■ **Activer la synchronisation périodique** – Permet au terminal de vérifier la date et l'heure à intervalles réguliers (en jours).

6 Cliquez sur **Enregistrer et publier**.

Créer un profil Workspace ONE Launcher (Android)

Workspace ONE Launcher est un lanceur d'applications qui vous permet de verrouiller les terminaux Android pour certains cas d'utilisation individuelles et de personnaliser l'apparence et le comportement des terminaux Android gérés. L'application Workspace ONE Launcher remplace l'interface de votre terminal par une interface personnalisée, adaptée aux besoins de votre entreprise.

Vous pouvez configurer les terminaux Android 6.0 Marshmallow (et versions ultérieures) en mode Propriété de l'entreprise, utilisation unique (COSU, Corporate-Owned, Single-Use). Le mode COSU vous permet de configurer des terminaux avec une seule finalité telle que le mode kiosque en ajoutant sur la liste blanche les applications internes et publiques prises en charge. Le mode COSU est pris en charge pour les modes Application unique, Applications multiples et Modèle. Pour plus d'informations sur le déploiement du profil Workspace ONE Launcher en mode COSU, reportez-vous à la publication Workspace ONE Launcher.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

Ces paramètres déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.

3 Sélectionnez le profil **Launcher**.

4 Choisissez un mode d'application :

Paramètre	Description
Application unique	Verrouillez un terminal sur un affichage de kiosque mobile pour limiter l'usage à une application unique.
Applications multiples	Permet de limiter l'accès du terminal à un ensemble d'applications défini.
Modèle	Permet de personnaliser l'écran d'accueil du terminal avec des images, du texte et des applications.

5 Configurez le mode d'application sélectionné.

6 Cliquez sur **Enregistrer** pour ajouter le profil à Workspace ONE UEM Console, ou sur **Enregistrer et publier** pour ajouter le profil et le déployer immédiatement sur les terminaux Android concernés.

Configuration de règles de pare-feu pour les terminaux Android

La section de configuration **Pare-feu** permet aux administrateurs de configurer des règles de pare-feu pour les terminaux Android. Chaque type de règle de pare-feu vous permet d'ajouter plusieurs règles.

Ce profil est disponible lorsque l'option **Paramètres OEM** est activée et que le champ **Sélectionner OEM** est défini sur Samsung dans les paramètres du profil général.

Note La section de configuration de pare-feu s'applique uniquement aux terminaux SAFE 2.0 et versions ultérieures.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

   Le profil **Pare-feu** s'affiche uniquement pour les profils **Android** lorsque le champ **Paramètres OEM** est activé et que Samsung est sélectionné dans le champ **Sélectionnez l'OEM**. Le champ **Paramètres OEM** du profil général s'applique uniquement aux profils Android et non aux configurations Android (héritées).

2 Cliquez sur **Terminal** pour déployer votre profil.

3 Configurez les paramètres du profil dans l'onglet **Général**.

   Les paramètres généraux déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.

4 Sélectionnez le profil **Pare-feu**.

5 Cliquez sur le bouton **Ajouter** sous la règle souhaitée et configurez les paramètres suivants :

Paramètre	Description
Règles d'autorisation	Permettent au terminal d'envoyer et de recevoir des données à partir d'un emplacement réseau spécifique.
Règles de refus	Empêchent le terminal d'envoyer et de recevoir des données à partir d'un emplacement réseau spécifique.
Règles de redirection	Redirigent le trafic provenant d'un emplacement réseau spécifique vers un autre réseau. Si un site Web autorisé redirige vers une autre URL, veuillez ajouter toutes les URL de redirection à la section Règles d'autorisation pour qu'il soit accessible.
Règles d'exception de redirection	Évite la redirection du trafic.

6 Cliquez sur **Enregistrer et publier**.

Configurer le profil APN (Android)

Configurez les paramètres du nom du point d'accès (APN) des terminaux Android pour unifier les paramètres d'opérateur de la flotte de terminaux et corriger les erreurs de configuration.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Cliquez sur **Terminal** pour déployer votre profil sur un terminal.

3 Configurez les paramètres du profil de l'onglet **Général**. Le profil APN s'affiche uniquement lorsque le champ **Paramètres OEM** est défini sur **Activé** et que Samsung est sélectionné dans le champ **Sélectionnez l'OEM**.

   Les paramètres du profil général déterminent la façon dont le profil est déployé et les utilisateurs qui le reçoivent.

4 Sélectionnez la section de configuration **APN**.

5 Configurez les paramètres **APN**, y compris :

Paramètre	Description
Nom d'affichage	Indiquez un nom convivial pour le nom de l'accès.
Nom du point d'accès (APN)	Saisissez l'APN fourni par votre opérateur (par exemple, come.moto.cellular).
Type de point d'accès	Spécifie les types de communication de données qui doivent utiliser cette configuration APN.
Code pays du réseau mobile (MCC)	Saisissez les 3 chiffres de l'indicatif du pays. Cette valeur permet de vérifier si les terminaux itinérants utilisent un opérateur différent de celui indiqué ici. Elle est utilisée conjointement avec un code d'opérateur de réseau (MNC) pour identifier de manière unique un opérateur de réseau mobile (opérateur) via les réseaux mobiles GSM (y compris GSM-R), UMTS et LTE.
Code du réseau mobile (MNC)	Saisissez les 3 chiffres du code d'opérateur de réseau. Cette valeur permet de vérifier si les terminaux itinérants utilisent un opérateur différent de celui indiqué ici. Elle est utilisée conjointement avec un indicatif de pays (MCC) pour identifier de manière unique un opérateur de réseau mobile via les réseaux mobiles GSM (y compris GSM-R), UMTS et LTE.
Serveur MMS (MMSC)	Indiquez l'adresse du serveur.
Numéro du serveur MMS proxy	Saisissez le numéro du port MMS.
Port du serveur proxy MMS	Indiquez le port cible du serveur proxy.
Serveur	Saisissez le nom ou l'adresse utilisé(e) pour la connexion.
Serveur proxy	Saisissez les détails du serveur proxy.
Port du serveur proxy	Indiquez le port du serveur proxy pour tout le trafic.
Nom d'utilisateur du point d'accès	Indiquez le nom d'utilisateur utilisé pour la connexion au point d'accès.
Mot de passe du point d'accès APN	Indiquez le mot de passe utilisé pour l'authentification du point d'accès.
Type d'authentification	Sélectionnez le protocole d'authentification.
Définir comme nom de point d'accès préféré	Activez cette option pour vous assurer que les terminaux des utilisateurs finaux présentent tous les mêmes paramètres APN et empêcher que des modifications ne soient effectuées depuis les terminaux ou par l'opérateur.

6 Cliquez sur **Enregistrer et publier**.

Protection d'entreprise contre la réinitialisation d'usine (Android)

La protection contre la réinitialisation d'usine (FRP, Factory Reset Protection) est une méthode de sécurité Android qui empêche l'utilisation d'un terminal après une réinitialisation aux paramètres d'usine non autorisée.

Lorsque ce paramètre est activé, le terminal protégé ne peut pas être utilisé après une réinitialisation d'usine jusqu'à ce que vous vous connectiez à l'aide du même compte Google précédemment configuré.

Si un utilisateur a activé FRP, lorsque le terminal est rendu à l'organisation (par exemple, lorsque l'utilisateur quitte la société), il se peut que vous ne puissiez pas configurer à nouveau le terminal en raison de cette fonctionnalité.

Le profil de protection contre la réinitialisation d'usine utilise un ID utilisateur Google qui vous permet de remplacer le compte Google après une réinitialisation d'usine pour attribuer le terminal à un autre utilisateur. Pour obtenir l'ID utilisateur Google, rendez-vous sur People:get.

Générer un ID d'utilisateur Google pour le profil de protection contre la réinitialisation d'usine pour les terminaux Android

Cet ID d'utilisateur Google vous permet de réinitialiser le terminal sans le compte Google d'origine. Obtenez votre ID d'utilisateur Google à l'aide de l'API People:get pour configurer le profil.

FRP peut également être supprimé lors de l'exécution d'une réinitialisation complète du terminal à partir des commandes de gestion du terminal. Pour plus d'informations sur la gestion des terminaux, consultez la section Commandes de gestion des terminaux (Android).

Procédure

1 Accédez à People:get.

2 Dans la fenêtre **Essayer cette API**, configurez les paramètres suivants.

Paramètre	Description
resourceName	Entrez **people/me**.
personFields	Entrez **metadata,emailAddresses**
requestMask.includefield	Laissez ce champ vide.
Identifiants	Activez les champs **Google OAuth 2.0** et **Clé API**.

3 Sélectionnez **Exécuter**.

4 Connectez-vous à votre compte Google, si vous y êtes invité. Il s'agit du compte utilisé pour déverrouiller des terminaux lorsque FRP est activé.

5 Sélectionnez **Autoriser** pour accorder des autorisations.

6 Recherchez le nombre à 21 chiffres dans l'onglet **application/json** dans le champ **id**.

7 Revenez dans Workspace ONE UEM console et configurez le profil de protection contre la réinitialisation d'usine d'entreprise.

Étape suivante

Entrez l'ID d'utilisateur Google dans le profil de protection contre la réinitialisation d'usine d'entreprise. Voir Configurez le profil de protection contre la réinitialisation d'usine d'entreprise pour Android.

Configurez le profil de protection contre la réinitialisation d'usine d'entreprise pour Android

Le profil Protection de la réinitialisation aux paramètres d'usine vous permet de créer les ID d'utilisateur Google devant configurer le terminal ou effectuer la réinitialisation.

FRP peut également être supprimé lors de l'exécution d'une réinitialisation complète du terminal à partir des commandes de gestion du terminal. Pour plus d'informations sur la gestion des terminaux, consultez la section Commandes de gestion des terminaux (Android).

Avant de commencer, obtenez votre ID utilisateur Google sur le site Web People:get. Voir Générer un ID d'utilisateur Google pour le profil de protection contre la réinitialisation d'usine pour les terminaux Android.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

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

3 Sélectionnez la section de configuration **Protection de la réinitialisation aux paramètres d'usine**.

4 Pour définir le niveau de contrôle de vos déploiements d'applications, configurez les paramètres suivants :

Paramètre	Description
ID d'utilisateur Google	Entrez l'ID d'utilisateur Google obtenu à partir de l'API People:get de Google.

5 Cliquez sur **Enregistrer et publier**.

Configurer le profil Zebra MX (Android)

Le profil Zebra MX vous permet de profiter des fonctionnalités supplémentaires offertes par l'application de service Zebra MX sur les terminaux Android. L'application de service Zebra MX peut être envoyée à partir de Google Play et distribuée depuis My Workspace ONE en tant qu'application interne dans la Workspace ONE UEM console avec ce profil.

Procédure

1 Accédez à **Ressources > Profils et lignes de base > Profils > Ajouter > Ajouter un profil > Android**.

2 Configurez les paramètres de profil appropriés dans l'onglet **Général**. Activez le champ **Paramètres OEM** et sélectionnez Zebra dans le champ **Sélectionnez l'OEM** pour activer le profil de service Zebra MX.

3 Configurez les paramètres de profil Zebra MX :

Paramètre	Description
Inclure les paramètres de Fusion	Activez ce paramètre pour étendre les options Fusion aux adaptateurs Fusion pour terminaux Motorola.
Configurer Fusion 802.11d	Définissez les paramètres Fusion 802.11d pour utiliser ce réseau.
Activer 802.11d	Activez ce paramètre pour utiliser la norme de réseau sans fil 802.11d dans des domaines réglementaires supplémentaires.
Configurer le code du pays	Activez cette option pour définir le code du pays à utiliser dans les spécifications 802.11d.
Configurer la bande RF	Choisissez la bande 2.4 GHz, 5 GHz ou les deux, avec les filtres de fréquence applicables.
Autoriser le mode avion	Activez cette option pour autoriser l'accès à l'écran des paramètres du mode Avion.
Autoriser les positions fictives	Activez ou désactivez les positions fictives (dans Paramètres > Options du développeur).
Autoriser les données en arrière-plan	Activez ou désactivez les données en arrière-plan.
Conserver le Wi-Fi activé en mode veille	**Toujours activé** – Le Wi-Fi reste activé lorsque le terminal passe en mode veille. **Uniquement en cas de connexion** – Le Wi-Fi reste activé lorsque le terminal passe en mode veille à la condition que ce dernier soit en cours de charge. **Jamais activé** – Le Wi-Fi est désactivé lorsque le terminal passe en mode veille.
Utilisation des données en itinérance	Activez cette option pour autoriser une connexion données en itinérance.
Forcer l'activation du Wi-Fi	Activez cette option pour forcer l'activation du Wi-Fi de sorte que l'utilisateur ne puisse pas le désactiver.
Autoriser Bluetooth	Activez cette option pour autoriser l'utilisation du Bluetooth.
Autoriser le presse-papiers	Activez cette option pour autoriser le copier/coller.
Autoriser une notification de surveillance du réseau	Activez cette option pour autoriser la notification Avertissement du module de surveillance du réseau, qui s'affiche normalement après l'installation des certificats.

Paramètre	Description
Activer les paramètres Date/Heure	Activez cette option pour définir les paramètres Date/heure : ■ **Format de la date** : définissez l'ordre d'affichage du mois, du jour et de l'année. ■ **Format de l'heure** : choisissez un format 12 ou 24 heures. ■ **Date/heure** : définissez la source de données que vos terminaux consulteront pour les paramètres de date et d'heure : ■ **Automatique** – Définit la date et l'heure à partir des paramètres natifs des terminaux. ■ **Heure du serveur** – Définit l'heure à partir de l'heure du serveur de Workspace ONE UEM Console. ■ **Définir le fuseau horaire** – Précisez le fuseau horaire. ■ **URL HTTP** : Workspace ONE UEM Intelligent Hub atteint l'URL et récupère l'horodatage à partir de l'en-tête HTTP. Il applique ensuite celui-ci au terminal. Il ne gère pas les sites de redirection ■ **URL** – Indiquez le site web utilisé pour la date et l'heure, ■ Doit inclure « http:// ». Exemple : http://www.google.com ■ HTTPS non pris en charge ■ **Activer la synchronisation périodique** – Permet au terminal de vérifier la date et l'heure à intervalles réguliers (en jours). ■ **Définir le fuseau horaire** – Précisez le fuseau horaire. ■ **Serveur SNTP** : les paramètres NTP sont appliqués directement au terminal. ■ **URL** : saisissez l'adresse Web du serveur NTP/SNTP. par exemple time.nist.gov. ■ **Activer la synchronisation périodique** – Permet au terminal de vérifier la date et l'heure à intervalles réguliers (en jours).

Paramètre	Description
Activer les paramètres du son	Activez les paramètres du son pour configurer les paramètres audio sur le terminal. ■ **Musique, vidéos, jeux et autres médias** : positionnez le curseur selon le volume sonore que vous souhaitez définir sur le terminal. ■ **Sonneries et notifications** : positionnez le curseur selon le volume sonore que vous souhaitez définir sur le terminal. ■ **Appels vocaux** : positionnez le curseur selon le volume sonore que vous souhaitez définir sur le terminal. ■ **Activer les notifications par défaut** : permet d'activer le son des notifications par défaut sur le terminal. ■ **Activer la tonalité des touches sur le pavé de numérotation** : permet d'activer le son des touches sur le pavé de numérotation. ■ **Activer les tonalités des touches** : permet de faire retentir les touches sur le terminal. ■ **Activer les sons de l'écran de verrouillage** : permet d'activer le son de verrouillage du terminal. ■ **Activer la fonction Vibrer au toucher** : permet d'activer les paramètres de vibration. ■
Activer les paramètres d'affichage	Activez cette option pour définir les paramètres d'affichage : ■ **Luminosité de l'écran** : positionnez le curseur selon le niveau de luminosité que vous souhaitez définir sur le terminal. ■ **Activer la rotation automatique de l'écran** : positionnez le curseur selon le niveau de luminosité que vous souhaitez définir sur le terminal. ■ **Configurer le mode veille** : indiquez le délai avant que l'écran ne passe en mode veille.

4 Cliquez sur **Enregistrer et publier**.

Utilisation des paramètres personnalisés (Android)

La section de configuration **Paramètres personnalisés** peut être utilisée en cas de mise à disposition d'une nouvelle version d'Android ou de nouvelles fonctions non prises en charge par les sections de configuration natives de Workspace ONE UEM Console. Utilisez la section de configuration **Paramètres personnalisés** et le code XML pour activer ou désactiver manuellement certains paramètres.

Assurez-vous d'utiliser le type de caractéristique approprié pour votre type de profil :

- Pour les profils Android, utilisez le type de caractéristique = « com.airwatch.android.androidwork.launcher ».
- Pour les profils Android (hérités), utilisez le type de caractéristique = « com.airwatch.android.kiosk.settings ».

Procédure

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

   Afin d'éviter tout impact sur les autres utilisateurs avant l'enregistrement et la publication de la configuration, vous pouvez travailler sur une copie de votre profil, enregistrée dans un groupe organisationnel « test ».
4. **Enregistrez** votre profil, mais ne le publiez pas.
5. Cliquez sur le bouton radio dans l'**affichage en liste des profils** pour la ligne du profil que vous souhaitez personnaliser.
6. Cliquez sur le bouton **XML** en haut pour afficher le profil XML.
7. Accédez à la section délimitée par <characteristic> ... <characteristic> que vous avez préalablement configurée (Restrictions ou Code d'accès, par exemple). Cette section contient un type de configuration identifiant l'objectif, par exemple les restrictions.
8. Copiez cette portion de texte et fermez la vue XML. Ouvrez votre profil.
9. Sélectionnez la section de configuration **Paramètres personnalisés** puis cliquez sur **Configurer**. Collez le code XML que vous venez de copier dans la zone de texte. Le code XML doit contenir un bloc de code complet, délimité par deux balises <characteristic>.
   - Ce fichier XML doit contenir le bloc complet de code tel qu'il est répertorié pour chaque XML personnalisé.
   - Les administrateurs doivent configurer chaque paramètre de <true /> à <false /> selon les besoins.
   - Si des certificats sont requis, configurez une charge utile de certificat dans le profil et référencez le PayloadUUID dans la charge utile des paramètres personnalisés.
10. Supprimez la section de configuration que vous aviez configurée à l'origine en sélectionnant la section de configuration de base et en cliquant sur le bouton moins (-). Vous pouvez maintenant améliorer le profil en ajoutant du code XML personnalisé pour les nouvelles fonctionnalités.

    les améliorations apportées ne s'appliquent pas aux terminaux qui n'ont pas été mis à niveau vers la dernière version. Une fois le code personnalisé, il est recommandé de tester les terminaux du profil avec des versions précédentes afin de vérifier leur comportement.
11. Cliquez sur **Enregistrer et publier**.

Terminaux partagés

5

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 :

Configurer Android pour une utilisation de terminaux partagée

Pour utiliser la fonction Terminaux partagés sur les périphériques Android, enrôlez ce dernier à l'aide de Workspace ONE Intelligent Hub, définissez l'application Workspace ONE Launcher comme écran d'accueil par défaut et créez, puis attribuez le profil Launcher. Workspace ONE Launcher est automatiquement téléchargé au cours de l'inscription, mais vous devrez déterminer la version du Launcher qui sera envoyée sur les terminaux.

Procédure

1 Naviguez vers **Terminaux > Paramètres des terminaux > Android > Applications de service**.

2 Configurez les paramètres appropriés :

Paramètre	Description
Toujours utiliser la dernière version de Launcher	Si ce paramètre est activé, la dernière version de l'application est automatiquement déployée sur les terminaux dès qu'elle est disponible.
Version de Launcher	Depuis le menu déroulant, choisissez manuellement la version de Launcher à déployer.

3 Cliquez sur **Enregistrer**.

4 Accédez à **Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android > Launcher** et configurez le profil Launcher pour chaque sous-groupe organisationnel. Ce profil devrait contenir tous les paramètres communs nécessaires à ce groupe organisationnel.

Important veillez à activer le paramètre **Conserver le code d'accès de l'administrateur si le profil Launcher est supprimé du terminal**. Ainsi, l'utilisateur du préenrôlement et les utilisateurs de terminaux partagés ne seront autorisés à quitter le module de lancement qu'après avoir saisi le code d'accès administrateur.

N'attribuez pas le profil Launcher à un utilisateur intermédiaire.

5 Enrôlez le terminal dans le groupe organisationnel d'enrôlement à l'aide de l'utilisateur du préenrôlement. Le fichier .apk du Launcher s'installe et l'écran de connexion s'affiche, par défaut.

Note Le fichier .apk du Launcher doit être installé avant que le profil Launcher ne soit envoyé dans le cadre des paramètres du terminal partagé.

6 Saisissez l'ID de groupe, le nom et le mot de passe de l'utilisateur du terminal partagé pour se connecter, en veillant à attribuer le terminal à l'Utilisateur du terminal partagé et au sous-groupe organisationnel approprié. Le profil Launcher sera appliqué au terminal et la console indiquera quel utilisateur est connecté au terminal.

Important saisissez uniquement l'ID de groupe si vous avez sélectionné **Demander à l'utilisateur de saisir le groupe organisationnel** dans le mode d'attribution de groupe dans les paramètres du terminal partagé.

7 Déconnectez-vous du profil Launcher sur le terminal. Cela permet de réattribuer le terminal à l'utilisateur du préenrôlement, de replacer le terminal dans son groupe organisationnel d'enrôlement d'origine et de supprimer le profil Launcher.

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	**(Pour terminaux iOS uniquement)**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.
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.
Autoriser le code PIN au démarrage	Activez ou désactivez le démarrage sécurisé Android, qui nécessite, la première fois, d'entrer un code PIN pour démarrer le terminal. S'il est désactivé, les utilisateurs ne peuvent pas activer le démarrage sécurisé lors de la configuration du code secret. Si le démarrage sécurisé est déjà désactivé sur le terminal, ce dernier doit être réinitialisé sur les paramètres d'usine pour l'activer. Cette fonctionnalité s'applique uniquement aux terminaux Android qui ne disposent pas d'un chiffrement basé sur des fichiers.
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.

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**.

Se connecter et se déconnecter des terminaux Android partagés

Pour utiliser la fonction Terminaux partagés sur un périphérique Android, enrôlez ce dernier à l'aide de Workspace ONE Intelligent Hub et définissez l'application VMware Workspace ONE Launcher comme écran d'accueil par défaut. Workspace ONE Launcher est automatiquement téléchargé lors de l'inscription.

Une fois l'application installée et définie comme écran d'accueil par défaut, le terminal est en état de check-in. Lorsqu'il est dans cet état, l'utilisateur ne peut pas quitter cette page et le terminal demande à l'utilisateur de procéder à la fermeture de session (check-out). Pour supprimer le profil et permettre à l'utilisateur d'accéder à nouveau à la totalité du terminal, effectuez une suppression des données d'entreprise sur le terminal préenrôlé depuis Workspace ONE UEM Console.

Procédure

1. Sur la page de connexion de Workspace ONE Launcher, l'utilisateur doit entrer son ID de groupe, son nom d'utilisateur et son mot de passe. Si l'option **Demander à l'utilisateur de saisir le groupe organisationnel** est activée dans la console, l'utilisateur doit saisir un **ID de groupe** pour ouvrir une session.
2. Appuyez sur **Connexion** et acceptez les Conditions d'utilisation, le cas échéant.

   Le terminal est alors configuré. Une fois l'utilisateur connecté, les profils utilisateur sont déployés en fonction du Smart Group et des associations de groupes d'utilisateurs.

Étape suivante

Pour vous déconnecter d'un terminal Android, sélectionnez **Paramètres de Launcher** et sélectionnez **Déconnexion** (icône de la porte).

Gestion des terminaux Android avec Workspace ONE UEM

6

Une fois vos terminaux enrôlés et configurés, gérez-les à l'aide de 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. La **Vue de la liste des terminaux** répertorie tous les terminaux actuellement inscrits dans votre environnement Workspace ONE UEM, ainsi que leur état. Vous pouvez filtrer l'affichage en liste spécifique d'Android et voir comment les terminaux sont gérés en un coup d'œil.

Pour plus d'informations sur le filtrage de l'affichage en liste reportez-vous à la section Filtrage des terminaux dans l'affichage en liste dans la publication Gestion des terminaux.

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 :

Commandes de gestion des terminaux (Android)

Vous pouvez exécuter des commandes ponctuelles, notamment le verrouillage et l'effacement du terminal, et modifier le code secret depuis Workspace ONE UEM console. Ces commandes s'appliquent en fonction du type d'inscription du terminal.

Les commandes suivantes sont disponibles à partir de cette vue :

- **Verrouiller le terminal** – Verrouillez tous les terminaux sélectionnés et forcez les utilisateurs à ressaisir le code PIN de sécurité de leurs terminaux. Cette option s'applique aux types Profil professionnel et Terminaux gérés pour le travail.
- **Réinitialisation du terminal** – Efface toutes les données du terminal sélectionné, notamment l'ensemble des données, e-mails, profils et capacités MDM et réinitialise le terminal. Ce paramètre s'applique uniquement au Terminaux gérés pour le travail. Si la protection de la réinitialisation aux paramètres d'usine est activée, vous verrez une invite qui vous permet de désactiver cette protection avant l'effacement.
- **Supprimer le code secret** :
  - Sélectionnez **Terminal** pour supprimer le code secret du terminal. Cette commande n'est pas disponible pour le profil professionnel.
  - Sélectionnez **Effacer le code secret professionnel** pour supprimer le niveau de sécurité professionnelle sur le terminal. Pour Android 8.0 ou versions ultérieures.
  - L'utilisateur reçoit un message d'alerte à plusieurs reprises, l'invitant à saisir un code secret. Il peut toutefois effectuer d'autres tâches sur son terminal. Vous pouvez configurer une stratégie de conformité ou utiliser les paramètres du Workspace ONE Intelligent Hub pour Android afin de créer et d'appliquer un code secret qui est à nouveau ajouté au terminal.
- **Gestion**
  - Sélectionnez **Modifier le code secret du terminal** pour modifier le code secret du terminal. Cette commande n'est pas disponible pour le profil professionnel.
  - Sélectionnez **Redémarrer le terminal** pour redémarrer le terminal à distance. Cette commande n'est pas prise en charge pour le mode profil professionnel.
  - Sélectionnez **Réinitialiser le code secret professionnel** pour modifier le code secret du profil professionnel.

Onglet des applications Détails des terminaux

L'onglet des applications **Détails des terminaux** dans Workspace ONE UEM console contient des options pour contrôler les applications publiques par terminal. Vous pouvez afficher les applications qui ont été attribuées dans UEM console et les applications personnelles en fonction du type d'enrôlement et des configurations de confidentialité.

Les administrateurs peuvent afficher des informations sur l'application, notamment le statut de l'installation, le type d'application, la version de l'application et l'identifiant de l'application.

L'option **Installer** du menu d'actions vous permet de sélectionner les applications attribuées dans l'affichage en liste et de les transférer directement vers le terminal. L'option **Supprimer** dans le menu d'actions permet de désinstaller l'application du terminal en mode silencieux.

Les enrôlements de profils professionnels affichent uniquement les applications attribuées par l'administrateur et n'affichent pas les applications personnelles installées par l'utilisateur. Les enrôlements gérés pour le travail affichent toutes les applications, car Workspace ONE UEM dispose d'un contrôle total sur le terminal et il n'y a aucun concept d'applications personnelles. Pour un enrôlement COPE, l'onglet applications des détails de terminal affiche les applications gérées, qui incluent des applications internes installées par défaut dans la partie personnelle.

Workspace ONE UEM console n'affiche pas les applications qui ne peuvent pas être lancées par les utilisateurs. La console UEM signale l'état des applications qui disposent d'une icône Launcher que l'utilisateur peut utiliser et ouvrir. Par conséquent, les applications en arrière-plan ou les applications de service ne sont pas affichées dans les détails du terminal.

Demander la journalisation du terminal

La commande Demander la journalisation du terminal vous permet de récupérer des journaux Workspace ONE Intelligent Hub ou des journaux système détaillés à partir de terminaux professionnels et de les afficher dans la console afin de résoudre rapidement les problèmes sur le terminal. La boîte de dialogue Demander la journalisation du terminal vous permet de personnaliser votre demande de journalisation pour les terminaux Android.

Procédure

1 Accédez à **Groupes et paramètres > Tous les paramètres > Terminaux et utilisateurs > Général > Confidentialité** et activez Demander la journalisation du terminal dans les paramètres de confidentialité.

   Les terminaux personnels ne peuvent pas être sélectionnés pour des raisons de confidentialité.

2 Accédez à **Terminaux > Affichage en liste > Sélectionner un terminal dans la liste > Plus d'actions > Demander la journalisation du terminal**.

3 Personnalisation des paramètres de journal :

Paramètre	Description
Source	Sélectionnez **Hub** pour collecter les journaux générés par Workspace ONE Intelligent Hub. Sélectionnez **Système** pour inclure toutes les applications et tous les événements sur le terminal. L'option Système est disponible en fonction de vos paramètres de confidentialité et est limitée aux fabricants de terminaux avec des applications de service de plateforme spécifiques. **Note** Disponible sur les terminaux exécutant Platform OEM Service version 3.3+, MSI Service version 1.3+ et Honeywell Service version 3.0+. Sélectionnez **Réseau** pour enregistrer les demandes DNS et les connexions réseau des applications dans un fichier journal pour la durée spécifiée. **Note** Disponible sur les terminaux gérés par Work exécutant Android 8 ou versions ultérieures. **Note** L'option Collecte de l'adresse IP publique doit être activée dans les paramètres de confidentialité.
Type	Sélectionnez **Snapshot** pour récupérer les derniers enregistrements de journaux disponibles sur les terminaux. Sélectionnez **Délai dépassé** pour collecter un journal glissant sur une période spécifiée. Plusieurs fichiers journaux peuvent être envoyés à UEM console. L'option Niveau n'est pas disponible lorsque Réseau est sélectionné.
Durée	Spécifiez la durée pendant laquelle le terminal collecte et signale les journaux à la console.
Niveau	Déterminez le niveau de détail inclus dans le journal (erreur, avertissement, informations, débogage, commentaires).

4 Cliquez sur **Enregistrer**.

5 Pour consulter les fichiers journaux, accédez à **Détails du terminal > Plus > Pièces jointes > Documents**.

6 Vous pouvez annuler la demande de journalisation du terminal une fois que les journaux ont été reçus et qu'il n'est plus nécessaire de collecter les journaux. Accédez à **Terminaux > Affichage en liste > Sélectionner un terminal dans la liste > Plus d'actions > Annuler la demande de journalisation du terminal** pour a annuler la demande de journalisation du terminal.

Mises à jour du système Android avec Workspace ONE UEM

Vous pouvez vérifier et transférer les mises à jour des terminaux Android à l'aide de Workspace ONE UEM. Cela vous permet d'effectuer des tests afin de résoudre tous les problèmes de compatibilité, et de surveiller les mises à jour disponibles sur les terminaux, avant de transférer les mises à jour du microprogramme vers votre flotte de terminaux. La page de la console Mises

à jour d'Android répertorie l'ensemble des mises à jour du microprogramme disponibles pour les périphériques Android.

Les mises à jour sont répertoriées par date de publication et données, incluant des informations sur des OEM, un modèle et des opérateurs spécifiques. Chaque combinaison modèle/opérateur correspond à une mise à jour différente du microprogramme. Par exemple, vous pouvez voir Samsung Galaxy S7 pour T-Mobile et une mise à jour distincte pour Samsung Galaxy S7 avec Sprint. La liste peut être triée par OEM et par opérateur.

Pour les terminaux Samsung, vous devez vous enregistrer pour une licence Samsung E-FOTA afin d'obtenir des mises à jour. Les fonctionnalités ne sont disponibles qu'une fois l'enregistrement réalisé.

Mises à jour du microprogramme à distance Samsung Enterprise Firmware Over The Air (EFOTA)

Le microprogramme Samsung Enterprise Firmware Over The Air (EFOTA) vous permet de gérer et de restreindre les mises à jour du microprogramme sur les terminaux Samsung exécutant Android 7.0 Nougat et les versions ultérieures.

Le flux Samsung EFOTA implique l'enregistrement de vos paramètres EFOTA fournis par votre revendeur agréé, ce qui permet de « s'enregistrer à Enterprise FOTA » dans le profil de restrictions Android, et d'afficher et de sélectionner les mises à jour applicables à envoyer sur des terminaux.

Samsung EFOTA ne peut être configuré qu'au niveau Groupe organisationnel du client, de sorte que tous les terminaux enregistrés sous ce groupe organisationnel reçoivent des mises à jour. Envisagez de créer un groupe organisationnel distinct pour le test avant l'envoi sur tous les terminaux.

S'inscrire aux mises à jour du microprogramme à distance Samsung Enterprise Firmware Over The Air

Utilisez la page Paramètres système des terminaux et utilisateurs pour entrer vos paramètres EFOTA fournis par Samsung ou votre revendeur agréé.

Procédure

1 Accédez à **Terminaux > Paramètres des terminaux > Terminaux et utilisateurs > Android > Samsung Enterprise FOTA**.

2 Entrez les paramètres :

Paramètre	Description
ID du client	Entrez l'ID fourni par votre revendeur agréé.
Licence	Entrez la licence fournie par votre revendeur agréé.
ID client	Entrez l'ID client fourni par votre revendeur agréé.
Client Secret	Entrez la clé secrète du client fournie par votre revendeur agréé.

3 Cliquez sur **Enregistrer**.

Configurer le profil de restrictions (Samsung EFOTA)

Les profils de restrictions verrouillent les fonctionnalités natives des périphériques Android et varient d'un fabricant à un autre. L'activation de la restriction « S'inscrire à Enterprise FOTA » verrouille la version du microprogramme actuelle des terminaux affectés.

Ce champ dans le profil de restrictions ne devient disponible que lorsque vous sélectionnez Samsung dans le champ paramètres OEM.

Procédure

1 Accédez à **Terminaux > Profils et ressources > Profils > Ajouter > Ajouter un profil > Android > Restrictions**.

2 Cliquez sur **Configurer**

3 Activez **S'inscrire à Enterprise FOTA**.

Autoriser la mise à niveau de OTA doit être activée ou les mises à jour du microprogramme seront bloquées.

4 Cliquez sur **Enregistrer et publier**.

Publier les mises à jour du microprogramme (Android)

La page de la console Mises à jour d'Android répertorie l'ensemble des mises à jour du microprogramme disponibles pour les périphériques Android. Elle vous permet également d'afficher des versions du microprogramme spécifiques et de choisir d'inviter l'utilisateur à installer la mise à jour.

Procédure

1 Accédez à **TerminauxMises à jour du terminal**.

2 Affichez et sélectionnez le bouton radio en regard de la mise à jour souhaitée.

3 Sélectionnez **Gérer la mise à jour**.

4 Configurez les paramètres :

Paramètres	Description
Méthode d'installation	Sélectionnez **Installation automatique** pour choisir la période de planification des mises à jour. Sélectionnez **Installer à la demande** et les utilisateurs seront invités à accepter les mises à jour du microprogramme avant qu'elles ne soient installées sur leur terminal.
Début du déploiement	Planifiez la date et l'heure de début de la mise à jour. Les mises à jour peuvent être planifiées jusqu'à 30 jours à l'avance avec une fenêtre de mise à jour maximale de 7 jours. Les mises à jour dans cette fenêtre seront publiées sur les terminaux toutes les 4 heures dans le fuseau horaire du serveur.
Fin du déploiement	Planifiez la date et l'heure de fin de la mise à jour.

Paramètres	Description
Fuseau horaire du serveur	Ce champ est en lecture seule car il est généré à partir du serveur.
Réseau	Indiquez si vous voulez déployer les mises à jour lorsque les terminaux sont connectés via **Wi-Fi uniquement** ou via **N'importe quel réseau**.

5 Sélectionnez **Publier**. La fenêtre Gérer la mise à jour se ferme et la console UEM renvoie à la page Mises à jour.

a Si, pour une raison quelconque, vous devez annuler ou modifier la mise à jour, sélectionnez la mise à jour souhaitée et cliquez sur **Annuler la planification** dans la fenêtre Gérer la mise à jour.

Les mises à jour étant regroupées par lots de terminaux, les terminaux mis à jour précédemment ne peuvent pas être révoqués.

Attestation SafetyNet

L'attestation SafetyNet est une API Google utilisée pour valider l'intégrité du terminal garantissant que le terminal n'est pas compromis.

SafetyNet valide les informations logicielles et matérielles sur le terminal et crée un profil pour ce terminal. Cette attestation aide à déterminer si un terminal particulier a été altéré ou modifié. Lorsque Workspace ONE UEM Console exécute l'API d'attestation SafetyNet et signale que le terminal a été compromis, la page Détails du terminal de UEM Console signale que le terminal est compromis. Si l'attestation SafetyNet détecte que le terminal est compromis, la seule façon de restaurer un état de terminal compromis consiste à réenrôler le terminal affecté.

Il est important de savoir que l'attestation SafetyNet ne réévalue pas les statuts compromis après leur signalement initial.

L'attestation SafetyNet est uniquement prise en charge avec Workspace ONE Intelligent Hub.

Pour plus d'informations, reportez-vous à Activation de l'attestation SafetyNet.

Activation de l'attestation SafetyNet

Activez l'API d'attestation SafetyNet dans UEM Console pour valider l'intégrité d'un terminal et déterminer si un terminal a été compromis.

Procédure

1 Naviguez vers **Groupes et paramètres > Tous les paramètres > Applications > Paramètres et stratégies > Paramètres > Paramètres personnalisés**

2 Collez le code XML personnalisé suivant dans le champ Paramètres personnalisés :
```
{ "SafetyNetEnabled":true }
```

3 Enregistrez le code XML personnalisé.

4 Vérifiez SafetyNet dans l'onglet Résumé de la page **Détails du terminal** de UEM Console. Si vous ne voyez pas l'état de l'attestation SafetyNet, vous pouvez envoyer une commande distante pour redémarrer le terminal.

Pour plus d'informations sur les commandes du terminal, reportez-vous à Chapitre 6 Gestion des terminaux Android avec Workspace ONE UEM

Fonctionnalités des profils spécifiques pour Android

Les matrices des fonctionnalités donnent un aperçu des fonctions clés spécifiques des OS disponibles et mettent en avant les plus importantes d'entre elles pour l'administration des terminaux pour Android.

Fonctionnalité	Profil professionnel	Géré pour le travail Les profils de terminaux
Contrôle des applications		
Désactiver l'accès aux applications sur liste noire	✓	✓
Empêcher la désinstallation des applications obligatoires	✓	✓
Activer la politique de mise à jour système		✓
Gestion des autorisations au moment de l'exécution	✓	✓
Navigateur		
Autoriser les cookies	✓	✓
Autoriser les images	✓	✓
Activer JavaScript	✓	✓
Autoriser les fenêtres pop-up	✓	✓
Autoriser le suivi de la localisation	✓	✓
Configurer les paramètres proxy	✓	✓
Forcer Google SafeSearch	✓	✓
Forcer le mode sécurisé de Youtube	✓	✓
Activer Touch to Search	✓	✓
Activer le moteur de recherche par défaut	✓	✓
Activer le gestionnaire de mots de passe	✓	✓
Autoriser les autres pages d'erreur	✓	✓
Activez la saisie automatique	✓	✓
Activer l'impression	✓	✓
Activer la fonction proxy de compression des données	✓	✓
Activer la navigation sécurisée	✓	✓
Désactiver la sauvegarde de l'historique du navigateur	✓	✓
Empêcher de continuer après une alerte de navigation sécurisée	✓	✓
Désactiver le protocole SPDY	✓	✓

Fonctionnalité	Profil professionnel	Géré pour le travail Les profils de terminaux
Activer la prédiction du réseau	✓	✓
Activer les fonctionnalités de plateformes Web obsolètes pour une durée limitée	✓	✓
Forcer la recherche sécurisée	✓	✓
Disponibilité de la navigation privée	✓	✓
Autorise la connexion à Chromium	✓	✓
Activer la suggestion de recherche	✓	✓
Autoriser la traduction	✓	✓
Autoriser les signets	✓	✓
Autoriser l'accès à certaines URL	✓	✓
Bloquer l'accès à certaines URL	✓	✓
Définir la version SSL minimale	✓	✓
Politique de mot de passe		
Demander à l'utilisateur de définir un nouveau code d'accès	✓	✓
Nombre maximum de tentatives de mot de passe ayant échoué	✓	✓
Autoriser les codes d'accès simples	✓	✓
Mot de passe alphanumérique autorisé	✓	✓
Définir le délai de verrouillage du terminal (min)	✓	✓
Définir la durée de vie maximale du code d'accès	✓	✓
Longueur de l'historique du mot de passe	✓	✓
Longueur de l'historique du mot de passe	✓	✓
Définir la longueur minimale du code d'accès	✓	✓
Définir le nombre minimum de chiffres	✓	✓
Définir le nombre minimum de minuscules	✓	✓
Définir le nombre minimum de majuscules	✓	✓
Définir le nombre minimum de majuscules	✓	✓
Définir le nombre minimum de caractères spéciaux	✓	✓
Définir le nombre minimum de symboles	✓	✓
Commandes		
Autoriser l'effacement des données professionnelles	✓	✓
Autoriser la réinitialisation du terminal		✓
Autoriser l'effacement du conteneur ou du profil	✓	
Autoriser l'effacement de la carte SD		✓
Verrouillage du terminal	✓	✓
Autoriser le verrouillage du conteneur ou du profil		

Fonctionnalité	Profil professionnel	Géré pour le travail Les profils de terminaux
E-mail		
Configuration de la messagerie native	✓	✓
Autoriser la synchronisation du calendrier et des contacts	✓	✓
Sécurité		
Configurer les types VPN	✓	✓
Activer le VPN par application (disponible uniquement pour les clients VPN spécifiques)	✓	✓
Utiliser l'ouverture de session Web pour l'authentification (disponible uniquement pour les clients VPN spécifiques)	✓	✓
Définir le proxy global HTTP	✓	✓
Autoriser la connexion données au Wi-Fi	✓	✓
VPN toujours actif	✓	✓
Chiffrement		
Exiger le chiffrement complet du terminal	✓	✓
Signaler le statut de chiffrement		

Restrictions spécifiques pour Android

Cette matrice fournit un aperçu des configurations de restrictions proposées par type de propriété du terminal.

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Fonctionnalités des terminaux		
Autoriser le rétablissement des paramètres d'origine	✓	✓
Autoriser la capture d'écran	✓	✓
Autoriser l'ajout de comptes Google	✓	✓
Autoriser la suppression du compte professionnel Android	✓	
Autoriser les appels téléphoniques sortants	✓	
Autoriser l'envoi/la réception de SMS	✓	
Autoriser les modifications d'identifiants	✓	
Autoriser toutes les fonctionnalités Keyguard	✓	
Autoriser l'appareil photo Keyguard	✓	
Autoriser les notifications Keyguard	✓	
Autoriser le capteur d'empreinte digitale Keyguard	✓	✓
Autoriser le statut Keyguard Trust Hub	✓	✓

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Autoriser les notifications non rédigées Keyguard	✓	
Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur CA (Android 6.0 et versions ultérieures)	✓	
Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur USB (Android 6.0 et versions ultérieures)	✓	
Forcer l'activation de l'écran lorsque le terminal est branché sur un chargeur sans fil (Android 6.0 et versions ultérieures)	✓	
Autoriser la modification du papier peint (Android 7.0 et versions ultérieures)	✓	
Barre d'état autorisée	✓	
Autoriser Keyguard (Android 6.0 et versions ultérieures)	✓	
Autoriser l'ajout d'utilisateurs		
Autoriser la suppression des utilisateurs		
Autoriser le démarrage sécurisé (Android 6.0 et versions ultérieures)	✓	
Autoriser la modification du papier peint (Android 7.0 et versions ultérieures)		
Autoriser le changement de l'icône utilisateur (Android 7.0 et versions ultérieures)	✓	✓
Autoriser l'ajout/la suppression de comptes	✓	✓
Limiter l'interface utilisateur du système (toasts, activités, alertes, erreurs, superpositions)	✓	
Application		
Autoriser la caméra	✓	✓
Autoriser Google Play	✓	✓
Autoriser le navigateur Chrome	✓	
Autoriser l'installation d'applications non disponibles dans les magasins publics	✓	✓
Autoriser la modification d'applications dans les paramètres	✓	
Autoriser l'installation d'applications	✓	✓
Autoriser la désinstallation d'applications	✓	✓
Autoriser la désactivation de la vérification d'application	✓	✓
Ignorer le tutoriel d'utilisation et les conseils d'introduction	✓	✓
Autoriser la mise sur liste blanche des services d'accessibilité	✓	
Synchronisation et stockage		
Autoriser le débogage USB	✓	
Autoriser le stockage de masse USB****	✓	

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Autoriser l'ajout de support de stockage physique	✓	
Autoriser le transfert de fichier par port USB	✓	
Autoriser le service de sauvegarde (Android 8.0 et versions ultérieures)****		
Réseau		
Autoriser les changements de Wi-Fi	✓	
Autoriser la connexion Bluetooth	✓	
Autoriser Bluetooth (Android 8.0 et versions ultérieures)	✓	
Autoriser le partage des contacts par Bluetooth (Android 8.0 et versions ultérieures)*****	✓	
Autoriser les connexions Bluetooth sortantes*****	✓	✓
Autoriser le partage de toutes les connexions	✓	
Autoriser les modifications de VPN	✓	
Autoriser les modifications de réseau mobile	✓	
Autoriser le NFC	✓	
Autoriser les modifications de profils Wi-Fi gérés (Android 6.0 et versions ultérieures)	✓	
Professionnel et personnel		
Autoriser la copie du presse-papiers entre les applications professionnelles et personnelles		✓
Autoriser les applications professionnelles à accéder aux documents depuis les applications personnelles		✓
Autoriser les applications personnelles à accéder aux documents depuis les applications professionnelles		✓
Autoriser les applications personnelles à partager des documents avec les applications professionnelles		○
Autoriser les applications professionnelles à partager des documents avec les applications personnelles		
Autoriser l'affichage des coordonnées professionnelles de l'ID sur le cadran du téléphone		✓
Autoriser l'ajout de widgets professionnels sur l'écran d'accueil personnel		✓
Autoriser l'ajout des contacts professionnels à l'application de contacts personnels (Android 7.0 et versions ultérieures)		
services de localisation		
S'applique aux terminaux gérés uniquement.		
Autoriser la fonction Aucun accès à la localisation	✓	✓
Autoriser la fonction Accès à la localisation	✓	✓

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Autoriser la localisation GPS uniquement	✓	✓
Autoriser l'économie d'énergie en limitant les mises à jour GPS	✓	✓
Autoriser la localisation de haute précision uniquement	✓	✓
Samsung Knox		
Les paramètres Samsung Knox s'affichent uniquement lorsque le champ **Paramètres OEM** est défini sur **Activé** et que Samsung est sélectionné dans le champ **Sélectionnez l'OEM**.		
Fonctionnalités des terminaux		
Autoriser le mode avion	✓	
Autoriser le microphone	✓	
Autoriser les positions fictives	✓	
Autoriser le presse-papiers	✓	
Autoriser la fonction « Éteindre »	✓	
Clé d'origine autorisée	✓	
Autoriser l'enregistrement audio lorsque le microphone est autorisé	✓	
Autoriser à filmer lorsque la caméra est autorisée	✓	
Autoriser la suppression de comptes e-mail	✓	
Autoriser l'arrêt de l'activité lorsque la session est inactive	✓	
Autoriser les utilisateurs à établir une limite du processus d'arrière-plan	✓	
Autoriser les écouteurs	✓	
Synchronisation et stockage		
Autoriser le déplacement de la carte SD	✓	
Autoriser une mise à niveau à distance (OTA)	✓	
Autoriser la synchronisation automatique des comptes Google	✓	
Autoriser la protection en écriture de la carte SD	✓	
Autoriser le stockage du contrôleur hôte USB	✓	
Win32		
Autoriser les modifications de paramètres	✓	
Autoriser les options du développeur	✓	
Autoriser les données en arrière-plan	✓	
Reconnaissance vocale autorisée	✓	
Autoriser les rapports d'incidents Google	✓	
Autoriser S Beam	✓	
Autoriser les demandes d'identifiants	✓	

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Autoriser S Voice	✓	
Autoriser les utilisateurs à interrompre les applications signées du système	✓	
Bluetooth		
Autoriser la connexion du bureau via Bluetooth	✓	
Autoriser le transfert de données Bluetooth	✓	
Autoriser les appels sortants via Bluetooth	✓	
Autoriser la détection du Bluetooth	✓	
Activer le mode sécurisé Bluetooth	✓	
Sécurité		
Autoriser le Wi-Fi	✓	
Autoriser les profils Wi-Fi	✓	
Wi-Fi non sécurisé autorisé	✓	
"Autoriser uniquement les connexions VPN	✓	
Autoriser le VPN	✓	
Autoriser la connexion automatique au Wi-Fi	✓	
Données mobiles autorisées	✓	
Autoriser le Wi-Fi direct	✓	
Itinérance		
Autoriser la synchronisation automatique en itinérance	✓	
Autoriser la synchronisation automatique lorsque l'itinérance est désactivée	✓	
Autoriser les appels en itinérance	✓	
Utilisation des données lors de l'itinérance	✓	
Autoriser l'envoi de messages en itinérance	✓	
Téléphone et données		
Autoriser les appels non urgents	✓	
Autoriser les utilisateurs à établir une limite des données mobiles	✓	
Autoriser les messages Push WAP	✓	
Restrictions matérielles		
Touche Menu autorisée	✓	
Touche Retour autorisée	✓	
Autoriser la touche Recherche	✓	
Autoriser le gestionnaire de tâches	✓	
Autoriser la barre système	✓	

Fonctionnalité	Mode Terminaux gérés pour le travail	Mode Profil professionnel
Autoriser la touche de volume	✓	
Sécurité		
Autoriser les paramètres de l'écran de verrouillage	✓	
Autoriser la récupération du micrologiciel	✓	
Partage de connexion		
Autoriser le partage de connexion USB	✓	
Restrictions sur les MMS		
Autoriser les MMS entrants	✓	
Autoriser les MMS sortants	✓	
Divers		
Configurer la police de caractères du terminal	✓	
Configurer la taille de la police du terminal	✓	
Autoriser les utilisateurs à interrompre les applications signées du système	✓	
"Autoriser uniquement les connexions VPN	✓	